ICSCoE_TLP:WHITE/CLEAR

クラウドにおける脅威検知

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
中核人材プログラム 8期生 クラウドにおける脅威検知プロジェクトメンバー 一同
2025/07/31

改版履歴

版数	発行日	改定箇所	改定内容
第1版	2025/7/31		初版発行

本資料に関する注意事項

・本資料は、クラウドにおける脅威検知の仕組みを学ぶことを目的とした学習・検証プロジェクトの成果をまとめたものである。
・本資料の内容は、独立行政法人情報処理推進機構（IPA）および産業サイバーセキュリティセンター（ICSCoE）の公式見解を示すものではなく、プロジェクト参加者の個人的な見解に基づいている。
・記載内容には、技術的あるいは表現上の誤りが含まれている可能性がある。正確性・完全性について保証するものではない。
・本資料は、特定の組織、製品、サービス、規格などを推奨・非難する意図を含むものではない。
・記載の組織名、製品名、サービス名、規格名等は、各社・各団体の商標または登録商標である。
・引用または参考にした外部資料・Webサイトの内容は、本資料作成時点の情報に基づいており、提供者の都合により変更またはアクセス不能となる場合がある。
・本資料は予告なく内容を変更する場合がある。
・また、本資料の利用に起因するいかなる損害についても、作成者および監修者は責任を負わない。
・本資料の有効期限は、発行日から2年間(2027/07/31まで)とする。

検証結果に関する注意事項

本プロジェクトはクラウドにおける脅威検知の検証（p.18「３．検証結果」参照）をもとに考察を実施する。それらの検証結果における注意事項を下記に記載する。

【注意事項】

・検証に使用した攻撃シナリオは、実際のサイバー攻撃事例やセキュリティベンダー等が公表している想定攻撃を参考に構成している。(p.15の7つの事例)

・本資料の検証環境は、学習目的および検証の再現性を高めるため、実運用とは異なる構成や条件にカスタマイズされている部分がある。

・検証は、AWSおよびAzureの両クラウド環境において同様の構成・操作を可能な限り再現しながら進めたが、一部のシナリオはアカウント権限制約やサービスモデルの違いにより、片方の環境でのみ実施したものもある。

・振る舞い検知型の製品については、通常は「正常状態の学習」や「既知の悪性IPとの照合」に基づく検知を前提とする場合が多いが、本検証ではこれらの前提条件（学習期間・悪性IPの使用）を省略している。これは、振る舞い検知が常に機能するとは限らないという前提に立ち、実環境における運用リスクや限界を体感的に理解することを目的としている。

・検証結果の「〇」「×」については、各STEPの挙動に対してのアラート発生有無の結果を表しており、詳細分析の結果として各STEPの挙動をとらえるログを確認することができた場合などは、「×」としている。

検証スコープ

本プロジェクトでは、CSPM（Cloud Security Posture Management）や脆弱性スキャンといった予防的なセキュリティ対策ではなく、実際の攻撃行為や不審な挙動が発生した際に検知が可能かどうかという“事後的対応”の観点から、クラウド環境における脅威検知の有効性を検証した。

つまり、意図的に設定ミスや脆弱性を含むクラウド環境を構築し、その上で疑似的な攻撃（例：漏洩したIAM資格情報を用いた権限昇格や、不正なインスタンスメタデータサービスへのアクセス）を実施し、各種セキュリティ製品がどのようにアラートを発するかを確認するという手法を取った。

なお本検証では、WAF（Web Application Firewall）やEDR（Endpoint Detection and Response）など、オンプレミス環境でも導入される一般的なセキュリティ対策はあえて利用せず、そうした対策が未実装の状態でも、CWPP（Cloud Workload Protection Platform）に代表されるクラウド特有の脅威検知機能がどのような役割を果たせるのかに注目した。これにより、クラウド固有の検知技術が実運用においてどこまで有効に機能するのかを明らかにすることを目的としている。

本紙の対象読者

□ 職種・役割：
- 情報システム部門やセキュリティ部門に所属するエンジニア
- クラウドセキュリティに関心のあるインフラエンジニアやDevSecOps担当者
- クラウド環境における脅威検知の実務をこれから担おうとする担当者

□ スキルレベル：
- クラウド基盤（AWS、Azureなど）の基本的な利用経験がある
- セキュリティに関する基礎知識はあるが、「CWPP」「ランタイム検知」などの実践的な理解を深めたいと考えている

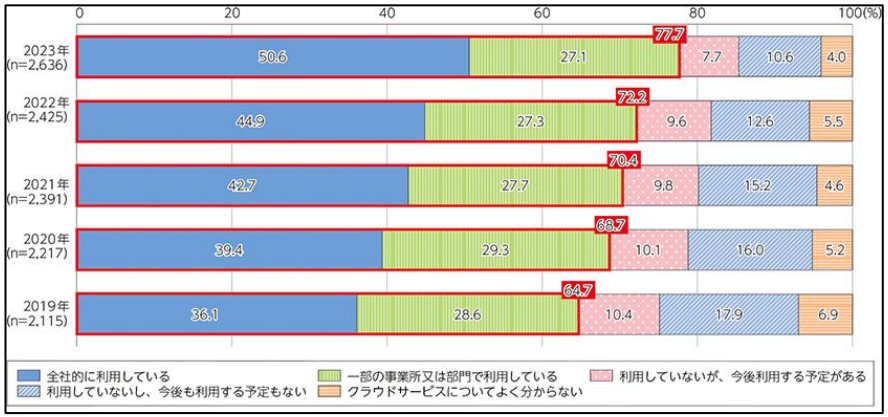
□ 目的・課題意識：
- クラウド環境での脅威検知の仕組みに対する共通認識が持てず、混乱や不明点を感じている
- 曖昧な用語やベンダーごとの差異に対する実態的な理解を求めている

目次

1. プロジェクト背景と目的

1）増加するクラウド利用とセキュリティインシデント

増加する クラウド利用



出典：「クラウドサービスの利用状況」令和6年通信利用動向調査（総務省）

- DX推進も背景に クラウドの活用率は右肩上がりで推移
- 2023年度には国内で**約78%の企業が**何らかの用途で**クラウドを活用**

増加する クラウドセキュリティインシデント

Q.1年以内にパブリッククラウドの利用に関連した**セキュリティインシデント**を**経験**したか？

2022:YES：27%
2023:YES：24%
2024:YES：61%

出典：「2024 CloudSecurity Report」(Check Point 社)

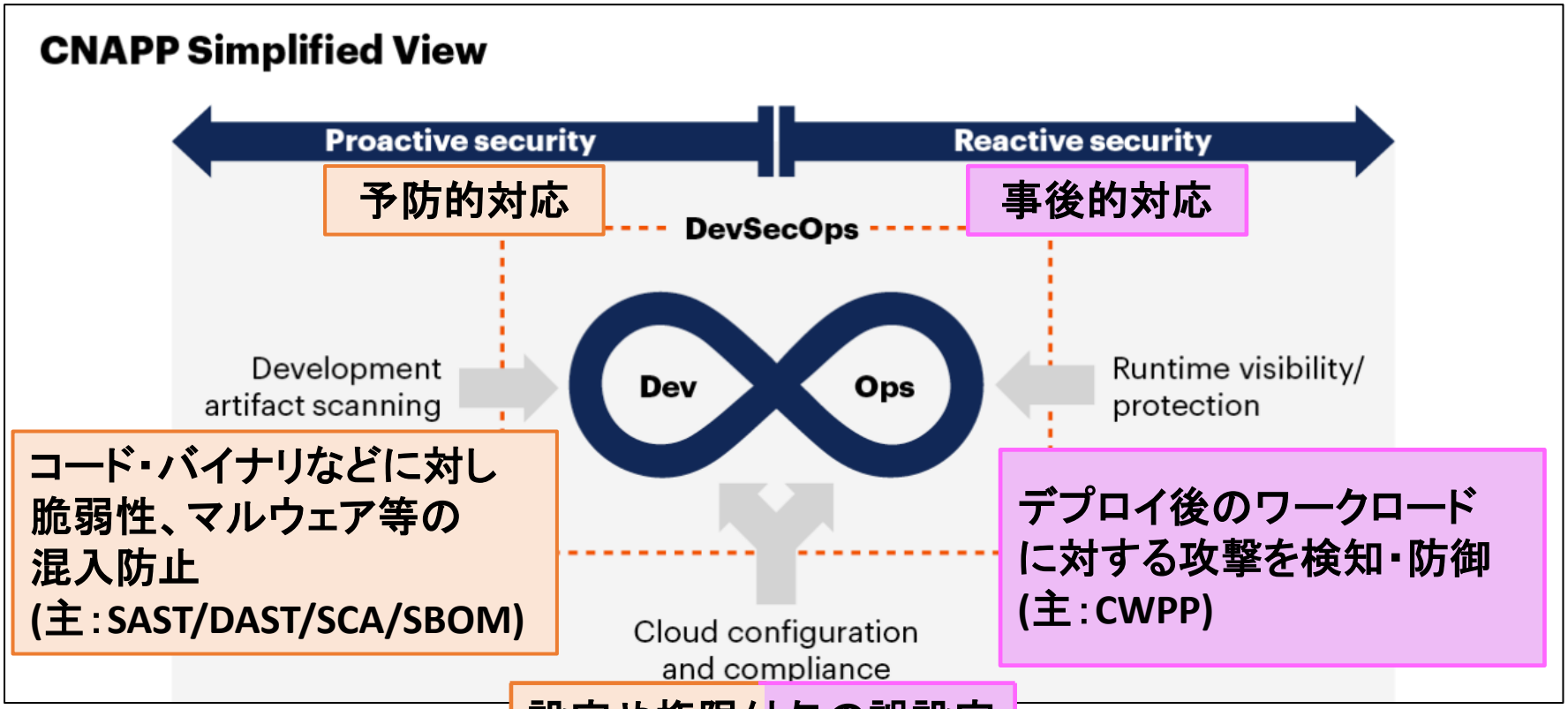
パブリッククラウドの利用に関連したセキュリティインシデントも増加傾向

Point

クラウドセキュリティ戦略はパブリッククラウドの移行・活用を進める組織にとって、重要な位置づけである

2）クラウドセキュリティ戦略におけるCWPPの役割

Gartnerは、クラウド特有の様々なセキュリティ課題に開発ライフサイクルを通して包括的かつ効率的に対応すべくCNAPP（Cloud-Native Application Protection Platform）を提唱



