CCM v4.0 実施ガイドライン

セキュリティ責任共有モデルによる
クラウドの保護

Version 2.0

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

CCM WG について

クラウドコントロールマトリックス（CCM）ワーキンググループ（WG）は、クラウドセキュリティの専門家、監査人、事業者、クラウドのプロバイダーと利用者の両方を代表する多数の組、コンサルティング／監査会社など、クラウド業界の専門家で構成されている。

CCM v4.0 とその実装ガイドラインは、グループの経験とフィードバックに基づく共同作業から生まれたものである。その結果、CCM v4.0 は、ベンダー中立のクラウドセキュリティとプライバシー管理のフレームワークとして、コミュニティにとって最良のものの 1 つとなりました。

Co-chair は WG の活動を監督する。これらの人々は、クラウドサービスプロバイダー（CSP）、クラウドサービス利用者（CSC）、クラウド監査人という、クラウド業界における 3 つの役割を代表する経験豊富な専門家である。

全ての寄稿は個人的なものであり、寄稿者または寄稿者の所属団体によるコミットメントや意見を構成するものではない。

謝辞

Lead Authors

Lefteris Skoutaris (Team Lead)
Michael Bayere
Akshay Bhardwaj
Geoff Bird
Daniele Catteddu
John Goodman
Ryan Green
Gaurav Gupta
Alana James-Aikins
Arpitha Kaushik
Yazad Khandhadia
Simon Leech
Debjyoti Mukherjee
Johan Olivier
John B. Oseh
Duronke Owoleso
Michael Ratemo
Ankit Sharma
David Skrdla
David Souto Rial
Gjoko Stamenkov
Kerry Steele
Rachelle Summers
Akash Verma

Contributors

Rinaldo Angelicola
Jon-Michael Brook
Daniele Catteddu
Troin Devon Artis
Jeremy Dannenmuller
Lanre Fagbayi
Alec Fernandez
Ed Fuller
Sarita Garg
David Gentry
Victoria Geronimo
Polly Gitau
Trevor Green
Sanjeev Gupta
Brian Hames
Hongtao Hao
Shamik Kacker
Jari Kiero
Hadir Labib
Chamber Lain Law
Jeff Levine
Fotis Loukos
Claus Matzke
Ahmed Mohammed
Mark Novak
Ashwani Parashar
Julien Perini
Alexander Rebo
Carlos Rombaldo Jr.
Gaurav Singh
Mark Sontz
Soo Stahl
Elizabeth Stremlau
Rachelle Summers
Katalin Szenes
Jonathan Villa

CCM Leadership

Jon-Michael Brook
Daniele Catteddu
Sean Cordero
David Nickles
Lefteris Skoutaris

CSA Global Staff:

Claire Lehnert
Stephen Lumpe

日本語版提供に際しての告知及び注意事項

本書「CCM v4.0 実施ガイドライン セキュリティ責任共有モデルによるクラウドの保護」は、Cloud Security Alliance (CSA)が公開している「CCM v4.0 Implementation Guidelines Securing the Cloud with the Shared Security Responsibility Model」の日本語訳です。本書は、CSA ジャパンが、CSA の許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2024 年 12 月 02 日	日本語版 1.0	初版発行

CSA ジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス（CSA ジャパン）は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

１．　責任の限定
CSA ジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。
(1)　本書の内容の真正性、正確性、無誤謬性
(2)　本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと

(3)　本書の内容に基づいて行われた判断や行為がもたらす結果
(4)　本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

２．　二次譲渡の制限
本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。
ただし、以下の場合は本項の例外とします。
(1)　本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2)　本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3)　CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4)　転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

３．　本書の適切な管理
(1)　本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2)　本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3)　本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4)　本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

４．　原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

５.　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「CCM v4.0 実施ガイドライン セキュリティ責任共有モデルによるクラウドの保護」は、CSA ジャパン会員の有志により行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

石井　英男
笠松　隆幸
釜山　公徳
木村　チエ
高尾　美由紀
高橋　久緒
松崎　祥三
満田　淳
村田　紗矢子
諸角　昌宏
山口　弘行
山澤　昌夫
山下　亮一

目次

エグゼクティブ サマリー

クラウドセキュリティアライアンス（CSA）のクラウドコントロールマトリックス（CCM）は、クラウドサービスのセキュリティリスクのセキュアな実装、評価、管理を求めるクラウドサービスプロバイダー（CSP）とクラウドサービス利用者（CSC）のための基本的なセキュリティ原則、管理策、管理策の標準を提供する。CSA CCM は、CSA のセキュリティガイダンス[1]に沿った詳細な管理フレームワークを提供する。このガイダンスでは、「最も重要なセキュリティ上の考慮点は、クラウドプロジェクトにおいて誰が何に責任を持つかを正確に把握することである」と述べられている。CCM には、クラウドセキュリティ責任共有モデル（SSRM）の定義と事前管理のための包括的な構造が盛り込まれ、クラウドエコシステム全体の透明性と説明責任が確保されている。2021 年に公表されたクラウドセキュリティアライアンスのクラウドコントロールマトリックス第 4 版（CCM v4.0）には、中核的なセキュリティとプライバシーの管理策と追加コンポーネントが含まれている。これには、CCM Implementation Guideline（本書に含まれる）、Consensus Assessment Initiative Questionnaire（CAIQ）、CCM Controls Auditing Guideline[2]が含まれる。また、CCM v4.0 には、CCM 管理策に関する有用な支援情報も含まれている。この情報には、SSRM における管理策の所有の割り当て、管理策の適用範囲と適用可能性に関する情報（アーキテクチャとの関連性、業界で認められている他のセキュリティフレームワーク（ISO/IEC、AICPA、NIST、FedRAMP など）とのマッピングなど）が含まれている。これらの作業は、CSA チームによって定期的にレビューされ、強化されている。

本書（CCM 実装ガイドライン）は、CCM 管理策の適用を支援し、CCM 管理策仕様の実装に関するさらなるガイダンスと推奨を提供することを目的としている。本書は、CSP と CSC の間のセキュリティ責任の明確な境界線を確立し、実装プロセスをより明確にし、説明責任を果たすという重要なニーズに対応するものである。各セキュリティ管理策の中でセキュリティ実装の責任を割り当てることで、クラウド組織は、共有セキュリティの複雑さを効果的に乗り切ることができる。このアプローチにより、CSP と CSC の双方が管理策の実装におけるそれぞれの役割を理解し、クラウドエコシステム全体のセキュリティポスチャを強化する協調的な環境が醸成される。

ただし、本書は CCM 管理策の導入に関する「ハウツー」マニュアルを意図したものではない。CCM 管理策の性質上、その運用は IT/サービスアーキテクチャ、使用するテクノロジーの種類、直面するリスク、適用される規制、組織のポリシー、その他の重要な要因に大きく依存する。したがって、CSA は、全ての組織とクラウドサービスの実装に適切な、詳細で規定的なガイダンスを提供することはできない。

CCM 実施ガイドラインは、クラウドサービスの実装とセキュリティ確保、および CCM 管理策の使用における

[1] https：//cloudsecurityalliance.org/research/guidance/ ,accessed on 5 March 2024.

[2] Released in December 2021.

CSP と CSC の共通の経験に基づく、CCM ワーキンググループの有志による共同成果物である。ワーキンググループの洞察は、組織がどのようにできるかを含む以下の無数のトピックや質問をカバーしている。

- 管理策を初めて導入するか、既存の導入を改善しているか?
- CCM マッピングを通じて、複数のフレームワークにわたるコントロールの実装を案内しているか?
- クラウドの実装における CSP と CSC のセキュリティ責任を明確にし、理解しているか?
- CAIQ と連携して CSP の実施評価を実施しているか?
- 組織のセキュリティポリシーに規定すべき最も効果的なベストプラクティスを特定しているか?
- クラウドセキュリティのベストプラクティスを CSP との契約条項に盛り込んでいるか?
- 特定のクラウドプラットフォームまたはアーキテクチャ内で CCM 管理策を活用し、実装しているか?

1　はじめに

1.1　クラウドコントロールマトリックスとは何か

CCM は、クラウドコンピューティングに関連するセキュリティとプライバシーの懸念に対処する一連の構造化され標準化された管理策を提供するために開発された包括的なサイバーセキュリティ管理フレームワークであり、組織がクラウドサービスの採用に関連するリスクを評価・管理するのに役立つ。2010 年に作成された当初、コンピューティングリスク管理は、従来のコンピューティングインフラへの対応にのみ焦点が当てられていた。CCM は、クラウドコンピューティングにおけるセキュリティとプライバシーのリスク管理を促進するために作成された。

このフレームワークは、CSA セキュリティガイダンス（CSA Security Guidance）v4 と密接に連携している。Security Guidance v4 がクラウドセキュリティのハイレベルな原則を提供しているのに対して、CCM はそれらの原則を、セキュリティを達成し維持するための具体的で実行可能な管理策に変換している。CSA は、CCM を CSA セキュリティガイダンスの手引きとして使用し、両者の補完的な価値を最適化することを組織に推奨している。

さらに、CCM 実施ガイドライン（本書）は、CCM の各管理策を実施、管理、および維持する際の CSP と CSC のセキュリティ責任を明確にするのに役立つ SSRM ガイドラインを提供することにより、CCM フレームワークを補完する。

CCM は、技術やセキュリティ環境の変化に対応するため、時間の経過とともに進化し、クラウドセキュリティの課題の動的な性質に対処する上で、適切かつ効果的なフレームワークであり続ける。CCM バージョン 4 は、このフレームワークの最新版であり、クラウド技術の全ての主要な側面をカバーする 17 のドメインにわたる 197 の管理目標を特徴とし、複数の業界およびベストプラクティスのセキュリティ標準、規制、フレームワークにマッピングされている。

1.1.1　CCM の目的と範囲

CCM の主な目的は、クラウドコンピューティングエコシステムにおける効果的かつ包括的なセキュリティとプライバシーのリスク管理を推進・促進することである。組織の種類（CSP または CSC）や規模（大企業と中小企業など）、またはクラウドの提供やデプロイのサービスモデル（IaaS、PaaS、または SaaS）にかかわらず、CCM は、クラウドコンピューティングエコシステムにおけるセキュリティおよびプライバシのリスク

管理を効果的かつ包括的に推進および促進する、

CCM は、セキュリティ要件を定義、実装、実施し、その実装を監視するために使用できる。CCM は、企業が社内の組織的、運用的、法的な規定を、クラウドに関連する標準化されたポリシー、手順、技術的な管理目標に変換するのを支援する。CCM はまた、社内外の評価や監査のためのツールでもある。CCM は、CAIQ と連携して使用されるように設計されており、CAIQ は、CCM のコントロールが満たされているかどうかを判断するための「Yes」または「No」の質問を提供する。両文書は、監査人が、組織が内部ガバナンスポリシーに従い、法的及び規制上の義務を果たしているかどうかを理解するのに役立つ。

例えば、内部リスクアセスメントに基づき、ある組織が製造工程に関連する情報の機密性、完全性、可用性を保護する必要性を特定するとする。データセットは、クラウドデータベースに保存され、複数のクラウドベースのアプリケーションで処理されるため、機密性と重要性のレベルはさまざまである。組織は、CCM を使用して特定のポリシー、手順、技術要件を特定し、組織のセキュリティプログラムに含める管理目標を定義することができる。組織は、これらの管理目標を使用して、内部ユーザー、ビジネスパートナー、CSP に関連する強制事項を実施し、内部ポリシーと外部コンプライアンス要件の遵守を監視する。

したがって、組織は、本文書の推奨事項やガイドラインを活用しながら、各組織固有の環境に固有のニーズを満たし、リスクを管理するための管理策を導入する必要がある。

1.1.2 CCM の構成

CCM v4.0 は、17 のセキュリティドメインと 197 の管理策で構成されている。17 のドメインは、CSA のセキュリティガイダンス文書に基づいており、ISO 27001：2022 などの主要なフレームワークから着想を得ている。CCM の各ドメインは、管理策がどのカテゴリーに該当するかを定義している。CCM は、既存のフレームワークとの親和性を活用するために、意図的にクラウドを意識しない既存の(先行例としての)情報セキュリティフレームワークと構成を合わせた設計としている。

A&A Audit and Assurance	IAM Identity & Access Management
AIS Application & Interface Security	IPY Interoperability & Portability
BCR Business Continuity Mgmt & Op Resilience	IVS Infrastructure & Virtualization Security
CCC Change Control and Configuration Management	LOG Logging and Monitoring
CEK Cryptography, Encryption and Key Management	SEF Sec. Incident Mgmt, E-Disc & Cloud Forensics
DCS Datacenter Security	STA Supply Chain Mgmt, Transparency & Accountability
DSP Data Security and Privacy	TVM Threat & Vulnerability Management
GRC Governance, Risk Management and Compliance	UEM Universal EndPoint Management
HRS Human Resources Security	

図 1：CCM v4 クラウドセキュリティドメインとその略語の一覧

A&A	監査と保証	**IAM**	アイデンティティとアクセス管理
AIS	アプリケーションとインタフェースのセキュリティ	**IPY**	相互運用性と移植容易性
BCR	事業継続管理とオペレーショナルレジリエンス	**IVS**	インフラストラクチャと仮想化のセキュリティ
CCC	変更管理と構成管理	**LOG**	ロギングと監視
CEK	暗号、暗号化、鍵管理	**SEF**	セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジック
DCS	データセンターセキュリティ	**STA**	サプライチェーン管理、透明性、説明責任
DSP	データセキュリティとプライバシーのライフサイクル管理	**TVM**	脅威と脆弱性管理
GRC	ガバナンス、リスク、コンプライアンス	**UEM**	ユニバーサルエンドポイント管理
HRS	人的リソースセキュリティ		

図 1：CCM v4 でのクラウドセキュリティドメイン分類とその頭文字

1.1.3 CCM ドメインの説明

CCM v4.0 には、17 のクラウドセキュリティドメインが含まれている。これらのドメインを、それぞれに固有の目的と用途の説明と併せて以下に示す。

（A&A）監査と保証

監査及び保証（Audit and Assurance：A&A）」ドメインは、6 つの管理規定から構成され、CCM に含まれる管理プロセスを含む重要なプロセスに関する重要な意思決定、意思疎通、及び報告に必要な信頼性を、評価、検証、及び検証活動を通じて CSP 及び CSC に提供し、確立することを可能にする。本ドメインは、CSP 及び CSC が、監査計画、リスク分析、セキュリティ管理策の評価、結論、是正、及び報告、並びに証明書及び裏付け証拠のレビュー及び依存を支援するために、それぞれの監査管理プロセスを定義し、実施することを支援するように設計されている。

SSRM は、クラウド環境における A&A コントロールの実施における CSP と CSC の責任を明確にしている。CSP と CSC はともに、強固な監査・保証ポリシーの確立、定期的なセキュリティ評価の実施、関連する標準や規制の要求事項の遵守について、独立した責任を負う。

CSP と CSC はそれぞれ、SSRM に沿った A&A 管理策を実施し、CCM の対象となるコントロールプロセスについて、両者が独立に特定の保証ニーズを満たすようにする。

（AIS）アプリケーションとインタフェースのセキュリティ

アプリケーションおよびインタフェースのセキュリティ（AIS ドメインは、7 つの管理仕様から構成され、クラウドで使用されるソフトウェアとインタフェースのセキュリティ確保に重点を置き、アプリケーションの設計および開発段階におけるクラウドランドスケープに対するリスクの特定と軽減を支援する。CSP がクラウド環境インタフェースションとインタフェースの完全性、機密性、および可用性を確保するためには、このドメインでクラウドセキュリティ管理策を実装することが極めて重要である。

SSRM において、CSP は、セキュアなコーディング手法に従い、セキュアなアプリケーションと API を提供する基盤となるインフラストラクチャのセキュリティを確保し、アプリケーションセキュリティベースラインを確立し、自動化されたアプリケーションセキュリティテストを実施し、セキュアなランタイム環境の可用性と保守性を確保する責任を負う。CSC は、アプリケーションとインタフェースのセキュア性を確保し、アプリケーションセキュリティベースラインを確立し、クラウドのデプロイモデルに応じてベストプラクティスに従って、セキュリティ設定の適切な構成、アップグレード、新システムや新バージョンのシステム及びアプリケーションのセキュアな統合を確保する責任を負う。

各当事者はセキュアなクラウド環境から恩恵を受け、アプリケーションの脆弱性リスクを低減し、データの機密性と完全性を確保する。コラボレーションはコミュニケーションを促進し、プロアクティブな脅威対応と迅速なインシデント解決を可能にする。

（BCR）事業継続管理とオペレーショナルレジリエンス

事業継続管理とオペレーショナルレジリエンス（Business Continuity Management and Operational Resilience)」のドメインは、11 の管理規定から構成され、重要なビジネスプロセス、インフラ、およびサービスの保護、中断の影響の最小化、および潜在的に破壊的な事象に直面した場合の事業継続性の確保に重点を置いている。このドメインにおけるクラウドセキュリティ管理策の実装は、CSP と CSC の両方にとって、中断のないサービスを提供し、オペレーショナルレジリエンスを確保するために最も重要である。

CSP と CSC は、クラウド環境におけるインフラのレジリエンスと事業継続性を確保する上で、それぞれ異なる役割を担っているが、相互に関連し合っている。CSP は、クラウドとクラウドサービスの継続性とオペレーショナルレジリエンスを管理する堅牢な技術、サービス、ポリシー、手順、およびプロセスを計画、開

発、実装する責任を負う。CSC は、クラウド上にホストされているデータその他のリソースや資産に関連する潜在的なビジネス中断リスクを評価し、管理する責任を負う。リスク分析に基づき、CSC は各自の要件と優先順位に合わせた強固な事業継続性計画を策定し、実施する必要がある。

CSP と CSC は、それぞれの責任と協力関係を果たすことで、障害に直面しても企業が事業を継続できるよう、レジリエントで信頼性の高いクラウドオペレーションの維持に貢献する。

（CCC）変更管理と構成管理

変更管理と構成理のドメインには 9 つの管理策が含まれ、クラウド環境への変更を管理し保護することに重点を置き、変更によって脆弱性がもたらされたり、クラウド環境のシステムのセキュリティが損なわれたりしないようにする。変更を効果的に管理することは、CSP と CSC の両方にとって、安定したセキュアなクラウドサービスを維持するために極めて重要である。

サービスが SaaS（Software as a Service）として提供される場合、CSP は通常、クラウドインフラストラクチャ内での変更実施に先立ち、構成ベースラインの確立、変更、リスクアセスメントの実施、および全ての変更が適切な認可の対象となることを保証し、セキュアな変更管理プロセスを確立および維持する責任を負う。IaaS（Infrastructure as a Service）の場合、CSP は通常、基盤となるネットワーキングとインフラストラクチャを、最大でも基本オペレーティングシステムレベルまでしか提供しないため、全てのオペレーティングシステムレベルとアプリケーションレベルの構成の変更管理は、CSC が設計、実装、検証、および管理する必要がある。PaaS（Platform as a Service）の場合、CSP は基盤となるインフラストラクチャとオペレーティングシステムの構成をアプリケーションレイヤーに提供する。CSC はアプリケーションの構成と実装を設計する必要があるため、適切な変更管理プロセスを CSC が確立し、必要なアプリケーションが脆弱性を導入することなく望ましい結果を得るようにセキュアに構成され、確立された構成ベースラインからの逸脱を監視するようにしなければならない。

CSP と CSC はともに、合意されたサービス要件をサポートするために、確立されたベースラインに従ってセキュアなクラウド環境が構成され維持されることを保証するために CCM 管理策を活用する。このドメインは、関連する CSP または CSC の変更管理権限が構成変更を承認した後に、IT 資産構成が承認されたベースラインに対してのみ変更されることを保証する。

（CEK）暗号、暗号化、鍵管理

暗号・暗号化・鍵管理（CEK）ドメインは、暗号技術、暗号化、鍵管理の実践により CSC のデータを保護することを目的とした 21 の管理仕様から構成される。CEK ドメインは、様々な規制標準の暗号化及び鍵管理要

件への準拠を保証し、クラウド環境における機微情報の機密性と完全性を促進する上で、重要な役割を果たす。

SSRM では、CSP は通常、スコープ定義が業界のベストプラクティスと規制要件に合致するようにしながら、暗号技術、暗号化、および鍵管理のガバナンスを監督する。CSP は、基盤となるインフラストラクチャと暗号化サービスを管理し、セキュアな鍵の保管と暗号化機能を提供する責任を負う。CSC は、特定のアプリケーションおよびデータにおける役割と責任の定義および割り当て、アップロード前の機微データの暗号化、独自の暗号鍵の管理、並びに特定の環境における暗号リスクおよび変更管理プロセスの実装について責任を負う。

CSP と CSC が協業して CEK のセキュリティ管理を実施することで、双方にメリットがもたらされる。CSP にとっては、CSC のデータの機密性と完全性が促進され、クラウドサービス全体のセキュリティとコンプライアンスが強化される。CSC にとっては、協業によって各自の暗号要件が確実に満たされることになる。

（DCS）データセンターセキュリティ

このドメインは、CSC のデータとアプリケーションをホストする CSP の物理的なインフラと環境のセキュア性を確保するために CSP に不可欠な 15 の管理仕様で構成される。これには、不正アクセスや環境上の危険などのセキュリティ上の脅威に対する、物理的インフラや機器などの物理的資産の保護が含まれる。SSRM では、CSP はデータセンターの物理的インフラ、環境管理、および施設全体のセキュリティの確保に専ら責任を負う。CSC はデータセンターのセキュリティに責任を負わないが、A&A ドメインにおいては、CSP が DCS の管理策に準拠していることを検証すべきである。

（DSP）データセキュリティとプライバシーのライフサイクル管理

データセキュリティとプライバシーのライフサイクル管理（DSP）ドメインは、プライバシーとデータセキュリティに関する 19 の管理策を特徴としている。これらの管理策は、業界やセクターに特化したものではなく、特定の国や規制に焦点を当てたものでもない。しかし、これらの管理策は、主要なプライバシー規制の共通要素および要件を考慮して策定されている。これらの管理策は一般的に世界中の組織に適用可能であり、一部の地域や部門で活動する組織では補足的なデータ保護管理策を実施しなければならない場合があるという注意点を踏まえた上で、価値ある基本標準として機能することが期待されている。

DSP 管理策は、データプライバシー、データ分類、インベントリ作成、保持、および適用される全ての法規制、標準、およびリスクレベルに従った廃棄手順を含む、データの作成から廃棄までの完全なデータライフサイクルをカバーする。DSP における管理は、CSP と CSC の双方が関連データを保護し、データ保護に関す

る法律や規制を遵守するのに役立つ。

SSRM の下では、CSP はクラウドの "Of" のセキュリティに責任を負い、データのセキュアな保存、アクセス、および廃棄のための機能を CSC に提供する。一方、CSC は、データの分類、暗号化などのデータ保護のための CSP の提供する機能の活用、データプライバシー規制の遵守を確保しながらのデータアクセスレベルの指定など、クラウドの "in"で保存または処理するデータのセキュア確保に責任を負う。

DSP 管理策の導入は、クラウド上のデータの全体的なセキュリティとプライバシーを強化するため、大きなメリットをもたらす。責任を共有することで、堅牢でコンプライアンスに準拠したクラウド環境が育まれ、両者にとって有益なものとなる。

（GRC）ガバナンス、リスク、コンプライアンス

ガバナンス、リスク、コンプライアンス（GRC）ドメインは、CSP と CSC が情報ガバナンスと関連する企業リスク管理（ERM）、情報セキュリティ管理、コンプライアンス管理プログラムがクラウドの提供と懸念に適切に対応できるようにするための 8 つの管理仕様で構成される。

通常、CSP と CSC は、クラウドベースの製品、サービス、資産、プロセス、プロバイダーを含め、自社の経営と業務をカバーするガバナンス、リスク、コンプライアンス管理策を実施する責任をそれぞれ独自に負っている。GRC プログラムの構築は、完全に内部的なものであり、各組織固有のものである。

GRC セキュリティ管理策を導入することで、クラウド企業は、リスクを管理し、規制へのコンプライアンスを確保し、セキュリティ対策をビジネス目標と整合させるための構造化されたガバナンスの枠組みを提供することで、自社のリソースと能力を効果的に指揮・管理できるようになる。

（HRS）人的リソースセキュリティ

人的リソースセキュリティ（HRS）ドメインは、クラウド組織が内部脅威に関するリスクを管理し、機密データを取り扱う要員が信頼に足る人物であり、適切な訓練を受けていることを保証する 13 の管理策を利用する。効果的な HRS 対策は、人的要因による不正アクセスやデータ漏洩を防ぎ、全体的なセキュリティ体制を維持する。

SSRM では、CSP と CSC の双方が HRS のセキュリティ管理を独自に実施する役割と責任を有する。両者とも、バックグラウンドチェックの実施、従業員への継続的なセキュリティトレーニングの提供、クラウドセキュリティリスクとセキュリティのベストプラクティスを従業員に周知徹底させることについては、一般的に独

立して責任を負う。

HRS を導入することで、クラウド企業は十分に訓練され、吟味された人材を採用することで、サービスのセキュア性を確保することができる。これにより、人為的ミスや悪意に起因するセキュリティインシデントのリスクを軽減することができる。

（IAM）アイデンティティとアクセス管理

アイデンティティとアクセス管理（IAM）ドメインは、CSP と CSC の両方がクラウド環境におけるセキュリティ機能とデータへのアイデンティティとアクセスを管理する際のセキュリティベストプラクティスを遵守するための 16 の管理仕様を特徴としている。最小特権の原則、職務の分離、多要素認証、役割ベースおよび属性ベースのアクセスコントロールなどのベストプラクティスは、クラウドリソースへのアクセスを管理する上で中心となる。

CSP と CSC はともに、クラウド環境へのセキュアなアクセスを確立する責任を共有する。CSP は通常、強力な ID およびアクセス能力、機能、制御、および関連メカニズムを CSC に提供する責任を負う。CSC は通常、最小特権の原則に基づいてユーザーの役割とアクセス許可を定義し、強力な認証メカニズムを適切に実施し、クラウドサービスに対するユーザーアクセスのプロビジョニング、変更、および失効を含む、アイデンティティとそのアクセスレベルの完全なライフサイクルを管理し、不審な行動を特定し、対応するためにユーザーの活動を監視する責任を負う。

効果的な IAM 機能を実装するために CSP と CSC が協力することで、CSC のデータを不正アクセスから保護するために必要な管理が実装される。

（IPY）相互運用性と移植容易性

CCM の相互運用性と移植容易性（IPY）ドメインには、クラウド環境における相互運用性と移植容易性に対応する 4 つの管理仕様がある。強固な相互運用性と移植容易性の管理を実装することで、複数のプラットフォームや CSP 間でのセキュアかつセキュアなデータ交換が容易になり、CSC はベンダーロックインを回避し、相互運用性と移植容易性がセキュリティ上の懸念によって妨げられない環境を醸成することができる。

CSP と CSC はそれぞれ、クラウドエコシステム内での相互運用性と移植容易性を確保する責任を共有している。CSP は通常、標準化された通信プロトコルの実装、セキュアな通信チャネルの確保、クロスプラットフォームの互換性の維持、標準化されたデータ形式、共通のデータ処理およびデータ交換プロトコルに責任を負う。CSC は、相互運用可能なデータ暗号化の利用を含め、セキュアなデータのバックアップ、転送、リス

トアのために CSP が提供するツールを理解し、利用する責任を負う。
CSC はまた、CSP が提供する管理、監視、およびレポーティングインタフェースと、複数環境間でのそれらのインタフェースの統合について理解する必要がある。CSP と CSC は共に、データの所有や移行手順の定義など、データ移植容易性に関する契約上の義務を文書化する共同責任を負う。

CSP と CSC の双方が相互運用性と移植容易性を共有することは、セキュアで柔軟なクラウドエコシステムを構築する上で重要である。

（IVS）インフラストラクチャと仮想化のセキュリティ

インフラストラクチャと仮想化セキュリティ（IVS）ドメインは、9 つの管理策で構成され、CSP および CSC がインフラストラクチャおよび仮想化技術を保護するための管理策を実施する際の指針となる。インフラストラクチャには、IT サービスの提供に必要な全てのハードウェア、ソフトウェア、ネットワーク、設備などが含まれる。仮想化技術は、ハードウェア要素（プロセッサ、メモリ、ストレージなど）を仮想コンピュータに分割できるようにする、コンピュータハードウェア上の抽象化レイヤーを作成するためにソフトウェアを使用する。

通常、CSP と CSC の両方が IVS 管理の実施に責任を負う。CSP は通常、プラットフォーム（ハイパーバイザ、VM、ホスト OS）およびネットワーク仮想化技術など、基盤となるインフラストラクチャのセキュリティ確保、ネットワークのセグメンテーションと分離の実装、容量およびリソース計画のための CSC への機能提供に責任を負う。CSC は通常、ゲスト OS の堅牢化、セキュリティパッチの適用、不要なサービスの無効化、プラットフォームやコントロールプレーンのユーザインタフェースへのアクセス管理など、仮想化環境内で割り当てられたリソースのセキュア確保に責任を負う。

インフラストラクチャと仮想化技術は、クラウドコンピューティングの基本的な構成要素であり、インフラストラクチャと仮想化のセキュリティ管理の実装における CSP と CSC の協力は、クラウド上で実行されるワークロードのセキュリティを確保するのに役立つ。

（LOG）ロギングと監視

ロギングと監視（LOG）ドメインは、CSP と CSC がクラウド環境で発生したアクティビティとイベントを収集、保存、分析、および報告できるようにする 13 の管理策を使用する。これにより、セキュリティインシデント、運用上の問題、およびシステムの異常の検出と対応、規制要件への準拠、セキュリティ管理の有効性の監査と検証、セキュリティポスチャとパフォーマンスの向上が可能になる。

通常、CSP と CSC の両方が、ロギングと監視の管理を実施する責任を負う。CSP は通常、ネットワークおよびシステムレベルの運用を含む、クラウドインフラストラクチャのロギングと監視に責任を負う。一方、CSC は通常、デプロイされたアプリケーションとサービス内の監視とロギングに責任を負い、それぞれのセキュリティ要件が満たされていることを保証する。

CSP と CSC が協力してロギングと監視を実施することで、クラウド運用の可視性、説明責任、透明性が向上する。ロギングと監視は、セキュリティリスクの特定と軽減、クラウドの利用とパフォーマンスの最適化、関連する標準や規制の遵守の実証に役立つ。

（SEF）セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジック

セキュリティインシデント管理、E-ディスカバリ、およびクラウドフォレンジック（SEF）ドメインには、セキュリティインシデントの効果的な管理と対応、E-ディスカバリの実施、およびクラウドでのフォレンジックの実施に不可欠な 8 つの管理仕様がある。これらのコントロールは、CSP と CSC がセキュリティインシデントをタイムリーに検出、分析、対応し、業務への影響を最小限に抑えるのに役立つ。

SSRM では、CSP と CSC は通常、明確に定義されたインシデント対応計画を策定し、明確な役割と責任を定め、測定標準を導入し、関連する利害関係者にインシデントを報告し、セキュリティインシデントに効率的に対処するための手順をエスカレーションする責任を負う。CSP と CSC の連携において重要な側面は、潜在的なセキュリティインシデントのトリアージである。一方、CSC は、自社のデータ、構成、アプリケーション、ユーザー活動に特有の情報を提供することができる。

SEF コントロールの実施における CSP と CSC のコラボレーションは、相互に効果的なインシデント管理とフォレンジック能力をもたらし、インシデントからの迅速な回復を保証し、法的および規制要件への準拠を促進する。

（STA）サプライチェーン管理、透明性、説明責任

サプライチェーン管理、透明性、説明責任（STA）ドメインは、CSP と CSC 間の SSRM の管理など、クラウドパーティが広範なサプライチェーンリスク管理策を定義する際に役立つ 14 の管理策仕様を特徴としている。これらの管理策により、サードパーティプロバイダーは、あらゆる技術スタックにまたがる情報、アプリケーション、およびサービスの機密性、完全性、および可用性を保護するために、適切なセキュリティ対策を採用することができる。また、これらの管理は、サプライチェーン全体にわたるセキュリティと規制のコンプライアンス管理にも役立つ。

SSRM では、CSP はサプライチェーンのセキュリティの確保と管理、および業務の透明性の確保に責任を負う。CSC は、選択した CSP とそのサプライチェーンベンダーに関連するリスクを評価・理解し、その要件が満たされるようにしなければならない。

STA 管理の実施における CSP と CSC の協力は、当事者間の透明性と説明責任につながり、より強固でセキュアなサプライチェーンを実現する。CSC にとっては、サプライチェーンセキュリティに関する CSC 固有の要件や懸念に対処するための協調が保証される。

（TVM）脅威と脆弱性管理

脅威と脆弱性管理（TVM）ドメインは、CSP と CSC の双方が、資産、セキュリティアーキテクチャ、設計、及びソリューションコンポーネントに影響を及ぼす可能性のある、クラウド環境におけるセキュリティの脅威及び脆弱性を事前に特定し、緩和することを支援するための 10 の管理策仕様で構成される。

SSRM では、通常、CSP と CSC の両方が TVM セキュリティ管理策の実施に責任を負う。CSP は通常、ホストインフラストラクチャ、ネットワークデバイス、仮想化技術、オペレーティングシステム、データベースや Web アプリケーションなどのプラットフォームアプリケーションの脆弱性の特定、評価、報告、是正の優先順位付けの責任を負う。一方、CSC は、アプリケーション/API のセキュリティ設定やアクセス設定ミスに関連する脆弱性の特定、評価、報告、是正の優先順位付けの責任を負う。

TVM 管理策の実装における CSP と CSC の連携は、基盤となるプラットフォームからデプロイされたアプリケーションに至るまで、クラウドインフラストラクチャ全体の脆弱性に対処することで、全体的なクラウドセキュリティポスチャを強化する。

（UEM）ユニバーサルエンドポイント管理

ユニバーサルエンドポイント管理（UEM）ドメインは、14 の管理策仕様から構成され、モバイルデバイスを含むエンドポイントに関連するリスクを軽減するための管理の実装に焦点を当てている。モバイルコンピューティングとエンドポイントセキュリティのリスクは、主にユーザーの行動と、デバイスとテクノロジーの許容可能な使用に対する企業のアプローチ（管理対非管理、企業所有対個人所有など）の認識（または認識不足）に関連する。

CSP と CSC の両方が、通常、独立して UEM セキュリティ管理の実装に責任を負う。CSP は主に、全てのエンドポイントのインベントリの管理、エンドポイントによる使用を許可するサービスやアプリケーションの承認、自動ロック画面、ファイアウォール、マルウェア検出対策などのセキュリティ対策の実装、防止技術、

ストレージの暗号化、データ損失防止技術の活用といったエンドポイント管理機能に責任を負う。一方、CSC はデバイスをセキュアにし、CSP が設定したセキュリティポリシーに準拠していることを確認し、データを保護する責任を負う。

UEM コントロールの実装における CSP と CSC の連携により、クラウドリソースへのアクセスに使用されるエンドポイントのクラウドセキュリティポスチャ全体が強化される。

1.1.4 コンポーネント

中核となる 197 のセキュリティとプライバシー管理とともに、CCM v4.0 には以下のような追加ツールが含まれている。(*訳注：CCM の EXCEL シートでは、2 行目および 3 行目の項目は英語の表記のままとしている。そのため、本資料でも英語表記のままとする*)

- CCM Control Specifications and Applicability Matrices
- Scope Applicability（Mapping）
- Consensus Assessment Initiative Questionnaire（CAIQ）
- Implementation Guidelines（本書に含まれる）
- Auditing Guidelines
- Continuous Audit Metrics Catalog

CCM Control Specifications and Applicability Matrices

CCM Control Specification は、3 つの主要グループからなる Applicability Matrices にマッピングされる：

- 代表的なコントロールの適用範囲と所有
- アーキテクチャの関連性 - クラウドスタックのコンポーネント
- 組織との関連性

典型的な管理策の適用可能性と所有のマトリクスは、3 つの主要なクラウドサービスモデル(IaaS、PaaS、SaaS)の全ての管理策について、標準的な SSRM Control の所有と適用可能性を説明している。一般的な SSRM の所有の指定は、管理策 STA-04 で要求されているように、所定の CCM 管理策を実施するための典型的な責任を CSP と CSC の間で割り当てている。一部の管理策は明らかに IaaS プロバイダーの管轄であるが（例：データセンターセキュリティ管理策)、他の管理策は全てのサービスモデルに適用可能である（例：ID およびアクセス管理)。この CCM マトリクスでは、3 つのクラウドサービスモデルに対する各管理策の適用可能性を説明しており、具体的なケースで何が関連するかを理解するのに役立つ。

architectural relevance group は、CSA クラウド参照モデルの観点から、クラウドスタックコンポーネントごとの各 CCM 管理策のアーキテクチャ関連性を示している。このセクションでは、物理、ネットワーク、コンピュート、ストレージ、アプリケーション、データなど、多数の要素に焦点を当てている。さらに、CCM は、さまざまな法規制フレームワークの既存のセキュリティ管理策の仕様にマッピングされ、同じマトリクスがアーキテクチャのセキュリティ機能にマッピングされているため、企業は、どの機能が適用される法規制やベストプラクティスのフレームワークに準拠しているかを容易に評価することができる。

organizational relevance group は、各 CCM 管理策と、組織内の各クラウド関連機能によるその実施との関連を示す。含まれる機能は以下のとおりである：「サイバーセキュリティ」、「内部監査」、「アーキテクチャチーム」、「ソフトウェア開発チーム」、「オペレーション」、「法務／プライバシー」、「ガバナンス／リスク／管理」、「サプライチェーン管理」、「人事」。

Scope Applicability (Mapping)

CCM の重要な側面は、他のセキュリティ標準、規制、およびフレームワークと対応していることである。CCM が策定された当時、すでにさまざまな情報セキュリティ標準、ベストプラクティス、規制が存在していた（ISO 27001： 2022、PCI DSS、NERC CIP、BITS、BSI など）。多くの企業は、すでに社内の構造やフレームワークを設定し、それらの標準に合わせていた。

CSA は、クラウド部門に特化した管理策を提供する一方で、組織が既存の管理策フレームワークやプログラムと CCM に含まれるクラウド関連の管理策を接続するための明確な経路を確保したいと考えていた。そのため、CSA は、CCM で作成される全ての管理策を、既存のフレームワークの管理策の拡張として構築した。CSA は、この目的を実現するために、フレームワーク管理（ISO 27001：2022 など）と CCM との間のマッピング（リンケージ）を構築した。次に、CCM はフレームワークをベースにして、クラウド分野に特化した管理策を提供し、さらに一歩進めて、管理策がクラウドアーキテクチャ内の特定のドメインにリンクするようにした。そして CCM は、特定の管理策が IaaS、PaaS、SaaS のいずれに関連するかを特定するのに役立つ。CCM はマッピングを通じてリンクを作成するため、クラウドジャーニーと導入プロセスを推進するために組織が制定すべき管理策を特定する最初の内部統制システムを提供する。

The Consensus Assessment Initiative Questionnaire (CAIQ)

CAIQ は、クラウドの利用者および監査人に対し、CSP のセキュリティポスチャ、CSA のベストプラクティス（CCM および CSA セキュリティガイダンス）の遵守、および CSC の SSRM 責任に関する質問を提供する。CAIQ は、CCM のより良い導入を支援するために設計された追加の文書である。CCM が 管理策の仕様と実施ガイドラインを定義しているのに対して、CAIQ は実施を評価し通知するための質問を定義している。さらに、CAIQ（および CSA STAR Registry）は、CCM 管理策 STA-01 から STA-06 に従って、CSP が現在および将来の CSC に対して、SSRM 所有および CSC のセキュリティ責任に関するガイダンスを提供するために使用されるべきである。

CCM 管理策と CAIQ の設問の関係は、1 対多であることが多い。CCM が 197 の管理策に基づいているのに対し、CAIQ の最新版（バージョン 4）には 261 の質問がある。CCM 管理策の性質と複雑さによって、ある管理策の実施を検証するために、1 つまたは複数の質問が出されている。

CAIQ は、CCM と同様に、CCM と同様の構造を持つスプレッドシート形式で提供されている。CAIQ には、CAIQ の質問に CSP が回答するための欄（「Yes」、「No」、または「NA」）があり、CAIQ の質問に関連する CCM 管理策の SSRM 所有を指定する。また、CAIQ には、CSP がどのように管理策を満たすか、および関連する利用者のセキュリティ責任を記述する欄もある。CSP は、SSRM の所有を明確にし、どのように管理要件を満たすかを説明し、質問レベルで CSC のセキュリティ責任を明確にすべきである。

CAIQ および CSA STAR Registry は、CSP が、現在および将来の CSC がどのように管理策が実施されたかを評価するために使用できる有用な情報を提供するためのフレームワークとフォーラムを提供する。さらに、これらのツールにより、CSP は、CSC の利益のために、SSRM の実装を明確にすることができる。

Implementation Guidelines

CCM Implementation Guidelines の主な目的は、CCM 管理策の導入に関するさらなるガイダンスと推奨を提供することである。本書は、セキュリティ責任共有モデルの下で CCM 管理策を使用しながらクラウドサービスを実装し、セキュリティを確保した CSP と CSC の経験に基づく共同成果物である。

SSRM の下で、CSP と CSC は、共有クラウドインフラストラクチャにおいて「誰が」「何を」行うかについて、 特定の共有セキュリティ責任を負わなければならない。本書は、CSP と CSC の両方に対して、そのような責任を管理策の仕様レベルで定義し、SSRM 特有のガイダンスを提供する。

しかし、本書は CCM 管理策導入のための「ハウツー」マニュアルとなることを意図したものではない。CCM 管理策の包括的な性質を考慮すると、その運用は、クラウドサービスとそのアーキテクチャの性質、使用される技術の種類、適用されるリスクと規制、組織のポリシー、脅威環境、およびその他の重要な要因に大きく依存する。したがって、CSA は、全ての組織とクラウドサービスの管理策の実施に適用できる詳細で規定的なガイダンスを提供することはできない。

Auditing Guidelines

CCM v4.0 Auditing Guidelines（AGs）は、クラウドコントロールマトリックスバージョン 4（CCM v4.0）の 17 のクラウドセキュリティドメインの各 Control Specification に合わせたものである。このガイドラインは、CCM v3.0.1 にはなかった CCM v4.0 の新しい構成要素である。

AG は、CCM 監査を容易にし、指導することを目的とする。監査人には、CCM v4.0 の管理策の仕様に従った評価ガイドラインが提供される。これらのガイドラインは、k 管理策の監査可能性を向上させ、組織が（内部

または外部の第三者によるクラウドセキュリティ監査で）より効率的にコンプライアンスを達成できるようにすることを目的としている。

Auditing Guidelines は、その性質上、網羅的あるいは規定的なものではない。むしろ、評価のための推奨事項を通じての一般的なガイドを示すものである。監査人は、説明、手順、リスク、統制、文書化をカスタマイズしなければならない。これらの要素は、具体的な監査目的に対応するために、組織特有の監査作業プログラム及び評価範囲内のサービスに適合していなければならない。

CSA の Auditing Guidelines は 2021 年 12 月に発表された。

Continuous Audit Metrics Catalog

評価指標とは、測定を実行し、測定結果を理解するためのルールを定義した測定の標準である（ISO/IEC 19086-1）。クラウドコンピューティングの文脈では、情報システムのセキュリティを評価するために使用できる評価指標を定義することへの関心が高まっている。

セキュリティ評価指標は、いくつかの目的に使用することができる。

- *情報システムの有効性を測定すること*：評価指標を使用することで、組織は情報システムのさまざまな属性に定性的または定量的な値を割り当てることができる。セキュリティ管理策の実装を反映する属性を慎重に選択することで、評価指標を使用してこれらの管理策の有効性を測定できる。
- *組織のガバナンスとリスク管理アプローチの成熟度を高めること*：セキュリティ評価評価指標を選択し導入する組織には、資産を明確に分類し、関連するセキュリティ属性を測定するために必要なツールを導入することが求められる。この作業は些細なことではないため、これを実施できるということは、その組織が情報セキュリティ管理において一定の成熟度に達していることを示す。
- *透明性と説明責任を高め、継続的なコンプライアンスを可能にすること*：評価指標を採用する組織は、関連する利害関係者にセキュリティとプライバシーの慣行を可視化し、サービスレベルアグリーメントをより適切に説明して正当化できる。評価指標は、従来のポイントインタイム認証が現在提供しているものを超える継続的な認証スキームの基盤としても使用できる。

Continuous Audit Metrics Catalog は、CSA Continuous Audit Metrics Working Group の業界専門家による作業の成果である。このカタログは、網羅的で完全なものではない。最初のリリースは、CCM 管理策の実施の効率性と有効性をより体系的に評価することを求める組織を支援することを目的としている。提案された測定標準は、CSP 内部のガバナンス、リスク、コンプライアンス（GRC）活動を支援し、サービスレベル契約の透明性に役立つ標準値を提供することを目的としている。さらに、これらの測定標準は、将来 STAR プログラムに統合され、継続的な認証の基盤となる可能性がある。

本書で示す CCM 実装ガイドラインでは、いくつかの管理策の正しい実装を確認するために、評価指標の使用を提案している。さらに、CSA は、クラウドコントロールマトリクス第 4 版（CCM v4.0）にマッピングされるクラウドセキュリティ評価指標のカタログ[3]を定義した。

1.1.5 CCM カラム

本書の発行日現在、CCM V4 のスプレッドシートには 6 つのタブがある。

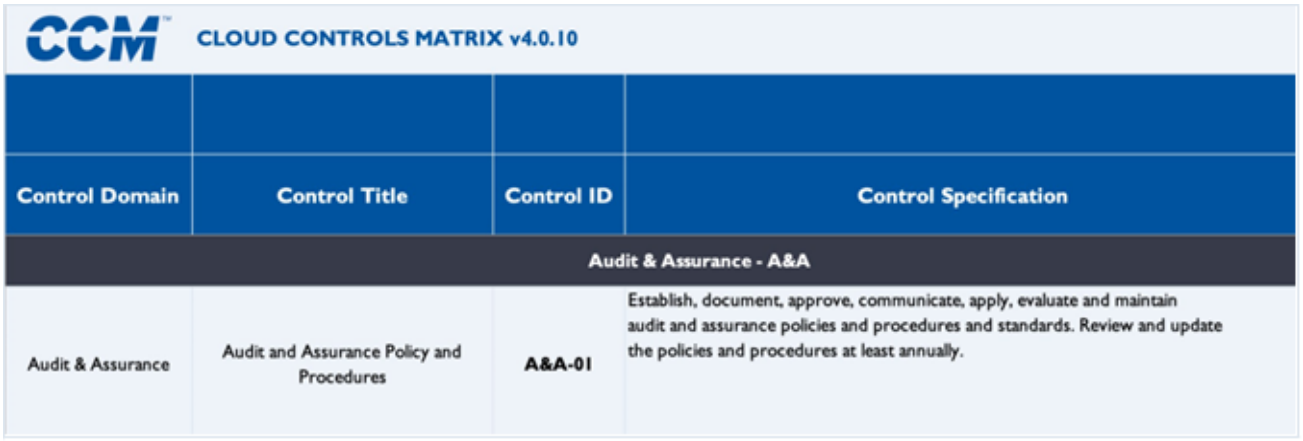
- Introduction
- CCM Controls
- Implementation Guidelines
- Auditing Guidelines
- Scope Applicability (Mappings)
- CAIQ
- Acknowledgements

a. CCM Controls

これが CCM V4 の中核である。17 のドメインで構成された 197 の管理策が含まれる。各管理策は以下である：

- Control Domain：各管理策が関連するドメイン名。
- Control Title：管理策のタイトル。
- Control ID：管理策の識別子。
- Control Specification：管理策の仕様の説明。

[3] https://cloudsecurityalliance.org/artifacts/the-continuous-audit-metrics-catalog , accessed on 5 March 2024.



CCM CLOUD CONTROLS MATRIX v4.0.10

Control Domain	Control Title	Control ID	Control Specification
Audit & Assurance - A&A			
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.

図 2：CCMv4 Audit & Assurance ドメインの管理策の仕様のスナップショット。

さらに、このタブには以下のセクション（列のグループ）がある：

- **Typical Control Applicability and Ownership matrix。**これらの列は、3 つの主要なクラウドデリバリーモデル(IaaS、PaaS、SaaS)の全ての管理策について、標準的な SSRM control の所有と適用可能性を記述している。一般的な SSRM の所有の指定は、所定の CCM control を実施するための典型的な責任を CSP と CSC の間に割り当てるものである。マトリクスは、コントロールの責任が通常、” CSP-Owned ”、”CSC-Owned “、または CSP と CSC の間で”Shared“のいずれであるかを示す（control STA-04 で要求されている）。SSRM control の所有は、クラウドサービスモデルと各特定のクラウドサービスの実装によって、サービスごとに異なる。したがって、CSP は、セキュアな利用者サービスの実装を促進するために、サービスごとに詳細な SSRM ガイダンスを提供する必要がある。CAIQ のバージョン 4 は、CSP がこの重要な情報を文書化し、現在および将来利用者と共有するためのフレームワークとフォーラムを提供するよう強化されている（CCM control STA-01～STA-06 による）。

CCM CLOUD CONTROLS MATRIX v4.0.10

Control Domain	Control Title	Control ID	Control Specification	CCM Lite	Typical Control Applicability and Ownership		
					IaaS	PaaS	SaaS
Audit & Assurance - A&A							
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	No	Shared	Shared	Shared

図 3：IaaS-PaaS-SaaS ごとの CCMv4「Audit & Assurance」ドメインとコントロールの適用可能性のスナップショット。

- **Architectural Relevance and Cloud Stack Components matrix。**これらの列は、CSA クラウド参照モデルの観点から見た、各 CCM control（クラウドスタックコンポーネントごと）のアーキテクチャ上の関連性を示している。このセクションでは、次のコンポーネントに焦点を当てて

いる：”物理”、”ネットワーク”、”コンピュート”、”ストレージ”、”アプリケーション”、”データ”。

各コンポーネントに関連する関連性ボックスは、そのコントロールがコンポーネントに関連する場合は ”TRUE”、関連しない場合は ”FALSE ”と表示される。

architectural relevance は、ハイレベルで単純化したものであり、CCM ユーザーは、特定のクラウド環境や使用する技術に応じて、これらの帰属を修正する必要がある。

CCM CLOUD CONTROLS MATRIX v4.0.10										
					Architectural Relevance - Cloud Stack Components					
Control Domain	Control Title	Control ID	Control Specification	CCM Lite	Phys	Network	Compute	Storage	App	Data
Audit & Assurance - A&A										
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	No	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE

図 4：CCMv4「監査と保証」ドメインと制御アーキテクチャの関連性のスナップショット

- **Organizational Relevance matrix。**この列のグループは、各 CCM control と、組織内の各クラウド関連機能によるその実施との関連性を示している。含まれる機能は次の通りである：サイバーセキュリティ”、”内部監査”、”アーキテクチャチーム”、”SW（ソフトウェア）開発チーム”、”オペレーション”、”法務／プライバシー”、”GRC（ガバナンス／リスク／コントロール）チーム”、”サプライチェーン管理”、”HR（人事）”。

  各コンポーネントに関連する”関連性ボックス”は、コントロールがコンポーネントに関連する場合は ”TRUE”、関連しない場合は ”FALSE ”とマークされる。

CCM CLOUD CONTROLS MATRIX v4.0.10													
					Organizational Relevance								
Control Domain	Control Title	Control ID	Control Specification	CCM Lite	Cybersecurity	Internal Audit	Architecture Team	SW Development	Operations	Legal/Privacy	GRC Team	Supply Chain Management	HR
Audit & Assurance - A&A													
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	No	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE

b. Implementation Guidelines

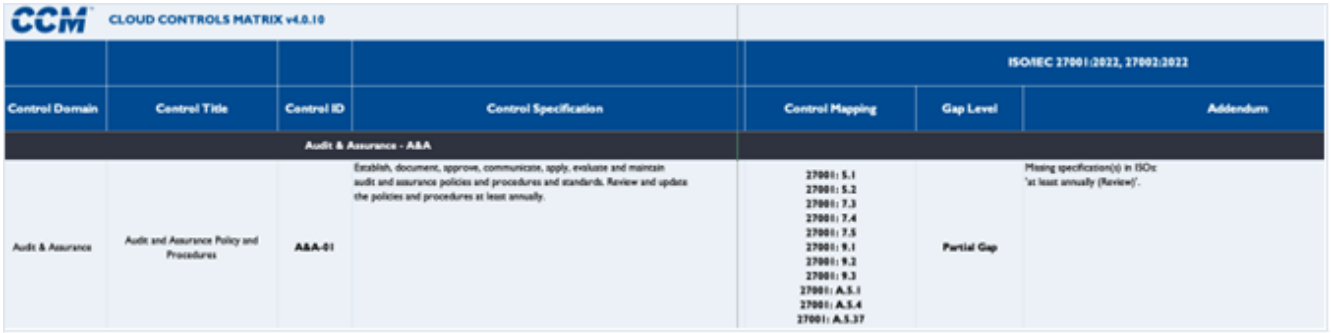
このタブには、共有セキュリティ責任モデルに沿った CCM 管理策の実施方法に関する提案、推奨、例を示す実施ガイドラインが含まれている。

c. CCM Scope Applicability(Mapping)

このタブには、CCM V4 と、クラウドコンピューティングに関連する数多くの規格（ISO 27001/2/17/18）およびベストプラクティス（CIS v8.0）の管理策セットとのマッピングが含まれている。

各規格について、CCM V4 は以下の 3 つの列を含むようにマッピングされている：

- Control Mapping。ターゲット規格（ISO27001： 2022 など）のどの管理策が CCM 管理策に対応するかを示す。
- Gap Level。CCM の管理策と比較したときの、ターゲット規格の管理策（または複数の管理策）のギャップレベル。使用されるギャップレベルは以下の通り：
    - No Gap：完全対応の場合。
    - Partial Gap：ターゲットスタンダードの管理策が、対応する CCM 管理策の要求事項を完全に満たしていない場合。
    - Full Gap：ターゲット規格の中に、対応する CCM 管理策の要求事項を満たす管理策がない場合。
- Addendum。ターゲット規格の管理策と対応する CCM 管理策との間のギャップをカバーするために、組織が実施可能な補完統制を提案する。



CCM CLOUD CONTROLS MATRIX v4.0.10

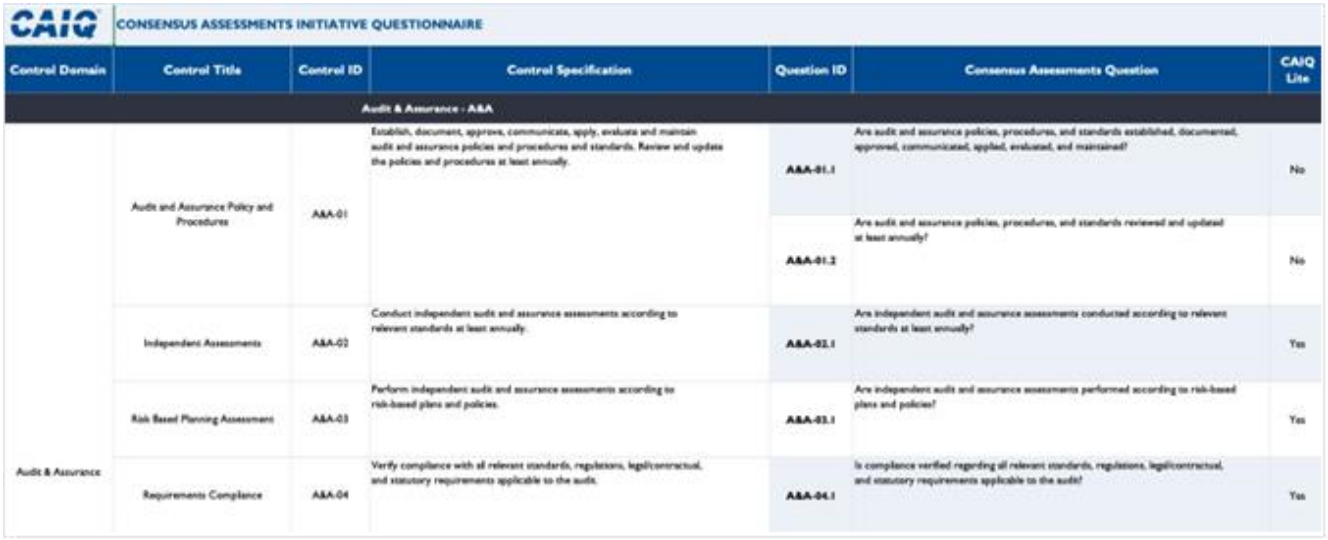
				ISO/IEC 27001:2022, 27002:2022		
Control Domain	Control Title	Control ID	Control Specification	Control Mapping	Gap Level	Addendum
Audit & Assurance - A&A						
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	27001: 5.1 27001: 5.2 27001: 7.3 27001: 7.4 27001: 7.5 27001: 9.1 27001: 9.2 27001: 9.3 27001: A.5.1 27001: A.5.4 27001: A.5.37	Partial Gap	Missing specification(s) in ISO: 'at least annually (Review)'.

図 6：ISO 規格にマッピングされた CCMv4 管理策のスナップショット。

d. Consensus Assessments Initiative Questionnaire(CAIQ)

このタブには、一般に CAIQ として知られる、CCM コントロールに関連したアンケートが含まれている。CAIQ は CCM の 17 のドメインで構成された 261 の質問からなる。各質問は以下のように説明される。

- Question ID：質問の識別子。
- Question ：質問の説明。



CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE

Control Domain	Control Title	Control ID	Control Specification	Question ID	Consensus Assessments Question	CAIQ Lite
Audit & Assurance - A&A						
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	No
				A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	No
	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes
	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes
	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes

図 7：CCMv4 管理策と対応する CAIQv4 評価質問のスナップショット。

e. Acknowledgements

このタブでは、CCM v4.0 の開発に貢献した専門家を紹介している。

1.1.6 CCM Target audience

CCM は、CSC、CSP、監査人、コンサルタントを支援するために作成されている。

クラウドサービス利用者（CSC）：CCM により、クラウドサービス利用者は、サードパーティーのリスク管理および調達プログラム全体の一環として、CSP に実装してもらいたい要件や管理の詳細なリストを作成することができる。また、CCM は、セキュリティに対する期待を正規化し、クラウドの分類法を提供し、クラウドサプライチェーンで実装されるセキュリティ対策の理解を深めるのに役立つ。

クラウドサプライチェーン内のアクターは独立した組織であるため、それぞれが独自の方法でセキュリティ要件を表現する。各アクターは、異なる用語を使用したり、他とは異なるポリシーを適用したりするかもしれない。このような状況では、さまざまな言語を標準化するために、分類法（合意された用語のセット）を定義することが不可欠である。これが、CCM が重要な役割を果たす理由であり、相互運用性を単純化するために、より包括的なフレームワークが必要とされる理由である。

CSC は、CCM 管理策を使って以下のことができる：

- 組織的、業務的、法的要件を管理目的にマッピングする。
- 運用クラウドリスク管理プログラムを構築する。
- 第三者リスク管理プログラムを構築する。

- 内部および外部のクラウド監査計画を構築する。

企業がクラウドのリスク管理プログラムを構築する際、CCM は CSP や特定のサービスに関連するリスクの測定、評価、監視に役立つ。CCM によって、利用者は自社のセキュリティニーズと CSP のセキュリティ能力とのギャップを理解することができる。その後、利用者は以下のことが可能になる。CCM を使用して、組織のニーズとプロバイダーの提供するサービスのギャップを埋めるための補完管理策を特定する。

サードパーティーのリスク管理プログラムを構築する際、CCM を利用することで、利用者はサービスライフサイクル全体を通じてクラウドサービスを評価することができる。例えば、買収前のサービス評価、異なる CSP の提供サービスの比較、サービス実行中の内部要件との整合性の監視などに利用できる。

クラウドサービスプロバイダー（CSP）：CCM は、CSP にとって複数の役割を果たす。最初に、CCM はクラウドに特化し、業界で検証されたベストプラクティスを提供し、CSP はこれに従って社内のセキュリティプログラムを導くことができる。次に、CCM は、CSP が利用者やビジネスパートナーとのコミュニケーションに使用できる標準化された言語を提供する。

CCM マッピング機能により、CSP は、他の国際的、国内的、および業界的に認知されたフレームワークとの整合性を実証し、CSA STAR プログラム（CSA STAR プログラムはその基礎フレームワークの 1 つとして CCM に依存している）への準拠を実証することができる（詳細については第 9 章を参照）。さらに、CSA STAR プログラムは、組織の透明性を高め、顧客に提供しなければならないセキュリティアンケートの数を減らすことを可能にする。これらの利点は、組織が CCM を拡大した質問の自己評価（CAIQ）を完了し、CSA STAR registry（CSP が提供するセキュリティ管理策を文書化した、無料で一般にアクセス可能なレジストリ）に提出することにより実現する。

CSP は、CCM 管理策を使って次のことができる。

- 成熟した、業界で認知されたベストプラクティスに基づく内部セキュリティプログラムを構築する。
- ビジネスパートナーや利用者とのコミュニケーションと相互運用性を促進する。
- セキュリティに対するコミットメントと、セキュリティポスチャに関する透明性を示す。
- CCM の管理策と他の国際的、国家的、業界的フレームワークの管理策とのマッピングを活用することにより、コンプライアンスを合理化する。
- 利用者アンケートに対応する時間と労力を削減する。
- CSA STAR プログラム（第 9 章参照）を遵守することで、規制当局にセキュリティに対するコミットメントを示す。
- クラウド内部・外部監査計画を構築する。

監査人とコンサルタント：監査人やコンサルタントは、CCM を利用して、CSC や CSP に特化した活動の設計、計画、実施をクライアントに指導することができる。

コンサルタントと監査人は、CSA のリソースを活用することができる：

- 組織がクラウドの成熟度を評価するのを支援する。
- CCM に沿った統制を確立する。
- ベンチマーキングを通じて、組織を市場の同業他社と比較する。

1.1.7 CCM コンプライアンス文書

組織的な記録を提供し、コンプライアンス監査に備えるために、CCM ユーザーは、クラウドサービスプロバイダー(CSP)とそのクラウドサービス利用者(CSC)の間に常に存在するセキュリティ責任共有モデル(SSRM)の下で、全体的または部分的に責任を負う CCM V4 管理策への準拠を文書化することに重点を置くべきである。

CCM ユーザーは、CSP や CSC など、それぞれのクラウドの役割に適した、高レベルの CCM コンプライアンスと SSRM コントロールの適用可能性と実施概要の文書を作成または組み立てることから始めるべきである。

- CSP ：Consensus Assessment Initiative Questionnaire v4 (CAIQ v4) を完全に記入したものは、一般的に良い出発点となる。完成した CAIQ アンケートは、CSA の Security, Trust, Assurance, and Risk (STAR) Registry[4]で公表することができる。完全に記入された調査票には、オプションの「CSP Implementation Description (Optional/Recommended)」と「CSC Responsibilities (Optional/Recommended)」の列が含まれる。
- CSC ：CSA はある特定の質問票やコンプライアンス文書テンプレートを持たない。しかし、組織は、(CCM STA 管理要件に従って CSP が定義する) SSRM 利用者のセキュリティ責任を組み込むために、何らかの形式の CCM コンプライアンス文書を持つ（または作成する）べきである。例えば、一部の CSC は CCM 管理策スプレッドシート及び／又は CSP の CAIQ アンケートのコピーをカスタマイズして、利用者のセキュリティコントロール対応情報を組み込む（例えば、標準的な成果物に列を追加する)。あるいは、CSC は内部 GR アプリケーションを利用して、同様の詳細を収集することもできる。このように集計されたデータにより、コンプライアンスレビュー及び監査を目的とした適切なレポートを作成することができる。

高レベルの SSRM の実施概要情報に加えて、より詳細な裏付け文書（例えば、技術的設計、プロセスと手順

[4] https：//cloudsecurityalliance.org/star/registry

書、遵守の証拠）を特定の管理ドメインと個々の管理（必要に応じて）について作成すべきである。この文書は、本書で強調されている詳細なガイドラインと、組織のセキュリティ監査人または評価者の要求事項に基づくべきである。

1.2　CCM SSRM 実施ガイドライン

このセクションでは、実施ガイドラインの目的と範囲を紹介する。

1.2.1　目的と範囲

この文書には、CCM の 17 のクラウドセキュリティドメインのそれぞれの Control Specifications に合わせた実施ガイドラインが含まれている。実施ガイドラインは、組織を支援し、全ての CCM のセキュリティとプライバシーの Control Specification を実施するためのガイダンスを提供することを目的としている。

実施ガイドラインは、クラウドインフラストラクチャとサービスのセキュリティを実施し管理する責任に関して、CSP と CSC の間で、明確性と透明性を提供する。これは、契約上の義務を果たすことの説明責任と信頼を確立するために重要である。SSRM 実施ガイドラインは、CSP と CSC 間のクラウドセキュリティ責任に関する誤解や盲目的な思い込みに伴うリスクを軽減する。
このガイドラインはテクノロジーやベンダーに依存しない。つまり、特定のテクノロジーに合わせたものではなく、各 CCM Control Specification と同様に高いレベルで定義されている。ただし、クラウド組織が推奨しているようなコントロールを実施するためのベストプラクティスに関する詳細が含まれている。

Implementation Guidelines は、網羅的なものではなく、規範的なものでもない。むしろ、推奨事項を強調した一般的なガイドである。したがって、セキュリティ実務者は、記述、手順、リスク、管理策、文書類をカスタマイズし、特定のセキュリティ目的と実施に対応するように、リスク管理プログラムと（リスクアセスメントの範囲内の）クラウドサービスに合わせてこれらを調整しなければならない。

1.2.2　SSRM の構造と定義

CSP と CSC の双方が、当事者ごとの「一般的な」管理策の所有と実施責任を理解するのを支援するため、Implementation Guidelines と各 CCM Control Specification 内に「CSP-Owned」、「CSC-Owned」、「Shared Independent／Dependent」という SSRM 表現を採用する。

これらの SSRM 表現の意味については、以下で詳しく説明する。

「Control Ownership」 **CSP-Owned**	この管理策は、「CSP-Owned CSP が所有」し、自ら実施する責任がある。 CSP は、CCM 管理策の実施に全責任と説明責任を負う。CSC は、管理策を実施する責任を負わない。

「Control Ownership」 **CSC-Owned**	この管理策は、「CSC-Owned CSC が所有」し、自ら実施する責任がある。 CSC は、CCM 管理策の実施に全責任と説明責任を負う。CSP は、管理策を実施する責任を負わない。
「Control Ownership」 **Shared** **(Independent)**	この管理策は、CSP と CSC の両者で「Shared Independent（互いに依存しない形で）共有」し、それぞれ独立して実施する責任がある。 CSP と CSC の両方が、CCMcal の実施責任および説明責任を共有する。 例 CSC が実施する独立監査は CSP に影響を与えず、逆もまた同様である。 CSP と CSC の両方が訓練演習を実施しなければならないが、それぞれ独立して実施する。
「Control Ownership」 **Shared** **(Dependent)**	この管理策は、CSP と CSC の両者で「Shared Dependent（互いに依存する形で）共有」し、それぞれ実施する責任がある。 (一方の当事者は他方の当事者にサポートを提供しなければならない)。 CSP と CSC の両方が、CCM 管理策の実施責任および説明責任を共有する。 例 CSP は、CSC が要求する地理的場所へデータを移動できるように、データ保管する地理的場所の変更を認めるべきである。CSP による移動を促進するために、CSC は希望する場所を選択すべきである。 CSP は ID およびアクセス管理ツールと機能を CSC に提供するが、CSC はアクセス権限を適切に設定する必要がある。

上記の SSRM 表現タイプは、CAIQ（Consensus Assessment Initiative Questionnaire）の「SSRM Control Ownership」欄と一部一致している。それに加えて、ここでは "Independent"と "Dependent"という新しい用語が導入されている。

CCM 管理策ごとに表示される実施ガイドラインの構成をここに示す。

Table1 は、各 CCM Control Specification を Title、ID、Specification の記述を引用して紹介し、SSRM 表現と実施ガイドラインの該当するコントロール範囲を設定する。

Table1： CCM Control Title, ID and Specification

Control Title	Control ID	Control Specification
監査・保証のポリシーと手順	**A&A-01**	監査・保証のポリシーと手順と標準について確立、文書化、承認、伝達、適用、評価、維持を少なくとも年 1 回レビューする。

Table2 は、SSRM 表現と、それが 3 つのクラウドサービスモデルにおいてどのような位置づけにあるかを紹介している。

Table2： SSRM Control Ownership by Service Model

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared （Independent）	Shared （Independent）	Shared （Independent）

Table3 は、SSRM と整合しており、SSRM 表現の選択についての正当性の根拠と、CSP と CSC の 2 つのクラウドパーティそれぞれに適用される内容に該当する実施ガイドラインを示している。

Table3： SSRM control ownership rationale and Implementation Guidelines

SSRM Guideline	
CSP	**CSC**
管理策所有権の根拠 （ここにテキストが表示される） 実施ガイドライン すべてのサービスモデルに適用可能： （ここにテキストが表示される）	管理策所有権の根拠 （ここにテキストが表示される） 実施ガイドライン すべてのサービスモデルに適用可能： （ここにテキストが表示される）

1.2.3 対象読者

本書の対象者は、クラウド利用者、クラウドプロバイダー、クラウド監査人、CCM の新規導入者を支援する専門家ユーザー、CCM 管理策導入の最適なアプローチを学ぶ初心者などである。

本書は、読者が CCM4.0、CAIQ、および CSA セキュリティガイダンスに精通し、知識を持っていることを前提としている。
読者の皆さんは、このガイダンスを参考に、業界標準のプラクティスに従い、導入過程を革新することが奨励される。

1.3 バージョン管理

CCM 実施ガイドラインが大幅に改訂され、バージョン 1.0 から現在のバージョン 2.0（2024 年 5 月 8 日）に移行した。今回の更新では、以下の拡張が行われている。

- クラウドコントロールマトリックス（CCM）管理策仕様に、セキュリティ責任共有モデル（SSRM）表現が追加された。これらの表現（「CSP-Owned」、「CSC-Owned」、または「Shared Independent/Dependent」）は、クラウド組織が CCM 管理策をデプロイする際に、セキュリティの実施責任を明確に定義するのに役立つ。
- 割り当てられた SSRM 表現をさらにサポートし、裏付けるために、各 CCM Control Specification に管理策所有権の根拠説明が追加された。
- セキュリティ責任共有モデルに沿った CCM Control Specifications には、クラウドサービスプロバイダー（CSP）とクラウドサービス利用者（CSC）の両方に合わせた、拡張され包括的かつ専用の実施ガイドラインが含まれるようになった。

2　実施ガイドライン

Control Domain A&A

2.1　監査と保証(A&A)

Control Title	Control ID	Control Specification
監査・保証のポリシーと手順	**A&A-01**	監査・保証のポリシーと手順と標準について確立、文書化、承認、伝達、適用、評価、維持を少なくとも年１回レビューする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； クラウドサービスプロバイダー(CSP)とクラウドサービス利用者(CSC)は、どちらもこの管理策の実施に責任を負うが、各当事者は、それぞれのビジネスニーズ、監査、保証、およびコンプライアンス要件を満たすために、ポリシーと手順を独自に策定する必要がある。 CSP のクラウドスタックの監査を実施するための CSP の言明は、CSC のクラウドの使用、および標準や規制の範囲に対するコンプライアンス要件には拡張されない。CSP の言明は、インフラストラクチャ・ホスティングなど、主要なサービスを提供するために依存しているサブサービス組織についても考慮すべきである。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； **全てのサービスモデルに適用：** CSP は、業界のベストプラクティスおよび関連する標準に基づく正式なポリシーと手順を確立し、情報セキュリティ標準およびガイドラインに必要な基本水準を従業員に教育すべきである。監査・保証活動を準備し計画するために、規制上及び契約上の要件、または ISO/IEC 27001、AICPA TSC (SOC 2)、CSA CCM などの標準におけるセキュリティ要件に対する、承認され組織化されたアプローチを確立し、文書化すべきである。 ポリシーには、以下に関する規定が含まれるべきである（ただし、	**実施ガイドライン；** **全てのサービスモデルに適用：** CSC は、CSP サービスを使用する場合、CSC が要求する管理策目標が十分に達成されていることを裏付ける適切な監査証拠と契約上の証明を提供することを、ポリシーと手順の中に明記すべきである。証明レビューでは、インフラストラクチャ・ホスティングなど、CSP が主要なサービスを提供するために依存しているサブサービス組織についても考慮すべきである。CSC は、CSP の利用が CSC の規制及びコンプライアンス範囲に準拠しているかどうかを把握すべきである。

これに限定されない）：

a. 範囲と目的
   i. 監査対象となるクラウドサービス、環境及びデータを含む、監査及び保証活動の範囲を定めるべきである。
   ii. リスクが最も高いドメインを優先し、定義されたビジネス目標に沿ったリスクベースの監査計画を策定すべきである。
   iii. 監査完了のための権限と説明責任を明確にし、監査に応じるおよび／または監査に協力するための要件を定めるべきである。
b. 独立した評価：関連する標準、セキュリティポリシー、法的及び契約上の要求事項への準拠を評価するために、資格のある独立した第三者監査人による独立した評価を実施するための要件。
   i. 監査人は、監査を実施するために必要かつ関連性のある情報およびリソースのみにアクセスできる最小限の特権を有するべきである。
   ii. 監査人の客観性と独立性を維持するために、利益相反ポリシーを設けるべきである。
c. リスクベースの計画評価：クラウド環境内のセキュリティリスクと潜在的なセキュリティ脆弱性を特定、評価、および軽減するための CSP のリスクベースの計画と内部ポリシーの有効性の評価に関する要件。
d. 遵守要件：データプライバシー法、業界固有の規制、および監査に適用される顧客の契約上の義務を含む、適用される全ての標準、規制、法的／契約要件に対する CSP のクラウドセキュリティの実務の遵守を検証するための要件。
e. 監査管理プロセス：クラウドセキュリティ監査の計画、実施、報告を管理する監査管理プロセス。これには、監査の範囲、頻度、方法論、監査要員の役割と責任の定義が含まれる。
f. 是正措置：監査発見事項に適時かつ効果的に対処するためのリスクベースの是正処置計画。計画には次の内容が含まれるべきである：
   i. 監査発見事項レビューを体系化し、あらゆる発見事項を把握する。
   ii. 潜在的な影響と発生可能性に基づいて、発見事項に優先順位をつける。
   iii. 改善のための明確なオーナーシップとスケジュールを割り当て、特定された問題の解決に向けた進捗を追跡する。

さらに、CSP は是正状況を定期的にレビューし、関連する利害関係者に報告すべきである。

g. 承認：組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与
   i. ポリシーと手順の変更または修正について、承認プロセスを確立すべきである。
   ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すべきである。

ポリシーには、以下に関する規定を含むべきである（ただし、これに限定されない）：
CSP に提供されるポリシーが適用される。

h. コミュニケーション：ポリシーと手順の効果的なコミュニケーションは、関係する全てのクラウド利害関係者に対して促進されるべきである。活動の記録を必要とする関連する利害関係者とのコミュニケーションチャネルを確立し、監査発見事項、監査に関連する問題及び是正戦略の報告書を提供すべきである。 i. 維持とレビュー：監査・保証のポリシーと手順は、進化するクラウドセキュリティの状況との整合性を確保し、クラウド技術、規制及びリスクの変化を反映するために、少なくとも年 1 回は文書化、レビュー、更新すべきである。	

Control Title	Control ID	Control Specification
独立した評価	**A&A-02**	少なくとも年 1 回、関連する標準に従って独立した監査および保証評価を実施する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC は、ともにこの管理策の実施に責任を負うが、各当事者はそれぞれの規制上及び契約上の義務に従い、独自にこの管理策を実施する必要がある。CSP の独立した監査・保証評価は、自らのクラウドサービスのインフラストラクチャのセキュリティポスチャを測定するために利用することができる。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。 CSC はまた、契約上の合意に基づき、CSC の要件が遵守されていることを証明するために、CSP に対して独立した評価を実施すべきである。
実施ガイドライン； **全てのサービスモデルに適用：** CSP は、A&A-01 で規定される独立した保証および監査活動を定期的に実施すべきである。CSP はまた、コンプライアンス・管理策が適用され、関連する標準に準拠していることを証明するためのプラットフォームを提供し、従うべきである。 監査活動は、組織全体およびそのサービス提供に年間を通じて少なくとも何らかの監査活動が含まれるように、ローテーション期間内で、多かれ少なかれ特定の分野をカバーするように範囲を変えてもよい。 この管理策の観点における監査・保証とは、以下の内容を意味する： a. 自己評価の第三者検証 b. 実体管理策レビューおよび証拠に基づく主張評価	**実施ガイドライン；** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。 CSC がクラウドサービスモデル（IaaS など）を選択し、CSP と契約することによって、独立した監査・保証活動において、どの程度の責任が求められ、何が要求されるかが決定される。

c. 侵入テスト、脆弱性スキャン、レッドチーム演習などの履行または管理策の有効性テスト 監査活動は、有能な独立した内部または外部の当事者によって実施されるべきである。	

Control Title	Control ID	Control Specification
リスクベースの計画評価	**A&A-03**	リスクベースの計画とポリシーに従って、独立した監査と保証評価を実施する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC は共にこの管理策の実施に責任を負うが、各当事者は、各自のリスクベースの計画及ポリシー、規制上及び契約上の義務に従って、独自に実施する必要がある。CSP の独立した監査・保証評価は、自社のクラウドサービスのインフラストラクチャのセキュリティ態勢を測定するために利用することができる。ただし、CSC は、自社（CSC）の要件への準拠を実証するために、CSP に対しても独立した評価を実施すべきである。CSP と CSC はともに、変化するリスクが監査・保証の評価に与える影響をレビューする責任がある。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。 CSC は、CSP の管理策及び評価に依拠する場合、自らのリスクに基づき、その適合性をレビューすべきである。
実施ガイドライン； **全てのサービスモデルに適用：** CSP は、リスクベースのアプローチを用いて、独立した保証・監査活動の体制を実装すべきである。CSP は、監査およびリスク管理標準における業務活動および手順を遵守することが推奨される。 CSC は一般的に、CSP によって、または CSP のために依頼された独立した監査、評価及び証明に依拠する必要があるため、CSP は、独立した保証活動の目的と範囲が明確に定義され、その目的と範囲が文書化され、十分な明確性と具体性をもって CSC に伝達されることを確保すべきである。 特に、CSP の目的および範囲の文書化は、明確かつ曖昧さを排除し、ど	**実施ガイドライン；** **全てのサービスモデルに適用：** CSC は、リスクベースの効果的な内部監査および外部監査スキームを実装すべきである。内部監査におけるリスク評価は、CSC の内部チームによって実施されるべきである。そこでは、優先順位、検討すべき詳細、監査の実施頻度、及び CSC が晒される一般的なリスクを決定するべきである。外部評価は、独立した組織により実施されるべきである。 CSC の監査マネジャーは、監査の範囲及びサイクルを記した報告書を作成すべきである。また、監査人と協働して、様々な部門や機能が抱えるリスクを評価すべきである。

のクラウドサービス、どのリソース（データを含む）、およびどのサービスの機能およびオプションが評価されたかについて具体的に記述されるべきである。これにより、CSC は、CSP が提供する保証活動及び報告書を十分かつ適切に信頼することができる。	監査では、独立した第三者組織による SOC（System and Organization Controls）報告書などが活用できる場合がある。 a. CSC のデプロイモデルの選択は、ビジネスニーズ及び CSC が負うべき責任によって決定される。 b. CSP が提供する独立した監査、評価、証明及びその他の第三者による保証に依拠しようとする場合、CSC は、文書化された目的及び範囲に細心の注意を払い、CSC が利用するサービスが適切にカバーされていることを確実にしなければならない。 CSC は、SSRM の中でその責務を果たすために、以下を実施すべきである： a. 規制及び標準に沿った、独立した第三者によるコンプライアンス監査・保証活動の実施 b. 監査・保証活動の範囲及び標準の、定期的な更新及び再評価

Control Title	Control ID	Control Specification
要件のコンプライアンス	**A&A-04**	監査に適用される全ての関連する標準、規則、法的／契約上の要件、法的要件への準拠を検証する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠； CSP と CSC は共にこの管理策の実施に責任を負うが、各当事者はそれぞれのクラウドセキュリティ、規制及び契約上の要件に従って独自に実施する必要がある。	**管理策所有権の根拠；** この管理策の実装責任は CSP と CSC の間で共有され、各当事者は独立して実装すべきである。 より具体的には、CSP の監査は、CSC が使用するテクノロジースタックの一部のみを対象とする場合がある。この監査では、CSC がどのようにスタックを利用し、サービスを構成し、アクセスを管理し、サービス利用を監視し、クラウドに配置するデータを選択するかは除外される。その結果、CSP が関連する標準、規制、法律／契約、および法的要求事項を遵守している場合でも、CSC は自らのクラウド活動が遵守しているかどうかを評価する必要がある。 この目的を達成するために、CSC は、CSP が同じ標準、規制、法的／契約的要件及び法律上の義務への遵守を実証しているか否かに関わらず、適切な管理策及びプロセスを実装すべきである。したがって、CSC は、CSP の独立した監査のみに依拠すべきではなく、独自の監査活動を実施する必要があることを認識すべきである。
実施ガイドライン； **全てのサービスモデルに適用：** CSP は、サービスおよび業務を行っている法域に応じて、業界標準、規制、および法的要件に対する監査および評価を実施するべきである。 CSP は、自社内と、自社に代わって業務を行うサードパーティーサプライヤとの両方において、自社のクラウドサービス提供に影響する法的および規制上の要件を特定し、文書化するプロセスを実装するべきである。 プロセスは次の通りであるべきである： a. 組織が事業を行う管轄区域、すなわち地域、国、州を網羅する。 b. 以下を組み込む： i. セキュリティに特化した法律または規制 ii. セキュリティ管理策に影響を及ぼす法律又は規制 c. クラウドサービス、それに関連するシステム、およびそのデータに適用される規制、法令、契約、またはその他のコンプライアンス要件を特定する。 d. クラウドサービスを構成し、サポートするためのデータ、技術及びプロセスに対して要求される、具体的な技術上および管理上のコンプライアンス要件を特定する。一般的に、これには、以下を含むべきである： i. 特別な規制要件の対象となるオブジェクト及びデータ要素、システム設定及び性能、メタデータ、イベント、アクティビティ及びプロセス ii. オブジェクト、システム設定、メタデータ、アクティビティ、プロセスにどのような特定の要件が適用されるか	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
監査管理プロセス	**A&A-05**	監査計画、リスク分析、セキュリティ管理評価、結論、是正スケジュール、レポート作成、過去のレポートと裏付け証拠の見直しをサポートするための監査管理プロセスを定義し、実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC は共にこの管理策の実施に責任を負うが、各当事者はそれぞれ、独自の法律、規制及び契約上の義務に従って、独自に実施する必要がある。	**管理策所有権の根拠；** この管理策はシェアードであり、これは、CSP と CSC はそれぞれ独立して管理策要件を実施すべきであることを意味する。それでもなお、CSC は CSP の独立した監査のみに依存すべきではなく、独自の監査活動を実施する必要があることを認識すべきである。
実施ガイドライン； **全てのサービスモデルに適用：** CSP は、実施頻度及びスケジュールを含む監査計画を策定すべきである。監査計画は、内部監査計画と外部監査計画の両方を有するべきである。 セキュリティ管理策評価計画は、管理策がどの程度正しく実装され、意図したとおりに運用され（有効であり）、望ましい結果をもたらしているかを判断するための内部監査活動の一部であるべきである。 監査の目的は次の通り： a. 該当分野に関連するポリシー、標準、手順が効果的に実装されていることを確実にする。 b. リスク管理の実装の有効性を確実にする。 c. 組織のセキュリティプログラム／情報セキュリティ管理システムに含まれる管理策の有効性を確実にする。 d. 必要に応じて、実装の不備を打開するための改善勧告を行う。 e. 管理策の実施が法律及び規制に準拠していることを確実にする。 CSP は、次のベストプラクティスを遵守すべきである： f. 十分な能力を有する人員の利用可能性を確保する。	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

g. 監査の重要性及び利点を強調する。 h. ワークフロー及びタイムラインを設計し、実装する。 i. 監査及びその他の成果物の十分なレビューの重要性を強調する。 j. 監査管理プロセスの有効性を評価するために、レビュープロセスのアウトプットを活用する。	

Control Title	Control ID	Control Specification
修復	**A&A-06**	監査結果を是正するためのリスクベースの是正措置計画を確立、文書化、承認、伝達、適用、評価、維持し、見直しおよび関連する利害関係者に是正状況を報告する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC は共に監査指摘事項を是正するためのリスクベースの是正措置計画を策定する責任を負うが、各当事者はそれぞれ独自の法律、規制及び契約上の義務に従って、独自にこれを実施する必要がある。	**管理策所有権の根拠；** この管理策はシェアードであり、これは、CSP と CSC はそれぞれ独立して管理策要件を実施すべきであることを意味する。しかし、CSC は、CSP が実施した独立した監査のみに依存してはならないことを認識することが重要である。CSC は、監査で発見された事項の是正活動に自ら取り組むべきである。 CSC は CSP を直接監査することはできないが、CSP との契約書に規定された範囲内において、監査権を行使する権限を保持している。
実施ガイドライン； **全てのサービスモデルに適用：** CSP は、リスクを低減し管理するために、リスク管理プログラムを維持しなければならない。経営陣は、自らの責任範囲内のリスクを特定し、それらのリスクに対処するための適切な手段を実装することを義務付けるプロセスを有するべきである。 監査・保証活動において発見された事項は、適切なレベルで十分な注意と配慮が払われるべきである。管理策の不備（発見事項）が識別された場合、その不備は優先順位を設定し、設定するために評価されなければならない。優先順位が設定された後、適切なリスク対応策が選択されるべきである。	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

リスク対応のための選択肢は明確に定義され、評価されるべきである。これには次のようなものを含む： a. 管理策の有効性を高めることにより、リスク低減する。 b. 代替となる管理策を実装する事により、リスク低減する。 c. リスクの全部または一部を回避する（すなわち、特定のビジネス上のイニシアチブを追求しないことを決定する）。 d. リスクの全部または一部を受容する。 リスク対応活動は次のようにすべきである： e. 承認されたリスク対応計画の文書化 f. 説明責任を確保するための割り当て g. 合意された目標期日に対するモニタリング h. 組織のポリシーに従った報告 i. 一連の完了指標の設定と、完了に向けた日常的なモニタリングが重要である。	

Control Domain AIS

2.2 アプリケーションとインタフェースのセキュリティ (AIS)

Control Title	Control ID	Control Specification
アプリケーションとインタフェースのセキュリティポリシーと手順	**AIS-01**	アプリケーションセキュリティのポリシーと手順を確立、文書化、承認、伝達、適用、評価、維持して、組織のアプリケーションセキュリティ機能の適切な計画、提供、およびサポートに指針を提供する。ポリシーと手順を少なくとも年 1 回レビューし、更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、クラウドのサービスモデル（IaaS、PaaS、SaaS）に影響されない。CSP と CSC の双方は、組織内で有効なクラウドサービスモデルに基づいて、アプリケーションセキュリティ機能の開発及び実装を指導するための独自のポリシーと手順を独自に確立する必要がある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、クラウドアプリケーションおよびアプリケーションインタフェースのセキュアな開発および実装を導くためのポリシーと手順を確立する必要がある。ポリシーは、CSP の目的および戦略、並びに継続的な改善に対する経営層のコミットメントに沿うものでなければならない。 ポリシーには、以下に関する規定を含める必要がある（ただし、これに限定するものではない）： a. 範囲と目的：クラウド組織は、AIS のポリシーと手順の範囲と目的を定義する必要がある。 i. 以下を含むポリシーと手続きの範囲： • クラウド環境とその中でカバーすべきアプリケーションやインタフェース（API） • クラウドベースのアプリケーションの開発およびデプ	**実施ガイドライン：** CSP の「実装ガイドライン」が適用される。

ロイに関与するサードパーティーベンダーに対するポリシーと手順の適用可能性
- 開発、セキュリティ、運用、法務など、さまざまなチームからの要件の取り入れ、部門横断的な側面への対処を含む。

ii. ポリシーと手順の目的：
- 機密データや個人データの保護、不正アクセスの防止、アプリケーションの可用性の維持
- ポリシーと手順が、組織全体のセキュリティ戦略及びコンプライアンス要件と整合していること
- ポリシーと手順を実施し遵守することによって期待される成果（例えば、脆弱性リスクの低減、セキュリティポスチャの改善）。

b. アプリケーションのセキュリティベースライン要件：全てのクラウドベースのアプリケーションと API の最小セキュリティ要件の概要を示す一元化されたセキュリティベースラインを確立し、文書化し、実装し、評価するための要件。このベースラインは、業界標準（OWASP など）、ベストプラクティス、組織固有のリスク許容度に基づく必要がある。

c. アプリケーションのセキュリティ指標：アプリケーションセキュリティ管理及びプロセスの有効性を追跡するために、定期的にレビュー・報告を行い、傾向と改善ドメインを特定可能な指標。

d. セキュアなアプリケーション開発：開発プロセス全体（脅威モデリング、セキュアな設計とコーディングのガイドライン、セキュリティテストとコードレビュー、是正措置、セキュアコーディングトレーニングなど）にわたってセキュリティの実践を取り入れた SSDLC ガバナンスフレームワークを定義し、確立するための要件。

e. アプリケーションセキュリティテストの自動化：開発プロセスの早い段階で脆弱性を特定するために、アプリケーションセキュリティテストツール（可能であれば自動化されたもの）を SSDLC に統合すること。

f. セキュアなアプリケーションの自動デプロイ：アプリケーションがセキュアかつ一貫してデプロイされることを確実にするためのデプロイパイプライン（可能であれば自動化）の要件（コードレビュー、脆弱性スキャン、セキュリティ構成管理など）。

g. 自社又はサードパーティーサプライヤによるアプリケーション開発：組織向けにクラウドベースのアプリケーションを開発またはデプロイするサードパーティーベンダーのセキュリティ要件（組織のセキュリティ基本ポリシーと整合させ、SSDLC の全フェーズをカバーする必要がある）

i. サードパーティーベンダーと契約する前に、各サードパーティーベンダーのリスク評価を行い、ベンダーのセキュリティ慣行、経験、評判を評価する。

ii. サードパーティーベンダーに対して、組織のセキュリティ要件に準拠する契約上の義務を設定する。

h. アプリケーションの脆弱性修復：クラウドベースのアプリケーションの脆弱性を特定し、優先順位を設定し、修復するための

脆弱性管理要件（可能な場合は自動化ツールを使用）。要件には、リスクの高い脆弱性に対する修復およびエスカレーション手順の明確なタイムラインを含める必要がある。 i. 組織の戦略目標とリスク選好との整合性を確保するための承認要件と上級管理職の関与。 i. AIS ポリシーと手順の変更または修正についての、承認プロセスの確立。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）の維持。 j. コミュニケーション：開発者、運用チーム、CSC など、関係する全てのクラウド関係者に、ポリシーと手順を効果的に伝える必要がある。 k. メンテナンスとレビュー：アプリケーションのセキュリティポリシーと手順を文書化し、少なくとも年 1 回見直し、更新して、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映する。	

Control Title	Control ID	Control Specification
アプリケーションセキュリティのベースライン要件	**AIS-02**	様々なアプリケーションを保護するためのベースライン要件を確立、文書化、維持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施は、提供するクラウドのサービスモデル（IaaS、PaaS、SaaS）に影響されない。CSP と CSC の両方が、提供または利用される様々なクラウドアプリケーションをセキュアにするためのベースライン要件を確立し、文書化し、維持する責任を負う。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。

実施ガイドライン：

全てのサービスモデルに適用：

ベースライン要件は、以下を含むべきであるが、これに限定されるものではない：

a. アプリケーションの分類：
   i. リスクベースのアプローチを使用して、機密性、重要性、扱うデータの種類、および規制要件に基づいて、関連する全てのクラウドアプリケーションと API を特定、分類、分類する必要がある。
   ii. アプリケーションの種類ごとに特定のセキュリティ要件を確立する必要がある。(例：構成、アクセス制御、暗号化、脆弱性管理、インシデント対応)
b. ベースライン要件の文書：
   i. セキュリティ要件仕様書(SRS)の中で、アプリケーションタイプごとにセキュリティ基本ポリシーを文書化する。
   ii. 各セキュリティ要件に対し、実施すべき具体的なセキュリティ管理策、構成、手順に関する詳細を含める。
c. ベースライン要件の実施：
   i. クラウドインフラストラクチャの機能とサードパーティセキュリティツールを使用して、文書化されたセキュリティ要件に対応するセキュリティ管理策を実装する。
   ii. セキュリティ制御の実装と構成は、Infrastructure as Code（IaC）ツールを使って実施する。
   iii. セキュリティ管理策を SSDLC に統合し、確立されたベースライン要件に準拠して、セキュリティがライフサイクルの全フェーズにわたって確実に組み込まれるようにする。
d. ベースライン要件の見直しと更新：
   i. セキュリティベースライン要件は、アプリケーション技術の変化、脅威の進化、業界標準、継続的なモニタリングとアセスメントプロセスから得られる可能性のある知見、組織のリスクプロファイルを反映して、定期的に見直して更新する。
   ii. セキュリティインシデントや監査から学んだ教訓を、セキュリティ基本ポリシーに組み入れる必要がある。
   iii. ベースライン要件は、定期的に、および／または、重要な変更があった場合に、経営陣によってレビューされ、承認される必要がある。
e. ベースライン要件の遵守：
   i. リスクアセスメントを実施し、クラウドアプリケーションのセキュリティと構成がベースライン要件と整合していることを評価する。
   ii. クラウド環境に統合する前に、サードパーティー製アプリケーションが確立済みのベースライン要件に適合していることを、徹底的なセキュリティ評価によって確認した上で、ベースライン要件をサードパーティー製アプリケーションにも拡大する。
   iii. セキュリティ違反の検出と是正には、自動化ツールを使

実施ガイドライン：

CSP の「実装ガイドライン」が適用される。

さらに、IaaS 及び PaaS の CSC は、提供されるクラウドサービス及びアプリケーションのセキュリティに関するベースライン要件を策定する。ただし、SaaS の CSC は、基盤となるインフラストラクチャ及びプラットフォームを管理する CSP 及びサードパーティーが提供するセキュリティベースライン要件の採用を検討する必要がある。CSC は、自社のアプリケーションスタックに対して、承認された構成が確実に適用されるようにする必要がある。

用する。 f. 継続的なモニタリングと評価継続的なセキュリティ監視、脆弱性評価、コンプライアンスチェックのために、自動化ツール、手動のレビュー、定期的な侵入テストを採用し、ベースライン要件の継続的な遵守を確保する。	

Control Title	Control ID	Control Specification
アプリケーションセキュリティ・評価指標	**AIS-03**	ビジネス目標、セキュリティ要件、コンプライアンス義務に合わせて、技術的および運用上の測定標準を定義し、実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施は、クラウドのサービスモデル（IaaS、PaaS、SaaS）に影響されない。CSP と CSC の両方が、提供または利用される様々なクラウドアプリケーションをセキュアにするためのベースライン要件を確立し、文書化し、維持する責任を負う。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、クラウドアプリケーションの技術的・運用的評価指標を導入することで、パフォーマンスを最適化し、コスト効率を高め、セキュリティを維持し、利用者の信頼を高めることができる。 クラウドアプリケーションセキュリティ評価指標を効果的に定義・開発するために、CSP は、ビジネス目標、セキュリティ要件、およびコンプライアンス義務に沿った構造化されたアプローチに従う必要がある。 評価指標は、その説明と基礎データを収集する効率的かつ効果的な方法を含むように文書化される必要がある。 a. 目的と範囲の決定：	**実施ガイドライン：** CSP の「実装ガイドライン」が適用される。

i. 指標の目的を決定する（例えば、セキュリティポスチャ、コンプライアンス遵守、リスク軽減の有効性を測定するため）。
ii. 指標の対象となる特定のクラウドアプリケーションまたは環境を特定する。

b. 主要なセキュリティドメイン
i. セキュリティ指標を、関連するドメイン（脆弱性管理、アクセス制御、データ保護、インシデント対応など）に分類する。
ii. 指標は、組織のセキュリティポスチャとビジネス目標に対する重要性に基づいて優先順位を付ける。

c. 測定可能なパラメータ：
i. 各セキュリティドメインについて、セキュリティポスチャを正確に反映する具体的な測定可能パラメータを特定する。
ii. 選択したパラメータが定量化可能で、一貫性があり、業界標準に沿ったものであることを確認する。

d. しきい値とベンチマーク：
i. 各評価指標の許容しきい値を定義し、セキュリティ性能の許容レベルを示す。
ii. 指標パフォーマンスを業界ベンチマークや社内目標値と比較し、セキュリティポスチャを評価する必要がある。

e. データ収集と集計：
i. セキュリティツール、ログ、クラウドプロバイダーのAPIなど、関連するソースから生データを収集する仕組みを確立する。
ii. 収集されたデータは、分析と報告のために意味のある指標に集約される必要がある。

f. データ分析と可視化：
i. データ可視化ツールを活用して、指標を明確で分かりやすいダッシュボードやレポートに表示する。
ii. 測定データの傾向とパターンを分析し、潜在的なセキュリティ上の問題点や改善点を特定する。

g. 既存のプロセスとの統合：
i. セキュリティ評価指標を、既存のセキュリティレポーティングとリスクマネジメントプロセスに統合することを検討する。
ii. 意思決定に情報を提供し、セキュリティ投資の優先順位を決定するために、指標が使用されるようにする。

h. 継続的なモニタリングと評価：
i. 指標のパフォーマンスは定期的に監視し、クラウドアプリケーションのセキュリティポスチャを測定する際の有効性を評価する。
ii. 指標は、セキュリティ要件とビジネス目標の進化に合わせて改良し、適合させる必要がある。
iii. アプリケーションセキュリティポスチャーの有効性を追跡し、定量化し、可視化するために、評価指標（KPIやKRIなど）から、さまざまな対象者を対象とした各種レ

ポートを作成する。

i. 指標の SMART フレームワーク：SMART フレームワークを採用することができる。SMART とは、Specific（具体的）、Measurable（測定可能）、Achievable（達成可能）、Relevant（関連性）、Time-bound（期限）の頭文字をとったものである。
   i. 具体的である事：指標は、曖昧さを残さないように明確に定義する必要がある。パフォーマンスや有効性の特定の側面に焦点を当てられるように具体的である必要がある。
   ii. 測定可能である事：指標は定量化可能であり、追跡や比較が可能な測定単位で表されるようにする。評価指標の価値を評価するためにデータを収集し、分析することが可能でなければならない。
   iii. 達成可能である事：指標は、組織の能力とリソースの範囲内で、現実的かつ達成可能なものでなければならない。過度に野心的な目標を設定すると、落胆やフラストレーションにつながる可能性があり。
   iv. 関連性がある事：指標は、組織の目標や目的に沿ったものでなければならない。戦略目標の達成に直接貢献する有意義な情報を提供するものである必要がある。
   v. 期限付きである事：指標は、測定と評価のための明確な時間枠を持つべきである。これにより、進捗状況を追跡し、長期的な傾向を把握することができる。

エラー削減と効率化のために、測定値収集、レポート作成、意思決定手順を自動化するツールやツールチェーンを採用する必要がある。

継続的な改善とサービスの成熟のために、傾向と比較分析を取り入れる必要がある。CSP は、測定結果を使用して SSDLC プロセスを改善する必要がある。全プロセスは、所定のスケジュールで、または組織の要求に応じてレビューされる必要がある。

ユースケース例：
「指定された期間内に修復された脆弱性の割合（Percentage of vulnerabilities remediated within a specified timeframe）」という評価指標を例にとって、本管理策で規定される技術的対策がどのように適用されるかを確認する。この指標は、脆弱性管理（Vulnerability Management）ドメインに該当し、脆弱性修復の取り組みの有効性を測定する。

a. 目的と範囲の決定：
   i. 目的：脆弱性を適時に是正し、潜在的な攻撃にさらされる機会を減らす組織の能力を測定する。
   ii. 範囲：全てのクラウドアプリケーションとインフラストラクチャコンポーネント
b. 主要なセキュリティドメイン
   i. パッチが適用されていない脆弱性は、攻撃者に悪用されて不正アクセスを受けたり、システムを侵害されたりする可能性がある。

c. 測定可能なパラメータ：
   i. 指標「指定された期間内に修復された脆弱性の割合」は、組織の脆弱性修復パフォーマンスを直接定量化する。
d. しきい値とベンチマーク：
   i. 重要な脆弱性の 90%を 7 日以内に、深刻度の高い脆弱性の 70%を 14 日以内に修復するなど、脆弱性修復の目標しきい値を設定する。
   ii. 業界ベンチマークまたは社内目標値に対する指標パフォーマンスを比較し、脆弱性修復の有効性を評価する。
e. データ収集と集計：
   i. 脆弱性スキャンツールを活用し、クラウドアプリケーションとインフラストラクチャコンポーネント全体の脆弱性を特定する。
   ii. 脆弱性スキャンの結果を一元的な脆弱性管理プラットフォームと統合し、修復の進捗を追跡する。
f. データ分析と可視化：
   i. 指定された期間内に修復された脆弱性の割合を追跡するレポートとダッシュボードを作成する。
   ii. 脆弱性修復のパフォーマンスの経時的な傾向を可視化し、改善すべきドメインを特定する。
g. 既存のプロセスとの統合：
   i. 組織のセキュリティリスク管理フレームワークに脆弱性修復の評価指標を組み込む。
   ii. 指標データを使用して、脆弱性修復作業のリソース配分と優先順位を設定を行う。
h. 継続的なモニタリングと改善：
   i. 確立されたしきい値およびベンチマークに照らして、脆弱性修復のパフォーマンスを定期的に監視する。
   ii. 脆弱性管理プロセスの有効性を評価し、必要に応じて調整を行う。

例（概要）：
ある CSP は、重要な脆弱性の 95%を 7 日以内に修復するという目標を設定した。過去 1 か月間で、7 日以内に修復された重要な脆弱性の平均割合が 88%であった。これは、組織が目標を達成しておらず、脆弱性の修復プロセスを改善する必要がある可能性を示す。

その他の技術的指標の例としては、以下のようなものがある：
a. 脆弱性管理：
   i. 弱点別の脆弱性の数または割合
   ii. クリティカルで深刻度の高い脆弱性の数
   iii. 検出ソース（設計レビュー、コードレビュー、SAST、DAST、侵入テスト、VDP、バグ報奨金など）別の脆弱性の数または割合
   iv. 指定された期間内に修復された脆弱性の割合
   v. 検出された環境別の脆弱性の数または割合（プリプロダクションとプロダクションの比較）
   vi. 改善サービスレベル目標（SLO）を上回る件数
   vii. テストタイプ（SAST、DAST、SCA） ごとに、自動セキュリティテストを使用しているアプリケーションの数ま

たは割合 viii. 過去 "n"か月間に侵入テストを完了したアプリケーションの数あるいは割合 ix. 直近「n」カ月の間にアプリケーションセキュリティ研修を修了した開発チーム又は個人の数又は割合 b. アクセスコントロール： i. 最小特権アクセス権を持つユーザーの割合 ii. 不正アクセス試行回数 c. データ保護： i. 静止時および転送時に暗号化されたデータの割合 ii. データ損失インシデント数 d. インシデントレスポンス i. セキュリティインシデントの平均検出時間（MTTD）と平均対応時間（MTTR） ii. 封じ込めと修復に成功したインシデントの数	

Control Title	Control ID	Control Specification
セキュアアプリケーションの設計と開発	**AIS-04**	組織によって定義されたセキュリティ要件に従って、アプリケーションの設計、開発、導入、運用のための SDLC プロセスを定義し、実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、クラウドサービスの種類（IaaS、PaaS、SaaS）には影響されない。CSP と CSC は共に各クラウド当事者によって定義されたシステムセキュリティ要件に従って、セキュアなアプリケーションの設計、開発、デプロイメント、および運用のためのセキュアソフトウェア開発ライフサイクル（SSDLC）プロセスを独自に定義し、実施する責任を負う。 SaaS モデルのデプロイメントでは、この管理策は CSP にある。SaaS CSP は通常、すぐに使用できるアプリケーションとサービスを提供するのに対し、SaaS CSC はサービスを利用し、アプリケーション開発のための SSDLC を実装する責任は負わない。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。

実施ガイドライン：

全てのサービスモデルに適用：

CSP は、SSDLC プロセスを活用して、アプリケーションと API がクラウド環境でセキュアに設計、開発、デプロイ、運用されるようにする必要がある。開発ライフサイクル全体を通じてセキュリティのベストプラクティスを統合することで、CSP はアプリケーションを脆弱性やサイバー攻撃から効果的に保護することができる。

セキュリティ要件を定義することは、開発の全ての段階を通じてセキュリティが統合されていることを確実にするための、SSDLC プロセスの最初のステップである。セキュリティ要件は、セキュリティ目的、及び／又は、組織目標、規制要件から導き出す必要がある。プロジェクトの開始時及び SSDLC プロセスの各段階において、業界標準を適用する必要がある。SSDLC セキュリティを効果的に推進するため、役割と期待事項を明確に定義し、公表し、関連する利害関係者に伝達することが重要である。

SSDLC を導入する際には、以下のベストプラクティスに従う必要がある：

a. SSDLC ガバナンス：SSDLC に合わせたセキュリティガバナンスの枠組みを導入し、SSDLC 全体のセキュリティに関する役割、責任、及び説明責任を定義する。
   i. CSP の SSDLC プロセスは、最低限、規制および CSC のビジネス要件を満たすものとする。
   ii. CSP は、CSC の開示ポリシーと互換性のある範囲で、SSDLC に関する情報を CSC に提供する必要がある。
b. DevSecOps： 計画・設計から開発、テスト、デプロイ、運用に至るまで、SSDLC の全段階にセキュリティ対策を統合する DevSecOps アプローチを定義し、実施する。
c. 脅威モデリング：脅威モデリングを SSDLC の初期段階に組み込んで、潜在的なセキュリティリスクを特定し、緩和策を設計することで、開発者がセキュリティ問題を予期し、事前に対処できるようにし、開発サイクルの後半に脆弱性が侵入する可能性を低減させる。
d. セキュアなコーディングの実践
   i. 包括的なセキュリティ設計要件を定義し、アプリケーションのアーキテクチャ全体に実装するセキュリティ対策と管理策を規定する。
   ii. 業界標準（OWASP など）のセキュアコーディングガイドラインを SSDLC に組み込む必要がある。
   iii. セキュアコーディングガイドラインをそれぞれ遵守し、実施する（例えば、セキュリティヘッダーの適切な実装と設定、入力検証、情報出力処理、エラー処理、暗号化ライブラリの適切な使用）。
e. オープンソースコンポーネントのセキュアな使用：オープンソースコンポーネントの管理には、徹底した脆弱性スキャン、依存関係の管理、既知の脆弱性の継続的な監視など、セキュアな慣行を採用する必要がある。信頼できるオープンソースリポジトリを使用し、適切な帰属とライセンスコンプライアンスを確

実施ガイドライン：

CSP の「実装ガイドライン」が適用される。

保する。

f. 脆弱性管理：コード、インフラ、サードパーティコンポーネントの脆弱性を継続的にスキャンし、修正する（TVM ドメインを参照）。

g. セキュリティテスト：潜在的なセキュリティ上の弱点を特定し、対処するために、定期的なセキュリティ監査、静的、動的なアプリケーションセキュリティテスト、及び侵入テストを実施する（AIS-05 及び TVM-06 を参照）。

h. セキュアなデプロイと構成管理：

  i. クラウドベースのアプリケーションがセキュアな方法でデプロイされ、構成されるように、セキュアなデプロイと構成管理のプラクティスを実施する必要がある。

  ii. 自動化ツールを使用して、一貫した設定を実施し、セキュリティポリシーからの逸脱を監視する。

i. EoL プロセス：アプリケーションがエンドオブライフに達したとき、CSP は最低限以下のことを行う必要がある：

  i. EoL の日付を CSC に通知し、代替サービスへの移行方法を明確に指示する。

  ii. アプリケーションの技術サポートとアップデートの提供を中止し、アプリケーションのソースコードとドキュメントをアーカイブする。

  iii. 全てのアプリケーション関連データが適切に削除されるか、または CSC の指定の場所に転送されることを確認する。

  iv. 廃止措置の過程において、潜在的なセキュリティの脆弱性を検討・評価する。

CSP は、そのセキュリティ慣行について透明性を保ち、CSC に対し、セキュリティ要件を満たすために必要なツールとサポートを提供する必要がある。CSC は、SSDLC 全体を通じて CSP のセキュリティ要件が確実に実施され維持されるよう、 CSP と積極的に関わる必要がある。

Control Title	Control ID	Control Specification
自動化されたアプリケーションセキュリティテスト	**AIS-05**	新しい情報系システムの受け入れ、アップグレード、新しいバージョンに対する標準を含むテスト戦略を導入する。これによりアプリケーションのセキュリティが保証され、コンプライアンスが維持されるとともに、組織の迅速な導入目標が達成される。可能な場合は自動化する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。両当事者及びそれぞれが独立して、新情報システム、アップグレード及び新バージョンの受入 標準を含む強固なテスト戦略を実施する責任を負う。	**管理策所有権の根拠：** IaaS モデルと PaaS モデルでは、CSC はアプリケーションスタックを所有し、そのセキュアなテストとクラウドへのデプロイを確認する必要がある（CSP のガイドラインを参照）。SaaS モデルでは、SaaS CSP が通常すぐに利用可能なアプリケーションとサービスを提供する一方で、CSC は特定のニーズと要件に合わせてこれらのサービスを構成しカスタマイズする責任を負うことから、CSC の責任が生じる。したがって、CSC は、アップグレード、変更、または新システムや新バージョンの受け入れの標準が、組織のセキュリティ標準、コンプライアンス要件、およびアプリケーション固有のニーズに合致していることを確認する必要があり。厳格なテスト戦略を実施することで、SaaS CSC は、組織のワークフローに統合する前に、アップグレードや新システムの互換性、適切なセキュリティ、適切な機能を検証することができる。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、SSDLC の開発フェーズの早い段階で、開発者によるセキュリティ上の欠陥の特定を容易にし、適時の是正を可能にし、脆弱性が本番環境に実装されるリスクを最小化するために、セキュリティテストを組み込む必要がある。 アプリケーションセキュリティテスト戦略を実施するためには、以下のベストプラクティスに従う必要がある： a. SSDLC とテスト管理：開発チームは、SSDLC とセキュリティのベストプラクティスに従って、設計上セキュアなコードを作成するとともに、静的および動的な解析ツールを使用して、コードに存在するセキュリティの抜け穴を特定する。 b. 継続的な CI/CD テスト：継続的テストは CI/CD パイプラインに組み込む必要がある： i. CI/CD は単にコードを配信するだけでなく、継続的テストによる「シフトレフト」アプローチを採用する機会でもあることを理解する必要がある。 ii. コミット前フックとコミット後フックを実装し、使用する必要がある。 iii. 脆弱性スキャナを使用して、サードパーティー製ライブラリの問題を特定する。 iv. 自動化されたスキャナを使用して、アクセスキー、共通鍵、認証情報、秘密鍵などを含む、ハードコードされた／デフォルトの秘密を特定する必要がある。 c. 静的アプリケーションセキュリティテスト（SAST）：SAST は、アプリケーションのソースコード、バイトコード、または、バイナリコ	**実施ガイドライン：** IaaS と PaaS の CSC については、包括的なテスト戦略の一環として、CSP と同じガイドラインが適用され、さらに、新しいシステムと新しいバージョンのシステムおよびアプリケーションの適切な構成、アップグレード、およびセキュアな統合が保証される。 特に SaaS CSC に関しては、以下の実施ガイドラインが適用される： アプリケーションの構成：SaaS カスタマーは、特定のビジネス要件に従ってアプリケーションの設定と権限を構成し、アクセス制御、ユーザー権限、データ暗号化が適切に設定されていることを確認して、セキュリティリスクを軽減し、データプライバシーを維持する必要がある。 アプリケーションのアップグレード：アプリケーションのアップグレードを実施する前に、SaaS カスタマーは、機能テスト、互換性テスト、セキュリティテストなどの徹底的なテストを実施し、アップグレードによって既存のワークフローが中断されたり、アプリケーションのセキュリティ体制が損なわれたりしないことを確認する必要がある。また、アップグレードプロセス中に何らかの問題が発生した場合に備えて、ロールバックプランを維持することも必要である。 新システムのセキュアな統合：SaaS カスタマーは、新システムと既存のインフラストラクチャとの互換性を評価し、総合的な統合テストを実施して、統合プロセス全体を通じてデータの整合性、セキュリティプロトコル、アプリケーションの機能が維持されていることを確認する必要がある。新バージ

