Security Guidance

For Critical Areas of Focus in Cloud Computing v5

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

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

The permanent and official location for the CSA Security Guidance Working Group is https://cloudsecurityalliance.org/research/working-groups/security-guidance

日本語版提供に際しての告知及び注意事項

本書「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」は、Cloud Security Alliance (CSA)が公開している「Security Guidance For Critical Areas of Focus in Cloud Computing v5」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10月15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

「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」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
太田　吏城
釜山　公徳
高尾　美由紀
高橋　久緒
富永　勇人
松浦　一郎
満田　淳
米山　努
山口　弘行
松崎　祥三
諸角　昌宏

Acknowledgments

Lead Authors

Rich Mogull
Mike Rothman

Contributors

Jackie Donnelly
Moshe Ferber
Larry Hughes
Michael Roza
Peter van Eijk

Reviewers

Mohammad Aamir
Frank Addo
Daniel Adjorlolo
Hafiz Ahmed Sheikh Adnan
Ilango Allikuzhi
Shonnie Almeida J.
Babs Alo
Aakash Alurkar
Agbu Amachundi Enoch
Stephen Amolo
Divya Aradhya
Robyn Bailey
Adeel Bakht
Suramya Bakshi
Mohamed Balushi Al
Vinay Bansal
Robin Basham
Myriam Batista
Allen Baylis
Renu Bedi
Paul Benedek
Bachir Benyammi
Jamie Beth
Shirin Bhambhani

Roberto Bonalumi
Karl Brooks
Jasper Brouwer
Amit Butail
Varun Carlay
Dhanushraj Chandrahasan
Senthilkumar Chandrasekaran
Akshay Chandrasekaran Sekar
Shankar Chebrolu
Anand Chirathadam Abraham
John Chiu
Anand Choksi
Vipul Dabhi
Joseph Dacuma
Michel-Ange Dagrain
Thomas Defise
Neelima Devana
Mankirat Dhodi Singh
Balaram Dhulipudi
Dr. Ivan Djordjevic
Ivan Djordjevic
Moses Dlamini
Keinaz Domingo N.
David Dorsey
Rob Doyon
Vinay Dubey
Swapna Dulganti
Nielet D'Mello
Mohamed Elbashir
Mahmood Elrefai
Joseph Emerick
Dr. Marco Ermini
Kingsley Ezeocha
Ahmed Fawzy

Lorena Ferreyro
Kenneth Ferris
Jonathan Fessenden
Jose Figueredo-Maseda C.
Elaine Flesch
Fernando Fonseca
Park Foreman
Adame Frances
Aadithya Francis
André Gaio Alexandre
Luca Gattobigio
Viktor Gazdag
Jan Gerst
Hussein Ghazy
Tulika Ghosh
Ricardo Giorgi
Andriana Gkaniatsou
Saurabh Goswami
Trevor Gregorio
Nageswara Gude Rao
Madhu Guthikonda
Ahmed Harris
Lyle Hearne
Johnny Hernandez
Dirce Hernandez Eduardo
Aldo Hernández Villaseca
Moreno Hill Sint
Matthew Hoerig
Abdulsalam Ibrahim B.
Ricci Ieong
Frank Iheonu
Arron Johnson
Rahul K
Prasannakumar K G
Patrick Kabongo B.
Nithin Kadumberi Mohan Thattiot
Ruchi Kandpal
Sivakumar Karthikeyan
Shakthi Kathirvelu Priya
Sunil Katwal
Arpitha Kaushik
Alon Kendler
Rohit Khosla
Vana Khurana
Jari Kiero
Brenda Killingsworth L.
Morgan King
Samantha Kloos-Kilkens
Simon Kok
Vivek Krishnan
Sunil Kumar
Francois Laas
Hadir Labib
Daniel Lai
Raymond Lai
Law Lain Chamber
Sundas Latif
Seshagirirao Lekkala
Yutao Ma
Stephen Macomber
Yuvaraj Madheswaran
Niclas Madsen
Ahmed Mahmoud Nabil
Vaibhav Malik
Mohamed Malki
Cecil Martin
Marcus Maxwell
Bilal Mazhar
Mark McDonagh
José Medina Carlos Vargas
Santiago Medranda
Ashish Mehta
Shobhit Mehta
Andre Mess
Enida Metaj
Akhil Mittal
Adeeb Mohammed
Victor Monga
Kenneth Moras
Masahiro Morozumi
Andrew Morrow B.
Venkata Nedunoori
Harry Ngai
Fredrick Ogonda

Esborn Okero
Opeyemi Onifade
Joseph Orsetto
John Oseh B.
Jed Owens
Iyiola Oyinloye
Mayur Pahwa
Govindaraj Palanisamy
Meghana Parwate
Vaibhav Patkar
Martino Pavone
Eric Peeters
Eliza Popa
Kunal Pradhan
Ramon Domingo Quimesó
Adnan Rafique
Sonali Rajesh ZolT R
Marappan Ramiah
Alex Rebo
Aldo Richner
Rangel Rodrigues
Vishakha Sadhwani
Shahid Saleem
Joshua Salvador
Mukund Sarma
Patnana Sayesu
Davide Scatto
Thomas Schmidt
Michael Schmitz
Kg.Seow
Vikrant Shah
Rakesh Sharma
Alex Sharpe
Akshay Shetty
Dr. Ian Silvester
Ryan Simon
Gurpratap Singh
Gaurav Singh
Anamika Singh
Serenity Smile
Heinrich Smit
Jorge Soboredo González
Silvano Sogus
Mikhail Sokolov
Dr. Chantal Spleiss
Dr. Manish Srivastava Kumar
Kevin Stander
Roy Stultiens
Yuanji Sun
Pratibha Swamy
Manjunath T A
Mohammed Tanveer
Billy Teow
Kim Tham Fui
Timothy Thatcher
Michael Theriault
Larry Timmins
Chee Tiong
Ilia Tivin
Wiem Tounsi
Micheal Troutman
Nsikak-Abasi Una Shammah
Pieter VanIperen
Ashish Vashishtha
Peter Ventura
Vaishnav Vijayakumar
Antonio Villamor Magallanes Jr
Alex Webling
Henry Werchan
Udith Wickramasuriya
Pawel Wilczynski
Rini Wilson
Wai Kong Wong
Ben Woods
Ezra Woods
James Yankelvich
Tsutomu Yoneyama
Bader Zyoud
Dennis de Caes
Peter van Loon
Tiaan van Schalkwyk

CSA Global Staff

Judy Bagwell
Hillary Baron
Marina Bregkou
Josh Buker
Daniele Catteddu
Emily Everett
Ryan Gifford
Frank Guanco
Sean Heide
Erik Johnson
Alex Kaluza
Claire Lehnert
Stephen Lumpe
Cion Mensidor
Hannah Rock
Andy Ruth
Anna Schorr Campbell
Stephen Smith
Adriano Sverko
John Yeoh

Table of Contents

内容

セキュリティガイダンス v5 イントロダクション

クラウドセキュリティアライアンスの「*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*」（*略して「セキュリティガイダンス*」）の第 5 版へようこそ。 進化し続けるテクノロジーとしてのクラウドコンピューティングの台頭は、多くのチャンスと課題をもたらしています。この文書では、クラウドコンピューティング技術の採用に伴うリスクを管理・軽減しながら、ビジネス目標をサポートするためのガイダンスとインスピレーションの両方を提供することを目的としています。

クラウドセキュリティアライアンスは、クラウドコンピューティングの領域でセキュリティ保証を提供するためのベストプラクティスの実装を推進し、クラウドパラダイムの導入を目指す組織向けに実用的で実行可能なロードマップを提供しています。セキュリティガイダンスの第 5 版は、これまでの*セキュリティガイダンス*の反復、熱心な研究、クラウドセキュリティアライアンスのメンバー、作業部会、コミュニティ内の業界専門家からの一般参加の上に構築されています。
このバージョンでは、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。

セキュアなクラウドコンピューティングの実現には、グローバルに分散した関係者の幅広い層の積極的な参加が必要です。CSA は、業界パートナーシップ、国際支部、作業部会、および個人を、この多様なコミュニティへ結集しています。このリリースにご協力いただいたすべての方々に深く感謝しています。

セキュアなクラウドコンピューティング環境を確保するためのベストプラクティスを特定し、推進するために、私たちとどのように協力できるかについては cloudsecurityalliance.com をご覧ください。

Jim Reavis
Chief Executive Officer (CEO)
Cloud Security Alliance

Illena Armstrong
President
Cloud Security Alliance

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

このドメインは、CSA(クラウドセキュリティアライアンス)*セキュリティガイダンス*の概念的枠組みを提供します。クラウドコンピューティングの説明と定義、ベースライン用語の設定、およびドキュメントの他のドメインで使用される全体的なコントロール、デプロイメント、およびアーキテクチャモデルの詳細について説明します。

クラウドコンピューティングは、技術、技術の集合体、運用モデル、ビジネスモデル、経済パラダイムなど、さまざまな視点から捉えることができます。クラウドコンピューティングは、従来のコンピューティングシステムに変革をもたらし、破壊的な影響を与えるものであり、支配的なデジタルトランスフォーメーションモデルとして取って代わりました。CSA CCSK *セキュリティガイダンス*の初期バージョンに含まれている参照モデルは引き続き適切ですが、業界の成熟に伴い、継続的な進歩（クラウドサービスプロバイダ(CSP) 、ゼロトラスト、AI、進化する慣行などの新しいツールや技術）を反映するためのアップデートが必要です。自動化と人工知能の能力の継続的な向上によって、このアップデートを行っても、今後数年間のすべての進化を説明することはできません。

クラウドコンピューティングは、俊敏性、レジリエンシー 、セキュリティ、および経済面で大きなメリットをもたらします。しかし、これらのメリットは、クラウドモデルを適切に理解して採用し、クラウドアーキテクチャとクラウドプラクティスをクラウドプラットフォームの特徴と機能に合わせて初めて実現されます。クラウドサービス利用者（CSC[1]）が、既存のアプリケーションや資産を何も変更せずに CSP に移動するだけでは（リホスティングまたは「リフト アンド シフト」と呼ばれる） 、 期待される俊敏性、レジリエンシー、およびセキュリティを提供できないことが多く、一方でコストは増大し続けます。要するに、クラウドコンピューティングのメリットは、クラウドコンピューティングモデル、クラウドネイティブの機能、サービスの適切な使用方法を理解することと密接に結びついています。

このドメインは、このガイドの残りの部分とその推奨事項の基礎を構築することを目的としています。クラウドと従来のコンピューティングの違いを強調しながら、クラウドコンピューティングの共通言語と理解を提供することを目的としています。このドメインは、すでに述べたクラウドのメリットに加えて、クラウドセキュリティの専門家やその他の関連する関係者を、より良いセキュリティ体制を確保するクラウドアプローチの採用に向けて導き支援します。

クラウドセキュリティアライアンスは、まったく新しい分類法や参照モデルを作成しようとしているものではありません。私たちの目的は、クラウド コンピューティング分野で働く専門家にとって最も関連

[1] The acronym CSC is used interchangeably to mean any cloud service customer, cloud service consumer, or cloud service client.

性の高いセキュリティ上の考慮事項に焦点を当て、既存のモデル（特に NIST SP 800-145[2]、ISO/IEC 22123-1:2023[3]、ISO/IEC 22123-2:2023[4]での作業）の本質を引き出し調和させることです。
基本原則の理解をさらに深め、クラウドセキュリティプラクティスを実装するための具体的なトピックと実践的な戦略を探るために、追加の参考資料が提供されています。

学習目標

このドメインでは、次のことを学びます。

- 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モデルの特定。
- クラウドコンピューティングにおける参照モデルとアーキテクチャモデルの認識。
- 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。

1.1 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は、コンピューティング、ネットワーク、ストレージなどの抽象化を通じて、コンピューティングリソースの共有プールを管理するために使用される運用モデルおよび一連の技術です。クラウドモデルは、コンポーネントとリソースを迅速にオーケストレーション、プロビジョニング、実装、スケールアップまたはスケールダウン、および廃棄できる世界を想定しており、割り当てと利用のためのオンデマンドユーティリティのようなモデルを提供します。利害関係者のコラボレーション、機敏性、弾力性、可用性、レジリエンシー、コスト削減などのメリットが含まれます。

米国国立標準技術研究所（NIST）並びに国際標準化機構（ISO）および国際電気標準会議（IEC）による*クラウドコンピューティングの定義を次に示します。*

NIST SP 800-145 では、クラウドコンピューティングを次のように定義しています: クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバ、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるものである。 ＜訳注：IPA 提供の日本語版より引用＞[5]

[2] NIST. (2011) SP 800-145: *The NIST Definition of Cloud Computing.*
[3] ISO/IEC. (2023) 22123-1:2023: Information technology - Cloud computing Part 1: Vocabulary
[4] ISO/IEC. (2023) 22123-2:2023: Information technology - Cloud computing Part 2: Concepts
[5] NIST. (2011) SP 800-145: *The NIST Definition of Cloud Computing.*

ISO/IEC 22123-1:2023 では、クラウドコンピューティングを次のように定義しています: *「セルフサービスプロビジョニング[6]とオンデマンド管理により、スケーラブルで柔軟な共有可能な物理または仮想リソースのプールへのネットワークアクセスを可能にするパラダイム」*[7]

クラウドをもっと簡単に説明すると、プロセッサやメモリなどのリソース群を大きなプールに入れることです(この場合は仮想化[8]を使用)。CSC は、要件（CPU8 基、メモリ 16GB など）に基づいて、プールから必要なリソースを要求します。基盤となるクラウドコンピューティング技術は、これらのリソースを CSC にオーケストレーションし、CSC はネットワークを介してリソースに接続して使用します。CSC は作業を完了すると、他のユーザが使用できるようにリソースをプールに戻せます。

クラウドは、プロセッサ、メモリ、ネットワークといった下位インフラストラクチャから、データベースやアプリケーションのような上位レベルのソフトウェアリソースまで、ほぼすべてのコンピューティングリソースで構成できます。たとえば、他の数百の組織が共有するサービス上で 500 人の従業員向けの CRM（顧客関係管理）アプリケーションをサブスクライブすることは、コンピューティングクラウド上で 100 台のリモートサーバーを起動するのと同様のクラウドコンピューティング事例です。

1.1.1 抽象化とオーケストレーション

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。リソースは、基盤となる物理インフラストラクチャから抽象化されたリソースのプールを作成し、オーケストレーション(および自動化)を使用してプールから CSC へ調整、割り当て、提供されます。これには固有の標準化レベルがあり、すべての CSC が基本的に同じ機能サービスを受けられ、その後、CSC 独自の柔軟な方法で統合されます。このように、これら 2 つの概念は、何かを「クラウド」として定義するために使用するすべての本質的な特性を作り出します。

クラウドはもともと*マルチテナント*[9]です。複数の CSC が同じリソースプールを共有しますが、論理的に、時には物理的に分離され、互いに切り離されます。分離により、CSP はさまざまな CSC にリソースを分割することができ、また、分離によって、CSC データの機密性と完全性にとって基本的な、相互に他者の資産の閲覧や変更ができなくなります。さらに、CSP がリソースの過剰使用を測定および制限できることは、各 CSC に提供されるサービスの民主的な使用と可用性にとって重要です。マルチテナントは、組織間での利用にとどまらず、「プライベートクラウド」とも呼ばれる 1 つの組織内のさまざまなユニット間のリソース分散も容易にします。

---

[6] *Self-service provisioning refers to the provisioning of resources provided to cloud services performed by CSCs through automated means. Examples of resources include servers, operating systems, networks, software, applications, and storage equipment*.

[7] ISO/IEC. (2023) Information Technology - Cloud Computing - Part 1: Vocabulary.

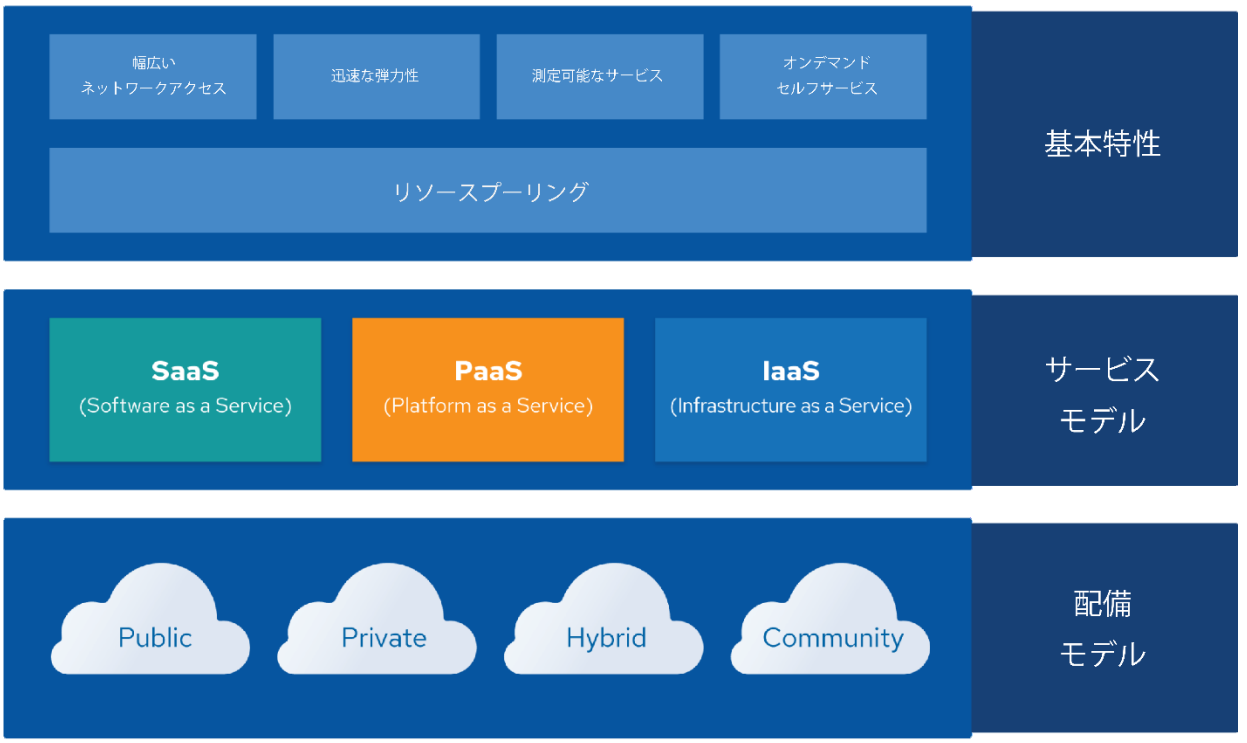
[8] NIST. (2018) SP 800-125A: Security Recommendations for Hypervisor Deployment on Servers *Virtualization*.

[9] In this reference to multi-tenant, a tenant is a cloud customer or CSC.

1.2 クラウドコンピューティングモデル

CSA は、クラウドコンピューティングを定義するための標準である NIST SP 800-145 モデルをクラウドコンピューティングに使用しています[10]。CSA はまた、参照モデルとして機能する、より詳細な ISO/IEC モデル 22123-1:2023 と 22123-2:2023 を支持しています。このドメイン全体では、両方を参照します。

NIST は、クラウドコンピューティングを、5 つの基本特性、3 つのクラウドサービスモデル、4 つのクラウド配備モデルに基づいて説明しています。これらのモデルの概要は、次のセクションで説明します。



[11]

図1: NIST および ISO/IEC 規格に基づくクラウドコンピューティングモデルの概要

1.2.1 基本特性

[10] CSA has chosen to align with the NIST definition of cloud computing (NIST 800-145) to drive consensus for a common language and focus on use cases rather than semantics. This material is intended to be broadly usable and applicable to organizations globally. While NIST is a U.S. government organization, the selection of this reference model should not be interpreted to suggest the exclusion of other points of view or geographies.

[11] Depiction of the NIST Model of Cloud Computing

NIST モデルでは、クラウドを 5 つの基本特性によって説明しています。この基本特性は、従来のホスティングサービスや、ホスティング、仮想化などの他の種類のクラウドサービスとクラウドコンピューティングを区別しています。これらの特性を理解することは、クラウドコンピューティングの可能性を最大限に活用し、クラウド導入の戦略的計画に不可欠です。

NIST が説明する 5 つの本質的な特徴は、以下の通りです。

- **リソースプーリング:** クラウドコンピューティングは、さまざまな物理リソースと仮想リソースをプールし、*マルチテナント*モデルを使用して複数の CSC にサービス提供します。ストレージ、プロセッサ、メモリ、ネットワーク帯域幅などのリソースは、需要に応じて動的に割り当てられ、また再割り当てされます。
- **幅広いネットワークアクセス:** サービスはネットワーク経由で利用でき、様々な機種のシンクライアントまたはシッククライアントプラットフォーム（サーバ、携帯電話、ノートパソコン、IoT デバイス、タブレットなど）で使用されやすい Web ブラウザまたは専用アプリケーションを介してアクセスします。
- **迅速な弾力性:** リソースを迅速かつ柔軟にプロビジョニングし、場合によっては自動的にスケールアウトやスケールバックを迅速に行うことができます。CSC から見れば、プロビジョニングされた機能は多くの場合は無制限に見え、いつでも任意の数量を購入可能です。
- **測定可能なサービス**: クラウドシステムは、サービスの種類（ストレージ、帯域幅、アクティブなユーザーアカウントなど）に適した抽象レベルの計測機能を活用して、リソースの使用を自動的に制御および最適化します。リソースの使用状況を測定、監視、制御、レポートできるため、利用するサービスの CSP と CSC の両方に透明性がもたらされます。これにより従量課金が可能となり、コスト効率とアカウンタビリティ（従量課金制など）が促進されます。
- **オンデマンドセルフサービス**: CSC は、CSP が自動プロビジョニングするオンデマンドのクラウドリソースを一方的に要求することができ、計算時間やネットワークストレージなどのコンピューティング機能を、各 CSP との人的介入なしに、必要に応じて要求できます。

ISO/IEC 22123:2023 は 6 つの主要な特性をリストしており、最初の 5 つは上にリストされた NIST 特性と同一です。唯一の追加はマルチテナンシーであり、リソースプールとは区別されています。

1.2.2 クラウドサービスモデル

NIST は、クラウドサービスのさまざまな基本カテゴリを説明する 3 つのサービスモデルを定義しています。

- **Software as a Service (SaaS) は、**CSP によって管理およびホストされるアプリケーションです。CSC は、Web ブラウザ、モバイルアプリケーション、アプリケーションプログラミングインターフェース（API）、または軽量クライアントアプリケーションを使用して SaaS にアクセ

スします。このモデルでは、CSC は基盤となるリソースではなく、アプリケーションの設定だけを気にします。

- **Platform as a Service (PaaS)** は、アプリケーションプラットフォーム（コードを開発して実行する場所など）、データベース、ファイルストレージ、コラボレーション環境などのプラットフォームを抽象化して提供します。その他の例としては、機械学習、ビッグデータ処理、または SaaS 機能への API アクセスのためのアプリケーション処理環境などがあります。主な違いは、PaaS の場合、CSC は基盤となるインフラストラクチャを管理しないことです。
- **Infrastructure as a Service (IaaS)** は、ネットワークやストレージなどの基本的なコンピューティングインフラストラクチャのリソースプールへのアクセスを提供します。IaaS では、CSC は仮想マシン、ネットワーキング、ストレージ、実行中のアプリケーションなど、基盤となる仮想インフラストラクチャの管理を担当します。

ISO/IEC 22123-3:2023 では、SaaS、PaaS、IaaS（SPI とも呼ばれる）のサービスモデル階層（アプリケーション、プラットフォーム、インフラストラクチャの機能タイプ）に密接に対応するクラウド機能タイプを備えた、より複雑な定義を使用しています。その後、CaaS（Communications-as-a-Service）、NaaS（Network-as-a-Service）、DSaaS（Data Storage as a Service）、DSaaS（Data Recovery as a Service）など、より細分化されたクラウドサービスのカテゴリに拡張しています。

これらのカテゴリはある程度浸透しています。SPI 階層にまたがるクラウドサービスもあれば、単一のサービスモデルに綺麗に分類されないクラウドサービスもあります。実践的に言えば、これら 3 つのカテゴリにすべてを割り当てる理由、あるいは ISO/IEC モデルのより細かいカテゴリに割り当てる理由はありません。これは記述ツールであり、厳格なフレームワークではありません。

どちらのアプローチも妥当ですが、NIST モデルはより簡潔かつ広く使用されているため、CSA リサーチで主に使用している定義です。

1.2.3 クラウド配備モデル

NIST と ISO/IEC は、同じ 4 つのクラウド配備モデルを使用しています。これらの技術は、サービスモデル全体にわたって導入、利用、および適用される方法です。

- **パブリッククラウド**: このクラウドインフラストラクチャは、一般ユーザーまたは大規模な業界団体が利用でき、CSP が所有します。
- **プライベートクラウド**: このクラウドインフラストラクチャは、単一の組織に対してのみ運用されます。組織またはサードパーティによって管理され、オンプレミスまたはオフプレミスに配置される場合もあります。
- **コミュニティクラウド:** クラウドインフラストラクチャは複数の組織で共有され、共通の懸念事項（ミッション、セキュリティ要件、ポリシー、コンプライアンスに関する考慮事項など）を持

つ特定のコミュニティをサポートします。組織またはサードパーティによって管理され、オンプレミスまたはオフプレミスに配置される場合もあります。

- **ハイブリッドクラウド:** クラウドのインフラストラクチャは 2 つ以上の異なるクラウドインフラストラクチャ（プライベート、コミュニティ、パブリック）の組み合わせです。各クラウドは独立した存在ですが、標準化された、あるいは固有の技術で結合され、データとアプリケーションの移植容易性を実現しています（例えばクラウド間のロードバランスのためのクラウドバースト[12]）[13]。

その他の配備モデル。

- **マルチクラウド:** マルチクラウド環境では、CSC は異なる CSP のアプリケーションやシステムなどの複数のクラウドサービスを利用します。このアプローチは、単一のクラウドプロバイダへの依存を減らし、アーキテクチャ設計に技術的なレジリエンスを組み込むために広く採用されています。
- **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です。通常は従来のデータセンターへの接続です。

1.3 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構築と運用に使用される技術と手法は幅広く進化しており、あらゆる単一の参照モデルやアーキテクチャモデルが時代遅れになる可能性があります。このセクションの目的は、いくつかの基礎を提供し、複雑で新しいモデルを理解するためのベースラインを提供して、セキュリティ専門家が情報に基づいた意思決定を行えるようにすることです。NIST クラウドコンピューティングの定義を補完する詳細なリファレンスアーキテクチャモデルとして ISO/IEC 22123 と NIST 500-292[14]を推奨します。さらに、4 つの個別の組織アーキテクチャから機能を統合することを目的とした CSA エンタープライズアーキテクチャモデル[15]の検討も提案します。

クラウドコンピューティングの見方の 1 つは、SaaS が PaaS 上に構築され、IaaS 上に構築されるスタックという考え方です。これは、すべての（またはほとんどの）実際の配備モデルを代表するものではありませんが、有用な参照ベースラインとして役立ちます。SPI スタックは進化しており、サービスの提供が成熟するにつれて、サービスモデル間の重複や明確な区別が薄れつつあります。まず、各クラウドサービスモデル（SPI スタックのレイヤー）の標準アーキテクチャを把握し、次にいくつかの例を挙げて線

[12] A configuration setup where an application running in a private cloud or data center dynamically extends to a public cloud to access additional computing resources when the demand exceeds the capacity of the primary environment, ensuring consistent performance and availability.

[13] Hybrid is also commonly used to describe a non-cloud data center bridged directly to a CSP. The original NIST definition refers to a mixture of cloud solutions. Since then it has become more narrowly focused on mixtures of cloud models.

[14] NIST. (2011) NIST Cloud Computing Reference Architecture

[15] CSA. (2021) CSA Enterprise Architecture Reference Guide.

がぼやけている様子を示します。最後に、CSA エンタープライズアーキテクチャモデルで締めくくります。このモデルは、クロスプラットフォームの機能とパターンを開発している人や、統合されたマルチクラウドアプローチに関心がある人を支援します。

1.3.1 Infrastructure as a Service

IaaS の基盤は物理設備とインフラストラクチャハードウェアです。クラウドコンピューティングでは、これらのリソースを抽象化してプールしますが、最も基本的なレベルでは、その上に構築するための物理ハードウェア、ネットワーク、ストレージが常に必要です。これらのリソースは、抽象化とオーケストレーションを使用してプールされます。抽象化は、多くの場合、仮想化によってリソースを物理的な制約から解放し、プーリングを可能にします。次に、一連のコア接続およびデリバリツール(オーケストレーション)が、これらの抽象化されたリソースを結び付け、プールを作成し、それらを CSC に割り当てて配信するための自動化を提供します。

オーケストレーションは、一般的に API を使用して促進されます。API は通常、クラウド内のコンポーネントの基盤となる通信方法であり、その一部はリソースと構成を管理するために CSC に公開されています。最近のほとんどのクラウド API は、HTTP 上で実行される REST（Representational State Transfer）を使用しているため、インターネットサービスに適しています。

ほとんどの場合、それらの API はリモートでアクセスでき、Web ベースのユーザーインターフェースにラップされます。この組み合わせはクラウド管理またはコントロールプレーンと呼ばれ、CSC はこれを使用して、仮想マシンインスタンスの起動や仮想ソフトウェア定義ネットワーク（SDN）の構成など、クラウドリソースの管理と構成を行います。セキュリティの観点からは、ネットワークを介してマネージメントインターフェースを利用できるため、オンプレミスのインフラストラクチャを保護することと大きく異なります。攻撃者がマネージメントプレーンを侵害すると、クラウドインフラストラクチャへの特権アクセスが可能になります。

以下は、コンピューティング IaaS プラットフォームのアーキテクチャ例を極めてシンプルに説明します。

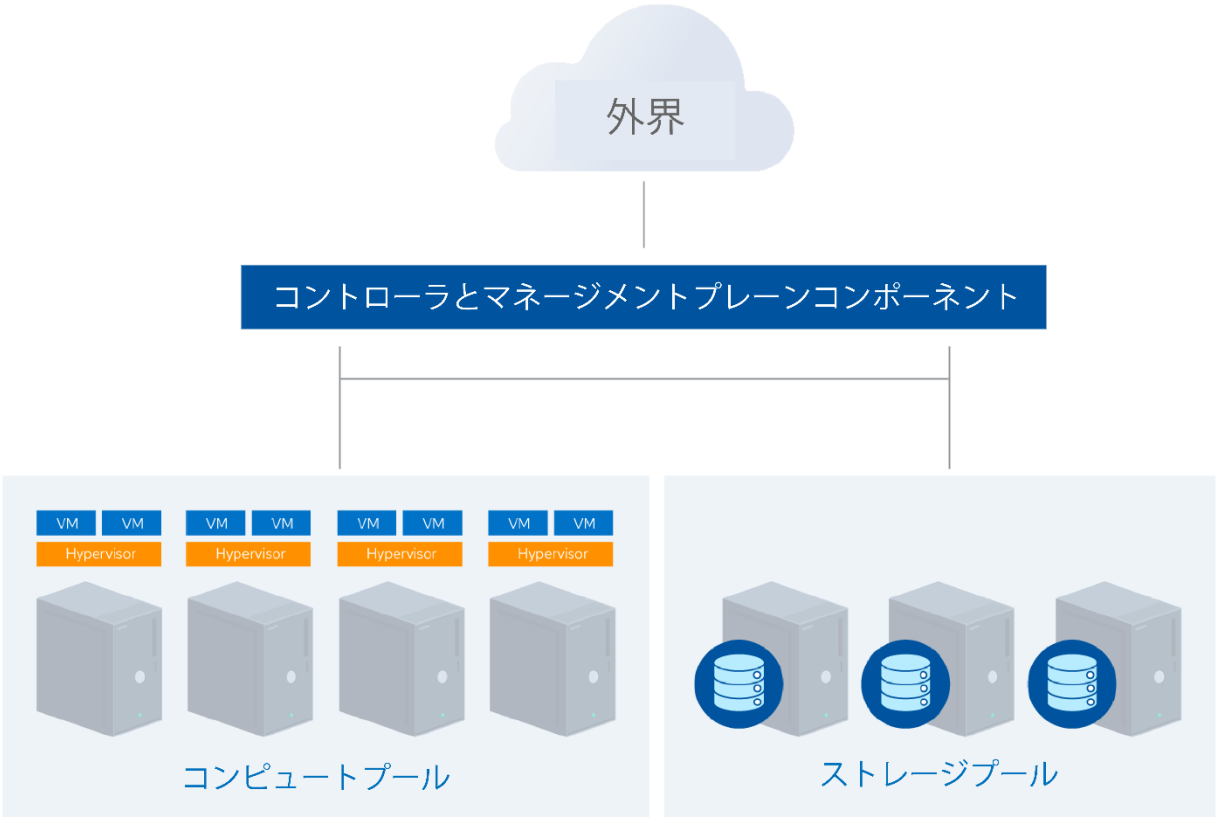


図 2: IaaS コンピューティングプラットフォームのシンプルなアーキテクチャ

この例は、ハイパーバイザー[16]とオーケストレーションソフトウェアを実行する物理サーバーを備えた IaaS コンピューティングプラットフォームを示しています。クラウドコントローラは、リソースの割り当て、仮想インスタンスの作成、ネットワーキングとストレージの構成、インスタンスにアクセスするための CSC の接続情報の仲介を行います。

1.3.2 Platform as a Service

PaaS はすべてのサービスモデルの中で、PaaS として提供するサービスの幅広さやアプローチの多様さから、明確に特徴付けることが最も難しいものです。 PaaS サービスは一般に、アプリケーション開発フレームワーク、ミドルウェア機能、およびデータベース、メッセージキュー、イベントロギン

[16] A hypervisor, also known as a virtual machine monitor (VMM), is a software, firmware, or hardware platform that creates and runs virtual machines by abstracting and managing the underlying physical hardware resources, allowing multiple operating systems to run concurrently on a single physical host.

グなどのサポートサービスを統合します。これらのサービスにより、開発者はスタックがサポートするプログラミング言語とツールを使用して、プラットフォーム上でアプリケーションを構築できます。
PaaS はすべてのサービスモデルの中で、PaaS として提供するサービスの幅広さやアプローチの多様さから、明確に特徴付けることが最も難しいものです。
実社会で頻繁に目にし、我々のモデルにも示されている選択肢の 1 つは、IaaS の上にプラットフォームを構築することです。たとえば、統合、永続化、ミドルウェアの各レイヤーは IaaS プラットフォーム上に構築され、それらをプールしてオーケストレーションし、PaaS サービスとして API を通じて CSC がアクセスできるようにします。

これは、変更されたデータベース管理システムソフトウェアインスタンスを使用して構築および導入された DBaaS(サービスとしてのデータベース)である可能性があります。CSC は API や Web コンソールを介してデータベースを管理し、通常のデータベースネットワークプロトコルや API を介してデータベースにアクセスします。

PaaS では、クラウド利用者はプラットフォーム（またはそれを活用するアプリケーション・プレゼンテーション・レイヤー）のみを認識し、基盤となるインフラストラクチャは認識しません。この例では、CSC が個々のサーバ、ネットワーキング、パッチなどを管理することなく、データベースサービスは使用状況に基づいて必要に応じ拡張または縮小します。

以下は、IaaS アーキテクチャ上で動作する PaaS を簡略化したアーキテクチャです。

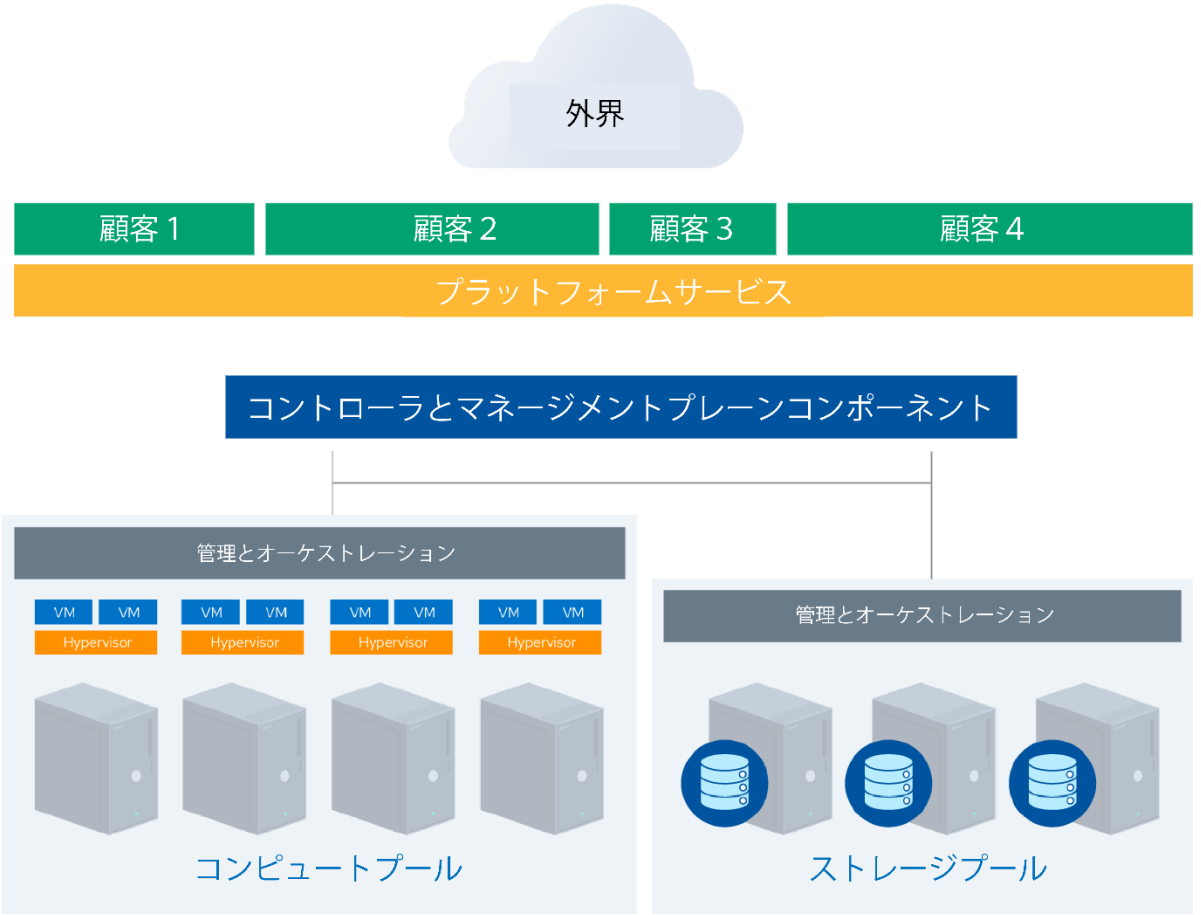


図 3: IaaS 上に構築された PaaS のシンプルなアーキテクチャ

PaaS は必ずしも IaaS 上に構築される必要はありません。カスタムビルドのスタンドアロンアーキテクチャにできない理由はありません。特徴的なのは、基盤となるクラウドインフラストラクチャではなく、CSC がプラットフォームにアクセスして管理することです。AI を活用した開発ツール、機械学習運用（MLOps）[17]、AI ライフサイクル管理などのユースケースをサポートするカスタム AI と機械学習の統合サービスも、その 1 つの例として考えられます。

[17] Machine Learning Operations (MLOps) is a set of practices that streamline the entire lifecycle of machine learning models. It unifies ML application development with ML system deployment and operations.

1.3.3 Software as a Service

SaaS サービスは完全なアプリケーションであり、あらゆる大規模なソフトウェアプラットフォームに典型的なアーキテクチャの複雑さをすべて網羅しています。多くの SaaS CSP は、俊敏性、レジリエンス、経済性の向上のために、IaaS と PaaS の上に構築されています。

最新のクラウド SaaS アプリケーションのほとんどは、IaaS と PaaS を組み合わせており、場合によっては異なる CSP にまたがっています。多くは、一部またはすべての機能に対して公開 API も提供しています。多くの場合、さまざまな CSC、特に Web ブラウザ、API、モバイルアプリケーションをサポートするために必要です。

SaaS サービスは、Web ブラウザやモバイルアプリケーションのユーザーインターフェース、インターネット API アクセスを共通にサポートするアプリケーション/ロジック層とデータストレージ、API、プレゼンテーション層のサービスを持つ傾向があります。

以下の単純化されたアーキテクチャは、実際の SaaS プラットフォームからの引用ですが、使用中の特定製品への参照を取り除くために一般化されています。

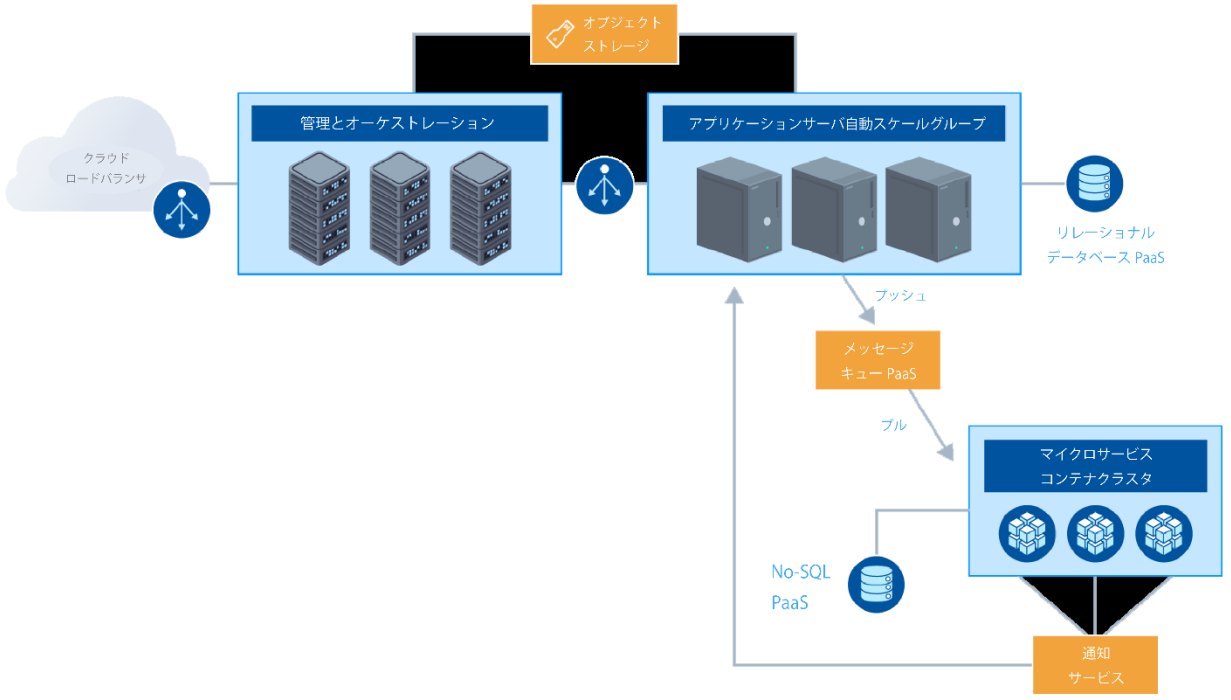


図 4: PaaS と IaaS を基盤とした SaaS プラットフォームのシンプルなアーキテクチャ

1.3.4 Anything as a Service

Anything as a Service (XaaS) は、ローカルやオンプレミスで提供されるものではなく、インターネット上で提供されるさまざまなサービスの本質を捉えた広義の包括的な用語です。このモデルはクラウドコンピューティングの基盤であり、"X"はサービスとしてユーザーに提供される事実上すべてのサービス、アプリケーション、プラットフォームコンポーネントを表すことができます。これらは、ほとんどの場合 IaaS/PaaS/SaaS モデルに当てはまりますが、より具体的でわかりやすいネーミングになっています。

1.3.5 オーバーラップするサービスモデル

SPI クラウドサービスモデルは階層構造で表現されることが多く、各レイヤーはその下のレイヤー（IaaS、PaaS、SaaS）上に構築されますが、これらのサービスを実際に実装して利用する方法は、はるかに柔軟です。SPI スタックは、さまざまなクラウドサービスモデルを理解するのに役立つガイドです。固有の柔軟性と重なり合うレイヤーを認識することが重要です。SPI の実装は厳密な階層構造で構築される必要はなく、オーバーラップするサービスモデルと呼ばれるモデル間の境界線があいまいになることが多くなります。オーバーラップするサービスモデルは厳密な階層によって定義されておらず、複数のサービスモデルの特性を同時にカプセル化することが多くなります。

例えば、多くのサービスは SaaS（Web ブラウザで完全に提供されるアプリケーション）と PaaS（プラットフォームの機能の一部を利用者のアーキテクチャに統合するための API）の両方の特性をカプセル化しています。

1.3.6 CSA エンタープライズアーキテクチャモデル

CSA Enterprise Architecture（EA）は方法論であり、ツールセットでもあります。 CSA EA はフレームワーク、つまりセキュアなクラウドインフラストラクチャのアーキテクチャのための包括的なアプローチです。 CSA EA を、改善の機会の評価、技術の導入のロードマップの作成、再利用可能なセキュリティパターンの特定、共通の機能セットに照らしてさまざまな CSP やセキュリティ技術ベンダーを評価するために使用できます。

CSA EA を作成するために、CSA リサーチ は次の 4 つのドメインにわたって 4 つの業界標準アーキテクチャモデルを活用しました。

- **Business Operation Support Services (BOSS)** – Sherwood Applied Business Security Architecture (SABSA)
- **IT Operation Services (ITOS)** – IT Infrastructure Library (ITIL)
- **Technology Solution Services (TSS)**, including Infrastructure (InfraSrv), Information (InfoSrv), application (AS), and Presentation (PS) Services – The Open Group Application Framework (TOGAF)
- **Security and Risk Management (SRM)** – OpenGroup Security Forum (formerly known as the Jericho Forum)

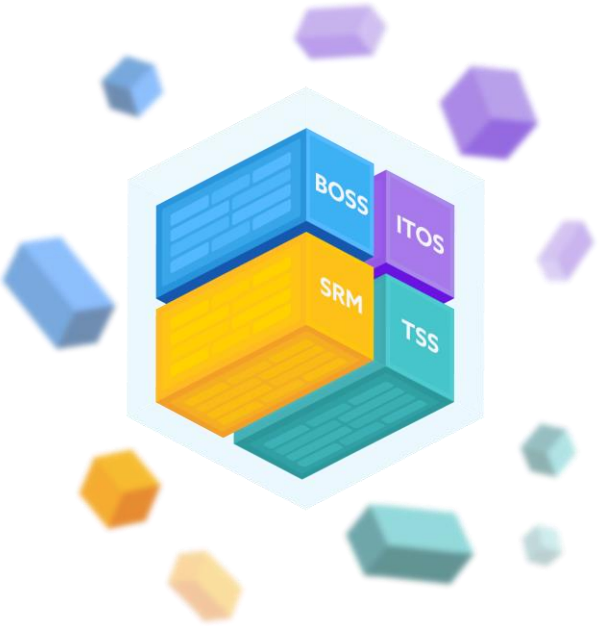


図 5: CSA エンタープライズ・アーキテクチャの構成要素

CSA は、ビジネスの推進要因を統合しながら、クラウドセキュリティへの包括的なアプローチに、最適なアーキテクチャパラダイムを組み込みます。CSA EA は、エンタープライズビジネスモデルにおけるクラウドサービスの価値提案をサポートします。

CSA EA は NIST SP 500-292 に採用され、CSA アプローチの重要性を確固たるものにしました。

1.4 クラウドセキュリティのスコープ、責任、モデル

クラウドのセキュリティとコンプライアンスには、セキュリティチームがすでに責任を負っているクラウド内におけるすべてのことが含まれています。クラウドコンピューティングにおけるリスクを効果的に軽減するために、セキュリティ要件の特定、適切なクラウドサービスの選択、コントロールの導入を反復的に行うプロセスは、*責任共有*の原則によって定義されています。この原理に基づいてモデルを記述します。CSP はインフラストラクチャのセキュリティ、CSC は導入したアプリケーションとデータを担当するというセキュリティ責任分担の概要を説明します。この責任の分離は、サービスモデル（IaaS、PaaS、SaaS）や CSP で異なっており、CSC が分担する義務を把握することの重要性を強調しています。さらに、CSA Consensus Assessments Initiative Questionnaire (CAIQ) や CSA Cloud Controls Matrix (CCM) などのフレームワークやツールが、セキュリティ標準への準拠と整合性を促進するための役割を探求します。従来のセキュリティドメインはすべて残っていますが、リスクの性質、役割と責任、コントロールの実施は頻繁かつ急速に変化します。

セキュリティとコンプライアンスの全体的なスコープは変わりませんが、特定のクラウドアクターが担当する部分は確実に変更されます。次のように考えてください。クラウドコンピューティングは、スタックの異なる部分の実装と管理を異なる組織が担当する共有技術モデルです。その結果、セキュリティの責任もスタック全体、ひいては関係する組織全体に分散されます。

これは一般にセキュリティ責任共有モデル（Shared Security Responsibility Model 、SSRM) と呼ばれ、SRM と略されることもあります。特定のクラウドプロバイダと機能/製品、サービス、および配備モデルに依存する責任マトリックスと考えてください。

1.4.1 セキュリティ責任共有モデル

クラウドコンピューティングでは、セキュリティは CSP と CSC の共同作業です。「責任共有」という用語は、複数の CSP によって広く使われており、CSP がセキュリティ運用とコントロールに責任を持つ区分を指します。境界より下は CSP の責任です。CSC が境界より上に構築したものはすべて CSC の責任です。これは、サービスモデルが変わると、大きく変わります。この SSRM モデルは、CSP がインフラストラクチャ、ハードウェア、ネットワークなど、「クラウドの(of the cloud)」セキュリティを担当することの概要を示しています。ただし、CSC はクラウドに何を展開するかという責任を持ちます。

責任の区分は IaaS、PaaS、SaaS で異なり、様々な CSP 間で異なることが多いです。CSC にとって重要なのは、自社のクラウドテナント、アプリケーション、データなどを適切に保護していることを確認するための境界を把握し、CSP に説明責任を負わせるためのベースラインを提供することです。

ハイレベルでは、セキュリティ責任は、特定のアクターがアーキテクチャスタックに対して持つコントロールの程度にマッピングされます。

- **Software as a Service:** クラウド利用者はアプリケーションへのアクセスと使用の管理のみが可能で、アプリケーションの動作を変更することはできないため、CSP がほとんどのセキュリティを担当します。CSC の責任範囲が各セキュリティドメインでより狭く限定されていても、ゼロになることはほとんどありません。 たとえば、SaaS の CSP は境界セキュリティ、ロギング/モニタリング/監査、アプリケーションセキュリティを担当しますが、CSC は依然として認可と権限の管理を担当します。
- **Platform as a Service:** CSP はプラットフォームのセキュリティを担当し、CSC は提供されるセキュリティ機能の設定方法など、プラットフォームに実装するすべてのことを担当します。したがって、責任はより均等に分割されます。たとえば、DBaaS を使用する場合、CSP は所定のサービスレベルで基本的なセキュリティ、パッチ適用、コア構成を管理します。CSC は、使用するデータベースのセキュリティ機能、アカウントの管理、さらには認証方式など、その他のすべてを担当します。
- **Infrastructure as a Service:** PaaS と同様に、CSP は基盤となるセキュリティを担当し、CSC はインフラストラクチャ上に構築するすべてのセキュリティを担当します。これは PaaS とは異なり、CSC にはるかに多くの責任を負わせます。たとえば、IaaS CSP は攻撃に関し境界を

監視する可能性が高くなりますが、サービスで利用できるツールに基づいて仮想ネットワークセキュリティを定義し実装する方法については、CSC が完全に責任を負います。

SPI スタックを下に行くにつれて、CSP の責任は減り、CSC の責任は大きくなります。IaaS はスタックの下位を押さえます。したがって、オペレーティングシステムとアプリケーションのセキュア化は利用者の責任になります。PaaS は中間に位置し、プラットフォーム内である程度のセキュリティを提供する可能性がありますが、アプリケーション内で API 呼び出しを行い、セキュアな構成を維持するためには、CSC が必要になるでしょう。SaaS は CSP がスタック全体を担当するため、少し違います。したがって、サービス内のすべての情報を保護することが CSP の負担となります。ご想像の通り、データセキュリティは SaaS 型 CSP にとって非常に重要です。なぜなら、情報漏えいや障害が発生すれば、いわゆる「取り付け騒ぎ(run on the bank)」が起こり、ビジネス全体が危険にさらされる可能性があるからです。

クラウドブローカーやその他の仲介業者やパートナーを利用する場合、これらの役割はさらに複雑になります。CSP の責任がどこで終わるのか、CSC の責任がどこから始まるのかを理解することが重要です。クラウドを活用するだけでなく、パートナーシップにおける CSC の役割を認識することで、クラウドをセキュアに活用することができます。CSC は、セキュリティポリシー/対策が組織内で使用中のデータやリソースの機密性と一致していることを確保するために、特に構成と管理における義務を定期的に確認し、理解する必要があります。

次の図は SSRM を示しており、異なるサービスモデル間での CSP と CSC の責任分担を強調しています。このモデルは、各アクターがアーキテクチャスタックに対して持つさまざまなコントロールと責任の度合いを強調します。

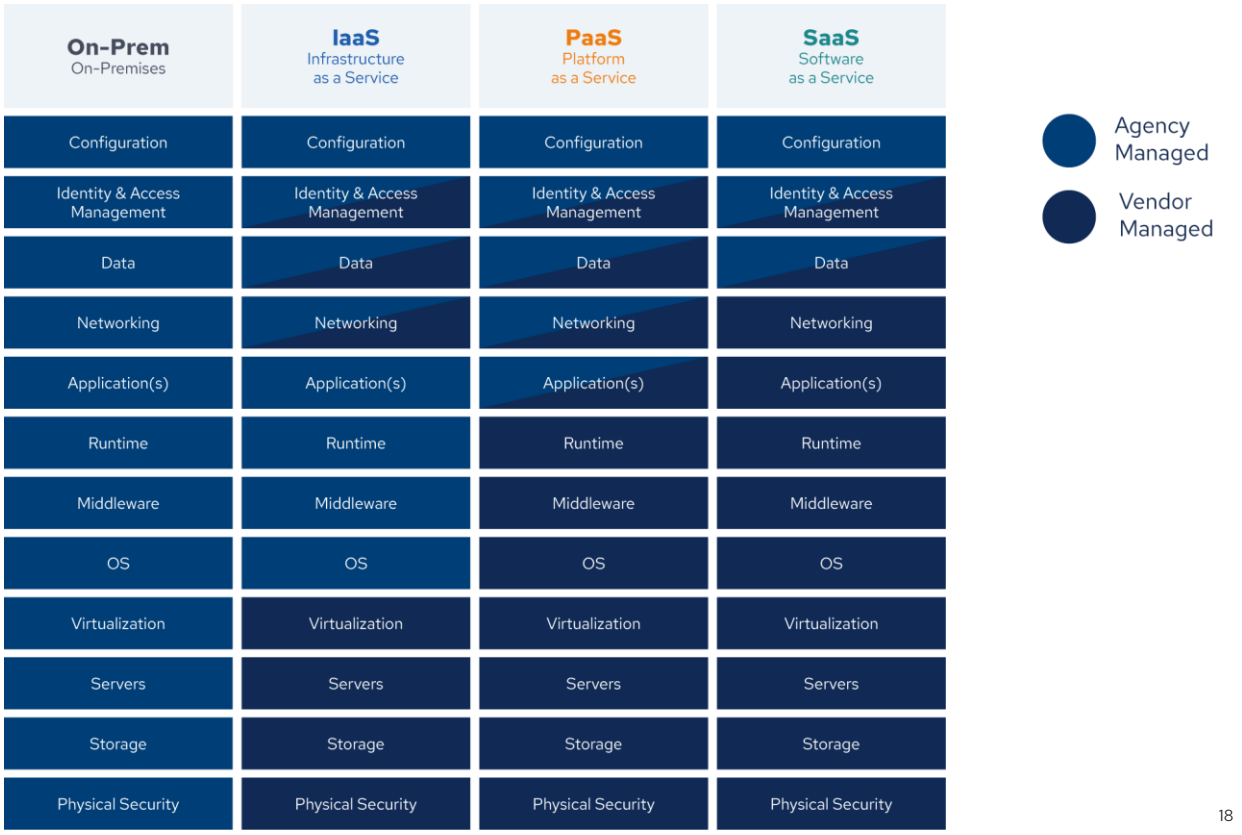


図 6: セキュリティの責任共有モデル

効果的なクラウドセキュリティの鍵は、あらゆるクラウドプロジェクトにおける責任分担を理解することです。 CSP が提供する特定のセキュリティコントロールに関係なく、誰が何に対して責任を負っているかを正確に把握することが重要です。 この理解により、組織はコントロールギャップを対策で埋めることや、代替 CSP を検討できます。セキュリティを直接コントロールするユーザーの力は IaaS では非常に高く、SaaS ではそれほど高くありません。

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います。

- **CSP** は、内部セキュリティコントロールと CSC の機能を徹底的に文書化し、十分な情報に基づいた意思決定ができるようにすべきです。また、CSP はそれらのコントロールを適切に設計し、実装する必要があります。
- **CSC** は、セキュリティ責任の役割と責任のマトリックスを構築する必要があります。このマトリックスは、特定のセキュリティコントロールを実装する責任者を文書化し、関連するコンプライアンス基準との整合性を確保する必要があります。

CSA は、次の要件を満たすのに役立つツールを提供しています。

[18] CISA. (2021) Cloud Security Technical Reference Architecture

- CAIQ は、CSP がセキュリティとコンプライアンスのコントロールを文書化するための標準テンプレートです。
- CCM はクラウドのセキュリティコントロールをリストし、複数のセキュリティおよびコンプライアンス標準にマッピングします。CCM は、セキュリティ責任を文書化するためにも使用できます。

どちらのドキュメントも、特定の組織要件やプロジェクト要件に合わせて調整する必要がありますが、開始時の包括的なテンプレートを提供し、コンプライアンス要件が満たされていることを確認するために特に役立ちます。

SSRM に関するその他のリソースとガイダンスは次のとおりです。

- CSA エンタープライズアーキテクチャー ～ このフレームワークは、セキュアなクラウドインフラストラクチャのアーキテクチャに向けた包括的なアプローチを提供します。CSA EA については、上記のセクションを参照してください。
- エンタープライズアーキテクチャから CCM 責任共有モデル ～ このマッピングは、ユーザーがクラウドのセキュリティ責任を理解するのに役立ちます。さまざまなサービスモデル（IaaS、PaaS、SaaS）について、CSP または CSC が責任を持つセキュリティコントロール（CCM ごと）を示します。
- CCM 実装ガイドライン ～ CCM に関連するものとして、CSP および CSC のコントロール所有権と実装ガイドラインです。

1.4.2 クラウドセキュリティフレームワークとパターン

クラウドのセキュリティフレームワークとパターンは、セキュリティに関する意思決定の指針となるツールです。「モデル」という用語は、やや不明瞭な場合があるため、次のタイプに分けて説明します。

- **概念モデル**または*フレームワーク*には、本書の NIST モデルなど、クラウドセキュリティの概念と原則を説明するために使用される視覚化と説明が含まれます。
- **コントロールモデル**またはフレームワークは、CSA CCM などの特定のクラウドセキュリティコントロールまたはコントロールのカテゴリを分類して詳述します。
- **リファレンスアーキテクチャ**は、クラウドセキュリティを実装するためのテンプレートであり、通常は一般化されています（IaaS セキュリティリファレンスアーキテクチャなど）。非常に抽象的で概念的なものから、特定のコントロールや機能に至るまで、かなり詳細なものまであります。
- **デザインパターン**は、特定の問題に対して再利用可能なソリューションです。セキュリティでは IaaS のログ管理がその一例です。リファレンスアーキテクチャと同様に、特定のクラウドプラットフォームでの一般的な実装パターンに至るまで、多かれ少なかれ抽象的であったり、具体的であったりします。

これらのモデルの境界線は、モデル開発者の目標によって曖昧になったり、重なったりすることがよくあります。「モデル」という見出しでこれらをグループ化することさえおそらく不正確ですが、さまざまなソース間でこの用語が同じような意味で使用されているのを目にすることから、グループ化することは理にかなっています。

CSA では、次のモデルを推奨しています。

- The CSA EA[19]
- The CSA CCM[20]
- ISO/IEC CD 27017.2[21]

1.4.2.1 シンプルなクラウドセキュリティプロセスモデル

実装の詳細、必要なコントロール、特定のプロセス、さまざまなリファレンスアーキテクチャや設計モデルは、個別のクラウド実装によって大きく異なりますが、クラウドセキュリティを管理するための比較的単純で高いレベルのプロセスがあります。

- 必要なセキュリティ要件とコンプライアンス要件、および既存のコントロールの特定
- CSP、サービスモデル、配備モデルの選択
- アーキテクチャの定義
- セキュリティコントロールの評価
- コントロールギャップの特定
- ギャップを埋めるコントロールの設計と実装
- コントロールの有効性を評価
- 時間の経過に伴う変更を管理

各クラウドプロジェクトは、同じ CSP 内であっても、固有の構成と技術を必要とする場合があります。したがって、各プロジェクトの具体的な要件や特性の評価が重要です。たとえば、1 つの CSP で純粋な IaaS にデプロイされたアプリケーションのセキュリティコントロールは、同じプロバイダの PaaS を多く使用する同様のプロジェクトとは大きく異なって見えることがあります。

重要なのは、要件を特定し、アーキテクチャを設計してから、基盤となるクラウドプラットフォームの機能に基づいてギャップを特定することです。そのため、セキュリティ要件を満たすためのコントロールを実装する前に、CSP とアーキテクチャを理解することが不可欠です。

これは通常、反復プロセスです。ネイティブクラウドサービスコントロールを使用するタイミングと、ギャップを埋めるためにコントロールを外部で実装するタイミングを理解することは、セキュリティアーキテクチャ全体に大きな影響を与える可能性がある重要な考慮事項です。

---

[19] CSA. (2024) Enterprise Architecture Working Group - Enterprise Architecture

[20] CSA. (2024) Cloud Controls Matrix

[21] ISO. (2024) Information Technology - Security Techniques - Code of Practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services. This draft is under development and is meant to replace ISO/IEC 27017:2015.

概要と重点分野 ～ ガバナンスとオペレーション

CSA セキュリティガイダンスの残りの部分を構成するその他の11 のドメインは、クラウドコンピューティングの懸念領域を強調し、クラウド環境における戦略的および戦術的なセキュリティの「ペインポイント」の両方に対応するように調整されており、クラウドサービスと配備モデルのあらゆる組み合わせに適用することができます。

ドメインはガバナンスとオペレーションの2 つに大別されます。ガバナンスのドメインは幅広く、クラウドコンピューティング環境における戦略やポリシーの課題を扱います。一方、オペレーションのドメインは、より戦術的なセキュリティの懸念やアーキテクチャ内での実装に焦点を当てます。

タイトル	説明
クラウドコンピューティングの概念とアーキテクチャ	クラウドセキュリティの専門家向けに、クラウドコンピューティングの概念とアーキテクチャについて説明します。クラウドモデル、セキュリティフレームワーク、クラウドネイティブ機能、抽象化、オーケストレーション、およびマルチテナント、また、俊敏性、レジリエンス、およびセキュリティの重要性をトピックに含みます。
クラウドガバナンス	DevOps、DevSecOps、ゼロトラスト、AI/ML などの戦略を取り上げ、セキュリティに焦点を当てたクラウドガバナンスを学びます。フレームワーク、リスク管理、コンプライアンスを理解し、CCoE やクラウドレジストリなどの効果的なガバナンス構造を確立します。
リスク、監査、コンプライアンス	クラウド環境におけるリスク管理、監査プロセス、およびコンプライアンスをカバーします。クラウドのリスク評価、コンプライアンス要件、法律、および監査プロセスを学習します。コンプライアンス継承と、規制基準への CSP コンプライアンスの活用をトピックに含みます。
組織運営	組織階層、IAM、ハイブリッド/マルチクラウドセキュリティ、およびゼロトラスト戦略を中心に、主要な CSP によるクラウド環境の管理とセキュア化をカバーします。一貫性のあるセキュリティコントロールを実装し、多様なクラウドインフラストラクチャを管理する方法を学びます。
アイデンティティとアクセスの管理	フェデレーション、強固な認証および認可に焦点を当て、クラウド環境における IAM（Identity and Access Management）をカバーします。クラウドのセキュリティとコンプライアンスを強化する高度な IAM モデル、ゼロトラスト戦略、自動化について学びます。
セキュリティモニタリング	クラウドテレメトリ、ログ、ハイブリッド/マルチクラウドのセットアップ、高度なモニタリングツールなど、クラウドセキュリティ監視の課題

	とソリューションをカバーします。SSRM、ログストレージ、カナリア、ハニートークン、クラウドセキュリティ強化における生成 AI の役割などのトピックを取り上げます。
インフラストラクチャとネットワーキング	セキュアなアーキテクチャ設計、SDN、IaC、セキュアなクラウド接続など、クラウドインフラストラクチャの管理とセキュア化をカバーします。ゼロトラスト、SASE、コンテナセキュリティ、クラウド資産を保護するための統合セキュリティ対策を強調しています。
クラウドワークロードセキュリティ	VM、コンテナ、サーバーレス機能、PaaS、AI などのクラウドワークロードのセキュア化をカバーします。VM イメージのセキュア化、コンテナの脆弱性の管理、暗号化、アクセスコントロール、ランタイム保護、および IAM のベストプラクティスの実装について説明します。
データセキュリティ	データ分類、暗号化、アクセスコントロール、さまざまなクラウドストレージタイプを中心に、クラウド環境におけるデータセキュリティをカバーします。AI システムのセキュリティや将来のデータセキュリティ技術とともに、保存中のデータ、移動中のデータ、使用中のデータのセキュア化に対応します。
アプリケーションセキュリティ	外部の脅威からアプリを保護することを中心に、クラウドアプリケーションのセキュリティについて説明します。SDLC、脅威モデリング、セキュアコーディング、およびテストについて説明します。トピックには、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が含まれます。
インシデントレスポンスとレジリエンス	組織のセキュリティに不可欠なクラウド環境におけるインシデント対応とレジリエンスをカバーします。CSA と NIST のガイドラインに基づいた CIR 戦略、ツール、プラクティスを学習します。トピックには、準備、検出、封じ込め、回復、レジリエンス戦略が含まれます。
関連技術と戦略	ゼロトラスト、AI 統合、脅威と脆弱性の管理を中心に、クラウドセキュリティ戦略をカバーします。多要素認証、暗号化、AI 脅威検出、および継続的なモニタリングを通じて、クラウドアプリケーション、システム、およびデータのセキュア化を確保する方法を学びます。

テーブル 1: セキュリティガイダンスドメインの一覧

推奨

- クラウドコンピューティングの違いと、抽象化とオーケストレーションがセキュリティにどのような影響を与えるかを理解します。

- クラウドコンピューティングの NIST モデルと CSA リファレンスアーキテクチャに精通します。
- SSRM ツールを使用して、CSC と CSP の間にセキュリティに対する責任と説明責任/義務を割り当てて、配置します。
- CSA CAIQ のようなツールやドキュメントを使用して、クラウドプロバイダの評価と比較を行います。
- クラウドプロバイダは、自社のセキュリティコントロールと機能を文書化し、CSA CAIQ のようなツールを使用して公開する必要があります。
- CSA CCM のようなツールを使用して、クラウドプロジェクトのセキュリティとコンプライアンスの要件とコントロール、およびそれぞれの責任者を評価し、文書化します。
- クラウドセキュリティプロセスモデルを使用して、プロバイダの選定、アーキテクチャの設計、コントロールギャップの特定、セキュリティおよびコンプライアンスコントロールの実装を行います。

追加のガイダンス

- CCSK PrepKit | CSA
- Cloud Security Alliance Glossary | CSA
- CSA Cloud Controls Matrix (CCM) | CSA
- CCM-Lite and CAIQ-Lite | CSA
- CCM v4 Implementation Guidelines | CSA
- CSA Enterprise Architecture Reference Guide | CSA
- Enterprise Architecture to CCM Shared Responsibility Model | CSA

ドメイン 2: クラウドガバナンスと戦略

このドメインは、セキュリティの役割を重視したクラウドガバナンスに焦点を置いています。ガバナンスは、定義された基準に対する透明性と説明責任を促進するように設計されたポリシー、手順、およびコントロールのフレームワークに基づいています。 強固なガバナンスプラクティスは、戦略的ガイダンス、リスク管理と軽減、コンプライアンスの監視と改善、予算割り当て、およびコストコントロールに対応します。 IT ガバナンスは、情報と関連する技術が企業戦略をサポートし、企業目標の達成を確かにします。

ISACA[22]では、ガバナンスを以下のように定義しています：「*企業がステークホルダーのニーズ、条件、オプションを評価し、達成すべきバランスの取れた合意された企業目標を決定する方法。優先順位付け、意思決定、合意された方向性と目的に対するパフォーマンスとコンプライアンスの監視を通じて方向性を定めることが含まれます*」

組織は、さまざまな業界固有のガバナンス基準やフレームワーク[23]に倣って、ガバナンスプラクティスを強化できます。たとえば、ISO/IEC 38500:2024 規格は、組織の IT ガバナンスに関するガイダンスを提供します。ISACA COBIT フレームワークは、企業 IT のガバナンスと管理のための包括的なガイドを提供します。

ガバナンス基準の詳細については下記のものがあります。

- ISO/IEC 38500:2024 - Information Technology - Governance of IT for the Organization
- ISACA - COBIT - A Business Framework for the Governance and Management of Enterprise IT
- ISO/IEC 27014:2020 - Information Technology - Security Techniques - Governance of Information Security
- The Open Group Cloud Computing Governance Framework

IT ガバナンス要件に影響を与える法規制の例をいくつか紹介します。

- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- The Health Insurance Portability and Accountability Act (HIPAA)

[22] ISACA. (2024) Glossary - Governance

[23] Frameworks are discussed in detail in *2.3 The Governance Hierarchy*

- General Data Protection Regulation (GDPR)

学習目標

このドメインでは、次のことを学びます。

- クラウドガバナンスの目的を明確にします。
- クラウドガバナンスにおけるガバナンス階層を定義します。
- クラウドコンピューティングにおけるガバナンスに影響を与える主要な戦略と概念について説明します。

2.1 クラウドガバナンス

クラウドコンピューティングのマルチテナンシー、責任の共有、機微データの再配置、重要なアプリケーションやインフラストラクチャのホスティング、セキュリティ、およびプライバシーに関する懸念事項は、管理のための効果的なガバナンスを要求します。

クラウドにデータを保存する場合、さまざまな規制、裁判管轄、セキュリティ、およびプライバシーの要件があるため、コンプライアンスも大きな懸念事項です。適切なガバナンスアプローチがなければ、クラウド運用に関連するセキュリティ、財務、および運用上のリスクが指数関数的に増大し、クラウドが企業にとって無意味な選択肢となりかねません。

クラウド導入の主な推進要因の1つは、コスト効率と市場投入までのスピードです。多くの組織は、クラウドコンピューティングを、資産を持ったデータセンターモデルから経費モデル（従量課金制やサブスクリプション制など）へ移行することによるコスト削減の手段と認識しています。その結果、既存のアプリケーションやインフラストラクチャをクラウドに「リフト＆シフト」することが、一般的な移行戦略となります。セキュリティとプライバシーのガバナンスは、このような移行において非常に重要です。新しいテクノロジープラットフォームへの移行は、たとえ（そして特に）アーキテクチャが変わらない場合でも、新たな技術的リスクをもたらす可能性があるためです。さらに現在では、当該のアプリケーションは、関係する CSP（クラウドサービスプロバイダ）と責任共有されます。

戦略的イノベーションもクラウド導入の大きな推進要因の 1 つです。多くの組織は、ソフトウェアを競争優位性をもたらす戦略的な資産と見なしています。クラウドは、ソフトウェアを迅速に開発および配備できる機能を提供し、組織が新しい製品やサービスを迅速に市場に投入できるようにします。しかし、ガバナンスの観点からは、迅速な配備による急激な変更を管理することは、設定ミスやソフトウェアサプライチェーンの危険などのリスクをもたらします。クラウドでのソフトウェア開発、テスト、デプロイがセキュアで信頼できるものであることを保証するには、堅牢なセキュアバイデザインプロセスが不可欠です。

このディスカッションの要点は、次のとおりです。

- クラウドの導入は、コスト削減、経費コストモデル、組織の目的、戦略的イノベーションの達成意欲などの要因によって促進されます。
- クラウド導入におけるガバナンスの考慮事項には、情報リスク（データ、アプリケーション、ホストオペレーティング システム、ネットワーク、サプライチェーン）と物理リスクを許容レベル（リスク選好と呼ばれる）まで管理することが含まれます。これは、IT 目標がビジネス目標に沿っているかを評価し、プライバシー義務を含む法規制要件の遵守を確実にすることで実施されます。
- 組織は、適切なクラウドサービスを選択し適切なガバナンス対策を実施するなど、特定のビジネス目標に合わせて移行戦略を調整する必要があります。

2.1.1 クラウドの導入とガバナンス

クラウドがセキュリティガバナンスに影響を与える主な道筋は 2 つあります。

1. 責任共有モデル（SRM）（訳注：原文は Mode となっているが Model の間違いと考える）の導入。セキュリティガバナンスの責任は、CSP と CSC の間で分担されるようになりました。さらに厄介なことに、それぞれが独自のセキュリティリスクを抱えているサードパーティのサービスプロバイダがサプライチェーンに取り入れられるケースもあります。そうしたサードパーティに責任の一部が委ねられるとしても、CSP か CSC のどちらかに説明責任が残ります。
2. クラウドコンピューティングの本質的な性質が生み出す技術的および運用上の相違点。

クラウドが登場する以前は、IT セキュリティガバナンスは、主にデータセンター内で運用するという固有の性質に大きく依存していました。限られたスペース、コンピュータ、ネットワークなどデータセンターには限定されたリソースしか存在せず、比較的隔離された物理環境です。組織の構造、ポリシー、コントロールは、これら施設のリソース不足に基づいてすべて調整されています。

パブリッククラウドはその逆です。クラウドプロバイダには容量が無限にあるわけではありませんが、顧客の要件に合わせて常に十分な容量を確保することがクラウドプロバイダの利益になります。クラウドは分散化されており、さまざまなチームがリソースのスタック全体をプロビジョニングができます。パブリッククラウドのいずれも、効果的なガバナンスコントロールがなければ、いかなる種類の集中管理の下にも置くことができません。

クラウドはまた、それらのリソースの管理方法を根本的に変えます。リソースを分散させることができますが、パブリッククラウドでは、コアの管理と管理用インターフェースが統合され、インターネットに開放されます。物理的なネットワーク境界はなく、適切なクレデンシャルがあれば誰でもマネージメントプレーンにアクセスし、仮想インフラストラクチャ全体を再構築できます。分散型の利用と、インターネットに開放された統合マネージメントプレーンとの組み合わせには、クラウド固有の新しいガバナンスアプローチが要求されます。

結論として、クラウドはインフラストラクチャ管理の分散化、統一された管理アクセスの提供、リソースへのアクセスを可能にすることで、IT ガバナンスに革命をもたらします。組織は、クラウドコンピュ

ーティングのメリットを最大限に活用するために、セキュリティとコントロールを確保しながら、これらの変化を受け入れる必要があります。

2.1.2 クラウドガバナンスの複雑さ

クラウドサービスの導入が進むにつれ、新しいビジネスモデル、技術、および管理アプローチに起因する固有のガバナンスの課題に直面しています。こうした課題に対応するため、組織はクラウド環境に合わせてガバナンスフレームワークを更新する必要があります。Paas、SaaS、IaaS に共通する考慮事項には、コントロールと説明責任、法令遵守、CSP とクラウドサービス利用者（CSC）の関係などがあります。

このセクションでは、課題と、クラウド環境を効率的に管理するために必要なガバナンスの調整に焦点を当てて、これらの考慮事項を列挙します。

次の考慮事項は、組織がクラウド環境を管理する際に対処する必要がある主要なガバナンスの課題と必要な調整の概要を示しています。

コントロールと説明責任

- クラウドは IT インフラストラクチャを直接コントロールできなくなる可能性があり、組織は新しいガバナンスフレームワークとプロセスの採用を余儀なくされます。
- クラウドソリューションを使用するということは、コントロールの説明責任を第三者や第四者に委託することを、必ずしも意味しません。
- クラウドは、様々な CSP や技術スタックに応じた、多数の異なる SRM を使用します。そうなると、クラウドサービスプロバイダと利用者との間でコントロールと責任を明確に割り当てる必要があります。
- CSC は実際にテストすることよりも評価作業に頼らざるを得ません。

法令等へのコンプライアンス

- クラウドサービスやデータは複数の裁判管轄にまたがっている可能性があり、特にプライバシーの面で、より多くの法規制を遵守することを利用者に強います。
- データの所有権や分類、プライバシー管理はくっきりと明確ではなく、慎重な検討が必要な場合があります。

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 には、CSC 固有の要件に応じてカスタマイズできない標準サービスがある場合があります。
- CSP は、すべてに対応可能な画一的なクラウドポリシーの導入を困難にする、異なる成熟度、多様なサービス、ライセンス、モデルを示す可能性があります。

ガバナンスの複雑さ

- クラウドサービスは、多くの場合、CSP の連鎖の上に構築されるため、ガバナンス活動のスコーピングが困難になります(別の IaaS プロバイダのインフラストラクチャで実行されている SaaS プロバイダなど)。
- CSP と CSC の責任範囲に明確な境界を設定することが複雑であるため、ハイブリッドクラウドモデルは、ガバナンスが複雑になる可能性があります。

CSP と CSC のダイナミクス

- CSP は急速に変化する可能性があり、ガバナンスモデルではこれを考慮しなければなりません。
- クラウドサービスの利用には、クラウド監査スキルやクラウドセキュリティスキル、クラウド指向のセキュリティツールに関する知識など、現在 CSC が有していない追加のスキルが必要となる場合があります。

次の図は、さまざまなクラウドサービスモデルに関連する特定の複雑さの概要を示し、各モデルに固有のガバナンスの課題と責任を強調しています。

図7: サービスモデル固有の複雑さ

効果的なクラウドガバナンスには、IaaS、PaaS、SaaS モデル固有の課題に対処するための柔軟で堅牢な戦略が必要です。これらの複雑さを把握して管理することで、組織はクラウド環境のセキュリティ、コンプライアンス、および業務効率化を確保できます。

2.1.2.1 クラウドガバナンスの複雑さ: 配備モデル

さまざまなクラウド配備モデルに関連するガバナンスの複雑さを考慮することも不可欠です。次のセクションでは、これらの配備モデルについて検討し、それぞれに固有のガバナンスの課題と責任に焦点を当てます。

図 8: 配備モデル固有の複雑さ

パブリッククラウド: パブリッククラウドは最も一般的なクラウド配備モデルで、すべての利用者に標準サービスを提供します。プロバイダは通常、カスタマイズ要求を受け入れず、彼ら独自のインフラストラクチャ、サービス、および従業員を彼らが管理するため、ガバナンスが複雑になります。ガバナンスの課題は、初期および時間の経過とともに、利用者の構成から生じます。

パブリッククラウドはマルチテナンシーに依存しており、セグメンテーションや隔離などのガバナンスの課題をもたらします。これにより、セキュリティスキャンや侵入テストなどのアクションが制限され、インフラストラクチャ可視性が低下することがよくあります。これらの課題には、ベンダーのリスク管理、SLA（Service Level Agreement）、第三者による監査、およびコンプライアンスレポートを使

用した新しいガバナンスアプローチが必要です。この新しいアプローチの有効性は、クラウドコンピューティングがもたらす固有のリスクを軽減するという、クラウド利用者の能力に基づいて判断されます。

プライベートクラウド: プライベートクラウドは、組織またはサードパーティが所有、管理、またはホストできます。セルフマネージドプライベートクラウドのガバナンスは、従来の IT ガバナンスと似ていますが、攻撃ベクトル、マルチテナンシー、および自動化などのクラウド固有の課題にも対処する必要があります。サードパーティが管理するプライベートクラウドのガバナンスは、すでに知られている従来のアウトソーシングモデルに最も近いものです。ガバナンスの課題には、責任共有マトリックスの理解、SLA の設定、ポリシー違反や内部脅威を追跡するサードパーティの監視機能の構築などがあります。プラットフォームを最新のサービスに更新し続けることが大きな課題であり、特に注意が必要です。

ハイブリッドクラウド: ハイブリッドクラウドサービスは、プライベートクラウドモデルとパブリッククラウドモデルを組み合わせたサービスです。実装方法はさまざまで、ポリシーガイドラインや SRM が複雑になります。ガバナンスの課題には、プロバイダと利用者間の SLA と責任の調整、内部境界の保護、セキュリティ構成の拡張、およびクラウドのセキュリティと成熟度のスキルギャップへの対応などがあります。

コミュニティクラウド: コミュニティクラウドとは、サードパーティが管理およびホストする一連のサービスを指します。複数の組織で共有されますが、完全にパブリックではないため、マルチテナンシーの課題が軽減されます。ガバナンスの課題には、ステークホルダーの特定、正しい SRM の構築、および同じコミュニティクラウドを使用している組織間の関係とリスクの重視などがあります。

2.2 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、クラウドリソースの効果的であり、セキュアでコンプライアンスを遵守した使用を確実にするための堅牢なフレームワークと一連のポリシーの確立が含まれます。クラウドリソースをセキュアに、コンプライアンスを遵守し、かつ効率的に管理するための強固なコントロールフレームワークとポリシーの実装が必要です。 これには以下が含まれます。

- 役割と責任の定義
- Cloud Center of Excellence（CCoE）またはそれに類似する組織の設立
- 要件収集の実施
- リスクベースのプランニング
- リスクと改善策の管理
- データとデジタル資産の分類
- 法規制要件への対応
- クラウドレジストリの維持[24]

[24] Additional details provided later in this section - *Domain 2: Cloud Governance*.

- ガバナンス階層[25]の構築
- クラウド固有のセキュリティフレームワークの活用
- クラウドセキュリティポリシーの定義
- コントロール目標の設定とコントロール仕様の指定

これらのコンポーネントを実装することで、組織は潜在的なリスクを軽減しながら、クラウドコンピューティングのメリットを最大化できます。 以下では、効果的なクラウドガバナンスの主要なコンポーネントについて説明します。

2.2.1 クラウドガバナンスの実装モデル

Cloud Center of Excellence（CCoE）と Cloud Advisory Council（CAC）モデルは、効果的なクラウドガバナンスを実装するためのアプローチとして広く採用されています。CCoE には作業メンバーとエバンジェリストが含まれます。CAC は経営層のスポンサーシップと承認を提供します。具体的には以下になります。

- CCoE は、クラウドの導入と使用に関するガイダンス、ベストプラクティス、およびサポートを組織の他の部分に提供する、一元化されたチームまたは部門です。CCoE は、CSC の目標や目的との一貫性、標準化、および整合性の確保に役立ちます。
- CAC には、CSC のクラウド戦略と運用計画のビジョンと方向性の設定を担当する、IT、リスク管理、コンプライアンス、セキュリティ、および一般的なビジネス部門のシニアリーダーのグループを含めることができます。CAC については、ここでは詳しく説明しませんが、注意することが重要です。

CCoE と CAC は、CSC 内の IT ガバナンスとセキュリティの推奨コンポーネントです。中央集中型のハブとして機能し、クラウドイニシアチブを主導し、戦略的、セキュア、コンプライアンス、および効果的なクラウド導入を推進します。すべての CSC が同じ用語を使用するわけではありませんが、機能的な観点から、これらの実装モデルは効果的なクラウドガバナンスのために必要とされる重要な要素に焦点を当てています。

2.2.1.1 Cloud Center of Excellence

CCoE の主要な機能の 1 つは、戦略的なガイダンスを提供することです。クラウドのイニシアチブが CSC の全体的なビジネス目標に沿っていることを確実にします。そうすることで、CCoE はクラウド導入が CSC の方向性をサポートし、成功への貢献を確実にします。

CCoE は、クラウド利用のためのガバナンスフレームワークの開発と実施も行います。これには、外部の規制や内部のベストプラクティスに準拠したポリシーや標準の作成が含まれます。CCoE は、クラウド

[25] Additional details provided later in this section - *Domain 2: Cloud Governance*.

環境におけるリスクの管理、データのプライバシーとセキュリティの確保、およびコンプライアンスの維持を担当します。

CCoE は、クラウド技術やセキュリティ対策に関する知識を発信します。トレーニングの機会とリソースを他の部門に提供し、組織全体で一貫したレベルのクラウド習熟を促進します。これにより、従業員はクラウドサービスを効果的かつセキュアに活用するために必要なスキルと知識を習得できます。

その責任の中でも、CCoE の主な焦点はセキュリティです。CCoE は、率先してクラウドインフラストラクチャにセキュリティを組み込み、クラウド導入が設計上セキュアであることを確実にします。CCoE は、CSC のセキュリティ要件とプライバシー要件を確実に満たし、進化する脅威の状況に対応します。

CCoE は、IT、セキュリティ、コンプライアンス、および財務など、さまざまな部門が関与する部門横断的なコラボレーションを促進します。このコラボレーションアプローチにより、コスト、セキュリティ、コンプライアンス、およびビジネスニーズを考慮して、クラウドに関する意思決定が総合的に行われることを確実にします。

また、CCoE は革新性と適応性を育みます。新しいクラウドサービスや技術の探求を奨励し、組織内のイノベーションの文化を促進します。同時に、CCoE は、技術やビジネス環境の変化に適応し続け、 CSC がクラウド技術の最新の進化を効果的に活用できるようにします。

究極的には、CCoE は、クラウド技術を効果的かつセキュアに活用しようとする CSC にとって有用です。CCoE は、技術の枠を超え、クラウド環境におけるガバナンス、セキュリティ、およびコンプライアンスを確保しながら、クラウドの採用とビジネス戦略を整合することに重点を置いています。次の図は、CCoE 内の主要な役割を示しています。

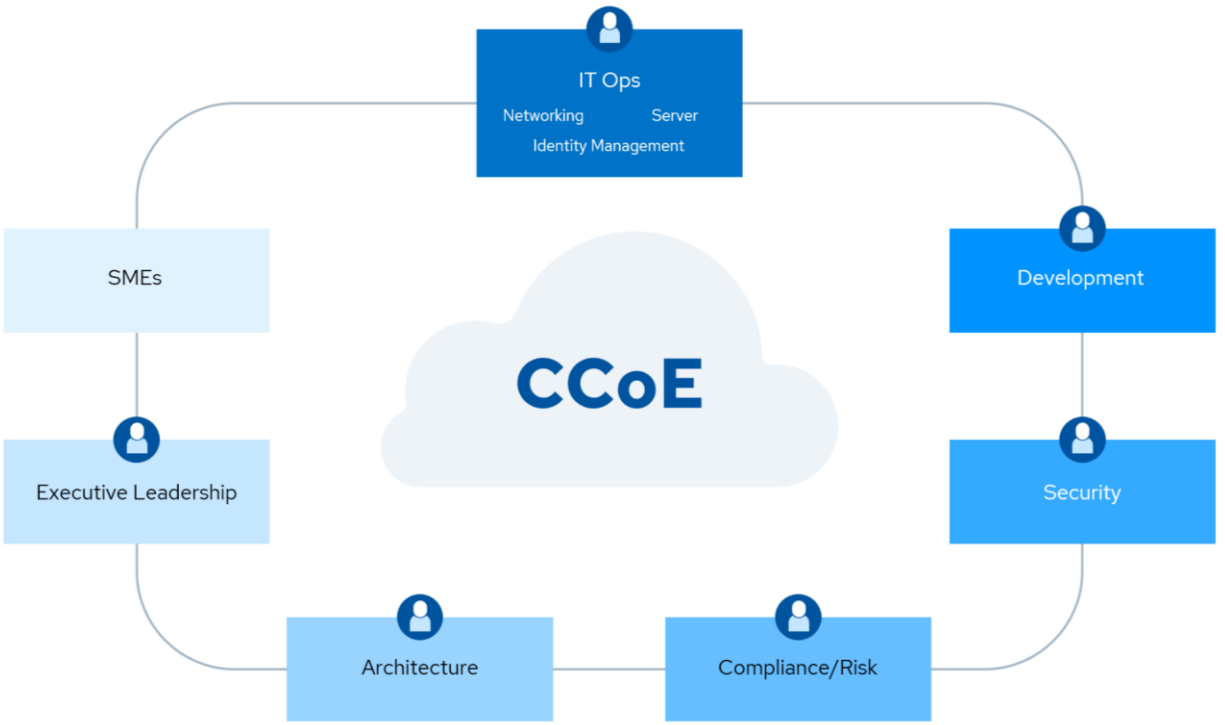


図 9: CCoE の主な役割

2.2.2 セキュリティチャンピオン

CSC は CCoE を設置するだけでなく、コンプライアンス、エンタープライズリスク、法務、人事、財務、IT などのビジネスユニット内にセキュリティチャンピオンを任命できます。セキュリティチャンピオンは、クラウドセキュリティの重要性を理解し、そのためセキュリティの提唱者として行動し、セキュリティのベストプラクティスとコントロールの導入を促進することができる人材です。

セキュリティチャンピオンはチーム内から任命され、実践的な役割を持つ必要があります。セキュリティチャンピオンは通常はセキュリティ組織のメンバーではなく、自身が所属するチームのメンバーです。この区別は、セキュリティチャンピオンを、特定のチームダイナミクスの中で実用的なセキュリティの実装に集中させることができます。セキュリティチャンピオンの役割を、ビジネス情報セキュリティ責任者（BISO）、最高情報セキュリティ責任者（CISO）、情報セキュリティ責任者（ISO）と区別することは不可欠です。

たとえば、DevOps チームでは、セキュリティチャンピオンの役割に理想的な候補者は、通常、開発者、システム管理者、またはすでにチームの一員である DevOps やプラットフォームエンジニアです。チームのダイナミクスと技術的なスキルに精通していることは、彼らが、内側から効果的にセキュリティを擁護できるようにします。彼らは、クラウドサービスと DevOps プラクティスにおける具体的なセキュリティの課題とソリューションを理解するための知識と専門知識を備えています。
セキュリティチャンピオンの役割は、DevSecOps プロセス内のセキュリティプラクティスの統合において非常に重要です。セキュリティチームと開発チームの連絡役となり、彼らは、責任の分散化において重要な役割を担っています。セキュリティチャンピオンは、チーム内でセキュリティを提唱することで、クラウドチームと DevOps/SRE（サイト信頼性エンジニアリング）チーム内のセキュリティ文化を促進します。セキュリティチャンピオンは、開発関連のチームではより一般的ですが、他のビジネスユニットでも重要な役割を果たすことができます。
セキュリティチャンピオンのスキルと関心を育むためには、魅力的でインタラクティブなセキュリティトレーニングを提供することが重要です。例えば、ホワイトハッカーに関するワークショップは、彼らの実践的なセキュリティスキルを高める効果的な方法となりえます。ただし、セキュリティチャンピオンをフルタイムのセキュリティ専門家に育てようとしないことが重要です。セキュリティチャンピオンは、チーム内の連絡役や専門家として、追加のセキュリティトレーニングを受ける開発者や管理者です。

セキュリティチャンピオンに権限を与えることの目的は、専任のセキュリティチームの方がより良いサービスを提供できる追加の職務を彼らに負担させるのではなく、アドバイザリとしての役割を果たすことができるようにすることです。燃え尽きないことが重要です。CSC は、セキュリティチャンピオンを強化することで、セキュリティと開発のギャップを効果的に埋め、クラウドチームと DevOps チーム内でセキュリティの文化を醸成することができます。

まとめると、セキュリティチャンピオンは、クラウド、DevOps チーム、およびビジネスチーム内でセキュリティ文化を促進する上で不可欠です。セキュリティチャンピオンに、経験、トレーニング、権限

を適切に組み合わせて与えることで、CSC は、セキュリティプラクティスを開発プロセス内に効果的に統合できます。これは最終的にセキュリティ上の成果の向上につながります。

2.3 ガバナンスの階層

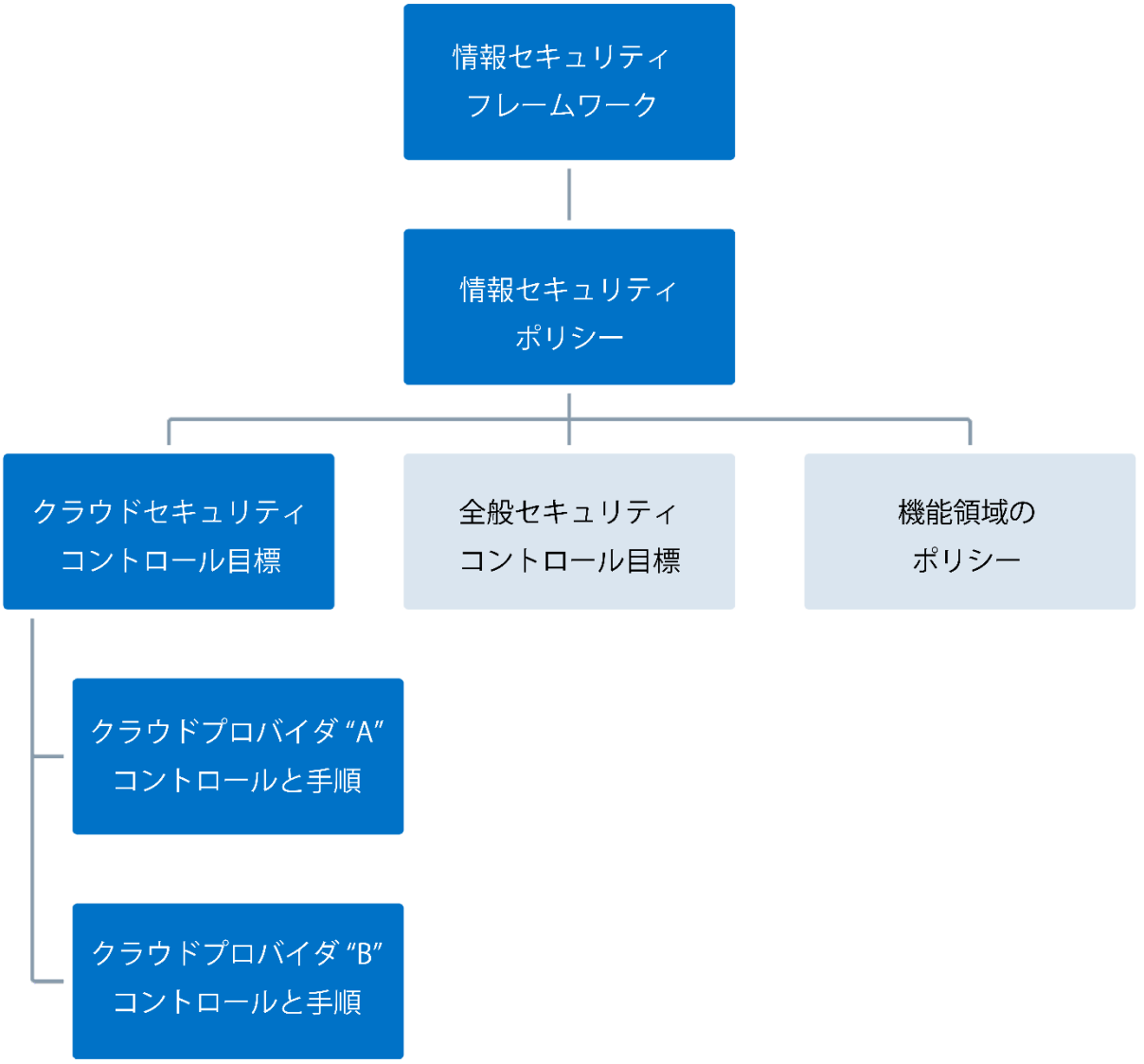
クラウドガバナンスの重要な側面は、**ガバナンス階層**の確立です。これには、クラウド関連の課題に対する意思決定プロセスとエスカレーションパスの定義が含まれます。ガバナンス階層により、CSC 内の適切なレベルで意思決定が行われることや、説明責任と責任の明確な線引きがされることを確実にします。CSC はクラウド固有のセキュリティフレームワークを活用して、クラウドガバナンスの取り組みを導くことができます。

情報セキュリティにおけるガバナンス階層は、組織のシステムやデータのセキュリティを確保するための構造化されたアプローチです。この階層の最上位には、サイバーセキュリティの実践に関する一連のガイドラインを提供する**フレームワーク**があります。フレームワークの例としては、NIST Cybersecurity Framework (CSF)、 Cloud Controls Matrix (CCM)、 Center for Internet Security (CIS)、および IANS Cloud Security Maturity Model (CSMM)[26]などがあります。これらのフレームワークは、組織が強固なサイバーセキュリティポスチャを確立および維持するために従うべき全体的な構造として機能します。

ポリシーは、ガバナンス階層の次のレベルです。組織のセキュリティ要件を概説した説明文書です。ポリシーは、フレームワークにある推奨事項を、組織のセキュリティプラクティスの指針となる明確で実行可能な文章に変換します。フレームワークは、多くの場合、規制要件やコンプライアンス要件を確実に遵守する特定のポリシーの導入を、組織に求めます。

コントロール目標はポリシーよりも具体的であり、セキュリティコントロールの望ましい結果に焦点を当てています。コントロール目標は、リスクを最小限に抑え、セキュアな環境を維持するためのゴールを定義します。たとえば、コントロール目標には、クラウドプラットフォームへのすべてのユーザーログインに MFA（多要素認証）を使用しなければならないと明記されている場合があります。コントロール目標は、達成すべきセキュリティ条件について明確な方向性を組織に提供します。

[26] IANS. (2024) Cloud Security Maturity Model Version 2.0 - *What is the Cloud Security Maturity Model*.



コントロール仕様と実装ガイダンスは、ガバナンス階層の下位レベルに存在します。これらがコントロール目標を満たす技術的な実現形態です。AWS や Azure など、利用する CSP やプラットフォームによってコントロール仕様は異なります。望ましいセキュリティ上の成果を達成するために導入すべき技術的コントロールの概要を、コントロール仕様は示しています。たとえば、MFA コントロール目標を達成するために、AWS のコントロール仕様では、すべてのユーザーからのコンソールアクセスに対して MFA を有効にしていることを要求することや、人間のアイデンティティおよびアクセス管理ユーザー(IAM ユーザー)には、API アクセスに対して「MFA Required」とするマネージドポリシーを要求する可能性があります。自動化により、これらのコントロール仕様への準拠を検証できます。クラウドインフラストラクチャ内の様々なさまざまな環境や技術により、望ましいセキュリティ上の成果を満たすためにカスタマイズされた実装が必要になる場合があるため、コントロール目標が複数のコントロール仕様につながる可能性があることに注意してください。

Figure 10: Structured Security Governance Hierarchy

ガバナンス階層は、情報セキュリティに対する構造化されたアプローチを組織に提供し、セキュリティプラクティスが業界標準、およびコンプライアンスと規制の要件に沿っていることを確実にします。この階層に従うことで、組織は強固なセキュリティポスチャを確立し、システムとデータを効果的に保護することができます。

2.3.1 ガバナンスの基本原則とガイドライン

クラウド導入のための強固なガバナンスフレームワークを確立する最初のステップの 1 つは、基本的なガバナンスの原則を決定することです。これらの原則は、クラウド環境のプライバシー、セキュリティ、および法令遵守を確実にするポリシー、標準、コントロール目標、コントロール仕様、および実装ガイダンスを定義するためのガイドラインとなります。クラウドガバナンスのフレームワークには、上級管理職、IT および技術担当者、ビジネスの専門家、およびセキュリティ関係者など、クラウド導入に責任を持つステークホルダーの主要な役割と責任の定義を含める必要があります。

ガバナンス階層により、業界標準や規制要件との整合性を確実にし、組織は強固なセキュリティポスチャを確立できます。次の図は、リスク許容度、データ分類、およびコントロール目標など、クラウドガバナンスプロセスの重要な要素を示しています。

図 11: クラウドガバナンスのプロセス

2.3.1.1 リスク許容度の決定

リスク許容度を理解することは、クラウド環境で運用する場合に許容できるリスクのレベルを決定する上で重要です[27]。リスク許容度とは、CSC が目的を遂行する際に、経営陣が特定のリスク受容を許可するレベルの変動値です。リスク許容度の決定では、財務、法律、評判、および業務への影響など、定性的要因と定量的要因の両方を考慮します。

CSC は、リスク許容度レベルを評価することで、明確なセキュリティポスチャを確立し、クラウド導入プロセス全体にわたってこの情報に基づいた意思決定を行うことができます。CCoE またはクラウドチ

[27] Details for cloud risks and categories is provided in *Domain 3: Risk, Audit, and Compliance*.

ームは、クラウドの導入に伴うリスクを文書化し、経営層に知らせ、定義されたリスク許容範囲内で運用する必要があります。

リスク評価は、組織に関連する有害なサイバーインシデントおよびオペレーショナルインシデントのシナリオについての発生可能性と影響の重大性に係る一貫した分析に基づく必要があります。これは、影響度/発生確率マトリックスまたは FAIR(Factor Analysis for Information Risk)[28]のような評価方法を使用して達成できます。

2.3.1.2 データと資産の分類

データと資産の分類[29]は、クラウドガバナンスの重要な側面です。CSC は、機密性、重要度、損失や侵害に関連する潜在的な影響に基づいてデータと資産を分類する必要があります。適切に分類されたデータは、セキュリティコントロールの適切な選択を促進し、データ保護に係る法律、規制、および契約上の要件への遵守を確実にします。

一般的な分類には、Public、Internal、Confidential、および Highly Confidential などがあります。データと資産の分類は、クラウドのどこでどのように保存し処理すべきか、また、データと資産を保護するために必要となり得るコントロール（法律、規制、組織の）に影響します。クラウドレジストリは、この分類を簡単に参照できるように文書化すべきです。

さらに、場合によっては CSC が知らないうちに、データが別の裁判管轄でホストされる可能性があり、クラウドコンピューティングではデータの場所が懸念事項となることがあります。政府や機関によっては、国境外へのデータ転送に制限があったり、EU の一般データ保護規則（GDPR）[30]などの追加コントロールが必要であったりします。

2.3.1.3 規制および法的要件の特定

裁判管轄および/または業界に適用される規制および法的要件と、取り扱われるデータの種類を特定することは不可欠です。例えば、CSC が EU 市民の個人データを扱う場合、GDPR に準拠する必要があります。同様に、CSC が米国で医療情報を扱う場合、HIPAA（Health Insurance Portability and Accountability Act）[31]に準拠する必要があります。

規制およびその他の法的要件に加えて、リスク評価中に特定された特定のリスクに基づいて追加の要件を決定することが重要です[32]。これにより、クラウドガバナンスフレームワークが包括的で、全体的なリスク管理戦略と一致することを確実にします。

---

[28] FAIR Institute. (2024) *What is FAIR?*

[29] Details on data classification are provided in *Domain 9: Data Security*.

[30] GDPR is not defined or restricted by the borders of its members. GDPR is also applicable to any company that processes the personal data of any EU citizen or resident.

[31] Health and Human Services. (2024) *Health Information Privacy.*

[32] Details for risk assessment is provided in *Domain 3: Risk, Audit, and Compliance*.

