情報セキュリティマネージャーが知っておくべき クラウドセキュリティと社内普及

佐古 伸晃

株式会社野村総合研究所

品質監理本部

情報セキュリティ部

2023年2月17日

NRI

Share the Next Values!

01 はじめに

02 クラウドセキュリティ

03 NRIにおける社内普及の取組

04 まとめ

自己紹介

■野村総合研究所(NRI)　情報セキュリティ部　佐古伸晃(SAKO Nobuaki)

- 経歴：金融・通信系インフラエンジニア→セールス・サービス企画→セキュリティ
- 職務：オフィスセキュリティ担当グループマネージャー
  - 社内OA系セキュリティ（社内システム・メール・インターネット・プロキシ）
  - 社内NWセキュリティ（社内LAN・無線）
  - 物理セキュリティ（端末・拠点・入退館）
  - 委託先セキュリティ
  - クラウドセキュリティ（社内からのクラウドサービス利用）
- ➢ クラウドサービス・クラウドネイティブ関連技術をいかに安全に使うか
  - 共通ガイドライン：IaaS / PaaS / SaaS 全般
  - 個別ガイドライン：AWS / Azure / Google Cloud (GCP) / OCI / Alibaba Cloud 向けの詳細版
  - Docker / Kubernetes、バージョン管理(GitHubなど)
- ➢ 発表内容はNRIでの取り組みであり、汎用的ではないかもしれませんが、何かのお役に立てたら幸いです

01 はじめに

02 クラウドセキュリティ

03 NRIにおける社内普及の取組

04 まとめ

そもそもセキュリティとは

■セキュリティ【security】

- 個人の安全、建物・施設の防犯、国家の安全保証、財産の担保・有価証券など、価値ある資産を守ること
- 情報を第三者からの侵入、攻撃、漏洩、改竄といった不正利用から阻止し、機密性や安全性を保持すること

■ISO/IEC 27002 ISMS(情報セキュリティマネジメントシステム) での定義

- 情報セキュリティ(Information Security)とは、情報の以下を維持すること(基本の三特性)
  - 機密性 (Confidentiality)　：許可されたものだけがアクセスできること、盗聴されないこと
  - 完全性 (Integrity)　：正しい状態で保持されていること、改竄されないこと
  - 可用性 (Availability)　：いつでも安全にアクセスできること、万一に備えバックアップすること
- 更に、情報に以下のような特性を含めることができること(追加の四特性)
  - 真正性 (Authenticity)　：対象が本当にその人・ものであること、認証すること
  - 責任追跡性 (Accountability)　：起きたことや原因を追跡できること、ロギングすること
  - 否認防止 (Non-Repudiation)　：後からなかったことにはできないこと、署名などで保護すること
  - 信頼性 (Reliability)　：安定して期待される役割を果たすこと、冗長化すること

脅威とは

■セキュリティは、次の三要素が存在する場合に必要になる

- 守るべき資産
- それを脅かす脅威
- 脅威が突いてくる脆弱性
  - ➢ Information Technology(IT) 企業・システム・エンジニアが扱い、守るべき資産は、情報である

■「脅威」とは？

- **リスクを発生させる要因のこと。**（情報セキュリティ用語辞典）
- 脅威にはおよそ心理学，生態学，国際関係の三つの側面がある。まず心理学的には，個人の心理的な安定や統合をおびやかすような人や物，あるいは状態が存在することをいう。たとえば，親の愛情を失う，もしくは失うのではないか，という子どもの不安や〈おびえ〉などは，脅威の一例である。脅威は外在的な事象から生まれることが多いが，〈現実〉の脅威と〈知覚された〉脅威とを区別して考えねばならない。現実に存在する脅威が，つねに正確に知覚されるとは限らないからである。（世界大百科事典 第２版）
  - ➢ 脅威を想定し、対策を取って、リスクコントロールをする必要がある

情報セキュリティマネージャーが知っておくべきクラウドセキュリティと社内普及

IPAの「情報セキュリティ10大脅威 2023」

■2022年に発生したセキュリティ事故や攻撃の状況などから脅威を選出し、投票により順位付け

- 個人では、10位に「ワンクリック請求等の不当請求による金銭被害」が2018年以来のランクイン、他は同じ傾向
- 組織では、10位に「犯罪のビジネス化（アンダーグラウンドサービス）」が2018年以来のランクイン、他は同じ傾向

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐取	**1位**	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	**2位**	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	**4位**	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	**5位**	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによるスマートフォン利用者への被害	**6位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	**7位**	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの個人情報の窃取	**8位**	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの不正ログイン	**9位**	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の不当請求による金銭被害	**10位**	犯罪のビジネス化（アンダーグラウンドサービス）	圏外
9位	インターネットバンキングの不正利用	**圏外**	予期せぬIT基盤の障害に伴う業務停止	9位

➢ 前回調査時、技術者300人の内83％がクラウドの設定ミスに関連するデータ侵害に対して脆弱であることを懸念

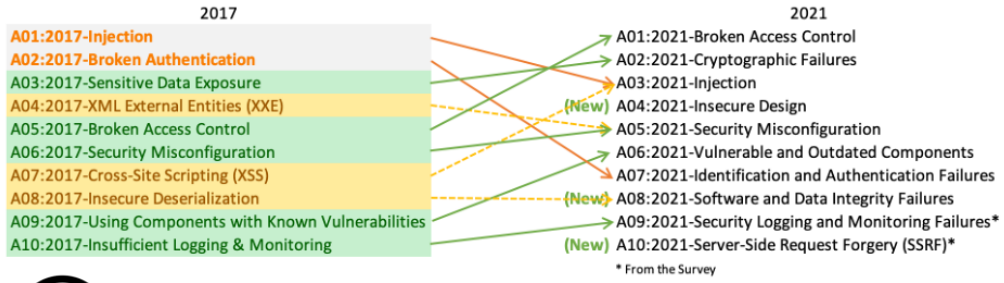
出典：情報セキュリティ10大脅威 2023 | IPA

OWASPの「OWASP Top 10」

■ Open Web Application Security Project（OWASP）が公開する脆弱性上位10項目

- 個別の脆弱性から大きな枠組みへ観点が変化（システム構築の方法・手段が多様化し抽象化）
- コンポーネントの活用に伴ったリスクの変化（クラウドのアクセス設定ミス、Log4Jライブラリ脆弱性）
- 構造の複雑化で増えるサーバサイドリクエストフォージェリ（マイクロサービス化で内部通信が多い）
- ➢ 脅威は毎年変化するので、常に脅威のトレンドを意識して対策を検討する必要がある

OWASP TOP 10＜2017＞		OWASP TOP 10＜2021＞		前回順位
A01	インジェクション	A01	アクセス制御の不備	5位
A02	認証の不備	A02	不適切な暗号化	3位
A03	機微な情報の露出	A03	インジェクション	1位
A04	XML外部エンティティ参照（XXE）	A04	安全が確認されない不安な設計	NEW
A05	アクセス制御の不備	A05	不適切なセキュリティ設計	6位
A06	不適切なセキュリティ設定	A06	脆弱で古いコンポーネント	9位
A07	クロスサイトスクリプティング（XSS）	A07	識別と認証の不備	2位
A08	安全でないデシアライゼーション	A08	ソフトウェアとデータの整合性の不備	NEW
A09	既知の脆弱性であるコンポーネントの使用	A09	セキュリティログとモニタリングの不備	10位
A10	不十分なロギングとモニタリング	A10	サーバサイドリクエストフォージェリ（SSRF）	NEW



OWASP®

https://owasp.org/www-project-top-ten/

出典：OWASP TOP10から知る脆弱性トレンドと対応 | UBsecure

脆弱性があることを知る

■CVE(共通脆弱性識別子)

- MITRE社が管理する一般公開されているセキュリティ脆弱性のリスト
- 世界中のITベンダー、セキュリティ企業、リサーチ組織がCVE採番機関(CNA)として登録、報告

➢ このリストや通知情報から、自組織の利用するプロダクトに該当する脆弱性を特定、対策を検討

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2022-23307	502			2022-01-18	2022-07-25	9.0	None	Remote	Low	???	Complete	Complete	Complete
CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists.														
2	CVE-2022-23305	89		Sql	2022-01-18	2022-07-25	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to be inserted are converters from PatternLayout. The message converter, %m, is likely to always be included. This allows attackers to manipulate the SQL by entering crafted strings into input fields or headers of an application that are logged allowing unintended SQL queries to be executed. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default. Beginning in version 2.0-beta8, the JDBCAppender was re-introduced with proper support for parameterized SQL queries and further customization over the columns written to in logs. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.														
3	CVE-2022-23302	502		Exec Code	2022-01-18	2022-07-25	6.0	None	Remote	Medium	???	Partial	Partial	Partial
JMSSink in all versions of Log4j 1.x is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration or if the configuration references an LDAP service the attacker has access to. The attacker can provide a TopicConnectionFactoryBindingName configuration causing JMSSink to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-4104. Note this issue only affects Log4j 1.x when specifically configured to use JMSSink, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.														
4	CVE-2021-44832	20		Exec Code	2021-12-28	2022-07-25	8.5	None	Remote	Medium	???	Complete	Complete	Complete
Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.														
5	CVE-2021-44228	502		Exec Code	2021-12-10	2022-07-22	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.														

