Amazon Inspector

AWS Black Belt Online Seminar

佐藤 航大 (Kodai Sato)

Solutions Architect

2023/02

AWS Black Belt Online Seminarとは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWSの技術担当者が、AWSの各サービスやソリューションについてテーマごとに動画を公開します
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- 以下のURLより、過去のセミナー含めた資料などをダウンロードすることができます
  - https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/
  - https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

内容についての注意点

- 本資料では2023年2月時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(https://aws.amazon.com)にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：佐藤 航大 (Kodai Sato)

所属：技術統括本部
　　ソリューションアーキテクト

好きなAWSサービス：

- Amazon Inspector
- Amazon Cognito

本セミナーの対象者

- AWS 環境における脆弱性管理に関心をお持ちの方
- これから Amazon Inspector をご利用予定の方や、理解を深めたい方

アジェンダ

1. 脆弱性管理の必要性
2. Amazon Inspector の概要
3. Amazon Inspector の機能詳細
4. Amazon Inspector を用いた脆弱性管理のプラクティス
5. 料金と対応リージョン
6. まとめ
7. Appendix

脆弱性管理の必要性

昨今のセキュリティ脅威

- IPA (情報処理推進機構) が公表した情報セキュリティ10大脅威 2023 【組織編】

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

- 脆弱性の公開前後による攻撃がランクイン
- それ以外の脅威においても脆弱性を利用した攻撃は多く存在

情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/security/vuln/10threats2023.html

脆弱性管理とは

- 組織の環境内にどのような脆弱性が存在しているのかを把握しリスク評価を行う一連の作業

情報取集

- 脆弱性情報の収集
- 環境内に存在していないかの確認

評価

- 存在する脆弱性にはどのようなリスクがあるか？
- 有効な対策は？

対応

- パッチ適用による対策
- ワークアラウンドの実施

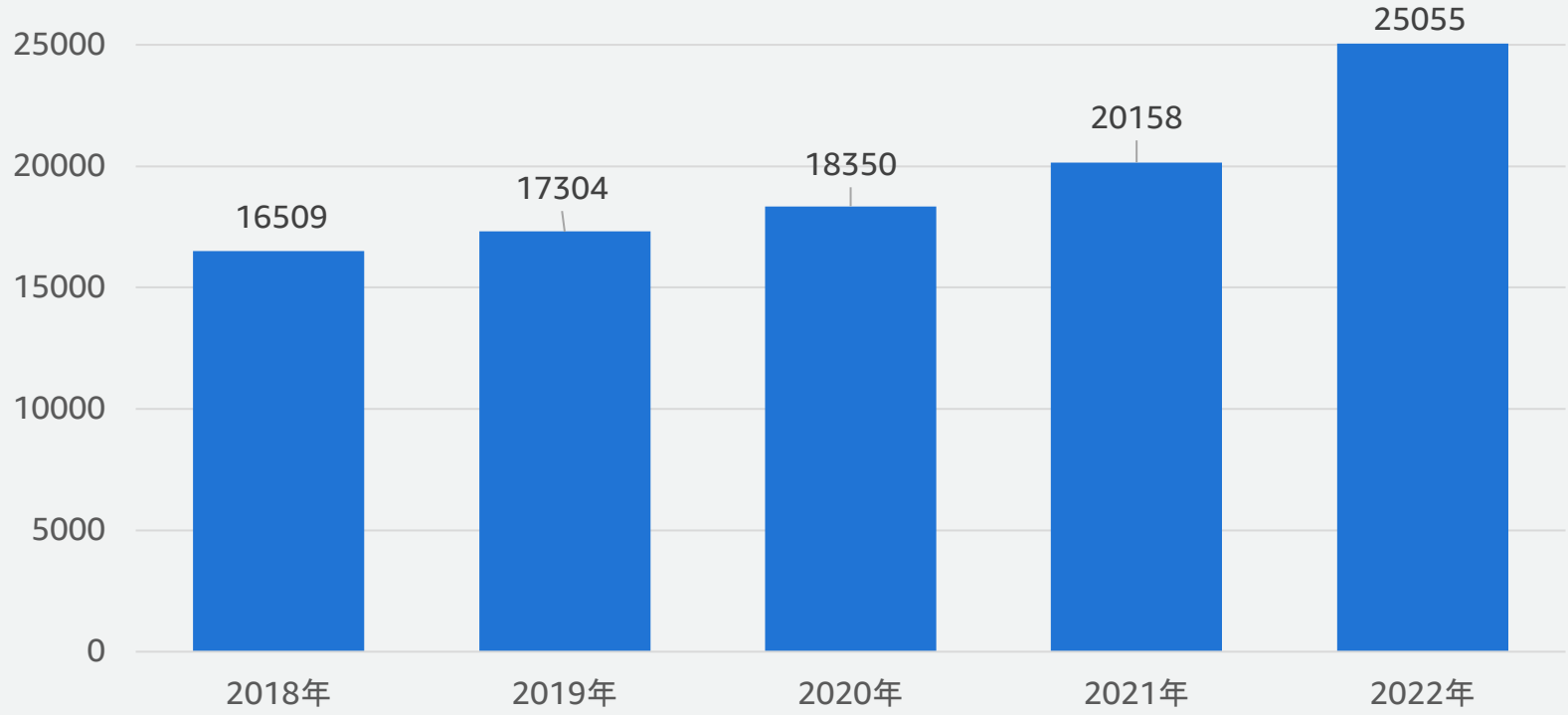
検証・継続監視

- リスク対応が完了したか確認
- その後も継続的に監視

NIST SP 800-40 Rev.4
https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

年々増加する脆弱性件数

- NVD (National Vulnerability Database) によって報告された各年次毎の公開された脆弱性の件数の推移
- 年々増加傾向にあり、増え続ける脆弱性情報を収集して環境内での存在有無の確認や、対処するべきか等の評価を行うと負担も増え続ける



CVSS v3 でスコアリングされた脆弱性の件数 (https://nvd.nist.gov/vuln/search をもとに集計)

