AWS オンラインセミナー

中級者向けセキュリティ勉強会

ランサムウエア対策特別編

Yuki Yoshida

セキュリティ勉強会について

セキュリティをテーマに定期開催しています。

- 初級編
  - アカウント保護の考え方
  - セキュリティを担保するうえで考慮すべきポイント
  - NIST Cyber Security Framework
  - 検知のためのセキュリティサービス

- 中級編
  - アーキテクチャに合わせた防御の検討
  - セキュリティ運用の効率化について

- ランサムウェア勉強会
  - **今回実施の内容** 

- ランサムウェア勉強会 workshop編
  - 開催企画中

今後の勉強会も参加を希望される場合は
アンケートに参加希望の旨ご記入ください

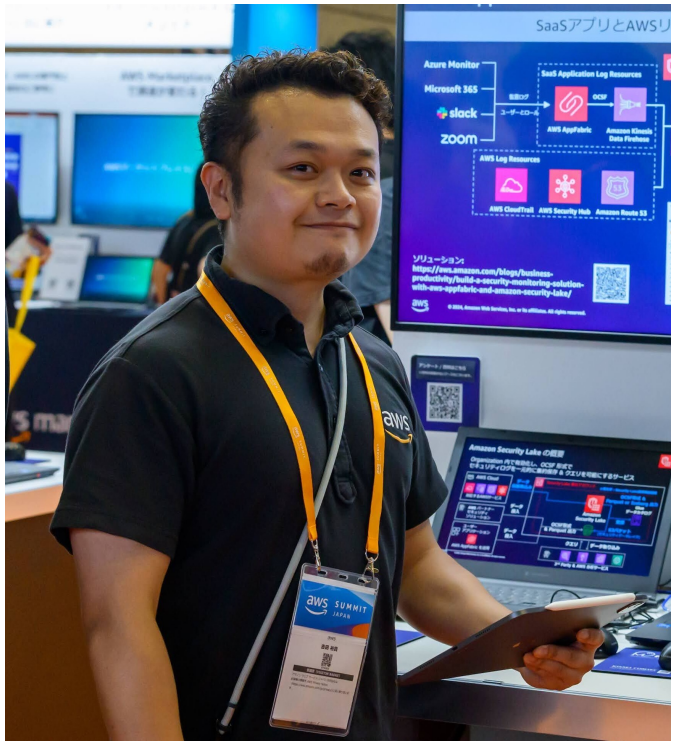
自己紹介

名前: 吉田 裕貴 (よしだ ゆうき)
所属: アマゾンウェブサービスジャパン合同会社
ISV/SaaS Solutions Architect

好きな技術領域: セキュリティ、運用の効率化

趣味: 筋トレ、バイク、旅

見習いハンター



What is Ransomware?

ランサムウエアとは

昨今話題になる「ランサムウエア」とは以下のような不正なプログラムを指します。

ランサムウエアとは、「Ransom(身代金)」と「Software(ソフトウェア)」を組み合わせた造語

- 感染したパソコンに特定の制限をかけ、その制限の解除と引き換えに金銭を要求する 不正なプログラム (=マルウエア)

2015 年以降、パソコンに保存されているファイルを暗号化し復号のための金銭を要求するランサムウエアが多く確認されている

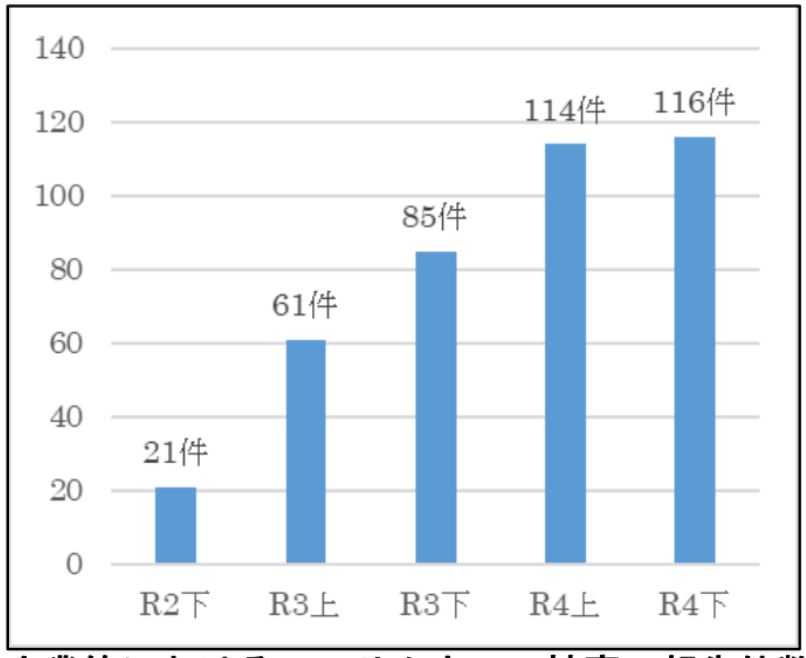
ランサムウエア対策特設ページ(IPA)
https://www.ipa.go.jp/security/anshin/measures/ransom_tokusetsu.html

情報セキュリティ 10 大脅威

順位	組織に対する 10 大脅威	掲載回数
1	**ランサムウエアによる被害**	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	6年連続6回目
3	内部不正による情報漏えい等の被害	9年連続9回目
4	標的型攻撃による機密情報の窃取	9年連続9回目
5	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	3年連続3回目
6	不注意による情報漏えい等の被害	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	4年連続7回目
8	ビジネスメール詐欺による金銭被害	7年連続7回目
9	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年連続4回目
10	犯罪のビジネス化(アンダーグラウンドサービス)	2年連続4回目

情報セキュリティ 10 大脅威 2024(IPA)
https://www.ipa.go.jp/security/10threats/10threats2024.html

国内のランサムウェアの被害報告数は増加傾向、事業継続に影響を及ぼす事案も発生している



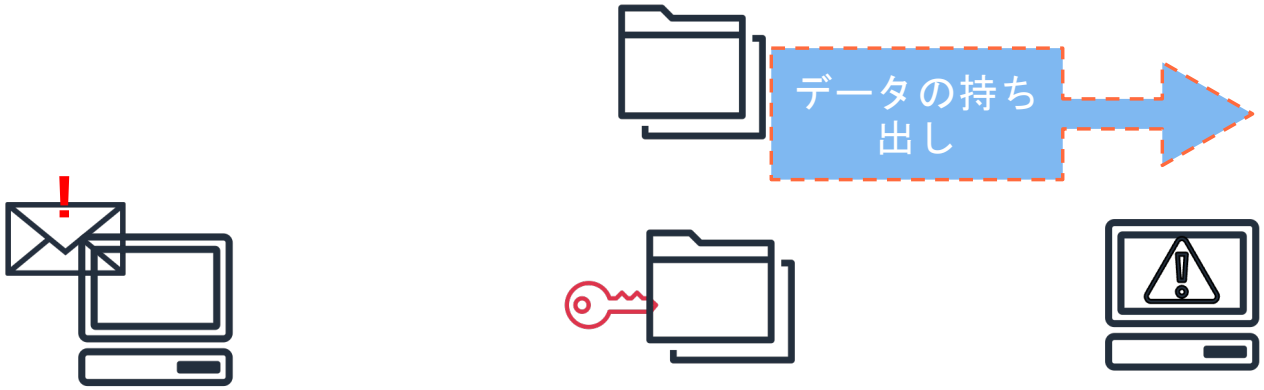
企業等におけるランサムウェア被害の報告件数

警察庁サイバー警察局：サイバー事案の被害の潜在化防止に向けた検討会報告書2023
https://www.npa.go.jp/bureau/cyber/pdf/20230406_2.pdf

