クラウドコンピューティングのための
セキュリティガイダンス V5
―要約版―

一般社団法人 日本クラウドセキュリティアライアンス（CSA ジャパン）
クラウドセキュリティワーキンググループ

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. 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。

本書執筆者

釜山 公徳
番 義樹
山田 俊宏
※五十音順

変更履歴

日付	版数	変更内容
2024 年 11 月 3 日	1.0	初版発行
2025 年 4 月 14 日	1.1	全般的な改訂

本書について

先般、CSA 本部が 2024 年 7 月公開した「Security Guidance For Critical Areas of Focus in Cloud Computing v5」の日本語訳「クラウドコンピューティングのためのセキュリティガイダンス V5」(以下、ガイダンス)が 2024 年 10 月に公開されました。このガイダンスは 12 のドメインで構成され、大変充実しております。広く遍く利用していただくために、要約版を作成するに至りました。なお、本書、並びにガイダンスは無料で公開しております。

生成 AI の利用による免責

本書は要約作業に Google DeepMind Technologies Limited の Gemini Pro 1.5 を使用しております。ハルシネーションやその他生成 AI による問題が無い様に注意しておりますが、修正漏れが発生する可能性がございますので、予めご容赦願います。

CSA とセキュリティガイダンスのご紹介

Cloud Security Alliance Global Headquarter が掲げるミッションステートメント

クラウド・コンピューティングのセキュリティを保証するベストプラクティスの使用を推進し、クラウド・コンピューティングを使用するにあたってあらゆるコンピューティング環境を安全にするための教育を提供する。

クラウドセキュリティワーキンググループ(CS-WG)

クラウドセキュリティの各分野に対して、推奨事項、技術的対策についてフォーカスし、クラウドセキュリティとして、技術的なベースラインを明確にすることで、より安全なクラウド利用に向けてのガイドラインを作成することを目的としております。

クラウドコンピューティングのためのセキュリティガイダンス V5

クラウド、セキュリティ、サポート技術の進歩を取り入れ、実際のクラウドセキュリティの実践を反映し、最新のクラウドセキュリティアライアンスの研究プロジェクトを統合し、関連技術のガイダンスを提供しています。特に、アプリケーションセキュリティにおける、IaC、DevOps、サードパーティライブラリ、新しいクラウドセキュリティ技術、クラウドワークロードのセキュリティとして、コンテナ、サーバーレス機能、AI などのセキュア化をカバーしています。また、CSPM、SSPM、CNAPP、IaC、SASE、SOAR など、様々なセキュリティソリューションをどのように有効に活用していくかについても解説しています。

ガイダンスは次の 12 ドメインで構成されています。

- ドメイン 1:クラウドコンピューティングの概念とアーキテクチャ
- ドメイン 2:クラウドガバナンスと戦略
- ドメイン 3:リスク、監査、コンプライアンス
- ドメイン 4:組織管理
- ドメイン 5:アイデンティティとアクセスの管理
- ドメイン 6:セキュリティモニタリング
- ドメイン 7:インフラストラクチャとネットワーク
- ドメイン 8:クラウドワークロードセキュリティ
- ドメイン 9:データセキュリティ

- ドメイン 10:アプリケーションセキュリティ
- ドメイン 11:インシデントレスポンスとレジリエンス
- ドメイン 12:関連技術と戦略

ドメイン 1:クラウドコンピューティングの概念とアーキテクチャ

クラウドコンピューティングの定義

クラウドコンピューティングとは、インターネット経由で必要な時に必要なだけコンピューティングリソース（サーバー、ストレージ、ネットワーク等）を利用できるサービスです。クラウド環境を実現する主要な概念は、抽象化とオーケストレーションです。クラウドはマルチテナントを前提とします。

CSP（クラウドサービスプロバイダー）はさまざまな CSC（クラウドサービス利用者）にリソースを分割することができます。リソースの分離によって、CSC がクラウド上に持つデータの機密性と完全性が保たれます。

クラウドコンピューティングモデル

クラウドコンピューティングの NIST モデルでは、クラウドを 5 つの基本特性、3 つのサービスモデル、4 つの配備モデルによって説明しています。

5 つの基本特性

1. **リソースプーリング**：複数のユーザーに共有リソースを動的に割り当てます。
2. **幅広いネットワークアクセス**：ネットワーク経由であらゆるデバイスからアクセスできます。
3. **迅速な弾力性**：リソースを迅速かつ自動的に増減できます。
4. **測定可能なサービス**：クラウドの使用状況を測定し、透明性と従量課金を実現します。
5. **オンデマンドセルフサービス**：必要なリソースをすぐに利用できます。

3 つのサービスモデル

1. **SaaS**： ソフトウェアをインターネット経由で利用するサービス
2. **PaaS**： アプリケーション開発や実行のプラットフォームを提供するサービス
3. **IaaS**： サーバーやストレージなどのインフラストラクチャを提供するサービス

4 つの配備モデル

1. **パブリッククラウド**： 誰でも利用可能なクラウド
2. **プライベートクラウド**： 特定の組織専用のクラウド
3. **コミュニティクラウド**： 複数の組織で共有するクラウド
4. **ハイブリッドクラウド**： 複数のパブリッククラウドやプライベートクラウドを組み合わせたクラウド

その他の配備モデル

1. **マルチクラウド**： 複数のクラウドサービスを利用し、単一のクラウドプロバイダーへの依存を減らす
2. **ハイブリッドマルチクラウド**： パブリッククラウドとプライベートリソースの組み合わせ