ードを分析して、開発ライフサイクルの早い段階で問題を検出し、セキュリティ脆弱性、コーディングエラー、攻撃者に悪用される可能性のある潜在的な弱点を特定するために使用されなければならない（例えば、データ／制御フロー、テイント分析）。

d. 動的アプリケーションセキュリティテスト（DAST）：DAST は、リクエストを送信し、レスポンスを分析することによって、セキュリティ脆弱性を特定するために、実行状態のアプリケーションをテストするために使用されなければならない（例えば、ファズテスト、セッションハイジャック、インジェクションテスト）。

e. 対話型アプリケーションセキュリティテスト（IAST）：IAST は、SAST と DAST の両方の要素を組み合わせ、ソースコードにアクセスすることなくセキュリティ問題を特定し、アプリケーションの実行中にセキュリティ脆弱性に関するリアルタイムのフィードバックを提供するために使用される必要がある。

f. 侵入テスト：潜在的な脆弱性を特定し、実施されているセキュリティ対策の有効性を評価するために、実際のサイバー攻撃をシミュレートする侵入テストを実施する必要がある。

g. 入力検証：入力検証のテストケースは、インジェクション攻撃（SQL インジェクション、コマンドインジェクション、クロスサイトスクリプティング（XSS）、クロスサイトリクエストフォージェリ（CSRF）など）を特定するために使用する必要がある。これには、入力データのタイプ、フォーマット、長さ、及び範囲をチェックし、入力データが事前に定義された規準を遵守し、悪意のある、あるいは、許可されていないコンテンツを含んでいないことを確認することが含まれる。

h. 情報出力処理：情報出力フィルタリングのテストケースは、情報流出攻撃（例えば、パスワードの平文出力）を特定するために使用する。

i. 業界のベストプラクティス：セキュリティのテストケースは、OWASP Top 10 に従って採用する。また、組織の戦略や要件に応じて、テストケースを各種コンプライアンス規格（ISO/IEC 27001、AICPA TSC など）と整合させることも検討する。

j. 継続的なモニタリング：アプリケーションがデプロイされたら、故障、DoS、DDoS、認証されていないスキャンなどをテストするために、継続的なモニタリングが必要である。

k. アプリケーションテストの自動化：
   i. テストチームは、テスト完了プロセスを迅速化し、エラーの削減とセキュリティギャップの顕在化に有効な自動化を活用する必要がある。
   ii. 自動化ツールは、既知と未知の両方の脆弱性についてアプリケーションをテストする必要がある。
   iii. 全てのシステムが同じように恩恵を受けるとは限らないため、アプリケーションに必要な自動化を評価するための標準を作成する必要がある。

SSDLC 全体を通して適切なレベルの保証を提供するためには、最低限、上記の複数のテストタイプと統合ポイントが必要となる。

ョンのシステム統合時に潜在的なセキュリティ脆弱性を軽減するために、セキュアな認証メカニズム、データ暗号化、アクセス制御を実装する必要がある。

セキュリティテストの自動化は、リスクとエラーを低減し、組織の要求に応じたセキュリティ対策の拡張を可能にするために実施する必要がある。SSDLC 全体を通じて適切なレベルの保証を提供するためには、複数のテストタイプと統合ポイントが必要になる可能性がある。全てのシステムが等しく恩恵を受けるわけではないので、アプリケーションに必要な自動化の評価標準を策定する必要がある。

Control Title	Control ID	Control Specification
セキュアなアプリケーション導入の自動化	**AIS-06**	セキュアで、標準化され、コンプライアンス準拠したアプリケーション導入のための戦略と機能を確立し、実装する。可能な場合は自動化する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。CSP は、セキュアなアプリケーションデプロイメントのための戦略を独自に確立し、実施する。	**管理策所有権の根拠：** IaaS モデルと PaaS モデルでは、CSC はアプリケーションとクラウドへのセキュアなデプロイメントを所有する。SaaS モデルでは、CSC は CSP からアプリケーションを消費するため、アプリケーションのセキュアなデプロイメントには責任を負わない。
実施ガイドライン： **全てのサービスモデルに適用：** アプリケーションのセキュアなデプロイメント戦略を実施するためには、以下のベストプラクティスに従う必要がある： a. 標準化されたデプロイメントプロセス：一貫性のあるセキュアなアプリケーションデプロイメントを保証するために、標準化されたデプロイメントプロセスを導入する必要がある。これには以下が含まれる： i. アプリケーションデプロイメントのニーズと業界標準に基づくセキュリティ要件の定義により、アプリケーションを不正アクセス、データ漏洩、その他のサイバーセキュリティの脅威から確実に保護する。 ii. 自動デプロイメント・パイプライン CI/CD を確立してデプロイメントプロセスを自動化し、手作業による介入やエラーを最小限に抑える。 iii. 一般的なアプリケーションシナリオのベストプラクティスとコンフィギュレーションをカプセル化した、標準化されたデプロイメントテンプレートを開発する必要がある。 iv. デプロイメントの失敗やセキュリティ上の問題が発生した場合は、自動または手動のロールバック手順を実施する。ロールバック手順を定期的にテストし、その有効性を確認する。 b. 自動化の要件：デプロイメントプロセスを合理化し、セキュリティ	**実施ガイドライン：** CSP の「実装ガイドライン」が適用される。

を強化し、全体的な効率を向上させるために、可能な限り自動化を優先する。これには以下が含まれる：

i. クラウドインフラストラクチャのプロビジョニングとコンフィギュレーションの自動化には、Infrastructure as Code（IaC）ツールを使用する必要がある。

ii. アプリケーションがクラウド環境に正しくセキュアにデプロイされていることを検証するために、自動テストを実施する必要がある（例：機能的な正しさのテスト、セキュリティ構成のテスト）。

iii. 自動パッチ管理システムの導入により、クラウドリソースとアプリケーションを最新のセキュリティパッチに適用する。

iv. セキュリティ対応タスク（脅威の検知、調査、修復など）を自動化するための自動化セキュリティオーケストレーション＆レスポンス（SOAR）プラットフォームを活用する。

c. デプロイメントと自動化技術：

i. セキュリティと、組織のインフラやアプリケーションとの互換性について厳密に吟味された、承認済みのデプロイメントおよび自動化テクノロジーの厳選されたリストを維持する。

ii. このリストを定期的に見直し、更新することで、セキュアなデプロイメント技術とベストプラクティスの最新の進歩を反映させる。

d. 既存のプロセスとの統合：

i. セキュアなアプリケーションデプロイメントの慣行を特定し、既存のアプリケーションデプロイメントプロセスとシームレスに統合することで、混乱を最小限に抑え、一貫したデプロイメントワークフローを確保する。

ii. セキュアなアプリケーションのデプロイ手順は、すでに使用されている特定のデプロイツール、方法論、および自動化フレームワークに適合させ、整合させる必要がある。

e. セキュアなアプリケーションデプロイメントのカスタマイズ：

i. セキュアなアプリケーションデプロイメント戦略は、さまざまなデプロイメント環境（異なるオペレーティングシステム、ネットワーク構成、クラウドプラットフォームなど）の固有の要件に対応するようにカスタマイズする必要がある。

ii. セキュリティ対策は、各デプロイメント環境に関連する特定の脆弱性とリスクに合わせ実施する必要がある。

f. アプリケーションデプロイメントのモニタリング：

i. セキュアなアプリケーションデプロイメントアクティビティを追跡し、異常を特定し、潜在的なセキュリティ侵害を検出するために、ログ記録と監視のメカニズムを確立する必要がある。

ii. デプロイメントプロセス中に不審な動きや不正な動きがあれば、速やかにセキュリティ担当者に警告するために、リアルタイムの監視を実施する必要がある。

g. デプロイメントパフォーマンス評価指標：

i. デプロイメント時間、エラー率、セキュリティコンプライア

	ンスレベルなど、セキュアなアプリケーションデプロイメントの成功を評価する定量的な指標を策定し、活用する。 ii. セキュアなアプリケーションデプロイメントプロセスを最適化するための改善ドメインを特定するために、指標を継続的に監視し、評価する必要がある。	

Control Title	Control ID	Control Specification
アプリケーション脆弱性の修復	**AIS-07**	アプリケーションセキュリティの脆弱性を修復するプロセスを定義して実装し、可能な場合は修復を自動化する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。CSP は、アプリケーションセキュリティの脆弱性を是正するプロセスを定義し、実装し、可能な場合は是正を自動化する責任を負う。	**管理策所有権の根拠：** 広範に存在する脆弱性は CSP と CSC の両方による対応が必要となる可能性があるが、CSC は自らのクラウド環境における脆弱性を是正する責任を負う。 SaaS モデルでは、CSC は CSC の管理範囲内にあるアプリケーションレベルの設定ミス（API 構成設定、アクセス制御設定など）に関連する脆弱性を特定する責任を負う。したがって、SaaS 利用者は、自らが利用する SaaS アプリケーション上のインフラストラクチャ及びセキュアでないコードに関連する脆弱性を特定する責任は負わないが、CSC が所有し管理するアプリケーションスタックに関連する脆弱性を特定し、理解し、管理するために、アプリケーションの脆弱性修正及び対応スケジュールを含め、CSP と調整が必要な場合もある。
実施ガイドライン： **全てのサービスモデルに適用：** アプリケーションセキュリティの脆弱性は、クラウドベースのアプリケーションにとって深刻な脅威である。これらの脆弱性は攻撃者に悪用され、アプリケーションへの不正アクセス、機密データの窃取、業務の妨害などを引き起こす可能性がある。CSP は、CSC がアプリケーションセキュリティの脆弱性を是正できるよう支援する上で重要な役割を果たすべきである。	**実施ガイドライン：** CSP に規定される実装ガイドラインは、IaaS、PaaS CSC に適用される。 さらに、SaaS CSC に関連することとして、設定ミスは、不注意によりアプリケーションをセキュリティリスクや潜在的な侵害にさらす可能性があるため、脆弱性とみなされる可能性がある。 アプリケーションのセキュリティ脆弱性を是正するための

脆弱性修復プロセスを実施するためには、以下のベストプラクティスに従う必要がある：

a. 脆弱性修正の範囲：脆弱性修正の範囲を定義するプロセスを確立する必要がある（例えば、IaaS CSP は基盤となるインフラストラクチャの脆弱性の修正のみを担当するが、PaaS CSP はプラットフォームソフトウェアの脆弱性の修正も担当する場合がある）。
b. 改善計画：各脆弱性の改善計画を策定し、その脆弱性を改善するために講じる必要のあるステップ、その脆弱性を改善するための推定時間、および必要となるリソースを含める。
    i. 計画には、開発チームや CSC と連携して脆弱性を是正し、セキュリティパッチをタイムリーに実装するためのプロセスと手順を含める必要がある。
c. 修復の優先順位を設定とリスク評価：
    i. 特定された脆弱性の重大性と潜在的な影響は、悪用可能性、対象範囲、潜在的な影響などの要因に基づいて評価される必要がある。
    ii. 脆弱性評価ツールを活用し、リスクスコアを提供する。
    iii. 脆弱性の修復は、ビジネス上の重要性、資産価値、規制遵守要件、および該当する場合は CVSS のような業界標準の脆弱性スコアリングシステムなどの要素を考慮し、リスクスコアに基づいて優先順位を決定する。
    iv. 攻撃者が積極的に悪用する脆弱性を特定するために、脅威インテリジェンスフィードを優先順位決定プロセスに組み込む必要がある。
d. 進捗の追跡と測定：改善努力の進捗を追跡し、脆弱性改善プロセスの有効性を測定する。
e. パッチ管理の自動化：脆弱性の修正に必要な時間と労力を削減し、クラウドベースのアプリケーションの全体的なセキュリティ体制を改善するために、パッチの適用を自動化する必要がある（TVM ドメインを参照）。
f. 修復の自動化：
    i. 構成管理ツールを活用して、誤ったセキュリティ設定を自動的に修正し、セキュア・バイ・デフォルトの原則を使用して、さまざまな環境でセキュアな構成を実施する。
    ii. アプリケーション内のセキュアでないコーディング慣行に対処し、セキュアなコーディングガイドラインを強制するため、自動コード・リファクタリングツールを使用する必要がある。
    iii. 自動化された依存関係管理ツールを活用して、脆弱なオープンソースコンポーネントをパッチが適用されたバージョンまたは更新されたバージョンにアップデートおよび置換える必要がある。
    iv. デプロイ前後に特定された脆弱性を自動的に修復するために、CI/CD パイプライン内に自動修復フックを実装する必要がある。
g. 修復の記録：修復プロセスを追跡し、潜在的な問題を特定するために、修復活動の包括的なロギングを確立する必要がある。
h. 修復後の検証：脆弱性が効果的に対処され、新たな脆弱性が生

SaaS CSC 実施ガイドラインには、以下が含まれる：

a. 構成管理：アプリケーションの構成設定が、組織のセキュリティ要件とベストプラクティスに合わせて適切に設定されていることを確認する。これには、アクセス制御、ユーザー権限、暗号化設定（強力な暗号化プロトコルと適切に管理された暗号化キーの使用を含む）を適切に構成することが含まれる。
b. デフォルトのセキュリティ構成：組織のセキュリティポリシーに合わせてデフォルトのセキュリティ構成をカスタマイズして強化する。このような脆弱性を修正するために、以下を実施する：
    i. 新たなセキュリティ脅威に対処するため、デフォルトのセキュリティ設定を定期的に見直し、更新する。
    ii. 定期的なセキュリティ評価を実施し、デフォルトのセキュリティ設定の弱点を特定する。
c. アクセス制御管理：堅牢なアクセス制御と認証メカニズムを実装して、SaaS アプリケーション内のユーザーアクセスと権限を規制する。これには、アプリケーション内での不正アクセスや不正行為を防止するための、ユーザーの役割、権限、本人確認の管理が含まれる。
d. 管理されていないシャドーIT 及び承認されていないアプリケーション：SaaS CSC 組織内の従業員による未承認または未管理のアプリケーションの使用は、SaaS CSP が適切に対処または監視できないセキュリティリスクや脆弱性をもたらす可能性がある。このような脆弱性を修正するために、以下を実施する：
    i. 認可されていないアプリケーションやシャドーITの使用を防ぐため、厳格なポリシーを導入する。
    ii. 承認されたアプリケーションと IT リソースについて、担当者に明確なガイドラインと推奨事項を提供する。
    iii. ネットワークトラフィックとアプリケーションの使用状況を監視し、許可されていないアプリケーションや管理されていないアプリケーションを検出する。

じていないことを確認するために、修復後の検証手順を策定する必要がある。

i. 修復の継続的なモニタリング：脆弱性修復プロセスの有効性を継続的に監視し、必要に応じて改善を行う。

j. 通知と報告：検出された脆弱性及び実施された是正措置について関係利害関係者に通知するため、通知及び報告の仕組みを確立する必要がある。

    i. 特定された脆弱性とその是正計画を CSC に伝達する。合意された SLA に従い、タイムリーかつ透明性のあるコミュニケーションを行う。

SSDLC では、脆弱性をできるだけ早く特定して修正する必要があり、自動化されたプロセスはそのようなタスクに最適である。

脆弱性のスキャンと修復の例：
アプリケーション開発プロセスにおいて、セキュアでハード化されたコンテナイメージのみが使用されるようにするには、「イメージ」スキャン専用の脆弱性スキャナを CI/CD パイプラインに統合する。これにより、セキュアな「イメージ」（ゴールデンイメージとも呼ばれる）のみがアプリケーションソフトウェアのビルドに組み込まれることが保証される。

自動スキャンツールは、このような問題を特定して修復するための効果的なソリューションである。たとえば、クラウドエージェントベースのツールをアクティブな VM インスタンスにデプロイすることで、サードパーティーのセキュリティ脆弱性を継続的にスキャンできる。スキャンの頻度は、組織のセキュリティ戦略(毎日、毎週など)によって決定される。

Control Domain BCR

2.3 事業継続管理とオペレーショナルレジリエンス (BCR)

Control Title	Control ID	Control Specification
事業継続管理ポリシーと手順	**BCR-01**	事業継続管理とオペレーショナルレジリエンスのポリシーと手順を、確立、文書化、承認、伝達、適用、評価、維持する。 少なくとも年に 1 回、ポリシーと手順をレビューし更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。各当事者は、地理的な位置、契約、および規制のエコシステムに応じて、それぞれ達成すべき、異なる事業継続管理とオペレーショナルレジリエンスの要件を持つことが期待される。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： 事業継続管理（BCM）とオペレーショナルレジリエンスに関するポリシーと手順を確立することは、CSP が中断のないクラウドサービスの提供を維持し、中断から迅速に回復し、危機を効果的に管理するために不可欠である。CSC にとって、これらのポリシーを実装する事で、不測事態やサイバー脅威に直面した場合でも、重要なサービスへの継続的なアクセスを提供できる。CSC は、中断から保護し、インシデントに迅速に対応するための堅牢な対策が講じられていることを確認することで、CSP のオペレーショナルレジリエンスへのコミットメントを信頼することができる。 CSP と CSC との連携は、強固な事業継続戦略を確保するために、不可欠である。またポリシーでは、協調的なインシデント対応と復旧作業を含み、破壊的なインシデント発生時に、CSP と CSC がどのように連携するかについての明確に理解する。 CSP は、事業継続とオペレーショナルレジリエンスの実装に必要な役割と責任を定義する。さらに具体的な責任は、クラウドサービスの種	**実施ガイドライン：** CSC は、事業継続とオペレーショナルレジリエンスの実施に必要な役割と責任を定義する。CSC は、ポリシーの適切性、目標の枠組み、リスク選好と許リスク許容度について責任を負う。 CSC は、以下の責任を負う： a. 選択したクラウドサービスモデルについて、文書化された事業継続管理およびオペレーショナルレジリエンスのポリシー、手順、方法、および標準を確立し、実施する。 b. CSP が提供するサービスを自社のインフラに統合し、自社の事業継続性およびオペレーショナルレジリエンスを確保する。 c. CSP のサービスモデルについて、実装されたコントロールの有効性と効率性を監視する。

類やサービスレベル契約の内容によって異なる場合がある。 CSP は、ポリシーの適切性、目標の枠組み、リスク選好とリスク許容度について責任を負う。	
IaaS プロバイダー： CSP は、サーバー、ストレージ、ネットワーキング、および仮想化で構成される基盤となる特定のインフラについて、文書化された事業継続管理およびオペレーショナルレジリエンスに関するポリシー、手続、手順、および標準を確立し、実装する責任を負う。 CSP は、CSC の事業継続と災害復旧を確実にする回復力のあるインフラストラクチャを提供する責任がある。	**SaaS 利用者：** CSC は、文書化された事業継続管理およびオペレーショナルレジリエンスのポリシー、手順、方法、および標準を確立し、実装する責任を負う。また CSC は、自らの事業継続性と事業環境回復力を確保するために、CSP が提供するサービスを組み込む責任もある。CSC は、CSP の IaaS インフラストラクチャに実装されたコントロールの有効性と効率性を監視し、契約と SLA の目標に適合しない場合には、サービス要求の手順に従う。
PaaS プロバイダー： CSP は、CSC が自からアプリケーションを構築できるようにする基盤となる開発プラットフォームについて、事業継続管理およびオペレーショナルレジリエンスに関するポリシー、手順、方法、および標準を確立し、実装する責任を負う。 CSP は、CSC が開発活動を継続できるようにする、回復力のある開発プラットフォームを提供する責任を負う。	**PaaS 利用者：** CSC は、文書化された事業継続管理およびオペレーショナルレジリエンスのポリシー、手順、方法、および標準を確立し、実装する責任を負う。 CSC は、CSP が提供するサービスを、CSC の手順に組み込む責任もある。CSC は、開発プラットフォームに関連する自らの事業継続性およびオペレーショナルレジリエンスをサポートする。CSC は、CSP の PaaS インフラストラクチャに実装されたコントロールの有効性と効率性を監視し、契約と SLA の目標に適合しない場合には、サービス要求の手順に従う。
SaaS プロバイダー： CSP は、CSC が自からビジネスプロセスを構築し、データをアップロードできるようにするアプリケーションと提供されるソフトウェアについて、事業継続管理およびオペレーショナルレジリエンスに関するポリシー、手順、方法、および標準を確立し、実装する責任を負う。 CSP は、災害が発生した場合でも、CSC がビジネス手順を継続できるよう、レジリエンスのあるアプリケーションとソフトウェアを提供する責任がある。	**SaaS 利用者：** CSC は、CSP のアプリケーションとソフトウェアに基づくインフラストラクチャについて文書化された事業継続管理とオペレーショナルレジリエンスのポリシー、手順、方法、標準を確立し、実装する責任を負う。 CSC は、クラウドにおけるデータコントロールに責任を負う。CSC は、実装されたコントロールの有効性と効率性を監視し、契約と SLA の目標に適合しない場合には、サービス要求手順に従う。
ポリシーには、以下に関する規定が含まれるべきである（但し、これに限定されない）： a. 範囲と目的： i. ポリシーの範囲となる、クラウドベースのシステム、アプリケーション、データおよび手順の概要。 ii. ポリシーのゴールと意図された成果（事業継続の確保、データ損失およびダウンタイムの最小化、規制要件の遵守の維持など）。 iii. ポリシーの目標と組織の全体的な戦略目標およびリスク管理フレームワーク。 b. ビジネスインパクトの中断とリスク： 重要な事業運営を中断させる可能性のある潜在的な脅威、脆弱	**ポリシーには、以下に関する規定が含まれるべきである（但し、これに限定されない）：** ポリシーは、CSP のポリシーが適用される。

性および危険を特定するために、包括的な BIA とリスク評価をする。

c. 事業継続戦略（BCS）：
組織の全体的なリスク許容度と事業継続戦略目標に整合するように事業継続戦略を策定する。

i. BIA とリスク評価で特定された潜在的な中断リスクを考慮して、重要なビジネスプロセス、資産、リソース毎にカスタマイズされた BCS を策定する。

ii. BCS は、重要な業務運営の適時かつ効果的な復旧を支援し、ダウンタイムを最小限に抑え、組織が顧客に製品やサービスを提供する能力を最大限に高めるように設計する。

iii. BCS は、詳細な復旧手順、役割と責任、コミュニケーション計画を含めて文書化する。

d. 事業継続計画（BCP）：
特定の種類のクラウド障害やシナリオに対応する BCP。

i. 文書化された BCS は、中断に対応してか復旧するための手順を段階的に説明する実用的な BCP に置き換える。

ii. BCP に概説されている各タスクに責任とタイムラインを割り当てて、全ての利害関係者が自分の役割と責任を認識できるようにする。

iii. 中断に対し調整された効果的な対応を支援するために、BCP を組織全体のインシデント対応および災害対応計画に統合する。

e. BCM と OR の文書化：
BCM 事業継続管理と OR オペレーショナルレジリエンスに関するポリシー、手続、計画を一元化して文書化し、アクセス可能な場所に配置する。

f. 事業継続訓練：
手続と計画の有効性をテストするために、BCM と OR の訓練を定期的に実施する。

g. 関連するクラウド利害関係者とのコミュニケーション：
主要な利害関係者が関与する BCM および OR 活動のためのコミュニケーションを計画する。

h. クラウドデータバックアップ：
データの損失、破損、不正アクセスから保護するクラウドデータのバックアップ戦略を立てる。

i. 災害対応計画：
大規模な災害発生時に取るべき行動の概説となる詳細な災害対応計画要件を策定する。

j. 災害対応計画の演習：
災害対応計画の有効性をテストするため、定期的に災害対応計画の演習を実施する。

k. 機器の冗長性：
地理的に分散したクラウドデータセンターを利用し、冗長化されたクラウドベースのインフラストラクチャコンポーネントを実装し、高可用性とオペレーショナルレジリエンスを確保する要件を定める。

l. 承認：

組織の戦略目標およびリスク選好との整合性を確保するための承認要件および上級管理職の関与を確立する。 i. BCM と OR ポリシーと手順の変更又は修正について、承認手順を確立する。 ii. 承認に関する文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持する。 m. コミュニケーション： ポリシーと手順の効果的なコミュニケーションは、関連する全てのクラウド利害関係者に対して促進する。 n. 維持とレビュー： 事業継続管理およびオペレーショナルレジリエンスに関するポリシーと手順は、進化するクラウドセキュリティの状況との整合性を確保し、クラウド技術、規制およびリスクの変化を反映するために、少なくとも年 1 回文書化し、レビューし、更新する。	

Control Title	Control ID	Control Specification
リスク評価と影響分析	**BCR-02**	ビジネスの中断の影響とリスクを判断し、事業継続、オペレーショナルレジリエンスの戦略、機能の標準を決定する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC が互いにこの管理策の実施責任を負うが、各当事者はインフラストラクチャとサービスの中断による影響を独自に評価する。具体的には、各当事者が独自のビジネスインパクト分析（BIA）を実施し、復旧目標時間（RTO）や復旧目標ポイント（RPO）などのパラメータを定義し、独立したリスク評価を実施すべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、CSP のサービスの事業継続性およびオペレーショナルレジリエンス戦略を確保する責任を負う。 ビジネスインパクト分析（BIA）とリスク評価の手順を実装すること	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

で、CSP は潜在的な障害とリスクを効果的に特定し、評価し、および軽減することができ、有害事象に直面しても CSC が事業運営を維持できるようになる。

CSP は、自社のビジネスインパクト分析（BIA）およびリスク評価の手順において、以下のベストプラクティスを実施する：

a. 情報ガバナンスの組込み：情報ガバナンスの組込み：BIA およびリスク評価の活動は、情報ガバナンスプログラム（GRC-01 を参照）に統合し、組織目標およびリスク許容度との整合性を確保する。
b. BIA(Business Impact Analysis)およびリスクアセスメントチーム：包括的な視点を確保するため、IT 部門、運用部門、ビジネスユニット、およびリスクマネジメントの代表者からなる部門横断的なチームを編成する。
c. BIA およびリスクアセスメント：BIA およびリスク評価を実施するための標準化された方法論を文書化し、一貫性および再現性を確保するために、体系的なリスク評価手順またはリスクベースのアプローチを企業リスク管理プログラム（ERM）（GRC-02）から実施し、維持する。
    i. 重要なビジネスプロセス、データ、システムに対する障害の潜在的影響を分析する。
    ii. リスクは、その可能性と潜在的な影響に基づいて優先順位を付け、クラウドベースのサービスのリスク許容レベルを設定する。

ビジネスインパクト分析（BIA）は、以下を含める（但し、これらに限定されない）：

d. 影響区分および標準の定義：組織固有のビジネス状況に合致する影響カテゴリと基準を決定する。これらのカテゴリは、組織の優先事項、障害に対する許容度、および障害の潜在的な影響を反映する。
e. 影響の測定：中断が重要なビジネス活動に及ぼす潜在的な影響を体系的に測定するために、確立された影響カテゴリと基準を測定する。これには、定義された基準に基づいて影響レベルを割り当てることが含まれる。
f. 重要な活動の特定：組織が製品やサービスを提供するために不可欠な活動をマッピングする。
g. 時間経過に伴う影響分析：中断が重要な活動に及ぼす影響は、時間の経過とともに変化し、中断が長期化した場合の累積的影響を考慮する。
h. 許容可能な復旧時間枠：中断が重要な活動に及ぼす影響が組織にとって許容できなくなる期間を定義する。これらの時間枠は、復旧戦略の優先順位を決定するためのベンチマークとして機能する。
i. 復旧活動の優先付け：：許容可能な影響期間を、特定の重要な活動に対する優先付けされた期間に細分化して、資源の配分と復旧作業の指針とする。
j. リソースの特定と依存関係のマッピング：
    i. 優先付けされた重要活動を支援および復旧するため

に、必要な資源を決定する。これには、物理的資源と人的資源の両方を特定することが含まれる。

ii. 優先付けされた重要な活動を支援える資源間の依存関係や相互依存関係を特定し、マッピングし、中断の連鎖的な影響を理解する。

k. インフラ資源のリストアップ：

i. クラウドサービスを提供するために必要な全てのインフラリソース（コンピューティング、ネットワークデバイス、ストレージ、ソフトウェアコンポーネントなど）の包括的なリストを作成する。

ii. インフラリソースの依存関係を特定するインフラリソース間の依存関係を特定し、文書化する。これにより、個々のリソースの中断がクラウドインフラストラクチャ全体に及ぼす潜在的な影響を理解するのに役立つ。

BIA リスク評価には、以下を含める。(但し、これらに限定されない)：

l. 優先活動の中断リスク：
優先される重要な活動の潜在的な中断リスクは、体系的に特定し、文書化する。これらのリスクは、組織の製品またはサービスの提供能力を妨げる可能性のある内部要因または外部要因がある。

m. 支援リソースの中断リスク：
優先される重要な活動を支援するクラウドの物理的資源と人的資源が中断する潜在的なリスクも特定し、文書化する。

n. 中断のリスク分析：
特定された中断リスクの体系的な分析は、各リスクの可能性と影響を評価し、その全体的な重大性を判断することにより実施する。

o. 対処が必要な中断リスク：
対処または緩和戦略を必要とする特定された中断リスクは、優先順位を付けて評価する。これには、対処を実施することによる潜在的な便益とコストを評価することが含まれる。

p. 自動化手順：
自動化ツールを活用して、データ収集、分析、報告を合理化し、効率性と有効性を向上させる。

q. BIA およびリスク評価のレビュー：
継続的な関連性と有効性を確保するため、BIA およびリスク評価の結果を定期的に見直す。

Control Title	Control ID	Control Specification
事業継続の戦略	**BCR-03**	リスク選好の範囲内で、ビジネスが中断する影響を軽減し、持ちこたえ、復旧するための戦略を確立する。
Control Ownership by Service Model		

IaaS	PaaS	SaaS
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、BIA およびリスクアセスメントのアウトプットに基づき、事業継続戦略を特定し、選択する。事業継続戦略は、1 つ以上のソリューションで構成する。 CSP は、サービス契約（SLO：Service Level Objective を含む）に従い、レジリエンスなクラウドインフラストラクチャおよびサービスを CSC に提供する責任を有し、CSC は、CSP が提供する情報を含む CSC の戦略の一部について、CSP が提供する特定のサービスおよびレジリエンス機能に依存する可能性がある。但し、CSP は、CSC の BC 戦略を策定、計画、文書化、採用、またはその他の形で確立する責任を負わない。	**管理策所有権の根拠：** CSC は、ビジネスインパクト分析およびリスクアセスメントの結果に基づき、事業継続戦略を特定し、選択する。事業継続戦略は、1 つまたは複数のソリューションで構成する。 CSC が採用する BC 戦略は、CSP が提供する特定のサービスやレジリエンス能力に依存する可能性があるが、CSC の戦略の策定、採用、またはその他の方法による確立において、CSP の関与に依存することはない。 事業継続戦略に基づいて RTO と RPO を達成するために、CSC はマルチクラウド戦略（事業目的を達成するための異なる製品とサービス）を選択することができる。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、事業継続の目標と、CSP が取り負う可能性のあるリスクの量と種類を考慮して、戦略とソリューションを特定し、選択する必要がある。 事業継続およびオペレーショナルレジリエンス戦略には、以下を含める（但し、これらに限定されない）： a. リスクベースの事業継続とオペレーショナルレジリエンス戦略 i. 潜在的な障害を特定し、その影響を評価し、許容可能なリスク許容レベルを決定するために、徹底したリスク評価を実施する。 ii. 障害を防止、緩和、対応、回復するための具体的な行動を概説する詳細な事業継続計画（BCP）を策定する（BCR-04 を参照）。 b. 障害の予測 i. インフラ、アプリケーション、データ、要員を含む全ての関連コンポーネントが利用できなくなる可能性を予測し、対処する。 ii. 冗長性とフェイルオーバーの仕組みを導入して、ダウンタイムを最小限に抑え、継続的なサービス提供を保証する。 iii. マルチクラウド戦略を活用して、複数のクラウドプロバイダーにワークロードを分散させ、単一インフラス	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、適切な事業継続戦略と解決策を特定し、その関連コストを考慮して選択する。 a. 障害対応コストの最適化： ダウンタイムとそれに伴う収益損失を最小化するため、障害の迅速な特定、封じ込め、回復を優先した、費用対効果の高い障害対応計画を実施する。 b. コスト効率の高いリソース提供： 最小限のコストで継続的にサービスを提供するために、スケーラブルなリソースの調達・準備と、優先順位の高い活動に対するコストの最適化を可能にするクラウドベースのインフラストラクチャを採用する。 優先順位を設定された活動について、CSC は、事業継続の目的、及 CSC が取り得るリスクの量と種類を考慮し、戦略および解決策を特定し、以下を含む選択をする。(但し、これに限定されない)： c. 障害の可能性の低減： 障害が発生する前に、潜在的な問題を特定し、対処するために、事前予防的なモニタリングおよび警告システムを導入する。 d. 障害期間の短縮： マルチクラウド戦略を活用し、ワークロードを複数のクラウドプロバイダーに分散させ、単一のインフラへの依存度

トラクチャへの依存度を下げる。

iv. 重要なデータを保護し、障害からの迅速な復旧を可能にするため、データレプリケーションとディザスタリカバリ（DR）ソリューションを採用する。

c. 回復期間

i. 中断中に維持しなければならない重要な事業活動を特定し、優先順位をつける。

ii. 優先順位を設定しされた各活動の復旧目標時間（RTO）および復旧目標ポイント（RPO）を定義する。

iii. iii. 各優先活動の詳細な復旧手順（タイムライン、リソースの割り当て、通信プロトコルを含む）が策定する。

iv. ビジネス上の優先順位とリスク評価の変更を反映する RTO と RPO は、定期的に見直し、更新する。

d. キャパシティプランニングとモニタリング

i. クラウドリソースが需要を満たすことができるよう、キャパシティプランニングを行う（IVS-02 を参照）。

ii. 事業継続性とオペレーショナルレジリエンス戦略を実施および維持するために、人員、インフラ、財政的支援を含む十分なリソースを割り当てる。

iii. 高可用性、拡張性、障害レジリエンスを提供するクラウドベースのソリューションを優先的に採用する。

iv. クラウド関連の潜在的な障害を迅速に特定して対応するために、プロアクティブな監視および警告システムを導入する。

e. 解決策と対策の文書化

i. 各事業継続およびオペレーショナルレジリエンス戦略は、具体的な解決策、対策および責任を含め、詳細に文書化する。

ii. 全ての関係者（例えば、要員、パートナー、CSC）は、文書化された戦略を認識し、理解しなければならない。

iii. 戦略、技術、ビジネス要件の変更を反映するため、文書化を定期的に見直し、更新する。

f. CSP と CSC の協働による戦略の策定。

i. 事業継続およびオペレーショナルレジリエンス戦略は、リスク選好とリスク許容度を考慮して、CSP および CSC の双方により策定する。

ii. インフラストラクチャの両当事者の役割と責任を明確にし、整合性と説明責任を確保する。

iii. 事業運営、リスク評価、およびクラウドインフラストラクチャの変化を反映するために、戦略を見直し、更新する。

を下げる。

e. 中断の影響の制限：
ロードバランシングとオートスケーリングを導入してトラフィックを分散し、障害時の過負荷を防ぐ。

f. 戦略の選択、ビジネス要件と標準：
障害に対する許容リスクレベルを定義し、重要なビジネス機能に対する復旧目標時間(RTO)と復旧目標ポイント(RPO)を設定する。

g. CSP の提供サービスと CSC のビジネス要件との整合性：
CSP が提供するサービスについて、機能、価格、サポートなどを含めて徹底的に評価し、ビジネス要件を明確に定義して、CSP に伝えるべきである。

CSC は、事業継続およびレジリエンスサービスを選択する選択肢を持つべきである：管理された事業継続およびレジリエンスサービスを利用する。CSP から支援を受ける。(CSC が）自ら行う（セルフサービス）。

事業継続およびオペレーショナルレジリエンス戦略には、次を含める（但し、これらに限定されない）：CSP が提供する戦略。

Control Title	Control ID	Control Specification

事業継続計画	**BCR-04**	オペレーショナルレジリエンス戦略と機能の結果に基づいて、事業継続計画を確立、文書化、承認、伝達、適用、評価、維持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、すべてのクラウドサービスモデルと、CSP と CSC の両者で共有される。CSP と CSC は、それぞれのビジネスニーズ、契約および規制要件を満たすために、それぞれ独自にビジネス継続計画を策定し、実装する必要がある。	**管理策所有権の根拠：** CSC は、自ら BCP を策定し、実施し、CSP の BCP をレビューすべきである。CSC が所有する管理策は、CSP が提供するクラウドサービスに関連する組織単位内のリソースおよび資産に関するものである。 BCP を策定する際、CSC は、CSP が提供するクラウドサービスに対応する事業継続の手順および技術を考慮すべきである。
実施ガイドライン： **IaaS プロバイダー：** CSP は、物理インフラストラクチャ(データベース、ホスト、およびネットワークを含む)の BCP を確立、文書化、実践、実施、レビュー、および維持する責任を負う。	**実施ガイドライン：** **IaaS 利用者：** CSC は、管理プレーン、仮想ホスト、仮想ネットワーク、アプリケーション、および CSC がクラウドインフラストラクチャ上にデプロイした関連リソースを含む BCP を確立し、文書化し、実施し、実施し、レビューし、維持する責任を負う。
PaaS プロバイダー： CSP は、プラットフォームの基盤となるリソース、ミドルウェア、および API を含む BCP の策定、文書化、実践、実施、レビューおよび維持に責任を負う。	**PaaS 利用者：** CSC は、CSC がプラットフォーム上にデプロイするアプリケーション、サービス、クラウドサービスにアクセスする際のプラットフォーム、データおよびその他のリソースを含む、BCP の策定、文書化、実践、実施、レビューおよび維持に責任を負う。
SaaS プロバイダー： CSP は、基盤となるプラットフォームリソース、仮想マシン、ネットワークリソース、およびクラウドサービスに関連する管理プレーンまたは管理インタフェースに対する BCP の策定、文書化、実践、実施、レビュー、および維持に責任を負う。	**SaaS 利用者：** CSC は、CSC 要員がクラウドサービスおよびアプリケーションデータにアクセスするために使用する PC およびその他のデバイスに関する、BCP の策定、文書化、実践、実施、レビュー、および維持に責任を負う。
全てのサービスモデルに適用： 事業継続計画（BCP）は、CSP にとって、運用上のオペレーショナルレジリエンス戦略および能力の重要な要素である。CSP は、自社のクラウドサービスがレジリエンスを持ち、障害に耐えられるように、BCP を導入すべきである。	**全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

BCP は、チームが障害に対応し、対応と復旧を支援するためのガイダンスと情報を提供すべきである。

BCP 策定に向けた実施上のベストプラクティスには、次のようなものがある（但し、これらに限定されない）：

a. BCM チームの設置：BCP の開発と実施を確立する BCM チームを設置する。BCM チームは、重要なビジネスプロセスを特定し、リスク評価を実施し、緩和計画の策定と、BCP テストの維持に責任を負う。
b. BCP の範囲：BCP の目的、範囲、境界を決定し、文書化する（システム、技術、サービス、手順、場所の制限と除外、シナリオ／不測事態の種類、対応するインシデントの規模を含む）。
    i. クラウドサービスの提供に不可欠な重要ビジネスプロセスとリソースを特定する（異なるクラウドプロセスとリソース間の依存関係を含む）。
    ii. 重要プロセスで許容されるダウンタイムに関する復旧目標時間（RTO）と、データ損失に関わる目標復旧時点（RPO）を定義する。
    iii. 重要プロセスについて、RTO 内で通常業務を復旧させるためのステップを概説する詳細な復旧戦略を定義する。
    iv. データ損失を防ぎ、タイムリーな復旧を可能にする堅牢なデータバックアップおよび復旧ソリューションを計画する。
    v. サービスの可用性を確保するために、複数のデータセンターやフェイルオーバー機能など、クラウドインフラ固有の冗長性を活用する。
    vi. CSP は、BCP の範囲を文書化し、CSC に伝える。
c. BCP の開発：BCP は、明確かつ簡潔な方法で策定し、文書化すべきである。文書化には、以下の情報を含める：
    i. 重要なビジネスプロセスの説明
    ii. リスクアセスメントと緩和計画
    iii. シームレスな実施および順守を確保するための、既存の手順および手続を BCP へ統合
    iv. BCM チームメンバーの役割と責任
    v. 障害に対応するための手順と手順
    vi. チームが所定の時間枠内で復旧手順を実施し、障害による影響を監視して対応する行動の詳細
    vii. 対応策を開始するための事前定義された閾値と、プロセスへの参照
    viii. 障害時に即時影響を管理するための詳細：
        - 優先活動のさらなる損失や利用不能の防止
        - 環境の保護
        - インシデント終了後の停止手順
    ix. 関連するテストとメンテナンス計画
d. BCP の文書化：BCP は、文書化され、全ての BC 関連文書とともに一元化されたセキュアな保管場所に保存する。

e. BCP の承認：計画が、実施に必要な権限とリソーを備えていることを確保するため、上級管理職の正式な承認を得る必要がある。 f. BCP コミュニケーション： i. BCP は、CSC、人員、および規制当局（必要な場合）を含む関連する全ての主要な利害関係者に伝達され、障害と復旧の進捗状況が通知される必要がある。 ii. 障害時にタイムリーで正確な情報共有を確実にするため、CSC との間で、コミュニケーションチャネルとプロトコル、メッセージ形式、エスカレーション手順を確立する。 g. BCP の実施とテスト： i. 定期的にシミュレーションと演習を実施して、BCP の有効性をテストし、改善点を特定する。 ii. テストには、シミュレーション、机上訓練、実規模訓練などを含める。 iii. 過去の事故から、学んだ教訓を計画に取り入れる。 h. インシデント発生後の BCP 有効性評価： i. インシデント後に、インシデント対応メトリックの継続的な監視に基づいて、インシデント後の徹底的なレビューを実施して、計画の有効性を評価し、改善すべき領域を特定し、それに応じて手順を更新する必要がある。 ii. 各障害インシデントから学んだ教訓は、文書化され、将来の備えを強化するために、その洞察を事業継続計画に組み込む。 i. BCP レビュー： i. BCP が現在の脅威、リスク、業界のベストプラクティスと合致し、事業目標やクラウド技術、インフラ、および事業運営の変化に適合していることを検証するため、少なくとも年 1 回レビューと更新を実施する。	

Control Title	Control ID	Control Specification
文書化	**BCR-05**	事業継続とオペレーショナルレジリエンスプログラムのサポートに関連する文書を作成し、特定し、取得する。承認された関係者が文書を利用できるようにし、定期的にレビューを行う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の所有権と実施責任は、CSP と CSC で独立して共有される。CSP は、サービス契約に従って、レジリエンスのあるクラウドインフラストラクチャとサービスを CSC に提供する責任を負う。従って CSC は、CSP が提供するサービスおよびレジリエンス機能に依存する可能性がある。文書化については、CSP は、自らのシステムおよびサービスの事業継続性とレジリエンスに関連する文書の作成、特定、および取得についてのみ責任を負い、CSC のそれについては責任を負わない。 CSP は、関連文書および情報を CSC と共有する。	**管理策所有権の根拠：** CSC は、自らの事業継続およびオペレーショナルレジリエンスプログラムを支援するための文書を作成し、特定し、策定する責任を負う。 文書は、CSC の事業運営に固有のものである。 この文書は、CSC の事業運営に固有のものである。CSC は、CSP から入手した情報や文書を自社の文章に含める場合もあるが、計画、戦略、ポリシー、アプローチなど、CSC の事業継続およびオペレーショナルレジリエンスプログラムの側面を文書化するのは、完全に CSC の責任である。 CSC は、CSP から提供された関連文書を特定する責任を負う。
実施ガイドライン **全てのサービスモデルに適用：** 事業継続とオペレーショナルレジリエンスプログラムを文書化することで、CSP は障害に対する準備、対応、回復を効果的に行うことが可能となる。 これより、準備体制が強化され、インシデント管理が効率化し、意思決定が改善され、規制遵守がサポートされ、知識が保持され、継続的な改善が促進され、利用者の信頼が高まる。 CSP は、BC および OR の関連文書を CSC に提供する責任を負う。 事業継続およびオペレーショナルレジリエンスプログラムを支援するための文書作成の追加ガイドラインには、以下が含まれる（但し、これらに限定されない）： a. 文書ガバナンス： i. 文書の作成、レビュー、承認に関する役割と責任を明確にする。 ii. 文書を特定し、作成し、維持するための構造化された手順を実施する。 b. 文書化の範囲と開発： i. 全てのビジネス継続性 (BC) およびオペレーショナルレジリエンス (OR) ドキュメントを保存および管理するためのクラウドベースのレジストリを作成し、承認された関係者が簡単にアクセスして検索できるようにする必要がある（それぞれの場所へのリンクを含む）。 ii. BCM と OR の訓練と訓練の記録を維持する。 iii. 一貫性を維持し、使いやすさを向上させるために、BC および OR の手順および計画の文書化のための標準化されたテンプレートおよびスタイルガイドを作成する。 iv. 変更を追跡し、履歴を管理し、必要に応じてロールバックを容易にするバージョン管理システムを導入する。 v. BC および OR 文書の作成と保守を合理化するために、自動化ツールを活用し、手作業を減らし、一貫性を高め、	**実施ガイドライン** **全てのサービスモデルに適用：** CSC は、自らのクラウドデプロイ環境を正確に反映した文書を作成し、維持することに責任を持つ必要がある。 この文書には、特定の実践に合わせた関連情報、手順、およびガイドラインを含める必要がある。 CSC は、クラウドサービスについてタイムリーかつ包括的な洞察を得るために、CSP から関連文書を積極的に入手し、正式に受け入れる必要がある。 CSC は、システム管理者、バックアップ管理者、エンドユーザー、消費者、顧客を含む利害関係者が、文書に容易にアクセスできるようにする第一の責任を負う必要がある。 CSC が定期的なレビュー手順を監督する一方で、文書の内容は、当然ながら CSP が提供するサービスや機能に沿ったものとする。 事業継続およびオペレーショナルレジリエンスプログラムを支援する文書作成の追加ガイドラインには、次を含める（但し、これらに限定されない）：CSP に適用される「実施ガイドライン」。

反復作業を自動化する。

c. 文書の特定と取得
   i. 既存の文書を徹底的にレビューして、BC および OR プログラムを支援する関連資料を特定する（内部文書、外部リソース、業界のベストプラクティスなど）。
   ii. 関連文書は、クラウドサービスプロバイダー、データセンター事業者、ネットワークサービスプロバイダーなどのサードパーティプロバイダーから収集する。
   iii. 業界標準、規制要件などの外部文書を特定し、取得する。
d. 承認された利害関係者のみがレジストリと、その機密文書にアクセスできるよう、「need-to-know の原則」に基づくアクセス管理を実施する。
e. クラウドベースの共同作業ツール：クラウドベースの共同作業ツールを用いて、BC および OR 文書の共有とレビューを容易にする。
f. CSC との文書共有：
   i. CSP の BC および OR 文書にアクセスすることで、CSC は障害に備え、より良い準備と対応が可能になる。CSP の計画と手順を理解することで、CSC は自らの BC および OR 計画が整合している事、適用範囲にギャップがない事を保証できる。
   ii. CSP と CSC の両方が同じプレイブックから作業していることを保証することで、ダウンタイムのリスクを低減し、障害発生時の混乱や貴重な時間の損失を回避する。
   iii. 規制当局は、CSP に対し、BC および OR に関する文書と要件を CSC と共有するよう求めることがある。この文書を共有することで、CSP と CSC の双方がこれらの要件に準拠していることが確認できる。
g. 文書のレビューと更新：
   i. BC および OR 文書の定期的なレビュー手順を実装する。この手順により、文書が正確で最新であり、クラウド環境の変化、現在のビジネス要件およびリスクの変化に合わせて調整されていることを確認する。
   ii. 文書の更新は、文書がビジネス慣行と一貫性を保つことを保証するために、変更管理手順の一部として実施する。
   iii. 文書の変更、レビュー活動、承認決定は、コンプライアンス目的の監査証跡を維持するために追跡する。

Control Title	Control ID	Control Specification
事業継続の演習	**BCR-06**	少なくとも年 1 回、または、大幅な変更があった場合に、事業継続とオペレーショナルレジリエンスの計画を演習およびテストを行う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、CSP と CSC で独立して共有される。この管理策の CSP の所有権は、CSC に提供される CSP 管理リソースの BCP の演習とテストに関わる。 両者がエンドツーエンドの事業継続計画およびオペレーショナルレジリエンス計画のテストに関与している場合は、本格的な演習またはテストを実施することが推奨される。そうでない場合は、CSP 自ら、CSC にテストの証拠を提供すべきである。 本管理策における CSC の所有権は、CSC のクラウド組織単位、インフラ、および資産内の CSC が管理するリソースに対する事業継続計画の実施とテストに関連する。 CSP は以下の責任を負う： • 物理インフラ（データベース、ホスト、ネットワークを含む）に対する BCP の演習とテストを確立、文書化、実施、およびレビューし、定期的に実施する。 • 演習およびテスト中の重要なシステムおよび機器の特定と優先順位を設定する。 • テーブルトップ演習（机上演習）への CSC の参加を伝達および要請をする。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 演習とテストは、事業継続手順が事業継続目標を確実にサポートすることを支援する。 演習とは、BCP または関連する手順の 1 つまたは複数の側面を検証するために設計された、人とプロセスが関与する作業または活動である。演習には、目的と目標に応じて様々な種類がある。その演習には、BCP 要素のシナリオに基づくシミュレーションが含まれる。例えば、シミュレートされた環境（すなわち、ファンクショナル）での職務遂行や、ディスカッションに基づくもの（すなわち、机上演習）が含まれる。 事業継続計画およびオペレーショナルレジリエンス計画を演習し、テストするために、CSP は以下を確立すべきである：	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

a. 演習とテストのフレームワーク：
   i. 演習およびテストプログラムの目標は、全体的な事業継続およびオペレーショナルレジリエンスの戦略および計画と整合するように定義する。
   ii. 障害時に維持する必須手順を、依存関係およびカスタマサービスへの潜在的影響を考慮して決定する。
   iii. 継続的な備えを支援するため、定期的なテスト計画を年単位または重要な変更時に確立する。
   iv. クラウドの停止、データ損失、サイバー攻撃など、様々な潜在的な障害に対応する、現実的で困難なシナリオを設計する。
   v. 役割、責任、通信プロトコルなど、演習とテストの手順を概説した文書を策定する。
b. コミュニケーションと協調：
   i. 演習およびテスト中のタイムリーで正確な情報共有を促進するために、明確に定義されたコミュニケーションチャネルを確立する。
   ii. 演習およびテスト活動に関与する全ての利害関係者の役割と責任を明確にし、説明責任と協調を確保する。
   iii. 問題を迅速に特定し対処するために、演習およびテスト手順を通じて、オープンで透明性のあるコミュニケーションを奨励する。
   iv. 演習およびテスト期間中、リアルタイムのコミュニケーション、情報共有および意思決定を促進するため、協調ツールとプラットフォームを使用する。
c. シミュレーション（外部再現）とエミュレーション（内部再現）技術：
   i. シミュレーションとエミュレーション技術は、現実世界の障害を再現する現実的で没入感のあるシナリオを作成する。
   ii. 様々な破壊的シナリオのもとで、クラウドインフラ、アプリケーション、データのレジリエンスをテストするために、シミュレーションとエミュレーションのツールを使用する。
   iii. 障害発生後に重要なデータやシステムを復元する能力を確保するため、バックアップと復旧手順をテストする。
   iv. シミュレーションとエミュレーション中の、システムとプロセスのパフォーマンスを分析し、改善点を特定して回レジリエンスを強化する。
   v. 事業継続計画およびオペレーショナルレジリエンスの有効性を評価するために、様々な演習を採用することが可能となる（例：机上演習、ウォークスルー演習、シミュレーション、並行および実大規模演習）。
d. 継続的改善：
   i. 各演習およびテストの結果は、特定された問題、学んだ教訓、取られた改善措置を含め、文書化する。
   ii. 複数の演習および試験を通じて特定された傾向およ

びパターンを分析し、繰り返し発生する脆弱性および改善のためのドメインに関する洞察を得る。 iii. 組織全体のレジリエンスを高めるために、演習やテストから得られた教訓を関連する利害関係者と共有する。 e. レビューと更新： 事業継続計画およびオペレーショナルレジリエンスプログラムのレビューと更新を行う。 CSP は、復旧テストを、少なくとも年 1 回または運用環境とアプリケーションやビジネス機能の重要性に応じて、それ以上の頻度で実施すべきである。	

Control Title	Control ID	Control Specification
コミュニケーション	**BCR-07**	事業継続とレジリエンスの手順において、関係者や参加者とのコミュニケーション手段を確立する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、CSP と CSC で独立して共有される。CSP は、事業継続およびレジリエンス手順の過程、および CSP 自身の事業継続計画とプログラムの全ての要素において、自らの利害関係者および参加者とのコミュニケーションを確立する責任を負う。この管理策は、CSP の組織単位と利用者の利害関係者である CSC を含み、その他の利害関係者のためのコミュニケーション計画の策定と確立に関係する。CSP は、CSC の利害関係者および参加者に直接コミュニケーションする責任はない。	**管理策所有権の根拠**： CSC の管理策所有権の根拠は、CSC の組織単位およびその他の利害関係者に対するコミュニケーション計画の策定と確立に関するものである。
実施ガイドライン **全てのサービスモデルに適用：** CSP は、社内および CSC やその他の利害関係者とのコミュニケーション計画の確立し、文書化し、実施し、レビューし、維持に責任を負う。	**実施ガイドライン** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

CSP は、全てのサービスデリバリモデルについて、社内のコミュニケーションチャネルを確立する責任を負う。
CSP は、コミュニケーション計画および戦略を CSC と交換することで、障害時や BCP/DR の演習時に、適切なチャネルと適切な担当者に、タイムリーに伝達できるようになる。

実施上のベストプラクティスには、以下が含まれる（但し、これらに限定されるものではない）：

a. コミュニケーション計画：
   i. コミュニケーション計画およびマトリクスを作成、維持する。このマトリクスには、関連する全ての利害関係者（例えば、CSC、パートナー、担当者、および規制機関）のリスト、連絡先の詳細、および望ましいコミュニケーションチャネルを含む。
   ii. 事業継続イベント中のコミュニケーションを担当するチームの役割と責任を定義する。
   iii. 様々な障害シナリオ（例えば、事業継続対応の発動、運営、調整、およびコミュニケーションに関するもの）に対して、予め準備されたコミュニケーションテンプレートおよびプレイブックを作成する。
   iv. 事業継続に関連するコミュニケーションを、いつ、どのように発信すべきか、誰が発信すべきか、誰に発信すべきかを示す標準、閾値、指標を含む。
   v. 事業継続コミュニケーションに必要な技術および手順を含む。
   vi. 関連する利害関係者へのタイムリーな警告および伝達を可能にするために確立された対応体制の確立を含む。
   vii. 計画は、関連する利害関係者に伝達する：
      - 効果的な事業継続の重要性と中断の結果
      - 事業継続とレジリエンスのポリシー、目的、およびこの計画
      - 全ての関連する利害関係者に対する役割、責任、権限、および予期される能力
b. コミュニケーション目標：停止に関する CSC への通知、新機能に関するパートナーへの最新情報の提供、レジリエンス対策に関する人員への懸念対応など、利害関係者グループごとに具体的なコミュニケーション目標を定める。
c. コミュニケーションメッセージ：コミュニケーションメッセージは、各利害関係者グループの具体的なニーズと関心に合わせて調整する。分かりやすい言葉を使い、専門用語を避け、実用的な情報を提供する。
d. 定期的なコミュニケーション：毎日または毎週のステータス更新、潜在的な中断や停止時の積極的なコミュニケーションなど、定期的なプロアクティブ・コミュニケーションを確立する。
e. マルチチャンネル・コミュニケーション：
   i. 冗長性を確保するため、複数のコミュニケーションチャネルを利用する。これには、電子メール、SMS、音声

通話、インスタントメッセージ、クラウドコラボレーションプラットフォームなどを含む。 ii. 中断中の可用性を確保するため、どこからでもアクセスできるクラウドベースのコミュニケーションツールを活用する。 f. 通信システムの冗長性： i. 重要な通信システムは、複数の地域に分散させ、地域的な障害による影響を軽減する。 ii. 一つのプロバイダーに問題が発生しても、継続的な通信を確保するため、複数の ISP を通じてインターネット接続の冗長化を実施する。 g. コミュニケーション演習：定期的にコミュニケーション演習を実施し、模擬的な危機または障害シナリオにおけるコミュニケーション計画および手順の有効性をテストする。 h. BCP とコミュニケーションとの統合：障害時のシームレスな連携と対応を確保するため、コミュニケーション計画と手順を事業継続計画およびオペレーショナルレジリエンスの全体に統合する。 i. フィードバックの収集： i. 利害関係者からのフィードバックを継続的に収集し、コミュニケーション活動の効果を評価し、改善点を特定する。 ii. 得られた教訓を基に、コミュニケーション計画やシステムを更新し、強化する。 j. 規制の準拠：クラウドサービス業界に適用される関連する規制要件や標準に、コミュニケーション手法が準拠していることを確認する。 k. レビューと更新：コミュニケーション計画と手順は、利害関係者のニーズ、テクノロジー、事業戦略の変化を反映するために、定期的にレビューし、更新すべきである。	

Control Title	Control ID	Control Specification
バックアップ	**BCR-08**	クラウドに保存したデータを定期的にバックアップする。バックアップの機密性、完全性、可用性を確保し、レジリエンスのためにバックアップからのデータ復元を検証する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines

CSP	CSC
管理策所有権の根拠： この管理策の実施は、CSP と CSC で責任共有である。また、CSP が CSC にバックアップ機能を提供し、CSC が独自のセキュリティポリシーとビジネス要件に従って適切に構成できるようにする責任があるため、「依存関係」になる。より具体的には、CSP はバックアップおよび復元サービスを提供し、これらのサービスをサポートするインフラストラクチャを担当する。一方で CSC は、これらのサービスを正しく活用してデータを保護する（バックアップするデータの選択、暗号化の有効化、データ復元機能の検証など）責任を負う。	**管理策所有権の根拠：** CSC は、クラウドに保存された全てのデータ（構成設定、カスタムコードなどのメタデータを含む）に責任を負う。 したがって、全ての構成は、CSC が設計し、実装し、検証し、およびその後の変更を管理する必要がある。
実施ガイドライン： **全てのサービスモデルに適用：** クラウドに保存されたデータの機密性、完全性、および可用性を確保するため、CSP は、データセキュリティ、バックアップ、およびリストア手順を含む包括的な技術的手段を実践すべきである。 CSC のために、クラウドに保存されたデータを定期的にバックアップする実装のベストプラクティスには、以下が含まれる（但し、これらに限定されない）： a. バックアップ戦略：定期的なバックアップスケジュール、増分バックアップ、およびバックアップファイルの物理的な場所を含むフルバックアップを含むバックアップ戦略を確立する。 i. クラウドベースのバックアップサービス、オンプレミスストレージ、オフラインバックアップを含む複数のバックアップ方法を利用する。 ii. 3-2-1 バックアップ方法を使用：2 つの異なるメディアにデータの 3 つのコピーを作成し、1 つのコピーをオフサイトに保管する。 b. 別の場所でのバックアップ：バックアップは、プライマリクラウドデータストレージとは物理的または論理的に隔離された別の場所に保存する。 c. バックアップの暗号化：バックアップデータは、不正アクセスを防止するため、強力な暗号化アルゴリズムとセキュアな鍵管理を用いて暗号化する。 d. バックアップの完全性の検証：バックアップの完全性は、暗号ハッシュ、チェックサム、メッセージ認証コード（MAC）などのデータ完全性検証メカニズムを使用して定期的に検証し、破損や改ざんがないことを確認する。 e. バックアップリポジトリのアクセス管理策：バックアップリポジトリへのアクセス管理策は、不正アクセスを防止するために実施されるべきであり、アクセス許可は定期的に見直し、更新する。 f. バックアップの保持とアーカイブ： i. データ保持ポリシーは、クラウドデータバックアップの範囲、頻度、および期間を決定するために、適用される法律／規制、契約上の合意（SLA）、および CSP の	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

ビジネス要件に従って策定する。

ii. データの長期保存と規制要件の順守を確実にするために、データアーカイブ戦略を実施する。

iii. 保持ポリシーに従って、古いバックアップを自動的に消去する。

g. バックアップの監視と監査：バックアップが正常に実行され、データの完全性が維持されていることを確認するため、バックアップ手順を継続的に監視すべきである。

h. データの復元とレジリエンス：

i. RPO および RTO を定義し、バックアップ頻度および復旧戦略を導く指標として使用する。

ii. データ損失または破損が発生した場合に、バックアップからデータを復元する手順を概説した包括的なデータ復元計画を策定する。定期的に計画をテストし、その有効性を確認する。

iii. バックアップの復元は、(CSC との契約上の合意または CSP の内部ポリシーに従って）権限を有する要員によって承認された後にのみ実施されるものとする。

iv. バックアップおよびデータ復元手順は、手作業による介入やダウンタイムを最小限に抑え、復旧を迅速化するために自動化する。

v. 自動化ツールを使用して、バックアップのスケジュール、バックアップの健全性の監視、リストアのトリガー、およびリストアワークフローを管理する。

vi. 複数のデータセンターまたは地理的地域にデータを複製し、地域的な停電や災害時にデータの可用性を確保する。同期または非同期レプリケーションなどのレプリケーション技術を使用する。

vii. バックアップのリストアは、定期的にテストし、データの損失や破損から回復できることをを確認する。

i. バックアップの監視と記録：
データのバックアップとリストア手順の継続的なモニタリングと記録を実施し、潜在的な問題を迅速に検出して対処する。監視ツールを使用して、バックアップの状態、データの完全性、リストアのパフォーマンスを追跡し、バックアップシステムの異常や障害に対する警告を設定する。

j. 第三者の評価：
第三者によるセキュリティ評価を実施し、バックアップとセキュリティ対策の有効性を検証する。

k. CSC とのコミュニケーション：
CSP は、妥当な場合、事業継続性およびレジリエンスの保証の一環として、バックアップおよびリストアのテスト結果を CSC に開示する。

l. バックアップの見直しと更新：
バックアップおよび復旧計画は、データ量、インフラストラクチャ、および規制要件の変化を反映して定期的に見直され、更新され、計画が現在のビジネスニーズおよびセキュリティ標準と整合していることを保証する。

Control Title	Control ID	Control Specification
災害対応計画	**BCR-09**	自然災害や人為的な災害から回復するための災害対応計画を確立、文書化、承認、伝達、適用、評価、維持する。少なくとも年 1 回、または、大幅な変更があった場合に、その計画を更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の責任は、CSP と CSC との間で共有(依存)であり、CSP は自分自身の災害対応計画 （DRP） と利用者に関連する計画を設計および実装する責任があるからです。 この管理策の CSP の所有権は、CSP がコントロールするリソースに対する災害対応を設計および管理するための DRP に関連する。	**管理策所有権の根拠：** CSC の管理策所有権は、CSC が管理するリソースに対する災害復旧を策定し、管理するための DRP に関わるものとする。 DRP を策定する際、CSC は、CSP による、利用可能にする災害復旧手順と技術を考慮すべきである。
実施ガイドライン **IaaS プロバイダー：** CSP は、クラウドの物理インフラストラクチャに関する DRP を確立し、文書化し、実践し、実施し、レビューし、維持する責任を負う。	**実施ガイドライン** **IaaS 利用者：** CSC は、CSC の管理計画、仮想ホスト、仮想ネットワーク、アプリケーション、および CSC がクラウドインフラストラクチャ上にデプロイする関連リソースを含む DRP を確立し、文書化し、実施し、実施し、レビューし、維持する責任を負う。
SaaS カスタマー： CSP は、基盤となるプラットフォームリソース、仮想マシン、ネットワークリソース、およびクラウドサービスが関連する管理プランまたは管理インタフェースに対する DRP を確立し、文書化し、実践し、実施し、レビューし、維持する責任を負う。 以下のガイドラインは、DR 計画（これらに限定されない）の確立、文書化、承認、連絡、実施、レビュー、維持に適用する： a. DR チームの設立： i. 部門横断的なチームは、クラウドインフラ、データ復旧、セキュリティ、カスタマサポート、通信の専門家から結成する。 ii. 各緊急対応チームメンバーの役割と責任は、明確に	**SaaS 利用者：** CSC は、CSC 担当者がクラウドサービス、アプリケーションデータへのアクセスに使用する PC およびその他のデバイスに対する DRP を確立し、文書化し、実施し、実施し、レビューし、維持する責任を負う。 以下のガイドラインは、DR 計画（これらに限定されない）の確立、文書化、承認、連絡、実施、レビュー、および保守に適用される： CSP の「実施ガイドライン」が適用される。

し、説明責任と効率的な連携を確保する。

b. 災害リスクの特定：

i. 徹底的なリスクアセスメントは、潜在的自然災害（洪水、地震、ハリケーンなど）および人為的脅威（サイバー攻撃、停電、人為的ミス）を特定するために、実施する。

ii. それぞれの災害の重大度と確率は、評価し、事業運営への潜在的影響に基づいてリスクの優先順位をつける。

c. DRP の開発：

i. 災害への備えと復旧に対する組織の全体的なアプローチの概要を示す DR 計画を策定し、文書化する。

ii. その DR 計画には、リスクアセスメント、復旧目的、復旧手順、連絡計画、連絡先情報を含める。

iii. 復旧手順は、重要なサービスまたはアプリケーションごとに概説する。これらの手順には、データ復旧、システム復旧、アプリケーション再実践、事業継続に必要な手順、責任者、リソースを明記する。

iv. 計画は、災害前、災害中、災害後に取るべき以下の手順に従って概説すべきである：

- 予防:データのバックアップ、インフラの堅牢化、セキュリティプロトコルなど、災害リスクを軽減するための事前対策を実施する。
- 検知：潜在的な脅威を検知し、迅速に対応プロトコルを開始するための早期警戒システムと監視ツールを確立する。
- 対応：影響を受けたシステムの隔離、サービスの復旧、カスタマーとの連絡のための明確な手順を定義する。
- 復旧：データ復旧、インフラ改善、検証テストなど、完全な機能回復のための手順を概説する。

d. DRP の文書化：

DR 計画を文書化し、全ての DR 関連文書とともに、一元化されたセキュアなリポジトリに保管すべきである。

e. DRP の承認：

DR 計画の実施に必要な権限とリソースを確保するため、上級管理職から正式な承認を得るべきである。

f. DRP コミュニケーション：

i. 計画は、人員、CSC、パートナーを含む全ての関係者にコミュニケーションする。

ii. 災害時のタイムリーで正確な情報共有を確実にするため、情報伝達経路、プロトコル、メッセージフォーマット、エスカレーション手順を CSC と確立する。

iii. CSC は、機体を管理するために、RPO および RTO を含め、CSP の災害準備および復旧能力について知らされるべきである。

iv. 状況および復旧作業に関する定期的な最新情報を提供する。

g. DRP の実施とテスト：

i. 定期的にシミュレーションと演習を実施し、DR 計画の有効性をテストし、改善点を特定する。 ii. テストには、シミュレーション、机上演習、実規模のテストを含む。 iii. 過去の事故から学び、教訓を計画に取り入れる。 h. 事故後の DRP 効果評価： i. 各災害事象の後、徹底的な事後レビューを実施し、計画の有効性を評価し、改善点を特定し、それに応じて手順を更新する。 ii. 各災害事象から学んだ教訓は文書化し、その洞察を災害対応計画に反映させ、将来の備えを強化する。 i. DRP のレビュー： DRP のレビューと更新は、少なくとも年 1 回実施し、DRP が現在の脅威、リスク、業界のベストプラクティスに合致し、ビジネス目標やクラウド技術、インフラ、ビジネスオペレーションの変化に準拠していることを確認すべきである。	

Control Title	Control ID	Control Specification
対応計画の演習	**BCR-10**	災害対応計画を毎年、または重要な変更があった場合は、可能であれば地元の緊急事態当局も含めて実施する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この所有権は、“Shared (Dependent)”である。何故なら、計画の作成など、多くの活動の側面は独立して行うことができるが、災害復旧とそれに関連するテストは、CSP サービスの復元とレジリエンステストを伴うため、対応計画の実施に CSC が CSP に依存する必要がある。特に CSP が提供する特定のレジリエンス機能（リージョン内またはリージョン間のフェイルオーバーなど）をテストする場合、CSC の CSP への依存を必要とする可能性があり、また多くの場合において必要とされるからである。CSP は、自社のインフラおよびサービスにおける DR のテストに責任を負う。 演習とテストは、重要なビジネス機能を支えるシステム、ネットワ	**管理策所有権の根拠：** CSC は、CSP のインフラとサービスに基づく、サービスの DR テストに責任を負う。

ーク、アプリケーション、データなどのテクノロジー・コンポーネントの継続性とレジリエンスを経営陣が検証するのに役立つ。手法の種類または組合せは、企業の規模、複雑さ、事業の性質に応じて決定されるべきである。全ての重要な機能およびアプリケーションの包括的なテストにより、CSP は潜在的な問題を特定できる。したがって、CSP は、BCP の実行可能性を検証するために、このセクションで説明する方法か、より徹底的なテスト方法のいずれかを使用する。演習には、シミュレートされた環境（すなわち、機能演習）での職務の実行、ディスカッションに基づくもの（すなわち、机上演習）、実規模または限定的な規模のものが含まれる。	
実施ガイドライン： **全てのサービスモデルに適用** 災害復旧計画の実施に関するベストプラクティスには、以下が含まれる（但し、これらに限定されない）： a. DRP 演習の範囲と目的： i. テストの対象となるシステム、人員、手順など、演習の範囲を特定する。 ii. DRP 演習の範囲は、CSP の特定のニーズとリスクに合わせて調整する。 iii. DRP の演習目的を明確にする。 b. 機能横断的なチームの設置： 演習の計画、実施、および評価を担当する横断的な専門チームを設置すべきである。(例えば、IT、セキュリティ、運用、通信、および関連部門の代表者を含める)。 c. DRP 演習計画の策定： DRP の演習計画には、演習の範囲、目標、目的、参加者、シナリオ、評価標準の概要を示すべきである。 i. 自然災害、サイバー攻撃、人為的ミスなど様々なタイプの災害を含め、対応計画の様々な側面が問われる現実的な災害シナリオをシミュレートする。 ii. DRP 演習は、本番サービスへの支障を避けるため、本番環境とは別の環境で実施する。 iii. 社外関係者（CSC、パートナー、緊急サービスなど）との連絡経路をシミュレートする。 iv. 全ての参加者は、DRP 演習計画および演習中に伝達される役割と責任を熟知する。 v. DRP の演習とテストの間、CSC を支援する。 vi. DRP 計画の演習は、毎年、または DRP 計画に重要な変更が生じたときに実施する。 d. 地域の緊急当局： CSP の DR 計画が地域の緊急対応活動と連携していることを確認するため、地域の緊急当局を計画と演習の手順に関与させるべきである。緊急当局は、災害対応の専門知識、他の組織との調整、公共セキュア要員や設備などのリソースへのアクセスを提供できる。 e. 机上演習： 机上演習を定期的に実施し、災害シナリオと対応手順を確認することで、改善点を特定し、その結果に基づいて計画を改	**実施ガイドライン：** **全てのサービスモデルに適用；** CSC は、以下を実施する責任を負う。: 進化する脅威と組織の脆弱性を考慮し、ビジネスのニーズと目標に沿った災害復旧計画（DRP）を策定する。 • DR 訓練に不可欠なリソースの開発 • 訓練結果に基づく継続的な改善プロセスの確立 • 年次 DR 計画の実行、または大幅変更時の実施 • 適切な機能を検証するための定期的な DR ソリューション・テストの実施 • CSP の RTO および RPO が CSC 要件に準拠していることを検証 • テストを通じて、その他の CSP-CSCSLA 定義パラメータを評価

善する。 f. 演習結果の文書化と伝達： i. 成功、課題、および行動項目を含む DR 演習計画の結果は、文書化され、全ての利害関係者に伝達する。 ii. 災害時の定期的な伝達は、CSC に状況を常に伝え、事業の中断を最小限に抑えるのに役立つ。 g. 継続的改善： 演習や実際の災害から得られたフィードバックや教訓は文書化し、DR 計画に反映させ、その有効性を向上させるべきである。 h. レビューと更新： i. DR 演習計画は、演習やテストの結果、および組織のビジネスプロセス、資産、リスクの進化に基づいて、定期的に見直し、更新し、適切かつ効果的であり続けるべきである。	

Control Title	Control ID	Control Specification
設備の冗長性	**BCR-11**	業界標準に従って、ビジネスクリティカルな機器に対して、合理的な範囲で最小限の離れた場所に独立して冗長機器を配置する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この所有権は、CSP が所有し、自ら実施する責任がある。何故なら CSP は、ビジネスクリティカルな機器の所有者であり、冗長性対策で補完し、許容可能なリスクの適切な場所に配置する責任が有るからである。CSP は、CSC に冗長機器と管理策の実施に関する情報を提供する責任を負う。	**管理策所有権の根拠：** CSC には、適用されない。
実施ガイドライン **全てのサービスモデルに適用：** データセンターの戦略的配置と建設は、CSP にとって極めて重要である。データセンターの立地は、自然現象による障害を最小限に抑えるために慎重に検討すべきである。冷却のしやすさ、耐震性、洪水リスク、地政学的安定性などの要因を綿密に評価すべきである。	**実施ガイドライン：** CSC には、適用されない。

データセンターの実装前に、CSP は包括的なサイトアセスメントを実施し、クラウドインフラに関連する潜在的なリスクを積極的に軽減すべきである。関連する業界団体や標準化団体と連携することで、意思決定手順において貴重な洞察や指針を得ることができる。

CSP の冗長化戦略は、CSC との契約や SLA で宣言された要件に準拠すべきである。

機器の冗長性に関する実施上のベストプラクティスには、以下が含まれる（但し、これらに限定されない）：

a. ビジネスクリティカルな機器の特定：
   中核的なビジネスオペレーションを維持するために不可欠な機器を特定する（例えば、サーバー、ストレージシステム、ネットワークデバイス、およびデータ処理、通信、アプリケーションの可用性に不可欠なその他のインフラストラクチャコンポーネント）。
b. 機器の冗長戦略：
   i. 冗長化戦略は、ビジネス要件、ビジネスインパクト分析、およびリスク評価と整合させ、最適なリソース配分と重要な障害からの保護を確保する。
   ii. 必要な冗長性のレベルは、ビジネスクリティカルな構成要素ごとに評価する。これは、機器の重要度、ダウンタイムの潜在的影響、および組織のリスク許容度によって異なる。
   iii. サービスの継続性を維持するために、地域又は場所固有の障害に関連する潜在的リスクを事前に評価し、緩和し、改善する。
   iv. 冗長性を効果的に管理し、サービス運営を中断なく維持するために、ツールやインタフェースを含む管理策計画を策定し、実施する。
   v. 複数の地理的な場所に冗長データセンターを提供し、信頼できる CSP からのクラウドインフラサービスを利用する。
   vi. システムの冗長性の例
      - 全ての重要なシステムに冗長電源を装備し、停電のリスクを軽減する。多様性を確保するために、別々の電力網または電力源を使用する。
      - 単一障害点を回避するために、多様なネットワーク経路を導入する。複数のインターネットサービスプロバイダー（ISP）を利用し、データセンター間の冗長接続を確立する。
      - サーバー、ストレージ、ネットワーク機器などのハードウェアを冗長化する。
      - ロードバランシングやフェイルオーバークラスタリングなどの技術を活用し、冗長システム間でワークロードを分散する。
      - 地理的に分散したデータセンター間でデータのレプリケーションやバックアップを実施し、サイト障害時のデ

ータ可用性を確保する。

c. 冗長アーキテクチャの文書化：
冗長化戦略、考案されたアーキテクチャと構成の詳細な文書を作成し、維持すべきである。

d. 地理的分散：
自然災害や停電のような局地的な事象による同時停電のリスクを最小化するために、ミラーリングされた機器または冗長化された機器は、互いに合理的な最小距離にある別々のデータセンターに設置すべきである。

i. 可能であれば、マルチロケーション（すなわち、冗長化システムを地域内の複数拠点にまたがって配置する）およびマルチリージョン冗長化戦略（冗長化システムを複数拠点からなる複数地域にまたがって配置する）を採用し、実施する。

ii. 冗長化されたデータセンター間で、データの一貫性と可用性を確保するため、データ複製戦略を導入する。

e. 自動フェイルオーバーメカニズム：
自動化されたフェイルオーバーメカニズムは、プライマリ装置に障害が発生した場合、トラフィックを冗長装置にシームレスに切り替え、手動による介入なしに運用が中断されることなく継続されるように構成すべきである。

f. テストと保守：
冗長機器の準備と機能性を確保するため、定期的なテストを実施すべきである。システムの性能と信頼性を維持するため、プライマリ機器と冗長機器の両方について包括的な保守計画を策定する。

g. 継続的改善：冗長化戦略は、進化するビジネスニーズ、技術の進歩に基づき、また業界標準や関連する規制要件に従って、定期的にレビューし、更新すべきである。

Control Domain CCC

2.4 変更管理と構成管理(CCC)

Control Title	Control ID	Control Specification
変更管理ポリシーと手順	**CCC-01**	資産が内部で管理されているか、外部で管理(例：外部委託)されているかに関わらず、アプリケーションやシステム、インフラストラクチャ、設定など、組織が持つ資産の変更に関連するリスクについて、それを管理するためのポリシーと手順を確立、文書化、承認、伝達、適用、評価、維持する。少なくとも年1回はポリシーと手順をレビューし更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。変更管理ポリシーと手順は、CSP および CSC が、それぞれの企業のビジネスニーズ、要件、および業界標準に沿う形で、それぞれ独自に管理し、ベースライン化するものとする。	**管理策所有権の根拠；** CSC は、契約サービスに対して提案された全ての変更が、影響分析、変更失敗時のロールバック、サービスの脅威／尤度分析を含む正式なプロセスを経て管理され、サービスが予期せぬ劣化や停止に見舞われないようにするためのポリシーと手順を含む、自身の変更管理プロセスを確立する責任を有する。十分に熟練した変更管理者を任命し、正式に予定されたレビュー会議において、計画された変更をレビューする。
実施ガイドライン； 堅牢な変更管理と構成管理プロセスの確立は、CSP がクラウドサービスの安定性、セキュリティ、信頼性を確保するために不可欠です。変更管理プロセスは、クラウド環境への変更が慎重に計画、レビュー、承認され、管理された方法で実装されることを保証する。これにより、サービスデリバリーを中断させたり、セキュリティを侵害する可能性のある、未承認または意図しない変更を防ぐことができる。一方、構成管理プロセスは、クラウド環境全体で一貫性のある正確な構成を維持することに重点を置き、システムが適切に構成され、セキュリティ標準やビジネス要件に準拠していることを保証する。 CSP は、仮想の弾力的なコンピュート、サーバーオペレーティングシステム、ストレージ、ネットワークなどのインフラストラクチ	**実施ガイドライン；** CSC は、アプリケーションのライフサイクルの全ての側面と、サポートするアプリケーションを使用して開発されたビジネスサービスを管理していることから、アプリケーションレイヤーとデータレイヤーについて、文書化され、毎年見直される完全な変更管理プロセスが実施されるべきである。 SaaS モデルでは、CSP は完全なソフトウェアソリューションを提供し、CSC はそれを従量制で購入する。CSC は、SaaS アプリケーションのセキュリティ管理及びサービスに接続するエンドポイントの管理を行う。 SaaS の CSC は、データを保護するために SaaS アプリケーションを管理する際に、様々なセキュアな構成ポリシーの要件と管理策

ャ、さらにはミドルウェア、開発ツール、ビジネスインテリジェンスサービス、データベース管理システムについての設計、実装、管理に責任を持つ。CSC が利用するサービスに対する全ての変更案が管理され、正式な手続きに従うことを保証するために、変更管理プロセスが運用されなければならない。アプリケーションは、契約で合意されたとおりに設定されなければならない。

ポリシーには、以下に関する規定が含まれるべきである（ただし、これに限定されない）：

a. 範囲と目的変更管理プロセスの範囲、目的、役割及び責任は、組織の戦略目標、ビジネス要件及びセキュリティポリシーと整合させ、関連する法律、規制及び標準に準拠させる。
   i. 全ての変更要求のレビューと承認を担当する変更管理委員会（CCB）を設置する。
   ii. 変更管理プロセスの監督と実行を担当する変更管理の専門チームを結成する。
   iii. 変更の開始、レビュー、承認、実施、テスト、実施後のレビューなど、変更管理プロセスの各フェーズについて、明確な役割と責任を割り当てる。
   iv. 構成変更、ソフトウェア更新、ハードウェア変更、データ変更など、変更を構成するものを定義する。
b. 変更管理プロセス：クラウドコンピューティング資産に対する変更を管理するための変更管理ワークフローの概要を示す正式なプロセスを確立するための要件を定義する必要がある。
c. 変更管理ベースライン：変更の標準点となる組織資産の標準的で承認された状態を含む、変更管理ベースラインの確立と維持のための要件。変更管理ベースラインは、正確で最新であることを確認するために定期的にレビューされなければならない。
d. ベースライン逸脱の検出：逸脱や異常を検出して報告するために、組織資産の構成を定期的に監視・監査し、変更管理のベースラインと比較するための、ベースライン逸脱の検出プロセスの確立に関する要求事項である。
e. 例外管理：変更管理ポリシーと手順に対する例外を管理するための手順、手続には、例外の要求、例外のレビュー、例外の承認、および例外の文書化のプロセスを含めるべきである。
f. 変更リスク評価：クラウドコンピューティング資産に対する全ての変更のリスク評価を行い、関連するリスクを十分に理解した上で変更が行われ、それらのリスクを最小限に抑えるために適切な措置が取られるようにする。
g. 品質テスト：定義された品質変更管理、承認、テストプロセスであり、ベースライン、テスト、リリースの標準が確立されていること。このプロセスには、テスト計画、テストケース、受入標準を含める。
h. 変更の承認：クラウドコンピューティング資産に対する全ての変更が承認され、正当な変更が本番稼動前に承認されるための承認プロセスである。
i. CSP と CSC の変更契約：変更の範囲、頻度、時期、期間、通を考慮する必要がある。以下に、注目すべき重要な分野をいくつか挙げる：
   a. アクセス制御:PoLP に準拠したアクセス制御をセキュアに設定し、SaaS アプリケーションの機密データへのアクセスを制限する。
   b. 強力な認証：全てのユーザーに対して多要素認証（MFA）を有効にし、パスワードだけでなく、さらなるセキュリティのレイヤーを追加する。
   c. データの暗号化：機微情報を不正アクセスや侵害から保護するために、保存中データと移動中データの両方に暗号化を設定する。
   d. デフォルト設定のハードニング:SaaS ベンダーが提供するデフォルト設定を見直し、ハードニングすることで、不要な機能を無効にし、潜在的な攻撃ベクトルを減らする。
   e. アプリケーションのセキュリティ更新：脆弱性に対処し、既知のエクスプロイトから保護するために、セキュリティアップデートの設定を有効にし、迅速に適用する。（可能であれば自動化します）
   f. サードパーティーとの統合：サードパーティーとの統合を精査し、セキュリティのベストプラクティスに準拠し、不必要なリスクをもたらさないようにする。
   g. ロギングと監視、ユーザーアクティビティ、システムイベント、セキュリティ関連のインシデントについて、適切な SaaS アプリケーションのロギングと監視を構成し、異常や潜在的な脅威を迅速に検出する。

CSP が提供するポリシーは適用される。

知、承認、報酬など、CSC が所有する環境／テナントに直接影響を与える変更の条件を定義する変更契約の要件。 j. 変更復元：インシデント、エラー、逸脱の原因または要因となった変更を元に戻し、クラウド資産とそのベースライン構成を以前の状態または望ましい状態に復元するための復元要件を変更する。 k. 承認：組織の戦略目標及びリスクアペタイトとの整合性を確保するための承認要件及び上級管理職の関与 i. ポリシーと手順の変更または修正については、承認プロセスを確立すべきである。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持する。 l. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進すべきである。 m. メンテナンスとレビュー：変更管理およびコンフィギュレーション管理のポリシーと手続きは、少なくとも年 1 回、以下のように文書化し、見直し、更新する。	

Control Title	Control ID	Control Specification
品質テスト	**CCC-02**	確立されたベースライン、テスト、リリース標準を含む、定義された品質変更管理プロセス、承認プロセス、テストプロセスに従う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。全ての品質変更管理プロセス及び適用されるシステム変更は、それぞれの企業ポリシーに従い、業界標準に沿った形で、独立してベースライン化、テスト、及び承認されるべきである。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； **全てのサービスモデルに適用：** CSP は、変更管理プロセス中にテストとレビューを行う計画を立て	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

るべきである。この計画には、テストのインプットと条件付き結果を含めるべきである。内部開発の場合、最初に変更を監督するチームがそのようなテストを実施できる。その後、独立した受入テストを実施して、システムが意図したとおりに機能するかどうかを判断することができる。

組織資産に対する計画的な変更を実施する前に、テスト記録を文書化すべきである。この記録は、テスト計画、変更前の構成ベースライン、テスト結果、新しい構成ベースラインから構成されるべきである。

この管理策の実施におけるベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）：

a. 品質変更管理ベースライン：
   i. 変更の影響を評価し、サービス品質とセキュリティが維持されていることを確認するために、主要業績評価指標（KPI）とセキュリティ指標によるベース ラインを設定する。
   ii. 変更の一貫性、信頼性、および既存のクラウド環境構成との互換性を確保するために、質の高い変更管理プロセスを導入する必要がある。
b. テスト戦略：単体テスト、統合テスト、パフォーマンステスト、セキュリティテスト、ユーザーテストを包含する包括的なテスト戦略を策定する。

受け入れテスト。テスト手順を合理化し、効率を向上させるために、可能な限り自動テストツールを活用すべきである。

c. リリース標準：クラウドサービスに新機能、アップデート、パッチをリリースする前に、リリース標準を定義すべきである。これらの標準は、コードの品質、互換性、セキュリティの脆弱性、バグ修正などの側面を扱うべきである。
d. テストとデプロイの自動化：テストは、変更が期待される結果、性能、機能を満たしていること、およびエラー、バグ、脆弱性をもたらさないことを検証する。
   i. クラウドコンピューティングの資産に対する全ての変更は、本番環境に実装する前に、非本番環境でテストすべきである。
   ii. 手作業を減らし、テストサイクルを迅速化するために、テスト工程は可能な限り自動化すべきである。
   iii. 継続的インテグレーション（CI）と継続的デリバリー（CD）のパイプラインは、本番環境への変更のデプロイを自動化するために利用されるべきである。
e. ユーザー受け入れテスト（UAT）：変更のテストにエンドユーザーを参加させるために、UAT 手順を実施すべきである。変更が機能要件およびユーザビリティ要件を満たしていることを確認するために、エンドユーザーからフィードバックを収集すること。

Control Title	Control ID	Control Specification
変更管理技術	**CCC-03**	資産が内部で管理されているか、外部で管理(例：外部委託)されているかに関わらず、アプリケーションやシステム、インフラストラクチャ、設定など、組織が持つ資産の変更に関連するリスクを管理する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。システムにおける全ての構成変更は、それぞれの企業ポリシーに従い、業界標準に沿って、独立してベースライン化、テスト、および承認されるものとする。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； リスク管理は、クラウド資産に対する変更がセキュアかつ管理された方法で実施されることを保証する上で、重要な役割を果たす。CSP は、変更に伴う潜在的なリスクを特定、評価、および軽減するためにリスク管理を活用し、クラウドサービスのエラー、セキュリティ侵害、中断の可能性を最小限に抑えるべきである。 **全てのサービスモデルに適用；** この管理策の実施におけるベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）： a. 変更管理プロセス：このプロセスには、変更要求書、レビューと承認プロセス、テスト、実施変更手順、成果文書が含まれるべきである。変更状況が継続的に追跡され、管理された一貫した方法で行われ、エラーや混乱のリスクを最小限に抑えることが保証されるべきである。 変更要求書には、以下を含めるべきである： i. 変更の内容 ii. 変更の正当性 iii. 変更の潜在的リスク iv. 事業運営への影響 v. 問題が発生した場合の変更の戻し手順 vi. 関係者の承認署名 b. 変更リスク管理：変更の影響と種類を評価し、適用前に変	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

更のリスクを決定する。 i. 変更を実施する前に、CSP は徹底的な影響評価を行い、クラウド資産、パフォーマンス、セキュリティ、およびコンプライアンス要件への潜在的な影響を特定する必要がある。 ii. 変更は、その影響、緊急性、リスクプロファイルに基づいて分類される。リスクの高い変更には優先的な注意が払われ、厳密なレビューとテストが行われる。 iii. クラウド資産と変更管理手法に関連するリスクの進化を定期的に特定し、リスク管理戦略を適宜見直し、更新する必要がある。 c. 変更管理ツール： i. 変更管理ワークフローを定義し、変更がセキュリティ、運用、開発チームを含む関連する利害関係者によって提出、レビュー、承認されるようにし、無許可の変更または不適切に管理された変更を防止する。 ii. 変更管理ワークフロープロセスを効果的に記録するために、変更管理ツールを採用すべきである。 d. 利害関係者の協力： i. 変更およびリスク管理プロセスに関わる社内外の関係者と協力する。 ii. 対象分野の専門家の適切なレベル、および変更のレビュワーと承認者の役割は、変更のタイプとリスクレベルの組み合わせによって決定されるべきである。 e. 継続的なモニタリングとロギングツール：変更に起因する新たなリスクの管理を支援するために、タイムリーな情報に基づく意思決定を行うことができるように、変更の進捗に関するリアルタイムの報告／監視機能を提供するために導入されるべきである。 f. 構成管理ツール：これらのツールは、クラウドインフラストラクチャの構成における追跡と管理を行い、変更管理ポリシーと手順における一貫性と遵守を保証する。 g. 変更レビュー委員会：セキュリティ、プライバシー、リスク、コンプライアンス担当者は、変更レビュー委員会の一員とすべきである。	

Control Title	Control ID	Control Specification
承認されていない変更からの保護	CCC-04	組織の持つ資産への承認されていない追加や削除、更新、管理などを制限する。

Control Ownership by Service Model		
IaaS	PaaS	SaaS

Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。システムに対する全ての構成変更は、それぞれの企業ポリシーに従い、業界標準に沿って、独立してベースライン化、テスト、および承認されるものとする。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； CSP は、アプリケーション、システム、インフラストラクチャ、構成など、運用中の組織資産に対する不要/不正な変更（追加、削除、更新など）を防止および/または検出するための手順を確立し、技術的な対策を実施するべきである。 組織は、変更を開始する目的で、資格と権限を持つ個人だけがシステムにアクセスすることを許可すべきである。アクセス制限には、暗号の管理策や MFA などの物理的および論理的なアクセス制御が含まれる。 **全てのサービスモデルに適用：** この管理策の実施におけるベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）： a. 一元化された資産管理システム：全組織資産の正確かつ最新のインベントリを活用し、資産の追加、撤去、更新を追跡するための単一ソースとして使用する（DCS-06 を参照）。 b. アイデンティティとアクセス管理の変更：強固な IAM システムを導入し、アイデンティティ、役割、権限に基づいて、ユーザーの資産へのアクセスや変更を管理する。資産への不正な変更を防ぐため、多要素認証（MFA）などの強力な認証メカニズムを使用することが必要である。 c. 最小特権の原則による変更：機微資産や設定へのアクセスを制限することで、不正または偶発的な変更のリスクを最小化するため、最小特権の原則を実施すべきである。 d. SoD による変更:同じチームが変更の開発と承認の両方を行うことができないように、十分な職務分掌が存在することを確認する。 e. 変更の監視とロギング： i. クラウド資産の設定、アクセスログ、ユーザーアクティビティを継続的に監視し、不正な変更や異常な動作を検出する必要がある。 ii. セキュリティを脅かしたり、クラウドサービスを中断させたりする可能性のある不正または意図しない変更は、検出、調査、報告されるべきである。	**実施ガイドライン；** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

iii. 自動監視ツールを使用して、潜在的なセキュリティ脅威を特定し、不正な変更を防止する。 f. 環境の分離：不正な変更やセキュリティ脆弱性が本番システムに影響を及ぼすリスクを最小化するために、本番システムと開発環境やテスト環境との分離を活用すべきである。	

Control Title	Control ID	Control Specification
合意事項の変更	**CCC-05**	CSC が所有する環境/テナントに直接影響を及ぼす変更について、CSP と CSC の間で定めたサービスレベル合意書で明示的に認められた要件に限定する条文を含める。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。利用されるシステムに対する全ての構成変更は、CSP と CSC 間の契約内で適切に管理されるべきである。CSP がこの管理を実施し、SLA にその規定（すなわち、CSC のシステムに影響を与える変更 の制限）を含めるためには、CSC が果たすべき役割、すなわちそのような規定を議論し、洗練し、承認する役割がある。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； CSP と CSC の双方によって確立されたプロセスと手順には、変更管理の責任を反映させるべきである。各当事者は他方の責任を認識し、これは書面による変更管理契約の一部とする。確認書には、CSC が所有する環境に影響を与える変更に関連する制限に関する言及が含まれるべきである。CSC は、変更を行うことができない場合の除外ウィンドウを構成、管理、または CSP に伝えることができるものとする。	**実施ガイドライン；** CSP と CSC の双方によって確立されたプロセスおよび手順は、それぞれの変更管理責任を反映すべきである。各当事者の責任を確認し、それを CSC と CSP 間の書面による変更管理契約の一部とする。確認書には、CSC が所有する環境/CSC に影響する変更に関連する制限事項への言及が含まれるべきです。CSC は、変更を行うことができない場合の除外ウィンドウを構成、管理、または CSP に伝達できるものとする。
IaaS プロバイダー： CSP は、IaaS サービスの一部として提供されるコンピュート、ストレージ、およびネットワークリソー スについてのみ、変更管理およびテストプロセスを確立する責任を負う。CSP が管理する資産が	**IaaS 利用者：** CSC は、サポートするインフラとネットワークを除く、アプリケーションサービス提供の全側面に対する責任を維持するため、CSP が管理するこれらの資産に対する変更は、事前に CSC によっ

変更されると、依存するアプリケーションに悪影響が及ぶ可能性があるため、 CSC に事前に通知することなく、これらのシステムに対して変更を行うべきではない。CSP のフォワードスケジュールオブチェンジ（FSC）プログラムは、サービスレベル合意の一部として CSC と合意されるものとする。	て承認されなければならない。このような変更に CSC からの承認を必要とする変更管理プロセスを組み込むことで、変更がサービスの低下を引き起こす可能性が低くなる。
PaaS プロバイダー： CSP は、仮想の柔軟なコンピュート、サーバーのオペレーティングシステム、ストレージ、ネットワーキングといったインフラだけでなく、ミドルウェア、開発ツール、ビジネスインテリジェンスサービス、データベース管理システムなど、サポートする全てのインフラの設計、実装、管理に責任を持つため、変更がある場合は、実装前に CSC が事前に同意する必要がある。	**PaaS 利用者：** CSC は、サポートするインフラストラクチャとネットワーキングを除く、アプリケーション サービス提供の全ての側面に対する責任を維持するため、CSP が管理するこれらの資産に対するいかなる変更も、事前に CSC によって承認されなければならない。このような変更に CSC からの承認を必要とする変更管理プロセスを組み込むことで、変更が CSC のサービス低下を引き起こす可能性が低くなる。
SaaS プロバイダー： CSP は、以下の設計、実施、資産管理に責任を持つ： a. 仮装の柔軟なコンピュート、サーバーのオペレーティングシステム、ストレージ、ネットワークなど、全てのサポートインフラストラクチャ b. ミドルウェア、開発ツール、ビジネスインテリジェンスサービス、データベース管理システム c. CSC との契約に従って設定されたアプリケーション	**SaaS 利用者：** このモデルでは、CSP は完全なソフトウェアソリューションを提供し、CSC はそれを従量制で購入する。CSC は、CSP とのサービス契約で合意されたとおり、変更を要求するか、少なくとも構成変更に関する相談を受けることが期待される。 CSC に適用されるその他の推奨事項は以下の通りである（ただし、これらに限定されるものではない）： a. 変更管理の通知と承認：CSC は、自社のクラウド環境に影響を及ぼす可能性のある全ての構成変更を確認し、承認しなければならない。 i. CS と協力し、効果的なコミュニケーションプロトコルを開発・実施する。 ii. 変更案を積極的に検討し、フィードバックを提供する。 iii. 懸念事項や潜在的な影響を CSP に伝えます。 iv. 提案された変更の承認または却下をタイムリーに行う。 b. 変更のロールバックと修正：CSC は変更の実施を監視し、問題があれば CSP に報告する。 i. ロールバックまたは修復作業中に CSP をサポートする。 ii. ロールバックおよび修復手順の有効性をテストし、検証する。 c. 継続的な監視と改善：CSC は、変更管理プロセスについて CSP にフィードバックを提供する。 i. CSP と協力して改善すべき分野を特定する。 ii. 継続的改善イニシアチブの実施に CSP と共に参加する。
全てのサービスモデルに適用： CSP に適用されるその他の推奨事項には、以下が含まれる（ただし、これらに限定されるものではない： a. SLA が認めた変更と定義：	**全てのサービスモデルに適用：** CSP に規定されている、この管理の実施に関するベストプラクティスが適用される。

i. 変更管理プロセスを SLA と統合し、CSC と CSP の双方がこのプロセスを遵守する責任を負うようにすべきである。
ii. 何が承認された変更であるかは、変更の種類、変更の範囲、および各変更の承認プロセスを明記するなど、SLA で定義されるべきである。

b. 変更管理の通知と承認：CSP は、自社のクラウド環境に影響を及ぼす可能性のある構成変更を CSC に通知し、確認および承認する機会を持つべきである。
i. CSC に対する明確な通知手順（例えば、提案された変更、その目的、影響、潜在的なリスク、及びロールバック手順に関する詳細情報を含む変更要求（CR）プロセス）を伴う正式な変更管理プロセスを確立すべきである。
ii. 環境に対する潜在的な影響を含め、提案されている変更に関する詳細情報を CSC に提供する。
iii. CSC に対し、CR、予想される影響、および実施時期を含む、提案された変更に関する通知を適時に提供する。
iv. CSC 環境に影響を与える変更案について、実施前に CSC の承認を得ることが必要である。
v. CSC が所有する環境／テナントに直接影響を与える変更は、合意された保守ウィンドウにスケジュールする。（可能な限り）

c. 変更のロールバックと修復：ロールバック戦略や補償の仕組みなど、無許可の変更や破壊的な変更が発生した場合の修復手順を SLA 内で確立する必要がある。

d. 変更後の報告書：CSC に対し、変更の実施、発生した問題、および環境の最終的な状態をまとめた変更後レポートを提供する。

e. 継続的な監視と評価：CSP は、CSC の環境への混乱を最小限に抑えるため、変更管理プロセスを継続的に監視し、改善すべきである。
i. SLA に変更管理のパフォーマンス指標を盛り込み、無許可または破壊的な変更を防止するプロセスの有効性を測定する。
ii. 変更管理プロセスに関する CSC からのフィードバックを求める。
iii. クラウドインフラ、アプリケーション、および CSC の要件の変更を反映するため、変更管理に関する SLA 条項を定期的に見直し、更新する。

注：緊急の場合、CSP のシステム全体のセキュリティのために必要な緊急の変更であれば、CSC の 明示的な承認なしに、CSC が所有する環境に影響を与える変更を CSP が適用する必要がある場合がある。そのような種類の変更を適用する場合は、できるだけ早く CSC に相談するものとする（CCC-08 の変更管理手順の例外を参照）。

Control Title	Control ID	Control Specification
変更管理のベースライン	**CCC-06**	組織の持つ資産に関連するすべての承認された変更について、変更管理のベースラインを確立する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。システムに対する全ての構成変更は、それぞれの企業ポリシーに従い、業界標準に沿って、独立してベースライン化、テスト、および承認されるものとする。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； 変更管理のベースラインは、特定の時点における全てのクラウド資産の現在の状態のスナップショットである。このベースラインは、クラウド資産に対するその後の全ての変更を評価・測定する際の標準点として機能する。 変更管理ベースラインを確立する目的は、変更が一貫した秩序ある方法で管理、承認、実施されることを保証し、意図しない結果のリスクを最小限に抑え、クラウド環境のセキュリティと完全性を維持することである。 CSP は現在のベースライン構成を開発し、文書化し、バージョン管理下で維持し、更新または新たにインストールされたコンポーネントのために必要な場合は、ベースライン構成を見直し、更新するものとする。	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。
全てのサービスモデルに適用： この管理策の実施におけるベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）： a. 変更管理ベースライン：変更の標準点となる、組織のクラウド資産の標準的で承認された状態を含む変更管理ベースラインを実装する必要がある。ベースラインには以下を含める： i. ハードウェア、ソフトウェアコンポーネント、関連データ、属性、関係を含む、全てのクラウド資産のリスト	

（CMDB など）。
ii. クラウド資産（仮想化、ネットワーク設定、セキュリティ設定、VM、アプリケーション／API 設定など）ごとに、変更管理の対象となる設定／セキュリティ設定、バージョン番号、パッチ状況を把握する。
iii. クラウド資産の健全性、パフォーマンス、利用状況を測定する主要業績評価指標（KPI）
iv. 脆弱性評価、リスク評価、コンプライアンス監査など、クラウド環境の現在のセキュリティポスチャ

b. 文書化：各クラウド資産のベースラインについて、作成日、作成者、関連する資産を含む正確な文書を維持する必要がある。
c. 変更の追跡と実施：
i. クラウド資産に加えられた全ての変更は、ベースラインに対して監視・追跡され、十分に文書化されるべきである（誰が、いつ、何を変更したか、発生した問題やインシデントの報告など）。
ii. バージョン管理システム（例：Git）は、ベースラインの変更を追跡し、履歴を管理するために利用されるべきである。
iii. 提案された変更は、承認前にベースラインと関連するポリシーに照らして評価されるべきである
iv. ベースラインは、新しい変更が実施されるたびに更新され、文書化され、セキュアでアクセス可能な場所に保管され、バックアップされるべきである。
v. 導入された変更は、承認されたバージョンと一致し、確立されたベースラインを遵守していることが事後検証されるべきである。

Control Title	Control ID	Control Specification
ベースラインからの逸脱の検出	**CCC-07**	定義したベースラインから逸脱するような変更があった場合に、プロアクティブに通知する方法を実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠；	**管理策所有権の根拠；**

この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。システムに対する全ての構成変更は、それぞれの企業ポリシーに従い、業界標準に沿って、独立してベースライン化、テスト、および承認されるものとする。	CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； 異常な変更をプロアクティブに検出して対処することで、CSP はセキュリティ侵害、データ損失、コンプライアンス違反のリスクを最小限に抑えることができる。問題が検出された場合、さらなる調査のために関係者に通知する自動化されたアラートを強く考慮すべきです。逸脱が検出された場合、組織はインシデント管理プロセス（SEF-01 を参照）に従うべきである。	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。 さらに、CSC は、契約したクラウドサービスに接続する資産のベースラインを設定し、CSP のベースラインを理解することが期待される。逸脱が検出された場合、CSC は可能な限り早急に CSP に通知することを含め、SEF-01 に定義されたインシデント管理ポリシーと手順に従うべきである。
全てのサービスモデルに適用： この管理策の実施におけるベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）： a. 変更管理ベースラインの逸脱：変更の逸脱は、そのような逸脱を特定するための標準点となる構成ベースラインに対して評価されるべきである（CCC-06 を参照）。 b. 異常検知の閾値：どの変更が確立されたベースラインから逸脱しているかを判断するための閾値は、過去のデータ、リスク評価、業界のベストプラクティスに基づいて定義されるべきである。 c. 変更監視ツール：構成スキャナ、変更検知器、構成監査などの自動および手動のツールや技法を利用して、構成データを収集・分析し、ベースラインとの差異や不一致を特定する。 d. リアルタイムの警告メカニズム：異常が検出されたときにセキュリティチームと関係者に通知するために、リアルタイムのアラートメカニズムを構成する。これらのアラートは、異常に関する詳細情報、潜在的な影響、推奨される対応策を提供する。 e. リスクに基づくアラートの優先順位を設定し：セキュリティチームが最も重要な問題に注意を集中し、迅速に対応できるように、検出された異常の潜在的な重大性と影響に基づいてアラートに優先順位を付ける。 f. 異常評価の自動化：検知された異常の初期調査ステップは、異常の根本原因を特定するのに必要な時間を短縮するために、可能な限り採用されるべきである。これには、イベントの自動相関、データ分析、脅威インテリジェンスの参照が含まれる。 g. エスカレーションプロセス：さらなる調査や修復が必要な異常の処理について、エスカレーションプロセスを定義すべきである。このプロセスには、各ステップの責任者、対応のタイムライン、およびコミュニケーション・プロトコルを明記する。 h. 異常と是正措置の文書化：検出された全ての異常、調査プロセス、及び問題を是正するために講じた措置は、文書化され	

るべきである（異常の根本原因を理解し、再発を防止し、セキュリティ規制の遵守を実証するため）。 i. 検知ルールと閾値のレビュー：検知ルールと閾値は、新たな脅威インテリジェンス、新たな脆弱性、クラウドインフラやアプリケーションの変更に基づいて定期的に見直し、改善する必要がある。 j. 利害関係者への通知：変更管理チーム、CSP、CSC などの関連利害関係者は、逸脱や異常があった場合に通知され、 警告され、さらなる調査と解決のために必要な情報と証拠を提供されなければならない。	

Control Title	Control ID	Control Specification
例外管理	**CCC-08**	変更や構成のプロセスにおいて、緊急事態を含めた例外管理の手順を実装する。手順は GRC-04：ポリシー例外手順の要件に従う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。システムに対する全ての構成変更は、それぞれの企業ポリシーに従い、業界標準に沿って、独立してベースライン化、テスト、および承認されるものとする。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； **全てのサービスモデルに適用：** CSP は、クラウドサービスの可用性、セキュリティ、および信頼性を確保するために、変更および構成プロセスにおいて、緊急事態を含む例外を管理するための堅牢な手順を実装する必要がある。効果的な例外管理により、予期せぬイベントや緊急事態に直面した場合でも、管理された方法で変更が実施されることが保証される。 この管理策の実施におけるベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）： a. 例外のカテゴリ：状況の重大性と緊急性に基づいて対応に優先順位をつけるため、日常的な例外、緊急の例外、緊急事	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

態など、さまざまな例外のカテゴリを定義すべきである。

b. カテゴリの承認プロセス：例外を承認する権限と必要書類を明記し、例外カテゴリごとの承認プロセスを定義する。緊急例外の承認プロセスを合理化し、遅延を最小限に抑える。

c. 例外要請の文書化：例外管理の透明性と説明責任を提供するために、例外の性質、例外の正当性、潜在的リスク、緩和策を含む、全ての例外要求の文書化を義務付けるべきである。

d. 例外の伝達：例外は、変更管理チーム、セキュリティチーム、及び影響を受ける CSC を含む、関連する利害関係者に速やかに伝達されるべきである。

e. 例外のロールバック手順：全ての例外、特に重要なシステムまたはデータに関わる例外について、ロールバック手順を確立する必要がある。

f. 例外発生後のレビュー：例外の根本原因を分析し、得られた教訓を特定し、今後同様の事故が発生する可能性を最小限に抑えるための予防策を実施するために、例外発生後の徹底的なレビューを実施すべきである。

g. 例外管理とインシデント対応の統合：例外管理をインシデント対応プロセスと統合し、セキュリティインシデントやその他の即時対応が必要な障害への協調的な対応を確保する。

h. 例外管理のレビュー例外管理手順は、例外発生後のレビューからのフィードバック、クラウドインフラストラクチャやアプリケーションの変更、セキュリティ脅威の進化に基づいて、定期的にレビューし、改善する必要がある。

i. 例外記録の文書化と維持：例外の性質、承認の詳細、ロールバックの手順、例外発生後のレビュー結果など、インシデント管理分析を目的とした証拠と保管文書の連鎖を収集・保存するために、例外の記録の一元化されたリポジトリが維持されるべきである。

Control Title	Control ID	Control Specification
変更の復元	**CCC-09**	エラーもしくはセキュリティ上の懸念事項が発生した場合、変更した箇所を以前の正常と認識している状態にプロアクティブにロールバックするプロセスを定義し実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の実施責任は、CSP と CSC の責任共有であるが、それぞれ独立して実施する。システムに対する全ての構成変更は、それぞれの企業ポリシーに従い、業界標準に沿って、独立してベースライン化され、テストされ、承認されるものとする。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； エラーやセキュリティ上の懸念が発生した場合に、プロアクティブに変更を以前の良好な状態にロールバックする堅牢なプロセスを実装することは、CSP がクラウドサービスの安定性、セキュリティ、信頼性を維持するために不可欠である。 明確に定義されたロールバックプロセスにより、変更を迅速かつ効果的に取り消すことができ、エラーやセキュリティインシデントによる潜在的な影響を最小限に抑えることができる。変更のデプロイが失敗し、ロールバックが発生した場合は、CSC に通知する。 **全てのサービスモデルに適用：** この管理策の実施におけるベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）： a. ロールバックのベースライン i. 全ての重要なクラウドアセットのスナップショット、バックアップ、復元ポイントを含むロールバックベースラインは、既知の安定した状態で、リカバリと環境のリストアの標準点として機能する必要がある。 ii. ロールバック手順を容易にするために、詳細な変更ログと設定のバックアップを維持する必要がある。 b. ロールバックのプロセス： i. 問題が発生した場合に迅速かつ効果的に実施できるロールバックプロセスとサポート手順を確立すべきである。 ii. ロールバック手順には、ロールバックポイントの特定、ロールバックのトリガー、ロールバックの成功の検証を含めるべきである。 iii. ロールバック手順は、可能な限り自動化し、変更を戻すのに必要な時間と労力を最小限に抑えるべきである（自動化ツールを使用して、ロールバックのベースラインから構成、データ、アプリケーションを復元することができる）。 c. ロールバックのトリガー：ロールバックを開始するトリガーは、特定のエラーコード、セキュリティアラートまたは許容可能な閾値を超えるパフォーマンス低下など、定義されるべきであり、CSP のリスク許容度およびセキュリティポリシーに沿って構成可能であるべきである。 d. ロールバックのテスト戦略：ロールバック手順が効果的で	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

あり、意図したとおりに機能していることを確認するために、ロールバック手順を定期的にテストする必要がある。ステージング環境または隔離されたテスト環境を使用して、本番システムに影響を与えずにロールバックのシミュレーションを実施する。

e. ロールバック手順の文書化：ロールバックの手順は、関係する手順、使用したツール、期待される結果を含めて文書化する。

f. ロールバックと変更管理の統合：ロールバック手順を変更管理プロセスと統合し、変更実施中にロールバック計画が考慮され、ロールバックのトリガーが変更承認プロセスとの整合をとる。

g. ロールバックの履歴：ロールバックイベントの履歴（ロールバックの日時、理由、具体的な変更内容など）を保持する。この履歴データは、パターンを特定し、ロールバック手順を改善し、セキュリティ規制への準拠を実証するための貴重な洞察を提供する。

h. ロールバック手順のレビュー：ロールバック手順は、テスト結果、ロールバックイベントからのフィードバック、セキュリティ脅威の進化やクラウドインフラの変更に基づいて、定期的にレビューし、改善する必要がある。

i. ロールバックのシミュレーション演習

  i. ロールバック手順の有効性をテストし、改善点を特定するために、ロールバックのシミュレーション演習を定期的に実施する。

  ii. 変更のロールバックと修復作業を担当する専門チームを持つ。

Control Domain CEK
2.5 暗号、暗号化、鍵管理(CEK)

Control Title	Control ID	Control Specification
暗号化と鍵管理のポリシーと手順	**CEK-01**	暗号、暗号化、鍵管理のポリシーと手順を、確立、承認、適用、評価、維持すること。また、少なくとも年 1 回はポリシーと手順をレビューし更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； 各当事者による暗号、暗号化及び鍵管理ポリシーの策定は、有効なセキュリティを確立するために不可欠であることから、これは CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSP は暗号サービスを提供する必要があり、その場合、CSP はこれらのサービスをサポートするインフラストラクチャに責任を負う。一方、CSC は、例えば、いつ、どのデータを暗号化するかを選択し、暗号化鍵へのアクセスを管理するなど、データを保護するためにこれらのサービスを正しく使用する責任を負う。	**管理策所有権の根拠；** すでに説明した CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； CSP は、鍵の生成、配付、ローテーション、失効、破棄、活性化、一時停止、非活性化、アーカイブ、危殆化、復元、棚卸リスト管理、用途及びアクセスを含む暗号化および鍵管理に関する明瞭なポリシーと手順を伴う、強固な暗号管理システムを有するべきである。これらのポリシーは、少なくとも年 1 回はレビューされ、更新されるべきである。	
IaaS プロバイダー： これらの暗号化方式をいつ、どのように使用するか、誰が鍵にアクセスできるか、これらの鍵のライフサイクルをどのように管理するか、役割と責任、データ保護、変更管理、リスク管理、監視、報告、インシデント処理、及び監査について規定したポリシーと手順を整備すべきである。IaaS プロバイダーは、鍵管理サービスと共に、全てのデータに対する移動中と保存中の両方の暗号化メカニズムを提供すべきである。CSP は、これらのサービスが最新のセキュリティ標準やベストプラクティスに準拠していることを確実にすべきである。	**実施ガイドライン；** **IaaS 利用者**： CSC は、CSP が提供するインフラストラクチャ内で自身のデータの暗号化を管理するための規定をポリシーに含めることを検討すべきである。CSC は、ベストプラクティスに従い、鍵管理のために CSP が提供するツールとリソースを使用すべきである。
PaaS プロバイダー： 変更管理とリスク管理の手法を含む、これら暗号化方式及び鍵の使用と管理のためのポリシーと手順を整備すべきである。PaaS プロバイダーは、セキュアな鍵管理システムを含む、保存中および移動中のデータに対するプラットフォームレベルの暗号化を提供すべきである。CSP は、データ暗号化やアルゴリズム選択といったデータ保護手順を含め、セキュリティのベストプラクティスや標準に準拠すべきである。	**PaaS 利用者**： CSC は、プラットフォームレベルで提供される暗号化の利用を含む、CSP が提供するセキュアなプラットフォームの効果的な利用を確実とするポリシーを作成すべきである。CSC のポリシーには、CSC のニーズ及び CSP により提供されるサービスに応じて、プラットフォーム内での追加の暗号化が含まれる。
SaaS プロバイダー： アプリケーションレベルでの暗号化の取り扱い方法を規定するポリシーと手順を整備すべきであり、これには鍵管理が含まれ、鍵管理活動の全ての側面が網羅されるべきである。プロバイダーは、承認済みの暗号保護方式によって保存中及び移動中の全てのデータ	**SaaS 利用者：** CSC は、ソフトウェアレベルで提供される暗号化の利用を含む、CSP が提供するセキュアなソフトウェアサービスの効果的な利用を確実とするポリシーを作成すべきである。CSC は、CSP と協力して、ソフトウェアサービス内において鍵がどのように管理されている

