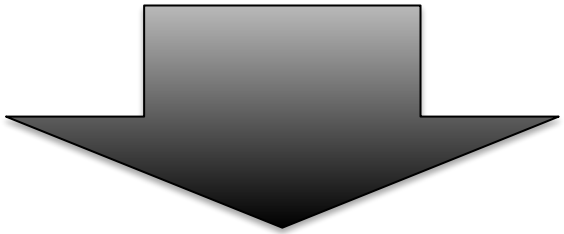
PAR-05

クラウドネイティブなワークロードは最新のテクノロジーで防御せよ 最先端のクラウドセキュリティはこれだ

西田 和弘
パロアルトネットワークス株式会社
技術本部
パブリッククラウド スペシャリスト システムズ エンジニア

クラウドネイティブ ワークロード保護には、従来の手法では困難な理由

- 従来：エージェントベースの静的なデプロイメントが主流
- AWS Auto scalingなどの動的なワークロードの拡大、縮小への対応が困難
- Dockerコマンド等など動的なリソースマッピングに対応が困難（ポートは固定でない）
- エージェントのインストールが必須であり、フルマネージドな環境への対応が困難
- セキュアな IaC (AWS CloudFormationなど) への対応 – そもそもできない？



クラウドネイティブ ワークロード専用のセキュリティ対策が必要

Prisma Cloud: パロアルトネットワークスが考える、包括的なクラウドネイティブアプリケーション保護プラットフォーム

本日のトピック

CSPM

顧客のクラウド設定の監視、脅威の検知とレスポンス、コンプライアンスの維持

導入
アドバイザー

CWP

単一のDefenderエージェントでホスト、コンテナ、サーバーレスを保護

エージェントレス・スキャン

クラウド・ID・セキュリティ(CIEM)

パーミッションの適正化
セキュアなIDを
クラウド全体で

マルチクラウド
サポート

クラウドネットワークセキュリティ(CNS)