参照モデルとアーキテクチャモデル

クラウドサービスの参照モデルとアーキテクチャモデルは、クラウド技術の進化とともに変化し続けています。NIST SP 800-145 や ISO/IEC 22123 などの既存のモデルは、クラウドコンピューティングを理解するための基礎を提供しています。

前述のとおり、クラウドサービスは、IaaS、PaaS、SaaS の 3 つのサービスモデルに分類されますが、これらのサービスモデルは、互いに重なり合う場合があり、明確な区別が難しいケースもあります。SPI スタックは、SaaS が PaaS 上に、PaaS が IaaS 上に構築されるという考え方ですが、実際のクラウドサービスは、このスタックに必ずしも従うわけではありません。クラウドセキュリティの専門家は、これらのモデルを理解し、最新の情報を入手しておく必要があります。

クラウドセキュリティのスコープ、責任、およびモデルの理解

クラウドのセキュリティは、CSP と CSC の共同責任です。セキュリティ責任共有モデル（Shared Security Responsibility Model(SSPM)）とは、 CSP と CSC のセキュリティ責任分担を明確にするモデルのことです。

クラウドにおけるセキュリティ責任を明確に割り当てるために、次の事項を推奨しております。

- CSP: セキュリティを文書化し、適切に設計・実装する責任があります。
- CSC: セキュリティ責任者を明確化し、コンプライアンス基準に準拠する責任があります。

CSA では、要件を満たすために、役立つツールを提供しております。

- CAIQ: CSP がセキュリティを文書化するための標準テンプレートです。
- CCM: クラウドのセキュリティをリスト化し、責任分担を明確化します。

ドメイン 2:クラウドガバナンスと戦略

クラウドガバナンス

クラウドコンピューティングでは、マルチテナンシー、責任共有、機密データの再配置など、従来の IT 環境とは異なる課題があるため、効果的なガバナンスが重要です。適切なガバナンスがないと、セキュリティリスク、財務リスク、運用リスクが増大し、クラウド導入のメリットを十分に享受できません。

組織がクラウド環境を管理する際には次の考慮事項が必要です。

- **コントロールと説明責任**：クラウド導入により、組織はガバナンス、責任分担、評価方法を見直す必要があります。
- **法令等へのコンプライアンス**： クラウド環境における法規制要件やデータ管理、プライバシー保護を遵守する必要があります。
- **可視性と透明性**：一部のクラウドサービスでは、可視性と透明性を確保することが困難です。
- **カスタマイズと標準化**：CSP のサービスやポリシーは標準化されており、CSC の個別要件への対応は難しい場合があります。
- **ガバナンスの複雑さ**：クラウドサービスは複雑なため、ガバナンスが難しく、CSP と CSC の責任範囲も曖昧になりがちです。前章で登場した配備モデルそれぞれについても固有のガバナンスの課題と責任があります。
- **CSP と CSC のダイナミクス**：CSP は変化しやすいため、ガバナンスモデルはそれに対応できる必要があります。クラウドサービスの利用には、CSC は新たなスキル習得が必要です。

効果的なクラウドガバナンス

効果的なクラウドガバナンスには、クラウドサービスの安全かつ効率的な利用を確保するためのフレームワークとポリシーが必要です。

クラウドガバナンスの実装モデルとして以下があります。

- **Cloud Center of Excellence（CCoE）**： クラウド導入と利用に関する専門チームを設置し、組織全体へのガイダンス、ベストプラクティス、サポートを提供する。
- **Cloud Advisory Council（CAC）**： CAC は、組織のクラウド戦略を率いる、様々な部門のリーダーで構成されるグループ。
- **セキュリティチャンピオン**： 各部門にセキュリティの専門家を配置し、セキュリティの推進と啓蒙活動を行う。

ガバナンスの階層

クラウドガバナンスには、NIST CSF、CCM などのフレームワーク、ポリシー、コントロール目標、そして具体的な実装方法であるコントロール仕様からなる階層構造があります。

フレームワークはセキュリティの全体像を、ポリシーは組織のセキュリティ要件を、コントロール目標はセキュリティの目的を、コントロール仕様は具体的な実装方法をそれぞれ規定します。

さらに、リスク許容度やデータの重要度に応じて適切なセキュリティレベルを設定する必要があり、法規制や業界標準、契約内容も考慮しなければなりません。

これらの要素を体系的に管理するために、CSA STAR のようなクラウドセキュリティ認証制度を活用することも有効です。

この階層構造とセキュリティレベル設定、各種法規制遵守により、セキュリティが体系的に整理され、効果的なガバナンスが実現します。

主要戦略とコンセプト

DevOps は、開発と運用の連携を強化し、迅速なソフトウェア提供を可能にする手法です。DevSecOps は、DevOps にセキュリティを組み込み、安全なアプリケーション開発を実現します。ゼロトラストは、境界の内外を問わず、すべてのユーザーとデバイスを信頼せず検証するセキュリティモデルです。AI と機械学習は、クラウドセキュリティの自動化と効率化に役立ちます。これらの戦略と概念は、クラウドガバナンスとセキュリティを強化するための重要な要素です。

ドメイン 3:リスク、監査、コンプライアンス

クラウドのリスク管理

クラウドのリスク管理では、まずクラウドサービスのリスクを特定し、そのリスクプロファイルを確立することが重要です。リスクプロファイルは、組織のビジネス戦略、情報セキュリティポリシー、クラウド移行計画などを考慮して作成します。

次に、リスクアセスメントを実施し、各リスクの可能性と影響を評価します。ここでは、脅威や脆弱性の分析、影響範囲の特定などが行われます。

最後に、リスク対応計画を策定し、リスクを軽減、移転、回避、または受容するための対策を講じます。リスク管理は継続的なプロセスであり、定期的な見直しと改善が必要です。