が暗号化されることを確実にするべきである。CSP は、可能であればCSC に自身の鍵を管理する手段を提供し、脅威と脆弱性の出現に対応するために技術を注意深く監視すべきである。CSP は、暗号化および鍵管理プロセスについてインシデント対応手順、監査メカニズム、およびアクティビティロギングを確実なものとすべきである。	か理解し、CSC のニーズ及び遵守要件を満たすことを確実とすべきである。
ポリシーには、次のような条項が含まれるべきである（ただし、これに限定されない）： a. 範囲と目的 i. 機微データを保護するために組織が暗号、暗号化及び鍵管理を実施する範囲の定義とガバナンス ii. データセキュリティのための暗号管理策のセキュアな実装に関する目標、及び暗号化鍵を不正アクセス、改ざん、漏えいから保護するための鍵管理手法の確立に関する目標 b. 役割と責任：暗号管理策および暗号化鍵ライフサイクルの管理に関与する全てのエンティティの責任。これには、鍵の生成、配付、保管、ローテーション、破棄に関する責任も含む。 c. 暗号化標準：移動中及び保存中のデータ両方に対する、必要とする暗号化標準、アルゴリズム及びベストプラクティスを網羅した、暗号データのセキュリティと保護の要件。 d. 暗号変更管理：変更を承認できる者、変更を文書化する方法、及び変更をテスト・監査するプロセスを含む、暗号管理策および暗号化鍵管理に変更を加える手順。 e. リスク管理：暗号管理策および鍵管理に関連するリスクの特定、評価及び低減のための手順。これは CSP の広範なリスク管理フレームワークに統合されるべきである。 f. 鍵管理活動：鍵の生成、配付、ローテーション、失効、破棄、活性化、一時停止、非活性化、アーカイブ、危殆化、復元、棚卸リスト管理、用途、目的、アクセスを含む鍵管理活動に関する要求事項。 g. 監視および報告：暗号管理策及び鍵管理の実践のモニタリングと、異常や違反の可能性を含む、CSC への定期的な状況の報告。 h. 承認：組織の戦略目標及びリスク選好度との整合性を確保するための、承認要件及び上級管理職の関与 i. 承認プロセスは、ポリシーと手順のいかなる変更または修正に対しても確立されるべきである。 ii. 文書化された承認の記録（日付、承認者名及び関連するコメントや議論を含む）が維持されるべきである。 i. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的なコミュニケーションが促進されるべきである。 j. メンテナンス及びレビュー：暗号、暗号化及び鍵管理のポリシーと手順は、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制及びリスクの変化を反映するために、少なくとも年 1 回は文書化し、レビューし、更	**ポリシーには、以下に関する規定を含むべきである（ただし、これに限定されない）：** CSP に提供されるポリシーが適用される。

新すべきである。	

Control Title	Control ID	Control Specification
CEK の役割と責任	**CEK-02**	暗号、暗号化、鍵管理の役割と責任を定義して実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP は組織内における暗号の運用および鍵管理の役割と責任を定義し、実施する責任を負うことから、これは CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSC の個別のセキュリティ要求に対応するため、CSP は、これらの責務に関連する構成可能なオプションを提供することが期待される。ただし、CSP は、CSC が提示されたオプションをどのように管理するかについて管理策することはできないため、その役割は「Independent」となる。提供されるツールや機能によっては、特に SaaS のようなサービスモデルでは、CSP が CSC の役割と責任に影響を及ぼす可能性がある。	**管理策所有権の根拠；** CSC の管理策の所有も「Shared (Independent)」である。これは、CSC が、CSP の暗号運用および鍵管理オプションを適切に利用および管理するための役割と責任を特定し、実装する必要があることに起因する。CSP は不可欠なツールとオプションを提供するが、その特定のニーズと運用状況に適した役割及び運用手順を策定するのは CSC の責任である。SaaS のような特定のサービスモデルでは、CSC の役割は CSP のオプションやツールによって形成されるかもしれないが、役割と責任を定義し実施する主たる責任は CSC にある。
実施ガイドライン； **IaaS プロバイダー：** a. 鍵管理者の役割と責任を定義し徹底することにより、鍵管理者が保護されたデータや暗号化エンジンにアクセスできないことを確実にする。同時に、強固なアクセス管理策及び役割の定義能力を CSC に提供する。これには、CSC が SoD の原則や知識分割 (split knowledge) を実装できるようにすることも含む。 b. SoD 知識分割、最小権限アクセスといったプラクティスを暗号リソースおよび暗号プロセスに組み入れる。 c. 運用中の鍵情報およびバックアップされた鍵情報の保管と回復の管理について、明確なポリシーを確立する。暗号利用期間の定義、鍵と電子証明書の棚卸リストの監督、及び使用前の保管鍵情報の完全性の検証においてカスタマーを支援する。危殆化した鍵を失効させ、代替の鍵ま	**実施ガイドライン；** **IaaS カスタマー：** a. システム内の暗号鍵管理に関する、明確に定義された役割と責任を確立する。これには、CMK を使用する場合の仮想マシンおよびアプリケーションレベルでの独自の鍵管理などの職務を含む。 b. CSP によって提供されるアクセス管理策及び役割の定義能力を効果的に活用するための職務を定義し、SoD 及び知識分割の原則の適切な実装を図る。 c. セキュアな暗号鍵の運用（生成、配付、失効、破棄）に関する責任を定義する。 d. 鍵のセキュアな配付、鍵および電子証明書の有効なインベントリ管理、危殆化した鍵の失効および交換の仕組みの確立のために、CSP と連携するタスクを定義する。

たは電子証明書を作成するプロセスを管理する。これらのプロセス全体を通じて透明性を維持する。 d. プライベート鍵、秘密鍵およびメタデータのセキュアな配布を含む、鍵の保管と管理のためのセキュアなソリューションを提供し、また、暗号化鍵をセキュアに生成、失効、破棄する能力をカスタマーに提供する。	e. CMK を使用する場合、仮想マシン及びアプリケーションレベルにおける、独自の鍵の生成、ローテーション、管理などの責任を定義する。 f. 保存されている鍵情報の完全性チェックを定期的に行う。
PaaS プロバイダー： a. 鍵管理システムの役割と責任を定義する。これには、運用上の全ての CKMS の役割に責任を持つポリシー権限者と、IT エグゼクティブへの報告も含まれる。 b. 暗号化および鍵管理をプラットフォームレベルで管理し、暗号鍵への不正アクセスを防ぐためにランタイム環境を保護し使用中の鍵を保護する。 c. アーカイブされた鍵情報の保管と復元、および保管された鍵情報の完全性チェックに関するポリシーを確実に実施する。 d. データ、アプリケーション、トランザクションの各レイヤーで暗号化ソリューションを提供し、必要に応じて CSC が独自の暗号化ソリューションを実装することをサポートする。	**PaaS カスタマー：** a. アプリケーションレベルでの暗号化と鍵管理の役割と責任を確立する。 b. CSP が提供するソリューションを活用し、使用中の鍵を保護するために要求される追加のセキュリティ対策を実装するために、責任を割り当てる。これには、ハードウェアセキュリティモジュール（HSM）、KMS、シークレット管理、または鍵の保管および使用に関するセキュアな手法の利用を含む。 c. CSP が提供するロギングおよびモニタリング能力を使用し、鍵の危殆化インシデントを迅速に検出し、対応する責任を定義する。 d. CSP と連携してプラットフォームレベルのセキュリティ対策を理解し、アプリケーションレベルの暗号化と鍵管理の要件が満たされていることを確実にする責任を定義する。 e. CMK を使用する場合、独自の鍵の生成、ローテーション、管理などの責任をアプリケーションレベルで定義する。
SaaS プロバイダー： a. ソフトウェアまたはアプリケーションの暗号化構成を設定および変更できる者を含む、スタック全体にわたる役割と責任を定義する。 b. 保存中、移動中及び使用中の CSC データに強固な暗号化および鍵管理の慣行を実装し、これらの慣行に関する透明性を提供する。 c. 可能であれば、CSC が独自の暗号化鍵を管理できるようなオプション（例：BYOK）を提供し、CSC がこれらのオプションをセキュアに実装できるようサポートする。 d. 運用中の鍵情報およびバックアップされた鍵情報の保管と復元の管理ルールを確立する。	**SaaS カスタマー：** a. 保存中、移動中、および使用中カスタマーデータに対する CSP の暗号化および鍵管理の手段を理解し、合意することを確実とする。 b. オプションが利用可能な場合は、独自の暗号鍵を管理する役割を検討する（BYOK など）。これには、SaaS アプリケーションで使用する、独自の鍵の生成、ローテーション及び管理を含む。 c. 鍵への不正アクセスまたは変更を防止するために CSP が鍵管理の役割を明確に定義し分離していることを検証する職務を委任する。
全てのサービスモデルに適用： a. 鍵の生成、配付、暗号利用期間の設定、鍵の失効、保管と復元、完全性チェック、及び不要になった鍵の破棄を含む、鍵のライフサイクルの責任を定義し、それに従う。 b. コンプライアンスを確保し、職務分掌、役割、責任の有効性をチェックするために、定期的な監査とレビューを実施する。	

Control Title	Control ID	Control Specification
データ暗号化	**CEK-03**	業界標準に認定された暗号化ライブラリを使用して、保存中および移動中のデータを暗号化する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	CSC
管理策所有権の根拠； IaaS、PaaS、および SaaS といったサービスデリバリモデルの文脈において、CSP は、認証された暗号ライブラリを使用して、保存中および移動中のデータを管理し、暗号保護を提供する第一の責任を負う。CSP と CSC の両者で「互いに依存する形で共有」し、それぞれ実施する責任がある。管理策の実装は CSC にも依存するため、共有責任ではあるが依存関係のある責任となる。	**管理策所有権の根拠；** 保存中のデータと移動中のデータの両方の暗号化の管理策の所有は、CSP と CSC の間に Dependent され Shared される。CSP が暗号ツールとライブラリを提供する一方、CSC は適切なデータ保護レベルを確保するために、これらのツールを正しく実装し使用する責任を負う。
実施ガイドライン； この対策は、機微情報を保存中および移動中の不正アクセスから保護することにより、セキュリティポスチャを強化するものである。承認された標準に認定された暗号ライブラリを使用することにより、暗号化に関する業界の標準を満たし、データの機密性と完全性に関して CSP と CSC の双方に信頼を与えることで、保証のレイヤーを追加する。	**実施ガイドライン；** CSC の観点からは、認証されたライブラリを使用した保存中および移動中のデータの暗号保護により、クラウド環境内での機微情報の機密性と完全性が保証される。この管理は、CSP が実施するセキュリティ対策と、潜在的なセキュリティ脅威に対する CSC のデータ保護について、CSC に保証を提供する。
IaaS プロバイダー： a. CSP は、FIPS 検証またはその他の関連する国際標準化機関の承認を満たすか、それを上回るセキュアな CKMS を維持すべきである。 b. 保管中のデータベースとファイルサーバーのフルディスク暗号化オプションと、移動中（ネットワーク）のデータの暗号化オプションを提供し、CSC が必要に応じて実装できる仕組みを提供する。 c. TLS などのセキュアなネットワーク通信プロトコルを提供して、仮想マシン、CSP サービス、およびユーザー間の移動中のデータを保護する。 d. これらの暗号サービスをサポートする基盤インフラストラクチャのセキュリティを維持する。 e. CSP による改ざんを含め、データ暗号化鍵を流出や改ざんから保護された環境でセキュアに保管するための仕組	**SaaS 利用者：** a. データベースやファイルを含む使用中のデータについて、保存中および移動中のデータが暗号化されていることを確実にし、信頼された実行環境（Trusted Execution Environments：TEE）を使用する。これには、適切な暗号化レベルの選択、フルディスク暗号化の有効化、特定のデータ構造の暗号化、機微データに対する暗号化の使用、及び暗号化鍵の管理を含む。 b. システムインターフェース、公共ネットワーク、電子メッセージング（電子メール、ビデオ、音声など）を含む、移動中のデータが暗号化されることを確実にする。TLS などの業界で認められている強力な暗号を使用したセキュアなネットワーク通信プロトコルを使用する。 c. セキュアな生成、配付、ローテーション、失効、破棄

みを提供する。	を含め、暗号化鍵をセキュアに管理する。 d. データ暗号化鍵を、信頼された実行環境のような保護された環境で、CSP の要員を含め、流出や改ざんからセキュアに保管するための仕組みを利用すべきである。
PaaS プロバイダー： a. IaaS について記載した責任に加えて、CSP は、保存中、使用中、および移動中のデータについて、プラットフォームレベルの暗号化オプションを提供すべきである。これには、さまざまなデータ構造やタイプ（ファイル、レコード、フィールドなど）を暗号化するオプションを含めるべきである。 b. 適切な暗号化アルゴリズムの選択を含む、CSC に暗号化構成を管理する能力を提供する。	**PaaS 利用者：** a. IaaS で述べたこととは別に、CSP と協力してプラットフォームレベルの暗号化オプションを理解し、データベース内のデータを保護するためのデータベース暗号化機能など、適切に設定する。 b. CSP によって提供される方法を使用して、アプリケーションレベルの暗号化鍵をセキュアに管理し、CSP による鍵へのアクセスを防止する。 c. 提供される API や SDK を活用して、アプリケーションに暗号化を実装する。
SaaS プロバイダー： a. IaaS と PaaS に記載されている責任以外にも、カスタマーデータが保存中及び移動中の両方で暗号化されていることを確実とする。 b. エンドユーザーのワークステーションとインタフェースが、および移動中のデータ暗号化によって保護されていることを確実にする。 c. エンドツーエンドの暗号化オプションを提供し、データの発生場所から使用場所まで暗号化された状態を維持する。 d. 使用中のデータが暗号化された信頼された実行環境のような、エンドツーエンドの暗号化オプションを提供する。 e. 暗号化鍵はセキュアに管理され、定期的にローテーションされ、許可されていない者に暴露されないようにする。CSP はまた、ソフトウェアサービス内で鍵の生成、ローテーション及び失効を含む、CSC が暗号鍵を管理するためのセキュアな方法を提供すべきである。	**SaaS 利用者：** a. 暗号化が必要なデータを特定し、分類する。 b. 保存中のデータと移動中のデータの両方で暗号化が有効かつ適切に設定されていることを確実とする。ビジネス要件に応じて、必要に応じてエンドツーエンドの暗号化を含めることができる。CKMS サービスは、効率的な管理のために活用することができる。 c. CSP が CSC マネージド鍵を許可している場合、セキュアな鍵管理方法を確実に実装する。これには、セキュアな鍵の生成、ローテーション、失効を含む。

Control Title	Control ID	Control Specification
暗号化アルゴリズム	**CEK-04**	データの分類、関連するリスク、および暗号化技術の使いやすさを考慮して、データ保護に適した暗号化アルゴリズムを使用する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； 暗号化アルゴリズムの管理策所有権は、「互いに依存しない形で共有」である。CSP は、堅牢なデータ保護を確実とするために、そのインフラストラクチャに適切な暗号化アルゴリズムを決定し実装する第一の責任を負う。CSP はこのタスクを実行するための専門知識とインフラストラクチャへのアクセス権を有するが、CSP の暗号化サービスを選択し、ビジネス要件、ベストプラクティス、および許容される業界標準に従って実装することは CSC の責任である。	**管理策所有権の根拠；** CSC は暗号化アルゴリズムの選択について独立した管理策を共有する。CSP が暗号能力を提供する一方で、CSC は、特定のデータの分類、関連するリスク、およびビジネス要件に基づいて、これらの暗号化サービスを適切に選択し使用する責任を負う。
実施ガイドライン； **全てのサービスモデルに適用：** CSP は、データの分類、関連リスク、および暗号化技術の使いやすさを考慮し、データ保護に最適な暗号化アルゴリズムを実装する責任を負う。 CSP は以下のようにあるべきである： a. 様々な種類のデータ保護に適したアルゴリズムを使用する暗号化サービスを提供する。これらのアルゴリズムは、業界の最新のベストプラクティスや標準と一致しているべきである。 b. 使用する暗号ライブラリが、FIPS 140-2 などの承認された標準に準拠していることを確実にする。 c. 使用される暗号化アルゴリズム、その長所と短所、及び適したデータの種類とリスクについて、CSC に明確かつ透明性をもって伝達する。 d. 暗号化技術の発展と暗号化セキュリティへの脅威を継続的に監視する。これには、新たな脆弱性に対応して暗号化サービスをアップグレードすることや、よりセキュアな新しいアルゴリズムが利用可能になった場合にそれを採用することを含む。 e. 適切な鍵サイズとアルゴリズムの種類を決定する際、データに対するリスクのレベルや費用対効果分析などの要因を考慮したリスクベースアプローチを採用する。 f. 最低限のセキュリティ標準を確保しつつ、アプリケーションの要件に応じて暗号化アルゴリズムを選択できる柔軟性を開発者に提供する。 g. CKMS のセキュリティポリシーが、全ての鍵のアルゴリズム、メタデータの機密性、完全性、可用性、およびソース認証を保護することを確実とする。	**実施ガイドライン；** **全てのサービスモデルに適用：** CSC は、以下のようにあるべきである： a. 利用可能な暗号化アルゴリズムとその適切なユースケースなど、CSP が提供する暗号化サービスを熟知する。 b. 機密性の高いデータほど強力な暗号化が必要であることを理解し、データの分類に基づいて適切な暗号化サービスを選択する。 c. 暗号化アルゴリズムを選択する際には、関連するリスクを考慮する。これには、データ漏洩の潜在的な影響を理解し、必要な暗号化レベルについて十分な情報を得た上で決定することが含まれる。 d. 選択した暗号化サービスが、関連する全てのコンプライアンス要件を満たしていることを確実にする。これには、暗号化サービスの使用のレビュー及び更新を含む、データ保護に関する業界固有の要件が含まれる場合がある。また、暗号化技術の発展や暗号化セキュリティに対する脅威について常に情報を入手し、それに応じて暗号化サービスの使用を調整することも含まれる。 e. 暗号化サービスを理解し使用するために、CSP が提供するあらゆるサポートを利用する。これには、文書、カスタマサポート、およびトレーニングリソースの活用を含む。

Control Title	Control ID	Control Specification
暗号化の変更管理	**CEK-05**	内的要因と外部要因からの変更に対応するための標準的な変更管理手順を確立する。 変更管理手順には暗号、暗号化および鍵管理に関する技術変更についてのレビュー、承認、実装、コミュニケーションが含まれる。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Dependent)	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； IaaS モデルでは、CSP が暗号化と鍵管理のためのプラットフォームを提供する。CSP は、基盤となるハードウェアやネットワークインフラストラクチャを含むクラウドインフラストラクチャの変更を監督し、独立して管理する。この独立した変更管理手続により、CSP と CSC 両者で「依存しない形で共有」し、それぞれ独立して実施する責任がある。 PaaS モデルでは、CSP は暗号処理が実行され、暗号材料が公開されるプラットフォームを提供する。プラットフォームに関する変更は CSP が行うが、変更管理プロセスには CSC のアプリケー ションレイヤとのやり取りが発生するため、依存関係が生じる。その結果、CSP と CSC 両者で「依存する形で共有」し、それぞれ実施する責任があるカテゴリに分類される。 SaaS モデルでは、CSP は、暗号化と鍵管理を含む完全なソフトウェアソリューションを提供する。したがって、CSP は、暗号処理を含むソフトウェアサービスの変更管理に全責任を負い、CSP で「CSP が所有」し、自ら実施責任がある。	**管理策所有権の根拠；** IaaS の場合、CSC は提供されたインフラストラクチャ上での暗号化と鍵管理の責任を負う。仮想マシンやアプリケーションレベルでの暗号方式や鍵に対する変更は、CSC が独自に行う。この結果、「Shared (Independent)」管理策の所有となる。 PaaS モデルでは、CSP がプラットフォームを提供し管理する一方で、CSC はそのプラットフォーム上にアプリケーションを実装する。アプリケーションレベルでの暗号化と鍵管理の変更は、提供されるプラットフォームとのやり取りを必要とし、CSC と CSP の相互依存につながる。したがって、管理策所有権は「(依存する形で) 共有」に分類される。 しかし、SaaS モデルでは、CSC は主に CSP が提供するソフトウェアサービスを利用する。暗号処理に対する変更は一般的に、暗号化および鍵管理に関連する変更も含め CSP によって管理される。したがって、この文脈における管理策の所有は「CSP が所有」とみなされる。
実施ガイドライン； **全てのサービスモデルに適用：** 実施ガイドラインには、以下が含まれるべきである（ただし、これに限定されない）： a. 暗号、暗号化および鍵管理技術の変更に対応するための標準的な変更管理手順を確立する。これには、内部レビューに起因する変更だけでなく、規制要件や業界標準の変更などの外部要因も含む。	**実施ガイドライン；** **IaaS 利用者：** a. システムおよびアプリケーションで使用する暗号、暗号化および鍵管理技術について、独自の変更管理手順を確立する。 b. セキュリティ及びコンプライアンスへの潜在的影響を考慮し、実装前に変更をレビューし、承認する。 c. 変更文書に、変更の理由、期待されるメリット、及び

b. セキュリティとコンプライアンスへの潜在的影響を考慮し、実装前に変更を徹底的にレビューし、承認する。 c. 変更管理手順の中に、変更の理由や期待される効果を含め、全ての変更を文書化する規定を設ける。この文書には、暗号化において新たに実装された変更に何らかのリスクや脆弱性が発見され、変更を取り消す必要が生じた場合のロールバック計画も含める。 d. ソフトウェアやシステムに対する不正な変更を防止し、不正な変更が検出された場合にシステムをセキュアな状態に回復するためのメカニズムを実装する。 e. 変更が正しく実装され、新たなセキュリティリスクが発生していないことを検証するために、セキュリティ監査を実施する。 f. 全ての監査結果をシステム当局に報告し、特定された問題に速やかに対処する。 g. 暗号及び鍵管理ライフサイクルに何らかの変更が生じた場合、CSC とコミュニケーションする。	ロールバック計画を含める。 d. 不正な変更がないかシステムを監視し、必要に応じてシステムを復旧させる準備をする。 **PaaS 利用者：** a. IaaS と同様、アプリケーションの変更管理手順を確立する。 b. アプリケーションに影響を及ぼす可能性のあるプラットフォームの暗号、暗号化および鍵管理テクノロジーの変更を CSP と連携して理解する。 **SaaS 利用者：** a. 暗号に関する設定を含め、SaaS アプリケーションで利用可能な設定を理解し、管理する。 b. CSP と緊密に連携し、アプリケーションの使用に影響を与える可能性のある CSP の変更を理解する。 c. CSP による変更に応じて、必要に応じて設定を見直し、変更を実施する手順を用意する。

Control Title	Control ID	Control Specification
暗号化の変更による費用対効果分析	**CEK-06**	残留リスク、コスト、および利益の分析など、提案された変更の下流への影響を十分考慮し、暗号、暗号化、鍵管理関連のシステム（ポリシーと手順を含む）への変更を管理及び採用する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともに、暗号および鍵管理関連システムの変更を管理し、採用する責任を負うため、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSP は、プラットフォームマネージド鍵に対して、この管理策を所有する。	**管理策所有権の根拠；** CSP と CSC はともに、暗号および鍵管理関連システムの変更を管理し、採用する責任を負うため、この管理策について独立した共有責任を有する。CSC は、クライアントマネージド鍵（CMK）に対して、この管理策を所有する。
実施ガイドライン；	**実施ガイドライン；**

全てのサービスモデルに適用： CSP は、暗号および鍵管理関連システムに対する全ての変更が適用されるセキュリティ要件に基づいていることを確実にすべきであることから、管理策の実装はサービスデリバリモデル（IaaS、PaaS、SaaS）に依存しない。 実施ガイドラインには、以下を含めるべきである（ただし、これに限定されない）： a. 全ての鍵管理関連システムの変更について、主要な変更管理の費用対効果分析／投資対効果 （ROI）を計算すべきである。 b. 全ての分析は、残留リスクを含め、提案された変更による下流への影響を十分に考慮すべきである。 c. 全ての分析はレビューされ、承認されるべきである。 d. 定期的に、あるいは変更後に、予想 ROI と実際の ROI を比較する。 e. 計画された ROI からの著しい逸脱は監査されるべきである。 f. 全ての監査結果をシステム当局に報告する。	**全てのサービスモデルに適用：** CSC は、暗号及び鍵管理関連システムに対する全ての変更が、適用されるセキュリティ要件に従っていることを確実にすべきであることから、管理策の実装はサービス・デリバリー・モデル（IaaS、PaaS、SaaS）に依存しない。 CSP に提供される実施ガイドラインが適用される。

Control Title	Control ID	Control Specification
暗号化リスク管理	**CEK-07**	リスク評価、リスク対応、リスクコンテキスト、監視、フィードバックの規定を含む暗号化と鍵管理リスクプログラムを確立及び維持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともにこの管理策に対して独立した責任共有である。ここでは、エンタープライズリスクプログラムを通じて暗号化および鍵管理が維持される。CSP は、プラットフォームマネージド鍵に対して、この管理策を所有する。	**管理策所有権の根拠；** CSP と CSC はともに、エンタープライズリスクプログラムを通じて暗号化および鍵管理が維持される管理策について、独立した共有責任を有する。CSC は、クライアントマネージド鍵（CMK）に対して、この管理策を所有する。

実施ガイドライン； **全てのサービスモデルに適用：** CSP は、エンタープライズリスクプログラムを通じて、暗号化および鍵管理が維持されるようにすべきであることから、管理策の実装はサービスデリバリモデル（IaaS、PaaS、SaaS）に依存しない。 鍵リスク管理とは、鍵管理のガバナンス、組織、インフラストラクチャ及び活動に対するリスクを管理するプロセスである。 a. 不正な開示、改ざん、破壊、情報損失のリスクを評価する。 b. 暗号利用期間の選択について、情報漏えいのリスクと結果を考慮する。 c. 手動鍵配付と自動鍵配付のトレードオフについて評価する。 d. 危殆化した鍵のリスクは、以下のように軽減する： i. そのような鍵を新たな暗号化活動に使用しない。 ii. 以前にこの鍵によって復号された材料を復号するためにのみ鍵を使用する。 e. リスク評価に合わせて監査範囲と頻度を調整する。 f. 情報漏えいのリスクに比例したアルゴリズム強度を適用する。 g. 鍵の復元を検討する際に、事業継続のリスクと重要なデータ漏えいのリスクを比較評価する。	**実施ガイドライン；** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
CSC の鍵管理機能	**CEK-08**	CSP は CSC がデータ暗号鍵を管理できる機能を適用しなければならない。

Control Ownership by Service Model		
IaaS	PaaS	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともにこの管理策の依存関係のある責任共有である。CSP は CSC が自身のデータ暗号化鍵を管理する能力を提供する。	**管理策所有権の根拠；** CSP と CSC はともに、この管理策について依存的な共有責任を有し、CSC は CSP のデータ暗号化鍵管理能力を利用する。

実施ガイドライン； **全てのサービスモデルに適用：** CSP は、サービスデリバリモデルを問わず CSC が自身のデータ暗号化鍵を管理する能力を提供することから、管理策の実装はサービスデリバリモデル（IaaS、PaaS、SaaS）に依存しない。 鍵管理能力とは、CSC が所有または生成した暗号化鍵を管理する手段を CSP が CSC に提供するプロセスである。 a. CSC と CSP は、CSC が管理する鍵の定義及び範囲について合意し、SLA、適用される契約、ポリシーと手順において文書化（責任共有）すべきである。 b. CSP は、CSC がポリシー、手順及びプロセスを管理できるようにすべきである。 c. CSP は、CSC が鍵およびデータ暗号化鍵を管理するための手段を提供すべきである。 d. CSP は、データ鍵の暗号化に使用される鍵暗号化鍵またはマスター鍵を CSC が管理できるようにすべきである。 e. CSP は、CSC による鍵管理システムの使用（トランザクション、報告など）を許可すべきである。 f. オプションとして、CSC は BYOK メカニズムを使用した、CSC が生成したマスター暗号化鍵の能力を提供すべきである。	**実施ガイドライン；** **全てのサービスモデルに適用：** CSC は自身のデータ暗号化鍵を管理する CSP の能力を利用するため、管理策の実装はサービスデリバリモデル（IaaS、PaaS、SaaS）に依存しない。 鍵管理能力とは、CSC が所有または生成した暗号鍵を管理する手段を CSP が CSC に提供するプロセスである。 a. CSC と CSP は、CSC が管理する鍵の定義及び範囲について合意し、SLA、適用される契約、ポリシーと手順において文書化（責任共有）すべきである。 b. CSC は、鍵およびデータ暗号化鍵を管理するために CSP の能力を活用すべきである。 c. CSC は、データ鍵の暗号化に使用される鍵暗号化鍵またはマスター鍵を管理するために、CSP の能力を活用すべきである。 d. CSP は、CSC による鍵管理システムの使用（トランザクション、報告など）を許可すべきである。 e. オプションとして、CSC は SLA に従い BYOK メカニズムを使用して、CSC が生成したマスター暗号化鍵を供給すべきである。

Control Title	Control ID	Control Specification
暗号化と鍵管理の監査	**CEK-09**	暗号化および鍵管理システム、ポリシー、およびプロセスを、システムのリスクレベルに比例する頻度で監査する。監査は、できれば継続的に、ただし少なくとも年 **1** 回実施し、またセキュリティイベントの後にも実施すること。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠； CSP と CSC は、暗号化および鍵管理のシステム、ポリシー及びプロセスの監査を確実に実施するべきであることから、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； **全てのサービスモデルに適用：** 暗号化および鍵管理システム、ポリシー、プロセスの監査は全てに適用されることから、管理策の実装はサービスデリバリモデル（IaaS、PaaS、SaaS プロバイダー）に依存しない。 鍵の監査とは、暗号鍵の使用と保護に関する、組織、ガバナンス、インフラストラクチャ、ポリシー、手順および活動を評価するプロセスである。 a. 監査は、鍵管理ポリシーと手順の遵守状況を評価するために使用されるべきである。 b. 監査は、鍵管理管理策および管理策環境のデザインと有効性の評価に使用されるべきである。 c. 監査は、業界および規制標準（例：HIPAA、PCI）への準拠を評価するために使用されるべきである。 d. 監査結果は、鍵管理システム当局に報告されるべきである。 e. 監査は、鍵管理ポリシーおよびリスク管理ポリシーに従って実施されるべきである。 f. CSP は、サードパーティーの監査／認証報告書を要求し、サードパーティーベンダー／CSP と共に問題を検討するべきである。 g. 少なくとも、機微な監査情報や機微な監査ツールは、被監査情報と同じセキュリティ要件に従って取り扱われるべきである。	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
鍵の生成	**CEK-10**	業界で認められている暗号化ライブラリを使用し、使用するアルゴリズムの強度と乱数ジェネレーターを指定して暗号鍵を生成する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともに、業界で認められている暗号ライブラリを使用して暗号鍵を生成する必要があることから、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； **全てのサービスモデルに適用：** CSP と CSC はともに、業界で認められた暗号ライブラリを使用して暗号鍵を生成する必要があることから、管理策の実装はサービスデリバリモデル（IaaS、PaaS、SaaS）に依存しない。 鍵の生成プロセスは暗号学的にセキュアであるべきである。 a. 鍵は、セキュアな乱数ビット生成器（RBG）及び場合によってはその他のパラメータを使用して生成されるか、またはこの方法で生成された鍵に基づいて生成されるべきである。 b. 鍵管理技術およびプロセスは、IST FIPS により検証済みであるべきである。 c. 全ての関連する移行／活動は、CKMS に記録（ログ）されるべきである。	**実施ガイドライン；** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
鍵の目的	**CEK-11**	それぞれの目的毎に暗号シークレットと秘密鍵を配布し、管理する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともに、クライアントが利用可能または選択したリソースおよび鍵所有モデルの範囲に応じて、CSP と CSC の両	**管理策所有権の根拠；** CSP と CSC はともに、クライアントが利用可能または選択したリソースおよび鍵所有モデルの範囲に応じて、この管理策につ

者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSP は、プラットフォームマネージド鍵に対して、この管理策を所有する。	いて独立した共有責任を負う。 CSC は、クライアントマネージド鍵（CMK）に対して、この管理策を所有する。 • IaaS 利用者：CMK モデル • PaaS 利用者：該当する場合は CMK • SaaS 利用者：利用可能な場合は CMK モデル
実施ガイドライン； **全てのサービスモデルに適用：** 鍵配付は、論理的または物理的に鍵を配送するプロセスである。 a. 非対称鍵ペアは、セキュアな鍵生成プロセスを用いて、理想的には HSM のようなセキュアな環境で、生成されるべきである。 b. プライベート鍵は、強力な暗号化及びアクセス・管理策を用いて保護し、許可されたユーザーのみがアクセスできるようにすべきである。 c. 公開鍵は改ざんやすり替えから保護されるべきである。 d. 共通鍵もまた、セキュアな鍵生成プロセスを用いて生成され、強力な暗号化によって保護されるである。 e. 共通鍵はセキュアな経路を使用して配付され、また許可されたユーザーにのみ使用を制限するためのアクセス・管理策を備えているべきである。 f. 共通鍵は、漏えいのリスクを最小限にするため、定期的に変更すべきである。 g. 鍵は、保存中、移動中、使用中を含むライフサイクルの全ての段階で保護されるべきである。 h. 鍵配付管理策は、鍵にアクセスする正当な権限を有する当事者のみに鍵が配付されることを確実にすべきである。 i. 鍵配付管理策は、配送中の改ざん、すり替え、傍受からも保護すべきである。 j. 鍵配付はまた、許可されたユーザーが必要なときにいつでも鍵を利用できることを確実にすべきである。 k. 全ての鍵配付活動は、CKMS または棚卸リスト管理システムにロギングされ、登録されるべきである。	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
鍵のローテーション	**CEK-12**	計算された暗号化期間に従って暗号化鍵をローテーションする。これには情報開示のリスクと法的要件及び規制要件を考慮するための規定が含まれる。

Control Ownership by Service Model		
IaaS	PaaS	**SaaS**

Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともに、クライアントが利用可能または選択したリソースおよび鍵所有モデルの範囲に応じて、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSP は、プラットフォームマネージド鍵に対して、この管理策を所有する。	**管理策所有権の根拠；** CSP と CSC はともに、クライアントが利用可能または選択したリソースおよび鍵所有モデルの範囲に応じて、この管理策について独立した共有責任を負う。 CSC は、クライアントマネージド鍵（CMK）に対して、この管理策を所有する。 • IaaS 利用者：CMK モデル • PaaS 利用者：該当する場合は CMK モデル
実施ガイドライン； **全てのサービスモデルに適用：** 鍵をローテーションする前に、過去に旧版の鍵で暗号化された全てのデータが復号できることを確実にする。組織のポリシーおよびシステムの技術能力に応じて、鍵のローテーション後に、古いデータを新版の鍵で自動的にまたは手動で再暗号化することがある。 鍵をローテーションさせる際は、以下の原則を考慮する： a. データの復号：新しい鍵でデータを再暗号化する前に、非プライマリ（古い）鍵を使用して、以前に暗号化されたデータを復号すべきである。 b. データの再暗号化：古いデータは、組織のポリシーと技術能力に基づいて、新しい鍵を使用して再暗号化することができる。 c. アルゴリズムの強度：これには暗号化アルゴリズムの強度、鍵長、使用される運用モードが含まれる。 d. トランザクション量：鍵のローテーションに要する処理時間や、鍵のローテーションが必要な頻度に影響を与える可能性のある情報流量またはトランザクション数。 e. データの機密性とライフタイム保護：これには、データを保護する必要がある期間、データの機密性、及びデータの漏えいに関連する潜在的なリスクを含む。 f. 暗号セキュリティ機能：データ暗号化、デジタル署名、鍵保護などの機能は、鍵のローテーションによって影響を受ける可能性があり、考慮すべきである。 g. 鍵のコピー数：鍵のコピー数およびそれらコピーの配付を管理し、ローテーションプロセス中に全ての関連する鍵のコピーが更新されることを確実にする。 h. 鍵のローテーションの記録：鍵のローテーション活動は全て、CKMS または棚卸リスト管理システムにロギングさ	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

れ、登録されるべきである。	

Control Title	Control ID	Control Specification
鍵の失効	**CEK-13**	暗号鍵が侵害された場合、又は、エンティティが組織の一部ではなくなった場合、設定された暗号化期間の終了前に暗号鍵を取り消し、削除するためのプロセス、手順、および技術的手段を定義、実装、および評価する。 なお、これには法的及び規制上の要件の規定を含む。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともに、クライアントが利用可能または選択するリソースおよび鍵所有モデルの範囲に応じて、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSP は、プラットフォームマネージド鍵に対して、この管理策を所有する。	**管理策所有権の根拠；** CSP と CSC はともに、クライアントが利用可能または選択するリソースおよび鍵所有モデルの範囲に応じて、この管理策について独立した共有責任を負う。CSC は、クライアントマネージド鍵（CMK）に対して、この管理策を所有する。
実施ガイドライン； **全てのサービスモデルに適用：** 鍵失効は、有効期限を迎える前に鍵を運用利用から外すことである。 a. 共通鍵の失効は、その鍵材料の使用を制限する。 b. 非対称鍵の失効は、特にプライベート鍵の失効を指す。 c. 緊急失効は、鍵の紛失や漏えいを指す。 d. 失効ステータスは、鍵に依拠した全ての人が利用できるようにすべきである。 e. デジタル証明書失効リスト（CRL）またはその他の関連するメカニズムを使用して、利害関係者に通知すべきである。 f. ROI:相当数の鍵保有者がいる大規模な分散データベース	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

を復号し、再度暗号化するためのコスト。適用可能な場合、鍵の失効による影響を最小限に抑えるために、データを暗号化する鍵と、データを暗号化する鍵を暗号化するための別の鍵を使用する二重の鍵システムを使用すべきである。 g. ROI:長期暗号利用期間のリスクと短期暗号利用期間のリスク、および1つの鍵で暗号化されるデータ量。 h. 全ての関連する遷移／活動は、CMKSまたは棚卸リスト管理システムに登録（ログ）されるべきである。	

Control Title	Control ID	Control Specification
鍵の破棄	**CEK-14**	必要が無くなった場合、外部のセキュアな環境に保存されている暗号鍵の破棄、及び、ハードウェアセキュリティモジュール（HSM）に保存されている暗号鍵を無効化とするための、プロセス、手順、および技術的手段を定義、実装、および評価する。なお、これには法的及び規制上の要件の規定を含む。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともに、クライアントが利用可能または選択するリソースおよび鍵所有モデルの範囲に応じて、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSPは、プラットフォームマネージド鍵に対して、この管理策を所有する。	**管理策所有権の根拠；** CSP と CSC はともに、クライアントが利用可能または選択するリソースおよび鍵所有モデルの範囲に応じて、この管理策について独立した共有責任を負う。CSCは、クライアントマネージド鍵（CMK）について、この管理策を所有する。
実施ガイドライン； **全てのサービスモデルに適用：** 鍵の破棄は、物理的または電子的手段による復元を防ぐため、全ての痕跡を削除する。 a. 鍵が破棄される際、全ての鍵のコピーが破棄されるべきである。 b. 漏えいのリスクを最小限に抑えるため、鍵は不要になった時点で破棄されるべきである。 c. シークレットおよびプライベート鍵は、いかなる手段に	**実施ガイドライン；** **全てのサービスモデルに適用：** 鍵の破棄は、物理的または電子的手段による復元を防ぐため、全ての痕跡を削除する。 a. 鍵が破棄される場合、全ての鍵のコピーが破棄されるべきである。 b. 漏えいのリスクを最小限に抑えるため、鍵は不要になった時点で破棄すべきである。 c. シークレットおよびプライベート鍵は、いかなる手段

よっても復元できないように破棄すべきである。 d. 公開鍵は保持または破棄される。 e. 鍵の破棄を事前に利害関係者に通知する。 f. 鍵及び／又はメタデータに関する、法律、規制及びそれらの保持要件を考慮する。 g. 鍵復元情報（KRI）は、不正な開示や破棄から保護されるべきである。 h. 全ての関連する遷移／活動は、CMKS または棚卸リスト管理システムに登録（ログ）されるべきである。	によっても復元できないように破棄すべきである。 d. プライベート鍵は常に破棄すべきであるが、公開鍵は保持または破棄される。 e. 鍵の破棄を事前に利害関係者に通知する。 f. 鍵及び／又はメタデータに関する、法律、規制及びそれらの保持要件を考慮する。 g. KRI は、不正な開示や破棄から保護されるべきである。 h. 全ての関連する遷移／活動は、CMKS または棚卸リスト管理システムに登録（ログ）されるべきである。

Control Title	Control ID	Control Specification
鍵のアクティベーション	**CEK-15**	暗号鍵が生成されたが使用が許可されていない場合、事前にアクティベートされた暗号鍵を作成するための、プロセス、手順、および技術的手段を定義、実装、および評価する。なお、これには法的及び規制上の要件の規定を含む。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともに、クライアントが利用可能または選択するリソースおよび鍵所有モデルの範囲に応じて、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSP は、プラットフォームマネージド鍵に対して、この管理策を所有する。	**管理策所有権の根拠；** CSP と CSC はともに、クライアントが利用可能または選択するリソース及び鍵所有モデルの範囲に応じて、この管理策について独立した共有責任を負う。CSC は、カスタママネージド鍵（CMK）に対して、この管理策を所有する。
実施ガイドライン； **全てのサービスモデルに適用：** アクティベートされた鍵は、情報を暗号学的に保護するために使用される。 a. アクティベート前の鍵は、有効期間/暗号利用期間の開始日を入力することでアクティベートされる。 b. アクティベートされていない鍵は、データを暗号化する準備ができていない。 c. アクティベートされていない鍵は、所持証明または鍵確認の実行にのみ使用すべきである。 d. アクティベート前の鍵が不要になった場合、破棄される	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

べきである。 e. ある鍵の完全性に疑義がある場合、その鍵は危殆化状態に遷移されるべきである。 f. 全ての関連する遷移／活動は、CKMS または棚卸リスト管理システムに（ログ）されるべきである。	

Control Title	Control ID	Control Specification
鍵の使用停止	**CEK-16**	暗号鍵が、ある状態から使用停止状態、または、使用停止状態から別の状態とするまでを、監視、レビュー、承認するための、プロセス、手順、および技術的手段を定義、実装および評価する。これには法的及び規制上の要件の規定を含む。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともに、クライアントが利用可能または選択するリソースおよび鍵所有モデルの範囲に応じて、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSP は、プラットフォームマネージド鍵に対して、この管理策を所有する。	**管理策所有権の根拠；** CSP と CSC はともに、クライアントが利用可能または選択するリソース及び鍵所有モデルの範囲に応じて、この管理策について独立した共有責任を負う。CSC は、カスタママネージド鍵（CMK）に対して、この管理策を所有する。
実施ガイドライン； **全てのサービスモデルに適用：** 一時停止された鍵は、一定期間使用されない。 a. 鍵は、休暇中または危殆化の疑いがある場合に一時停止されることがある。 b. 一時停止は、アクティベート、失効または交換に遷移する前に調査されるべきである。 c. 一時停止された鍵はデータを暗号化するために使うべきではないが、データを復号することはできる。 d. 一時停止期間開始後に適用された暗号化は処理しない。 e. 全ての関連する遷移／活動は、CKMS または棚卸リスト管理システムに（ログ）されるべきである。	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
鍵の非アクティブ化	**CEK-17**	有効期限日となったときに鍵を非不活性化するためのプロセス、手順、および技術的手段を定義、実装、および評価する。なお、これには法的及び規制上の要件の規定を含む。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともに、クライアントが利用可能または選択するリソースおよび鍵所有モデルの範囲に応じて、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSP は、プラットフォームマネージド鍵に対して、この管理策を所有する。	**管理策所有権の根拠；** CSP と CSC はともに、クライアントが利用可能または選択するリソース及び鍵所有モデルの範囲に応じて、この管理策について独立した共有責任を負う。CSC は、カスタママネージド鍵（CMK）に対して、この管理策を所有する。
実施ガイドライン； **全てのサービスモデルに適用：** 非アクティベート化した鍵は暗号化には使用すべきでないが、復号には使用できる。 a. 有効期限が切れると、鍵はデータを暗号化できなくなるべきである。 b. 非アクティベート状態は、鍵が不要になった時点で破棄状態に遷移すべきである。 c. メタデータは、監査目的で保持されるべきである。 d. 全ての関連する遷移／活動は、CKMS または棚卸リスト管理システムに（ログ）されるべきである。	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。 **全てのサービスモデルに適用：** クライアントマネージド鍵の場合

Control Title	Control ID	Control Specification
鍵のアーカイブ	**CEK-18**	アーカイブされた鍵を、最低限の権限でアクセスできるセキュアなリポジトリで管理するためのプロセス、手順、技術的手段を定義、実施、評価すること。これには法的及び規制上の要件の規定を含む。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC はともに、クライアントが利用可能または選択するリソースおよび鍵所有モデルの範囲に応じて、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSP は、プラットフォームマネージド鍵に対して、この管理策を所有する。	**管理策所有権の根拠；** CSP と CSC はともに、クライアントが利用可能または選択するリソース及び鍵所有モデルの範囲に応じて、この管理策について独立した共有責任を負う。CSC は、カスタママネージド鍵（CMK）に対して、この管理策を所有する。
実施ガイドライン； **全てのサービスモデルに適用：** 鍵のアーカイブでは、鍵を長期間保管する。 a. アーカイブされた鍵材料は、後に情報の復元をサポートすることができる。 b. アーカイブされた鍵材料は、将来必要になる可能性があるが、不要になったら破棄すべきである。 c. 鍵の復元プロセスには、バックアップおよびアーカイブされた鍵情報を保護するために使用される長期保管鍵の生成、保管、およびアクセスを含めるべきである。 d. アーカイブは、長期鍵アクセスに使用されるべきである。 e. 棚卸リストシステムは、アーカイブされた鍵情報の保管及び復元を記録すべきである。 f. 全ての関連する遷移／活動は、CKMS または棚卸リスト管理システムに（ログ）されるべきである。	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。 **全てのサービスモデルに適用：** クライアントマネージド鍵の場合。

Control Title	Control ID	Control Specification
鍵の危殆化	**CEK-19**	侵害された暗号鍵を、管理された状況下でデータの復号のためだけに使用し、それ以降はデータの暗号化に使用しないためのプロセス、手順、技術的手段を定義し、実施し、評価すること。これには法的及び規制上の要件の規定を含む。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； これは、両当事者による実行が有効なセキュリティに不可欠であることから、この管理策は「Dependent」に分類される。CSP は暗号化および鍵管理サービスを提供し、これらのサービスをサポートするインフラストラクチャに責任を負う。一方、CSC は、例えば、いつどのデータを暗号化するかを選択したり、暗号化鍵へのアクセスを管理したりするなど、データを保護するためにこれらのサービスを正しく使用する責任を負う。	**管理策所有権の根拠；** これは Shared かつ Dependent 責任である。なぜなら、CSP にはセキュアな暗号化および鍵管理サービスを提供する責任がある一方で、CSC には CSP の特定のニーズに従って、また CSC のポリシーと手順に従って、これらのサービスを構成および管理する役割を担うからである。
実施ガイドライン； 該当する場合、CSP は、以前にデータの暗号化に使用されていた鍵が危殆化し、それらの鍵が暗号化に使用されなくなったことを CSC に通知すべきである。	**実施ガイドライン；** 該当する場合、CSP は、以前にデータの暗号化に使用されていた鍵が危殆化し、それらの鍵が暗号化に使用されなくなったことを CSC に通知すべきである。
IaaS プロバイダー： IaaS プロバイダーは、鍵管理サービスとともに、全てのデータについて移動中と保存中の両方で暗号化の仕組みを提供すべきである。CSP は、これらのサービスが最新のセキュリティ標準およびベストプラクティスに準拠していることを確実とすべきである。CSP は、ベストプラクティスに従って、セキュアな鍵管理および暗号化のためのツールとリソースを提供すべきである。	**IaaS 利用者**： CSC は、CSP が提供するインフラストラクチャ内でデータの暗号化を実装し管理する責任を負う。CSC は、ベストプラクティスに従い、鍵管理のために CSP が提供するツールおよびリソースを使用すべきである。
PaaS プロバイダー： PaaS プロバイダーは、セキュアな鍵管理システムを含む、保存中および移動中のデータに対するプラットフォームレベルの暗号化を提供すべきである。PaaS プロバイダーは、CSC が管理するアプリケーションレベルの暗号化オプションも提供すべきである。CSP は、セキュリティのベストプラクティスおよび標準を遵守すべきである。CSP は、実現可能であれば、CSC に独自の鍵管理能力を提供すべきである。	**PaaS 利用者**： CSC は、プラットフォームレベルで提供される暗号化を使用することを含め、CSP が提供するセキュアなプラットフォームを効果的に使用することを確実にすべきである。 CSC はまた、自身のニーズと CSP が提供するサービスに応じて、プラットフォーム内に追加の暗号化を実装する必要がある場合がある。
SaaS プロバイダー： SaaS プロバイダーは、鍵管理を含むアプリケーションレベルでの暗号化を扱うべきである。プロバイダーは、保存中および移動中のデータが全て暗号化されていることを確実とするべきである。CSP は、実現可能であれば、CSC に独自の鍵管理能力を提供すべきである。	**SaaS 利用者**： CSC は、ソフトウェアレベルで提供される暗号化の使用を含め、CSP が提供するセキュアなソフトウェアサービスを効果的に使用することを確実にすべきである。 CSC は、CSP と協力して、ソフトウェアサービス内における鍵の管理方法を理解し、それが自身のニーズおよびコンプライアンス要件を満たしていることを確実にすべきである。

全てのサービスモデルに適用： CSP のポリシー、手順およびプロセスは、危殆化した鍵が廃棄を決定するための調査を待つことを確実にすべきである。 a. 鍵の紛失や危殆化した時は緊急失効を実施する。 b. 危殆化状態は、鍵に依存している全ての人が知ることができるべきである。 c. 危殆化鍵リスト（CKL）を用いて利害関係者に知らせる。 d. また、危殆化状態を棚卸リスト管理システムに反映させる。 e. 監査を用いて、未検出の危殆化した鍵を発見する。 f. 危殆化からの回復をサポートするためにイベントを分析する。 g. 危殆化した鍵の失効および鍵設定の方法を詳述する。 h. 暗号利用期間を用いて、危殆化した鍵の被害を抑制する。 i. 危殆化した鍵は、その鍵が保護したデータを復号化する目的でのみ使用すべきである。 j. 全ての遷移／活動は登録（ログに記録）され、CKMS または棚卸リスト管理システムにおける鍵の状態が更新されるべきである。	**全てのサービスモデルに適用：** CSP のポリシー、手順およびプロセスは、危殆化した鍵が廃棄を決定するための調査を待つことを確実にすべきである。 a. 鍵の紛失や危殆化した時は緊急失効を実施する。 b. 危殆化状態は、鍵に依存している全ての人が知ることができるべきである。 c. 危殆化鍵リスト(CKL)を用いて利害関係者に知らせる。 d. また、危殆化状態を棚卸リスト管理システムに反映させる。 e. 監査を用いて、未検出の危殆化した鍵を発見する。 f. 危殆化からの回復をサポートするためにイベントを分析する。 g. 危殆化した鍵の失効および鍵設定の方法を詳述する。 h. 暗号利用期間を用いて、危殆化した鍵の被害を抑制する。 i. 危殆化した鍵は、その鍵が保護したデータを復号化する目的でのみ使用すべきである。 j. 全ての遷移／活動は登録（ログに記録）され、CKMS または棚卸リスト管理システムにおける鍵の状態が更新されるべきである。

Control Title	Control ID	Control Specification
鍵の復旧	**CEK-20**	キーマテリアルに関する情報のコントロールが失われた場合、運用の継続性に対するリスクと、キーマテリアルおよびそれにより保護される情報が漏洩するリスクを比較評価するための、プロセス、手順、および技術的手段を定義、実装、および評価する。これには法的及び規制上の要件の規定を含む。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； 両当事者による実行が有効なセキュリティに不可欠であることから、この管理策は「Dependent」に分類される。CSP は暗号化および鍵管理サービスを提供し、これらのサービスをサポートするインフラストラクチャに責任を負う。一方、CSC は、例えば、いつどのデータを暗号化するかを選択したり、暗号化鍵へ	**管理策所有権の根拠；** これは Shared かつ Dependent 責任である。なぜなら、CSP にはセキュアな暗号化および鍵管理サービスを提供する責任がある一方で、CSC には CSP の特定のニーズに従って、また CSC のポリシーと手順に従って、これらのサービスを構成および管理する役割を担うからである。

のアクセスを管理したりするなど、データを保護するためにこれらのサービスを正しく使用する責任を負う	
実施ガイドライン； **IaaS プロバイダー**： IaaS プロバイダーは、鍵管理サービスとともに、全てのデータについて移動中および保存中の暗号化メカニズムを提供すべきである。CSP は、これらのサービスが最新のセキュリティ標準およびベストプラクティスに準拠していることを確実にすべきである。CSP は、ベストプラクティスに従って、セキュアな鍵管理及および暗号化のためのツールとリソースを提供すべきである。	**実施ガイドライン；** **IaaS 利用者**： CSC は CSP が提供するインフラストラクチャ内でデータの暗号化を実装し管理する責任を負う。CSC は、ベストプラクティスに従い、鍵管理のために CSP が提供するツールおよびリソースを使用すべきである。
PaaS プロバイダー： PaaS プロバイダーは、セキュアな鍵管理システムを含む、保存中および移動中のデータに対するプラットフォームレベルの暗号化を提供すべきである。PaaS プロバイダーは、CSC が管理するアプリケーションレベルの暗号化オプションも提供すべきである。CSP は、セキュリティのベストプラクティスおよび標準を遵守すべきである。	**PaaS 利用者**： CSC は、プラットフォームレベルで提供される暗号化を使用することを含め、CSP が提供するセキュアなプラットフォームを効果的に使用することを確実にすべきである。 CSC はまた、自身のニーズと CSP が提供するサービスに応じて、プラットフォーム内に追加の暗号化を実装する必要がある場合がある。
SaaS プロバイダー： SaaS プロバイダーは、鍵管理を含むアプリケーションレベルでの暗号化を扱うべきである。プロバイダーは、保存中および移動中のデータが全て暗号化されていることを確実とするべきである。CSP は、実現可能であれば、CSC に独自の鍵管理能力を提供すべきである。	**Saa 利用者：** CSC は、ソフトウェアレベルで提供される暗号化の使用を含め、CSP が提供するセキュアなソフトウェアサービスを効果的に使用することを確実にすべきである。 CSC は、CSP と協力して、ソフトウェアサービス内における鍵の管理方法を理解し、それが自身のニーズおよびコンプライアンス要件を満たしていることを確実にすべきである。
全てのサービスモデルに適用： 鍵の復元は、バックアップまたはアーカイブから鍵を取得または再構築する。CSP のポリシー、手順およびプロセスは、以下を確実にすべきである： a. 鍵の種類（例えばプライベート署名鍵や対称データ暗号化鍵など） b. 鍵が使用されるアプリケーション（例えば双方向通信、ファイルストレージなど） c. 鍵所有者がローカルエンティティか、他のエンティティか、共有されているか。 d. コミュニケーションにおけるエンティティの役割（すなわち、送信者または受信者）。 e. 鍵が使用されるアルゴリズムまたは計算。 f. 全ての関連する遷移／活動は、CKMS または棚卸リスト管理システムに（ログ）されるべきである。	**全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
鍵のイベントリ管理	**CEK-21**	鍵管理システムがすべての暗号マテリアルとその状態の変化を追跡し、報告するためのプロセス、手順、および技術的手段を定義、実装、および評価する。これには法的及び規制上の要件の規定を含む。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； 両当事者による実行が有効なセキュリティに不可欠であることから、この管理策は「Dependent」に分類される。CSP は暗号化および鍵管理サービスを提供し、これらのサービスをサポートするインフラストラクチャに責任を負う。一方、CSC は、例えば、いつどのデータを暗号化するかを選択したり、暗号化鍵へのアクセスを管理したりするなど、データを保護するためにこれらのサービスを正しく使用する責任を負う。	**管理策所有権の根拠；** これは Shared かつ Dependent 責任である。なぜなら、CSP にはセキュアな暗号化および鍵管理サービスを提供する責任がある一方で、CSC には CSP の特定のニーズに従って、また CSC のポリシーと手順に従って、これらのサービスを構成および管理する役割を担うからである。
実施ガイドライン； **IaaS プロバイダー**： IaaS プロバイダーは、鍵管理サービスとともに、全てのデータについて移動中および保存中の暗号化メカニズムを提供すべきである。CSP は、これらのサービスが最新のセキュリティ標準およびベストプラクティスに準拠していることを確実にすべきである。CSP は、ベストプラクティスに従って、セキュアな鍵管理及および暗号化のためのツールとリソースを提供すべきである。	**実施ガイドライン；** **IaaS 利用者**： CSC は、CSP が提供するインフラストラクチャ内でデータの暗号化を実装し管理する責任を負う。CSC は、ベストプラクティスに従い、鍵管理のために CSP が提供するツールおよびリソースを使用すべきである。
PaaS プロバイダー： PaaS プロバイダーは、セキュアな鍵管理システムを含む、保存中および移動中のデータに対するプラットフォームレベルの暗号化を提供すべきである。PaaS プロバイダーは、CSC が管理するアプリケーションレベルの暗号化オプションも提供すべきである。CSP は、セキュリティのベストプラクティスおよび標準を遵守すべきである。	**PaaS 利用者**： CSC は、プラットフォームレベルで提供される暗号化を使用することを含め、CSP が提供するセキュアなプラットフォームを効果的に使用することを確実にすべきである。 CSC はまた、自身のニーズと CSP が提供するサービスに応じて、プラットフォーム内に追加の暗号化を実装する必要がある場合がある。
SaaS プロバイダー： SaaS プロバイダーは、鍵管理を含むアプリケーションレベルでの暗号化を扱うべきである。プロバイダーは、保存中および移動中のデータが全て暗号化されていることを確実とするべきで	**SaaS 利用者**： CSC は、ソフトウェアレベルで提供される暗号化の使用を含め、CSP が提供するセキュアなソフトウェアサービスを効果的に使用することを確実にすべきである。

ある。CSP は、実現可能であれば、CSC に独自の鍵管理能力を提供すべきである。	CSC は CSP と協力して、ソフトウェアサービス内における鍵の管理方法を理解し、それが自身のニーズおよびコンプライアンス要件を満たしていることを確実にすべきである。
全てのサービスモデルに適用： CKMS は、手動であるか自動であるかにかかわらず、鍵管理活動を処理、制御、保管および報告するために存在する。CSP のポリシー、手順およびプロセスは、CKMS が以下を確実となるようにすべきである： a. 状態の全ての変更の捕捉、追跡およびラベル付け。 b. 未知の暗号資産の継続的な監視。 c. 鍵情報を生成および配付。 d. 公開鍵証明書の取得または生成 e. 鍵情報のバックアップ、アーカイブおよび棚卸リスト f. CSP のデジタル証明書または鍵構造にエンティティをマッピングするデータベースの維持。 g. 失効した鍵または電子証明書に関するレポートの保守及び配付の提供。 h. 監査要求の生成および監査回答の処理。 i. 暗号材料には、鍵、デジタル証明書および HSM を含む。 j. 鍵管理技術およびプロセスが FIPS 検証済みであることの確認。 k. 全ての鍵、デジタル証明書、アルゴリズム、およびメタデータの機密性、完全性、可用性、およびソース認証の保護。 l. 全ての関連する遷移／活動の棚卸リストの CKMS への登録（ログ）。	**全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

Control Domain DCS

2.6 データセンターセキュリティ(DCS)

Control Title	Control ID	Control Specification
オフサイト機器の廃棄ポリシーと手順	**DCS-01**	組織の外部で使用される機器をセキュアに廃棄するためのポリシーと手順を確立、文書化、承認、伝達、適用、評価、および維持する。機器が物理的に破壊されていない場合は、情報の回復を不可能にするデータ破壊手順が適用されるべきである。ポリシーと手順を少なくとも年 1 回確認して更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、インフラストラクチャとデータへの直接アクセス、契約上の義務、専門知識、およびリソースにより、クライアントがクラウドプラットフォームから削除、離脱、または退出するときに、クライアントデータがプロバイダー環境から効果的に削除されるようにする管理策を所有する。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、データセンター内の物理的な機器の廃棄に関する要件と手順を概説するポリシーを策定する必要がある。 ポリシーには、以下のような規定が含まれる必要がある（ただし、これに限定しない）： a. 廃棄許可：機器廃棄要請の承認手続き。権限を与えられた担当者のみが、要請を開始し、承認することができる必要がある。 b. 機器の廃棄：サーバー、ストレージデバイス、ネットワークハードウェアなど、物理的な機器のライフサイクルが終了した場合の廃棄手順。 c. 資産目録および廃止手順：正確な資産目録を維持するための手順（DCS-06 を参照）であり、データ破棄プロセスの開始を含め、機器の廃止時に取るべき手順を定義する。 d. セキュアな輸送と廃棄:廃棄施設までのセキュアな輸送、盗難や不正アクセスからの保護など、物理的な廃棄プロ	**実施ガイドライン：** CSC には適用されない。

セスにおいて講じられるべきセキュリティ対策。

e. データ破棄：機器を物理的に廃棄する前に、業界承認の方法を使用して、機器に保存されている全てのデータを完全に破壊する手順（DSP-02 を参照）。ストレージデバイスからデータを回復できないようにするために、セキュアなデータ消去手順を確立する必要がある。これには、メディアの物理的破壊（ハードドライブの消磁、紙の細断など）、データ暗号化消去、またはソフトウェアベースの消去方法が含まれる場合がある。

f. 機器破壊の検証：文書化され、監査可能な検証メカニズムを通じて、廃止された機器のデータが正常かつ完全に破壊されたことを検証するための体系的プロセスの要件。

g. 廃棄の記録管理と監査：全ての機器およびデータの廃棄イベントの詳細な記録を、クリアされたか、パージされたか、または破棄されたかを明確に示すメディア処分のデジタル証明書とともに追跡システムに記録すること。記録には、監査およびコンプライアンス目的のため、日付、機器／データの種類、機器のシリアル番号、廃棄方法、廃棄日、関係権限者、検証結果を含めること。

h. 機器廃棄業者の認定：認定された業界標準を遵守し、データと機器の適切な廃棄を証明する文書を提供する認定データ廃棄業者を利用するための要件

i. 保管の連鎖手順：廃棄が予定されている機器の移動と取り扱いを追跡し、説明責任を確保し、不正アクセスを防止するための保管チェーン手順。

j. 承認組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与

  i. ポリシーと手順の変更または修正については、承認プロセスを確立する必要がある。

  ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。

k. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進する必要がある。

l. 維持管理と見直しデータセンターおよび機器の廃棄に関するセキュリティポリシーと手順を文書化し、少なくとも年１回見直し、更新する。これは、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映させるために必要である。

Control Title	Control ID	Control Specification

オフサイト転送承認ポリシーと手順	**DCS-02**	ハードウェア、ソフトウェア、またはデータ/情報をオフサイトまたは代替場所に再配置または転送するためのポリシーと手順を確立、文書化、承認、伝達、適用、評価、および維持する。再配置または転送要求には、書面または暗号手法により検証可能な承認が必要である。ポリシーと手順を少なくとも年1回確認して更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、利用者のクラウドサービスとデータをホストするデータセンターとインフラストラクチャを運用するため、この管理策を所有する。この管理策は、ディザスタリカバリ、事業継続性、または拡張などのさまざまな理由で必要となる、ハードウェア、ソフトウェア、またはデータ/情報の別のデータセンターへのセキュアな移転または転送を保証するために不可欠なものである。 CSP は、障害発生時にサービスをタイムリーに復旧させるため、効果的な事業継続計画および災害復旧計画を確実に実施する責任を負う。これには、緊急時に引き継ぎ可能な代替ストレージサイトの事前承認と準備、顧客環境とデータの復旧が含まれる。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、移転または移管中にハードウェア、ソフトウェア、およびデータ/情報を保護するために、強固なセキュリティ対策を実施する必要がある。 これらの対策には、暗号化、アクセス制御、セキュアな転送、インシデント報告手順などが含まれる。CSP は、CSC との明確なコミュニケーションチャネルを確立し、全ての移転または転送活動の包括的な文書を維持する必要がある。 これらの責任を果たすため、CSP は以下のポリシーと手順を維持する必要がある。 ポリシーには、以下に関する規定が含まれる必要がある（ただし、これに限定されない）： a. 移転認可：ハードウェア、ソフトウェア、またはデータ／情報の移転または移管を開始する前に、 CSC から書面または暗号的に検証可能な承認を得るための要件。こ	**実施ガイドライン：** CSC には適用されない。

の承認は、関係する資産、移転先、および時間枠を含む移転または移転の範囲を明確に指定するものでなければならない。

b. CSC への通知：移転または移籍手続きの開始を速やかに CSC に通知し、移転または移籍の進捗と完了に関する最新情報を定期的に提供する手続き。

c. 保管の連鎖手順：移転プロセス全体を通じて、ハードウェアおよびソフトウェアコンポーネントの移動と取り扱いを追跡し、セキュアかつ監査可能な記録を維持するための保管連鎖手順。

d. ハードウェア／ソフトウェアの目録：サーバー、ネットワーク機器、ストレージ機器など、移転が予定されているハードウェア／ソフトウェアコンポーネントのインベントリを確立する手順。現在の構成を文書化し、監査目的で移転後に更新する。

e. アクセス制御とログ：全てのアクセス試行、変更、および転送のロギングによってサポートされる、移転または転送プロセス中のデータ/情報へのアクセスを制限するアクセス制御のためのプロセス。

f. セキュアな輸送：ハードウェアまたはデータ記憶装置の物理的移転のためのセキュアな輸送方法。輸送中は、改ざん防止包装、セキュアな追跡メカニズム、物理的セキュリティ対策を採用すること。

g. データの機密性：移転または移管に関わる機微データ／情報に対するデータ分類とタグ付けの慣行を確立し、機密性の高いデータに対する追加のセキュリティ対策（暗号化、DLP 対策など）を実施するための要件。

    i. 難読化または非特定化技術を採用し、送信中に個人データのような機密データを不明瞭にすること。

h. データの暗号化：クラウド環境からオフサイトへの転送プロセスにおけるデータの暗号化要件

    i. 強力な暗号化アルゴリズム（AES-256 など）を使用し、暗号鍵をセキュアに管理する（CEK-03 参照）

    ii. オフサイトでのデータ保管を保護し、暗号化とアクセス制御の使用を強調して、目的地に到達した後のデータを保護する。

    iii. 転送中の暗号化またはデータ難読化に使用されるべき暗号鍵、パスワード、またはその他のクレデンシャルが適切に管理され、権限を有する要員に制限されていること。

i. 規制標準の遵守：ハードウェア、ソフトウェア、データ／情報の移転または移管中に、関連する規制標準およびデータ保護法の遵守を評価し、必要な承認を取得し、検証するための要件。

j. 承認組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与

    i. ポリシーと手順の変更または修正については、承認

プロセスを確立する必要がある。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。 k. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進する必要がある。 l. メンテナンスとレビューデータセンター、ハードウェア、ソフトウェアの移転、データ転送のセキュリティポリシーと手順を文書化し、少なくとも年１回は見直し、更新して、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映させる必要がある。	

Control Title	Control ID	Control Specification
保護区域ポリシーと手順	**DCS-03**	オフィス、部屋、施設でセキュアでセキュアな作業環境を維持するためのポリシーと手順を確立、文書化、承認、伝達、適用、評価、および維持する。ポリシーと手順を少なくとも年１回確認して更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、提供するクラウドサービスの物理的なインフラを提供し、維持する責任を負うため、管理策を所有する。これには、ハードウェア、ソフトウェア、データが保管され処理されるデータセンター、オフィス、部屋、施設が含まれる。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、包括的なセキュリティ対策をポリシーおよび手続きに組み込み、従業員にとってセキュアな職場環境を維持する必要がある。これには、厳格なアクセス制御の実装、監視システム、およびセキュリティポリシーを監視および適用するためのセキュリティ担当者が含まれる。 CSP の従業員は、物理的なセキュリティプロトコル、セキュアな	**実施ガイドライン：** CSC には適用されない。

データの取り扱い、インシデント報告手順、および緊急時対応計画を含むセキュリティ意識向上トレーニングを受ける必要がある。ソーシャルエンジニアリングに関する認識、ワークステーションのセキュリティとセキュア対策、機微データの取り扱い方法などの対策を重視する必要がある。CSP のポリシーは、リモートワークや出張のセキュリティにも対応し、従業員のセキュアに対する総合的なアプローチを確保する必要がある。

これらの責任を果たすため、CSP は以下のポリシーと手順を維持する必要がある。
ポリシーには、以下に関する規定が含まれる必要がある（ただし、これに限定されない）：

a. アクセス制御：許可された人員のみが入室できるよう、オフィススペース、部屋、施設に特化した物理的な入退室管理を確立し、実施するための要件。入退室には、セキュアなキーカードや生体認証など、セキュアな方法を考慮する必要がある。
b. アクセス要求および承認プロセス：全てのデータセンター施設について、アクセス要求および承認プロセスを定義し、アクセスは権限を与えられた者のみに付与され、最小特権の原則に基づくことを保証するための要件。
c. セキュアな保管場所：セキュアな保管場所： 機密機器、データ保管機器、機密文書および個人所有物のために、オフィス内にセキュアな保管場所を維持するための要件。無許可の取り扱いや持ち出しを防ぐため、これらの保管場所へのアクセス管理および監視システムを採用する。
d. ワークステーションのセキュリティ従業員のワークステーションを保護するための要件：
    i. 強固なパスワードポリシーとセキュアなログインの実践
    ii. 無人のワークステーションをロックし、不正アクセスを防止する。
    iii. 機密情報やアクセス認証情報を見える場所に放置することの禁止
e. 警備の監視と人員：目に見える警備態勢を維持し、セキュア性を高め、不正アクセスを抑止するための警備要員のデプロイ要件。CCTV カメラを含む監視システムを設置し、警備を監視し、強化する。
f. 環境セキュア対策：従業員のセキュアのため、温度、湿度、電力条件を安定的に維持するための環境管理の実施に関する要件。火災時の避難手順を従業員に周知徹底するため、定期的な消防訓練を実施する手順を確立する。
g. 機器管理：機器管理：作業環境における機器、電子機器、および物理的機器のセキュアな管理に関する統制。日常業務で使用する機器およびデータのセキュアな取り扱い、撤去、および廃棄に関するポリシーを実施する（DSP-01 および DSP-02 を参照）。
h. セキュリティ評価：全ての労働環境において定期的な検

査を実施すること。発見事項は文書化し、特定された問題に対処するための是正措置を講じること。 i. 承認：組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与 i. ポリシーと手順の変更または修正については、承認プロセスを確立する必要がある。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持する必要がある。 j. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進する必要がある。 k. メンテナンスとレビューセキュアでセキュアな作業環境のためのポリシーと手順は、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映するために文書化し、少なくとも年 1 回は見直し、更新する。	

Control Title	Control ID	Control Specification
セキュアなメディア輸送ポリシーと手順	**DCS-04**	物理メディアのセキュアな輸送のためのポリシーと手順を確立、文書化、承認、伝達、適用、評価、および維持する。ポリシーと手順を少なくとも年 1 回確認して更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、物理メディアの輸送中も含め、データのライフサイクル全体を通じてデータのセキュリティと完全性を確保する責任を負うため、この管理策の実装は CSP が独占的に所有する。物理メディアをセキュアに輸送するためのポリシーと手順を確立し維持することで、CSP はセキュアな環境を維持し、機微情報を保護することができる。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** 物理メディアのセキュアな輸送を確保するため、CSP は、その	**実施ガイドライン：** CSC には適用されない。

ポリシーと手順において包括的なセキュリティ対策を実施する必要がある。これらの対策には、セキュアな梱包、追跡および監視、保管の連鎖手順、セキュアな保管、物理的保護、権限付与、護送手順、アクセス制限、データの暗号化および消去、インシデントの報告、調査および対応、並びにインシデント発生後の分析が含まれる必要がある。
出発地と目的地の両方における定期的な研修、訓練、および文書化手順により、輸送される物理メディアの完全性と機密性が保証される。これらの手段を組み込むことで、輸送プロセスにおける CSP の全体的なセキュリティポスチャが強化される。

これらの責任を果たすため、CSP は以下のポリシーと手順を維持するものとする。
ポリシーには、以下に関する規定が含まれる必要がある（ただし、これに限定されない）：

a. メディア輸送認可:物理メディアの輸送に関する書面または暗号的に検証可能な承認。この認可には、メディアの種類、目的地、関係する認定要員を明記する。
b. メディアデータの暗号化と消去：
   i. 物理メディアに保存された機密データは、強力な暗号化アルゴリズムを使用して暗号化される必要がある。
   ii. 物理メディアのセキュアなデータ消去手順は、物理的破壊、消磁、暗号消去などの業界で承認された方法に従って確立する必要がある。
c. セキュアな梱包:輸送中の損傷や改ざんから物理メディアを保護するためのセキュアな梱包標準の要件。梱包は、不正な識別を防ぐためにメディアの性質を隠す必要がある。
d. セキュアな保管：物理メディアを、保管庫、セキュアなキャビネット、または以下のような、アクセス制御が制限され指定されたセキュアな場所にセキュアに保管するための要件。物理メディアの保管エリアを保護するために、物理的なセキュリティ対策を含める必要がある（例： アラーム、監視システム、セキュリティ担当者）。
e. 管理の連鎖：輸送中に物理的媒体を取り扱う全ての個人の記録を維持するための管理の連鎖手順
f. 追跡および監視：輸送中の物理的媒体の位置と状態を追跡するためのリアルタイムの追跡・監視システムの導入要件（GPS 追跡、セキュアな輸送サービス、追跡機能付き宅配便サービスなど）。
g. ルート計画：犯罪多発地域や潜在的なセキュリティ上の脅威などを考慮し、リスクを最小限に抑える輸送ルートを計画すること。
h. エスコート手順：機密性の高い物理的メディアの輸送のための護衛手順。
i. 物理メディアのセキュアな引渡し：輸送されるメディアの完全性を確保するための検証手順を含む、物理メディアのセキュアかつ確実な引渡しを確認するための、目的

地到着後の物理メディアの文書化、セキュアな荷降ろし、取扱いの手順 j. アクセス制限：権限のない個人によるメディアの取り扱いやアクセスを防止するため、輸送中の物理メディアへのアクセスを権限のある人員のみに制限するプロセス。 k. 承認組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与 i. ポリシーと手順の変更または修正については、承認プロセスを確立する必要がある。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。 l. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進する必要がある。 m. 維持と見直し物理メディアの輸送セキュリティポリシーと手順は、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映するために文書化し、少なくとも年 1 回は、見直し、更新する。	

Control Title	Control ID	Control Specification
資産の分類	**DCS-05**	組織のビジネスリスクに基づいて、物理的および論理的な資産（アプリケーションなど）を分類して文書化する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、CSP と CSC で責任を共有し、依存関係のある責任である。これは、CSP が管理するクラウドインフラストラクチャの物理資産と論理資産を適切に分類するために、CSC がクラウドにデプロイされたデータの機密レベルを CSP に伝える必要があるためである。物理資産と論理資産は、処理するデータの機密レベルを継承し、CSP がそれらを分類できるようにする。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。

CSP は、以下の責任を負う： • CS のデータのセキュリティ要件を満たすセキュアなクラウド環境の提供。 • CSC データの演算、保管、伝送に使用される物理的及び論理的資産を、当該データの機密性レベルに従って分類し、文書化すること。 • CSC データの機密性レベルに適したセキュリティ管理の実施。	
実施ガイドライン： CSP は、CSC が定義するデータ機密性レベルに沿った包括的なアプローチを遵守する必要がある。 これには、CSC のデータ分類ポリシーの理解、各資産に保存されているデータの機密性の特定と評価、適切なセキュリティ制御の実装、資産セキュリティの継続的な監視と監査が含まれる。 さらに CSP は、資産分類とセキュリティ管理を文書化し、従業員を教育し、自動化ツールを活用してプロセスを合理化し、データ保護対策を強化する必要がある。これらのベストプラクティスを採用することで、CSP は機密データを効果的に保護し、クラウドエコシステムにおける信頼できるパートナーとしての契約上の責任を果たすことができる。 CSP が物理的資産および論理的資産を分類し、文書化するための実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定しない）： a. 資産のインベントリと追跡：CSP は、CSC データの保管、処理、または伝送に使用される全ての物理的および論理的資産のインベントリを活用する（DCS-06 を参照）。このインベントリには、サーバーやストレージデバイスなどの物理的機器、およびネットワーク資産や構成、仮想マシン、オペレーティングシステム、アプリケーションなどのソフトウェアコンポーネントが含まれる。 b. 資産の分類：CSP は、CSC のデータ分類ポリシーに基づいて、各資産に保管されるデータの機密性を評価する必要がある。この評価では、CSC データの種類、データが侵害された場合に発生する可能性のある損害、およびデータ保護に関 する法律上および規制上の要件を考慮する。 c. 資産分類のための自動化ツール：CSP は、自動化ツールを使用して資産の分類とセキュリティを支援できる。これらのツールは、資産の脆弱性をスキャンし、資産分類ポリシーに準拠していない資産を特定することができる。 d. 資産の分類の文書化：CSP は、各資産の分類と当該資産に適用されるセキュリティ管理を文書化する。この文書は、要求に応じて CSC に提供される。 e. 資産のタグ付け：CSP は、識別、追跡、および管理を容易にするため、物理的資産および論理的資産に固有のタグ	**実施ガイドライン：** CSC は、データが適切に保護され、CSP が当該データの機密性に基づき物理的資産および論理的資産に対して適切な分類およびセキュリティ管理を実施することを保証する必要がある。 以下のベストプラクティスが CSC に適用される： a. データ分類ポリシー：CSC は、様々なデータ機密性レベル及びそのレベルにデータを分類するための標準を定義する、包括的なデータ分類ポリシー（DSP-01 及び DSP-04 を参照）を策定する必要がある。このポリシーは、資産分類プロセスの指針として CSP に通知する必要がある。 b. データ使用パターン：データアクセス頻度、データフロー、データ処理アクティビティなどのデータ使用パターンを CSP と共有することができる。この情報は、CSP が利用者のデータが使用されるコンテキストを理解し、物理的および論理的資産に関して情報に基づいた分類の決定を下すのに役立つ。 c. 規制遵守要件：CSP は、業界標準や政府規制など、CSC データに適用される法的および規制コンプライアンス要件について通知される必要がある。これにより、資産の分類およびセキュリティ管理の実装時に、これらの要件が CSP によって考慮されるようになる。 d. 変更管理とコミュニケーション：CSC のデータを取扱う物理的及び論理的資産の変更、または CSC のデータ分類ポリシーや使用 パターンの変更については、CSP との間でオープンな連絡手段を維持する必要がある。このコミュニケーションにより、CSP は資産の分類およびセキュリティ管理を、CSC の進化するデータセキュリティおよび保護要件と整合させることができる。

またはラベルを割り当てる必要がある(DCS-06 を参照)。 f. セキュリティ管理の適用：物理資産と論理資産に適切な分類レベルを適用し、クラウド資産に保存、処理、伝送されるデータの機密性に応じて、適切なセキュリティ保護と管理を行う。 g. 継続的な監視と評価：CSP は、定期的に、または資産の変更時に、資産のセキュリティを監視および監査し、適用されるセキュリティ管理が効果的であり、CSC データの機密性レベルに基づいて適切であることを確認する。	

Control Title	Control ID	Control Specification
資産のカタログ化と追跡	**DCS-06**	CSP の全てのサイトにある関係する物理的および論理的資産を、セキュアなシステム内でカタログ化し追跡する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC はどちらも、所有するクラウド資産をカタログ化して追跡する責任を共有する。これは、CSP が CSC に、CSC データの計算と保存に使用される CSP 資産のカタログへのアクセスを許可する必要があるためである。CSC には、資産のリストを取得する権限が与えられている必要がある。効率的でタイムリーな追跡、コスト分析、アクセス制御の決定、およびアラート(該当する場合は自動化による)のために、資産に説明的なメタデータ(タグ)を割り当てることは、CSP のサポート範囲内である必要がある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、インベントリを追跡し、サーバーやその他のデータセンター資産の物理的なロケーションを管理するための包括的なソリューション（CMDB など）を採用し、紙ベースの手動プロセスを廃止する必要がある。サーバー、スイッチ、データセンター資産追跡、およびラック用のホスト型資産追跡ソリューションは、	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は CSP と連絡を取り、CSP が提供するツール（カタログマネージャや API を介したクラウド管理プレーンへのアクセスなど）のうち、CSC のデータ処理に使用されるクラウド資産のリストを CSC が取得できるものを把握する必要がある。

通常、パッシブ無線周波数識別（RFID）、全地球測位システム（GPS）、Bluetooth Low Energy（BLE）、および／またはハードウェア・ルートオブトラスト（HROT）を備えた信頼された実行環境（TEE）などの技術の組み合わせを活用する。

CSP は、CSC が使用している資産（クラウドストレージなど）またはプロビジョニングした資産（VM など）のリストを管理し、CSC が CMDB にアクセスし、CSC のデータを扱う資産を識別してタグ付けするためのツールを CSC に提供する必要がある。例えば、CSP は、CSC のデータの保存に使用される資産（およびそれらにアクセスする手段）に関する情報を共有する必要がある。

この情報は、CSP が提供する全てのクラウド関連資産とサービスのカタログ化、タグ付け、追跡、および CSC データの処理と保存（ネットワーク、コンピュート、ストレージサービスなど）に CSC が使用できる。

全ての棚卸資産の EoL（使用期限）追跡システムが維持される必要がある。クラウド環境内の全ての棚卸資産の正確な EoL 情報（例えば、ハードウェア及びソフトウェアの製造者の EoL 日付、ソフトウェア／サービスの有効期限、パッチの利用可能スケジュール）を収集し、維持するプロセスを確立する必要がある。資産インベントリシステム内に自動化された EoL 通知を導入し、資産廃棄のスケジュール、ワークロードの移行、耐用年数が近づいた脆弱な資産の無効化など、事前予防的なセキュリティ対策を実施する。このような通知は、CSC の変更管理フレームワークにシームレスに統合するために、適時に CSC に伝達される必要がある。

CSC は、カタログ内の資産と資産所有者を分類するためのタグのリストを作成するという、環境のタグ付け戦略を定義する必要がある。標準化された命名規則は、クラウドでホストされるリソースを整理するための出発点である。タグの同じ命名規則は、複数の CSP(マルチクラウド環境など)で一貫して使用する必要がある。また、可能であれば、クラウド資産は自動化された手段で追跡し、それに基づいて迅速な決定(アクセス制御の決定、監視とアラート、アカウンティングなど)が行えるようにする必要がある。

資産の命名とタグ付けの規約を定義するためのテンプレートは、全ての主要 CSP によって定義されている。CSC は、CSP の命名標準を採用するか、またはクラウド導入の一環として導入予定の各資産タイプに適用する独自の命名標準を定義するかを選択することができる。

クラウドサービスモデル（ただし、これらに限定されない）ごとに、タグ付けの規則と、カタログ化され追跡されるべきそれぞれのクラウドアセットタイプの例を以下に示す：

a. アセットタグの種類
   i. 環境タグ：本番環境、開発環境、テスト環境など、異なる環境に属するリソースを識別する。
   ii. 機能/アプリケーションタグ:リソースをクラウド環境内の特定のアプリケーションやサービスに関連付ける。
   iii. 部門タグ：リソースを組織内の特定の部門に関連付ける。
   iv. ロケーションタグ：地理的な場所やデータセンターの地域に基づいてリソースをタグ付けする。
   v. オーナータグ：特定のリソースを担当する個人またはチームの指定
   vi. リリースバージョンタグ：関連するソフトウェアまたはアプリケーションのバージョン番号
   vii. Security Classification Tag（セキュリティ分類タグ):リソースのセキュリティ分類または機密レベルを示す。
   viii. コンプライアンス／規制タグ：特定の規制や標準に準拠していることを示す
   ix. 自動化タグ：スクリプト、スキャナ、またはその他の自動化によって、アセットが選択されるべきかどうかを示す。
   x. アクティブタグ：生産、開発、またはその他の関連目的のために現在使用中のリソースを指定する。
   xi. 非推奨タグ：引退が予定されている、またはアクティブに使用されなくなったリソースを指定する。
b. クラウド資産の種類：

	i. 仮想マシン（VM インスタンス/イメージ、OS 名/バージョンなど）、 ii. 仮想ネットワーキング（VPC ネットワークとサブネット、DNS レコード、IP アドレスなど）、 iii. データベース（データベース/SQL サーバーなど）、 iv. ストレージ（ブロック、ファイル、オブジェクトストレージタイプなど）、 v. アプリケーション(カスタムアプリケーション、コンテナイメージ、ソフトウェアライセンスなど） カタログには、全てのデバイスステータスの変更（パッチレベル、紛失／退役ステータス、資産タイプの割り当て先、または BYOD の承認先など）を含める必要がある。 クラウド資産のカタログ化と追跡は、最もセキュリティに関連する資産や重要な資産に優先順位をつけて行い、次にリスクが最小またはゼロに関連する残りの資産タイプを含める必要がある。 CSP がサポートする場合は、タグ付けされていない資産、または CSC のタグ付けルールに沿っていないタグ値を持つ資産（例えば､「分類レベル」の値でタグ付けされた資産またはタグ付けされていない資産）を特定するために、自動スキャンを行う必要がある。 CSP からタグ付けツールが提供されていない場合､CSC は手動でアセットのタグ付けとカタログ作成を行う必要がある。カタログの管理と保守をより効率的に行うには、解析しやすい形式（JSON、YAML、XML）が推奨される。 CSC は、該当するセキュリティリスクを予防、検出、回復、及び対応するために、セキュリティツールをカタログに含まれる資産に対応付ける必要がある（例えば、予防的及び検知的なセキュリティ管理として、VM/OS 資産に脆弱性パッチ及びウイルス対策ツールを使用する)。 「セキュリティ分類レベル」キータイプでタグ付けされた資産は、特定の資産タイプがそのようなデータに対してコンピュート、ネットワーク、またはストレージ操作を実行するために使用するデータのさまざまな分類レベルの中で、最も高いデータ分類レベル(最高水準点)値を継承する必要がある。

Control Title	Control ID	Control Specification

制御されたアクセスポイント	**DCS-07**	人員、データ、および情報システムを保護するために、物理的なセキュリティ境界を実装する。管理ドメイン、ビジネスドメインとデータのストレージおよび処理施設エリアの間に物理的なセキュリティ境界を確立する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、CSC に提供されるクラウドサービスに関連するデータセンター、管理、およびビジネスドメインの人員、データ、およびシステムを保護するために、物理的な境界セキュリティ管理の実装に関する全責任を負う。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は CSC の機微データや情報システムを扱うため、物理的セキュリティ侵害の格好の標的となる。強固な物理的セキュリティ境界線を確立することで、CSP は CSP 施設内の人員、データ、および情報システムを保護することができる。本ガイドラインは、CSP の資産を保護するために効果的な物理的セキュリティ境界を導入するためのベストプラクティスを概説する。 物理的な境界セキュリティに関する実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 周辺警備： i. CSP の物理的境界を画定するため、アクセスポイントを管理する高いセキュリティフェンスを設置する。 ii. 多要素認証（MFA）は、ゲート、ドア、搬入口を含む全ての入口に対して導入される必要がある。従業員と訪問者は、入館前に有効な証明書を提示し、本人確認を受ける必要がある。 iii. 周囲および立入禁止区域内に、高解像度のモーションアクティベーテッド監視カメラの包括的なネットワークを設置する。 iv. 不正アクセスを抑止し、警備員や監視システムの視認性を向上させるため、周囲に適切で整備された照明を設置する必要がある。 b. 行政・事業分野	**実施ガイドライン：** CSC には適用されない。

i. 管理・業務エリアとデータ保管・処理施設エリアを物理的に分離する必要がある。 ii. データ保管・処理施設エリアへの入退室管理をより厳格化し、関係者以外の立ち入りを禁止する。 iii. 正式な訪問者管理プロセスを確立し、訪問者には常に許可された職員が同伴することを義務づける必要がある。訪問者記録を管理し、機密エリアへの立ち入りを制限する。 iv. ベンダーの行動を監視し、その存在と行動の適切な文書化を確実にするために、ベンダーのアクセスは指定されたエリアに分離され、機密エリアへのアクセスは制限される必要がある。 c. データ保管・処理施設エリア i. 機微データや重要な IT 資産は、強化された壁、ドア、入退室管理システムを備えたセキュアな専用室内に保管する必要がある。侵入を制御し、不正アクセスを防止するために、マントラップまたはその他の物理的バリアを設置する。 ii. 納品および点検のための指定区域を設ける必要がある。納入品および備品には、改ざん防止シール、追跡システムを導入する必要がある。搬入エリアへの立ち入りを制限し、全ての搬入に関する文書を管理する必要がある。 iii. 停電や電力サージが発生した場合でも、IT インフラストラクチャの中断のない運用と保護を保証するために、信頼性の高い電源バックアップシステムとサージ保護を導入する必要がある。 d. 継続的な監視と評価：CSP は、定期的に、または資産の変更時に、資産のセキュリティを監視および監査し、適用されるセキュリティ管理が効果的であり、CSC データの機密性レベルに基づいて適切であることを確認する。	

Control Title	Control ID	Control Specification
機器の識別	**DCS-08**	接続の認証方法として、機器の識別を使う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実装責任は、CSP によって排他的に所有される。そして、該当する場合はロケーション認識技術を使用して、既知の機器のロケーションに基づいて接続認証の完全性を検証する。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** 接続認証の方法として物理的な機器識別を実装することで、クラウドリソースに接続する機器の真正性を検証し、クラウドセキュリティを強化する。このアプローチにより、従来のユーザー名とパスワードの認証を超えた保護レイヤーが追加され、不正アクセスや資格情報の盗難に関連するリスクが軽減される。 機器認証の実装のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 機器の登録と識別： i. 全ての許可された機器の包括的な目録を維持すること（DCS-06 を参照）。 ii. クラウド環境に接続する機器を発見し、登録するための自動化されたメカニズムを採用する必要がある。 iii. 機器の識別は、きめ細かなアクセスポリシーを実施するために、クラウドのアクセス・管理策・メカニズムと統合される必要がある。 b. 識別子の割り当てと保護： i. クラウドインフラに接続されている全ての物理的機器（サーバー、ネットワーク機器、ストレージ機器、その他接続されているハードウェアなど）には、一意の識別子（MAC アドレス、シリアル番号など）を割り当てる必要がある。 ii. 機器の識別子には、一貫性のある標準化された命名規則を使用する必要がある。 iii. 機器識別子の不正な改変を防止するため、改ざん防止機構を採用する必要がある（例えば、ハードウェアベースの識別子、暗号技術、またはセキュアな改ざん防止ラベル） c. 機器の信頼性評価： i. 接続機器の完全性と信頼性を検証するため、機器認証プロトコルを導入する必要がある。 ii. セキュアブートメカニズムは、機器が真正かつ変更されていないファームウェアを実行していることを保証するために利用される必要がある。 iii. 機器のセキュリティポスチャを維持するために、脆	**実施ガイドライン：** CSC には適用されない。

弱性スキャンとパッチ適用技術を採用する。 d. 接続認証メカニズム： i. 機器の識別情報、リスク評価、ユーザー権限レベルに基づくきめ細かなアクセス制御ポリシーを採用する必要がある。 ii. 機密性の高いリソースや特権的な機能へのアクセスは、機器の信頼性とユーザー権限に基づいて制限される必要がある。 iii. クラウドインフラストラクチャと認証対象機器との間にセキュアな通信チャネルを確立する必要がある（TLS、SSH 暗号化、または専用の認証プロトコルを使用するなど）。 iv. 認証プロセス中にクラウドインフラストラクチャに固有の識別子を提示するための機器メカニズムを実装する必要がある(例：暗号化ハンドシェイク、チャレンジレスポンスメカニズム、またはセキュアな構成プロトコル) v. 機器識別子の信頼性は、信頼できる機器情報源（集中型機器レジストリ、分散型台帳技術、信頼できるハードウェアセキュリティモジュール（HSM）など）を使用して検証する必要がある。 e. 継続的なモニタリングと評価： i. 機器認証管理の有効性を継続的に監視し、評価する（SIEM ツールやクラウドベースのセキュリティ監視サービスを使用するなど）。 ii. 機器の識別および認証に関連する潜在的なセキュリティ侵害、不正アクセス試行、または設定ミスを特定するために、監査ログ（機器の識別子、認証方法、タイムスタンプ、接続状態など）を維持し、定期的にレビューする。	

Control Title	Control ID	Control Specification
保護区域における認証	**DCS-09**	認可された担当者のみに保護エリアへのアクセスを許可し、全ての入口と出口のポイントを物理的なアクセス制御メカニズムによって制限し、文書化し、監視する。組織が適切と見なす期間で定期的にアクセス制御記録を保持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、データセンターのセキュアなエリアへの物理的なアクセスを許可された担当者のみに許可する管理策を実施する責任を有する。この管理策の最終的な所有は、データセンター・インフラストラクチャを所有し運用する主体である IaaS プロバイダーにある。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、クラウド環境内のセキュアなドメインへのアクセスを制限する包括的な枠組みを確立し、権限を付与された担当者のみが入室できるようにし、全ての入退室アクティビティが文書化され、監視され、指定された期間保管されるようにする。 セキュアなエリアへのアクセスに関する実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 物理的なアクセス制御： i. 物理的バリア、電子入退室管理システム、およびセキュリティ要員を組み合わせて、物理的入退室管理の階レイヤー化アプローチを実施する必要がある。 ii. セキュア区域の出入り口を指定する。 iii. セキュア区域への不正侵入を防ぐため、物理的バリアを設置する必要がある（フェンス、壁、ドア、マントラップなど）。 iv. 電子入退室管理システムを導入する必要がある（例：キーカード、近接カード、バイオ評価指標・スキャナ）。 v. セキュリティ要員を採用し、物理的・電子的にセキュアなエリアを監視・巡回させる。 vi. 許可されていない人物の出入りを追跡・管理するため、訪問者管理手順を実施する必要がある。 b. アクセス管理記録の文書化： i. 入退室管理記録システムを導入し、セキュア区域内での全ての出入りを記録・把握する。 ii. セキュア区域に出入りする全ての人員の身元を、出入りの日時とともに記録する必要がある。 iii. 物理的アクセス、論理的アクセス、リモートアクセスなど、付与されたアクセスの種類を文書化する。 iv. アクセス管理記録は、組織が適切とみなす期間、規制要件および組織のポリシーに従って維持されなければならない。 c. 出入り口の監視： i. 出入り口は、監視カメラやその他の監視システムを使用して、セキュアなエリアへの出入りを常時監視	**実施ガイドライン：** CSC には適用されない。

する。 ii. 監視システムは入退室管理システムと統合し、入退室イベントとビデオ映像を関連付ける。 iii. 不審なアクセス事象を速やかに確認し、調査する手順を確立する必要がある。 d. 継続的なモニタリングと評価：物理的アクセス管理の有効性を継続的に監視し、潜在的な脆弱性を特定し対処するために、定期的に物理的セキュリティ評価を実施する。	

Control Title	Control ID	Control Specification
監視システム	**DCS-10**	許可されていない入場および退場の試行を検出するために、外部境界および全ての入口と出口のポイントで、データセンター監視システムを実装、保守、および運用する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、外部境界および全ての出入口におけるデータセンター監視システムの実装、維持、および運用の責任を負う。この管理策の所有は IaaS プロバイダーにあり、IaaS プロバイダーはデータセンターインフラを所有し運用する主体である。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** CSP が、不正な出入りを検知するためのデータセンター監視システムを効果的に実装、維持、運用するために、実装のベストプラクティスには以下を含める（ただし、これらに限定されない）： a. 物理アクセス制御システム(PACS)： PACS は、データセンターの境界（エントリポイント、サーバールーム、立ち入り禁止区域など)へのアクセスを制御するために実装する必要がある。PACS は、多要素認証（MFA）やキーカード、生体認証などのさまざまな認証方法を利用できる。 b. ビデオ監視： 鮮明な画像を撮影し、不審な活動を特定するために、暗視機能、モーション検出、分析機能を備えた	**実施ガイドライン：** CSC には適用されない。

高解像度カメラをデータセンターの周囲(入口、フェンス、駐車場など)に配置する必要がある。テクノロジーには次のものが含まれる(ただし、これらに限定されない):

i. 赤外線サーマルカメラで熱を検知し、暗い場所や視界の悪い場所でも監視を可能にする。

ii. 車両進入口にナンバープレート認識装置を設置し、ナンバープレートを捕捉・識別することで、許可車両と許可されていない車両の監視を可能にする。

iii. AI を搭載した監視システムにより、脅威の検知と分析を強化し、潜在的な脅威をリアルタイムで特定できるようにする。

c. 境界侵入検知システム（PIDS）：データセンター境界への不正侵入を検知するため、PIDS センサーをデプロイする（モーションセンサー、赤外線ビーム、光ファイバーセンサー、地中レーダーなど）。

d. 境界侵入防止システム（PIPS）：PIPS は、不正侵入を積極的に防止するために、周辺に沿ってデプロイする必要がある（例：電化フェンス、開閉式ボラード、音波抑止装置）。

e. ビデオ分析：監視カメラの映像を分析し、不審な行動（うろつき、不正アクセス、異常行動など）を自動的に検出するために、ビデオ分析ソフトウェアを活用する必要がある。

f. 継続的な監視と評価：データセンター監視システムの有効性は継続的に監視され、進化する脅威や脆弱性に基づいて適切に構成、維持、更新されるようにセキュリティ対策が適応される必要がある。

Control Title	Control ID	Control Specification
不正アクセスに対する対応訓練	**DCS-11**	不正な入場または退場の試行に対応するようにデータセンター担当者をトレーニングする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠： CSP は、不正な出入りの試みに対応するためにデータセンターの要員を訓練する責任を負う。この管理策の最終的な所有は、データセンター・インフラストラクチャの所有者兼運用者である IaaS プロバイダーにある。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： データセンター要員は、CSP の環境のセキュリティを維持するために、不正な物理的アクセスの試みに効果的に対応できるよう適切に訓練する必要がある。 無許可の出入りに対応する要員の訓練における実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 研修プログラム：物理的セキュリティのさまざまな側面（不正アクセスの認識、事故への対応、確立された手順の遵守など）をカバーするトレーニングプログラムを設計し、実施する。 i. データセンター要員は、不正な物理的アクセスの試みに関するインシデント対応計画に精通している必要がある。 ii. 職員は、無許可の出入りが発生した場合に取るべき具体的な手順について訓練を受ける必要がある。 iii. 担当者は、出入国管理インシデントの正確かつタイムリーな文書化の重要性と、分析、調査、およびコンプライアンス目的に使用できる詳細な報告書の必要性について、研修を受ける必要がある。 b. 緊急時の手順：緊急手順に関する詳細な訓練を実施する（避難、施錠、その他セキュリティインシデント発生時に必要となりうる対応措置など）。 c. シミュレーション演習：担当者が不正な物理的アクセスの試みに対応できるよう、定期的に模擬演習を実施する必要がある。 d. コミュニケーション手順：従業員は、警備チーム、経営陣、および必要に応じて法執行機関など、適切な当局に迅速かつ正確に事件を報告する方法について訓練を受ける必要がある。 e. セキュリティ技術の使用：要員は、セキュリティ技術（監視カメラ、入退室管理システム、侵入検知システムなど）の使用法、警報の解釈法、適切な対応法について訓練を受ける必要がある。 f. 警備チームの調整： i. データセンター要員と専任のセキュリティチームとの間で、協力と協調を促進する必要がある。 ii. セキュリティインシデント発生時に、関連チームが役割と責任を理解する必要がある。 g. エスコートの手順 i. 職員は、セキュア区域内での訪問者や請負業者に	**実施ガイドライン：** CSC には適用されない。

対する適切な付き添い手順について訓練を受ける必要がある。 ii. 適切な資格証明書を持たない個人の身元を確認するために、チャレンジ手続きを実施する必要がある。 h. 法的および倫理的配慮：不正な物理的アクセスの試みに対応する際の法的および倫理的側面、並びに職員の権限の限界と法律の範囲内で取るべき適切な行動について理解するための教育が提供する必要がある。 i. 事後レビュー：模擬訓練や実際の事故が発生するたびに、事故後のレビューを実施し、確認された改善点を特定し、得られた教訓を今後の訓練セッションに反映する。	

Control Title	Control ID	Control Specification
ケーブルのセキュリティ	**DCS-12**	全ての施設、オフィス、および部屋において、電力および通信ケーブルを傍受、干渉、または損傷の脅威からリスクベースで保護し保証するプロセス、手順、および技術的対策を定義、実装、および評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、全ての施設、オフィス、および部屋において、傍受、干渉、または損傷の脅威から電力および電気通信ケーブルをリスクベースで確実に保護するために、この管理策を実施する責任を負う。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** 電力および通信ケーブルは、データセンター、オフィス、および部屋の運用を支える重要なインフラコンポーネントである。これらのケーブルは、傍受、干渉、損傷など、さまざまな脅威に対して脆弱である。 • 傍受は、権限のない個人が機微データにアクセスすることを可能にする。	**実施ガイドライン：** CSC には適用されない。

- 干渉は、重要なシステムを混乱させたり、不能にする可能性がある。
- 損傷により停電やデータ損失が発生する可能性がある。

これらの脅威から電力ケーブルおよび通信ケーブルを保護するために、CSP は以下の対策を含む（ただし、これらに限定されない）リスクベースのアプローチを実装する必要がある：

a. ケーブルセキュリティリスク評価：物理的なアクセス、電磁干渉（EMI）、意図的な妨害行為など、電力ケーブルや電気通信ケーブルに対する潜在的な脅威を特定するために、リスクアセスメントを実施する必要がある。
b. ケーブル・物理的アクセス障壁：電力ケーブルおよび通信ケーブルへの不正アクセスを制限するために、物理的なバリアが導入される必要がある（フェンス、セキュリティゲート、アクセス制御システムなど）。
c. セキュアなケーブル配線：ケーブルはセキュアな経路（電線管や専用ケーブルトレイなど）を通ることを確実にする。
d. ケーブルのシールド：電磁干渉（EMI）を最小限に抑え、不正な信号の盗聴を防ぐため、シールドケーブルまたは保護筐体を使用する。
e. 電源ケーブルと通信ケーブルの分離：電源ケーブルと通信ケーブルを分離することで、EMI が通信信号に干渉するのを防ぐことができる。
f. 接地とボンディング：電気サージや落雷からケーブルを保護するため、適切な接地とボンディングを実施する。
g. モニタリングとサーベイランス：ケーブルインフラの改ざんや損傷の兆候を監視する監視システムを設置し、維持する。
h. 継続的なモニタリングと評価：
   i. ギャップや弱点を特定するため、定期的なテストとモニタリングを通じて、実施されたケーブルセキュリティ管理の有効性を評価する。
   ii. ケーブルの損傷、干渉、または傍受のインシデントの傾向を分析し、教訓と新たな脅威を組み込んで、パターンと改善のための潜在的なドメインを特定する。

Control Title	Control ID	Control Specification
環境システム	**DCS-13**	温度と湿度の状態が承認された業界標準範囲内にあることを継続的に監視、維持、およびテストするデータセンター環境制御システムを実装および保守する。
Control Ownership by Service Model		

IaaS	PaaS	SaaS
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、データセンターの環境制御システムを実装および維持する責任を所有する。このシステムは、許容される業界標準の範囲内で、温度および湿度の状態を継続的に監視、維持、およびテストする。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、データセンターの最適なパフォーマンスと信頼性を確保するために、効果的なデータセンター環境制御システムを導入し、維持する必要がある。 CSP がデータセンターの環境制御システムのセキュリティを確保するための実装のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 環境モニタリングシステム： i. 温度と湿度レベルをリアルタイムで追跡する高度な環境モニタリングシステム。 ii. データセンター全体に戦略的に配置された分散型センサーにより、さまざまなゾーンから正確な測定値を取得。 b. 自動環境制御：集中制御と自動化のためにビル管理システム（BMS）と統合された、事前定義されたしきい値に基づいて温度と湿度を調整する自動制御システム。 c. 冗長性とフェイルオーバー： i. 冗長 HVAC(暖房、換気、空調)システムを実装し、1つのシステムに障害が発生しても継続的な運用を確保する。 ii. 異なる環境制御システム間をシームレスに切り替えるために実装されたフェイルオーバーメカニズム。 d. エネルギー効率： i. 冷却システムの効率は、ホット/コールドアイルの封じ込め、気流管理、可変速ファンなどの技術によって最適化する必要がある。 ii. 外気の節約など外部条件が許す場合は、フリークーリング方式を利用する必要がある。 e. 遠隔監視と管理： i. 管理者がどこからでも環境状態を監視・管理できる	**実施ガイドライン：** CSC には適用されない。

よう、リモート監視・管理機能を有効にする。

ii. 迅速な対応を可能にするため、範囲外の状態に対するアラートと通知を実施する必要がある。

f. 定期的なメンテナンス：

i. 清掃、フィルター交換、センサーの較正など、HVAC機器の定期的なメンテナンススケジュールを設定する。

ii. 故障につながる前に潜在的な問題を特定するため、定期的な点検を実施する必要がある。

g. 定期的なパフォーマンステスト：

i. 環境制御システムの定期的な性能試験を実施し、業界標準を満たしていることを確認する。

ii. 極限状態をシミュレートし、システムのピーク負荷処理能力を検証する。

h. 熱画像と解析：

i. ホットスポットを特定し、冷却装置の配置を最適化する赤外線サーマルカメラ

ii. データセンター全体の温度分布を均一にするための熱解析

i. 規格への整合：環境セキュリティ管理システムの業界標準（例えば、ISA/IEC 62443）への整合と遵守のためのプロセス。

j. 文書化と報告：

i. 環境制御の設定、試験手順、結果を文書化し、維持する。

ii. システムの性能と環境条件について定期的なレポートを作成し、レビューと分析を行う。

k. 環境システムのアクセス管理：環境制御システムへの物理的なアクセス制御を実施し、不正な改ざんを防止するとともに、セキュアなプロトコルを使用して許可された担当者に限定したリモートアクセスを行う。

l. 監査証跡：環境制御設定の変更を追跡するために詳細な監査証跡を有効にし、異常な活動を特定し調査するために定期的にレビューする。

m. システム／ソフトウェアのパッチ適用：環境制御システムおよび関連ソフトウェアは、最新のセキュリティパッチを適用する。

n. クラウドベースの監視と管理：

i. クラウドベースの監視・管理プラットフォームを活用して、複数のデータセンターの環境状態を一元的に監視する必要がある。

ii. クラウドベースのソリューションは、環境データをリアルタイムで可視化し、データ分析を容易にし、制御システムの遠隔管理を可能にする必要がある。

iii. クラウドベースの予測分析ツールを活用して、センサーデータを分析し、重要な IT インフラに影響を与える前に潜在的な環境危険を特定する必要がある。

Control Title	Control ID	Control Specification
セキュアなユーティリティ	**DCS-14**	継続的な効果を得るために、ユーティリティサービスのセキュア化、監視、保守、およびテストを計画された間隔でおこなう。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、ユーティリティサービスが計画された間隔で継続的に有効であることを確保し、監視し、維持し、テストする責任を負う。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** データセンターユーティリティサービスとは、データセンターの機能をサポートする不可欠なインフラコンポーネントを指す。これらのサービスは、データセンター環境の運用の完全性、パフォーマンス、および信頼性を維持するために不可欠である。 主なデータセンターユーティリティサービスには以下が含まれる：電源とバックアップ、冷却/空調、消火、ラックとキャビネット、水と漏水検知システム。 ユーティリティサービスのセキュア性を確保するための実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 電源とバックアップシステム： i. データセンター内のサーバー、ネットワーク機器、その他のハードウェアに電力を供給するための、継続的で信頼性の高い電力源。 ii. 配電システム（PDU）、変圧器、発電機を不正アクセス、妨害行為、サイバー攻撃から保護するための物理的・論理的セキュリティ対策	**実施ガイドライン：** CSC には適用されない。

iii. 電力消費量を継続的に監視し、異常、過負荷の可能性、差し迫った故障を特定し、アラートを生成。 iv. ダウンタイムを最小限に抑え、機器の寿命を延ばすための、清掃、点検、テストなどの動力機器の定期メンテナンス v. 電源システムおよびバックアップ電源システム（例：バックアップ発電機、UPS システム）は、定期的にテストおよび保守を行い、中断や停止なしにピーク需要に対応できるようにする。 vi. 継続的な稼働を確保するために冗長電源を導入し、バックアップ発電機や UPS システムを定期的に点検・テストを実施。 vii. バックアップ電源システムは、改ざんを防止するための独自のセキュリティ対策が必要です。 viii. バックアップ電源システムに関連するログイベントは、セキュリティ分析のために監視する必要がある。 b. 冷却システムと HVAC（暖房、換気、空調）： i. データセンター内の温度と湿度を調整する冷却システムにより、機器の過熱を防ぎ、最適な稼動状態を確保する。 ii. 空調装置、冷凍機、冷却塔を含む HVAC システムを不正アクセス、妨害行為、サイバー攻撃から保護するための物理的・論理的セキュリティ対策 iii. 潜在的な問題を特定し、最適な冷却状態を維持するために、温度、湿度、エアフローを含む冷却システムの性能を継続的に監視する必要がある。 iv. 効率的な運転を確保し、故障を防ぐために、冷却装置のメンテナンスは定期的に行う必要がある。 v. バックアップ冷却システム（発電機や非常用冷却装置など）は、プライマリシステムが故障した場合にも適切な冷却を維持できるよう、定期的にテストする必要がある。 vi. HVAC システムは、遠隔監視および制御機能を備えたものを使用する必要がある。 c. 消火システム： i. 火災の危険から保護し、機器への潜在的な損傷を最小限に抑える自動火災検知・抑制メカニズム ii. 消火制御システムへの物理的および論理的アクセスは制限され、定期的に見直する必要がある。 iii. 火災検知センサーの継続的な監視を可能にし、消火システムの定期的な試験と点検を実施する必要がある。 iv. 防火設備の定期的な点検と保守を計画する。 v. 消火システムとソフトウェアは、業界のベストプラクティスに基づいて更新する必要がある。 d. ラックおよびキャビネットシステム： i. サーバーラックは、物理的なロックとアクセス制御で保護する必要がある。	

ii. 無秩序なケーブル配線に伴うセキュリティリスクを回避するため、ケーブル管理を実施する必要がある。 iii. 不正アクセスを検出するために、改ざん防止シールを使用する必要がある。 e. 水と漏水検知： i. 水検知システムを導入し、リアルタイムで警告を発する必要がある。 ii. 水の浸入を防ぐため、物理的なバリアと防水対策を設置する必要がある。 iii. 潜在的な水関連リスクを特定するため、インフラを定期的に点検・整備する必要がある。 iv. 水に関する緊急事態に対応するため、定期的な訓練を実施する必要がある。 f. 電気通信とインターネット接続 i. 電気通信およびインターネットインフラへの物理的なアクセスは、権限を与えられた担当者のみに制限する必要がある。 ii. 電気通信/インターネット機器への不正アクセスを検出するために、改ざん防止シールとアラームを使用する必要がある。 iii. インターネットやネットワーク機器は、セキュリティの脆弱性に対処するため、定期的に更新し、パッチを当てる必要がある。 iv. 信頼できる電気通信サービスプロバイダーは、セキュリティに重点を置いて吟味し、選定する必要がある。 v. 障害発生時に異なる通信経路を切り替えるため、冗長通信およびインターネットフェイルオーバーメカニズムを導入する必要がある。 g. 継続的なモニタリングと評価：ユーティリティサービスのセキュリティ管理の有効性は、進化するセキュリティ脅威と技術の進歩に適応するために、継続的に監視、評価、更新される必要がある。	

