



このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar] AWS Systems Manager

サービスカットシリーズ

Solutions Architect 石橋 香代子
2020/02/12

AWS 公式 Webinar
<https://amzn.to/JPWebinar>



過去資料
<https://amzn.to/JPArchive>





石橋 香代子 (いしばし かよこ)

ソリューションアーキテクト

- 流通・小売業界のエンタープライズ企業をサポート
- 運用系サービス

好きなAWSのサービス : **AWS Systems Manager**
Amazon CloudWatch

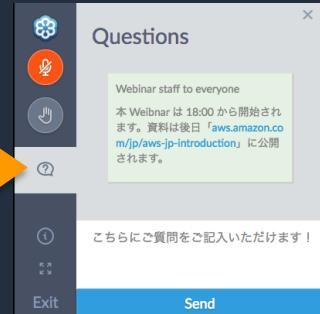
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、Amazon ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問はお答えできませんのでご了承下さい

- ① 吹き出しをクリック
- ② 質問を入力
- ③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2020年02月12日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(<http://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。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

本セッションの目的

- AWS Systems Managerの全体像をご理解いただく。
- AWS Systems Managerの各機能の概要を掴んでいただき、どんなことができるのか、イメージを持っていただく。

本日お話ししないこと

- AWS Systems Managerの各機能の詳細

アジェンダ

1. AWS Systems Manager 全体像
2. AWS Systems Managerを使ってみよう
 1. 準備編
 2. リソースの“今”を把握しよう
 3. SSMで定型運用を実施しよう
 4. 非定型なインタラクティブ操作もSSMで
 5. アプリケーションの設定管理もSSMで
3. AWS Systems Managerのセキュリティーベストプラクティス
4. まとめ

アジェンダ

- 1. AWS Systems Manager 全体像**
2. AWS Systems Managerを使ってみよう
 1. 準備編
 2. リソースの“今”を把握しよう
 3. SSMで定型運用を実施しよう
 4. 非定型なインタラクティブ操作もSSMで
 5. アプリケーションの設定管理もSSMで
3. AWS Systems Managerのセキュリティーベストプラクティス
4. まとめ

AWS マネジメント & ガバナンス サービス

AWS環境の運用管理を スケーラブルかつコスト効率よく行うサービス群

Enable (準備) |



AWS
Control Tower



AWS
Organizations



AWS
Budgets



AWS
License Manager



AWS Well-
Architected Tool

Provision (展開) |



AWS
CloudFormation



AWS
Service Catalog



AWS
OpsWorks



AWS
Marketplace

Operate (操作) |



Amazon
CloudWatch



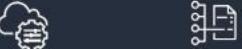
AWS
CloudTrail



AWS
Config



AWS Systems
Manager



AWS Cost and
Usage Report



AWS
Cost Explorer

ビジネスアジャリティとガバナンスコントロールの両立

AWS マネジメント & ガバナンス サービス

AWS環境の運用管理を スケーラブルかつコスト効率よく行うサービス群

Enable (準備) |



AWS
Control Tower



AWS
Organizations



AWS
Budgets



AWS
License Manager



AWS Well-
Architected Tool

Provision (展開) |



AWS
CloudFormation



AWS
Service Catalog



AWS
OpsWorks



AWS
Marketplace

Operate (操作) |



Amazon
CloudWatch



AWS
CloudTrail



AWS
Config



AWS Systems
Manager



AWS Cost and
Usage Report



AWS
Cost Explorer



ビジネスアジャリティとガバナンスコントロールの両立

AWS Systems Manager (AWS SSM)

安全かつスケーラブルにAWS環境を運用するためのコックピット



グループ化

アプリケーションのリソース群をグループ化



可視化

アプリケーション運用上の洞察を可視化
多数のAWSリソースを1つのコンソールで



対応

安全性高いAWSのベストプラクティスで対応

AWSとオンプレミス 両方をサポート

クロスプラットフォーム対応
WindowsもLinuxも

Systems Manager = SSMと略します



AWS SSM : Features (1/2)

全体

AWS Systems Manager ×

高速セットアップ

▼ 運用管理

エクスプローラー 新規

OpsCenter

CloudWatch ダッシュボード

Trusted Advisor と PHD

▼ アプリケーション管理

リソースグループ

AppConfig 新規

パラメータストア

▼ アクションと変更

自動化

カレンダーの変更 新規

メンテナンスウィンドウ

クイックセットアップ

インスタンスをSSMで管理するよう自動構成

オペレーションの管理

Explorer

運用アイテム情報のダッシュボード(XRXA*)

OpsCenter

運用アイテム（対応が必要なイベント）の管理

アプリケーションマネジメント

リソースグループ

タグによるサーバ群のグループ管理

AppConfig

アプリケーション設定（機能フラグ等）の管理

パラメータストア

設定パラメータの集中管理用データストア

アクションと変更

Automation

AWS環境全体に対する自動化処理の実行

Change Calendar

実行可否を制御するカレンダー

メンテナンスウィンドウ

自動化処理のスケジュールと順序の管理

AWS SSM : Features (2/2)

インスタンスとノード

▼ インスタンスとノード

コンプライアンス
インベントリ
マネージドインスタンス
ハイブリッドアクティベーション
セッションマネージャー

Run Command
ステートマネージャー
パッチマネージャー
ディストリビューター

▼ 共有リソース

ドキュメント

コンプライアンス	コンプライアンスの適合状態ダッシュボード
インベントリ	サーバ構成情報のインベントリを閲覧する
マネージドインスタンス	SSM管理対象のサーバ一覧
ハイブリッド アクティベーション	オンプレミスサーバをSSM管理下に入れる
セッションマネージャー	SSMを使ったサーバへリモートアクセスする
Run Command	サーバ群の上でコマンドを実行する
ステートマネージャー	サーバ群の構成を指定した状態に維持する
パッチマネージャー	サーバ群に指定ルールに基づきパッチを適用する
ディストリビューター	サーバ群にパッケージをインストールする

共有リソース

ドキュメント

SSMで実行する処理を記述したドキュメント

アジェンダ

1. AWS Systems Manager 全体像
2. **AWS Systems Managerを使ってみよう**
 1. **準備編**
 2. リソースの”今”を把握しよう
 3. SSMで定型運用を実施しよう
 4. 非定型なインタラクティブ操作もSSMで
 5. アプリケーションの設定管理もSSMで
3. AWS Systems Managerのセキュリティーベストプラクティス
4. まとめ

Step1. まずは、マネージドインスタンスにしよう

The screenshot shows the AWS Systems Manager console with the 'Managed Instances' section selected. On the left, there's a sidebar with various navigation options like 'High-Performance Setups', 'Operational Management', 'Application Management', 'Actions and Changes', and 'Instances and Nodes'. Under 'Instances and Nodes', 'Managed Instances' is highlighted with a red box and has an orange arrow pointing to it from the bottom-left. The main area displays a table of managed instances with columns for 'Instance ID', 'Name', 'Ping Status', and 'Platform Type'. All instances listed are online and belong to the Linux platform type.

Instance ID	Name	Ping の状態	プラットフォームタイプ
i-09605275b13e116e8	-	オンライン	Linux
i-079c3a197ab5682cb	1aPrv_CFnVPC	オンライン	Linux
i-0b177d2cc112d4816	SSMHandsOnWin	オンライン	Windows
i-09e060cf3bee46033	TGWtest	オンライン	Linux

マネージドインスタンス：

- SSM管理下のインスタンス群
- EC2インスタンスのほか、オンプレミスのインスタンスも含まれられる。

マネージドインスタンスにすることで、
オンプレミス/AWSハイブリッド環境のインスタンス管理が可能に

マネージドインスタンスにするために ①SSM 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のオフィシャルイメージには導入済み
 - それ以外のAMI、及びオンプレミスサーバは、手動でインストール
- 幅広い対応OS (WindowsServer2003～、RHEL6.0～、Ubuntu12.04～、Raspbian等)
 - https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/prereqs-operating-systems.html



詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/ssm-agent.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

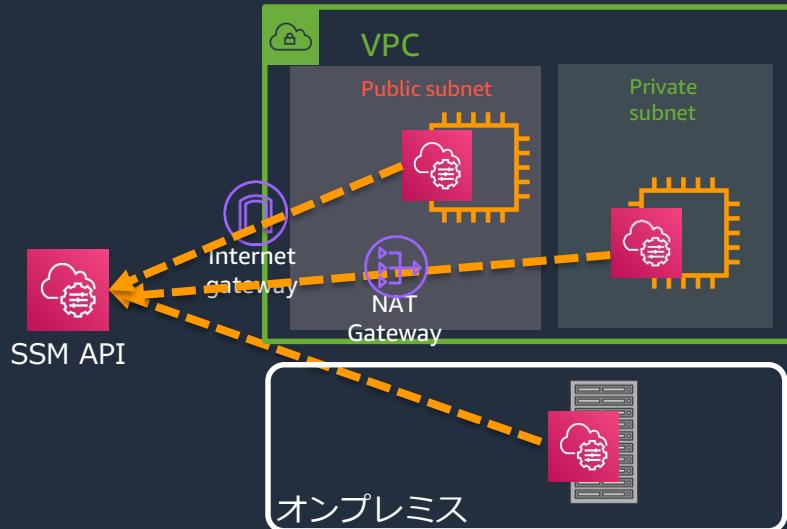


マネージドインスタンスにするために ②SSM APIへの経路確保

- 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。

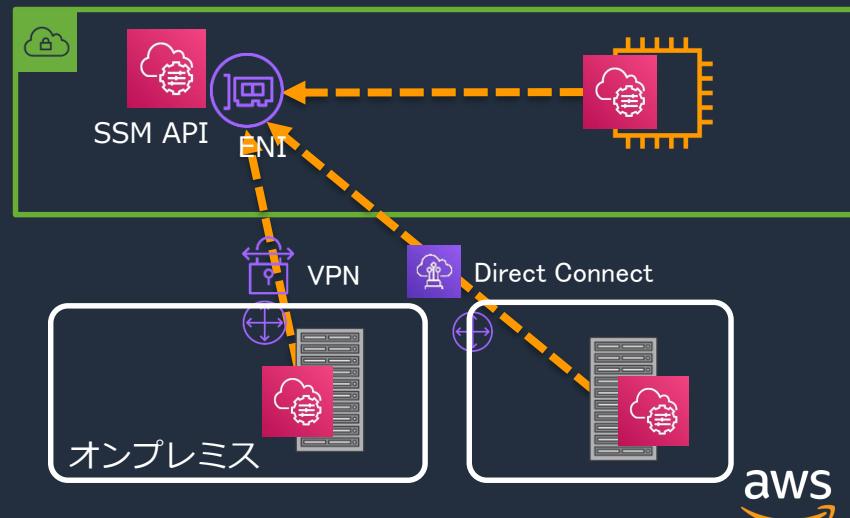
1. インターネット経由

- 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



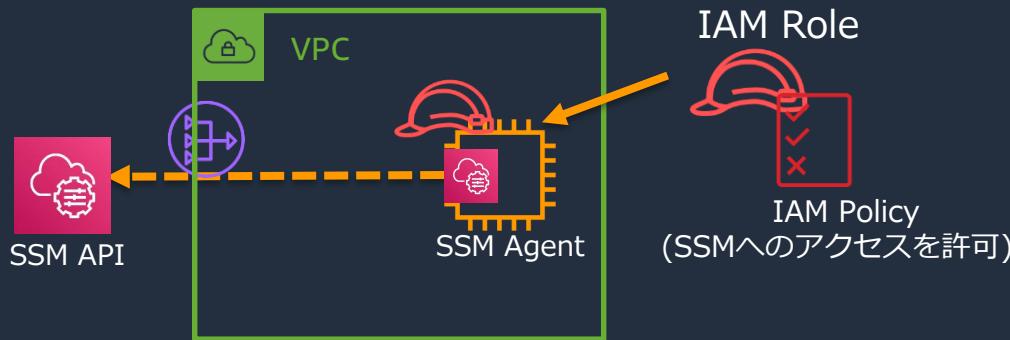
2. VPC エンドポイント経由

- プライベートネットワークによる接続が可能
- オンプレミスからもAWS Direct ConnectやVPN経由で閉域網経由のアクセスが可能



マネージドインスタンスにするために ③ IAMロール付与

- IAMロールを作成し、EC2にアタッチ
- IAMポリシー
 - 1, 「AmazonSSMManagedInstanceCore」でコア機能をアタッチ(必須)
 - 2, 必要に応じて、S3などのポリシーをアタッチ(option)
(※)以前からある「AmazonEC2RoleforSSM」ポリシーの使用も可能だが、権限が広いため、「AmazonSSMManagedInstanceCore」をベースに割り当てる 것을 推奨



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

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



ここまでやれば、晴れてマネージドインスタンスに！

- マネージドインスタンスにするための手順の復習
 - 1, SSM Agentの導入
 - 2, SSM APIへの経路確保
 - 3, IAMロール付与
- しかし、ここで出てくるよくある悩み

全てのインスタンスで、
これを徹底できるかが不安

Agentは導入済みのものを使って
いるし、VPCエンドポイントは一
度作れば問題ないけど、ロールは
一つ一つに設定が必要だし・・・

→ クイックセットアップ

クイックセットアップ[®] (高速セットアップ)

必要なセキュリティロールと一般的に使用される SSM機能をEC2インスタンスですばやく設定



2019/08~

- インスタンスのSSM設定の自動構成ができる機能

- SSM の IAMインスタンスプロファイルのロール
- SSM Agent のスケジュールされた隔週ごとの更新
- 30 分ごとにスケジュールされたイベントリメタデータの収集
- 欠落しているパッチを特定するために、インスタンスを毎日スキヤン
- Amazon CloudWatch エージェントの 1 回限りのインストールと設定
- CloudWatch エージェントのスケジュールに基づく毎月の更新

The screenshot shows the AWS Systems Manager Quick Setup interface. It consists of three main panels:

- Left Panel (Navigation):** Shows the AWS Systems Manager navigation bar with "Quick Setup" highlighted.
- Middle Panel (Main View):** Titled "Systems Manager Quick Setup". It asks for permission roles and provides options for instance profile roles (using default or existing) and CloudWatch agent configuration.
- Right Panel (Options):** Titled "Quick Setup options". It details what Quick Setup configures (agent updates, inventory collection, patch scanning), target selection methods (choose all instances in account/region, specify tags, choose instances manually), and specifies targets as Amazon EC2 instances.

Three blue callout boxes with Japanese text are overlaid on the interface:

- 1, 付与するロールを選択し、
- 2, 実施するジョブを選択し、
- 3, ターゲットを指定する。

クイックセットアップ（高速セットアップ）

必要なセキュリティロールと一般的に使用される SSM機能をEC2インスタンスですばやく設定

- クイックセットアップを使うと・・・
- （いいところ1）新規インスタンスも自動でマネージドインスタンスにすることが可能
 - ただし、SSM Agentが導入されていること、SSM APIへの経路確保されていることが前提
 - すでにロールが割り当てられている場合は、置き換えはしないので注意
- （いいところ2）SSMのベストプラクティスに則って管理できる。
 - 2週間毎のSSM Agentの自動更新、30分おきのインベントリー収集など

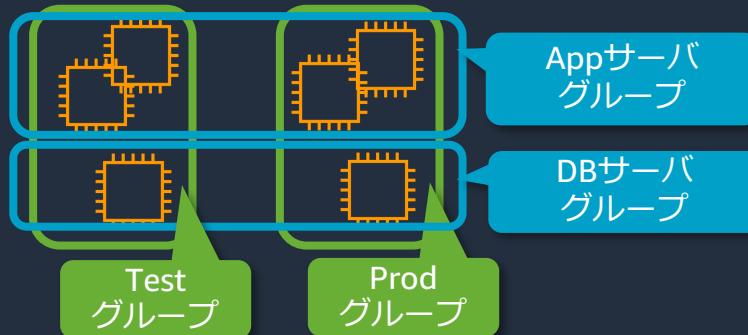
詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-quick-setup.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Step2. インスタンスをグループ化しよう - リソースグループ

- 「リソースグループ」は、AWS リソースをグルーピングすることで、整理・管理をしやすくする機能
 - タグベース or CloudFormationスタックベース で指定できる



- 一括アクションを行うターゲットとして、リソースグループを指定できる。

Run Commandの指定画面

Screenshot of the Run Command target selection interface. It shows three options: 'ターゲット' (Target), 'インスタンスタグの指定' (Specify instance tag), 'インスタンスを手動で選択する' (Select instances manually), and 'リソースグループの選択' (Select resource group). The 'リソースグループの選択' option is highlighted with a red box.

→ リソースグループを
整理しておくと便利

(参考) タグ付けの便利機能 タグエディター

- タグエディターを使用することで、一度に複数のリソースのタグを追加・編集・削除が可能になる。

The screenshot illustrates the Tag Editor feature in the AWS Management Console, specifically for managing EC2 instances. It is divided into three main sections:

- 1, リソースを検索**: The first step shows the "Manager" interface where a new resource group has been saved. A red box highlights the "タグエディター" (Tag Editor) button.
- 2, 結果からタグ管理したいリソースを選択**: The second step shows the search results for EC2 instances. Three instances are listed, each with a checkbox next to its name. A blue box highlights the "リソースを検索する" (Search resources) button.
- 3, タグの一括編集が可能**: The third step shows the Tag Editor interface for the selected instances. It displays a table with columns for Name, Service, and Tags. A blue box highlights the "タグを追加" (Add tag) button.

マネジメントコンソール 上部バー

サービス ▾ **リソースグループ** ▾

Manager X グループを保存しました
グループを作成します

タグエディター

Regions
Select regions ▾
ap-northeast-1 X

リソースタイプ
リソースタイプを選択してください... AWS::EC2::Instance X

タグ - オプション
タグキー オプションのタグ値 **追加**

検索したいリソースが共有するタグキーとオプションの値を入力してから、[追加] を選択、または Enter を押してください。

リソースを検索する

リソースの検索結果 (30 個の中から選択された 3 個)
30 resources を CSV にエクスポートする 選択されたリソースのタグを管理する

タグの編集を行いたいリソースを最大 500 個選択してください。

リソースをフィルタする

名前 サービス リソース

名前	サービス	リソース
EC2 Instance i-0bd8395a07d58c818	EC2	Inst
EC2 Instance i-04de8d0fdbebdb8460	EC2	Inst
EC2 Instance i-062d3c7e98bd5a0de	EC2	Inst

選択されたすべてのリソースのタグの編集
選択されたすべてのリソースのタグを上書きする、またはそれらに新しいタグを追加することができます。 詳細は [こちら](#)

タグキー タグ値 - オプション タグを削除

Environment Prod

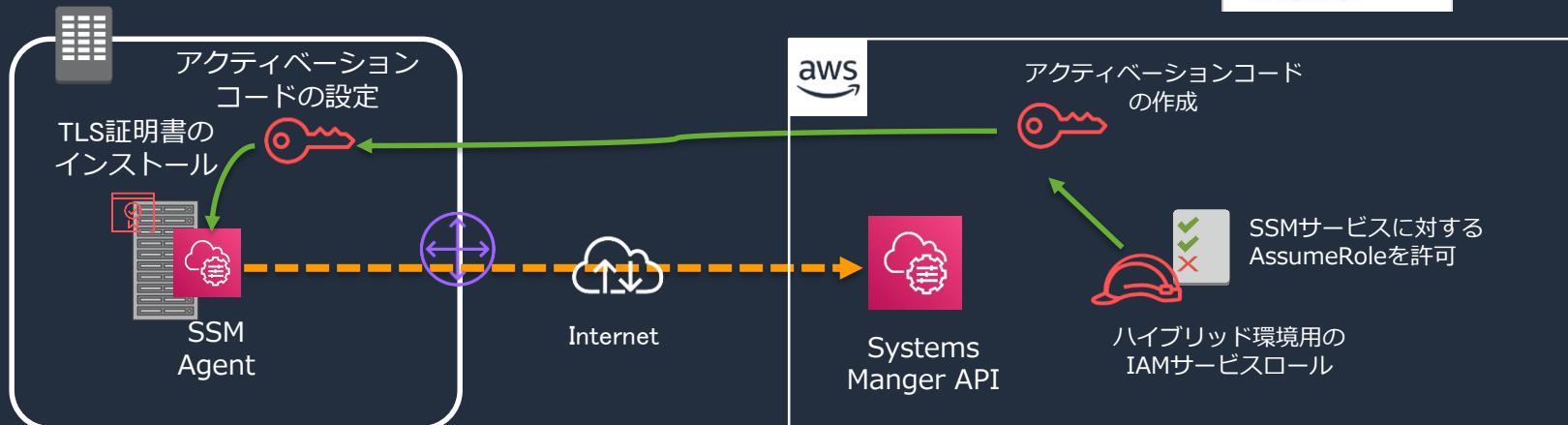
Name

タグを追加

タグを削除

オンプレミスの場合

1. (Option) TLS証明書のインストール
2. ハイブリッド環境用のIAMロールを作成（初回のみ）
3. SSMでアクティベーションコードを生成
4. インスタンスにアクティベーションコードを設定



詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-managedinstances.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



1. 準備編 まとめ

- SSMの管理下におくためには、マネージドインスタンスにする必要がある。
 - そのための3点セット
 - SSMエージェント
 - SSM APIへのアクセス経路
 - EC2ロール
- クイックセットアップでセットアップするのがオススメ
 - 管理されていないインスタンスの排除に有効
 - SSMベストプラクティスに則った管理が可能
- 一括実行の単位となるリソースグループを作成しておくと管理しやすい。
 - タグエディターをうまく使って、インスタンスにタグ定義を
- オンプレミスも管理できる。
 - SSMを使ってEC2もオンプレミスも同じように運用を

アジェンダ

1. AWS Systems Manager 全体像
2. **AWS Systems Managerを使ってみよう**
 1. 準備編
 2. **リソースの“今”を把握しよう**
 3. SSMで定型運用を実施しよう
 4. 非定型なインタラクティブ操作もSSMで
 5. アプリケーションの設定管理もSSMで
3. AWS Systems Managerのセキュリティーベストプラクティス
4. まとめ

2.リソースの“今”を把握しよう

1、AWSリソースに関する情報を把握するためのダッシュボード

ご紹介する機能

- SSM Explorer
- SSM OpsCenter
- コンプライアンス

2、インスタンスの“中身”を把握するための機能

ご紹介する機能

- SSM インベントリ

2.リソースの“今”を把握しよう

1、AWSリソースに関する情報を把握するためのダッシュボード

ご紹介する機能

- SSM Explorer
- SSM OpsCenter
- コンプライアンス

2、インスタンスの“中身”を把握するための機能

ご紹介する機能

- SSM インベントリ

AWSリソースに関する情報を把握する（デモ）

- みなさまが運用担当者なら・・・
 - 朝出社して、まずインスタンスの状況を確認
 - そして、何か問題が起きていないか、確認
 - 問題が起きているようだと、その詳細を確認
 - 必要に応じて修復のためのアクションを実施

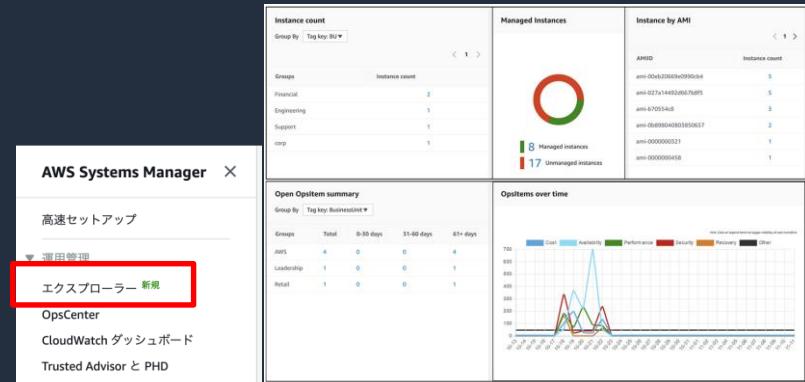
AWS SSM Explorer

AWSリソースに関する情報をレポートするオペレーションダッシュボード



2019/11～

- クロスアカウント、クロスリージョンで、"今"のリソース状況を可視化できる。
 - Explorerでは、一つ一つのオペレーションデータを"OpsData"と呼ぶ。
 - Explorerは、アカウントおよびリージョン全体のOpsDataの集約ビュー
 - クロスアカウントは AWS Organizationsが前提
- デフォルトのダッシュボードに表示されるOpsData
 - EC2情報
 - EC2インスタンス数
 - マネージドインスタンス数
 - AMI別インスタンス
 - OpsCenter OpsItems
 - パッチコンプライアンス



詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/Explorer.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



AWS SSM OpsCenter



AWSリソースに関する運用作業項目 (OpsItems) を表示、調査、解決できるダッシュボード



2019/06～

- 運用作業項目 (OpsItems) を表示、調査、解決できるダッシュボード
 - サマリは、Explorerのダッシュボードにも表示される。
- OpsItemsに対して修復を行ったり、対応の完了を記録してクローズするなど、運用タスク管理に利用できる。
- CloudWatch Eventsのルールとして登録する。
 - デフォルトでEC2やRDS、SSMなどのイベントが登録済み
 - Amazon EventBridgeと連携でき、外部アラートも登録することが可能

The screenshot shows the AWS Systems Manager console. In the top navigation bar, there is a dropdown menu labeled "AWS Systems Manager" with "OpsCenter" highlighted by a red box. Below the navigation bar, there are sections for "高速セットアップ", "運用管理", and "CloudWatchダッシュボード". On the right side of the screen, there is a detailed dashboard titled "Opsitem のステータス概要" showing counts for resolved, unresolved, and in-progress items across SSM, EC2, and RDS. Below this, there is a table titled "ソースと年齢別の Opsitem" showing item counts grouped by source and age range.

詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/OpsCenter.html
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



AWS SSM コンプライアンス

コンプライアンスに準拠していないリソースを表示できるダッシュボード

- コンプライアンス準拠していないリソースを特定できるダッシュボード
- デフォルトでは、以下がコンプライアンスとして定義済み
 - パッチ適用状況(Patch)
 - SSM パッチマネージャーのScan結果を集計
 - SSM Explorerのダッシュボードにも
 - ステートマネージャの関連づけ状況(Association)
 - SSM ステートマネージャの稼働状況を集計
- カスタムコンプライアンスタイルの定義も可能
 - 例)ソフトウェアXのバージョン4.0以外のインスタンスは非準拠とする。

The screenshot shows the AWS Systems Manager Compliance Dashboard. On the left, there's a sidebar with a navigation menu. The 'Compliance' option is highlighted with a red box. Below it, there's a summary table with two rows: 'Association' and 'Patch'. The 'Association' row has values: 10 (green), 5 (red), 0 (green), 0 (green), 0 (green), 0 (green), 0 (green), 0 (green). The 'Patch' row has values: 11 (green), 1 (red), 0 (green), 0 (green), 0 (green), 0 (green), 0 (green), 0 (green).

コンプライアンスタイル	準拠リソース	非準拠リソース	重要なリソース	高リソース	中リソース	低リソース	信頼リソース
Association	10	5	0	0	0	0	0
Patch	11	1	0	0	0	0	0

2.リソースの“今”を把握しよう

1、AWSリソースに関する情報を把握するためのダッシュボード

ご紹介する機能

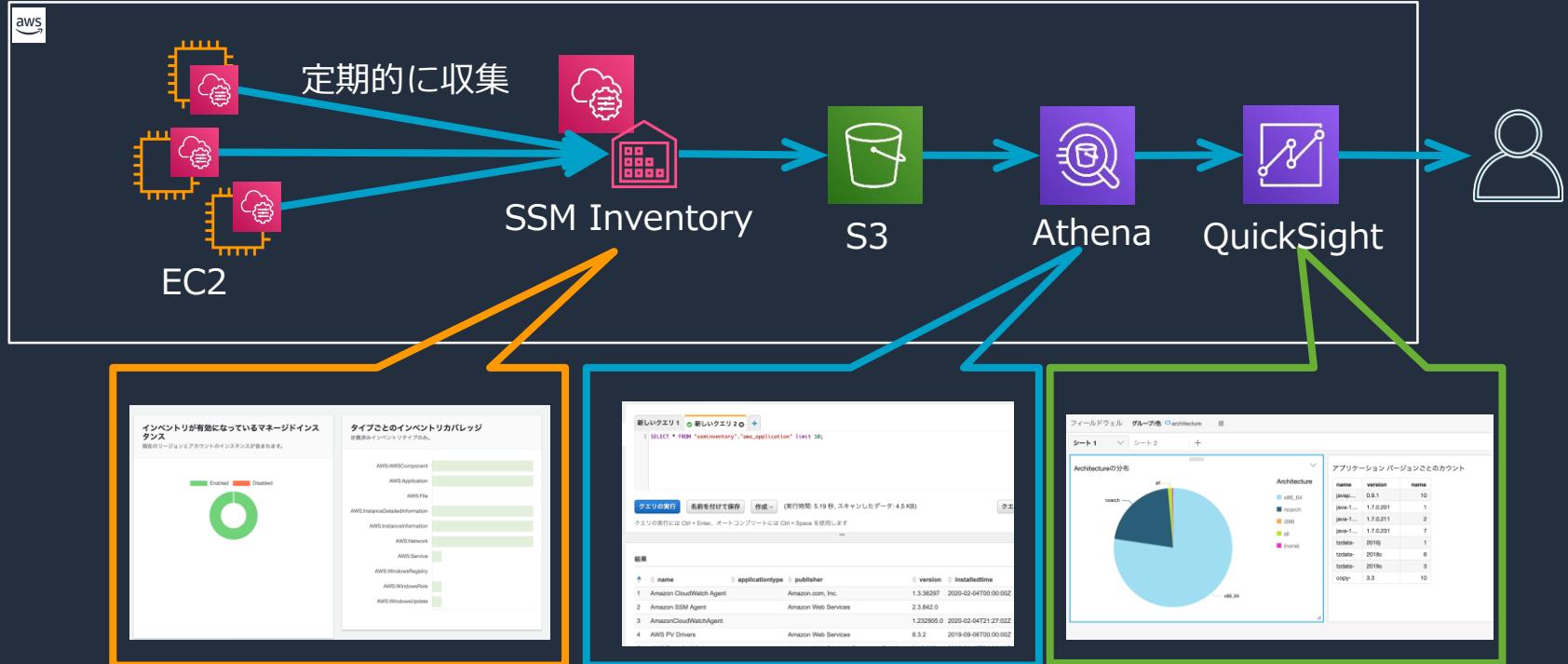
- SSM Explorer
- SSM OpsCenter
- コンプライアンス

2、インスタンスの“中身”を把握するための機能

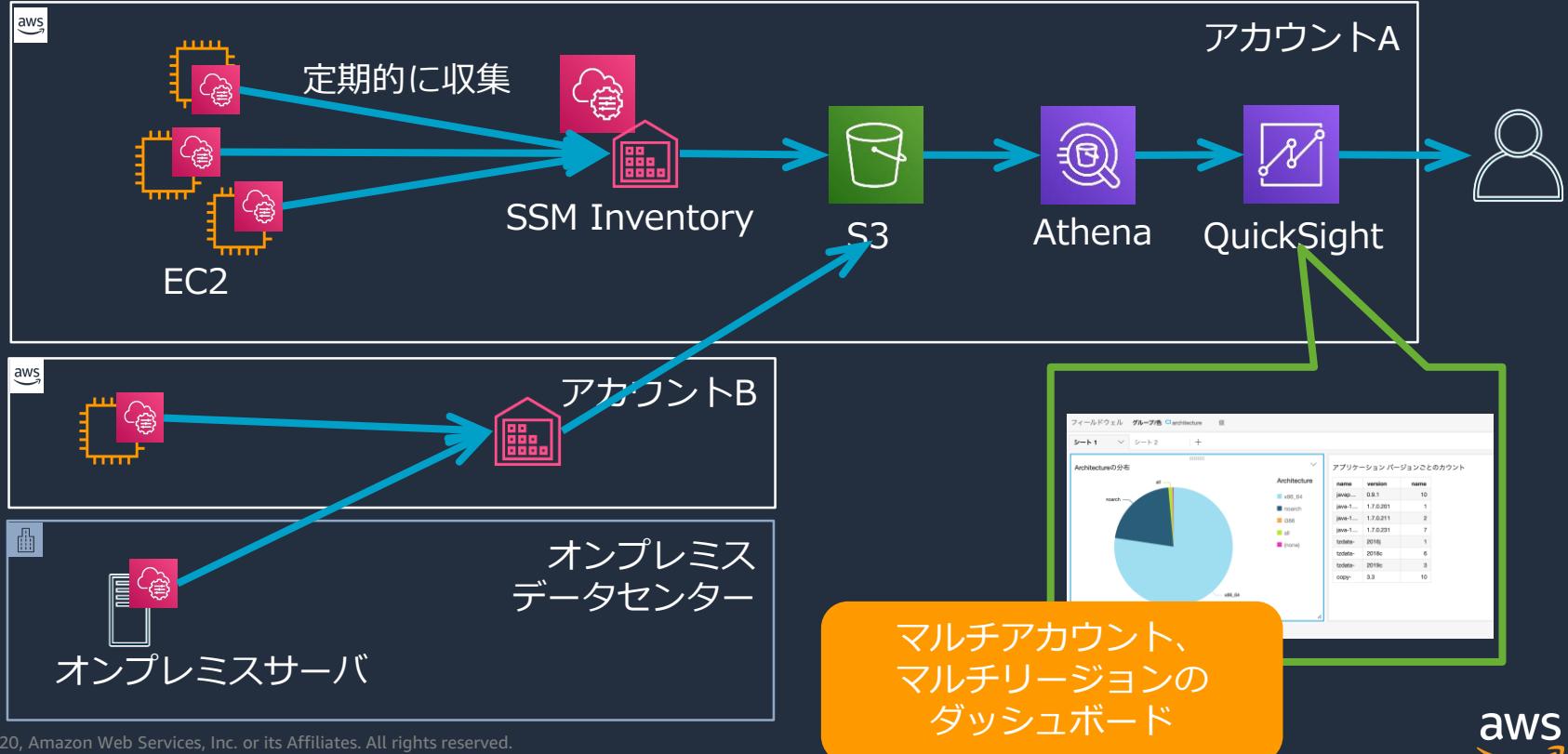
ご紹介する機能

- SSM インベントリ

デモの流れ



マルチアカウント/マルチリージョンのダッシュボード

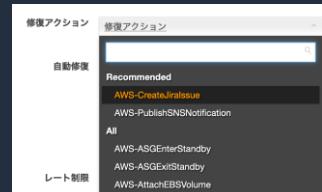
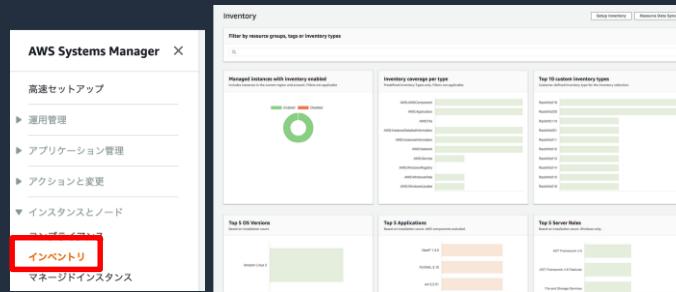


AWS SSM インベントリ



マネージドインスタンスからメタデータを収集し可視化

- OS上のアプリケーション一覧など構成情報を記録し、可視化する。
- ステートマネージャーを使用して定期的に収集
 - クイックセットアップにてセットアップできる
 - 構成情報データはS3バケットに保管
- Athena, QuickSightを用いてマルチアカウント/マルチリージョン横断分析も
- AWS Configに構成情報を送信し、
インベントリ情報の変更追跡が可能
 - Config Rulesで準拠状況をチェック
 - 修復アクションで自動対応も



詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-inventory.html
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



AWS SSM インベントリ



マネージドインスタンスからメタデータを収集し可視化

- インベントリで収集できるメタデータタイプの一覧

取得できる情報	詳細
アプリケーション	アプリケーション名、発行元、バージョンなど。
AWS コンポーネント	EC2 ドライバ、エージェント、バージョンなど
ファイル	名前、サイズ、バージョン、インストール日、変更および最新アクセス時間など パス(C:\Program Files など)、パターン(*.exe, *.logなど)を指定し、再帰的に抽出できる
ネットワーク設定の詳細	IP アドレス、MAC アドレス、DNS、ゲートウェイ、サブネットマスクなど
Windows アップデート (Winのみ)	Windows Updateに関する情報 (Hotfix ID、インストール者、インストール日など)
インスタンスの詳細	OS名、OSバージョン、最終起動、DNS、ドメイン、ワークグループ、OS アーキテクチャなど
Windows サービス (Winのみ)	名前、表示名、ステータス、依存サービス、サービスのタイプ、起動タイプなど
タグ	インスタンスに割り当てられているタグ
Windows レジストリ (Winのみ)	レジストリキーのパス、値の名前、値タイプおよび値
Windows ロール (Winのみ)	名前、表示名、パス、機能タイプ、インストール日など
カスタムインベントリ	カスタムに割り当てられるメタデータ。例えばオンプレミスの各インスタンスのラック位置など。

- 上記のほか、SSM 設定コンプライアンスで取得されるパッチコンプライアンス、関連づけコンプライアンス情報も、インベントリとして保存される。

2.リソースの“今”を把握しよう　まとめ

1、AWS リソースに関する情報は
AWS Explorerで。
マルチアカウント/マルチリージョン



- ・インスタンス数
- ・マネージドインスタンス
- ・AMI別インスタンス

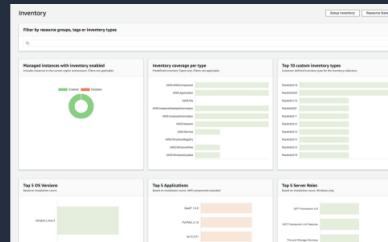
詳細は、**SSM OpsCenter**へ

- ・運用タスクリスト
- ・関連リソースの調査
- ・修復アクションの実行

詳細は、**コンプライアンス**へ

- ・パッチ適用状況
- ・ステートマネージャ適用状況
- ・その他コンプラ定義準拠状況

2、インスタンスの“中身”は
SSM インベントリ で。



- ・インストール済アプリ
- ・ファイル情報
- ・OS情報 など

Athena/QuickSightと連携し
マルチアカウント/マルチリージョン
分析が可能



Java 6がインストールされている
インスタンス一覧は？



アジェンダ

1. AWS Systems Manager 全体像
2. **AWS Systems Managerを使ってみよう**
 1. 準備編
 2. リソースの“今”を把握しよう
 - 3. SSMで定型運用を実施しよう**
 4. 非定型なインタラクティブ操作もSSMで
 5. アプリケーションの設定管理もSSMで
3. AWS Systems Managerのセキュリティーベストプラクティス
4. まとめ

SSMができる定型作業の整理

1、SSMでは、運用処理をSSMドキュメントにて定義し、実行する。

- 汎用的な処理は、事前定義されたドキュメントあり
- カスタマイズした処理を実現したい場合は、ドキュメントを自作する。

The screenshot shows the AWS Systems Manager console with the 'AWS Systems Manager > ドキュメント' page. It displays three categories of documents: 'Amazon が所有' (Predefined), '自己所有' (Self-owned), and 'Shared with me'. A red box highlights the 'ドキュメント' tab under '共有リソース', which is labeled '共有されたドキュメント'. To the right, a large green box contains the text '実体は JSON or YAML' and a snippet of JSON/YAML code for a document named 'aws-downLoadContent'. The code defines actions like downloading content and running shell scripts.

AWS Systems Manager > ドキュメント

Amazon が所有 | 自己所有 | Shared with me

事前定義ドキュメント

自作ドキュメント

共有されたドキュメント

ドキュメント

SSMドキュメント

実体は
JSON or YAML

```
mainSteps: [
  {
    "action": "aws:downloadContent",
    "name": "downloadContent",
    "inputs": {
      "SourceType": "{{ SourceType }}",
      "SourceInfo": "{{ SourceInfo }}"
    }
  },
  {
    "action": "aws:runShellScript",
    "name": "runShellScript",
    "inputs": {
      "runCommand": [
        "#!/bin/bash",
        "if [[ ${!AWS_SSM_DOCUMENT_DEPENDENCIES} == True ]]; then",
        "  echo \"Ingesting and updating required tools: ${AWS_SSM_DOCUMENT_DEPENDENCIES}\""
      ]
    }
  }
],
```

2、事前定義ドキュメントの中でも、需要が多く複雑な処理は、ドキュメントの実行フレームワークをSSMの機能として提供

	処理内容	実行するSSMドキュメント	実行フレームワーク
1	サーバの構成情報の収集	AWS-GatherSoftwareInventory	SSM インベントリ
2	パッチ適用プロセスの自動化	AWS-RunPatchBaseline	SSM パッチマネージャー
3	ソフトウェアパッケージの配布	AWS-ConfigureAWSPackage	SSM ディストリビューター

詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-ssm-docs.html
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



SSMができる定型作業の整理

1、SSMでは、運用処理をSSMドキュメントにて定義し、実行する。

- 汎用的な処理は、事前定義されたドキュメントあり
- カスタマイズした処理を実現したい場合は、ドキュメントを自作する。

AWS Systems Manager > ドキュメント

Amazon が所有 | 自己所有 | Shared with me

事前定義ドキュメント | 自作ドキュメント | 共有されたドキュメント

ドキュメント

SSMドキュメント

```
mainSteps: [
  {
    "action": "aws:downloadContent",
    "name": "downloadContent",
    "inputs": {
      "SourceInfo": "{{ SourceType }}",
      "SourceInfo": "{{ SourceInfo }}"
    }
  },
  {
    "action": "aws:runShellScript",
    "name": "runShellScript",
    "inputs": {
      "runCommand": [
        "#!/bin/bash",
        "if [[ ${!AWS_SSM_DOCUMENT_DEPENDENCIES} == True ]]; then",
        "  echo ${!AWS_SSM_DOCUMENT_DEPENDENCIES} and updating required tools: ${!AWS_SSM_DOCUMENT_REQUIRED_TOOLS}"
        "fi"
      ]
    }
  }
]
```

実体は JSON or YAML

2、事前定義ドキュメントの中でも、需要が多く複雑な処理は、ドキュメントの実行フレームワークをSSMの機能として提供

	処理内容	実行するSSMドキュメント	実行フレームワーク
1	サーバの構成情報の収集	AWS-GatherSoftwareInventory	SSM インベントリ
2	パッチ適用プロセスの自動化	AWS-RunPatchBaseline	SSM パッチマネージャー
3	ソフトウェアパッケージの配布	AWS-ConfigureAWSPackage	SSM ディストリビューター

詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-ssm-docs.html
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



SSMドキュメントで運用を定義し実行する(デモ)

- 例えば・・・
 - あるタスクの日には、プロジェクトチームがやってくる
 - その日には、プロジェクトチーム用のEC2を立ち上げておきたい
- デモでやること
 1. タスクがある日をカレンダーで定義
 2. カレンダーで実施可否を確認後、EC2を立ち上げ、ステータスチェックをするSSMドキュメントを作成
 3. 作成したSSMドキュメントを実行

デモの流れ

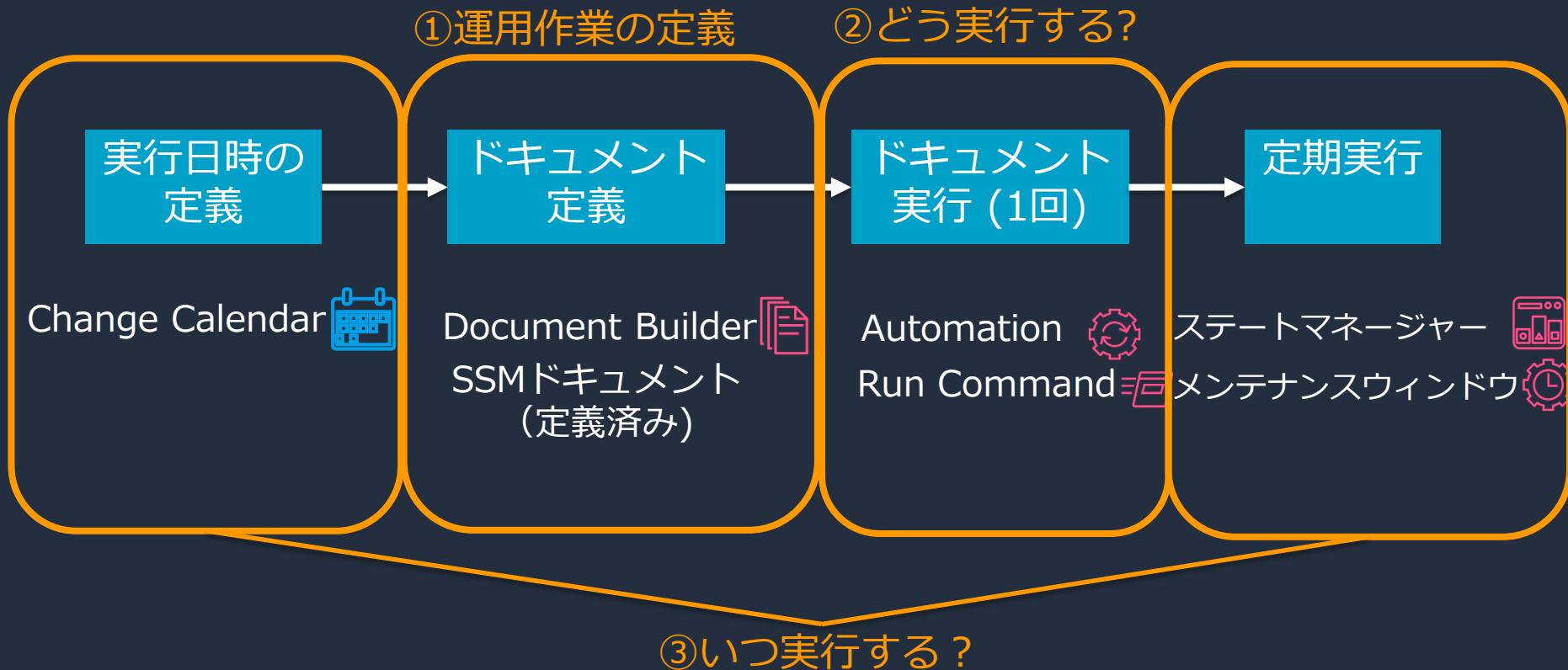


Change Calendar

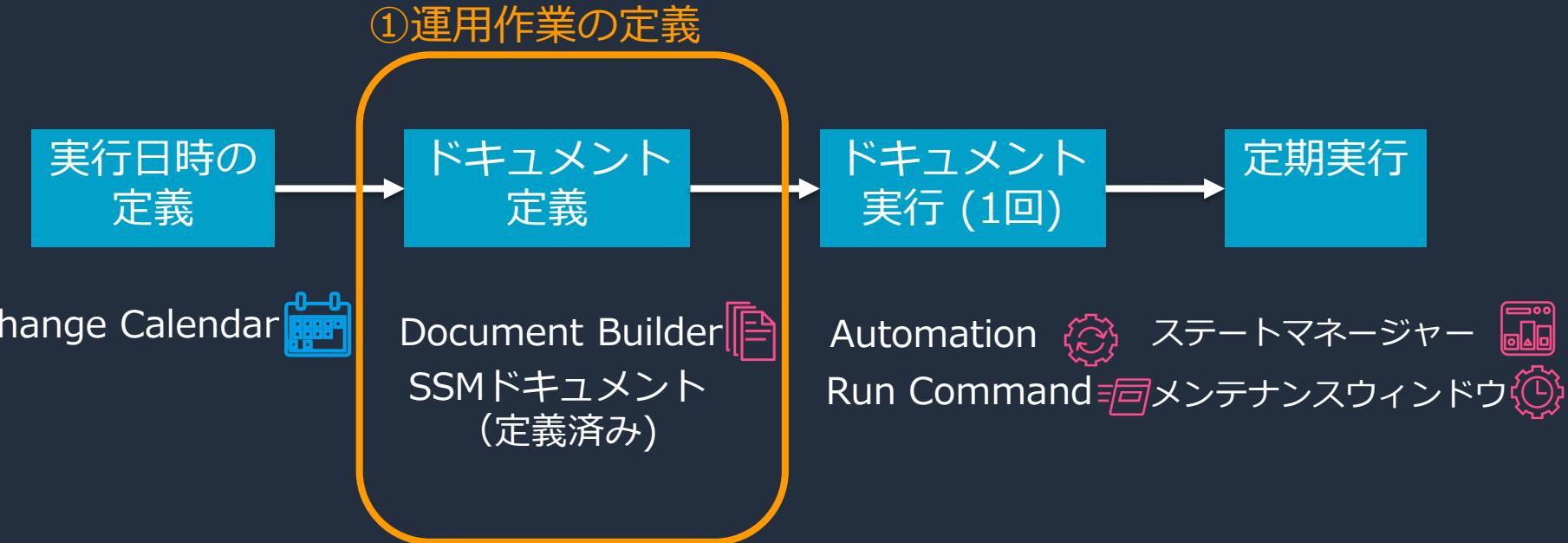
Document Builder
SSM ドキュメント
(定義済み)

Automation ステートマネージャー
Run Command メンテナンスウィンドウ

運用作業の定義・実行の流れ

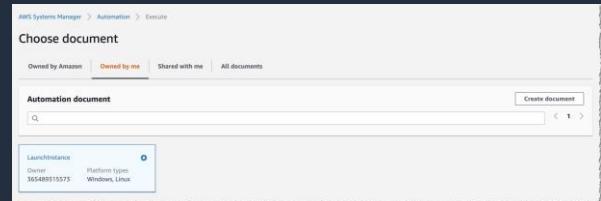
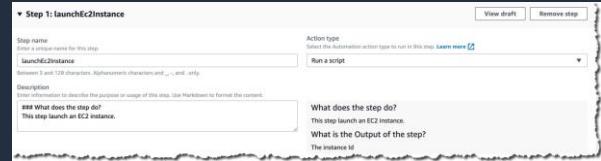


運用作業の定義・実行の流れ



① まずは運用作業の定義 Document Builder

- 自動化ドキュメント (Automation Playbook) を作成するための**ウィザード形式**のツール
 - PythonやPowerShellのコードを直接記述することも可能
 - 使い方や目的の説明をMarkdown形式で残すことができる
- 条件分岐を使用した動的ワークフローも可能
- AWSの操作もOS上での操作もこれ一本で記述できるため、運用の自動化がさらに容易に



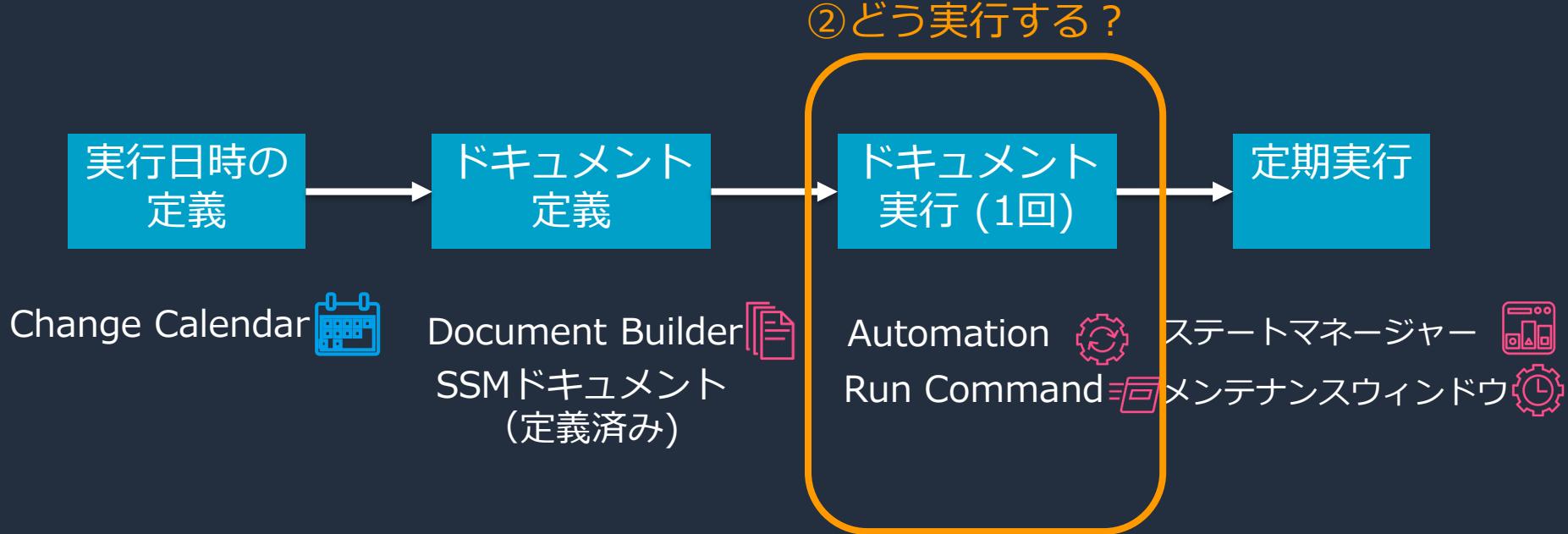
詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/automation-document-builder.html
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



2019/11~



運用作業の定義・実行の流れ



② 定義したもの (SSMドキュメント)をどう実行する？

• Run Command : OS上でコマンドを実行

例) ShellScriptの実行、AnsiblePlaybookの実行

- コマンドドキュメントを実行する
- サーバログイン不要
- RDPやSSHのためのインバウンドポート開放不要



• Automation : AWSサービス全体に渡ったワークフロー

例) RDS Snapshot作成、任意のAWS API実行

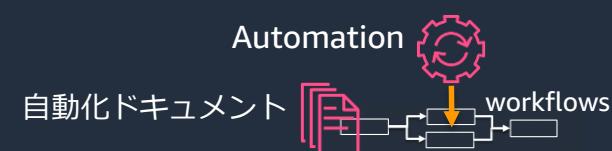
- 自動化ドキュメントを実行する
- AWSの操作もOS上での操作も



詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/execute-remote-commands.html

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-automation.html

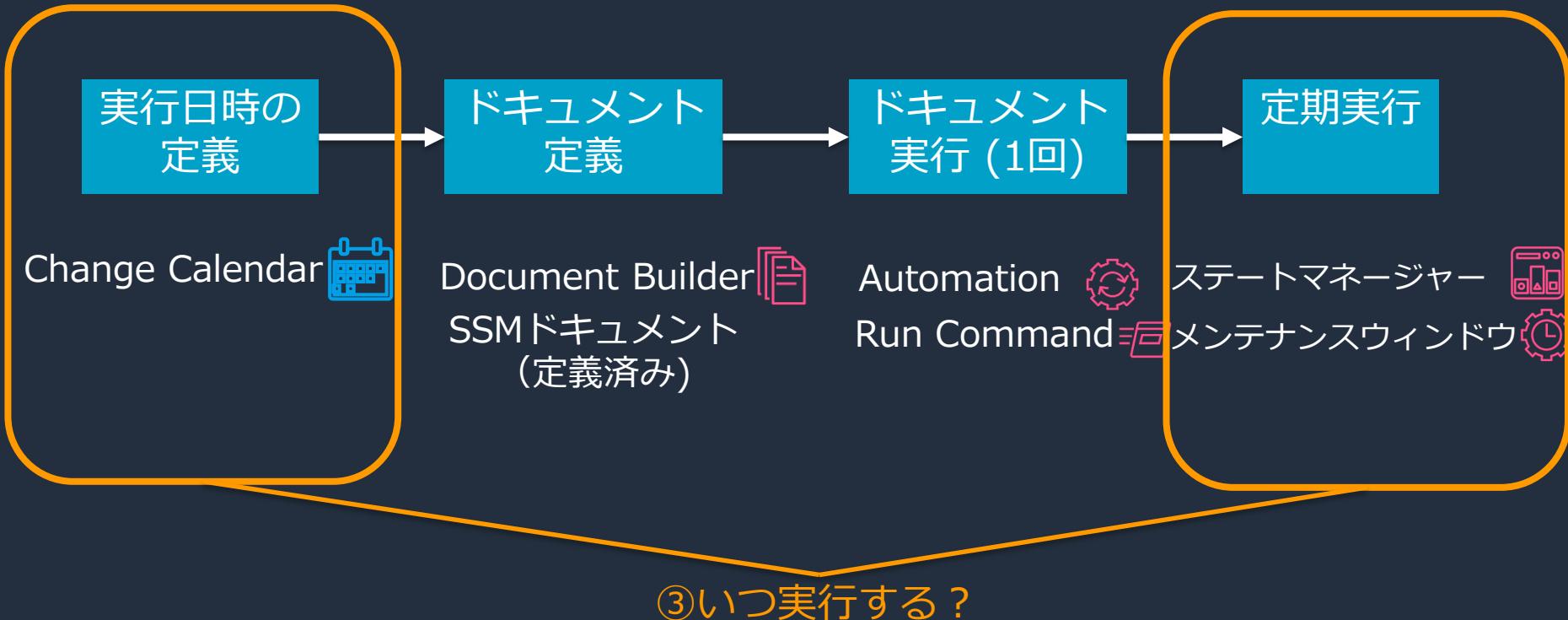
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



任意のAWS APIの実行
AWS lambdaの実行
Change Calendar確認 etc



運用作業の定義・実行の流れ



③ いつ実行する？

- 1度きりの手動実行なら
 - Run Command をそのまま「実行」
 - Automation をそのまま「実行」
- 繰り返し実行したい定期実行なら
 - ステートマネージャー
 - メンテナンスウィンドウ
- (手動実行でも定期実行でも) 実行できる日時を制御するなら
 - Change Calendar

SSM ステートマネージャー

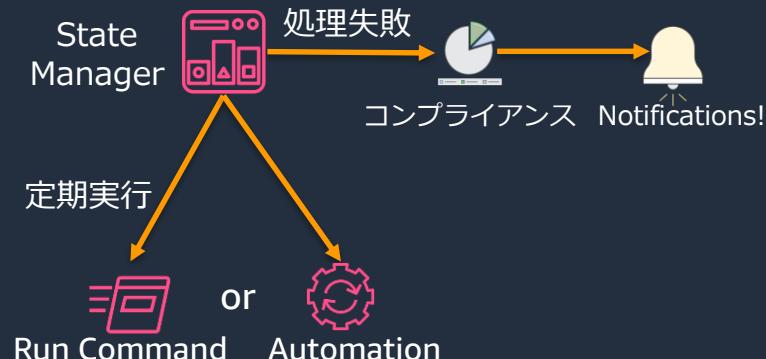
定義された状態に保つプロセスを自動化



- サーバ群に対して定期的に処理を行うためのフレームワーク
 - サーバの状態を確認・是正するための定期的な処理に向く
 - 例) インベントリ収集、SSM Agentの定期更新
 - 処理が失敗すると、求める状態を維持できていないと判断され、コンプライアンスにレポートされる

The screenshot shows the AWS Systems Manager console with the 'State Manager' tab selected. The main area displays a configuration for a scheduled task named 'AWS-UpdateSSMAgent'. Key details include:

- ターゲット**: Who (The target resources)
- ドキュメント名**: AWS-UpdateSSMAgent
- ドキュメントのバージョン**: \$DEFAULT
- ステータス**: 活動中 (Active)
- 作成日**: Sat, 04 Jan 2020 01:22:54 GMT
- 関連付けの最終更新日**: Sat, 25 Jan 2020 14:22:03 GMT
- スケジュール式**: rate(14 days)
- 最終実行日**: Sun, 26 Jan 2020 03:26:54 GMT
- 出力 S3 パケット**: -
- MaxConcurrency**: -
- MaxErrors**: -
- 関連付けステータス別インスタンス数**: Pending:3, Success:13
- コンプライアンスの重要度**: 指定しない



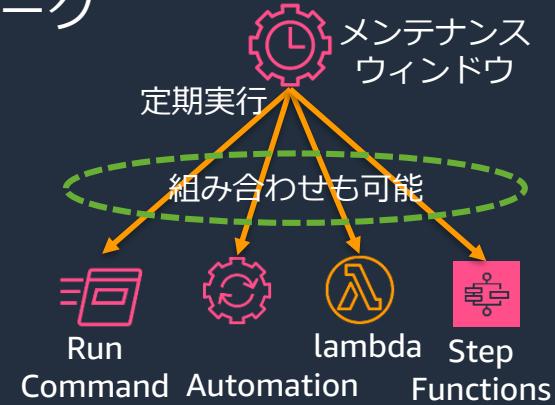
詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-state.html
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



SSM メンテナンスウィンドウ

アクションを実行するスケジュールを定義

- ・ サーバ群に対して定期的に処理を行うためのフレームワーク
 - ・ サービス停止を伴うような比較的重い処理に向く
 - ・ 例) OSパッチ適用、バックアップ取得
 - ・ ステートマネージャーと比べ、精緻な制御が可能
 - ・ 複数のタスク同士の関連性の定義
 - ・ 残り時間がない場合は処理を起動しない etc
 - ・ Lambda、Step Functionsも実行可能



AWS Systems Manager X

説明 タスク 履歴 ターゲット タグ

誰に

ターゲット

タスク

タグ

高機能セットアップ

運用管理

アプリケーション管理

アクションと変更

自動化

カレンダーの変更 新規

メンテナンスウィンドウ

説明

ウィンドウ ID: mw-0000d5625bf5315d0

名前: test-patchApply

状態: 有効

次に実行時間: 2020年2月9日(日) 16:30:00 UTC

期間: 3時間

タスク

タスク ID

優先度

名前

タスク ARN

385d0305-f1a7-4673-adf3-a126a2ac800f

1

patch-apply

AWS-RunPatchBaseline

f5abb5a9-bfa6-4c44-af93-bb9d355cd924

2

lambda-task

arn:aws:lambda:ap-northeast-1:123456789012:lambda-task

タスクのスケジュールタイムゾーン: Asia/Tokyo

未登録ターゲットを許可: はい

カットオフポイント: ウィンドウが閉じる前の 1 分

ウィンドウの終了日: -

いつ:

ウィンドウの開始時間、長さ、タスク実行開始を許可する残り時間を指定可能

何を :

タスクを複数定義でき 優先順位も指定可能

詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-maintenance.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



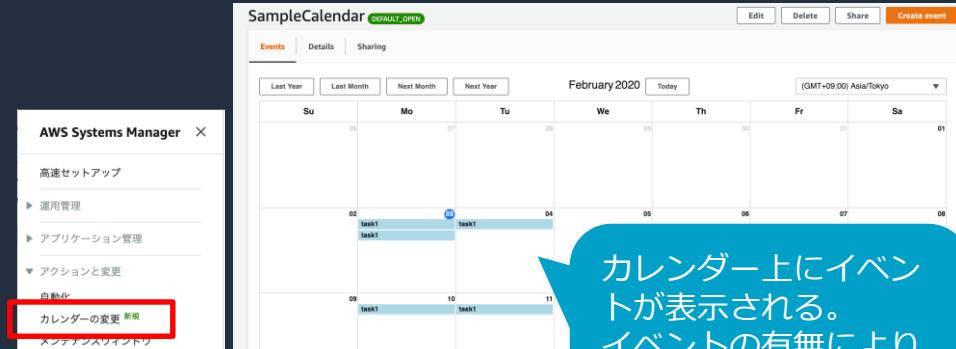
SSM Change Calendar

NEW

指定したアクションが実行できるまたはできない日付と時刻の範囲を設定

2019/12～

- システム内で利用するカレンダー情報を集中管理するサービス
- 実行可否の判定結果を提供する (Open/Closed)
- Calendarタイプは2種類
 - Open by default
 - Closed by default
- マルチアカウントでの共有が可能
- SSM Automationには統合ずみ
他のサービスとも統合を予定



カレンダー上にイベントが表示される。
イベントの有無により
「Open」「Closed」が
判定される。

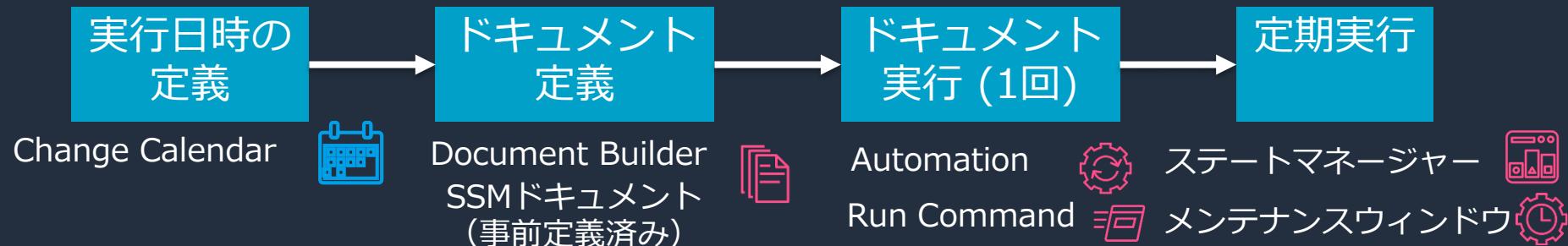
詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-change-calendar.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



SSMができる定型作業の整理

1、運用処理をSSMドキュメントにて定義し、実行する。



2、SSMの機能として、ドキュメントの実行フレームワークが提供されている処理を実行する。

	処理内容	実行するSSMドキュメント	実行フレームワーク
1	サーバの構成情報の収集	AWS-GatherSoftwareInventory	SSM インベントリ
2	パッチ適用プロセスの自動化	AWS-RunPatchBaseline	SSM パッチマネージャー
3	ソフトウェアパッケージの配布	AWS-ConfigureAWSPackage	SSM ディストリビューター

AWS SSM パッチマネージャー

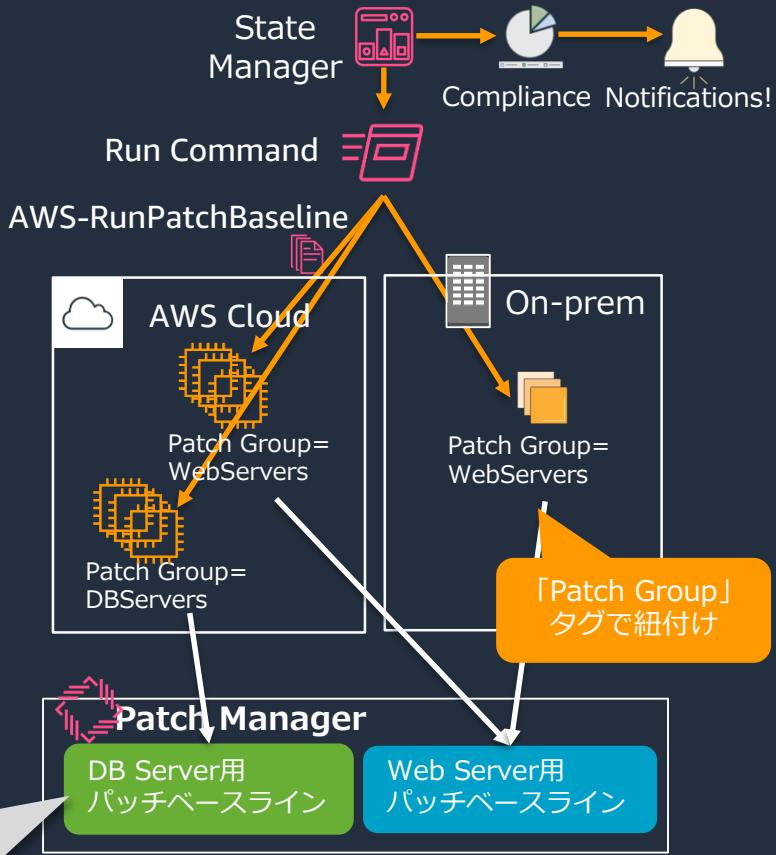


マネージドインスタンスにパッチを適用するプロセスを自動化

- ・ パッチルール準拠の確認、インスタンスへのパッチ適用が可能
- ・ Scanのみ | Scan & Installの2通り
 - ・ Scanの定期実行はクイックセットアップで設定され、結果を設定コンプライアンスにレポート
- ・ パッチベースラインをOSの種類ごとに作成
 - ・ パッチ適用ルール
 - ・ OS+用途で分けるなど、複数作成可能
- ・ パッチベースラインは「Patch Group」タグ(固定)で紐付け

パッチベースラインの例

OS: Windows
製品 : Windows Server 2016
分類 : Security Update
重要度 : Critical
自動承認の遅延 : 7日
承認済みパッチ : KB111111
拒否済みパッチ : KB222222



AWS SSM パッチマネージャー



マネージドインスタンスにパッチを適用するプロセスを自動化

- パッチマネージャー その他

- インスタンスに指定されたパッチダウンロードサイトへのアクセス経路の確保が必要
 - Windowsインスタンスは、Microsoft Windows Update サイトにアクセスできること
 - プライベートネットワーク内のWSUSサーバをレポジトリに構成することも可能
 - Linuxインスタンスは、インスタンスに設定されたリポジトリへ接続できること
- パッチ適用後の再起動は、NoRebootオプションでタイミングを制御可能
- パッチ自動承認のタイミング指定は以下の2通りから選択
 - パッチがリリースされてからX日経過したらパッチを承認する
 - 特定の日付までにリリースされたパッチを承認する
- パッチマネージャーがサポートするOSは、SSMサポートOSと異なるので注意
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-patch.html



2020/01～



2020/02～



詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-patch.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



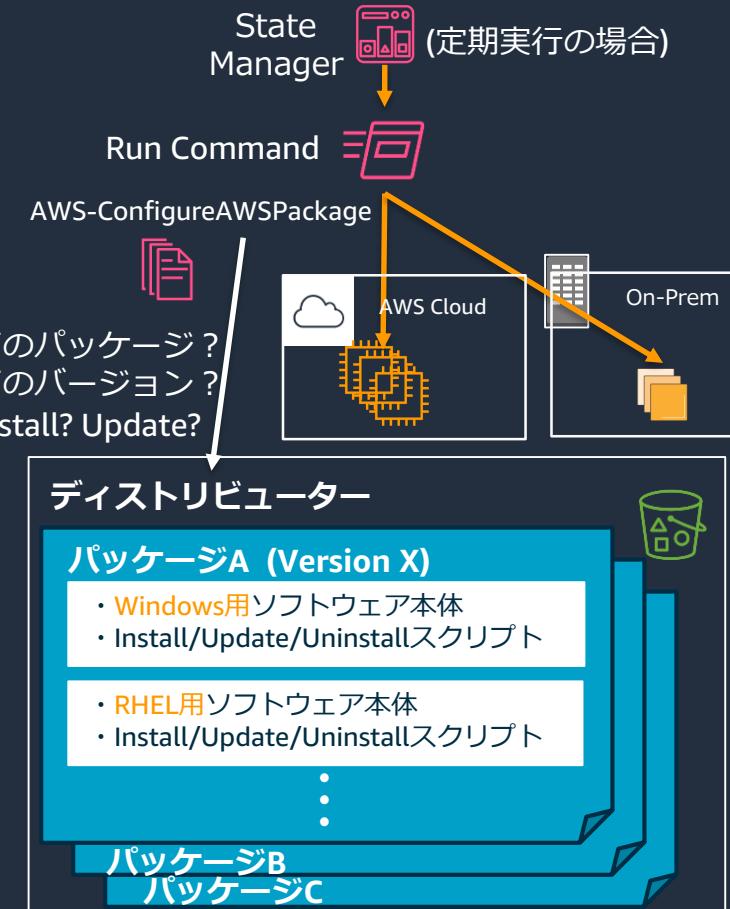
AWS SSM ディストリビューター

ソフトウェアパッケージを安全に保存し配信

- 独自のソフトウェアパッケージの配布、インストールが可能
 - 指定したサーバ群への配布（一回・定期）
 - 複数のプラットフォームに対応
 - 配布パッケージのバージョン管理
- パッケージは他アカウントへ共有可能
- AWSの各種のパッケージが事前定義されておりその導入・更新にも有効



詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/distributor.html
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



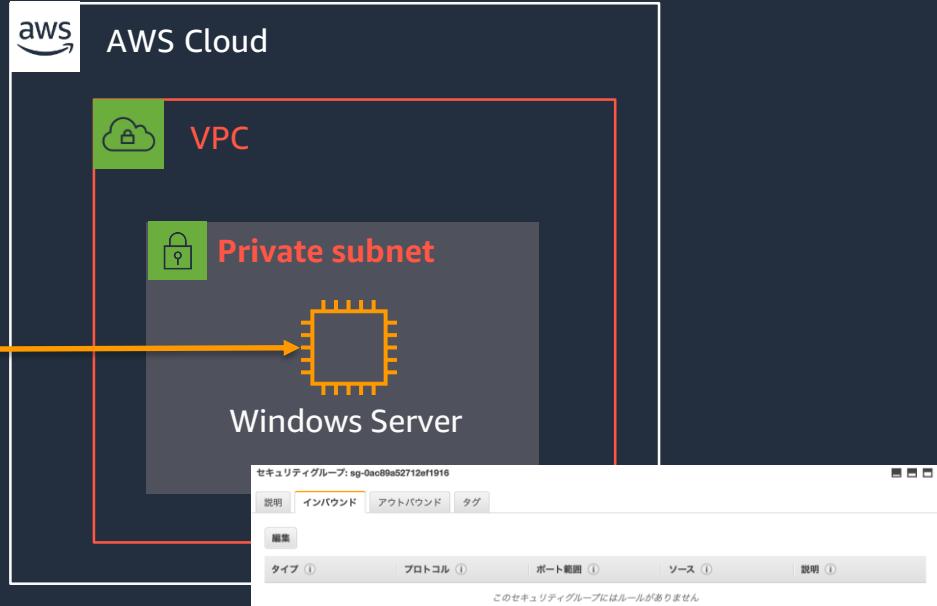
アジェンダ

1. AWS Systems Manager 全体像
2. **AWS Systems Managerを使ってみよう**
 1. 準備編
 2. リソースの“今”を把握しよう
 3. SSMで定型運用を実施しよう
 4. **非定型なインタラクティブ操作もSSMで**
 5. アプリケーションの設定管理もSSMで
3. AWS Systems Managerのセキュリティーベストプラクティス
4. まとめ

セッションマネージャー RDPアクセス



localhost:13389



セキュリティグループでポート開放無し

SSM セッションマネージャー

インバウンドポートを開くことなく、インタラクティブなシェルアクセスを実現

- 通信ポートを開放せずにサーバへのシェルアクセスが可能
 - セキュリティグループでの通信ポートの穴あけ不要。インスタンスをセキュアに維持。
 - プライベートサブネットのインスタンスにもアクセス可能。
踏み台サーバいらずに。
- アクセス制御はIAMユーザに対しIAM Policyで指定する。
- セッションマネージャーで用意されている接続手段
 - SSM Agent 経由で直接アクセス
 - SSM Agent でトンネルを作成してSSHなどでアクセス



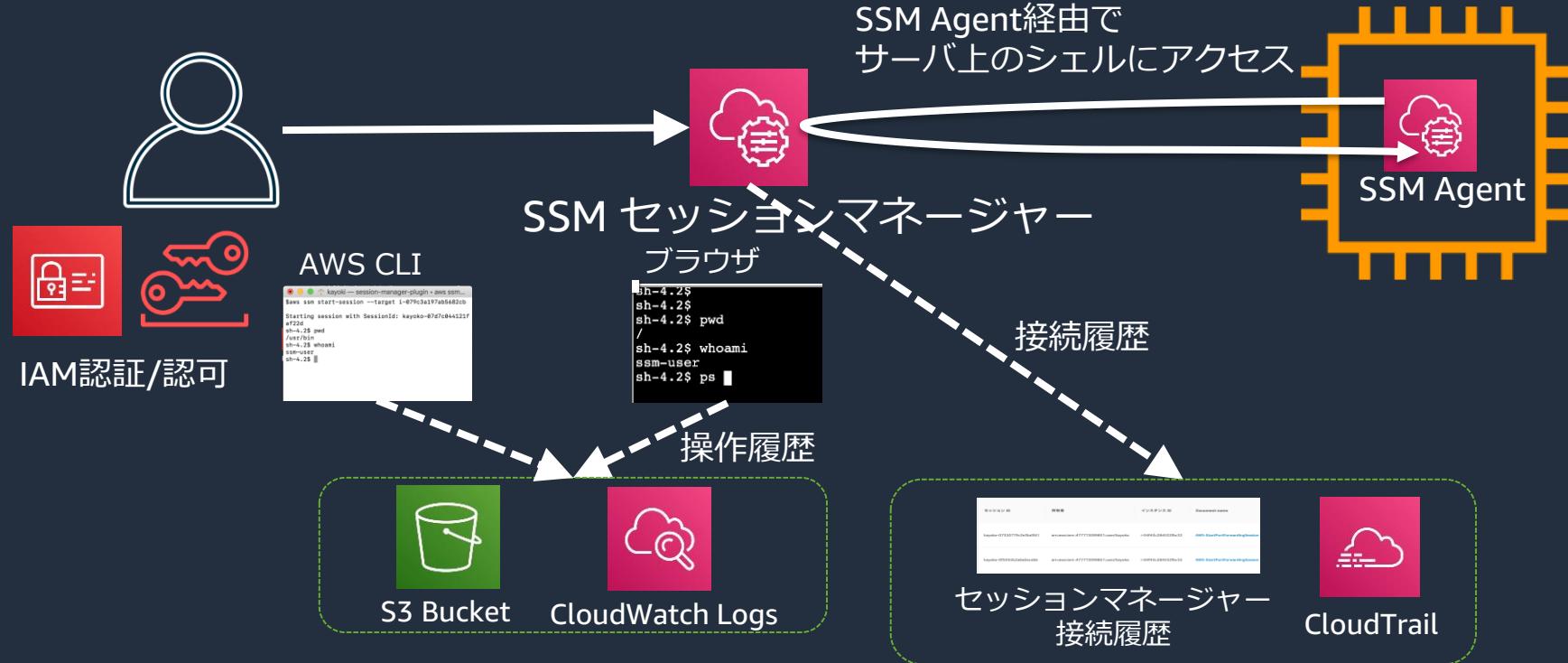
2019/7

詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/session-manager.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



セッションマネージャー SSM Agent経由で直接アクセス



セッションマネージャー SSM Agent経由で直接アクセス

- ブラウザのみでインタラクティブなシェルアクセスを実現可能
 - サーバのログイン情報（キーペアおよびID・パスワード）が不要（IAM認証）
 - Linuxはbash、WindowsはPowerShellが利用可能
- その他
 - 操作ログをCloudWatch LogsやS3に保存。暗号化も可能。
 - セッションマネージャーでの接続履歴や、CloudTrailにて接続情報を追跡可能
 - Linuxはセッションを開始するOSユーザを設定可能。（デフォルトはssm-user）
 - インスタンスでSSHを起動させる必要はない。ポート穴あけも不要。
 - AWS CLIからアクセスすることも可能。session-manager-pluginの導入要

```
$ aws ssm start-session --target i-079c3a197ab5682cb
```

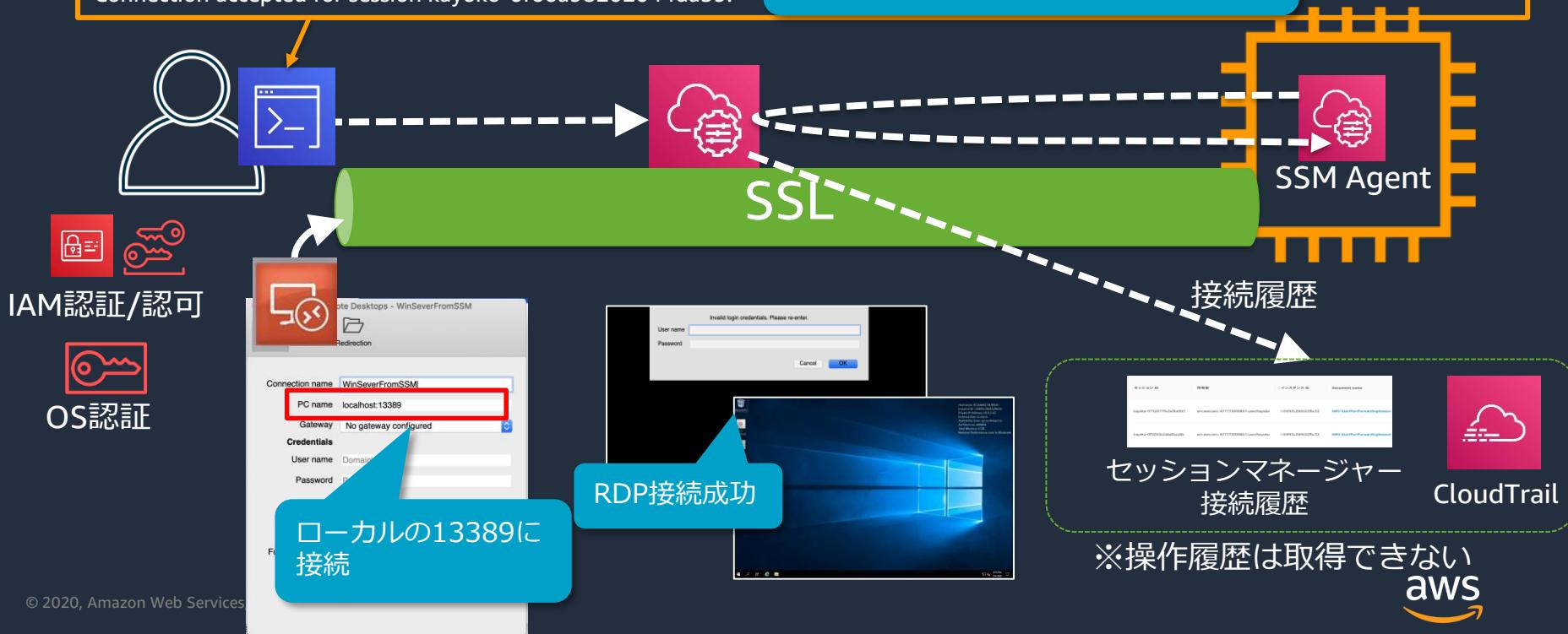
```
Starting session with SessionId: kayoko-024e90a532f59ad5e  
sh-4.2$
```

セッションマネージャー トンネリングアクセス (RDP接続)

```
$ aws ssm start-session --target i-04f43c284532fb32 --document-name AWS-StartPortForwardingSession --parameters "portNumber=3389, localPortNumber=13389"
```

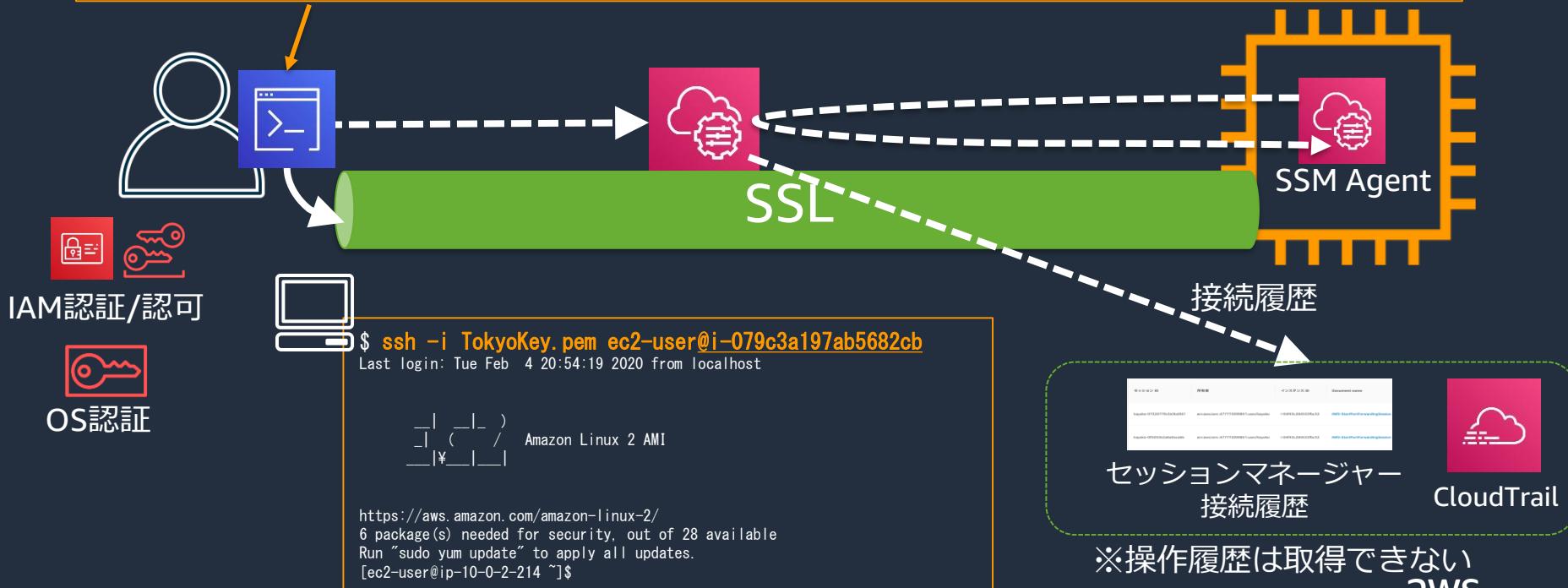
Starting session with SessionId: kayoko-0f66a98202044da39
Port 13389 opened for sessionId kayoko-0f66a98202044da39.
Connection accepted for session kayoko-0f66a98202044da39.