2.3.1.4 要件、規格、ベストプラクティス、契約上の義務

堅牢なガバナンスフレームワークを構築するには、確立された基準、ベストプラクティス、および契約上の義務に整合させることが重要です。これには、CSA CCM、ISO/IEC 27001、ISO/IEC 27017、NIST CSF、または CIS ベンチマークなどの標準およびベストプラクティスへの準拠が含まれます。

CSP の契約上の義務を理解することが重要です。これには、CSC と CSP の間で共有されるセキュリティ責任、および CSC と CSP の間の契約で説明されている特定のセキュリティ要件についての決定が含まれます。さらに、クラウド化の計画に影響を与える可能性があるため、CSC と第三者パートナーとの契約上の義務も考慮する必要があります。これには、クラウドサプライチェーンにおいて、組織が CSC と CSP の役割を果たすことができるパートナーシップが含まれます。

現在のベストプラクティスを常に把握することも重要です。CSP は、CSP のサービスを使用する上で推奨されるベストプラクティス（AWS Well-Architected Framework、Azure Well-Architected Framework、IBM Cloud Well Architected Framework、Google Cloud Architecture Framework など）を伝える場合がよくあります。CSC は特定のニーズに基づいてこれらのプラクティスから逸脱する必要があるかもしれませんが、ベストプラクティスはセキュアなクラウド環境を構築するための貴重な参照ポイントとなります。クラウドセキュリティは万能ではありません。業界、リスク許容度、および規制要件など、特定のコンテキストに基づいたカスタマイズが必要です。新たな脅威の出現と規制の変化に伴い、継続的なモニタリングと適応が不可欠です。CSC は、さまざまなベンダーが提供する適切なサービスを特定し、要件とコンプライアンス基準を満たすようにこれらのサービスを構成するという課題を抱えています。

2.3.1.5 主要ステークホルダーとの協議

クラウド導入に向けた強力なガバナンス体制の構築を進めるためには、主要な関係者と協議することが重要です。これにより、クラウドのセキュリティ戦略がビジネス目標に沿っていることを確認できます。

さらに、CSC は、特定された要件を満たすために適切なセキュリティ、プライバシー、およびデータ保護コントロールを実装するための明確なアクションプランを作成する必要があります。このプランでは、クラウド環境のセキュリティ、プライバシー、およびコンプライアンスを確保するために必要なコントロールを実施するための具体的な手順とスケジュールを説明する必要があります。

2.3.2 クラウドレジストリ

効果的なクラウドガバナンスを促進するために、CSC はクラウドデプロイメントレジストリとクラウドサービスレジストリを確立できます。これらはそれぞれ、クラウドガバナンスにおいて異なる役割を果たします(CSC は異なる用語を使用する場合があります)。

大まかに言うと、**クラウドサービスレジストリ**は、どのクラウドプラットフォームやサービスが、どの種類のデータに対して承認されているかを表すリストです（例えば、SaaS プロバイダ X は分類 Y のデータに対して承認されます）。

クラウドデプロイメントレジストリは、複数のプロバイダやサービスにまたがる組織のクラウドプレゼンスのインベントリを維持するために使用されるツールです。これは、所有権、使用状況、およびセキュリティコントロールなどの詳細情報を含む、組織の導入済みクラウドリソースに関する情報を保持する中央集中型のリポジトリです。このクラウドレジストリは、クラウドリソース管理における透明性と説明責任の確保に役立ちます。資産レジストリと同様の性質を持ち、包括的なクラウドレジストリを持つことで、CSC はクラウドリソースを効果的に管理し、セキュアにすることができます。

一部の CSC は、標準的なリスクレジスタを使用して、クラウドサービスとデプロイメントを追跡します。これは、そのリスクレジスタがセキュリティチームと運用チームに通常公開され、最新の状態に保たれ、本説を含む本書内のセクション中で説明されている情報が含まれている限り、許容できます。

クラウドデプロイメントレジストリを構築する際には、次のような要素を含めることが重要です。

1. **CSP(クラウドサービスプロバイダ):** AWS、Azure、GCP などの大手プロバイダや、Salesforce、Microsoft 365 などの SaaS プラットフォームなど、アカウントごとにクラウドサービスプロバイダを文書化します。この情報は、利用される基盤となるインフラストラクチャとサービスを理解するために役立ちます。
2. **環境 ID:** 各クラウド環境に一意の識別子を割り当て、追跡と管理を容易にします。この ID はログやその他の監視ツールに表示され、各環境の正確な参照ポイントとなります。
3. **記述名:** 各クラウド環境の目的や性質を的確に表すわかりやすい名前を付けます。これにより、組織内の各環境の役割の特定と理解が容易になります。
4. **コンプライアンスの分類:** PCI DSS、HIPAA、GDPR など、規制やコンプライアンスのニーズに基づいて各環境を分類します。適切な分類により、コンプライアンス要件を満たすための適切なセキュリティ対策とコントロールの適用を確実にします。
5. **リスクの分類**: CSC のリスク管理戦略に合わせて、各環境のリスクレベルを評価およびラベル付けします。これにより、リスク軽減のためのリソースと作業の優先順位付けが可能になり、適切なレベルのセキュリティコントロールが確実に実施されます。
6. **環境分類:** 開発環境、ステージング環境、本番環境など、異なるタイプの環境を区別します。この分類は、特定の要件に基づいて各環境を管理およびガバナンスするために役立ちます。
7. **オーナー:** 各クラウド環境を担当するビジネスオーナーを特定します。これにより、説明責任と責任を果たし、意思決定とリソース配分のための明確なコミュニケーションラインを確実にします。

8. **技術担当者:** 各環境の技術的な課題や運用管理に関する窓口を指定します。これにより、コミュニケーションを効率化し、技術的な課題を迅速に解決できます。

9. **CSP の連絡先**: CSP（訳注：原文では CAP となっているが、CSP の間違いと思われる）の顧客サポートとアカウント管理の連絡先情報を含めます。この情報は、サービス関連のあらゆる課題に対処し、CSP との良好な関係を維持するために不可欠です。

2.3.2.1 クラウドデプロイメンレジストリ機能

適切に保守されたクラウドデプロイメントレジストリには、次のようなメリットがあります。

- クラウドリソースに対する可視性とコントロールの向上：包括的なレジストリにより、CSC はクラウドの存在を明確に把握、文書化、および追跡できるため、効果的なリソース管理、最適化、および変更管理が可能になります。
- ガバナンスフレームワークの一貫した適用：詳細なレジストリを持つことで、CSC は適切なガバナンスフレームワーク、ポリシー、および手順がすべての環境で一貫して適用されることを確実にします。
- インシデント対応のサポート：クラウドレジストリは、必要なすべての連絡先情報を提供するため、セキュリティインシデントや業務停止時の迅速なインシデント対応と効果的な調整が可能です。
- ポリシーと規制の遵守：CSC はコンプライアンスのニーズに基づいて環境を分類することで、社内ポリシーや社外規制に準拠していることを確認できるため、コンプライアンス違反を最小限に抑えることができます。

クラウドレジストリがまだ導入されていない場合は、まずクラウドレジストリを集めるところから始めます。必要なすべての要素を特定し、各環境に必要な情報を収集します。計画した間隔で定期的にクラウドレジストリを確認して更新します。さらに、ビジネス環境、法律/規制/契約上の重要な変更、クラウド環境、または組織構造の変更があるたびに、レジストリを更新します。これにより、レジストリは正確かつ最新の状態に保たれ、効果的なガバナンスとリスク管理をサポートします。

2.3.3 クラウドセキュリティフレームワーク

フレームワークの主要な目的の 1 つは、セキュリティ管理の目標を整理し、優先順位を付けることです。これらの目標は、組織が望ましいセキュリティ上の成果を達成するために設定する具体的なゴールを表します。フレームワークは、これらの目標を分類するための構造を提供し、組織がそれら目標の最も効果的な実装と管理の方法を決定するために役立ちます。セキュリティコントロールの目標を整理することで、フレームワークは、CSC がクラウドセキュリティに対して体系的なアプローチをとり、必要なすべてのコントロールが実施されることを確実にします。

クラウド固有のセキュリティフレームワークは、クラウドコンピューティング固有の特性を考慮して、クラウド環境専用に設計されています。これらのフレームワークは、オンデマンドのリソース割り当て、SRM、および迅速な弾力性などの側面に対応します。クラウド固有のフレームワークを使用するこ

とで、CSC は、自社のセキュリティプログラムがクラウド固有の要件や課題に整合していることを確認できます。

クラウド関連のフレームワークの例[33]。

- CSA Cloud Control Matrix (CCM) - learn more below.
- ISO/IEC 27017:2015
- BSI Cloud Computing Compliance Criteria Catalog (C5)
- NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations
- PCI DSS Council Cloud Computing Guidelines

CSC がすでに情報セキュリティフレームワークを使用しているものの、そのフレームワークがクラウドの固有の側面を効果的にカバーしていない場合は、「サイドカー」 つまり補足的なフレームワークの概念を検討することができます。この概念では、既存のプライマリフレームワークとともにクラウド固有のセキュリティフレームワークを使用します。既存のセキュリティフレームワークの多くは、もともとクラウドコンピューティング用に設計されたものではなく、クラウド固有のアクティビティに適切に対応できていない可能性があります。サイドカーフレームワークを使用することで、CSC は、既存のフレームワークを他のセキュリティ分野に活用しながら、クラウドのセキュリティ活動に集中できます。

2.3.3.1 NIST サイバーセキュリティフレームワーク

いくつかのセキュリティフレームワークが存在しますが、NIST サイバーセキュリティフレームワーク（CSF）[34]は、クラウドに特化していないものの、広く認知されている構造化されたセキュリティアプローチを、業界や政府機関、その他の組織に提供しています。CSF コアとも呼ばれるこのフレームワークは、規模、セクター、または成熟度に関係なく、あらゆる組織がサイバーセキュリティポスチャとプログラムをよりよく理解、評価、優先順位付け、伝達するために使用できる、ハイレベルのサイバーセキュリティを達成する 6 つの機能分類を提供します。次の CSF 機能は、組織のサイバーセキュリティリスク管理のライフサイクルに関する、ハイレベルで戦略的なビューを提供します。

- **GOVERN (GV):** 組織のサイバーセキュリティリスク管理戦略、期待、およびポリシーを確立し、モニタリングします。
- **IDENTIFY (ID):** 組織に対する現在のサイバーセキュリティリスクの判断を支援します。
- **PROTECT (PR):** セーフガードを使用してサイバーセキュリティのリスクを防止または軽減します。

[33] For additional details about these frameworks, take the Certificate of Cloud Auditing Knowledge (CCAK) course available through ISACA.
[34] NIST. (2024) *The NIST Cybersecurity Framework (CSF) 2.0*

- **DETECT (DE):** 考えられるサイバーセキュリティ攻撃や侵害を見つけて分析します。
- **RESPOND (RS):** 検知されたサイバーセキュリティインシデントに関するアクションを実行します。
- **RECOVER (RC):** サイバーセキュリティインシデントの影響を受けた資産と運用を復元します。

2.3.3.2 CSA Security, Trust, Assurance, & Risk Registry

CSA Security, Trust, Assurance, and Risk (STAR) Registry は、クラウドサービスの透明性と信頼性を高めるために開始されたプログラムです。このプログラムは、CSP がセキュリティプラクティスを文書化し、CSC が CSP のセキュリティポスチャを評価するためのフレームワークを提供します。

CSA STAR プログラムは、次の 2 つの主要なコンポーネントで構成されています。

1. **CSA STAR Attestation:** ここでは、CSP が CSA CCM に対するセキュリティコントロールを自己評価し、その評価結果を公開します。これにより、プロバイダのセキュリティポスチャを透過的に把握でき、CSC は自社でのサービス利用について十分な情報に基づいた意思決定を行うことができます。
2. **CSA STAR Certification:** これは、CSA CCM や ISO/IEC 27001 のような他の広く認められている業界標準に対する CSP のセキュリティコントロールを独立した第三者が評価することを意味します。CSA STAR Certification の取得は、CSP が堅牢なセキュリティ対策と実践を実施していることを示します。

CSA STAR プログラムは、標準化されたセキュリティ評価を促進し、透明性を促進することで、CSC が CSP のセキュリティ、プライバシー、およびコンプライアンスの実践を評価できるようにします。これにより、CSC がクラウドサービスを選択および利用する際のリスクを意識した意思決定を支援し、クラウド業界における信頼と信用を醸成します。

2.3.3.3 Cloud Controls Matrix

CSA CCM v4[35] は、17 のドメインで構成されたコントロール目標のライブラリです。ガバナンスやリスク管理から運用上のセキュリティ、データプライバシーまで、幅広いセキュリティトピックを包括的にカバーし

[35] CSA. (2024) Cloud Controls Matrix (CCM)

ます。これにより、クラウドセキュリティの強化を目指す CSP と CSC にとって貴重なリソースとなります。

CCM の主な強みの 1 つは、ISO/IEC 27001/27002、PCI DSS、NIST CSF などの主要標準と関連付けていることです。CCM は、これらの確立されたフレームワークと調和することで、組織が複数の標準や規制にわたってコンプライアンスを達成できます。この STAR プログラムの関連付けは、業界での信頼性と関連性をさらに高めています。

CCM はクラウド環境に合わせて調整されているため、マルチテナント、分散、動的なクラウドシステムをセキュアにするのに最適です。クラウドコンピューティング特有の課題に焦点を当てているため、NIST CSF のようなより汎用的なセキュリティフレームワークとは一線を画しています。さらに、CCM はコントロールのカスタマイズが可能であり、CSC は、クラウドアーキテクチャ、配備モデル（IaaS、PaaS、SaaS）、コンプライアンスについてのニーズに、セキュリティコントロールを適合できます。

CCM のもう 1 つの主なメリットは、クラウドガバナンスのサポートです。CCM は、CSP がクラウドのリスクを効果的に管理および監督する強固なクラウドガバナンスプログラムを確立および維持するために役立ちます。これは、クラウドの導入が組織の目的と一致し、関連する規制を遵守していることを確認するために有効です。

CCM は、最新のクラウドセキュリティベストプラクティスを反映するために継続的に更新されます。CSP と CSC は、最新の情報を入手することで、彼らのクラウドセキュリティのニーズに係る信頼できるリソースとして、CCM を頼りにすることができます。
全体として、フレームワークは、堅牢で効果的なクラウドセキュリティプログラムの確立を目指す CSC にとって不可欠なツールです。クラウド固有のフレームワークを選択し、サイドカーフレームワークを使用し、セキュリティコントロールの目標を整理することで、CSC は、すべてのセキュリティコントロールに包括的に対処し、プログラムをクラウド固有の要件に合わせることができます。

2.3.4 ポリシー

強固なセキュリティポスチャを構築するためには、情報セキュリティポリシーが重要となります。ポリシーは、組織の情報資産の保護を規定し、必要なコントロール目標を概説します。たとえば、CIS[36]が発行する「NIST CSF Policy Template Guide」を参照してください。

ポリシーの実効性を確保するためには、組織の経営層がポリシーを正式に承認することが推奨されます。このような承認はポリシーに重みと権威を与え、ポリシーの執行に対する経営層のコミットメントを示します。経営層の後ろ盾があれば、ポリシーはより一貫して効果的に実施されます。

[36] CIS. (2024) *Policy Template Guide*.

データプライバシーに関する GDPR や、財務報告に関する SOX 法（Sarbanes-Oxley 法）など、さまざまな規制や法的枠組みへの準拠は、多くの場合、情報セキュリティポリシーの策定に大きな役割を果たします。組織は、これらのコンプライアンス基準を満たすための具体的なポリシーを用意する必要があります。これらのポリシーは、外部要件を確実に遵守し、ペナルティを回避するために重要です。

2.3.4.1 ポリシーのタイプ

組織が一般的に導入する情報セキュリティポリシーには、以下のようないくつかの主要な例があります。

- **情報セキュリティポリシー**は、情報セキュリティプログラムの実行方法を定めた最上位のポリシーです。情報セキュリティポリシーに、特定の技術要件をすべて盛り込もうとするのではなく、コントロール目標などの他のポリシーや文書を参照することが理想的です。
- **AUP（Acceptable Use Policy、利用規定）**は、組織の IT リソースの適切な使用を定義します。
- **リモートワークポリシー**では、従業員がリモートワークを行う際に想定されるセキュリティ対策や行動についてまとめています。
- **クラウドサービス利用ポリシー (Use of Cloud Services Policy)**では、クラウド内でデータを使用するための要件を設定します。
- **データ取扱方針**では、データの機密性、完全性、および可用性を維持するために、データの分類、取り扱い、保存、および破棄を行う方法を説明しています。

情報セキュリティポリシーは、セキュリティの実践と振る舞いについての明確なフレームワークを提供することで、セキュリティの実践を推進し、強固なサイバーセキュリティ文化を強化する必要不可欠で実用的な文書です。これらは、さまざまな環境に適切なレベルの保護が適用されることを確実にします。自社固有の情報セキュリティポリシーを熟知し、セキュリティポスチャ全体に貢献するためにポリシーを遵守する上での彼らの役割を理解していることが、従業員にとって重要です。

2.3.5 クラウドのセキュリティコントロール目標

クラウドのセキュリティコントロール目標は、クラウド環境内で望ましいコントロールまたは必要なコントロールのチェックリストとして機能します。これらの目標は、成果を重視するように書かれています。つまり、実行方法を指定するのではなく、結果を優先します。目標は、S.M.A.R.T.法（Specific、Measurable、Achievable、Relevant、Time-bound の頭文字）に従って測定可能である必要があります。

コントロール目標はプラットフォームに依存せず、特定の CSP や技術に縛られないようにする必要があります。これにより、コントール目標は幅広いクラウド環境に適用でき、関連性と有効性を確実にします。

実装される各セキュリティコントロールは、少なくとも1つの特定のコントロール目標にマッピングされる必要があります。これは、すべての対策が明確な目的を持ち、クラウド環境の全体的なセキュリティゴールに貢献することを確実にします。

最後に、コントロールを明確に定義し、あまりに広く解釈される可能性があるあいまいな指示を避け、代わりに実際に求められるセキュリティ上の成果に焦点を当てる必要があります。目標は詳細で、明確な方向性を示す必要がありますが、規範的な方法となるほど細かいものではありません。

まとめると、クラウドのセキュリティ管理目標は、クラウドにおける堅牢なセキュリティポスチャの確立の指針となります。クラウドコンピューティングの動的な性質に合わせて、適応性、測定可能性、および成果指向性を備えています。組織はこれらの目的に従うことで、クラウドのセキュリティを強化し、潜在的なリスクを軽減できます。

2.3.5.1 コントロール目標とフレームワークのマッピング

セキュリティプログラムにおけるコントロール目標は、使用しているフレームワークと整合させる必要があります。この整合により、プログラムが構造化され、必要な分野をすべてカバーできるようになることを確実にします。この整合では、大規模な組織における組織構造と業務上の責任に紐づけられる場合があります。

フレームワークはセキュリティプログラムの基盤であり、全体的な構造とアプローチの概要を示します。一方、コントロール目標は、望ましい成果と目標を定義します。コントロール目標をフレームワークにリンクすることで、プログラムが適切なカバレッジと明確なスコープを持つようになります。

コントロール目標がフレームワークに沿っていない場合は、戦略にギャップがあることを示している点に注意が必要です。このギャップは、プログラムが包括的で効果的となることを確かにするために対処が必要です。同様に、フレームワークの特定のカテゴリに係るコントロール目標が不十分である場合は、対処が必要な運用上の欠陥を示唆している可能性があります。

このマッピングを維持するには、コントロール目標リポジトリに、直接マッピングを含めることをお勧めします。これにより、参照が容易になり、整合性が文書化されます。CSA CCM は、関連するフレームワーク、標準、法規制要件へのマッピングの包括的なリストを備えた模範的なフレームワークとして機能し、ガバナンスとコンプライアンスの複雑さを管理するための貴重なリソースとなります。

2.3.5.2 コントロール仕様

コントロール仕様は、クラウド環境のセキュリティを確保するために不可欠な要素です。これらの仕様は、特定のセキュリティ要件を満たすために実装する必要がある詳細な技術コントロール機能の概要を示しています。コントロールの仕様はベンダーや技術に固有である必要があり、異なる CSP 間で大きな違いが生じる可能性があることに注意してください。

たとえば、MFA の実装要件を考えてみましょう。MFA を有効にする技術的な手順は、クラウドプロバイダによって異なります。CSP ごとに MFA の構成と実施方法が異なり、CSP 固有のコントロール仕様を作成する必要があります。

コントロール仕様が異なる可能性があるもう 1 つの分野は、ネットワークセキュリティです。デフォルトでは、Azure はインバウンド接続に対してネットワークをオープンに設定します。つまり、セキュアな環境を確保するためには、追加のネットワークセキュリティグループ設定を構成する必要があります。一方、AWS は、ネットワークのインバウンド接続について最小特権の設定にすることをデフォルトとして、より高いセキュリティレベルを提供しています。さらに、Azure は許可と拒否の両方のネットワークセキュリティルールをサポートしていますが、AWS は許可ルールのみをサポートし、その他のトラフィックはすべて拒否します。これらの違いは、使用する特定の CSP に合わせてコントロール仕様を調整する必要性を強調しています。

さらに、コントロール要件はデータやリソースの分類によって異なる場合があります。たとえば、CSC が Personal Identifiable Information（PII；個人識別情報）を扱う場合、デフォルト設定での配備に対してコントロール要件がより厳しくなることがあります。一方、公開されているとみなされるデータには、制限の少ないコントロール要件が適用される場合があります。コントロール仕様を定義する際には、データやリソースの機微性を考慮することが重要です。

場合によっては、CSP のエコシステム内でコントロールを完全に実施できず、サードパーティのツールが必要になることもあります。これらのツールは追加機能を提供し、クラウド環境のセキュリティ対策を強化できます。サードパーティ製のツールを使用する場合、コントロールの目標と要件を満たすために、ツールをどのように構成すべきかといった概要を示すコントロール仕様を定義することが重要です。これにより、サードパーティ製ツールがセキュリティ戦略に効果的に統合されます。

コントロール仕様は、技術の進歩、新製品、および新しい脅威と攻撃ベクトルを考慮して、一定期間にわたって改定する必要があります。改訂仕様の見直しと選択は極めて重要です。

2.3.6 セキュリティ責任共有モデル

セキュリティ責任共有モデル (SSRM)[37]は、クラウドセキュリティの基本的な概念です。クラウドサービスが適切に動作し、保護され続けられていることを確実にするため、CSC と CPS は別個の、しかし補完的な義務を負うことを、このモデルは確立します。この責任の共有は、CSP と CSC だけでなく、CSP を支援する企業、エージェント、クラウドプラットフォームインテグレータなど、サービスの提供に携わる他の関係者にも拡張できます。

CSC は、組織内の透明性の観点から、社内の IT チームが組織内のさまざまなコントロール機能にわたって責任共有モデルをどのようにマッピングしているかを明確に把握する必要があります。組織は、導入

[37] Additional details provided in *Domain 1: Cloud Computing Concepts & Architectures*

予定のワークロード数やクラウドで利用するサービスについて、適切なレベルの調査を実施する必要があります。たとえば、サービスが信頼できるようにコントロールを運用するには何人の人員が必要か、などです。これにより、いくつかの決定が下されます。例：組織は内部的にスケールアップする必要がありますか(専任スタッフを雇用するか、外部のコンサルタントと協力するか)。組織の責任の終了とCSP の責任の始まりの間にギャップが生じないように、組織内では、責任を明確に示し、また、組織固有のビジネスの運営方法に反映させる必要があります。双方の合意の中で、それらの責任～そして正確な解釈～を説明することは役に立ちます。

クラウドサービスは、その性質上、従来の IT サービスよりもはるかに急速に変化します。新しいサービスがリリースされたり、古いサービスが非推奨になったりします。したがって、責任共有モデルは、プロバイダが新しいサービスを追加し、既存のサービスをアップグレードするにつれて、時間の経過とともに進化する可能性があります。たとえば、CSP が特定のサービスを廃止した場合、データの移行と新しいサービスへ変換するライフサイクルを管理する責任者が誰であるかを把握することが重要です。したがって、すべての当事者は、特定の時点だけでなく、サービスのライフサイクルを通じてそれぞれの責任を考慮する必要があります。

また、クラウドの利用者は、クラウドサービスの性質により彼らのリスクを高める可能性があるという点も注目すべきです。クラウドの非コアサービスは、置き換えや大幅な変更のリスクにさらされる可能性があります。コアサービスとの依存関係は、今後しばらく継続されるという確信を与えることができます。また、コアサービスの変更は、そのサービスのすべてのユーザーにはるかに高いコストをもたらします。

要約すると、SSRM はセキュリティと一部のガバナンスの責任を明確にしています。これらの責任は、クラウドサービスモデルとセキュリティ領域によって異なります。

2.3.6.1 責任と説明責任

CSC は、CSP の基盤となるインフラストラクチャとプロセスを完全に把握しているわけではありませんが、クラウド利用のガバナンス責任は負います。従業員や部門が IT チームやセキュリティチームの知らないところでクラウドサービスを利用する「シャドーIT」と呼ばれる未認可なクラウドサービスの利用によって、社内にさらなる課題が生じます。このリスクを管理するには、シャドーIT と関連するリスクをカバーするアウェアネスプログラムを設計し、実装する必要があります[38]。

2.4 主要戦略とコンセプト

このセクションでは、クラウドコンピューティングのセキュリティとガバナンスにおける重要な戦略と概念について説明します。まず、ソフトウェア開発を円滑かつ安全にする上でとても役立つ、 DevOps と DevSecOps から始めます。また、新たな脅威を阻止するためのアクセスの継続的な検証とコントロ

[38] CSA. (2023) *Defining Shadow Access: The Emerging IAM Security Challenge*

ールに焦点を当てたゼロトラストセキュリティ戦略についても考察します。最後に、問題を予測し迅速に特定するために、人工知能（AI）と機械学習（ML）がクラウドセキュリティでどのように活用されているかを見ていきます。全体として、このセクションでは、これらの考え方がどのようにクラウドコンピューティングにおけるセキュリティとガバナンスを形成し、理解とコントロールを容易にするかを示しています。

2.4.1 DevOps

DevOps は、ソフトウェア開発（Dev）と IT 運用（Ops）を組み合わせて、セキュアなソフトウェア開発ライフサイクル（SSDLC[39]）を短縮すると同時に、ビジネス目標と密接に連携して機能、修正、およびアップデートを頻繁に提供することを目的とした一連のプラクティスです。クラウドコンピューティングでは、クラウドの俊敏性、拡張性、および柔軟性により、アプリケーションとインフラストラクチャの導入と管理に DevOps 手法が不可欠です。CSC は、アプリケーション開発のための戦術的な DevOps アプローチを、自動化により戦略的でアジャイルな組織全体のアプローチに拡張できます。

2.4.1.1 DevSecOps

DevSecOps は、初期設計から配備、継続的なモニタリングまで、SSDLC 全体にわたってセキュリティプラクティスを統合するセキュリティアプローチです。DevSecOps は、すべての段階でセキュリティプラクティスを統合することで、CSC が潜在的なセキュリティリスクと脆弱性を早期に特定して軽減し、よりセキュアでレジリエンスのあるソフトウェアアプリケーションを実現します。

CSA は、セキュアで効率的な DevSecOps の実装を支える 6 つの主要な柱（下の図に示す）を特定しました[40]。これらの柱は、DevOps デリバリーパイプラインの 5 つの段階に沿っており、ソフトウェア開発プロセスそのものにセキュリティを構築するための包括的な基盤を生成します。

[39] SSDLC incorporate security into all stages of the development process. Additional details are provided in *Domain 10: Application Security.*
[40] CSA. (2024) *Six Pillars of DevSecOps Series.*

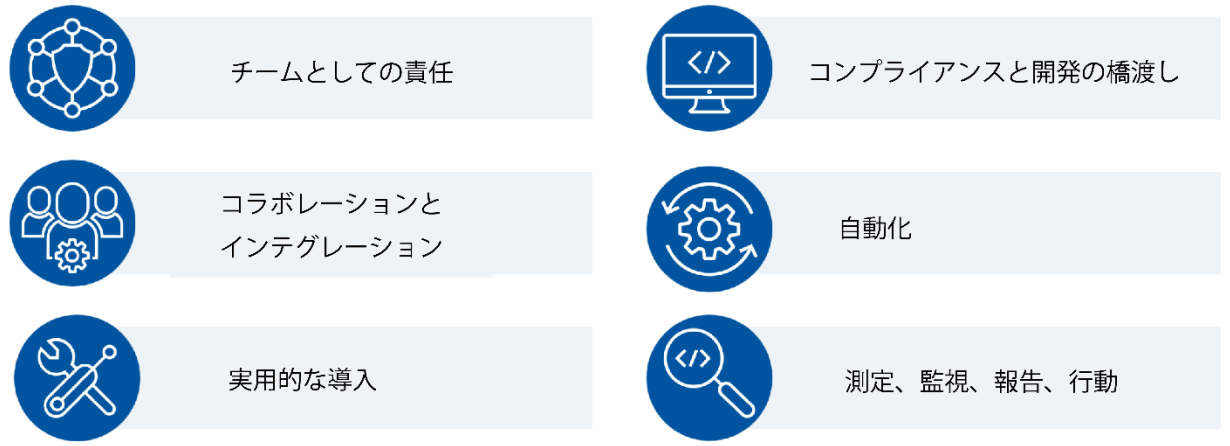


図 12: CSA Six Pillars of DevSecOps

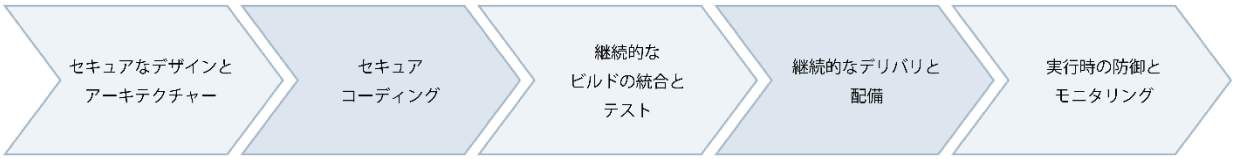


図 13: CSA Five Stages of the SSDLC Pipeline

CSC は、CSA DevSecOps デリバリーパイプラインの 6 つの柱と 5 つのステージを活用することで、セキュアで効率的な開発プロセスを構築し、セキュリティとコンプライアンスが最初から組み込まれた高品質で信頼性の高いアプリケーションを提供することができます。

2.4.2 ゼロトラストセキュリティ戦略

従来の「城と堀」の境界セキュリティアーキテクチャは、現在のクラウドコンピューティングとリモートワークの時代では効果がありません。ますます巧妙化する脅威アクターは、インターネット接続を多用する最新の分散型企業ネットワークにおいて、さらされているあらゆる技術的または人的脆弱性をエクスプロイトすることに長けています。重大なセキュリティ侵害は世界中で頻繁に公表されています。これらのインシデントは、ますます普及し継続的に成熟しているゼロトラスト[41][42]セキュリティ戦略に基づく最新のセキュリティアーキテクチャの実装に費やすよりも、多くのコストを CSC にかける可能性があります。

ゼロトラストは、クラウド/マルチクラウド、社内外のパートナー/ステークホルダーのユーザーエンドポイント、オンプレミス/ハイブリッドシステム、運用技術（OT）と IoT の両方を含む総合的なセキュリティ戦略です。ゼロトラストの実装では、リスクベースの設計原則に従ったエンタープライズセキュ

[41] Additional details on Zero Trust are provided in *Domain 12: Related Technologies & Strategies.*

[42] CSA. (2024) *Zero Trust Resource Hub*.

リティアーキテクチャの定義と、複数の製品/サービス、確立されたセキュリティ原則（"need to know"、" least privilege"）の活用が含まれます。ゼロトラストは、"アウトサイドイン"ではなく"インサイドアウト"によるセキュアな設計をアドバイスし、可視性を高め、進化する脅威環境に組織が対応できるように自動化されたリアルタイム対応を促進します。

ゼロトラストは、ますます高度化し攻撃的な脅威アクターの状況に対応します。これは、いかなるユーザーや資産も暗黙のうちに信頼されるべきではないという考えを前提としたサイバーセキュリティ戦略です。ゼロトラストは、侵害がすでに発生している、または今後発生することを前提としています。したがって、組織の境界で実行される1回の検証でユーザーに機密情報へのアクセスを許可すべきではありません。その代わり、各ユーザー、デバイス、アプリケーション、およびトランザクションを継続的に検証する必要があります[43]。ゼロトラストの重要な設計原則は次のとおりです。

- アクセスコントロールを組織リソースの近くに移動
- デフォルトでアクセスを拒否
- ユーザーおよびデバイスに対して明示的に許可された詳細なアクセス権を継続的に検証
- ラテラルムーブメントを制限するネットワークマイクロセグメンテーションの実装
- すべてのアクセスを詳細に監視
- すべてのネットワークトラフィックの暗号化
- アクセスパターンをリアルタイムで分析し、異常を迅速に検知して対応

ゼロトラスト戦略とそれを支えるアーキテクチャを正しく実装すれば、よりシンプルでセキュアで柔軟なビジネス運用のための環境を提供できる可能性があります。

2.4.3 人工知能と機械学習

クラウドセキュリティにおけるAIやMLの利用には、自動推論の利用が含まれます。AIの下位分野であるMLには、データを取り込み、そこから学習し、学習したことを適用した情報に基づく意思決定を行うアルゴリズムが含まれます。

クラウドプロバイダは、人間の監視だけに頼るには複雑すぎる場合があり、膨大なデータを分析することでセキュリティの設定ミスや脅威を検出するためにAI技術をしばしば活用します。例えば、MLの一種である教師なし学習は、ラベリングに頼らずに正当なアクセスから特定の脅威を識別するために使用されます。これらの技法は、自動化された改善策と組み合わせると特に強力です。

大規模言語モデル（LLM）を含む生成AIは、大規模なデータセットからパターンと構造を学習し、テキスト、画像、および動画などのコンテンツを生成します。これらのAIモデルは、計算能力とデータストレージへの要求が高く変動しやすいため、クラウドで運用することが多いです。特にデータの分離と保護が最も重要とされる共有リソースを扱う場合に、生成AIをクラウドで実行すると、データプライバシーとアプリケーション設計に関する重要な考慮事項が提起されます。

[43] CISA. (2022) THE PRESIDENT’S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE - *NSTAC REPORT TO THE PRESIDENT*. Page 1, adopted as the official CSA definition of Zero Trust.

NIST は、AI や ML 技術によってもたらされる複雑さを認識し、AI システムとモデルの利用に関するガバナンスと信頼性の向上を目的とした AI Risk Management Framework[44]を発表しました。このフレームワーク自体は、AI システムに関連するリスクの特定に関するガイダンスを提供し、AI のライフサイクル全体にわたってリスクを管理、マッピング、測定、および管理するための 4 ステップのアプローチを推奨しています。[45]

図 14: AI Risk Management Framework

ISO/IEC は、NIST フレームワークと連動して、組織内での人工知能管理システムの確立、実装、維持、継続的な改善のための要件を定めた ISO/IEC 42001:2023「*Information technology-Artificial intelligence-Management system*」を発表しました。これは、AI ベースの製品やサービスを提供または利用する事業者向けに設計されており、AI システムの責任ある開発と利用を確実にします。倫理的な配慮、透明性、

[44] NIST (2024) *AI RISK MANAGEMENT FRAMEWORK*.
[45] CSA. (2024) AI Governance & Compliance Resource Links Hub

継続的な学習など、AI が直面する独自の課題に対応します。これは、組織のために、イノベーションとガバナンスのバランスを取りながら、AI に関連するリスクと機会を管理するための構造化された方法を示します。

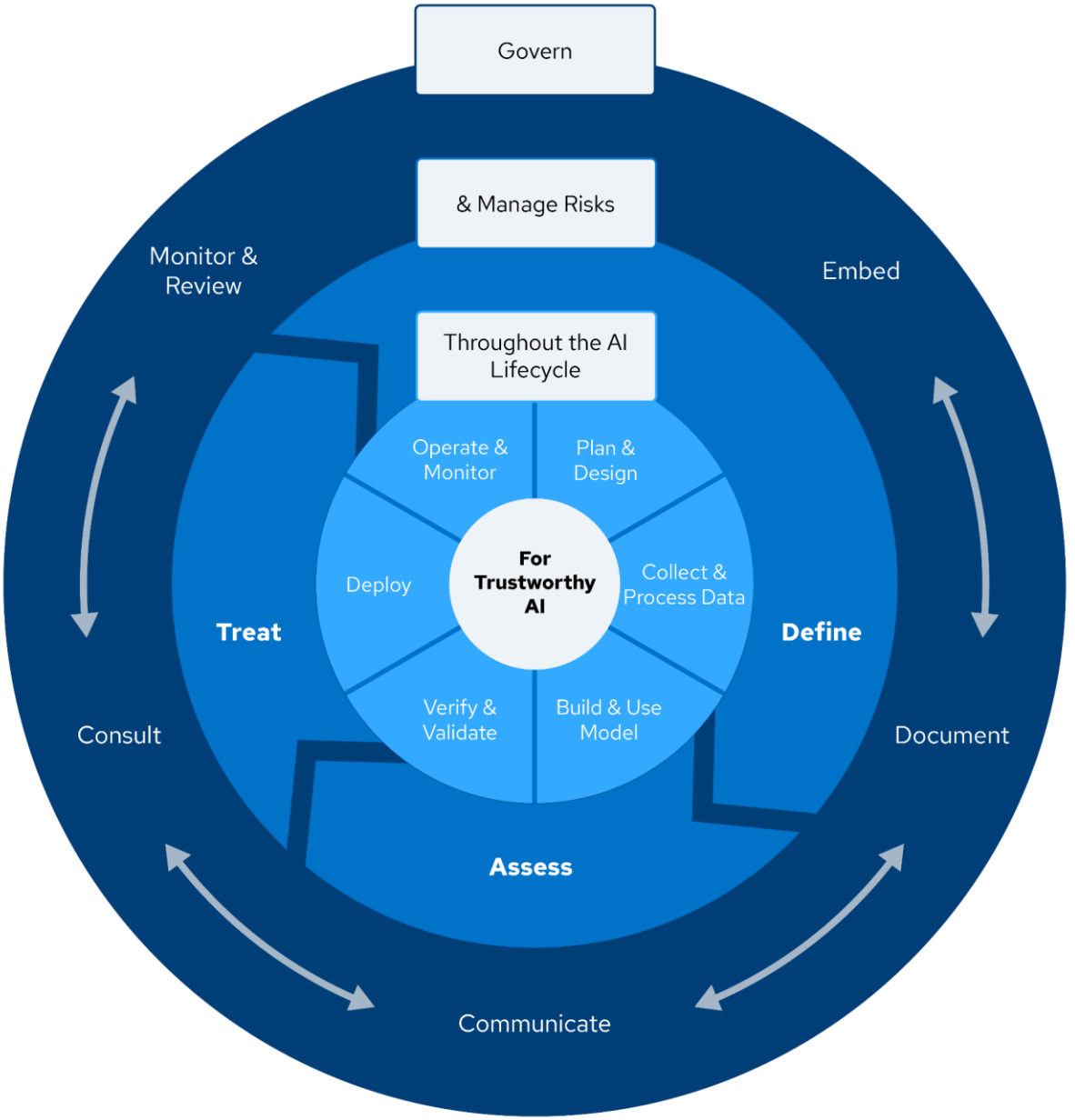


図 15: ISO/IEC AI Risk Management Lifecycle

ISO/IEC 42001:2023 などのフレームワークへの準拠と合わせた、DevSecOps、ゼロトラスト、AI/ML 統合などの戦略の導入は、堅牢でセキュアなクラウド環境を実現します。これらのプラクティスは、リスクを軽減するだけでなく、クラウドベースのシステムの安全性や信頼性を高めます。

サマリ

効果的なクラウドガバナンスは、クラウドで IT インフラストラクチャを管理する上で重要な側面であり、効果的なコーポレートガバナンスに不可欠です。一元化されたチームが IT インフラストラクチャ全体をコントロールできる従来のデータセンターでは、クラウドとは異なるガバナンスアプローチが必要です。

効果的なクラウドガバナンスには、組織的な調整が不可欠です。従来の階層はもはや適さないかもしれません。クラウド環境に即した明確な役割と責任を確立するには、組織構造を再評価することが重要です。

また、リスク、規制、およびセキュリティの要件を特定し、文書化することも重要です。クラウドでは、さまざまな規制やコンプライアンス基準の対象となる多数の場所にデータが保存され、処理される可能性があります。これらの要件を特定し、文書化することは、クラウドインフラストラクチャのコンプライアンスとセキュリティを維持するために不可欠です。

選択されたガバナンスフレームワークは、ガバナンス要件の概要を提供し、残りのガバナンスプロセスの方向性を設定します。CSC は、適切なコントロールとガイドラインの採用を確かにするために、常にガバナンス要件をビジネス戦略と整合させる必要があります。

CSC は、明確な役割と責任を確立し、CCoE を確立し、リスクを評価および管理し、クラウド資産、アクセス、および内部リソースのガバナンスのプロセスと手順を確立する必要があります。ガバナンスには、組織と CSP のセキュリティポスチャについての主要な指標と測定基準の確立、定期的な再評価を含める必要があります[46]。

推奨事項

- クラウドコンピューティングの技術面と運用面の違いは、効果的なセキュリティを維持するために新しいガバナンスアプローチが必要であることを理解してください。
- CCoE や CACI といった概念で組織構造を適応させ、クラウドのガバナンス能力を向上させます。
- セキュリティチャンピオンプログラムを導入し、特に開発チームやクラウドチームにセキュリティ知識をより効果的に浸透させます。
- リスク許容度、コンプライアンス義務、ビジネスニーズ、および既存のクラウド使用状況など、基本的な要件を収集して把握します。
- セキュリティフレームワークから始めて、セキュリティポリシー、コントロール目標、およびコントロール仕様を明確なガバナンス階層に整理します。
- DevOps、ゼロトラスト、AI など、クラウドで作業するときによく見られる他の戦略や概念からのセキュリティとガバナンスへの影響を理解します。

[46] For additional details on metrics, take the Certificate of Cloud Auditing Knowledge (CCAK) course available through ISACA.

追加のガイダンス

- Cloud Security Technical Reference Architecture | CISA
- Communicating the Business Value of Zero Trust | CSA
- Zero Trust Guiding Principles | CSA
- SaaS Governance Best Practices for Cloud Customers | CSA
- COBIT Framework | ISACA
- ISO/IEC TR 3445:2022 Information Technology Cloud Computing Audit of Cloud Services

ドメイン 3: リスク、監査、コンプライアンス

このドメインは、リスク、監査、コンプライアンスの問題に関連する、クラウドセキュリティのコアな側面に焦点を当てています。ただし、包括的なリスク、監査、およびコンプライアンスに関する徹底したトレーニングと経験の必要性に、このドメインが取って代わるものではないことに注意してください。これらの主題を深く掘り下げたい人には、CSA が ISACA と共同で*提供する* CCAK（Certificate of Cloud Computing Audit Knowledge）をお勧めします。

クラウドリスクに関しては、このドメインではクラウドサービスプロバイダ（CSP）を評価するアプローチを探ります。これはクラウドリスクレジストリの確立と承認プロセスの実装をカバーしています。さらに、CSA の *Top Threats*[47] を参照し、一般的なリスクに関するコンテキストを提供します。

このドメインでは、コンプライアンスと監査、さまざまなタイプのコンプライアンス、およびコンプライアンス継承の概念について概説します。GRC（ガバナンス、リスク、コンプライアンス）プロセスを支援するために、このドメインでは、さまざまなツールや技術を紹介しています。これには、ポリシー、手順、コントロール、自動化の役割、ソフトウェア部品表（SBOM）、および関連技術が含まれます。これらのコンポーネントは全体として、ガバナンスフレームワークをサポートし、クラウドコンピューティングのリスクとコンプライアンス要件の複雑な概観を管理するのに役立ちます。

学習目標

このドメインでは、次のことを学びます。

- クラウドのリスクを定義、分類し、ツールを使用して管理します。
- クラウドベースの環境で監査を受けなければならない規制やコンプライアンスの制約を特定します。
- GRC を管理する際に使用する技術ツールと非技術ツールのセットを特定します。

3.1. クラウドのリスク管理

組織がクラウドサービスへの依存度を高めている今日のデジタルランドスケープでは、効果的なクラウドリスク管理が不可欠です。このセクションでは、クラウドリスクを理解することの重要性について掘り下げ、クラウドリスクプロファイルの確立、CSP の評価、クラウドリスクレジストリの維持、リスク

[47] CSA. (2021) Research Topic: Top Threats

評価、脅威インテリジェンス、および脅威モデリングの実施に関する洞察を提供します。堅牢なクラウドリスク管理手法を導入することで、組織は潜在的なリスクをプロアクティブに特定して軽減し、クラウド環境のセキュリティとレジリエンスを確保できます。

3.1.1 クラウドのリスク

まずは例から見ていきましょう。ある企業には、顧客の個人情報が格納されたクラウドストレージバケットがあります。これを**資産**と呼びます。攻撃者（**脅威アクター**とも呼ばれます）にとっては、資産が**ターゲット**になります。クラウドストレージバケットの弱点の1つは、設定が間違っている可能性があることです。これを**脆弱性**と呼び、攻撃者にとっては**攻撃ベクトル**となります。

リスクとしては、バケット内の個人データが漏洩し、規制当局から罰金を科せられる可能性のことです。もう1つのリスクは、何らかの操作によって、データが使用できなくなったり、破損したりする可能性のことです。

コントロールや**対策**は、リスクを軽減する方法です。ここでの典型的なコントロールは、これらのストレージバケットがインターネット全体、より具体的には脅威アクターにアクセスできないようにするポリシーです。

理想を言えば、リスクを許容できるレベルまで下げるための十分なコントロールが必要です。これには、重要な資産と脅威アクターが何であるかを理解することが含まれます。このプロセスは**脅威モデリング**と呼ばれ、アプリケーションセキュリティなど、このガイダンスの他の場所で説明します。クラウドの世界における脅威モデリングは、データが保存されているさまざまな場所やクラウドサービス、それらの間でデータがどのように流れるかを特定することから始まります。CSA research[48]も参照してください。

全般的なリスクとセキュリティリスクの両方について、最も一般的なリスク要因とカテゴリーの例を次に示します。また、クラウドセキュリティアライアンスの「Top Threats」調査レポート[49]を確認することもお勧めします。2022 年版の「Pandemic Eleven」では、以下のカテゴリーが上位となりました。

- 不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵の管理
- セキュアでないインターフェースや API
- 設定ミスと不適切な変更管理
- クラウドセキュリティのアーキテクチャと戦略の欠如
- セキュアでないソフトウェア開発
- セキュアでないサードパーティーのリソース
- システムの脆弱性
- 予想外のクラウドデータ公開
- サーバレスやコンテナワークロードの構成ミスやエクスプロイト

[48] CSA. (2021) Publications: Cloud Threat Modeling

[49] CSA. (2021) Research Topic: Top Threats

- 組織犯罪/ハッカー/APT(Advanced Persistent Threat)
- クラウドストレージデータ流出

クラウド脅威インテリジェンスのソースは他にも多数あります。最新情報については、CSA のウェブサイトを参照してください。さらに、**MITRE ATT&CK**[50]フレームワークは、脅威アクター戦術の包括的なマトリックスを提供します。

3.1.2 クラウドリスクプロファイルの確立

クラウドリスクプロファイルはクラウドのリスク分析結果のことであり、クラウドサービスに依存している組織にとって重要な評価です。このプロファイルは、サイバーリスクアナリストや監査人のための基礎的なガイドとして機能し、CSC のリスクランドスケープに関する洞察を提供します。これにより、組織はリスクエクスポージャーを把握できるようになり、リスク選好の範囲内でクラウド戦略とビジネス目標の整合性を確保できます。

3.1.2.1 クラウドリスクプロファイルの最初の質問

リスク評価の最初のステップは、組織のクラウドリスクプロファイルを確立することです。これは、リスク評価の質問で実現できます。 組織がリスクプロファイルを評価するための出発点として、次の質問を検討してください。これらは必ずしも網羅的ではなく、特定のクラウドサービス利用者（CSC）が使用すべき正確な質問でないことに注意してください。

- **ビジネス戦略との整合性:**
    - クラウドコンピューティング技術は、ビジネス戦略全体とどのように連携していますか?
    - クラウドコンピューティングの導入は、組織の戦略目標をどのようにサポートしていますか?
    - クラウドコンピューティングはビジネスモデルにどのようなメリットをもたらし、業務効率や市場競争力を高めますか？
- **情報セキュリティまたはサイバーセキュリティポリシー:**
    - 情報セキュリティまたはサイバーセキュリティポリシーは、クラウド技術管理を反映するように更新されていますか？
    - クラウドコンピューティングの導入による変更を組み込むために、情報セキュリティまたはサイバーセキュリティポリシーはどのくらいの頻度で見直され、更新されていますか？
    - 関連するすべての関係者が、情報セキュリティまたはサイバーセキュリティポリシーの見直しと更新に関与していますか？

[50] MITRE. (2024) Cloud Matrix

- **クラウドコンピューティングのサードパーティーリスクの評価:**
    - サードパーティーリスクの評価には、クラウドコンピューティング技術に固有のリスク（データプライバシーおよびセキュリティに関する法律に基づくリスクなど）が含まれていますか？
    - CSP の評価において、サードパーティーリスクの評価はどの程度網羅的ですか？
    - 評価は、データプライバシー、セキュリティ法、および業界規制へのコンプライアンスに特有のリスクに対処していますか？
    - クラウドリスクの評価は、組織の全体的なリスク選好およびリスク許容度と一致していますか?
- **クラウド移行のリスクアセスメント:**
    - クラウド移行前に、特にクラウド技術関連のリスクに焦点を当てた徹底的なリスク評価が行われていますか？
    - クラウド移行のリスク評価の結果は、リスク管理計画全体にどのように統合されましたか?
- **CSP と契約のインベントリ:**
    - 契約の詳細、サービスレベルアグリーメント(SLA)、第三者による評価または保証レポートなど、すべての CSP のインベントリが一元化されていますか？
    - CSP のパフォーマンスとコンプライアンスは、契約に照らしてどのように監視され、レビューされていますか？
- **BC/DR（事業継続/災害復旧）計画:**
    - 組織の BC/DR 計画は、クラウド導入を反映するために更新されていますか?
    - 組織の BC/DR 計画は、クラウドサービスにどのように適応していますか?
    - クラウドサービスに障害が発生した場合の BC/DR について、特に考慮すべき点はありますか?
    - BC/DR 計画は、CSP の責任と依存関係を文書化していますか?
- **クラウド移行後のプライバシーポリシーの更新:**
    - クラウドの採用を盛り込むために、組織のプライバシーポリシーを更新していますか？
    - クラウドでのデータ収集、保存、処理、管理、保存、破棄に対応するために、組織のプライバシーポリシーはどのように改訂されましたか？
    - 更新されたプライバシーポリシーは、データレジデンシー、国境を越えたデータ転送、およびユーザーの同意メカニズムを十分にカバーしていますか？

- **インシデント管理ポリシー:**
    - クラウドサービスが関係するインシデントを含めるために、インシデント管理ポリシーはどのように更新されましたか？
    - クラウドベースの資産が関係するセキュリティ侵害やデータ漏洩に対応する明確な手順はありますか？
    - CSP とのインシデント関連のコミュニケーションチャネルが定義され、文書化されていますか？
- **SSDLC（セキュアなソフトウェア開発ライフサイクル）:**
    - クラウドへの移行を反映するために、組織の SSDLC は更新されましたか?
    - 特に API のセキュリティ、アイデンティティとアクセスの管理、暗号化に関する、クラウド固有のセキュリティ上の考慮事項を組み込むために、SSDLC はどのように変更されましたか？
    - クラウド対応のセキュリティツールとプラクティスは 、SSDLC の開発、配備、保守の各フェーズに統合されていますか？

3.1.2.2 クラウドリスクプロファイルの使用

クラウドリスクプロファイルを確立した結果は、残りのクラウドリスク管理プロセスに情報提供するために使用できます。ゴールは、リスク許容度と現在のクラウドリスクポスチャの両方を特定することです。クラウドリスクプロファイルは、リスクの観点から、CSC がクラウドに移行する準備がどの程度整っているかを示す必要があります。

CSC は、CSA が提供するようなクラウドセキュリティフレームワークや標準を採用することも検討する必要があります。これにより、より詳細なベンチマークプラクティスや、クラウド環境での包括的なリスク管理を確実に行うことを支援します。

3.1.3 クラウドリスク管理への理解

クラウドリスク管理を理解するには、クラウドコンピューティングに関連するリスクを特定、評価、および対処するための構造化されたアプローチが必要です。クラウドコンピューティングで使用されるリスク管理や方法論は、オンプレミスの世界で採用されているものと変わりません。しかし、スコープと環境の定義、およびリスク評価とリスク対応プロセスの間にとられた特定のアクションのいくつかによって、変更が予想されるかもしれません。

欧州ネットワーク・情報セキュリティ機関（ENISA）の Risk Management Process [51]は、組織がこれらのリスクを効果的に管理するために適応できるフレームワークを提供します。このプロセスは、CSC のよ

[51] ENISA. (2022) The Risk Management Process

り広範な運用プロセスに統合するように設計されており、リスク管理に対する包括的なアプローチを確実にします。このプロセスの主要なコンポーネントの詳細は次のとおりです。

- 企業のリスク管理戦略
    - ○ リスクコミュニケーション、リスク認識、コンサルティングを含む
- リスクアセスメント
- リスク対応
    - ○ リスク受容を含む
- 他の運用プロセスおよび製品プロセスとのインターフェース
- 計画、イベント、および品質のモニタリングとレビュー

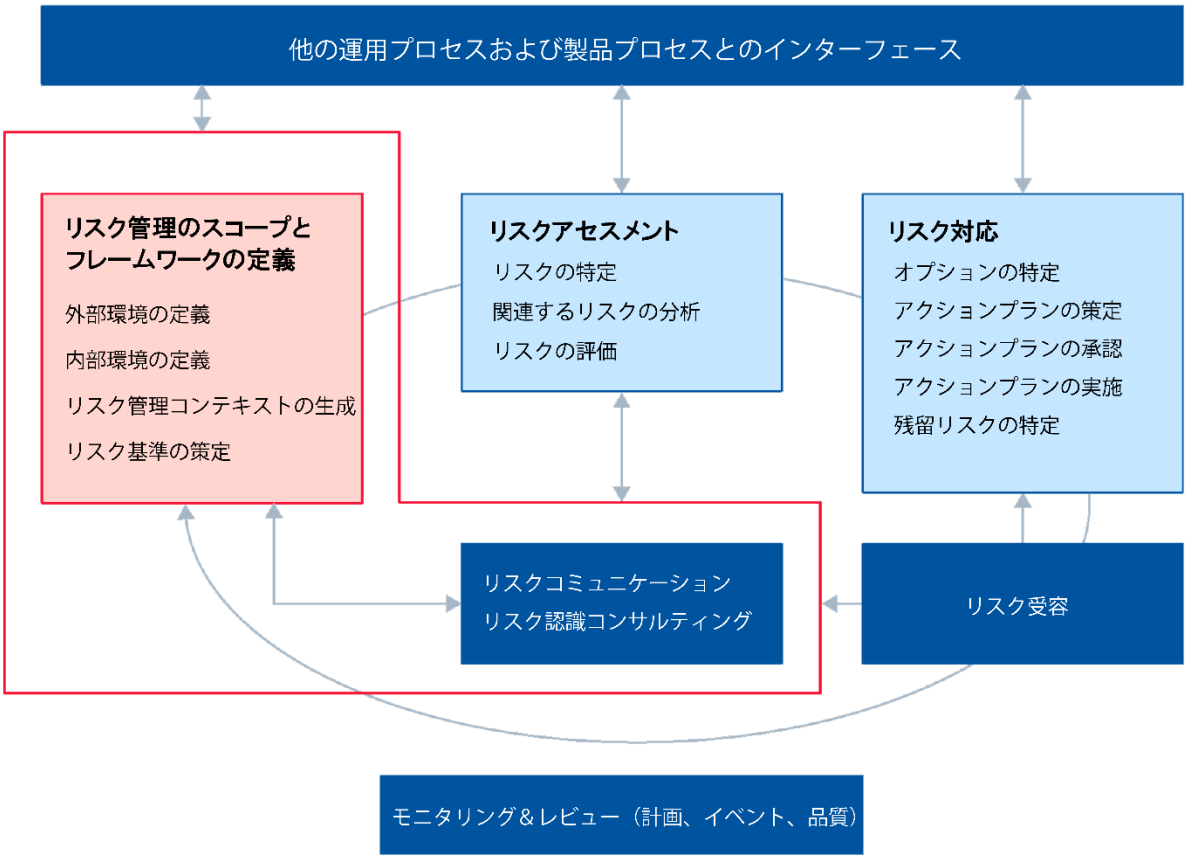


図16: 包括的なクラウドリスク管理フレームワーク

3.1.3.1 企業のリスク管理戦略

このフェーズでは、リスク管理のコンテキストを作成し、評価プロセスの指針となる具体的なリスク基準を策定します。

- **リスク管理のスコープとフレームワークの定義：**クラウドサービスや運用の具体的な側面を含

め、リスク管理プロセスの対象範囲に明確な境界を設定します。

- **外部環境の定義：**規制要件、市場状況、および技術の進歩など、クラウド運用に影響を与える可能性のある外部要因を把握します。
- **内部環境の定義：**組織構造、文化、リスク選好、リスク許容度、および既存のコントロールなど、リスク管理に影響を与える内部要因を評価します。
- **リスク管理コンテキストの生成：**集中的かつ効果的なリスク管理戦略を可能にする、組織の目標に沿ったコンテキストを作成します。
- **リスク基準の策定：**特定の状況に合わせて、発生の可能性や潜在的な影響を含むリスクの評価基準を作成します。
- **リスクコミュニケーション：**リスクに対する意識を高め、関連するステークホルダーと協議し、リスクやリスク管理活動に関する情報が適切に共有されるようにします。
- **リスク認識：**クラウドリスク管理の重要性と、対処すべき具体的なリスクについての認識を高めます。リスクとリスク管理活動に関する情報を効果的に発信するためのメカニズムを導入し、関連するすべてのステークホルダーに周知徹底します。
- **コンサルティング：**利害関係者と協力して見識を収集し、リスク管理プロセスにおいて多様な視点が考慮されるようにします。

3.1.3.2 リスクアセスメント

これには、発生の可能性とその結果の重大度を判断するために各リスクを評価することが含まれます。

- **リスクの特定：** セキュリティ侵害、データ損失、およびコンプライアンス違反など、クラウドサービスに関連する潜在的なリスクを体系的に特定します。
- **関連するリスクの分析：**特定されたリスクを分析し、その性質、原因、および潜在的な影響を把握します。
- **リスクの評価：**各リスクの可能性と影響を評価し、目標に対する潜在的な影響に基づいて優先順位付けを行います。

3.1.3.3 リスク対応

リスクを評価した後、各リスクを軽減、移転、回避、または受容するための行動計画を作成し、承認します。これらのアクションプランを実行し、残っている（残留する）リスクを特定します。

- **オプションの特定：**軽減、移転、回避、受容など、さまざまなリスク管理戦略を検討します。
- **アクションプランの策定：**リソースとリスク選好を考慮し、各リスクを軽減または対処するための具体的なアクションを策定します。
- **アクションプランの承認：**行動計画が適切な意思決定者と利害関係者によってレビューされ、承認されるようにします。
- **アクションプランの実施：**許容される期間内に、特定されたリスクを管理するための承認されたアクションを実行します。
- **残留リスクの特定：**リスク対応実施後の残留リスクを評価し、文書化します。

- **リスク受容：**残留リスクがリスク選好の範囲内にあり、さらにリスクを軽減するためのコストがその影響よりも大きい場合は、リスクを受容します。
    - リスクを受け入れる決定は、影響と起こりうる結果を十分に理解した上で、費用対効果分析に従い、ビジネスオーナーによってなされます。
    - 残留リスク、分析、受け入れを明確に文書化する必要があります。
    - 受容されたリスクは、リスクプロファイル、リスク選好、または利用可能な費用対効果の高い軽減策についての変化を認識するために、定期的に再評価される必要があります。

3.1.3.4 他の運用プロセスおよび製品プロセスとのインターフェース

リスク管理はサイロ化されるべきではなく、リスクの考慮が、CSC の運用と製品ライフサイクル全体に組み込まれていることを確実にするために、他のビジネスプロセスとのインターフェースが必要です。

3.1.3.5 モニタリングとレビュー（計画、イベント、品質）

リスク管理計画、イベント、およびリスク管理活動の品質を継続的にモニタリングします。定期的なレビューにより、リスク管理プロセスの有効性を維持し、ビジネス環境の変化に適応できるようにします。

- クラウド環境、リスク管理計画、実装されたコントロールの有効性を継続的にモニタリングします。
- 進化するリスクランドスケープと組織の変化に対処する上で、リスク管理プロセスが適切かつ効果的に維持されることを確実にするため、リスク管理プロセスの定期的なレビューを実施します。
- 「Key Control Indicators」[52]など、実施されたリスク対応の有効性と効率性を評価するための関連指標を導入します。
- 残留リスクを評価して、依然として許容レベル以下であることを確認します。「Key Risk Indicators 」[53]は、 クラウドのリスクポスチャの適時なモニタリングに役立ちます。

ENISA *Risk Management Process* に従うことで、CSC は、自身の全体的なリスク管理戦略と運用プラクティスと統合された、クラウドのリスクを管理するための堅牢なフレームワークを確立できます。このアプローチは、特定のクラウド関連のリスクを軽減し、クラウドコンピューティング環境の複雑さにうまく対処する、組織のレジリエンスと俊敏性を高めることを支援します。

[52] Key control indicators are metrics that provide information about the extent a risk control is meeting its intended objectives.

[53] Key risk indicators are metrics that provide early signals of increasing risk exposures in various areas of the enterprise. They are also known as emergent risks.

3.1.4 クラウドサービスの評価

クラウドのリスクを管理する最初のステップの 1 つは、CSP とそのサービスのリスクを評価する体系的なプロセスを持つことです。この評価は、ビジネスニーズとリスク許容度に合わせる必要があります。CSP を評価する際の課題は、CSC がすべての CSP の内部オペレーションと技術を可視化できることがほとんどないことです。CSP は常にサービスを変更しています。場合によっては、毎週大きなサービス変更が加えられることもあります。CSC は、SLA や契約のカスタマイズを補完する能力が不足している可能性があります。

次のプロセスは、これらの違いを考慮して設計されています。

- ビジネス要件
- CSP のドキュメントのレビュー
- 外部ソースの確認
- コンプライアンス要件へのマップ
- データ分類へのマッピング
- 必要なコントロールと補完コントロールの定義
- 承認プロセス

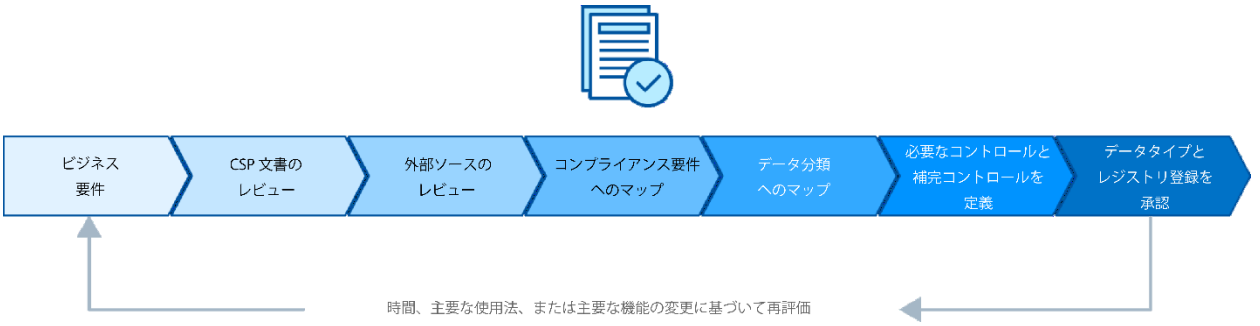


図 17: クラウドサービスの評価と承認のための体系的なプロセス

3.1.4.1 ビジネス要件

CSC のビジネスユニットは、CSP とサービス（例：Azure のような大規模なプロバイダーの PaaS サービス）の使用を要求します。必要な特定の CSP やサービスを含むビジネス要件を理解することは、特定のクラウドソリューションを採用するリスクを評価する最初のステップです。

- **ビジネス要件の理解：** クラウドサービスを要求するビジネスユニットやその他の関係者から詳細な要件を収集します。これには、特定の機能、パフォーマンスに対する期待、規制またはデータ処理の要件が含まれます。
- **プロバイダとサービスの選択：**想定される CSP とそのサービス（PaaS、IaaS、SaaS など）を評価し、ビジネス要件に最も適したものを決定します。

3.1.4.2 クラウドサービスプロバイダのドキュメントのレビュー

CSP のドキュメントを徹底的に精査します。ドキュメントに、セキュリティの詳細のための CSA Consensus Assessments Initiative Questionnaire (CAIQ)[54]、CSP が保持する認定、詳細なセキュリティおよびプライバシーポリシー、およびサービス利用規約(ToS)が含まれることを確認します。

- **CAIQ と Certification** ：CAIQ は、CSP がセキュリティコントロールを開示するために回答する一連の包括的な質問を提供します。CSP certification（ISO/IEC 27001、SOC2 など）は、セキュリティプラクティスの第三者評価を提供します。
- **セキュリティとプライバシーに関するドキュメント:**CSP が公表しているセキュリティポリシー、プライバシーポリシー、およびデータの取り扱い慣行をレビューし、関連する標準に準拠していることを確認します。
- **SLA（Service Level Agreement）と契約：** SLA は、CSP のパフォーマンスと稼働時間のコミットメントを概説し、契約書には、責任と賠償を含むサービス利用規約を詳細化します。
- **サービス利用規約:** ToS を理解することは、導入後の法的または運用上の不測の事態を避けるために重要です。ToS は、CSC と CSP の間の唯一の法的契約である可能性があります。

3.1.4.3 外部ソースのレビュー

CSC は、CSP のドキュメントを確認するだけでなく、独立した評価のために、Cloud Access Security Brokers (CASB), Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP) および SaaS Security Posture Management (SSPM) ソリューションなどのツールの使用を検討できます。CSP に関連するレビュー、脆弱性、およびセキュリティインシデントについて、CSC は、追加の調査を実施する必要があります。大規模なプロジェクトや小規模な CSP に限定される場合もありますが、多くの場合、これは、プロバイダと調査結果を確認する良い機会です。

- **ツール:** サードパーティリスクの継続的なモニタリングのためのツールを利用します。
- **調査:** 外部のレビュー、報告された脆弱性、および CSP に関連する過去のセキュリティインシデントを調査し、CSP のセキュリティポスチャと対応能力を測定します。
- **プロバイダーとのやり取り：** 重要なプロジェクトの場合は、CSP と直接連携して調査結果や懸念事項を話し合うことを検討します。これにより、明確さと安心感を得ることができます。

3.1.4.4 コンプライアンス要件へのマップ

CSP を選択する際には、 General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), または Payment Card Industry Data Security Standard (PCI DSS).など、

[54] CSA. (2024) Cloud Controls Matrix and CAIQ v4

CSP の機能とポリシーを組織のコンプライアンスニーズに合わせることが不可欠です。これにより、規制要件が満たされ、データセキュリティが保たれます。ほとんどの CSP は、さまざまな標準や規制に彼らが準拠していることを示す、詳細なコンプライアンス文書を公開しています。

3.1.4.5 データ分類へのマップ

すべてのデータが同じリスク管理プロセスを必要とするわけではありません。さまざまな CSC のニーズと要件に柔軟に対応できるように、 CSP とサービスは、データの分類に基づいて承認される必要があります。たとえば、価値の低いもしくは公開されたデータは、よりリスクの高いサービスで処理することが許容されるかもしれません。

- **データの機微性評価：** 移動中および保存中のデータの機微性を評価します。すべてのデータに同じリスクがあるわけではありません。したがって、すべてのクラウドサービスが最高のセキュリティ基準を満たす必要があるわけではありません。
- **データの分類に基づくサービス承認:** 取り扱うデータの分類に基づいて CSP とそのサービスを承認します。このアプローチにより、リソースの柔軟性と効率的な使用を可能にします。

3.1.4.6 必要なコントロールと補完コントロールを定義

最終的な承認の前に、クラウドリスクを軽減するための適切なレベルのセキュリティを提供するための、必須のコントロール（CSP 内の構成設定など）と任意の補完コントロール（サードパーティツールなど）を選択し、文書化することが重要です。

3.1.4.7 承認プロセス

収集した情報とマッピングに基づいて、CSP のサービスが意図したデータ分類に適しているかどうかを判断します。適している場合は、使用を承認し、クラウドサービスレジストリに組み込みます。

3.1.5 クラウドレジスタ

クラウドレジスタは、承認された CSP とサービス、および特定のリスクレベルで取り扱うことが承認されている、データの分類についての集中リポジトリです。これにより、どのプロバイダやサービスをどのプロジェクトに使用するかを、社内で決定する指針となります。また、データがコンプライアンスを遵守しているプロバイダとのみ使用されることを保証するのにも役立ちます。

3.1.5.1 クラウドレジスタの理解

クラウドレジスタは、CSC が使用するすべてのクラウドサービスを、クラウドサービスが取り扱うデー

タの分類、評価されたリスクレベル、およびリスク評価を見直すタイミングに関する情報とともにカタログ化する戦略的なツールです。クラウドレジスタは、さまざまなデータ分類（たとえば、公開情報、機密情報、個人を特定できる情報）を区別し、クラウドサービスの使用をガイドするために、リスクレベルを割り当てます。

3.1.5.2 クラウドレジスタのコンポーネント

クラウドレジスタ[55]には、サービスに係る CSP、サービスそのもの、サービスによって処理が許可されるデータの分類、リスクレベル（重要、高、中、低など）、有効期限、および、いつリスク評価を再実施しなければならないかのその他の主要な属性のための項目が含まれます。属性には、名前、説明、所有者、期待される/実際の頻度、潜在的な/実際の規模、潜在的な/実際のビジネスへの影響、および処分が含まれる可能性があります。

3.1.5.3 クラウドレジスタの用途

クラウドレジスタは、 CSP のデータと運用が該当する要件を満たしているかどうかを評価する監査中に使用され、意思決定プロセスを合理化します。一元化されたデータベースとして機能し、承認されたクラウドサービスを一覧表示し、CSP が取り扱うことが承認されているデータの種類に基づいて分類します。これにより、チームが組織の標準やコンプライアンス要件に整合するだけでなく、CSP を評価する作業の重複を最小限に抑えることができます。レジストリを参照することで、チームは個別のデータ管理要件に対する利用可能なサービスをすばやく特定できるため、プロジェクトの開始を早め、管理オーバーヘッドを削減できます。

3.1.5.4 リスクレベル&有効期限

固有リスクと残留リスクは通常、重要、高、中、および低などのリスクレベルで表されます。リスクは影響と発生可能性に基づいて導き出されます。リスクレベルは、レビューと監査の頻度と深度を決定します。例えば、PII (個人識別情報)[56]を扱い、重大なリスクに分類されるサービスは、中程度のリスクに分類されるサービスよりも頻繁にレビューされる可能性があります。

Provider	Service	Data Types	Risk	Expiration
ABC	Object storage	Public, sensitive	Low	Annual

[55] Aligned with the requirements included in the definition of risk register in CSA’s *Certificate of Cloud Computing Audit Knowledge* (CCAK), create a repository of the key attributes of potential and known IT risk issues.

[56] NIST (2015) PII stands for Personally Identifiable Information; Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

ABC	Virtual networks	All	Low	Annual
GHI	CRM SaaS	PII	Moderate	Quarterly

テーブル 2: クラウドレジストリの例

この架空の例では、2 つのプロバイダの 3 つの特定のサービスを示し、処理が許可されるデータ分類をリストしています。それに基づいてリスクを割り当て、必要なレビュー頻度を設定します。これにより、チームはリスク評価を加速できます。

3.1.6 リスクアセスメント、脅威インテリジェンスとモデリング

特にクラウドコンピューティングのコンテキストにおいて、脅威インテリジェンスと脅威モデリングを伴うリスク評価は、CSC のサイバーセキュリティポスチャを改善します。これには、脅威の状況とクラウド技術の両方が進化するため、継続的な取り組みと更新が必要です。組織は、CSA や MITRE が提供するようなフレームワークを活用し、SSDLC の一部として徹底した脅威モデリングを実施することで、クラウドコンピューティングに関連するリスクに対して、より適切な準備と軽減ができます。サイバーセキュリティに対するこのプロアクティブなアプローチにより、クラウドの導入は効率的、効果的、かつセキュアになります。

- **リスク対脅威:**
    - リスクは、潜在的なマイナスの結果を指す広範なカテゴリです。一方、脅威は、攻撃者にとっての機会を表します。リスクには、脆弱性やその他のセキュリティ欠陥を悪用する脅威アクターによる資産の損失、損傷、または破壊の可能性が組み込まれています。
    - 脅威はより具体的で、それらの脆弱性を悪用しようとする攻撃者の攻撃に直接関連するリスクのサブセットを表します。
- **現在の脅威の状況:**
    - 脅威の状況はダイナミックで常に進化しているため、クラウドセキュリティにおける最新の脅威について常に情報を得ることが重要です。CSP とそのサービスが実際に直面する脅威を把握することは、クラウド導入におけるリスクを効果的に評価し、軽減するための鍵となります。
- **脅威モデリング**
    - 脅威モデリングは SSDLC に不可欠な要素です。これは、構造的な脆弱性やプライバシーギャップなどの潜在的な脅威を特定し、特定のアプリケーションやシステムを保護する文脈において、その脅威を軽減する構造化されたアプローチです。

- **CSA Top Threat:**
    - CSA *Top Threats*[57]は、主要なクラウドの脅威を特定するために頻繁に更新され、特定の技法や公開された侵害の例を含みます。
- **その他の脅威インテリジェンスソース:**
    - 脅威インテリジェンスのその他の貴重なリソースは次のとおりです。
        - **MITRE ATT&CK**[58]フレームワークは戦術の包括的なマトリックスを提供します。クラウド固有のマトリックスがあります。
        - **CSA Research**[59]**:** 業界のために業界によって作成され、ベンダー中立であり、コンセンサス主導でもあります。

3.2 コンプライアンスと監査

データの完全性、可用性、および機密性を保護するための、確立された標準、法律、規制、およびポリシーに、情報システムが準拠していることを確認する、コンプライアンスと監査は不可欠です。これらのプロセスは、情報資産に対する脅威の軽減のため、脆弱性を特定する、リスクを評価する、およびコントロールを実施する目的で設計されています。

コンプライアンスには、セキュリティ慣行を規定する一連の定義済みの標準または規制の遵守が含まれます。コンプライアンスは、組織が、機密情報とシステムを保護するための定められた一連のセキュリティ対策を実装することを確実にします。

監査とは、セキュリティポリシー、標準、および規制への準拠を確認するための、記録、運用、プロセス、およびコントロールについての独立した調査です。監査は、セキュリティ対策のギャップを特定し、実装されたコントロールの有効性を検証するために役立ちます。監査には、CSC 独自の監査スタッフによって実施される内部監査と、独立した第三者によって実施される外部監査があります。定期的な監査により、コンプライアンスを確保し、セキュリティポスチャの改善を推進し、利用者やパートナーとの信頼関係を構築します。

3.2.1 コンプライアンスの種類とクラウドへの影響

クラウド環境におけるコンプライアンスは、法規制要件の網羅、国際基準、国内基準、地域基準、業界標準の遵守、および社内のポリシーや標準との整合など、多面的です。クラウドコンピューティングの

[57] CSA. (2023) Top Threats to Cloud Computing: Pandemic 11 Deep Dive
[58] MITRE. (2024) Cloud Matrix
[59] CSA. (2023) Understanding Cloud Attack Vectors

動的、分散、およびスケーラブルな特性は、コンプライアンスに関する固有の課題と懸念をもたらします。以下では、これらの側面をさらに掘り下げていきます。

3.2.1.1 コンプライアンス要件

CSC は、クラウドサービスのメリットを活用することと、自社の資産を保護し、法的および規制上の義務を果たすためのコンプライアンスの維持とを両立させる必要があります。

以下に、コンプライアンス要件に影響を与える契約要件、基準、および社内ポリシーの例を示します。

- **法的、規制、契約上の要件:**
    - クラウドサービスは、複数の裁判管轄にまたがって運営されていることが多く、法的要件や規制要件が異なる場合があります。これらの変更を追跡することは、コンプライアンスを維持するために不可欠です。
    - コンプライアンス継承とは、すでに一定のコンプライアンス基準を満たしているクラウドサービスを利用することを指します。
    - データを保存または処理する裁判管轄全体で、法規制要件の変更を継続的にモニタリングします。エンドツーエンドのコンプライアンスを確保しながら、CSP の認証を活用して、コンプライアンス継承戦略を賢く導入します。
    - 国境を越えたデータ転送を管理する法的および規制のフレームワークを遵守します。これらのフレームワークは、複数の国にまたがる業務にとって重要です。これは、国際および地域のデータ保護規制への包括的な遵守を求めます。
- **国際標準、国内標準、業界標準:**
    - コンプライアンスを証明する証拠の収集は、手動または自動で実行できます。クラウド環境では、自動化が促進されます。これは、より効率的ですが、適切なツールが必要とされます。
    - 大きな課題は、確立された標準の多くがクラウドコンピューティング固有のニーズや特性を反映するように更新されておらず、コンプライアンスにギャップが生じる可能性があることです。
    - コンプライアンスのための証拠収集の自動化ツールに投資し、効率性と正確性を強化します。クラウドコンピューティングの現実を反映した最新の標準を提唱し、開発に貢献するために、業界のフォーラムや規制機関に積極的に参加します。
- **内部ポリシーと標準:**
    - CSC は、自社の既存の内部標準やコントロールが、クラウド環境に完全に適合していないことに気付くかもしれません。包括的なガバナンスを確保するためには、これらの標準をクラウドに適応させる必要があります。

- 既存の内部標準とクラウド環境の乖離を特定するために、ギャップ分析を実施します。データレジデンシー、主権とローカリゼーション、アクセスコントロール、およびクラウドコンテキストでのインシデント対応など、クラウド固有の課題をカバーするクラウド専用のガイドラインを作成するか、既存のポリシーを適応させます。

3.2.2 クラウド関連の法規制の例

個人情報、財務データ、および重要な国家インフラストラクチャ技術など、さまざまなデータタイプを保護するために多くの法規制が存在します。処理すべき規制は無数にあり、各 CSC には固有の法的および規制要件を理解する義務があります。以下は、クラウドのセキュリティとコンプライアンスに一般的に影響する規制と業界標準の代表的な例です。

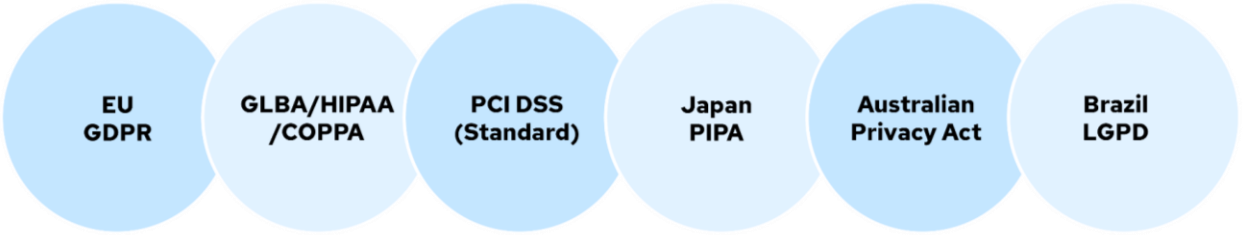


図 18: クラウドサービスに影響する主なプライバシーおよびセキュリティ規制

3.2.2.1 プライバシーに関する法律と規制

- **EU GDPR:** 個人データに対する個人の権利を重視し、データ処理には同意を求め、違反した場合には厳しい罰則を科すなど、データ保護に関する高い基準を設定しています。
- **米国の規制(CCPA/COPPA):** 特定のセクターに焦点を当てたプライバシー保護法。
  - 児童オンラインプライバシー保護法 (COPPA)
  - カリフォルニア州消費者プライバシー法 (CCPA)、および類似するその他の州レベルの法律には、データの取り扱いと保護に関する詳細な要件が定められています。
- **ブラジル LGPD:** EU の GDPR に強く基づいた一般個人データ保護法の略。個人データに対する個人の権利を重視し、データ処理には同意を求め、違反した場合には厳しい罰則を科すなど、データ保護に関する高い基準を設定しています。
- **日本の個人情報保護法、オーストラリアのプライバシー法:** ユーザーの同意、データの正確性、国境を越えたデータフローの制限に重点を置き、個人情報の収集、使用、開示を規制する国内法。

3.2.2.2 その他の関連法令

- **米国の規制:**
    - Gramm-Leach-Bliley Act (GLBA)は、 米国の金融機関に消費者情報の保護を義務付けています。
    - HIPAA（Health Insurance Portability and Accountability Act）は、データを取り扱う医療機関や保険者などが、どのように医療情報を利用・開示できるかに関する規制を設けることで、医療プライバシーを保護しています。
- **EU の法律と規制:**
    - EU Digital Operational Resilience Act (DORA)は、パブリッククラウドプラットフォームで動作する重要な金融市場インフラストラクチャの運用レジリエンスを確実にします。
    - EU AI Act は、人工知能（AI）システムの信頼性を確保するために不可欠な規制を定めています。
    - NIS 2 は、最近施行された Network and Information Systems Directive の改訂版で、EU 全域の重要なサービスのサイバーセキュリティ対策を強化します。
    - 現在提案中の EU Cybersecurity Act は、EU 機関自体のデジタル防衛を強化することを目的としています。
    - EBA Guidelines は、European Banking Authority による委託契約についての法令です。
- **中国のサイバーセキュリティ法:** 企業のセキュリティ義務について概説し、サイバー脅威に対する一般市民の認識を高め、サイバー空間を監視および規制する広範な権限を当局に与えることで、国のオンラインインフラストラクチャとデータを保護することに重点を置いています。
- **PCI DSS:** 包括的なセキュリティ対策による金融データの保護を重視する、クレジットカード会員情報を取り扱いおよび処理する組織のための、裁判管轄をまたぐ規格です。

3.2.2.3 クラウドにおけるコンプライアンス

- **セキュアな取り扱い:** 機密データへのアクセスが厳密に管理され、機密性と完全性を維持するためにそのデータが処理されることを確実にします。
- **セキュアなストレージ：** 暗号化などの保護手段を導入して、保管時および転送中のデータを保護し、適切なデータの保持および削除作業を確実にします。
- **デューケア：** 業界のベストプラクティスとセキュリティ基準に準拠し、データを脅威や脆弱性から保護します。
- **監査証跡：** 規制要件への遵守を証明し、監査を支援するために、データ処理活動の包括的な記録を維持します。

3.2.2.4 規制および標準への準拠

クラウドプロバイダは、多くの場合、認定、保証、およびその他の形式の認可によって、さまざまな規制、業界および国の標準に対する準拠を達成します。これには以下が含まれます。

- ISO/IEC 27001-2022
- ISO/IEC 27017 Information security controls for cloud computing services
- ISO/IEC 27018 - Protecting PII in the Public Clouds
- Payment Card Industry Data Security Standard (PCI DSS)
- American Institute of Certified Public Accountants (AICPA)
- Service Organization Control Reports (SOC 1 and SOC 2)
- Cloud Security Alliance STAR Certification
- Cloud Security Alliance STAR Attestation
- U.S. Federal Risk and Authorization Management Program (FedRAMP)
- Singapore Multi-Tier Cloud Security standard
- Germany Cloud Computing Compliance Criteria Catalog (C5)
- Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)
- EU Cloud Code of Conduct for GDPR

CSP が高い水準のセキュリティとデータ保護を維持するというコミットメントを示す上で、これらの認定、保証、認可は、非常に重要です。

3.2.3 コンプライアンス継承

コンプライアンス継承は、クラウドコンピューティングにおける法令順守の重要な側面を表し、さまざまな規制や業界標準を満たすために、CSP のセキュリティポスチャとコンプライアンスポスチャを活用する方法を CSC に提供します。金融サービス、医療、および機微の個人データを扱うセクターなど、厳格なデータ保護とセキュリティ基準が義務付けられている環境で、この概念は特に重要です。

クラウドコンプライアンスは通常、CSP と CSC がそれぞれコンプライアンスの特定の側面を担当する責任共有モデルに従います。コンプライアンス継承は、CSP の協力のもとにコントロールセットを取得できるようにすることで、CSC の負担を軽減することを目的としています。PCI DSS に準拠したクラウドインフラストラクチャプロバイダを考えてみましょう。同社のインフラストラクチャサービスを使用する CSC は、この一連のコントロールを継承し、インフラストラクチャレベルにおいて PCI DSS に準拠します。ただし、CSC は、このインフラストラクチャ上に構築されたソフトウェアが PCI DSS にも準拠していることを確認する追加の責任を負います。

CSP と CSC の両方が独立して監査され、それぞれのコントロールが準拠していることを確認する必要があります。

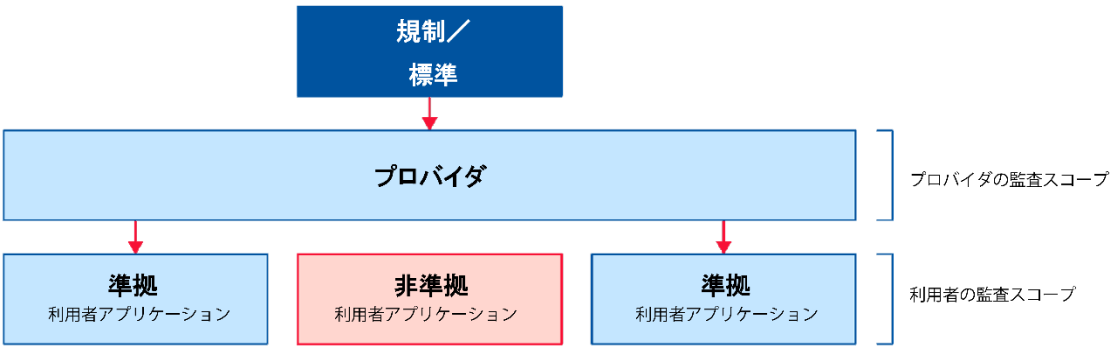


図 19: 監査のスコープ：プロバイダ対利用者の責務

3.2.3.1 コンプライアンス継承の制限

コンプライアンス継承は、一般的にコンプライアンス責任を移転しません。CSP によってデプロイされたアクティビティとコントロールを、CSC が活用できるようにするだけです。 CSC の義務の全部または一部の範囲を CSP に依存することを CSC が選択した場合でも、CSC は技術スタック全体にわたるコンプライアンスの責任を保持します。ISO 27001 や SOC 2 などの一部の標準やフレームワークでは、CSP が引き続き準拠していることを検証するために、少なくとも年次で、CSC は明確な措置を講じなければなりません。

- **プロバイダ監査のスコープ:** コンプライアンス継承モデルでは、CSP のインフラストラクチャとサービスは、特定のコンプライアンス基準に準拠していることを確認するために厳しい監査を受けます。 パススルー監査とも呼ばれる CSP のコンプライアンスを検証するこれらの監査は、CSP のインフラストラクチャとサービスを CSC 自身が監査する必要から CSC を解放します。CSP は、これら認定のコストと継続的なメンテナンスの責任を負います。
- **利用者の監査スコープ：** CSP は準拠したインフラストラクチャを提供する場合がありますが、このインフラストラクチャ上で準拠したアプリケーションを構築および維持する責任は CSC にあります。この責任の明確化は、CSP のサービスは準拠していたとしても、CSC がこのインフラストラクチャ上で開発するアプリケーションやサービスは、その準拠性について個別に評価される必要があることを意味します。
    - **準拠した利用者アプリケーション：** CSC が特定の標準や規制（PCIDSS など）に準拠した CSP のプラットフォーム上でサービスを構築する場合、CSP が提供するインフラストラクチャや運用は準拠しているとみなされ、CSC の監査スコープ外となります。これにより、CSC は自社のアプリケーションとデータ管理手法にコンプライアンスの取り組みを集中させることができます。
    - **非準拠の利用者アプリケーション：** 準拠したクラウドインフラストラクチャを利用する場合でも、アプリケーションが関連標準に準拠するように適切に設計されていないと、CSC は規制要件を満たせない可能性があります。これは、CSC のアプリケーション、

プロセス、およびデータ処理慣行がコンプライアンス要件に準拠していることを確実にするという CSC の責任の重大性を強調しています。

3.2.4 裁判管轄

クラウドのデプロイメントの多くは、さまざまな法規制の裁判管轄にまたがっている可能性があります。データのプライバシー、セキュリティ、およびその他の重要な要素をガバナンスする独自の法的および規制フレームワークを持つ複数の地域に業務がまたがると、コンプライアンスの複雑さは増大します。

複数の地域で事業を展開する CSP や CSC は、さまざまな法規制が適用される裁判管轄のマトリックスに直面することになります。この影響を受けるのは以下です。

- CSP の場所。
- CSC の場所。
- データサブジェクトの場所。
- データが保存されている場所。
- CSP/CSC 契約の法的管轄権。利害関係者の所在地とは異なる場合があります。
- それらのさまざまな場所の間の条約またはその他の法的フレームワーク。

たとえば、データが別の地域でホストされていたとしても、CSP が運営されている国で侵害通知を発行する要件が考えられます。

図 20: クラウド管轄のコンプライアンスに影響を与える要因

3.2.5 クラウド保証メカニズム

保証とは、コンプライアンスの検証に使用されるプロセスおよび方法です。保証には、さまざまな監査、適合性証明、および評価を含み、それぞれに明確な焦点と方法論があり、CSP 間で大きく異なる可能性があります。これらのプロセスでは、規制、セキュリティ、および運用基準への準拠を検証します。

用語	定義	目的	範囲	保証のレベル	焦点	例
監査	IT システム、プロセス、およびコントロールの体系的な検査	IT コントロールが効果的かつセキュアであることを合理的に保証	IT システム、セキュリティ、およびコンプライアンスに注力	高：IT コントロールの厳格な調査と検証	基準に対する IT 準拠性について独立した意見を提供	ネットワークの脆弱性とアクセスコントロールを評価する IT セキュリティ監査

適合性証明	態勢に係る声明に照らした IT プラクティスのレビュー	定められた目的、内部統制、またはシステムに照らして正確性を評価	財務諸表以外のさまざまな IT の主題を含める	中：IT プラクティスの監査の簡易版を提供	特定の IT 統制または情報を、合意された手続に照らして検証	SOC 2 は、IT 統制の評価を記載し、保証報告書を発行
保証	信頼を構築するための IT 情報の公平な評価	IT プロセスとシステムへの信頼を高める	特定の情報に限定されない、IT のさまざまな側面をカバー	IT エンゲージメントの種類によって異なる	組織の IT インフラストラクチャの信頼性とセキュリティに対する信頼の構築	評価と監査の組み合わせに基づく IT DR 計画の有効性に対する信頼の向上
評価	IT のパフォーマンス、有効性、または成果を基準に照らして評価	成功を測定し、改善すべき領域を特定し、IT 部門の意思決定に通知	IT プログラム、プロジェクト、プロセス、またはシステムに適用	コンテキストに依存します。IT コンテキストでは必ずしも保証を提供できないことがある	IT 側面の価値、有効性、成果の評価	IT DR 計画またはソフトウェア開発プロセスの有効性の評価
査定	IT プロセス、リスク、またはパフォーマンスの包括的な分析または評価	IT プラクティス、リスク、およびコンプライアンスを徹底的に評価・分析	リスク評価やコンプライアンスチェックなど、幅広い IT 関連評価に対応	具体的な評価目的と手法によって異なる	クラウド移行戦略のリスク評価の実施	IT ガバナンスフレームワークの全体的な成熟度を評価

テーブル 3: クラウド保証メカニズム：定義と目的

3.2.5.1 サードパーティプロバイダおよび監査

一部の CSC はサードパーティプロバイダの監査を利用することに慣れているかもしれませんが、クラウドコンピューティングの性質や CSP との契約によって、現地監査（on-premises audits）などが妨げられることがよくあります。CSP がマルチテナントサービスを提供している場合、現地監査をセキュリティリスクと見なす可能性がある（そして多くの場合、そうすべき）ことを、CSC は理解する必要があります。多数の利用者からの複数回の現地監査は、特にプロバイダがリソースプールの作成を共有資産に依存している場合、明らかにロジスティックスとセキュリティ上の課題をもたらします。

これらのプロバイダを利用する利用者は、自社で実施する監査よりも、第三者による保証に頼らざるを得なくなるでしょう。監査基準によっては、実際の結果は機密保持契約（NDA）の下でのみ公表される可能性があります。つまり、CSP は、リスク評価やその他の評価目的で証拠にアクセスさせる前に、法的契約を締結する必要があります。これは多くの場合、監査法人との法的または契約上の要件によるもので、CSP による企てや難読化によるものではありません。

利用者は契約上および規制上の義務を満たしているという保証を依然として必要としていることを、CSP は理解する必要があります。したがって、特に CSP が利用者による直接評価を許可していない場

合、義務を満たしていることを証明するために、厳格な第三者による監査証明を提供する必要があります。これらは、明確に定義された範囲と、評価のための特定のコントロールリストからなる業界標準に基づく必要があります。認証と監査証明を（法的に許される範囲で）公開することは、クラウドの利用者がプロバイダを評価する上で大いに役立ちます。CSA STAR Registry[60]がこれらのドキュメントを一般に公開するための中央リポジトリになります。

3.2.6 コンプライアンスアーティファクト

コンプライアンスアーティファクトは、コンプライアンス活動をサポートするために必要なログ、ドキュメント、およびその他の資料です。CSP と CSC の双方は、それぞれのアーティファクトの作成と管理に責任を持ちます。CSC は監査をサポートするために必要なアーティファクトの最終的な責任を負っているため、CSP が何を提供するかを知る必要があり、それによりギャップを埋めるためのアーティファクトを作成できます（たとえば、PaaS 上のサーバーログが利用できない可能性があるため、アプリケーションへのより堅牢なログインを構築など）。

コンプライアンスアーティファクトは、クラウド環境内における、さまざまな規制およびセキュリティ標準への準拠を示します。これらのアーティファクトは監査時に具体的な証拠となり、効果的にデータを管理しセキュアにする組織の能力を示します。

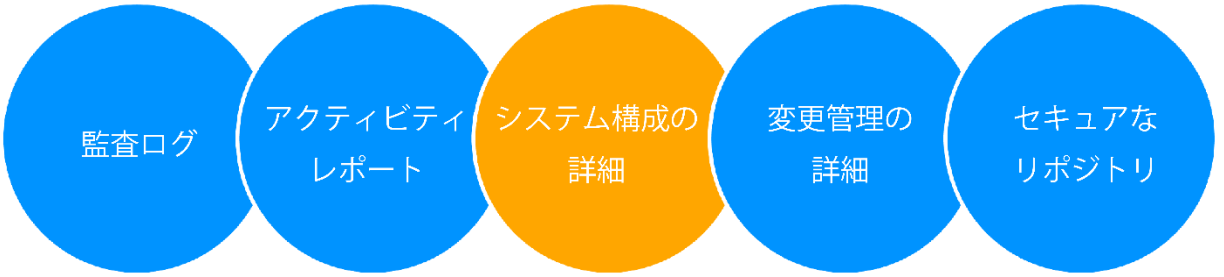


図 21: クラウド環境におけるコンプライアンスに不可欠なアーティファクト

次に、コンプライアンスアーティファクトの例を示します。

- **監査ログ：** イベント、アクション、および変更の詳細な記録
- **アクティビティレポート：**ユーザーアクティビティ、アクセスパターン、およびシステム操作をまとめたレポート。アクティビティレポートは、未認可なアクセスの特定、ユーザーアクションの追跡、および運用プラクティスがコンプライアンス要件に準拠していることの確認に役立ちます
- **システム構成の詳細:**ネットワーク構成、アクセス制御、およびセキュリティ対策などのシステム構成の文書化
- **変更管理の詳細:**アップデート、修正、パッチなど、システムに加えられた変更の記録。これらの詳細は、環境の整合性とセキュリティを維持する方法で、変更が認可され、テストされ、および実装されたことを確認するために重要です

[60] CSA. (2023) CSA Star Registry

- **セキュアなリポジトリ：**コンプライアンスアーティファクトを保存するには、データの完全性と機密性を保護するセキュアでアクセス可能なリポジトリが必要です。これらのリポジトリは、セキュリティ標準に準拠し、許可された担当者のみにアクセスを制限できる必要があります。場合によっては、これらのリポジトリの管理が CSC/CSP の境界を越える可能性があるため、アクセス制御とデータ保護対策に関する明確な合意が必要です。

3.3 ガバナンス、リスク、コンプライアンスツールと技術

GRC ツールキットには、技術的なツールと非技術的なツールの両方が含まれています。責任、契約、および維持されているリスクレジストリとサービスレジストリが保存されたリポジトリについての明確なドキュメントが含まれます。また、CSC 全体のチームのためのビジネスコンテキストと採用プロセスに合わせて調整されたフレームワークとプロセスを説明するドキュメントも含まれています。また、人間が人的なプロセスによって行うには人手がかかりすぎる作業を自動化するために使用される多種多様な技術的ツールもあります。次に、CSC が目にする可能性があるさまざまなタイプのツールと、それぞれの簡単な説明を示します。

3.3.1 ガバナンス、保証、コンプライアンスを支える非技術的なツール

非技術的なツールは、クラウドコンピューティングのガバナンス、保証、およびコンプライアンスの側面で役割を果たし、リスク管理、責任の明確化、規制要件へのコンプライアンスの確保に必要なフレームワークと方法論を組織に提供します。

非技術的なツールの例を以下に示します。

- **責任共有モデル:**
    - すでに説明したように、責任共有モデルでは、CSP と CSC の間で共有されるセキュリティ責任を明確にします。クラウド環境では、セキュリティ管理、データ保護、およびコンプライアンス義務に関連するタスクの分担を理解するのが基本です。RACI チャート（responsible(実行責任者)、 accountable(説明責任者)、 consulted(相談先)、 informed(報告先)）は、役割と責任を文書化するために使用できます。
    - データの暗号化、ネットワークセキュリティのコントロール、インシデント対応など、特定のセキュリティタスクの責任者を明確に定義できるため、セキュリティ適用範囲のギャップを防ぐことができます。
- **契約:**
    - 契約は、クラウドプロバイダと利用者との関係における法的役割、責任、および期待事項を特定します。SLA、データ処理契約、および機密保持条項などが含まれます。

- 両当事者が、彼らの義務、法的権利、および救済策を理解することを確実にし、それにより紛争やコンプライアンス違反が発生した場合の説明責任と法的措置の基礎を築きます。

- **リスクレジスタ:**
  - リスクレジスタは、特定されたすべてのリスクとその重大度、管理のためのアクションをリストした文書です。
  - 組織がリスクを体系的に優先順位付けして対処できるようにすることで、プロアクティブなリスク管理を容易にし、リスク軽減の取り組みを組織のリスク選好に合わせるようにします。
- **サードパーティのリスク管理/プロバイダー/クラウドレジスタ:**
  - サードパーティプロバイダのレジスタを保持し、それらのリスクを評価することにより、すべての外部エンティティが、潜在的なリスクやセキュリティ上の影響について評価および監視されることを確実にします。
- **Cloud security maturity model (CSMM):**
  - 業界のベンチマークに基づいて、クラウドセキュリティプログラム全体を測定および改善するための指針となります。
  - クラウドセキュリティを継続的に改善するためのロードマップを提供し、企業が弱点を特定し、時間をかけてより強力なセキュリティ対策を実施できるように支援します。
- **サービスレジストリ:**
  - サービスレジストリは、デプロイされた内部サービスに関する情報を含むデータベースです。チームが統合または使用する可能性のある動的なサービスを管理および検出するために、クラウドサービスにおいてサービスレジストリが使用されます。
  - サービスレジストリは、チームが既存のサービスを簡単に見つけて統合できるようにします。それにより、冗長性が削減され、再利用が促進されることで、サービスの相互運用性と効率性が向上します。
- **コントロールフレームワーク:**
  - これは、リスクを管理し、組織内で効果的なコントロールを実施するために使用する一連のガイドラインまたはベストプラクティスで構成されます。
  - これは、リスク管理とコントロールの実施を組織全体で標準化し、一貫性のある効果的なガバナンスの実践を確実にします。

- **モニタリングおよび監査フレームワーク:**
    - これらのフレームワークは継続的なモニタリングのためのものであり、異常やセキュリティインシデントの検出を可能にし、コントロールが意図したとおりに機能していることを確認します。
    - 潜在的なセキュリティ脅威を迅速に特定して対応する能力を強化し、規制や社内ポリシーへのコンプライアンスを確保します。
- **データ/資産の分類とカタログ:**
    - データと資産を体系的に分類することは、機密性と重要度に基づいて適切なセキュリティコントロールを適用するために役立ちます。
    - コンプライアンスとデータ保護の要件に合わせて、より機密性の高い資産に高レベルのセキュリティを適用することで、重要な情報とリソースを保護します。
- **ユーザー/エンティティのマッピング:**
    - ユーザーとエンティティを対応するデータアクセスおよび処理アクティビティにマッピングすることで、データガバナンスの維持と未認可なアクセスの防止に役立ちます。
    - マッピングは、許可された個人のみが特定のデータセットにアクセスできるようして、データ侵害やコンプライアンス違反のリスクを最小限に抑えることで、データガバナンスを強化します。

3.3.2 ガバナンス、保証、コンプライアンスを支える技術

クラウドではガバナンス、保証、およびコンプライアンスを支援するさまざまな技術が使用されています。これらの技術は、セキュリティポリシーの適用を容易にし、コンプライアンスのリアルタイム監視を可能にし、クラウドリソースの管理を自動化して、人為的ミスや設定ミスに伴うリスクを最小限に抑えます。

3.3.2.1 クラウドサービスプロバイダポリシー

CSP ポリシーは、アクセス、運用、および構成をコントロール・管理するための、クラウドプラットフォーム内に統合された予防的および技術的なルールのセットです。

CSP ポリシーの作成と適用には、組織のセキュリティ目標とクラウド環境の機能[61]を深く理解する必要があります。堅牢なセキュリティガバナンスを確保するため、CSP ポリシーをベストプラクティスや規制要件に合わせる必要があります。

3.3.2.2 予防統制と発見統制

Security Information Event Management (SIEM), Cloud Security Posture Management (CSPM), cloud-native application protection platform (CNAPP), cloud workload protection platform (CWPP), および Security Service Edge (SSE)などのツールは、セキュリティとコンプライアンスのベースラインからの逸脱を監視および管理する機能を提供します。これらのツールは、設定ミス、脆弱性、および規制基準への不適合の検出を自動化できます[62]。

3.3.2.3 Software Bill of Materials(SBOM)
SBOM は、オープンソースコンポーネントを含む、ソフトウェアアプリケーションを構成するすべてのコンポーネントの包括的なインベントリです。セキュアでコンプライアンスに準拠したソフトウェアサプライチェーンを確保するため、 SBOM は、ソフトウェアの透明性と依存関係の追跡のために重要です。SBOM を実装すると、組織はソフトウェア内のコンポーネントを追跡して検証できるため、最新の状態に保たれ、既知の脆弱性が含まれていないことを確認できます。

3.3.2.4 自動化

クラウドデプロイメントは、多くの場合、標準イメージや IaC(Infrastructure as Code)などの自動化を使用して定義および配備されます。これらは一貫性と監査可能性を高めます[63]。

サマリー

クラウド環境におけるリスク、監査、およびコンプライアンスの管理は、CSP と CSC の両方のセキュリティと整合性を確保するために重要です。このドメインは、堅牢なリスク管理フレームワークの確立、規制基準へのコンプライアンスの維持、および効果的なガバナンスのためのさまざまなツールと技術の活用に重点を置いています。

クラウドリスク管理には、クラウドサービスに関連するリスクの把握と軽減が含まれます。主なプラクティスには、CSP の評価、クラウドレジスタの維持、包括的なリスク管理戦略の実装などがあります。これらの戦略により、クラウドリスクをプロアクティブに特定、評価、管理できるようになります。

---

[61] See *Domain 4: Organization Management* for a deeper dive into how CSP policies can be crafted and enforced to align with organizational security objectives.
[62] See *Domain 4: Organization Management* for more context on these tools.
[63] Auditability is covered in context throughout all of the relevant domains covered in the CCSK.

標準、法規制の遵守にはコンプライアンスと監査が不可欠です。コンプライアンスは、セキュリティ対策が規制要件を満たしていることを確保し、監査はこれらの対策の有効性を検証します。クラウドの動的な性質上、複数の管轄区域にまたがる法律、規制、および契約上の課題に対処する必要があります。組織は、従来の環境とクラウド環境の両方でコンプライアンスを維持するため、内部ポリシーを適応させる必要があります。

コンプライアンスの継承は、CSP のコンプライアンス認定を活用して規制基準を満たします。この責任共有モデルでは、CSC はアプリケーションのコンプライアンスに対する責任を維持しながら、CSP からコンプライアンスコントロールを継承することができます。このアプローチはコンプライアンス管理を簡素化しますが、継続的な監視と検証が必要です。

GRC ツールと技術は、セキュリティポリシーとコンプライアンス要件の適用をサポートします。SIEM、CSPM、SBOM などの技術ツールとともに、責任共有モデルやリスクレジスタなどの非技術ツールを使用すると、セキュリティガバナンスを強化できます。自動化は、一貫性のある監査可能なクラウドデプロイメントを維持するために重要な役割を果たします。

監査ログ、アクティビティレポート、システム構成などのコンプライアンスのアーティファクトは、規制基準への準拠を示すために不可欠です。これらのアーティファクトのセキュアなリポジトリは、その完全性と機密性を確保し、効果的なコンプライアンス管理をサポートします。

まとめると、クラウド環境をセキュアにするには、リスク管理、コンプライアンスの遵守、および継続的な監視についての包括的なアプローチが必要です。非技術的なツールと技術的なツールの両方を活用することで、組織はクラウドのリスクを効果的に管理し、コンプライアンスを確保し、クラウドインフラストラクチャのセキュリティとレジリエンスを維持できます。

推奨

コンプライアンス、監査、および保証は継続的に行う必要があります。これらは単なる 1 つの時点でのアクティビティとして捉えるべきではなく、多くの標準や規制がこのモデルへと向かっています。 CSP と CSC の両方が常に流動的なクラウドコンピューティングには、特に当てはまります。

クラウドコンピューティングにおけるコンプライアンス、監査、および保証への継続的なアプローチの採用は、クラウドサービスの複雑さを乗り切り、CSP と CSC が規制とセキュリティの義務を確実に満たすために不可欠です。これらの推奨事項に従うことで、CSP と CSC は、よりセキュアで準拠性の高いクラウドエコシステムを育み、リスクを効果的に軽減し、またクラウドサービスへの信頼を高めることができます。

クラウドサービスプロバイダ

- **透過的なコミュニケーション：**サービスプロバイダの監査結果、 certification と attestation を以下の点に特に注意してやり取りします。

    - **評価範囲：**特定の機能やサービスなど、クラウドサービスのどの側面を評価するかを明確に定義します。
    - **対象範囲の詳細：**さまざまな場所や裁判管轄でカバーされるサービスを特定し、CSC が準拠アプリケーションをデプロイできる場所と方法を理解することを支援します。
    - **デプロイメントに関するガイドライン:**CSC が関連する標準や規制に準拠してアプリケーションやサービスを配備する方法に関するガイダンスを提供します。
    - **利用者の責任：**コンプライアンスに影響を与える可能性のあるサービス制限など、利用者が認識する必要があるその他の責任を強調します。
- **認証の維持：** CSP は、certification/attestation を長期にわたって維持し、ステータスの変更があれば積極的に伝達する必要があります。
- **継続的なコンプライアンス活動：**CSP は、ギャップ、さらにはエクスポージャーを生じさせないよう、CSC のために、継続的なコンプライアンス活動に取り組む必要があります。
- **コンプライアンスアーティファクトの提供：**CSC が独自に収集できない管理アクティビティのログなど、一般的に必要とされるコンプライアンスの証拠とアーティファクトを CSC に提供します。

クラウドサービス利用者

- **コンプライアンス義務の理解**：CSC は、クラウドにデプロイ、移行、または開発を行う前に、コンプライアンス義務を十分に理解する必要があります。この理解は、適切なクラウドサービスを選択し、規制要件に準拠して構成するために重要です。
- **プロバイダのクレデンシャルの評価:**CSP の第三者証明と認定をコンプライアンスニーズに照らして評価します。これらのクレデンシャルが特定のコンプライアンス義務に適合しているかを確認します。
- **評価範囲とカバーされている範囲：** CSP の評価範囲と認定されている範囲を明確に把握し、対象となる具体的なコントロールやサービスなどを確認します。この知識は、CSC のコンプライアンス戦略と CSP のサービスの整合性を取るために役立ちます。
- **経験豊富な監査人の選定：**可能であれば、特にパススルー監査や認定を活用して監査スコープを効果的に管理するために、クラウドコンピューティングの専門知識を持つ監査人を選択します。
- **コンプライアンスアーティファクトの管理：** プロバイダが提供するコンプライアンスアーティファクトを理解し、これらのアーティファクトの効率的な収集と管理を確実にします。CSP が残したギャップを埋めるために、必要に応じてコンプライアンスアーティファクトを作成および管理します。
- **クラウドプロバイダーレジスタの維持:** 利用するすべての CSP サービスの最新の登録レジスターを維持し、関連するコンプライアンス要件と各サービスの現在のコンプライアンス状況を記録します。CSA CCM のようなツールは、さまざまなクラウドサービス全体でコンプライアンスを管理するための構造化されたアプローチを提供することで、この活動に役立ちます。

追加のガイダンス

- CSA's Perspective on Cloud Risk Management

- CSA Code of Conduct Gap Resolution and Annex 10 to the CSA Code of Conduct for GDPR Compliance
- Top Threats to Cloud Computing: Pandemic 11 Deep Dive | CSA
- Third-Party Vendor Risk Management in Healthcare | CSA
- Mitigating Hybrid Clouds Risks | CSA
- Enterprise Resource Planning and Cloud Adoption | CSA

ドメイン 4: 組織管理

はじめに

組織管理とは、クラウドサービスプロバイダ（CSP）のセキュリティ保証の整理と検証、個々のクラウドサービスデプロイメントのセキュア化など、クラウド環境の管理全般を指します。これらのトップレベルのセキュリティ上の懸念は、配備方法にまたがり、最適な「影響範囲(blast radius)」[64]の コントロールと最適なセキュリティ管理のための構成方法を含みます。各 CSP の基盤となる技術機能を備えています。

マルチテナント環境における利用者のリソース割り当てであるテナンシーは、クラウド環境の管理において重要な役割を果たします。階層を管理し、トップレベルのセキュリティとコンプライアンスの懸念に対処するための重要なコントロールを確立することは、可視性と構造を維持するために不可欠です。

企業がマルチクラウド戦略を採用するケースが増えているため、AWS、Azure、Google Cloud などの大手 CSP が使用する階層モデルを理解することが重要です。このドメインでは、複数のクラウド導入を管理およびセキュアにするためのさまざまな組織階層モデル、その機能、およびベストプラクティスについて説明します。構造の違いを検証し、アプローチを標準化することで、クラウドサービス利用者（CSC）は、統合されたセキュリティコントロールとポリシーを実装し、クラウド管理戦略を強化し、セキュリティリスクを最小限に抑えることができます。

このドメインはまた、アイデンティティプロバイダのマッピング、CSP ポリシー、共有サービス、ハイブリッドおよびマルチクラウド環境に関する考慮事項など、組織レベルのセキュリティ管理のニュアンスも取り上げます。CSC は通常、SaaS（Software as a Service）、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）など、複数のクラウドサービスを使用します。これにハイブリッド接続や M&A（合併・買収）が組み合わさると、無秩序な成長、いわゆるクラウドの無秩序な増加を招き、コストとセキュリティリスクが増大する可能性があります。

クラウドセキュリティにおける最初のステップは、必須ではないことの無秩序な広がりに対するコントロール、フットプリントの整理、各 CSP 内だけでなく CSP 間全体でも機能するセキュリティコントロールの実装であり、個々の配備環境のセキュリティを確保することが含まれます。これは、クラウ

[64] The potential amount of damage an incident can cause.