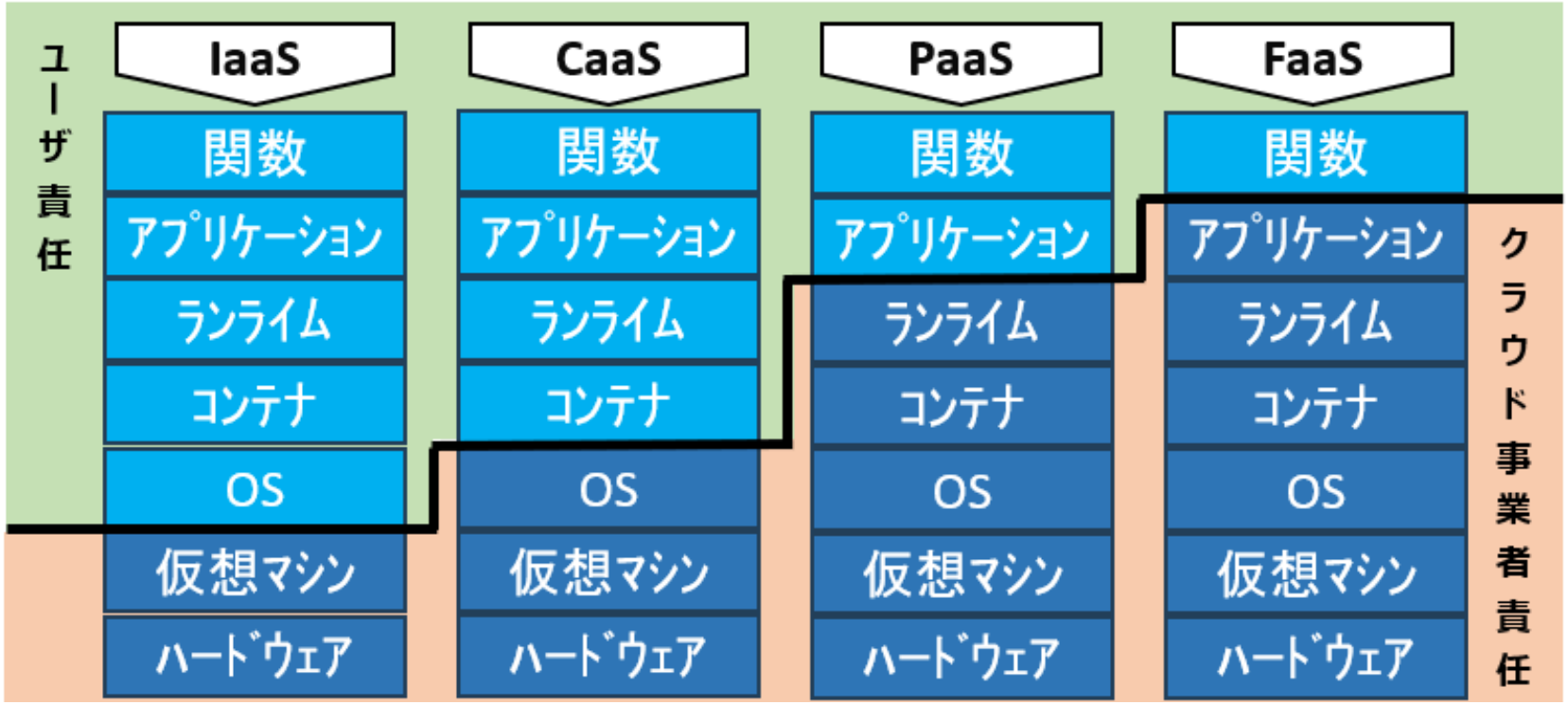
出典：Gartner

Point

事後的対応である**CWPP(Cloud Workload Protection Platform)は**、設定ミスを含む**脆弱性の悪用(脅威)を防御・検知する「最後の砦」**

3）CWPPの定義

■**GartnerによるCWPPの定義(2021 Gartner Market Guide for CWPP)**
ハイブリッド、マルチクラウド データセンター環境におけるサーバーワークロードを保護するワークロード中心のセキュリティ製品
→クラウド責任共有モデルのユーザ責任領域全体(緑部分)を保護するサービス・仕組み



4）ベンダーごとのCWPP機能の違い

Microsoft

・脆弱性の管理
・ネットワークセグメント化
・不変性
・整合性保護
・メモリ保護
・許可リスト
・侵入防止
・エンドポイントでの検出と対応
・マルウェア対策スキャン

https://www.microsoft.com/ja-jp/security/business/security-101/what-is-cwpp

PaloAlto

・脆弱性管理
・ホスト侵入検知/防止
・コンプライアンス管理
・イメージスキャン
・ラインタイム保護
・ワークロード振る舞い監視
・CI/CDパイプライン統合
・設定ミス
・WAAS/WAF

https://www.paloaltonetworks.com/cyberpedia/what-is-cwpp-cloud-workload-protection-platform

Crowdstrike

・脆弱性スキャン
・コンテナとKubernetesのセキュリティオーケストレーション
・ランタイム保護
・CI/CDパイプラインのセキュリティ
・セキュリティ体制とコンプライアンス
・ホワイトリスト
・クラウドネットワークセキュリティ
・可視性と発見
・侵入防止
・マイクロセグメンテーション
・アプリケーションセキュリティ

https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-workload-protection-platform-cwpp/

Wiz

・ランタイム保護
・リアルタイムの脅威検出とインシデント対応
・エージェントレススキャン
・脆弱性管理
・CI/CD統合
・コンプライアンス評価

https://www.wiz.io/ja-jp/academy/cloud-workload-protection-platforms-cwpp

Fortinet

・マルウェア対策スキャン
・脅威の検知と対応
・脆弱性管理
・可視化
・侵入防止
・アプリケーション制御
・システムの完全補償
・エクスプロイトの防止とメモリ保護

https://www.fortinet.com/jp/resources/cyberglossary/cwpp

Cloudflare

・強化、構成、脆弱性管理
・ネットワークファイアウォール、可視性、マイクロセグメンテーション
・システム整合性の保証
・アプリケーション制御と許可リスト
・エクスプロイト防止とメモリ保護
・サーバワークロードのエンドポイント検出と応答
・脆弱性シールドを備えたホストベースの侵入防止
・マルウェア対策スキャン

https://www.cloudflare.com/learning/cloud/what-is-cwpp/

Point

CWPPの定義がベンダによって異なっている

5）プロジェクトの目的

目的

CWPPの検証を通じて
クラウドにおける脅威と検知の仕組みを理解する

背景にある疑問

〇事後的対応としてのCWPPの必要性は？

〇クラウドサービスモデルごとの具体的な脅威やリスクはなにか？

〇IaaSに関しては、EDRを導入すれば十分なのでは？

〇ベンダーごとに定義が異なるが、結局なにをしてくれるの？

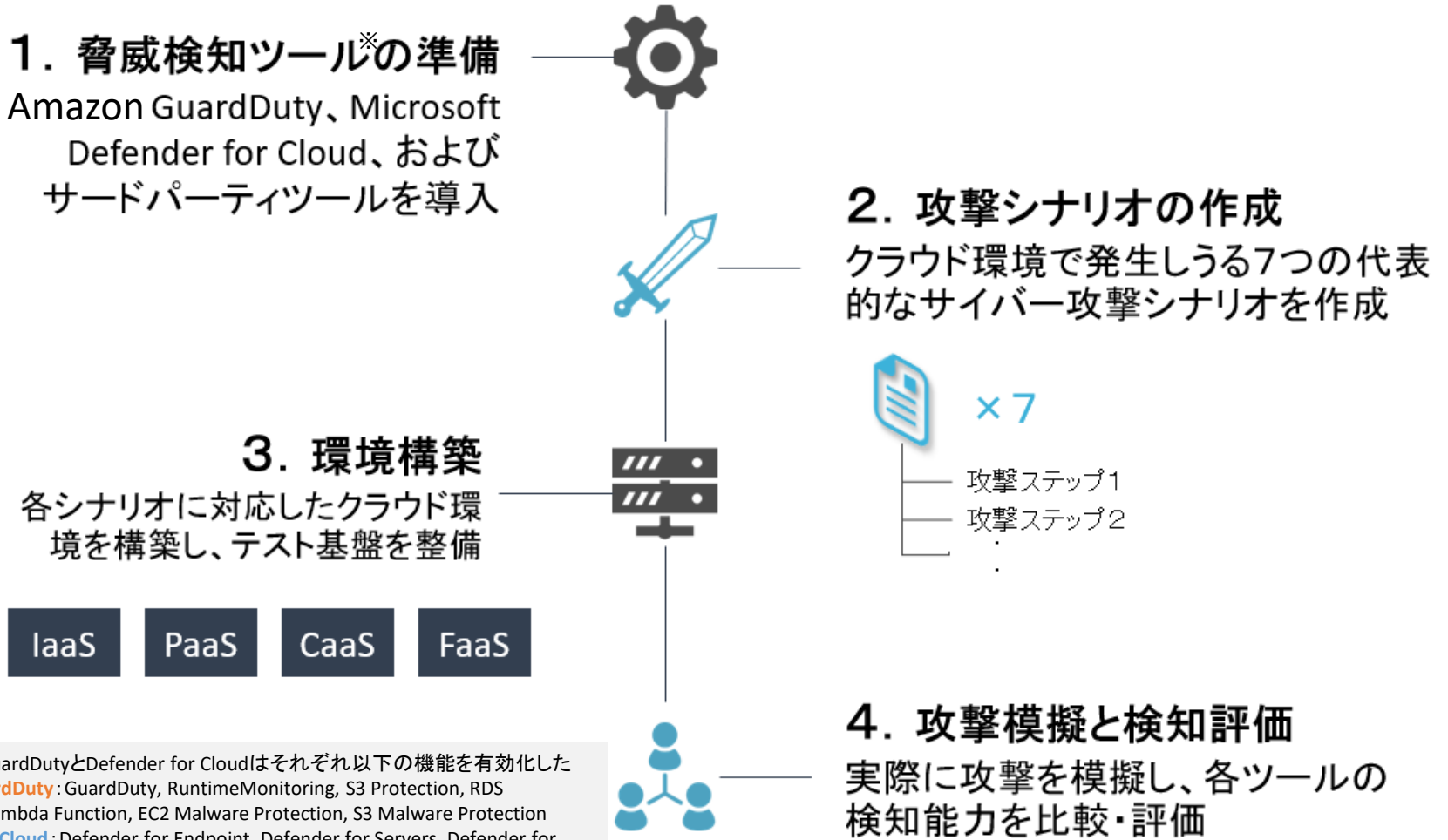
〇CWPPのユースケースは？

〇検知用のエージェントはIaaS以外にも導入できるの？

2. 検証の進め方

1）進め方

検証は下記の流れに沿って実施した。単なる座学にとどまらず、環境構築から攻撃の再現までを自ら手を動かして実践することで、より深い理解の獲得を目指した。



※Amazon GuardDutyとDefender for Cloudはそれぞれ以下の機能を有効化した
Amazon GuardDuty：GuardDuty, RuntimeMonitoring, S3 Protection, RDS Protection, Lambda Function, EC2 Malware Protection, S3 Malware Protection
Defender for Cloud：Defender for Endpoint, Defender for Servers, Defender for Containers, Defender for App Service, Defender for Storage