ローカル側の tcp13389 へのアクセスが
リモート側の tcp3389 に転送される



セッションマネージャー トンネリングアクセス (SSH接続)

```
$ cat ~/.ssh/config  
# SSH over Session Manager  
host i-* mi-*  
ProxyCommand sh -c "aws ssm start-session --target %h --document-name AWS-StartSSHSession --parameters 'portNumber=%p'"  
$
```



セッションマネージャー トンネリングアクセス

- 使い慣れたSSHクライアントから、SSH/SCPが実現可能
 - プロキシ設定で、AWS CLIのコマンド設定要
- AWS CLIを用いてポートフォワーディングが可能
 - プライベートサブネットにあるRDSに開発端末から接続
 - Windowsインスタンスに対するRDP接続 etc
- その他
 - 操作ログは保管されない。従来通り、SSHクライアント側で取得する。
 - IAM認証に加え、サーバのログイン情報（キーペアおよびID・パスワード）が必要。
 - インスタンスで SSH/RDP が実行されている必要がある。
ただしポート穴あけは不要
 - セッションマネージャーでの接続履歴や、CloudTrailにて接続情報を追跡可能。
 - 利用には、session-manager-pluginの導入が必要

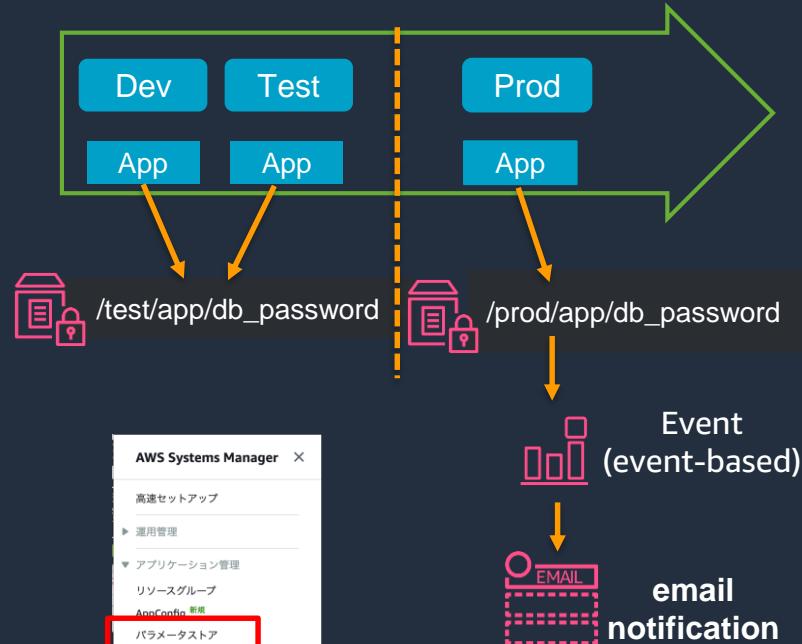
アジェンダ

1. AWS Systems Manager 全体像
2. **AWS Systems Managerを使ってみよう**
 1. 準備編
 2. リソースの“今”を把握しよう
 3. SSMで定型運用を実施しよう
 4. 非定型なインタラクティブ操作もSSMで
 5. アプリケーションの設定管理もSSMで
3. AWS Systems Managerのセキュリティーベストプラクティス
4. まとめ

SSM パラメータストア

構成や設定情報の管理のための安全な階層型ストレージ

- コンフィグレーションや設定値を権限別の階層型で保存
 - IAMによるアクセス制御
- パスワードなど機密情報をKMSで暗号化
- パブリックパラメータあり
 - AWSが提供するパラメータ
 - 例) AMI情報
- CloudFormation, Lambda, ECS, CodeBuild, CodeDeployなどのサービスと統合済み
 - 環境変数を渡す用途などに使用



詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-parameter-store.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



SSM AppConfig

アプリケーション設定を作成、管理し、迅速なデプロイをサポート

- アプリケーションの設定情報を迅速に展開するための機能
 - EC2、コンテナ、Lambdaへスケーラブルかつアプリケーションの再起動なしに展開可能
- 開発や本番など環境毎に異なる設定情報をデプロイできる
 - 設定情報はパラメータストアもしくはSSMドキュメントとして保管
 - アプリケーションコードから AppConfig の GetConfiguration API でパラメータを取得。その値で動作を変えるよう開発する。
- 展開前にバリデーションも実施できる
- デプロイ戦略を定義でき、カナリアリリースも可能

The screenshot shows the AWS Systems Manager interface for AppConfig. It includes three main panels: 1) A sidebar with 'AWS Systems Manager' and 'AppConfig' highlighted. 2) A central panel titled 'Add configuration profile details' with fields for 'Name' (ProductionProfile), 'Description' (optional), and 'Service role' (choosing 'Existing service role' and selecting 'arn:aws:iam::role/appConfigProductionProfileRole'). 3) A bottom panel titled 'ProductionProfile' showing 'Configuration profile details' (Source: SSM Parameter /MyappConfig/RevertX, switch), 'Versions' (listing two versions with values 'true' and 'false'), and 'Versions' (listing two versions with values 'true' and 'false').

詳細は、[Https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/appconfig.html](https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/appconfig.html)

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



2019/12~



アジェンダ

1. AWS Systems Manager 全体像
2. AWS Systems Managerを使ってみよう
 1. 準備編
 2. リソースの“今”を把握しよう
 3. SSMで定型運用を実施しよう
 4. 非定型なインタラクティブ操作もSSMで
 5. アプリケーションの設定管理もSSMで
3. **AWS Systems Managerのセキュリティベストプラクティス**
4. まとめ

SSMを使用する上でのセキュリティーベストプラクティス

「**Systems Manager のセキュリティのベストプラクティス**」をご参照ください

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/security-best-practices.html

- **最小限の特権アクセスを実装する**
 - ユーザのIAMポリシーは、該当リソース・特定アクションについてのみ有効に
 - 例えば”ssm.StartSession”をDenyすることで、セッションマネージャを使用しない設定が可能。
- **VPCエンドポイントを使用可能**
- 特別セキュアな処理が必要な場合はSession Managerに**対話型コマンド**のみを使用する
- AWSおよびSSMツールを**最新に保つ**
- CloudWatch / CloudTrail / AWS Configを使用

SSMの料金

- AWS Systems Manager の利用は基本的に無料
- 一部の機能は有料
 - OpsCenter (OpsItem の数とAPI コールの数に基づく課金)
 - Explorer (ダッシュボード表示の際のOpsCenter APIコールのみ課金)
 - パラメータストア (パラメータサイズが4KB以上、パラメータ数10000以上の場合)
 - ディストリビューターの独自パッケージ
 - Automation (ステップカウント、ステップ実行時間、プレイブックに対して課金)
 - AppConfig (APIコールの数とターゲットごとの構成更新の合計数に対してのみ課金)
 - オンプレミス管理のアドバンストインスタンスティア
- その他関連サービスの使用量に応じた料金
 - Athena + QuickSight / Config / CloudWatch (カスタムメトリクス、Logs) / S3に格納したログデータ

詳細は、<https://aws.amazon.com/jp/systems-manager/pricing/>

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



(参考) オンプレミスインスタンス管理

- SSMでは、オンプレミスインスタンス管理用に2つのティアがある。

	標準インスタンスティア (デフォルト)	アドバンストインスタンスティア
課金	無料	インスタンス実行時間に基づく 従量課金
登録できる サーバ数	リージョン/アカウントごとに 最大1000まで	リージョン/アカウントごとに 1000を超えるサーバを登録可能
機能差異	<ul style="list-style-type: none">セッションマネージャーが 使えないパッチパネージャーで、Microsoftアプ リケーションのパッチ管理ができない	<ul style="list-style-type: none">セッションマネージャーも使用可能パッチパネージャーで、Microsoftアプ リケーションのパッチ管理が可能

「マネジドインスタンス」 > 「設定」 > 「インスタンス枠」 > 「アカウント設定の変更」から
インスタンスティアを変更可能

詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-managedinstances-advanced.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



アジェンダ

1. AWS Systems Manager 全体像
2. AWS Systems Managerを使ってみよう
 1. 準備編
 2. リソースの“今”を把握しよう
 3. SSMで定型運用を実施しよう
 4. 非定型なインタラクティブ操作もSSMで
 5. アプリケーションの設定管理もSSMで
3. AWS Systems Managerのセキュリティーベストプラクティス
4. まとめ

まとめ

- AWS SSMを用いることで、**オンプレミス／AWS両環境で運用に必要な作業を、実施することができます。**
 - リソース状況の可視化
 - 定型作業の実施
 - インタラクティブな操作
 - アプリケーションの設定管理
- **何か一つの機能から始めてみてはいかがでしょうか。**

Q&A

お答えできなかったご質問については
AWS Japan Blog 「<https://aws.amazon.com/jp/blogs/news/>」にて
後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索



The screenshot shows the AWS Japan Language Resources page. At the top, there's a navigation bar with the AWS logo, search bar, and links for "日本担当チームへお問い合わせ", "サポート", "日本語", "アカウント", and "コンソールにサインイン". Below the navigation is a horizontal menu with links for "製品", "ソリューション", "料金", "ドキュメント", "学習", "パートナー", "AWS Marketplace", "その他", and a search icon. The main content area features a large title "AWS クラウドサービス活用資料集トップ" and a descriptive paragraph about the service. At the bottom, there are four call-to-action buttons: "AWS Webinar お申込", "AWS 初心者向け", "業種・ソリューション別資料", and "サービス別資料".

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

AWS Webinar お申込 »

AWS 初心者向け »

業種・ソリューション別資料 »

サービス別資料 »

<https://amzn.to/JPArchive>

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に
対策などを相談することも可能

• 申込みはイベント告知サイトから

(<https://aws.amazon.com/jp/about-aws/events/>)

AWS イベント で[検索]

ご視聴ありがとうございました

AWS 公式 Webinar
<https://amzn.to/JPWebinar>



過去資料
<https://amzn.to/JPArchive>





AWS Systems Manager

Distributor 編

村田 京介

Solutions Architect

2023/9

自己紹介

名前：村田 京介 (Kyosuke Murata)

所属：技術統括本部 エンタープライズ技術本部
サービスソリューション部

経歴：

ソフトウェアベンダーのコンサルタントを経て、
現在はソリューションアーキテクトとして
エンタープライズのお客様を担当

好きなAWSサービス：
AWS Systems Manager、AWS Chatbot



本セミナーの対象者

AWS の運用をされている方、これから運用される予定の方

本セミナーの目的

- AWS Systems Manager Distributor の機能とユースケースをご理解いただく。

本日お話ししないこと

- AWS Systems Manager の全体的な説明
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager Distributor 以外の機能の詳細
→ [AWS サービス別資料](#)より各機能にフォーカスしたセッションをご参照ください。
検索結果に表示されない機能については今後公開予定です。

アジェンダ

1. AWS Systems Manager (SSM) の概要
2. SSM Distributor とは
3. SSM Distributor の料金
4. まとめ

AWS Systems Manager (SSM) の概要

AWS Systems Manager (SSM)

ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション



AWS Config

Configuration history



Amazon EventBridge

Notification and remediation



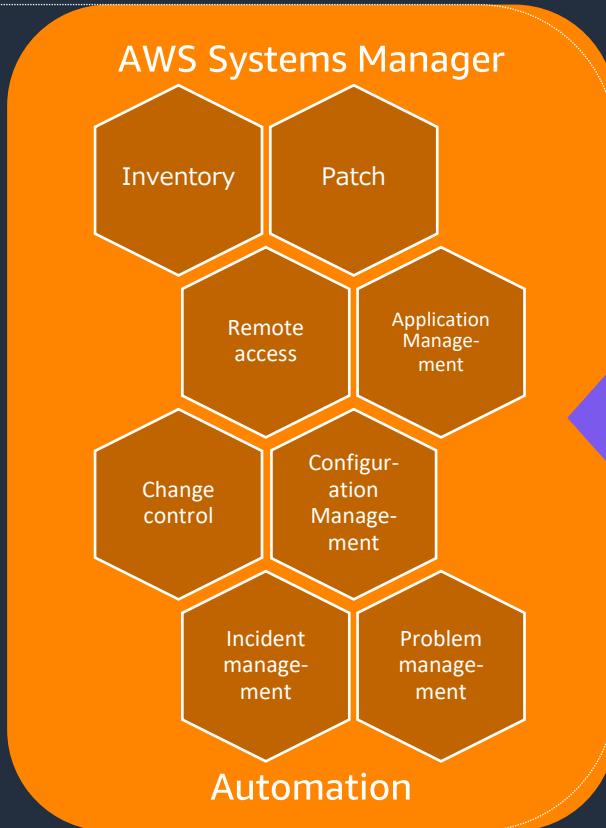
AWS CloudTrail

Audited actions



AWS Identity and Access Management (IAM)

Role-based access control



Integration
connectors
and APIs

- Third-party tools
- ITSM
- Custom solutions

AWS の他のサービスや
3rd Party のツールと統合された
管理ソリューションを提供

SSM の機能



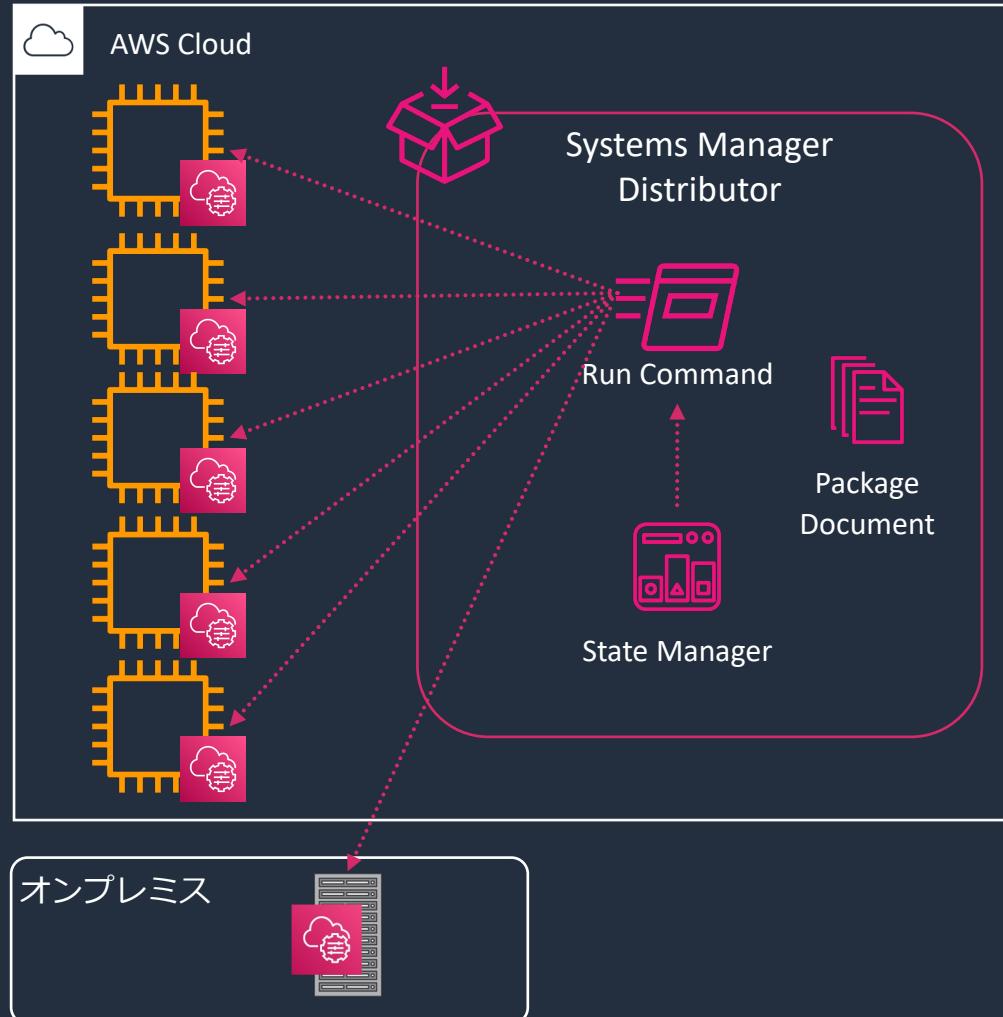
SSM Distributor とは

ソフトウェア管理における従来の課題

例) エージェントの管理



SSM Distributor とは



ソフトウェアの一元的な管理が可能

- ・ ソフトウェアをパッケージ化し、パッケージドキュメントとして管理
- ・ パッケージドキュメントは 3 種類
 - ✓ AWS 提供
 - ✓ サードパーティー提供
 - ✓ お客様独自で作成
- ・ Run Command や State Manager を使用して一回だけであったり、スケジュールに従ってソフトウェアを EC2 インスタンスやオンプレミスのサーバーに配布してインストール / アンインストールすることが可能

Package Document の構成要素

Distributor がターゲットへの
ソフトウェア配布時に取り扱う単位

パッケージドキュメント

マニュフェストファイル
(json ファイル : 1 つ)

ターゲットのオペレーティングシステム、バージョン、
プロセッサのアーキテクチャにより利用する
インストール可能なアセットのマッピング情報と
インストール可能なアセットのチェックサム

インストール可能なアセット
(zip ファイル : 1 つ以上 20 以下)

ソフトウェアファイル
(.rpm, .msi, .deb : 1 GB まで)

インストールスクリプト

アンインストールスクリプト

アップデートスクリプト (オプション)

AWS / サードパーティ提供のパッケージドキュメント

The screenshot displays two views of the AWS Lambda console interface for managing packages.

Left View (Amazon-managed packages):

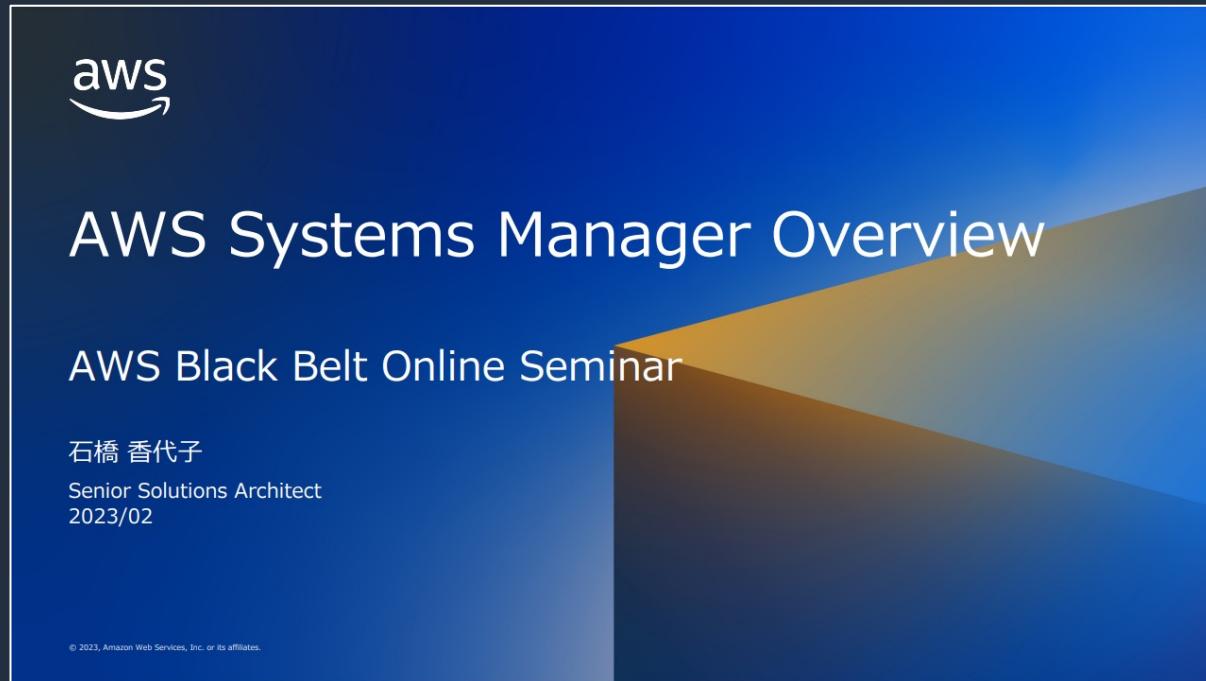
- Header tabs: Amazonが所有, 自己所有, 自分と共有, サードパーティー, すべてのドキュメント.
- Sub-tabs: パッケージ, 詳細の表示, スケジュールへのインストール, 1回限りのインストール, パッケージの作成.
- Search bar: キーワードで検索するか、タグまたは属性でフィルタリングします.
- Table of packages:
 - AWSCodeDeployAgent (Owner: Amazon)
 - AWSKinesisTap (Owner: Amazon)
 - AWSDistroOTel-Co (Owner: Amazon)
 - AWSNVMe (Owner: Amazon)

Right View (Third-party packages):

- Header tabs: Amazonが所有, 自己所有, 自分と共有, サードパーティー, すべてのドキュメント.
- Sub-tabs: パッケージ, 詳細の表示, スケジュールへのインストール, 1回限りのインストール, パッケージの作成.
- Search bar: キーワードで検索するか、タグまたは属性でフィルタリングします.
- Table of packages:
 - AlertLogic-MDR (Owner: AlertLogic, Alert Logic logo)
 - FalconSensor-Windows (Owner: CrowdStrike, Inc., CrowdStrike logo)
 - DynatraceOneAgent (Owner: Dynatrace, Dynatrace logo)
 - New-Relic-infrastructure-monitoring-agent (Owner: NewRelic, new relic logo)
 - FalconSensor-Linux (Owner: CrowdStrike, Inc., CrowdStrike logo)
 - TrendMicro-CloudOne-WorkloadSecurity (Owner: Trend Micro Cloud One, Trend MICRO logo)

SSM Distributor を利用する前に

ソフトウェアパッケージ配布対象のサーバーを SSM の管理対象（マネージドノード）にする必要があります。詳細は、対象が EC2 の場合 「[AWS Systems Manager Overview](#)」、EC2 以外の場合 「[AWS Systems Manager Hybrid Activations 編](#)」をご覧ください

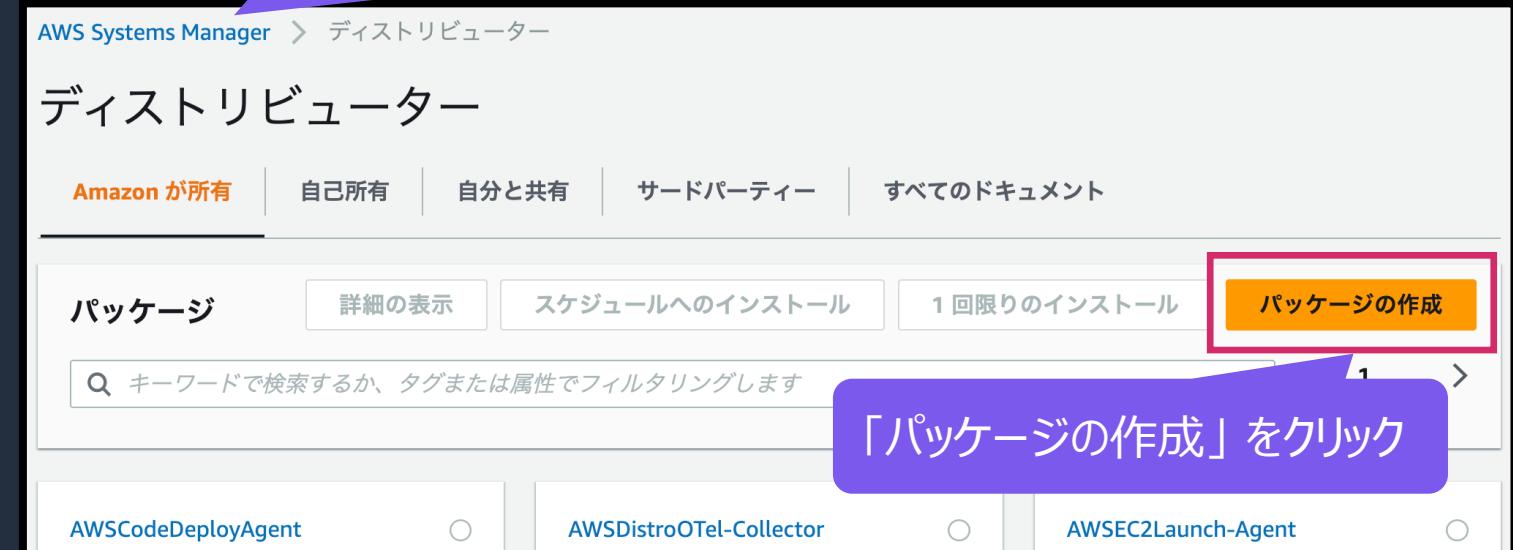


独自のソフトウェアパッケージの準備 (1/5)

ドキュメントパッケージの構成要素を
配置するバケットを S3 の管理画面で作成



AWS Systems Manager
のディストリビューターのページに遷移



「パッケージの作成」をクリック

独自のソフトウェアパッケージの準備 (2/5)

AWS Systems Manager > ディストリビューター > パッケージの作成

パッケージの作成

簡単
パッケージを作成し、ディストリビューターでパッケージマニフェストとインストールスクリプト、アンインストールスクリプトを作成します。

高度
パッケージを作成し、固有のインストールスクリプトとアンインストールスクリプト、および固有のパッケージマニフェストを提供します。

「簡単」を選択

詳細
パッケージ名とバージョン名を指定してください。 詳細情報は[こちらをご覧ください](#) [i]

名前
Kinesis-Agent
パッケージ名に特殊文字やスペースを含めることはできません。最大 128 文字まで使用できます。

バージョン名 - オプション
バージョン名に特殊文字やスペースを含める

「名前」に任意の名前を入力
本セッションでは Kinesis Agent の
パッケージを作成します。

簡単

マニュフェストファイル、およびインストール可能なアセットの作成補助をしてくれる。
ユーザーは配布するソフトウェアファイルを準備すればよい。

高度

マニュフェストファイル、およびインストール可能なアセットをユーザーが準備する必要がある。
パッケージドキュメントの仕様を熟知して
手元の PC で準備したいユーザーや作成済みのものをクロスリージョンに展開したいユーザーの利用などに適している。

パッケージドキュメント

Distributor がターゲットへの
ソフトウェア配布時に取り扱う単位

マニュフェストファイル (json ファイル : 1 つ)

ターゲットのオペレーティングシステム、バージョン、
プロセッサのアーキテクチャにより利用する
インストール可能なアセットのマッピング情報と
インストール可能なアセットのチェックサム

インストール可能なアセット (zip ファイル : 1 つ以上 20 以下)

ソフトウェアファイル (.rpm, .msi, .deb : 1 GB まで)

インストールスクリプト

アンインストールスクリプト

アップデートスクリプト (オプション)

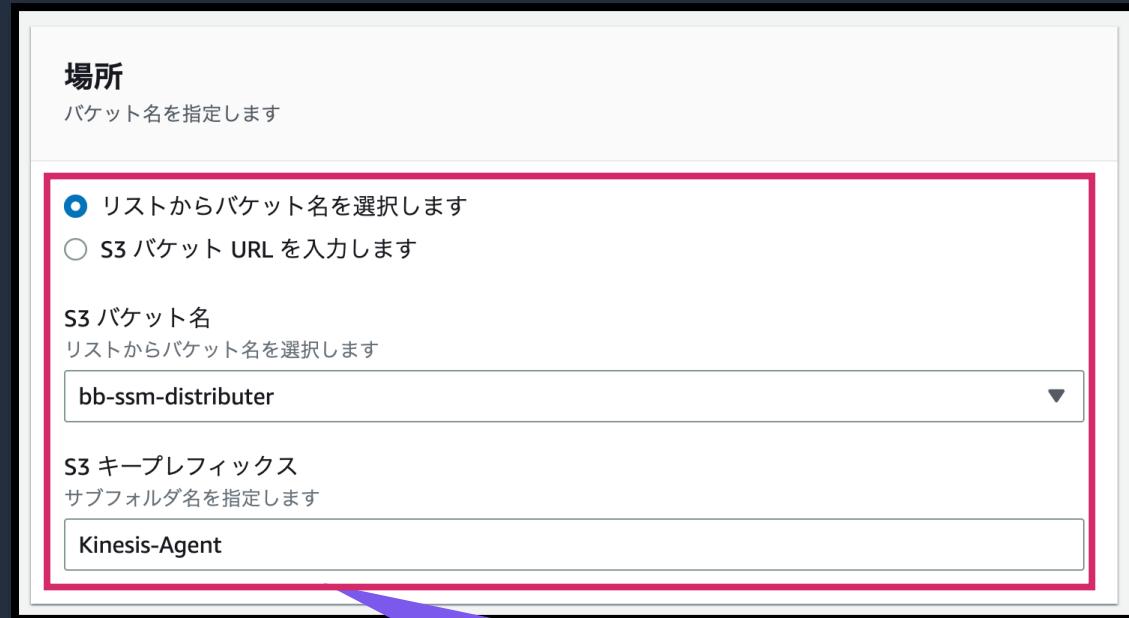
独自のソフトウェアパッケージの準備 (3/5)

場所
バケット名を指定します

リストからバケット名を選択します
 S3 バケット URL を入力します

S3 バケット名
リストからバケット名を選択します
bb-ssm-distributer

S3 キープレフィックス
サブフォルダ名を指定します
Kinesis-Agent



事前に作成した
S3 バケット名とサブフォルダ名
を指定します。

ソフトウェアをアップロード
パッケージの一部となる msi、deb、rpm ファイルを選択してください。

ソフトウェア 1 × ソフトウェアを削除

ソフトウェアパッケージ名
aws-kinesis-agent-latest.amzn2.noarch.rpm

プラットフォームのバージョン
ターゲットオペレーティングシステムのバージョン。
_any

ターゲットプラットフォーム
オペレーティングシステムを選択します。
amazon

アーキテクチャ
ターゲットオペレーティングシステムのプロセッサー
アーキテクチャです。
_any

▶ スクリプト

ソフトウェアを追加



ローカルファイルから、配布する
ソフトウェアパッケージを選択し、
ターゲットのプラットフォームを
指定します。

独自のソフトウェアパッケージの準備 (4/5)

▼ スクリプト クリック

インストールスクリプト | スクリプトを更新 | アンインストールスクリプト

```
1 #!/bin/bash
2
3 sudo yum install -y aws-kinesis-agent-latest.amzn2.noarch
```

▼ スクリプト

インストールスクリプト | スクリプトを更新 | アンインストールスクリプト

```
1
```

▼ スクリプト

インストールスクリプト | スクリプトを更新 | アンインストールスクリプト

```
1 #!/bin/bash
2
3 sudo yum remove -y aws-kinesis-agent-latest.amzn2.noarch
```

更新スクリプトは必須ではありませんので
自動生成されません。

独自のソフトウェアパッケージの準備 (5/5)

The screenshot illustrates the process of preparing a custom software package for deployment. It consists of two main parts:

- Left Panel (CloudFormation):** Shows the CloudFormation template for the "Kinesis-Agent" package. A purple callout box labeled "クリック" (Click) points to the "manifest.json" file, which is highlighted with a red border. The manifest file contains the following JSON code:

```
1 {  
2   "schemaVersion": "2"  
3   "version": "Auto-Ge  
4   "packages": {  
5     "amazon": {  
6       "_any": {  
7         "_any": "  
8           fi  
9         }  
10      }  
11    },  
12    "files": {  
13      "aws-kinesis-ag  
14      "checksums"  
15      "sha256"  
16    }  
17  }  
18 }  
19 }  
20 }
```

- Right Panel (AWS Systems Manager):** Shows the "Distribution" tab of the "Kinesis-Agent" distribution. A purple callout box labeled "クリック" (Click) points to the "aws-kinesis-agent-latest.amzn2.noarch.rpm.zip" file, which is highlighted with a red border. The distribution page includes tabs for "Amazon が所有", "自己所有" (selected), "自分と共有", "サードパーティー", and "すべてのドキュメント". It also features buttons for "アップロード", "S3 URI をコピー", and "パッケージの作成".

【参考】「高度」なパッケージドキュメントの登録

Amazon S3 > パケット > bb-ssm-distributer > Kinesis-Agent/

Kinesis-Agent/

オブジェクト プロパティ

準備したマニュフェストファイルやインストール可能なアセットをアップロードした S3 バケットとキープレフィックスの確認

アップロード

検索

名前	タイプ	最終更新日時
aws-kinesis-agent-latest.amzn2.noarch.rpm.zip	zip	2023/08/18 06:06:57 PM JST
manifest.json	json	2023/08/18 06:06:49 PM JST

場所
パケット名を指定します

リストからパケット名を選択します
 S3 パケット URL を入力します

S3 パケット名
リストからパケット名を選択します
bb-distributer

S3 キープレフィックス
サブフォルダ名を指定します
Kinesis-Agent

マニフェスト
パッケージマニフェストは、インストールするソフトウェアを提供します。詳細情報は[こちら](#)をご覧ください

パッケージからの抽出
上記で指定した S3 パケットにあるパッケージからマニフェストを抽出します。

新しいマニフェスト
コンテンツエディタを使用して新しいマニフェストを作成します。

マニフェストファイルの表示

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/distributor-working-with-packages-create.html

パッケージの配布 - Run Command(1/4)

The screenshot shows the AWS Systems Manager Distributor interface. At the top, it says "AWS Systems Manager > ディストリビューター". Below that is the title "ディストリビューター". There are four tabs: "Amazon が所有" (selected), "自己所有" (highlighted with a red box), "自分と共有", "サードパーティー", and "すべてのドキュメント". Underneath, there are four buttons: "パッケージ" (selected), "詳細の表示", "スケジュールへのインストール", "1回限りのインストール" (highlighted with a red box), and "パッケージの作成". A search bar says "キーワードで検索するか、タグまたは属性でフィルタリングします". To the right, there are navigation arrows and a page number "1". A purple callout bubble points to the "1回限りのインストール" button with the text "「1回限りのインストール」をクリック". Another purple callout bubble points to the "自己所有" tab with the text "ディストリビューターの「自己所有」に遷移し、作成したパッケージドキュメントを選択する". On the left, there's a card for "Kinesis-Agent" with "所有者" and a QR code.

AWS Systems Manager > ディストリビューター

ディストリビューター

Amazon が所有 **自己所有** 自分と共有 サードパーティー すべてのドキュメント

パッケージ 詳細の表示 スケジュールへのインストール **1回限りのインストール** パッケージの作成

キーワードで検索するか、タグまたは属性でフィルタリングします < 1 >

「1回限りのインストール」をクリック

Kinesis-Agent

所有者

ディストリビューターの「自己所有」に遷移し、作成したパッケージドキュメントを選択する

パッケージの配布 - Run Command(2/4)

コマンドドキュメント
実行するコマンドのタイプを選択します。

検索 キーワードで検索、またはタグや属性でフィルタリング

ドキュメント名のプレフィックス: Equals: AWS-ConfigureAWSPackage X Clear filters

名前	所有者	プラット
AWS-ConfigureAWSPackage	Amazon	Windows

Action (Required) Specify whether or not to install or uninstall the package.

Action: Install

Installation Type (Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place update: The application is available while new or updated files are added to the installation.

Installation Type: Uninstall and reinstall

Name (Required) The package to install/uninstall.
Name: Kinesis-Agent

Version (Optional) The version of the package to install or uninstall. If you don't specify a version, the system installs the latest published version by default. The system will only attempt to uninstall the version that is currently installed. If no version of the package is installed, the system returns an error.

Additional Arguments (Optional) The additional arguments for the command.

Additional Arguments: {
 "version": "1.0",
 "script": "script.sh",
 "args": "arg1 arg2",
 "path": "/tmp"}
オプションでパッケージドキュメントのバージョン指定や、スクリプトに
引き渡す変数を定義することが可能

※ 変数の使い方は以下の Command document plugin reference を参照
<https://docs.aws.amazon.com/systems-manager/latest/userguide/documents-command-ssm-plugin-reference.html>

パッケージの配布 - Run Command(3/4)

⌚ コマンド ID: f6bdc4da-e649-476d-bebf-40af9ef7abb1 が正常に送信されました!

AWS Systems Manager > Run Command > コマンド ID: f6bdc4da-e649-476d-bebf-40af9ef7abb1

コマンド ID: f6bdc4da-e649-476d-bebf-40af9ef7abb1

C コマンドのキャンセル コマンドの再実行 Copy to new

コマンドのステータス

全体的なステータス	詳細なステータス	ターゲット数	完了数
① 進行中	① 進行中	1	0

ターゲットと出力

インスタンス ID	インスタンス名	ステータス
i-05b95b9ae7760f362		①

▼ コマンドの説明

コマンド ID f6bdc4da-e649-476d-bebf-40af9ef7abb1	コマンドのステップ 2
コマンドドキュメント AWS-ConfigureAWSPackage	コメント
ドキュメントのバージョン 1	リクエストした日付 Mon, 21 Aug 2023 19:40:11 GMT

▼ コマンドのパラメータ

パラメータ	action	配信タイムアウト (秒) 600
	additionalArguments	実行タイムアウト (秒) 7200
	installationType	
	name	
	version	

action: "Install"
additionalArguments: "{}"
installationType: "Uninstall and reinstall"
name: "Kinesis-Agent"
version: ""

パッケージの配布 - Run Command(4/4)

ターゲットと出力

出力の表示

検索

インスタンス ID	インスタンス名
i-05b95b9ae7760f362	ip-10-0-4-250.ap-northeast-1.compute.internal

ステップ 2 - コマンドの説明とステータス

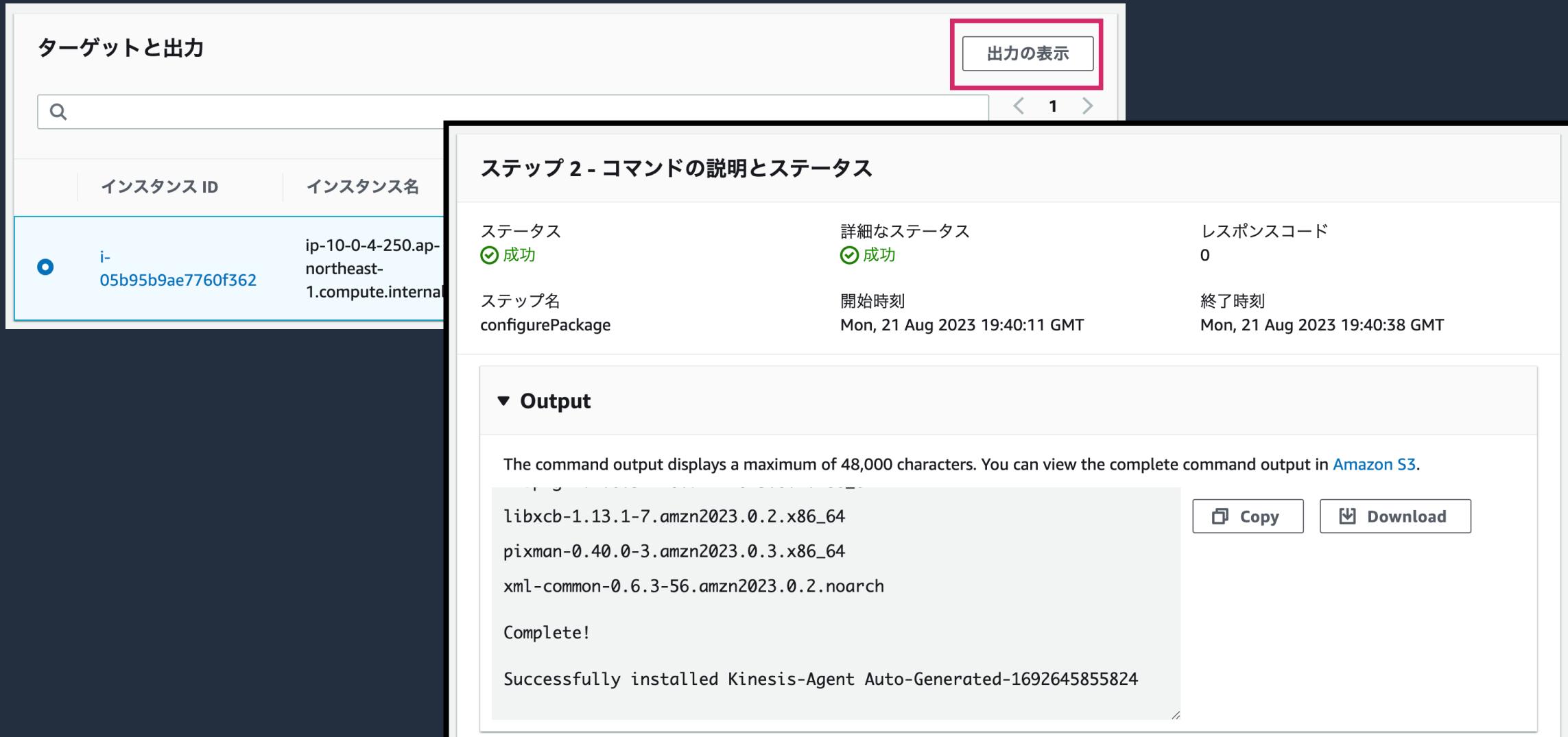
ステータス 成功	詳細なステータス 成功	レスポンスコード 0
ステップ名 configurePackage	開始時刻 Mon, 21 Aug 2023 19:40:11 GMT	終了時刻 Mon, 21 Aug 2023 19:40:38 GMT

▼ Output

The command output displays a maximum of 48,000 characters. You can view the complete command output in [Amazon S3](#).

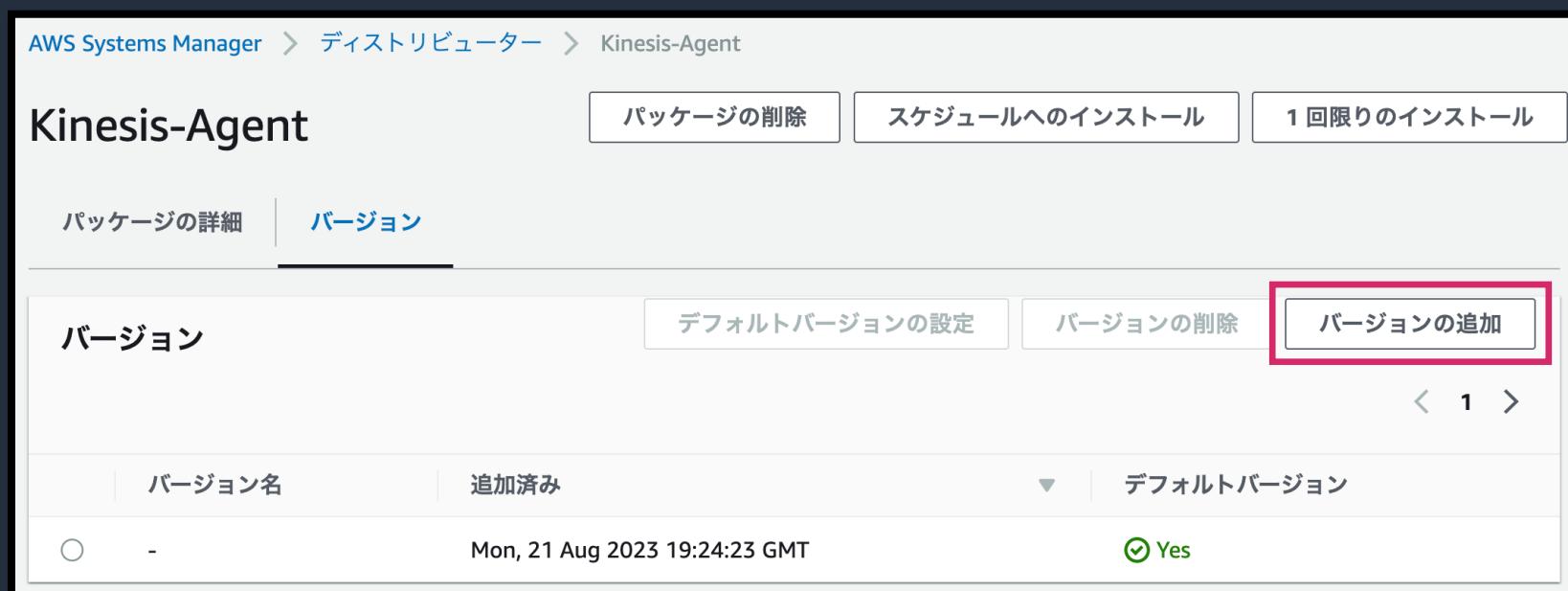
```
libxcb-1.13.1-7.amzn2023.0.2.x86_64
pixman-0.40.0-3.amzn2023.0.3.x86_64
xml-common-0.6.3-56.amzn2023.0.2.noarch
Complete!
Successfully installed Kinesis-Agent Auto-Generated-1692645855824
```

Copy Download



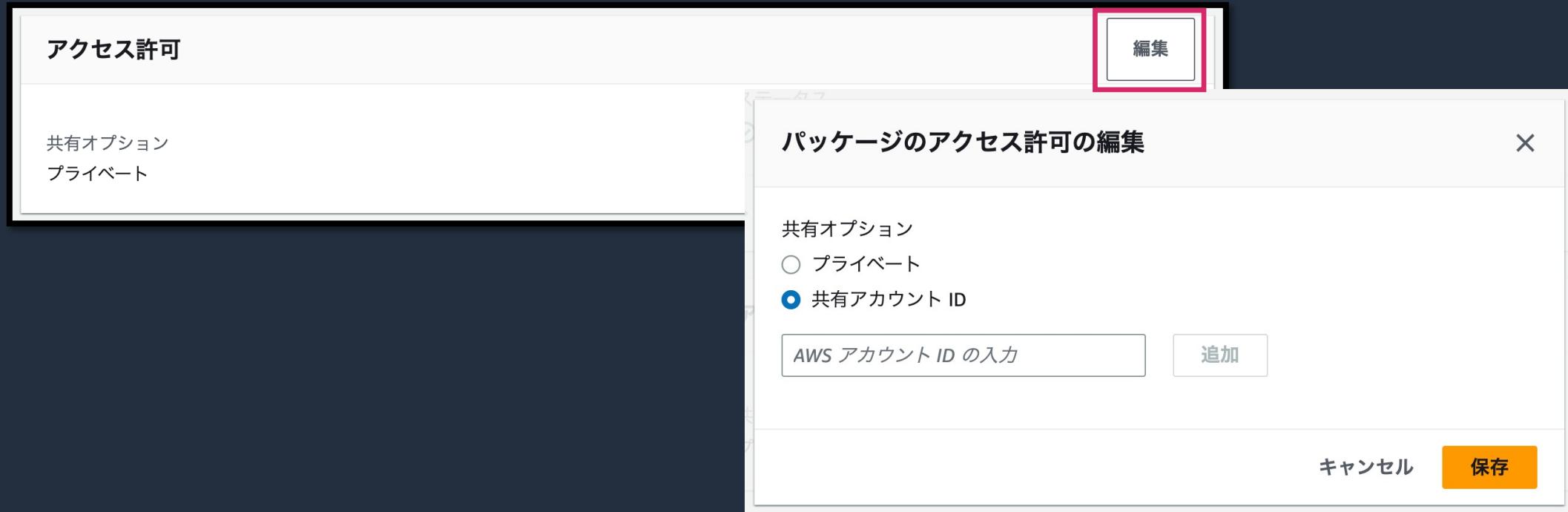
パッケージドキュメントのバージョン管理

- Distributor ではパッケージドキュメントのバージョン管理が可能（最大で 25 バージョン）
 - アタッチされているソフトウェアファイルの置き換え
 - 追加のプラットフォームをサポート
 - 特定のプラットフォームサポートの中止

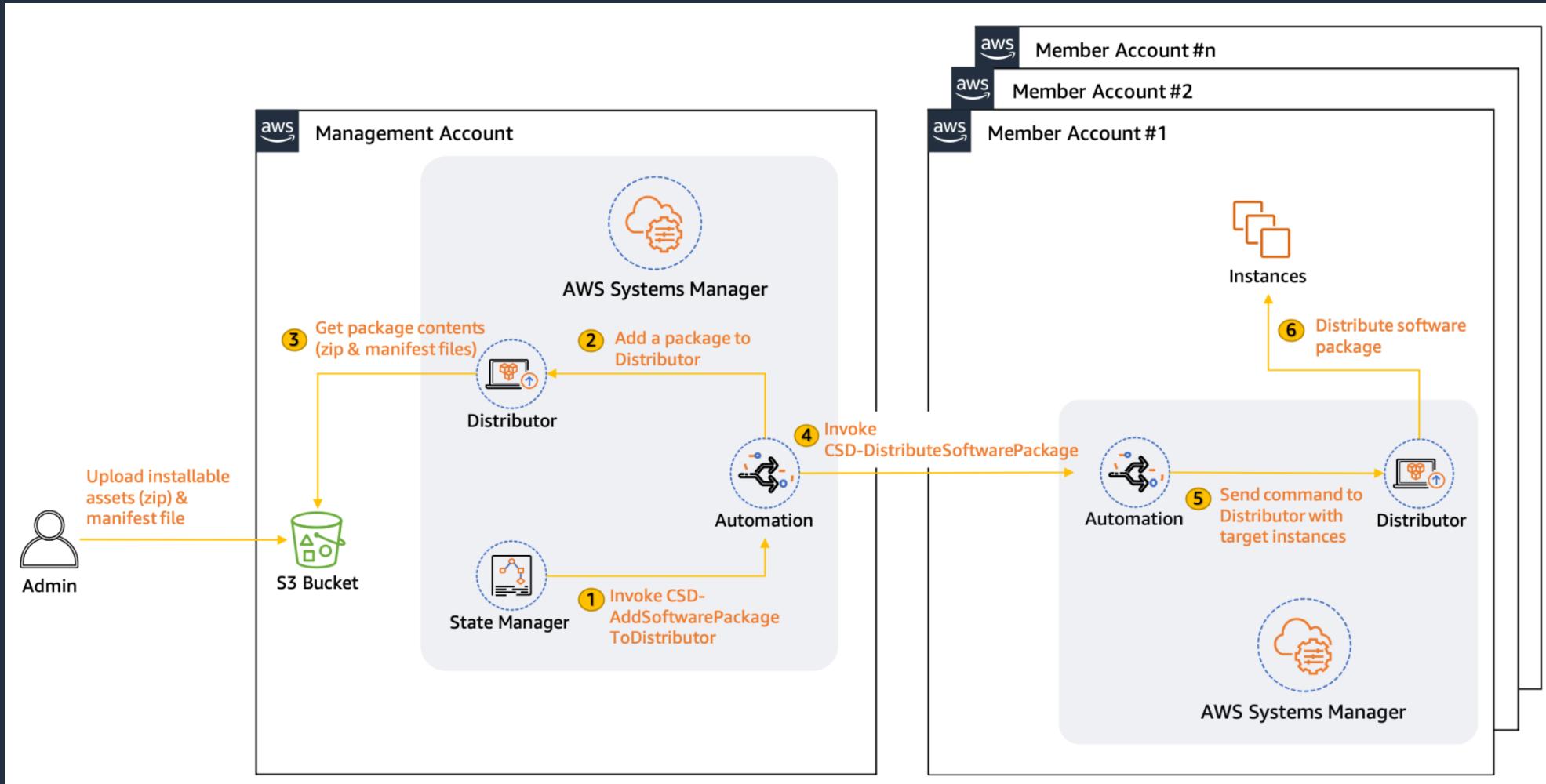


パッケージドキュメントのアクセス許可

- パッケージドキュメントはデフォルトで Private (パッケージ作成者の AWS アカウントへのアクセスが許可されているユーザのみがパッケージ情報の表示、パッケージの管理ができる)
- 他の AWS アカウント (同じリージョン) を追加可能



マルチアカウント実行



「AWS Systems Manager Distributor による AWS Organizations 管理下のアカウントへのソフトウェアパッケージ配布」

<https://aws.amazon.com/jp/blogs/news/centralized-software-package-distribution-across-multiple-regions-and-accounts-in-an-aws-organization-using-aws-systems-manager-distributor/>

SSM Distributor の料金

SSM Distributor の料金

- AWS およびサードパーティー所有パッケージドキュメントの利用は無料
- 非 AWS (お客様独自の) パッケージドキュメントについての料金は以下です。

	料金
ストレージ	1か月あたり 0.046 USD/GB
Get または Describe API コール	Get または Describe API コール 1,000 回あたり 0.025 USD
データ転送 (リージョン外または オンプレミス転送のみ)	ディストリビューターから転送されたデータ 1 GB あたり 0.900 USD

注) アプリケーションのワークフローで他の AWS サービスを使用している場合、
またはデータを転送している場合は、別料金が請求される場合があります。

【参考】

AWS Systems Manager の料金

<https://aws.amazon.com/jp/systems-manager/pricing/>



計算例

ケース

100 の Amazon EC2 インスタンスと 25 のオンプレミスインスタンスがあり、それに、3 つの AWS パッケージと 100 MB の 2 つの非 AWS パッケージを毎月更新する必要があり、1 日に 2 回更新をチェックするものとします。

料金

125 インスタンス間での 3 つの AWS パッケージの配信にかかるコスト = 0 USD
非 AWS パッケージの管理にかかる料金は以下の通り

	料金
ストレージ	2 つの非 AWS パッケージの保存にかかるコスト = $2 * 100 \text{ MB} * 1 \text{ GB}$ あたり 0.046 USD = 0.0092 USD
Get, Describe API コール	15,000 API コールにかかるコスト = $15,000 * \text{API コール } 1,000 \text{ 回}$ あたり 0.025 USD = 0.375 USD
データ転送	25 のオンプレミスインスタンスでの 2 つの非 AWS パッケージの更新にかかるコスト = $25 * 2 * 100 \text{ MB} * 1 \text{ GB}$ あたり 0.90 USD = 4.50 USD
合計月額コスト	$0.0092 \text{ USD} + 0.375 \text{ USD} + 4.50 \text{ USD} = 4.88 \text{ USD}$ (インスタンスあたり 0.0391 USD)

【参考】

AWS Systems Manager の料金

<https://aws.amazon.com/jp/systems-manager/pricing/>



まとめ



まとめ

- Systems Manager Distributor はソフトウェアファイルをパッケージ化して一元管理でき、マネージドノードに対して安全に配信およびインストール可能
- 一度に複数のマネージドノードに対して、ソフトウェアを配信およびインストールしたいケースでの利用に適しています。

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
- ・ 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>



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

内容についての注意点

- ・ 本資料では資料作成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。AWS のサービスは常にアップデートを続けているため、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
- ・ 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
- ・ 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）



Thank you!



AWS Systems Manager

Explorer / OpsCenter 編

AWS Black Belt Online Seminar

小野 卓人

Solutions Architect
2023/03

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3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：小野 卓人 (Takuto Ono)

所属：技術統括本部 金融ソリューション本部
保険ソリューション部

経歴：

SIer で金融機関向けシステムの受託開発
インフラ設計・構築・運用保守

現在は、ソリューションアーキテクトとして主に保険業界のお客様を担当

好きなAWSサービス： AWS Systems Manager



本セミナーの対象者

AWS の運用をされている方、これから運用される予定の方

本セミナーの目的

- AWS Systems Manager Explorer、OpsCenter の機能とユースケースをご理解いただく。

本日お話ししないこと

- AWS Systems Manager の全体的な説明
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager Explorer、OpsCenter 以外の機能の詳細
→ 今後公開を予定している、各機能にフォーカスしたセッションをお待ちください！

アジェンダ

1. AWS Systems Manager 概要紹介
2. Explorer / OpsCenter の位置づけと概要
3. AWS Systems Manager Explorer の紹介
4. AWS Systems Manager OpsCenter の紹介
5. 料金
6. まとめ

AWS Systems Manager の概要

AWS Systems Manager

ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション



AWS Config

Configuration history



Amazon EventBridge

Notification and remediation



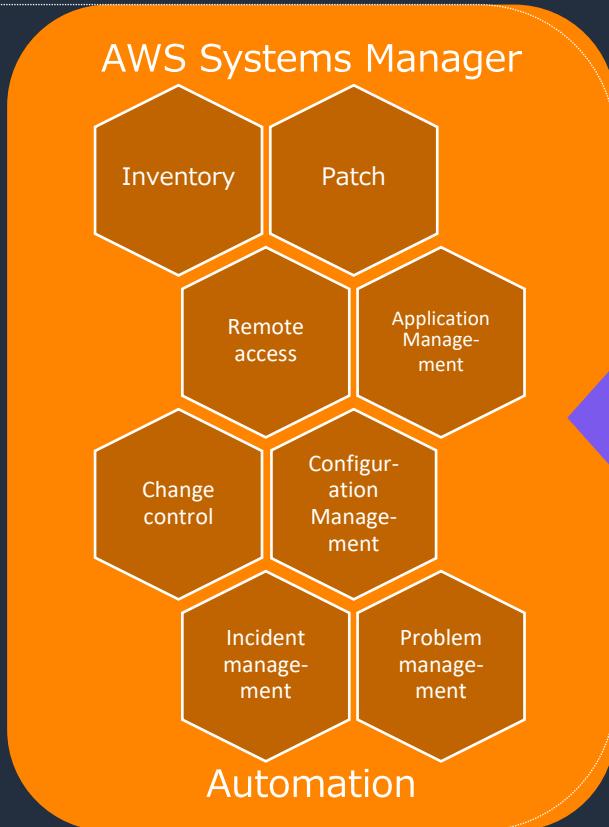
AWS CloudTrail

Audited actions



AWS Identity and Access Management (IAM)

Role-based access control



Cloud



On-premises



Edge

Integration
connectors
and APIs

- Third-party tools
- ITSM
- Custom solutions

AWS の他のサービスや
3rd Party のツールと統合された
管理ソリューションを提供

(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

運用管理

-  Explorer
-  OpsCenter
-  Incident Manager

アプリケーション管理

-  Application Manager
-  AppConfig
-  Parameter Store

変更管理

-  Change Manager
-  Automation
-  Maintenance Windows
-  Change Calendar

ノード管理

-  Fleet Manager
-  Session Manager
-  Inventory
-  Run Command
-  Patch Manager
-  Distributor
-  State Manager

Quick Setup

AWS Systems Manager の機能

運用管理	アプリケーション管理	変更管理	ノード管理
 Explorer  OpsCenter  Incident Manager	 Application Manager  AppConfig  Parameter Store	 Change Manager  Automation  Maintenance Windows  Change Calendar	 Fleet Manager  Session Manager  Inventory  Run Command  Patch Manager  Distributor  State Manager
Quick Setup			

Explorer / OpsCenter の 位置づけと概要

Explorer と OpsCenter の位置づけと想定利用者



Explorer

- ・ カスタマイズ可能な**運用ダッシュボード**
- ・ 複数のサービスの運用データ (**OpsData**) をマルチアカウント・マルチリージョンで集約し、サマリーを表示してくれる
- ・ 主にDevOpsマネージャー向け

運用管理者が**組織全体の運用状況を俯瞰**し、対処が必要な領域を素早く特定



OpsCenter

- ・ AWSリソースに関する運用作業項目 (**OpsItem**) を表示、調査、解決するための一元的な場所
- ・ OpsItem が集約および標準化され、問題の診断と是正に役立つデータが提供される
- ・ 主に運用エンジニアやITプロフェッショナル向け

運用エンジニアが**担当システムの運用作業項目を管理**し、迅速に対応

Explorer が役立つ場面

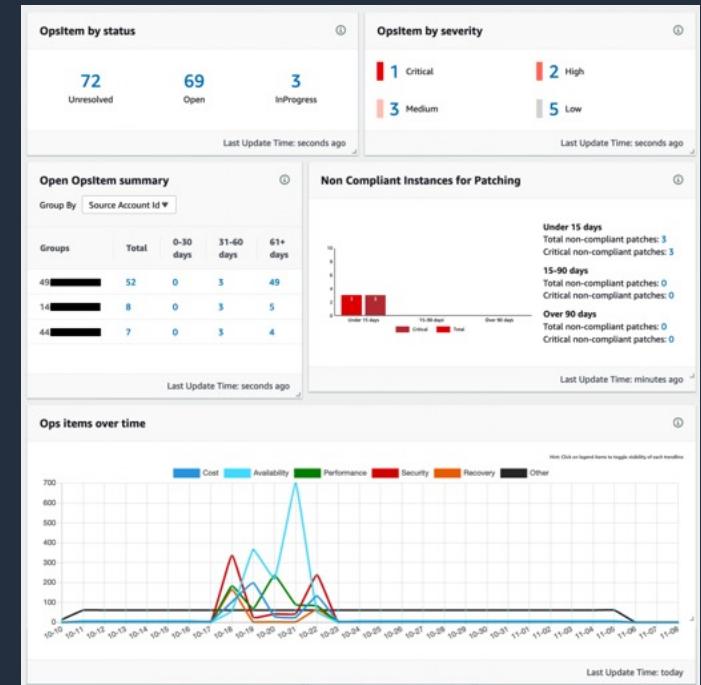
- 複数のリージョンやアカウントで AWS の利用が拡大
- 管理対象のマネージドノードがどんどん増える
- オンプレとクラウドのハイブリッド構成で管理がさらに複雑に



運用責任者は、現在の運用状況の概要をひと目で把握し、アクションが必要な箇所を素早く特定したい



Explorer



そんなときに Explorer が便利！



Explorer

ハイレベルの運用ダッシュボード

- マルチアカウント・マルチリージョンのハイレベルな運用ダッシュボード。
- 複数のサービスからの情報が集約される。

Instance / Compute Optimizer

Amazon Elastic Compute Cloud (Amazon EC2)

AWS Config Compliance

AWS Config

Trusted Advisor (※)

AWS Trusted Advisor

Security Hub Findings

AWS Security Hub

- Patch Compliance
- OpsItems
- Inventory
- Association

AWS Systems Manager

Support Center (※)

AWS Support

※ Enterprise Support、Business Support プランが必要

aws Explorerについての詳細は[こちら](#)。



OpsCenter が役立つ場面

- 日々さまざまな運用上の問題が発生
- 最新ステータスがわからない、管理できていない
- 運用上の問題へ対処するために複数のコンソール画面を確認する必要があり、調査や対応に時間がかかる



運用エンジニアは、運用上の問題を迅速に調査、対処したい



OpsCenter

AWS Systems Manager > OpsCenter

OpsCenter

未解決および対応中の OpsItem

合計数	未解決	進行中
8	8	0

ソースと年齢別の OpsItem

ソース別にグループ化	カウント	0~30 日	31~90 日	90 日以上
EC2	4	4	0	0
Security Hub	3	3	0	0
CloudWatch Alarm	1	1	0	0

OpsItem が最も多いソース

Source	Total count
EC2	4
Security Hub	3
CloudWatch Alarm	1

運用上のインサイト (0)

Insight のタイプ	未解決
OpsItems を複製	0
ほとんどの OpsItems を生成するソース	0

すべての運用上のインサイトを表示

そんなときに OpsCenter が便利！



OpsCenter

対応すべき運用アイテムの可視化、問題解決の支援

- ④ 運用上の問題 (OpsItem) の集約ビューを提供。
- ④ OpsItem に関するデータを一元的に提供し、問題解決までの時間短縮を支援する。
- ④ マルチアカウントでの OpsItem の表示や操作も可能。
- ④ ServiceNow, Jira Service Management と連携も。

NEW
2022/11

AWS Systems Manager > OpsCenter

OpsCenter

概要 | OpsItems

未解決および対応中の OpsItem

合計数	未解決	進行中
8	8	0

ソースと年齢別の OpsItem

ソース別にグループ化	カウント	0~30 日	31~90 日	90 日以上
EC2	4	4	0	0
Security Hub	3	3	0	0
CloudWatch Alarm	1	1	0	0

運用上のインサイト (0)

Insight のタイプ	未解決
OpsItems を複製	0
ほとんどの OpsItems を生成するソース	0

すべての運用上のインサイトを表示

OpsItem が最も多いソース

Source	Total count
EC2	4
Security Hub	3
CloudWatch Alarm	1

OpsCenterについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

Explorer と OpsCenter の開始方法

Explorer と OpsCenter の開始方法

まずは Systems Manager コンソールで「統合セットアップ」を開始する

統合セットアップでは Explorer と OpsCenter の利用に必要な以下のタスクが実行される

1. ロールとアクセス権限の設定
2. OpsItem 作成のデフォルトルールを許可
3. OpsData ソースを許可
4. レポートタグキー指定の許可

詳細は公式ドキュメントも参照ください

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/Explorer-setup.html

統合セットアップ手順 (1/4)

The screenshot shows the AWS Systems Manager Explorer landing page. On the left, there's a sidebar with navigation links for 'AWS Systems Manager' (High-Speed Setup, Operations Management: Explorer (highlighted), OpsCenter, CloudWatch Dashboard, Incident Manager), Application Management (Application Manager, AppConfig, Parameter Store), and Change Management (Change Manager, Automation, Change Calendar, Maintenance Window). The main content area has a title 'Explorer' and a subtitle 'OpsData をすばやく表示し、OpsItems に対してアクションを実行する'. It describes the service as a customizable operations dashboard for AWS resources across accounts and regions, showing aggregate views of OpsData and OpsItems, and their distribution across business units or applications over time. A call-to-action button 'ご利用開始' is highlighted with an orange border. Below the main content, there's a section titled 'しきみ' with numbered steps: ① Explorer を使 ② ドラッグアンドロード ③ 項目の評価、④ 自動化された. To the right, there are two boxes: 'Explorer の使用を開始する' (with text about starting with Explorer Setup) and 'ご利用開始' (with links to 'Explorer をセットアップ' and 'Explorer ダッシュボードをカスタマイズ').

AWS Systems Manager X

オペレーション管理

Explorer

OpsData をすばやく表示し、OpsItems に対してアクションを実行する

AWS Systems Manager Explorer は、AWS リソースのカスタマイズ可能なオペレーションダッシュボードです。Explorer は、AWS アカウントおよびリージョン間のオペレーションデータ (OpsData) およびオペレーション作業項目 (OpsItems) の集計ビューを表示します。Explorer は、OpsItems がビジネスユニットまたはアプリケーションにどのように分散されるか、時間の経過に伴う動向、およびカテゴリ別の変化についてのコンテキストを提供します。

ご利用開始

しきみ

① Explorer を使 ② ドラッグアンドロード ③ 項目の評価、④ 自動化された

Explorer の使用を開始する

開始するには、Explorer Setup を使用して設定とユーザー設定を行います。

ご利用開始

Explorer をセットアップ

Explorer ダッシュボードをカスタマイズ

統合セットアップ手順 (2/4)

Explorer のセットアップ画面

IAM ロール

セットアップにより、以下の AWS Identity and Access Management (IAM) ロールが作成されます。 [詳細はこちら](#)

OpsItems-CWE-Role: Amazon CloudWatch Events が OpsItems を作成できるようにするサービスロール。 [ロールポリシーを表示](#)

OpsItems のデフォルトルール

AWS CloudWatch Events でデフォルトのルールを有効にします。これらのルールは、一般的なイベントに応じて OpsItems を自動的に作成します。 [詳細はこちら](#)

このオプションを有効にすると、Explorer で AWS Config と AWS CloudWatch Events を設定して、一般的に使用されるルールとイベントに基づいて OpsItem を自動的に作成します。Config ルールと CloudWatch Events の詳細なリストについては、Systems Manager ユーザーガイドを参照してください。

↑デフォルトで有効になっている（詳細は次スライド）

補足：OpsItems のデフォルトルール

- 統合セットアップでこのプロンプトをオンにすると、EventBridge (CloudWatch Events) のルールが自動的に作成される
 - 特定のイベントをトリガーに OpsItems が自動的に作成されるように
- デフォルトルールを参考にして任意のイベントに対応したルールを作成することも可能
- 後から個々のデフォルトルールの ON/OFF 切り替えも可能
- 統合セットアップではデフォルトルールを作成せず、後から作成することも可能

補足：OpsItems のデフォルトルール

ルール名	検出するイベント
SSMOpsItems-Autoscaling-instance-launch-failure	EC2 Auto Scaling がインスタンスの起動に失敗
SSMOpsItems-Autoscaling-instance-termination-failure	EC2 Auto Scaling がインスタンスの終了に失敗
SSMOpsItems-EBS-snapshot-copy-failed	EBS snapshot のコピーが失敗
SSMOpsItems-EBS-snapshot-creation-failed	EBS snapshot の作成が失敗
SSMOpsItems-EBS-volume-performance-issue	EBS volume のパフォーマンスの問題
SSMOpsItems-EC2-issue	EC2 関連の問題
SSMOpsItems-EC2-scheduled-change	EC2 のメンテナンススケジュールの変更
SSMOpsItems-RDS-issue	RDS 関連の問題
SSMOpsItems-RDS-scheduled-change	RDS のメンテナンススケジュールの変更
SSMOpsItems-SSM-maintenance-window-execution-failed	SSM メンテナンスウィンドウの実行の失敗
SSMOpsItems-SSM-maintenance-window-execution-timedout	SSM メンテナンスウィンドウの実行タイムアウト

統合セットアップ手順 (3/4)

Explorer のセットアップ画面

The screenshot shows the AWS Explorer setup screen. On the left, a sidebar lists various AWS services as potential OpsData sources. A callout bubble highlights a message box in the center-right area.

OpsData ソース
Explorer は、AWS 全体のオペレーションデータを OpsData として集計します。

セットアップにより、以下の OpsData ソースが有効になります。

- AWS Config Compliance
- Security Hub
- OpsCenter OpsItems
- Systems Manager Patch Compliance
- Amazon EC2
- Systems Manager Inventory
- Trusted Advisor
- Support Center
- Compute Optimizer
- Systems Manager Association

前提となるAWSサービスの状況によっては、各AWSサービスの有効化など追加のセットアップを案内するメッセージが表示される場合があります

追加のセットアップを推奨
このソースのデータを表示するには、Security Hub を有効にする必要があります。 詳細は[こちら](#)

レポートのタグ
Explorer ダッシュボードで OpsData フィルタリングのリソースタグキーを最大 5 つ入力または選択します。

タグキー X 削除

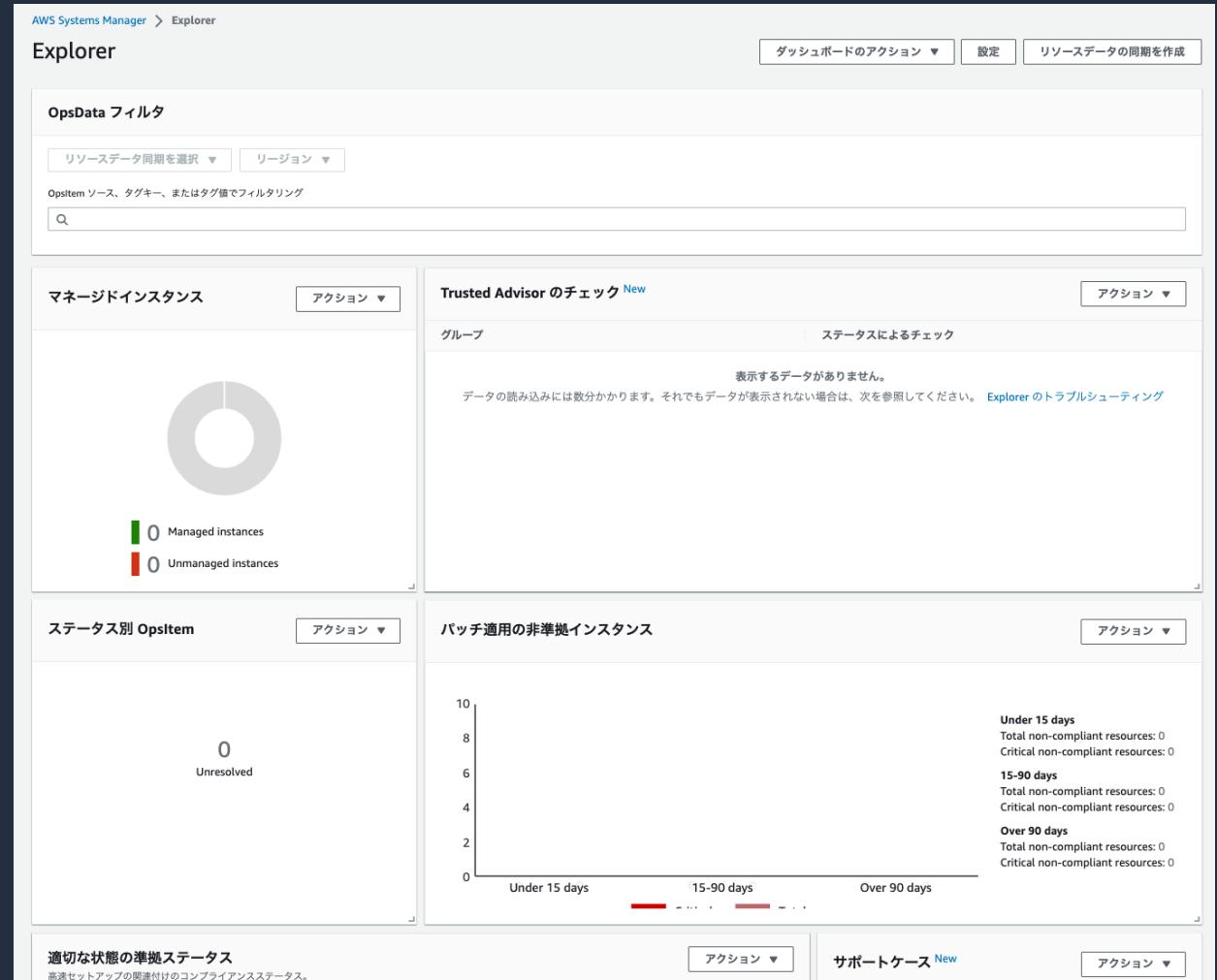
新しいタグキーを追加

キャンセル エクスプローラーの有効化

統合セットアップ手順 (4/4)

統合セットアップが完了し、
Explorer のダッシュボードが
表示される

- ✓ データの反映まで時間がかかる場合があります



期待どおりのデータが表示されない場合はトラブルшу
テイティングのドキュメントも参照ください

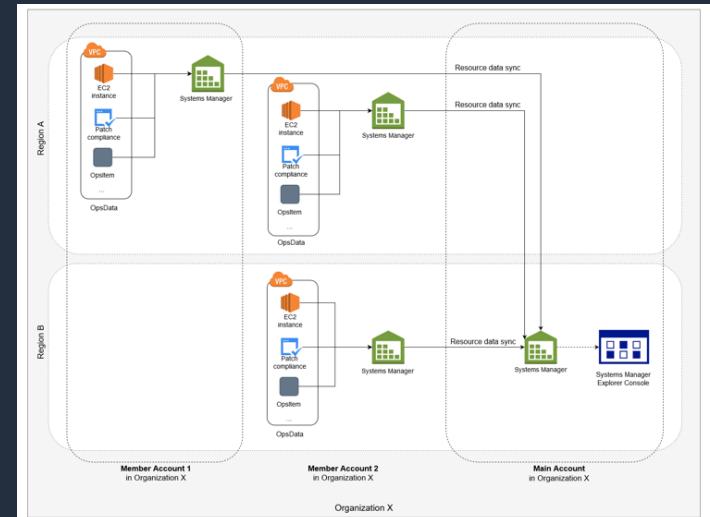
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/Explorer-troubleshooting.html



マルチアカウント/マルチリージョン対応

1. リソースデータ同期

- OpsData の集約を行う設定
- 2つの集約オプションから選択可能
 1. 単一アカウント/複数リージョン
 2. 複数アカウント/複数リージョン (Organizations 前提)



2. Organizations における委任管理者

- Organizations の管理アカウントを使用せず、委任管理者がリソースデータ同期の設定を管理できる
- これにより、委任管理者アカウントの Explorer に OpsData が集約される

https://docs.aws.amazon.com/ja_ip/systems-manager/latest/userguide/Explorer-resource-data-sync.html

AWS Systems Manager Explorer の使い方

Demo

The screenshot shows the AWS Systems Manager Explorer interface. It includes sections for Managed Instances (6), Unmanaged Instances (0), Instance Status (28 Unresolved, 28 Open), and AWS Config Compliance (概要). The interface is dark-themed with green and white highlights.