コンプライアンスと監査

コンプライアンスと監査は、データの完全性、可用性、機密性を保護するために重要です。

クラウド環境では、コンプライアンス継承と呼ばれる概念が適用されます。これは、CSP のコンプライアンス認証を、CSC が活用できるようにするものです。コンプライアンス継承により、CSC は CSP のコンプライアンス認証を利用することで、自社のコンプライアンス責任を軽減できます。

ただし、コンプライアンス継承は、CSC のコンプライアンス責任を完全に免除するものではありません。CSC は、CSP のサービスだけでなく、自社が構築したアプリケーションやサービスについても、コンプライアンス責任を負います。

コンプライアンス継承を効果的に活用するには、CSP と CSC 間の責任分担を明確にし、協力してコンプライアンスに取り組むことが重要です。

ガバナンス、リスク、コンプライアンスツールと技術

ガバナンス、リスク、コンプライアンス（GRC）は、クラウド環境のセキュリティを維持するための重要な要素です。GRC ツールと技術は、ポリシーの施行、コンプライアンスの監視、クラウドセキュリティの管理を支援します。

非技術的なツールには、責任共有モデル、契約、リスクレジスタ、クラウドセキュリティ成熟度モデルなどがあります。これらのツールは、リスク管理、責任の明確化、コンプライアンス遵守に必要なフレームワークを提供します。

技術的なツールには、CSP ポリシー、予防/発見コントロール、自動化などがあります。これらのツールは、セキュリティポリシーの施行、コンプライアンスのリアルタイム監視、人的ミスの削減に役立ちます。

GRC ツールと技術を効果的に組み合わせることで、組織はクラウド環境のセキュリティリスクを軽減し、コンプライアンスを維持できます。

ドメイン 4:組織管理

組織階層モデル

CSP には、Amazon Web Services(AWS)、Microsoft Azure(Azure)、Google Cloud など、さまざまなものがあります。それぞれが独自の用語や構造を使用しており、クラウドのリソースを階層的に管理しています。

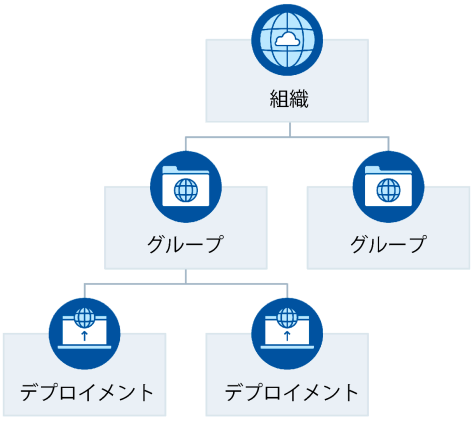

図: クラウドリソース管理の階層構造

クラウドサービスプロバイダー	組織	グループ	デプロイメント
AWS	組織	組織単位	アカウント
Google Cloud	組織	フォルダ	プロジェクト
Microsoft Azure	テナント	リソースグループ	サブスクリプション

組織レベルのセキュリティの管理

組織レベルのセキュリティ管理では、クラウド環境の特性を理解し、適切な対策を講じる必要があります。以下のような要素を活用し組み合わせることで、組織はクラウド環境のセキュリティを効果的に管理できます。

- ID プロバイダー：プロバイダーの認証とアクセス制御を一元的に管理します。
- 組織ポリシー：クラウドサービスの利用を制限するルールを定義します。
- 共通する組織共有サービス：セキュリティを効率化するためのツールやサービスを提供します。

ハイブリッドとマルチクラウドのデプロイメントに関する考察

ハイブリッドクラウドとマルチクラウド、SaaS それぞれ、セキュリティが必要です。

- **ハイブリッドクラウド**： オンプレミスとクラウド間の安全な接続が重要です。VPN や専用回線を使用し、それぞれの環境に適したセキュリティを組み合わせる必要があります。
- **マルチクラウド**： 複数のクラウドサービスを利用する際は、セキュリティの一貫性が課題となります。各クラウドサービスのセキュリティ機能を理解し、共通のセキュリティポリシーを適用することが重要です。
- **SaaS**： 利用者側のセキュリティ責任は軽減されますが、データの機密性に応じてアクセス制御を設定するなど、適切な対策が必要です。

ドメイン 5:アイデンティティとアクセスの管理

クラウドにおける IAM（アイデンティティとアクセス管理）の違い

クラウドにおける IAM は従来のオンプレミス環境とは異なる課題と特性を持っています。

1. 複数の組織にまたがる
   CSP とクラウドサービス利用者 CSC 間、または複数の CSP 間で IAM を連携させる必要があり、アイデンティティフェデレーションが重要となります。
2. CSP ごとに IAM システムが異なる
   CSC は、多様な CSP の IAM システムを理解し、管理する必要があります。
3. マネジメントインターフェースがインターネットに公開されている
   これにより、IAM の重要性が増すと同時に、不正アクセスのリスクも高まります。

これらの違いを踏まえ、クラウド環境では、適切な IAM の設計と運用が不可欠です。

フェデレーション

ID フェデレーションとは、異なる組織間でユーザー認証を共有する仕組みです。CSC は、自社の ID 管理システムと CSP のシステムを連携させることで、シングルサインオン（Single Sign-On (SSO)）を実現できます。主な標準規格として、SAML、OAuth、OpenID Connect などがあります。

フェデレーションには、ハブ＆スポーク型とフリーフォーム型の 2 つのアーキテクチャモデルがあります。適切なモデルを選択することで、クラウド環境におけるアイデンティティ管理を効率化し、セキュリティを向上させることができます。