ドサービスをより小さなコントロール単位に分割する方法を理解し、デプロイメント環境の外に存在するエンタープライズおよびテナント全体のコントロールを確立することから始まります。

学習目標

このドメインでは、次のことを学びます。

- プロバイダ内の組織レベルのセキュリティを管理します。
- 組織階層を活用して、クラウドデプロイメントの重要な側面を管理します。
- ハイブリッド/マルチクラウドの導入に関するセキュリティ上の考慮事項を確認します。
- さまざまなクラウド組織階層モデルを特定します。

4.1 組織階層モデル

クラウド環境で利用される組織階層にはさまざまなモデルがあり、各モデルは、さまざまな CSP にまたがるクラウドリソースを管理する複雑さを持ちます。CSC がクラウド技術の利用を拡大する中で、AWS、Azure、Google Cloud などの主要な CSP が使用する用語や構造の違いを理解することが重要です。本節では、これらの概念を明確にし、クラウドにおける組織構造を議論し実装するための標準化されたアプローチを提示することを目的とします。AWS、Azure、Google Cloud の階層モデルを比較することで、異なるクラウドプラットフォーム間でセキュリティコントロールとポリシーを効果的に適用し、統合されたセキュアなクラウド管理戦略を実現するための洞察を提供します。

4.1.1 定義

企業の技術的フットプリント（オンプレミス、クラウド、OT、ICS など）が客観的に複雑であるだけでなく、類似した組織構造に対して異なる CSP が使用する語彙や用語という単純な問題も伴うため、クラウド組織構築のトピックをナビゲートするのは困難な場合があります。たとえば、Amazon Web Services（AWS）では、Organization（組織）、Organization Units（組織単位）、Accounts（アカウント）などの用語が使用されています。これに対し、Microsoft Azure はその構造を、テナント、管理グループ、サブスクリプションに分類しています。Google Cloud Platform（GCP）は、そのサービスを、組織、フォルダ、プロジェクトに分類しています。

これらの用語と関連する機能は同一ではありませんが、さまざまな CSP にわたって適用可能な、汎用的セキュリティ原則を導出できるだけの十分な類似性を持っています。これらの構造の階層化は、主に複数のデプロイメントにわたってセキュリティコントロールとポリシーの一貫した適用を容易にします。

議論を単純化し、明瞭さを保つため、以下の標準化された用語セットを用います。

- 「組織」とは、CSP 内の最上位の階層構造で、AWS や GCP では組織、Azure ではテナントに該当します。
- 「グループ」は、AWS の組織単位 、Azure の管理グループ、または GCP のフォルダと同様に、デプロイメントの集合を表します。
- 「デプロイメント」とは、CSP 内の隔離された環境を指し、AWS のアカウント、Azure のサブスクリプション、GCP のプロジェクトに似ています。

以下に、主要な CSP が使用するさまざまな用語の概要を示します。

クラウドサービスプロバイダ	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
GCP	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

テーブル 4: クラウドサービスプロバイダの用語比較

使用する正確な用語は、CSP によって異なる場合があることに注意してください。例えば、「アカウント」という用語は一般的に ID とアクセス管理（IAM）を連想させ、「サブスクリプション」は定期的に電子メールの更新を受信することを指し、「フォルダ」はファイルを格納する場所として理解される可能性があります。

次の図は、さまざまな CSP にわたるクラウドリソース管理の階層構造を示しており、類似点と相違点の視覚化に役立ちます。

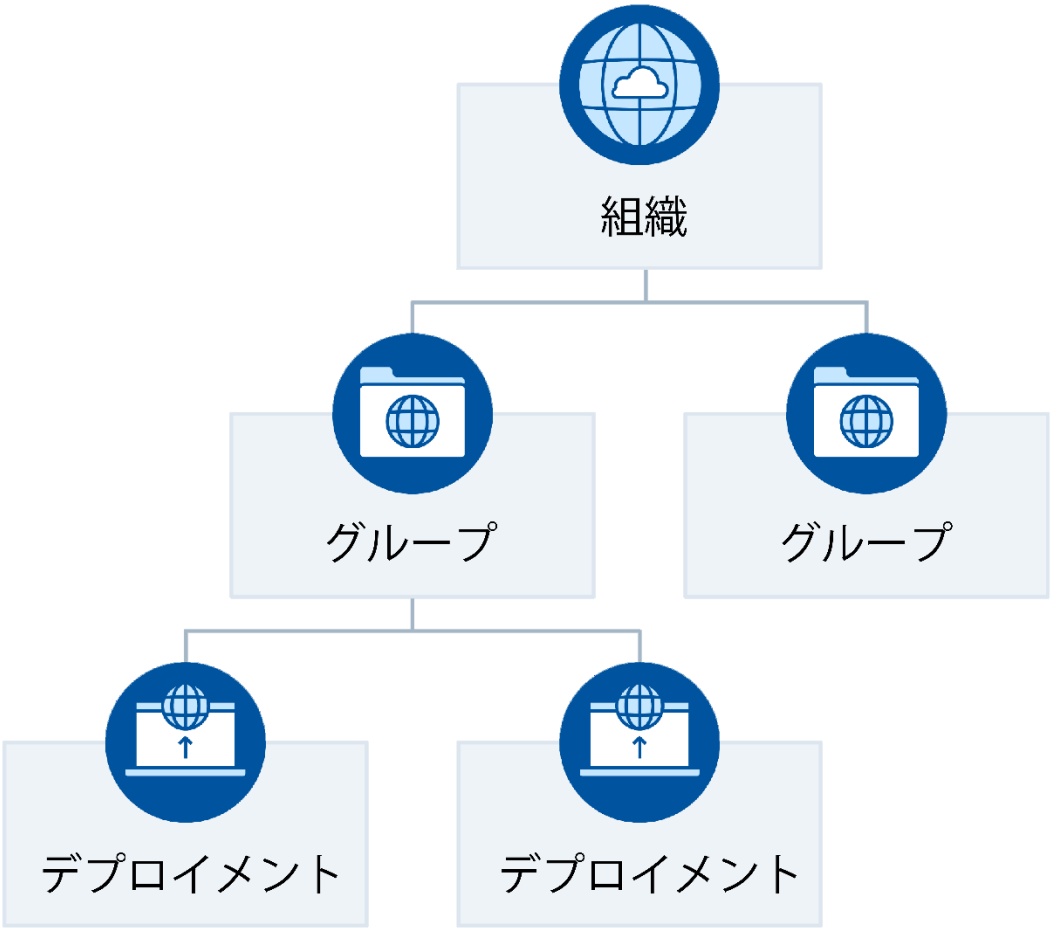


図 22: クラウドリソース管理の階層構造

複数のデプロイメントを活用することは、有害事象や侵害の影響を軽減し、CSP により課されるサービス制限を守り、異なる技術スタックの論理的な分離を促進するための戦略的なアプローチです。このアプローチは、クラウドリソースを整理するための構造化および階層化されたモデルを採用することの重要性を強調し、それによってセキュリティを強化し、クラウド環境全体でリソースの管理を合理化することが可能となります。

4.1.2 組織のセキュリティ目標

悪意のあるアクター（内部だけでなく外部も含む）から企業を保護するための一貫したセキュリティアプローチを提供することは、多層防御コントロールを構築するために重要です。目標は、技術指向とビジネス指向の両方でなければなりません。成功の測定には、リスクの軽減、ガバナンスと法令順守の向上、組織文化を組織のリーダーシップのリスク選好と一致させることが含まれます。

4.1.2.1 組織

適切に構造化されたデプロイメント階層は基本です。それは、効率的な管理と運用の明確化を促進する、クラウド環境内のリソースとサービスの配置を明確にします。

包括的なタグ付け戦略を導入し、正確なリソースレジストリを維持することで、資産の識別、分類、管理が容易になり、配備とメンテナンスのプロセスを効率化できます。

4.1.2.2 可視性

すべてのリソース構成を明確に把握することは、セキュリティと運用効率にとって重要です。この可視性により、脆弱性につながる可能性のある設定ミスを迅速に特定し、修正できます。サービスが正しい設定で実行されていることと、セキュリティのベストプラクティスに準拠していることを確認するために、サービス構成を追跡する必要があります。クラウド環境全体のアクティビティをモニタリングすることで、セキュリティの脅威を示す可能性のある異常なアクションや未認可なアクションを検知できます。

4.1.2.3 ガバナンス

認可されたユーザーのみが機密リソースにアクセスでき、権限の範囲内でアクションを実行できるようにするには、堅牢なアイデンティティとアクセス管理（IAM）プラクティスが不可欠です。ガバナンスは構成にまで及びます。構成は、セキュリティベースラインからのずれを避けるために、定義された標準に従って管理される必要があります。

4.1.2.4 一貫性

アイデンティティプロバイダや脅威検出システムなどの一元化された共有セキュリティサービスにより、クラウドランドスケープ全体で均一なセキュリティカバレッジが提供されます。「アカウントファクトリ」は、デプロイメント全体での一貫性を確保するための組織標準とセキュリティ要件に準拠したクラウドアカウントを、迅速かつ一貫して作成できます。アカウントファクトリサービスの例としては、AWS Control Tower、Azure Blueprints、Google Cloud Resource Manager などがあります。

4.1.3 クラウドサービスプロバイダ内の組織の機能

すべての IaaS および PaaS CSP は、マルチテナントの導入に不可欠な、セグメント化および分離された利用者環境を提供します。これにより、すべての CSC が、CSP のリソースプールから割り当てられた独自のセキュアで安全なリソースの集まりを持つようになります。CSC は、CSP を使用して複数の独立したデプロイメントを持ち、それぞれの環境に異なるアプリケーションをデプロイすることで、セキュリティ課題の影響範囲を効果的に制限できるという利点をすぐに理解しました。これは、各デプロイメント環境が異なる CSC に属するものと同様に分離・隔離されているため、複数の分離されたデータセンターを利用することと同様の強固なセキュリティバリアとなるためです。

しかし、こうした複数のデプロイメントを整理して管理するには課題が生じますが、CSC は CSP よりも前からこの戦略を採用していました。時が経つにつれ、CSP は複数のデプロイメントを管理およびセキュアにする機能を導入するケースが増え、このアプローチはベストプラクティスとして確立されました。

CSC が組織全体のセキュリティを大幅に強化できるようにする、すべての主要なクラウドサービスプロバイダが提供する 4 つの主な機能があります。

- グループを使用すると、CSC はデプロイメントを分離された階層に構造化できます。
- ポリシーは、グループまたはデプロイメントに適用できるセキュリティ規則です。これらは通常、特定の API 呼び出しや個々のパラメータに至るまで、機能を有効または無効にします。
- IAM の集中管理および/またはフェデレーションは、CSC のユーザーの集中管理をサポートします。
- 各 CSP は、独自の共有セキュリティサービスセットをサポートしています。これらは大きく異なりますが、中央化したロギングのサポートはほぼ常に利用可能です。

また、一部の CSP では、「アカウントファクトリ」（別名「ランディングゾーン」「アカウントベンディングマシーン」） という概念が導入されています。この機能により、通常は Infrastructure as Code (IaC) を活用し、事前構成されたセキュリティ構成とコントロールのベースラインを備えた標準化されたデプロイメントの作成が容易になります。このようなアプローチでは、個々のポリシー調整の柔軟性が低下する可能性があるものの、アカウントのプロビジョニングを迅速に行うことができます。これらの方法によって、CSC はセキュリティポスチャを強化すると同時に、複数のデプロイメントを効率的に管理し、高いレベルのセキュリティと運用効率を維持できます。

4.1.4 プロバイダ内での階層の構築

クラウド環境内にデプロイメントの全体的な階層を確立する場合、CSC は次のようなセキュリティと一般的な管理上の考慮事項を検討する必要があります。

- **階層はポリシーの効果的な使用をサポートしますか？** ポリシーは、アカウント内で実行できるアクションを定義および制限します。ほとんどの CSC は、グループまたはデプロイメントレベルでポリ

シーの適用をサポートしています。これらをグループレベルで適用すると、ネストされたグループのツリー全体とそのブランチ内のデプロイメントのセキュリティが確立されます。

- **階層は IAM 要件をサポートしますか？** ほとんどの CSP では、CSC はデプロイメント内だけでなく、グループレベルでユーザー権限を定義できます。
- **ビジネスユニットやガバナンスなどの観点から、階層は CSC の構造と互換性がありますか？** 厳密にはセキュリティ要因ではありませんが、デプロイメント階層は IAM 階層と密接に結びついていることが多く、課金やコスト管理などのさまざまなリソースに影響を与える可能性があります。

CSC は通常、以下の 3 つのモデルのいずれかを採用して階層を定義しますが、それぞれに利点と運用上の影響があります。単一のモデルが普遍的に優れているわけではなく、CSC によっては、運用実態を最もよく反映している異なるモデルの要素を組み合わせる場合もあります。

- **ビジネスユニットおよびアプリケーションベース：** このモデルでは、クラウドの階層はビジネスユニットを頂点とし、次にこれらのユニット内のアプリケーション、そして環境（本番環境と開発環境など）によって構成されます。この配置は、ビジネスユニットに焦点を当てた IAM 階層とよく一致していますが、クラウド機能がビジネスユニットやアプリケーションと密接に一致していない限り、ポリシー管理が非効率となる可能性があります。
- **環境ベース：** このモデルでは、開発環境、本番環境、テスト環境などの環境が階層の最上位に位置づけられ、次にビジネスユニットまたはアプリケーションが配置されます。このアプローチは、ポリシー管理に有益であり、さなざまな環境のベースラインセキュリティおよび運用ポリシーを確立できます。しかし、IAM 階層や課金およびコスト管理のニーズとあまりうまく整合しない可能性があります。
- **地域ベース:** グローバルに事業を展開する CSC にとって、地域ベースのモデルが最適な構造です。まず、地理的な地域（EMEA、NA、特定の国など）が上位に表示されます。その後、下位レベルのビジネスユニットや環境を統合します。この構造は、各地域に固有の多様なセキュリティ要件や規制要件に直面しているグローバル CSC に有益な場合が多くあります。

必須ではありませんが、ほとんどの CSC では、CSP ごとに 1 つの組織を維持することが最適です。ただし、国際的な規制要件やセキュリティ要件を満たす場合や、1 つの CSC 内でのデプロイメントで CSP のサービス制限を超える大規模な組織など、複数の組織やテナントをサポートする必要があるシナリオもあります。また、これらのチームがインフラストラクチャ全体にデプロイする共有サービスに対応するため、運用とセキュリティの専用ブランチを階層に含めることも一般的です。このクラウドデプロイメントの戦略的組織により、CSC はセキュリティ、コンプライアンス、および運用効率を効果的に管理できます。

ゼロトラストアーキテクチャを検討する場合、高度な成熟度または最適な成熟度を達成するには、この 3 つの要素の一部が必要です。ポリシーの管理および適用ポイントでは、3 つの要素すべてから動的に考慮する必要があります[65]。

[65] Additional material on Zero Trust is provided in Domain 12: *Related Technologies & Strategies*. Context-specific material is also provided on Domain 2: *Cloud Governance & Strategies*, Domain 4: *Organization, Tenancy, & Enterprise Management*, Domain 5: *Identity and Access Management*, and Domain 7: *Infrastructure & Networking*.

4.2 組織レベルのセキュリティ管理

クラウドと従来のインフラストラクチャの最も影響の大きな違いの 1 つは、クラウドでは通常、チームがデータセンター全体に相当する仮想環境を作成および管理できることです。物理的な施設内で作業するために従来のインフラストラクチャで依存していた、ネットワーキングチーム、サーバチームなど、多くの従来のサイロは、本質的に必要ありません。確かに、すべてのクラウドは依然としてデータセンターで実行されますが、CSC が物理層を見たり操作したりすることはほとんどなく、Web インターフェースと API コールでネットワーク全体とアプリケーションスタックを作成します。

クラウドセキュリティのゴールは、クラウドコンピューティングのメリットを軽減または排除する摩擦を生じさせることなく、許容できるリスクを維持することです。ビジネス目標を阻害することなく、クラウドフットプリントのコントロールを維持することが重要です。CSP は、ネットワークやアプリケーションのセキュリティなどの従来のセキュリティ領域以外のガバナンスとセキュリティをサポートするさまざまな機能を提供します。これは、明確に定義されたテナント構造から始まり、追加のコントロールとして拡張できます。

4.2.1 アイデンティティプロバイダとユーザー/グループ/ロールのマッピング

アイデンティティプロバイダ（IdP）は、ユーザーのアイデンティティと認証を管理する中央集中型のシステムです。個別のクラウドデプロイメントとは切り離されているため、SaaS プラットフォームなど、さまざまなクラウドサービスで単一のアイデンティティを使用できます。IdP とユーザー/グループ/ロールのマッピングは、デプロイメントアクセスを定義するために使用されます。これはデプロイメントの外に存在する IAM ですが、デプロイメント内に追加の IAM[66]があります。組織マネジメントの観点では、次の 2 つの重要な要素を考慮する必要があります。

- 組織の「root」へのアクセスを最小限に抑えます。その目的は、階層の下位にあるデプロイメントを改変・アクセスしたり、連鎖的な影響やデプロイメントへの権限昇格の可能性のある共有サービスを改変できる高レベルのアクセス権を持つ個人をできるだけ少なくすることです。
- デプロイメントを作成できるユーザーとその方法を制限しますが、摩擦の小さいプロセスをサポートし、チームがポリシーに従って新しいアカウントを簡単に取得できるようにします。たとえば、そのチームの階層のブランチに、要求されたタイプ（開発、サンドボックス、本番環境など）の適切に構成されたアカウントを作成するアカウントファクトリを設定します。

IdP は、1 つの CSP 内でセットアップされた場合でも、複数の CSP や SaaS プラットフォームで使用できます。IdP はユーザー、グループ、およびロールのマッピングを定義します。これらのマッピングはフェデレーションプロセス中に CSP と共有され、CSP の IAM システムはこれらのマッピングに基づいて

[66] Additional material on IAM is provided in Domain 5: *Identity and Access Management*.

権限を割り当てます。さらに、ビジネスユニットなどの属性を使用して、アクセスコントロールを細かく設定できます。CSP によっては、これらのマッピングを組織の階層に合わせることができます。

4.2.2 クラウドサービスプロバイダ(組織)ポリシー

ほとんどの CSP において、組織ポリシー（「組織ポリシータイプ」と呼ばれることもあります）は、デプロイメントまたはグループレベルでデプロイメントのサービスを有効にしたり無効にしたりできる構造です。一部の CSP は、ポリシー違反を特定し、正しい設定を復元して自動的に修正する検知ポリシーまたは修正ポリシーもサポートしています。修正および検知ポリシーは、CSP のオーケストレーションエンジンが複数のリソースを調整する複数のステップを含み、かつ、個々のステップでは判断が難しい場合に便利です。たとえば、リソースを作成しタグを追加する場合には、プロバイダ内の 2 つ以上の API 呼び出しが含まれる場合があります。タグが適用されていない場合、修正コントロールは作成後にリソースを削除する可能性があります。一方、予防コントロールは、最初のリソース作成ステップでタグが適用されているかどうかを評価できないため、失敗します。

ポリシーは、デプロイメントから独立したまま、デプロイメントのセキュリティパラメータを定義できることで注目に値します。この外部的な位置づけにより、デプロイメントを完全に制御できる管理者であっても、これらのポリシーを変更または削除できないようにします。

ポリシーは、次のようなさまざまなシナリオでアプリケーションを判断します。

- 未承認のプラットフォームサービスの導入禁止など、特定のサービスを有効化および無効化します。
- 特定の API 呼び出しをブロックして、未認可な操作や有害な操作を防ぎます。
- 地理的な規制要件に準拠し、データレジデンシーと主権要件を維持するために地域を選択できないようにします。
- 許可されたネットワークソース（IP アドレスなど）からの特定の API コールのみを許可するなどの条件を定義します。ただし、これには CSP レベルとサービスレベルの両方のサポートが必要であり、プロバイダ間で一貫性のない機能の 1 つとなっています。
- IAM プラクティスを強化し、組織レベルのアクセスと運用ツールをセキュアにします。これには、デプロイメント管理者による重要な可視性と管理用アカウントへのアクセスを制限することを防ぐことも含まれます（管理者のクレデンシャルが侵害された場合など）。

CSP ポリシーは、そのスコープに基づいて 3 つのレベルに分類できます。

- **組織全体のポリシーは、**CSC によって定義され、すべてのデプロイメントに適用されます。通常、この分類には、このような広範な規模で例外を管理するという課題があるため、限られたポリシーのセットが含まれます。

- **グループレベルのポリシーは、**特定のグループ内のすべてのデプロイメントを対象とします。このレベルは、ポリシーの適用に最も一般的に使用されます。このレベルのポリシーは、特にサブグループに適用される場合に、相互に積み重ね、強化することができます。CSP は組み合わせた一連の

ポリシーを適用します。アクションを拒否するポリシーは、通常、上位レベルの許可ポリシーよりも優先されます。

- **デプロイメントレベルのポリシーは、**個々のデプロイメントに合わせて調整されるため、セキュリティを正確に調整できます。一般に、グループレベルでポリシーを適用する方が優れた管理手法と見なされますが、特定のシナリオでは、特に具体的できめ細かいセキュリティ要件を持つデプロイメントにおいて、デプロイメントレベルのポリシーが必要になります。

では、メインアカウントに追加されたすべてのユーザーにコントロールを設定する、階層の一番上のポリシーコントロールを具体的に適用する方法を見てみましょう。サービスコントロールポリシー（SCP）を使用すると、メインアカウントに対してアクセスおよび使用できるサービスや機能を特定およびコントロールできます。（CSP によっては、これを組織、テナント、テナンシーと呼びます）。

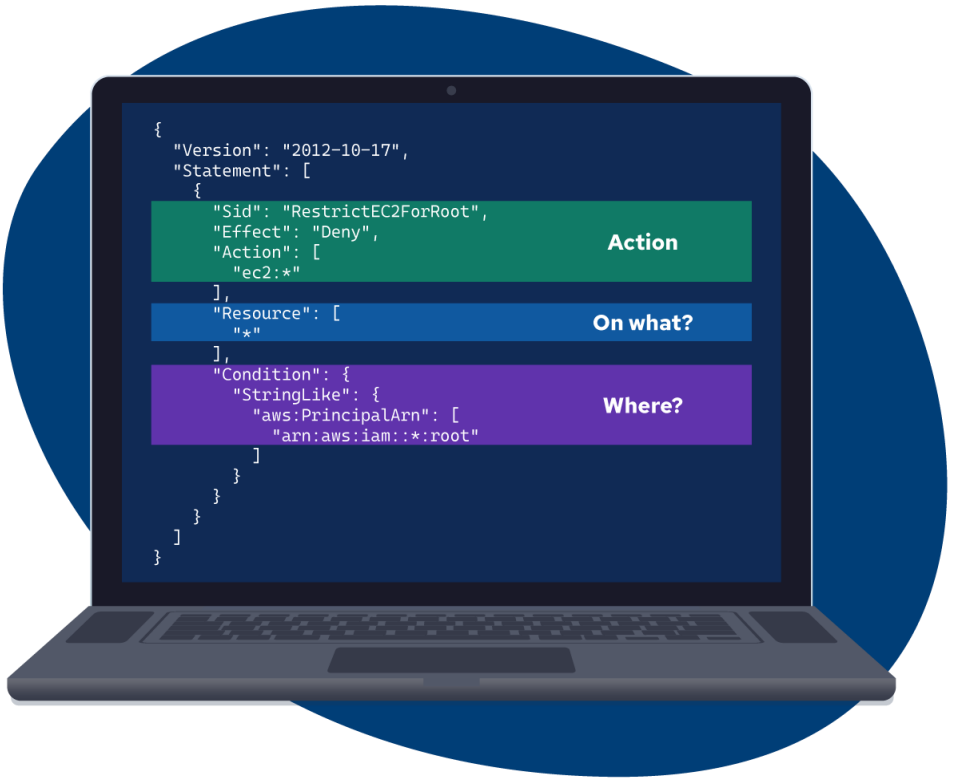


図 23: root ユーザーのアクションを制限する AWS SCP の例

図の例では、AWS SCP が AWS Organization の階層の最上位に適用され、すべてのメンバーアカウントにわたって一貫して権限をコントロールしています。SCP は個々のアカウントに直接権限を与えるものではありません。代わりに、アカウントで可能なアクションのガードレールまたはリミットを定義します。

SCP を使用すると、組織内のすべてのデプロイメントでセキュリティコントロールを一元的に管理および実施できます。これらのポリシーは、ガードレールを確立し、セキュリティ標準に一貫して準拠するための強力なメカニズムを提供します。具体的には、SCP にはいくつかの重要な特徴があります。

- **パーミッションの構造:** SCP は 、「拒否リスト」アプローチを使用して、許可されたサービスとアクションを明示的に指定し、その他すべてを暗黙的に拒否します。
- **施行：** SCP は組織レベルで制限を設定し、個々のユーザーまたはロールに付与された許可 IAM ポリシーを上書きします。
- **階層:** SCP は IAM ポリシーと連携し、CSC の AWS アカウント全体にわたる最大権限を定義します。
- **一般的な使用例:** SCP は多くの場合、セキュリティとコンプライアンスの基準を適用し、組織全体の特定のサービスや機能へのアクセスを制限します。

4.2.3 共通する組織共有サービス

一元的なロギングとセキュリティテレメトリにより、さまざまなデプロイメントや地域からのフィードを複雑で手動による転送ではなく、必要とされるセキュリティフィードを 1 つの宛先に収集することを支援します。これは、効果的なセキュリティ監視、脅威の検出、分析、およびコンプライアンスのために必要です。また、テレメトリを Security Information and Event Management（SIEM）プラットフォームやセキュリティデータレイク[67]に送信する際にも非常に有用です。

CSP 脅威検出サービス（AWS GuardDuty[68]など）は、クラウド環境内の悪意のある活動や未認可な行動を継続的に監視します。これらのサービスは、潜在的な脅威をリアルタイムで特定し、迅速な対応でリスクを軽減してクラウド資産を守ることで、デプロイメントとワークロードを保護するように設計されています。

タギングポリシーと標準化は、多くの場合、コスト配分（どの内部チームがリソースについて支払うべきかを特定するため）によって推進されますが、IAM 戦略の一環として ABAC（属性ベースのアクセス制御）を実装する際にも役立ちます[69]。

これらのツールはそれぞれ CSC の組織階層にマッピングされ、グループとデプロイメントのセキュリティ要件を満たすように調整される必要があります。例えば、開発環境と本番環境には異なるポリシーが適用されるのが一般的です。本番環境はより厳重にロックダウンされますが、インターネット公開リソースではより多く許可されます。また、開発環境ではクラウドサービスをよりオープンに使用できますが、オープンなインターネット公開リソースは厳しく制限または禁止されます。

必ずしも必要なセキュリティコントロールではありませんが、組織レベルのセキュリティを実装する上で非常に役立つツールが他に 2 つあります。

- **アカウントファクトリ**は、新しいクラウドデプロイメントを作成するための自動化プラットフォームです。この用語は、AWS アカウントの作成に関して初めて登場し、他の CSP と作業する場合で

[67] Additional material on security monitoring for data lakes is provided in Domain 6: *Security Monitoring*.

[68] AWS. (2024) Amazon GuardDuty features

[69] Additional material on IAM is provided in Domain 5: *Identity and Access Management*.

も、一般的に使用されています。アカウントファクトリは新しいデプロイメントを作成し、開始時の構成を定義します。これらは、必要なセキュリティコントロールと構成が最初から実装されていることを確かにする、セキュリティのための強力なツールです。

- **IaC テンプレート**は、単一のサービスの構成から複雑なアプリケーションスタック全体まで、あらゆるものを定義します。通常、アカウントファクトリの中核となりますが、最新の開発およびデプロイメントプロセスでも幅広く使用されています。セキュリティチームは、スタックをデプロイし、セキュアなベースライン構成を提供し、セキュリティコントロールをプロジェクトに統合するために、IaC テンプレートを活用できます。

可能な限り、組織レベルのセキュリティは組織/テナントのルート外で管理する必要があります。日常的に使用するサードパーティ製ツールや CSP ツールは、専用のセキュリティデプロイメントに分離する必要があります。これにより、組織階層の最上位が侵害され、すべてのデプロイメントに影響を与えるために利用される可能性が低くなります。

4.2.4 統合されたクラウドセキュリティおよび管理プラットフォーム

Cloud security posture management（CSPM）ツールは、API を使用して CSP に接続し、クラウドリソースの現在の構成を評価します。それらはマネージメントプレーンレベルでポスチャ/構成を評価しますが、仮想マシンのようなリソースに接続して OS や内部構成を調べることはありません。 Cloud workload protection platform（CWPP）は、ワークロード（VM、コンテナ、またはサーバーレス構成）を評価するためのさまざまな技術を使用するツールです。

Cloud-native application protection platform(CNAPP) は、CSPM と CWPP を組み合わせたもので、IaC コードスキャンやクラウドデータリポジトリ (CDR) のような他の機能を含む場合もあります。

CSPM の基本的な機能はインベントリ機能です。これには、クラウド環境内のすべての資産を識別する詳細なプロセスが含まれます。このプロセスには、サーバ、ストレージソリューション、データベース、さまざまなサービス構成など、多種多様なリソースが含まれます。また、時間の経過に伴う変化を追跡して特定することもあります。次の図は、CSPM のコア機能を示しています。

図 24: Cloud security posture management（CSPM）のコア機能

リソース構成評価は、CSPM ツールにより実行される、次に重要な機能です。これには、クラウドリソースが確立されたセキュリティのベストプラクティスと標準に準拠していることを確認する構成の調査が含まれます。CSPM ツールは、良く知られている業界のベンチマークや特定の内部ポリシーと、リソース設定を比較することで設定ミスを検出できるため、潜在的なセキュリティリスクを軽減できます。

サービス構成監視は、リソース構成機能を補完します。クラウドサービスの構成がセキュアで、セキュリティとコンプライアンスの期待に準拠していることを確認することに重点を置いています。クラウド

サービスは新しい機能によって継続的に更新および拡張されるため、セキュアな環境を維持するために定期的な構成のレビューが必要になることから、これは特に重要です。

設定ミスの検出は CSPM ソリューションのコア機能であり、クラウドのセキュリティに重大な脅威をもたらす可能性がある構成エラーを特定することを目的としています。これらの設定ミスを迅速に検出することで、CSC は設定ミスを迅速に修正することができ、攻撃者によるエクスプロイトの機会を減らすことができます。

次の表は、CSPM と CNAPP の主な違いと使用例を示し、それぞれの明確なスコープと機能を示しています。

	CSPM	CNAPP
スコープ	次のような幅広いクラウドセキュリティの側面：	クラウドネイティブアプリケーションに特に焦点を当て、次のことへ取り組む：
	インフラストラクチャの構成：サーバ、ネットワーク、およびストレージの適切なセットアップ	アプリケーション開発のセキュリティ：開発時にセキュリティをコードに組み込む
	アクセスコントロール：ユーザー権限と認証メカニズムの管理	デプロイメントのセキュリティ：セキュアなデプロイメントとランタイムな保護の確保
	データ暗号化：データ保存中と移動中の暗号化の実装	脅威インテリジェンスの統合：重大な脆弱性の優先順位付け
	ロギングとモニタリング：継続的な監視のためのログとアラートの設定	コンプライアンス管理の一元化：標準への準拠の確保
	コンプライアンス監査：業界標準への準拠チェック	パーミッションコントロール：最小特権アクセスの実施
	IAM：ユーザーとアイデンティティ管理	DevOps のセキュリティをシフトレフト：プロセスの初期段階での開発者とのコラボレーション
	ネットワークセキュリティグループ(NSG)：ファイアウォールルールの定義	包括的なクラウドワークロード保護：脆弱性の検出
	シークレット管理：シークレット情報の保護	使いやすさ：セキュリティツールスタックの簡素化
	パッチ管理：ソフトウェアを最新の状態に保つ	洞察の深さと幅:洞察の隙間をなくす
機能性	設定ミスの検出 - 公開されているリソースの特定 - コンプライアンスの管理	クラウドネイティブアプリを開始から導入まで保護 - CSPM 機能とワークロードセキュリティを統合 - 継続的インテグレーション/継続的デプロイ（CI/CD）パイプラインの統合を含む
主な違い	インフラストラクチャ重視 主に事後対応型 ポリシーの実施に重点を置く 他のツールとの統合が必要になる可能性	アプリケーション重視 プロアクティブと予防 脅威の検出と対応に重点を置く より総合的な統合ビューを提供

オーディエンス	主に、セキュリティチームとコンプライアンス担当者	DevOps、セキュリティ、および開発チーム

テーブル 5: CSPM 対 CNAPP:主な違いと使用例

コンプライアンス管理は、CSPM のもう 1 つの重要な機能です。さまざまな標準や規制の枠組みの準拠に関する評価プロセスを自動化します。この自動化により、コンプライアンス監査に伴う手作業が大幅に削減され、コンプライアンス状況の継続的な監視が可能になります。

CWPP は、単なる 1 つの時点での構成チェック以上のランタイムセキュリティをクラウド環境に提供します。ホストベースのセンサーを活用することで、ワークロードを可視化し、脅威や悪意のあるアクティビティを監視します。統合型の脅威インテリジェンスにより、既知のアクターを検知することができます。また、ファイアウォールでのブロックなどの自動アクションにより、攻撃を防ぐことができます。リソースが拡張しても継続的な保護が維持されます。全体として、CWPP は、構成チェックとランタイムの監視、可視性、および応答を組み合わせることで、クラウドワークロードのライフサイクル全体へのセキュリティを実現します。

CNAPP は、クラウドセキュリティに対するより包括的なアプローチであり、複数の機能を兼ね備えています。CNAPP は、開発ライフサイクル全体およびクラウドインフラストラクチャ全体でクラウドネイティブアプリケーションを保護するように設計されています。通常、CSPM 機能とワークロードのセキュリティ対策、および CI/CD パイプラインとの統合などの追加機能を統合します。このアプローチは、クラウドベースの運用に固有の広範なセキュリティ考慮事項を一元化します。

4.3 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

今日の多様な IT ランドスケープにおいて、CSC は多くの場合、運用ニーズを満たすためにハイブリッドとマルチクラウドの両方の環境に依存しています。ハイブリッドクラウドのデプロイメントは、オンプレミスのデータセンターとパブリッククラウドサービスを接続することで、柔軟性と拡張性を強化すると同時に、固有のセキュリティ課題を与えます。一方、マルチクラウド戦略では、複数の CSP を使用して、ベンダーロックインを回避し、パフォーマンスを最適化しますが、セキュリティ管理の複雑さも増します。このセクションでは、効果的な組織管理、IAM、ネットワークセキュリティ、およびセキュリティツールの戦略的使用に焦点を当て、ハイブリッドおよびマルチクラウド環境のセキュア化に関する主な考慮事項について説明します。これらの側面を理解することは、相互接続された多様なクラウドインフラストラクチャ全体で堅牢なセキュリティを維持するために重要です。

4.3.1 ハイブリッドクラウドセキュリティのための組織管理

ハイブリッドクラウドは、仮想プライベートネットワーク（VPN）または専用ネットワークリンクを使用して、既存のデータセンターや施設を CSP に接続します。ハイブリッドクラウドは、以前はネットワークセキュリティの観点だけで考えられていましたが、CSP はその機能を拡張し続けています。たとえば、次のようなものがあります。

1. CSP サービスを専用ハードウェアを用いるデータセンターにデプロイする。たとえば、仮想マシンやデータベースで、CSP が施設内で使用しているものと類似または同じ技術スタックを使用可能。
2. 管理ツールを拡張し、通常はエージェントを介して、クラウドマネージメントプレーンからデータセンター内のリソース(仮想または物理)を管理。
3. データセンターで使用する ID 構成の拡張。

一般的な戦略として、優れたクラウドとデータセンターのセキュリティは、優れたハイブリッドクラウドセキュリティにつながります。どちらかが弱い場合は、それが他方にまで広がらないように、それらの弱点を分離し、区分することに集中します。

ハイブリッドクラウドのセキュリティで最初に注目する 2 つの分野は、IAM とネットワーキングです。アイデンティティプロバイダが侵害されると、両方の環境に影響が及びます。どちらかの側のネットワークセキュリティが弱いと、攻撃の影響範囲が拡大する可能性があります。クラウドが弱点だと思い込まないでください。攻撃者は現在、データセンターからクラウドデプロイメントへの橋渡し方法を模索しています。IAM とクラウドは、2 つの環境をつなぐ最も一般的なタッチポイントです。たとえば、SSH 鍵が両方の環境で共有され、データセンターの侵害後にクラウドのワークロードが公開される可能性や、その逆もあります。

対照的に、ポリシーやツールを含め各環境間のセキュリティの標準化は避けてください。これがハイブリッドクラウドの主な落とし穴です。クラウドは、データセンターで使用される従来のテクノロジーとは根本的に異なるため、単一のコントロールセットを実行しようとするとギャップが生じ、障害が発生します。適切なジョブに適切なツールを使用することが重要です。

クラウド環境とデータセンター環境の異なる性質は、2 つ目の落とし穴を生み出します。ハイブリッドクラウドの無秩序な増加です。従来のインフラストラクチャは硬直的で、パブリック CSP と比較して相対的にリソースが不足しています。これは常に当てはまるわけではありませんが、一般的に最大規模の CSC を除くすべての CSC にほぼ当てはまります。最もモダナイズされたデータセンターを除くすべてのデータセンターは、IP アドレス範囲や、ネットワークアーキテクチャがプリセットされており、静的 IP アドレス上で長時間実行されるワークロードの割合が大きくなる傾向があります。一方、クラウドはより短期間で、境界が少なく、より分散された組織構造で運用されており、より小規模なデータセンターの集団（組織階層に関する前述の推奨事項による）に近いです。

ハイブリッドクラウドの無秩序な広がりとは、少数のデータセンターを多数のクラウドデプロイメント環境に直接接続する際に生じる複雑さです。明確に言うと、これは特定のデータセンターから複数のクラウドデプロイメントへの大量の VPN または専用ネットワークリンクを直接指します。また、複数のオンプレミスの ID プロバイダを複数のクラウドデプロイメントに接続することも含まれており、多くの場

合、社内の IAM 管理や M&A が不十分であることが原因です。この複雑さは、さらなるセキュリティ上の課題を生み出します。重要なハイブリッドクラウドのセキュリティ戦略により、無秩序な広がりを可能な限り最小限に抑えます。

効果的なハイブリッドクラウドのセキュリティは、オンプレミスとクラウドの両方にわたる強固なセキュリティ基盤から始まり、環境間の接続を慎重に整理して管理します。セキュアに開始し、タッチポイントを知り、影響範囲を管理します。

4.3.2 マルチクラウドセキュリティのための組織管理

複数の IaaS/PaaS CSP に移行すること、特に単一の CSP のサービス提供が成熟する前に移行する場合には、セキュリティ上の大きな課題が生じます。すべての CSP は、最も基本的な技術レベルにおいて本質的に異なり、効果的なセキュリティを実現するには、各 CSP およびサービス特有の特性を深く理解する必要があります。また、共有セキュリティサービスで複数の CSP をサポートすることは、最も成熟した CSC を除くすべての組織にとって非常に困難です。CSC は、プライマリ CSP に効果的かつ効率的なセキュリティプログラムを確立するまで、2 つ目の IaaS CSP に移行すべきではありません。

この推奨事項は、ほとんどの CSC が従うことが困難です。単一の IaaS CSP に焦点を当てた厳密なガバナンスが実施されている CSC であっても、M&A やビジネス関係/パートナーの要件により、追加の CSP を使用する可能性があります。マルチクラウドは非常に困難なセキュリティ上の課題ですが、十分な人員配置、組織の管理戦略、および実際にマルチクラウド向けに設計された主要なセキュリティ共有サービスによって管理することができます。

マルチクラウドのよくある誤解の 1 つは、クラウドに依存しないコンテナ戦略は、CSC が任意の時点で任意の CSP を選択することを可能とし、おそらく動的なコスト管理を可能にする、完全にポータブルなワークロードをサポートするということです。実際には、クラウドに依存しない実装の実現には大きな障害があります。これらは、セキュリティ上の課題と同じくらい運用上の課題があります。

- コンテナはワークロードのポータビリティを生み出しますが、管理インフラストラクチャのポータビリティは生み出しません。コンテナのランタイム環境とオーケストレーション環境を構築するには、依然としてかなりのオーバーヘッドが必要です。
- 共有サービスは、完全にステートレスでコンテナ化されていない限り、通常はポータビリティが低いです。データベース、メッセージ・キュー、通知バスなど、最新のアプリケーションの根幹をなすサービスは、通常、専用でポータビリティのないリソース上の CSP サービスの方が優れています。
- CSP の PaaS サービスによって提供される経済的、セキュリティ的、および運用上のメリットを失う可能性があります。

4.3.3 IaaS/PaaS マルチクラウドのための組織管理

クラウドインフラストラクチャの複雑さに対処している CSC は、IaaS デプロイメントにおける CSP の使用に関して、さまざまな戦略を採用することがよくあります。これらの戦略は、CSC の運用ニーズ、成熟度、および戦略的ゴールに基づいて、複数の CSP とのさまざまなレベルのエンゲージメントを反映した 3 つの異なるアプローチに大別されます。

マルチクラウドへの取り組みには、次の 3 つの戦略があります。

- **単一のプロバイダ：** CSC は IaaS のデプロイメントに 1 つの CSP を使用します。M&A によって CSP が追加された場合、そのデプロイメントはプライマリ CSP に移行されます。
- **プライマリ/セカンダリプロバイダ:** すべての新規デプロイメントは、CSC のプライマリクラウドフットプリントを表すプライマリ CSP に行われます。追加の CSP は、限定/分離されたデプロイメントのためにサポートされます。これらのデプロイメントは、ビジネス上または技術的なニーズがプライマリプロバイダで対応できない場合のみ、承認されるべきです。また、必要性に応じて、M&A もサポートします。セキュリティと運用管理の複雑さを軽減するために、セカンダリプロバイダは厳密にロックダウンされ、可能な限り最小のサービスセットを使用します。
- **マルチクラウドの完全サポート：** CSC は 2 つ以上の主要な CSP を等しくサポートします。

理想的な世界では、CSC はその成熟度に合わせて最適な戦略を選択します。 CSC は、1 つのプロバイダから開始し、必要に応じ、追加の CSP により区画化された島を選択的にサポートし、最終的には複数の CSP をサポートできるほどに成熟します。以上は我々の推奨事項ですが、我々は、多くの CSC は、実際の現実から社内政治やビジネス関係までのさまざまな理由から、期待される成熟度レベルに達する前にマルチクラウドのサポートを余儀なくされていることも理解しています。

ただし、マルチクラウド導入への道のりは必ずしも直線的ではなく、CSC の対応状況によってのみ推進されるわけでもありません。多くの場合、外部要因によってマルチクラウド戦略への移行が促進され、CSC は理想的な成熟度レベルに達する前にマルチクラウドの複雑さに対処する必要性に迫られます。この現実は、ビジネス、テクノロジー、および脅威状況の非常に動的な性質に対応するために、適応可能で拡張可能なクラウド管理手法とゼロトラストなどのセキュリティ戦略の必要性を強調しています。

4.3.3.1 IaaS と PaaS マルチクラウド向けツールおよび人員配置

ハイブリッドクラウドと同様に、適切なジョブに適切なツールを使用するなど、マルチクラウドのセキュリティは、各 CSP 内での良好なセキュリティから始まります。このドメインを通じて、これらのツールについて説明します。この部分は、マルチクラウドセキュリティで重要な役割を果たすことができます。

- **IAM/SSO/Federated Identity Broker:** クラウドのセキュリティ不備の大半は IAM が関係しています。堅固なアイデンティティプロバイダから始めることは、マルチクラウドのセキュリティにとって重要です。アイデンティティプロバイダによっては、シングルサインオン (SSO) 接続と、複数のプロバイダおよびデプロイメントへのグループ/ロールのマッピングを一元化および正規化するために、Federated Identity Broker が必要になる場合があります。

- **クラウドにフォーカスした SIEM:** 全てのプロバイダは、 CSP 毎にそれぞれ異なる複数のソースと形式を持った、独自のセキュリティテレメトリの範囲を持ちます。主要な CSP（訳注：原文は CSPS となっているが、CSPs の間違いと思われる）と簡単に統合できるように設計されたツールには、さまざまな事前にビルド済みの脅威検出機能も含まれているため、マルチクラウドサポートの負担を軽減できます。
- **CSPM:** CSPM は進化するカテゴリであり、他の新規または既存の製品カテゴリにまで浸透するような機能拡張を伴っています。CSPM を使用すると、複数の CSP の構成、セキュリティ、およびコンプライアンスを中央のツールから監視できます。

他の多くのツールがセキュリティプログラムをサポートしますが、このセットはマルチクラウドの基本です。これは複数のクラウドへのユーザーの接続性を管理し、重要なセキュリティテレメトリを一元的に追跡し、マルチクラウドのセキュリティとコンプライアンスの構成を可視化します。

人員配置はツールよりも大きな課題です。市場にセキュリティ製品ベンダーは不足していませんが、クラウドセキュリティの熟練した専門家は依然として不足しています。また、多くの CSC は人員を増やさずにクラウドへの移行を試みており、従来のインフラストラクチャをサポートしながらクラウドのスキルを身に付けることを既存のスタッフに強いています。

各 CSP は最も深い技術レベルで根本的に異なり、それぞれが特定の知識を必要とします。特定の CSP から提供されるサービスが増えるほど、さまざまなサービスをセキュアにするための広い知識が要求されます。CSC には、重要な（または重大な）フットプリントをホストするクラウドプラットフォームごとに、少なくとも 1 人の特定分野のエキスパートを配置する必要があります。プライマリ/セカンダリ戦略により、各プラットフォームの専任エキスパートの必要性を軽減できます。

多くの CSC、特に小規模な CSC は、十分なスキルを持つスタッフレベルを提供する負担をマネージド CSP（*マネージドサービスプロバイダ*とも呼ばれる）にシフトしようとしています。これは多くの場合、実行可能な戦略になり得ますが、セキュリティとガバナンスに関する説明責任がシフトすることはありません。さらに、マネージドサービスプロバイダのビジョン、戦略、および能力が、CSC の望ましい将来の状態と整合していることを確認することが極めて重要です。

4.3.4 SaaS ハイブリッドとマルチクラウドの組織管理

現在の CSC は、オペレーション能力を強化するためにさまざまな SaaS CSP を活用しています。CSC に対して、統合や、より高い柔軟性とセキュリティ責任を伴うことが多い IaaS とは異なり、SaaS ランドスケープには独自の課題があります。これには、さまざまなビジネスアプリケーションに対応する幅広い製品、幅広いセキュリティ成熟度、および CSP 全体の多様な技術が含まれます。しかし、 SaaS は通常、利用者のセキュリティ責任をより低いレベルで要求します。このばらつきは、SaaS が CSC に、ビジネスニーズを満たすためにイノベーションを活用する効果的で的を絞った手段を提供できることに起因しています。

CSC 内の効果的な SaaS セキュリティ管理は、ポートフォリオ管理を入念に行うことから始まります。SaaS CSP はビジネスニーズを機能的に満たす能力が評価されると同時に、セキュリティやコンプライアンス対策についても徹底した評価を受ける必要があります。その後、分類に基づいて特定の種類のデータを扱う権限を彼らに与えることができます。この承認プロセスと、各 SaaS CSP の詳細は、綿密に文書化し、中央レジストリに保持する必要があります。ビジネスユニット内から、すでにサービスを提供しているカテゴリ内で新しい SaaS CSP を採用してほしいというリクエストがあった場合、すでに承認された CSP に加えて、またはそれと一緒に新しい CSP を追加することをサポートするための、確かなビジネス上の正当性が必要になる可能性があります。

SaaS ソリューションでは、ハイブリッドクラウドモデルの内部アプリケーションであれ、他の SaaS 製品であれ、他のアプリケーションとの統合が頻繁に必要になります。これらの統合は、場合により個々のユーザーには直接リンクしない方法で、アプリケーション間のデータの流れを容易にします。したがって、これらの統合に対するガバナンスを確立することは、データ移動のセキュリティとコントロールの維持に役立ちます。

セキュリティプログラム内で複数の SaaS CSP を管理するには、次の 2 種類のツールが役立ちます。

1. **Federated Identity Broker:** Federated Identity Broker は Identity-as-a-Service のサービス提供に不可欠であり、CSC のアイデンティティプロバイダとそのクラウドサービスインスタンス間のフェデレーションアイデンティティ管理の接続を仲介するために役立ちます。主要な CSP 向けに事前構築されている統合と、さまざまなサービスへのユーザーアクセス用の一元化されたダッシュボードにより、Federated Identity Broker は、ユーザーのアクセスと権限のライフサイクル管理と CSC を大幅に合理化します。

2. **Cloud Access and Security Brokers (CASB):** CASB は、アクセス制御と監視機能の提供により CSC の SaaS ポートフォリオ管理を支援し、また、どの SaaS CSP が、どのユーザーにより、どの場所から利用されるかを強制することに役立ちます。ゼロトラストのセキュリティ原則の実装など、CASB を取り巻く環境が進化するにつれ、一部のベンダーは構成セキュリティにまでフォーカスを広げ、SaaS Security Posture Management（SSPM）の概念を生み出しています。CASB の主な利点は、CSC の SaaS 利用に関する洞察と、一定程度のコントロールを提供することです。一方、SSPM はセキュリティハイジーンの監視と維持にフォーカスしています。高度な CASB ソリューションでは、SaaS のセキュリティを強化するために、リアルタイム監視、データ損失防止（DLP）などの機能を備えている場合もあります。

これらのツールと戦略を統合することで（ゼロトラストのセキュリティ戦略と原則に沿っているのが理想的）、CSC は、SaaS プロバイダが提供する革新的なソリューションを活用しながら、セキュリティとコンプライアンスの確保のための支援により、SaaS ポートフォリオをより効果的に管理できるようになります。

4.3.5 ハイブリッドとマルチクラウドのゼロトラストセキュリティ戦略

成功するサイバー攻撃は、一般的に何らかの方法で信頼を悪用します。これにより、「信頼」は軽減および管理されるべき危険な脆弱性となります。ゼロトラストは、いかなるユーザーや資産も暗黙のうちに信頼されるべきではないという考えを前提としたサイバーセキュリティ戦略です。情報漏洩がすでに発生している、または今後発生することを前提としています。したがって、企業の境界で実行される 1 回の検証でユーザーに機密情報へのアクセスを許可すべきではありません。その代わり、各ユーザー、デバイス、アプリケーション、およびトランザクションを継続的に検証する必要があります[70]。

ゼロトラストは、クラウド/マルチクラウド、オンプレミスおよびハイブリッドシステム、社内外のパートナー/ステークホルダーユーザー（CSC の管理端末、BYOD）のエンドポイントを網羅する、エンタープライズセキュリティ戦略であり、ゼロトラストには、運用技術（OT）、産業制御システム（ICS）、モノのインターネット（IoT）、および物理セキュリティが含まれます。ゼロトラストは、現在の、リモートワーカーと OT/IoT コンポーネントが多く存在する分散型エンタープライズクラウド/マルチクラウド、およびハイブリッド環境にとって最適なエンタープライズセキュリティ戦略であると、多くのセキュリティ専門家が述べています。本質的に、そして一貫して、この戦略は、前のセクションで推奨したタイプのローカライズされたアクセスコントロール、および環境とアプリケーション間のセグメンテーションと分離につながります。

サマリ

クラウド環境内の組織またはテナント階層を活用することは、クラウドデプロイメントのいくつかの重要な側面を管理するための戦略的なアプローチです。これには、潜在的なセキュリティインシデントの影響範囲の最小化、サービス制限の遵守、およびデプロイメント環境の論理的な分離の実現などが含まれます。この階層構造は、さまざまなセキュリティコントロールを整合させるための基盤であり、思慮深く戦略的な実装の重要性を強調しています。階層化は、効果的な管理を容易にするだけでなく、クラウドデプロイメントのセキュリティポスチャを強化します。

アイデンティティプロバイダまたはディレクトリは、CSP の環境内のアクセスと権限の管理の最前線にあります。このコンポーネントは、個々の権限を管理するための最初のレイヤーであり、その後、CSP のサービス全体に適用されます。CSP ポリシーは、階層全体のガバナンスに堅牢なメカニズムを提供する予防的コントロールとして重要な役割を果たします。これらのポリシーにより、CSC にサービスの使用をコントロールし、特定の設定を強制することを可能にします。それによりセキュリティとコンプライアンスのレイヤーがさらに追加されます。

Security Information and Event Management（SIEM）、セキュリティデータレイク、および CSPM などのツールはクラウド環境内の一元的な可視化を実現するために不可欠です。これらのツールは、クラウドデプロイメント環境全体のセキュリティイベント、構成、コンプライアンスステータスに関する包括的な洞察を提供し、潜在的なセキュリティ脅威を効果的に検出して対応する CSC の能力を強化します。

[70] CISA. (2022) *NSTAC Report to the President on Zero Trust and Trusted Identity Management,* page 1, and adopted as the official CSA definition of Zero Trust.

ハイブリッドクラウド環境では、IAM、特にディレクトリとネットワーク接続ポイントに重点が移ります。これらのコンポーネントは、オンプレミスインフラストラクチャとクラウドサービス間のインターフェースを保護し、異なる環境間のセキュアなアクセスとデータフローを確保するために重要です。

マルチクラウド戦略の複雑さに対処する CSC にとって、最も価値のある資産は十分な対象分野の専門知識です。特定のクラウドプラットフォームとサービスに関する深い専門知識を持つ個人は、マルチクラウドのデプロイメントによってもたらされる固有の課題と機会に対処する際に役立ちます。これらの人材は、セキュリティ、コンプライアンス、および運用効率が最高レベルで維持されることを確実にする、さまざまな CSP 間でクラウドサービスの利用を最適化するために必要な知識や洞察を提供します。階層的な組織、予防的コントロール、一元化された可視性、および専門家によるガイダンスを重視したこのクラウド管理のための戦略的アプローチは、セキュアで効率的なクラウドインフラストラクチャを実現する上で不可欠です。

推奨事項

クラウドのガバナンスと管理

- 一元化されたクラウドデプロイメントレジストリを作成します
- 複数のデプロイメントを使用した組織階層を定義します
- 特別な用途のための例外を含めます
- 新しいデプロイメントを作成するための軋轢の小さいプロセスをサポートします
- CSP ポリシーを使用してサービスと機能を管理します

セキュリティ戦略とコントロール

- 包括的でモダンなエンタープライズセキュリティ戦略を採用します
- CSP の「ルート」または「グローバル管理者」のクレデンシャル情報へのアクセスを最小限に抑えます
- CSPM ツールを使用してセキュリティとコンプライアンスを監視および維持します
- 組織/テナントのルート外のデプロイメント環境からセキュリティツールを実行します
- クラウドとデータセンターのデプロイメントに適したセキュリティポリシーを確立します
- ハイブリッドデプロイメントでは IAM とネットワーク接続に注意します
- ハイブリッド接続の要件を正式化します
- ハイブリッド/マルチクラウド環境におけるコンテナのセキュリティコントロールを確立します

マルチクラウド戦略

- 十分に熟練していない限り、本番環境でマルチクラウドを試みません
- クラウドの成熟度に応じたマルチクラウド戦略を確立します
- プロバイダ固有のセキュリティ分野の専門家を配置します
- マルチクラウドに十分なセキュリティ要員を確保します

クラウドセキュリティの監視と管理

- 使用中のすべての CSP をサポートする CSPM を使用します
- CASB ツールによる SaaS サービスの管理を検討します
- SaaS プラットフォームの可視化に SSPM ツールの活用を検討します

クラウドの相互運用性と移植容易性

- 相互運用性と移植容易性の戦略を検討します

SaaS ガバナンス

- 承認された SaaS プラットフォームのレジストリを維持します

追加のリソース

- Roles and Responsibilities of Third-Party Security Services | CSA
- AWS Landing Zone
- Azure Landing Zone
- Google Landing Zone
- Oracle Cloud Infrastructure - Landing Zone

ドメイン 5:アイデンティティとアクセスの管理

はじめに

IAM（Identity and Access Management）は、承認されたアイデンティティのみが適切なリソースに適切なアクセス権を持つようにします。データセンターやサービスの多数の管理機能が、インターネットからアクセス可能な統合された Web コンソールやアプリケーションプログラミングインターフェース（API）に統合されているクラウドプラットフォームにおいて、IAM は、クラウドネイティブセキュリティの新たな境界として機能し、機密性の高いリソースを未許可のアクセスや悪用から保護します。

パブリッククラウドとプライベートクラウドの両方で、CSP（クラウドサービスプロバイダ）と CSC（クラウドサービス利用者）は、IAM を許容可能なリスク許容範囲内で管理する責任があります。本セクションでは基本的な IAM の概念を確認する一方で、クラウドにおける IAM の特性と課題、および効果的な管理の確保に焦点を当てます。

オンプレミスシステムと比較して、クラウドコンピューティングは、IAM の管理に新しい次元をもたらします。中核となるセキュリティの課題は今に始まったことではないかもしれませんが、その影響は拡大しており、クラウドのランドスケープに波紋を広げる可能性があります。

主な違いは次のとおりです。

- CSP と CSC の関係、およびそれぞれの責務
- 複数のマネジメントインターフェースの統合
- 特にパブリッククラウド環境において、これらのインターフェースがインターネットにさらされること

IAM は CSP や CSC だけで管理することはできません。双方の信頼関係、責任の明確化、および管理を円滑に進めるための技術的な仕組みが必要です。さらに、複数の CSP を扱う CSC では、各プロバイダ独自のポリシーに沿って複数の IAM ソリューションを管理するという複雑さが増します。

このドメインは、主に CSC と CSP 間、または CSP とサービス間の IAM に重点を置いています。Infrastructure as a Service (IaaS) 上で実行されるエンタープライズアプリケーション内部の IAM など、クラウドアプリケーション内での IAM の管理に関するすべての側面については説明していません。

学習目標

このドメインでは、次のことを学びます。

- アイデンティティフェデレーションとその認証における役割を定義します。
- クラウド環境の IAM ポリシータイプを区別します。
- IAM（Identity and Access Management）の主要なコンポーネントを特定します。
- クラウドアプリケーションで利用者のアイデンティティを効果的に管理します。

5.1 クラウドにおける IAM の違い

IAM は常に複雑です。基本的に、何らかの種類のエンティティ（例えば、人、システム、コードの一部）は、さまざまな属性（現在の状況に基づいて変更される可能性がある）に関連付けられた検証可能なアイデンティティにマッピングされ、次に、権限に基づいてエンティティが何をできるか、できないかを決定します。これを検証可能な形で正しく行うことの複雑さは、さまざまなシステム、サービス、およびテクノロジーが関与するにつれて増大します。

クラウドコンピューティングにおける IAM の主な違いは次の 3 つです。

1. IAM はクラウドコンピューティングの複数の組織にまたがるようになりました。どの CSC にも複数の CSP が存在する可能性があります。そのような CSC は、クラウドサービスモデルのあらゆる範囲にわたって多数のサービスを利用している可能性があります。アイデンティティフェデレーションは、組織間の信頼関係を構築し、標準ベースの技術を通じてそれを適用することにより、この問題を管理するための主要なツールです。
2. CSP はすべて独自の IAM システムを使用しています。彼らの技術が異なるだけでなく、アーキテクチャ全体、さらには用語の多くも異なります。CSC は、複数の異なるモデルを学び、理解し、実装する必要があります。これは従来のアーキテクチャのさまざまなアプリケーションやソフトウェアスタックにも当てはまると同時に、クラウドはマネージメントプレーン全体、さらにはコネクテッドサービスのインフラストラクチャにまでこのレイヤーを追加します。

3. CSP は、マネジメントおよび管理用機能を統合 Web コンソールや API に集約します。パブリッククラウドの場合、これらは一般にインターネット上にあり、通常はユーザー名とパスワード（およびオプションの強固な認証やポリシー条件）程度で保護されます。プライベートクラウドやコンテナプラットフォームは、マネージメントプレーンを直接またはセキュリティの設定ミスを介してインターネットに公開してしまうことがよくあります。

フェデレーションと多数の IAM システムは、クラウドのアイデンティティとアクセスの管理の複雑さの多くを明らかにします。一方、管理機能を統一することと、それらをインターネット上に配置することの組み合わせは、それらの重要性を劇的に高めます。これらの課題は理論的なものではありません。クラウドネイティブのセキュリティ侵害の大部分は、一般的に IAM の不備に起因しています。

クラウドへの移行は、IAM の改善の機会も生み出します。主要なプロバイダは、属性ベースのアクセスコントロール (ABAC)、ポリシーベースのアクセスコントロール (PBAC)、ロールベースのアクセスコントロール (RBAC)、リスクベースの認証と認可、一時的なクレデンシャル、シークレット管理、ジャストインタイム (JIT)[71] アクセス、その他の高度なオプションなど、最新の機能をサポートしていることが多いです。これらは、セキュリティ専門家が長年取り組んできた、コントロールの即応性と粒度のポテンシャルを生み出します。

IAM は、基本的に CCSK のすべてのドメインにまたがります。次のセクションでは、まず、すべての読者が馴染みのない基本的な IAM の概念と用語を確認し、次にクラウドへの影響について掘り下げます。最初にアイデンティティについて、次にアクセス管理についてです。

5.1 基本用語

IAM は、特にいくつかの用語は異なる文脈で異なる意味を持つため（IAM 以外の分野でも使用されています）、混乱を招く可能性がある独自の用語を使用する幅広いプラクティス分野です。「IAM」という用語でさえ普遍的ではなく、アイデンティティ管理（IdM）とも呼ばれています。

ガートナーは、IAM を「適切な個人が適切な理由 で適切なリソースに適切なタイミングでアクセスできるようにするセキュリティ規律」[72]と定義しています。詳細に入る前に、クラウドコンピューティングにおける IAM の説明に最も関連性の高い用語を次に示します。

- **アクセスコントロール:** エンティティに付与された権限に基づいて、リソースへのアクセスを制限することです。

- **アサーション:** アイデンティティプロバイダ（IdP）からリライングパーティー（RP）への、エンティティに関する情報を含むステートメントです。フェデレーション技術は、一般的に IdP と RP が単一のエンティティではない場合、または共通の管理下にない場合に使用されます。RP はアサーション内の情報を使用してエンティティを識別し、RP がコントロールするリソースへのアクセスに関する認可決定を行います。

- **属性:** エンティティの状態、外観、またはその他の関連する側面を記述するエンティティの特性またはプロパティです。属性には、個人情報、ユーザーの役割、セキュリティクリアランスレベル、アクセス要求の時間、または要求元の場所などのさまざまな情報を含めることができます。

[71] JIT access reduces the window for abuse by eliminating static credentials. Access is requested for a session and externally approved, then revoked at the end of the session.
[72] Gartner. (2024) *Gartner Glossary: Identity and Access Management*

- **属性ベースのアクセス制御[73](ABAC):** 管理対象システムからログインするユーザー、特定のタグを持つ対象リソースなど、多要素認証 (MFA)のような、特定の複数属性を必要とするアクセスコントロールまたは権限です。

- **認証：** ユーザー、プロセス、またはデバイスのアイデンティティを確認します。多くの場合、システム内のリソースへのアクセスを許可する前提条件となります。

- **信頼できるソース:** エンティティのアイデンティティ属性に関する最も正確で最新の情報を保持する信頼できるシステムです。この情報は、他の IAM コンポーネントによって認証や認可などのタスクに使用されます。

- **認可:** システムオブジェクト（ネットワーク、データ、アプリケーション、サービスなど）へのサブジェクトのアクセスを、許可または拒否を決定することです。

- **権限:** アイデンティティを要求される属性を持つ認可にマップします（例えば、Z 属性が指定された値を持つ場合に、ユーザーX はリソース Y へのアクセスを許可される）。一般的に、これらの権限のマップを権限マトリックスと呼びます。権限は、多くの場合、配布と適用のために機械読み取り可能なポリシーとしてエンコードされます。

- **エンティティ:** エンティティとは、コンピュータシステムにおいて識別可能な固有のアクターを指します。サイバーセキュリティの文脈では、エンティティは、 IAM システムによって識別され認証されるユーザー、デバイス、アプリケーション、またはシステムです。エンティティは、システム内でさまざまなロールと権限を持つことができます。通常、監査とセキュリティの目的で、エンティティのアクションとリソースへのアクセスがログに記録されます。

- **フェデレーテッド IdM：** 多くの場合、IdP によって提供される単一のクレデンシャルセットを使用して、ユーザーが複数のシステムまたはアプリケーションにアクセスできるようにします。これはシングルサインオン (SSO) を実現する主要な機能であり、クラウドコンピューティングの中核となる機能です。

- **IAM プリンシパル：** CSP リソースに対するアクションまたは操作を要求できるユーザー、ロール、またはその他のアイデンティティタイプ。

- **識別子:** アイデンティティの証明に使用されるアーティファクト。これは暗号トークンの場合のようにデジタルの場合もあれば、運転免許証やパスポートなどの物理的な場合もあります。

- **アイデンティティ**：特定の名前空間内におけるエンティティの固有の表現。1 人の個人が仕事上のアイデンティティ（システムによっては複数のアイデンティティ）を持ち、ソーシャルメディア上のアイデンティティを持ち、また個人のアイデンティティを持つなど、 1 つのエンティティは、複数のデジタルアイデンティティを持つことができます。

[73] NIST (2024) *CSRC: Attribute Based Access Control*

- **アイデンティティプロバイダ(IdP):** フェデレーション内のアイデンティティのソースです。認証ポリシーの適用を担います。IdP は、CSP ロールを IdP 属性にマッピングすることで、認可戦略においても重要な役割を果たすことができます。IdP は必ずしも信頼性のあるソースではありませんが、信頼性のあるソースに依存できます。

- **多要素認証（MFA):** あなたが知っている何か、あなたが持っている何か、またはあなたが何者であるかなどの付加的な要素を介してアイデンティティが認証されるメカニズムです。これは、盗まれたユーザーID/パスワードなどのアイデンティティベースの攻撃を封じ込める上で重要な技法です。一般的に、財務、保健などの重要なシステムへのアクセスを許可する前に、アイデンティティの認証に使用されます。この技法は、未知のデバイスからや、未知の場所/国 （「ありえない移動」）からのログイン（訳注：原文は logging であるが、login の間違いと思われる）などの、条件付きアクセスでも使用されます。

- **ペルソナ:** ユーザー中心のビューで、さまざまなユーザータイプがシステムとやり取りする方法を理解するために役立ちます。似た特徴を持つユーザーのカテゴリーを表し、ロールの開発につながります。たとえば、クラウドシステムでは、開発者、セキュリティアナリスト、営業担当者、またはコンテンツ作成者のペルソナを、それぞれが行う必要がある行為を記述することで定義できます。これにより、固有のロールや特定の権限の開発につながる可能性があります。

- **ポリシーベースのアクセス制御（PBAC）：** アクセス要件は、機械で読み取り可能なポリシードキュメントで定義されます。その定義は、通常、さまざまな条件や属性などのその他の変数をサポートし、広範な柔軟性と細かさを提供します。PBAC は RBAC と ABAC を補完するものであり、多くの場合、それらの定義と管理の方法です。PBAC ポリシー文書もバージョン管理リポジトリと infrastructure as code（IaC）を使用して管理され、条件付きアクセスと呼ばれることもあります。

- **リライングパーティー (RP):** IdP に依頼してユーザーのアイデンティティとアクセス権を確認し、そして自身のリソースに対して権限を付与するサービスです。サービスプロバイダと呼ばれることもあります。

- **ロール（役割）:** 権限中心のビューを提供し、ユーザーが特定のタスクを実行するためのアクセスレベルを定義します。ロールは、ユーザー固有にすることも、ユーザー間で共有することもできます。1 人のユーザーの責任範囲によっては、複数のロールを持つ場合もあります。逆に、同じアクセスニーズがあれば、複数のユーザーが同じロールを共有できます。たとえば、"営業担当者"の下に定義されたすべてのペルソナに同じ権限が与えられます。

- **ロールベースアクセス制御** (RBAC)**:** ABAC よりも一般的なモデルで、特定のロール（開発者や管理者など）を持つすべてのユーザーにアクセス権が付与されます。

主要な IAM 標準を含むいくつかの用語については、以下の関連セクションで説明します。CSA の「IAM Glossary」で IAM[74]

5.2 フェデレーション

アイデンティティフェデレーションは、認証を処理する IdP と認可を管理する RP の関係を確立します。クラウドでは、RP は通常、クラウドサービスまたはアプリケーションです。1 つの IdP は 多数の RP とフェデレートできるため[75]、分散システム間の認可やアクセスコントロールをサポートしながら、ユーザー管理（作成、ロール割り当て、属性、認証、削除）を統合します。

IAM の標準やフレームワークはたくさんあり、クラウドコンピューティングで使えるものも多いです。幅広い選択肢があるにもかかわらず、クラウドセキュリティ業界は、ほとんどの IdP で一般的に見られ、サポートされているコアセットに集約しつつあります。

5.2.1 一般的に使用されるフェデレーションの標準

以下は、一般的に使用されている規格の一部です。このリストは特定の推薦を反映せず、すべてのオプションが含まれているものではなく、単に、プロバイダによって最も幅広く一般的にサポートされているものの代表的なサンプルになります。

- **Security Assertion Markup Language (SAML)** は、認証と認可をサポートするフェデレーション IdM の OASIS（Organization for the Advancement of Structured Information Standards）規格です。XML を使用して IdP と RP の間でアサーションを行います。アサーションには、認証ステートメント、属性ステートメント、認可決定ステートメントを含めることができます。エンタープライズツールと CSP の両方が広く SAML をサポートしていますが、初期設定が複雑になる場合があります。SAML は、従来の Web ベースのクライアント/サーバーアプリケーションに適しています。
- **OAuth** は IETF（Internet Engineering Task Force）の認可規格で、Web サービス（コンシューマーサービスを含む）で広く利用されています。OAuth は、サードパーティのアプリケーションに対してユーザーの資格情報（パスワードなど）を直接共有することなく、リソースへのアクセスを制限してユーザーを許可するという認可プロトコルと見なされます。OAuth は API アクセスを許可したり、サードパーティをアプリケーションに接続したりするのに良く使われます。OAuth は HTTP 上で動作するように設計されており、サービス間のアクセス制御と認可の委任に最もよく使用されます。

[74] CSA. (2024) *Identity and Access Management Glossary*

[75] The process of linking the identity management systems of different organizations to allow users from one organization to access resources and services of another organization securely and seamlessly.

- **OpenID Connect (OIDC)** は、Web サービスで広くサポートされているフェデレーション認証の標準規格です。OAuth に認証レイヤーを追加し、IdP とユーザー/ID を識別するために使用される URL（例：http://identity.identityprovider.com）を持つ HTTP に基づいています。OIDC 1.0 はコンシューマー向けサービスで非常に一般的に見られ、また、商用製品でのサポートも広がっています。1 つの例は、Single Page Applications（Facebook などの SPA）です。OpenID は認証の標準であり、OIDC とは異なります。 OpenID 2.0 は非推奨であり、大部分が OIDC に取って代わられています。

その他、一般的ではありませんがクラウドコンピューティングに有用な規格として、以下の 2 つが挙げられます。

- **eXtensible Access Control Markup Language (XACML)** は、ABAC と認可を定義するための規格です。PDP（Policy Decision Point）でアクセス制御を定義し、PEP（Policy Enforcement Point）に渡すためのポリシー言語です。ログインや権限委譲の処理とは対照的に、これにより、一連の属性によりエンティティは何の実行が許されているかというような問題の別の部分を解決することから、SAML または OAuth と組み合わせて使用できます。
- **System for Cross-domain Identity Management** （訳注：原文には略語が書かれていないが、SCIM のことである）は、ドメイン間でアイデンティティ情報を交換するための規格です。外部システムのアカウントのプロビジョニングやプロビジョニング解除、属性情報の交換に使用できます。

5.2.2 ID フェデレーションの仕組み

フェデレーションでは、IdP が RP との間に暗号による信頼関係を構築した後、RP に対してアサーションを行います。実践的な例として、ユーザーが、アカウント用のディレクトリサーバをホストする職場のネットワークにログインします。IdP と RP はシークレットを共有します。ユーザーが SaaS アプリケーションへのブラウザー接続を開くと、ログイン処理が開始されるのではなく、IdP（内部ディレクトリサーバー）がユーザーのアイデンティティをアサートし、ユーザーを認証し、場合によっては必要な属性を転送するという、一連の裏側での操作（図のステップ 1〜6）が行われます。すると、RP はそれらのアサーションを信頼し、その結果、ユーザーが資格情報を入力せずにログインできるようになります。RP は、自身の名前空間でそのユーザーのユーザー名やパスワードを必要としません。代わりに、IdP に依頼して正常な認証をアサートします。ユーザーは、内部ディレクトリで正常に認証されたと仮定し、単に SaaS アプリケーションの Web サイトにアクセスすることでログインできます。

これは、クラウドコンピューティングのアイデンティティ、認証、および認可で使用される他の技術や標準がないことを意味するものではありません。ほとんどの CSP、特に IaaS は、これらの規格を使用して（使用していない可能性もあります）CSC が接続することが可能な、内部 IAM システムを持っています。例えば、HTTP リクエスト署名[76]は REST API の認証に一般的に使用され、CSP 側の内部ポリシーは

[76] IETF. (2024) RFC 9421

認可の決定を管理するために使用されます。リクエスト署名はまだ SAML による SSO をサポートしているかもしれないし、API は完全に OAuth ベースだったり、独自のトークンメカニズムを使ったりするかもしれません。いずれもよく目にしますが、ほとんどのエンタープライズクラスの CSP はフェデレーションをサポートしています。

アイデンティティプロトコルを選択する際に不可欠な概念は以下です。

- どのプロトコルも、アイデンティティとアクセス制御の問題をすべて解決する特効薬ではありません。
- アイデンティティプロトコルは、特定のユースケースコンテキストで分析する必要があります。たとえば、ブラウザベースの SSO、API キー、モバイルからクラウドへの認証など、異なるアプローチからそれぞれの恩恵を受ける可能性があります。
- アイデンティティは、非武装地帯（DMZ）[77]と似たようにそれ自体が境界であるということが、鍵となる前提です。

次の図は、クラウドセキュリティにおける OpenID フェデレーションのワークフローを示しており、IdP によるユーザー認証から、リライングパーティー のサービスへのアクセスまでの手順を詳細に説明しています。

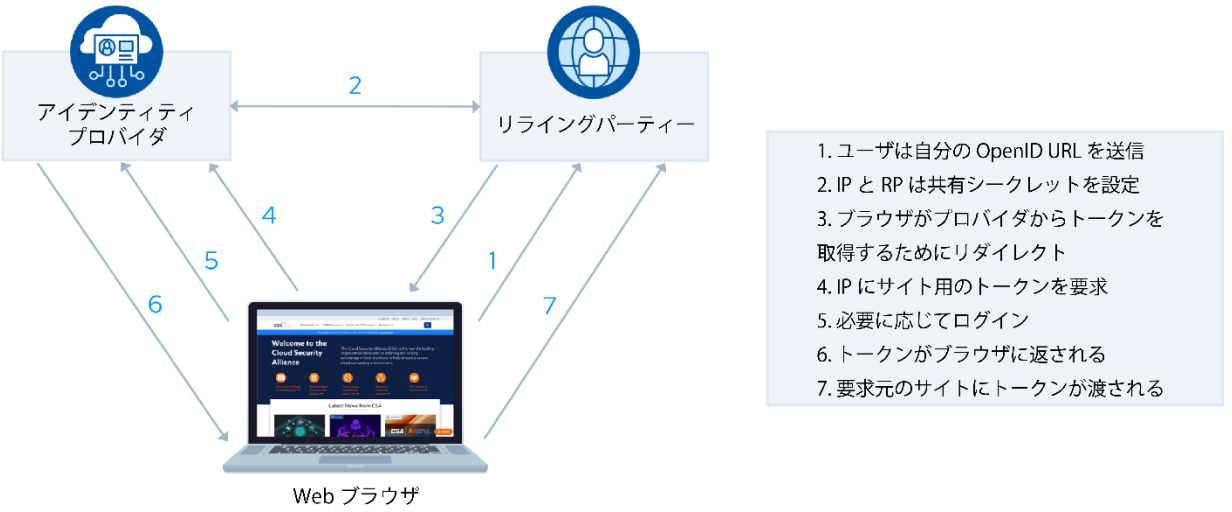


図 25: クラウドセキュリティにおける OpenID フェデレーションのワークフロー

5.2.3 クラウドコンピューティングのユーザーとアイデンティティの管理

[77] A demilitarized zone is a physical or logical subnetwork that acts as a buffer zone between an internal network (such as a corporate LAN) and an external network (typically the internet).

アイデンティティ管理の「アイデンティティ」部分は、アイデンティティの登録、プロビジョニング、伝播、管理、およびプロビジョニング解除のプロセスとテクノロジーに焦点を当てています。アイデンティティの管理と、システムでのアイデンティティのプロビジョニングは、情報セキュリティ部門が何十年も取り組んできた課題です。IT 管理者がさまざまな社内システム毎にユーザーを個別にプロビジョニングする必要があったのは、それほど昔のことではありません。ディレクトリサーバーが一元化され、さまざまな標準が揃っている今日でも、すべてに対する真の SSO は比較的稀です。昔に比べるとはるかに少ないとはいえ、ユーザーは認証情報を必要とします。

クラウドコンピューティングのユーザーとアイデンティティの管理方法を決定する場合、CSP と CSC はアイデンティティの管理方法に関する 2 つの基本的な決定から始める必要があります。

- CSP は、サービスに直接アクセスするユーザーのために、彼らが管理する名前空間の内部アイデンティティ、識別子、属性をサポートする必要があります。さらに、CSC がプロバイダーのシステム内のすべてのユーザーを手動でプロビジョニングおよび管理し、それぞれに個別の資格情報を発行せずにすむように、フェデレーションをサポートする必要があります。
- CSC は、アイデンティティを管理するための最適な場所を決定し、CSP と結合するための適切なアーキテクチャモデルと技術を選択する必要があります。

CSC は CSP にログインし、システム内に CSC のすべてのアイデンティティを作成できます。しかし、このアプローチは、おそらく小規模を除くほとんどの CSC にとって拡張性に欠けるため、多くがフェデレーションに移行する理由となっています。アイデンティティのすべてまたは一部を CSP から分離しておくことに意味があるような例外もありえます。たとえば、フェデレーションアイデンティティ接続に関する問題のデバッグに役立つバックアップ管理者アカウントなどです。

フェデレーションを使用する場合、CSC は固有のアイデンティティについての信頼できるソース（多くの場合、内部ディレクトリサービス）を特定する必要があります。次に、このソースを直接 IdP として使用するか、別のアイデンティティソース（人事システムのディレクトリなど）からの供給を使用するか、アイデンティティブローカーと結合するかを決定する必要があります[78]。以下の 2 つの主要なアーキテクチャがあります。

- ハブ＆スポーク：内部 IdP/ソースは、CSP とのフェデレーションのための IdP として機能する中央ブローカーまたはリポジトリと通信します。
- フリーフォーム：内部 IdP/ソース（多くの場合ディレクトリサーバー）が CSP に直接接続されます。

[78] *Broker* is an intermediary service that connects multiple service providers with multiple IdPs.

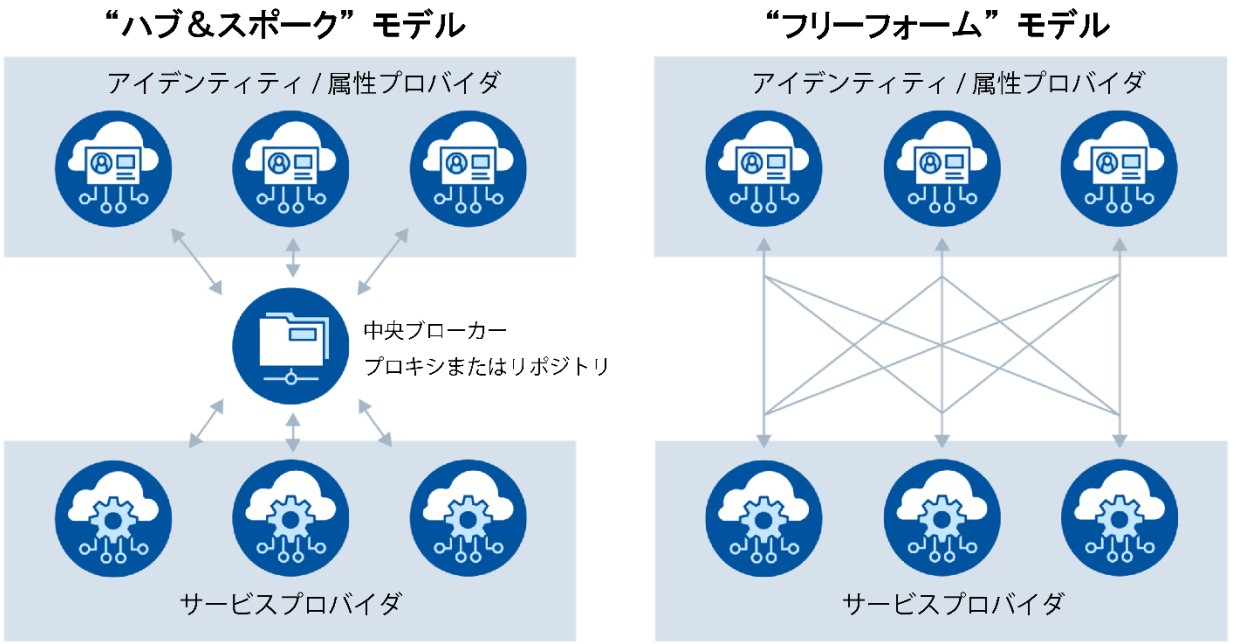


図 26: ID フェデレーション管理のアーキテクチャモデル:ハブ&スポークとフリーフォーム

フリーフォームモデルで内部ディレクトリサービスサーバを直接フェデレーションすると、いくつかの課題が発生します。

- ディレクトリにはインターネットアクセスが必要です。それがセキュリティポリシー違反になると問題になる可能性があります。
- クラウドサービスにアクセスする前に、ユーザーが企業ネットワークに VPN 接続し直す必要がありえます。
- 既存のディレクトリサービスサーバーによっては、特に複数のディレクトリサービスサーバーがさまざまな組織のサイロにある場合、外部プロバイダとのフェデレーションは複雑で技術的に難しい場合があります。

フェデレーションアイデンティティブローカーは、IdP と RP 間のフェデレーションを処理します。これらは、Web SSO を有効にするために、ネットワークエッジまたはクラウドに配置することもできます。IdP はオンプレミスのみに配置する必要はありません。現在、多くの CSP は、社内および他のクラウドサービスとのフェデレーションを管理できるクラウドベースのディレクトリサービスをサポートしています。

例えば、より複雑なアーキテクチャでは、CSC のアイデンティティの一部をアイデンティティブローカーを介して内部ディレクトリからクラウドホストされたディレクトリに同期またはフェデレートさせることができます。このクラウドホストされたディレクトリは、その後、他のフェデレーション接続のための IdP として機能することができます。

これらのソリューションを実装する場合、考慮すべきプロセスおよびアーキテクチャ上の決定がいくつかあります。

- アプリケーションコード、システム、デバイス、およびその他のサービスのアイデンティティを管理する方法。クラウドのデプロイメントやアプリケーション内で、同じモデルや標準が活用されたり、異なるアプローチを取ることが決定されたりすることがあります。ID プロビジョニングプロセスの定義とクラウドデプロイメントへの統合方法。また、異なるユースケースに対して複数のプロビジョニングプロセスが存在する場合もありますが、ゴールは統一されたプロセスを持つことです。よく見られる例は、スタッフの受入準備プロセスに対する請負業者の受入準備プロセスに関連します。
- プロビジョニング解除プロセスを確立します。適切なガバナンスには、アイデンティティとアクセス権限の適切な、時には迅速な削除が必要であり、同時にそれらの権限の使用に関する適切なフォレンジック証跡を維持する必要があります。
    - CSC が従来のインフラストラクチャに対して効果的なプロビジョニングプロセスを導入している場合は、理想的にはこれをクラウドデプロイメントに拡張すべきです。しかし、既存の内部プロセスに問題がある場合、CSC はクラウドへの移行を、より効果的な新しいプロセスを構築する機会として代わりに使用すべきです。
- 個々の CSP とデプロイメントのプロビジョニングとサポート。IAM インフラストラクチャに新しい CSP を追加する正式なプロセスがあるべきです。これには、必要なフェデレーション接続を確立するプロセスだけでなく、以下を含みます。
    - IdP と RP の間の属性（ロールを含む）のマッピング。
    - ABAC/PBAC をサポートするための属性（MFA ステータスやユーザーが認証した IP アドレスなど）を渡す。
    - 行動分析などの アイデンティティ関連のセキュリティ監視を含む、必要な監視/ロギングを可能にする。
    - 権限マトリックスの構築(次のセクションで詳しく説明します)。
    - リレーションシップに使用されるいずれかのフェデレーション(またはその他の技術)についての技術的な障害が発生した場合に備えて、あらゆる故障/修正シナリオを文書化します。もし、IdP がダウンした場合、CSP へのインターネット接続がダウンした場合、あるいは CSP のフェデレーションサポートがダウンした場合の、事業継続計画はありますか？
    - アカウント乗っ取りの可能性に対するインシデント対応計画が適用されていることを確認。
    - ID および CSP のプロビジョニング解除または権限変更プロセスの実装。フェデレーションにおいて、これにはリレーションシップの両側での取り組みが必要です。

最後に、CSP はどの IdM 標準をサポートするかを決定する必要があります。いくつかの CSP はフェデレーションのみをサポートしますが、その他の CSP は複数の IAM 標準に加えて独自の内部ユーザーアカウント管理をサポートします。エンタープライズ市場にサービスを提供する CSP は、通常、フェデレーションアイデンティティや、ほとんどの場合 SAML をサポートする必要があります。

5.3 強固な認証と認可

クラウドセキュリティには、強固な認証と許可の確保が不可欠です。このセクションでは、クラウドアクセスのセキュリティ保護のための主なプラクティスの概要を説明します。

認証は、クラウドサービスへのアクセスに不可欠なユーザーの本人確認を行います。パスワード以外にセキュリティ層を追加する MFA は極めて重要です。方式にはハードトークン、ソフトトークン、生体認証があり、それぞれ保護レベルが異なります。

認可によってユーザーの権限が決まります。RBAC や PBAC のような効果的なモデルでは、これらの権限を管理および適用し、きめ細かなコントロールを実現します。

CSP はこれらのポリシーを実施しますが、CSC はポリシーを定義して管理する必要があります。ABAC のような高度なモデルでは、コンテキストに応じたアクセス決定が可能になるため、セキュリティが強化されます。強力な認証および認可手段を実装することで、組織はクラウドリソースを保護し、セキュアなアクセスを確保できます。

5.3.1 認証とクレデンシャル

認証とは、アイデンティティの確認を行うためのプロセスです。ログインのためだけでなく、アイデンティティの検証や、システムまたはプロセス内の特定の権限または役割へアイデンティティをリンクする必要があるすべての状況で重要です。信頼できる認証を確保する義務は IdP にあります。

クラウドコンピューティングが認証にもたらす最大の影響は、主に 2 つの課題により、強固な MFA の必要性が増すことです。

- **幅広いネットワークアクセス**:クラウドサービスは、常にネットワーク経由で、多くの場合インターネット経由でアクセスされます。つまり、クレデンシャルが紛失したり盗まれたりした場合、攻撃はローカルネットワークに限定されないため、アカウントの乗っ取りにつながりやすくなります。
- **シングルサインオン(SSO)のためのフェデレーションの利用拡大:** 複数のクラウドサービスに単一のクレデンシャルセットを使用すると、それらのクレデンシャルが漏洩した場合、より多くのサービスが危険にさらされる可能性があります。

MFA は、アカウントの乗っ取りを減らすための最も強力なオプションの 1 つを提供します。万能薬ではありませんが、クラウドサービスを単一の要素（パスワード）に依存することは高いリスクを生み出します。フェデレーションで MFA を使用する場合、IdP は MFA ステータスを属性として RP に渡すことができ、また渡す必要があります。

MFA には、次のような複数のオプションがあります。

- ハードトークンは、人間が入力するためのワンタイムパスワード（OTP）を生成するか、読み取り機に接続する必要がある物理的なデバイスです。これらは、最高レベルのセキュリティが必要な場合に最適なオプションです。
    - プラグインされたトークンは、ユーザーが入力する OTP を生成するトークンよりも信頼性が高くなります。
    - フィッシングやその他の標的型攻撃によって、ユーザーが騙されて OTP コードを入力したり共有したりしてしまう例が複数あります。
- ソフトトークンはハードトークンと同様に動作しますが、スマートフォンやコンピュータ上で実行されるソフトウェアアプリケーションによって生成されます。ソフトトークンは優れた選択肢ですが、ユーザーのデバイスが侵害された場合に侵害される可能性があり、このリスクはどのような脅威モデルにおいても考慮される必要があります。
- アウトオブバンドパスワードは、通常、ユーザーの携帯電話に送信されるテキストまたはその他のメッセージで、トークンによって生成される他の OTP と同様に、その後入力されます。これも良い選択肢ですが、どの脅威モデルにおいても、特に SMS によるメッセージの傍受を考慮する必要があります。SIM スワップやその他のインフラへの攻撃により、SMS は推奨されなくなりました。
- 携帯電話で一般的に利用できるようになった生体認証リーダーのおかげで、生体認証はますます選択肢になっています。クラウドサービスの場合、生体認証は、CSP に生体情報を送信しないローカルでの保護機能であり、代わりに属性をプロバイダへ送信可能です。そのため、ローカルデバイスのセキュリティと所有権を考慮する必要があります。

組織が認証メカニズムを強化しようとする中、従来のアプローチを超えた追加の方法が採用されています。これらの手法は、ユーザーの利便性を向上させながらセキュリティを強化することを目的としています。

5.3.1.1 その他の認証方法

パスワードレス認証：このアプローチは、パスワードの必要性を回避するためにローカルトークンまたは証明書を利用し、また、サービス、ユーザー、およびデバイスに関連付けられた SSO トークンと似ています。このアプローチは、ユーザーエクスペリエンスを簡素化し、データ侵害時のフィッシングやパスワード漏洩のリスクを軽減します。とはいえ、パスワードレス方式は、管理者レベルのクラウドサービスアカウントには推奨されず、主にコンシューマアプリケーションのユーザー認証に使用されます。パスワードレスシステムは MFA に取って代わるものではないことに注意する必要があります。

FIDO (Fast IDentity Online): 現在のパスワードレス認証の業界標準である FIDO は、「Passkeys（パスキー）」や「Webauthn（訳注：原文では Webauthz と記載されているが、 Webauthn の誤り。）」など、フィッシングに強い認証方法を提供することで、技術の進歩を表すさまざまな名前で認知されています。FIDO を使用すると、ユーザーはログインプロセス中に認証要素として使用できる信頼できるデバイスを定義できます。FIDO は、アクセスデバイスにプラグインまたはワイヤレスで接続された物理トークンによって拡張することもできます。パスワードレス認証の標準規格を策定している FIDO Alliance

は、CSP やアイデンティアクセス管理（IAM）ソリューションプロバイダーなどの主要な IT ベンダーで構成されています。

5.3.2 エンタイトルメントとアクセスの管理

認可とアクセス制御という用語は多少重複しており、文脈によって定義が異なります。

- 認可とは、ファイルやネットワークへのアクセス、特定のリソースに対する API 呼び出しのような特定の機能の実行など、何かを行うための許可のことです。
- アクセス制御は、その認可の使用を許可または拒否し、そのために、アクセスを認める前にユーザーが認証されているかを確認するといった側面が含まれます。
- クラウドエンタイトルメントとは、特定のリソースやサービスにアクセスするためにクラウド環境のユーザーに付与される権限や権利を指します。通常、エンタイトルメントは、データの読み取り、データの書き込み、設定の構成、他のユーザーの管理など、ユーザーが特定のリソースに対して実行できるアクションを決定します。

エンタイトルメントは、アイデンティティを認可および必要な属性にマッピングします（例えば、属性 Z が指定された値を持つ場合、ユーザーX はリソース Y へのアクセスが許可される）。一般的に、これらのエンタイトルメントのマップをエンタイトルメントマトリックスと呼びます。PBAC を使用する場合、エンタイトルメントは配布および実施のための技術ポリシーとしてエンコードされることが多いです。

Entitlement	Super-Admin	Service-1 Admin	Service-2 Admin	Dev	Security - Audit	Security - Admin
Service 1 List	X	X		X	X	X
Service 2 List	X		X	X	X	X
Service 1 Modify Network	X	X		X		X
Service 2 Modify Security Rule	X	X				X
Read Audit Logs	X				X	X

テーブル 6: クラウドアクセス管理のエンタイトルメントマトリックスの例

クラウドは、エンタイトルメント、認可、およびアクセス管理にさまざまな影響を与えます。

- CSP とプラットフォームには、それぞれ固有の潜在的な認可のセットがあります。CSP が XACML をサポートしていない限り (今日では珍しい) 、CSC ユーザーは通常、クラウドプラットフォーム内でエンタイトルメントを直接設定する必要があります。
- CSP は、認可とアクセス制御を実施する責任があります。
- クラウド利用者には、クラウドプラットフォーム内でエンタイトルメントを定義し、それらを適切に設定する責任があります。
- クラウドプラットフォームは、RBAC モデルよりも柔軟性とセキュリティに優れた IAM 向けの ABAC モデルと PBAC モデルをサポートする傾向があります。RBAC は認可を実施するための伝統的なモデルであり、多くの場合単一の属性（つまり定義されたロール）を拠り所にします。ABAC は、ロール、場所、認証方式など、複数の属性を組み込むことで、よりきめ細かくコンテキストを意識した意思決定を可能にします。
- ABAC をサポートする PBAC は、クラウドベースのアクセス管理に適したモデルです。
- フェデレーションを使用する場合、クラウド利用者はロールやグループを含む属性を CSP にマッピングし、認証時にこれらが適切に伝達されるようにする責任があります。

CSP は、クラウド利用者のために ABAC と効果的なセキュリティを実現するための、きめ細かい属性と認可をサポートする責任があります。

実際のクラウドの例をご紹介します。CSP には、新しい仮想マシン（VM）を起動するための API があります。その API は、新しい VM の起動を許可するための対応する権限と、ユーザーがその VM をどの仮想ネットワークにおいて起動できるかについての追加の権限オプションを持ちます。
クラウド管理者は、開発者グループのユーザーが、 MFA で認証された場合にのみ自分のプロジェクトネットワーク内でのみ VM を起動できるとするエンタイトルメントを作成します。このグループや、MFA の使用は、ユーザーアイデンティティの属性です。実施のために、そのエンタイトルメントは、CSP のシステムにロードされるポリシーとして記述されます。

5.3.2.1 リソースアクセス制御とポリシー

これまで、CSP のエンティティがプラットフォームの集中 IAM 管理にアクションを要求するという文脈で、認可とエンタイトルメントについて議論してきました。多くの CSP は、個々のリソース（保管場所など）に適用されるルールやポリシーもサポートしており、CSP 内でプロビジョニングされたエンティティ以外からのアクセスを考慮できます。

たとえば、ほとんどのストレージサービスでは、共有リンク、IP 制限、または一時パスコードを使用して、別の場所のユーザーがオブジェクトに直接外部からアクセスすることを許可します。

これらのエンタイトルメントは、中央の IAM ガバナンスを回避する可能性のあるリソースレベルのポリシーで実装されます。特にストレージサービスでは、これがデータ漏洩の原因となりがちです。CSC 内の IAM ユーザーがプライマリ IAM システム内のリソースへのアクセスを明示的に拒否されても、リソースポリシーが脆弱であるためにリソースにアクセスできるという状況さえあり得ます。

このリスクを軽減するために、一部の CSP は、外部への共有や、パブリックや外部からのアクセスを有効にする可能性のあるリソースポリシーの使用を制限するトップレベルのセキュリティコントロールを提供しています。CSC は自動化を使用して、これらのポリシーを特定および管理することもできます。

5.3.3 条件付きアクセス、トークン、セッション、IAM 境界管理

「IAM は新しい境界」と言うのは簡単ですが、その意味を正確に理解することが重要です。クラウド内、またはネットワーク経由でサービスが提供されるたびに、攻撃者はアイデンティティを直接標的にすることができます。攻撃者がアイデンティティや IAM システムの一部を侵害した場合、ネットワーク攻撃を行わずにリソースを侵害できます。ネットワークを保護する能力の向上に伴い、フィッシング、公開された認証情報のスキャン、マルウェアを介した認証情報の窃盗などの IAM ベースの攻撃が増加し、今ではクラウドネイティブ侵害の唯一最大の起点となっています。

IAM 境界には、認証と認可の両方、すべてのタイプのエンティティ（ユーザー、システム、コードなど）が含まれ、 IAM 境界はフェデレーション接続全体に広がります。一歩下がって IAM システムを見ると、ユーザーのパスワードのフィッシングから、パブリックコンテナ定義ファイルで公開されている認証情報の悪用まで、境界とは、潜在的にアクセス可能なすべてのタッチポイントです。

前述のように、フェデレーション認証アクションによってトークンが生成されます。このトークンはセッションに関連付けられており、セッションの長さに対応する定義済みの TTL（Time To Live）を持ちます。IAM システムは、セッションの有効期限が切れる前に自動的に要求され、その後、バックグラウンドでセッションを拡張し新しいセッションを作成するリフレッシュトークンの概念を統合できます。

トークンは認証の生成物であり、盗まれ悪用されることにより、パスワードが侵害されることなく、未承認のアクセスを提供する可能性があることを理解することが重要です。これは非常に一般的な攻撃手法です。攻撃者はトークンを盗むことができ、多くの場合、セッションが期限切れになるかトークンが手動で無効化されるまで、自分の管理下にある他の場所にあるシステムからトークンを使用することさえできます。

IAM 境界を保護することは、IdP と RP の間で分担される複数の技術に依存します。目的は、クレデンシャルとトークンの両方についての侵害と悪用を減らすことです。これを実現するためのコアテクノロジーの 1 つに、条件付きアクセスがあります。条件付きアクセスは、通常、条件文をサポートする PBAC ポリシーを使用してクラウドに実装されます。条件付きアクセスは、認証、認可、またはその両方において実施される場合があります。

実装は技術固有のものになりますが、IAM 境界防御戦略にはいくつかの重要な要素があります。

- 強力な認証（主に MFA）は、IAM 境界を防御するための重要な第一歩ですが、これはユーザー（および一部のシステム）認証を取り扱うだけで、依然として悪用される可能性があります。
- 可能な場合は、自動的にプロビジョニング、ローテーション、プロビジョニング解除されるクラウドプロバイダが管理するアクセス資格情報を使用します。VM、サーバーレスファンクション、および CSP 内の他のリソースやサービスにアクセスするその他のリソースタイプのために、これ（クラウドプロバイダが管理するアクセス資格情報）は、すべての主要な CSP で一般的にサポートされています。
- 認証時におけるデバイスと場所の制約により、どのデバイスが許可される、およびどこからのネットワークロケーションが許可されるかを制限できます。これは、分散した組織のユーザーにとっては実装が難しいかもしれませんが、それでもシステム/サービス認証に簡単に使用できます。高度に分散化された CSC でも、VPN/SASE[79]を設定することを検討できます。
- 多くの場合 PBAC システムは、各認可要求における、発信 IP アドレス、MFA ステータス、およびその他の制限についての条件をサポートしています。API を呼び出すたびに認証ポリシーがチェックされるため、盗まれたトークンの悪用を防ぐことができ、これは非常に強力です。攻撃者がトークンを盗んだ場合でも、認可における IP 制限が実施されていれば、そのトークンは外部から動作しません。
- JIT アクセスを用いた場合、静的クレデンシャルを排除することにより、悪用のための機会が削減されます。アクセスはセッションに対して要求され、外部で承認され、セッション終了時に取り消されます。承認ステップは二重認可（Dual authority）[80]の形式であり、セッション作成とは異なる帯域で管理されます。これは一部の CSP やサードパーティ製ツールでサポートされています。主な利点は、アタックサーフェスの削減です。ユーザーに永続的な権限がないため、攻撃者にとっての好機が大幅に縮小されます。
- ほとんどの IaaS プロバイダは、ネットワークアーキテクチャ内で何らかの形で内部サービスエンドポイントをサポートしており、システム/リソース API コールが内部ネットワーク接続からのみ発信されるよう、これらを IAM ポリシーで活用することができます。
- 一部の PBAC ポリシーは、特定のエンタイトルメントに対し、同じペルソナのためにさまざまな認可要件をサポートします。たとえば、変更要求は読み取りアクセスよりも厳しい属性セットを必要とする場合があります。これにより、管理者は、企業ネットワークからのみネットワークまたは IAM の変更を行うことができます。しかし、これにより、彼らはデバッグ目的でどこからでもログにアクセスできます。

[79] CISCO. (2023) *What is Gartner’s SASE model, and how will it affect your security stack?*

[80] NIST. (2024) Information Technology Laboratory: Computer Security Resource Center - dual authorization.