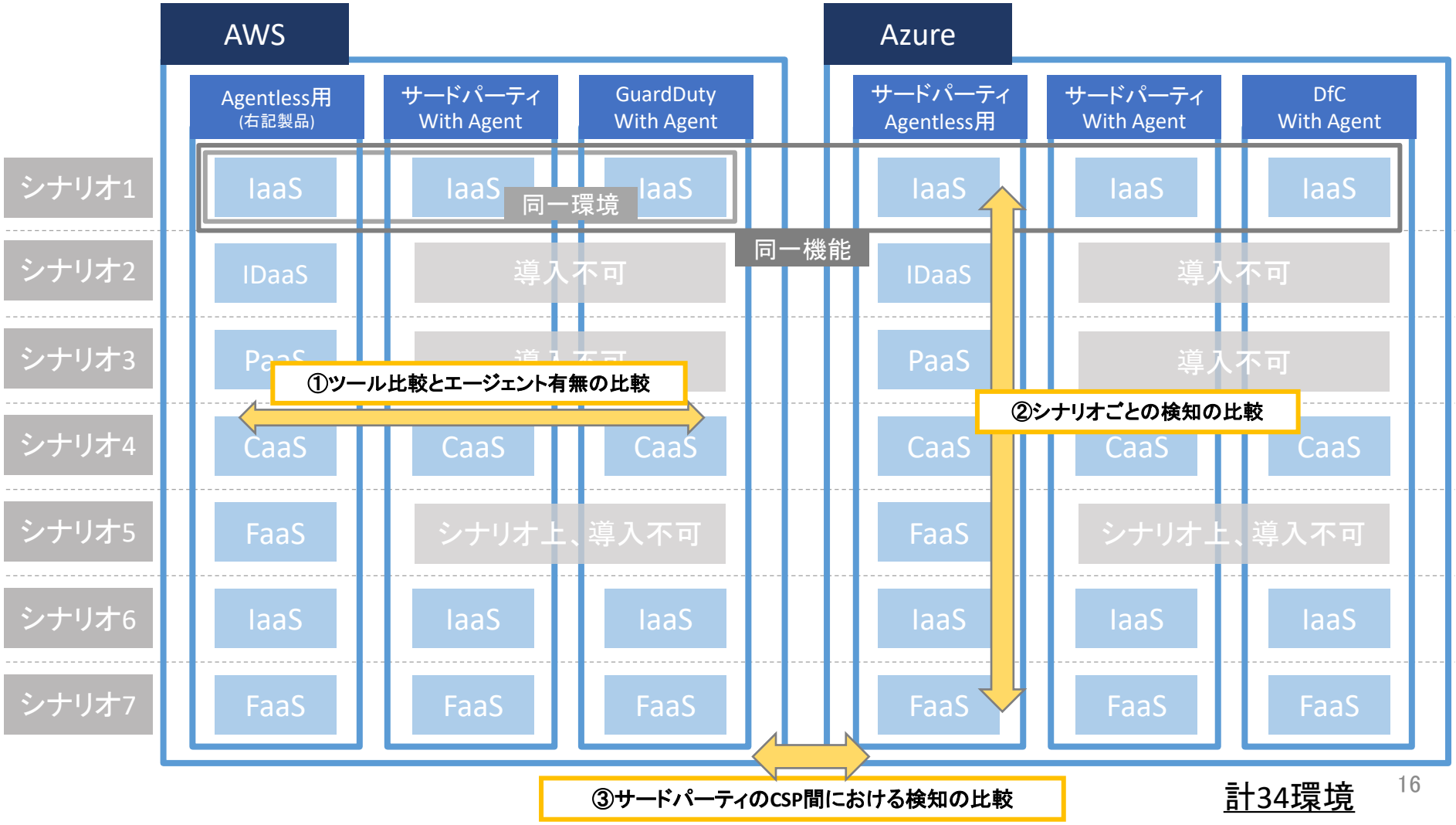
2）攻撃シナリオの選定

本プロジェクトでは、クラウドにおける脅威に対する理解を深めることを目的として、特定の攻撃ジャンルに偏ることなく、複数の脅威カテゴリを横断的に取り上げ、代表的な事例を選定したうえで多角的な検証を実施した。

No.	脅威カテゴリ	検証する攻撃シナリオ	参考事例	参考URL
1	Webアプリ脆弱性・構成不備	SSRFを悪用したMetadataAPIへのアクセス	Capital Oneのデータ侵害事件(2019年)	https://www.capitalone.com/digital/facts2019/
2	認証情報漏洩	漏洩したIAMクレデンシャルによる特権昇格	クラスメソッド株式会社のアクセスキー流出事件(2019年)	https://dev.classmethod.jp/articles/accesskey-leak/#toc-1
3	設定ミス	ストレージ設定誤りによる情報漏洩	Verizonのデータ漏洩事件(2017年)	https://www.itmedia.co.jp/enterprise/articles/1707/13/news055.html
4	コンテナ侵害	コンテナの脆弱性を悪用したホスト侵害	DockerHubへのバックドア付きDockerイメージアップロード(2017年)	https://www.bleepingcomputer.com/news/security/17-backdoored-docker-images-removed-from-docker-hub/?
5	IAM悪用	iamPassRoleを悪用したアクセス制御バイパス	AWS IAM Privilege Escalation –Methods and Mitigation(2018年)	https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/
6	ミドルウェア脆弱性	OMI認証バイパスの脆弱性を悪用したリモートコード実行	AzureOMIの脆弱性(2021年)	https://www.wiz.io/blog/omigod-critical-vulnerabilities-in-omi-azure
7	FaaS侵害	サーバレスで実装したコードの脆弱性悪用による機密情報窃取	クラウドコンピュートのクレデンシャル侵害(2022年)	https://unit42.paloaltonetworks.com/compromised-cloud-compute-credentials/

3）検証環境

脅威検知ツールとして、AWS標準のAmazon GuardDuty、Azure標準のDefender for Cloud(以降DfC)、サードパーティの3種類を下記のように適用して検証を実施した。

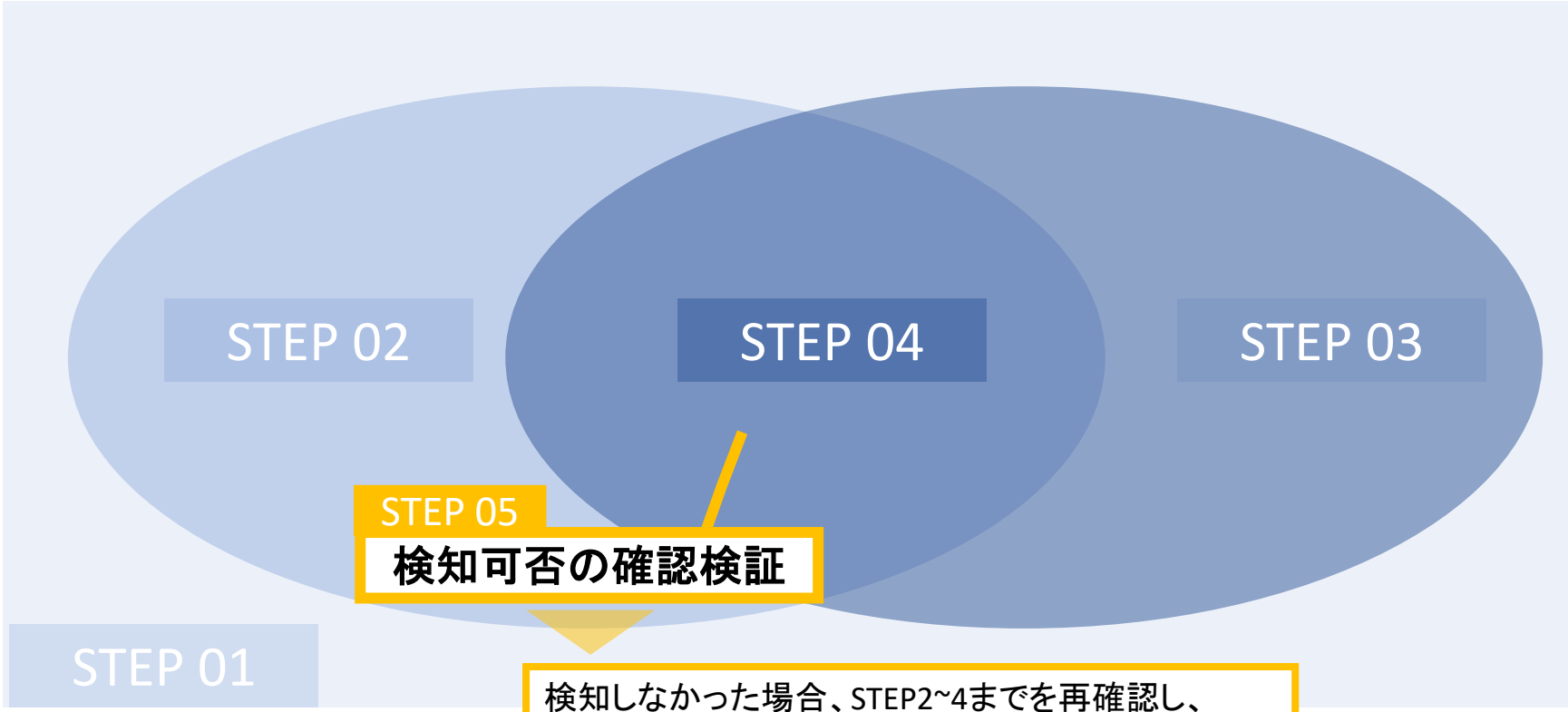


4）脅威検知の仕組み理解までのステップ

STEP 01	STEP 02	STEP 03	STEP 04	STEP 05
クラウド上で攻撃の痕跡が残りうる部分の整理（≒全ログの整理）	CWPPが監視している部分の整理	各攻撃シナリオにおいて痕跡が残る部分の整理	STEP2,3の合致した点を机上における検知期待領域と設定	机上整理（STEP4）と検証結果との突合