効率的な脆弱性管理を行うためには

1. リアルタイムな脆弱性の確認と評価の支援

- リアルタイムで脆弱性情報を収集して環境内に存在する脆弱性を検出できること
- 各脆弱性の詳細を提供し、リスク評価を支援できること

2. スケーラブルな脆弱性監視

- 新しいリソースが継続的に追加・削除される動的な環境でもスケーラブル
  かつ継続的に監視できること

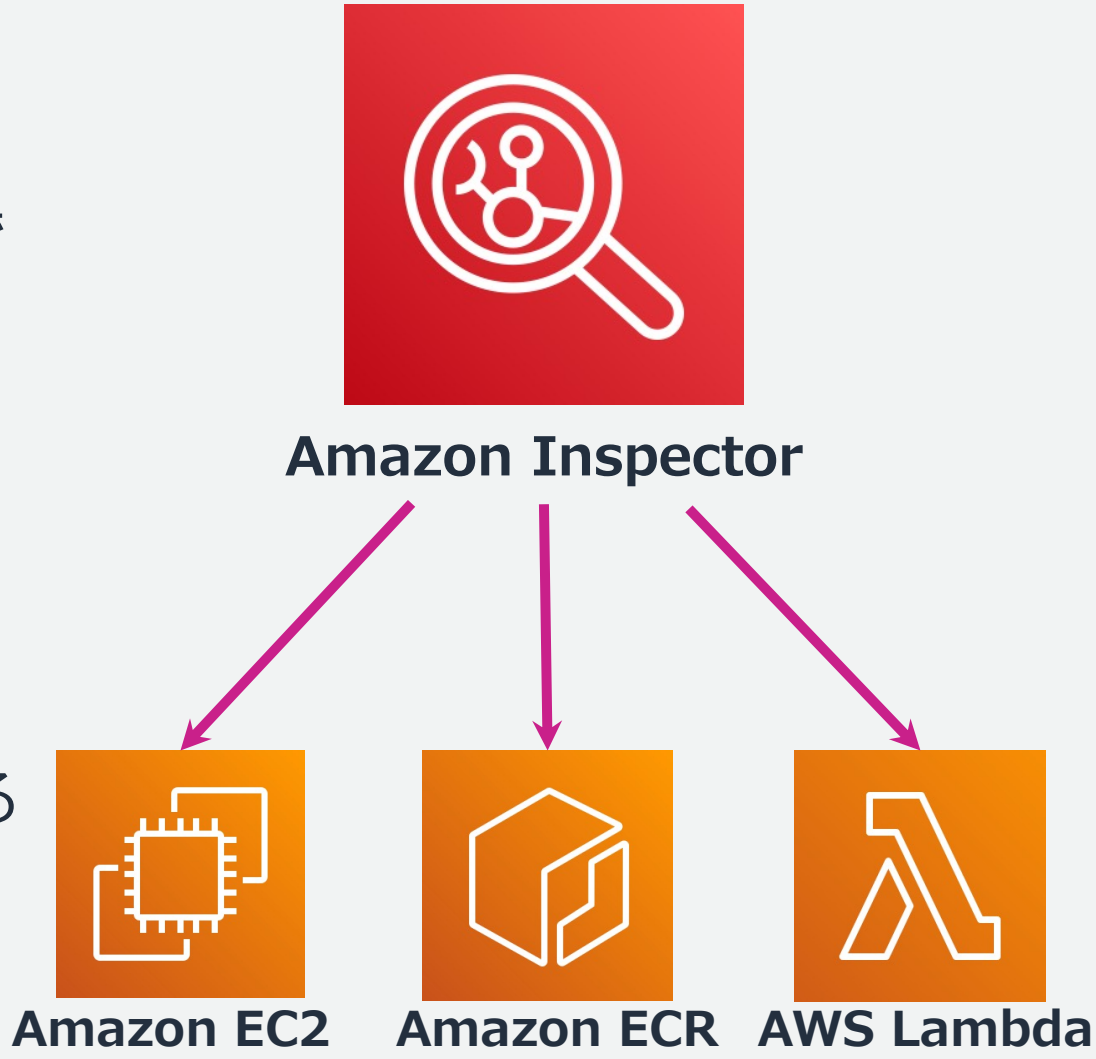
3. 簡単な使い方

- 導入が簡単で少ない工数で管理することができること

Amazon Inspector の概要

Amazon Inspector とは

- 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 Elastic Compute Cloud
    (Amazon EC2)
  - Amazon Elastic Container Registry
    (Amazon ECR)
  - AWS Lambda に対応
- 数クリックで簡単に有効化することができる
- 2021年の re:invent でアップデート
  - 以前のバージョンは Inspector Classic
    と名称変更



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

CVE (Common Vulnerabilities & Exposures)

- 個別製品中の脆弱性を対象として、米国の非営利団体の MITRE 社 (https://cve.mitre.org/) が採番している識別子
- 識別番号は「CVE-西暦-連番」で表現される
  - 例) CVE-2021-44228
- 日本語で共通脆弱性識別子

CVSS (Common Vulnerability Scoring System)

- 各脆弱性に対するオープンで汎用的な評価手法でベンダに依存しない共通の評価方法を提供
- 3つの評価項目で脆弱性を評価
  - 基本評価基準 (Base Metrics)
  - 現状評価基準 (Temporal Metrics)
  - 環境評価基準 (Environmental Metrics)
- 基本評価基準では各評価項目をもとに 0 から 10 の範囲でスコアリングを行う
  - 重大度の把握や修復する優先順位決定の指標となる

CVSS v3 の 基本評価基準の項目
AV: Attack Vector (攻撃元区分)
AC: Attack Complexity (攻撃条件の複雑さ)
PR: Privileges Required (必要な特権レベル)
UI: User Interaction (ユーザ関与レベル)
S: Scope (スコープ)
C: Confidentiality Impact (機密性への影響)
I: Integrity Impact (完全性への影響)
A: Availability Impact (可用性への影響)

https://www.ipa.go.jp/security/vuln/CVSSv3.html
https://nvd.nist.gov/vuln-metrics/cvss

Amazon Inspector の機能詳細

Amazon Inspector の特徴

自動検出と継続的なスキャン

- リソースの自動検出
- 脆弱性とネットワーク到達可能性の継続的スキャン

一元的に集約し可視化

- AWS Organizations との統合
- ダッシュボードによる適用範囲の確認とリソース毎の状況を集約

スコア算出による優先順位付け

- コンテキストを考慮した実用的なリスクスコアを算出
- 対策措置の優先順位を列挙

シンプルで大規模な管理

- ワンクリックで有効化
- AWS Systems Manager Agent (SSM Agent) との統合

対策措置のワークフロー自動化

- APIで操作可能
- Amazon EventBridgeと連携
- AWS Security Hub と統合

1. 自動検出と継続的なスキャン

全てのワークロードを自動的に検出し、組織全体の脆弱性を継続的にスキャン

リソースの自動検出 - 対象となるすべてのリソースを自動的に検出し、パッケージの脆弱性や意図しないネットワークへの露出がないか、リソースのスキャンを開始

継続的なスキャン - 専用のスキャンエンジンを使用してワークロードの危険性、リソースの悪意ある使用、データへの不正アクセスの原因となるパッケージの脆弱性やネットワーク露出がないか監視

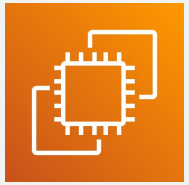
新しいアプリケーションやパッチのインストール後など、イベントに応じてスキャンを実行することで、リソースのライフサイクルを通して環境を監視

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 EC2 スキャン: パッケージの脆弱性



- Systems Manager (SSM) Agent によって Amazon EC2 インスタンスの ソフトウェアパッケージの情報を収集し Amazon Inspector がスキャンを実施
  - Systems Manager で管理されているインスタンス (マネージドインスタンス) をスキャン
    - マネージドインスタンスにする方法については Appendix 参照
- パッケージの脆弱性スキャンのタイミング
  - Amazon Inspector によってインスタンスが検出されたとき
  - 新しいインスタンスを起動するとき
  - 既存のインスタンスに新しいソフトウェアをインストールするとき (Linux のみ)
  - Amazon Inspector が新しい脆弱性項目をデータベースに追加したとき (Linux のみ)
  - Windows インスタンスではデフォルトで 6 時間毎に自動スキャン (間隔は CLI コマンドにて変更可能)

https://docs.aws.amazon.com/inspector/latest/user/enable-disable-scanning-ec2.html

