ICSCoE　TLP:WHITE

クラウドセキュリティ

～設定ミスとの付き合い方～

2023 年 7 月

独立行政法人情報処理推進機構

産業サイバーセキュリティセンター

中核人材育成プログラム　6 期生

クラウドセキュリティプロジェクト

まえがき

昨今、クラウドサービスは社会基盤を支える重要な ICT 基盤となっており多くの企業や組織で活用されている。経済産業省より発表された DX レポートにおいても、「2025 年の壁[1]」克服の手段としてクラウドサービスについて言及されており、戦略に沿った効果的な利用の必要性が強調されている。特に導入コストが低く、柔軟な使い方のできるパブリッククラウドが注目を集めており、導入を進めている企業は多い。

一方で、パブリッククラウドにおける重大なインシデントも度々発生しており、その原因の多くは利用者側の「設定ミス」によるものである。設定ミスと聞くとしっかり設定を確認すれば解決すると思うかもしれないが、パブリッククラウドにおける利用者側の設定箇所は多岐に渡り、ミスを完全になくすことならびにミスの発生に気づくことはなかなか難しい。

今回、上記の課題を解決すべく本プロジェクトを立ち上げ、文献調査や技術要素の機能検証を実施した。また、パブリッククラウドを先進的に活用している企業・組織に対してヒアリングを実施し、具体的な取り組みについての調査も行った。

本書では、パブリッククラウドを利用しているまたは今後導入を進めていこうと考えている利用者側の企業において、設定ミスによるインシデントを防ぐために必要な心構えや効果的なアプローチ手段について重要なポイントをまとめた。

最後に、本書で紹介する内容は設定ミスによるセキュリティリスクにフォーカスしたものであり、パブリッククラウドにおけるすべてのリスクを網羅的に記載したものではないことをご留意いただきたい。

---

[1] 経済産業省が DX レポートにおいて提示したキーワード。企業が DX の取り組みを十分に行わなかった場合、2025 年以降に大きな経済損失が発生し、国際競争力を失うという課題を表す言葉

目次

本書の構成

「第1章　はじめに」では、クラウドサービスの概要紹介ならびに、企業や組織における利用実態について記載する。

「第2章　パブリッククラウドにおける設定ミス」では、インシデント事例や設定ミスの悪用シナリオ、設定ミスが引き起こす脅威について記載する。

「第3章　設定ミスによるインシデントを防ぐために」では、設定ミスと付き合っていくための心構えとそのために必要な予防的統制と発見的統制について記載する。

「第4章　統制効率化のための技術的アプローチ」では、企業において２つの統制を効率的に機能させるためのアプローチとして CSPM(Cloud Security Posture Management)といったソリューションや IaC(Infrastructure as Code)といった技術を、ヒアリングや技術検証などから得た知見をもとに記載する。

「第5章　統制効率化のための組織的アプローチ」では、統制効率化のための組織的なアプローチである CCoE（Cloud Center of Excellence）についてヒアリングや文献調査などから得た知見をもとに記載する。

「第6章　まとめ」では、本書のまとめを記載する。

免責事項

- 本書は単に情報として提供され、内容は予告なしに変更される可能性がある。
- 本書に誤りが無いことの保証や、商品性又は特定目的への適合性の黙示的な保証や条件を含め、明示的又は黙示的な保証や条件は一切無いものとする。
- 本書に記載の内容は、独立行政法人情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、作成者の見解に基づいている。
- 本書の利用によるトラブルに対し、本書作成者ならびに監修者は一切の責任を負わないものとする。
- 本書の有効期限は、発行日から２年間とする。

本書で使用する他企業の商標・登録商標について

- Microsoft、Azure、Azure Active Directory は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標である。
- AWS、AWS Identity and Access Management は、米国 Amazon.com,Inc.の米国およびその他の国における商標または登録商標である。

第1章 はじめに

1.1. クラウドサービスとは

クラウドサービス（クラウドコンピューティング）の定義については、NIST（米国国立標準技術研究所）[2]が 2011 年に SP800-145 The NIST Definition of Cloud Computing において提唱しており、IPA（独立行政法人情報処理推進機構）の翻訳によると以下のとおりである。本書においても、この定義に則り記載する。

“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、サーバー、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る。また利用者は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。”[3]

“このクラウドモデルは 5 つの基本的な特徴(オンデマンド・セルフサービス、幅広いネットワークアクセス、リソースの共用、スピーディな拡張性、サービスが計測可能であること)がある。また、3 つのサービスモデル(SaaS、PaaS、IaaS)、および 4 つの実装モデル(プライベートクラウド、コミュニティクラウド、パブリッククラウド、ハイブリットクラウド)によって構成される。”[3]

1.2. 責任共有モデル

クラウドサービスの活用にあたっては「責任共有モデル」について確実に理解しておく必要がある。責任共有モデルとは、クラウドサービスの利用者とクラウド事業者が、責任分界点を定めるだけでなく、運用責任を共有し合うという考えのことである。図 1.1 に責任共有モデルの基本的な考え方の例を示す。ハードウェアや仮想化ソフトウェアなどの基盤となる環境を整備しているサービスが IaaS（Infrastructure as a Service)、そして OS やアプリケーションを制御、支援するミドルウェアまでの環境を整備しているサービスが PaaS（Platform as a Service)、さらにアプリケーションまでの環境を整備しているサービスが SaaS（Software as a Service）と分類される。利用者はクラウド事業者が提供しているクラウドサービスがどの分類に当てはまる（または折衷的に提供している）サービスなのかを理解した上でクラウドサービスを活用し、利用者の責任範囲を明確にする必要がある。

---

[2] National Institute of Standards and Technology：米国立標準技術研究所 米国商務省配下の科学技術分野における計測と標準に関わる研究所。

[3] NIST,” The NIST Definition of Cloud Computing”,2011.

また、昨今ではさらに細分化された考え方もあり、例えばさまざまな環境で利用可能なアプリケーションの開発ができる CaaS(Container as a Service)や、サーバーレス[4]でアプリケーション開発ができる FaaS（Function as a Service）等の形態が存在し、それらを組み合わせてシステム構築がされるようになり、より複雑化している。

図 1.1 クラウドサービスの責任共有モデル
（出典：内閣官房内閣サイバーセキュリティセンター、クラウドを利用したシステム運用に関するガイダンス（詳細版））

1.3. クラウドサービス利用形態

クラウドサービスは、クラウド環境を利用者の要件に合わせて構築するものか、クラウド事業者が提供するものかでプライベートクラウド、パブリッククラウドに分類される。以下にそれぞれの特徴を示す。なお、比較のためオンプレミスも合わせて取り上げる。

オンプレミス

- 利用者の要件に合わせてサーバー機器やソフトウェアを調達してシステムを構築する形態
- 利用者が所有するデータセンターに構築する形態、クラウド事業者が提供するデータセンターに構築する形態（ハウジング）、サービス事業者が提供するデータセン

[4] 自社でのサーバー構築・管理などを必要とせず、サーバーレス提供会社の基盤を用いプログラムを実行できる仕組み

ターとハードウェアを利用して構築する形態（ホスティング）がある

プライベートクラウド

- 利用者の要件に合わせてサーバー機器やソフトウェアを調達あるいはサービス事業者と契約して構築するクラウドサービスの形態
- 利用者がクラウド環境を構築するオンプレ型と、サービス事業者が所有するクラウド環境を利用者の要件に合わせて長期契約で利用するホスティング型がある

パブリッククラウド

- サービス事業者がサービスメニューに基づき提供するクラウドサービスの形態
- サービス事業者が提供する範囲により主に IaaS、PaaS、SaaS の 3 つに分類される

図 1.2 クラウドサービス利用形態の比較

（参考：経済産業省、令和 3 年度 重要技術管理体制強化事業（クラウドを活用した重要情報管理体制強化に向けた調査事業）調査報告書）

それぞれの特徴として、オンプレミスとプライベートクラウドは、利用者の業務要件に合わせたシステム・インフラ環境を構築することができるが、拡張性が低く、初期コストや運用コストが高価になるケースが多い。一方でパブリッククラウドは、拡張性が高く、初期コストや運用コストを比較的安価に抑えることができる反面、サービス事業者への依

存度が高く、カスタマイズ性も低い。また、障害発生時に即時対応や個別対応が難しいといった特徴があるが、市場の拡大は顕著となっている。パブリッククラウドの市場動向については総務省による令和 4 年情報通信に関する現状報告においてまとめられており、PaaS 市場が特に成長し、新型コロナウイルス感染症の感染拡大の影響を受けた企業活動で重要な役割を果たしたと考えられる。また、予測によると IaaS から SaaS まで、パブリッククラウド市場は今後も伸びていくと考えられる。以降、本書においてはこのパブリッククラウドについて着目する。

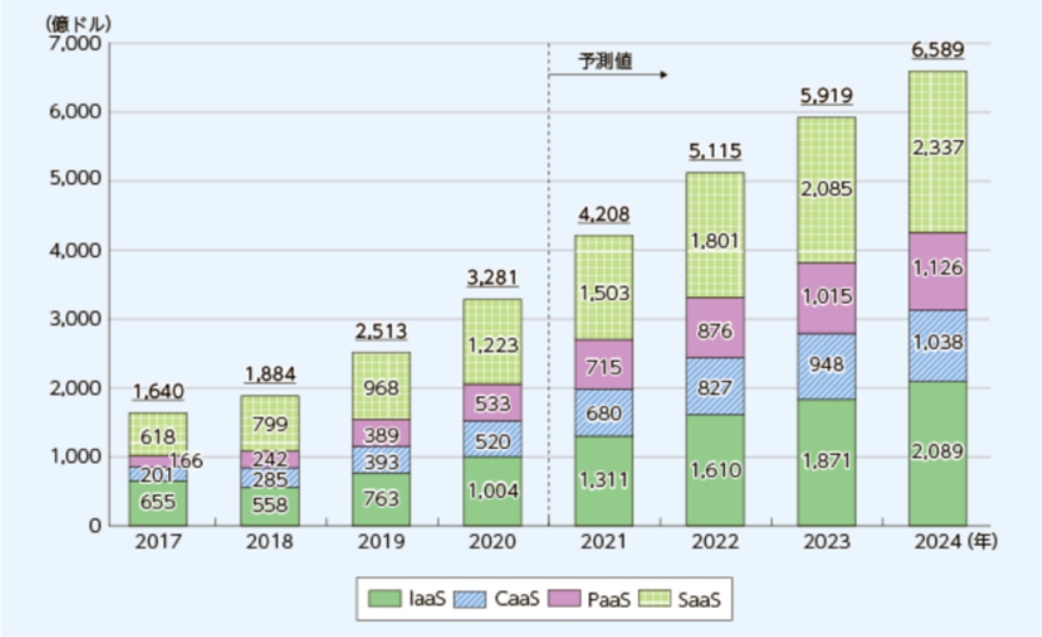

図 1.3 世界のパブリッククラウドサービス市場規模（売上高）の推移及び予測
（出典：総務省、令和 4 年情報通信に関する現状報告
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nd236800.html）

1.4. パブリッククラウドのメリットおよびデメリット

パブリッククラウドは導入や構築が素早く行え、拡張性が高いなどといった利点から多くの企業で活用されている。一方で、外部の資源を活用しているため、組織のリスク管理そのものに影響し、自組織だけでは完結し難い状況になるといった課題も挙げられる。クラウドサービスであってもシステムを運用し続けている意識を持つことが大切であり、むしろクラウド事業者のタイミングで仕様や約款などの変更が行われるため、新たな仕様の確認や、設定の再確認等、運用にはそれ相応のコストがかかることは気をつけておかなければならない。

表 1.1 パブリッククラウドのメリットおよびデメリット

（参考：経済産業省、令和 3 年度 重要技術管理体制強化事業（クラウドを活用した重要情報管理体制強化に向けた調査事業）調査報告書）

	メリット	デメリット
サーバーの共有範囲	-	• 共有範囲において、他の利用者の高負荷な利用により、遅延等の大きな影響がでる可能性がある
可用性	• 機器の障害時はクラウド事業者が用意するフェールオーバー[5]や切り戻しの機能を利用できる • 複数データセンターにサービスが分散され、大規模災害発生時も事業継続が可能	• クラウド事業者の責任範囲について、事業者の SLA に従うため、可用性要件をクラウドサービスにあわせる必要がある
機密性 完全性	• クラウド事業者の責任範囲は事業者の高度なセキュリティ対策が実施される • クラウド事業者の用意するセキュリティ機能を利用できる	• インターネット経由で接続できる場合、常にサイバー攻撃の脅威に晒される • データ保管場所の管理情報が不透明
初期コスト 運用コスト	• 多くの場合は初期投資が不要 • 従量課金により適正なコストで利用が可能	• 月額費用が変動するため予算を立てにくい
拡張性 柔軟性 カスタマイズ性	• 急激なサービス需要変化や業務見直しに伴うリソースの追加や変更が容易	• カスタマイズや自社システムとの連携には一定の制限がある • 提供サービスの増加に伴い適切なサービス選択が難しくなる • クラウド事業者の個別機能の利用が進むとベンダーロックインのリスクがある
先進技術の活用	• 技術革新による新しい機能が随時追加され、先端技術の活用が容易	• クラウド事業者の独自性が高く、他社サービスとの互換性が低い
保守	-	• クラウド事業者の復旧対応について利用者側で状況把握や個別対応は困難 • システムメンテナンス等の計画停止の実施時期等、個別の事前調整が難しい

[5] システムやサービスが予期せず停止した場合に、別の冗長なシステムやバックアップシステムに自動的に切り替わること

1.5. パブリッククラウド実装トレンド

前節の表 1.1 にあるパブリッククラウドのデメリットを解消するクラウドサービスや技術として、ハイブリッドクラウドやマルチクラウドなどが注目されている。以下にその特徴を示す。

ハイブリッドクラウド

パブリッククラウドとプライベートクラウドあるいはオンプレミスを組み合わせたクラウド利用形態

マルチクラウド

複数のパブリッククラウドプロバイダーが提供するクラウドサービスを意図的に使用するクラウド利用形態

表 1.2 パブリッククラウドの課題に対して効果的な実装トレンド
（参考：経済産業省、令和 3 年度 重要技術管理体制強化事業（クラウドを活用した重要情報管理体制強化に向けた調査事業）調査報告書）

○：課題解決に効果的

	パブリッククラウドの主な課題	ハイブリッドクラウド	マルチクラウド
サーバーの共有範囲	共有範囲において、他の利用者の高負荷な利用により、遅延等の大きな影響がでる可能性がある	○	
可用性	サービス事業者の SLA[6]に従う	○	○
機密性 完全性	データ保管場所の管理情報が不透明	○	
拡張性 柔軟性 カスタマイズ性	カスタマイズや自社システムとの連携には一定の制限がある	○	○
先進技術の活用	サービス事業者の個別機能の利用が進むとベンダーロックイン[7]のリスクがある		○