机上整理

検証突合

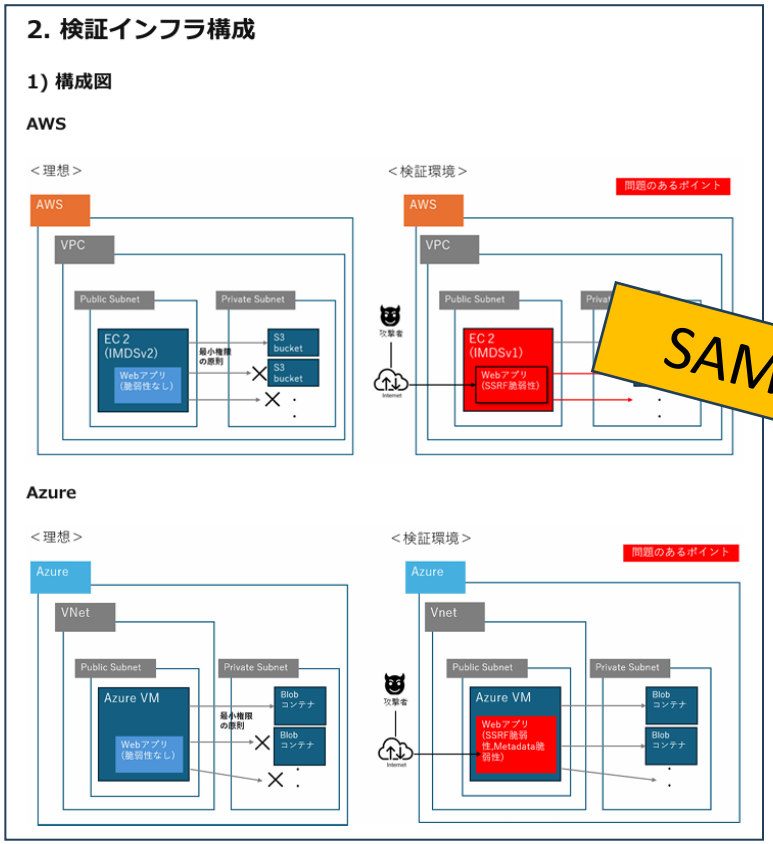


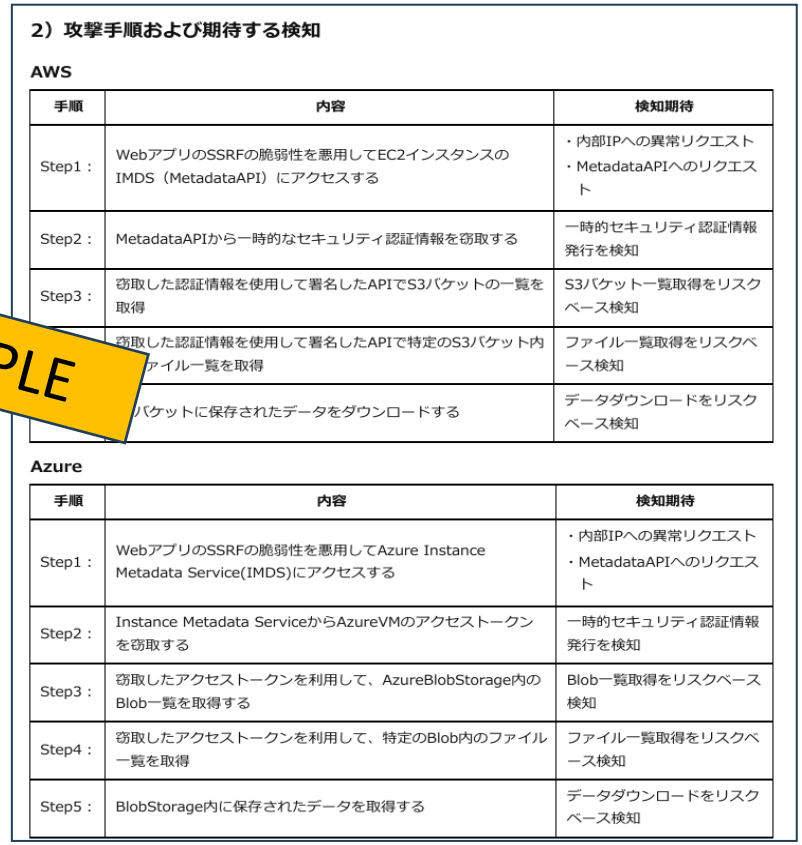
3. 検証結果

1）検知結果

検証で参考にした事例や検証で構築したインフラ構成・攻撃手順を含めた検知結果を資料にまとめた。なお、検知結果の詳細は別添に記載している。

《検知結果イメージ》





2）考察サマリ

本検証では、検知結果に差異が生じる要因として、主に以下の3つの観点が影響しているのではないかという仮説を立て、検証を実施した。その結果を踏まえた考察は、以下の通りである。

No	差異の観点	結果	詳細（考察）
1	ツールとエージェント	検知差異あり（エージェント導入可否と検知ロジックの差異が影響）	エージェントの導入可否の違いにより、各サービス間で検知結果に差異が生じる。 また、検知ロジックについても、検知ロジックの違いに加え、一部のサービスはログ連携の構成やアラートポリシーのカスタマイズを前提としていることから、そうした設定の有無によって検知結果に違いが出たと想定される。 なお、本検証は特別なカスタマイズを行わず、各製品の標準設定に基づいて実施した。 さらに、各製品がカバーする脅威の範囲や注力している領域には明確な違いが見られたことから、その背景要因を明らかにするために、ベンダー企業の沿革や提供機能の変遷について調査を実施した。 その結果、製品ごとの設計思想や開発の経緯が、検知機能の違いとして表れている可能性があることが分かり、本検証における新たな示唆として、「検知差はベンダーの成り立ちに起因している可能性がある」という仮説を導き出すに至った。 例えば、外資系ベンダーの多くは、機能拡張を目的とした買収を積極的に行う傾向があり、同じCNAPPカテゴリに属する製品であっても、それぞれが異なる強みを有している場合などである。買収により機能を統合してきた製品では、各機能の独立性を活かしつつ段階的に連携を深めていくアプローチが多く見られる一方で、設計段階から機能間の統合や連携を前提に開発された製品では、CNAPPとしての一体的な強みがより発揮されやすい傾向にあるのではないかと考えた。

2）考察サマリ

No	差異の観点	結果	詳細（考察）
2	シナリオ （サービスモデル）	エージェントあり：検知差異あり エージェントレス： 検知差異なし	IaaS環境ではエージェントの導入が可能であるため、各種脅威に対する検知が比較的容易である。一方で、PaaSやFaaSといったサービスモデルでは、技術的または構造的な制約によりエージェントの導入が困難な場合が多く、同等の検知レベルを実現することが難しい傾向がある。なお、エージェントの導入可否は製品ごとに異なり、一般的にはサードパーティ製品の方がより多様なサービスモデルに対応している傾向が見受けられた。 一方で、エージェントレス型の監視方式はサービスモデルに依存せず、共通の監視レイヤを通じて情報を取得することが可能であるため、IaaS・PaaS・FaaSを問わず、一貫性のある検知結果が期待できる。
	シナリオ （インシデント原因）	検知差異あり	脆弱性を悪用した攻撃に対しては、各製品とも比較的高い検知精度を示す傾向が見られた。一方で、クラウド環境における設定ミスを起点とした攻撃に対しては、検知が困難であるケースが多く確認された。

2）考察サマリ

No	差異の観点	結果	詳細（考察）
3	CSP（AWS、Azure）	検知差異なし	本検証では、サードパーティ製品を活用することで、クラウドサービスプロバイダ（CSP）間の環境差異を超えた検知精度の比較を実施した。その結果、当該製品においては、AWSやAzureといったCSPの違いによらず、検知内容に大きな差異は見られなかった。このことから、サードパーティ製品を導入することで、クラウド環境を問わず一定水準の検知性能を確保できる可能性が示唆された。 一方で、AWSのAmazon GuardDutyやAzureのDefender for Cloudといった各クラウドのネイティブサービス間では、検知対象や内容に一定の違いが確認されており、CSPごとの特性を踏まえた対策の検討が必要である。

4. プロジェクトを通しての学び

1）クラウドにおける脅威検知の仕組み理解
i）脅威の観測ポイント

検証の結果、クラウド環境における脅威検知は、主に「API※操作」「IAMの振る舞い」「ネットワーク」「ワークロード内の挙動」の4つの領域を監視対象とすることで行われることが分かった。

※CSPの各サービスを操作するAPIを指す

API※操作

想定脅威
不正なリソース作成、ストレージ操作など、異常なAPI呼び出し

IAMの振る舞い

想定脅威
異常な地理的アクセス、特権の使用等、異常なIAMの振る舞い

ネットワーク

想定脅威
不審なポート通信、不審なドメインとの通信など、異常な通信

ワークロード内の挙動

想定脅威
悪意のあるプロセスやコマンド実行などワークロード内の異常な挙動

1）クラウドにおける脅威検知の仕組み理解
ii）エージェントの監視範囲

前スライドで整理した4つの観測ポイントのうち、エージェントを導入することで監視可能となる領域を示したものが本スライドである。オレンジ色で強調された「ワークロード内の挙動」は、エージェントを通じて初めて可視化される領域であり、他の観測手段では把握が困難な内部挙動の検知に寄与する。

API※操作

想定脅威
不正なリソース作成、ストレージ操作など、異常なAPI呼び出し

IAMの振る舞い

想定脅威
異常な地理的アクセス、特権の使用等、異常なIAMの振る舞い

※CSPの各サービスを操作するAPIを指す

ネットワーク

想定脅威
不審なポート通信、不審なドメインとの通信など、異常な通信

ワークロード内の挙動

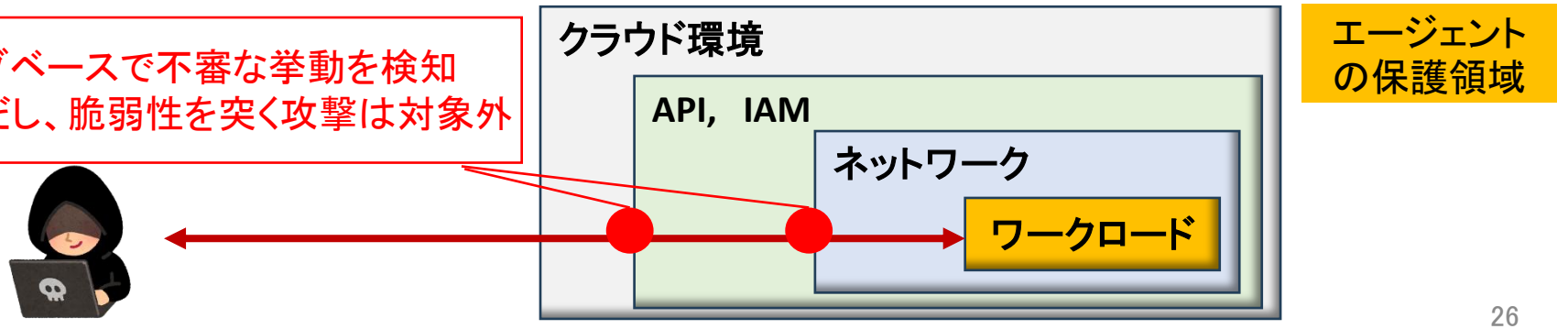
想定脅威
悪意のあるプロセスやコマンド実行などワークロード内の異常な挙動

1）クラウドにおける脅威検知の仕組み理解
iii）エージェントの詳細理解

○エージェントなしの場合、クラウドが提供するログを活用することで、ワークロードへの攻撃前後の操作や通信の痕跡を監視することが可能である。
○一方で、エージェントはワークロード内部の挙動を直接監視できることが強みである。
○このことからエージェントはクラウドが提供するログベースの監視を補完する手段として位置づけることができる。