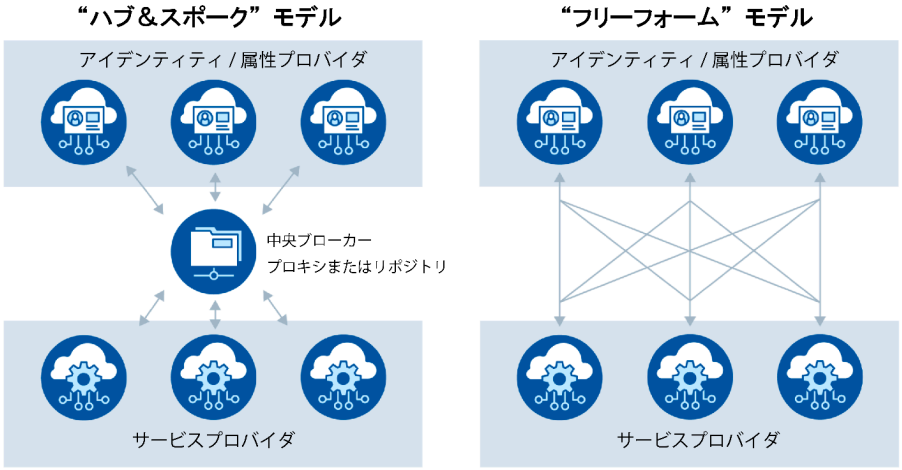

図 26: ID フェデレーション管理のアーキテクチャモデル:ハブ&スポークとフリーフォーム

強固な認証と認可

クラウドのセキュリティ強化には、強固な認証と認可が必須です。

認証では、多要素認証(Multi-Factor Authentication (MFA))が重要です。ハードトークン、ソフトトークン、生体認証など、さまざまな MFA 方式があり、それぞれに利点とリスクがあります。

認可では、ロールベースアクセス制御（RBAC）やポリシーベースアクセス制御（PBAC）などのモデルがあります。CSP は認可ポリシーを実施し、CSC はポリシーを定義・管理します。属性ベースアクセス制御（ABAC）のような高度なモデルでは、状況に応じたアクセス制御が可能になります。

パブリッククラウドの IAM ポリシータイプ

パブリッククラウドの IAM ポリシーには、デバイスベース、アイデンティティベース、リソースベース、組織ベースの 4 つの種類があります。これらのポリシーを組み合わせることで、多層的なアクセス制御を実現できます。

- デバイスベースポリシー：デバイスの登録状態やコンプライアンスに基づいてアクセスを制御します。
- アイデンティティベースポリシー：ユーザーやグループに紐づけて権限を付与します。
- リソースベースポリシー：特定のリソースへのアクセスを制御するポリシーです。
- 組織ベースポリシー：組織全体のクラウド環境に適用されるポリシーです。

最小権限と自動化

クラウド環境では、最小権限の原則に基づき、必要なアクセス権限のみを付与することが重要です。しかし、権限管理は複雑になりがちで、過剰な権限付与や権限不足のリスクがあります。

そこで、自動化技術が有効です。使用状況の追跡、リスクスコアリング、JIT（Just-In-Time）権限付与、継続的な評価など、様々な自動化手法があります。例えば、ユーザーの行動分析に基づいて異常なアクセスを検知したり、必要最低限の権限を必要な時にのみ付与したりすることができます。

これらの技術を活用することで、セキュリティを向上させながら、業務効率も高めることができます。

ドメイン 6:セキュリティモニタリング

クラウドモニタリング

クラウドのセキュリティ監視は、従来の環境と比べて複雑で、変化のスピードが速く、リソースが分散しているといった特徴があります。CSP と CSC 間で責任を分担するセキュリティ責任共有モデルを採用していることも、監視を複雑にする要因となります。そのため、クラウド環境では、迅速な対応と全体を俯瞰できる監視体制が必要です。

一方で、API を通じた構成確認などの監視手法も活用できます。例えば、CSP が提供している監視サービス（例 AWS CloudWatch、Azure Monitor）や、サードパーティの監視ツールが該当します。

クラウドテレメトリ・ソース

クラウドテレメトリは、クラウド環境で何が起こっているかを把握するための重要な情報源です。具体的には、以下のようなソースから情報を収集します。

- **マネジメントプレーンのログ**：クラウド環境へのアクセスや操作履歴の記録
- **サービスログとリソースログ**：API アクセスやネットワークトラフィック、リソースの使用状況の記録
- **クラウドツール**：CSPM、CASB、CNAPP などがあり、セキュリティの脅威や設定ミスなどを検知するために利用されるツール。

これらの情報源から得られたデータは、セキュリティツールや管理者によって分析され、クラウド環境のセキュリティ維持に役立てられます。

収集アーキテクチャ

クラウドのセキュリティ監視では、様々な場所やプロバイダーに分散したリソースからログデータを効率的に収集することが重要です。クラウド環境には、マネジメントプレーン、クラウドイベント、セキュリティツールフィードなど、従来の環境にはないログソースが存在し、ログの種類によって生成速度も異なります。

ログの保存先としては、CSP のストレージ、オンプレミス、サードパーティの SIEM など、様々な選択肢があり、コストや性能を考慮して最適なものを選択する必要があります。

収集アーキテクチャには、「カスケード型」の他に、「エージェント型」や「プッシュ型」などがあり、それぞれにメリットとデメリットがあります。

- **カスケード型**：複数のアカウントや環境からログを集約するのに適しています。
- **エージェント型**：各リソースにエージェントをインストールしてログを収集す