IDベースマイクロ・セグメンテーションによるゼロトラストの実現

自動プロファイリング
と標準提供ルール

本日のトピック

クラウド・コードセキュリティ

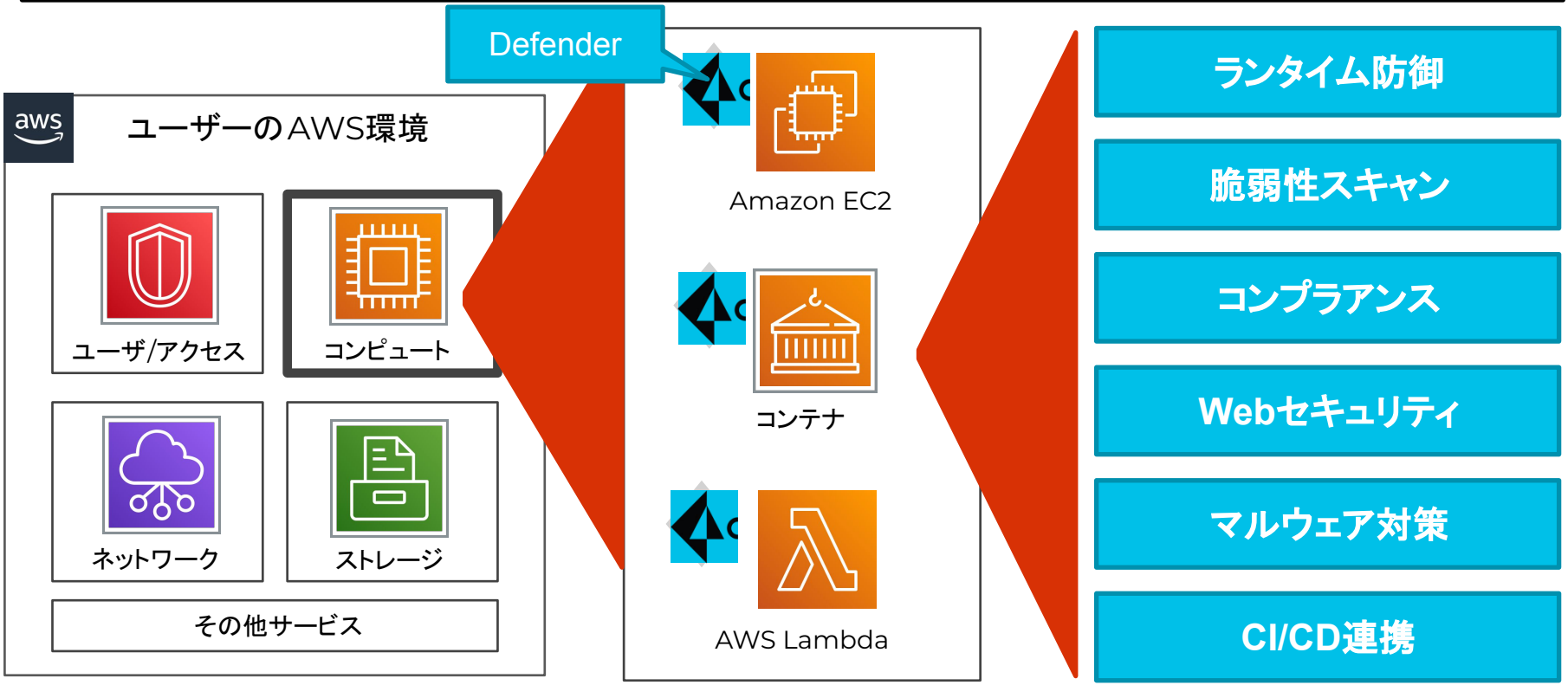
IaCコードを分析し、CIツールと連携したコードの自動修正

IaC
セキュリティ

アプリケーションのフルライフサイクル
アプリケーションのライフサイクル(ビルド -デプロイ-実行)における安全性の確保

Cloud Workload Protection(CWP): クラウド ワークロードをトータルで保護

顧客のクラウドネイティブなワークロードの保護に必要なセキュリティ機能を網羅



CWP: サポート対象のAWSサービス

コンテナ

Amazon EKS

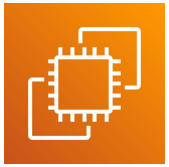
Amazon ECS

AWS Fargate

サーバーレス

AWS Lambda

仮想マシン



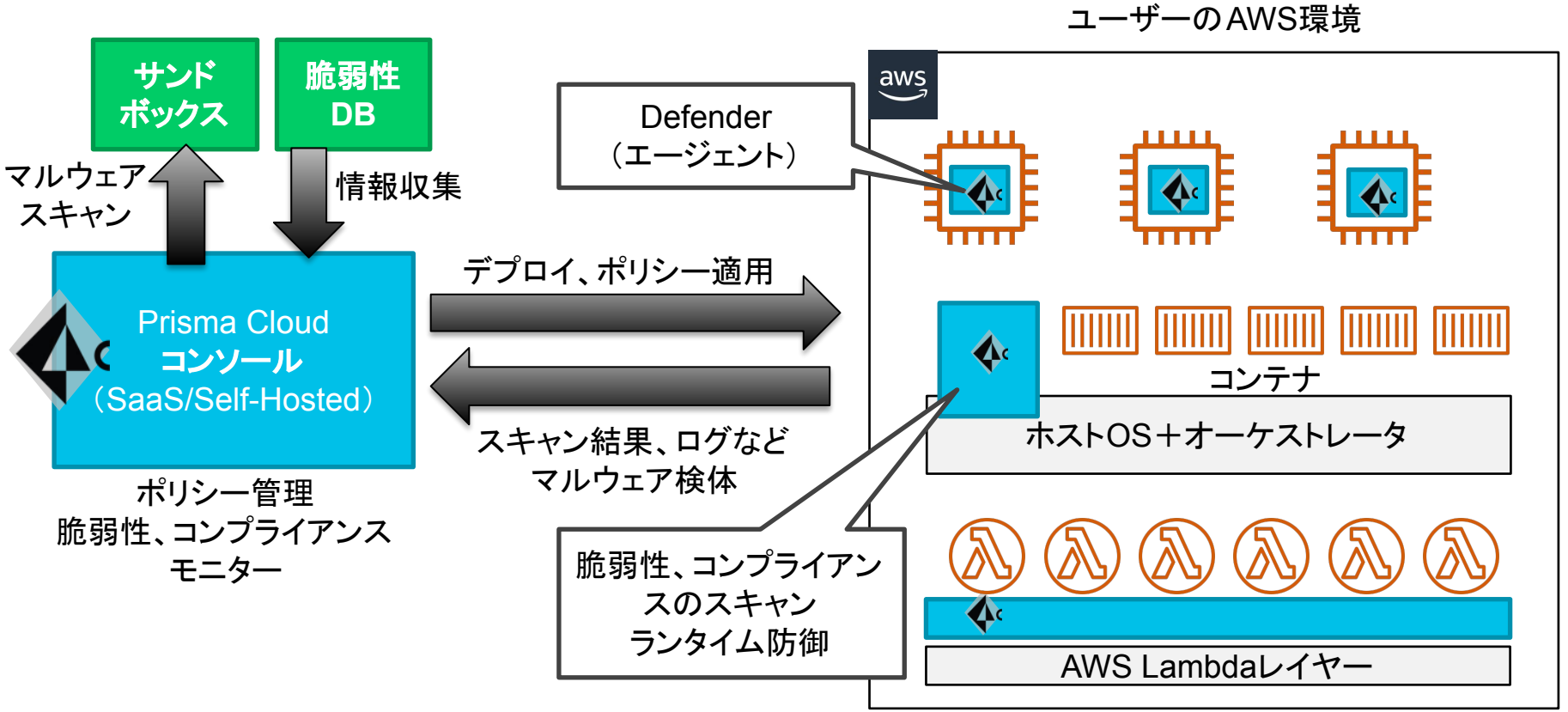
Amazon EC2

レジストリ、イメージ

Amazon ECR

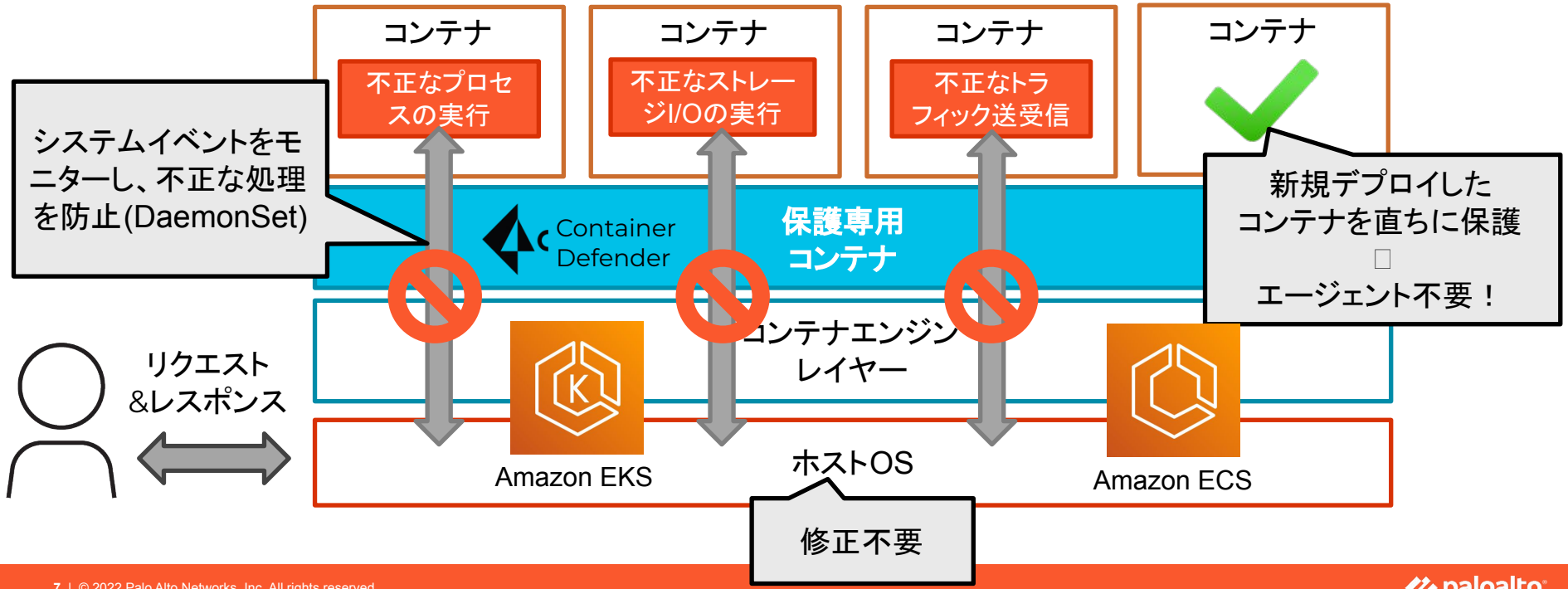
AMI

Prisma Cloud CWPの仕組み – コンソールとDefender



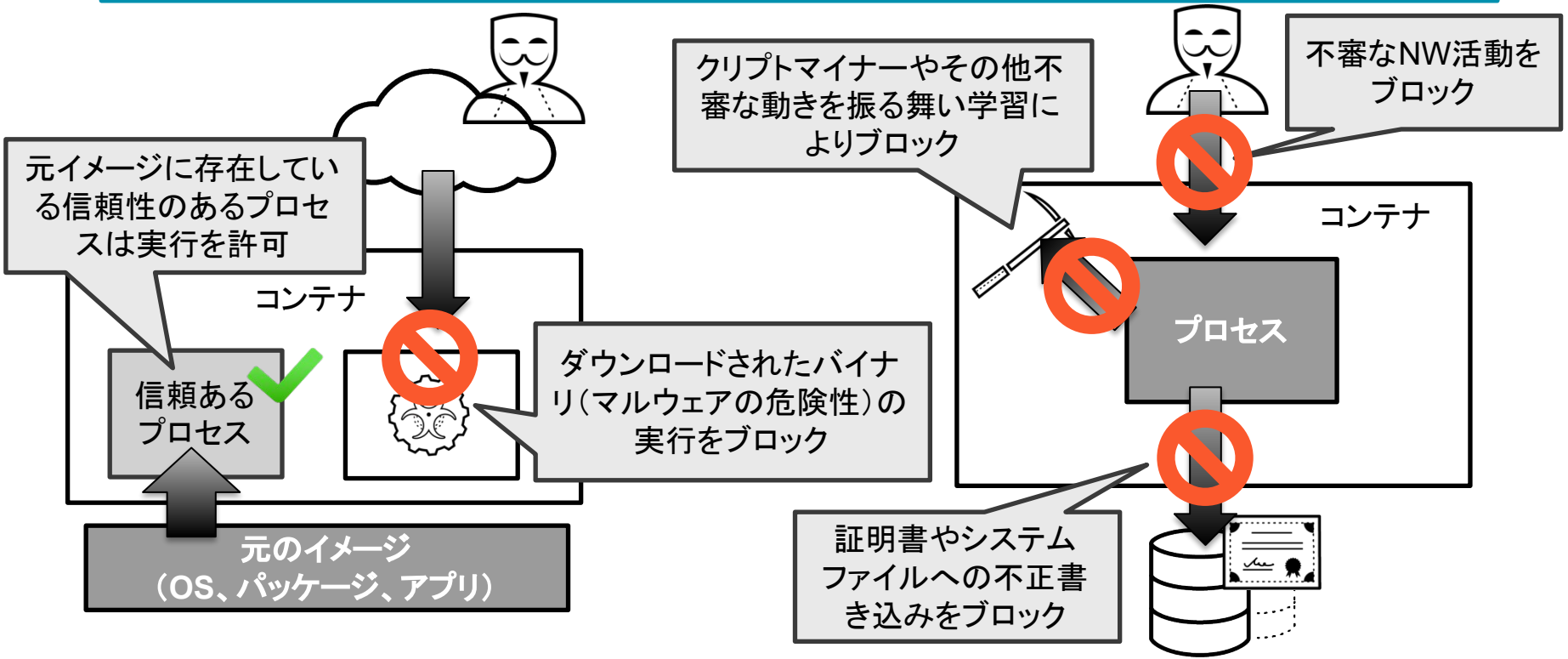