	エージェントあり	エージェントなし
検知範囲	ワークロード内部の詳細な挙動（プロセス、ファイル、メモリ操作、システムコール、バイナリ、ネットワーク接続など）	クラウドサービスにおける、操作ログ(API操作、IAMの振る舞い)、ネットワークログなど、クラウドが提供するログ
検知手段	ワークロード上に常駐し、リアルタイム監視	ログやイベントを集約・分析
検知例	不審なバイナリ実行、プロセスの不審な挙動	IAMの異常操作、DoS通信、特定ポート通信
メリット	ワークロードの内部動作(プロセスやカーネル)を詳細に観測できるため、OS内部での異常な挙動を検知可能	・ログベースで監視するため、導入が容易でクラウド環境全体を広くカバー可能 ・資格情報の悪用、外部からの試行といった攻撃の前後も含めて検知可能

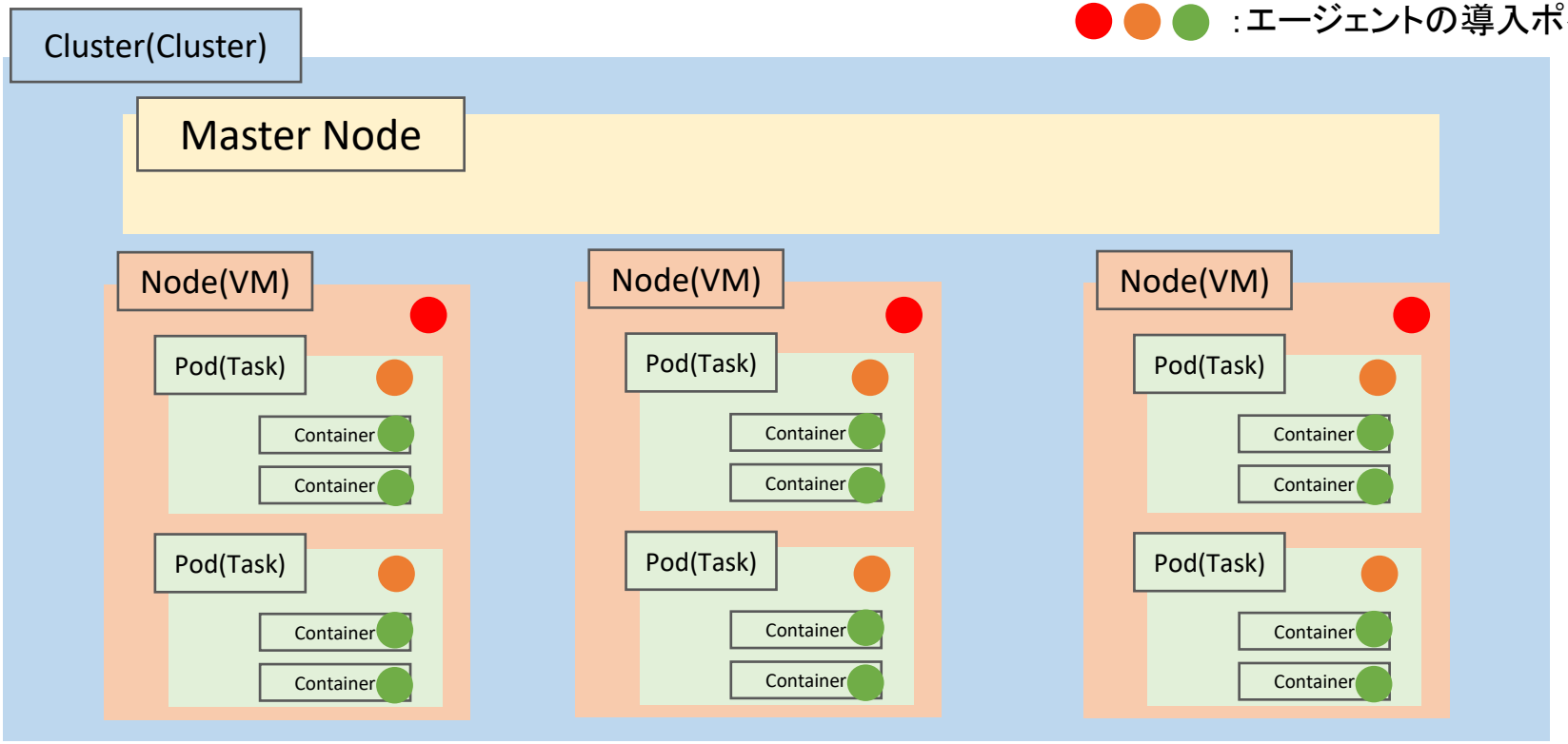
・ログベースで不審な挙動を検知
・ただし、脆弱性を突く攻撃は対象外



エージェントの保護領域

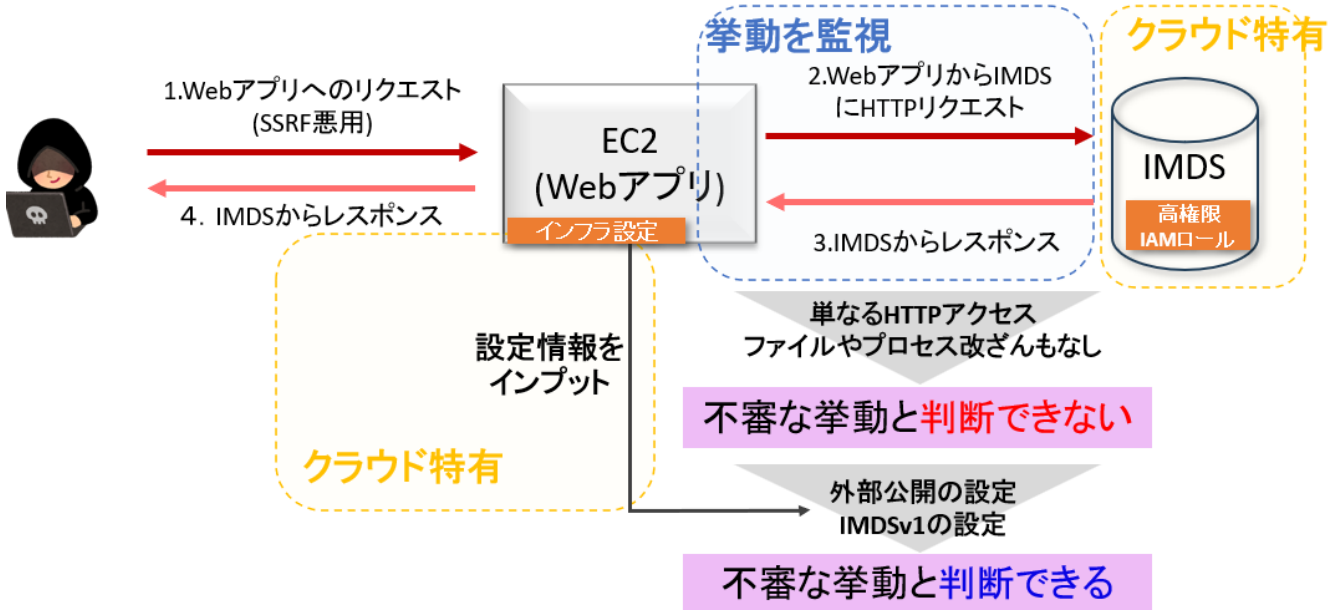
1）クラウドにおける脅威検知の仕組み理解
ⅳ）コンテナ環境のエージェント種類

〇コンテナ環境における脅威検知のためのエージェントの配置パターンを整理した。
〇Kubernetesなどのオーケストレーション環境では、クラスタを構成する複数のノード上でコンテナが稼働しており、エージェントの配置レイヤー（ホストVM、Pod、コンテナ）によって、導入や運用管理の難易度・柔軟性に違いが生じる場合がある。
〇本整理は、代表的なCWPP製品ベンダーの公開情報をもとに構成要素間の関係性を視覚化したものであり、エージェント方式の理解を支援することを目的としている。



1）クラウドにおける脅威検知の仕組み理解
v）クラウド特有の検知

〇図は、攻撃者がWebアプリのSSRFの脆弱性を悪用して、Amazon EC2インスタンス上のIMDS※1にアクセスし、高権限なIAMロールの認証情報を取得する一連の流れを示している。
〇Amazon EC2からIMDSへのHTTPリクエストの挙動自体はオンプレ前提のEDR等でも検知可能な範囲ではある(図中青枠部分)。しかし、この通信のみではリスクの有無を的確に判断することは難しい。
〇この挙動に対して、IMDSv1が有効化されている※2といった設定上の脆弱性や、EC2に高権限のIAMロールが付与されているといったクラウド環境固有の情報を組み合わせて分析することで、初めて「リスクの高いアクセス」であると判断することが可能となる。このように、クラウド特有の構成情報や設定を考慮したうえでの高度な判断が可能である点が、クラウド対応のツールの強みである。



※1：IMDS（Instance Metadata Service）とは、クラウド環境においてインスタンス(仮想マシン)自身が、自らの構成情報や認証情報などのメタデータを取得するための仕組み。https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html
※2：現在AWSではIMDSv2の設定がデフォルトとなっている。また仮にIMDSv1が設定されたとしても検知できる仕組みも存在する。