出典：MITRE | CVE Details

CSAの「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」

■ Cloud Security Alliance（CSA）が数年に 1 回公開しているクラウドの11の脅威

- クラウドプロバイダ起因のランキングが下がり続け、利用者起因のものが増えている
- システムとして堅牢なクラウドは、人間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）

➢ クラウドそのものへの懸念は少なくなってきているため、現在のCSAはクラウド技術の実装により焦点を当てる

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

出典：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 | CSA Japan

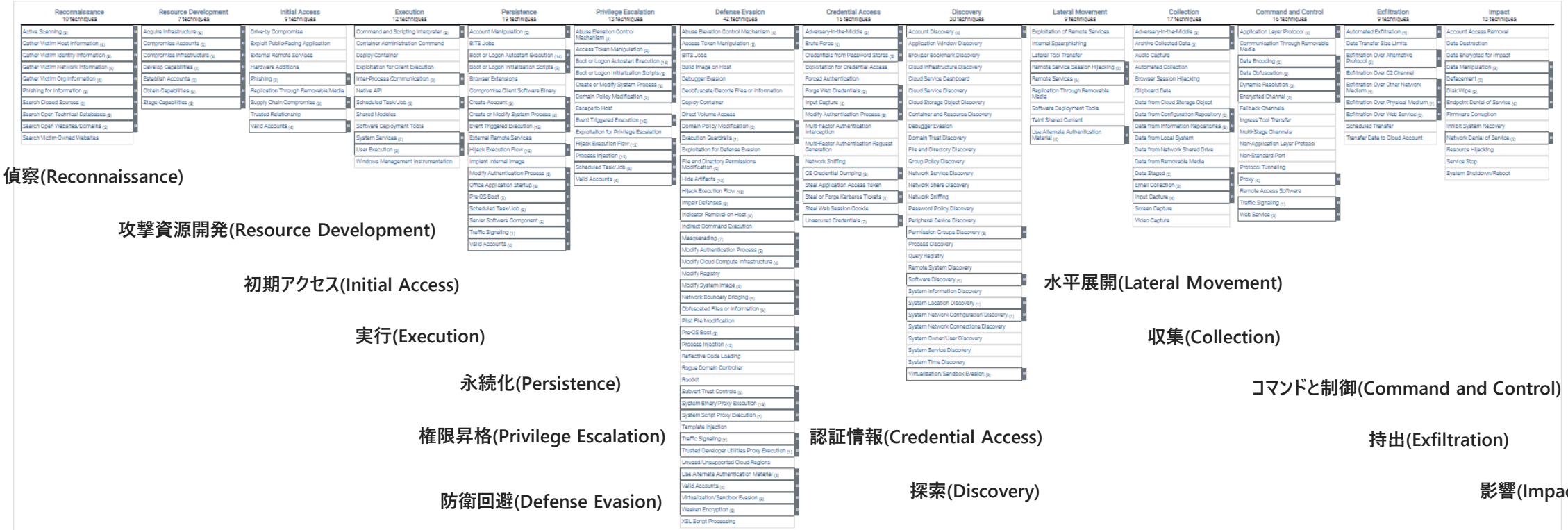
情報セキュリティマネージャーが知っておくべきクラウドセキュリティと社内普及

MITREの「MITRE ATT&CK®」

■ MITRE ATT&CK®(マイター・アタック: Adversarial Tactics, Techniques, and Common Knowledge)

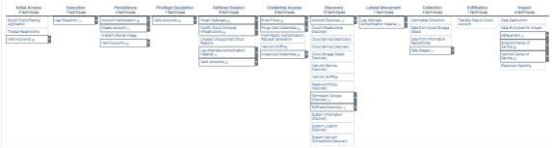
- MITRE社の管理する、現実の観測に基づく、敵対戦術とテクニック(脅威)のナレッジベース
- 偵察、初期アクセス、実行、永続化、権限昇格、探索など14プロセスで、どのような事が行われるかパターン化

➢ 敵対者の戦術とテクニックを知ることで、どのような脅威に対策をとるか想定し、具体的な対策に落とし込む



出典：MITRE ATT&CK | MITRE

MITRE ATT&CK IaaS Matrix (公式IaaS抜粋版)



初期アクセス(Initial Access)
- 公開アプリケーションの悪用
- 信頼関係のある組織の悪用
- クラウドアカウントの窃取

実行(Execution)
- ユーザーの誤操作誘発

永続化(Persistence)
- アカウントの操作、作成
- マシンイメージへの埋め込み
- クラウドアカウントの窃取

権限昇格(Privilege Escalation)
- クラウドアカウントの窃取

防衛回避(Defense Evasion)
- FWの無効化、ログの消去
- クラウドインフラの変更
- 未使用リージョンの利用
- 代替認証情報の利用
- クラウドアカウントの窃取

認証情報(Credential Access)
- ブルートフォース
- Web認証情報の偽造
- 多要素認証リクエストの発行
- ネットワークフィッシング
- 保護されていない認証情報

探索(Discovery)
- クラウドアカウントの探索
- クラウドインフラ、サービス、オブジェクトストレージ、ネットワークの検出
- ネットワークスニッフィング
- ソフトウェアの特定
- 管理コンソールへのアクセス
- 管理用アクセス経路の特定
- パスワードポリシー、権限の特定

水平展開(Lateral Movement)
- 代替認証情報の利用

収集(Collection)
- 自動収集
- リポジトリデータの窃取
- オブジェクトストレージの窃取
- ステージング環境へのコピー

持出(Exfiltration)
- 他アカウントへデータ移送

影響(Impact)
- データの破壊
- データの暗号化（ランサム）
- データの改ざん
- エンドポイントサービスの拒否
- ネットワークサービスの拒否
- リソースの不正利用

➢ 攻撃者はアカウントをなんとか窃取しようとする

出典：IaaS Matrix | MITRE ATT&CK®

クラウドセキュリティの考え方

■オンプレミスとクラウドでも、守るべき資産(情報)は変わらない。

■その管理主体・アクセス経路・外部接続点の違いから、脅威と脆弱性は異なってくる。

- オンプレミス
  - 利用者が管理し、物理的に閉じたネットワークでアクセスが限定され、外部接続点は専任チームで統制されることが多い。
  - 物理ネットワーク内にいる者はなりすましが困難なため、脅威ではない信頼された存在として扱われてきた。
- クラウド
  - プロバイダが管理し、世界中どこからでもアクセスでき、利用者の権限・設定次第で外部接続点はフルオープンになる。
  - クラウド環境では、インターネット上にいるモノを物理的に信頼できる存在と証明するのは困難。

➢クラウドにおけるセキュリティの考え方・役割分担も自ずと変わってくる。

クラウドセキュリティの役割分担

■代表例：責任共有モデル

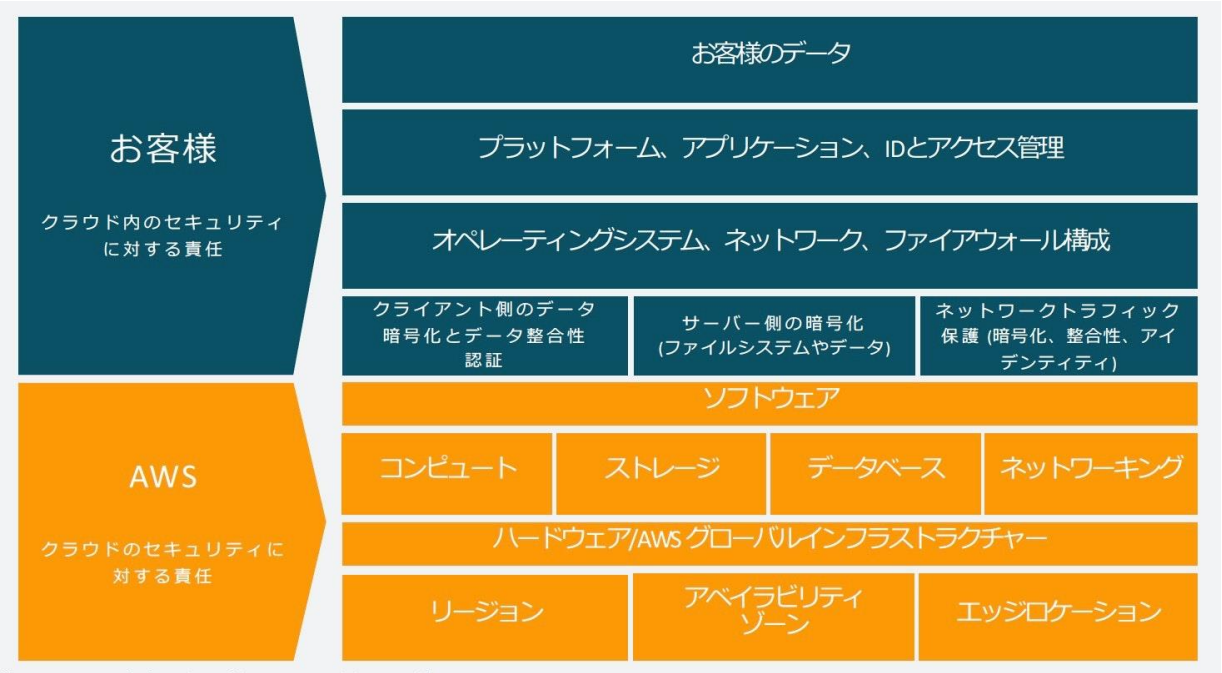
- 利用者の責任：クラウド ‘における’ セキュリティ(Security ‘in’ the cloud)
- プロバイダの責任：クラウド ‘の’ セキュリティ(Security ‘of’ the Cloud)

■クラウド利用の基本的な考え方

- セキュリティだけではなく、予算・調達・契約・精算・ガバナンスなどその他の分野にも及ぶ

■多くのクラウドサービスでも同じモデルを採用。

- 利用者側の責任は必ずある
- 自分の責任範囲を押さえる



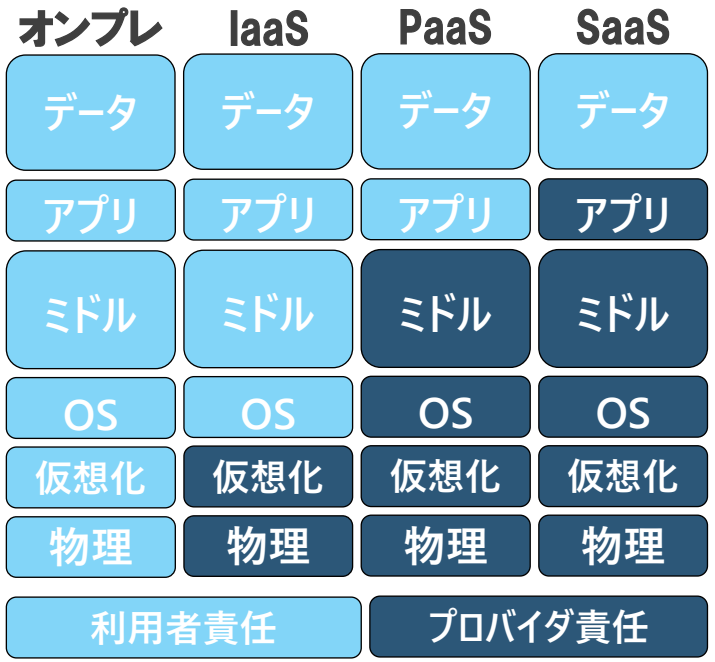
出典：Amazon Web Services ブログ 責任共有モデルとは何か、を改めて考える