日本国内でランサムウェアが事業継続に影響を及ぼした事例：

- 港湾物流管理システムの被害 (2023年7月)
- 工場の生産管理システム（2023年3月）

ランサムウエアによるファイルの暗号化



何らかの方法で侵入

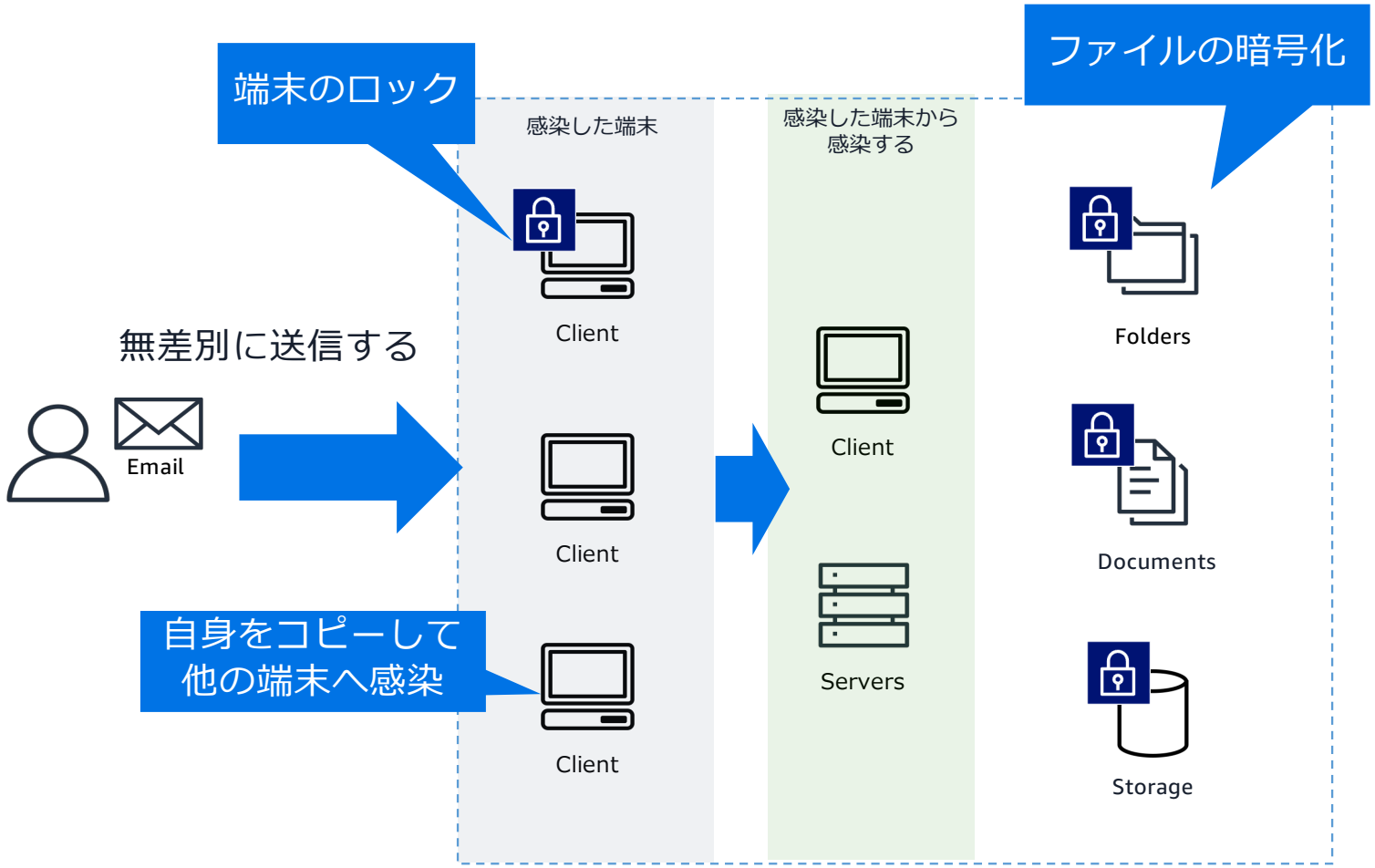
ランサムウエアに感染

感染した端末上のファイルを暗号化する

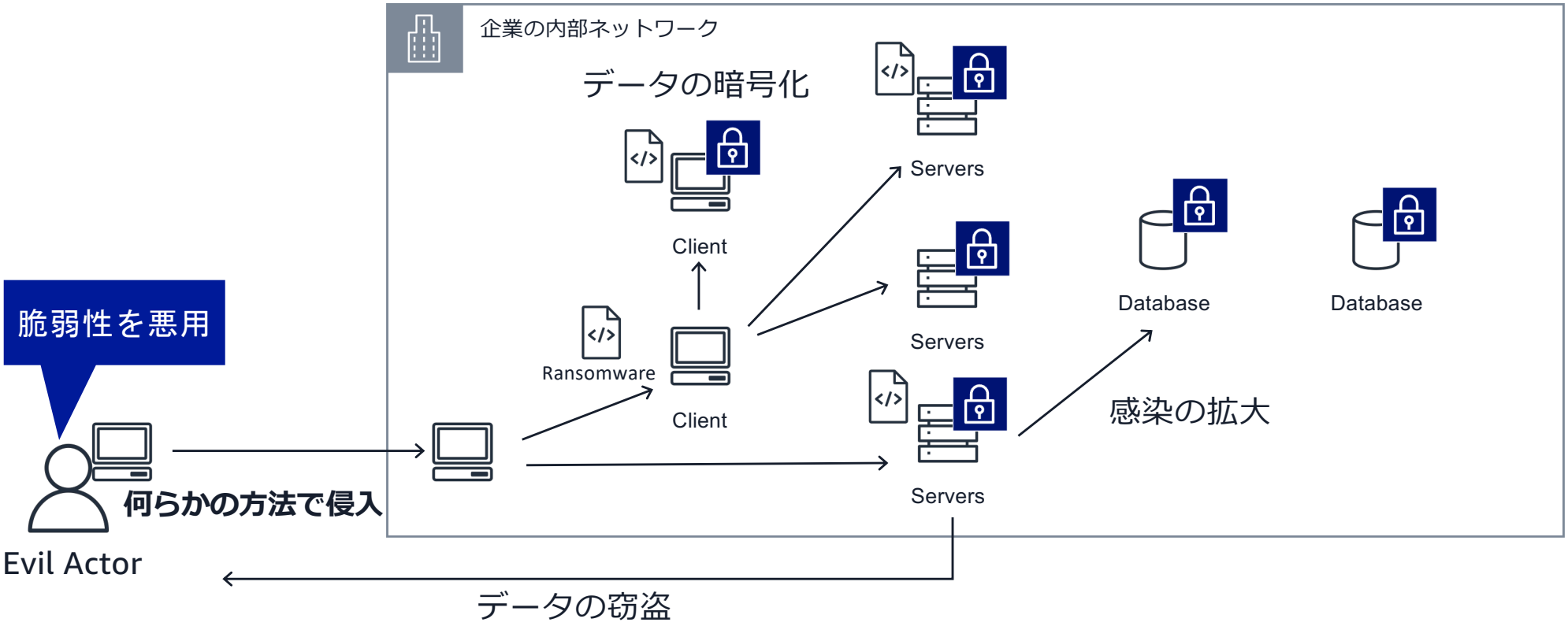
端末に脅迫メッセージを表示

感染した不正プログラムが端末上のファイルを暗号化し、暗号化されたファイルを復号する代わりに金銭を支払うように要求する

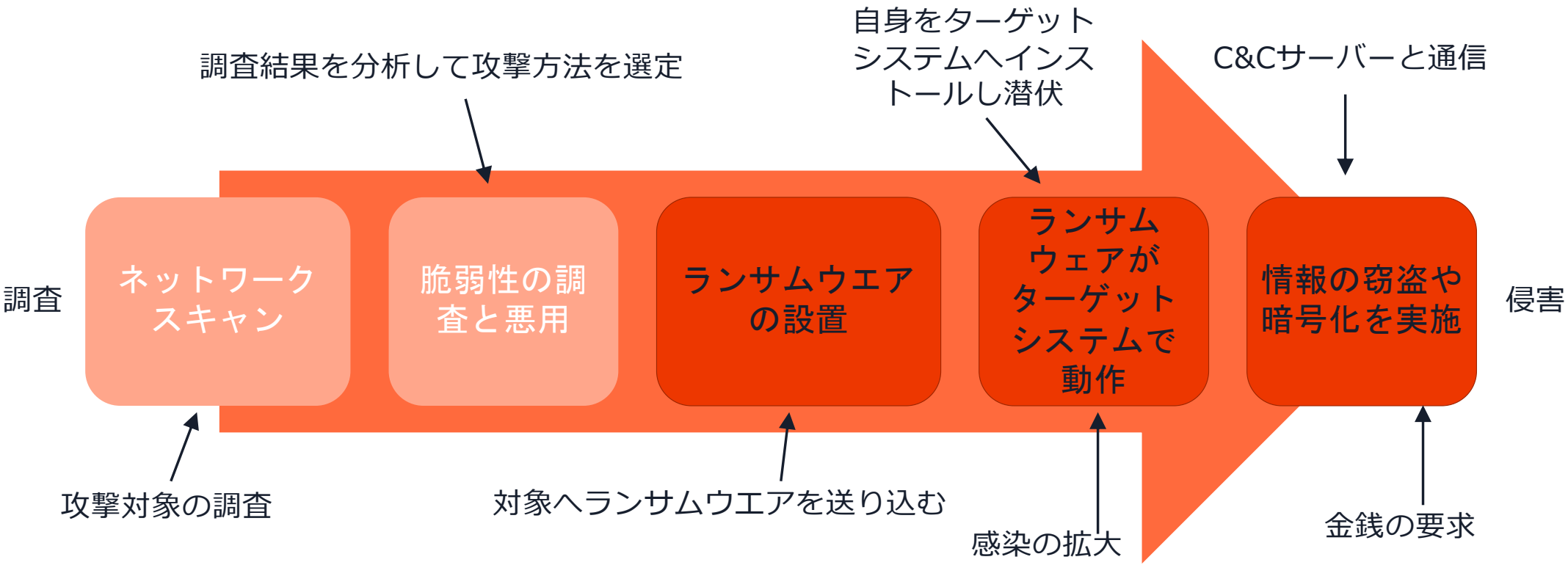
伝統的なランサムウエアの感染経路（例）



ネットワークを介して感染するランサムウエアの感染経路（例）



標的を絞ったランサムウエアの感染経路

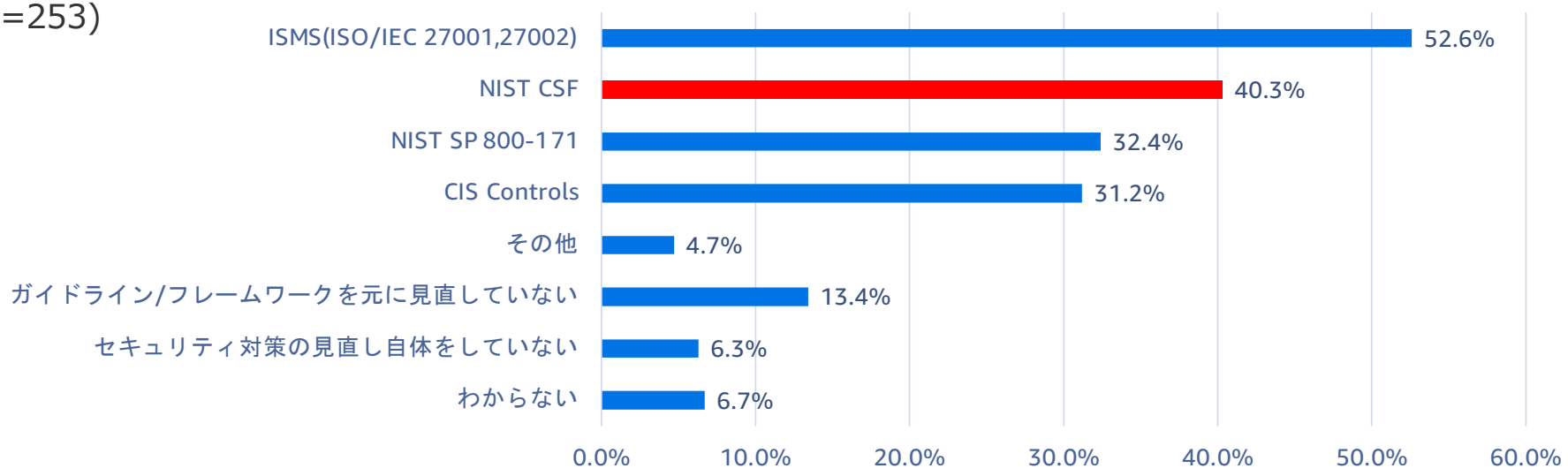


対象を調査し、脆弱な部分を利用して攻撃を仕掛けます。
つまり、これは**標準的なサイバー攻撃と同様の感染経路**

「一般的なサイバー攻撃への対策」は十分でしょうか？

セキュリティ対策の参考にするガイドライン

質問「次のガイドライン/フレームワーク/文書を参考に自組織のセキュリティ対策を見直していますか?」（複数回答）
(n=253)