ここがすごい – ホストOSの改変なしにコンテナのランタイム防御を実現

個々のコンテナにDefenderのインストールは不要、コンテナは常に保護される

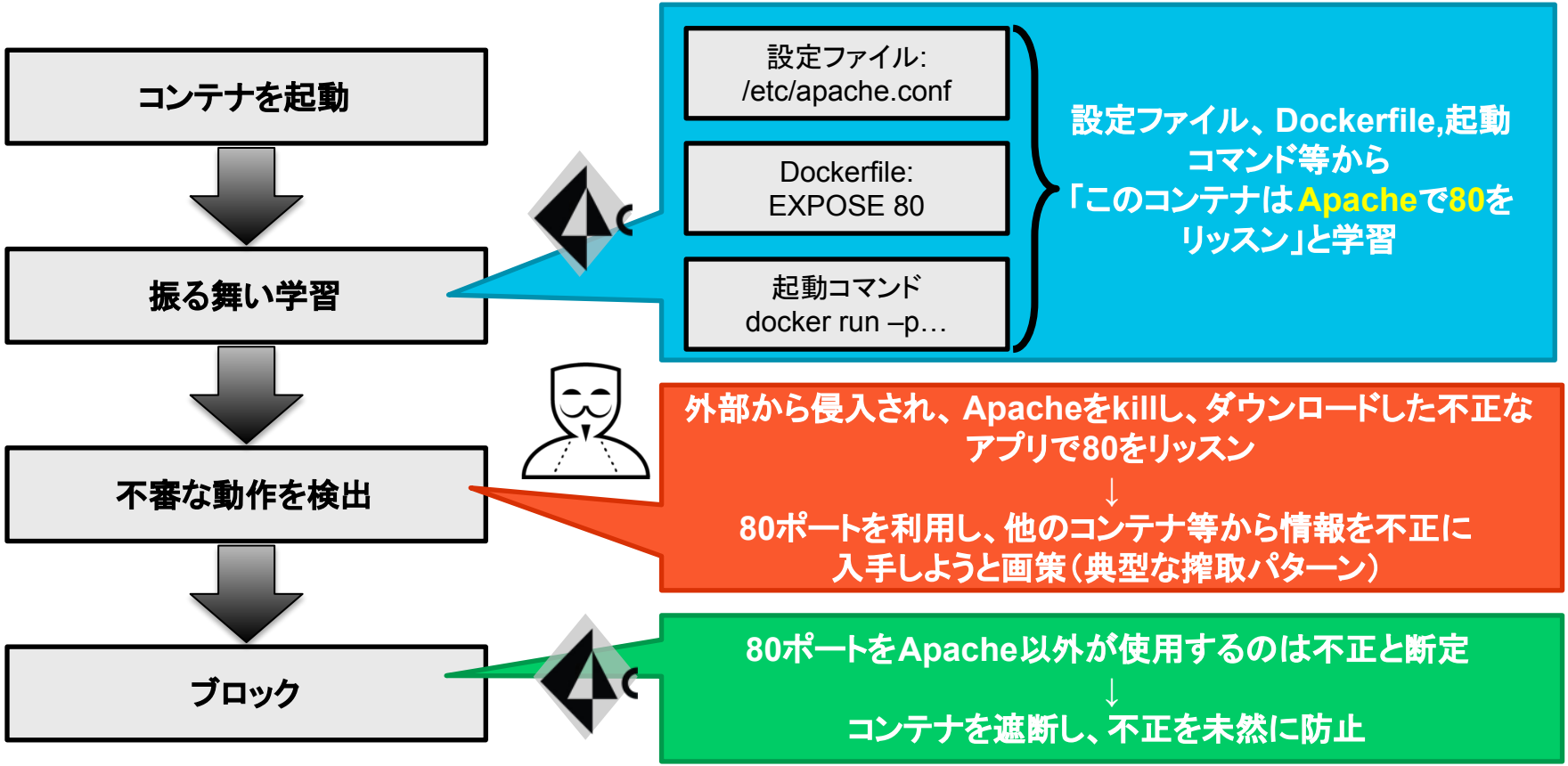


コンテナランタイム防御 – あらゆる不審な動作、未知のマルウェアをブロック

振る舞い学習 により 面倒な設定は不要で自動保護

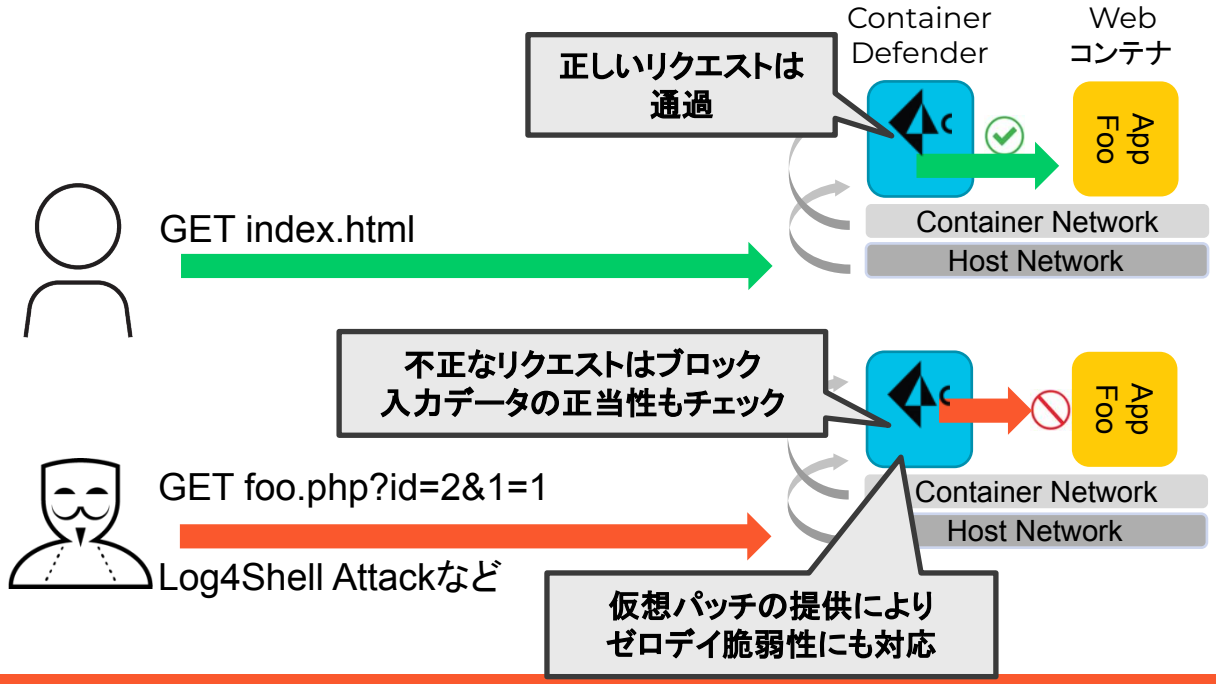


ここがすごいランタイム防御 – 振舞い学習により、アプリへの不正行為をブロック



Web Application & API Security (WAAS) –
Webサーバーへの不正行為、ゼロデイ脆弱性のブロック

OWASP Top 10準拠の防御(WAF)だけでなく入力データ検査 (RASP)などより高度な防御機能

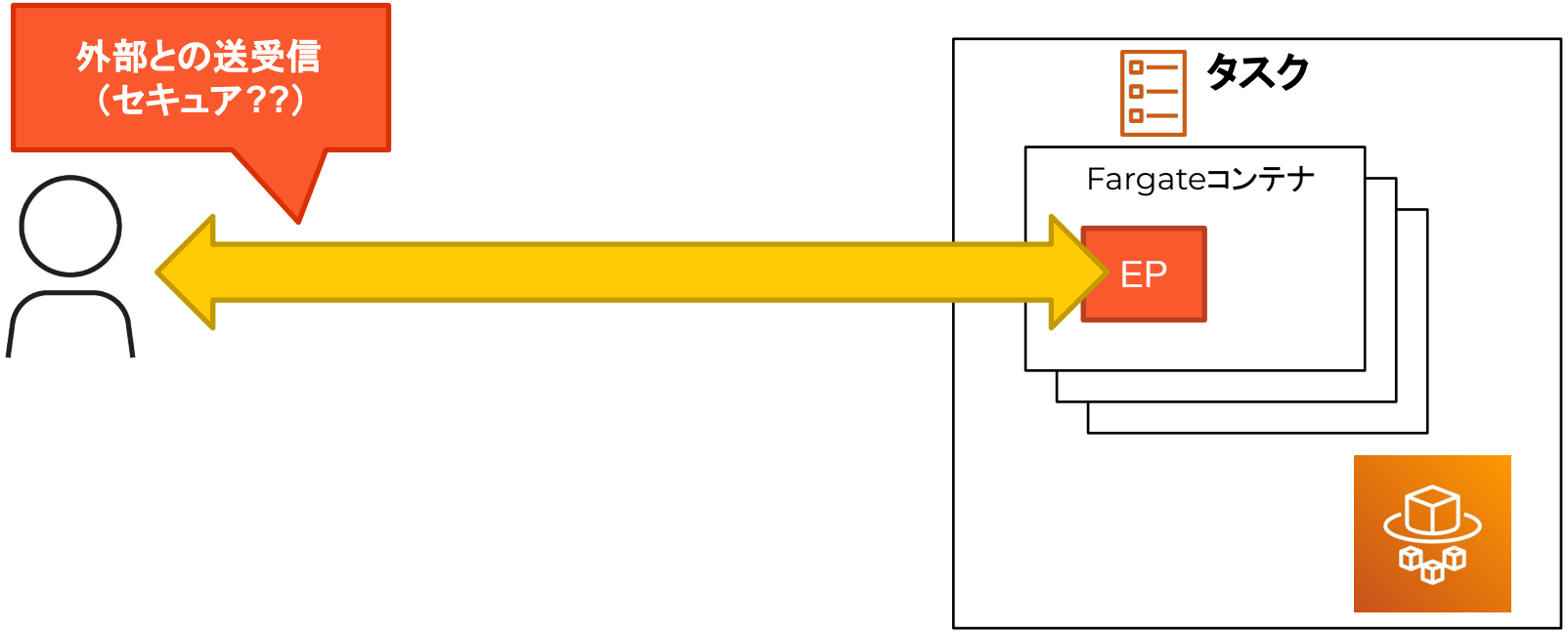


OWASP Top 10等に
対応した保護機能

- SQL Injection
- Cross-Site Scripting
- OS Command Injection
- Code Injection
- Local File Inclusion
- Attack Tools & Vuln Scanner
- Shellshock
- Malformed HTTP Request
- Cross Site Request Forgery
- Clickjacking