The screenshot shows the AWS Systems Manager Settings interface. It includes sections for OpItem rules (Availability, Cost, Performance, Security, Recovery) and OpsData source configuration (AWS Config Compliance, Security Hub, Systems Manager Patch Compliance, AWS Systems Manager Explorer, Systems Manager Patch Summary, Trusted Advisor, Support Center, Compute, Systems). The interface is light-themed with blue and grey highlights.



Explorer のデータソース (OpsData) (1/2)

データソース	内容
Systems Manager OpsCenter	ステータス別の OpsItems の数、重要度別の OpsItems の数、グループ全体で過去の一定期間中にOpenとなった OpsItems の数、OpsItems の長期の履歴データ
Systems Manager Patch Manager	パッチに準拠していないノードの数
Systems Manager State Manager	関連付けのコンプライアンスリソースの合計数、非準拠リソースの合計数、コンプライアンス準拠の割合
Systems Manager Inventory	マネージドノードとアンマネージドノードの総数
Amazon EC2	ノードの総数、特定の Amazon Machine Image (AMI) を使用するノードの数

Explorer のデータソース (OpsData) (2/2)

データソース	内容
AWS Compute Optimizer	アンダープロビジョニングおよびオーバープロビジョニングされた EC2 インスタンスの数、最適化の結果、オンデマンド料金の詳細、インスタンスタイプと価格の推奨事項
AWS Support Center のケース ※	ケース ID、重大度、ステータス、作成時刻、件名、サービス、カテゴリ
AWS Config	準拠および非準拠の AWS Config ルールの全体的な要約、準拠および非準拠のリソースの数
AWS Security Hub	Security Hub の結果の全体的な概要、重要度別にグループ化された各検出の数
AWS Trusted Advisor ※	コストの最適化、セキュリティ、耐障害性、パフォーマンス、サービス制限の各分野における EC2 リザーブドインスタンスのベストプラクティスチェックのステータス

- ✓ AWS Trusted Advisor および AWS Support Center のケースを表示するには
エンタープライズまたはビジネスサポートプランが必要

AWS Systems Manager OpsCenter の使い方

OpsItem とは？

AWS リソースのパフォーマンスと健全性に影響を与える、運用上の対処が必要な作業項目

OpsItem の例：

- ・ セキュリティの問題 ・・・ Security Hub からの緊急度の高いアラート
- ・ パフォーマンスの問題 ・・・ DynamoDB のスロットリングイベント
- ・ 処理の失敗 ・・・ EC2 Auto Scaling によるインスタンス起動の失敗
- ・ 健全性のアラート ・・・ RDSやEC2のメンテナンス通知
- ・ 状態の変更 ・・・ EC2 インスタンスの状態が [実行中] から [停止] に変わる

OpsItems を作成するサービス (1/2)

サービスや機能	内容
Amazon DevOps Guru	DevOps Guru の Systems Manager 統合を有効にした場合、DevOps Guru の検出した各インサイトの OpsItems を自動的に生成する
AWS Security Hub	Security Hub を有効にし、Explorer で Security Hub データソースを有効にした場合、EventBridge ルール経由で OpsItems が自動的に生成される
OpsCenter オペレーションインサイト	OpsCenter のオペレーションインサイトを有効化することで、アカウント内の OpsItems を自動的に分析し、重複する OpsItem を集約してレポートするために insight タイプの OpsItems を自動的に生成する
AWS Incident Manager	Incident Manager をセットアップして設定すると、Incident Manager でインシデントが作成される際に自動的に OpsItems を作成する
CloudWatch Application Insights for .NET and SQL Server	.NET および SQL Server 用の CloudWatch Application Insights でアプリケーションリソースを設定する場合、問題が検出されたときにシステムが OpsCenter で OpsItems を作成するように選択できる

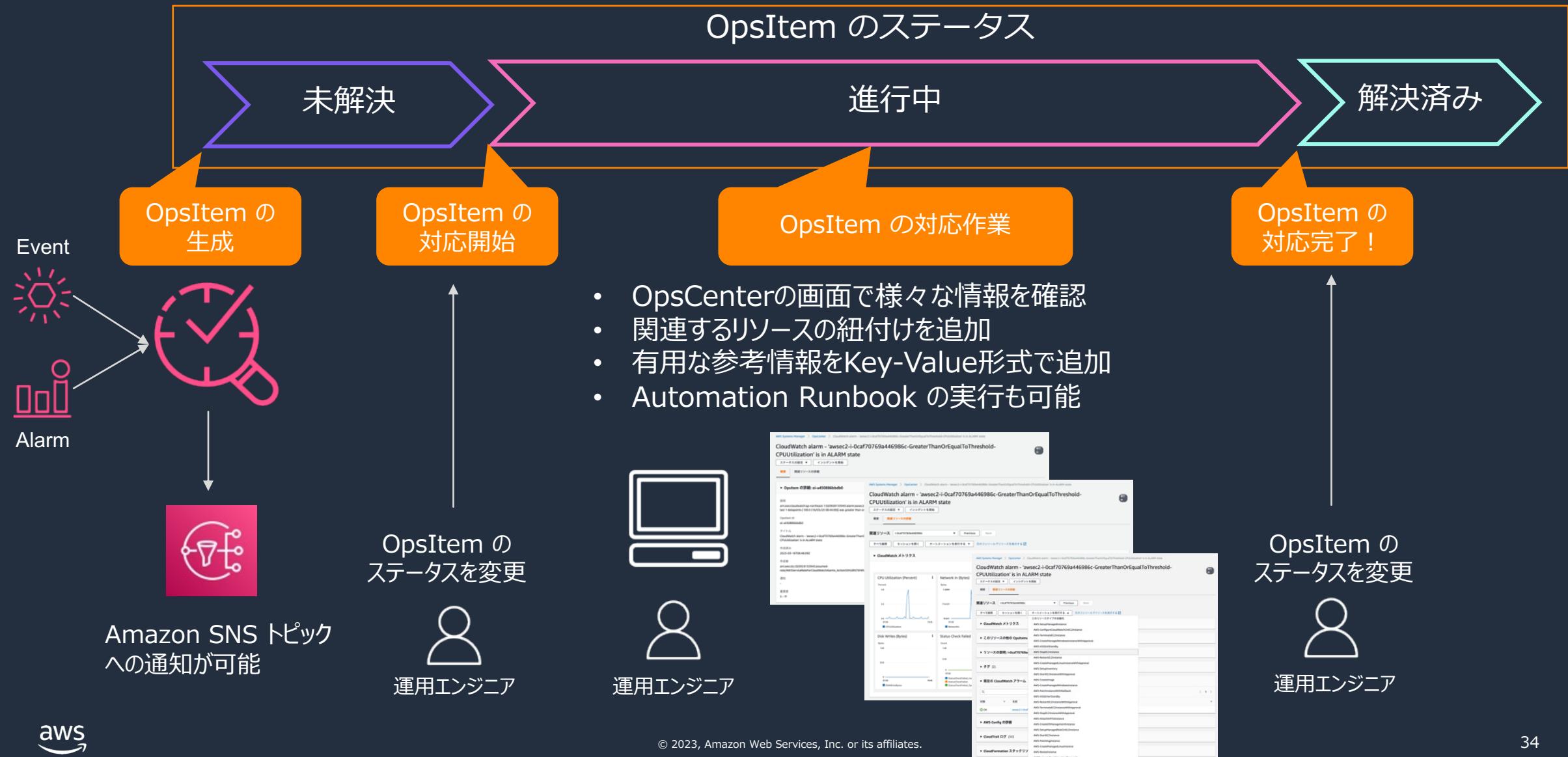
OpsItems を作成するサービス (2/2)

サービスや機能	内容
Amazon EventBridge	Amazon EventBridge のイベントルールを作成することで、イベントをトリガーに OpsCenter の OpsItem を自動的に作成可能
Amazon CloudWatch	CloudWatch アラームが ALARM 状態になったときに OpsCenter で OpsItem が自動的に作成されるように Amazon CloudWatch を設定可能



この他、AWS CLI や AWS SDK を使用して手動で OpsItems を作成することも可能

OpsItems のライフサイクル



OpsCenter の画面構成 (1/4)

The screenshot shows the AWS OpsCenter Overview page. At the top, there are three summary counts: '未解決および対応中の OpsItem' (Total: 8), '未解決' (Unresolved: 8), and '進行中' (In Progress: 0). Below this is a section titled 'ソースと年齢別の Opsitem' with a table showing counts for EC2, Security Hub, and CloudWatch Alarm across 0~30, 31~90, and 90+ day ranges. To the right is a chart titled 'OpsItem が最も多いソース' showing the total count of items from EC2 (4), Security Hub (3), and CloudWatch Alarm (1). At the bottom is a section titled '運用上のインサイト (0)' with a table showing 0 insights for various categories like 'Insight のタイプ' and 'Opsitems を複製'.

ソース別にグループ化	カウント	0~30 日	31~90 日	90 日以上
EC2	4	4	0	0
Security Hub	3	3	0	0
CloudWatch Alarm	1	1	0	0

Source	Total count
EC2	4
Security Hub	3
CloudWatch Alarm	1

OpsCenter の [概要] 画面 では以下の OpsItem 数をサマリ表示

- 合計/未解決/進行中
- 経過日数別 & ソースごと
- 生成した数の多いソース順
- 運用上のインサイト (後述)

OpsCenter の画面構成 (2/4)

[OpsItems] 画面では OpsItem をリスト表示

フィルタや検索が可能

OpsItems (3)

未解決 進行中▼

ID	タイトル	タイプ	重要度	ステータス	ソース	カテゴリ	作成済み	更新済み	件数
oi-bfecfc8e2df2	CloudWatch alarm - 'TEST-CreateOpsItem' is in ALARM state	/aws/issue	4	未解決	CloudWatch Alarm	Performance	Mar 06 2023	Mar 06 2023	0209
oi-1e027f9260e8	CloudWatch alarm - 'do-not-delete-rds-custom-agent-heartbeat-i-08cf1e2436f7675ae' is in ALARM state	/aws/issue	4	未解決	CloudWatch Alarm	Performance	Jan 06 2023	Mar 03 2023	02092815
oi-13ce15237691	CloudWatch alarm - '0001' is in ALARM state	/aws/issue	4	未解決	CloudWatch Alarm	Availability	Jan 06 2023	Mar 05 2023	02092815

ステータスでのフィルタも可能

- 未解決
- 進行中
- 解決済み
- 未解決 進行中
- すべて

OpsCenter の画面構成 (3/4)

OpsItem の [概要] 画面

The screenshot shows the AWS Systems Manager OpsCenter interface. At the top, it displays a CloudWatch alarm named 'TEST-CreateOpsitem' in an ALARM state. Below this, the 'Opsitem の詳細' section shows the ARN 'oi-bfecfcBe2df2'. The '関連リソース' section lists two resources: 'arn:aws:cloudwatch:ap-northeast-1:020928153945:alarm:TEST-CreateOpsitem' (AWS::CloudWatch::Alarm) and 'arn:aws:ec2:ap-northeast-1:020928153945:instance/i-0caf70769446986c' (AWS::EC2::Instance). The '過去 30 日間のオートメーション実行' section is empty. The 'ランブック' section lists five Automation Runbooks: 'AWS-CreateServiceNowIncident', 'AWS-ConfigureMaintenanceWindows', 'AWS-EnableCWAlarm', 'AWS-EnableCloudTrailKmsEncryption', and 'AWS-SetupManagedInstance'. The 'Opsitem タグ' section is empty. The '関連する Opsitem' section is also empty.

- **OpsItem の詳細** : OpsItem のステータスや優先度、重要度、カテゴリ等の表示と編集が可能
- **関連リソース** : 影響を受けたAWSリソースや OpsItem を作成したリソース。手動で関連リソースのARNを追加可能
- **過去 30 日間のオートメーション実行**
- **ランブック** : Automation Runbook のリスト
- **OpsItem タグ**
- **類似の OpsItem** : 同様の用語を使用している OpsItem が自動的に抽出され、表示される
- **運用データ** : OpsItem に関する有用なリファレンスの詳細を提供するカスタムデータ
- **関連する OpsItem**

OpsCenter の画面構成 (4/4)

OpsItem の [関連リソースの詳細] 画面の例

EC2.8 EC2 instances should use Instance Metadata Service Version

概要 関連リソースの詳細

関連リソース i-0caf70769a446986c Previous Next

すべて展開 セッションを開く オートメーションを実行する 元のコンソールでリソースを表示する

▶ CloudWatch メトリクス

▶ このリソースの他の OpsItems (1)

▶ リソースの説明: i-0caf70769a446986c

▶ タグ (2)

▶ 現在の CloudWatch アラーム (1)

▶ AWS Config の詳細

▶ CloudTrail ログ (4)

▶ CloudFormation スタックリソース (0)

OpsItem に紐づいているリソースのリストから 1 つを選択すると、リソースに関する以下の情報を確認できる

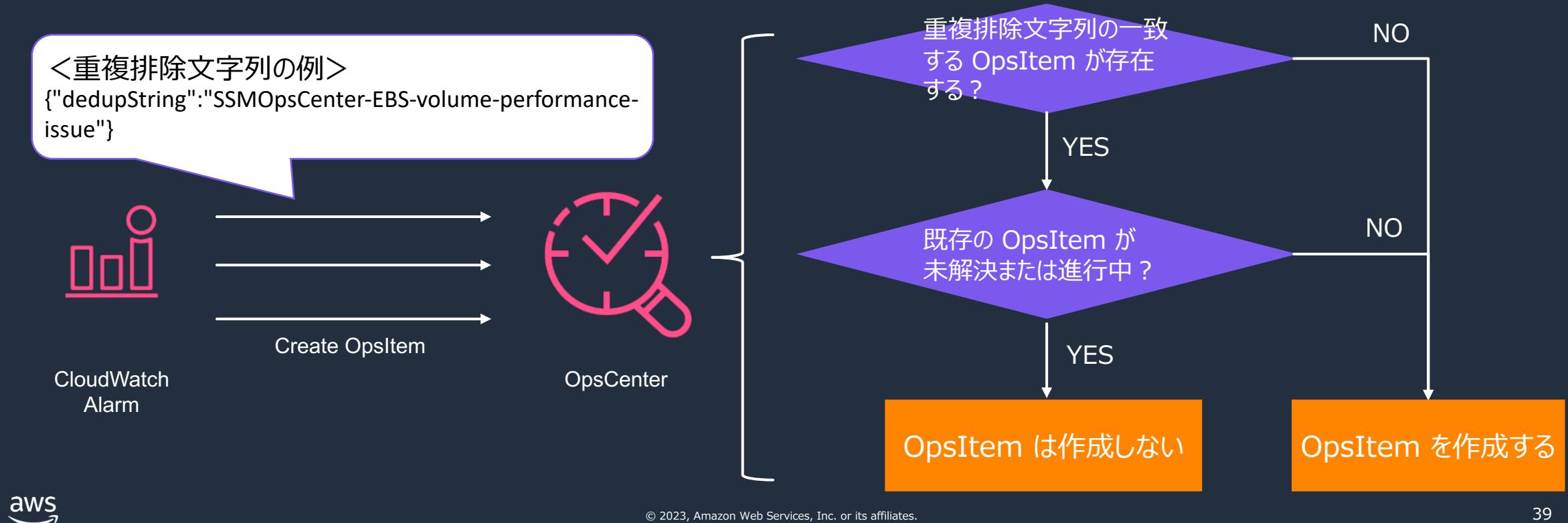
- CloudWatch メトリクス
- このリソースの他の OpsItems
- リソースの説明
- タグ
- 現在の CloudWatch アラーム
- AWS Config の詳細
- CloudTrail ログ
- CloudFormation スタックリソース

※表示される項目はリソースにより異なります

その他の便利な機能 (1/4)

重複排除

対応中の事象に対して何度も同じ内容の OpsItem が作成されることを防ぐ機能。
OpsItem 作成時に指定する重複排除文字列をもとにチェック。



その他の便利な機能 (2/4)

運用上のインサイト (Operational Insights)

OpsItem を自動的に分析し、複数の OpsItem を集約する OpsItem を生成してくれる。関連する OpsItem のステータスをまとめて変更するのに便利



以下の条件に合致する場合、insight タイプの OpsItem が自動生成される

- **重複する OpsItem** : 8つ以上のOpsItemが同じリソースに対して同じタイトルをもつ
- **最も多くの OpsItem を生成するリソース** : 50以上のOpsItemが同じタイトルをもつ

※デフォルトでは無効化されているため、明示的に有効化する必要あり

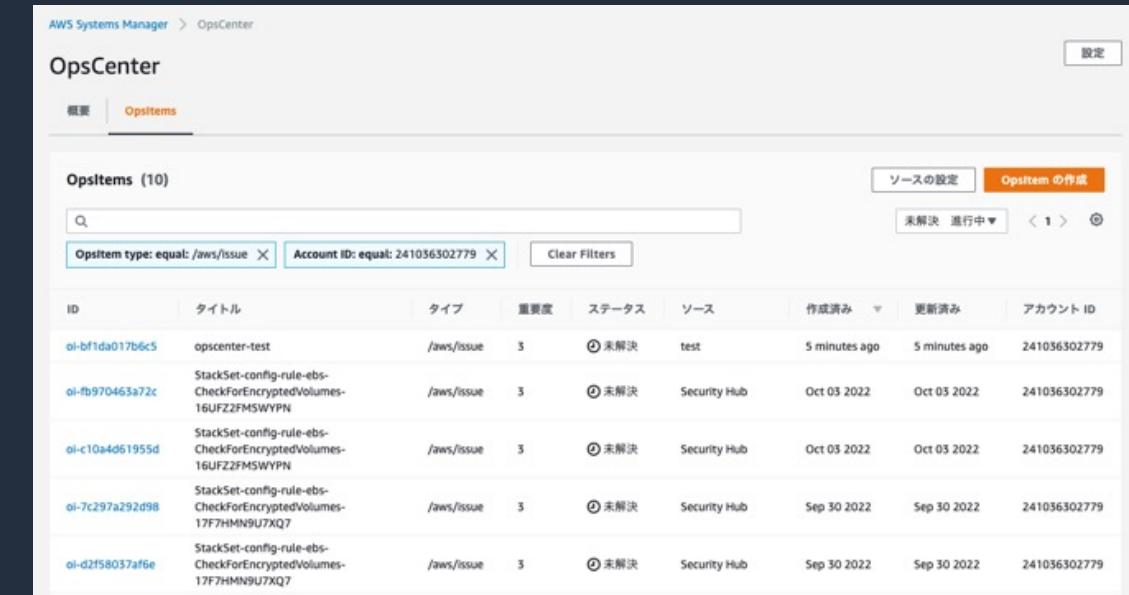
参考Blogは[こちら](#)。

その他の便利な機能 (3/4)

クロスアカウント対応

OpsCenter ダッシュボードから別アカウントの運用の問題を診断して修復可能

- Organizations の管理アカウントまたは委任された管理者アカウントがメンバーアカウントの OpsItems を作成、表示、更新可能
- メンバーアカウントのAWSリソースの問題を修正するために、管理アカウントまたは委任された管理者アカウントから Automation の Runbook を起動することも可能
- 事前にドキュメント記載のセットアップタスクの実行 (CloudFormation スタックの作成) が必要



The screenshot shows the AWS Systems Manager OpsCenter interface. The top navigation bar includes 'AWS Systems Manager' and 'OpsCenter'. Below the navigation, there are two tabs: '概要' (Overview) and 'OpsItems' (selected), which is highlighted in orange. A search bar is present above the main table. The table has columns for 'ID', 'タイトル' (Title), 'タイプ' (Type), '重要度' (Severity), 'ステータス' (Status), 'ソース' (Source), '作成済み' (Created), '更新済み' (Updated), and 'アカウント ID' (Account ID). There are 10 items listed, all of which are '未解決' (Unresolved) and have a severity of 3. The table also includes filters at the bottom: 'Opsitem type: equal: /aws/issue' and 'Account ID: equal: 241036302779'. Buttons for 'ソースの設定' (Source Settings) and 'OpsItem の作成' (Create OpsItem) are located on the right side of the table.

ID	タイトル	タイプ	重要度	ステータス	ソース	作成済み	更新済み	アカウント ID
oi-bf1da017b6c5	opscenter-test	/aws/issue	3	未解決	test	5 minutes ago	5 minutes ago	241036302779
oi-fb970463a72c	StackSet-config-rule-ebs-CheckForEncryptedVolumes-16UFZ2FMSWYPN	/aws/issue	3	未解決	Security Hub	Oct 03 2022	Oct 03 2022	241036302779
oi-c10a4d61955d	StackSet-config-rule-ebs-CheckForEncryptedVolumes-16UFZ2FMSWYPN	/aws/issue	3	未解決	Security Hub	Oct 03 2022	Oct 03 2022	241036302779
oi-7c297a292d98	StackSet-config-rule-ebs-CheckForEncryptedVolumes-17F7HMMN9U7XQ7	/aws/issue	3	未解決	Security Hub	Sep 30 2022	Sep 30 2022	241036302779
oi-d2ff58037af6e	StackSet-config-rule-ebs-CheckForEncryptedVolumes-17F7HMMN9U7XQ7	/aws/issue	3	未解決	Security Hub	Sep 30 2022	Sep 30 2022	241036302779

<https://docs.aws.amazon.com/systems-manager/latest/userguide/OpsCenter-getting-started-multiple-accounts.html>



その他の便利な機能 (4/4)

ServiceNow や Jira Service Managementとの連携

- ServiceNow や Jira Service Management の管理者が AWS Service Management Connector (SMC) を使用することで、OpsCenter を始めとする Systems Manager の各種機能やその他のAWSサービスと統合可能
- ServiceNow 向けの SMC は ServiceNow ストアで入手可能（無償）
- Jira Service Management Data Center 向けの SMC は Atlassian Marketplace で入手可能（無償）

<https://docs.aws.amazon.com/smc/latest/ag/sn-what-is.html>

<https://docs.aws.amazon.com/smc/latest/ag/integrations-jiraservicedesk.html>



OpsCenter と Incident Manager の使い分け

OpsCenter

- ・ 管理対象は、 OpsItem（運用上の対処が必要な項目）
- ・ OpsItem を集約および標準化し、問題の診断と是正に役立つデータを提供する
- ・ インシデントに紐付いていない OpsItem を Incident Manager へエスカレーションすることも可能

Incident Manager

- ・ 管理対象は、インシデント（計画外のサービスの中止または品質低下）
- ・ 対応計画によるインシデントへの備えと、インシデント発生時のアラートとエンゲージメント／トリアージ／調査と緩和／事後分析を支援
- ・ インシデントへの対応開始時、OpsItem も自動的に作成される。事後分析で必要な改善アクションが発生した場合、それらを OpsItem として管理することも可能

使いたい機能から使ってみるのがおすすめ！

AWS Systems Manager Explorer/OpsCenter の料金

Explorer と OpsCenter の料金

Explorer

- Explorer の利用自体は無料
- ダッシュボード表示時に Call する OpsCenter API (GetOpsSummary) の課金
- OpsData のエクスポート時に実行する Automation Runbook の課金

OpsCenter

- その月に作成した OpsItem の数と、リクエストされた API コール (Get、Describe、Update、GetOpsSummary) の数に基づく課金

項目	料金
OpsItem の数	OpsItem 1,000 個あたり 2.97 USD
API リクエスト (Get, Describe, Update, GetOpsSummary)	リクエスト 1,000 件あたり 0.039 USD

<https://aws.amazon.com/jp/systems-manager/pricing/>



まとめ



まとめ

- Systems Manager Explorer は
 - 複数の AWS アカウントとリージョンからオペレーションデータを集約して表示する、カスタマイズ可能なダッシュボードです
 - 運用管理者が組織全体の運用状況を俯瞰し、対処が必要な領域を素早く特定するのに役立ちます
- Systems Manager OpsCenter は
 - 運用作業項目(OpsItem)を一元的に表示、調査、および解決できる場所を提供します
 - 運用エンジニアが担当システムの運用作業項目を管理し、迅速に対応するのに役立ちます

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!



AWS Systems Manager

Hybrid Activations 編

AWS Black Belt Online Seminar

村田 京介

Solutions Architect
2023/06

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=PLzWGOASvSx6FlwIC2X1nObr1KcMCBBlqY>

内容についての注意点

- ・ 本資料では 2023 年 5 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

本セミナーの対象者

AWS の運用をされている方、これから運用される予定の方

本セミナーの目的

- AWS Systems Manager Hybrid Activations の機能とユースケースをご理解いただく。

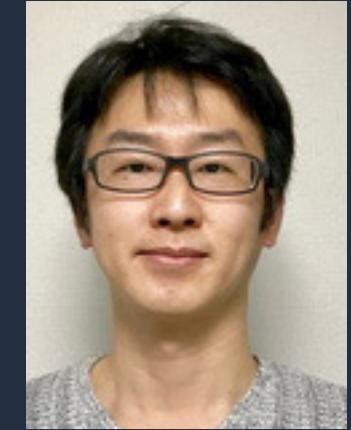
本日お話ししないこと

- AWS Systems Manager の全体的な説明
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager Hybrid Activations 以外の機能の詳細
→ [AWS サービス別資料](#)より各機能にフォーカスしたセッションをご参照ください。
検索結果に表示されない機能については今後公開予定です。

自己紹介

名前：村田 京介 (Kyosuke Murata)

所属：技術統括本部 エンタープライズ技術本部
サービスソリューション部



経歴：

ソフトウェアベンダーのコンサルタントを経て、
現在はソリューションアーキテクトとしてエンタープライズのお客様を担当

好きな AWS サービス： AWS Systems Manager



AWS Chatbot



アジェンダ

1. AWS Systems Manager (SSM) の概要
2. EC2 インスタンス以外を SSM で管理するには？
3. 具体的な構成手順とデモ
4. SSM Hybrid Activations の料金
5. まとめ

AWS Systems Manager (SSM) の概要



AWS Systems Manager (SSM)

ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション



AWS Config

Configuration history



Amazon EventBridge

Notification and remediation



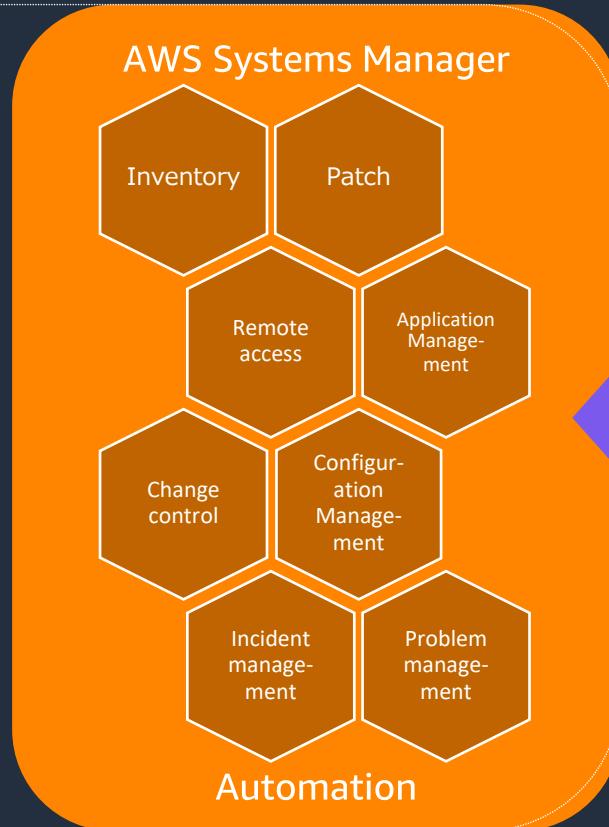
AWS CloudTrail

Audited actions



AWS Identity and Access Management (IAM)

Role-based access control



Integration
connectors
and APIs

- Third-party tools
- ITSM
- Custom solutions

AWS の他のサービスや
3rd Party のツールと統合された
管理ソリューションを提供

SSM の機能

運用管理	アプリケーション管理	変更管理	ノード管理
 Explorer	 Application Manager	 Change Manager	 Fleet Manager
 OpsCenter	 AppConfig	 Automation	 Session Manager
 Incident Manager	 Parameter Store	 Maintenance Windows	 Inventory
		 Change Calendar	 Run Command
			 Patch Manager
			 Distributor
			 State Manager

Quick Setup

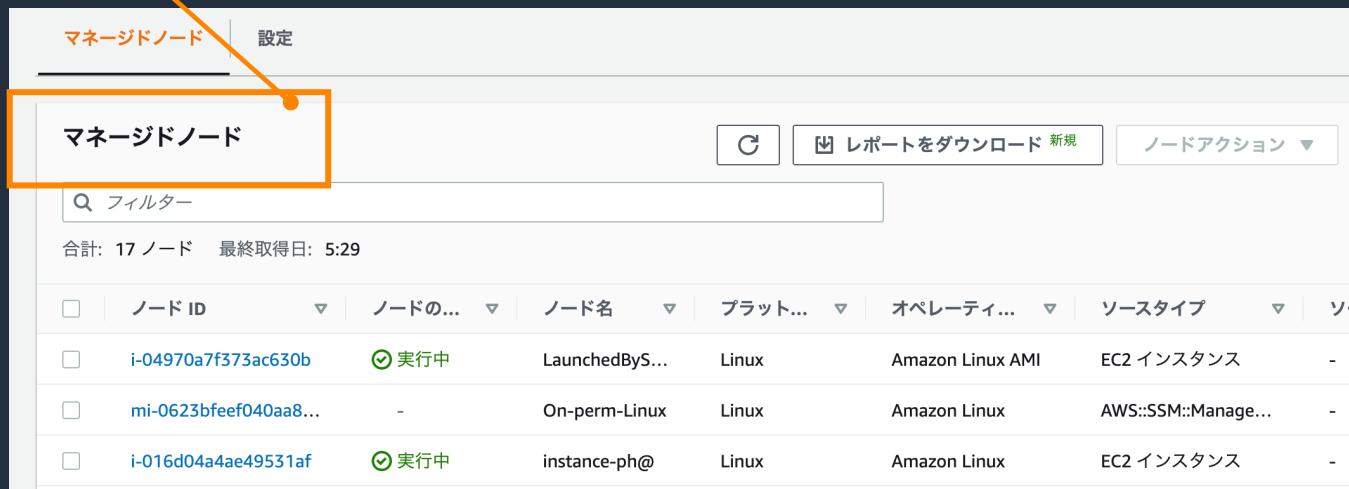
EC2 インスタンス以外を SSM で管理するには？



SSM を使って管理を行うためには

“マネージドノード”にする

ここに一覧で出てくるようになります



The screenshot shows the AWS Systems Manager Managed Nodes console. At the top, there are two tabs: "マネージドノード" (selected) and "設定". Below the tabs is a search bar labeled "フィルター" and a status message "合計: 17 ノード 最終取得日: 5:29". To the right of the search bar are three buttons: "C" (refresh), "レポートをダウンロード" (download report), and "ノードアクション" (node actions). The main area is a table with columns: "ノード ID", "ノードの...", "ノード名", "プラット...", "オペレーター...", "ソースタイプ", and "ソースアーティ...", which is partially cut off. Three rows of data are visible:

ノード ID	ノードの...	ノード名	プラット...	オペレーター...	ソースタイプ	ソースアーティ...
i-04970a7f373ac630b	実行中	LaunchedByS...	Linux	Amazon Linux AMI	EC2 インスタンス	-
mi-0623bfeef040aa8...	-	On-perm-Linux	Linux	Amazon Linux	AWS::SSM::Manage...	-
i-016d04a4ae49531af	実行中	instance-ph@	Linux	Amazon Linux	EC2 インスタンス	-

マネージドノード：

- SSM 管理下のインスタンス群
- EC2 インスタンスのほか、
オンプレミスのサーバも
含まれられる。

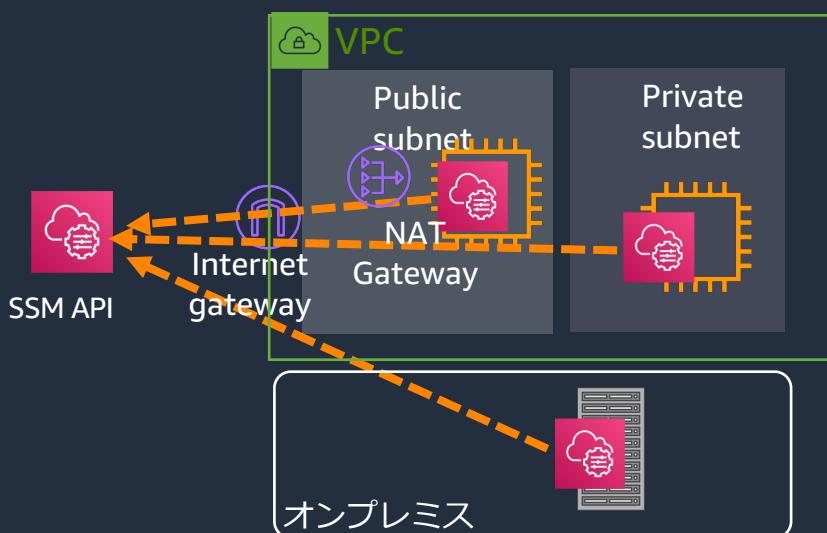
SSM でサポートされている EC2 以外のマシンタイプ

- オンプレミスサーバ
- 他のクラウド環境およびオンプレミスの仮想マシン
- エッジデバイス

① アウトバウンド経路の確保

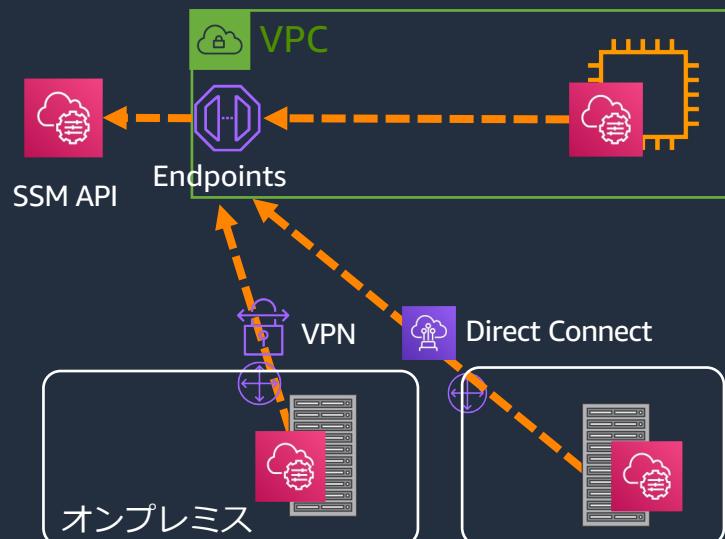
- 以下のいずれかのパターンで、SSM Agent からの HTTPS のアウトバウンド経路を確保
- インバウンドアクセスは不要

1. インターネット経由



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
- ・オンプレミスからも AWS Direct Connect や VPN 経由で閉域網経由のアクセスが可能



② IAM サービスロールの作成

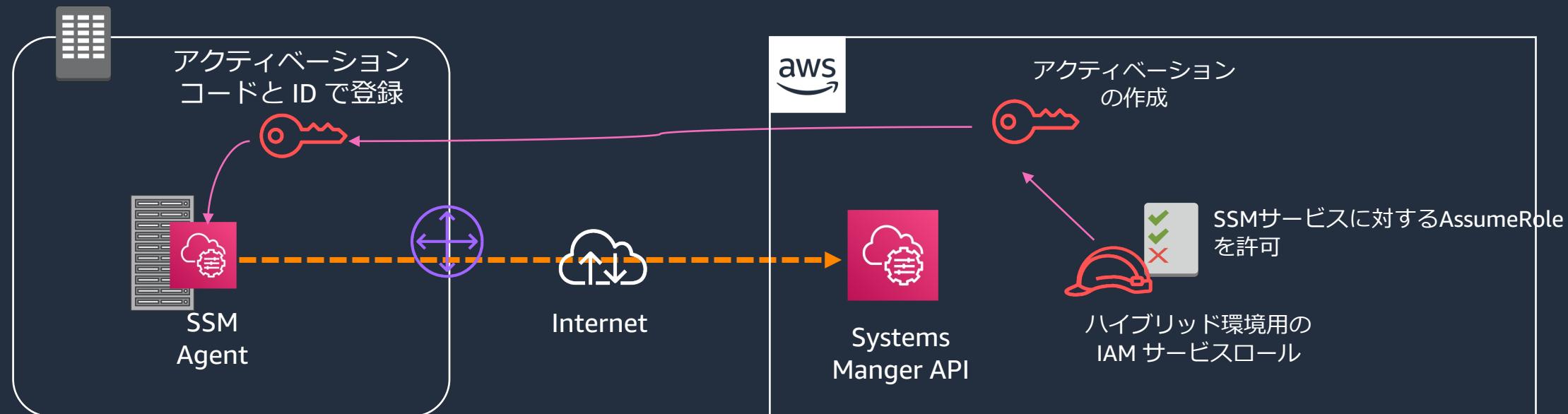
- マネージドノードが SSM と通信するために IAM サービスロールを作成
 1. 信頼できるエンティティに「Systems Manager」を選択 (必須)
 2. IAM ポリシーについては、まず「AmazonSSMManagedInstanceCore」でコア機能をアタッチ (必須)
 3. S3 などのポリシーをアタッチ (オプション)

IAM サービスロール作成の詳細は[こちら](#)

③ アクティベーション作成

1. アクティベーションコードとアクティベーション ID を生成
2. ハイブリッドノード(※)登録時に生成されたアクティベーションコードとアクティベーション ID を利用

※ ハイブリッドノードとは、オンプレミスサーバ、エッジデバイス、仮想マシンのことを指します。



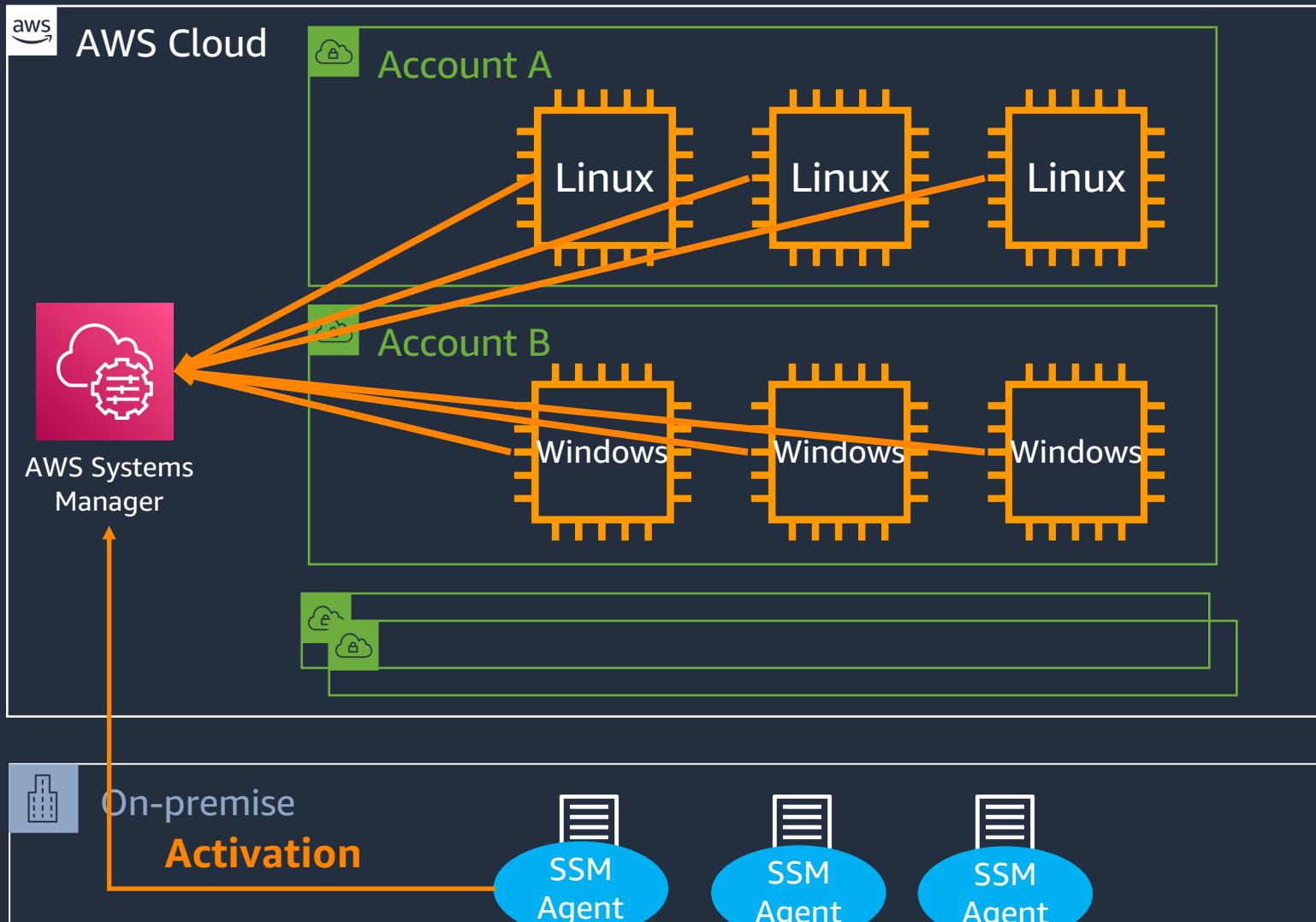
④ SSM Agent のインストールと登録

- ハイブリッドノードは、手動で SSM Agent をインストールし、マネージドノードとして SSM に登録する。

Linuxへのインストール手順は[こちら](#)、Windowsのインストール手順は[こちら](#)

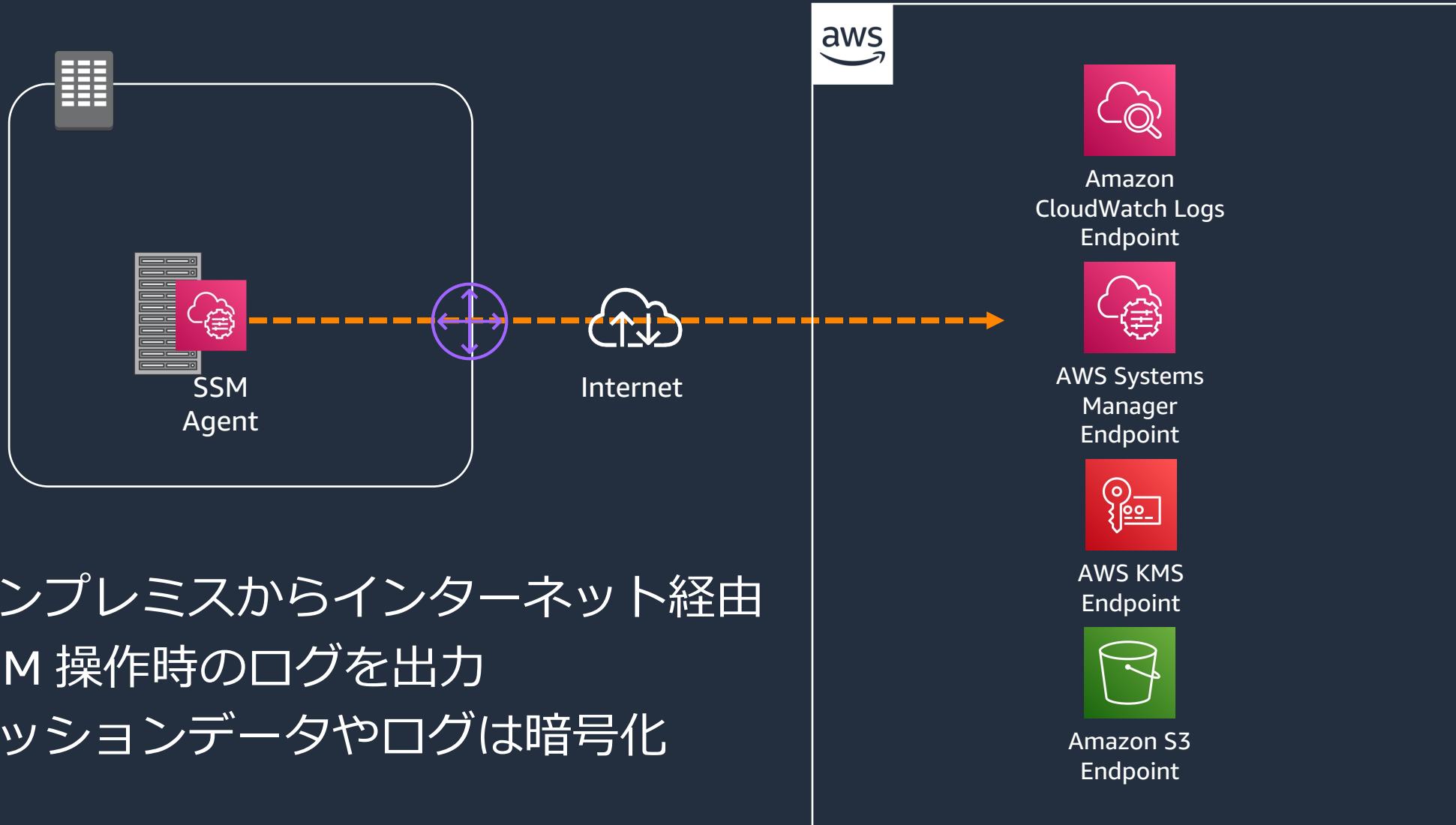


ここまでやれば、晴れてマネージドノードに！



具体的な構成手順とデモ

前提



- オンプレミスからインターネット経由
- SSM 操作時のログを出力
- セッションデータやログは暗号化

【ご参考】閉域網での構成例

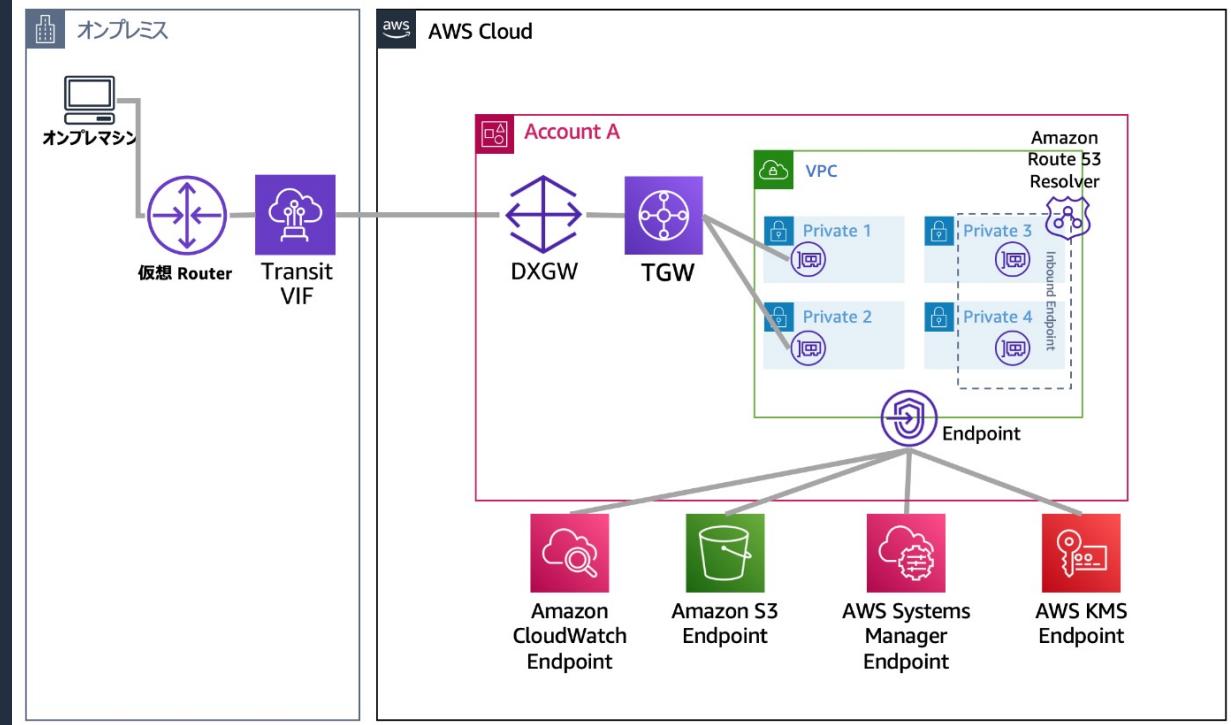
Amazon Web Services ブログ

ハイブリッド環境の運用・監視の実現 – 閉域網で AWS Systems Manager と Amazon CloudWatch を構成する

by Kyosuke Murata | on 26 7月 2022 | in [Amazon CloudWatch](#), [AWS Systems Manager](#), [Hybrid Cloud Management](#), [Management & Governance](#) | [Permalink](#) | [Share](#)

こんにちは。ソリューションアーキテクトの村田と申します。

昨今オンプレミスとクラウドを併用した環境が多く、運用・監視の仕組みを集約したいと考えたことはないでしょうか。私がソリューションアーキテクトとして仕事をさせて頂く中で、オンプレミスサーバを AWS の仕組みで運用・監視する場合の構成方法についてお客様からご相談頂くことがあります。オンプレミスと AWS は閉域網で接続したいというご要望を頂くことがあります。2022年7月時点できました情報が公開されていないため、このブログでは閉域接続のオンプレミスサーバを [AWS Systems Manager](#) と [Amazon CloudWatch](#) で運用・監視するための構成方法について詳しくご紹介します。



閉域網での構成例について記載したブログは[こちら](#)

手順 1. インターネットへの疎通確認

Ubuntu Server 20.04 LTS の場合

インターネット向けの HTTPS アクセスができることの確認

```
$ curl https://checkip.amazonaws.com/
```

SSM の各種エンドポイントと通信プロトコルについては[こちら](#)

手順 2-1. IAM サービスロールの作成

IAM > ロール > ロールを作成

ステップ 1
信頼されたエンティティを選択

ステップ 2
許可を追加

ステップ 3
名前、確認、および作成

信頼されたエンティティを選択 情報

信頼されたエンティティタイプ

- AWS のサービス
EC2、Lambda、その他の AWS サービスが、このアカウントでアクションを実行することを許可します。
- AWS アカウント
お客様またはサードパーティに属する他の AWS アカウントのエンティティが、このアカウントでアクションを実行することを許可します。
- ウェブアイデンティティ
指定された外部ウェブアイデンティティ プロバイダーによってフェデレーションされたユーザーが、このロールを引き受け、このアカウントでアクションを実行することを許可します。
- SAML 2.0 フェデレーション
会社のディレクトリから SAML 2.0 を使用してフェデレーションされたユーザーが、このアカウントでアクションを実行することを許可します。
- カスタム信頼ポリシー
カスタム信頼ポリシーを作成して、他のユーザーがこのアカウントでアクションを実行できるようにします。

ユースケース

EC2、Lambda、その他の AWS のサービスがこのアカウントでアクションを実行することを許可します。

一般的なユースケース

- EC2
Allows EC2 instances to call AWS services on your behalf.
- Lambda
Allows Lambda functions to call AWS services on your behalf.

他の AWS のサービスのユースケース:

- Systems Manager
- Systems Manager
Allows SSM to call AWS services on your behalf
- Systems Manager - Inventory and Maintenance Windows
Allow AWS Systems Manager to call AWS resources on your behalf.

キャンセル 次へ

手順 2-2. IAM サービスロールの作成

The screenshot shows the AWS IAM service role configuration page. At the top, it displays the ARN: arn:aws:iam::[REDACTED]:role/BB_Hybrid_Activation and the maximum session duration: 1 hour. Below this, there are tabs for Permissions, Trust Relationships, Tags, Access Advisor, and Session Tokens. The Permissions tab is selected, showing four attached policies: CloudWatchAgentServerPolicy, AmazonSSMManagedInstanceCore, bb_hybrid_activations_kms, and bb_hybrid_activations_s3_access. The last two policies are highlighted with an orange border.

Amazon CloudWatch Logs へのセッションデータのログ記録と暗号化については[こちら](#)

Amazon S3 へのセッションデータをログ記録と暗号化については[こちら](#)

Session Manager のセッションデータ暗号化については[こちら](#)

Session Manager、S3 や CloudWatch Logs の暗号化を利用する場合、適したポリシーを IAM サービスロールにアタッチする必要があります。

今回の構成では、セッションデータやログの暗号化を行っています。

手順 3-1. アクティベーションの作成

The screenshot shows the AWS Systems Manager console. On the left, there's a sidebar with navigation links for Change Management and Node Management, with 'Hybrid Applications' highlighted in orange. The main content area has a title 'AWS Systems Manager のアクティベーション ハイブリッド環境の一元管理' and a description about registering on-premises servers or devices. A prominent orange button labeled 'アクティベーションを作成する' is highlighted with a red border.

▼ 変更管理

Change Manager
オートメーション
Change Calendar
メンテナンスウィンドウ

▼ ノード管理

フリートマネージャー
コンプライアンス
インベントリ
ハイブリッドアクティベーション

マネジメント

AWS Systems Manager のアクティベーション ハイブリッド環境の一元管理

オンプレミスのサーバーまたはデバイスの登録

アクティベーションを作成する

手順 3-2. アクティベーションの作成

AWS Systems Manager > アクティベーション > アクティベーションの作成

アクティベーションの作成

アクティベーション設定
新しいアクティベーションを作成します。アクティベーションの完了後、アクティベーションコードと ID が送信されます。このコードと ID を使用して SSM エージェントをハイブリッドおよびオンプレミスのサーバー、または仮想マシンに登録してください。[詳細情報はこちらをご覧ください](#)

アクティベーションの説明- オプション
最大 256 文字です。

インスタンス制限
AWS に登録するサーバーと VM の合計数を指定します。

1

IAM ロール
マネージドインスタンス上の SSM エージェントと AWS の間での通信を有効にするには、IAM ロールを指定します

システムによって作成されたデフォルトのロール
(AmazonEC2RunCommandRoleForManagedInstances) を使用する

必要な許可を持つ既存のカスタム IAM ロールを選択する

① このオプションを選択すると、AWS はユーザーが指定している既存のロールを使用します。ロールには必要な許可を持たせておく必要があります。許可がない場合、コマンドの実行に失敗します。[詳細情報はこちらをご覧ください](#)

BB_Hybrid_Activation

アクティベーションの有効期限
この日付はアクティベーションの有効期限が切れる日付を指定します。有効期限日後に追加のマネージドインスタンスを登録したい場合は、新しいアクティベーションを作成する必要があります。この有効期限日は、既に登録済みで実行中のインスタンスには影響しません。

2023-04-27T12:00+09:00

有効期限日は、今日から 30 日以内の日付に設定してください

デフォルトのインスタンス名- オプション
このマネージドインスタンスがコントロールされるとき、または List API を呼び出すときに、このマネージドインスタンスの特定に役立つ名前を指定します。

最大 256 文字です。

キャンセル アクティベーションの作成

設定項目	内容
アクティベーションの説明 (オプション)	このアクティベーションの説明を入力
インスタンス制限	このアクティベーションで登録するノードの合計数 ※ デフォルト値は 1 インスタンス
IAM ロール	事前に作成した IAM サービスロールを選択 ※ デフォルトはシステムによって作成されたデフォルトのロール
アクティベーション有効期限	アクティベーションが期限切れになる時間を指定 (例 : 2023-04-27T12:00+09:00) ※ 有効期限は将来の日付で 30 日以内で入力、デフォルト値は 24 時間
デフォルトのインスタンス名 (オプション)	このアクティベーションで関連付けられる全てのノードに表示する識別名 (ノード名に表示される。指定しないと “-” となる。)

② 新しいアクティベーションが正常に作成されました。アクティベーションコードを以下に記載します。このコードに再度アクセスすることはできないため、コードをコピーして安全な場所に保存してください。

Activation Code



Activation ID 255996e5-f42d-44c8-8fb8-eb17f76696bc

これで、amazon-ssm-agent をインストールして、Run Command でインスタンスを管理できるようになりました。 [詳細情報はこちらをご覧ください](#)

手順 4. SSM Agent インストール

Ubuntu Server 20.04 LTS の場合 (.deb パッケージ使用)

```
$ mkdir /tmp/ssm
```

```
$ curl https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/debian_amd64/amazon-ssm-agent.deb -o /tmp/ssm/amazon-ssm-agent.deb
```

```
$ sudo dpkg -i /tmp/ssm/amazon-ssm-agent.deb
```

```
$ sudo service amazon-ssm-agent stop
```

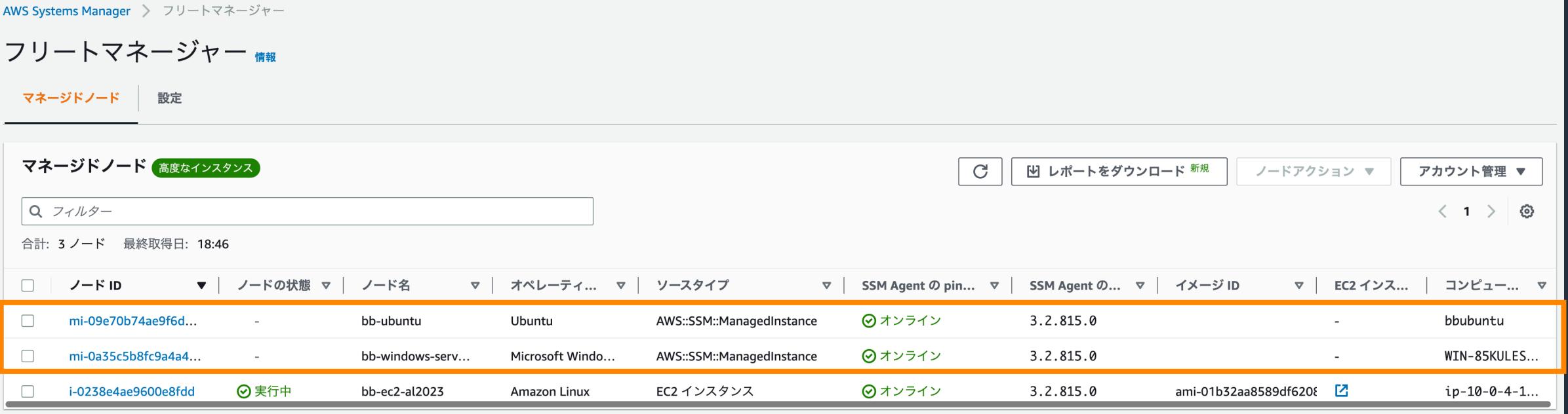
```
$ sudo -E amazon-ssm-agent -register -code "activation-code" -id "activation-id" -region "region"
```

```
$ sudo service amazon-ssm-agent start
```

※ Linuxへのインストール手順は[こちら](#)、Windowsのインストール手順は[こちら](#)



晴れてマネージドノードに

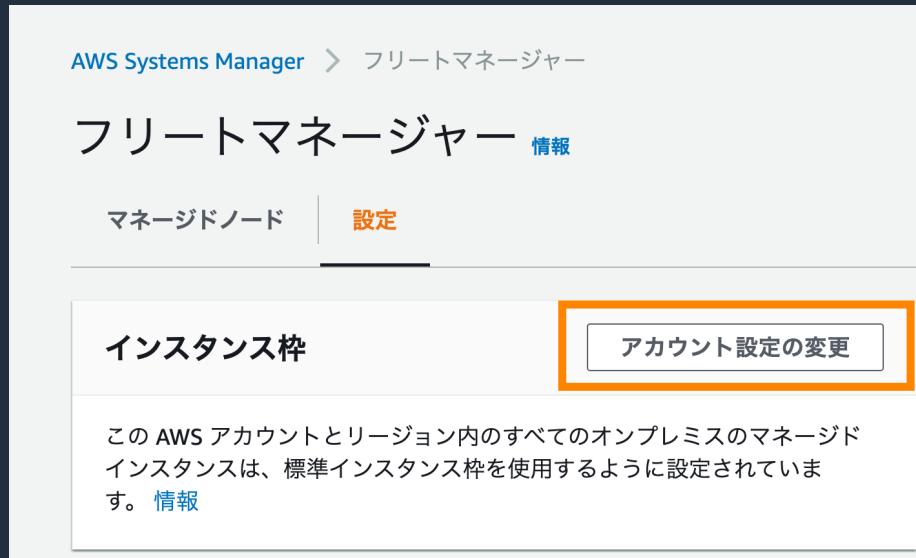


The screenshot shows the AWS Systems Manager Fleet Manager interface. The top navigation bar includes 'AWS Systems Manager' and 'フリートマネージャー'. Below it, the title 'フリートマネージャー' has a '情報' link. The main section is titled 'マネージドノード' with a '高度なインスタンス' button. The table lists three nodes:

ノード ID	ノードの状態	ノード名	オペレーティ...	ソースタイプ	SSM Agent の pin...	SSM Agent の...	イメージ ID	EC2 インス...	コンピュー...
mi-09e70b74ae9f6d...	-	bb-ubuntu	Ubuntu	AWS::SSM::ManagedInstance	オンライン	3.2.815.0	-	-	bbubuntu
mi-0a35c5b8fc9a4a4...	-	bb-windows-serv...	Microsoft Windo...	AWS::SSM::ManagedInstance	オンライン	3.2.815.0	-	-	WIN-85KULES...
i-0238e4ae9600e8fdd	実行中	bb-ec2-al2023	Amazon Linux	EC2 インスタンス	オンライン	3.2.815.0	ami-01b32aa8589df620e	ip-10-0-4-1...	

- ハイブリッドノードの Fleet Manager への表示のされ方
 - ノード ID は “mi-” から始まる
 - ソースタイプは “AWS::SSM::ManagedInstance”
 - ノード名の列は “アクティベーション時の入力値” (ホスト名はコンピュータ名の列)

手順 5. インスタンス枠を変更（オプション）



- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
 - アカウント毎にリージョンあたり 1,000 を越えるハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を登録
 - ハイブリッドノードに接続するために Session Manager を使用
 - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

手順 5. インスタンス枠を変更（オプション）



- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
 - アカウント毎にリージョンあたり 1,000 を越えるハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を登録
 - ハイブリッドノードに接続するために Session Manager を使用
 - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

手順 5. インスタンス枠を変更（オプション）

The screenshot shows the AWS Systems Manager Fleet Manager interface. On the left, there's a sidebar with 'AWS Systems Manager > フリートマネージャー' and tabs for 'マネージドノード' (selected) and '設定'. The main content area has a title '標準層から高度な層への変更を確認' (Confirm migration from standard layer to advanced layer). It contains text about the action changing instance types to advanced ones, mentioning session manager and EC2 instances, and a note about regional limits. A checkbox is checked for 'アカウントとリージョン内のすべてのオンプレミスのインスタンス (または Systems Manager Session Manager を使用する Amazon EC2 インスタンス) を高度なインスタンスに変更する' (Change all on-premises instances (or Amazon EC2 instances using Systems Manager Session Manager) in the account and region to advanced instances). The 'マネージドノード' tab is highlighted with an orange border.

AWS Systems Manager > フリートマネージャー

標準層から高度な層への変更を確認

このアクションにより、高度なインスタンス枠が現在の AWS アカウントおよびリージョンは、スタンダードインスタンスで設定されている 1,000 のインスタンス制限を超えると、Systems Manager セッションマネージャーを使用してオンラインで変更できます。セッションマネージャーを使用すると、インスタンスへのインテラクティブ接続もできます。セッションマネージャーを使用すると、インスタンスへのインテラクティブ接続もできます。

アドバンスドインスタンスは、従量料金にて利用可能です。詳細については、[AWS ドキュメント](#)をご覧ください。

この設定を変更すると、現在のアカウントとリージョンのすべての標準インスタンスを高度なインスタンスに変更します。この操作には、アカウントとリージョンのすべての標準インスタンスを高度なインスタンスに変更する権限が必要です。詳細は[こちら](#)を参照してください。

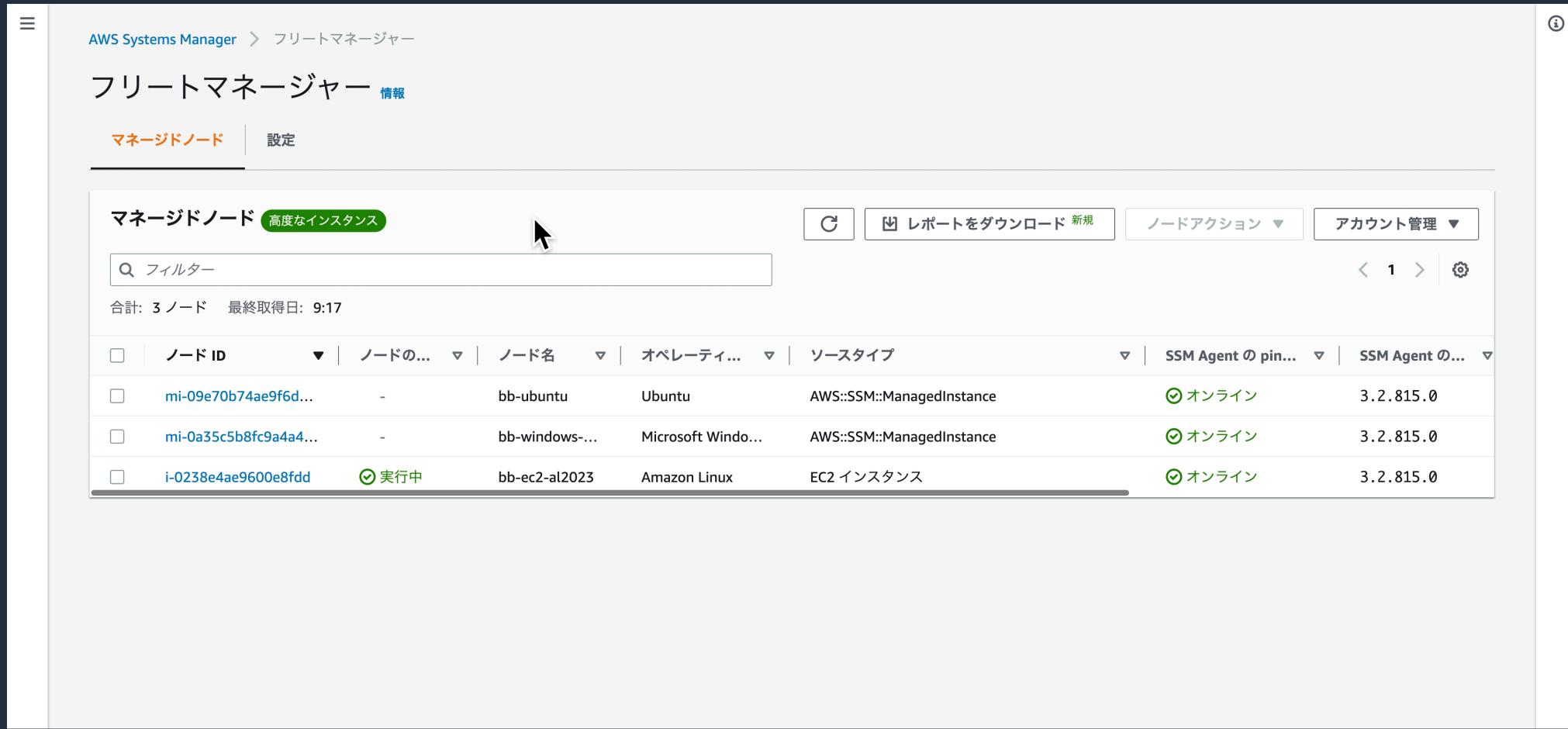
アカウントとリージョン内のすべてのオンプレミスのインスタンス (または Systems Manager Session Manager を使用する Amazon EC2 インスタンス) を高度なインスタンスに変更する

マネージドノード 情報 設定

マネージドノード 高度なインスタンス

- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
 - アカウント毎にリージョンあたり 1,000 を越えるハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を登録
 - ハイブリッドノードに接続するために Session Manager を使用
 - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

デモ 1



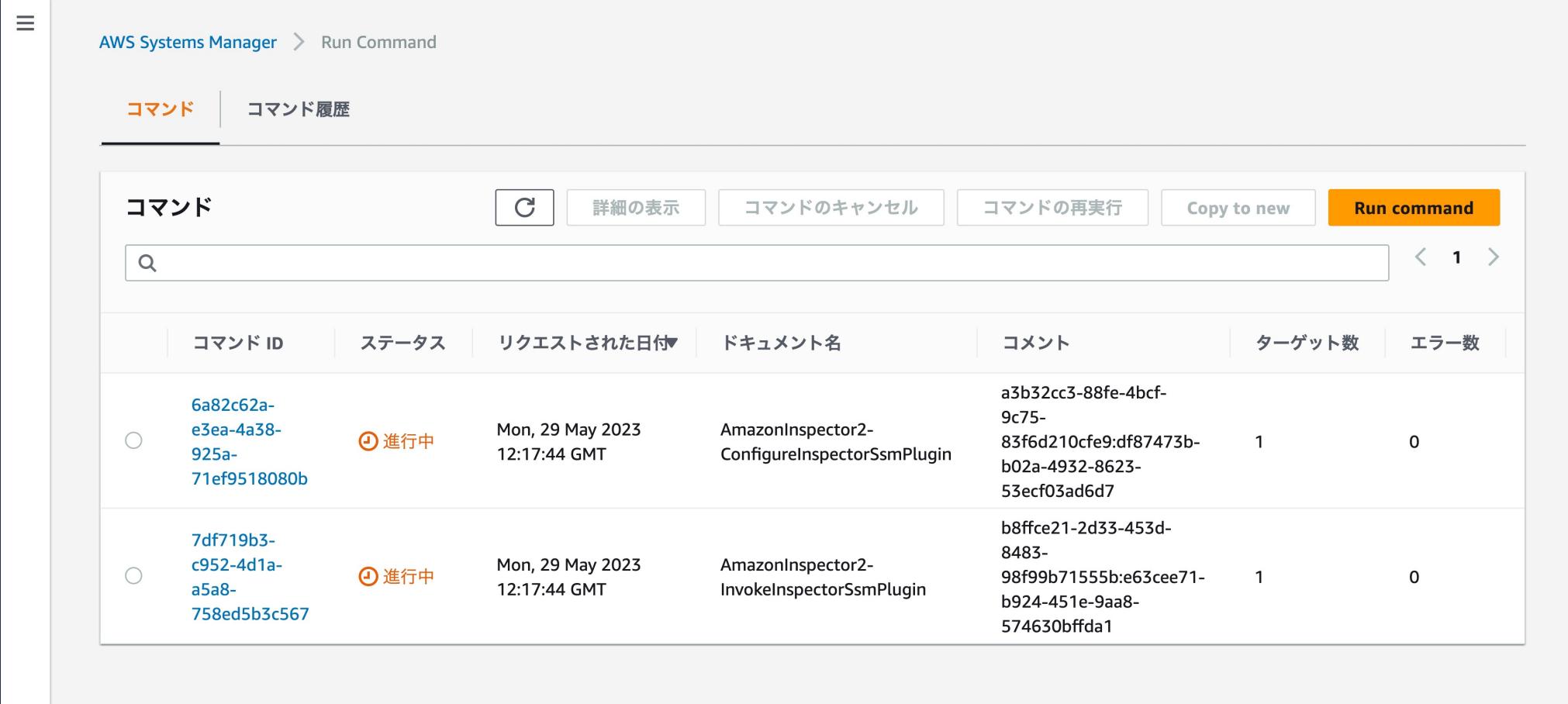
The screenshot shows the AWS Systems Manager Fleet Manager interface. The top navigation bar includes the AWS logo, account information, and a search bar. The main header reads "AWS Systems Manager > フリートマネージャー" and the sub-header "フリートマネージャー 情報". Below this, there are two tabs: "マネージドノード" (selected) and "設定". A sub-header "マネージドノード 高度なインスタンス" is displayed above the table.

The table lists three managed nodes:

ノード ID	ノードの状態	ノード名	オペレーティングシステム	ソースタイプ	SSM Agent の状態	SSM Agent のバージョン
mi-09e70b74ae9f6d...	-	bb-ubuntu	Ubuntu	AWS::SSM::ManagedInstance	オンライン	3.2.815.0
mi-0a35c5b8fc9a4a4...	-	bb-windows-...	Microsoft Windo...	AWS::SSM::ManagedInstance	オンライン	3.2.815.0
i-0238e4ae9600e8fdd	実行中	bb-ec2-al2023	Amazon Linux	EC2 インスタンス	オンライン	3.2.815.0

Table controls include a refresh button, a "Report to Download" button, and buttons for "Node Actions" and "Account Management". A search bar labeled "フィルター" is also present.

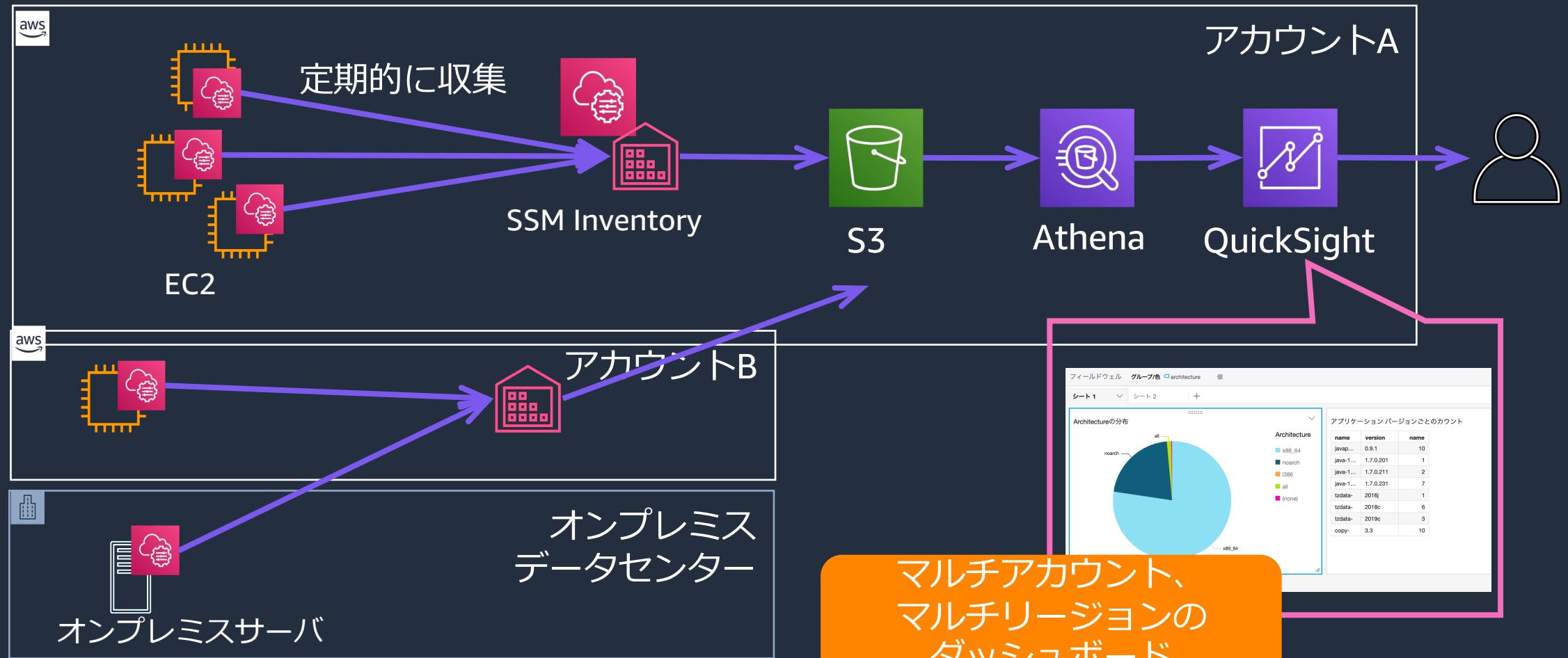
デモ 2



The screenshot shows the AWS Systems Manager Run Command page. At the top, there are tabs for "コマンド" (Command) and "コマンド履歴" (Command History), with "コマンド" being the active tab. Below the tabs is a search bar and a toolbar with buttons for "C" (Cancel), "詳細の表示" (Detailed View), "コマンドのキャンセル" (Cancel Command), "コマンドの再実行" (Re-run Command), "Copy to new" (Copy to New), and "Run command" (Run Command). The main area displays a table of command executions:

コマンド ID	ステータス	リクエストされた日付	ドキュメント名	コメント	ターゲット数	エラー数
6a82c62a-e3ea-4a38-925a-71ef9518080b	① 進行中	Mon, 29 May 2023 12:17:44 GMT	AmazonInspector2-ConfigureInspectorSsmPlugin	a3b32cc3-88fe-4bcf-9c75-83f6d210cfe9:df87473b-b02a-4932-8623-53ecf03ad6d7	1	0
7df719b3-c952-4d1a-a5a8-758ed5b3c567	① 進行中	Mon, 29 May 2023 12:17:44 GMT	AmazonInspector2-InvokeInspectorSsmPlugin	b8ffce21-2d33-453d-8483-98f99b71555b:e63cee71-b924-451e-9aa8-574630bffda1	1	0

【ご参考】Inventory の活用例： マルチアカウント/マルチリージョンのダッシュボードの作成



詳細はこちらの[チュートリアル](#)参照

「チュートリアル: リソースデータの同期を使用してインベントリデータを集約する」

SSM Hybrid Activations の料金

Hybrid Activations の料金

- アカウント毎にリージョンあたり 1,000 のハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を追加料金なしで登録可能
- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
 - 1,000 を越えるハイブリッドノードを登録
 - ハイブリッドノードに接続するために Session Manager を使用
 - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

インスタンスティア	料金
スタンダード	追加料金無し アカウントごとにリージョンあたり最大 1,000 までの制限
アドバンスド	Systems Manager Hybrid Activations を使用して登録されたノードごとに時間あたり 0.00695 USD 無料利用枠なし

【参考】

インスタンス層の設定

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-managed-instances-tiers.html

AWS Systems Manager の料金

<https://aws.amazon.com/jp/systems-manager/pricing/>



計算例

アカウント A でインスタンスティアをスタンダードで 500 のオンプレミスサーバを登録、
アカウント B でインスタンスティアをアドバンスドで 1,500 のオンプレミスサーバを登録し、
10 日間経過しているとします。

アカウント	インスタンスティア	管理台数	料金
A	スタンダード	オンプレミス サーバ 500 台	請求無し
B	アドバンスド	オンプレミス サーバ 1,500 台	$1,500 \text{ (台)} * 0.00695 \text{ USD (/時間)} * 10 \text{ (日)} * 24 \text{ (時間)} = 2,502 \text{ USD}$

【参考】

AWS Systems Manager の料金

<https://aws.amazon.com/jp/systems-manager/pricing/>

まとめ



まとめ

- SSM は EC2 インスタンスはもちろん、ハイブリッドノード（AWS 以外の仮想マシン、オンプレミスサーバー、さらにはエッジデバイス）を管理可能
- アクティベーションは、ハイブリッドノードをマネージドノードとして登録する際に利用する機能

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!