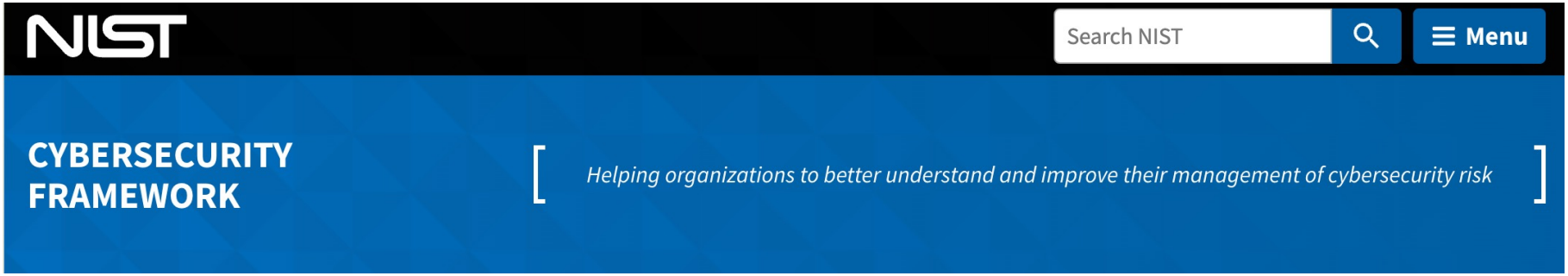
出所：トレンドマイクロ「法人組織のセキュリティ成熟度調査」を基に作成

セキュリティのガイドラインに則している

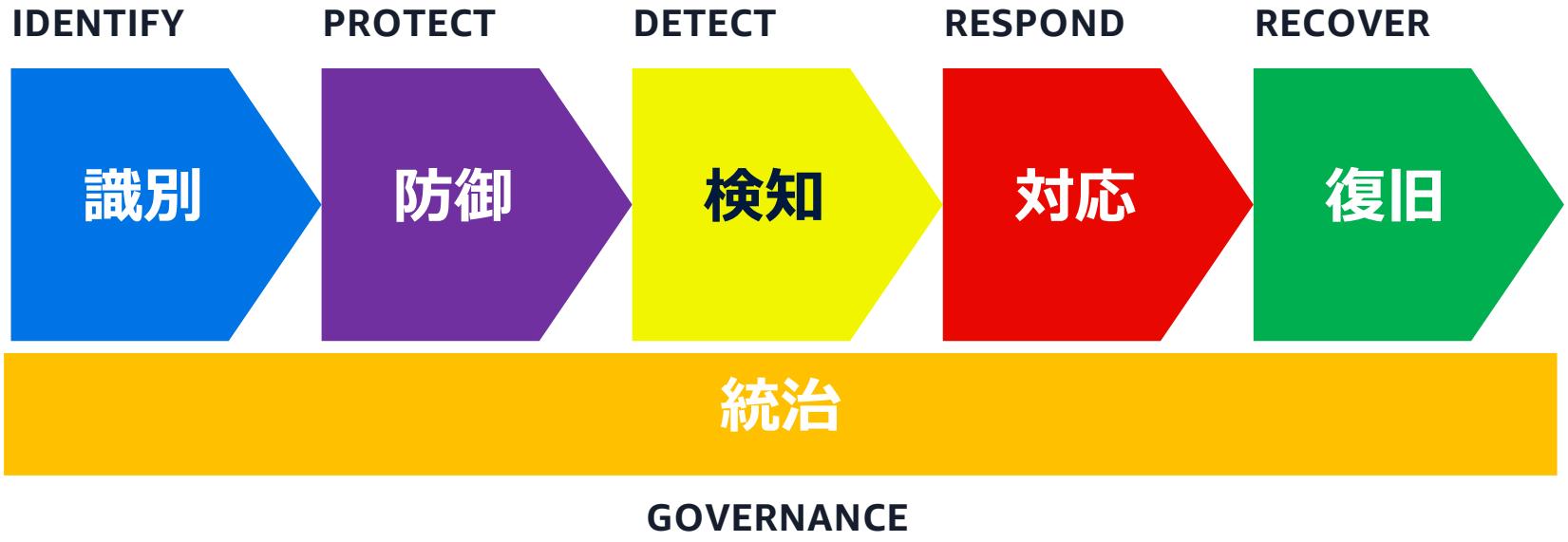
これは、一般的なサイバー攻撃への対策のステークホルダーに対する説明になる

NIST CyberSecurity Framework (CSF)

- 元々はオバマ政権時代にアメリカの重要インフラのサイバーセキュリティを強化するために発令された大統領令を受け作成されたガイドライン
- リスク軽減策の確立において汎用的な内容となっているため、現在は様々な国や組織で利用されている



NIST CyberSecurity Framework (CSF)

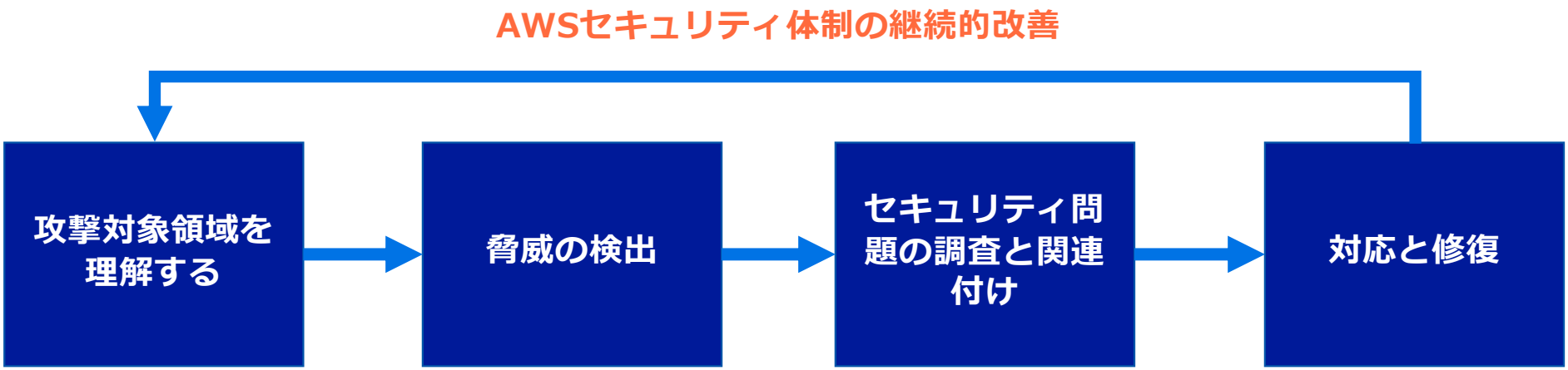


AWS サービスのカテゴライズ

IDENTIFY	PROTECT		DETECT	RESPOND	RECOVER
AWS Security Hub	Amazon VPC	AWS Transit Gateway	AWS Security Hub	Amazon CloudWatch	AWS Backup
AWS Control Tower	AWS Key Management Service (KMS)	AWS Private Link	Amazon GuardDuty	AWS CloudTrail	AWS Elastic Disaster Recovery
AWS Organizations	AWS Secrets Manager	AWS Direct Connect	Amazon Macie	Amazon Detective	AWS CloudFormation
AWS Trusted Advisor	AWS Firewall Manager	AWS Resource Access Manager	Amazon Inspector	Amazon Route 53	Amazon S3
AWS Service Catalog	AWS Identity and Access Management (IAM)	Amazon Cloud Directory		AWS Systems Manager	Amazon S3 Glacier
AWS Config	AWS Shield	AWS Directory Service		AWS Step Functions	Snapshot
AWS Systems Manager	AWS IoT Device Defender	AWS Secrets Manager		AWS Lambda	
AWS Well-Architected Tool	AWS IAM Identity Center	AWS Certificate Manager (ACM)		AWS Personal Health Dashboard	
	AWS WAF	AWS CloudHSM			
	AWS Network Firewall	Amazon Cognito			

※NIST Cyber Security Framework をもとに AWS サービスをカテゴライズしたもの

AWSの継続的なセキュリティ監視



Inspector
CVEスキャン
OSレベルの設定

Macie
データ分類

Security Hub
リソース/アカウントレベルの設定

NIST CSF function:
IDENTIFY

GuardDuty
インテリジェントな脅威の自動検出

NIST CSF function:
DETECT

Detective
セキュリティ調査

Security Hub
アラートの集約

NIST CSF function:
DETECT RESPOND

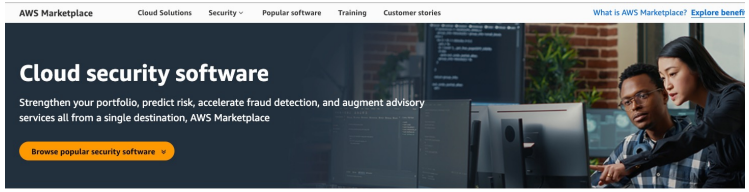
Security Hub
自動化された修復アクションの実行

NIST CSF function:
RESPOND RECOVER

NIST CSF functions covered by other AWS services:
- **PROTECT - AWS Identity and Access Management (IAM)、暗号、エッジ保護サービスなど**
- **RECOVER – AWS Backup**

AWS のパートナーソリューション

AWS Marketplace



Maintain a secure environment with security tools and cloud security software in AWS Marketplace

Whether you are securing endpoints, identifying vulnerabilities, or safeguarding sensitive data, you can find the security software and security tools you need on AWS Marketplace to enhance protection for your entire Amazon Web Services (AWS) environment with compatible security solutions.

AWS WAF デリバリーパートナーは、セキュリティを危険にさらしたり、アプリケーションの可用性に影響を与えたり、過剰なリソースを消費したりする可能性のある、一般的なウェブの脆弱性からウェブアプリケーションを保護するための、AWS WAF の実装を行う AWS パートナーです。AWS WAF デリバリーパートナーと協力することで、ウェブアプリケーションのセキュリティを強化し、SQL インジェクションやクロスサイトスクリプティングなどの一般的な攻撃パターンをブロックするカスタムルールを作成できます。