Amazon ECR スキャン

- リポジトリ毎にオンプッシュスキャンと連続スキャンの2種類のスキャン方法を設定可能
  - オンプッシュスキャン: イメージがリポジトリにプッシュされた場合のみスキャンを行う
  - 連続スキャン：オンプッシュスキャンに加えて, Amazon Inspector が CVE 情報をデータベースに追加する度にスキャンを行う
    - 連続スキャン期間は、Lifetime (デフォルト)、180日、30日から選択可能
- Amazon Inspector が提供するコンテナイメージスキャンでは、OS とプログラミング言語のパッケージの両方をスキャン可能

https://docs.aws.amazon.com/inspector/latest/user/enable-disable-scanning-ecr.html

Amazon ECR における拡張スキャンとベーシックスキャンの主な違い

	拡張スキャン	ベーシックスキャン
スキャンエンジン	Amazon Inspector を使用	オープンソースの Clair を使用
カバレッジ	OS とプログラミング言語のパッケージ	OS パッケージのみ
スキャン頻度	プッシュ時、継続的スキャン	プッシュ時、オンデマンドスキャン
脆弱性インテリジェンス	詳細なインテリジェンスを提供 (修復バージョンの存在、攻撃が可能か否かなど)	脆弱性に関する基本情報のみを提供
脆弱性スコアリング	NVD とベンダの両方から CVSS v2、v3 を取得	CVSS v2 のみ取得
AWS サービスとの統合	AWS Security Hub, AWS Organizations 等との統合	組み込みの統合はなし
料金	Amazon Inspector の利用料金が発生 (料金スライド参照)	無料

Lambda 関数 スキャン

- Lambda 関数コード内、Lambda Layer で使用されているアプリケーション パッケージの脆弱性を検出する
- 以下のタイミングでスキャンを実施
  - Amazon Inspector が Lambda 関数を検出したとき
  - 新しい Lambda 関数をデプロイしたとき
  - 既存の Lambda 関数を更新したとき
  - Amazon Inspector が新しい脆弱性項目をデータベースに追加したとき

https://docs.aws.amazon.com/inspector/latest/user/enable-disable-scanning-lambda.html

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 EC2 スキャン: ネットワーク到達性 (Network Reachability)

- 環境内の Amazon EC2 インスタンスで許可されているネットワークパスを検出
  - インターネットゲートウェイ、仮想プライベートゲートウェイ、ピアリングしている VPC 等からのネットワークパスがあるかを検出[1]
- サービスやプロトコル、インターネット経由のネットワークパスか否かによって重大度を評価[2]
- 24時間ごとにネットワーク到達性をスキャン

サービス	TCP ポート	UDP ポート	Internet Path Rating	Open Path Rating
HTTP	80	80	Low	Informatinal
SSH	22	22	Medium	Low

ネットワーク到達性の検出結果の例

[1] https://docs.aws.amazon.com/inspector/latest/user/findings-types.html
[2] https://docs.aws.amazon.com/inspector/latest/user/findings-understanding-severity.html

検出結果の管理

- Amazon Inspector は、発見した脆弱性とネットワーク到達性を自動的に追跡・保存する
  - ステータスは active、suppressed、closed の3種類
  - Amazon Inspector は環境内を継続的にスキャンして、アクティブな検出結果を監視する。脆弱性への対応が完了すると、Amazon Inspector は自動的に検出結果のステータスを closed に変更

抑制ルール (Suppression Rule)

- 指定した条件に一致する Amazon Inspector の検出結果を自動的に非表示にする
  - 検出結果の重大度、リソースタグ、作成日など、様々な条件でフィルタリング可能
    - 重大度の低い検出結果を非表示にする
    - 開発環境のリソースの検出結果を非表示にする等
- 抑制ルールで除外した検出結果はステータスが suppressed となりデフォルトでは表示されない

2. 一元的に集約して可視化

ダッシュボードにより AWS 環境の脆弱性状況の概要を確認

- 適用範囲の確認– 環境内でどのくらいの割合が Amazon Inspector のスキャン対象になっているかを確認
- Critical な検出結果の表示 – リソースごとに未修正の Critical な脆弱性を表示
- リスクに応じた優先順位付け– 各検出結果の重大度から、修正すべきパッケージ情報を表示

環境の状況を把握できるダッシュボード画面 (その1)

環境の状況を把握できるダッシュボード画面 (その2)

Critical な脆弱性を多くもつリソース

最も緊急の検出結果がある ECR コンテナイメージ

最も緊急の検出結果がある Elastic Container Registry (ECR) コンテナイメージ。

イメージタグ	リポジトリ	ECR コンテ...	AWS アカウ...	緊急	すべて
latest、さらに 1 個	dev-51275059055	sha256:f28c2527b	512750590557	3	35

検出結果があるすべてのコンテナイメージを表示

最も緊急の検出結果があるインスタンス

最も緊急の検出結果があるインスタンス。

インスタンス ID	AWS アカウント	AMI ID	緊急	すべて
i-00927b317e2b8c0ac	512750590557	ami-0ea1d45dcdd4...	3	41
i-0c6e35c72a8a9da5c	512750590557	ami-0ea1d45dcdd4...	1	38

検出結果があるすべてのインスタンスを表示

最も緊急の検出結果がある Amazon マシンイメージ (AMI)

緊急の検出結果の合計数が最も多い AMI があるインスタンス

AMI	影響を...	オペレー...	緊急 (平均)	すべて (平均)
amzn2-ami-hvm-2.0.20221210.1-x86_64-gp2 (ami-0ea1d45dcdd47e...	2	Linux/UNIX	2	40

検出結果があるすべてのインスタンスを表示

最も緊急の検出結果がある Lambda 関数

関数名	AWS アカウ...	ランタイム	最終変更日	緊急	すべて

リスクがある上位の Lambda 関数なし

リスクがある上位の Lambda 関数であって、表示するものはありません。

検出結果があるすべての Lambda 関数を表示

各リソースの脆弱性情報等も確認することが可能

3. スコア算出による優先順位付け

コンテキストを考慮したスコアリングにより優先順位付けを支援

実用的なスコアリング– CVE 情報をリソースのネットワークアクセスなどと関連付けて Amazon Inspector 独自のスコアを算出

例：リモートでしか悪用できない CVE を Amazon EC2 インスタンス上で発見したが、その Amazon EC2 インスタンスはインターネット経由でアクセスできない設定になっていた場合、実際に悪用される可能性は低いのでリスクスコアは下がる