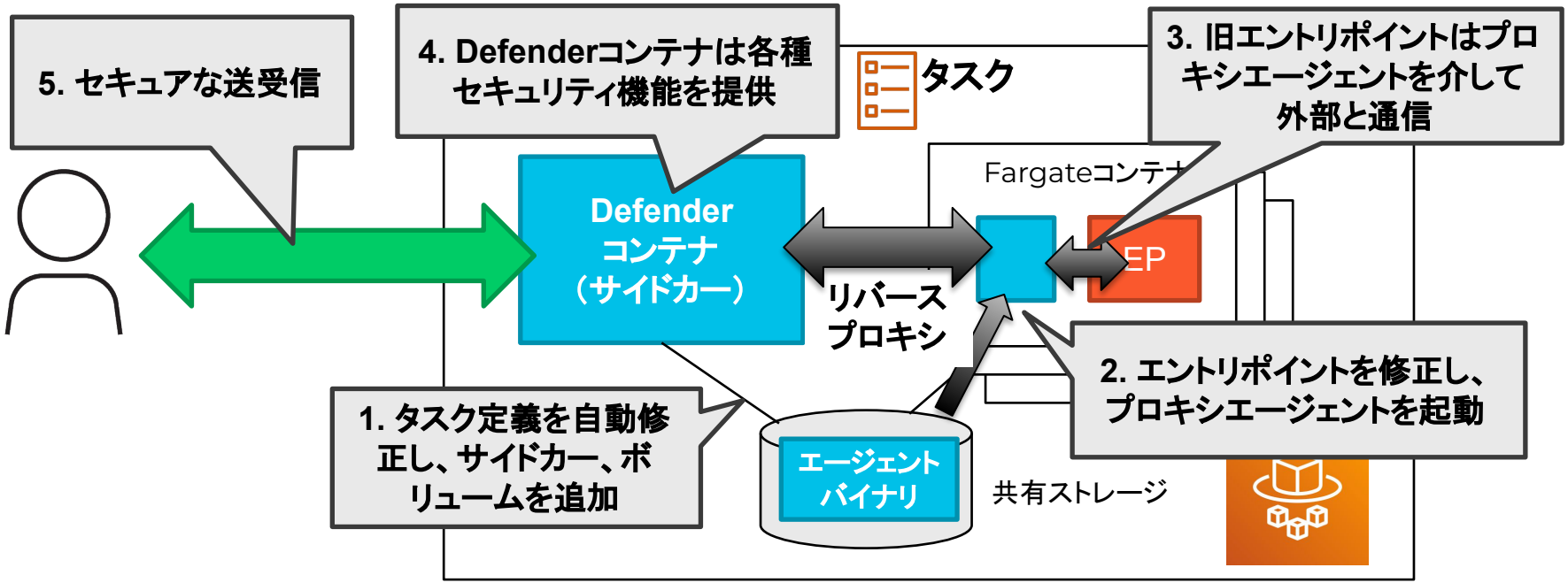
- DoS **防御**
- **ボット防御**
- **仮想パッチ（ゼロデイ防御）**
- **不正IP、ヘッダー**
- **ファイルアップロード**

AWS Fargate – 従来型のセキュリティ対策が困難



ここがすごい – AWS Fargateにも対応※

サイドカーコンテナとして動作し、WAAS・ランタイム防御



※現時点では若干機能制限がありますが、近日中にフル機能をサポート予定

イメージスキャン機能 – コンプライアンス、脆弱性、マルウェア等を検出、スコア化

元イメージが安全で
あるという保証はない！

プライベート
レジストリ

パブリック
レジストリ

多様なレジストリに対応
AWS ECR/Docker Hub/
OpenShift/Harbor/JFogなど

レジストリ上のイメージをスキャンし、脆弱性、マルウェア、秘密情報等を検出

Repository	Provi...	Vulnerabl...	Vulnerabilities	Risk Factors
ppradnesh/gradle	GitHub	56	10 26 44 34	10
contiv/testing	GitHub	1	3 3	8
ppradnesh/neowal1	GitHub	6	3 2	6
ppradnesh/kubernetes	GitHub	1	7 3 5	7
contiv/aci_django_port	GitHub	1	2 2	6