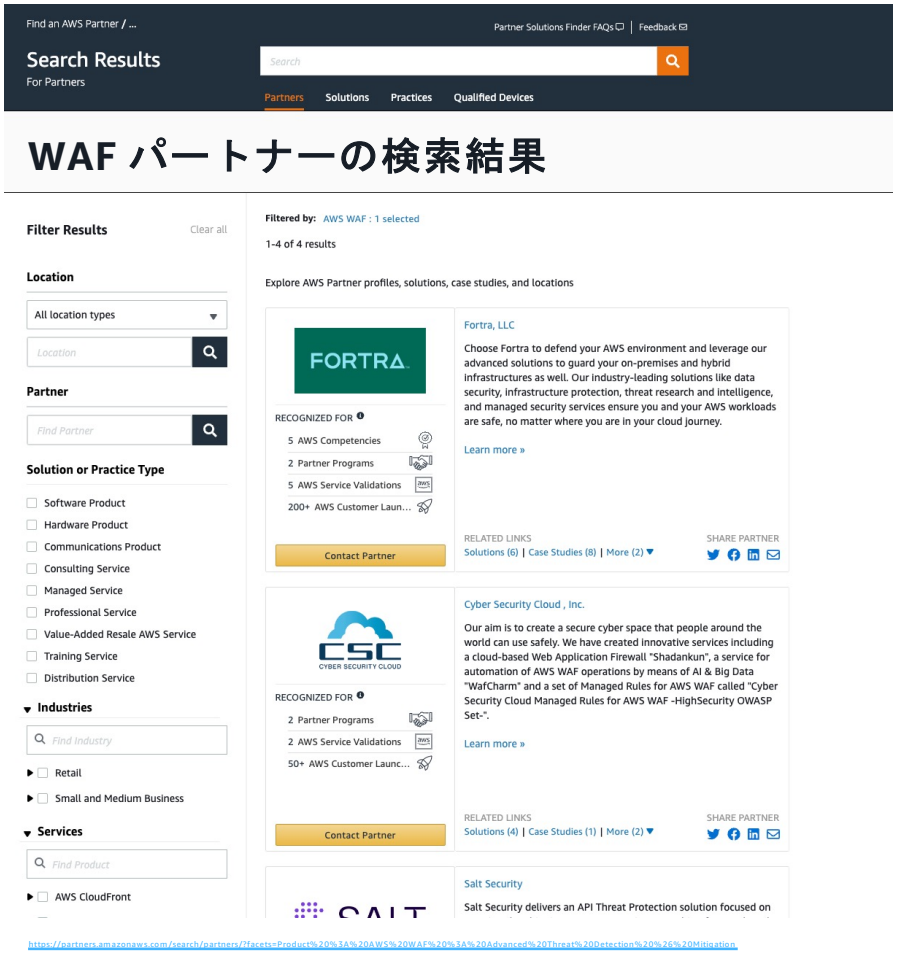
AWS WAF Ready パートナーは、アプリケーション層のセキュリティソリューションのデプロイと維持のためのシンプルなソリューションをお客様に提供します。AWS WAF Ready ソフトウェア製品は、堅牢な WAF ルールセットと緩和ツールを提供し、お客様は特定のアプリケーションのユースケースに応じて選択することができます。

AWS Service Delivery と AWS Service Ready プログラムは、個別の AWS のサービスやソフトウェアソリューションに関する経験と深い理解がある AWS パートナーを AWS のお客様が特定できるようにするサービスです。これらのパートナーは、AWS WAF のベストプラクティスに従っていることを確認するための厳格な技術検証に合格しており、また、お客様からの実績も実証されています。

aws partner network | service delivery

AWS ISV Accelerate

https://aws.amazon.com/jp/waf/partners/?pg=cpg&sec=cat&cp=tb&blog-posts-cards.sort-by=item.additionalFields.modifiedDate&blog-posts-cards.sort-order=desc



https://partners.amazonaws.com/search/partners/?facets=Product%20%3A%20AWS%20WAF%20%3A%20Advanced%20Threat%20Detection%20%26%20Mitigation

データ保護の実践

重要なデータを特定する

データへのアクセスを管理・制御する
データの暗号化を導入する
自動化されたデータ保護を導入する

データガバナンスとコンプライアンスの実践
モニタリングとアラートの導入

バックアップと復旧手段の計画
DR・BCPのプラン策定

ランサムウェア復旧手段の計画

AWS サービスのカテゴライズ

IDENTIFY	PROTECT		DETECT	RESPOND	RECOVER
AWS Security Hub	**Amazon VPC**	AWS Transit Gateway	AWS Security Hub	Amazon CloudWatch	**AWS Backup**
AWS Control Tower	AWS Key Management Service (KMS)	AWS Private Link	**Amazon GuardDuty**	AWS CloudTrail	AWS Elastic Disaster Recovery
AWS Organizations	AWS Secrets Manager	AWS Direct Connect	Amazon Macie	Amazon Detective	AWS CloudFormation
AWS Trusted Advisor	AWS Firewall Manager	AWS Resource Access Manager	**Amazon Inspector**	**Amazon Route 53**	Amazon S3
AWS Service Catalog	AWS Identity and Access Management (IAM)	Amazon Cloud Directory		**AWS Systems Manager**	Amazon S3 Glacier
AWS Config	AWS Shield	AWS Directory Service		AWS Step Functions	Snapshot
AWS Systems Manager	AWS IoT Device Defender	AWS Secrets Manager		AWS Lambda	
AWS Well-Architected Tool	AWS IAM Identity Center	AWS Certificate Manager (ACM)		AWS Personal Health Dashboard	
	AWS WAF	AWS CloudHSM			
	AWS Network Firewall	Amazon Cognito			

※NIST Cyber Security Framework をもとに AWS サービスをカテゴライズしたもの

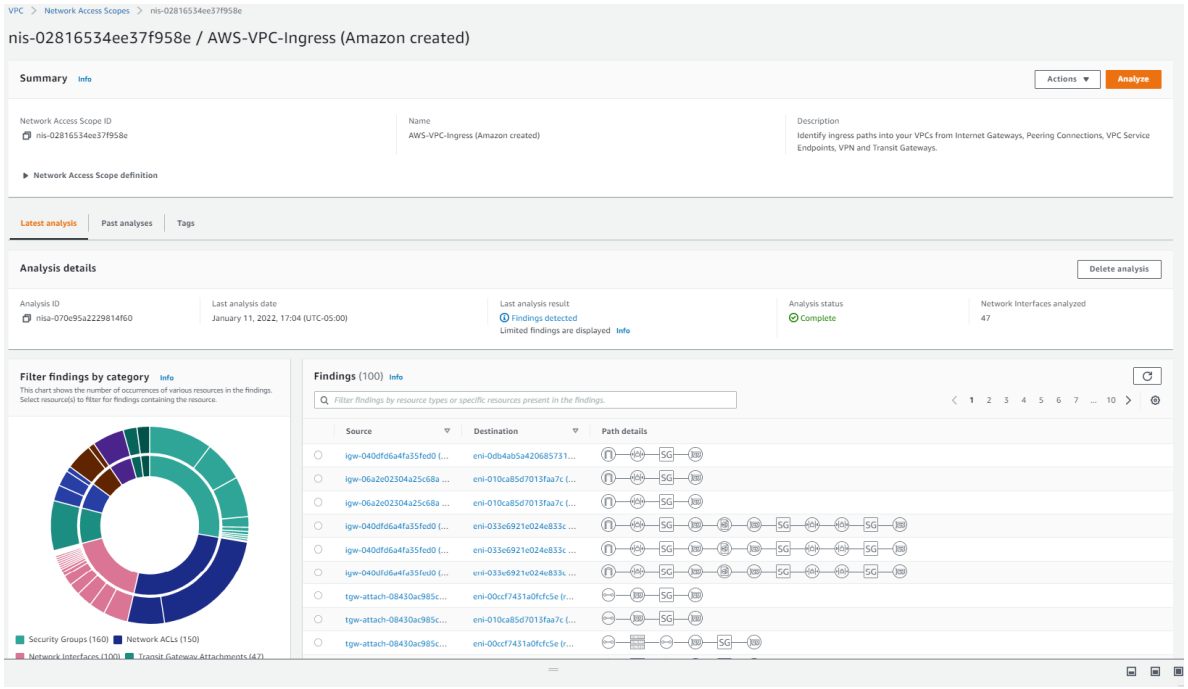
Amazon VPC Network Access Analyzer

Amazon VPC Network Access Analyzer

AWS上のリソースへの意図しないネットワークアクセスを特定する機能

Network Access Analyzer のユースケース

- ネットワークのセグメンテーションがどうなっているか？
- インターネットへの疎通の確認
- ネットワーク・パスの確認
- ネットワーク・アクセスの確認



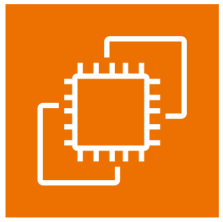
Amazon Inspector

Amazon Inspector

自動化された脆弱性管理サービス

Amazon Inspector

AWSのワークロードを継続的にスキャンしパッケージの脆弱性や意図しないネットワーク露出領域を継続的なスキャンで検出する脆弱性管理サービス



Amazon EC2

Amazon ECR

AWS Lambda

Amazon Inspector の検出結果のタイプ

パッケージの脆弱性 – 検出された Amazon EC2 インスタンス、Amazon ECR コンテナイメージ、Lambda 関数のソフトウェアパッケージをスキャンして検出した脆弱性に該当する CVE (Common Vulnerabilities and Exposures) を示す

ネットワーク到達性 - Amazon EC2 インスタンスへの許可されたネットワークパスがあるかどうかを示す。インターネットゲートウェイ、ロードバランサー、VPC ピアリング接続、仮想ゲートウェイを介した VPN などの VPC から到達可能かどうかスキャンする

Amazon Inspector が備える脅威インテリジェンス

脅威インテリジェンスを活かして、優先順位付けや、対策検討へとつなげていく

CVSS(共通脆弱性評価システム)

脆弱性の深刻度を示す評価手法で、10.0が最高

EPSS(Exploit Prediction Scoring System)

今後 30 日間で脆弱性が悪用される可能性を表現した FIRST が運用するスコア(0.99->99%)

CISA KEV カタログ

米 CISA が運用する、既知の悪用された脆弱性(Known Exploited Vulnerability)の情報
対象政府機関に期日までの対応を義務付け

既知のマルウェア

脆弱性を悪用する既知のマルウェアの一覧

MITRE ATT&CK

敵対的な活動で用いられる戦略・技術・手続を分類し、手口の分析に役立てるフレームワーク

各種エビデンス

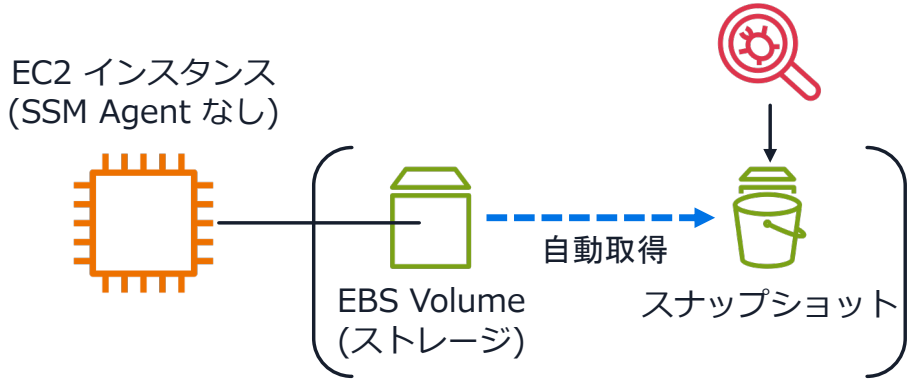
以下のような様々な関連情報
- 既知の Exploit/PoC コード
- マルウェアによる悪用情報