この結果、より実用的な脆弱性リスクスコアが得られる

4. シンプルで大規模な管理

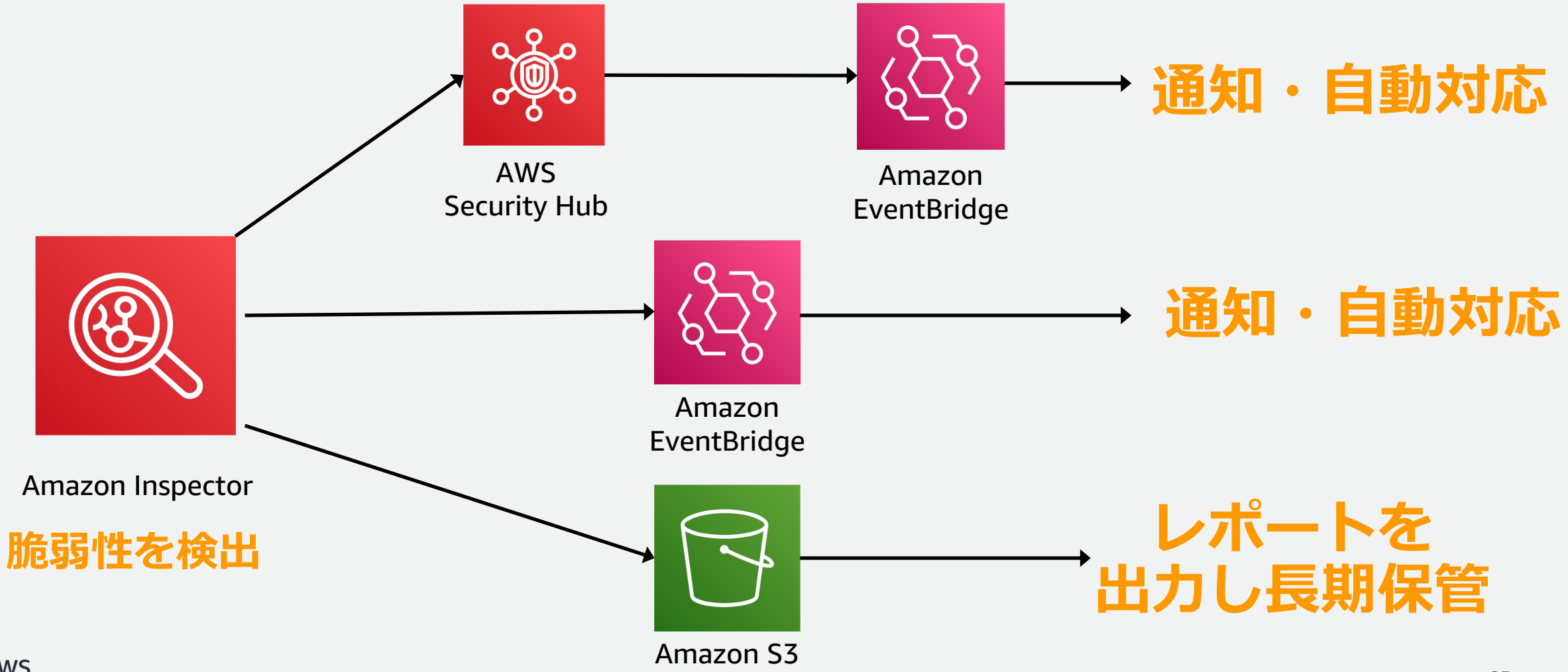
AWS Organizations との統合で複数アカウントの管理が可能

- Organizations 内の一つのアカウントを委任管理者アカウントに指定
- Organizations 内の全てのメンバアカウントを一元的に管理及び設定可能
  - 各メンバアカウントの Amazon Inspector の有効化、無効化、どのスキャンを有効にするか等の設定が可能
  - メンバアカウントでも自アカウントの有効化は可能 (メンバアカウントの無効化は委任管理者のみ可能)
- 委任管理者アカウントでは Organizations 内の検出結果を集約して確認可能
  - ダッシュボードに Critical な検出結果が多いアカウント等も確認可能
  - アカウントごとの検出結果のフィルタリング等も可能

https://docs.aws.amazon.com/inspector/latest/user/managing-multiple-accounts.html

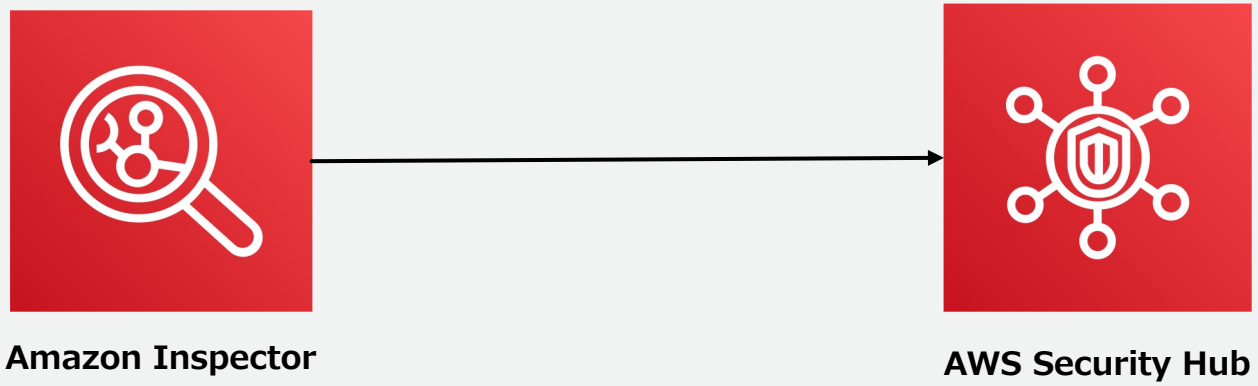
5. 対策措置のワークフロー自動化

AWS サービスとの連携によりユースケースに応じて多様な活用方法を提供



AWS Security Hub との統合

- AWS Security Hub は AWS セキュリティサービス、パートナーサービスからの検出結果を標準化されたデータ形式で自動的に集約するサービス
- Amazon Inspector は Security Hub に検出結果を送信することが可能



https://docs.aws.amazon.com/inspector/latest/user/securityhub-integration.html

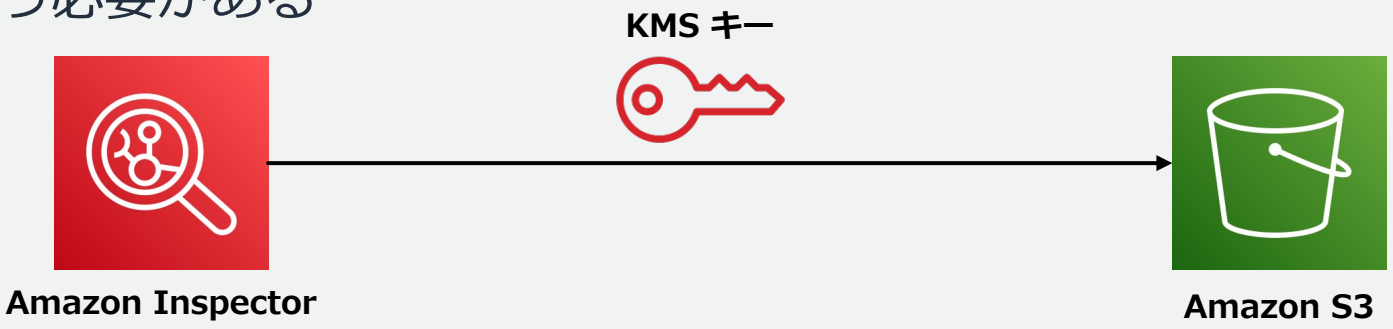
Amazon EventBridge との統合

- Amazon Inspector は以下のイベントを詳細情報を含め EventBridge へ送信
  - パッケージの脆弱性、ネットワーク露出を検出したとき
  - 初回スキャンが完了したとき
  - 適用範囲に変更が生じたとき
- イベントパターンによってイベントをフィルタリングして後続処理を行うことも可能
  - 例) 重大度が high 以上の検出結果が発見されるとメール通知

https://docs.aws.amazon.com/inspector/latest/user/eventbridge-integration.html

検出結果のレポートを Amazon S3 へエクスポート

- 検出結果のレポートを S3 バケットに保存することが可能
  - レポートの形式は CSV、JSON
- レポートはマネジメントコンソール、API を使用してエクスポート可能
  - 検出結果のステータス、Inspector Score、重大度等でフィルタリングしてエクスポートも可能
  - レポートは KMS キーによって暗号化された状態で保管
  - Amazon Inspector が KMS キーへのアクセス、S3 へのアクセスを行うためのアクセス権の設定をおこなう必要がある



https://docs.aws.amazon.com/ja_jp/inspector/latest/user/findings-managing-exporting-reports.html