る方法で、リアルタイム性に優れています。

- **プッシュ型**：各リソースからログを中央のサーバーに送信する方法で、シンプルで導入しやすいというメリットがあります。

ログの保存期間や保持ポリシーについても、運用ニーズや法規制などを考慮して適切に決定する必要があります。

検知とセキュリティ分析

クラウドのセキュリティ監視では、ログ、イベント、構成検出の 3 つの要素が重要です。

- **ログ**：詳細な情報を記録しており、時間経過に伴うパターンの分析に役立ちますが、分析に時間がかかるというデメリットがあります。
- **イベント**：リアルタイム性が高く、迅速な対応に役立ちます。
- **構成検出**：クラウド環境の設定ミスや脆弱性を検知するのに役立ちます。

これらの要素を組み合わせることで、効果的なセキュリティ監視システムを構築できます。

セキュリティモニタリングのための生成 AI

生成 AI は、クラウドのセキュリティモニタリングにおいて、ログデータ分析の自動化、脅威検知の精度向上、模擬攻撃シナリオの作成など、様々な活用が期待されています。具体的には、ログデータから異常な行動を検知したり、脆弱性を発見したり、攻撃経路を予測したりすることが可能になります。しかし、プライバシー保護や敵対的 AI への対策など、課題も存在します。生成 AI は、クラウドセキュリティの分野で急速に進化しており、今後の発展が期待されます。

ドメイン 7:インフラストラクチャとネットワーキング

クラウドインフラストラクチャのセキュリティ

クラウドインフラストラクチャのセキュリティ確保は CSP、CSC 双方にとって重要です。

- **CSP**：物理的な施設、ハードウェア、仮想化レイヤー、管理インターフェースのセキュリティを担う。
- **CSC**：クラウドサービスの設計・構築、セキュリティの実装、適切な構成などに責任を持つ。

「Well-Architected Framework」のようなフレームワークを参考に、セキュリティ、運用性、信頼性、パフォーマンス、コスト、持続可能性を考慮した設計が重要です。また、開発ライフサイクルの早い段階からセキュリティを組み込む「シフトレフト」という考え方も重要です。

クラウドネットワークの基礎

クラウドネットワークは、Software-Defined Networking（SDN）を基盤としています。SDN は、ネットワークの構成と管理をソフトウェアで制御することで、柔軟性と俊敏性を向上させます。セキュリティ面でも、デフォルト拒否ポリシー、ポリシーベースの管理、詳細なセグメンテーションといった利点があります。さらに、Minimum Viable Network (MVN) の概念により、必要最低限のネットワークコンポーネントと接続のみを許可することで、セキュリティを強化できます。

SDN には仮想ネットワーク、サブネット、ルートテーブル、セキュリティグループ、ネットワークアクセス制御リスト (NACL) など様々なコンポーネントがあります。これらのコンポーネントを理解し、適切に構成することで、セキュアなクラウドネットワークを構築できます。

クラウド接続性

クラウド接続では、リソースへの接続、仮想ネットワーク間の接続、データセンターやプロバイダー間の接続という 3 つの種類があります。

- **リソースへの接続**：インターネット経由の接続、専用線、VPN、CSP 接続サービスなど、様々な方法があります。
- **仮想ネットワーク間の接続**：ピアリング、トランジット、メッシュ、サービスエンドポイントなどがあり、セキュリティやパフォーマンスを考慮して最適な方法を選択する必要があります。
- **データセンターやプロバイダー間の接続**：専用線、VPN、ハイブリッドメッシ

ュなどがあり、それぞれにメリットとデメリットがあります。

接続方法によってセキュリティレベルやコスト、パフォーマンスなどが異なるため、要件に合わせて適切な方法を選択することが重要です。

ゼロトラストとセキュアアクセスサービスエッジ

ゼロトラストは、決して信頼を仮定せず、常に検証を行うというセキュリティ戦略です。ネットワークにアクセスするユーザーやデバイスは、継続的に認証と認可を受ける必要があります。

クラウド環境では、Software-Defined Perimeter (SDP) やゼロトラストネットワークアクセス (ZTNA) が、ゼロトラストを実現するための技術として注目されています。

- SDP は、許可されたサブジェクトにリソースへのアクセスを許可する、セキュアなネットワーク境界を構築します。
- ZTNA は、ユーザーの ID、デバイス、コンテキストに基づいて、アプリケーションへのきめ細かいアクセス制御を提供します。

セキュアアクセスサービスエッジ(Secure Access Service Edge (SASE)) は、これらのセキュリティ機能を統合的に提供するクラウドサービスです。SD-WAN、SWG、CASB、ZTNA、FWaaS などの機能を組み合わせることで、包括的なセキュリティを実現します。

SASE は、クラウドファースト、モバイルファーストの現代において、ゼロトラストセキュリティモデルを実現する上で重要な役割を果たします。ユーザーの場所やデバイスに依存せず、一貫したセキュリティポリシーを適用できるため、クラウド環境のセキュリティ強化に大きく貢献します。

ドメイン 8:クラウドワークロードセキュリティ

クラウドワークロードセキュリティ入門

クラウドワークロードのセキュリティ確保は、データ保護だけでなく、コンプライアンス遵守と事業継続も重要です。クラウド環境は動的で拡張性が高く、多様なワークロードが存在するため、従来とは異なるセキュリティが必要です。仮想マシン、コンテナー、PaaS、サーバーレス、AI など、様々な種類のワークロードがあり、それぞれに適したセキュリティを講じる必要があります。

クラウドワークロードでは、データの完全性、機密性、可用性を維持することが重要です。これらの要素をバランスよく維持することが、クラウドワークロードのセキュリティ確保に不可欠です。