[6] Service Level Agreement：サービス提供者と利用者との間で結ばれるサービスのレベル（定義、範囲、内容　等）に関する合意

[7] 特定企業の製品・サービスに依存しており、他社の製品・サービスへの切り替えが困難になっている状況

これらのハイブリッドクラウドやマルチクラウドは課題に対するメリットもあれば複雑さ、コスト面でのデメリットもある。個社の企業戦略およびビジネスモデルに合わせたモデルの使い分けをよく検討することが大切である。

第2章 パブリッククラウドにおける設定ミス

2.1. 設定ミスというセキュリティ脅威

「1.2 責任共有モデル」に示すように、IaaS ではオペレーティングシステム、PaaS ではアプリケーションより上位レイヤーならびにその設定管理は利用者に責任がある。そして、クラウドサービスにおけるセキュリティインシデントの原因は単なる設定ミスであることがほとんどである。Cloud Security Alliance（CSA）[8]により 2022 年に公開されている Top Threats to Cloud Computing – Pandemic Eleven によると、クラウド事業者起因の脅威ランキングは下がり続け、ユーザー起因のものが増えてきており、ユーザーのオペレーションが弱点（管理不備や設定ミス、戻し忘れなど）であるとされる。列挙されている 11 の脅威のうち「設定ミスと不適切な変更管理」は 3 位に位置づけられている。さらに、他の脅威においても設定ミスが関係しているものがいくつかあり、設定ミスが深刻な脅威として捉えられていることが分かる。

表 2.1 クラウドセキュリティ 11 大脅威
（出典：CSA、Top Threats to Cloud Computing – Pandemic Eleven（訳：CSA ジャパン、クラウドコンピューティングの重大脅威　パンデミックイレブン）

ランク	脅威名
1	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、ならびに特権アカウント
2	セキュアでないインターフェースや API
3	設定ミスと不適切な変更管理
4	クラウドセキュリティのアーキテクチャと戦略の欠如
5	セキュアでないソフトウェア開発
6	セキュアではないサードパーティーのリソース
7	システムの脆弱性
8	予想外のクラウドデータ公開
9	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
10	組織的な犯罪、ハッカーと APT
11	クラウドストレージデータ流出

[8] Cloud Security Alliance：クラウドコンピューティングのセキュリティに関するグローバルな非営利団体

また、ガートナー社が 2019 年に公開した「Is the Cloud Secure?」の記事ではクラウドセキュリティの今後の課題について以下のように述べられている。

「2025 年には、パブリッククラウドの使用を制御できない組織の 90%が機密データを不適切に共有してしまう」[9]

「2025 年までに、クラウドセキュリティ障害の 99%が利用者の責任となる」[9]

これまでも設定ミスによるセキュリティインシデントは数多く発生しているが、今後もその傾向は変わらず、むしろリスクは増加していくことが予測されている。

2.2. 設定ミスによるインシデント事例

設定ミスを原因とするインシデントは国内外で数多く発生している。ここでは、パブリッククラウドにおける代表的なインシデント事例を表 2.2 にまとめた。公開されている情報の範囲では、機密情報や個人情報の漏えいといった事例が多く、原因としては機密情報を保持したストレージの公開設定によるものが多い印象を受ける。

[9] ガートナージャパン株式会社,"Is the Cloud Secure?",2019-10-10,https://www.gartner.com/smarterwithgartner/is-the-cloud-secure, (参照 2023-06-08)

表 2.2 設定ミスによるインシデント事例

#	企業	事例	原因	出典
1	Capital One	1 億件を超える個人情報の漏えい	WAF の設定ミスに起因し、システムのアクセス権限が奪取されたため	https://japan.zdnet.com/article/35189167/
2	UpGuard	1 億 2 千万件以上の世帯情報の漏えい	データへのアクセス権の過剰付与	https://news.yahoo.co.jp/byline/ohmototakashi/20171221-00079554
3	Advantage Capital Funding / Argus Capital Funding	50 万件を超える非常に機密性の高い非公開の法律文書や財務文書	ストレージを公開設定としていたため	https://www.vpnmentor.com/blog/report-mca-wizard-leak/#How-and-Why-We-Discovered-the-Breach
4	株式会社 JTB	1 万件を超える顧客情報の漏えい	データへのアクセス権の過剰付与	https://www.dataclasys.com/column/jtb_20221026/
5	Honda Cars India	5 万件を超える顧客情報の漏えい	ストレージを公開設定としていたため	https://www.bleepingcomputer.com/news/security/honda-india-left-details-of-50-000-customers-exposed-on-an-aws-s3-server/
6	GoDaddy	2 万 4 千のシステム機密設定情報や価格交渉情報	ストレージを公開設定としていたため	https://japan.zdnet.com/article/35123924/
7	アメリカ連邦政府	75 万件を超える出生証明書の漏えい	ストレージを公開設定としていたため	https://techcrunch.com/2019/12/09/birth-certificate-applications-exposed/
8	ケアプロ株式会社	622 件の顧客情報の漏えい	委託先企業がバックアップ先のストレージを公開設定としていたため	https://carepro.co.jp/about/yobou_news_20200604.pdf
9	Tesla	仮想通貨のマイニングに計算資源を不正利用	システムの管理コンソールが保護されていなかったため	https://japan.cnet.com/article/35114995/

2.3. 設定ミスと悪用シナリオ

運良くインシデントにはつながっていない設定ミスでも、インシデントにつながってもおかしくないヒヤリハットが数多くある。以下に、ついやってしまいがちな設定ミス事例を文献調査やクラウド利用者に対して行ったヒアリングを通じて収集し、プロジェクトメンバーでカテゴリごとにまとめた (表 2.3)。なお、一部に権限の管理ミスや設定者の想定ミスについても記載している点はご了承いただきたい。

表 2.3 発生しやすい設定ミス

カテゴリ	設定ミス概要	想定されるリスク
ID とアクセス管理	退職者の認証情報を失効させずに放置してしまう	ユーザー情報が悪用される
	API のアクセスキーやシークレットアクセスキーなどをパブリックのリポジトリに誤って登録してしまう	アクセスキーやシークレットアクセスキーが漏えいし不正アクセスに利用される
	ゲストの利用者に対して誤って強力な権限を付与してしまっていた	ゲスト（第 3 者）に機密データアクセスを許し、持ち出される
ロギング	ロギングの設定ができていない	インシデント発生時に影響範囲の特定ができない
	想定していたよりもログ容量が大きくなってしまう	想定以上に多額の料金を請求される
オブジェクトストレージ・データベース	適切なライフサイクル設定ができていない	保存しているデータを喪失してしまう
	暗号化の設定ができていない	情報漏えい時にデータの内容を保護できない
	誤ってストレージが公開設定となっており、第三者に閲覧可能な状況となっていた	インターネットからデータにアクセスされ、情報漏えいする
	サービス停止と共に主なリソースは削除したが、ストレージが公開設定のまま残っていた	インターネットからデータにアクセスされ、情報漏えいする
仮想サーバー	運用中の仮想サーバーを誤って削除してしまう	稼働中のサービスが意図せず停止する
	不要な仮想サーバーを誤って起動する、起動したままにする	脆弱性の放置された仮想サーバーが攻撃の踏み台に悪用される
ネットワーク	仮想サーバーに接続できず、トラブルシューティングのために任意の IP アドレスからの SSH 接続[10]を許可したが、元に戻すことを忘れてしまう	SSH ポートから不正アクセスを受ける
	一時的なメンテナンスのために RDP 接続を許可したが、元に戻すことを忘れてしまう	RDP ポートから不正アクセスを受ける
	DNS[11]設定手順を誤ってしまう	ドメイン名ハイジャックを受ける

[10] Secure Shell 接続：ネットワークを介して安全にリモートコンピュータにアクセスする仕組み
[11] Domain Name System：インターネット上でドメイン名を管理・運用するために開発されたシステム

これらの設定ミスが複合的に重なることで、インシデントの発生および対応の遅れにつながる。以下に、攻撃者のアタックパス[12]に設定ミスがどのように影響するか簡単に紹介する。

例１：クラウドサーバーへの不正アクセスによる情報漏えい

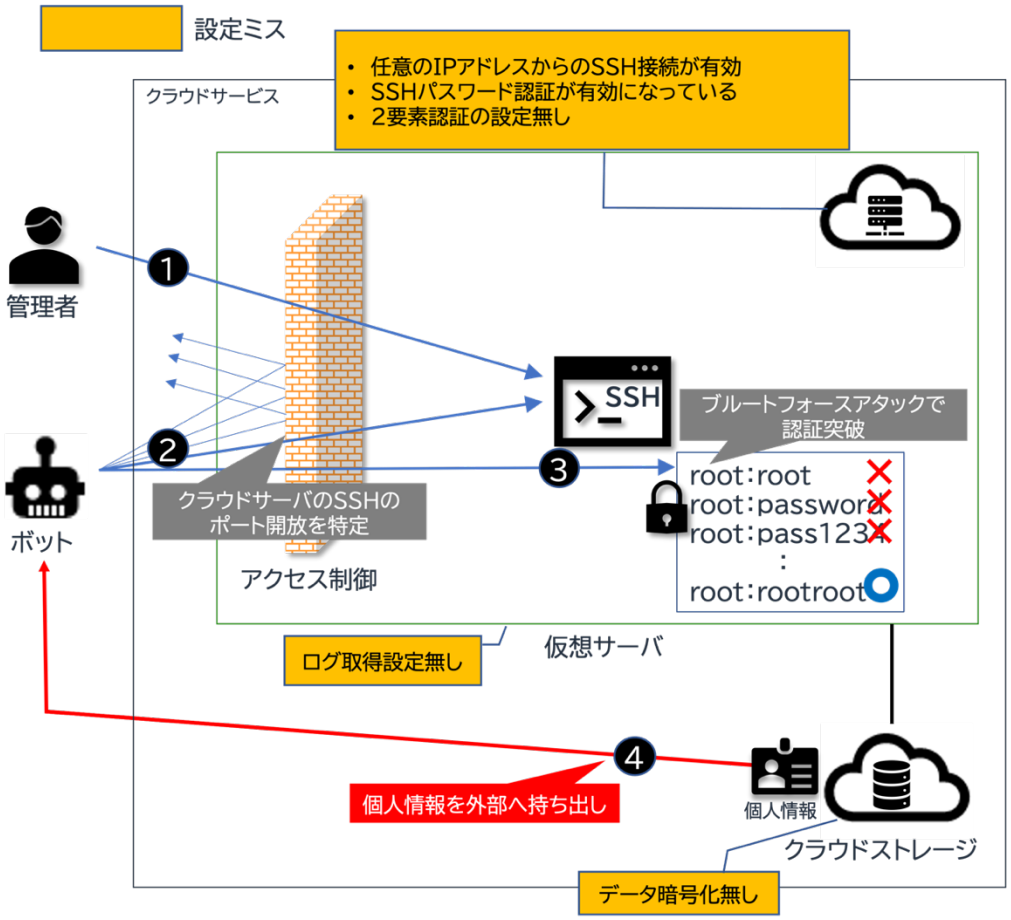

図 2.1 クラウドサーバーへの不正アクセスによる情報漏えい

① 管理者がクラウド上の仮想サーバーに接続できず、トラブルシューティングのために任意の IP アドレス（0.0.0.0/0）からの SSH 接続を許可した。しかし、アクセス制御を元に戻すことを忘れてしまった。

② 攻撃者のボットにサーバーを特定され、ポートスキャン[13]により SSH が開放されていることが晒される。

---

[12] コンピュータシステムやネットワークにおいて、攻撃者が潜在的に侵入し、目標にアクセスするための経路や手順

[13] ネットワーク上のコンピュータやサーバーに対して、利用可能なネットワークポートを探索するための活動

③　SSH に対するブルートフォースアタック[14]により、攻撃者に仮想サーバーの管理者アカウントの認証を突破される。
④　仮想サーバーからアクセス可能なクラウドストレージ上の個人情報データを参照され、外部へ持ち出しされる。

管理者がクラウド上の仮想サーバーの SSH 接続許可をトラブルシューティング後に元に戻し忘れ、攻撃者に悪用されてしまったケースである。仮想サーバーへの接続認証を強力にしていれば攻撃は困難になったはずだが、組織のポリシーとして禁止している SSH 接続をパスワード認証で運用していることや管理者の 2 要素認証[15]が設定されていないといった不備があり、攻撃を容易にさせてしまっている。

例 2：ユーザー認証情報の管理不備による情報漏えい

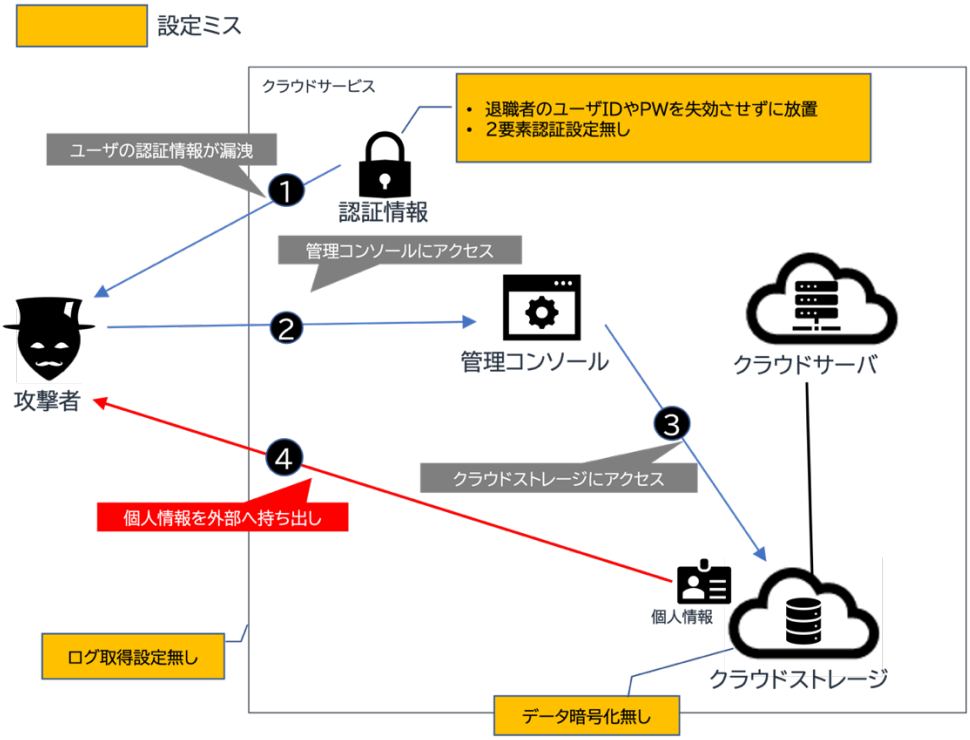

図 2.2 ユーザー認証情報の管理不備による情報漏えい

①　退職者の管理コンソールへの認証情報（ID、パスワード）が攻撃者に漏えいする。
②　攻撃者に退職者の認証情報で管理コンソールにアクセスされ、クラウドストレージの

[14] 暗号や認証メカニズムに対する攻撃手法の一つ。全ての可能性を網羅的に試行し、正しいパスワードや鍵を見つけ出す攻撃手法
[15] アカウントのセキュリティを強化するための認証手法。2 つの要素を用いてユーザーを認証する仕組み