サポートされている OS と プログラミング言語 (抜粋)

2023年2月現在

Amazon EC2 スキャン

- Amazon Linux 2
- Cent OS
- Debian Server
- RedHat Enterprise Linux
- Ubuntu
- Windows Server

Amazon ECR スキャン

- 対応OS
  - Amazon Linux 2
  - Cent OS
  - Debian Server
  - RedHat Enterprise Linux
  - Ubuntu Server
- 対応プログラミング言語
  - C#, Go, Java, JavaScript, PHP, Python, Ruby, Rust

AWS Lambda スキャン

- Java
- NodeJS
- Python
- Go

各スキャンにおける対応 OS, プログラミング言語とそのバージョンの詳細と最新の情報はこちらをご覧ください
https://docs.aws.amazon.com/inspector/latest/user/supported.html

Amazon Inspector 用いた脆弱性管理のプラクティス

脆弱性管理とは (再掲)

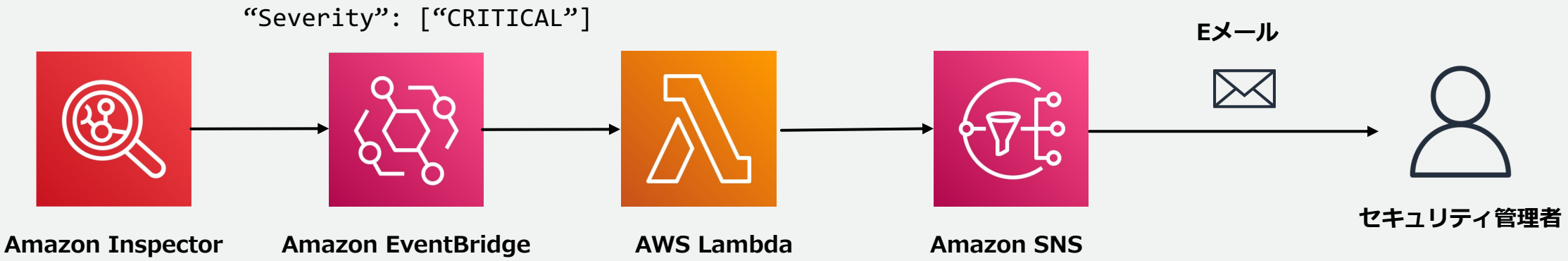
- 組織の環境内にどのような脆弱性が存在しているのかを把握してリスク評価を行う一連の作業

情報収集	評価	対応	検証・継続監視
• 脆弱性情報の収集 • 環境内に存在していないかの確認	• 存在する脆弱性にはどのようなリスクがあるか？ • 有効な対策は？	• パッチ適用による対策 • ワークアラウンドの実施	• リスク対応が完了したか確認 • その後も継続的に監視

NIST SP 800-40 Rev.4
https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

脆弱性管理プロセス: 情報収集

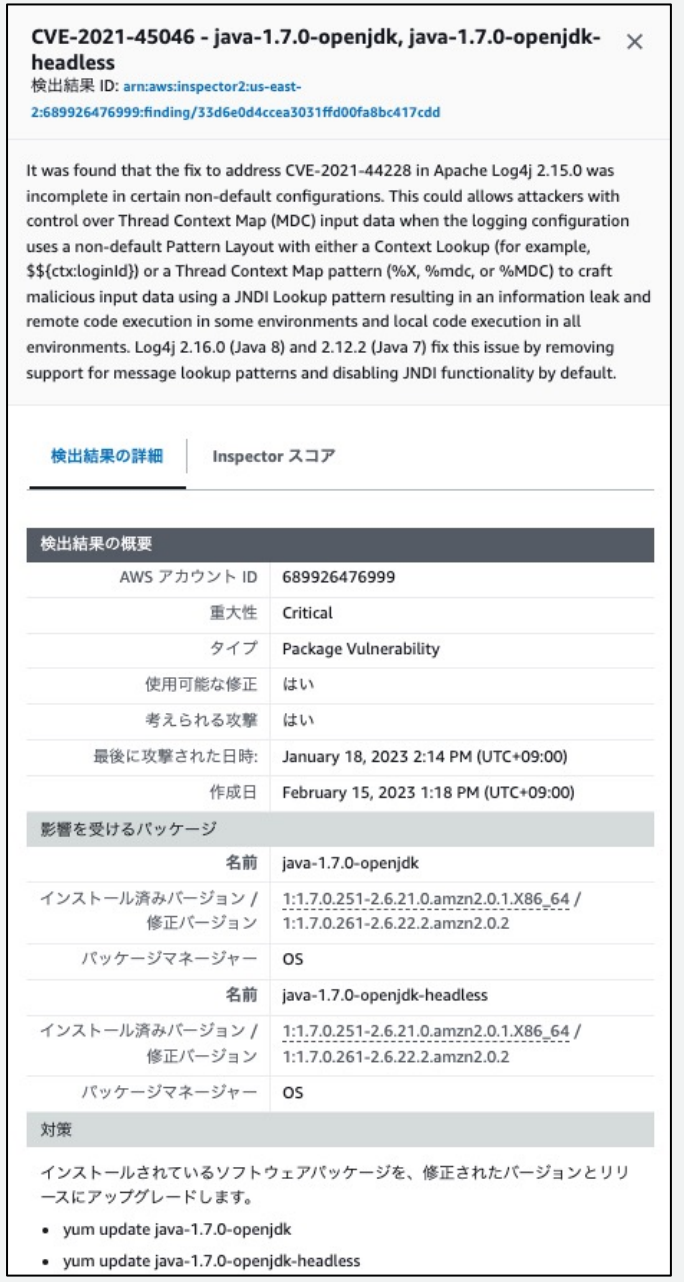
- Amazon Inspector はコンソールから環境内の脆弱性情報をニアリアルタイムで確認
- Amazon EventBridge、AWS Lambda、Amazon SNS 等の連携により管理者へ通知も可能
  - 重大な脆弱性が発見された場合に管理者に通知
  - 週次で脆弱性情報のサマリーを管理者に通知