AWS Systems Manager

Incident Manager 編

AWS Black Belt Online Seminar

上野 涼平

Solutions Architect
2023/04

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 4 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：上野 涼平

所属：ソリューションアーキテクト

経歴：AWS ユーザーの立場で、オンプレミスからの移行、AWS 環境の運用改善



好きなAWSサービス：AWS Systems Manager



本セミナーの対象者

- AWS の運用をされている方、これから運用される予定の方
- インシデント管理に携わる方

本セミナーの目的

- AWS Systems Manager Incident Manager の機能とユースケースをご理解いただく

本日お話ししないこと

- AWS Systems Manager の全体像
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager Incident Manager 以外の機能の詳細
→ 今後公開を予定している、各機能にフォーカスしたセッションをお待ちください！

アジェンダ

1. AWS Systems Manager の概要
2. Incident Manager とは
3. Incident Manager を使ったインシデント管理方法
4. その他機能・Tips
5. 料金
6. まとめ

AWS Systems Manager の概要

AWS Systems Manager

ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション



AWS Config

Configuration history



Amazon EventBridge

Notification and remediation



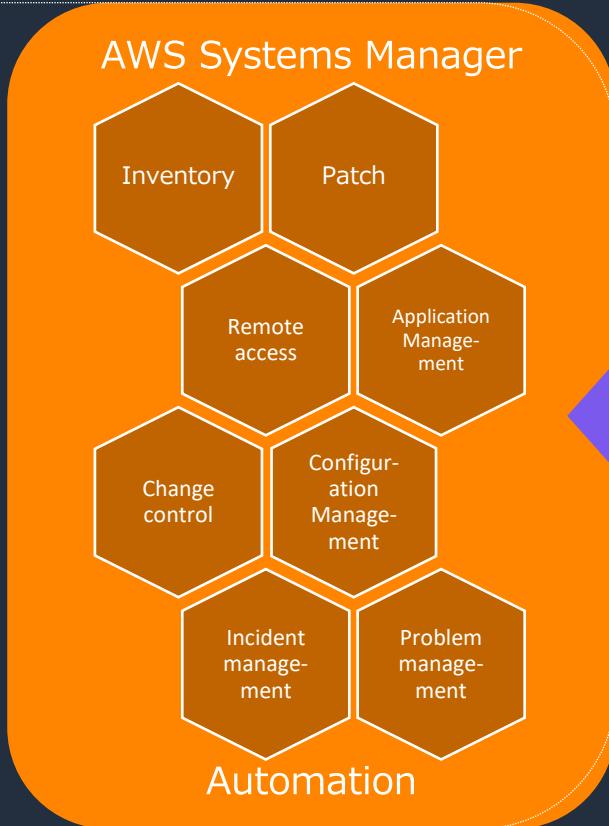
AWS CloudTrail

Audited actions



AWS Identity and Access Management (IAM)

Role-based access control



(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

運用管理

-  Explorer
-  OpsCenter
-  Incident Manager

アプリケーション管理

-  Application Manager
-  AppConfig
-  Parameter Store

変更管理

-  Change Manager
-  Automation
-  Maintenance Windows
-  Change Calendar

ノード管理

-  Fleet Manager
-  Session Manager
-  Inventory
-  Run Command
-  Patch Manager
-  Distributor
-  State Manager

Quick Setup

AWS Systems Manager の機能

運用管理

 Explorer

 OpsCenter

 Incident Manager

アプリケーション管理

 Application Manager

 AppConfig

 Parameter Store

変更管理

 Change Manager

 Automation

 Maintenance Windows

 Change Calendar

ノード管理

 Fleet Manager

 Session Manager

 Inventory

 Run Command

 Patch Manager

 Distributor

 State Manager

Quick Setup

Incident Manager とは

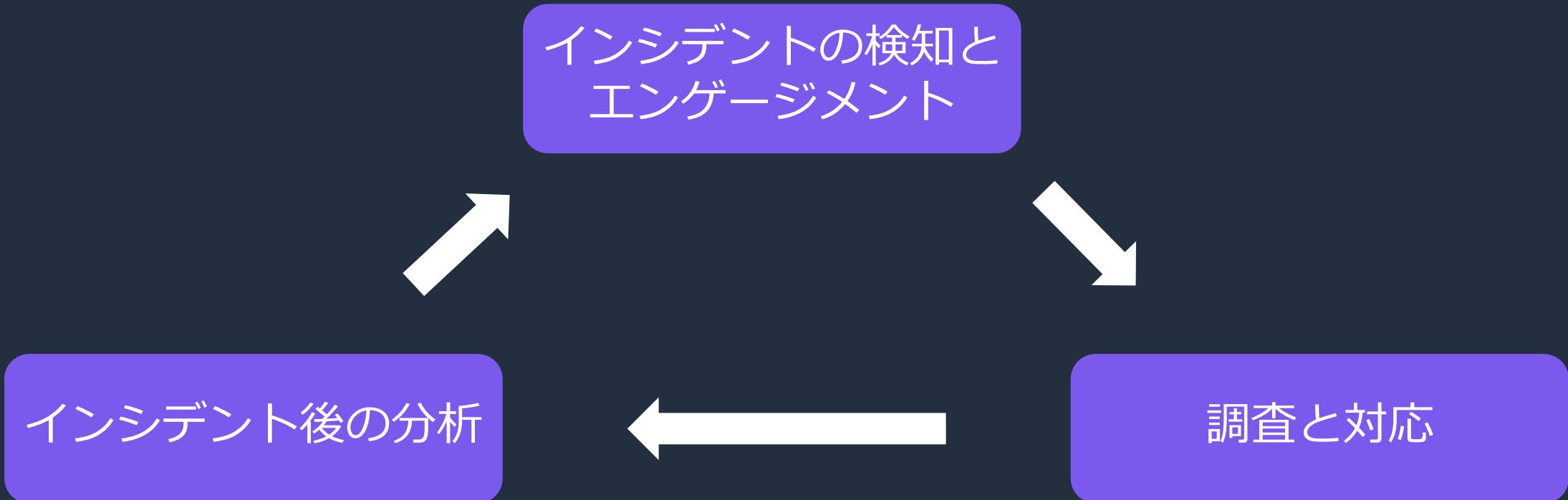
インシデントとは？

インシデントとは
サービスにおける**計画外の中斷や**
サービス品質の低下をもたらすもの

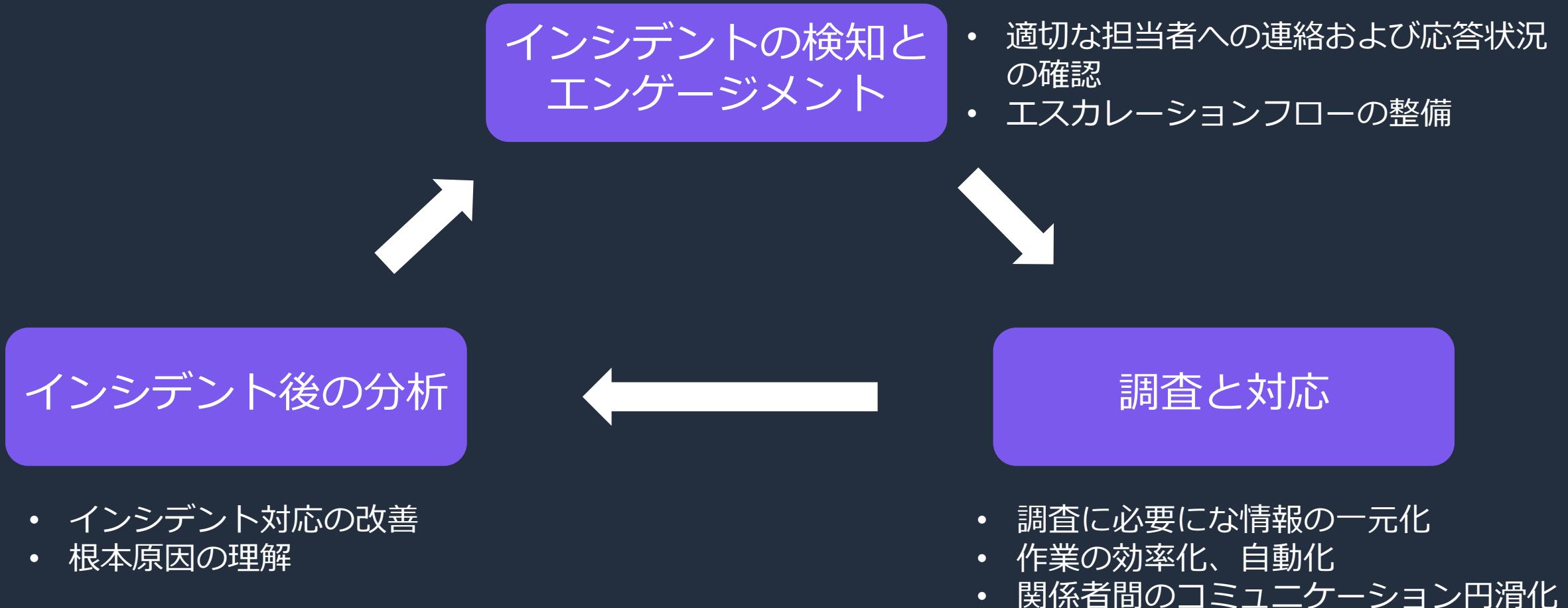
AWS 公式ドキュメント: AWS Systems Manager Incident Manager とは? より抜粋

https://docs.aws.amazon.com/ja_jp/incident-manager/latest/userguide/what-is-incident-manager.html

インシデントのハンドリング



インシデントのハンドリング

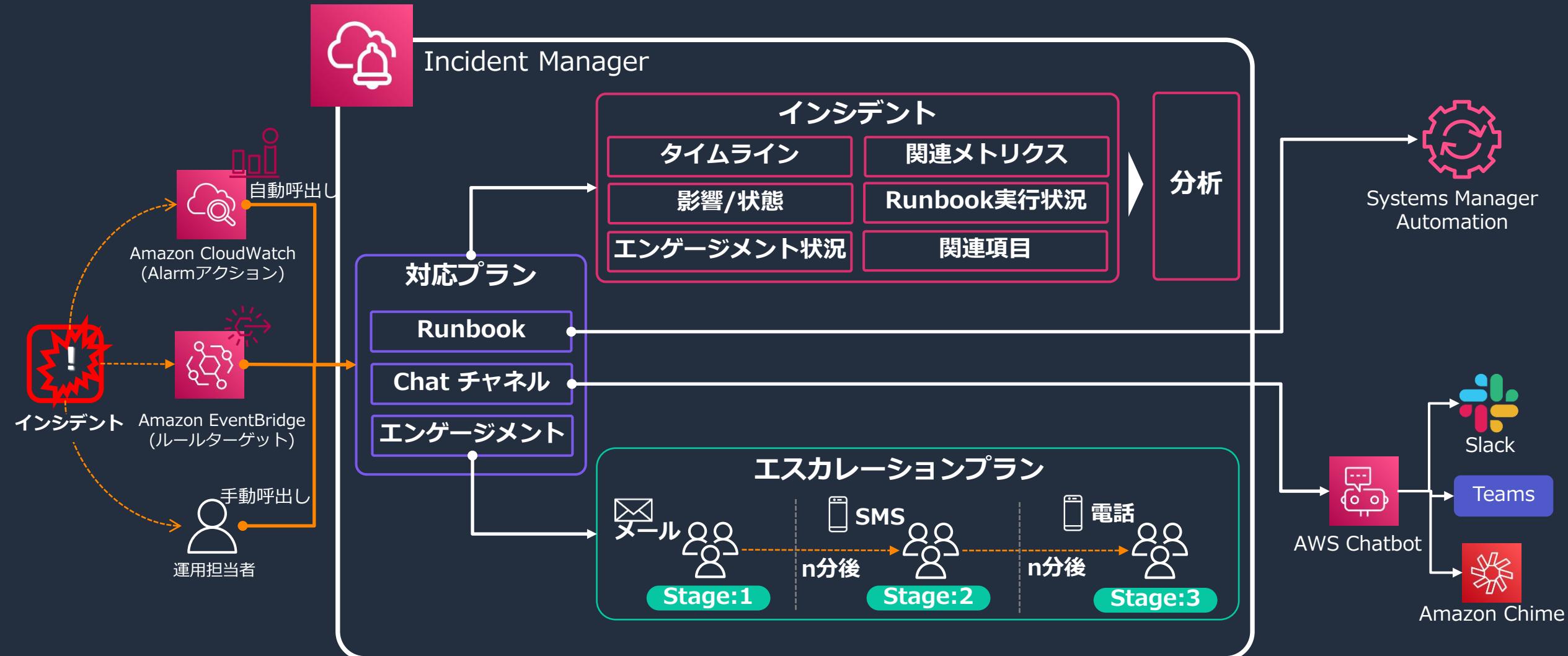


Incident Manager とは



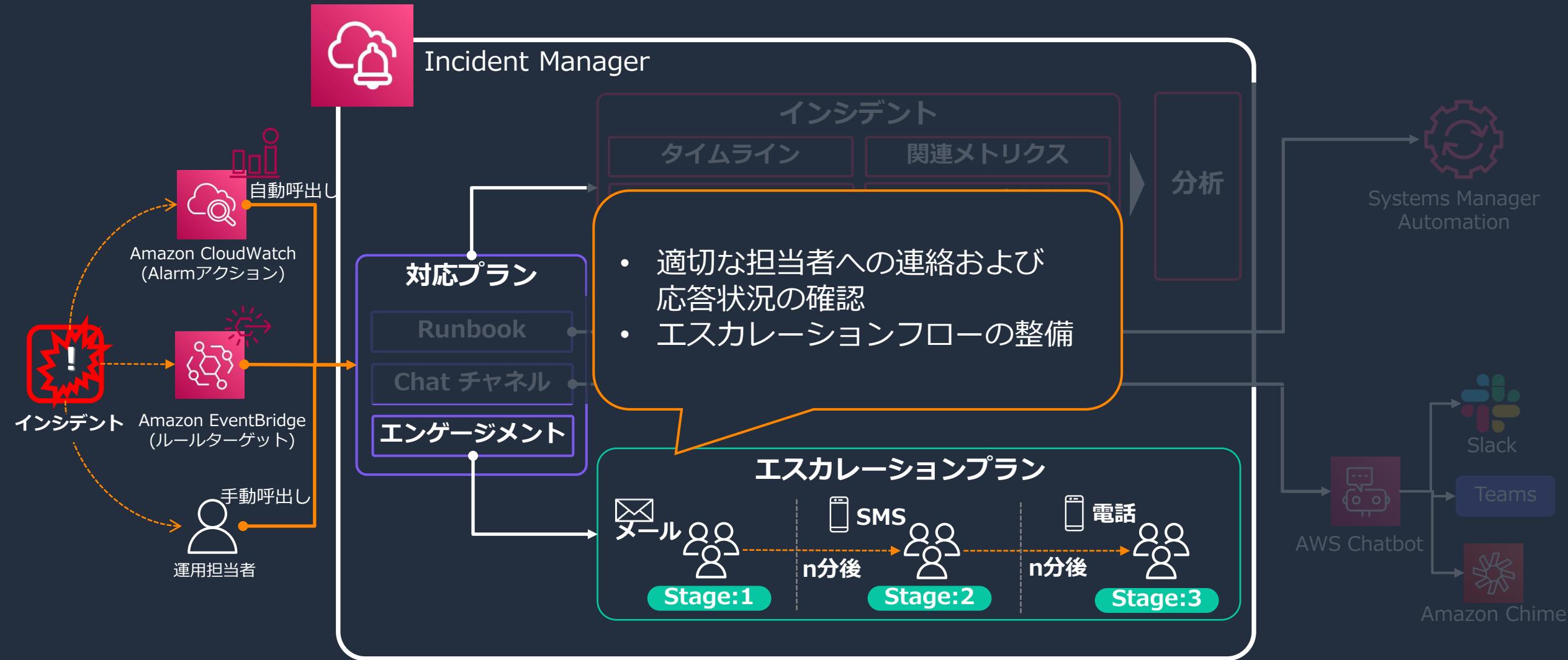
インシデントの解決、影響を軽減するまでの
時間を短縮させるための機能

Incident Manager 全体図



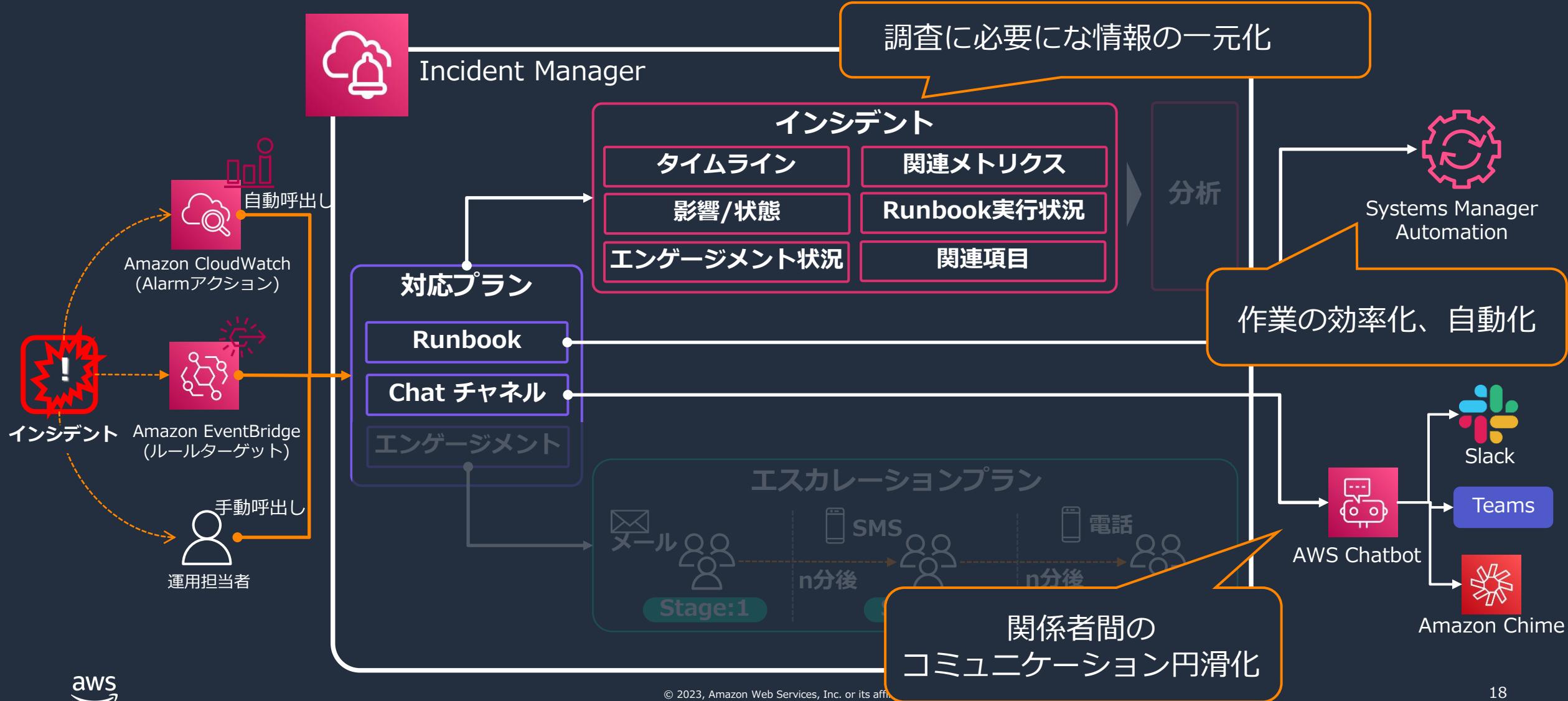
Incident Manager 全体図

インシデントの検知と
エンゲージメント



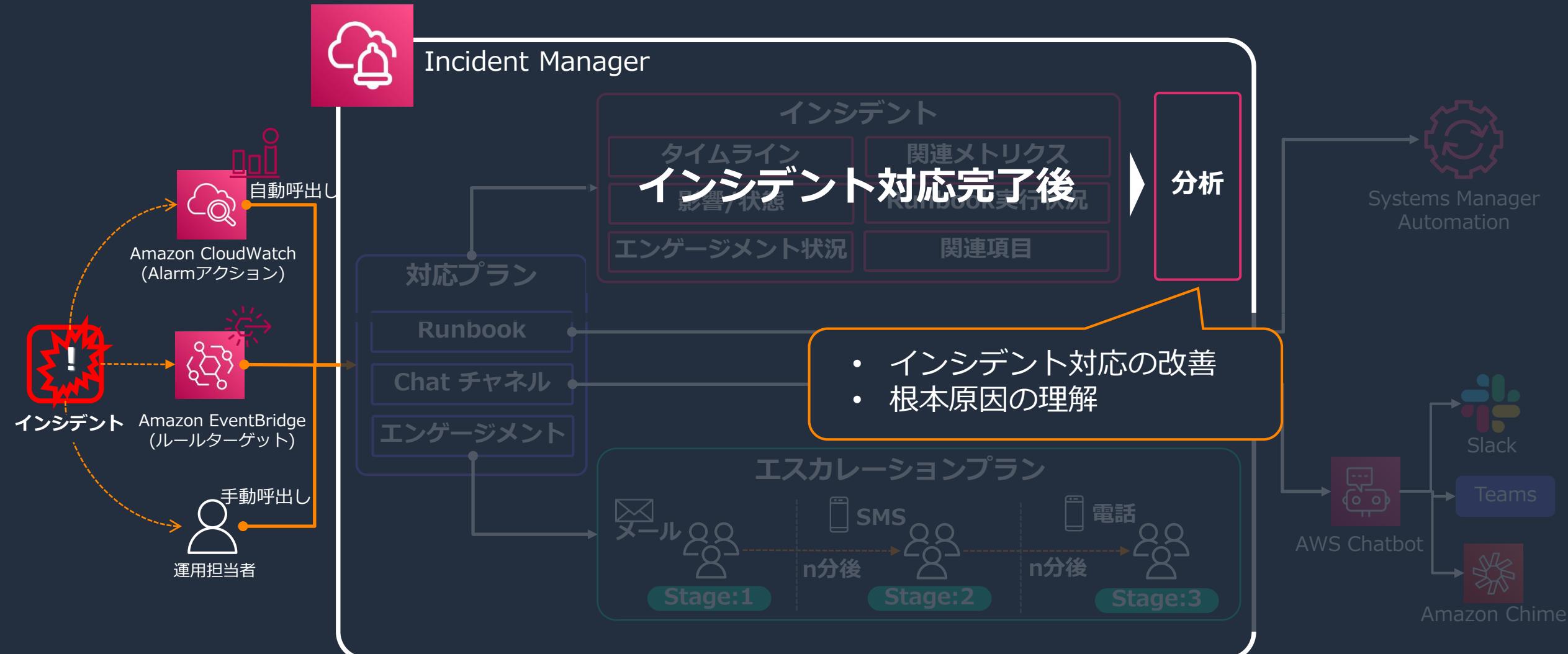
Incident Manager 全体図

調査と対応



Incident Manager 全体図

インシデント後の分析



Incident Manager を使った インシデント管理办法

Incident Manager 関連リソース

連絡先

- ・ インシデント発生時の連絡先
- ・ E メール、SMS、音声(電話)による連絡が可能

エスカレーションプラン

- ・ エスカレーションパス
- ・ 輪番コールのように連絡先の応答有無に応じて次の連絡先へ連絡を行う

オンコールスケジュール

- ・ インシデント時の連絡先ローテーションや連絡を行うスケジュールの設定
- ・ 日、週、月の単位でローテーションが可能

チャットチャネル

- ・ インシデントの更新と通知をチャットチャネルに連携可能
- ・ Slack、Teams、Amazon Chimeに対応

Runbook

- ・ インシデント対応に必要な手順書の役割を持つ（手動ステップ）
- ・ アプリケーションおよびインフラストラクチャタスクを自動化することも可能

対応プラン

- ・ 連絡先、エスカレーションプラン、オンコールスケジュール、チャットチャネル、Runbookをまとめたものの
- ・ インシデント発生時は関連する対応プランが呼び出される

New!

連絡先 - 連絡先チャネル -

連絡先チャネル

連絡先チャネルは、Incident Manager が連絡先をエンゲージするために使用できる方法です。連絡先チャネルを使用して、エンゲージメントプランを定義し、連絡先をエンゲージします。

タイプ	チャネル名	詳細	
E メール	email	incident@example.com	削除
SMS	SMS	+819999999	削除
音声	phone	+819999999	削除

[連絡先チャネルを追加](#)



- E メール、SMS、音声(電話)から選択可能
- 一つの連絡先に複数の連絡先チャネルを設定可能

連絡先 - エンゲージメントプラン -

エンゲージメントプラン

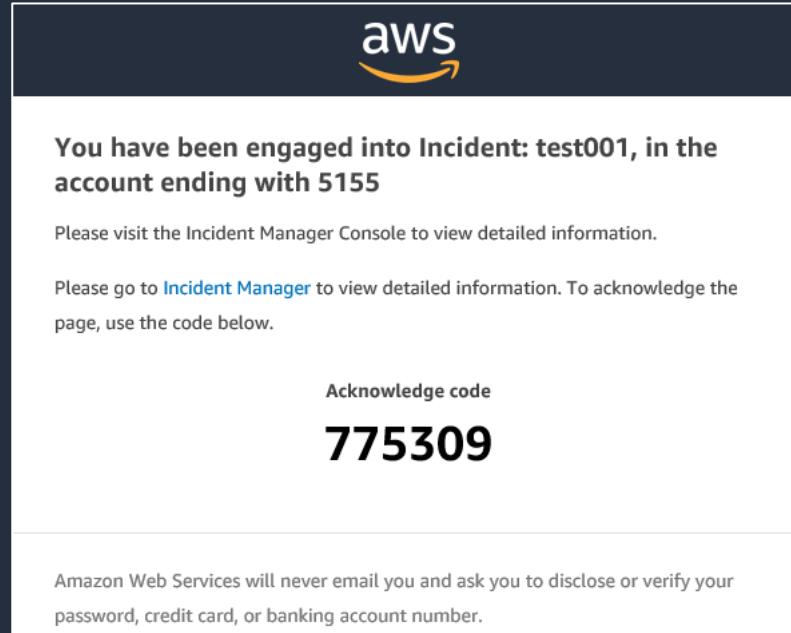
連絡先チャネル名	エンゲージメント時間 (分)	
email	0	削除
	ステージ開始後の時間 (分)。	
SMS	1	削除
	ステージ開始後の時間 (分)。	
phone	0	削除
	ステージ開始後の時間 (分)。	

エンゲージメントを追加

- 連絡先チャネルごとに連絡が来るタイミングを設定可能
- 図の設定は、E メールと音声通知が即座に行われ、1分後に SMSでの連絡も行われる例

連絡先 - エンゲージメント例 -

E メール



SMS※



音声(電話)



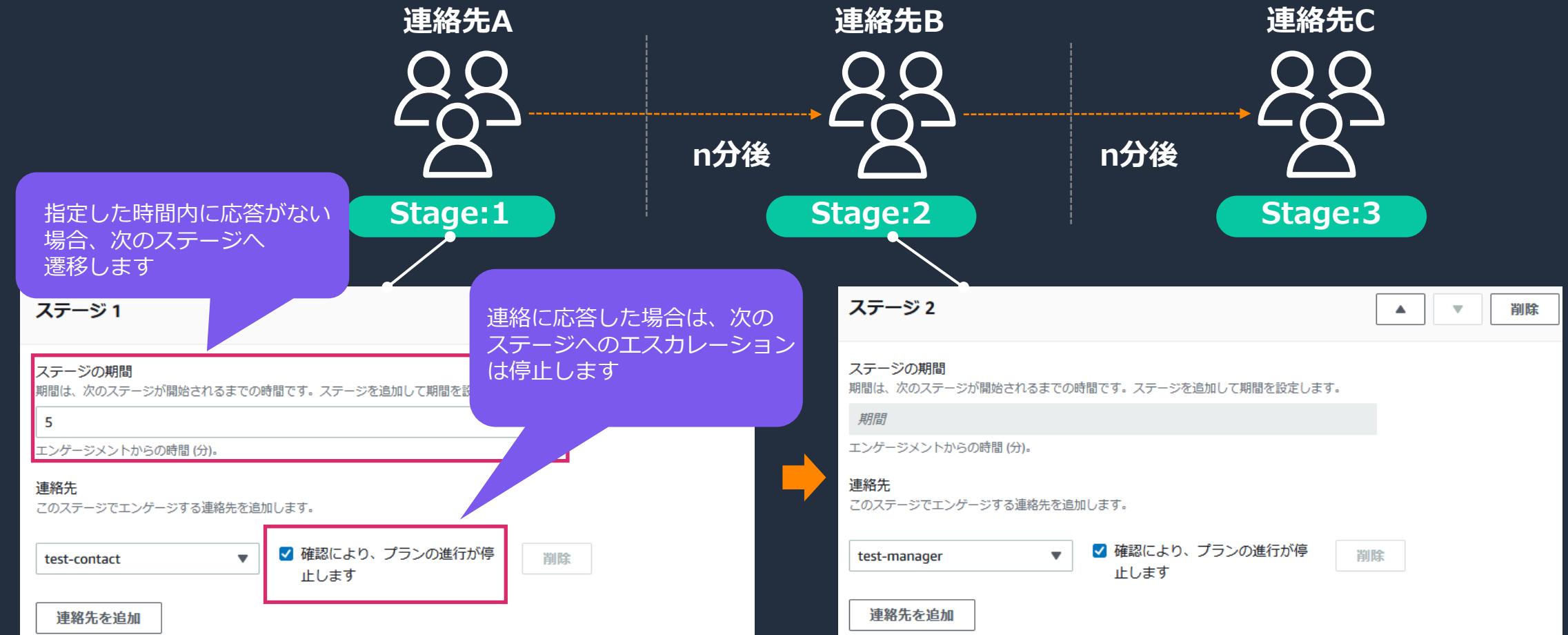
Incident Manager からの SMS 通知または音声通知において、通知元が Incident Manager であることを確認するために、vcfファイルが公開されております。

https://docs.aws.amazon.com/ja_jp/incident-manager/latest/userguide/contacts.html#contacts-details-file

※2023年4月時点では、日本の番号宛てのSMSには Acknowledge code が送信されません。

エスカレーションプラン

インシデント発生時のエスカレーションフローを定義



オンコールスケジュール

- ・ オンコール担当者のグループ内で、ローテーションを設定可能
- ・ ローテーションの頻度は、日、週、月から選択可能
- ・ 設定したスケジュールに対して例外の設定も可能

4/1~4/7

4/8~4/14

4/15~4/21

第1連絡者



Aさん



Bさん

第2連絡者



Bさん



Aさん



Aさん



Bさん (4/17だけ第1連絡者)

オンコールスケジュールの設定

The screenshot shows the configuration page for a new rotation named "test-rotation". The left side contains fields for the rotation's name, start date (2023/04/01), start time (00:00), end time (00:00), and active days (Monday through Friday). The right side shows the contact sequence and scheduling details.

ローテーションの名前: test-rotation

開始日: 2023/04/01

ローテーションの開始時刻: 00:00

アクティブな曜日: 日曜日 (未選択), 月曜日 (選択), 火曜日 (選択), 水曜日 (選択), 木曜日 (選択), 金曜日 (選択), 土曜日 (未選択)

ローテーションを削除: ボタン

コンタクト:

順番	コンタクト
1	sms-test01
2	mail01

繰り返しの設定:

シフトの繰り返しの頻度: 毎週

シフトの長さ: 1

オンコールスケジュールを有効にする曜日を指定可能。こちらは平日のみオンコールを行う設定例

オンコールを行う連絡先(コンタクト)を追加し、順番を設定する

繰り返しの設定

シフトの繰り返しの頻度
シフトを繰り返す頻度を選択します。

毎週

シフトの長さ
シフトが継続する週数を入力します。

1

オンコールスケジュールのカレンダー

4月2023								シフトオーバーライドを作成	
月曜日	火曜日	水曜日	木曜日	金曜日	土曜日	日曜日			
27	28	29	30	31	01	02			
03 00:00 - 23:59 sms-test01	04 00:00 - 23:59 sms-test01	05 00:00 - 23:59 sms-test01	06 00:00 - 23:59 sms-test01	07 00:00 - 23:59 sms-test01	08	09			
10 00:00 - 23:59 mail01	11 00:00 - 23:59 mail01	12 00:00 - 23:59 mail01	13 00:00 - 23:59 mail01	14 00:00 - 23:59 mail01	15	16			
17 00:00 - 23:59 sms-test01	18 00:00 - 23:59 sms-test01	19 00:00 - 23:59 sms-test01	20 00:00 - 23:59 sms-test01	21 00:00 - 23:59 sms-test01	22	23			

オンコールスケジュールのシフトオーバーライド

Create shift override

① オーバーライドは、選択したローテーションのアクティブなカバレッジウィンドウでのみ有効になります。

ローテーションを選択
オーバーライドするシフトを含むローテーションを選択します。
rotation01

開始日
オーバーライドの開始日を選択します
2023/04/17
YYYY/MM/DD の形式を使用してください。

終了日
オーバーライドの終了日を選択します
2023/04/18
YYYY/MM/DD の形式を使用してください。

オーバーライドのコンタクトを選択
現在のシフトをオーバーライドするコンタクトを選択します。
sms-test01

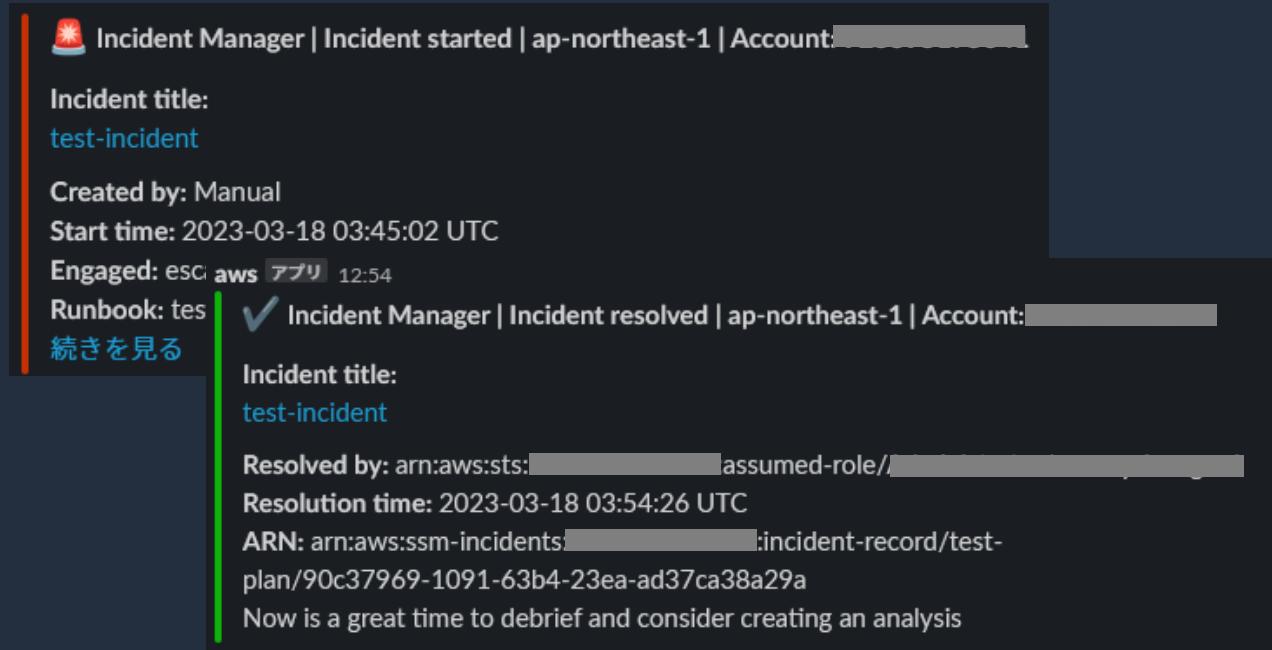
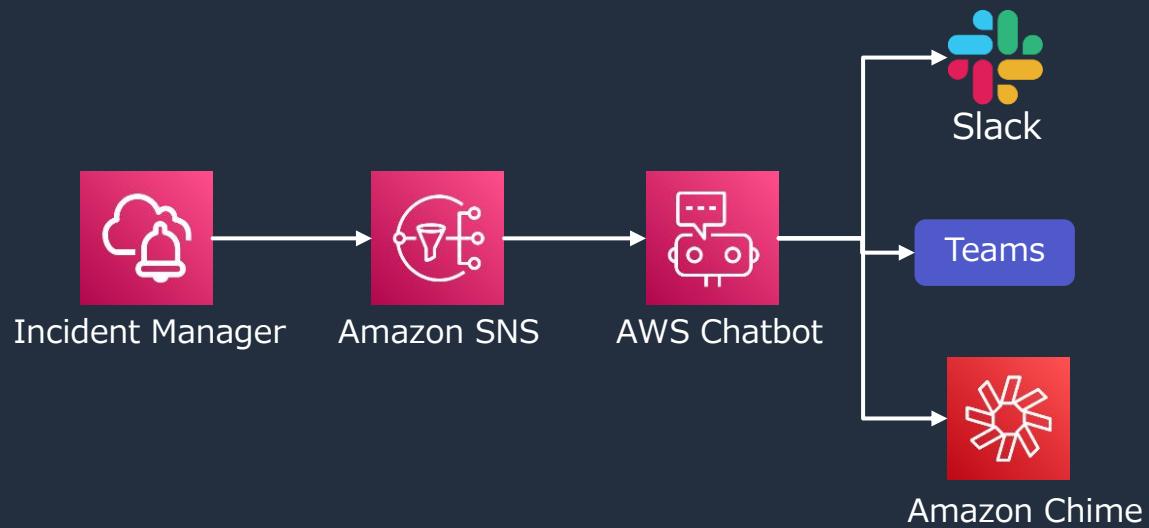
キャンセル シフトオーバーライドを作成

例外設定を行う日付を設定

ローテーションに含まれるコンタクト
(連絡先)の中から、設定

チャットチャネル

- インシデントの更新と通知をチャットチャネルにプッシュ



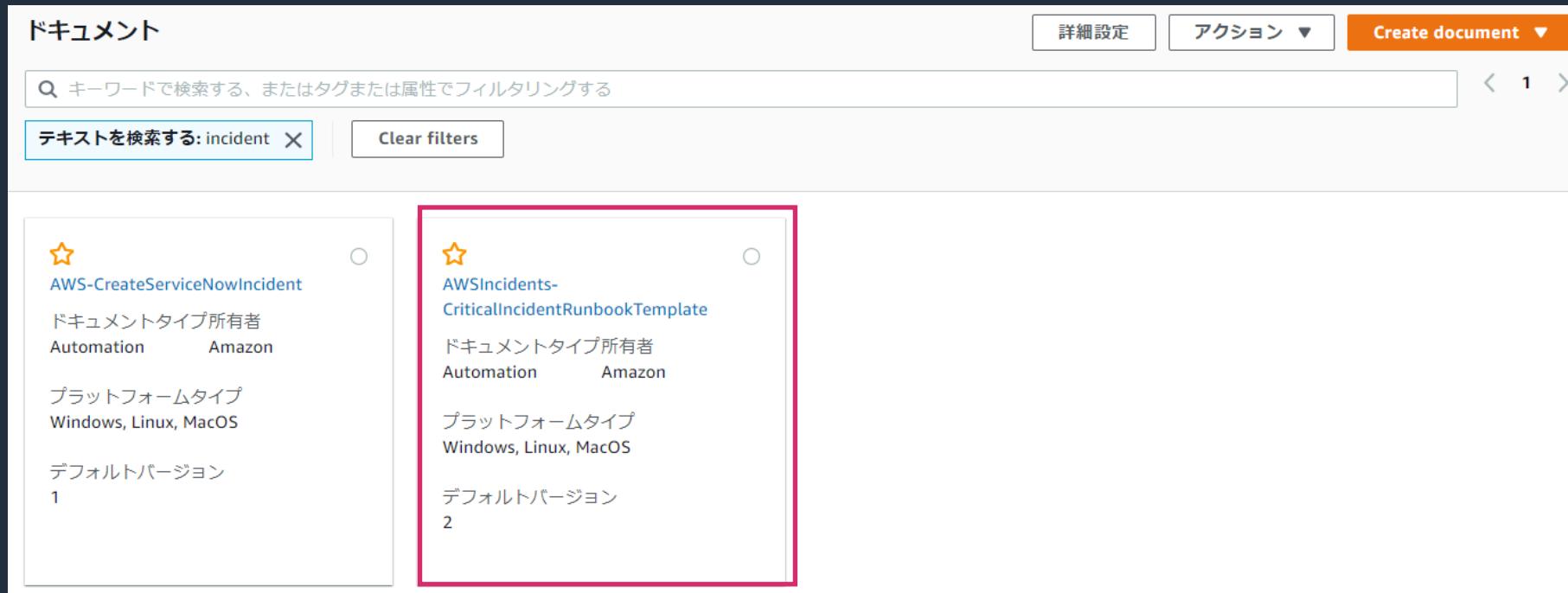
- チャットチャネルから、コマンドでインシデント情報の取得、更新が可能※

※Slack および Teams のみ対応

<https://docs.aws.amazon.com/incident-manager/latest/userguide/chat.html#chat-interact>

Runbook

- ・ インシデント発生時に、AWS Systems Manager Automation の Runbook を呼び出し可能
- ・ インシデント対応に必要な手順や処理をステップとして定義することで、インシデント対応時間の短縮に役立つ
- ・ インシデント対応用の Runbook テンプレートが提供されている



https://docs.aws.amazon.com/ja_jp/incident-manager/latest/userguide/runbooks.html#runbooks-template

© 2023, Amazon Web Services, Inc. or its affiliates.

補足: AWSIncidents-CriticalIncidentRunbookTemplate

インシデント対応の一般的なステップが定義されており、各ステップで行うべきアクションが記載されている。手順書のような扱いで利用することが可能。

The screenshot shows the AWS Incidents Critical Incident Runbook Template. On the left, there is a vertical navigation bar with four steps: Step 1: Triage (highlighted in pink), Step 2: Diagnosis (highlighted in green), Step 3: Mitigation (highlighted in purple), and Step 4: Recovery (highlighted in orange). The main content area is titled "Step 1: Triage". It includes a table with "Step Name" (Triage) and "Action" (aws:pause). Below the table, there are two sections: "Determine customer impact" and "Communicate customer impact". The "Determine customer impact" section contains a bulleted list of actions. The "Communicate customer impact" section contains instructions to update fields and a bulleted list of requirements for the title, summary, and impact rating. At the bottom, there is a "Step Input" section.

▶ ステップ 1: Triage 影響判断

▶ ステップ 2: Diagnosis 診断

▶ ステップ 3: Mitigation 緩和

▶ ステップ 4: Recovery リカバリー

▼ ステップ 1: Triage

ステップ名	アクション
Triage	aws:pause

Determine customer impact

- View the [Metrics](#) tab of the incident or navigate to your [CloudWatch Dashboards](#) to find key performance indicators (KPIs) that show the extent of customer impact.
- Use [CloudWatch Synthetics](#) and [Contributor Insights](#) to identify real-time failures in customer workflows.

Communicate customer impact

Update the following fields to accurately describe the incident:

- Title** - The title should be quickly recognizable by the team and specific to the particular incident.
- Summary** - The summary should contain the most important and up-to-date information to quickly onboard new responders to the incident.
- Impact** - Select one of the following impact ratings to describe the incident:
 - 1 – Critical impact, full application failure that impacts many to all customers.
 - 2 – High impact, partial application failure with impact to many customers.
 - 3 – Medium impact, the application is providing reduced service to many customers.
 - 4 – Low impact, the application is providing reduced service to few customers.
 - 5 – No impact, customers are not currently impacted but urgent action is needed to avoid impact.

▶ ステップ入力

対応プラン

インシデントの対応に必要な設定をまとめたもの

以下の項目を設定

- ・ インシデントのデフォルト
 - ・ タイトル
 - ・ 影響
 - ・ 概要
- ・ Runbook
- ・ チャットチャネル
- ・ エンゲージメント
 - ・ 連絡先
 - ・ エスカレーションプラン
 - ・ オンコールスケジュール

インシデントの作成

手動または、CloudWatch アラーム、EventBridge イベントによる自動作成が可能

手動

インシデントを開始

対応プラン
応答プランは自動的に連絡先をエンゲージし、ランプックを実行します。

対応プランを選択

インシデントのタイトル オーバーライド - オプション
インシデントリストでインシデントをより簡単に見つけるには、わかりやすいタイトルを入力します。
ここにタイトルを入力すると、対応プランで指定されるタイトルが上書きされます。

タイトル

インシデントへの影響 オーバーライド - オプション
影響は、インシデントの範囲を表します。ここで影響を変更すると、対応プランで指定される影響が上書きされます。

影響を選択

キャンセル 開始

自動 (CloudWatch アラームの例)

Systems Manager アクション 情報

削除

このアクションは、アラームが **アラーム状態** 状態になっているとき
にのみトリガーされます。

OpsItem を作成
指定された重要度とカテゴリのある OpsCenter 内に
OpsItem が作成されます。

インシデントを作成
これにより、レスポンスプランがテンプレートとして
使用されてインシデントが開始されます。

レスポンスプラン
レスポンスプランを選択

plan01 X

インシデントの確認

ステータス、影響、チャットチャネル、インシデントが発生している期間、Runbook の進行状況、エンゲージメント(連絡・応答)状況の概要を確認できる

関連メトリクス、タイムライン等の詳細については、各タブから確認可能

The screenshot shows the AWS Systems Manager Incident Manager interface for a test incident. The top navigation bar includes 'AWS Systems Manager > Incident Manager > test-incident'. The main title is 'test-incident'. On the right, there are buttons for 'G' (grid view), 'オフ ▾' (Off), 'プロパティを編集' (Edit Properties), and a prominent orange button 'インシデントを解決' (Resolve Incident). Below the title, there are four main status boxes: 'ステータス' (Status) with '開く' (Open) in red, '影響' (Impact) with '中' (Medium) in a red circle, 'チャットチャネル' (Chat Channel) with '#技術検証' (Technical Verification), and '期間' (Duration) with '3 分' (3 minutes). A summary section below lists 'ランブック' (Runbook) with '1 入力を待機中' (1 input pending) and 'エンゲージメント' (Engagement) with 'エンゲージ済み 1' (Engaged 1). At the bottom, a navigation bar offers tabs for '概要' (Overview), 'メトリクス' (Metrics), 'タイムライン' (Timeline), 'ランブック' (Runbook), 'エンゲージメント' (Engagement), '関連項目' (Related Items), and 'プロパティ' (Properties). The '概要' tab is currently selected.

インシデントの確認 - タイムラインの詳細

概要 | メトリクス | **タイムライン** | ランブック | エンゲージメント | 関連項目 | プロパティ

タイムライン 情報 削除 編集 追加

最新のものから表示 ▼ カスタムイベントのみを表示

日付 UTC オフセット
2023年3月18日 UTC+9:00

12:45:04 - 親 OpsItem arn:aws:ssm:ap-northeast-1:925395175041:opsitem/oi-3a9d7c5a90f8 が関連項目に追加されました。 項目が追加されました

12:45:04 - Triage (aws:pause) ランブックのステータスは InProgress です。 ランブックのステップ

12:45:03 - esca01 エスカレーションプランからのエンゲージ済み mail01 エンゲージ済み問い合わせ

12:45:03 - Triage (aws:pause) ランブックのステータスは InProgress です。 ランブックのステップ

12:45:03 - test-runbook ランブックのステータスは InProgress です。 ランブックのステータスが更新されました

12:45:03 - test-runbook ランブックバージョン 1 のステータスは Pending です。 ランブックのステータスが更新されました

12:45:02 - インシデント test-incident が作成されました。 インシデントレコードが作成されました

インシデントの対応

インシデント対応に利用する Runbook を Incident Manager のコンソールから操作可能

The screenshot shows the AWS Incident Manager Runbook editor interface. At the top, there's a navigation bar with tabs: フラグ (Flag), ハッシュ (Hash), フィルター (Filter), ステータス (Status), 実行の詳細 (Execution Details), and 開始時間 (Start Time). Below the navigation bar, a table provides details about the runbook:

名前	バージョン	ステータス	実行の詳細	開始時間
test-runbook	1	対応プラン	待機中	70c94fdc-1b8f-4cc3-a90... 5 分前

The main area is titled "ランブックのステップ" (Runbook Step) and displays the "Triage" step. The timeline shows two points: 0:00:00 (UTC+9:00) and 12:45:04. The "Triage" step is highlighted with a blue border. It contains two sections: "Determine customer impact" and "Communicate customer impact".

Determine customer impact

- View the Metrics tab of the incident or navigate to your CloudWatch Dashboards to find key performance indicators (KPIs) that show the extent of customer impact.
- Use CloudWatch Synthetics and Contributor Insights to identify real-time failures in customer workflows.

Communicate customer impact

Update the following fields to accurately describe the incident:

- Title** - The title should be quickly recognizable by the team and specific to the particular incident.
- Summary** - The summary should contain the most important and up-to-date information to quickly onboard new responders to the incident.
- Impact** - Select one of the following impact ratings to describe the incident:
 - 1 – Critical impact, full application failure that impacts many to all customers.
 - 2 – High impact, partial application failure with impact to many customers.
 - 3 – Medium impact, the application is providing reduced service to many customers.
 - 4 – Low impact, the application is providing reduced service to few customers.
 - 5 – No impact, customers are not currently impacted but urgent action is needed to avoid impact.

A red box highlights the "再開" (Restart) button at the bottom of the "Triage" step card.

Below the "Triage" step, there's a partially visible "Diagnosis" step.

インシデントの対応

インシデントのメモ (2) X

インシデントノートを使用して、インシデントに関連するメッセージを強調表示する

インシデントのメモを追加

2023年3月18日 12:57:18 (UTC+9:00) :
原因を発見

2023年3月18日 12:54:53 (UTC+9:00) :
インシデント対応中

タイムライン 情報

最新のものから表示 ▼ カスタムイベントのみを表示

削除 編集 追加

日付 UTC オフセット
2023年3月18日 UTC+9:00

12:57:18 - メモが追加されました: 原因を発見 メモ

12:54:53 - メモが追加されました: インシデント対応中 メモ

インシデント対応状況をメモ機能で残すことができて、追加したメモはタイムラインにも反映される

インシデント後の分析

インシデント後の分析を行う理由

- ・ インシデント対応の改善が行える
- ・ 問題の根本原因の理解、対処ができる
- ・ インシデントによる影響を分析できる
- ・ インシデントから学んだことを共有できる

分析用のテンプレートが利用可能

- ・ テンプレート内に用意された質問に回答することで、インシデントの根本原因の掘り下げに役立つ
- ・ テンプレート：**AWSIncidents-PostIncidentAnalysisTemplate**

分析後の具体的なアクションは、「アクション項目の作成」で、OpsCenter の OpsItem として管理可能

分析テンプレート入力項目

項目	入力内容
概要	インシデントの概要
影響	インシデントの影響
インシデントの検出に関する質問	インシデントの検出にかかる時間を短縮するために改善できることはあるか
インシデントの診断に関する質問	インシデントの診断にかかる時間の短縮や担当者への連絡に関して改善の余地があるか
インシデントの緩和・軽減に関する質問	インシデントによる影響の緩和・軽減や対応完了までの時間を短縮するために改善できることはあるか
インシデントの防止に関する質問	なぜ問題が発生したか、得られた教訓

分析の詳細

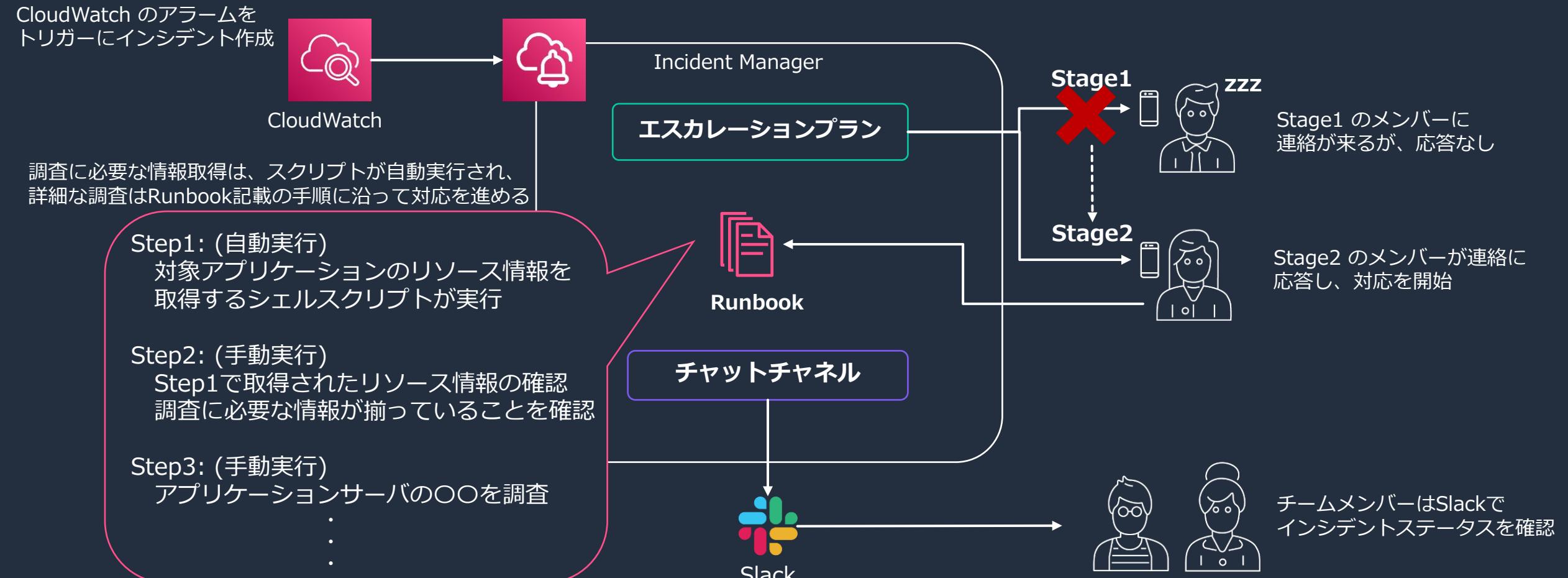
<https://docs.aws.amazon.com/incident-manager/latest/userguide/analysis.html#analysis-details>

correction of error (COE) を開発すべき理由

<https://aws.amazon.com/jp/blogs/news/why-you-should-develop-a-correction-of-error-coe/>



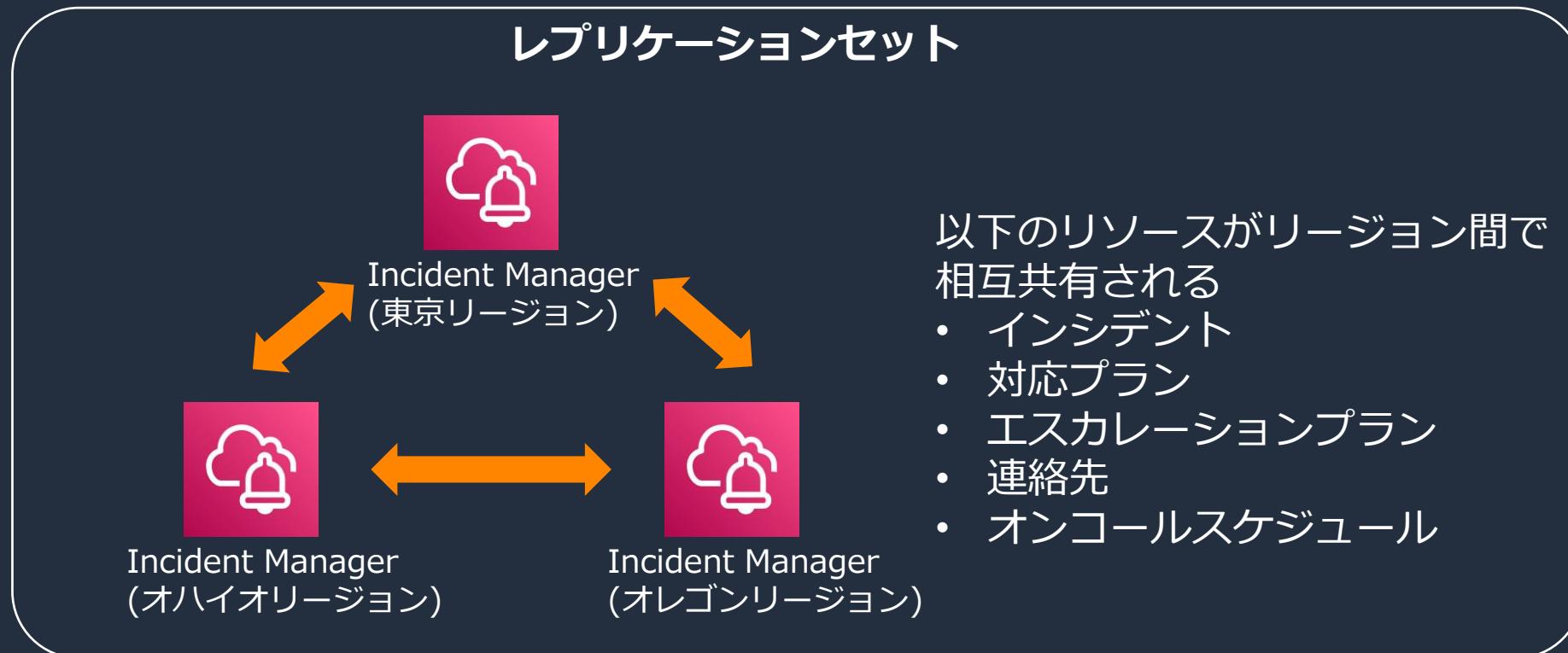
インシデント例：アプリケーションのレスポンス遅延が発生 レスポンスが遅延する原因は毎回固定ではないため、都度調査が必要なケース



その他機能・Tips

クロスリージョン対応

- インシデント対応、管理に必要なリソースをリージョン間で共有
- 最低でも2つのAWSリージョンでレプリケーションセットを作ることを推奨



<https://docs.aws.amazon.com/incident-manager/latest/userguide/incident-manager-cross-account-cross-region.html#incident-manager-cross-region>

レプリケーションセット

レプリケーションセット 情報

データのレプリケート先のリージョンと、データの暗号化に使用される AWS KMS キーを管理します。リージョンレプリケーションは、インシデント発生中に高い可用性と耐障害性を提供します。

リージョン

データをレプリケートするリージョンを選択します。

リージョンを選択

▼

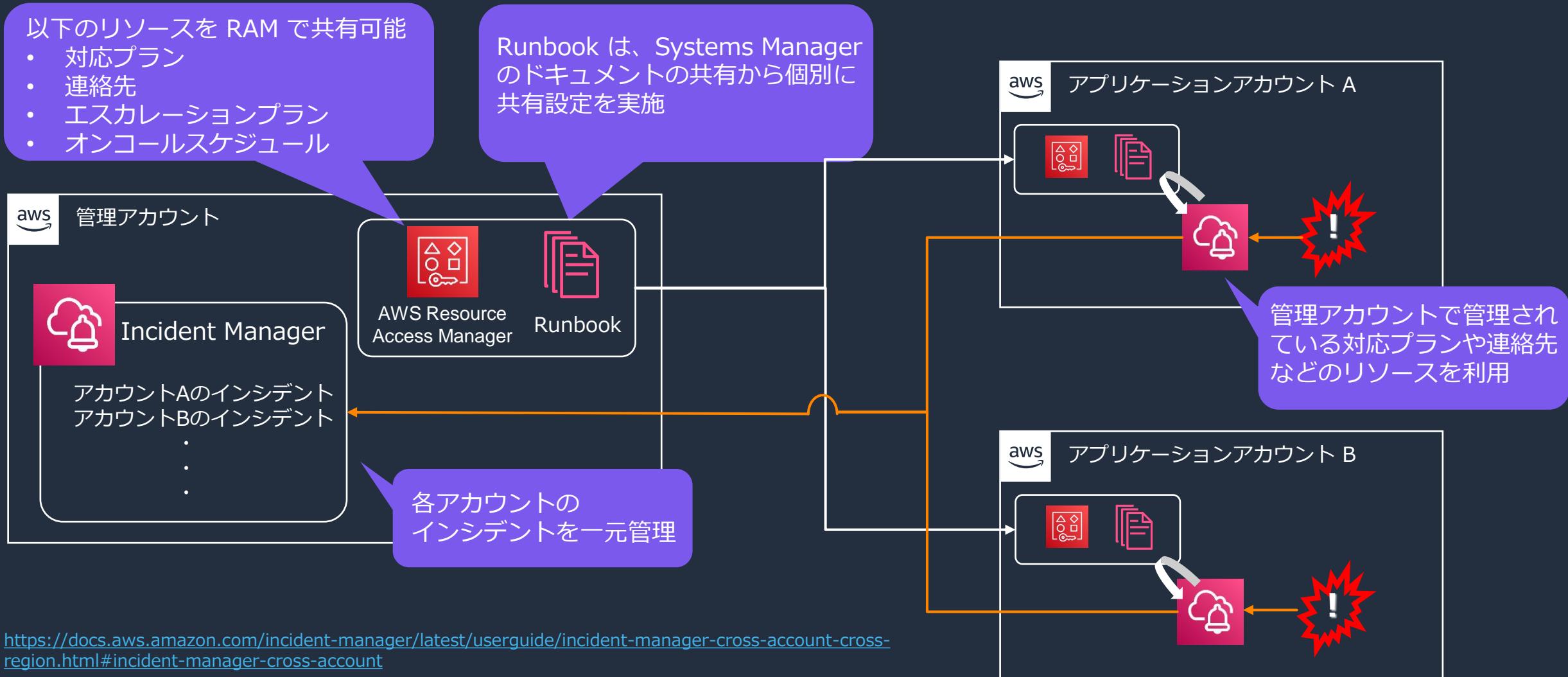
米国東部 (バージニア北部) X
us-east-1

米国東部 (オハイオ) X
us-east-2

米国西部 (オレゴン) X
us-west-2

最大で3つのリージョンを選択可能
最低でも2つのリージョン利用が推奨

クロスアカウント対応



Tips: 対応プランで利用する Runbook へのパラメータ受け渡し

- 対応プランに Runbook を追加する場合、Runbook 実行時に使用するパラメータを指定可能
- インシデントのトリガーによって受け渡されるパラメータは異なる(CloudWatch アラーム、EventBridge ルール)

例：EC2 のCPU 使用率にしきい値を設けたアラームの場合、EC2 の ARNが連携される



Runbook に渡すパラメータとして、“**関連リソース**”を選択すると、インシデントのトリガーに応じて関連するサービスの ARN が Runbook のパラメータとして受け渡される

<https://docs.aws.amazon.com/incident-manager/latest/userguide/runbooks.html#runbooks-parameters>

Tips: 対応プランで利用する Runbook へのパラメータ受け渡し

- Runbook のパラメータには関連リソースの情報が **ARN** で連携されるため、Runbook で実行する処理によってはパラメータの成形が必要なケースがある (EC2 インスタンスの Instance Id のみ必要な場合など)
- そのため、Runbook のはじめのステップで、文字列加工を行うようなステップを追加し、加工後の文字列を次のステップに連携するような設定が必要となる

例 :

Step1: 文字列加工

ARN から Instance Id のみを抽出
次の Step に Instance Id を連携

Step2: Runbook の AWS-StopEC2Instance を呼び出す

Step1 から受け取ったパラメータ(Instance Id)を使い、 AWS-StopEC2Instance 呼び出す

Automation Runbookの作成についてはこちらを参照

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/automation-actions.html



製品・サービス統合

- ServiceNow、Jira Service Management、Jira Cloud、PagerDuty と統合
- Incident Manager から作成されたインシデントが上記のサービスに連携される
- 上記のサービスをメインツールとして利用している場合、Incident Manager が作成するインシデントもまとめて管理が可能

<https://docs.aws.amazon.com/incident-manager/latest/userguide/integration.html>



Incident Manager と OpsCenter の関係性

Incident Manager

“インシデント”の管理、対応を行うために設計されたインシデント管理コンソール

OpsCenter

AWSリソースに関する運用作業項目(**OpsItem**)を表示、調査、解決するための一元的な場所

Incident Manager
がカバーする領域

AWS リソースに関する運用作業項目(OpsItem)

インシデント
管理・対応

メンテナンス

定型作業

...

OpsCenter がカバー
する領域

料金

料金

Incident Manager の料金

- 1か月でアクティブな対応プランの数に基づいて課金されます
- 1か月あたり最大 100 件の SMS または音声メッセージが無料。追加のメッセージは、受信者の国に応じて課金されます

詳細	料金
対応プラン	対応プランごとに月額 7 USD
SMS および音声メッセージ	メッセージごと、SMS および 1 分間の音声メッセージの宛先国の料金に基づく https://aws.amazon.com/jp/systems-manager/pricing/country-rates/

関連機能の料金

- 対応プランでは Systems Manager OpsCenter と Automation を使用して、アクションを追跡し、Runbook を実行します。作成された OpsItems と実行された Runbook ステップに対する OpsCenter と Automation の料金に基づいて課金されます。

<https://aws.amazon.com/jp/systems-manager/pricing/>

まとめ



まとめ

- インシデントとは
 - サービスにおける計画外の中止やサービス品質の低下をもたらすもの
- Incident Manager とは
 - インシデントの解決、影響を軽減するまでの時間を短縮させるための機能
- Incident Manager を使うことで
 - インシデント発生時に適切なメンバーのアサイン、連絡、エスカレーション、関係者間のコミュニケーション円滑化に役立つ
 - Runbook を利用することで、インシデント対応の効率化にもつながる

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!



AWS Systems Manager

Inventory 編

AWS Black Belt Online Seminar

上野 涼平

Solutions Architect
2023/06

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=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBIqY>

内容についての注意点

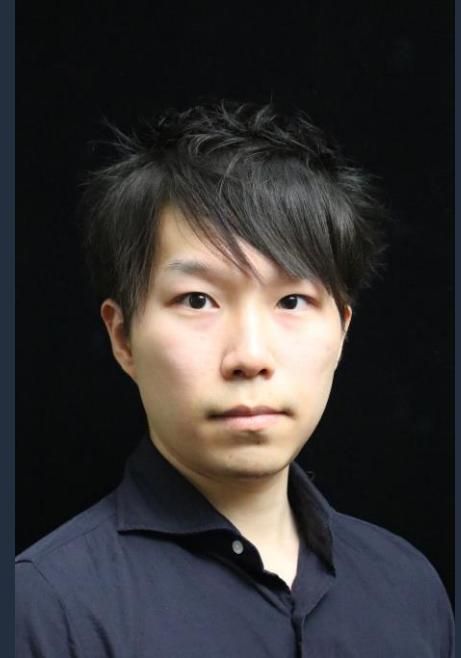
- ・ 本資料では 2023 年 6 月時点のサービス内容および価格についてご説明しています。最新の情報は AWS 公式ウェブサイト(<https://aws.amazon.com/>)にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：上野 涼平

所属：ソリューションアーキテクト

経歴：AWS ユーザーの立場で、オンプレミスからの移行、AWS 環境の運用改善



好きなAWSサービス：AWS Systems Manager



本セミナーの対象者

- AWS の運用を担当されている方
- これから AWS の運用を担当予定の方

本セミナーの目的

- AWS Systems Manager Inventory の機能とユースケースをご理解いただく

本日お話ししないこと

- AWS Systems Manager の全体像
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager Inventory 以外の機能の詳細
→ 今後公開を予定している、各機能にフォーカスしたセッションをお待ちください！

アジェンダ

1. AWS Systems Manager の概要
2. Systems Manager Inventory とは
3. Inventory 応用編
4. まとめ

AWS Systems Manager の概要

AWS Systems Manager

ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション



AWS Config

Configuration history



Amazon EventBridge

Notification and remediation



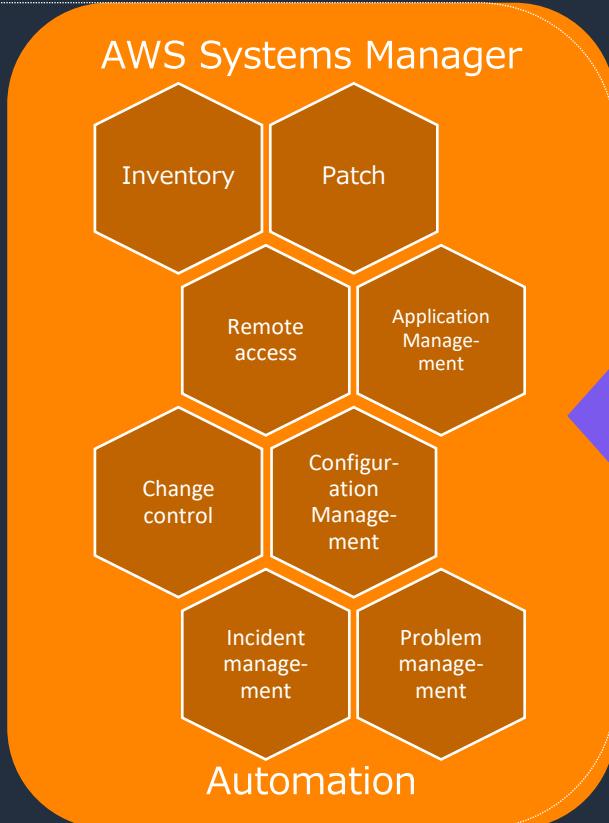
AWS CloudTrail

Audited actions



AWS Identity and Access Management (IAM)

Role-based access control



Integration
connectors
and APIs

- Third-party tools
- ITSM
- Custom solutions

AWS の他のサービスや
3rd Party のツールと統合された
管理ソリューションを提供

(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

運用管理

-  Explorer
-  OpsCenter
-  Incident Manager

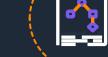
アプリケーション管理

-  Application Manager
-  AppConfig
-  Parameter Store

変更管理

-  Change Manager
-  Automation
-  Maintenance Windows
-  Change Calendar

ノード管理

-  Fleet Manager
-  Session Manager
-  Inventory
-  Run Command
-  Patch Manager
-  Distributor
-  State Manager

Quick Setup

AWS Systems Manager の機能

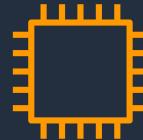
運用管理	アプリケーション管理	変更管理	ノード管理
 Explorer  OpsCenter  Incident Manager	 Application Manager  AppConfig  Parameter Store	 Change Manager  Automation  Maintenance Windows  Change Calendar	 Fleet Manager  Session Manager  Inventory  Run Command  Patch Manager  Distributor  State Manager

Quick Setup

Systems Manager Inventory とは

インベントリデータ管理における従来の課題

インベントリデータとは？



- OS 情報
- ソフトウェア情報
- ファイル情報
- ネットワーク構成情報 etc

○○の脆弱性が
見つかったから
該当するサーバーの
調査よろしく！



管理表の最終更新が
2年前になっている…
直接確認しないと…

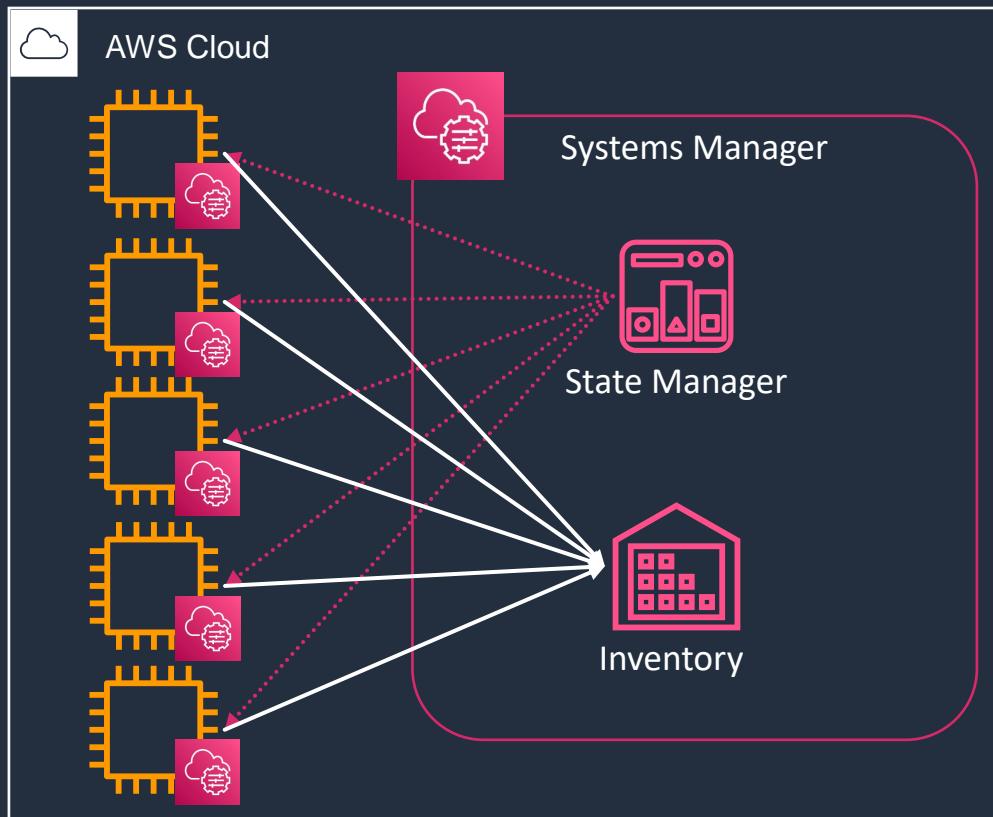


インベントリデータ管理の例

- Excel で手動管理している
- 管理表の更新漏れで実機と差異が発生
- 正しい情報確認のためにサーバー1台ずつ接続して確認しないといけない



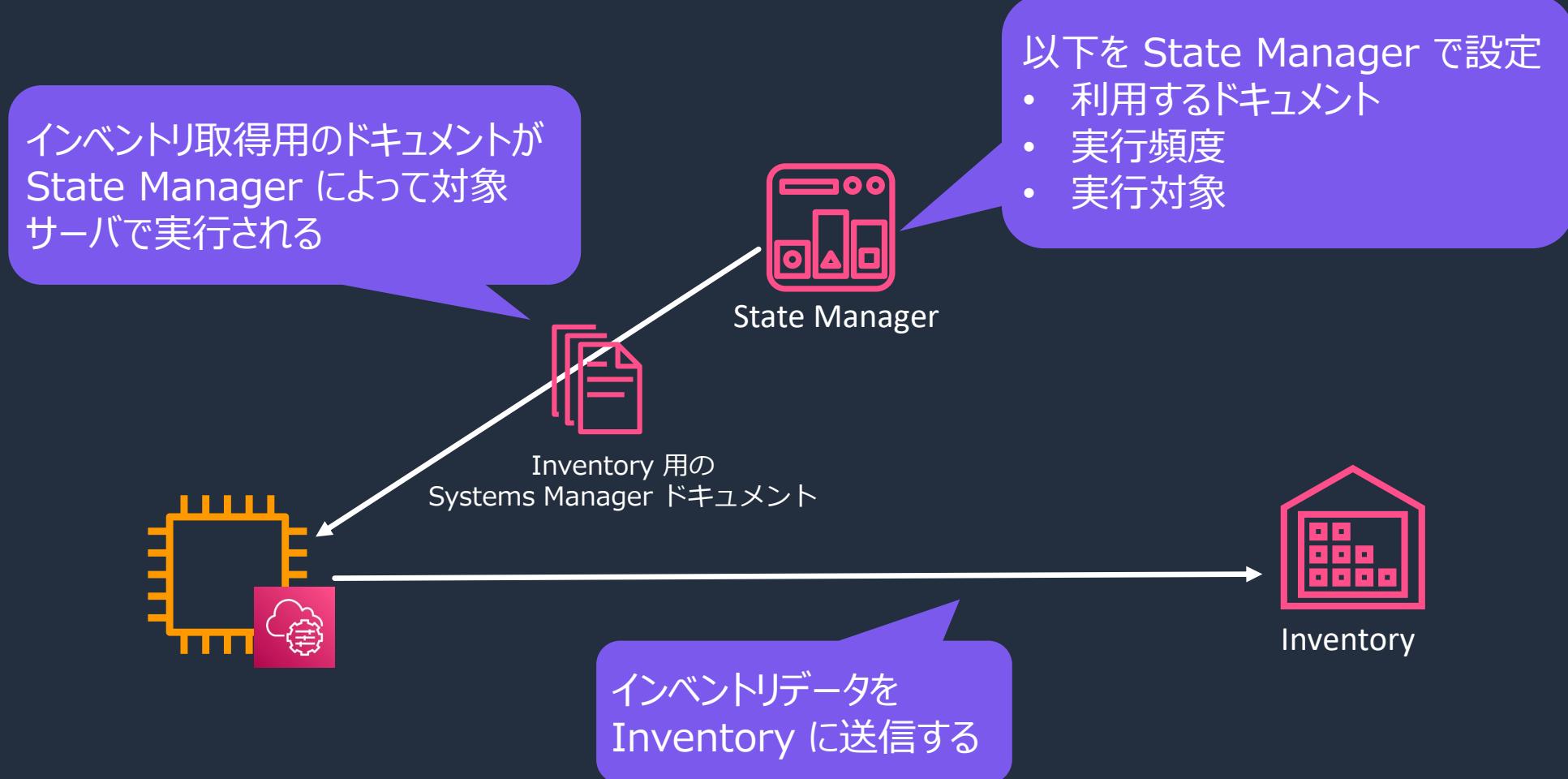
Systems Manager Inventory とは



インベントリデータの収集、一元的な管理が可能

- 最短 30分ごとにサーバーのインベントリデータを定期的に収集し、最新の状態を保つ
- Fleet Manager からマネージドノードごとにインベントリデータを確認可能
- ダッシュボードから特定のバージョン・ソフトウェア名などの条件もとにフィルタリングが可能
- State Manager の associations (関連付け)の設定により、インベントリデータの収集が行われる
- データは30日間保持。30日以上保存する必要がある場合、後述するリソースデータの同期を利用
- Inventory 利用に料金はかかりません

Inventory と State Manager



Inventory で収集出来るデータ

インベントリタイプ	詳細
アプリケーション	アプリケーション名、発行元、バージョンなど
AWS コンポーネント	EC2 ドライバ、エージェント、バージョンなど
ファイル	名前、サイズ、バージョン、インストール日、変更および最新アクセス時間など
ネットワーク構成情報	IP アドレス、MAC アドレス、DNS、ゲートウェイ、サブネットマスクなど
Windows Update	Windows Updateに関する情報 (Hotfix ID、インストール者、インストール日など)
インスタンスの詳細	OS名、OSバージョン、最終起動、DNS、ドメイン、ワークグループ、OS アーキテクチャなど
サービス	名前、表示名、ステータス、依存サービス、サービスのタイプ、起動タイプなど
タグ	インスタンスに割り当てられているタグ
Windows レジストリ	レジストリキーのパス、値の名前、値タイプおよび値
Windows ロール	名前、表示名、パス、機能タイプ、インストール日など
カスタムインベントリ	カスタムに割り当てられるメタデータ。例えばオンプレミスの各インスタンスのラック位置など

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-inventory.html>



補足：Inventory で取得されるアプリケーション情報

- インベントリタイプ：アプリケーションでは、OS 系パッケージを取得します。
- そのため、npm、pip、Composer などの各言語系のパッケージは取得対象外となっております。

Linux 系の例

```
// rpm commands related constants
  rpmCmd          = "rpm"
  rpmCmdArgToGetAllApplications = "-qa"    ➔ rpm -qa コマンド
  rpmQueryFormat      = "--queryformat"
  rpmQueryFormatArgs   = `¥{"Name":`` + mark(`%{NAME}`) + `","Publisher":`` + mark(`%{VENDOR}`) + `","Version":`` +
    mark(`%{VERSION}`) + `","Release":`` + mark(`%{RELEASE}`) + `","Epoch":`` + mark(`%{EPOCH}`) + `",
    "InstalledTime":`` + mark(`%{INSTALLTIME}`) + `","ApplicationType":`` + mark(`%{GROUP}`) + `",
    "Architecture":`` + mark(`%{ARCH}`) + `","Url":`` + mark(`%{URL}`) + `",
    "Summary":`` + mark(`%{Summary}`) + `","PackageId":`` + mark(`%{SourceRPM}`) + `"}},`
```

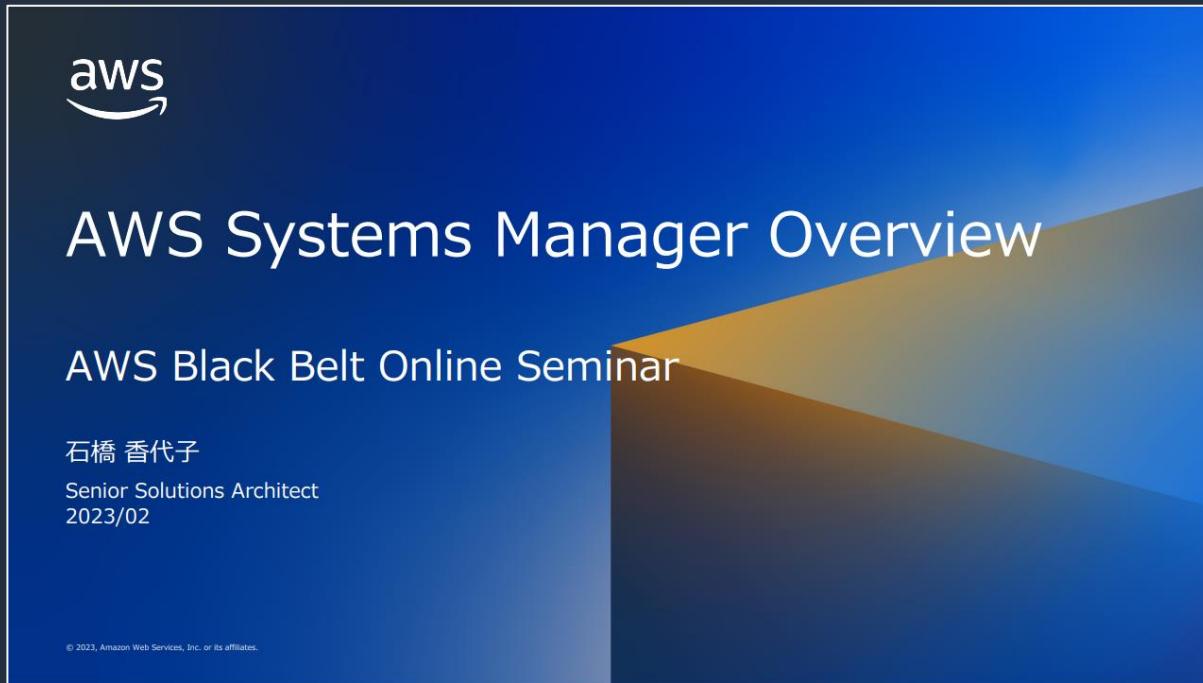
詳細は ssm-agent のソースコードをご確認ください

<https://github.com/aws/amazon-ssm-agent/tree/b292a1dae6be49964e1f10836bfe8eed766f6b44/agent/plugins/inventory/gatherers/application>

Inventory を利用する前に

インベントリデータ収集対象のサーバーをマネージドノードにする必要があります。

詳細は、AWS Black Belt Online Seminar の「[AWS Systems Manager Overview](#)」をご覧ください



AWS Systems Manager を使ってサーバ管理を行うためには

サーバを“マネージドノード”にする

ここに一覧で出てくるようになります

The screenshot shows the 'Managed Nodes' section of the AWS Systems Manager console. A callout box points to the 'Managed Nodes' tab in the navigation bar. The main area displays a table of 17 nodes, each with details like Node ID, Status, Launched By, Platform, Operation System, and Source Type. One node, 'i-04970a7f373ac630b', is highlighted with a green circle and labeled '実行中' (Running). The table has columns for Node ID, Node Type, Node Name, Platform, Operation System, Source Type, and more.