データを参照される。

③　クラウドストレージにアクセスされる。

④　個人情報を外部に持ち出しされる。

退職者のユーザー情報や認証情報が適切に管理・棚卸されず放置され、何らかの理由で管理コンソールへの認証情報を攻撃者に悪用されてしまうケースである。管理コンソールへのアクセスを許してしまうと、当該ユーザーの権限が強い場合は、ストレージへのアクセスキーを発行され、個人情報にアクセスされてしまう。

紹介した２つの例の様に適切なアクセス制御設定やユーザー認証情報の設定・管理はインシデントを防ぐために必須といえるが、データの暗号化やログ取得の設定も重要である。データの暗号化設定に不備があると、データ漏えい時に個人情報を守ることができない。また、ログ取得設定が出来ていないと影響範囲の特定ができない。このように、被害を受けた後の影響最小化や対応に必要な設定についても留意することがポイントとなる。

第3章 設定ミスによるインシデントを防ぐために

3.1. 必要な心構え

設定ミスという脅威からクラウドサービスで構築したシステムおよび重要な情報を守るためにはどうすればよいのか。設定ミスは人間の様々な原因・理由により発生し、人間は完璧ではなくミスをしてしまうため、発生そのものを防ぐことは難しい。

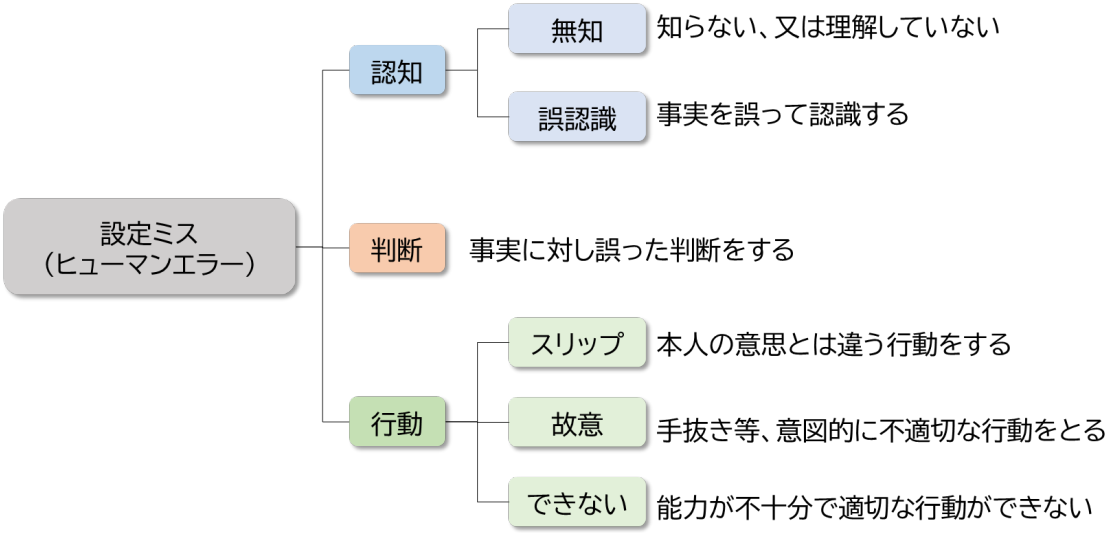

図 3.1 設定ミスの主な原因
(参考：株式会社アイリンク、人間の行動から見たヒューマンエラーの分類、https://www.humanerror.jp/composition/classification.html)

人間のミスを確率的な事象として受け入れ、リスクアセスメントに組み入れるという考えもあるように、設定ミス自体の発生を完全に防ぐというのではなく、設定ミスは発生するものとして許容し、インシデントに繋がらないように是正していくという心構えが大事である。

3.2. ゲートキーパー型セキュリティとガードレール型セキュリティ

ここで、クラウドにおけるセキュリティの考え方として、ゲートキーパー型セキュリティとガードレール型セキュリティについて紹介する。

ゲートキーパー型セキュリティ

設定変更を毎回個別にレビューし、セキュリティに問題がないか設計や運用を評価する

方式。品質の維持管理が非効率的になることや、セキュリティ制限を意識することにより事業部門が事業に注力できないといったデメリットがある。

ガードレール型セキュリティ

セキュリティ要件を明確にし、逸脱が起きないように制御し、逸脱があれば発見できるような仕組みをサービス全体に取り入れる方式。品質の維持管理が効率的で、事業部門は過度にセキュリティを意識せず、事業に注力することができる。

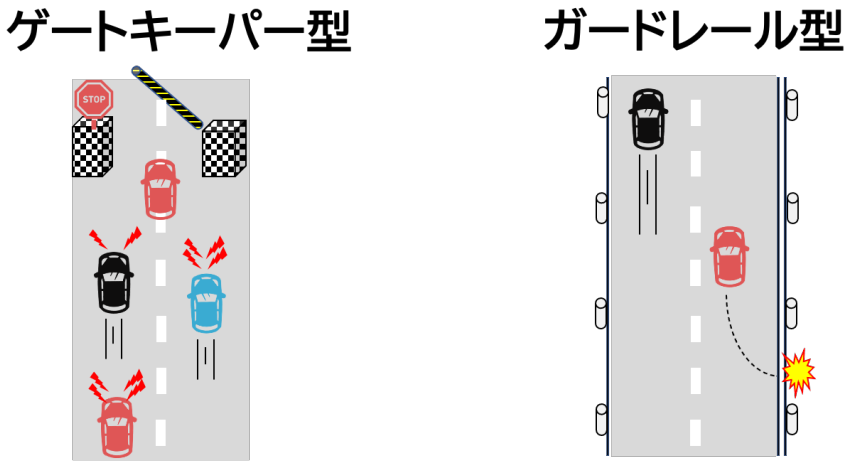

図 3.2 ゲートキーパー型セキュリティとガードレール型セキュリティ

クラウドを利用するメリットの 1 つに、第 1 章でも取り上げたような導入や構築をスピーディに行うことによるビジネスメリットがある。しかし、関所のように一時的に止めて内容を確認し、ルールを守っているか確認するゲートキーパー型だとクラウドのメリットである開発のスピードは落ちてしまう。ガードレール型にすることで、開発の流れを止めずスピードを維持しつつ、セキュリティ要件を担保していくことができる。ここではクラウド開発のスピードについて述べたが、設定ミスについてもこの考えは当てはまる。設定ミスは発生するものであり、発生自体は防ぐことが難しいという前提のもと、ガードレール（ルール）を設けておき、ルールを逸脱するような設定ミスが発生した場合には即座に是正するといった考えが必要である。

3.3. ガードレール型セキュリティに必要な 2 つの統制

ガードレール型セキュリティによって設定ミスによるクラウドインシデントを防ぐことが大事であると述べたが、その上で必要となってくる予防的統制と発見的統制について紹介する。2022 年にデジタル庁により公表された政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針では以下のように述べられている。

「予防的統制とは不正な操作を事前に防止することであり、発見的統制とはリソースが不正な状況になっていないかを継続的に監視し修正する機能である」[16]

「予防的統制では、組織で定めたポリシー（国外サービスの利用禁止、必要なログの取得、高権限アカウントの管理等）を設定しシステムに実装する。発見的統制では、前述のポリシーの準拠状況、暗号化や監視の実施状況、外部公開設定等を定期的に監視し必要に応じて修正する。」[16]

クラウド利活用を進める企業においては、この 2 つの統制を組織内でうまく機能させることがとても重要である。

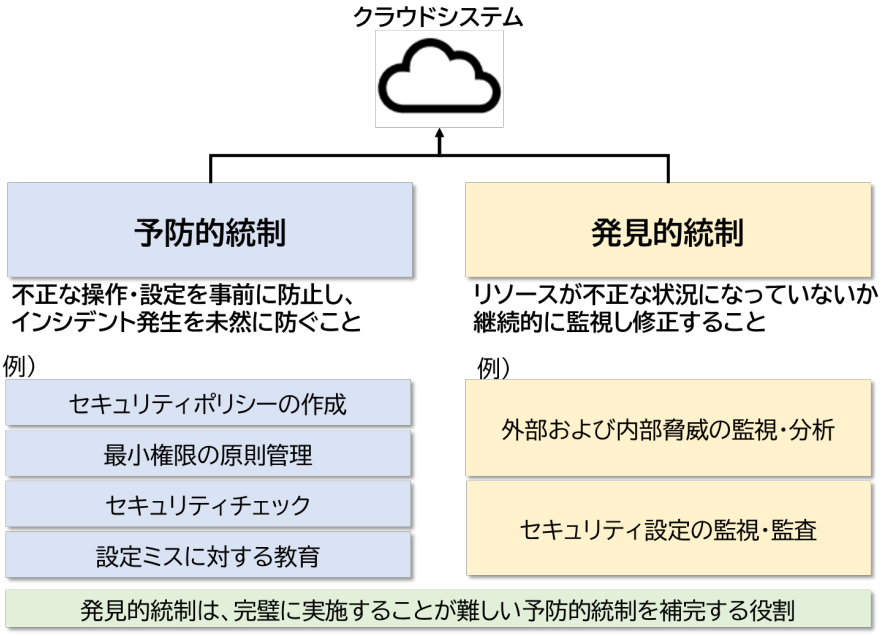

図 3.3 予防的統制と発見的統制

3.4. 予防的統制

予防的統制とは前述した通り、不正な操作・設定を事前に防ぐことである。ここではクラウドを活用していく企業が予防的統制として具体的にどのようなことを行っていけば良いのかについて紹介する。

3.4.1. セキュリティポリシーの作成

予防的統制として、まず必要なのがセキュリティポリシー、つまりルールを作成することである。法や規制、セキュリティのベストプラクティスを理解し、運用ルールを規定することで、大規模な組織においてトラブル回避やセキュリティリスク低減につなげること

[16] デジタル庁,「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」,2022.

が可能となる。セキュリティポリシーは単一の文書を指すこともあれば、組織のセキュリティ文書全体を指す場合もあるが、「基本方針」、「対策基準」、「実施手順」の構成をとることが多い。

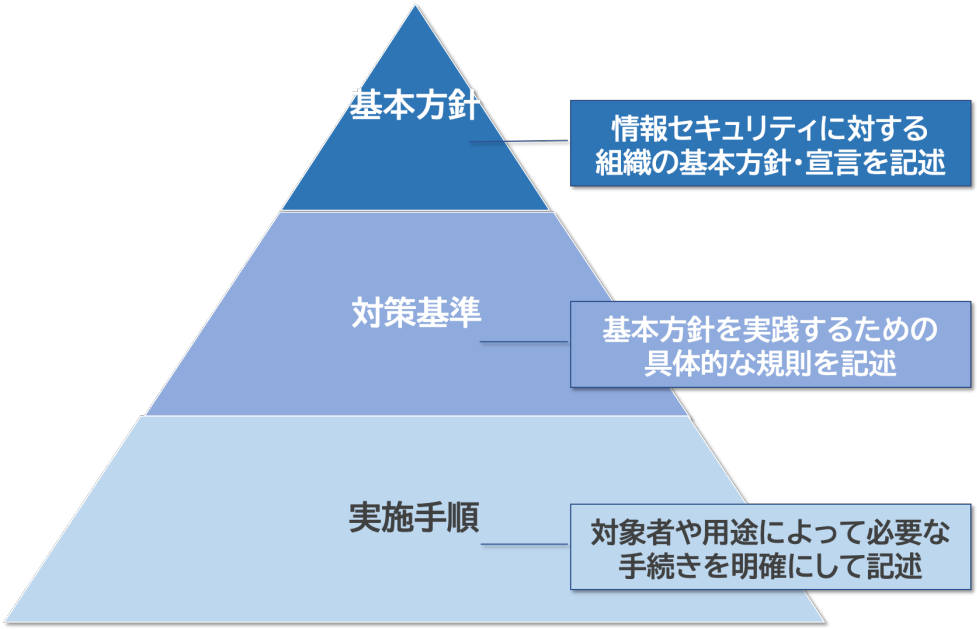

図 3.4 情報セキュリティポリシーの構成

一般的な情報セキュリティのポリシーは既に整備されている組織は多いが、クラウドサービス利用も考慮したセキュリティポリシーに更新する必要がある。更新する内容としては、クラウドサービスのアカウント管理やアクセス制御、暗号化やログ取得などの各種設定、そしてシステムの変更があった際の管理方法など、責任共有モデルにおける利用者の責任範囲を盛り込んでおくことが必要となる。

クラウドサービス利用も考慮したセキュリティポリシーの作成・更新にあたって注意しなければならないのは、オンプレミスとクラウドサービスの仕組みの違いを踏まえた内容にすることである。例えば、オンプレミスでは権限管理は OS やアプリケーションで実装されてきた。クラウドサービスでも変わらない部分はあるものの、クラウドサービスの操作権限に関する制御や、クラウド事業者が提供する権限管理サービス（AWS の AWS Identity and Access Management や Azure の Azure Active Directory など）の活用を考慮する必要がある。通信のアクセス制御においてもクラウド事業者固有のゾーニングやファイアウォールなどの利用を考慮しなければならない。

また、各クラウド事業者において提供するサービスの特徴はそれぞれ異なるため、ポリシーに則ったシステム構成を推奨デザインパターンとして作成しておくことが効果的である。これにより、クラウドシステムを構築していく事業部門はポリシーに準じたセキュアな設定パターンとして参照することが可能となる。

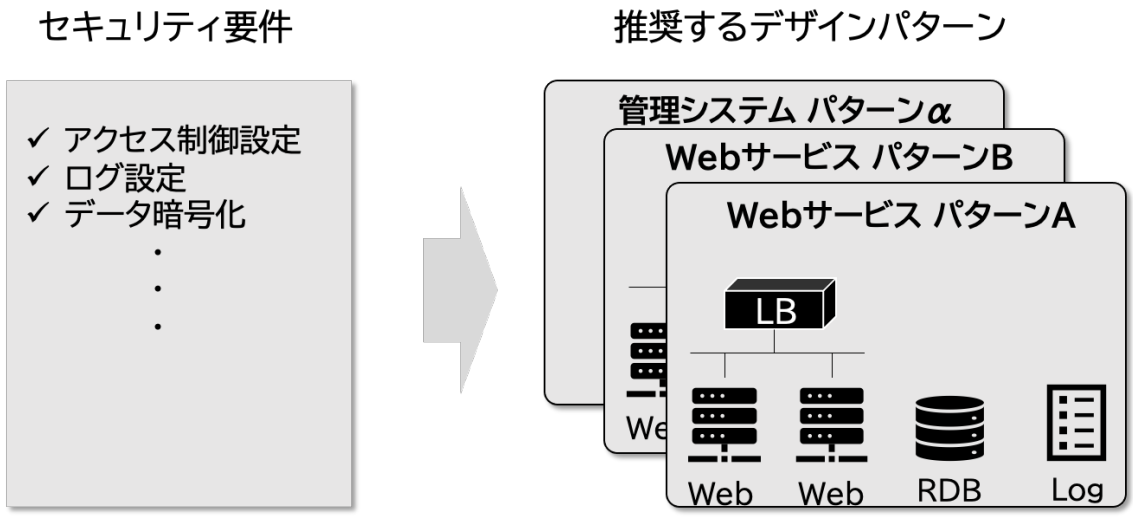

図 3.5 推奨デザインパターン

3.4.2. 最小権限の原則

不備のある設定の発生を少しでも抑制するために重要な、アクセス権限管理について説明する。アクセス権の運用においては、そのユーザーが必要とされる最小限の権限を与える必要があり、これを最小権限の原則という。前項でも述べたとおり、アクセス権限管理はクラウド事業者ごとにサービスが提供されており、それぞれで仕様が異なる。一般的にはオンプレミスの権限よりも粒度が細かいことが多く、権限設定が難しいことが多い。したがって、クラウド事業者ごとに異なる細かい粒度の権限を理解し、使いこなさなくてはならない。