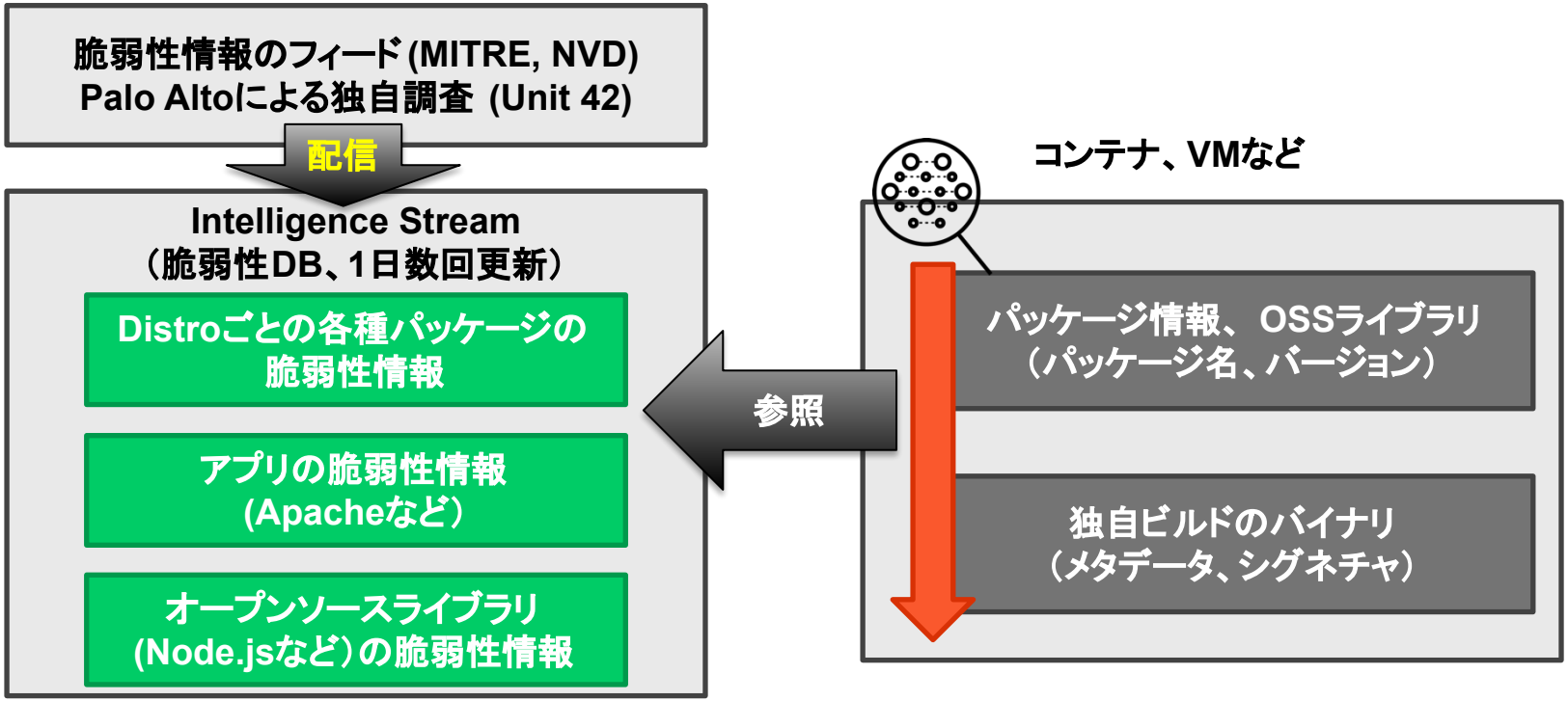
Binary critical node version 4.8.0 has 9 vulnerabilities.

Severity	Package	CVE	Fix status	Grace period	Risk factors	Description	Tags
critical	node	CVE-2016-6303	Fixed in: 1.1.0	>4 years ago	5	Impacted versions: <=6.6.0 Discovered: >4 months ago Published: >4 years ago	In progress x, For review x, DevOps notes x, Add Tags to CVE

 |

ここがすごい – 非常に広範かつ最新の脆弱性検出のしくみ

パッケージに加えビルドしたアプリ、オープンソースライブラリの脆弱性を検出



検出可能な脆弱性

- **Linux**
  - Amazon Linux 2
  - Alpine
  - Debian
  - Photon
  - RHEL/CentOS
  - Ubuntu
- **Windows**
  - Windows Server 2016/2019
- **オープンソース ライブラリ**
  - Ruby (Gem)
  - Node.js
  - Java (jar)
  - Python
- **アプリケーション※**
  - Apache
  - ElasticSearch
  - HAProxy
  - Kibana
  - MariaDB
  - MongoDB
  - MySQL
  - Nginx
  - PostgreSQL
  - RabbitMQ
  - Redis
  - Tomcat
  - WordPress
  - BusyBox など

※最新情報は下記 URLを参照してください
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/technology_overviews/app_specific_network_intelligence

Prisma Cloudでコンテナイメージを調べてみると

- イメージ
  - Nginx: latest
  - CentOS: latest
  - Ubuntu: latest
  - Debian: latest

Latestイメージでも脆弱性はそれなりにある

yum, apt-getなどで常に最新に！

Repository	Tag	Vulnerabilities	Risk factors
centos	latest	13 86 15	10
debian	latest	28 11	8
nginx	latest	40 3	8
ubuntu	latest	13	6

アップデート後の脆弱性は？

- それぞれのコンテナ上で以下を実行
- CentOS
  - `$ yum update`
- CentOS以外
  - `$ apt-get update`
  - `$ apt-get dist-upgrade`

改善された！

パブリック イメージをそのまま使うのではなく、更新したイメージを使うべき！

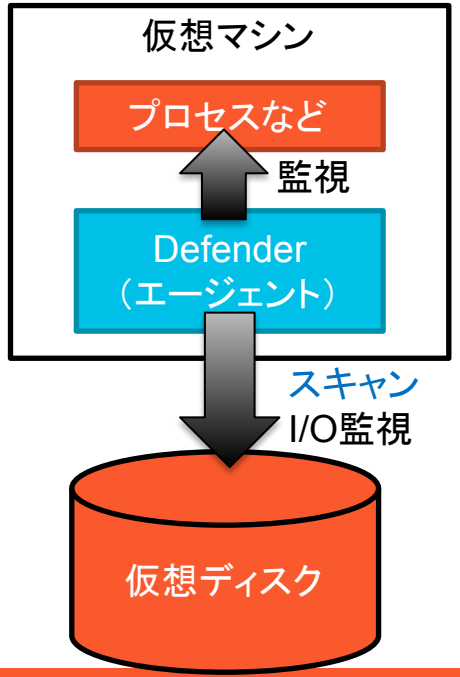
Repository	Tag	Vulnerabilities
centos	latest	13 86 15
debian	latest	28 11
nginx	latest	40 3
ubuntu	latest	13