Control Title	Control ID	Control Specification
設備の場所	**DCS-15**	ビジネス上重要な機器を、環境に関するリスクイベントの可能性が高い場所から遠ざける。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、環境リスク事象の可能性が高い場所からビジネスクリティカルな機器を遠ざける責任を負う。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、自然災害、サイバー攻撃、停電などの環境や人為的なリスクからインフラを保護する上で、さまざまな課題に直面している。これらのリスクは、ビジネスに重大なダウンタイム、データ損失、経済的損害をもたらす可能性がある。 これらのリスクを軽減するために、CSP は以下のベストプラクティスを含む（ただし、これらに限定されない）包括的な戦略を実施する必要がある： a. 環境リスク評価： i. リスクアセスメントを実施し、地理的に異なる場所における潜在的な自然環境リスク（例えば、火災や洪水（湛水、水道管への暴露）、ほこり、風（開いたドア／窓への暴露）、大気中の放電、太陽による地磁気嵐、自然災害（地震、津波、火山活動、土石流、地殻変動））を特定する。 ii. 産業活動、地政学的安定性、重要インフラへの近接性など、人為的なリスクや要因を考慮する必要がある（例：意図的な攻撃には、火災、洪水、原子力事故、生物学的ハザード、内乱などが含まれる）。 b. 高リスク地域からの距離： i. データセンターの立地は、自然災害の発生確率が低い地域（高潮の影響を受けやすい沿岸地域や洪水が発生しやすい地域）を選ぶ必要がある。 ii. 産業事故、政情不安、内乱の歴史がある地域を含め、人為的なリスクが生じやすい地域は避ける必要がある。 iii. 発電所、化学施設、輸送拠点などの重要なインフラからセキュアな距離を保つ必要がある。 c. 地理的多様性： i. 地域特有のリスクの影響を軽減するため、データセンターは地理的に多様な場所に設置する必要がある。 ii. 同時中断の可能性を最小限にするため、2 つのデータセンターを近接させるべきではない。	**実施ガイドライン：** CSC には適用されない。

d. ゾーニングと土地利用計画
   i. ゾーニング規制の遵守や、環境・セキュア上のリスクが確認されている地域を避けるための土地利用計画について、地元当局との協力体制を確立する必要がある。
   ii. 用地選定にあたっては、将来の開発と都市拡大を考慮する必要がある。
e. 地形：良好な地形がある場所を評価し、選ぶ必要がある（例：洪水や水関連災害のリスクを軽減するための高台、水はけや地震活動の影響を受けやすさなどの局所的な地形要因）。
f. 規制の遵守：データセンターの建設と運用に適用される国内および国際的な規制を遵守する。
g. 緊急事態への備えと対応：各拠点特有のリスクに合わせた緊急事態への備えと対応計画を策定し、定期的に更新する。
h. 保険の適用範囲：環境災害や事業の中断など、選択した場所に関連する潜在的リスクに対する保険に加入する。
i. サプライヤとベンダーの評価：電力プロバイダーやネットワーク・キャリアなどの重要なサプライヤやベンダーの回復力を評価し、それらが低リスク地域に位置していることを確認する。
j. 継続的なモニタリングと評価：選ばれた場所の継続的な適合性を評価するための継続的モニタリングプログラムを実施し、リスク評価と緩和戦略を定期的に見直し、選ばれた場所に影響を及ぼす可能性のある規制の変更に応じて更新する。

Control Domain DSP

2.7 データセキュリティとプライバシーのライフサイクル管理(DSP)

Control Title	Control ID	Control Specification
セキュリティおよびプライバシーについてのポリシーと手順	**DSP-01**	データの分類、保護、取り扱いに関するポリシーと手順を、そのライフサイクルを通じて、適用されるすべての法律および規制、標準、およびリスクレベルに応じて確立し、文書化し、承認し、伝達し、適用し、評価し、維持する。少なくとも年1回、ポリシーと手順を見直し、更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の実施責任は、CSP と CSC で独立して共有される。なぜなら、CSP と CSC の両方が、それぞれの組織の包括的なデータガバナンスフレームワークの一部として、データライフサイクル管理のためのポリシーと手順を独立して設立する必要があるためである。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン **全てのサービスモデルに適用：** CSP は、データのライフサイクル全体を通して、データ分類、プライバシー、保護、および取り扱いの包括的なフレームワークをポリシーと手順に含めるべきである。これには、明確に定義されたデータ保管標準及びセキュアなデータ廃棄方法が含まれる。ポリシーは、利用者データのセキュリティを確保するために、関連規制の準拠、定期的なセキュリティ監査、および継続的な監視を重視するものとする。 ポリシーには以下に関する規定が含まれるべきである（ただし、これに限定されない）： a. 範囲と目的 i. ポリシーの範囲と目的、達成すべきこと ii. 経営幹部、リーダーシップ委員会（EXCO）、および／または取締役会レベルのメンバーによ	**実施ガイドライン** **全てのサービスモデルに適用：** CSC のポリシーと手順には、機微データを適切に分類するためのガイドライン（DSP-04 を参照）を盛り込み、アクセスレベル及びセキュリティ保護要件を規定する。さらに、ポリシーは、データライフサイクル全体を通じて相互に合意されたセキュリティ目標を確実に遵守するために、データのセキュアな取扱い、定期的なレビュー、および CSP との協働のための手順を定義するものとする。 CSP のポリシーが適用される。

る正式な承認 iii. 収集、作成、送信、保管、使用、共有／開示を含むがこれらに限定されない、データ／情報のライフサイクルの全ての段階、保存／保管および破棄 iv. 組織が事業デプロイしている関連組織、管轄区域および/または地理的地域 v. 事業体に適用される関連規制または適用される業界標準 vi. データの所有者または保管者／管理者となる利害関係者（例えば、利害関係者には顧客、ビジネスパートナー、第三者、従業員が含まれる） vii. 関連する全ての利害関係者にポリシーを伝達するための要件。ポリシーと手順の伝達は、全スタッフに送信される電子デジタルメーラー（EDM）、または e ラーニングプラットフォームなどの方法で処理することができる。 viii. 企業規範、目的、価値観との整合性（＝信頼管理） b. データの分類：データ分類のポリシーと手順には、以下を含めるべきである： i. 明確な定義と例を用いたデータの分類とラベル付け（例：公開、内部、制限付き、社外秘） ii. データを保存又は処理する可能性のある資産の資産評価（例えば、機密性、完全性、可用性、及び財務、評判、顧客サービス、運用、規制などの影響に対して、「高」、「中」、「低」などの資産評価レーティングをマッピングしたもの。格付けは、データ／データセットに適用されるラベルと、それが表す全体的なリスクに基づいて決定されるべきである。 iii. 特に従業員／個人の入社前に、関係する全ての利害関係者に「利用同意書（AUA）」を伝え、署名してもらう必要がある。AUA は、データを保護する意識と意思を確認する宣言であるべきである。 iv. インフラストラクチャのさまざまなレイヤー（電子メール・ゲートウェイ、エンドポイントなど）でデータ／情報に自動的にラベルを付けるか、エンドユーザーが分類を選択できるようにする技術の導入を検討すべきである。 v. データと資産の分類は、技術資産やサービスが設計され、最終的に生産に入る前に行われるべきである。インベントリ内の全ての資産に資産価値評価を割り当てるべきである。 vi. 全てのデータとそれに関連する資産が計上されていること（すなわち、データと資産のインベントリが存在すること）	

vii. データ所有者、スチュワード／管理者、処理者のいずれかの役割を果たす各役割または個人のタスクを明記した RACI（Responsible, Accountable, Consulted, and Informed）マトリックス。

viii. データフロー図は、特定のデータ要素がエコシステム内をどのように流れ、どこに保存・処理されるかを理解するために利用できるべきである。

注：管理策の実装の観点から、CSP は、既知の規制（HIPAA、PCI-DSS など）やカスタムルール（金融データや専有データなど）に基づいてデータを分類してラベル付けできるクラウドアクセスセキュリティブローカー（CASB）ソリューションや、DLP を提供すべきである。

c. データプライバシー：データプライバシーのポリシーと手順には、以下を含めるべきである：

i. データの最小化、特に個人情報保護規制との整合性を確保することを目的としたデータ収集時の最小化

ii. どのようなデータが収集されるのか、どのように使用されるのか、誰がデータにアクセスできるのか、誰と共有または開示されるのか（第三者を含む）、いつまで保持されるのか、どのように保護されるのかを網羅したプライバシー通知。実装の観点から、プライバシー通知は、ポップアップ、バナー、レイヤー通知、または同様の形式を取ることができる。

iii. 同意、選択、収集の制限、データの質、信頼できる情報源、一次的及び二次的使用、内部及び外部開示などの追加概念

iv. データ主体へのアクセスと、それがどのような条件の下で提供されるか（すなわち、データ主体が自分のデータにどのようにアクセスおよび／またはエクスポートできるか、また、プライバシーに関する質問や懸念がある場合に組織にどのように連絡できるか）。

d. データの取り扱いと保護データの取り扱いと保護に関するポリシーと手順には、以下を含むべきである：

i. データ保護管理は、データの分類、それに関連するラベル、および（必要な承認が取られている）データを保管または処理する資産の全体的な価値に見合ったものでなければならない。

ii. 論理的管理には、保存中および移動中のデータの暗号化、使用中のデータに対する Trusted Execution Environments（TEE）の使用、認証、認可（アクセス制御とアクセス許可）、監査証跡、デジタル著作権管理（DRM）、データ漏洩防止（DLP）、アウトバウンド

プロキシ、SSL/TLS バイパス、データベースアクセス管理（DAM）、匿名化、トークン化、仮名化などが含まれるが、これらに限定されない。

注：暗号化の種類、アルゴリズム、鍵のサイズ、鍵の管理については、CCM の「暗号、暗号化、鍵の管理」ドメインを参照すること。

iii. 鍵、生体認証、スマートカード、耐火金庫の開錠のための二重管理義務などの物理的なアクセス管理を含むが、これらに限定されない。
iv. 極端な温度、湿度、火災、その他の自然現象に対する保護を含むがこれに限定されない環境管理
v. 戦争行為（テロリズム、生物・化学兵器など）に対する保護を含むが、これに限定されない追加的な規制
vi. ハードコピーおよびデジタルのあらゆる種類のデータの取り扱い管理
vii. エンドポイント、サーバー、モバイルデバイス、リムーバブルメディア(USB ドライブ、SD カードなど)、バックアップメディア（バックアップテープの暗号化など）など、さまざまな種類のデバイス上のデータを保護。
viii. データの機密性、完全性、可用性を確保するための事業継続および災害復旧対策（例：特別な ランサムウェア攻撃からの復旧のためのエアギャップ保管庫、オフサイトのテープ、ホットサイト、ウォームサイト、コールドサイトからの復旧、定期的な復旧テスト）
ix. 外部セキュリティテスト、脆弱性評価、認証のアプローチ
x. リスク管理のアプローチと責任の共有
xi. セキュリティインシデントおよびデータ侵害通知を管理するためのアプローチ。

e. データの保管と保持：データ保管・保存のポリシーと手順には、以下を含むべきである：
i. 法律、規制、ビジネス要件に従ってデータを保持する期間／期間
ii. 顧客データ、バックアップ、監査ログ、フォレンジック調査に役立つデータを含むがこれらに限定されないデータの種類
iii. 証拠の収集・保持、ハードコピー記録、モニタリング、記録の仕組みに関する要件
iv. 記録の改ざん防止を含む、管理の連鎖（Chain of custody）の取り扱い
v. 記録管理およびその他の記録要件に関する組織のトピック別ポリシーと整合させる。
vi. 満たすべき要件に応じて、必要な記録を許容できる期間と形式で検索できるように選択する。

vii. 保管および取り扱い手順は、記録媒体のメーカーが提供する推奨事項に従って実施される。記録の保管に使用される媒体の劣化の可能性を考慮すべきである。 viii. 記録の文脈、内容、構造を記述するメタデータの取り扱い、および長期にわたる管理 f. データ破棄：データ破棄のポリシーと手順には以下を含めるべきである： i. CSC によるサービス終了、一定期間（例えば 30 日）経過後の自動削除（該当する場合）、または CSC の要請があった場合、もしくは保存デバイスが寿命に達した場合等、データが破棄される条件。 ii. データを破壊するために使用される具体的な方法（暗号消去、ゼロの書き込み、デゴーシング（消磁）、物理的破壊、またはメディアのサニタイズガイドラインに従った方法など）。 g. 承認組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与 i. ポリシーと手順の変更または修正については、承認プロセスを確立すべきである。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。 h. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進すべきである。 i. 維持と見直しデータの分類、保護、および取扱いに関するポリシーと手順は、進化するクラウドセキュリティの状況との整合性を確保し、クラウド技術、規制、およびリスクの変化を反映するために、少なくとも年 1 回は文書化し、見直し、更新する。	

Control Title	Control ID	Control Specification
セキュアな廃棄	**DSP-02**	業界で認められている方法を用いて、ストレージメディアからデータをセキュアに廃棄し、いかなるフォレンジック手段によってもデータが復元できないようにする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines

CSP	CSC
管理策所有権の根拠； DSP-02 の実施責任は共有され、CSP と CSC の両方で実装する必要がある。これは、CSP または CSC のいずれかが、固有の要件（例えば、規制、記憶媒体の耐用年数の終了）に応じて、記憶媒体からデータをセキュアに廃棄することを求められる可能性があるためである。 CSP は、CSC から要求されたとき、または保管デバイスの寿命が尽き、廃棄する必要があるときに、取得不可能な方法でデータを削除する、業界で認められている方法をサポートする技術的能力を有することが期待されるため、この管理も「依存」である。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** a. データ廃棄の承認：データ廃棄要求の承認手順を確立する。権限を与えられた担当者のみが、そのような要求を開始し承認できるようにする。 b. 廃棄要求後のアクセスの制限： CSP は、データ削除要求が提出され承認された後は、データへの新たなアクセスを許可しないようにする。 c. データ廃棄オプション：様々なデータ廃棄オプションを検討し、データの機密性、メディアの種類、規制要件に基づいて最適な方法を選択する。 d. 敷地外輸送の制限：データメディアストレージは、サニタイズまたは破壊されることなく、組織の構外に持ち出したり、CSP のデータセンター外に持ち出したりすることを許可されるべきではない。 e. データの破棄：物理的なメディアを廃棄する前に、そのようなメディアに保存されている全てのデータを、業界 承認の方法を用いて完全に破壊しなければならない。ストレージデバイスからデータを復元不可能にするために、セキュアなデータ消去手順を導入する。これには、メディアの物理的破壊（ハードドライブの消磁、紙のシュレッダーなど）、データ暗号化消去、またはソフトウェアベースの消去方法が含まれる。 f. 暗号消去： i. データを暗号化し、暗号鍵を破棄することで、データを復元不可能にする。 ii. CSP は、鍵マテリアル（鍵、シード、初期化ベクタを含むがこれらに限定されない）がフォレンジック的に健全な方法で削除されることを確認するものとする。 g. データ消去：廃止プロセスの一環として、または CSC によるデータ消去の要求に基 づき、NIST SP 800-88 Guidelines for Media Sanitization、または DOD 5220.22-M に規定されているような方法など、業界で受け入れられている方法に基づき、メディア上のセキュアな論理的または物理的な	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。 CSC に関するその他のガイドラインは以下の通り： a. 稼動データとバックアップデータの廃棄：CSC は、稼動データとバックアップデータの両方の記憶媒体からデータを確実に削除すべきである。 b. 暗号化消去：CSC は、利用でき且つ可能な場合、暗号化消去を可能にする管理鍵を導入すべきである。 c. CSP との契約合意： i. CSP との契約において、データ廃棄要件が明確に規定され、CSP が組織のデータ廃棄ポリシーを遵守していることを確認する。 ii. データの論理的および物理的な破棄は、データの分類に見合ったものであり、要求される法規制に沿ったものである。 注：アクティブストレージシステムは本番サーバーであり、バックアップストレージシステムはアクティブストレージシステムのフルまたは増分バックアップ／コピーである。

データ消去方法（ゼロ化、クロスカットシュレッダー、脱気、焼却、または粉砕を含むが、これらに限定されない）を使用すべきである。 h. データ破棄の検証：文書化され、監査可能な検証メカニズムを通じて、廃棄メディア上のデータの完全な破壊が成功したことを検証するための体系的なプロセスを要求する。 i. 機器廃棄業者の認定：認定された業界標準を遵守し、データの適切な廃棄を証明する文書を提供する認定データ廃棄業者を利用する。 j. 廃棄の記録管理と監査：全てのデータ廃棄イベントの詳細な記録を、クリア、パージ、または破棄されたかを明確に示すメディア廃棄のデジタル証明書とともに追跡システムに維持する。記録には、監査およびコンプライアンス目的のため、日付、データの種類、廃棄方法、廃棄日、関係権限者、および検証結果を含めること。 k. 稼働データとバックアップデータの廃棄：データは、一時的なファイルや古いファイルが保存されている場所を含むがこれに限定されない、稼働とバックアップの両方のストレージメディアから削除されるべきである。 l. データ廃棄の変更管理：全てのセキュアなデータ廃棄プロセスは、明確に定義された変更管理承認プロセスを用いてのみ実施されるべきである。 m. データプライバシー規制の遵守：データ廃棄プロセスが、一般データ保護規則（GDPR）やカリフォルニア州消費者プライバシー法（CCPA）など、適用される全てのデータプライバシー規制に準拠していることを確認する。 n. 定期的な監査とレビュー：継続的なコンプライアンスと有効性を確保するために、物理的なメディア廃棄とデー タ破棄の両方を含む、データ破棄プロセスの定期的な監査とレビューの予定を定める。 注：アクティブストレージシステムは本番サーバーであり、バックアップストレージシステムはアクティブストレージシステムのフルまたは増分バックアップ／コピーである。	

Control Title	Control ID	Control Specification
データインベントリ	**DSP-03**	少なくとも機微なデータや個人情報については、データインベントリを作成し、維持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の所有権は「互いに依存する形で共有」と定義される。なぜなら、両当事者がデータインベントリの実施と維持に責任を負うため、CSP は、CSC カスタマーデータ（該当する場合及び可能な場合）及びクラウド派生データのインベントリを維持する必要があり、CSC は、少なくとも機微データ及び／又は個人データのインベントリを維持する必要がある。 この管理策はデータディスカバリとして知られる重要なデータインベントリ活動を実行するために CSP が利用可能な技術的能力に依存するため、「依存」である。また、CSP は、e-ディスカバリを含む法的な要求に応じる際に、CSC の機微データまたは個人情報へのアクセスを要求する可能性がある。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 少なくとも「機微」または「個人データ」と表示されているデータ（バイオデータなど）については、データのライフサイクル全体を通じて、データフィールドの包括的なインベントリ（以後、データインベントリと呼ぶ）を作成し、維持する必要がある。また、コンプライアンス要請に対応するために必要なデータも含めるべきである。 データインベントリは以下である： a. CSC データと CSP 由来のデータを明示的に識別する。 b. 機微データや個人データの場所（クラウドサービスの識別など）、量、コンテキストを可視化する。これは、データディスカバリや定期的な監査などの方法を用いて行うことができる。 c. 構造化データ（データベースに保存されているものなど）、非構造化データ（ファイルや電子メールに保存されているものなど）、メタデータを含むが、これらに限定されないデータタイプをカバーする。 d. 特定、エクスポート、削除が困難なデータの特定 e. 機微な個人データの使用方法、アクセス権限者、共有者、保存場所、保存期間を詳細に説明すること。 f. 組織内、組織間、組織外（サードパーティー、ビジネスパートナー、ベンダーなど）でのデータの動きを追跡する。 g. データがどのように保護され、組織内の誰がデータ保護に責任を持つかを明記する。 h. 初期のマスターリストとしてデータインベントリマト	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

リックスを含め、特定の条件下または日常的に自動バッチ処理を実行するべきである。これにはシステムアーキテクチャの変更、データの分類の変更、当該データの保管、転送、処理に基づくリスク態勢の変更、法律や規制の変更などを含み、（ただしこれらに限定されない）これにより、データインベントリを定期的に更新する。	

Control Title	Control ID	Control Specification
データ分類	**DSP-04**	データをタイプと機微のレベルに応じて分類する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； IaaS の場合、この管理策は、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。それは以下の理由からである： • CSC は IaaS をよりコントロールすることができ、データ分類を行うために好きなツールをインストールすることができる。 • CSP は、IaaS インフラによって生成されたデータ（クラウド派生データなど）を分類する必要がある。 CSP と CSC はデータの種類に応じて独立に分類できるため（例えば、CSP は IaaS サービ スのログデータ／クラウド由来データを分類したい。一方で CSC は IaaS に保管する機微データや個人データを分類したい。）、IaaS の管理策所有権は「独立」である。 PaaS と SaaS の場合、この管理策は、CSP と CSC の両者で「互いに依存する形で共有」し、それぞれ実施する責任がある。それは以下の理由からである： • CSC は基礎となるインフラストラクチャをあまり制御できず、データを分類するツールを提供するために CSP に依存しなければならない。 • CSP は、CSC とクラウドサービスとの相互作用に基づ	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。

いてクラウド由来のデータを分類する必要があるため、CSC に依存する。	
実施ガイドライン： **全てのサービスモデルに適用：** a. データを分類し、明確な定義と例（公開、内部、制限、機密など）を用いてラベル付けする。ラベルはセキュリティとプライバシーの両方の属性を含むべきである。カーネギーメロン大学（Carnegie Mellon University）のようなラベル付け標準がある：データ分類のためのガイドライン」や「SANS Institute：データ漏洩を防ぐためのデータへのタグ付け（コンテンツリポジトリの形成）を考慮すべきである。 b. 例えば、機密性、完全性、可用性、財務、風評、顧客サービス、運用、規制などの影響に対して、「高」、「中」、「低」のような資産評価レーティングがマッピングされている）が存在するはずである。格付けは、データセットに適用されるラベルと、それが表す全体的なリスクに基づいて決定されるべきである。 c. インフラのさまざまなレイヤー（電子メール・ゲートウェイ、エンドポイントなど）でデータに自動的にラベルを付けるか、エンドユーザーが分類を選択できるようにする技術の導入を検討すべきである。 項目 c に関する注記：管理策の実装の観点から、CSP は、既知の規制（HIPAA や PCI-DSS など）またはカスタムルール（財務データや専有データなど）に基づいてデータを分類してラベル付けし、データ漏えい防止（DLP）を実行できるクラウドアクセスセキュリティブローカー（CASB）ソリューションを提供すべきである。 d. データおよび資産の分類は、テクノロジー資産またはサービスが設計され、本番稼動する前に行われるべきである。インベントリ内の全ての資産に資産価値評価を割り当てるべきであるが、クラウド由来のデータはこの推奨事項の例外である。 e. データ所有者、スチュワード／管理者、処理者のいずれかの役割を果たす各役割または個人のタスクを明記した RACI マトリックスが存在すること。 f. データ保護管理は、データの分類、関連ラベル、データを保管または処理する資産の全体的な価値に見合ったものであるべきであり、以下を含むべきであるが、これらに限定されない： i. 輸送中のデータの暗号化、認証、認可（アクセス制御とアクセス許可）、監査証跡、デジタル著作権管理（DRM）、DLP、アウトバウンドプロキシ、SSL/TLS バイパス、データベースアクセス管理（DAM）、匿名化、トークン化、仮名化を含むが、これらに限定されない論理的管理。暗号化の種	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。 さらに、CSC は、提案依頼書（RFP）提出時に CSP が提供するデータ分類およびラベル付け技術を考慮すべきである。

類、アルゴリズム、鍵のサイズ、鍵管理は、暗号化・暗号化・鍵管理（CEK）管理ドメインで参照する。 ii. ロック＆キー、バイオ、スマートカード、耐火金庫およびカメラの開錠のための必須デュアル管理策などの物理的アクセス制御を含むが、これらに限定されない。 iii. 極端な温度、湿度、火災、その他の自然現象に対する保護を含むがこれに限定されない環境制御 iv. 戦争行為（テロリズム、生物・化学兵器など）に対する保護を含むが、これに限定されない追加の規制 g. データの取り扱いには、ハードコピーやデジタルデータなど、あらゆる種類のデータの管理が含まれる。 h. エンドポイント、サーバー、モバイルデバイス、リムーバブルメディア（USB ドライブ、SD カードなど）、バックアップメディア（バックアップテープの暗号化など）など、さまざまなタイプのデバイス上のデータ保護。 i. データの機密性、完全性、可用性を保証する事業継続および災害復旧対策（例：ランサムウェア攻撃から復旧するための特別なエアギャップ保管庫の使用、テープのオフサイト化、ホットサイト、ウォームサイト、コールドサイトからの復旧、定期的な復旧テスト j. データおよび資産の分類の見直しは、少なくとも年 1 回、またはデータの分類の変更や法規制の変更など（ただしこれに限定されない）一定の条件に基づいて実施すべきである。	

Control Title	Control ID	Control Specification
データフロー文書	**DSP-05**	どういったデータがどこで処理され、保存され、伝送されるかを明確にするために、データフロー文書を作成する。データフロー文書は、定められた間隔で（少なくとも年 1 回）、および変更があった場合にレビューする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines

CSP	CSC
管理策所有権の根拠； この管理策の所有権は、「互いに独立した形で共有」と定義される。「共有」とは CSP と CSC の双方が、どのデータがどこで処理され、保存され、伝送されるかを知る必要があるためである。「独立」とは、CSP が CSC に依存することなく、またその逆もなく、文書を作成できることを意味する。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** データフローダイアグラム（DFD）文書は、以下を視覚的に表現したものでなければならない： a. 最低限、機微データ（個人情報、極秘、秘密、制限、内部と表示されたデータなど）がどこで処理、保管、伝送されるかを明示すべきである。 b. ソース*（通常、接続の起点となる場所）、宛先*（通常、接続の終点となる場所）、サブジェクト**（ユーザー、システム/資産、またはプロセス）、およびオブジェクト（システム/資産、またはプロセス）。サブジェクトまたはオブジェクトには、データが保存、処理、または伝送される技術コンポーネント（別名、システムまたは資産）が含まれる可能性があるため、これらを効果的に描写する推奨方法は表示されるコンポーネントの詳細のバランスを維持することである（例えば、使用されている技術に名前を付ける）。これにより、技術的、非技術的を問わず、ほとんどの利用者が容易に理解できるようになる。 c. 通信が一方通行か双方向かを示す矢印 d. ソース、宛先、サブジェクト、オブジェクトの間をデータがどのように移動するかを表す。これを描写する一つの推奨される方法は、情報の連続的な流れを示す数字（例えば、1→2、2→3、3→4）を使用し、データが実際にどの方向に流れているかを示す矢印と組み合わせることである。また、モニタリングやデータ取得における地理的な違いを考慮するため、データがどこに存在するかを理解するためのアプリケーションスタックマップを導入することも推奨される。 e. 必要に応じて、データに対する操作の種類（例：読み取りと読み取り/書き込み）、データ送信に使用されるプロトコル（例：HTTP、SMTP、REST）などの追加情報***、ポート番号（例：443、80）、内部ネットワークと外部ネットワーク（例：公衆インターネットとバックエンドデータベース）の分離を強調する境界線を含めるべきである。 f. ワイヤーフレームを使ってデータフローを構成するのも、データの流れを説明するのによく使われる方法である。 g. データの作成、使用、共有、アーカイブ、破棄に至る	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

データライフサイクルの様々な段階

h. DFD 文書は、少なくとも年 1 回、またはデータの保存、処理、送信先に関する重要な変更があった場合、あるいはデータの分類が変更された場合（例えば、以前は機微な個人データを保存していなかった資産が、そのようなデータを保存するようになった場合）、見直し、更新されるべきである。

i. DFD は、SDLC のシステム設計の段階で、文書化の準備ができ、完成していなければならない。このアプローチは、高レベル設計（HLD）がより包括的で、完成され、実装可能である確率が高い。

j. 可能な場合、CSP および CSC は、システムエンジニアリングチームと協力して、全てのシステムコンポーネントサーバ（We アプリケーション、Windows、データベース、ネットワーク、SAN、インターネットなど）とデータの流れを示すシステム論理設計（SLD）を設計し、最終的な設計と実装について関係者全員でレビューする。

*例としては、以下のようなものがある（ただし、これらに限定されるものではない）：

- 全世界に公開されているシステム（すなわち、0.0.0.0 に公開されているシステム）
- 限定された人／数のシステムに公開されるシステム（例えば、ベータ版顧客デバイスのグループにのみ公開されるなど）
- ビジネスパートナーに公開されるシステム
- 第三者に公開されるシステム

**例としては、以下のようなものがある（ただし、これらに限定されるものではない）：

- お客様
- ビジネスパートナー
- ベンダー
- サードパーティ
- 一般大衆

***一般的に、DFD はルーターやスイッチのような低レベルのネットワークコンポーネントについては詳述しない。とはいえ、ファイアウォール、侵入防御システム（IPS）、ファイルスキャン＆サンドボックスシステム、コンテンツデリバリーネットワーク（CDN）など、その他のコンポーネントが DFD に含まれている可能性はある。

Control Title	Control ID	Control Specification

データ所有と管理	**DSP-06**	全ての関連する個人情報および機微なデータの所有および管理責任を文書化する。少なくとも年 1 回のレビューを行う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の所有権は、「互いに独立した形で共有」と定義される。「共有」とは、CSP と CSC の両方が、それぞれのデータ所有、スチュワードシップ、およびカストディアンシップの責任を文書化する必要があるためである。「独立」とは、CSP と CSC は互いに依存することなくこれを行うことができるからである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** データ責任マトリクスを定義し、文書化し、伝達することができる。マトリックスには、以下に限定されないが、以下を含むべきである： a. 最低限、データの種類には個人データ、機密とラベル付けされたデータを含める。別のラベルとしては、機密、制限、極秘、最高機密またはそれに類するもの)、およびデータ保存期間。 b. データの所有者またはスチュワードとして機能する個人の名前または役割。RACI マトリクスを追加することを推奨する。 c. データ所有者、データスチュワード（企業、機能、その他)、データ管理者、データ消費者、データ生産者、データ保護責任者という用語が何を意味し、データに対して何をすることが許されているのかについての明確な定義。 d. 各データ要素／フィールドに関連する義務。これには規制、契約、その他の義務が含まれる。 e. 文書化された個人データおよび機微データを見直す頻度。少なくとも年 1 回見直す。 f. データ責任マトリクスは、ポリシー、標準、電子メール、教育ワークショップ、オンラインセキュリティ意識向上プログラムを含むがこれらに限定されない方法で、組織内の全ての利害関係者に周知されるべきである。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
デザイン段階からのデータ保護とデフォルト設定	**DSP-07**	セキュリティバイデザインの原則と業界のベストプラクティスに基づいて、システム、製品、およびビジネスプラクティスを開発する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の所有権は、「互いに依存した形で共有」と定義される。共有される理由は、CSP と CSC が、実装を希望する製品およびサービスについて、設計によるセキュリティ／プライバシー活動を完了する必要があるためである（例えば、CSP は提供しようとする製品またはサービスについて活動を実施し、CSC はその製品またはサービスを自社の利害関係者（顧客、ビジネスパートナー、従業員、第三者、または一般市民）に提供するために同様の活動を実施する）。 依存の理由は、両当事者はセキュリティとプライバシーの「組み込み」において互いに依存しているためである。例えば、CSP は、既存の製品やサービスを改善するためのインプットとして CSC のフィードバックに依存する。CSC が CSP に依存するのは、設計によるセキュリティとプライバシーを実現するためには、セキュリティアーキテクトが上位レイヤー部にメリット、デメリット、コストとともに選択肢を提案する必要があるからである。そのため、CSC は、（CSP マーケットプレイスまたはネイティブなど）利用可能な製品の数々や、CSC のクラウドおよび／またはハイブリッドのエコシステムに適したセキュアな方法で実装する方法について完全な知識を持っていない可能性があるため、CSP への依存が不可欠になる。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** a. セキュリティ及びプライバシーの設計活動を開始する前に、少なくとも、データ及び資産のインベントリ、データの分類及び資産の評価、DFD の文書化及び HLD を完了しておく。これは、設計されるセキュリティ又	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。 また、以下は CSC のみに適用される： a. RFP 及び見積依頼書（RFQ）の選定に使用されるチェ

はプライバシー管理が、データ及び関連資産の価値に見合ったものであり、効率的な方法で実行できることを確実にするための前提条件として推奨される。

b. セキュリティ及びプライバシー・バイ・デザインの活動は、最低限、DFD と HLD 文書を検討することから始めるべきである。可能であれば、低レベル設計（LLD）もレビューする。

c. この活動の一環として、脅威モデリングを実施し、特定の脅威行為者（スクリプトキディ、ハクティビスト、犯罪者、国家など、誰が）特定の資産を攻撃する可能性があるか、その動機（金銭、政治、スパイ活動など）は何か、具体的にどのような脅威（どのような方法で攻撃するか、どのような弱点を突くか）が資産やデータのセキュリティ及び／又はプライバシーに与えるかを想定する。脅威モデリングは、STRIDE、DREAD、PASTA などのアプローチやフレームワークを使用して実行することができる。組織内でスクラムやかんばん方式などのアジャイル手法を使用している場合、脅威モデリングは、スプリント中に作成される全てのユーザーストーリーについて、悪のストーリーや悪用事例を文書化することによって実施できる。また、信頼境界の概念、隔離、各資産に影響を及ぼす脅威、推奨される対策を視覚的に描いた脅威モデリング図を作成することも推奨される。脅威は、人、プロセス、技術に分類することができる。

d. 脅威モデリング後は、セキュリティ要件を詳述した包括的なセキュリティパターン*を作成する。セキュリティ要件は、特定された脅威、潜在的な弱点、規制要件を考慮し、データの保存、処理、送信を行う資産の予防、検知、対応、回復につながる対策を推奨する。NIST の「識別（Identify）」、「保護（Protect）」、「検知（Detect）」、「対応（Response）」、「復旧（Recovery）」モデルは、推奨されるベースラインとして適用されることがある。

e. セキュリティ要件は、フィージビリティスタディから、設計、構築、実行（運用）、保守に至るまで、SDLC の全ての段階で作成されなければならない。

f. これには、設計範囲に含まれる全ての技術資産と、それらの資産間のネットワーク接続が含まれるが、これらに限定されない。

g. セキュリティ要件は、人（例：ユーザー教育、顧客教育）、プロセス（例：顔認証や初回に電子メールで送信されるワンタイムコードなど、複数の認証方法を介したモバイルバンキングアプリカスタマー登録）、テクノロジー（例：サードパーティーに接続する全ての API の双方向 TLS）に関わるシナリオをカバーする必要がある。

h. セキュリティ要求事項の一部は、プライバシーにも適用される可能性があるが、 DAM の認証、認可、およびチェックリストに、必要なセキュリティ要件を全て規定すべきである。

b. データの移行（例えば、レガシーシステムからマイクロサービスベースの実装へ、あるいは、本番環境からテスト環境へ）、ファイルのアップロード／ダウンロード（例えば、マルウェアのスキャン、サンドボックス化、ファイルサイズの制限）をカバーするシナリオのセキュリティ要件については、特に注意を払う必要がある。

c. 基本サービス契約（MSA）には、特定の管轄区域の規制当局が義務付ける特定のセキュリティ要件、技術的債務を軽減し、長期的にサイバーセキュリティリスクを軽減する管理策の実施を支援する一般的なセキュリティ要件、および（サプライチェーンリスクをカバーするために）CSP の下請業者および／または依存当事者に適用される要件を含むが、これらに限定されない、セキュリティ要件をカバーする条項を含めるべきである。

d. 特定の CSP を選定するために実施される RFP/RFQ の一部であるチェックリストの一部として、 CSC が推奨するセキュリティ条項のリストを CSP に送付する。セキュリティ条項のサンプルには以下が含まれるが、これらに限定されない。

   i. Critical または High と評価された脆弱性またはリスクの改善に関する SLA

   ii. CSC に報告書を送付する頻度（例えば、年 1 回）を特定した上で、定期的に CSP による脅威及び脆弱性の管理を行う。

   iii. 製品のセキュリティ（例：製品はマルウェアやバックドアがないこと）

アカウンティング（AAA）を含むべきであるが、これらに限定されるものではない。 注：AAA の概念は、MFA、役割ベースまたは属性ベースのアクセス制御（RBAC/ABAC）、条件付きアクセスポリシー、特権アクセス管理（PAM）などの概念をカバーするアイデンティティおよびアクセス管理セキュリティ要件によってもカバーされる。 i. アプリケーションセキュリティ（例えば、Web 向け ASVS、モバイルアプリケーションセキュリティ検証標準 MASVS、OWASP Top 10 API、CI/CD 向け OWASP Top 10 への整合性） j. インフラセキュリティ（例：業界標準ベンチマークに基づく技術資産の強化） i. ネットワークセキュリティ（移動中のデータのセキュリティ、双方向 TLS の使用、TLS のバージョンと推奨暗号など） ii. 透過的データ暗号化（TDE）、ボリュームベース暗号化、ストレージベース暗号化などの概念を用いた保存中データの暗号化、フォーマット保持暗号化（FPE）、および順序を保持する暗号化を考慮すべきである。 iii. ロギングギングと監視（LOG ドメイン参照） iv. インシデントレスポンスとフォレンジック（LOG ドメイン参照） v. 事業継続と災害復旧（LOG ドメイン参照） 注：暗号化もプライバシー・バイ・デザインの重要な管理策である。重複を避けるため、プライバシー・バイ・デザインのセクションにはあえて記載していない。ここで述べられている推奨事項は、DSP-07 と DSP-08 に適用される。 k. セキュリティ管理策は、作成から使用、共有、アーカイブ、破棄に至るまで、データライフサイクルのあらゆる段階に組み込まれるべきである。 *セキュリティパターンとは、同一または類似のユースケースに対して反復可能な方法で使用できるセキュリティ要件を定義した、文書化されたアプローチのことである。	

Control Title	Control ID	Control Specification
データプライバシー・バイ・デザインとデフォルト構成	**DSP-08**	プライバシー・バイ・デザインの原則および業界のベストプラクティスに基づいて、システム、製品、およびビジネスプラクティスを開発する。適用されるすべての法律および規制に従って、システムのプライバシー設定がデフォルトで構成

		されていることを確認する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の所有権は、「互いに依存した形で共有」と定義される。「共有」とは、CSP と CSC は、実装を希望する製品およびサービスについて、プライバシー・バイ・デザインおよびデフォルトの活動を完了しなければならないからである（例えば、CSP は CSC に提供しようとする製品またはサービスについて活動を実施し、CSC はその製品またはサービスを自社の利害関係者（顧客、ビジネスパートナー、従業員、第三者または一般市民）に提供するために同様の活動を実施する）。 「依存」の理由として、両当事者は（DSP-07 で特定されるセキュリティ管理ガイダンスを通じて）プライバシーの侵害について互いに依存しているためである。例えば、CSP は、既存の製品またはサービスを改善するためのインプットとして CSC のフィードバックに依存する。設計及び既定によるプライバシーでは、セキュリティアーキテクトが上級管理職の利害関係者に利点、欠点及びコストを伴う選択肢を提案する必要があるため、CSC は CSP に依存する。そのため、CSC は（CSP のマーケットプレイスまたはネイティブなど）利用可能な製品群や、CSC のクラウドおよび／またはハイブリッドのエコシステムに適合するセキュアな実装方法について完全な知識を持っていない可能性があるため、CSP への依存が不可欠になる。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** a. プライバシー・バイ・デザイン及びデフォルトの活動を開始する前に、データ及び資産のインベントリ（管理 DSP-03 による）、データの分類及び資産の評価（DSP-04 による）、DFD 及び HLD を最低限完了しておくべきである。これは、セキュリティまたはプライバシーの管理が、その価値に見合ったものであることを保証するための前提条件として推奨される。 データおよび関連する資産に関する情報を、効率的な方法で実行することができる（すなわち、セキュリテ	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。 また、以下は CSC のみに適用される： a. 要求されるプライバシー要件は全て、CSP の選定に使用されるチェックリスト（RFP、RFQ）に規定されるべきである。 b. データの移行（レガシーシステムからマイクロサービスベースの実装へ、あるいは本番環境からテスト環境への移行など）をカバーするシナリオでは、プライバシー要件に特別な注意を払う必要がある。

ィとプライバシーの管理体制の構築に関する決定が、手元にある完全かつ正確な情報に基づいて行われる)。

b. プライバシー・バイ・デザインの活動は、最低でも DFD と HLD を検討することから始めるべきである。可能であれば、LLD も検討すべきである。

c. この活動の一環として、脅威モデリングを実施し、特定の脅威行為者(スクリプトキディ、ハクティビスト、犯罪者、国家など、誰が)特定の資産を攻撃する可能性があるか、その動機(金銭、政治、スパイ活動など)は何か、また、具体的にどのような脅威(どのような方法で攻撃するか、どのような弱点を突くか)が資産やデータのセキュリティ及び/又はプライバシーに影響を与えるかを想定する。脅威モデリングは、STRIDE、DREAD、PASTA などのアプローチやフレームワークを使用して実行することができる。組織内でスクラムやかんばん方式などのアジャイル技法を使用している場合、脅威モデリングは、スプリント中に作成される全てのユーザーストーリーについて、悪のストーリーや悪用事例を文書化することによって実施できる。また、信頼境界の概念、隔離、各資産に影響を及ぼす脅威、推奨される対策を視覚的に描いた脅威モデリング図を作成することも推奨される。脅威は、人、プロセス、技術に分類することができる。

d. 脅威モデリング後は、セキュリティ要件を詳述した包括的なセキュリティパターン* を作成する。セキュリティ要件は、特定された脅威、潜在的な弱点、規制上の要件を考慮し、データの保存、処理、送信を行う資産の予防、検知、対応、回復のための管理策を推奨する。注:NIST の「識別(Identify)」、「保護(Protect)」、「検知(Detect)」、「対応(Response)」、「復旧(Recover)」モデルは、推奨ベースラインとしてここに適用されている。

e. プライバシー要求は、フィージビリティスタディから設計、構築、実行(運用)、保守に至るまで、SDLC の全ての段階で作成されなければならない。

f. プライバシー要件は、設計の全てのコンポーネントに対して作成されなければならない。これには、設計の範囲に含まれる全ての技術資産と、それらの資産間のネットワーク接続が含まれますが、これらに限定されない。

g. プライバシー要件は、人(例:ユーザー教育、顧客教育)、プロセス(例:許可されたビジネス利害関係者が、プライバシー規制の対象となるデータにどのようにアクセスするか)、技術(例:全ての JSON Web トークンは、データに対する全ての操作にデータ対象者の認証と承認が必要であることを保証するスコープセクションを含む)を含むシナリオをカバーする必要がある。

h. プライバシー・バイ・デザインの要件は、各組織の管轄区域における規制要件に沿ったものでなければなら

c. マスターサービス契約(MSA)には、特定の法域の規制当局が義務付ける特定のプライバシー要件、技術的負債を軽減し、または長期的にプライバシーリスクを軽減する管理の実装を支援する 一般的なプライバシー要件、および(サプライチェーンリスクをカバーするために)CSP の下請業者および/または依存当事者に適用される要件を含むが、これらに限定されないプライバシー要件をカバーする条項を含めるべきである。

d. 特定の CSP を選定するために実施される RFP/RFQ のチェックリストの一部として、CSC が希望する個人情報保護条項のリストを CSP に送付する。個人情報保護条項のサンプルには以下が含まれるが、これらに限定されない:

  i. データ侵害の通知(例えば、CSP は、72 時間以内に現地の規制当局に通知するという自らのコミットメントを満たすために、48 時間以内にデータ侵害を CSC に通知すべきである。
  指定された期限内に地元の規制当局に報告するという自らのコミットメントを守る。

  ii. データ処理者としての CSP、その下請業者および従属当事者に適用されるべき、特定のデータ保護要件。

  iii. 国境を越えた規制要件。

ない。

推奨されるプライバシー・バイ・デザインの要件には、以下が含まれる（ただし、これらに限定されない）：

i. データの最小化（特に、プライバシー規制との整合性を確保することを目的としたデータ収集時
j. どのようなデータが収集されるのか、どのように使用されるのか、誰がデータにアクセスできるのか、誰と共有または開示されるのか（第三者を含む）、どれくらいの期間保持されるのか、どのように保護されるのか、などを網羅したプライバシー通知。実装の観点から、プライバシー通知は、ポップアップ、バナー、レイヤー通知または同様の形式を取ることができる。
k. 同意、選択、収集の制限、データの質、信頼できる情報源、一次利用と二次利用、内部公開と外部公開などの追加概念
l. データ主体によるアクセス、およびそれがどのような条件の下で提供されるか（データ主体が自分のデータにアクセスおよび/またはエクスポートする方法、およびプライバシーに関する質問や懸念がある場合に CSP に連絡する方法など）。
m. 非摂動（マスキング、抑制、汎化、仮名化など）、摂動（ノイズ付加、マイクロアグリゲーションなど）、暗号化（同形、形式保存、決定論的、順序保存などの暗号化技術など）、k-匿名性、l-多様性などのプライバシーモデルなど、プライバシーを向上させる技術（PET）を導入する技術。
n. クロスボーダー転送中のデータ保護方法に関するルールは、規制要件に基づいて検討されるべきである。
o. デフォルトの設定/初期設定は、適用可能な地域のプライバシー規制に準拠するべきである。例としては以下のようなものがあるが、これらに限定されるものではない：
    i. 明示的な同意／選択に基づく手動でのオプトインは、データ対象者が明示的に同意するために手動でボックスにチェックを入れるか、何らかのアクションを実行する必要があり、データ対象者による手動でのオプトアウトを必要とする自動オプトインとは対照的に、デフォルトで利用可能なプライバシーオプションであるべきである。
        - クッキーについては、厳密に必要なもののみを自動的に有効にし、その他のタイプの追加クッキーは自動的に無効にする。追加的なクッキー（厳密に必要なクッキー以外）を有効にする必要がある場合は、データ対象者の明示的な同意を求めるものとする。
        - デフォルトで有効になっている場合、グラフィカルユーザーインターフェース

（GUI）は、必要最小限のデータのみを要求して（例えば、Web フォームを介して）データ収集を行うべきである（例えば、正当な使用原則に基づいて年齢範囲のみが要求される場合、特定の年齢はドロップダウンメニューで利用できないようにすべきである）。 ▪ デフォルトでは、個人情報保護に関する情報の通知方法（シンプルまたはレイヤード）は、情報主体から情報を要求されるたびに表示されるべきである。 p. CSP は、それぞれの下請業者または従属当事者との MSA に、必要なデータプライバシー条項が含まれていることを確認する必要がある（例えば、「キャリアプロバイダーは、必要な規定に従って、またはキャリアの指示に基づき、合理的な期間内あるいは直ちにデータ侵害をキャリアに通知すること（例： CSC がデータ管理者である場合）」といったデータ侵害通知条項。 q. プライバシー・バイ・デザインの管理は、データの作成から使用、共有、保管、破棄に至るまで、データライフサイクルのあらゆる段階に組み込まれるべきである。	

Control Title	Control ID	Control Specification
データ保護影響評価	**DSP-09**	データ保護影響評価（DPIA：Data Protection Impact Assessment）を実施し、適用される法律、規制および業界のベストプラクティスに従って、個人データの処理に伴うリスクの発生源、性質、特殊性および重大性を評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**

管理策権所有の根拠； この管理策の所有権は、「互いに依存した形で共有」と定義される。「共有」とは、CSC は通常データ管理者として機能し、ほとんどの場合、CSP のクラウドに置くデータを所有するため、共有される。データ管理者として、一定の条件（例えば、個人の権利と自由に高いリスクをもたらす可能性のあるデータ処理活動）によっては、データ保護影響評価（DPIA）を実施する義務がある。CSP は、個人データが CSC からクラウドに送信される可能性があるため、DPIA を実施する。 「依存」の理由として、CSC は、リスクを軽減するための措置（例：セーフガード、セキュリティメカニズム）として利用可能な CSP が提供するツールや技術を評価する必要があるかもしれないからである。一方、CSP は CSC に依存している。なぜなら、CSC が個人データをどのように処理しているかを理解するために、CSC の DPIA をインプットとして取り入れるからである。CSP は、他の CSC が DPIA のコミットメントを満たすことができるように、将来的に他の CSC に提供できる機能を製品やツールに組み込むことで、これをセキュリティやプライバシー・バイ・デザイン、デフォルトのアプローチに組み入れる。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** データ保護影響アセスメント（DPIA）は、以下の概念をカバーすべきである： a. データ処理活動の性質の説明（例：データの収集、使用、保存、削除の方法、データの共有者、データへのアクセス権者、データの保持期間など） b. 処理の範囲の説明（データの性質、特別なカテゴリのデータ、収集されるデータ量、保存期間、収集の範囲頻度、関係するデータ主体の数、処理の期間、対象地域など） c. データ処理の背景の説明（例えば、データの出所、個人またはデータ対象者との関係の性質、データ対象者が持つことになる管理レベル、データ処理に先立ち、データ対象者が持つことになる管理レベル、データ処理に先立ち、データ対象者が持つことになる管理レベル、データ処理に先立ち、データ対象者が持つことになる管理レベルなどこの種の処理の経験、社会的関心事項） d. データ処理の目的の説明（正当な利益、データ処理の目的、データ処理の利益、データ対象者への影響など） e. 関連する利害関係者との協議方法に関する検討（例：情報セキュリティの専門家による協議、特定の個人、グループ又は組織からの助言・助言を求めるなど） f. コンプライアンスと比例措置の記述（合法的根拠、データの質と最小化の確保など） g. 個人またはデータ対象者に対するリスクおよび潜在的影響（たとえば、可能性-遠隔、可能性あるいは蓋然性、	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

重大性-被害の最小、重大あるいは壊滅的、総合的リスク-低、中あるいは高など）を特定し、評価する。潜在的な影響の例としては、権利（プライバシーの権利を含むがこれに限定されない）を行使できないこと、サービスや機会を利用できないこと、個人データの使用を制御できなくなること、差別、なりすましや詐欺、経済的損失、評判の低下、身体的損害などが挙げられるが、これらに限定されない、
仮名化されたデータの再特定化、その他経済的または社会的な重大な不利益。

h. 内在するリスクを軽減または除去するための措置（保護措置、セキュリティメカニズム、その他個人データ保護を確保するためのメカニズムなど）を特定し、残存リスクの値（低、中、高など）について合意する。リスク軽減の例としては、特定の種類のデータを収集しないことを決定すること、処理の範囲を縮小すること、保存期間を短縮すること、追加の技術的セキュリティ対策を講じること、リスクを確実に予測し管理するためにスタッフを訓練すること、可能であればデータを匿名化または仮名化すること、リスクを回避するための内部ガイダンスまたはプロセスを作成すること、別の技術を使用すること、明確なデータ共有契約を締結すること、プライバシー通知を変更すること、適切であれば個人にオプトアウトの機会を提供すること、個人の権利行使を支援する新しいシステムを導入することなどが挙げられるが、これらに限定されない。

i. 結果を記録し、承認された対策と残留リスクについてサインオフする。

j. DPIA のプロセスと結果を記録するために、DPIA のテンプレートを使用することを推奨する。情報コミッショナー事務局（ICO）が推奨するテンプレートは、以下 https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf

k. DPIA は、データ処理活動を開始する前に実施されるべきである。例えば、新しいプロジェクトや戦略の計画前および計画中に DPIA を実施することが推奨される。

l. DPIA は少なくとも年 1 回見直すか、データ処理の結果リスクの変化が予想される場合に見直すべきである。

m. 必要な場合には、DPIA の実施に際してデータ保護オフィサー（DPO）の助言を得ること。DPIA は、CSC データ、サービスデータ（またはサービスにより生成されたデータ）* 及びサポートデータ** の両方について実施されなければならない。

注釈
DPIA に移行する前に、データ分類のようなプロセス（プロジェクトの開始時）においてティニシャル・スクリーニング・アセスメント（ISA）を実施することが推奨される。これは、DPIA に移

行する前に、データ分類のようなプロセス（プロジェクト開始時）において、初期スクリーニングアセスメント（ISA）を実施することを推奨する。	

Control Title	Control ID	Control Specification
機微なデータの転送	**DSP-10**	個人情報または機微なデータの転送が、不正なアクセスから保護され、それぞれの法令で認められている範囲内でのみ処理されることを保証するプロセス、手順、技術的手段を定義、実施、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： これは、CSP と CSC の双方で「互いに独立した形で共有」の管理策である。盗聴またはデータ転送の傍受による不正アクセスを防止するために、データ転送の手順と手続および技術的手段（強力な暗号化または類似の技術）を定義する必要があるためである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 管理策の実装は、サービスデリバリモデル（IaaS、PaaS、または SaaS）に固有ではない。サービスデリバリモデルに関係なく、CSP は組織内外のデータ転送に関する技術的措置を実施する責任を負う。 CSP への提言は以下の通り： a. CSP は、特定のデータ保護法および規制によって義務付けられ、データ管理者（CSC）によって指定された管轄区域内でのみ、データを保管および処理するものとする。 b. 不正な個人データまたは機微データへのアクセスから保護するためのセキュリティ対策の詳細を文書化する。権限付与および法規制遵守のための役割と責任、処理者および管理者の責任（各法規制に基づく）を定義する（規則による）：処理者利用者の責任（規則によ	**実施ガイドライン：** **全てのサービスモデルに適用：** サービスデリバリモデルに関係なく、CSC は組織内外のデータ転送に関する技術的措置を実施する責任を負う。 CSC への提言は以下の通り： a. CSP のサービスに含まれるデータの管理責任を負う。 b. CSP は、CSC がクラウドに置くことを選択したコンテンツのタイプについて一切関知せず、CSC がそのコンテンツをどのように分類し、どこに保管し、使用し、開示から保護するかを完全に管理できるようにする。これは、BYOK（Bring Your Own Key）暗号化などの技術的なセキュリティ対策を実施することで可能である。 c. 「二重性」または「四つ目の原則」を実施することで、SoD を確保する。分離を実施できない場合は、適切な緩和策を適用する。

る)。

c. 個人データまたは機微データへの不正アクセスから保護するために、個人データまたは機微データの移動に関わるセキュリティ対策を文書化すべきである。

d. 第三者又はサブプロセスが顧客の個人データ又は機微データの処理に関与する場合は、個人データに関連する影響評価を実施すべきである。契約、SLA、ベンダーの内部ポリシーを見直し、サードパーティーが関与するセキュリティ、可用性、機密性に関連するリスクを管理すべきである。

e. 顧客、サプライヤ、第三者に対し、以下のような適切なセーフガードを実施するよう、契約条項で要求事項を規定すべきである：

  i. 不正アクセス、不正使用、不正開示から情報を保護するためのアクセス制限（すなわち、従業員、請負業者、および、情報提供者に対し、以下の権限を付与すること。
  サブプロセッサは、「指示」に従うために厳密に必要な場合に限り、顧客データにアクセスすること）

  ii. 従業員、請負業者、および下請業者が、その履行範囲に適用される範囲でセキュリティ対策を遵守することを保証し、顧客データの処理を許可された全ての者に守秘義務があることを保証するために、適切な措置を講じること。

  iii. クラウドサービスと CSC 間でのデータ転送時には、TLS を使用してデータを保護する。RSA ベースの 2048 ビットの鍵長で、一意の鍵による接続の保護を使用する。データ転送メカニズムとして API を使用する場合は、双方向 TLS を推奨する。

  iv. 利用者による削除、期間終了時の返却または削除、繰延削除などの削除条件指示

  v. システムおよびサービスの機密性、完全性、可用性、レジリエンスを継続的に確保する。

  vi. インシデント発生後、利用者データへのタイムリーなアクセスを回復し、有効性を定期的にテストする。

  vii. データインシデントを認識した後、不当な遅延なく速やかに顧客にインシデント通知を行い、被害を最小限に抑え、顧客データを保護するための合理的な措置を速やかに講じる。

  viii. コンプライアンス認証および SOC レポートの取得と維持の徹底

  ix. 顧客の責任、データへのアクセス、対象者の権利、データエクスポート、データ移転について規定する。

  x. データセンターとネットワークのセキュリティ

  xi. データの保存、分離、ロギング

  xii. アクセス制御

  xiii. 廃止データ資産およびデータ資産消去ポリシー

d. 個人情報保護規則を遵守する責任

e. 契約条件やアクセスなど、顧客、サプライヤ、第三者に対する適切な保護措置を実施する。
不正なアクセス、使用、開示から保護するための制限

f. 該当する場合、CSC が指名した独立した監査人（検査を含む）を通じて、CSP の SOC 2 レポート、セキュリティ追加条項、または監査権条項義務の下でのセキュリティ条項のレビューを要求することで、CSP のコンプライアンスを確認するための監査を実施する。

g. 当該管理者が許可した継続的な保証：

  i. 指示

  ii. プロセッサの任命

  iii. サブプロセッサの変更に異議申し立ての機会を含む、CSP のサブプロセッサへの関与の検証

h. 指示通知/インシデント通知／要請に対する責任/の規定に基づいて CSP が提供した通知を、関連する管理者に直ちに転送すること。

xiv. 人員のセキュリティ（すなわち、法的に許容される範囲内で、適用される現地の労働法に従い、合理的に適切な身元調査を実施する。 その役割（認証など）、承認なしに顧客データを処理しない人員） xv. サブプロセッサのセキュリティ（すなわち、サブプロセッサのセキュリティおよびプライバシーの慣行について監査を実施し、データへのアクセスおよびサブプロセッサが提供するサービスの範囲に適切なレベルのセキュリティおよびプライバシーが提供されていることを確認する。） xvi. EU と EU 域外との間の個人データおよび機微データの移転について、CSP は以下を保証するものとする: • データ移転先の国が、EU によって適切なデータ保護法を有するとみなされた場合。 • 拘束力のある会社規則の定義と制定 • 標準契約条項の制定と実施 • データが移転される個人から明示的な同意を得る。 • 政府機関へのデータ開示要件を含め、仕向け国の現地法に基づく法的義務を考慮、検討し、組み入れる。 • 転送・処理されるデータのセキュア性と機密性を確保するための適切な技術的・組織的措置を実施する。	

Control Title	Control ID	Control Specification
個人情報へのアクセス、取り消し、修正および削除	**DSP-11**	適用される法律および規制に従って、データ主体が自身の個人情報へのアクセス、修正、または削除を要求できるようにするためのプロセス、手順、および技術的措置を定義し、実施する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠； これは、CSP と CSC の双方で「互いに独立した形で共有」する管理策である。なぜなら、両社はそれぞれおよび技術的な管理を定義しなければならないからである。データ対象者がシステム内の個人データにアクセス、閲覧、修正、または削除できるようにするための措置、または CSP に要求を記録することによる措置である。CSP は、関連するデータ保護法に従って、そのような要求に対応するものとする。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 管理策の実装は、サービスデリバリモデル（IaaS、PaaS、または SaaS）に固有ではない。サービスデリバリモデルに関係なく、CSP は、データ対象者がシステム内または CSP にリクエストを記録することで、自分の個人データにアクセス、閲覧、修正、または削除できるようにするためのおよび技術的手段を定義する責任を負う。 CSP への提言は以下の通り： a. 個々のデータ主体が自己のデータへのアクセス権を有するためのプロセスを確立し、プライバシーステートメントおよび（または）グローバルプライバシー慣行として公表する。プライバシーポリシーは、CSP のサービス利用者、Web サイトの訪問者、および CSP カスタマー、ベンダー、およびパートナーの代理として働く個人を含む、業務上の連絡先から CSP が受け取る可能性のある個人データを特定するものとする。このポリシーは、CSP がこの情報をどのように使用するか、および保持と使用を理解し管理するために個人が利用可能な選択肢を説明する。外部プライバシーポリシーには、CSP が管理者として保有するデータに関するデータ主体の要請にどのように対応するかについての説明を含めるものとする。 b. GDPR に基づき、組織はデータ主体の権利要求に対して 30 日以内に対応する義務がある。データ対象者の国の法律がデータポータビリティ、個人データへのアクセス、修正、および削除の権利を明示的に付与していない場合でも、CSC（CSC がデータ管理者である場合）の承認を経て、CSP はそのような利用者の要求に全て応じるものとする。データ主体の権利には以下が含まれる： i. 個人データの削除 - 全てのデータから 1 つのデータポイントまで、さまざまなサイズの要求が可能。 ii. 個人データへのアクセス - サービス内またはダウンロード内のデータの閲覧 iii. 個人データのエクスポート - ダウンロード可能な形式でコピーを受け取る iv. 個人データ処理に対する異議 - CSP はデータを	**実施ガイドライン：** **全てのサービスモデルに適用：** サービスデリバリモデルにかかわらず、データ対象者がシステム内の個人データにアクセスし、閲覧し、修正し、または削除できるようにするためのおよび技術的手段を定めること、またはデータ対象者がシステム内の個人データにアクセスし、閲覧し、修正し、または削除できるようにするためのおよび技術的手段を定めることは、CSC の責任である。 CSC への提言は以下の通り： a. CSP は、CSC が IaaS CSP のクラウドに保管するデータを管理する。CSP は、CSC がどのような種類のコンテンツをクラウドに保存するかについて一切関知せず、コンテンツをどのように分類し、どこに保存し、どのように利用し、どのように開示から保護するかについてを管理する。 b. 個々のデータ主体が要求し、データへのアクセス権を有し、プライバシーステートメントとして公表し、及び／又はグローバルなプライバシー慣行を行えるよう、使いやすいポータルを確立すること。個人情報保護ポリシーは、CSC が業務上の連絡先、Web サイトの訪問者、及び顧客、ベンダー、パートナーの代理として働く個人から受領する可能性のある個人情報を特定するものでなければならない。プライバシーポリシーは、CSC がこれらの情報をどのように利用するのか、及びその保持と利用を理解し管理するために利用可能な選択肢を説明しなければならない。外部プライバシーポリシーは、CSC が処理者として保有するデータについて、データ主体の要求にどのように対応するかについての説明を含むものとする。 c. GDPR に基づき、組織はデータ主体の権利要求に対して 30 日以内に回答する義務がある。データ対象者の国の法律が、データポータビリティ、個人データへのアクセス、訂正、および削除の権利について、これらの権利を明示的に付与していない場合であっても、CSC はそのような利用者の要請を全て尊重すべきである。 データ主体の権利には、以下が含まれる： i. 個人データの削除 - 全てのデータから 1 つのデータポイントまで、さまざまなサイズの要求

使用する権利を有していないと主張する

v. 個人データの制限 – CSP に自分の代わりにデータのコピーを保持するよう依頼する

注 – データ主体の種類によって、これらの権利を行使するための仕組みが異なる。

c. CSC の個人情報へのアクセス、削除、変更を要求するプロセス及び手順は、顧客との合意（MSA 等）に従うものとする。また、CSP は、契約管理上の理由から、当社の製品またはサービスの正規ユーザーに関する情報の要求および収集を許可される場合がある（注：MSA には、個人情報保護条項を含むデータ処理契約（DPA）へのリンクが含まれる場合がある）。

が可能です。

ii. 個人データへのアクセス – サービス内またはダウンロード内のデータの閲覧

iii. 個人データのエクスポート – ダウンロード可能な形式でコピーを受け取る

iv. 個人データ処理に対する異議 – CSC はデータを使用する権利を有していないと主張する。

v. 個人データの制限 – CSC に自分の代わりにデータのコピーを保有するよう依頼する。

注 – データ主体の種類によって、これらの権利を行使するための仕組みが異なる。

Control Title	Control ID	Control Specification
個人情報処理における利用目的の制限	**DSP-12**	適用される法令に従い、かつデータ主体に宣言された目的のために、個人情報が処理されることを保証するためのプロセス、手順、および技術的手段を定義し、実施し、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； これは、CSP と CSC が双方で「互いに独立した形で共有」する管理策である。CSP と CSC はそれぞれ、以下を確実にするためのプロセスと手順および技術的手段を定義する必要があるからである： a. 情報主体が情報収集の性質および目的を認識すること。 b. 情報が関連性があり、処理要件に限定されている c. データ主体のプライバシーを侵害しない合理的な方法で処理が行われること。 d. 処理は、責任ある当事者の機能または活動に関連する、特定かつ明確に定義された、合法的な目的のために行われる。 e. 管理者が、個人データが収集された目的とは別の目的	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。

のために個人データをさらに処理することを意図している場合、データ主体は事前にその目的を通知され、同意を提供するものとする。 f. 情報は必要な期間だけ保存される。	
実施ガイドライン： **全てのサービスモデルに適用：** 管理策の実装は、サービスデリバリモデル（IaaS、PaaS、またはSaaS）に固有ではない。サービスデリバリモデルに関係なく、CSP は、個人データ処理における目的制限のための手順と手続および技術的措置を定義する責任を負う。 CSP への提言は以下の通り： a. GDPR またはその他の適用される規則に従って、正式なデータ対象者アクセス要求（DSAR）を確立する。 b. 個人データが適用される法律および規制に従って処理され、データ処理条件およびセキュリティ条件においてデータ主体に対して宣言された目的のために処理されることを保証するための合意を詳述する。 c. DPA の条項は、CSP が顧客の個人データを処理する方法を規定する EU モデル条項に対応している。 d. CSP は個人データの管理者ではなく、処理者とみなされる。 e. 法務チームとコンプライアンスチームが規制義務を監視する。 f. 暗号管理に関連する適用される輸出規制への準拠を保証するための技術的手段を導入し、活動ログとレポートを使用して、既存の内部認証およびハードウェア・ポリシーへの準拠を判断する。CSC は、希望するデータ保管地域を選択することができる。データ転送に関する標準契約条項（SCCS）を定める。 g. 個人データの処理が適用される法律および規制に準拠して行われるように設計されたポリシーおよび標準を実施し、実施すること。 h. ポリシーと標準、および適用される法律と規制が遵守されていることを確認するために、定期的な評価と監査を実施するか、または第三者と契約する。	**実施ガイドライン：** **全てのサービスモデルに適用：** 管理策の実施は、サービスデリバリモデル（IaaS、PaaS、SaaS）に依存しない。サービスデリバリモデルに関係なく、CSC は、個人データ処理における目的制限のための手順と手続および技術的手段を定義する責任を負う。 CSP の「実施ガイドライン」が適用される。 CSC への追加提言は以下の通り： a. CSP のサービスに取り込むデータを管理する（適用される法規制の遵守を含む）。 b. CSC がどのような種類のコンテンツを CSP の環境に保存することを選択するかについて CSP が一切関知しないことを保証するための手段を導入すること、および CSC がコンテンツの分類方法、保存場所、使用場所、および開示からの保護について完全な管理を保持すること。 c. CSP に最新かつ正確な情報を確実に提供すること。 d. アプリケーションへ、アプリケーション内、またはアプリケーションからのデータの入力、処理、保持、出力、破棄の間に行われる不正なアクセス、使用、開示を防止または検出するための管理的および技術的な防止措置を設計、開発、テスト、実装、運用、維持すること。

Control Title	Control ID	Control Specification
個人情報のサブプロセッシング	**DSP-13**	適用される法律および規制に従って、サービスのサプライチェーン内での個人情報の転送およびサブプロセッシングのためのプロセス、手順、および技術的措置を定義、実施、および評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； これは、「互いに独立した形で共有」の管理策である。なぜなら、両者は、適用されるあらゆる法規制に従って、サービスサプライチェーン内での個人データの移転およびサブプロセスに関する手順と手続および技術的手段を定義しなければならないからである。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 管理策の実装は、サービスデリバリモデル（IaaS、PaaS、またはSaaS）に固有ではない。クラウドサービスデリバリモデルに関係なく、CSP は、個人データのサブプロセスに関する手順と手続および技術的措置を定義する責任を負う。 CSP が実施すべき勧告は以下の通りである： a. データ処理およびセキュリティ規約において、法令に基づくサービスサプライチェーン内での個人データの移転およびサブプロセスに関する合意を詳述する。また、手順、手続、措置を定義し、ベストプラクティスに従う。M&A によって影響を受けたシステムを統合するためのプラクティス。 b. サブプロセッサエンゲージメントへの同意：CSP は CSC に対し、情報（サブプロセッサの名称、所在地、および活動）に従い、サブプロセッサとしてのエンゲージメントを承認するよう要請する。サブプロセッサについて提供される。 c. サブプロセッサエンゲージメントに関する要件は、サブプロセッサと契約する際、CSP が 書面による契約を通じて以下を保証するように規定される： i. サブプロセッサは、委託された義務を遂行するために必要な範囲でのみ利用者データにアクセスし、使用し、適用可能な契約に従う。 ii. 利用者の個人データの処理が欧州のデータ保護法に従う場合、データ保護義務がサブプロセッサに課され、サブプロセッサに委託された全ての義務と、サブプロセッサの全ての行為と過失について完全に責任を負う。 d. 契約期間中に新たなサブプロセッサと契約する場合、CSP	**実施ガイドライン：** **全てのサービスモデルに適用：** 管理策の実装は、サービスデリバリモデル（IaaS、PaaS、または SaaS）に固有ではない。クラウドサービスデリバリモデルに関係なく、CSP は、個人データのサブプロセスに関する手順と手続および技術的措置を定義する責任を負う。 CSC が実施すべき提言は以下の通り： a. CSP のサービスに配置するデータを管理する。 b. CSP は、利用者がどのような種類のコンテンツを CSP の環境に保存することを選択するかについて洞察できないため、コンテンツをどのように分類し、どこに保存し、使用し、開示から保護するかを完全に管理する。 c. サブプロセッサとの契約に対する同意。CSC は、CSP によって開示されたサブプロセッサの名前、所在地、および活動を確認した上で、そのサブプロセッサの雇用を特に承認する。 d. 期間中に新たなサブプロセッサが関与した場合、CSC は、CSP から新たなサブプロセッサの関与の通知受領 90 日以内に CSP に通知することにより、該当する契約を便宜上直ちに終了させることにより異議を申し立てることができる。 e. アプリケーションへ、アプリケーション内、またはアプリケーションからのデータの入力、処理、保持、出力、破棄の間に行われる不正なアクセス、使用、開示を防止または検出するための管理的および技術的な防止措置を設計、開発、テスト、実装、運用、維持すること。

	は、新たなサブプロセッサが利用者データの処理を開始する少なくとも 30 日前までに、当該契約について（新規サブプロセッサの名称、所在地及び活動を含む）CSC に通知するものとする。	

Control Title	Control ID	Control Specification
データのサブプロセッシング先の開示	**DSP-14**	サブプロセッサによる個人情報または機微なデータへのアクセスの詳細を、その処理を開始する前にデータ所有者に開示するためのプロセス、手順、および技術的手段を定義し、実施し、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： これは、CSP と CSC 双方が「互いに依存する形で共有」する管理策である。なぜなら、両者は、サブプロセッサがアクセスする個人データまたは機微データの詳細を、その処理を開始する前にデータ所有者に開示することを定義、実施、および評価するための手順と手続および技術的手段を定義する必要があるためである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 管理策の実装は、サービスモモデル（IaaS、PaaS、または SaaS）に固有ではない。クラウドデリバリモデルに関係なく、CSP は、サブプロセッサへのデータ開示に関する手順と手続および技術的手段を定義する責任を負う。 CSP への提言は以下の通り： a. CSC と CSP が合意したデータ処理およびセキュリティ条件を通じて、処理を開始する前のサブプロセッサによる個人データまたは機密情報の開示の詳細をあきら明らかにする。 b. 処理が CSP のデータ保護補遺に記載されているポリシーと手順に従っていることを確認する。 c. CSC にサポート、コンサルティング、クラウド、またはその他のサービスを提供する際に、CSP 及びその子会社・関連会社が採用する慣行をプライバシーポリシーに記載すること。サービス提供のためにアクセスを提供される可能性のある情報の利用が、CSP の一般的なプライバシーポリシーが対象とする情報の利用よりも限定的であることを明確にするために、当該のプライ	**実施ガイドライン：** **全てのサービスモデルに適用：** 管理の実装は、サービスデリバリモデル（IaaS、PaaS、または SaaS）に特有ではない。クラウドサービスデリバリモデルに関係なく、CSP は、サブプロセッサへのデータ開示に関する手順と手続および技術的手段を定義する責任を負う。 CSC への提言は以下の通り： a. CSP のサービスに配置するデータを管理する。 b. CSP は、顧客がどのような種類のコンテンツを CSP の環境に保存することを選択するかについて洞察できないため、コンテンツをどのように分類し、どこに保存し、使用し、開示から保護するかを完全に管理する。 c. サブプロセッサとの契約に対する同意。CSC は、CSP によって開示されたサブプロセッサの名前、所在地、および活動を確認した上で、そのサブプロセッサの雇用を特に承認する。 d. 期間中に新たなサブプロセッサが関与した場合、CSC は、CSP から新たなサブプロセッサの関与の通知を受けてから 90 日以内に、CSP に通知することによ

バシーポリシーを設定すること。 d. Web サイト、アプリケーション開発、ホスティング、メンテナンス、バックアップ、ストレージ、仮想インフラ、支払い処理、分析、およびその他のサービスを提供するために、第三者の下請業者と協力すること。これらのサービスプロバイダーは、これらのサービスを提供する目的で、個人データにアクセスしたり、個人データを処理したりすることがある。 e. 個人データを処理する可能性のある下請業者の使用について、処理が行われる前に関連顧客に開示する。CSP と共に業務を行う下請業者の対外的なリストを提供するものとする。新しいサブプロセッサが導入されたときに通知する RSS フィードを購読するよう、閲覧者を招待する。 f. サブプロセッサが EU データ保護法の対象となる個人データを処理する場合、CSP は以下のことを保証するものとする。 サブプロセッサは、EU データ保護法の要件を満たす、個人データに関する契約上の義務を負う。	り、該当する契約を便宜上直ちに終了させることにより異議を申し立てることができる。 e. アプリケーションへ、アプリケーション内、またはアプリケーションからのデータの入力、処理、保持、出力、破棄の間に行われる不正なアクセス、使用、開示を防止または検出するための管理的および技術的な防止措置を設計、開発、テスト、実装、運用、維持すること。

Control Title	Control ID	Control Specification
本番データ利用の制限	**DSP-15**	本番データを非本番環境で複製または使用する前に、データ所有者の承認の取得と関連するリスクの管理を行う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； これは、CSP と CSC が「互いに独立した形で共有」する管理策である。なぜなら、両者は本番データを非本番環境で複製または使用する前に（そしてその後は第三者関係のリスクレベルに見合って定期的に）デューデリジェンスを実施すべきだからである。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：**	**実施ガイドライン：** **全てのサービスモデルに適用：**

クラウドサービスデリバリモデルにかかわらず、CSP は本番データの使用を防止または複製する責任がある。

CSP への提言は以下の通り：

a. インフラ／プラットフォーム／アプリケーションのガバナンスと監視のためのポリシーとプロセスを維持する。
b. 物理的および論理的なネットワーク境界を定義し、本番データが本番環境のネットワーク境界内に留まるようにする。
c. 変更管理ポリシーとプロセスの実施
d. SDLC コーディングの実践、品質テスト、コーディングスキャン、ネットワークとアプリケーションの侵入テスト、コードデプロイメント、コードバックアップ、統合コードテストの確実な実施
e. 該当する場合、サニタイズ、匿名化、仮名化、難読化、切り捨て、トークン化、またはダミーデータへの置き換えを行わずに、本番データを非本番環境で使用しないことを要求する手順を確立する。
f. 環境へのアクセスに業務上の承認を必要とするよう、職務を分離する。
g. 最小特権の原則に基づき、本番クラウド環境への物理的および論理的アクセスを基本とする。
h. 物理的にセキュアなデータセンター（ハードウェア管理、データセンター・セキュリティトレーニング、警報など）
i. 従業員に対し、セキュリティ、プライバシー、セキュアなインフラ管理、およびコーディング方法に関する定期的な意識向上トレーニングを実施する。
j. 従業員の適時解雇
k. 資産インベントリ追跡、セキュアな構成管理、自動脆弱性スキャン、パッチ管理を実施する。
l. システムアクセスを継続的にログに記録し、監査する。
m. 定期的なコンプライアンス監査を実施し、統制の有効性を確認する。

クラウドサービスの提供モデルにかかわらず、CSC は本番データの使用を防止または複製する責任がある。

CSC は、レプリケーションや高可用性、本番環境の区分に関して、本番データをどのように維持するかについて、ポリシーを定義し、管理策を確立する責任がある。

CSC への提言は以下の通り：

a. アプリケーションへ、アプリケーション内、またはアプリケーションからのデータの入力、処理、保持、出力、破棄の間に行われる不正なアクセス、使用、開示を防止または検出するための管理的および技術的な防止措置を設計、開発、テスト、実装、運用、維持すること。
b. 監視およびインシデント対応プロセスをサポートするために、管理者の操作、システムエラー、認証チェック、データ削除などのイベントに対する適切なロギングが行われていることを確認する。
c. 全てのサービスで利用可能な場合は、サービス固有のロギング機能を有効にして設定し、適切なモニタリングとインシデント対応プロセスを実装する。
d. ネットワークとファイアウォールの設定に責任を負う。
e. クライアント側のデータ暗号化とデータ完全性、サーバー側の暗号化（ファイルシステムおよび/またはデータ）、および永続性に責任を負う。
f. 秘密鍵はセキュアな経路で送信すること。利用者は、Web ページやその他の一般にアクセス可能なソースコードに秘密鍵を埋め込むことを避けるべきである。利用者は、機微データをネットワーク経由だけでなく、保存中でも暗号化すべきである。
g. 利用者の要件を満たすために、利用可能な暗号化オプションを適切に設定し、使用および実装を管理する。
h. ネットワークトラフィックの TLS 接続、完全性検証（チェックサム）、ID チェックを確実に行う。
i. CMK の年次での鍵ローテーションを選択する。
j. サニタイズ、匿名化、仮名化、難読化、切り捨て、トークン化、または該当する場合はダミーデータへの置き換えを行わずに、本番データを非本番環境で使用しないことを契約で規定し、手順を確立する。

Control Title	Control ID	Control Specification
データの保持と廃棄	**DSP-16**	データの保持、アーカイブ、削除は、ビジネス要件、適用される法律および規制に従って管理する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； これは、CSP と CSC が「互いに独立した形で共有」する管理策である。なぜなら、両者とも、ビジネス要件及び適用される法規制に従って、(第三者との関係のリスクレベルに見合って定期的に) データの保持、保管、及び削除が管理されていることを保証しなければならないからである。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 管理策の実装は、サービスデリバリモデル（IaaS、PaaS、またはSaaS）に固有ではない。クラウドサービスデリバリモデルに関係なく、CSP は、物理データと電子データの両方を包含する保持と削除の方法を確保する責任を負う。 CSP への提言は以下の通り： a. 情報保護ポリシーを定義し、機微情報の分類および取り扱いの要件を規定する。このポリシーは、情報が CSP、利用者、または CSP のサードパーティーに属するかどうかに関係なく、全ての機微情報に適用されるものとする。このポリシーは、少なくとも年 1 回、法務チームによって見直され、改訂されるものとする。 b. CSP のサービスの運営を継続するために、規制、法令、契約、および事業上の要件に従って、データ保持、アーカイブ、および削除のポリシーと手順を維持すること。 c. CSP は、データ処理条件およびセキュリティ条件において、適用される法律および規制に従って、デー タの削除（保持を含む）およびデータのエクスポートに関する合意を詳述するものとする。 d. CSP は、監査証拠およびログ記録、並びにバックアップおよび冗長性プログラムを含む重要なシステムコン	**実施ガイドライン：** **全てのサービスモデルに適用：** 管理策の実施は、サービスデリバリモデル（IaaS、PaaS、SaaS）に依存しない。クラウドサービスデリバリモデルに関係なく、CSC は、物理的データと電子的データの両方を包含する保持と削除方法を確保する責任がある。 CSC への提言は以下の通り： a. CSC は必要に応じて手動でデータバックアップのスケジュールと設定を行う。 b. CSC は、各自の環境に関連する全ての必要なポリシーと手順を維持する責任を負うべきである。 c. CSC は、その要件及びポリシーに沿ったバックアップ及び／又はレプリケーションプロセスの実施に責任を負う。 d. CSC は、アプリケーションへ、アプリケーション内、またはアプリケーションからのデータの入力、処理、保持、出力、および廃棄において、不正アクセス、不正使用、および不正開示を防止または検出するための管理上および技術上のセキュア対策を設計、開発、テスト、実施、運用、および維持する責任を負う。 e. CSC は独自のデータ保持ポリシーを実施する責任を負う。一方、CSC は偶発的なデータ損失を防ぐため、サブスクリプションとストレージアカウントの削除

ポーネントが、災害復旧を目的として、少なくとも年に 1 回、維持、監視、レビュー、および検証されることを保証するものとする。 e. CSP は、地理的に複製されたコピーのプライマリロケーションからインデックスを非同期に削除するなど、データをセキュアに削除するツールを提供するものとする。データの消去は、NIST 800-88 に準拠するものとする。データの破棄には、媒体のセキュアな消去と、情報の読み取りや再構築ができないような記録のセキュアな廃棄が含まれるべきである。 f. CSP は、データを合理的に復元できない程度まで欠陥ディスクを破壊するように設計された廃棄プロセスに従うべきである。該当する場合、セキュアな破棄のためマネージドサービス・プロバイダーを使用する際は、破棄証明書を取得すべきである。 g. CSP は、合意された期間内に「保持される利用者データ」を破棄するよう書面で求められた場合、実務上可能な範囲で速やかにこれに応じ、CSC の書面による要求に応じて「保持される利用者データ」の破棄を書面で証明するものとする。 h. CSP は、セキュアな FTP サイト、データベース、ハードドライブ、および仮想マシンからのデータの削除、並びに仮想会議セッションの削除を含め、サポートサービス調査の終了時に利用者データを削除すべきである。	に予め定められた期間（日単位）を提供する。 f. CSC は、そのデータの管理及び所有を保持し、その要求に従ってデータ保持ポリシーを実施する責任を負うものとする。該当する場合、データを永久に削除する能力を持つ CSC の管理者とユーザーは、それに従ってデータを削除するものとする。

Control Title	Control ID	Control Specification
機微なデータの保護	**DSP-17**	機微なデータをライフサイクル全体で保護するためのプロセス、手順、技術的手段を定義し、実施する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠； これは、CSP が所有権を持つ管理策である。利用者データのセキュリティは最優先事項であり、機微データがライフサイクルを通じて保護されることを保証するために、いくつかの異なるメカニズムが導入されるべきであるからである。	**管理策所有権の根拠；** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** 管理策の実装は、サービスデリバリモデル（IaaS、PaaS、または SaaS）に固有ではない。クラウドサービスデリバリモデルに関係なく、CSP は、データのライフサイクル全体を通じてデータを保護するためのメカニズムが整備されていることを保証する責任を負う。 CSP への提言は以下の通り： a. CSP は、プライバシーステートメントを公表し、機微データの処理プロセスについて説明するものとする。これは正式なものであり、署名され、法的に有効であり、連邦法または地域の法律および規則に従って発行されるものでなければならない。このプロセスでカバーされるべき属性の一部を以下に示す： i. 「個人データ」、「データ主体」、「処理」、「管理者」、「処理者」などの重要な定義。 ii. データ保護法の適用範囲 iii. 処理者、管理者、利用者の役割と責任 iv. 姓、名、ユーザー名、パスワードを含む利用者のユーザー認証情報のみを収集、保存するなど、処理の範囲を限定すること。生年月日、個人住所、社会保障番号、健康情報、財務データ（SOX）、クレジットカード情報などの機微データを保存、処理、送信しない。 v. データ削除：利用者による削除、期間終了時の返却または削除、繰延削除指示 vi. セキュリティ対策、管理、支援アクセスおよびコンプライアンス、暗号化、利用者データがサービス内で論理的に分離されていることを保証するために、利用者ごとに固有の暗号化鍵を使用する。使用中のデータには信頼された実行環境（Trusted Execution Environments：TEE）を使用し、利用者の本番データをテスト環境や開発環境で使用しない。テスト目的で本番データを使用することが絶対に必要であると判断された場合は、本番環境と全く同じ管理を適用し、複製しなければならない。 vii. 本番環境内の全ての仮想マシンインスタンスは、特定のポートおよびプロトコルのみで相互通信するよう許可リストに登録され、ハイパーバイザおよびゲストインスタンスレイヤで IDS/IPS お	**実施ガイドライン：** CSC には適用されない。 CSC は、利用者コンテンツの管理及び所有を保持し、処理開始前に、サブプロセッサによる個人データ又は機微データへのアクセスの詳細をデータ所有者に開示する責任を負う。

よび厳格なファイアウォールが実装され、本番環境から発信されるアウトバウンド通信は一切許可されない。ネットワークレイヤの制御により、許可リストに登録された IP およびホストを通じて特権アクセスが常に強制され、非標準ポートを介して暗号化された VPN トンネルが使用される、二要素認証は、物理的に分離されたハードウェア MFA トークンによって提供される。異常なクエリや利用者データの大量エクスポートを検出するためのデータベースへのトランザクション監視の実装、CSP の本番環境からの全てのアウトバウンドトラフィックに異常がないか、専有および市販のトラフィック監視および侵入検知システムの両方を使用して監視し、技術運用とセキュリティの両方にアラートを送信する。

viii. データインシデント管理
ix. 利用者のセキュリティ責任
x. コンプライアンス認証および SOC レポート
xi. 利用者の監査権
xii. アクセス等、データ主体の権利、データ輸出
xiii. データ転送
xiv. サブプロセッサの使用

b. 該当する場合、CSP、全ての機微データについて情報著作権管理（IRM）技術を実装するものとする。
c. CSP は、非コンテンツを開示する前に召喚状またはそれに相当するものを要求し、令状（またはそれに相当するローカルなもの）に応じてのみ法執行機関にコンテンツを開示する。
d. CSP は、法的に許可されている場合、政府やその他の規制当局が CSC 自身にデータを求めるよう誘導すべきである。
e. CSP は、セキュアなポータルを介して全ての法執行機関の要求を取り込むプロセスを確立し、そのプロセスでは、審査された法執行機関のみがアクセスを受けるようにする。CSP が要求を検討し、データを提供する必要があると判断した後は、有効な法的命令で指定されたデータを、同じセキュアなポータルを通じて法執行機関に提供するものとする。
f. CSP は、従業員、サプライヤ、請負業者、およびパートナーが情報とそのシステムおよびリソースのセキュリティと完全性を保護できるように、システムおよびリソースの許容される使用ポリシー（AUP）を策定し、職務の遂行中にシステムおよびリソースをどのように使用してよいか、または使用してはならないかを指定する。

Control Title	Control ID	Control Specification
開示通知	**DSP-18**	CSP は、適用される法律および規制に従って、法執行機関による個人情報の開示要求を管理および対応する手順を整備し、CSC に説明しなければならない。CSP は、法執行機関の調査の機密性を保持するために刑法で禁止されている場合など、特に禁止されていない限り、関心のある CSC への通知手順に特別な注意を払わなければならない。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： これは、CSP が所有権を持つ管理策である。CSC のプライバシーは最優先事項であるため、これは CSP が所有する管理策である。CSP は、法律または政府機関もしくは規制機関の有効かつ拘束力のある命令に従う必要がある場合を除き、CSC のデータの開示を禁止するポリシーを持つべきである。CSP は、法執行機関に CSC のコンテンツを開示する前に CSC に通知し、開示からの保護を求めることができるようにする。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** クラウドサービスデリバリモデルにかかわらず、CSP は、法律または政府機関もしくは規制機関による有効かつ拘束力のある命令に従う必要がない限り、CSC のデータの開示を禁止するポリシーを有する責任を負う。 CSP への提言は以下の通り： a. CSP は、第三者からの機密情報へのアクセス要求に対応し、アクセス要求が法的に必須であるかどうかを評価し、一般市民、CSC、影響を受ける個人、または法執行当局への必要な通知または開示を含む適切な対応を決定するための要件を規定する、適用される法律および規制に沿ったポリシーおよびプロセスを定義するものとする。 b. CSP は、受領した情報要求の種類と量に関する報告書を定期的に公表することで、CSC に対する透明性の必要性に対処すべきである。 c. CSP は、関連当局（規制当局、法執行機関、政府当局など）、およびセキュリティ、リスク、コンプライアンス、	**実施ガイドライン：** CSC は、アプリケーションへの、アプリケーション内での、又はアプリケーションからのデータの入力、処理、保持、出力、及び処分において、不正アクセス、不正使用、及び不正開示を防止又は検知するための管理上及び技術上の保護措置を設計、開発、試験、実施、運用、及び維持する責任を負う。

およびポリシー組織などの業界団体と適切な連絡を維持し、定期的に要求リストを評価し、必要に応じて指導を求めるために、法務チームを指名する。	

Control Title	Control ID	Control Specification
データの所在地	**DSP-19**	データが処理またはバックアップされる場所を含む、データの物理的な場所を特定および文書化するためのプロセス、手順、および技術的な手段を定義し、実施する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： これは、CSP と CSC が「互いに依存した形で共有」する管理策である。なぜなら、CSP は、CSC からのインプットに従って（そしてその後も第三者関係のリスクレベルに応じて定期的に）、データの保管場所、処理場所、バックアップ場所を確保するからである。共有賃借の場合、CSC は顧客データの物理的な場所を要求することが認められるべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** この管理策の実装は、サービスデリバリモデル（IaaS、PaaS、または SaaS）に固有ではない。クラウドサービスデリバリモデルに関わらず、CSP は、CSC との契約に規定された要件に従って、データの保存、処理、及びバックアップのための手順、手続、及び技術的手段を定義し、実施する責任を負う。 CSP への提言は以下の通り： a. 全ての資産（すなわち、サーバーのハードウェア、ソフトウェア、情報システム上に保持されるデータ、災害復旧および事業継続の目的に必要な情報）を識別、分類、および属性を記録する要件を定義したポリシーを維持する。全ての資産は、ポリシーに従ってインベントリシステムで追跡されるべきである。所有者、分類、所在を特定し、資産追跡システムで追跡すべきである。資産のインベントリは、各資産がその分類に従	**実施ガイドライン：** **全てのサービスモデルに適用：** この管理策の実装は、サービスデリバリモデル（IaaS、PaaS、SaaS）に特定されるものではない。クラウドのサービスデリバリモデルに関わらず、CSC は最初にテナント、つまりデータを置く地理的な場所（「ホームリージョン」と呼ばれることもある）を確立する責任がある。 CSC への提言は以下の通り： a. 利用者のコンテンツ、サービス、リソースへのアクセスを管理する。 b. CSP が提供する強力な暗号化（移動中または保存中）を使用して、コンテンツをどのように保護するかについてのポリシーおよびプロセスを導入する。オプションが利用可能な場合、CSC は独自の暗号鍵を管理するものとする。

って保護されていることを確認し、データのインベントリが正確であることを検証するために、少なくとも四半期ごとに見直されるべきである。

b. CSC は、データが保存される特定の地域を指定する必要がある。CSP は、冗長性を確保するため、選択された地理的地域内のみでデータが複製されるようにすべきである。法律で義務付けられている場合を除き、初めに CSC に通知することなく、指定された地域以外の場所にデータを複製すべきではない。

c. クラスタリングなど、低レイテンシーで可用性の高い地理的に分散したストレージサービスを設計、構築し、システムソフトウェアとデータを最小限の損失で利用できるようにバックアップするためのレプリケーションを提供する。

d. CSP は、アクセス、暗号化、およびログ機能を構成するためのサービスおよびツールを提供し、CSC による効果的な運用管理を支援する。CSP は、独自の暗号鍵を管理するオプションを CSC に提供するものとする。

e. 法律上必要な目的及び CSC に提供されるサービスを維持する目的以外の目的で、利用者のコンテンツにアクセス又は使用しないこと。

f. ジオタグが設定されたデータセンターで稼働するシステム上で伝送、処理、保存される暗号化されていないデータにはアクセスしないこと。異なるアベイラビリティゾーンやリージョン間で同期レプリカとして保存されるデータ、および関連するサービスは、アベイラビリティゾーンやリージョンのデータ障害から迅速に回復するように設計されるべきである。

g. ベンダーのリスク管理プログラムの一環として、データセンターを毎年監査し、SOC2 タイプ 2 などの認証報告書の写しをレビュー／保管する。

c. 使用中のデータには信頼された実行環境（TEE）を使用する。

d. インシデント管理プロセスのロギング機能を有効にする。

Control Domain GRC

2.8 ガバナンス、リスク管理、コンプライアンス(GRC)

Control Title	Control ID	Control Specification
ガバナンスプログラムのポリシーと手順	**GRC-01**	組織のリーダーシップによって提供される情報ガバナンスプログラムのポリシーと手順を確立、文書化、承認、伝達、適用、評価、および維持する。少なくとも年 1 回ポリシーと手順を見直して更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： IaaS/PaaS/SaaS の場合、この所有権は、CSP と CSC の両者で「互いに独立した形で共有」し、それぞれ独立して実施する責任がある。 全てのサービスモデル（IaaS、PaaS、SaaS）に適用される為、ガバナンス、リスク、コンプライアンス（GRC）の実施は、クラウドサービスモデルに関係なく組織レベルで行われる。 適切な情報とテクノロジーガバナンス（データ保護法などの技術統治）、リスク管理、およびコンプライアンスのためのプログラムを確立することは、サービスのコンシューマーまたはサービスのプロバイダーの役割を問わず、全ての組織にとって重要である。 この管理策の実装責任は「共有」である。なぜなら、CSP と CSC の両方が、それぞれの業務、製品、およびサービスをカバーするために、それぞれ独自のガバナンス、リスク、およびコンプライアンス（GRC）プログラムを持つ必要があり、そのようなプログラムの確立は、関連するポリシーと手順を含め、完全に内部的で各組織に固有のものだからである。CSP と CSC は、それぞれ独自に、これらの機能に関するそれぞれのポリシーと手続きを策定する。GRC プログラムは、組織レベルの機能であるため、提供または消費されるクラウドサービスの種類に関係なく、この（互いに依存しない）統制権を所有し共有することが適用される。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。

実施ガイドライン： **全てのサービスモデルに適用：** 情報ガバナンスプログラムのための強固なポリシーと手続を確立することは、クラウドコンピューティングとセキュリティのコンテキストにおいて、CSP と CSC にとって最も重要である。 明確に定義されたリスク管理プログラムにより、クラウドサービスに関連する潜在的な脅威と脆弱性が体系的に特定され、評価され、緩和され、セキュリティ侵害の可能性が低減される。組織のポリシーと手順は、運用の明確性と一貫性に寄与し、CSC を含む全ての利害関係者が確立された標準と規制要件を準拠することを保証する。 ポリシーは、組織のコントロール使命を中心にマッピングされるべきであり、常に組織の方向性とニーズに合わせて最新であるべきである。 情報セキュリティプログラムの導入は、暗号化標準、アクセス制御、インシデント対応計画を明確化し、全体的なセキュリティ態勢を強化することで、CSP が機微データを保護するのに役立ちます。これらのポリシーは、レジリエンスのある情報ガバナンスの枠組みの礎石となり、リスクに対処し、コンプライアンスを確保し、全体的なクラウドセキュリティを強化することで、CSP と CSC の双方に信頼を与える。 CSP と CSC の両者は、強固なガバナンスプログラムを導入すべきである。トップのリーダーシップは、プログラムが適切に実施されることを保証する最終的な責任を負う。ガバナンスの核となる要素は、それを担当する者がそれを実施する権限を持つことである。 CSP と CSC は、それぞれ独自のビジネスニーズ、ポリシーと手順に関する要件を有している。これらのポリシーと手順には、クラウド組織の主なセキュリティ目標、目標の根拠、承認、およびレビュー手順を含めるべきである。ポリシーは、またクラウド組織内の役割と責任を明確にし、誰が、いつ、どこで、何を、どのように行うべきかを示すべきである。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が提適用される。
ポリシーは、以下に関する規定が含まれるべきである（但し、これに限定されない）： a. 範囲と目的： 包括的な情報ガバナンスプログラムは、組織の情報資産を効果的に管理・保護し、適用される規制を遵守しながら、ビジネス目標を支援するために確立すべきである。情報ガバナンスプログラムの適用範囲は、対象となる情報の種類、関係する組織単位、およびプログラムが適用される地理的な場所を特定し、定義すべきである。 適用範囲には以下を含む（但し、これらに限定されない）： i. データ、文書、記録、知的財産を含む、関連する全ての情報資産	

ii. 情報資産の所有および管財権
iii. 作成・保管・アクセス・保持・廃棄を含む、情報資産の適切なライフサイクル管理
iv. 個人データや保護されるべき医療情報（PHI）など、機微情報の取扱いガイドライン

b. リスク管理プログラム：
組織全体のリスク選好と事業目的に沿ったリスク管理のフレームワークを確立すべきである。
エンタープライズリスク管理(ERM)は、以下のことを行うべきである：
i. データセキュリティ、プライバシー、コンプライアンス、オペレーショナルリスクなど、クラウド関連のリスクを特定、評価、優先順位を設定する。
ii. データの暗号化、アクセス制御、定期的なセキュリティ監査など、適切なリスク軽減戦略を実施する。
iii. クラウド関連リスクを継続的に監視・評価し、必要に応じてリスク軽減戦略を適応させる。

c. 組織ポリシーのレビュー：
組織のポリシーと手順は、組織の進化するビジネスニーズおよび規制要件との整合性を維持するために、定期的にレビューし、更新すべきである。

d. ポリシーの例外手順：
透明性があり、説明責任を果たし、監査可能な正式なポリシーの例外プロセスを確立すべきである。
i. ポリシーの例外を承認するための標準を定め、緊急時および／又は十分に正当化された状況下でのみ例外が認められるようにする。
ii. 全てのポリシーの例外について、上級管理者の承認を必要とする。
iii. 全てのポリシー例外は、承認の根拠および実施された改善措置を含め、文書化し、追跡する。

e. 情報セキュリティプログラム：
業界のベストプラクティスおよび関連する規制要件に合致し、クラウドコントロールマトリックス（CCM）の最新版の全ての関連ドメインを含む情報セキュリティプログラムを実施すべきである。

f. ガバナンス責任モデル：
クラウドガバナンスプログラムの計画、実施、運用、評価、改善のための役割と責任を明確にする。
i. IT 部門、法務部門、コンプライアンス部門、リスク管理部門など、様々な部門から代表者を集めたガバナンス委員会または運営グループを設置する。
ii. 具体的な責任を個々のチームまたは役割に委譲し、説明責任を明確にし、文書化する。
iii. 全ての利害関係者に対し、ガバナンスの責任に関する定期的な研修を実施する。

g. 情報システム規制マッピング：
クラウドベースの情報システムに適用される全ての関連する標準、規制、法的／契約上の要求事項を、特定し、文

書化し。規制要件の変更を反映し、定期的に更新する為に、規制マッピングレジストリを維持すべきである。

h. 特別利益団体：
関連するクラウド関連の特別利益団体、業界団体、政府機関との関係を確立し、維持すべきである。
  i. 業界フォーラム、カンファレンス、ワークショップに参加し、新たなクラウド技術、トレンド、規制の動向について常に最新の情報を得る。
  ii. 業界フォーラムや出版物を通じて、他のクラウド組織とベストプラクティスや見識を共有する。
  iii. クラウド業界の専門家と協力し、クラウドに関連する共通の課題に取り組み、革新的なソリューションを開発する。

i. 承認：
組織の戦略目標およびリスク選好との整合性を確保するための承認要件および上級管理職の関与を確立すべきである。
  i. ポリシーおよび手順の変更又は、修正の承認手順を確立する。
  ii. 承認に関する文書化された記録（日付、承認者名、関連するコメント又は議論を含む）を維持する。

j. コミュニケーション：
ポリシーおよび手続の効果的な伝達は、関連する全てのクラウド利害関係者に対して促進すべきである。

k. 維持とレビュー：
情報ガバナンスポリシーおよび手順は、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制およびリスクの変化を反映するために、少なくとも年１回は文書化し、レビューし、更新すべきである。

Control Title	Control ID	Control Specification
リスク管理プログラム	**GRC-02**	クラウドセキュリティとプライバシーリスクの特定、評価、所有、処理、および受容のためのポリシーと手順を含む、正式で、文書化され、リーダーシップが支援するエンタープライズリスク管理（ERM）プログラムを確立する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines

CSP	CSC
管理策所有権の根拠： この管理策の実装責任は、基本的に CSP と CSC の両者で共有し、それぞれ独立して実施する責任がある。なぜなら、リスク管理プログラムの構築は、完全に内部的で各組織に固有のものであり、各組織がその業務、製品、およびサービスを対象とする独自の ERM プログラムを策定すべきである。 CSP と CSC は、それぞれ独自にクラウドセキュリティリスクとプライバシーリスクに関するものを含め、リスクの特定、評価、所有、対応、および受容に関するそれぞれのポリシーと手順を定める。組織のリスク管理は、最終的には組織のリーダーシップが所有する。 ERM プログラムは、ガバナンスとリスクおよびコンプライアンス（GRC）に関する全てのトピックと同様に、組織レベルで実施されるべきであり、クラウドサービスモデルの種類や、提供または利用されるクラウドサービスの種類に関係なく実施されるべきである。クラウド組織は、クラウドサービスの利用者としての役割であれ、クラウドサービスプロバイダーとしての役割であれ、リスクを適切に管理し、正式に文書化された、リーダーシップが後援するエンタープライズリスク管理プログラムを確立すべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** エンタープライズリスク管理（ERM）とは、組織のリスク管理全般のことである。サービス契約又は契約は、CSP と CSC との間のサービス範囲、サービスレベル、責任及び義務 などの重要な要素を定義する。契約において役割と責任が詳細に定義され、リスク管理に関する責任について言及される場合とされない場合があるが、企業はリスク管理に関する最終的な責任と説明責任を外部のプロバイダーに完全にアウトソーシングすることはできない。リスク管理の目的は、価値の創造と保護である。リスク管理プロセスには、ポリシー、手順、および実践を体系的に適用することが含まれる。これは、コミュニケーションとコンサルティング、状況の確立、リスクの評価、対応、モニタリング、レビュー、記録、および報告といった活動に適用される。CSP のリスクは、管理及びその他の措置が講じられた後に受け入れるリスク容量または残余リスクの最大量を定義するリスク選好度フレームワークを用いて算出されるべきである。 リスク管理手順は、経営及び意思決定の不可欠な一部であり、組織の構造、運営及びプロセスに統合されるべきである。リスク管理プロセスは、戦略レベル、業務レベル、プログラムレベル、プロジェクトレベルで適用することができる。リスク管理手順は、目的を達成するために、また、適用される外部及び内部の状況に合わせてカスタマイズされ、組織内で多くの適用が可能である。ERP プログラムの一部として、情報セキュリティリ	**実施ガイドライン：** **全てのサービスモデルに適用：** CPS の「実施ガイドライン」が適用される。 また、情報セキュリティリスク管理には、該当する場合、クラウドに関連する情報セキュリティリスクとデータプライバシーリスクを含めるべきである。 CSP を利用する場合、CSC は特定のリスクについて一定の責任を負い、それらのリスクを管理（受容、軽減、移転）する最終的な責任を負う。 CSP を利用する場合、CSC は特定のリスクについて一定の責任を負い、それらのリスクを管理（受容、軽減、移転）する最終的な責任を負う。CSC は、リスクを正しく管理できるよう、リスク選好度とリスク許容度を定めるべきである。CSC は、効果的なリスクポジションを保持できるよう、CSP の文書を見直すべきである。

スク管理手順が存在する。 情報セキュリティリスク管理には、組織に該当する場合、クラウドに関連する情報セキュリティリスクとデータプライバシーリスクも含めるべきである。 CSP と CSP は共に、情報セキュリティリスク管理プロセスを有するべきである。両者は、STAR プログラムやその他の広く知られたサイバー/クラウドセキュリティのフレームワークや標準に整合させることが推奨される。 CSP が他のプロバイダーのサービスを利用する場合、CSP は、CSC に対する情報セキュリティレベルが維持されるか、または維持されていることを保証するものとする。CSP がサプライチェーンに基づいてサービスを提供する場合、CSP は、サプライヤに情報セキュリティ目標を提供し、各サプライヤが目標を達成するためにリスク管理活動を実施するよう要求するものとする。	

Control Title	Control ID	Control Specification
組織のポリシーの見直し	**GRC-03**	少なくとも年 1 回、または組織内で大幅な変更が生じたときに、関連する全ての組織のポリシーと関連する手順をレビューする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、すべてのサービスモデル(IaaS/PaaS/SaaS)のに適用される。何故なら、全てのガバナンス・リスク・コンプライアンス（GRC）のトピックと同様に、ポリシーと手順の定期的な見直しは、組織レベルで実施され、クラウドサービスモデルの種類に関係なく、ポリシーと手順が組織にとって最新かつ適切で有効であることを確認すべきである。 CSP と CSC はそれぞれ個別に組織のポリシーと手順の定期的なレビューを実施する必要があり、各組織は自組織のポリシーのレビューの実施に全責任を負うが、他組織のポリシーのレビューについては責任を負わないため、この管理策の所有は共有	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。

（独立）される。組織のポリシーのレビューの必要性は、企業の全ての業務、製品、サービスをカバーする組織レベルの機能であるため、この管理策の共有（独立）所有は、提供または使用されるクラウドサービスの種類に関係なく適用される。	
実施ガイドライン： **全てのサービスモデルに適用：** 経営陣または上級管理職が情報セキュリティポリシーを承認し、コミットメントすることは、情報セキュリティ専門家の必要性と行為を正当化し、情報セキュリティ戦略が組織の戦略と期待の重要かつ適切な一部であることを保証するために必要である。 上級経営責任者（CISO、CSO、またはそれに相当する責任者）は、情報セキュリティ戦略やプログラムを成功裏に実施するために、情報セキュリティビジョンとミッションについて経営層に簡単に伝え、理解してもらわなければならない。経営層は、必要な支援、予算、リソースを提供するために、この情報を理解する必要がある。情報セキュリティポリシーは、セキュリティ戦略やセキュリティプログラムの基礎であり、組織の全スタッフが認識し、参加し、何をすべきかを知っていることを保証する方法である。 ポリシー、標準、および関連するガイダンスを定期的に更新することは、そのガイダンスが現在もビジネスニーズに適合しているか、新しい法律や規制に適合しなくなったか、または現在使用されている環境やテクノロジーに対して有効でなくなったかを確認するために重要である。ポリシー、標準、および関連するガイダンスは、少なくとも年 1 回、または組織内で大幅な変更が発生した場合（組織に導入された新技術、サイバーセキュリティ事件、大規模な業務変更、法規制環境の変更など）に見直すことを推奨する。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。 また、特定のクラウド環境やソリューションをスコープとする、特定のクラウド関連のポリシーや標準については、経営層の承認とサポートがあれば、遵守が容易になり、変更に対する抵抗が最小限に抑えられる。

Control Title	Control ID	Control Specification
ポリシーの例外プロセス	**GRC-04**	ガバナンスプログラムで義務付けられている承認された例外プロセスを確立し、ポリシーからの逸脱が発生した場合にはそれに常に従う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、すべてのサービスモデル(IaaS/PaaS/SaaS)のに適用される。なぜなら、GRC-01 に従えば、双方とも独自のセキュリティポリシーがあるからである。これらのポリシーの例外は、クラウドサービスモデルに依存しない。 組織のポリシー、標準、手順、およびその他の指示に対する例外を管理することは、組織のリスク管理の重要な側面である。CSP と CSC はそれぞれ、各組織のポリシーと手順を独自に策定し、各組織のリスクを独自に管理しており、そのようなポリシーに対する例外を管理する関連プロセスも同様に、それに応じて共有（独立）する機能である。 組織のポリシー管理及び組織のリスク管理プログラムは組織レベルの機能であるため、この管理策の共有（独立）所有権は、提供又は消費されるクラウドサービスの種類に関係なく適用される。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 例外プロセスを導入することは、実施する必要のある管理策を決定する際のリスク管理プロセスの重要な部分である。 セキュリティポリシーまたはポリシーの特定の部分に対する例外は、標準からの逸脱である。例外は、定義上、組織のリスクレベルを高めることになるため、新たなビジネスニーズと考えるべきではない。 例外は、組織標準、またはリスク改善標準を含む他の義務化された標準に照らして、セキュリティ対策が完全に実施されていないことに基づく。 そのため、例外が発生するたびに、以下の措置を実施する： a. 全ての適切な承認、一時的な継続期間、および代償となる管理策を含む例外登録簿を更新する。 b. 例外承認前にリスクを再評価し、リスクレベルが組織のリスク選好度を超えないようにする。 CSP は、CSC のセキュリティ体制に影響を及ぼす可能性のある例外について、CSC に通知する。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。 また、CSC は CSP と緊密に連絡を取り、オープンな対話を継続し、例外や例外の引き金となったリスクを将来的に CSP のセキュリティロードマップに含めるべきかどうかを理解することが推奨される。

Control Title	Control ID	Control Specification
情報セキュリティプログラム	**GRC-05**	全ての CCM の関連するドメインのプログラムを含む情報セキュリティプログラムを開発して実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実装責任は、CSP と CSC の両者で「互いに依存しない形で共有」し、それぞれ独立して実施する責任がある。CSP および CSC が、それぞれ別の情報セキュリティプログラムを策定することは、完全かつ独立した各自の責任である。CSC の情報セキュリティプログラムを策定または実施する責任は、CSP になく、CSP の情報セキュリティプログラムを策定または実施する責任は CSC にない。 この管理策の CSP の所有権は、CSP 自身の内部組織単位および関連する資産およびプロセス、並びに CSC に提供されるサービスおよび関連する資産およびプロセスを対象とする、1 つ以上の情報セキュリティプログラムの策定および実施に関連する。CSP には、CSC のための情報セキュリティプログラムを策定または実施する責任はない。 「互いに依存しない形で共有」する管理策は、提供される全てのサービスモデル（IaaS、PaaS、SaaS）に適用される。なぜなら、CSP のプログラムは CSC に対して提供されるすべてのサービスに適用さえるからである。 CCM ドメインを使用することで、関連する全てのクラウドセキュリティの側面が情報セキュリティプログラムに含まれ、STAR やその他の広く知られたサイバー／クラウドセキュリティのフレームワークや標準との整合性が確保される。	**管理策所有権の根拠：** この管理策の CSC の所有は、CSC 内部の組織単位、関連するクラウド資産および非クラウド資産、並びに、その他の利害関係者を対象とする情報セキュリティプログラムの策定及び実施に関連する。 Shared Independent（互いに依存しない形で）共有する所有は、利用される全てのサービスモデル（IaaS、PaaS、 SaaS）に適用される。何故なら、CSC のプログラムの対象範囲は、サービスモデルに関係なく、外部プロバイダーからサービスを取得し、実装し、またはその他の方法で関連付けられる全ての資産とプロセスを含むからである。 CCM のドメインを使用することで、関連する全てのクラウドセキュリティの考慮事項が情報セキュリティプログラムに含まれ、STAR やその他の広く知られているサイバー／クラウドセキュリティのフレームワークや標準との整合性が確保される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、業界のベストプラクティスが推奨する独自のセキュリティプログラムを有し、技術、情報、手順、および人員の全ての側面を対象とすべきである。 適切な場合には、組織内で連携する役割と責任を指定し、CSC お	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、クラウドセキュリティと CSP のリスク選好度を考慮した情報セキュリティプログラムを策定する。このプログラムの目的は、クラウドを含む全ての CSC 環境において、組織のデータ、サービス、プロセス、システム、その他のクラウド関

よびその第三者プロバイダーとの責任分担を文書化する。 CSP は、情報セキュリティプログラムを強化するために、CSC からのフィードバックや報告を利用すべきである。情報セキュリティプログラムは、CSC のニーズおよび特定の規制・法的要件（HIPAA、 PCI DSS、GDPR、Fred RAMP など）をカバーするように努めるべきである。CSP は、CSC が契約上および規制上の義務が満たされていることを保証すべきことを理解することが重要である。 CSP は、CSC が CSP のインフラストラクチャのセキュリティ評価を実施することを許可するかもしれない。また、CSP は、その範囲、条件、および評価された具体的な管理策を明確に定義して、公式な認証と証明書を公表することができる。STAR は、プロバイダーがそのような文書を公開するためのセントラルリポジトリを提供する。	連資産、アクティビティ、および運用がセキュアであり、機密性、完全性、および可用性が確保されていることを確認することである。 CSC は、企業全体のセキュリティ戦略およびセキュリティポリシーを遵守し、それに従うためにクラウドプログラムについて、詳細な RACI マトリックスを含む情報セキュリティ責任を持つ必要がある。このプログラムには、CSC に直接影響する全てのビジネス要件、セキュリティ要件、規制、および法律を含める必要がある。また CSP との責任分担に関する合意を理解し、文書化する。 CSC がクラウド環境を利用する場合、CSP は、その情報セキュリティプログラムにとって重要な部分であり、ERM の一部であるべきである。