- **完全性**： データが改ざんされていないこと。
- **機密性**： 許可された人だけがデータにアクセスできること。
- **可用性**： 必要なときにデータを利用できること。

仮想マシン

仮想マシン（VM）は、クラウドサービスで利用される主要なワークロードで活用されます。

VM は、分離された環境を提供し、セキュリティ境界を適用することで、ワークロード間のセキュリティを確保します。VM イメージの管理、パッチ適用、変更管理、攻撃対象領域の極小化、ライフサイクル管理、ネットワークセキュリティなどが VM のセキュリティ施策として重要です。セキュアなベースイメージの使用、脆弱性スキャン、不要なコンポーネントの削除、構成管理、監視とロギングなどが対策として挙げられます。

コンテナーのセキュア化

コンテナーのセキュリティは、イメージ作成からデプロイ、実行まで、ライフサイクル全体で考慮する必要があります。セキュアなベースイメージを使用し、イメージリポジトリを適切に管理することが重要です。Kubernetes などのオーケストレーションツールを利用する場合は、設定の確認とセキュリティポリシーの適用が必要です。また、ランタイム保護として、コンテナーの動作を監視し、異常を検知する仕組みも必要です。

PaaS セキュリティ

PaaS のセキュリティは、共通のセキュリティに加え、各サービス特有の対策も必要です。共通のセキュリティとしては、セキュリティ監査、ログ監視、最小権限の原則、多要素認証、アクセス権限の見直しなどが挙げられます。暗号化、アクセス制御、ネットワークセグメンテーションなども重要です。

各サービス特有の対策としては、CDN、通知サービス、メッセージキューなどを講じる必要があります。

サーバーレスコンピューティングまたは Function as a Service（FaaS）のセキュア化

サーバーレスコンピューティング（サーバーレス、または FaaS という）は、サーバー管理を CSP に任せることで開発者の負担を軽減するサービスですが、特有のセキュリティ課題も存在します。

主な課題として、外部サービスや API への依存、脆弱性が含まれる依存関係、設定ミス、過剰な権限付与、インターネットへの直接アクセスなどが挙げられます。さらに、サーバーレスはステートレス（状態を保持しない）で、イベント駆動型であり、CSP への依存度が高いという特徴があります。

これらの特徴を踏まえ、開発者はコードのセキュリティ、アクセス制御、機密データ保護などを適切に行う必要があります。具体的には、最小権限の原則に基づいたアクセス制御、緻密な権限設定、コンテキストを考慮した認可、環境変数、シークレット管理、IAM ポリシーの定期的な見直しなどが重要となります。

AI ワークロード

AI ワークロードは大量のデータと計算を必要とし、クラウドの活用が不可欠です。AI システムの脅威には、データポイズニング、プライバシー侵害、モデル盗難、敵対的攻撃などがあります。対策としては、データの暗号化、モデルのハードニング、インフラストラクチャのセキュリティ強化、サプライチェーンリスク管理などが重要です。

- **データポイズニング**： AI モデルの学習データに誤った情報を混入させる攻撃。
- **モデル盗難**： AI モデルを不正にコピーすること。
- **敵対的攻撃**： AI モデルの弱点を突いて誤動作させる攻撃。

ドメイン 9:データセキュリティ

データ分類とストレージタイプ

データの種類、機密性、および重要性に基づいてデータを分類することで、組織はデータタイプごとに 適切なセキュリティ方法を実装できます。データは、その種類や重要度に応じて適切に分類し、保管する必要があります。

- **データ分類**： データの種類、機密性、重要度に基づいて分類します。
- **データの状態**： 保存中、移動中、使用中など、データの状態に応じて適切なセキュリティを講じます。
- **クラウドストレージの種類**： オブジェクトストレージ、ボリュームストレージ、データベースストレージなど、さまざまな種類があります。

特定のクラウドワークロードタイプのセキュア化

クラウドワークロードのセキュリティには以下の様々なツールと技法があります。

- **IAM**：クラウド環境におけるリソースへのアクセスを管理します。
- **アクセスポリシー**：リソースへのアクセスと許可されるアクションを定義します。
- **暗号化と鍵管理**：データの機密性と完全性を保護します。
- **マスキング、トークン化、匿名化**：機密データを保護するための技法です。
- **DLP**：データ損失防止。機密データの漏洩を防止します。
- **DSPM**：データセキュリティポスチャ管理。クラウドデータのセキュリティポスチャを継続的に評価、監視、および修正します。

特定のストレージタイプのセキュア化

オブジェクトストレージ（Amazon Simple Storage Service(S3)、Azure Blob Storage など）は設定ミスによるデータ漏洩のリスクが高く、アクセス制御、暗号化、コンテンツ配信ネットワーク（CDN）の利用、継続的な監視など、多層的なセキュリティが必要です。

クラウドデータベースには、従来型のデータベースサービス（DBaaS）とクラウドネイティブデータベースの 2 種類があります。

- **従来型 DBaaS**：セキュリティとしてセキュアな構成、アクセス制御、最小権限の原則などが重要です。
- **クラウドネイティブデータベース**：マネージメントプレーンとデータプレーンのアクセス制御、パブリックアクセスの無効化、セキュアな接続などが求められます。

データレイクは多様なデータを統合するため、機密性やセキュリティレベルに基づいたデータの分離と区分化、アクセス制御、暗号化、ネットワークセキュリティ、継続的な監視などが重要です。

人工知能（AI）のデータセキュリティは、AIaaS（AI as a Service）とセルフ/クラウドホスト型 AI の導入形態によって考慮すべき点が異なります。