Vulnerabilities	Risk factors
9 21	6
28 1	6
38 3	6
11	5

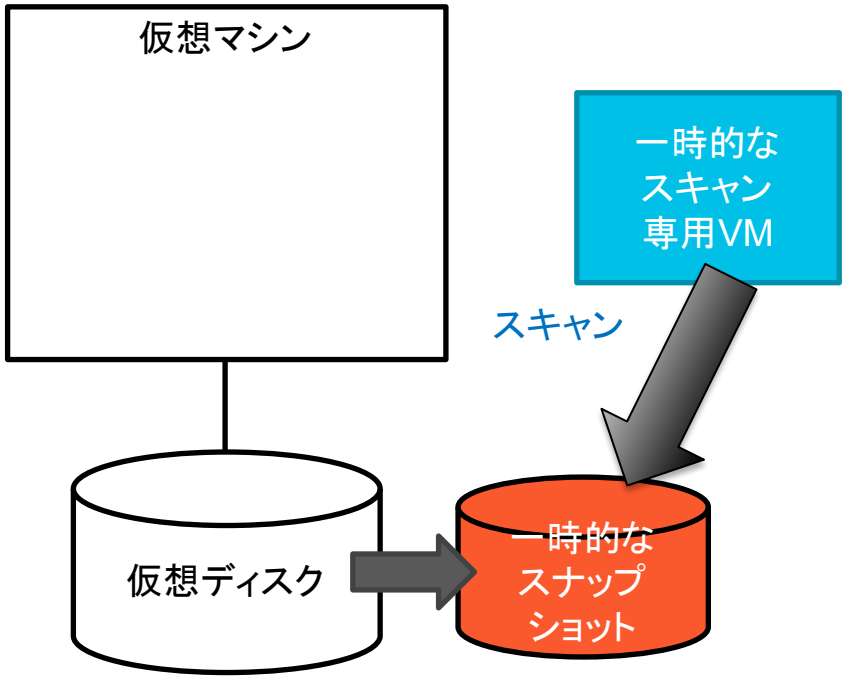
ここがすごい – 仮想マシン脆弱性のエージェントレススキャン

仮想マシンのパフォーマンスに影響を与えないで脆弱性の検査が可能

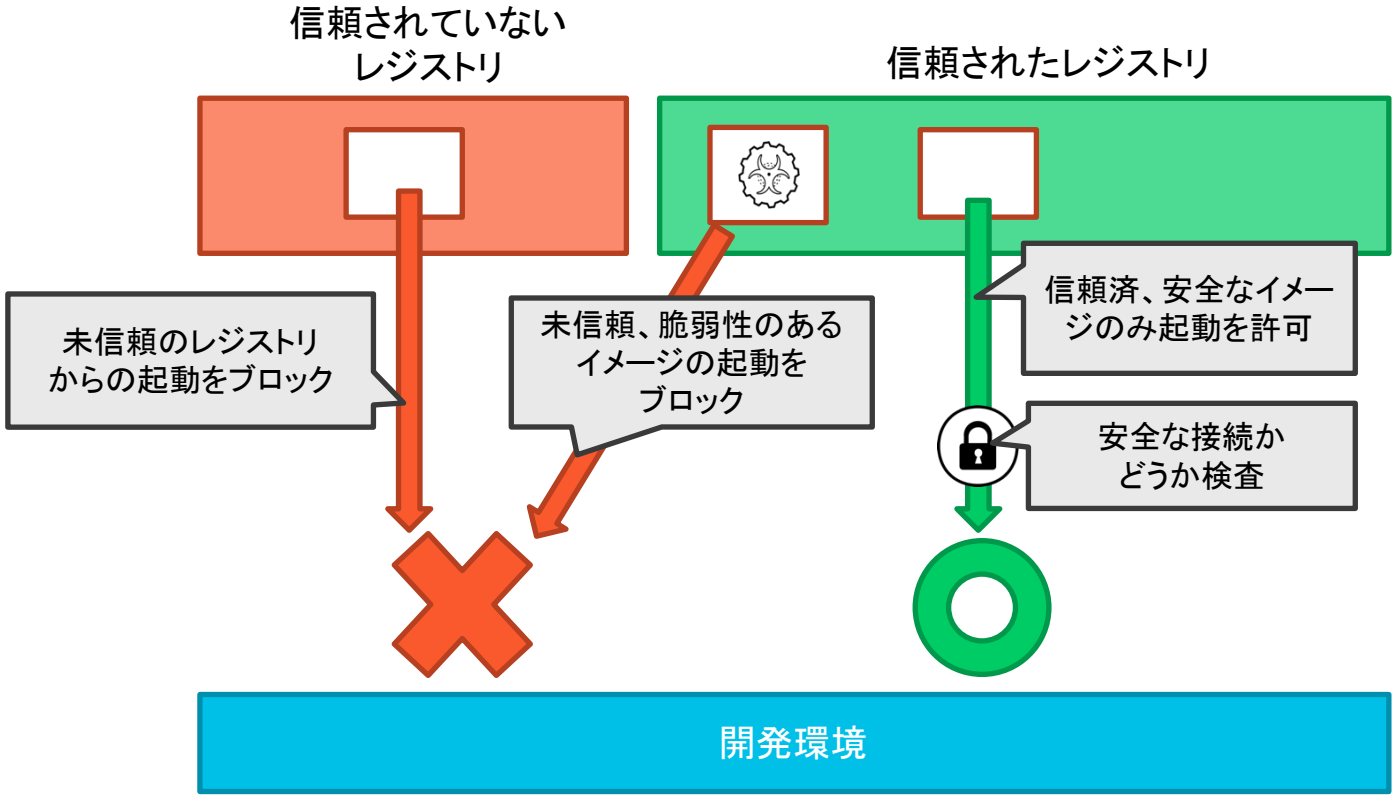
- **オプション1: エージェントあり**
  - 脆弱性スキャン、ランタイム防御、WAAS