EC2 インスタンスのエージェントレススキャン

ネットワーク構成に依存しないスキャンにより、さらに幅広いワークロードが対象に

- 従来は AWS Systems Manager Agent(SSM Agent) および NW レベルでの到達性を確保した構成が対象だった

- 今後は SSM Agent を導入していない場合は、EBS のスナップショットに対してスキャンを行うこともできるように



Amazon GuardDuty

Amazon GuardDuty

AWS が提供するマネージド脅威検出サービス

- AWS 上のリソースと AWS のアカウントに対する脅威を検出※1
- 有効化のみで AWS が提供するメカニズムを利用して脅威検出を開始可能
- AWS が継続的に開発し機能改善の恩恵を受けることができる

Amazon GuardDuty

※1 AWS Identity and Access Management (IAM) や Amazon Simple Storage Service (Amazon S3) バケットなど、AWS 上のリソースに対する疑わしい挙動

GuardDuty の脅威検出フロー

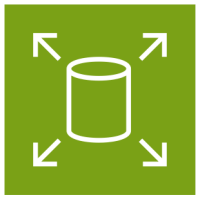
Amazon GuardDuty の拡張機能

S3 Protection

S3 バケットに対するオブジェクトレベルの API オペレーションをモニタリング

EKS Protection

EKS クラスターとコンテナランタイムについて不審なアクティビティや侵害の可能性を検出



Malware Protection

マルウェア感染の可能性がある検出をした場合、または任意のタイミングで EBS ボリュームのスキャンを実施

RDS Protection

Amazon Aurora データベースへのアクセスアクティビティをモニタリング

Lambda Protection

Lambda 関数の不審なアクティビティをモニタリング

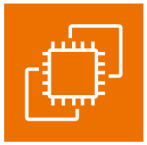
Runtime Monitoring

AWS Fargate を含む ECS クラスターと Amazon EC2 についてファイルアクセス、プロセス実行、ネットワーク接続などのランタイム動作を可視化

GuardDuty Malware Protection の対象範囲

Amazon EC2 対象範囲

Amazon EC2 instances



Amazon Elastic Container Service (ECS) EC2 起動タイプ

Amazon Elastic Kubernetes Service (EKS)

Amazon EC2 上で独自に管理しているコンテナ

マルウェアスキャンの実行タイミング

- GuardDuty が潜在的に感染した可能性のある Amazon EC2 インスタンスの活動を検知すると自動的にスキャン開始
- 一つの EC2 インスタンスにおけるスキャン間隔は24時間。GuardDuty による検出が複数回あったとしても、前回のスキャンから 24 時間未満であれば追加のスキャンは開始されない
- オンデマンドスキャン。設定は不要で、任意のタイミングで、スキャンする Amazon EC2 インスタンスの Amazon ARN を指定してスキャン開始

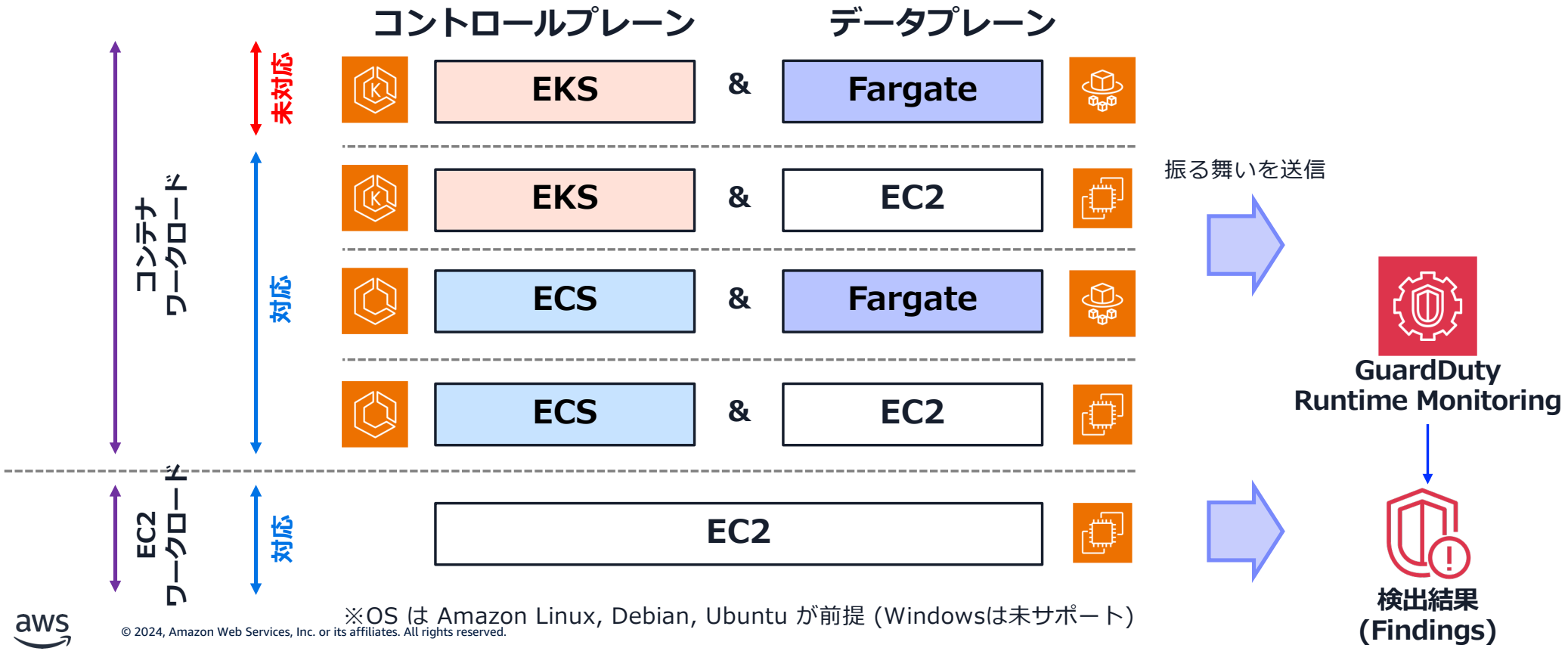
Amazon GuardDuty Malware Protection for S3

特定の S3 バケットへの悪意のあるファイルのアップロードを検出するための GuardDuty Malware Protection の拡張機能

S3 バケットにアップロードされた新しいオブジェクトにマルウェアがないか継続的に評価し、見つかったマルウェアを隔離または排除するためのアクションを実行可能

GuardDuty Runtime Monitoring

GuardDuty Runtime Monitoring は、下記対応ワークロードにおける振る舞いを GuardDutyエージェント を通じて収集し、検出結果を生成



※OS は Amazon Linux, Debian, Ubuntu が前提 (Windowsは未サポート)

GuardDuty Runtime Monitoring – EC2

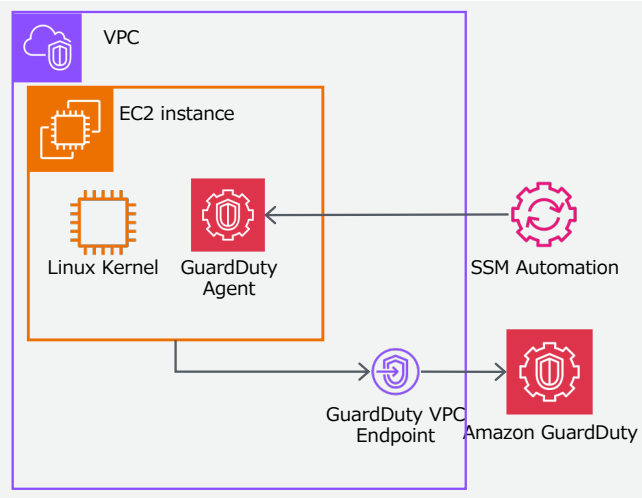
Amazon EC2 のランタイムに関する脅威を検出

Amazon EC2 ワークロードの脅威検出範囲を拡張

ホスト上の OS レベルのアクティビティを可視化

インストールされたエージェントによるスキャン

対応 OS は Amazon Linux 2 / 2023



脅威検出例

C&C への不正な通信をネットワークで検出 (基本機能)

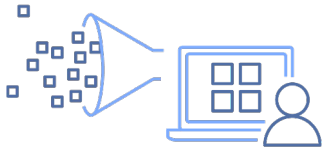
マルウェアプロテクションで実行ファイルを検出 (Malware Protection)

実行プロセスをランタイムモニタリングで検出 (Runtime Monitoring)

Route 53
Resolver DNS Firewall

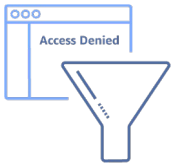
Route 53 Resolver DNS Firewall – Features

ROUTE 53リゾルバのファイアウォール



DNSフィルタリング

- ドメイン名ベースのフィルタリング
- 拒否リスト、許可リスト
- カスタム拒否アクション



マネージドルール

- AWS が管理するドメイン名ベースのリスト
- 利用可能な 3 つのオプション
  - 集約リスト
  - マルウェア
  - ボットネットのコマンド＆コントロール（C&C）
- Recorded Future との脅威インテリジェンス連携

中央管理

- AWS Firewall Manager を使用したクロスアカウント管理
- ポリシーの一貫した実施
- ルールの可視化と管理
- AWS Resource Access Manager (AWS RAM) を使用したルールの共有