- **AIaaS**：サービスレベル合意書（SLA）やプロバイダーのセキュリティなどを確認する必要があります。
- **セルフ/クラウドホスト型 AI**：データ保護、アクセス制御、モデルポイズニングやプロンプトインジェクションなどの攻撃への対策を講じる必要があります。

ドメイン 10:アプリケーションセキュリティ

セキュア開発ライフサイクル

セキュアなアプリケーション開発には、セキュアな開発プロセスが不可欠です。従来のソフトウェア開発ライフサイクル（SDLC）にセキュリティを組み込んだセキュアソフトウェア開発ライフサイクル（SSDLC）が重要となります。

クラウド環境では、アプリケーションとインフラストラクチャの緊密な統合、DevOps のような迅速な開発手法、IaC の利用など、従来とは異なる考慮事項があります。CSA は、SSDLC を 5 つのステージに分割し、各ステージで必要なセキュリティを定義しています。

1. **セキュアな設計とアーキテクチャ**： 設計段階からセキュリティを考慮することで、後からセキュリティを追加するよりもコストを抑えられます。
2. **セキュアコーディング**： 自動化ツールなどを活用し、開発段階でセキュリティの脆弱性や欠陥を特定します。
3. **継続的なビルド、統合、テスト**： アプリケーションをテスト環境にデプロイする前に、セキュリティの脆弱性をテストします。
4. **継続的なデリバリーとデプロイメント**： アプリケーションを本番環境にデプロイする前に、セキュリティチェックを行います。
5. **ランタイム防御とモニタリング**： アプリケーションの本番環境稼働後も、継続的にセキュリティを監視し、改善します。

セキュアなクラウドアプリケーションアーキテクチャ

クラウドアプリケーションのセキュリティには、アーキテクチャレベルでの考慮が重要です。クラウド環境特有の要素として、インフラストラクチャとアプリケーションの統合、アプリケーションコンポーネントのクレデンシャル管理、IaC とパイプラインのセキュリティ、イミュータブルインフラストラクチャなどがあります。これらの要素を考慮した上で、適切なセキュリティを設計・実装することで、セキュアなクラウドアプリケーションを構築できます。

アイデンティティとアクセス管理アプリケーションセキュリティ

アプリケーションセキュリティにおいて、IAM は、適切なユーザーに適切なリソースへのアクセスを許可する上で重要な役割を果たします。

最小権限の原則、継続的な監視、職務分掌、フェデレーションといった概念が重要です。シークレット管理も IAM と同様に重要で、アプリケーションの認証情報を安全に管理するためのツールとポリシーが必要です。

DevSecOps: CI/CD とアプリケーションテスト

DevSecOps は、開発プロセス全体にセキュリティを組み込むことで、安全なアプリケーションを迅速に提供する手法です。継続的インテグレーション（CI）と継続的デリバリー（CD）を組み合わせた CI/CD パイプラインに、セキュリティテストを統合することで、開発のスピードを落とさずにセキュリティを確保します。DevSecOps では、チーム全体でセキュリティの責任を共有し、協力してセキュリティに取り組むことが重要です。

サーバーレスとコンテナー化アプリケーションに関する考察

サーバーレスとコンテナーは、クラウドアプリケーション開発で利用が増えています。サーバーレスはサーバー管理が不要で、コンテナーはアプリケーションの可搬性が高いというメリットがあります。

しかし、それぞれ特有のセキュリティ課題も抱えています。サーバーレスでは、外部サービスへの依存、脆弱性を含む依存関係、設定ミス、過剰な権限付与、インターネットへの直接アクセスなどが課題です。コンテナーでは、不十分な分離、複雑な構成管理などが課題です。これらの課題に対して、適切なセキュリティを講じる必要があります。サーバーレスでは、コードのセキュリティ、アクセス制御、機密データ保護などが重要です。コンテナーでは、イメージのセキュリティ、オーケストレーションシステムのセキュリティ、ランタイム保護などが重要です。

ドメイン 11:インシデント対応とレジリエンス

インシデント対応

インシデント対応（IR）とは、セキュリティ侵害などの予期せぬ出来事に対処するプロセスです。クラウド環境では、従来の IR とは異なる対応が必要になります。

まず、イベント、インシデント、侵害を区別することが重要です。イベントはシステム内で観察される出来事、インシデントはセキュリティポリシーに違反するイベント、侵害はシステムへの不正アクセスやデータ漏洩を引き起こすインシデントです。

クラウドにおける IR ライフサイクルは、準備、検知と分析、封じ込め、根絶と回復、インシデント後の分析という段階で構成されます。クラウド IR では、CSP との連携、レスポンダーのトレーニング、クラウド特有のプロセスと技術への対応が重要となります。

準備

クラウドインシデント対応の準備段階では、以下の 3 つが重要です。これらの準備を適切に行うことで、クラウドインシデント発生時に迅速かつ効果的な対応が可能となります。

- **CSP との連携**：SLA やインシデントサポートオプションを理解し、CSP からの通知に適切に対応できる体制を整える必要があります。
- **レスポンダーのトレーニング**：クラウド特有の技術やツールに関する知識を習得し、実践的な演習を通して対応能力を高める必要があります。
- **プロセスと技術のアップデート**：クラウド環境の特性を考慮したインシデント対応プロセスを整備し、必要なツールや技術を導入する必要があります。

検知と分析

クラウドではマネジメントプレーンや IAM のアクティビティログが重要な情報源です。また、クラウド環境の動的な性質から、リアルタイム性と全体を俯瞰できる監視体制が必要です。CSP のセキュリティ警告や、構成変更の監視も有効な手段です。