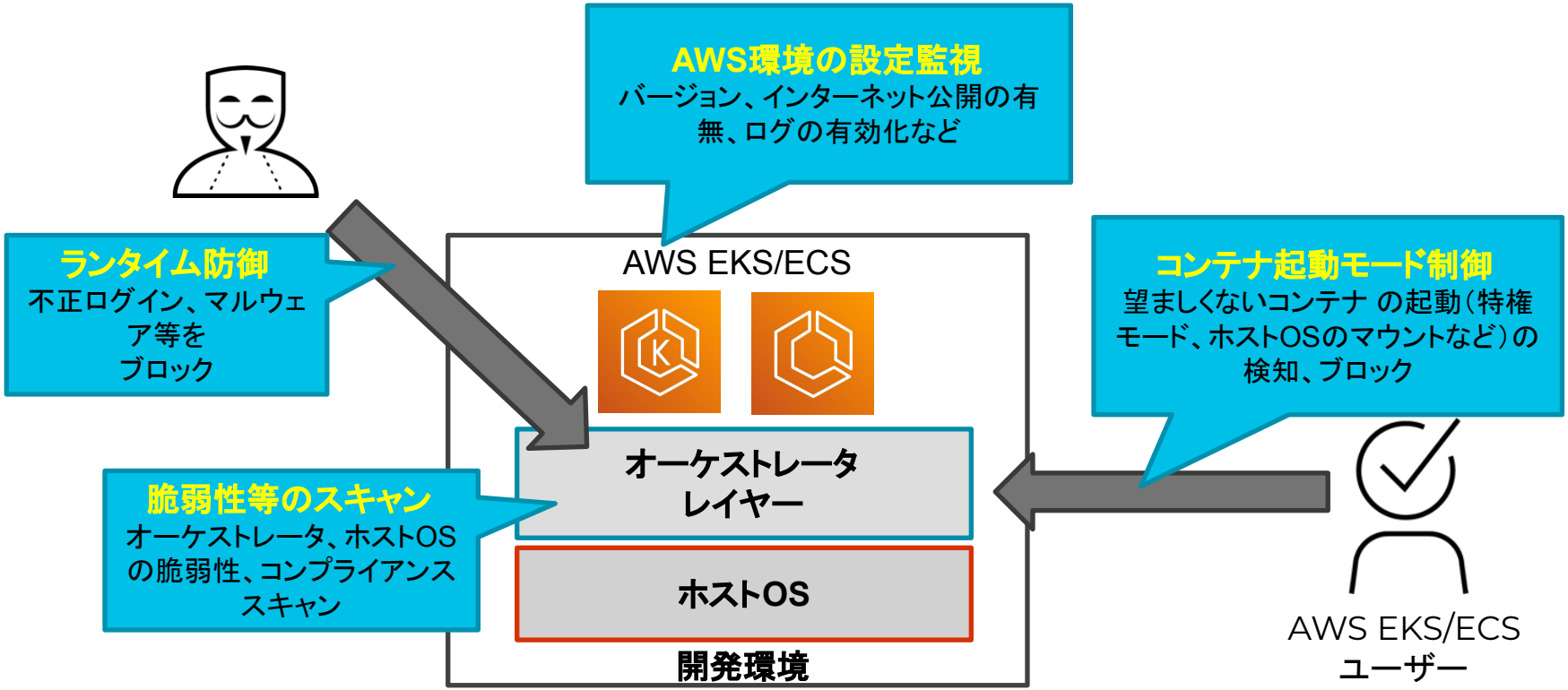
- **オプション2: エージェントレス**
  - 脆弱性スキャンのみ



レジストリ、イメージ信頼性 – 信頼されたもののみコンテナ実行を許可



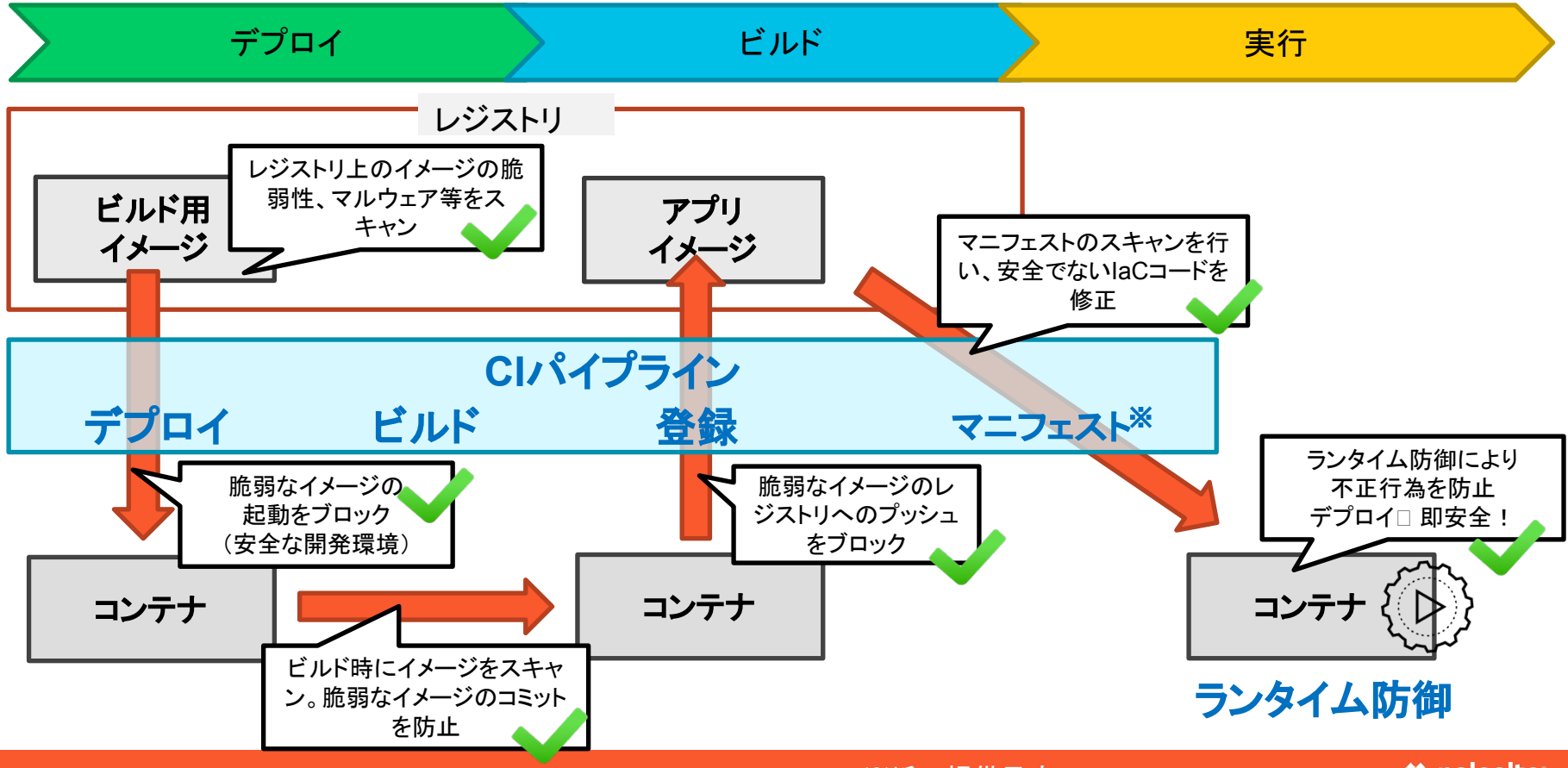
ホストOS、オーケストレータの保護、不適切なコンテナ起動の防止



 |

※ Dockerのみ対応

CIツール連携 – 開発ライフサイクルのあらゆるステップでセキュリティを実施



※近日提供予定

 |

監視：インシデントの自動生成 – AIにより不正な活動を自動検知しアラート

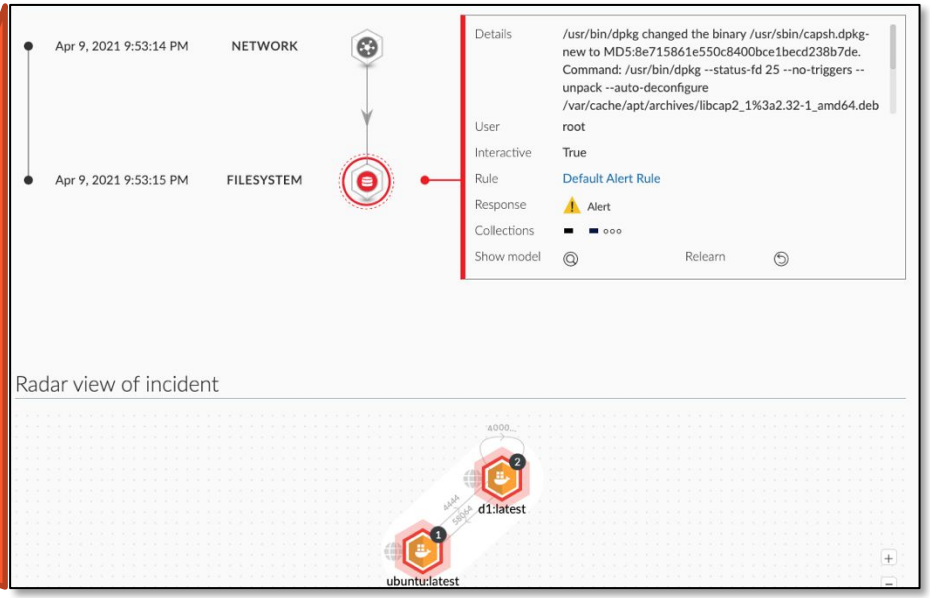
繰り返し学習

異常なイベント

監査、分析

インシデント自動生成

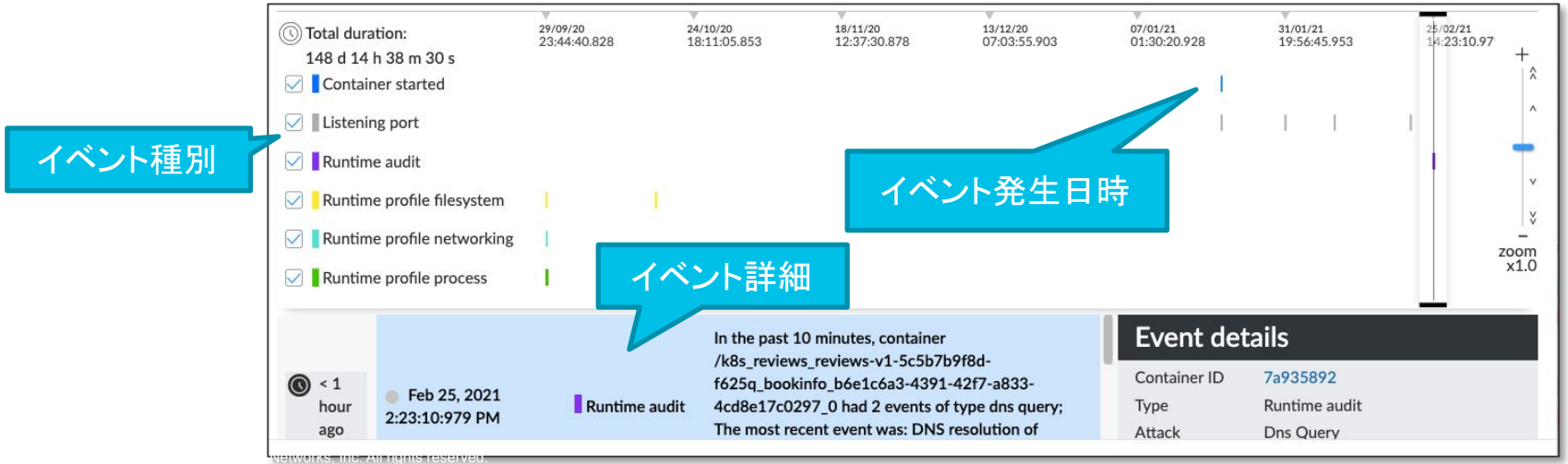
フォレンジック



 |

フォレンジック – ワークロード上の主要なイベントをログ、可視化

- **対応イベントの種別**
  - **プロセスの実行** – タイムスタンプ、コンテナID、PID、PPID、パス、コマンド、引数
  - **コンテナの起動** – タイムスタンプ、コンテナID
  - **バイナリの生成** – 実行形式もしくはバイナリBlobの生成（タイムスタンプ、ユーザー、パスなど
  - **ポートのリッスン** – 実行形式へのパス、開始時間、ポート番号など
  - **コネクションの確立** –タイムスタンプ、送信元、先、ポート
  - **ランタイムプロファイル** – 学習モード時に許可されたアクション（タイムスタンプ、PID、パス、コマンドなど
  - **ランタイム監査** – ランタイムポリシー（ML＋ルール）に違反したイベントの発生（ユーザー、監査メッセージ、攻撃タイプ、効果など