マネージドノード :

- SSM管理下のインスタンス群
- EC2インスタンスのほか、オンプレミスのインスタンスも含まれられる。

aws

© 2023, Amazon Web Services, Inc. or its affiliates.

Inventory のセットアップ

ターゲット

ターゲットの選択

- このアカウントのすべてのマネージドインスタンスの選択
- タグの指定
- インスタンスの手動選択

すべてのマネージドインスタンスを指定することが可能

スケジュール
(SSMAgent バージョン 2.0.790.0 以降が必要です)

インベントリデータの収集毎 分 ▾

最短30分の設定が可能

ファイルと Windows レジストリの情報を収集したい場合はパス指定で設定が必要

パラメーター

- Applications
(Optional) Collect data for installed applications.
- AWS Components
(Optional) Collect data for AWS Components like amazon-ssm-agent.
- Network Config
(Optional) Collect data for Network configurations.
- Windows Updates
(Optional, Windows OS only) Collect data for all Windows Updates.
- Instance Detailed Information
(Optional) Collect additional information about the instance, including the CPU model, speed, and the number of cores, to name a few.
- Services
(Optional, Windows OS only, requires SSMAgent version 2.2.64.0 and above) Collect data for service configurations.
- Windows Roles
(Optional, Windows OS only, requires SSMAgent version 2.2.64.0 and above) Collect data for Microsoft Windows role configurations.
- Custom Inventory
(Optional) Collect data for custom inventory.
- Billing Info
(Optional) Collect billing info for license included applications.
- ファイル
(省略可能、 SSMAgent バージョン 2.2.64.0 以降が必要) ファイルに関する情報を収集します。

パス	<input type="text" value="C:\Program Files"/>	パターン - オプション	<input type="text" value=".exe, *.log"/>	再帰的
<input type="button" value="Add another row"/>				
- Windows レジストリ
(省略可能、 Windows OSのみ、 SSMAgent バージョン 2.2.64.0 以降が必要) Microsoft Windows レジストリに関する情報を収集します。

パス	<input type="text" value="HKEY_LOCAL_MACHINE\Software"/>	値の名前 - オプション	<input type="text" value="Name1, Name2"/>	再帰的
----	--	--------------	---	-----



Fleet Manager からインベントリデータを確認可能

ノードの詳細ページに遷移し、インベントリタブを開く

The screenshot shows the AWS Fleet Manager interface with the 'Events' tab selected. A dropdown menu is open under the 'Event Type' heading, showing 'AWS:Application' as the current selection. A purple callout bubble points to this dropdown with the text 'インベントリタイプごとにデータを確認出来る' (You can verify data by event type). Below the dropdown is a search bar and a table listing various software packages with columns for Name, Version, Publisher, Application Type, Install Time, Architecture, URL, and Release Date.

名前	バージョン	公開者	アプリケーションタイプ	インストール時刻 (UTC)	アーキテクチャ	URL	Release
vim-data	9.0.1314	Amazon Linux	Unspecified	Fri, 12 May 2023 07:25:46 GMT	noarch	http://www.vim.org/	1.amz
fuse-libs	2.9.2	Amazon Linux	System Environment/Libraries	Mon, 24 Jan 2022 18:28:11 GMT	x86_64	https://github.com/libfuse/libfuse	11.am
kbd-legacy	1.15.5	Amazon Linux	System Environment/Base	Mon, 24 Jan 2022 18:28:00 GMT	noarch	http://ftp.altlinux.org/pub/people/legion/kbd	15.am
nss-softokn	3.79.0	Amazon Linux	System Environment/Libraries	Fri, 12 May 2023 07:25:46 GMT	x86_64	http://www.mozilla.org/projects/security/pki/nss/	4.amz
...	0.11	Amazon	System Environment/Base	Mon, 24 Jan 2022	...	http://www.mozilla.org/projects/security/pki/nss/	...

ダッシュボード

AWS Systems Manager > インベントリ

ダッシュボード | 詳細ビュー | 設定

インベントリ

リソースグループ、タグ、またはインベントリタイプによるフィルタリング
オフラインインスタンスは含まれません (削除済みおよび停止状態 - EC2、削除済み - オンプレミス)

検索:

インベントリが有効になっているマネージドインスタンス

現在のリージョンとアカウントのインスタンスが含まれます。

Enabled Disabled



タイプごとのインベントリカバレッジ

定義済みインベントリタイプのみ。

インベントリタイプ	カバレッジ
AWS:AWSComponent	100%
AWS:Application	100%
AWS:File	100%
AWS:InstanceDetailedInformation	100%
AWS:InstanceInformation	100%
AWS:Network	100%
AWS:Service	100%
AWS:WindowsRegistry	100%
AWS:WindowsRole	100%
AWS:WindowsUpdate	100%

カスタムインベントリタイプのトップ 10

インベントリコレクションに対してお客様が定義したインベントリタイプ。

インベントリタイプ	カバレッジ
RackInfo	100%
RackInformation	100%

インベントリデータのフィルタリング

インベントリ

インベントリデータの項目等で絞り込みが出来る

The screenshot shows the AWS CloudWatch Metrics Insights interface. On the left, there's a sidebar with a search bar and a list of filter categories: Resource groups, Tag key, Tag value, Custom, AWS:Application, AWS:Application.ApplicationType, AWS:Application.Architecture, AWS:Application.Epoch, AWS:Application.InstalledTime, AWS:Application.Name, AWS:Application.PackageId, AWS:Application.Publisher, AWS:Application.Release, AWS:Application.Summary, AWS:Application.URL, and AWS:Application.Version. The 'AWS:Application' category is highlighted with a red box. On the right, the main pane displays a search bar and two selected filters: 'AWS:AWSComponent.Name: Equal: amazon-ssm-agent' and 'AWS:AWSComponent.Version: Less than: 3.3'. A red box highlights these filters. Below the filters, there's a 'Clear filters' button. A purple callout bubble points to the filters with the text 'ssm agent のバージョンが3.3以下という条件で絞り込みをした例' (Example of filtering by the condition that the ssm agent version is less than 3.3). At the bottom, there's a copyright notice: '© 2023, Amazon Web Services, Inc. or its affiliates.'

インベントリ履歴と変更の追跡

AWS Config を使用することで、インベントリの変更履歴を確認することができます

リソースタイプ	詳細
SSM:ManagedInstanceInventory	マネージドノードのインベントリデータ
SSM:PatchCompliance	Systems Manager Patch Managerでのパッチ適用状況
SSM:AssociationCompliance	Systems Manager State Manager の associations(関連付け)の適用状況
SSM:FileData	サーバー内のファイル (Inventory でインベントリタイプ「AWS : File」を収集している場合)

イベント

すべての時刻 Asia/Tokyo (UTC+09:00)

2023年5月23日

17:52:26 設定変更

JSON diff - 1 フィールドの変更

開始

```
{}
```

終了

```
{
  Configuration.AWS:Application.Content.Amazon CloudWatch Agent: {"InstalledTime": "2023-05-23T00:00:00Z", "PackageId": "(877DABD0-D306-4CF4-BBA1-5E3B8682A179)", "Publisher": "Amazon.com, Inc.", "Architecture": "x86_64", "Version": "1.3.50751", "Name": "Amazon CloudWatch Agent"}
}
```

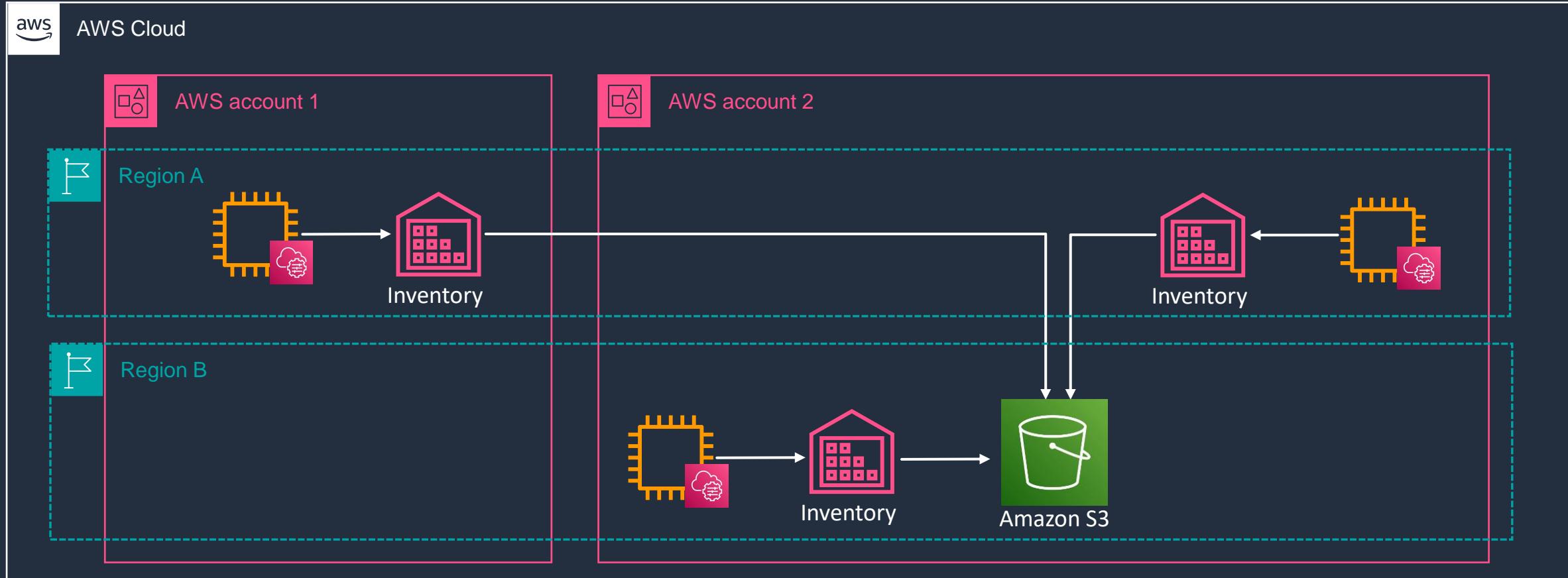
CloudWatch Agent のインストール前後

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-inventory-history.html



リソースデータの同期 1/3

リソースデータ同期を使用して、リージョンおよび AWS アカウントを横断ですべてのマネージドノードから収集されたインベントリデータを、1 つの Amazon S3 バケットに送信できます。

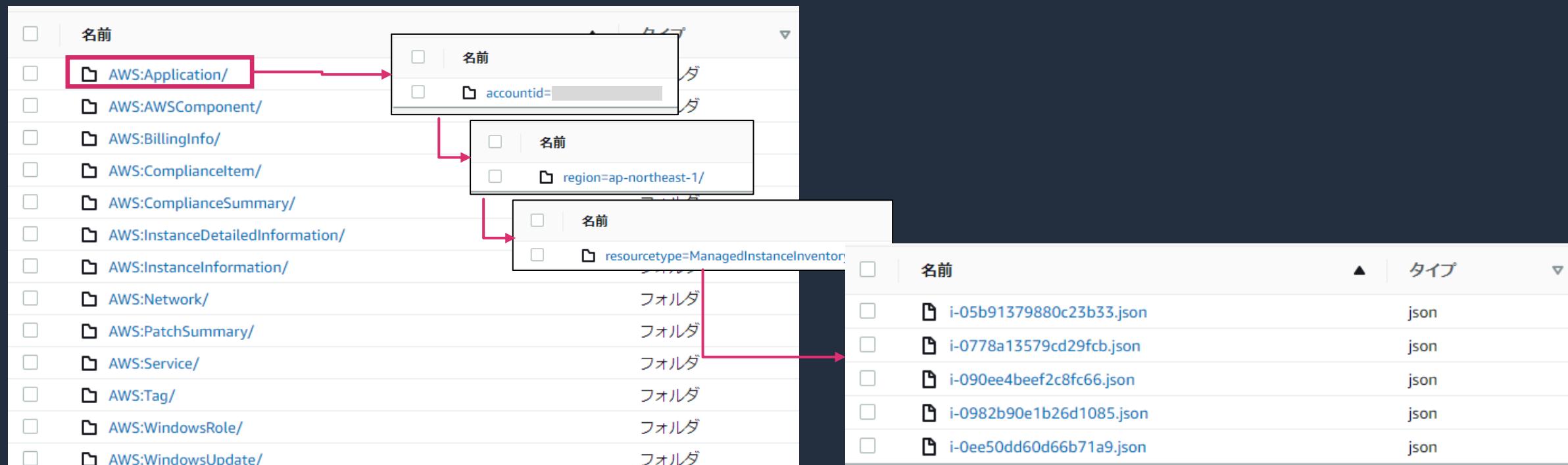


リソースデータの同期 2/3

同期タイミング

新しいイベントリデータが収集されると、Systems Manager は Amazon S3 バケットのデータを自動的に更新します。

リソースデータの同期によってS3に保存されたデータ



リソースデータの同期 3/3

AWS Systems Manager > インベントリ

ダッシュボード 詳細ビュー 設定

この機能では、AWS Athena、AWS Glue、リソースデータの同期を使用してインベントリデータを表示します。この機能を使用するには、リソースデータの同期を選択する必要があります。料金が適用される場合があります。

リソースデータの同期 リソースデータの同期の作成

test01-single
同期日: Mon May 22 2023 14:47:32 GMT+0900 (日本標準時) 前回のステータス: Successful 最終の同期: Wed May 24 2023 15:40:19 GMT+0900 (日本標準時) 最後に成功した同期: Wed May 24 2023 15:40:19 GMT+0900 (日本標準時)

インベントリタイプ AWS:Application

インベントリデータ

詳細ビューから作成したリソースデータの同期を選択すると、Amazon Athena、AWS Glue によってインベントリデータに対してクエリが実行できるようになる

Region	Account ID	Region	Installed time	Architecture	Version	Summary	Package ID
-		ap-northeast-1	-	i386	1.3.175.27	-	
-		ap-northeast-1	-	i386	2.3.28307	-	
-		ap-northeast-1	2023-03-15T00:00:00Z	i386	113.0.1774.35	-	
-		ap-northeast-1	-	i386	14.29.30139.0	-	

ポート Query History Run Advanced Queries

詳細ビューからは Region と Account ID によるフィルターしか出来ないため、細やかなクエリを実行したい場合は、[Run Advanced Queries]から Athena のコンソールへ遷移

Inventory 應用編

カスタムインベントリ

- ・ カスタムインベントリを作成することで、任意の固定値やコマンド実行で得られる結果などノードに必要なあらゆるメタデータを割り当てることが可能
- ・ API 実行（ PutInventory API ）または、 JSON ファイルを所定のパス配下に配置
- ・ API 実行では実行時にカスタムインベントリデータが割り当てられる。 JSON ファイル配置の場合、 State Manager の associations (関連付け) の設定に基づき JSON ファイル記載の内容が収集される

OS	JSON ファイル配置パス
Linux	/var/lib/amazon/ssm/ <i>node-id</i> /inventory/custom
macOS	/opt/aws/ssm/data/ <i>node-id</i> /inventory/custom
Windows	%SystemDrive%¥ProgramData¥Amazon¥SSM¥InstanceId ¥ <i>node-id</i> ¥inventory¥custom

JSON ファイルの例

```
{  
  "SchemaVersion": "1.0",  
  "TypeName": "Custom:RackInformation",  
  "Content": {  
    "Location": "US-EAST-02.CMH.RACK1",  
    "InstalledTime": "2016-01-01T01:01:01Z",  
    "vendor": "DELL",  
    "Zone" : "BJS12",  
    "TimeZone": "UTC-8"  
  }  
}
```

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-inventory-custom.html



動的なカスタムインベントリの設定

- JSON ファイルに定義した固定値ではなく、都度コマンド実行した動的な結果をカスタムインベントリデータとして収集することも可能
- Inventory はインベントリデータの収集アクションを定義した Systems Manager のドキュメントを State Manager が実行する仕組みになっている
- デフォルトで利用される”ドキュメント”の処理に、必要な情報を取得するコマンド実行およびその結果を JSON ファイルに上書きするステップを追加し、カスタムしたドキュメントを State Manager から実行することで実現可能

AWS-GatherSoftwareInventory
ドキュメント(デフォルト利用)



```
mainStep:  
"action": "aws:softwareInventory"
```



カスタムインベントリ用ドキュメント



```
mainStep:  
"action": "runPowerShellScript"  
"inputs": {  
  コマンド実行&JSONファイル上書き  
}  
"action": "aws:softwareInventory"
```

AWS Systems Manager カスタムインベントリを使ったマネージドノード上の Log4j ファイル検索

<https://aws.amazon.com/jp/blogs/news/use-aws-systems-manager-custom-inventory-to-locate-log4j-files-on-managed-nodes/>



マルチリージョン、マルチアカウント設定

マルチリージョン、マルチアカウントで横断的にインベントリデータの収集、可視化を行うには各リージョン・アカウントで**インベントリデータ収集の設定**および**リソースデータの同期設定**を実施する必要があります。

インベントリデータ収集の設定

AWS Systems Manager Quick Setup の Host Management を利用する

- Organizations の管理アカウントから実施
- 組織全体、OU 単位でインベントリデータ収集の設定を反映可能
- Inventory の画面から設定する場合と比較して、取得できるインベントリタイプに差異がある※
- カスタムインベントリ等でカスタマイズしたドキュメントを使う場合は、Quick Setup は利用できません

※Quick Setup ホスト管理

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/quick-setup-host-management.html



リソースデータの同期設定

マネージメントコンソールまたは API でリソースデータの同期を各リージョン、アカウントで作成

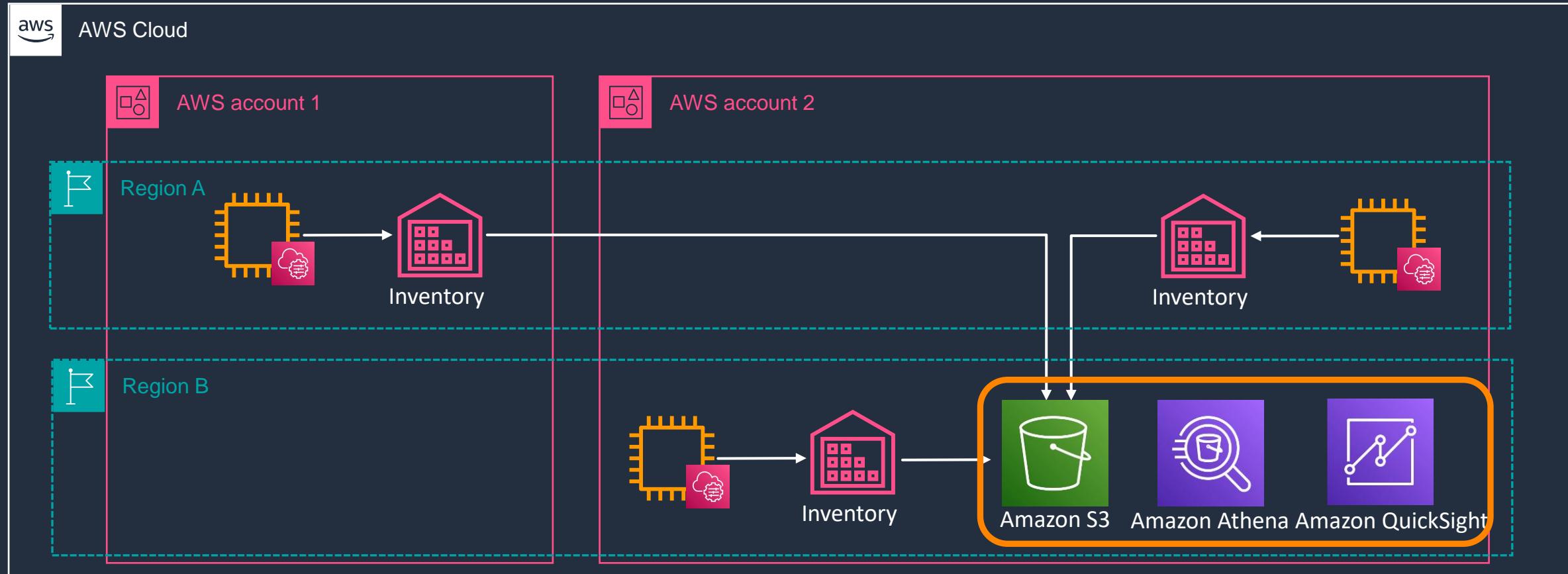
- データを集約する S3 のバケットポリシーにアカウントごとに許可設定を入れる必要あり

リソースデータの同期を作成する API で DestinationDataSharingType=Organization を指定して各リージョン、アカウントで実行

- データを集約する S3 のバケットポリシーには、組織 ID のみを指定

Amazon QuickSight による可視化

リソースデータの同期を設定することでデータが S3 に集約および Amazon Athena のテーブル作成まで行われるため、QuickSight による可視化がすぐに設定可能



Systems Manager & QuickSight ハンズオン

<https://catalog.us-east-1.prod.workshops.aws/workshops/b97f7cb6-0ec4-41c7-97ea-c4156f4f1e0d/ja-JP>

まとめ



まとめ

- Inventory を利用することで、インベントリデータの収集、一元的な管理が可能
 - サーバーに1台ずつ接続して構成情報を確認する運用から解放
- インベントリデータの検索やフィルタリングも可能
 - ダッシュボードの利用またはリソースデータの同期で出力されたデータを Athena や QuickSight で分析も可能
- マルチリージョン、マルチアカウントでインベントリデータの収集が可能

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!



AWS Systems Manager Maintenance Windows 編

AWS Black Belt Online Seminar

小野 卓人

Solutions Architect
2023/09

自己紹介

名前：小野 卓人 (Takuto Ono)

所属：技術統括本部 金融ソリューション本部
保険ソリューション部

経歴：

SIer で金融機関向けシステムの受託開発
インフラ設計・構築・運用保守

現在は、ソリューションアーキテクトとして主に保険業界のお客様を担当

好きなAWSサービス： AWS Systems Manager



本セミナーの対象者

AWS の運用をされている方、これから運用される予定の方

本セミナーの目的

- AWS Systems Manager Maintenance Windows の機能とユースケースをご理解いただく。

本日お話ししないこと

- AWS Systems Manager の全体的な説明
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager Maintenance Windows 以外の機能の詳細
→ 各機能にフォーカスしたセッションを参照ください（今後も続々と公開予定です！）

アジェンダ

1. Maintenance Windows の概要
2. Maintenance Windows の主要な構成要素
3. メンテナンスウィンドウの作成
4. ターゲットの登録
5. タスクの登録
6. 実行結果の確認
7. TIPSとクオータ
8. まとめ

AWS Systems Manager Maintenance Windows の概要

AWS Systems Manager

ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション



AWS Config

Configuration history



Amazon EventBridge

Notification and remediation



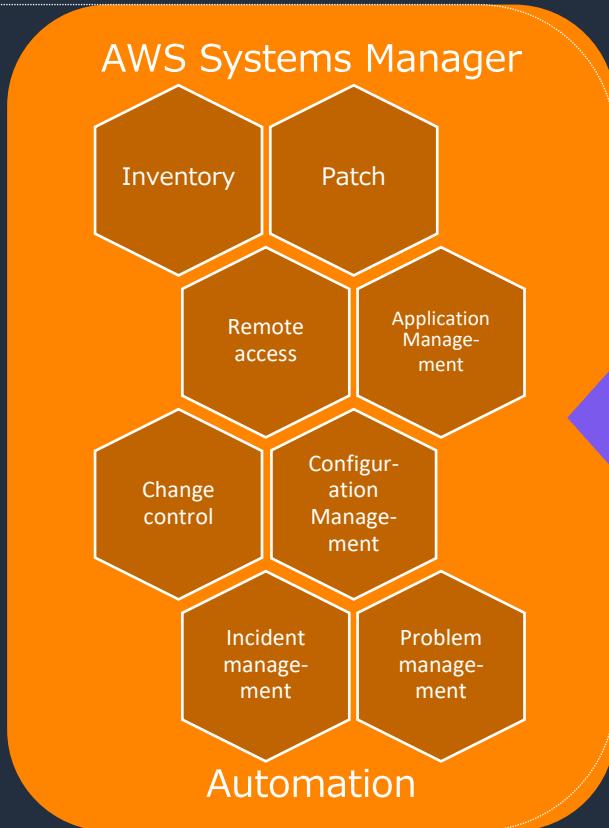
AWS CloudTrail

Audited actions



AWS Identity and Access Management (IAM)

Role-based access control



(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

運用管理

-  Explorer
-  OpsCenter
-  Incident Manager

アプリケーション管理

-  Application Manager
-  AppConfig
-  Parameter Store

変更管理

-  Change Manager
-  Automation
-  Maintenance Windows
-  Change Calendar

ノード管理

-  Fleet Manager
-  Session Manager
-  Inventory
-  Run Command
-  Patch Manager
-  Distributor
- State Manager

Quick Setup

AWS Systems Manager の機能

運用管理

-  Explorer
-  OpsCenter
-  Incident Manager

アプリケーション管理

-  Application Manager
-  AppConfig
-  Parameter Store

変更管理

-  Change Manager
-  Automation
-  Maintenance Windows
-  Change Calendar

ノード管理

-  Fleet Manager
-  Session Manager
-  Inventory
-  Run Command
-  Patch Manager
-  Distributor
-  State Manager

Quick Setup

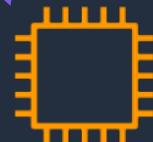
メンテナンスタスクとは

メンテナンスタスクとは？

- OSのパッチ適用
- ソフトウェアのバージョンアップ
- 不要ファイルの削除
- バックアップ
- サービスやサーバの再起動
-

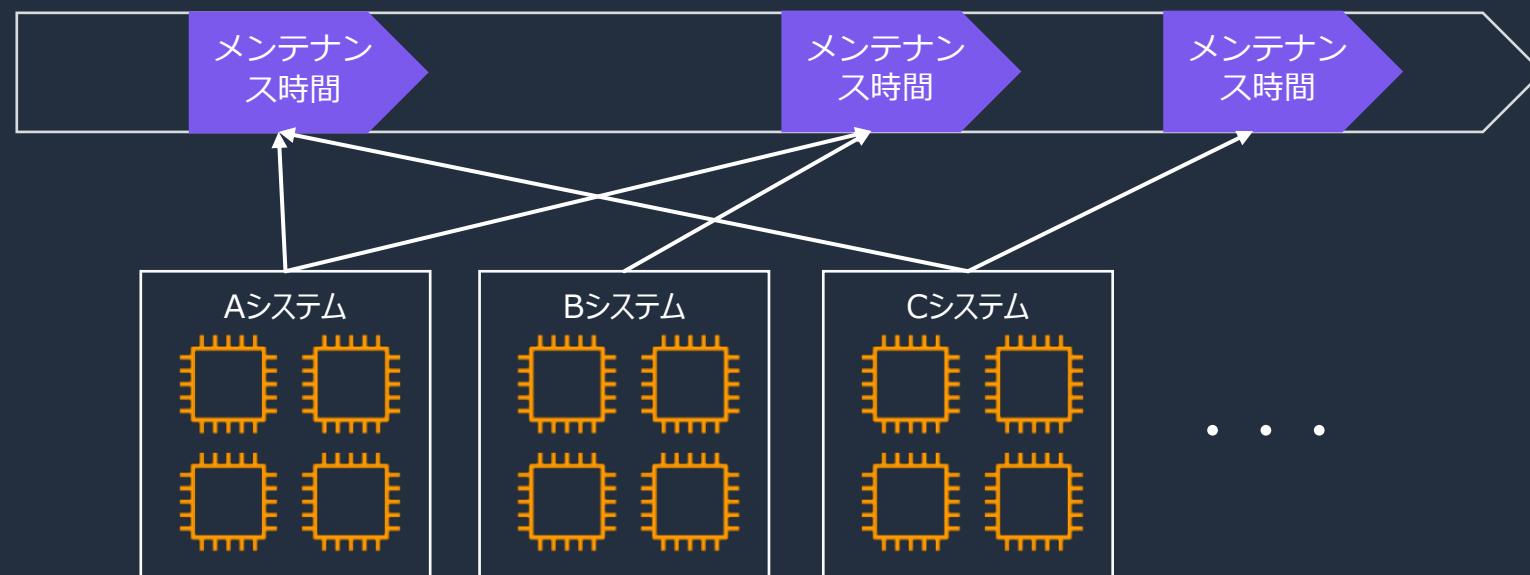
メンテナンスタスクの特徴

- サービス停止を伴う場合がある
- 実施可能な時間帯が決まっている
- 複数のタスクを優先度順に実行したい
- 終了時刻までに完了する必要がある



メンテナンスタスクにおける従来の課題

- ・ システムごとにバラバラなメンテナンス時間
- ・ 大量のメンテナンスタスクの管理
- ・ サーバごとに乱立する Cron ジョブ
- ・ 高機能なジョブスケジューラは高価、そして運用負荷の課題も
- ・ メンテナンス時間内に終わらないメンテナンスタスク …



AWS Systems Manager Maintenance Windows とは



- 管理タスクやメンテナンスタスクを複数のターゲットに実行するための時間枠(=メンテナンスウィンドウ)をスケジュール
 - メンテナンスウィンドウは開始時刻と終了時刻を持ち、複数のタスクを実行可能
 - パッチやアップデートのインストールなどのメンテナンスタスクを行うのに適した時間帯を確実に選択できる
 - Maintenance Windows は追加料金なしでご利用可能

メンテナスウィンドウ				
	詳細の表示	編集	削除	アクション
<input type="checkbox"/>	<input type="text"/> 検索			
<input type="checkbox"/>	ウィンドウ ID	名前	状態	次の実行時間
<input type="checkbox"/>	mw-00ace69c08a271958	mw-resourcegroup	有効	2023年9月15日(金) 2:08:33 UTC
<input type="checkbox"/>	mw-016f4de9ea7fad7d0	mw-parallels-test	無効	-
<input type="checkbox"/>	mw-03a864c53ed6cea9a	maintenance-01	有効	2023年9月15日(金) 2:09:49 UTC
<input type="checkbox"/>	mw-03rd229f376c5363r5	mw-runoff	有効	2023年9月15日(金) 12:08:17 UTC
<input type="checkbox"/>	mw-04			
<input type="checkbox"/>	mw-05			
	説明	タスク	履歴	ターゲット
				タグ
履歴				実行のキャンセル
<input type="checkbox"/>	<input type="text"/> 検索			
	ウィンドウ実行 ID	ステータス	ステータスの詳細	開始時刻
<input type="radio"/>	a2444033-a56d-45f8-9002-6a88324feffa	成功	-	2023年9月15日(金) 2:07:13
<input type="radio"/>	2b39edce-8efd-494f-992d-9ff921daa190	成功	-	2023年9月15日(金) 2:04:12
<input type="radio"/>	cecb014d-696b-4958-a7be-9e62a7fd118a	成功	-	2023年9月15日(金) 2:01:12
<input type="radio"/>	59b30db7-6156-430d-96c2-7113f1aef0ce	成功	-	2023年9月15日(金) 1:58:12
<input type="radio"/>	bf5d285a-0e6e-4577-8e06-01df3775e6bc	成功	-	2023年9月15日(金) 1:55:12
<input type="radio"/>	47917ec8-47f0-447a-b878-7acbb5760649	成功	-	2023年9月15日(金) 1:52:12

Maintenance Windows のユースケース例

マネージドノード上でのメンテナンスタスクの実行

- ・ アプリケーションをインストールまたは更新する
- ・ SSM Agent などのエージェントソフトウェアを更新する
- ・ ドライバーを更新する
- ・ パッチを適用する※

より複雑なタスクの実行

- ・ Automation Runbook を使用して、AMI の作成、ソフトウェアのブートストラップ、ノードの設定を行う
- ・ Step Functions ステートマシンを実行して、ノードを ELB からデタッチし、ノードにパッチを適用してから ELB へアタッチする

※広範囲かつ一元的な OS パッチ適用には Patch Manager の「パッチポリシー」も利用可能です
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-policies.html

State Manager との使い分け



Maintenance Windows

- 開始時刻と終了時刻を持つ「タイムウインドウ」内で複数のタスクを実行
- パッチ適用など、ノードの停止を伴うような変更をスケジュール実行
- SSM ドキュメント以外にも Lambda 関数と Step Functions の実行をサポート

時間的制約のあるタスクを
タイムウインドウ内に実行する



State Manager

- SSM ドキュメントを定期実行し、「定義された状態」を維持するプロセスを自動化
- 「定義された状態」への準拠状況をレポート
- マネージドノードのブートストラップ (Auto Scaling シナリオにも有効)

リソースを定義された状態に維持する



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/state-manager-vs-maintenance-windows.html

(補足) マネージドノードとは

Systems Manager で使用するように設定されたマシン

Maintenance Windows の一部の機能では処理対象のサーバーをマネージドノードにする必要があります。
詳細は、AWS Black Belt Online Seminar の「[AWS Systems Manager Overview](#)」をご覧ください



AWS Systems Manager を使ってサーバ管理を行うためには

サーバを“マネージドノード”にする

ここに一覧で出てくるようになります

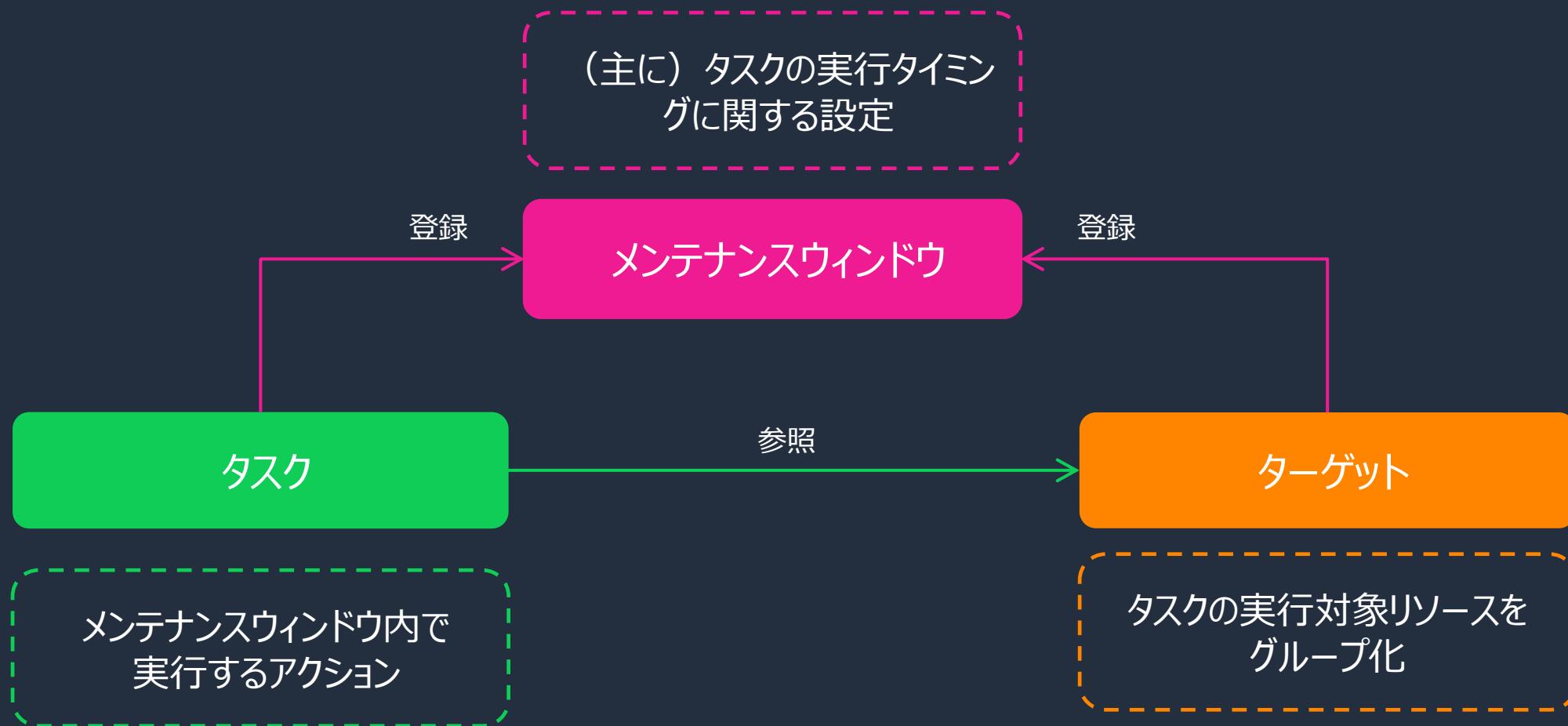
The screenshot shows a table titled "マネージドノード" (Managed Nodes). The table has columns for "ノード ID", "ノードの...", "ノード名", "ラント...", "オペレーティ...", and "ソースタイプ". There are three rows of data:

ノード ID	ノードの...	ノード名	ラント...	オペレーティ...	ソースタイプ
i-04970a7f373ac630b	実行中	LaunchedByS...	Linux	Amazon Linux AMI	EC2 インスタンス
mi-0623bfeef040aa8...	-	On-perm-Linux	Linux	Amazon Linux	AWS::SSM::Manage...
i-016d04a4ae49531af	実行中	instance-ph@	Linux	Amazon Linux	EC2 インスタンス

マネージドノード：
➢ SSM管理下のインスタンス群
➢ EC2インスタンスのほか、
オンプレミスのインスタンスも
含まれられる。

Maintenance Windows の 主要な構成要素

Maintenance Windows の主要な構成要素



メンテナンスウィンドウの作成

メンテナنسウィンドウの作成



メンテナنسウインドウの設定項目(1/4)

- メンテナансウインドウの名前
- 説明

未登録ターゲット

✓ 未登録ターゲットを許可する

メンテナансウインドウに登録されていないマネージドノードもタスクのターゲットとして選択できる

メンテナансウインドウの詳細の入力

名前
このメンテナансウインドウの名前を入力します。

3~128 文字である必要があります。有効な文字は、a~z、A~Z、0~9、_ です。

説明 - オプション
このメンテナансウインドウの説明を入力します。

1~128 文字である必要があります。

未登録ターゲット
このメンテナансウインドウでスケジュールされたメンテナンスタスクに対して、このメンテナансウインドウに現在登録されていないターゲットでの実行を許可します。

未登録ターゲットを許可する

✓ 未登録ターゲットを許可しない

メンテナансウインドウに登録されたターゲットのみをタスクのターゲットとして選択できる

メンテナンスウィンドウの設定項目(2/4)

- スケジュール (Cron/Rate)
- タイムゾーン
- スケジュールのオフセット
 - cron式の場合のみ
 - 1日～6日まで指定可



(補足) Cron 式 / Rate 式

Maintenance Windows / State Manager で使われるスケジュール表記法

- cron 式 … 時間を指定

例) 每月第3火曜日の午後11:30

cron(30 23 ? * TUE#3 *)

- rate 式 … 頻度を指定

例) 15日おき

rate(15 days)

- 1回限りのスケジュール実行

例) 2023年9月20日15時55分

at(2023-09-20T15:55:00)

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/reference-cron-and-rate-expressions.html



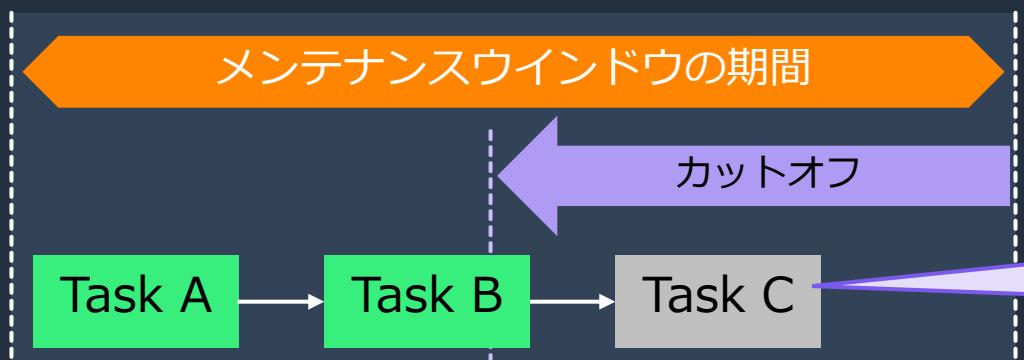
© 2023, Amazon Web Services, Inc. or its affiliates.

メンテナنسウインドウの設定項目(3/4)

- メンテナスウインドウの期間
- タスクの開始を停止する時間（カットオフ）
ウインドウの終了時刻より前にタスクの開始を抑止する時間
- ウインドウの開始日、終了日
メンテナスウインドウをアクティブにする期間

メンテナスウインドウの
開始時刻

メンテナスウインドウの
終了時刻



期間
メンテナスウインドウの期間です
 時間
1~24 の値です。

タスクの開始を停止する
メンテナスウインドウの終了前にスケジュールされたタスクが開始されることを停止する時間です
 ウィンドウが閉じるまでの時間
0~23 の値です。

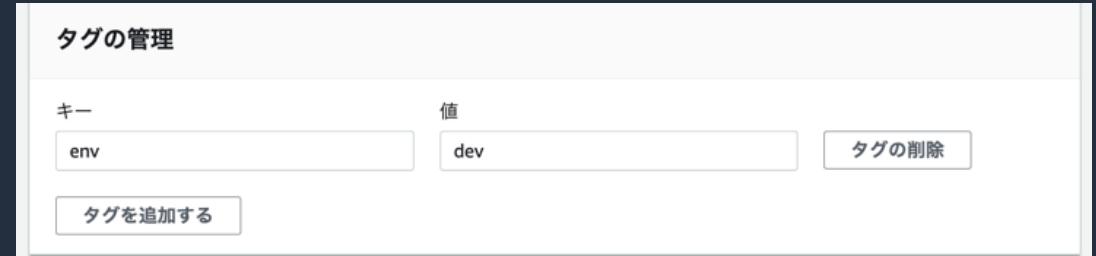
ウィンドウ開始日 - オプション
メンテナスウインドウの開始日時
YYYY/MM/DD hh:mm:ss ▾

ウィンドウ終了日 - オプション
メンテナスウиндウの停止日時
YYYY/MM/DD hh:mm:ss ▾

カットオフタイム以降の
タスク開始は抑止される
(※タスクの設定にも依存)

メンテナنسウインドウの設定項目(4/4)

- メンテナансウインドウの作成時または作成後、メンテナансウインドウにタグを付与できる



- メンテナансウインドウの作成後、有効化・無効化の設定変更が可能

ウィンドウ ID: mw-0462ab96320ecaf9c

説明 | タスク | 補助 | ターゲット | タグ

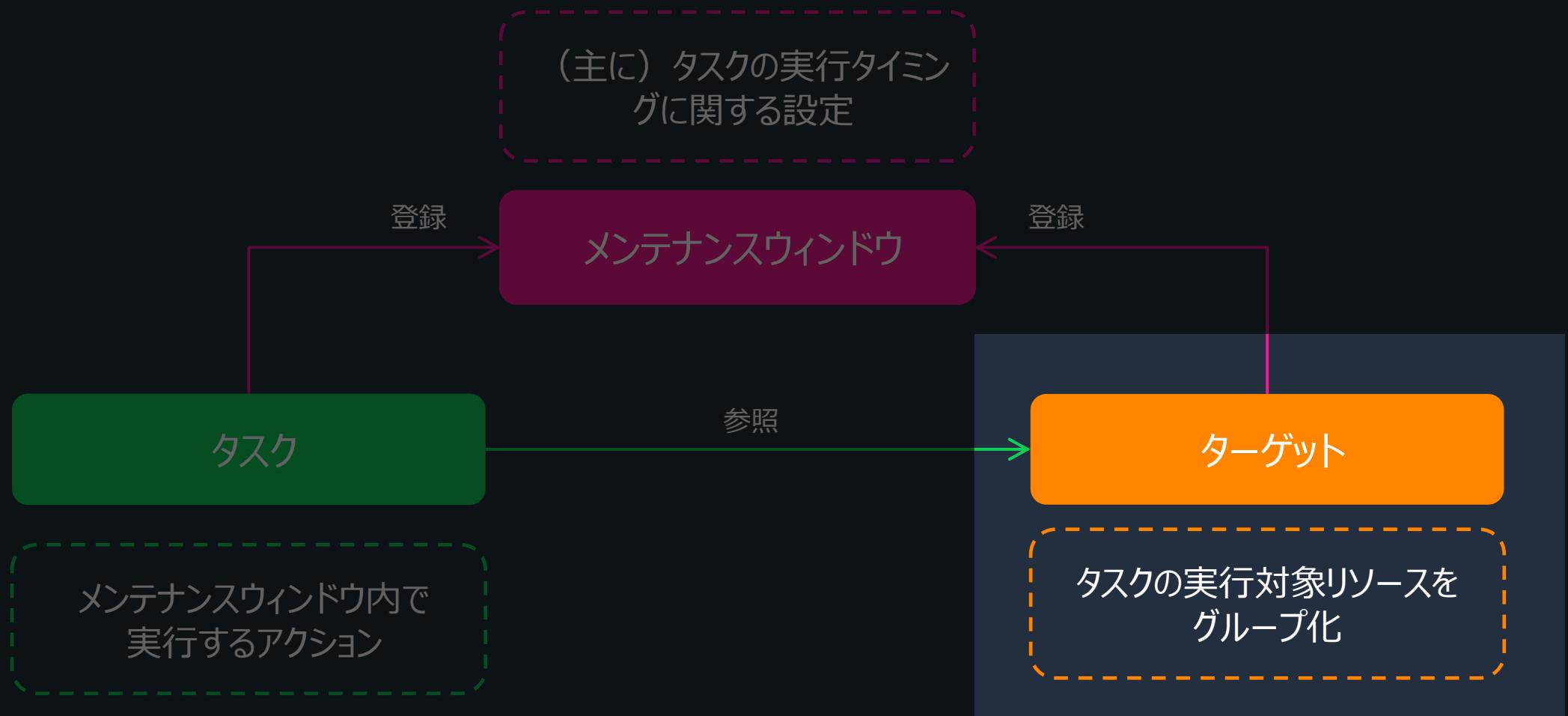
名前: test-mw
状態: 有効
期間: 3 hours
カットオフポイント: ウィンドウが閉じるまで 1 hours
ウィンドウ開始日: 2023年8月31日(木) 0:00:00 UTC
ウィンドウ終了日: -
未登録ターゲットを許可する: はい

アクション ▾

ターゲットの登録
Run Command タスクの登録
オートメーションタスクの登録
Lambda タスクの登録
Step Functions タスクの登録
メンテナансウインドウの有効化
メンテナансウインドウの無効化

ターゲットの登録

ターゲットの登録



Maintenance Windows のターゲット

- タスクが処理対象とすることのできるリソースのグループ
- ターゲットにはマネージドノードまたはその他の AWS リソースを含めることができる
- メンテナンスウィンドウあたり最大 100 のターゲットを登録可能
- ターゲットあたり以下の設定が可能
 - ✓ 5つまでのタグキーまたはタグキーと値のペア または
 - ✓ 最大 50 のマネージドノードID または
 - ✓ 1つのリソースグループ

ターゲットの選択方法

インスタンスタグを指定

対象はマネージドノード

1つ以上のタグキーと値（オプション）を指定することで、該当するタグが付与されているマネージドノードを対象にできる

インスタンスを手動で選択

対象はマネージドノード

複数のマネージドノードのIDを直接指定

リソースグループを選択

対象は AWS リソース

- 選択したリソースグループに含まれる AWS リソースを対象にできる
- リソースタイプによるフィルタも可能
- タスクが対応していないリソースタイプが含まれる場合、エラーがレポートされる場合がある

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-maintenance-assign-targets.html

ターゲットの設定項目(1/2)

- ターゲット名
- 説明
- 所有者情報
 - ✓ このターゲットに対してタスクを実行する際に発生する EventBridge イベントに所有者情報が含まれる

Register target

Assign a set of instances to your maintenance window. You can choose to target by a tag group or managed instances.

Maintenance window target details

Maintenance window
mw-00ace69c08a271958

Target name - オプション

It has to be between 3 and 128 characters. Valid characters contain the following: a-z, A-Z, 0-9, and _-

Description - オプション

It has to be between 1 to 128 characters.

Owner information - オプション

It has to be between 1 to 128 characters.

ターゲットの設定項目(2/2)

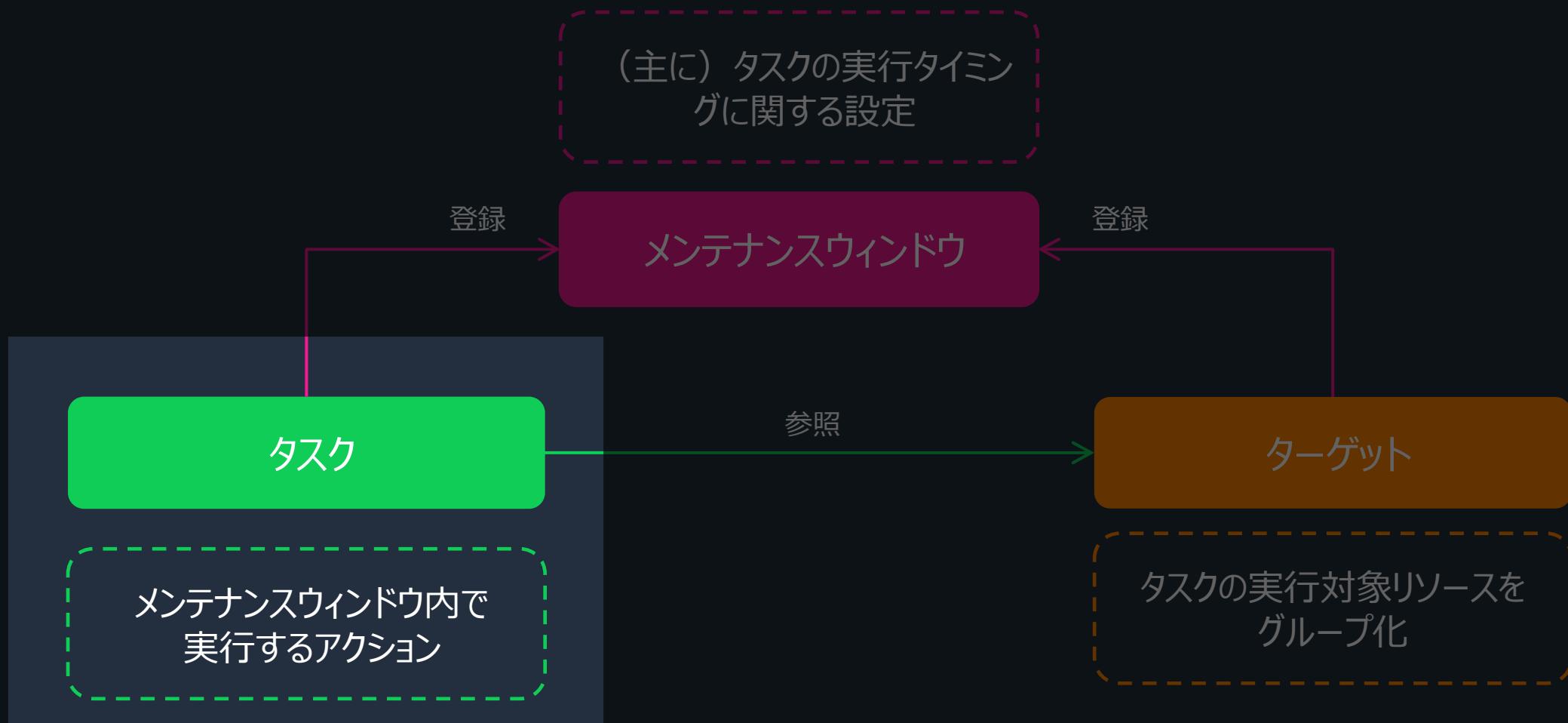
ターゲットの選択方法は3種類

- ・ インスタンスタグを指定
- ・ インスタンスを手動で選択
- ・ リソースグループを選択



タスクの登録

タスクの登録



Maintenance Windows のタスク

- ・ タスクとは、メンテナンスウィンドウ内で実行したい処理
- ・ メンテナンスウィンドウあたり最大 20 のタスクを登録できる
- ・ タスクの種類としてサポートしているのは以下の 4つ

SSM Run Command

SSM Automation Runbook

Lambda 関数

Step Functions ステートマシン

タスクの共通設定項目(1/5)

- タスク名
- 説明
- 新しいタスク呼び出しのカットオフ
 - ✓ 有効の場合、メンテナスウィンドウのカットオフ 時間に達した後のタスクを実行しない



メンテナスウィンドウタスクの詳細

メンテナスウィンドウ

mw-0462ab96320ecaf9c

名前 - オプション

runcommand

3~128 文字である必要があります。有効な文字は、a~z、A~Z、0~9、_ です。

説明 - オプション

1~128 文字である必要があります。

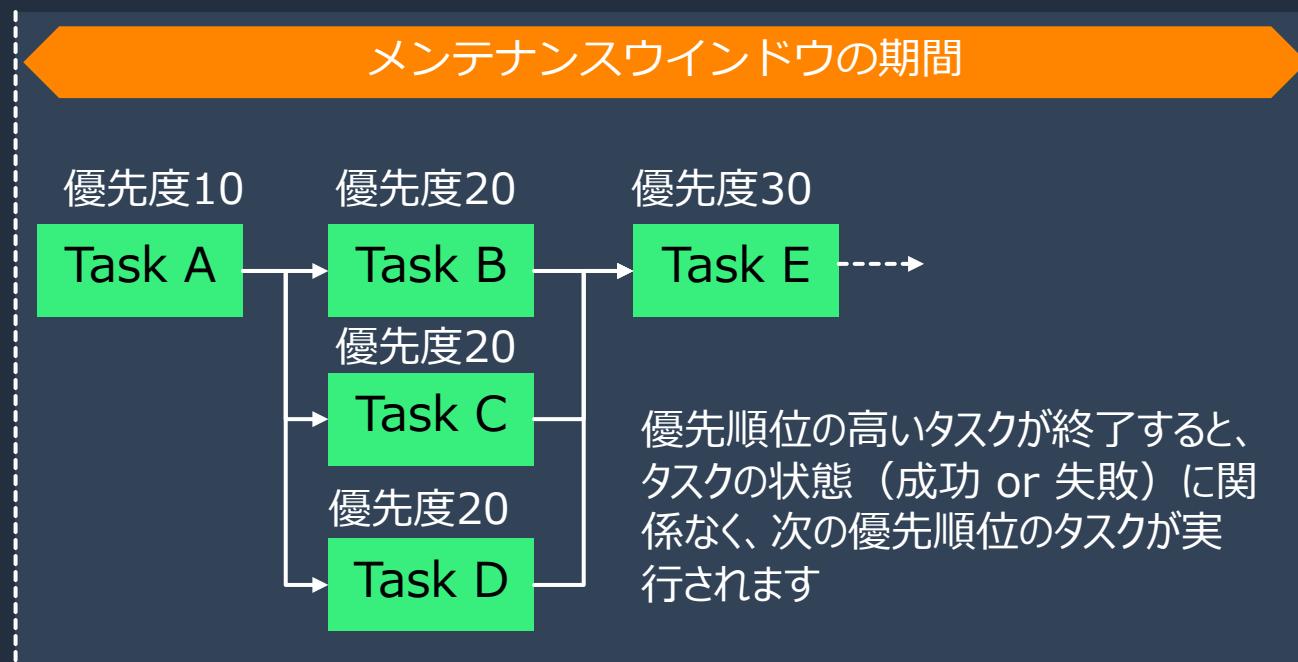
New task invocation cutoff - オプション

Prevent new task invocations from starting when the maintenance window cutoff time is reached.

Enabled

タスクの共通設定項目(2/5)

- タスク優先度
 - 0以上の整数を指定
 - 数値の小さいタスクから順に実行される
 - 優先度の同じタスクは並列実行



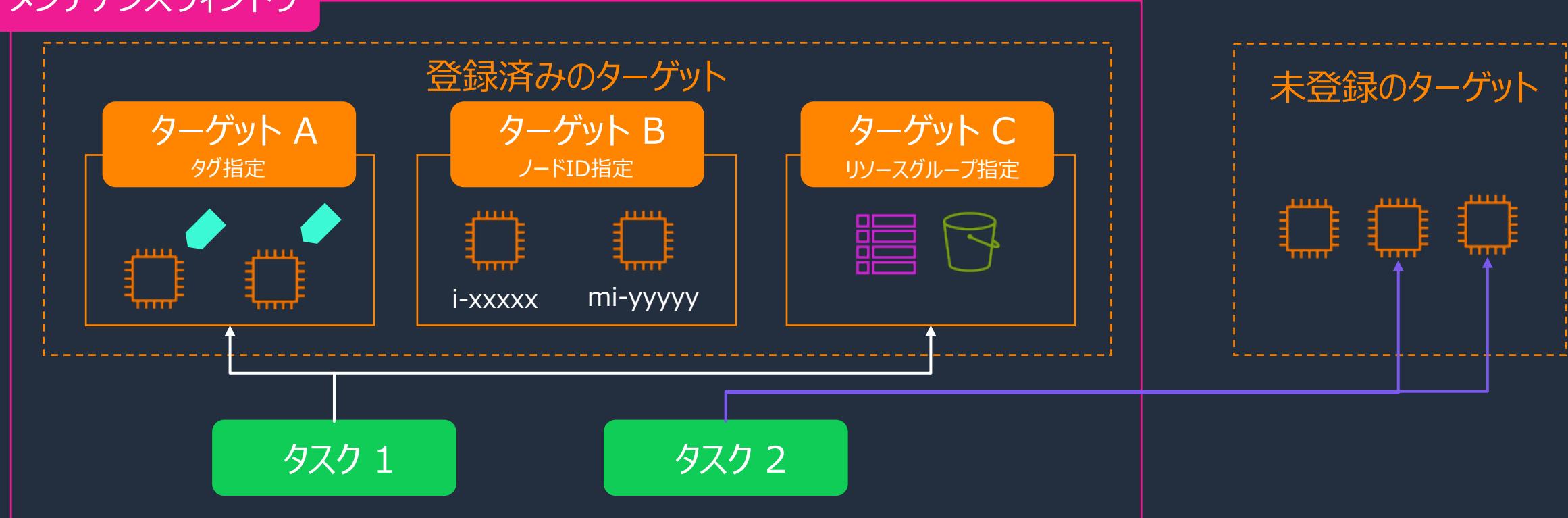
タスクの共通設定項目(3/5)

- ターゲット
 - タスクの処理対象を指定する
 - ✓ Run Command → ターゲットの指定は必須
 - ✓ それ以外のタスクタイプ → ターゲットの指定は任意
 - ターゲットの指定方法は3種類
 1. 登録済みターゲットグループの中から選択
 2. マネージドノードの中から選択（メンテナンスウインドウが許可している場合）
 3. ターゲットを指定しない（Run Command 以外の場合）



(補足) タスクにおけるターゲット設定

メンテナنسウィンドウ



1. 登録済みターゲットグループの中から選択
2. マネージドノードの中から選択
3. ターゲットを指定しない (Run Command 以外の場合)

タスクの共通設定項目(4/5)

- レート制御
タスクに対してターゲットを指定した場合、レート制御の設定によって処理対象の同時実行を制御する



同時実行数

- 同時に処理を実行する処理対象リソースの数、または割合を指定

エラーのしきい値

- この値を超えてタスクが失敗したらそのタスクの停止を指示する
- ※後続のタスクへは影響しない

タスクの共通設定項目(5/5)

- IAM サービスロール
 - Systems Manager がユーザに代わってタスクを実行するためのサービスロールを指定する
 - あらかじめカスタムサービスロールを作成しておく必要あり
 - IAM サービスロールを指定しない場合、**AWSServiceRoleForAmazonSSM** という IAM ロールが使用される
 - ✓ デフォルトのロールを使用する場合、タスクとして実行する Lambda 関数および Step Functions ステータクションの名前は SSM で開始する必要あり
 - ✓ デフォルトのロールではなく、必要な権限を絞ったカスタムロールの利用が推奨

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-maintenance-perm-console.html#sysman-maintenance-role



その他の設定項目

- 出力オプション (Run Command のみ)
 - コマンド出力を S3 バケットへ書き込む
 - コマンド出力を CloudWatch Logs へ書き込む
- SNS 通知 (Run Command のみ)
 - タスクの実行状況に応じてイベント通知する
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/monitoring-sns-mw-register.html
- CloudWatch アラーム (Run Command 、 Automation のみ)
 - アラーム状態の場合にタスクの実行をスキップする

実行結果の確認方法

実行結果の確認 - コンソール画面

ウィンドウ ID: mw-03a864c53ed6cea9a

説明 タスク **履歴** ターゲット タグ

履歴

実行のキャンセル 詳細の表示

ウィンドウ実行 ID	ステータス	ステータスの詳細	開始時刻	終了時刻
acb5b629-755b-4587-9e71-e8b1ac52daf1	成功	-	2023年8月15日(火) 14:00:31 UTC	2023年8月15日(火) 14:00:31 UTC
86400e81-4ca8-49b0-9cc5-88c3af132997	成功	-	2023年8月15日(火) 13:30:31 UTC	2023年8月15日(火) 13:30:31 UTC
bc83f7fe-3963-4b65-9885-830767d3d32c	成功	-	2023年8月15日(火) 13:00:31 UTC	2023年8月15日(火) 13:00:31 UTC
c8e978a9-ff01-4d7d-b528-7c3ae7f4dbd8	成功	-	2023年8月15日(火) 12:30:31 UTC	2023年8月15日(火) 12:30:31 UTC
5b18b58f-95d4-4190-98a2-7c4a8c0fc08	成功	-	2023年8月15日(火) 12:00:31 UTC	2023年8月15日(火) 12:00:31 UTC
315c8380-64ef-4460-8bba-5aaa9684c984	成功	-	2023年8月15日(火) 11:30:31 UTC	2023年8月15日(火) 11:30:31 UTC

View execution history

The following tasks were run on this execution of maintenance window mw-00ace69c08a271958

Execution Details

Maintenance window mw-00ace69c08a271958	Run ID 74be35cc-dd86-48a2-9670-4d2bed09e8f0
Start time 2023年9月15日(金) 4:21:05 UTC	End time 2023年9月15日(金) 4:25:19 UTC

Execution Tasks

ID	Task ARN	Status	Status details	Start time	End time
7b158a5-b5df-4e9f-9d4a-e1219203b206	AWS-RestartEC2Instance	成功	-	2023年9月15日(金) 4:21:05 UTC	2023年9月15日(金) 4:25:18 UTC
c83b6a1-d027-4c0f-872f-03700cdc8ede	AWS-RunShellScript	成功	-	2023年9月15日(金) 4:21:05 UTC	2023年9月15日(金) 4:21:10 UTC
d6032b43-34d6-4499-b3bb-655973a92ed8	arn:aws:lambda:ap-northeast-1:020928153945:function:SSM-helloworld	成功	-	2023年9月15日(金) 4:25:18 UTC	2023年9月15日(金) 4:25:19 UTC

タスク呼び出し

ID	ステータス	ステータスの詳細	開始時刻	終了時刻	所有者情報
09680ac8-151d-4000-ad7e-07ffa0e05385	成功	-	2023年9月15日(金) 4:25:18 UTC	2023年9月15日(金) 4:25:19 UTC	-
c8c9a4d1-9424-4d0d-9b2-94b1df8eecc5	成功	-	2023年9月15日(金) 4:25:18 UTC	2023年9月15日(金) 4:25:18 UTC	-
d11a2297-44d4-4dda-a691-fe6c505b457b	成功	-	2023年9月15日(金) 4:25:18 UTC	2023年9月15日(金) 4:25:18 UTC	-

aws

© 2023, Amazon Web Services, Inc. or its affiliates.

41

TIPSとクオータ

疑似パラメータ

- タスク実行時、メンテナンスウィンドウの実行 ID やターゲットとなるリソースの ID などの情報を動的に参照できる機能
- タスク登録時に疑似パラメータ構文を使用して設定する

<疑似パラメータ構文>

`{{疑似パラメータ名}}`

<疑似パラメータの例>

実行対象のリソースのID（ここではインスタンスID）を参照する疑似パラメータ

入力パラメータ		
変数名	説明	値
InstanceId		<code>{{RESOURCE_ID}}</code>
BucketName		<code>test-bucket-name</code>

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/mw-cli-register-tasks-parameters.html

Systems Manager のメンテナンスウィンドウでオートメーションタスクを登録するときに擬似パラメータを追加するにはどうすればよいですか？

<https://repost.aws/ja/knowledge-center/ssm-maintenance-window-pseudo-parameter>

サポートされる疑似パラメータ

疑似パラメータ	説明
WINDOW_ID	メンテナンスウインドウのID
WINDOW_TASK_ID	実行されるタスクのID
WINDOW_TARGET_ID	実行対象のターゲットID
WINDOW_EXECUTION_ID	メンテナンスウインドウの実行ID
TASK_EXECUTION_ID	タスクの実行ID
INVOCATION_ID	タスク実行におけるターゲットごとの呼び出しID
TARGET_TYPE	ターゲットのタイプ。 RESOURCE_GROUP や INSTANCE がセットされる
TARGET_ID	<ul style="list-style-type: none">リソースの完全な ARN (TARGET_TYPE が RESOURCE_GROUP の場合)インスタンスの ID (TARGET_TYPE が INSTANCE の場合) <p>※Run Command タスクでは未サポート</p>
RESOURCE_ID	リソースグループに含まれるリソースタイプの短い ID (EC2 のインスタンス ID や DynamoDB のテーブル名、S3 のバケット名 など) ※Run Command タスクでは未サポート

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/mw-cli-register-tasks-parameters.html



Maintenance Windows のクオータ

項目	クオータ	上限緩和申請
AWSアカウントごとのメンテナنسウインドウ	50	可
メンテナансウインドウごとのタスク数	20	可
メンテナансウインドウごとのターゲット数	100	可
ターゲットごとのインスタンスID	50	
タスクごとのターゲット	10	
1つのメンテナансウインドウの同時実行数	1	
異なるメンテナансウインドウの同時実行数	5	可
実行履歴の保持	30 日間	

https://docs.aws.amazon.com/ja_jp/general/latest/gr/ssm.html#limits_ssm



State Manager との比較 (1/2)

機能	Maintenance Windows	State Manager
主な目的	タイムウインドウ内でのタスクの実行	ポリシーの維持
タスク	<ul style="list-style-type: none">Command ドキュメントAutomation RunbookLambda 関数Step Functions	<ul style="list-style-type: none">Command ドキュメントAutomation RunbookPolicy ドキュメント
タスクの数	メンテナンスウィンドウあたり最大20タスク	関連付けあたり1タスク
タスクの優先度付け	可能	不可
スケジュール	Rate/Cron によるスケジュール起動 ※Cron 式での月の指定も可能	Rate/Cron/スケジュール無し/オンデマンド実行 ※ノードの状態によってはスケジュール外で実行される場合あり



State Manager との比較 (2/2)

機能	Maintenance Windows	State Manager
ターゲット	<ul style="list-style-type: none">タグ、ノードID指定、リソースグループタスクによってはターゲットを指定しないことも可能複数のターゲット設定をタスクへ割り当てることも可能	<ul style="list-style-type: none">タグ、ノードID指定、リソースグループ、全マネージドノード
スケジュールのタイムゾーン指定	可	不可
SSM Compliance との連携	不可	可
有効化／無効化	可（期間を指定したアクティブ化/非アクティブ化も可）	不可

Systems Manager State Manager の Black Belt 資料もご参照ください
<https://aws.amazon.com/jp/events/aws-event-resource/archive/>

まとめ

まとめ

Systems Manager Maintenance Windows の特徴

- 開始時刻と終了時刻を持つ「メンテナンスウインドウ」をスケジュールするサービス
- メンテナンスウインドウでは優先度に応じて複数のタスクを複数のターゲットへ実行
- メンテナンスウインドウの終了時に間に合わない可能性のあるタスクの起動を抑止
- Command ドキュメントや Automation Runbook のほか、Lambda 関数や Step Functions ステートマシン の定期実行が可能

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
- ・ 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>



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

内容についての注意点

- ・ 本資料では資料作成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。AWS のサービスは常にアップデートを続けているため、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
- ・ 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
- ・ 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）



Thank you!