IAM 境界の管理は複雑になる可能性がありますが、ABAC と PBAC の機能が向上したおかげで、誰が何であるかという静的な概念に基づいてアイデンティティを管理するだけでなく、その人がどこにいるか、使用しているデバイス、および継続的に評価されるその他の属性に基づいてアイデンティティを管理できるようになりました。

最終的に、PBAC はクラウドベースのアクセス管理にますます好まれています。PBAC により、CSC はクラウドサービスの複雑で動的な性質に対応したセキュリティポリシーを実施でき、機密性の高いデータを保護するためのアクセス権限は十分に厳密であるにもかかわらず、生産性を実現するために十分な柔軟性を確保できます。これらの高度なアクセス制御メカニズムをサポートする CSP の役割は非常に重要であり、クラウド利用者のセキュリティと運用のニーズを支援するきめ細かい属性と認可の実装を可能にします。

5.3.4 特権ユーザー管理

ある王国にとって非常に重要なもの、例えば金と銀の蓄えを保管する金庫室を想像してみてください。王国の王や王妃が金庫室に入ったとしても、書記は入室した日時を記録する必要があります。これが特権アイデンティティ管理（PIM）と特権アクセス管理（PAM）を理解する出発点です。

PIM と PAM は、組織の IT 環境、特にマネージメントプレーンのセキュアなガバナンスにおける重要な柱です。PIM は特権アイデンティティ（重要なシステムや機密データにアクセスし変更するための高い権限を保有するユーザー）の監視と制御に関係しています。PAM は、これらの資産やリソースにアクセスするチャネルの規制と保護に専念しています。これには、アクセスを許可するユーザーと、そのアクセスを構成する作業の方法、タイミング、範囲の決定が含まれます。

PIM と PAM の両方のフレームワークに内在する基本的な原理は、JIT アクセスです。JIT アクセスは、必要な期間だけアクセス権限を割り当てると同時に、アクセスが適切に記録されるようにすることで、永続的な特権付与や、アクセス監査の欠如に伴うリスクを軽減します。チェックされない場合は、永続的な特権アクセスは、アカウント侵害やセッションハイジャックによって悪用される可能性のある脆弱性となります。

JIT アクセスの実践は、最小特権の原則の実践的な適用であり、ユーザーには本来の職務を遂行するために必要なアクセスレベルしか与えられないようにします。同様に、職務分掌の原則は、特権（管理者）アクセスと非特権（一般ユーザー）アクセスに、別々のアイデンティティまたはアカウントを提供する際に適用できます。たとえば、個人が電子メールを読むために使用するものと同じアイデンティティ/アカウントに特権アクセスを付与すべきではありません。PIM および PAM サービスでサポートされているもう 1 つの重要な職務分掌の用途は、認められた別の当事者（例：管理者）が承認したときにのみアクセスを許可する機能です。これらの原則を一貫して適用することで、機密性の高いシステムの公開やアクセスが削減され、セキュリティポスチャが向上します。

PIM と PAM を企業のセキュリティフレームワークに統合することで、防御が強化されます。この動きによって、重要なリソースへの不正アクセスの可能性が低減され、全体的なセキュリティポスチャが強化

されます。常に有効な特権アカウントの数を最小化すると、サイバー犯罪者がエクスプロイトする可能性のある攻撃ベクトルが狭まります。この統合により、特権アカウントに関連するアクティビティを監視、文書化、および監査可能にするシステムが確立され、機密性の高い操作に対する CSC のコントロールが強化されるため、規制コンプライアンス要件への準拠を確実にします。

PIM および PAM ソリューションは、セキュアでコンプライアンスに準拠した IT 環境を維持するためのいくつかの重要な機能を示しています。最も重要な機能の 1 つは、クレデンシャルの自動ローテーションです。これにより、古いクレデンシャルや侵害されたクレデンシャルによるアクセスを維持することができなくなり、システムセキュリティの一般的な脆弱性を排除できます。さらに、これらのソリューションは MFA を強制します。また、包括的な監査およびレポート作成ツールも備えています。これらのツールは、詳細なフォレンジック分析の実施や、組織ポリシーや規制基準へのコンプライアンスの追跡に不可欠であり、情報に基づいたセキュリティ上の意思決定に必要な洞察を提供します。

5.4 パブリッククラウドの IAM ポリシータイプ

クラウドコンピューティングでは、アクセス制御は、権限を微調整し、セキュリティを強化するように設計されたさまざまなポリシーレイヤーによって管理されます。ポリシーの主なタイプは、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、および組織ベースまたはテナントベースです。

アイデンティティベースのポリシーは、IAM アイデンティティに関連付けられたポリシーです。これは、IdP を使用してクラウド環境への一時的なアクセスを取得するフェデレーションユーザー、または、CSC に内在する内部（クラウドネイティブ）IAM アイデンティティのいずれかになります。このアイデンティティに対する権限は、ポリシーによって定義されます。ポリシーは、許可または拒否するアクションを決定し、ユーザー、ロールに具体的に関連付けることや、グループ全体への配布ができます。CSP によって使用される用語はさまざまですが、基本的な概念は一貫しています。これらは、個々のアイデンティティに付与される権限です。

デバイスベースのポリシーは、デバイスアイデンティティの登録とコンプライアンスの状態に関連付けられます。デバイスは管理対象または非管理対象に分類されます。機密性の高い情報やリソースへのアクセスは、ステータスとコンプライアンスが特定レベルにあるデバイスに制限することができます。たとえば、デバイスは OS のバージョンが更新され、パッチが適用されており、CSC 管理対象デバイスとして登録されている必要があります。機密性の低いデータやリソースへのアクセスは、管理対象外のデバイスからのアクセスなど、コンプライアンスの低い状態に対して許可できます。

リソースベースのポリシーは、S3 バケット、Lambda 関数、その他のサービスなどの、クラウドリソースに直接リンクされるという点で、デバイスおよびアイデンティティベースのポリシーとは異なります。このようなポリシーは、誰がリソースにアクセスできるかを規制し、そのリソースに対する他のアカウント、デバイス、またはユーザーが許可されるアクションを決定します。それらのポリシーは、アカウント間のやり取りを管理し、許可されたエンティティのみがリソースに対して特定のアクションを実行できるようにするなど、インターネットに公開されるリソースへのアクセスを規制します。

組織ベースまたはテナントベースのポリシーは、CSC アカウント内のクラウドデプロイメント全体、サブスクリプション全体、またはプロジェクト全体と、はるかに広い範囲をカバーします。これらのポリシーは、CSC のすべてのクラウドリソースにわたって一貫したコンプライアンスとセキュリティ基準を適用する上で不可欠です。通常、これらのポリシーはクラウド管理者によって確立され、個々のユーザーまたはサービスによって、もしくは、個々のユーザーまたはサービスのために変更されることはありません。これにより、デプロイメント環境全体で一貫したセキュアなベースラインが維持されます。

これらのポリシーは、それぞれ用途と範囲が明確に区別されており、 多くのクラウドサービス 内で実現可能な多層的なアクセス制御の指針となっています。CSP は、PBAC モデルを採用することで、最小特権の原則に従ったきめ細かい権限付与を可能にします。このモデルでは、ユーザーとサービスがタスクを完了するために必要なアクセス権のみを保持し、セキュリティ攻撃につながる可能性のある過剰な権限から保護します。

5.5 最小特権と自動化

最小特権の原則は、セキュリティの基本原則であり、職務を遂行するために必要な最小レベルのアクセスを個人に提供するという概念に基づいています。この原則を大規模に効果的に実施するには、並外れた困難が伴う場合があります。クラウドサービス、特に IaaS は、セキュリティポスチャを強化する可能性がある一方で、複雑さを大幅に増す可能性がある綿密なエンタイトルメントを提供します。エンタイトルメントは、特定の規則として理解できます。*このエンティティは、これらの属性を持つ条件下で、これらのリソースに対してアクションを実行できます。* オプション、エンティティ、リソース、条件の数が増えると、これらの変数の管理と予測は複雑になります。この複雑さは、多くの場合、過剰な権限、セキュリティリスクの発生、権限不足につながり、業務に支障をきたすことがあります。

クラウドベースの IAM の規模が大きくなるにつれ、自動化は権限の効果的なバランスを実現するための数少ない実現可能な戦略の 1 つになりつつあります。IAM 権限を自動化するための単一の標準はありません。そのアプローチは、使用されている特定のテクノロジーによって異なります。しかし、以下のように、ある種の自動化手法がクラウドのセキュリティ強化に成功しています。

- **使用状況のトラッキング：** これには、クラウドプラットフォーム内のエンティティのアクティビティを長期にわたって監視することが含まれます。次に、割り当てられた権限と実際の使用状況を分析します。一定期間内に利用されなかった権限は、セキュリティ強化のために自動的に取り消されます。
- **リスクスコアリング:** この方法では、各エンティティとアクションに、アクションの IP アドレスや時間などのさまざまな属性に基づいてリスクスコアが割り当てられます。これらのスコアはポリシーエンジンに入力され、アクションを許可または拒否します。ポリシーエンジンでは、あらかじめ設定されたエンタイトルメントのみに基づくのではなく、特定の状況でリスクレベルが許容できるかどうかも評価されます。
- **JIT 権限：** JIT 権限は、必要に応じて要求され付与されます。エンティティは、メンテナンスウィンドウの間など、指定された時間枠内で特定のリソースに対する事前に定義された権限セットにアクセスするために、テンプレートを使用します。 JIT アクセスはポリシー制約に準拠してい

る場合に許可され、また、追加の許可が必要になる場合があります。リスクスコアリングシステムとの統合により、JIT をさらに強化できます。

- **継続的な評価：** cloud security posture management（CSPM）などのツール、またはアイデンティティにフォーカスしたソフトウェアは、クラウド環境内の IAM 設定と実際のアクセスパターンを継続的に評価し、設定ミス、不要な権限、およびその他のセキュリティの欠陥がないかどうかを調べます。これらの問題は、手動または自動修復で対処できます。例えば、ツールは多数のデプロイメント環境をスキャンして、MFA なしで管理者のロールを使用することにフラグを付けたり、許可されていない静的アクセスキーの存在を識別したりします。

Cloud Identity and Entitlement Management のようなツール類は、これらの機能を組み合わせて実装することができ、さらには修正処置などの追加オプションを含めることもできます。

5.5.1 アイデンティティとゼロトラスト

アイデンティティは、あらゆるゼロトラスト戦略の中核要素の 1 つです。ゼロトラストには複数の定義とモデルがありますが、そのどれもが次のような IAM の原則を共有する傾向があります。

- アクセスと接続はアイデンティティを意識します。
- アイデンティティの意識は、人間だけでなく、すべてのエンティティタイプに拡張されます。
- 属性が追跡され、意思決定に利用されます。
- エンティティ、属性、接続、要求されたアクション、およびリソースに基づくリスクスコアは、ポリシーに基づく意思決定に使用されます。

例えば、ゼロトラストの実装では、ユーザーが信頼できないシステムからのウェブメールへのアクセスを、特定の時間帯に限り、 MFA が有効になっている状態で、特定の地域に限り、添付ファイルのダウンロードが無効になっている状態で許可される場合があります。同ユーザーは、公式の企業システムからのみ添付ファイルにアクセスできます。

ゼロトラストは、本ドメインを通じて議論されている多くの原則に沿っており、クラウド固有のものではありませんが、分散化とクラウドコンピューティングへの移行を進める CSC においてアクセスを可能にするための主要な戦略として、ますます注目されています。ゼロトラストは、IAM 境界の実装を改善する強力な選択肢にもなります。

5.5.2 利用者のアイデンティティ

クラウドでホストされるアプリケーションは、独自のアイデンティを管理しなければならない場合があります。開発者には、このニーズに対応するいくつかのオプションがあり、それぞれに固有の利点と考慮事項があります。アプリケーション固有のユーザーデータベース内で利用者アイデンティを直接管理することも、そのような選択肢の 1 つです。このアプローチでは、セキュアでスケーラブルなアイデンティティストアを確立し、ユーザーデータを安全に処理し、増大する要求に迅速に対応できるように維持する必要があります。

あるいは、フェデレーションは、Google、Facebook、またはさまざまなエンタープライズ SSO システムなどの外部 IdP の既存の認証情報を活用できます。この方法により、CSC は既存のアカウントを使用してサービスにアクセスできるため、ログインプロセスが簡素化され、ユーザーの利便性が向上します。ハイブリッドアプローチは、フェデレーションログイン方式をサポートしながら、自己管理のアイデンティティの柔軟性を提供するため、両方の長所を兼ね備えています。この戦略は、多様なユーザーの嗜好や要件に対応することで、カスタマイズされたユーザーエクスペリエンスを可能にします。

アプリケーションが CSC からクラウドサービスへの直接 API コールを可能にする場合、このアクセスのセキュリティ保護が最も重要になります。API キー、OAuth トークン、またはその他のメカニズムなどのセキュアな認証方法の実装は、アクセスの制御およびアクターが実行できるアクションの範囲の定義に使用されます。特定のユーザーの役割に応じて、読み取り専用機能、書き込み機能、完全な管理者権限など、さまざまなアクセスレベルにわたって権限を定義するには、堅固な認可管理の実施を確実にすることが不可欠です。

AWS Cognito を提供する AWS や、B2C を提供する Azure を含む CSP は、利用者アイデンティティの管理を効率化します。これらのサービスは、サインアップ、サインイン、アクセス制御などの機能を提供し、IdM の複雑さを簡素化します。サードパーティのアイデンティティソリューションは、これらの機能をさらに拡張し、ユーザーエクスペリエンスを強化し、セキュリティ機能を強化し、複数のプラットフォーム間の統合を容易にします。

サマリ

IAM は極めて重要であり、パブリッククラウドサービスとデプロイメント環境へのアクセスを管理する主な手段として、アイデンティティが従来のネットワーク境界よりも優先されます。クラウドセキュリティの中核をなす原則は、クラウドネイティブのセキュリティ侵害の大半はクレデンシャルの漏洩に起因するという認識であり、堅牢なアイデンティティ確認方法の重要性が強調されています。

MFA は、すべてのクラウドアクセスに不可欠な要件として推奨されています。この対策では、パスワードだけでなく、複数の認証要素が必要になるため、不正アクセスのリスクが大幅に軽減されます。さらに、管理者権限レベルのアクセスには、JIT アクセスまたはその他の高度な特権 IdM メカニズムの実装が推奨されており、これにより、必要なときに、必要な期間だけ権限が付与されます。

CSP は通常、独自のアイデンティプールを提供しますが、企業がフェデレーションを採用するための強い理由があります。フェデレーションにより、既存の IdP とのシームレスな統合が可能になり、ユーザーは他のサービスから確立されたクレデンシャルを使用して認証できるようになり、ユーザーエクスペリエンスが簡素化され、IdM が統合されます。

主要な CSP は、アクセス権限をきめ細かく制御できる PBAC を採用しています。PBAC は詳細なポリシー適用によってセキュリティを強化する一方で、IAM フレームワークにさらなる複雑さをもたらします。

効果的な IAM 戦略は、セキュアな IdP と強力な認証プロトコルを組み合わせることです。業務に必要なアクセスだけをユーザーに提供することに重点を置いています。さまざまな状況やポリシーの種類に基づいたルールを使用します。

包括的な IAM 戦略を構築する際には、クラウドアーキテクチャのさまざまなコンポーネントにまたがるこれらのプラクティスを詳細に文書化し、明確にすることが重要です。このような文書は、MFA の採用の背後にある論理的根拠、特権アカウントでの JIT の使用、独自のアイデンティティストアを上回るフェデレーションの利点、PBAC システムの複雑さをカバーする必要があります。また、IAM プラクティスとビジネス目標の整合、セキュリティ対策とユーザーエクスペリエンスのバランス、新たな脅威やテクノロジーに対応する IAM の継続的な進化についても掘り下げる必要があります。

推奨事項

アイデンティティ管理

- クラウドサービスのアイデンティと認可を管理するための包括的なポリシー、計画、プロセスを策定します。
- アイデンティティブローカーを使用してアイデンティティソースに対するガバナンスを強化することを検討します（該当する場合）。
- CSP は、オープンスタンダードを使用して内部アイデンティティとフェデレーションを提供する必要があります。
- 魔法の杖はありません:まずユースケースと制約を選択し、次に適切なソリューションを見つけます。

アクセス管理

- 外部 CSP に接続する場合は、可能であればフェデレーションを使用して既存の IdM を拡張します。クラウド CSC が提供するアイデンティに紐付けられないアイデンティのサイロを最小限に抑えます。
- CSC には、IdP を維持し、信頼できる情報源に基づいてアイデンティと属性を定義する責任があります。
- クラウド利用者は、すべてのクラウドアクセスに MFA を使用すべきで、フェデレーション認証を使用する場合は MFA ステータスを属性として送信すべきです。
- セキュリティおよびビジネス要件に沿った各クラウドデプロイメントのエンタイトルメントマトリックスを文書化します。
- CSP またはプラットフォームでサポートされている場合、エンタイトルメントマトリックスを技術ポリシーに変換します。
- RBAC よりも ABAC や PBAC を優先します。
- 最小権限、JIT アクセス、リスクスコアリングの改善のための使用状況トラッキングなど、よりモダンな IAM プロセスとテクノロジーを評価して採用します。

セキュリティ対策

- 盗まれたクレデンシャルやセッショントークンを使用した攻撃のリスクを軽減するために、特に機密性の高いリソースや管理アクセスに対して、ロケーションベースの制限を備えた IAM 境界を実装することを検討します。
- 静的なクラウドクレデンシャル（ハードコードされた API キーなど）の使用を可能な限り排除します。
- 自動評価ツールを使用して、IAM の設定ミス、過剰なアクセス、コンプライアンス違反、その他の課題を監視します。重大なポリシー違反に対する自動修復を検討します。
- IdP と RP の両方ですべての IAM の変更を記録し、監視します。

インシデントレスポンス

- 悪用された IAM セッショントークンを無効化または制限するための計画と手順をインシデント対応プログラムに統合します。

追加のガイダンス

- Machine Identity in Cybersecurity and IAM | CSA
- What is IAM for the Cloud? | CSA
- Zero Trust Principles and Guidance for Identity and Access | CSA
- Identity and Access Management Glossary | CSA

ドメイン 6: セキュリティモニタリング

はじめに

このドメインでは、クラウド環境に固有のセキュリティモニタリングの課題とソリューションを提供します。ここでは、クラウドテレメトリ、マネジメントプレーンログ、サービスログとリソースログ、高度なモニタリングツールの統合といった異なる側面に重点を置いています。相互運用性やセキュリティの考慮事項など、ハイブリッドとマルチクラウドのセットアップの複雑さについて解説します。さらに、包括的なセキュリティ監視におけるログ、イベント、構成検出の重要な役割が強調されています。最後に、クラウドのセキュリティを強化し、クラウドインフラストラクチャを保護するための多面的なアプローチを提供する革新的なツールとして生成 AI（Generative Artificial Intelligence）を紹介します。

学習目標

このドメインでは、次のことを学びます。

- クラウド環境におけるセキュリティ監視の固有の課題を特定します。
- クラウド環境の監視におけるクラウドテレメトリ・ソースの重要性を説明します。
- クラウド環境のセキュリティテレメトリのためのコレクションアーキテクチャを分析します。
- モニタリングとアラートをクラウドセキュリティの基盤コンポーネントとして認識します。
- 包括的なセキュリティ監視のための検出パスを実装します。

6.1 クラウドモニタリング

クラウドインフラストラクチャの動的な性質は、クラウドのセキュリティモニタリングに固有の課題をもたらします。アラートとログのタイミング[81]は、クラウド内の変化のペースが速いことと、リソースの分散方法によって異なる場合があります。特別な戦略が必要です。さらに、セキュリティ責任共有モデル（SSRM）は、モニタリングの一面はクラウドサービス利用者（CSC）が担当し、その他の側面はクラウドサービスプロバイダ（CSP）が担当することを示しています。

[81] Alerts are different from events. In the context of security monitoring, events represent the raw data or activities captured within a system or network, while alerts are actionable notifications derived from the analysis of events, signaling potential security threats or incidents that demand attention and response from security teams. Events serve as the input for generating alerts, which help security professionals prioritize and respond to security events effectively and promptly.

クラウドでは、次のような点でセキュリティモニタリングの複雑さを増加させます。

1. **マネージメントプレーン：** マネージメントプレーンは、船長が船を操縦するように、すべての管理行動をコントロールします。クラウドコンソールは最も重要な決定を行い、クラウド内のすべてのものへのアクセスを許可するため、厳密に監視する必要があります。

2. **速度:** クラウドでは変化が高速で起こります。この急速なペースは、セキュリティプロセスを俊敏にする必要があり、潜在的な脅威に対応するための自動化された対応が必要であることを意味します。

3. **分散と隔離：** クラウドリソースは、大きな倉庫の区画のように分散して隔離されています。適切な分散と隔離により、1つの領域への侵害によってシステム全体が危険にさらされることはありません。とはいえ、クラウド全体を俯瞰するためには、ログをある程度集中化することも必要です。

4. **クラウドスプロール**とは、CSC のクラウド環境内で多様なワークロードタイプが広範囲に拡散し、複数の CSP が採用されていることを指します。このようなクラウド資産がさまざまなプラットフォームやサービスに分散するという現象は、セキュリティの監視と管理を複雑にしています。クラウドの無秩序な増加を管理するには、多様なクラウド資産の監視と保護の複雑さに対処する包括的な戦略が必要です。

一方、クラウドコンピューティングは、新しいセキュリティ監視手法の機会も生み出します。ほとんどの CSP サービスの構成はシンプルな API を通じて確認できるため、構成を分析して洞察を得る高度なポスチャ管理ツールの機会が生まれます。

6.1.1 ログとイベント

ログとイベントは、セキュリティモニタリング、コンプライアンス、アカウンタビリティの基本であり、クラウドセキュリティとリスク管理の実践の広範なコンテキストです。これらは、クラウドシステム、ネットワーク、およびアプリケーション内で発生しているアクティビティや動作に関する重要な洞察を提供します。これらは CSP 毎に異なります。

ログはアクティビティ（作成、読み取り、更新、削除など）の比較的完全な記録を提供し、非常に詳細で、通常は永続的に保存されます。ただし、ログの品質はサービスによって異なり、バッチ配信が遅れる場合もあります。ログは耐久性があり、通常は保存され、ストリーミングされることもあります。

一方、**イベント**は通常、変更（すなわち、作成、更新、削除（C-UD））のみを記録する点で異なります。Amazon Web Services（AWS）GuardDuty、Microsoft Sentinel、Google Cloud Platform（GCP）Security Command Center などのサービスから、特定の条件によってセキュリティアラートが発せられることがよくあります。ログとは異なり、イベントは一過性であり、明示的に保存されない限り保持されません。イベントは、ログが提供するコンテキストの詳細に欠ける場合がありますが、通常は高速で、多くの場合、記録されたアクティビティから数秒以内に使用可能になります。

ログは調査に必要なデータの深さを提供し、一方、イベントから得られたアラートは迅速な対応策に不可欠なタイムリーな通知を提供します。

ログとイベントは、次のような活動において重要な役割を果たします。

- **継続的な監視とリスク管理：**ログやイベントをリアルタイムまたはほぼリアルタイムで監視することで、組織は、セキュリティインシデントを迅速に検知し対応する能力を強化できます。
- **異常と脅威の検出：** ログとイベントは、統計分析、機械学習アルゴリズム、またはルールベースのシステムを使用して評価され、異常なアクセスパターン、構成の不正な変更、異常なネットワークトラフィックなどの異常な動作を検出します。異常な活動とは、アクティブな脅威についての明確な指標というより、むしろ潜在的な課題についての早期の警告です。
- **インシデント対応とフォレンジック：** ログとイベントにより、インシデントの発生前と発生後のアクティビティを詳細に追跡できるため、根本原因、影響範囲、および改善作業の特定に役立ちます。
- **コンプライアンスと監査の要件：** 多くの規制フレームワークは、監査目的でのログの収集と保持を義務付けており、クラウドセキュリティプラクティスの説明責任と透明性を確保します。
- **パフォーマンスと運用に関する洞察：** セキュリティに焦点を合わせた内容ではありませんが、リソース使用率、ネットワークトラフィックパターン、アプリケーションパフォーマンス指標などのメトリクスを監視することで、クラウドインフラストラクチャを最適化し、全体的な運用効率を高めることができます。[82]

6.1.2 アラートとモニタリング

クラウドでは、その能力により攻撃の実行を加速できるため、従来の検出方法を大幅に上回る多くの攻撃を自動化して迅速に実行できます[83]。この特性は、脅威を迅速に特定して対応するために、クラウドマネージメントプレーン（コンソールとも呼ばれる）を監視するアラートシステムを必要とします。このタイプのシステムの要は、AWS CloudTrail、Azure Monitor、GCP Cloud Monitoring が提供する包括的なログの維持です。これにより、クラウド環境内のリソース、ユーザー、API、およびネットワークアクティビティへの包括的な可視性を提供します。

さらに、堅牢なセキュリティモニタリング戦略を設計するには、クラウド環境を標的にすることが多いさまざまな攻撃ベクトルを理解することが不可欠です。IaaS 環境や PaaS 環境など、さまざまなクラウドサービスモデルに共通する攻撃ベクトルとエクスプロイト手法を調べることで、組織は直面するセキュリティリスクをよりよく理解し、それに応じて監視作業をカスタマイズできます。[84]

---

[82] In practice, logs can be considered as more permanent records of events, often retained for long periods and archived or stored in centralized repositories for future reference. It is technically possible to store all events and organize them into logs, however, organizations may need to prioritize what data to log based on factors such as storage, performance, and regulatory requirements.
[83] While attacks can be automated and executed quickly regardless of the hosting environment, the characteristics of cloud environments, such as elastic compute resources and automated provisioning, may enable attackers to scale their operations more efficiently, and rapidly perform malicious activities.
[84] CSA. (2023) Understanding Cloud Attack Vectors

6.1.3 ログとアラートの適時性

クラウドセキュリティの重要な違いの1つは、ログとイベントデータを受信し処理し、そして、関連するアラートを生成するペースです。クラウド攻撃が加速度的に進行するように、同様の迅速な対応が求められるため、アラートの大幅な遅延は受け入れられません。さらに、マネージメントコンソールのコントロールを失うリスクが高いため、疑わしいアクティビティを即座に検出して対処できるように、アラートはマネージメントプレーンを総合的にカバーする必要があります。

そのためには、新たな攻撃をタイムリーかつ正確に検出することを優先する方法でログが収集され、分析されることを確実にするよう、ログ管理戦略を詳細に掘り下げることが要求されます。

6.1.4 主要な指標の監視

特に未使用の地域における異常なアイデンティティアクセス管理（IAM）やネットワークセキュリティ活動などの重要な指標は、サイバー攻撃の初期段階を示すことが多いため、注意深く監視する必要があります。 MITRE ATT&CK®[85]フレームワークは、どの指標がどの攻撃戦術に関連しているかを示すコンテキストを提供できるリソースであり、組織は自社の環境に最も関連する攻撃に集中できます。

6.2 クラウドテレメトリ・ソース

クラウドテレメトリ・ソースは、組織のクラウド環境を可視化し、管理アクションから個々のサービスのやり取り、リソースパフォーマンスまでを追跡します。詳細な情報を継続的に収集して共有することで、クラウド環境で何が起こっているかを「見る」「聞く」機能を提供します。この情報は、それから、 CSC のクラウド環境の健全性、パフォーマンス、セキュリティを分析して把握するために、セキュリティツール、管理者、または 自動化プロセスによって処理されます。次のセクションで詳しく説明するクラウドテレメトリ・ソースの概要については、次の図を参照してください。

[85] MITRE (2024) MITRE ATT&CK®

図27: クラウドテレメトリ・ソース

6.2.1 マネージメントプレーンのログ

マネージメントプレーンのログは、クラウド環境で実行されたコマンドやコントロールの詳細を示す日誌のようなものです。クラウドリソースの管理方法に関する重要な洞察を提供します。マネージメントプレーンのログ分析は、誰がクラウドインフラストラクチャにアクセスし、どのようなアクションが実行され、いつ実行されたかについて、組織に可視性を提供します。この可視性は、クラウド環境でガバナンス、コンプライアンス、セキュリティを維持するために重要です。

6.2.2 サービスログやアプリケーションログ

サービスログやアプリケーションログは、個々のサービスやアプリケーションの日誌のように機能し、API アクセスやネットワークトラフィックなどのあらゆる操作を記録します。これらは、疑わしいアクティビティの発見やフォレンジック調査に不可欠です。これらのログは、ユーザー認証の試行、ネットワークトラフィック、データ転送、サービス固有のイベントなど、幅広いアクティビティを収集します。サービスログを調べると、CSC はクラウドサービスの健全性、パフォーマンス、セキュリティを監視するために役立ちます。

6.2.3 リソースログ

リソースログは、仮想マシン（VM）、データベース、SDN などのリソースに特化したログで、あらゆる操作や変更が記録されます。これには、リソースのプロビジョニング、構成の変更、データアクセスと転送、システムレベルのアクティビティなどのイベントが含まれます。組織は、リソースログを分析

することで、リソース使用率の最適化、課題のトラブルシューティング、個々のクラウドリソースに影響を与える不正または異常な動作の検出を行うことができます。

6.2.4 クラウドネイティブツール

クラウドツールは、ログの解釈や対応の自動化に欠かせないコンポーネントです。クラウドテレメトリ・ソースに含まれる豊富な情報を解釈し、活用する上で重要な役割を果たします。一般的に使用されるクラウドツールには、Cloud Security Posture Management（CSPM）、Cloud Detection and Response（CDR）、SaaS Security Posture Management（SSPM）、Data Security Posture Management（DSPM）、Cloud Workload Protection Platform（CWPP）、Cloud Native Application Protection Platform（CNAPP）などがあります。これらのツールは、リアルタイムの脅威検出、コンプライアンス監視、構成管理、インシデント対応の自動化などの機能を提供します。組織は、クラウドツールをセキュリティ運用に統合することで、クラウド環境全体のセキュリティイベントを効果的に監視、分析、対応できます。

以下に、クラウドセキュリティとコンプライアンス管理の特定の側面に対応するように設計された特定のタイプのクラウドツールのセット（CSPM、CDR、SSPM、DSPM、CWPP、CNAPP など）について説明します。

- **Cloud Security Posture Management（CSPM）**は、組織がクラウドインフラストラクチャのセキュリティステータスを継続的に監視、評価、改善するために役立つツールとプラクティスです。クラウドサービスやリソース全体の設定ミス、コンプライアンス違反、セキュリティリスクの特定に役立ちます。CSPM ツールが提供する機能には、継続的な監視、自動修復、コンプライアンスレポートなどがあり、CSC は全体的なセキュリティポスチャを強化し、規制要件に準拠することができます。これは、要塞の錠前、警報機、壁を補強しながら、すべての防御が設定された基準に達していることを確認するようなものです。
- **Cloud Detection and Response（CDR）**は、クラウド環境内のセキュリティの脅威やインシデントを検出して対応するために設計されたツールです。高度な分析、脅威インテリジェンス、場合によっては機械学習アルゴリズムを活用して、疑わしい活動、異常な行動、侵害の指標（IoC）を特定します。CDR ツールは、インシデントの迅速な検出、調査、対応を促進し、クラウドにおけるセキュリティ侵害や不正アクセスの試みの影響を軽減するために役立ちます。
- **SaaS Security Posture Management（SSPM）**は、適切な構成とエンタイトルメントを確保し、組織が SaaS アプリケーションを管理および監視できるようにするためのツールです。これらのツールは、複数の SaaS アプリケーションにわたるセキュリティコントロール、構成、コンプライアンスステータスを一元的に可視化します。SSPM ツールは、SaaS セキュリティの有効性の評価、セキュリティポリシーの適用、契約上の義務や規制要件との整合性の確保に役立ちます。
- **Data Security Posture Management（DSPM）**は、機密データを保護し、クラウド環境内のデータ保護規制へのコンプライアンスを確保するツールです。DSPM ツールは、データの検出、分類、暗号化ポリシーの適用、不正アクセス、データ漏洩、内部脅威からデータを保護するための適切なアクセス制御を確保する機能を提供します。DSPM ツールは、クラウドベースのアプリケーション、データベース、ストレージリポジトリ間でデータのプライバシー、完全性、機密性

を維持するために役立ちます。クラウド環境における DSPM ツールは、銀行のリスク管理担当者のようなものです。機密データが適切に保護され、これらのデータの取り扱いがすべて厳格な規制に従っていることを確保します。これは、銀行が資産を保護し、金融関連の法令に従って盗難を防止し、完全性を確保することと似ています。

- **Cloud Workload Platform Protection（CWPP）**は、ハイブリッドクラウドアーキテクチャ全体に展開されるワークロードにターゲットを絞ったセキュリティを提供するツールです。これらのツールは、場所（オンプレミスまたはパブリッククラウド）に関係なく、物理サーバー、仮想マシン、コンテナ、およびクラウドの導入を保護します。CWPP は、継続的な監視を利用して疑わしいアクティビティと潜在的な脅威を特定し、重要なワークロードの運用上のセキュリティと完全性を確保します。
- **Cloud-Native Application Protection Platform (CNAPP)** は、クラウドアプリケーションスタック全体の包括的なセキュリティのための統合プラットフォームを提供することで、ライフサイクル全体を通じてクラウドアプリケーションのセキュリティを確保することに重点を置いたツールです。これらのツールは、CSPM や CWPP などの機能を統合し、アプリケーションのセキュリティポスチャを総合的に把握できます。これにより、プロアクティブな脅威検出、脆弱性管理、きめ細かな権限管理が可能になり、アプリケーションを保護できます。さらに、CNAPP ツールはしばしばコンプライアンスの自動化を統合し、データ保護規制の遵守を簡素化します。

6.2.5 クラウドネイティブ CSP セキュリティツールとコンテナ監視

CSP セキュリティツールとコンテナ監視は、セキュリティ環境の拡張です。これらのツールはそれぞれ異なりますが補完的な役割を果たします。

AWS Security Hub[86], Azure Defender[87], GCP Security Command Center[88]など、CSP が提供するクラウドネイティブのセキュリティツールは、組み込みのセキュリティインテリジェンスを提供するクラウドプラットフォームに組み込まれ、統合された専用のセキュリティサービスです。テレメトリ・ソースとアグリゲーションポイントの両方として機能し、このインテリジェンスを提供するためにデータを分析します。これらのツールはクラウドテレメトリ・ソースの重要なコンポーネントであり、ユーザー認証の試行、ネットワークトラフィック、サービス固有のイベントなど、さまざまなアクティビティに関する洞察を提供します。ただし、CSP ごとに独自のツールセットがあるため、制限があり、マルチクラウドの管理が複雑になります。したがって、収集されるテレメトリデータの量と、それを分析および相関付ける機能のバランスを取り、最も重要なセキュリティアラートに対処できるようにする必要があります。

コンテナ監視ツールは、AWS Security Hub、Azure Defender、GCP Security Command Center などの CSP が提供するセキュリティツールやサービスと統合し、クラウドネイティブアプリケーションの包括的なセキュリティカバレッジを以下の方法で提供します。

---

[86] AWS Security Hub is a CSPM service that performs security checks, aggregates alerts, and enables automated remediation.

[87] Microsoft Defender for Cloud is a CNAPP that is made up of security measures and practices that are designed to protect cloud-based applications from various cyber threats and vulnerabilities.

[88] Security Command Center provides proactive and reactive security for posture management and threat detection for code, identities and data.

- **データ集約：** コンテナ監視ツールは、多くの場合、コンテナログ、パフォーマンスメトリック、セキュリティイベントなど、複数のソースのデータを集約するために CSP が提供するセキュリティツールと統合されます。この統合により、クラウド環境全体のセキュリティ関連アクティビティを一元的に可視化できます。
- **相関と分析：** CSP ツールと統合することで、コンテナ監視ツールはコンテナ固有のデータとより広範なセキュリティテレメトリを関連付けることができます。この相関により、セキュリティ侵害や脆弱性を示す可能性のあるパターンや異常を特定することで、より正確な脅威の検出とインシデント対応が可能になります。
- **自動修復：** 一部のコンテナ監視ツールは、CSP が提供する自動化およびオーケストレーションサービスとの統合を提供し、セキュリティインシデントに対応した修復アクションを自動化します。たとえば、コンテナが不審な挙動を示していることが判明した場合、監視ツールは自動化されたアクションを起動してコンテナを隔離したり、ネットワークアクセスをブロックしたり、リソースをスケールダウンしてインシデントの影響を軽減したりできます。

コンテナ監視における主な課題は、以下です。

- **データ量:** これには、複数のホストで実行されている多数のコンテナによって生成される監視データのボリュームを管理する必要があります。ベストプラクティスは、重要なイベントの優先順位付けとノイズ低減のためのデータ集約とフィルタリングメカニズムの実装、および大量の監視データに対応するための拡張性の高いストレージソリューションの活用が含まれます。
- **動的な環境間での可視性：** コンテナ環境は非常に動的であり、ワークロードの要求に応じてコンテナが動的に作成、デプロイ、終了されます。ベストプラクティスは、新しく作成されたコンテナを自動的に検出して監視できる監視ソリューションの実装や、コンテナのライフサイクルイベントの追跡によって、これらの動的な環境全体を確実に可視化することが含まれます。
- **アラートとインシデント対応：** これには、コンテナ化された環境でセキュリティの脅威をタイムリーに検出して軽減するための効果的なアラートとインシデント対応が含まれます。ベストプラクティスは、事前定義された閾値または異常検出アルゴリズムに基づいたアラートの設定、セキュリティインシデントを迅速に調査および修正するためのインシデント対応手順の確立、インシデント対応の準備状況をテストするための机上演習またはシミュレーションの定期的な実施、などがあります。

次の表は、CWPP および CSPM ソリューションを含むコンテナ監視の主な特徴、機能、ユースケース、および利点の概要を示しています。

特徴[89]	コンテナ監視ツール	CWPP	CSPM
焦点	個々のコンテナとコンテナ化されたアプリケーション	コンテナやサーバーレスランタイムの監視など、クラウドワークロードの脆弱性や設定ミスを検出	クラウドマネージメントプレーンのクラウドセキュリティポスチャの脆弱性と設定ミスを検出

[89] Table 7 provides a high-level comparison between CWPP and CSPM.

主な機能	• リソース使用率の監視（CPU、メモリ、ネットワーク） • 稼働状態とパフォーマンスを追跡 • クラッシュとエラーの特定 • 基本的なセキュリティ機能（脆弱性スキャン） • コンテナログに関する洞察	• コンテナイメージと環境の脆弱性を特定 • 設定ミス • コンプライアンスチェック • ランタイム異常	• クラウドのセキュリティポスチャを監視 • クラウドサービスの設定ミスを検出 • コンプライアンス管理に対するテスト構成
ユースケース	• コンテナに関する課題のトラブルシューティング • コンテナのパフォーマンスを最適化 • アプリケーションを健全に維持	• ワークロードを脆弱性から保護 • セキュリティポリシーの導入 • 設定ミスの確実な検出と修正	• セキュリティリスクをプロアクティブに特定して軽減 • 規制へのコンプライアンスを確保
メリット	• コンテナの状態とパフォーマンスをリアルタイムで把握 • コンテナの問題の迅速な特定とトラブルシューティング	• ワークロードのセキュリティに関するリアルタイムの洞察 • コンプライアンスと脆弱性の迅速な特定 • コンテナ化されたアプリケーションの高度なセキュリティ	• プロアクティブなクラウドセキュリティ管理 • エクスプロイト前にセキュリティリスクを軽減 • コンプライアンス保証 • クラウドのセキュリティポスチャの全体像

テーブル 7: CWPP と CSPM の大まかな比較

6.2.6 クラウドテレメトリの限界

テレメトリシステムは、分散したネットワーク間でデータをセキュアに共有するための課題に直面します。これは、分散した異なる環境間でのデータフローの監視と追跡を効果的に行うことに苦労するためです。これらの限界は、包括的なセキュリティ戦略の重要性を強調しています。

重大な制限の一つは、オンプレミスおよび非クラウド環境での監視とデータ収集を含む、従来の手段ではログに記録されない API コールをキャプチャできないことです。CSP は新しい API を頻繁に更新して配備しており、一部の API は文書化が不十分であったり、既存のテレメトリシステムに統合されていなかったりします。その結果、これらの新しい API コールやログに記録されない API コールが気付かれなくなり、セキュリティ監視や脅威検出の死角につながる可能性があります。

さらに、クラウド環境によって生成されるテレメトリデータの量が膨大であるため、監視ツールに過大な負荷がかかり、正当な行動と疑わしい行動の区別が遅れる可能性があります。この遅延は、潜在的なセキュリティ脅威のタイムリーな検出と対応に影響を与える可能性があります。

テレメトリの制限を軽減するために、CSC はクラウドテレメトリをホストベースのセキュリティツール、脅威インテリジェンスフィード、SIEM プラットフォームなどの他のセキュリティコントロールで補完し、包括的なカバレッジと効果的な脅威の検出および対応機能を確保する必要があります。クラウドベースの脅威に効果的に対抗するには、高度な脅威検出技術を組み合わせることが不可欠です。このアプローチは、内部脅威や巧妙な標的型攻撃など、検出が難しい脅威を含む、多様かつ進化する脅威の特性に対応します。

6.3 収集アーキテクチャ

クラウドコンピューティングは、組織がセキュリティテレメトリを収集する方法を大きく変えます。複数のデータセンターとクラウドプロバイダにまたがるクラウド配備の分散性には、テレメトリ収集の新しいアプローチが必要です。これらの変化を進める主な要因は次のとおりです。

1. **分散化：** 従来の中央集中型のデータセンターとは異なり、クラウドの配備はさまざまな場所やプロバイダに分散していることが多く、IaaS、PaaS、SaaS の各モデルにまたがる多様なテレメトリ収集方法が必要となります。

2. **新しいテレメトリ・ソース**：クラウド環境では、クラウドマネージメントプレーン、クラウドイベント（デフォルトではログに記録されないことが多い）、クラウドセキュリティツールフィード、さまざまなサービス固有のログなど、追加のテレメトリ・ソースが導入されます。

3. **様々なスピード:** 様々なログソースによってデータを生成するスピードが異なるため、ほぼリアルタイムでの脅威の検出と対応が求められるようになり、ログ管理が複雑化しています。
4. **ログの保存と分析オプション：** 組織は、テレメトリを効率的に管理するために、セキュリティデータレイクを含むさまざまなログストレージおよび分析ソリューションから選択することができます。

１つの正しい収集アーキテクチャはありません。各プロバイダと技術スタックは固有の要件を提示します。このセクションでは、クラウド環境でセキュリティテレメトリを効果的に管理するための中心となる原則、さまざまな収集オプション、および主要なアーキテクチャアプローチについて説明します。

6.3.1 ログの保存と保持

クラウドコンピューティングでは、大量のデータを保存するための新しい機能を導入しており、CSP は通常、最初に CSP のストレージサービスにログを保存します。クラウド利用者は、このストレージに対して課金されますが、そのデータをオンプレミスの SIEM など他の場所にエクスポートするときにもデータ転送料金が課金されます。

効果的で効率的なログ収集アーキテクチャでは、ログを移動する際のコストと複雑さを考慮することになります。最もコスト効率の高い選択肢は、CSP のストレージサービスにログを残すことですが、検

出、分析、およびその他のアクティビティに問題が生じる可能性があります。その場合、組織は、他のセキュリティモニタリング活動と互換性のない CSP の分析ツールの使用のみに制限されるか、性能要件を満たさない可能性があります。ログをオンプレミスに戻すと、データ転送と物理ストレージ要件の面でさらに大きなコストが発生する可能性があります。サードパーティの SIEM/分析ツールを使用する方法もあります。セキュリティデータレイクは、さまざまなソースや形式のログを受け入れる大規模なストレージプールです。

ログ保持に関する考慮事項は、効果的な監視、トラブルシューティング、コンプライアンスの遵守、およびシステムのコストを確保する上でも役割を果たします。適切なログ保持期間の決定には、運用ニーズ、規制要件、およびコストに関する考慮事項のバランスが必要です。ログを適切な期間保持することで、CSC は履歴データを分析し、傾向の特定、セキュリティインシデントの検出、システム課題のトラブルシューティングを行うことができます。また、耐障害性と規制の目的で、一部のログイベントをクラウド外のストレージに移動する必要性にも注意してください。しかし、保持期間の長期化は保管コストの増加につながり、プライバシーに関わる可能性があります。したがって、CSC は、どのログを、どのくらいの期間、どのレベルのアクセス制御で保持するかを定義する明確なポリシーを確立する必要があります。

通常、ログの保存場所の決定には次の要因が影響します。

- CSP のデフォルトの保存場所
- デフォルトのストレージコスト
- 分析ツール（CSP またはサードパーティ、SIEM、 SOAR[90]、 SIEM as a Service など）との統合
- ログを移動するためのデータ転送コスト
- ログ移動時の移動先ストレージコスト
- 効果的なアクセス制御を実装する能力。運用要件を満たすために、クラウドチームにログへのアクセスを提供する必要がありますが、他の配備環境のログにはアクセスできない可能性があります。

6.3.2 カスケードログアーキテクチャ

カスケードログアーキテクチャは、ログ管理に対する階層的なアプローチです。これを使用すると、ログの収集、集約、分析がカスケード方式で行われます。これにより、あるレイヤーから別のレイヤーへと流れ、集中監視と分析が容易になります。カスケードログアーキテクチャは、本質的にハイブリッドまたはマルチクラウド環境に固有のものではなく、さまざまなインフラストラクチャレイヤにわたって複数のソースからのログを集約して分析する必要があるあらゆる環境に実装できます。ただし、カスケードログは、これらのアーキテクチャの分散性、およびさまざまなオンプレミスおよびクラウドベースのリソースからログを収集する必要がある可能性があるため、ハイブリッドまたはマルチクラウド環境で特に有益です。

[90] SOAR is the acronym for Security orchestration, automation and response.

次の図は、クラウド環境でログを管理する場合の、セキュリティを目的とした賢明なアーキテクチャを示しています。開発環境（Dev）、テスト環境（Test）、本番環境（Prod）ではそれぞれログが生成され、特定のプロジェクトに関連付けられた複数のアカウントの集中ログ管理システムに送信されます[91]。

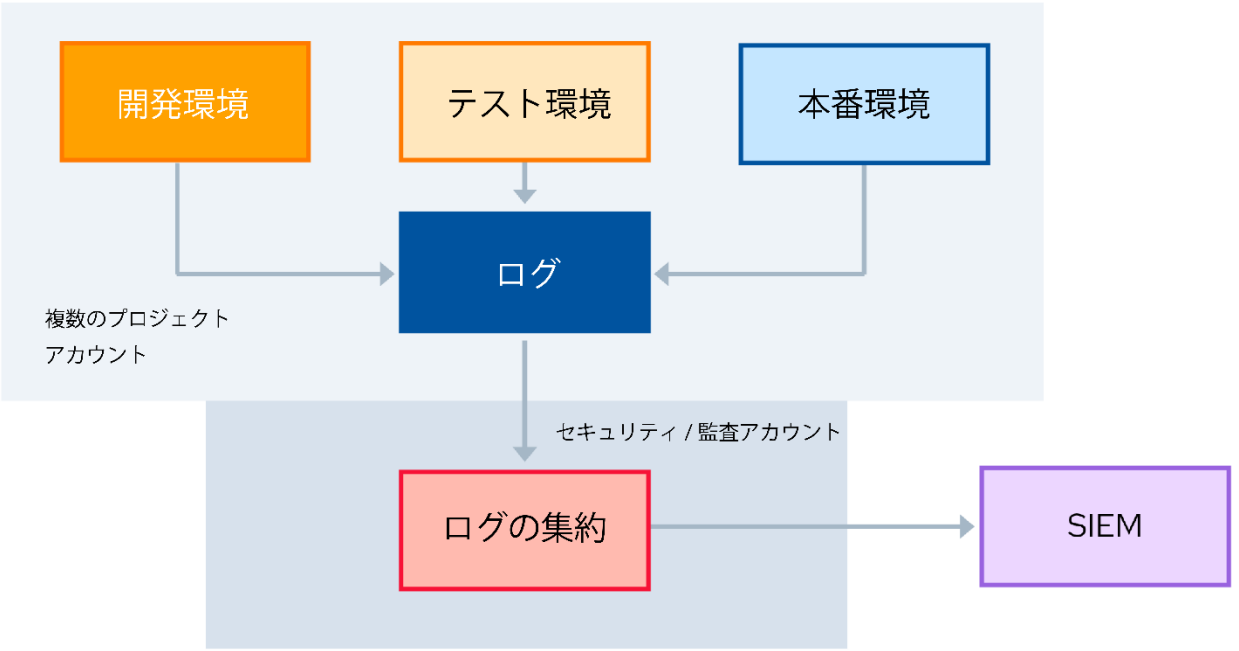


図 28: カスケードログアーキテクチャ

各環境（Dev、Test、Prod）は、中央リポジトリにログを転送するように設定できます。中央ログシステムは、これらのログを集約し、セキュリティに関連するログを単一のセキュリティ/監査環境に送信します。これにより、ログがセキュアに保持され、統合されます。これは、効果的なセキュリティ分析とコンプライアンスのために不可欠です。

最終的に、集約されたログをデータセンターやクラウド SIEM システムにフィードできます。SIEM システムはこれらのログを分析し、潜在的なセキュリティインシデントを特定します。このアーキテクチャは、すべてのクラウド環境にわたるセキュリティ関連イベントを表示し、脅威のタイムリーな検出と対応を促進します。

6.3.3 クラウドセキュリティモニタリング戦略ガイダンス

モニタリング戦略を構築する場合、特にマルチクラウド設定では、ログを 1 か所に統合することが必ずしも最適ではないことを理解してください。代わりに、前のセクションで示したように、カスケードとフィルタリングのアプローチが推奨されます。

[91] The CSC’s account hierarchy must be considered when designing the cascading log architecture.

これは次のことを意味します。

- ログ生成の速度と検出作業におけるソースの重要性を考慮し、ログとアラートの明確な経路を構築します。
- 関連するすべてのアラートと選択したログをセキュリティオペレーションセンター（SOC）に転送すると同時に、ほとんどの生ログをローカライズされたアカウントに保持し、コスト効率とリソースの最適化を実現します。
- 使用率の低いログを低コストのストレージ環境に移動すると、ログシステムに無駄な拡張を加えることなく、ログをアーカイブできます。

SOC は、まずアラートに焦点を当て、次に選択されたログを掘り下げてインシデントを検証し、対応し、プロアクティブに脅威を探す必要があります。

商用ツールの選択は、このようなアーキテクチャの実現可能性に影響を与える可能性があります。したがって、ログデータの近接性[92]と分析の深さのバランスが非常に重要です。この繊細な戦略は、堅牢なクラウドセキュリティを維持するために不可欠な、効果的な監視と迅速なインシデント対応を容易にします。

6.3.3.1 ログの処理速度

モニタリングを理解する上でもう 1 つの重要な概念は、さまざまなクラウドサービスにおけるログの処理速度を区別することです。モニタリングと分析は通常、スローパスとファストパスの 2 つの別々のトラックに分類されます。スローパスはログ専用であり、分析に使用できるまでに最大 15 分の遅延が発生するといった場合があります。ファストパスは通常イベント用ですが、一部のログ用に設計することもでき、ほぼリアルタイムで分析してアラートを生成できます。

AWS のセキュリティツールの例で説明します。

- CloudTrail[93] や Resource Log （S3 アクセスログ、ALB ログなど）のような「スローパス」のログは、通常、詳細な調査に使用されますが、すぐに分析できるとは限りません。
- 一方、CloudWatch[94] のようなサービスが提供する「ファストパス」イベントは、迅速な検出と対応を目的として設計されています。影響の大きい潜在的な課題に対する迅速なアラートをトリガーします。

[92] Log data proximity refers to how physically or logically closely located log data are to the system responsible for collecting and processing those logs. A lesser proximity implies that the log data sources are closer to the central logging system, while a greater proximity indicates that there may be delays or inefficiencies in collecting and processing log data.

[93] AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS accounts.

[94] Amazon CloudWatch is a service that monitors applications, responds to performance changes, optimizes resource use, and provides insights into operational health.

- これらのソリューションは相互に排他的ではなく、異なる機能を提供することを理解することが重要です。包括的なセキュリティ監視のためには、これらのソリューションを併用する必要があります。
- 迅速なセキュリティインシデント対応にはファストパスログが不可欠ですが、インシデント後の徹底した分析やフォレンジックにはスローパスログが有効です。GuardDuty[95]などのサービスは脅威インテリジェンスと監視を提供し、Detective や Athena[96]などのツールはセキュリティイベントの分析と対応を支援します。
- 重要な点は、両方のパスを活用して、脅威へのタイムリーな対応とセキュリティインシデントの詳細な調査を確実に行うことです。

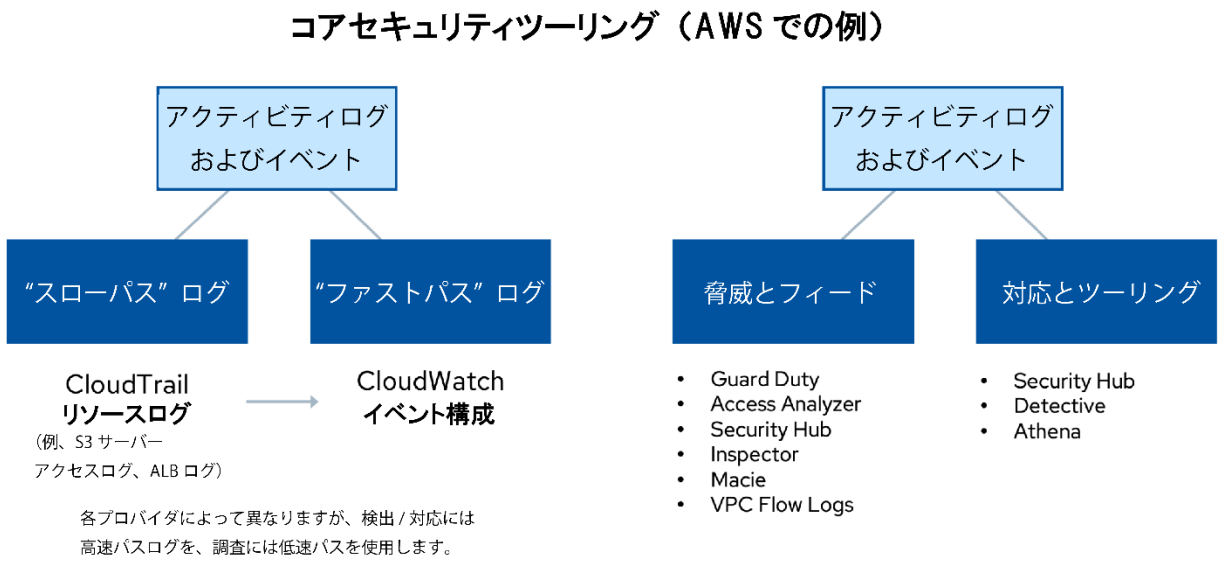


図 29: AWS のセキュリティツールを使用した、さまざまなクラウドサービス内のログ処理速度

6.3.4 セキュリティデータレイク

セキュリティデータレイクとは、多様なクラウド環境やツールから収集されたセキュリティデータの量や関連する種類のデータを処理および分析するために設計された、一元化されたリポジトリのことです。このデータアーキテクチャでは、構造化および非構造化形式を含む大容量データを管理するためのスケーラビリティを提供する必要があります。その柔軟性は、高度な分析がサポートされ、機械学習と AI がセキュリティデータから洞察を抽出し、脅威を効率的に特定できるようにする必要があります。セキュリティデータの一元化と統合の目的は、インシデントの検出、分析、対応を改善し、全体的なセキュリティポスチャを強化することです。

[95] Amazon GuardDuty combines ML and integrated threat intelligence from AWS and leading third parties to help protect your AWS accounts, workloads, and data from threats.

[96] Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL.

セキュリティデータレイクは以下の機能を提供します。

- インシデント対応とフォレンジック分析の向上
- 対応と脅威ハンティングのための包括的で履歴のあるデータセットへのアクセス

6.4 検知とセキュリティ分析

さまざまなセキュリティ課題を検出して対応する包括的な監視システムには、ログ、イベント、構成検出パスが不可欠です。

すでに説明したように、ログは、その量と複雑さのために、より多くの分析時間を必要とするスローパスとなります。しかし、これらは包括的であり、異なる IP からのログイン試行の繰り返しなど、時間の経過に伴うパターンに基づいたアラートをサポートできます。ログは通常、サードパーティまたは社内で開発されたツールを使用して分析されます。

イベントは、ほぼリアルタイムのアラートを提供するファストパスとなります。ログに似たデータが含まれる場合もありますが、クラウド内の C-UD[97]に焦点を当てています。イベントは、AWS GuardDuty、Azure Defender、GCP Security Command Center などの CSP セキュリティツールによって生成されることが多いです。キャプチャするのは困難ですが、価値の高いデータを提供します。

構成検出では、クラウド配備の脆弱な設定を特定します。脆弱性は、ログ、イベント、または CSPM ツール内で検出できます。適切に設定すると、設定ミスや悪意のあるアクティビティを特定する上で非常に重要になります。Infrastructure as Code (IaC) は、配備前に脆弱性をスキャンできる構成情報の優れたソースにもなります。

[97] C-UD is an acronym for Create, Update, and Delete, where a bad actor will perform an action like creating an administrative account that is used to create a second administrative account, then change the second account so that MFA is not required to authenticate, then delete the first administrative account created. The goal is to make actions performed on behalf of the bad actor hard to detect or trace through log files.

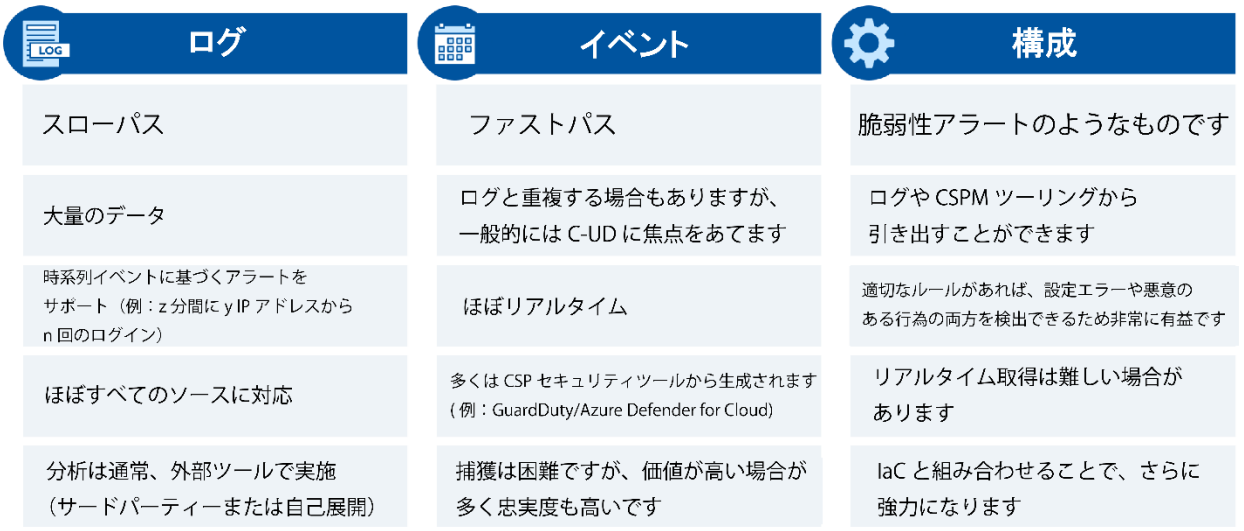


図 30: クラウドセキュリティにおける主要な検出パス: ログ、イベント、および構成

6.4.1 異なる検出ツールの比較

次の表は、クラウドセキュリティ監視で使用される一般的なツールのいくつかを比較した例です。ツールの機能を網羅したものではありません。

特徴	SIEM	CSP アラート	CSPM
焦点	• IT インフラストラクチャ全体	• クラウド特有の課題	• 継続的なクラウド監視
データソース	• さまざまなセキュリティソース(ネットワークデバイス、アプリケーション、クラウドプラットフォームなど)からのログとイベント	• CSPM ツールで生成されるアラート • 環境固有のフィルタリングが必要なため、いくつかの課題がある • アラートはクラウド固有であり、形式や詳細が大きく異なるため、集計が困難	• クラウドのリソース、構成、アクティビティ • 効果と正確性を確保するために、ヘビーチューニングが必要
機能性	• セキュリティデータの集約、分析、関連付け • 通常はスローパスですが、ほとんどのログベースの分析に最適なオプション	• クラウドの潜在的なセキュリティ問題の通知を提供 • ソース/タイミングの把握が必要（アラートは特定のルールが実行された場合にのみ生成される場合があり	• 設定ミス、脆弱性、コンプライアンスリスクの監視 • 検出・分析機能を補完する SIEM と並行して

		ます。例：ルールは 24 時間ごとに実行される）	動作するものもあります • アラートよりもレポートが得意 • クラウドの検出と対応ツール
ユースケース	• セキュリティインシデントの調査、傾向の特定、全体的なセキュリティ態勢の監視	• クラウドセキュリティの潜在的な問題にプロアクティブに対応	• クラウドのセキュリティポスチャを継続的に改善
例	• SIEM で確認された不審なログイン試行をセキュリティアナリストが調査	• クラウドセキュリティチームは、CSPM によってフラグ設定されたオープン S3 バケットに関するアラートを受信	• CSPM は、クラウドストレージリソース上の非準拠の暗号化設定を識別
アラート	• セキュリティデータの相関に基づいてさまざまなアラートを生成	• セキュリティの設定ミス、脆弱性、コンプライアンス違反に関連する特定のアラート	• 特定されたセキュリティ課題に対して CSP アラートを発することがある
メリット	• IT インフラストラクチャ全体のセキュリティポスチャを一元管理	• プロアクティブなクラウドセキュリティ管理を実現	• セキュアなクラウド環境の維持とセキュリティインシデントの回避を支援

テーブル 8: クラウドセキュリティ監視におけるツール比較

6.4.2 実際のセキュリティモニタリングと分析

脅威の検出と対応のためにセキュリティ分析で使用される一般的なアプローチは、次に示すカスケードとフィルタのパターンです。複数の検出メカニズム、つまりフィルタを着信データストリームまたはログに順次適用します。カスケード内の後続の各フィルタは、潜在的な脅威の特定の基準または指標に焦点を当てて、データを調整し、優先順位を付けます。初期データストリームには、さまざまなログエントリまたはネットワークトラフィックデータが含まれます。次に例を示します。

- カスケードの最初のフィルタは、異常なログイン試行や異常なネットワーク動作など、疑わしいアクティビティの高レベルインジケータに焦点を当てる場合があります。
- 後続のフィルタは、既知の攻撃ベクトルまたは脅威アクターに関連する特定の属性またはパターンに焦点を当てて、分析の範囲を段階的に狭めていきます。
- 最終的にセキュリティの脅威が検出された場合、カスケードの最終フィルタによってアラートまたは応答アクションがトリガーされる可能性があります。

- 最後に、カスケード内の検出メカニズムの有効性を高めるために、機械学習や行動分析などの高度な分析手法を活用することが重要です。

次に、カスケードおよびフィルタパターンの例を示します。

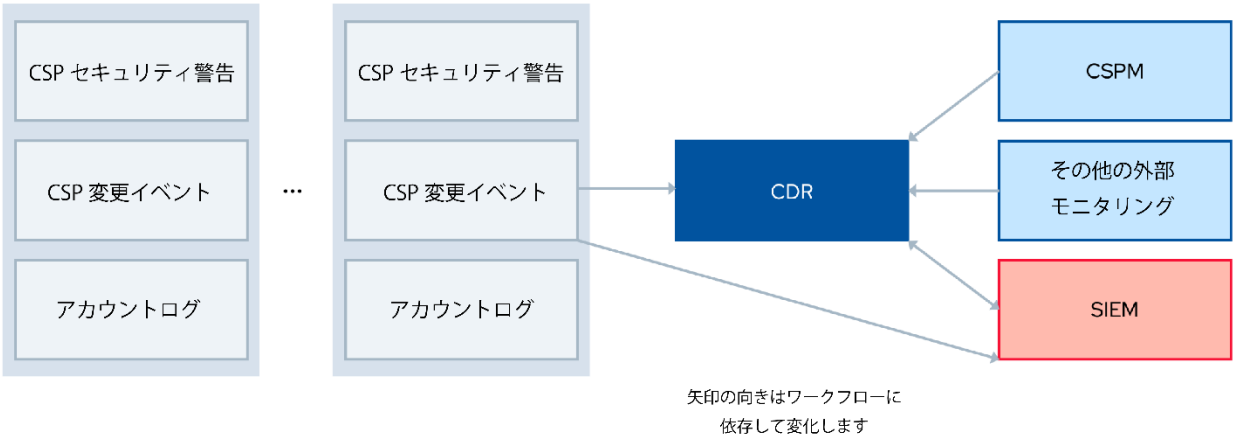


図 31: カスケードおよびフィルタパターンの例

この例では、CSP のセキュリティ警告、変更イベント、およびアカウントログが複数のアカウントから収集されます。これらはフィルタリングされ、適切なツールに送られてさらに処理されます。CDR 経路は、特定された脅威に即座に自動対応するように設計されています。CSPM はセキュリティポスチャの評価と改善に焦点を当てており、多くの場合、コンプライアンスと構成管理に対応しています。SIEM システムは、さまざまなソースからのデータを統合した包括的な分析プラットフォームで、詳細な検討が可能です。

鍵となるのは、複数のツールと経路を活用してセキュアなクラウド環境を確保する、適切に整理された検出および対応戦略です。効果的なクラウドセキュリティ運用には、セキュリティ情報を適切にフィルタリングし、チャネル化する方法を理解することが重要です。

6.4.3 クラウドの検出と対応（Cloud Detection & Response）

ログの集約はモニタリングの最初のステップですが、CDR プロセスはイベントのルールと処理を通じて効果を発揮します。CDR は、複数の機能を組み込むことで、単なるログ集約にとどまりません。CDR は、以下を行います。

- データをフィルタリングしてノイズを排除し、定義されたパターンに基づいて潜在的な脅威を検出します。
- 分析に役立つように情報をコンテキストに応じて充実させます。
- 必要とされる人員またはシステムに通知します。

- SOAR（Security Orchestration, Automation, and Response）機能が含まれている場合があり、自動応答と調査サポートが提供されます。

クラウドイベントは CDR 内でほぼリアルタイムで管理されるため、脅威にタイムリーに対応できます。ただし、SIEM システムと CDR の統合は、採用するツールや構成によって異なります。

6.4.3.1 クラウド検出のベストプラクティス

クラウド攻撃検知のベストプラクティスを考える際には、たとえ仮想ワークロードであっても Indicators of Compromise (IOC[98])は従来のワークロードと同様に機能することを覚えておいてください。

以下のように、セキュリティ上の課題を最も示唆する特定のデータソースを優先する必要があります。

- マネージメントプレーンからのログ
- IAM 活動
- 公開されているリソースの変更
- 構造的なネットワークの変更
- クロスアカウントアクセスやサブスクリプションピアリングなど
- 本番環境の構成変更

クラウド検出機能を強化するために、外部の脅威インテリジェンスと高度な技術を活用することができ、セキュリティ脅威の早期発見には次の 2 つの方法を使用できます。

- 脅威インテリジェンスフィードをクラウド検出システムに統合します。こうすることで、組織は新たな脅威、攻撃ベクトル、セキュリティ侵害の指標（IOC）に関する最新情報を常に把握することができます。脅威インテリジェンスを統合することで、外部の専門知識や知識を活用してセキュリティリスクを特定し、軽減することができます。
- 機械学習アルゴリズムと高度な分析を活用して、潜在的なセキュリティ脅威を示す異常なアクティビティを検出します。大量のデータを分析し、クラウド環境内の異常なアクティビティを特定する機械学習アルゴリズムと高度な分析により、セキュリティの脅威や侵害を示す可能性のあるパターンや行動を検出できます。

開発環境（または非本番環境）のモニタリングは、プロトタイプというこれら環境の性質を考えると、データ量が多く、ノイズが発生する可能性があるため、困難な場合があります。ノイズを管理するには、堅牢なフィルタリング（Robust filtering）が必要です。さらに、意図された変更と悪意を持つ可能性のある変更を区別するために「I intentionally did this」ボタンまたは同様のメカニズムが推奨されます。

[98] CISA. (2023) *Understanding Indicators of Compromise* - IOCs are the digital and informational "clues" that incident responders use to detect, diagnose, halt, and remediate malicious activity in their networks.

6.4.3.2 ディテクタの例（CIS ベンチマーク）

以下に、潜在的なセキュリティの脅威を検出するために監視する必要がある、クラウド環境内の具体的なアクティビティと変更を示します。これらの指標は、Center for Internet Security (CIS[99]) ベンチマークと、IT システムやデータを攻撃から保護するためのさまざまなベストプラクティスに基づいています。

アクセス管理：

- 不正な API 呼び出し
- MFA なしでマネージメントコンソールにログイン
- 顧客管理キーの削除の無効化またはスケジュール設定
- IAM ポリシーのいかなる変更
- root アカウントのいかなる使用

リソース管理：

- クラウドストレージポリシーの変更
- 構成モニタリングの変更
- セキュリティグループの変更
- ネットワークアクセス制御リスト（ACL）の変更
- ネットワークゲートウェイの変更
- VPC の変更(サブネット、ルーティングテーブル、サービスエンドポイントなど)

ロギングとモニタリング:

- ロギングサービスの設定変更
- マネージメントコンソールの認証の失敗

6.4.4 高度な監視：カナリアトークンとハニートークン

攻撃の検出に真にプロアクティブなステータスが存在するはずはありませんが、攻撃から検出までの時間を大幅に短縮する方法があります。このような手法には、「カナリアトークン」や「ハニートークン」などがあり、これらは本物のリソースを模倣するために設計された、おとりの認証情報やデータです。

カナリアトークンやハニートークンは不正アクセスを監視するために使用されます。攻撃者がこれらのおとりと対話すると、警告がトリガーされ、侵害の試みまたは実際の侵害が示されます。たとえば、カナリアトークンをクレデンシャルストアに配置して、正当なユーザーデータとして表示させる

[99] CIS. (2024) *CIS Benchmarks List*.

ことができます。ハニートークンは、データベースやドキュメントなど、攻撃者を引き付ける可能性のあるさまざまな場所に展開できます。

6.5 セキュリティモニタリングのための生成 AI

生成 AI（GenAI）は、ログデータ分析の自動化、処理データのスケーリング、および悪意のあるアクティビティの識別精度の向上など、SOC の効率性と有効性を劇的に向上させる大きな可能性を秘めています。

さらに生成 AI は、堅牢な脆弱性テストの一形態として機能する、模擬攻撃シナリオの作成を支援します。観測されたネットワーク行動パターンに適応し、ログデータを広範なコンテキストで補強することで、アラートの関連性と精度を向上させます。これは、アナリスト、特に経験の浅いアナリストが、複雑なセキュリティイベントと攻撃が通る可能性のある経路を理解するために役立ちます。

さらに、生成 AI はワークフローの提案を提供し、効果的なセキュリティポスチャを維持するために重要なアラートの検証と対応に関するガイダンスを提供します。この AI 主導のアプローチは、クラウドセキュリティツールによってますます活用され、クラウドセキュリティインフラストラクチャに不可欠なものとなりつつあり、チームは脅威をより適切に予測、特定、対応できるようになります。

以下は生成 AI が影響を与える可能性のある項目のリストです。

- 予測分析モデルによるリアルタイムの脅威検出の強化
- ログ分析の自動化と拡張、潜在的な悪意のあるアクティビティの発見、効率性と正確性の向上
- 堅牢な脆弱性テストのための模擬攻撃の生成
- 学習したネットワーク行動パターンに基づいて時間の経過とともにアラートを改善し、アラートによる疲弊を軽減
- ログを充実させ、さまざまなセキュリティログ/イベントに広範なコンテキストを追加
- 若手アナリストが攻撃経路を理解できるよう支援
- アラートの検証と対応においてアナリストを導くためのワークフローの提案
- 実際のシナリオを模倣したテストおよびトレーニング用の合成データを生成。これにより、機密情報を漏洩することなく、セキュリティモデルのテストを行うことが可能。

生成 AI ベースのセキュリティソリューションは、これまでのセキュリティ業界にないイノベーションのペースを示しています。SOC の仕組みを変革する、継続的な迅速なイノベーションと機能を期待しています。

6.5.1 生成 AI の課題と考慮事項

生成 AI はクラウド攻撃の検出と解決を強化する上で大きな期待を持たせていますが、クラウド攻撃がもたらす潜在的な課題と倫理的なジレンマを認識することが重要です。AI モデルを適切かつ効果的に維持

するには、継続的なデータとトレーニングが必要です。しかし、大規模なデータセットに対するこの必要性は、特に大規模言語モデル（LLM）が応答に学習データを組み込む場合に、プライバシーとデータ保護の懸念を引き起こす可能性があります。

さらに、AI 能力の急速な進歩により、スケーラブルなセキュリティソリューションが求められています。正当なアクティビティと AI によって生成されたアクティビティを区別することもまた、セキュリティモニタリングの取り組みを誤解させ、システムにさらなるノイズを生じさせる可能性があるため、ますます困難になります。

最も差し迫った懸念の 1 つは、セキュリティメカニズムを回避または欺くように設計された高度な AI システムである敵対的 AI です。同様に重要なのは、AI が人間の調査活動や監視活動に関与することを取り巻く倫理的な考慮事項であり、プライバシーの基準や規制との整合性を取る必要があります。

AI のような新しい画期的な技術を採用するには、バランスの取れた思慮深いアプローチを取ることが重要です。しかし、AI のセキュリティ運用への統合は避けられず、実践者は堅牢で倫理的なセキュリティプラクティスを維持するために適応する必要があります。

生成 AI の詳細については、Cloud Security Alliance のトレーニング *Introduction to Generative AI & Prompt Engineering*[100] *および Cloud Security Alliance の AI Safety Initiative*[101] *で行われている作業を参照してください。*

サマリ

このドメインは、クラウドテレメトリ、マネージメントプレーン ログ、サービス/リソース ログ、高度なツールに重点を置き、クラウドセキュリティモニタリングに関する固有の課題に対処しています。ハイブリッド/マルチクラウドの複雑さ、ログ/イベントの重要な役割、生成 AI（GenAI）の革新的な使用について取り上げています。

テレメトリはクラウド環境を可視化し、アクションとリソースパフォーマンスを追跡します。しかし、API 呼び出しログやデータ量管理の死角のような課題に直面しています。効果的な戦略には、他のセキュリティコントロールによるテレメトリの補完や、高度な脅威検出技術の使用などがあります。

ログ管理、コストとリソースの効率のバランスを取るには、カスケードとフィルタのアプローチが推奨されます。関連するアラートを SOC に転送し、使用頻度の低いログをコスト効率よくアーカイブすることに重点を置きます。ログ処理速度を区別し、脅威へのタイムリーな対応（ファストパス）と詳細な分析（スローパス）を実現します。

大量のセキュリティデータを処理および分析するための一元化されたリポジトリで、インシデントの検出と対応を強化する高度な分析をサポートします。

[100] CSA, (2023) *Introduction to Generative AI & Prompt Engineering.*

[101] CSA. (2024) AI Saftey Initiative.

包括的な監視には、ログ（スローパス）とイベント（ファストパス）が不可欠です。カナリアトークンやハニートークンのような高度なモニタリング方法で、検出時間を短縮できます。監視する主なアクティビティには、不正な API 呼び出し、IAM ポリシーの変更、ネットワーク構成の変更などがあります。

生成 AI は、ログ分析の自動化、模擬攻撃の生成、アラート精度の向上、アナリストの支援によってセキュリティを強化します。課題には、プライバシーの維持、データの管理、敵対的な AI リスクへの対応などが含まれます。

推奨事項

モニタリングとアラートは、クラウドセキュリティの基本となるコンポーネントです。次のことが重要になります。

- 自動化されたクラウド攻撃に対する迅速な検出に重点を置いています。
- マネージメントプレーンを監視します。
- ログ管理とアラートタイミング戦略を組み合わせて活用します（たとえば、レスポンスとフォレンジックにスローパスログを利用し、ファストパスイベントにアラートを送信して、マネージメントプレーンを含むハイリスクアクティビティを検出します）。
- テレメトリとクラウドツールの使用状況（マネージメントプレーンログ、サービスログ、CSPM、CASB、CNAPP の適用など）を監視し、セキュリティモニタリングを強化します。
- ログを戦略的に収集して分析します（例：カスケードログアーキテクチャと選択的アラートの導入を検討し、マルチクラウド環境でのコスト管理と SOC の効率化を図る）。
- カナリアトークンとハニートークンを導入して誤検知のない確定的なアラートを提供し、生成 AI は脅威の検出と対応効率を向上させる潜在的な道筋を提供します。

追加のガイダンス

- Understanding Cloud Attack Vectors | CSA
- AI Safety Initiative | CSA
- MITRE ATT&CK® Cloud Matrix

ドメイン 7: インフラストラクチャとネットワーク

はじめに

このドメインでは、インフラストラクチャ全体のフットプリントとネットワークセキュリティの管理について説明します。また、クラウドサービスプロバイダ（CSP）のインフラストラクチャセキュリティ責任に関する小さなセクションも含まれています。Infrastructure as a Service (IaaS) におけるインフラストラクチャとは、クラウドに存在するコンピュート、ネットワーク、およびストレージのリソース プールを指します。

以前のバージョンの CSA セキュリティガイダンスと Certificate of Cloud Security Knowledge (CCSK) トレーニング[102]では、パブリックまたはプライベートを問わず、クラウドサービスの構築とホスティングに使用するインフラストラクチャについて、より深い説明が含まれていました。基盤となる技術は幅広く進化しているため、CSP ではなく、クラウドサービス利用者（CSC）で働くセキュリティ専門家を対象としたこのトレーニングでは、その内容については説明していません。他のドメインでは、コンピュート (ワークロード)とストレージ(データ)のセキュリティに関する懸念をカバーしています。

インフラストラクチャのセキュリティの多くは、ワークロード、データ、およびネットワークのセクションでカバーされますが、クラウドインフラストラクチャのすべてのオプションをカバーするいくつかの上位レベルの機能があります。これには以下が含まれます。

- シフトレフト、ガードレール、モニタリングなど、中核となるセキュリティ技法
- セキュアなアーキテクチャ(適切に構築されたフレームワークを含む)
- Infrastructure as Code (IaC)
- 様々なクラウド移行戦略(リフトアンドシフトなど)

このドメインはネットワークセキュリティに重点を置いています。すべての IaaS プラットフォームで使用されている SDN（Software Defined Network）の概念から始まります。コンテナネットワーキングだけでなく、セキュリティグループやその先にあるものにも触れていきます。その後、CSC のデータセンター（ハイブリッド）やワークロードへの接続など、さまざまな接続オプションをカバーします。このドメインはゼロトラストアーキテクチャ（ZTA）と SASE の議論で終わります。SASE フレームワークは、急速にクラウドネットワーキングを実装するための支配的なモデルとなりつつあり、セキュリティ要件によって推進されています。

[102] https://cloudsecurityalliance.org/education/ccsk#
（訳注：原文では参照が空欄となっているが、こちらのウエブサイトを指しているものと思われる）

学習目標

このドメインでは、次のことを学びます。

- クラウドインフラストラクチャのセキュリティ保護に使用される領域と技法を理解します
- クラウドネットワークの基礎を理解します
- コンテナネットワーキングを管理します
- クラウドネットワークのセキュリティを管理し、セキュアなアーキテクチャを設計します
- クラウドインフラストラクチャとネットワークのセキュリティ保護にゼロトラストの手法を適用します
- Secure Access Service Edge（SASE）のセキュリティ管理に使用される技法

7.1 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とは、クラウドコンピューティングのサービスとリソースのインターネット経由での提供をサポートするために必要な、サーバー、ストレージ、ネットワーキング、および仮想化ツールなどの、ハードウェア、ファームウェア、およびソフトウェアコンポーネントを指します。拡張性、柔軟性、コストパフォーマンスに優れた方法でアプリケーションとデータを構築、配備、管理することが可能になります。CSP が提供するセキュアなサービスに基づいてアーキテクチャを設計および構築するのは、CSC の責任です。IaaS と PaaS（Platform as a Service）の設計の多くは CSC に依存しているため、インフラストラクチャの適切な使用と、クラウドのメリットを達成するために役立つ適切に設計（well-architected）された実装を構築する方法を理解することが重要です。

図32: Well-Architected の中心となる柱

7.1.1 セキュアなアーキテクチャ： Well-Architected Pillars

クラウドプロバイダによって若干異なる方法でサポートされるアーキテクトアプローチの1つは、Well-Architected Framework[103]の原則に従うことです。これらの柱に従うことで、クラウドを使用する場合の利用者の成果（セキュリティやコストなど）を向上するための設計と実装の意思決定をガイドします。

Well Architected Framework には以下の 6 つの柱があります。

柱 1：セキュリティ

- ビジネスバリューを提供しながら、情報、システム、および資産を保護
- すべてのアーキテクチャレイヤに対してセキュリティを適用
- セキュリティのベストプラクティスの自動化、トレーサビリティの実現、およびアクセス制御の管理

柱 2：優れた運用性

- システムの実行とモニタリングに注力し、ビジネス価値を実現
- プロセスと手順の継続的な改善
- 変更の自動化、イベントへの対応、および日常業務を管理するための標準の定義

柱 3：信頼性

- ワークロードが意図した機能を確実に正しく一貫して実行できるようにする
- 障害から迅速に復旧し、ビジネスと顧客の需要を達成する
- リカバリ手順のテスト、水平方向の拡張による可用性の向上、および障害からの自動リカバリ

柱 4：パフォーマンスの効率化

- システム要件を満たすためにコンピューティングリソースを効率的に使用
- 需要の変化と技術の進化に応じて効率性を維持
- 実験の頻度を増やし、サーバーレスアーキテクチャを使用し、数分でグローバル化できるようにシステムを設計

柱 5：コストの最適化

- システムを実行して、最小の価格でビジネス価値を実現
- コスト効率の高い資源の利用、需要と供給のマッチング、支出意識の向上
- リソースの使用率を測定、監視、および改善することで、徐々に最適化

柱 6：持続可能性

- クラウドワークロードの実行による環境への影響を最小化
- 影響を把握し、使用率を最大化して必要なリソースを最小限に抑え、下流への影響を軽減

これらの柱は、アーキテクチャを評価し、スケーラブルでセキュアで効率的な設計を実装するための一貫したアプローチの開発に役立ちます。これにより、CSC は自社のアプリケーションとサービスを通じてビジネス価値を提供することに集中できます。

[103] AWS. (2024) AWS Well-Architected.

7.1.2 基盤インフラストラクチャのセキュリティ技法

セキュアなインフラストラクチャを作成および維持する際に考慮すべき重要な基礎技術は、次の 4 つです。

- **セキュアなアーキテクチャ：** これは、セキュリティを主要原則としてクラウドインフラストラクチャを設計することから始まります。これには、リソースとネットワークの適切な分離、最小特権のアクセスの実装、セキュアなストレージ、通信、およびサービス構成の確保が含まれます。すべての環境で一貫したセキュリティを確保するために、ランディングゾーンとベースライン構成を設定する必要があります。IaC ツールは、セキュアなアーキテクチャの導入を自動化し、手動による設定ミスのリスクを軽減できます。

- **セキュアな配備と構成：** これには、リソースとサービスの構成および/または配備、仮想マシン(VM)、コンテナ、ストレージ、ネットワーキングを含むすべてのクラウドインフラストラクチャコンポーネントの強化が含まれます。Center for Internet Security（CIS）ベンチマーク[104]などのセキュリティベンチマークやベストプラクティスを適用して、 クラウド資産の適切な構成を確実にすることも含まれます。

- **セキュリティシフトレフト**：これは、セキュリティ管理を後付けとして捉えるのではなく、開発ライフサイクルの早い段階で組み込み、テストを行うことを意味します。コード分析ツールの実装、自動セキュリティテスト、継続的インテグレーション/継続的デプロイメント（CI/CD）パイプラインセキュリティゲートなどが含まれます。開発者はセキュアな IaC コーディングの実践に関するトレーニングを受け、アプリケーションにセキュリティを組み込むためのツールとフレームワークを提供する必要があります。

- **継続的モニタリングとガードレール[105]:** これらはセキュリティのためのものです。自動化システムを使用してクラウド環境を監視し、ポリシーを適用する作業が含まれます。ロギング、監視、継続的な評価に Cloud Security Posture Management（CSPM）または Cloud-Native Application Protection Platform（CNAPP）ツールを使用することや、ポリシーを適用し、確立された標準からの逸脱を防ぐための AWS Config ルール、サービス制御ポリシー、または Azure ポリシーの実装が含まれます。定期的なセキュリティ監査と侵入テストにより、これらの対策の有効性を検証します。

7.1.3 CSP インフラストラクチャのセキュリティ責任

[104] CIS. (2024) *Foundational Cloud Security with CIS Benchmarks*.

[105] Guardrails are preventative and reactive controls that either block an undesired outcome (e.g., block use of regions, public object storage, or specific cloud services that aren’t approved) or auto-remediate or correct a policy violation.

インフラストラクチャのセキュリティは CSP から始まります。これにより、CSC が構築できるセキュアなプラットフォームが確保されます。セキュリティ責任共有モデル（SSRM）では、インフラストラクチャのセキュリティは主に CSP の責任です。CSP インフラストラクチャのセキュリティ責任は、次のとおりです。

- **施設**:CSP は、クラウドインフラストラクチャが収容されている施設の物理的なセキュリティを確保する責任があります。これには、アクセス制御、監視、環境保護などの対策が含まれます。
- **従業員**:CSP は、クラウドインフラストラクチャにアクセスできる従業員のスクリーニング、トレーニング、および管理を行い、組織の完全性と信頼性の維持を支援します。
- **物理ネットワーク、ストレージ、コンピュート**：CSP は、サーバー、ストレージデバイス、ネットワーク機器など、クラウドインフラストラクチャの基盤となる物理コンポーネントを保護し、保守します。
- **仮想化レイヤー**：CSP は、物理インフラストラクチャ上で動作する VM とコンテナの作成と分離を可能にする仮想化技術のセキュリティ保護を担当します。
- **マネージメントプレーン**：CSP は、利用者がクラウドリソースとサービスの管理に使用する Web ベースのインターフェイスと API エンドポイントへのアクセスを保護し、制御します。
- **PaaS および SaaS サービス**：CSP は、SSRM に基づいて基盤となるインフラストラクチャとアプリケーションのセキュリティを処理する上位レベルのプラットフォームとソフトウェアサービスを提供します。

要約すると、CSP はクラウドインフラストラクチャを構成する物理設備、ハードウェア、仮想化レイヤー、および管理インターフェイスを保護します。CSC は、そのインフラストラクチャを利用し、デプロイする物のセキュリティ保護に重点を置いています。次の図は、クラウドサービスモデル（IaaS、PaaS、SaaS）のレイヤードコンポーネントの概要を示し、クラウドサービスを提供するためのさまざまな要素とその統合を示しています。

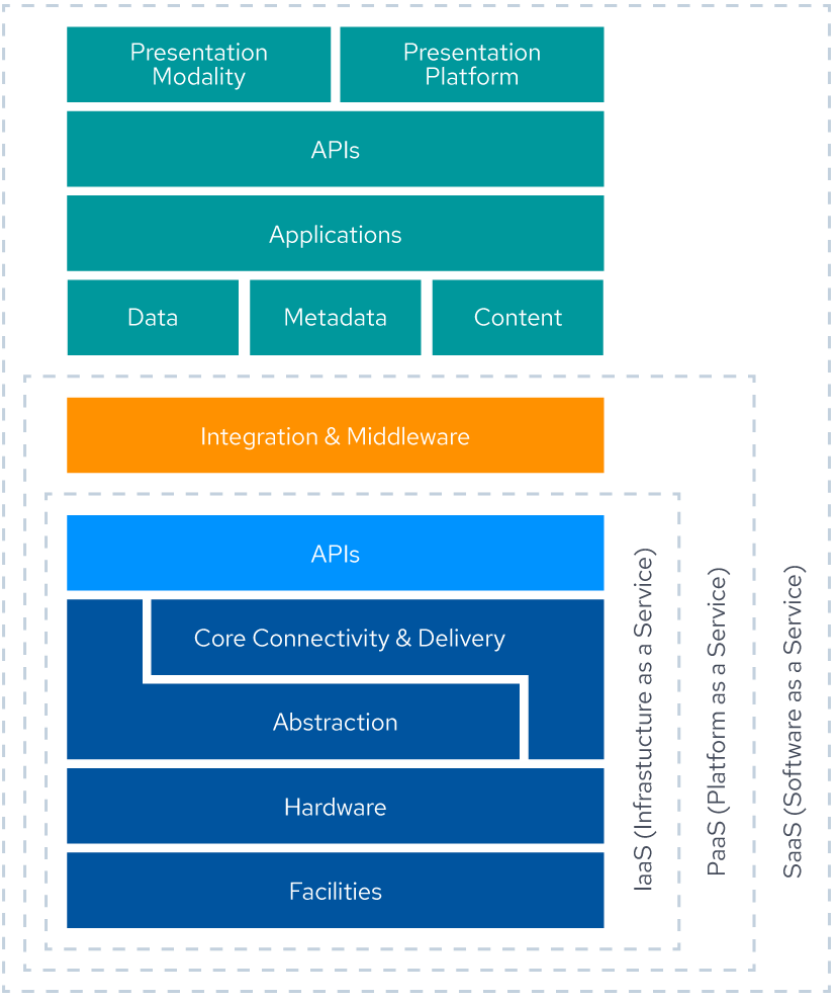


図 33: クラウドサービスモデルのレイヤードコンポーネント:IaaS、PaaS、SaaS

7.1.4 Infrastructure as Code

IaC は NIST SP 800-172 で「物理的なハードウェア構成や対話型構成ツールを採用するのではなく、機械読み取り可能な構成ファイルを使用して組織の IT インフラストラクチャを管理およびプロビジョニングするプロセス」[106]と定義されています。IaC はクラウドリソースの導入において主要なモデルであり、あらゆる主要なプロバイダによってサポートされています。IaC の主要な概念には、低レベルのネットワーク設計から高レベルのアプリケーションコンポーネントまで、機械可読な形式でアーキテクチャを定義し、通常は自動化された CI/CD パイプラインを使用して配備されることが含まれます。設定ミスに対するセキュリティスキャンをパイプラインに統合し、完全なバージョンとコントロールの変更追跡を行うことで、一貫性のあるセキュアなデプロイメントを実現します。シフトレフト・インフラストラクチャセキュリティとして知られるこの手法は、開発プロセスの早い段階でセキュリティを埋め込みま

[106] NIST (2024) Glossary - infrastructure as code (IaC)

す。IaC は、アプリケーションとワークロードのセキュリティに関するセクションを含む、このトレーニングの複数のドメインで議論されています。

IaC は、以下に示すいくつかのセキュリティ上のメリットを提供します。

1. **一貫性と標準化:**

    - IaC により、すべての環境で一貫したセキュアな構成の定義と実施が可能になります。
    - 最小特権アクセスなどのセキュリティのベストプラクティスは、IaC テンプレートにコード化できます。
    - 設定ミスのリスクを軽減し、標準化されたセキュリティポスチャを確保できます。

2. **バージョン管理と監査性**：

    - インフラストラクチャコードファイルはバージョン管理システムに保存でき、インフラストラクチャの変更の完全な履歴を提供します。
    - 変更の追跡、確認、および監査が可能になり、可視性と説明責任が向上します。
    - インフラストラクチャコードのコラボレーションとピアレビューを促進し、セキュリティ上の課題を特定して対処します。

3. **セキュリティテストの自動化:**

    - セキュリティスキャンとテストを配備パイプラインに統合できます。
    - 自動化ツールは、配備前にインフラストラクチャコードのセキュリティを検証できます。
    - 開発プロセスの早い段階でセキュリティの課題をキャッチでき、本番環境での脆弱性のリスクを軽減できます。

4. **迅速かつ安全な配備:**

    - IaC は、迅速かつ反復可能なインフラストラクチャの配備を可能にし、必要な時間と労力を削減します。
    - 配備時にセキュリティコントロールを自動的に適用できるため、一貫した保護が可能になります。
    - セキュアなインフラストラクチャを迅速に再配備できるため、セキュリティインシデントへの迅速な対応が可能です。

5. **拡張性と柔軟性:**

    - IaC は、需要に応じたリソースの動的なスケーリングとプロビジョニングをサポートします。

- セキュリティポリシーとコントロールは、新しいリソースが作成されたときに自動的に適用できます。
- 非常に動的で分散したクラウド環境でセキュリティを維持できます。

IaC を活用することで、CSC はクラウドインフラストラクチャの基盤にセキュリティを組み込むことができます。セキュアでコンプライアンスに準拠したインフラストラクチャを大規模に定義、配備、管理する手段を提供します。IaC は、セキュリティをシフトレフトさせ、課題を早期にキャッチし、開発ライフサイクルを通じて一貫してセキュアな環境を確保するために役立ちます。

7.1.5 クラウド移行アーキテクチャとセキュリティへの影響

クラウドの導入には、まったく新しいものもありますが、 多くの IaaS 配備では、データセンターや、場合によっては他のプロバイダからの移行による導入が多いです。利用可能なセキュリティ機能が異なり、まったく形式が異なるインフラストラクチャ間を移動する場合、移行は必ずしも単純なプロセスではありません。移行にはさまざまなモデルがあり、それぞれにセキュリティとコストのトレードオフがあります。次のガイダンスの考慮事項とアプローチは、クラウド移行イニシアティブのセキュリティとアーキテクチャに適用されます。

要件を明確に定義し、現在のセキュリティポスチャを徹底的に評価することが、移行のアプローチと実装の指針となるはずです。組織は、クラウド移行のアプローチを組み合わせて使用する必要があるかもしれません。使用される戦術は、各アプリケーション固有のニーズとリスクによって異なります。通常、組織は既存のアプリケーションを再設計/再構築、リファクタリング、またはリホストします。

図 34: クラウド移行戦略：再構築、リファクタリング、リホスト

7.1.5.1 再設計/再構築

アプリケーションを完全に再設計またはスクラッチから再構築してクラウドネイティブにする場合、クラウドのメリットを最大化することは、最も時間とリソースを消費するアプローチです。このアプローチにより、*セキュリティバイデザイン*を確保でき、開発プロセス全体にセキュリティ管理とプラクティ

スが組み込まれます。アプリケーションを再構築することで、クラウドネイティブのセキュリティ機能と自動化を十分に活用できます。しかし、そのためにはセキュリティプロセス、ツール、スタッフのスキルを大幅に変更する必要があります。再構築されたアプリケーションのセキュアな設計、構成、およびテストを確実にすることが不可欠です。

7.1.5.2 リファクタリング

クラウドネイティブのサービスや機能を可能な限り活用するようにアプリケーションを修正および最適化する場合、リホストよりも時間がかかりますが、パフォーマンス、スケーラビリティ、およびレジリエンスを向上できます。リファクタリングされたアプリケーションのセキュリティポリシー、手順、およびスタッフのスキルを更新する必要があります。このアプローチは、セキュリティのベストプラクティスとコントロールをリファクタリングされたアプリケーションに統合し、IAM、暗号化、およびロギングなどの CSP セキュリティサービスを活用する機会を提供します。しかし、適切に設計および構成しないと、新たなリスクが生じる可能性があります。

7.1.5.3 リホスト(リフト&シフト)

既存のアーキテクチャを保持したまま、最小限の変更でアプリケーションをクラウドに移行することは最も迅速な移行アプローチですが、クラウドへの最適化は最も不十分です。セキュリティの観点では、アーキテクチャの違いにより、既存のセキュリティ管理や課題が効果的にクラウドに移行できない可能性があります。さらに、既存のセキュリティ管理では、クラウドネイティブのセキュリティ機能と自動化を十分に活用できない可能性があります。このアプローチでは、クラウドモニタリングとインシデント対応のためのセキュリティプロセスとツールを適応させる必要があります。

7.2 クラウドネットワークの基礎

クラウドネットワークは SDN です。利用者のテナント環境間の強固な分離の実施が鍵となります。SDN は、ネットワークの設計、管理、および運用に革命をもたらす主要技術として登場しました。SDN は、ネットワークコントロールプレーンをデータプレーンから分離し、ソフトウェアを通じてネットワークをプログラム的に構成およびコントロールできるようにします。コントロールプレーンはルーティング、ネットワーク/サブネット定義などを管理し、データプレーンはリソースとネットワーク間でネットワークトラフィックを移動させます。従来のハードウェアベースのネットワーキングからソフトウェア定義によるアプローチへの移行は、クラウド環境に多くのメリットをもたらします。

次の図は、SDN 環境でのネットワーク制御ロジックを示しており、パケットがネットワーク制御ロジックを介して物理ホスト間を通過する際のカプセル化と非カプセル化を示しています。

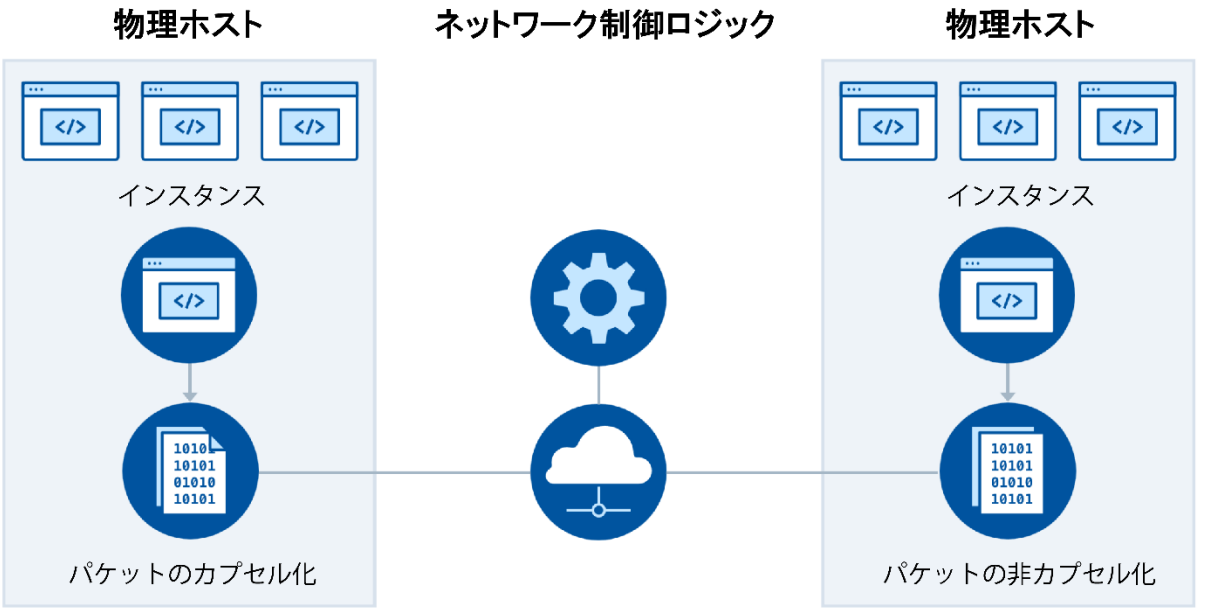


図 35: ネットワーク制御ロジック

SDN の主な利点の 1 つは、柔軟性と機敏性の強化です。SDN を使用すると、ネットワーク管理者はソフトウェアを通じてネットワークリソースを動的に構成および管理できるため、ネットワークサービスの迅速なプロビジョニングと変更が可能になります。この柔軟性により、CSP は CSC 要件の変化に迅速に対応し、ネットワークリソースをオンデマンドで拡張し、リアルタイムのトラフィックパターンに基づいてネットワークパフォーマンスを最適化することができます。また、SDN はネットワーク仮想化の実装を容易にし、共有物理インフラストラクチャ上に複数の論理ネットワークを構築できます。これにより、ネットワークリソースの使用率の向上、ネットワークセグメンテーションの向上、およびマルチテナント環境の管理が容易になります。SDN はどのネットワークでも使用できますが、すべての IaaS プラットフォームではデフォルトです。

SDN は、ネットワークの運用と管理を簡素化します。SDN は、ネットワークコントロールを一元化し、ネットワークを統一的に表示することで、大規模なクラウドネットワークの管理の複雑さを軽減します。ネットワーク管理者は SDN コントローラーと API を使用して、ネットワーク構成タスクの自動化、ネットワークパフォーマンスの監視、および課題のトラブルシューティングをより効率的に行うことができます。また、SDN はネットワークサービスとクラウドオーケストレーションプラットフォームの統合を可能にし、コンピューティングおよびストレージリソースとともにネットワークリソースのシームレスなプロビジョニングと管理を可能にします。この統合により、クラウドアプリケーションの配備と運用が合理化され、全体的な効率が向上し、運用コストが削減されます。

7.2.1 SDN のセキュリティ上の利点

主要なクラウドコンピューティングプラットフォームに共通する SDN は、それぞれ異なるものの、強力なセキュリティ上のメリットのコアセットをサポートする傾向があります。

- ネットワークはデフォルトで拒否（default deny）であるか、またはそのようにすぐに設定できます。つまり、定義された経路と特定の宛先があり、かつ、ポート/プロトコルがセキュリティグループによって承認されていない限り、ネットワーキングファブリックはパケットを伝送しません。（セキュリティグループは、トラフィックを許可または破棄するためのネットワーク内のルールです）。これにより、ポートスキャンやスニッフィングなどの一般的なネットワーク攻撃手法が削減または排除されます。

- ポリシーベースの管理とは、ネットワークが構成ポリシーによって管理されることを意味します。異なる技術を構成することではありません。これにより、一貫性と制御性が向上します。

- 細かいセグメンテーションは、SDN コントロールプレーンで管理され、物理的な設定を必要としないため、物理ネットワークよりもはるかに簡単に実装できます。これは驚くほど柔軟で強力であり、特定のアプリケーションに必要なネットワークコンポーネント（サブネットなど）のみを簡単に導入できます。

- セキュリティグループ、場合によってはその他のセキュリティ機能がネットワークファブリックに組み込まれています。それらを維持するためのファイアウォールは必要ありません。

7.2.2 Minimum Viable Network

SDN 機能は、Minimum Viable Network（MVN）と呼ばれる概念を可能にします。MVN では、最小接続に必要なネットワーク コンポーネントだけが配備され、アーキテクチャの各レイヤでは、アプリケーションに必要な最小限の経路、ポート、およびプロトコルだけが許可されます。これはリソースごとに実施可能で、ネットワーク設計に固有のものであり、マイクロセグメンテーションを可能にし、サポートします。したがって、インターネットは HTTPS ポート(443)でのみロードバランサーと通信できます。ウェブサーバーは指定されたロードバランサーからのポート 443 上の接続を受け付けます。アプリケーションサーバーは、ウェブサーバーからの着信接続を予期されるポートでのみ許可します。データベースサーバーは、アプリケーションサーバーの承認されたポートへの接続のみを受け入れます。これらのすべては、追加のセキュリティツールを必要とせずに、ネットワークファブリックでネイティブに実行されます。たとえば、攻撃者が（アプリケーションの脆弱性以外で）データベースを侵害できる経路はありません。また、アウトバウンドトラフィックに同様のルールが適用された場合、コマンド/コントロールインフラストラクチャに接続する方法もありません。

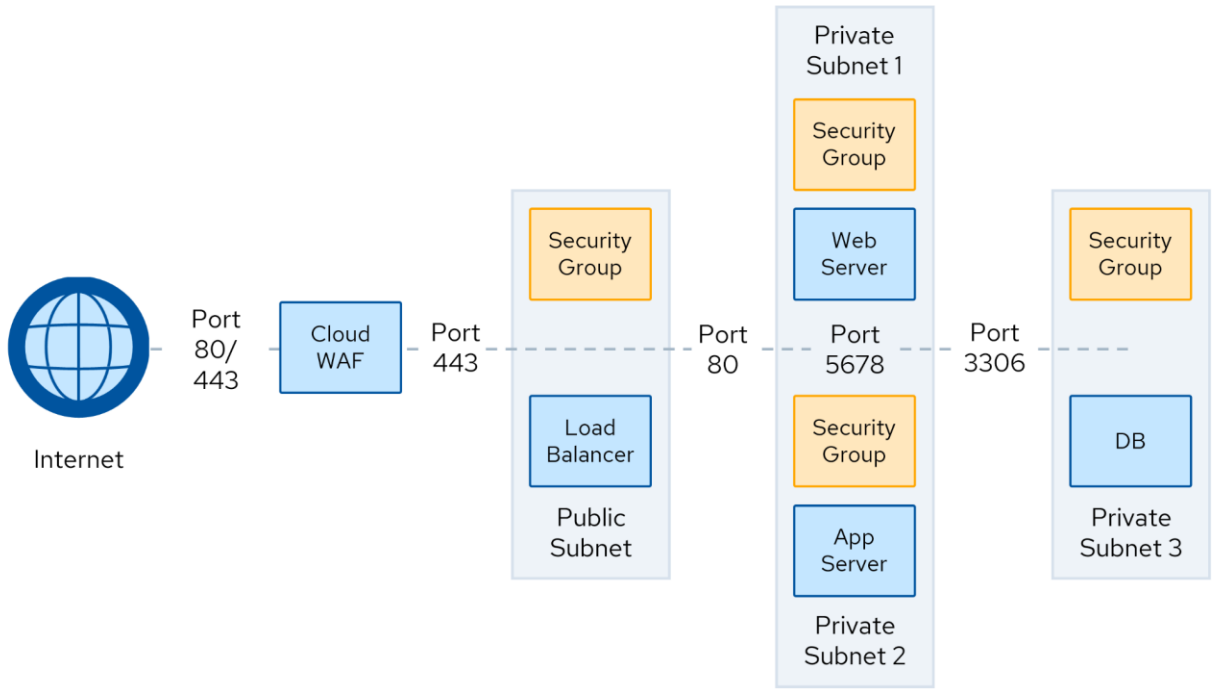


図36: MVN におけるセキュアなレイヤードアーキテクチャ

上の例では、インターネットトラフィックはまず、プライマリエントリポイントとして機能するクラウド Web アプリケーションファイアウォール（WAF）によって受信されます。WAF はすべての着信トラフィックを受け入れ、ロードバランサーに正当なトラフィックを転送する前に悪意のある要求を除外します。一方、ロードバランサーは WAF からのトラフィックのみを受け入れ、Web サーバーレイヤに配信します。後続の各レイヤ（Web サーバー、アプリケーションサーバー、およびデータベース）は、そのすぐ上のレイヤからのトラフィックのみを受け入れるため、回線交換のような緊密に制御されたネットワークが構築されます。

図のポート番号は、レイヤ間の通信に許可される特定のポートを表します。たとえば、ウェブサーバーはロードバランサーからポート 80 (HTTP) とポート 443 (HTTPS) のトラフィックを受け入れ、アプリケーションサーバーはウェブサーバーから特定のポート (例えば 5678) のトラフィックを受け入れます。別のプライベートサブネットにあるデータベースは、指定ポート上のアプリケーションサーバーからのトラフィックのみを受け入れます。セキュリティグループによって明示的に許可されていない他のすべてのトラフィックは、デフォルトで破棄されます。

この MVN アーキテクチャは、攻撃者がネットワークを探索し、内部コンポーネントに直接アクセスする能力を制限するため、システムへの侵入を非常に困難にします。ネットワークポートが直接エクスプロイトされないため、攻撃者の狙いは基本的にアプリケーションレイヤの脆弱性に限定されます。システムを侵害するには、攻撃者がクラウド WAF、ロードバランサー、および後続の各レイヤを首尾よく突破する必要があり、アタックサーフェスが限られ、クラウドプラットフォームが提供する固有のセキュリティコントロールを考えると、これは大きな挑戦となります。

7.2.3 SDN ベースの共通コンポーネント

ほとんどのクラウドネットワークは、一貫した基盤コンポーネント一式を共有しています。以下に、クラウド向けの一般的な SDN ベースのコンポーネントを示します。

仮想ネットワーク/仮想プライベートクラウド[107]

- あるプロバイダは「仮想ネットワーク（VNet）」と呼び、別のプロバイダは「仮想プライベートクラウド（VPC）」と呼びます
- クラウド環境内の仮想ネットワークを論理的に分離します
- CSC が IP アドレス範囲とネットワークトポロジを定義可能にします
- クラウドリソースのための安全でプライベートなネットワーキング環境を提供します

サブネット(パブリックとプライベート):

- VNet/VPC 内の小規模ネットワークセグメント
- リソースのさらなる細分化と整理が可能にします
- 異なるセキュリティおよびアクセス制御ポリシーの適用が可能にします

ルートテーブル:

- VNet/VPC 内でのネットワークトラフィックの方向を定義します
- サブネットと外部ネットワーク間のトラフィックのパスを指定します
- 最適なネットワークパフォーマンスを実現するカスタムルーティング構成の実現します

クラウドネットワークセキュリティグループ:

- セキュリティグループはステートフルファイアウォールに似ていますが、ネットワークファブリック自体に実装します
- ネットワークインターフェイス、インスタンス、サブネットレベルで仮想ファイアウォールとして機能します
- IP アドレス、ポート、プロトコル、およびその他の基準に基づいて送受信トラフィックを制御します
- 個々のリソースまたはリソースグループに対してきめ細かいセキュリティレベルを提供します

クラウドネットワークアクセス制御リスト (NACL):

[107] VNet is a term commonly used by Microsoft Azure, whereas VPC is used by Amazon Web Services (AWS) and Google Cloud Platform (GCP). Both terms refer to the network environment residing in the cloud, controlled by software, and able to replace the on-premises data center or network infrastructure.

- ACL は、ネットワークデバイスや環境を通過できるパケットを指定することで、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制御します
- ACL はセキュリティグループよりもネットワークスタックの下位で機能し、通常はステートレス[108]です
- ACL がサブネット/ネットワークに適用されるのに対し、セキュリティグループはほとんどの場合リソース(インスタンスなど)に適用されることが多いです
- NSG と NACL の実装はさまざまな CSP で異なります

ネットワークアドレス変換（NAT）ゲートウェイ:

- プライベートサブネット内のインスタンスがインターネットまたはその他の外部サービスにアクセスできるようにします
- プライベート IP アドレスをパブリック IP アドレスに変換して発信トラフィックに対応します
- 内部 IP アドレスをパブリックインターネットから隠蔽することで、セキュリティレイヤーを提供します

インターネットゲートウェイ:

- VNet/VPC におけるインターネットトラフィックの入口および出口として機能します
- VNet/VPC 内のリソースがパブリックインターネットと通信できるようにします
- クラウドリソースの送受信インターネット接続を可能にします

ハイブリッド専用回線:

- オンプレミスインフラストラクチャとクラウド間の専用プライベートネットワーク接続
- ハイブリッドクラウド環境に高帯域幅、低レイテンシ、安全な接続を提供
- オンプレミスとクラウドのリソースのシームレスな統合を実現
- 例：マルチプロトコルラベルスイッチング、AWS DirectConnect、Azure ExpressRoute など

VPN ゲートウェイ:

- オンプレミスネットワークとクラウド間のセキュアな暗号化接続を確立
- リモートユーザーやオフィスがクラウドリソースにセキュアにアクセスできるようにします
- より小規模な接続のために、専用回線に代わるコスト効率の高い代替回線を提供します

サービスエンドポイント:

- VNet/VPC と他のクラウドサービス間のプライベート接続を可能にします
- VNet/VPC 内のリソースがパブリックインターネットを経由せずにクラウドサービスにアクセスできるようにします

[108] A stateful firewall is a firewall that maintains a “state” or stores information about active network connections.