最小権限の原則は、ユーザー業務の環境や内容に応じてその実装方法を変えていくことも大事である。例としてシステム環境を挙げる。重要な保護すべきデータがないように構成されている開発環境において細かな権限付与を行いすぎると、開発作業のスピードを落としてしまう可能性がある。そのため、ログ取得などといったセキュリティ機構を変更されない程度の権限にすることで十分である、と考えることができる。一方本番環境においては、定型業務と非定型業務で使い分けが必要である。定型業務の場合、作業内容が明確であるため、その内容に即した比較的詳細な制御を行う。非定型業務の場合、作業内容が不明確なトラブルシューティングなどであるため、ある程度柔軟な作業ができるよう、開発環境と同様にセキュリティ機構を変更されない程度の権限制御を行う。このように、最小権限の原則はあくまでも原則であり、運用性や組織のリスク受容の水準に応じて緩和することも考えられる。

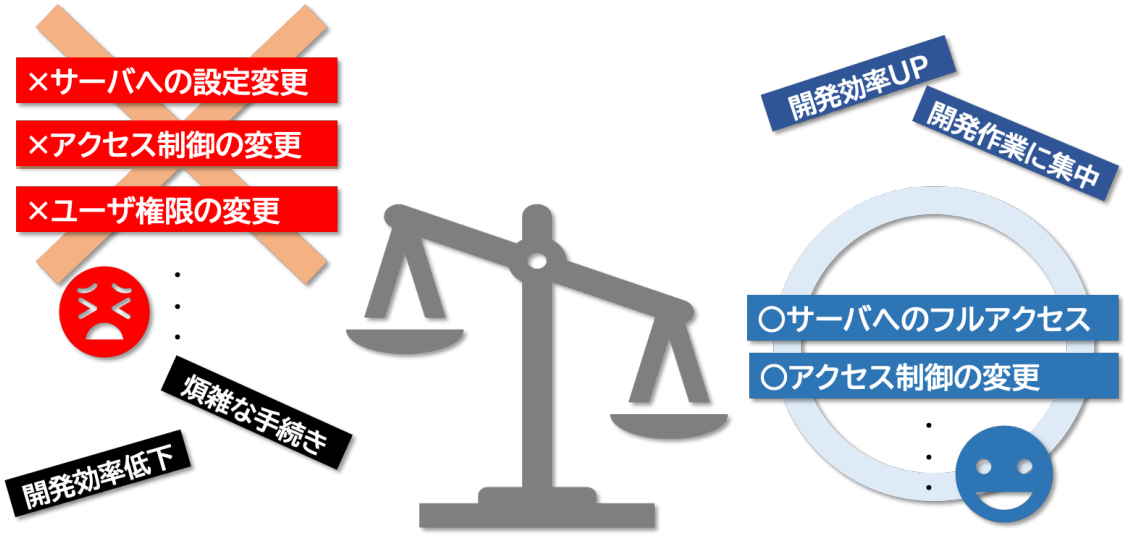

図 3.6 開発環境における最小権限の原則

このように最小権限の原則を適用し、権限のないユーザーや知識の浅いユーザーが誤ってリソースの設定を変えてしまうことを未然に防ぐことが重要である。

3.4.3. システムリリース前のセキュリティチェック

システムリリース前のセキュリティチェックを行うことも重要である。ペネトレーションテスト[17]やクラウド設定診断などにより、ポリシーに準拠した設定になっているか事前チェックを実施することが望ましい。ヒアリングなどで机上チェックすることもコストはかからず経済的ではあるが、設定確認箇所が多い場合、煩雑になってしまうといったデメリットがある。

3.4.4. 設定ミスに対する教育

設定ミスの予防には教育も必須である。前章で述べたような設定ミスによるインシデント事例や悪用シナリオなどをクラウドサービス開発者や運用者に対して教育することで、設定ミスに対する注意意識が高まり、予防につながる。また、クラウド事業者が提供している教育コンテンツを利用することや、クラウド事業者の資格取得を奨励することでクラウドサービスの設定内容について理解を深めることも重要である。

---

[17] 対象システムに外部からの侵入を試みることによって脆弱性を発見するセキュリティテスト手法

3.5. 発見的統制

発見的統制とは、リソースが不正な状況になっていないか継続的に監視し修正することである。設定ミスをヒヤリハットで食い止め、インシデントにつなげないために脅威の監視・分析を行うことも重要なポイントとなる。

3.5.1. 外部および内部脅威の監視・分析

クラウドサービスをはじめ情報セキュリティにおける脅威は、外部脅威（不正アクセス、Web サイト改ざん、脆弱性攻撃など）と内部脅威（組織内の個人が意図的または偶発的にもたらす脅威）に分けられる。それらに対し、攻撃および不正行為の予兆および実行中の攻撃・行為をリアルタイムに発見し検知する監視業務や、ログ等を対象に不審な攻撃・行為の洗い出しと影響範囲の確認を行う分析業務などが必要となる。これらの監視と分析の仕組みを整えておくことで、設定ミスが発生してもそれらを悪用する攻撃をいち早く検出し未然に防ぐことができ、設定ミスを「ヒヤリハット」として抑えることができる。この脅威の監視・分析にはオンプレミスにおいては IDS（Intrusion Detection System）[18]や IPS（Intrusion Prevention System）[19]、WAF(Web Application Firewall)[20]が監視ツールとして、SIEM（Security Information and Event Management）[21]が分析ツールとして活用されることが一般的である。クラウドサービスにおいては、これらのツールはクラウド事業者がセキュリティサービスとして提供していることが多いため、それらサービスの理解と効果的な使い方についてきちんと把握しておくことが必要である。

3.5.2. セキュリティ設定の監視・監査

設定の監視・監査では、対象となるクラウドサービスの設定があらかじめ作成したポリシーを満たしているかのチェックを行う。このとき重要になるのは、リソースの設定が問題ないことを確認することはもちろんであるが、前節で述べたセキュリティサービスが十分に機能していることの確認も重要である。セキュリティサービスが機能する設定になっていないと、脅威の監視や分析が十分にできない。また、3.4.2 で述べたアクセス制御につ

---

[18] Intrusion Detection System：侵入検知システムと呼ばれ、不正や異常な通信を検知し管理者に通知するソリューション

[19] Intrusion Prevention System：侵入防御システムと呼ばれ、不正や異常な通信を検知し防御・遮断を実施するソリューション。 IPS は不正通信検知後、通信遮断を実施するところが IDS と異なる

[20] Web Application Firewall：主にアプリケーション層の通信の不正や異常を検知・防御するソリューション。製品により IDS・IPS がカバーする範囲が重複している場合もある

[21] Security Information and Event Management ：IT（OT）機器のログを一元的に収集・管理・解析し、ネットワークの監視やサイバー攻撃やマルウェア感染などのインシデントにつながる脅威を検知する仕組み

いても監査が必要である。開発環境において作業効率を優先するために権限管理を緩くする場合には、作業がルールの範囲内で行われているかを検知し、検証することが大事である。

3.5.3. 統制を機能させるための課題とアプローチ

ここまでクラウドサービスの設定ミスによるインシデントを防ぐために必要な心構えや統制について紹介してきたが、企業のクラウド利用形態や規模においては機能させることが難しいケースもある。例えば、ベンダーロックインの回避や複数のクラウド事業者のサービスをカスタマイズして最適なシステムを構築する目的でマルチクラウド構成をとっている企業は多い。マルチクラウド環境においては、クラウド事業者ごとにサービスの特徴は異なるため、各々の特徴を理解し一元的なクラウドポリシーを定め管理することが必要となる。そして、膨大かつ複雑なクラウドシステムを構築している場合は、設定状態の監査をチェックリスト等により 1 つ 1 つ確認していくことは非常に非効率的であり、システム担当者が多忙な場合、チェックリストの解答精度をおろそかにしてしまい適切な監査ができない懸念もある。また、パブリッククラウドにおいては提供されるコンソール画面から GUI 操作でシステムを構築することが直感的でわかりやすいが、複雑なシステムほど設定箇所が多く、設定ミスの誘発につながるといったシステム的なデメリットもある。

上述に挙げた様に、企業における各種統制の課題について 4 P（People, Process, Products, Partners）分析[22]を行った。また、課題に対するアプローチの一例について、文献調査やヒアリングにより得られた知見などから表 3.1 および表 3.2 にまとめ、本書にて解説する章について記載した。

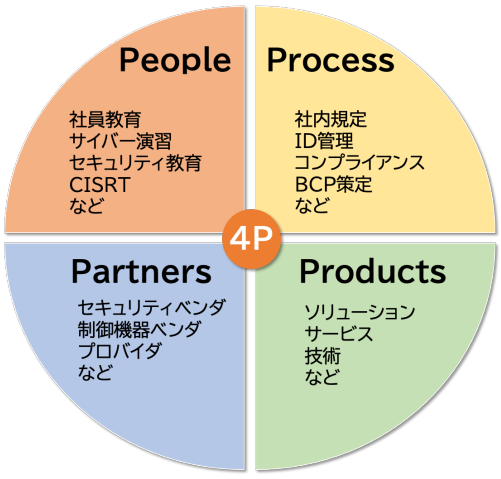

図 3.7　4 P 分析の概要

[22] セキュリティの課題と対策を 4 つの側面（People, Process, Products, Partners）から分析する手法

表 3.1 予防的統制実装における課題とアプローチ例

分類	課題	アプローチ例	解説する章
組織 People	セキュリティ教育不足やオンプレミスとパブリッククラウドの違いの理解不足から、設定ミスが増える	パブリッククラウドのセキュリティ教育の実施	5 章
		パブリッククラウド資格取得の奨励	
運用 Process	マルチクラウド利用企業では、クラウド事業者ごとにサービスの特徴が異なることにより、一元的なポリシー管理が難しい	CCoE やクラウドガバナンス組織を構築し、ポリシーやアカウントの一括管理体制を整える	5 章
	シャドークラウド[23]が発生し、統制漏れが出てしまう		
システム Products	業務要件を確認し、設定ミスをチェックするためのセキュリティチェックが必要であり、その結果業務負担が増え、事業部門の開発スピードに影響を及ぼす	セキュリティ要件の整った共通基盤を整備することで、チェックにかかる負担を緩和	5 章
	GUI 操作による開発・運用では設定箇所が多く、構成管理が難しいため、設定ミスが起こりやすい	IaC によるテンプレート化	4 章
パートナー Partners	最新のクラウドサービスの情報をタイムリーに取得・発信できず、ポリシー不備に気付けない	CCoE やクラウドガバナンス組織を構築し、パブリッククラウド最新情報を収集し、社内発信する	5 章

[23] 企業が使用許可をしていない、あるいは従業員が利用していることを企業側が把握できていないクラウドサービス

表 3.2 発見的統制実装における課題とアプローチ例

分類	課題	アプローチ例	解説する章
組織 People	パブリッククラウドのセキュリティ教育不足により、脅威の監視や分析、設定の監査を効果的に行えない	パブリッククラウドのセキュリティ教育の実施	5 章
		パブリッククラウド資格取得の奨励	
運用 Process	手動での監査は業務負担が大きく、正確性の保証も難しい	CSPM によるタイムリーな自動検知	4 章
システム Products	設定ミスを自動検知できず、セキュリティリスクが長期化する	CSPM によるタイムリーな自動検知	4 章
	GUI の設定項目は複雑であり、人の目では確認に限界がある	IaC によるテンプレート化 CSPM によるタイムリーな自動検知	4 章
パートナー Partners	最新のクラウドサービス情報の取得と発信が遅れ、監査項目の不備に気付けない	CCoE やクラウドガバナンス組織を構築し、パブリッククラウド最新情報を収集し、社内発信する	5 章

発見的統制をタイムリーに実施できないと、設定ミスが長期化してしまいセキュリティリスクが非常に高まる。図 3.8 に Palo Alto Networks 社が 2021 年に実施した、ハニーポットを用いたポート誤公開時の侵害速度調査の結果を示す。報告によると、sshd サービスのポートが公開されていた場合、最短 184 分で攻撃者に最初の侵害が実施されている。また、調査では 320 のハニーポットのうち 80%が 24 時間以内に侵害されたという結果も出ており、設定ミスを長期間放置してしまうことは、非常に大きなリスクとなることが分かる。

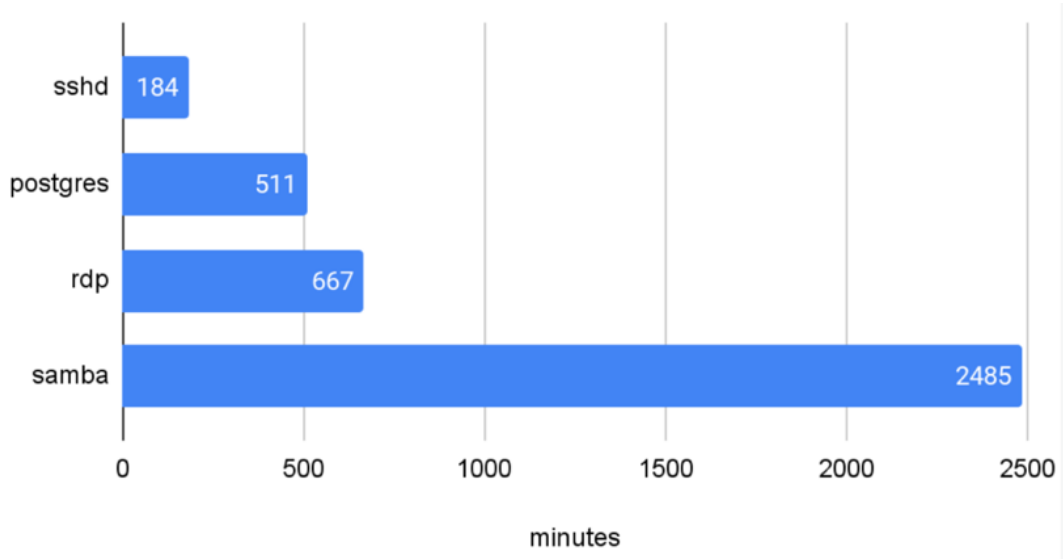

図 3.8 ハニーポットの展開から最初の侵害イベントまでの時間

（出典：Palo Alto Networks 社、Observing Attacks Against Hundreds of Exposed Services in Public Clouds、https://unit42.paloaltonetworks.com/exposed-services-public-clouds/）