AWS Systems Manager Overview

AWS Black Belt Online Seminar

石橋 香代子

Senior 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02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：石橋 香代子

所属：エンタープライズ技術本部
小売・消費財ソリューション部

経歴：-2018/06 @外資SIer
2018/07- ソリューションアーキテクト @AWS
• 小売・消費財のお客様を担当
• Cloud Operations サービスの推進も



好きなAWSサービス：AWS Systems Manager

本セミナーの対象者

AWS の運用をされている方、これから運用される予定の方

本セミナーの目的

- AWS Systems Manager の全体像をご理解いただく。
- AWS Systems Manager の各機能の概要を掴んでいただき、どんなことができるのか、イメージを持っていただく。

本日お話ししないこと

- AWS Systems Manager の各機能の詳細
- 今後公開を予定している、各機能にフォーカスしたセッションをお待ちください。

アジェンダ

1. 運用管理における課題と AWS Systems Manager
2. AWS Systems Manager を使うには？
3. AWS Systems Manager で始める運用管理
4. 3rd Party の ITSM ツールとの連携
5. まとめ

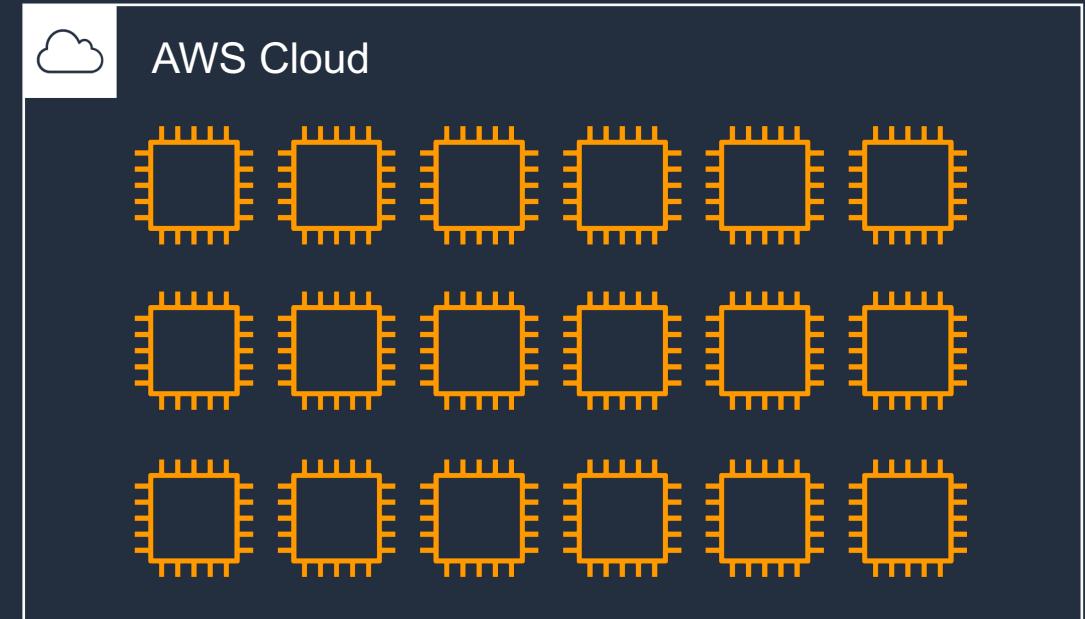
運用管理における課題と AWS Systems Manager

運用管理における課題

使い始め

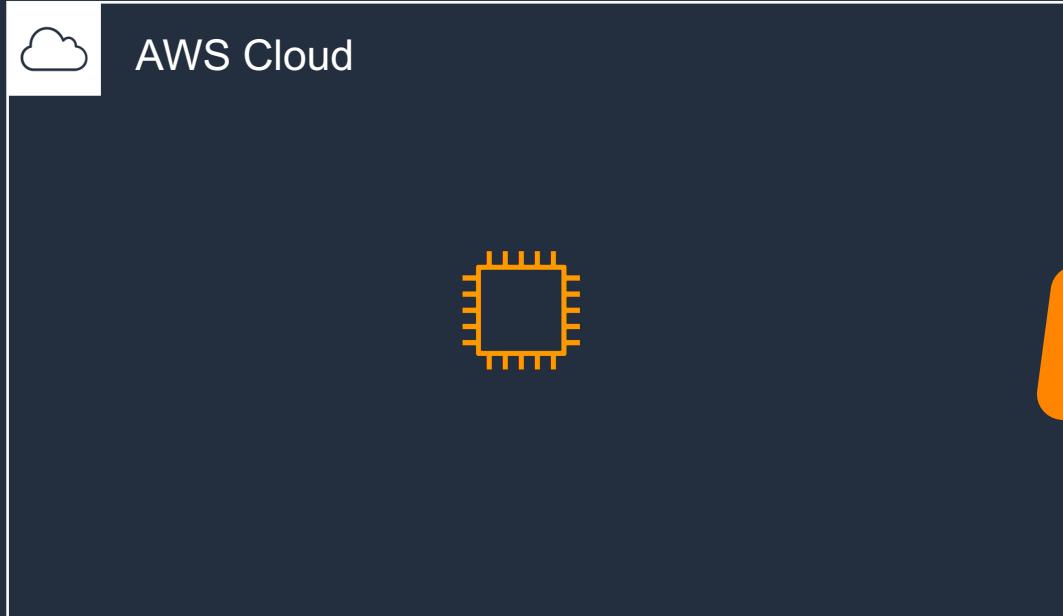


利用が進むと

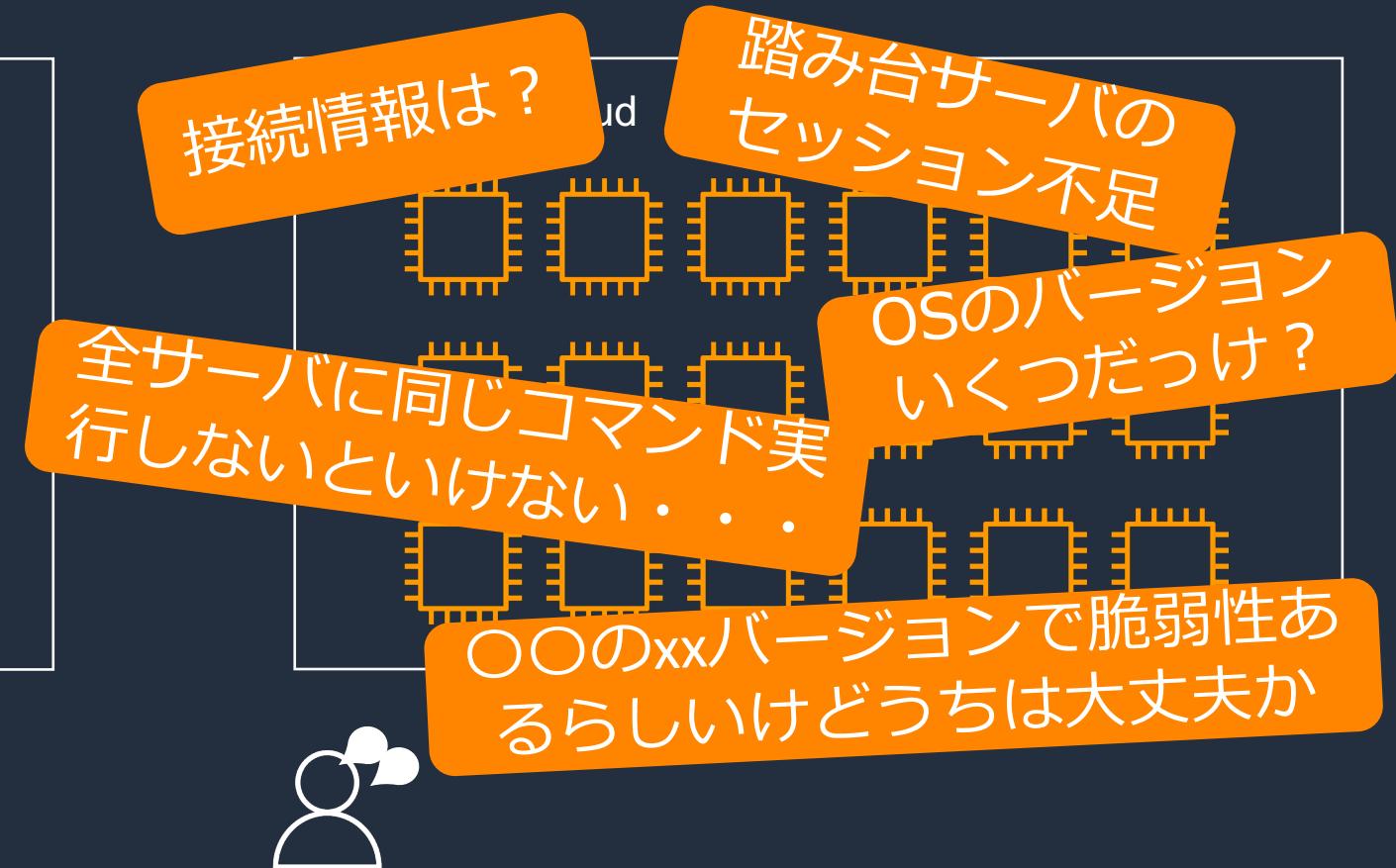


運用管理における課題

使い始め

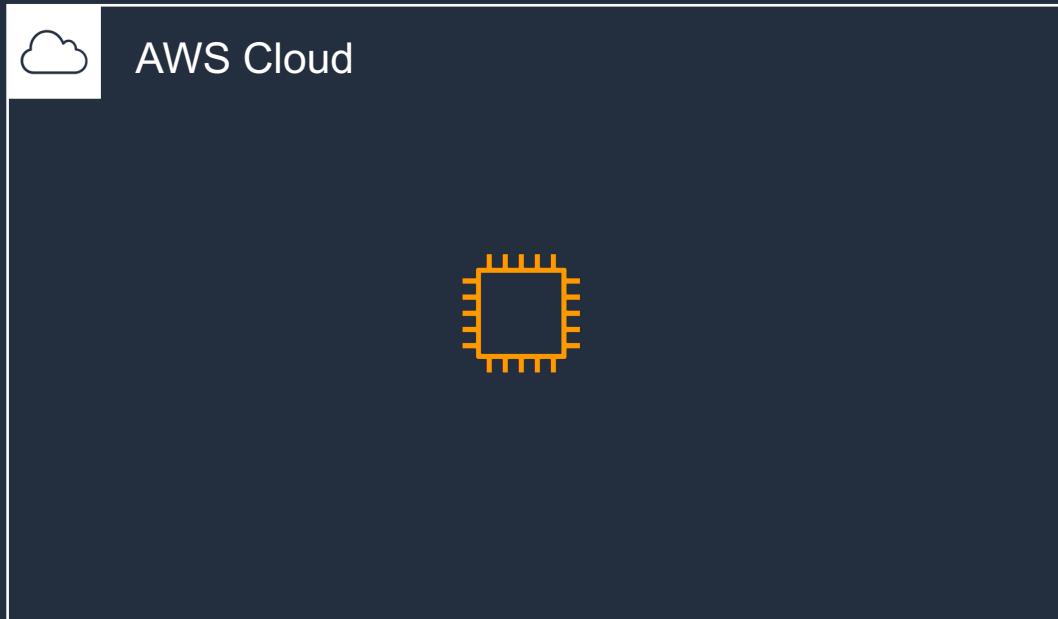


利用が進むと



運用管理における課題

使い始め

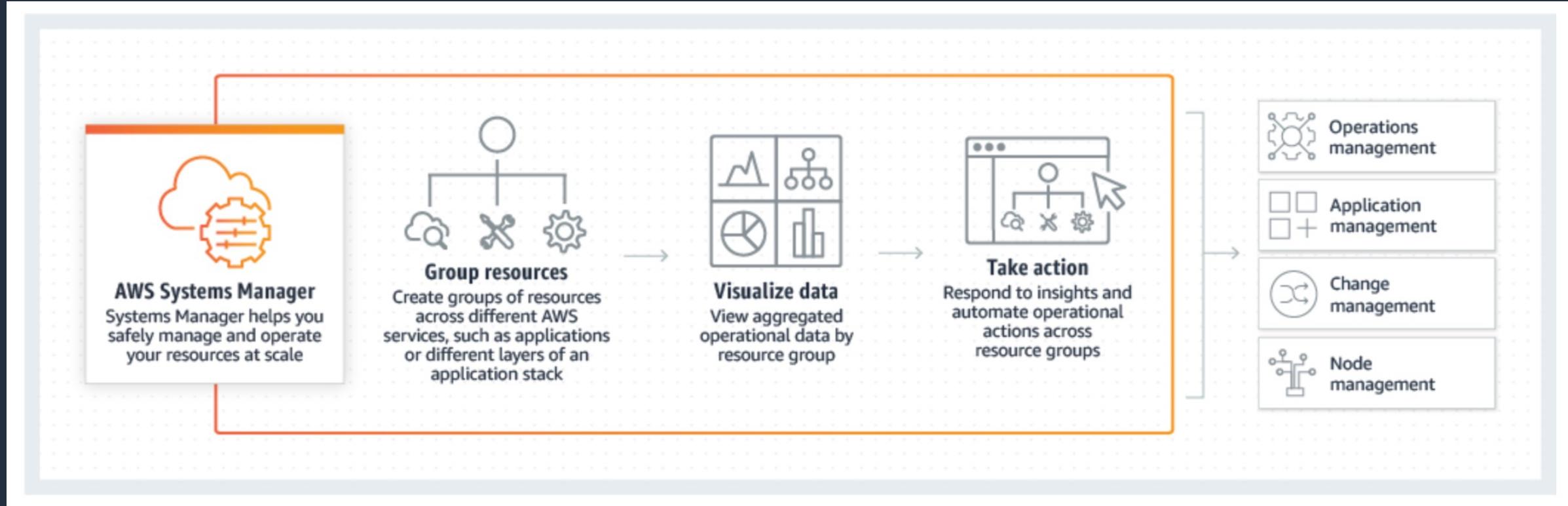


利用が進むと



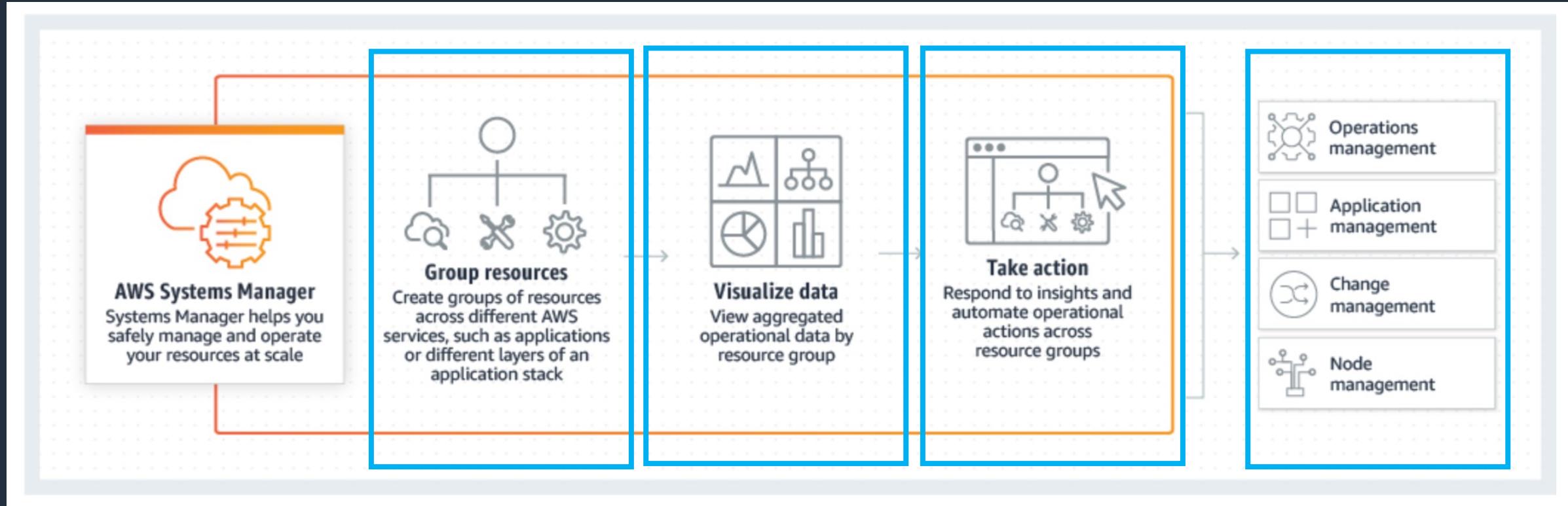
AWS Systems Manager (SSM) とは

ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション



AWS Systems Manager (SSM) とは

ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション



AWS Systems Manager (SSM) とは



AWS Config
Configuration history



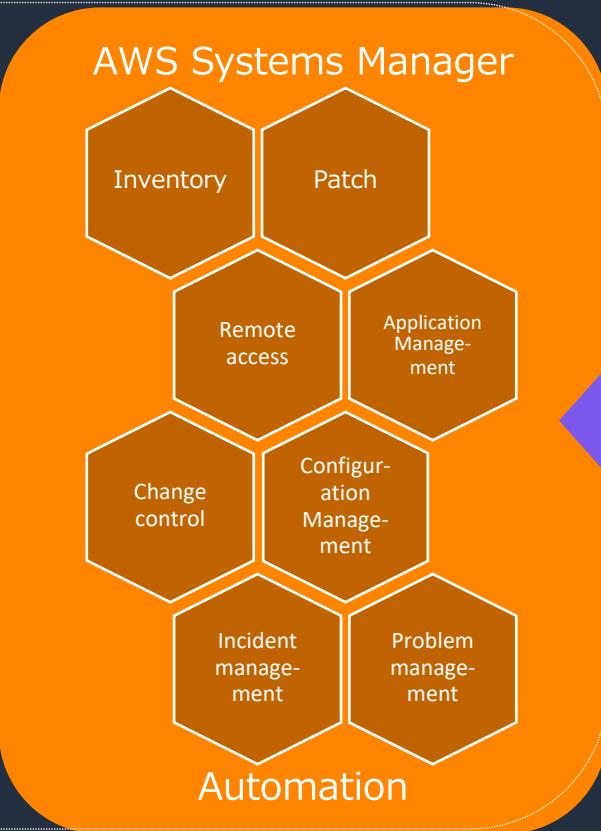
Amazon EventBridge
Notification and remediation



AWS CloudTrail
Audited actions



AWS Identity and Access Management (IAM)
Role-based access control



Cloud



On-premises



Edge

Integration
connectors
and APIs

- Third-party tools
- ITSM
- Custom solutions

AWS の他のサービスや
3rd Party のツールと統合された
管理ソリューションを提供

(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

運用管理	アプリケーション管理	変更管理	ノード管理
 Explorer	 Application Manager	 Change Manager	 Fleet Manager
 OpsCenter	 AppConfig	 Automation	 Session Manager
 Incident Manager	 Parameter Store	 Maintenance Windows	 Inventory
		 Change Calendar	 Run Command
			 Patch Manager
			 Distributor
			 State Manager

Quick Setup

AWS Systems Manager を使うには？

AWS Systems Manager を使ってサーバ管理を行うためには

サーバを“マネージドノード”にする

ここに一覧で出てくるようになります

□	ノード ID	ノードの... ▾	ノード名	プラット... ▾	オペレーティ... ▾	ソースタイプ	ソ...
□	i-04970a7f373ac630b	実行中	LaunchedByS...	Linux	Amazon Linux AMI	EC2 インスタンス	-
□	mi-0623bfeef040aa8...	-	On-perm-Linux	Linux	Amazon Linux	AWS::SSM::Manage...	-
□	i-016d04a4ae49531af	実行中	instance-ph@	Linux	Amazon Linux	EC2 インスタンス	-

マネージドノード：
➤ SSM管理下のインスタンス群
➤ EC2インスタンスのほか、
オンプレミスのインスタンスも
含まれられる。

マネージドノードにするために ①SSM Agent の導入

- SSM Agent が Systems Manager と連携し各種操作、コントロールを行う。
- Amazon Linux やWindows、Ubuntu などの一部のオフィシャルイメージ(AMIs) には導入済み
 - プリインストールされたAMIsの一覧は[こちら](#)
- それ以外のAMI、及びオンプレミスサーバは、手動でインストール



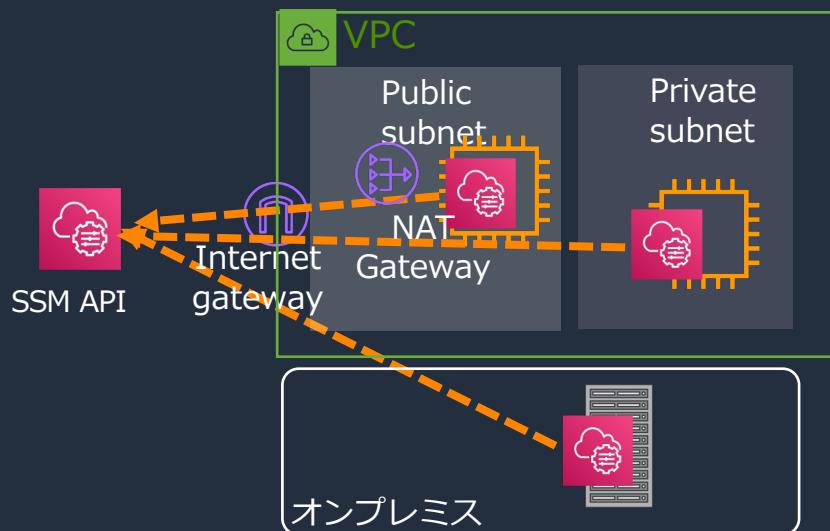
aws SSMS Agent の詳細は[こちら](#)

マネージドノードにするために ②アウトバウンド経路確保

- 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。
- インバウンドアクセスは不要

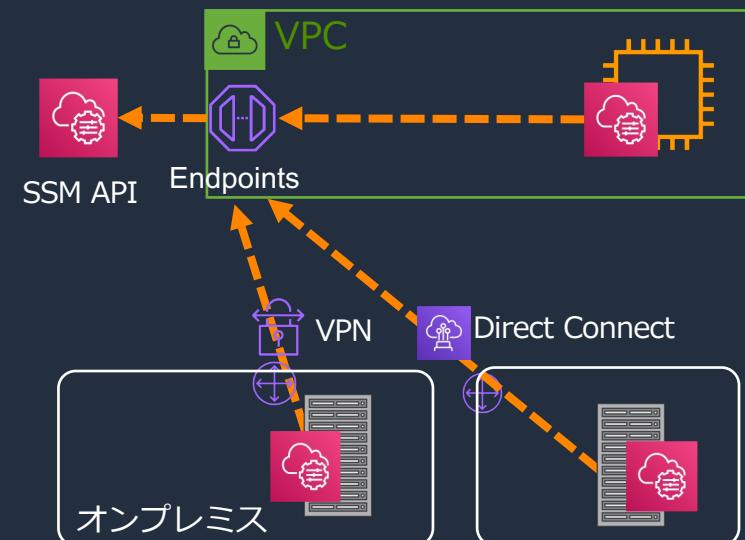
1. インターネット経由

- ・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
- ・オンプレミスからも AWS Direct Connect や
VPN 経由で閉域網経由のアクセスが可能



マネージドノードにするために ③権限付与

- Systems Manager に接続するための権限を付与する。
付与方法は以下の二通り。
- (方法 1) Systems Manager の管理下におきたい EC2 に明示的に付与 (従来の方法)
 - IAM ロールを作成し、EC2 にアタッチする。
 - 1, IAMポリシーについては、まず「AmazonSSMManagedInstanceCore」でコア機能をアタッチ(必須)
 - 2, 必要に応じて、S3などのポリシーをアタッチ(option)
- (方法 2) 「デフォルトのホスト管理設定(DHMC)」を有効にし、アカウント内の全 EC2 を自動で管理下にする。 (次ページ)



デフォルトのホスト管理設定

Default Host Management Configuration (DHMC)



- 明示的に EC2 にロール付与せずとも、 Systems Manager がアカウント内のすべてのインスタンスを管理する権限を持つようにできる機能
 - 設定は、アカウントごと、リージョンごとの単位
 - DHMC で指定したロールを SSM Agent が使用する。
 - デフォルトで「AWSSystemsManagerDefaultEC2InstanceManagementRole」が用意
 - EC2 にロールがアタッチされている場合には、 SSM Agent はまずそれを使用しようとする。
- 対象の EC2 は、以下が前提
 - SSM Agent は Ver.3.2.582.0 以降がインストールされていること
 - Instance Metadata Service Version 2 (IMDSv2) が有効化されていること

この機能により、自動で全インスタンスをマネージドノードにすることが可能に！



DHMCについての詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

マネージドノードまでの 3ステップ まとめ



1、SSM Agentの導入

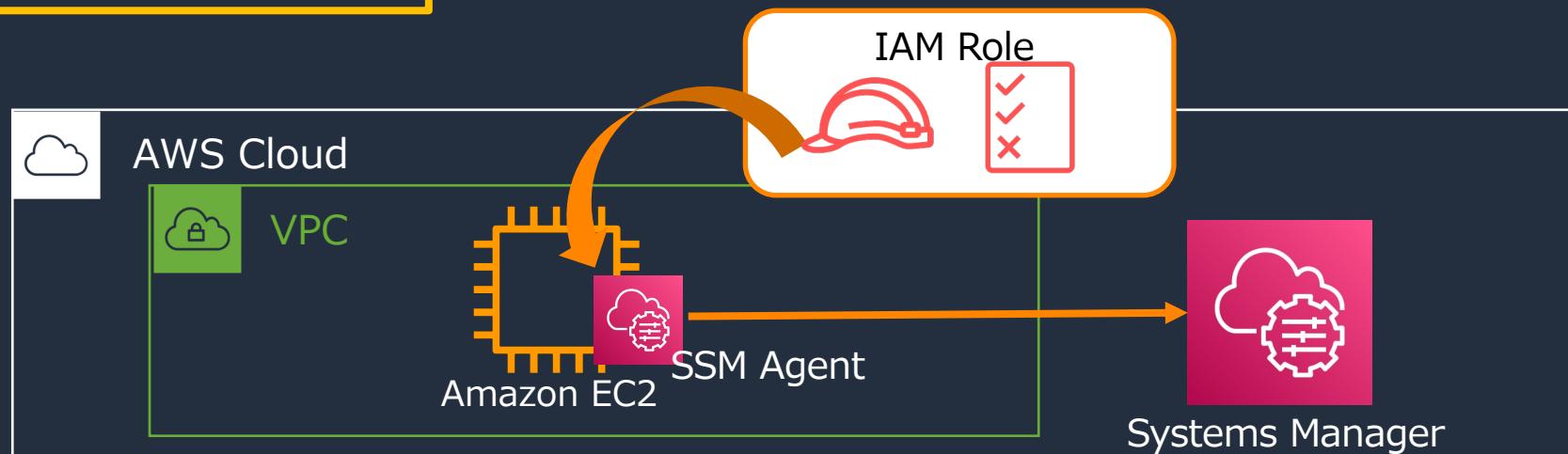
- ✓ SSM Agent が Systems Manager と連携して動作する
- ✓ 一部のオフィシャルイメージにはプリインストール済み

2、アウトバウンド経路の確保

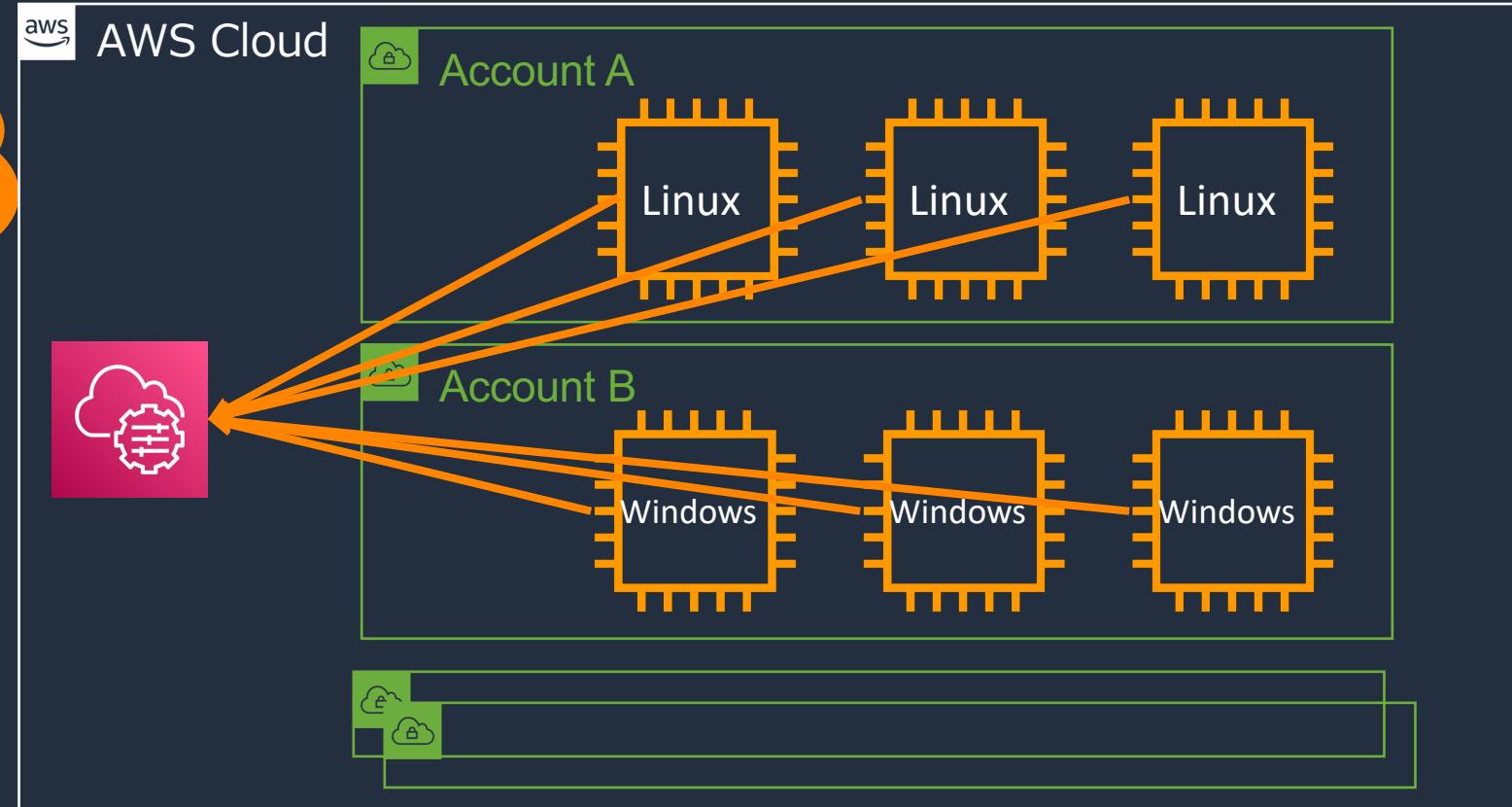
- ✓ インターネット 経由
- ✓ Or VPC Endpoint 経由 (閉域でのアクセスも可能)

3、Systems Manager 権限の付与

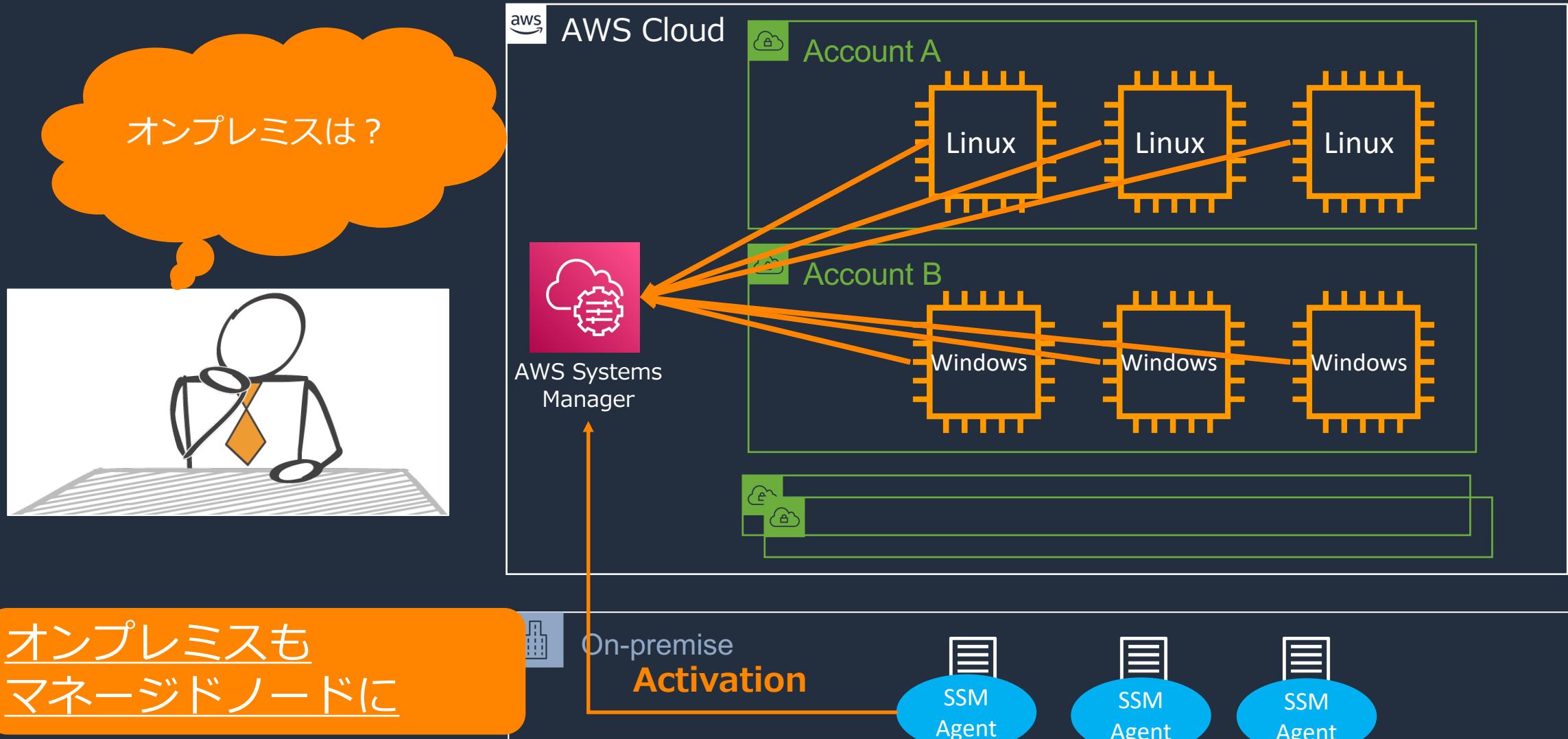
- ✓ 管理下におきたい EC2 に明示的にロールを付与
- ✓ Or DHMC を有効にして、アカウント内の全インスタンスを自動で管理下に



ここまでやれば、晴れてマネージドノードに！

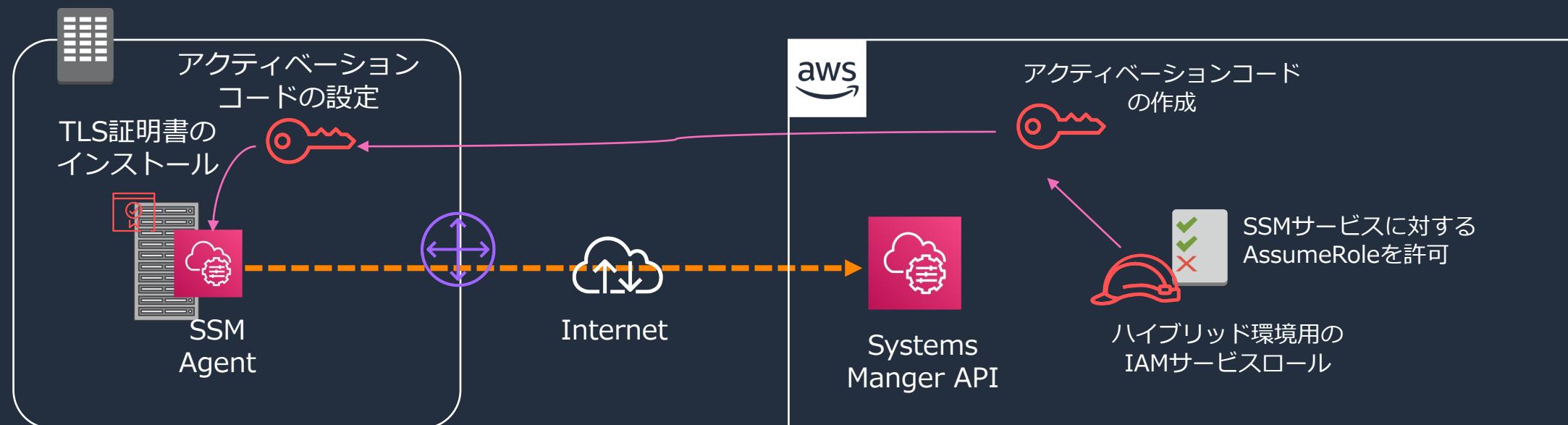


ここまでやれば、晴れてマネージドノードに！



オンプレミスのサーバをマネージドノードにするには

1. (Option) TLS 証明書のインストール
2. ハイブリッド環境用の IAM ロールを作成 (初回のみ)
3. SSM でアクティベーションコードを生成
4. インスタンスにアクティベーションコードを設定



aws ハイブリッド環境での設定の詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

AWS Systems Manager で始める 運用管理



AWS Systems Manager の機能

運用管理	アプリケーション管理	変更管理	ノード管理
 Explorer	 Application Manager	 Change Manager	 Fleet Manager
 OpsCenter	 AppConfig	 Automation	 Session Manager
 Incident Manager	 Parameter Store	 Maintenance Windows	 Inventory
		 Change Calendar	 Run Command
			 Patch Manager
			 Distributor
			 State Manager

Quick Setup

Systems Manager Fundamentals

Systems Manager Agent (SSM Agent)



- 任意のノードをリモートで管理
 - EC2 インスタンス
 - IoT Greengrass を使用したエッジデバイス
 - オンプレミスや他のクラウドサーバ、VMs
- Linux, macOS, Raspberry Pi, Windows Server をサポート
 - サポート OS の一覧は[こちら](#)
 - Amazon Linux やWindows、Ubuntu などの一部のオフィシャルイメージには導入済み。プリインストールされた AMIs の一覧は[こちら](#)
- SSM Agent は、SYSTEM (Windows) 、 root (Linux) で稼働
- SSM Agent はオープンソース。[GitHub](#)にて公開されている

Systems Manager ドキュメント (1/3)

- 実行するアクションを定義したもの
 - 一般的なタスクを自動化し、ヒューマンエラーを減らす
- 100以上の事前設定済みのドキュメント
 - カスタムドキュメントの作成も可能
- JSON or YAML 形式
- バージョニング、タグをサポート

The screenshot shows the AWS Systems Manager Documents interface. On the left, there's a sidebar with categories like Automation documents, Command documents, Policy documents, and Session documents. The main area displays two documents: 'AWS-ASGEnterStandby' and 'AWS-ASGEExitStandby'. Both documents are listed under the 'Automation' category and are owned by Amazon. They support Windows, Linux, and MacOS platforms. The 'AWS-ASGEnterStandby' document is currently selected.

aws ドキュメントについて詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

```
{  
  "schemaVersion": "2.2",  
  "description": "Cross-platform demo document",  
  "mainSteps": [  
    {  
      "action": "aws:runPowerShellScript",  
      "precondition": {  
        "StringEquals": ["platformType", "Windows"]  
      },  
      "name": "WindowsOpenPorts",  
      "inputs": {  
        "runCommand": ["netstat -a"]  
      }  
    },  
    {  
      "action": "aws:runShellScript",  
      "precondition": {  
        "StringEquals": ["platformType", "Linux"]  
      },  
      "name": "LinuxOpenPorts",  
      "inputs": {  
        "runCommand": ["netstat -lntu"]  
      }  
    }  
  ]  
}
```

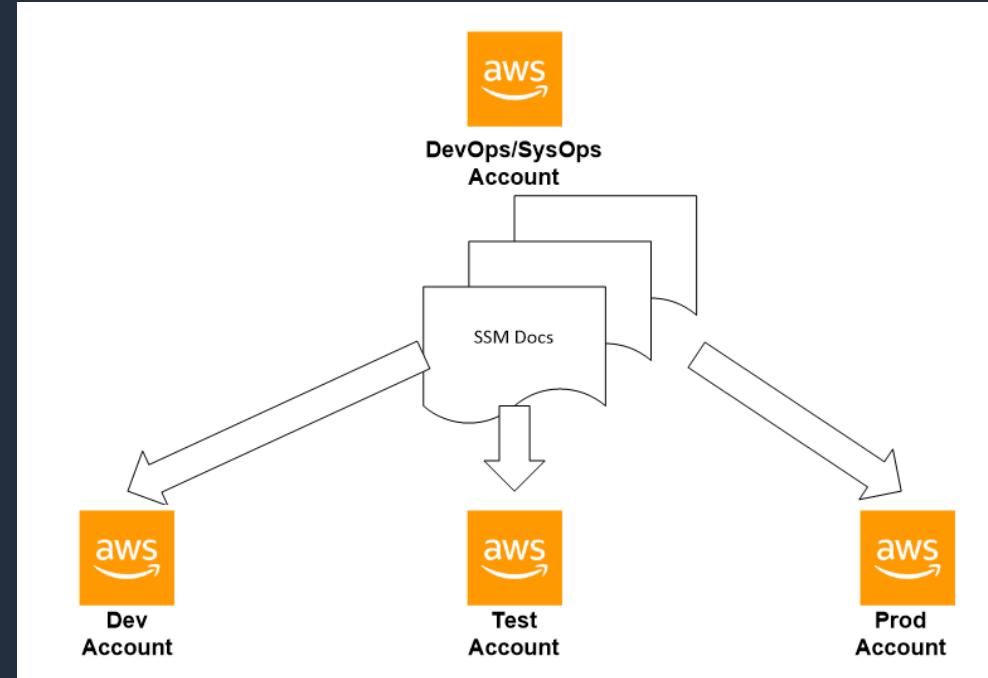
Systems Manager ドキュメント (2/3)

- ・主なドキュメントタイプ

Type	Usage with	Usage with
Automation (runbook)	✓ Automation	Automation runbook として 自動化ワークフローを定義
Command	✓ Run Command	Run Command にて使用する、 サーバで実行するコマンドを定義
Session	✓ Session Manager	Session Manager にて開始する セッションのタイプを定義
Policy	✓ Inventory	Inventory にてインベントリデータを 収集する際に使用

Systems Manager ドキュメント (3/3)

- ドキュメントの共有が可能
 - 中央リポジトリを維持すれば良い
 - ベストプラクティスの共有を容易に実現

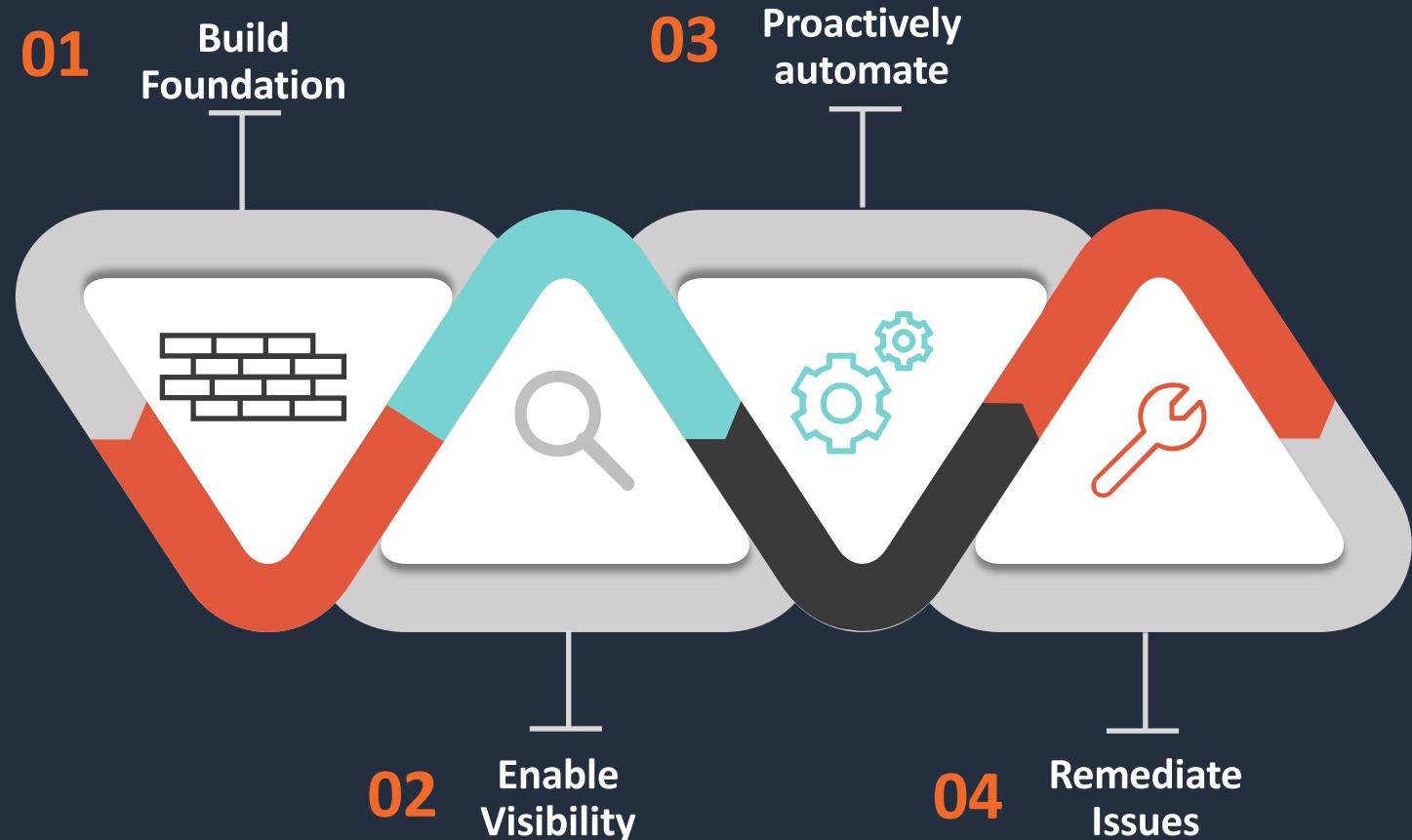


Systems Manager Features

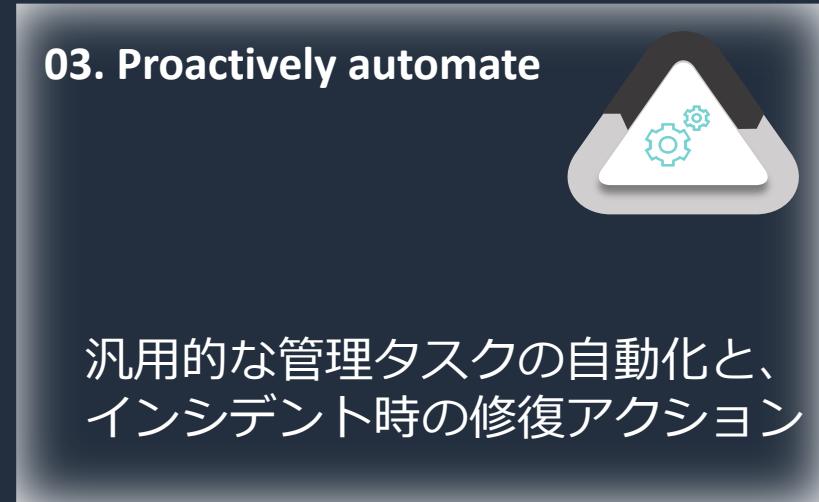
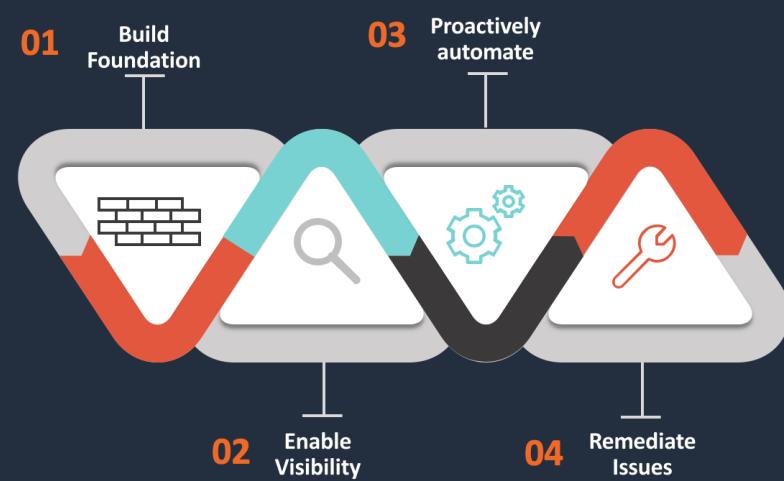
AWS Systems Manager の機能



コンプライアンスを実現するための 4 段階の実装



コンプライアンスを実現するための 4 段階の実装



01. Build Foundation

運用のベストプラクティスを展開し、それを維持する仕組みを確立



運用上のベストプラクティスを展開

Quick Setup

展開したベストプラクティスを維持する仕組み



State Manager



Build Foundation

Quick Setup

運用のベストプラクティスを簡単に展開

→ マルチアカウント、マルチリージョンに、
ベストプラクティスを展開できる。

Host Management

AWS Systems Manager

Config Recording

AWS Config

Conformance packs

AWS Config

Patch Manager

AWS Systems Manager

Change Manager

AWS Systems Manager

DevOps Guru

Amazon DevOps Guru

Distributor

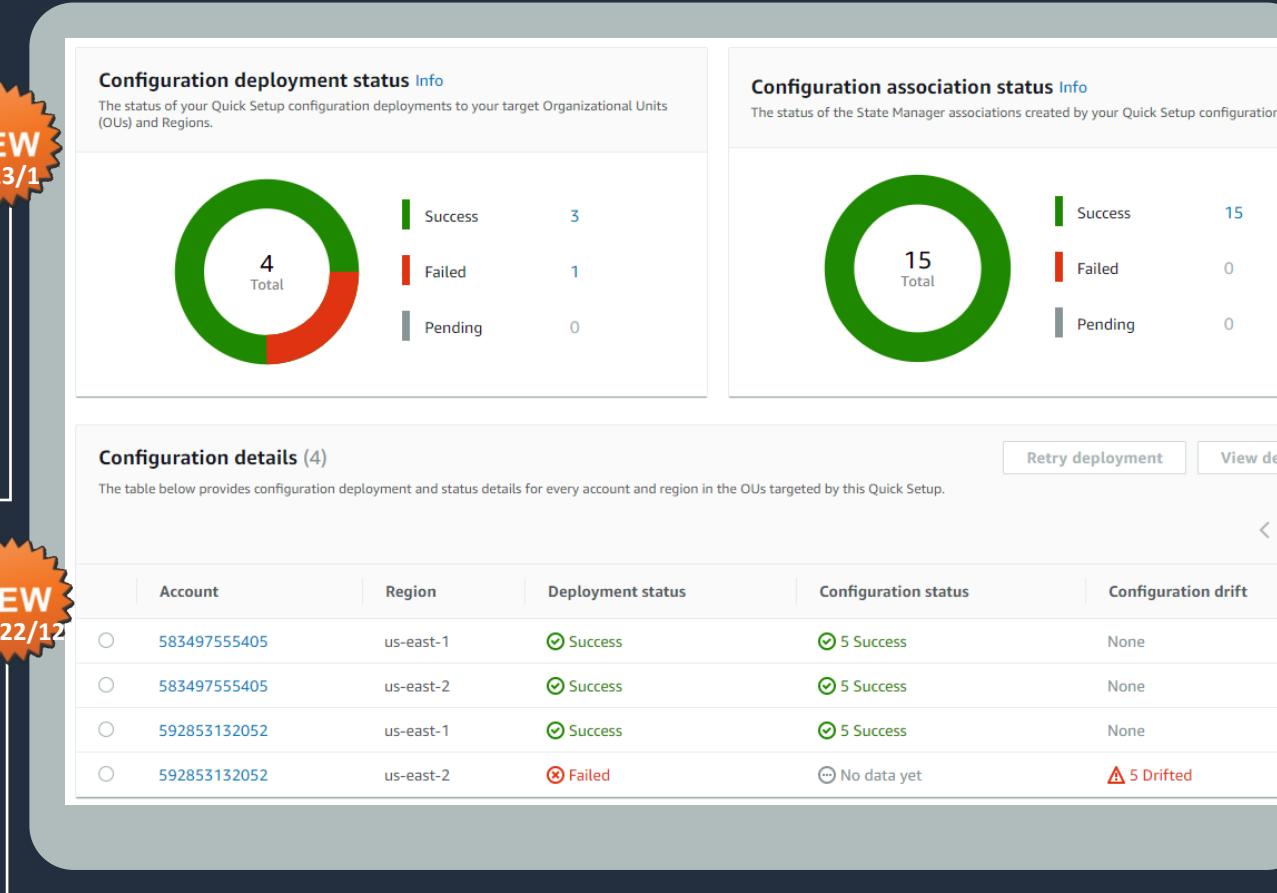
AWS Systems Manager

Resource Scheduler

AWS Solutions

NEW
2023/1

NEW
2022/12



Quick Setup の詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

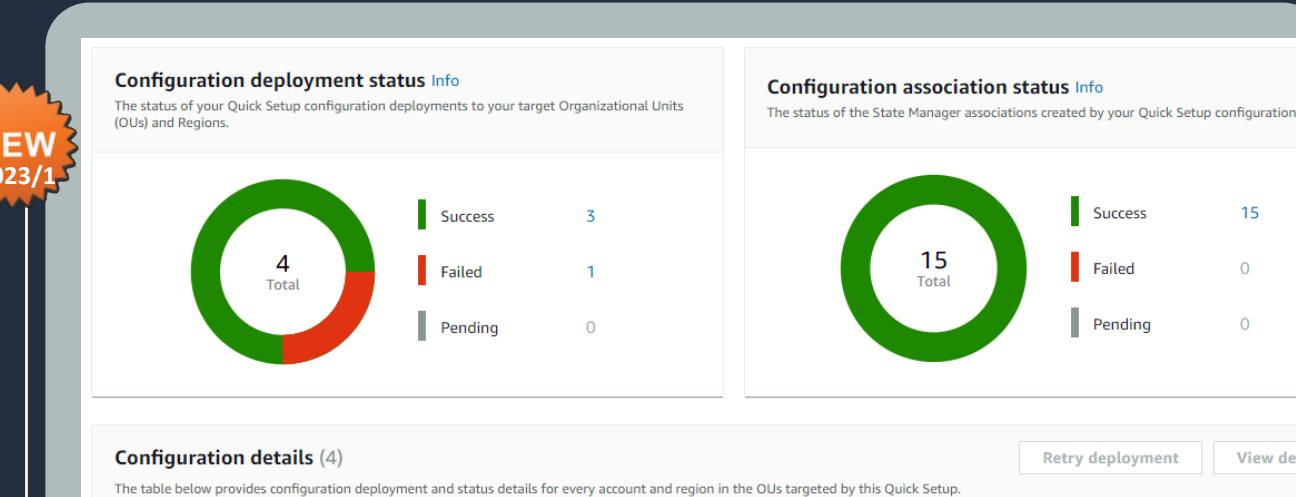
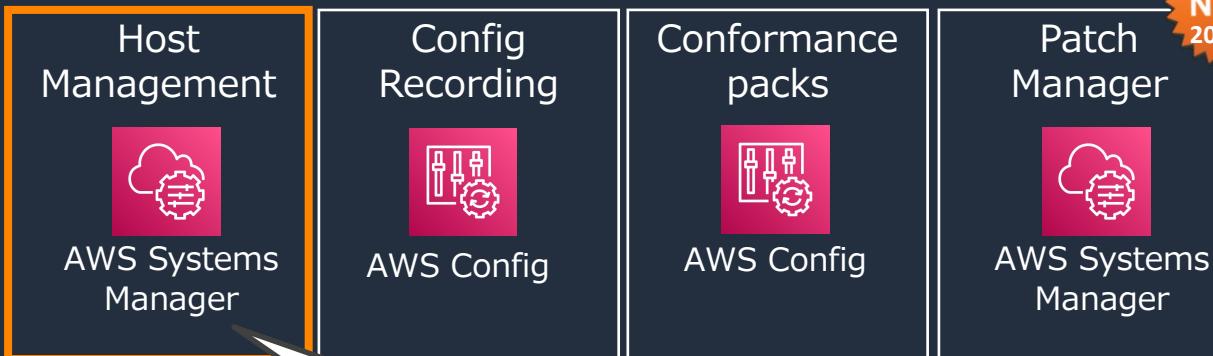


Build Foundation

Quick Setup

運用のベストプラクティスを簡単に展開

→ マルチアカウント、マルチリージョンに、
ベストプラクティスを展開できる。



SSM が提供するベストプラクティスの構築

- SSM Agent の定期更新
- Inventory の定期収集
- パッチスキヤンの定期実行
- CloudWatch Agent のインストールと構成
- CloudWatch Agent の定期更新



Host Management の詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.



Build Foundation

Quick Setup

運用のベストプラクティスを簡単に展開

→ マルチアカウント、マルチリージョンに、
ベストプラクティスを展開できる。

Host Management
 AWS Systems Manager

Config Recording
 AWS Config

Conformance packs
 AWS Config

Patch Manager
 AWS Systems Manager

NEW
2023/1

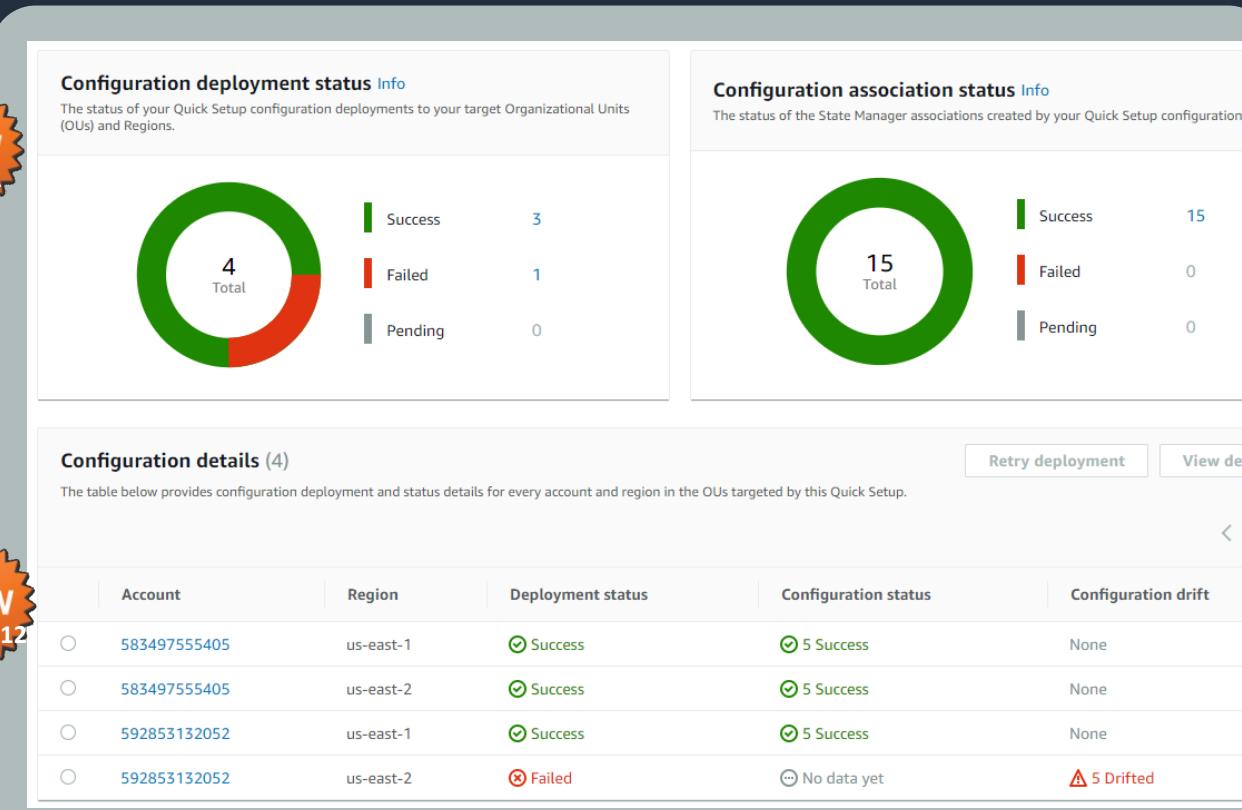
Change Manager
 AWS Systems Manager

DevOps Guru
 Amazon DevOps Guru

Distributor
 AWS Systems Manager

Resource Scheduler
 AWS Solutions

NEW
2022/12



EC2 の自動起動・停止が実装できる新機能



Resource Scheduler の詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

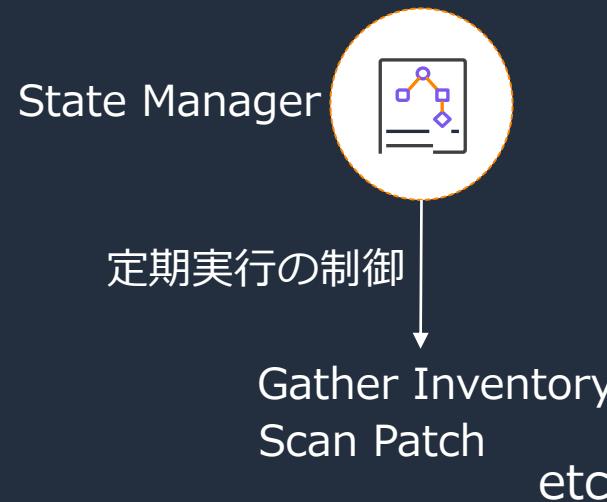


Build Foundation

State Manager

フリート全体の設定管理ソリューション

- Quick Setup で展開した SSM の定期実行処理は State Manager にて管理される。
- State Manager は、ノードを定義された状態に保つためのプロセスを自動化する。



The screenshot shows the AWS Systems Manager Compliance dashboard. The top navigation bar includes "AWS Systems Manager" and "Compliance". The main section is titled "Compliance dashboard filtering" with a sub-section "Group dashboard results based on". It shows two selected options: "Compliance type" (radio button selected) and "Patch group" (radio button unselected). Below this is a search bar labeled "Filter further".

The next section is "Compliance resources summary", featuring a table with columns: "Compliance type", "Compliant resources", "Non-Compliant resources", "Critical resources", "High resources", "Medium resources", and "Low resources". The data shows:

Compliance type	Compliant resources	Non-Compliant resources	Critical resources	High resources	Medium resources	Low resources
Association	⌚ 4	⚠ 0	⚠ 0	⚠ 0	⚠ 0	⚠ 0
Patch	⌚ 0	⚠ 4	⚠ 0	⚠ 0	⚠ 0	⚠ 0

The final section is "Details overview for resources", titled "Resource". It lists one item:

ID	Resource type	Compliance type	Overall severity	Overall compliance
i-00bcf16c41d508093	ManagedInstance	Association	Unspecified	⌚ Compliant

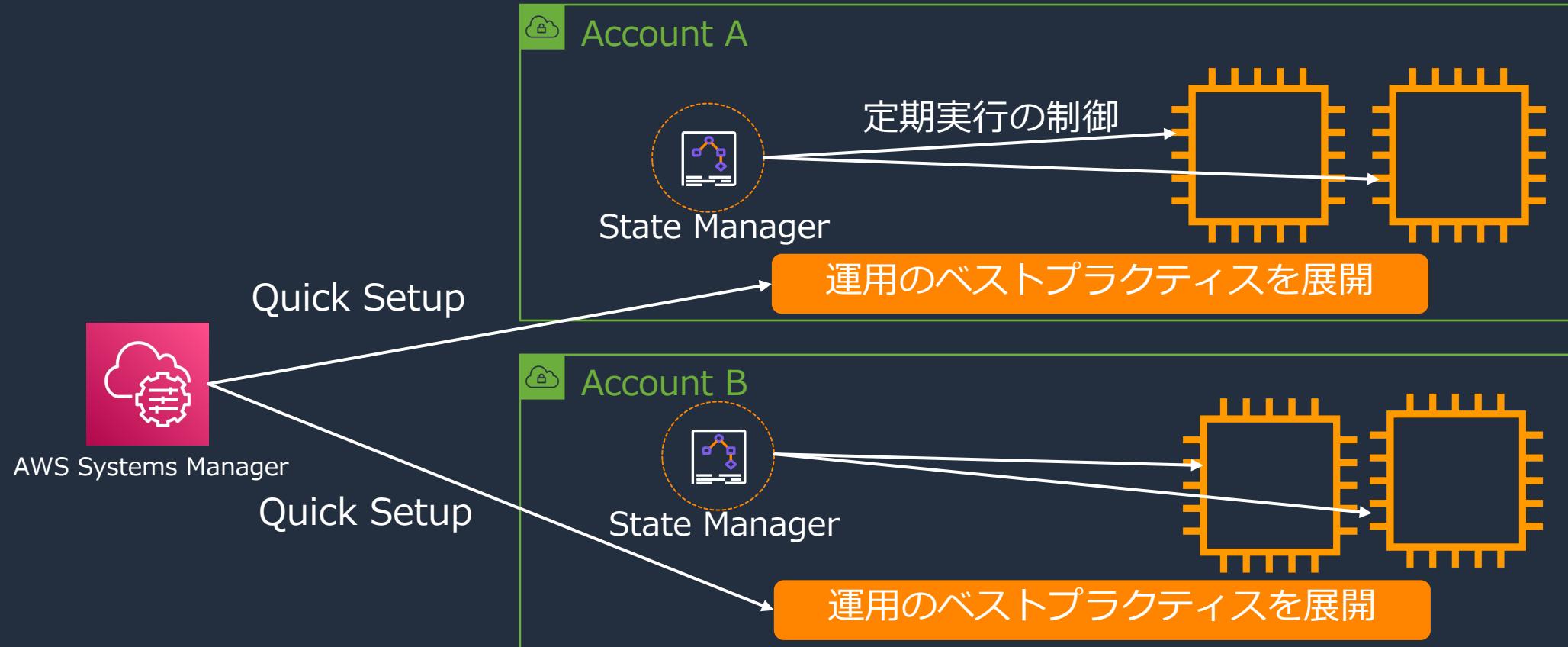


State Manager については、[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

おさらい

ここまで何ができたかというと・・・

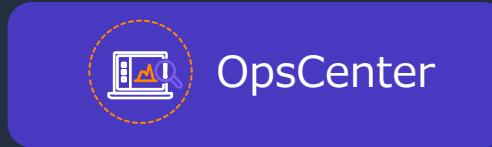
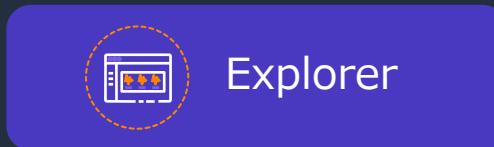


02. Enable Visibility

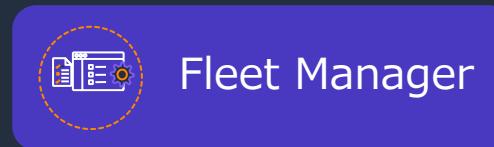
ハイレベルやノードレベルのダッシュボードと管理



AWS 環境全体を俯瞰・確認する



ノードの状態を俯瞰・確認する





Explorer

ハイレベルの運用ダッシュボード

Enable Visibility

- マルチアカウント・マルチリージョンのハイレベルな運用ダッシュボード。
- 複数のサービスからの情報が集約される。

Instance / Compute Optimizer

Amazon Elastic Compute Cloud (Amazon EC2)

AWS Config Compliance

AWS Config

Trusted Advisor (※)

AWS Trusted Advisor

Security Hub Findings

AWS Security Hub

- Patch Compliance
- OpsItems
- Inventory
- Association

AWS Systems Manager

Support Center (※)

AWS Support

aws Explorerについての詳細は[こちら](#)。

※ Enterprise Support、Business Support プランが必要

© 2023, Amazon Web Services, Inc. or its affiliates.





Enable Visibility

OpsCenter

対応すべき運用アイテムの可視化、問題解決の支援

- 運用上の問題 (OpsItem) の集約ビューを提供。
- OpsItem に関するデータを一元的に提供し、問題解決までの時間短縮を支援する。
- マルチアカウントでの OpsItem の表示や操作も可能。
- ServiceNow, Jira Service Management と連携も。

The screenshot shows the AWS Systems Manager console with the 'OpsCenter' feature selected. The 'Summary' tab is active, displaying the 'OpsItem status summary' and 'Sources with most open OpsItems' sections. The 'OpsItem status summary' section shows 11 total items, with 10 labeled as 'Open' and 1 as 'In progress'. The 'Sources with most open OpsItems' section shows EC2 with 7 items and RDS with 3 items. Below these, the 'OpsItems by source and age' section provides a breakdown of item counts by source and age range (0-30 days, 31-90 days, > 90 days). The data is as follows:

Grouped by source	Count	0 - 30 days	31 - 90 days	> 90 days
EC2	8	8	0	0
RDS	3	3	0	0

aws OpsCenterについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.



OpsCenter

対応すべき運用アイテムの可視化、問題解決の支援

Enable Visibility



© 2023, Amazon Web Services, Inc. or its affiliates.

Runbook の提供



Automation

ランブック (361)

名前	タイプ
AWS-CreateManagedWindowsInstance	Associated AWS:SSM:Automation
AWS-CreateManagedLinuxInstance	Associated AWS:SSM:Automation

関連リソースの情報

▼ CloudWatch メトリクス



Amazon CloudWatch

▼ AWS Config の詳細

検出された時間	キー	値から
3 hours ago	imageId	ami-08d56ac42
3 hours ago	instanceId	i-03695dbe27e
3 hours ago	instanceType	t2.micro

AWS Config

▼ CloudTrail ログ (4)

イベント時間	ユーザー名
3 hours ago	imagebuilder08cd5-4a36-47e6-ab15-c15ba95745d1
3 hours ago	-
3 hours ago	-

AWS CloudTrail



Enable Visibility

Fleet Manager

ノードフリートの管理

④ マネジメントコンソールからノードフリートの管理ができるビジュアルツール

- ・ファイルシステム
- ・パフォーマンスカウンタ
- ・プロセス
- ・ユーザー・グループ
- ・Windows レジストリ (Windowsのみ)
- ・Windows イベントログ (Windowsのみ)

ログのTail

プレビューファイル: messages

テールファイル

```
Feb 25 23:19:34 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 122570ms.
Feb 25 23:21:36 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 112900ms.
Feb 25 23:23:29 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 109720ms.
Feb 25 23:25:19 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 118120ms.
Feb 25 23:27:17 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 127520ms.
Feb 25 23:29:25 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 108910ms.
Feb 25 23:31:14 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 122110ms.
Feb 25 23:33:16 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 109760ms.
Feb 25 23:35:06 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 129830ms.
Feb 25 23:37:16 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 124770ms.
```

プロセス稼働状況

Instance ID: i-03170a [REDACTED]

Tools

- Node overview
- File system
- Performance counters
- Processes New
- Users and groups
- Windows event logs
- Windows registry

Instance overview

Instance ID i-03170a	OS name Microsoft Windows Server 2019 Datacenter	Availability zone us-east-1a
Platform type Windows	SSM Agent version 3.0.529.0	SSH key name
Instance type t2.small	IP address 10.0.1.8	IAM role arn:aws:iam::2869:instance-profile/ManagedInstanceProfile
SSM Agent ping status Online		

Tags

You can use tags to group and filter your managed instances. A tag consists of a case-sensitive key-value pair.

Key	Value
Name	Windows

Processes (56/56)

The table provides information about the processes that are currently running on your node.

Process name	Process ID	CPU usage	Memory usage
svchost#11	1184	0	9.47
svchost#5	492	0	8.56

aws Fleet Managerについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

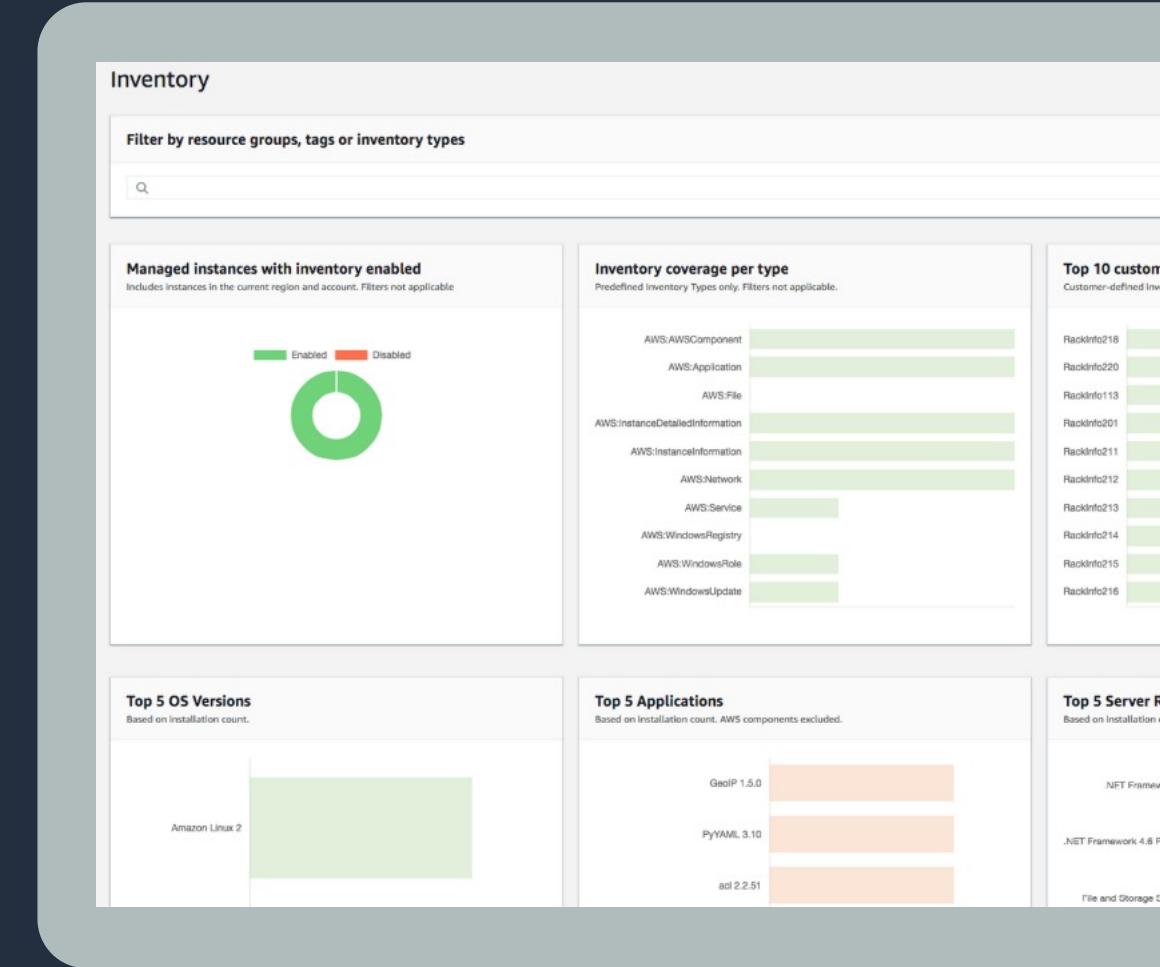


Inventory

ノードのメタデータ可視化

Enable Visibility

- ④ マネージドノードのメタデータを収集。
アプリケーション、ファイル、NW構成
インスタンス情報など
- ④ カスタムインベントリとして独自アイテムも
収集可能
- ④ リソースデータの同期を行うことで、自身
でマルチアカウント、マルチリージョンの
ダッシュボードを作成可能

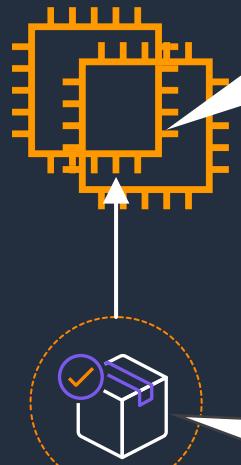


 Inventoryについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

Inventory の活用例：Log4j の探索

- カスタムインベントリを活用することで、独自の収集項目が取得できる。
- この例では、Log4j の使用有無を探索し、それをカスタムインベントリとして登録している。



Inventory

詳細は[こちらのブログ](#)を参照

aws 「AWS Systems Manager カスタムインベントリを使ったマネージドノード上の Log4j ファイル検索」

Amazon Athena

Query 1

```
1 SELECT
2     resourceid, accountid, filename, path
3 FROM
4     custom_log4j
```

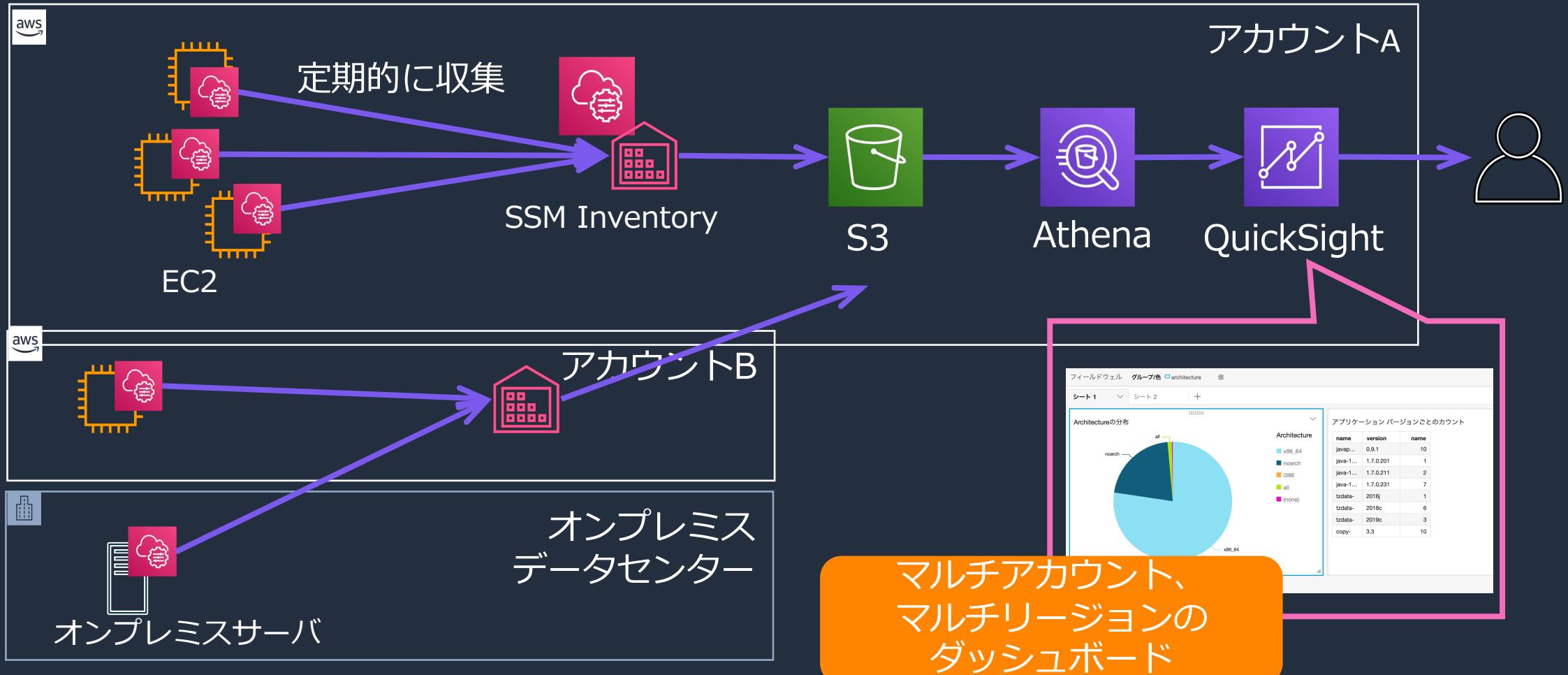
Completed

Time in queue: 0.149 sec Run time: 0.954 sec Data scanned: 1.10 KB

resourceid	accountid	filename	path
i-0f500...	31734	log4j-core-2.12.0.jar	C:\SampleApp\apache-log4j-2.12.0-bin\apache-log4j-2.12.0-bin\lo...
i-0f500...	31734	log4j-core-2.11.0.jar	C:\Users\Administrator\Desktop\apache-log4j-2.11.0-bin\apache-l...
mi-06eb5...	31734	log4j-core-2.11.0.jar	C:\Users\Administrator\Downloads\apache-log4j-2.11.0-bin\apach...
i-00d87...	31734	log4j-core-2.12.0.jar	/tmp/log4j/apache-log4j-2.12.0-bin/log4j-core-2.12.0.jar
i-00d87...	31734	log4j-core-2.11.0.jar	/tmp/log4j-2.11/apache-log4j-2.11.0-bin/log4j-core-2.11.0.jar

© 2023, Amazon Web Services, Inc. or its affiliates.