- CSP のネットワーク内にトラフィックを保持することでセキュリティを強化

ピアリング/中継接続:

- 同じクラウドリージョン内の VNet/VPC 間で直接プライベート接続を確立します
- 異なる VNet/VPC 内のリソースが相互に通信できるようにします
- VPC 間通信にコスト効率と低遅延のオプションを提供します

これらの要素が連携して、クラウド上に堅牢でセキュアな SDN 環境を構築し、拡張性、柔軟性、およびカスタマイズに優れたネットワークアーキテクチャを構築できます。

7.2.4 クラウドネットワークセキュリティグループ

SDN コンポーネント内では、クラウドネットワークセキュリティグループは、クラウド環境内のリソースを保護するための基本となります。これらは、インスタンス、VM、またはサブネットレベルで送受信トラフィックを制御する仮想ファイアウォールであり、個々のリソースまたはリソースグループに対してきめ細かいレベルのセキュリティを提供します。セキュリティグループは、IP アドレス、ポート、プロトコルなどのさまざまなパラメータに基づいてトラフィックを許可または拒否するルールを定義することで活用されます。AWS のようにデフォルトですべてのポリシーを拒否するプロバイダーもあり、CSC は許可ルールを作成する必要があります。一方、Azure はデフォルトで許可ポリシーが設定されており、CSC は拒否ルールを作成できます。セキュリティグループは、他のセキュリティグループを内部的に参照することもできるため、ルールに IP アドレスを定義する必要がありません。

セキュリティグループの主要な原則の 1 つは、ポリシーにルールを定義することです。管理者は、ネットワークトラフィックを管理する一連のルールを含むセキュリティグループポリシーを作成します。これらのルールは、セキュアシェル（SSH）、リモートデスクトッププロトコル（RDP）、HTTP/HTTPS などの特定のタイプのトラフィックを許可または拒否するように設定できます。これらのルールを慎重に作成することで、管理者は最小特権の原則を実装し、他のすべてのトラフィックをブロックしながら、リソースが正常に機能するために必要な権限だけを付与できます。

セキュリティグループポリシーを定義すると、クラウド環境内の特定のリソースに適用できます。リソースにポリシーを適用することで、インフラストラクチャ全体で必要なセキュリティ対策を一貫して実施できます。セキュリティグループは、個々のインスタンス、ネットワークインターフェイス、またはサブネット全体（CSP によって異なる）に関連付けることができ、柔軟性を提供します。共通のセキュリティ要件を持つリソースをグループ化し、同じセキュリティグループを割り当てることができるため、管理が簡素化され、設定ミスの可能性が低くなります。

セキュリティグループのもう 1 つの重要な原則は、ネットワークファブリックによってリソースごとに適用されることです。セキュリティグループ内の各リソースには、独自のインバウンドおよびアウトバウンドルールのセットが適用されます。同じセキュリティグループに属するリソース間のトラフィックは自動的に許可されません。同じセキュリティグループ内のリソース間の通信が必要な場合は、そのトラフィックを許可する明示的なルールを定義する必要があります。この明示的な許可の原則

は、厳重なセキュリティポスチャを維持し、リソース間の意図しない通信を防ぐために役立ちます。

注目すべきは、セキュリティグループがあらゆる主要 CSP によってサポートされていることです。AWS、Microsoft Azure、Google Cloud Platform（GCP）、その他の CSP のいずれを使用していても、CSC はセキュリティグループを標準機能にすることができます。特定の用語や設定インターフェイスは CSP によって若干異なる場合がありますが、セキュリティグループの中核となる原則と機能は一貫しています。この広範なサポートにより、セキュリティグループはさまざまなクラウド環境にわたって信頼性が高く移植性の高いセキュリティメカニズムとなります。

まとめると、クラウドネットワークセキュリティグループは、リソースレベルできめ細かいセキュリティポリシーを実施するための強力なツールです。セキュリティグループは、ポリシーでルールを定義し、そのポリシーをリソースに適用し、ネットワークファブリックを通じて適用することで、堅牢な防御レイヤーを提供します。同じセキュリティグループ内のリソース間の明示的な許可の原則により、セキュリティがさらに強化されます。CSP 全体でセキュリティグループを一貫してサポートしているため、CSC はこの機能を確実に活用してクラウドベースの資産を保護し、強固なセキュリティポスチャを維持できます。

7.2.5 セキュリティグループを超えて

一般的な CSP クラウドアーキテクチャツールのいくつかを取り上げましたが、その他のツールについては、まだ説明していません。CSC がクラウドベースのネットワーク環境の開発経験を積むにつれ、推奨されるリファレンスアーキテクチャについても学ぶことになります。CSC がオンプレミスに関して、どのような混合や整合を行うかにかかわらず、これらの CSP サービスのそれぞれが何をするのか、そしてなぜそれらがすべての主要なハイパースケーラーと CSP（AWS、Azure、GCP、IBM、Oracle など）上で構築されているのかをしっかりと理解することが重要です。

予防的セキュリティ対策:

- **CSP ファイアウォール：** Amazon VPC Firewall や Azure Firewall などの CSP ファイアウォールがクラウドプラットフォームに組み込まれています。保守（訳注：ファイアウォールの管理保守）のための追加のインスタンスやサーバを必要としないため、管理が簡素化され、運用上のオーバーヘッドが削減されるという利点があります。ただし、仮想アプライアンスに比べてカスタマイズ性や高度な機能に限界がある場合があります。
- **仮想アプライアンス：** 仮想ファイアウォールアプライアンスは、ファイアウォールのルールと構成をより柔軟に制御します。負荷分散構成で配備することで、高可用性を確保できます。ただし、この方法では複雑さが増し、ファイアウォールソフトウェアを実行している VM またはインスタンスの継続的なメンテナンスが必要になります。仮想アプライアンスは、次世代ファイアウォール（NGFW）や侵入検知システム、侵入防御システム（IDS/IPS）製品で一般的に利用できます。

- **WAF:** WAF は、SQL インジェクション、クロスサイトスクリプティング（XSS ）、その他の OWASP Top 10[109]に含まれる脆弱性のような一般的なエクスプロイトから Web に面したアプリケーションを保護します。CSP と CSC の要件に応じて、WAF はクラウドネイティブサービスまたは仮想アプライアンスとして導入できます。（CSP によってはネイティブサービスとして提供している場合もあります）。

- **出口（Egress）フィルタリング/管理:**出口フィルタリングは、インターネットまたはその他のネットワークへの発信トラフィックを制御します。CSP ファイアウォール、セルフホストプロキシ、または仮想アプライアンスを使用して実現できます。それでも注意しなければならないことは、フィルタが配備された特定のネットワーク内のリソースのみが対象となることです。

発見的セキュリティ対策:

- **フローログと DNS ログ：** フローログと DNS ログは、ネットワークトラフィックパターンの貴重な可視性を提供し、異常なアクティビティの検出に役立ちます。フローログは、ネットワークフローの送信元、宛先、プロトコル、およびその他の属性に関する情報を取得します。一方、DNS ログは、ドメイン名解決の要求と応答を記録します。これらのログは、潜在的なセキュリティ侵害、不正アクセスの試み、およびデータの流出を特定するのに役立ちます。
- **トラフィックのミラーリング：** トラフィックミラーリングを使用すると、監視および分析目的でネットワークトラフィックを複製できます。しかし、 Cybersecurity and Infrastructure Security Agency (CISA)[110] は、それを潜在的なセキュリティリスクとして指摘しています。攻撃者がミラーリングされたトラフィックにアクセスすると、機密データが傍受される可能性があります。このリスクを軽減するには、厳格なアクセス制御を実装し、ミラーリングされたトラフィックを暗号化してセキュアに保存し、構成とアクセスログを定期的に監査することをお勧めします。

PaaS のセキュリティに関する考慮事項:

- **API ゲートウェイ：** API ゲートウェイは、PaaS サービスにアクセスするためのエントリーポイントです。認証、レート制限、要求/応答変換などの機能を提供します。セキュリティ機能が組み込まれているものもあります。
- **リソースポリシー：** CSP は、AWS IAM ポリシーや Azure Role-Based Access Control（RBAC）などのリソースレベルのアクセス制御ポリシーを提供し、PaaS サービスにアクセスするためのきめ細かい権限を定義します。これらのポリシーを最小特権の原則に基づいて適切に設定することが不可欠です。
- **WAF/CDN:** 多くの PaaS サービスを WAF や CDN（Content Delivery Network）サービスと統合することで、セキュリティとパフォーマンスを強化できます。WAF は Web ベースの脅威から

[109] OWASP. (2021) OWASP Top Ten - *Top Ten Web Application Security Risks*.

[110] CISA (2024) *Identifying and Mitigating Living Off the Land Techniques*.

保護し、CDN は悪意のあるトラフィックを吸収しフィルタリングすることで分散型サービス拒否（DDoS）攻撃を軽減します。

- **VPC/VNet 上のサービスエンドポイント:** サービスエンドポイントは、PaaS サービスを VPC または VNet に直接接続し、CSC が一貫したセキュリティポリシーを適用してサービスと仮想ネットワーク間のトラフィックフローを制御できるようにします。
- **ネットワークセキュリティの継承：** PaaS サービスは、多くの場合、ネットワーク経由で接続したときに関連付けられている VPC または VNet に適用されるネットワークセキュリティ制御を継承します。（多くはインターネットへの直接接続がデフォルトです）。つまり、ネットワークに対して構成されているものと同じファイアウォールルール、アクセス制御、およびモニタリングが PaaS サービスにも拡張され、クラウド環境全体で一貫したセキュリティポスチャが提供されます。

7.2.6 コンテナネットワーキング

コンテナ特有の脆弱性や脅威に対処するためには、専用のコンテナセキュリティコントロールが必要です。コンテナはエフェメラル、軽量、非常に動的であるため、従来のセキュリティ対策の効果は低くなります。コンテナはアタックサーフェスが大きいため、攻撃者の潜在的な侵入口になります。コンテナイメージ、オーケストレーションプラットフォーム、またはネットワーク構成の脆弱性がエクスプロイトされ、不正アクセスを受けたり、攻撃の発信源となる場合があります。コンテナ化されたアプリケーションを配備する場合、オーバーレイネットワーク、ホストネットワーキング、クラウドネイティブネットワーキングソリューションなど、ネットワークスタックには複数のオプションがあります。各ネットワークスタックにはセキュリティ上の影響と考慮事項があり、選択したアーキテクチャに基づいてカスタマイズされたセキュリティ対策の必要性が強調されています。

CSC は、コンテナレベルだけですべてのネットワークセキュリティを管理できることを前提としてはいけません。コンテナホストシステムを保護するためには、セキュリティグループと境界セキュリティが依然として必要です。これらの対策は、多くの場合、より効果的でスケーラブルな専用サービスまたは VM を活用するため、境界セキュリティに対してより効果的です。コンテナネットワーキングに関しては、Docker[111]と Kubernetes[112]で利用できる主要なオプションがいくつかあります。

Docker のネットワークオプション:

- **ブリッジネットワーク：** Docker のデフォルトのネットワークモードです。各コンテナはホスト上の仮想ブリッジネットワークに接続し、コンテナ同士が通信できます。ブリッジネットワークはホストのスタックから分離され、ネットワークの分離を実現します。

- **ホストネットワーク：** このモードでは、コンテナはホストマシンと同じネットワークスタックを共有します。これは、コンテナがホストのネットワークインターフェイスに直接アクセスし、

[111] Docker. (2016) *Understanding Docker Networking Drivers and their use cases*.

[112] Kubernetes. (2023) *Extending Kubernetes*.

ホストポートにバインドできることを意味します。ただし、このモードでは簡略化のためにネットワークの分離が犠牲になります。

- **オーバーレイネットワーク:**オーバーレイネットワークにより、異なるホストで動作するコンテナがシームレスに通信できます。これは、virtual extensible LAN(VXLAN)または IPSec トンネルを使用して複数のホストに分散ネットワークを構築することで実現されます。オーバーレイネットワークは、マルチホスト Docker の導入で一般的に使用されます。

- **Macvlan ネットワーク：** Macvlan ネットワークは、各コンテナに一意の MAC アドレスを割り当て、ネットワーク上の異なる物理デバイスとして認識させます。コンテナは、ホストのネットワークスタックをバイパスして、物理ネットワークに直接接続できます。このモードは、コンテナが物理ネットワーク上で IP アドレスを持つ必要がある場合に便利です。

Kubernetes のネットワークオプション:

- **ポッドネットワーキング:** Kubernetes では、ポッドはデプロイ可能な最小単位であり、1 つ以上のコンテナを含めることができます。各ポッドは IP アドレスを取得し、ポッド内のコンテナは同じネットワーク名前空間を共有するため、localhost を使用して通信できます。Kubernetes では、ポッドネットワーキングを処理するために Container Network Interface (CNI) プラグインが必要です。

- **サービスネットワーキング:** Kubernetes のサービスは、一連のポッドに対して永続的な IP アドレスと DNS 名を提供します。サービスはロードバランサーとして機能し、ラベルとセレクタに基づいてポッドにトラフィックを分散します。ClusterIP（クラスタ内部）、NodePort（各ノードの IP 上に公開）、LoadBalancer（CSP のロードバランサーを介して外部からアクセス可能）など、いくつかのタイプのサービスがあります。

- **Ingress[113]:** Ingress は、クラスタ内のサービスへの外部アクセスを管理する Kubernetes リソースです。HTTP/HTTPS トラフィックの単一のエントリーポイントとして機能し、URL ルーティング、SSL 終端、バーチャルホスティングなどの機能を提供します。NGINX[114]や Traefik[115]などの入力コントローラは、Ingress ルールを実装します。

- **ネットワークポリシー：** Kubernetes のネットワークポリシーでは、ポッドと名前空間の間のトラフィックフローを制御するルール定義が可能です。CSC は、ラベルとセレクタに基づいて、相互に通信できるポッドを指定できます。ネットワークポリシーは、ネットワークセグメンテーションを実施し、クラスタ内の不正アクセスを制限する手段を提供します。

[113] The ingress concept is used in controlling external access to services running within the containerized environment.

[114] NGINX is open-source web server software used for reverse proxy, load balancing, and caching.

[115] Traefik is a open source reverse proxy and ingress controller that streamlines deploying services and APIs.

- **CNI[116]プラグイン:** Kubernetes はポッドネットワーキングを処理するために CNI プラグインに依存しています。一般的な CNI プラグインには、次のようなものがあります。
    - Flannel。各ノードにサブネットを割り当て、ノード間通信に VXLAN または host-gw を使用するシンプルなオーバーレイネットワークです。
    - Calico。オーバーレイモードと非オーバーレイモードの両方、および高度なネットワークポリシー適用をサポートする、拡張性とパフォーマンスに優れたネットワーキングソリューションです。
    - Weave Net。ゴシッププロトコル[117]を使用して複数のホスト間で VNet を作成し、自動検出と暗号化を可能にするオーバーレイネットワークです。

これらは Docker や Kubernetes のコンテナネットワーキングオプションのほんの一例です。セキュリティは、コンテナレイヤとクラウドネットワーキングレイヤの両方で実施する必要がありますが、これは、選択したネットワークスタックによって大きく異なります。

7.3 クラウド接続性

*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」*で紹介した NIST モデルからクラウドの本質的な特徴の 1 つは、幅広いネットワークアクセスです。プライベートクラウドでも、構成やリソースはネットワーク経由で管理され、アクセスされます。パブリッククラウドの場合、このネットワークはパブリックインターネットまたはハイブリッド接続を作成するために使用される専用回線のいずれかです。

クラウドの接続性は大きく 3 つに分類できます。

- クラウド内のリソース(仮想マシンなど)への接続
- CSP 内の別々の仮想ネットワークを相互に接続
- データセンターネットワークからクラウドへの接続、または 2 つの異なる CSP 間の接続

7.3.1 リソースへの接続

この図は、クラウドで実行されている VM やコンテナなどのリソースにセキュアに接続するための概要を示しています。

[116] CNI plugins are modular components that implement the CNI specification, allowing container runtimes to configure network interfaces, manage IP addresses, and establish connectivity for containers within the networking environment

[117] Github. (2019) weaveworks/mesh - gossip protocol is also known as epidemic protocol used in peer-to-peer communications.

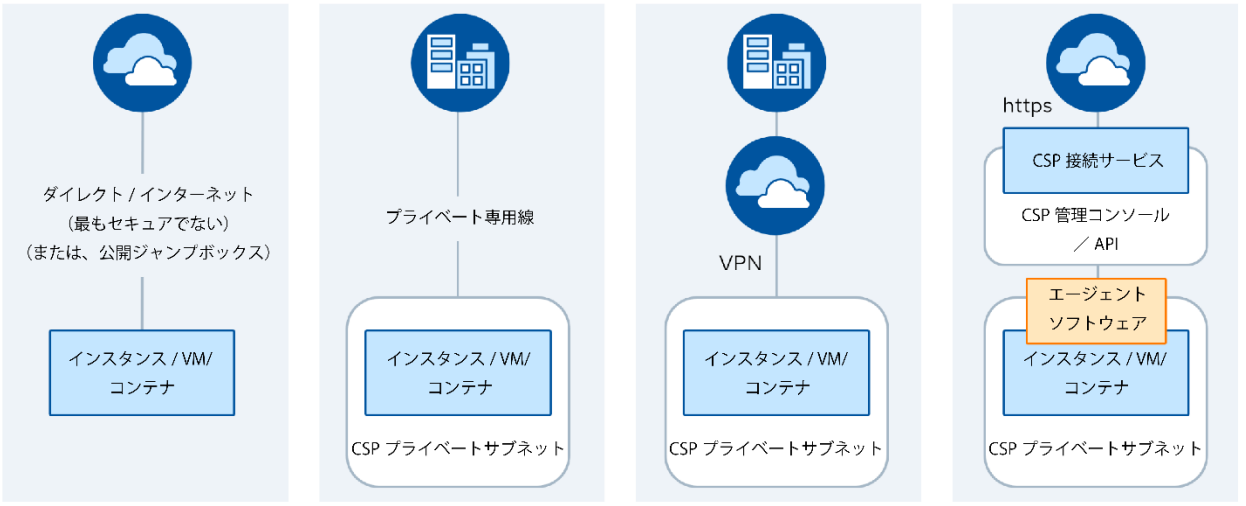


図 37: クラウドリソースへの接続方法

ダイレクトインターネットまたは専用線
最も直接的な方法は、パブリックインターネットを介して接続することで、それはまた、最もセキュリティが低いものです。よりセキュアな方法として、オンプレミスネットワークと CSP の間に専用線を確立する方法があります。これにより、専用のプライベート接続が提供されます。

VPN
もう 1 つの一般的なアプローチは、VPN を使用する方法です。VPN は、CSC のネットワークとクラウドベースのリソースの間に、パブリックインターネット上で暗号化されたトンネルを作成します。

CSP 接続サービス
実際の VM やコンテナにアクセスするには、CSC が AWS Session Manager や Azure just-in-time（JIT）などの*接続サービス*と呼ばれるものを介して接続する必要があり、それによって Web コンソールやポートフォワーディングをサポートするように設計されたソフトウェアからアクセスできるようになります。この重要な CSP サービスは、セキュアなゲートウェイとして機能します。また、CSC はクラウドリソースへのアクセスを管理、監視、および監査できます。メリットの 1 つは、これらのサービスがクラウドマネージメントプレーンから IAM/RBAC パーミッションを使用できることで、SSH キーやその他のクレデンシャルの必要性を軽減または排除できることです。

この図では、VM(承認されたセキュアな VM イメージに基づく)とインスタンス(承認されたコンテナによって生成される)がプライベートサブネットにグループ化されていることに注意してください。これらはネットワークレベルの分離とセキュリティを提供します。接続サービスにより、許可されたユーザーは、インターネットに露出されることなく、それらのプライベートサブネット内のリソースにセキュアに接続できます。接続サービスは、中央管理コンソールと API を通じて管理されます。これにより、CSC はアクセスポリシーの設定、接続の監視、およびアクティビティの監査を行うことができます。これは、後に述べるゼロトラストの一形態と考えることができます。

その他のオプションは、エージェントベースのネットワークオーバーレイ、さまざまな形式のポートトンネリング、さらにはフリート管理ソフトウェアによる非同期コマンドの発行など、常に進化しています。

要約すると、プライベートネットワーキングとの接続サービスを使用することで、クラウドベースのリソースをリモート管理しながら、アクセスに対する厳密なコントロールと可視性を維持するためのセキュアな方法を提供します。

7.3.2 仮想ネットワークの接続（CSP 内）

企業やアプリケーションのさまざまな要件をサポートするために、CSP 内で異なる仮想ネットワーク（VNet や VPC など）を接続するための幅広いオプションとアーキテクチャが用意されています。サービスエンドポイントのように、ネットワークが重複する IP アドレス範囲を共有する場合でも、特定のサービスにのみ接続するように設計されているものもあります。次に、CSP 内の仮想ネットワークを接続する例を示します。

ピアリング：

- 2 つの仮想ネットワーク（VNet/VPC）間のプライベートな直接接続を確立
- トラフィックがパブリックインターネットを通過することがないため、高セキュア
- シンプルなアーキテクチャのための迅速かつ簡単なセットアップ
- ネットワークが増えると複雑さが急速に増し、接続のメッシュ化が進み、管理やトラブルシューティングが困難になります

トランジット/メッシュ:

- 仮想ネットワークを接続するハブアンドスポークモデルを提供
- AWS Transit Gateway や Azure Virtual WAN などのマネージドサービスを中央接続ポイントとして使用
- 複雑なピアリングメッシュと比較して、ネットワークアーキテクチャと管理を簡素化
- 接続されたネットワーク全体で一貫したセキュリティ、監視、およびルーティングポリシーの実装が容易
- トランジットサービスの追加コストが発生し、直接接続に比べてレイテンシが若干増加する場合があります

サービスエンドポイント:

- 選択したサービスを仮想ネットワークに投影し、サービスをプライベートアクセスできるようにします
- 例えば、パブリックインターネットを経由せずに、複数のアプリケーション VPC を共有データベースに接続

- パブリックエンドポイントを完全に無効にし、許可されたサブネットからのアクセスのみを許可するため、高セキュリティ
- 特定のサポート対象サービスに限定(CSP によって異なる)
- 重要なデータストアのセキュリティ保護には有用ですが、汎用ネットワーク接続ソリューションではありません

その他のオプション:

- ソフトウェアゲートウェイと SD-WAN[118]ソリューションを使用してクラウドネットワークをオーバーレイし、コントロールと柔軟性を向上
- アカウント間でプライベートにアクセスする共有プライベート接続（AWS PrivateLink、Azure Private Endpoints など）
- 単一の仮想ネットワークを複数のクラウド配備と共有することで(クロス配備権限を使用)、異なるチームが同じネットワークにワークロードを配備できる

適切な選択は、規模、セキュリティニーズ、管理オーバーヘッド、および接続するリソースのタイプによって異なります。一般的なアーキテクチャでは、複数のアプローチを組み合わせます。重要なのは、セキュリティ、パフォーマンス、複雑さ、およびコストの適切なバランスを取ることです。

7.3.2.1 例: クラウドネットワーク境界の統合

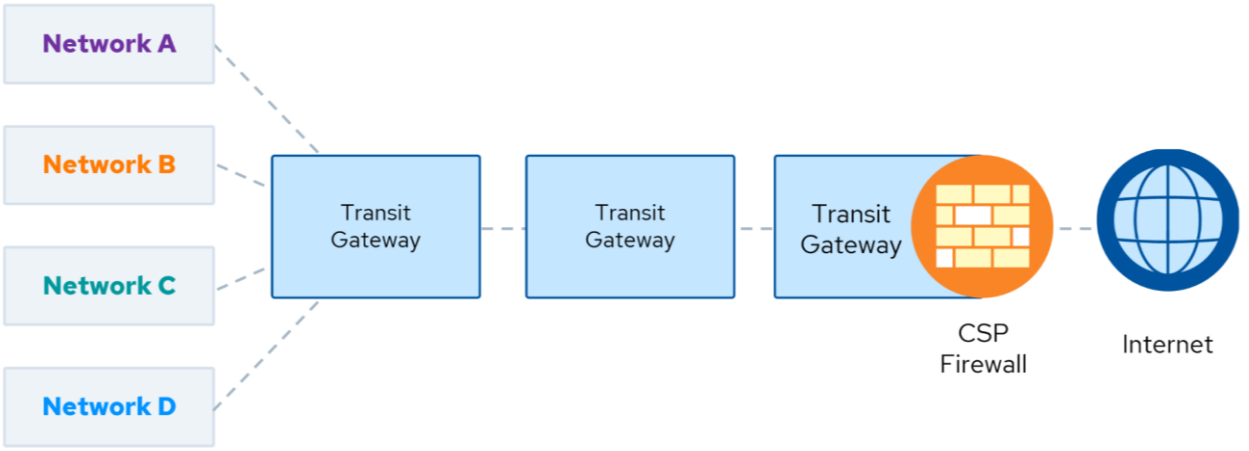


図 38: アウトバウンドトラフィックの統合クラウドネットワーク境界

この例では、A、B、C、および D というラベルの付いたそれぞれ異なるネットワークから発信される外向きインターネットトラフィックを、統合境界ネットワークを介して誘導することによって、管理およびセキュリティ保護するために設計されたアーキテクチャ フレームワークを検討しています。このセットアップは、CSP が提供するファイアウォールサービスを採用しています。

[118] SD-WAN is a software-defined approach to managing the WAN.

このアーキテクチャでは、ネットワーク A から D が中央中継ゲートウェイに接続されます。重要な点として、これらのネットワークはインターネットに直接にはアクセスできない設定になっています。代わりに、インターネットに接続されたすべてのトラフィックはトランジットゲートウェイを経由し、その後、専用の境界ネットワーク（VNet や VPC など）に誘導されます。この境界ネットワーク内では、AWS Network Firewall または Azure Firewall という CSP ファイアウォールが稼働し、結合されたトラフィックを精査してフィルタリングします。

この設計は、各ネットワークが自律的にインターネットにアクセスすることを許可することとは対照的に、インターネットを宛先とするすべてのトラフィックに対して、単独で管理された出口ポイントを作成します。このような出口フィルタリングの一元的なアプローチは、インターネットアクセスのためのすべてのネットワークで統一されたセキュリティプロトコルの確立、発信トラフィックの管理と監視の効率化など、複数のメリットをもたらします。インターネットへの露出を単一の強固なネットワークに集中させることで、潜在的なアタックサーフェスを効果的に縮小し、ネットワークから出るトラフィックのロギング、検査、および監視の特異性を高めます。このアーキテクチャは、IDS/IPS、Web フィルタリング、およびデータ損失防止（DLP）などの追加のセキュリティ機能を境界内に統合する柔軟性も提供します。

ただし、このアーキテクチャを最適化するには、いくつかの事項を考慮する必要があります。パフォーマンスのボトルネックを回避するには、境界ネットワークとファイアウォールの双方について、適切なサイジングを行い、高可用性を維持することが重要です。ルーティングおよびセキュリティプロトコルは、必要不可欠な発信トラフィックのみを許可するように慎重に調整する必要があります。さらに、堅牢性、レジリエンス、および継続性を確保するためには、冗長性とフェイルオーバー機能のために、複数のアカウントまたは CSP およびアベイラビリティゾーンの使用が推奨されます。

7.3.3 データセンターとプロバイダ間の接続

マルチクラウドネットワーキングを含むハイブリッドネットワークを構築する場合、インターネットまたはプライベートバックボーン上でトラフィックを伝送するために異なる技術が使用されます。以下は、データセンターや CSP との接続オプションの例です。

専用線:

- オンプレミスのデータセンターとクラウド間の専用プライベート高速接続を提供
- 半永久的な性質は、ファイバーでの構築に比べて設置や撤去が比較的短時間で済むことを意味します
- 接続が共有されないため、パフォーマンスの予測が可能で非常に高速
- 両端に互換性のあるハードウェアと IP アドレス指定が必要であり、複雑さが生じる可能性があります
- 通常、ネットワークキャリアが提供するミートミーポイントへの接続が必要です。そこから CSP のネットワークに接続します
- CSP は独自の相互接続を持つため、クラウド間の接続には使用されません

VPN:

- ネットワーク、データセンター、およびクラウド VPC/VNet 間にインターネット上で暗号化トンネルを確立
- 柔軟性が高く、ソフトウェア設定によるセットアップと撤去が可能
- VPN トンネルを終端するには、各終端に適切なハードウェア（または仮想アプライアンス）が必要
- パフォーマンスはインターネット接続の品質に依存。CSC のネットワーク外の輻輳の影響を受ける可能性があります
- 通常、CSP のトランジットネットワーク（AWS Transit Gateway, AzureVirtual WAN など）に接続する方が望ましい
- バックアップ接続やクラウドリソースへのセキュアなリモートアクセスに一般的に使用されます

ハイブリッドメッシュ:

- SD-WAN またはソフトウェアゲートウェイを使用して、オンプレミスと複数のクラウド間の any-to-any 接続を提供
- ソフトウェアとポリシーを使用してトポロジーとトラフィックフローを定義し、既存の接続の上にオーバーレイネットワークを構築
- 多くのポイントツーポイントリンクと比較して優れた柔軟性と管理性を提供
- 基盤となる物理ネットワークへの依存を減らすことで、耐障害性を向上
- 抽象化と自動化により、設定の負担とエラーの可能性を大幅に軽減
- 各ホップでのトラフィック処理と追加のソフトウェア/ライセンスコストにより、ある程度のパフォーマンスコストが発生します
- ソフトウェアデファインドポリシーとネットワークコントローラを維持する必要があります

どれを選択するかは、接続するワークロードの規模、重要度、および可変性によって異なります。専用回線は最高のパフォーマンスを提供しますが、柔軟性は劣ります。VPN は迅速かつ柔軟ですが、予測不可能な場合があります。SD-WAN とハイブリッドメッシュは、オンプレミスと複数のクラウドでの大規模な配備のためのプログラム可能な中間領域を提供します。多くの CSC では、プライマリデータセンターのクラウド接続用の専用線、バックアップとユーザーアクセス用の VPN、管理を統一するためのソフトウェアオーバーレイなど、混在して使用されています。重要なのは、トレードオフを理解し、ビジネス要件に合わせて選択をすることです。

7.3.3.1 例：トランジットゲートウェイ・ハブアンドスポークモデル

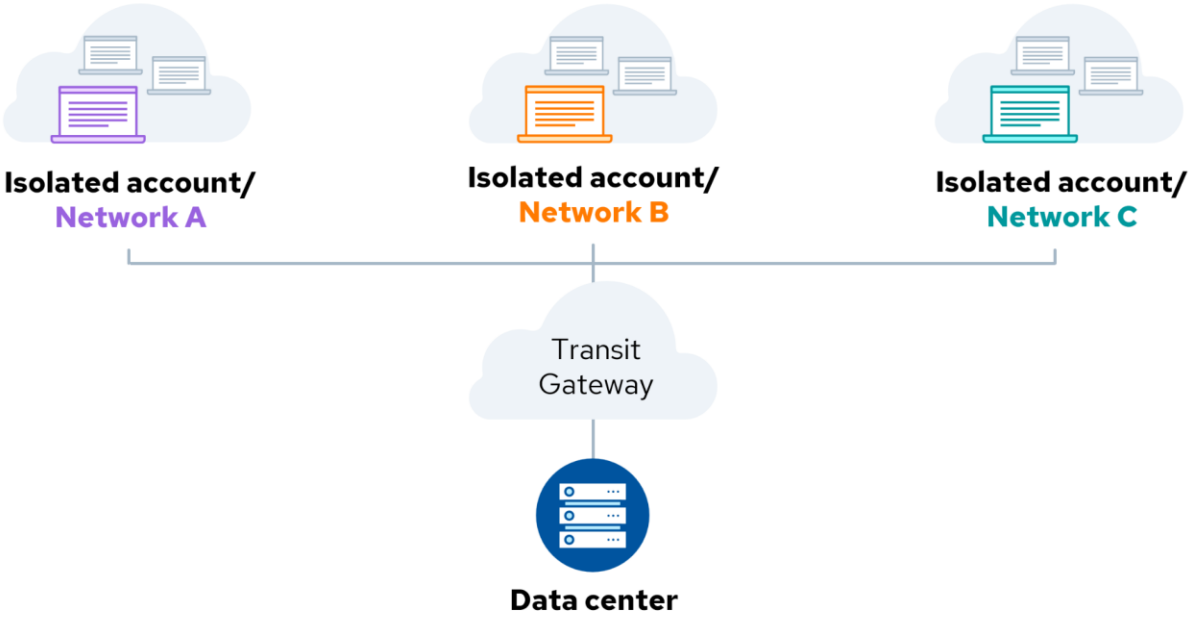


図 39: トランジットゲートウェイ・ハブアンドスポークアーキテクチャ

この例では、中央集中型のデータセンターを介して独立したネットワークの接続を可能にする強力なネットワーキングサービスであるトランジットゲートウェイを利用したネットワークアーキテクチャの図を示しています。具体的には、AWS では Transit Gateway、Azure では Azure WAN と呼ばれるトランジットゲートウェイが、独立したネットワーク間のトラフィックのルーティングをオーケストレーションする重要なハブとして機能する仕組みについて概説します。

このアーキテクチャではトランジットゲートウェイ内のルートテーブルによって管理され、ネットワーク間の許可されるトラフィックフローをきめ細かく規定します。ルートテーブルは、以下を規定します。

- ネットワーク A および C には、トラフィックをデータセンターにルーティングする機能を付与
- ネットワーク A をプロビジョニングしてネットワーク B との通信リンクを確立
- ネットワーク B はネットワーク C との接続を許可

重要な点は、アーキテクチャがネットワーク A がネットワーク C との直接通信経路を確立することを制限し、同様にネットワーク B がデータセンターに直接アクセスすることを禁止していることです。

AWS のコンテキストでは、トランジットゲートウェイはトランジットゲートウェイアタッチメントによって各アカウントにわたって VPC にリンクされます。Azure エコシステムでは、この接続は仮想ネットワークを結び付ける Virtual WAN を介して実現されます。
さらに、このアーキテクチャは専用線を活用して、オンプレミスのデータセンターとクラウドベースのトランジットゲートウェイ間の物理的な接続を形成します。このハブアンドスポークモデルを採用することで、ネットワーク設計は複数の独立したネットワーク間のトラフィックフローをセグメント化して管理することに成功します。この構成では、ルーティングおよびセキュリティポリシーの実施が一元化

されるだけでなく、データセンターに配置された共有サービスの可用性も向上します。選択的なアクセシビリティにより、指定されたネットワークからこれらのサービスを利用できるため、すべてのネットワークセグメントにわたって直接通信する必要がなくなります。

7.4 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（ZT）は、信頼が決して暗黙的ではないという前提で動作し、ネットワークにアクセスするユーザーやデバイスには、常に強固な検証が求められます。このセクションでは、ゼロトラストアーキテクチャフレームワークとそれを支える技術である software-defined perimeter（SDP）やゼロトラストネットワークアクセス（ZTNA）について紹介します。さらに、SASE がどのように様々なセキュリティ機能を統合し、クラウドで提供されるサービスとして、ますます分散化する環境のニーズに対応しているかについても詳しく説明します。SASE は、ネットワーク機能とセキュリティ機能を統合してクラウドサービスへのセキュアでスケーラブルなアクセスを実現し、分散環境のパフォーマンスとセキュリティを最適化することで、これを補完します。このセクションでは、ゼロトラストと SASE の基本的な概念、メリット、実装戦略を説明し、クラウドアーキテクチャとネットワークを効果的に保護する方法について詳しく説明します。

7.4.1 クラウドインフラストラクチャとネットワークのゼロトラスト

一般的なセキュリティ戦略としてのゼロトラストについては、「ドメイン 2：クラウドガバナンス」で説明されているほか、CSA Zero Trust Resource Hub[119] には、ZT Guiding Principles 文書をはじめ、有用な参考資料が多数掲載されています。

ゼロトラストとは、いかなるユーザーや資産も暗黙のうちに信頼されるべきではないという考えを前提としたサイバーセキュリティ戦略です。侵害がすでに発生している、または今後発生することを前提としています。したがって、企業の境界で実行される 1 回の検証でユーザーに機微情報へのアクセスを許可すべきではありません。その代わりに、各ユーザー、デバイス、アプリケーション、およびトランザクションは継続的に検証されなければなりません。

ZTA の実装には、ネットワーク境界の内外からアクセスが要求されても、信用しないことを前提とした、包括的なフルスタックのマルチピラーアプローチによるセキュリティが含まれます。[120]

[119] CSA. (2024) Zero Trust Resource Hub.

[120] Zero Trust pillars are covered in more detail in *Domain 11: Incidence Response & Resilience*.

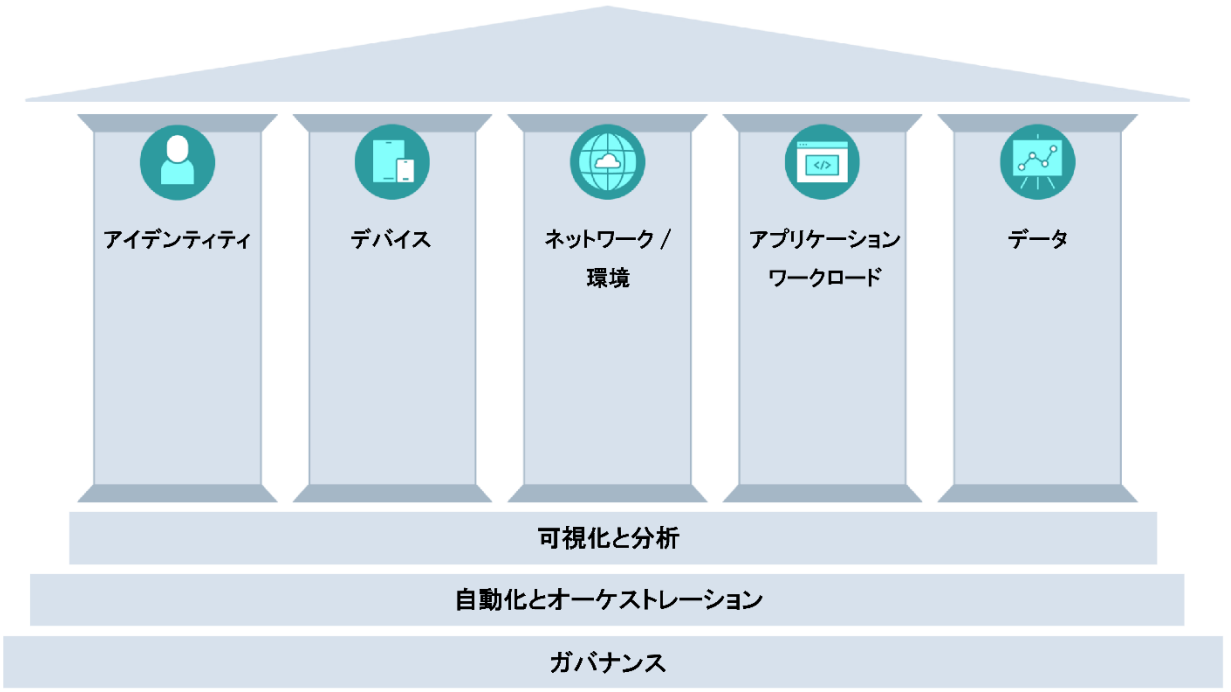


図 40: ZTMM の 5 つの柱

7.4.1.1 ZT の基本概念と機能

ゼロトラストは、ビジネスアプリケーションや資産がさまざまな環境に分散し、ユーザーがリモートからインターネット経由で業務システムに頻繁にアクセスすることが多い現代のクラウドインフラやネットワークに特に関連するセキュリティ戦略です。ゼロトラストの原則に従うことで、組織はクラウド環境のセキュリティ対策を強化し、セキュリティ侵害、不正アクセス、および攻撃者によるラテラルムーブメントのリスクと潜在的な影響を軽減できます。しかし、一般的にゼロトラストを実装するには、クラウドランドスケープ全体で人材、プロセス、および技術を統合する、総合的なフルスタックアプローチが必要です。これは、以下のセキュリティ対策を適切に組み合わせて実施することで実現できます。

継続的な検証:

- クラウドコンソールアクセスや API コールを含む、すべてのユーザーと管理者のアクセスに対して、フィッシングに強い多要素認証 （MFA）を実装します。
- Context Based Access Control（CBAC）を実装することで、ユーザーのセッションを通じてユーザーID、デバイスポスチャ、およびセッションコンテキストを継続的に検証します。CBAC には、RBAC と Attribute-Based Access Control（ABAC）を含めることができます。
- セキュリティ分析とユーザーとエンティティの行動分析（UEBA）を使用して、特に機密性が高い管理者アクセスに対して、異常や危険な行動を検出します。

最小特権アクセス:

- 最小特権の原則に従い、業務機能に必要な最小限の権限のみをユーザーとアプリケーションに付与します。
- 権限昇格には、JIT アクセスと期限付き認証情報を使用します。
- 未使用または過剰な権限を定期的に確認して取り消し、アクセスガバナンスプロセスを通じて、終了したユーザーのすべてのアクセスを迅速に取り消します。

マイクロセグメンテーション:

- VPC、VNet、仮想ファイアウォール、および同様の構造を使用してネットワークセグメンテーションを実装します。
- ネットワークセキュリティグループ（NSG）とネットワークアクセス制御リスト（NACL）を使用して、ワークロードの重要度とセキュリティ要件に基づいて、クラウドネットワークをより小さく分離されたセグメントに分割します。
- きめ細かなセグメンテーションポリシーを適用し、セグメント間のラテラルムーブメントを制御します。
- 最小特権の原則に基づいて、セグメントとサービス間の通信を制限します。

インフラストラクチャとワークロードのセキュリティ:

- IDS/IPS を導入して、悪意のあるトラフィックを検出し、ブロックします。
- セキュアな境界を持つ専用の分離環境（VM、コンテナ、サーバーレス機能など）にワークロードを配備します。
- サービスメッシュアーキテクチャとマイクロサービス間のアイデンティティベースの通信を利用します。
- ワークロードとコンテナのランタイム保護、脆弱性管理、およびファイアウォールを実装します。
- 暗号化された VM やコンフィデンシャルコンピューティングなどのハードウェアセキュリティ機能を活用します。
- DevSecOps の手法を使用して、脆弱性スキャン、パッチ管理、および構成管理などのセキュリティプロセスを自動化します。
- イミュータブルインフラストラクチャとエフェメラルなワークロードパターンを採用し、セキュリティと一貫性を確保します。
- IaC ツールを活用して、クラウドリソースをセキュアにプロビジョニングおよび構成します。

データセキュリティ:

- 強固な暗号化アルゴリズムと堅牢な鍵管理手段を使用して、保存中および移動中のデータを暗号化します（相互認証された TLS 接続など）。
- 堅牢なバックアップおよびディザスタリカバリ（DR）メカニズムを実装し、セキュリティ侵害、ランサムウェア攻撃、またはデータ損失が発生した場合にビジネス継続性（BC）を確保します。
- データのアクセスや使用パターンを監視し、悪用や持ち出しの試みがないか監査します。

- DLP コントロールとデータマスキング技法を実装します。

監視とロギング:

- クラウドインフラストラクチャ、ネットワーク、およびワークロードに対して、アクセスとトラフィックのロギングとモニタリングを一元的に実装します。
- クラウドネイティブのロギング、モニタリング、およびアラートサービスを活用して、セキュリティログ、フローログ、および監査証跡を収集し、脅威の検出とインシデント対応に役立てます。
- 疑わしいアクティビティやセキュリティ違反を管理者に通知するアラートとトリガーを設定します。
- セキュリティ情報およびイベント管理を実装します（ログの集約、相関、分析のための SIEM システム）。
- security orchestration and automation（SOAR）ツールを使用して、セキュリティの対応と修復を自動化します。

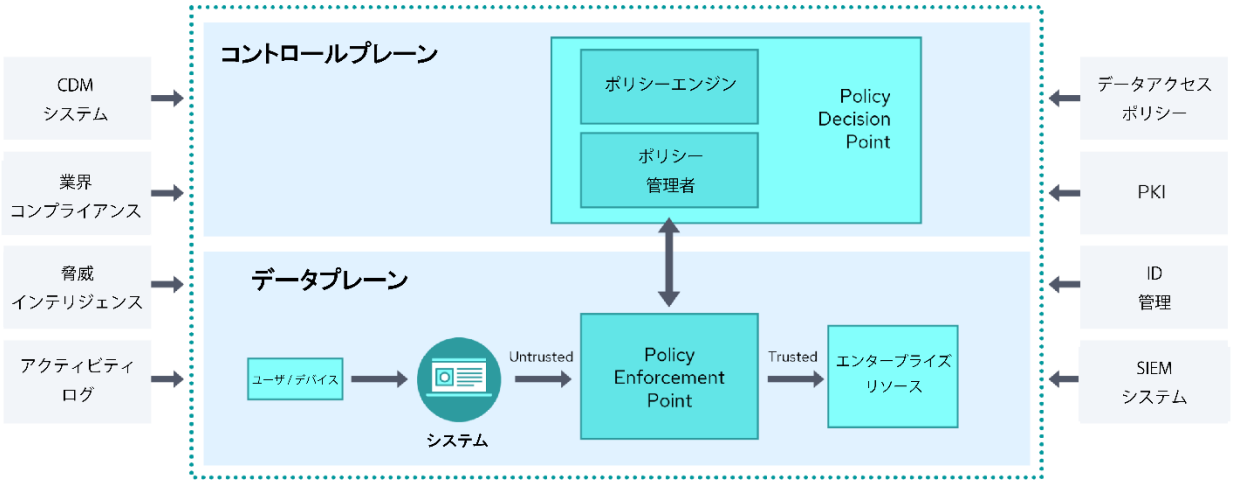
例： クラウド上の機微性の高い情報に対するゼロトラストのきめ細かいアクセス制御ポリシーには、いくつかのステップがあります。まず、ユーザーの強固で最新の認証を検証します。次に、エンドポイントデバイスの ID とセキュリティハイジーンを確認します。要求されたデータおよびワークロードアクセスの時間およびタイプに対して、ネットワークと地理的位置が許容できることを確認します。さらに、複数の地理的な場所から同時にログインしていないことを確認します。最後に、行動分析を使用して、要求されたアクセスがインサイダーのリスクアクセスプロファイルに適合していないことを確実にします。

これらのガイドラインと原則に従うことで、CSC はゼロトラスト戦略に基づいて、クラウドインフラストラクチャとネットワークの堅牢なセキュリティポスチャを確立でき、セキュリティリスクの軽減と機微データやリソースの保護に役立ちます。

7.4.1.2 ゼロトラストの概念アーキテクチャ

NIST SP 800-207 ゼロトラストアーキテクチャ (ZTA) は、CSA CCZT トレーニング[121]でも詳しく説明されているコンポーネントモデルを提供します。

[121] Training on zero trust architecture is available in CSA’s Certificate of Competence in Zero Trust (CCZT).



ゼロトラストは、IaaS や SaaS のクラウド展開においてますます利用されるようになっています

図 41: ZTA Core Logical Components (NIST 800-207, p.9)

NIST 2020 SP 800-207 は、ZTA の主要な論理コンポーネントを簡単に表現しています（上図）。NIST ZT モデルでは、ZT アクセスポリシーは Policy Decision Point（PDP）と Policy Enforcement Point（PEP）を使用して定義、管理、および実施されます。PDP および PEP は、リソースアクセスをトラフィックアクセスワークフローに配置することによって、リソースアクセスを制限します。PDP はポリシー管理者とポリシーエンジンで構成され、ポリシーエンジンはルールを決定し、PEP に伝達します。PEP はゲートウェイとして機能し、承認されたリソースに対して正しいアクセスレベルを持つ適切なエンティティに正しいアクセスが付与されていることを確認します。

NIST は PDP をコントロールプレーンに存在するものと定義し、論理アーキテクチャの構成要素として、データを収集、分析、および変換し、まずデータをインテリジェンスに変換し、次にリソースへのアクセスを管理するルールに変換します。PEP はデータプレーンに存在し、コントロールプレーンから渡された入力に基づいて、ルールを適用し、リソース（データ）へのアクセスを提供する責任を持つ ZT コンポーネントです。

セキュリティ関連のさまざまなデータソースは、PDP に情報をフィードしてルールを維持し、意思決定プロセス全体を最新の状態に保ちます。さまざまなインテリジェンスソースがポリシーエンジンにフィードされ、ポリシー管理者によるアクセスルールの定義と改良をサポートします。[122]

7.4.2 Software Defined Perimeter とゼロトラストネットワークアクセス

[122] Training on PDPs available in CSA’s Certificate of Competence in Zero Trust (CCZT)

ゼロトラストのネットワークセキュリティを実現する 2 つの主要な技術アプローチは、SDP と ZTNA です。これらのアプローチは相互に排他的ではなく、それぞれの要素を組み合わせてカスタマイズされた ZT セキュリティ実装にすることができます。

Software Defined Perimeter (SDP)

- 不正なユーザーやデバイスからは見えない、セキュアで「ダーク」なネットワークを確立します。
- デフォルトではネットワークにアクセスできない「ブラックアウト」アプローチを実装します。
- ユーザーおよびデバイスは、SDP で保護されたリソースにアクセスする前に認証および認可を受ける必要があります。
- SDP は、アイデンティティ中心のコントロールとマイクロセグメンテーションを活用して、ラテラルムーブメントを制限します。

ZTNA

- 従来の VPN を、より詳細なアプリケーション固有のアクセス制御モデルに置き換えます。
- ユーザーは、アイデンティ、デバイス、場所、およびその他のコンテキスト要因に基づいて検証および認可されます。
- 広範なネットワークアクセスを許可するのではなく、特定のアプリケーションまたはリソースへのアクセスを提供します。
- ZTNA ソリューションは、クラウドホスト型（ZTNA-as-a-Service）とオンプレミス型があります。

ゼロトラストのネットワークセキュリティ原則を導入することで、組織は全体的なセキュリティポスチャを大幅に強化し、データ漏洩のリスクを軽減し、進化するサイバー脅威に直面しても資産をより適切に保護することができます。ZTNA と SDP の組み合わせは、クラウド中心でリモートアクセス集中型の最新の IT 環境を保護するための堅牢なフレームワークを提供します。これらのトピックについては、NIST SP 800-215, Guide to a Secure Enterprise Network Landscape[123]が参考になります。

7.4.2.1 Software Defined Perimeter

SDP[124] は、フル（OSI ネットワーク）スタックセキュリティを提供するために実装されたゼロトラストネットワークセキュリティアーキテクチャです。SDP の実装では、資産を隠し、隠された資産への接続を許可する前に、別のコントロールプレーンとデータプレーンを使用してアクセスを認可します。SDP はゼロトラストの基本原則を実装しています。

ZT の実装では、資産にアクセスしようとするあらゆるものを、認可の前に検証する必要があります。さらに、ZT では、セッションとそのリスクレベルを接続している間は継続的に評価する必要があります。SDP を使用した ZT の実装により、組織は既存のネットワークおよびインフラストラクチャの境界中心

[123] *NIST. (2022) Guide to a Secure Enterprise Network Landscape*
[124] CSA. (2020) *Software-Defined Perimeter (SDP) and Zero Trust.*

のネットワーキングモデルで、絶え間なく浮上する古い攻撃手法の新しいバリエーションを防御できます。SDP を導入することで、ますます複雑化するアタックサーフェスの拡大に継続的に適応するという課題に直面している企業のセキュリティポスチャが向上します[125]。 CSC は資産のセキュリティポスチャを監視する必要があります。SDP は、ユーザー/デバイスが適切に認証され、隠された資産へのアクセスが許可されるまで、デフォルトのドロップオールゲートウェイを有効にすることで、このアクセス管理戦略を実施します。接続の事前検証を要求することで、SDP は、誰が、どのデバイスから、どのサービスやインフラストラクチャに接続できるか、およびその他の条件やコンテキスト要因（稼働時間や位置情報など）を完全にコントロールできます。

SDP アーキテクチャガイド v2 で説明されているように、SDP は次の主要なコンポーネントで構成されています。

- client/initiating host
- NIST の ZTA モデルで PEP とも呼ばれる service/accepting host
- NIST の ZTA モデルでは PDP とも呼ばれる accepting host と initiating host の両方が接続する SDP controller
- ドロップオールファイアウォールを実装する SDP gateway

SDP アーキテクチャガイド v2 によると、SDP は次のように動作します。

- initiating host の SDP クライアントソフトウェアが SDP への接続を開きます。ラップトップ、タブレット、スマートフォンなどの initiating host デバイスは、ユーザー向けです。つまり、SDP クライアントソフトウェアはデバイス上で実行されます。ネットワークは、SDP を運用する企業の管理外になる可能性があります。
- accepting host デバイスは、 initiating host からの接続を受信し、SDP 保護/セキュリティ保護された一連のサービスを提供します。通常、 accepting host は CSC の管理下にある（および/または直接の代表者の管理下にある）ネットワーク上に存在します。[126]
- SDP gateway は、許可されたユーザーおよびデバイスに、保護されたプロセスおよびサービスへのアクセスを提供します。ゲートウェイは、これらの接続のモニタリング、ロギング、およびレポートを実施することもできます。

initiating host および accepting host デバイスは、 SDP controller に接続します。SDP controller は、次のことを確認することで、分離されたサービスへのアクセスをセキュアにする、デバイス/アプライアンスまたはプロセスです。

1. ユーザーは認証され、承認されます
2. デバイスは検証済み
3. セキュアな通信を確立
4. ユーザーと管理トラフィックはネットワーク上で分離されたままです

[125] *CSA. (2020) Software-Defined Perimeter (SDP) and Zero Trust.*

[126] CSA. (2022) Software-Defined Perimeter (SDP) Specification v2.0 - *SDP Accepting Hosts (AH).*

controller と accepting host は見えず、権限のないユーザーやデバイスからはアクセスできません。SDP 実装は、さまざまな通信ユースケースに対して複数の異なる接続構成をサポートできます。詳細については、Software Defined Perimeter （SDP）仕様書 v2.0 を参照してください。

7.4.2.2 ゼロトラストネットワークアクセス

ZTNA はゼロトラストセキュリティモデルの主要なコンポーネントであり、特にアプリケーションとリソースへのセキュアなリモートアクセスに焦点を当てています。ZTNA は、従来の VPN を、より細かいルールとアプリケーション固有のアクセス制御モデルで置き換えます。ユーザーは、ID、デバイス、場所、およびその他の状況要因に基づいて、特定のアプリケーションまたはリソースへのアクセスが検証され、許可されます。

ZTNA の原則を導入することで、組織はアタックサーフェスを大幅に削減し、きめ細かなアクセス制御を実施して、ネットワークやアプリケーション内での不正アクセス、データ侵害、およびラテラルムーブメントのリスクを軽減できます。[127]

7.4.3 SASE

SASE は、ネットワークセキュリティ機能と WAN およびプロキシ機能を組み合わせて包括的なクラウドネイティブサービスを提供する新しいサイバーセキュリティの概念です。クラウドファースト、モバイルファーストの世界で、従来のネットワーク境界の外側にユーザーとリソースがますます分散される中で、エンドポイントデバイスとアプリケーションおよびデータへのアクセスを保護するという課題に対処するように設計されています。

7.4.3.1 SASE フレームワークとアーキテクチャの概要

SASE は、ネットワーキング機能とセキュリティ機能を単一のクラウド提供サービスに統合するフレームワークまたはアーキテクチャアプローチです。SASE は、ユーザーの場所に関係なく、アプリケーションとデータへのセキュアなアクセスを提供すると同時に、組織のネットワーク全体で一貫したセキュリティポリシーとコントロールを確保することを目指しています。

[127] Training on ZTNA available in CSA’s Certificate of Competence in Zero Trust (CCZT).

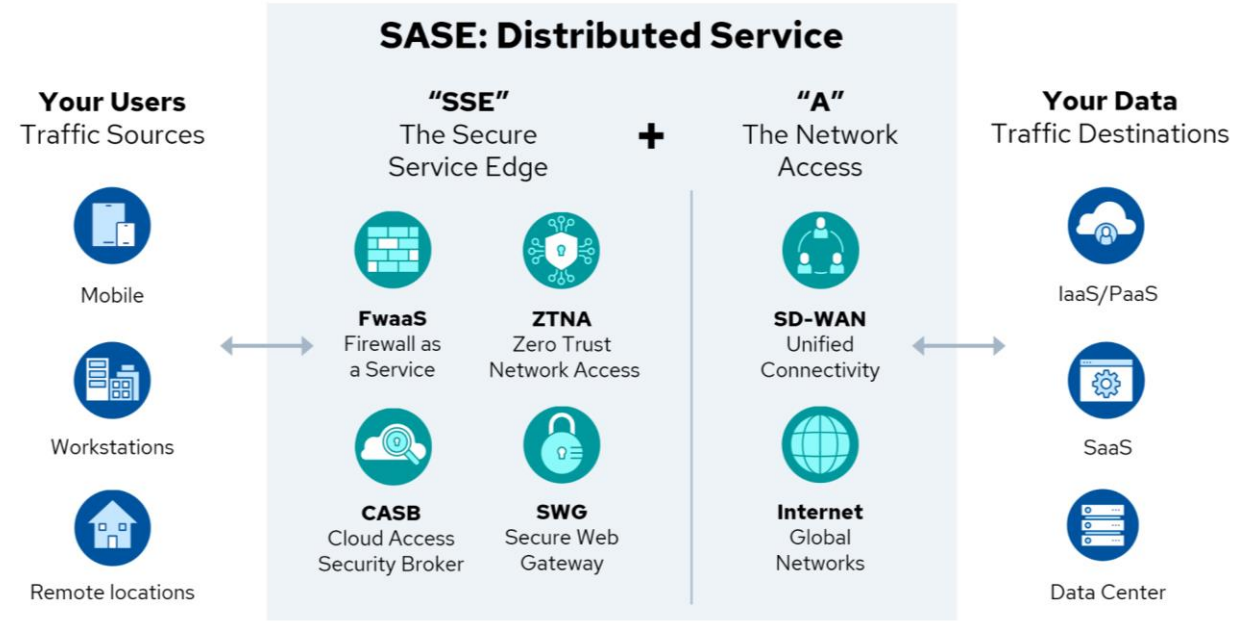


図 42: SASE フレームワークとアーキテクチャの概要

SASE は、クラウド環境でゼロトラストセキュリティを実現する上で大きな役割を果たします。ゼロトラストは、暗黙的な信頼を前提とせず、アクセス要求の発生場所に関係なく、すべてのアクセス要求を継続的に検証するセキュリティモデルです。SASE は、すべてのユーザー、デバイス、およびアプリケーションにわたってきめ細かいコンテキスト対応アクセスポリシーを適用するための統合プラットフォームを提供することで、これをサポートします。セキュアな Web ゲートウェイ、クラウドアクセスセキュリティブローカー（CASB）、ZTNA、および従来のファイアウォール機能などのセキュリティ機能を、単一のクラウド提供サービスに統合します。これにより組織は、ユーザーの場所やデバイスに関係なく、一貫してセキュリティポリシーを適用し、クラウドリソースへのアクセスを監視することができます。

7.4.3.2 SASE の実装とメリット

SASE のネットワーク層とアプリケーション層のセキュリティメカニズムの統合により、クラウド環境におけるゼロトラストの導入と管理がシンプルになります。SASE は、セキュリティをクラウドネイティブサービスとして提供することで、複数のポイント製品を管理する必要性を軽減または排除し、組織がクラウドフットプリントの拡大に合わせてセキュリティインフラストラクチャを迅速に拡張できるようにします。また、ユーザーのアイデンティティ、デバイスのポスチャ、およびアプリケーションの機密性に基づいてポリシーを適用する機能など、よりユーザー中心のセキュリティアプローチを提供します。これは、リモートユーザーがネットワーク全体ではなく、特定のアプリケーションやデータへのアクセスを必要とするクラウドで最小特権アクセスを実装するために不可欠です。

組織がクラウドサービスの導入やリモートワークの導入を進める中で、SASE はゼロトラストセキュリティの可能性を最大限に引き出すのに役立つでしょう。SASE は、あらゆるデバイスから、あらゆるネット

ワークを介して、あらゆるアプリケーションへのアクセスを保護するための統合クラウド提供プラットフォームを提供することで、組織がクラウド、オンプレミス、およびハイブリッド環境を含むデジタル資産全体でゼロトラストポリシーを一貫して適用できるようにします。これにより、全体的なセキュリティポスチャが向上するだけでなく、企業のセキュリティを損なうことなく、クラウドの俊敏性と拡張性を十分に活用できるようになります。

サマリ

クラウドインフラストラクチャのセキュリティ保護は、CSP のセットアップと CSC が展開する構成の両方を保護するデュアルフォーカスタスクです。インフラストラクチャセキュリティの柱は、セキュアなアーキテクチャの作成、最初の構成時からのセキュリティの確保、開発ライフサイクルの初期段階でのセキュリティの統合（シフトレフトプラクティス）、および監視とガードレールの適用によるモニタリングの維持です。

SDN の原則に基づいて構築されたクラウドネットワークは、デフォルト拒否ポリシーの実装、ポリシーに基づいたアクセスとルールの管理、および詳細なネットワークセグメンテーションを可能にするなど、高度なセキュリティ機能を提供します。これらの機能により、クラウド環境内のセキュリティフレームワークが大幅に強化されます。

SDP や SASE に代表されるゼロトラストの原則を取り入れることは、マルチクラウド接続のセキュリティを確保し、セキュアなリモートアクセスを実現するために不可欠です。これらのモデルでは、検証されたアイデンティティとコンテキストに基づいてアクセスが厳密に制御および提供されるため、分散環境でのセキュリティが強化されます。

コンテナネットワーキングは、従来の仮想化クラウドネットワークの上に抽象化レイヤーを追加することで、新たな複雑性のレイヤーをもたらします。そのため、コンテナとクラウドの両方のネットワーク層でセキュリティ対策を適用し、脆弱性がエクスプロイトされないようにする必要があります。

最後に、クラウドネットワークのセキュリティは、セキュリティグループに限定されません。また、ファイアウォール、IDS/IPS、WAF の導入といった予防的対策に加え、フローログやトラフィックのミラーリングといった発見的対策も含まれます。これらの要素が連携してサイバー脅威に対する堅牢な防御を形成し、クラウド技術を活用する企業のクラウドインフラストラクチャの完全性とレジリエンスを確保します。

推奨事項

クラウドインフラストラクチャのセキュリティ

- Well-Architected Framework の原則または同等の原則に従い、クラウドを使用する際の設計と実装の決定を導き、セキュリティとコスト効率を向上させます。
- セキュリティをシフトレフトする:セキュリティ管理とテストを後付けとして捉えるのではなく、開発ライフサイクルの早い段階に組み込みます。
- IaC を使用して、機械読み取り可能な設定ファイルを使用して IT インフラストラクチャを管理およびプロビジョニングします。

クラウドネットワークの基礎

- Software-Defined Networking (SDN）を導入し、柔軟性、俊敏性、およびネットワークの運用と管理の簡素化を強化します。
- クラウドネットワークセキュリティグループを活用します。
- 予防的、および発見的セキュリティ対策を検討します。

クラウド接続

- プライベートネットワーキングとの接続サービスを使用して、クラウドベースのリソースをセキュアにリモート管理します。
- CSP 内の仮想ネットワークを接続するピアリングまたはトランジット/メッシュアーキテクチャを検討します。
- ハイブリッドネットワークにおけるデータセンターと CSP 間の接続に関するさまざまなオプションを評価します。

ゼロトラストとセキュアアクセスサービスエッジ

- ゼロトラストを導入します：ユーザーや資産が暗黙に信頼されないと仮定し、すべてのユーザー、デバイス、アプリケーション、およびトランザクションについて継続的な検証を必要とするサイバーセキュリティ戦略。
- SASE を使用すると、ユーザーの場所に関係なく、アプリケーションやデータにセキュアにアクセスできます。

追加のガイダンス

- How to Design a Secure Serverless Architecture | CSA
- Cloud OS Security Specification v2.0 | CSA
- The Six Pillars of DevSecOps: Automation | CSA
- Software-Defined Perimeter as a DDoS Prevention Mechanism | CSA
- CSA IoT Security Controls Framework | CSA

ドメイン 8: クラウドワークロードセキュリティ

はじめに

このドメインでは、クラウドワークロードの保護について説明します。**クラウドワークロード**とは、クラウドコンピューティング環境で実行されるさまざまなタスク、アプリケーション、サービス、およびプロセスを指します。クラウドワークロードは、拡張性、柔軟性、および効率性を実現し、企業や個人が物理ハードウェアに多額の投資をすることなく、アプリケーションやデータ処理タスクにアクセスして実行できるようにします。クラウドワークロードには、仮想マシン（VM）、コンテナ、サーバーレスファンクション（Function as a Service（FaaS）とも呼ばれる）、AI、および Platform as a Service（PaaS）など、さまざまなリソースが含まれます。クラウド環境はリソースが常に変化し拡大するという動的な性質を持っているため、従来の方法と比較して、セキュリティに対する明確なアプローチが必要です。

学習目標

このドメインでは、次のことを学びます。

- クラウドセキュリティのワークロードに対するセキュリティアプローチを作成するための課題と独自性を理解します。
- 仮想マシンのセキュリティに関する考慮事項を理解します。
- コンテナの保護に使用されるセキュリティ上の考慮事項を理解します。
- PaaS のセキュリティを提供するためのセキュリティ上の考慮事項を理解します。
- サーバーレスまたは function as a service ワークロードに関するセキュリティ上の考慮事項を理解します。
- AI ワークロードのセキュリティ上の考慮事項を理解します。

8.1 クラウドワークロードセキュリティ入門

クラウドを使用する事業にとって、ワークロードのセキュリティ保護は、データ保護だけではありません。データ保護やプライバシー規制を含む法規制を遵守すること、また、業務を中断することなく継続することも重要です。

以下に、クラウドワークロードと従来の環境の主な違いを示します。

- **ダイナミックで拡張性が高い**:データとワークロードが比較的静的な従来の環境とは異なり、クラウドは常に進化し続ける動的で拡張性の高いキャンバスです。この環境の流動的な性質から、俊敏性と適応性を兼ね備えたセキュリティアプローチが求められます。クラウドに挑戦するセキュリティ専門家にとっては、標準的なセキュリティ対策を再考し、エンゲージメントルールが継続的に書き換えられる環境に適応することを意味します。
- **複雑さと多様性**：ワークロードにはさまざまなタイプがあり、それぞれに要件があるため、セキュリティに対する画一的なアプローチは機能しません。
- **完全性、機密性、可用性**：クラウドワークロードセキュリティの中核は、データの完全性、機密性、および可用性を維持することにあります。これは、サイバーセキュリティの根幹をなす原則です。クラウドでは、データが改ざんされず（完全性）、認可されたユーザーのみがアクセスでき（機密性）、必要なときに利用できる（可用性）ことが極めて重要です。

8.1.1 クラウドワークロードのタイプ

さまざまなクラウドワークロードがクラウド環境内で利用されており、それぞれに明確な特性とセキュリティ上の意味合いがあります。仮想インスタンスの管理やコンテナ化されたアプリケーションのセキュリティ保護から、サーバーレスや人工知能（AI）運用の安全性の確保まで、クラウドセキュリティの複雑なランドスケープをナビゲートするために不可欠なガイダンスを提供し、厳格なガバナンスとプロアクティブなセキュリティ対策の重要性を強調します。

- **仮想マシン(VM)とインスタンス**:仮想マシンはインスタンスとも呼ばれ、クラウドコンピューティングの基盤です。個別のオペレーティングシステムによる分離と、ハイパーバイザーおよびその他のマネージメントプレーンコンポーネントによるセキュリティ境界の適用を提供します。ハイパーバイザーは、クラウドサービスプロバイダ (CSP)が保守する主要なコンポーネントです。しかし、各 VM 内のゲスト OS のセキュリティは通常、クラウドサービス利用者（CSC）が担当するため、綿密な構成とパッチ適用が必要となります。さらに、「VM スプロール」は重大なセキュリティリスクをもたらす可能性があります。さらに、機密データの漏洩を防ぐためにはスナップショットやイメージの管理が不可欠であり、厳格なガバナンスの必要性が浮き彫りになっています。
- **コンテナ**:これは分離されたランタイム環境であり、ホストオペレーティングシステムのカーネルを共有しますが、独自のファイルシステム、ライブラリ、および構成を持つ独立した自己完結型のプロセスとして実行されます。コンテナは VM に代わる軽量で効率的な手段を提供しますが、セキュリティ上の課題は異なります。コンテナはホスト OS カーネルを共有するため、本質的に分離機能が弱くなります。コンテナ化された環境でのセキュリティは、OS レベルのコントロールを正しく構成し、コンテナイメージのセキュリティを維持し、コンテナのランタイム環境が適切に構成されるかどうかにかかっています。Kubernetes のようなオーケストレーターには、セキュリティを強化するメリットがあるにもかかわらず、オーケストレーターは、侵害を防ぐために慎重にナビゲートしなければならないというさらなる複雑さをもたらします。
- **Platform as a Service (PaaS)**: このワークロードは、より高い効率性とより少ないオーバーヘッドでアプリケーションの開発、配備、および管理を容易にするツールとサービスのスイートを

提供することで、クラウドプラットフォームの機能を拡張します。これらのサービスは、データベースやメッセージングシステムからコンテンツ配信ネットワーク（CDN）まで、さまざまなセキュリティ上の考慮事項があります。

- **サーバーレスまたは Function as a Service(FaaS)**:FaaS は、開発者がイベントや要求に応じて実行される個々の関数を記述してデプロイするクラウドコンピューティングモデルで、基盤となるインフラストラクチャを管理する必要はありません。このサーバーレスモデルは、CSP にセキュリティ責任のより大きな分担を委ねます。この信頼の再配置は、CSP の専門的なセキュリティ専門知識と高度な保護手段を活用するため、アタックサーフェスを最小限に抑えることができます。実行環境の短時間の実行の特性と、CSP による強制隔離が相まって、固有のセキュリティ上のメリットがあります。しかし、サーバレスアプリケーションを不正アクセスや潜在的な攻撃（サービス拒否や自動スケーリングによる金銭的枯渇など）から保護するには、シークレットを管理し、最小限の権限でファンクションを設定することが最も重要です。
- **AI ワークロード**：このワークロードは、学習、意思決定、または予測の提供のために膨大なデータを処理します。そのため、固有のセキュリティ上の課題が生じます。データの完全性とプライバシーの確保が最優先されます。特に、敵対する攻撃からの保護、モデルの盗難の防止、プロンプトインジェクションからの保護に重点を置いています。これらの脆弱性にもかかわらず、AI ワークロードはクラウド環境の高度な計算リソースと拡張性を活用しています。

一般的に、クラウドワークロードに関しては、特にサーバーレスコンピューティングのようなモデルでは、管理の責任は CSP に移ります。アタックサーフェスが縮小する可能性がありますが、可視性、制御性、およびガバナンスの課題は残ります。したがって、セキュリティの監視とガバナンスは、すべてのクラウドワークロードにわたって堅牢なセキュリティポスチャを維持し、運用を中断することなく、データ保護規制を遵守して継続できるようにする上で非常に重要になります。

8.1.2 クラウドワークロード:短期実行と長期実行

クラウドワークロードにおける*短期実行(エフェメラル)*と*長期実行(イミュータブル)*の概念は、ワークロードの管理と保護に対する 2 つの異なるアプローチを表しています。短期実行/エフェメラルアプローチでは、ワークロードを交換可能な使い捨てリソースとして扱います。これに対し、長期実行型/イミュータブルのアプローチでは、ワークロードを不可欠なものとして扱い、手動での維持管理が必要です。従来のコンピューティングでは、インフラストラクチャは主に短期実行モデルによって扱われてきましたが、クラウドコンピューティングの導入により、そのアプローチを再考する必要があります。どちらのモデルも、セキュリティ、運用管理、およびスケーラビリティに影響を及ぼします。そのため、それぞれのアプローチの違いと適切なタイミングを理解することが重要です。

短期実行(エフェメラル)
クラウドネイティブアーキテクチャでは、ほとんどのワークロードは短期実行モデルで動作します。これらは一過性のサービスであり、必要に応じて出入りし、特定のタスクやワークロードを処理するために短期間だけ存在することもあります。実行時間が短いワークロードのセキュリティはプロアクティブかつ組み込み型であり、VM またはコンテナイメージの作成プロセスの一部であり、手動での設定や導入後の作業は必要ありません。イミュータブルインフラストラクチャの使用とは、パッチ適用や再構成

の代わりに、新しいワークロードを立ち上げて、危険や有害なものを置き換えるということを意味します。このモデルは自動スケーリングと自己修復機能をサポートしており、その効率性と強化されたセキュリティポスチャにより、最新のクラウドネイティブアプリケーションアーキテクチャにおいて支配的なパターンとなりつつあります。

長期実行（イミュータブル）
対照的に、長期実行されるワークロードは、長期間にわたって注意深く育てられ維持されるワークロードです。これらのワークロードは、多くの場合、手動で構築および管理され、セキュリティソフトウェアが手動でインストールおよび更新されています。このようなアプローチは時間がかかり、人為的ミスを招きやすいため、一貫性のないセキュリティプラクティスにつながる可能性があります。 長時間実行されるワークロードは通常、基盤となる管理理念を変更せずに従来のオンプレミスワークロードをクラウドに移行するシナリオ（リフトアンドシフト[128]と呼ばれる）で見られます。長時間実行されるワークロードは、特別な配慮が必要なデータベースなど、特定のアプリケーションにとって鍵となる可能性がありますが、耐障害性が低く、課題が発生した場合のメンテナンスにコストがかかる可能性があります。

クラウドセキュリティにおける短期実行と長期実行の比較
セキュリティに関して言えば、短期実行のワークロードは長期実行のワークロードよりもセキュアである傾向があります。なぜなら、短期実行のワークロードは脅威への暴露を制限し、構成の自動化によって一貫性を確保し、エラーを減らすことができるからです。イミュータブルインフラストラクチャにより、構成のずれやパッチ未適用の脆弱性を防ぎ、セキュリティ対策の維持と拡張を容易にします。イメージのセキュリティのテストも、長期実行のワークロードよりも簡単です。

短期実行モデルは、セキュリティを自動化し、デプロイメントパイプラインに統合するための先行投資を提唱するもので、規模が大きくなればなるほど、その効果は大きくなります。この戦略は効率的ですが、すべてのケースに適しているとは限りません。一部の短期実行されるワークロードは、その性質上、またはビジネスの要件上、長期実行されるものとして扱われ続けます。これらはルールではなく例外とすべきで、クラウド環境内で保護され、リスクを最小限に抑えるために分離されます。デフォルトで短期実行モデルを採用し、長期実行の使用を特殊なケースに限定することは、クラウドセキュリティのベストプラクティスと考えられます。

技術の実践者にとって、エフェメラルでイミュータブルなワークロードへの移行は、使用と置き換え(use-and-replace)の方法論に向けた戦略的な動きを表しています。従来の修正とパッチ（fix-and-patch）モデルから決定的な一歩を踏み出し、堅牢性を重視し、脆弱性を最小限に抑える運用環境へと舵を切りました。この進化したフレームワークでは、クラウド環境は仮想リソースをホスティングするためのよりセキュアで信頼性が高く、予測可能な空間になります。

8.1.3 従来のワークロードセキュリティコントロールへの影響

[128] The “Lift and Shift” approach to cloud migration is also covered in *Domain 7: Infrastructure and Networking*.

技術を始めたばかりの人にとって、クラウドのワークロードセキュリティとは、適切なガードレール（技術的予防策[129]）を設定し、それを効率的に監視（モニタリング[130]）し、定期的に健全性と準備状況を確認（アセスメント）することだと考えてください。しかし、従来のコンピューティング環境よりもはるかに速いペースで物事が動き、変化し、非常に大規模で、常に変化する仮想空間でそれを行います。

以下に、クラウドワークロードのセキュリティコントロールに関する重要な考慮事項を示します。

コントロールの適用： 多くの組織はエンドポイント保護プラットフォームや endpoint detection and response (EDR）などのセキュリティエージェント[131]をクラウドワークロードに使用しています。これらのツールは、クラウドの動的で仮想化された性質を取り入れ、サポートする必要があります。エージェントは、コンピューティングコストが大幅に増加しないように、軽量である必要があります。クラウドに対応し、固定 IP アドレスやその他の静的構成に頼らない必要があります。エージェントは、新しいワークロードが起動すると自己登録して、自動スケールグループやイミュータブルシナリオで使用できるようにする必要があります。また、セキュリティグループ内のインバウンドネットワークポートも必要としないはずです。インバウンドネットワークポートがあることで攻撃者が仮想ネットワークに侵入した場合、アタックサーフェスが増加する可能性があります。

監視： 通常、エージェントを使用して OS が生成するワークロードログを取得するツール。クラウドリソースは一過性のものであるため、これらのログは中央ロケーションに迅速に送信される必要があります。非クラウド環境では、監視エージェントは通常、ログをネットワーク経由でログサーバーに移動しますが、クラウドでは、それらのログをネイティブクラウドストレージに直接保存できるため、コスト効率が向上する場合があります。クラウドのさまざまなストレージ要件やコンピュート要件に対応できるコスト効率と柔軟性が重要です。IP アドレスやシステム名だけでは複数のワークロードを参照する可能性があり、名前やアドレスがスケーリング操作されたり異なるクラウドデプロイメント間で再利用されたり頻繁に変更されたりするため、ログエントリを充実させてワークロードのアイデンティティをサポートする必要があります。これは、名前とアドレスは拡張操作中や異なるクラウド配備間で再利用されるためです。

評価： 従来、脆弱性診断（スキャン）はネットワーク経由で実施されていましたが、クラウドでは内部ネットワークでも「デフォルト拒否」コントロールが行われており、セキュリティグループによってワークロード単位で接続が制限されるため、この方法は有効でない可能性があります。評価サーバを同じサブネットに配置し、脆弱性をスキャンすることに頼ることはできません。クラウドの導入により適した 3 つのオプションがあります。1 つ目は、仮想マシンやコンテナイメージを配備する前、すなわち構築時に評価することです。イメージの脆弱性を修正し、イメージの履歴を追跡することで、新しい VM の脆弱性を防ぎ、脆弱なバージョンで実行されている VM を迅速に監査できます。2 つ目は、実行中のワークロードに影響を与えることなく、VM のスナップショットを作成し、オフラインで評価することで、

[129] This reference is specific to technical preventative controls. Additional control mechanisms are covered in *Domain 2: Cloud Governance*.

[130] Security monitoring is covered in detain in *Domain 6: Security Monitoring*.

[131] Agents are specialized software components that are installed on devices for performing specific security-related "actions”.

実行時の脆弱性評価を実行できます。最後は、脆弱性評価エージェントをイメージに組み込むオプションです。

Cloud Workload Protection Platforms (CWPP): これは、複数のワークロードセキュリティ機能を提供するクラウドおよびコンテナ固有のワークロードツールです。クラウドワークロード（VM、コンテナ、サーバーレスなど）全体にわたる詳細な脆弱性スキャンを実行し、エクスプロイトの可能性とビジネスへの影響に基づいて調査結果に優先順位を付けることができます。一部のツールでは、ログとアクティビティの収集、追加の監視、さらにはランタイム保護も統合されています。

8.1.4 ソフトウェア構成分析（Software Composition Analysis）

ソフトウェア構成分析（SCA）ツールとソフトウェア部品表 (SBOM[132])は、ワークロードのセキュリティを向上させるためにイメージパイプラインで使用される重要なツールです。これらのツールは、依存関係の管理、脆弱性の特定、さまざまなクラウドサービスモデル間のコンプライアンスの確保に不可欠です。

SCA ツールは、オープンソースおよび商用コンポーネントのクラウドワークロードを調べるために不可欠です。VM、コンテナ、またはサーバーレス機能のいずれを扱う場合でも、SCA はこれらのコンポーネント内の既知の脆弱性とライセンスの課題を特定するために役立ちます。開発者は、SCA を継続的インテグレーション/継続的デプロイメント（CI/CD）パイプラインに統合することで、アプリケーションのライフサイクルの早い段階で潜在的なセキュリティリスクを確実に解決できます。SCA によって促進されるプロアクティブな脆弱性管理により、チームは依存関係の脆弱性を検出して対処できるため、すべてのコンポーネントが組織のライセンスポリシーに準拠し、法的課題やセキュリティ課題のリスクを軽減できます。

クラウドワークロード全体にわたる SCA の主なメリットは次のとおりです。

- **プロアクティブな脆弱性管理**：配備前の脆弱性の特定と修正を支援し、クラウド環境のセキュリティ対策を強化します。
- **ライセンスコンプライアンス**：すべてのソフトウェアコンポーネントが組織のライセンス契約に準拠していることを確実にするため、法的な課題を回避できます。
- **リスクアセスメント**；特定された脆弱性ごとにリスクスコアを提供し、潜在的な影響に基づいて修正の優先順位付けを支援します。

8.1.5 ソフトウェア部品表（Software Bill of Materials）

[132] NIST. (2021) *Executive Order 14028* - A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open-source and commercial software components. The SBOM enumerates these components in a product.

SBOM は、ソフトウェアの詳細なレシピとして機能し、個々のコンポーネントとそのバージョン、また当該コンポーネントのソフトウェア環境内での相互作用を一覧表示します。このレベルの詳細情報は、潜在的な脆弱性を管理し、あらゆるタイプのクラウドワークロードにわたって品質を保証するために重要です。SBOM を生成することで、効果的な脆弱性管理と法令順守に不可欠な透明性が提供され、オープンソースコンポーネントとプロプライエタリコンポーネントの使用と相互作用の追跡が容易になります。

クラウドワークロードにおける SBOM の重要性は次のとおりです。

- **透明性の向上：** すべてのソフトウェアコンポーネントの包括的な内訳を提供し、クラウドワークロードのソフトウェアサプライチェーンに対するガバナンスとコントロールの向上に貢献します。
- **セキュリティレスポンスの向上：** 影響を受けるコンポーネントを正確に特定することで、脆弱性の迅速な特定と修復を促進します。
- **法令順守：** ソフトウェアコンポーネントの開示を義務付けるコンプライアンス要件への対応を支援します。これは、規制要件が厳しい業界において極めて重要なものです。

要約すると、SCA と SBOM を VM、コンテナ、またはサーバーレスアーキテクチャなど、クラウドワークロードの開発と配備プロセスに統合すると、セキュリティが強化されるだけでなく、これらの環境の信頼性とコンプライアンスも確実になります。これらのプラクティスは、進化するサイバー脅威の状況に対してクラウド運用のセキュリティを確保しようとする組織にとって不可欠です。

8.2 仮想マシン

VM はハイパーバイザー上で動作するオペレーティングシステム全体です。VM はインスタンスとも呼ばれ、ハードウェアに近く、一般的に理解されているため、クラウドワークロードを実行する主な方法です。VM は、ハイパーバイザーによって実施される分離により、ワークロード間および利用者間で厳格に分離されます。この分離により、各 VM がフルスタック OS を維持することを確実にします。

VM の配備は標準化されたベースイメージから一貫して開始され、セキュリティ構成の統一的な基盤を確立します。また、クラウドの VM の自動スケーリング機能により、イミュータブルワークロードの使用が容易になり、効率が向上し、需要の変動に適応できます。

8.2.1 仮想マシンの課題と軽減策

分離によって得られるセキュリティにもかかわらず、共有の物理ハードウェアで動作する VM はサイドチャネル攻撃の影響を受けやすい可能性があります。サイドチャネル攻撃では、攻撃者がハードウェアの動作を分析することで VM の情報を推測できます。このようなリスクを軽減するために、各 VM は個別にアクセスできるだけでなく、ベースとなる VM イメージから確立されるきめ細かいセキュリティ

構成が要求されます。これにより、確実なセキュリティポスチャが維持され、VM の不正アクセスに対する保護が強化され、クラウドインフラストラクチャ全体で一貫した保護レイヤーを提供します。

VM 固有のセキュリティ上の課題として以下があります。

- **イメージコントロール：** VM イメージをセキュアに配備し、常に最新の状態に保つことは、特にユーザーが独自のイメージを提供する場合に課題となります。
- **パッチ管理**： 最新のセキュリティパッチを適用したベースイメージの定期的な更新が不可欠ですが、リソースを大量に消費する可能性があります。
- **変更管理：** CSC が実行中の VM を変更できるようにすると、意図せず脆弱性が発生したり、設定のずれを招く可能性があります。
- **アタックサーフェスの管理：** VM 内のオペレーティングシステムとアプリケーションは、コンテナなど、より合理化されたワークロードタイプと比較して、より大きなアタックサーフェスを作成します。
- **ライフサイクル管理：** 長期間稼働し、手動で設定された VM は、頻繁に交換されないため、強固なセキュリティポスチャの維持が困難になります。
- **ネットワークセキュリティ**： VM インスタンスへのアクセスに使用される SSH 秘密鍵の不注意による漏洩という課題に対処するため、Secure Shell (SSH)を含む、VM へのネットワークアクセスの安全性を確保するために必要なきめ細かな制御メカニズムが必要となります。
- **ルートキットとブートキット：** カーネルレベルの権限を持つルートキットおよびブートキットを使用して、ファームウェアおよびオペレーティングシステムへ感染します。

VM の効果的な脆弱性管理には、悪用される前にセキュリティの欠陥を特定、評価、および軽減することが含まれます。脆弱性管理の課題に対処するには、定期的な評価、優先順位付け、自動化、および統合を重視した戦略的なアプローチが不可欠です。ランタイムの脆弱性の管理は非常に重要ですが、イメージの脆弱性を軽減することは常に優先されるべきです。

これらの課題に対処するには、次の対策を講じる必要があります。

- **セキュアなベースイメージ：** 一元管理されたカタログからセキュアなベース VM イメージを適用します。イメージはバージョン管理され、ビルド後は不変である必要があります。これらのイメージは通常、自動化された場合には「イメージファクトリ」と呼ばれる配備パイプラインを使用して作成されます。

- **スキャン：** VM イメージの使用を承認する前に、脆弱性や設定ミスがないかスキャンします。
- **アタックサーフェスを最小限に抑える：** 不要な OS コンポーネントを削除し、OS 構成のハードニングを実施します。
- **優先順位付け:**エクスプロイト可能性と潜在的な影響を考慮し、環境内で最もリスクが高い脆弱性に焦点を当てます。
- **自動化**： スキャン、パッチ適用、およびレポート作成の自動化を活用して効率を高め、人為的ミスを削減します。
- **統合:** 脆弱性管理ツールを既存のセキュリティおよび IT 管理システムと統合し、統一されたアプローチを実現します。

- **短期実行の仮想マシンの採用:** 可能な場合は、VM がエフェメラルで交換可能なイミュータブルのインフラストラクチャプローチを採用し、セキュアに維持することが困難な長時間実行される VM を最小限に抑えます。
- **コンフィギュレーション管理：** 構成管理と infrastructure as code（IaC）を使用して、望ましい状態を維持し、構成のずれを回避します。
- **モニタリングとロギング：** ログの収集を一元化し、侵入の試みや不審な活動を示す指標を実装します。効果的なモニタリングとロギングにより、VM のアクティビティを可視化し、セキュリティインシデントをタイムリーに検出して対応します。
- **アクセス制御と最小特権：** アプリケーションとユーザーに、VM に関連する認可されたソフトウェアパッケージ、ライブラリ、およびその他のデジタル資産にのみアクセスできる最小限の特権を付与します。最小特権の原則を実装すると、アタックサーフェスが減少し、セキュリティ侵害の潜在的な影響を制限できます。
- **ホストベースのファイアウォールと SSH の強化：** Linux の IP tables ファイアウォールなどのホストベースのファイアウォールを使用してポート、プロトコル、およびパケットタイプを制御することで、VM インスタンスへのネットワークアクセスを制限します。SSH 構成オプションの使用により、すべての VM インスタンスで SSH を強化します。
- **セキュアブート：** OS やウイルス対策ソフトウェアを出し抜くために起動前環境を攻撃する可能性のある潜在的なマルウェアから保護します。
- **特化したセキュリティツール：** ハイパーバイザーを継続的に監視するクラウド環境向けに設計されたツールを実装します。集合住宅内のフロア全体を統括する警備員に匹敵する監視機能で、仮想インフラの安全性と完全性を確保します。

VM の適切なセキュリティコントロールと管理により、クラウドワークロードのセキュアで柔軟な基盤を実現できます。しかし、サーフェスとコントロールが増えると、セキュリティに対する責任や設定ミスが発生する可能性が高まります。イミュータブルインフラストラクチャ、エフェメラルワークロード、および自動構成管理などのクラウドセキュリティのベストプラクティスを遵守することで、これらのリスクを大幅に軽減し、セキュアで効率的、かつレジリエントなクラウド環境を確保できます。

8.2.2 ファクトリを使用した安全な仮想マシンイメージの作成

VM イメージの作成と管理は、VM 環境のセキュリティ保護の要です。このプロセスでは、セキュリティ対策を始めから組み込みます。そのため、VM イメージの作成を効率化し、セキュリティをすべてのレイヤーにシームレスに統合する一連のプラクティスを確立することが不可欠です。セキュアな VM イメージ作成の 2 つの主要な側面は、イメージファクトリとイメージソースです。

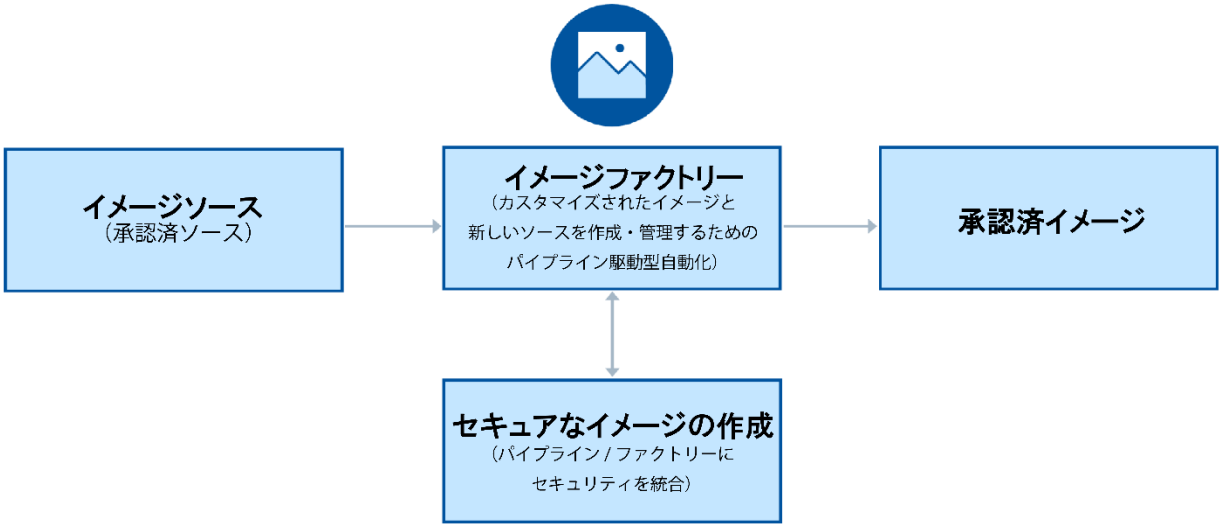


図 43: 仮想マシンイメージの安全な作成プロセス

イメージファクトリは、VM イメージの組み立てとカスタマイズを自動化するプロセスおよびツールです。これらを、レシピ（イメージソースを使用）に従って最終的な VM イメージ（食事）を作成するキッチンと考えてください。イメージファクトリは、セキュリティに重点を置き、VM の作成プロセスにおける一貫性と再現性を確実にします。

イメージファクトリは、一貫性、セキュリティ、および効率性が最優先される VM イメージの組み立てラインとして機能します。これには次のものが含まれます。

- VM イメージのビルド、テスト、およびファインチューニングを行い、配備環境全体での一貫性を確実にします。
- セキュリティの脆弱性につながる不一致を最小限に抑えます。
- セキュリティアップデートと設定変更の統合を合理化します。

イメージソースは、VM イメージをビルドするための出発点です。OS、アプリケーション、ライブラリ、および設定ファイルなどのコアコンポーネントを提供します。VM のレシピの材料と考えてください。

イメージソースは、次のような VM イメージを構成するコンポーネントの入念なキュレーションとメンテナンスに重点を置いています。

- VM イメージの作成に不可欠なソースコードと設定のライブラリを保持します。
- ビルドプロセス内にセキュリティチェックを組み込みます。
- 課題発生時のロールバックを容易にするため、包括的なバージョン履歴を保持します。

セキュアな VM イメージの作成には、VM イメージのセキュリティポスチャを強化することを目的とした一連のベストプラクティスが含まれます。これらのベストプラクティスは以下です。

- **最小特権**： 潜在的な脆弱性を最小限に抑えるには、必要不可欠のソフトウェアとアクセス権だけで VM イメージを設定します。
- **パッチ管理**： VM イメージを定期的に最新のセキュリティアップデートで更新し、新たな脅威から保護します。
- **構成管理：** 標準化されたテンプレートとスクリプトを使用して、すべての VM イメージが必要なセキュリティ基準を満たしていることを確認して、イメージ作成ワークフローを自動化し、手作業によるエラーを削減します。
- **検証とテスト：** VM イメージを使用する前に、セキュリティの脆弱性と運用上の課題について十分にチェックし、VM イメージが安全で正しく機能していることを確認します。VM イメージは常に信頼できるソースから取得する必要があります。
- **ゴールデンイメージを使用:**「ゴールデン」イメージを作成します。これは、必要不可欠の OS と構成設定のみが含まれた、まっさらな最小限の VM イメージです。このイメージは他のすべての VM イメージのベースとなり、一貫性を促進し、無秩序な増加を抑えることができます。

最終的には、VM イメージのセキュリティ保護とは、VM の設計図にセキュリティを組み込む一貫性のある反復可能なプロセスを作成することであり、新しい VM がインスタンス化して稼働しても、サイバー脅威に抵抗できるようにすでに準備されていることを確実にすることです。

8.2.2.1 仮想マシンの推奨ツールとベストプラクティス

あらゆる脆弱性管理プログラムを成功させるためには、適切なツールを活用することが重要です。これらのツールは、VM セキュリティの多様なニーズに対応する特殊な機能を提供します。

- **CWPP（Cloud Workload Protection Platforms）**には通常、クラウドワークロード（VM、コンテナ、サーバーレス）全体にわたる詳細な脆弱性スキャンの機能が搭載されており、発見事項はエクスプロイト可能性とビジネスへの影響に基づいて優先順位付けされます。

- **従来の脆弱性スキャナ**はクラウドではあまり効果を発揮しない傾向がありましたが、現在では多くの脆弱性スキャナがエージェントもサポートしています。これらの製品は、製品によっては CWPP としてブランド変更されている場合があります。
- **構成管理ツール**は、パッチの配備と構成のセキュリティ強化を自動化します。
- **Endpoint Detection and Response（EDR）**エージェントはランタイム監視を実行し、一部のエージェントは脆弱性評価をサポートします。
- **Security Information and Event Management（SIEM）**によるリアルタイムのモニタリングとレポート作成。

以下の脆弱性管理ライフサイクルは、VM の脆弱性の発見から解決までを体系的に扱うアプローチを表しています。クラウドでは、このサイクルはイメージとパッチ適用の代替手段をカバーするように拡大す

べきです。たとえば、実行中の VM を更新されたイメージに置き換えることができます(イミュータブルの背景にある概念)。このサイクルは次の要素で構成されています。

- **識別:** VM に既知の脆弱性がないか自動ツールを使用してスキャンします。
- **評価** ：VM の役割や、データの機密性など、処理/保存されるデータの分類を考慮し、特定された脆弱性に関連するリスクを分析および評価します。
- **軽減とレポート作成:** パッチを適用し、セキュリティ設定を行い、脆弱性に対処する回避策を採用します。
- **文書化**：レポート、コンプライアンス、および監査のために、脆弱性、評価、改善処置の詳細な記録を保持します。

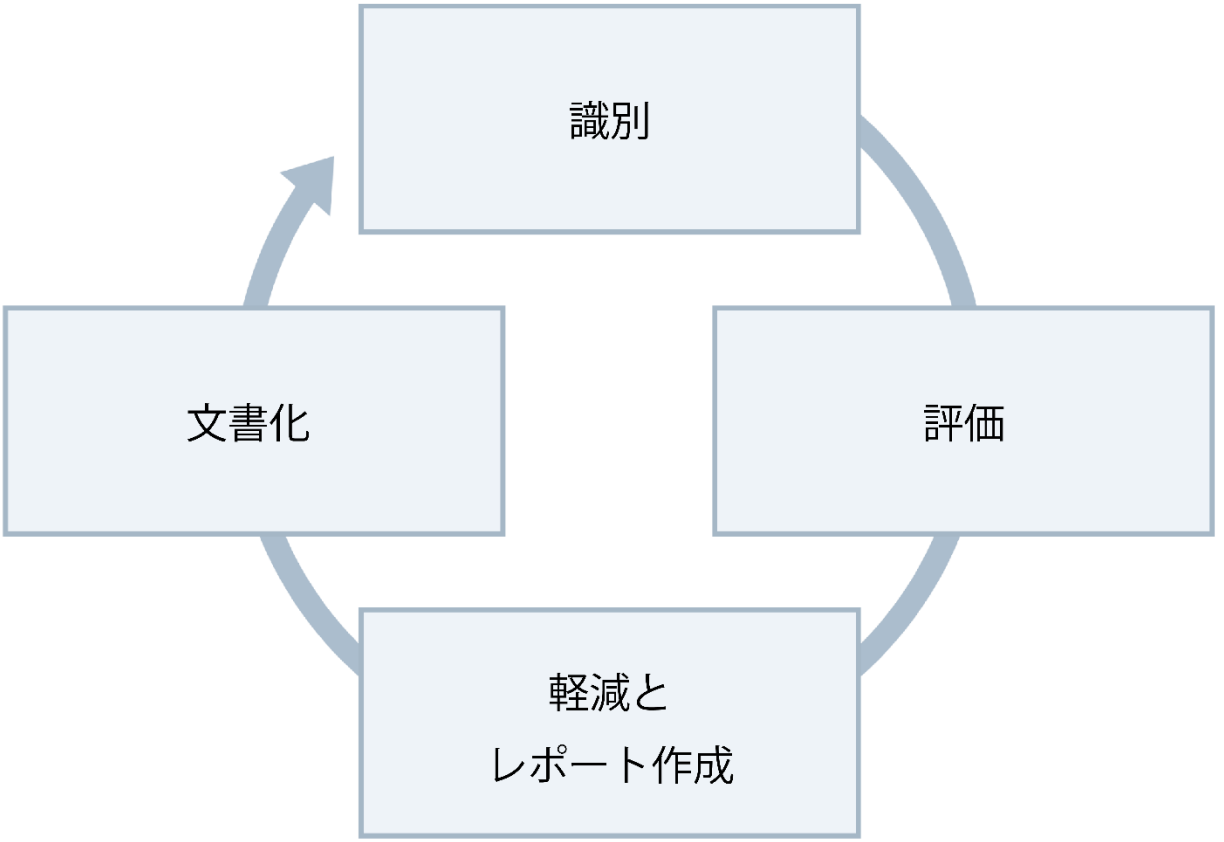


図 44: VM の脆弱性管理ライフサイクル

これらの戦略、ツール、およびプラクティスをセキュリティフレームワークに統合することで、組織は、現代のサイバーセキュリティのランドスケープにおいてデジタル資産を脅かす多くの脆弱性に対する VM 環境の保護を大幅に強化できます。

8.2.3 配備パイプラインによる安全なイメージの作成

配備パイプラインを通じてセキュアなイメージを作成する(イメージファクトリ内で行う場合もある)ことは、セキュリティを中核として仮想環境を構築することを保証する構造化されたプロセスです。この方法論は DevSecOps の原則に沿っており、開発ライフサイクルの基本コンポーネントとしてセキュリティを統合しています。セキュアなイメージの作成は、単一のアクションではなく、配備パイプライン内で慎重に調整された一連のステップです。

次の図は、セキュアなイメージ配備パイプラインのプロセスを示しています。ソースコードから本番環境への配備までの各ステップを示し、開発ライフサイクルを通じてセキュリティ対策を統合しています。

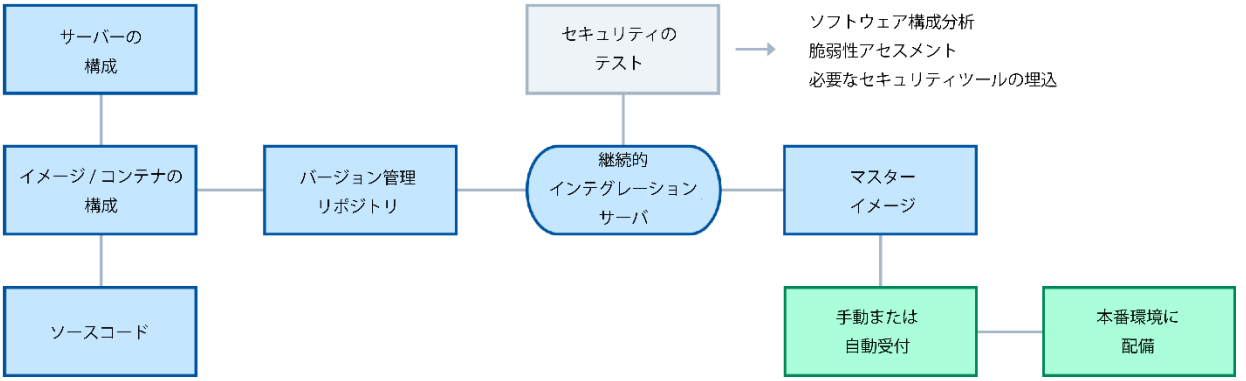


図 45: セキュアなイメージ配備パイプラインプロセス

手順は次のとおりです。

1. **ソースコード:**イメージにコンパイルおよびインストールされる可能性のあるソースコード。
2. **サーバーの構成:** セキュアイメージの基盤は、明確に定義されたサーバー構成から始まります。IaC を利用して、サーバー環境のベースラインとなる OS、ネットワーク設定、セキュリティポリシーを指定します。

3. **イメージ構成：** イメージまたはコンテナにフォーカスが移ります。このステージでは、事前定義されたサーバーセットアップに基づいて、アプリケーションとその依存関係を無駄のないセキュアな構成でパッケージ化します。

4. **バージョン管理リポジトリ：** イメージ設定ファイルの旅は、バージョン管理システムにチェックインされながら続きます。Git リポジトリやコンテナレジストリのようなツールを採用しているため、ビルドプロセスにおける変更追跡、コラボレーション、およびアカウンタビリティが容易になります。

5. **継続的インテグレーションサーバー：** ここで中心となるのは自動化です。継続的インテグレーションサービスまたはサーバーは、構成ファイルからイメージをビルドし、変更がコミットされるたびにセキュリティチェックを実行します。

6. **セキュリティのテストと実施：** ここで、セキュリティテストは統合されたパイプラインコンポーネントになります。SCA と脆弱性スキャン用のツールにより、パイプラインはセキュリティ上の課題を特定して修正し、イメージ作業が進行する前に強化します。

7. **マスターイメージ:** セキュアなマスターイメージが生まれます。プロセスの集大成として、徹底的に吟味されたマスターイメージがセキュアに保管され、すぐに配備できます。

8. **手動または自動受付：** この段階で、イメージは厳密な検査を受けます。リスクと重要度に応じて、手動レビューまたは自動受け入れテストを通過します。

9. **本番環境に配備：** マスターイメージは本番環境にあります。イメージの本番環境への移行は、IaC と自動化ツールを使用して、一貫性があり、セキュアで、正確に配備されます。

これらのステップを実践に組み込むことで、組織はデジタル世界の脅威に対して精査され、準備されたセキュアなイメージを確実に配備できます。このアプローチにより、脆弱性を最小限に抑え、セキュリティが配備のスピードに追随し、環境全体にわたって効率的に拡張できます。データセキュリティについてさらに掘り下げていくと、これらのプラクティスは、クラウドで情報を保護し、堅牢な防御を維持するための基盤となります。

8.2.4 スナップショットとパブリック露出/流出

スナップショットは VM のライフサイクルを管理する上で不可欠であり、保存とリカバリのためにストレージボリュームにほぼ瞬時のコピーを提供します。スナップショットは、特定の瞬間の VM の保存された状態であり、ワークスペースの詳細な写真とよく似ており、ファイルから設定まですべてをキャプチャします。これには機微データも含まれます。そのため、不正アクセスや不用意な漏洩、およびデータの流出を防ぐため、スナップショットは慎重な取り扱いが必要です。

パブリックへの露出の軽減
有益な反面、スナップショットの包括的な性質は、特に機密データを含む場合にリスクをもたらします。スナップショットを作成または取得できるユーザーを管理するために、厳格なアクセス制御を確立することが重要です。これらのコントロールをマスター鍵に相当するものとして想像してみてください。信頼できる担当者のみがそのような権限を振るうべきです。

スナップショットの暗号化は、意図しない受信者が秘密のメッセージを読み取れないようにする暗号のように、不可欠なセキュリティレイヤーを追加します。スナップショットが不用意に公開されても、暗号化されたデータは保護され、対応する復号鍵がなければアクセスできなくなります。

データの流出を防ぐ
スナップショットの維持には、不要になった機密文書をシュレッダーにかけるといったような、定期的な見直しも必要です。このプロセスによってセキュリティが強化され、不要なデータ保存を排除することでクラウドリソースの支出も最適化します。

Cloud Security Posture Management（CSPM）のようなモニタリングツールは、スナップショットに対して警戒監視員として機能し、誰がアクセスしたり変更を加えたりするかを精査します。異常な行動に対するアラートの導入は、脆弱なポイントを監視する監視カメラの設置に匹敵し、不正な試みを確実に検知して迅速に対処することができます。

スナップショットは、それが表す本番システムと同じレベルのセキュリティが与えられる必要があります。仮想マシンの作成時にすべてのデータと構成をカプセル化するため、管理を誤るとデータ漏洩の潜在的なベクトルになる可能性があります。スナップショットのセキュリティに対する包括的なアプローチは、単なるデータの保護にとどまりません。また、これらのスナップショットがリスクや負債を生じないようにすることも含まれます。

8.3 コンテナのセキュア化

このセクションでは、セキュアなコンテナイメージの構築、コンテナの効率的かつ安全なオーケストレーション、およびコンテナ化された環境で発生する無数のセキュリティ課題の管理の重要性について詳しく説明します。コンテナイメージの作成から Kubernetes のようなシステムによるデプロイのオーケストレーションまで、コンテナライフサイクルの各ステップのセキュリティ保護に関する包括的な洞察を提供します。

8.3.1 コンテナイメージの作成

コンテナイメージは、アプリケーションの実行に必要なコード、ランタイム、システムツール、ライブラリ、および設定を含む、軽量でスタンドアロンの実行可能なソフトウェアパッケージです。コンテナイメージは、通常 Dockerfile[133]で定義される、ベース OS、依存関係、およびアプリケーションコードを指定する一連の命令から作成されます。これらのイメージは、異なる環境で容易に共有および配備できるため、アプリケーションの一貫性と移植性を確保できます。

コンテナは、承認されたセキュアなベースイメージを使用して構築する必要があります。命令を評価するツール（Dockerfile）を使用して、セキュリティを追加および評価できます。*アーティファクトリポジトリ*のセキュリティを確保することも重要です。アーティファクトリポジトリは、コンテナイメージが登録および保存される場所です。

コンテナは本質的にイミュータブルインフラストラクチャの概念を促進します。コンテナイメージをビルドしてデプロイすると、そのイメージは変更されません。更新と変更は、コンテナを新しいイメージに置き換えることによって行われます。これは、機械の不良部品を修理するのではなく、新品と交換することと同等です。

[133] A Dockerfile is a text document that contains all the commands a user could call on the command line to assemble an image.