第4章 統制効率化のための技術的アプローチ

本章では、前章で紹介した企業における発見的統制を支援する技術的アプローチについて紹介する。

4.1. CSPM

CSPM(Cloud Security Posture Management)とは、クラウドインフラストラクチャのリスクの予防、検出、対応を通じて IaaS および PaaS のセキュリティ態勢を継続的に管理するソリューションのことであり、日本語ではクラウドセキュリティ態勢管理と呼ばれることが多い。共通のフレームワーク、規制要件、エンタープライズポリシーを適用して、クラウドサービスの構成とセキュリティ設定のリスク/信頼性を評価し、適切な設定への修正を支援する。CSPM はクラウド事業者が提供するセキュリティサービスや 3rd パーティのベンダーが提供するソリューションがあり、CWPP（Cloud Workload Protection Platform）と称され、コンテナ[24]/サーバーレス/仮想マシンなどのクラウドワークロード保護機能を提供するものやリソースのアクセス権限を監視し、適切な権限制御内で動作しているかを確認し、最小権限の原則を支援する CIEM（Cloud Infrastructure Entitlement Management）などと併せて提供されているものも多い。なお、これらは日本語でクラウドワークロード保護プラットフォームやクラウドインフラ権限管理と呼ばれることが多い。

本書では、設定監査効率化に効果的なアプローチである CSPM について特筆する。

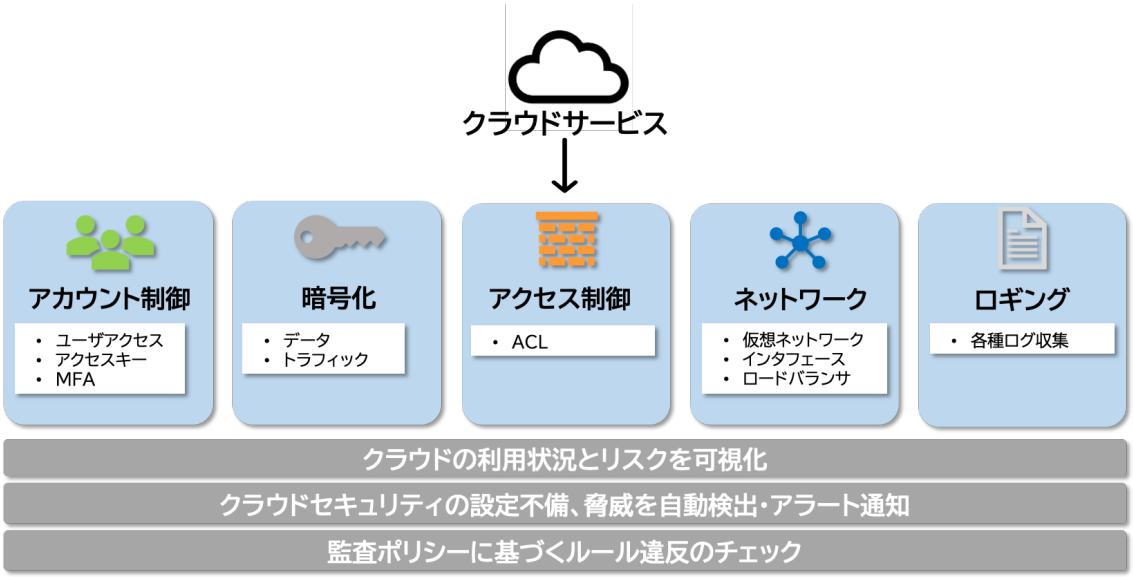

図 4.1 CSPM の概要

[24] アプリケーションやサービスを実行するための独立した環境を提供する技術

（コラム）CNAPP とは

クラウドサービスのセキュリティについて調査をすると、CNAPP（Cloud Native Application Protection Platform）という言葉をよく目にする。CNAPP とは、複数のセキュリティおよびコンプライアンス機能を 1 つに統合しているクラウド・セキュリティプラットフォームのことである。上述した CSPM や CIEM、CWPP をはじめ、コンテナの運用管理と自動化に用いられる Kubernetes のセキュリティとコンプライアンスの問題を解決する KSPM（Kubernetes Security Posture Management）や 4.2 で紹介する IaC(Infrastructure as Code)のコード評価を行う IaC scanning のようなものも構成要素に含まれる。クラウドサービスのセキュリティを効率的に確保するためには、必要に応じてこれらのサービスを活用していくことも重要である。

4.1.1. CSPM で用いられる代表的なセキュリティ基準

CSPM では検出した設定状態について、セキュリティ基準に照らし合わせた自動評価が可能だが、そこで用いられるものには、CIS Benchmarks や NIST-SP800-53、PCI-DSS をはじめ、クラウド事業者が提供するベストプラクティスなどがある。

表 4.1 代表的な CSPM のセキュリティ基準

セキュリティ基準	特徴
CIS Benchmarks	• セキュリティ推奨事項、設定値を記載したドキュメント • OS やミドルウェアのセキュアな設定のベストプラクティス
NIST-SP800-53	• 米国連邦政府の内部セキュリティ基準を示すガイドライン • セキュリティ対策のリスクマネジメントの方法から、ベースライン・セキュリティ統制の考え方、セキュリティ対策管理の指定方法について記載
PCI-DSS	• クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準
Well-Architected	• クラウドサービス事業者が公開しているクラウド設計・運用のベストプラクティス集

これらは、適用するクラウドシステムの用途や組織で定めたポリシーなどに応じて使い分けることが可能である。また、システムによっては検知したい設定ミスが検知項目にない規格もあるため、対象システムのリスク分析を行い、検知すべき設定ミスを洗い出し、カスタマイズすることも必要となる。

（コラム）デフォルトのセキュリティ基準で見つけにくい「設定ミス」

CSPM にデフォルトで準備されているセキュリティ基準として代表的なものを表 4.1 で紹介したが、それらには検知対象としてリストアップされていない、発見しにくい設定ミスもある。

例 1 ：不要な仮想サーバーの誤作成

開発環境などにおいて仮で作成した仮想サーバーを、そのまま本番環境に残してしまったり、運用中に誤って作成してしまったりすることがある。これらを放置してしまうと、脆弱性未対応の仮想サーバーが攻撃の踏み台に悪用されるリスクがある。対策としては運用ルールとして本番環境のリソースの命名規則を設定することにより、ルールから逸脱したものを早期に発見することなどが考えられる。

例 2 ：不適切なロギング容量設定

ログ容量を必要な量より小さく設定してしまうと、必要な期間のログが消失し、発見的統制に穴が生じる懸念がある。逆に必要なログ容量より大きく設定してしまうことで従量課金による想定外の費用負担が発生する。ログ容量が必要量より小さい場合の対策としては、ログの出力先を既定の場所以外に転送することで、容量超過によるログの消失回避が考えられる。過剰なログ容量設定に対しては、定常的なコスト監視を行うことで、想定以上の課金が発生しているサービスを特定し、設定ミスに気づくこともできる。

4.1.2. CSPM の運用例

CSPM の運用例についてモデルケースにて紹介する。CSPM を利用している企業へのヒアリング等によると、以下の様な使い方をしていることが一般的である。

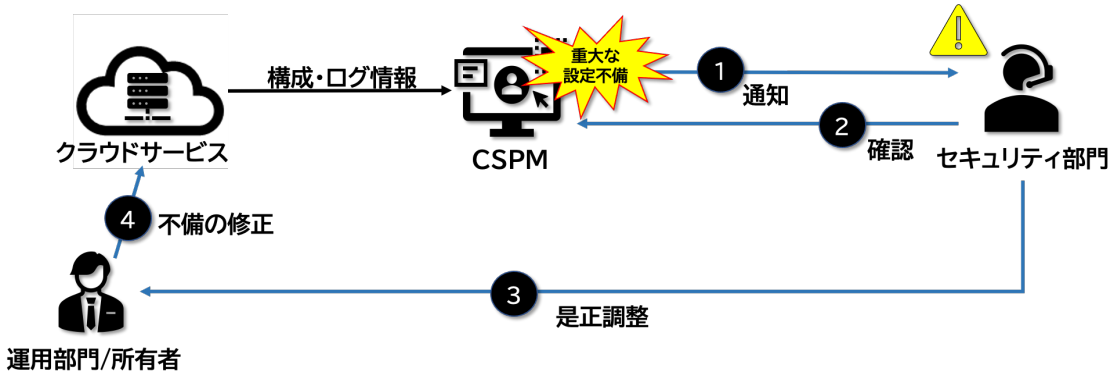

図 4.2.CSPM の運用例

① 事業部門が運用しているパブリッククラウドの設定ミスを CSPM が検知

② セキュリティ部門が CSPM の検知内容を確認する
③ セキュリティ部門から事業部門に対し設定ミスの是正調整を行う
④ 事業部門が不備を修正する

セキュリティ部門が設定ミスを直接修正することも不可能ではないが、不備修正により稼働中のシステムの可用性が失われる懸念がある。そのため、事業部門との調整によるシステムへの影響有無の確認をした上で不備を是正していくことが必要となる。

4.1.3. 検証およびヒアリングで得られた知見

本書の執筆に当たって、実際にパブリッククラウドに模擬 WEB サービスを構築し、ソリューションの検証を実施した。クラウド事業者を 2 つ利用した環境を想定し、クラウド事業者自身が提供する CSPM サービスと 3rd-パーティのベンダが提供する CSPM を適用し、設定ミス検出可否と併せてそれぞれの特徴を検証した。

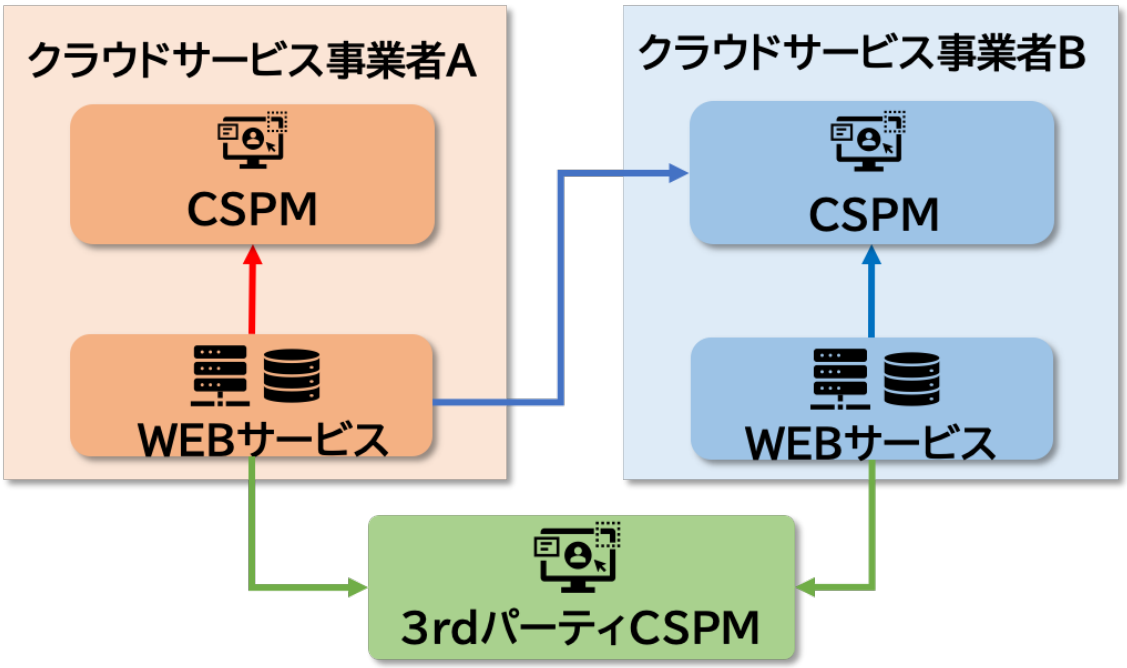

図 4.3 検証環境イメージ

以下のような代表的な設定ミスについて検証を行った。
① ユーザーの MFA 設定ミス
② 仮想サーバーの SSH 0.0.0.0/0 アクセス許可
③ オブジェクトストレージのパブリックアクセス誤設定
④ ネットワークログの取得設定ミス
⑤ ストレージデータ暗号化設定ミス

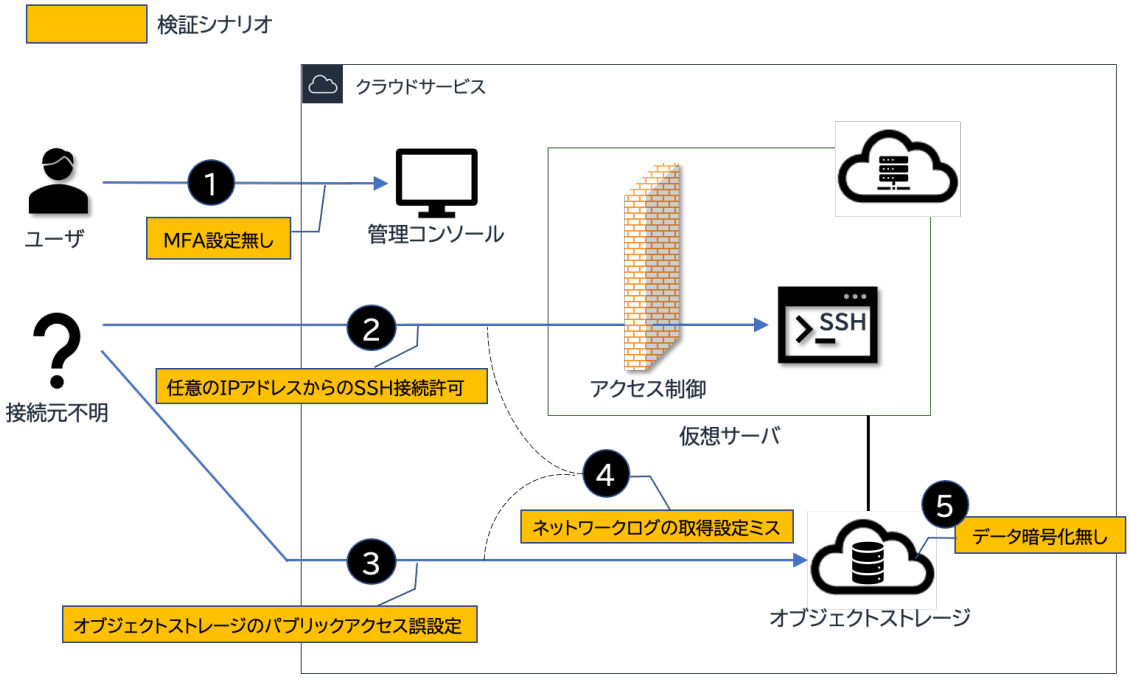

図 4.4 構築したシステム構成とシナリオのマッピング図

結果として、全ての CSPM で全シナリオを検知することができた。検証により、設定ミスが発生してから検知されるまでの時間や、コンソール画面の使いやすさ、設定ミスの検知をカスタマイズする柔軟性など、各ソリューションにはそれぞれ異なる特徴がみられた。また、設定ミスが検知された際のメールアラートや SNS 連携の設定、そして自動的な設定修正機能の実装の容易さも、ソリューションごとに異なる特徴が見られた。