Inventory の活用例： マルチアカウント/マルチリージョンのダッシュボードの作成



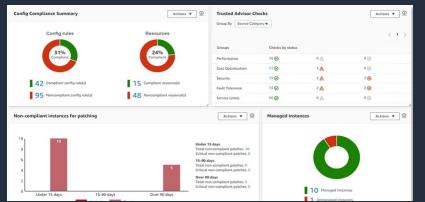
おさらい

ここまで何ができたかというと・・・

AWS環境全体を
俯瞰・確認する

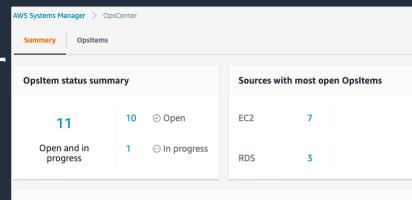


ハイレベルの運用ダッシュボード



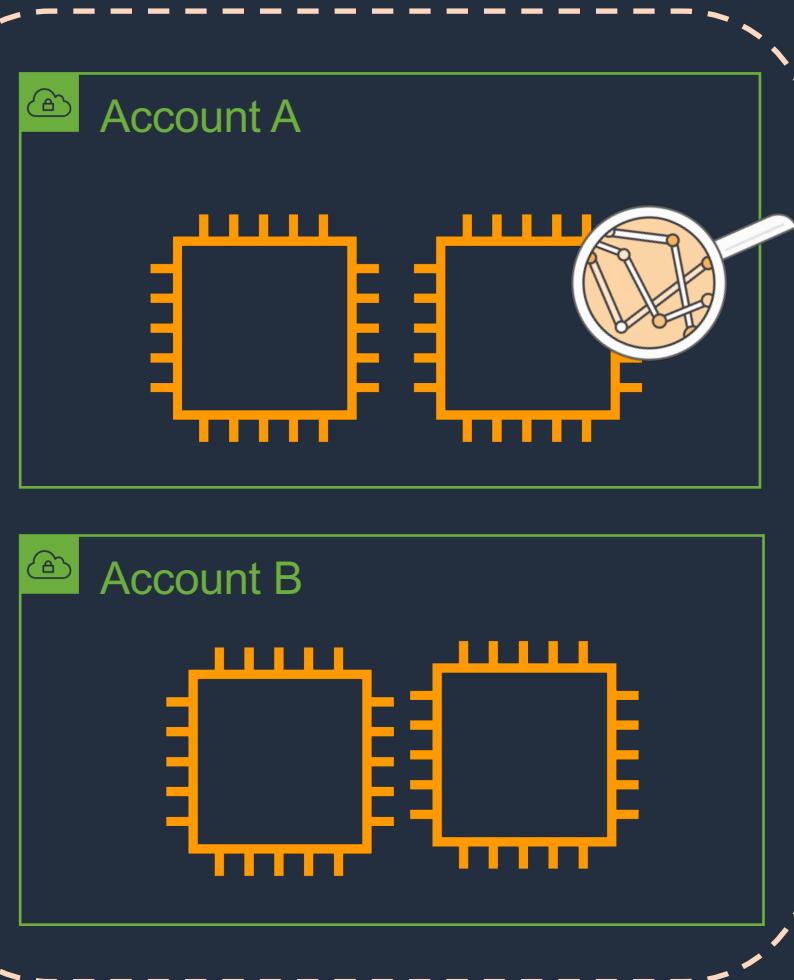
Explorer

運用アイテムの管理



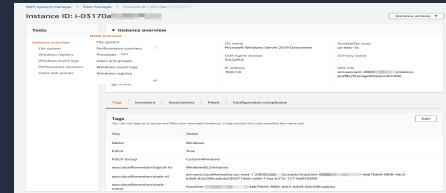
OpsCenter

aws



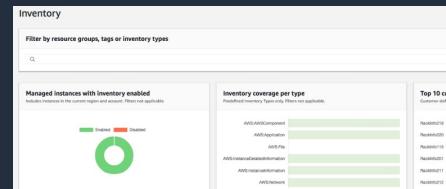
ノードの状態を
俯瞰・確認する

ノードフリート管理



Fleet
Manager

ノードのメタデータ可視化



Inventory

03. Proactively Automate

汎用的な管理タスクの自動化と、インシデント時の修復アクション



汎用的な管理作業の自動化



Patch Manager



Distributor



Automation

自動化処理のタイミング制御



Maintenance
Windows



Change Calendar

自動修復の実装



Automation



Patch Manager

パッチ適用を自動化

Proactively Automate

- ④ マネージドノードに対して、パッチの自動スキャン、自動パッチ適用を実現。
- ④ Patch Manager サポート OS は SSM Agent サポートOSとは異なるので注意。サポート OS は[こちら](#)。
- ④ パッチポリシーをマルチアカウント、マルチリージョンにデプロイ可能

パッチベースラインの設定例

OS : Amazon Linux / Windows など

製品 : Amazon Linux2 など

分類 : All, Security, Bugfix など

重要度 : All, Critical, Important など

自動承認 : **リリースされてからX日後に適用 or**

特定の日付までにリリースされたパッチを適用

パッチの例外 : 承認済みパッチ、拒否パッチ

aws Patch Manager についての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

The screenshot shows the AWS Systems Manager Patch Manager dashboard. At the top, there's a navigation bar with links for Dashboard, Reporting, Patch baselines, Patches, Patch groups, and Settings. On the right, there are two orange buttons: 'Configure patching' and 'Patch now'. The main area is divided into several sections:

- Instance Patch Compliance Summary:** A donut chart showing patch compliance status. Legend: Green (5 Compliant), Yellow (1 Other non compliant), Red (0 Critical non compliant, 0 High non compliant). Data: Total managed instances: 6, Instances with missing patches: 1, Instances with failed patches: 0, Instances pending reboot: 0.
- Instance Patch States:** Shows counts for managed instances based on patch states.
- Compliance Reporting Age:** A donut chart showing reporting age for all managed instances. Legend: Green (6 Reported within the past 7 days), Yellow (0 Not reported within the past 7 days), Red (0 Never reported).
- Recent Patch Operations:** A table listing recent patching commands. Columns include Patch Operation, Execution Mechanism, Document name, End time, Status, and Targets. Examples include 'Scan' (Other, AWS-RunPatchBaseline) at April 13, 2021, 5:30 AM, 'Scan' (Association, AWS-RunPatchBaseline) at April 12, 2021, 10:00 PM, and 'Install' (Other, AWS-RunPatchBaseline) at April 12, 2021, 3:06 PM.
- Recurring Patching Tasks:** A table listing patching tasks. Columns include Patching task name, Task type, Document name, and Schedule. Examples include 'AWS-PatchNowAssociation' (Association, AWS-RunPatchBaseline, cron(0 00 02 ? * *)) and 'AWS-QuickSetup-SSMHostMgmt-ScanForPatches-b5mbv' (Association, AWS-RunPatchBaselineAssociation, rate(1 day)).



Distributor

ソフトウェアのインストール・更新の自動化

Proactively Automate

- ④ ソフトウェアパッケージのデプロイ自動化を実現。
- ④ 一つのパッケージで Windows も Linux も。
- ④ 独自で定義したパッケージのデプロイはもちろん、CloudWatch Agent など AWS 提供のパッケージや 3rd Party のパッケージの利用もおすすめ

利用できる3rd Party パッケージ

- TrendMicro-CloudOne-WorkloadSecurity
- DynatraceOneAgent
- AlertLogic-MDR

NEW
2022/2

The screenshot shows the AWS Systems Manager Distributor interface. At the top, there are tabs for 'Owned by Amazon' (which is selected), 'Owned by me', 'Shared with me', 'Third Party', and 'All documents'. Below this is a search bar labeled 'Search by keyword or filter by tag or attributes'. The main area displays a grid of package cards, each with a name, owner information, and a circular selection button. The packages listed are: AmazonCloudWatchAgent, AWSupport-EC2Rescue, AWSSAP-Backint, AWSEC2Launch-Agent, AmazonEFSUtils, AWSObservabilityExporter-JMXExporterInstallAndConfigure, AWSCodeDeployAgent, AWSKinesisTap, AwsVssComponents, AWSPVDriver, AWSNVMe, and AwsEnaNetworkDriver. All packages are owned by Amazon.

aws Distributor についての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

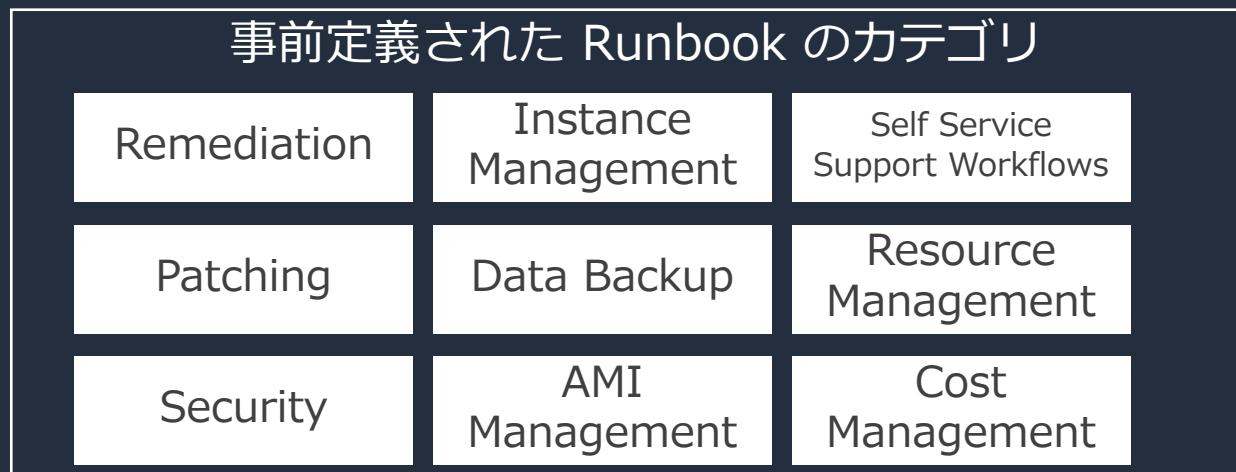


Automation

カスタム処理の自動化と修復アクション

Proactively Automate

- 自動化ワークフローである Runbook を実行できる。
- マルチアカウント/マルチリージョンでの実行も可能。
- 事前定義された Runbook が多数あるので、それを利用するのがおすすめ。



Execute automation document

Step 2 of 2

Simple execution
Execute on targets.

Multi-account and Region
Execute in multiple accounts and Regions.

Rate control
Execute safely on multiple targets by defining concurrency and error thresholds.

Manual execution
Step-by-step runbook mode.

Document details

Document name	Document version
AWS-PatchAsgInstance	\$DEFAULT
▼ Document description	
Systems Manager Automation - Patch instances in an Auto Scaling Group	

aws Automation についての詳細は[こちら](#)。

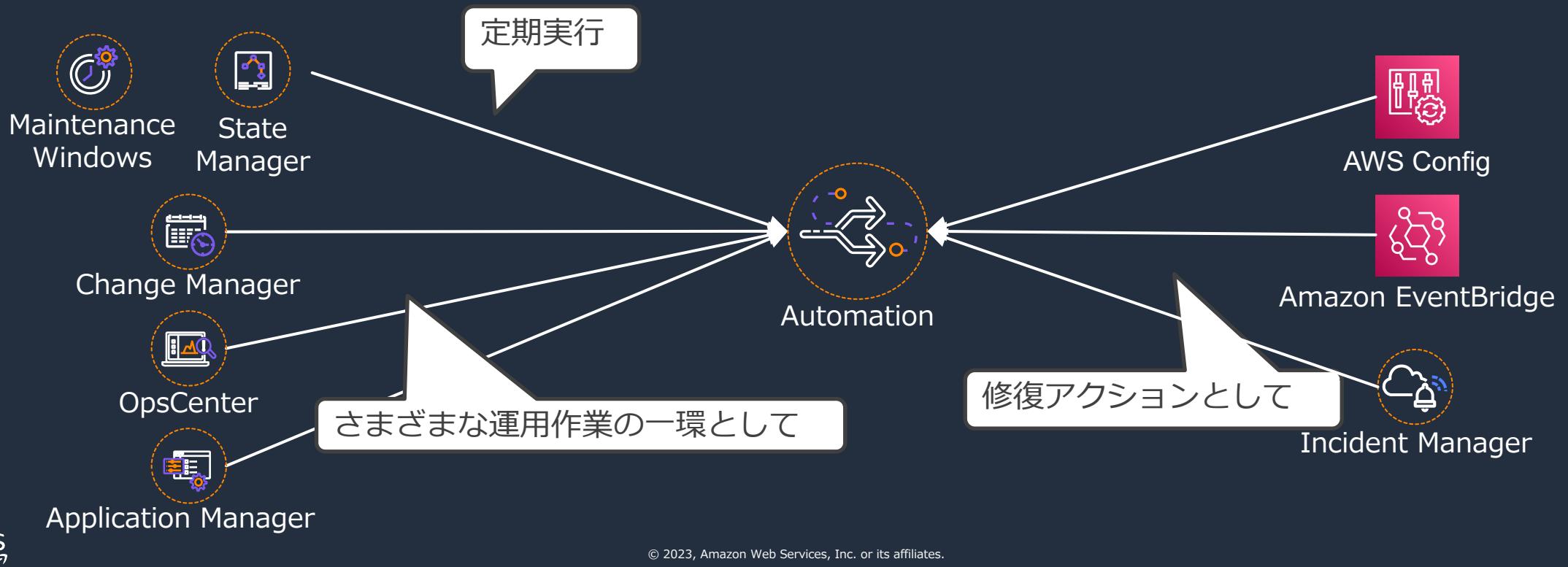
© 2023, Amazon Web Services, Inc. or its affiliates.



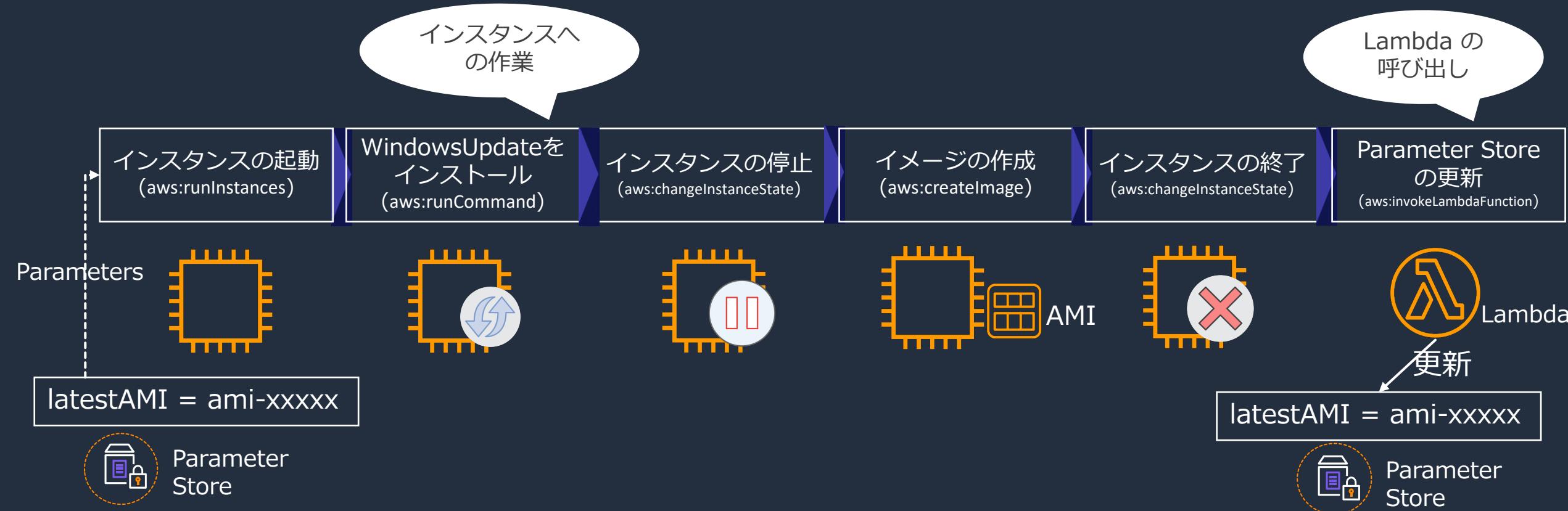
Proactively Automate

Automation – さまざまなトリガーで起動 カスタム処理の自動化と修復アクション

- ④ Runbook はさまざまなサービスからトリガーできる。
- ④ コンプライアンス違反やインシデント発生時の、自動で修復するアクションの定義としても活躍。



Runbook 例：カスタム AMI パッチ適用

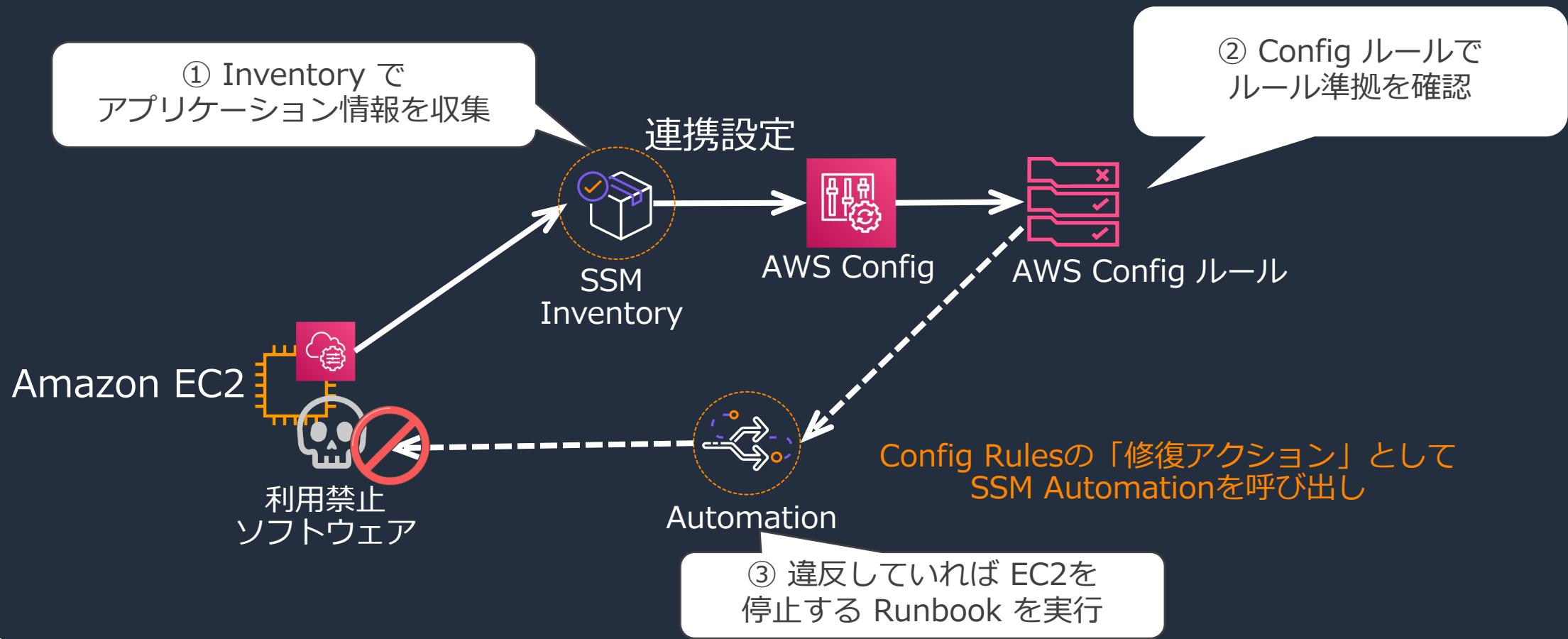


詳細は[こちら](#)のチュートリアルを参照
aws 「チュートリアル: オートメーション、AWS Lambda、Parameter Store を使用した AMI パッチ適用の簡素化」

© 2023, Amazon Web Services, Inc. or its affiliates.

修復自動化例：不正 SW の検知・自動停止

- ④ SSM Inventory でインベントリ情報を収集。
- ⑤ 不正 SW を検知したら、ノードを停止する Runbook を実行。



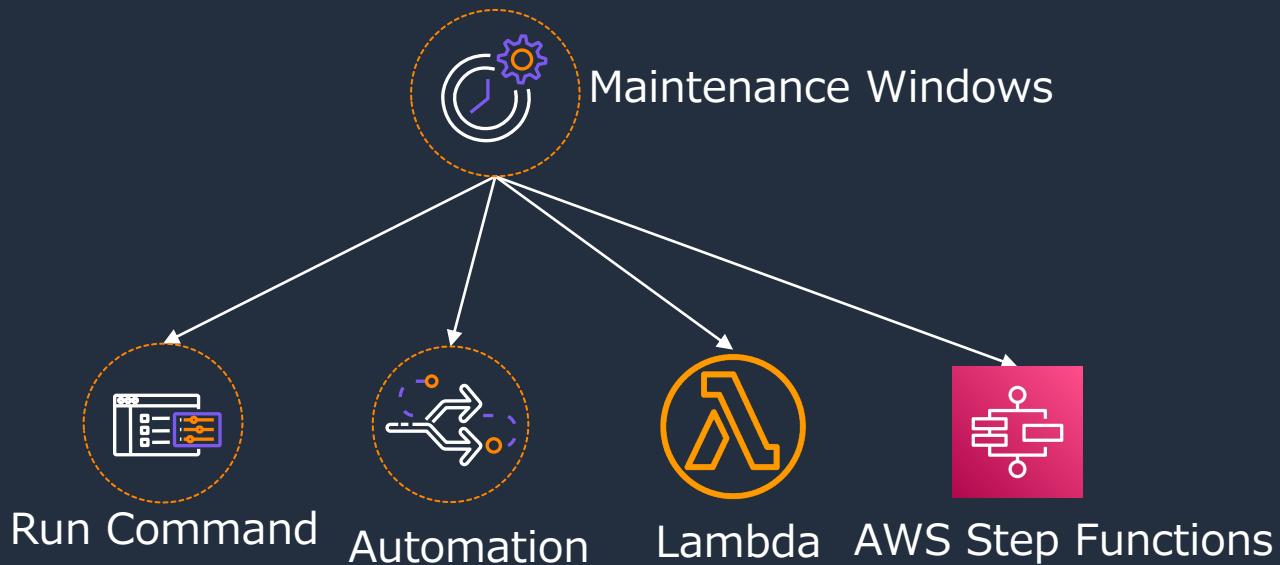


Maintenance Windows

タイムウィンドウ内のタスクを実行制御

Proactively Automate

- タスクのスケジュール制御ができる。
- 複数のタスクを登録でき、優先度に応じて実行順序を制御する。



aws Maintenance Windows についての詳細は[こちら](#)。© 2023, Amazon Web Services, Inc. or its affiliates.

AWS Systems Manager > Maintenance Windows > Create maintenance window

Create maintenance window

A maintenance windows lets you specify when a target set of managed instances should install updates or perform maintenance activities. Specify the details below to create a new maintenance window:

Provide maintenance window details

Name
Type a name for this maintenance window.

It has to be between 3 and 128 characters. Valid characters contain the following: a-z, A-Z, 0-9, and _.

Description - optional
Type description for this maintenance window.

It has to be between 1 and 128 characters.

Unregistered targets
Allow maintenance tasks scheduled for this maintenance window to run on targets that are not currently registered with this maintenance window.
 Allow unregistered targets

Schedule

Specify with
 Cron schedule builder
 Rate schedule builder
 CRON/Rate expression

Window starts
 Every 30 minutes
 Every hours

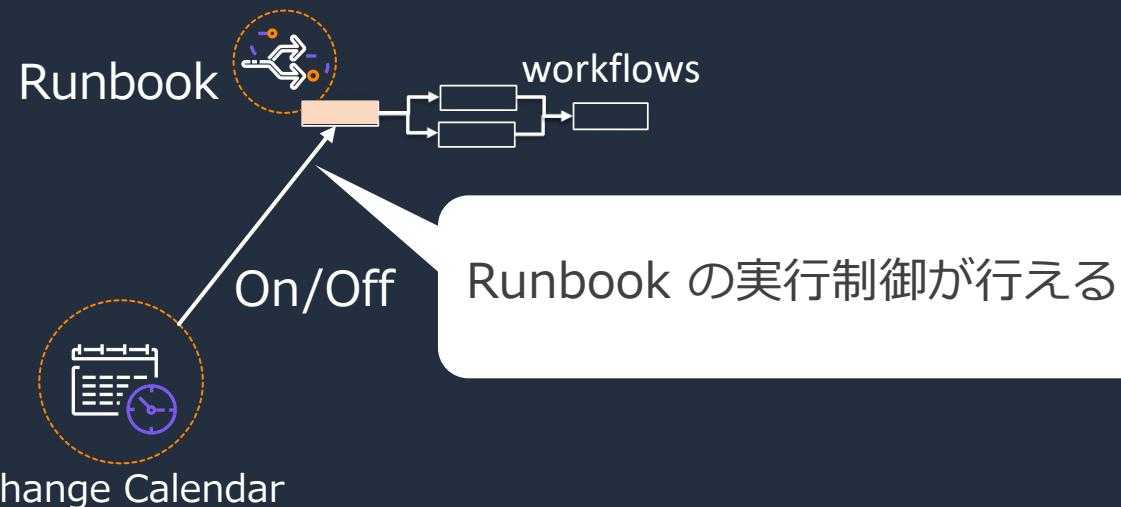


Change Calendar

自動処理のタイミング制御

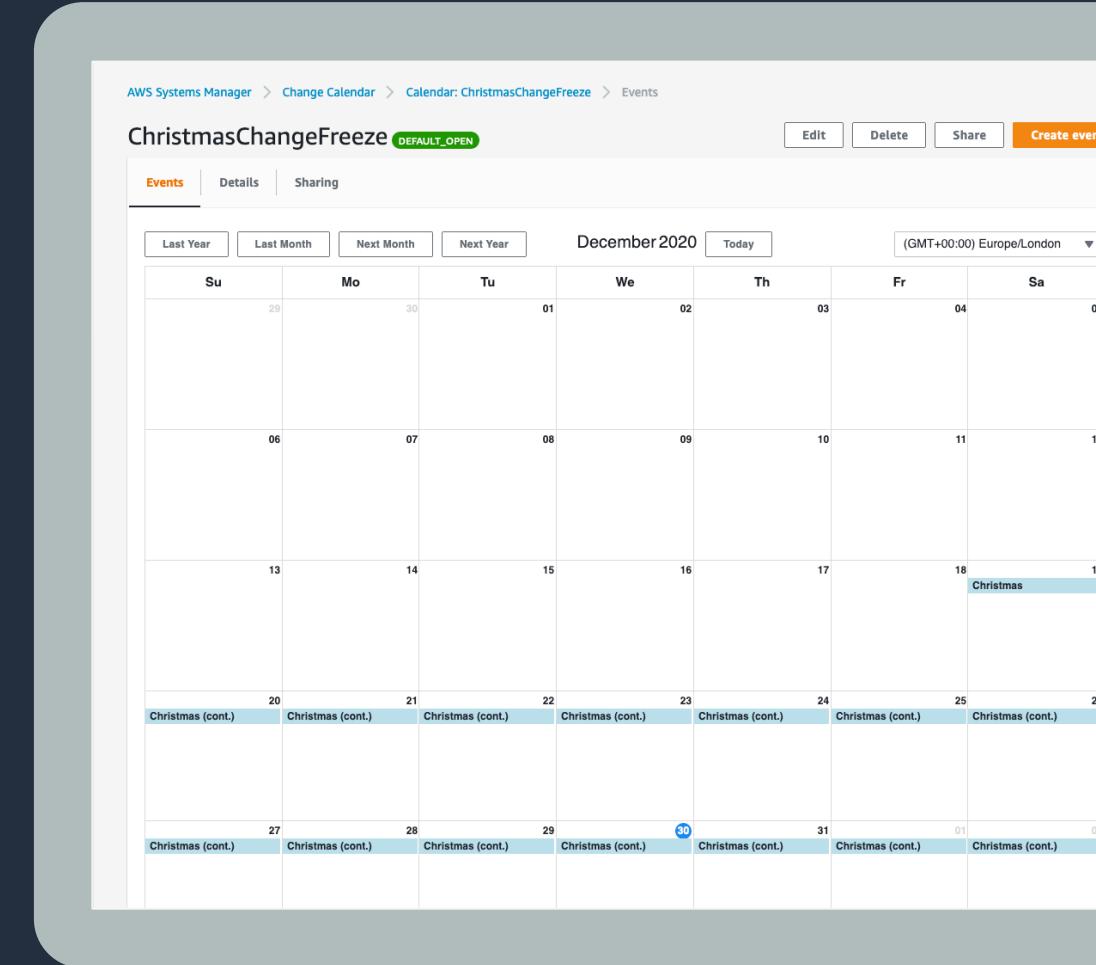
Proactively Automate

- ④ カレンダーイベントを作成し、そのイベント有無で実行を制御できる。
- ④ 3rd Partyのカレンダーのインポートも。Google Calendar, Microsoft Outlook, iCloud カレンダー
- ④ 作成したカレンダーは他のアカウントにも共有可能。



aws Change Calendarについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.



おさらい

汎用的な管理作業の自動化

- パッチ適用



Patch Manager

- SW インストール、更新



Distributor

- その他カスタム処理



Automation



AWS Systems Manager



タイミング制御

- 定期実行



Maintenance Windows

- カレンダーでの制御



Change Calendar

問題発生時のアクション自動化



- 修復アクション



Automation

おさらい

汎用的な管理作業の自動化



Patch Manager

Distributor

Automation



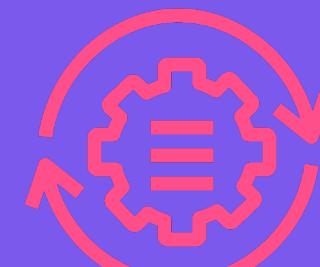
問題発生時のアクション自動化



修復アクション



重要な変更は、
変更管理が必要だ・・・



Change Manager

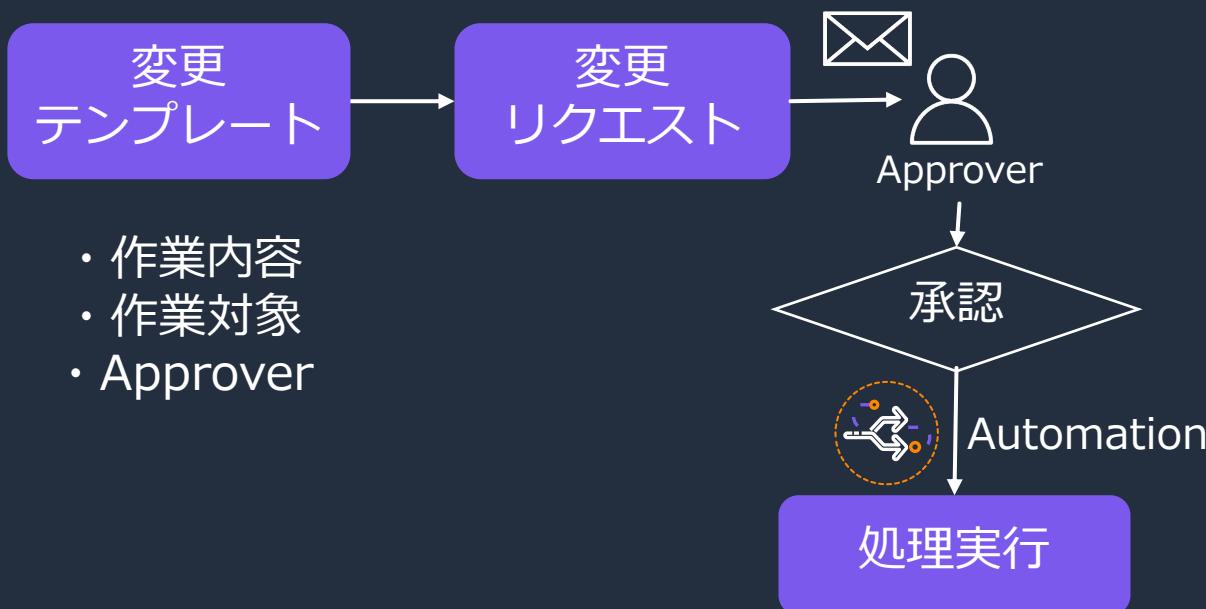


Change Manager

変更を安全に行うための承認ワークフローの自動化

Proactively Automate

- 承認ワークフローを使用して意図しない変更が発生しないことを防ぐ。
- Service Now との連携も可能。



aws Change Managerについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

The screenshot shows the AWS Change Manager console's Overview page. It includes sections for Change overview, Change requests, Change templates, Pending requests by time, Top 5 templates used in the last 30 days, and Scheduled changes for August 2020. Key data points visible include 84 member accounts, 0 active requests, 0 pending approvals, 1 template, and a bar chart showing the most common actions taken.

おさらい

汎用的な管理作業の自動化

パッチ適用



Patch Manager

SWインストール、更新



Distributor

その他カスタム処理



Automation



タイミング制御

定期実行



Maintenance Windows

カレンダーでの制御



Change Calendar

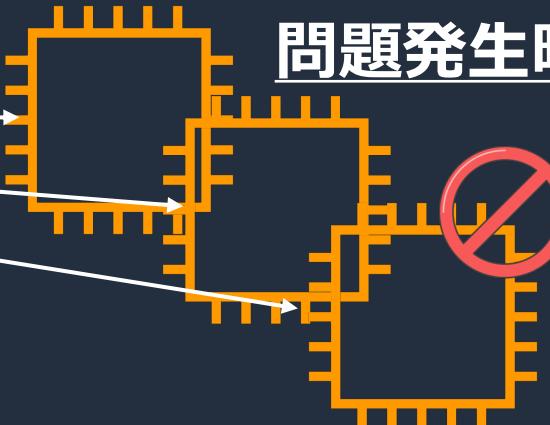
© 2023, Amazon Web Services, Inc. or its affiliate

問題発生時のアクション自動化

修復アクション



Automation



変更管理

承認ワークフローの自動化



Change Manager

04. Remediate Issues

ノードへの一括コマンド発行や、安全な特権アクセス



ノードへの一括コマンド発行



ノードへのセキュアな特権アクセス





Remediate Issues

Run Command

ノードへの一括コマンド発行

- ④ サーバにログインすることなく、マネージドノードに対してコマンドを一括実行。
- ④ “コマンドドキュメント”を実行する。

任意のシェルスクリプトを流せる **AWS-RunShellScript** や Ansible を流せる **AWS-ApplyAnsiblePlaybooks** などが用意されていて便利！



aws → Run Command についての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

Command parameters

Action
(Required) Specify whether or not to install or uninstall the package.
Install

Installation Type
(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place update: The application is available while new or updated files are added to the installation.
Uninstall and reinstall

Name
(Required) The package to install/uninstall.
AmazonCloudWatchAgent

Version
(Optional) The version of the package to install or uninstall. If you don't specify a version, the system installs the latest published version by default. The system will only attempt to uninstall the version that is currently installed. If no version of the package is installed, the system returns an error.

Targets

Choose a method for selecting targets.

Specify instance tags
Specify one or more tag key-value pairs to select instances that share those tags.

Choose instances manually
Manually select the instances you want to register as targets.

Choose a resource group
Choose a resource group that includes the resources you want to target.

Resource group
Select the resource group that you want to use as a target. [View resource groups](#)
EC2Instances

Resource types - optional
Select one or more available resource types to narrow down the target group.
Select resource types
All available resource types X



Remediate Issues

Session Manager

ノードへのセキュアな特権アクセス

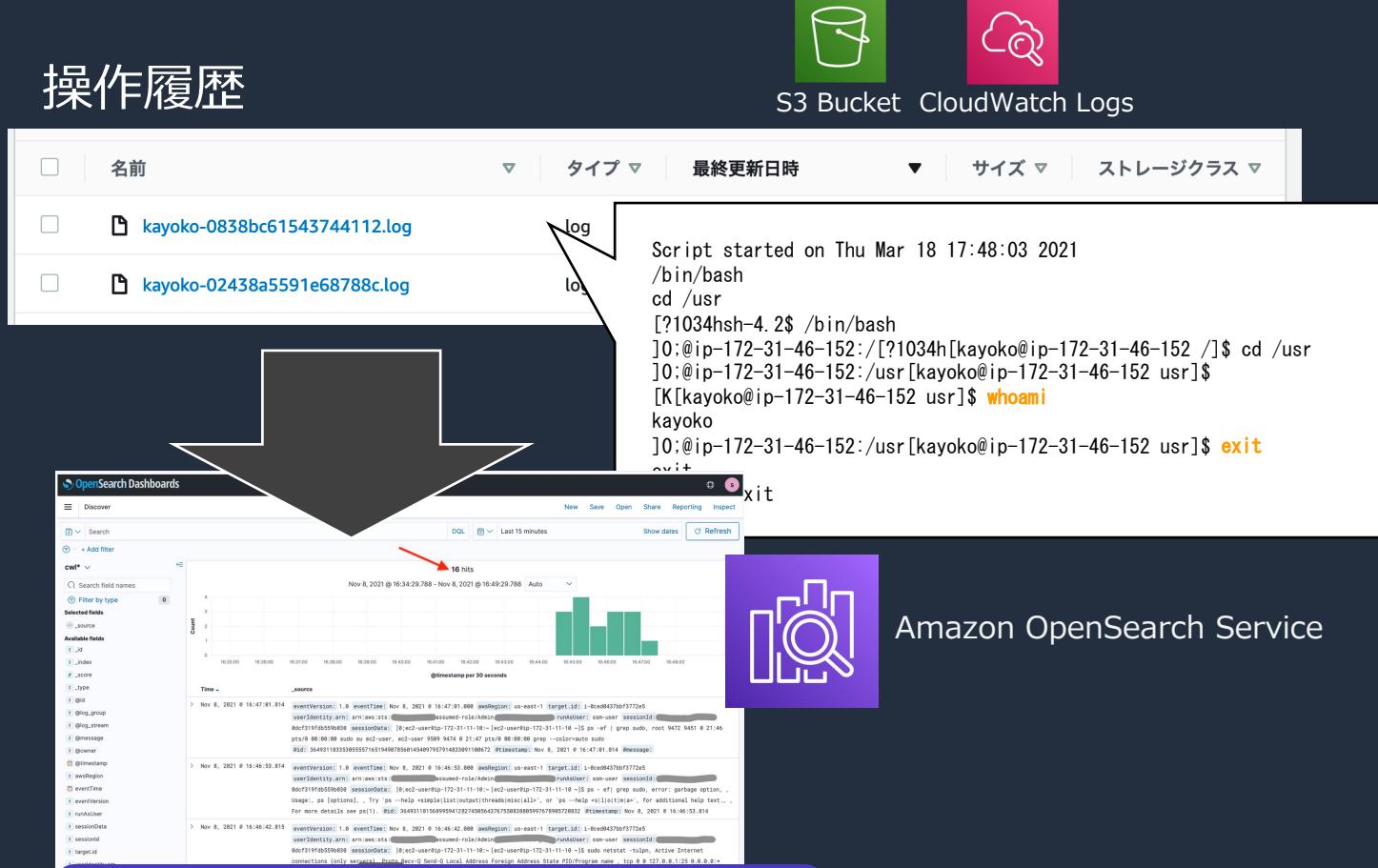
- インバウンドポートを開くことなく、ブラウザや CLI からインタラクティブなシェルアクセスを実現。
- ポートフォワーディングでのアクセスも可能。



Session Managerについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

Session Manager でのアクセス統制例



誰かがサーバにアクセスすると、 Slack に通知

「sudo」など特権コマンドの使用状況の確認(*)

(*) 詳細は[こちらのブログ](#)を参照
 「AWS Systems Manager Session Manager コンソールログを探索する」
© 2023, Amazon Web Services, Inc. or its affiliates.

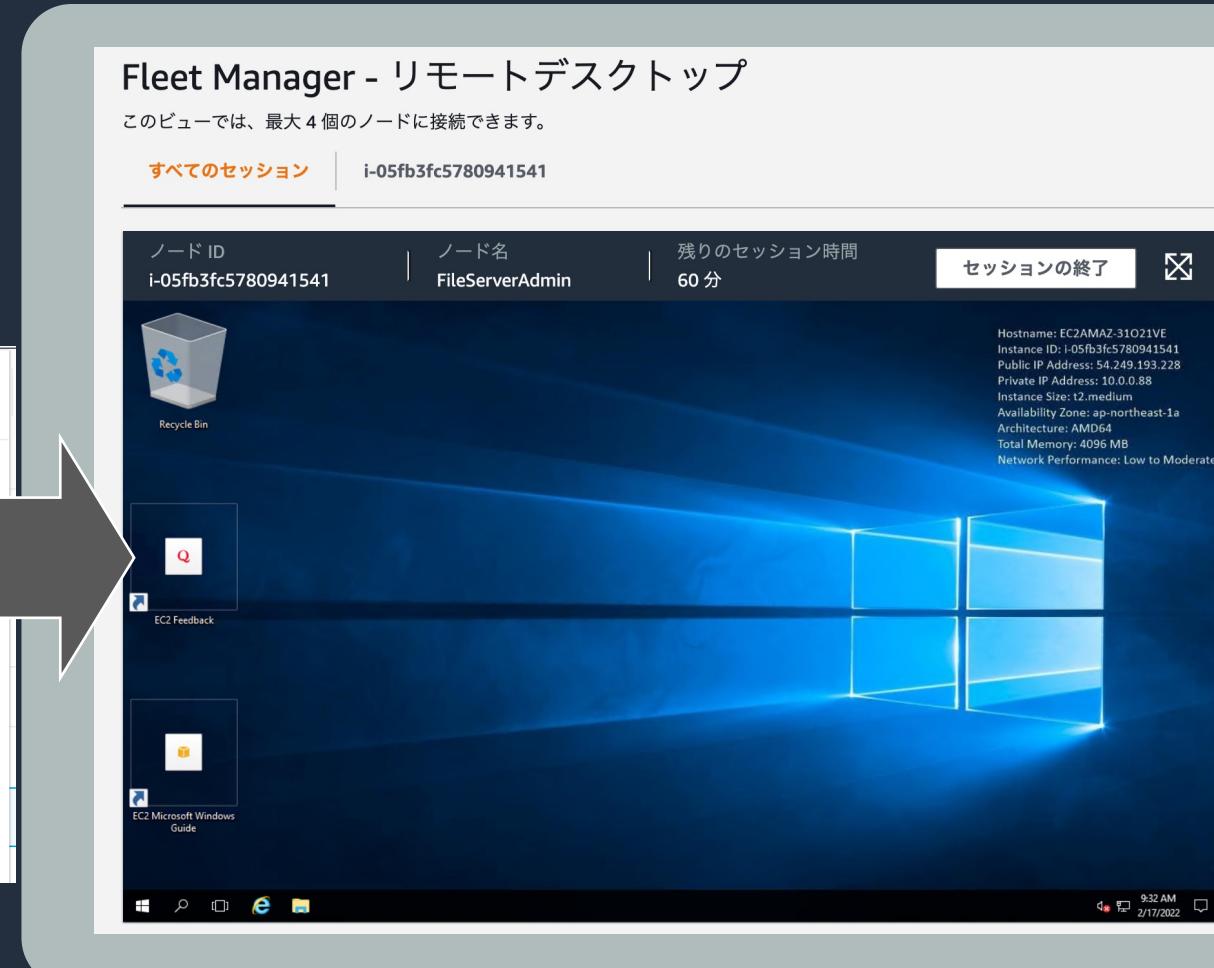
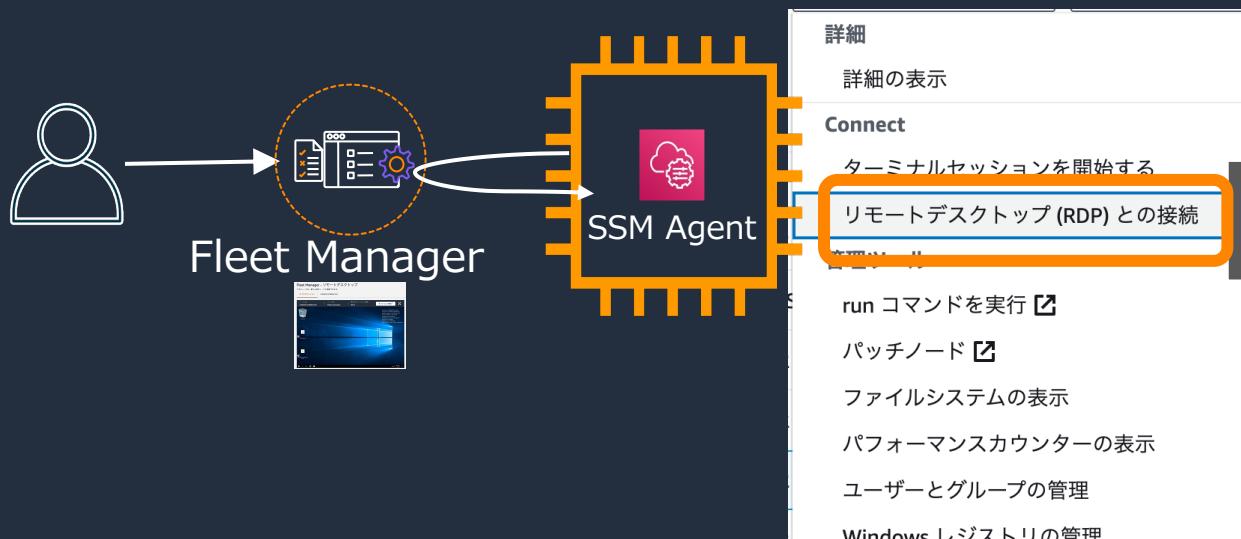


Remediate Issues

Fleet Manager

Windows サーバへのリモートデスクトップ機能

- Windows サーバーには、マネジメントコンソールからリモートデスクトップ (RDP) 接続も可能。

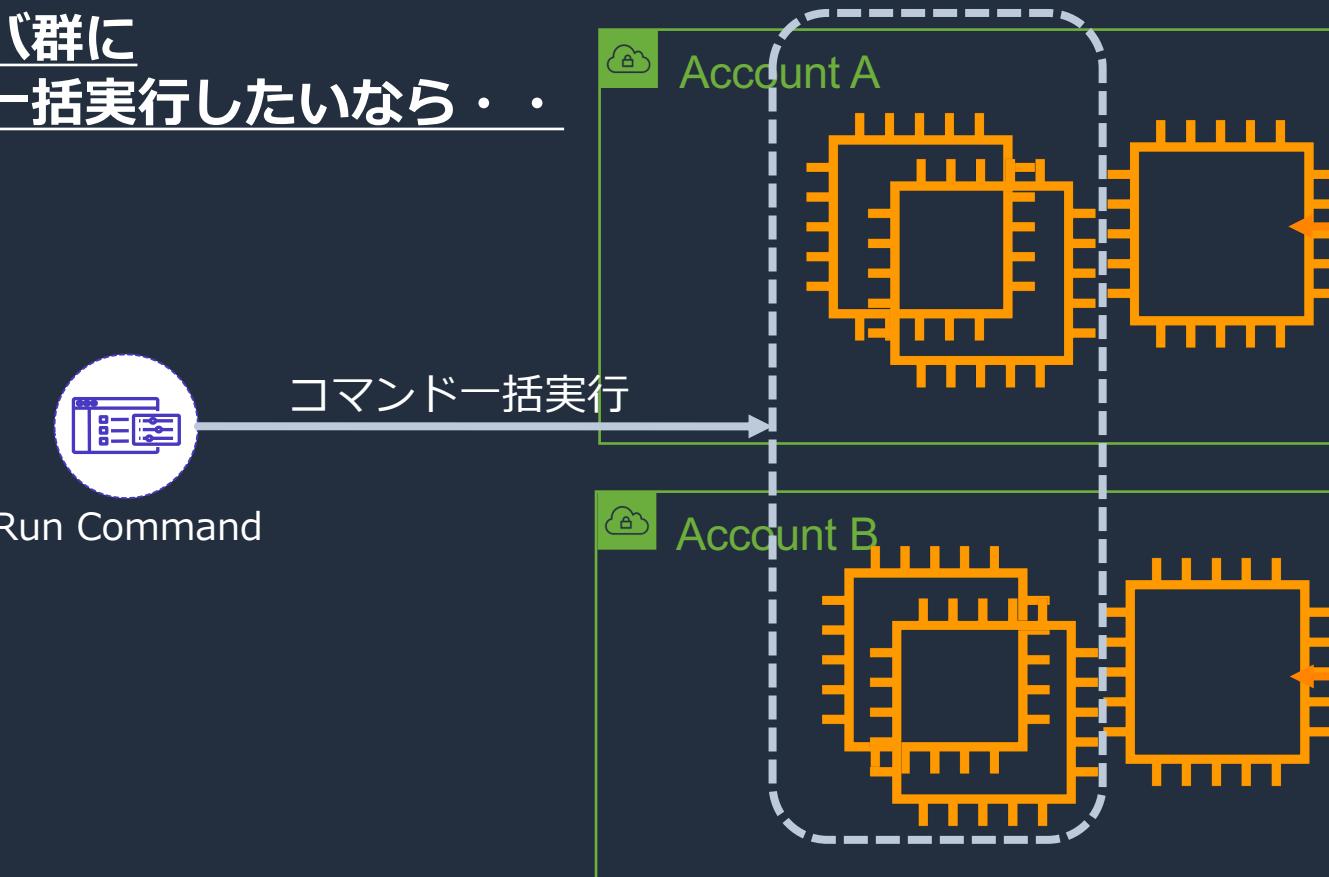


aws Fleet Manager の RDP 接続機能については[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

おさらい

対象サーバ群に
コマンド一括実行したいなら・・



個々のサーバに対して
インタラクティブにコマンド
操作したいなら・・



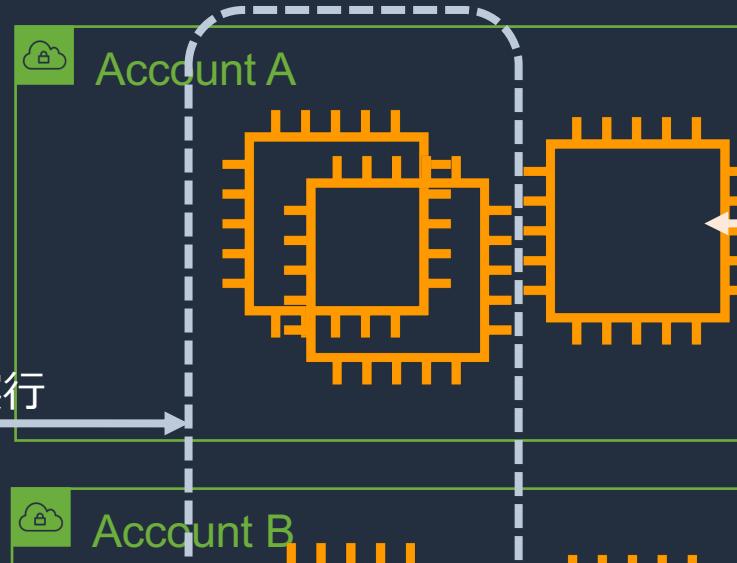
おさらい

対象サーバ群に
コマンド一括実行したいなら・・



Run Command

コマンド一括実行



個々のサーバに対して
インタラクティブにコマンド
操作したいなら・・

シェルアクセスなど



Session Manager

インシデント管理って
どうしたらしいいの？



Incident Manager



Incident Manager

事前に準備された対応計画、ランブック、分析による改善

Remediate Issues

- アラームへの対応計画を指定し、適切な連絡先に自動通知、Runbook を自動起動し、迅速な対応が可能になる。
- チームはチャットで共同作業を行いながら問題を解決できる。
- インシデント後の分析ができ、将来の再発を防止できる。
- ServiceNow, Jira Service Management と連携可能



The screenshot shows the AWS Systems Manager Incident Manager interface. At the top, there's a navigation bar with 'AWS Systems Manager > Incident Manager > [BananaStand] Customer checkout failures'. On the right side of the header, there's a 'Resolve Incident' button. Below the header, there's a summary card with the following details:

- Title:** [BananaStand] Customer checkout failures
- Impact:** Critical
- Chat channel:** #order-processor
- Duration:** 8m
- Edit** button

Below the summary card, there are tabs for 'Overview', 'Metrics', 'Timeline', 'Runbook', 'Contacts', and 'Related items'. The 'Overview' tab is selected. Under the 'Summary' section, it says 'Incident in Progress' with three orange exclamation marks. The 'Summary of Incident' section contains a message: 'customers are unable to checkout due to connectivity failures in the OrderProcessor. Escalating to the Orders team on-call and manager for immediate resolution.' The 'Current Status' section shows three yellow question marks. In the 'Recent timeline events' section, there are several entries with timestamps and event types:

- April 8, 2021
 - 12:39:10 PM - OrderVolume added to metrics. (Metric added)
 - 12:39:10 PM - ErrorCount added to metrics. (Metric added)
 - 12:38:53 PM - Incident summary updated. (Summary updated)
 - 12:33:13 PM - The CriticalIncidentRunbook (\$LATEST) runbook step status is Pending. (Runbook status updated)
 - 12:33:12 PM - Incident Started (Custom event)

aws Incident Manager についての詳細は[こちら](#)。

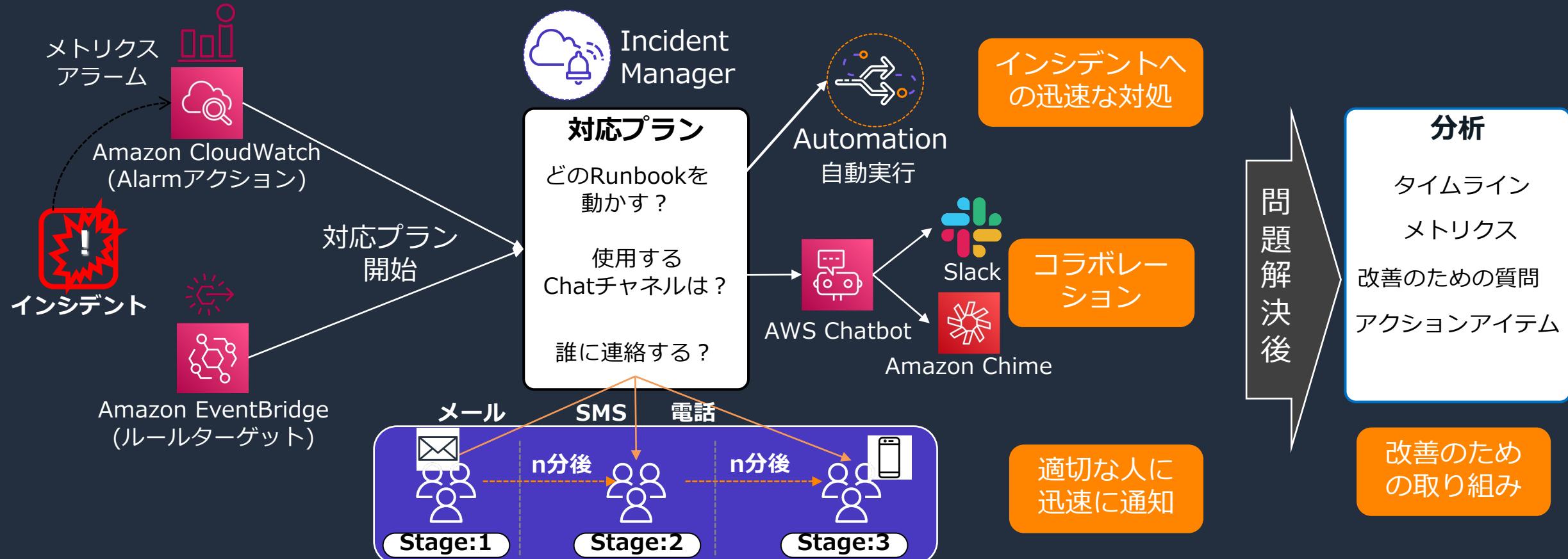
© 2023, Amazon Web Services, Inc. or its affiliates.



Remediate Issues

Incident Manager

事前に準備された対応計画、ランブック、分析による改善



aws Incident Managerについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

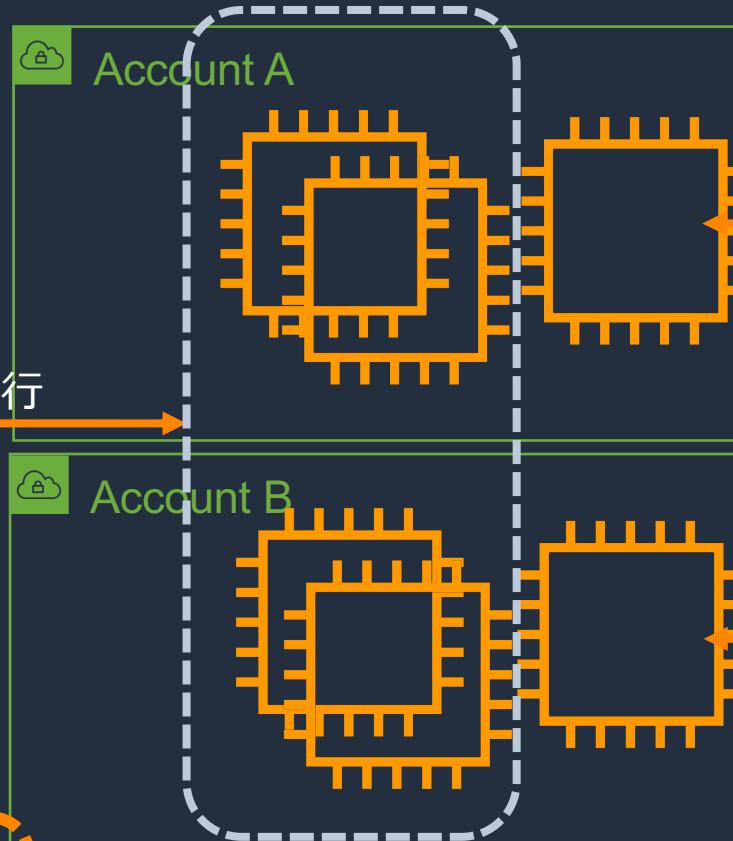
おさらい

対象サーバ群に
コマンド一括実行したいなら・・



Run Command

コマンド一括実行



インシデント管理



Incident Manager

個々のサーバに対して
インタラクティブにコマンド
操作したいなら・・

シェルアクセスなど



Session Manager

リモートデスクトップ接続



Fleet Manager

AWS Systems Manager の機能

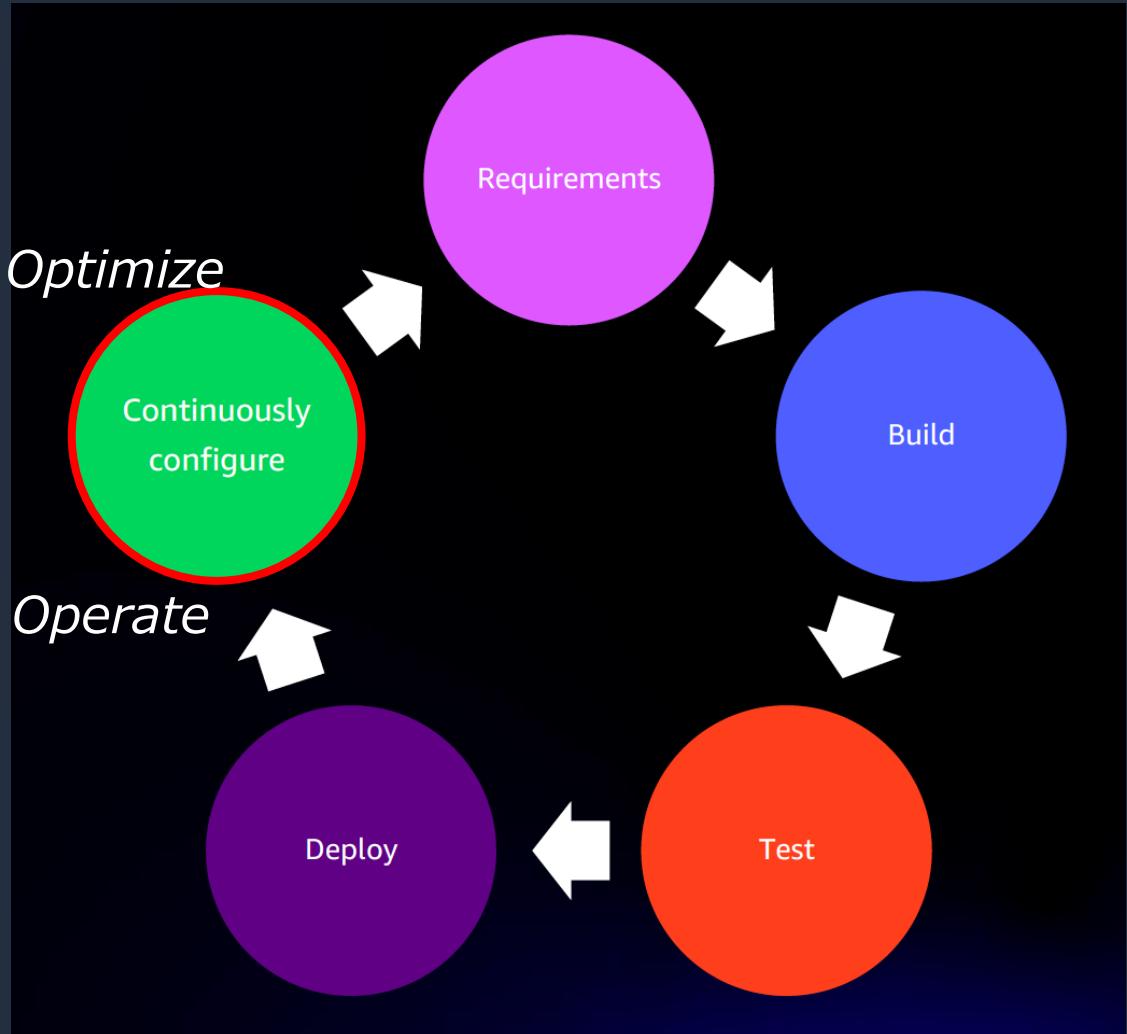


AWS Systems Manager の機能



Application Management

- アプリケーションはローンチして終わりではない。
- メンテナンスも含めて、ライフサイクルの管理が必要。
- 運用し、最適化していくための機能を用意。

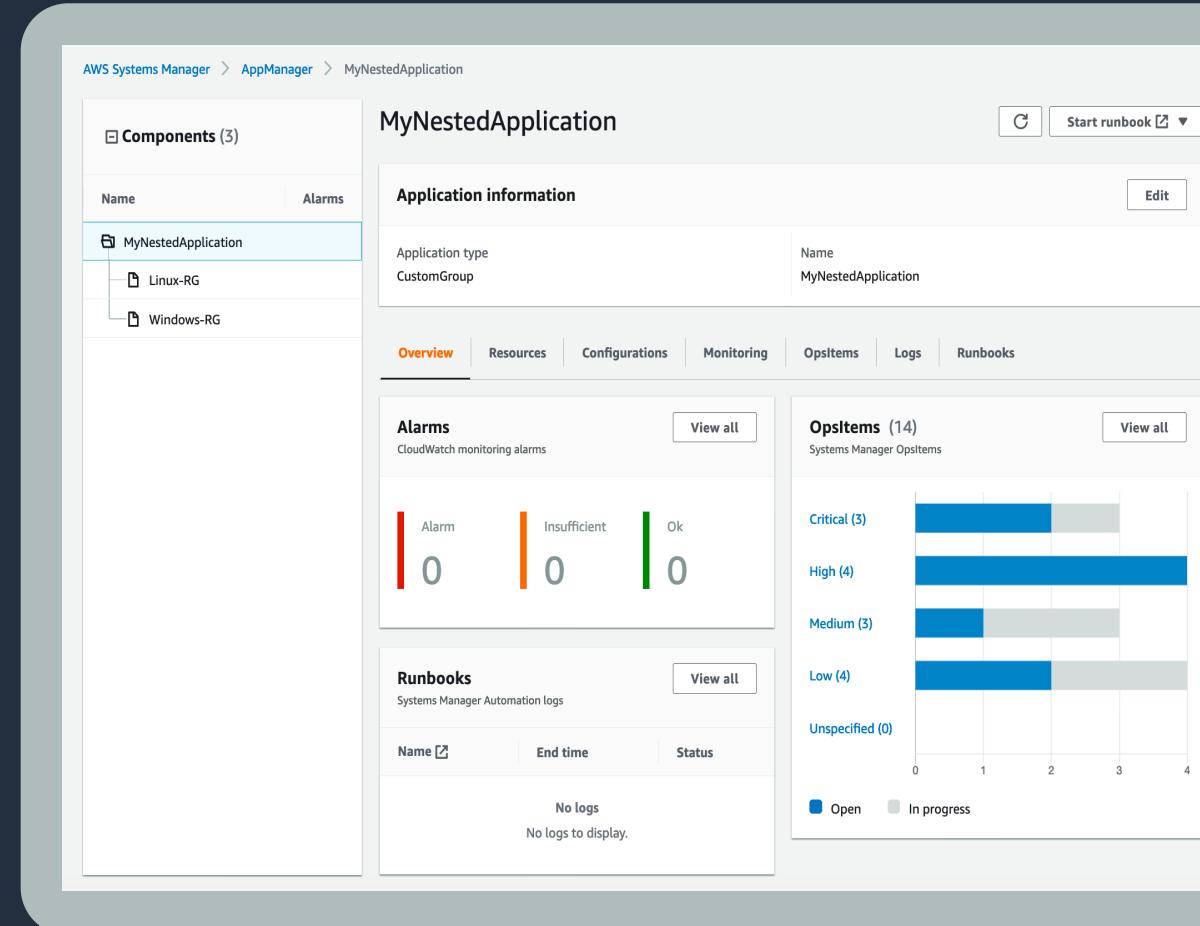


Application Manager

個々のリソースだけでなく、アプリケーションを管理する

- 一つのコンソールからアプリケーションを管理できる。
- アプリケーションのコンテキストで、CloudWatch アラームやコンプライアンスステータス、アプリケーションコストなどが確認できる。
- これらの AWS サービスをまだ有効にしている場合、Application Manager のコンソールから簡単に設定も可能

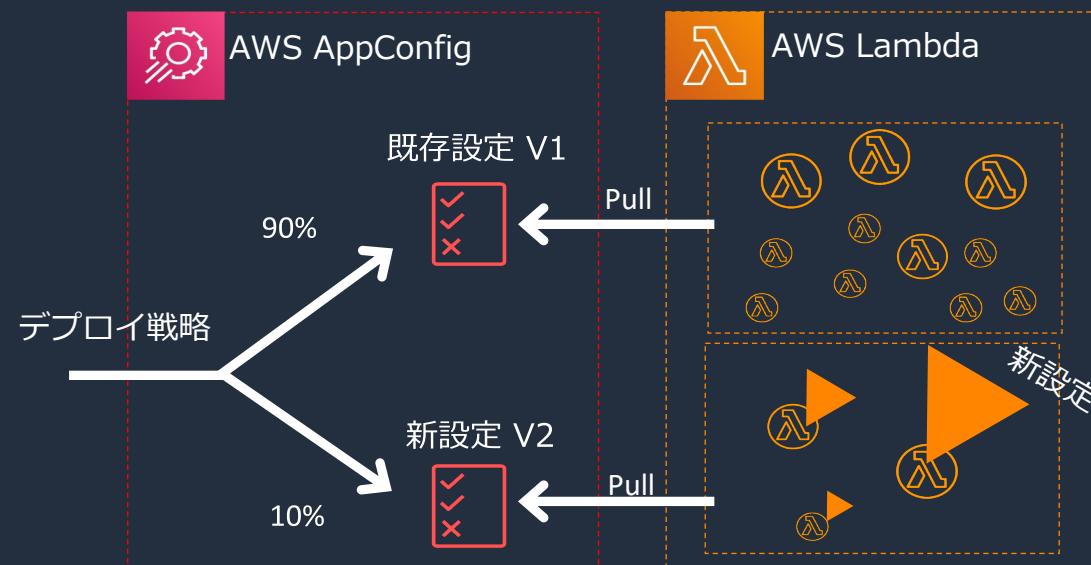
NEW
2022/07



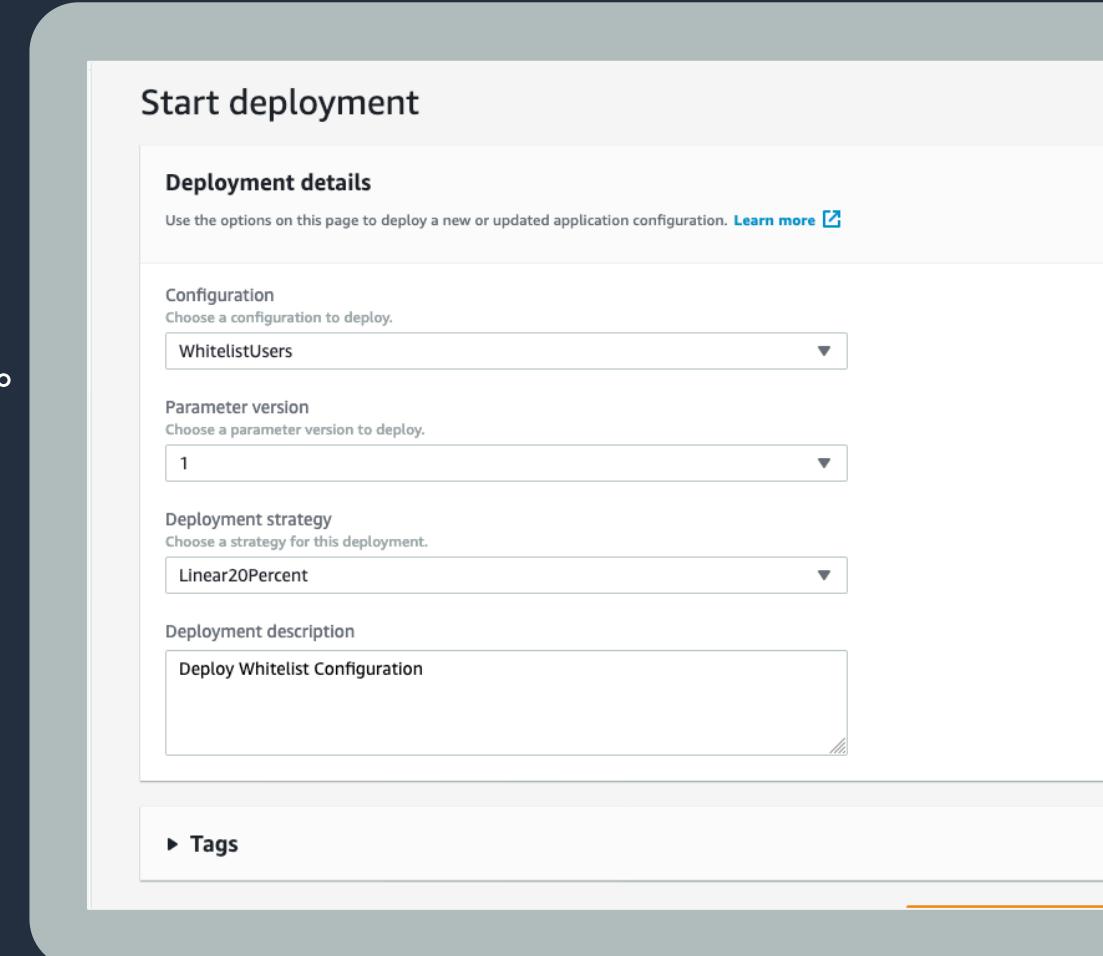
AppConfig

アプリケーション構成を作成、管理、デプロイ

- アプリケーションを実行したまま、
アプリケーション構成の変更をデプロイ。
- 製品の新発表など、タイムリーな展開が必要な
新機能の展開を、機能フラグで実現。
- デプロイ戦略を指定でき、少しずつデプロイが可能。



aws AppConfig についての詳細は[こちら](#)。



Parameter Store

アプリケーション構成値の一元的な格納

- ④ アプリケーションの設定値とシークレットを格納。
- ④ すべてのパラメーターを 1 か所で一元的に更新することで、コードのメンテナンスと自動化を簡素化。

The screenshot shows the AWS Systems Manager Parameter Store interface. The top navigation bar includes 'AWS Systems Manager' and 'Parameter Store'. Below the navigation, there are two tabs: 'Parameters' (which is selected) and 'Settings'. The main area is titled 'Parameters' and contains a search bar. A table lists five parameters:

Name	Tier
/prod/dbstring	Advanced
/prod/licensecode	Standard
/prod/licensecode_dbcluster2	Standard
/test/dbstring	Standard

 Parameter Store についての詳細は[こちら](#)。

AWS Systems Manager の機能

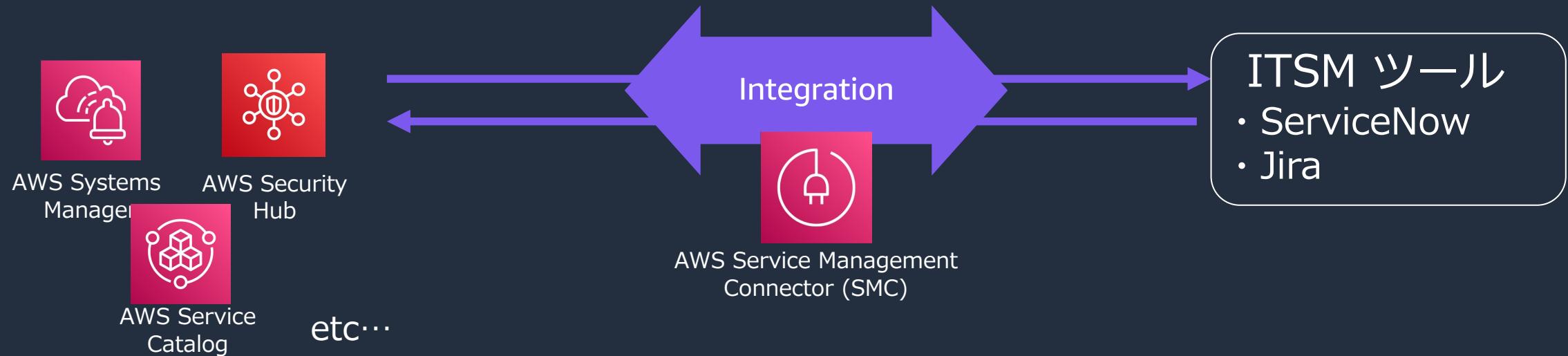
運用管理	アプリケーション管理	変更管理	ノード管理
 Explorer	 Application Manager	 Change Manager	 Fleet Manager
 OpsCenter	 AppConfig	 Automation	 Session Manager
 Incident Manager	 Parameter Store	 Maintenance Windows	 Inventory
		 Change Calendar	 Run Command
			 Patch Manager
			 Distributor
			 State Manager

Quick Setup

3rd Party の ITSM ツールとの連携

AWS Service Management Connector (SMC)

- ServiceNow や Jira などの使い慣れた ITSM ツールで AWS ネイティブのリソースと機能を管理、操作するためのコネクター
- 対象の ITSM ツール (2023/2現在)
 - ServiceNow
 - Atlassian Jira Service Management



aws SMCの詳細は[こちら](#)。

AWS Systems Manager にて連携できる機能

ITSM ツール	SSM Features	詳細
ServiceNow	OpsCenter	ServiceNow で OpsCenter 統合機能を有効にできる。ServiceNow で実行されたアクションを OpsCenter と同期、また、その逆の場合も同様に同期可能
	Incident Manager	Incident Manager でインシデント対応計画を自動化し、インシデントを ServiceNow に自動的に同期できる。インシデントの解決も可能。
	Automation	ServiceNow にて Runbook の実行・確認が可能。
	Change Manager	変更テンプレート、変更リクエストの確認、変更リクエストの実施、関連する CloudTrail イベントの確認が可能。 ※ 変更テンプレートがApprove済みなど前提あり。詳細は こちら
Jira Service Management	OpsCenter	Jira で OpsCenter 統合機能を有効にできる。ServiceNow で実行されたアクションを OpsCenter と同期、また、その逆の場合も同様に同期可能。
	Incident Manager	Incident Manager でインシデント対応計画を自動化し、インシデントを JSM に自動的に同期できる。インシデントの解決も可能。
	Automation	Jira にて Runbook の実行・確認が可能。

NEW
2022/6

NEW
2022/10

AWS Service Management Connector for ServiceNow の詳細は[こちら](#)

AWS Service Management Connector for Jira Service Management Data Center の詳細は[こちら](#)

AWS Service Management Connector for Jira Service Management Cloud の詳細は[こちら](#)



Systems Manager の セキュリティベストプラクティス



SSM を使用する上でのセキュリティーベストプラクティス

- ・ 「Systems Manager のセキュリティのベストプラクティス」をご参照ください
 - https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/security-best-practices.html

<一部を紹介>

- ・ 最小特権アクセスを実装する
 - ・ ユーザの IAM ポリシーは、該当リソース・特定アクションについてのみ有効に
 - ・ 例えば“ssm.StartSession”を Deny することで、セッションマネージャを使用しない設定が可能。
- ・ VPC エンドポイントを使用可能
- ・ 特別セキュアな処理が必要な場合は Session Manager に对话型コマンドのみを使用する
- ・ AWS および Systems Manager ツールを最新に保つ
- ・ CloudWatch / CloudTrail / AWS Config を使用

Systems Manager の料金

AWS Systems Manager の料金

- AWS Systems Manager の利用は**基本的に無料**
- 一部の機能は有料。詳細は[料金ページ](#)を参照してください。
 - OpsCenter (OpsItem の数とAPI コールの数に基づく課金)
 - IncidentManager (対応計画の数とSMS/音声メッセージの数に基づく課金)
 - AppConfig (APIコールの数とターゲットごとの構成更新の合計数に対して課金)
 - Parameter Store (アドバンスドパラメータ/スループットの上限を上げた場合課金)
 - Change Manager (変更リクエストの件数と API リクエスト数に基づく課金)
 - Automation (ステップカウント、ステップ実行時間、プレイブックに対して課金)
 - Distributor (独自パッケージのストレージ、APIコール、データ転送に基づく課金)
 - オンプレミス管理のアドバンストインスタンスティア (次ページ参照)
- その他関連サービスの使用量に応じた料金
 - Athena + QuickSight / Config / CloudWatch (カスタムメトリクス、Logs) / S3に格納したログデータ など

(参考) インスタンスティアの設定

- SSMでは、ハイブリッド環境のオンプレミスサーバ、エッジサービスおよび仮想マシン(VM)に、標準インスタンスティアとアドバンストインスタンスティアを提供。

	標準インスタンスティア (デフォルト)	アドバンストインスタンスティア
課金	無料	インスタンス実行時間に基づく 従量課金
登録できる サーバ数	リージョン/アカウントごとに 最大1000まで	リージョン/アカウントごとに 1000を超えるサーバを登録可能
その他	登録されているハイブリッドノードが 1,000 未満であっても、以下の場合はアドバンストインスタンスティアが必要 <ul style="list-style-type: none">EC2 以外のノードに接続するために Session Manager を使用したい。EC2 以外のノードで Microsoft がリリースしたアプリケーションにパッチを適用したい ※両者とも、EC2インスタンスでは無料で使用できます。	

まとめ



まとめ

- AWS Systems Manager は一つの統合された運用ソリューションとして進化しています。
- まずは SSM Agent を立ち上げてマネージドノードにするところから、ぜひ始めてみてください。
- AWS Systems Manager の活用により、みなさまの運用が、少しでも楽になりますように。

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!