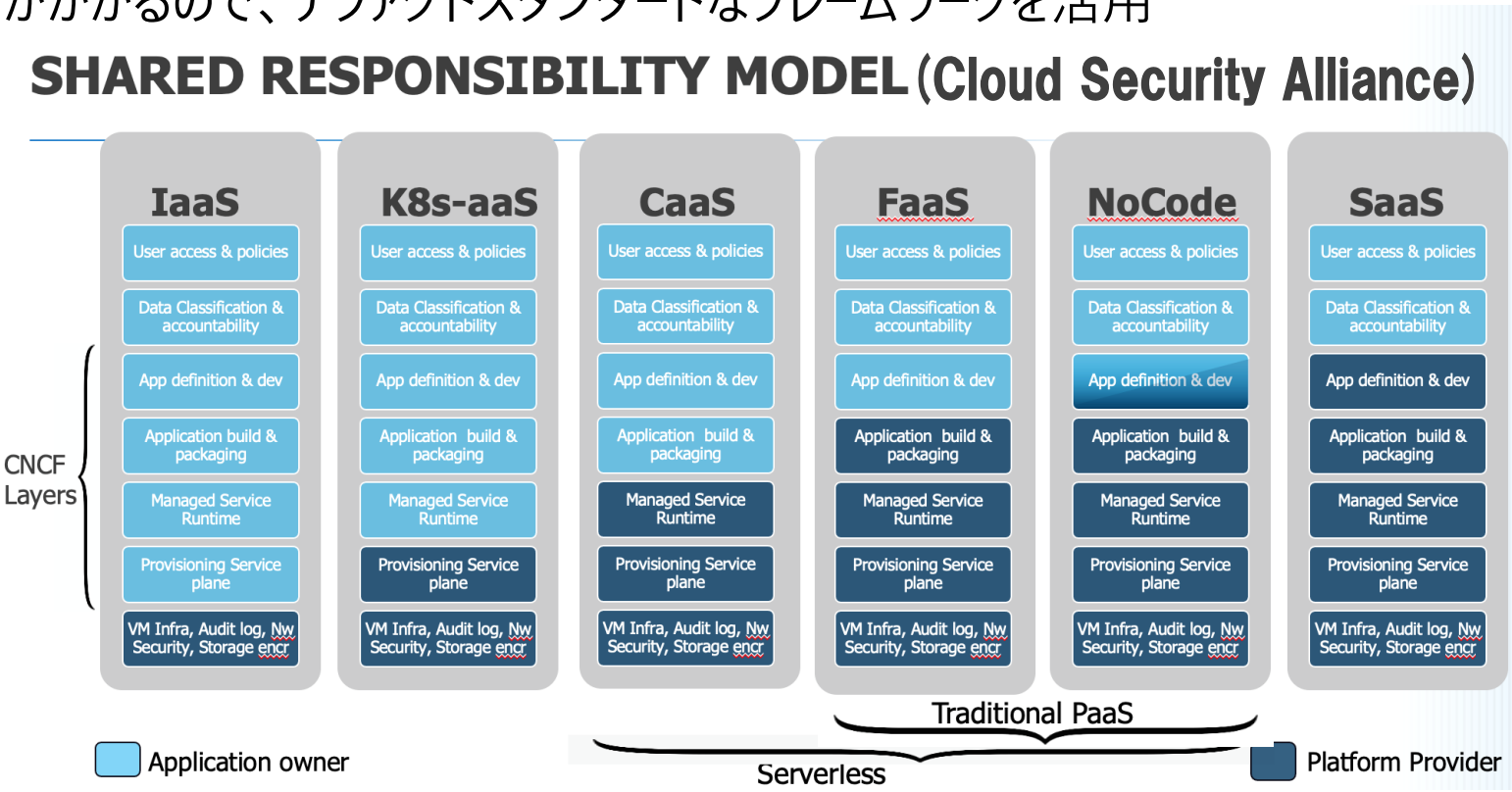
新たな責任共有モデル

■IaaS / PaaS / SaaS 以外の as-a-Service が増え、クラウドネイティブが担うレイヤーが細分化

- レイヤーごとにセキュリティ対策する必要があるが、レイヤーが複数に渡るため対策・役割分担が困難
  - ➢ 全てのレイヤーを網羅するのは労力がかかるので、デファクトスタンダードなフレームワークを活用

従来モデル
（NIST SP800-145）





出典：クラウドコンピューティングの進化と新たな責任共有モデル | CSA

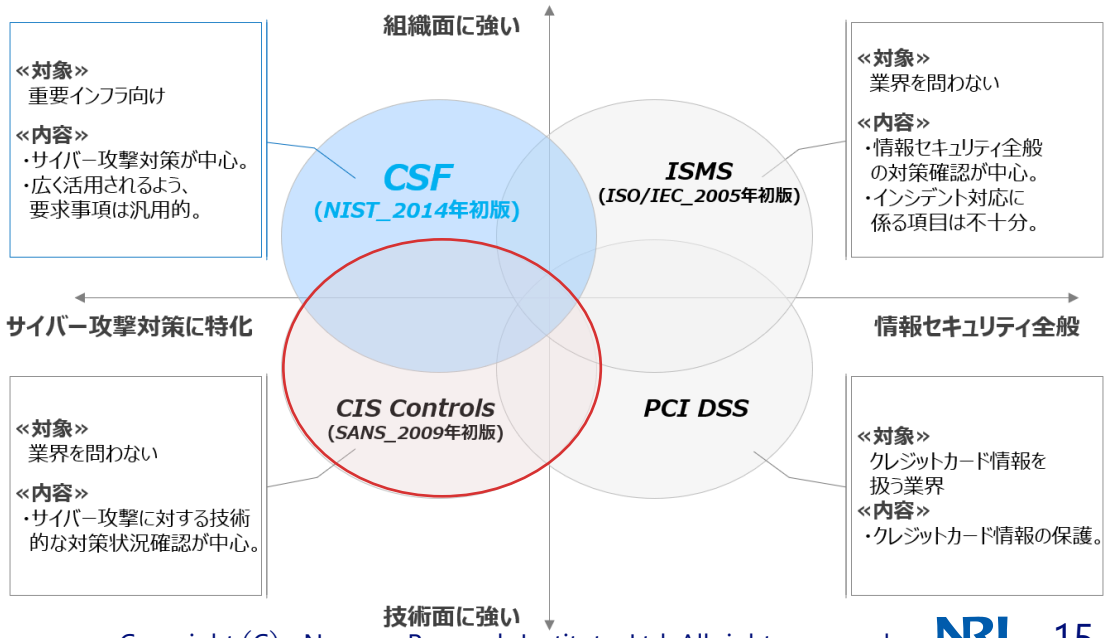
代表的なセキュリティフレームワーク

■デファクトスタンダードとなっているセキュリティフレームワークには以下のようなものがあり、それぞれサイバー攻撃対策・内部不正対策、組織面・技術面の四象限

- NIST CSF： 米国立標準研究所(NIST) 発行のCyber Security Framework(CSF)
- CIS Controls：米インターネットセキュリティセンター(CIS) 発行のセキュリティ管理策
- ISMS： JISQ27001(ISO/IEC27001) に基づいた情報セキュリティ管理の仕組み
- PCI DSS： クレジットカード業界セキュリティ団体(PCI SSC) 発行の対策基準

■クラウドサービス利用時のセキュリティ判断基準

➢ NRIでは、サイバー攻撃対策に特化し、業界を問わず、具体的な技術面での対策・設定に強みを持つ
CISの提供するリソースを活用



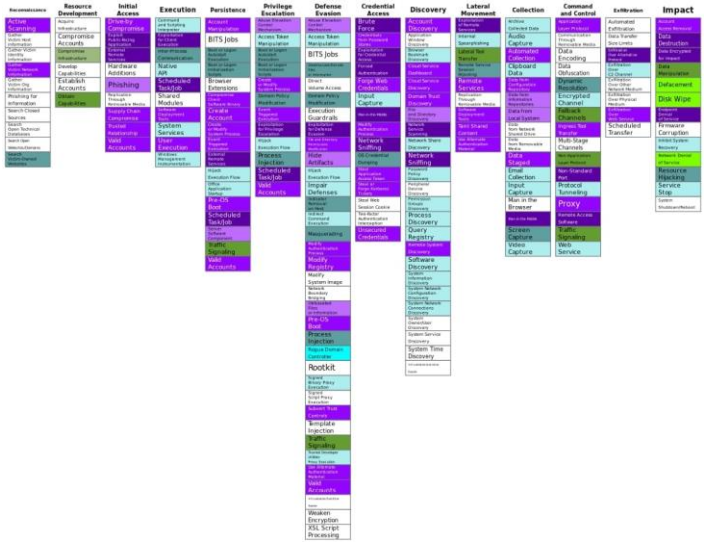
出典：NRIセキュア｜【解説】NIST サイバーセキュリティフレームワークの実践的な使い方

(参考)セキュリティフレームワークやナレッジの利用例

■セキュリティフレームワークやナレッジを活用したセキュリティ対策の評価・分析手法

	ベースラインアプローチ	リスクベースアプローチ		
	ハンズオフ（机上評価）		ハンズオン（実機評価）	
評価対象	組織・情報システム全体		特定の情報システム	
評価に用いる基準や手法の例	•CIS Controls •NIST CSF •ISO/IEC 27001, 27002 等	•MITRE ATT&CK	•レッドチーム演習	•ペネトレーションテスト
概要	基準が定義する対策項目に関して、情報セキュリティ担当者へのヒアリングを実施し評価	導入済みのツール、監視ログ、情報セキュリティ担当者へのヒアリング結果等を元に、攻撃に対する防御能力を評価	システムの脆弱性だけではなく、人・物理のそれぞれの側面からセキュリティ耐性を評価	システムの脆弱性のみを対象として、侵入テストを行い評価
特徴	1.短期間で評価可能 2.情報システムに侵入する必要がない 3.リスクの洗い出しが困難 4.組織全体の対策状況を把握	1.短期間で評価可能 2.情報システムに侵入する必要がない 3.即効性のある対策案が得られる 4.防御可能なおおよその範囲を把握	1.準備や評価に時間がかかる 2.情報システムに侵入する必要がある 3.即効性のある対策案が得られる 4.ピンポイントの評価だが、詳細かつ正確な結果を得られる	