Critical な脆弱性が発見された際にセキュリティ管理者へ通知するアーキテクチャの例

脆弱性管理プロセス: 評価

- Amazon Inspector は各リソースで検出された脆弱性の詳細について確認することが可能
  - 修正バージョンが提供されているか
  - 考えられる攻撃
  - 対策方法についてなど
- Amazon Inspector は検出された脆弱性の CVSS スコアだけでなく、リソースのネットワーク情報を考慮した独自のスコアリングも提供
  - 対策を講じるリソースの優先順位付けの参考に



CVE-2021-45046 - java-1.7.0-openjdk, java-1.7.0-openjdk-headless

検出結果 ID: arn:aws:inspector2:us-east-2:689926476999:finding/33d6e0d4ccea3031ffd00fa8bc417cdd

It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

検出結果の詳細 | Inspector スコア

検出結果の概要	
AWS アカウント ID	689926476999
重大性	Critical
タイプ	Package Vulnerability
使用可能な修正	はい
考えられる攻撃	はい
最後に攻撃された日時:	January 18, 2023 2:14 PM (UTC+09:00)
作成日	February 15, 2023 1:18 PM (UTC+09:00)
影響を受けるパッケージ	
名前	java-1.7.0-openjdk
インストール済みバージョン / 修正バージョン	1:1.7.0.251-2.6.21.0.amzn2.0.1.X86_64 / 1:1.7.0.261-2.6.22.2.amzn2.0.2
パッケージマネージャー	OS
名前	java-1.7.0-openjdk-headless
インストール済みバージョン / 修正バージョン	1:1.7.0.251-2.6.21.0.amzn2.0.1.X86_64 / 1:1.7.0.261-2.6.22.2.amzn2.0.2
パッケージマネージャー	OS

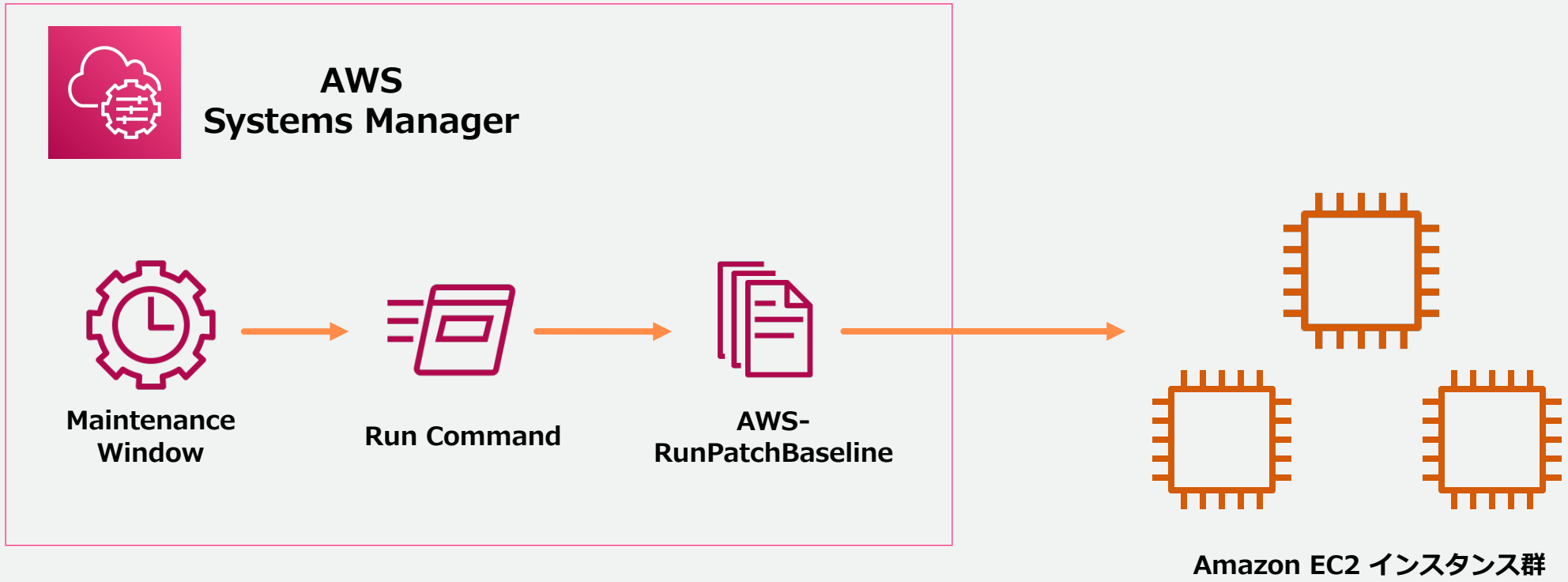
対策

インストールされているソフトウェアパッケージを、修正されたバージョンとリリースにアップグレードします。

- yum update java-1.7.0-openjdk
- yum update java-1.7.0-openjdk-headless

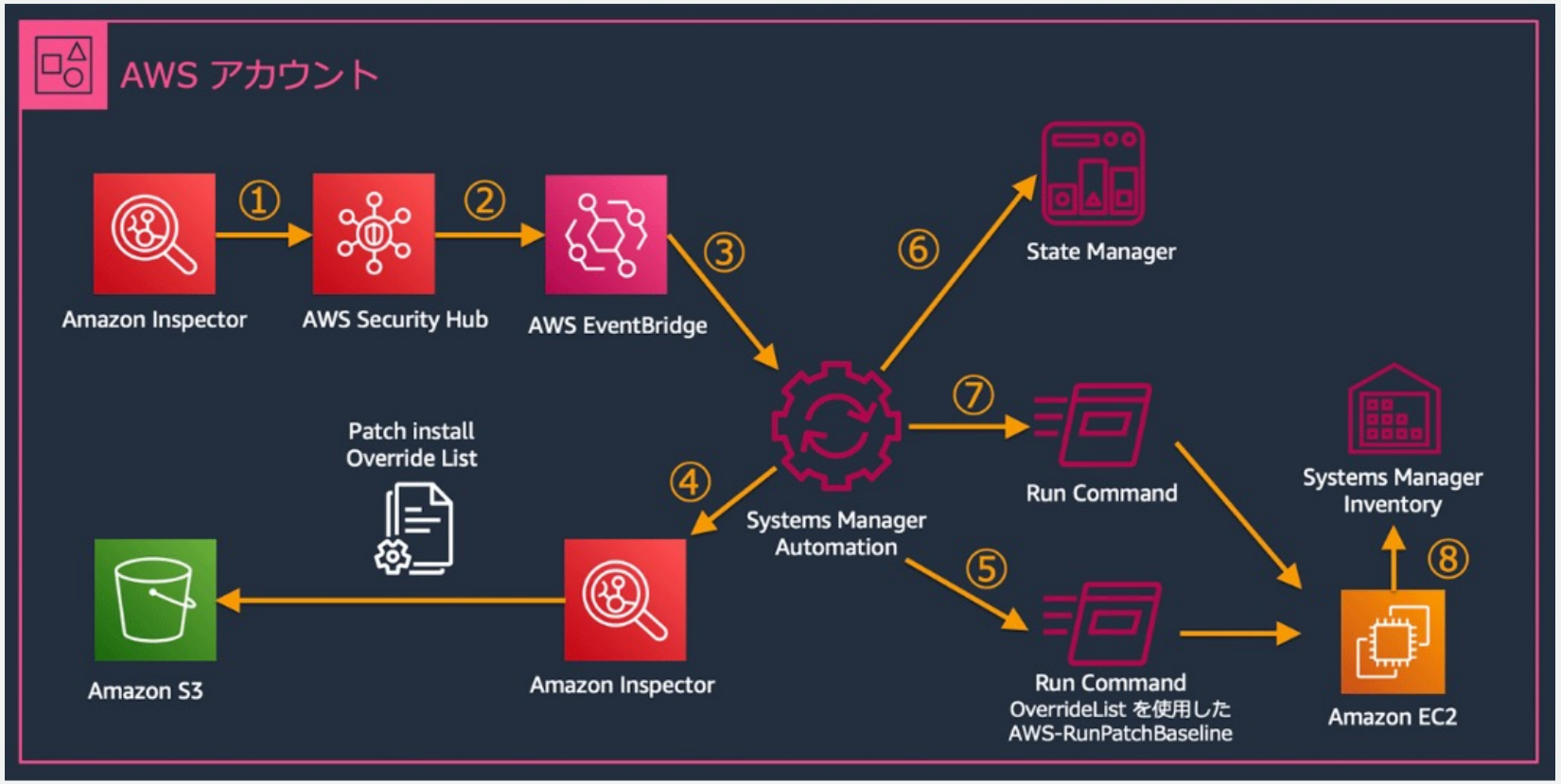
脆弱性管理プロセス: 対応 (定期的なパッチ適用)