8.3.2 コンテナネットワーキング

コンテナネットワーキングは、ホストオペレーティングシステム（多くの場合 Linux）ネットワーキングの拡張です。

Kubernetes のネットワーク化、ひいてはネットワークの分離は、個々のコンテナからアプリケーション対応のロードバランサー（Ingress Controller など）に至るまで、複数のレベルで行われます。ネットワークポリシーを定義するためのさまざまな技術が存在します。繰り返しになりますが、これらの一部はプロバイダのサービスである可能性がありますが、自己管理型である可能性もあります。

8.3.3 コンテナオーケストレーションと管理システム

コンテナオーケストレーションシステムは、コンテナ化されたアプリケーションの複雑なライフサイクルを管理するための不可欠なツールとなっています。Kubernetes（K8s）は、その柔軟性と包括的な機能セットにより、これらのシステムの中でも有数のオープンソースプラットフォームとなっています。Kubernetes は、コンテナにデプロイされたアプリケーションに関する配備、スケーリング、および管理をマシンクラスタ間でオーケストレーションし、シームレスな自動化と一貫した運用を可能にします。コンテナはマイクロサービス(アプリケーションコンポーネント)をホストし、コンポーネントが一貫した環境で実行されるようにします。

主要な CSP は Kubernetes を採用・適応し、クラウド環境に合わせてカスタマイズしたバージョンを提供しています（例：AmazonEKS、Microsoft Azure Kubernetes Service、Google GKE ）。これらのサービスは、標準の Kubernetes の堅牢な基盤に独自の機能を追加し、ユーザーに使い慣れた機能とプロバイダー固有の拡張機能の組み合わせを提供します。

オープンソースの Kubernetes を使用している場合、デフォルト設定はセキュアでなかったり、希望するセキュリティポスチャと整合していなかったりする可能性があるため、注意が必要です。これらのデフォルトには次のものがあります。

- ダッシュボードを開くと、適切に保護されていない場合、貴重な情報が不注意に公開される可能性があります。
- 必要以上のアクセスを許可する可能性のある広範な権限を持つデフォルトのサービスアカウント
- 特定の配備環境における厳しいセキュリティ要件を満たさないネットワーク構成

このイメージは、基本的な Kubernetes アーキテクチャと、コアとなる管理コンポーネント、コンテナが実行される 2 つの「ポッド」 、 ユーザーがデプロイされたアプリケーションにアクセスするロードバランサーを示しています。

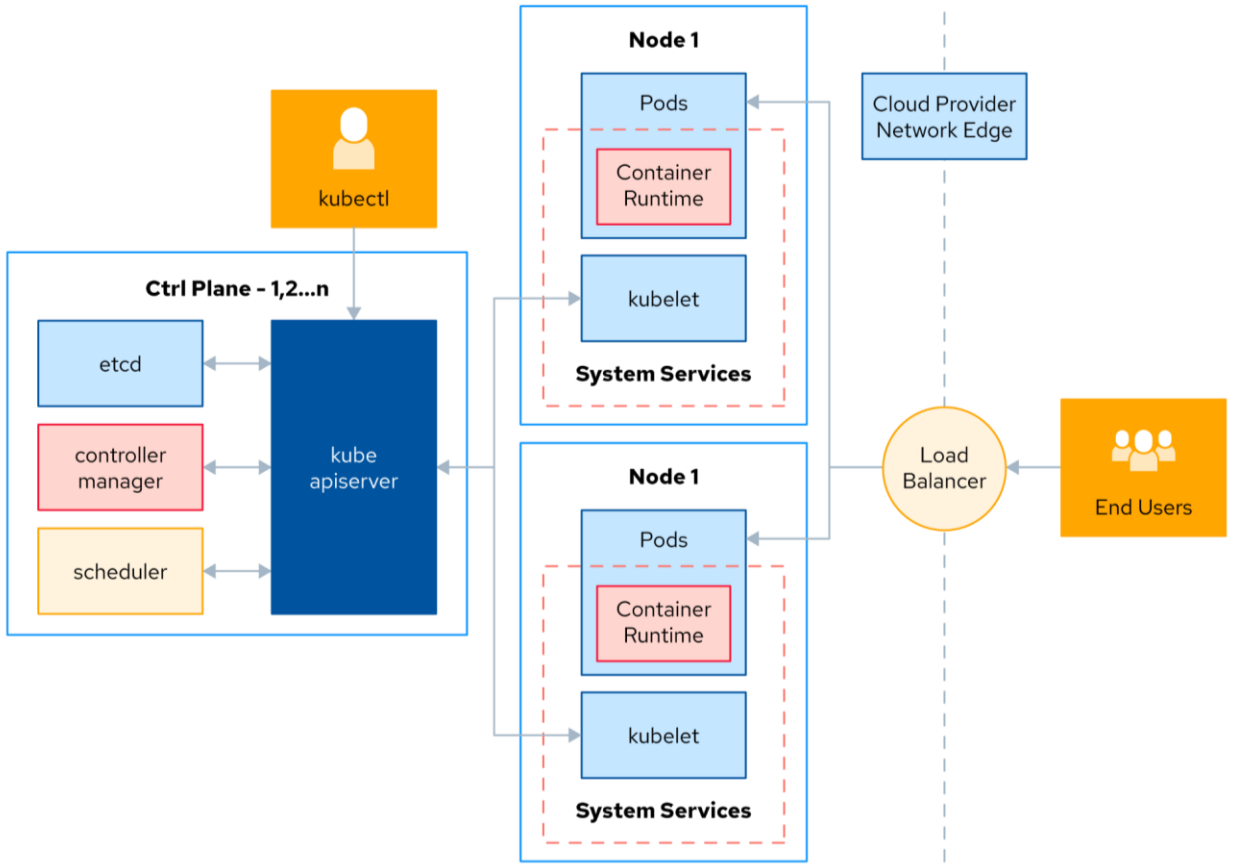


図 46: ロードバランサーと Pod による Kubernetes の基本的なセットアップ

8.3.4 コンテナオーケストレーションのセキュリティ

Kubernetes のようなコンテナオーケストレーションプラットフォームは、コンテナ化されたワークロードをクラウドで管理するために不可欠になっています。しかし、これらの複雑なプラットフォームのセキュリティ保護は困難な場合があります。Kubernetes は、複数のコンポーネント、アプリケーションプログラミングインターフェイス（API）、およびネットワークインターフェイスで構成され、適切に構成およびハードニングされていない場合、攻撃者が標的にできます。設定ミス、パッチ未適用の脆弱性、および許可が過大なアクセス制御は、コンテナ環境の侵害や危険につながる可能性があります。

ベストプラクティスは次のとおりです。

- **CSP サービスを利用:** コンテナ化されたアプリケーションを導入する場合は、CSP サービスが利用できる場合はそれを利用することが最適です。CSP は通常、セキュリティを自動化および強化するために設計されたツールスイートを提供します。これには、Kubernetes-as-a-Service のようなオーケストレーションのためのマネージドサービスが含まれる場合があり、セキュリティに重点を置き、コンプライアンスに対応したデフォルト設定が付属しています。

- **サービスのハードニング：**サービスのハードニングは、システムのアタックサーフェスを最小限に抑えるためのプロアクティブなアプローチです。これには、不要な機能を無効にし、最小特権アクセスを確実にし、またコンテナ間のトラフィックを制限するネットワークポリシーとファイアウォールを実装することで、オーケストレーターを保護することが含まれます。ハードニングには、コンテナのセキュアなベースイメージの使用、Kubernetes 内のセキュリティコンテキスト設定の採用、いわゆる「アドミッションコントローラー」を利用して適切なセキュリティプラクティスを実施することも含める必要があります。
- **パッチ/アップデート:**コンテナエコシステム内のすべてのコンポーネントの定期的なパッチ適用と更新が極めて重要です。これにはコンテナ自体だけでなく、ホスト、Kubernetes のようなオーケストレーションプラットフォーム、その他のサポートサービスも含まれます。パッチ管理プロセスを自動化することで、パッチが利用可能になった時点でパッチを確実に適用できるため、脆弱性が悪用されるリスクを軽減できます。
- **コンテナのセキュリティポリシー：** Kubernetes Security Policy、PodSecurityPolicy、Network Policy などのツールを使用してセキュリティポリシーを定義し、適用することで、ポッド間のネットワークアクセスを制限および監視できます。
- **セキュリティベンチマークとツールの活用：**Kubernetes の CIS ベンチマーク[134]などの標準および標準化ツールは、セキュアでないデフォルトを検出して改善するための構造化されたアプローチを提供します。

- **セキュアなイメージリポジトリ：**セキュアなイメージリポジトリは、コンテナセキュリティの中心です。ロールベースのアクセス制御（RBAC）を備えたプライベートリポジトリを使用して、イメージをプッシュおよびプルできるユーザーを管理します。コンテナイメージのスキャンと脆弱性検出を、配備前と本番環境で日常的に実施します。イメージ署名を利用して信頼の連鎖を確立し、イメージが作成時から配備時まで改ざんされていないことを確認します。

- **セキュアな構成:**コンテナ化された環境の完全性とセキュリティを確保するには、堅牢でセキュアな構成から始めることが重要です。これらの基本設定はコンテナ環境のあらゆる側面をカバーし、セキュリティ環境を提供するために不可欠です。
    - *クラスタホスト：* ホストの OS を強化し、最小限のインストールを維持し、ホストレベルのセキュリティ管理を確実に行うことで、クラスタリソースを保護します。
    - *ストレージレイヤー：* 保存中および移動中のデータには暗号化を適用し、アクセス制御リスト（ACL）またはポリシーを使用して永続的なボリュームへのアクセスを制限します。また、機微データへのアクセスを監視するためにロギングを使用します。
    - *ネットワークレイヤ：* ネットワークセグメンテーションとファイアウォールを実装して、サービス間のトラフィックの流れを制御します。ネットワークポリシーを使用して、コンテナ間の通信方法や外部ネットワークとの通信方法に関するルールを適用します。
    - *イメージの検証/署名:* CI/CD パイプラインに手順を組み込み、イメージの検証と署名を行います。これには、既知の脆弱性をチェックするツールの使用や、信頼できる機関によって署名されたイメージのみがオーケストレーターによって実行されるようにすることなどが含まれます。

[134] CIS. (2024) Center for Internet Security: *CIS Benchmarks*

8.3.4.1 アーティファクトリポジトリの保護

セキュアなアーティファクトリポジトリは、コンテナイメージを含むソフトウェアコンポーネントの保管庫として機能し、次のことを保証します。

- リポジトリは、デジタル署名や検証などのコンテンツ信頼メカニズムを適用して、コンテナイメージの信頼性と完全性を保証します。
- アクセスは厳密に制御され、認証されたユーザーのみがイメージをプッシュまたはプルできます。これは、認証された顧客からのみトランザクションを許可する銀行とよく似ています。
- 定期的にイメージをスキャンし、脆弱性の有無を調べます。これは、病気の兆候を早期に把握するための定期的な健康診断と同様です。
- コンテナイメージはイミュータブルである必要があります。
- イメージの証明は徹底的に文書化され、保護されており、保存状態の良い公的登録簿と同様に、その出所と製作者の明確な系譜を提供しています。
- セキュアなアーティファクトリポジトリは、継続的インテグレーションおよび配備パイプラインとシームレスに統合され、配備前のコンテナイメージのスキャンと検証を自動化します。

8.3.4.2 セキュアリポジトリを使用するためのベストプラクティス

アーティファクトリポジトリのセキュリティ保護には、以下に示すような、より広範なサイバーセキュリティの原則を反映した勤勉なプラクティスが必要です。

- **セキュアなソースのみを有効にする:** 重要な機械に出所不明の怪しいスペアパーツを使用することを避けるように、開発者はセキュアで信頼できるソースからのイメージのみを使用するべきです。
- **イメージの署名と検証:** デジタル署名は真正性を証明する印鑑の役割を果たし、歴史上の手紙の蝋印のように、イメージが改ざんされずにそのまま残っていることを確認します。
- **脆弱性のスキャン：** 配備前に、イメージは徹底した脆弱性スキャンを受ける必要があります。これは航空機の包括的な飛行前検査に例えることができます。
- **アクセスコントロール** リポジトリへのアクセスを制限することで、セキュリティで保護された施設内の機密情報にアクセスすることになぞらえて、正当なニーズを持つユーザーだけがイメージを取得または変更できるようにします。
- **監査証跡：** 誰がリポジトリのコンテンツにアクセスしたか、または変更したかを詳細に記録することが重要です。これにより、船舶のログが船上で発生した事象を把握していることと同様に、透明性が高まり、コンプライアンスに役立ちます。
- **定期的なアップデート：** リポジトリソフトウェアの継続的な更新とパッチ適用により、既知の脆弱性から保護し、イメージを保存するためのセキュアな環境を維持します。

コンテナイメージのセキュリティ保護は、強固な基盤を確立し、厳格なプロセス、完全性、きめ細かな記録管理を実施するための演習です。コンテナイメージのライフサイクルの各段階にセキュリティを組

み込むことで、組織はコンテナ化されたアプリケーションを脅威から守り、コンプライアンス要件を満たすことができます。

8.3.5 コンテナの脆弱性の管理

最新のソフトウェア配備プロセスのセキュリティ保護には、コンテナの脆弱性の管理が含まれます。他の技術と同様に、コンテナには、体系的な管理を必要とする独自の潜在的なセキュリティ課題が存在します。

コンテナの脆弱性を管理する場合の主な考慮事項は次のとおりです。

- **CI/CD パイプラインの統合：**脆弱性管理ツールを CI/CD パイプラインに統合することは、厳格な品質保証プロセスを生産ラインに組み込むことに似ています。この統合により、コンテナの開発と配備のすべての段階で、徹底したセキュリティチェックが実施されます。これは、各製品コンポーネントが組み立てラインを移動する前に行う綿密な検査と同様です。

- **定期的なアップデート：** コンテナイメージとその依存関係を常に最新の状態に維持する必要があります。
- **イミュータブルコンテナ：** コンテナ管理におけるイミュータブルの原則は、極めて重要な防御戦術です。一度配備されたコンテナは変更されません。必要な更新が行われると、新しいコンテナが配備されます。この方法は、その場しのぎで修正するのではなく、機械の交換可能な部品を使用して最適な性能を確保するようなものです。
- **セキュリティポリシーの実施：** 配備のために事前にスキャンし、承認されたイメージを使用するように指示するセキュリティポリシーを実装および実施することで、セキュアなゲートが作成されます。これは、確認されたゲストのみが会場への入場を許可されるようにする用心棒のようなものです。
- **役割ベースのアクセス制御（RBAC）：**RBAC はコンテナ管理ツールとリソースへのアクセスを制限します。チームメンバーは、その役割を果たすために必要なアクセス権しか与えられないことを保証します。それ以上でもそれ以下でもないです。これは、セキュリティで保護された施設内のエリアごとに異なる鍵を発行し、自分の責任に基づいてアクセスを制限することに似ています。

- **属性ベースのアクセス制御 (ABAC[135]):** ABAC は、その固有の柔軟性と動的な性質により、コンテナ化された環境に特化したよりきめ細かいアプローチを提供します。ABAC では、ロールに加えて属性も考慮してアクセスを決定します。これらの属性には、ユーザーの場所、デバイスのタイプ、コンテナ内に保存されたデータの分類（機密、公開など）情報、またはその他の関連する特性を含めることができます。これにより、コンテナ化されたクラウド環境内で、より柔軟で動的なアクセス制御が可能になります。

[135] NIST. (2024) *CSRC Projects: Attribute Based Access Control (ABAC)*.

これらのプラクティスをコンテナのライフサイクル(開発開始から配備、さらにはその先まで)に組み込むことで、強化されたワークフローを作成できます。セキュリティは単なる後付けではなく、プロセスの不可欠な部分であるという考えを支持しています。さらに、RBAC を導入することで、組織はセキュアで効率的なワークフローを維持しながら、適切な個人に適切なレベルのアクセスを常に確保することができます。

8.3.6 コンテナのランタイム保護

コンテナのランタイム保護は、潜在的な脅威や誤動作の発生時に確実に検出して管理し、コンテナ化されたアプリケーションをセキュアに保ち、スムーズに実行できるようにします。

コンテナのランタイム保護には、いくつかの重要な側面があります。

- **リアルタイムの可視性：** 効果的なランタイム保護は、リアルタイムの可視化から始まります。監視ツールは、コンテナのアクティビティを継続的に監視する目であり、セキュリティ上の脅威や運用上の異常を示す可能性のある異常な動作をスキャンします。
- **ロギングと監査：** 綿密なロギングと監査により、コンテナアクティビティとユーザー操作の詳細なログブックが作成されます。ログの記録は、犯罪捜査における防犯カメラの映像と同じ目的を果たす、事件後の分析にとって貴重なものです。
- **マイクロセグメンテーション：** 漏洩の影響を最小限に抑えるために、ネットワークセグメンテーションが実装され、船の水密区画と同様にコンテナ用の隔離区画が作成されます。水と同様に、侵害が発生しても脅威は封じ込められます。
- **コンテナ固有のファイアウォール：** このファイアウォールはトラフィックレギュレータとして機能し、ネットワークトラフィックフローを管理するルールを確立し、実施します。これらは、車両の出入りを制御し、秩序とセキュリティを確保する戦略的に配置された検問所のようなものです。
- **自動応答：** 最後の側面は、自動応答機能です。この緊急プロトコルは、脅威が検出されるとすぐに実行に移され、侵害されたコンテナを隔離したり、アクセスを拒否したり、システムを既知の良好な状態に戻したりします。これは、人間の介入なしに侵入に対応する自動防御システムとよく似ています。

ランタイム保護とは、常に警戒を怠らないことです。コンテナを監視し、プロアクティブおよびリアクティブなセキュリティ対策によってあらゆる脅威を迅速に無効化する堅牢で応答性の高いシステムを構築し、コンテナ化されたアプリケーションのライフサイクル全体にわたって完全性とレジリエンスを確保します。

8.4 PaaS セキュリティ

CSP の PaaS には、多くの場合、ワークロードコンポーネントを置き換えるサービス（たとえば、サーバ上のキューイングソフトウェアの必要性を置き換えるメッセージキューサービス）や、コンテナのようにワークロード自体を実行するためのサポートホスティングプラットフォームが含まれます。PaaS サ

ービスは、SQL Server や Oracle のデータベースサービスのように、VM 上の標準的なソフトウェアスタックを自動化およびオーケストレーションし、基盤となる VM を管理するため、利用者は構成設定とそのデータベースを管理するだけで済みます。

つまり、PaaS は、一般的なソフトウェアプラットフォームを自動化して調整するサービスから、コンテナやサーバーレス機能のような任意のワークロードをホストするもの、メッセージキューのような機能を完全に抽象化するサービスまで、非常に幅広い選択肢をカバーします。

8.4.1 PaaS の一般的なセキュリティプラクティス

PaaS のセキュリティは、一般的なセキュリティ対策と、PaaS 環境固有のコンポーネントに合わせた具体的な対策を統合する、多層的なアプローチにかかっています。

- **セキュリティ監査：** 潜在的なセキュリティ脅威を特定して軽減するには、PaaS コンポーネントの定期的な脆弱性評価、つまりヘルスチェックが不可欠です。これらの監査は、PaaS 環境内の進化する脅威や変化に適応するために定期的に実施する必要があります。
- **ロギングとモニタリング** ：効果的なセキュリティは可視化にかかっています。PaaS プラットフォーム内に包括的なロギングとアクティビティのリアルタイム監視を実装すると、不審な行動や侵害の可能性を早期に検出できるため、迅速な対応と軽減の取り組みが促進されます。
- **最小特権**： 最小特権の原則に従うことで、不正アクセスやデータ漏洩のリスクを最小限に抑えることができます。組織は、役割に必要な最小限のアクセスレベルのみをユーザーとサービスに付与することで、アタックサーフェスを大幅に削減できます。
- **MFA(多要素認証)**: MFA でアクセス制御を強化すると、セキュリティのレイヤーが追加されるため、攻撃者による不正アクセスが非常に困難になります。このアプローチは、取引にカードと暗証番号の両方を必要とする銀行と同様であり、機密性の高い業務のセキュリティを強化します。
- **アクセスレビュー:** アクセス権の定期的な再評価により、適切な個人とサービスのみが重要なリソースにアクセスできるようにします。このプロセスにより、不要になったアクセスを速やかに取り消すことができるため、セキュリティポスチャがさらに強化されます。

8.4.2 暗号化とアクセス制御

PaaS セキュリティでは、アイデンティティ管理、データの暗号化、およびアクセス制御が強固なセキュリティポスチャの柱となります。このセクションでは、PaaS 環境のセキュリティ保護における暗号化とアクセス制御に不可欠な役割について説明します。

暗号化: 堅牢な暗号化方式によって保存中および移動中のデータを保護することは、貴重品を金庫で保護し、セキュアな転送を提供することと似ています。暗号化鍵を細心の注意を払って管理することにより、許可されたエンティティのみが暗号化されたデータにアクセスできることが保証されます。

アクセス制御:

- **ネットワークセグメンテーションとファイアウォール：** ネットワークセグメンテーションの実装とファイアウォールの導入により、PaaS 環境内にセキュアゾーンを作成し、トラフィックフローを制御し、情報漏洩の潜在的な影響を軽減できます。
- **RBAC:** システムは特定の役割に基づいてアクセスを割り当て、個人またはサービスが割り当てられた機能に必要なリソースにのみアクセスできるようにします。
- **ABAC:** 属性に基づいてアクセスを割り当て、クラウド環境におけるより柔軟で動的なアクセス決定を可能にします。
- **API ゲートウェイポリシー：** API ゲートウェイの厳格なポリシーは、入場を管理する用心棒のように、外部エンティティが PaaS とやり取りする方法を制御します。

これらのプラクティスは、PaaS 環境に対して多層的な防御戦略を構築し、さまざまなセキュリティの脅威に対して可能な限りレジリエンスを確実にすることを意味します。

8.4.3 特定の PaaS のセキュリティ保護

一般的なセキュリティ対策以外にも、特定の PaaS プラットフォームでは、その固有な脆弱性によって、特別な保護戦略が求められます。このセクションでは、CDN、通知サービス、およびメッセージキューなど、それぞれ脅威から保護するためにカスタマイズされたセキュリティ対策を必要とする特定の PaaS のセキュリティ保護に焦点を当てます。

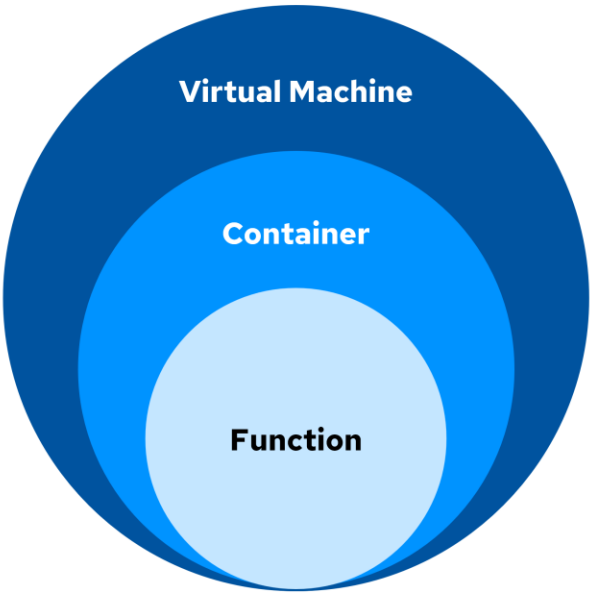
- **コンテンツ配信ネットワーク（CDN）：** CDN を経由して移動するデータのセキュアソケットレイヤー（SSL）またはトランスポートレイヤーセキュリティ（TLS）暗号化は、情報の機密性と改ざんされていないことを保証します。強固なアクセス制御と認証メカニズムが、保存されたコンテンツへのアクセスを制限します。
- **通知サービス：** 通知を暗号化し、セキュアな配信チャネルを使用することで、信頼できる宅配便を通じて機密文書を送信することと同様に、内部の情報を保護します。強固な認証方式では、通知の送信が認可されたサービスとユーザーの正当性が確認されます。
- **メッセージキュー：** 保存中および移動中のメッセージの暗号化、およびセキュアなアクセスポリシーと RBAC により、メッセージキュー内の機密データが保護されます。これにより、許可されたエンティティのみがキューをパブリッシュまたはサブスクライブできることが保証され、通信の完全性が維持されます。

PaaS の各コンポーネント固有の脆弱性があり、データの完全性を保護し、プライバシーを確保し、信頼性の高いサービス運用を維持するためには、カスタマイズされたセキュリティ対策が必要であることを理解することが不可欠です。PaaS のセキュリティには、一般およびサービス固有の脆弱性に対処する勤勉で詳細なアプローチが必要です。これらの戦略を実施することで、組織はさまざまなセキュリティの脅威に対する弾力的な防御を構築し、クラウドベースのアプリケーションやサービスの完全性、プライバシー、および信頼性を確保できます。

8.5 サーバーレスまたは Function as a Service のセキュア化

サーバーレスコンピューティングは、一般に Function as a Service（FaaS）として知られており、開発者が基盤となるインフラストラクチャを取扱うことなくコードを作成してデプロイする方法です。サーバーの管理はクラウドプロバイダーが行い、これらには、サーバーのプロビジョニング、さまざまな負荷を処理するための拡張、およびメンテナンスなどが含まれます。これにより、開発者はサーバー管理に関わる下層の作業を気にすることなく、純粋にコーディングに集中できます。

「サーバーレス」という用語は、まだアプリケーションの実行にサーバーが使用されているため、やや誤った呼び方です。ただし、これらのサーバーの管理は、アプリケーションの所有者の方には降りかかりません。その代わり、CSP によって抽象化されます。このように従来のインフラ重視から脱却すると、開発者は使用したコンピューティング能力に対してのみ課金されるようになり、多くの場合、コード実行の正確なミリ秒単位で課金されます。



サーバレスコンピューティングの主な利点は、運用のシンプルさです。開発者がコードを提供し、システムのメンテナンスや拡張性などの運用面はすべてクラウドプロバイダが取り扱います。このシステムは、アプリケーションのニーズに基づいてコンピューティングリソースを自動的に調整するため、アプリケーションの構築と拡張を迅速かつ最小限のオーバーヘッドで行いたい開発者にとって、非常に柔軟で効率的なソリューションを提供します。

サーバーレスの各ファンクションは、通常、使い捨ての仮想マシン上に存在する軽量な使い捨てコンテナ内で実行されます。この方法では、各ファンクション呼び出しは明確に分離された環境で動作し、強固な分離を促進し、ファンクション間の干渉を防ぎます。これらの実行環境はエフェメラルであり、管理が必要な永続的な OS がないためアタックサーフェスが大幅に縮小され、潜在的なセキュリティリスクを最小限に抑えることができます。さらに、このモデルでは、各ファンクションの実行が分離され、一時的であることを確実にすることで、セキュリティが強化されます。

それにもかかわらず、クラウドプロバイダがセキュリティ責任の多くを引き受けてはいるものの、開発者は、アプリケーションコードを保護し、アクセス制御を効果的に管理し、ファンクションとの間で転送される機密データを保護しなければならないことを覚えておかなければなりません。FaaS を正しく活用することで、開発者はインフラストラクチャのセキュリティ管理をクラウドプロバイダに任せながらコーディングに集中できるため、FaaS は運

Figure 47: The FaaS Paradigm

用の複雑さを軽減しながらアプリケーションロジックを実行するためのセキュアでスケーラブルなオプションとなります。

図は、FaaS モデルにおけるファンクション、コンテナ、および仮想マシンの関係を示しています。

- 一番内側の円は個々のファンクションを表し、アプリケーションコードが含まれています。
- ファンクションはコンテナ内にカプセル化され、必要なランタイム環境と依存関係を提供します。
- そして、コンテナは CSP が管理する仮想マシン上で実行されます。

8.5.1 FaaS のセキュリティ課題

サーバレスコンピューティングに関しては、共通して注意すべきセキュリティ上の課題があります。

- **サードパーティサービスと API**：これらは攻撃の可能性を生み出します。これらのインターフェースが侵害された場合、攻撃者は不正な設定を行ったり、クラウド環境をスパイしたりできる権限がユーザーに付与される可能性があります。
- **脆弱な依存関係:** サーバーレスファンクションは外部ライブラリに依存することが多く、脆弱性や悪意のあるコードが潜んでいる可能性があります。これらの依存関係を厳密にチェックして更新しないと、攻撃者のバックドアとして機能する可能性があります。
- **誤設定:** 設定が正しくない、または許容しすぎると、サーバレスアーキテクチャ内の機密リソースへのアクセスが不用意に開かれる可能性があります。アクションを制限するには、ファンクションを実行可能なユーザーとそのファンクションがアクセスできる内容に関するセキュリティ設定を厳密にコントロールする必要があります。
- **あるファンクションに対する IAM の過剰な特権：** ファンクションに過剰な権限を与えると、不正アクセスやデータ漏洩のリスクが大幅に高まります。このような設定により、ファンクションに必要以上なアクセスを許可し、攻撃者はこれらの特権を邪悪な目的のためにエクスプロイトできるようになります。
- **ファンクションのための直接インターネットアクセス：** ファンクションは、ネットワークセグメンテーションや ACL などの適切なネットワーク制御なしで直接インターネットにアクセスできる場合があります。この制限の欠如は、ファンクションを外部の脅威に露出させるだけでなく、外部エンティティによるデータ流出の潜在的なチャネルにもなります。

上記の各課題は、サードパーティ API の吟味から、依存関係や構成の入念な管理まで、サーバーレスモデル内での慎重なセキュリティプラクティスの必要性を強調しています。サーバーレスモデルはスケーラビリティとコストの点で有利ですが、脆弱性から保護するには、これらの分野における警戒が不可欠です。さらに、独自のサーバーレス環境は、他のワークロードタイプでは課題にならない特定のセキュリティ上の考慮事項をもたらします。

次に、サーバレス固有のセキュリティに関する考慮事項を示します。

- **ステートレスな性質:** サーバーレスファンクションは内部状態を保持せずに動作するため、セキュリティアプローチが大きく変わります。監視対象の永続的なサーバー環境が無いため、コード自体のセキュリティとさまざまな依存関係にスポットライトが当てられます。この変化では、コードの書き方、呼び出すライブラリ、および処理するデータを完全に理解する必要があります。開発者は、実行環境に必要なすべてのセキュリティ対策を施して、ファンクションが自己完結型であることを確認する必要があります。
- **イベント駆動型セキュリティ：** サーバレスコンピューティングのイベント駆動型の特性は、固有の課題をもたらします。サーバーレスファンクションは通常、イベントに応じて実行されます。イベントは、ユーザー要求からスケジュールされたタスクまでさまざまです。このモデルでは、悪意のあるトリガーを防ぐために、イベントの厳格な検証が必要です。ファンクションが正当で意図したトリガーにのみ応答するように、イベント入力の慎重な作成と検証が重要になります。これらのイベントのセキュリティを確保するには、ファンクションの実行を許可する前に、イベントソースを精査し、厳密な検証チェックを実行する必要があります。
- **CSP への依存：** サーバーレスアーキテクチャでは、多くの場合、利用可能なセキュリティ対策が CSP の提供するサービスによって定義されます。この制限は、責任共有モデルを理解して活用することが重要であることを意味します。CSP がクラウドインフラストラクチャを保護する一方で、CSC は自社のコードとデータの保護に注力する必要があります。アイデンティティアクセス管理（IAM）、コードセキュリティ、データ暗号化、ポリシー適用など、プロバイダがどのセキュリティ面を取扱い、どの責任が CSC にあるのかを知ることが重要です。この共有された状況をナビゲートすることは、CSP のツールやサービスについて常に情報を入手し、それらを効果的に統合することを意味します。

サーバーレスセキュリティを効果的に運用するには、サーバーの管理が自分のコントロールから外れていても、コードと実行環境のセキュリティを確保する責任は残るというモデルに適応する必要があります。この適応には、CSP のツールに依存し、構成、イベント管理、依存関係のセキュリティのベストプラクティスに厳密に従う必要があります。セキュアなサーバーレスアプリケーションを構築するには、ステートレス、イベント駆動型トリガー、および責任共有モデルのニュアンスを理解することが重要です。

8.5.2 サーバーレスのための IAM

IAM は、サーバーレスアーキテクチャのセキュリティ保護の要です。サーバーレスアプリケーションはドメインを越えてさまざまなサービスを統合し、連携できるため、信頼とアクセスの管理が複雑になります。不正アクセスや潜在的な侵害から保護するための厳格な IAM プラクティスを確立し、維持することが極めて重要です。

以下に、サーバーレスアーキテクチャの IAM ベストプラクティスをいくつか示します。

- **最小特権アクセス:** サーバレスコンピューティングでは、最小特権の原則を実装する必要があります。これは、ファンクションの操作に必要な最小限のアクセスレベル、つまり権限を与えることを意味します。これらの権限を定期的に更新することで、ファンクションに不必要なアクセス

権を与えないようにします。これにより、機密性の高いシステムやデータが脅威にさらされることがなくなります。

- **きめ細かなアクセス制御：** 事前定義されたロールに基づいてアクセスを制御する RBAC に加えて、サーバーレス環境ではきめ細かなアクセス制御のメリットが得られます。このアプローチにより、個々の機能やリソースのレベルで権限を正確に指定できるようになり、特権アクセスを最小限に抑え、アタックサーフェスを減らすことができます。
- **コンテキストを考慮した認可：** サーバーレスアーキテクチャは、従来の RBAC を超えて、コンテキストを考慮した認可に向いています。ユーザーアイデンティティ、デバイス特性、アクセス時刻、環境要因などのコンテキスト属性は、アクセスの決定に動的に影響を与える可能性があります。コンテキストを考慮したポリシーを実装すると、リアルタイムの状況に基づいてアクセス制御が適応されるため、セキュリティが強化されます。
- **イミュータブルインフラストラクチャとシークレット管理：** サーバレスファンクションはステートレスでエフェメラルです。ベストプラクティスには、CSP が提供するシークレット管理サービスの活用、クレデンシャルの定期的なローテーション、クレデンシャルの漏洩リスクを軽減するイミュータブルインフラストラクチャの原則の採用などがあります。
- **IAM ポリシーのレビューと更新：** IAM ポリシーを定期的に見直して更新し、権限が現在の要件に合っていることを確認することも重要です。サーバーレスアプリケーションの進化に伴い、アクセスニーズも高まっています。これらのポリシーを定期的に監査することで、権限が緩すぎず、不必要に厳格にならないようにし、運用効率とセキュリティのバランスを取ることができます。

サーバーレスファンクションのセキュリティを確保しようとするチームにとって、これらの IAM ベストプラクティスを採用し、Security Production Identity Framework For Everyone（SPIFFE）や SPIFFE Runtime Environment (SPIRE)[136]のような新しい業界ソリューションに目を光らせることは不可欠です。これらのソリューションは、複数のプラットフォームやドメインにわたって安全に拡張できる、セキュアで管理しやすく信頼性の高いサーバーレス環境を構築します。

8.5.3 ネットワーク接続とアクセスパターン

ネットワーク設計は、サーバーレスアーキテクチャのセキュリティに不可欠な役割を果たします。仮想ネットワーク内でサーバーレスファンクションを分離することで、不正アクセスのリスクを軽減し、セキュリティを強化します。ACL などのきめ細かいアクセス制御を設定することで、これらのファンクションに誰が、どのような条件でアクセスできるかを定義できます。

サーバーレスファンクションと他のサービスとの相互作用のセキュリティも不可欠です。API ゲートウェイは、多くの場合、受信要求のエントリポイントであり、厳重にセキュアにする必要があります。API ゲートウェイの堅牢性確保に加え、通信データの暗号化も重要です。ネットワークセキュリティは主に CSP の管理下にありますが、CSC はアプリケーションレイヤのデータ移動を保護するセキュリティ設定を構成する必要があります。

[136] SPIFFE. (2024) SPIFFE is a set of open-source standards for securely identifying software systems in dynamic and heterogeneous environments. SPIRE is a production-ready implementation of the SPIFFE APIs.

8.5.4 環境変数とシークレット

サーバレスアプリケーション内での機微情報の取り扱いには、慎重な検討が必要です。パスワードや API 鍵などのシークレットをコードにハードコーディングするのではなく、環境変数[137]を利用する必要があります。これらの変数を動的に管理し、実行時に注入できるため、機微情報の漏えいを最小限に抑えることができます。

AWS Secrets Manager や Azure Key Vault などのクラウドサービスは、シークレット管理のための信頼性の高いメカニズムを提供し、クレデンシャルのセキュアな保存、取得、およびローテーションを可能にします。これらのシークレットを定期的にローテーションすることで、古い、侵害される可能性のあるクレデンシャルがエクスプロイトされるリスクを軽減できます。さらに、IAM ロールを介してこれらのシークレットへのアクセスを制御することで、許可されたエンティティのみがそれらのシークレットを取得または変更できることが保証されます。

これらの手法を採用することで、ネットワーク接続や機微データをセキュアかつ効率的に管理するサーバレス環境を構築できます。これにより、サーバーレスアプリケーションの完全性と機密性を維持し、信頼は決して仮定されず、継続的に検証する必要があるゼロトラストセキュリティモデルに準拠します。

8.6 AI ワークロード

AI は技術の進歩の最前線に立ち、私たちの暮らしや働き方、および関わり方を変革します。AI ワークロードとは、AI 機能の構築、提供、または活用に関わる、タスク、プロセス、または運用を指します。これらのワークロードにより、意思決定プロセスにおいて、マシンはデータから学習し、予測を行い、また、人間の知能をシミュレートすることができます。ユーザーの行動に基づいた製品の推奨から、自動車の自律運転まで、AI ワークロードは幅広い複雑さとアプリケーションを包含します。

AI ワークロードの特徴は、大量のデータ要件と計算の複雑さです。モデルのトレーニングには大規模なデータセットと相当な処理能力が必要で、グラフィックス処理装置（GPU）やテンソル処理装置（TPU）のような専用ハードウェアを活用して効率化を図ります。さらに、これらのワークロードは変動する需要に応じて動的に拡張する必要があり、クラウド環境によって提供されるリソースなど、柔軟なコンピューティングリソースの重要性が強調されています。

AI ワークロードのアプリケーションは膨大で多様です。タスクの自動化、カスタマーエクスペリエンスの強化、および複雑な問題に対する前例のない洞察を提供することで、業界を再編します。AI 技術が進化するにつれ、AI の可能性を最大限に活用しようとする組織にとって、これらのワークロードを理解し、管理することが非常に重要になります。AI ワークロードへの取り組みは、単に計算能力を活用する

[137] Environment variabilities are dynamic values that are used to configure application settings, manage secrets, and control behavior without altering the source code, allowing for easier deployment and environment-specific customization.

だけでなく、データ、アルゴリズム、およびリアルタイム処理の複雑さをナビゲートし、さまざまなセクターでイノベーションと価値を引き出すことにもつながります。

8.6.1 AI システムの脅威

AI インフラのセキュリティは、侵害された場合の潜在的な影響から重大な懸念事項となります。このインフラストラクチャには複数のコンポーネントがあり、それぞれに固有の課題があり、カスタマイズしたセキュリティ対策が必要です。具体的な脅威を理解し、適切な軽減戦略を実施することで、AI システムの完全性、機密性、および可用性を確保できます。

以下に、主要な AI システムの脅威をカテゴリ別にグループ化します。

データセキュリティに関する脅威:

- *データポイズニング：*データポイズニングとは、悪意を持って誤った情報が導入され、不正確なモデル出力につながることを指します。
- *プライバシー侵害:* 機微データへの不正アクセスは、プライバシー侵害や関連する法的問題につながる可能性があります。
- *データ漏えい：* モデル出力を通じて学習データを誤って暴露すると、機微情報を漏洩する危険性があります。

モデルセキュリティに関する脅威:

- *モデル盗難：*機械学習モデルの不正コピー。これにより、攻撃者は知的財産法を迂回することができ、モデルを騙す方法も明らかになり、リスクが複雑化する可能性があります。
- *敵対的攻撃：* 入力を操作して設計上の弱点をエクスプロイトし、誤った予測を引き起こす可能性があります。
- *学習データを復元する攻撃：*この攻撃は、モデル出力から入力データを再構築し、学習データの機密性を脅かす可能性があります。
- *プロンプトインジェクション：* 悪意を持って細工された入力は、AI モデルの脆弱性をエクスプロイトして意図しないアクションを引き起こしたり、機微情報を暴露したりする可能性があります。これは、ソーシャルエンジニアリングが個人をだましてセキュリティを危険にさらすのと同様です。

インフラストラクチャセキュリティの脅威:

- *不正アクセス:* AI インフラストラクチャへの侵入は、データの盗難や悪意のある改ざん、有害なソフトウェアの導入につながる可能性があります。
- *DDoS 攻撃：* 過剰なトラフィックによってサービスが中断される可能性があります。

- *ハードウェアの脆弱性：* GPU や TPU を狙ったエクスプロイトにはサイドチャネル攻撃が含まれ、機微情報が漏えいする危険性があります。

サプライチェーンの脅威:

- *ソフトウェアの依存関係：* サードパーティのライブラリが脆弱性や悪意のあるコードをもたらす可能性があります。
- *サードパーティサービス：* 外部のデータ処理やストレージサービスに依存すると、脆弱性をもたらす可能性があります。

8.6.2 AI 軽減戦略

以下は、主要な AI システムの移行戦略をカテゴリごとにまとめたものです。

データセキュリティ:

- *暗号化:* 移動中および保存中のデータの機密性を保護します。
- *差分プライバシー:* データやクエリにランダム性を導入し、個々のレコードが人物まで追跡できないようにします。会話にノイズを加えて、プライベートな詳細をマスクするようなものです。
- *秘匿マルチパーティ計算：* 機微情報をフローの一部として匿名化またはトークン化することにより、機微情報を公開することなく、複数のソースからのデータを処理します。
- *コンフィデンシャルコンピューティング:* Trusted Execution Environments[138]を使用して、処理中のデータを保護し、AI モデルの実行を保護します。

モデルセキュリティ:

- *モデルのハードニング:* モデルのレジリエンスを強化するために、敵対的攻撃から防御します。
- *堅牢なトレーニング:*一般化可能性を高め、過剰適合を減らす技法[139]を採用します。
- *敵対的トレーニング：* AI モデルのトレーニングデータに操作済みの事例を組み込むことで、攻撃に対する AI モデルのレジリエンスを強化します。
- *モデルの透かし：*固有の識別子を埋め込んで所有権を主張し、盗難を抑止します。
- *アウトプット操作：* AI の応答を変更して意思決定プロセスを不明瞭にすると、ポーカープレイヤーのハッタリのように、潜在的な窃盗犯を阻止できます。

インフラストラクチャセキュリティ:

[138] TEEs are secure areas within a processor that ensure code and data loaded inside are protected with confidentiality and integrity, providing a safe execution environment resistant to software and hardware attacks.
[139] A scenario where a machine learning model learns the training data too well, including noise and outliers, resulting in poor generalization to new, unseen data, and potentially making the model vulnerable to adversarial attacks.

- *GPU と TPU:* システムの完全性を維持するには、ハードウェアベースのセキュリティ機能、定期的なファームウェアアップデート、およびネットワークセキュリティ対策を利用します。

- *AI サービス：* アクセス制御やリアルタイム監視など、クラウドサービスのベストプラクティスに従います。
- *クォータとレート制限：* クォータとレート制限を適用して、DoS および DDoS 攻撃を特定して防止します。

サプライチェーンのセキュリティ:

- ポリシー：サプライチェーンのサイバーセキュリティポリシーを定義し、承認します。
- *ソフトウェアサプライチェーンリスク管理：* サードパーティの依存関係を定期的に監査し、更新します。
- *サードパーティサービスの精査:* 統合前にセキュリティ評価を実施します。
- *信頼できるソース:* ソフトウェアの依存関係を信頼できるソースに任せ、承認リストを維持します。

このような脅威に対して積極的に対処することで、企業は AI インフラストラクチャを現在の脅威や新たな脅威に対して強化し、AI システムのレジリエンスを確実にします。[140]

サマリ

クラウドワークロード保護は、クラウド環境の多様で動的な性質に見られる固有のセキュリティ課題に対処する、進化する学問分野です。クラウドでは、従来のセキュリティ対策では不十分です。そのため、さまざまなワークロードを効果的に保護するには、専門的な管理が必要です。

VM の場合、セキュリティはイメージレベルから始まります。VM イメージのセキュリティ自動化により、配備サイクルの早い段階で保護を組み込むことができます。最小特権の原則の徹底や定期的な脆弱性評価の優先順位付けなどの慣行は、脅威に対する堅牢な防御を維持するための基礎となります。

Kubernetes によるコンテナオーケストレーションでは、セキュリティを強化するために構成をカスタマイズすることが重要です。コンテナイメージの脆弱性をスキャンし、これらのイメージにアクセスして管理する権限を持つユーザーを制御することは、極めて重要な手段です。さらに、ランタイム保護メカニズムを実装することで、コンテナを継続的に監視し、継続的な脅威から保護します。

サーバーレスアプリケーションは、厳格な IAM ポリシーから始まり、セキュリティに焦点を当てたアプローチを必要とします。API エンドポイントを不正アクセスから保護し、機微情報を厳重に管理することがエクスプロイトを防ぐ鍵となります。

---

[140] MITRE. (2024) *Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS)* is a globally accessible, living knowledge base of adversary tactics and techniques against AI-enabled systems. It is based on real-world attack observations and realistic demonstrations from AI red teams and security groups and can help in the safeguarding of AI infrastructures.

AI ワークロードセキュリティの分野は特にペースが速く、継続的な学習が必要です。AI ワークロードをセキュリティ侵害から守るには、敵対的トレーニングを取り入れ、AI モデルを不正アクセスや盗難から保護し、差分プライバシーなどのデータプライバシー技術を採用することが不可欠です。

PaaS 環境では、脆弱性を特定して修正するために定期的なセキュリティ監査が必要です。厳格な IAM 制御とセキュアな通信チャネルとともに、保存中および移動中のデータの暗号化が基盤となります。

クラウドのワークロード保護は、汎用的なソリューションではなく、各ワークロードタイプの特性に合わせてカスタマイズされるアプローチです。セキュアなクラウドエコシステムを維持するためには、最新の脅威と軽減戦略を常に把握することが不可欠です。

推奨事項

クラウドワークロード管理

- 一元化されたクラウド配備レジストリの作成: すべてのクラウドワークロードと配備の包括的なインベントリを維持し、効率的な追跡と管理を実現します。
- 複数のデプロイメントを使用する組織階層の定義: クラウド環境を組織単位で構成し、セキュリティと管理制御を強化します。
- 新しいデプロイメントを作成するための摩擦の少ないプロセスをサポート: プロセスを合理化し、業務効率を妨げずにセキュリティポリシーを遵守できるようにします。

仮想マシン(VM)のセキュリティ

- セキュアなベース VM イメージの適用: すべての配備で、一元管理、バージョン管理、およびイミュータブルベースイメージを使用します。
- イメージファクトリを実装する:VM イメージの作成、テスト、および配備を自動化して、一貫性とセキュリティを確保します。
- VM イメージの脆弱性をスキャン： VM イメージを定期的にスキャンして更新し、セキュリティリスクを軽減します。
- 短期実行仮想マシンの採用: イミュータブルインフラストラクチャとエフェメラル VM を使用して、長時間実行されるインスタンスに関連するリスクを軽減します。
- 構成管理と Infrastructure as Code (IaC)の使用: 望ましい状態を維持し、設定のずれを防ぎます。
- ホストベースのファイアウォールと SSH 強化を実装: VM インスタンスでネットワークアクセスを制御し、SSH 構成をセキュアにします。

コンテナオーケストレーションセキュリティ

- CSP サービスを使用してオーケストレーション: Kubernetes-as-a-Service などのマネージドサービスを活用してセキュリティを強化します。
- オーケストレーションサービスのハードニング: 不要な機能を無効にし、最小特権アクセスを確保し、ネットワークポリシーとファイアウォールを実装します。
- 定期的なパッチ適用とアップデート： コンテナ、ホスト、およびオーケストレーションプラットフォームのパッチ管理を自動化します。
- セキュリティポリシーの定義と適用： Kubernetes セキュリティポリシー、PodSecurityPolicy、ネットワークポリシーなどのツールを使用します。
- セキュリティベンチマークとツールを活用: Kubernetes の CIS ベンチマークに従って、セキュアな構成を確実にします。
- クラスタホストとストレージの保護： ホストの OS をハードニングし、保存中データと移動中データの暗号化を適用し、アクセス制御リスト（ACL）を使用します。

モニタリングと評価

- CSPM ツールの利用: Cloud Security Posture Management（CSPM）ツールを使用して、クラウドのセキュリティポスチャを継続的に監視します。
- 継続的なモニタリングを実施： リアルタイム監視ツールを使用してワークロードアクティビティを追跡し、潜在的なセキュリティインシデントをすばやく検出します。
- SCA ツールを使用: ソフトウェア組成分析（SCA）ツールを CI/CD パイプラインに統合し、依存関係を管理し、脆弱性を早期に特定します。
- SBOM の生成とメンテナンス: すべてのワークロードに対応するソフトウェア部品表（SBOM）を作成し、透明性、セキュリティ対応、および法令順守を強化します。
- Endpoint Detection and Response（EDR）エージェント： ランタイム監視を実行し、脆弱性評価をサポートします。
- Security Information and Event Management（SIEM）： リアルタイムのモニタリングとレポートを提供します。

トレーニングと意識向上

- 定期的にセキュリティ演習を実施: シナリオベースの演習と机上訓練を行い、チームを実際のインシデントに備えます。
- Just Culture アプローチを奨励: セキュリティインシデントに関する過度な責任を負わせることなく、システム全体の改善と説明責任に注力します。

PaaS セキュリティ

- 定期的なセキュリティ監査： 脆弱性アセスメントを実施し、潜在的な脅威を特定して軽減します。
- 包括的なロギングとモニタリング： ロギングとリアルタイムモニタリングを実装し、疑わしい動作を検出して対応します。
- 最小特権の原則： 必要最小限のアクセスレベルのみをユーザーとサービスに付与します。

- 多要素認証(MFA)：MFA でアクセス制御を強化します。
- 定期的なアクセスレビュー：アクセス権限を定期的に再評価し、適切なアクセスレベルを確保します。

サーバーレスまたは Function as a Service のセキュア化

- サードパーティサービスと API の精査: 未認可な設定やデータの露出を防ぐため、セキュリティと信頼性を確保します。
- 脆弱な依存関係の管理: 外部ライブラリの脆弱性や悪意のあるコードを定期的にチェックし、更新します。
- 設定ミスの修正: セキュリティ設定による適切なファンクションの実行とアクセスの制限を確実にします。
- 関数の IAM 権限を制限： 不正アクセスやデータ漏洩のリスクを低減するために必要最小限の権限を付与します。
- インターネットへの直接アクセスの制御：ネットワークセグメンテーションと ACL を実装して、ファンクションがインターネットに直接アクセスできないようにします。

AI 軽減戦略

- データセキュリティ: 暗号化、差分プライバシー、秘匿マルチパーティ計算を使用してデータを保護します。
- モデルセキュリティ: モデルを攻撃者の攻撃から強化し、堅牢なトレーニング手法を使用し、一意の識別子を埋め込んで盗難を抑止します。
- インフラストラクチャセキュリティ: クォータとレート制限を実装し、クラウドサービスのベストプラクティスに従います。
- サプライチェーンのセキュリティ： サイバーセキュリティポリシーを定義し、サードパーティの依存関係を定期的に監査し、信頼できるソースを使用します。

追加のガイダンス

- Cloud Industrial Internet of Things (IIoT) - Industrial Control Systems Security Glossary | CSA
- Best Practices in Implementing a Secure Microservices Architecture | CSA
- Cloud Adversarial Vectors, Exploits, and Threats (CAVEaT™): An Emerging Threat Matrix for Industry Collaboration | CSA
- Integrating SDP and DNS: Enhanced Zero Trust Policy Enforcement | CSA
- Ransomware in the Healthcare Cloud | CSA
- Cloud Security Complexity | CSA
- The 12 Most Critical Risks for Serverless Applications | CSA

ドメイン 9: データセキュリティ

はじめに

クラウドサービスの急速な拡大と適応、サイバー脅威の巧妙化により、情報保護のためのレジリエントなアプローチが求められています。データセキュリティの実践は、組織の完全性、機密性、および利用者の信頼を維持しながら、規制要件の遵守を確実にするために重要です。

このドメインでは、クラウド内のデータセキュリティの複雑さについて掘り下げ、データが移動中および保存中に確実に保護されるために組織が採用できる重要な戦略、ツール、およびプラクティスを検討します。データの分類とクラウドストレージの種類に関するニュアンスの理解から、高度な暗号化方式とアクセス制御の実装まで、このセクションでは、進化し続けるデータセキュリティのランドスケープをナビゲートするためのガイドを提供します。このドメインはクラウドストレージの入門書でもあります。さらに、クラウド環境でデータを保護する方法の未来を形作る主要な概念と技術について考察し、データ漏洩を防ぎ、データプライバシーを維持するために必要な重要な対策に関する読者の理解を確実にします。

学習目標

このドメインの学習目標は、読者に以下の知識を提供することです。

- データセキュリティの基礎の理解。
- データの分類と状態。
- クラウドストレージの種類と関連するセキュリティ対策。
- 鍵管理などのデータセキュリティ技法。
- さまざまなタイプのコンピューティングワークロードの保護。
- ポスチャ管理。
- 高度なデータセキュリティの概念。

9.1 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。データの不適切な取り扱いは、データ漏洩、コンプライアンス違反、およびデータ損失につながる可能性があります。戦略の観点から見ると、データ分類のプラク

ティスを理解し実装することで、組織は運用戦略とコンプライアンス戦略を整合させることができます。

組織のニーズと規制の状況が進化するにつれて、データ分類を適応させ、データガバナンスの取り組みの効果を確実にし、またインシデントに対応し続ける必要があります。さらに、保存中、移動中、および使用中といった異なるデータ状態を認識するには、カスタマイズされたセキュリティ対策が必要です。これと相まって、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、 Software as a Service（SaaS）ストレージ、PaaS 専用ストレージなど、さまざまなクラウドストレージタイプを把握することで、組織固有のデータニーズやセキュリティ要件に最適なソリューションを選択できるようになります。

9.1.1 データ分類

データ分類は、運用面とコンプライアンス面の両方を考慮し、タイプ、機密性、重要度、およびデータ漏洩による潜在的な影響に基づいてデータを分類する、極めて重要な継続的なプロセスです。組織のデータガバナンスプラクティスにデータ分類プロセスを組み込むことは、データライフサイクル全体を保護するために不可欠です。堅牢なデータ分類アプローチは、資産保護の優先順位を明確に把握することで、データ漏洩のリスクへの対処と軽減に役立ちます。本質的に、データ分類は運用上のセキュリティとコンプライアンス戦略の定義を促進します。

組織が進化するにつれて事業環境が変化し、また、新しい法規制が組織の活動要件に影響を与えます。堅牢なデータ分類戦略と明確な資産およびデータ所有権の割り当てを組み合わせることで、組織はインシデントに迅速に対応し、多様なデータガバナンスの取り組みを成功裏に推進できます。

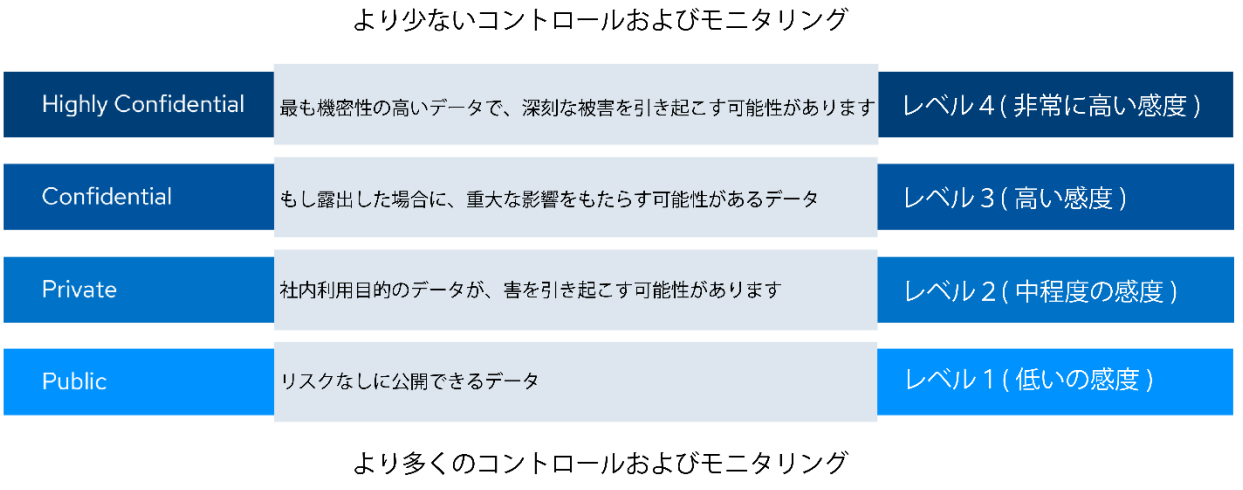


図 48: データ分類のスケール

9.1.2 データの状態

クラウドセキュリティのコンテキストでは、データがさまざまな状態を継続的に遷移し、それぞれの状態が特定のセキュリティ対策を必要とすることを認識しておくことが不可欠です。このディスカッションでは、保存中データ(ストレージ内)、移動中データ、および使用中データの 3 つの主要なデータ状態について説明します。

保存中データとは、クラウド環境内にさまざまな形式で保存されているデータに関するものです。これには、仮想ディスク、オブジェクトストレージ内のファイルのようなオブジェクト、データベース、platform as a service （PaaS）製品など、ボリュームに保持されているデータが網羅されます。ストレージ内のデータの効果的なセキュリティ対策には、通常、暗号化、アクセス制御の確立、およびデータの完全性を保護するための定期的なバックアップの維持が含まれます。

移動中データとは、拠点間で活発に送信または転送されているデータを指します。この移動は、内部ネットワーク内、インターネット全体、または USB ドライブや外付けハードドライブなどの物理メディアを介して行われます。移動中のデータを保護するには、暗号化プロトコルの使用、通信チャネルの確保、および移動中のデータの完全性と機密性の確保が不可欠です。

使用中データとは、アプリケーションまたはサービスによって現在処理、操作、または相互作用が行われているデータです。これには、アプリケーションが利用するデータ、AI の学習や推論に関わるデータ、分析処理を受けるデータなどが含まれます。使用中のデータのセキュリティ対策には、厳格なアクセス制御の実施、ユーザーアクティビティのモニタリング、処理中のデータの完全性と機密性の保護などがあります。

データのセキュリティは、あらゆるレベルと状態で守られなければならないことを理解することが重要です。データは保存中、移動中、および使用中の間を移行するため、データのライフサイクル全体にわたって保護するには、カスタマイズされたセキュリティ対策が不可欠です。さまざまなデータの状態を把握し、各段階でターゲットを絞ったセキュリティ管理を適用することで、組織はクラウドセキュリティに包括的なアプローチを採用できるため、機微データを不正アクセス、改ざん、または漏洩から保護できます。

9.1.3 クラウドストレージの種類

さまざまなタイプのクラウドストレージを理解することで、特定のデータニーズに最適なストレージソリューションを特定できます。

クラウドストレージには、次のような種類があります。

- 大量の非構造化データのオブジェクトストレージ
- 仮想ハードドライブと同様の低レイテンシアクセスを実現するボリュームストレージ
- リレーショナルデータと非リレーショナルデータを管理するためのデータベースストレージ
- PaaS および SaaS 環境で使用されるその他の専用ストレージタイプ

各カテゴリには、独自の特性、ユースケース、および主要なクラウドプロバイダの製品があります。

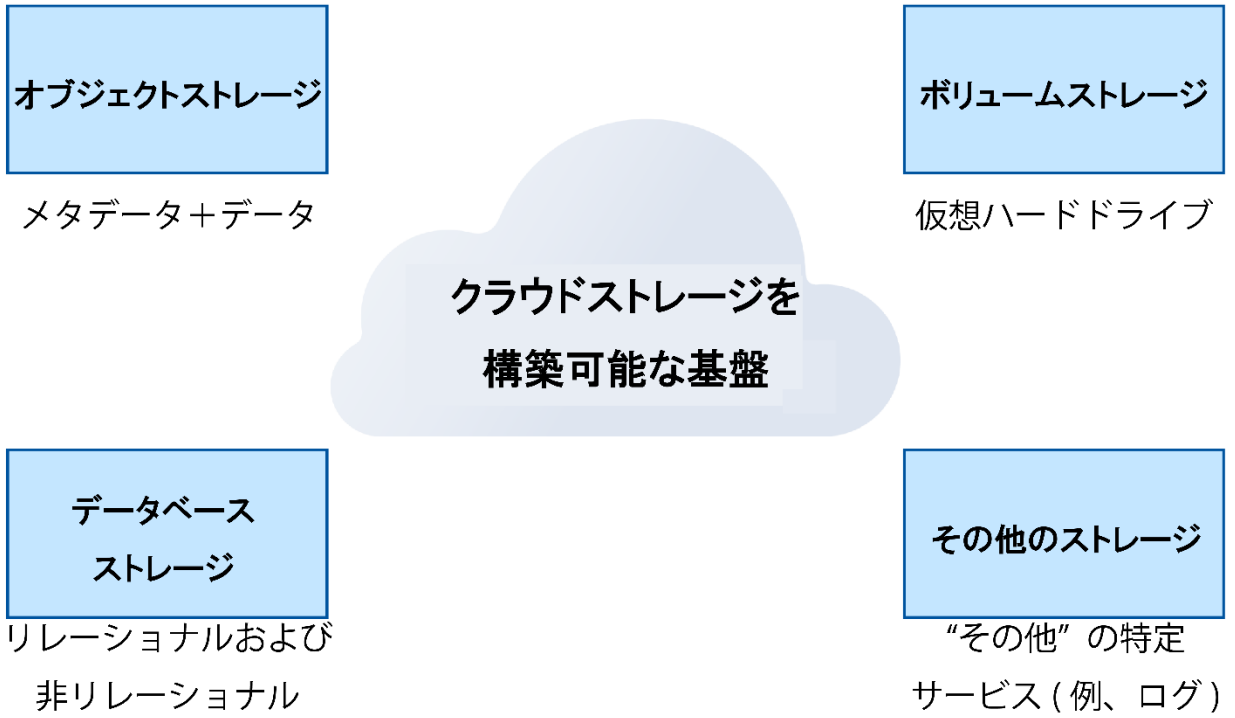


図 49: クラウドストレージソリューションの種類

9.1.3.1 オブジェクトストレージ

オブジェクトストレージは、ドキュメント、イメージ、ビデオ、およびバックアップなど、大量の非構造化データを格納および取得するように設計されています。一意の鍵で識別されるオブジェクトを格納およびアクセスするためのシンプルなアプリケーションプログラミングインターフェイス (API) を提供します。オブジェクトストレージは拡張性と耐久性に優れており、バックアップ、アーカイブ、静的ウェブサイトコンテンツの提供など、さまざまなユースケースに適しています。これらの種類のストレージは、クラウドプロバイダがストレージインフラストラクチャを提供するため、 infrastructure as a service（IaaS）サービスに分類されます。オブジェクトストレージサービスの例としては、Amazon S3、Google Cloud Storage、Azure Blob Storage などがあります。

9.1.3.2 ボリュームストレージ

ボリュームストレージは、クラウド内の仮想マシンに接続できる仮想ハードドライブを提供します。これにより、従来のハードドライブと同様の方法でデータを保存およびアクセスできます。ボリュームストレージは通常、オペレーティングシステムファイル、アプリケーションデータ、および低レイテンシのアクセスを必要とするその他の永続データに使用されます。オブジェクトストレージとは用途が異なりますが、このカテゴリーのストレージも IaaS サービスとみなされます。クラウドプロバイダは、

Amazon Elastic Block Store（EBS）、Google Persistent Disk、Azure Managed Disks など、さまざまなタイプのボリュームストレージを提供しており、パフォーマンス特性や価格オプションもさまざまです。

9.1.3.3 データベースストレージ

これにはリレーショナルデータベースと非リレーショナルデータベースの両方が含まれます。クラウドプロバイダは、Amazon Relational Database Service、Google Cloud Structured Query Language（SQL）、Microsoft Azure SQL Database、Oracle Database サービスなどのリレーショナルデータベースのマネージドサービスを提供しています。これらのサービスは、MySQL、Oracle、PostgreSQL、SQL Server などの使い慣れたデータベースエンジンを提供します。NoSQL データベースとも呼ばれる非リレーショナルデータベースは、スケーラビリティと柔軟性を考慮して設計されています。たとえば、Amazon DynamoDB、Google Cloud Datastore、Oracle NoSQL Cloud DB、Azure Cosmos DB などです。これらのデータベースは拡張性が高く、大量の非構造化データを処理できます。

9.1.3.4 その他のストレージの種類

PaaS ストレージとは、クラウドプラットフォームのさまざまなサービス固有のストレージオプションを指します。これには、Amazon CloudWatch、Google Cloud Logging、Oracle Events、Azure Monitor などのロギングサービスが含まれ、アプリケーションやインフラストラクチャからのログデータを保存および分析できます。メッセージキューは、Amazon Simple Queue Service（SQS）、Google Cloud Pub/Sub、Azure Queue Storage などの分散アプリケーションコンポーネント間の信頼性の高い通信を可能にします。Oracle Cloud Infrastructure (OCI) Streaming やその他の PaaS ストレージサービスには、キャッシュ、インメモリデータベースなどが含まれる場合があります。クラウドストレージは、Google ドライブ、Dropbox、Microsoft OneDrive、Box などの SaaS（Software as a Service）としても提供される可能性があります。これらのサービスにより、ユーザーはファイルやリソースへのセキュアなアクセスと共有が可能になり、インターネット上での強固なコラボレーションが可能になります。

9.2 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タイプごとに、固有のセキュリティニーズと課題があります。これらのバリエーションに効果的に対処するには、さまざまなツールと技法が必要です。このセクションでは、クラウド内のデータストレージを保護する中核となる必須のデータセキュリティツールについて説明します。これには、アクセスを管理するアイデンティティおよびアクセス管理（IAM）システム、権限とネットワークルールを定義するアクセスポリシー、データの完全性と機密性を保護する暗号化と鍵管理などがあります。さらに、マスキング、トークン化、匿名化などの技法は、データ損失防止（DLP）や data security posture management（DSPM）ツールとともに、堅牢なデータセキュリティを確保するために

重要な役割を果たします。これらの対策を実施することで、組織はクラウドデータの保存と処理に関連するリスクを効果的に管理し、軽減することができます。

9.2.1 データセキュリティツールと技法

技術的には、すべての情報セキュリティはデータセキュリティですが、これらのツールは、データストレージ自体のセキュリティに集中するためのコアツールキットを形成しています。これらの各ツールの詳細については、このドメインの残りの部分で説明します。

- **アイデンティティとアクセスの管理 (IAM[141])**: IAM システムは、API 呼び出しを行ったり、プラットフォーム内のユーザーとデータが存在するサービス内で作業したりする際に、クラウド環境内の特定のリソースへのエンティティのアクセスを管理します。これは、外部アクセスも管理できるアクセス制御とは異なります。例えば IaaS や PaaS では、ユーザーベースの IAM ポリシーやストレージに付加されたリソースポリシーでアクセスを管理できます。

- **アクセスポリシー**：アクセスポリシーはリソースアクセスを管理します。これらは、特定のリソースに対するアクセスと許可されるアクション（つまり権限）を定義し、リソース間のトラフィックフローを制御するネットワークルールを決定します。リソースポリシーとネットワークポリシーの両方がセキュリティ境界の適用に役立ちます。

- **暗号化と鍵管理：** 暗号化は、データを判読できない暗号文に変換することでデータを保護します。この暗号文は、適切な復号鍵を持つ者だけが復号できます。鍵管理システムは、これらの暗号化鍵をセキュアに保管および管理し、クラウドインフラストラクチャ内または外部の鍵管理サーバーのいずれかで、クラウドサービスプロバイダ（CSP）から分離された状態に保ちます。この組み合わせたアプローチにより、クラウド環境内のデータの機密性と完全性が確保されます。

- **マスキング:** 形式と長さを保持したまま、機微データを架空または部分的に不明瞭な値に置き換える技法です。たとえば、クレジットカード番号の下 4 桁だけを表示したり、テスト環境用に偽の PII（個人識別情報）データを作成したりします。
- **トークン化**：参照整合性とセキュリティを維持しながら、機微データを一意の識別子（トークン）に置き換えるプロセスです。トークンを元のデータ値に戻すには、元のデータと関連するトークンを格納する別のデータベースが必要です。
- **匿名化**:データセットから PII を削除し、個人を識別不能にするプロセスです。通常、匿名化手法は不可逆なため、元のデータに復元することはできません。
- **情報漏えい対策(DLP): DLP** とは、知的財産や顧客情報などの重要データを保護するためのポリシーを適用し、企業から意図しない第三者に流出しないようにするシステムを指します。DLP ソリューションは、クラウド環境に保存されたデータを含む機密データの識別、監視、および保護に役立ちます。これらのソリューションは、機微情報の検出と分類、セキュリティポリシーの適用、および不正なデータの共有や持ち出しの防止が可能です。
- **Data Security Posture Management (DSPM)**: DSPM ツールは、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。セキュリティイベント、設定ミス、およびコンプライアンスの課題を可視化し、組織がセキュリティギャップをプロアクティブに特定して対処できるようにし、リスク管理をサポートします。

[141] IAM is covered in detail in *Domain 5: Identity and Access Management*.

9.2.2 アクセス制御とポリシー

クラウドコンピューティングでは、アクセスの管理は、セキュリティと運用の完全性を確保するための基礎となります。IAM やロールベースアクセス制御（RBAC）などのフレームワークを通じて実装されるアクセス制御とポリシーは、多様なクラウドサービスにわたってユーザー権限を定義し、適用します。これらのメカニズムは、API と非 API の相互作用を含むさまざまなアクセス方法を処理し、リソースレベルのポリシーによってオーバーライドされる可能性がある場合でも、一貫した権限が適用されるようにします。アクセスポリシーは、リソースに対して許可されるアクションの明確なルールを設定し、クラウド内でのネットワークのやり取りを管理することで、これらのコントロールをさらにサポートします。このセクションでは、これらのメカニズムについて、実践的な例を示しながら、クラウドのセキュリティを維持する上での役割を説明します。[142]

9.2.2.1 アクセス制御

アクセス制御はクラウドセキュリティの重要な構成要素であり、通常は IAM や RBAC ポリシーのようなメカニズムを通じて、特定のユーザーに個別に適用されます。これらのコントロールは、API コール、非 API インタラクション、および CSP によって大きく異なる可能性のあるその他のアクセスアプローチの管理を確実にするなど、さまざまなアクセス方法を管理するために必要です。リソースベースのポリシーは、リソースが IAM ポリシーによって考慮されないチャネルを介してアクセスされた場合、ユーザーまたは IAM ポリシーの拒否を上書きする可能性があることに注意することが重要です。例えば、ユーザーはウェブインターフェースや API コールを伴わないアプリケーションを介してリソースにアクセスする可能性があります。

次の例を考えてみましょう。Amazon Web Services（AWS）の IAM ポリシーが作成され、「AppRead」ロールが「ApplicationData」S3 バケットとやり取りできるようになりました。このポリシーは JSON 形式を使用し、ポリシーのバージョン、ステートメント、効果（この場合は「許可」）、プリンシパル（「AppRead」ロールとなる）、アクション（具体的には「s3:GetObject」および「s3:ListBucket」パーミッション）、指定リソース（S3 バケット内の「ApplicationData/*」および「ApplicationData/」として識別）など、さまざまな側面について詳述します。

このシナリオでは、役割に正確な権限を割り当てるための IAM ポリシーの戦略的な使用を強調し、指定された S3 バケットとその内容へのアクセスを容易にします。クラウド内のリソースの完全性とセキュリティを維持するためには、綿密なアクセス制御の計画と実行が不可欠です。

9.2.2.2 アクセスポリシー

アクセスポリシーはリソースアクセスを管理します。これらは、特定のリソースに対するアクセスと許可されるアクション（つまり権限）を定義し、リソース間のトラフィックフローを制御するネットワー

[142] Details for risk assessment is provided in *Domain 5: Identity and Access Management*.

クルールを決定します。リソースポリシーとネットワークポリシーの両方がセキュリティ境界の適用に役立ちます。

リソースポリシーは、オブジェクトストレージなどの特定のリソースに直接アタッチされたルールセットとして機能し、API 呼び出しとは無関係に、たとえば HTTP を介してリソースにアクセスできるようにします。これらのポリシーは、CSP が IAM ユーザーグループに含まれていないエンティティのリソースへのアクセスを容易にするシナリオでは不可欠です。さらに、多くの場合、ネットワークルールをカプセル化し、IP アドレスに基づく制限を課すことができます。

これらのリソースポリシーは、以前の構成で確立されたアクセス制御やアイデンティティベースのポリシーよりも優先される可能性があることを理解することが重要です。たとえば、アイデンティティベースのポリシーでロールがリソースにアクセスすることを事前に禁止していた場合、クラウドプロバイダは通常、直接アクセスのシナリオに関してはアイデンティティポリシーよりもリソースポリシーの評価を優先するため、リソース ポリシーでアクセスを許可できます。このメカニズムは、アクセスの柔軟性を維持しながら、クラウドプラットフォームにセキュリティパラメータを適用する上で非常に重要です。

ネットワークポリシーは、ネットワーク上のデータフローを管理する一連のルールであり、Microsoft Azure など、そのネットワーク内のリソースに直接適用することもできます。主に、IP アドレスまたは指定された IP 範囲によるアクセスの管理に使用され、ネットワークリソースとやり取りできるユーザーまたはできないユーザーを決定する通信の境界を確立します。

例として、外部の AWS アカウントからロールを許可し、特定の承認済み IP アドレスからのアクセス権限を付与するように設計されている S3 バケットに適用されるリソースポリシーを考えてみます。このポリシーは JSON 形式で明示され、ポリシーのバージョン、詳細ステートメント、および「許可」するであろう効果などの要素を指定します。ここでのプリンシパルは、AWS アカウント ID と特定のロールの組み合わせになります。's3:GetObject'や's3:ListBucket'のようなアクションを定義し、S3 バケット内で 'ApplicationData / * 'や'ApplicationData / ' として識別されるリソースに適用します。このポリシーの重要な部分は、アクセスを許可する IP アドレスを指定する条件です。

この構成は、クラウド環境におけるリソースポリシーの柔軟性を例示しており、さまざまなアカウントからロールにアクセスを許可すると同時に、IP ベースの制限を実装してセキュリティを強化できます。リソースとネットワークの両方のポリシーを綿密に作成して実行し、組織が必要とする正確なレベルのアクセス制御とネットワークセキュリティを確保する必要があります。

9.2.3 クラウドデータの暗号化

以下の図は、クラウドでデータを暗号化できるさまざまなレイヤーを示しています。最下層のレイヤー(ボリュームまたはオブジェクト ストレージ)から始まり、アプリケーションレイヤーへと上がっていきます。暗号化レイヤーが上に行くほど、データのきめ細かい制御と保護が可能になりますが、実装と管理が複雑になります。データの機密性、コンプライアンス要件、パフォーマンスニーズ、および必要なコントロールと管理のレベルに基づいて、適切な暗号化レイヤーを選択する必要があります。

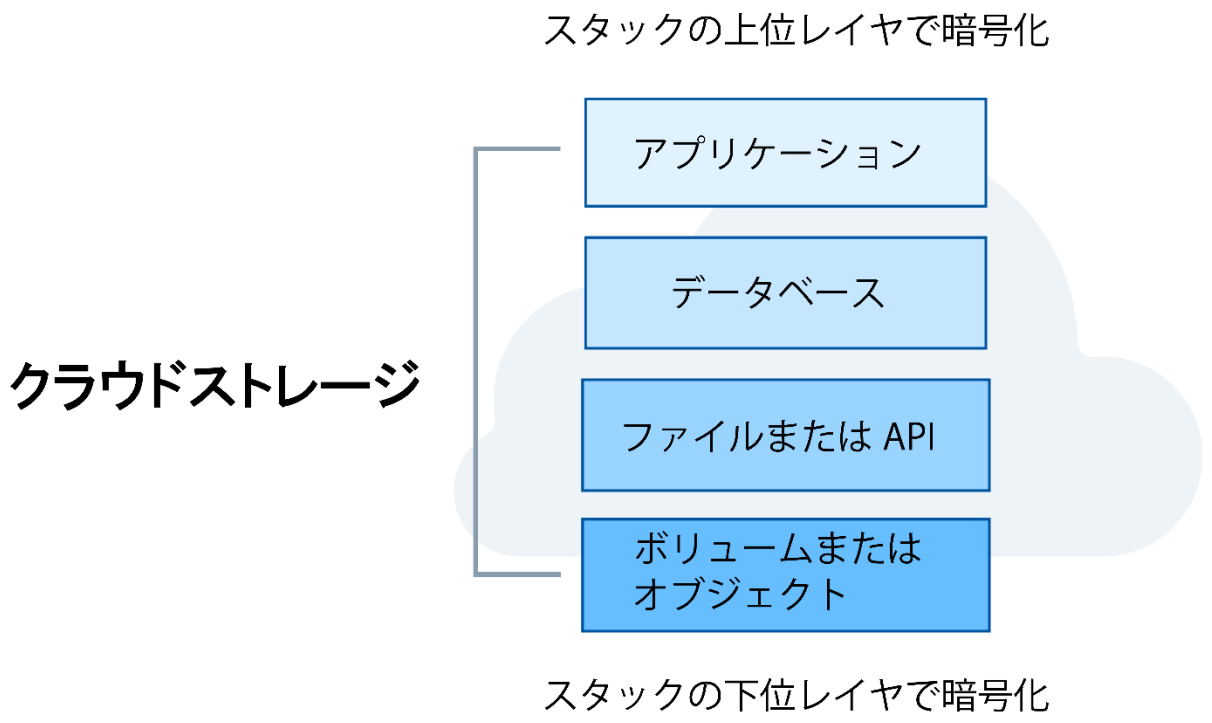


図 50: クラウドデータ暗号化レイヤー

アプリケーション
アプリケーションレイヤでデータを暗号化することで、ビジネスデータの保護とコントロールを実現します。アプリケーションは特定の機微データ要素を暗号化できるため、まさにその部分の保護を確実にします。しかし、アプリケーションレイヤの暗号化は、下位レイヤの暗号化と比較して、実装と管理により多くの労力を必要とします。

データベース
データベースレイヤでデータを暗号化することにより、データベースとそのバックアップ内のすべての情報が保護されます。暗号化方式により、どのデータを暗号化するかを詳細にコントロールでき、コンプライアンス要件への対応に役立ちます。

ファイル/API
ファイルや API レベルでの暗号化は、ボリュームやオブジェクトストレージの暗号化よりもきめ細かい保護を提供します。このレイヤーにより、API を通じてアクセスする特定のファイルやデータを暗号化できるため、よりターゲットを絞ったセキュリティが実現します。

ボリュームまたはオブジェクトストレージ
この最下層では、データは保存時に暗号化されます。このレベルの暗号化は、上位レイヤよりも管理が

容易で、パフォーマンスも優れています。ただし、暗号化はボリューム全体またはオブジェクトリポジトリに適用されるため、データの保護の細かさは劣ります。ボリューム暗号化は Total Disk Encryption の一形態であり、オブジェクトリポジトリ（バケットやストレージアカウントなど）は、そのリポジトリ内のすべてのオブジェクトを暗号化するように設定できます。通常、CSP はデフォルトですべてのストレージを暗号化しますが、利用者が自分で鍵を選択して管理できる場合もあります。これについては、このドキュメントの後半の「Bring Your Own Key」セクションで説明します。

9.2.3.1 クラウドデータ暗号化戦略

すべての暗号化システムは、次の 3 つの主要なコンポーネントで構成されています。

- 暗号化の対象となるデータ
- 暗号化エンジン(暗号化/復号を行うコンポーネント)
- 暗号化鍵

これらの機能コンポーネントは異なる場所に配置でき、これはクラウド暗号化の中核となる原則です。例えば、データはクラウドサービス内にあっても、保存する前に利用者によって暗号化され、その暗号化に使用する鍵は第 3 の場所に保管することができます（クライアントサイド暗号化の一種）。あるいは、利用者が鍵を保持し、実行時にプロバイダに提供して、データを CSP が暗号化することもできます（サーバーサイド暗号化の一形態）。最後に、鍵はプロバイダのサービスによって管理されるものの、その管理は利用者がコントロールし、サーバーサイド暗号化で使用することもできます（Bring Your Own Key）。

9.2.3.2 クライアントサイド暗号化

クライアントサイド暗号化は、クラウドプロバイダが暗号化されたデータのみを保存する場合に採用されるセキュリティ対策です。このモデルでは、利用者はクラウドに送信する前にデータを暗号化する責任を負います。これにより、クラウドプロバイダが暗号化されていない状態のデータにアクセスできないことを保証します。自社内の暗号化ツールを使用して機密ファイルを暗号化することを決定した組織について考えてみましょう。暗号化後、これらのファイルを Amazon S3 や Google Cloud Storage などのクラウドストレージサービスにアップロードします。暗号化ファイルの性質上、アクティブな処理には使用できないため、このアプローチは通常、データのバックアップ、アーカイブ、またはアクセス頻度の低い「コールド」状態での保存を目的として採用されます。

9.2.3.3 サーバサイド暗号化

サーバーサイド暗号化は、ほとんどのクラウドプロバイダが提供するサービスで、プロバイダ自身が管理する鍵を使用してデータを暗号化します。セットアップが容易なように設計されており、通常、利用者による特定の設定を必要としないため、セキュリティニーズがそれほど厳しくない組織にとって魅力的な選択肢となります。サーバーサイド暗号化のセキュリティは、クラウドプロバイダ独自の暗号化プ

ロトコルと、その暗号化鍵の管理に依存します。このタイプの暗号化によって提供される主な保護は、ハードドライブに直接アクセスしようとするなど、ストレージハードウェアへの物理的なアクセスを伴う攻撃に対するものです。実際にサーバーサイドで暗号化が行われている例としては、AWS S3 のデフォルト暗号化機能があり、Amazon が暗号化鍵を管理し、保存時にすべてのデータを自動的に暗号化します。

9.2.3.4 利用者管理暗号化鍵

利用者管理暗号化鍵は、クラウドプロバイダの鍵管理サービス（KMS）を通じて、利用者が暗号化鍵の管理に積極的な役割を果たすことを可能にします。鍵を管理しているにもかかわらず、実際の暗号化プロセスはクラウドプロバイダによって実行されます。この方法は、暗号化鍵の作成、ローテーション、削除を含む暗号化鍵のライフサイクルに対する権限を利用者に与えます。一方、クラウドプロバイダのインフラストラクチャは、データの暗号化の実行を担当します。利用者管理暗号化鍵を正しく採用すると、責任が明確に分離されます。つまり、鍵の管理は利用者が行い、暗号化は CSP が行います。一般的に、これは鍵のコントロールの維持と利便性のバランスを取るため、多くの組織にとって好ましい選択肢となります。利用者管理暗号化鍵の実用的な応用は、組織が Azure Key Vault のようなサービスを鍵管理に使用し、これらの鍵を使用して Azure Blob Storage や Azure File Storage などの Azure のストレージソリューションに保存されたデータを暗号化する場合に歴然となります。

9.2.3.5 利用者提供暗号化鍵

Bring Your Own Key（BYOK）とも呼ばれる利用者提供暗号化鍵は、データをクラウドにアップロードした後に暗号化が行われ、クラウドプロバイダが暗号化処理を実行するモデルです。このシステムでは、通常、利用者はクラウドプロバイダの KMS に独自の暗号化鍵を提供する必要があります。このプロセスでは、CSP の KMS に暗号化鍵を移す必要があり、セキュリティ上のリスクが増える可能性があります。これは BYOK の一形態で、鍵がクラウドプロバイダで保管・管理される一方で利用者の管理下にある KMS を使用することとは対照的に、鍵は利用者側で管理され、使用時にのみ提供されます。

このアプローチは、CSP が使用する暗号化鍵を利用者がより詳細にコントロールできるようにする一方で、CSP の暗号化サービスにも依存します。このソリューションを選択すると、外部鍵の管理による制限があるため、CSP が提供できるサービスや機能の範囲が制限される可能性があります。この暗号化モデルを示す一般的なシナリオの 1 つは、組織が Google Cloud Storage に保存されたデータを暗号化する目的で、Google Cloud Platform の Cloud KMS に独自の鍵を持ち込む場合です。

9.2.3.6 カスタムアプリケーションレベルの暗号化

この方法は、暗号化と暗号化鍵の管理の両方について利用者が全責任を負うハイブリッドな状況とアプリケーションレベルの暗号化を包含します。利用者が暗号化鍵を CSP から完全に分離し、代わりにサードパーティのソリューションを通じて暗号化プロセスで処理するか、堅牢な鍵管理機能を備えた業界標準の暗号化ライブラリを利用することを選択する必要があります。

この戦略では、暗号化と鍵を最高度にコントロールできますが、それに伴って複雑さが増し、利用者の管理負担も大きくなります。このアプローチの実践例は、AWS Encryption Software Development Kit（SDK）などのツールを使用したカスタムアプリケーション内でのクライアントサイド暗号化の実装です。このような場合、アプリケーションはデータをクラウドに送信する前に暗号化するように設計されており、暗号化鍵はすべてクラウドではなくクライアント側で管理されます。

クラウドデータ暗号化戦略を選択する際には、データの機密性、規制要件（PCI-DSS、HIPAA、GDPRなど）、望ましいコントロールレベル、セキュリティ、使いやすさ、可用性のバランスなどの要素を考慮する必要があります。適切な戦略は、各組織固有のニーズと制約によって異なります。各アプローチのリスクとメリットを慎重に評価し、組織のセキュリティ目標とリソースに最も適したアプローチを選択することが不可欠です。

9.2.3.7 コンフィデンシャルコンピューティング

コンフィデンシャルコンピューティングは、機密データが処理中または分析中（データ使用中）であっても、暗号化されたセキュアな状態を維持することに重点を置いたアプローチです。ハードウェアベースのエンクレーブを使用することで、ワークロードランタイムとメモリ全体が暗号化され、処理スタックのすべてのレイヤーで非常に厳重なセキュリティが実施可能になります。

9.2.4 鍵管理サービスと Bring Your Own Key

現在、利用者提供の暗号化鍵/BYOK ソリューションのサービスのほとんどは、CSP サービスの使用に重点を置いています。利用者は、外部のソースから鍵を持ってくる場合とそうでない場合があります。以下の図は、技術レベルでは CSP ごとに異なりますが、これらの暗号化システムがどのように機能するかの概要を示しています。

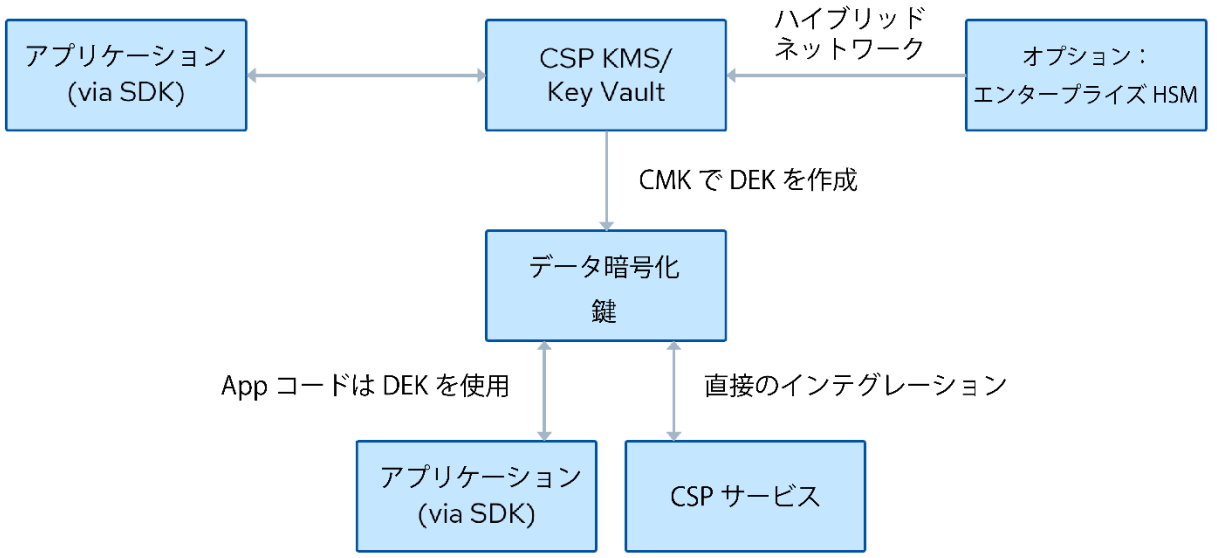


図 51: 鍵管理サービスと Bring Your Own Key 暗号化

CSP は、AWS KMS、Google Cloud KMS、Azure Key Vault、OCI KMS などの鍵管理サービスを提供します。これらのサービスは、鍵の生成、削除、保管、ポリシー、ローテーションなど、さまざまな機能を実行します。これらは通常、従来のハードウェアセキュリティモジュール (HSM) と類似した、すべての CSP 利用者向けのマルチテナンシーシステムとして実装されます。さらに、プロバイダによっては、非マルチテナンシーオプションを提供する専用のクラウドベースの HSM も提供しています。

通常、利用者は CSP の KMS を使用して利用者管理暗号化鍵（CMEK）を作成することで暗号化を管理します。特定の状況では、オンプレミスの HSM 内で鍵を作成したり、HSM を使用して初期鍵材料を生成したりすることがあります。これは、すでにデータセンターで HSM を利用しており、ハイブリッドまたはマルチクラウドアプリケーション間で鍵の同期が必要な利用者によく見られます。

CMEK は個々のデータ暗号化鍵（DEK）を生成するために利用されます。CMEK は KMS 内に残り、DEK が実際の暗号化タスクに採用されるのが標準的な方法です。AWS S3 のようなサービスは KMS 鍵を利用して利用者のバケット内のオブジェクトを暗号化でき、Azure Key Vault には管理対象のストレージボリュームを暗号化する機能があります。

アプリケーションレベルの暗号化の場合、利用者は一般的に暗号化操作を実行するために特別に設計された CSP 提供の SDK を通じて、DEK を使用します。これにより、利用者は CSP が提供する堅牢な暗号化フレームワークを活用しながら、アプリケーションのセキュリティを維持できます。

一部の KMS システムでは、利用者が API を使用してサービスにプレーンテキストデータを送信できるオプション機能を提供しています。その後、サービスはデータを暗号化し、暗号文が返されます。このプロセスは、アプリケーションレベルで鍵の漏洩を防ぐのに役立ちます。この機能をサポートするエンタープライズ HSM ソリューションを選択した場合は、追加のセキュリティ対策として統合できます。

9.2.5 データ暗号化の推奨事項

ここまで、クラウド環境におけるデータ暗号化の基礎について説明してきました。次に、データ暗号化を強化するための推奨戦略を示します。それぞれの戦略は、クラウドベースの運用におけるセキュリティ、コンプライアンス、および全体的なデータ保護の向上を目的としています。

- **Key Management Services (KMS):** クラウドアプリケーションとサービスをセキュリティ保護するには、クラウドプロバイダが提供する KMS を利用することをお勧めします。これらのサービスは、組織の暗号化鍵の管理に役立ちます。
- **SaaS に関する考慮事項:** SaaS を使用している場合、KMS が唯一の暗号化オプションになる可能性があります。SaaS では、カスタマイズできないことが多いため、データ保護はプロバイダのツールに頼ることになります。
- **デフォルトの暗号化：**これは通常、クラウドプロバイダの鍵を使用して保存データを暗号化することを意味します。通常、追加コストなしでサービスに含まれており、データ保護に関連するコンプライアンス要件に対応できます。
- **サービスごとのさまざまな鍵:** サービスや配備ごとに異なる暗号化鍵を使用することをお勧めします。このアプローチは、暗号化ドメインを分離し、侵害された鍵の潜在的な影響を制限することでセキュリティを強化します。
- **鍵に関する IAM ポリシー:**IAM ポリシーを鍵に適用して、最小特権の原則を適用します。こうすることで、許可されたユーザーとサービスだけが特定の鍵を使用できるようになり、ユーザーがその鍵を使用して実行できるアクションを定義できます。
- **脅威モデルとの整合性：**暗号化戦略が脅威モデルと整合していることを確認します。たとえば、攻撃者がアプリケーションのクレデンシャルやデータベース管理者のクレデンシャルを漏洩させることができた場合、データベースの暗号化をしたとしてもその効果は低くなります。このような場合、攻撃者は正規の経路を通じて暗号化されたデータにアクセスしたり、データを抜き取ったりすることができます。

9.2.6 クラウド DLP

DLP ツールは、機微データの検出、使用の監視、およびポリシー違反の防止または警告に使用されます。クラウドでの DLP は、膨大な量のデータが存在するため、固有の課題があります。特に IaaS や PaaS 環境では、膨大なボリュームとそれに伴うコストが包括的な DLP スキャンを困難にしています。そのため、SaaS アプリケーションでは IaaS や PaaS よりも DLP の利用が多い傾向にあります。

IaaS や PaaS 向けに DLP を実装する場合、クラウドプロバイダのネイティブ DLP サービスの範囲が限られていることが多くあります。たとえば、AWS Macie は主に S3 ストレージに重点を置いています。IaaS や PaaS と統合する外部 DLP ツールは、ボリュームを管理し、コストを削減するために、データサンプリング技法を頻繁に利用する必要があります。

組織は IaaS や PaaS の DLP を、「データセンター向け DLP」（複雑さと規模から歴史的に実装されていない可能性が高い）に類似していると捉えるべきです。対照的に、SaaS 向けの DLP は、E メール、Web ブラウジング、およびクラウドアプリケーションの使用状況全体にわたるユーザーアクティビティの監視に焦点を当てた従来の DLP プラクティスにより合致しています。

効果的なクラウド DLP 戦略を構築するには、組織はデータランドスケープを慎重に評価し、リスクの高い環境に優先順位を付け、クラウドネイティブとサードパーティの DLP ソリューションの使用のバランスを取る必要があります。リスクベースのアプローチと強力なアクセス制御を組み合わせることで、企業のクラウドフットプリント全体で機微情報を保護しながら、大規模なクラウド DLP の課題を管理することに役立ちます。

Cloud DLP は、Cloud Access Security Broker（CASB）の主要な機能であり、クラウド上のユーザーの操作を監視し、手順に従い定義されたポリシーを採用することで、可視化とセキュリティ制御を提供します。CASB は、複数のタイプのセキュリティポリシーの実施を統合します。セキュリティポリシーの例には、暗号化、トークン化などがあります。

9.2.7 Data Security Posture Management

DSPM は、データ中心のセキュリティに焦点を当てて設計されたツールの新しいカテゴリです。cloudsecurity posture management（CSPM）が IaaS クラウドの構成とポスチャを管理し、SaaS security posture management（SSPM）が SaaS セキュリティを管理することに対し、DSPM はデータの可視化と管理機能を提供します。

これには、データの検出と分類が含まれます。これには、データが存在する場所とその機密性を理解するのに役立つ DLP のような機能が含まれる場合もあります。DSPM ツールは、重複するアクセス制御、IAM ポリシー、リソース、ネットワークポリシーをすべて引き出して評価し、誰がデータにどのようにアクセスできるかを評価および可視化します。その後、これらのツールは提案を提供したり、修正を直接管理したり、 Infrastructure as Code （IaC）テンプレートやポリシーなどの特定の推奨事項を提供したりします。

クラウドデータセキュリティにおける課題は、重複する可能性のあるすべてのコントロールを処理することです。これらのコントロールはすべて異なる領域で管理され、データの使用と漏えいを完全に把握できるとは限りません。DSPM はそのギャップを埋めるように設計されています。

9.3 特定のストレージタイプのセキュア化

AWS S3 や Azure Blob Storage などのオブジェクトストレージサービスは、CSP 製品の重要なコンポーネントです。サイバーセキュリティの専門家は、組織的なデータ漏洩リスクが大きい分野だと考えています。注目度の高いインシデントは、これらの脆弱性を浮き彫りにします。多くの場合、設定ミスが原因です。通常、クラウドプロバイダはストレージオブジェクトをデフォルトでプライベートに設定しま

すが、ユーザーが不用意にこれらの設定を変更し、ビジネスやプライベートの機微データが公開される可能性があります。アクセス設定が複雑であるため、セキュリティがさらに複雑になります。

リスクを軽減するために、クラウドプロバイダはパブリックアクセスを導入レベルでブロックする機能を提供していますが、これは正当なデータアクセスのニーズを妨げる場合があります。後述するように、データを暗号化し、コンテンツ配信ネットワーク（CDN）を使用すると、セキュリティがさらに強化されます。継続的な監視とプロアクティブなセキュリティ戦略は、侵害を回避し、影響範囲を最小限に抑えるための追加の保護レイヤーです。

9.3.1 オブジェクトストレージのセキュリティ

AWS S3 や Azure Blob Storage などのオブジェクトストレージサービスは、クラウド運用に不可欠ですが、データ漏洩の大きなリスクがあります。注目すべきインシデント[143]は、これらの脆弱性を浮き彫りにします。通常、クラウドプロバイダは、ストレージオブジェクトをデフォルトでプライベート設定に設定して、データを保護します。それにもかかわらず、ユーザーが不用意にこれらの設定を変更すると、情報漏洩が頻繁に発生し、機密データが一般に公開されます。

複雑なアクセス設定の設定ミスや誤解は、さらにデータ漏洩の一因となります。AWS のきめ細やかな権限システムは、リソースベースのポリシーとともに IAM の役割とポリシーを含んでおり、これらの要素を十分に理解せずにクラウドストレージを保護することの難しさを例証しています。クラウドプロバイダは、意図しないパブリックデータの漏洩に対処するため、パブリックアクセスをデプロイメントレベルでブロックする機能を導入しています。たとえば、AWS では、バケット権限の設定ミスによるデータ漏洩を防ぐアカウント全体の設定を適用できます。

しかし、パブリックアクセスを普遍的にブロックすると、オープンデータアクセスを正当に必要とするアプリケーションに支障をきたす可能性があります。これらのブロックの例外を管理するには、必要なデータだけがパブリックにアクセスできるように慎重に構成する必要があります。セキュリティをさらに強化し、クラウドプロバイダの KMS のようなサービスを使用してデータを暗号化すると、暗号化鍵がオブジェクトストレージの権限を変更する機能を持つアイデンティティとは別に管理されることを条件に、データが保護されます。これにより、ストレージコンテナが不用意に公開された場合でも、暗号化鍵のセキュリティが維持されます。

アプリケーションによっては、パブリック向け CDN にリンクされたプライベート S3 バケットのように、プライベートオブジェクトストレージに格納されているデータを配布するために CDN を利用する場合があります。このセットアップではストレージが直接公開されることはありませんが、CDN を介したパブリックデータアクセスが可能になります。CSPM や Data Security Posture Management （DSPM）などのツールを使用した継続的なモニタリングが不可欠です。これらのツールは、セキュリティポスチ

[143] CSA. (2024) *Research Topic - Top Threats*. CSA sponsors a working group and discussion community to track and address threats like the Capital One breach in its Top Threats report.

ャを継続的に監視することで、セキュリティのベストプラクティスからの逸脱を検出し、修正するのに役立ちます。

サイバーセキュリティにおける「シフトレフト」の概念は、クラウドインフラストラクチャのセキュリティを強化する上で重要な役割を果たします。IaC における構成ミスの早期発見と防止が関係し、開発プロセスの早い段階でベストプラクティスが確実に統合されるようにするものです。このプロアクティブなアプローチにより、本番環境で重大な問題が発生する前に、潜在的なセキュリティ課題を回避できます。したがって、クラウドベースのオブジェクトストレージでデータの完全性と機密性を維持するためには、継続的なモニタリングとプロアクティブなセキュリティ戦略が不可欠です。

9.3.2 クラウドデータベースのセキュリティ

クラウドにデータベースを配備する場合、組織は主に次の 2 つのアプローチのいずれかを選択します。

- 従来の database as a service（DBaaS）
- クラウドネイティブデータベース

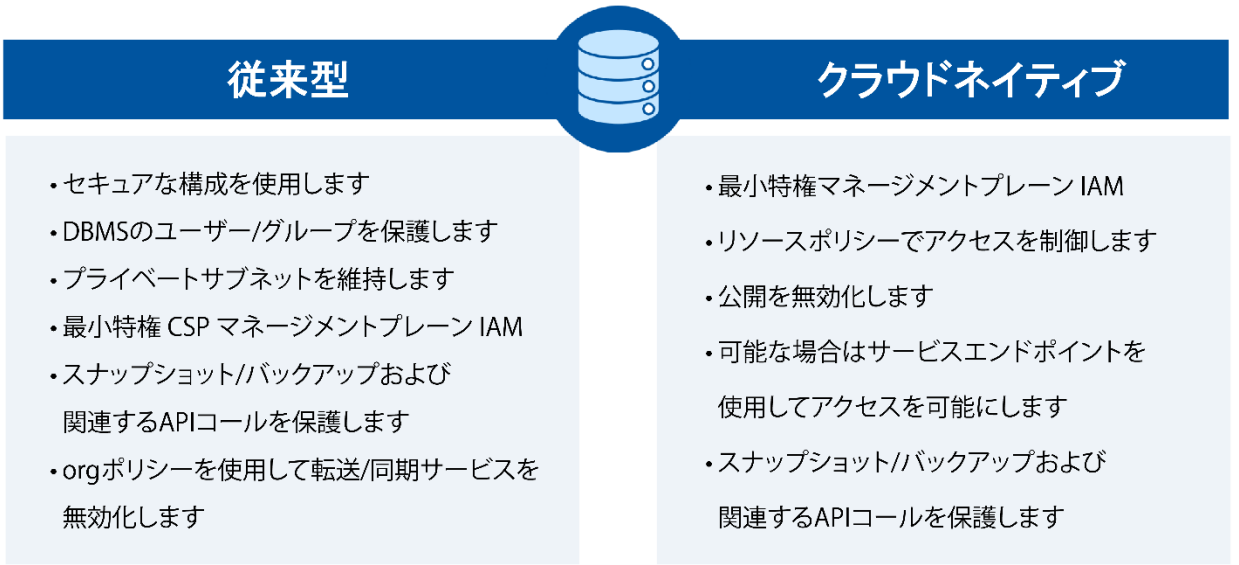


図 52: 従来の DBaaS とクラウドネイティブデータベース

従来の Database as a Service (DBaaS)
組織は、MySQL、PostgreSQL、Microsoft SQL Server など、クラウドプロバイダがマネージドサービスとして提供する有名なデータベースエンジンを選択できます。これらのデータベースを保護するには、確立されたベストプラクティスに従うことをお勧めします。これには、強固な認証手段と包括的なアクセス制御を組み込んだセキュアな構成の採用が含まれます。セキュアなデータベースユーザーアカウントとロールを作成し、プライベートサブネット内にデータを保存し、CSP のマネージメントプレーン IAM ロールへの最小権限アクセスの原則を実装することも重要です。さらに、CSP により管理されたバックアップとスナップショット機能を活用するとデータ保護を強化できる一方で、データ流出の一般

的な手法である不正アクセスを防ぐために、セキュアに管理する必要があります。リージョン間のレプリケーションのようなサービスが不要な場合は、組織のポリシーとコンプライアンスの要求に従うようにそれらを非アクティブにする必要があります。従来の DBaaS の有名な例としては、Amazon RDS、Azure SQL Database、Google Cloud SQL などがあります。

クラウドネイティブデータベース
別な方法として、サーバーレス運用や自動スケーリングなどの機能を備えた、クラウドプラットフォーム向けに特別に設計および最適化されたクラウドネイティブデータベースを検討する組織もあります。これらのデータベースを保護するには、まずマネージメントプレーンの IAM ロールに最小特権を割り当てることが不可欠です。データプレーンへのアクセスはリソースベースのポリシーで規制し、不正なデータ漏洩を防ぐためにパブリックアクセスを無効にする必要があります。可能であれば、専用のプライベートエンドポイントまたは仮想プライベートクラウド (VPC) を統合することで、アプリケーションがこれらのデータベースに接続するためのセキュアな経路を提供できます。アプリケーション統合のためのセキュアな API 呼び出しとともに、サービスの自動バックアップとスナップショット機能を活用することも有効です。クラウドネイティブデータベースの例としては、Amazon DynamoDB、Azure Cosmos DB、Google Cloud Firestore などがあります。

どちらのタイプのクラウドデータベースでも、次のことが極めて重要です。

- 責任共有モデルに従い、データベース構成を強化します。
- コンプライアンス要件を満たすために、必要に応じてデータを暗号化します。
- 強固な認証手段を導入し、最小特権の原則を守ります。
- ログを積極的に監視し、クラウドネイティブの脅威検出サービスを利用します。データレベルのログ/イベントのアクティブ化の検討をお勧めします。デフォルトでは有効になっていない場合があります。
- 包括的なバックアップ/リカバリ計画を作成し、維持します。

9.3.3 データレイクのセキュリティ

ビッグデータ時代には、多数のソースからの膨大なデータを管理、分析するための中枢要素としてデータレイクの概念が登場しています。CSA の Data Security Glossary[144]では、「データレイクとは、大量のデータを元の形式で取り込み、保存する中央集中型のリポジトリです。データは処理され、さまざまな分析ニーズのベースとして使用できます。オープンでスケーラブルなアーキテクチャにより、データレイクは構造化データ（データベーステーブル、Excel シート）から半構造化データ（XML ファイル、ウェブページ ）、非構造化データ（画像、音声ファイル、ツイート）まで、あらゆる種類のデータを、忠実さを犠牲にすることなく収容できます」と定義しています。この定義は、データレイクの本質を、多様なデータ形態の複雑さを処理および保持するために装備された包括的なデータ統合ポイントとしてカプセル化したものです。

[144] CSA. (2024) Download Publication - *CSA Data Security Glossary*.