出典：NRIセキュア | MITRE ATT&CKを用いたサイバー攻撃対策の評価サービス



出典：Microsoft | MITRE ATT&CK® と組み込み Azure security control とのマッピングを発表

■セキュリティベンチマーク／コントロールでの対策／方針と、セキュリティフレームワークとのマッピング

IM-1: 一元化された ID と認証システムを使用する

CIS Controls v8 ID(s)	NIST SP 800-53 r4 ID(s)	PCI-DSS ID(s) v3.2.1
3.12, 13.4, 4.4	AC-4, SC-2, SC-7	1.1, 1.2, 1.3

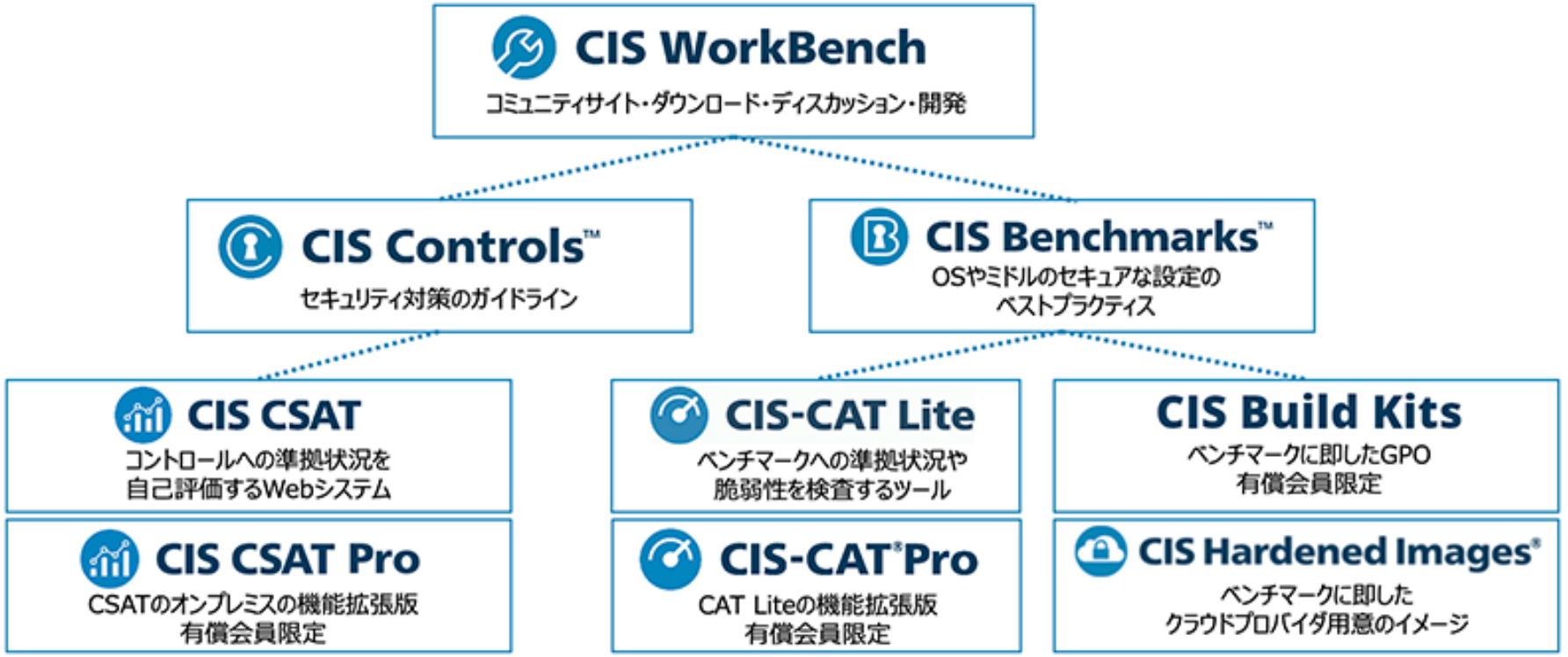
セキュリティの原則: 一元化された ID と認証システムを使用して、クラウドリソースと非クラウドリソースに対する組織の ID と認証を管理します。

出典：Microsoft | Azure セキュリティベンチマーク

Center for Internet Security(CIS)の提供リソース

■米国の政府・学術機関・企業がインターネット・セキュリティ標準化に取り組む団体

- CIS Controls：サイバー攻撃に焦点を当てた具体的技術対策を示す18種類のフレームワーク
- 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



出典：LAC I CIS Controls v8日本語版をリリース

「クラウドのセキュリティ」は信頼できるのか？

プロバイダ責任

■クラウドプロバイダの責任は果たされているか？

- 責任を共有するには、利用するクラウドサービスが信頼できるか、コンプライアンスの観点で判断する
- 企業のセキュリティポリシーに合致するか、独自の質問票（セキュリティチェックシート）を用意するケースもあるが、クラウドサービス事業者と一問一答をやり取りするのは双方ともに非常に労力・時間がかかる

■コンプライアンスに関しては、以下のような第三者基準の認証取得状況を確認

- ISO27001：情報セキュリティマネジメントシステム(ISMS)
- ISO27017：クラウドベースの情報セキュリティの統制
- ISO27018：クラウド上での個人データ保護
- SOC1：財務報告に係る内部統制報告書
- SOC2：セキュリティや可用性などの内部統制報告書
- HIPPA、PCI-DSS、FISCなど：特定業界ごとの統制基準
- ISMAP、FedRAMP / SP800-53、NIST SP800-171、GDPR、マイナンバー法など：国ごとの統制基準

➢ 取得状況に応じて、クラウド事業者のセキュリティ対策が実施済みと判断し、アセスメントを一部/全部省略可

➢ ISO27001の場合は一部（共通ガイドラインチェックリストにマッピング）

➢ ISO27017、SOC2、ISMAPの場合は全部省略可

「クラウドにおけるセキュリティ」をどう対策するか？

利用者責任

■ CIS Benchmarks は、非常に広範囲な製品・サービスを対象とするドキュメント群

- 各クラウドプロバイダ、Docker/Kubernetes、OS/ミドルなどをカバー
- 以下の観点では対策が手薄なので、追加対策を実施
  - コンテナイメージの署名、レジストリの定期・依存関係先スキャン、CI/CDパイプライン保護、バージョン管理

カテゴリ	対象の製品・サービス(例)
Cloud Provider	Alibaba Cloud, Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud, OCI
Desktops & Web Browsers	Apple Desktop OSX, Apple Safari Browser, Google Chrome, Microsoft Internet Explorer, Microsoft Windows Desktop 10/XP/NT, Mozilla Firefox Browser, Opera Browser, Mobile Devices, Zoom
Mobile Devices	Apple Mobile Platform iOS, Google Mobile Platform
Network Devices	Agnostic Print Devices, Check Point Firewall, Cisco Firewall Devices, Cisco Routers/Switches IOS, Cisco Wireless LAN Controller, Juniper Routers/Switches JunOS, Palo Alto Networks
Server Software - Operating Systems	Amazon Linux, CentOS, Debian Linux Server, IBM AIX Server, IBM Z series, Microsoft Windows Server, Novell Netware, Oracle Linux, Oracle Solaris Server, Red Hat Linux Server, Slackware Linux Server, SUSE Linux Enterprise Server, Ubuntu LTS Server
Server Software - Other	Apache HTTP Server, Apache Tomcat Server, BIND DNS Server, FreeRADIUS, Microsoft IIS Server, IBM DB2 Server, Microsoft Exchange, Microsoft SharePoint Server, Microsoft SQL Server, MIT Kerberos, MySQL Database Server, Novell eDirectory, OpenLDAP Server, Oracle Database Server, PostgreSQL Database Server, Sybase Database Server
Security Metrics	Quick Start Guide, Security Metrics
Virtualization Platforms	Agnostic VM Server, Docker, Kubernetes, VMware Server, Xen Server
Other	Microsoft Access, Microsoft Excel, Microsoft Office, Microsoft Outlook , Microsoft PowerPoint, Microsoft Word

出典：CIS Benchmarks | CIS

CIS Cloud Provider Benchmarks

■ 主要なパブリッククラウドのIaaS中心の対策

- ①IAM、②ネットワーク、③コンピュート、④ロギング／モニタリング、⑤セキュリティ／コンプライアンスの５分類
- 各クラウドベンダごとに利用できる機能、設定の細かさ・複雑さが異なるが、考え方は共通
- 上記をベースに、各クラウドのベストプラクティスや、自組織のセキュリティ要件を加えてガイドライン化
- コンテナ、サーバレス、SaaS機能は独自色が強いので個別対応

		AWS	Azure	Google Cloud	OCI	Alibaba Cloud
Version		1.5.0	1.5.0	2.0.0	1.2.0	1.0.0
最終更新		2022/8/12	2022/8/23	2022/12/31	2022/4/13	2020/12/11
① IAM		21	33	18	13	16
② Networking		5	7	10	8	5
③ Compute	VM	-	6	12	-	6
	Storage	10	15	2	6	9
	Database	-	25	25	-	9
	Serverless	-	11	3	-	-
④ Logging / Monitoring		11+16	18	16	16	23
⑤ Security / Compliance		-	23+9	-	2	8
合計		63	147	84	45	76