Control Title	Control ID	Control Specification
ガバナンス責任モデル	**GRC-06**	ガバナンスプログラムを計画、実装、運用、評価、および改善するための役割と責任を定義し、文書化する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、IaaS, PaaS, SaaS で「独立」である。なぜなら、ガバナンス・リスク・コンプライアンス（GRC）は、全てのサービスモデルに適用されるためである。CSP と CSC の両者は、それぞれの組織における役割、責任、および経営コミットメントを定義し、実施すべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、ガバナンス業務の一環として、情報セキュリティが中核的な責任であることを強調するために、明確な RACI モデルを公式化すべきである。関連する情報セキュリティとリスクを含め、	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、ガバナンスの一環として、明確な RACI（Responsible, Accountable, Consulted, and Informed）モデルを公式化し、情報セキュリティが中核的な責任であるこ

クラウドサービスの提供を指示し、実現し、監督する責任と権限を有する個人を特定すべきである。 具体的には、CSP は、そのプラットフォーム上でホストされるインフラストラクチャ及びアプリケーションに関連する CSC のセキュリティプログラムに対応する責任ある個人又はグループを任命すべきである。この担当者またはグループは、CSC の全てのセキュリティ上の懸念に対応する責任を負い、関連するセキュリティ情報が入手可能になり、公開の準備が整った時点で、明確かつ透明性の高いコミュニケーションを行うべきである。	とを強調すべきである。関連する情報セキュリティとリスクを含め、クラウドサービスの提供を指揮し、実現し、監督する説明責任と権限を有する個人を特定すべきである。

Control Title	Control ID	Control Specification
情報システムに対する規制へのマッピング	**GRC-07**	組織に適用されるすべての関連する標準、規制、法律/契約、および法定要件を特定し、文書化する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、GRC が全てに適用される為、サービスモデル（IaaS、PaaS、SaaS）またはオンプレミスアーキテクチャに依存しない。CSP と CSC は、それぞれ適用される全ての関連標準、規制、法律／契約、および／または、法定のセキュリティ管理、並びに、これらの管理策がビジネスニーズとユースケースに、どのように役立つかを独自に分析し、情報セキュリティプログラムに含めるものとする。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、全ての契約上の要件が適切に満たされるように、管理要件マッピングの整合性と適切性を慎重に検討すべきである。CSP は、その運営国または業界サービスに関連するものを含め、全ての法的、規制上、契約上、法令上、または業界標準とその要件を特定し、検討し、文書化するために多大な努力を払うべきである。 利用される内部統制の枠組み、および組織内で実施される全てのポリシーとガバナンスポスチャは、組織の責任に対する一貫	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、運営国または業界サービスに関連するものを含め、全ての法的、規制的、契約上、法令上、または業界標準およびその要件を特定し、検討し、文書化するために多大な努力を払うべきである。 CSC は、CSP の選定を検討する際、自社の特定の要件を考慮すべきであり、CSA CAIQ またはその他の関連文書など、CSP の管理および管理の枠組みや評価を確認し、自社の目的を達成するためにサービスを利用できるかどうかを判断できるよう

性のある首尾一貫したアプローチを維持するために、上記の要件を具体的に参照するか、または組み込むべきである。CCM 管理策 A&A-04 は、この管理策内で定義されている要件の検証を要求している。CSP は、様々な要求事項への具体的な適用可能性を特定し、文書化することを確認すべきである。 次に、CSP は、CSC に対してデューデリジェンスが実施されていることを証明するために、認証、監査、評価、または証明書（例えば、ペイメントカード業界標準への準拠を示す PCI DSS 認証の取得）を通じた外部検証の取得を目指すべきである。 CSP は、大半の CSC の要件を考慮すべきであり、その地位を向上させ、新たな分野での成長を促進するために、特定のまたは追加の管理策を実施することを望むかもしれない。 CSP は、自社のサプライヤとのサービス手配において、サブサービス組織／アップストリームサプライヤの（各サービス提供契約／サービス契約に関連する）管理要件のマッピングと CSP 自身の要件との整合性および妥当性を慎重に検討し、ギャップの意味を分析および特定することで、自社の目的を達成するためにサービスを利用できるかどうかを判断し、自社の要件を満たすために必要な追加的な利用者側の管理策を実装および管理できるようにすべきである。	にアプリケーションを分析および特定し、補完的利用者主体管理（CUECs： Complementary user entity controls 委託会社の相補的な内部統制）を含め、自社の要件を満たすために必要な追加の利用者側管理を実装および管理することを推奨する。 CSC は、特定の要件に準拠する、または準拠の維持を支援できる CSP を選択すべきである。 利用される内部統制の枠組み、および組織内で実施される全てのポリシーとガバナンスポスチャは、組織の責任に対する首尾一貫したアプローチを維持するために、上記の要件を具体的に参照するか、または組込むべきである。CCM 管理策 A&A-04 は、この管理策内で定義されている要件の検証を要求している。CSP は、様々な要求事項への具体的な適用可能性を特定し、文書化することを確認するものとする。 次に、CSP は、クライアントに対して実証可能な場合（ペイメントカード業界標準への準拠を示す PCI DSS 認証の取得など）、認証、監査、評価、または証明を通じて外部からの検証を得るよう努めるべきである。

Control Title	Control ID	Control Specification
SIG 特別利益団体	**GRC-08**	ビジネスの背景に応じ、クラウド関連の SIG 特別利益団体やその他の関連組織との連絡手段を確立し、維持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠： この管理策は、GRC が全てに適用されるため、全てのサービスモデル（IaaS、PaaS、SaaS）に依存しない。各組織は、自社サービスのセキュリティポスチャを強化しうる（例えば、IoC、脅威レポート、脆弱性／欠陥の早期発見を利用した）助言と追加のセキュリティ及びガバナンス情報を提供する関連グループ、および／または、セキュリティ専門家を独自に特定し、それらとの緊密な連絡を構築する。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 情報セキュリティプログラムを維持し、継続的に改善し、インフラストラクチャと CSC との基礎的なインタフェースおよび接続の知識を深めるために、CSP は関連する利害関係者との連絡を維持すべきである。 CSP は、例えばバグ報奨金プログラム、セキュリティ研究および専門家コミュニティを利用して、自社のクラウド環境における潜在的な欠陥を調査し、テストすることを検討することができる（注：侵入的なセキュリティテストを行う場合、ユーザーは、CSP が設定した全てのパラメータおよび関連する法律上の要件の範囲内で運用するよう注意すること）。 さらに、CSP は、情報セキュリティポスチャを強化するために、公開および非公開のセキュリティフィード（訳注；セキュリティ情報をまとめたデータ配信など）の一部になるべきである。CSP は、利用者に関連する全ての情報（ホワイトペーパー、ポジションペーパー、研究コミュニティフォーラムへの参加など）を CSC に提供するものとする。 SaaS CSP が他の CSP（例えば、IaaS や他の SaaS プロバイダー）を利用する場合は、それらから得られた情報も提供する。	**実施ガイドライン：** **全てのサービスモデルに適用：** 情報セキュリティプログラムを維持し、継続的に改善し、インフラストラクチャとその基礎となるインタフェースおよび接続に関する知識を深めるために、CSC は、CSP と緊密な関係を維持し、最新の関連情報を可能な限り速やかに入手すべきである。 CSC は、ユーザーおよび研究コミュニティ、情報セキュリティの専門家、および様々なドメインの専門家、並びに事業に影響を与えるか、または事業に影響を及ぼす当局を含むが、これらに限定されない。 CSC は、例えばバグ報奨金プログラム、セキュリティ研究および専門家コミュニティを利用して、自社のクラウド環境における潜在的な欠陥を調査し、テストすることを検討しても良い（注：侵入的なセキュリティテストを行う場合、ユーザーは、CSP が設定した全てのパラメータおよび関連する法律上の要件の範囲内で運用するように、注意する必要がある）。

Control Domain HRS

2.9 人的リソースセキュリティ(HRS)

Control Title	Control ID	Control Specification
身元調査のポリシーと手順	**HRS-01**	アクセスするデータの分類、ビジネス要件、および許容可能なリスクと、現地の法律、規制、倫理、および契約上の制約に従って、全ての新入社員（リモート従業員、請負業者、およびサードパーティーを含むがこれらに限定されない）の身元調査のポリシーと手順を確立、文書化、承認、伝達、適用、評価、および維持する。少なくとも年１回ポリシーと手順をレビューし、更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： GRC は全てのサービスモデルに適用されるため、本管理策の実装責任はサービスモデル（IaaS、 PaaS、SaaS）に依存しない。これは共有され、各当事者、CSC および CSP によって実装される必要があるが、互いに独立している。両者は、それぞれの国、契約上および規制上の要件を満たすべき異なる審査方法及び審査プロセスを有することがある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、正社員および派遣社員、外部委託されたコンサルタント、およびその他のサードパーティーベンダーが、その役割によって必要とされるシステムまたはサイトへのアクセスのレベル、量、および頻度に関して、適切に審査され、吟味されていることを保証するための内部対策を実施する責任を負う。審査プロセスを確立し、システムへのアクセスを許可するいかなる活動に先行させることが望ましい。 審査プロセスは、当該プロセス中に収集された全ての個人データ／機微情報を区分するために、認可された専門部門によって実施されるべきである。CSP はスタッフの信頼レベルを CSC に保証するための合理的な手配を行うべきである。必要に応じて、政府機関や法執行機関など、CSC のシステムにアクセスするス	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

タッフの要件に対して、利用者固有の審査を実施すべきである。例えば、推薦者と連絡が取れない、あるいは確認チェックに時間がかかるなど、審査が遅延する場合には、暫定的に以下のような緩和策を実施すべきである： a. 入社日の延期 b. アクセスや認証情報を発行しない c. アクセスは許可するが、権限を制限または制限する 状況が複雑になる場合、または犯罪歴や懸念材料となる情報など、以前の問題が審査で検出された場合は、問題を上席に報告する、雇用のオファーを打ち切るためのプロセスが整備されているべきである。	
ポリシーには、以下に関する規定が含まれるべきである（ただし、これに限定されない）： a. 範囲と目的：身元調査を必要とする従業員、請負業者、および第三者の役職、役割、およびアクセスレベルの種類を含む、身元調査の範囲と目的。審査プロセスは、機微データへのアクセスレベルおよび責任の性質に合わせて調整されるべきである。 b. 現地の法規制の遵守：身元調査およびデータプライバシーに関する現地、地域、および国際的な法令を確実に遵守する。 i. 必要な同意の取得、データプライバシーを確保し、記録保持要件を遵守する。 ii. 異なる管轄区域における個人情報の取り扱いに関する具体的な規制を検討する。 c. 倫理および契約上の制約：倫理的配慮および顧客やパートナーとの契約上の義務。差別やプライバシーの侵害の可能性を最小限に抑え、公正かつ公平な方法で身元調査が行われることを保証すべきである。 d. 身元確認のリスク評価：身元確認の範囲は、アクセスするデータ分類、ビジネス要件、および許容可能なリスクレベルに比例すべきである。機密性の高い役割や機密性の高いデータへのアクセスは、より厳格な身元調査を必要とする場合がある。 e. 検証チェック：実施される具体的な検証チェックの概要を説明する。 i. 身元確認：政府発行の有効な書類によって個人の身元を確認すること。 ii. 教育の検証：要求された学歴や資格の検証（例えば主張されている学位や資格など） iii. 職歴の確認：過去の職歴や職務内容（役職、期間、退職理由など）を確認すること。 iv. リファレンスチェック：候補者のスキル、仕事習慣、信頼性を評価するため、専門家によるリファレンスチェックを実施する。 v. 犯罪歴調査：現地の法律や規則に従って犯罪歴調査を実施し、犯罪の性質に応じて不適格の標準を定め	

る。

f. サードパーティーの身元調査サービス：サードパーティーの身元調査業者を使用する場合、ポリシーは、評判が高くセキュアなサービスベンダーを選択するための厳格なガイドラインを確立する必要がある。
   i. サードパーティーベンダーや請負業者との契約に身元確認要件を盛り込む
   ii. 提供されるサービスと付与されるアクセスに基づき、精査のレベルを指定する。
   iii. 請負業者やサードパーティーベンダーに対して、組織のセキュリティポリシーに沿ったセキュリティ意識向上トレーニングの受講を義務付ける。

g. 開示と承認：身元調査を実施するために必要な同意と承認を個人から得るためのプロセスの概要を示す。また、身元調査の目的、情報の使用方法、保護方法を明確にする。

h. 記録の保持：データプライバシー規制および契約上の義務（個人情報の保管および廃棄に関する義務も含む）の遵守を確保しつつ、身元調査記録を保持する期間に関する要件を定める。説明責任およびコンプライアンス目的のため、身元確認プロセスの監査証跡を維持する。

i. インシデント対応：身元確認の検証プロセスにおいて、不利または予期せぬ発見が明らかになった場合のインシデント対応プロトコル。

j. 承認：組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与
   i. ポリシーと手順の変更または修正については、承認プロセスを確立することが望ましい。
   ii. 文書化した承認の記録（日付、承認者の氏名、および関連するコメントまたはディスカッションを含む）を維持すること。

k. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進すべきである。

l. 維持と見直し：身元確認チェックのポリシーと手続は、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映するために、少なくとも年 1 回は文書化、レビュー、および更新すべきである。

Control Title	Control ID	Control Specification
テクノロジーの適正利用に関するポリシーと手順の使用	HRS-02	組織が所有または管理する資産の適正な使用のために、割り当てとその条件を定義するためのポリシーと手順を確立、文書化、承認、伝達、適用、評価、および維持する。少なくとも年１回ポリシーと手順を見直して更新する。

Control Ownership by Service Model		
IaaS	PaaS	SaaS
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	CSC
管理策の根拠： 管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく同じであり、基本的に本管理策は CSC と CSP の両方で共有されるが、互いに独立している。両者は、それぞれの国、契約上、または規制上の要件に応じて、自社のポリシーとプロセス内で満たすべき技術標準や要件について、異なる利用ポリシーの要件を有している可能性がある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、システムと顧客の情報を保護するために、スタッフが組織のテクノロジーを適切に使用することを保証する責任を有する。これらのポリシーは、スタッフに提供され、年次セキュリティ研修に含まれるべきである。 ポリシーには以下を含むテクノロジーを使用する全ての要素を包含するものでなければならない：ソーシャルメディアの利用、電子メールの送受信、インターネットの閲覧・利用、コンテンツの送信・転送、電子通信およびインスタントメッセージ、ビデオ、アプリケーションの使用、ソフトウェアのセキュリティ、設定の変更など。 これらのポリシーは、組織の IT システムに対する一般的な「やるべきこと」と「やってはいけないこと」として機能すべきである。また、権限の付与や資産の保護など、組織資産の使用方法の概要を示す。さらに、組織がこれらのデバイスの個人使用を許可するかどうかも規定する必要がある。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

ポリシーには、以下に関する規定を含むべきである（但し、これに限定されない）：

a. 範囲と目的：クラウドリソース、デバイス、ソフトウェア、データなど、対象となる資産の範囲を定義する。
   i. その目的は、クラウドサービスが責任ある倫理的な方法で使用されることを保証することにより、組織の資産、データ、評判を保護することであると明記されるべきである。
   ii. 「許容される使用」、「不正使用」、「機微情報」などの重要な用語の定義を提供すること。
b. 禁止される使用：組織が所有または管理するクラウド資産について、以下を含む禁止される用途を概説する。会社所有のデバイス、個人所有のデバイス、クラウドベースのサービスおよびアプリケーション。禁止される使用例には以下が含まれる：
   i. 資産を個人的または業務外の活動に使用する
   ii. 許可されていないソフトウェアやアプリケーションのインストール
   iii. 違法または不適切なコンテンツへのアクセスまたは共有
   iv. 資産のセキュリティに損害を与えたり、危険にさらしたりする可能性のある行為に従事すること
c. 許容される使用：ポリシーは、組織が所有または管理する資産の許容される使用に関するガイドラインを示すべきである。許容される用途の例には、以下が含まれる：
   i. 仕事関連の活動に資産を使用する
   ii. 承認されたソフトウェアアプリケーションのインストール
   iii. 業務関連情報へのアクセスと共有
   iv. 責任ある倫理的な方法で資産を使用する
d. 法規制の遵守：ポリシーは、組織が所有または管理する資産の使用に関して適用される全ての法律および規制を遵守する必要性を強調すべきである。
e. 違反の結果：ポリシーは、懲戒処分（解雇を含む）を含む、ポリシーに違反した場合の結果を概説すべきである。
f. 承認組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与
   i. ポリシーと手順の変更または修正については、承認プロセスを確立すべきである。
   ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。
g. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進すべきである。
h. メンテナンスとレビューポリシーと手順は、進化する

クラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映するために、少なくとも年 1 回は文書化、レビュー、更新する。	

Control Title	Control ID	Control Specification
クリーンデスクポリシーと手順	**HRS-03**	無人のワークスペースに公然と見える形で機微データがないようにするポリシーと手順を確立、文書化、承認、伝達、適用、評価、および維持する。少なくとも年 1 回ポリシーと手順を見直して更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： 管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく同じであり、基本的に本管理策は CSC と CSP の両方で共有されるが、互いに独立している。両者は、それぞれの国、契約上、または規制上の要件に応じて、満たすべきポリシーとプロセスで概説する必要のある異なるクリーンデスク標準または要件を有している可能性がある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、組織内にセキュリティ文化を醸成し、偶発的な行為と悪意のある行為の両方から CSP 自身とその利用者を保護する責任を負う。 クリーンデスクポリシーは、情報セキュリティの基本要素であり、機微データを盗難から物理的に保護する。このポリシーは、指定された家具、金庫、ロッカーに資産をセキュアに保管することを義務付け、機微情報を不正アクセスから効果的に保護する。さらに、画面ロックを実施することで、見過ごし、ショルダーサーフィン、潜在的な悪意ある行為から保護し、特に仮想化環境におけるセッションキャプチャのリスクを低減する。 セキュリティをさらに強化するため、ホワイトボード、書き込み可能な壁、その他の書き込み可能な面、ノート、付箋紙、同様	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

の資料は、使用しないときは片付けるか、セキュアにシュレッダーにかけるか、きれいに拭き取るべきである。モバイル機器やデスクトップは、盗難防止のために物理的なケーブルロックを装備し、サーバーや機密性の高い機器は、セキュアなラックやケージ内に保管する。 プリンタに文書を送る場合、機微情報への不正アクセスを防ぐため、これらの文書は速やかに回収されるべきである。	
ポリシーには、以下に関する規定が含まれるべきである（ただし、これに限定されない）： a. 適用範囲と目的：このポリシーは、物理的なワークステーション、ノートパソコン、モバイルデバイス、およびクラウドベースのワークスペースを含む全てのワークスペースに適用され、ワークスペースを無人にする全ての従業員、請負業者、および第三者に対して、データの機密性を保護し、機密情報への不正アクセスを防止する。 b. 画面ロック機構： i. 全てのデバイスに、一定時間（例えば5分を超えない）操作されないと作動する自動画面ロック機構を義務付ける。 ii. 画面のロックを解除するために、強力なパスワード、PIN、または生体認証を要求する（IAM-02を参照） iii. 全ユーザーに二要素認証（2FA）を導入し、画面ロックのセキュリティをさらに強化する。 c. 自動ログアウト： i. ユーザーが不注意でセッションを開いたままにしないように、一定時間操作がない場合は自動的にセッションをログアウトする機能を実装する。 ii. 未使用時にリモートデスクトップセッションを自動的にロックし、再アクセス時にセキュアな認証を要求する。 d. プライバシー画面：近くにいる人に画面が見えるのを制限するため、デバイスにプライバシー画面の使用を奨励または義務付ける。 e. クリーンデスクポリシー：従業員はワークスペースを清潔に保ち、デスクから離れているときに機微情報が公然と見えないようにする。機密文書には、文書カバーまたは施錠可能な保管キャビネットを推奨する。 i. 機密文書、プリントアウト、メモを目につく場所に放置しないこと。 ii. 機密文書は、不要になったらシュレッダーにかけるか、厳重に廃棄する（DSP-02を参照）。 f. セキュアな物理デバイス： i. ワークステーション、ノートパソコン、モバイル機器を短時間でも放置する場合はロックすること	

ii. 強力なパスワードを使用し、全てのデバイスで多要素認証（MFA）を有効にする。 iii. 暗号化されていない限り、USB ドライブなどのリムーバブルメディアに機密データを保存しない。 g. 承認：組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与 i. ポリシーと手順の変更または修正については、承認プロセスを確立すべきである。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。 h. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進すべきである。 i. メンテナンスとレビュー：ワークスペースのポリシーと手順は、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映するために、少なくとも年 1 回文書化、レビュー、更新する。	

Control Title	Control ID	Control Specification
リモートおよび在宅勤務に関するポリシーと手順	**HRS-04**	リモートの拠点や場所でアクセス、処理、または保存される情報を保護するためのポリシーと手順を確立、文書化、承認、伝達、適用、評価、維持する。少なくとも年 1 回ポリシーと手順を見直して更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： 管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく同じであり、基本的に本管理策は CSC と CSP の両方で共有されるが、互いに独立している。両者は、それぞれ異なるリモートワーク及び在宅勤務のポリシーと手順を持っている可能性があり、それは、各組織がそれぞれの国、契約上、又は規制上の要件に応じて達成すべきポリシー及びプロセス内の標準及び要件にリンクする。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。

実施ガイドライン： **全てのサービスモデルに適用：** リモートおよび在宅勤務のポリシーは、CSP が担当者にそのような活動を許可する場合に導入されるべきである。リモートワークは、クラウド組織のリスクと脅威のプロファイルを増大させる。CSP には、自社のコアシステムと CSC のデータを保護する責任がある。担当者がリモートで作業する際に従うべき適切なセキュリティ要件、管理、および手順を提供するために、ポリシーを定義し、デプロイする必要がある。 分散化された職場環境への移行は、個人が警戒しなければならない様々なサイバーセキュリティの脅威をもたらすため、担当者はリモートで仕事をする際のリスクについて訓練を受け、情報を得る必要がある。 一般的なリスクのひとつは、フィッシング攻撃を受けやすくなることである。さらに、家庭環境でセキュアでない Wi-Fi ネットワークを使用することは、不正アクセスやデータ傍受の道を開くことになり、潜在的な脅威となる。ノートパソコンやモバイルデバイスの紛失や盗難は、企業データへの不正アクセスにつながる可能性があるため、リモートワーカーはデバイスのセキュリティにも注意する必要がある。 さらに、個人所有のデバイスやセキュアでないアプリケーションを業務に利用することは、組織をデータ侵害にさらし、機密情報の機密性を損なう可能性がある。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。
ポリシーには、以下に関する規定が含まれるべきである（ただし、これに限定されない）： a. 適用範囲と目的：本ポリシーは、以下の事項にアクセス、処理、または関与する全ての従業員、請負業者、およびサードパーティーベンダーに適用される。 クラウドコンピューティングとクラウドセキュリティの観点から、遠隔地や遠隔地でのアクセス、処理、保管される情報を保管する。ポリシーの目的は、遠隔地の従業員が組織のクラウドセキュリティポリシーと手順を認識し、遵守することを保証することである。 b. セキュアなネットワーク接続：リモートデバイスと企業ネットワークの間で、強力な暗号化プロトコルと認証メカニズムを備えたセキュアで暗号化された通信を行うために、VPN の使用を義務付ける。 c. リモートワークの MFA アクセス：企業システムやクラウドサービスへのアクセスに MFA の使用を義務付ける。全てのデバイスとアプリケーションで MFA を使用し、セキュリティのレイヤーを追加することを推奨する。 d. エンドポイントの保護：マルウェアやその他のセキュ	

リティ脅威を検出・防止するためのエンドポイント保護ソフトウェアの導入を義務付ける。

i. モバイルデバイス管理（MDM）またはエンドポイント管理ソリューションを導入し、リモートデバイスの設定、監視、セキュリティの実施を行う（マルウェア対策、デバイスの暗号化、セキュアな電子メールなど）（UEM ドメインを参照）

ii. リモートワーカーに公衆 Wi-Fi を使用するリスクについて教育し、公衆ネットワークに接続する際には VPN の使用を推奨する。

iii. 強力な暗号化（WPA3）の使用やデフォルトの認証情報の変更など、家庭用 Wi-Fi ネットワークを保護するためのガイドラインを提供する。

e. セキュアなリモートデスクトップソリューション：該当する場合、強力な暗号化と認証を備えたセキュアなリモートデスクトップソリューションの使用を義務付ける。

f. セキュアなファイル転送：個人的な電子メールアカウントやセキュアでないファイル共有サービスを、業務に関連するタスクに使用しないようにする。

g. 定期的なソフトウェアアップデート：可能な限り自動アップデートを有効にし、ソフトウェアを最新の状態に保つことの重要性をユーザーに教育する。

h. リモートデータのバックアップ：リモートデバイスに保存されている重要データの定期的なバックアップを義務付け、データの復元手順を定期的にテストし、紛失やセキュリティインシデントが発生した場合にデータを復元できることを確認する。

i. セキュアなファイル転送：個人的な電子メールアカウントやセキュアでないファイル共有サービスを、業務に関連する作業に使用しないようにする。

j. セキュアな印刷：機微データを含む印刷文書を直ちに取り出すなど、リモートワーカーにセキュアな印刷方法を教育する。

k. 承認組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与

i. ポリシーと手順の変更または修正については、承認プロセスを確立すべきである。

ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。

l. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進すべきである。

m. メンテナンスとレビュー：リモートワークのポリシーと手順は、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映するために、少なくとも年 1 回は文書化、レビュー、更新する必要がある。

Control Title	Control ID	Control Specification
資産の返却	**HRS-05**	退職した従業員による組織所有資産の返却手順を確立し、文書化する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく同じであり、基本的に本管理策は CSC と CSP の両方で共有されるが、互いに独立している。両者は、それぞれ異なるリモートワーク及び在宅勤務のポリシーと手順を持っている可能性があり、それは、各組織がそれぞれの国、契約上、又は規制上の要件に応じて達成すべきポリシー及びプロセス内の標準及び要件にリンクする。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、退職した、または退職予定の従業員に対して、組織所有のデータを含む企業所有の資産を返却するための手順を確立し、文書化する責任を有する。そのためには CSP 資産の追跡または管理手続を実施する必要があると推測される。即時の返却が不可能な場合、デバイスを遠隔操作で消去またはロックする機能を導入する必要がある。 整理用具の返却には、以下を含むべきである： a. ユーザーのエンドポイント機器（ラップトップ、モバイル、タブレット） b. ポータブルストレージ機器（USB、リムーバブルハードドライブなど） c. 特殊装置 d. IT システム、物理的サイト、物理的アーカイブ用の認証ハードウェア（FIDO キー、メカニカルキー、トークン、スマートカード e. 情報の物理的コピー（手書き、印刷物など）	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、退職した、または退職予定の従業員に対して、組織所有のデータを含む企業所有の資産を返却するための手順を確立し、文書化する責任を有する。そのためには CSC は資産の追跡または管理手順を定めておく必要があると推測される。即座の返却が不可能な場合は、デバイスを遠隔操作で消去またはロックする機能を導入する必要がある。 組織の資産返却には、以下を含むべきである： a. ユーザーのエンドポイント機器（ラップトップ、モバイル、タブレット） b. ポータブルストレージ機器（USB、リムーバブルハードドライブなど） c. 特殊装置 d. IT システム、物理的サイト、物理的アーカイブ用の認証ハードウェア（FIDO キー、メカニカルキー、トークン、スマートカード e. 情報の物理的コピー（手書き、印刷物など）

CSP は、また、技術的な手順またはポリシー（NDA など）を通じて、解約通知期間中の個人による情 報の不正コピー、複製、または転送を防止および抑止するよう努めなければならない。	CSC は、また、技術的な手続きやポリシー（NDA 等）を通じて、契約解除通知期間中の個人による情報の不正なコピー、複製、転送を防止し、抑止するよう努めなければならない。

Control Title	Control ID	Control Specification
雇用の終了	**HRS-06**	雇用の変更に関する役割と責任の要点を説明する手順を確立し、文書化し、全ての従業員に伝達する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく同じであり、基本的に本管理策は CSC と CSP の両方で共有されるが、互いに独立している。両者は、それぞれ異なるリモートワーク及び在宅勤務のポリシーと手順を持っている可能性があり、それは、各組織がそれぞれの国、契約上、又は規制上の要件に応じて達成すべきポリシー及びプロセス内の標準及び要件にリンクする。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、雇用契約終了後に適用される責任と義務を従業員に認識させる雇用終了ポリシーまたは手順を確立し、伝達する責任がある。契約終了後の義務は、更新された NDA、競業避止義務、またはその他の法的文書の形で、雇用終了する従業員に提示される場合がある。これらは雇用モデルの変更にも適用される。 ポリシーまたは文書には、企業秘密、知的財産、顧客データ、その他組織にとって価値ある情報など、組織情報の守秘義務を維持するための要件を含めるべきである。その責務は、雇用条件の詳細とリンクさせるべきである。 契約や職務が終了した場合、または役割、チーム、部署が変更された場合、社外要員も同じプロセスで解雇または変更される	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、雇用契約終了後に適用される責任と義務を従業員に認識させる雇用終了ポリシーまたは手順を確立し、伝える責任がある。契約終了後の義務は、更新された NDA、競業避止義務、またはその他の法的文書の形で、解雇する従業員に提示される場合がある。これらは雇用モデルの変更にも適用される。 ポリシーまたは文書には、企業秘密、知的財産、顧客データ、その他組織にとって価値ある情報など、組織情報の守秘義務を維持するための要件を含めるべきである。その責務は、雇用条件の詳細とリンクさせるべきである。 契約や職務が終了した場合、または役割、チーム、部署が変更された場合、社外要員も同じプロセスで解雇または変更され

べきである。 CSP は特定の CSC に対し、その要件または契約上の合意に関して行った制限または追加規定について注意を払うべきである。	るべきである。 さらに、CSC は重要な変更があった場合、または該当する場合、クラウド環境に対する重要な管理権限を有する者が解任された場合は、その旨を CSP に通知する必要がある。CSP は、当該者のアクセスを無効化または制限する必要がある場合がある。

Control Title	Control ID	Control Specification
雇用契約プロセス	**HRS-07**	従業員が雇用契約に署名してから、組織の情報システム、リソース、および資産へのアクセスを許可する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく同じであり、基本的に本管理策は CSC と CSP の両方で共有されるが、互いに独立している。両社は、アクセス契約に署名または同意する際、従業員に対して異なる要件を課すことができる。NDA、AUP、契約などである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、従業員が組織の資産、情報システム、またはリソース（付き添いなしの物理的な場所を含む）へのアクセスを許可される前に同意書に署名する手順を確立し、周知する責任を負う。合意には、雇用条件、役割と責任、またはセキュリティ標準が含まれる。 協約の概要を定める際には、署名された協約なしでのアクセスを防止するための規定、協約違反に対するアクセスの取り消し、懲戒手続きなどを設けるべきである。 利用規約は、社内のポリシーおよび要件、規制、または法律の変更に合わせて見直し、更新されなければならない。変更点は	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、従業員が組織の資産、情報システム、又はリソース（付き添いなしの物理的な場所を含む）へのアクセスを許可される前に同意書に署名する手順を確立し、周知する責任を負う。合意には、雇用条件、役割及び責任、またはセキュリティ標準が含まれる。 協約の概要を定める際には、署名された協約なしでのアクセスを防止するための規定、協約違反に対するアクセスの取り消し、懲戒手続きなどを設けるべきである。 利用規約は、社内のポリシーおよび要件、規制、または法律の変更に合わせて見直し、更新されなければならない。変更点は

スタッフに伝え、新しい条件に同意できるようにする。 CSP は契約上、署名が必要となる可能性のある CSC 協定についてもスタッフに周知することが求められる場合がある。	スタッフに伝え、新しい条件に同意できるようにする。

Control Title	Control ID	Control Specification
雇用契約書の内容	**HRS-08**	組織は、確立された情報ガバナンスおよびセキュリティポリシーを遵守するための条項や条件を雇用契約に含める。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： 基本的に、この管理策は CSC と CSP の両者で共有される。ただし本統制は各当事者が独立して実施する。両当事者は、確立された情報ガバナンス及びセキュリティポリシーの遵守を条件とする雇用契約を確実に締結すべきであるが、そのような契約は適用される法律及び規制要件に依存する。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は従業員および請負業者の採用時に、関連する行動規範、情報ガバナンス、およびセキュリティとプライバシーのポリシーを伝達するものとする。全ての従業員および請負業者は、採用時およびその後毎年、関連する研修を受講する。従業員および請負業者は、定められたポリシーの確認書に署名するものとする。ポリシーの変更は、従業員および請負業者に通知され、承認の署名を必要とする。雇用契約および業務委託契約には、守秘義務条項を盛り込むべきである。CSP はポリシーを守らなかった場合の結果を伝え、従業員が契約に違反した場合は適切かつ相応の措置を講じるべきである。	**実施ガイドライン：** CSC は従業員および契約社員の採用時に、関連する行動規範、情報ガバナンス、およびセキュリティとプライバシーのポリシーを伝達するものとする。全ての従業員および請負業者は、採用時およびその後毎年、関連する研修を受講する。従業員および請負業者は、定められたポリシーの確認書に署名するものとする。ポリシーの変更は、従業員および請負業者に通知され、承認の署名を必要とする。雇用契約および業務委託契約には、守秘義務条項を盛り込むべきである。CSC はポリシーを守らなかった場合の結果を伝え、従業員が契約に違反した場合は適切かつ相応の措置を講じるべきである。

Control Title	Control ID	Control Specification
各人の役割と責任	**HRS-09**	情報資産とセキュリティに関連する従業員の役割と責任を文書化し、伝達する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく変わらない。基本的に、本統制は CSC と CSP の両方で共有されるが、統制は互いに独立している。しかし両者は、情報資産、プライバシー、セキュリティに関連する従業員の役割と責任を文書化し、伝達すべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は情報資産保護のガイダンスと責任を特定し、定義し、文書化し、伝達すべきである。 全ての従業員、請負業者、臨時職員は、以下のタイミングでアクセス、職務、責任に見合った役割ベースのセキュリティトレーニングを受ける必要がある：サービス契約の開始時の企業の施設、リソース、資産へのアクセスを許可される前、およびその後毎年。 関連ポリシーの変更は、従業員、請負業者、臨時職員に通知されるべきである。	**実施ガイドライン：** CSC は情報資産保護に関するガイダンスと責任を特定し、定義し、文書化し、伝達すべきである。 また、これらは毎年レビューされ、更新する必要がある。 全ての従業員、請負業者、臨時職員は、以下のタイミングでアクセス、職務、責任に見合った役割ベースのセキュリティトレーニングを受ける必要がある：サービス契約の開始時の企業の施設、リソース、資産へのアクセスを許可される前、およびその後毎年。 関連ポリシーの変更は、従業員、請負業者、臨時職員に伝達されるべきである。

Control Title	Control ID	Control Specification
機密保持契約	**HRS-10**	計画された間隔で、データの保護と運用の詳細に関する組織のニーズを反映した非開示／機密保持契約の要件を特定、文書化、およびレビューする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく変わらない。基本的に本管理策は、CSC と CSP の両方で共有されるが、互いに独立している。両組織は、データ及び業務詳細の保護に関する組織のニーズを反映した非開示／秘密保持契約の要件を特定し、文書化し、計画的な間隔でレビューすべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、NDA/秘密保持契約のテンプレートを維持し、定期的なレビューを通じて適切性と最新性を確保すべきである。 契約条件は、組織の情報セキュリティ要件に基づくべきである。対象となる情報の種類は、許容されるアクセスおよび情報取扱プロトコルを定めるべきである。合意には、以下に限定されないが、以下を含めるべきである： a. 保護される情報 b. 契約期間 c. 契約当事者 d. 契約における各当事者の責任 e. 契約終了後のデータ破棄に関する条件 f. 契約条項違反が発生した場合に予想される措置 g. CSP は、秘密情報を第三者と共有する前に、NDA/秘密保持契約を締結するよう要求すべきである。 雇用条件、従業員、および請負業者は、CSP 情報資産にアクセスする前に、機密保持契約または非開示契約に署名することを義務付けられるべきである。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
セキュリティ意識向上トレーニング	**HRS-11**	組織の全ての従業員に向けたセキュリティ意識向上トレーニングプログラムを確立、文書化、承認、伝達、適用、評価、維持し、定期的にトレーニングの更新を行う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく変わらない。基本的に本統制は CSC と CSP の両方で共有されるが、統制は互いに独立している。両者は、組織の全従業員を対象としたセキュリティ意識向上トレーニングプログラムを確立、文書化、承認、伝達、適用、評価、維持、定期的にトレーニングの更新を行う。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** これには、対話型トレーニングモジュール、イントラネットコンテンツ、オンラインウェビナー、ビデオ、電子メールコミュニケーション、ポスター、チェックリスト、ヒントカードなどが含まれるが、これらに限定されない。セキュリティ及びプライバシーに関する意識向上トレーニングは、全従業員及び請負業者に対し、入社時及びその後毎年実施し、従業員の責任と企業資産を保護するための必要な手段について教育する必要がある。 研修受講簿を整備すること。組織メンバーの役割と責任を考慮し、それに応じたトレーニングを実施する。開発者に的を絞ったセキュアコーディングに関するトレーニングを実施する。セキュリティ意識向上トレーニングプログラムは、少なくとも年 1 回見直し、必要に応じて更新する。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
個人データおよび機微データの意識向上とトレーニング	**HRS-12**	機微性の高い組織および個人データにアクセスする全ての従業員に、適切なセキュリティ意識向上トレーニングと、組織に関連する職務についての手順、プロセス、およびポリシーの定期的な更新を提供する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく変わらない。基本的に本統制は CSC と CSP の両方で共有されるが、互いに独立している。両者は、機密性の高い組織データ及び個人データにアクセスする内部要員及び外部要員に対して、適切なセキュリティ意識向上トレーニングを実施し、組織に関連する専門的な職務に関連する組織の手順、プロセス、及びポリシーを定期的に更新する。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** セキュリティ意識向上トレーニングは、担当者の責任と、個人データや機微データを保護するために必要な手段について教育するものでなければならない。トレーニングには、個人データや機微データの取り扱いに影響する様々な規制や法的要件を含めるべきである。 さらに、組織の手順、プロセス、ポリシーの変更を取り入れるために、定期的にトレーニングを行うべきである。 研修は、全従業員および契約社員に対し、入社時およびその後毎年実施されなければならない。研修の出席簿を管理すること。 システムにアクセスできる全ての人は、情報セキュリティとプライバシーポリシーを認識すべきである。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
コンプライアンスに関するユーザーの責任	**HRS-13**	従業員に、確立されたポリシーと手順、および適用される法律、法令、または規制のコンプライアンス義務の認識と、コンプライアンスを維持するための役割と責任を認識させる。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines

CSP	CSC
管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャの採用に関係なく変わらない。基本的に本管理策は CSC と CSP の両方で共有されるが、互いに独立している。両組織は、確立されたポリシーと手順、規制、および法的枠組みに対する認識と遵守を維持するための役割と責任を従業員に認識させるべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、職員にその責任を定期的に思い出させる研修および意識向上プログラムを維持すべきである。これらの責任には、確立されたポリシーと手順、規制、および法的枠組みに対する認識と遵守の維持が含まれる。 研修と意識向上プログラムには、次のようなものが含まれる。キャンペーン、小冊子、ポスター、ニュースレター、Web サイト、説明会、ブリーフィング、e ラーニングモジュール、E メールなど、適切な物理的または仮想的チャネルを通じた啓発活動。 全ての従業員、請負業者、およびインターンは、各自の担当分野に関連するセキュリティとプライバシーのポリシー、手順、および標準を認識し、遵守する責任を負う。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Domain IAM

2.10 アイデンティティとアクセス管理(IAM)

Control Title	Control ID	Control Specification
アイデンティティおよびアクセス管理のポリシーと手順	**IAM-01**	アイデンティティおよびアクセス管理のポリシーと手順を確立、文書化、承認、周知、実装、評価、維持する。少なくとも年１回、ポリシーと手順を見直して更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP の管理策の所有権は、ID（すなわちユーザー、システム／プロセス、サービスおよびそのほかのセキュリティ主体）と、CSC に提供されるクラウドサービスに関連する組織単位、基盤、および資産内の CSP が統制するリソースへのアクセスを管理するためのポリシーと手順に関係する。	**管理策所有権の根拠：** CSC の管理策の所有権は、ID（すなわち、ユーザー、システム／プロセス、サービス、およびその他のセキュリティ主体）と、組織単位内のリソースおよび CSP のリソースに関連する資産へのアクセスを管理するためのポリシーと手順に関連する。 CSC は ID およびアクセス管理策のポリシーと手順を確立する際に、CSP によってサポートされ、利用可能になっている ID およびアクセス管理機能および技術について考慮する必要がある。
実施ガイドライン： **IaaS プロバイダー：** CSP は、物理インフラストラクチャ（ホストおよびネットワークを含む）および関連管理インタフェースの ID およびアクセス管理ポリシーと手順の確立、文書化、実装、実施、レビュー、および維持に責任を負う。	**実施ガイドライン：** **IaaS 利用者：** CSC は、CSC の管理プレーン、CSC がクラウド基盤上に配置する仮想ホスト、仮想ネットワーク、アプリケーション、及び関連リソース、並びにクラウドサービスにアクセスするためのユーザーエンドポイントに対する識別、認証、及びアクセス管理のポリシーと手順を確立、文書化、実装、実施、レビュー、および維持する責任を負う。
PaaS プロバイダー： CSP は、クラウドサービスの基盤となるプラットフォーム資源、ミドルウェア、および API に対する ID とアクセスを管理するためのポリシーと手順を確立、文書化、実装、実施、レビュー、および維持する責任を負う。	**PaaS 利用者：** CSC は、CSC 担当者、請負業者およびサービスプロバイダーが、CSC がプラットフォーム上にデプロイするクラウドサービス、データおよびその他リソースにアクセスするために使用するアプリケーション、ディレクトリおよび管理サービス、PC およびモバイル機器に対する ID、認証及びアクセス管理のポ

	リシーと手順を確立、文書化、実装、実施、レビュー、および維持する責任を負う。
SaaS プロバイダー： CSP は、クラウドサービスの基盤となるプラットフォーム資源、仮想マシン、ネットワーク資源、および関連する管理プレーンまたは管理インタフェースに対する ID とアクセスを管理するため のポリシーと手順を確立、文書化、実装、実施、レビュー、および維持する責任を負う。 3 つのサービスモデルそれぞれについて、CSP は、ID およびアクセス管理の機能と技術を文書化し、CSC に伝えるべきである。	**SaaS 利用者：** CSC は、CSC 担当者がクラウドサービス、データ（アプリケーション、利用者提供データ、ユーザーデータ、設定データを含む）、ユーザー、管理者アカウントにアクセスするために使用する PC およびモバイル機器について、ID およびアクセス管理のポリシーと手順を確立、文書化、実装、実施、レビュー、および維持する責任を負う。 CSP のポリシーが適用される。
ポリシーには、以下に関する規定を含むべきである（但し、これに限定されない）： a. 範囲と目的：IAM ポリシーの適用範囲は、ポリシーの対象となる ID、システム、およびデータを含めて定義されなければならない。IAM ポリシーの目的は、データの機密性、完全性、可用性の確保、関連する規制の遵守など、明確に示す必要がある。 b. ID のインベントリ：クラウド環境内の ID のインベントリを確立し、維持するための要件。アクティブでなくなり、必要でなくなった ID は、無効化または削除されるべきである。 c. 職務の分離（SoD）：クラウド環境を侵害するために使用される可能性のある過度なアクセスを ID が持つことを防ぐ。 d. 最小特権の原則（PoLP）：職務を遂行するために必要な最小レベルのアクセス権のみを ID に付与すること。アクセス許可は、職務の役割に沿ったものであることを確認するため、定期的にレビューし、更新する。 e. アクセスの提供：アクセス規定を承認、記録、伝達するためのプロセス、時間枠、責任を概説する。 f. アクセスの変更および取り消し：転居者、離職者、または身分証明書の変更に伴うアクセス削除のプロセス、時間枠、および責任を概説する。 g. アクセスの見直し：最小特権および職務分掌の原則の遵守を確保するために、ID アクセスを見直し、再検証する手順。 h. 特権アクセスロールの分離：クラウド環境を侵害するために使用される可能性のある過剰な特権アクセスを、どの ID にも持たせないようにする。管理、ロギング、暗号化アクセスなどの特権アクセスロールを異なる ID 間で分離する。 i. 特権アクセスロールの管理：アクセス権限のライフサイクル管理（プロビジョニング、使用、監視、および失効）と、アクセス権限と進化するビジネス要件および ID の役割との整合性を確保するための定期的な見直しに関する要件。	

j. 合意された特権的アクセスの役割に対する CSC の承認: CSP が機微データまたはシステムに対する特権的アクセスを付与及び変更する前に、CSC が関与する正式な承認手順及びプロセス。 k. ログの完全性の保護：監査証跡の完全性を確保するために、不正な変更や削除からログファイルを保護するための要件。緊急事態におけるログファイルへのアクセスと修正のためのブレークグラス手順を定義すべきである。 l. 一意に識別可能なユーザー：クラウド環境内の全ての ID に割り当てられる一意の識別子を確立するための要件。一意の ID は、アクセスを追跡・管理するためにクラウド環境全体で一貫して使用されるべきである。 m. 強力な認証とクレデンシャル：システム、アプリケーション、及びデータ資産にアクセスするためのセキュリティ対策の認証要件を定義し、確立すること（認証頻度及び範囲、メカニズム、セキュアなクレデンシャル、データの機密性に関連した認証など）。 n. 認可メカニズム：権限付与要件：異なるユーザーグループおよびその他の ID に付与されるアクセス権限は、それぞれの役割と責任、データの機密性、およびビジネス要件に基づいている。要件は、各ユーザーグループにアクセス権限が付与される特定のデータおよびシステム機能の概要を示すものでなければならない。 o. 承認組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与 i. IAM ポリシーと手順の変更または修正については、承認プロセスを確立すべきである。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。 p. コミュニケーション：IAM ポリシーと手順の効果的なコミュニケーションは、関連する全てのクラウド利害関係者に促進されるべきである。 q. メンテナンスと見直し：IAM ポリシーと手順は、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映するために、少なくとも年 1 回は文書化、見直し、更新する。	

Control Title	Control ID	Control Specification
強固なパスワードポリシーと手順	**IAM-02**	強固なパスワードポリシーと手順を確立、文書化、承認、周知、実装、評価、維持する。少なくとも年 1 回、ポリシーと手順を見直して更新する。
Control Ownership by Service Model		

IaaS	PaaS	SaaS
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP が所有する管理策は、CSC に提供されるクラウドサービスに関連する CSP の組織単位、基盤、および資産内の、CSP が管理するリソースに対する認証のパスワードポリシーおよび手続に関連する。	**管理策所有権の根拠：** CSC が所有する管理策は、CSP が提供するクラウドサービスに関連する CSC の組織体、基盤、資産内の CSC が管理するリソースに対する認証のためのパスワードポリシー及び手続に関連する。
実施ガイドライン： **IaaS プロバイダー：** CSP は、その内部基盤リソース（ネットワーク機器および物理ホストを含む）に対する強固なパスワードポリシーを確立し、その管理プレーンに対する CSC 認証を確立する責任を負う。	**実施ガイドライン：** **IaaS 利用者：** CSC は、CSC のユーザー認証、管理プレーン、及びクラウド基盤上に配置されたリソース（仮想ホスト、アプリケーション、データベース、ユーザーアカウント、CSC 担当者がクラウドサービスにアクセスする際に使用するエンドポイントを含む）に対して、強固なパスワードポリシーを設定する責任を負う。
PaaS プロバイダー： CSP は、CSP の内部ユーザーと、プラットフォーム基盤リソース、ミドルウェア、API に対する顧客の認証、およびクラウドサービスの管理インタフェース（管理プレーン）に対する利用者の認証について、強力なパスワードポリシーを確立する責任を負う。	**PaaS 利用者：** CSC は、CSC の内部ユーザー及び利用者がディレクトリ及び管理サービス、ユーザーアカウント、アプリケーション、並びに CSC 担当者がプラットフォーム上にデプロイされたクラウドサービス、データ及びその他のリソースにアクセスする際に使用するエンドポイントに対する認証について、強固なパスワードポリシーを確立する責任を負う。
SaaS プロバイダー： CSP は、アプリケーション環境に対する CSP 内部ユーザーの認証について、強力なパスワードポリシーを確立する責任を負う。	**SaaS 利用者：** CSC は、CSC の利用者（社内および社外）がクラウドサービス、アプリケーションデータにアクセスする際に使用する管理用アカウント、利用者アカウント、エンドポイントに対する強固なパスワードポリシーを確立する責任を負う。 CSP のポリシーが適用される。
ポリシーには、以下に関する規定が含むべきである（但し、これに限定されない）： a. 適用範囲と目的：適用範囲：従業員、請負業者、およびシステムにアクセスできる第三者を含め、ポリシーが適用されるユーザーおよびアカウントを定義する。目的には、パスワードの強度に関する要件や、個人データの再利用の制限を含める。 b. パスワードの複雑さ、長さ、履歴、有効期限：業界標準に従ったパスワードの複雑さ、長さ、履歴、有効期	

限の要件 c. ブルートフォース攻撃防止：レート制限に基づくブルートフォース攻撃防止メカニズム（例：ログイン試行失敗回数指定後のアカウントロックアウトなど） d. パスワード保護：強力なストレージとトランジット暗号化を使用したパスワード保護、定期的な更新とソルティングによるセキュアなハッシュアルゴリズムの利用、業界標準に沿った暗号化プラクティスの定期的な評価と更新の実施。 e. パスワードのローテーション:全ての ID に対するパスワードのローテーション要件の定義と実施 f. パスワードリセットパスワードを忘れた場合に、不正アクセスを防止するためのセキュアなパスワードリセットプロセス。 g. パスワード復旧：不正アクセスを防止するための検証ステップを含む、セキュアなパスワード回復プロセス h. 多要素認証（MFA）：多要素認証の使用を奨励または義務付けることで、パスワードに加えてセキュリティのレイヤーを追加する。 i. サードパーティーとの統合：サードパーティーのアプリケーションやサービスのシステムとの統合に対応し、強力なパスワード要件の遵守を保証する。 j. 承認組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与 i. IAM ポリシーと手順の変更または修正については、承認プロセスを確立すべきである。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。 k. コミュニケーション：IAM ポリシーと手順の効果的なコミュニケーションは、関連する全てのクラウド利害関係者に促進されるべきである。 l. メンテナンスとレビューパスワードポリシーと手順の文書化、見直し、更新を少なくとも年 1 回行い、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映させる。 これらの規定は、CSP 及び CSC の特定のニーズとクラウド環境の性質に基づいてカスタマイズされるべきである。	

Control Title	Control ID	Control Specification
アイデンティティ・インベントリ	**IAM-03**	システムアイデンティティとアクセスレベルの情報を管理、保存、およびレビューする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、クラウド環境において CSP の管理下にあるリソースにアクセスするシステム ID に関する管理策を所有する。このようなリソースの範囲は、以下に詳述するように、CSP が提供するクラウドサービスモデルのタイプに依存する。	**管理策所有権の根拠：** CSC は、クラウド環境と相互作用するオンプレミスリソースを含め、クラウド環境において CSC の管理下にあるリソースにアクセスするシステム ID に関する管理策を所有する。このようなリソースの範囲は、クラウドサービスモデルのタイプによって部分的に決定される。
実施ガイドライン： **IaaS プロバイダー：** CSP は、電力、冷却、およびネットワーク用の物理データセンター基盤、コンピューティング、ストレージ、およびネットワーク用のハードウェア、ハイパーバイザ、およびその他の仮想化資産など、クラウド環境内のリソースにアクセスするシステム ID のインベントリを維持し、レビューする責任を負う。文書化されるシステム ID には、各資産にアクセスできるユーザー、サービス、アプリケーション、役割、およびグループと、それらに付与されるアクセスタイプが含まれるべきである。	**実施ガイドライン：** **IaaS 利用者：** CSC は、仮想マシン、コンテナ、コンテナレジストリ OS、アプリケーション、仮想ネットワーク、ファイアウォール、ロードバランサ、アプリケーションデータ及び監視ログ、分析及び管理ツール、アプリケーションコード、鍵、デジタル証明書、シークレットボールト、ユーザーエンドポイントなど、CSC が管理するリソースにアクセスするシステム ID のインベントリを管理し、レビューする責任を負う。 文書化されるシステム ID には、各資産にアクセスできるユーザー、サービス、アプリケーション、役割、グループ、およびそれらに付与されるアクセスタイプが含まれるべきである。
PaaS プロバイダー： CSP は、電力、冷却、およびネットワーク用の物理データセンター基盤、コンピューティング、ストレージ、およびネットワーク用のハードウェア、ハイパーバイザおよびその他の仮想化リソース、仮想マシンイメージおよびインスタンス、オペレーティングシステム、ミドルウェア、データベース、および管理ツールにアクセスするシステム ID のインベントリを維持し、レビューする責任を負う。文書化されるシステム ID には、各資産にアクセスできるユーザー、サービス、アプリケーション、役割、グループ、およびそれらに付与されるアクセスの種類が含まれる。	**PaaS 利用者：** CSC は、構成ポリシー及びデータ、アプリケーションデータ及び監視ログ、分析及び管理ツール、アプリケーションコード、鍵、デジタル証明書、シークレット保管庫、ユーザーエンドポイントにアクセスできるシステム ID のインベントリを維持し、レビューする責任を負う。文書化されるシステム ID には、各資産にアクセスできるユーザー、サービス、アプリケーション、ロール、グループ、およびそれらに付与されたアクセスタイプが含まれるべきである。
SaaS プロバイダー： CS は、電源、冷却、およびネットワーク用の物理データセンター基盤、コンピューティング、ストレージ、およびネットワーク用のハードウェア、ハイパーバイザおよびその他の仮想化リソース、仮想マシンイメージおよびインスタンス、オペレーテ	**SaaS 利用者：** CSC は、アプリケーションデータ及びログ、管理者アカウント及びユーザーアカウント、鍵、デジタル証明書及びシークレット、ユーザーエンドポイントにアクセスできるシステム ID のインベントリを維持し、レビューする責任を負う。文書化され

ィングシステム、ミドルウェア、データベース、および管理ツール、アプリケーション、およびそれらのデータストレージにアクセスするシステム ID のインベントリを維持し、レビューする責任を負う。文書化されるシステム ID には、各資産にアクセスできるユーザー、サービス、アプリケーション、役割、グループ、およびそれらに付与されるアクセスタイプが含まれるべきである。	るシステム ID には、各資産にアクセスできるユーザー、サービス、アプリケーション、役割、グループ、及びそれらに付与されるアクセスの種類が含まれる。
全てのサービスモデルに適用： ID インベントリを確立し維持するための実施ガイドラインには、以下のものが含まれる（ただし、これらに限定されるものではない）： a. ID 管理システム（IDaaS）：さまざまなクラウドアプリケーションやサービスからの ID データを統合する集中型 IDaaS 基盤を実装する必要がある。この基盤は、全ての ID とそのアクセス権限（最低特権、SoD、ACL など）を可視化する必要がある。 b. ID の分類：ID は、その役割、目的、機密性に基づき、アクセスするリソースと関連付けて分類および分類されるべきである（すなわち、適切なアクセス権限を割り当て、重要な ID に対してより厳格な管理を実施する）。 c. ID の発見とインベントリ：自動化ツールを活用してクラウド環境を継続的にスキャンし、既存の ID を全て特定する。 d. 脅威インテリジェンスの統合：脅威インテリジェンスソースを活用し、潜在的な ID ベースの脅威を特定して優先順位を付け、新たなリスクに積極的に対処する。 e. インベントリへのアクセス：ID 情報はセキュアな場所に保管し、アクセスは許可された担当者に制限すべきである。 f. システム ID の所有：説明責任を維持し、将来の管理を容易にし、管理されていないアカウントに関連するセキュリティリスクを軽減するために、各システムおよびサービスアカウントに指定された所有者を割り当てるべきである。 g. 在庫のレビューと更新： i. インベントリは、正確性と完全性を確保し、ID の現状とアクセスレベルを反映し、矛盾や異常を特定し、必要に応じてアクセスを確実に取り消しまたは変更するために、最新のものでなければならない。 ii. レビューは、定期的に、または ID およびそのアクセスレベルに変更があったときに、CSP のリスク評価およびその他のコンプライアンス要件に従って実施されるものとする。	

Control Title	Control ID	Control Specification
職務の分離	**IAM-04**	情報システムへのアクセスを実施する際には、職務の分離の原則を採用する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は以下を含む、CSP が提供し維持するクラウド環境へのアクセスを持つエンティティに関する管理策を所有する。 内部ユーザー、外部ユーザー（ベンダーや顧客）、アプリケーション、サービス。	**管理策所有権の根拠：** CSC は以下を含む、CSC が提供し維持するクラウド環境へのアクセス権を有するエンティティに関する管理策を所有する。 従業員、外部ユーザー（ベンダーや顧客）、アプリケーション、サービス。
実施ガイドライン： CSP は、クラウド環境を保護し、不正アクセス、不正行為、エラーを防止するために、職務分掌（SoD）を実施すべきである。CSP と CSC の双方は、SoD の原則を効果的に実施する責任を共有する。	
実施ガイドライン： **IaaS プロバイダー：** CSP は、クラウド基盤リソースのプロビジョニングとプロビジョニング解除に責任を負うクラウド管理者、セキュリティポリシーと手順の策定と実施に責任を負うセキュリティ管理者、リソースのパフォーマンスと可用性の監視、トラブルシューティング、運用上の問題の解決に責任を負うシステムおよび運用サポート要員を含め、相反する機能を持つユーザーにシステムアクセスを割り当てる際に SoD 原則が適用されるようにする責任を負う。	**実施ガイドライン：** **IaaS 利用者：** CSC は、クラウドサービスのリソース（VM、仮想ネットワーク、ロードバランサ、データベース、アプリケーションなど）のプロビジョニングを担当するクラウドサービス管理者、管理プレーン、VM、仮想ネットワーク、ロードバランサ、データベース、オペレーティングシステム、アプリケーションのセキュリティ制御の設計と実装を担当するセキュリティ管理者、システムの可用性とパフォーマンスの監視、トラブルシューティングと問題解決を担当するシステムおよび運用サポート担当者、クラウドサービスのその他のユーザーを含む、互換性のない機能のためにシステムアクセスをその環境に割り当てる際に、SoD 原則が適用されることを保証する責任がある。
PaaS プロバイダー： CSP は、クラウド基盤およびプラットフォームリソースのプロビジョニングとプロビジョニング解除に責任を負うクラウド管理者、セキュリティポリシーと手順の策定と実装に責任を負う	**PaaS 利用者：** CSC は、相反する機能のシステムアクセスを割り当てる際に、SoD 原則が適用されることを保証する責任を負う。これにはアプリケーションおよびデータベースの構築と実装を担当する

セキュリティ管理者、リソースのパフォーマンスと可用性の監視、トラブルシューティング、および運用上の問題の解決に責任を負うシステムおよび運用サポートチームなど、相反する機能を持つユーザーにシステムアクセスを割り当てる際に、SoD 原則が適用されるようにする責任を負う。	開発者、アプリケーションおよびデータベースのセキュリティ管理の設計と実装に責任を負うセキュリティ管理者、システムの可用性と性能の監視、トラブルシューティングと問題解決に責任を負うシステムおよび運用サポート担当者、およびクラウドサービスのその他のユーザーが含まれる。
SaaS プロバイダー： CSP は、クラウド基盤およびプラットフォームリソースのプロビジョニングとプロビジョニング解除を担当するクラウド管理者、セキュリティポリシーと手順の策定と実装を担当するセキュリティ管理者、クラウド環境へのアプリケーションの開発とデプロイを担当する開発者、リソースとアプリケーションのパフォーマンスと可用性の監視、トラブルシューティング、および運用上の問題の解決を担当するシステムサポートチーム、および運用サポートチームなど、相反する機能を持つユーザーにシステムアクセスを割り当てる際に SoD 原則が適用されるようにする責任を負う。	**SaaS 利用者：** CSC は、相反する機能のシステムアクセスを割り当てる際に、SoD 原則が適用されることを保証する責任を負う。これには、使用するアプリケーションの設定やカスタマイズに責任を負う開発者、アプリケーションやユーザーアカウントのセキュリティ設定の実装に責任を負うセキュリティ管理者、ユーザーアカウントのプロビジョニング、管理、デプロビジョニングに責任を負うユーザーアカウント管理者、システムの可用性とパフォーマンスの監視、トラブルシューティング、問題の解決に責任を負うサポートチーム、クラウドサービスのその他のユーザーが含まれる。
全てのサービスモデルに適用： CSP が SoD を効果的に採用するための実装のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. SoD の役割管理とアクセス： i. ロールの権限を管理・維持するために、一元化されたロール管理システムを導入すべきである。 ii. SoD を強化するために、責任の重複する役割は最小限にすべきである。 iii. ロールは、クラウド環境内のさまざまな機能に対して特定の権限を持つように作成されるべきである。このようにすることで、不正なアクションを可能にする可能性のある過剰な権限を単一 ID に割り当てることを避けることができる（例えば、実装、承認、実行などの重要な機能は、異なる ID 間で分離されるべきである）。 iv. クラウド環境の特定の部分へのロールとそのアクセスを制限するために、アクセスレベルを分離すべきである。 v. トランザクションの承認や機密データの変更など、高リスクまたは重要な活動については、マルチレベルの承認プロセスを導入すべきである（すなわち、異なる役割の複数の個人がアクションを承認する）。 b. 役割の割り当てとプロビジョニング：職務上の役割と必要なアクセスレベルに基づいてユーザーの役割を割り当て、管理するためのツールを利用すべきである（可能であれば自動化）。 c. 役割の見直し：職務が競合するリスクを最小化し、現在のビジネスニーズと合致し、適切な職務分掌を維持するために、役割の定義とその権限について定期的なレビューを実施すべきである。	**全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

d. 役割変更の監視：ID の役割と権限の変更を追跡するために、監視とロギングの仕組みを実装する。 e. ロールの例外管理：一人のユーザーに複数のロールを付与しなければならない場合の例外管理プロセスを確立すべきである。これには、上級管理職の承認と正当な理由の文書化が必要である。 f. 違反の報告：SoD 違反の疑いまたは確認された場合の報告手順を定めるべきである。 g. SoD 管理策のモニタリング：SoD の管理策は、その有効性を確保し、ギャップや脆弱性に対処するために、定期的に評価されなければならない。	

Control Title	Control ID	Control Specification
最小権限	**IAM-05**	情報システムへのアクセスを実装するときは、最小権限の原則を採用する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、CSP の内部ユーザー、外部ユーザー（ベンダーおよび顧客）、アプリケーション、およびサービスを含め、CSP がクラウド環境へのアクセスを提供し維持するエンティティに関連する管理策を所有する。	**管理策所有権の根拠：** CSC は、要員、外部ユーザー（ベンダー及び顧客）、アプリケーション及びサービスを含む、CSC が提供し維持するクラウド環境へのアクセス主体に関する管理策を所有する。
実施ガイドライン： **IaaS プロバイダー：** CSP は、ユーザーへのシステムアクセスの割り当て時に最小特権の原則が確実に適用されるようにする責任を負う。これには、クラウドインフラリソースのプロビジョニングとプロビジョニング解除に責任を負うクラウド管理者、以下の責任を負うセキュリティ管理者が含まれる。 リソースのパフォーマンスと可用性を監視し、トラブルシューティングを行い、運用上の問題を解決するシステムオペレータ。	**実施ガイドライン：** **IaaS 利用者：** CSC は、クラウドサービスのリソース（VM、仮想ネットワーク、ロードバランサ、データベース、アプリケーションなど）のプロビジョニングを担当するクラウドサービス管理者を含め、システムへのアクセスをユーザーに割り当てる際に最小特権原則が適用されることを保証する責任を負う。 管理プレーン、VM、仮想ネットワーク、ロードバランサ、データベース、オペレーティングシステム、アプリケーションのセキュリティ管理の設計と実装を担当するセキュリティ管理者、システムの可用性とパフォーマンスの監視、トラブルシュ

	ーティング、問題の解決を担当するシステムおよび運用サポート担当者、クラウドサービスのその他のユーザー。
PaaS プロバイダー： CSP は、ユーザーへのシステムアクセスの割り当て時に最小特権の原則が適用されるようにする責任を負う。これには、クラウドインフラストラクチャおよびプラットフォームリソースのプロビジョニングとプロビジョニング解除に責任を負うクラウド管理者、セキュリティポリシーと手順の策定と実装に責任を負うセキュリティ管理者、リソースのパフォーマンスと可用性の監視、運用上の問題のトラブルシューティングと解決に責任を負うシステムおよび運用サポートチームが含まれる。	**PaaS 利用者：** CSC は、アプリケーションやデータベースの構築・実装を担当する開発者、アプリケーションやデータベースのセキュリティ管理の設計・実装を担当するセキュリティ管理者、システムの可用性やパフォーマンスの監視、トラブルシューティング、問題解決を担当するシステム・運用サポート担当者、その他クラウドサービスの利用者を含む利用者にシステムアクセスを割り当てる際に、最小特権の原則が適用されることを保証する責任を負う。
SaaS プロバイダー： CSP は、ユーザーへのシステムアクセスの割り当て時に最小特権の原則が確実に適用されるようにする責任を負う。これには、クラウドインフラストラクチャとプラットフォームリソースのプロビジョニングとプロビジョニング解除に責任を負うクラウド管理者、セキュリティポリシーと手順の策定と実装に責任を負うセキュリティ管理者、クラウド環境へのアプリケーションの開発とデプロイに責任を負う開発者、リソースとアプリケーションのパフォーマンスと可用性の監視、トラブルシューティング、および運用上の問題の解決に責任を負うシステムサポートチームと運用サポートチームが含まれる。	**SaaS 利用者：** CSC は、システムへのアクセスをユーザーに割り当てる際に、最小特権の原則が適用されるようにする責任がある。これには、使用するアプリケーションの設定やカスタマイズを担当する開発者、アプリケーションやユーザーアカウントのセキュリティ設定の実装を担当するセキュリティ管理者、ユーザーアカウントのプロビジョニング、管理、デプロビジョニングを担当するユーザーアカウント管理者、システムの可用性とパフォーマンスの監視、トラブルシューティング、問題の解決を行うサポートチーム、クラウドサービスのその他のユーザーが含まれる。
全てのサービスモデルに適用： CSP が最小特権の原則（PoLP）を効果的に採用するための実装のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. LP インフラ：クラウドインフラストラクチャは、PoLP を念頭に置いて設計・構成されるべきである。 b. LP 役割と権限：職務を遂行するために各役割がアクセスする必要のある具体的なアクション、データ、リソースは、各役割/アイデンティティに基づく適切なアクセスレベルを決定するために特定されるべきである（アクセス制御の許可を実施するために RBAC が利用されるべきである）。 c. 管理アカウントの LP アクセス： i. 管理者アカウント（root や administrator アカウントなど）は、特定のタスクや環境に限定し、絶対に必要なときのみ使用されるよう、最も制限されたアクセス権を持つべきである。 ii. 全ての管理者アカウントおよびその他のリスクの高いアクセスポイントに対して MFA を実施する必要がある。 d. 機密データへのアクセス制限：機密データへのアクセスは、職務遂行に必要な最小限の ID に制限されるべきである。 e. 未使用権限の取り消し：PoLP を維持し、攻撃対象ドメイ	**全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

ンを減らすために、未使用または過剰な権限を取り消すために、ID のアクセス権限を定期的にプロアクティブにレビューする必要がある。 f. LP アクセスレビュー i. アクセス権限は、定期的に見直し、評価し、現在の職務／機能要件に合致していることを確認し、不必要または過剰なアクセスを特定し、それに応じて調整する。 ii. PoLP プラクティスの効果を監視・評価し、潜在的なギャップや設定ミスを特定するために自動化ツールを導入すべきである。	

Control Title	Control ID	Control Specification
ユーザーアクセスのプロビジョニング	**IAM-06**	データと資産へのアクセスの変更を承認、記録、および伝達するためのユーザーアクセスプロビジョニングのプロセスを定義および実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策に対する CSP の責任は、クラウドサービス環境において CSP が管理および管理するデータおよび資産へのユーザーアクセスのプロビジョニングに関連する。	**管理策所有権の根拠：** この管理策に対する CSC の責任は、クラウドサービス環境において CSC が管理および管理するデータおよび資産へのユーザーアクセスのプロビジョニングに関連する。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、データおよび資産へのユーザーおよびシステムアクセスをセキュアかつ統制するために、アクセスプロビジョニング・プロセスを確実に導入すべきである。このプロセスを効果的に実施するには、権限付与、記録保持、およびアクセス変更の連絡を管理するベストプラクティスを順守することが必要である。 CSP がユーザーアクセスプロビジョニングプロセスを効果的に実装するための実装のベストプラクティスには、以下のものが含まれる（ただし、これらに限定されない）：	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

a. アクセスプロビジョニングのための IDaaS：IDaaS システム（IAM-03 参照）を活用して、全てのクラウドサービスとアプリケーションの ID 管理とアクセスプロビジョニングを統合する。
b. 人事システムとの同期：IDaaS システムは人事システムと統合され、従業員の入社や役割の変更に基づいてユーザーアカウントを自動的にプロビジョニングする必要がある。
c. プロビジョニングワークフローの自動化：プロビジョニングプロセスは、ワークフロー自動化ツールを使用して自動化し、エラーを減らし、タイムリーで一貫性のある変更を保証する必要がある。
d. アクセスプロビジョニング管理のためのシングルポイントオブコンタクト（SPOC）：
    i. プロビジョニングアクションが関連するロール間で効果的に伝達されるように、ロールの階レイヤーと委譲構造を定義する必要がある。
    ii. プロビジョニングアクセスリクエストの受信と管理のために、一元化された SPOC を指定すべきである。
e. アクセス要請および承認プロセス：新たなアクセス権の付与または既存のアクセス権の変更のための正式なアクセス要求および承認プロセスを確立し、アクセス権の変更がビジネスニーズおよびリスク評価に基づいて上級管理者によりレビューされ、承認されるようにする。
f. アクセスプロビジョニングイベントのログ：
    i. アカウントの作成、変更、削除、アクセス権限、失敗した試行、リソースの利用など、ID に関連する全てのイベントを監視し、記録する。
    ii. 調査およびコンプライアンス監査を容易にするため、全てのアクセスイベントの正確かつ最新の記録を作成し、指定された保存期間維持すべきである。
g. アクセスプロビジョニングの変更通知：
    i. アカウントの作成や更新などのアクセスに関する変更は、電子メールやアプリ内通知などのセキュアなチャネルを通じてユーザーに通知する必要がある。
    ii. 全てのアクセス変更とプロビジョニングのアクションについて、担当のセキュリティマネジャーに定期的に報告し、再鑑してもらう。
h. アクセスプロビジョニング監査：ID アクセスのプロビジョニングプロセスの有効性を評価し、潜在的な脆弱性または設定ミスを特定するために、セキュリティ監査を定期的に実施する。

Control Title	Control ID	Control Specification
ユーザーアクセスの変更と取り消し	**IAM-07**	アイデンティティとアクセスの管理ポリシーを効果的に採用して伝達するために、異動者／退職者のアクセスまたはシステムアイデンティティの変更をタイムリーにプロビジョニング解除または変更する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC はともに、それぞれの環境における定期的な見直し、移管、または終了に起因する要員（従業員および請負業者）のアクセス権限削除に関連するプロセスおよび手続を統制する独立した責任を有するため、本統制の実施責任は「(依存しない形で）共有」となる。CSP は、CSP 内部を含め、CSP がクラウド環境へのアクセスを提供し維持するエンティティに関連する管理策を所有する。 ユーザー、外部ユーザー（ベンダーや顧客）、アプリケーション、サービス。	**管理策所有権の根拠：** CSP と CSC はともに、それぞれの環境における定期的な見直し、移管、または終了に起因する要員（従業員および請負業者）のアクセス権限削除に関連するプロセスおよび手続を統制する独立した責任を有するため、本統制の実施責任は「(依存しない形で）共有」とする。CSC は、CSP 内部を含む、CSC が提供し維持するクラウド環境へのアクセスを有するエンティティに関する管理策を所有する。 ユーザー、外部ユーザー（ベンダーや顧客）、アプリケーション、サービス。
実施ガイドライン： **全てのサービスモデルに適用：** ユーザーに以前付与されたアクセスが不要になったと判断されると、CSP はユーザーのアクセスをプロビジョニング解除する責任を負う。管理の範囲には、アクセス管理プロセスによって管理される全てのアクセスおよび権限が含まれる。 ユーザーアクセスをタイムリーにデプロビジョニングまたは変更するための実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. IDaaS によるアクセスデプロビジョニング：IDaaS システム（IAM-03 参照）を活用して、全てのクラウドサービスとアプリケーションの ID 管理とアクセスデプロビジョニングを統合する。 i. アカウントの終了または再割り当て時にアクセス権を取り消すための IAM プロセスの一環として、デプロビジョニングツールまたはスクリプトを利用する（可能であれば自動化する）。 ii. アクセス権は、終了日以降、関連する全ての ID 内で失効されるべきである。	**実施ガイドライン：** **全てのサービスモデルに適用：** ユーザーに付与されたアクセスが不要になったと判断された場合、CSC はユーザーのアクセスをプロビジョニング解除する責任を負う。管理範囲には、「アクセス管理プロセス」によって管理される全てのアクセス及び権限が含まれる。 CSP の「実施ガイドライン」が適用される。

b. 人事システムとの同期：IDaaS システムは、従業員の解雇や役割の変更に基づいて自動的にユーザーアカウントのプロビジョニングを解除するために、人事システムと統合する必要がある。
c. プロビジョニング解除ワークフローの自動化：プロビジョニング解除プロセスは、エラーを減らし、タイムリーで一貫した変更を保証するために、ワークフロー自動化ツールを使用して自動化されるべきである。
d. アクセスプロビジョニング解除管理のための単一窓口（SPOC）：
    i. プロビジョニング解除のアクションが関連するロールに効果的に伝播するように、ロールの階レイヤーと委譲構造を定義する必要がある。
    ii. プロビジョニング解除アクセス要求の受領と管理のために、一元化された SPOC の責任者が指定されるべきである。
e. アクセスプロビジョニング解除イベントログ：
    i. アカウントの変更と削除、アクセス権限、失敗した試行、リソースの利用など、ID に関連する全てのイベントを監視し、記録する。
    ii. 調査およびコンプライアンス監査を容易にするため、全てのアクセスイベントの正確かつ最新の記録を作成し、指定された保存期間維持すべきである。
f. アクセスデプロビジョニングの変更通知：
    i. 定期的なアクセス再認証、譲渡、アカウント終了などによる）アクセス権限のデプロビジョニングや変更などのアクセス変更は、電子メールやアプリ内通知などのセキュアなチャネルを通じてユーザーに通知されるべきである。
    ii. 全てのアクセス変更とデプロビジョニングのアクションを定期的に報告し、担当のセキュリティマネジャーに再鑑してもらう。
g. 失効および一時停止の仕組み：アクセス権を失効または一時停止するためのプロセスを導入すべきである。セキュリティ違反やコンプライアンス違反に対処するため、必要に応じて一時的に対応する。
h. 非アクティブな ID のプロビジョニング解除：非アクティブなアカウントを検出し、レビューのためにフラグを立て、必要に応じて未使用または非アクティブの ID をプロビジョニング解除するプロセスを導入する（可能であれば自動化する）。
i. プロビジョニング解除の危機管理計画への組み込み：インシデントや緊急事態が発生した場合、タイムリーかつ効果的にアクセス権を剥奪できるよう、プロビジョニング解除手順を危機管理計画に組み込むべきである。
j. アクセスプロビジョニング解除監査：ユーザーアクセスのプロビジョニング解除プロセスの有効性を評価し、潜在的な脆弱性や設定ミスを特定するために、セキュリテ

ィ監査を定期的に実施すべきである。	

Control Title	Control ID	Control Specification
ユーザーアクセスのレビュー	**IAM-08**	組織のリスク許容度に見合った頻度で、最小権限と職務の分離のためのユーザーアクセスをレビューして再検証する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP 及び CSC は、それぞれの環境における要員（従業員及び請負業者）の監督者による定期的なアクセス見直しに関連するプロセス及び手続の管理策について個別に責任を有するため、本管理策の実施責任は「(依存しない形で）共有」である。CSP は、内部ユーザー、外部ユーザー（ベンダーおよび顧客)、アプリケーション、およびサービスを含む、CSP が提供し維持するクラウド環境へのアクセス主体に関連する管理策を所有する。	**管理策所有権の根拠：** CSP と CSC は、それぞれの環境における要員（従業員及び請負業者）の監督者による定期的なアクセス見直しに関連するプロセス及び手続の統制ついて個別に責任を有するため、本管理策の実施責任は「(依存しない形で）共有」である。CSC は、社内ユーザー、外部ユーザー（ベンダー及び顧客)、アプリケーション及びサービスを含む、CSC が提供し維持するクラウド環境へのアクセス主体に関する管理策を所有する。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、組織にもたらすリスクによってアクセスタイプを分類し、定期的（リスクレベルに基づいて決定される頻度）に、または人員の解雇や異動など特定のイベントが発生したときに、ユーザーのアクセスのレビューを促進する責任を負う。 最小特権と職務分掌のために、ユーザーアクセスを効果的に見直し検証するために、CSP は、導入のベストプラクティスを包含する包括的なアプローチと、そのようなレビューのリスクベースの頻度を導入すべきである： a. アクセス管理とレビュー i. アクセス管理プロセスと記録は、ID アクセスのレビューを容易にし、異なるクラウドシステム間での不整合のリスクを減らすために、一元化されるべきである。 ii. 時代遅れのアクセス、過剰なアクセス、不必要なアクセスを是正するためにアクセスレビューを実施	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、リスクに応じてアクセスタイプを分類し、定期的（リスクレベルに基づいて決定される頻度）に、または人員の解雇や異動など特定の事象が発生した場合に、ユーザーのアクセスの見直しを促進する責任を負う。管理の範囲には、アクセス管理プロセスによって管理される全てのアクセスおよび権限が含まれる。 CSP の「実施ガイドライン」が適用される。

し、アクセス権が役割と責任、最小限の特権、SoDの原則に準拠していることを確認する。 iii. アクセスレビューは、可能であれば自動化ツールやスクリプトを用いて自動化すべきである。 iv. 管理者アカウントや機密データへのアクセスなど、リスクの高いアクセス構成のレビューは、優先的にスケジューリングされるべきである。 v. アクセスレビューの結果、各 ID が職責を果たすために引き続き必要とする PoLP、SoD、またはその他の資格が再承認されるか、またはユーザーの役割の現在および将来の職責に基づいて、相反する資格の組み合わせが拒否されなければならない。 b. アクセスレビューの頻度：ID アクセスレビューの頻度は、組織のリスク許容度、および保護されるデータおよびシステムの機微性に見合ったものでなければならない。リスクの高い環境では、レビューを毎日または週単位で実施し、機密性の低いシステムは月または四半期ごとにレビューする。 c. アクセス審査の文書化：アクセスレビューの結果は文書化し、監査目的のために記録を保持すべきである。 d. 監査およびロギング：ID のアクセス活動を追跡し、誰が、どのリソースに、いつアクセスしたかの記録を作成し、調査を容易にし、疑わしい活動を特定するために、監査およびロギング機能を実装すべきである。 e. 継続的なモニタリングと評価：不正または異常な活動をスキャンし、アクセスパターンの変化、特権の昇格、その他の潜在的なセキュリティ侵害を検出するために、継続的な監視ソリューションを導入すべきである。 f. アクセス認証：アクセス認証プロセスを導入し、ユーザーが定期的に自分のアクセス権限を正当化し、現在の役割に必要かつ適切なアクセスであることを確認する。	

Control Title	Control ID	Control Specification
特権的なアクセスロールの分離	**IAM-09**	データへの管理者アクセス、暗号化および鍵管理機能、ロギング機能が明確かつ分離されるように、特権的なアクセスロールを分離するためのプロセス、手順、および技術的手段を定義、実装、および評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： データまたは暗号化鍵への管理アクセスを持つ特権ロールと、データまたは鍵へのアクセスを記録するログ機能（ロギング構成やストレージ内のログファイルなど）へのアクセスを持つロールの間の SoD を維持するため、CSP と CSC は共に責任を負うが、それぞれのプロセスと手順も独立して統制するため、本管理策の実施責任は「(依存しない形で）共有」である。CSP は、CSP 内部ユーザー、外部ユーザー（ベンダーおよび顧客)、アプリケーション、およびサービスなど、 CSP が提供し維持するクラウド環境へのアクセスを持つエンティティに関連する管理策を所有する。	**管理策所有権の根拠：** データまたは暗号化鍵への管理アクセスを有する特権的な役割と、データまたは鍵へのアクセスを記録するロギング機能（ロギング設定やストレージ内のログファイルなど）へのアクセスを有する役割との間の SoD を維持するためのプロセスおよび手順は、CSP と CSC の両方が責任を負うとともに、それぞれ独立して統制するため、本管理策の実施責任は「(依存しない形で）共有」である。CSC は、CSC 内部ユーザー、外部ユーザー（ベンダー及び顧客)、アプリケーション及びサービスを含む､CSC が提供し維持するクラウド環境へのアクセス権を有するエンティティに関連する管理策を所有する。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、データへの管理アクセスを持つ特権ロール、データの暗号化に使用される鍵、およびデータまたは鍵へのアクセスを記録するロギング機能間の SoD を確保する責任を負う。CSP はまた、本番環境と非本番環境間のアカウントとアクセス権限の分離を維持し､非本番アカウントにのみア クセスできる要員が非本番アカウントを使用して本番環境にアクセスできないようにする責任も負う。 特権アクセスロールの分離のための実装のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 特権アクセスロールの分離： i. 職務の分離を確立し、不正使用のリスクを低減するために､各特権 ID の役割と責任を定義し、単一の ID が過剰な特権を保持しないようにする。 ii. 組み合わされた場合、競合するアクセスの組み合わせが生じる特権ロールは、PAM システムで明示的に識別し、ラベル付けすべきである。 iii. 非本番環境へのアクセスを許可する役割と権限 非本番環境は、本番環境へのアクセスを許可するロールやパーミッションから分離すべきである。 b. 異なる特権ドメインへのアクセス分離： i. 特権機能および管理機能へのアクセスは、管理アクセス､暗号化/鍵管理､設定変更､ロギングなど､個別のドメインに分割して､単一の ID がこれら全てのドメインへのアクセスを同時に危険にさらすことを防ぐ必要がある。 ii. 特権的な活動は、可能であれば、別の環境または仮想マシン内に隔離すべきである。 c. 機微データおよびシステムへのアクセス制限： i. 特権ユーザーが職務に直接関係のない機密システ	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、データへの管理アクセスを持つ特権的役割、データの暗号化に使用される鍵、及びデータや鍵へのアクセスを記録するロギング機能の間の SoD を保証する責任を負う。また、CSC は､本番環境と非本番環境の間でアカウントとアクセス許可の分離を維持し、非本番アカウントのみにアクセスできる要員が非本番アカウントを使用して本番環境にアクセスできないようにする責任も負う。 CSP の「実施ガイドライン」が適用される。

ムやデータにアクセスできないように、アクセス制御を実施する(特権アカウントの PoLP を実施する)。 ii. SSH 接続による特権アクセスの認証には、強力な鍵の暗号化とローテーションが可能な SSH 鍵を使用する。 d. 特権アクセス分離のレビュー i. 特権および管理機能を持つアクセスロールは、適切な分離を確保するため、CSP の IAM ポリシーで指定された合理的な頻度で定期的に見直され、更新されるものとする。 ii. 自動化されたプロセスを導入して、アイデンティティの分離された特権アクセス許可を定期的にレビューする。 e. 継続的な監視と評価:特権アクセスロールの分離およびセキュリティ対策(データ、暗号鍵、システム構成に対する)の有効性を監視し、ログに記録し、定期的に評価すること。	

Control Title	Control ID	Control Specification
特権的なアクセスロールの管理	**IAM-10**	特権的なアクセスロールと権限が限られた期間のみ付与されることを保証するためのアクセスプロセスを定義および実装し、分離された特権アクセスが極大化するのを防ぐための手順を実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠: CSP と CSC はともに、それぞれの環境における特権アクセスを管理するためのそれぞれのプロセスおよび手続を統制する責任を負うため、この管理策は「依存しない形で共有」である。CSP は、CSP 内部ユーザー、外部ユーザー(ベンダーおよび顧客)、アプリケーション、およびサービスを含む、 CSP が提供し維持するクラウド環境へのアクセスを持つエンティティに関連する管理策を所有する。	**管理策所有権の根拠:** CSP と CSC はともに、それぞれの環境における特権アクセスを管理するためのプロセスおよび手順を統制する責任を負うため、この管理体制は「(依存しない形で)共有」である。CSC は、CSC 内部ユーザー、外部ユーザー(ベンダーおよび顧客)、アプリケーション、およびサービスを含む、 CSP が提供し維持するクラウド環境へのアクセス権を有するエンティティに関して、管理策を所有する。

実施ガイドライン：

全てのサービスモデルに適用：

CSP は、特権アクセスおよび権限が一定の期間にわたって適切に承認され、ユーザーにその期間のみ特権アクセスが提供されるようにする責任を負う。
承認された期間が経過したら、そのユーザーのアクセス権は削除されなければならない。

アクセス範囲には、クラウド基盤リソースのプロビジョニングとプロビジョニング解除を担当するクラウド管理者、セキュリティポリシーと手順の策定と実装を担当するセキュリティ管理者、およびリソースのパフォーマンスと可用性の監視、トラブルシューティング、運用上の問題の解決を担当するシステムオペレータの権限が含まれる。

実施上のベストプラクティスには以下が含まれる（ただし、これらに限定されるものではない）：

a. 特権アクセス管理（PAM）：
   i. 特権アクセスのライフサイクル管理プロセス（プロビジョニング、使用、監視、失効を含む）を確立し、定期的に見直して、アクセス権限を更新し、ビジネス要件やユーザーの役割の変化に対応させる。
   ii. 特権とみなされるアクセスおよび権利は、定義され、全ての資産所有者を含む全ての関係者に通知されるべきである。
   iii. 特権アクセスを要求できるロールは定義され、文書化されるべきである。
   iv. 高リスクのアクセスに対する権限のエスカレーションを含め、さまざまなタイプの特権ロールのアクセスレベルを定義すべきである。
   v. PAM ソリューションは、特権アカウントへのアクセスや資格情報の管理・監視、特権資格情報のセキュアな保管とローテーション、アクセス活動の監査とログ記録、特権セッションの MFA の実施に活用されるべきである。
   vi. 重要なアカウントと機密データのセキュリティを確保するため、特権アクセスに対する全ての変更を、セキュリティ管理者にリアルタイムで通知し、レビューさせる。
b. 特権アクセス要求：
   i. ユーザーが特権アカウントにアクセスすることを正当化し、承認を得ることを要求する、正式な特権アクセス要求プロセスを確立すべきである。
   ii. 特権アクセスは、正当性の確認と複数レベルの承認の後にのみ付与されるべきである。
c. 特権アクセス制限：特定のリソースやシステムへの特権的なアクセスを制限し、ユーザーが許可された範囲を超えてアクセスできないようにする。
d. 特権失効の自動化：雇用の終了、役割の変更、またはその

実施ガイドライン：

全てのサービスモデルに適用：

CSP の「実施ガイドライン」が適用される。

他の関連するイベントが発生した場合に、特権アクセスを取り消すための自動化されたプロセスを実装する必要がある。 e. 特権アクセスセッションの期間： i. セッション管理機能を実装し、特権アクセスセッションの継続時間を制限し、非アクティブ期間終了後にセッションをタイムアウトさせる。 ii. ジャストインタイムアクセス（JIT）を活用し、不正アクセスの機会を最小化するため、永続的なアクセスを許可するのではなく、必要な特定の期間のみアクセスを許可する。 f. 特権アクセスのパスワード管理：パスワードの定期的な変更や複雑性の要求など、特権アカウントの強力なパスワード管理を実施する。 g. アクセス例外プロセス： i. 特権アカウントについて、例外的な状況においてのみ、一時的または例外的なアクセスを許可するプロセスを確立すべきである（CCC-08 を参照）。 ii. 上級管理職の承認を取得し、アクセス要求の正当性を文書化すべきである。 h. クレデンシャルの保管庫およびローテーション：特権アクセス・クレデンシャルの保管および管理には、セキュアなクレデンシャル保管庫を使用する。クレデンシャルは、不正アクセスのリスクを最小化するために定期的にローテーションされるべきである。 i. 特権アクセス昇格の防止：特権の昇格を防止するメカニズムを導入し、ユーザーが割り当てられた特権以上にアクセス権を昇格できないようにする（例えば、RBAC や MAC アクセス制御メカニズムを使用する）。 j. 特権アクセスロールのレビュー：特権アクセスおよび特権権限を持つロールは、ID およびアクセス管理ポリシーで指定された妥当な頻度で実行される定期的なアクセスレビュー活動に含めるべきである。 k. 継続的な監視と記録：特権アクセスの役割の有効性を監視し、ログに記録し、定期的に評価する。PAM ソリューション、オペレーティングシステム、および関連ソフトウェアは、潜在的な脆弱性に対処するために更新されるべきである。	

Control Title	Control ID	Control Specification
合意された特権アクセスロールに対する CSC の承認	**IAM-11**	合意された高リスク（組織のリスクアセスメントによって定義された）特権アクセスロールに対するアクセス権を付与する場合、可能であれば、利用者が参加するためのプロセスと手順を定義、実装、および評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC 共に、高リスクデータの決定と CSP ユーザーへの特権アクセス付与を担当するため、この管理策の実施責任は「依存する形で共有」である。CSP は、CSP 内部ユーザー、外部ユーザー（ベンダーおよび顧客）、アプリケーション、サービスなど CSP が提供し維持するクラウド環境へのアクセスを持つエンティティに関連する管理策を所有する。	**管理策所有権の根拠：** CSP と CSC 共に、高リスクデータの決定と CSP ユーザーへの特権アクセス付与を担当するため、この管理策の実施責任は「依存する形で共有」である。CSP は、CSP 内部ユーザー、外部ユーザー（ベンダーおよび顧客）、アプリケーション、サービスなど CSP が提供し維持するクラウド環境へのアクセスを持つエンティティに関連する管理策を所有する。CSC は、自分たちの環境に対する特権的なアクセスと見なされるものの決定に参加する責任、および正当な理由がある場合に CSP ユーザーに対するそのような特権的なアクセスの要求を承認する管理策を所有する。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、CSP ユーザーによる CSC のデータへのアクセスを提供する特権的な役割を特定する責任を負う。また、CSP は、CSP ユーザーが特権的な役割を一時的または継続的に提供される前に、CSC の権限を有する者から承認を得るプロセスが存在することを保証する責任を負う（CSP ユーザーの特権的なアクセスは、その権限付きアクセス要求システムにおいて適切に承認される）。CSP ユーザーの特権的な活動は、ログに記録され、報告され、疑わしい活動がないか監視されるものとする。 実施上のベストプラクティスには以下が含まれる（ただし、これらに限定されるものではない）： a. スコープと特権的役割の定義： i. 高リスクデータ（個人データ、財務データ、知的財産、医療記録など）の範囲と、CSP アクセスに CSC の承認が必要な特権的役割の種類を定義する。 ii. CSC は、スケジュール、通知、文書化を含む承認プロセスを確立すべきである。これらの要件は、CSC の組織的なリスクアセスメント及びデータ分類のポリシーと整合させるべきである。 b. CSP-CSC 承認ワークフロー： i. リスクの高いデータを含む CSP 特権アクセス要求については、関連する CSC 担当者の明示的な承認を必要とする。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、CSC が指定する要員による承認の前に、CSP からの特権的アクセス要求が正当な理由と承認について適切に審査されることを保証する責任を負う。 a. 契約上の合意： i. CSC と CSP は、高リスクデータへの特権的アクセスを許可するための具体的な条件を概説する正式な契約（SLA）を締結すべきである。 ii. SLA は、高リスクデータへのアクセスに関する CSP と CSC 双方の役割、責任、および期待事項を概説するものとする。これらの SLA には、以下の条項を含める（ただし、これらに限定されない） iii. CSC の高リスクデータへの CSP 特権アクセスの要求、承認、および取り消しのプロセス。 iv. タイムスタンプ、ユーザーID、アクティビティ詳細を含む、高リスクデータへの全アクセスの監査とロギングの要件 v. 情報漏えいの範囲、影響を受けるデータ、影響を軽減するために取られた措置を含む、情報漏えいの迅速な通知に関する要件 vi. いつでもアクセスを撤回する権利を含む、CSC のデータに対する所有および管理権 vii. 情報漏洩やシステム障害が発生した場合のデー

ii. 承認には複数の権限レベル（例えば、指定された CSC の代表者、法務担当者またはコンプライアンス担当者、上級管理職の承認）が関与し、特権的アクセスを要求される許容される理由や正当性を含め、アクセス決定の説明責任と追跡可能性を維持するために、文書化し、セキュアに保管されなければならない。

iii. CSP と CSC 双方の手順と役割を含む、正式な CSC 承認ワークフロープロセスを確立すべきである。CSC の承認と CSP の措置のスケジュールを定め、関係者に通知する。

iv. アクセス要請の状況を双方に通知するため、自動通知システムを導入すべきである。

c. アクセス要求のテンプレート

i. CSP と CSC の双方が使用するための標準化されたアクセス要求テンプレートを確立すべきである。

ii. テンプレートには、アクセス目的、アクセス対象データ、アクセス期間など、必要な情報を全て含めること。

iii. アクセスが許可される前に、両当事者がテンプレートに署名する必要がある。

d. アクセス制御：セキュアな PAM システムを活用し、リスクの高い CSC データへの特権的アクセスを管理し、特権的アクセスを特定の業務に必要な最小限のアクセスに制限する（IAM-10 を参照）。

e. 監査と監視:

i. 監査および監視機能は、CSC の高リスクデータに関連するすべてのアクセス要求、承認、およびアクティビティを追跡するために実装されるべきである（例えば、アクセスの試行、成功したアクセス、アクセス権限の変更、不審な活動や不正 な活動の記録など）。

ii. CSP は、リスクの高い CSC データへの全てのアクセスについて監査ログへのアクセスを CSC に提供し、誰がいつアクセスしたかを CSC が追跡できるようにする。

iii. CSP と CSC の双方に透明性を提供するために、報告メカニズムを確立すべきである。例えば、以下のような行為は記録され、報告されるべきである：

- 他のローカルシステムアカウントのパーミッションの変更
- カスタム SSH キーの確立など、バックドアの作成
- UNIX/Linux オペレーティングシステムでの sudo 設定ファイルの変更

iv. 改善すべき点を特定し、必要な調整を行い、そのプロセスが CSC の組織的リスク評価及びデータ保護要件に準拠していることを確認する。

f. アクセスレベルアグリーメント：

i. リスクの高い CSC データへのアクセスを CSP に許可するためのサービスレベルは、以下に沿って定義されるべきである。

要求提出の応答時間、承認プロセス、およびアクセス期間を含む、CSP と CSC の契約上の合意。不遵守に対

タ復旧手順。

viii. 情報漏えいや不正アクセスにより CSC が被った損害の補償

b. リスクの高いデータの範囲：

i. CSP は、以下のスコープを定義すべきである。

リスクの高いデータについては、誤解や許可されていない機微データへのアクセスの可能性を避けるため、両者が同じ見解であることを確認するために、CSC もそうすべきである。

ii. 特権とみなされるアクセスに関するガイドラインを定め、CSC の全資産所有者に周知する。

c. リクエスト承認プロセス：

i. CSC は、リスクの高いデータに関わるアクセス要求について、関連する代表者の明示的な承認を求めるべきである。

ii. CSP の特権アクセス要求を承認する権限を有する CSC の要員は、以下のように指定される。

iii. 高リスクデータへの特権的アクセス要請を承認するための正式なプロセスを確立すべきである。

iv. 特権アクセス要求の不承認は、適切に正当化され、文書化されるべきである。

d. 監査と監視：高リスクデータへのアクセスを継続的に監視・監査し、疑わしい行為や不正な行為を検出して対応する。これには以下が含まれる：

i. 監視のアクセス状況を監視するツールを活用する。

リアルタイムで、CSC の担当者に異常や違反の可能性を警告する。

ii. パターンと潜在的なリスクを特定するために、アクセスログとアクティビティ記録の定期的な監査を実施する。

iii. リスクの高いデータを含むセキュリティ侵害を迅速に調査し、是正するために、明確なインシデント対応計画を策定する。

iv. CSC と CSP の間で、CSC の高リスクデータへの CSP のアクセスに関連する懸念や不審な行動を報告するための連絡手段を確立すべきである。

e. レビューと評価リスクの高いデータへの特権的アクセスの必要性を定期的にレビューし、評価する。これには以下が含まれる：

i. アクセス許可の定期的な見直しを実施し、非アクティブまたは不要なアクセスを特定し、取り消す。

ii. 定期的なリスクアセスメントを実施し、アクセス制御メカニズムにおける潜在的な脆弱性を特定し、緩和する。

	するエスカレーションパスを確立すること（STA ドメインを参照）。 ii. アクセス協定とアクセス権は、アクセス権が CSC の組織的リスクアセスメントに沿うよう、定期的に見直されるべきである。	

Control Title	Control ID	Control Specification
ログの完全性を保護する	**IAM-12**	プロセス、手順、および技術的手段を定義、実装、および評価して、ログ基盤が特権アクセスロールを含む書き込みアクセス権を持つすべてのユーザーに対して読み取り専用であること、および、ログ基盤を無効にする機能が、職務の分離とブレークグラス（訳注：緊急停止）を確実に行える手順を通して制御する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC は共に、それぞれの環境におけるロギングインフラストラクチャーの管理、およびログへのユーザーアクセス（特権アクセスを含む）を提供するプロセスおよび手順に独立した責任を負うため、本管理策の実施責任は「依存しない形で共有」となる。CSP は、内部ユーザー、外部ユーザー（ベンダーおよび顧客）、アプリケーション、およびサービスを含め、 CSP が提供し維持するクラウド環境へのアクセスを持つエンティティに関する管理策を所有する。	**管理策所有権の根拠：** CSP と CSC は、それぞれの環境におけるロギングインフラストラクチャー、およびログへのユーザーアクセス（特権アクセスを含む）を提供するためのプロセスおよび手順の統制について、独立した責任を有するため、本管理策の実施責任は「依存しない形で共有」である。CSC は、内部ユーザー、外部ユーザー（ベンダーおよび顧客）、アプリケーション、およびサービスを含む、CSC が提供し維持するクラウド環境へのアクセス主体に関する管理策を所有する。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、アクティビティログが、できれば一元化された場所に確実に保管され、維持されるようにする責任を負う。ログの改ざんを防止するため、認証されたユーザーには読み取り専用アクセスのみを提供するものとする。特権アクセスがユーザーに提供される場合は、SoD の原則に従うべきであり、特権アクティビティは、管理者によるレビューのために別途記録および報告されるべきである。ロギングシステムは、リアルタイムの監視と、必要な場合のアラート送信のために、SIEM ソリューションと統合される	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

べきである。システムを無効にする能力は、SoD の原則をきちんと守った上で、緊急アクセス経路（break Glass）手順に従うべきである。

アクセス制御の範囲には、一般的な非特権ユーザーと、クラウドインフラストラクチャリソースのプロビジョニングとデプロビジョニングを担当するクラウド管理者、セキュリティポリシーと手順の策定と実装を担当するセキュリティ管理者、リソースのパフォーマンスと可用性の監視、トラブルシューティング、運用上の問題の解決を担当するシステムオペレータなどの全ての特権ユーザーが含まれる。

CSP がログの完全性を保護するための実装のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）：

a. 読み取り専用アクセスの制限：ログへのアクセスは、最小特権の原則に従い、常に読み取り専用に制限されるべきであり、許可された ID のみに制限されるべきである。
b. イミュータブルログストレージ：ログが改ざんされないことを保証し、システムイベントの正確な記録を提供するために、一度作成されたログが変更または削除されないような、イミュータブルログストレージソリューション（例えば、Write-once-read-many（WORM）ストレージ）を活用すべきである。
c. ログの完全性の検証：
    i. データの完全性を検証する技術（暗号ハッシュ関数など）を採用し、検証結果を監視して、矛盾や改ざんの兆候を特定する。
    ii. データの完全性の検証中に検出された不一致や異常の処理手順を実施すべきである。
d. 制御された読み取り専用アクセスの無効化：
    i. ログへの読み取り専用アクセスを無効にするために、SoD を採用すべきである。
    読み取り専用アクセスには、異なるユーザーまたはチーム間のコラボレーションが必要です。
    ii. 読み取り専用アクセスを無効にする責任を負う ID は、ログを修正する能力も持つべきではない。
    iii. ログへの読み取り専用アクセスを無効にできる特定のツールや特権コマンドへのアクセスを制限すべきである。
    iv. 読み取り専用アクセスを無効にするための複数段階の承認プロセスを定義し、実施すべきである（例えば、複数のユーザーからの承認と正当化）。
e. 緊急アクセス経路（Break-glass）手順
    i. 緊急事態における優先手順（読み取り専用アクセスを無効化できるようにする）を最高レベルのセキュリティクリアランスを持つ権限を与えられた人員のみが実施するよう文書化され、実施すべきである。
    ii. 緊急事態の場合、ログの読み取り専用アクセスを無効にするには、少なくとも 2 名の権限を有する者の承認

を必要とする。 f. ログのバックアップ：定期的なバックアップ、およびログのセキュアな復元手順を実施・確立し、データ損失や破損が発生した場合でもログが保護されるようにする。 g. 監査ログと監視： i. 読み取り、書き込み、および削除操作を含む、ログへの全てのアクセス試行を監視し、ログに対して実行されたアクションの監査証跡を提供し、不正な変更を検出できるようにする。 ii. ログデータは、ログを改ざんしようとしている可能性を示す異常、不整合、または不審なアクティビティを監視する必要がある。 iii. ログへの読み取り専用アクセスを無効化および有効化するための全てのアクションは、タイムスタンプ、ユーザーID、およびアクションの理由を含め、文書化されるべきである。	

Control Title	Control ID	Control Specification
一意に識別可能なユーザー	**IAM-13**	一意の ID またはユーザーID の使用を個人に関連づけることにより、ユーザーを識別できるようにするプロセス、手順、および技術的手段を定義、実装、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC は、それぞれの組織内のユーザーに一意な識別子を生成し割り当てるプロセスと手順を統制する責任を個別に負うため、本管理策の実施責任は「依存しない形で共有」となる。CSP は、内部ユーザー、外部ユーザー（ベンダーおよび顧客）、アプリケーション、およびサービスを含む、 CSP が提供し維持するクラウド環境へのアクセスを持つエンティティに関連して、本管理策を所有する。	**管理策所有権の根拠：** CSP と CSC は、それぞれの組織において、一意の識別子を生成し、ユーザーに割り当てるプロセスと手順を統制する責任を個別に負うため、本管理策の実施責任は「依存しない形で共有」となる。CSC は、内部ユーザー、外部ユーザー（ベンダー及び顧客）、アプリケーション、及びサービスを含む、 CSC が提供及び維持するクラウド環境へのアクセス権を有するエンティティに関して、本管理策を所有する。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、システムアクセスを要求するユーザーが一意に識別可	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

能であり、その行為に直接責任を負うことができることを保証する責任がある。CSP が特権アクセスまたは機能に共有アカウントの使用を許可する場合、システムログは、共有アカウントに代わって行動するユーザーの一意の ID を記録して、個人の説明責任を確保する必要がある。

このような共有アカウントの範囲には、クラウドインフラストラクチャリソースのプロビジョニングとプロビジョニング解除に責任を持つクラウド管理者、セキュリティポリシーと手順の策定と実装に責任を持つセキュリティ管理者、リソースのパフォーマンスと可用性の監視、トラブルシューティング、運用上の問題の解決に責任を持つシステム運用者のアカウントが含まれる。

ユーザーの識別と一意な ID との関連付けを確実にするための実施ガイドラインには、以下が含まれる（ただし、これらに限定されるものではない）：

a. ユニーク ID 管理：
   i. ユーザーID の収集目的、使用方法、および保持を確立し、文書化し、CSP のプライバシーおよびセキュリティ規制と整合させ、データの収集、処理、および共有方法について透明性のある情報をユー ザに提供する。
   ii. ユーザー識別のためのユースケースと、ユーザーID に関連付けられるデータの機密レベルを定義すべきである。
   iii. 各ユーザーアカウントは、アクセスが許可される前に、固有の ID を持つべきである。共有アカウントの使用が許可されている場合、共有アカウントの最新リストと、共有アカウントの代わりに行動できる全てのユーザー（一意の ID と権限を含む）が、常に維持されるべきである。
   iv. 共有アカウントの使用は、そのアカウントを代表して行動した一意のユーザーID まで追跡可能でなければならない。
   v. 一意な識別子の要件を実施するために、自動制御を導入すべきである。
b. ユニーク ID の生成：ID の衝突や再利用の可能性を防ぐため、ユーザーに固有の ID を生成する暗号的にセキュアなアルゴリズムを採用すべきである。
c. 仮名 ID：ユーザーID を直接個人データと関連付けるのではなく、仮名化技術を採用し、実装すべきである。
d. ID アクセス制御：ユーザーID へのアクセスを許可された人員、システム、プロセスに制限するために、アクセ ス制御手段を導入すべきである。
e. ID の暗号化：全てのユーザーID は、無許可のアクセスやデータ漏洩から保護するために、保存時および転送時に暗号化されるべきである。
f. ID のマッピングとリンク：ユーザーID を個人情報またはそ

の他の機密データに対応付けるための、セキュアかつ監査可能なメカニズムを導入すべきである。 g. ID の有効期限： i. 時間の経過とともに過剰な個人情報が蓄積されるのを防ぐため、ユーザーID の有効期限に制限を設けるべきである。 ii. 特定の目的に必要なデータ以上の収集は制限されるべきであり、別途収集される追加データは、明示的なユーザーの同意が必要である。 h. ユーザーの同意およびオプトアウト・オプション：ユーザーは、ID の収集、使用、および共有について明示的な同意オプションを提供され、特定の ID の使用をオプトアウトすること、または CSP のデータベースからの削除を要求することを許可されるものとする。 i. 継続的な監視と評価：ユーザーID の使用、アクセス、変更、および削除を追跡および評価するための監視メカニズムを実装し、異常または潜在的なセキュリティ侵害を検出するために定期的に見直すこと。 j. 規制の変更：進化するデータプライバシー規制（GDPR、CCPA など）を常に把握し、それに応じて ID 管理慣行を適応させる。	

Control Title	Control ID	Control Specification
強固な認証	**IAM-14**	システム、アプリケーション、およびデータ資産へのアクセスを認証するためのプロセス、手順、および技術的手段を定義、実装、および評価する。これには、少なくとも特権ユーザーおよび機微データへのアクセスに対する多要素認証が含まれる。システムアイデンティティに対して同等レベルのセキュリティを実現するデジタル証明書または代替手段を採用する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠： CSP と CSC はともに責任を負うが、非コンソールの管理者アクセスおよびリモートアクセスを認証するためのプロセスと手順をそれぞれ独立して統制するため、本管理策の実施責任は「依存しない形で共有」 である。CSP は、CSP 内部ユーザー、外部ユーザー（ベンダーや顧客）、アプリケーション、サービスを含め、CSP が提供し維持するクラウド環境へのアクセスを持つエンティティに関連して本管理策を所有する。	**管理策所有権の根拠：** CSP と CSC は共に責任を負うが、非コンソールの管理者アクセスおよびリモートアクセスを認証するためのプロセスおよび手順をそれぞれ独自に統制するため、本管理策の実施責任は「依存しない形で共有」である。CSC は、CSC 内部ユーザー、外部ユーザー（ベンダーや顧客）、アプリケーション、サービスを含む、CSP が提供し維持するクラウド環境へのアクセスを持つエンティティに関連して本管理策を所有する。
実施ガイドライン： **全てのサービスモデルに適用：** システム、アプリケーション、および機微データへのアクセスを認証するための手順と手続および技術的手段を定義し、維持すべきである。 CSP は、コンソール以外の管理アクセスおよびリモートアクセスに MFA が必要であることを保証する責任を負う。 機微データへのアクセスにおける MFA および電子証明書の実装のベストプラクティスには、以下が 含まれる（ただし、これらに限定されない）： a. 認証管理： i. 全てのクラウドサービスにおいて、ID、認証情報、アクセス制御権限を管理できる集中型認証システムを導入すべきである。 ii. 特権アクセスが必要なユーザー（管理者や IT スタッフなど）を特定し、より厳格な認証手段を確立する。 iii. 特権 ID や機密データへのアクセスに対する MFA を含め、アクセスレベルごとに具体的な認証要素と技術的手段を定義し、実施する。 b. MFA の使用範囲： i. 機密データへのアクセス：全てのユーザーアカウントで、ユーザーが知っているもの（パスワードなど）、持っているもの（モバイルデバイスやトークンなど）、属性があるもの（生体認証など）の組み合わせを必要とする強力な認証を実施する：知っている（パスワードなど）、持っている（モバイルデバイスやトークンなど）、属性があるもの（生体認証など）。 ii. 管理アクセス：全ての管理アクセス（クラウド管理コンソール、仮想マシン、リモートアクセスゲートウェイ、その他の重要なクラウドインフラ要素へのアクセスなど）に対して MFA を実施すべきである。特定の状況で MFA を実施できない場合は、そのリスクを正式に登録する。 iii. リモートアクセス：VPN、Web アプリケーション、モバイルデバイスを問わず、全てのリモートアクセスに対して MFA を実施する。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

iv. 第三者アクセス：API やクラウドサービスを介したサードパーティーからのアクセスには MFA を実施し、外部からの不正アクセスから保護する。

c. 二要素認証：第二要素認証は、パスワードに加えて、第二の要素を要求することでセキュリティのレイヤーを追加するために活用されるべきである：

i. タイムベースワンタイムパスワード（TOTP）は、SMS、電子メール、認証サーバーと同期したスマートフォンアプリを通じて、ユーザーが一時的なコードを生成できるようにする。

ii. 認証用のユニークなコードを生成するハードウェアトークンまたは USB キー

d. パスワードレス認証：フィッシングに強い MFA や FIDO2 準拠のセキュリティ鍵、生体認証など、従来のパスワードをセキュアな代替手段に置き換えるパスワードレス認証ソリューションを導入すべきである。

e. 認証クレデンシャルの保護：全ての認証クレデンシャルは、セキュアなチャネル（TLS/HTTPS など）を通じて送信され、決して平文で保存されることなく、強力な暗号を使用して全てのシステムコンポーネントのストレージで読み取り不可能にされるべきである。

f. 認証クレデンシャルの変更承認：認証クレデンシャルの変更または修正（パスワードのリセット、新しいトークンのプロビジョニング、新しい鍵の生成など）のリクエストは、ユーザーの本人確認後にのみ承認されるべきである。

g. 継続的ユーザー認証（CUA）：CUA は、セッションを通してユーザー認証を維持する方法として活用されるべきであり、定期的な再認証を必要とすることで、ユーザーがまだ認証されており、危険にさらされていないことを確認する。

h. シングルサインオン（SSO）：ユーザーの認証プロセスを簡素化するため、1 つのログインクレデンシャルで複数のサービスやアプリケーションにアクセスできる SSO を実装する必要がある。

i. デジタル証明書：デジタル証明書は、特にシステムアイデンティティの認証および認可の目的で利用されるべきである。

j. CRL および OCSP チェック証明書失効リスト（CRL）とオンライン証明書ステータスプロトコル（OCSP）チェックは、デジタル証明書の有効性と失効ステータスを検証するために実装されるべきである。

k. 証明書のライフサイクル：電子証明書のライフサイクルは、発行、更新、失効を含めてセキュアに管理されるべきである。

l. 証明書の保管：デジタル証明書は、暗号化およびアクセス制御の仕組みを用いてセキュアに保管する。

m. 認証使用状況の監視：

i. 全ての認証メカニズムおよび有効化された機能は、適切にインストール、設定され、認証ログが望まし

	い結果および期待される結果について監視されなければならない。 ii. MFA、クレデンシャル、電子証明書の使用パターンを継続的に監視およびレビューし、潜在的な脆弱性や侵害を事前に特定する。	