- AWS Systems Manager を活用して定期的にパッチを適用



脆弱性管理プロセス: 対応 (緊急時のパッチ適用)

- 指定した脆弱性を包含しているパッケージのパッチ適用をオンデマンドで実行するソリューション



https://aws.amazon.com/jp/blogs/news/automate-vulnerability-management-and-remediation-in-aws-using-amazon-inspector-and-aws-systems-manager-part-1/

脆弱性管理プロセス: 検証・継続監視

- 脆弱性の解消を検出結果のステータス変化で確認可能
- 検出結果のフィルタリングで Closed された検出結果のみを確認することも可能
  - Closed の検出結果は30日後に削除される

料金と対応リージョン

料金体系(東京リージョン、2023 年 2 月現在)

Amazon EC2、Amazon ECR、AWS Lambda に対するスキャンによって料金がそれぞれ発生

Amazon EC2 スキャン料金

- スキャンされたインスタンスの**月間平均数**※に基づいて算出

スキャンタイプ	月間料金
EC2スキャン	1.512 USD / インスタンス

Amazon ECR コンテナイメージ スキャン料金

- **オンプッシュスキャン**、**継続スキャン**から選択
- 継続スキャンの場合は、初回のオンプッシュスキャンと自動再スキャンのたびに料金が発生

スキャンタイプ	月間料金
初回スキャン料金	0.11 USD / イメージ
再スキャン料金	0.01 USD / スキャン

AWS Lambda スキャン料金

- スキャンされた Lambda 関数の**月間平均数**に基づいて算出

スキャンタイプ	月間料金
Lambda スキャン	0.36 USD / Lambda 関数

※インスタンスの月間平均数 = 各インスタンスで Amazon Inspector が有効化された合計時間/月間時間数

15日間無制限の無料トライアルをご利用できます

最新の情報は以下のリンクよりご確認ください
https://aws.amazon.com/jp/inspector/pricing/

コスト試算例 (東京リージョン)

- (例1) 100 台の Amazon EC2 を一ヶ月スキャンしている場合、月間請求額は

100 (インスタンス数) × 1.512 USD = **151.2 USD**

- (例2) 100 個のコンテナイメージを継続スキャン用に設定されたリポジトリにプッシュし、再スキャンが 15 回実行された場合の月間請求額は

初回スキャン料金: 100 (コンテナイメージ数) × 0.11 USD = 11 USD

再スキャン料金: 100 (コンテナイメージ数) × 15 (回) × 0.01USD = 15 USD

合計: 26 USD

Amazon Inspector 対応リージョン (2023 年 2 月現在)

19のリージョンでご利用いただけます

- **東京 リージョンにも対応**

- バージニア北部
- オハイオ
- 北カリフォルニア
- オレゴン
- 香港
- ムンバイ
- ソウル
- シンガポール
- シドニー
- 東京
- カナダ
- フランクフルト
- アイルランド
- ロンドン
- ミラノ
- パリ
- ストックホルム
- バーレーン
- サンパウロ

最新の情報は以下のリンクよりご確認ください
https://aws.amazon.com/jp/about-aws/global-infrastructure/regional-product-services/

まとめ

まとめ

- Amazon Inspector はネットワーク到達性やソフトウェアパッケージの脆弱性を継続的にスキャンすることで検出する脆弱性管理サービス
- ソフトウェアのインストール、新しい脆弱性が発見された場合等にスキャンが自動で行われリアルタイムで脆弱性情報を確認できる
- 環境内のリソースを自動で認識することでスケーラブルな監視が可能
- 数クリックで簡単に有効化して即座に利用できる

Amazon Inspector を活用することで、
AWS 環境の脆弱性管理を強力にサポートします！

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へ
お問い合わせください

https://aws.amazon.com/jp/premiumsupport/

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
お問い合わせください（マネジメントコンソールへのログインが必要です）

https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

https://aws.amazon.com/jp/events/

ハンズオンコンテンツ

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html

Thank you!

Appendix

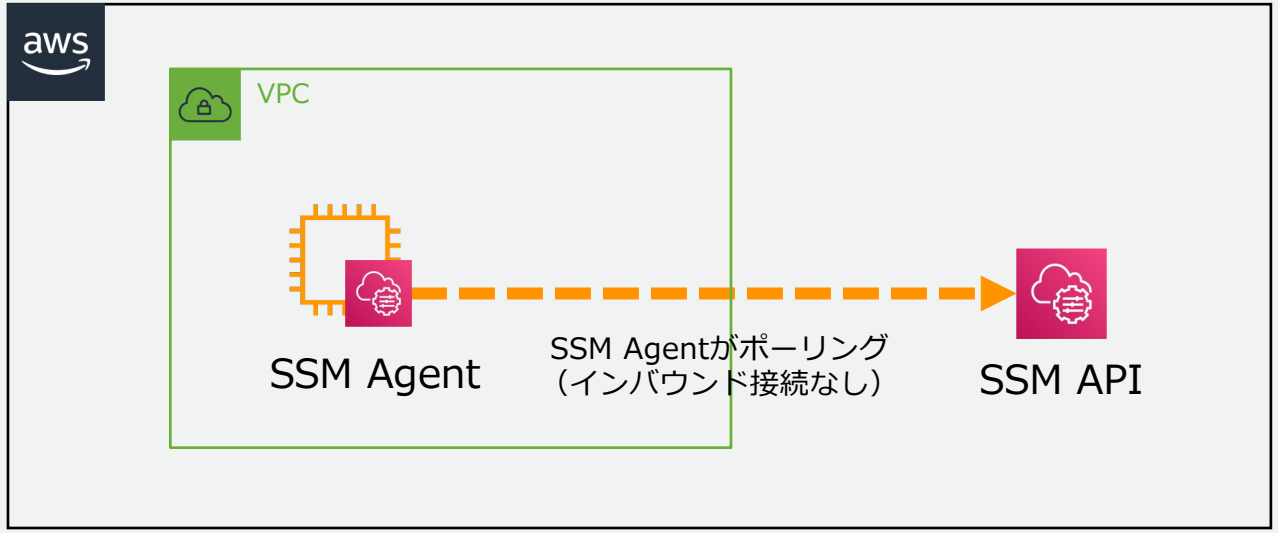
Inspector Classic からの主な変更点

- Amazon ECR 上のコンテナイメージ、Lambda 関数のスキャンをサポート
- SSM Agent による EC2 スキャン
  - AWS が提供する AMI では多くの OS でプリインストールされている[1]
- マルチアカウント管理のサポート
- リスクスコアの算出による検出結果の優先順位付け
- スキャンできるインスタンスが無制限に