出典：CIS Benchmarks | CIS

CIS Cloud Provider Benchmarks での対策

■ 主要なパブリッククラウドのIaaS中心の対策

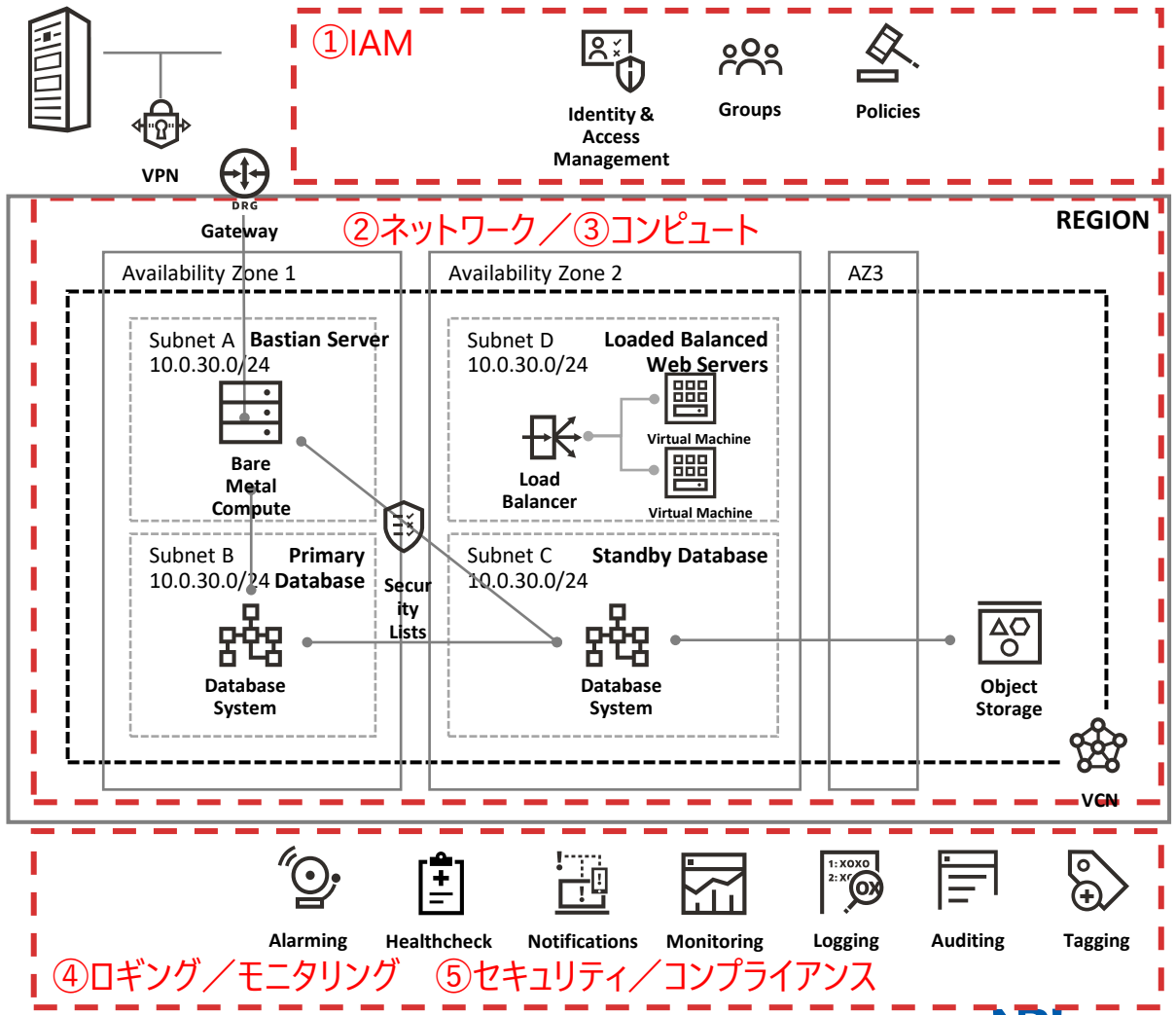
① IAM(Identity and Access Management)
- 最小権限、パスワードポリシー、MFA、プリンシパル
- クレデンシャル、APIキー、rootユーザの利用制限

② ネットワーク
- 0.0.0.0/0からSSH/RDPを許可しない、from IP制限
- 許可されたソースのみに制限

③ コンピュート
- パブリックバケット作成制限
- 暗号化、CMK・BYOK、ローテーション

④ ロギング／モニタリング
- ログ記録、保管、監視、作成・変更・削除の通知
- 可視化、スコアリング、ダッシュボード

⑤ セキュリティ／コンプライアンス
- 自社セキュリティサービスの有効化



(参考)CIS Benchmarks 本文

推奨事項

プロファイル

説明

根拠

監査方法
コンソール

監査方法
コマンドライン

修復方法

参考URL

CIS Control
との対応

1.7 Eliminate use of the 'root' user for administrative and daily tasks (Automated)

Profile Applicability:

- Level 1

Description:

With the creation of an AWS account, a 'root user' is created that cannot be disabled or deleted. That user has unrestricted access to and control over all resources in the AWS account. It is highly recommended that the use of this account be avoided for everyday tasks.

Rationale:

The 'root user' has unrestricted access to and control over all account resources. Use of it is inconsistent with the principles of least privilege and separation of duties, and can lead to unnecessary harm due to error or account compromise.

Audit:

From Console:

1. Login to the AWS Management Console at `https://console.aws.amazon.com/iam/`
2. In the left pane, click `Credential Report`
3. Click on `Download Report`
4. Open of Save the file locally
5. Locate the `<root account>` under the user column
6. Review `password_last_used, access_key_1_last_used_date, access_key_2_last_used_date` to determine when the 'root user' was last used.

From Command Line:
Run the following CLI commands to provide a credential report for determining the last time the 'root user' was used:

```
aws iam generate-credential-report

aws iam get-credential-report --query 'Content' --output text | base64 -d |
cut -d, -f1,5,11,16 | grep -B1 '<root_account>'
```

Review `password_last_used, access_key_1_last_used_date, access_key_2_last_used_date` to determine when the *root user* was last used.

28 | Page

Note: There are a few conditions under which the use of the 'root' user account is required. Please see the reference links for all of the tasks that require use of the 'root' user.

Remediation:

If you find that the 'root' user account is being used for daily activity to include administrative tasks that do not require the 'root' user:

1. Change the 'root' user password.
2. Deactivate or delete any access keys associate with the 'root' user.

**Remember, anyone who has 'root' user credentials for your AWS account has unrestricted access to and control of all the resources in your account, including billing information.

References:

1. https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
2. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html
3. https://docs.aws.amazon.com/general/latest/gr/aws_tasks-that-require-root.html

Additional Information:

The 'root' user for us-gov cloud regions is not enabled by default. However, on request to AWS support, they can enable the 'root' user and grant access only through access-keys (CLI, API methods) for us-gov cloud region. If the 'root' user for us-gov cloud regions is enabled, this recommendation is applicable.

Monitoring usage of the 'root' user can be accomplished by implementing recommendation 3.3 Ensure a log metric filter and alarm exist for usage of the 'root' user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or	●	●	●

29 | Page

*MITRE ATT&CKとのマッピング情報は別紙一覧表(Excel)に記載

出典：CIS Benchmarks

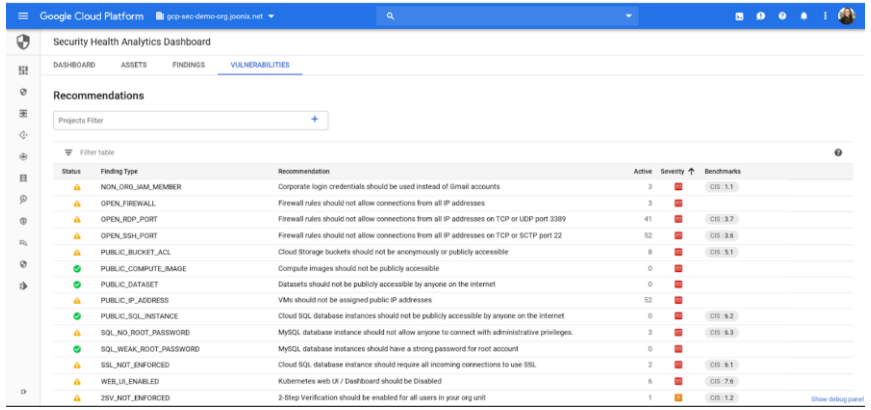
(参考)パブリッククラウドのCISベンチマーク準拠チェックサービス

AWS Security Hub

- AWS独自、CIS v1.2.0/1.4.0、PCI DSSなどに対応

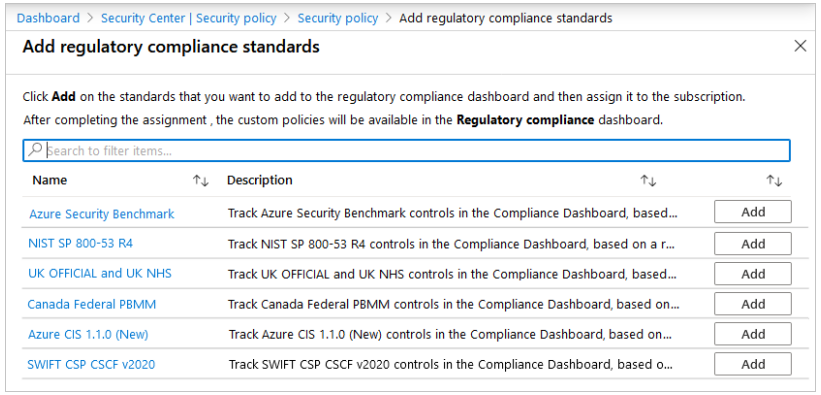
Google Cloud Security Health Analytics (Security Command Center)

- GCP CIS v1.1.0、PCI DSS、NIST SP 800-53などに対応



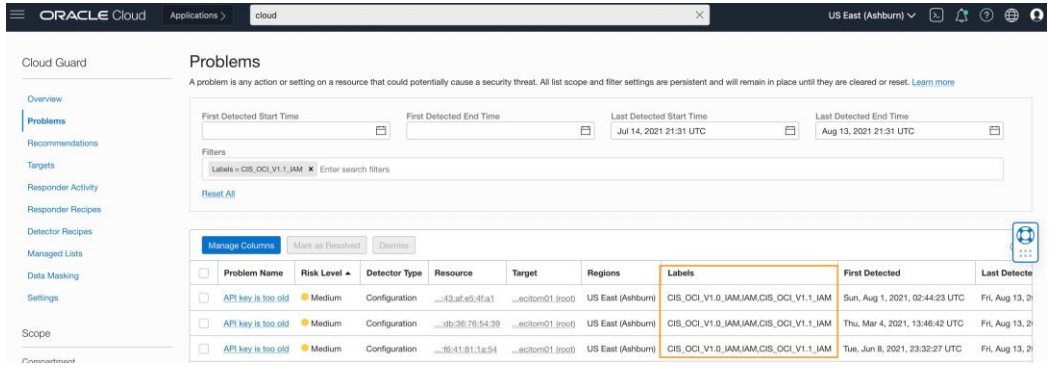
Microsoft Defender for Cloud(旧Security Center)