分析の優先順位としては、RECIPE PICKS と呼ばれるニーモニックが参考になります。クラウドフォレンジックでは、スナップショット、揮発性メモリの取得、ログ分析などが重要となります。

- **R**esource (current config/state)
- **E**vents (API call(s) on that resource)
- **C**hanges (diff plus associated API calls)
- **I**dentity (who made the triggering change or API call)
- **P**ermissions (of the identity; informs the blast radius)
- **E**ntitlements (of the resource; e.g., it's IAM role or managed identity)
- **P**ublic (is it public?)
- **I**P (all API calls from that IP address)
- **C**aller (all other API calls from the calling identity)
- Trac**K** (look for indications of a pivot; e.g., role chaining)
- Foren**S**ics (on a resource, or digging into resource logs)

図 *RECIPE PICKS: IR 分析の優先順位*

封じ込め、根絶、復旧

クラウド環境のインシデント対応では、封じ込め、根絶、復旧の各フェーズで、従来の環境とは異なるアプローチが必要となります。

- **封じ込め**：IAM とマネージメントプレーンの封じ込めを最優先に行います。クラウドネットワークの特性を理解し、迅速にアクセス制御を実施することが重要です。
- **根絶**：侵害されたリソースを特定し、原因を排除します。クラウド環境では、リソースを置き換える方が容易な場合があり、自動スケーリングや IaC を活用することで効率的に対応できます。
- **復旧**：IaC や自動スケーリングを活用し、迅速にシステムを復旧します。復旧に使用するイメージやリソースの安全性を確認することも重要です

インシデント後の分析

インシデント後の分析は、インシデントから教訓を学び、再発防止と対応改善を図る重要なフェーズです。クラウド環境では、クラウド担当チームを分析に含めることが重要です。また、新たなインシデントタイプに対応するランブックやプレイブックを作成し、継続的な改善を図る必要があります。

分析の焦点は、責任追及ではなく、システムの欠陥を特定することです。ここで、Just Culture のアプローチを採用することが重要になります。Just Culture とは、ミスが起こった際に個人を責めるのではなく、システム全体の改善を促す考え方です。具体的には、以下の点を重視します。

- ミスの報告を奨励し、隠蔽を防ぐ
- ミスの原因を分析し、再発防止策を講じる
- 個人の責任を問うのは、意図的な違反や重大な過失があった場合のみ

Just Culture のアプローチを採用することで、組織文化全体の改善に繋がり、より安全

なクラウド環境を構築することができます。

レジリエンス

クラウド環境におけるレジリエンスとは、障害発生時にもアプリケーションやシステムが稼働し続ける能力のことです。レジリエンスには、単一リージョン、マルチリージョン、マルチプロバイダーの 3 つのレベルがあります。単一リージョンは最もコスト効率が高く、マルチプロバイダーは最も障害耐性が高いですが、コストも高くなります。マルチリージョンは、単一リージョンの障害に備え、同一 CSP の複数リージョンにシステムを展開することで、可用性を高めます。

IaaS/PaaS では、自動スケーリング、サーバーレス、IaC、CI/CD パイプライン、カオスエンジニアリングなど、様々なツールがレジリエンス向上に役立ちます。

SaaS では、プロバイダーのレジリエンス能力に依存するため、SLA をよく確認し、必要に応じてデータ抽出や冗長化などの対策を検討する必要があります。

ドメイン 12:関連技術と戦略

ゼロトラスト

ゼロトラスト（ZT）は、境界の内外を問わず、あらゆるユーザーやデバイスを信頼せず、常に検証を行うセキュリティ戦略です。多要素認証、マイクロセグメンテーション、暗号化などを用いて、アクセス制御を強化します。ZT は、従来の境界ベースのセキュリティモデルが効果を失いつつあるクラウド環境において、特に重要性を増しています。ZT の導入により、セキュリティ侵害のリスクを低減し、機密データを保護することができます。

人工知能

人工知能（AI）は、クラウドセキュリティにおいて、サービスとして利用されるだけでなく、セキュリティを強化するツールとしても活用されています。AI サービスは、クラウドでホストされる場合が多く、AI as a Service (AIaaS)として提供されます。

AI は、クラウドセキュリティを強化する一方、新たな攻撃ツールとして悪用されるリスクもはらんでいます。AI を用いたセキュリティとしては、脅威検知、ログ分析、インシデントレスポンス、ポスチャ評価、セキュアコード解析、マルウェア分析、リスクの優先順位付け、エンタイトルメント管理など、様々な分野で活用が期待されています。

しかし、AI の利用には、バイアス、説明可能性、敵対的攻撃など、潜在的なリスクと制限事項も存在します。例えば、AI モデルの学習データに偏りがあると、AI が出力する結果にも偏りが生じる可能性があります。また、AI の判断プロセスは複雑で、人間には理解しにくい場合があり、説明責任を果たすのが難しいという課題もあります。さらに、AI システム自体が攻撃対象となり、誤動作や悪用される可能性もあります。

脅威と脆弱性の管理

脅威と脆弱性管理（TVM）は、クラウド環境のセキュリティリスクを継続的に特定・評価・軽減するプロセスです。クラウド特有の脅威や脆弱性に対処するには、従来の TVM をクラウド環境に適応させる必要があります。具体的には、マネージメントプレーンの保護、脆弱性スキャン、コンテナーと VM のセキュリティ保護、クレデンシャルの盗難対策、クラウドネイティブな脅威検出、ソフトウェアサプライチェーンのセキュリティ確保、脅威インテリジェンスの活用などが重要となります。