1）クラウドにおける脅威検知の仕組み理解
vi）クラウド特有の検知

項目	CWPP	EDR
主な保護対象	クラウドワークロード（仮想マシン、コンテナ、サーバレス等）	エンドポイント（PC、サーバー、端末等）
導入形態	エージェント型 エージェントレス型	エージェント型
検知対象	クラウド上の仮想基盤、Kubernetes、サーバーレス等が基本だが、オンプレ端末にエージェント導入が可能な製品も有	端末全般（クラウド・オンプレ問わず）
検知ソース・方法	クラウドの構成情報（IAM, IMDS等）と実行時の挙動を組み合わせ、環境全体を横断的に分析して検知	端末内のログやプロセス挙動、メモリ操作に基づき、端末内の情報に閉じた詳細な振る舞い分析し、検知
対応（Response）への紐づけ	他製品との組み合わせにより対応可	可能

総括

EDRとCWPPはオーバーラップしている領域が多いものの、
部分的に互いを補完しあう関係でもある

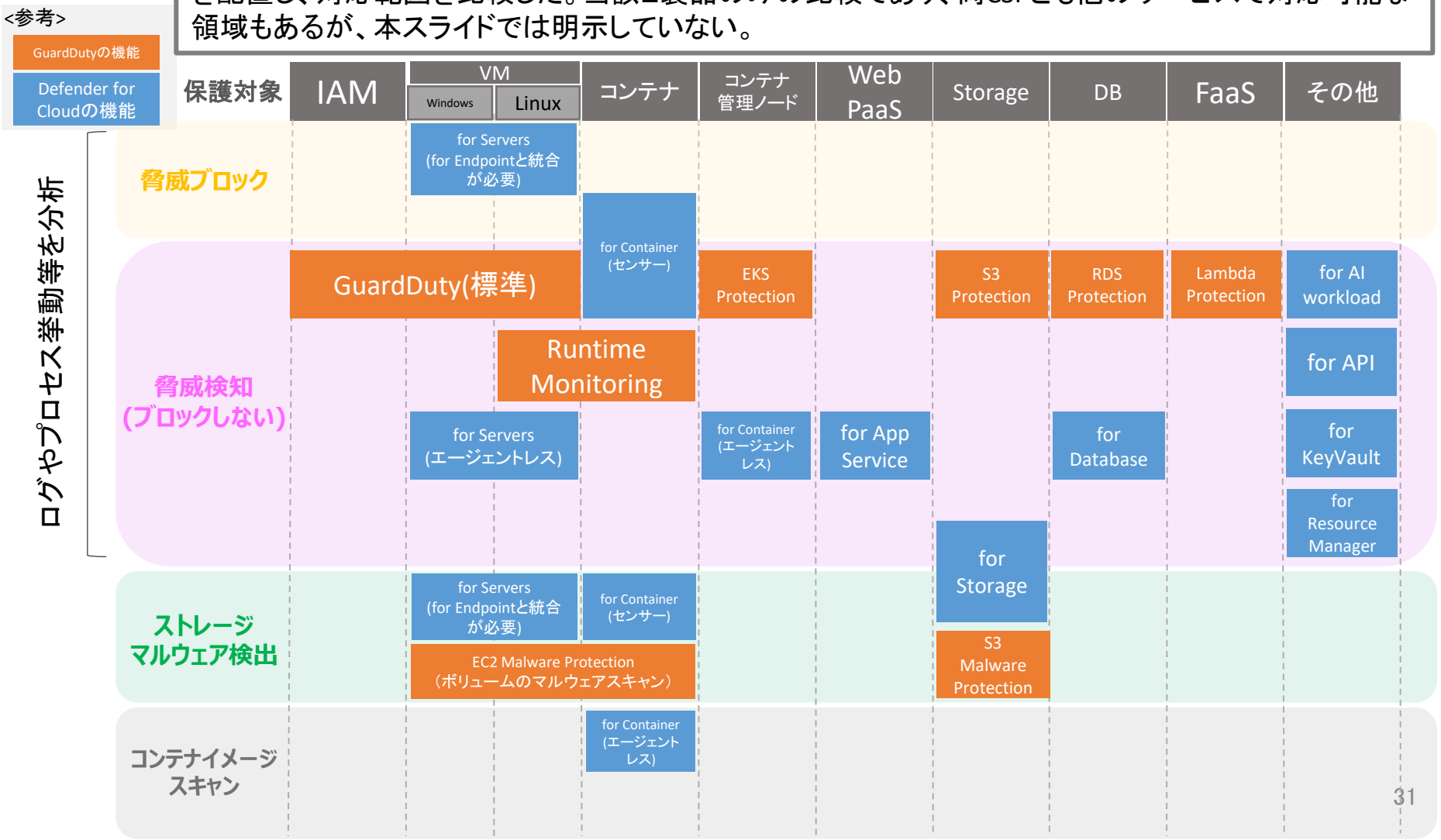
1）クラウドにおける脅威検知の仕組み理解
vii）サービスモデル毎の代表的な脅威検知手段

○クラウド利用者の視点で、各サービスモデルに適用可能な脅威検知手段を下記表に整理した。
○なお、各検知製品の検知領域等は、提供ベンダーの方針や技術の進化により変化する可能性があるため、本表はあくまで参考情報としてご確認いただきたい。

分類			ネットワーク型		ホスト型（エージェント）	クラウド固有	
						ホスト型（エージェント）	その他
検知製品			WAF（Webアプリの保護）	IPS（ミドル、OSの保護）	EDR（パターンマッチ、ふるまい）	CWPP（エージェント）	CWPP（エージェントなし）
検知領域（製品により異なる）			OSI L7	OSI L3～L6	OS内部	クラウドワークロード	・OSI L3, L4 ・CSP API層
サービスモデルとユーザ責任範囲	IaaS	VM	適用可能	適用可能	適用可能	適用可能	適用可能
	CaaS	VM	適用可能	適用可能	適用可能	適用可能	適用可能
		コンテナ			対策不要		
	PaaS	コンテナ	適用可能	適用可能	対策不要	専用製品なし	適用可能
		ミドル					
	FaaS		適用可能	対策不要	対策不要	適用可能	適用可能

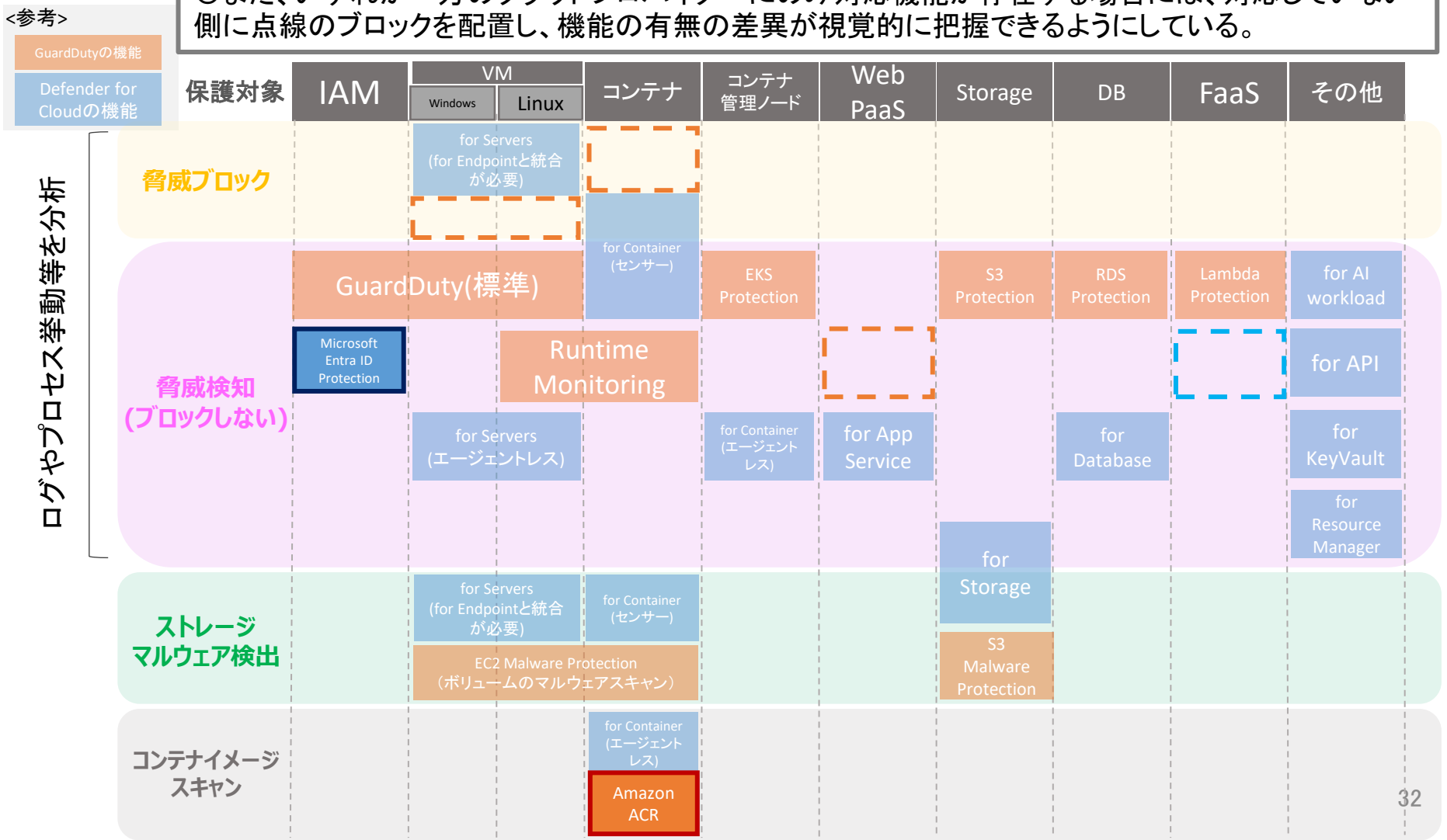
1）クラウドにおける脅威検知の仕組み理解
viii）Amazon GuardDutyとDefender for Cloudの保護対象の比較

○本スライドでは、AWSおよびAzureにおける代表的な脅威検知製品であるAmazon GuardDutyとMicrosoft Defender for Cloudについて、縦軸に脅威検知機能、横軸に保護対象となるクラウドリソースを配置し、対応範囲を比較した。当該2製品のみの比較であり、両CSPとも他のサービスで対応可能な領域もあるが、本スライドでは明示していない。