検証を通して、CSPM の設定ミス自動検出機能により、目視による設定確認の負担軽減や、設定ミス放置によるセキュリティリスクの長期化を防ぐことに大きな効果があることが分かった。一方で、企業や組織が CSPM の効果を活かすためには検討しておくべき様々な課題があることも分かった。

ここで、機能検証および実際に CSPM を運用している企業へのヒアリングより、CSPM を活用していく上での運用上の課題とそれに対するアプローチ方法について表 4.2 にまとめた。

表 4.2 CSPM 活用における課題とアプローチ例

分類	課題	アプローチ例
組織 People	パブリッククラウドのセキュリティ理解不足により、事業部門が修正指示に対応しづらい状況や指示内容の不明確さが生じる	パブリッククラウドのセキュリティ教育の実施 パブリッククラウド資格取得の奨励
運用 Process	セキュリティ部門が膨大なアラートに対応できず、遅延や未処理のアラートが発生する	対応するアラートの優先順位づけの実施 アラートを放置しない運用体制の構築
システム Products	アラートの内容が設定不備か意図した設定か判断できない	アラートの棚卸を行う
	過剰な機能や使いこなせない機能が存在し、コストの浪費が起こる	組織のクラウド戦略を理解し、必要な機能要件を整理しておく PoC[25]を十分に行う
パートナー Partners	クラウド事業者のサービスや CSPM のアップデートに対応できず、検知機能に不備が生じる	アップデート時の連絡体制を確認しておく 社内のアップデート対応担当者を決めておく

[25] Proof of Concept：新しいアイデアやコンセプトの実現可能性を評価するために行われる実証実験

4.1.4. CSPM 活用にあたって気をつけるべきこと

これまでの知見を踏まえ、CSPM を企業が使っていく上で気を付けておくべき事項を導入から廃棄までのフェーズごとに図 4.5 にまとめた。

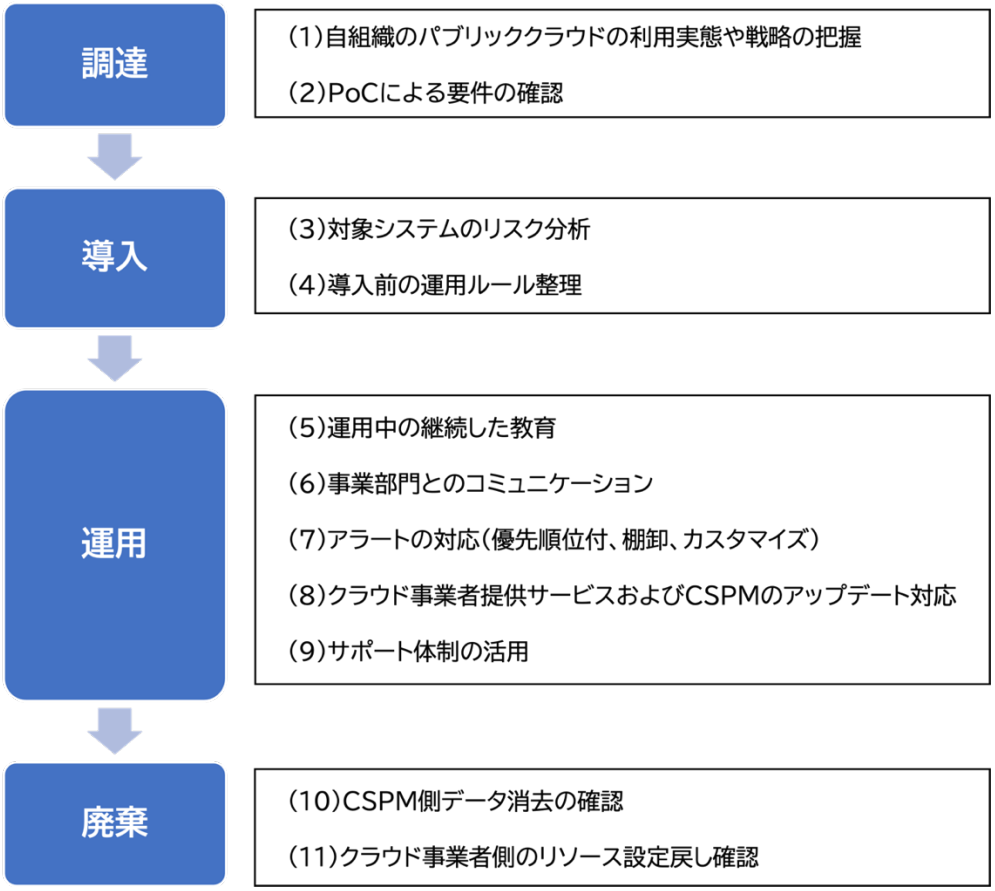

図 4.5 各フェーズにおける CSPM 活用の留意点

調達

(1) 自組織のパブリッククラウドの利用実態や戦略の把握

自組織でパブリッククラウドをどのような目的で使っているのかを把握することが必要である。特に業界のガイドラインに準拠しなければならないシステムがある場合は、CSPM に備わっているセキュリティ基準が十分であるか判断するためにも把握が必須となる。また、CWPP や CIEM などの機能が兼ね備わっているか、それらが必要かどうかについての判断材料としても自組織の環境について把握しておくことがポイントとなる。

(2) PoC による要件の確認

把握した自組織のクラウド用途に応じた CSPM を採用するために PoC を行い、機能要件および非機能要件の確認を行う。要件の確認結果から、最も適した CSPM を選択することとなる。

表 4.3 CSPM の機能要件および非機能要件の例

■機能要件例

評価軸	概要
網羅性	企業のポリシーと規制要件を満たすために、十分なセキュリティ基準が提供されているか
正確性	取り込んだ情報が正確かどうか
カスタマイズ性	セキュリティ基準の検知項目がカスタマイズできるか（項目の追加・削除、重大度の変更など）
アラート機能	設定ミスを検知した際に、メールや SNS 連携ができるか、またはそのやりやすさはどうか
システムへの影響	スキャンすることにより対象のシステムへ影響はないか
マルチ対応	検知対応可能なクラウド事業者は何があるか
自動修正機能	設定ミスを自動で修正する機能があるか
付加機能	CWPP や CIEM など CSPM 以外にどのような機能があるか

■非機能要件例

評価軸	概要
可用性	機能が常に利用可能かどうか
拡張性	クラウド環境の規模や複雑性に応じてスキャン対象範囲の拡大ができるかどうか
導入前提条件	CSPM としての機能を満たすために設定が必要なクラウドサービスの種類は何があるか
レポーティング	レポートを出力できるか 出力されたレポートは見やすく使いやすいか
検知速度	設定ミス発生から検知までの速度はどうか
ユーザービリティ	セキュリティエキスパートでなくても解析可能か
コスト	導入および運用に必要なコストはどうか
セキュリティ	CSPM に利用権限設定、不正アクセス防止などセキュリティ機能があるか

導入

(3)　対象システムのリスク分析

システムのリスク分析を行い、守るべき資産と脅威について洗い出し、CSPM で検知すべき必要な設定を洗い出す。そして検知すべき設定ミスを把握する。これにより、検知したいセキュリティ基準のカスタマイズや対応優先順位付のベースラインを作成しておく。

(4)　導入前の運用ルール整理

CSPM でのアラート確認から設定ミス修正までの流れを整理し、運用ルールとして整備しておくことは重要なポイントであり、事業部門に確実に周知しておかないと対応遅れによるリスク増大につながる。

運用

(5)　運用中の継続した教育

継続的に CSPM の扱い方についての教育を行うことで、担当者によって対応レベルが変わらないようにすることが大事である。

(6)　事業部門とのコミュニケーション

設定ミスを修正するためには、クラウドを運用している事業部門の協力が欠かせない。日々事業部門とはコミュニケーションをとり、対応フローにのっとって円滑に対処できるようにしておく必要がある。

(7)　アラートの対応（優先順位付、棚卸、カスタマイズ）

組織のクラウド利用規模によっては、設定ミスのアラートが膨大になり、対応に遅れが発生するケースも大いに考えられる。そのため、リスク分析結果を踏まえた検知内容の優先順位付けを行う。また、意図した設定が設定ミスとしてアラートされる場合もあるので、対応が不要な検知結果をアラートから解除することも必要となる。逆に、デフォルトで備わっているセキュリティ基準ではセキュリティリスクを網羅できていない場合もあるため、独自の検知項目にカスタマイズすることも求められる。

(8)　クラウド事業者提供サービスおよび CSPM のアップデート対応

クラウド事業者の提供するサービスは日々サービスアップデートがされており、それにより CSPM がアップデートに対応できず設定ミスを検知できないケースも考えられる。逆に、CSPM 側のアップデートも想定され、そのような場合の連絡体制を事前に確認しておくことが必要である。また、アップデート対応者を組織内であらかじめ決めておくことも望ましい。また、クラウド事業者のサービスがアップデートされた場合、シ

ステムの仕様変更に併せてリスクも変わる場合もあるため、リスク分析結果を見直す必要がある。

(9)　サポート体制の活用

CSPM を提供するクラウド事業者および 3rd-Party ベンダーのサポート体制をうまく活用し、トラブル時にいち早くサービスを復旧できる体制を整えておく。

廃棄

(10) CSPM 側データ消去の確認

クラウドシステムの運用を停止する場合、これまで CSPM に流れていたデータが CSPM 利用停止に伴いデータ削除されているかの証跡を確認できるようにしておく。

(11) クラウド事業者側のリソース設定戻し確認

CSPM を利用する場合、当該システム以外にも CSPM へ連携するためのログ収集設定やストレージ設定などが必要になるケースがある。そのようなリソース設定は廃棄と共に設定解除を行うべきであり、放置すると従量制課金により不要なコストの発生や、残った不要なリソースが悪用される可能性もある。

CSPM は発見的統制において大きな効果をもたらすため、積極的な導入が望ましい一方で、あるべきステップを踏まなければ、機能に過不足が発生し、宝の持ち腐れになりかねない。本項を参考に検討を進めていただければ幸いである。

4.2. IaC

本章では、構成管理や設定ミス削減に効果的な技術である IaC(Infrastructure as Code)について紹介する。IaC によって予防および発見の 2 つの統制を支援することが可能となる。

4.2.1. IaC とは

IaC はクラウドサービスに対して、GUI を介した手動のプロセスではなく、コードを使用してインフラストラクチャの管理と調達や設定を行うことである。文字通り、仮想マシンやストレージ、ネットワークなどのインフラをコードとして表現することができる。

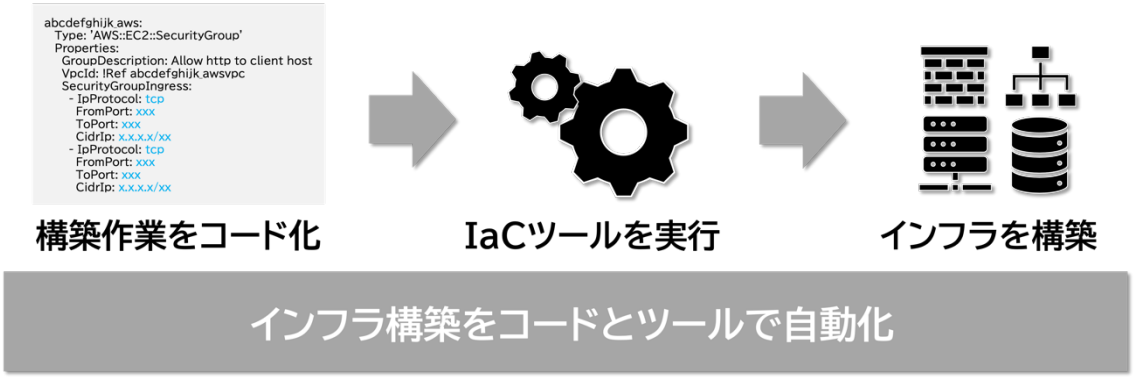

図 4.6 IaC の概要

4.2.2. IaC 活用により得られる効果

IaC を活用したクラウドシステムの構築により享受できるメリットについて以下に示す。

1. 作業の効率化による工数削減

   コードを記述してインフラ環境の構築・管理業務を自動化することで、手作業で行うよりも工数を削減できるため作業効率が上がる。また、一度記述したコードは再利用可能であることから、同じ構成のシステムを複数構築する必要がある場合に、ゼロから何度も構築する手間を省略できる。

2. 管理・メンテナンス負荷削減

   従来のインフラ管理とは異なり、バージョン管理ツール[26]などを活用することでコードのバージョン管理が可能になる。そして、コードの変更履歴や過去に実施した作業の

[26] ソフトウェア開発やファイル管理において、ファイルの変更履歴やバージョンを管理するためのツール

確認ができ、大規模な環境でも管理・メンテナンスがしやすくなるほか、インフラがコード化されているため、構成のブラックボックス化を防ぐこともできる。

3. GUI による設定ミスの削減

IaC ではコード記述によりシステム構築が自動で実行されるため、GUI 操作が不要になるため、設定ミス発生を抑えることができる。特に複数のテスト環境を用意する場合や、同じ構成をユーザーごとに用意しなければならない場合など、同じ環境の構築が繰り返し必要な場面で、べき等性（複数回実行しても同じ結果になること）を保つために IaC は非常に有効である。

このように、IaC の利用は GUI 操作による設定ミスの発生そのものを削減することや、システム構成の把握・管理がしやすくなることによる予防的統制および発見的統制の効率化に大きく貢献する。

4.2.3. IaC 活用事例

ここで、IaC を実際に導入している事例をいくつか紹介する。

政府機関の例：デジタル庁

デジタル庁は政府機関と自治体のための共通クラウドサービス利用環境としてガバメントクラウドを整備している。サーバーなどの構築・運用管理を行うためのマネージドサービスや、IaC によりインフラ環境をコード管理で自動生成することでシステムの構築・運用管理のコストを大きく削減できるとしている。そして、主要なセキュリティ設定を組み込んだ IaC テンプレートの活用が、インフラ構成を適切に管理でき、セキュリティ維持に役立つとしている。

企業の例：中外製薬株式会社

中外製薬株式会社ではアカデミアや医療機関、パートナー企業など外部ユーザーとの共同研究プロジェクトを迅速に推進するための研究環境をクラウドサービス上に構築している。研究環境の提供においては、IaC を使用して環境構築作業を共通化・自動化しており、結果、従来 6 か月かかっていた作業を最短 1 週間まで短縮できたとしている。また、IaC を利用することで標準化されたセキュリティ関連サービスや機能を自動的に適用できるため、システム環境構築・導入に要するコストは、他クラウドサービスを利用していた際と比較して 90%削減したとしている。