可視性とレポート

- ルールごとの Amazon CloudWatch メトリクス
- Amazon S3、CloudWatch、Amazon Kinesis にログの送信が可能

AWS Managed Domain Lists

- 定期的な更新
- 集約リストとDNS脅威カテゴリリスト - マルウェアとボットネットC&C
- 複数のDNS脅威から一度に保護する集約リスト

DNS threat protections

マルウエア

ボットネット

フィッシング

C&C

暗号通貨のマイニング

DGA

DNS トンネリング

…など

AWS Network Firewall

AWS Network Firewall

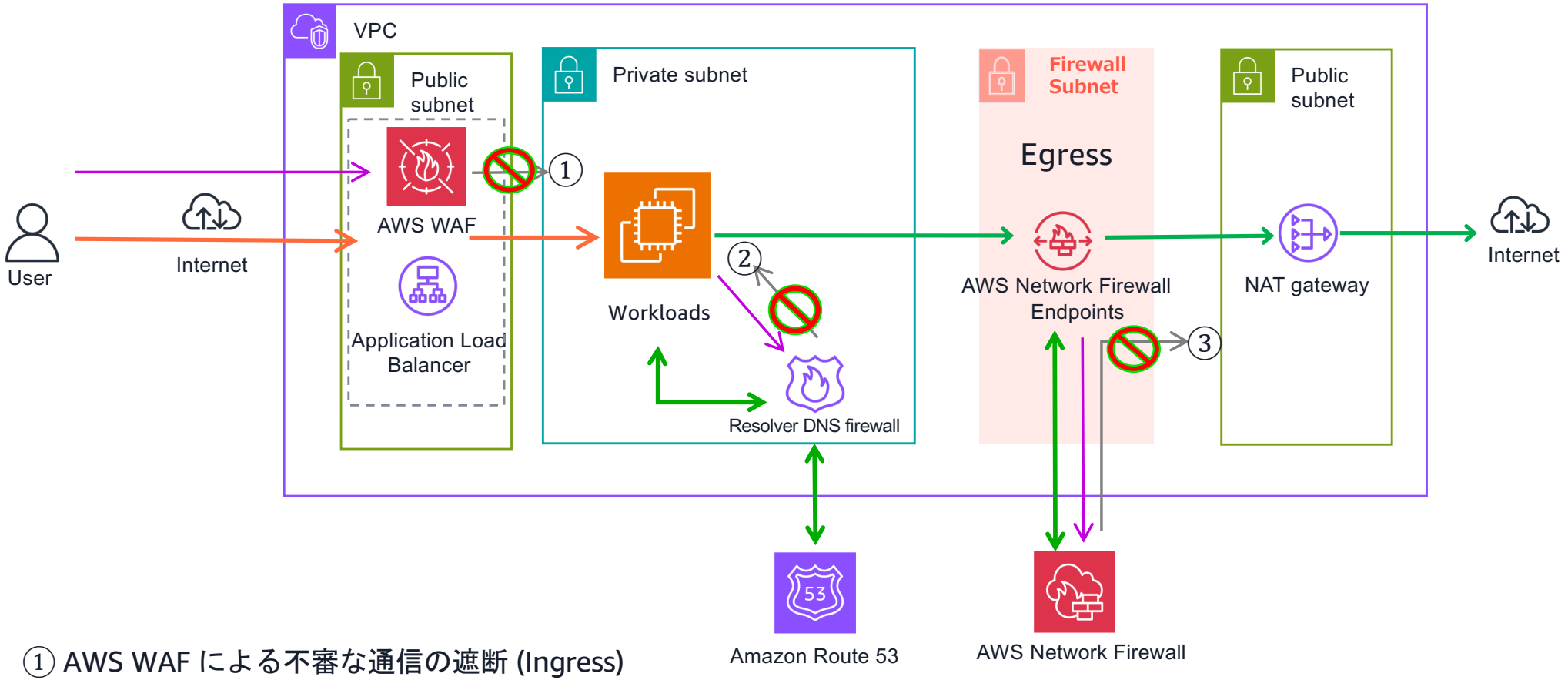
AWS Network Firewall

- きめ細かい制御による柔軟な保護
- VPC とアカウントにわたり一貫したポリシー管理
- 高可用性のマネージド型インフラストラクチャ
- AWS マネージドルールグループの利用が可能

AWS マネージドルールグループ

- 追加料金なしで利用いただけるルール
- 新たな脆弱性や脅威が確認された際に AWS により自動的にアップデート
  - 一日から一週間に 1 度ほどのペースで更新される
  - 場合によってはプライベートコミュニティからの脆弱性情報を元に、新たな脅威が一般公開される前にルールグループを更新する場合もある
- マネージドルールグループが更新された場合 SNS トピックに通知が行われる
- Domain list rule groups と Threat signature rule groups の 2 種類を提供
  - Threat signature rule は Suricata 互換ルールを開示しており、利用者が内容をコピーして変更することが可能（過検知を発生させる特定のルールを除外するなど）

導入パターンの一例

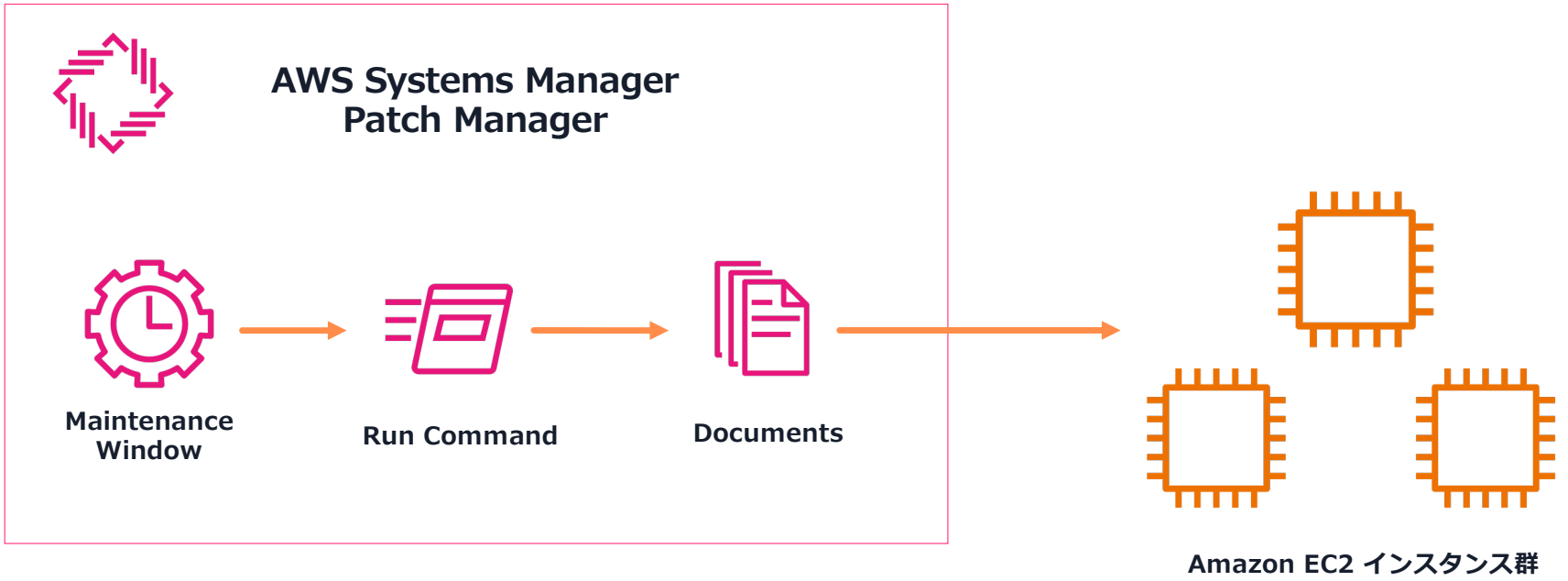


① AWS WAF による不審な通信の遮断 (Ingress)
② Route53 Resolver DNS firewall による不審な DNS フィルタリング (Egress)
③ AWS Network Firewall による不審な通信の遮断 (Egress)