- Azure独自、CIS v1.1.0、NIST SP 800-53などに対応



OCI Cloud Guard

- OCI独自、CIS v1.1.0などに対応



01 はじめに

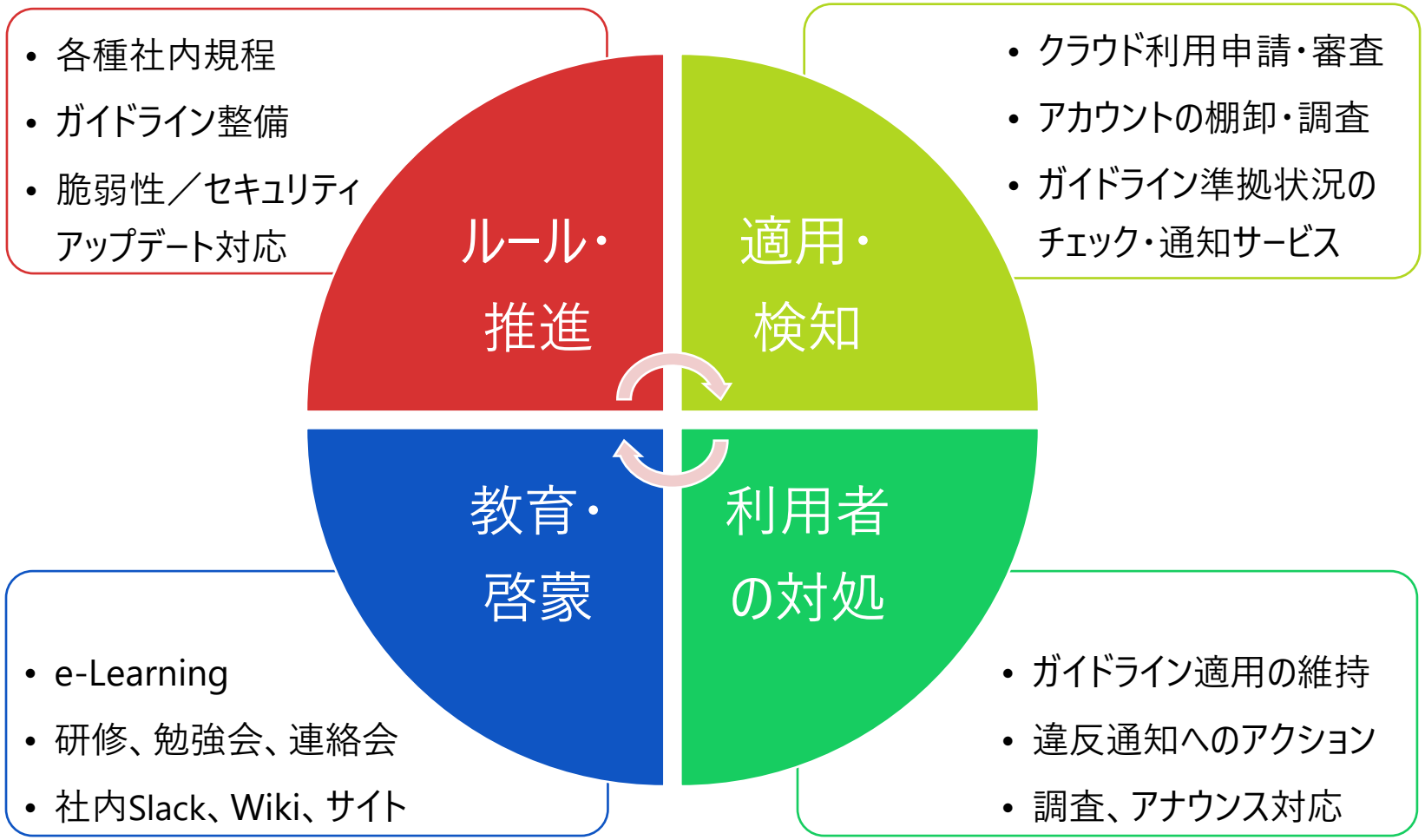
02 クラウドセキュリティ

03 NRIにおける社内普及の取組

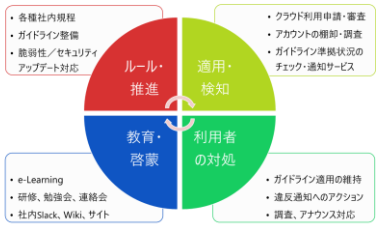
04 まとめ

NRIにおけるクラウドセキュリティの取り組み

■ルール・推進、適用・検知、利用者の対処、教育・啓蒙を通じ、継続的な対策を社内普及



ルール・推進：脆弱性／セキュリティアップデート対応

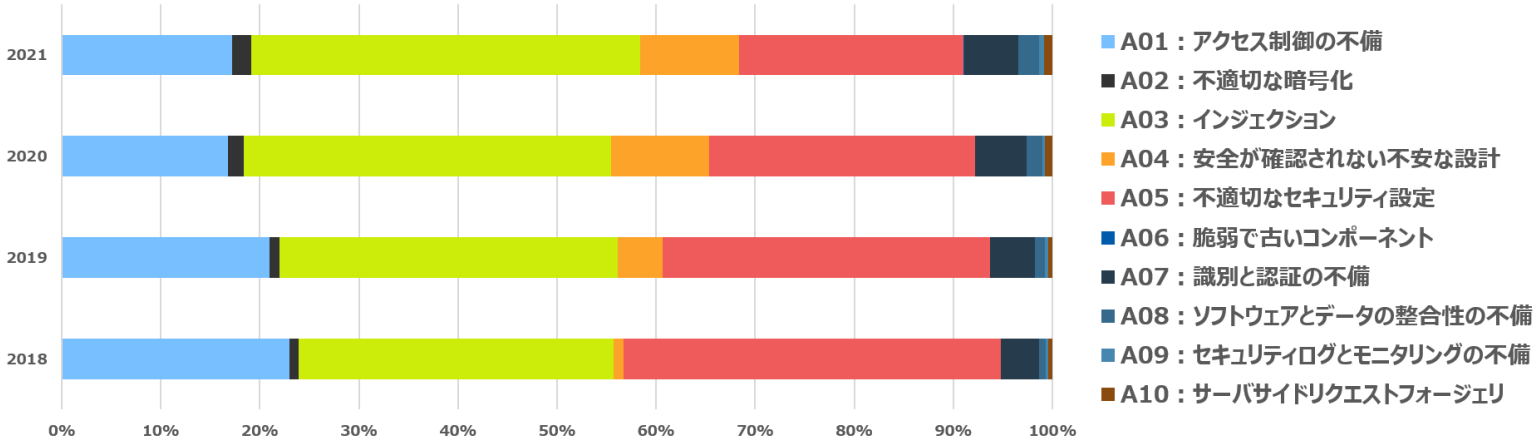


■JPCERTコーディネーションセンターのJVN(Japan Vulnerability Notes)の活用

- 日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供
- 「情報セキュリティ早期警戒パートナーシップ」制度に基づいて報告された脆弱性情報や、CERT/CCなど海外機関と連携した脆弱性情報を公表。自組織の利用するプロダクトに該当する脆弱性を特定、対策を検討。
- 日本では「アクセス制御の不備」、「インジェクション」、「不適切なセキュリティ設定」の3カテゴリが大半

➢ 日本での傾向も加味し、重点的に対策する脆弱性を把握

JVNでの報告データ（2018-2021）とOWASP Top 10のマッピング




JVN Japan Vulnerability Notes

Japan Vulnerability Notes JP 一覧

最新12ヶ月 | 2021年 | 2020年 | 2019年 | 2018年 | 2017年 | 2016年 | 2015年 | 2014年 | 2013

2022年

2022/12/15 JVN#96321933:
電子入札コアシステムにおける複数の脆弱性

2022/12/13 JVN#60211811:
Redmine におけるクロスサイトスクリプティングの脆弱性

2022/11/25 JVN#87895771:
サイボウズ リモートサービスにおけるリソース枯渇に至る脆弱性

2022/11/25 JVN#53682526:
baserCMS における複数のクロスサイトスクリプティングの脆弱性

2022/11/24 JVN#29657972:
TP-Link RE300 V1 の tdpServer における入力データの不適切な処理に関する脆弱性

2022/11/21 JVN#26044739:
Typora における JavaScript コードの無効化処理が不十分な問題

2022/11/18 JVN#13927745:
WordPress 用プラグイン WordPress Popular Posts における外部入力の不適切な使用に関する脆弱性

2022/11/16 JVN#24659622:
RICOH IPSiO SP 4210 におけるクロスサイトスクリプティングの脆弱性

2022/11/16 JVN#37014768:
Movable Type における複数の脆弱性

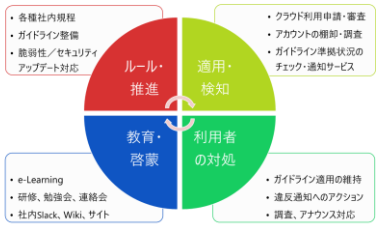
https://jvn.jp/jp/index.html

➢その他、複数のソースから情報収集、必要に応じて社内連絡

出典：OWASP TOP10から知る脆弱性トレンドと対応 | UBsecure

情報セキュリティマネージャーが知っておくべきクラウドセキュリティと社内普及

ルール・推進：各種社内規程、ガイドライン整備



■各レイヤーごとに規程・ガイドラインを整備、管理する仕組み・サービスと連携、第三者基準を参照

レイヤー	規程・ガイドライン	仕組み・サービス	
運営	本番ｱｸｾｽ、ﾌﾟﾛｼﾞｪｸﾄｾｷｭﾘﾃｨﾙｰﾙ	情報ｾｷｭﾘﾃｨ障害管理 CSIRT	ISO、個人情報保護法など
データ	機密情報・個人情報、委託先管理		
	Webｻｲﾄ運営・ｺﾝﾃﾝﾂ・SNS		
アプリ	Webアプリケーション	Webアプリケーション診断	FISC、PCIDSS、NIST OWASPなど
	スマートフォンアプリケーション		
ミドル	インターネット公開サーバ	プラットフォーム診断	CIS Benchmark、CIS Control MITRE ATT&CKなど
	バージョン管理		
	データベース		
OS	OS		
仮想化	Docker/Kubernetes	CWPP	
物理	クラウド	CSPM	
端末	社内ｼｽﾃﾑ利用、機器・NW管理	EDR	参照するベンチマークや基準、ナレッジ