Control Title	Control ID	Control Specification
パスワード管理	**IAM-15**	パスワードのセキュアな管理のプロセス、手順、および技術的手段を定義、実装、および評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC は共に責任を負うが、それぞれの組織においてユーザーのパスワードをセキュアに管理するためのプロセスと手順を独立して統制するため、本管理策の実施責任は「依存しない形で共有」である。CSP は、内部ユーザー、外部ユーザー（ベンダーおよび顧客）、アプリケーション、およびサービスを含む、CSP が提供し維持するクラウド環境へのアクセス主体に関連して、本管理策を所有する。	**管理策所有権の根拠：** CSP と CSC はともに責任を負うが、それぞれの組織においてユーザーのパスワードをセキュアに管理するプロセスと手順を独立して統制するため、本管理策の実施責任は「依存しない形で共有」である。CSC は、内部ユーザー、外部ユーザー（ベンダーおよび顧客）、アプリケーション、およびサービスを含む、CSC が提供し維持するクラウド環境へのアクセス主体に関連して、本管理策を所有する。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、認証クレデンシャル（パスワード、PIN、トークンなどを含む）をセキュアに管理するためのプロセスおよび技術的手段を定義、実装、および評価する責任を負う。全ての関連ポリシー、標準、および手順は、全てのユーザーに周知されるものとする。パスワードを使用する場合は、使用可能なライフサイクル全体を通じてセキュアに管理し、以下に述べるような優れたパスワードセキュリティ慣行に従う必要がある。 セキュアなパスワード管理のための実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. パスワード強度の要件：パスワードの強度を高め、ブルートフォース攻撃への耐性を高めるため、パスワードの要件を業界標準に従って実施する。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

b. パスワードの複雑さ：パスワードの複雑さの要件は実装されるべきである。
    i. 大文字と小文字を混在させる。
    ii. 数字と特殊文字を使用する
    iii. 一般的な単語やパターンなど、推測されやすい情報は避ける。
c. 最小パスワード長：パスワードが短すぎて簡単に漏洩しないように、パスワードの最小長を設定する必要がある。
d. パスワード履歴：パスワード履歴ポリシーを実施し、ユーザーが以前のパスワードを再利用するのを防ぐために、以前に使用したパスワードの記録を保管すべきである。
e. パスワードの有効期限：パスワードの有効期限ポリシーを実施し、頻繁なパスワード変更を促すプロセスを導入すべきである。
f. パスワードのローテーション：予測可能なパターンを避けるため、強力でユニークなパスワードの必要性とバランスを取りながら、パスワードを定期的に更新するようユーザーに奨励すべきである。
g. デフォルトパスワードの更新：ベンダーが提供するアイデンティティおよびアカウントのパスワードのデフォルト設定は全て削除し、組織のパスワード管理ポリシーに従ってリセットする。
h. パスワード保護：
    i. 強力なパスワードハッシュアルゴリズムを使用し（PBKDF2やbcryptなど）、必要な場合は最新の（非推奨の）業界標準に従って更新（パスワードの再ハッシュ化）すべきである。
    ii. 攻撃者が事前に計算したテーブル（レインボーテーブル）を攻撃に使用するのを防ぐため、各パスワードに固有の「salt」を生成し、ハッシュ化する前にパスワードと組み合わせる。
    iii. 強力な暗号化を使用して、保存中および移動中（特にログインプロセス中）のパスワードを保護する。
i. パスワードの永続性：
    i. パスワードの永続化はクライアント側のアプリケーションで、パスワードがユーザーのデバイスにローカルに保存されるのを防ぐ。
    ii. Web ブラウザや電子メールアプリケーションにパスワードを保存することは避けるべきである。
j. アカウントロックアウトの仕組み：認証に一定回数失敗した場合、一時的にアクセスを制限するアカウントロックアウトの仕組みを導入すべきである。
k. 公開表示の防止：アプリケーションは、どの画面にもパスワードを平文で表示しないようにデフォルトで

設定されるべきである（すなわち、パスワードの画面表示をマスクする）。入力中にパスワードを表示する」オプションを選択できるようにすべきである。

l. パスワード管理者：ユーザーは、パスワードマネージャまたは統合されたパスワード保存機能にアクセスできるようにし、異なるアカウント用の強力で一意のパスワードを生成、管理できるようにする。

m. パスワードの自動生成：自動的に選択されるパスワード/パスフレーズは、暗号的にセキュアな擬似乱数生成器（CSPRNG）で生成されるべきである。

n. パスワードのリセット

  i. ユーザーが独自にパスワードをリセットできるセルフサービスパスワードリセット（SSPR）メカニズムの使用

  ii. パスワード再設定時、ユーザーは組織のパスワード複雑性要件に従うこと。

  iii. 全てのパスワードリセット活動の正確な記録が維持されるべきである（例えば、関係するユーザー、リセットの日時、リセットの理由）。

  iv. 高度に特権化されたアカウント（例：テナントのルート／管理者）のパスワードリセットには、MFAまたはその他の追加認証ステップ（例：対面／電話確認）を使用する。

o. パスワードリカバリ：パスワードリカバリのための安全な仕組みを導入すること（例：電子メール、期間限定のリカバリーリンク）。

p. パスワード管理の監視：監視ツールを活用し、パスワードの変更やログインの試行に関する不審な行為を検知し、警告する。

Control Title	Control ID	Control Specification
認可メカニズム	**IAM-16**	データおよびシステム機能へのアクセスが認可されていることを確認するためのプロセス、手順、および技術的手段を定義、実装、および評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines

CSP	CSC
管理策所有権の根拠： CSP と CSC が共に責任を負うが、それぞれの組織内のユーザーに付与されるアクセスについて正式な承認を確実に取得するためのプロセスと手順も独立して統制するため、本管理策の実施責任は「依存しない形で共有」である。CSP は、内部ユーザー、外部ユーザー（ベンダーおよび顧客）、アプリケーション、およびサービスを含む、 CSP が提供し維持するクラウド環境へのアクセス主体に関連して、本管理策を所有する。	**管理策所有権の根拠：** CSP と CSC が共に責任を負うが、それぞれの組織内のユーザーに付与されるアクセスについて正式な承認を確実に取得するためのプロセスと手順も独立して統制するため、本管理策の実施責任は「依存しない形で共有」である。CCP は、内部ユーザー、外部ユーザー（ベンダーおよび顧客）、アプリケーション、およびサービスを含む、CCP が提供し維持するクラウド環境へのアクセス主体に関連して、本管理策を所有する。
実施ガイドライン： **全てのサービスモデルに適用：** アクセス認可の検証は、効果的なアクセス制御の基本的な要素であり、ユーザーが正当な必要性に基づいてアクセス権を与えられ、不正なアクセスの試みが速やかに特定され、防止されることを保証する。 CSP は、認可を検証し、不正アクセスを防止するための強固な技術的手段を導入する上で重要な役割を果たす。 これらの対策を定義し、実施し、評価するための実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）： a. 認可メカニズ i. ID は、PoLP に従って職務を遂行するために必要なアクセスのみが提供されるべきである。 ii. 動的 RBAC、ABAC、およびコンテキストを考慮したアクセス制御メカニズムは、アクセス制御の意思決定プロセスの一環として、定義された特権と許可を持つ特定のロールをユーザーに割り当てるために実装されるべきである。 iii. 個々のリソース（ファイル、データベース、アプリケーションなど）に対して、ユーザーまたはグループに明示的なパーミッション（読み取り、書き込み、実行）を割り当てる。 iv. アクセス許可を与える前に、アクセスが許可されていることを確認するプロセスを導入すべきである。 b. 承認要求と承認： i. 上級管理者は、リソースへのアクセスを要求する新規ユーザーを知らされるべきであり、十分な正当性をもって、そのような要求をレビューし、承認し、文書化すべきである。 ii. 緊急事態（セキュリティインシデントの解決や大規模停電からの復旧など）の場合は例外として、上級管理職の承認を得るべきであるが、承認なしのアドホックなアクセス要求は認めるべきではない。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

iii. 特権の付与には、2 つのレベルの承認が必要である（すなわち、ユーザーの管理者または監督者の承認と資産所有者の承認が必要である）。 iv. 正式な承認なしに付与されたアクセスを特定し、報告するための検知メカニズムを導入すべきである。 v. アクセスの種類及び関連する要請を承認する権限を有する者のリストを文書化し、維持すること。 vi. アクセス権は、そのようなアクセスのビジネス上の正当な理由が存在しなくなった後、直ちに取り消されるべきである。 c. 認可の監視と見直し：権限の仕組みは定期的に見直し、更新する。認可されたIDのみがアクセスできるように、アクセス要求、ログイン試行の成功および失敗、リソースの使用など、IDの活動の記録についてレビューを実施する。	

Control Domain IPY

2.11 相互運用性と移植容易性(IPY)

Control Title	Control ID	Control Specification
特権的なアクセスロールの管理	**IPY-01**	次の事項の要件を含む相互運用性と移植容易性のためのポリシーと手順を確立、文書化、承認、周知、実装、評価、維持する。 a. アプリケーションインタフェース間コミュニケーション b. 情報処理の相互運用性 c. アプリケーション開発の移植容易性 d. 情報/データ交換、利用、移植容易性、完全性、永続性ポリシーと手順を少なくとも年1回レビュー、更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP はデータおよび関連するメタデータとコードの相互運用性と移植容易性に関連する情報の伝達におけるポリシー、標準、ガイドライン、手順および透明性に責任を負う。	**管理策所有権の根拠：** CSC はデータ形式、開発言語、デザインパターンおよびクラウド導入のアーキテクチャ要件について、相互運用性と移植容易性をサポートするポリシー、手順、プロセス及び標準を導入する責任を負う。ベンダーロックインを避けるため、相互運用性と移植容易性は、ベンダー選定のプロセス、継続的なベンダーの監査及び撤退計画に反映されなければならない。
実施ガイドライン： システムの相互運用性は CSC の最大の関心事である。CSP が一般的に公開または標準化されている技術に基づいてサービスを提供する度合いによって、クラウドシステム間の相互運用性は向上する。相互運用性と移植容易性の管理は、CSP が停止した場合でも CSC のビジネスを障害から保護できるようにすることを目的としている。これには他の CSP または現在利用しているプロバイダーとは異なるリージョンとの相互運用性や移植容易性についての計画も含む。	**実施ガイドライン** 移植容易性と相互運用性を組み合わせることでクラウドソリューションの互換性が実現される。これらはクラウドプランニングの重要な考慮事項となる。なぜなら、これらを組み合わせることで、クラウドソリューションが（相互運用性により）継続的に動作し、（移植容易性により）変更することなく動作し続けることが保証されるからである。コンポーネント間の移植容易性と相互運用性が確保されない場合、予期しない処理障害が発生し、それに伴うコストが発生するビジネス中断が発生する可能性がある。 クラウドコンピューティングでは、ビジネスニーズの変化によりサービスプロバイダーを変更する必要が生じた場合、相互運用性への影響がしばしば生じる。

	ある CSP ではシステムが仕様通りに機能していても、新たな CSP ではそうでない場合もある。洞察力の欠如は 1 つのクラウドサービスプロバイダーに縛られることにつながる。必然的なビジネス上の意思決定により、時間の経過とともに変化が生じ、プロバイダーの変更につながる可能性がある（プロバイダーやプラットフォームの移行の必要性、異なる機能セットの要望、プロバイダーの完全な喪失、法的紛争など）。 CSC は、契約期間中だけでなく、調達プロセスにおいても、CSP の独立した監査報告書と文書をレビューする必要がある。CSC は、相互運用性と移植容易性を得るために継続的なデータリスク評価を実施し、変更を反映するための内部ポリシーと手順を見直し、更新されるようにしなければならない。
IaaS プロバイダー： CSP は、最小限の労力でさまざまな異なるシステムが相互運用できる標準化されたハードウェアとコンピューティングリソースを提供すべきであり、相互運用性を維持するために業界標準に厳密に準拠する必要がある。CSP は、クラウドブローカー、クラウドバースティング、ハイブリッドクラウド、マルチクラウド連携などの複雑なシナリオをサポートできなければならない。 CSP は、複数の CSP、ハイブリッドモデル、または別の CSP やプライベートクラウドへの移行を含むアーキテクチャを CSC がデプロイできるように、ポリシー、手順と手続および標準を実装する責任を負う。ポリシー、プロセスおよび手順は、最新の状態を維持し、毎年レビューし、毎年監査し、独立した監査報告書を CSC に提供しなければならない。	**IaaS 利用者：** 移植容易性と相互運用性に関して、CSC がポリシーと手順を策定する際に考慮すべきさまざまな要素は、以下のとおり。 a. 仮想マシンをキャプチャし、異なる仮想化技術を用いる新たな CSP に移植する方法を理解する。 例） DMTF （Distributed Management Task Force）、OVF （Open Virtualization format）など。 b. 仮想マシン環境に対するプロバイダー固有の拡張を特定し、排除する（または少なくとも文書化する）。 c. アプリケーションが CSP から移植された後、仮想マシンイメージの適切なプロビジョニング解除が行われるようどのような方法が講じられているかを理解する。 d. アプリケーション／データの移行前に特定する必要があるハードウェアおよびプラットフォームベースの依存関係を理解する。 e. 新しいサービスプロバイダーが劣っていることが判明した場合に、レガシーCSP にてサービスの一部または全部を再開または延長するオプションを特定する。 f. 新しいプロバイダーと互換性のない、あるいは未実装の管理レベル関数、インタフェース、API が使用されていないかどうかを判断する。
PaaS プロバイダー： CSP は、CSC がシステムを構築するためのプラットフォームを提供する責任を負う。CSP はランタイム環境と統合アプリケーションスタックを提供する。これにより開発者はインフラストラクチャを構築する必要がなく、提供されるプラットフォーム上でカスタムアプリケーションを迅速に開発し、デプロイすることができる。CSP は、インフラストラクチャ全体とそのメンテナンスを CSC に提供する。 CSP は、他の CSP またはプライベートクラウドに移行可能なアプリケーションの開発及びデプロイにおいて CSC をサポートするポリシー、手順、手続及び標準を実装する責任を負う。ポリシー、プロセスおよび手順は、最新の状態を維持し、毎	**PaaS 利用者：** 移植容易性と相互運用性に関して、CSC がポリシーと手順を策定する際に考慮すべきさまざまな要素は、以下のとおり。 a. 可能であれば標準的な構文、オープン API、オープンスタンダードのプラットフォームコンポーネントを使用する。 例）OCCI（Open Cloud Computing Interface）など b. セキュアなデータ転送、バックアップ、復元に利用できるツールを理解する。 c. PaaS プロバイダー固有のアプリケーションコンポーネントとモジュールを理解し、文書化する。また、抽象化されたレイヤーを持つアプリケーションアーキテクチャを開発し、独自のモジュールへの直接アクセスを最小限に抑える。

年レビューし、毎年監査し、独立した監査報告書を CSC に提供しなければならない。	d. 新しいプラットフォームに移行する場合、アプリケーションのパフォーマンスと可用性に与える影響とこれらの影響をどのように測定するかを理解する。 e. 移行前および移行後にアプリケーションテストがどのように完了するのかを理解し、サービスまたはアプリケーションが正しく動作していることを確認する。テストに関するプロバイダーとユーザーの双方の責任が十分に認識され、文書化されていることを確認する。
SaaS プロバイダー： CSP は、クラウド上でアプリケーション機能を提供し、CSC はその管理とシステム内外の情報の流れを管理する。エンドユーザーはブラウザを必要とし、あらゆるレベルの管理の大部分はプロバイダーに委ねられる。 CSP は、CSC が自社のデータ保持標準に従ってデータとメタデータを保持し、サービス停止時、または他の CSP やプライベートクラウドに移行する際に全てのデータとメタデータを復元することをサポートするポリシー、手順と手続および標準を実装する責任を負う。ポリシー、プロセスおよび手順は、最新の状態を維持し、毎年レビューし、毎年監査し、独立した監査報告書を CSC に提供しなければならない。	**SaaS 利用者：** 移植容易性と相互運用性に関して、CSC がポリシーと手順を策定する際に考慮すべきさまざまな要素は、以下のとおり。 a. バックアップおよびログ、アクセス記録、その他の関連情報の複製が移行できることを保証する。 b. SaaS プロバイダーなしで使用可能な形式への定期的なデータ抽出とバックアップを実施し、メタデータの保存と移行が可能かどうかを把握する。可能であればデータエクスローサービスを利用する。 c. 非構造化データを相互運用可能な ZIP 形式のような確立されたポータブルフォーマットで保存することでストレージと転送の両方の要件を削減する。ファイルを ZIP アーカイブに集約し、複数のファイルセットを移動する複雑さを軽減する。 d. 選択したストレージフォーマットが基盤となるプラットフォームに関係なく相互運用できるようにする。データは、モバイル、デスクトップ、メインフレームのいずれからもアクセスできる必要がある。 e. 導入されるカスタムツールを再開発する必要があるのか、新しいベンダーがそれらのツールを提供できるのかを理解する。 f. 管理、モニタリング、レポーティングのインタフェースと環境間の統合について理解する。 g. 移行前に新しいベンダーがアプリケーションをテストし評価する方法があることを保証する。
ポリシーには、以下に関する規定を含まなければならない（ただし、これらに限定されない）： a. 標準化された通信プロトコル：広く受け入れられている通信プロトコル（RESTful API、JSON、XML など）の使用を義務付けることで、異なるアプリケーションインタフェース間のシームレスな相互運用を保証する。 i. RESTful API や SOAP API など、業界標準の API プロトコルを採用する。 ii. API 仕様を明確に文書化し、開発者向けにソフトウェア開発キット（SDK）を提供する。 iii. API ゲートウェイを実装し、API トラフィックを管理、保護する。利用ガイドライン、リクエスト例、レスポンス例を含む API ドキュメントを提供する。	**ポリシーには、以下に関する規定を含まなければならない（ただし、これらに限定されない）：** a. クラウドサービスオファリングの全てのクラウド機能にアクセスするための共通および／またはオープンインタフェースを CSP が公開していることを確認する。 b. より高レベルのスケーラビリティを可能にするため、異なる CSP とのフェデレーション能力を確保する。 c. CSP とのデータ移行にかかるコストの見積もり計画。 d. CSP 間のセキュリティポリシーや管理、鍵管理、データ保護の違いを理解し、新しいプロバイダーやプラットフォームに移行する際に、未発見のセキュリティギャップを回避する。 e. 新旧プロバイダー間で、セキュリティとプライバシーの管理策の実施効果を保証する。

iv. 変更を管理し、後方互換性を維持するためにバージョニングを実施する。

b. セキュアな通信：トランスポートレイヤーセキュリティ（TLS/SSL）を実装し、認証および認可メカニズムを実装することにより、アプリケーションインタフェース間で交換されるデータがセキュアであり、不正アクセスから保護されていることを保証する。

c. 標準化されたデータフォーマット：アプリケーションとデータ処理システム間の相互運用性を促進するために、標準化されたデータフォーマットを定義し、遵守することにより多様なシステム間で一貫したデータ処理を保証する。

i. データ表現には、XML、JSON、CSV などの標準化されたデータ形式を利用する。

ii. データの一貫性を確保するために、データ変換と正規化技術を導入する。

iii. 相互運用可能なデータ処理を促進するため、共通のデータモデルとデータ交換プロトコルを採用する。

d. クロスプラットフォーム互換性：プラットフォームにとらわれないアプリケーションや処理ワークフローを設計することで、異なるプラットフォームや環境での情報処理をサポートする。コンテナ化技術（Docker など）を使用してアプリケーションをカプセル化する。

i. サーバレスコンピューティングプラットフォームやコンテナ化技術など、クラウドに中立的な開発フレームワークやツールを活用する。

ii. クラウドにとらわれないプログラミング言語とライブラリを採用する。

iii. クラウドプラットフォームの標準かれた導入プロセスと構成管理ツールを採用する。

e. 共通のデータ処理標準：確立された標準（データベースなら SQL、ビッグデータ処理なら Apache Spark など）に基づいた処理ロジックを実装することで、情報処理が業界で認められた標準に準拠するようにする。

f. クロスプラットフォーム開発ツール：クロスプラットフォーム開発をサポートする開発ツールやフレームワークを提供することで、開発者が大きな変更を加えることなく異なるプラットフォーム上で動作するアプリケーションを作成できるようにする。

g. コンテナ化のサポート：アプリケーションをカプセル化するコンテナ化技術（Kubernetes など）をサポートすることで、さまざまな環境にまたがるアプリケーションのデプロイと実行を簡素化し、基盤となるインフラストラクチャに依存しない相互運用可能なアプリケーションを実現する。

h. IaC（Infrastructure As Code）の実践：IaC ツール（Terraform、Ansible など）の使用を奨励し、インフラストラクチャ、構成を相互運用可能な方法で定義・

f. CSP 間の法律、規制、コンプライアンス、運用の観点からの違いを理解する。カスタマーのデータやアプリケーションに厳格なコンプライアンスやプライバシーの要件がある場合、移行を決定する前に、新しいクラウド・ベンダーの要件を評価する必要がある。

g. 監視、ロギング、監査などの基本サービスが、どのように新しいベンダーに引き継がれるかを理解する。

h. クラウド上のデータが変更されないことを保証するために、データの完全性対策を取り入れるべきである（透かしの使用、デジタル署名など）。

i. クラウドとの間で移動するデータには相互運用可能なデータ圧縮を使用し、移動するデータ量を減らし、移動に要する時間を短縮する。

j. 公開されている仕様（OpenPGP、ZIP など）を通じて利用できるような相互運用可能な暗号化を使用し、プラットフォーム、ストレージシステム、存在する場所に関係なく、データとファイルを直接かつ永続的に保護する。

k. クラウドに置く前にデータを暗号化し、マルチテナントによるリスクや、CSP の不注意なスタッフや不機嫌なスタッフによるリスクを回避する。

l. 誰がデータ暗号化鍵へのアクセス権を保持しているかを理解し、暗号化および鍵管理ポリシーの要求に従い、全ての暗号化鍵の管理を保持する。

管理することで、環境間の一貫性を確保するために、インフラストラクチャの記述とプロビジョニングを標準化する。

i. 標準化されたデータ交換フォーマット：標準化されたデータ交換フォーマットと構造を定義し遵守することで、システム間の一貫した明確なデータ交換を促進し、互換性を確保し、データ変換の複雑さを軽減する。

j. データの完全性と永続性：データの完全性チェックを実施し、信頼性の高いストレージシステムを使用し、データの永続性を維持するためのバックアップとリカバリの仕組みを確立することにより、異なるシステムやストレージ環境にわたるデータの信頼性と完全性を確保する。

    i. データ完全性検証メカニズムを活用し、移動中のデータの正確性を確保する。

    ii. ログやスクリーンショットに含まれる機微データを保護するためにデータマスキング技術を採用する。

k. 共通のデータ使用ポリシー：一貫性とセキュリティを維持するために、データ使用ポリシー、アクセス制御、アクセス許可を定義し実施することで、異なるアプリケーション間でのデータのアクセス、利用、共有方法を標準化する。

l. データ移植容易性に関する契約上の義務：

    i. 移植容易性を促進するため、データ交換のための標準化されたフォーマットを定義し、文書化する。

    ii. データ保持期間に関し、法的および規制上の要件を考慮した上で、データが保存される期間を定める。データの保持および削除のための自動化されたプロセスを実装する。

    iii. 保持するデータの範囲を定め、CSC が利用できるようにする。

    iv. 保持データの包括的なデータ削除ポリシーを定義し、セキュアな削除方法を含める。（DCS-01 および DSP-02 を参照）

m. 契約の終了：契約終了時、CSP は CSC のデータを別のクラウド環境またはオンプレミスシステムにエクスポートし、移行するための合理的なサポートを提供する。このサポートには、技術文書、データエクスポートツールおよびシームレスなデータ移行を促進するために必要なサポートの提供が含まれる。

    i. 契約終了時に CSC がデータにアクセスできることを契約書に明記する。

    ii. CSC へのデータの引継または転送のためのセキュアな方法を実装する。

    iii. CSC へのサービスとデータの円滑な移行を確実にするための終了計画を策定し、文書化する。

    iv. 移行期間中のデータを保護するためのセキュ

リティ対策を含む。 v. データの所有と契約終了時の所有の移転を明確に定義する。 vi. データの機密性と完全性を確保するための法的および技術的なメカニズムを含める。 n. 承認：組織の戦略目標とリスク許容度との整合性を確保するための承認要件と上級管理職の関与 i. ポリシーと手順の変更または修正については、承認プロセスを確立しなければならない。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。 o. コミュニケーション：関係する全てのクライド利害関係者に対して、ポリシーと手順の効果的な伝達を促進しなければならない。 p. メンテナンスとレビュー：相互運用性と移植容易性に関するポリシーと手順は、進化するクラウドセキュリティの状況との整合性を確保し、クラウド技術、規制、リスクの変化を反映するために、少なくとも年 1 回は文書化し、見直し、更新する。	

Control Title	Control ID	Control Specification
アプリケーションインタフェースの可用性	**IPY-02**	CSC がプログラム的にデータを検索して相互運用性と移植容易性を可能にすることができるように、CSC に対してアプリケーションインタフェースを提供する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、セキュリティ、可用性およびユーザビリティについてテストされた、世界的に認められ標準化されたガイドラインおよびプロトコルを活用したセキュアな API を CSC に提供する責任を負う。CSP は CSC が利用できるドキュメントを提供しなければならない。	**管理策所有権の根拠：** CSC は、利用可能な API、そのセキュリティ、標準の相互運用性、ベンダーロックインにつながる可能性のある複雑さ、データ転送や回復に関連するコストを理解する責任を負う。
実施ガイドライン：	**実施ガイドライン：**

全てのサービスモデルに適用：
CSP は、その API が相互運用可能であることを保証し、環境間でのアプリケーションとデータのセキュアな移行を促進しなければならない。

API は、CSC が分散型クラウドのデプロイに使用し、環境からセキュアにデータを削除できるよう、設計上セキュアで、世界的に認められた標準化されたガイドラインとプロトコルに従ったものでなければならない。

CSP は、CSC に正確な文書を提供し、計画されている変更や更新について伝えなければならない。ドキュメントは API の機能をサポートし、定期的に更新され、新しい API のバージョンとともにカスタマーに提供されなければならない。さらに、開発および更新の際には、セキュリティ問題を考慮しなければならない。

全てのサービスモデルに適用：
CSC には、API の形でクラウドサービスと相互作用するためのさまざまな方法がある。CSP の移植容易性をと相互運用性のために登場した重要な標準や技術（OCCI、OVF など）は、大半の CSP でサポートされている。プラットフォームプロバイダーによって提供されるクラウドアプリケーションフレームワークは異なり、API の互換性や相互運用性に影響を与える差異も存在する。

CSC が CSP が提供する API を使用してデータを取得する場合、CSC は CSP のガイドライン（OWASP などの関連する情報源についても考慮）に準拠した構成、デプロイの文書化、実装中および終了計画アクティビティを通じてのデータおよびメタデータの転送と回復機能のテストに責任を負う。

CSC は、CSP の文書、独立した監査報告書およびセキュリティテストをレビューしなければならない。CSC は、CSP が提供するリソースを監視し、サービスに影響を与える可能性のある API の停止、変更および CSC による対応が必要となる脆弱性の警告をカスタマーに通知する責任を負う。

CSC は、クラウド内にデプロイされたインフラストラクチャが CSP により提供される、またはデプロイされる中でオープンスタンダードを使用して相互運用性と移植容易性を実現する責任を負う。CSC は、CSP が全てのクラウド機能にアクセスするための共通および／またはオープンインタフェースを公開することを保証しなければならない。

CSC は、API の相互運用性と移植容易性を確保するために、以下のガイドラインを考慮しなければならない：

a. CSP が提供するリソースを監視し、サービスに影響を及ぼす可能性のある停止や変更を認識する。CSC がストレージからのデータ転送を CSP の API に依存する場合、CSC は実装中及び事業継続または 終了計画のテスト活動を通じて、API をテストするものとする。
b. クラウド上のアプリケーションはインターネット上で相互運用され、停止が予測される。CSC は 1 つのコンポーネントの障害が他のコンポーネントに影響を与え、リモートコンポーネントの障害時にシステムデータの整合性を危険にさらす可能性のあるステートフルな依存関係を回避しなければならない。
c. 可能であれば、標準化された構文、オープン API、オープンスタンダード（OCCI など）のプラットフォームコンポーネントを使用する。
d. API のドキュメントが最新かつ正確であることを確認する。
e. API を調査し、相違点がどこにあるかを見極め、新しいプロバイダーに移行する際にアプリケーション処理に必要となる可能性のある変更を計画する。

	f. オープンかつ公開された API を使用することで、コンポーネント間の相互運用性を幅広くサポートし、CSP の変更が必要になった場合にアプリケーションとデータの移行を容易にする。 g. 文書化されていない/独自の API を提供する CSP を避ける。 h. 新しいプロバイダーと互換性がない、または実装されていない管理レベルの機能(例えば、VM イメージ管理、仮想ネットワーク管理、VM 管理、ストレージ管理)、インタフェース、または API が使用されているかどうかを判断する。 i. CSP の選定プロセスにおいて、API のドキュメントとテスト結果をレビューする。 j. 相互運用性、移植容易性、撤退計画の要件を考慮する際、データ転送コストを考慮する。

Control Title	Control ID	Control Specification
セキュアな相互運用性と移植容易性の管理	**IPY-03**	データのインポート、エクスポートの管理のために、暗号論的にセキュアで標準化されたネットワークプロトコルを実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、業界標準のプロトコルと暗号化アルゴリズムを使用して通信を暗号化する責任を負う。CSP は、設計および構成のドキュメントを CSC に提供しなければならない。	**管理策所有権の根拠：** CSC は、API をセキュアに使用またはデプロイし、ポリシー要件や規制または契約上の義務を満たすプロトコルと暗号化アルゴリズムを使用する責任を負う。
実施ガイドライン： CSP は、その管理下にある全ての API について、セキュアな設定、監視、証明書の更新および鍵管理に責任を負う。CSP は、適用される規制上の義務に従わなければならない。 CSP は、CSC に正確な文書を提供し、計画されている変更や更新について伝え、独立したセキュリティ監査結果を公開しなければ	**実施ガイドライン：** クラウド上の機微データを保護する最も重要な方法は暗号化である。クラウドシステムで使用される全ての情報が機密情報に該当するとは限らないし、保護が必要な規制対象に該当するとは限らない。CSC はデータを評価・分類し、データの性質上、暗号化や鍵管理が必要でない場合は、暗号化や鍵管理のための追加作業発生を避けなければならない。

ならない。脆弱性が検出された場合、CSP は CSC に問題を警告し、ステータスの更新を提供し、必要に応じ緩和策についての助言を提供しなければならない。	CSC は、データの改ざんや消失のリスクを低減するために、確立された業界標準のプロトコル（TLS、IPsec など）および暗号化アルゴリズム（AES など）により暗号化（移動中および保存中の両方）し、データのインポートおよびエクスポート時のネットワークトラフィックを保護しなければならない。CSC は、サーバー認証を提供する HTTPS（TLS）で保護されたエンドポイントを介して CSP の API および管理コンソールとの全てのやり取りに TLS を使用しなければならない。 CSC は、データのインポート／エクスポートに暗号化を使用する場合、以下のガイドラインを考慮しなければならない： a. データをクラウドに置く前に暗号化し、不適切なアクセスができないようにする。 b. 業界の精査を受けていない暗号化アルゴリズムおよびセキュアなネットワークプロトコル（または非推奨／セキュアではないバージョン）に依存しない。 c. CSP のセキュリティサービスが、CSP が準拠すべきものと同じ規制上の義務に準拠していることを確認する。 d. ZIP や OpenPGP のような公開された仕様で利用できるような相互運用可能な暗号化手段を用い、プラットフォーム、ストレージシステム、ファイルのある場所に関係なく、データとファイルを直接かつ永続的に保護する。 e. 鍵を保持することで暗号化されたデータの制御を失うことを回避し、たとえその第三者が CSP であっても、第三者に鍵託さないようする。鍵の所有者だけがデータにアクセスできる。 f. 鍵が CSP から提供される場合、CSC は、これらの鍵が何を保護するのか（データまたは他の鍵など）を確実に理解なければならない。 g. CSC は、どの CSP スタッフがどのような条件下で暗号鍵にアクセスできるかを理解しなければならない。 h. CSC は、CSP が提供する保護方法の予期せぬギャップによって侵害が発生した場合の責任と義務を理解しなければならない。 i. パスワードの暗号化が使用される場合、CSC は、パスワードの共有の困難さを回避するため、公開鍵／秘密鍵などのより強力な手段が必要かどうかを判断しなければならない。

Control Title	Control ID	Control Specification

データ移植容易性の契約遵守事項	**IPY-04**	合意には、契約終了時の CSC によるデータアクセスに係る条項を含まなければならない。合意は、下記事項を含む。 a. データ形式 b. データ保存時間の長さ c. CSC が保持し、利用できるデータの範囲 d. データ削除ポリシー

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、サービス契約中および CSC がクラウドサービスの利用を終了する際、データライフサイクル管理に関する情報を提供しなければならない。これには、データ形式、データ保持、データアーカイブおよびデータ削除などが含まれるが、これらに限定されない。 CSP は、CSC のデータとメタデータの回復を支援する情報、および CSP が CSC のデータを削除する方法とタイミングに関する情報を提供する。サービスレベル契約のコンテキストでは、契約終了時のデータ移植容易性に関する規定について両当事者が決定し、合意する必要があるため、管理策の実施責任は「共有」と「依存する」の両方であると判断される。	**管理策所有権の根拠：** CSC は、CSP サプライヤの選定および継続的なデューデリジェンスにおいて、サービス終了の計画およびプロセスを考慮しなければならない。CSC は、データおよびメタデータの形式、保持、サービス終了時のデータ回復手段および関連するコストについて理解しなければならない。
実施ガイドライン： CSP は、CSC がサービス利用を開始および終了する際のデータおよびメタデータの形式と保持についてのタイムラインを文書化しなければならない。一時的なデータまたは保持されないデータは明言されていなければならない。 CSP は、サービス終了時に CSP が環境からデータとメタデータをセキュアに削除できるよう、詳細な手順を公表し、維持しなければならない。 独立した監査は、カスタマーの退出をサポートするプロセスと CSC に提供されるレポートを対象としなければならない。	**実施ガイドライン：** CSC は、終了計画を維持し、テストしなければならない。最低でもデータとメタデータの復旧、アプリケーション内の削除、関連するストレージとバックアップ、暗号化鍵の削除が含まれる。終了計画には、構成、コード、イメージの転移および環境の廃止が含まれる。 CSC は、CSP により提供されるサプライヤの文書と独立監査報告書を確認し、変更を監視して、終了計画が正確であることを確認しなければならない。CSC は、保持要件がポリシーおよび規制または契約上の義務に継続的に一致するようにし、変更があった場合に適切な措置を講じなければならない。

Control Domain IVS

2.12 インフラストラクチャと仮想化のセキュリティ (IVS)

Control Title	Control ID	Control Specification
インフラストラクチャと仮想化のセキュリティポリシーと手順	**IVS-01**	インフラストラクチャセキュリティと仮想化セキュリティのためのポリシーと手順を確立、文書化、承認、周知、実装、評価、維持する。少なくとも年 1 回ポリシーと手順をレビュー、更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、選択したクラウドアーキテクチャによって異なる。IaaS の場合、この管理策は、CSP と CSC の両者で「互いに依存する形で共有」し、それぞれ実施する責任がある。一方、CSP は VM のライフサイクルをサポートするツールやインフラストラクチャに関するポリシーや手順、VM に関するポリシーや手順を提供するが、そのガバナンスは CSC に属する。PaaS と SaaS の場合、この管理策は、「CSP が所有」し、自ら実施する責任がある。CSC はプラットフォームまたはアプリケーションを利用することで VM レイヤーから抽象化され、全てのポリシーと手順は、CSP が責任を有することとなる。	**管理策所有権の根拠：** CSP の「管理策の根拠」が適用される。
実施ガイドライン： **IaaS プロバイダー：** CSP は、サービスを提供するために使用するインフラストラクチャ、仮想マシンおよびクラウドオーケースとレーションツールに関するポリシーと手順を作成する責任を負う。ただし、CSC が IaaS 環境に導入または構築する仮想マシンインタフェースに関するポリシーと手順を作成する責任はない。CSP は、CSC とポリシーや手順の例を共有するか、CSC がこれらのポリシーや手順を構築するのを支援するサービスを提供する。CSP は、CSC がポリシーと手順を適用できるようにするための機能および／または技術（例えば、個々の VM インスタンスを互いに分離するためのネットワークセキュリティ制御機能など）を提供する必	**実施ガイドライン：** **IaaS 利用者：** CSC は、VM のライフサイクル管理とセキュリティに関する全てのポリシーと手順を作成し、管理する責任を負う。CSP がポリシーと手順の例を提供する場合もあるが、導入される環境に関連するよう解釈し調整するのは CSC の責任である。あるいは、CSC は既存のポリシーと手順を IaaS 環境で適用するように修正することもできる。CSP は、このようなポリシーと手順の作成をサポートするサービスを CSC に提供することもできる。CSC は、全てのポリシーと手順書のガバナンスに責任を負い、毎年これらを見直し、適切に更新することが推奨される。CSC は、サービスを提供するために使用される物理的およ

要があるが、これらの機能を使用するためのポリシーと手順を作成するのは CSC に任されている。	び仮想的なインフラストラクチャに関するポリシーと手順については責任を負わない。
PaaS プロバイダー： CSP は、仮想化セキュリティに関連するポリシーと手順を実装し、管理する責任を負う。CSC は、VM 上で実行される開発環境を利用する以外の方法で、PaaS 環境の VM とインタフェースすることは想定されていない。よって、CSP は、VM のライフサイクル、ストレージおよび VM 環境のネットワークセキュリティを管理するためのポリシー管理と実施の枠組みを構築しなければならない。ポリシーと手順は、少なくとも年 1 回見直されるべきで、そのアプローチ（必ずしも具体的なポリシー／手順の詳細ではない）は、CSP の Web サイト、CAIQ および／または独立した監査報告書の一部としてカスタマーと共有される。	**PaaS 利用者：** CSC は、提供されるプラットフォームの一部として仮想マシンを用いる。CSC はこれらの VM のライフサイクルやセキュリティを管理するためのポリシーや手順を作成する必要はなく、CSP の Web サイト、CAIQ および／または独立した監査を参照し、これらがどのように処理されるかを理解することができる。
SaaS プロバイダー： CSP は、仮想化セキュリティに関連するポリシーと手順を実装し、管理する責任を負う。SaaS 環境の VM は単にアプリケーションを実行するだけであることから、CSC は VM とのインタフェースを持たない。よって、CSP は、SaaS アプリケーションの下で実行される VM 環境のライフサイクル、ストレージおよびネットワークセキュリティを管理するためのポリシー管理と実施の枠組みを構築しなければならない。ポリシーと手順は、少なくとも年 1 回見直されるべきで、そのアプローチ（必ずしも具体的なポリシー／手順の詳細ではあり）は、CSP の Web サイト、CAIQ および／または独立した監査報告書の一部としてカスタマーと共有される。	**SaaS 利用者：** CSC は、アプリケーションを利用し、アプリケーションを実行する VM から抽象化されている。CSC は、ＶＭ環境を管理するポリシーと手順には関与せず、CSP の Web サイト、CAIQ および／または独立した監査により、これらがどのように処理されるかを理解することができる。 CSP より提供されるポリシーが適用される。
ポリシーには、以下に関する規定が含まれなければならない（ただし、これに限定されない）： a. 範囲と目的： i. インフラストラクチャと仮想化のセキュリティポリシーの適用範囲と、そのポリシーが根とワーク、オペレーティングシステム、仮想マシンなど、クラウド環境内の全ての関連コンポーネントに適用されることを確認する。 ii. セキュリティ目標は明確であり、CSP に適用される業界標準および記載要件と整合していること。 b. キャパシティ・リソースプランニング：リソースが効率的に割り当てられ、スケーラビリティ要件が満たされるように計画されたキャパシティプランニングの要件と評価 c. ネットワークセキュリティ：ネットワークデバイス、アプリケーション、オペレーティングシステムに対して許容される物理および仮想ネットワーク構成を定義するネットワークセキュリティベースライン。ネットワークのセグメンテーション、アクセス制御、トラフィック管理のガイドラインも定義し、定期的にレビューしなければならない。 d. OS の堅牢化と基本管理：全てのゲスト／ホストのオペレ	

ーティングシステム（OS）、ハイパーバイザ、VM（VM ライフサイクル管理を伴う）のセキュリティベースライン構成（標準化されたハードニング構成と、最新のセキュリティパッチとアップデートを適用する手順を含む）

e. 本番環境と非本番環境：本番環境と非本番環境の分離に関する要求事項（各環境の特定のリスクと要件に合わせた関連するアクセス制限を含む）

f. 分割（Segmentation）と分離（Segregation）：

  i. 異なるカスタマー環境（CSP、CSC、テナント内）を隔離（isolate）し、それらの間の不正アクセスを防止するためのネットワークの物理的および／または論理的な分割と分離の要件

  ii. テナント内アクセス要件を定義し、許可されたユーザーと各テナントのリソースおよびデータへのアクセスを制限する。

g. クラウド環境への移行：セキュアなプロトコルに基づく暗号化を使用したクラウド環境へのデータ移行のためのセキュアなチャネルの確立に関する要件

h. ネットワークアーキテクチャ文書：

  i. ネットワークトポロジ、デバイス構成、データフロー、セキュリティ管理策の詳細を含む、クラウドネットワークアーキテクチャの最新の文書化

  ii. ネットワーク環境の変化を反映するために定期的に見直し、更新すべき文書

i. ネットワークディフェンス：

  i. さまざまな攻撃ベクトルからクラウドインフラストラクチャを守るためのレイヤー防御戦略

  ii. 最新の脅威情報フィード、定期的な脆弱性評価と侵入テストを実施し、ネットワークセキュリティの弱点を特定し是正する。

j. インフラストラクチャと仮想化セキュリティ指標：リースの使用率、ネットワークトラフィックパターン、セキュリティアラートなど、インフラストラクチャと仮想化セキュリティに関連する監視指標と主要業績評価指標（KPI）を定義する。

k. 承認：組織の戦略目標およびリスク許容度との整合性を確保するための承認要件と上級管理職の関与

  i. ポリシーと手順の変更または修正については、承認プロセスを確立しなければならない。

  ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。

l. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進しなければならない。

m. メンテナンスとレビュー：インフラストラクチャと仮想化のセキュリティポリシーと手順を文書化し、少なくとも年１回レビューし、更新し、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映させる。

Control Title	Control ID	Control Specification
容量と資源の計画	**IVS-02**	事業で決定された通りの必要なシステムパフォーマンスを提供するために、資源の可用性、品質、および適切な容量を計画しモニタリングする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の責任は、すべてのクラウドアーキテクチャで同様であり、CSP が責任を所有する。一方、CSC は、特定のサービスまたはリソースのキャパシティを要求することができるが、要求されたシステムパフォーマンスがこれらの要件に従って提供されることを保証するのは CSP の責任である。これは提供されるサービスが IaaS、PaaS、SaaS のいずれであっても同様に適用される。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、CSC に提供されるインフラストラクチャ、プラットフォームまたはアプリケーションの使用状況を評価するためのリソース計画フレームワークを策定し、維持しなければならない。このフレームワークは、定期的に見直され、サービスの必要な成長が CSC の要求を満たすかどうか判断するため、計画、エンジニアリングおよびインフラストラクチャの各チームが使用する。また、CSP は CSC との間で内部運用レベル合意（OLA）および SLA を維持しなければならない。この SLA には、CSP が容量および可用性を提供できない場合のサービス・ペナルティが含まれる場合がある。 内部チームとの間で決定された SLA および CSC との間で約束されている SLA に沿ってリソースのキャパシティプランニングモデルを確立するため、指標を活用し、監視しなければならない。計画チームが必用なリソースのキャパシティ変更に迅速に対応できるよう、定期的なレビューサイクルを採用しなければならない。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、SLA を監視し、サービス容量要件が満たされていることを確認する。これらの SLA は、標準的な CSP SLA である場合もあれば、契約交渉中に合意されたカスタム SLA である場合もある。 これらの SLA を遵守する責任は CSP にある。クラウドモデルによっては、長期的なサービス・キャパシティ・プランニングに役立てるため、CSP が CSC に独自の評価指標を提供するよう求める場合がある。 CSC は、評価指標を活用して CSP が定められた SLA を満たしていることを監視し、確認しなければならない。CSP が提供するサービスレベルが、決定された SLA の範囲外に低下していないことを確認するため、定期的なレビューサイクルを採用しなければならない。 CSP より提供されるポリシーが適用される。

CSPの実施におけるベストプラクティスには以下が含まれる(ただし、これらに限定されない):

a. リソース・プランニングの枠組み:
   i. さまざまなクラウドサービスについて、ビジネス目標、ユーザーの期待、パフォーマンス要件を理解する必要がある。
   ii. コストの最適化、パオフォーマンスの最適化、スケーラビリティの必要性などの要素を考慮し、異なるクラウドサービス間でリソースを割り当てるための戦略を策定する必要がある。
   iii. 過去の使用パターン、将来の成長予測、ピーク時の需要シナリオを分析し、各サービスの適切なリソース容量を決定しなければならない。
   iv. 潜在的なボトルネックを特定し、インフラストラクチャを最適化するため、リソースの利用動向と予測を毎年見直す。

b. リソース監視と警告システム:
   i. 潜在的なボトルネックやリソースの制約を特定するため、CPU、メモリ、ストレージ、ネットワーク帯域幅などのリソース利用指標を継続的に追跡しなければならない。
   ii. VMの異常な作成時間、リソースの急増、または割り当てられたリソースの急激な変化を監視し、不正な活動やリソースを大量に消費する攻撃を検出しなければならない。
   iii. 逸脱や潜在的な問題を事前に特定するため、各重要指標についてベースライン・パフォーマンス・レベル決定しなければならない。
   iv. リソースの使用率がしきい値を超えたり、パフォーマンスが著しく低下した場合に、関連チームに通知するよう自動アラートを設定する。

c. オートスケーリングとリソース最適化技術:
   i. ロードバランシング、仮想マシンの統合、インスタンスの終了などのリソース最適化技術を採用し、リソースの利用率を最大化し、アイドルリソースを最小化しなければならない。
   ii. 自動スケーリング機能を活用し、需要の変動に基づきリソースの容量をリアルタイムで自動的に調整し、最適なパフォーマンスとコスト効率を確保する。

d. 継続的なモニタリングと評価:
   i. モニタリングデータを分析し、傾向、異常、リソース計画と最適化の改善点を特定する。
   ii. リソース計画と戦略は、変化するビジネス要件、技術の進歩、市場の変動に応じて適応されなければならない。
   iii. リソース計画を定期的に見直し、進化するビジネスニーズ、使用状況、キャパシティパターン、全体的

なパフォーマンス要件との整合性を確認する。	

Control Title	Control ID	Control Specification
ネットワークセキュリティ	**IVS-03**	事業によって正当化される形態で認証、認可された接続に制限するように、環境間のコミュニケーションをモニタリング、暗号化、制限する。少なくとも年 1 回構成をレビューし、許可された全てのサービス、プロトコル、ポート、補完的コントロールの文書による正当性を文書化し、構成を支持する。

Control Ownership by Service Model		
IaaS	PaaS	SaaS
Shared (Dependent)	Shared (Dependent)	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、選択したクラウドアーキテクチャによって異なる。IaaS と PaaS の場合、これは「依存した形で共有」する管理策である。それは、CSP がインフラストラクチャ、プラットフォーム、オーケストレーションレベルの通信セキュリティに責任を負う一方、CSC は、提供されたインフラストラクチャ／プラットフォームより上位の通信セキュリティまたは異なる環境同士を接続する場合の通信セキュリティに責任を負う。SaaS の場合、これは CSP が所有権を持つ管理策である。通信セキュリティは、提供されるソフトウェアアプリケーションの標準的な構成要素であるべきであり、CSC が SaaS サービスとやりとりするためのセキュアな環境を提供する。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **IaaS プロバイダー：** CSP は、オーケストレーションレイヤ（クラウド管理プラットフォーム）と CSC、オーケストレーションレイヤとプロビジョニングされたインフラストラクチャ間の通信を監視し、暗号化し、制限する責任を負う。これはセキュアなプロトコル（TLS／HTTPS）、セキュアな API、境界セキュリティ制御および潜在的な攻撃ベクトルを識別するために CSP によりプロビジョニングされたセキュリティ監視機能を用いて実施しなければならない。IaaS 環境を保護するセキュリティアーキテクチャは、十分に文書化され、管理された変更管理プロセスに従わなければならない。構成と関連ドキュメントは、改善すべきドメインを特定し	**実施ガイドライン：** **IaaS 利用者：** CSC は、インフラストラクチャサービス上にデプロイされるコンポーネント間の通信を監視し、暗号化し、制限する責任を負う。これには移動中のデータを保護するためのセキュアなプロトコルの適切な使用を含む通信セキュリティアーキテクチャの設計が含まれる。CSC は、クラウドネイティブまたは既存の SOC プラットフォームへの統合によりセキュリティ監視機能を実装し、IaaS ワークロード環境のログを統合し、不審なイベントを識別しなければならない。CSC は、リソースへの不要なアクセスや露出を防止し、環境内部での横方向の動きと環境外部からの悪意ある攻撃者の両方からワークロードを保

たり、新たな攻撃ベクトルに対処するためにセキュリティポリシーを適応させたりするため、少なくとも年 1 回は定期的にレビューしなければならない。CSP は、CSC が独自の通信セキュリティアーキテクチャを構築および設計できるようツール（サービスの一部として、またはマーケットプレイスを通じて）を提供しなければならないが、適切なセキュリティ制御をデプロイおよび管理するのは CSC の責任となる。	護するために適切なネットワークレベルの制御が行われていることを確認しなければならない。通信セキュリティに関する構成と関連文書は、改善すべきドメインを特定したり、新たな攻撃ベクトルに対処するためにセキュリティポリシーを適応させたりするため、少なくとも年 1 回は定期的にレビューしなければならない。環境の変更管理は、適切に管理されたプロセスによって定義されなければならない。
PaaS プロバイダー： CSP は、CSC にサービスとして提供されるインフラストラクチャとプラットフォーム全体の通信を監視、暗号化および制御する責任を負う。これには、CSC がプラットフォームサービスにアクセスできるようにするためのセキュアなプロトコル（TLS／HTTPS）とセキュアな API の使用および境界セキュリティ制御と PaaS 環境の外部からの悪意のある可能性のあるアクティビティを識別するための監視機能が含まれる。セキュリティモデルは CSP によって十分に文書化され、定期的にレビューされなければならない。また、CSC が対話する API は、CSC がサービスとセキュアに対話する方法を理解できるよう文書化され、外部に共有されなければならない。CSP は、CSC によってデプロイされるアプリケーションまたは機能のセキュリティについては責任を負わないが、CSC をサポートするためのツールを提供することはできる。	**PaaS 利用者：** CSC は、プラットフォームサービス上のコンポ—ネット間の通信を監視、暗号化、制限する責任を負う。これには、セキュアなプロトコル（TLS／SSL）およびセキュアな API を採用し、環境へのアクセスを暗号化または保護することが含まれる。プラットフォーム上で開発されるアプリケーションに関連するセキュリティモデルは、CSC のセキュリティモデルに影響を及ぼす可能性のある CSP 提供の API またはインフラストラクチャへの変更を考慮した上で、CSC により十分に文書化され、定期的にレビューされなければなりません。
SaaS プロバイダー： CSP は CSC に提供されるアプリケーションに至るまで、インフラストラクチャの全てのレイヤーを通じた通信を監視、暗号化および制御する責任を負う。CSP は、移動中のデータを保護し、環境への不正アクセスを防止するための認証および認可のメカニズムを提供し、CSC 環境間でのラテラルムーブメントを防止するためのセキュリティ制御を実装する環境を CSC に提供しなければならない。セキュリティモデルの構成は、成熟した変更管理プロセスを導入し、社内で十分に文書化しなければならない。さらに CSP は、サービスとして提供されるソフトウェアのセキュリティに関して十分な情報に基づいた決定を下せるよう、セキュリティ制御の概要を CSC と共有することが推奨される。 クラウドネットワークセキュリティ実装のベストプラクティスには以下が含まれる（ただし、これらに限定されない）： a. ネットワーク設計の原則： i. セキュリティ、リソースのスケーラビリティ、パフォーマンス、法規制への準拠など、ネットワーク設計の指針となる原則を十分に理解し、明確にしておくべきである。 ii. クラウドネットワーク環境間の通信に認可されたサービス、プロトコル、ポートのイベントリを確立し、維持すること。 iii. ネットワークセキュリティベースラインは、変更管	**SaaS 利用者：** CSC は、ソフトウェアスタック全体をサービスとして利用するため、通信セキュリティや通信監視に関連するセキュリティ制御については責任を負わない。ただし、CSC は、サービスとして提供されるソフトウェアのセキュリティについて十分な情報に基づいた決定を下すため、CSP が提供するドキュメントを確認しなければならない。

理フレームワーク（CCC-06 を参照）の一部として実装され、ネットワーク仮想化およびネットワークセキュリティ構成のパラメータを包含するとともに、逸脱および潜在的脅威を検知するための通常のネットワークトラフィックパターンを定義する。

iv. ネットワークのセグメンテーション、アクセス制御、トラフィック管理に関するガイドラインを定めなければならない。

b. ネットワーク通信のモニタリング：

i. ネットワークトラフィックの特定と分析を実施し、情報データの流れの経路（起点、終点、センシティブなネットワークドメインを通過する経路を含む）に焦点を当てる。

ii. ネットワークトラフィックの監視・分析ツールは、以下の機能を備えたものを導入すべきである：

・パケットキャプチャと解析
・フローモニタリング
・異常検知と行動分析
・ユーザーのアクティビティ追跡

iii. 監視ツールは、ネットワークトラフィックの集中ロギングと分析のために SIEM システムと統合されるべきである

c. ネットワーク通信の暗号化：ネットワーク通信チャネルを経由するデータのセキュリティを確保するには、エンドツーエンドの暗号化を実装する必要がある。

i. ネットワーク機器は、特定のプロトコルとポートに対して強力な暗号化を強制するように設定すべきである。

ii. 分離されたネットワークセグメント間のセキュアな通信には、VPN トンネルを利用すべきである。

d. ネットワーク通信の制限：

i. アクセス制御は、ファイアウォール、アクセス制御リスト（ACL）、VPN、IAM システムを使用して定義し、実施しなければならない。

ii. ファイアウォールは、クラウドネットワークアーキテクチャ内の重要なポイントに導入し、内部と外部のネットワーク接続間のゲートウェイとして機能し、事前に定義されたセキュリティルールに基づいて受信トラフィックと送信トラフィックをフィルタリングしなければならない。

iii. ファイアウォールは、IP アドレス範囲、プロトコル、ポートを含むきめ細かなアクセス制御ルールを設定しなければならない。

iv. クラウド環境で Web サーバーやメールサーバのような一般にアクセス可能なサービスが必要な場合は、DMZ（Demilitarized Zone）を設定し、機密性の高い内部リソースを外部の潜在的脅威から隔離するための緩衝地帯として機能させること。

e. ゼロトラストネットワークアクセス（ZTNA）：

クラウドネットワークのアクセス制御にゼロトラストアプローチを採用し、検証されるまではユーザーやネットワークデバイスは本質的に信頼されないと仮定し、ユーザーID、デバイスのポスチャ、コンテキストに基づいて動的にアクセス制御を実施する。 f. ネットワーク設定の見直し： i. 許可されたネットワークサービス、プロトコル、ポートおよび補完的管理策、ネットワークセキュリティとアクセス制御の構成、暗号化実施のインベントリは、少なくとも年1回はレビューし、更新されなければならない。 ii. 手当の根拠は、ビジネスニーズとリスク評価に基づいて十分に正当化されなければならない。	
コンテナ固有の実装ガイドライン： 業務上正当なネットワーク通信は許可されるべきであり、暗号化され、承認される必要がある。逆に不当なネットワーク通信は許可されるべきではない。 コンテナアプリケーション対応ネットワークモニタリングツールは、以下のような目的で提供されなければならない： コンテナネットワークサーフェス：インバウンドポートとプロセスバインディングの両方を含む、適切なコンテナネットワークサーフェスの自動決定 コンテナのトラフィックフロー：ワイヤートラフィックとカプセル化されたトラフィックの両方で、コンテナと他のネットワークエンティティ間のトラフィックフローを検出する。 ネットワーク異常検知：組織のネットワーク内での予期せぬトラフィックフロー、ポートスキャン、潜在的に危険な宛先へのアウトバウンドアクセスなど、ネットワークの異常を検知する。 悪意のあるコンテンツの検出：コンテナ環境に導入された無効または予期しない悪意のあるプロセスやデータの検出	**コンテナ固有の実装ガイドライン：** CSPの「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
OS要塞化とベース管理策	**IVS-04**	ホストOSとゲストOS、ハイパーバイザまたはインフラストラクチャの管理プレーンそれぞれのベストプラクティスに従って、セキュリティベースラインの一部として、技術的管理策のサポートにより要塞化する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Independent)	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、3 つのクラウドサービスモデルにより CSP と CSC の間の責任が異なる。IaaS の場合、CSP がホスト（OS および／またはハイパーバイザ）の要塞化に責任を負い、CSC がゲスト VM と OS の要塞化に責任を負うため、ホストとゲストの OS の要塞化については、CSP と CSC の間で分担および独立した実施責任がある。PaaS と SaaS の場合、OS、ハイパーバイザおよび基盤となるインフラストラクチャの要塞化は CSC のクラウドスタックの一部ではなく、CSC はそれらのセキュアな実装をコントロールすることはできないため、実施責任は CSP のみにある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **IaaS プロバイダー：** CSP は、カスタマーの仮想マシンをサポートするハードウェアのプロビジョニングに責任を負う。このプロビジョニングには、ハイパーバイザ、ホスト OS、ファームウェアの要塞化とアップデートの維持およびハードウェアに根差した信頼性評価を含む機密コンピューティングの利用並びに検証済みの信頼できるサプライヤを介して入手した TEE（Trusted Execution Environments）と TPM（Trusted Platform Modules）および、その他の信頼され、保証された機器の利用が含まれる。CSP は、ホストインフラストラクチャの上にインストールされた OS のアップデーについて責任を負わない。	**実施ガイドライン：** **IaaS 利用者：** CSC は、攻撃対象ドメインを減らすため、デプロイされたオペレーティングシステムの要塞化とアップデートを維持する責任を負う。これは、パッチ管理システムによって達成される。CSC は、ホスト OS やハイパーバイザのアップデートや要塞化には責任を負わない。CSC は、アンチウイルス、ファイアウォール、監視、ロギング、コンフィデンシャルコンピューティングなどのセキュリティツールを利用することで、ゲスト OS に要塞化されたベースラインを提供しなければならない。ゲスト OS の要塞化は、認知された業界標準にあわせなければならない。
PaaS プロバイダー： CSP は、インフラストラクチャプレーン全体にわたる全てのシステム要塞化およびゲスト OS のパッチ適用を担い、クライアントの要件またはベストプラクティスの定義に従いこれら実施する必要があるが、アプリケーションレベルのパッチ適用については責任を負わない。	**PaaS 利用者：** CSC は、自社のアプリケーションとインストールされたソフトウェアのアップデートを維持する責任を負う。また、アプリケーションとアプリケーションに含まれる保存データの監視、ロギング、保護など、追加のセキュリティ強化制御も担う。CSC は、アクセスを必要とするユーザーに対する承認とアクセスを維持し、正当化する責任も負う。
SaaS プロバイダー： CSP は、アプリケーションレベルの要件を含め、システムパッチ適用の全ての要素に責任を負う。 CSP がホスト（ハイパーバイザ）／ゲストの更新およびその他のシステムのパッチ適用を担っている場合は、アップデートをデプロイする前に適切なテスト方法を導入しなければならない。アップデートは契約上の合意に応じて適切な時間枠で導入しな	**SaaS 利用者：** CSC は、適切な制御が実装あれ、要件に準拠し、リスク標準に従ってソフトウェアが使用されていることを確認しなければならない。CSC は、サービスの更新やベースラインについては責任を負わない。この管理策の一環として、統合プロバイダーやサービスへのアクセスに使用されるエンドポイントデバイスなどの CSC タッチポイントを強化し、企業ポリシーまたは適切な業界標準にしがって管理することが推奨される。

ければなり。

クラウドプラットフォームの要塞化のための実装のベストプラクティスには以下が含まれる(ただし、これらに限定されない):

a. ホスト／ゲスト OS、ハイパーバイザ、VM、管理策プレーンの要塞化：
   i. 全てのプラットフォームで一貫性を確保するため、業界ベンダーとベンチマークを使用したセキュアな構成ベースラインを作成し、活用すべきである。
   ii. ベースラインに従って事前に設定されたセキュアテンプレートを使用し、必要なシステムサービス／プロセスのみを有効にする（不要なポート、プロトコル、ネットワークサービスは無効化または削除し、攻撃対象ドメインを減らす)。
   iii. ソフトウェア（OS、ハイパーバイザ、VM、アプリケーション）は、最新のセキュリティパッチを適用して最新の状態に保つ。
   iv. ハイパーバイザ／VM／OS 管理インタフェースへのアクセスには、強力な認証(複雑なパスワードやMFAなど）を設定する必要がある。
   v. ファイアウォール、アンチマルウェア、システムログなどのセキュリティ機能を有効にする。
   vi. 必要な機能のみが有効になっていることを確認するために、構成は構成ベースラインに対して定期的にレビューされ、更新されるべきである。
   vii. 機密性の高い CSC ワークロードの場合：
      - ハイバーバイザーの脆弱性が悪用される可能性を避けるために、専用のシングルテナントまたはベアメタルハイパーバイザインスタンスを使用すべきである。
      - セキュリティ強化のため、従来の仮想マシン（VM)をコンフィデンシャル VM に置き換えるべきである。
      - セキュリティ強化のために、セキュアブートと仮想トラステッドプラットフォームモジュール（vTPM）を利用すべきである。
      - ハイパーバイザ／OS／VM は、厳格にセキュリティテストされたものを選択する（コモンクライテリア（CC）の保護プロファイル（PP）に対して評価し、評価保護レベル（EAL）を割り当てる)。

仮想マシンライフライクル管理固有の実施ガイドライン：

a. 生成：
   i. セキュアな VM テンプレートを使用する必要がある。このテンプレートには、要塞化された OS 構成、パッチ適用スケジュール、アクセス制御などのセキュリティ設定があらかじめ設定されている。
   ii. VM イメージは、CSC にプロビジョニングする前に脆

弱性をスキャンしなければならない。

iii. 攻撃対象ドメインを減らすため、VM イメージから不要なアプリケーション、サービス、ドライバを削除すべきである。

iv. 全ての VM の詳細なインベントリを維持し、作成し、デプロイし、ステータスを追跡すること。

v. VM がセキュリティ要件と規制要件を満たしていることを確認するため、コンプライアンスチェックを実施しなければならない。

b. デプロイ：

i. VM の不正なデプロイを防止するため、プロビジョニング・管理策を導入すべきである。

ii. ネットワークのセグメンテーションは、VM 同士や他のネットワークから隔離するために使用されるべきである。

iii. クラウド IAM アクセス・管理策・ポリシーに基づいて、VM への ID アクセスを制限するアクセス・管理策を実装しなければならない。

iv. 不審な活動や潜在的なセキュリティ侵害を検知するために監視・警告システムを導入・設定する。

v. VM に対する変更を管理・追跡するために、変更管理プロセスを導入しなければならない（CCC ドメインを参照）。

c. 運用：

i. 脆弱性に対処し、既知のエクスプロイトを防ぐために、セキュリティパッチとアップデートを VM に定期的に適用しなければならない。

ii. 脆弱性スキャンを定期的に実施し、セキュリティ上の弱点を特定し、是正する。

iii. 構成管理ツールは、VM の一貫したセキュアな構成を強制するために使用されるべきである。

iv. VM は、リソースの使用状況、セキュリティベント、潜在的な異常を継続的に監視しなければならない。

v. 変更とイベントを追跡するために、VM アクティビティログと監査を有効にすべきである。

d. 保守：

i. VM のデータを損失や破損から保護するため、バックアップとリカバリ戦略を実施しなければならない。

ii. VM の保守タスクは、変更管理プロセスに従わなければならない。

iii. VM に加えた変更は、本番環境にデプロイする前にテストし、検証しなければならない。

iv. VM の構成、保守手順、セキュリティポリシーの文書化を維持する。

e. 廃止：

i. 機微データを不正アクセスから保護するため、VM ディスクは廃止前に暗号化されるべきである。

ii. VM ディスクはデータの復元を防ぐため、セキュア

に破棄または消去すること。 iii. 廃止された VM は、インベントリとトラッキングシステムから削除され、適切な権限をかくするために廃止プロセスが文書化されなければならない。 iv. 監査証跡は、廃止活動とデータ廃棄手順を記録するために維持されるべきである。	
コンテナ固有の実施ガイドライン： 技術的管理策は、ビジネスニーズを満たすために必要なポート、プロトコルおよびサービスのみが提供されるような状況を支援する必要がある。このような管理策は、共通のベンチマークに基づく必要があり。 CSP は、マルウェア対策、ファイル整合性監視およびロギングを実装し、コンフィデンシャルコンピューティング（CC）および仮想トラステッドプラットフォームモジュール（vTPM）でハードウェアルートの信頼を活用しなければならない。 組織は可能な限り、他の全てのサービスと機能を無効にし、読み取り専用ファイルシステムやその他の強化手法を使用して攻撃対象ドメインを削減し、最小限のコンテナ固有のホスト OS を使用しなければならない。 コンテナを保護するための以下のようなベストプラクティスも推奨される： a. 専用コンテナホスト：コンテナを実行するホストは、コンテナのみを実行し、コンテナ以外の他のアプリケーション（Web サーバーやデータベースなど）を実行してはならない。 b. コンテナホストのパッチ管理：コンテナを実行するホストは、継続的に脆弱性をスキャンし、迅速に更新する必要がある。 c. 要塞化されたコンテナホスト：ホスト OS は不要なシステムサービスを実行しない。 d. コンテナホストへのアクセス：コンテナホストへのアクセスは知る必要性と最小特権の原則に基づくべきである。 e. コンテナセキュリティ監視：ファイルの完全性監視とホストの侵入検知をコンテナに活用すべきである。 f. CC の保護：該当する場合、ホストは機密コンピューティングハードウェアにより測定され、信頼性を検証するために証明されなければならない。これにより、OS が実行される前であっても、ファームウェア、CPU シリコンからのブートコードを含むホストが依存するプラットフォームが測定され証明されていることを検証できる。	**コンテナ固有の実装ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
本番環境と非本番環境	**IVS-05**	本番環境と非本番環境を分離する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC の双方がこの管理策の実施に責任を負うが、互いに依存しない形で実施する。本番環境と非本番環境を分離し、非本番環境の変更に影響されない安定した本番環境を確保し、テストデータが本番環境に入らないようにする（同様に本番データが非本番環境に入らないようにする）ことは、標準的なベストプラクティスである。これは、提供されるサービスが IaaS、PaaS または SaaS のいずれであっても、CSP と CSC の双方に等しく適用される。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、非本番環境における潜在的な脅威から本番システムを保護するため、本番環境から完全に分離された非本番環境を維持しなければならない。非本番環境は、適切なセキュリティコントロール管理を用い本番環境から論理的および物理的に分離されたアーキテクチャ的に類似した環境で実行されなければならない。 非本番環境は、本番前のリリースをテストするために使用しなければならず、実際の CSC／ビジネスデータではなく、テストデータのみで使用しなければならない。 CSP 実施におけるベストプラクティスには以下のものが含まれる（ただし、これらに限定されるものではない）： a. アカウントとアクセス許可の分離： i. アクセス制御ルールと権限レベルを厳密に定義し、環境ごとに異なる IAM ポリシーが存在し、実装されるべきである。 ii. アクセス許可は、各環境に関連する特定の役割とタスクに基づいて付与され、必要最小限の特権が提供されるようにしなければならない。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実装ガイドライン」が適用される。

iii. 本番環境と非本番環境にアクセスし、管理するための別個のアカウントを作成すべきである。

b. ネットワークの論理的／物理的分離：

i. 本番環境と非本番環境は論理的に分離すべきである（仮想ネットワーク（VNet）、仮想プライベートネットワーク（VPC）、クラウドネットワークセキュリティグループ（NSG）の使用など）。

ii. 各環境には独自の VNet があり、独自のネットワークセキュリティグループ（NSG）内にカプセル化され、環境間の偶発的または意図的な通信を防がなければならない。

iii. 物理的な分離も考慮すべきである（例えば、別々のデータセンター、ラックあるいは物理的に異なる場所を使用するなど）。

iv. 本番環境と非本番環境を互いに隔離するために、ネットワークセグメンテーションツールを利用すべきである（例えば、環境間を不正なトラフィックが通過しないよう、個別のサブネット、ファイアウォール、アクセス制御リスト（ACL）を使用するなど）。

c. 開発とテストのためのサンドボックス環境：

i. 開発およびテスト用に特別に設計されたサンドボックス環境を構築すべきである。

ii. サンドボックスは、偶発的または悪意のあるコードのデプロイが重要なデータやシステムに影響を与えないよう本番システムから隔離されなければならない。

iii. 本番環境へのデプロイに先立って、非本番環境の機能性とセキュリティを検証するために、自動テスト手順を導入すべきである。

d. リソース管理の分離：

i. 誤った環境での誤ったプロビジョニング、設定変更、削除を防ぐため、環境ごとに個別のリソース管理ツールを導入すべきである。

ii. 本番データと非本番データの偶発的な混在を防ぐため、データ分離戦略を実施すべきである（例えば、異なるストレージソリューションの使用、データマスキング技術、データリポジトリ内でのデータ分離ツールの導入など）。

iii. 本番環境と非本番環境で異なるバージョン管理システムを使用し、リリース間の競合を回避し、テスト済みで承認済みの変更のみが本番環境にデプロイされるようにすること。

iv. 本番環境と非本番環境のリソースには、混乱や誤った環境への偶発的な変更を避けるため、異なる命名規則を採用すべきである。

e. 文書化：本番環境と非本番環境のそれぞれについて、分離ポリシー、アクセス制御、ネットワーク構成、テスト手順を概説する文書を作成、維持すること。

f. アップデートの管理：パッチとアップデートは、まず非本

番環境に適用し、テストに成功した後、本番環境に適用する。 g. 継続的な監視と評価：本番環境と非本番環境の双方について継続的な監視と評価を実施し、十分なセキュリティが確保され、セキュリティ標準に合致していることを確認する（例えば、システムログ、ネットワークトラフィック、脆弱性スキャン、ユーザー活動を監視し、疑わしい行動や潜在的なセキュリティ侵害を検出するなど）。	

Control Title	Control ID	Control Specification
分割と分離	**IVS-06**	CSP と CSC（テナント）のユーザーアクセス、およびテナント間のアクセスが、各々のテナントから適切に分割、分離、モニタリング、制限されるように、アプリケーションとインフラストラクチャを設計、開発、デプロイ、構成する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： IaaS と PaaS の場合、この管理策は「依存した形で共有」である。SaaS の場合、この管理策は、「CSP が所有」である。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： ネットワークおよびシステム制御は、複数の CSC 環境内および CSP と CSC 環境間で CSC を隔離（分割かつ分離）するよう設計しデプロイしなければならない。	
IaaS プロバイダー： CSP は、CSP および CSC ユーザーアクセスと CSC ないアクセスが適切に分割され、監視され、他の CSC から制限されるよう、ネットワーク、ホストインフラストラクチャ、仮想化プラットフォームの設計、開発、デプロイ、構成を担う。	**実施ガイドライン：** **IaaS 利用者：** CSC は、CSP および CSC のユーザーアクセスと CSC 内アクセスが適切に分割かつ分離され、他の CSC から監視および制限されるよう、仮想マシン、オペレーティングシステム、プラットフォームソフトウェア、アプリケーションおよびデータを設計、開発、デプロイおよび構成する責任を負う。
PaaS プロバイダー：	**PaaS 利用者一：**

CSP は、CSP および CSC のユーザーアクセスと CSC 内アクセスが適切に分割され、他の CSC から分離、監視および監視されるよう、ネットワーク、ホストインフラストラクチャ、仮想化プラットフォーム、仮想マシン、オペレーティングシステム、プラットフォームを設計、開発、デプロイ、構成する責任を負う。	CSC は、CSP および CSC のユーザーアクセスと CSC 内アクセスが適切に分割され、他の CSC から分離、監視、制限されるよう、インストールされたソフトウェア、アプリケーションおよびデータを設計、開発、デプロイおよび構成する責任を負う。
SaaS プロバイダー： CSP は、ネットワーク、ホストインフラストラクチャ、仮想化プラットフォーム、仮想マシン、オペレーティングシステム、プラットフォームソフトウェアおよびアプリケーションの設計、開発、デプロイ、構成を担います。CSP および CSC のユーザーアクセスと CSP 内アクセスは、適切に分割され、他の CSCI から分離、監視および制限される。	**SaaS 利用者：** SaaS 利用者は、CSP が適切な CSC 間の保護と隔離を実施していること、および利用者環境が論理的に分割され、他の CSP ユーザーや利用者が自分に割り当てられていないリソースにアクセスできないようにしていることを確認しなければならない。
全てのサービスモデルに適用： 実施上のベストプラクティスには以下が含まれる（ただし、これらに限定されるものではない）： a. 分割の定義：ビジネス上重要な資産や個人データ、機密性の高いユーザーデータおよびセッションの「完全な分離」から「部分的な論理的分離」までの範囲を含む分割の定義を明確に定め、理解しなければならない。 b. マルチテナントインフラストラクチャの隔離： マルチテナント環境は、ネットワーク分割、仮想マシン、コンテナ化などのさまざまな分離技術を用い、各テナントに隔離されたコンパートメントを作成し、異なるテナント間の不正アクセスを防ぐため、物理的および論理的に分離し、隔離しなければならない。 c. ネットワーク分割： i. テナント内およびテナント間のネットワークトラフィックを制限し、テナント間の不正アクセスを防止するため、仮想プライベートクラウド（VPC）、サブネット、セキュリティグループなど、さまざまなレベルでネットワーク分割を実施しなければならない。 ii. 仮想化ネットワーク（VNet）は、各テナントにプライベートで隔離されたネットワークを作成し、テナントデータとアプリケーションを区分し、他のテナント環境からの不正アクセスを防ぐために利用しなければならない。ネットワークセキュリティグループ（NSG）を実装し、各 VNet 内できめ細かなアクセス制御を実施する。 d. アクセスの分離： i. クラウドリソースへのアクセスを管理し、クラウドリソースへのアクセスを制御し、分離を実施する。RBAC、MFA、および PoLP を使用して、ユーザーの役割と責任に基づいてアクセスを制限する。 ii. クラウドリソースへの CSP と CSC のユーザーアクセスは分離されるべきである。CSP にはインフラコンポーネントと管理ツールへのアクセスを提供し、	**全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

CSC にはテナントのリソースへのアクセスを制限する。 iii. CSC が CSP のアプリケーションを侵害して他の CSC の情報に不正アクセスできないよう、アプリケーションレイヤーにおいて CSC 間横断的な保護を実施し、CSC ユーザーアクセスと CSC 内アクセスを適切に区分し、他の CSC から分離、監視、制限する。 e. アクセスの監視とレビュー：潜在的なセキュリティ侵害や不正アクセスの試みを可視化するため、CSP およびテナントのアクセス活動は継続的に監視およびレビューされるものとする。	

Control Title	Control ID	Control Specification
クラウド環境への移行	**IVS-07**	サーバー、サービス、アプリケーション、データをクラウド環境に移行する際、セキュアで暗号化されたコミュニケーションチャネルを使用する。これらのチャンネルは最新の承認されたプロトコルだけを含まなければならない。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、サービスモデルに関係なく「依存した形で共有」である。CSP と CSC の双方が実施／運用しなければならない。 CSP と CSC は、境界内外のサーバー、サービス、アプリケーションまたはデータを移行する際に、最新の承認済みプロトコル（FIPS など）を含む、セキュアで暗号化された通信チャネルを使用しなければならない。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** サーバー、サービス、アプリケーションまたはデータをクラウド環境に移行する場合、CSP は機微情報を保護するためにセキュアで暗号化された通信チャネルを実装しなければならない。これにより、移行プロセス全体とその後のクラウドでの操作中もデータが保護された状態が保たれる。	**実施ガイドライン：** CSP の「実装ガイドライン」が適用される。

CSP は、以下の実装ベストプラクティスを遵守しなければならない：

a. エンドツーエンドのデータ暗号化：
   i. データは、保存から送信、処理に至るまでライフサイクルの全ての段階で暗号化されなければならない。
   ii. クラウド内のディスクや永続的ストレージデバイスに保存されたデータを保護するため、保存中のデータの暗号化を採用すべきである。
   iii. クラウドコンポーネント間およびクライアントとクラウド間で送信されるデータを保護するため、データ移動中の暗号化を利用すべきである。

b. セキュアトランスポートプロトコル：
   i. クラウドインフラストラクチャコンポーネント間およびクライアントとクラウド間の通信には、さまざまな OSI レイヤーにおいて、最新の業界承認済みの暗号化プロトコルを活用すべきである（例えば、HTTPS／TLS、FTPS（トランスポートレイヤー）、IPSEC（ネットワークレイヤ）、セキュアなファイルテインレイヤープロトコル SFTP、SCP over SSH（アプリケーションレイヤー）などを利用）。
   ii. これらのプロトコルは強力な暗号スイートと認証メカニズム（CEK ドメインを参照）で構成し、企業のセキュリティ標準と業界のベストプラクティスに従って使用しなければならない。

c. VPN 技術：
   i. オンプレミスのネットワークとクラウド環境の間にセキュアで暗号化されたトンネルを確立するために VPN を導入すべきである。
   ii. IPSec や TLS のような VPN プロトコルは、強力な暗号化と認証メカニズムとともに採用されるべきである。

d. API セキュリティ：
   移行プロセスで API を使用する場合、適切な認証、認可、データ検証の仕組みで保護する必要がある。

e. 認証メカニズム：
   MFA は、データ転送に参加するユーザーとシステムの身元を確認するために利用されるべきである。

f. データ暴露の制限：
   i. 機微データの転送量は最小限にとどめ、必要なものだけを公開しなければならない。
   ii. 機微データについては、移行時にデータのマスキングや難読化技術を使用することで、データ漏えいのリスクをさらに低減することを検討すべきである。

g. 移行の監視とロギング：
   i. 全てのデータ転送は、移行プロセス中に継続的な監視が行われ、ログに記録されるべきである。
   ii. 移行プロセスに関与するサードパーティーベンダ

ーのセキュリティ慣行を評価し、監視すべきである。	

Control Title	Control ID	Control Specification
ネットワークアーキテクチャの文書化	**IVS-08**	高リスク環境を特定し文書化する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： IaaS と PaaS の CSP の場合、この管理策は「依存した形で共有」である。CSC は、CSC が管理するワークロード内の高リスク環境を特定して文書化する責任があるが、CSC 間の隔離と分離の技術的機能の提供は CSP に依存する。 SaaS CSP の場合、SaaS アプリケーション内の高リスク環境を特定して文書化する責任がある。データフロー図では、高リスク環境を明確に特定し、データ分類、信頼レベルまたはコンプライアンスと規制要件が異なるゾーン間のデータフローを明確に定義しなければならない。	**管理策所有権の根拠：** これは、IaaS と PaaS において CSP と CSC の双方に対する「依存した形の共有」となる管理策である。CSC は、CSC が管理するワークロード内の高リスク環境を特定して文書化する責任があるが、CSC 間の隔離と分離の技術的機能の提供は CSP に依存する。 この管理策は SaaS 利用者には適用されない。これは CSP が所有する管理策となる。
実施ガイドライン： CSP は、クラウドインフラストラクチャのセキュアで効率的かつスケーラブルな運用を確保するため、ネットワークアーキテクチャを文書化しなければならない。この文書は、詳細かつ一貫性を保ち、ネットワークエンジニア、セキュリティ専門家、カスタマーサポートチームなど、全ての関係者が容易にアクセスできるものでなければならない。	
IaaS プロバイダー： CSP は、ネットワーク、ホストインフラストラクチャ、仮想化プラットフォーム内の高リスク環境を特定し、文書化する責任を負う。	**実施ガイドライン：** **IaaS 利用者：** CSC は、デプロイされた仮想マシン、オペレーティングシステム、プラットフォームソフトウェア、アプリケーションおよびデータ内の高リスク環境を特定し、文書化する責任を負う。

PaaS プロバイダー： CSP は、ネットワーク、ホストインフラストラクチャ、仮想化プラットフォーム、仮想マシン、オペレーティングシステムおよびプラットフォームソフトウェア内の高リスク環境を特定し、文書化する責任を負う。	**PaaS 利用者：** CSC は、インストールされたソフトウェア、アプリケーション、データ内の高リスク環境を特定し、文書化する責任を負う。
SaaS プロバイダー： CSP は、ネットワーク、ホストインフラストラクチャ、仮想化プラットフォーム、仮想マシン、オペレーティングシステム、プラットフォームソフトウェアおよびアプリケーション内の高リスク環境を特定し、文書化する責任を負う。CSP は、要求に応じ、文書の複製を CSC に提供しなければならない。	**SaaS 利用者：** これは CSP が所有する管理策であり該当しない。CSC は、CSP が高リスク環境を特定し、文書化していることを確認しなければならない。
全てのサービスモデルに適用： ネットワークアーキテクチャの文書化に関する実装のベストプラクティスには以下が含まれる（ただし、これらに限定はされない）： a. 文書化の範囲と目的： ネットワークアーキテクチャ図のスコープを確立しなければならない。例えば、ネットワークの種類、物理コンポーネント、論理コンポーネント、サービスおよび対象となるアプリケーションおよび文書化の具体的な目的などである。 b. 用語と定義の標準化： ネットワーク図、アーキテクチャモデル、その他の文書化要素にまでおよぶ一貫性のある標準化された用語と定義のセットを採用する。 c. 高リスク環境の特 i. ネットワークトポロジの潜在的な脆弱性と高リスクドメインを特定するため、徹底的なリスク評価を実施しなければならない。 ii. 攻撃を受けやすく、侵害された場合に最も大きな被害をもたらす、大量のデータや機密データ転送を伴うネットワークセグメントやトラフィックフローなどの高リスクネットワークドメインは、優先順位をつけ、より強力なセキュリティ対策を適用しなければならない。 d. ネットワーク図とアーキテクチャモデル： i. 物理および仮想ネットワークコンポーネントとそれらに対応するセキュリティゾーンの説明、ハイパーバイザ、信頼できる実行環境、各ホスト上のワークロードとそれらの相互接続および通信パス（トラフィック風呂ｋー、帯域外通信チャネルなど）を含む、ネットワークトポロジ全体を視覚化する、正確で、最新のアーキテクチャ図を作成しなければならない。 ii. ネットワークスキャンツール（オープンソースの Nmap、Zenmap など）を使用し、サーバー、ワークステーション、ネットワークデバイス、クラウドリソ	**全てのサービスモデルに適用：** CSP より提供される実装ガイドラインが適用される。

ースなど、全てのネットワークコンポーネントのトポロジを識別および検証しなければならない。 iii. 図にはネットワークコンポーネントの論理的な構成と相互作用を表すアーキテクチャモデルと関連ツール（オープンソースの GNS3、Ansible、LibreNMS など）で補足されなければならない。 iv. ネットワークアーキテクチャを視覚的に表現するためのネットワーク図ソフトウェアなｄのツールの使用が推奨される（例：オープンソースの Diagrams.net、NetBox など）。 v. ネットワーク図と関連ソフトウェアは、権限のある担当者がアクセスでき、不正アクセスから保護されなければならない。 e. ネットワークセキュリティ管理策の文書化： ネットワークに実装されている全てのセキュリティコントールの詳細な説明を文書化しなければならない： i. 全てのネットワークアーキテクチャコンポーネントのバージョン番号、パッチレベル、構成設定（ファイアウォールルール、アクセス制御リスト、セキュリティプロトコルなど） ii. アクセス、認証、認可、データ保護を統制するネットワーク要件とこれらがネットワークインフラストラクチャ全体でどのように実装され、適用されるか f. ネットワーク変更管理： i. ネットワークの変更と更新に関する変更管理プロセスを定義しなければならない（承認手順、テストプロトコル、ロールバックメカニズムを含む） ii. ネットワーク構成と文書の変更を長期的に追跡するため、バージョン管理を実装しなければならない。 g. ネットワーク文書のレビューと更新： ネットワークアーキテクチャと関連するリスク評価文書はリビングドキュメント（継続的に更新される文書）として扱い、ネットワークトポロジ、セキュリティポリシー、新たなセキュリティ上の脅威、進化するコンプライアンス要件の変化を反映するため、定期的に更新されなければならない。	

Control Title	Control ID	Control Specification
ネットワーク防御	**IVS-09**	ネットワークベースの攻撃に係る保護、検知、タイムリーな対応のために、プロセス、手順、多レイヤー防御技術を定義、実装、評価する。

Control Ownership by Service Model

IaaS	PaaS	SaaS
Shared (Dependent)	Shared (Dependent)	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： これは、IaaS と PaaS の CSP と CSC の双方に対する「依存した形で共有」となる管理策である。SaaS ソリューションの場合は、CSP 所有の管理策となる。 IaaS サービスでは、CSC と CSP は共同でネットワークソリューションのデプロイ、管理、セキュア化、構成の責任を担う。PaaS ソリューションのネットワークセキュリティ管理策のほとんどは CSP によって提供される。SaaS サービスの場合、ネットワークインフラストラクチャが抽象化されているため、ネットワークセキュリティ管理策はソフトウェアコアサービスの一部として CSC のために管理および保護される。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： ネットワークベースの攻撃（第 3 レイヤーDDoS、中間者攻撃、SQL インジェクション、IP スプーフィング、フィッシング、マルウェアなど）は、資産や情報の機密性、完全性、可用性を侵害するためにネットワークインフラストラクチャへの不正アクセスを試みます。 ネットワークセキュリティ管理策（多レイヤー防御委技術）は、高度な脅威インテリジェンスとプロトコル分析、異常検出、侵害指標のブロック、シグネチャベースの手法を使用して攻撃を検知し、防御する。 CSP はまた、CSC がネットワークセキュリティを適切に構成および管理できるよう、セキュリティ管理策を CSC に公開しなければならない。 物理環境に存在する脆弱性は、仮想環境にも適用される。アプリケーション、ファイアウォールまたはネットワーク構成上の欠陥／脆弱性は悪用される可能性がある。物理的、論理的の双方および管理的管理策に多レイヤー防御手法を活用しなければならない。	**実施ガイドライン：** ネットワークベースの攻撃（第 3 レイヤーDDoS、中間者攻撃、SQL インジェクション、IP スプーフィング、フィッシング、マルウェアなど）は、資産や情報の機密性、完全性、可用性を侵害するためにネットワークインフラストラクチャへの不正アクセスを試みます。 ネットワークセキュリティ管理策（多レイヤー防御委技術）は、高度な脅威インテリジェンスとプロトコル分析、異常検出、侵害指標のブロック、シグネチャベースの手法を使用して攻撃を検知し、防御する。 CSP はまた、CSC がネットワークセキュリティを適切に構成および管理できるよう、セキュリティ管理策を CSC に公開しなければならない。 物理環境に存在する脆弱性は、仮想環境にも適用される。アプリケーション、ファイアウォールまたはネットワーク構成上の欠陥／脆弱性は悪用される可能性がある。物理的、論理的の双方および管理的管理策に多レイヤー防御手法を活用しなければならない。
IaaS プロバイダー： CSP は、ホストインフラストラクチャ（ハイパーバイザとオペレーティングシステム）およびストレージデバイスに対するネットワークベースの攻撃に対する保護、検出およびタイムリーな対応のための手順と手続および多レイヤー防御技術（DDoS 緩和	**IaaS 利用者：** CSC は、CSP がプロビジョニングしたインフラストラクチャ上にデプロイされ使用されるゲストオペレーティングシステムおよび仮想マシンに対するネットワークベースの攻撃に対する保護、検出およびタイムリーな対応のための手順と手続お

ソリューション、ネットワークフィルタリング、ファイアウォール、IDS/IPS など）を定義、実装および評価しなければならない。	および多レイヤー防御技術（DDoS 緩和ソリューション、ネットワークフィルタリング、ファイアウォール、IDS/IPS など）を定義、実装および評価しなければならない。
PaaS プロバイダー： CSP は、ホストインフラストラクチャ（ハイパーバイザとオペレーティングシステム）、ストレージデバイス、仮想マシン、コンテナおよびプラットフォーム管理ソフトウェア（Web サービス、データベースサービスおよびアナリティクスを含む）に対するネットワークベースの攻撃に対する保護、検出およびタイムリーな対応のための手順と手続および多層防御技術（DDoS 緩和ソリューション、ネットワークフィルタリング、ファイアウォール、IDS/IPS など）を定義、実装および評価しなければならない。	**PaaS 利用者：** CSC は、CSP がプロビジョニングしたプラットフォーム上で開発およびホストするアプリケーションに対するネットワークベースの攻撃に対する保護、検出およびタイムリーな対応のための手順と手続および多層防御技術（DDoS 緩和ソリューション、ネットワークフィルタリング、ファイアウォール、IDS/IPS など）を定義、実装および評価しなければならない。
SaaS プロバイダー： CSP は、ホストインフラストラクチャ（ハイパーバイザとオペレーティングシステム）、ストレージデバイス、仮想マシン、コンテナ、プラットフォーム管理ソフトウェア（Web サービス、データベースサービス、アナリティクス、アプリケーションを含む）およびデータに対するネットワークベースの攻撃に対する保護、検出およびタイムリーな対応のための手順と手続および多層防御技術（DDoS 緩和ソリューション、ネットワークフィルタリング、ファイアウォール、IDS/IPS など）を定義、実装および評価しなければならない。	**SaaS 利用者：** 該当しません。SaaS カスタマーは、CSP がネットワークベースの攻撃に対する保護、検出およびタイムリーな対応のための手順と手続および多層防御技術を定義、実装および評価していることを確認しなければならない。 SaaS アプリケーションへの認証に SSO が使用される場合、CSC は SaaS プロバイダーと ID 情報を交換する間、そのネットワークを保護する責任を負う。
全てのサービスモデルに適用： 考慮すべき多層防御のテクニック／洞察には以下のものが含まれる（ただし、これらに限定されるものではない）： a. ネットワーク資産の範囲と保護の優先順位： i. クラウド環境内の全てのクラウドネットワークテクノロジーとタイプの詳細なインベントリを作成し、定期的に更新しなければならない。これには有線と無線の双方のネットワーク資産が含まれる。 ii. データの機密性と分類に基づき、最も重要なネットワーク資産に優先的に保護対策を施す。 b. ファイアウォール管理： i. セキュリティルールに基づいてトラフィックをフィルタリングし、不正アクセスを防止するために、クラウドネットワークの各レイヤー（仮想プライベートクラウド（VPC）、サブネット、アプレイケーションレベルなど）にファイアウォールを導入しなければならない。 ii. Web アプリケーションファイアウォールを導入し、一般的な Web ベースの攻撃からアプリケーションを保護し、悪意のあるリクエスト（SQL インジェクション、クロスサイトスクリプティング、サービス拒否（DoS）攻撃など）がアプリケーションサーバに到達する前にブロックしなければならない。 c. 侵入検知・防御システム（IDS／IPS）：	**全てのサービスモデルに適用：** CSP の「実装ガイドライン」が適用される。

IDS／IPS ソリューションは、ネットワークトラフィックの不審な動きを監視し、潜在的な侵入や攻撃を特定するために導入しなければならない（IPS は受動的に異常を検出し、IPS は能動的に悪意あるトラフィックをブロックする）。

d. ネットワークトラフィック解析（NTA）：
   i. NTA ツールは、ネットワークトラフィックパターンに関するより深い洞察を得て、悪意のあるアクティビティを示す可能性のある以上を特定するために利用しなければならない（例：ディープパケット解析、トラフィックスロットリングによる DDoS 攻撃防御、ブラックホール化など）。
   ii. 入出力トラフィックパターンには、MAC スプーフィング、ARP ポイズニング攻撃、分散型サービス拒否（DDoS）攻撃などが含まれる場合がある。

e. ネットワークトラフィックの暗号化：
   移動中の機微データは、クラウド内およびクラウドとオンプレミス環境間のデータ転送に TLS／IPsec などのセキュアなネットワークプロトコルを用いて暗号化し、傍受や不正アクセスから保護しなければならない。

f. ネットワーク脅威インテリジェンス：
   i. 脅威インテリジェンスフィードは、クラウド環境における新たなネットワークの脅威、脆弱性、攻撃手法に関する情報を常に入手するために活用すべきである。
   ii. 脅威インテリジェンスをネットワークセキュリティシステムに統合し、クラウドネットワーク攻撃をプロアクティブに検知・防御する。

g. ネットワークインフラストラクチャのパッチ適用と更新：
   i. 脆弱性管理プログラムは、クラウドネットワークインフラストラクチャとソフトウェア／アプリケーションの脆弱性を特定、評価、修正するために活用されなければならない（TVM ドメイン参照）。
   ii. 攻撃者に悪用される可能性のある脆弱性を軽減するために、クラウドネットワークインフラストラクチャ・コンポーネントの最新のセキュリティパッチと更新プログラムを常に入手する。

h. ネットワークのセキュアな構成管理：
   i. クラウドネットワークリソースのセキュアな設定標準を適用しなければならない（例：仮想マシン、ネットワークデバイスの設定、クラウドベースのアプケーションデプロイの構成）。
   ii. 認証と送信のための強力な暗号化によるセキュリティ設定を有効にし、ベンダーのデフォルト設定（暗号化鍵、パスワード、SNMP コミュニティ文字列など）を置き換えなければならない。

i. ベンダーのセキュリティ管理策の多様性：
   単一障害点や脆弱性のリスクを軽減するため、さまざま

なベンダーのさまざまなネットワークおよびシステムコンポーネントを使用し、統合すべきである。 j. 継続的なモニタリングと評価： i. 監査およびログ機能（SIEM ソリューションなど）を実装し、さまざまなネットワーク資産からのネットワークアクティビティ、ユーザーアクション、セキュリティベントを追跡しなければならない。ログを監視し、異常、疑わしいアクティビティ、潜在的な侵害を検出する。 ii. ネットワーク内の不正なネットワークデバイスを検出し、迅速に切断する機能を開発しなければならない。	

Control Domain LOG

2.13 ロギングと監視(LOG)

Control Title	Control ID	Control Specification
ロギングおよびモニタリングに関するポリシーと手順	**LOG-01**	ロギングおよびモニタリングのためのポリシーと手順を確立、文書化、承認、周知、実装、評価、維持する。少なくとも年 1 回、ポリシーと手順をレビューし更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は CSC と CSP の双方で共有されるが、管理策の実施はそれぞれ独自に行われる。各当事者は、地理的位置、契約上、および規制上の要件に応じて、それぞれ達成すべきエコシステム内で定義され採用される、異なるロギングおよび監視ポリシー要件および手順を有することが期待される。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用可能：** CSP は、明確な目的、範囲、役割、責任、および組織体間の調整活動を定義した、ロギングおよび監視に関する独自のポリシーと手順、並びに提供されるトレーニング演習を持つべきである。 前者は、契約、法律、および規制の枠組みの中で定義される特定の要件に適合するように調整されるべきであり、異なるクラウドアーキテクチャモデルのセキュリティ責任分担のガイドラインに適合すべきである。CSP は、その内部システム及び CSC に提供されるシステム（クラウドサービス）を監視するための規定を設けるべきである。 ポリシーと手順は、システムに重要な変更が加えられたとき、インシデントが発生したとき、または少なくとも年 1 回、見直しまたは更新されるべきである。 ポリシーには、以下に関する規定が含まれるべきである（(ただし、これに限定されない）： a. 範囲と目的：規制及びリスク分析活動によって導入された、	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

対象となるシステム、アプリケーション及びデータを特定した、ロギング及び監視活動の目的、範囲および目的。ポリシーには、ロギングの "試行 "を定義、分類及び記録するための標準及びパラメータを、より具体的に含めること。

b. ロギングの標準：
   i. 全てのクラウドコンポーネントに対する統一されたロギング標準要件。
   ii. 定義されたデータ分類フレームワーク（DSP-04 を参照）に基づき、機微データに対応するロギング要件が、割り当てられた分類レベルに従って規定されること。

c. 実行時要件：継続的なリスク評価を統合しながら、監査ログの初期化、停止、又は一時停止の条件を決定。

d. 保持要件：運用、フォレンジック分析、コンプライアンス目的に対応する、規制要件に基づくログ保持およびアーカイブ要件

e. 監視ツールと技術：
   i. ログの監視と分析に使用するツールや技術を、業界のベストプラクティスに沿ったものにすること。
   ii. 通信プロトコル、エスカレーション手順、文書化要件を含む、異常検知とログとの相関、および対応自動化のためのプロセスと手順

f. 警告と対応セキュリティ上の脅威を示す可能性のある特定のセキュリティイベントについて、ログに基づいて警告と利害関係者への通知標準を設定し、タイムリーな対応と緩和策を確保する。

g. タイムスタンプ：社内アプリケーションからのログを含む、全てのログのタイムスタンプ要件

h. アクセス制御：誰がログにアクセスできるかを指定するアクセス制御要件、ログアクセスのための強力な認証および承認メカニズム
   i. 権限の昇格を含む、識別および認証ロギングメカニズムの使用と変更
   ii. 物理的アクセス制御システムのログ要件
   iii. 提供されたクラウドサービスに関連するログにアクセスするための、確立された SLA に従った CSC の有効化（API 経由など）。

i. ログの保護：
   i. ログの保護と、ログデータを保護するための暗号化および暗号化の使用に関する要件
   ii. 鍵管理システムのログの要件（鍵管理システムの管理者アクセス、鍵のライフサイクル管理ログなど）

j. システムの設計と構成：
   i. ログシステム自体の要件（例：ログシステムへのアクセスの成否、認証スキームの変更、 ログまたはインデックスの削除）
   ii. ハイレベル設計（HLD）が満たすべきログシステムの要件

k. 可用性と完全性：ログシステムと情報データの可用性と検証可能な完全性を達成すべき。セキュリティ強化とコンプ

ライアンス遵守のため、改ざん防止台帳を利用すべき。 l. 定期的なログの監査とレビュー：ログの完全性、正確性、妥当性を確保するための定期的な監査とレビューの規定 m. 承認：組織の戦略的目標およびリスク選好度との整合性を確保するための承認要件および上級管理職の関与 i. ポリシーと手順の変更または修正のための承認プロセスを確立すること。 ii. 承認に関する文書化された記録（日付、承認者の氏名、関連するコメントや議論を含む）を維持すること。 n. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進すべきである。 o. メンテナンスとレビュー：ロギングと監視のポリシーと手順を文書化し、少なくとも年 1 回見直し、更新することにより、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映させること。	

Control Title	Control ID	Control Specification
監査ログの保護	**LOG-02**	監査ログのセキュリティと保持を確実にするためのプロセス、手順、技術的手段について定義、実施、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は CSC と CSP の双方で共有されるが、管理策の実施はそれぞれ独自に行われることが期待される。両当事者は、監査ログの保護および保持に関して、契約上、規制上、または法律上の要因により要求される異なる手順と手続および技術的な管理手段を有する可能性がある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、法律、規制、または契約上のコンプライアンス要件に沿ったログの保護を保証するために、物理的および論理的な管理を含む強力な保護体制を実装する必要がある。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。 また、ログデータの保存やその他のサービスを提供するために CSP を利用する場合、CSC は、利用前に、CSP が契約上のセ

これらの要件が適用されない場合、グッドプラクティスガイドラインに確実に従うこと。 ログの保護は、不正アクセスの制限、ログへのアクセスおよび変更の監視および監査、セキュアな環境での保管など、ログファイルおよびデータのフォレンジック上の完全性を確保する必要がある。 ログデータは、法的要件および／または CSC との契約上の合意により定義される最低期間、業務上および法律上の調査、または悪意ある行為の検知を可能にするために保持されるべきである。 監査ログのセキュリティ確保と保存を目的とするその他の推奨事項（ただし、これらに限定されない）: a. 監査ログの一元化：監査ログをセキュリティ情報イベント管理（SIEM）システムと統合し、一元的に保存・管理し、セキュリティベントを効率的に監視・相関させること。 b. 監査ログの構成:クログの保存・保管ポリシーや規制要件に従って、包括的な監査保存ログを生成するようにクラウドサービスを構成すること。 c. ログの保持と CSC： i. ログがセキュアに保存され、将来の調査のためにアクセスできるように、アーカイブの仕組みを導入すること（可能であれば自動化されるべき）。 ii. 監査ログの保存期間または保護メカニズムの変更を含め、監査ログの保存ポリシーについて CSC と透明性のあるコミュニケーションを維持すること。 iii. CSC は、短期および長期のデータ保持のオプションにより、各自のコンプライアンスおよびビジネス上のニーズに基づいてデータ保持設定をカスタマイズする能力を提供されるべきである。 iv. CSC が記録したデータの保存期間が終了した場合、または CSC が要求した場合に、CSC が記録したデータを永久に削除するために、セキュアなデータ削除プロセスを導入すること。 d. セキュアで効率的なログ保存 i. 監査ログは、不正アクセスや改ざんを防止するため、改ざん防止されたセキュアなストレージに保存すること。 ii. 改ざんを防ぐため、ログを WORM（write-once-read-many）形式で保存し、不変のストレージを採用すること。 iii. データ重複排除と圧縮技術を利用して、冗長なデータブロックを特定・削除し、保持ログの全体的なストレージフットプリントを削減すること。 iv. 関連する最新データへのアクセスを維持しながら、古いログを定期的にアーカイブストレージに移動するログローテーションメカニズムを実装すること（可能	キュリティ要件を満たしていることを確認する。

であれば自動化）。 v. 保存時、使用時、および移動時に保持されるログデータを保護するために、暗号化メカニズムを実装すること。 e. ログへのアクセス制限： i. 保持された監査ログに対する厳格なアクセス制御を実施し、権限のある担当者のみにアクセスを制限すること。 ii. 保持されている監査ログへのアクセスの監査証跡を維持し、誰が、いつ、どのような目的でログにアクセスしたかなどの詳細を記録すること。 f. レビューと監視：監査ログの定期的なレビューと自動監視プロセスを導入し、以下を検知すること。 監査ログへのアクセスや変更に関連する異常や不審な行動に対する警告	

Control Title	Control ID	Control Specification
セキュリティモニタリングとアラート	**LOG-03**	アプリケーションおよび基盤となるインフラストラクチャの内部におけるセキュリティ関連イベントを特定し監視する。そのようなイベントや、各々のイベントの評価指標に基づいて、責任を持つステークホルダへアラートを生成するシステムを定義し、実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は CSC と CSP の双方で共有されるが、CSP がアクセス、転送、または CSC がインフラストラクチャとアプリケーションに対する独自のロギングと監視要件をデプロイする能力を提供する必要があるため、両者間の依存関係が生じる。CSP と CSC 間の効果的なコミュニケーションと連携により、両当事者はクラウド環境におけるセキュリティ関連のイベントを監視し、迅速に検出、分析、および対応することができる。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **IaaS プロバイダー：**	**実施ガイドライン：** **IaaS 利用者：**

CSP は、必要に応じて CSC の機能をサポートするためのインフラを用意するべきである。	CSC は、可能な場合、インフラストラクチャの追加的な監視を独自に実施すること。また、IaaS プラットフォーム上にデプロイされたアプリケーションについても、独自に監視を実施すること。
PaaS プロバイダー： PaaS プロバイダー：CSP は、PaaS 環境内にインストールされるアプリケーションについて、PaaS 内の一部でこの責任を負う。この場合、CSC が PaaS プラットフォームにインストールするアプリケーションは除外される。	**PaaS 利用者：** CSC は、可能な限り、インフラストラクチャについて独自に追加的な監視を実施することが望ましい。また、PaaS プラットフォーム上にデプロイされたアプリケーションの監視を独自に実施すること。
SaaS プロバイダー： CSP は、グッドプラクティスレベルでのインフラストラクチャとアプリケーションの監視を実施する責任を負う。CSC がオンデマンドで監視をカスタマイズできるようにし、CSC が独自の活動を実施できる能力を維持することで、追加レベルをサポートすることが望ましい。	**SaaS 利用者：** CSC は、可能な限り、SaaS プラットフォーム上にデプロイされたインフラストラクチャとアプリケーションについて、独自に追加的な監視を実施すること。
全てのサービスモデルに適用： セキュリティ事象の特定および監視の実施に関するベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）： a. 監視の範囲と目的： i. クラウド固有の環境、基盤となるクラウドインフラストラクチャコンポーネントおよびリソースを含む監視範囲を決定すること。 ii. セキュリティイベント監視の目的（違反の特定、不正行為の検出、データ損失の防止など）を定義すること。 iii. セキュリティイベント監視ツールは、クラウド環境の監視目的、監視範囲、および 技術的能力に適合したものを使用すること。 iv. CSP は、自社のリスク、ビジネス要件、および影響に関する CSC の分類に基づいて、監視機能に優先順位を付けること。 b. ログの収集と分析：全てのユーザー活動、API 呼び出し、異常な活動を特定するためのシステムイベント（例：不正アクセスの試行、ネットワークトラフィックの急増、システムの異常を示すシステムログ）など、セキュリティに関連する幅広いイベントを捕捉するためにログを収集し、分析すること。 c. データの正規化：収集したイベントを標準化・正規化し、一貫性のある分析・比較を実現（イベントを共通のフォーマットに変換し、命名規則やデータ構造の不一致を解決するなど）。 d. 脅威インテリジェンスの統合：脅威インテリジェンスフィードをログシステムおよびセキュリティイベント分析と統合して、脅威の検出を強化し、既知の脆弱性や攻撃パターンに基づいてアラートの優先順位を決定すること。	**全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

e. 機械学習と異常検知：機械学習技術とツールを活用して、正常な行動のパターンを特定し、異常を検知すること。
f. セキュリティ分析と相関：セキュリティ分析ツールを使用して、識別されたセキュリティベントを異なるソース間で相関させ、一見無関係に見えるイベント間の関係を特定し、隠れた攻撃パターンを明らかにする可能性があること。

アラート導入のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）：
g. 警告ルールの設定：
  i. 特定のタイプのセキュリティベント（不正アクセス試行、データ流出、異常なトラフィックパターンなど）に対してアラートを生成するように、監視ルールを策定し、構成すること。
  ii. アラートは、確立または合意されたしきい値を超えるリスク、イベント、またはインシデントを示 す測定標準（例えば、CSC 要件に基づく）に基づいて、生成すること。
h. 警告ルールの見直し：警告ルールは、セキュリティ動向、脅威インテリジェンスの更新、利害関係者からのフィードバックに基づいて定期的に評価し、改善すべきである。
i. アラートの分類：アラートは、高、中、低優先度、異常検知、侵入検知、ログ分析イベントなど、重要度とタイプに基づいて分類されること。
j. アラートの優先順位を設定：重要度と影響度に基づいてアラートに優先順位を付け、適切な利害関係者にルーティングするために、階層的なアラートシステムを導入すること。
k. アラートデータの履歴：過去のアラートデータは、パターン、傾向、および監視範囲における潜在的なギャップを特定するために分析すること。

生成されたアラートの定義（ただし、これらに限定されない）：
l. アラートの内容；
  i. イベントタイプ：アラートのトリガーとなるイベントのタイプ（例：アクセス、変更、削除）。
  ii. 影響を受けるリソース：インシデント調査を合理化するための、イベントに関与した特定のリソースまたは資産（ユーザーアカウント、サーバー、データベースなど）に関する情報
  iii. タイムスタンプ：他のログとの相関のためにインシデントのタイミングを確立し、対応の緊急性を判断するためのイベントのタイムスタンプ。
  iv. 責任のあるユーザーまたはエンティティ：インシデント対応中の迅速な帰属と説明責任を可能にする。
  v. ソース IP または場所：イベントの発信元 IP アドレスまたは場所により、活動の発信元および潜在的な地理的背景を理解する。
  vi. アクションの詳細：アクセス、変更、削除、コピーされた特定のデータ、影響を受けた構成や設定など、実

行されたアクション。 vii. 成功／失敗のステータス：潜在的なセキュリティインシデントと通常の運用を区別するのに役立ち。 viii. しきい値または異常値：しきい値または異常値を超えると警告が発生するもの（例えば、ログイン試行失敗の回数が異常に多い場合は、ブルートフォース攻撃を示している可能性がある） ix. コンテキスト情報：アクセスの状況（例：営業時間外）、または悪意のある活動を示す可能性のある異常なパターンなど、アクションに関連するコンテキスト情報。 x. 重大度レベル：イベントの潜在的な影響と重要性に基づくアラートの重大度レベルであり、対応の緊急性を示す（例えば、アラートの重大度を調査するための標準作業手順（SOP）を定義する。 xi. コンプライアンス指標：規制要件の遵守を確実にするために早急な対応が必要な関連するコンプライアンス指標または違反。	

Control Title	Control ID	Control Specification
監査ログへのアクセスとアカウンタビリティ	**LOG-04**	監査ログへのアクセスを認可されている担当者に限定し、個々のアクセスのアカウンタビリティのある記録を維持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は CSC と CSP の双方で共有されるが、CSP が CSC にこのようなロギング機能、およびログのアクセス制限とアクセスの説明責任を可能にする機能を提供する必要があるため、両者の間には依存関係がある。 CSC が独自の能力を必要とせず、全てのデプロイモデルについてこれらの義務を CSP に移行した場合、CSP は管理の所有者となるが、ログへのアクセスを許可される人物について CSC のガイダンスが必要である。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。

実施ガイドライン：

全てのサービスモデルに適用：

CSP は、クラウド運用の完全性と説明責任を維持するために、監査ログを保護する必要がある。CSP と CSC の両者には、監査ログを不正アクセスから保護し、改ざん防止を確実にするための適切な対策を実施する責任がある。

監査ログには、アクティビティ、アクション、およびイベントに関する情報が含まれ、その性質上、機密性が高い可能性がある。不正アクセスから保護するために、適切な制限を実施すべきである。監査ログは、不審な活動の識別及び検知を支援するためのアクセス追跡に使用することができる。監査ログは、不審な活動の特定と検知を支援するためのアクセス追跡に使用することができる。また、分析およびセキュリティインシデントに関連する調査ニーズをサポートするデータも含まれる。

監査ログへのアクセスを制限することを目的とした実装のベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）：

a. RBAC を使用したログアクセス：組組織内の異なる役割に特定の監査ログアクセス権限を定義し、割り当てる RBAC システムを実装する必要がある。
b. ログのアクセス制限：
   i. 監査ログへの MFA アクセスは、「知る必要がある」全ての要員（特権アカウントを含む）に対して、最小特権の原則に従って実装すること。
   ii. 個人による権限のエスカレーションや、許可された役割を超えた機微なログ情報へのアクセスを防止するために SoD を実施すること。
   iii. 生の監査ログに直接アクセスできる人数を制限する（アクセス制御リストまたは専用のログ閲覧ツールを使用してアクセスを制御する）。
   iv. 内部システムおよび CSC に提供されるシステムの監査ログへのアクセスを制限すること。
   v. CSP は、ログへのアクセスが必要な CSC 要員の承認確認を受けることが望ましい。
   vi. CSC が監査ログを独自に記録することを要求した場合、CSP は、関連する構成および転送をサポートすることを許可するものとする。
c. 一意のアクセス説明責任：監査ログエントリは、法的／規制上の要件に従って、調査およびフォレンジック分析のために、個々のユーザーの行動、説明責任、および使用状況を正確に追跡できるように、ID（ユーザー名、関連する役割、アクセス目的、アクセスしたリソース、IP アドレス、およびタイムスタンプを含む）と関連付けられるものとする。
d. セッションタイムアウト：セッションタイムアウトを強制し、監査ログアクセスの再認証を要求すること。
e. ログアクセス基盤：監査ログへのアクセスをホストし管理するインフラストラクチャは、サイバー攻撃や不正アクセ

実施ガイドライン：

監査ログへのアクセスを制限することを目的とした推奨事項には、以下が含まれる（ただし、これらに限定されない）：

a. 監査ロギングとアクセス有効化：
   i. クラウドサービスの監査ログは、セキュリティ要件およびコンプライアンス要件に基づいて構成され、有効化されること。
   ii. CSP の監査ログ保持ポリシー、アクセス制御、および暗号化の実施方法を検討し、理解し、セキュリティおよびプライバシーの要件との整合性を確保すること。
   iii. 合意された SLA に従って取得、維持、およびアクセスされる監査ログの範囲について、CSP と協力して合意すること。
   iv. 監査ログを要求しアクセスするための明確な手順を CSP と共有し確立すること。
b. 監査ログの転送制限：
   i. 監査ログの外部システムまたは場所への転送は SLA に従った厳密なデータ取扱手順に従って、必要な場合に最小限に抑えるものとする。
   ii. セキュリティツール（例えば、DLP）を利用して、監査ログからの機微情報の不正なエクスポートまたは転送を監視し、防止すること。
c. 監査ログへのアクセス：監査ログへの MFA アクセスは、「知る必要がある」全ての要員（特権アカウントを含む）に対して、最小特権の原則に従って実施すること。
d. 一意のアクセス説明責任：監査ログエントリは、法的/規制要件に従った調査およびフォレンジック分析のために、個々のユーザーの行動、説明責任、および使用状況を正確に追跡できるように、ID に関連付けること。
e. ログアクセスの監視と報告：監査ログへのアクセスを監視し、異常や違反の可能性を特定する。
f. ログアクセスレビュー
   i. CSC 要員のアクセス許可は、その役割と責任に基づいて定期的に見直し、更新、管理すること。
   ii. アクセス権を必要としなくなった個人については、アクセス権を失効させること。不正アクセスを試みた場合は調査すること。
   iii. 監査ログへのアクセスを効果的に制限するための内部セキュリティ対策を定期的に見直し、強化するために、CSP からのベストプラクティスおよびセキュリティ更新を遵守し、活用すること。
g. 内部監査：監査ログは、調査およびコンプライアンス監査のために CSC がアクセスできるようにする必要がある。