しかし、さまざまなソースからのこのような広範なデータセットを統合することは、データレイクがサイバー脅威の格好の標的となるため、セキュリティ上の大きな課題があります。したがって、データレイク内に配備されるセキュリティ戦略は、アクセス性と実用性を維持しながら機密情報を保護するために多面的に行う必要があります。機微性と機密性に基づくデータの分離と区分化、および堅牢なアクセス制御システムの実装は、データの完全性とセキュリティを維持するために重要です。暗号化、ネットワークセキュリティ、継続的な監視などの対策により、組織は潜在的な脆弱性に対するデータレイクの強化に努め、統合されたデータリソースを安全かつ効果的に利用できます。

その膨大かつ多様なデータのセキュリティと完全性を確保するため、以下のような戦略を立てます。

- **データ統合ポイントとしてのデータレイク:** データレイクは、機微性やセキュリティ分類が大きく異なる多数のソースからの多種多様なデータを統合するため、強力です。課題は、この多様なデータセット全体で強固なセキュリティを維持することです。
- **セキュリティレベルとデータの分離：** データレイク内のデータの多様性を考えると、すべてのユーザーやアプリケーションがすべてのデータにアクセスできる必要はありません。公開されているデータもあれば、機密性の高いデータもあります。このデータを効果的に分離することが重要です。
- **ビュー/アクセスポイントによる区分化：** データレイクへのウィンドウとして機能するビューまたはアクセスポイントを作成します。各ビューは、特定のユーザーまたはアプリケーションのアクセスに関連があり、許可されているデータのみを表示するように調整されています。これは、データレイク内に仮想パーティションを作成することと似ています。

9.3.3.1 ベースラインのデータセキュリティプラクティス

以下は、利用者のデータ環境のセキュリティ強化策です。これらの根本的な対策は、脆弱性や脅威に対する防御の基礎を確立し、必要に応じてより専門的または高度なセキュリティ戦略を実施するための準備を整えます。

- **継続的な脆弱性評価と修復管理：** 脆弱性から保護するには、データレイクとやり取りするすべてのコンポーネントに最新のセキュリティパッチが適用されていることを確認します。
- **アイデンティティとアクセスの管理** ： 詳細な IAM ポリシーを実装します。アクセスは最小特権の原則に基づくべきであり、ユーザーとアプリケーションは、その機能を実行するために必要な権限のみを持つようにする必要があります。
- **暗号化:** 保存中、移動中、および使用中の暗号化を適用し、他のコントロールが機能しなくなった場合にデータの露出を防ぎます。たとえば、AWS KMS を使用して、データレイク内の S3 バケットの暗号化鍵を管理します。
- **ネットワークセキュリティ**： VPC、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などのネットワークセキュリティ対策を利用して、データレイクに出入りするトラフィックを制御します。
- **継続的なログ管理、監視、アラート：** アクセスパターンを継続的に監視し、実行されたセキュリティ対策が長期間にわたって有効であり続けることを確実にする権限の見直しを行います。データレイクのセキュリティ保護は、1 回限りのタスクではなく、新しいデータの追加やアクセス

要件の変更に応じて定期的に見直しや更新を行う継続的なプロセスであることを覚えておいてください。

- **侵入テスト：** コントロール（人、プロセス、技術）の弱点を特定してエクスプロイトし、攻撃者の目的と行動をシミュレーションすることで、情報資産の有効性とレジリエンスをテストします。

9.3.4 人工知能のデータセキュリティ

AI 技術が普及し、重要なビジネスプロセスに統合されるにつれ、AI システムのセキュリティと完全性の確保は最重要課題となっています。AI のデータセキュリティでは、AI システム、アルゴリズム、およびデータ資産をさまざまなセキュリティの脅威や脆弱性から保護するための対策を実装する必要があります。AI の導入には、主に 2 つのアプローチがあります。AI as a Service（AIaaS）とセルフ/クラウドホスト型 AI です。

9.3.4.1 AI as a Service

AIaaS モデルでは、サードパーティープロバイダがインターネット経由で AI 機能やサービスをサブスクリプション形式で提供します。組織は、事前にトレーニングされた AI モデル、API、ツールにアクセスして、AI 機能をアプリケーションやワークフローに統合できます。例えば、Anthropic の Claude、OpenAI の ChatGPT、Google Cloud の Vertex AI などがあります。AIaaS を使用する場合、以下の事項が不可欠です。

- サービスレベル合意書(SLA)を理解し、プロバイダが利用者の可用性、パフォーマンス、およびサポート要件を満たしていることを確認します。
- 暗号化方式、アクセス制御、不正アクセスからデータを保護するためのモニタリング機能など、プロバイダのデータセキュリティプラクティスを徹底的に評価します。
- プロバイダが GDPR、HIPAA、SOC 2 などの関連規制や標準に準拠していることを検証し、機微データの保護と業界のベストプラクティスへの準拠を確認します。
- プロバイダがセキュアエンクレーブや専用環境を提供していない場合、専有データや機密データの送信は避けます。
- プロバイダとデータ削除および保持ポリシーを明確にして、データライフサイクル管理がセキュリティ要件を満たすようにします。
- モデルポイズニング、プロンプトインジェクションなどの敵対的攻撃に対する保護を含むプロバイダの AI セキュリティ対策を評価し、AI 主導のサービスやアプリケーションの完全性と信頼性を確保します。

9.3.4.2 セルフ/クラウドホスト型 AI

セルフ/クラウドホスト型 AI アプローチでは、組織はオンプレミスまたはクラウドで AI モデルとインフラストラクチャを開発、配備、および管理します。組織は、データ収集、モデルトレーニング、最適

化、および配備などの AI 開発プロセスを完全にコントロールできます。組織は AI システムのセキュリティについて全責任を負います。主な考慮事項は次のとおりです。

- アクセス制御、暗号化メカニズム、およびデータガバナンスポリシーを実装して、機微データを不正アクセスや改ざんから保護することにより、トレーニングデータリポジトリを保護します。
- ネットワークセグメンテーション、ファイアウォール構成、および権限を持つユーザーやエンティティへのシステムアクセスを制御および制限するきめ細かな IAM ポリシーなど、セキュアな AI システムアクセスを確立します。
- AI の挙動操作を目的としたモデルポイズニングを防ぐ学習データのフィルタリングを行います。
- 入力メカニズムの脆弱性をエクスプロイトして、悪意のある入力によって AI の意図する動作を迂回しようとするプロンプトインジェクション攻撃に対するセーフガードを実装します。
- AI システム内でデータを検出しブロックする堅牢なプロンプトスキャンメカニズムを導入することで、AI ジェイルブレイクの試みから保護します。
- AI システムの定期的なアップデートとパッチ適用を行い、新たなセキュリティ脆弱性に対処します。
- AI システムが関連する AI 倫理ガイドラインや規制の遵守を確実にし、バイアスや差別的な出力を防止します。

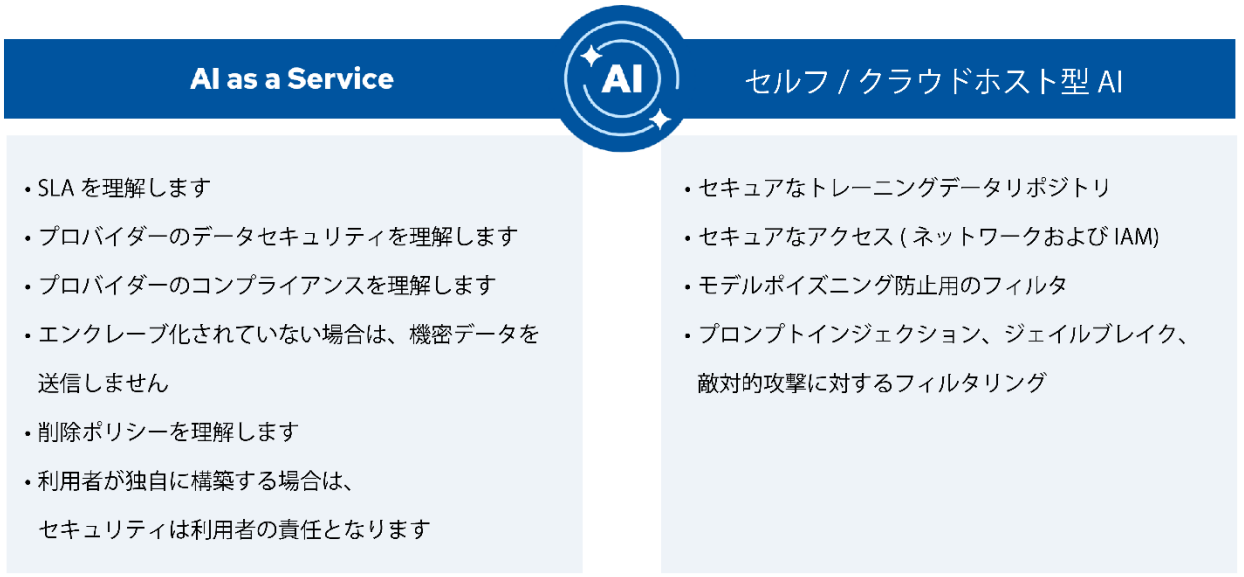


図 53: AIaaS とセルフクラウドホスト型 AI

9.3.4.3 AI に関するその他の考慮事項

AI システムのセキュリティを強化し、セキュアに統合・運用するために、以下のセキュリティプラクティスを検討します。

- AI システムを他のアプリケーションと統合する際に、セキュアな API と暗号化プロトコルを採用します。
- AI システムを操作するユーザーのための強固な認証とアクセス制御を実装します。

- 侵入テストや脅威モデリングなど、AI システムの定期的な監査とセキュリティ評価を実施します。
- AI セキュリティインシデントまたは侵害を検出、調査、および修正するためのインシデント対応計画を作成および維持します。
- AI セキュリティ意識の文化を醸成し、開発者、管理者、およびユーザーを育成します。

サマリ

このドメインは、クラウドサービスの急速な進化とサイバー脅威の増加の中で、クラウド環境における堅牢なデータセキュリティのニーズに対応しています。組織の完全性、機密性、顧客の信頼、および法令順守を維持するために、データセキュリティの重要性を強調しています。このドメインでは、データの分類、クラウドストレージの種類、さまざまなデータ状態（保存中、移動中、使用中）に対する特定のセキュリティ対策など、データセキュリティのさまざまな側面について調査します。IAM、暗号化、アクセス制御ポリシーなど、必須のセキュリティツールと技法をカバーし、クラウドデータを保護するための包括的なガイドを提供します。全体として、このドメインは、クラウドでのデータセキュリティプラクティスの強化を目指す組織にとって、基本的なガイドとして機能します。

推奨事項

- クラウドのセキュリティは、クラウドに移動するデータの把握と管理、アクセス制御の適用から始まります。
- IAM ベースのアクセス制御、リソースポリシー、ネットワークポリシーの違いを理解します。データの漏洩を防ぐため、これらをすべて揃える必要があります。
- 暗号化は、それが脅威モデルと一致し、鍵とデータ（およびそれぞれへのアクセス）が分離されている場合にのみ、セキュリティを向上させます。攻撃者が SQL インジェクション攻撃を実行し、アプリケーションを通じてデータ（訳注：原文は date となっているが data の誤りと思われる）を取得できれば、暗号化は価値がありません。
- IaaS や PaaS で暗号化を実装する場合は、まず CSP KMS サービスから導入します。
- IaaS のクラウド DLP は、従来のデータセンターにおける DLP を反映しています。SaaS 向けの DLP は、メールサービスやアプリケーションの DLP と同じです。
- 特定のデータへのアクセスを制御する（およびコアデータストレージのセキュリティコントロールに従う）ことにより、データレイクのセキュリティを確保します。
- AI セキュリティは、潜在的なデータ漏洩に焦点を当てるべきであり、それはパブリックサービスとセルフホスティングモデルのどちらを精査するかによって異なります。

追加のガイダンス

- Key Management in Cloud Services | CSA
- Cloud Key Management System with External Origin Key | CSA
- Recommendations for Using a Customer Controlled Key Store | CSA

- Cloud Key Management Foundations | CSA
- Cloud Key Management Foundations II | CSA
- Key Management Lifecycle Best Practices | CSA
- An Agile Data Doctrine for a Secure Data Lake | CSA
- Understanding Cloud Data Security and Priorities | CSA

ドメイン 10: アプリケーションセキュリティ

はじめに

このドメインは、セキュリティコントロールを使用してコンピュータアプリケーションを外部の脅威から保護するプラクティスであるアプリケーションセキュリティを対象としています。アプリケーションセキュリティには、初期の設計や脅威のモデリングから本番環境のアプリケーションの保守や防御まで、非常に複雑で膨大な知識が含まれています。アプリケーション開発の実践が進歩を続け、新しいプロセス、パターン、技術を取り入れるにつれて、アプリケーションセキュリティも急速に進化しています。クラウドコンピューティングは、これらの進歩の最大の推進要因の 1 つであり、進歩の安定性、拡張性、およびセキュリティを確保することが緊急かつ急務となっています。

クラウドベースのアプリケーションのセキュリティは、初期設計段階から継続的なメンテナンスまで、慎重な検討と事前対策が必要です。クラウド環境（多くのプライベートクラウド環境やオンプレミス環境にも適用される）におけるアプリケーションセキュリティがもたらす固有の課題と機会の概要を以下に示します。

- アプリケーションは多くの場合、マイクロサービスと外部サービスのコンステレーションとして構築されるため、アタックサーフェスとコントロール境界のより詳細な分析が必要になります。
- アタックサーフェスには、API に対する重大なエクスポージャーがしばしば含まれます。
- クラウドのコンテキストでは、迅速な機能開発を伴う DevOps アプローチを使用してアプリケーションを開発することが多いため、リスクであると同時に機会でもあります。
- アプリケーションは、プロバイダの管理下にあるライブラリ（PaaS プロバイダ、サーバーレスなど）上に構築される可能性があるため、責任共有モデルに注意する必要があります。
- アプリケーションは、オープンソースコンポーネントを含むサードパーティライブラリを頻繁に活用し、サプライチェーンのリスクと追加の攻撃ベクトルをもたらします。バージョン管理と開発リポジトリのための Software as a Service（SaaS）ソリューションの統合を検討する場合、この複雑さはさらに増し、外部依存に伴うリスクを軽減する堅牢なセキュリティ対策が必要になります。
- アイデンティティ管理、ロギング、モニタリングなどのセキュリティ機能は、多くの場合、クラウドプロバイダから提供されます。これは、アプリケーションのセキュリティ要件と一致する場合と一致しない場合があります。
- アプリケーションは、プログラマブルなインフラストラクチャ（Infrastructure as a Code（IaC）、または Kubernetes などのオーケストレータ）上にしばしば配備されます。
- クラウド環境内で大規模に動作するアプリケーションは、基盤となるインフラストラクチャの脆弱性を強く認識する必要があります。インフラストラクチャの障害の影響を軽減するために、スケーラビリティとレジリエンスを優先するステートレスアーキテクチャが一般的に採用されています。しか

し、これらのアーキテクチャは柔軟性と俊敏性を提供する一方で、全体的なセキュリティポスチャを損なう可能性のある複雑さももたらします。

学習目標

このドメインの学習目標は、読者に以下の知識を提供することです。

- セキュアなアプリケーションを作成するためのセキュアな開発プロセスを実装します。
- クラウドアプリケーションのセキュリティ確保におけるアーキテクチャの重要な役割を認識します。
- DevSecOps を使用して、セキュアソフトウェア開発ライフサイクル（SSDLC）全体のセキュリティの統合を自動化します。

10.1 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は、セキュアな開発プロセスから始まります。安全でセキュアなコードが、機能構築を主な仕事とする開発者チームによって作成されることを期待するだけでは十分ではありません。これらの懸念に対処するため、開発とセキュリティの専門家はソフトウェア開発ライフサイクル（SDLC）と呼ばれる一連のプロセスを中心に融合し、セキュアソフトウェア開発ライフサイクル（SSDLC）とも呼ばれるようになりました。

クラウドは、これらのプロセスのさまざまな部分にいくつかの新しい意味をもたらします。これは主に、アプリケーションとクラウドインフラストラクチャ間の緊密な統合に起因しています。また、開発者はクラウドでの作業時に、DevOps のようなより新しく高速な方法論を使用する傾向があります。最後に、IaC とデプロイメントパイプラインは、クラウドでは標準的なプラクティスですが、従来のデータセンターアプリケーションでは必ずしも同じ程度まで使用されているわけではありません。

10.1.1 CSA セキュア開発ライフサイクル

The Cloud Security Alliance (CSA) Development, Security, Operations (DevSecOps) *Secure Development Lifecycle*[145] (SSDLC) は、アプリケーション開発の一般的に合意されたフェーズに対応する 5 つのステージを定義しています[146]。これらの各段階では、成功する DevSecOps プログラム に実装すべき主要なプロセス、ツール、およびデザインパターンを特定します[147]。

[145] CSA. (2024) Secure Development Lifecycle.

[146] Similar development lifecycles have been created by software vendors, such as Microsoft’s Security Development Lifecycle (SDL) that offer additional guidance of secure development practices.

[147] CSA. (2022) Specific implementation details are available in Pillar 3 - Pragmatic Implementation of the Six Pillars of DevSecOps Series.

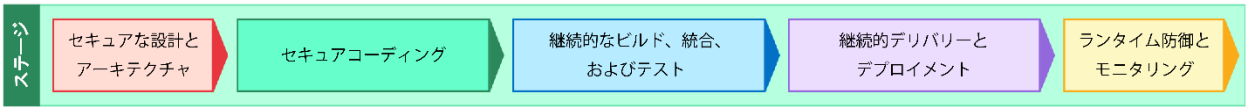


図 54: SSDLC（セキュアなソフトウェア開発ライフサイクル）の段階

SSDLC のステージ

1. **セキュアな設計とアーキテクチャ：** 設計セクションでは、製品の設計時に適用できる技術やツールについて言及します。設計は継続的であり、新製品の機能や変更は設計活動を通じて行われます。設計フェーズにセキュリティを含めないと、セキュリティ対策は後に導入されることになり、配備時や実行時の運用への影響やコストが大きくなってしまいます。また、対策は拡張が難しく、セキュリティのボトルネックにより開発スピードが遅くなり、リリーススケジュールにも影響が出てしまいます。
2. **セキュアコーディング：** これらの機能は開発段階で適用され、アプリケーションの構築時にセキュリティが確実に統合されるようにします。自動化ツールに依存するコーディングセキュリティコントロールは、手作業でのレビューと比較して、コードの弱点や脆弱性をより適切かつ一貫して特定できます。開発段階でセキュリティ分析や設計を含めないと、SSDLC の後の段階でソースコードの脆弱性が特定され、修正にコストがかかる本番環境に配備されてしまうリスクがあります。

3. **継続的なビルド、統合、テスト：** 統合とテストには、配備前にアプリケーション/製品のセキュリティ脆弱性をテストするツールとプロセスが含まれます。これらが無いと、セキュリティの脆弱性がエクスプロイトされ、データ漏洩、不正アクセス、およびアプリケーション/サービスの可用性に対するさまざまな影響などのエクスプロイトにつながる可能性があります。

4. **継続的デリバリーとデプロイメント**：配備前の安全性チェックは、アプリケーション/製品がセキュアなインフラストラクチャに配備されることを確認します。配備段階でセキュリティ分析を含めないと、脆弱性や不十分なセキュリティ手法により、アプリケーション、製品、およびサービスが本番環境でエクスプロイトや攻撃にさらされるリスクがあります。

5. **ランタイム防御とモニタリング：** これらの機能とプラクティスは、アプリケーション/製品が本番環境にリリースされた後に適用されます。ランタイムセキュリティは、非効率、脆弱性、弱点を特定し、インシデント対応を可能にすることで、継続的な改善を可能にします。

10.1.2 脅威モデリング

脅威モデリング[148]は、組織の資産に対する潜在的なセキュリティ脅威を特定、評価、および修正するためにリスク管理で使用される構造化されたプロセスです。システムアーキテクチャの把握、セキュリテ

[148] OWASP. (2024) *Threat Modeling Process*.

ィ目標の特定、および目標に影響を与える可能性のある潜在的な脅威の分析が含まれます。脅威モデリングを実行することで、特定された脅威の重要度と発生可能性に基づいて優先順位を付け、関連するリスクを軽減または防止するための戦略を策定できます。このプロセスにより、攻撃に対してより脆弱な部分に注意を向け、開発ライフサイクルの早い段階でセキュリティ対策が統合されるため、よりセキュアなシステム設計が可能になります。

STRIDE は、セキュリティ上の脅威の特定と分類に使用されるフレームワークです。 **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of Service, and **E**levation of Privilege の略です。各脅威カテゴリの概要を示します。

1. **スプーフィング**:これには、攻撃者がユーザーやシステムなどの他人になりすまして不正アクセスを行うことが含まれます。たとえば、攻撃者が正規のサイトを模倣してログインクレデンシャルを盗むフィッシング攻撃などがあります。

2. **改ざん**:データやメッセージを不正に改変することをいいます。転送中またはストレージシステム内で発生する可能性があり、データの完全性が損なわれます。

3. **否認**：これは、当事者が行為を行ったにもかかわらず、行為を否定する場合に発生します。これは、正しい情報源に行動を帰属させるシステムの能力を損ない、説明責任を複雑にします。

4. **情報開示**：これには機密情報への不正アクセスが含まれます。セキュリティで保護されていない通信を盗聴したり、脆弱性をエクスプロイトして機密データにアクセスする手法などがあります。

5. **サービス拒否**：システムリソースが枯渇し、システムが利用できなくなることです。業務が中断され、大幅なダウンタイムが発生する可能性があります。

6. **権限昇格**：攻撃者が許可される以上のアクセスレベルを取得すると、アクセス制御をバイパスして、より特権の高いアカウント用に用意されたアクションを実行します。

これらの脅威を把握することで、システムの潜在的な脆弱性を特定でき、これらのセキュリティリスクから保護するための効果的な対応策の開発の指針となります[149]。

10.1.3 セキュアな設計と開発

クラウドでは一般に、アーキテクチャとアプリケーションコードの結合が高くなります。インフラストラクチャとサービスは、同じバージョン管理リポジトリと継続的なデプロイメントパイプラインを使用して、アプリケーションコードと完全に統合された IaC を使用してデプロイされるのが一般的です。

[149] CSA. (2022) Specific techniques in Pillar 3 - Pragmatic Implementation of the Six Pillars of DevSecOps Series.

ほとんどのクラウドアプリケーションは、クラウドサービスプロバイダ（CSP）の Platform as a Service（PaaS）サービスも多用しており、これらはすべて、アプリケーションとセキュリティの両方の要件に合わせて適切に構成する必要があります。これには通常、アプリケーションコードとサービスに、それらのサービスを使用するための API 呼び出しを行う権限を割り当てる必要があり、潜在的なアタックサーフェスをマネージメントプレーンに拡大します。

セキュアなアプリケーション設計は常に重要ですが、このようなアプリケーション、インフラストラクチャ、およびマネージメントプレーン間のより深い絡み合いは、あらゆるプロジェクトの開始時にセキュアな設計に一層重点を置く必要があります。クラウドアーキテクチャは、アプリケーションセキュリティの基本です。クラウドアーキテクチャ(およびサービス)だけでも、さまざまなセキュリティリスクを軽減できます。たとえば、静的オブジェクトストレージバケットで単一ページアプリケーションをホストすることは、アプリケーションが Web サーバーを必要としないことを意味します。

クラウドアプリケーションを設計する際には、次の項目を含むセキュリティの原則を考慮する必要があります。

- PaaS サービスは、CSP へより多くのセキュリティ責任を転嫁でき、利用者がセキュアで完全にパッチが適用された構成済みのサーバーやサービスを維持する必要性を軽減または排除できる可能性があります。
- すべてのアプリケーションコンポーネントと PaaS サービスに最小特権の Identity and Access Management（IAM）を実装します。
- ロードバランサーや非常に制限の厳しいセキュリティグループなどの CSP サービスを利用すると、インターネットへの露出を減らすことができます。

設計が完了したら、標準的なセキュアな開発方法に従う必要があります。Cloud Security Alliance（CSA）は、DevSecOps プロセスの使用を推奨しており、それは、セクション 10.5 で取り上げています。

10.1.4 テスト:配備前

配備前のテストは、ソフトウェアの本番稼働前にセキュリティと機能を確認するための重要なステップです。チームは、開発プロセスの初期段階、特に配備前のテストを統合することで、時間とリソースを大幅に節約できます。このアプローチにより、課題の早期発見と修正が可能となり、よりセキュアで信頼性の高いソフトウェア製品の実現に貢献します。

配備前の主なテスト方法の例を次に示します。

1. **静的アプリケーションセキュリティテスト(SAST)**:アプリケーションのソースコードを調べて、既存のセキュリティ上の欠陥や脆弱性を特定するプロセスです。これはセキュリティコードレビューを自動化する方法であり、継続的インテグレーション/継続的デプロイ（CI/CD）パイプラインや開発者の統合開発環境（IDE）に統合される可能性があります。具体的には、ロジックエラーを探し、仕様の実装を検証し、またスタイルガイドラインやセキュリティ上の欠陥

（OWASP Top 10 や SANS Top 25 にリストされているものなど）をチェックします。さらに、ハードコードされたクレデンシャル、鍵、トークン、およびシークレットがないかコードをスキャンしてリポジトリに入ることを防ぎ、その他のアクティビティの中で潜在的なリークを特定します。SAST は誤検知を起こしやすいため、開発者を遠ざけないためにチューニングと優先順位付けが必要です。

   a. **手動のセキュリティコードレビュー**：このプロセスでは、経験豊富な開発者が提出された各コードレビューを検証し、欠陥を探します。自動化されたプロセスでは、ビジネスロジックエラーのような重要なエラーは検出されないため、手動でのコードレビューを強く推奨します。これはプルリクエスト（PR）プロセスを使用して実施できます。最適なアプローチは、自動プロセスと手動プロセスを実行することです。これらは互いに補完し合うからです。

2. **ソフトウェア構成分析 (SCA)**：SCA には、ライブラリやシステムコンポーネントなど、ソフトウェアが依存する外部コンポーネントの監査が含まれます。この方法は、これらのコンポーネントが最新のものであり、既知の脆弱性がないことを確実にします。また、これらのコンポーネントのライセンスの種類は、プロジェクトにライセンスリスクをもたらすことを避けるために役立ちます。これはセキュアな仮想マシン(VM)、コンテナイメージ、およびサーバーレス機能を作成するために不可欠です。SCA は、ソフトウェア部品表（SBOM）の作成を支援することもでき、ソフトウェアで使用されるすべてのコンポーネントの透明性を提供します。

3. **静的脆弱性スキャン：**クラウド環境では、潜在的なセキュリティの脅威を特定して軽減するために、脆弱性スキャンが非常に重要です。スキャンには大きく分けて静的スキャンと動的スキャンの 2 種類があります。静的スキャンは、VM イメージまたはテンプレート、コンテナイメージ、Docker ファイル、Docker-compose ファイル、Kubernetes YAML、Terraform または Cloudformation ファイルなどのファイルを含む、保存中のソースコード（IaC）と構成を分析します。このタイプのスキャンは通常、SSDLC の配備前段階で実行され、配備前に設定ファイル、インフラストラクチャテンプレート、およびソースコードを調べます。静的スキャンは、本番環境で課題が発生する前に対処できる脆弱性や構成エラーを特定するために役立ちます。

10.1.5 テスト:配備後

配備後のテストでは、配備後のソフトウェアのセキュリティと機能を検証します。特にクラウドアプリケーションでは、設計や統合の際に想定されている事項に対して挑戦します。このフェーズでは、従来のデータセンターのテストプロセスを反映し、ソフトウェアが実環境で効果的に動作することを確認します。

以下に、配備後に不可欠なテストの例を示します。

1. **動的な脆弱性スキャン：** SSDLC への配備後に動的スキャンが行われます。実行環境を積極的に調査し、実際の攻撃シナリオをエミュレートして悪意のあるアクターにエクスプロイトされる可能性のある脆弱性を特定します。保存中のコードや構成を調べる静的分析とは異なり、動的スキャンはシステムのセキュリティポスチャをリアルタイムで評価するため、配備前の静的分析で見

落としていた潜在的な弱点を把握できます。動的スキャンは、攻撃をシミュレートすることで、さまざまな脅威に対するシステムの耐障害性を把握し、エクスプロイトされる前に脆弱性を修復できます。配備前にコードや構成の脆弱性を特定する静的分析と組み合わせることで、動的スキャンはクラウド環境を保護するための包括的なアプローチを提供し、SSDLC 全体でアプリケーションとインフラストラクチャを潜在的な脅威からの保護を確実にします。

2. **動的アプリケーションセキュリティテスト** (DAST)：DAST はテスト手法の 1 つで、テスト担当者は、実行中に Web アプリケーションを検査しますが、アプリケーション、システムレベルでの相互作用、あるいは設計に関する知識を持たず、ソースプログラムへのアクセスや可視性も持っていません。DAST は「ブラックボックス」テストとも呼ばれ、特定の手法とテストツールを使用して、外部からアプリケーションを見て実行状態を調べ、疑似攻撃テストに対する応答を観察します。これらのシミュレーションに対するアプリケーションの反応は、アプリケーションが脆弱であり、実際の悪意のある攻撃の影響を受けやすいかどうかを判断するために役立ちます。

    - **動的解析(ファジング):**ソフトウェアに想定外なデータを入力し、運用中にエクスプロイトされる可能性のあるエラーや脆弱性を特定します。
    - **インタラクティブアプリケーションセキュリティテスト** (IAST)：IAST は、自動テスト、人間、またはアプリケーション機能と相互作用する任意のアクティビティによってアプリケーションが実行されながら、アプリケーションをテストするアプリケーションセキュリティテストの手法です。IAST は、ソースコード上の問題の概要を把握し、ランタイム上で実行するという目的を達成するという点で、SAST と DAST を組み合わせたものと見なすことができます。

3. **侵入テスト**：侵入テストは、サイバー攻撃の疑似攻撃テストとして実施され、既知の脆弱性をエクスプロイトすることを目的として、セキュリティ対策の耐障害性や攻撃に耐えるソフトウェアの能力をテストします。当該テストは、自動化ツールまたは手作業を使用して適用できます。長期的には、両方を適用することをお勧めします。侵入テストを適用してアプリケーションコンポーネントレベルをテストすることも、クラウド配備レベルで実行してクラウド構成の欠陥を特定することもできます。

4. **バグバウンティプログラム:**このプログラムは、ライブアプリケーションの脆弱性やバグを首尾よく発見し報告することで、倫理的なハッカーに金銭的な報酬を提供します。バグバウンティプログラムにより、組織は倫理的なハッカーコミュニティを活用して、システムのセキュリティポスチャを徐々に改善することができます。バグバウンティプログラムは必ずしも必須ではありませんが、組織がセキュリティ戦略の一環として検討することは可能です。

10.2 セキュアなクラウドアプリケーションアーキテクチャ

システムのアーキテクチャは、クラウドアプリケーションのセキュリティを確保する上で重要な役割を果たします。それは、セキュアなクラウドベースのソリューションを設計および配備するための青写真として機能します。セキュリティの原則とプラクティスをアーキテクチャレベルで統合することによ

り、組織はデータ保護、プライバシーの維持、および規制基準の遵守を確保するための強固な基盤を構築できます。これには、潜在的な脅威を軽減し、データ伝送を保護し、またアクセス制御を効果的に管理するために、クラウド環境内のコンポーネントと相互作用を慎重に計画する必要があります。コンポーネントを移動することや、" 機能"を実装しないことで、特定の資産/データフローに対する脅威が存在しなくなる可能性があります。適切に設計されたアーキテクチャにより、セキュリティが強化され、クラウドアプリケーションのスケーラビリティ、信頼性、および全体的なパフォーマンスが向上します。

10.2.1 アーキテクチャレベルのセキュリティに対するクラウドの影響

クラウドコンピューティングは、従来のソフトウェア開発およびインフラ開発のパラダイムをシフトし、すべてがソフトウェアであることを強調します。このシフトにより、運用が合理化され、インフラストラクチャとアプリケーションが緊密に統合されるため、セキュリティに対する新しいアプローチが必要になります。

1. **インフラストラクチャとアプリケーションの統合：**クラウドはインフラストラクチャとアプリケーションを融合させ、サーバやデータベースなどの要素をアプリケーションの機能と統合します。この連携により、シームレスな運用によるセキュリティ強化が可能です。しかし、不正確な許可が侵害につながるという IAM リスクももたらします。ここで重要なのは、潜在的な脆弱性を軽減するためのアイデンティティとアクセスの綿密な管理です。

2. **アプリケーションコンポーネントのクレデンシャル:**クラウドでは、マイクロサービスなどのコンポーネントは、多くの場合、そのサービスのためだけに指定された特定の権限とクレデンシャルを使用して通信します。情報漏洩や管理ミスは、重大なセキュリティインシデントにつながる可能性があります。侵害を防ぐためには、クレデンシャルをセキュアに取扱い、アクセスを厳密に制御することが重要です。

3. **Infrastructure as Code とパイプライン:**コードを通じてインフラストラクチャを定義することは、クラウドプラクティスの特徴となっており、配備における一貫性と効率性を提供しています。しかし、これらの配備パイプラインは攻撃者を呼び込む可能性があります。パイプラインが侵害されれば、ソフトウェアサプライチェーン全体が侵害される可能性があります。これらのパイプラインを保護することで、開発および配備プロセスが保護されます。

4. **イミュータブルインフラストラクチャ**：仮想化と Infrastructure as a Service（IaaS）技術の成熟に伴い、多くのセキュリティ専門家は、マシン構成の管理と配備がメンテナンスされたり改ざんされたりすることがないというパラダイムに移行しています。具体的には、アプリケーション、サーバ、またはシステム構成のインスタンスが一度作成されると、変更されることはありません。代わりに、変更が必要な場合は、共通のテンプレートから新しいインスタンスを構築し、完全に置き換えられます。このアプローチは、ミュータブルインフラストラクチャなどの従来のメンテナンス手法とは対照的です。

まとめると、クラウドコンピューティングへの移行には、統合システム固有の課題と機会に焦点を当て、アーキテクチャレベルでのセキュリティの再評価が必要です。早期かつプロアクティブなセキュリティ計画とアイデンティティおよびクレデンシャルの堅牢な管理は、セキュアなクラウドベースアーキテクチャの基盤となります。

10.2.2 アプリケーション設計とアーキテクチャに対するクラウドの影響

クラウド環境では、柔軟性、拡張性、およびセキュリティを重視して、アプリケーションの設計とアーキテクチャを変革する必要があります。アプリケーションのセキュリティについては、要件構築フェーズの早い段階で検討し、プロジェクトに組み込む必要があります。 開発プロセスにセキュリティ対策を統合することに関する詳細なガイドである NIST 800-64[150]や、IT システムのライフサイクルにセキュリティを織り込む方法に関するガイドラインである ISO/IEC 27034[151]など、SSDLC に情報を提供している主要なフレームワークやガイドラインを参照することもできます。

DAST は実行中のアプリケーションをテストし、Web の脆弱性テストやファジングなどのテストを含みます。CSP の利用規約により、DAST が制限されていたり、プロバイダの事前テスト許可が必要な場合があり、CSP によっては許可に時間を要する場合があります。クラウドと自動配備パイプラインにより、IaC を使用して完全に機能するテスト環境を構築し、本番環境の変更を承認する前に詳細な評価を実施することができます。

以下に、クラウド環境向けの開発、統合、配備における最も一般的なプラクティスを示します。

1. **デフォルトでの分離：**クラウドプラットフォームでは、個別の仮想ネットワークやアカウント/サブアカウントなど、分離された環境でアプリケーションを実行できます。この分離により、開発環境と本番環境を区分し、必要に応じてより厳格なアクセス制御が可能になるため、セキュリティが向上します。クラウドコンピューティングにより、異なるサーバやコンテナへのサービスの分離が容易になり、スケーラビリティとセキュリティが向上します。通常、マイクロサービスを伴うこのアプローチでは、マイクロサービス間の通信セキュリティを慎重に管理し、サービスの検出、スケジューリング、およびルーティングのセキュアな設定を行う必要があります。

2. **配備とテストの自動化：**クラウドプラットフォームでは、組織はこれまでよりも迅速なソフトウェアの開発と配備を目指しています。つまり、セキュリティチームや運用チームにとっては、テスト環境の配備やアプリケーションコードに対するセキュリティテストなど、これまで手作業で行っていた作業は、効率とペースを上げるために自動化されるべきです。自動化のニーズは、新しいツールの採用と CI/CD パイプラインでの使用の増加につながります。

[150] NIST. (2022) *NIST 800-64* originally provided NIST guidance for secure development but has be withdrawn and replaced with *NIST SP 800-64 Revision 2*. We provide both for clarity as you browse the Internet for details.
[151] ISO/IEC. (2018) *ISO/IEC 27034-3:2018(E)*.

3. **イミュータブルインフラストラクチャ：**イミュータブルインフラストラクチャは、リモートログインを無効にし、ファイル完全性モニタリングを追加し、またインシデントリカバリにこれらのプラクティスを組み込むことで、セキュリティ侵害のリスクを軽減します。

4. **PaaS とサーバーレスアーキテクチャ:**PaaS とサーバーレスコンピューティングは、基盤となるサービスやオペレーティングシステムの管理をクラウドプロバイダにオフロードすることで、アタックサーフェスを減らします。これらのアーキテクチャのセキュリティは、プラットフォームを保護し、ユーザーのセキュリティ要件を満たすというクラウドプロバイダのコミットメントに大きく依存します。

これらの各側面は、クラウドコンピューティングがもたらす固有の機会と課題にセキュリティ戦略を適応させることの重要性を強調しています。

10.2.3 Infrastructure as Code とアプリケーションセキュリティ

IaC は、設計図から建物を自動構築することと同様に、設定ファイルを使用してリソースの定義と管理を行うことで、IT インフラストラクチャのセットアップに革命をもたらします。

このアプローチにより、クラウドリソースの配備と管理が合理化され、アプリケーションのセキュリティが大幅に強化されます。

1. **コンプライアンスチェックの自動化：**IaC は、セキュリティ標準や規制に対する自動検証を容易にし、インフラストラクチャのプロビジョニングや変更が行われるたびにコンプライアンスを確保します。この自動化は容赦ない検査官のように機能し、セキュリティポリシーの遵守を常に確実にします。

2. **一貫したセキュリティポスチャ：**IaC は、インフラストラクチャのセットアップを成文化することで、サーバーからデータベースまで、あらゆる要素がセキュリティのベストプラクティスに従って一貫して構成されていることを保証します。これにより、手動セットアップに伴う人的ミスを排除し、構成のずれを検出して排除し、すべてのリソースで均一なセキュリティレベルを維持できます。重要なことは、IaC は、一元的な例外管理を通じて、これらのセキュリティポリシーの例外管理もサポートしていることです。たとえば、特定のリソースでは、Simple Storage Service (S3)バケットがパブリックアクセス用に構成されているなど、有効なビジネスニーズのために標準構成からの逸脱が必要になる場合があります。これらの例外を IaC フレームワーク内で文書化して管理することで、組織はこのような逸脱を確実に認識、承認、および追跡し、必要な運用の柔軟性をサポートしながらセキュリティ監視を維持できます。

3. **脅威への迅速な対応：**IaC は、特定された脆弱性に対応するインフラストラクチャコードの迅速な変更を可能にし、インフラストラクチャ全体へのパッチ適用とホットフィックスの導入を可能にします。この機能は、物理的に介入することなく、遠隔から建物のセキュリティシステムを更新して弱点に対処することに似ています。

4. **迅速な CI/CD ロールバック:**IaC は迅速な CI/CD ロールバック機能をサポートし、運用のレジリエンスを強化します。コンテナや仮想化環境の更新が行われると、パフォーマンスをベンチマークと統計的に比較することができます。カナリアリリースなどの新しい自動ロールアウトがこれらのベンチマークを満たさない場合、IaC は以前の安定した構成への自動ロールバックを可能にします。これにより、ダウンタイムを最小限に抑えるだけでなく、新たな変更によってセキュリティや動作の安定性が損なわれることもありません。

次の図は、セキュアなクラウドアーキテクチャでの設計、自動化のコーディング、インフラストラクチャテンプレートの作成、およびデプロイの繰り返しプロセスを示しています。

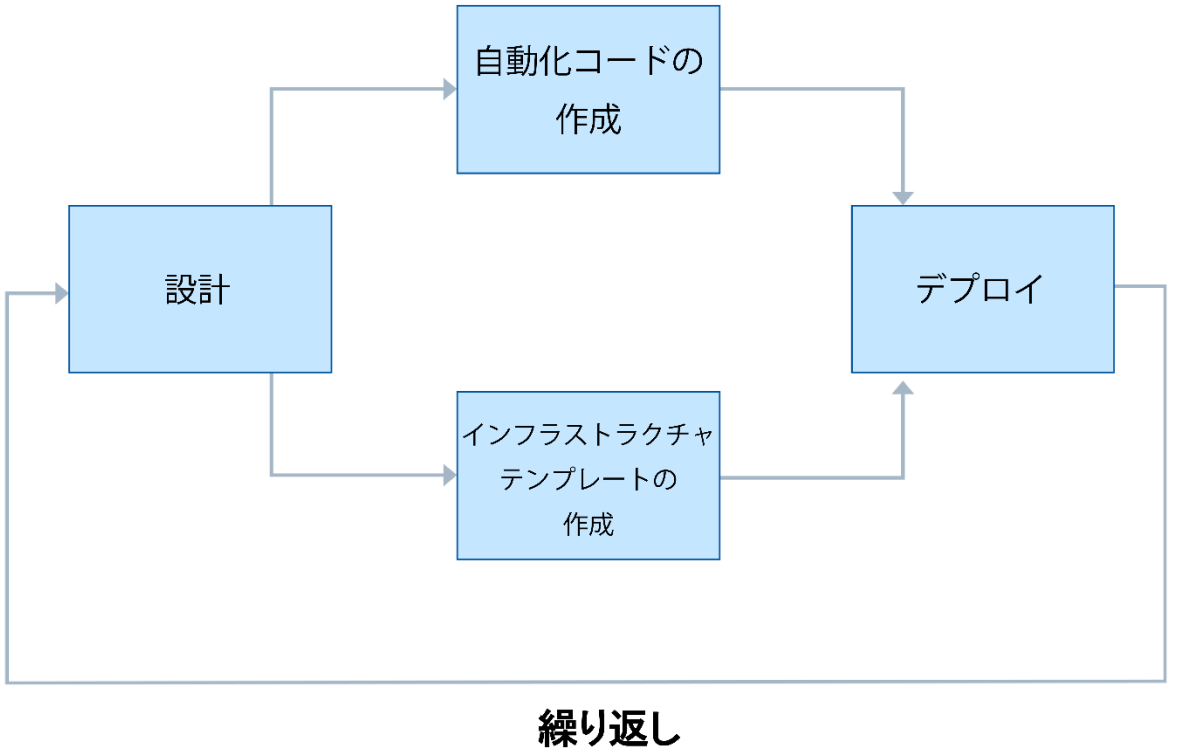


図 55: コードとしてのインフラストラクチャ:自動化によるセキュリティの強化

組織は、クラウドでの自動テストにもっと依存すべきです。IaC では、インフラストラクチャ自体がテンプレートと自動化によって定義および実装されるため、インフラストラクチャがアプリケーションテストの対象になることが多くなっています。IaC を活用すると、運用効率が向上するだけでなく、インフラストラクチャの基盤そのものにセキュリティを組み込むことで、クラウドベースのアプリケーションのセキュリティポスチャが大幅に向上します。

10.2.4 API セキュリティのベストプラクティス

API の保護に関しては、いくつかの選択肢があります。1 つの選択肢は、API ゲートウェイを使用することです。API ゲートウェイは、受信 API リクエストの認証、レート制限、およびアクセス制御を管理するための中心となるポイントとして機能します。これにより、認可されたユーザーとシステムのみが API にアクセスできるようになります。別の選択肢として、サービスメッシュを実装する方法もあります。サービスメッシュは、アプリケーション内の異なるサービス間の通信を保護することに重点を置いています。サービスメッシュは、組み込みの暗号化および認証メカニズムを提供し、サービス間を移動する機微データの保護に役立ちます。

これらの対策に加え、機微情報の漏洩を未然に防ぐために API コントラクトを慎重に定義することが重要です。API コントラクトは過度に許容すべきではなく、アクセスは必要なデータと機能のみに制限する必要があります。さらに、自動化された API セキュリティテストを CI/CD パイプラインに組み込む必要があります。これにより、開発プロセスの早い段階で脆弱性を検出できるため、迅速な修正が可能になり、セキュリティ侵害のリスクを軽減できます。

これらの保護オプションを実装し、ベストプラクティスに従うことで、組織は API のセキュリティを強化し、機微データを不正アクセスや情報漏えいから保護することができます。

10.3 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

IAM は、アプリケーションのセキュリティを強化する上で重要な役割を果たします。アイデンティティを管理し、組織内のユーザーアクセスを制限するために設計された技術とポリシーを網羅しています。IAM システムは、誰がどのリソースにアクセスでき、そのアクセスがどのように許可および取り消されるかを効果的に制御することで、適切な個人が、適切な理由で、適切なリソースに、適切なタイミングでアクセスできるようにします。IAM とアプリケーションのセキュリティ戦略を統合することは、不正アクセスを防ぎ、潜在的な脅威から機微データを保護するために重要です。

10.3.1 アプリケーションコンポーネントに対する権限の設定

IAM[152]をデジタル資産のゲートキーパーとして、各エンティティのクレデンシャルを注意深く確認してからアクセスを許可することを想像してみてください。このシステムは、クラブでの用心棒の役割と同様に、デジタル領域内で誰が入場できるかを定義し、その能力の概要を示します。

- **最小特権の原則：**自分の役割に必要なドアのみを解錠するキーカードの配布と同様にアクセス権を割り当て、機微領域への不正アクセスのリスクを最小限に抑えます。

[152] IAM is covered in detail in *Domain 5: Identity and Access Management*.

- **継続的なモニタリング**：CCTV の映像を監視するセキュリティチームと同様に、常時監視によって警戒を維持し、異常なアクセスパターンを迅速に検出して対処します。
- **職務分掌**：建物内のさまざまなチェックポイントのように複数のセキュリティレイヤーを実装して、アクセス権限の集中を希薄化することで、潜在的な悪用や侵害を回避します。これはまた、開発者が環境ごとに異なる権限を使用する必要があることを意味します(例: Dev と Prod)
- **フェデレーション**：汎用的に受け入れられているキーカードとよく似たユニバーサルアクセスプロトコルを実装することで、多様なシステムや組織間のアクセスを合理化し、クロスプラットフォームのやり取りを簡素化し、セキュアにします。

次の図は IAM プロセスを示しており、ユーザー、アイデンティティプロバイダ、およびサービスプロバイダが認証とアクセス許可を行う際の相互作用を示しています。

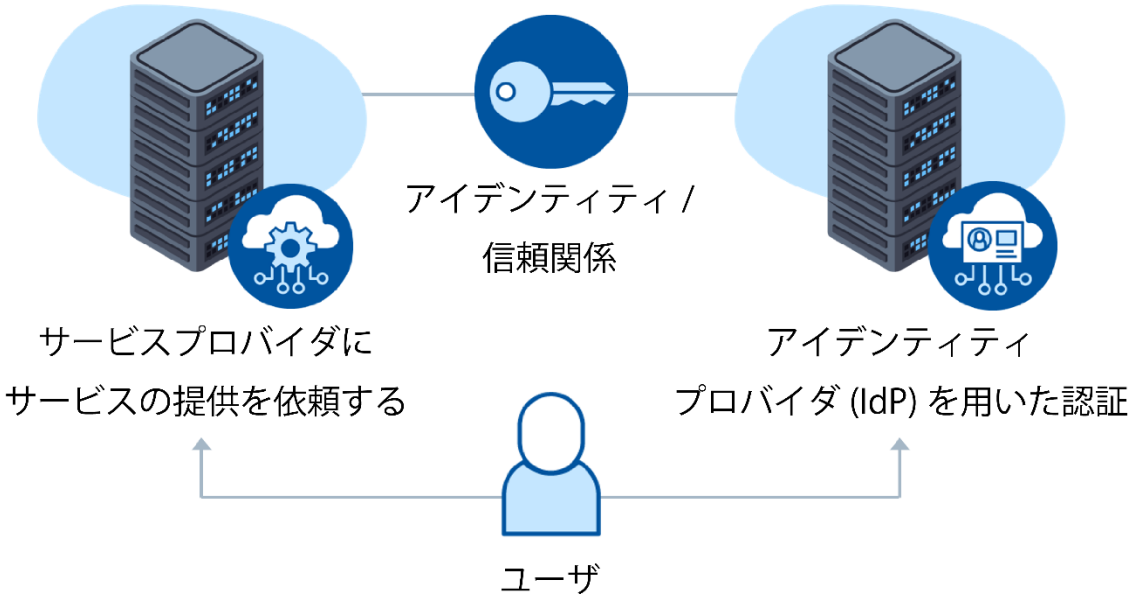


図 56: アプリケーションセキュリティのための IAM とシークレット管理

10.3.2 シークレット管理

シークレットとは、アプリケーションサービスやインフラストラクチャサービス間で、または他のサービスとの通信に使用するデジタルクレデンシャル (パスワード、キー、トークンなど)です(人間が使用するクレデンシャルとは対照的)。シークレット管理とは、それらの認証情報を安全に扱う方法です。効果的なシークレット管理により、これらのシークレット要素が安全に保存、アクセス、管理され、不正アクセスを防止し、データ漏洩のリスクを軽減します。これには、シークレット漏洩の検出とともに、アクセス資格情報を体系的に作成、配布、ローテーション、および無効にするためのツールとポリシーが含まれ、これにより、インフラストラクチャ全体のデータの完全性と機密性が保護されます。

シークレット管理の機能の一部を次に示します。

- **クレデンシャルを自動的に提供:** これは、信頼できるアシスタントが適切な鍵を適切なタイミングで提供し、サービスが人手（およびヒューマンエラー）をかけずに必要なものにアクセスできるようにすることと同じです。
- **セキュアなストレージ**： シークレットはセキュアな方法で保管します。貴重品が銀行の金庫に保管されることと同様です。
- **API との統合：** シークレットは、アイデンティティを尋ねられたときに提示するなど、自身を確認する必要がある場合に、セキュアなチャネルを介してアプリケーションに提供されます。
- **チーム間でのシークレットの共有：**チームが同じクレデンシャルを使用する必要がある場合、シークレット管理システムでは、アカウント番号を知らなくてもお金を使うことのできる共有銀行口座のように、シークレットを見ることなく使用できます。

シークレット管理は通常、組み込みまたはクライアントサーバのいずれかの方法で配備されます。どちらのモデルも、シークレット情報をセキュアに保ちながら、アプリケーションの認可された部分にアクセスできるようにすることを目的としています。組み込みモデルとクライアントサーバーモデルのどちらを選択するかは、多くの場合、スケーラビリティやセキュリティ要件など、アプリケーション固有のニーズによって異なります。王国へのデジタル鍵であるシークレットが、アプリケーションのエコシステム内で適切に保護されながらも機能していることを確実にするには、適切なモデルの選択が不可欠です。

- **組み込みモデル:** このモデルでは、シークレット管理はアプリケーションまたはシステムに直接組み込まれています。ホテルのすべての部屋に金庫があると考えてください。主に Kubernetes のようなコンテナ化された環境で見られ、アプリケーションがすべての依存関係（シークレットを含む）とともにパッケージ化されています。シークレットは一度だけ使用し、コンテナ環境内で広く共有することができますが、部屋を出るときに金庫の鍵を開けっ放しにするなど、少しオープンすぎることもあります。

- **クライアントサーバモデル:** この配備モデルにおけるシークレット管理は、複数の支店を持つ銀行に似ています。すべてのシークレットが格納される中央サーバー（メインブランチ）があり、クライアント（他のブランチ）は必要に応じてこれらのシークレットへのアクセスを要求します。このセットアップは、複数のサーバーにワークロードを分散するように設計されているため、大量のリクエストを処理できます。さらに、シークレットを異なるサーバー間で複製して、必要なときにいつでも利用できるようにし、1 台のサーバーに障害が発生した場合のバックアップを提供します。このアプローチは、セキュリティとアクセシビリティのバランスを取り、シークレットは安全であるものの、システムの許可された部分からすぐに利用できることを確実にします。

今日のほとんどのクラウドプロバイダは、静的シークレットの代替手段を提供しています。配備シナリオによっては、IAM ロール/アイデンティティをサービスに割り当てることでシークレットを回避できます。シークレットを使用しなければならないシナリオの場合、すべての IaaS/PaaS プロバイダは、シークレットを安全に保持するためのセキュアなストレージサービスを提供しています。これらは IAM と統

合され、アプリケーションコード、設定ファイル、またはその他のセキュアでないストレージにシークレットを保持する必要がなくなります。マルチクラウドとオンプレミスの導入には、サードパーティのサービスも存在します。

次の図は、鍵ペアの作成、証明書署名要求（CSR）の提出、および認証局 （CA）による発行など、X.509 証明書の生成と管理のプロセスを示しています。

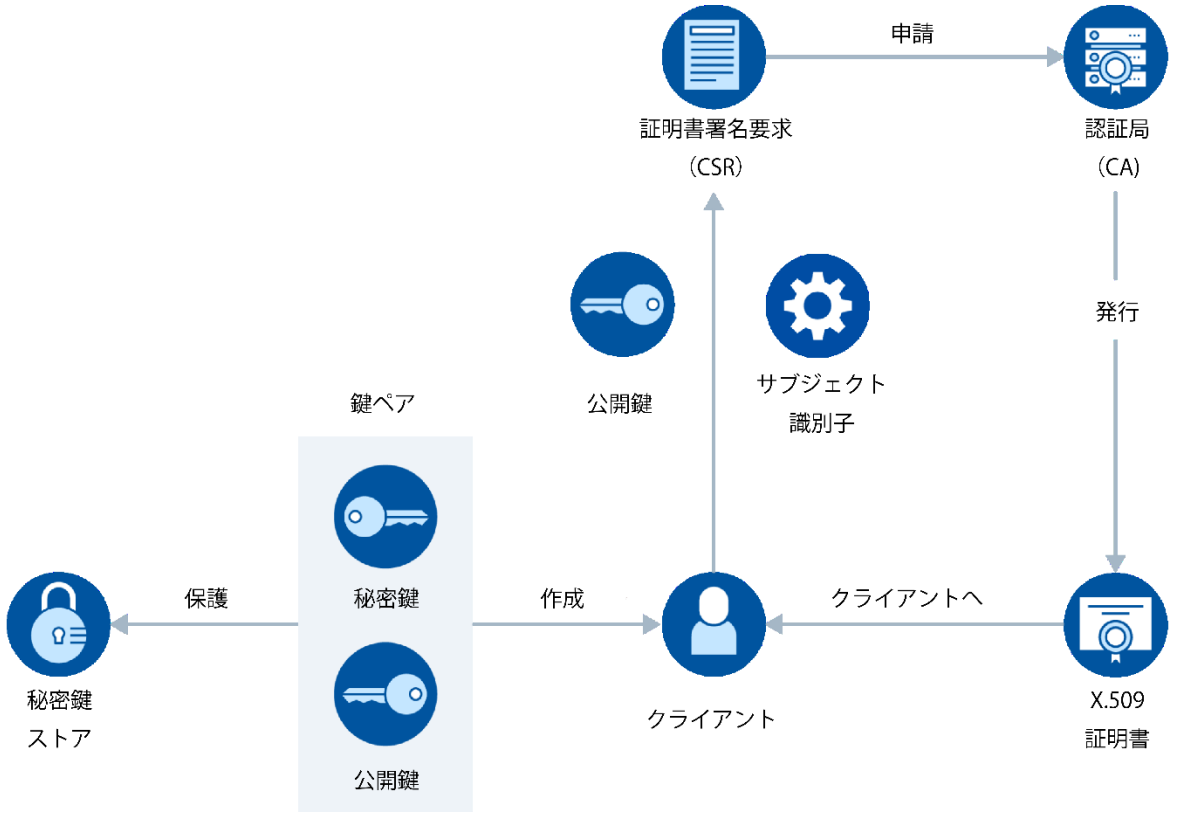


図 57: IAM とシークレットの管理プロセス

10.4 DevSecOps: CI/CD とアプリケーションテスト

DevSecOps は、SSDLC 全体のセキュリティの統合を自動化する開発、セキュリティ、および運用の略称です。DevSecOps は、DevOps パイプラインに「セキュリティ」要素を導入します。DevOps パイプラインは自動化されたプロセスとツールのセットであり、開発者と運用プロフェッショナルが協力して本番環境へのコードの構築とデプロイを行い、ソフトウェア製品を迅速に生産できるようにします。これは、CI/CD モデルを持つという概念の上に成り立っています。DevSecOps は、セキュリティの一体化を確実にすることで、この DevOps CI/CD モデルを強化します。

- **継続的インテグレーション (CI):** 開発者は頻繁にコードの変更を共有リポジトリにマージします。このフェーズ (SAST など) ではデプロイ前の自動セキュリティテストが必要です。

- **継続的デプロイメント (CD):** コードが CI ステージを通過すると、自動的にテスト環境またはステージング環境にデプロイされます。これにより、コードの変更が迅速かつ一貫して提供されるようになります。このフェーズ（DAST など）では、デプロイ後の自動セキュリティテストが必要です。

DevSecOps は、CI/CD パイプラインの初期段階からセキュリティ対策とテストの存在を強調し、アプリケーションの開発とデプロイサイクルにおいてセキュリティ上の考慮事項が不可欠であることを確実にします。このアプローチは、セキュリティチェック、スキャン、およびテストを CI/CD ワークフローに組み込むことで、コアセキュリティタスクを自動化し、コード変更の迅速かつセキュアな提供を促進することを目的としています。

10.4.1 DevSecOps

DevSecOps は、セキュリティと DevOps の俊敏なコラボレーションと自動化を融合し、ソフトウェア開発とデプロイへの総合的なアプローチを重視しています。その中核として、CI/CD を活用してプロセスを自動化および合理化し、クラウド統合をシームレスかつセキュアにします。標準化を採用することで、開発から本番環境まで、すべての環境に一貫性を持たせ、エラーの可能性を低減できます。自動テストはセキュリティチェックを CI/CD パイプラインに統合し、スピードを犠牲にすることなくセキュリティを強化します。環境を迅速かつ確実に構築するインフラストラクチャにおけるイミュータブルの概念は、自動デプロイメントをサポートし、手動変更に伴うリスクを軽減します。

さらに、監査と変更管理機能の向上により、変更の透明性とトレーサビリティが確保され、セキュリティポスチャが強化されます。DevSecOps は、セキュリティプラクティスを DevOps に統合することで、運用効率を最適化し、アプリケーションとインフラストラクチャのセキュリティレジリエンスを大幅に強化します。

次の図は、DevSecOps の CI/CD サイクルを示しています。DevSecOps の各フェーズを統合することで、継続的かつセキュアなソフトウェアの提供を実現しています。

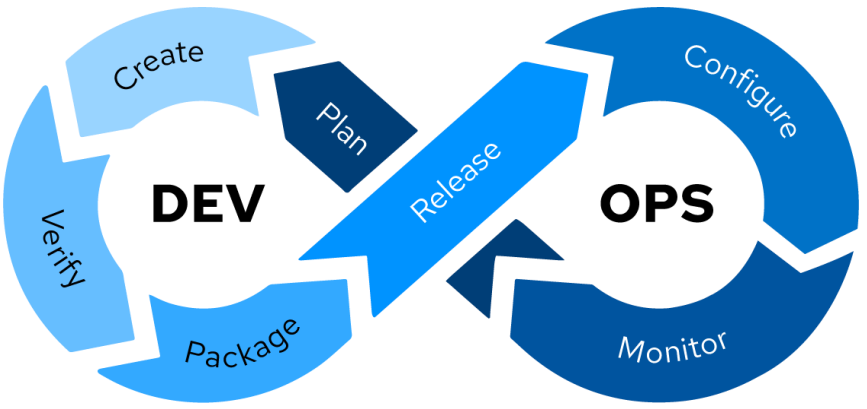


Figure 58: DevSecOps CI/CD Cycle

10.4.2 DevSecOps の 6 つの柱

DevSecOps の 6 つの柱は、セキュリティを DevOps プラクティスに統合するための包括的なフレームワークを提供し、セキュアなソフトウェアの効率的な開発を目指しています。これらの柱は、責任の共有、コラボレーション、実用的なツール、プラクティスの選択、コンプライアンスと開発の調和、エラーを最小限に抑える自動化、および実行可能な指標による継続的な改善の重要性を強調しています。それぞれの柱は、ソフトウェア開発で使用される文化、プロセス、およびツールを変革するための基盤であり、セキュリティは、立ち上げから導入までのライフサイクルに不可欠な要素です。この総合的なアプローチは、すべてのチームメンバーがプロジェクトのセキュリティポスチャに貢献する権限を与えられ、開発チーム、運用チーム、およびセキュリティチーム間の従来のギャップを埋める、プロアクティブなセキュリティプラクティスへの移行を促進します。

DevSecOps の 6 つの柱:

1. **チームとしての責任**[153]
    a. セキュリティは、全チーム共通の責任です。
    b. プロアクティブでセキュリティを意識した組織文化を醸成します。
2. **コラボレーションとインテグレーション**[154]
    a. 部門横断的なチームワークによる DevSecOps の成功に不可欠。
    b. 知識のギャップを埋め、統一されたセキュリティ意識の高い考え方を促進します。
3. **実用的な導入**[155]
    a. 組織のニーズに合ったツールとプラクティスを選択します。
    b. 開発プロセスへのシームレスなセキュリティ統合に重点を置きます。
4. **コンプライアンスと開発の橋渡し**[156]

[153] CSA. (2020) The Six Pillars of DevSecOps: Collective Responsibility.
[154] CSA. (2024) The Six Pillars of DevSecOps: Collaboration and Integration.
[155] CSA. (2022) The Six Pillars of DevSecOps: Pragmatic Implementation.
[156] CSA. (2022) The Six Pillars of DevSecOps: Compliance and Development.

a. 自動化により、コンプライアンスとアジャイルプラクティスを整合させます。

b. ソフトウェアライフサイクル内にセキュリティ対策を統合し、リスク軽減を強化します。

5. **自動化**[157]

a. DevSecOps の中心となり、プロセスの合理化とエラーの削減を実現します。

b. 効率的で一貫したセキュリティチェックを確実にし、ソフトウェア品質を向上させます。

6. **測定、監視、報告、行動**[158]

a. 継続的改善のために、測定可能で実行可能な指標を導入します。

b. デプロイメント頻度、パッチ適用時間、テスト範囲、および脆弱性対応に重点を置きます。

このフレームワークは、セキュリティを DevOps に統合するための包括的なアプローチを強調し、コラボレーション、自動化、および継続的な改善を通じてセキュアなソフトウェア開発を保証します。

10.4.3 DevSecOps の実際

DevSecOps を実際に機能させるための提供された概念を拡張し、セキュリティを DevOps プロセスにシームレスに統合するための構造化されたアプローチを開発します。

- **検出:**警戒心の強い番兵（sentinel）のように機能するリアルタイム監視システムを導入し、セキュリティの課題、脅威、または設定ミスをできるだけ早くスキャンして特定し、迅速な対応を確実にします。

- **自動化：**技術を活用して、パッチの導入から構成の管理まで、独立して動作するスマートシステムと同様に、繰り返し行われるセキュリティタスクを自動化し、セキュリティ対策を常に最新の状態に保ち、一貫した方法で実施できるようにします。
- **配送:**効率的で直接的な通信プロトコルを確立し、使い慣れたツールを通じてセキュリティアラートが適切な専門家に届くようにすることで、チームのアクションの応答時間と有効性を最適化します。
- **修正:**日常的な清掃がレストランの衛生基準を維持することと同じように、セキュリティのメンテナンスを日常業務に統合し、セキュリティの課題を定期的かつプロアクティブに解決します。

[157] CSA. (2020) The Six Pillars of DevSecOps: Automation.

[158] CSA. (2024) The Six Pillars of DevSecOps: Measure, Monitor, Report, and Action.

これらの主要な要件に従うことで、組織は日常業務にセキュリティを組み込むことができ、セキュリティと開発が連携してセキュリティポスチャを継続的に維持および改善する文化が醸成されます。

10.4.3.1 シフトレフトとビルドセキュリティイン

SSDLC を水平的なステップのプロセスとして捉えた場合、セキュリティはほとんどの場合、最後のステップであるメンテナンスフェーズでのみ存在していました。それは、本番アプリケーションでセキュリティインシデントが発生した後の事後対応策としてです。シフトレフトとは、セキュアバイデザインおよびセキュアバイデフォルトの製品を確保するために、SSDLC でセキュリティをより早いフェーズに移行する必要があることを示すために使用される語句です。シフトレフトは、SSDLC の開始から計画までの各フェーズをセキュリティのレンズを通した確認を確実にすることで、プロアクティブなセキュリティを推進します。このアプローチは、SSDLC の後のフェーズでボルトオンセキュリティを導入することに比べてもコスト効果に優れています。

次の図は、DevSecOps モデルにおける、アーキテクチャと開発から本番環境までのさまざまな開発フェーズにわたるセキュリティの統合の概要を示しており、継続的なセキュリティテストとモニタリングに重点を置いています。

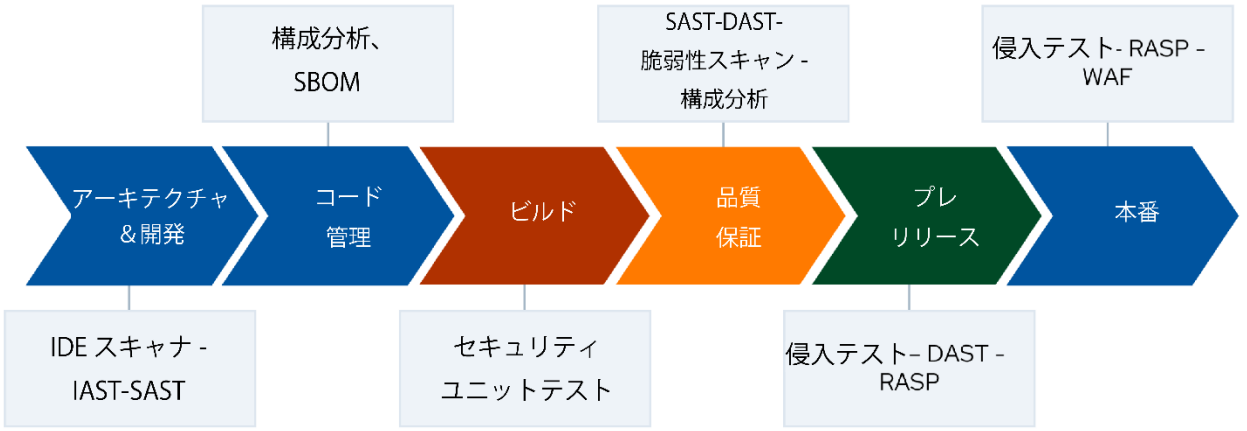


図 59: DevSecOps:開発フェーズ間のセキュリティの統合

シフトレフトは脆弱性の早期発見にも役立ちます。シフトレフトセキュリティツールは、完全に構築された製品のテストを待つことや、脆弱性をエクスプロイトする攻撃者が野放しになった一層深刻な状態となることを待つのではなく、開発者が脆弱性を早期に発見して修正できるようにすることで、開発プロセス全体を強化し、レジリエンスのある製品を作り出すことができます。

次の表は、SSDLC のさまざまな段階で適用されるプロアクティブなセキュリティ対策をまとめたもので、特定のセキュリティ手法が実装されている場所とその目的に焦点を当てています。

WHERE?	WHAT?	WHY?
IDE（統合開発環境）	SAST	ソースコードの脆弱性を検出し、コーディング時に開発者にリアルタイムのフィードバックを提供
リポジトリ	Software Composition Analysis (SCA)	脆弱な依存関係とライブラリの検出
ビルドフェーズ	セキュリティユニットテスト	モジュールレベルのセキュリティ脆弱性を検出
品質保証フェーズ	SAST IAST DAST	静的コードと動作の脆弱性を検出
プレリリースフェーズ	DAST	オペレーションの脆弱性を検出
プロダクション	Web Application Firewall (WAF) Runtime Application Security Protection (RASP)	攻撃の監視と防御

図 9: SSDLC 全体のプロアクティブなセキュリティ対策

10.4.3.2 SecOps: Web アプリケーションファイアウォールと DDoS

Web アプリケーションは、配備後も堅牢なセキュリティ対策が求められます。ゲートウェイサービス、分散型サービス拒否（DDoS）保護、および Web アプリケーションファイアウォール（WAF）の実装が不可欠です。これらのツールは、アプリケーションを正規のユーザーがアクセスできる状態を維持し、Web トラフィックの流入を効率的に管理でき、過負荷による潜在的なクラッシュからの保護を確実にするように設計されています。WAF は予防的管理策であり、是正管理策または下手に開発されたアプリケーションの保護として使用してはならないことを強調することが重要です。先に説明したように、SSDLC では常に左側にセキュリティを持ってくることを忘れないでください。

IaaS/PaaS サービスにおける WAF と DDoS 保護には、次の 4 つの一般的な導入シナリオがあります。

1. **エージェントの導入:** IaaS VM を Web サーバーとして使用する場合は、OS 上に WAF Agent をインストールできます。このオプションには通常、DDoS 軽減機能はありません。
2. **クラウドプロバイダーサービス：** IaaS/PaaS プロバイダは、WAF と DDoS の統合保護サービスを提供しており、通常はロードバランサーサービス上に配備されます。

3. **サードパーティマーケットプレイスサービス:** IaaS/PaaS マーケットプレイスでは、専用の VM に配備されるさまざまなサードパーティ製商用 WAF ソフトウェアを提供しています。WAF の配備並びにルーティング、冗長性、およびロードバランシングの確保は、利用者の責任となります。

4. **WAF と DDoS as a Service**:DNS リダイレクトを使用して、コンシューマートラフィックはサードパーティの WAF サービスにルーティングされ、検査とフィルタリングが行われ、その後クラウドプロバイダー環境にルーティングされます。

次の図は API Gateway のセキュリティアーキテクチャを示しており、WAF と DDoS 保護の統合により、Web トラフィックを安全かつ効率的に管理できることを強調しています。

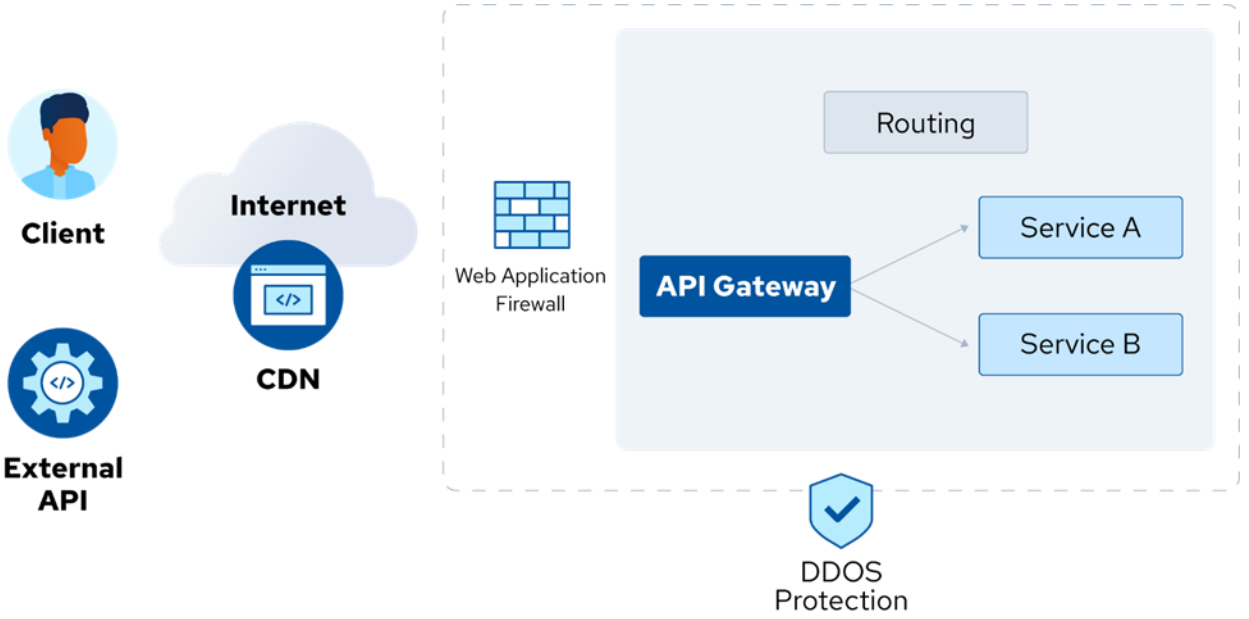


図 60: API ゲートウェイのセキュリティアーキテクチャ

10.5 サーバーレスとコンテナ化アプリケーションに関する考察

進化するアプリケーション展開環境において、サーバーレスコンピューティングとコンテナ化の重要性は高まっています。サーバーレスコンピューティングにより、基盤となるインフラストラクチャを管理せずにアプリケーションを構築でき、拡張性とコスト効率が向上します。一方、コンテナ化はアプリケーションを一貫した環境にカプセル化し、移植性を強化します。どちらの技術も、独自の利点を持つ最新の導入手法を形成するため、それぞれの固有のセキュリティの意味を理解する必要があります。このセクションでは、その両方について説明します。

10.5.1 サーバーレスおよびコンテナによるアプリケーションセキュリティへの影響

進化するアプリケーション配備のランドスケープでは、サーバーレスおよびコンテナ技術がセキュリティプラクティスを再構築しています。セキュリティ対策と戦略は、これらの新しい環境に適応する必要があり、それぞれに固有の考慮事項があります。これらの考慮事項を理解することは、配備手法の進歩に伴ってアプリケーションのセキュリティを維持するために重要です。

10.5.1.1 サーバーレスに関する考慮事項

サーバーレスの考慮事項の例を次に示します。

- **アタックサーフェスの減少**：永続的なストレージを使用せずに単一の短命な操作を実行するというサーバレス機能の一時的な性質は、本質的に攻撃に露出される可能性を制限します。
- **依存関係リスク**：外部コードやサービスへの依存は、製品の製造時に安全性の記録が不明なサードパーティコンポーネントを使用することと同様に、セキュリティリスクをもたらします。
- **IAM の複雑**さ：サーバーレス機能のエフェメラルかつ分散的な性質により、常に変化する多数のアクセスポイント間でセキュリティを維持することに匹敵する複雑なアクセス管理が必要になります。

10.5.1.2 コンテナに関する考慮事項

コンテナに関する考慮事項の例を次に示します。

- **隔離のリスク**: コンテナ化された環境での隔離が不十分だと、セキュリティ侵害につながる可能性があります。これは、コネクテッドルームのバリアが不十分で、侵入者が簡単に通行できてしまうのと同様です。
- **イミュータブルインフラストラクチャ**：コンテナは配備後にイミュータブルとなるように設計されており、一貫性を促進し、改ざん防止パッケージを活用する場合のようにリスクを軽減します。
- **複雑な構成管理**：規模が大きくなると、複数の施設にまたがる高度なセキュリティシステムの複雑なネットワークを監視することと同様に、コンテナの複雑なセキュリティ構成の管理が困難になります。

次の図は、コンテナ化されたアプリケーションで堅牢なセキュリティを維持するために不可欠な、コード、ランタイム、ライブラリ、環境、構成といった、コンテナのセキュリティに関する主な考慮事項を示しています。

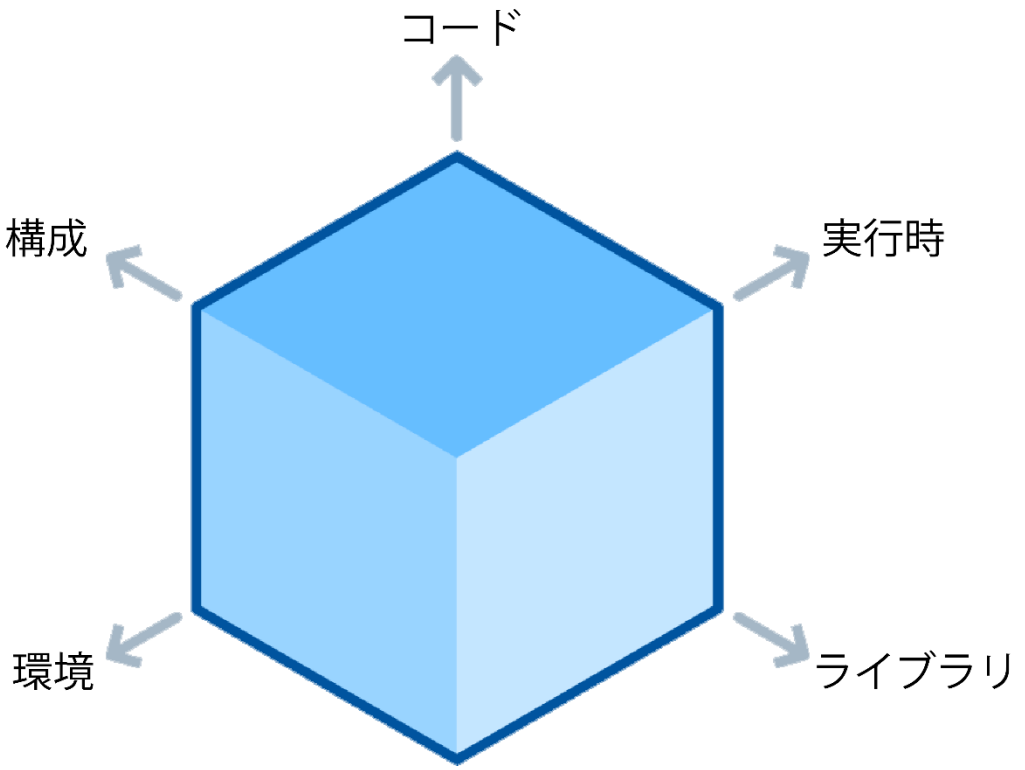


図 61: コンテナの考慮事項

サマリ

クラウドコンピューティングは、アプリケーションセキュリティの進歩を牽引する大きな要因であり、その進歩には安定性、拡張性、およびセキュリティが求められます。セキュア開発ライフサイクルは、セキュアなクラウドアプリケーションの構築と維持に役立つ必須の技法と方法論のガイドラインを提供します。

進化し続けるサイバー脅威に対してデジタルエコシステムを真に強化するには、クラウドコンピューティング戦略の中核にアプリケーションセキュリティの原則を組み込むことが重要です。これには、最初の設計段階から配備、継続的なメンテナンスに至るまでのセキュリティの統合が含まれます。

主な要素は次のとおりです。

- **セキュアなアーキテクチャ：** セキュリティ対策を設計フェーズに組み込んでセキュアな基盤を構築することで、潜在的な脅威に対する強固な保護を実現します。

- **アイデンティティとアクセス管理（IAM）**：アプリケーションによって処理されるビジネスデータを保護するためのシークレット管理ポリシーの導入は不可欠です。IAM とシークレット管理は、ともにアクセス制御とデータ保護戦略のバックボーンを形成します。
- **DevSecOps:** DevSecOps の統合は、開発ライフサイクル全体を通じたアプリケーションセキュリティへの取り組みを強調しています。このアプローチは、サーバレスコンピューティングやコンテナ化などの最新の導入手法で特に重要です。
- **継続的なモニタリングと改善：** 継続的なモニタリング、脅威モデリング、および自動セキュリティテストの採用により、脆弱性を早期に特定して軽減し、レジリエンスの高いアプリケーションセキュリティポスチャを確保できます。

これらのガイドラインに従い、Cloud Security Alliance （CSA）の推奨事項を活用することで、組織は、クラウドコンピューティングがもたらす固有の課題と機会に対応する、セキュアでレジリエンスがあり、スケーラブルなアプリケーション環境を構築できます。

推奨事項

CSA セキュア開発ライフサイクル (SSDLC):

- **セキュアなデザインとアーキテクチャ**：設計段階で技術とツールを適用することで、セキュリティを早期に統合し、後のコスト増加やボトルネックを回避します。
- **継続的ビルド、統合、テスト**：配備前に脆弱性をテストするツールとプロセスを採用し、セキュリティ侵害を防止します。
- **継続的なデリバリーとデプロイメント**：配備前の安全性チェックを実施し、アプリケーションがセキュアなインフラストラクチャに配備されることを確実にします。
- **ランタイムの防御とモニタリング**：導入後の脆弱性や非効率性を継続的に特定し、軽減するためのプラクティスを導入します。

構造化脅威モデリングの採用:

- STRIDE フレームワークを適用して脅威を分類します：スプーフィング、改ざん、否認防止、情報開示、サービス拒否、および特権の昇格。

セキュアなクラウド設計に注力:

- Platform as a Service（PaaS）やその他の CSP サービスを使用して、セキュリティ責任をプロバイダにオフロードします。
- すべてのコンポーネントに最小特権のアイデンティティとアクセス管理（IAM）を実装します。
- ロードバランサーやセキュリティグループなどの CSP サービスを利用すると、インターネットへの露出を最小限に抑えることができます。

セキュリティテスト方法の統合:

- **静的アプリケーションセキュリティテスト**（SAST）：コードレビューを自動化して、配備前に脆弱性とロジックエラーを特定します。
- **ソフトウエア構成分析**(SCA)：外部コンポーネントの脆弱性とライセンスのリスクを監査し、透明性のためにソフトウェア部品表（SBOM）を作成します。

配備後の包括的なテストの実施:

- **動的アプリケーションセキュリティテスト**（DAST）：ブラックボックステストを実行して、アプリケーションのセキュリティポスチャを外部の視点から評価します。
- **動的解析(ファジング)**：想定外なデータを入力し、運用中のエラーや脆弱性を特定します。
- **Interactive Application Security Testing (IAST)**：SAST と DAST を組み合わせて、コードと実行時の両方で脆弱性を特定します。
- **侵入テスト**：既知の脆弱性をエクスプロイトする疑似攻撃を実施し、システムのレジリエンスをテストします。
- **バグバウンティプログラム**:倫理的なハッカーコミュニティを活用して、脆弱性を発見して報告します。

アクセス制御の強化:

- 最小特権の原則を適用して、不正アクセスを最小限に抑えます。
- 異常なアクセスパターンを検出して対処するための継続的なモニタリングを実装します。
- 職務分掌を用いてアクセス権限を希薄化し、誤用を防ぎます。
- フェデレーションを採用して、クロスプラットフォームのやり取りを効率化し、セキュリティを確保します。

シークレット管理:

- クレデンシャルを自動的に提供し、人的ミスを最小限に抑えます。
- 金庫室の貴重品と同様に、シークレットをセキュアに保管します。
- セキュアなチャネルを介して API とシークレットを統合します。
- 共同名義の銀行口座のように、シークレットを漏らすことなく、シークレットの共有を容易にします。

CI/CD パイプラインへのセキュリティの統合:

- セキュリティチェックが組み込まれた継続的な統合と配備を実装します。
- SSDLC の早い段階で脆弱性を特定して対処するには、シフトレフト戦略を使用します。
- 繰り返し行われるセキュリティタスクを自動化し、一貫した実施とタイムリーな更新を実現します。
- 開発チーム、運用チーム、セキュリティチーム間のコラボレーションを促進します。

最新の導入環境に適応したセキュリティ戦略:

- サーバーレスに関する考慮事項:
  - 短期的なサーバーレスファンクションのアタックサーフェスの減少を活用します。
  - 依存関係のリスクに対応し、複雑な IAM 要件を管理します。
- コンテナに関する考慮事項:
  - セキュリティ侵害を防ぐために、堅牢な分離を確保します。
  - イミュータブルインフラストラクチャを使用して、一貫性とセキュリティを促進します。
  - コンテナの配備規模に応じて、複雑なセキュリティ構成を管理します。

追加のガイダンス

- Six Pillars of DevSecOps | CSA
- Information Security Management through Reflexive Security | CSA
- FaaS Serverless Control Framework (Set) based on NIST 800-53 R5 Controls | CSA
- The Six Pillars of DevSecOps - Pragmatic Implementation | CSA
- Recommendations for Adopting a Cloud-Native Key Management Service | CSA
- Security Guidelines for Providing and Consuming APIs | CSA
- C-Level Guidance to Securing Serverless Architectures | CSA
- The Six Pillars of DevSecOps: Collective Responsibility |CSA

ドメイン 11: インシデントレスポンスとレジリエンス

はじめに

インシデントレスポンス（IR）は、どのような情報セキュリティプログラムにおいても重要な要素です。セキュリティポスチャの強度にかかわらず、いずれセキュリティ侵害が発生する可能性が高いからです。多くの組織では攻撃調査のための IR 計画を策定していますが、クラウド適応ではプロセス、技術、およびガバナンスに明確なばらつきが生じ、インシデントへの対応が複雑になります。

このドメインは、セキュリティ専門家が独自のインシデント計画とプロセス を開発する際に参照できるクラウドインシデントレスポンス（CIR）とレジリエンスのベストプラクティスを特定し、説明することを目指しています。このドメインは、 CSA Cloud Incident Response Framework[159]と NIST Computer Security Incident Handling Guide (NIST SP 800-61 Rev.2)[160]に記載されている、一般的に受け入れられている IR ライフサイクルに従って編成されています。その他、CSA incident response research hub[161]や ISO/IEC 27035 ENISA Strategies for IR and cyber crisis cooperation[162]など、IR に関するその他の国際標準フレームワークもリソースに含まれます。セキュリティ担当者は、IR ライフサイクルにおいて IR 計画の策定やその他の活動を行う際に、これらを参考にすることができます。

学習目標

このドメインの学習目標は、読者に以下の知識を提供することです。

- イベント、インシデント、および侵害を区別し、対応プロセスを使用して対応します。
- インシデントへの準備と対応。
- 関連データの検出と分析。
- 封じ込め、根絶、回復。
- 障害に対するレジリエンス計画の実行。

[159] CSA. (2021) Cloud Incident Response Framework.
[160] NIST. (2012) Computer Security Incident Handling Guide. Comment period for potential revisions closed mid-2024.
[161] CSA. (2024) CSA Research landing page.
[162] ENISA. (2024) Cyber Crisis Management.

11.1 インシデントレスポンス

IR とは、予期せぬ出来事に対処することです。そのためには、イベント、インシデント、および侵害を明確に区別する必要があります。これらはそれぞれ脅威のレベルが異なっており、それぞれに合わせた対応戦略が必要です。これらの事象を正確に認識して分類することは、クラウドサービスの完全性、可用性、および機密性を維持し、最終的には、利害関係者のデジタル資産と信頼を保護する上での基礎となります。

クラウドセキュリティのコンテキストにおける*イベント*とは、システムやネットワーク内で観察可能な事象のことであり、セキュリティに関連する根本的な課題を示している場合と示していない場合があります[163]。すべてのインシデントはイベントですが、明示的または暗黙的なセキュリティポリシーに違反し、通常の運用を危険にさらしたり、クラウド環境に脅威を与えたりしない限り、すべてのイベントがインシデントになるわけではありません。インシデントは、その影響を封じ込め、軽減し、拡大を防止する早急な対応を必要とします。頂点に位置するのは、不正アクセスやデータ流出につながる、侵入の成功やセキュリティ対策への回避による侵害です。イベントからインシデント、侵害に至る段階を把握することで、効果的な IR 戦略を構築します。

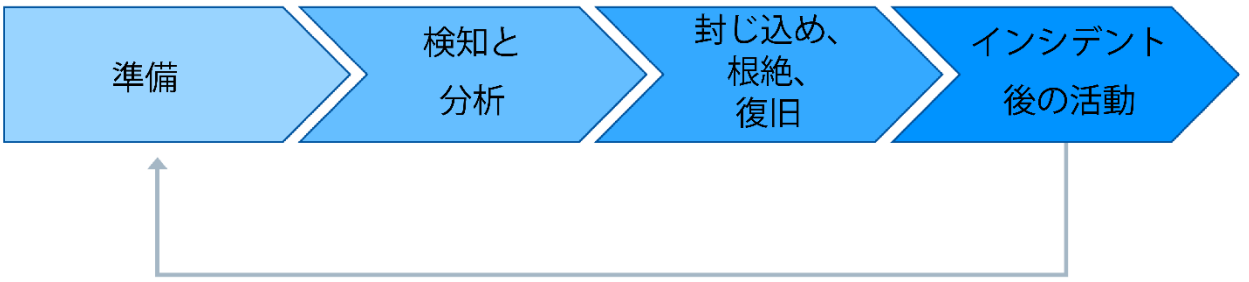
11.1.1 インシデントレスポンスライフサイクル

IR とマネジメントのフレームワークは、多くの組織によって開発され、文書化されています。フレームワークによって目的や対象読者は異なります。CSA は、 NIST Computer Security Incident Handling Guide (NIST 800-61 rev2 08/2012)[164]に記載されているインシデントレスポンスライフサイクルの一般的に受け入れられているフレーズを採用しています。
IR ライフサイクルは、クラウドの利用者がクラウドインシデントに効果的に備え、管理するための頼りになるガイドとして機能します。NIST が説明する IR ライフサイクルには、以下のフェーズと次の主な活動が含まれます：準備、検知と分析、封じ込め、根絶と回復、およびインシデント後の活動[165]。

[163] Additional detail on events is covered in Domain 6: *Security Monitoring*.

[164] NIST. (2012) Computer Security Incident Handling Guide. Comment period for potential revisions closed mid-2024.

[165] The Incident Response Life Cycle is described in the CSA Cloud Incident Response Framework and NIST 800-61rev2. This content focuses on incident response for the cloud environment, however, while cloud IR is primarily separate, it often overlaps with traditional IR. Responders focused on both environments should work closely together using this consistent response process.



NIST 800-61 rev2 に基づく（ポストモーテムをインシデント後の活動へ置き換え）

[166]

図 62: クラウドセキュリティにおける IR ライフサイクルのフェーズ

準備： IR プロセスを確立します。

- 役割と責任を割り当てたチームを作ります。トレーニングを含め、演習を実施します。
- コミュニケーション計画と設備を確立します。
- インシデント分析サービス、ハードウェア、ソフトウェアなどの環境やツールへのアクセスをレスポンダーに許可します。
- 社内文書(ポートリスト、資産リスト、ネットワークトラフィックのベースライン)を作成します。
- インフラストラクチャの評価:　プロアクティブなスキャンとモニタリング、脆弱性とリスクの評価。
- サードパーティの脅威インテリジェンスサービスを購読します。
- 利用するサービス/リソースに関する IR に役立つクラウドサービスプロバイダとその能力を評価します。
    - 監査ログ、スナップショット、フォレンジック機能、および電子情報開示機能。
- IR 計画が最新かつ効果的であることを確実にするために、バックアップ復元テストを定期的に実施し、DR テストを年に 1 回以上実施します。

検知と分析： セキュリティインシデントを特定し、その影響を分析します。

- 検知エンジニアリングを実施します。
- Cloud Security Posture Management（CSPM）、Security Information and Event Management（SIEM）、ワークロード保護、およびネットワークセキュリティ監視のアラートを活用します。
- アラートを検証し、誤検出とエスカレーションを削減します。
- インシデントの範囲を予測します。
- インシデントマネージャを割り当てて、今後のアクションを調整します。
- 攻撃のタイムラインを構築します。
- 潜在的なデータ損失や影響の範囲を特定します。

[166] NIST. (2012) Computer Security Incident Handling Guide, Figure 3-1. Incident Response Life Cycle, Page 21.

- 適切なチャネルを通知し、アクティビティを調整します。
- インシデントの封じ込めと復旧状況を経営幹部に伝えます。

封じ込め、根絶、回復：インシデントを切り分けて被害の拡大を防ぎ、根本原因を解決します。影響を受けたシステムを復旧および復元します。

- 封じ込め:　アイデンティティやワークロードを分離し、システムやサービスをオフラインにし、データ損失とサービスの可用性を考慮します。
- 根絶と回復：侵害された資産をクリーンアップし、システムとサービスを通常の運用に復元します。類似のインシデントを防止するコントロールを配備します。
- インシデントデータのキャプチャ：インシデントを記録し、フォレンジックの証拠（管理の連鎖（Chain of Custody））を収集します。

インシデント後の活動[167]**:**インシデントから学び、文書化し、今後の対応を改善します。

- 得られた教訓:　何がもっとうまくできたでしょうか？もっと早く攻撃を検知できたでしょうか？攻撃をより迅速に切り分けるために、どのような追加データが役立ったでしょうか？IR プロセスの変更は必要でしょうか？もしそうなら、どのように？
- 教訓の共有：より広範なセキュリティコミュニティと教訓を共有します。

クラウドはすべての IR フェーズの活動に影響を与え、新たなメリットと課題をもたらします。同時に、多くのインシデントがクラウドと従来のインフラストラクチャやデバイスにまたがって発生する可能性があるため、インシデントレスポンダーは、インシデントの一面のみに目を向けず、視野狭窄に陥らないようにする必要があります。

11.2 準備

準備フェーズは、次のセクションで詳しく説明する以下の 4 つの主要なカテゴリに分けることができます。

- クラウドプロバイダとの関係性による変更
- レスポンダートレーニングの変更
- CIR プロセスをサポートするために必要な変更
- CIR 技術をサポートするために必要な変更

準備フェーズは、多くの場合、CIR プログラムを開始する上で最も困難な部分です。IR プロセスの基本は変わりませんが、クラウドコンピューティングの技術面と運用面の違いは、プロセスの仕組みに大き

[167] Some incident response framework versions describe a postmortem phase that the industry now refers to as *Post-Incident Analysis*. CSA, NIST, and other industry authoritative bodies follow this change in nomenclature.

な影響を与えます。準備段階でこれらの違いを考慮しないと、効果的な対応能力が厳しく制約されます。

CIR の主な違いを次に示します。

- クラウドの運用は、個々のチームが独自のインフラストラクチャを定義して管理するため、分散化が進む傾向にあります。これはアクセスとテレメトリ収集の課題につながります。
- すべてのクラウドプラットフォームは、最も基本的な技術レベルで互いに深く異なります。IR には、適切で互換性のあるツールと、各分野の深い専門知識が必要です。
- クラウド攻撃は高度に自動化され、信じられないほど迅速に発生します。クラウドリソースは、単一の構成変更だけで、簡単にインターネット上に公開したり、共有したりされます。これは、特定のインシデントタイプに関して極めて迅速な対応が必要で、24 時間 365 日の迅速な対応機能のサポートを可能とするプロセスおよび技術的な変更が必要になる場合があります。
- レスポンダーは多くの場合、影響を受ける配備やリソースをオンデマンドで広範囲に直接アクセスする必要があります。クラウドインシデントを完全に分析して対応するには、通常、ログアクセスだけでは不十分です。アナリストおよびレスポンダーは、ログに表示される内容のコンテキストを迅速に理解する必要があり、これには、アプリケーションプログラミングインターフェイス（API）または Web UI を通じて構成とリソースを直接確認することが含まれる可能性が高いです。

11.2.1 インシデントレスポンスの準備とクラウドサービスプロバイダ

クラウドインシデントは、影響を受けるリソースのすべてを利用者が所有している場合でも、共有インシデントです。パブリッククラウドを使用したインシデントでは、特定のサービスレベル合意書（SLA）を含む契約上の取り決めと、プロバイダが提供するリソースを把握する必要があります。プロバイダとの関係によっては、直接の窓口がなく、標準サポートを通じて提供されるものに限定される場合があります。多くのプロバイダにはさまざまなサポートレベルがあります。サービスのビジネス上の重要性に適したサポートレベル(例えば、ビジネスクリティカルな配備に関する直接の連絡や迅速なサポート、あるいは、機密性の高いまたは規制を受けるデータの配備など)に加入すべきです。
有料サポートに加えて、一部のプロバイダは追加費用なしで利用者にある程度の IR サポートを提供します。利用するプロバイダごとに、インシデントサポートオプション（有料と無料）のリストと、それぞれの連絡先を用意することが重要です。これはクラウド配備レジストリに統合する必要があります[168]。

プロバイダは、ある時点で、リソース/配備に関連するインシデントを検出する可能性があります。したがって、各配備およびプロバイダでは、連絡先情報を常に最新の状態に保ち、デフォルトの受信者の 1 人として自組織のセキュリティチームに確実にルーティングすることが重要です。

これらの通知は、次のカテゴリに分類される傾向があります。

[168] Cloud deployment registry is covered in detail in *Domain 2: Cloud Governance*.

- プロバイダが、あなたのリソースが他人へ危害を加えるために使用されている可能性を検出すると、不正使用に関する通知が送信されます。これらは必ずしも正確ではなく、検証が必要になることに注意してください。
- 公開コードリポジトリに投稿された私的なアクセスクレデンシャルの検出など、リソース内のセキュリティ露出の通知。
- 侵害を示す可能性のある不審な活動の通知。
- 利用者のデータまたはリソースに影響を与える可能性のある、クラウドプロバイダでのインシデントの通知（例えば、プロバイダが侵害を受けた、攻撃の成功を検出した、データ露出が発生した、など）。
- クリックスルーサービスの場合、通知は登録メールアドレス宛てに送信される可能性があります。これらの通知は企業が管理し、継続的に監視される必要があります。

この段階では、プロバイダに影響し、自分の手に負えないインシデントに備えることも重要です。たとえば、プロバイダに影響を与える、公開された脆弱性やサービス拒否攻撃の事例が文書化されています。利用者として、必ずしも無力なわけではありませんし、インシデントの内容によっては、自分で対応できる活動があるかもしれません。IR チームはこのリスクを把握し、それに対応するいくつかのシナリオと関連する緩和策を計画する必要があります。これには通常、事業継続活動との調整が必要になります。

11.2.2 クラウドインシデントレスポンダーためのトレーニング

CIR プラクティスは従来の IR プラクティスと多くの特性やプロセスを共有していますが、レスポンダーはプロセスや技術の違いを理解する必要があります。

訓練とさまざまな演習を組み合わせることで、レスポンダーやチームは次のような必要スキルを迅速に習得できます。

- 汎用的な CIR トレーニングは、複数のクラウドプロバイダ間をまたがって機能する基礎スキルの構築に役立ちます。これは、クラウドインシデントに専従しないレスポンダーでもクラウドの認知度を向上させるための良い選択でもあります。
- プロバイダ固有の技術トレーニングは、主要なプラットフォーム、特に IaaS で作業するレスポンダーにとって不可欠です。このトレーニングは、プロバイダが提供する IR ツールだけを使用するのではなく、露出されたサービスクレデンシャルの検疫方法、ログの分析方法など、深い部分まで踏み込む必要があります。
- シミュレーション環境でのシナリオベースの演習は、ログ分析、脅威ハンティング、およびリソース検疫などのコアスキルでの練習に役立ちます。
- フル演習とレッドチーミングは、IR プロセス全体をテストするように設計されています。
- 分散クラウドチームとリーダーシップによる机上演習は、さまざまなチームが連携して取り組みを調整できることを確実にするために役立ちます。机上演習には、プロバイダ侵害などの大規模インシデントのシミュレーションが含まれる場合があります。

11.2.3 クラウドインシデントレスポンスプロセスをサポートするアップデート

IR プロセスの中核部分はあまり変わりませんが、IR チームはその違いをある程度考慮してプロセスを調整したいと思うかもしれません。標準的な IR ランブック[169]やプレイブック[170]は、ほとんどのクラウドインシデントに対して最適化されていません。ネットワークパケットキャプチャ、フォレンジック、およびその他のアクティビティに焦点を当てる傾向があり、クラウドに必要な場合でも、Identity and Access Management（IAM）やマネージメントプレーンの権限昇格がなかったことを確認するなどといった他の優先事項の後に行われます。予想されるクラウド特有のインシデントタイプに合わせて新しいプレイブックとランブックを作成する必要があります。クラウドのプレイブックとランブックには、ハイブリッド接続を介してデータセンター内のリソースにまで及ぶクラウド侵害や、侵害されたクラウドリソースに対するマルウェア分析など、スキルとプロセスの両方のセットが必要なインシデントに対して、CIR 以外のエキスパートとプロセスを関与させるタイミングを含める必要があります。

オンプレミスプレイブックとランブックも、2 つの主要なインシデントタイプに合わせて更新する必要があります。まず最初に、非クラウド攻撃で攻撃者が取得したクラウドクレデンシャルの露出と悪用が検出されます。次に、非クラウド環境のサーバーやワークステーションなどの侵害されたリソースからクラウドリソースへ攻撃します。プロセスとして、新しいタイプのインシデントの後に、そのインシデントタイプに対応するプレイブックまたはランブックを作成するという要件があるはずです。厳密にクラウドでない限り、従業員のデバイスが関係するインシデントなど、クラウドと従来のインフラストラクチャを橋渡しするインシデントが発生します。したがって、クラウド専任のレスポンダーがいる場合、両方の環境にまたがるハイブリッドインシデントを処理するプロセスが存在することを確実とすることが重要です。

ビジネス継続、リーダーシップ、法務、およびコンプライアンスの各チームは、クラウドインシデントにおける役割を理解し、それに応じてプロセスを調整する必要があります。クラウドプロバイダによる利用者データの露出は、危機コミュニケーションや法的および規制要件が異なります。プレイブック、ランブック、および全体的なプロセスを含むレスポンスプロセスは、マネージメントプレーンが関係するクラウドインシデントの影響に特に注意を払う必要があります。今日の攻撃者は、マネージメントプレーンに侵入して特権を昇格する可能性があります。レスポンダーが侵害された仮想マシン（VM）などのクラウドリソースだけに注目すると、攻撃の最も被害の大きい側面を見逃す可能性があります。攻撃者による自動化により、クラウドインシデントは目を見張るほど高速になる可能性があります。プロセスはこの速度の違いを考慮する必要があります。たとえば、インシデントハンドラーが 15〜60 分前のログデータを処理している場合、リアルタイムのクラウドインシデントに効果的に対応することはできません。

11.2.3.1 レスポンダーアクセスを有効にする

[169] A *runbook* is a set of instructions for completing a routine task.

[170] A *playbook* outlines the organization’s approach and worker responsibilities. More details provided in 11.2.4.1.

CIR をサポートするには、他のチームや組織がいくつかの重要な調整を行う必要があります。CIR チームは、すべての配備に対して永続的な読み取りアクセス権を持っている必要があります。クラウドインシデントの調査は、関連するリソースや構成を確認できないと事実上不可能です。これらの権限の使用はすべてログに記録し、レビューされる必要があります。クラウドプロバイダの機能に応じて、次の 2 つのレベルをサポートする必要があります。

- メタデータと構成への読み取りアクセス（*セキュリティ監査*と呼ばれることもあります）は永続的である必要があり、レスポンダーのデフォルトアクセスレベルであるべきです。
- メタデータだけでなくデータのレビューも可能なフル読み取りアクセスは、使用するために複数の承認が必要になる場合があり、多くの場合、ブレークグラスプロセスに従ってそのようにするべきです。

上位のレスポンダーは、データの露出などといった迅速な対応が必要な深刻な事態に備えて、書き込みアクセスを持つ必要があります。ファイアウォールでアクセスを遮断するような従来のアプローチは使えないかもしれません。このアクセスは厳重に管理され、承認を必要とし、プレークグラスプロセスを使用する必要がありますが、24 時間 365 日利用可能である必要があります。これらのレスポンダーは、クラウドプラットフォームに非常に精通している必要があり、最も危機的なインシデントの場合にのみこのアクセスを使用する必要があります。これには通常、上層部の承認が必要であり、これにより、ビジネスの継続性とセキュリティをトレードオフする権限が与えられます。

クラウド環境では、分散したチームが自社のインフラ（IaaS/PaaS）を直接管理する傾向が強いです。その結果、攻撃と区別しにくいタイプのアクティビティが増加する可能性があります。集中管理された IR チームは、目にするものの多くが攻撃を示唆しているのか、意図された活動なのかを理解するためのコンテキストや知識が不足します。配備オーナーとの明確なリアルタイムコミュニケーションを確立し、IR プロセスに組み込むことが不可欠です。多くの組織が、ChatOps を使用してチームに課題を送信し、それが意図的なものなのか、攻撃の潜在的な指標なのかを検証することで成功を収めています。これはさまざまな方法で統合でき、チームはレスポンスをクリックして潜在的なインシデントをエスカレーションしたり、エスカレーションを解除したりできます。ChatOps は、複数のチームが同じコミュニケーションツールを使用してセキュリティを統合できるため、クラウドチームがすでに使用している場合は特に優れたオプションになります。電子メールやチケットシステムも選択肢の 1 つですが、処理速度が遅く、それらの時間の遅延により、レスポンダーは連絡先を探し回ることになりかねない場合があります。

IR チームは、クラウド配備レジストリにアクセスできる必要があり、そのレジストリには、ビジネスオーナーやテクニカルリードに連絡するための最新情報が必要です。インシデントレスポンダーは、継続的インテグレーション/継続的デプロイメント（CI/CD）パイプライン、コードリポジトリ、およびクラウド構成を管理および変更するその他の場所へのアクセスが必要になる場合があります。封じ込め、根絶、および回復のための対応プロセスでは、これらのリソースとサービスを使用する必要があるでしょう。これは、IR チームと配備担当者またはアプリケーション所有者が協力する準備をしなければならないケースです。

11.2.4 クラウドインシデントレスポンスを支える技術アップデート

CIR をサポートするために必要な最も重要な技術的変更は、必要なセキュリティテレメトリの収集とクラウドネイティブの脅威ディテクターの実装です[171]。このセクションでは、CIR プロセスをサポートするための追加の準備技術の変更に焦点を当てます。

主な技術アップデートは以下の通りです。

- **インシデントレスポンス分析環境を構築：** これは通常、必要な分析ツールを備え、他のクラウド環境に接続してフォレンジック、ログ、その他のデータを抽出する機能を備えた配備です。他のアカウントへのアクセスには、ブレークグラス緊急アクセスプロセスが含まれる場合があります。

- **インシデントレスポンス環境を構築：** この環境は多くの場合、個別のクラウド配備であり、ターゲット配備のリソースと構成を変更できるレスポンスツールを備えています。IR 分析環境と同じ配備が可能ですが、完全な管理者権限など、必要となるリスクの高い権限があるため、理想的には分離されます。
- **クラウド検出およびレスポンス（CDR）：** CDR ツールは SIEM 技術と重複する可能性がありますが、（ログではなく）リアルタイムのセキュリティイベントデータの処理、アラートのルーティングとトリアージ、およびアラートの自動的な補強に重点を置いています。これらのツールは、クラウドの脅威検出が常駐する場所であり、多くの場合、トリアージ、エスカレーション、自動修復/レスポンスの開始に使用されます。
- **フォレンジック:** VM とコンテナのクラウドフォレンジックでは、ソースリソースと同じクラウドプロバイダ内で実行する必要がある、最新のツールが必要です。ソースログファイルなどの他のフォレンジックソースは、コピーして保存する必要がある場合があります。これは、プロバイダによってのみ実行される場合もあります。
- **Security, Orchestration, Automation and Response （SOAR）：**SOAR ツールは、クラウドプロバイダーに接続して分析の充実とサポート、フォレンジックイメージングの自動実行、その他のクラウドアクションなど、クラウド運用と自動化をサポートします。
- **その他の自動化およびレスポンスツール（「ジャンプキット」など）：**ほとんどのクラウドインシデントレスポンダーは、調査やレスポンスをサポートするために、商用ツール、カスタムスクリプト、およびオープンソースツールを組み合わせて使用しています。これらは、利用可能な他のツールに応じて、Cloud SOAR および CDR プラットフォームに統合される場合とそうでない場合があります。これらのツールが統合されていない場合でも、多くのレスポンダーは、さまざまなタイプの調査に使用できる追加のツールを用意しています。
- **攻撃シミュレーション：**指定されたシミュレーション配備または本番環境での障害インジェクション/シミュレーションのいずれかで攻撃をシミュレートすることにより、レスポンダートレー

[171] Additional details for telemetry and cloud incident response are covered in *Domain 4: Organization, Tenancy, & Enterprise Management* and *Domain 6: Security Monitoring*.