4.2.4. 活用にあたって気をつけるべきこと

IaC はメリットも多い反面、使い方を間違えるとかえってセキュリティリスクが大きく

なってしまう。ここでは検証やヒアリングをもとに IaC を企業が活用していく上での課題とそのアプローチについて整理を行い、表 4.4 にまとめた。

表 4.4 IaC 活用における課題とアプローチ例

分類	課題	アプローチ例
組織・人材	• IaC スキル取得の学習コストが高く、属人化する恐れがある • GUI 操作に慣れた開発者がコード構築に参入するハードルが高い	• IaC スキル取得に向けた教育を継続的に行う • IaC の仕組みとメリットを開発者が理解する • 抽象化したツールを活用する
方針・規定	• IaC 構築後の管理方法（IaC または GUI 操作）が統一されておらず、つい GUI 操作を行ってしまい、設定ミスにつながる	• IaC 構築・管理における変更手順等の運用ルールを設ける • IaC の仕組みとメリットを運用者が理解する
技術・プロセス	• 記述するコードそのものに設定ミスが発生してしまう • 機密情報をコードに書き込んでしまい、攻撃者に悪用されるリスク	• バージョン管理や CI/CD[27]などの管理・テスト体制などの整備体制を整える • IaC チェックツールの導入

[27] Continuous Integration／Continuous Delivery：継続的インティグレーション/継続的デリバリーと呼ばれ、ソフトウェアの変更を常にテストし、自動で本番環境に適用できるような状態にしておく開発手法

また、整理した内容を踏まえ、IaC 活用にあたっての留意すべき事項を導入～廃棄の各フェーズに分けて図 4.7 まとめた。

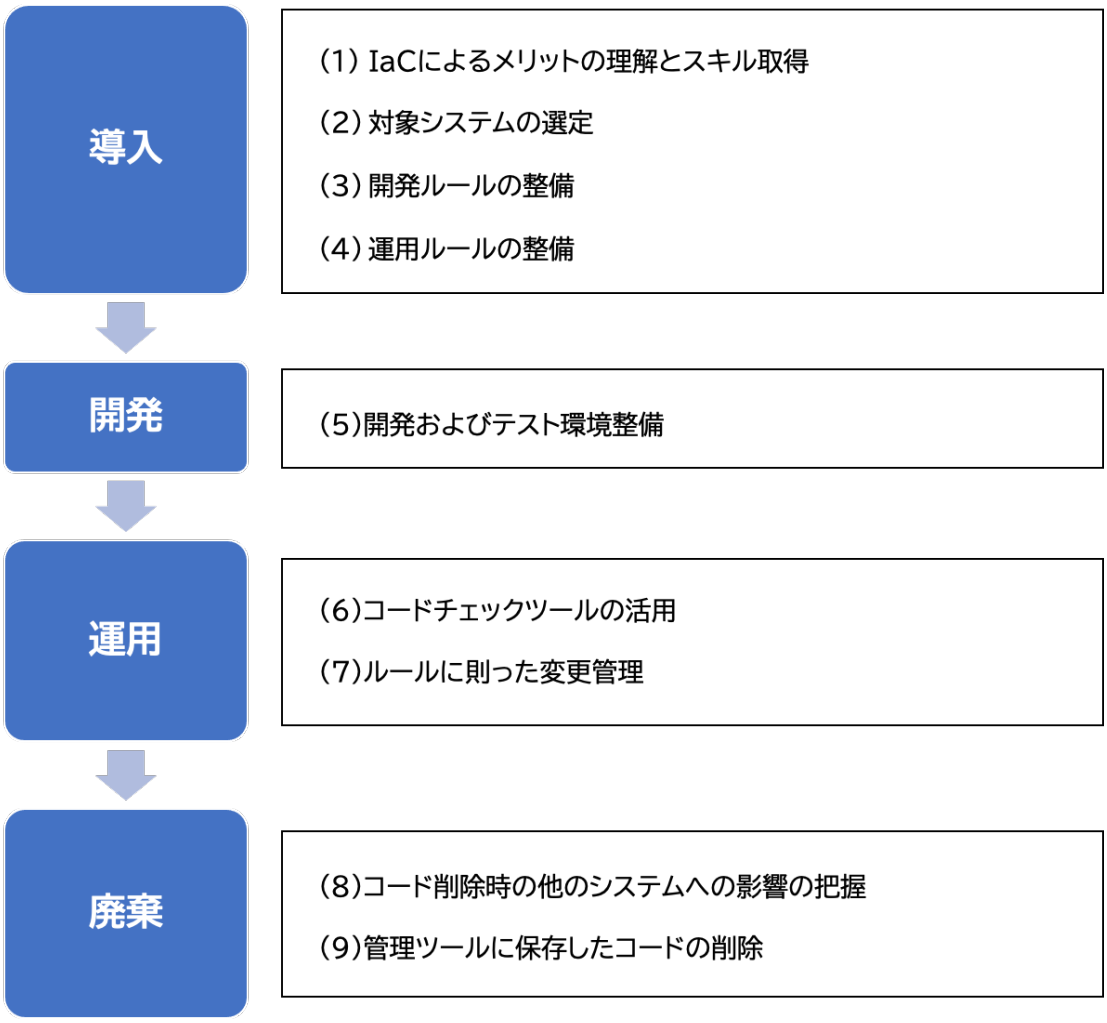

図 4.7 各フェーズにおける IaC 活用の留意点

導入

(1)　IaC によるメリットの理解とスキル取得

IaC を機能的に使うためには、継続した教育により IaC への理解を深めることが重要である。特に GUI 操作に慣れている開発者にとって IaC を使うことは、コードや構築ルールがわからないことによる心理的障壁や、高い学習コストが必要になるといった参入のしにくさを感じる可能性がある。そこで必要なのが IaC のメリットをしっかりと理解することである。GUI、CLI、そして IaC によるシステム構築についてそれぞれの特徴とクラウドが動く仕組みを知り、なぜ IaC が効果的なのか納得することが大事である。

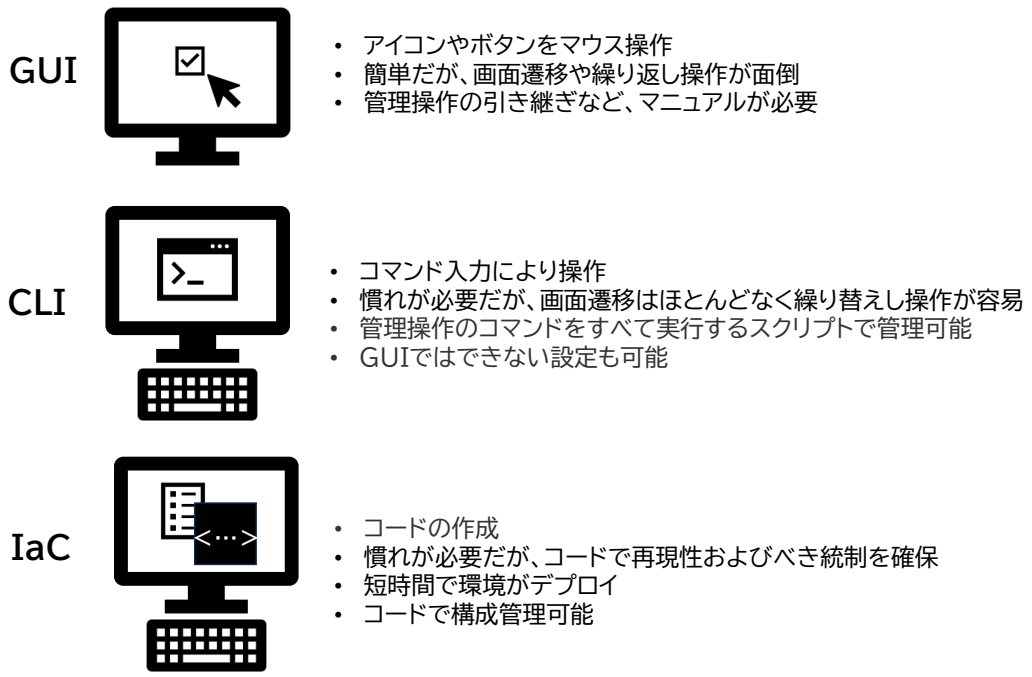

図 4.8 クラウドシステム構築手法の特徴

(2)　対象システムの選定

IaC 活用の対象となるシステムを選定する。IaC はコード化に時間を要するため、汎用性のない構成をコード化するのに多くの時間と人材を費やしても費用対効果が見込めない場合もある。構成把握に長け、セキュリティメリットの大きい IaC だが、あくまでビジネス手段であることに注意する。

(3)　開発ルールの整備

GUI を用いず、一貫して IaC での開発を行うようにルールを決める。また、CI/CD などテストを行う上での社内ルールを定めておく。

(4)　運用ルールの整備

運用開始後に IaC で管理を行う範囲について明確化し、緊急時を除き IaC で構築した環境を変更しないようルールを定める。システム的に権限を限定するのも有効である。

開発

(5)　開発およびテスト環境整備

チームで構築する場合に共用でバージョン管理がしやすい開発ツールを用いることや、CI/CD によるテスト環境の自動化などを整備することで IaC を安全に利用しメリットを

最大限に活かすことができる。

運用

（6） ルールに則った変更管理

IaC で構築したシステムでも GUI による設定変更は可能である。そのため、定めた運用ルールに則り、緊急な場合を除いて GUI による変更は行わないことが重要である。

（7） コード変更検知ツールの活用

IaC のコードに対して、ドリフト（コード変更差異）を自動で検知してくれるツールを活用することも有効である。また、前節で述べた CSPM と組み合わせて、設定変更を検知する仕組みを作っておくことも効果的である。

廃棄

（8） システム廃棄時の他のシステムへの影響の把握

他のシステムと連携している場合、コードを削除するとサービスに影響が出る可能性があるため、影響を把握してから削除するべきである。

（9） 管理ツールに保存したコードの削除

IaC 構築システムを廃棄する際は、バージョン管理ツールに保存しているコードの廃棄にも注意する。廃棄システムのコードがツール上に不要意に残ると、悪用されるリスクや、誤って公開されるリスクもある。

IaC は構成管理や設定ミス防止におけるメリットが大きい反面、コードのテストを確実に実施しなければリスク範囲も大きくなる。IaC は手段であり目的ではないことを理解し、IaC によって自動化する目的をはっきりした上で使うことが重要である。

（コラム）IaC を活用した教育コンテンツの作成

IaC を利用することで、教育コンテンツの作成にもメリットを活かすことができる。本プロジェクトでは、設定ミスのリスクについての教育を、ハンズオン形式のゲームで学ぶコンテンツを作成した。

このコンテンツでは、実際のクラウド環境で必要な予防的統制と発見的統制を設定ミスと関連付けて学ぶことができる。また、IaC を使用して演習環境を構築することで、環境構築にかかる手間を削減できるだけでなく、演習環境の一貫性を保つことができ、運営者としても大きなメリットがある。

さらに、環境構築に IaC を活用していることを受講者に伝えることで、IaC のメリットを普及させる一助にもなる。

第5章 統制効率化のための組織的アプローチ

5.1. CCoE（Cloud Center of Excellence）とは

CCoE とは、クラウド戦略を全社的に推進していくために、必要な人材やリソースなどを集約したクラウド活用推進組織を指す。各部門に点在するクラウドに関する優れた人材や技術、ノウハウ、設備を集約した組織として設置され、部門の垣根を超えた全社的なクラウド活用の推進を担う。昨今、クラウド活用に着手したものの「思ったほど活用が進まない」「良さを活かしきれていない」「セキュリティに不安がある」といった課題に多くの企業が直面し、その組織的な解決策の 1 つとして注目を集めている。

CCoE に期待される役割としては「(攻め) 積極的なクラウド活用の推進」と「(守り) クラウド統制」の 2 つの側面がある。攻めの側面として、クラウドのメリットを最大限に引き出すような全社的なクラウド活用の牽引があり、一方で守りの側面として、セキュリティなどのリスクを最小限に抑えたクラウドの安全な活用推進がある。攻めと守りの両面をバランスよく遂行することで、企業のビジネス価値の向上に寄与することが期待される。本章においては、以下、CCoE が果たす守りの側面に着目する。

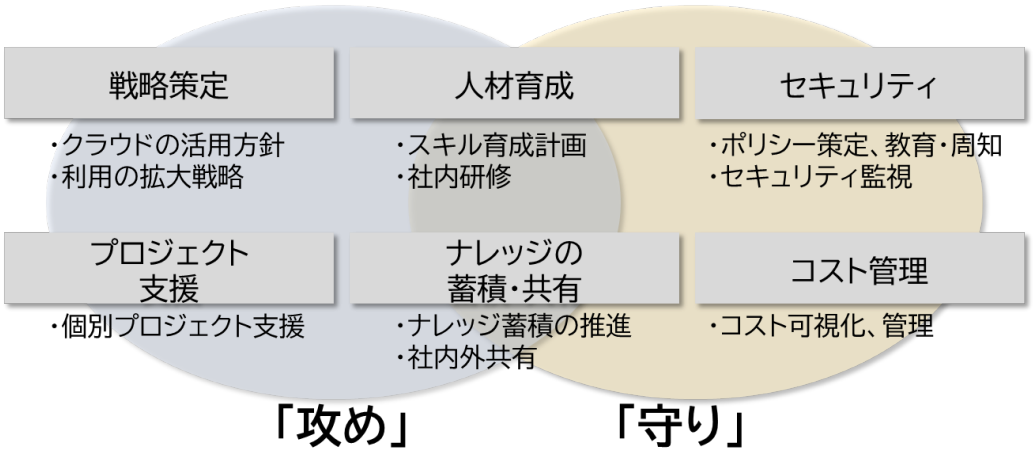

図 5.1 CCoE に期待される役割

5.2. CCoE によるセキュリティガバナンス

前節で述べたように、CCoE には全社的なクラウド統制が期待される。その中でも重要な役割として、セキュリティが挙げられる。本節では、CCoE が果たすセキュリティに関する役割について述べる。

クラウド活用推進に際して、多くの企業で「自由と統制のバランス」というセキュリテ

ィ課題に直面する。クラウド活用を重視しユーザーに高い自由度を与えた場合、セキュリティに関する不安が高まる。一方で、セキュリティを重視し強い統制を行った場合、クラウドのメリットである機動性が損なわれてしまう。そこで、リスクを抑えつつも機動性を損なわないためにセキュリティに関する予防的統制と発見的統制の 2 つをバランスよく遂行することが求められ、CCoE がその役割を担う。CCoE は全社のクラウド戦略を担当する組織であり、ビジネスの視点からセキュリティリスクと機動性の 2 つのバランスを見極める役割を果たす。

また、多くの企業が直面する別の課題として「クラウドの進化への追従」「人材育成」が挙げられる。「自由と統制のバランス」という課題をいったん乗り越えたとしても、クラウドは常に進化するものであるため、何もしなければ整えた仕組みやスキルの陳腐化は免れない。そこで、クラウドは常に進化するものであるという前提のもと、整備した仕組み・プロセス・人材・スキルを常にアップデートすることが求められる。CCoE には技術、ノウハウを集約した組織として、上記の役割も期待される。なお、これを実現するためにも、CCoE を担う人材にはクラウドに対する理解だけでなく、新しいことに取り組むチャレンジ精神や全体最適の視点、コミュニケーション力、強いリーダーシップ等が求められる。