スから保護されるべきである。ネットワークおよびシステムのセキュリティ対策を実施する必要があります(IVS ドメインを参照)。 f. 監査ログの転送制限： i. 監査ログの外部システムまたは場所への転送は SLA に従った厳密なデータ取扱手順に従い、必要に応じて最小限に抑えること。 ii. セキュリティツール（例えば、DLP）を利用して、監査ログからの機密情報の不正なエクスポートまたは転送を監視し、防止すること。 g. ロギングの標準化：全てのクラウド環境とサービスにおいて、標準化されたロギングとアクセス方法を確立すること。 h. ログアクセスの監視と報告：監査ログへのアクセスを監視し、異常や違反の可能性を特定すること。 i. ログアクセスレビュー：実施されたアクセス制御の定期的なレビューを実施し、監査ログへのアクセスが許可された要員のみであることを確認し、不必要な権限を取り消すこと。	

Control Title	Control ID	Control Specification
監査ログのモニタリングとレスポンス	**LOG-05**	セキュリティ監査ログを監視し、典型的な、または予期されるパターン以外の活動を検知する。検知された異常をレビューし、適切かつタイムリーな措置を取るための定義されたプロセスを確立し、それに従う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、クラウドインフラストラクチャ内およびクラウドリソースへのアクセスにおいて予期されるアクティビティの標準値を定義し、標準値から逸脱するその他のアクティビティについて監査ログを分析する責任を負う。CSP はまた、アラートを生成して適切な措置を講じることにより、逸脱を調査するプロセスを確立する。この管理策の実施責任は、調査または是正措置に CSC の要員の関与が必要な場合は、CSP が CSC に関与する必要があるため、CSP と CSC の双方で依存した形で共有される。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。

実施ガイドライン： **全てのサービスモデルに適用：** 監査ログには、クラウド環境で発生しているアクティビティ、アクション、およびイベントに関する情報が含まれる。これらのログを監視、分析することで、「いつ」「何が」「誰に」発生したのか、また発生した可能性のある悪意のある行為を特定することができる。影響範囲とビジネスへの影響を最小化するために、必要に応じて SLA 内で修復アクションを検討する必要がある。 通常の期待される活動のベースラインを定義し、悪意のある行為がないかログを継続的に監視する必要がある。 ログ監視の実装のベストプラクティスには以下が含まれる（ただし、これらに限定されない）： a. ログ監視： i. 監査ログは、異常および疑わしいパターンを監視し、設定の変更、削除、コピーまたはその他の変更などの全ての関連するアクション（成功／失敗）を監視すること。 ii. 監査ログを SIEM システムと統合して、ログデータを関連付け、セキュリティ異常や潜在的なセキュリティベントを全体的に把握できるようにすること。 b. 収集と分析： i. 監査ログをリアルタイムまたはほぼリアルタイムで収集・分析するために、自動化ツールを活用する。 ii. ログに記録される詳細レベルは、特に機微データについては制限すること。 iii. 個人データまたはその他の機微データのロギングは、法令に従い、避けること。 iv. セキュリティインシデントまたはコンプライアンス監査に備えて、監査ログを分析するためのフォレンジックプロセスが確立されていること。 c. 対応手順： i. 初期対応の指示またはエスカレーション手順（異常検知後直ちに誰に連絡するか、またはどのような行動をとるかを含む）が定義され、実施されること（例えば、CSC の要員を関与させるための改善措置の SOP）。 ii. 検知された異常の調査、警告の発行、脅威の封じ込め、脆弱性の是正のプロセスを合理化するために、対応手順を実装（可能であれば自動化）すること。 iii. 対応および解決に要する時間を短縮するために、異常	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

および潜在的なセキュリティ事象をほぼリアルタイムで可視化するレポーティングソリューションを提供すること。

d. 利害関係者とのコミュニケーション：
   i. セキュリティアラートの受信と関連利害関係者へのエスカレーションについて、役割と責任を定義する。
   ii. アラートのタイムリーな伝達を確実にするために、複数のコミュニケーションチャネルを採用すべきであること。
   iii. 利害関係者がアラートの傾向を監視し、データを視覚化し、特定のイベントにドリルダウンできるように、一元化されたダッシュボードを提供する必要がある。

以下のクラウドシステムおよびアプリケーションを含む（ただし、これらに限定されない）、関連する全ての種類のログの監視を有効にすること：

e. 管理アクティビティログ：これらのログは、クラウドスタックのあらゆるレベルの特権ユーザーのログインと管理者に関係し、機微データへの不正アクセスを特定するために使用することができる（アイデンティティとアクセス管理（IAM）システム、クラウドストレージシステム、認証サーバー、シングルサインオン（SSO）ソリューションなど）。

f. ネットワークトラフィックログ：不正アクセスの試み、悪質なトラフィック、データの流出を特定するために使用できるツールのログである（ファイアウォール、侵入検知・防止システム（IDS/IPS）、ロードバランサ、Web アプリケーションファイアウォール（WAF）、仮想プライベートネットワーク（VPN）、アンチウイルス（AV）ソフトウェア、アンチ DDoS、Endpoint Detection and Response（EDR）、データ損失防止（DLP）ソリューションなど）。

g. オペレーティングシステムのログ：オペレーティングシステム、仮想マシン、クラウドインスタンス、コンテナなどのシステムに適用される不正アクセスの試行、権限の昇格、マルウェア感染を特定するために使用する。

h. アプリケーションログ：CSC が所有するアプリケーション、またはサードパーティー製アプリケーションの使用に関するログであり、エラー、例外、不審な動作を特定するために使用される。これらのログは、アプリケーションサーバ、Web サーバー、データベース、コンテナ化されたアプリケーション、アプリケーションサーバ、Platform-as-a-Service（PaaS）環境、サーバレスコンピューティングサービスなどのシステムに適用される。

i. 暗号化と鍵管理のログ：暗号化および鍵管理システム/サービスからのログである。

j. API ログ：CPU、ネットワーク、クラウドストレージの I/O、データベース/メッセージキュー、クラウド管理コンソール、プラットフォームサービスのログや評価指標など、クラウドサービスプロバイダーが提供するクラウドサービスの API からのログや評価指標で、インフラ構成の変更を示す。

全てのログタイプについて、アクセス、変更、削除、データのコピー、その他構成や設定の変更などのアクション（成功／失敗）を監視し、関連するログを収集・分析する必要がある。	

Control Title	Control ID	Control Specification
時刻の同期	**LOG-06**	関連する全ての情報処理システムで、信頼できる１つの時刻源を使用する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は、クラウドインフラストラクチャおよびシステム全体にわたってシステムクロックを同期し、システム全体にわたってイベントのシーケンスを適切に再構築できるようにする責任を負うべきである。	**管理策所有権の根拠：** IaaS および PaaS サービスモデルの場合、CSP は全てのハードウェアのクロックを同期させる主な 技術的責任を有し、CSC は時刻同期に関連するいくつかの技術的または管理的管理を実施する責任を有するものとする。SaaS の場合、CSP はこの管理の実施に専ら責任を負う。
実施ガイドライン **全てのサービスモデルに適用：** 監査ログ生成メカニズムは、ログファイルに記録される各イベントの日付とタイムスタンプを取得するために、ネットワークタイムプロトコル（NTP）を使用して、全てのシステム上で同期されるべきである。システムログが適切に同期されていない場合、システムやインフラストラクチャ間でクロック設定に違いが生じ、アクティビティの日付とタイムスタンプがリアルタイムで発生したものと一致しなくなるため、これらのログはセキュリティインシデントの調査において有益ではなく、証拠として認められない。 以下のガイドラインを適用するべきである： a. 集中タイムサービス： i. 全ての資産とシステムの起動、開始、または再起動時にクロック同期を提供するために、集中タイムサービスを作成し、維持する必要がある。	**実施ガイドライン** **IaaS 利用者：** CSC は、信頼できる時間ソースを同期するようにゲスト OS を構成する必要がある。CSP が提供するタイムソースを使用することを推奨する。 CSC は、ゲスト OS およびアプリケーションで時間を正確に構成し、その整合性を保証するよう技術担当者に義務付ける管理制御を実施する必要があり。時刻同期に対する無許可の変更はリスクと見なされ、ログイベントを発生させる必要がある。 **PaaS 利用者：** CSC は、技術担当者が時刻設定の完全性を保証することを義務付ける管理統制を実施すること。 時刻同期に対する不正な変更はリスクとみなされ、ログイベントが発生すること。

ii. さまざまなシステムとの互換性と相互運用性を確保し、集中化された信頼性の高い時刻ソースとして機能するため、ネットワークタイムプロトコル（NTP）の RFC 5905 など、時刻同期の業界標準に準拠すること。

b. 定期的なクロック同期：

i. クラウド環境内の全てのサーバーは、集中管理された NTP サーバーと定期的に同期し、インフラ全体の一貫性を維持する必要がある。

ii. CSC がホスト資産の同期に利用できる時計同期サービスを提供すること。

c. システムの構成：全ての資産およびシステムが、集中型サービスから時刻同期用の時刻を取得するように設定されることを保証するプロセスを作成すること。

d. 時計設定の完全性：時刻情報への不正アクセスや改ざんを防止し、時刻同期プロセスの完全性を保護するため、認証の仕組みが実装されていること。

e. 同期の監視とアラート：

i. 時刻同期における逸脱または不一致を検出するために、監視システムを設定すること。

ii. 関連する利害関係者（例：管理者、CSC）に時刻同期に関する問題を通知するためのアラートメカ ニズムを設けること。

SaaS 利用者：

この管理策の実装は CSP にのみ適用される。

以下のガイドラインを適用するべきである：

a. CSP の時間管理の検証：インフラストラクチャ全体で正確な時間を維持するために、CSP が NTP サーバーなどの集中型で信頼できる時間ソースを実装していることを検証する。

b. 構成設定: CSC システムおよびアプリケーションは、CSP が提供する集中型 NTP サーバーと時刻を同期するように構成される必要がある。

c. 定期的な時間チェック：正確で一貫性のある時刻管理を保証するため、CSC アプリケーションに定期的な時刻チェックと同期ルーチンを導入すること。

d. 依存性の考慮：時間の影響を受けやすい操作やイベントが正しく調整されるよう、アプリケーションを設計・デプロイする際には、時間同期の依存関係を考慮する必要がある。

e. 文書化とコンプライアンス：CSC システム内に導入される時刻同期手順は文書化され、時刻管理に関連する業界標準または規制標準に準拠していること。

f. 監査証跡：時間関連のイベントを記録する監査証跡は、トレーサビリティおよび不一致やセキュリティインシデント発生時の説明責任を容易にするために維持されなければならない。

g. CSP とのコミュニケーション：整合性を維持し、懸念事項や特定の要件に対処するために、時刻同期の実務に関して CSP とのオープンなコミュニケーションが維持されるものとする。

Control Title	Control ID	Control Specification
ロギングスコープ	**LOG-07**	どのようなメタ情報／データ情報システムのイベントを記録すべきかを確立、文書化、および実装する。少なくとも年 1 回、または脅威環境に変化があった場合には、スコープのレビューおよび更新を行う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines

CSP	CSC
管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャの採用に関わらず変わらない。この管理策は、CSC と CSP の間で共有される。しかし、管理策の実装はそれぞれ独立している。両者は、それぞれの国や契約上または規制上の要件を考慮し、それぞれのエコシステム内のイベントを捕捉するための異なるログ記録およびモニタリング基準を設けている可能性がある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、ロギングを必要とするシステムイベント分類の独自のディレクトリを持つべきである。これらの分類を満たすイベントは、契約、法律、または規制の枠組みの中で定義される特定の要件を満たすために、必要な詳細とともにログに記録されるべきである。CSP は、内部システムおよび CSC に提供するシステムのアクティビティをログに記録するべきである。 イベントタイプのメタデータには、「誰が」、「何を」、「いつ」、「どこで」、「なぜ」、および各イベントタイプに関連する追加的な詳細に答えるために必要な全てを含めるべきである。 ログに記録されるべきイベントには以下が含まれる（ただし、これらに限定されない）： a. 認証とアイデンティティイベント： i. クラウドサービスへのログインの成功と失敗（例：ユーザー名とパスワードによるログイン、SSH 鍵によるログインの失敗、SMS コード、認証アプリ、バイオメトリックの種類など） ii. クラウド IAM システム内でのユーザーアカウントの作成、変更、削除（特に管理者権限を持つアカウントの作成） iii. アイデンティティのフェデレーションおよびフェデレーション解除アクティビティ iv. 特権ユーザーによるアクティビティ（管理者のログインやアクティビティなど） b. 認証とアクセス制御： i. クラウドサービスにおけるアクセス制御ポリシーの変更 ii. クラウドリソースおよび/または機微データへの不正アクセスまたは不正アクセス未遂の事例 iii. セキュリティグループとファイアウォールルールの変更 c. リソースのプロビジョニングとプロビジョニング解除： i. クラウドリソース（VM インスタンス、ストレージバケットなど）の作成、変更、削除 ii. オートスケーリングイベントとリソース割り当ての調整	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

iii. リソースのプロビジョニングと管理に関する API コール iv. 重要資産のリブート d. クラウドネットワークのイベント i. 仮想ネットワークのルール/設定、サブネット、ルートの変更 ii. クラウド環境内の不審なネットワークアクティビティの検出（IDS/IPS アラートイベント） iii. ネットワークトラフィックの異常と潜在的なセキュリティインシデント e. クラウドストレージのイベント i. クラウドストレージ内のファイルまたはデータへのアクセス、変更、削除、コピー ii. ストレージ構成と権限の変更 iii. 異常または不正なデータ移動に対する警告 f. クラウドサービス API コール： i. infrastructure-as-code のデプロイメントを含む、クラウドサービスの利用に関連する API コール（使用された API 鍵／トークンなど） ii. API 認証および認可設定の変更 iii. 通常とは異なる、または予期しない API アクティビティの監視 g. クラウドセキュリティグループのイベント i. セキュリティグループのルールと設定の変更 ii. セキュリティグループポリシーに基づいて拒否または許可されたトラフィックのインスタンス iii. セキュリティグループ活動の異常 h. 監査ログとコンプライアンスイベント： i. クラウド環境内の監査ログレビューとコンプライアンスチェック、およびセキュリティのベストプラクティス ii. 業界標準または規制標準に対するコンプライアンス違反のアラート i. コンテナとオーケストレーションのイベント： i. コンテナオーケストレーションプラットフォーム（例：Kubernetes）におけるコンテナのデプロイとスケーリングイベント ii. コンテナ構成とイメージの変更 iii. コンテナ実行時のセキュリティイベント j. サーバーレスコンピューティングのイベント i. サーバーレス関数の呼び出しと実行に関連するイベント ii. サーバーレスファンクション構成の変更 iii. サーバーレスの異常な動作や不審な動作を監視 k. クラウドベースのファイアウォールと WAF のイベント： i. クラウドベースのファイアウォールルールおよび設定の変更 ii. Web アプリケーションファイアウォール（WAF）のイベントとアラートの検出	

iii. 潜在的なセキュリティ脅威を示すトラフィックパターンの異常 l. クラウドベースの DDoS 防御イベント： i. 分散型サービス拒否（DDoS）攻撃に関するアラートとイベント ii. DDoS 防御の設定としきい値の変更 iii. DDoS 攻撃に対する緩和措置 m. クラウドコンプライアンス評価イベント i. クラウドリソースの脆弱性の評価とスキャンに関するイベント ii. コンプライアンス違反のアラートと推奨される是正措置 iii. コンプライアンス態勢に影響を与える変化の継続的監視 n. クラウドインシデント対応イベント： i. クラウド環境におけるインシデント対応活動中に発生したイベントとアラート ii. 調査、封じ込め、根絶、復旧作業に関するログ iii. クラウドのセキュリティインシデントに対処するために実施した措置の文書化 イベントタイプの分類は、少なくとも年 1 回、または脅威の状況に重大な変化があった場合に見直すべきである。	

Control Title	Control ID	Control Specification
ログの記録	**LOG-08**	関連するセキュリティ情報を含む監査記録を作成する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャに関係なく変わらない。この管理策は、CSP と CSC の両方で共有される。ただし、管理策の実装は互いに独立している。関連するメタデータを含むセキュリティイベントの監査ログは、調査または規制上の課題への対応を支援するために維持されるべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、セキュリティイベントの監査ログを維持するものとする。CSP は、内部システムおよび CSC に提供するシステムのアクティビティをログに記録するように規定し、全ての監査記録に関連するユーザーID を記録するものとする。 セキュリティ関連のログ情報には、以下を含むべきである（ただし、これらに限定されない）： a. LOG セキュリティ情報： i. イベントタイプ ii. イベント ID iii. イベントインデックス iv. イベントレベル v. イベント発生時刻（イベントが発生した時刻） vi. イベント記録時間（イベントが記録された時間） vii. イベントの説明 viii. イベントの場所 ix. イベントソース x. イベント結果 xi. イベントに関連するユーザーまたはシステムの ID	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
ログの保護	**LOG-09**	当該の情報システム（訳注：ログが保存されている情報システムを指す）は、未認可なアクセス、変更、および削除から監査記録を保護する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines

CSP	CSC
管理策所有権の根拠： この管理策の目的の決定は、クラウドアーキテクチャに関係なく変わらない。基本的に、この管理策は CSP と CSC の両方で共有される。ただし、管理策の実装は互いに独立している。監査ログは、不正なアクセスや不正な変更から保護され、調査や法的手続きのための真正な証拠として認められる必要があり、また監査およびログ情報の損失がないように定期的にバックアップされる必要がある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、以下のガイドラインに従って監査ログを保護するべきである： a. アクセス制御： i. ログデータへのアクセスを制限するために、厳格なアクセス制御メカニズムを実装すること（例えば、RBAC、MFA、SoD、読み取り専用アクセスの PoLP など）。 ii. ログデータにアクセスできる特権ユーザーのアクセスは、定期的にレビューされ、再検証されること。 iii. ログプロセスへの書き込み／削除アクセス要求には、上級管理者の承認が必要。 b. ログの暗号化： i. ログデータは、厳格な業界標準に従った強力な暗号化アルゴリズムと定期的に更新される暗号鍵を使用して、保存中と移動中の両方で暗号化すること。 ii. 監査ログデータを外部ストレージや分析ツールに送信する際は、セキュアなチャネル（暗号化された接続など）を使用すること。 c. ログの改ざん防止：ログデータの不正な変更または削除を防止する仕組みを導入すること（デジタル署名、改ざん防止ログ、イミュータブルログストレージソリューションの使用など）。 d. ログ保管の隔離：不正アクセスやデータ改ざんを防止するため、本番システムから切り離されたセキュアで隔離された環境にログを保存する。 e. ログの監視と警告：ログ管理システムおよびログ保管場所への全てのアクセス試行を追跡する監査証跡の仕組みを導入し（試行の成功と失敗を含む）、継続的に監視し、監査すること。 f. ログシステムの脆弱性管理とパッチ適用：ログ保存・管理システムの脆弱性を定期的にスキャンし、パッチを適用する。 全ての監査ログの変更または削除は、別の読み取り専用の変更トラッカーに別々に記録されるべきである。 監査ログの変更トラッカーは、以下を含むべきである（ただし、これらに限定されるものではない）：	**実施ガイドライン：** **全てのサービスモデルに適用：** CSC は、以下のガイドラインに従って監査ログを保護するものとする： a. アクセス制御： i. CSP が提供するアクセス管理策機能を活用して、ログデータへのアクセスを制限すること。 ii. ログリポジトリのアクセスログを定期的に監視およびレビューして、不正なアクセスを特定し、不審なアクティビティに対するアラートを確立すること。 b. ログの暗号化：ログデータはセキュアに設定され、暗号化されたチャネル（HTTPS など）を使用してクラウド内でセキュアに転送され、転送中の傍受を防ぐべきである。 c. 設定のバックアップ：ログ保存、アクセスメカニズム、ツールに関連する構成は、定期的にバックアップするべきである。 d. ログの監査とレビュー不一致、不正アクセス、または変更を特定するために、ログを監査およびレビューするプロセスを導入すべきである。 e. データの所在地と主権：ログデータが関連する規制を遵守し、承認された地域に保存されることを確実にするため、データの所在地と主権に関する要件を認識すること。 f. CSP との連携：CSP と連携して、CSP がログ保護のために提供するセキュリティ管理を理解し、セキュリティ要件とベストプラクティスとの整合性を確保する。

a. 変更タイプ（変更または削除） b. 変更時刻（日付とタイムスタンプ） c. 変更箇所（ページ番号、行番号） d. 変更理由（監査ログへの変更を許可する、事前に公表された理由のカタログ） e. 変更ステータス（成功または失敗） f. 変更に関連する個人またはシステムの ID。少なくとも以下のソース属性を含むべきです： i. ホスト名 ii. IP アドレス iii. MAC アドレス iv. サービスアカウント ID	

Control Title	Control ID	Control Specification
暗号化の監視とレポート	**LOG-10**	暗号、暗号化、鍵管理のポリシー、プロセス、手順、統制の運用に関する監視および内部報告機能を確立し、維持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠 CSP および CSC は、暗号運用に関する内部監視および内部報告プロセスを独自に実施する責任を負う。CSP は暗号化プロトコルの実装に責任を負うが、共有クラウドインフラストラクチャの自らの部分における暗号化操作の適切な使用を監視しテストする責任は CSC にある（暗号化に関するポリシー、プロセス、および管理の詳細については、CEK ドメインを参照）。	**管理策所有権の根拠** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン **すべてのサービスモデルに適用可能** 不正な開示や改ざんから機微データを保護するために暗号を使用する場合、明確に定義されたポリ シー、標準、手順（詳細は CEK-01 を参照）を通じて管理する必要があり。暗号鍵の使用は監視されるべきであり、逸脱があれば報告され、ポリシーに従って処理されるべきである。 暗号化操作は、ログに記録され、監視され、報告され、不正な鍵使用事象がセキュリティインシデント管理プロセスを通じてエスカレーションされ、是正されるようにしなければならない。 ファイルの整合性を保護するさまざまなソリューションを実装することにより、ログデータを不正な改ざんから保護すべきである。 CSP が、暗号化および鍵管理に関する効果的な監視および内部報告機能を確立し維持するための実施ベストプラクティスには、以下のものが含まれるべきである（ただし、これらに限定されない）： a. 鍵の暗号化と管理システムを監視する： i. 暗号化および鍵管理活動が行われるクラウドインフラストラクチャ内の重要なクラウドコンポーネントを特	**実施ガイドライン** CSP の「実施ガイドライン」が適用される。

定する必要があります（エンドポイント、データセンター、ストレージシステム、ネットワークデバイス、鍵管理サーバーなど）。 ii. 鍵生成、暗号化/復号化操作、鍵ローテーションイベント、アクセス試行を追跡するために、継続的な監視を実施すること。 b. ログとイベントデータの分析： i. ログ収集・分析ツールを導入し、暗号化および鍵管理活動に関連するデータを収集します。 ii. 収集したログを分析し、異常、疑わしい活動、潜在的なセキュリティ脅威を特定する。 iii. 暗号化と鍵管理の監視データを SIEM システムに統合し、一元的に集計、相関、分析できるようにする。 c. ベースラインとしきい値：通常の暗号化および鍵管理の運用に関するベースラインおよびしきい値を設定すること（鍵の使用状況、アクセスパターン、エラー率など）。 d. 警告と報告のメカニズム： i. 確立されたベースラインから逸脱したり、定義されたしきい値を超えたりした活動をセキュリティチームに通知するために、注意喚起と報 告の仕組みを導入すべきである。 ii. 暗号化と鍵の管理活動（傾向、異常、潜在的リスクを含む）をまとめた定期的な報告書を作成すべき。 iii. 報告書は、透明性と説明責任を促進するために、セキュリティチーム、コンプラ イアンス担当者、CSC を含む利害関係者と共有すべき。 e. 監視プロセスの見直し： i. 暗号操作の監視プロセスを定期的に見直し、セキュリティ脅威の検知と対処に有効であり続けるようにする。 ii. 暗号に関連するイベントのアラートトリガーを見直し、過去のデータを分析し、セキュ リティインシデントからのフィードバックを取り入れて監視プロセスを改善する。	

Control Title	Control ID	Control Specification
トランザクション／アクティビティのロギング	**LOG-11**	暗号鍵の使用状況の監査と報告を可能とするために、鍵のライフサイクル管理イベントについてログの取得および監視を行う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、CSP と CSC の双方で依存関係なしで共有される。機微データの機密性と完全性を保持するために、組織のポリシーと手順に従った暗号化技術を使用することが望ましい。暗号化鍵の使用は、監視および報告されるものとする。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、鍵の使用状況を効果的に監査および報告し、潜在的なセキュリティリスクを事前に特定し、改善することができる。CSP は、暗号化鍵のライフサイクルイベント（CEK ドメインを参照）の監視および報告が存在することを確認するものとする： a. KMS ログ：KMS のログと評価指標は一元化されたログ管理システムに統合され、さまざまなクラウドサービスからのログデータを統合できるようにし、包括的な監査とレポーティングを可能にする。 b. 鍵管理サービス（KMS）のログと評価指標： i. CSP の KMS サービスに内蔵されているログおよび監視機能を活用して KMS イベントをログし、鍵を記録すること： • 世代 • 配布 • アクセス • 使用（暗号化、復号、デジタル署名） • 破棄 • 失効 • ローテーション • 削除 ii. KMS ベースの指標を確立し、可能であれば自動化して、主要なパフォーマンス指標を追跡し、潜在的な使用異常を特定する必要がある。 c. 鍵のログアクセス管理：権限のある者のみが主要な資料にアクセスでき、全てのアクセス試行は記録され、レビューされること。 d. 保管とアーカイブの構成：KMS ログと評価指標の保存要件を特定すること。 e. 継続的な監視と評価： i. 暗号鍵のロギングおよび監視要件は、取得すべき特定のイベント、保存期間、アクセス制御の概要を定義すること。 ii. 不正、異常または疑わしい鍵のライフサイクルイベン	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

トに対して警告を発すること。 iii. 実施されたロギングおよび監視の有効性は、定期的にレビューおよび評価されること。 f. ログデータのレビューの監査：ログデータの定期的なレビューを実施し、潜在的な異常、不審な活動、または確立された規範から逸脱した使用パターンを特定すること。このプロアクティブなアプローチは、新たに出現したセキュリティリスクを迅速に検出して対処するのに役立つ。 g. 報告のメカニズム； i. KMS のログと指標データから意味のある洞察を引き出すために、標準的な報告メカニズムを開発すること。 ii. CSP は、CSC、監査委員会、およびセキュリティチームを含む関係利害関係者に、実用的なレポートを提供すべきである。	

Control Title	Control ID	Control Specification
アクセスコントロールログ	**LOG-12**	監査可能なアクセスコントロールシステムを使用して、物理的なアクセスを監視しログする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP は物理的インフラストラクチャのセキュリティを管理する当事者であるため、この管理策の実施責任は専ら CSP に属する。したがって、CSP は、物理インフラへの物理的なアクセスを監視および記録する責任を負う。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** CSP が、監査可能なアクセス管理策システムを使用して物理的アクセスを効果的に監視し、ログ記録するための実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 入退室管理システムの導入：	**実施ガイドライン：** CSC には適用されない。

i. 物理的入退室管理システムは、ドア、ゲート、管理区域を含む、全ての物理的入室ポイントにデプロイすること。
ii. セキュリティを強化するために、指紋スキャン、顔認証、虹彩認証などのバイオ評価指標認証方式を利用すること。
iii. アクセスは、職務と責任に基づいて権限を与えられた職員に制限されるべきであり、解雇時には直ちに取り消されるべきである。全ての物理的アクセス機構(例:鍵、アクセスカード)は、返却および/または無効化されること。
iv. 一般にアクセス可能なネットワークジャックへのアクセスを制限すべきである(例えば、未使用ポート、無線アクセスポイント、ゲートウェイ、ハンドヘルドデバイス、ネットワーク/通信ハードウェア、通信回線への物理的アクセスを制限する)。

b. アクセス制御クレデンシャル:
i. 電子入退室管理カードまたはバッジを許可された要員に発行し、カードリーダーと統合してセキュアな入退室認証を行う。
ii. カードの使用状況を追跡し、説明責任と監査目的でカードスワイプイベントを記録する。

c. ビデオ監視:
i. 全ての重要エリア(入口、データセンター、サーバールームなど)に高画質のセキュリティカメラを設置すべき。詳細な監視のため、鮮明な画像と音声による継続的なビデオ録画を使用すること。
ii. 記録された映像は、潜在的な調査や法医学的分析のためにセキュアに保管すること。

d. 監査ログ管理:
i. 全ての物理的入退室管理イベントを記録・保存する監査ログ管理システムを導入すべき(入退室管理カード、ACP、ビデオ監視システムからのログなど)。
ii. アクセス制御ログは、少なくとも年2回、または関連法規の要件に従ってレビューされるものとする。
iii. ログデータは収集され、他のログエントリと関連付けられ、データ保持に関する法律で制限されていない限り、少なくとも3ヶ月間保存すること。

e. 訪問者管理システム:
i. 訪問者管理システムを導入し、訪問者の出入りを特定、追跡、規制すること。
ii. 訪問者は付き添われ、身分証明書、訪問目的、連絡先などの情報を登録する必要がある。
iii. 現場職員と訪問者の識別(例えば、別個のバッジの割り当て)、および現場職員と期限切れの訪問者の識別の取り消しまたは終了のための手順を作成すべき。

f. 認証と認可のメカニズム:
i. 全ての物理的アクセスには、生体認証、アクセスカード、その他の認証方法を組み合わせた多要素認証

（MFA）を採用すること。 ii. アクセスは許可された担当者のみに制限し、本人確認と特定のエリアやリソースを利用する資格を確認する。 g. アクセス制御システムの監視と監査： i. 全ての物理的アクセス制御イベントに対して、リアルタイムの監視と監査を実施する。異常または不正なアクセス試行に対する自動アラートを設定すること。 ii. アクセスログとインシデントレポートを定期的にレビューし、繰り返し発生するパターンや潜在的なセキュリティリスクを特定すること。 iii. アクセス管理措置の有効性を評価し、改善すべきドメインを特定するために、セキュリティ監査を定期的に実施すること。	

Control Title	Control ID	Control Specification
障害と異常の報告	**LOG-13**	モニタリングシステムの異常や障害を報告するためのプロセス、手順および技術的手段を定義、実施および評価し、説明責任者へ即時通知する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の目的の決定は、採用されるクラウドアーキテクチャに関係なく変わらない。この管理策は、CSP と CSC によって独立して実施される。ログとバックアップがポリシーに従って取得され、維持されていることを確認するために、ロギングプロセスの実行パフォーマンスを監視すべきである。ロギングに関連する障害は特定され、代替のリカバリステップを使用して修正すべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、ロギングおよび監視の障害のタイプに応じて、取るべきアクションを定義するべきである。異常には、ソフトウェアエラー、ログの一部または全部の取得の失敗、監査ログのバック	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

アップの失敗、ストレージ超過の通知などがある。このガイダンスは、全ての情報システムログに適用されるものとする。

CSP は、以下のような（ただしこれに限定されない）重要なセキュリティ管理システムの障害を適時に検出および報告するプロセスを実装すべきである：

a. 監視システムの種類
   i. ファイアウォール
   ii. IDS/IPS
   iii. ファイル整合性監視（FIM）
   iv. ウイルス対策ツール
   v. 物理的アクセス制御
   vi. 論理的アクセス制御
   vii. 監査ログの仕組み

監視システムの異常および障害を検出し報告するためのベストプラクティスには、以下が含まれる（ただし、これらに限定されない）：

a. 監視のベースラインとしきい値：
   i. 重要業績評価指標（KPI）および評価指標のベースラインは、監視システムの正常な動作を表すように設定し、潜在的な異常や障害を示すしきい値を設定する。
   ii. しきい値は、ワークロードのパターン、リソースの利用状況、サービスレベルアグリーメント（SLA）などの要因を考慮し、特定のクラウドサービスやアプリケーションに合わせて調整すべきである。
   iii. 機械学習アルゴリズムを活用して、過去のデータを分析し、従来のしきい値処理では捉えられないような異常を特定する。
   iv. 正常なシステム動作からの逸脱を識別し、潜在的な異常や障害にフラグを立てるために、パターン認識アルゴリズムを採用すること。
b. システム動作のログ：監視システムには、次のようなログ機能を組み込むべきである。タイムスタンプ、イベントタイプ、エラーメッセージなど、システム動作に関する詳細情報
c. イベント相関の活用：イベント相関技術を使用して、ログに記録されたイベント間のパターンと関係を特定する。
d. アラートメカニズム：アラートメカニズムは、検出された異常または監視システムの障害が定義されたしきい値を超えた場合に、関連する利害関係者に通知をトリガーするために統合され、自動化されていること。
e. 相関と集約：異常の根本原因を特定し、システムの健全性をより全体的に理解するために、複数のソースからのデータのパターンを特定・分析するために、相関・集約技術を活用すること。
f. イベントストリーム処理（ESP）： ESP 技術を導入し、監視システムからのリアルタイムデータストリームを処理することで、異常や障害をほぼ瞬時に検知し、迅速な対応と緩和活動を促進すること。

g. 説明責任者への通知； i. 通知の受領、問題のトリアージ、是正措置の実施を担当するセキュリティ専門家またはチームを特定し、通知されること。 ii. サードパーティー製の通知ツールを統合し、柔軟性を高める（カスタムのインシデント管理システムや自動通信用のチャットボットなど）。 h. 自動応答メカニズム：監視システムに異常や障害が発生した場合、修復アクションを開始するためのレスポンスメカニズムを監視システムに実装する（可能であれば自動化する）（例：サービスの再起動、リソース割り当ての調整、ロールバックまたはフェイルオーバーメカニズムのトリガー）。 i. 継続的な監視と評価： i. 異常および障害報告プロセスの有効性を継続的に監視し、評価すること。 ii. 通知ログ、応答時間、解決率は定期的に見直され、教訓に基づいて更新されること。	

Control Domain SEF

2.14　セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジック(SEF)

Control Title	Control ID	Control Specification
セキュリティインシデント管理ポリシーと手順	**SEF-01**	セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックのためのポリシーと手順を確立、文書化、承認、周知、実装、評価、維持する。少なくとも年 1 回、ポリシーと手順をレビューし更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC の両方が、セキュリティインシデント管理に関する独自のポリシーと手順を独自に確立する必要があるため、この管理策の所有は「依存しない形で共有」である。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** セキュリティインシデント管理、E-ディスカバリ、クラウドフォレンジックのポリシーと手順は、役割と責任を明確に定義し、クラウドサービスモデル（IaaS、PaaS、SaaS）ごとに確立し、文書化する。可能であれば、KSSRI（Key Shared Security Responsibility Indicator）または KSCSRI（Key Shared Cloud Security Responsibility Indicator）を使用して、共有責任を特定する。 ポリシー、手順、および支援システムは、フォレンジックの保管の連鎖に関する規定を組み入れるべきであり、そのような証拠が法的に認められるようにすべきである。 CSP は、インシデントの管理、e ディスカバリおよびフォレンジックに基づく調査の実施に関して規定された会社ポリシー、リソース管理、規制および保険の要件を確立し、これに従う責任を負う。CSP は、CSC に代わってフォレンジックに関する知識を維持したり、フォレンジック調査を実施したりする責任を負わ	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

ない。ただし、CSP は、フォレンジックに基づく調査中、特にインシデントが CSP およびサプライチェーン内の第三者ベンダーに起因する可能性がある場合は、CSC と協力すべきである。

ポリシーと手順には、IR ライフサイクルのフェーズを含め、CSC に影響を与えるセキュリティインシデントについて CSP がいつ CSC に関与すべきか、及びインシデント発生中に CSP が最新情報を提供することが期待される頻度を示すべきである。

CSP は、セキュリティインシデント管理、E ディスカバリ、及びクラウドフォレンジックの各ポリシーを組織内で伝達すべきであり、CSC のアウェアネスために IR ポリシーを公表または共有してもよい。

ポリシーには、適切に評価し、対応し、学習し、伝達する能力を有する中核的で資格があり、かつ常設の IR チームの設置を義務づけるべきである。
ポリシーには、以下に関する規定が含まれるべきである（ただし、これに限定されない）:

a. インシデントハンドリングプロセス：IR プロセスにおけるアクティビティのタイムスタンプ記録は、評価指標、SLA、サービス回復、および可用性のために必要である。
b. 検出：
   i. インシデントの原因となったアクティビティの場所：SaaS（例えば、api、GUI、ユーザー、データ）、PaaS（例えば、api、GUI、ユーザー、アプリケーション、データ）、IaaS（例えば、PaaS（例：api、GUI、ユーザー、アプリケーション、ソリューションスタック、VM、データ）、又はハイパーバイザ、OS、コンピュート及びストレージ、ネットワーク、又は施設におけるイベントソースログ、及びアクティビティ（成功及び/又は失敗）ログに責任を持つ当事者（CSP 又は CSC のいずれか）、並びに検知及びその他のセキュリティインシデント管理フェーズに使用されるログの可用性を含む。
   ii. 自動アラート機能を備えた高度な検知ツール（行動ベースおよびルールベース）を CSP と CSC の双方に導入して、潜在的なインシデントの早期検知と兆候を示すとともに、エンドユーザーと第三者がチケット、電子メール、ヘルプデ スクへの電話、またはその他の利用可能なチャネルを介してインシデントを自己報告するためのメカニズムを提供する。
c. 分析：
   i. このプロセスには、Mitre ATT&CK IaaS, PaaS, SaaS の戦術とテクニックを参照することも含まれる。
   ii. インシデントの範囲、種類、影響（機能的および情報的）、重大性を定義する必要があり、これにはインシデントに関係するデータ分類（個人データ、最高機密、秘密、機密、健康など）も含まれる。

iii. データ侵害、DDoS、マルウェア、データ漏えい（DL）に関連する主なインシデント、エクスプロイトの種類、ローカル対リモート、内部対外部、境界、管理プレーンのインシデント、予想される IR の手順と結果について、CSC のクラウド環境が影響を受ける場合に理解し、実証すること。

iv. 参考にしたインシデントの分類と分類技術
組織が承認した情報源（US-CERT 連邦インシデント通知ガイドラインや FedRAMP インシデント通信手順など）。CSC は、CSP のカスタマインシデント対応チーム（CIRT）を介して CSP のサポートを得ることができる。

d. 封じ込め：

i. 最も一般的な封じ込め技術（ネットワーク、フィルタリング、ルーティング、トラフィックを拒否するためのファイアウォールやポートルールの変更、トラフィックフィルタリングや隔離など）は、通常 CSP の責任であり、有能な SIEM/SOAR、ロジックアプリ、およびワークブックによって自動化できる。

ii. CSP は、攻撃者がその機能を引き続き悪用する能力を低減または除去することで、セキュリティインシデントを抑制する必要がある。

iii. CSP は、フォレンジック証拠が漏洩しないようにし、読み取り専用のバックアップを取るか、スナップショットを作成する（クラウドブロックストレージスナップショットなど）。

iv. CSP は、影響を受けたシステム、デバイス、クラウドサービス、アプリケーション、および人から収集されたフォレンジック証拠の管理の連鎖に関するガイドラインに従うべきである。
これらのポリシー、手順、およびサポートシステムは、法的に認められる証拠をもたらすべきである。

e. 根絶：

i. 根本原因に対処し、環境をセキュアな状態に戻す責任は、CSP と CSC の間で定義するか、共有する場所を示す必要がある（例えば、マルウェアの削除は CSP と CSC の両方の責任となる可能性がある）。

ii. エクスポージャの閉鎖、認証情報の削除またはリセット、鍵のローテーション/失効の実行、インスタンスの停止、セキュアなリソースへの移動、特権アクセスの制限、最小特権の確保、知る必要性、および使用する必要性の原則に対する責任は、適宜更新されるべきである。

f. 回復：

i. バックアップからのリストアは、同じ CSP 内または別の CSP 内のバックアップ戦略に応じて、ポリシーに示され、BCP または DR 計画に従って、リソースの優先順位を設定しされた順次リストアとリカバリを維持する必要がある。

ii. CSP と CSC の両者は、オートスケーリンググループ、ストレージの増加、データ消費量の増加など、サービスを提供するリソースが動的に拡張された場合、適応可能な RTO/RPO 機能によってスケーラブルな環境の変化するニーズに対応する必要がある。

iii. 復旧を達成するためのシステムの再構築とリソースの割り当て、および復旧した環境のセキュリティを確保するための責任を、CSP と CSC の間で定義する必要がある。

g. 事後検証：

i. CSP と CSC が合意した場合、将来のインシデントを防止または軽減するために、環境に対する構成変更を推奨し、教訓を含み、IR プロセスとトレーニングのための KPI を定義して実施する。

h. レスポンスタイム協定：

i. CSP と CSC の間でセキュリティインシデントの重大度と対応時間について合意する。

ii. 組織が承認した業界標準を参照すること。

i. CSC とのコミュニケーションパス：セキュリティインシデントに先立ち、ポリシーと手順において以下の事項を定義する：

i. 報告経路：どの種類のセキュリティインシデントを CSC に報告すべきか。

ii. エスカレーション経路：セキュリティンシデントが発生する前の CSC とのエスカレーション経路

iii. 通知経路：可能であれば、セキュリティンシデント管理ツール、または電子メールによる警告サービスを介して自動化する。帯域外の通知経路を定義する必要があるかもしれない。IR ポリシーと手順には、規制及び法的要件、特に「情報漏えい通知」要件に従った通知要件及びタイムラインを含める。該当する場合は、連邦インシデント通知ガイドラインを参照する。

j. IR 計画のテスト：

i. CSP と CSC の両者およびその他の関係者の参加を得て、紙上ウォークスルー/テーブルトップ演習またはシミュレーションにより、IR 計画を定期的にテストする。

k. 承認組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与

i. ポリシーと手順の変更または修正については、承認プロセスを確立すべきである。

ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。

l. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進すべきである。

m. メンテナンスとレビュー：セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックのポリシーと手順は、進化するクラウドセキュリティ環境との整合性を確保

し、クラウド技術、規制、リスクの変化を反映するために、少なくとも年１回は文書化し、見直し、更新する。	

Control Title	Control ID	Control Specification
サービス管理ポリシーと手順	**SEF-02**	セキュリティインシデントの適時な管理のためのポリシーと手順を確立、文書化、承認、周知、実装、評価、維持する。少なくとも年１回、ポリシーと手順をレビューし更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP 及び CSC は、セキュリティインシデント管理のための独自のポリシーと手順を独自に確立するため、本管理策の所有は「依存しない形で共有」である。当該ポリシーと手順は、フォレンジック証拠の保管連鎖及び CSP と CSC 間の法的義務を含め、セキュリティインシデント管理プロセスの全段階を通じて KSSRI または KSCSRI の使用に関する役割と責任、及び共有される責任を明確に定義するものとする。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** ポリシーには、以下に関する規定が含まれるべきである（ただし、これに限定されない）： a. CSP-CSC コラボレーション：CSP と CSC の間でインシデントを報告するよう指定された要員、設定された時間枠、およびインシデント管理の実務について CSC と CSP に適用される影響度と重大度の評価について合意する。これにより、CSP または CSC によって分類されたインシデントが、インシデントを封じ込め、根絶するための適切な対応策を否定したり、指示したりすることがないようにする。また、どちらか一方の当事者による適切な対応策（例えば、個人情報漏えいは DDoS 攻撃よりも短い対応時間を必要とする）、インシデントのライフサイクル全体を通じて報告書を提出する頻度、およびインシデントの報告方法について理解を深める。 b. 役割と責任：インシデントおよびイベント管理のライフサイクル全体における担当者の明確な役割と責任が定義され	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

るべきである。

c. 予防的対策：可能であれば、多層防御戦略、最小特権モデル、知る必要性モデル、使用する必要性モデル、およびゼロトラストモデルに従った予防措置を含めることにより、IR 時間を短縮することを目指す。一部の防御メカニズムは、サービスの一部として、または CSC の費用負担で CSP から提供される。

d. SOA での IR 自動化 ：Security Orchestration and Automation Response（SOAR）ソリューションによる自動化に対応し、インシデントの警告、封じ込め、修復、および根絶までの時間を自動的に短縮する（例えば、マルウェア攻撃が検出された場合、影響を受けたシステムを隔離し、SOAR でプログラムされたとおりに自動的にクリーニング、イメージの再作成、またはその他の活動を実行する）。CSP は、SOAR 技術が使用される場合に CSC に提供可能な自動応答を定義する必要がある。

e. IR の封じ込め：封じ込め戦略における CSC と CSP の役割を明確にする。また、タイムリーで費用対効果の高い封じ込め及び管理を確実にするために、インシデントの封じ込め方法を通知する所定の標準を手順書に定めるべきである。KSCSRI の使用は、CSP と CSC がそれぞれの封じ込め責任を確実に認識するのに役立つ。

f. 証拠のクラウド保管：証拠の保管のために、別のクラウドアカウントまたは別の CSP の利用を検討する。CSP はこの方法を CSC に通知する必要がある。

g. 承認組織の戦略目標及びリスク選好度との整合性を確保するための承認要件及び上級管理職の関与

   i. ポリシーと手順の変更または修正については、承認プロセスを確立すべきである。

   ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。

h. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進すべきである。

i. 維持管理とレビュー：セキュリティインシデントの管理に関するポリシーと手順を文書化し、少なくとも年 1 回レビューし、更新する。

CSP と CSC の双方にとって、セキュリティインシデントを適時に管理するためのその他のポリシー及び手順に関する考慮事項には、以下の合意事項を含めるべきである：

a. IR アラート：イベント、重大性、影響、脅威インテリジェンスに基づき、アラート手順を定義し、定められた時間枠内で実施する。

b. IR 対応時間：契約上の合意または SLA に従った、インシデントの重大性に応じた対応時間（セキュリティレベルごとに分単位／時間単位とするなど）

c. KSCSRI は、証拠取扱いの各発生日時（タイムゾーンを含む）、インシデントに関連する情報または証拠の作成

（セキュアな監査、ロギング、監視を通じた）、収集、セキュアな保管（暗号化と完全性を伴う）、および転送に関する共有責任を調査するために使用される。KSCSRI の使用は、証拠保管に別の CSP が使用される場合に、CSP と CSC の間で責任の所在が変わるとき、またその逆のときを特定するのに役立つ。 d. RTO 指標：RTO と SLA に基づく復旧時間枠。KSCSRI を使用することで、これらの要求時間枠を満たすことができる。 e. IR 記録：CSP と CSC の間で合意された時間枠に従って通知、報告、連絡を行う指標を含む、インシデントライフサイクル中の全活動の時系列記録。 CSP は、セキュリティインシデント管理、E ディスカバリ、及びクラウドフォレンジック、サービス管理のポリシーと手順を組織内で伝達するものとし、インシデント対応ポリシーを公表するか、または CSC と共有して周知を図ることができる。	

Control Title	Control ID	Control Specification
インシデントレスポンス計画	**SEF-03**	セキュリティインシデントレスポンス計画を確立、文書化、承認、周知、実装、評価、維持する。本計画には、関連する社内部門、影響を受ける CSC、影響を受ける可能性のあるその他のビジネス上での重要な関係（サプライチェーン等）が含まれるが、これらに限定されない。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： インシデント対応計画の管理策の所有は「依存しない形で共有」である。これは、CSP と CSC の双方が独自にセキュリティ IR 計画を策定し、責任を負う必要があるためである。IR 計画は、役割と責任を明確に定義し、可能であれば KSSR または KSCSRI を使用して責任共有を定義する。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：**	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

IR 計画は、SEF-01 の実施ガイドラインに関連し、IR ライフサイクルの全ての段階において、対応するポリシーと手順の要件が確実に組み込まれるようにする。

IR 計画は、組織のクラウド製品及びサービス（SaaS、PaaS、IaaS）のセキュリティインシデントを効率的に管理できる方法論を提供し、連携した対応を実現するために依存する CSP のサービスを明確に定義する必要がある。IR 計画が策定され、文書化されたら、計画は承認され、伝達される必要がある。

IR 計画には、以下の条項を含めるべきである：

a. スコープ：IR 計画は、社内の依存関係（IT、運用、サポート、法務など）と社外の依存関係（サプライヤ、ベンダー、パートナー、顧客、その他の第三者）の両方に適用されるべきである。対象範囲のクラウドサービス、システム、アプリケーション、ユーザー、およびデータで、イベントとインシデントを監視する。対象範囲のネットワークとインフラストラクチャが CSP によって監視されていることを確認する。
b. インシデント対応チームと利害関係者：利害関係者には、インシデントに関する情報を受け取る顧客、法執行機関、および／またはインシデント管理に関与できる者が含まれる。
c. インシデントの追跡と分類：インシデントの記録に使用する問題と追跡システムを定義する。脅威インテリジェンス、PaaS、IaaS および SaaS の戦術と技術に関する攻撃ベクトル分類法 Mitre ATT&CK、および関係するデータ、インシデントのスコープ、影響に関するデータ分類を使用して、インシデントを重大度と緊急度（高、中、低、大、小など）によって分類する。
d. 対応のタイプと予想される対応時間枠：計画では、CSP または CSC によって手動対応と自動対応のどちらが求められるか、いつまでに対応するか（例えば、平均確認時間（Mean Time to acknowledge aka MTTA））、いつまでに CSP または CSC がインシデントを報告する必要があるか、誰がインシデントの封じ込めに責任を持つか、封じ込めまでの平均予想時間（MTTC）を示すべきである。対応は、暗号化セキュリティサービスを復旧するための暗号化鍵漏洩復旧計画など、後続の IR 計画を呼び出すことができる。
e. 証拠の収集と取扱い：証拠を収集し、その完全性を維持するための手順、いつ、どこでコピーを作成するか、分析のために正確な複製をいつ使用するか、ログ、その他の収集された証拠、制限付き読み取り専用リポジトリへの保管、別アカウントまたは別の CSP の使用、ハッシュ手順、および法的手続において証拠としての適格性を確保するため管理の連鎖に関する CSP または CSC の責任を提示する。
f. インシデントのライフサイクルのフェーズと手順：インシデントの準備、検知と分析、根絶と復旧、各フェーズでの継続的な分析による有効性の判断、IDS/IPS などの CSC の予防措置、および責任分担によるインシデントの具体化の手順。
g. 役割と責任：インシデント対応に関して CSP と CSC の間で

共有される共通のセキュリティ責任：

i. クライアントとエンドポイントのインシデント - (SaaS) 共有 CSC と CSP

ii. アイデンティティとアクセスのインシデント - (PaaS, SaaS) CSC と CSP の共有

iii. アプリケーションインシデント - (PaaS) 共有 CSC および CSP

iv. ネットワークインシデント -(IaaS) CSC と CSP の共有

v. ホストインシデント - (IaaS) 共有 CSC および CSP 共通の非共有責任

vi. データの分類と説明責任に関するインシデント - CSC

vii. クライアントおよびエンドポイントのインシデント（IaaS、PaaS） - CSC

viii. アイデンティティとアクセスのインシデント（IaaS） - CSC

ix. アプリケーションインシデント（IaaS） - CSC

x. アプリケーションインシデント（SaaS） - CSP

xi. ネットワークインシデント（PaaS、SaaS） - CSP

xii. ホストインシデント（PaaS、SaaS） - CSP

xiii. インフラインシデント（IaaS、PaaS、SaaS） - CSP

h. 通知と報告：CSP および CSC の要員、サードパーティーの要員、および通知用の配信リスト。インシデントおよびサービス停止情報が公開され、定期的に更新される内部および外部の Web サイトまたはポータルを使用して、主要サービスに影響するインシデントの状況を通知する。US-CERT（米国連邦政府機関および連邦政府に代わって運用されるシステムに必要)は、連邦インシデント対応センターとして機能する。

i. ビジネス影響評価の情報：CSP および CSC は、各資産、システム、アプリケーション、および関連する機微データについて、所有者、関連する社内部門、上流/下流の相互依存関係、サービス（IaaS、PaaS、SaaS)、および影響を受ける可能性のあるその他のビジネスクリティカルな関係（サプライチェーンなど）を特定した BIA 情報を持っている必要がある。

j. 参考情報：事業継続性を維持するために、CSC と CSP の間の合意に従って、影響を受けるサービス、ログ、およびデータをリストアするためのバックアップからのリストア手順について、特定のシステムまたはシステムセットの適用される RPO、RTO、および MTD を決定する方法に関する情報。リストア、再構築、置換、リダイレクト、または削除など、適切な根絶および復旧の選択肢を選択するために必要な標準を概説する。

k. スケジュール：計画のレビュー、テスト、評価、維持、承認のスケジュール。レビュー、テスト調整、計画の承認を行う頻度またはスケジュールを定める。

l. テストの計画：実行可能な場合は、スケジュールに定められたとおり、CSP と CSC の両方の参加を得て、紙上でのウォー

クスルー/テーブルトップ演習またはシミュレーションを実施する。計画を評価し、適宜維持／更新する： i. 得られた教訓を踏まえて、計画をテストした後 ii. 例えば、新たな攻撃ベクター、封じ込め戦略、フォールスポジティブ(偽陽性)、フォールスネガティブ(偽陰性)、対応計画からの逸脱、侵入テストから検出されたエクスポージャなどである。 iii. 時機：サービス（IaaS、PaaS、SaaS)、重要な資産、アプリケーション、機密データが追加または削除されたとき。 iv. 計画の再承認：必要な全ての変更がなされた後、計画は再承認されるべきである。 v. 変更管理：IR 計画には、計画がいってストされたかを示す文書管理セクションと、各反復に伴う計画内容の変更点を示すセクションを設けるべきである。	

Control Title	Control ID	Control Specification
インシデントレスポンスのテスト	**SEF-04**	予定された間隔で、あるいは組織や環境が大きく変化した場合に、インシデントレスポンス計画をテストし、必要に応じて更新し、その有効性を確認する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC の両方が、それぞれの組織の IR 計画を独自にテストし、更新する必要があるため、管理策の所有は「依存しない形で共有」である。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** a. 全ての連絡先および IR チームメンバーの確認と更新 b. 内部依存関係（IT、運用、サポート、法務など）と外部依存関係（サプライヤ、ベンダー、パートナー、顧客、その他の第三者）の両方について、IR 計画の範囲を検証し、更新する。スコープに含まれるクラウドサービス、システム、アプリケーション、ユーザー、デ	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

ータについて、イベントとインシデントを監視する。対象範囲のネットワークとインフラストラクチャがCSPによって監視されていることを確認する。

c. IRテストの範囲を定義する（例えば、IR計画テストのための環境は、以下の選択肢を含むべきであるが、これらに限定されるものではない。代替の非本番環境、およびサードパーティーのCSPクラウドサービス/アカウント）

d. 例えば、攻撃手口（初期アクセス、実行、永続化、権限昇格、防衛回避、認証情報へのアクセス、探索、ラテラルムーブメント(侵入拡大)）を使用して、IR計画をテストする脅威のドメインを決定する。IaaS、PaaS、SaaSの戦術とテクニックに関するMitre ATT&CKを使用した攻撃ベクトル分類プロセスに従い、インシデントにつながるイベントと活動をシミュレートする。

e. IR計画テストのスケジュール – 計画に定められているとおり、参加者、CSP、およびCSCとの会議を手配する。

f. IR計画およびインシデントの全てのフェーズに続いて、紙のウォークスルーまたはシミュレーションを実施する。計画に記載された全ての時間制限のある活動やステップを成功裏に完了したことを示す指標や指標を得るために、テスト活動の時系列ログを維持する。

g. 手動プロセスおよび自動化されたインシデント管理機能、検知、アラート、プレイブック、ロジックアプリ、ルール、封じ込め、根絶、復旧戦略の調整テスト、レビュー、更新

h. 組織のBCおよびDR計画とIR計画を照合し、不一致に対処する。

i. IR計画のテスト結果を文書化し、伝達する。その結果、テスト中に失敗した分野、対応方法から逸脱した分野、封じ込め戦略、フォールスポジティブ(偽陽性)、フォールスネガティブ(偽陰性)、または実行できなかった分野に対処するアクションアイテムが示される。

j. 矛盾や失敗に対処するために計画を更新し、計画の再承認を得る。

また、CSPとCSCは以下の際にIR計画をテストし、更新し、改善する必要がある：

a. 重要な組織変更時

b. 外部サプライチェーンの混乱と自然災害時

c. セキュリティ攻撃、特にセキュリティ侵害につながる攻撃時

Control Title	Control ID	Control Specification

インシデントレスポンスの評価指標	SEF-05	情報セキュリティインシデントの評価指標を確立し、監視する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： これは、適切なセキュリティインシデントの測定基準が設定され、監視されることを確実にするために、CSP と CSC の間の責任共有である。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン； **全てのサービスモデルに適用：** 効果的なインシデント管理を支援するために、運用プロセスや技術的管理の弱点を検出するためのセキュリティ指標を確立し、監視し、分析する必要がある。 CSP は、以下に関連するセキュリティインシデント評価指標を定義、実装、および監視するものとする： a. 仮想エラスティックコンピュート、サーバーOS、ストレージ、ネットワークなど、全てのサポートインフラストラクチャ b. ミドルウェア、開発ツール、BI サービス、データベース管理システム c. CSC との契約に基づき設定されたアプリケーション セキュリティインシデントの指標を設定し、監視するための実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 検出指標： i. 特定までの時間（TTI）評価指標は、インシデントを特定するまでの平均時間を測定する。 ii. 誤検知評価指標は、実際のインシデントではなかったアラートの割合を追跡する。 b. レスポンスの指標： i. TTC（Time to Contain）は、損害を隔離し、それ以上の損害を防止するまでの平均時間を測定する。 ii. 平均応答時間（MTTR）評価指標は、インシデントに対応し、完全に解決するまでの平均時間を追跡する。 c. 復旧の指標：	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。 さらに、CSC は、CSP との契約に基づき、職員によるアプリケーションへのアクセスに関連するセキュリティインシデント指標を定義し、実施し、監視すべきである。

i. データ復旧時間（DRT）は、影響を受けたシステムやデータを復旧させるまでの平均時間を測定する（インシデントによるダウンタイムなど）。 ii. ダウンタイムコスト」指標は、インシデントによるサービスの中断が財務に与える影響を追跡する。 d. セキュリティベントを定量化する： i. セキュリティツールによって生成されたアラートの量を追跡するセキュリティアラート数評価指標 ii. インシデント量評価指標は、監視するイベントの量と、インシデントに対するイベントの比率を監視する。 e. ビジネスへの影響： i. ダウンタイム指標は、セキュリティインシデントによるサービスの中断期間を追跡する。 ii. データ損失評価指標は、インシデント発生時に漏洩したデータ量を測定する。 f. SLA におけるインシデント指標セキュリティインシデント評価標準のベースラインと目標を SLA に定め、CSC に対する透明性と説明責任を確保する。 g. 評価指標の優先順位を設定し：事業継続と CSC への影響（例：重要システムの MTTR）に焦点を当てる。 h. インシデントの指標を監視する： i. SIEM ソリューションを活用して、セキュリティデータを収集、分析、可視化し、潜在的なインシデントに関する洞察をリアルタイムで提供する。 ii. SIEM ソリューションは、選択した評価指標について事前に定義されたしきい値に基づいて、不審なアクティビティに対する自動アラートをトリガーするように構成されるべきである。 i. インシデント指標の見直し： i. セキュリティインシデントの指標を定期的に見直し、改善すべきドメインを特定するとともに、インシデントや進化する脅威から学んだ教訓に基づいて更新する。 ii. 改善すべきドメインを特定するため、（可能な場合は）業界標準や他の CSP と指標を比較すべきである。	

Control Title	Control ID	Control Specification
イベントのトリアージプロセス	**SEF-06**	セキュリティ関連のイベントをトリアージするためのプロセス、手順、および技術的措置を定義し実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； セキュリティベントの効果的なトリアージには協力が必要であるため、CSP と CSC の間の実施責任は、通常、共有されるとともに依存する。トリアージは、両当事者に影響を与えるセキュリティベント（及び潜在的なインシデント）の特定、 評価、優先順位を設定し、及び対応に使用される。CSP は、セキュリティイベントの潜在的な発生源や根本原因に関する貴重な洞察を提供することができ、CSC は、自社のデータ、構成、アプリケーション、ユーザー活動に特有の情報を提供することができる。この共同作業は、イベントの範囲と潜在的な影響を特定するのに役立ち、より的を絞った効率的な対応につながる。 例えば、IaaS インフラのプラットフォームレイヤーで発生したセキュリティンシデントは、CSC と CSP が共同で対応し、CSC の環境に起因するものか、CSP の環境に起因するものかを判断する。 これには、影響を受けたリソースの隔離など、CSP が実施する封じ込め措置が含まれる可能性がある。一方、CSC は特定の事象に応じて、ユーザーアカウントの停止やデータ復旧などの措置を講じることができる。	**管理策所有権の根拠；** CSC の責任には、不審な動きがあれば速やかに CSP に報告すること、及び契約上の合意に従って、セキュリティベント（及び潜在的なインシデント）を評価し、優先順位を付け、対応するために CSP と協力することが含まれる。
実施ガイドライン： **全てのサービスモデルに適用：** 全てのセキュリティベントが適時に調査・評価されるよう、トリアージ管理プロセスが完全に文書化され、毎年見直され、承認される必要がある。 CSP は、仮想エラスティックコンピュート、サーバーOS、ストレージ、ネットワーク並びにミドルウェア、開発ツール、BI サービス、データベース管理システム、および CSC が使用するように構成されたアプリケーションについても、全てのサポートインフラストラクチャのトリアージプロセスを実行する必要がある。 CSP は、セキュリティインシデント管理プロセスが契約上合意されたとおりに実施されることを保証するために、トリアージプロセスを可視化すべきである。 セキュリティベントのトリアージに関する実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）：	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。 さらに、CSC は以下のベストプラクティスを遵守すべきである： a. CSP 契約に基づくインシデントコラボレーション： i. CSP との契約により、セキュリティインシデント発生時の責任と対応スケジュールを明確に定義する。 ii. CSP にセキュリティインシデントを報告するための、CSP との契約上の合意に概説されている通信プロトコルを十分に理解する。 iii. セキュリティインシデントに関する関連情報を迅速に共有するために、CSP とのコミュニケーションチャネルを確立すべきである。 iv. CSC は、CSP のトリアージプロセスを可視化し、セキュリティンシデント管理プロセスが契約上の合意に従って確実に実施されるようにすべきである。

a. 利害関係者の協力：
   i. 社内のセキュリティチーム、CSC のサポート、及びインシデント対応に関与する外部パートナーについて、契約上の合意に従って、役割と責任を確立する。
   ii. 社内チーム、影響を受ける CSC、及び規制機関（必要な場合）を含む関連利害関係者に通知するためのコミュニケーション計画を策定する。
b. イベントの分類スキーム：イベントの優先順位を設定し支援するために、重大度、潜在的影響、緊急性に基づいてセキュリティベントを分類する標準的な方法を定義する。多段階のアプローチも考えられる：
   i. Tier1. 低リスクのイベントには、自動封じ込めと基本的な調査（不審なログイン試行など）が含まれる可能性がある。
   ii. Tier2. 中程度のリスク事象の場合、より詳細な調査が必要であり、CSC に通知する可能性がある（マルウェア感染の可能性など）。
   iii. Tier 3. リスクの高い事象が発生した場合、早急な対応、完全な調査、規制当局への報告の可能性がある（データ漏洩が確認された場合など）。
c. 標準化されたプレイブック：各段階のステップの概要を文書化したプレイブックを作成する：
   i. 初期評価の手順、および発生源、期間、侵害の可能性を示す指標（IOC）を含む、事象に関する初期詳細の収集
   ii. 被害を食い止め、被害を拡大させないための対策を実施すべきである（例：侵害されたシステムの隔離、ユーザーアクセスの制限）。
   iii. 根本原因、インシデントの範囲、潜在的なデータ損失を特定するため、徹底的な調査を実施すること（ログ分析、脅威インテリジェンスフィード、セキュリティツールなど）。
   iv. 脅威を根絶し、影響を受けたシステムを復旧させ、将来の発生を防止するための措置を実施すべきである。
   v. CSC のトリアージプロセスを定義し、実施するにあたっては、CSP のセキュリティチームか らの指導と支援が推奨される。

Control Title	Control ID	Control Specification
セキュリティ侵害の通知	**SEF-07**	セキュリティ侵害の通知のためのプロセス、手順、および技術的措置を定義し実装する。適用される SLA、法令および規制に従い、関連するサプライチェーンの侵害を含む、実際のもしくは想定されるセキュリティ違反を報告する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC の両方が、サービス契約に記載されているとおり、現地の法的及び規制的要件に従ってセキュリティ侵害通知を確実に開示する責任を負っているため、これは「依存しない形で共有」である。ただし、管理策は互いに独立している。両エンティティは、異なる手順、手続、及び技術的管理を必要とする可能性がある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、仮想エラスティックコンピュート、サーバーOS、ストレージ、およびネットワークといった全てのサポートインフラストラクチャ、並びにミドルウェア、開発ツール、BI サービス、データベース管理システム、および CSC が使用するために契約上合意された構成によるアプリケーションについて、セキュリティ侵害および想定されるセキュリティ侵害を報告するプロセスと手順を導入するものとする。 セキュリティ侵害通知の実施に関するベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 侵害通知計画： i. 何をもってセキュリティ侵害とするか、また、通知を必要とするインシデントの種類（不正アクセスの試み、データの流出）を定義すべきである。 ii. 侵害情報は、侵害通知に含まれるべきであり、侵害の性質、影響を受けるデータの種類、潜在的リスク、および講じられた緩和措置を明記すべきである。 iii. 影響を受ける CSC、規制当局、社内の利害関係者を含め、SLA や関連規則に従って、関連当事者に通知する手順を定めなければならない。 iv. 情報漏えいの重大性と関連規制に基づき、影響を受ける当事者への通知の時間枠を定めるべきである（例えば、一部のデータ漏えい法で義務付けられている 72 時間など）。 b. サプライチェーンの侵害通知： i. ベンダーの契約には、CSP のサービスに影響を与えるセキュリティインシデントの通知を義務付ける条項を含めるべきである。 ii. 情報漏えい通知手続きは、データ保護規則に準拠すべきである。 c. 情報漏えいの通知チャネル：セキュリティ侵害について影	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

響を受ける当事者に通知するための適切なコミュニケーションチャネルを確立する。	

Control Title	Control ID	Control Specification
連絡先の維持	**SEF-08**	対応する規制当局、国および地域の法執行機関、およびその他の法的管轄権を有する当局に対する連絡先を維持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC の両方が、適用される規制当局、国及び地域の法執行機関、並びにその他の法的管轄権限を有する当局の連絡先の維持及び文書化に責任を負うため、この管理策は「依存しない形で共有」である。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、関連当局とのセキュリティインシデントの連絡先情報を文書化し維持し、コミュニケーションプロセスを実施し、コミュニケーションチーム（通知を送信する権限を持つ要員）および法執行機関との関与が必要な調査に備えるために外部の規制機関に責任を割り当てる必要がある。 連絡先を維持するための実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）： a. 当局の識別； i. CSP が事業を行う各地域において、関連する規制機関を検索し、特定する必要がある（例：金融規制当局、データ保護当局）。 ii. 活動地域の国家および地方法執行機関内に連絡窓口を設置すべきである。 iii. 国際的な業務のため、CSC データが保存または処理される可能性のある法的管轄区域を特定しなければならない。 b. 連絡先リポジトリの一元化：	**実施ガイドライン；** CSP の「実施ガイドライン」が適用される。

i. 特定された全ての当局の連絡先情報（氏名、役職、電話番号、E メールアドレス、管轄地域、希望する連絡方法など）を含むセキュアなリポジトリが作成されるべきである。 ii. リポジトリは、少なくとも年 1 回、および含まれる当局内の担当者または連絡先情報に変更があった場合に更新されるべきである。 c. コミュニケーションチャネル： i. 当局の種類ごとに通信プロトコルを確立すべきである（例えば、規制機関にはセキュアな電子メール、法執行機関には専用のホットライン）。 ii. クレーム当局から受け取った通信の正当性を検証するプロセスを実施すべきである。 d. 法律顧問：当局とのやりとりを行う際に、適切な手順とデータ共有プロトコルが守られるよう、法律顧問の利用を検討すべきである。	

Control Domain STA

2.15 サプライチェーン管理、透明性、説明責任(STA)

Control Title	Control ID	Control Specification
SSRM のポリシーと手順	**STA-01**	セキュリティ責任共有モデル（SSRM）を適用するため、組織内でポリシーと手順を文書化、承認し、組織内に周知、それを適用し、効果を評価しつつ維持しなければならない。ポリシーと実行手順は、少なくとも年 1 回、レビューと更新を行う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSC と CSP は、それぞれ独自に、SSRM を共有しつつも独立したポリシーと手順を確立し、維持すべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** SSRM は、包括的かつ効果的なサイバーセキュリティリスク管理を確保する上で極めて重要です。CSC と CSP は共同でクラウドサービスの実装、管理、及び監視を行う。様々な管理（例えば、CCM から）は、どちらか一方が行うか、双方が独立して行うか、双方が依存し合って行う。 SSRM はそのための重要なメカニズムである： a. クラウドサービスをセキュアな方法で実装、使用、管理、および監視するために必要な管理を包括的に詳しく説明する。 b. CSP と CSC の間で、管理に関するそれぞれの責任と期待について共通の合意を確立し、文書化する。 c. サービス契約および継続的な契約管理とコンプライアンスの基礎となる。 d. 効果的な継続的統制の実行、管理、監視、評価活動を支援する。 e. 責任の明確化とコミュニケーションの規約により、迅速かつ効果的な IR と管理を促進する。 f. 責任と期待される関係について透明性を高める。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。 異なるクラウドサービスモデルの実装、または特殊なクラウドサービス（IDaaS など）の実装に必要な具体的な手順にも差異があるかもしれない。例えば、IaaS の実装を管理するために採用される SSRM 手順は、IaaS モデル下で CSC に課される責任がより大きいことを考慮すると、SaaS の実装の場合よりも広範囲に及ぶ可能性がある。 CSP のポリシーが適用される。

クラウドサービスの提供をサポートするために、CSP または CSC が関与する他の関係者が関与することもある。例えば、ある CSP が提供する SaaS サービスは、その基礎となる IaaS サービスを提供する別の CSP の利用を伴うかもしれない。サプライチェーンにおける支援サービスプロバイダーのセキュリティ責任も、SSRM に反映させるべきである。

SSRM が効果的なクラウドセキュリティの実践を支援する上で重要な役割を果たすことを考慮すると、CSC と CSP は、それぞれのクラウドサービス全体で SSRM を適用するためのポリシーと手順を確立し、維持すべきである。これにより、全てのサービスにわたる一貫性と適切な適用範囲が保証される。

CSP または CSC に必要な具体的な SSRM ポリシーと手順は、多くの要因に影響される可能性がある。これらは、クラウドサービス特有の考慮事項とリスクに適切に対処するために、調達と契約管理、サードパーティリスク管理、およびサイバーセキュリティリスク管理に関するより広範な組織のポリシーと手順と整合し、これらを補強する必要がある。

さらに、組織の SSRM ポリシーと手順の厳格さと包括性は、その組織が使用または提供するクラウドサービスのリスク、複雑性、重要性に見合ったものでなければならない。例えば、少数の非重要な SaaS サービスを利用する CSC の SSRM ポリシーと手順は、ビジネスが基本的に広範な IaaS に依存している CSC ほど広範で厳格である必要はありません。さらに、セキュリティプログラム管理に対する CSC の期待は、SSRM のポリシーと手順の範囲と厳格さを決定する。

CSP のポリシーと手順は、クラウドサービスの実装において生じ得る多くの CSP および CSC 特有の状況を認識し、考慮するものとする。特に、ポリシーと手順に対する例外は、正式に管理され、適切な管理レベルで承認されるべきである。本ガイダンスは、CSP 又は CSC に潜在的により大きなリスクをもたらす当事者間の契約上のコミットメント（例えば、小規模な組織では交渉力がないために妥協する必要があるかもしれない）に特に関連する。

SSRM ポリシーと手順は、進化するクラウドセキュリティのランドスケープとの整合性を確保し、クラウド技術、規制、およびリスクの変化を反映するために文書化し、少なくとも毎年レビューと更新を行う。更新は、CSP 自身のクラウドサービスの実装から得られた教訓、並びに現行の業界標準およびガイダンス（CCM の現行バージョンや実装ガイドラインなど）を考慮し、取り入れるべきである。さらに、著しく大規模、複雑、かつ／またはビジネスクリティカルなクラウドサービスの実装が計画されている場合、CSP はまず、既存の SSRM ポリシーと手順を見直し、それらが予想されるリスクと複雑性に適切に対応していること

を確認するとよい。 SSRM のポリシーと手順を実装し維持する必要性は、全てのクラウドサービスモデルで同じであるが、異なるクラウドサービスモデルや、特殊なクラウドサービス（IDaaS など）については、必要とされる具体的な手順に違いがあるかもしれない。 例えば、IaaS モデルでは CSC に課される責任が大きいため、IaaS 実装を管理するために採用される SSRM 手順は SaaS 実装の場合よりも広範囲に及ぶ可能性がある。 ポリシーには、以下に関する規定が含まれるべきである（ただし、これに限定されない）： a. 組織の SSRM リスク管理目標 b. SSRM のポリシーおよび手続きを、調達、法務、第三者リスク管理、サイバーリスク管理のポリシーおよび手続きと統合し、整合させる。 c. SSRM をどのように統合し、サービス契約と整合させるか。 d. クラウド配備のライフサイクル全体（デューデリジェンス、契約、導入、管理・監視、サービス終了など）における SSRM 導入の役割と責任 e. デューデリジェンス、管理、モニタリング活動および手順の程度と厳格さに適用されるリスクレベルの定義 f. SSRM が、クラウドサービスの実装のライフサイクルにわたって、CSP との協働により、どのようにレビューされ、検証され、維持されるか（例えば、異なるリスクレベルごとに）。 g. SSRM ポリシーの例外、および／または、責任の配分や遂行に関する問題や例外が、どのように特定され、管理されるか。 h. SSRM プログラムの活動とパフォーマンスに関する報告要件 i. SSRM 関連の決定に必要な承認レベル	

Control Title	Control ID	Control Specification
SSRM サプライチェーン	**STA-02**	クラウドサービスオファリングのサプライチェーン全体に、セキュリティ責任共有モデル（SSRM）を適用、文書化、実装、および管理する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； この管理策の所有は「依存して共有」である。SSRM の初期バージョンは CSP がその製品提供のために開発するが、SSRM の最終化、実装、および管理は協働して行うべきである。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CCM 管理策 STA-02 は、特定のクラウドサービス実装の SSRM が文書化され、実装され、管理される主要な管理策である。 **SSRM の文書** CCM 管理策の STA-03 と STA-04 は、CSP から CSC への SSRM ガイダンス（STA-03）、および CSP と CSC が協働して全ての CCM 管理策のオーナーシップと責任を明確にする（STA-04）という形で、この管理策へのインプットを提供する。 CSC が所有する管理については、CSP は、CSC の SSRM 責任に対する期待に関する明確かつ簡潔なガイダンスを CSC に提供すべきである。 CSP が所有する管理または「(依存しない形で) 共有」の管理については、CSP は、CSP が全面的または部分的に責任を負う管理について文書化する責任を負う。この文書は、サービス提供を完全に文書化し、将来の CSC に SSRM ガイダンスを提供するために、管理策 STA-03 に基づき作成される。CSP は、管理責任を果たすために雇用した第三者の責任を具体的に文書化するものとする。当該文書では、特に、サードパーティー、CSC、および CSP 間で必要な調整について記述する。 共有（依存）」における管理については、CSP は、各当事者の責任が完全に文書化され、STA-04 に基づいて作成された責任の区分と整合していることを確実にするために、CSC と協力するものとする。 SSRM 文書は、サービスレベルの期待、作業負荷管理、連絡、エスカレーション、支援ツール、報告、または CSC と CSP の各責任を管理する上で必要もしくは有用と思われるその他の情報についても言及または参照すべきである。 十分な適用範囲を確保するために、たとえ適用されないと明記されている場合であっても、全ての CCM 管理策は SSRM で扱われ	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

るべきである。さらに、SSRM における責任の明確化は、STA-09 に基づき当事者間で合意された契約条件と整合させるべきである。CSC 及び CSP は、SSRM の特定の詳細について、契約締結後またはサービス実施後まで文書化を延期できるが、SSRM は常に契約上の合意との整合性を保つべきです。

SSRM の実施と管理

一旦 CSP と CSC によって合意されると、特定のクラウドサービス実装のための SSRM は、継続的な関係の多くの側面をガイドする。

各当事者は、SSRM（STA-06 参照）に規定された各 CCM 管理策について、それぞれの責任をもって実施、管理、監視、監査する責任を負う。管理責任に関して疑問や問題が生じた場合は、SSRM 及び契約合意書を参照し、曖昧さに対処し解決すべきである。CSP 及び CSC は、少なくとも年 1 回、サプライチェーンの合意事項及び関連するサービスの SSRM を見直すべきである（STA-10 を参照）。共有セキュリティ責任の変更または明確化に対応するため、SSRM は必要に応じて更新されるべきである。SSRM の更新が必要な場合、CSP は、その更新が特定の CSC の実装に特有なのか、それともサービス全体の SSRM を更新すべきなのかを判断するものとする（STA-03 を参照）。

CSP は、SSRM または基礎となるサービスの管理の継続的な監視および管理を促進するために、自動化されたツールまたはレポートを実装することを選択できる。

CSP と CSC がクラウドサービスの実装のために SSRM を文書化し、実装し、維持する必要性は、全てのクラウドサービスモデルで変わらない。しかし、各 SSRM の具体的な内容は、実装ごとに変わる可能性がある。

Control Title	Control ID	Control Specification
SSRM ガイダンス	**STA-03**	SSRM のサプライチェーンに対する適用可能性に関する詳細情報を、CSC に SSRM ガイダンスとして提供する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： STA-03 の実施責任は CSP のみにある。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、提供するクラウドサービスごとに、SSRM ガイダンス文書を作成すべきである。この文書は、CSP の透明性を実証し、CSP とそれを支援するプロバイダーが提供するセキュリティ責任に対する期待を明確に示すべきである。 管理策 STA-03 と STA-04 は、このガイダンスの策定に対応している。 SSRM ガイダンスは、サービス提供の各管理策に関する CSP の責任、および CSP のサプライチェーン内のサードパーティーが引き受ける必要のある責任を詳述すべきである。ガイダンスは、特に管理策が CSP とそのサプライチェーンとの間で共有される責任を有する場合、可能な限り詳細かつ明確であるべきである。 クラウドオファリングのサービス提供に関与する第三者サプライヤは、SSRM 文書において特定されるべきである。この情報は、CSP がそのサプライヤのセキュリティ責任をどのように管理するかに対応する管理策 STA-12 および CSP のサプライヤ管理に関するコミットメントに対応する STA-09 を補完するものでなければならない。 CAIQ は、CSP が提供するクラウドサービスに関する管理策の所有を文書化するため、徹底的かつ簡便な手段を提供する。 CSP がサービス提供のために CSC に SSRM ガイダンスを提供する必要性は、全てのクラウドサービスモデルで同じである。	**実施ガイドライン：** CSC には適用されない。

Control Title	Control ID	Control Specification
SSRM コントロールオーナーシップ	**STA-04**	クラウドサービスオファリングの SSRM に従って、共有オーナーシップとすべての CSA CCM 管理策の適用可能性を明確にする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

CSP-Owned	CSP-Owned	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： STA-04 の実施責任は CSP のみにある。	**管理策所有権の根拠：** CSC には適用されない。
実施ガイドライン： **全てのサービスモデルに適用：** **SSRM ガイダンス文書** CSP は、提供するクラウドサービスごとに SSRM ガイダンス文書を作成する。この文書は、CSP の CSC に対する透明性を実証し、CSC に期待されるセキュリティ責任を明確に示すべきである。 SSRM ガイダンスは、サービス提供の各管理策に関する CSP の責任、および CSP のサプライチェーン内のサードパーティーが引き受ける必要のある責任を詳述すべきである。ガイダンスは、特に管理策が CSP とそのサプライチェーンとの間で共有される責任を有する場合、可能な限り詳細かつ明確であるべきである。 SSRM ガイダンスは、CSC（または場合によっては CSC のサプライチェーン）が引き受ける CSP の期待についても詳述すべきである。ガイダンスは、CSC が全責任を負うことが期待される管理及び CSP と責任を共有する管理について詳述すべきである。責任を共有する分野については、CSP は、その共有責任がどのように実施され、管理されるかについての期待事項を提示すべきである。 以下の責任区分は、SSRM の各管理策について、また各クラウドサービスモデルについて、文書化されなければならない： a. CSP 所有：CSP は、以下を実施、管理、および評価する全責任を負う。 b. CSC 所有： CSC は、管理策の実施、管理、評価に全責任を負う。 c. 共有（独立）：CSP と CSC の両方が管理策を実装する必要があるが、その実装は互いに独立している。 d. 共有（依存）：CSP と CSC は、管理策の実施、管理、および評価について共同責任を有する。 サービスオファリングの中には、CSP が条件付きで、または追加料金で責任を請け負う管理策もある。例えば、CSP は追加サービス提供としてバックアップサービスを提供することができる。そのような偶発的なサービスや、SSRM 責任が後日決定	**実施ガイドライン：** CSC には適用されない。

される可能性のあるドメインは、SSRM ガイダンスの中で明確にされるべきである。 CAIQ は、CSP がそのクラウドサービスオファリングの管理策の SSRM 所有を文書化するための、徹底的かつ簡便な手段を提供する。SSRM 製品提供ガイダンスは、さらに、他の管理策または製品文書、サービスレベル目標、 テストまたは評価結果、コンプライアンスマッピングなどを参照することができる。 **CSC への指導** CSP は、SSRM ガイダンス文書を CSC になろうとする者に提供するものとする。この文書は、STA-05 管理の下、CSP と CSC との間で行われる SSRM 責任の詳細なレビューの基礎となる。この文書は、販売サイクルにおいて、他の製品情報、CSP の組織情報、技術プレゼンテー ション、販売プレゼンテーションなどによって補強されてもよい。 CSC に提供される SSRM ガイダンスは、透明性を確保し、サービス責任や契約条件に 関連する後々の問題を回避するための重要な要素である。CSP は、それぞれの SSRM 責任を効果的に割り当て、文書化し、実施するために、SSRM の原則と実施について CSC 候補を教育し、支援する準備をすべきである。	

Control Title	Control ID	Control Specification
SSRM ドキュメントレビュー	**STA-05**	組織が使用するすべてのクラウドサービスオファリングの SSRM ドキュメントをレビューし検証する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC は共同で SSRM 文書をレビューし、クラウドサービスオファリングの責任を最終決定する。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン：	**実施ガイドライン：**

全てのサービスモデルに適用： CSP と CSC は、各クラウドサービスの実装について、SSRM 文書とガイダンスを独立して共同でレビューするものとする。CSP については、これらのレビューには、CSC にサービスを提供するために使用されるクラウドサービスだけでなく、組織内部の目的で使用されるクラウドサービス（クラウドベースの財務アプリケーションや人事アプリケーションなど）も含めるべきである。 STA-03 及び STA-04 に基づくクラウドサービス提供のための SSRM ガイダンスは、初期レビューの基礎となるべきである。CSC は、管理策の実施と責任について CSC が有する疑問を明確にするために、合同会議を要請すべきである。CSP は、クラウドサービスの SSRM ガイダンスを調整し改善するために、このフィードバックを利用すべきである。 SSRM の見直しは、SSRM において「(依存する形で) 共有」と指定された管理策に特に焦点を当てるべきである。両当事者は、調整された業務に対するそれぞれの責任を明確にしておくべきである。 レビューには、CSP がオプションとして提供する管理についても議論することが含まれる。CSP は、そのようなオプションサービスの追加料金または条件について、CSC に明確に通知するものとする。 SSRM は、レビューによって正当化される変更を反映するために更新されるべきである。必要に応じて、クラウドサービス契約書も（管理 STA-10 の下で）変更を反映するように更新されるべきです。SSRM 文書と契約書が整合し、一貫していることが重要である。	CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
SSRM コントロールの実施	**STA-06**	組織が責任を負う SSRM の部分を実施、運用、監査、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines

CSP	CSC
管理策所有権の根拠； SSRM の実施と継続的な運用は、CSC と CSP の共有した活動である。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** **SSRM の実施** SSRM が CSC と CSP の間で合意され、契約契約が締結されると、CSC と CSP はクラウドサービスの管理策環境の実装を開始する。関連する統制は、クラウドサービスが構築される際に設計され、コンポーネントがサービスに投入される際に反復的にテストされるべきである。 SSRM に記載されているように、CCM 管理策の一部は CSP と CSC が独立して実施することができる。 CSP と CSC は、SSRM の中で「(依存する形で) 共有」と特定された管理策の実施について調整し、協力することが重要である。これらの管理策は、長期間にわたってある程度の調整が必要となる可能性があるため、当初から管理策の設計と運用を両当事者がよく理解しておくことが重要である。 **SSRM の運用** クラウドサービスの運用中、CSP と CSC はそれぞれ、SSRM において割り当てられた管理策の運用に責任を負う。共有（依存)」と特定された管理策は、当事者の合意により共同で運用される。各 CCM ドメインの「-01」管理策には、管理策の運用の指針となるべき管理策ポリシーと手順が記述されている。 **SSRM の管理、監視、監査** 管理策の実施、運用、および管理は、継続的に監視されるべきである。さらに、管理策は、組織内の独立した監査グループ（すなわち、サードライン機能）及び／又は外部の監査会社により定期的に監査されるべきである。管理策の設計及び運用は、内部の企業リスク管理グループ（すなわち、第二線の機能）によってもレビューされる。 監査・保証（A&A）ドメインは、管理策監査プログラムに関するガイダンスを提供する。さらに、CAIQ は、評価方法を確立するための健全な基礎を提供する。 CSP は、セキュリティ評価の結果を、将来的に CSC になる予定の者と既存の CSC の両方と共有することを期待すべきである。具体的な情報は契約で合意されるべきである。管理策 STA-10 は、既存のクラウドサービス実装における SSRM と契約遵守の継続的な共同レビューについて記述している。管理策 STA-08、STA-	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

13、及び STA-14 は、さらに CSC による継続的なレビューについて記述している。これらのレビューは、SSRM または契約のいずれかを変更する必要があるかどうかを判断する機会を提供する。	

Control Title	Control ID	Control Specification
サプライチェーン・インベントリー	**STA-07**	全てのサプライチェーン関係についてのインベントリを作成および維持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC で独自に実施される。各当事者のサプライチェーン在庫及び在庫管理慣行は、他方から独立している。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、全てのサプライチェーン関係のインベントリを確立し、維持するものとする。このインベントリは、以下を含む様々なサプライチェーン管理活動を支援するために使用できる： a. デューデリジェンスレビューのスケジューリングと調整 b. 契約および法的事項の管理（更新、通知、紛争など） c. SSRM の継続的な管理 d. サプライチェーンリスク管理プログラムの経営陣への報告 e. ライセンス管理 f. 事業継続マネジメントプログラムの BIA g. サイバーセキュリティや可用性のインシデント発生時のコミュニケーション、調整、エスカレーション h. サプライチェーン集中リスクの分析 サプライチェーンインベントリーは、上記の活動を支援するために、必要に応じて、一般的に以下の主要な情報を追跡すべきである：	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

a. 社内およびサプライヤとの連絡先（ビジネスオーナー、リレーションシップマネージャー、法務、技術、サポートサービス、緊急時など） b. サプライヤーリスクランキング c. 一般的な契約条件（契約期間、更新日、解約日など） d. ライセンス数または使用制限 e. 主要なビジネスプロセスサポートまたは依存情報（BIAのサポートなど） f. デューデリジェンス、定期的レビュー、モニタリングの継続的要件とスケジュール CSP は、サプライヤの「リスクランク付け」またはリスクベースの分類スキームの作成を選択することができる。サプライヤのリスクランク付けは、サプライヤのデューデリジェンスと継続的な管理・モニタリング活動の適切な努力レベルと包括性の決定を容易にする。サプライヤのリスクランク付けは、サプライチェーン全体のリスク分析にも役立つ。 CSP は、通常の組織的調達慣行以外の方法で確立されたサプライチェーン関係（製品またはサービスのいわゆる「影の」購入）を特定する、または組み込むための実務を実施することができる。 サプライチェーン在庫の維持管理は、調達及びサプライヤのセキュリティ管理手続に組み込まれるべきであり、在庫維持のための責任を明確に定めるべきである。 インベントリは、契約終了を含め、サプライヤとの関係のライフサイクルにわたる様々な重要な時点で更新されるべきです。インベントリは、少なくとも年 1 回見直し、必要であれば更新すべきである。	

Control Title	Control ID	Control Specification
サプライチェーン・リスクマネジメント	**STA-08**	CSP は、サプライチェーン内の全ての組織に関連するリスク要因を定期的にレビューする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC で独自に実施される。各当事者のサプライチェーンリスクのレビューは、他方から独立している。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** サプライチェーンのリスクは、ほとんどの組織にとって重要である。これらのリスクの評価と管理は、サプライヤとの契約が締結された時点で完了するわけではない。サプライチェーンリスクを監視・管理するための継続的なプログラムが必要である。 CSP のサプライチェーンリスクをレビューするポリシー、手順、および結果は、CSC 候補者による最初のデューデリジェンスレビューの対象となる。CSP は、これらの実務において透明性を確保すべきである。 CSP は、重要性に見合った程度と範囲でサプライチェーン関係を管理および監視するため、必要な知識と経験を有する手順を実施し、十分なリソースを割り当てるべきである（参照管理 STA-07）。 定期的に評価すべきサプライヤのリスク要因の例としては、以下が挙げられる： a. 組織に不利なリスクをもたらす可能性のあるサプライヤの事業姿勢の変化（財務状況、評判、不利なニュース、コンプライアンス／規制上の問題、主要人員の損失、取引関係、消費者からの苦情など）。 b. サプライヤの財務諸表、独立監査報告書、プール／共有評価、独立管理テスト報告書、内部スコアカードおよび評価 c. サプライヤのサービスレベル合意、製品仕様、パフォーマンス指標、リソースレベル／スキルコミットメント、および期待品質の遵守。 d. ソフトウエアの完全性、トレーサビリティ、出所を確保するためのサプライヤのソフトウエアサプライチェーンリスク管理手法（ソフトウエア構築手法、コンポーネント管理、ソフトウエア部品表（SBOM）の使用など）。 e. サプライヤのプログラムと、自社のサプライヤおよびパートナー（第 4 者）を管理する能力、および第 4 者がもたらす可能性のあるリスク。 f. サプライヤまたは第 4 者の海外を拠点とする事業および活動	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

g. 代替ソリューションや撤退戦略・計画の策定を正当化する可能性のある、サプライヤへの重大な依存関係 STA-13 及び STA-14 は、それぞれサプライヤの IT ガバナンスポリシーと手順、サプライヤのセキュリティプログラムの定期的なレビューに関して参照する。継続的なサプライヤの管理とモニタリング、及びより広範なサプライチェーンリスク管理プログラムの構築について、より多くのガイダンスを提供する様々な業界参考資料や標準が入手可能である。 重要な製品またはサービスのサプライヤに対しては、現地訪問および独立監査（契約に規定がある場合）が保証される場合がある。 レビューで特定された懸念事項、契約例外、ポリシー例外、その他のリスクは、必要に応じて契約オーナーおよびその他の責任ある経営陣に報告されるべきである。 特定のサプライヤに関連する継続的なリスクを評価することに加えて、全てのサプライヤにわたる総合的なリスクエクスポージャーを定期的に評価することが推奨される。このような分析では、ベンダー、第三者、地理的、外国拠点、又は組織のサプライヤにまたがるその他のリスク集中要因や依存関係に焦点を当てることができる。 サプライチェーンのリスク管理の活動は、より広範な企業のリスク管理プログラムと整合し、統合されることが推奨される。	

Control Title	Control ID	Control Specification
主要なサービスと契約上の合意	**STA-09**	**CSP** と **CSC** (テナント) の間のサービス契約には、少なくとも次の条項について相互に合意した内容を組み込む必要がある： · 提供されるビジネス関係とサービスの範囲、特徴、場所 · 情報セキュリティ要件 **(SSRM** を含む**)** · 変更管理プロセス · ロギングと監視能力 · インシデント管理とコミュニケーション手順 · 監査および第三者評価を行う権利 · サービスの終了条件 · 相互運用性と移植容易性の要件 · データプライバシー
Control Ownership by Service Model		

IaaS	PaaS	SaaS
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSC と CSP は共同で、クラウドサービス提供のセキュリティ条項に対応する契約書を交渉し、締結すべきです。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** a. 一般的な契約事項 i. クラウドサービス提供の契約は、CSC と CSP との間の法的拘束力のある合意である。契約書と SSRM が一貫していることが重要である。契約に至るまでの営業段階やデューデリジェンス段階で SSRM に確立された期待は、契約に盛り込まれていなければ何の効力も持たないかもしれない。場合によっては、SSRM は契約書の添付資料として含まれることも CSP と CSC は、SSRM における全ての CCM 管理責任がカバーされ、提案された契約に正確に反映されていることをクロスチェックすべきである。 ii. 契約は、支払条件、責任制限、知的財産権など、SSRM やセキュリティに関する考慮事項にとどまらない事項をカバーすべきである。通常、CSP は最初の契約文書案を、あらゆる付属文書や参照規定（オンラインで管理されているサービス提供の説明など）とともに提供する。CSC は、その特定の要件または規制上の期待に対応する雛形の条項を起草することもできる。弁護士（内部弁護士または外部弁護士）は、交渉プロセスや署名前の最終文書のレビューに関与する可能性が高い。クラウドサービス契約や情報セキュリティ問題の経験がある弁護士に依頼することが望ましい。 b. 共通の SSRM とセキュリティ条項 c. クラウドサービスモデル、関係する特定のサービスの性質と範囲、セキュリティ責任の分担に応じて、契約は CCM の管理ドメインの多くに対処することができる。例えば、データのバックアップ頻度、保存場所、およびイミュータブルについては、SaaS サービスの場合、または IaaS サービスの場合、サービス提供に含まれている場合に対応することができる。それ以外の場合、バックアップは CSC の責任であり、契約では特に規定されていない。 クラウドサービスの契約において、対処すべきセキュリティ条	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

項の非網羅的リストには、以下のものが含まれる： a. 研修と意識向上、身元調査、解雇手続き、内部脅威管理などを含む、人事のセキュリティ慣行に関する要件。 b. 様々なタイプの問題に対する可用性とサポート対応に関する SLA（SLA を満たせなかった場合の罰則を含む。 c. 共有される情報の種類と方法に適した秘密保持および守秘義務規定 d. データ保管場所の制限（例：国境を越えたデータ転送）、環境の分離、CSC の分離、データへのアクセス、データの使用、およびデータの廃棄を含む、データ保護およびデータプライバシーに関する考慮事項。 e. 法律、規制、標準、またはその他の契約（ライセンス契約や下請契約など）に準拠するための要件 f. ロギングと監視、ネットワークサービスの保護など、技術的な管理策の実施と維持。 g. コンフィデンシャルコンピューティングおよびワークロードの分離に関する要件（該当する場合） h. ネットワーク接続、API、データ転送、アクセス制御インタフェースの共同メンテナンスおよび監視責任 i. 変更管理に関する責任、コミュニケーション、制約事項 j. 脅威・脆弱性管理および脅威インテリジェンス情報交換に関する条項 k. セキュリティインシデントの報告に関する要件（閾値、最短時間枠、エスカレーションパス、IR における連携と情報共有に関する期待事項を含む）。 l. CSP による BC および DR 計画の維持管理、定期的な復旧計画のテスト、および CSC との共同テストまたは二者間テストに対する期待 m. 冗長サービスの利用可能性を含む、物理的および環境的セキュリティの要件 n. CSP のサービスの独立した評価の実施に関する要件、CSC 監査の権利、および契約のセキュリティ規定の継続的な遵守を実証するための要件。 o. CCM 管理策 STA-12 と整合するように、CSP がサプライヤのセキュリティ要件を設定し、管理するための要件。 p. ポータビリティやデータ返却の期待など、契約終了や移行に関連するあらゆる要件 管理策と SSRM は、共に、必要なセキュリティ要件が全て契約合意で対処されていることを検証するための健全なメカニズムを提供する。		

Control Title	Control ID	Control Specification

サプライチェーン合意のレビュー	**STA-10**	CSP と CSC の間のサプライチェーン合意を少なくとも年 1 回レビューする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； 毎年行われる契約内容の見直しは、CSP と CSC が共同で行う。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠』が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP 及び CSC は、契約書レビューの年次サイクルを確立すべきである。このレビューは、管理策 STA-08（サプライチェーンリスク要因の定期的な見直し）、STA-11（内部統制の評価）、STA-13（サプライヤーガバナンスポリシーと手順の定期的なレビュー）、及び STA-14（定期的なセキュリティ評価）について説明される継続的な見直しにおいて提起される可能性のある問題、リスク、又はその他の検討事項を考慮するものとする。 契約の不履行、定義された SLA を満たすことができない、またはどちらかの当事者のニーズや期待が完全に満たされていない状況などの問題は、議論して解決する必要がある。継続的なレビューは、ビジネス関係における完全な透明性を維持する機会を提供する。 レビューは、継続的な関係に影響を及ぼす可能性のある CSP や CSC のサービスまたはビジネス状況の変化にも対処すべきである。例えば、新製品や新たなパートナーシップは、相手方の関心を引く可能性がある。 必要であれば、契約合意は正式に再交渉され、必要な変更が反映されるように修正されるべきである。必要であれば、SSRM も契約合意書に加えられた変更を反映するよう更新され、2 つの文書の整合性が保たれるようにすべきである。 レビューサイクル活動を計画する際、CSP および CSC は、契約解除またはサービス価格の値上げの 60 日前通知など、事前の通知期間を考慮すべきである。	**実施ガイドライン** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
内部コンプライアンス・テスト	**STA-11**	スタンダード、ポリシー、手順、およびサービスレベルアグリーメントのアクティビティへの準拠状況と効果を確認するため、少なくとも年 1 回、内部評価を実施するためのプロセスを定義し、実行する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC はともに、それぞれの管理策の実施について独立した内部評価を実施すべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP と CSC は、継続的な内部統制評価プログラムを確立すべきである。 評価プログラムの範囲と厳格さは、クラウドサービスオファリングの範囲と重要性、組織の規模、業種、及び規制要件やコンプライアンス要件に基づいて大きく異なる可能性がある。評価プログラムは、セキュリティ組織が実施するレビュー（「第一線」のプログラムレビュー）、内部であるが独立したリスクマネジメント組織が実施するレビュー（「第二線」のプログラムレビュー）、内部監査チーム又は独立監査人が実施する監査（「第三線」のプログラムレビュー）にまたがることがある。監査・保証（Audit & Assurance：A&A）ドメインは、推奨される監査プログラムの管理策について記述している。この管理策のもとで実施される内部プログラム評価は、管理策環境の全体像を把握するため、STA-14 管理策のもとで実施される CSP のサプライチェーンの評価を考慮すべきである。 評価プログラムには、定期的、定期的な手作業による統制のレビューと、継続的または自動化された要素を組み合わせることができる。手作業による統制の評価には、様々な検査、サンプリング、面談の技法が含まれる。自動化された統制及び統制報告は、統制運用の継続的な保証を確保するのに役立つものであ	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

り、可能な限り実施されるべきである。 SSRM の対象となる全ての管理策を評価に含める必要があり、クラウドサービス提供の全てのコンポーネントまたは要素、および関連する活動に対処する必要が各ドメインの"-01"各ドメインの CCM 管理策は、管理策の設計及び運用の有効性の評価の指針となるべき管理策のポリシー及び手順を記述している。ポリシーと手順の適用範囲と適切性のレビューも評価に含めるべきである。 CSP は、SSRM において「(依存する形で) 共有」として特定された管理策の評価において CSC を支援するよう求められることがある。 CSC と CSP がそれぞれ独立して SSRM の管理プログラムを評価する必要性は、全てのクラウドサービスモデルにおいて共通である。	

Control Title	Control ID	Control Specification
サプライチェーンにおけるサービスアグリーメント準拠	**STA-12**	サプライチェーン全体のすべての CSP に、情報セキュリティ、機密性、アクセス制御、プライバシー、監査、人事ポリシー、およびサービスレベル要求と適用標準規格に対して、準拠を要求したポリシーを実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠； CSP と CSC は、サプライチェーン内の全ての組織がクラウドサービスオファリングに関連する適切なセキュリティプログラムの管理策を実施することを要求するためのポリシーと契約条項を独自に実装すべきである。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** クラウドサービスの SSRM 管理の実施に直接的または間接的に関与する全ての組織は、健全なセキュリティプログラムと演習	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

を実装すべきである。CSP と CSC はそれぞれ、サプライヤに期待されるセキュリティプログラムとセキュリティ管理策を確立するためのポリシーを定め、契約上の合意においてそれらのポリシーを実装すべきである。 ポリシーは、サービスの直接的サプライヤと間接的サプライヤの両方（すなわち、第三、第四・・・第 n の関係）を考慮すべきである。考慮すべき間接的な関係の例としては、データセンターインフラサービスの一次サプライヤが存在するが、そのサプライヤが施設の清掃サービスを外注している場合がある。清掃サービスを行う従業員（機密性の高い機器やデータに直接物理的にアクセスできる）に対する身元調査要件に対処すべきである。 CSP 及び CSC は、サプライヤのセキュリティ管理に関するサプライヤの要件に対応する条項を、サプライヤとの契約に含めるべきである。当該契約条項は、サプライヤのセキュリティプログラム及びプラクティスが導入され、適切であることを最初に判断すること（初期デューデリジェンス）と、継続的な遵守を確認するためのサプライヤの継続的な管理及びモニタリング（管理体制 STA-11 を参照）の両方に対応すべきである。このようなサプライヤ管理契約に関する考慮事項は、STA-11 の実施において扱われるべきである。 STA-09 では、その他の契約関連のセキュリティに関する考慮事項も取り上げられている。	

Control Title	Control ID	Control Specification
サプライチェーンにおけるガバナンスレビュー	**STA-13**	組織のサプライチェーンパートナーの IT ガバナンスポリシーと手順を定期的にレビューする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠； この管理策は、CSC と CSC の双方で独自に実施する。各当事者によるサプライヤの IT ガバナンスポリシーと手順のレビューは、互いに独立したものである。	**管理策所有権の根拠；** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 管理策 STA-08 に記述されるサプライチェーンにおける継続的なリスク管理の一環として、 CSP は、主要サプライヤの IT ガバナンスポリシーと手順を定期的に評価するものとする。この管理策は、管理策 STA-08 と連携して CSP が実施するものとする。 IT ガバナンスポリシーと手順は、テクノロジーとサイバーセキュリティリスク管理に対する組織の全体的なアプローチを指導し、束縛し、監督するものである。CSP の主要なサプライヤの IT ガバナンスプラクティスが、CSP 自体のニーズと CSC のニーズに合致していることが重要である。 以下のサプライヤ IT ガバナンスのトピックは、CSP によって定期的に見直される場合がある： a. テクノロジー、サイバーセキュリティ、リスクに関する事項を取締役会または管理当局に定期的に報告するための要件 b. 組織のミッション、戦略、戦術的イニシアチブに対する IT の整合性 c. 経営陣および取締役会または管理当局へのリスク事項のエスカレーションの要件 d. 取締役会または管理当局による正式なリスク選好度およびリスク選好度の設定 e. 関連する法律、規制、および契約上の合意の遵守 f. 技術、サイバーセキュリティ、リスク管理プログラムの役割と責任 g. IT ポリシーと手順の適用範囲と程度 h. 業界標準およびベストプラクティスとの整合と遵守 i. リソース（スタッフおよびその他の IT 投資）の妥当性を判断するためのプラクティス 関連するサプライヤのレビューに関する考慮事項については、管理策 STA-08 を参照し、IT ガバナンスに関するさらなるガイダンスについては、ガバナンス、リスク、コンプライアンス（GOV）管理策ドメインを参照する。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification

サプライチェーンにおけるデータセキュリティアセスメント	**STA-14**	サプライチェーン内のすべての組織に対して、定期的にセキュリティアセスメントを実施するためのプロセスを策定し実装する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSC と CSC の双方で独自に実施する。各当事者によるサプライヤのセキュリティプログラムのレビューは、互いに独立している。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 管理策 STA-08 に記述されるサプライチェーンの継続的なリスク管理の一環として、CSP は、定期的または継続的に、サプライヤのセキュリティプログラムと管理策を評価すべきである。 サプライヤのセキュリティに関する CSP の継続的なレビューのポリシー、手順、結果は、たいていの場合、CSC による初期デューデリジェンス、および既存の CSC 利用者による継続的なデューデリジェンスの対象となる。CSP は、これらの実務において透明性を確保すべきである。 可能であれば、CSP がサプライヤの管理策のセキュリティを評価する機能は自動化され、可能な限りリアルタイムに近い形で提供されるべきである。管理報告、アラートメカニズム、および、このような継続的な管理モニタリング手法は、可能な限り、クラウドサービスその他の IT サービスに組み込まれるべきである。サプライヤの管理が自動化されていない場合、または管理運用データがサプライヤからプロアクティブに提供されない場合、定期的な手作業によるレビューと評価が必要となる可能性がこのようなレビューは、一般に、管理 STA-08 と連携して CSP が実施する。 レビューの一般的な目的は、サプライヤのセキュリティプログラムおよびプラクティスが CSP の要件に対して十分であるかどうか、またサプライヤが SSRM および契約書に規定された期待事項を遵守しているかどうかを判断することである。レビューには、CSP が主要サービス（インフラストラクチャのホスティング	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

など）を提供するために依存する、直接的および間接的な全てのサプライヤを含めるべきである。

以下のサプライヤのセキュリティプログラムおよびセキュリティ管理策要素は、CSP によって定期的にレビューされる場合がある：

a. セキュリティポリシー、手順、標準、および業界標準と慣行への継続的なコンプライアンス
b. サプライヤのリスク管理、リスク評価、統制評価とテスト、例外管理手順
c. 製品またはサービスをサポートするために実装された特定の技術的管理策の文書化およびテスト（ID およびアクセス管理、ネットワーク設計、セキュリティなど）。
d. 構成管理、変更管理、製品ライフサイクル、および運用のポリシー、手順、および管理
e. ソフトウエアの完全性、追跡可能性、出所を確保するためのソフトウエアサプライチェーンリスク管理の実践（ソフトウエア構築の実践、コンポーネント管理、ソフトウエア部品表（SBOM）の使用など）
f. サプライヤ自身のサプライチェーンリスク管理ポリシーと手順、サプライヤのレビュー、サプライヤがサプライヤを継続的に管理・監視するために採用する手順
g. サプライヤの BC プログラム計画、DR 手順、IR および復旧計画のテスト報告書。
h. 脅威管理、ロギング、モニタリング、イベント分析の機能と手順
i. サプライヤのインシデント管理手順、インシデント報告標準、およびセキュリティまたは可用性に関するインシデントに関する提供された報告書
j. サプライヤの人事管理慣行（許容される使用ポリシー、内部脅威管理プログラム、ポリシー違反に対する慣行を含む
k. データセンター、環境、物理的なプラクティスと管理策
l. プライバシーおよびデータ管理に関するポリシー、手順、統制
m. 独立したセキュリティ監査慣行

レビューされる具体的な要素は、SSRM、契約合意、及び製品又はサービス提供の重要性に依存する。要求されるデューデリジェンスのレベルに応じて、様々なレビュー、評価、テストの方法が採用される。レビューには、現地訪問、サプライヤから提供された独立監査又は評価のレビュー、共有評価のレビュー、サプライヤから提供された報告書及び管理テストのレビュー、及び直接管理テストが含まれる。

関連するサプライヤーレビューの考慮事項については管理策 STA-08 を参照し、具体的なセキュリティ管理ポリシーと手順については、CCM の各管理策ドメインのポリシー関連管理策を参

照する。	

Control Domain TVM

2.16 脅威と脆弱性管理(TVM)

Control Title	Control ID	Control Specification
脅威と脆弱性管理ポリシーと手続	**TVM-01**	脆弱性の悪用からシステムを保護するために、脆弱性を特定、報告、その修復に優先順位をつけるためのポリシーと手順を確立、文書化、承認、周知、実装、評価、維持する。少なくとも年１回、ポリシーと手順を見直して更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、CSP と CSC の双方で共有され、CSP と CSC の両当事者は、クラウドサービスモデル（IaaS/PaaS/SaaS）に関係なく、各自のビジネスニーズとコンプライアンス要件に従って、脆弱性を特定し、報告し、改善の優先順位をつけて、改善するためのポリシーと手順を独自に実施する責任を負う。 CSP は、脆弱性を特定し、ワークロード（仮想マシン、サーバーレス、データベース、ネットワーク、コンテナ、Web アプリケーションを含むが、これらに限定されない）を保護するための合理的かつ十分な機能とツールを CSC に提供するものとする。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： CSP は、脅威および脆弱性管理（TVM）に関するポリシーを確立するものとする。このポリシーには、SSRM に基づいて CSP がそれぞれの対象範囲について脅威および脆弱性を特定し、対処する方法の意図、目的、およびガバナンスが含まれる。 CSP は、ホストインフラストラクチャ、ネットワークデバイス、仮想化テクノロジー、オペレーティングシステム、データベースや Web アプリケーションなどのプラットフォームアプリケーション上の脆弱性を特定し、評価し、報告し、優先順位を設定し、改善する手順を確立し、実施する責任を負う。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。 加えて、SaaS 利用者は、利用する SaaS アプリケーション上のインフラストラクチャおよびセキュアでないコードに関連する脆弱性を特定する責任は負わないが、脆弱性の悪用からアプリケーションを保護するために、CSP が SaaS アプリケーション上の脆弱性を、どのように特定し、報告し（CSC に通知する手順）、優先順位を設定し、改善する手順を確立して、実践するために CSP と交渉する場合がある。 SaaS 利用者は、アプリケーションのセキュリティ設定および潜在的な誤設定に関連する脆弱性を特定し、評価し、報告し、および優先的に改善するための手順を確立して、実践する責

	任がある。
ポリシーは、以下に関する規定を含むべきである（但し、これに限定されない）： a. 範囲と目的： i. オンプレミスとクラウドベースのインフラ（クラウドシステム、アプリケーション、データ）の両方を含む。 ii. 適用される法律、規制、および契約要件の遵守の必要性に重点を置いた、包括的かつ効果的な脆弱性管理プログラムを確立することを目的とする。 b. 脆弱性管理プログラム： 脅威と脆弱性を管理するために使用すべき方法（クラウド環境とクラウドサービス提供における脅威のモデル化、分析、脅威情報、評価、脆弱性スキャニングの方法、評価、優先順位を設定し、改善プロセス、関連するセキュリティ検証方法を含む）を包む脆弱性管理プログラム。 c. 検出ツールの更新： 検出ツールおよび構成を更新するプロセスの要件。 i. 全ての検知ツール（脆弱性スキャナ、脅威インテリジェンスフィード、IDS/IPS シグネチャなど）の定期的な更新スケジュールを計る。 ii. 検出ツールの更新（可能であれば自動化）：更新プロセスを合理化し、手動による介入を最小化する自動化ツールを活用することで、タイムリーな更新と継続的な保護を実現する。 d. 外部ライブラリの脆弱性： 外部ライブラリのインベントリ作成と監視、およびアプリケーションとインフラストラクチャ内の外部ライブラリ、並びにコンポーネントを追跡する手順。 e. 侵入テスト： 潜在的な脆弱性とセキュリティ上の弱点を発見するために、クラウドインフラストラクチャとアプリケーションの侵入テストを定期的に実施するための要件。 i. 適切なモデルのセキュリティテスト（侵入テスト、レッド／ブルー／パープルチーミング、侵入および攻撃シミュレーションなど）。 ii. 侵入テスト中の機密データの取扱い方法に関する要件。 iii. 侵入テスト中に特定された脆弱性の優先順位を設定し、改善に関する要求事項。 f. 脆弱性の特定： 自動化された脆弱性スキャンツールをし使用して、クラウドインフラストラクチャ、アプリケーション、ソフトウェアコンポーネントにわたる既知の脆弱性を特定するための要件。 g. 脆弱性の優先順位を設定し： 特定された脆弱性を、その重大性とデータセキュリティへの潜在的影響に基づいて優先順位を設定しするための要	

件。

h. 脆弱性の改善スケジュール：
脆弱性の優先度および緊急度に基づき、脆弱性を改善するための明確に定義されたスケジュール。

i. 脆弱性管理報告：
特定された脆弱性の概要、深刻度レベル、および改善状況を含む、定期的な報告書を作成し、利害関係者に伝達するための要件。

j. 脆弱性管理指標：
脆弱性管理プロセスの有効性を測定するために定義された主要業績評価指標（KPI）。

k. 承認：
組織の戦略目標およびリスク選好度との整合性を確保するための承認要件および上級管理者の関与。

  i. ポリシーと手順に対する変更又は修正のための承認プロセスを確立する。

  ii. 承認に関する文書化された記録（日付、承認者名、関連するコメント又は議論を含む）を維持する。

l. コミュニケーション：
ポリシーと手順の効果的なコミュニケーションは、関連する全てのクラウド利害関係者に対して促進すべきである。

m. 維持管理とレビュー：
脆弱性管理ポリシーと手順は、進化するクラウドセキュリティの状況に確実に合致し、クラウド技術、規制およびリスクの変化を反映するために、文書化し、レビューし、少なくとも年１回更新する。