AWS Systems Manager

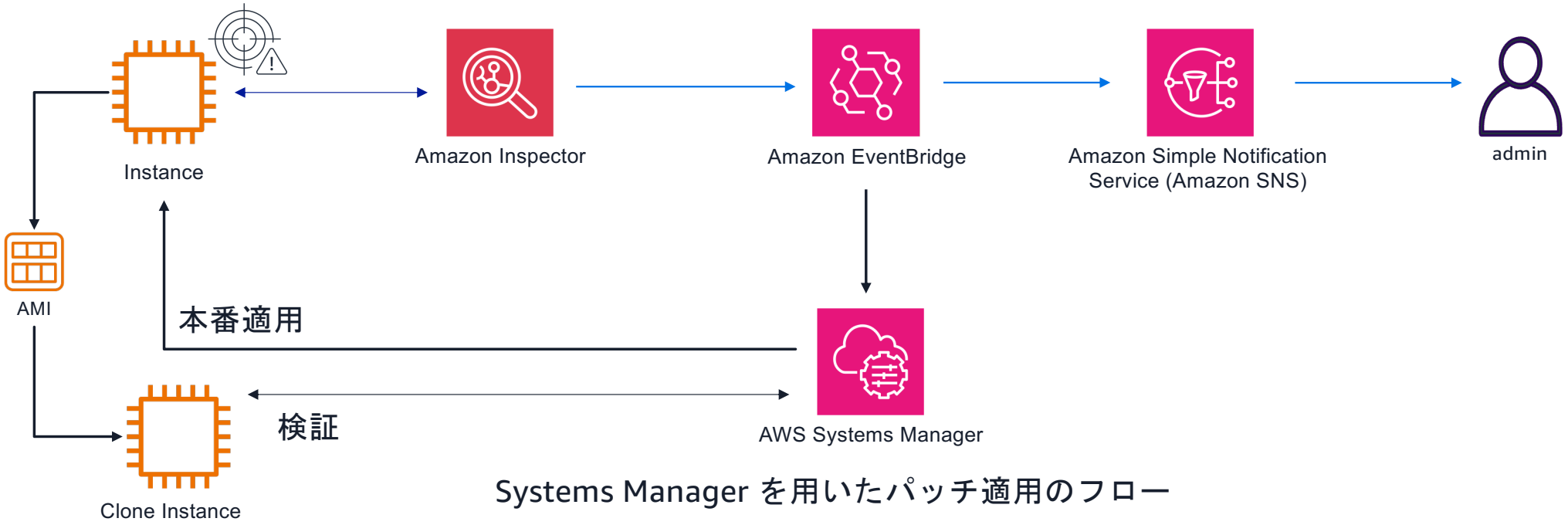
定期的なパッチ適用

- AWS Systems Manager Patch Manager を活用して定期的にパッチを適用



脆弱性の検知とパッチ適用のフロー

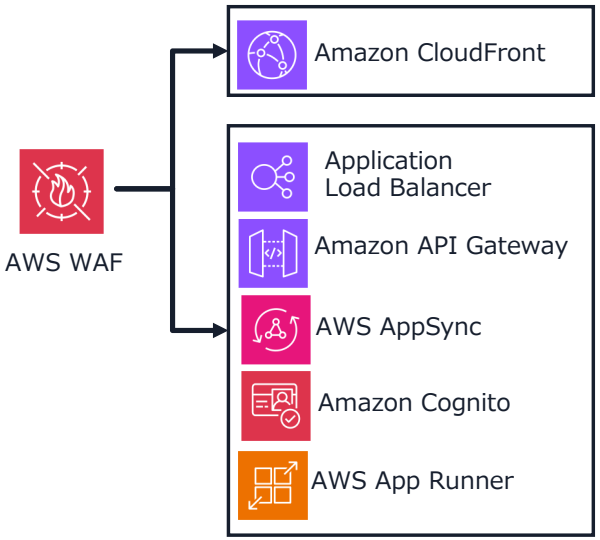
脆弱性が検知された際の管理者への通知フロー



Systems Manager を用いたパッチ適用のフロー

Systems Manager を用いることで緊急パッチ適用や定期定期なパッチ適用が可能

パッチ適用の時間稼ぎに WAF を活用する



スムーズなセットアップ: 既存のアーキテクチャを変更せずに導入可能、TLS/SSL や DNS 設定も不要

Bot Control の統合: AWS が管理するボットルールを有効にして、一般的なボット、標的型ボット、アカウント乗っ取りボットからの保護を実現

マネージドルールとカスタムルール: あらゆる受信リクエストをレイテンシーの影響なく検査する柔軟性の高いルールエンジン

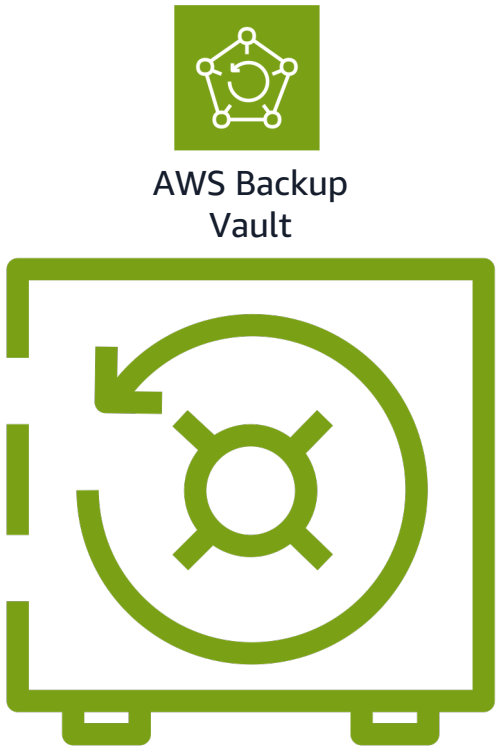
サードパーティのルール: 業界をリードするセキュリティパートナーのルールをマーケットプレイスから選択して、AWS Web ACL に簡単に追加が可能

ウェブアプリケーションを、アプリケーションの可用性、セキュリティの侵害、リソースの過剰な消費などに影響を与えかねない一般的なウェブの弱点から保護するウェブアプリケーションファイアウォール

AWS Backup

バックアップボールト

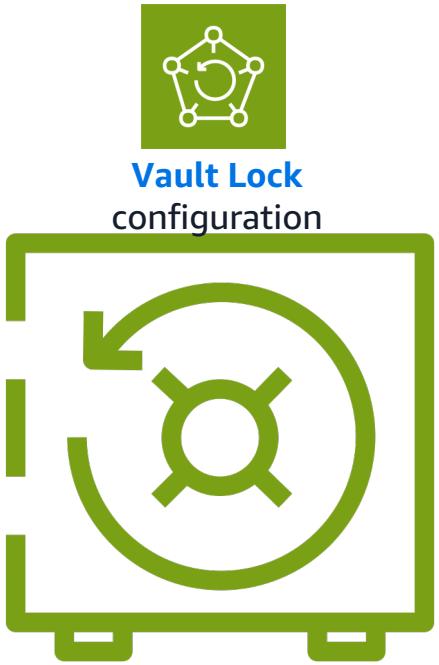
セキュリティ強化の為の設定



- 論理構成 – バックアップボールトは AWS Backup が管理するバックアップデータを保管するためのリソースです。
- アクセス管理 – IAM によるリソースレベルのパーミッションと、バックアップごとにパーミッションを分けることができます。
- 暗号化 –各ボルトに CMK またはサービス固有のデフォルトキーを使用します。
- 誤った削除からの保護 – ボールトのデータは各サービスから見えますが、vault access policy によって管理されています。

AWS Backup Vault Lock

悪意ある行為や意図しない削除からバックアップを保護



- VAULT の有効化 – AWS Backup Vault のレベルで Vault Lock の設定を有効にします。
- 削除からの保護 – ルートアカウントを含むどのユーザーも、バックアップを削除することはできません
- バックアップ設定変更に対する保護 –ルートアカウントを含むどのユーザーも、バックアップの保存期間を変更したり、バックアップのコールドストレージ設定への移行を更新したりすることはできません

AWS Backup Vault Lock

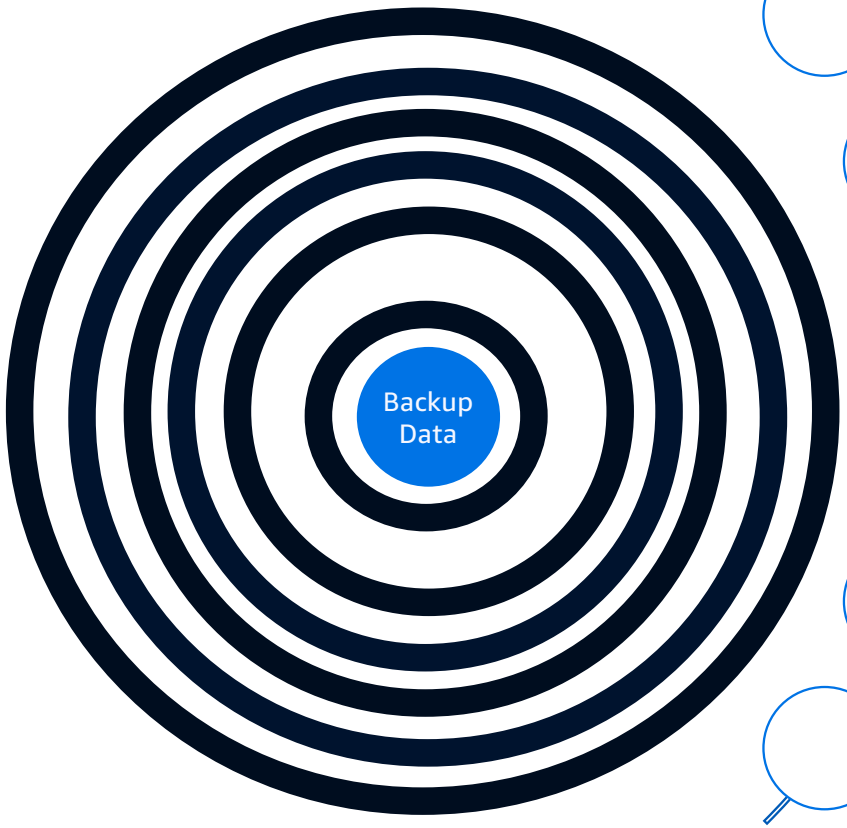
Vault Lock 適用前

Vault Lock 適用時

Backup vault 単位で設定することができ、復旧ポイントの削除を防止することができる
Amazon S3 のオブジェクトロックと同様に、リーガルホールドが設定できる

Vault Lock モード	特徴
ガバナンスモード	ガバナンスの効いた「データ保護」を提供する 特別な権限では、WORM 保護された復旧ポイントの削除ができる
コンプライアンスモード	「コンプライアンス」の目的で利用する いかなるユーザーも上書き/削除/設定の変更ができない 適用が開始されるまでの猶予期間を設定できる

バックアップデータに対する多層防御の構築



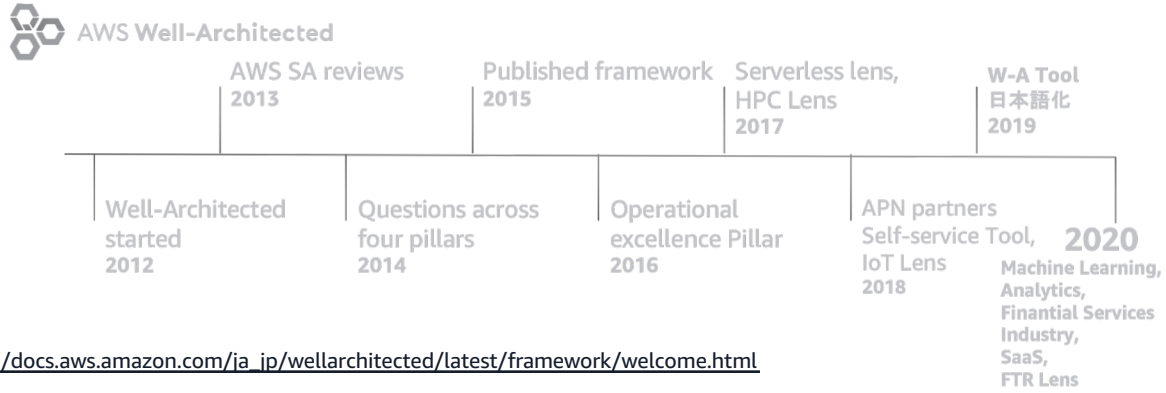
- IAM Policy によるアクセスの制限
- MFA の有効化
- WORM・クロスアカウントでのバックアップ
- AWS KMS を用いたデータの暗号化
- 役割に応じたバックアップへのアクセス制限
- 監査ログの有効化

AWS Well-Architected

AWS Well-Architected Framework(W-A) とは?