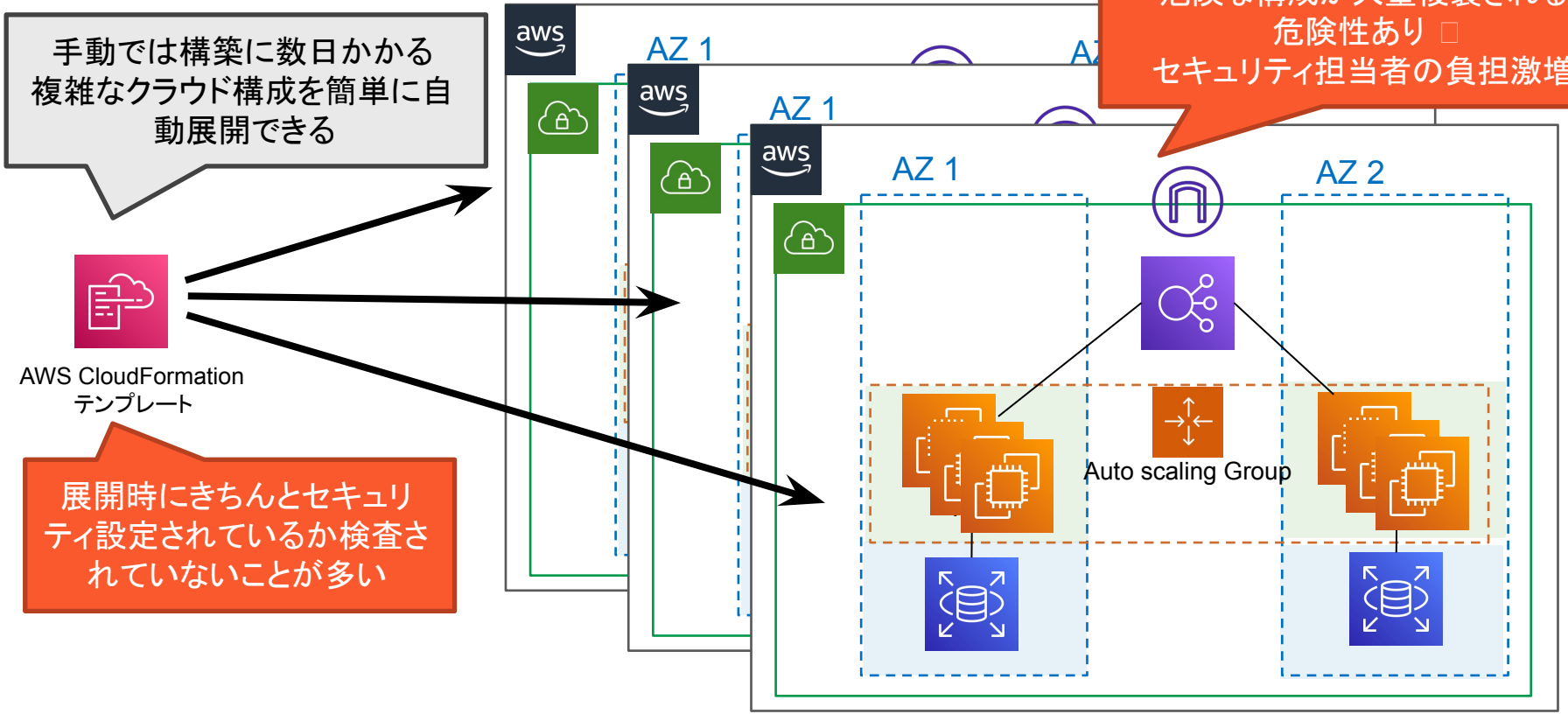


クラウド コード セキュリティ
IaCへのセキュリティ対策

IaC(Infrasture as Code)のメリットとセキュリティの考慮点

手動では構築に数日かかる
複雑なクラウド構成を簡単に自動展開できる

危険な構成が大量複製される
危険性あり
セキュリティ担当者の負担激増



AWS CloudFormation
テンプレート

展開時にきちんとセキュリティ設定されているか検査されていないことが多い

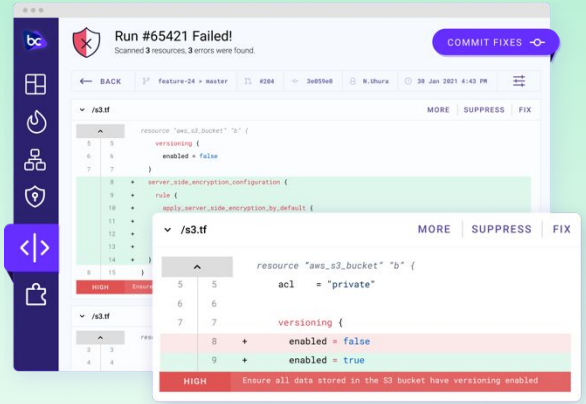
 |

IaCの実際 – 各ステップと課題

- **コード開発時の課題**
  - 開発に手間がかかる
  - 修正が多い
  - セキュリティを考慮する余裕なし
- **実行時の課題**
  - 適切な構成とのずれ（ドリフト）が頻発
  - ドリフトが可視化できず、修復が難しい

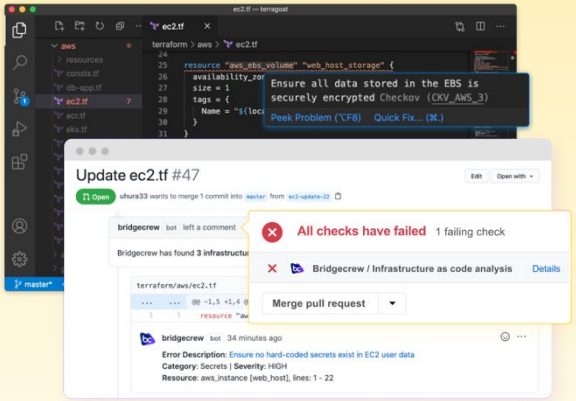
DevOpsライフサイクル全体にインフラストラクチャセキュリティを組み込む

継続的なカバレッジと修正



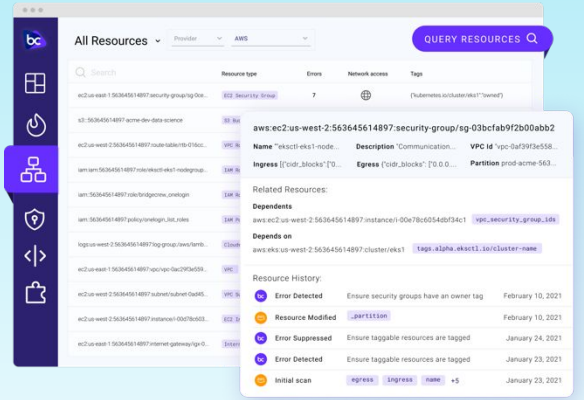
- セキュリティとコンプライアンスのベンチマーク全体で数百の組み込みポリシーを備えた、最速で最もサポートされているIaCスキャナー
- 直感的なUIにより、開発者のエクスペリエンスが合理化され、修正にかかる時間を短縮

開発者ツールと統合



- **IDE(統合開発環境)拡張機能**と完全に拡張可能なCLIにより、早期のローカルスキャンが可能に
- **ネイティブVCS(バージョン管理システム)と CI/CD連携**により、DevOpsライフサイクルの各ステップを通じてセキュリティガードレールを有効化

ランタイム分析とドリフト検出



- 独自のグラフベースのフレームワークにより、コンテキストを理解したフィードバックを提供
- ビルド時およびランタイムスキャンのネイティブサポートにより、クラウドリソースとIaC構成間のドリフト検出が可能に

Thank you!

西田 和弘

パロアルトネットワークス株式会社
技術本部
パブリッククラウド スペシャリスト システムズ エンジニア