不正アクセス予防

CI/CD

Dev Sec Ops

NRIのクラウドガイドラインの考え方

■各サービスごとに設定できる対策と想定される脅威は様々だが、大別して７つを設定

対策の大項目	想定される脅威
1. アイデンティティによる認証・認可	不正アクセス、アカウント乗っ取り、過大権限による誤操作
2. ネットワークによるアクセス制御・境界線防御	インターネットからのログイン施行、侵入・攻撃、横移動
3. 暗号化による保存データ・通信経路の保護	情報漏洩、盗聴、改ざん
4. 多重化・冗長化構成による可用性の向上	HW故障、SW障害、広域障害
5. バックアップ取得によるデータロストへの備え	運用ミス、データセンター被災、ランサムウェア
6. ロギング・モニタリングによる記録・監視	攻撃、不正行動、疑わしい挙動、戻し忘れ
7. 分析・レポーティングによる可視化・監査	攻撃、障害、設定不備の見落とし

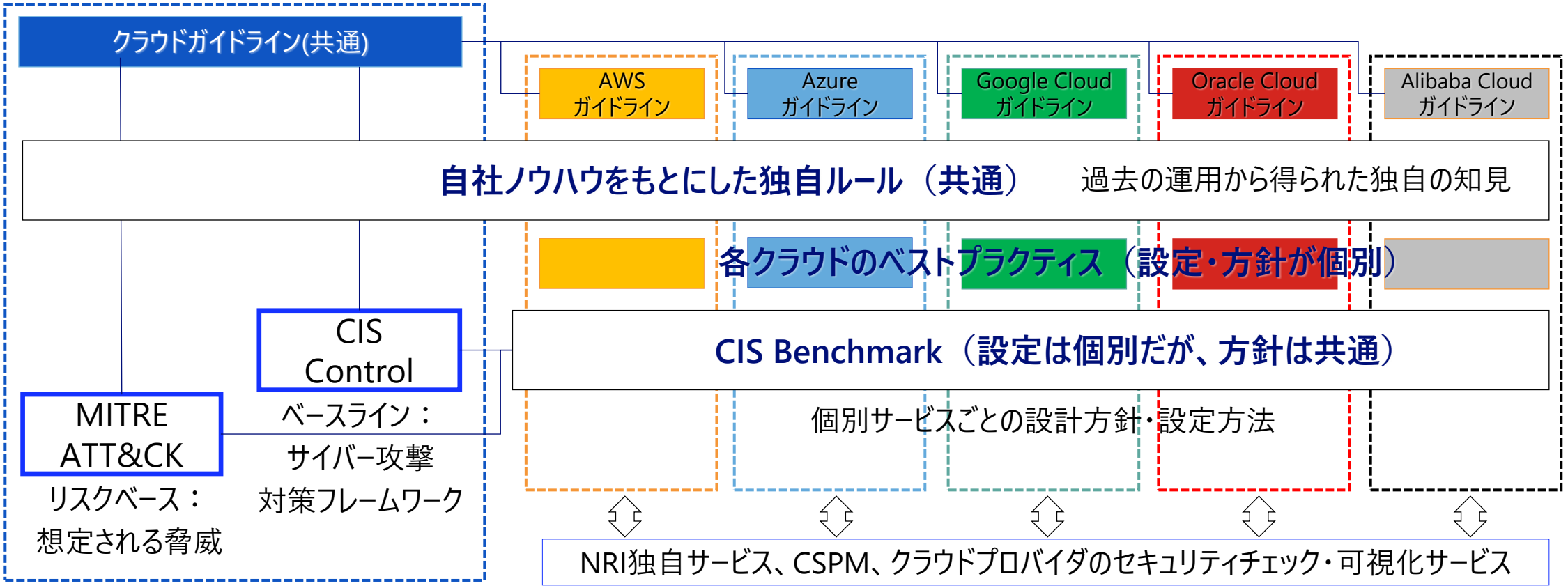
■ セキュリティ以外の関連する観点も追加し、より包括的なガイドラインを作成

8. 統制レベルに応じたアカウント分割	コンプライアンス違反、本番環境とその他環境の混同
9. 予算設定、利用金額超過アラート	使い過ぎ、無駄なリソース利用、不正利用

NRIにおけるクラウドセキュリティガイドラインの構成

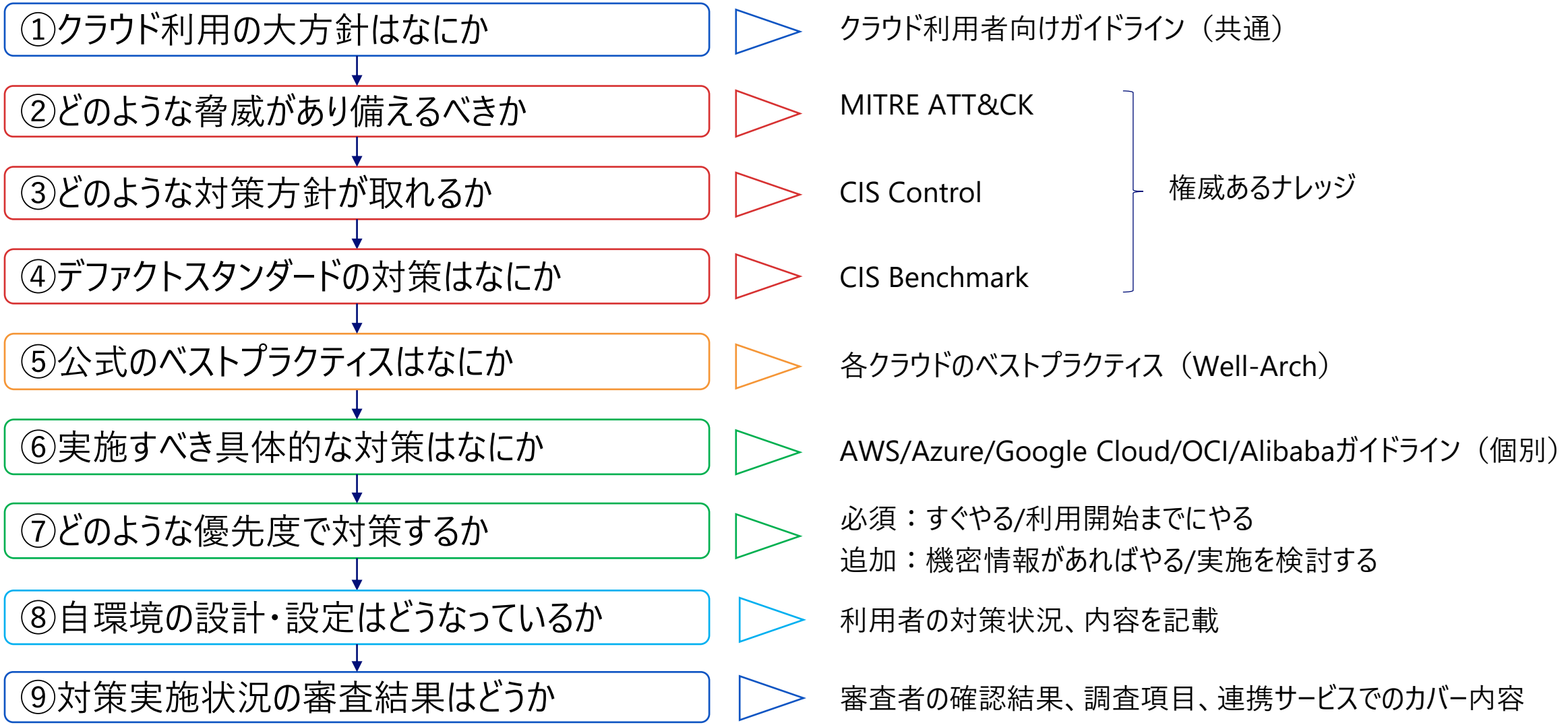
■独自ルール／ベストプラクティス／CIS Benchmarkの三階建て、メガクラウドは個別詳細版あり

- 権威あるスタンダードとして、MITRE ATT&CK および CIS Control ともマッピング



各クラウドサービスのアカウントを監視、違反があれば利用者へ通知

ガイドラインの利用フロー



ガイドラインの内容

■共通ガイドライン、権威あるナレッジ、ベストプラクティス、個別ガイドラインを横串でマッピング

- 各ルール、ベストプラクティス間の関連性を把握することで、根拠と具体的な対策が明確になる
- 外部リソースを活用することで、セキュリティの傾向変化・アップデートへの追従が容易となる
- 共通的な考え方で対策するため、ベンチマークやベストプラクティスにない対応にも先手が打てる
  - ➢ 社内勉強会などで有識者と連携して現場レベルで調整のうえ、定期的に見直し・アップデートを実施

NRIのクラウド共通ガイドライン			MITRE ATT&CK			CIS		Well-Architected		NRIの個別ガイドライン				利用者
タイトル	本文	根拠	戦術	技術	緩和策	Control	Benchmark	分類	ベストプラクティス	サービス	対策	対策例	優先度	状況
ユーザアカウントの多要素認証	クラウド利用者はユーザアカウントに多要素認証(MFA)を設定しなければならない。	多要素認証であれば防げたインシデントが発生し、パスワード保護だけでは不十分であるとの認識が広まっている。	TA0001：初期アクセス 攻撃者はあなたのネットワークに入ろうとしています。	T1078：有効なアカウント 攻撃者は既存のアカウントの資格情報を取得し、悪用する可能性があります。	M1018：ユーザーアカウント管理 ユーザーアカウントに関連する作成、変更、使用、および権限を管理する。	6.3 外部に公開されているアプリケーションにMFAを要求する 6.4 リモートネットワークアクセスに対するMFAの必要性 6.5 管理者アクセスにMFAを必要とする	1.5 rootユーザアカウントでMFAを有効化する	アイデンティティ管理	強力なサインインメカニズムを使用する MFA サインインを強制するアクセス管理 (IAM) ポリシーを作成する	ポリシー	MFAの強制	ポリシーでMFA利用を強制し、リソースへのアクセスを制限する。	アカウント開設後すぐやる	対策例実施済／予定 代替策実施済／予定 対象外