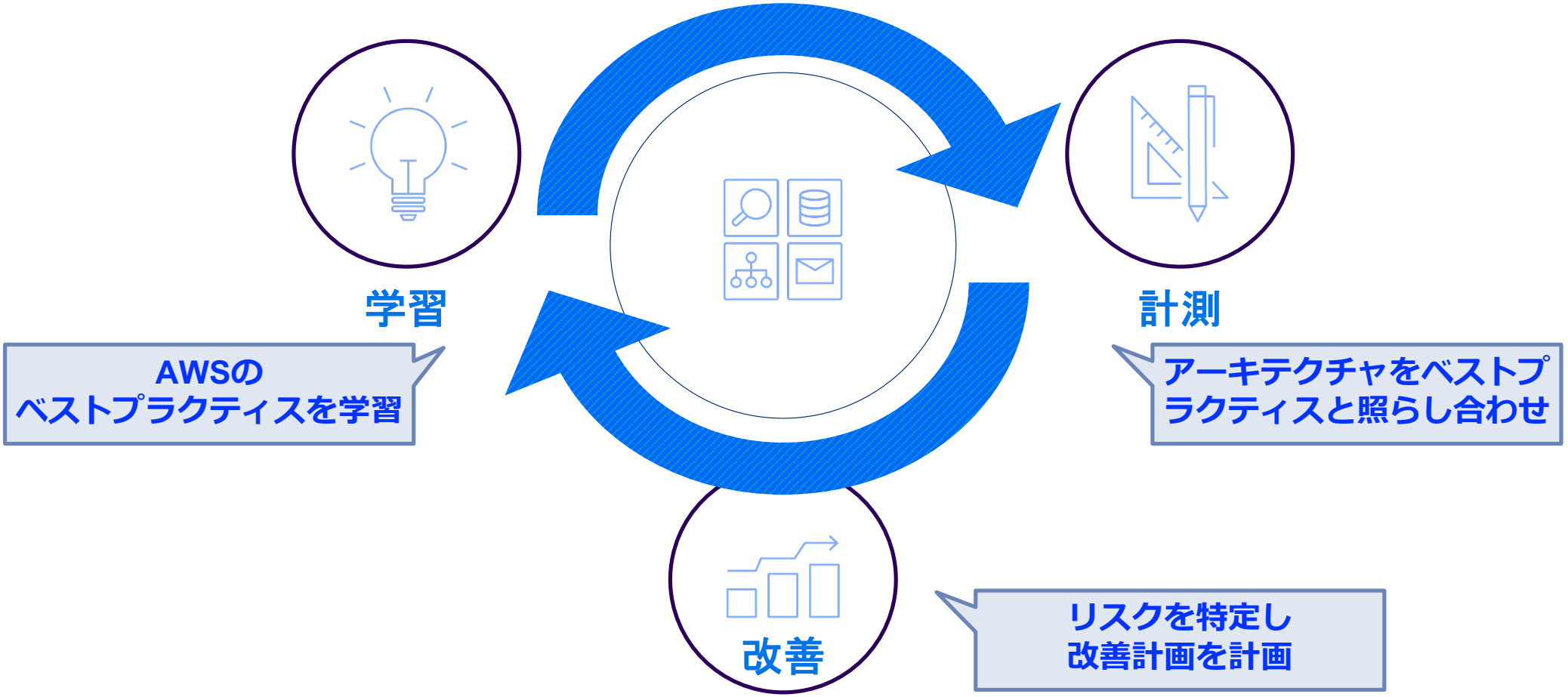
システム設計・運用の”大局的な”考え方と
ベストプラクティス集

- ・AWS のソリューションアーキテクト (SA)、パートナー様、お客様の 10 年以上にわたる**経験**から作り上げたもの
- ・AWS と**お客様**と共に、W-A も**常に進化し続ける**

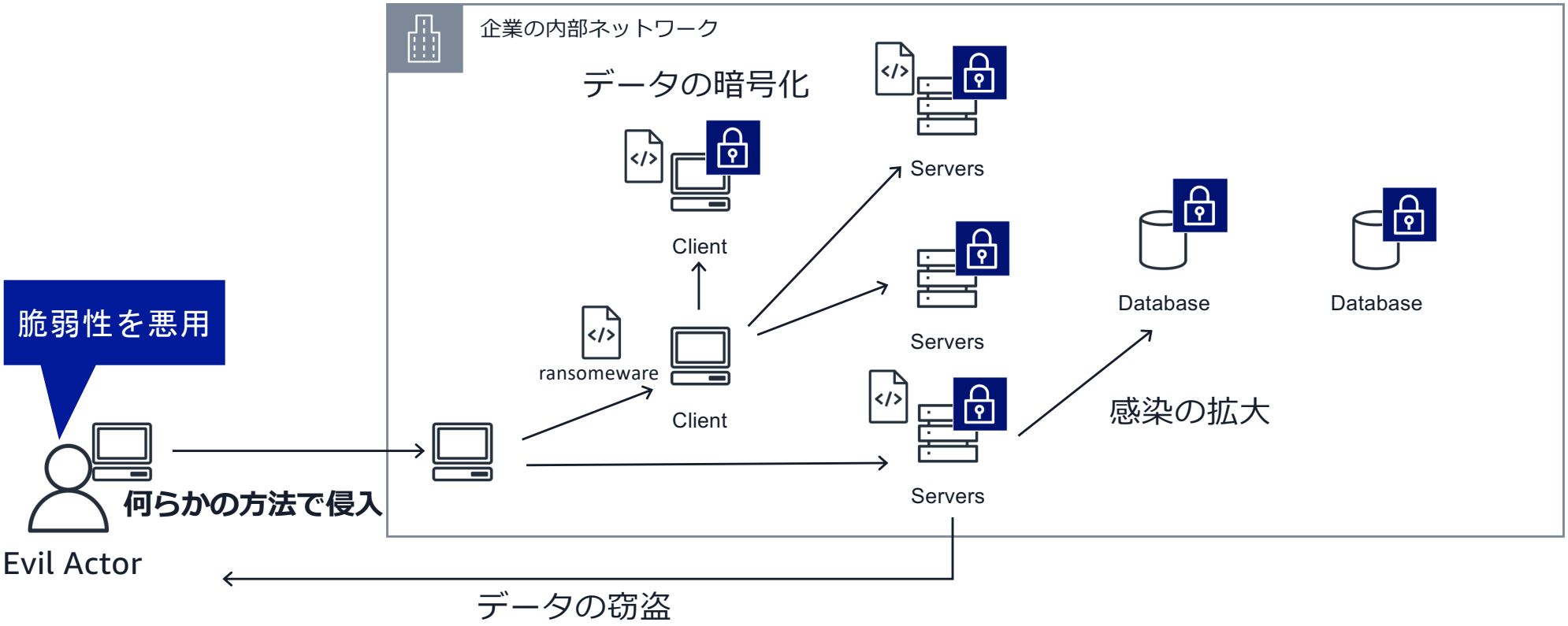


https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/framework/welcome.html

W-A Framework Review - レビューサイクル



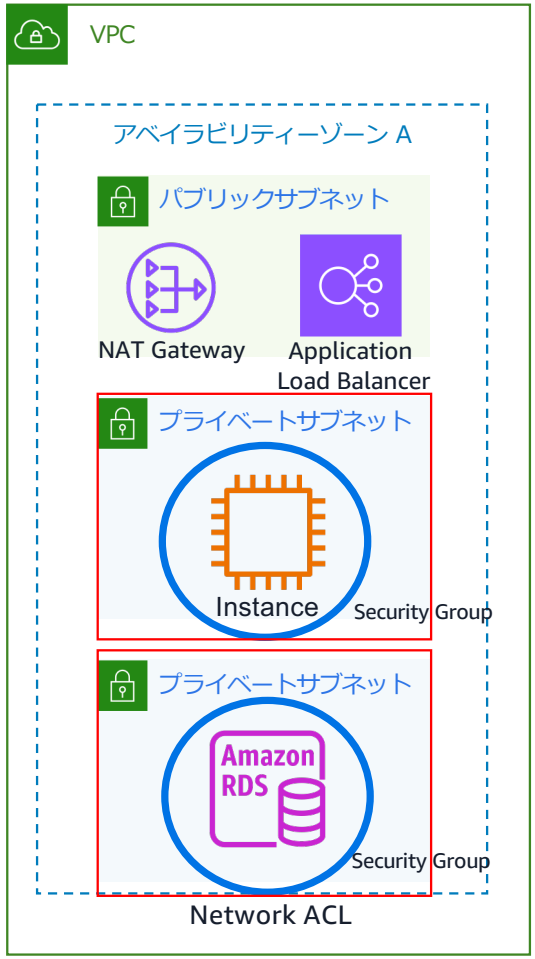
ネットワークを介して感染するランサムウエアの感染経路（再掲）



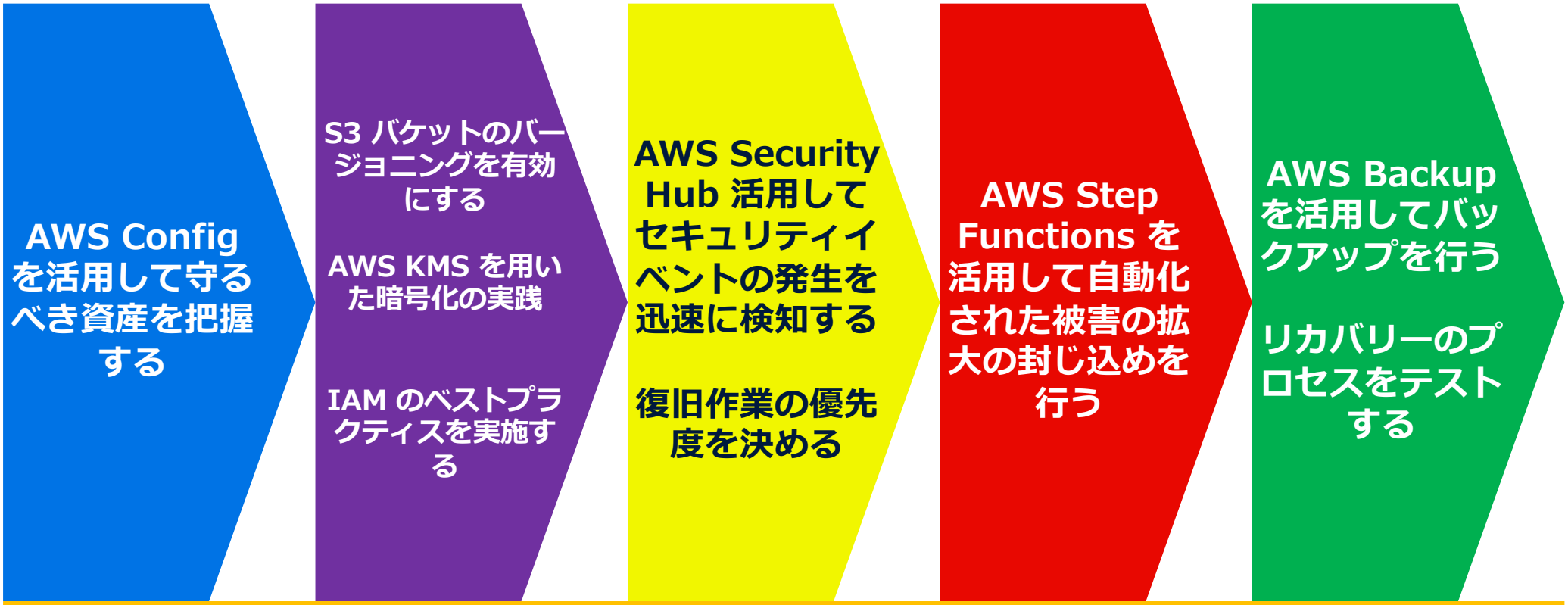
クラウドのメリットを活用する

Amazon GuardDuty はネットワーク内部に侵入したマルウエアが他の端末に感染可能か調査を行った際にアクティビティを検知できます。

Security Group や Network ACL を活用することで瞬時に通信の制御を行うことができるため、 AWS の自動化ツールを組み合わせて対応を行うことで被害の拡大の封じ込めが可能になります。



今日から実践するランサムウエア対策



Thank you!

ご視聴ありがとうございました。

アプリケーションを終了すると本セッションのアンケートが表示されます
アンケート記入にご協力ください
今後の勉強会も参加を希望される場合はアンケートに参加希望の旨ご記入ください

アンケートは５段階評価となっており、「５」からの減点評価での入力をよろしくお願いします

Appendix

参考資料

参考資料

- Protecting your AWS environment from ransomware
- AWS Blueprint for Ransomware Defense
- Protecting against ransomware