このポリシーは、サービス合意／契約書、SLA、およびその他の条項で決定された責任の分担を反映し、管理策・ギャップ評価で決定された未対応のニーズに対処するための割り当てを行うべきである。

Control Title	Control ID	Control Specification
マルウェア対策ポリシーと手続	**TVM-02**	脆弱性の悪用からシステムを保護するために、脆弱性を特定、報告、その修復に優先順位をつけるためのポリシーと手順を確立、文書化、承認、周知、実装、評価、維持する。少なくとも年１回、ポリシーと手順を見直して更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： マルウェア防御のポリシーと手順は、コンピュート、ネットワークデバイス、エンドポイント、およびセキュアアクセスゲートウェイを含む、全てのコンピューティングインフラストラクチャ全体に導入され、統合すべきである。従って、この管理策の実施責任は、3 つのクラウドサービスモデル（IaaS/PaaS/SaaS）に関係なく、CSP と CSC の双方にあり、各当事者によって独立して実施すべきである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、クラウド環境におけるマルウェア保護を目的としたポリシーと手順の効果的な実施について、第一義的な責任を負う。これには、セキュリティのレイヤ化アプローチを導入し、全てのクラウドインスタンスにウイルス対策ソフトウェアやマルウェア対策ソフトウェアなどの堅牢なマルウェア対策ツールを導入し、維持することで、進化するマルウェアの脅威から CSC のデータとクラウドインフラを保護することが含まれる。 CSP は、ファイアウォールや侵入検知/防止システムなどのネットワークセキュリティ管理策を真摯に実施し、マルウェアの脅威の可能性がある送受信トラフィックを監視およびフィルタリングするほか、アクセス制御、データ暗号化、脆弱性管理のベストプラクティスを実施しなければならない。	**実施ガイドライン：** **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。
ポリシーは、以下に関する規定を含むべきである（但し、これに限定されない）： a. 範囲と目的： i. マルウェア感染からの保護が必要な管理対象デバイスを使用する CSP と CSC の両方に対する要件 ii. クラウドコンピューティング環境におけるマルウェア保護ソリューションの開発および実践の目的 b. 階層レイヤ構造のマルウェア対策： アンチウイルス、アンチマルウェア、ホストベースファイアウォール、ネットワークセキュリティ管理、エンドポイント検知（EDR）ツールなどのセキュリティソリューションを組合せて、マルウェアをレイヤ構造化して防御する。 i. 仮想マシン、ネットワークデバイス、エンドポイントの OS、セキュアアクセスゲートウェイなど、全てのクラウドコンピューティングインフラストラクチャにマルウェア対策を統合する。 ii. マルウェア防御の一元管理（計画、実践、評価、認可、および組織で定義されたマルウェア防御の監視を含む）、組織的に定義されたマルウェア対策セキュリテ	

ィ管理の計画、実施、評価、承認、監視を含む、マルウェア対策の一元管理をする。

iii. インバウンドトラフィックとアウトバウンドトラフィックの両方を検査し、マルウェアを検出、防止、ブロック、除去するための制御を実施するマルウェア対策をする。

iv. リアルタイム保護、スケジュールスキャン、自動更新の有効化など、効果を最適化するためのマルウェア保護ソリューションのセキュリティ構成をする。

v. ファイアウォール、(IDS) 侵入検知システム、(DLP) データ損失防止ツールなど、他のセキュリティ対策とマルウェア対策ソリューションを統合し、統一されたセキュリティポスチャを構築する。

vi. 自動マルウェアスキャンを電子メールおよびファイルアップロードシステムに統合することによるマルウェアの改善（可能であれば自動化）をする。

c. 脅威インテリジェンスの統合：
脅威インテリジェンス配信をマルウェア対策ソリューションに統合し、最新の脅威、侵害指標（IoC： Indicator of Compromise)、攻撃手法に関する最新情報を提供する。

d. 機械学習と人工知能（ML/AI）：
膨大な量のデータを分析し、パターンを特定し、マルウェア感染を示す異常を検出するために ML/AI 技術を活用する。

e. サンドボックス分析：
疑わしいファイルやコードを隔離してセキュアに実行し、その挙動を観察して、悪意のある意図を特定するサンドボックス環境を構築する。

f. シグネチャベースおよびシグネチャレス検知：
既知のマルウェアのシグネチャに依存するシグネチャベースの検知と、未知の脅威を特定するためにファイルの動作やヒューリスティックを分析するシグネチャレス検知を組合せたアプローチをする。

g. マルウェアソリューションのアップデート：
進化する脅威に対する有効性を維持するために、最新のシグネチャ、パッチ、検出メカニズムを備えたマルウェア保護ソリューションの定期的な更新をする。

h. マルウェアソリューションのテスト
マルウェア防御ソリューションの性能、精度、システム性能への影響を評価するための厳密なテストと評価をする。

i. 監視および警告：
マルウェア感染を迅速に特定し、対応するための監視と警告メカニズムを確立する。

j. 承認：
組織の戦略的目標およびリスク選好度との整合性を確保するための、承認要件および上級管理職の関与を確立する。

i. ポリシーと手順の変更又は修正については、承認プロ

セスを確立する。 ii. 承認に関する文書化された記録（日付、承認者名、関連するコメントや議論を含む）は、維持する k. コミュニケーション： ポリシーと手順の効果的なコミュニケーションは、関係する全てのクラウド利害関係者に促進すべきである。 l. メンテナンスとレビュー： マルウェア防御のポリシーと手順は、進化するクラウドセキュリティの状況との整合性を確保し、クラウド技術、規制、リスクの変化を反映するために、少なくとも年１回は文書化し、レビューし、更新すべきである。 ポリシーには、システムが企業のコンピューティングリソースに接続する際に、マルウェアに感染していないことを保証しようとする改善プログラムの時間目標に対する期待も含めるべきである。 シグネチャベースまたはビヘイビアベースの検出プロセスを使用するウイルス、またはマルウェアアプリケーションによってマルウェアが識別された場合、その除去は、適用される契約上の合意および組織の標準に従って更新すべきである。	

Control Title	Control ID	Control Specification
脆弱性の修復スケジュール	**TVM-03**	特定されたリスクに基づいて脆弱性が特定された場合に、計画された対応と緊急時の対応の両方を可能にするためのプロセス、手順、技術的手段を定義、実施、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は共有である。CSP と CSC の両当事者は、クラウドサービスデリバリーモデル（IaaS/PaaS/SaaS）に関係なく、それぞれのビジネスニーズとコンプライアンス要件に従って、脆弱性改善スケジュールを実施する責任を負う。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン：	**実施ガイドライン：**

包括的なクラウドサービスの脆弱性改善スケジュール(VRS)は、クラウド環境全体の脆弱性を特定し、優先順位を付け、修正し、検証するための構造化されたアプローチの概要を示すべきである。VRS は、タイムリーで効果的な脆弱性改善管理策を保証するための技術的手段、プロセス、およびスケジュールを包含めるべきである。

IaaS プロバイダー：
ホストインフラストラクチャ、ネットワーク機器、および仮想化技術について、CSP は、定期対応と緊急対応の両方を可能にする手順と手続、および技術的手段を定義し、実装および評価する責任を負う。

発見された脆弱性の改善に優先順位をつけるために、リスク評価プロセスを活用すべきである。

IaaS CSP が実施する脆弱性修正のガイドラインには、以下が含まれる（但し、これらに限定されない）：

a. パッチ管理：
IaaS リソース（VM、OS、ネットワークデバイスソフトウェア）にセキュリティパッチを迅速に適用するため、可能な限り自動化を活用した迅速なパッチ適用プロセスを導入する。パッチ管理プロセスを確立し、メンテナンス期間中に更新をスケジュールする。

b. 構成管理：
構成管理ツールを使用し、必要に応じて構成管理を自動化することで、IaaS 環境全体で一貫性のあるセキュアな構成を確保する。

c. ネットワークセキュリティ：
ファイアウォール、侵入検知/防止システム（IDS/IPS)、ネットワークセグメンテーションなどのネットワークセキュリティ管理策を実装し、不正アクセスや悪意のあるトラフィックから IaaS リソースを保護する。

d. ロギングと監視：
一元化されたロギングソリューションを導入し、様々な IaaS リソースからログを収集して分析し、セキュリティに関する洞察を得る。

PaaS プロバイダー：
ホストインフラストラクチャ、ネットワークデバイス、仮想化技術、オペレーティングシステム、およびデータベースなどのプラットフォームアプリケーションについて、CSP は、計画された対応と緊急時の対応の両方を可能にする手順と手続および技術的手段を定義し、実装し、および評価する責任を負う。
発見された脆弱性の修正に優先順位を付けるために、リスク評価プロセスを利用する。

PaaS の CSP に関わる、脆弱性修正の実装ガイドラインには、以

仮想マシンおよびデプロイされたプラットフォームアプリケーションについて、CSC は、定期対応と緊急対応の両方を可能にする手順と手続および技術的手段を定義し、実装し、評価する責任を負う。
発見された脆弱性の改善に優先順位を付けるために、リスク評価プロセスを利用する。

CSP の「実施ガイドライン」が適用される。

SaaS の CSC は、SaaS クラウド環境内のデータとアプリケーションを保護すべきである。CSP は、独自のセキュリティ対策を実施するが、利用者にも脆弱性に対処し、防御を強化するための具体的な実施責任がある。

SaaS の CSC が実施する脆弱性改善のためのガイドラインには、以下が含まれる（但し、これらに限定されない）：

a. 設定の逸脱の改善：
契約している SaaS アプリケーションについて、セキュアな構成のベースラインからの逸脱があれば、速やかに対処し、改善し、セキュアな構成を実施・監視するための自動化ツールを導入する。

b. アクセス制御の誤設定：
誤設定されたアクセスレベルは修正され、ユーザーの役割と権限レベル（最小特権の原則）に基づいてデータと機能へのアクセスを制限する適切なアクセス制御が実装されるべきである。

c. 脆弱なデフォルト設定の更新：
   i. 脆弱なデフォルトセキュリティ設定を修正する。
   ii. 例えば、強力なパスワードの有効化、不要な機能の無効化、データ暗号化の実施などである。
   iii. SaaS プロバイダーのセキュリティ慣行との整合性を確保し、アプリケーション固有のセキュリティ設定要件への対応に関する SaaS プロバイダーの専門知識を活用する。

d. API の誤設定の修正：
API の設定ミスを修正し、API 鍵、OAuth、クライアント証明書など、強力な API 認証・認可メカニズムを実装する。

e. データ暗号化の使用：
SaaS アプリケーションに保存され、移動中の機微データは、最新の業界標準に従った強力な暗号化アルゴリズムを用いて暗号化されるべきである。

f. MFA の使用：
全ての SaaS アプリケーションで MFA を有効にし、パスワード以外のセキュリティレイヤーを追加する。

g. ログと監査の使用：
全ての SaaS アプリケーションのアクティビティとアクセス試行について、ログと監査を有効にすべきである。

下のものが含まれる（但し、これらに限定されない）：

a. 脆弱性のパッチ適用：
PaaS 固有の脆弱性スキャンツールを活用して PaaS アプリケーションとサービスの脆弱性を特定し、PaaS プロバイダーと協力して特定された脆弱性に迅速に対処する。

b. セキュアなコーディングとランタイムアプリケーションセキュリティ保護：
導入前に PaaS アプリケーションの脆弱性を特定し、修正するために、セキュアなコーディングプラクティスと静的コード分析ツールを実施する。

i. コンテナのセキュリティ：

ii. コンテナスキャンツールを活用してコンテナイメージを評価し、セキュア性を確保する。ベースイメージとその依存関係を更新し、コンテナセキュリティを CI/CD パイプラインに統合する。

iii. サーバーレスセキュリティ：
サーバーレスセキュリティに特化したツールを活用する。サーバーレスサービスの適切なアクセス制御を実装し、サーバーレス構成を定期的に更新する。

c. PaaS 構成管理と PaaS セキュリティ評価：
PaaS 固有の構成管理ツールを活用し、PaaS アプリケーションとサービスのセキュアな構成を実施する。

d. ランタイムアプリケーションセキュリティ保護（RASP）：
実行時に PaaS アプリケーションを監視・保護する RASP ツールを導入し、アプリケーションの脆弱性を悪用する攻撃を検出してブロックする。

SaaS プロバイダー：

ホストインフラストラクチャ、ネットワークデバイス、仮想化技術、オペレーティングシステム、およびデータベースや Web アプリケーションなどのプラットフォームアプリケーションについて、CSP は、定期対応と緊急対応の両方を可能にする手順と手続および技術的手段を定義し、実装し、評価する責任を負う。発見された脆弱性の修正に優先順位を付けるために、リスク評価プロセスを利用する。

SaaS の CSP に関する脆弱性修正の実施ガイドラインには、以下のものが含まれる（但し、これらに限定されない）：

a. API セキュリティ：
強力なアクセス認証と認可の仕組みを実装し、API 通信を暗号化し、API セキュリティ設定を見直し、更新することによって、SaaS アプリケーションで使用される API を評価し、セキュアにする。

b. アプリケーションとデータのアクセス制御構成：
SaaS アプリケーション、クラウドサービス、およびデー

h. パッチの欠落の改善：

i. CSP が提供するパッチまたはアップデートを適用して、特定された脆弱性に対処する。

ii. パッチ適用スケジュールを実施し、デプロイ前にパッチを十分にテストして、混乱や予期しない結果を回避する。

i. ネットワークセキュリティの誤設定の修正：
ファイアウォールルールおよびネットワークセキュリティ設定は、不正アクセスや悪意のある活動をブロックする一方で、正当なトラフィックを許可するように適切に設定すべきである。

j. シャドーIT の改善：
社員は、認可されていない SaaS アプリケーションの使用を報告するよう奨励されるべきである。

k. 不適切なデータ保持の改善：
データの保管、アクセス、および廃棄を管理するデータリテンション・管理策は、保持ポリシー、規制、およびビジネス目標に従って実施すべきである。

脆弱性の改善スケジュールは、承認され、全ての関係者に通知され、SLA に含むべきである。

全てのサービスモデルに適用：

CSP の「実施ガイドライン」が適用される。

タに対するセキュアなアクセス制御構成を実施する（2要素認証または多要素認証：2FA,MFA の有効化、データアクセスの制限、および不要な機能の無効化）。

c. SaaS 利用状況のモニタリング：
SaaS アプリケーションの使用状況を監視し、疑わしい活動や潜在的なデータ侵害を検出する。SIEM ツールを導入して、SaaS アプリケーションのデータを他のセキュリティソースと関連付け、脆弱性を事前に改善する。

全てのサービスモデルに適用：

脆弱性の改善に関する実施上のベストプラクティスには、以下が含まれる（但し、これらに限定されるものではない）：

a. 脆弱性改善スケジュール（VRS）：
脆弱性改善のための構造化されたスケジュールを定義し、実施すべきである。
その脆弱性改善スケジュール（VRS）の概要は、
   i. リスクに基づいて、深刻度、環境への脅威、TVM ポリシーの期待との整合性の順に、改善のための脆弱性の分類と優先順位を設定しする。
   ii. 重大性に基づく脆弱性改善の時間枠は、ハイリスクの脆弱性改善のために優先される。一方、中リスクおよび低リスクの脆弱性は将来の改善努力のためにスケジュールされる。
   iii. クラウド環境全体にわたるセキュリティパッチとセキュリティ設定のデプロイを合理化する、パッチと設定の一元管理をする。
   iv. 脆弱性管理のためのネイティブ機能を活用するため、CSP のツールとの統合可能性を計る。
   v. 特に大規模なクラウド環境では、アプリケーションやインフラストラクチャコンポーネントにセキュリティパッチを自動的にデプロイするための、改善ワークフローを自動化する。
   vi. 改善の進捗を監視し、特定された脆弱性の終結を追跡することで、セキュリティリスクをタイムリーかつ効果的に軽減する。

b. 修正とパッチの管理セキュリティパッチとセキュリティ設定のデプロイを合理化するために、一元化されたパッチと設定の管理システムを導入すべきである。
   i. 手作業による介入を減らし、脆弱性にさらされる期間を最小化するため、パッチ適用を可能な限り自動化する。
   ii. 脆弱性管理ツールを活用し、脆弱なソフトウェアコンポーネントに対して利用可能なパッチの通知をリアルタイムで受信する。
   iii. 自動化できないパッチに対する例外処理メカニズムを確立し、手動によるパッチ適用手順に対する改善指示を提供すべきである。
   iv. パッチ適用により予期せぬ問題や競合が発生した場合、以前のソフトウェアバージョンに戻すた

めのロールバックメカニズムを実装する。 v. サービスの中断を最小限に抑えるため、パッチを適用するための定期的な maintenance windows をスケジュールすべきである。 c. 構成管理： 構成管理ツールを使用し、クラウドリソースのセキュアな構成をする。 i. 構成ベースライン、テンプレート、自動化を確立し、クラウド環境全体で一貫性のあるセキュアな構成を確保する。 ii. 構成管理ツールを使用して、クラウドリソースのセキュアな構成を実施し、脆弱性をもたらす可能性のある誤構成を防止する。 d. 脆弱性改善の検証： パッチ適用後に影響を受けるシステムを再スキャンし、脆弱性への対処が成功したことを確認することで、対処の有効性を検証するプロセスを導入すべきである。 e. レビューと更新： クラウド環境、セキュリティ脅威、脆弱性管理ツールの変化を反映するため、VRS の定期的なレビューと更新を実施する。スケジュールは、新たな脆弱性、進化する脅威、および新たに出現するセキュリティのベストプラクティスに対処するために適応されるべきである。 脆弱性対応スケジュールは、全ての関係者に承認・伝達され、SLA に盛り込まれるべきである。	

Control Title	Control ID	Control Specification
検出の更新	**TVM-04**	検出ツール、脅威シグネチャ、IoC（セキュリティ侵害インディケータ）を毎週またはそれ以上の頻度で更新するためのプロセス、手順、技術的手段を定義、実施、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠： この管理策は、IaaS,PaaS,SaaS で「依存しない共有」であり、CSP と CSC によって実装され運営される。検知ツール、シグネチャ、および侵害の指標が、定義され実装され評価される活動、イベント、状態のタイプは、IaaS、PaaS、および SaaS のインスタンスごとに異なる。CSP と CSC は、それぞれの要件に必要な検知仕様を決定し、それらが適切に定義し、実装し、および運用されることを保証する責任を、それぞれ独自に負う。 SaaS の実装については、CSP がこの管理に責任を負うのが一般的であるが、CSC と CSP がこの分野で責任を共有する特定のユースケースもある。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 効果的な脅威検知態勢を維持するため、CSP は、検知ツール（ネットワークファイアウォール、WAF、NIDS、NIPS、HIDS、HIPS、ネットワークレイヤー分散型 DDoS 防御、アプリケーションレイヤーDDoS 防御、マルウェア対策ソフトウェアなど）の最新安定版がインストールされ、脅威のシグネチャと侵害の指標（IoC）が定期的に、できれば毎週またはそれ以上の頻度で更新されるようにすべきである。 CSP は、関連する更新を CSC が適用できるようにすべきである。 検出ツール、脅威シグネチャ、および侵害の脆弱性の指標を更新するための実施上のベストプラクティスには、以下が含まれる（但し、これらに限定されない）： a. 脅威インテリジェンスプラットフォーム 内部セキュリティフィード、業界レポート、外部脅威インテリジェンスプロバイダー、オープンソースインテリジェンス（OSINT）など、様々なソースからの脅威データを集約・管理し、脅威インジケータ、シグネチャ、脆弱性への統一的なアクセスを提供するために、一元化された脅威インテリジェンスプラットフォームを導入すべきである。 b. 脅威データの収集と処理： 様々なソースから脅威データを収集し処理するプロセスを自動化し（スクリプト、API、専用脅威インテリジェンスフィードなど）、脅威データを脅威インテリジェンスプラットフォームに統合して分析と相関を行う。 c. 脅威の優先順位を設定し標準： 脅威データの優先順位を設定しの標準は、脅威の重大性、クラウドインフラストラクチャおよび CSC のデータへの潜在的な影響などの要因に基づいて設定すべきである。 d. 脅威シグネチャと更新フレームワーク： 検知ツールの脅威シグネチャを更新するためのフレームワークを作成すべきである。 このフレームワークは以下を含むべきである： i. 脅威情報フィードと内部セキュリティログを継続	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。 さらに、SaaS 実装の場合、CSP は通常この管理に責任を負うが、このドメインにおいて CSC と CSP が責任を共有する特定のユースケースもある。 特定のユースケースにおいて、SaaS の CSC は、一般的に、検知ツール、シグネチャ、および危殆化の指標が望まれ、必要とされ、したがって特定の SaaS 実装のために定義し、実装し、および評価される必要がある活動、イベント、又は状態のタイプを決定する責任を負う。 SaaS CSC は、関連する検知仕様が適切に定義され、実装され、運用されることを保証する責任を負う。 これらは、元の CSP との追加サービス契約や、別のサードパーティプロバイダーの代替サービスとの統合など、様々な方法で達成することができる。 例えば、CSC は、SaaS アプリケーションおよびその関連データのインスタンスとの関係において、適切なアプリケーションデータアクセス、データ使用、およびデータの移動又はエクスポートに関わる検知ツールを更新するための手順と手続および技術的手段を定義し、実施し、評価することに特に責任を負うことが多い。

的に監視し、新たな脅威と侵害の脅威(IoC) を発見する。

ii. 新たに特定された脅威を分析し、CSP のクラウド環境および CSC 基盤との関連性を判断する。

iii. 新たな脅威の分析に基づく脅威シグネチャと IoC の更新をする。

iv. 実装前に新しいシグネチャと IoC のテストと検証を行い、誤検出を起こさずに脅威を正確に検出できるようにする。

e. 検知ツールの更新：
検知ツールのアップデートは定期的に実施し、ベンダーまたは脅威インテリジェンスプラットフォーム（IDS/IPS ツール、マルウェア対策ソフトウェア、ファイアウォールなど)からのアップデートを自動的に受信するように設定すべきである。

f. シグネチャと IoC のバージョン管理：
脅威シグネチャと IoC のバージョン管理プロセスは、変更を追跡し、必要に応じてロールバックを容易にするために維持されるべきである。シグネチャと IoC の管理と保存には、バージョン管理システム（Git など）を使用することができる。

g. 継続的なモニタリングと評価：

i. 検出ツールの有効性、およびシステムパフォーマンスとリソース使用率に対する更新の影響を継続的に監視する。脅威検知プロセスの成功を測定するために指標を使用する（検知された脅威の数、誤検知率、脅威への対応に要した時間など)。

ii. セキュリティインシデントや脅威分析から得た教訓を脅威検知プロセスに組み込む。

iii. 脅威検知プロセスの有効性を評価し、潜在的なギャップや弱点を特定するために、セキュリティ監査および侵入テストを定期的に実施する。発見された結果は、脅威検知戦略を改善するために使用する。

Control Title	Control ID	Control Specification
外部ライブラリの脆弱性	**TVM-05**	組織の脆弱性管理ポリシーに従って、サードパーティーやオープンソースのライブラリを使用しているアプリケーションのアップデートを特定するためのプロセス、手順、技術的手段を定義、実施、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Independent)	Shared (Independent)	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、IaaS,PaaS で「依存しない共有」である。IaaS と SaaS サービスモデルにおいて、外部ライブラリおよび関連する脆弱性を含む外部ライブラリの管理に関する能力と責任は、CSP と CSC の両方の管理レイヤに存在する可能性がある。それゆえ、IaaS,SaaS の場合、管理策の仕様は CSP と CSC それぞれが実施する。 SaaS の場合、この管理策は、「CSP-Owned CSP が所有」し、自ら実施する責任がある。外部ライブラリ、および関連する脆弱性を含む外部ライブラリの管理機能と責任は、専ら CSP レイヤに存在し、CSP は本制御の実装と運用に単独で責任を負う。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン **全てのサービスモデルに適用：** サードパーティーまたはオープンソースのライブラリを利用するアプリケーションの更新を効果的に特定するため、CSP は、以下の実装を含む包括的な脆弱性管理戦略を実施すべきである。 ベストプラクティス： a. 第三者ライブラリーの目録:クラウド環境全体で使用される全てのサードパーティライブラリの正確なインベントリを維持すべきである。 i. インベントリには、ライブラリ名、バージョン、関連するアプリケーションを含める。 ii. このプロセスを自動化し、ライブラリの使用状況の変化を継続的に監視するためのツール（ソフトウェア構成分析（SCA）、依存関係管理ソリューションなど）を利用すべきである。 b. 脆弱性データベースの統合： インベントリは、CSP 環境で使用されるサードパーティライブラリに影響する新たな脆弱性に関する通知をタイムリーに取得するために、脆弱性データベース（CVE など）と関連付けるべきである。 c. パッチ適用とデプロイ： サードパーティライブラリのパッチ適用とデプロイのプロセスは、可能な限り自動化すべきである。 d. オープンソースライブラリのセキュリティ:オープンソースライブラリを組み込む場合は、ライブラリのコードをレビューし、既知の脆弱性をチェックし、ライブラリが積極的に保守されていることを確認するなど、オープンソースセキュリティのベストプラクティスに従う。	**実施ガイドライン** CSP の「実施ガイドライン」が適用される。 **SaaS カスタマー：** 該当しない。CSP は、この管理の実施と運用に単独で責任を負う。

e. 依存関係管理ツール： 依存関係管理ツールを使用して、ライブラリの依存関係を追跡し、新しいバージョンがリリースされたときに自動的にライブラリを更新する。 f. 自動スキャンツール： i. 自動スキャンツール： 自動スキャンツールを使用して、サードパーティライブラリに関連するものも含め、アプリケーションの脆弱性を定期的にスキャンする。 ii. サードパーティライブラリにパッチを適用しても、新たな脆弱性や互換性の問題が生じないようにする。 g. サードパーティーベンダーの管理： i. ベンダ管理プロセスを導入し、サードパーティライブラリベンダーが、組織のセキュリティ要件に準拠しているかどうかを評価する。 ii. 外部のライブラリベンダーについて、脆弱性開示ポリシーを定め、脆弱性開示と改善のための報告手続と期限を概説する。 iii. サードパーティーベンダーとオープンなコミュニケーションチャネルを確立し、脆弱性や更新に関する情報をタイムリーに受け取る。 h. サードパーティライブラリの更新： サードパーティライブラリに関するセキュリティ勧告やメーリングリストを購読し、最新の脆弱性やパッチに関する最新情報を入手する。 i. CI/CD の統合： 新しいコードやライブラリのアップデートの統合とデプロイを自動化するために、CI/CD パイプラインを採用する。 j. サードパーティライブラリのライセンス： サードパーティライブラリに関連するオープンソースライセンスと法的義務（ライセンス変更の追跡、ライセンス条項の遵守など）の遵守を維持すべきである。	

Control Title	Control ID	Control Specification
ペネトレーションテスト	**TVM-06**	独立した第三者によるペネトレーションテストを定期的に実施するためのプロセス、手順、技術的手段を定義、実施、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**

Shared (Dependent)	Shared (Dependent)	CSP-Owned

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、IaaS と PaaS で「依存する共有」である。IaaS と PaaS のサービスモデルでは、システム、リソース、および技術が、CSP または CSC の管理下に存在する可能性があり、そのようなシステム、リソース、およびテクノロジーは、設定ミス、設計または実装の不備、あるいは脆弱性が真正であるかどうかを判断するために、模擬攻撃の実行が望ましい。IaaS と PaaS では、この管理策の仕様は CSP と CSC がそれぞれ実装する。 SaaS の場合、この管理策は、「CSP が所有」し、自ら実施する責任がある。 侵入テストに価値があるシステム、リソース、および技術は、専ら CSP レイヤに存在し、CSP はこの管理策の実装と運用に単独で責任を負う。 SaaS アプリケーションの構成内には、侵入テストの一環として悪用される可能性があり、CSC が管理し改善する責任を負う脆弱性が存在する可能性がある。しかし、この様な脆弱性は、この管理策を通じて対処される侵入テストの責任ではなく、他の多くの TVM ファミリの管理策を通じて対処される脆弱性管理の責任である。 クラウドで侵入テストを実施する場合、責任共有モデルと、CSP がどのような侵入テスト活動を許可しているかをよく理解しておく必要がある。サービスレベル契約では、許可されるテストの範囲とその頻度が定義される可能性が高い。 クラウドサービスの提供モデルにかかわらず、CSP は、独立した第三者による侵入テストを定期的に実施するための手順と手続および技術的手段を定義し、実装し、評価する責任を負う。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン **全てのサービスモデルに適用：** CSP は、以下の実装のベストプラクティスを包含する包括的な侵入テスト戦略を実装すること： a. 侵入テストの範囲 i. 侵入テストの範囲は、クラウドインフラ、アプリケーション、およびデータストレージを包含するように定義されなければならない。 ii. 重要な脆弱性の特定、セキュリティ対策の有効性の評価、業界標準への準拠の検証など、各作業の目的を定める。 iii. テスト時間や本番システムへの潜在的影響など、制限事項や制約事項を特定する。 b. 承認と通知	**SaaS カスタマー：** 該当しない。 CSP は、この管理策の実装および運用に単独で責任を負う。

i. 正式な承認を上級管理職から得て、クラウド侵入テストポリシーとの整合性を確保する。
ii. CSP は、侵入テストを実施する前に、関連する利害関係者から明確な承認を取得する。
iii. CSC および関係者は、不要な警告やエスカレーションを防止するために、近日中に実施され侵入テストについて通知されるべきである。

c. 第三者ペンテスターの選定：
クラウドセキュリティよび侵入テスト手法の専門知識を有する、評判が高く経験豊富な第三者侵入テストを選定すべきである。
i. 第三者のペンテスターの資格、経験、および機密データを取り扱う能力を評価する。
ii. テスト会社は、業界標準および認証(例えば、ISO27001,CREST,OffensiveSecurityCertified Professional) に準拠すべきである。

d. エンゲージメント手続：
計画、承認から実行、報告までのプロセスを概説するエンゲージメント手続を確立すべきである。コミュニケーションチャネル、タイムライン、成果物を明記すべきである。

e. 非本番環境：
本番サービスの中断を最小限に抑え、機微データを保護するため、侵入テストの実施には非本番環境を利用すべきである。非本番環境は、現実的なテストシナリオを提供するために、本番環境を複製すべきである。

f. データの取扱いとプライバシー：
データの匿名化技術またはサニタイズされたデータセットを実装し、機微情報への不正アクセスまたは漏洩を防止すべきである。

g. 侵入テストの方法論：
侵入テストの実施は、CSP のセキュリティチームおよび関連する利害関係者との調整によって開始されるべきである。業界標準の侵入テスト手法には、OWASP、NIST、または PTES が含まれる。
i. 徹底的な偵察を実施して、アーキテクチャ、構成、潜在的な脆弱性など、クラウド環境に関する情報を収集する。
ii. オープンソースインテリジェンス (OSINT)、脆弱性スキャナ、ネットワークマッピングツールを活用し、特定された脆弱性を分析し、その重大性と潜在的な影響を評価する。
iii. 特定された脆弱性を悪用して、その実世界への影響を実証するための概念実証 (PoC) を推奨する。
iv. 特定された脆弱性、その重大性、潜在的な影響の概要を明確にするために、侵入テストの実施結果を文書化する。
v. 改善のための詳細な推奨事項は、緩和戦略および推奨されるスケジュールを含めて提供されるべ

きである。 vi. 侵入テストの結果に基づき、脆弱性改善の進捗を追跡する仕組みを確立する。 vii. 報告された脆弱性の終結を監視し、緩和戦略のタイムリーな実施を確保する。 viii. 改善努力の有効性を検証し、新たに導入された脆弱性を特定するために、フォローアップのペネトレーションテストの実施を予定すべきである。 h. 侵入テストの結果の伝達： 侵入テストの結果は、セキュリティの強化および改善に関する洞察を提供するために、上級管理職および CSC に伝達されるべきである。 i. 継続的改善： i. クラウド侵入テストのプロセスは、進化するセキュリティ脅威、クラウド技術、および業界のベストプラクティスに基づいて定期的に見直し、更新する。プログラムの有効性を維持するために、範囲、目的、および実施手順を継続的に改善する。 ii. 特定された脆弱性の数、改善された脆弱性の割合、クラウドセキュリティポスチャの全体的な改善など、クラウド侵入テストプログラムの成功を測定するための指標を定めるべきである。 CSP の許可なく侵入テストを実施することは、ほぼ確実に制限を設ける。CSP と CSC は、侵入テストの範囲が、それぞれの担当する境界に限定されるようにすべきである。 秘密保持契約（NDA）に基づき、CSC は CSP に対し、CSP が使用するアプリケーションに関する侵入テストの結果の概要を要求し、特定された脆弱性がどのように追跡され、改善後に検証されるかを知ることができるかもしれない。	

Control Title	Control ID	Control Specification
脆弱性の特定	**TVM-07**	組織が管理する資産の脆弱性を検出するためのプロセス、手順、技術的手段を、少なくとも月１回、定義、実施、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、IaaS,PaaS,SaaS で「依存しない共有」である。3 つのサービスモデルにおける資産とリソースは、CSP または CSC のいずれかの統制下に存在する可能性があり、それぞれのシステムおよびテクノロジーは、検出および管理されるべき脆弱性の潜在的な対象となり得るからである。IaaS と PaaS の場合、資産とリソースの潜在的な脆弱性として多くの場合、ソフトウェアの欠陥と設定ミスおよび管理上のギャップが両方に含まれ、CSP の管理下にある資産とリソースだけでなく、CSC の管理下にある資産とリソースにも存在する可能性がある。 SaaS の場合、資産およびリソースの潜在的な脆弱性には、一般に CSP の管理ドメインにおけるソフトウェアの欠陥のみが含まれ、CSP の管理ドメインと CSC の管理ドメインの両方における設定ミスおよび管理策・ギャップの脆弱性が含まれる。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **IaaS プロバイダー：** CSP は、組織が管理する資産（ホストインフラストラクチャ、ネットワークデバイス、および仮想化テクノロジ）の脆弱性を検出するための手順と手続および技術的手段を、少なくとも月次で、定義し、実装し、および評価する責任を負う。 IaaS の CSP が実施する脆弱性識別のガイドラインには、以下が含まれる（但し、これらに限定されない）： a. 自動化された脆弱性スキャン： 脆弱性スキャンツール（オープンソースの OpenVAS など）を定期的に使用し、IaaS 環境内の仮想マシン、オペレーティングシステム、ネットワークデバイス、ストレージの脆弱性を特定し、評価する。 b. ネットワークトラフィックの監視： ネットワークトラフィックを監視し、脆弱性の存在を示す不審なパターンを検出する。大量のデータ転送や不正なソースからの接続など、異常なトラフィックパターンを探す（Nmap、Wireshark、Nikto などのオープンソースツールを活用するなど）。 c. 侵入テスト： ツール（オープンソースの Metasploit など）を使って、仮想マシンやネットワークデバイスの設定など、IaaS コンポーネントへの攻撃をシミュレートする侵入テストを定期的に実施する。 **PaaS プロバイダー：** CSP は、組織が管理する資産（ホストインフラストラクチャ、仮想化技術、オペレーティングシステムプラットフォーム、アプ	**実施ガイドライン：** **IaaS 利用者：** CSC は、組織が管理する資産（ホストインフラストラクチャ、ネットワークデバイス、仮想化技術）の脆弱性を検出するための手順と手続および技術的手段を、少なくとも月次で、定義し、実装し、および評価する責任を負う。 CSP に提供される「実施ガイドライン」とツールが適用される。 **PaaS 利用者：** CSC は、組織が管理する資産（プラットフォームアプリケーション）上の脆弱性を検知するための手順と手続および技術的手段を、少なくとも月次で、定義し、実施し、および評価する責任を負う。 CSP に提供される「実施ガイドライン」およびツールが適用される。 **SaaS 利用者：** CSP は、独自のセキュリティ対策を実施するが、CSC もまた、脆弱性に対処し、防御を強化するための具体的な実施責任を負う。 SaaS の CSC が脆弱性を特定するための実施ガイドラインには、以下が含まれる（但し、これらに限定されない）： a. 設定の逸脱の特定： 契約している SaaS アプリケーションについて、セキュアな設定標準を確立し、設定標準に照らし合わせて設定を定期的に見直し、逸脱の可能性を特定すべきで

リケーションのソフトウェア開発、データベースなど）の脆弱性を検出するための手順と手続および技術的手段を、少なくとも月次で、定義し、実装し、および評価する責任を負う。

PaaS の CSP が実施する脆弱性識別のガイドラインには、以下が含まれる（但し、これらに限定されない）：

a. 静的アプリケーションセキュリティテスト(SAST):SAST ツール（オープンソースの SonarQube、OSV-Scanner など）を開発ライフサイクルに統合し、PaaS プラットフォーム上に構築されたアプリケーションのソースコードと依存関係の脆弱性を特定する。このようなツールは、ソースコードをスキャンして、SQL インジェクション脆弱性やクロスサイトスクリプティング（XSS）脆弱性などの潜在的なセキュリティ上の欠陥を特定することができる（例えば、オープンソースのツール sqlmap を活用する）。

b. 動的アプリケーションセキュリティテスト（DAST）：
アプリケーションの実行中に脆弱性を特定するための動的テストを実施する（OWASP Zed Attack Proxy（ZAP）のようなオープンソースツールの活用を検討する）。

c. コンテナセキュリティスキャン：
コンテナセキュリティスキャンツール(オープンソースの Clair など）を CI/CD パイプラインに統合し、コンテナイメージの脆弱性を特定する。

SaaS プロバイダー：

CSP は、組織が管理する資産（ホストインフラストラクチャ、ネットワークデバイス、仮想化技術、オペレーティングシステム、データベースなどのプラットフォームアプリケーション、および Web アプリケーション）上の脆弱性を検出するための手順と手続および技術的手段を、少なくとも月次で、定義し、実装し、および評価する責任を負う。

SaaS の CSP の脆弱性識別の実施ガイドラインには、以下が含まれる（但し、これらに限定されない）：

a. アプリケーションセキュリティ評価:手作業によるコードレビューとオープンソースの自動スキャナ（Bandit、ESLint、Wapiti、OpenSCAP、Nikto2、Burp Suite Community Edition、MobSF など）を組み合わせて、SaaS アプリケーションと Web アプリケーションの徹底したセキュリティ評価を実施する。

b. API セキュリティテスト：
関連ツール（オープンソースの Postman や OWASP API Security Project など）を使用して、SaaS アプリケーションで使用される API のセキュリティをテストする。

c. データ保護対策：
暗号化、アクセス制御、データ損失防止（DLP）ポリシー（OpenDLP のようなオープンソースツールの活用など）など、SaaS アプリケーション内機微データを保護ある。

b. アクセス制御の誤設定の特定：
ユーザーアクセスの役割とユーザプロセスのアクセス許可をレビューし、最小特権の原則に沿っていることを確認する。

c. 脆弱なデフォルト設定の特定：

i. SaaS アプリケーションのデフォルトアプリケーション設定及び構成をレビューし、潜在的なセキュリティ上の弱点を特定する。

ii. SaaS アプリケーション設定のセキュアな構成について、SaaS の CSP セキュリティガイドラインとの整合性を確保するため、及び／又は、業界のベストプラクティスを確保するため、デフォルト設定を定期的に評価する。

d. API の誤設定の特定：
API ドキュメントとアクセスログをレビューし、潜在的な API の脆弱性を特定する。

e. データ暗号化特定の欠如：
SaaS アプリケーション内に保存されている機密データを特定し、それが静止時および転送時に暗号化されているかどうかを判断する。

f. MFA の欠如：
SaaS アプリケーションの認証設定を確認し、MFA が有効になっているかどうかを判断する。

g. 不十分なログと監査の識別：
ロギングと監査の構成を見直して、SaaS アプリケーションに関連するセキュリティイベントが記録されていることを確認する。

h. パッチ欠落の特定：
SaaS アプリケーションとクラウドサービスのセキュリティ更新を定期的に確認し、適用する。

i. ネットワークセキュリティの誤設定の特定：
ファイアウォールルール及びネットワークセキュリティ設定を見直し、SaaS アプリケーションを保護するように適切に設定されていることを確認する。

j. シャドーIT の特定：
シャドーIT 検出ツールを導入し、未承認の SaaS アプリケーションの使用を特定する。承認されていない SaaS アプリケーションの使用を報告するよう従業員に奨励する。

k. 不適切なデータ保有の特定：
保有データとデータ保有ポリシーを見直し、規制要件とビジネスニーズに合致していることを確認する。

l. インシデント対応手順の欠如：
SaaS アプリケーションが関係するセキュリティインシデントに対処するための明確なインシデント対応手順を確立する。

m. CSP 脆弱性レポート：
SaaS アプリケーションの脆弱性を特定するために、

するための対策を実施する。

全てのサービスモデルに適用：

脆弱性を特定するための実施上のベストプラクティスには、以下が含まれる（但し、これらに限定されるものではない）：

a. 脆弱性スキャンツールとスケジュール：
   i. 脆弱性スキャンツール（可能であれば自動化）を活用し、クラウドインフラ、アプリケーション、データについて既知の脆弱性を定期的にスキャンする。
   ii. 脆弱性スキャンツールを CI/CD パイプラインに統合し、開発プロセスの早い段階で脆弱性を特定し、対処する。
   iii. 新たに発見された脆弱性をタイムリーに検出し、潜在的な攻撃にさらされる機会を最小化するために、定期的なスキャンスケジュールを定めるべきである。
b. ログ分析：
   クラウドインフラストラクチャコンポーネントからのログを分析し、異常や潜在的なオープン脆弱性（不適切に定義されたアクセスルール、システム構成のギャップなど）を特定すべきである。
c. 脅威インテリジェンスフィード：
   脅威インテリジェンスフィードを活用して、新たな脆弱性、脅威の傾向、悪用された脆弱性に関する情報を常に入手し、攻撃者に積極的に狙われている脆弱性に焦点を当てながら、脆弱性のスキャンと修正作業の優先順位をつけるべきである。
d. 脆弱性データベースと CVE：
   i. 既知の脆弱性に関する脆弱性データベースは、脆弱性インシデントから学んだ教訓を継続的な改善のために統合する。
   ii. このデータベースは、脆弱性を特定し、優先順位をつけるための参照点として機能する最新の共通脆弱性（Common Vulnerabilities and Exposures：CVEs）で維持され、定期的に更新する。
e. 脆弱性評価と侵入テスト（VAPT）：
   自動化されたスキャンツールでは、検出されない潜在的脆弱性を特定し、悪用するために、定期的に VAPT の訓練に参加する（TVM-06 を参照）。
f. 構成管理：
   構成管理ツール（オープンソースの Ansible など）を活用し、セキュアな構成を実施し、構成ミスのリスクを低減する。
g. 報告とエスカレーションの手順：
   特定された脆弱性の報告およびエスカレーション手順を実装すべきである。
   i. これらの手続は、改善の責任者、脆弱性に対処するためのスケジュール、重大またはハイリスクの脆弱性の場合のエスカレーションの仕組みの概要を示

SaaS ベンダーからの脆弱性レポートを定期的にレビューする。

CSC は、CSP に対して、自らが利用するアプリケーションについて特定された脆弱性の概要を要求できるようにし、その脆弱性がどのように追跡され、改善後に検証されるかを知ることができるようにする。

全てのサービスモデルに適用：

CSP の「実施ガイドライン」が適用される。

す。 ii. CSP は、リスク許容度の範囲内で、適切なツール、関連する自動化、及び運用フレームワークを使用して、脅威及び脆弱性、並びに外部ライブラリの脆弱性から保護するためのガイドラインを CSC に提供する。 h. 継続的なモニタリングと評価： 脆弱性特定プロセスの有効性は、継続的に監視し、評価し、必要に応じて調整を行う。 統合 TVM システムは、脆弱性を終結まで追跡し、残存リスクの監視を構築するために報告すべきである。さらに、システムは、将来の改善活動で再利用可能な情報を保持すべきである。 CSP は、検出された脆弱性を外部の関係者に伝達できるようにするために、外部向けの脆弱性開示プログラムの確立を検討すべきである。	

Control Title	Control ID	Control Specification
脆弱性の優先順位付け	**TVM-08**	業界で認知されているフレームワークを使用して、脆弱性修正の優先順位を効果的に行うためのリスクベースのモデルを使用する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策の実施責任は、CSP と CSC で共有され、クラウドサービスモデル（IaaS/PaaS/SaaS）に関係なく、自らのビジネスニーズとコンプライアンス要件に従って、脆弱性の優先順位を設定するためのリスクベースモデルを実施する独立した責任を負う。CSP と CSC の各当事者は、自らが所有しセキュアに管理する資産内で特定された脆弱性の改善に責任を負う	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 脆弱性の優先順位の設定は、CSP がクラウド環境のセキュリテ	**実施ガイドライン：** 仮想マシン、プラットフォームアプリケーション上の全ての特定された脆弱性について、CSC は、以下に限定されないが、

ィリスクを効果的に管理・軽減するために不可欠なセキュリティ管理策である。潜在的な影響と悪用の可能性に基づいて脆弱性に優先順位を付けることで、CSP は最も重要な脅威にリソースを集中し、クラウドインフラストラクチャの全体的な攻撃対象ドメインを縮小することができる。

ホストインフラストラクチャ、ネットワークデバイス、仮想化技術、オペレーティングシステム、データベースなどのプラットフォームアプリケーション、および Web アプリケーションで特定された全ての脆弱性について、CSP は、脆弱性修正の効果的な優先順位を設定しのために、リスクベースのモデルを使用する：CVSS、OWASP リスク評価手法など（但しこれらに限定されない）。

脆弱性は、相対的なリスク、重要性、組織への影響、および緊急性の観点から優先順位を設定しされるべきである。影響度を評価する場合、CSP は、その特定の使用方法、および/または、実装から適用可能な脅威への曝露レベルを考慮するものとする。重要性を評価する場合、CSP は、影響を受ける資産の重要性と価値を考慮するものとする。最後に、緊急性を評価する場合、CSP は、CVSS 評価と時間枠、現在進行中の脅威との関連性、および改善に必要な労力を考慮する。

脆弱性の優先順位を設定しの実施におけるベストプラクティスには、以下のものが含まれる（但し、これらに限定されない）：

a. リスクに基づく脆弱性の優先順位を設定し：
   i. クラウド組織にとって最大のリスクをもたらす脆弱性は、その重大性、悪用の可能性、潜在的な影響に基づいて、最初に優先順位を設定する。
   ii. 脆弱性の優先順位を設定しマトリックスは、意思決定の指針となり、脆弱性管理への一貫したアプローチを保証するために使用する。
b. 脆弱性スコアリングシステム（CVSS）：
   CVSS は、脆弱性管理プロセスに統合され、潜在的な影響と悪用可能性に基づいて脆弱性の深刻度を評価するために使用すべきである。CVSS を使用することで、CSP は、脆弱性に客観的な優先順位を設定し、改善の取り組みについて情報に基づいた意思決定を行うべきである。
c. 脅威インテリジェンスフィード：
   脅威インテリジェンスフィードは、新たな脅威、脆弱性、エクスプロイトに関するリアルタイムの情報を提供し、脆弱性の優先順位を動的に決定するために脆弱性管理プロセスに統合すべきである。
d. 資産の重要性：
   脆弱性の優先順位を設定しは、影響を受ける資産の重要性を考慮すべきである（すなわち、機微データを保存している資産や重要なビジネス機能をサポートしている資産など、重要性の高い資産を優先的に改善する必要がある）。

業界で認知されたフレームワークを使用して、脆弱性改善の効果的な優先順位を設定しのためにリスクベースモデルを使用すべきである：
CVSS、OWASP リスク評価手法、EPSS、SSVC などの業界で認知されたフレームワークを使用する。

SaaS の CSC は、データを保護し、事業継続性を維持し、セキュリティ規制を遵守するために、利用するクラウドサービスの一部として、SaaS アプリケーションの脆弱性に優先順位をつけることを検討すべきである。

以下は、SaaS の CSC が脆弱性の優先順位を設定しのために取るべき主要なステップである：

a. SaaS の CSP の脆弱性管理（VM）プログラムを理解する：
   SaaS ベンダーの脆弱性管理（VM）プログラムの成熟度と有効性を評価し、理解すべきである。これには、SaaS ベンダーの脆弱性スキャン頻度、優先順位を設定し標準、修正プロセス、および通信プロトコルの理解が含まれる。
b. 脆弱性の開示と改善：
   脆弱性の開示、改善のスケジュール、および連絡手順に関する CSP の責任を理解する。ベンダーのサービスレベル契約（SLA）に、脆弱性管理に関連する具体的なコミットメントが含まれていることを確認すべきである。
c. 脆弱性レポートと改善の進捗状況：
   SaaS の CSP が提供する脆弱性レポートを定期的にレビューし、重要な脆弱性の改善の進捗を追跡する。この情報は、ベンダーの対応力と VM 全体の有効性を評価するために使用すべきである。
d. 独立した脆弱性スキャン：
   SaaS アプリケーションについて独立した脆弱性スキャンを実施し、CSP のスキャン作業を補完することを検討すべきである。これにより、さらなる保証を提供し、ベンダーのスキャンで見落とされた可能性のある脆弱性を特定すべきである。
e. CSC のリスク許容度：
   脆弱性の深刻度は、SaaS の CSC のリスク許容度とそのビジネスへの潜在的影響に基づいて評価されるべきである。悪用される可能性が高い場合、重要なデータに影響する脆弱性を優先し、必要不可欠なビジネス機能をサポートすべきである。
f. SaaS の CSP とのコミュニケーション：
   SaaS ベンダーと脆弱性に関するオープンなコミュニケーションを維持する。脆弱性に迅速かつ効果的に対処するために、優先順位を設定しの標準を共有し、改善計画について協力する。
g. サードパーティーによる脆弱性管理：

e. 改善ワークフロー：
CSP は、優先順位を設定しされた脆弱性に迅速かつ効果的に対処するために、明確な改善ワークフローを確立すべきである。

f. 優先順位を設定しの有効性：
脆弱性の優先順位を設定し戦略の有効性を継続的に測定し（例えば、改善時間の追跡など）、優先順位を設定し標準を改善し、全体的なセキュリティの有効性を向上させるべきである。

g. CSC との連携：
CSP は、脆弱性の優先順位設定戦略を CSC のニーズとリスク許容度により適合するように調整し、CSC と連携して、CSC が特定するセキュリティ要件と優先順位を理解すべきである。

h. 継続的な監視と評価：
CSP は、脆弱性の優先順位を設定しに関連するものを含め、進化するクラウドセキュリティのベストプラクティスを継続的に監視し、評価すべきである。

SaaS アプリケーションのセキュリティ体制の独立した評価を提供し、潜在的な脆弱性を特定するために、サードパーティーの脆弱性管理サービスの利用を検討すべきである。

h. 新たな脅威と脆弱性：
SaaS アプリケーションに影響を及ぼす可能性のある新たな脅威や脆弱性について、常に最新情報を入手できるよう、セキュリティ勧告や脅威情報フィードを継続的に監視すべきである。

i. 脆弱性優先順位決定戦略の更新：
キャピタル・サーヴィシングのビジネスニーズ及び脅威の状況が変化する中、脆弱性優先順位決定戦略を定期的に見直し、更新して、現在のリスク許容度及びセキュリティ要件に合致すべきである。

これらのステップに従うことで、SaaS の CSC は、脆弱性に効果的に優先順位をつけ、セキュリティリスクを低減し、潜在的な脅威からデータと事業運営を保護することができる。

注：秘密保持契約（NDA）の下で、かつ契約上の合意に基づいて、CSC は CSP に対し、利用するアプリケーション上で特定された脆弱性の概要と、その脆弱性がどのように追跡され、改善後に検証されるかを要求すべきである。

全てのサービスモデルに適用：
CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
脆弱性管理レポート	**TVM-09**	関係者への通知を含む、脆弱性の特定および修正活動の追跡と報告のためのプロセスを定義、実施する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠： この管理策の実施責任は、CSP と CSC で共有され、クラウドサービスデリバリモデル（IaaS/PaaS/SaaS）に関係なく、自らのビジネスニーズとコンプライアンス要件に従って、脆弱性の追跡および報告プロセスを実施する責任を負う。 CSP と CSC は、自らが所有しセキュアに管理する資産内の脆弱性識別を追跡し、報告する責任を負う。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、ホストインフラストラクチャ、ネットワークデバイス、仮想化技術、オペレーティングシステム、データベースなどのプラットフォームアプリケーション、および Web アプリケーションで特定された全ての脆弱性について、利害関係者への通知を含む、脆弱性の特定および修正活動を追跡および報告するためのプロセスを定義し、実施する責任を負う。 統合 TVM システムは、包括的な脆弱性追跡機能を持つべきである。機能には、発見と改善がいつ行われたか、影響を受けたシステム、遅延の理由（該当する場合）、利害関係者との連絡事項の追跡が含まれるものとする。 実施ガイドラインには、全てのサービスモデルに対する追跡・報告システムの以下が含まれる（但し、これらに限定されるものではない）： a. 追跡システム： 特定され、優先順位を設定しされ、改善された全ての脆弱性の記録を維持するために、追跡システムを確立する。このシステムにより、脆弱性の履歴、改善状況、および未解決の問題が表示される。 i. 追跡システムに保存される脆弱性データの形式と構造は、標準化されるべきである。 ii. 様々なソースからの脆弱性データの集計は、脆弱性スキャナ、改善ツール、サードパーティーのフィードを含め、可能な限り自動化されるべきである。 iii. CSP の API を活用して、クラウド・サービスやリソースから脆弱性データを自動的に収集し、クラウド特有の脆弱性に関するリアルタイムの可視性を提供する。 ii. 脅威インテリジェンスと脆弱性情報を CSC と共有するためのセキュアなプラットフォームを確立する。CSC が脆弱性の改善データを自社のセキュリティツールに組み込むための API と統合オプションを提供する。 b. 報告および通知： i. 改善計画を利害関係者に伝達するためのプロセス及び手順を実施し、脆弱性解決のための明確なタイムライン及び期待される結果を提供するこ	**実施ガイドライン：** アプリケーションの設定ミスの結果として特定された全ての脆弱性について、CSC は、脆弱性の特定と改善活動を追跡し、報告するためのプロセスを定義し、実施する責任があり、これには利害関係者への通知も含まれる。 さらに、秘密保持契約（NDA）または契約上の合意に基づき、CSC は、CSP が利用するアプリケーション上で特定された脆弱性の概要、及びそれらがどのように追跡され、改善後に検証されるかを CSP に要求することができる。 **全てのサービスモデルに適用：** CSP の「実施ガイドライン」が適用される。

と。 ii. 脆弱性に関するコンテキストや内容、資産の分類、脆弱性の重大性、潜在的影響、推奨される改善手順など、脆弱性情報を伝達する標準化された報告テンプレートを作成する。 iii. 報告書は、セキュリティチーム、アプリケーション所有者、ビジネス利害関係者など、さまざまな利害関係者グループの特定のニーズや関心に合わせて調整することができる。 iv. 脆弱性報告書の配布は自動化され、電子メール、セキュアなファイル共有プラットフォーム、または指定されたイントラネットチャネルを通じて、関連する利害関係者に送信される可能性がある。 v. 脆弱性の特定及び改善活動に関する通知を受ける必要のある全ての関係者を特定する（例えば、セキュリティチーム、製品開発チーム、CSC サポートチーム、及び外部監査員）。 vi. 新たに特定された脆弱性について利害関係者に通知するための通知プロトコルを定義する。このプロトコルには、通知のトリガーとなる重要度の閾値、連絡チャネル、及び重要な脆弱性のエスカレーション手順を定める。 vii. 利害関係者に送信された全ての通知の記録（日時、受信者、脆弱性の詳細を含む）を維持する。 viii. 深刻または広範な脆弱性が発生した場合に、上級管理職または外部の関係者に通知するためのエスカレーション手順が存在すべきである。	

Control Title	Control ID	Control Specification
脆弱性管理の評価指標	**TVM-10**	あらかじめ定められた間隔で、脆弱性の特定と修正に関する評価指標を確立、監視、報告する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠： この管理策の実施責任は、CSP と CSC で共有され、両者は、それぞれのビジネスニーズとコンプライアンス要件に従って、またクラウドサービスモデル（IaaS/PaaS/SaaS）に関係なく、脆弱性の特定と改善に関する測定標準を確立し、監視し、報告する責任を独立して負う。CSP と CSC はそれぞれ、自らが所有しセキュアに管理する資産内の脆弱性の特定、改善、および報告に関する評価指標の収集頻度を定めなければならない。この活動は、TVM、脆弱性スキャン、パッチ管理ポリシーなど、既存の包括的なポリシーや標準の一部とすることができる。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** ホストインフラストラクチャ、ネットワークデバイス、仮想化技術、オペレーティングシステム、データベースなどのプラットフォームアプリケーション、および Web アプリケーション上で特定された全ての脆弱性について、CSP は、脆弱性の特定と修正のための評価指標を定義された間隔で確立し、監視し、および報告する責任を負う。 統合 TVM システムを使用して、脆弱性管理プログラムに関する評価指標を収集し報告する。評価指標は、運用上の TVM 活動の対象範囲、有効性、および効率性を示すべきである。 脆弱性管理評価指標は、脆弱性を特定し、優先順位を付け、改善するための組織の取り組みの有効性を評価する際に使用されるべきである。 a. 脆弱性管理の指標を長期的に追跡し、傾向を把握し、進捗状況を評価し、セキュリティポスチャを強化するためのデータ駆動型の意思決定を行うためのプロセスを導入する（例えば、脆弱性を改善するまでの時間、クローズした脆弱性の数、脆弱性の再発などの指標について）。 b. 脆弱性管理の指標を業界標準やベストプラクティスに照らしてベンチマークし、改善ドメインを特定する。 脆弱性管理指標の例をいくつか示す： c. 脆弱性の特定率： i. 定義：組織のシステム内で新たな脆弱性が特定される割合。 ii. 指標の計算：新たに特定された脆弱性の数／総資産またはシステムの数 d. 改善までの期間： i. 定義：特定された脆弱性の修正または軽減に要する平均時間。 ii. 指標の計算：脆弱性の発見から解決までの平均時間。 e. 脆弱性の深刻度分布： i. 定義：特定された脆弱性の重大度レベルに基づく内訳（例えば、重要、高、中、低）。 ii. 指標の計算：重要度レベル別の脆弱性の割合分布。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

f. オープンな脆弱性：
    i. 定義：特定の期間にわたって追跡されたオープンな脆弱性の傾向。
    ii. 指標の計算：特定の間隔（日次、週次、月次）におけるオープンな脆弱性の数。
g. パッチ適合率：
    i. 定義：最新のパッチが適用されているシステムまたは資産の割合。
    ii. 測定標準の計算：（パッチが適用されたシステムの数／システムの総数）x100。
h. 誤検出率：
    i. 定義：報告された脆弱性のうち、後に誤検出と判断された脆弱性の割合。
    ii. 指標の計算：（偽陽性の数 / 報告された脆弱性の総数）x100。
i. 脆弱性の再スキャン率：
    i. 定義：改善効果を検証するために脆弱性スキャンを繰り返す頻度。
    ii. 指標の計算：月または四半期ごとの脆弱性再スキャンイベント数。
j. 改善された脆弱性のトップ
    i. 定義：最も頻繁に改善された脆弱性の特定。
    ii. 指標の計算：特定の脆弱性が改善された回数。
k. 脆弱性のエージング：
    i. 定義：未解決の脆弱性の平均年齢。
    ii. 指標の計算：平均脆弱性保有期間の計算方法は、脆弱性が未解決である平均時間（現在の日付-発見日）。
l. 脆弱性評価の対象範囲：
    i. 定義：脆弱性評価を定期的に受けているシステムまたは資産の割合。
    ii. 評価指標の計算：（評価対象システム数／全システム数）×100。

これらの指標は、組織が脆弱性管理プログラムの効率を測定し、改善すべきドメインを特定し、全体的なセキュリティポスチャを示すのに役立つ。

Control Domain UEM

2.17 ユニバーサルエンドポイント管理(UEM)

Control Title	Control ID	Control Specification
エンドポイントデバイスに対するポリシーと手順	**UEM-01**	全てのエンドポイントを対象とするポリシーと手順を確立、文書化、承認、周知、実装、評価、維持する。ポリシーと手順は、少なくとも年１回、レビューし、更新する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： クラウドサービスにアクセスするために使用される全てのエンドポイントデバイスは、企業ポリシーの範囲内で、業界標準に沿って管理されるべきであり、この管理策は CSP と CSC の両方にとって「依存しない形で共有」である。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** クラウドサービスデリバリモデルにかかわらず、CSP は、全てのエンドポイントに対するポリシー、標準、手順と手続およびツールの確立、通知、および実装に責任を負う。 ポリシーには、以下に関する規定が含まれるべきである（ただし、これらに限定されない）： 管理対象エンドポイントおよび非管理対象エンドポイント（BYOD を含む）の両方に対するポリシーおよび手順には、以下の構成要素を含めるべきであるべきである。 a. 対象範囲と目的：エンドポイントの定義と範囲、全てのエンドポイント（モバイルデバイス、仮想デバイス、デスクトップなど）に対する使用許容ポリシーの目的と要件。 注：物理サーバー、仮想サーバー、コンテナ、および類似のエンドポイントは、DCS および IVS ドメインで扱われ、アプリケーションおよびインタフェースのエンドポイントは、AIS ドメインで議論されている。 b. アプリケーションとサービスの承認：人員がエンドポイン	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

トで使用することを許可された、承認されたクラウドサービスおよびアプリケーションのリストを維持すること。このリストは定期的に見直し、更新されるべき（承認されたシステム、サーバー、アプリケーション、アプリケーションストア、アプリケーション拡張機能、プラグインを含む）。

c. エンドポイントの互換性：必必須アプリケーション及びセキュリティツールとの互換性を確保するため、エンドポイントに対するOSの最低要件を設定すべき。承認されたアプリケーションの互換性マトリクスを維持し、サポートされているOS上で適切に機能するようにすること。

d. エンドポイントインベントリ：ラップトップ、デスクトップ、タブレット、携帯電話、IoTデバイス、サーバー、仮想環境など、組織のネットワークに接続されている全てのエンドポイントのインベントリ（デバイスの詳細、所有者情報、セキュリティステータス、ソフトウェア構成が含まれること）を管理すること。

注：各エンドポイントデバイスは、そのデバイスに責任を持つ指名された人に割り当てられるべきである。そのようなデバイスは共有されていてもよいが（例えば、共有ワークエリア内）、一個人が責任を負うべきである。デバイス以外のエンドポイントにも、リスクを評価し、適切な管理を確保する責任を負う所有者を置くべきである。

e. エンドポイント管理：許可されたシステムやリソースへのエンドポイントのアクセスを制限するための、きめ細かなアクセス制御メカニズム。エンドポイントにおける不正なデータの保存、送信、処理を防止するため、データアクセスの制限を実施するべきである。

f. エンドポイントオペレーティングシステム：エンドポイントオペレーティングシステムの変更管理プロセスにより、構成、ソフトウェアのインストール、パッチ、および更新に対する変更を管理およびレビューすること。

g. ストレージの暗号化：ディスク全体の暗号化を全てのエンドポイントで利用し、保存中の機微データを保護すること。

h. マルウェアの検出と防止：全てのエンドポイントにリアルタイムマルウェア対策ソフトウェアを導入し、定期的なスキャンをスケジューリングすることで、悪意のあるソフトウェアの感染を検出・防止する。

i. ソフトウェアファイアウォール：全てのエンドポイントにソフトウェアファイアウォールを設定し、インバウンドおよびアウトバウンドネットワークトラフィックを制御すること。

j. データ損失防止：エンドポイントからの機微データの移動を監視および制御するために、DLPテクノロジーを構成する必要がある。データアクセス制限を実施し、外部デバイスやクラウドサービスへの不正なデータ転送を防止する。

k. リモートロケート：紛失や盗難の際に、モバイルデバイスの位置を追跡するためのリモートジオロケーション機能。

l. リモートワイプ：紛失や盗難の際に会社のデータをリモー

トで消去するため、全てのエンドポイントでリモートワイプ機能を有効にすること。デバイスの完全または部分的なワイプが必要な場合、会社以外のデータ損失に関する要件を定義すること。 m. サードパーティエンドポイントのセキュリティ体制：契約書および SLA における、サードパーティエンドポイントアクセスに関するセキュリティ要件、責任、および義務。 n. プライバシー：遠隔地での位置特定、訴訟、e ディスカバリ、証拠保全（特に個人所有のデバイス）に対するプライバシーの期待に関する要件を定義されていること。 o. 承認：組織の戦略目標およびリスク選好度との整合性を確保するための承認要件および上級管理職の関与 i. ポリシーと手順の変更または修正については、承認プロセスを確立すること。 ii. 承認の文書化された記録（日付、承認者名、関連するコメントや議論を含む）を維持すること。 p. コミュニケーション：関係する全てのクラウド利害関係者に対して、ポリシーと手順の効果的な伝達を促進すべきである。 q. 維持管理とレビュー：エンドポイントセキュリティポリシーと手順は、進化するクラウドセキュリティ環境との整合性を確保し、クラウド技術、規制、リスクの変化を反映するために、少なくとも年 1 回文書化し、レビューし、更新すべきべきである。	

Control Title	Control ID	Control Specification
アプリケーションおよびサービスの承認	**UEM-02**	組織管理のデータへのアクセスや保存の際、エンドポイントでの使用を許可する、承認済のサービス、アプリケーション、および、アプリケーションの入手先（ストア）の一覧を定義、文書化、適用、評価を行う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**

管理策所有権の根拠： CSP と CSC は、オペレーティングシステム（OS）／プラットフォーム（これらに限定されない）に基づくクラウドサービスへのアクセスに利用される全てのエンドポイントデバイスにインストール可能なアプリケーションの承認済みリストを維持する必要があるため、この管理策は CSP と CSC の両方にとって「依存しない形で共有」である：Linux、Windows、MacOS、Android、iOS など。これは、サービスデリバリモデル（IaaS、PaaS、SaaS）を特定するものではない。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** クラウドサービスデリバリモデルに関係なく、CSP は、組織が管理するデータへのアクセスまたは保存時にエンドポイントが使用することが許容される、承認されたサービス、アプリケーション、およびアプリケーションのソース（ストア）のリストを定義、文書化、適用、および評価する責任を負う。 実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. 集中型構成：管理対象エンドポイントに対して、1 つまたは複数の集中型構成管理ツールによってポリシーを普遍的に適用する。 b. 管理対象外エンドポイントのリスク管理：管理されていないエンドポイントを使用して、どのような（もしあれば）情報またはシステムにアクセスまたは保存される可能性があるかを判断するために、リスクアセスメントを実施すること。 c. 承認されたストアの使用：公式アプリストアや社内リポジトリ（Linux、Windows、MacOS、Android、iOS など）など、信頼できるベンダーのアプリケーションのみを入手するための承認されたソース（ストア）を維持すること。 d. 無許可の店舗利用の例外：組織の例外承認プロセス/サイクルに従った後、ビジネス上の必要性が存在しない限り、未承認ソースからのアプリケーションのインストールは禁止されるべきである。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
互換性	**UEM-03**	オペレーティングシステムやアプリケーションに対する、エンドポイントデバイスの互換性を検証するプロセスを定義し、実装する。
Control Ownership by Service Model		

IaaS	PaaS	SaaS
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC の双方にとって「依存しない形で共有」である。なぜなら、CSP と CSC の両方は、オペレーティングシステムおよびアプリケーションとエンドポイントデバイスの互換性を確保するために、文書化されたプロセスと手順を備えているはずだからである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** クラウドサービスの提供モデルにかかわらず、CSP は、エンドポイントデバイスとオペレーティングシステムおよびアプリケーションとの互換性を検証するプロセスを定義し、実装する責任を負う。 CSP は、エンドポイントが企業ネットワークにアクセスすることを許可される前に、エンドポイントのセキュリティ機能のコンプライアンス違反をチェックし、改善活動を自動化する診断ツールを実装すべきである。 CSP は、モバイルデバイス、オペレーティングスステム、およびアプリケーションに関する互換性の問題をテストするための、文書化されたアプリケーション検証プロセスを持つべきである。管理を簡素化し、互換性の問題を軽減するために、組織全体でオペレーティングシステムのバージョンを統一すべきである。 エンドポイントの設定ミスは、運用に影響を与えるだけでなく、攻撃ベクトルをもたらす可能性があり。不適切な構成設定には、オープンポート、時代遅れの例外、許可されたセキュアでないプロトコルが含まれる可能性がある。本番稼動後の設定変更は、変更管理ガイドライン（なぜ、何を、どのように）に従い、適切な承認を得るべきである。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification

エンドポイントのインベントリ	**UEM-04**	企業データの保存やアクセスに使う全てのエンドポイントをインベントリに保持する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC はともに、組織データの保存およびアクセスに使用される全てのエンドポイントの正確かつ最新の集中管理されたインベントリを維持する必要があるため、この管理策は CSP と CSC の両方にとって「依存しない形で共有」である。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** クラウドサービスデリバリモデルに関係なく、CSP は、組織のデータの保存およびアクセスに使用される全てのエンドポイントの正確かつ最新の一元的なインベントリ（DCS-06 を参照）を維持する責任を負う。 CSP は、組織のネットワークに接続されている全てのエンドポイントデバイスを識別し、資産インベントリを更新するために、ディスカバリツールを実装するものとする。 可能な場合、CSP は、資産目録に、各資産のネットワークアドレス、ハードウェアアドレス、デバイス名、資産所有者、および部署、並びに資産がネットワークに接続することを承認されているかどうかが記録されるようにする。 CSP は、許可されていないエンドポイントがネットワークから削除され、隔離され、または適時にインベントリに追加されるようにするべきである。 会社のデータを保存し、アクセスするために使用される全てのモバイルデバイスのインベントリを保管、維持し、デバイスの所有、構成、およびソフトウェアのバージョンの変更を反映するために定期的に更新すべきである。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
エンドポイントの管理	**UEM-05**	システムへのアクセスを許可されている、もしくは、組織のデータを保存、転送、処理する、全てのエンドポイントに対して、ポリシーと管理策を強制するため、プロセス、手続き、および技術的対策を定義し、実装、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： CSP と CSC はそれぞれ、理想的には一元化された構成管理ツールを使用して、全てのエンドポイントに対してそれぞれのポリシーと管理を一律に実施するための対策を実施する必要があるため、この管理策は CSP と CSC の両方にとって「依存しない形で共有」である。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. エンドポイントの管理：システムへのアクセスおよび／または組織データの保存、送信、処理を許可されたエンドポイントを管理するための管理を実施するための技術的手段。 b. エンドポイントのアクセス制御：代替の保護メカニズムが使用される場合、どのようなエンドポイントタイプがシステムアクセスや情報保管に許容されるかを判断するためのリスク評価。 c. 集中型構成：管理されたエンドポイントでは、1 つ以上の集中型構成管理ツールによるポリシーの普遍的な実施 d. エンドポイントのセキュリティ侵害防止：エンドポイントにおける、ベンダーがサポートする、または統合された（ビルトインの）セキュリティ制御の侵害（ジェイルブレイクやルート化など）は禁止されるべきです。これらの制限は、一元化されたシステム（エンドポイントシステム構成管理、またはモバイルデバイス管理システムなど）を通じて管理される、エンドポイント上の検知および予防的管理策を通じて実施されるべきである。 e. 非管理エンドポイントの堅牢化管理対象外のエンドポイントについては、デフォルト設定の更新、不要なサービスの無効化、エンドポイント上のデータの暗号化、管理対象外のエ	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

ンドポイントをメインネットワークからセグメント化するなど、エンドポイントを堅牢化するためのベストプラクティスを検討するべきべきである。	

Control Title	Control ID	Control Specification
自動ロック画面	**UEM-06**	対話型に使用する全てのエンドポイントに、自動ロック画面を構成する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC の双方にとって「依存しない形で共有」である。なぜなら、それぞれの対話式使用エンドポイントが自動ロック画面を要求するように構成するべきであるからである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 非アクティブタイムアウトは、エンドポイントデバイスが指定された期間アイドル状態になると自動的にロック画面が起動するように設定するべきである。セキュリティロックアウト制御は、あらかじめ定義された時間が経過してもエンドポイントがユーザーとの対話からアイドル状態のままである場合に、自動的に開始するべきである。その後、ユーザーはエンドポイントにアクセスするために認証情報を再入力すべきである。 ロック画面の設定は、ロック解除に強力なパスワード、バイオ評価指標認証、またはパスワードレス認証（デバイスの PIN、指紋認証）を必要とするように構成すべきである。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification

オペレーティングシステム	**UEM-07**	企業の変更管理プロセスを通して、エンドポイントのオペレーティングシステム、パッチレベル、および、アプリケーションの変更を管理する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC の双方にとって「依存しない形で共有」である。なぜなら、CSP と CSC はそれぞれ、それぞれの変更管理プロセスを通じて、エンドポイント OS とアプリケーションへのパッチを含む変更を管理すべきであるからである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 組織は、エンドポイントのオペレーティングシステムとアプリケーションに最新のセキュリティパッチを適用し、変更が管理された一貫性のある方法で実行されるように、正式な変更とパッチの管理プロセスを含めるべきである(CCC ドメインを参照)。脆弱性ウィンドウを最小化し、悪用のリスクを低減するために、パッチのデプロイを自動化する。 エンドポイント OS の変更管理に関する実装のベストプラクティスには、以下が含まれま（ただし、これらに限定されない）： a. エンドポイントの変更管理： i. 重要な変更の特定と記録 ii. 変更の計画とテスト iii. 当該変更の潜在的影響（セキュリティ上の影響を含む）の評価 iv. 変更案の正式承認 v. 各利害関係者への変更内容の伝達 vi. 変更に失敗した場合や不測の事態が発生した場合のロールバック手順	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification

ストレージの暗号化	**UEM-08**	ストレージの暗号化により、管理対象エンドポイントデバイスの情報を不正な開示から保護する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC の双方にとって「依存しない形で共有」である。その実施は、サービスデリバリモデル（IaaS、PaaS、または SaaS）に固有ではない。CSP と CSC の両方が、それぞれのエンドポイントデバイス上でストレージ暗号化を実施する責任を負う。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** CSP は、保護対象のデータの機密性に基づいて、正式な暗号化ポリシーを文書化すべきである。さらに、CSP は、ファイル暗号化、フルディスク暗号化、エンドポイント保護など、さまざまなレベルの暗号化を実施する技術を活用すべきである。 CSP は、業界標準の暗号化アルゴリズムを利用し、機微データとして識別されるデータには強力な暗号化 を使用するものとする。 可能な限り、CSP はまた、以下を行うべきである： a. エンドポイントのディスク暗号化：機微データとして認識されるデータを保存するエンドポイントデバイスに、フルディスク暗号化を導入する。 b. エンドポイントコンテナセキュリティ：コンテナテクノロジーを活用し、モバイルデバイス上の機微データを保護・暗号化する。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
マルウェア対策による検知と保護	**UEM-09**	管理対象のエンドポイントに、マルウェア対策による検知と保護に必要な技術やサービスを構成する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC の双方にとって「依存しない形で共有」である。なぜなら、両者とも悪意ある行為者による悪用のリスクを軽減するために、マルウェア対策ソフトウェアを含むプロセスと技術について、エンドポイントセキュリティを実施すべきであるからである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 最新の脅威から確実に保護するために、マルウェア対策ソフトウェア、シグネチャ、ウイルス定義のインストールと定期的な更新（自動更新）を含みます（TVM-02 も参照）。 CSP は、インストールされたソフトウェアおよびシステムデータコンテンツを定期的に見直してスキャンし、可能な場合は不正なコード/ソフトウェアを特定して削除するものとする。悪意のあるコードまたは未承認ソフトウェアの特定に対応する手順を定義するものとする。 外部ネットワークからデータやソフトウェアを入手することを制限するなど、不正なソフトウェアの使用やインストールを禁止するための技術的対策を実施すべきである。 また、可能な限り、組織は以下を行うべきである： a. エンドポイントリムーバブルメディア管理：USB、CD、DVD、ハードドライブ、FireWire デバイス、eSATA デバイスなどのリムーバブルメディアの使用を管理する。 b. エンドポイントアプリケーションのホワイトリスト化：許可されたソフトウェアのみが実行され、マルウェアを含む全ての許可されていないソフトウェアがブロックされるように、アプリケーションホワイトリスト技術を導入する。 c. BYOD マルウェア対策：全ての BYOD デバイスがマルウェア対策ソフトウェアを活用するようにする。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
ソフトウェアファイアウォール	**UEM-10**	管理対象のエンドポイントに、適切に設定したソフトウェアファイアウォールを構成する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC の双方にとって「依存しない形で共有」である。それぞれのエンドポイントにおいて、適切に構成されたファイアウォールを維持すべきである。エンドポイントファイアウォールは、トラフィックを検査し、ルールを適用し、動作監視を実行する。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** 構成には、全てのエンドポイントにファイアウォールソフトウェアおよびファイアウォールルールを（自動的に）インストールし、定期的に更新することが含まれるものとする。CSP は、ファイアウォールルールを定期的にレビューおよびスキャンして、未承認のルールが存在しないことを確認すべきである。 実施上のベストプラクティスには、以下が含まれる（ただし、これらに限定されません）： a. エンドポイントファイアウォールセキュリティ i. 全てのエンドポイントに現在有効な基本ルールセットがあることを確認すること。 ii. 基本ルールの変更が、文書化された変更管理プロセスを通じて適切に承認されるようにする。 iii. 文書化された変更管理プロセスを通じて、新しいルールが適切に承認されていること。 iv. ハイパーテキストマークアップ言語（HTML）、JavaScript、ハイパーテキストトランスファープロトコル（HTTP）などの Web トラフィックに悪意のあるコードが含まれていないかチェックすること。 v. 通常のトラフィックパターンを超える異常に注意し、適切な対処を行うこと。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
データ漏洩防止	**UEM-11**	管理対象のエンドポイントに、データ漏洩防止（DLP）技術を構成し、リスクアセスメントに従ったルールを構成する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC の双方にとって「依存しない形で共有」である。なぜなら、CSP と CSC はそれぞれ、全てのエンドポイントをカバーし、適切なルールが定義され、実施され、監視、警告、および対応プロセスが整備された、効果的なデータ漏えい防止（DLP）プログラムを実施することによって、データ漏えいを防止すべきであるからである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** DLP プログラムの実装のベストプラクティスには以下が含まれる（ただし、これらに限定されるものではない）： a. エンドポイントのデータ分類：ビジネス、顧客、クライアント、パートナー、および規制上の義務に対する機密性に基づいてデータを分類する正式なデータ分類標準（DSP ドメインを参照）。 b. エンドポイントデータインベントリ：構造化データおよび非構造化データのインベントリ。 c. エンドポイントデータ保護：ネットワーク、ストレージ、エンドポイントシステムを横断し、転送中および静止中に規制やコンプライアンスに関わるデータを発見、監視、保護する。 d. エンドポイントデータ監視：機密情報（個人情報、特殊キーワード、メタデータなど）を監視し、ネットワーク境界を越えた不正な開示の試みを発見し、情報セキュリティ担当者に警告することでそのような転送をブロッ	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

クする。組織は、データがサーバーからコピーされた場合でも ACL が適用されるように DLP ソリューションを構成すべきである。 e. エンドポイント SOP の定義：データ漏えい事象を処理するために定義された標準作業手順（SOP） f. エンドポイント DLP ポリシー違反の検出：DLP ポリシー違反を検出し、SOP に基づいて是正措置を講じる。さらに、正常なトラフィックパターンを超える異常があれば、それを指摘し、適切な対処を行うこと。	

Control Title	Control ID	Control Specification
リモート追跡	**UEM-12**	全ての管理対象のモバイルエンドポイントに、リモートからの位置情報追跡を有効にする。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： エンドポイントデバイスが紛失または盗難された場合、CSP と CSC の両方がエンドポイントデバイスをリモートで管理できる必要があるため、この管理策は CSP と CSC の両方にとって「依存しない形で共有」である。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** クラウドサービスの提供モデルにかかわらず、CSP と CSC はともに、エンドポイントデバイスが紛失または盗難にあった場合、リモートで追跡できるようにする責任がある。 リモートジオロケーションの実施におけるベストプラクティスには、以下が含まれる（ただし、これらに限定されるものではない）： a. エンドポイントリモートロケート i. プロビジョニングまたは BYOD を問わず、エンドポイントデバイスのインベントリ ii. デバイスの所在を特定するために利用される、GPS またはネットワークベースの位置情報サービス。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

iii. エンドポイントがトラッキングから外れたら、レスポンスチームにアラートを出すこと CSP は、BYOD プログラムがサポートするさまざまな種類のエンドポイントデバイスでリモートワイプ機能を定期的にテストし、テスト証拠を保存すべきである。	

Control Title	Control ID	Control Specification
リモートワイプ	**UEM-13**	管理対象のエンドポイントデバイスから企業のデータをリモート消去するため、プロセス、手順、および技術的対策を定義し、実装、評価する。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC の双方にとって「依存しない形で共有」である。なぜなら、CSP と CSC はそれぞれ、モバイルデバイスを紛失または盗難された場合に、リモートで管理すべきであるからである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** クラウドサービスの提供モデルに関係なく、CSP と CSC はともに、プロビジョニングまたは BYOD を問わず、エンドポイントデバイスを紛失または盗難した場合、リモートで追跡し、企業データを削除し、または完全に消去できるようにする責任がある。 リモートデータ消去の実施におけるベストプラクティスには、以下が含まれる（ただし、これらに限定されない）： a. エンドポイントのリモートワイプ： i. プロビジョニングまたは BYOD を問わず、エンドポイントデバイスのインベントリ。 ii. ジオロケーショントラッキングを設定し、GPS またはネットワークベースのロケーションサービスを利用してデバイスの所在を特定。	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

Control Title	Control ID	Control Specification
サードパーティーのエンドポイントに対するセキュリティポスチャ	**UEM-14**	サードパーティーのエンドポイントが組織の資産にアクセスする際、適切なセキュリティを維持するため、プロセス、手順、および、技術や契約による対策を定義、実装、評価を行う。

Control Ownership by Service Model		
IaaS	**PaaS**	**SaaS**
Shared (Independent)	Shared (Independent)	Shared (Independent)

SSRM Guidelines	
CSP	**CSC**
管理策所有権の根拠： この管理策は、CSP と CSC の双方にとって「依存しない形で共有」である。なぜなら、CSP と CSC はそれぞれ、サードパーティーに組織のデータへのアクセスを許可する前、または接続を確立する前に（そしてその後、サードパーティーとの関係のリスクレベルに応じて定期的に）、デューデリジェンスを実施すべきであるからである。	**管理策所有権の根拠：** CSP の「管理策所有権の根拠」が適用される。
実施ガイドライン： **全てのサービスモデルに適用：** クラウドサービスの提供モデルにかかわらず、CSP と CSC はともに、組織の資産にアクセスするサードパーティー製エンドポイントの適切なセキュリティを確保する責任を負う。 a. *サードパーティエンドポイントのアクセス管理*：クラウドアイデンティティとクラウドアイデンティティアンドアクセス管理（IAM）ツールを活用する。 b. サードパーティエンドポイントの隔離：サードパーティエンドポイントのトラフィックを機密性の高い内部リソースから隔離するために、ネットワークのセグメンテーションを実施する。 c. サードパーティー製エンドポイントセキュリティツール：エンドポイントセキュリティソフトウェア（ウイルス対策、エンドポイント検出および対応）のインストールおよび設定は、全ての許可されたサードパーティデバイスに対して実施されるべきである。 d. サードパーティエンドポイントのセキュアな経路：サードパーティエンドポイントと組織資産との間の全てのデータ	**実施ガイドライン：** CSP の「実施ガイドライン」が適用される。

転送について、セキュアな通信経路（VPN など）を確保する。

e. サードパーティエンドポイント契約：CSP とサードパーティーの間で、サードパーティーが CSP に代わってデータを保存、処理、または送信する際のセキュリティについて責任を負うことを認める書面合意（契約）を締結し、維持するものとする。契約には、認証、承認、データ暗号化、およびデバイス管理に関するガイドラインなど、サードパーティーのエンドポイントアクセスに関連する情報セキュリティリスクに対処するための要件を含めるべきある。これらの要件は、その後、サプライチェーン全体を通じて関連する第 3 者下請業者に適用される。

f. 第三者契約条項：最低限、以下を明記した正式な契約：

  i. 組織のクラウド資産にアクセスするサードパーティーのエンドポイントに関連する潜在的な脆弱性を特定するための、CSC との共同リスク評価。

  ii. 対象となる情報の機密性と価値

  iii. セキュアなアクセスに対応するデバイスとオペレーティングシステムの種類

  iv. 適用される連邦法、行政命令、指令、ポリシー、規制、標準、ガイダンスによって要求される、実施および/または遵守されるセキュリティ対策。
  サードパーティエンドポイントのアクセス制限

  v. サードパーティー製エンドポイントソフトウェアのパッチ適用とアップデートの責任

  vi. 提供されるサービスにおいて達成されるべきサービスレベル

  vii. CSP の情報セキュリティ管理フォーラムへの報告の形式と頻度

  viii. 適切な組織の会合や作業部会における第三者代表の手配

  ix. 契約上の合意や規制要件への準拠を確保するための第三者によるセキュリティ評価の取り決め（STA 参照）

  x. 前述の規定のいずれかに違反した場合に科される罰則

g. サードパーティエンドポイントの責任：サードパーティーは、CSP システムおよびデータへのアクセスを必要とする自社の要員に付与されるアクセス権限（要員のアクセス変更、アクセス権限、サードパーティーの要員による資格情報管理など）の管理を担当する特定の個人または役割（契約またはサプライチェーン機能内など）を指定すべきである。

h. 継続的な監視と評価：サードパーティーのエンドポイントアクセスに関連するログを継続的に監視し、不審なアクティビティを監視すること。

Acronyms

A

AAA: Authentication, Authorization, and Accounting
ABAC: Attribute-Based Access Control
AES: Advanced Encryption Standard
AI: Artificial Intelligence
AIS: Application and Interface Security
API: Application Programming Interface
ARP: Address Resolution Protocol
ASHRAE: American Society of Heating, Refrigerating and Air-Conditioning Engineers
AST: application security testing
ASVS: Application Security Verification Standard
AUA: Acceptable Use Agreement
AUP: acceptable use policy
AV: Anti-Virus

B

BC: Business Continuity
BCM: Business Continuity Management
BCP: Business Continuity Plan
BCR: Business Continuity Management and Operational Resilience
BCS: Business Continuity Strategy
BI: Business Intelligence
BIA: Business Impact Assessment
BLE: Bluetooth Low Energy
BMS: Building Management Systems
BSI: British Standards Institution
BYOD: Bring-Your-Own-Device
BYOK: Bring-Your-Own-Key

C

CAIQ: Consensus Assessment Initiative Questionnaire
CASB: Cloud Access Security Broker
CCB: Change Control Board
CCC: Change Control and Configuration Management
CCM: Cloud Controls Matrix
CCPA: California Consumer Privacy Act
CCTV: Closed-Circuit Television
CC: Common Criteria
CDN: Content Delivery Networks
CEK: Cryptography, Encryption and Key Management
CERT: Community Emergency Response Team
CI/CD: Continuous integration and continuous delivery
CIRT: Customer Incident Response Team
CISO: Chief Information Security Officer
CKL: Compromised Key Lists
CKMS: Cryptographic Key Management System
CMDB: Configuration Management Database
CMK: IaaS Customer: CMK model
CMK: Client Managed Key
CPU: Central Processing Unit
CR: change request
CREST: Certificateless Registry for Electronic Share Transfer
CRL: Certificate Revocation Lists
CSA: Cloud Security Alliance
CSC: Cloud Service Customer
CSO: Chief Sales Officer
CSP: Cloud Service Provider
CSRF: Cross-Site Request Forgery
CSV: Comma-Separated Values
CUA: Continuous User Authentication
CVE: Common Vulnerabilities and Exposures
CVSS: Common Vulnerability Scoring System

D

DAM: database access management
DAST: dynamic application security testing
DB: Database
DBO: Database Owner
DCS: Datacenter Security
DFD: Data Flow Diagram
DLP: data loss prevention
DMTF: Distributed Management Task Force
DMZ: Demilitarized Zone
DNS: Domain Name System
DoD: Department of Defense
DPA: Data Processing Agreement
DPIA: Data Protection Impact Assessment
DPO: Data Protection Officer
DR: Disaster Recovery
DRT: Data Recovery Time

DREAD: Damage, Reproducibility, Exploitability, Affected users, and Discoverability
DRM: digital rights management
DRP: Disaster Recovery Plan
DSAR: Data Subject Access Request
DSP: Data Security and Privacy Lifecycle Management

E

EAL: Evaluation Assurance Level
EDR: Endpoint Detection and Response
EMI: electromagnetic interference
EoL: End of Life
EPSS: Exploit Prediction Scoring System
ERM: Enterprise Risk Management
ERP: Enterprise Risk Management Program
ESP: Event Stream Processing
EU: European Union
EXCO: Executive Management/Leadership/Committee

F

FIDO: Fast Identity Online
FIM: File Integrity Monitoring
FIPS: Federal Information Processing Standard
FPE: Format-preserving Encryption
FSC: Forward Schedule of Changes
FTP: File Transfer Protocol
FTPS: File Transfer Protocol Secure

G

GDPR: General Data Protection Regulation
GPS: Global Positioning System
GRC: Governance, Risk Management and Compliance
GUI: Graphical User Interface

H

HIDS: Host-based Intrusion Detection Systems
HIPAA: Health Insurance Portability and Accountability Act
HIPS: Host-based Intrusion Prevention systems
HITRUST: Health Information Trust Alliance
HLD: High-Level Design
HROT: Hardware Roots-of-Trust
HRS: Human Resources
HSM: Hardware Security Module
HTML: Hypertext Markup Language
HTTP: Hypertext Transfer Protocol
HTTPS: Hypertext Transfer Protocol Secure
HVAC: Heating, Ventilation, and Air Conditioning

I

IAM: Identity and Access Management (IAM)
IAST: Interactive Application Security Testing
ICMP: Internet Control Message Protocol
ICO: Information Commissioner's Office
IDOR: Insecure Direct Object References
IDS: Intrusion Detection Systems
IOC: Inversion of Control
IPS: Intrusion Prevention Systems
IPSEC: Internet Protocol Security
IPY: Interoperability and Portability
IR: Incident Response
IRAP: Integrated Risk Assessment and Prioritization
IRP: Incident Response Plan
ISA: Initial Screening Assessment
IST: Instruction Specification Table
IT: Information Technology
IVS: Infrastructure and Virtualization Security

J

JIT: Just-in-Time
JSON: JavaScript Object Notation

K

KMS: Key Management System
KRI: Key Recovery Information
KSCSRI: Key Shared Cloud Security Responsibility Indicator
KSSRI: Key Shared Security Responsibility Indicators

L

LLD: Low Level Design
LOG: Logging and Monitoring

LP: Least Privilege
LPR: License Plate Recognition

M

MAC: Message Authentication Code
MASVS: Mobile Application Security Verification Standard
MDM: Mobile Device Management
MFA: Multi-factor Authentication
ML: Machine Learning
MSA: Master Service Agreements
MTCS: Managed Technology Capability Standard
MTD: Maximum Tolerable Downtime
MTTA: Mean Time to Acknowledge
MTTC: Mean Time to Containment
MTTD: Mean Time to Detect
MTTR: Mean Time to Respond

N

NDA: Non-Disclosure Agreement
NIDS: Network Intrusion Detection Systems
NIPS: Network Intrusion Prevention Systems
NIST: National Institute of Standards and Technology
NSA: National Security Agency
NTA: Network Traffic Analysis
NTP: Network Time Protocol

O

OCCI: Open Cloud Computing Interface
OCSP: Online Certificate Status Protocol
OLA: Operational Level Agreement
OR: Operational Resilience
OS: Operating Systems
OSI: Open Systems Interconnection
OSINT: Open-Source Intelligence
OSV: Open Source Vulnerabilities Database
OVF: Open Virtualization format
OWASP: Open Worldwide Application Security Project

P

PACS: Physical Access Control Systems
PAM: Privileged Access Management
PASTA: Process for Attack Simulation and Threat Analysis
PCI-DSS: Payment Card Industry Data Security Standard
PET: Privacy Enhancing Techniques
PHI: protected health information
PIDS: Perimeter Intrusion Detection Systems
PII: Personal Identifiable Information
PIN: Personal Identification Number
PIPS: Perimeter Intrusion Prevention Systems
PP: Protection Profiles
PPTP: Point-to-Point Tunneling Protocol
PTES: Penetration Testing Execution Standard

Q (empty)

R

RACI: Responsible, Accountable, Consulted, and Informed
RASP: Runtime Application Security Protection
RBAC: Role-based Access Control
REST: Representational State Transfer
RFC: Request for Comments
RFID: radio frequency identification
RFP: Request For Proposal
RFQ: Request for Quote
ROI: return on investment
RPO: Recovery Point Objective
RSA: Rivest–Shamir–Adleman
RSS: Really Simple Syndication
RTO: Recovery Time Objective

S

SAN: Storage Area Network
SANS: SysAdmin, Audit, Network, and Security
SAST: Static Application Security Testing
SCA: Software Composition Analysis
SCP: Secure Copy Protocol
SCCS: Standard Contractual Clauses
SD: Secure Digital
SDLC: Software Development Lifecycle
SEF: Security Incident Management, E-Discovery, and Cloud Forensics
SFTP: Secure File Transfer Protocol
SIEM: Security information and Event Management
SLA: Service Level Agreement
SLD: Systems Logical Design

SMART: Specific, Measurable, Achievable, Relevant, and Time-bound.
SME: Subject Matter Expert
SMS: Short Message Service
SMTP: Simple Mail Transfer Protocol
SMART: Specific, Measurable, Achievable, Relevant, and Time-bound.
SME: Subject Matter Expert
SMS: Short Message Service
SMTP: Simple Mail Transfer Protocol
SNMP: Simple Network Management Protocol
SOAP: Simple Object Access Protocol
SOAR: Automated Security Orchestration and Response
SOC: System and Organization Controls Audit Report
SOP: Standard Operating Procedures
SOX: Sarbanes-Oxley Act
SPOC: Single-Point of Contact
SQL: Structured Query Language
SRS: Security Requirements Specification
SSDLC: Secure Software Development Lifecycle
SSH: Secure Shell
SSL: Secure Socket Layer
SSO: Single Sign-On
SSPR: Self-Service Password Reset
SSRM: Shared Security Responsibility Model
SSVC: Stakeholder-Specific Vulnerability Categorization
STA: Supply Chain Management, Transparency, and Accountability
STAR: Security, Trust & Assurance Registry
STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege

T

TDE: Transparent Data Encryption
TEE: Trusted Execution Environments
TLS: Transport Layer Security
TPM: Trusted Platform Modules
TTC: Time to Contain
TTI: Time to Identify
TVM: Threat and Vulnerability Management

U

UAT: User Acceptance Testing
UEM: Universal Endpoint Management
UPS: Uninterruptible Power Supply
USB: Universal Serial Bus

V

VAPT: Vulnerability Assessments and Penetration Testing
VDP: Vulnerability Disclosure Policy
VM: Virtual Machine
VPC: Virtual Private Cloud
VPN: Virtual Private Network
VRS: Vulnerability Remediation Schedule

W

WAF: Web Application Firewall
WORM: Write-Once-Read-Many

X

XML: Extensible Markup Language
XSS: Cross-Site Scripting

Y

YAML: Human-readable Data Serialization Language

Z

ZAP: Zed Attack Proxy
ZIP: N/A (meaning of “zip” is "move at high speed")

Glossary

Access Control
The selective restriction of access to data or a place. In cloud security, this often refers to the processes that control who can access certain resources and under what conditions.

Application Layer Security
Security measures applied at the OSI Application Layer (Layer 7), which can include protocols and security measures for specific applications.

Asset Categorization
The process of classifying assets, in this context digital assets, based on their sensitivity, value, and criticality to the organization.

Asset Security
Measures and controls used to protect the digital assets of an organization, encompassing both the information contained and the physical devices that store or transmit it.

Attribute-Based Access Control
An access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. These attributes can be user attributes, resource attributes, and environment conditions.

Audit Logging
The process of recording events and changes in a system. In cloud security, this often refers to logging access to cloud resources and changes made to those resources.

Authentication, Authorization, and Accounting
A framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.

Automated Remediation
The process of automatically resolving security vulnerabilities or issues detected in a system or network.

Automated Security Tools
Tools used to automate security processes, such as vulnerability scanning, compliance checks, or network monitoring.

Baseline Requirements
Minimum standards or benchmarks used to measure and compare the security posture of systems or networks.

Cloud Application Security Metrics
Metrics specifically designed to evaluate the security of applications hosted in the cloud. These may include measurements of compliance with security policies, the effectiveness of security controls, and the impact of security incidents.

Cloud Asset Management
The process of managing cloud-based IT assets to ensure they are properly operated, maintained, upgraded, and disposed of when necessary. This includes tracking the assets for financial, contractual, and inventory purposes.

Cloud Controls Matrix
A cybersecurity control framework for cloud computing, covering all key aspects of the cloud technology and enabling cloud organizations efficiently and effectively managing risk in the cloud. The CCM is widely used for implementing and assessing cloud security.

Cloud Environment Coverage
The extent to which security controls and policies are applied across different environments in cloud computing, including public, private, and hybrid clouds.

Cloud-hosted Resources
Any resources that are provided via cloud computing. This can include software, platforms, infrastructure, applications, data storage, and more.

Cloud Service API Calls
Interactions made with a cloud service through its Application Programming Interface (API). These calls allow users to manage and interact with cloud services programmatically.

Cloud Service Customer
An entity that engages with a cloud service provider to use cloud computing services. The CSC may be an individual, company, or organization.

Cloud Service Provider
A company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals.

Cloud Security Group Events
Events or logs generated by security groups in cloud environments. Security groups are a type of virtual firewall that controls inbound and outbound traffic to cloud resources.

Cloud Storage Events
Activities or occurrences within cloud storage environments that are logged or monitored. This can include data access, data modification, and security-related incidents.

Communications Security
Measures and controls designed to protect the confidentiality, integrity, and availability of information in transit. This includes securing methods of communication such as email, instant messaging, and other forms of online communication in cloud environments.

Compliance Checks
Processes or assessments conducted to ensure that cloud services and operations adhere to relevant laws, regulations, guidelines, and standards.

Compliance Events
Specific occurrences or actions within a cloud environment that are relevant to compliance standards. This can include audit findings, security incidents, or changes in data handling that impact compliance status.

Compliance with Laws and Regulations
Adherence to all legal and regulatory requirements applicable to cloud services and operations. This includes data protection laws, industry-specific regulations, and international standards.

Consent and Choice in Data Collection
The practice of obtaining explicit permission from users before collecting their personal data in cloud services, as well as providing them choices about how their data is used.

Container and Orchestration Security
Security measures focused on protecting containerized applications and their orchestration platforms in the cloud. This includes ensuring the security of the containers, the orchestration tools, and the underlying infrastructure.

Continuous Monitoring
The ongoing process of detecting, reporting, and responding to security threats in real-time in cloud environments. It involves the continuous analysis of security logs, performance data, and network traffic.

Continuous Security Assessment
The regular and systematic evaluation of the security posture of cloud services and infrastructure. This involves identifying and assessing vulnerabilities and risks, and implementing measures to mitigate them.

Cost Efficiency in Security
The practice of achieving effective security measures in cloud environments while optimizing costs. This includes balancing the investments in security technologies and personnel against the potential risks and impacts of security incidents.

Customer Trust
The confidence that customers have in a cloud service provider's ability to securely handle their data and provide reliable services. It is built through demonstrated security competence, transparency, and adherence to best practices.

Data Access and Use Policies
Policies that define the rules for how data is accessed and used within a cloud environment. These policies ensure that data is handled securely and in compliance with legal and regulatory requirements.

Data Backup and Recovery
The process of creating copies of data (backup) and restoring them (recovery) in case of data loss, corruption, or disaster. In cloud environments, these processes are often automated and can be scaled based on the needs of the organization.

Data Classification
The process of categorizing data based on its level of sensitivity, confidentiality, and criticality to the organization. This helps in applying appropriate security controls and compliance measures in cloud storage and processing.

Data Encryption
The method of converting plaintext data into a coded form (ciphertext) to prevent unauthorized access. In cloud computing, encryption is used to secure data both at rest (stored data) and in transit (data being transferred).

Data Exfiltration Prevention
Measures taken to protect against unauthorized transfer or retrieval of data from a computer or server. In cloud security, this includes tools and policies to detect and block the unauthorized movement of data out of the cloud environment.

Data Integrity Measures
Security controls implemented to ensure data remains accurate, complete, and reliable throughout its lifecycle. This includes protecting data from unauthorized changes, deletions, or fabrication.

Data Lifecycle Protection
Ensuring the security and privacy of data throughout its entire lifecycle, from creation and storage to use, sharing, archiving, and destruction. This includes applying appropriate controls at each stage of the data lifecycle in cloud environments.

Data Loss Prevention
A set of tools and processes used to ensure that sensitive or critical information is not lost, misused, or accessed by unauthorized users. DLP solutions in the cloud can monitor, detect, and block sensitive data while in use, in motion, and at rest.

Data Minimization
The practice of collecting and processing only the minimum amount of data necessary for a specific purpose. In cloud computing, this principle is important for reducing the risk of data breaches and ensuring compliance with privacy regulations.

Data Privacy Policies
Formal documents outlining how an organization manages the privacy and security of personal data, including how data is collected, processed, shared, protected, and disposed of, particularly in cloud environments.

Data Protection and Privacy
Practices and technologies used to ensure the confidentiality and integrity of personal or sensitive data. This includes measures to protect against unauthorized access, use, disclosure, disruption, modification, or destruction of data.

Data Subject Access Rights
The rights of individuals to access their personal data held by an organization and to request information about how this data is processed, used, and shared.

Data Transfer Protocols
Set of rules that define how data is formatted and transmitted between different systems or entities. In cloud computing, secure data transfer protocols are crucial for maintaining the integrity and confidentiality of data in transit.

Defense-in-Depth
Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

Dynamic Application Security Testing
Security testing that analyzes a running application by exercising application functionality and detecting vulnerabilities based on application behavior and response. Note 1 to entry: Also called “black box testing”.

Encryption
The process of converting data into a coded format to prevent unauthorized access. Encryption is a critical component of cloud security, safeguarding data both at rest and in transit.

Encryption Key Management
The administration of tasks involved with protecting, storing, backing up, and organizing encryption keys. Effective key management is essential in cloud environments to ensure that encrypted data remains secure.

Endpoint Device
An endpoint device is the most remote element at the end of the network. These are computers or simple input devices such as laptops, desktops, tablets,

mobile phones, Internet-of- things devices, servers, virtual environments, etc., operated by humans, remotely managed or fully automated devices collecting information or responding to commands issued from centralized control points.

Environment Segregation
The practice of separating different computing environments to reduce the risk of unauthorized access or data leakage. In cloud computing, this may involve using separate virtual machines or containers for different applications or data sets.

Format-Preserving Encryption
A type of encryption that encrypts data while preserving its original format. This is particularly useful in cloud environments where data needs to remain in a specific format for processing or compliance reasons.

Geotagging
The process of adding geographical identification metadata to various media such as photographs, video, websites, or SMS messages. In cloud security, controlling and managing geotagging is important to protect location privacy and sensitive information related to location.

Human Resource Security Practices
Security measures and protocols related to the management of personnel who have access to sensitive data and information systems. This includes background checks, security training, and access control based on roles and responsibilities.

Identity
A unique digital representation of an entity such as a user, system, application, service, or device, associated with a security principal, often used to ensure that access to resources and data is authorized only to the appropriate users or systems.

Identity and Access Management
Frameworks and technologies used to ensure that the right individuals have access to the right resources at the right times for the right reasons. IAM is a key component in managing user identities and access privileges in cloud environments.

Incident Response
The methodology an organization uses to respond to and manage a cyberattack or data breach. An effective incident response plan in a cloud environment involves preparing for, detecting, containing, eradicating, and recovering from security incidents.

Information Security Program
A set of policies, procedures, guidelines, and associated resources and activities, collectively managed to protect and manage the integrity, confidentiality, and availability of organizational information. In cloud computing, this includes adapting these practices to the cloud's shared responsibility model.

Infrastructure as Code
A process for managing and provisioning computing infrastructure through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools. In cloud environments, IaC helps in automating the setup and maintenance of infrastructure.

Infrastructure Security
Measures and policies put in place to protect the infrastructure (especially IT infrastructure) of an organization from threats and vulnerabilities. In cloud computing, this includes securing the underlying hardware and software that supports the cloud services.

Intrusion Detection/Prevention Systems
Tools and technologies used to detect and prevent unauthorized access and attacks on networks and systems. In cloud environments, IDS/IPS can monitor and analyze both inbound and outbound network traffic to identify potential threats.

Key Performance Indicators
Measurable values that demonstrate how effectively a company is achieving key business objectives. In cloud security, KPIs might include metrics related to incident response times, system uptime, and compliance with security policies.

Logical Separation of Data
A method of segregating data within a shared storage environment so that each tenant's data is inaccessible to other tenants. This is crucial in multi-tenant cloud architectures to ensure data privacy and security.

Logging and Monitoring
The processes of capturing, storing, and analyzing log files to detect and investigate security incidents and maintain operational functionality in cloud environments. Effective logging and monitoring are key for identifying and responding to security threats.

Monitoring and Auditing
The continuous processes of examining and reviewing cloud computing services and activities to ensure compliance with policies and standards, and to detect anomalies or malicious activities. This involves both real-time monitoring and regular audits.

Mutual TLS
A method in Transport Layer Security (TLS) where both the client and the server authenticate each other to ensure a higher level of security. This is particularly important in cloud environments for secure communications between services.

Network Architecture
The design of a computer network; it's a framework that describes the structure and behavior of network elements (like routers and switches) and their interconnections. In cloud computing, network architecture is critical for ensuring efficient and secure data flow.

Network Defense
The practices and technologies used to protect a network from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure. This includes a range of measures such as firewalls, intrusion detection systems, and encryption in cloud networks.

Network Layer Security
Security measures implemented at the network layer of the OSI model to protect data as it travels over the internet or other networks. In cloud environments, this involves securing the communications between cloud services and users.

Network Traffic Analysis
The process of intercepting, recording, and analyzing network traffic patterns to detect and respond to security threats. In cloud computing, NTA tools are used to monitor and protect cloud-based assets.

Penetration Testing
The practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit. In the context of cloud computing, penetration testing is used to assess the security of cloud infrastructures and services.

Policy Approval Process
The steps and procedures followed to develop, review, approve, and implement policies, especially those related to security and privacy. In cloud environments, this includes policies for data protection, access control, and incident response.

Privacy Statement
A document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. In cloud computing, a privacy statement is crucial for detailing how user data is handled and protected.

Privileged Access Management
A set of practices and technologies for granting and controlling elevated access (or privileges) to an organization's IT environment. In cloud computing, PAM is important for managing access to cloud resources and services.

RACI Matrix
A tool that identifies the roles and responsibilities of individuals in completing tasks or deliverables for a project or process. In the context of cloud security, it helps clarify who is Responsible, Accountable, Consulted, and Informed for each task.

Risk Assessments
The process of identifying, analyzing, and evaluating risks. In cloud computing, risk assessments are crucial for understanding the potential security threats to cloud services and data, and for implementing appropriate mitigation strategies.

Risk Mitigation Effectiveness
The measurement of how successful a strategy or action is in reducing or controlling risk. In cloud computing, this involves assessing the effectiveness of security measures and controls in reducing the potential impact of identified risks.

Role-Based Access Control
A method of regulating access to computer or network resources based on the roles of individual users within an organization. In cloud environments, RBAC helps in managing user access to resources based on their role and responsibilities.

Secure APIs
Application Programming Interfaces that are designed with security as a primary consideration. In cloud computing, secure APIs ensure that interactions between different services and applications are conducted safely and securely.

Secure Protocols
Protocols used to secure communications over a computer network. In cloud environments, Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure (HTTPS) are commonly used to encrypt data in transit.

Security and Risk Management
The process of identifying, assessing, and implementing strategies to manage and mitigate risks to an organization's information assets. In the context of cloud computing, SRM involves adapting these processes to the cloud's shared responsibility model.

Security Baseline Review
The process of comparing the current security state of an organization's IT infrastructure to a set of standard baseline security criteria. In cloud environments, this includes reviewing configurations, access controls, and other security measures against established benchmarks.

Security Control Implementation
The specific technical and procedural measures put in place to safeguard an organization's information assets. In cloud computing, this includes a wide range of security mechanisms such as encryption, access control, and network security.

Security Domain Analysis
The process of examining and evaluating the various domains (such as network, application, user, etc.) within an organization's IT environment from a security perspective. In cloud computing, this includes assessing the security of cloud services and infrastructure.

Security Group
Are sets of IP filter rules that are applied to all project instances, which define networking access to the instance. Cloud security groups can be effectively used with a SDP, by being set to ensure that inbound network access to cloud-based resources is only permitted from an SDP gateway. By doing so, the SDP policy will act as the access control enforcement point, rather than the cloud security group. The cloud security group can also be used to require that outbound traffic be directed through the SDP gateway, if supported by the SDP implementation.

Security Information and Event Management
This technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).

Security Incident Management
The process of identifying, managing, recording, and analyzing security threats or incidents in real-time. In cloud environments, this involves preparing for and responding to security incidents that affect cloud-based resources.

Security Monitoring Capabilities
The tools and processes used to continuously monitor and detect security threats and vulnerabilities in an IT environment. In cloud computing, this includes the monitoring of cloud infrastructure and services for unusual or unauthorized activities.

Security Posture Measurement
The process of assessing and quantifying the overall security status of an IT environment. In cloud computing, this involves evaluating the security measures and policies in place for cloud services and infrastructure.

Security Requirements Specification
A detailed description of the security needs and expectations for an IT system or application. In the context of cloud computing, the SRS outlines the

security requirements for cloud services and platforms.

Security Software Development Life Cycle
A process that incorporates security considerations and practices into each phase of the software development life cycle. In cloud environments, SSDLC ensures that cloud applications and services are designed and built with security in mind from the outset.

Secure Shell
A protocol for secure remote login and other secure network services over an insecure network, which typically runs on top of TCP/IP. The protocol can be used as a basis for a number of secure network services. It provides strong encryption, server authentication, and integrity protection. It may also provide compression.

Security Violation Detection
The process of identifying activities or actions that breach security policies or standards. In cloud computing, this includes detecting unauthorized access, data breaches, and other security threats.

Sensitive data
Sensitive data is any information that must be protected due to its potential for harm if disclosed to unauthorized parties. This can include specific categories of personal data (e.g., financial, health records) and other types of sensitive data (e.g., corporate or trade secrets) that in the case of loss, misuse, or modification, could lead to potential financial loss, reputational damage, legal issues, or loss of competitive advantage.

Service Level Agreements
Formal agreements between service providers and their clients that define the level of service expected. In cloud computing, SLAs typically cover aspects like service availability, performance, and security.

Service Models
Different categories of cloud computing services: Infrastructure as a Service (IaaS) provides virtualized computing resources over the internet, Platform as a Service (PaaS) offers hardware and software tools, and Software as a Service (SaaS) delivers software applications over the internet.

Tagging Strategy
The use of tags (metadata) for resource identification and management in cloud environments. This helps in categorizing and organizing cloud resources for easier monitoring, management, and billing.

Third-party Application Security Assessment
The evaluation of security measures and vulnerabilities in applications developed by third parties. In cloud computing, this involves assessing the security of third-party apps before integrating them into the cloud environment.

Threat Intelligence
Information used to understand and identify potential security threats. In cloud security, threat intelligence involves collecting and analyzing data about emerging or existing threats to cloud-based systems.

Transparent Data Encryption
A method of encrypting data at the storage level. In cloud environments, TDE is used to encrypt data at rest, ensuring that stored data is secure even if the storage medium is compromised.

Vendor Risk Management
The process of assessing and managing the risks associated with third-party vendors, especially those who provide cloud services or have access to an organization's cloud-based systems. It involves evaluating the security and compliance practices of the vendors.

Virtual Private Networks
A technology that creates a safe and encrypted connection over a less secure network, such as the internet. VPNs are often used in cloud computing to establish secure connections between cloud services and users or between different cloud services.

Virtualization Security
The practice of securing virtual machines and other virtualized components in a cloud environment. This includes protecting the virtualization infrastructure and ensuring the security of virtual machines against various threats.

Vulnerability Identification
The process of discovering security weaknesses in systems, software, or networks. In cloud environments,

this involves identifying vulnerabilities in cloud services and infrastructure that could be exploited by attackers.

Vulnerability Management
The continuous process of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities. In the context of cloud computing, it's vital for maintaining the security and integrity of cloud services.

Web Application Firewalls
A specific type of firewall that filters, monitors, and blocks HTTP traffic to and from a web application to protect against malicious attacks. In cloud environments, WAFs are used to protect cloud-based web applications.

Workload Segmentation
The practice of dividing and isolating workloads (applications, services, processes) within a cloud environment to enhance security. This helps in reducing the attack surface and containing potential breaches within isolated segment

Note: For further reference, please refer to CSA's glossary at:
https://cloudsecurityalliance.org/cloud-security-glossary/ "