[1] https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/ami-preinstalled-agent.html

マネージドインスタンスにする方法 ① SSM Agent の導入

- SSM Agent が SSM API と連携し各種操作、コントロールを行う
- Amazon Linux や Windows、Ubuntu Server 等のオフィシャルイメージには導入済み
  - https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/ami-preinstalled-agent.html
- 幅広い OS に対応
  - https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/prereqs-operating-systems.html



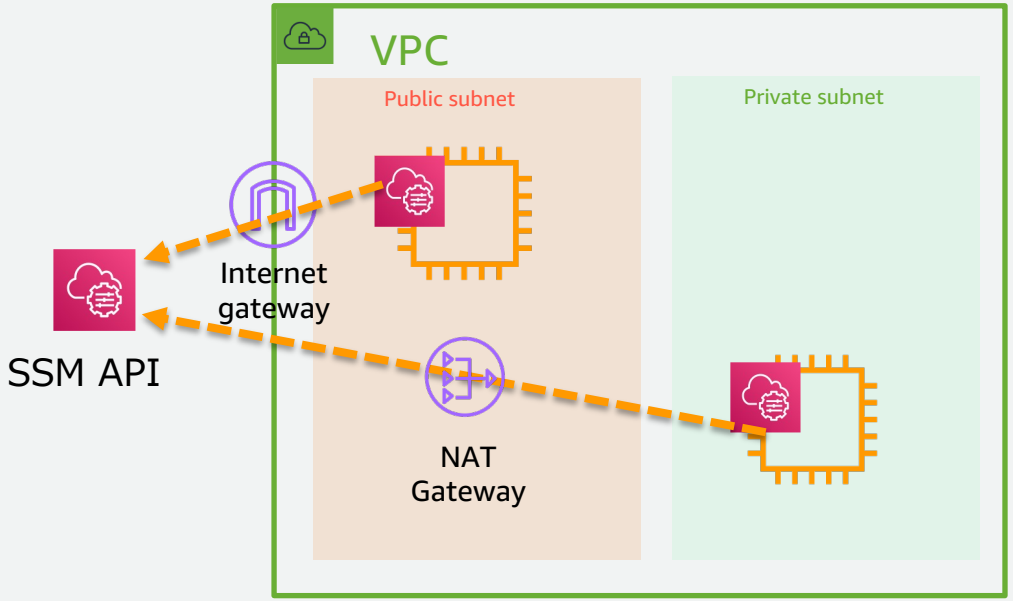
マネージドインスタンスにする方法 ② SSM API への経路確保

- 以下 2 パターンのどちらかで SSM Agent からの アウトバウンド経路を確保する

1. インターネット経由

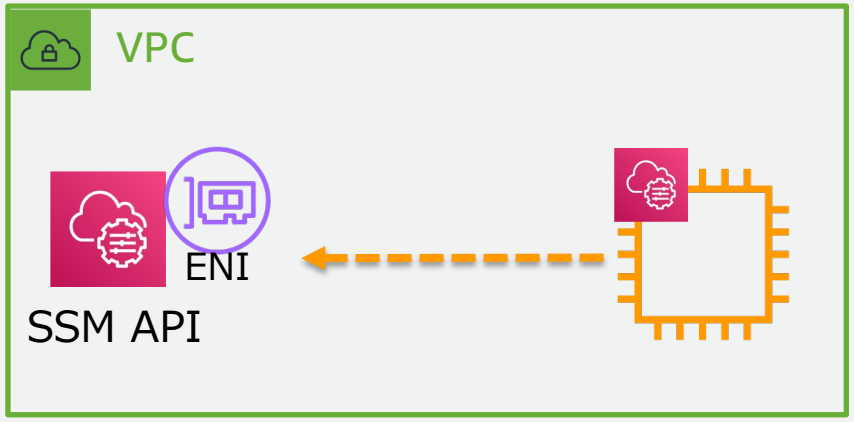
・インバウンドアクセスは不要

・パブリックサブネットやNAT Gatewayを使用



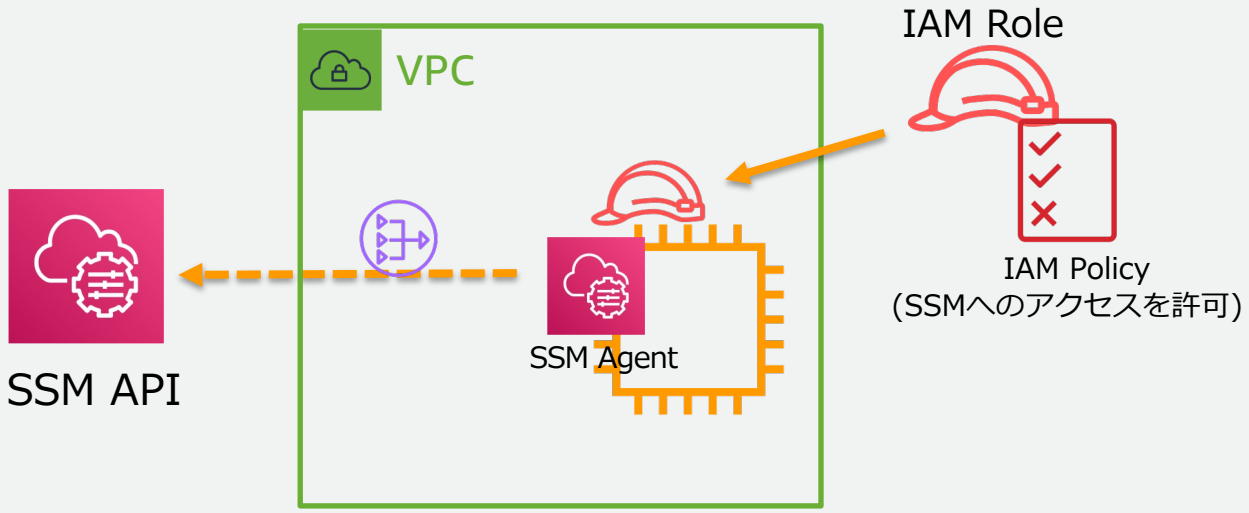
2. VPC エンドポイント経由

・プライベートネットワークによる接続が可能



マネージドインスタンスにする方法 ③ IAM ロール付与

- IAM ロールを作成して EC2 インスタンスにアタッチ
- IAM ポリシー のアタッチ
  - 「AmazonSSMManagedInstanceCore」 でコア機能をアタッチ(必須)



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/session-manager-getting-started-instance-profile.html