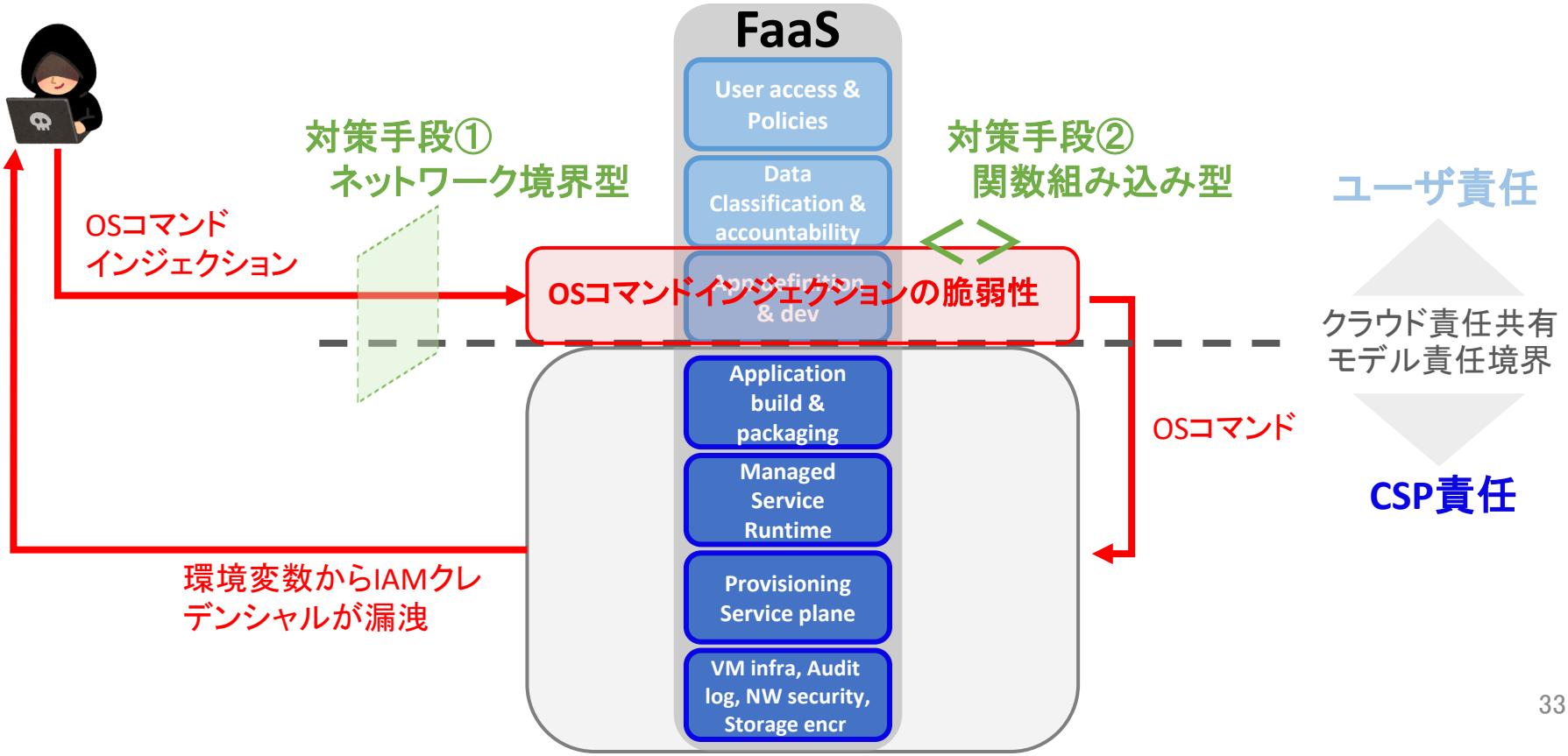
1）クラウドにおける脅威検知の仕組み理解
viii）Amazon GuardDutyとDefender for Cloudの保護対象の比較

〇本スライドでは、Amazon GuardDutyおよびMicrosoft Defender for Cloud以外のセキュリティサービスについても整理し、各保護対象領域に対応する機能をマッピングした。
〇また、いずれか一方のクラウドプロバイダーにのみ対応機能が存在する場合には、対応していない側に点線のブロックを配置し、機能の有無の差異が視覚的に把握できるようにしている。



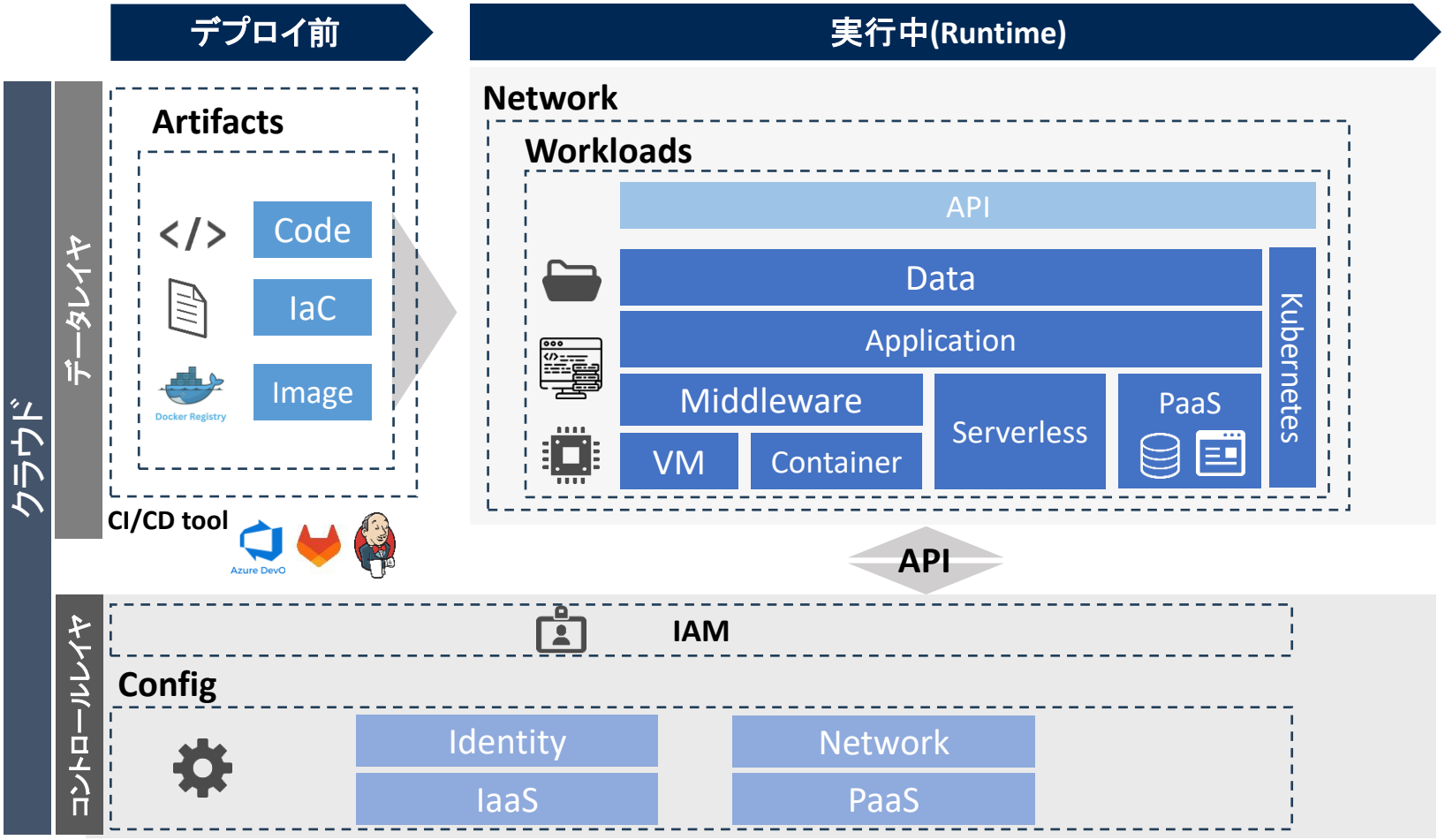
2）クラウドにおける脅威と対策の一例(FaaS)

〇FaaS環境における脅威を把握することを目的に、FaaS上に実装した関数に対してOSコマンドインジェクションを模擬した攻撃検証を実施した。その結果、関数実行環境のOSレイヤーに設定されていた環境変数からIAMクレデンシャルの窃取に成功し、脅威が現実的に発生し得ることを再現できた。
〇また、本脅威に対する検知対策として、WAFなどのネットワーク境界型ソリューションのほか、一部のセキュリティ製品では関数単位での入力・出力監視機能を提供しており、本攻撃シナリオに対しても有効に機能することを確認した。