以下、CCoE に期待される予防的統制と発見的統制について簡単に述べる。なお、CCoE には決められた形があるわけではない。下記は一例であり、企業のビジネスや文化、課題等に合わせて適切な体制・役割の検討が求められる。

予防的統制

全社のセキュリティ水準の統一を図るためには、全社に適用するセキュリティポリシーの存在が大前提となる。CCoE には、部門の垣根を超えた組織としてセキュリティ部門やコンプライアンス部門など関係各部門を巻き込み、セキュリティポリシーを策定することが最初に求められる。また、策定したセキュリティポリシーの周知、徹底を図るうえで人材育成が欠かせないが、クラウドサービスは移り変わりが激しく、教育内容の陳腐化が起こり易い。CCoE には、集約した人材を活かし最新情報のキャッチアップを行いつつ、クラウドを扱う人材が必要なスキルを身に着けることができるよう、全社的な教育や訓練プログラムの策定、適切な情報提供を行うことが求められる。他にも、全社アカウントの一括管理、新規開発にあたってのセキュリティ水準の統一を図るためのクラウド設計/開発の標準化、共通基盤の構築なども CCoE の役割となり得る。

発見的統制

複数あるクラウドの品質を一定水準に維持するためには、全社一括でのセキュリティ監視が重要となる。また、オンプレミスとは異なるクラウド固有の特長として、設定ミスが大きなセキュリティ事故を引き起こすことを考えると、インシデント発生を未然に防止するためのクラウドセキュリティリスク監視等の実施も求められる。CCoE は全社のクラウドを統

括管理する組織としてこれらの役割を担い、クラウドを一括監視することも考えられる。なおその際、これまでに紹介した CSPM や IaC などのセキュリティ強化のための技術的なアプローチの活用が有効となってくる。このような最新の技術を円滑に運用するためには、スキルの維持向上や最新情報のキャッチアップが欠かせない。CCoE は、この課題に対する組織的な解決策としても期待される。

5.3. 共通基盤によるガバナンス強化

本節では、セキュリティガバナンスのベストプラクティスの 1 つとして、クラウド環境における共通基盤の構築について紹介する。

前節で述べた「自由と統制」のうち「自由」を重視し、クラウド活用の推進を各部門に任せた場合、構築されたクラウドのセキュリティレベルのバラつきや、認証や決済などの各部門で利用する機能の重複、またそれによる運用負荷の増大などの問題が発生する。一方で「統制」を重視し、構築するクラウドに対して事前のチェック等を行った場合、クラウドのメリットである機動性が損なわれる可能性がある。そこで、機動性を損なわず、セキュリティレベルの統一と共通機能の単一化を実現するための施策として、各部で共通して利用する機能を高いセキュリティを確保した形で構築し、共通基盤として提供する手法が注目を集めている。各部門でクラウドを構築する際は、この準備された共通基盤を利用することで、一部機能の構築の手間が省けるだけでなく、高いセキュリティが担保されることになる。

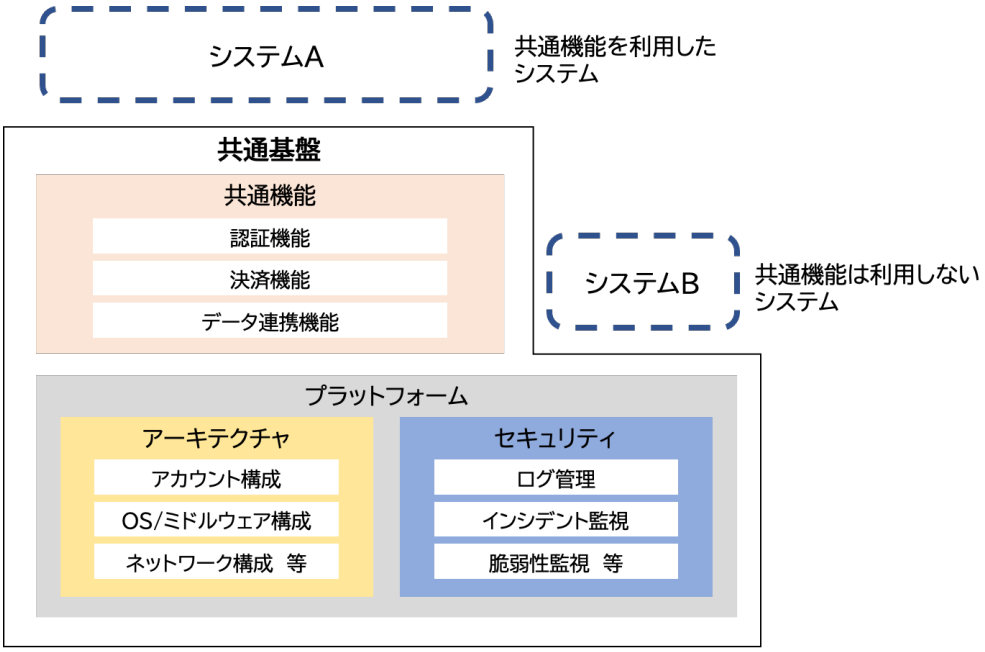

図 5.2 クラウド共通基盤の概要

5.4. CCoE は必ず必要なのか

本章では、クラウド戦略を全社的に推進していくための組織として注目を集めている CCoE について紹介した。ここまで述べてきたように、CCoE は、企業がクラウドを安全かつ最大限に活用するために非常に役立つ存在であると考える。ただし、クラウド活用において CCoE は手段であり目的ではない。これまでに紹介した課題を解決することができる情報システム部門があるのであれば、CCoE は不要となる。企業のビジネスや文化、課題、クラウド活用の状況などによって、CCoE は必ずしも最適な選択肢とはならないことを留意いただきたい。

第6章 まとめ

本書では、クラウドサービス利用における設定ミスという脅威の紹介と重要な 2 つの統制、ならびに効果的なアプローチについて解説を行った。

クラウドサービスを利用する際には、設定ミスの発生を最小限に抑えるための予防的統制と、設定ミスが発生してもそれをインシデントにつなげないための発見的統制をバランス良く活用することが重要である。これによって、設定ミスと上手く付き合いながらクラウドサービスのメリットを最大限に享受することが可能となる。

また、CSPM といったソリューションは設定ミスを自動で検出でき、目視による設定確認の負担軽減や、設定ミス放置によるセキュリティリスクの長期化を防ぐことに大きな効果がある。しかし、導入すれば設定ミスによるインシデントを防ぐことができるわけではなく、多くの企業が導入後の運用上の課題に直面している。そのため、導入前の PoC や運用ルールの整理などを行い、スムーズな運用を実現することが重要である。

IaC は、設定ミス対策や構成管理に優れた技術であるが、コードチェックを怠ると脆弱な環境が容易に構築されるリスクがある。必要なテスト環境やルールの整備、そして IaC のメリットを理解することで、最大限の効果を得ることができる。

組織的アプローチである CCoE は、近年のクラウド利活用が進んだ企業においてクラウドガバナンスを組織横断的に機能させるために大きな効果をもたらす。ただ、CCoE の構築が正解であり、あるべき姿というわけではなく、組織においてクラウドガバナンスを効かせることが重要であり、それは CCoE に限らないということは留意されたい。

本書で示した設定ミスと上手く付き合うためのポイントは、様々な企業・個人へのヒアリングおよび技術検証をもとに作成したが、あくまでプロジェクトメンバーで考察した結果であり、ヒアリングにご協力いただいた企業・個人の主張とは異なる点がある。そのため、本書が唯一無二の正解だとは考えていない。しかし、クラウドサービスの設定ミスによるインシデント対策をこれから検討していく読者にとっては参考になる内容だと考える。

なお、本書は 2023 年 6 月時点の考えをもとに執筆したものであり、クラウド技術の進展を踏まえ、免責事項で本書の利用期限として定めた 2 年後にも本書の内容がそのまま通用するとは考え難い。クラウドサービスやソリューションは日々刷新されているため、最新の情報や技術を常にアップデートし続ける必要がある。

本書が、企業や組織のクラウド戦略におけるセキュリティに対する懸念の緩和になれば幸いである。

参考文献

- 経済産業省,”DX レポート～IT システム「2025 年の壁」の克服と DX の本格的な展開～”,2018.
- NIST,” The NIST Definition of Cloud Computing”,2011.
- 独立行政法人情報処理推進機構,”NIST によるクラウドコンピューティングの定義”,2011.
- 内閣官房内閣サイバーセキュリティセンター,”クラウドを利用したシステム運用に関するガイダンス（詳細版）”,2022.
- 経済産業省,”令和 3 年度 重要技術管理体制強化事業（クラウドを活用した重要情報管理体制強化に向けた調査事業）調査報告書”,2021.
- 総務省,”令和 4 年情報通信に関する現状報告”,2022-08-30,https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nd236800.html,（参照 2023-06-08）
- CSA ジャパン,”クラウドコンピューティングの重大脅威　パンデミックイレブン”,2022.
- 松本 省吾、桐谷 章一、畠中 亮、前田 駿介,”AWS ではじめるクラウドセキュリティ”,2023.
- 総務省,”クラウドサービス利用・提供における適切な設定のためのガイドライン”,2022.
- デジタル庁,”政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針”,2022.
- Palo Alto Networks,”Observing Attacks Against Hundreds of Exposed Services in Public Clouds”,2021-11-22,https://unit42.paloaltonetworks.com/exposed-services-public-clouds/,（参照 2023-06-08）
- 佐々木　弘志,”製造業のサイバーセキュリティ 産業サイバーセキュリティ体制の構築と運用”,2021.
- Kief Morris,”Infrastructure as Code-クラウドにおけるサーバ管理の原則とプラクティス”,2017.
- 大澤 文考,”AWS Lambda 実践ガイド　第 2 版”,2022.
- 中外製薬株式会社,”AWS 導入事例:中外製薬株式会社”,2023-05-12, https://aws.amazon.com/jp/solutions/case-studies/chugaiseiyaku/,（参照 2023-06-11）
- 黒須 義一、酒井 真弓、遠山 陽介、伊藤 利樹、饒村 吉晴,”DX を成功に導くクラウド活用推進ガイド CCoE ベストプラクティス”,2021.

謝辞

本書の作成にあたりまして、デジタル庁様、大日本印刷株式会社様、株式会社竹中工務店様、NEC ソリューションイノベータ株式会社様、また個人として松本照吾様、他にもご協力いただいた組織の皆様には、貴重なご意見や情報をご提供いただくなど、多大なるご支援・ご尽力を賜りました。お世話になりました皆様にこの場を借りて心より御礼申し上げます。

また、産業サイバーセキュリティセンター中核人材育成プログラムの講師であられる、門林雄基先生、満永拓邦先生、小林和真先生には、多くのご指導・ご助言を賜りました。先生方の専門知識と情熱により、本プロジェクトを完遂することができました。改めて御礼申し上げます。

そして、本書の作成や本プロジェクトをともに実施した、下記メンバーの皆様にも感謝を伝えたいと思います。

＜クラウドセキュリティプロジェクト＞

（総勢 13 名）

【リーダー】

上池　雄一郎

【サブリーダー】

濱野　智明　　福田　哲也

【メンバー】

上野　泰寛　　時田　輝

大塚　真緒　　内藤　義仁

金子　英司　　平岡　侑祐

高橋　奈央美　　村上　由佳

土屋　拓仁　　吉原　尚史

用語集

用語	意味・解説
CI/CD	Continuous Integration／Continuous Delivery：継続的インティグレーション/継続的デリバリーと呼ばれ、ソフトウェアの変更を常にテストし、自動で本番環境に適用できるような状態にしておく開発手法。
CSA	Cloud Security Alliance：クラウドコンピューティングのセキュリティに関するグローバルな非営利団体。
DNS	Domain Name System：インターネット上で ドメイン名 を管理・運用するために開発されたシステム。
IDS	Intrusion Detection System：侵入検知システムと呼ばれ、不正や異常な通信を検知し管理者に通知するソリューション。
IPS	Intrusion Prevention System：侵入防御システムと呼ばれ、不正や異常な通信を検知し防御・遮断を実施するソリューション。 IPS は不正通信検知後、通信遮断を実施するところが IDS と異なる。
NIST	National Institute of Standards and Technology：米国立標準技術研究所 米国商務省配下の科学技術分野における計測と標準に関わる研究所。
PoC	Proof of Concept：新しいアイデアやコンセプトの実現可能性を評価するために行われる実証実験。
SIEM	Security Information and Event Management ：IT（OT）機器のログを一元的に収集・管理・解析し、ネットワークの監視やサイバー攻撃やマルウェア感染などのインシデントにつながる脅威を検知する仕組み。
SLA	Service Level Agreement：サービス提供者と利用者との間で結ばれるサービスのレベル（定義、範囲、内容　等）に関する合意。
SSH 接続	Secure Shell 接続：ネットワークを介して安全にリモートコンピュータにアクセスする仕組み。
WAF	Web Application Firewall：主にアプリケーション層の通信の不正や異常を検知・防御するソリューション。製品により IDS・IPS がカバーする範囲が重複している場合もある。
アタックパス	コンピュータシステムやネットワークにおいて、攻撃者が潜在的に侵入し、目標にアクセスするための経路や手順。
コンテナ	アプリケーションやサービスを実行するための独立した環境を提供する技術。
サーバーレス	自社でのサーバー構築・管理などを必要とせず、サーバーレス提供会社の基盤を用いプログラムを実行できる仕組み。

シャドークラウド	企業が使用許可をしていない、あるいは従業員が利用していることを企業側が把握できていないクラウドサービス。
バージョン管理ツール	ソフトウェア開発やファイル管理において、ファイルの変更履歴やバージョンを管理するためのツール。
フェールオーバー	システムやサービスが予期せず停止した場合に、別の冗長なシステムやバックアップシステムに自動的に切り替わること。
ブルートフォースアタック	暗号や認証メカニズムに対する攻撃手法の一つ。全ての可能性を網羅的に試行し、正しいパスワードや鍵を見つけ出す攻撃手法。
ペネトレーションテスト	対象システムに外部からの侵入を試みることによって脆弱性を発見するセキュリティテスト手法。
ベンダーロックイン	特定企業の製品・サービスに依存しており、他社の製品・サービスへの切り替えが困難になっている状況。
ポートスキャン	ネットワーク上のコンピュータやサーバーに対して、利用可能なネットワークポートを探索するための活動。
2025 年の壁	経済産業省が DX レポートにおいて提示したキーワード。企業が DX の取り組みを十分に行わなかった場合、2025 年以降に大きな経済損失が発生し、国際競争力を失うという課題を表す言葉。
2 要素認証	アカウントのセキュリティを強化するための認証手法。2 つの要素を用いてユーザーを認証する仕組み。
4P 分析	セキュリティ対策を 4 つの側面（People, Process, Products, Partners）から分析する手法。