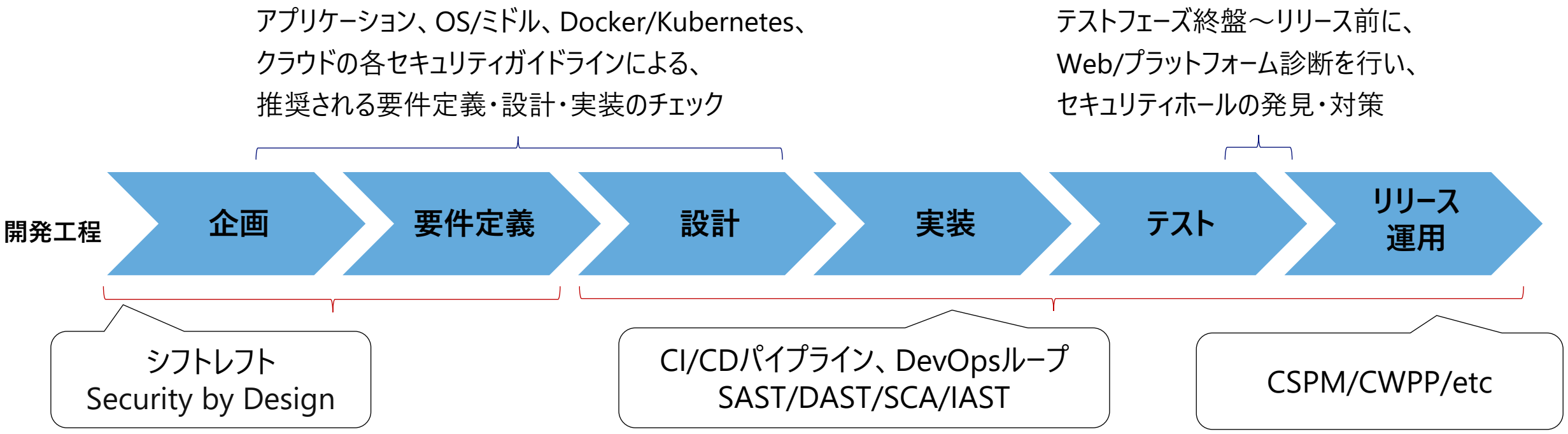
NRIのクラウドガイドラインでの記載(イメージ)

- ➢ 対策が実施できない場合は、代替策がリスク低減策として有効か、対象外とする理由は妥当か、を確認

ガイドラインが活用される工程は限定的

■従来のガイドラインを用いた品質担保を実施する運用では、カバーされる工程が少ない

- 企画の最上流、実装～テスト中盤、リリース運用では、ドキュメントであるガイドラインが活用されにくい

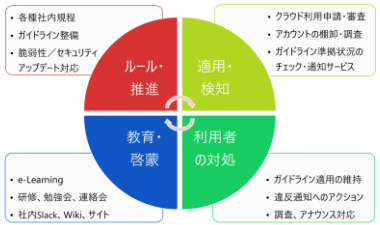


- シフトレフト、CI/CD・DevSecOps、継続監視・通知、セキュリティの可視化・自動化が必要

➢ 全ての工程にセキュリティの概念・機能を取り込む

情報セキュリティマネージャーが知っておくべきクラウドセキュリティと社内普及

適用・検知：利用申請・審査、棚卸・調査



■クラウド利用申請・審査

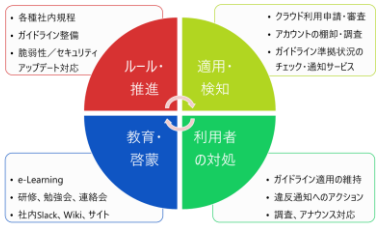
- クラウドサービスを利用する際は、申請して審査を受ける
- 各種ガイドラインに沿って審査を行い、不備があれば是正を促す
  - ガイドラインの項目と異なる対処であっても、代替コントロール策としてリスク低減できるか、判断が必要となる

■アカウントの棚卸・調査

- 申請漏れ、廃止漏れのチェックのため、クラウドサービスのアカウント棚卸を実施
- 利用者の申告ベースだと実態が把握しきれない場合があり、利用料支払い実績などからも追う
  - 地道な活動の繰り返し

情報セキュリティマネージャーが知っておくべきクラウドセキュリティと社内普及

適用・検知：準拠状況のチェック・通知サービス

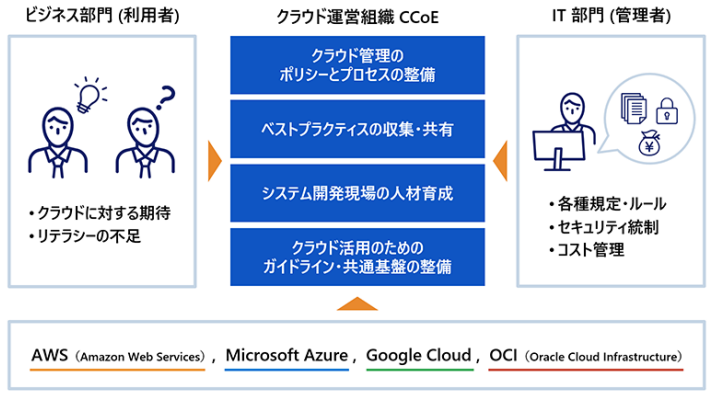


■ガイドライン準拠状況のチェック・通知サービス

- ガイドラインの準拠状況は、継続的なチェックを行わないと適切な状態か把握できない
- パブリッククラウドのセキュリティ設定検査サービスや、CSPM（Cloud Security Posture Management : クラウドセキュリティ態勢管理）でもチェック可能
- 独自ルールは作り込みが必要、対応スタンダードが最新でなかったり、通知内容が日本語対応していなかったり、利用者のネクストアクションに繋がらない場合も。→ 継続チェック・通知サービスを独自実装
  - ➢ 設計ポリシーやユーザ棚卸など、人の判断が必要な方針・運営は、利用者の役割・定常業務として残る

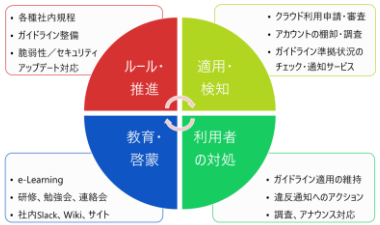
■連携先組織

- CCoE：クラウド活用を推進する横断組織。利用者との間を埋める役割も。
- CSIRT：セキュリティ事故対応チーム。インシデントが発生した場合に連携。
- セキュリティ担当：各本部・部署でのセキュリティ対策推進担当。
- クラウド技術部門、アカウント管理運営チーム、品質監理、経理など



出典：クラウド活用推進組織（CCoE）| NRI

利用者の対応



■ガイドライン適用の維持

- 審査は完璧でも、その後の構築・テストや、運用中に変更や戻し忘れが発生する
- 追加費用がかかるなどの理由で自力でやろうとするが、業務に忙殺されがち

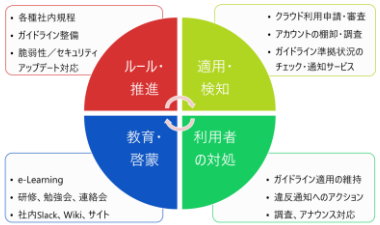
■違反通知へのアクション

- 通知が来ていても、日常的に来ていると見なくなる

➢調査、アナウンス対応

- ガイドライン準拠状況の変化がないか、インシデントに繋がりやすい項目の調査を実施、注意喚起アナウンス
  - 人間の認証に対して多要素認証を設定しているか　※サービスの認証は設定不可の場合も
  - 受け渡し可能な認証情報（アクセスキーなど）を作成していないか　※システム間連携で必要な場合も
  - インターネットAny（0.0.0.0/0）にSSHやRDPなどのポートが開いていないか　※テストや切り分けなどで全開放しがち
  - オブジェクトストレージなどの公開設定は適切か

教育・啓蒙：現場の理解を得るための情報発信



■e-Learning

- プライバシーマーク確認の一環で、全役職員向けに個人情報保護および情報セキュリティ対策として実施
- 設問に、世間的に注目されたインシデントや、クラウド関連の基本動作・対策を盛り込む

■研修、勉強会、連絡会

- 情報セキュリティ部門として現場に伝えたいことを情報発信する場
- 社内のクラウド関連勉強会で、ガイドライン改定内容の事前共有やフィードバックを行う

■社内Slack、Wiki、サイト

- Slack：素早く気軽な情報共有、コミュニケーション用（フロー情報）
- Wiki：コミュニケーションで得られた知見をまとめて記載（ストック情報）
- サイト：公式な見解を文書・社内規程として掲載

非公式な個人の見解扱い
発信に対する心理的安全性の確保
現場との距離感を縮める

01 はじめに

02 クラウドセキュリティ

03 NRIにおける社内普及の取組

04 まとめ

まとめ

- プロバイダと利用者の責任範囲を把握し、外部リソースを活用する
  - プロバイダの「クラウドのセキュリティ」は、第三者認証の取得状況、ホワイトペーパーを確認
  - 利用者の「クラウドにおけるセキュリティ」は、公開ナレッジ、ベンチマーク、ベストプラクティスを活用

- 「クラウドにおけるセキュリティ」は共通する考え方で対処できることが多い
  - IAM・認証認可、ネットワーク保護、ロギング・モニタリングの３つが基本
  - 暗号化、多重化・冗長化、バックアップ、分析・レポーティング、アカウント分割、予算設定でより強固にする

- 全ての工程にセキュリティの概念・機能を取り込む
  - 初期段階からセキュリティを取り込む（シフトレフト：早い段階から相談を）
  - ツール・サービス活用により継続監視・改善を省力化・自動化
  - ルール・推進、適用・検知、利用者の対処、教育・啓蒙を通じ、継続的な対策を普及
  - ➢ 開発現場の理解を得るためには、情報発信が必須


Share the Next Values!