ニングとレッドチーミング[172]を支援するツールです。これらは訓練だけでなく、ディテクターやテレメトリが正常に動作していることを検証するためにも重要です。

- **検知エンジニアリング:** クラウドネイティブの脅威ディテクターは、通常、ログ分析、リアルタイムのイベント監視、および構成変更監視が組み合わされています。検知エンジニアリング活動は、これらの新しい種類のデータソースとアクティビティフローを考慮する必要があり、クラウド脅威ディテクターのライフサイクル管理をサポートするために技術の変更が必要になる可能性があります。

11.2.4.1 ランブックとプレイブック

ランブックとプレイブックは、特定のインシデントタイプを処理するための文書化されたプロセスです。組織は、クラウドインシデントのためにこれらを更新し、新しいクラウドインシデントタイプに対応するための新しいランブック/プレイブックを作成する必要があります。ランブックとプレイブックの定義は異なりますが、根底では同じ目標を達成します。IR のコンテキストでは、特定のインシデントタイプを調査し、対応する際に実行する一連の手順を文書化したものです。

例えば、未知のソース IP からのクレデンシャルの外部からの悪用の可能性についてアラートが発せられた場合、ランブック/プレイブックは調査と対応方法についてステップバイステップのガイダンスを提供します。現代のプレイブックは多くの場合、自動化システム（SOAR プラットフォームなど）に実装され、自動化を使用していくつかの手順を実行でき、構築前の分析クエリのような他の手順を含めることができます[173]。

ランブックとプレイブックに関する重要な考慮事項は次のとおりです。

- **ランブックとプレイブックの特殊性：** まず、ランブックとプレイブックを特定のプラットフォームとサービスに合わせて調整する必要があることを強調します。これにより、対応がそれぞれの状況の固有の側面に適切で効果的であることを確実にします。
- **バージョン管理：** これらのドキュメントをバージョン管理されたリポジトリや SOAR システムで管理することの重要性を強調します。このプラクティスは、時間の経過に伴う変化を追跡するのに役立ち、チームが常に最新の情報で作業できることを確実にします。
- **新しいランブック/プレイブックの作成:** 新しいタイプのインシデントが発生するたびに、それに対応するプレイブックを作成することが重要です。このプロアクティブなアプローチにより、このタイプのインシデントが再び発生した場合、チームはそれに準備済みであることを確実にします。
- **SOAR 障害時の計画：** SOAR システムが導入されていても、その潜在的な障害に対する計画が必要です。技術が機能しなくなる可能性があることを理解し、手動のプロセスやバックアップ計画が不可欠です。

[172] Redteam.guide. (2022) The process of using Tactics, Techniques, and Procedures (TTPs) to emulate a real-world threat with the goals of training and measuring the effectiveness of the people, processes, and technology used to defend an environment.
[173] AWS. (2020) Well-Architected Framework: Concepts - Runbook and Playbook.

- **自動化の統合：** IR プロセスに自動化を織り込む方法について議論します。自動化はインシデントの迅速な解決に役立つアクションをトリガーする必要がありますが、自動化によって課題が妨害されたり悪化したりしないことを確実にするためのチェックも必要であることを説明します。

11.3 検知と分析

インシデントの検出や分析の基礎は、クラウドの導入によってハイレベルでは変わりませんが、細部は大きく変わります。

クラウドの主な違いは次のとおりです。

- クラウドが配備する検出と分析のための新しいテレメトリ。
- どんな対応でも、マネジメントプレーンのアタックサーフェスを第一に考えなければなりません。
- クラウドにおける活動の速度には、攻撃者のスピード（高度に自動化されている）とクラウド環境自体の変化のスピードが含まれます。
- 従来のネットワーク境界がなく、IAM の影響範囲が追加されています。
- API ドリブンのクラウドの性質と、リソースのエフェメラルな性質。
- クラウドと開発チームによるインフラストラクチャの分散管理。
- 自動化、infrastructure as code、サーバーレス、その他のクラウドネイティブ技術。

これらの違いは、インシデントの検出と分析能力を向上させる場合もあれば、新たな課題を生み出す場合もあります。このセクションのガイダンスでは、これらの大きな違いと、検出およびレスポンスアクティビティを調整する方法について説明します。

11.3.1 検出および脅威ディテクター

マネジメントプレーンや IAM 活動のための脅威ディテクターを構築する必要があります。攻撃者が直接インフラストラクチャを変更する可能性があるため、最も破壊的な活動が発生する可能性がある場所です。これらのディテクターは、脅威アクターではなく活動にフォーカスする必要があります。クラウド攻撃者は、IP リストや接続ヘッダーを使って現れることはあまりありません。活動は API レベルで直接行われ、多くの場合、同じクラウドプロバイダ内の侵害された環境から発生します。たとえば、未知の配備からのスナップショットを共有する API コールなどです。
クラウドマネージメントプレーンに対する攻撃のほとんどは、紛失、盗難、または悪用されたクレデンシャルに依存しています。既知のネットワークの外部や IAM 境界からのクレデンシャルの使用は、潜在的なインシデントを示す可能性があります。攻撃の多くは、侵害されたアイデンティティ/クレデンシ

ャルで実行されるため、この種の侵入を検出できるものは振る舞い検知（behavioral detector）[174]だけです。さらに、クラウド攻撃は大幅に自動化され、驚くほど迅速に移動するため、最初の侵害から数秒から数分でデータが抜き取られたり、一般に公開されることさえあります。最も重要なアクティビティ（プライベートデータの公開など）のディテクターは、可能な場合はリアルタイムで、もしくは少なくとも数分以内に動作する必要があります。これは、ほとんどのレスポンダーが従来のインフラストラクチャで対応し慣れているよりもはるかに厳しい期間です。

新しい IAM ユーザーを作成したり、未知のアカウント/サブスクリプション/プロジェクトとリソースを共有したりといった構成変更は、クラウドディテクターの優れたソースになる可能性があります。これらの「構成アラート」のソースは、直接計測する場合と、CSPM ツール（クラウドサービスプロバイダ（CSP）、サードパーティ、自作、オープンソース）を使用する場合があります。インシデントレスポンダーは、特定の設定ミスが攻撃なのか、ミスなのか、もしくはそのアプリケーションスタックに必要なものなのか、おそらく見分けがつきません。そのため、クラウドアカウントチームとの明確で直接的なコミュニケーションが重要になり、レスポンダーがミスか攻撃かを迅速に判断できるようになります。ChatOps やそれに類するコミュニケーションを採用し、担当チームに直接アラートを送信している組織もあります。そのため、ミス、例外リクエスト、またはアクティビティが予期されておらずエスカレーションする必要があることを示す、アプリ内のボタンで対応できます。

CSP のセキュリティ警告は、多くの場合、検出の優れたソースですが、チューニングやフィルタリングが行われていない場合、問題となる可能性があります。たとえば、ロックダウンされた本番環境では高品質であっても、開発環境では大量の誤検知が発生する可能性があります。暗号マイニングや潜在的なランサムウェアなどの一部のアラートは、構造化されていない環境でも品質が高くなる傾向があります。ユーザーの行動に焦点を当てた他のものは、より動的な非本番環境ではあまり役に立たない傾向があります。

検出エンジニアリングでは、侵害されたオペレーティングシステム、Web 攻撃、およびデータベース攻撃などの「従来の」イベントの発生源も考慮する必要があります。クラウドネットワークは、ソフトウェアデファインドネットワークに固有の違いがあるため、完全なパケットキャプチャとモニタリングのために計測されることはほとんどありません。しかし、フローと DNS アクティビティは、クラウドネイティブのネットワーク脅威検出を構築する優れたソースになる可能性があります。検出エンジニアは、CSA の Top Threats レポートや MITRE ATT&CK for Cloud[175]に関する最新のソースを使用できますし、使用すべきです。これらのモデルは、ツールやオリジンシグネチャだけでなく、攻撃者のアクションに基づいて脅威検出を構築するために使用できる攻撃者アクティビティを記述します。

ディテクターはライフサイクルがあり、最新の DevOps/DevSecOps プラクティスと互換性のあるバージョン管理と CI/CD パイプラインを使用して管理することが理想的です。侵害され悪用されたクレデン

[174] NIST (2021) *Detecting Abnormal Cyber Behavior Before a Cyberattack* - Behavioral anomaly detection involves the continuous monitoring of systems for unusual events or trends. The monitor looks in real time for evidence of compromise, rather than for the cyberattack itself.
[175] MITRE. (2024) *Threat Intelligence Program*.

シャルはクラウド侵害の主要な発生源であるため、カナリアトークンやハニートークンの使用は侵害されたアイデンティティリポジトリを特定する優れた検出ツールになる可能性があります[176]。

カナリアトークンやハニートークンを IR プロセスに統合し、クレデンシャルの取得方法を追跡し、これを使用して攻撃者を追跡することに焦点を当てた調査をすぐに開始する必要があります。ハニーポットを使用する場合もあります。これは、クレデンシャルに焦点を当てたカナリア/ハニートークンとは対照的に、システム/ネットワークベースです。

11.3.2 インシデントレスポンス分析に対するクラウドの影響

クラウドコンピューティング環境は、そのエフェメラルな性質、拡張性、および分散制御性のため、従来の IR 分析から脱却する必要があります。クラウド設定におけるインシデント分析の焦点は、多くの場合、ログを通じてクラウドアクティビティの包括的な眺望を提供するマネージメントプレーンです。これらのログは、不正アクセス、設定ミス、およびセキュリティインシデントを示す可能性のあるその他の異常を特定する上で非常に重要です。

リソースを迅速にプロビジョニングおよび廃棄できるクラウド環境の動的な性質により、IR チームは方法論を適応させる必要があります。これには、自動化と機械学習を活用して、クラウド運用と構成変更のスピードに対応することが含まれます。また、クラウド環境での分析では、公開されているリソースを特定することを優先するため、潜在的な侵害やコンプライアンスの課題を軽減するための迅速な対応が求められます。

クラウドの性質が異なるため、分析の優先順位が変わるはずです。リソースではなく、マネージメントプレーンの活動に主眼を置くべきです。攻撃者は、マネージメントプレーンへのアクセス能力に応じて、甚大な損害やデータ盗難を引き起こす可能性があります。また、攻撃者は配備内のリソースの侵害を試み、次に、リソース特権を使用してマネージメントプレーンに橋を架けようとします。したがって、ハッキングされた VM のような孤立したリソース侵害であっても、そのリソースに何らかの内部権限や保存されたクレデンシャルがあれば、攻撃者はマネージメントプレーンを開くことができます。

もう 1 つの重要な焦点は、公開されていたリソースや、意図せず別のクラウド配備と共有されていたリソースです。これらは一般的な流出技法であり、完全な公の場への露出は、明らかに非常に大きな懸念です。インシデントの残りの範囲を完全に調査する前に、迅速な封じ込めが必要になる場合があります。クレデンシャルの紛失、盗難、または悪用はクラウドネイティブ侵害の最も一般的な発生源であるため、分析では、アカウントに関与している IAM エンティティを特定し、その資格の範囲（「IAM 影響範囲」）と対応するすべてのアクティビティを特定することに焦点を当てる必要があります。異なる送信元 IP アドレスなどのインジケータは、これらのクレデンシャルの予想される使用と予期しない使用を区別するために役立ちます。

[176] These techniques are covered in more detail in *Domain 6: Security Monitoring*.

クラウドマネージメントプレーンのアクティビティログは、すべてのアクティビティを示すことが多く、攻撃者によって変更または削除できないため、攻撃をトレースする非常に強力なツールです。たとえ攻撃者が保存されたログを削除できたとしても、ほとんどの大手クラウドプロバイダは API ログから約 90 日間ほどのアクティビティから何かを提供できるか、あるいは、インシデントサポートを契約すれば取得可能なログのコピーを保管しているでしょう。プロバイダによっては、変更イベントのみを API ログに記録し、読み取りアクティビティを表示しません。この場合は、偵察を追跡する機能の削減となります。

セキュリティテレメトリが中央の SIEM またはセキュリティデータレイクにフィードされる場合[177]、アナリストは読み取りアクセスを使用してログのローカルバージョンに直接アクセスし、レビューする必要がある場合があります。ログがログプラットフォームによって取り込まれて正規化された後、元の完全バージョンを保持していない場合、生のログを参照する必要がある場合があります。分析では多くの場合、インシデントを適切に処理するために、アナリストが関係するリソースの設定を確認する必要があります。必ずしもログ解析だけに頼ることはできないでしょう。例えば、セキュリティグループを変更しても、そのグループを使用している露出されたリソースがあるかどうか、および露出される可能性のあるリスクが何かを理解する助けにはなりません。

クラウド侵害は必ずしもクラウドプラットフォームだけにとどまらないため、分析には依然として従来のスキルが必要かもしれません。たとえば、クラウドアナリストは、従業員のノートパソコンからクレデンシャルが盗まれたり、従業員の関与なしにノートパソコン自体が攻撃の発信元であると判断することがあります。アナリストは、対象分野を横断する攻撃のスキルを持つ適切な同僚と連携する必要があります。CI/CD を使用して管理される環境では、攻撃者の主要なターゲットであり、クラウドアプリケーションとインフラストラクチャを侵害する強力なベクトルであるため、分析にはパイプラインを含める必要があります。

次のページの図に示すように、検出を実行する場所は複数あります[178]。

- CDR
- SIEM
- CSPM/Cloud Native Application Protection Platform (CNAPP)
- CSP/Identity Provider (IdP)

[177] This topic is covered in more detail in *Domain 6: Security Monitoring*.

[178] This topic is covered in more detail in *Domain 6: Security Monitoring*.

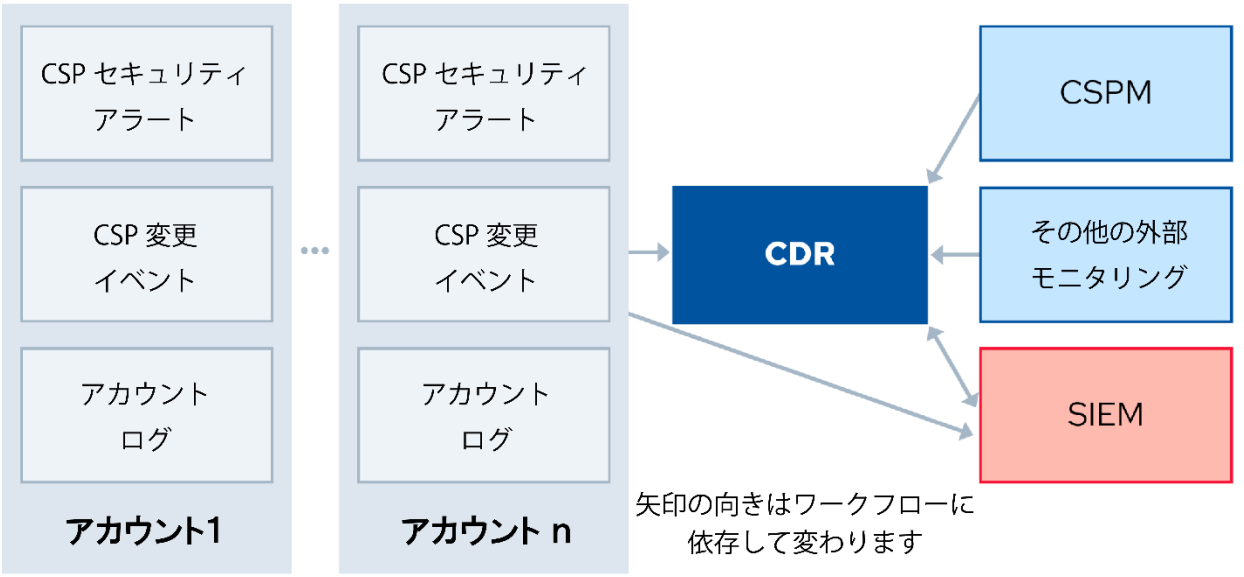


図 63: IR 分析ワークフロー

11.3.3 分析の優先順位: RECIPE PICKS

RECIPE PICKS は、Securosis の Rich Mogull 氏が開発した、クラウドインシデントレスポンダーの初期分析優先度をトレーニングするためのニーモニックです。これらは、クラウドマネージメントプレーンでのインシデント発生時に最初に分析の焦点を当てる場所を表し、インシデントの大部分を解決するために使用できます。

- **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 64: RECIPE PICKS: IR 分析の優先順位

注：最後の 2 つ（特にフォレンジック）を除いて、図中の項目の順序は優先順位に関連しません。プロセスの早い段階でこれらのすべての情報を収集し、分析することがより重要です。

11.3.4 クラウドシステムフォレンジック

クラウドフォレンジックは、マネジメントプレーンやサービスなどのログの分析と、VM やコンテナのシステムフォレンジックの 2 つに大別されます。従来のデジタル（システム）フォレンジック手法は、ハードウェアやローカルデータストレージへの物理的なアクセスに依存することが多く、クラウドでは実現できませんでした。代わりに、クラウドフォレンジックでは、IR チームが CSP が提供する制約と機能の範囲内で作業する必要があります。

クラウドフォレンジックの主な機能は次のとおりです。

- **スナップショット:**ほぼすべてのクラウドプロバイダとコンテナ管理システムがスナップショットをサポートしており、フォレンジック分析に使用できます。インシデントが検出されたときにストレージボリュームのスナップショットを即座に取得する方法と理由を把握し、分析のために VM の状態を保持します。

- **揮発性メモリの取得：**ハードウェアを実装する機能が無いため、メモリフォレンジックが必要な場合、レスポンダーはシステムにも影響するソフトウェアツールをインストールする必要があります。
- **ログ分析：**マネージメントプレーンのログは、システム、アプリケーション、およびユーザーアクティビティのログとともに、VM/コンテナに焦点を当てている場合でもインシデントの全体像を示すために使用できます。たとえば、システムのクレデンシャルを取得してマネージメントプレーンに移動した攻撃者を特定するために役立ちます。
- **証拠保全：**クラウド環境でデジタル証拠を保全するには、CSP と CSC の両方のバックアップとデータ保持ポリシー、およびスナップショットの管理の連鎖を十分に理解する必要があります。

次に、フォレンジック取得および分析環境を使用し、別の配備で、侵害されたワークロードからストレージボリュームスナップショットを収集する例を示します。

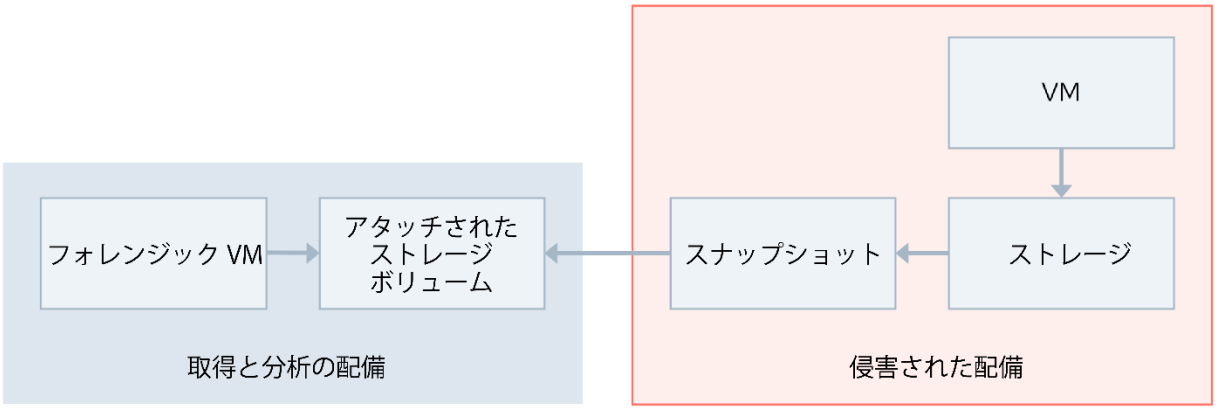


図 65: クラウドフォレンジック:スナップショットの取得と分析プロセス

11.3.4.1 クラウドフォレンジック:コンテナとサーバーレスに関する考慮事項

コンテナ化とサーバーレスコンピューティングの台頭は、クラウドフォレンジックにさらなる複雑さをもたらします。

コンテナとサーバーレスに関する主な考慮事項は次のとおりです。

- **コンテナ：** コンテナは必然的にエフェメラルで、短期間しか存在しないことが多いです。この一過性は、フォレンジックデータの収集と分析に大きな課題をもたらします。フォレンジック戦略には、アクティビティとデータコンテナプロセスに関する洞察を提供するため、コンテナログとコンテナの状態のスナップショットの取得を含める必要があります。そのため、コンテナログ、VM ログ、およびすべてのサービスログを外部ログストレージにリダイレクトすることを強く推奨します。このアプローチの利点は、これらのログを SIEM/SOAR ツールに統合することで、脅威の検出/対応を改善し、コンテナやその他のクラウドサービスのライフサイクルが短いことから、フォレンジック分析を実行できるようになる可能性があることです。フォレンジック目的で実行中のコンテナの状態を一時停止してダンプできる場合もあります。
- **サーバーレスコンピューティング:** サーバーレスアーキテクチャは、実行環境をユーザーからさらに抽象化し、CSP が基盤となるインフラストラクチャを管理します。サーバーレス環境でのフォレンジック分析は、実行ログ、アクセスログ、およびアプリケーションログなど、サーバーレスファンクションによって生成されるログに大きく依存します。サーバーレスファンクションの呼び出しと実行パターンを理解することは、インシデント発生中のイベントを再構築するために重要です。また、進行中の攻撃を潜在的に捉えるための堅牢なモニタリングと、フォレンジックのための詳細なログの提供も重要です。

11.4 封じ込め、根絶、復旧

すべての IR 活動の中で、封じ込め、根絶、および復旧フェーズの IR 活動は、クラウド配備で使用される特定の技術モデルとアーキテクチャモデルの影響を最も強く受けます。イミュータブルな Infrastructure as Code Infrastructure as Code (IaC)、自動スケーリング、マイクロサービス、アイデンティティフェデレーション、および基盤となる技術は、これらの活動で利用可能なプロセスと技法に大きな影響を与えます。多くの場合、これは従来のデータセンターでの対応に比べて、大きな利点をもたらします。

11.4.1 封じ込め

適切な封じ込め計画を決定するにあたっては、可能であれば、クラウドおよびアプリケーションのオーナーの協力を得ることも重要となります。また、当該オーナーは、どの中心となる IR チームよりも配備環境を熟知しているため、計画を実装するために最適な場合もあります。IAM とマネージメントプレーンの封じ込めは、あらゆるセキュリティインシデントにおいて最優先事項となります。認証（AuthN）

メカニズムと認可（AuthZ Gap）メカニズムが分離されているため、適切な IAM の封じ込めは非常に困難になる可能性があります。クラウドアプリケーションは、認証と認可が分離され、多くの場合、異なるプラットフォームで実行される場合には、フェデレーションアイデンティティに依存します。通常、IdP は認証されたユーザーにセッショントークンを発行し、このトークンはリライングパーティー（認可）によって使用されます。リライングパーティーは通常、Time to Live (TTL) が終了するか、セッションが終了するまでトークンを受け入れ続けます。多くのシステムでは、ユーザー/エンティティがシステムからブロックまたは削除された場合でも、セッショントークンを保持します。リライングパーティーは、有効期限が切れておらず、トークンの別の検証をトリガーするアクションも起こっていないため、TTL に基づいてセッション終了までそのトークンを受け入れる可能性があります。しかし、ほとんどの認可システムは要求のたびにエンタイトルメントをチェックします。その結果、封じ込めには、IdP とリライングパーティーの両方で異なるアクションが必要になる場合があります。リライングパーティーがエンタイトルメントを変更したり（拒否ポリシーを使用するなど）、条件を追加したり（特定の時刻以降に発行されたトークンのみを受け入れるなど）する必要があります。ゼロトラストアーキテクチャでは、エンタイトルメントを継続的に（10 分ごとに）確認することを推奨しています。

2 つ目の複雑さは、サービスアカウントのクレデンシャルが侵害されて悪用された場合です。クラウドやアプリケーション所有者との調整なしにこれらを阻止すると、必要なアプリケーション機能が壊れる可能性があります。レスポンダーは、拒否ポリシーを追加してエンタイトルメントを変更する代わりに、送信元 IP アドレス制限などの条件を挿入する必要がある場合があります。このタイプの属性ベースアクセス制御（ABAC）は、すべてのクラウドプロバイダ、特に SaaS プロバイダにおいて普遍的にサポートされているものではありません。攻撃者が単にアクセスを再度悪用して新しいセッションを確立できないように、悪用されたクレデンシャルのソースを特定することは分析にとって重要です。IAM の封じ込めには、ネットワークを中心にピボットする攻撃者を追跡することと同様に、攻撃者がそのアクセスを利用して異なるアイデンティティにエスカレーションまたはピボットできたかどうかも十分に理解する必要があります。この場合、アナリストとレスポンダーが別々の役割であれば、両者が緊密に連携する必要があります。

マネージメントプレーンの封じ込めは、IAM の封じ込めだけにとどまりません。相互接続されたサービスを確認し、影響を受けたサービスやリソースの影響範囲を特定することも重要です。これは IAM 権限の見直しによって明確に示されることが多いですが、一部のクラウドプラットフォームでは、サービスやリソース構成に直接表示されるサービス間のみで内部接続が許可されている場合があります。

クラウドネットワークでは、ソフトウェアデファインドネットワーキングに依存しているため、ネットワークの封じ込めが容易であることが多いです。API 呼び出しと Web コンソールを使用して、ルールを非常に迅速かつ簡単に変更できます。ただし、レスポンダーはプラットフォームのネットワークの詳細を理解する必要があります。たとえば、IAM の場合と同様に、一部のプロバイダでネットワークセキュリティグループルールを変更すると、アクティブなネットワークセッションが中断されるとは限りません（接続時にロジックが評価され、セッションが終了するまで維持されるため）。

一時的なリソース（FaaS、サーバーレスなど）に自動スケーリングを使用すると、封じ込めを強化できます。レスポンダーまたはアプリケーション所有者は、自動スケーリンググループの起動要件を変更し

て、ワークロードのパッチを適用したバージョンを使用できるようにします。その後、侵害されたリソースを分離し、詳細な分析を行うことができます。封じ込めアクティビティでは、公開されているリソース、または不明な宛先と共有されているリソース（不明なクラウドアカウント、サブスクリプション、同じプロバイダー内のプロジェクトなど）にも優先順位を付ける必要があります。重要なデータについては、一時的にアプリケーション機能を破壊するリスクを冒すことが必要な場合があります。インシデントレスポンダーは、極めて重要な状況でこの決定を下し、アクションを起こす権限と能力へのタイムリーなエスカレーションパスを用意する必要があります。VM、コンテナ、サーバーレスコードなどのリソースが侵害されると、攻撃者はマネージメントプレーンにピボットできるようになります。解析の結果、この IAM の影響範囲が特定され、封じ込めの優先順位に貢献しているはずです。関連する CI/CD パイプラインには特に注意してください。攻撃者のパイプラインへのアクセスを封じ込めることも最優先事項です。攻撃者は通常、配備に影響を与える完全な管理機能を取得しているからです。

11.4.2 根絶

根絶は通常、クラウドとアプリケーションの所有者、およびその管理者と開発者によって実装されることが最適です。分析および封じ込めと同様に、根絶の主な焦点は、攻撃者をマネージメントプレーンから排除することです。今日での恒久的な方策には、クレデンシャルのローテーション、追加のポリシー条件の付加、多要素認証（MFA）またはデジタル証明書の追加、および類似の手法が考えられます。これは、ソース IAM/アクセスをロックダウンできるようにインシデントの原因が特定された場合にのみ可能です。攻撃者がマネージメントプレーンまたは IAM システム内でピボットできたかどうかを特定するには、インシデント検出時だけでなくインシデント中およびインシデント後に分析を実行する必要があります。

クラウドでは、攻撃者をリソースから追い出そうとするよりも、リソースを置き換える方が簡単な場合が多いです。自動スケーリングや Infrastructure as Code (IaC) のおかげでリソースがエフェメラルな場合は特にそうです。修理しようとしないでください。できるだけ拭き取って交換してください。このタイプの根絶は、クラウドネイティブアプリケーションと併用するとはるかに容易になり、リフトアンドシフトアプローチでアプリケーションが配備されると、より困難になります。

根絶のためには、古いバージョンのイメージ、サーバーレスコード、および IaC の削除が必要になることが多いです。攻撃者は、特に従業員が誤って古いバージョンの全体または一部を再配備した場合に、これらを使用して配備を再侵害する可能性があります。根絶には、CI/CD パイプラインとバージョン管理およびアーティファクトリポジトリに保存されているすべての資料の完全なレビューが必要になる場合もあります。

11.4.3 復旧

IaC、自動スケーリング、その他の自動化は、インシデントのリカバリに非常に有効です。アプリケーションやインフラストラクチャのハードニングされたバージョンを迅速に配備したり、まったく新しい環境にクリーンバージョンを配備することも可能です。復旧に使用されるすべてのイメージ、リソー

ス、およびテンプレートを分析し、根本原因が取り除かれ、攻撃者がバックドアを残し続けないようにする必要があります。たとえば、攻撃者は、インシデントとは無関係と思われる IAM エンティティへのアクセス権を自分自身に与え、最初の攻撃では使用されなかった可能性があります。あるいは、攻撃者がアプリケーションやイメージにバックドアの鍵やコードを埋め込み、将来のアクセスを可能にしてしまっている可能性もあります。

11.5 インシデント後の分析

IR の最も重要な、しかし見過ごされがちな段階の一つは、教訓を見つけ出し、その後、将来の同様のイベントの可能性または影響を減らすための積極的な措置を講じることです。これは、インシデント後の分析フェーズで行われます。このフェーズでは、レスポンダーはインシデントの根本原因を特定し、対応プロセスを分析し、改善点を特定しようとします。これは責任の所在を明らかにすることよりも、将来のイベントを防ぐために、あるいは制限するために修正可能な、構造上の課題を特定しようとすることです。

インシデント後の分析フェーズの基本はクラウドでも変わりませんが、注目すべきベストプラクティスがいくつかあります。

- クラウドインシデントの多くは、クラウド配備を管理したチームとの連携を伴うため、当該チームをインシデント発生後の分析に含める必要があります。
- レスポンダーは、遭遇する新しいインシデントタイプに対応する新しいランブック/プレイブックを作成する必要があります。
- クラウドセキュリティインシデントの多くは、設定ミスが原因です。クラウドセキュリティアライアンスは、責任の追及ではなく、個人の責任の所在を明らかにする前にシステムの欠陥を特定することに焦点を当てた Just Culture[179]のアプローチに従うことを推奨していますが、たとえば、セキュリティは一般的な基準を提供し、チームと協力して権限を見直すかもしれません。あるいは、組織は静的なクレデンシャルから、強力な認証と組み合わせたジャストインタイムのエンタイトルメントに移行するかもしれません。ただし、開発者の作業を妨げない摩擦のないツールを使用するでしょう。

11.6 レジリエンス

クラウドコンピューティングの分野では、レジリエンスとは、軽微な障害から大規模なシステム停止まで、さまざまな種類の障害に直面しても、アプリケーションやシステムがシームレスに動作し続ける能力を指します。クラウドのレジリエンスの概念は階層化されており、対象となるサービスの重要度と予算の制約に応じてスケールできます。

[179] Just Culture is a concept that is related to systems thinking. The concept emphasizes that mistakes are typically a fault of the organizational culture rather than a fault of a person. The idea is to shift from “who did it” to “what went wrong”.

基本レベルでは、*単一リージョンのレジリエンス*は、ほとんどのアプリケーションがレジリエンスの実現に向けた取り組みを開始する場所です。このセットアップでは、アプリケーションは単一のクラウドプロバイダのリージョン内でホストされます。自動スケーリングやロードバランシングなどの戦略を採用して、トラフィックの急増に対処し、個々のコンポーネントの障害に対するフォールトトレランスを実現します。データを保護するためのバックアップおよびリカバリ戦略も導入されています。この基礎レベルは、リソースを大幅に重複させることなく、クラウドプロバイダの既存のインフラストラクチャとサービスを利用できるため、最もコスト効率の高いオプションでもあります。

図 66: グローバルなクラウドのレジリエンス戦略

ただし、単一リージョンの配備は、まれではありますが、アプリケーションの可用性に大きな影響を与える可能性のある地域全体の停止に対して脆弱です。このリスクを軽減するために、組織は*マルチリージョンレジリエンス*にステップアップすることができます。これには、同じクラウドプロバイダのネットワーク内の複数のリージョン間でアプリケーションの並列配備を実行することが含まれます。これによりフォールトトレランスと地理的多様性が大幅に向上する一方で、追加コストも発生します。これらのコストは、アプリケーションの複数のインスタンスを実行することだけでなく、リージョン間でデータを同期する必要があることからも生じます。さらに、リージョン間のデータ移動に発生するデータ転送料は、瞬く間に莫大なものとなる可能性があり、単一リージョンでの導入よりも高価なオプションとなります。

最も困難なクラウドのレジリエンスは、*マルチプロバイダのレジリエンス*です。このレベルは、アプリケーションのフットプリントを複数のクラウドプロバイダに分散することで達成されます。これは、クラウドプロバイダ全体がダウンするシナリオからアプリケーションを保護することを意図しています。マルチプロバイダのレジリエンスの達成は、クラウドプロバイダ間の技術の違いからも複雑になります。コンテナ化技術は、基盤となるインフラストラクチャからアプリケーションを抽象化することで、この複雑さをいくらか緩和できますが、課題は残ります。これには、異なるネットワーキング、ストレージ、およびセキュリティモデルの管理や、根本的に異なる環境間での配備と運用のオーケストレーションが含まれます。コストは、直接的な運用コストだけでなく、設計、開発、テスト、および継続的なメンテナンスに必要なオーバーヘッドの増加により、急速に増大する可能性があります。コストと複雑さにもかかわらず、最大限の可用性を必要とする重要なアプリケーション

（金融取引、医療サービス、国際商取引など）の場合、マルチプロバイダのレジリエンスは必要な投資となる可能性があります。

11.6.1 IaaS/PaaS のレジリエンスツール

IaaS と PaaS は、抽象化（仮想化）とオーケストレーションをコアとしています。生のハードウェアに対するこれらの追加レイヤーは、より多くの障害の可能性をもたらします。これを説明するため、CSP は利用者に、単一障害に対するレジリエンスを向上させるための複数の設計オプションを提供しています。IaaS と PaaS には、レジリエンスを向上させるために活用できる多数のツールが含まれています。

- **アーキテクチャ:**
  - *自動スケーリング:* 自動スケーリング機能を活用することで、システムはリソースを動的に調整し、障害発生時にリソースを交換できます。
  - *サーバーレスコンピューティング：* サーバーレスは本質的に需要に応じて拡張できるように設計されているため、フォールトトレラント性に優れています。
  - Platform as a Service：PaaS 製品は、オペレーティングシステムとインフラストラクチャを維持する必要が無いように抽象化されており、その多くは非常に高レジリエンスな SLA を持っています。
- **Infrastructure as Code (IaC):**
  - *イメージの定義:* イメージに IaC を使用して VM とコンテナを定義することで、置き換えを生成し、迅速に適応する能力が向上します。
  - *インフラストラクチャの定義：* IaC はアプリケーションスタック全体に移植容易性を提供できます。
- **自動化とバックアップ:**
  - *CI/CD パイプライン：* 新しい環境への修正または新しいスタックの導入を迅速に自動化します。
  - *バックアップ：* 多くのプロバイダは、特にデータベースなどの PaaS サービスの自動バックアップもサポートしています。
- **カオスエンジニアリング:**
  - *原則とツール：* 開発および本番アプリケーションに故意に障害を注入し、レジリエンスを継続的に検証するために使用します。これにより、ダウンタイムがほとんどな

い、またはまったくないと仮定するのではなく、インフラストラクチャやサービスの障害が発生することを想定してチームの構築をガイドできます。

11.6.2 SaaS のレジリエンス

SaaS（Software as a Service）アプリケーションのレジリエンスの概念を議論する場合、本質的には、さまざまな途絶に直面してもサービスの運用を継続できる能力を指します。この場合のレジリエンスとは、SaaS プロバイダにシステム停止などの課題が発生した場合でも、事業継続と災害復旧（BCP/DR）計画を確実に実行できるようにすることです。IaaS や PaaS とは異なり、サービス利用時に利用者が自身のレジリエンスの側面を管理できる選択肢は、ほとんどあるいは全くないことが通常です。

SaaS には次のような課題があります。

- **非常に限られた選択肢：** SaaS アプリケーションは多くの場合、プロバイダのインフラストラクチャ上で実行されます。つまり、アプリケーションの耐障害性や冗長性のコントロールは、エンドユーザー側ではなく、プロバイダに委ねられています。レジリエンスを高めるオプションは、プロバイダが提供する内容によって制限されます。したがって、企業は堅牢な災害復旧能力と高可用性機能を提供する SaaS プロバイダを選択することが重要です。
- **データの抽出/移行サポート：**いくつかの主要なプラットフォームではデータの抽出と移行がサポートされていますが、これらの機能は、リアルタイムの災害復旧のためではなく、プラットフォームの切り替えやバックアップのために設計されていることが一般的です。当該のプロセスは連続的ではなく、データエクスポートの間に大きな遅延が発生する可能性があります。システムが停止した場合、直近のデータはエクスポート上では利用できない可能性があり、最新のデータを必要とする業務では問題となります。
- **定期的なデータ抽出：** 多くの場合、企業が利用できる最善の選択肢は、定期的にデータの抽出を実行することです。これには、可能な場合はローカルデータ同期も含まれます。これにより、リアルタイムのリカバリはできませんが、データ損失のリスクを軽減できます。これらの抽出をどの程度の頻度で実行するかは、ビジネスの性質とデータの重要度によって異なります。夜間のバックアップで十分な場合もあれば、より頻繁な間隔が必要な場合もあります。
- **SaaS の SLA を調べて把握する:** SLA は、アップタイム保証やサービス中断時のプロバイダの責任など、SaaS プロバイダに期待できるサービスレベルを定義する重要な文書です。これらの契約を十分に吟味して、どのような継続性とリカバリオプションが約束されているか、プロバイダがデータバックアップをどのように処理しているか、およびサービスが合意された基準を満たさない場合にどのような補償が提供されるかを理解することが重要です。

SaaS アプリケーションとの継続性を確保するためには、上記のポイントに加えて、次の戦略を検討する必要があります。

- **複数のプロバイダ：** サービスの重要度によっては、冗長化のために複数の SaaS プロバイダを利用する価値がある場合もあります。これは、ビジネス運営に不可欠なサービスに特に当てはまります。

- **ハイブリッドソリューション：** ビジネスによっては、必須アプリケーションがオンプレミスまたはプライベートクラウドでホストされ、重要度の低いアプリケーションは SaaS プロバイダでホストされるハイブリッドソリューションを選択する場合もあります。
- **定期的に更新される復旧計画：** 企業は、十分に文書化され、定期的にテストされた復旧計画を用意する必要があります。この計画は、SaaS アプリケーションとそれらがサポートするビジネス運用の変更を考慮して更新する必要があります。
- **保険：** 企業によっては、SaaS のダウンタイムによる損失をカバーする保険の選択肢を検討する場合もありますが、これは継続性ソリューションではなく、財務上のバッファです。
- **トレーニングと準備：** 障害発生時にバックアップシステムまたは手動プロセスに切り替える手順について、スタッフのトレーニング実施を確実にします。

SaaS アプリケーションのレジリエンス計画では、最小限の途絶でビジネス運用を継続できるように、当該 SaaS の制限を理解し、それを取り巻く積極的な計画が必要です。

サマリ

組織は、CIR プロセス（およびその IR 機能）についてしっかりと理解して、潜在的なインシデントに備える必要があります。

このドメインでは、CIR フレームワークとインシデントに効果的に対応するために必要な準備について説明しています。破壊的なイベントに対するライフサイクル全体を通じたクラウドインシデントの準備と管理を行うための CSC の頼れるガイドとして機能します。また、CSP と CSC が CIR プラクティスを共有するための透過的で共通のフレームワークも提供します。

強固な基盤の構築： CIR フレームワークは、組織がクラウドでセキュリティ侵害に対処できるようにします。第 1 段階の*「準備」*では、強固な基盤の構築に焦点を当てます。これには、インシデントを管理するための専用のクラウドインシデントレスポンスチーム（CIRT）の設置が含まれます。その後、CIRT は対応の指針となる包括的な戦略、手順、およびコミュニケーション計画を策定します。さらに、クラウド、特にセキュリティテレメトリとレスポンダーアクセスの違いを説明するには、技術的な準備が必要です。これには、早期発見のためのセキュリティーツールの実装、詳細な調査のためのフォレンジックおよび分析機能の確保が含まれます。

対応と学習: セキュリティ侵害が発生すると、クラウドインシデントレスポンスフレームワークは*検出と分析*フェーズに移行します。ここでは、インシデントの早期発見と根本原因の把握に焦点を当てています。これを実現するために複数の検知方法が採用されており、フレームワークでは、潜在的なビジネスインパクトに基づく迅速な通知と解決の重要性が強調されています。脅威が封じ込められると、*封じ込め、根絶、復旧*フェーズに入ります。この段階では、攻撃者を阻止し、調査やフォレンジックが行われている間に被害の拡大を防ぐために、適切な戦略を選択します。

継続的な改善： クラウドインシデントレスポンスフレームワークは、*インシデント後の分析*フェーズで終了します。この段階は経験から学ぶために不可欠です。CIRT はインシデントを分析し、人員、プロセ

ス、または技術の弱点を特定します。これらの教訓は準備フェーズにフィードバックされ、組織のインシデントレスポンス能力を継続的に向上させます。この循環的なアプローチにより、常に進化するセキュリティポスチャが確保され、組織はクラウドで絶えず変化する脅威のランドスケープを効果的にナビゲートできます。

調整と情報共有： クラウドセキュリティインシデントの「共有」という性質上、効果的なコミュニケーションが不可欠です。これには、CSP とユーザー間の明確なチャネルの確立、影響を受けるユーザーの定期的な最新情報提供の促進、および関係者間の情報共有の促進が含まれます。さらに、社内 IR チーム、法執行機関、および主要パートナーとのコミュニケーションを早期に計画することで、全体的な CIR 能力を強化します。

推奨事項

インシデントレスポンス計画

- クラウド環境に合わせた包括的なインシデントレスポンス（IR）計画を策定します。
- 役割と責任が定義された専用のクラウドインシデントレスポンスチーム（CIRT）を設置します。
- インシデント分析サービス、ハードウェア、ソフトウェアなど、必要な環境とツールにレスポンダーがアクセスできるようにします。
- ポートリスト、資産リスト、ネットワークトラフィックのベースラインなどの内部ドキュメントを管理します。

準備

- プロアクティブなスキャン、モニタリング、脆弱性とリスクの評価を実行します。
- サードパーティの脅威インテリジェンスサービスを購読します。
- クラウドサービスプロバイダーの IR 対応能力を評価します。
- ログ、スナップショット、フォレンジック機能、および電子情報開示機能を定期的に監査します。
- 定期的なバックアップ復元およびディザスタリカバリテストを実施します。

検知と分析

- 脅威検出の主要領域として、マネージメントプレーンと IAM アクティビティに重点を置きます。
- 脅威アクターにフォーカスした脅威ディテクターではなく、アクティビティにフォーカスした脅威ディテクターを実装します。
- 構成変更をクラウドディテクターのソースとして使用し、CSPM ツールに統合します。
- クラウドアカウントチームとの明確で直接的なコミュニケーションによる迅速なインシデント検証を確実にします。

- カナリアトークンやハニートークンを採用して、侵害されたアイデンティティリポジトリを検出し、即座に調査を開始します。
- 自動化と機械学習を活用して、クラウド環境の動的な性質を管理します。
- スナップショットを使用して VM の状態を保持し、フォレンジック分析を行います。

封じ込め、根絶、回復

- IAM およびマネージメントプレーンの封じ込めを優先します。
- アイデンティティとワークロードを分離し、必要に応じてシステムやサービスをオフラインにします。
- 可能な限り、自動スケーリングと Infrastructure as Code（IaC）を使用して、侵害されたリソースを置き換えます。
- クレデンシャルのローテーション、ポリシー条件の追加、および根絶のために多要素認証（MFA）を実装します。
- 古いバージョンのイメージ、サーバーレスコード、および IaC を削除し、再侵害を防止します。

インシデント後の分析

- Just Culture のアプローチに従って、責任の所在を明らかにするのではなく、システム的な欠陥を特定します。

レジリエンス計画

- 自動スケーリング、ロードバランシング、およびバックアップ戦略を使用して、単一リージョンのレジリエンスから始めます。
- フォールトトレランスと地理的多様性を向上させるために、複数リージョンのレジリエンスを検討します。
- 最高の可用性を必要とする重要なアプリケーションのために、マルチプロバイダのレジリエンスを評価します。
- 自動スケーリング、サーバーレスコンピューティング、および Infrastructure as Code（IaC）などの IaaS および PaaS ツールを活用して、レジリエンスを向上させます。
- CI/CD パイプラインを使用して、修正と新しいスタックの配備を自動化します。
- カオスエンジニアリングの原則を導入し、意図的な障害注入によってレジリエンスを検証します。

追加のガイダンス

- Cloud Incident Response Framework | CSA
- Cloud Incident Response Framework – A Quick Guide | CSA
- CSA Medical Device Incident Response Playbook | CSA
- Cloud Penetration Testing Playbook | CSA
- Cloud Penetration Testing Guidance | CSA

ドメイン 12: 関連技術と戦略

はじめに

クラウドセキュリティでは、さまざまな角度から分析を行い、クラウドセキュリティの課題を理解する必要があります。その *レンズ*は本質的に視点であり、さまざまな視点から課題を検討するうえでユニークな方法を提供するため、戦略的な検討を考慮することができます。*プロセス*は、情報に基づいた意思決定を行い、必要なアクションを繰り返し実行するための指針となる方法論とフレームワークを提供します。この 2 つを組み合わせることで、クラウドアプリケーション、システム、およびデータのセキュリティとコンプライアンスを確実にする包括的な戦略を構築します。

組織管理、アイデンティティおよびアクセス管理（IAM）、セキュリティモニタリング、ネットワーク、ワークロード、アプリケーション、およびデータなど、さまざまな重要なセキュリティドメインを横断するレンズとプロセスのスペクトルを探ります。レンズとプロセスは、複数のドメインにまたがる重要なセキュリティ領域です。

学習目標

このドメインの学習目標は、読者に以下の知識を提供することです。

- クラウドセキュリティの脅威と脆弱性管理に AI を統合するメリットについて議論します。
- クラウドセキュリティにおける人工知能の役割を説明します。
- ゼロトラストサイバーセキュリティアプローチの主要コンポーネントを特定します。

12.1 ゼロトラスト

ゼロトラスト（ZT）は、ネットワーク境界を越えてリソース、ユーザー、資産、およびデータを保護することに焦点を置いたサイバーセキュリティのアプローチです[180]。ZT は、信頼できる、または信頼できないユーザーやネットワークを超え、継続的な多要素認証（CMFA）、マイクロセグメンテーション、暗号化、エンドポイントセキュリティ、自動化、および分析に依存しています。さらに、ZT は

[180] Zero Trust is also covered in *Domain 2: Cloud Governance & Strategies*, *Domain 7: Infrastructure and Networking*, and the CSA CCZT Training.

DAAS（データ、アプリケーション、資産、およびサービス）の強化された監査に対応しています。ゼロトラストアーキテクチャ（ZTA）の主な目的は、信頼の前提、もしくは不十分なアクセス制御に内在するセキュリティリスクを軽減することです。これらのリスクを軽減するための一般的な戦略には、アタックサーフェスを最小限に抑えること、およびセキュリティ対策の効率と粒度を強化することなどがあります。クラウドでは、マルチテナンシー、高度に分散されたアクセス、およびインターネットに面する広範なアタックサーフェスを管理する必要があるため、これらの優先順位は特に重要です。

ZTA は、企業を社内外の脅威や攻撃から保護する、包括的で一貫したセキュリティアプローチを提供します。これらの脅威や攻撃は、従来の保護方法や深層防御のコントロールに内在する、あるいは導入されたギャップをエクスプロイトする可能性があります。

ZTA の主な差別化要因は、リソース、データ、およびコンピューティングワークロードの要求側に対して与えられるアクセスのエフェメラルな性質です。この差別化要因は、動的なポリシー適用や動的なポリシー決定などの機能と組み合わせることで、クラウドとオンプレミスのセグメントにまたがるエンタープライズ環境を強化します。これは、公開されたアクセスメカニズムをエクスプロイトする内部脅威と外部脅威の両方に当てはまります。
ZT アプローチは、技術目的とビジネス目的の両方に役立ちます。技術的には、リソースを保護するためのフレームワークを提供し、ユーザーエクスペリエンスを合理化し、アタックサーフェスと複雑さを最小限に抑え、最小限の権限を適用し、コントロールとレジリエンスを強化し、影響範囲を削減します。ビジネスの観点から、ZT はリスクの軽減、コンプライアンスの向上、および組織の文化とリーダーシップのリスク選好[181]およびガバナンスフレームワーク[182]との整合を支援します。

12.1.1 ゼロトラストの技術目標

ZT の技術目標はすべて、クラウドのセキュリティを向上させるために使用することができます。以下に、いくつかの技術目的と ZT との関係を示します。

保護フレームワーク

ZT は、サイバーセキュリティの保護フレームワークと新しいアプローチを確立します。ZT の核心的な仮定は、組織がその境界の内外でいかなる原則も本質的に信頼してはならないということです。新しい保護フレームワークにより、データの価値と特定の保護ニーズに基づいて設計されたシステムで、よりビジネス指向の目標に焦点を移すことができます。以前は成功していた多くのセキュリティ手順や戦略は、もはや完全には有効ではありません。その結果、古いサイバーセキュリティ技法や技術に対する組織の投資は、限定的な結果と不十分な保護をますますもたらしています。

物理的なオブジェクトやコードシグネチャに固定されたアプローチやフレームワークに依存することはもはや不可能です。攻撃の頻度と規模が増加し、今日の世界が相互接続されている状況では、企業はネ

[181] NIST. (2024) Computer Security Resource Center - Risk Appetite is defined in the glossary with links to the standards that provide more detail on risk appetite in cybersecurity.
[182] NIST. (2020) *NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)*.

ットワーク構成から検出および防止方法まで、すべてを再評価する必要があります。

シンプルなユーザーエクスペリエンス

ZTA は、ネットワークとその他のコンポーネントの両方を含む環境全体で統一的なアクセスモデルを実装することで、ユーザーエクスペリエンスを合理化します。すべてのアクセス要求は、明示的であれ暗黙的であれ、次のようなさまざまな決定を含む同じロジックで提示されます。あなたは誰ですか？具体的にどのデータが必要ですか？今すぐこのアクセスが必要ですか？承認されると、ユーザーは指定された期間、特定のリソースへのアクセスを許可されます。

ZTA モードでは、以下はありません。

- 許可または拒否する可能性のあるレガシーアクセス制御リスト（ACL）を持つネストされたグループの複雑な図。これは予期しない結果をもたらします。
- 無関係になる可能性のある意思決定者によって管理されるグループのレイヤー。
- 所有者が移動した孤立したグループ、またはローカル対グローバルなどの予測不可能な認可メカニズム。
- プロビジョニング、プロビジョニング解除、またはアクセスの取り消しのいずれかが遅延した場合。すべてのアクセス要求は、一貫してジャストインタイムでポリシー決定ポイント（PDP）によって処理されます。

アタックサーフェスの減少

ZTA は、厳格なアクセス制御、継続的な認証、および最小特権の原則をネットワークとインフラストラクチャ全体に実装しています。これには、ネットワーク内にすでに脅威が存在する可能性があると仮定し、アクセスと権限に対して「決して信頼せず、常に検証する」アプローチを採用することが含まれます。ゼロトラストは、ユーザー、デバイス、およびアプリケーションのアイデンティティとセキュリティポスチャを継続的に検証することで、攻撃者によるラテラルムーブメントを防止し、セキュリティ侵害の潜在的な影響を制限することを目的としています。

複雑さの軽減

本書の冒頭で述べたように、企業のデジタルフットプリントは拡大の一途をたどっており、IT 環境を複雑化させる可能性があります。特に、実際のアクセスの決定は、それが要求されたり、使用されたり、必要になったりする数ヶ月から数年前に行われます。それらの意思決定者は、多くの場合、時間の経過とともに有機的に移動し、誰もアクセス権を取り締まることのない孤立したオブジェクトを残します。このような複雑さは、組織にとって最大のセキュリティ課題の 1 つで、これにより、可視性の低下、複雑な構成、弱点、および脆弱性が追加で発生することが多く、攻撃者によるエクスプロイトが容易になります。ZT アプローチは、この複雑さを軽減します。

このような複雑さの例を次に示します。

- クラウド環境とオンプレミス環境のハイブリッド統合
- マルチクラウドアーキテクチャ
- エッジコンピューティング

アクセスコントロールポリシーの観点からは、これらの各例はきわめて複雑です。ZT 環境では、すべてのアプリケーションアクセスが潜在的に悪意がある、または望ましくないと想定されます。したがって、組織のネットワーク全体にわたるすべての境界とパスを取り締まろうとする代わりに、アプリケーションとデータの島が作成されます。これらの島々は、もっと集中的に保護することができます。これは、ZT 戦略を確立するために、標準的なセキュリティメカニズムよりもはるかに多くの属性が必要となるためです。組織がネットワークを簡素化し、俊敏性を優先してデータセンターを統合する中、ZT は、アプリケーションとアイデンティティの周囲に境界を作成することで、あらゆるセキュリティアーキテクチャの複雑さを軽減する拡張セキュリティメカニズムを提供します。これは、各ユーザーアイデンティティが実行できる操作の厳密な管理と、個人のアクセス権と権限に関する可視性の厳格化も意味します。特にサードパーティーやサプライヤーが対象となります。

最小特権の原則の適用

この原則は、ユーザーとプログラムはタスクを完了するために必要な権限のみを持つべきであるというものです。基本的に、ユーザーはビジネスを遂行するために必要なものに、必要なときに正確にアクセスできます。アクセスプロビジョニングの簡素化により、セキュリティ運用チームとガバナンスチームにとって、絶えず変化するセキュリティランドスケープの管理が非常に容易になります。また、適切なサービスを適切なタイミングで提供することで、エンドユーザーのエクスペリエンスを高めます。

セキュリティポスチャをさらに強化するには、User and Entity Behavior Analytics (UEBA), Privileged Access Management (PAM) 、アイデンティティアクセスガバナンスなどの追加対策の導入を検討する必要があります。これらのプラクティスは、ユーザーの行動に関する洞察を提供し、特権アクセスを管理し、アイデンティティ関連のアクセス制御に対するガバナンスを確実にすることで、ZTA フレームワーク内の最小特権の原則を強化します。

セキュリティポスチャとレジリエンスの向上

組織の外部から、ZTA は IT インフラと個々の資産に対するハッカーの可視性を低減し、攻撃者のアタックサーフェスを狭めます。

組織内からは、ZTA は次のことを強調しています。

- 最小限のラテラルムーブメント
- クロスネットワークおよびクロスシステム攻撃の機会の制限
- あらゆるセグメントの内部に侵入した悪意のある行為者への露出の低減

外部ユーザーをネットワークの狭い領域内に封じ込めコントロールすることで、IT インフラストラクチャ全体のレジリエンスを確保します。そのため、攻撃の発生を封じ込め、小さな影響範囲で対処し、素

早く以前の状態に戻せます。アタックサーフェスが縮小されているため、ZT 実装内でユーザーに権限が与えられない限り、内部または外部のユーザーが開始したすべてのソーススキャンとマッピングは失敗します。コントロールプレーンとデータプレーンが分離された 2 層アーキテクチャは、ユーザーとそれぞれのデバイスの適切な認証と認可があって初めて、ユーザーが組織のネットワーク内で許可されるようにします。

インシデントの抑制と管理の向上

組織のインシデント管理プロセスをより効果的かつ効率的にすることは、ZTA の主な目標の 1 つです。この目的を達成するためのキードライバーは、ZTA の背後にあるコアと設計の原則に組み込まれています。一つは、他の証明がない限り、いかなる実体も信頼できないという仮定です。もう 1 つは、侵害が継続的に発生する可能性があり、システム内のエンティティの振る舞いを継続的に監視する必要があるという前提です。ネットワークアクセスのマイクロセグメンテーションと継続的な認可により、攻撃者のラテラルムーブメントをより適切に制御できるため、潜在的な侵害の影響範囲が縮小されます。侵害が発生した場合、組織は、インシデントの範囲が限られているため、より効果的な封じ込めと、根絶と修復が容易になることで、イベントの影響を制限できます。さらに、ZTA に含まれる継続的なモニタリング機能により、異常やインシデントをより効果的に特定できます。インシデント関連のデータは PDP の更新にも使用されます。これにより、動的なポリシー定義とその適用が可能になります。これらの予防措置により、組織のネットワーク全体へのインシデントの拡散がさらに制限されます。

12.1.2 ゼロトラストのビジネス目標

技術目標と同様に、ゼロトラストのビジネス目標も、組織のセキュリティポスチャの強化、機微データの保護、および ZT の実際のビジネス価値の実証に役立ちます。以下にいくつかの事業目的と ZT との関係を示します。

リスクの軽減

- ゼロトラストは、組織全体のサイバーセキュリティリスクの軽減に役立ちます。このアプローチを採用することで、企業はネットワーク境界の内外に脅威が存在することを想定したプロアクティブなセキュリティモデルを実装します。
- 従来のセキュリティモデルは、ネットワーク内部のすべてが信頼できることを前提に、境界ベースの防御に依存していました。しかし、サイバー脅威の巧妙化が進み、リモートワークやクラウドコンピューティングの台頭により、こうした境界中心のアプローチは、もはや不十分です。
- ゼロトラストは、厳格なアクセス制御、継続的な認証、および最小特権の原則を適用することでリスクを軽減します。つまり、脅威アクターがネットワークにアクセスできたとしても、その移動や機微リソースへのアクセスが制限されるため、セキュリティ侵害の潜在的な影響が制限できます。

コンプライアンスの向上

- 規制要件や業界標準への準拠は、企業、特に規制の厳しい金融、医療、および政府機関で業務を行う企業にとって非常に重要です。
- ZT は、機密データやリソースへのアクセスをきめ細かくコントロールすることで、組織のコンプライアンス向上を支援します。ZT の原則を導入することで、企業は規制当局や監査人に対して、データやシステムを保護するための積極的な措置を講じていることを立証できます。
- GDPR や HIPAA のような規制では、組織は強固なアクセス制御とデータ保護対策を実装する必要があります。ZT は、厳格な認証、暗号化、およびアクセスポリシーを適用することで、これらの要件に対応しています。

組織文化とリーダーシップのリスク選好との整合

- ゼロトラストの導入には、現場の従業員から経営トップまで、組織のあらゆるレベルからの支持が必要です。セキュリティ意識、アカウンタビリティ、および継続的改善の文化が醸成されます。
- ZT は、リスクの軽減とレジリエンスを優先するプロアクティブおよび適応的なセキュリティアプローチを提供することで、経営陣のリスク選好と一致します。事後対応型のセキュリティ対策だけに頼らず、リスクを継続的に評価・軽減することの重要性を強調しています。
- ZT の原則を取り入れることで、組織はサイバーセキュリティとレジリエンスへの取り組みを示すことができ、顧客、パートナー、および利害関係者との間の信頼と信用を高めることができます。

12.1.3 ゼロトラストの柱と成熟度モデル

ZT のセキュリティ原則は、次の図に示すように、組織の管理ドメインに広く一致する柱に分類されています。これらは連携して動作し、重要な資産やリソースの保護を強化するように設計されています。これらの柱とそれぞれの能力および機能は、US Cybersecurity and Infrastructure Security Agency（CISA）の ZT 成熟度モデル[183]および DoD ZT Reference Architecture[184] で説明されています。柱の描写は一部異なりますが、モデルは基本的に同等であり、根本的に一致しています。

ZT のセキュリティ戦略とフレームワークの機能は、クラウドセキュリティ責任共有モデル（SSRM）と組み合わせて使用し、CSP が提供するインフラストラクチャのセキュリティとサービスを活用して、クラウド配備のセキュリティを確保できます。エンタープライズセキュリティ戦略として、ZT はマルチクラウドおよびハイブリッド環境のセキュリティ保護にも適用できます。

CISA ZTMM の柱と横断的能力を以下に示します。

[183] CISA. (2023) Zero Trust Maturity Model

[184] DOD. (2022) Department of Defence (DOD) - Zero Trust Reference Architecture

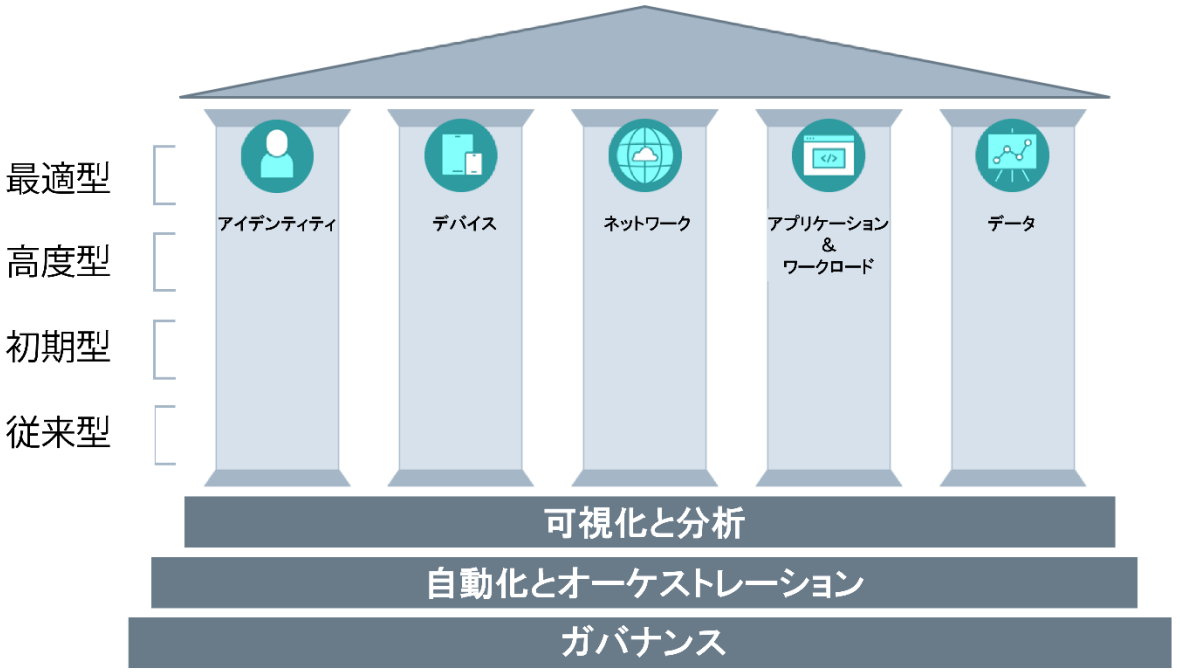


図 67: CISA ゼロトラスト成熟度モデル

- **アイデンティティ（一部のモデルではユーザーとも呼ばれる）：** 個人、非個人、および統合されたエンティティによるデータ、アプリケーション、資産、サービス（DAAS）へのアクセスに関する、保護、制限、および強制で、これらには、多要素認証（MFA）や CMFA などのアイデンティティ、クレデンシャル、およびアクセス管理機能の使用が含まれます。組織は、すべてのインタラクションを保護およびセキュアにしながら、ユーザーのアクセスと特権を統制するために、アクティビティパターンを継続的に認証、認可、および監視する機能を必要としています。ロールベースアクセス制御（RBAC）と属性ベースアクセス制御（ABAC）は、この柱内のポリシーに適用され、動的なコンテキストベースのアクセスポリシーに基づいてユーザーがアプリケーションやデータにアクセスすることを認可します。
- **デバイス:** ZT アプローチでは、すべてのデバイスの識別、認証、認可、インベントリ、隔離、セキュリティ保護、修復、およびコントロールを行う機能を備えることが重要です。エンタープライズデバイスのリアルタイム保証検証とパッチ適用は、この点で重要な機能です。モバイルデバイスマネージャや接続コンプライアンスプログラム（compliance-to-connect）などの一部のソリューションは、デバイスのセキュリティハイジーンを検証するための貴重なデータを提供します。すべてのアクセス要求に対して、適切な検証（侵害状態、異常検出、ソフトウェアのバージョンとパッチ状況、保護状況、暗号化の有効化など）を実施する必要があります。
- **ネットワーク:** ZT アプローチでは、組織はネットワーク環境（オンプレミスとクラウド/オフプレミス）を論理的に（仮想的に）セグメント化し、また、物理的に分離、隔離、およびコントロールする必要があります。これには、きめ細かいアクセス制御とポリシー制限の実装が含まれます。マクロセグメンテーションによって周辺がより洗練されるにつれて、マイクロセグメンテーションを有効にすると、DAAS の要素の保護とコントロールが強化されます。次のことが重要になります。

- 特権アクセスの制御
- 内外のデータフローの管理
- ラテラルムーブメントを防ぐ

- **アプリケーションとワークロード**:アプリケーションとワークロードには、オンプレミスのシステムまたはサービスのタスクと、クラウド環境で実行されるアプリケーションまたはサービスのタスクを含める必要があります。ZT ワークロードは、アプリケーションレイヤーからハイパーバイザーまで、完全なアプリケーションスタックにまたがる必要があります。アプリケーション層、コンピューティングコンテナ、および仮想マシンのセキュリティ保護と適切な管理は、ZT の導入の中心となるはずです。コードレビュー、脆弱性スキャン、およびセキュリティテストのための堅牢なプロセスをソフトウェア開発ライフサイクル全体にわたって実装して、リスクを軽減し、セキュリティ侵害を防止することが重要です。内部のソースコードと共通ライブラリは、アプリケーションのセキュリティを最初から確保するために、DevSecOps の開発手法を通じて精査する必要があります。
- **データ：** ZTA は重要な DAAS を保護します。ZTA の導入を成功させるには、組織の DAAS を明確に理解することが重要です。組織は、DAAS をミッションクリティカル度に応じて分類し、この情報を使用して ZT アプローチ全体の包括的なデータ管理戦略を開発する必要があります。これは、データの分類、スキーマの開発、および保存中データと移動中データの暗号化によって実現できます。データ著作権管理（DRM）、データ損失防止（DLP）、ソフトウェアデファインドネットワーキング（SDN）、および粒度の高いデータタグ付けなどのソリューションは、データを保護する上で重要です。
- **可視性と分析**（CISA モデルにおけるクロスカッティング機能）：パフォーマンス行動、およびさまざまな ZT の柱にわたるアクティビティのベースラインをよりよく理解するために、状況に応じた重要な詳細情報を含める必要があります。この可視性により、異常検出が改善され、セキュリティポリシーの動的な変更や、状況に応じたリアルタイムのアクセス決定が可能になります。さらに、センサーデータやテレメトリなど、他のモニタリングシステムを使用して、環境に何が起きているかを全体像を把握するために役立ちます。これはレスポンスに使用するアラートのトリガーに役立ちます。ZT エンタープライズはトラフィックをキャプチャして検査し、ネットワークテレメトリを超えた先をパケットを調べて見通し、脅威を観察し、防御を適切に方向づけます。
- **自動化とオーケストレーション**（CISA モデルのクロスカッティング機能）：手動のセキュリティプロセスを自動化して、ポリシーベースのアクションを全社規模で迅速かつスケーラブルに実行できます。Security orchestration, automation, and response（SOAR）により、セキュリティが向上し、応答時間が短縮されます。セキュリティオーケストレーションは、security information and event management（SIEM）やその他の自動化セキュリティツールを統合し、さまざまなセキュリティシステムの管理を支援します。自動化されたセキュリティ対応には、事前対応的な指揮統制のために、定義されたプロセスと、すべての ZT エンタープライズにわたる一貫したセキュリティポリシーの実施が必要です。
- **ガバナンス**（CISA モデルにおけるクロスカッティング機能）：ガバナンスは、ビジネス戦略、リスク、および IT の視点について相互の整合を確実にする重要な機能です。ガバナンスは、アクセスやプロセスデータなどの ZTA ポリシーを定義するために役立ちます。技術以外の観点からも、ガバナンスによって複雑さを管理し、軽減する必要があります。複雑さの軽減に成功する

には、プロテクトサーフェスに焦点を当てる必要があります。技術的な観点からは、ガバナンスポリシーは ポリシー実施ポイント（PEP）によって実施される必要があります。

CISA ZTMM は、ZT の柱（アイデンティティ、デバイス、ネットワーク、アプリケーションとワークロード、およびデータ）と機能（可視性、自動化、ガバナンス）にわたる成熟段階（従来型、初期型、高度型、最適型）の概要を示すので、組織が ZT 戦略を強化するために役立ちます。これらの成熟段階は、組織がより安全な ZTA に向けて前進するために必要な施策を評価、計画、実施するのに役立ちます。以下の図に示されている CISA ZTMM の道のりは、最適な ZT の成熟に向けた道筋を表しています。この実践的なビジュアル表現は、ZT のさまざまな成熟度レベルを通じて企業が前進する方法を示しています。

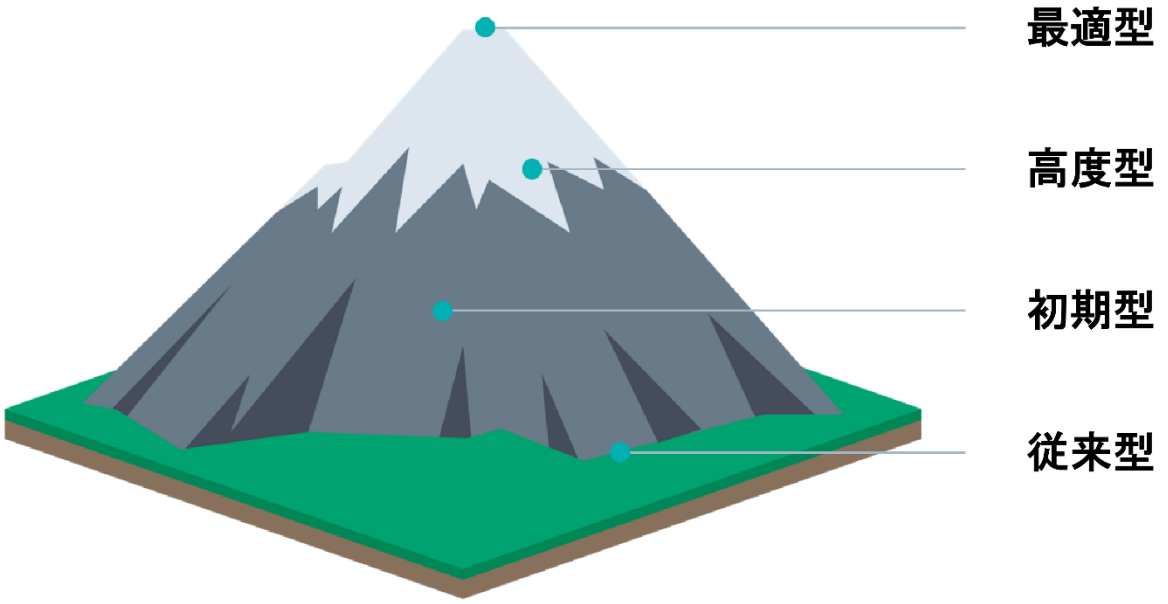


図 68: ZT 成熟度の推移

CISA ZTMM を効果的に活用するには、フレームワークを把握し、機能を磨き、現在の ZT の成熟度を評価します。最後に、成熟度を上げるためのステップを計画し、優先順位付けモデルを使用して、組織のプロジェクトや優先順位と整合させます。

各成熟段階に関連する特性と目的を把握することで、組織は現在の状態を評価し、改善すべき領域を特定し、ゼロトラスト成熟過程を進めるためのロードマップを開発できます。ゼロトラスト成熟度モデルの各成熟度の特徴を下表に示します。

成熟度のステージ	説明	特徴
従来	従来の成熟段階は、組織がゼロトラストを目指す出発点を表しています。この段階では、内部ネットワークトラフィックに暗黙	· セキュリティ制御は、主にファイアウォールや侵入検知システム（IDS）などの境界防御に基づいています。

	の信頼を置くなど、通常、セキュリティ手段は境界に焦点を当てています。	・ リソースへのアクセスは、多くの場合、ユーザーのアイデンティティやデバイスのポスチャではなく、ネットワークの場所に基づいて許可されます。 ・ セキュリティポリシーは静的で事後対応的な傾向があり、ユーザーアクティビティやネットワークトラフィックに対する可視性に制限があります。
初期	組織は、セキュリティポスチャを強化するために、初期の成熟段階でゼロトラストの基本原則と技術を採用しています。	・ 組織はアイデンティティ管理プロセスを一元化し、重要なシステムのパスワードポリシーや MFA などの基本的な認証コントロールを実装し始めます。 ・ エンドポイントの保護ソフトウェアやデバイスの暗号化などのデバイスセキュリティ対策は、エンドポイントのセキュリティポスチャを改善するために導入されることがあります。 ・ アタックサーフェスを減らし、ネットワーク環境内のラテラルムーブメントを制限するために、ネットワークセグメンテーションの取り組みが開始される可能性があります。
高度	高度の成熟段階では、組織は複数のドメインにわたってゼロトラストの実践と技術の導入を大幅に進めています。	・ アイデンティティアクセス管理の一元化と自動化が進み、アダプティブ認証や継続的認証などの強固な認証メカニズムが導入されます。 ・ デバイスの健全性やコンプライアンス状況の継続的なモニタリング、セキュリティ脆弱性の自動修復など、デバイスのセキュリティ対策が強化されます。 ・ ネットワークセグメンテーションの取り組みは拡大され、ユーザーコンテキストとアプリケーションの機密性に基づく動的なアクセス制御と、暗号化された通信チャネルが広く展開されます。
最適	最適成熟段階は、ゼロトラストの成熟度が最も高い段階であり、組織はセキュリティ戦略と運用にゼロトラストの原則を完全に統合しています。	・ アイデンティティガバナンスプロセスは完全に自動化されており、ユーザーのオンボーディング、オフボーディング、アクセスリクエストのためのセルフサービス機能、アイデンティティ関連の脅威を検出して軽減する高度な分析機能を備えています。 ・ デバイスのセキュリティ対策は、包括的な endpoint detection and response（EDR）機能とプロアクティブな脅威ハンティングのための高度な脅威インテリジェンスを含むゼロ

		トラストアーキテクチャに緊密に統合されています。 · ネットワークセグメンテーションは、自動化された脅威の検出と対応メカニズムをネットワークファブリックに統合し、ゼロトラストアクセス制御をアプリケーションレベルで実施することで、きめ細かく適応します。

テーブル 10: ゼロトラスト瀬熟度ステージ

12.1.4 ZT の設計および実装手順

ZT の採用の戦術的な側面を考慮すると、レジリエントなアーキテクチャを構築するための 4 つの主要な設計原則と、リスクベースの優先順位付けで組織資産を保護するための対話型および段階的な実行のための反復可能な 5 ステップの実装プロセスがあります。

これらと並んで、CISA ZTMM は、5 つのステップの一部ではないが、組織のゼロトラスト導入への旅における ZT の段階的な進行を理解する上で重要です。

ZT の設計原則には次のものが含まれます。

- **ビジネス成果にフォーカス**:ZT が組織の主要なビジネス目標とどのように連携し、サポートしているかを理解します。
- **徹底設計**:外部に拡張する前に、組織内から開始するセキュリティ戦略の策定。
- **アクセスが必要なユーザーまたは対象の特定:**特定のリソースへのアクセスを必要とするユーザーおよびデバイスの識別。
- **主要トラフィックの検査とログ**:標的を絞ったアプローチとして、潜在的な脅威に対する重要なアクティビティの監視と記録を目指します。

反復可能な ZT 実装プロセスの 5 つのステップは次のとおりです。

- **ステップ 1: プロテクトサーフェスを定義**[185]します。構成データやリソース（DAAS 要素）を含む重要なビジネス情報システムを特定および評価し、ビジネスリスクレベルを分類し、実装の優先順位付けに役立つ現在のセキュリティ成熟度を評価します。
- **ステップ 2: トランザクションフローのマッピング**:　システムや組織内外の情報の移動、各フローの潜在的な分類を理解します。その目的は、ZTA の設計と開発へのインプットとして、最も機密性の高い情報と資産がどこにあるのか、アクセスを制御するために最も影響を与えることができる場所はどこかを理解することです。

[185] CSA. (2024) *Defining the Zero Trust Protect Surface*.

- **ステップ 3: ゼロトラストアーキテクチャ（ZTA）の構築**：主要なビジネスシステムと資産に対する ZT 保護の実装に必要なインフラストラクチャ、機能、およびコントロールを設計および開発します。
- **ステップ 4: ZT ポリシーの作成**：ポリシー制御を実装し、ネットワーク、システム、データアクセス、および主要なビジネスシステムと資産のセキュリティに関するガイドラインとルールを確立します。
- **ステップ 5: ネットワーク（環境）の監視と保守:**継続的なセキュリティを確保し、新たな脅威に適応するために、ZT 環境を継続的に監視します。

これらの要素は、組織の目的とリスクに沿った効果的な ZT セキュリティ戦略を形成し、実行するために不可欠です。

12.1.5 ゼロトラストとクラウドセキュリティ

以下の表は、ZT の原則をセキュリティドメインにマッピングして、リスクを軽減し、組織全体のサイバーセキュリティポスチャを強化する方法をまとめたものです。

セキュリティドメイン	ゼロトラストの原則
組織マネジメント	企業のセキュリティおよび接続戦略としての ZT、ZT 文化で最適に実装
アイデンティティとアクセス管理	コンテキストベースでユーザー、デバイス、 およびアクセス要求を認証する、継続的でフィッシング耐性のある MFA
セキュリティモニタリング	すべてを監視。侵害を推定し、疑わしいアクティビティを早期発見し、アクセスを動的に調整
ネットワーク	マイクロセグメンテーション、ZT ネットワークアーキテクチャ、Software-Defined Perimeter
ワークロード	ZT デバイスとワークロードのセキュリティと完全性の検証、マルウェアとデータ流出のモニタリング 、ZT ワークロードアクセス制御
アプリケーション	きめ細かい最小特権でのアクセス認可と職務分掌。ユーザー権限は必要最小限のデータと機能に限定
データ	厳密な ZT データアクセス制御により、保存中、移動中、および使用中のデータを分類、保護、監視

テーブル 11: CCSK のセキュリティドメインと対応するゼロトラストの原則

ここでは、ZT セキュリティの重要な原則が主要なクラウドセキュリティドメインにどのように影響するかを説明します。

- ***アイデンティティとアクセス管理（IAM）***：ゼロトラストの実装の中心であり、強固で継続的な認証と詳細な認可に焦点を当て、リソースへのセキュアなコンテキスト認識アクセスを実現します。
- **セキュリティモニタリング**：ゼロトラストの原則を統合し、潜在的な侵害を想定し、戦略的なネットワークアクセス制御と厳格なインシデントレスポンス手順を通じて影響を最小限に抑えることで、運用上のセキュリティ監視とアラートを強化します。
- **ネットワーク**：ゼロトラストアクセスを実施し、マイクロセグメンテーションを使用してアタックサーフェスを減らし、仮想ファイアウォールと暗号化を適用してセキュリティを確保し、最小特権や継続的な認証などのゼロトラストの原則に従ってネットワークアクセスを効果的にコントロールします。
- **エンドポイントセキュリティ**：ゼロトラストの原則を適用し、マルウェアやランサムウェアなどの脅威から保護し、クラウドリソースにアクセスするデバイスの厳格な認証、認可、およびアクセス制御を実現します。

これらを徹底的に調べるには、経験豊富なサイバーセキュリティの専門家が提供する ZT ユースケースを研究することをお勧めします。ゼロトラストトレーニングの Certificate of Competence in Zero Trust Training に記載されている CSA のユースケース集を勉強することもできます。

12.2 人工知能

人工知能（AI）は、クラウドでホストされるサービスとして、およびクラウドのセキュリティを強化する新しいツールの両方として機能します。通常、AI サービスはクラウドでホストされますが、オンプレミスのホスティングソリューションは特定のアプリケーションとして使用できることに注意してください。さらに、AI はクラウドセキュリティにおいて二面的な役割を果たします。クラウドセキュリティ対策の強化に活用できる一方で、新たな攻撃ツールとしてのリスクも伴います。AI を搭載したアルゴリズムには、脆弱性を発見し、エクスプロイト攻撃を作成し、高度な攻撃を実行する機能があり、AI 駆動型の脅威から保護するために AI サービスをセキュアにし、堅牢なセキュリティ対策を実施することの重要性が強調されています。

12.2.1 人工知能とクラウドセキュリティ

先に説明したゼロトラストと同様に、AI は複数の重要なクラウドセキュリティドメインと交差しています。さらに、今日のゼロトラストアーキテクチャは、不可能な旅行ポリシーの適用やコンテキストに応じたアクセス決定など、さまざまなタスクを AI 技術に多く依存しています。この交差点は、クラウドランドスケープ全体でセキュリティプラクティスを強化する上で AI が果たす役割の進化を強調しています。

セキュリティドメイン	AI アスペクト
組織マネジメント	AI がどこでどのように
アイデンティティとアクセス管理（IAM）	AuthN/Z
セキュリティモニタリング	AI のモニタリングとロギング、検出と分析のための AI
ネットワーク	自前またはクラウドが AI をホスティングする際のネットワークセキュリティ
ワークロード	セキュアな AI ワークロードホスティング
アプリケーション	AI 統合、API セキュリティ
データ	トレーニングデータ、データストレージ、データ漏洩

テーブル 12: セキュリティドメインと AI アスペクトの交差

- 組織管理のためには、組織は AI ポリシー、プロバイダ、および期待値を決定する必要があります。サービスの詳細に基づいてアカウントとサービスが確立され、セキュリティコントロールが有効になります。
- 他のクラウドサービスと同様に、IAM は最も重要なセキュリティコントロールになるでしょう。AI の場合、これはユーザー、管理者、AI モデル/ワークロード自体、および基盤となるトレーニングや分析データへのアクセスに影響します。
- モニタリングには、プロンプト、出力、およびデータアクセスを含める必要があります。
- AI サービスをホストする際には、基盤となるネットワークのセキュリティを確保する必要があります。また、任意の AI as a Service（AIaaS）プラットフォームへのアクセスを制限するために、ネットワークセキュリティが必要になる場合もあります。
- AI を実行する、または AI にアクセスするワークロードは、基本的なセキュリティプラクティスに従う必要があります。
- アプリケーションレイヤーには、アプリケーションロジックや API セキュリティなど、多くの AI セキュリティが実装されています。
- すべてのトレーニング、分析、およびその他のデータリポジトリのセキュリティを確保する必要があります。こうした保管場所には、しばしば膨大な量のデータが存在します。

12.2.1.1 AI とクラウドセキュリティの相互作用

AI は、進化するサイバーセキュリティの課題に対処するために、組織がデジタル環境でセキュリティにアプローチする方法を再構築しており、クラウドセキュリティとの交差はパラダイムシフトを表しています。

組織が重要なワークロードや機密データをホストするためにクラウドサービスへの依存度が高まる中、AI 技術を統合することで、セキュリティ対策を強化し、リスクを軽減する新たな機会が生まれます。AIaaS の提案から、AI モデルの配備のためのクラウドインフラストラクチャの活用まで、クラウド環境のセキュリティ保護に AI の力を活用するためのさまざまなオプションがあります。

AI で強化されたセキュリティツールは、脅威の検出、アクセス制御、およびポリシーの適用に影響を与えます。さまざまな AI 利用モデルとクラウドセキュリティツールとの統合を理解することは、防御を強化し、現代のサイバーセキュリティランドスケープの複雑さをナビゲートしようとする組織にとって不可欠になります。

AI とクラウドセキュリティは、次の 4 つの主要なカテゴリに分類され、さまざまな方法で交差します。

1. **利用者のための AI as a Service (完全な SaaS)**: このモデルでは、AI はクラウドプロバイダによってすぐに利用できる完全なサービスとして提供されます。Claude のようなオファーリングでは、組織独自のモデルを構築またはトレーニングすることなく、AI 機能を活用することができます。完全な SaaS（Software as a Service）は、組織で承認されたサービスだけを簡単に選択できるため、技術的な深い専門知識を持たずに AI を迅速に導入したい組織に最適です。このカテゴリのほとんどの製品には、データプライバシーのアップグレード、承認されたデータのみを許可するオプション、およびプロンプトと結果を簡単に追跡する機能が含まれています。

2. **AI as a Service (PaaS と基盤モデルのホスティング[186])**: クラウドプロバイダは、AI モデルをホストして実行するための基盤となるインフラストラクチャとツールを提供しますが、モデルの開発とアプリケーションの構築は利用者に任せています。AWS Bedrock はその一例で、基盤モデルとホスティング環境を提供しますが、利用者はその上に構築する独自のソリューションを作成します。このモデルでは、組織による高度なコントロールとカスタマイズが可能になり、インジェクションやジェイルブレイクなどの敵対的な攻撃から保護します。その他の機能には、セキュアなトレーニングデータ、セキュアなアプリケーション統合および配備環境、およびセキュアなユーザーとアクセスなどがあります。

3. **Cloud as workload host for AI (Bring Your Own Model)**: このシナリオでは、組織は独自の AI モデルをゼロから開発するか、市販のモデル（コード）を配備して、クラウドをホスティング環境としてのみ使用します。データの準備からモデルのトレーニングと導入まで、AI のライフサイクル全体を担います。クラウドは生のコンピュートリソースを提供するだけです。これは、最も柔軟性に優れていますが、組織内の AI スキルが最も必要であり、組織内アプリケーションを構築する場合と同じ責任があります。

4. **AI 拡張セキュリティツール**: ホスティングの選択肢に加え、AI をさまざまなクラウドセキュリティ製品に組み込み、よりスマートで効果的なものにします。AI を活用した脅威の検出、インテリジェントなアクセス制御、およびポリシーの自動適用などが考えられます。AI が成熟するにつれて、従来のセキュリティソリューションがさらに強化されることを期待できます。

[186] In the context of AI as a service (AIaaS) within a platform as a service (PaaS) model, foundation model hosting involves offering infrastructure and resources optimized for deploying, running, and managing foundational AI models.

12.2.2 AI 拡張セキュリティツール

AI と機械学習（ML）は、マルウェア検出やユーザー行動分析などのユースケースで、すでにセキュリティ分野で幅広く使用されています。大規模言語モデル（LLM）の出現により、特にデータセットの分析と優先順位付けのために、AI で強化されたセキュリティツールの新しいカテゴリが急速に出現しています。

図 69: AI がセキュリティツールとプロセスを強化するユースケース

セキュリティにおける AI および LLM アプリケーションの主要な分野は、次のとおりです。

- **脅威の検出**：AI と ML を活用してネットワークトラフィックとシステムの動作を分析し、新たな脅威の特定を強化すると同時に、LLM を活用して洞察力のある脅威インテリジェンスレポートを生成します。AI アルゴリズムは、膨大なデータをふるいにかけて、疑わしいパターンや潜在的な脅威を、従来のルールベースのシステムよりもはるかに高速かつ正確に特定できます。これにより、セキュリティチームは絶えず進化する脅威の状況を先取りすることができます。
- **ログ分析**：自然言語処理を含む AI と ML を活用して、非構造化ログデータを分析し、セキュリティパターンと異常を検出し、実用的な洞察を提供します。現代のクラウド環境では、人間が手動でレビューすることが不可能な膨大な量のログデータが生成されます。AI はこれらのログを自動的に解析し、異なるシステム間でイベントを相関し、セキュリティインシデントを示す可能性のある異常にフラグを付けることができます。
- **インシデントレスポンス**：AI は、ワークフローの自動化、ML モデルを用いたリスク別のアラートの優先順位付け、および LLM の採用による詳細なインシデントレポートの生成とアクションの推奨により、インシデントレスポンスを強化します。脅威が検出されると、AI は侵害の範囲を調査し、根本原因を特定し、影響を受けたシステムの分離、または侵害されたクレデンシャルの無効化で、被害を自動的に封じ込めることもできます。これにより、応答時間が大幅に短縮されます。

- **ポスチャ評価：**AI を活用して、すべてのドメインに渡って組織のセキュリティを継続的に監視および評価し、ML を活用して設定ミスやセキュリティの不備をピンポイントで特定し、同時に LLM はセキュリティ対策を強化するための詳細なサマリーと実行可能な推奨事項を提供します。
- **セキュアなコード解析：**AI を活用してソースコードの脆弱性を精査し、ML モデルを通じて推奨事項を精緻化し、さらに LLM を活用してセキュアなコーディング技法を解説および提案します。アーキテクチャリスク分析、動的分析、およびその他のプロアクティブな手法を含むこの「シフトレフト」アプローチは、本番環境に移行する前に課題をキャッチし、リスクを軽減します。
- **マルウェア分析：**AI はコード解読や動作分析などのタスクを自動化することでマルウェアのリバースエンジニアリングを強化し、同時に ML はマルウェアファミリーを分類してパターンを特定し、さらに LLM は詳細な分析レポートを生成してリサーチャーのコラボレーションを促進します。
- **リスクの優先順位付け**：AI と ML を活用して、セキュリティツールや外部ソースからのデータを分析し、複数の要因に基づいてリスクを定量化し、そしてリスク評価を明確にして関係者に効果的に連携します。リスクを定量化することで、組織は最大限の効果を得るために限られたセキュリティリソースをどこに集中すべきかについて、データに基づいた意思決定を行うことができます。
- **エンタイトルメント管理**:AI と ML は、ロールとアクティビティパターンを分析することでアクセス制御を強化し、アクセス許可の合理化、最小特権に基づくポリシーの最適化、およびアクセスレビューレポートの生成の自動化を実現します。

AI や LLM の進歩が進む中、サイバーセキュリティ領域では、さらに革新的な応用が期待されます。ただし、組織は、バイアス、説明可能性、敵対的攻撃など、AI の潜在的なリスクと制限にも留意する必要があります。AI のパワーと人間の専門知識および監視を組み合わせることで、セキュリティチームは機能を強化し、ますます複雑化するデジタルランドスケープで進化する脅威の先を行くことができます。

12.3 脅威と脆弱性の管理

脅威と脆弱性の管理（TVM）により、組織は動的なクラウド環境における脅威をより適切に予測、検出、および対応できるようになり、サイバー攻撃に対する脆弱性を軽減し、継続的なセキュリティコンプライアンスを確実にします。さらに、TVM への AI の統合は、クラウド環境のセキュリティ保護における標準的なプラクティスになると予想されています。このセクションでは、クラウドサービスの脅威管理におけるさらなる革新と課題を議論する舞台を設定します。

次の表に、セキュリティドメインと交差する TVM の側面を示します。

セキュリティドメイン	**TVM** アスペクト

組織マネジメント	組織ポリシー、影響範囲のコントロール、CSPM/CNAPP[187]
IAM	クレデンシャル保護、PIM/PAM
セキュリティモニタリング	検出と分析
ネットワーク	影響範囲のコントロール、フロー、DNS モニタリング
ワークロード	エンドポイントの保護、検出、対応
アプリケーション	アプリケーションと API のセキュリティ
データ	リソースポリシー、データログ

テーブル 13: 脅威と脆弱性の管理に属するセキュリティドメイン

TVM にマッピングされた各セキュリティドメインの簡単な分析を次に示します。

- **組織管理**： クラウド環境全体の影響範囲のコントロールやセキュリティポスチャ管理（CSPM/CNAPP）アクティビティの設定など、組織全体のセキュリティポリシーを確立します。
- **IAM:**クレデンシャルの保護を処理し、特権 ID 管理(PIM)と特権アクセス管理(PAM)を実装します[188]。
- **セキュリティモニタリング**： プロアクティブな脅威の検出とセキュリティイベントおよびアラートの分析のためのコアドメイン。
- **ネットワーク：** ネットワークセグメンテーションとネットワークトラフィック監視（フローログ、DNS クエリなど）による影響範囲のコントロールにより、ネットワークアクセスとトラフィックフローを制御します。
- **ワークロード:**エンドポイントの保護、脅威の検出、およびインシデント対応アクションの調整に焦点を当て、アプリケーションを実行するコンピュートインスタンス、コンテナ、およびサーバーレス機能を保護します。
- **アプリケーション** ：セキュアな設計、厳格なアクセス制御、およびアクティブな保護によってアプリケーション層を保護します。また、アプリや API 固有の脆弱性に対応するツールを活用します。

[187] Cloud Security Posture Management (CSPM) is a continuous and automated process to identify and remediate risks. Cloud-native application protection platform (CNAPP) secures the full application development lifecycle from code to production, and can replace tools, such as CSPM, System Information and Event Management (SIEM), and Cloud Workload Protection Platform (CWPP).

[188] PIM specifically deals with managing and protecting privileged identities and PAM focuses on controlling and monitoring privileged access to resources.

- **データ：**データの取り扱いに関するポリシーを定義し、データイベントを記録し、異常なアクセスパターンをスキャンし、またデータ漏洩インシデントを調査します。

12.3.1 クラウドの脅威管理のアップデート

クラウドサービスの脅威管理戦略の維持と更新に関して、それらのクラウドサービスのセキュリティ保護の責任は、関係する状況や組織によって様々な当事者に属します。たとえば、CSP はサービスをセキュアに維持する責任を負い、 組織や利用者[189]はそれらのサービスの設定と使用に責任を負います。

クラウドでは、マネージメントプレーン（CSP コンソール、API など）が攻撃者の主要なターゲットになります。アクセス鍵とクレデンシャルをローテーションし、異常な動作や不審なアクションをモニタリングすることに加えて、保護によってクラウドマネージメントプレーンのアクセスとアクティビティを防御および監視することに焦点を置くことが重要です。

マネージメントプレーンを新たな攻撃対象領域として捉える場合、以下の点を考慮します。

- **新たなアタックサーフェスとしてのマネージメントプレーン：**マネージメントプレーンが攻撃者の主要なターゲットになるため、クラウドマネージメントプレーンのアクセスとアクティビティの防御と監視に焦点を置きます。
- **脆弱性スキャン：** 脆弱性スキャンでは、CSPM、SSPM、CASB などのツールを使用して IaaS や SaaS のセットアップにおけるセキュリティ課題を特定し、修正します。また、Infrastructure as Code(IaC)スキャナを使用して、開発の早期段階で設定ミスを修正します。
- **コンテナと仮想マシンのセキュリティ保護:** CWPP/CNAPP のような最新の脆弱性管理ツールを動的なクラウド環境に活用し、スキャンを継続的インテグレーション/継続的デリバリ（CI/CD）パイプラインに統合することで、コンテナのようなエフェメラルな資産では従来の手法が頓挫する課題をプロアクティブに検出します。
- **クレデンシャルの盗難と権限のエスカレーション：** クレデンシャルの盗難や権限のエスカレーションのリスクを軽減するには、堅牢な IAM 制御の実装、最小特権アクセスポリシーの適用、定期的な権限の調整とレビュー、および疑わしいクレデンシャルの使用状況の監視が不可欠です。
- **クラウドネイティブの脅威検出:** VPC フローログ、DNS ログ、およびエージェントベースとエージェントレスの両方のソリューションなどのクラウドプラットフォーム機能を利用して、ネットワークとクラウドワークロード（CWPP/CNAPP）全体の脅威を監視および特定します。
- **ソフトウェアサプライチェーンセキュリティ：** コードまたはイメージの署名、自動化された脆弱性スキャン、セキュアなアーティファクト管理などの対策を実装し、ソフトウェアの依存関係を保護し、コードの脆弱性への対応を強化します。
- **脅威インテリジェンス：** CSP やサードパーティフィードからの脅威インテリジェンスを活用して常に情報を把握し、脅威インテリジェンスを活用して侵害の兆候を事前に探します。

[189] Cloud security practitioners, IT administrators, cybersecurity professionals, and individuals responsible for managing and securing cloud environments.

クラウド上の新たな脅威を特定し、緩和し、対応するために、組織内のチームが協力するための推奨事項と戦略は、以下の表のとおりです。

セキュリティのプラクティスまたは戦略	実装に関する推奨事項
新たなアタックサーフェスとしてのマネジメントプレーン	クラウドでは、マネージメントプレーン（CSP コンソール、API など）が攻撃者の主要なターゲットになります。 ● クラウドマネージメントプレーンのアクセスとアクティビティの防御と監視に注力 ● アクセスキーとクレデンシャルの保護とローテーション ● マネージメントプレーンのログに異常な動作や不審な動作がないか調べます
脆弱性スキャン	● Cloud Security Posture Management（CSPM）ツールは、組織の IaaS 環境をスキャンし、設定ミスやセキュリティギャップを特定します。 ● SaaS Security Posture Management（SSPM）とクラウドアクセスセキュリティブローカー（CASB）は、組織の SaaS セキュリティ設定と使用状況を評価します ● これらのツールを定期的に使用し、攻撃者がエクスプロイトする前に脆弱性や設定ミスを発見して修正します。組織にはこれらの設定をコントロールするネットワーク境界がないため、これらの設定ミスはインターネット上で即座にアクセス可能であることがしばしばあります ● IaaC（Infrastructure as a Code）スキャナを使用して、変更が本番環境に配備される前にセキュリティの誤設定を検出します。つまり、ソフトウェア開発ライフサイクルの早い段階で脆弱性を減らすためにシフトレフト戦略が配備されます。
コンテナと VM のセキュリティ保護	● 動的なクラウド環境（CWPP/CNAPP など）向けに設計された最新の脆弱性管理ツールとプロセスを使用します ● コンテナのような寿命が短い資産では、従来のスキャン手法ではうまく機能しません ● 脆弱性スキャンを CI/CD パイプラインに統合し、課題を早期にキャッチします
クレデンシャルの盗難と権限のエスカレーション	● 攻撃者は、クラウドのクレデンシャルや特権を狙って不正アクセスやピボット攻撃を行うケースが増えています ● 強固な IAM コントロールを実装します： 　○ 最小特権アクセスポリシーを使用します 　○ 権限の定期的な確認と適切なサイジング 　○ 疑わしいクレデンシャルの使用状況を監視します
クラウドネイティブの脅威検出	● クラウドプラットフォームは、ネットワークおよびホストベースの脅威検出のためのネイティブ機能を提供します

	● VPC フローログや DNS ログなどの機能をネットワークセキュリティモニタリングに活用 ● クラウドワークロード上の脅威検出にエージェントベースまたはエージェントレスソリューションを使用（CWPP/CNAPP）
ソフトウェアサプライチェーンセキュリティ	● 組織のソフトウェア依存関係を保護し、ソフトウェア部品表を把握することで、コードベースやイメージベースの脆弱性に効率的に対応できるようになります。 ● 次のようなコントロールを実装します。 ○ コードまたはイメージの署名と整合性の検証 ○ 脆弱性スキャンとパッチ適用の自動化 ○ セキュアなアーティファクトリポジトリとリリース管理プロセス
脅威インテリジェンス	● 組織の CSP の脅威インテリジェンスフィードを活用して、クラウド固有の脅威とトレンドを常に把握 ● サードパーティの脅威インテリジェンスで補足し、より包括的なビューを得ます ● 脅威情報を使用して、セキュリティ侵害の兆候をプロアクティブに探し、検出を改善します。

テーブル 14: クラウドセキュリティプラクティスと実装に関する推奨事項

12.3.2 クラウド脅威インテリジェンスソース

多くの脅威インテリジェンスソースは、クラウドとは関係のない、またはクラウド固有のものではない脅威アクターとセキュリティ侵害の指標に焦点を当てています。クラウドに対する組織の脅威インテリジェンスを強化できる情報源は、次のとおりです。

- CSA *Top Threats*[190] レポートには、公開インシデントで見られるような、最も一般的なアクティブ侵害に対する脅威モデリングが含まれています。このプロジェクトには、重大インシデントの掘り下げも含まれています。これは、実際の情報漏洩の発生状況を把握する上で非常に有用です[191]。
- MITRE ATT&CK®[192]には、攻撃者がエンタープライズクラウドの導入を標的にするために使用する戦術と技法（および副技法）を説明するクラウドマトリックスが含まれています。
- 多くのベンダーが脅威の調査とレポートをリリースしています。これらには、調査チームと対応チームが目にするクラウド攻撃に関する情報が含まれる場合が多くなっています。ただし、これ

[190] CSA. (2022) *Top Threats to Cloud Computing Pandemic Eleven*.

[191] CSA. (2023) *The Common Cloud Miscofigurations That Lead to Cloud Data*.

[192] MITRE (2024) ATT&CK®.

らのレポートは、ベンダーの事業や製品、過去の経験に基づいて選択バイアスを含んでいる可能性があるため、慎重に評価する必要があります。

- オープンソースは独立して運営され、公開された脅威データを収集・共有してします。Breaches.cloud[193]は、既知のパブリックな侵害を追跡し、積極的に維持されている例です。

サマリ

関連の技術や戦略のプリズムを通じて、クラウドセキュリティの課題を分析し始めています。ZT では、リソースを保護するための多要素認証、マイクロセグメンテーション、暗号化などの技法を使用して、すべてのユーザーとデバイスを継続的に検証し、信頼を最小限に抑え、最小特権の原則を適用することで、アタックサーフェスを減らし、セキュリティのレジリエンスを強化します。AI により、脅威の検出、アクセス制御、およびポリシーの適用を通じてクラウドのセキュリティを強化できます。AI は機械学習を活用して、異常の検出とリスク管理を向上させることもできます。TVM では、CSPM や継続的な監視などのツールを使用して、セキュリティの脅威を特定、評価、および軽減できます。TVM は、クラウド環境の保護とコンプライアンスの確保にも役立ちます。TVM に AI を統合することで、脅威の検出と対応戦略が強化され、強固なセキュリティポスチャを維持できます。

推奨事項

効果的なクラウドセキュリティは、常に責任の整理、リスクの特定、およびポリシーコントロールを管理するためのフレームワークを提供する強固なガバナンスモデルの確立から始まります。

ガバナンスとフレームワーク：これには、組織全体の役割と責任を明確に定義し、クラウドの利用に関連する主要なリスクを特定し、セキュリティ管理を一貫して管理するフレームワークを実装することが含まれます。ガバナンス構造は、適切な監督と説明責任を提供しながら、全体的なビジネス目標に沿っている必要があります。

IANS Cloud Security Maturity Model[194]は、セキュリティプログラムをガイドし、サポートできます。

IaaS から SaaS まで、IAM はセキュリティ管理の取り組みに最初に焦点を当てる場所です。

- 組織管理を使用して、組織の影響範囲とクラウドセキュリティポスチャをコントロールします。
- 効果的なモニタリングのための一貫したセキュリティテレメトリ収集を確立します。
- ネットワーク、ワークロード、アプリケーション、およびデータのセキュリティには通常、一連の共有サービスがありますが、セキュリティはさまざまな配備のニーズに合わせてカスタマイズする必要があります。

[193] Public Cloud Security Breaches is a website that tracks security breaches on public clouds.

[194] IANS. (2024) Cloud Security Maturity Model Version 2.0 - *What is the Cloud Security Maturity Model*.

- 組織のクラウドセキュリティコントロール仕様はベースライン要件を定義することになりますが、セキュアな設計とアーキテクチャについては DevOps やクラウドチームと連携する必要があります。
- 継続的アセスメントを使用して、公開露出につながる設定ミスや IAM の脆弱性を特定し、インシデント対応（脅威の検出を含む）を使用して、攻撃や露出を迅速に特定して修正します。

クラウドセキュリティ成熟度モデルは、クラウドセキュリティプログラムの構造化と開発ガイドにも役立ちます。いくつかの推奨事項を以下に示します。

優先事項としての IAM

IAM は、サービスモデル（IaaS、PaaS、SaaS）に関係なく、あらゆるクラウドセキュリティプログラムにとって最優先事項であるべきです。IAM は、誰がどのリソースにアクセスし、どのアクションを実行できるかをコントロールします。IAM の設定ミスや不十分な管理は、不正アクセス、データ侵害、その他のセキュリティインシデントにつながる可能性があります。強固な認証メカニズムの実装、最小特権の原則の適用、アクセス鍵の定期的な見直しとローテーション、および異常なアクティビティのモニタリングに焦点を置きます。

影響範囲のコントロール・監視の組織管理

クラウドプラットフォームが提供する組織管理機能を使用して、影響範囲（セキュリティインシデントの潜在的な影響）をコントロールします。これは、適切なアカウントの構造化、異なる環境（本番、ステージング、開発など）間での別のアカウントの使用、およびネットワークセグメンテーションの実装によって実現できます。一貫したセキュリティテレメトリ収集プロセスを確立して、さまざまなソースからのログとイベントを一元化し、効果的なモニタリングとインシデント対応を可能にします。

さまざまな配備におけるセキュリティのカスタマイズ

組織全体で一連の共有セキュリティサービスが存在する場合もありますが、さまざまな配備の特定のニーズに応じてセキュリティコントロールを調整することが重要です。公開ウエブアプリケーションのネットワークセキュリティ要件は、内部データベースの要件とは異なります。同様に、コンテナワークロードのセキュリティ対策も、サーバーレス機能の場合とは異なります。アプリケーションチームと緊密に連携して、固有のセキュリティ要件を把握し、適切なコントロールを実装します。

DevOps やクラウドチームとの連携

クラウドのセキュリティはサイロで運用すべきではありません。DevOps やクラウドチームと連携し、プロジェクトの設計やアーキテクチャフェーズにセキュリティを組み込みます。チームが参照できるベースラインのセキュリティコントロール仕様を定義しますが、特定のユースケースに基づいて率直に適応できるようにします。セキュリティポスチャの維持に全員が役割を果たす、共有責任の文化を醸成します。

継続的な評価とインシデント対応

継続的な評価プロセスを実施し、リソースの公開や IAM の脆弱性など、セキュリティリスクにつながる設定ミスを事前に特定します。これらの課題を定期的にスキャンして修正します。セキュリティインシデントを迅速に検出、調査、および軽減するための堅牢なインシデント対応計画を策定します。脅威検出ツールを活用し、対応ワークフローを自動化して、潜在的な侵害の影響を最小限に抑えます。

クラウドセキュリティは継続的な監視、評価、および改善を必要とする継続的なプロセスであることを覚えることが重要です。進化する脅威の状況とクラウド環境の変化に対応するために、組織のセキュリティポリシー、手順、およびコントロールを定期的に見直し、更新することをお勧めします。

追加のガイダンス

- Introduction to Generative AI & Prompt Engineering | CSA
- Principles to Practice: Responsible AI in a Dynamic Regulatory Environment | CSA
- AI Resilience: A Revolutionary Benchmarking Model for AI Safety | CSA
- AI Organizational Responsibilities - Core Security Responsibilities | CSA
- Certificate of Competence in Zero Trust (CCZT) | CSA
- DoD Zero Trust Reference Architecture | DoD
- Zero Trust Maturity Model | CISA
- Cybersecurity Framework | NIST
- SP 800-207A, A Zero Trust Architectural Model | NIST
- CIS Critical Security Controls
- ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems requirements