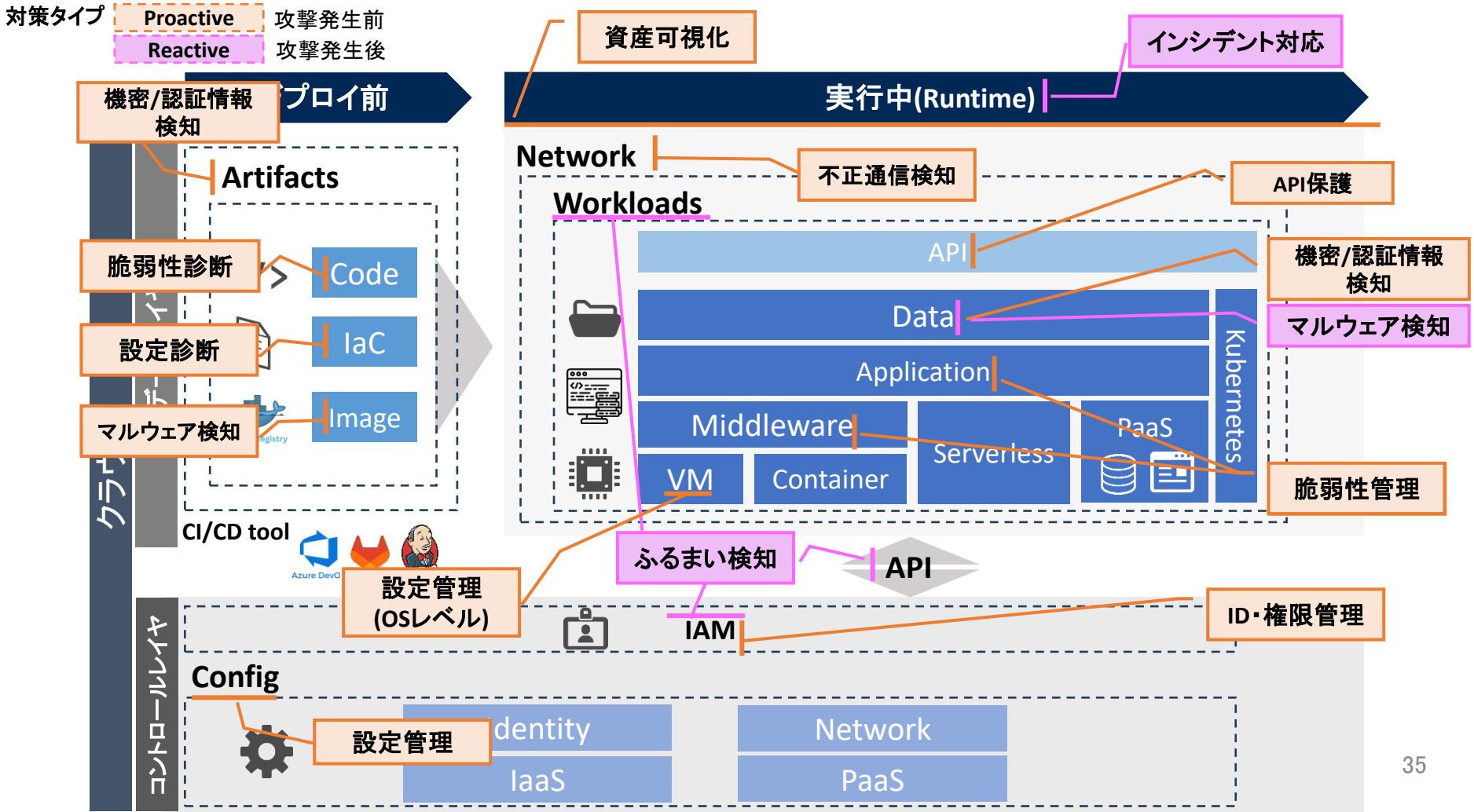
3）クラウドセキュリティ要件の理解

○クラウドのセキュリティ対策を検討するにあたり、CSPM、CWPP、CIEM、WAASなど、多様な用語やソリューションが混在しており、体系的に整理することが難しい状況にある。
○本資料では、まずクラウドの構成要素およびシステムライフサイクルフェーズを整理したうえで、求められるセキュリティ要件を明確化し、それらに対応する代表的なセキュリティソリューションをマッピングすることで、「やるべきこと」と「使用する手段」を対応付けて可視化することを試みた。



3）クラウドセキュリティ要件の理解

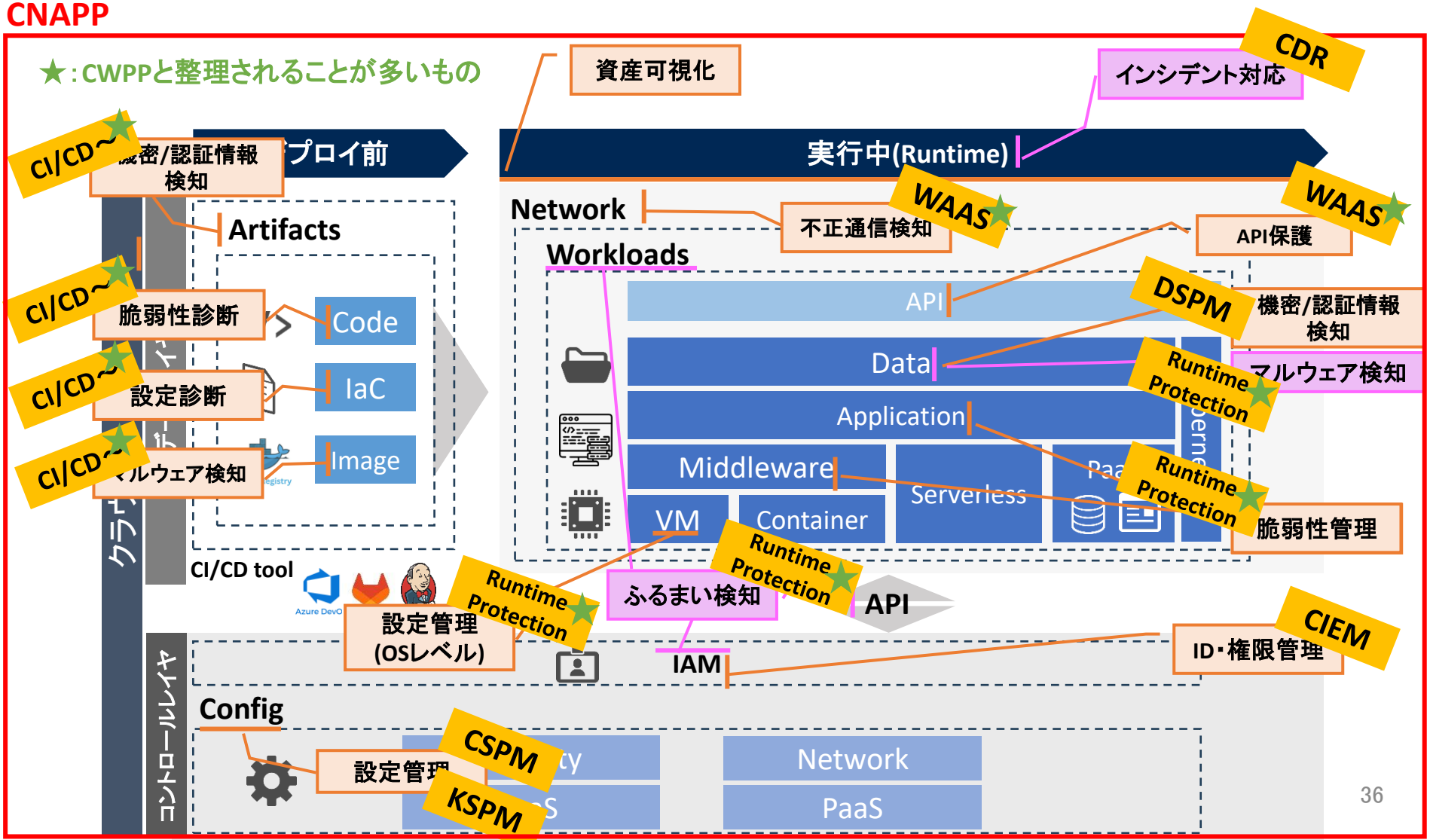
○複数のセキュリティベンダーが提示する情報を参照しながら、どのようなセキュリティ要件がクラウド環境において整理・定義されているのかを調査し、再整理を行った。
○プロアクティブ（攻撃前）／リアクティブ（攻撃後）といった対策の性質や、構成要素ごとに求められるセキュリティ対策の観点を可視化することで、全体像を把握しやすくすることを目的としている。



3）クラウドセキュリティ要件の理解

○クラウドにおける各セキュリティ要件に対して、代表的なソリューション名や概念をマッピングした。これはあくまで一例であり、ベンダーごとに提供機能や呼称には差異があるが、全体像を把握する上での整理の起点として活用できる。

CNAPP



4）クラウド脅威検知ツールのユースケース

各社のクラウド活用状況、今後の方針、ガバナンス、予算感を考慮したうえで、
下記の表を参考に脅威検知ツールを導入することを提案する

成熟度	クラウドリフト	クラウドシフト	クラウドネイティブ
Phase			
状況	オンプレ中心に活用しており、クラウド活用はあまり進んでおらず、IaaSは一部使い始めたものの、コンテナやサーバレス環境はほとんど利用していない	サーバ周り（IaaS）に関してはクラウド活用が徐々に進んでおり、コンテナやサーバレスの活用も一部部署で始まったものの機密情報までは預けていない	クラウド活用が進んでおり、コンテナやサーバレス環境を活用したサービスを提供しているかつそれらのサービスで機密情報を扱っている

ユースケース	クラウドリフト	クラウドシフト	クラウドネイティブ
サービスモデル	導入が推奨されるツールセット		
IaaS	EDR	EDR+CWPP(Agentless)	EDR+CWPP(with Agent)
PaaS	対策なし	CWPP(Agentless)	CWPP(with Agent)
CaaS	対策なし	CWPP(Agentless)	CWPP(with Agent)
FaaS	対策なし	CWPP(Agentless)	CWPP(with Agent)
導入タイプ	コスト優先型	バランス型	セキュリティ重視型

5. おわりに

おわりに

本プロジェクトの出発点には、CNAPP や CWPP といったクラウドセキュリティに関する用語へのモヤモヤ感がありました。

検討を進めるなかで、「ワークロード」や「ランタイム」などの言葉がメンバー間で意図する意味が微妙に異なっていたり、CNAPP のような統合的な概念に対しても人によって理解がバラバラであることが明らかになりました。その認識のずれを解消しようと文献や資料を調べてみても、ベンダーごとに定義や前提が異なり、「何をどこまでカバーするものなのか」がはっきりせず、かえって混乱が深まるような場面も多くありました。用語に振り回されて本質的な理解が進みにくいという、課題感を強く実感しました。

そこで本プロジェクトでは、CNAPPの中でも特に「脅威検知」の領域にテーマを絞り、実際にクラウド環境を構築して各種検知手段の検証を行いました。この領域を選んだ理由は、メンバーの関心が高く、加えて「自ら環境を構築して手を動かすことでクラウドスキルを高める」という本プロジェクトのもう一つの目的にも合致する題材であったためです。観点を絞って実践を通じた検証を進めたことで、言葉では捉えきれなかった技術や機能の実態に直接触れることができ、クラウドにおける脅威検知の全体像や、CWPPを含む各ソリューションの立ち位置への理解が深まりました。結果として、検証対象外だった CNAPP の他要素（CSPM、CIEM、リスク可視化など）についても、実装のイメージや役割を自分たちの中で整理することができ、最終的にはCNAPP全体の構成と意義を体系的に捉えるための基盤を得ることができました。

今後も新たな用語や製品は次々と登場すると想定されますが、それに振り回されるのではなく、自組織にとって必要なセキュリティ要件を起点に考える姿勢を持つことで、定義の差異やベンダーの主張に惑わされることなく、本質的に必要な機能を選び取る力を持つことが重要であると、本取り組みを通じて改めて実感しました。

6. 謝辞

謝辞

本プロジェクトの実施および本書の作成にあたりまして、アスピレイション株式会社様、SCSK株式会社様には、製品環境の提供や技術仕様のご説明およびクラウドにおける脅威検知機能の技術的検証に関して多大なるご支援とご助言を賜りました。お忙しい中お力添えを賜りましたことに、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、満永拓邦先生には、本プロジェクトの方向性の整理や視座の提供、検討内容の具体化・改善に関して多くのご指導・ご助言をいただきました。改めて厚く御礼申し上げます。

最後に、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の意を表したいと思います。

＜クラウドにおける脅威検知プロジェクトメンバー＞

【リーダー】
田川　卓哉

【サブリーダー】
田中　貴道　　山本　大貴

【メンバー】
伊江　将一　　佐藤　蘭丸　　前川　将一　　結城　直也
伊藤　直　　酢谷　友博　　森山　響　　吉田　晋久
川崎　政吾　　野崎　晴臣　　栁　輝幸