AWS Black Belt Online Seminar

AWS Systems Manager

Quick Setup 編

渡邊 良臣

Solutions Architect
2023/12

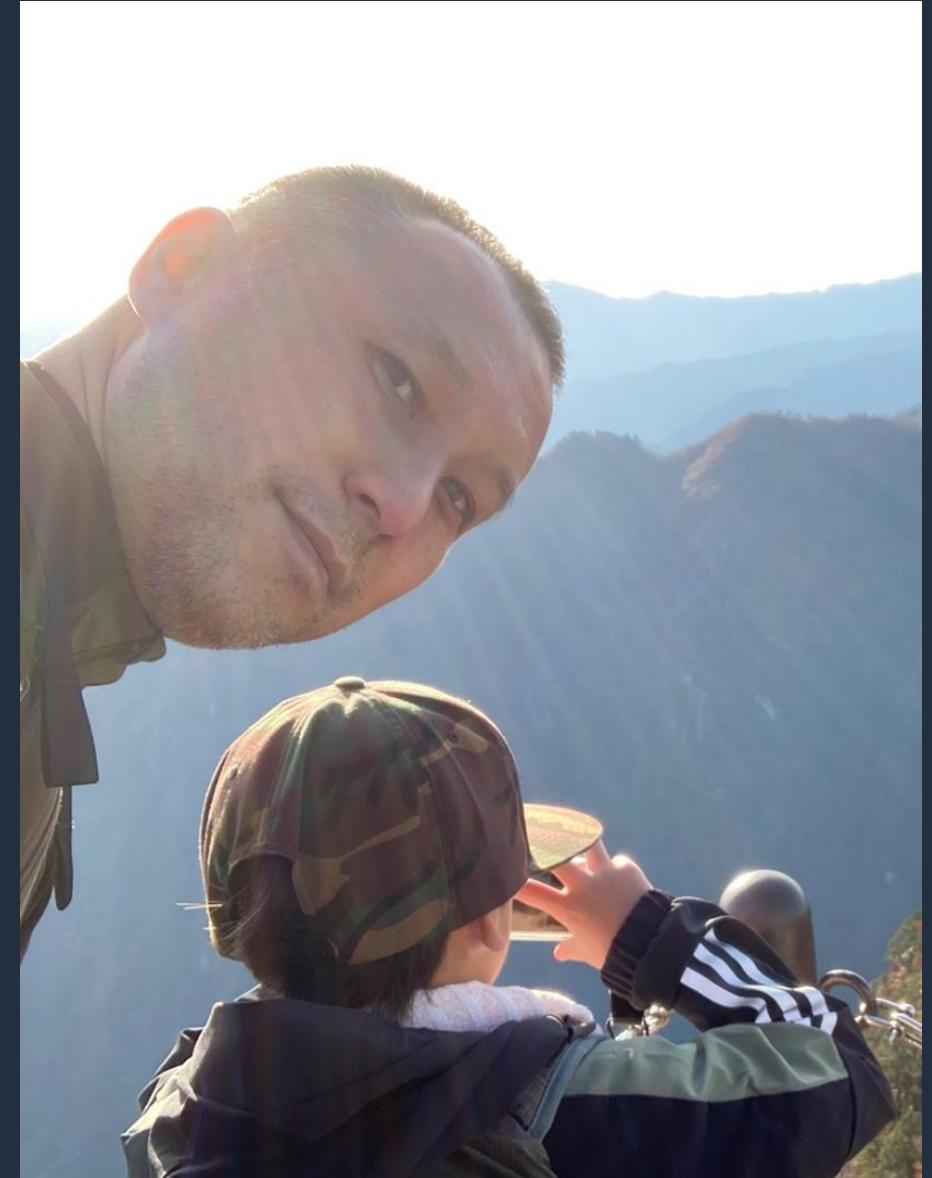
自己紹介

渡邊 良臣

アマゾンウェブサービスジャパン
ソリューションアーキテクト

西日本のお客様を中心にご支援しています。

好きな AWS サービス
AWS サポート



本セミナーの対象者

- ・既に AWS を利用されている運用担当者
- ・これから AWS を利用される予定の運用担当者
- ・ベストプラクティスを取り入れた運用設定を迅速にデプロイされたい方

アジェンダ

1. AWS Systems Manager とは
2. AWS Systems Manager Quick Setup の概要

3. 個別機能のご紹介

- Host Management
- Default Host Management Configuration
- Config Recording
- Conformance Packs
- Patch Manager
- DevOps Guru
- Change Manager
- Distributor
- Resource Scheduler
- OpsCenter
- Resource Explorer
- 補足

4. まとめ

1. AWS Systems Manager とは

AWS Systems Manager (SSM) とは



AWS Config
Configuration history



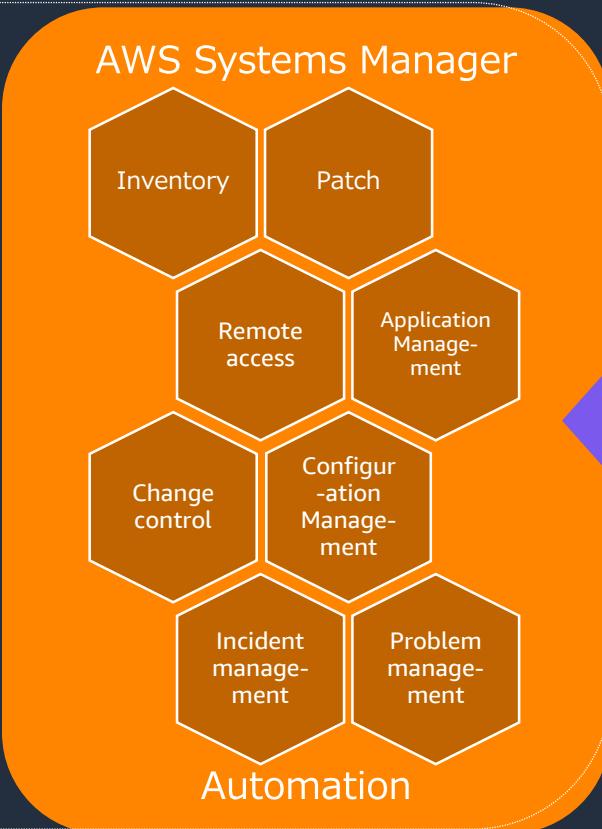
Amazon EventBridge
Notification and remediation



AWS CloudTrail
Audited actions



AWS Identity and Access Management (IAM)
Role-based access control



- Third-party tools
- ITSM
- Custom solutions

AWS の他のサービスや
3rd Party のツールと統合された
管理ソリューションを提供

(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

運用管理	アプリケーション管理	変更管理	ノード管理
 Explorer	 Application Manager	 Change Manager	 Fleet Manager
 OpsCenter	 AppConfig	 Automation	 Session Manager
 Incident Manager	 Parameter Store	 Maintenance Windows	 Inventory
		 Change Calendar	 Run Command
			 Patch Manager
			 Distributor
			 State Manager

Quick Setup

Systems Manager Agent (SSM Agent)

- 任意のノードをリモートで管理
 - EC2 インスタンス
 - IoT Greengrass を使用したエッジデバイス
 - オンプレミスや他のクラウドサーバー、VMs
- Linux, macOS, Raspberry Pi, Windows Server をサポート
 - サポート OS の一覧は[こちら](#)
 - Amazon Linux やWindows、Ubuntu などの一部のオフィシャルイメージには導入済み。プリインストールされた AMIs の一覧は[こちら](#)
- SSM Agent は、 SYSTEM (Windows) 、 root (Linux) で稼働
- SSM Agent はオープンソース。[GitHub](#)にて公開されている



2. AWS Systems Manager Quick Setup の概要

AWS Systems Manager Quick Setup の概要

- ・運用に役立つ AWS のサービスと機能を、推奨されるベストプラクティスで迅速に設定できる
- ・ダッシュボードに、構成デプロイのステータスがリアルタイムで表示される
- ・個別の AWS アカウントや、AWS Organizations と統合して複数 AWS アカウントにまたがって使用することができる
- ・複数の AWS リージョンに対しても展開が可能
- ・設定に差異が生じた場合は、修正が試みられる
- ・Quick Setup の使用にはコストがかからない

Quick Setup を利用するメリット

運用に有用な機能を利用する場合、アカウント毎やリージョン毎に個別で有効化や設定などの対応が必要



Quick Setup を利用すれば、マルチアカウント/マルチリージョンに対して容易にセットアップを行う事ができる



運用担当者の負荷が軽減

AWS Quick Setup の使用開始

The screenshot shows the AWS Systems Manager console with the Quick Setup feature. A red box labeled ① highlights the 'AWS Systems Manager' sidebar. Another red box labeled ② highlights the 'Quick Setup の使用を開始' section. A third red box labeled ③ highlights the '使用開始' button.

AWS Systems Manager

① 高速セットアップ

管理とガバナンス

AWS Quick Setup

ベストプラクティスに基づく、自動化されたシンプルな設定

AWS Quick Setup は、少ないクリック数で、組織全体で頻繁に使用される AWS のサービスと機能を設定するのに役立ちます。

仕組み

1. ホームリージョンを選択する
2. 設定タイプを選択する

Quick Setup は、指定した AWS リージョンですべての設定をデプロイするために使用される AWS リソースを作成します。ホームリージョンを一度選択すると、その後に変更することはできません。

Quick Setup には、一般的な設定タスクを自動化し、ベストプラクティスに基づいてサービスの設定をデプロイする設定タイプのライブラリが用意されています。

Quick Setup の使用を開始

まず、Quick Setup のためにホーム AWS リージョンを選択します。Quick Setup は、指定したリージョンで設定をデプロイするための AWS リソースを作成します。ホームリージョンを一度選択すると、その後に変更することはできません。

ホームリージョン
ap-northeast-1

使用開始

他のリソース

ドキュメント

よくある質問

サポートフォーラム

ホームリージョンを選択
② ap-northeast-1
③ 使用開始
④

AWS Quick Setup の使用開始

オンボーディング（使用開始）

Quick Setup が設定のデプロイに使用するホームリージョンを選択（後から変更不可）



「使用開始」をクリック

Quick Setup の利用に必要な IAM ロールを自動で作成



管理アカウントで開始した場合

AWS Organizations と AWS CloudFormation の間で信頼されたアクセスを有効

Quick Setup の開始に必要な IAM 権限と自動で作成される IAM ロールについては、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/quick-setup-getting-started.html

管理アカウントについて（AWS Organizations の用語と概念）については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_getting-started_concepts.html

Quick Setup の設定画面（作成）

Conformance Packs
AWS Config の使用

設定ステータス
○ 設定なし

説明
AWS Config が提供するコンフォーマンスパックをデプロイします。コンフォーマンスパックは、1つのエンティティとしてデプロイできる AWS Config ルールと修復アクションを集めたものです。

作成 ②

The screenshot shows the AWS Systems Manager Quick Setup interface. On the left, there's a sidebar with navigation links like 'Resource Management', 'Application Management', 'Change Management', 'Node Management', and 'Shared Resources'. The main area displays nine configuration options: Host Management, Config Recording, Conformance Packs, Patch Manager, Change Manager, DevOps Guru, Distributor, Resource Scheduler, and OpsCenter. The 'Conformance Packs' section is highlighted with a red box and labeled ①. A callout box on the right, also labeled ②, highlights the 'Create' button within this section.

Quick Setup の設定画面（削除）

The screenshot shows the AWS Systems Manager Quick Setup settings page. The interface includes a left sidebar with navigation links for various AWS services like AWS Lambda, CloudWatch Metrics, and CloudWatch Metrics Insights. The main area is titled 'Quick Setup' and has tabs for 'ライブラリ' (Library) and '設定' (Settings), with '設定' selected. A red box labeled ② highlights the '設定' tab. On the left, there's a filter section with 'フィルター条件' (Filter Conditions) and a list of '設定タイプ' (Setting Types). A red box labeled ③ highlights the 'Change Manager' entry in this list. The main content area displays a table of '設定' (Settings) with columns for '設定タイプ' (Setting Type), 'デプロイタイプ' (Deployment Type), '組織' (Organization), 'リージョン' (Region), 'デプロイのステータス' (Deployment Status), '関連付けのステータス' (Associated Status), and '最終更新日' (Last Updated Date). A red box labeled ④ highlights the 'アクション' (Actions) button at the top right of the table. Another red box labeled ⑤ highlights the '設定を削除' (Delete Setting) button within the actions menu. The table lists several entries, with the first one being 'Change Manager'.

設定タイプ	デプロイタイプ	組織	リージョン	デプロイのステータス	関連付けのステータス	最終更新日
Change Manager	組織	SSM-QS	該当なし (グローバル)	SUCCEEDED	なし	5日前
Config Recording	組織	SSM-QS	ap-northeast-1, us-east-2	SUCCEEDED	6 Success	1週間前
Conformance Packs	組織		該当なし	SUCCEEDED	2 Failed 2 Success	5日前
Default Host Management Configuration	組織	Root	ap-northeast-1, ap-northeast-2, ap-south-1...	SUCCEEDED	96 Success	5日前
DevOps Guru	組織	SSM-QS	ap-northeast-1, us-east-2	SUCCEEDED	8 Success	5日前
Distributor	組織	SSM-QS	ap-northeast-1, us-east-2	SUCCEEDED	2 Failed 22 Success	5日前
Host Management	組織	SSM-QS	ap-northeast-1, us-east-2	SUCCEEDED	1 Failed	5日前

各設定タイプで共通の処理概要



AWS Cloud

Quick Setup を設定するアカウント

設定リージョン

AWS Systems Manager

① 設定タイプの作成

ホームリージョン (※)

AWS CloudFormation

③ スタックセットの作成

AWS Identity and Access Management (IAM)

② IAM ロールの作成

ターゲットアカウント

ターゲットリージョン

④ スタックの作成

⑥ Runbook の作成

⑦ 関連付けの作成

⑤ IAM ロールの作成



処理概要

項目番	概要
①	任意のリージョンで設定タイプを作成する（ユーザー操作）
②	設定タイプのデプロイに必要な IAM ロールが作成される
③	Quick Setup を使用開始時に指定したホームリージョンにて、スタックセットが作成される
④	デプロイ先（ターゲット）のリージョンに、スタックセットのスタックが作成される
⑤	スタックから、設定タイプに必要な IAM ロールが作成される
⑥	スタックから、設定タイプに必要な Runbook（旧名：ドキュメント）が作成される
⑦	スタックから、設定タイプに必要な関連付けが作成される

スタックなどの用語については、以下をご参照ください。 (AWS CloudFormation#1 基礎編)

<https://www.youtube.com/watch?v=4dyiPsYXG8I>

Runbook や関連付けなどの用語については、以下をご参照ください。 (AWS Systems Manager State Manager)

<https://www.youtube.com/watch?v=vSAbhWZFtKU>



設定状況の可視化

設定の詳細から、設定デプロイや設定の関連付けのステータスを確認可能。



The screenshot shows the 'Quick Setup' section of the AWS Systems Manager console. On the left is a sidebar with filter conditions for 'Setting Type' and 'Deployment Type'. The main area is a table titled '設定' (Settings) showing deployment history:

リージョンまたはデプロイステータスで検索	詳細を表示	アクション	作成			
○ Change Manager	組織	QuickSetup	該当なし (グローバル)	○ SUCCEEDED	○ 2 Success	2 時間前
○ Config Recording	組織	QuickSetup	us-east-2, us-west-2	○ SUCCEEDED	○ 2 Success	2 時間前
○ Conformance Packs	組織	QuickSetup	該当なし	○ SUCCEEDED	○ 2 Success	2 時間前
○ DevOps Guru	組織	QuickSetup	us-east-2, us-west-2	○ SUCCEEDED	○ 2 Success	2 時間前
○ Distributor	組織	QuickSetup	us-east-2, us-west-2	○ SUCCEEDED	○ 1 Failed ○ 4 Success	2 時間前
○ Host Management	組織	QuickSetup	us-east-2, us-west-2	○ SUCCEEDED	○ 2 Failed ○ 5 Success	2 時間前
○ Patch Manager	組織	QuickSetup	us-east-2, us-west-2	○ SUCCEEDED	○ 1 Pending	2 時間前
○ Resource Scheduler	組織	QuickSetup	us-east-2, us-west-2	○ SUCCEEDED	○ 3 Success	2 時間前

設定テーブルから、デプロイタイプやデプロイ先のリージョンを確認可能。

3. 個別機能のご紹介

Host Management

Host Management の概要

- Amazon EC2 インスタンスの管理に必要な権限を、最小限の権限で付与
- 最新状態の維持が推奨されるエージェントについて、更新を自動化
- コンピューティング環境を可視化
- EC2 インスタンスの管理に慣れている方であれば、複数の EC2 インスタンスを纏めて効率的に管理する事が可能
- 以下の場合、Host Management はアンマッチの可能性がある
 - AWS の機能を試す等の目的で、初めて EC2 インスタンスを作成する場合
 - EC2 インスタンスの管理に不慣れな場合
- 同じ AWS リージョンを対象として、複数の Host Management 設定を作成することはできない

Host Management の設定画面（設定オプション）

設定オプション

Quick Setup は、ベストプラクティスに基づいて次の Systems Manager のコンポーネントを設定します。スケジュールするアクションのチェックボックスをオンにします。 詳細はこちら [\[リンク\]](#)

Systems Manager

Systems Manager (SSM) Agent を 2 週間ごとに更新します。

30 分ごとにインスタンスからインベントリを収集します。

不足しているパッチがないかインスタンスを毎日スキャンします。

Amazon CloudWatch

CloudWatch エージェントをインストールして設定します。

CloudWatch エージェントを 30 日に 1 回更新します。

Amazon EC2 起動エージェント

EC2 起動エージェントを 30 日ごとに 1 回更新します。
チェックボックスを選択すると、サポートされているオペレーティングシステムバージョン [\[リンク\]](#) にインストールされている EC2 Windows、Linux、Mac 起動エージェントのアップデートを受け取ることができます。

この設定を実行すると、Systems Manager Explorer [\[リンク\]](#) が有効になります。

CloudWatch エージェントの基本設定 [\[リンク\]](#) と Amazon CloudWatch の料金 [\[リンク\]](#) に含まれるメトリクスの詳細をご覧ください。

2 週間毎に SSM エージェントのアップデートをチェックし、新しいバージョンがリリースされていれば自動的に更新する。

SSM エージェントについては、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/ssm-agent.html

<https://www.youtube.com/watch?v=g5ndLFklyb4>

Host Management の設定画面（設定オプション）

設定オプション

Quick Setup は、ベストプラクティスに基づいて次の Systems Manager のコンポーネントを設定します。スケジュールするアクションのチェックボックスをオンにします。 詳細はこちら [\[リンク\]](#)

Systems Manager

Systems Manager (SSM) Agent を 2 週間ごとに更新します。

30 分ごとにインスタンスからインベントリを収集します。

不足しているパッチがないかインスタンスを毎日スキャンします。

Amazon CloudWatch

CloudWatch エージェントをインストールして設定します。

CloudWatch エージェントを 30 日に 1 回更新します。

Amazon EC2 起動エージェント

EC2 起動エージェントを 30 日ごとに 1 回更新します。
チェックボックスを選択すると、サポートされているオペレーティングシステムバージョン [\[リンク\]](#) にインストールされている EC2 Windows、Linux、Mac 起動エージェントのアップデートを受け取ることができます。

この設定を実行すると、Systems Manager Explorer [\[リンク\]](#) が有効になります。

CloudWatch エージェントの基本設定 [\[リンク\]](#) と Amazon CloudWatch の料金 [\[リンク\]](#) に含まれるメトリクスの詳細をご覧ください。

30 分毎に、以下のタイプのメタデータを収集する。

- AWS コンポーネント
- アプリケーション
- ノードの詳細
- ネットワーク設定
- サービス
- Windows ロール
- Windows の更新プログラム

インベントリについては、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-inventory.html

https://www.youtube.com/watch?v=2_6YcNmNFCg

Host Management の設定画面（設定オプション）

設定オプション

Quick Setup は、ベストプラクティスに基づいて次の Systems Manager のコンポーネントを設定します。スケジュールするアクションのチェックボックスをオンにします。 詳細はこちら [\[リンク\]](#)

Systems Manager

- Systems Manager (SSM) Agent を 2 週間ごとに更新します。
- 30 分ごとにインスタンスからインベントリを収集します。
- 不足しているパッチがないかインスタンスを毎日スキャンします。

Amazon CloudWatch

- CloudWatch エージェントをインストールして設定します。
- CloudWatch エージェントを 30 日に 1 回更新します。

Amazon EC2 起動エージェント

- EC2 起動エージェントを 30 日ごとに 1 回更新します。
チェックボックスを選択すると、サポートされているオペレーティングシステムバージョン [\[リンク\]](#) にインストールされている EC2 Windows、Linux、Mac 起動エージェントのアップデートを受け取ることができます。

この設定を実行すると、Systems Manager Explorer [\[リンク\]](#) が有効になります。

CloudWatch エージェントの基本設定 [\[リンク\]](#) と Amazon CloudWatch の料金 [\[リンク\]](#) に含まれるメトリクスの詳細をご覧ください。

デフォルトのパッチベースラインに基づいて、パッチの適用状況を毎日スキャンする。スキャンした結果は「コンプライアンス」のコンソール（ダッシュボード）に表示される。

パッチのスキャンとコンプライアンスレポートについては、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager.html

Host Management の設定画面（設定オプション）

Basic レベルについては、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/monitoring/create-cloudwatch-agent-configuration-file-wizard.html#cloudwatch-agent-preset-metrics



Host Management の設定画面（設定オプション）

設定オプション

Quick Setup は、ベストプラクティスに基づいて次の Systems Manager のコンポーネントを設定します。スケジュールするアクションのチェックボックスをオンにします。 詳細はこちら [\[リンク\]](#)

Systems Manager

- Systems Manager (SSM) Agent を 2 週間ごとに更新します。
- 30 分ごとにインスタンスからインベントリを収集します。
- 不足しているパッチがないかインスタンスを毎日スキャンします。

Amazon CloudWatch

- CloudWatch エージェントをインストールして設定します。
- CloudWatch エージェントを 30 日に 1 回更新します。

Amazon EC2 起動エージェント

- EC2 起動エージェントを 30 日ごとに 1 回更新します。
チェックボックスを選択すると、サポートされているオペレーティングシステムバージョン [\[リンク\]](#) にインストールされている EC2 Windows、Linux、Mac 起動エージェントのアップデートを受け取ることができます。

この設定を実行すると、Systems Manager Explorer [\[リンク\]](#) が有効になります。

CloudWatch エージェントの基本設定 [\[リンク\]](#) と Amazon CloudWatch の料金 [\[リンク\]](#) に含まれるメトリクスの詳細をご覧ください。

30 日毎に CloudWatch エージェントのアップデートをチェックし、新しいバージョンがリリースされていれば自動的に更新する。

CloudWatch エージェントについては、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html

<https://www.youtube.com/watch?v=fzVkJne3OMI>

Host Management の設定画面（設定オプション）

設定オプション

Quick Setup は、ベストプラクティスに基づいて次の Systems Manager のコンポーネントを設定します。スケジュールするアクションのチェックボックスをオンにします。 詳細はこちら [\[リンク\]](#)

Systems Manager

Systems Manager (SSM) Agent を 2 週間ごとに更新します。

30 分ごとにインスタンスからイベントリトリートを収集します。

不足しているパッチがないかインスタンスを毎日スキャンします。

Amazon CloudWatch

CloudWatch エージェントをインストールして設定します。

CloudWatch エージェントを 30 日に 1 回更新します。

Amazon EC2 起動エージェント

EC2 起動エージェントを 30 日ごとに 1 回更新します。

この設定を実行すると、Systems Manager Explorer [\[リンク\]](#) が有効になります。

30 日毎に、以下の起動エージェントのアップデートを
チェックし、新しいバージョンがリリースされていれば自動
的に更新する。

Windows インスタンス : EC2Config / EC2Launch / EC2Launch v2
Linux インスタンス (Amazon Linux 2023 はサポート外) : cloud-init
Mac インスタンス : ec2-macos-init

起動エージェントについては、以下をご参照ください。

Windows : https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/WindowsGuide/ec2-windows-instances.html

Linux : https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/user-data.html

macOS : https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2-mac-instances.html#ec2-macos-init

Host Management の設定画面 (ターゲット)

管理アカウントからの設定

ターゲット

ターゲットは、この設定のデプロイ場所を決定します。

この設定をデプロイするアカウントとリージョンを選択します。

組織全体

組織内のすべての OU とリージョンに設定をデプロイします。

カスタム

この設定をデプロイする OU とリージョンを選択します。

現在のアカウント

現在サインインしているアカウント内でこの設定をデプロイするリージョンを選択します。

組織内のすべてのアカウントとリージョンを対象とする。タグなどによるインスタンスの指定は不可。

組織内の OU とリージョンを選択可能。タグなどによるインスタンスの指定は不可。

「現在のアカウント」を選択した場合、次頁の非管理アカウントで設定する際と同様の選択となる。

Host Management の設定画面 (ターゲット)

非管理アカウントからの設定

The screenshot shows two side-by-side configurations of the 'Target' settings page. Both pages have identical top sections: 'Target' (ターゲット) and its description ('Target is where this setting is deployed.'), followed by a note about choosing between regions or custom sets.

Left Configuration (Non-managed Account):

- Region Selection:** The 'Current Region' radio button (現在のリージョン) is selected. A red box highlights this choice, and a red arrow points down to the instance targeting section.
- Instance Targeting:** The 'All Instances' radio button (すべてのインスタンス) is selected. A red box highlights this choice, and another red arrow points down to the 'Target Region' section.
- Right Configuration (Non-managed Account):**
- Region Selection:** The 'Select Region' radio button (リージョンを選択) is selected. A red box highlights this choice, and a red arrow points down to the 'Target Region' section.
- Instance Targeting:** The 'All Instances' radio button (すべてのインスタンス) is selected. A red box highlights this choice, and another red arrow points down to the 'Target Region' section.

Bottom Notes:

 - Left Note:** 'Non-managed account target "Current Region" selection leads to targeting via Region, Resource Group, Tag, or Manual for 4 choices.'
 - Right Note:** 'Non-managed account target "Select Region" selection leads to targeting via "All Instances" or "Tag" choice only.'

Host Management の設定（インスタンスプロファイル）

管理アカウントからの設定

インスタンスプロファイルのオプション

必要な IAM ポリシーを、インスタンスにアタッチされている既存のインスタンスプロファイルに追加します。



このオプションを有効にすると、デフォルトの動作が変更されます

デフォルトでは、Quick Setup は、選択した設定に必要な許可を持つ IAM ポリシーとインスタンスプロファイルを作成します。その後、Quick Setup によって作成されたインスタンスプロファイルは、インスタンスプロファイルがアタッチされていないインスタンスにのみアタッチされます。このオプションを有効にすると、Quick Setup は、インスタンスプロファイルがアタッチされたインスタンスにも IAM ポリシーを追加します。

管理アカウントにて設定する場合のみ、インスタンスプロファイルのオプションが表示される。

チェックを入れる事で、EC2 にアタッチされている既存の IAM ロール（インスタンスプロファイル）に対して、必要な権限（IAM ポリシー）がアタッチされる。

3. 個別機能のご紹介

Default Host Management Configuration

Default Host Management Configuration の概要

- EC2 インスタンスに IAM ロール（インスタンスプロファイル）をアタッチしなくても、SSM で管理する事ができる
- EC2 インスタンスを管理するために必要となる最小限のアクセス許可が使用される
- Default Host Management Configuration (DHMC) を設定する前に、以下の要件が満たされている必要がある
 - 対象の EC2 インスタンスに、最新バージョン（3.2.582.0 以降）の SSM エージェントがインストールされている事
 - 対象の EC2 インスタンスが、Instance Metadata Service Version 2 (IMDSv2) を使用している事

Default Host Management Configuration (DHMC) については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/managed-instances-default-host-management.html

設定タイプの差違

非管理アカウントからの設定

AWS Systems Manager X

Systems Manager > Quick Setup

Quick Setup

設定タイプ

Q 以下の結果をフィルタリング

 Host Management Systems Manager の使用 設定ステータス <input checked="" type="radio"/> 設定なし 説明 IAM ロールを設定し、Amazon EC2 インスタンスを安全に管理するために一般的に使用されている Systems Manager 機能を利用します。 <button>作成</button>	 Config Recording AWS Config の使用 設定ステータス <input checked="" type="radio"/> 設定なし 説明 選択した AWS リソースタイプへの変更を追跡し記録できるようにします。記録されたデータの配偶イプションと通知オプションを設定します。 <button>作成</button>	 Conformance Packs AWS Config の使用 設定ステータス <input checked="" type="radio"/> 設定なし 説明 AWS Config が提供するコンフォーマンスパックをデプロイします。コンフォーマンスパックは、1つのエンティティとしてデプロイされると AWS Config ルールと修復アクションを集めたものです。 <button>作成</button>
 Patch Manager Systems Manager の使用 設定ステータス <input checked="" type="radio"/> 設定なし 説明 1つのアカウントまたは組織全体で、アプリケーションとノードパッチ適用を自動化します。 <button>作成</button>	 DevOps Guru DevOps Guru の使用 設定ステータス <input checked="" type="radio"/> 設定なし 説明 アプリケーションの運用パフォーマンスと可用性の向上に寄与。機械学習を活用した DevOps Guru サービスを有効にします。 <button>作成</button>	 Distributor Systems Manager の使用 設定ステータス <input checked="" type="radio"/> 設定なし 説明 エージェントなどのソフトウェアパッケージを Amazon EC2 インスタンスに配布できるようにします。 <button>作成</button>
 Resource Scheduler AWS リソリューションを利用 設定ステータス <input checked="" type="radio"/> 設定なし 説明 指定した時間にインスタンスが停止および開始するようにスケジュールします。 <button>作成</button>		

管理アカウントで設定
プを表示した時だけ
Default Host Manager
Configuration が表示さ
る

管理アカウントで設定タイプを表示した時だけ
Default Host Management Configuration が表示される

管理アカウントからの設定

AWS Systems Manager X

Systems Manager > Quick Setup

Quick Setup

監定タイプ

Q 以下の結果をフィルタリング

<p>Host Management Systems Manager の使用</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 IAM ロールを除むし、Amazon EC2 インスタンスを安全に管理するため一括的に使用されている Systems Manager 能力を有効にします。</p> <p>作成</p>	<p>Config Recording AWS Config の使用</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 選択した AWS リソースタイプへの変更を追跡し記録できるようになります。収集されたデータの配信オプションと通知オプションを指定します。</p> <p>作成</p>	<p>Conformance Packs AWS Config の使用</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 AWS Config が提供するコンフォーマンスパックをデプロイします。コンフォーマンスパックは、1つのエンティティとしてデプロイできる AWS Config ルールと修復アクションを集めたもので</p> <p>作成</p>
<p>Patch Manager Systems Manager の使用</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 1つのマガメントまたは網羅全体で、アプリケーションノードのパッチ適用を自動化します。</p> <p>作成</p>	<p>Change Manager Systems Manager の使用</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 Change Manager が網羅全体で行なう変更を呼び出すために必要な IAM ロールを設定します。</p> <p>作成</p>	<p>DevOps Guru DevOps Guru の使用</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 アプリケーションの運用パフォーマンスと可用性の向上に役立つ、機械学習を活用した DevOps Guru サービスを効率的にします。</p> <p>作成</p>
<p>Distributor Systems Manager の使用</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 エージェントなどのソフトウェアパッケージを Amazon EC2 インスタンスに配布できるようにします。</p> <p>作成</p>	<p>Resource Scheduler AWS ソリューションを利用</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 指定期間にインスタンスが停止および開始するようにスケジュールします。</p> <p>作成</p>	<p>OpsCenter Powered by Systems Manager</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 Enables OpsCenter を中央化して複数の AWS アカウントの問題を一元化して監視します。</p> <p>作成</p>
<p>Default Host Management Configuration Systems Manager の利用</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 網羅内のすべてのマガメントリージョンのデフォルトホスト管理構成を有効にします。</p> <p>作成</p>	<p>Resource Explorer AWS Resource Explorer を利用</p> <p>指定ステータス <input checked="" type="radio"/> 指定なし</p> <p>説明 AWS Resource Explorer を使用して、リージョン全体でリソースを検索および抽出するために必要なリソースを投票します。</p> <p>作成</p>	

Default Host Management Configuration の設定画面 (設定オプション)

設定オプション

SSM エージェントの自動更新を 2 週間ごとに有効にする (推奨)

情報
このオプションを有効にすると、AWS 組織内のすべての EC2 インスタンスが SSM エージェントの最新バージョンに自動的にアップグレードされます。これにより、インスタンスはフリート全体で常に最新の機能とバグ修正を受けられるようになります。詳細は[こちら](#)

2 週間毎に SSM エージェントのアップデートをチェックし、新しいバージョンがリリースされていれば自動的に更新する。

3. 個別機能のご紹介

Config Recording

Config Recording の概要

- 利用が推奨されている AWS Config を迅速に有効化できる
- ターゲットの Config 設定が変更された場合は、Config Recording から設定の修復が試みられる
- 既存の Config 設定がある場合は、Config Recording で指定したリソースタイプが追加される
- 既に指定しているリソースタイプは削除されずにマージされる
- Quick Setup の Config Recording の設定を削除しても、有効化された Config は無効化されない
- 作成した S3 バケットと SNS トピックも保持される

AWS Config については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/WhatIsConfig.html

AWS Config のベストプラクティスについては、以下をご参照ください。

<https://aws.amazon.com/jp/blogs/news/aws-config-best-practices/>

Config Recording の設定画面（設定オプション）

設定オプション

Config で記録する対象を選択する。

記録する AWS リソースタイプを選択

- このリージョンでサポートされているすべてのリソースタイプ
- 特定のリソースタイプを記録

グローバルリソース (AWS IAM リソースなど) を含める
サポートされているグローバルリソースタイプは、IAM ユーザー、グループ

IAM などのグローバルリソース（特定のリージョンに結びついていないサービス）を対象にする。

配信設定

- 新しい S3 バケットを作成
- 既存の S3 バケットを選択

通知オプション

AWS Config は Amazon Simple Notification Service (SNS) を使用して、変更された AWS リソースを監視します。

Config の設定スナップショットを送信する先のバケットを指定する。

- 通知をストリーミングしない
- 既存の SNS トピックを使用
AWS Config で通知に使用するアカウント ID と SNS トピック名を、そのアカウント内に指定します。
- SNS トピックを作成
SNS トピックは、選択する組織単位 (OU) 内の各アカウントについて作成されます。

Config イベントを通知するトピックを選択する。
既存トピックを使用する場合は、トピック名の制約に注意する。

Config Recording の設定画面（グローバルリソースの記録）

設定オプション

記録する AWS リソースタイプを選択

このリージョンでサポートされているすべてのリソースタイプ

特定のリソースタイプを記録

グローバルリソース (AWS IAM リソースなど) を含める
サポートされているグローバルリソースタイプは、IAM ユーザー、グル
グローバルリソースを記録するリージョンを選択

us-east-1 (N. Virginia) ▾

グローバルリソースの記録を、指定した
リージョンに記録させる。

配信設定

新しい S3 バケットを作成

既存の S3 バケットを選択

通知オプション

AWS Config は Amazon Simple Notification Service (Amazon SNS) トピックを使用して、重要な AWS Config イベントについて通知します。

通知をストリーミングしない

既存の SNS トピックを使用
AWS Config で通知に使用するアカウント ID と SNS トピック名を、そのアカウント内で指定します。

SNS トピックを作成
SNS トピックは、選択する組織単位 (OU) 内の各アカウントについて作成されます。

Config Recording の設定画面（スケジュール）

The screenshot shows two views of the AWS Config Recording settings screen, specifically the 'Schedule' tab. Both views have a red box highlighting the 'Schedule' section.

Left View (Default Selection):

- スケジュール**: 選択した設定オプションを Quick Setup が適用する頻度
- デフォルト
1回適用
- カスタム
指定した設定オプションを適用する頻度を選択

説明文: ① 設定の頻度を指定することで、Quick Setup は、適用する設定に加えられた変更を修復できます。

Right View (Custom Selection):

- スケジュール**: 選択した設定オプションを Quick Setup が適用する頻度
- デフォルト
1回適用
- カスタム
指定した設定オプションを適用する頻度を選択

説明文: Quick Setup は、適用する設定に加えられた変更を修復できます。

スケジュール頻度選択肢:

- 無効
- 毎日
- 7 日ごと
- 30 日ごと
- 無効

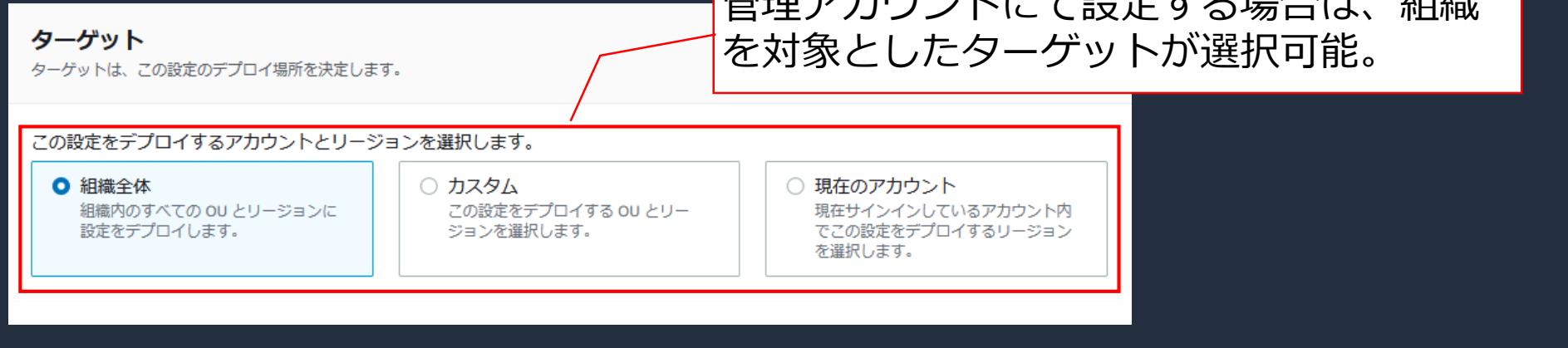
Red arrows point from the 'Default' and 'Custom' sections of the left view to their corresponding sections in the right view. Red boxes highlight the 'Default' section in the left view and the 'Custom' section in the right view. A large red box encloses the entire 'Schedule' section in both views.

Left View Callout: 「デフォルト」を選択すると、1回だけ実行される。

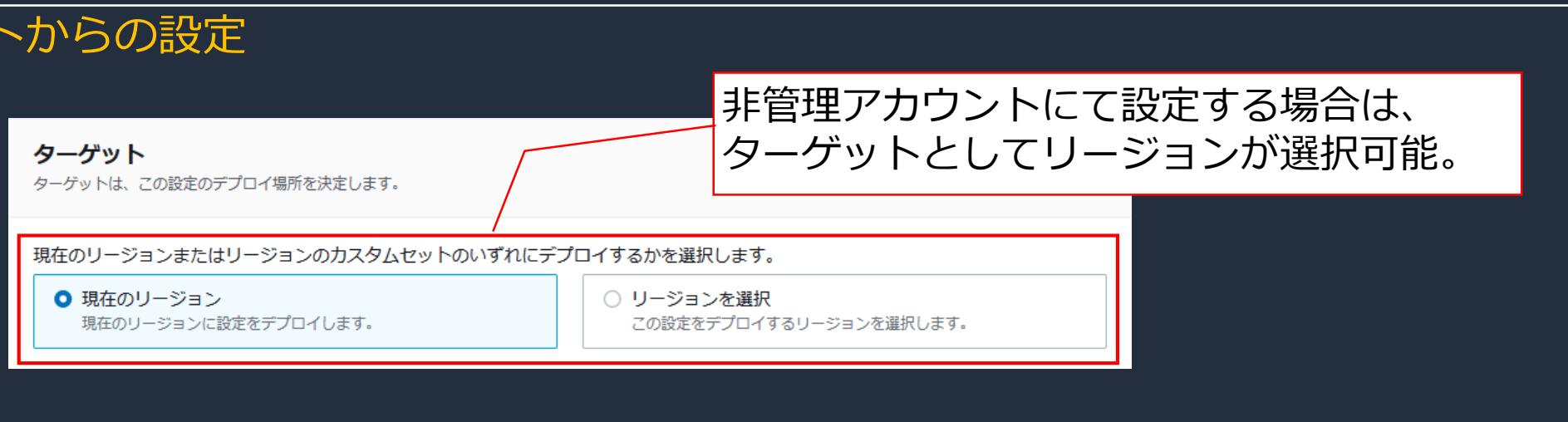
Right View Callout: 「カスタム」を選択すると、指定したスケジュールに基づいて設定差違の修復を試みることが出来る。

Config Recording の設定画面 (ターゲット)

管理アカウントからの設定



非管理アカウントからの設定



3. 個別機能のご紹介

Conformance Packs

Conformance Packs の概要

- AWS Config ルールと修復アクションの集まりであるコンフォーマンスパックを、マルチアカウント / マルチリージョンにデプロイできる
- 複数のコンフォーマンスパックを選択し、纏めて適用が可能
- 前提として、Config Recording が有効になっている事
- Quick Setup から設定を削除しても、既に適用されたコンフォーマンスパックは削除されない

AWS Config conformance packs については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/conformance-packs.html

Conformance Packs の設定画面 (コンフォーマンスパックの選択)

コンフォーマンスパックを選択

デプロイするコンフォーマンスパックを選択。

コンフォーマンスパックのサンプルテンプレートを選択 ▾

Operational Best Practices for AWS Well Architected Security Pillar X

 最大 5 個のコンフォーマンスパックを選択できます
また、サービス制限が適用されます。AWS Config サービスの制限の詳細をご覧ください [↗](#)。

Conformance Packs の設定画面（スケジュール）

スケジュール

選択した設定オプションを Quick Setup が適用する頻度

Config Recording と同様に、定期的に設定差違の修正を試みることが出来る。

- デフォルト
1回適用

- カスタム
指定した設定オプションを適用する頻度を選択

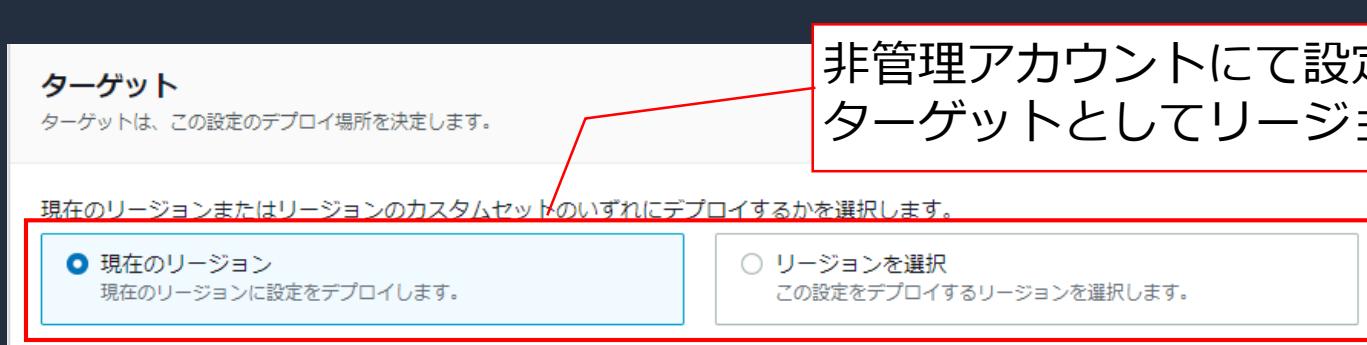
① 設定の頻度を指定することで、Quick Setup は、適用する設定に加えられた変更を修復できます。

Conformance Packs の設定画面（ターゲット）

管理アカウントからの設定



非管理アカウントからの設定



Conformance Packs の設定画面 (委任管理者アカウントの指定)

管理アカウントからの設定

コンフォーマンスパックの管理を委任するアカウントの指定。

管理アカウントでのターゲット設定時に、「組織全体」か「カスタム」を選択した時だけ表示される。

委任された管理者アカウント

委任されたアカウントは、組織内の複数のアカウントを表示し、これらのアカウントに対する変更を開始できます。

委任された管理者として登録する AWS Organization メンバーアカウントのアカウント ID を入力します。

123456789321

コンフォーマンスパックの委任管理者については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/conformance-pack-organization-apis.html

3. 個別機能のご紹介

Patch Manager

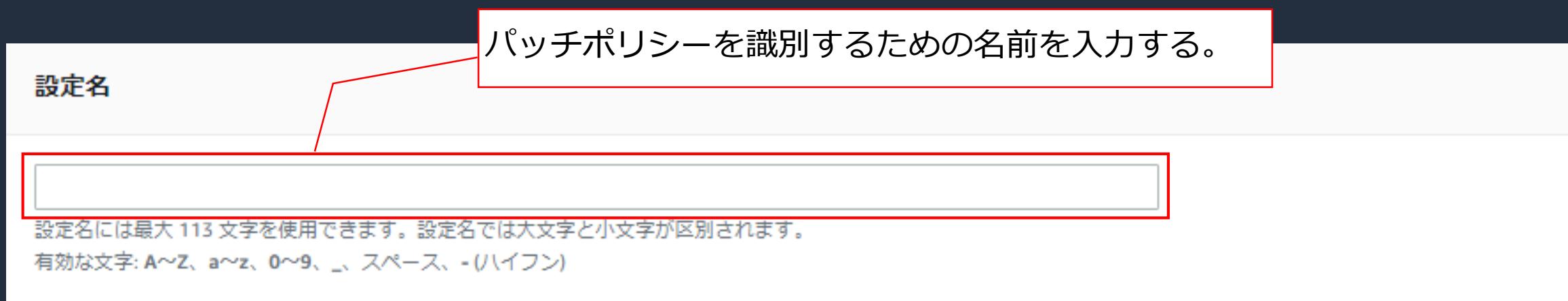
Patch Manager の概要

- Patch Manager は、オペレーティングシステムとアプリケーションのパッチ適用を自動化する事ができる
 - Windows Server では、Microsoft がリリースしたアプリケーションに限定
- Quick Setup を利用する事で、パッチポリシー（Amazon EC2 インスタンスやその他の管理ノードに、自動的にパッチを適用するスケジュールとベースラインを定義したもの）を作成可能
- カスタムパッチベースラインに変更を加えた場合、Quick Setup に同期されるまで 1 時間程度要する場合がある
- パッチコンプライアンス情報が予期せず更新される事を防止する為に、スキャンする方法は複数利用しない方が良い

Patch Manager の詳細については、別途公開予定の BlackBelt をご視聴ください。

https://aws.amazon.com/jp/events/aws-event-resource/archive/?cards.sort-by=item.additionalFields.SortDate&cards.sort-order=desc&awsf.tech-category=*all&cards.q=systems%2Bmanager&cards.q_operator=AND

Patch Manager の設定画面（設定名）



Patch Manager の設定画面（スキャンとインストール）

スキャンとインストール

「スキャン」だけか「スキャンとインストール」を行うかを選択する。

パッチオペレーション
ターゲットをスキャンし、インストールされているパッチをパッチベースライン内の承認済みパッチのリストと比較します。選択してスキャンするか、見つからないパッチをスキャンしてインストールします。

スキャン
 スキャンとインストール

スキャンのスケジュール

推奨される既定値を使用
パッチマネージャーは、毎日 1:00 AM UTC にノードをスキャンします。

カスタムスキャンスケジュール
カスタムのスキャンスケジュールを作成します。

「推奨される既定値を使用」する場合、
推奨の既定値である「毎日 1:00 AM UTC」にスキャンが行われる。

カスタムスキャンスケジュールを選択した場合は次頁を参照。

Patch Manager の設定画面（カスタムスキャンスケジュール）

スキャンとインストール

日次でスキャンする時刻を UTC で入力する。

スキャンの頻度
日単位
毎日 : UTC

スケジュールを CRON式として入力する。

スキャンの頻度
カスタム CRON 式
スケジュールを CRON 式として入力します。 詳細はこちら [\[リンク\]](#)
`cron(0 10 * * ? *)`
分 | 時 | 日 | 月 | 曜日 | 年の形式を使用します。

○ スキャンとインストール

スキャンのスケジュール
○ 推奨される既定値を使用
パッチマネージャーは、毎日 1:00 AM UTC にノードをスキャンします。

○ カスタムスキャンスケジュール
カスタムのスキャンスケジュールを作成します。

スキャンの頻度
頻度を選択
日単位
カスタム CRON 式

最初の CRON 間隔までターゲットのスキャンを待ちます。

チェックを入れない場合、ノードがターゲットになると直ちにスキャンを行う。



Patch Manager の設定画面（インストールスケジュール）

スキャンとインストール

パッチオペレーション
ターゲットをスキャンし、インストールされてい
ないパッチをスキャンしてインストールします。

スキャン
 スキャンとインストール

スキャンのスケジュール

推奨の既定値であれば「毎週日曜日 2:00
AM UTC」にインストールが行われる。

「スキャンとインストール」を選択すると「インス
トルスケジュール」を設定できるようになる。

「カスタムインストールスケジュール」
を選択した場合は「カスタムスキャニ
スケジュール」と同様に「日単位」と「カ
スタム CRON 式」を選択可能。

インストールスケジュール

推奨される既定値を使用
パッチマネージャーは、週に1回、日曜日の 2:00 AM UTC にパッチ
をインストールします。

カスタムインストールスケジュール
カスタムのインストールスケジュールを作成します。

インストールの頻度

頻度を選択 ▾

最初の CRON 間隔まで更新プログラムのインストールを待ちます。

必要に応じて再起動
パッチのインストール後 必要に応じてノードを再起動します。インストールのたびに再起動することを推奨します。

チェックを外した場合、ノードがターゲット
になると直ちにインストールを行う。

パッチインストール後の再起動を管理する。

Patch Manager の設定画面（パッチベースライン）

パッチベースライン

パッチベースラインには、承認されたパッチと拒否されたパッチのリストに加えて、リリースから数日以内にパッチを自動承認するルールが含まれます。 詳細は [こちら](#)

- 推奨される既定値を使用
AWS がサポートするオペレーティングシステムごとに定義されているデフォルトのパッチベースライン。
- カスタムパッチベースライン
カスタムパッチベースラインを選択します。カスタムパッチベースラインは、Quick Setup (ap-northeast-1) で指定されたホーム AWS リージョンに存在する必要があります、最大 3,336 バイトまでです。

定義済みのパッチベース
ラインを選択する場合。

独自に作成したパッチベースラインを利用する場合。

パッチベースラインには、承認されたルールが含まれます。 詳細は

こちら

推奨される既定値を使用
AWS がサポートするオペレーティングシステムごとに定義されているデフォルトのパッチベースライン。

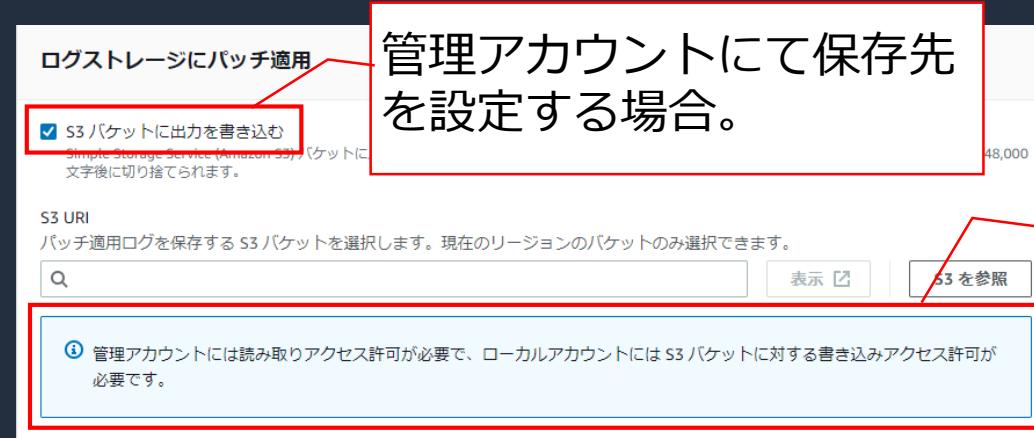
カスタムパッチベースライン
カスタムパッチベースラインを選択します。カスタムパッチベースラインは、Quick Setup (ap-northeast-1) で指定されたホーム AWS リージョンに存在する必要があります、最大 3,336 バイトまでです。

▼ ベースラインを表示または変更

オペレーティングシステム	ベースラインを選択	ベースライン ID
Amazon Linux	AWS-AmazonLinuxDefaultPatchBa...	pb-0221829c157d721d8
Amazon Linux 2	AWS-AmazonLinux2DefaultPatchB...	pb-00fd5699d1ae3942
Amazon Linux 2022	<input type="text"/>	pb-067dab85430494167
CentOS	AWS-AmazonLinux2DefaultPatchBaseline	pb-0b4917141375bc4b5
Debian Server	Default Patch Baseline for Amazon Linux 2 Provided by AWS.	pb-0d5f3f8560fc606e3
Oracle Linux		pb-04ed5d5c38572bb74
Raspberry Pi OS		pb-04e6dbcacf1dc4ef
Red Hat Enterprise Linux (RHEL)	Test-BlackBelt-Baseline	pb-0adff5cb7136a2984d
	Test-BlackBelt-Baseline	
	Test-BlackBelt-Baseline	

Patch Manager の設定画面（パッチログの保存先）

管理アカウントからの設定



管理アカウントにて保存先を設定する場合。

バケットは事前に作成する必要があります、組織で利用する場合はアクセス権の考慮が必要。

非管理アカウントからの設定



非管理アカウントにて保存先を設定する場合。

Patch Manager の設定画面（ターゲット）

管理アカウントからの設定

ターゲット

パッチポリシーをデプロイするノードを選択します。

このパッチポリシーをデプロイするアカウントとリージョンを選択します。

組織全体

Deploys your patch policy to all nodes in the OUs and Regions in your organization.

カスタム

このパッチポリシーをデプロイする OU とリージョンを選択します。

現在のアカウント

現在の AWS アカウントで、このパッチポリシーをデプロイするリージョンを選択します。

組織内のすべてのアカウントとリージョンを対象とする。

組織内のOUとリージョンを選択可能。
ノードの指定は、全てを対象とするかタグで選定する。

「現在のアカウント」を選択する場合、非管理アカウント（次頁）で設定する時と同様の選択が可能。

Patch Manager の設定画面（ターゲット）

非管理アカウントからの設定

ターゲット
パッチポリシーをデプロイするノードを選択します。

現在のリージョンまたはリージョンのカスタムセットのいずれにデプロイするかを選択します。

現在のリージョン
現在のリージョンに設定をデプロイします。

リージョン
他の設定をデプロイするリージョンを選択します。

ホームリージョンで「現在のリージョン」を選択した場合、ターゲットインスタンスの選択にリソースグループなどの4つから選択する事が可能。

インスタンスをどのようにターゲットにするかを選択

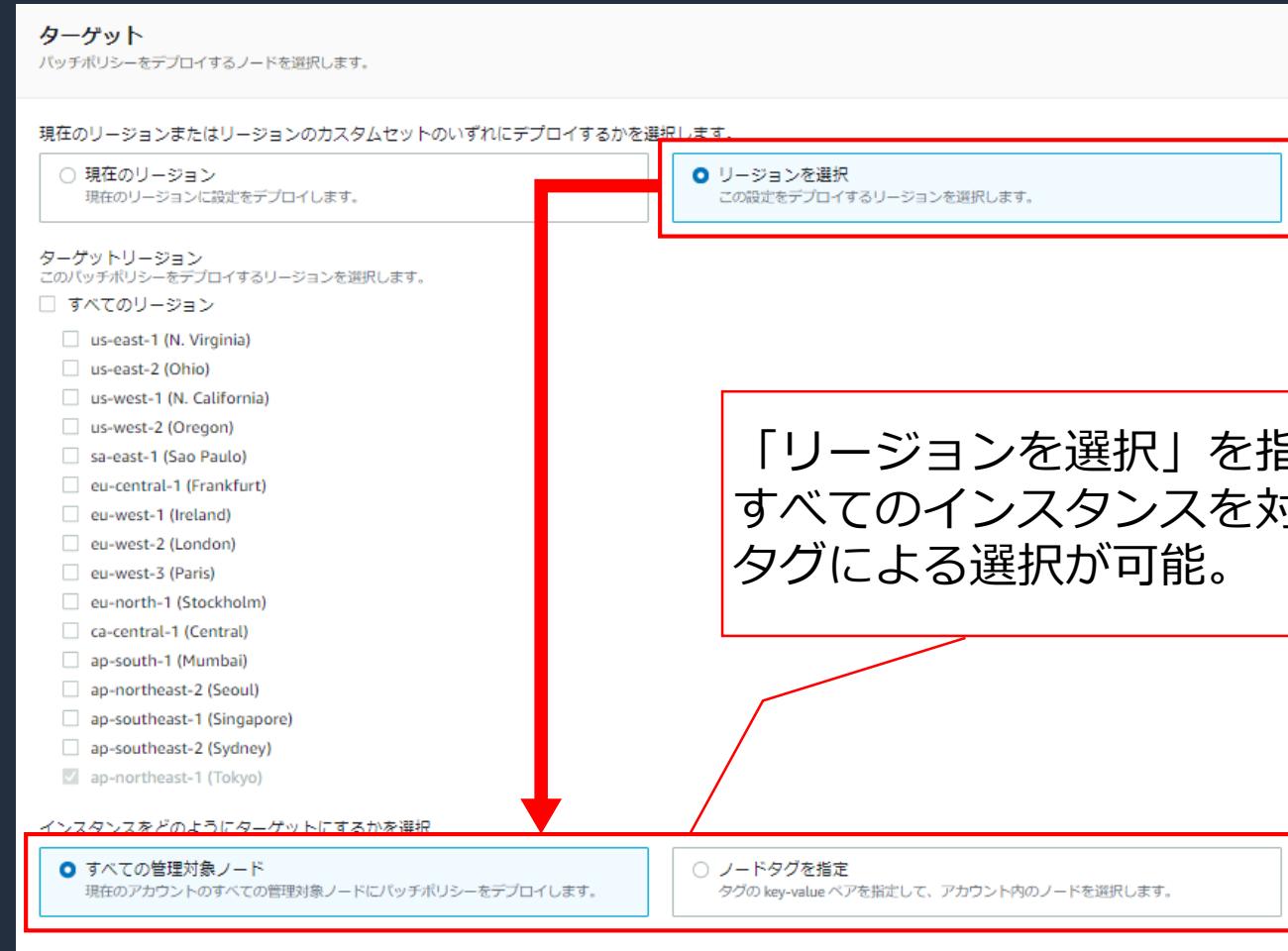
すべての管理対象ノード
現在のアカウントのすべての管理対象ノードにパッチポリシーをデプロイします。

ノードタグを指定
タグの key-value ペアを指定して、アカウント内のノードを選択します。

手動
設定するインスタンスを手動で指定します。

Patch Manager の設定画面（ターゲット）

非管理アカウントからの設定



「リージョンを選択」を指定した場合、
すべてのインスタンスを対象とするか、
タグによる選択が可能。

Patch Manager の設定画面（レートの制御）

レートの制御

パッチポリシーを実行する際の同時実行率とエラー率を指定します。

パッチポリシーを同時に実行するノードの数または割合を入力する。

同時実行数

パッチポリシーを同時に実行するノードの数または割合を指定します。

10

ノードの割合 ▼

ノードの割合は 1 から 100 の間でなければなりません。

エラーのしきい値

パッチポリシーが失敗する前にエラーを許可するノードの数または割合を指定します。

2

ノードの割合 ▼

ノードの割合は 0 から 100 の間でなければなりません。

エラーが発生したノードの数または割合がこの値を超えると、パッチポリシーはエラーとなる。

Patch Manager の設定画面（インスタンスプロファイル）

チェックを入れる事で、EC2 にアタッチされている既存の IAM ロール（インスタンスプロファイル）に対して、必要な権限（IAM ポリシー）がアタッチされる。

インスタンスプロファイルのオプション

- 必要な IAM ポリシーを、インスタンスにアタッチされている既存のインスタンスプロファイルに追加します。



このオプションを有効にすると、デフォルトの動作が変更されます

デフォルトでは、Quick Setup は、選択した設定に必要な許可を持つ IAM ポリシーとインスタンスプロファイルを作成します。その後、Quick Setup によって作成されたインスタンスプロファイルは、インスタンスプロファイルがアタッチされていないインスタンスにのみアタッチされます。このオプションを有効にすると、Quick Setup は、インスタンスプロファイルがアタッチされたインスタンスにも IAM ポリシーを追加します。

次のポリシーがアタッチされます。

- AmazonSSMManagedInstanceCore
- aws-quickssetup-patchpolicy-baselineoverrides-s3

3. 個別機能のご紹介

DevOps Guru

DevOps Guru の概要

- 機械学習を利用して運用データやアプリケーションのメトリクスやイベントを分析し、通常の運用パターンから逸脱した動作を特定することが出来る DevOps Guru を素早く設定する事が可能
- Quick Setup で有効化した DevOps Guru を無効化（課金を停止）するには、カバレッジ設定を更新してリソースを分析しないようにする
 - 停止した後も、過去のインサイトを確認した場合に少額の料金が発生する可能性がある

DevOps Guru については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/devops-guru/latest/userguide/welcome.html

カバレッジ設定の更新については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/devops-guru/latest/userguide/view-analyzed-resources.html

DevOps Guru の設定画面（設定オプション）

設定オプション

選択した設定オプションは、選択した組織単位とリージョンのすべての AWS アカウントを分析する。

分析するリソースを指定。

組織内のすべてのアカウントにあるすべての AWS リソースを分析

選択内容に基づいて、アクティブなリソースごとに、分析された AWS リソース時間数についての料金をお支払いいただきます。詳細については、[DevOps Guru の料金のページ](#)を参照してください。今すぐ選択しない場合でも、アカウントの各ユーザーは、[DevOps Guru の \[Settings\] \(設定\) のページ](#)に移動して適切な AWS CloudFormation スタックを選択することで、後でリソースを指定できます。

SNS 通知を有効化

選択内容に応じて、OU 内の各アカウントについて SNS トピックが作成されます。重要な DevOps Guru イベントについて通知します。個々のアカウントユーザーは、DevOps Guru の設定のページからこの設定を変更できます。

通知用に SNS トピックが作成される。

AWS Systems Manager OpsItems を有効化

OpsItem の作成を有効にすると、AWS Systems Manager の標準料金に基づいて追加料金が発生します。

OpsItems 有効化する事で、発見された問題について Systems Manager OpsCenter から追跡と管理を行うことができる。

OpsItems (OpsCenter) については、以下をご参照ください。

https://www.youtube.com/watch?v=XXG88mXS6_E

DevOps Guru の設定画面（スケジュール）

スケジュール

選択した設定オプションを Quick Setup が適用する頻度。Quick Setup は、以下で選択した頻度で、選択した設定をターゲットアカウントで再適用し、設定に加えられたアウトオブバンドの変更を元に戻します。

デフォルトのスケジュールを選択するか、独自のスケジュールを選択

- デフォルト
1回適用

- カスタム
指定した設定オプションを適用する頻度を選択

① 設定の頻度を指定することで、Quick Setup は、適用する設定に加えられた変更を修復できます。

他の設定タイプと同様に、定期的に設定差違の修正を試みることが出来る。

DevOps Guru の設定画面（ターゲット）

管理アカウントからの設定

ターゲット

ターゲットは、この設定のデプロイ場所を決定します。

この設定をデプロイするアカウントとリージョンを選択します。

カスタム

この設定をデプロイする OU とリージョンを選択します。

現在のアカウント

現在サインインしているアカウント内でこの設定をデプロイするリージョンを選択します。

非管理アカウントからの設定

ターゲット

ターゲットは、この設定のデプロイ場所を決定します。

現在のリージョンまたはリージョンのカスタムセットのいずれにデプロイするかを選択します。

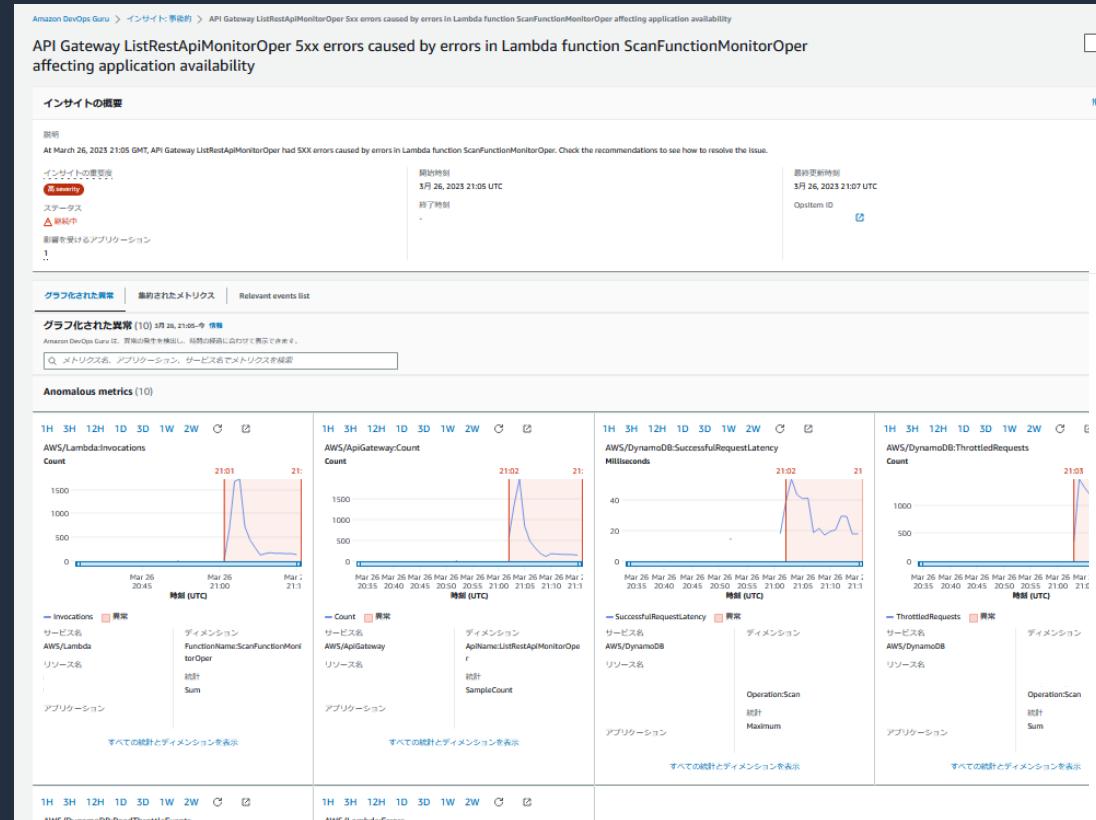
現在のリージョン

現在のリージョンに設定をデプロイします。

リージョンを選択

この設定をデプロイするリージョンを選択します。

運用データの分析と問題の特定



特定された問題をインサイトとして表示。

This section lists five recommendations from DevOps Guru:

- Resolve errors in Lambda ScanFunctionMonitorOper**: Investigate errors by checking Lambda function logs.
- Amazon DynamoDB のスロットリミッティングのトラブルシューティング**: Fix slot limit events.
- Amazon DynamoDB テーブルの高レイテンシーのトラブルシューティング**: Reduce request latency.
- AWS Lambda のエラーのトラブルシューティングおよび自動再試行の設定**: Troubleshoot Lambda errors.
- Amazon API Gateway の 5XX エラーのトラブルシューティング**: Troubleshoot 5XX errors.

インサイトに関する推奨事項。

3. 個別機能のご紹介

Change Manager

Change Manager の概要

- Change Manager（アプリケーションの設定やインフラストラクチャに対する運用上の変更を要求、承認、実装、報告するための変更管理フレームワーク）を AWS Organizations で設定された組織で使用する場合に利用する
- Quick Setup を利用する事で、Change Manager で利用する権限をマルチアカウント/マルチリージョンにデプロイ可能
- Quick Setup から設定可能な構成は最大で 15 個までなので、権限付与は計画的に行う必要がある

Change Manager については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/change-manager.html

Change Manager については、BlackBelt も別途公開予定となっております。

https://aws.amazon.com/jp/events/aws-event-resource/archive/?cards.sort-by=item.additionalFields.SortDate&cards.sort-order=desc&awsf.tech-category=*all&cards.q=systems%2Bmanager&cards.q_operator=AND

設定タイプの差違

非管理アカウントからの設定

The screenshot shows the 'Quick Setup' page of the AWS Systems Manager console. On the left, a sidebar lists various service categories like 'Host Management', 'Patch Manager', and 'Resource Scheduler'. The main area displays several configuration options with '作成' (Create) buttons:

- Host Management**: Systems Manager の使用 (選択済み).
説明: IAM ロールを設定し、Amazon EC2 インスタンスを安全に管理するために一般的に使用されている Systems Manager 機能を有効にします。
作成
- Config Recording**: AWS Config の使用 (選択済み).
説明: AWS Config が提供するコンフォーマンスパックをデプロイします。コンフォーマンスパックは、1つのエンティティとしてデプロイできる AWS Config ルールと修復アクションを集めたものです。
作成
- Conformance Packs**: AWS Config の使用 (選択済み).
説明: AWS Config が提供するコンフォーマンスパックをデプロイします。コンフォーマンスパックは、1つのエンティティとしてデプロイできる AWS Config ルールと修復アクションを集めたものです。
作成
- Patch Manager**: Systems Manager の使用 (選択済み).
説明: 1つのノードまたは組織全体で、アプリケーションとノードのパッチ適用を自動化します。
作成
- DevOps Guru**: DevOps Guru の使用 (選択済み).
説明: エージェントなどのソフトウェアパッケージを Amazon EC2 インスタンスに配布できるようにします。
作成
- Distributor**: Systems Manager の使用 (選択済み).
説明: フリートマネージャー、コンプライアンス、イベントリードアクティベーション、セッションマネージャー、Run Command、スタートマネージャー、パッチマネージャー、ディストリビューター。
作成
- Resource Scheduler**: AWS リソーススケジューラー (選択済み).
説明: 指定した時間にインスタンスが停止および開始するようにスケジュールします。
作成

管理アカウントからの設定

The screenshot shows the 'Quick Setup' page of the AWS Systems Manager console for managed accounts. The sidebar and overall layout are similar to the non-managed account view, but the 'Change Manager' section is highlighted with a red box:

Change Manager: Systems Manager の使用 (選択済み).
説明: 1つのノードまたは組織全体で、アプリケーションとノードのパッチ適用を自動化します。
作成

A red box highlights the 'Change Manager' section, which is only visible when setting up from a managed account. Other sections like 'Distributor' and 'Resource Scheduler' are also visible.

管理アカウントで設定タイプ
を表示した時だけ Change
Manager が表示される

Change Manager の設定画面（委任された管理者アカウント）

委任された管理者アカウント

委任されたアカウントは、組織内の複数のアカウントを表示し、これらのアカウントに対する変更を開始できます。

委任された管理者として登録する AWS Organization メンバーアカウントのアカウント ID を入力します。

123456789321

Change Manager を含む Systems Manager 全体の運用アクティビティを管理するための AWS アカウントを指定する。

Change Manager の設定画面 (リクエストと変更を行うための許可)

リクエストと変更を行うための許可

デプロイする Change Manager の各 Quick Setup 設定は、選択した組織単位で、Change Manager テンプレートとオートメーションランプックを実行するための許可を持つ、委任された管理者アカウントでジョブ機能を作成します。最大 15 個の Change Manager の Quick Setup 設定を作成できます。 [詳細については](#)

ロールとその権限を識別するための名前を入力する。

ジョブ機能
許可が適用される組織内のロールを識別する名前を入力します。ジョブ機能名は最大 10 文字です。

ロールと許可のオプション

カスタム許可
ランプックへのアクセス権を付与するための許可をカスタマイズして、テンプレートを変更します。

管理者許可
すべての AWS のサービスに対する完全な管理アクセス権を付与します。

許可ポリシーエディタ
JSON を使用して、作成するジョブ機能用の Identity and Access Management (IAM) 許可を指定します。 IAM Visual エディタを使用してポリシーを作成し、Access Analyzer を使用してテストしてから、ここに貼り付けることができます。

```
1 [{}]
2   "Version": "2012-10-17",
3     "Statement": [
4       {
5         "Effect": "Allow",
6         "Action": "*",
7         "Resource": "*"
8       }
9     ]
10 ]
```

検証

委任管理者アカウントから Change Manager で変更管理タスクを実行するための権限。

Change Manager の設定画面（ターゲット）

ターゲット

ターゲットは、この設定のデプロイ場所を決定します。

この設定をデプロイするアカウントとリージョンを選択します。

組織全体

組織内のすべての OU とリージョンに設定をデプロイします。

カスタム

この設定をデプロイする OU とリージョンを選択します。

組織内のすべてのアカウントと
リージョンを対象とする。

1 つまたは複数の OU を選択する。
(リージョンは選択できない)

3. 個別機能のご紹介

Distributor

Distributor の概要

- Distributor パッケージを AWS アカウントと AWS リージョン、または AWS Organizations の組織全体にデプロイできる
- 現在デプロイ可能なパッケージ（2023/11 時点）
 - Amazon Elastic File System (Amazon EFS) ユーティリティパッケージ
 - Amazon CloudWatch エージェント
 - EC2Launch v2 エージェント

Distributorについては、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/distributor.html

<https://www.youtube.com/watch?v=wjyzvKRT9zw>

Amazon Elastic File System tools (amazon-efs-utils パッケージ)については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/efs/latest/ug/using-amazon-efs-utils.html

Distributor の設定画面（パッケージの選択と更新頻度）

設定オプション

ソフトウェアパッケージ
EC2 インスタンスにデプロイするパッケージを選択します。

パッケージを選択

- Amazon Elastic File System tools
Amazon Elastic File System (EFS) のユーティリティ
- Amazon CloudWatch agent
メトリクスとログを CloudWatch に報告するエージェント
- Amazon EC2Launch v2 agent
AWS が推奨する設定を Windows インスタンスに適用するエージェント

更新頻度 i

- 30 日ごと
- 2 日ごと
- 14 日ごと
- 30 日ごと
- 無効

デプロイするパッケージを選択する。

更新頻度を指定する。

Distributor の設定画面（ターゲット）

管理アカウントからの設定

ターゲット

ターゲットは、この設定のデプロイ場所を決定します。

この設定をデプロイするアカウントとリージョンを選択します。

組織全体

組織内のすべての OU とリージョンに設定をデプロイします。

カスタム

この設定をデプロイする OU とリージョンを選択します。

現在のアカウント

現在サインインしているアカウント内でこの設定をデプロイするリージョンを選択します。

組織内のすべてのアカウントとリージョンを対象とする。

組織内の OU とリージョンを選択可能。
タグなどによるノードの指定は不可。

「現在のアカウント」を選択する場合、非管理アカウントで設定する時と同様の選択が可能。

Distributor の設定画面（ターゲット）

非管理アカウントからの設定

ターゲット
ターゲットは、この設定のデプロイ場所を決定します。

現在のリージョンまたはリージョンのカスタムセットのいずれにデプロイするかを選択します。

現在のリージョン
現在のリージョンに設定をデプロイします。

リージョンを選択
この設定をデプロイするリージョンを選択します。

インスタンスをどのようにターゲットにするかを選択

すべてのインスタンス
ターゲットアカウントとリージョンのすべてのインスタンスに設定をデプロイします。

タグ
ターゲットにするタグの key-value ペア。タグを指定すると、そのタグの付いたすべてのインスタンスが選択されます。

リソースグループ
リソースグループを指定します。そのグループ内のインスタンスのみが設定されます。

手動
設定するインスタンスを手動で指定します。

「リージョンを選択」した場合、ターゲットインスタンスの選択は「すべてのインスタンス」か「タグ」のみとなる。

「現在のリージョン」を選択した場合、ターゲットインスタンスの選択はリソースグループなどの 4 つから選択する事が可能。

Distributor の設定画面（インスタンスプロファイル）

チェックを入れる事で、EC2 にアタッチされている既存の IAM ロール（インスタンスプロファイル）に対して、必要な権限（IAM ポリシー）がアタッチされる。

インスタンスプロファイルのオプション

- 必要な IAM ポリシーを、インスタンスにアタッチされている既存のインスタンスプロファイルに追加します。



このオプションを有効にすると、デフォルトの動作が変更されます

デフォルトでは、Quick Setup は、選択した設定に必要な許可を持つ IAM ポリシーとインスタンスプロファイルを作成します。その後、Quick Setup によって作成されたインスタンスプロファイルは、インスタンスプロファイルがアタッチされていないインスタンスにのみアタッチされます。このオプションを有効にすると、Quick Setup は、インスタンスプロファイルがアタッチされたインスタンスにも IAM ポリシーを追加します。

次のポリシーがアタッチされます。

- AmazonSSMManagedInstanceCore

3. 個別機能のご紹介

Resource Scheduler

Resource Scheduler の概要

- スケジュールに基づいて、Amazon EC2 インスタンスの起動と停止を自動化する事が可能
- 不必要な EC2 インスタンスを停止させる事で、コストの削減が期待できる
- 設定で指定した値に一致するタグを持つ EC2 インスタンスだけが対象となる
- 各設定は、リージョン毎に 5000 インスタンスまでサポート
- 5000 を超える場合は、タグキー値を分けて設定を分割する
- Instance Scheduler との比較は、P.82 を参照

Instance Scheduler については、以下をご参照ください。

<https://aws.amazon.com/jp/solutions/implementations/instance-scheduler-on-aws/>

<https://aws.amazon.com/jp/builders-flash/202110/instance-scheduler/>

Resource Scheduler の設定画面（インスタンスタグ）

インスタンスタグ

ターゲットにするタグのキーと値のペアを指定します。タグが適用された最大 5,000 個のインスタンスがターゲットとなります。

キーを入力

値を入力

スケジュールと関連付けるインスタンスに適用するタグキー値を指定する。

Resource Scheduler の設定画面（スケジュールオプション）

スケジュールオプション

タイムゾーンをスケジュール
スケジュールに使用したいタイムゾーンを選択します。選択するタイムゾーンは、タイムゾーンが異なるリージョンでインスタンスを開始および停止するタイミングに影響します。

(GMT +09:00) Asia/Tokyo

スケジュールの曜日
Resource Scheduler でインスタンスを開始および停止させる曜日を選択します。

スケジュールの曜日を選択

月曜日 X 火曜日 X 水曜日 X
木曜日 X 金曜日 X

指定したタイムゾーンに基づいて、インスタンスを起動 / 停止する「曜日」と「時刻」を設定する。

インスタンスの開始時刻と停止時刻
インスタンスを開始および停止する時刻を指定します。午前と午後を区別するには、24 時間形式を使用してください。

インスタンスの開始時刻:
09:00:00

インスタンスの停止時刻:
17:00:00

The screenshot displays the 'Schedule Options' configuration screen for AWS Resource Scheduler. It includes three main sections highlighted by red boxes: 1) 'Time Zone Selection' (Time Zone dropdown set to '(GMT +09:00) Asia/Tokyo'), 2) 'Day Selection' (Days dropdown set to 'Schedule days: Monday, Tuesday, Wednesday, Thursday, Friday'), and 3) 'Time Range Selection' (Start Time dropdown set to '09:00:00' and Stop Time dropdown set to '17:00:00'). A large red bracket on the right side points to a descriptive text block stating: '指定したタイムゾーンに基づいて、インスタンスを起動 / 停止する「曜日」と「時刻」を設定する。' (Configure the days and times to start and stop instances based on the specified time zone.)

Resource Scheduler の設定画面（ターゲット）

管理アカウントからの設定

デプロイする OU とリージョンの指定が可能。

「現在のアカウント」を選択した場合、非管理アカウントでのターゲット設定と同様にリージョンの選択が可能

ターゲット
ターゲットは、この設定のデプロイ場所を決定します。

この設定をデプロイするアカウントとリージョンを選択します。

カスタム
この設定をデプロイする OU とリージョンを選択します。

現在のアカウント
現在サインインしているアカウント内でこの設定をデプロイするリージョンを選択します。

非管理アカウントからの設定

ターゲット
ターゲットは、この設定のデプロイ場所を決定します。

現在のリージョンまたはリージョンのカスタムセットのいずれにデプロイするかを選択します。

現在のリージョン
現在のリージョンに設定をデプロイします。

リージョンを選択
この設定をデプロイするリージョンを選択します。

Instance Scheduler との比較

項目	Instance Scheduler	Resource Scheduler
対象	EC2・RDS・Aurora	EC2
機能	タグの自動付与や起動/停止時のコントロールなど多機能	起動/停止のみ
スケジューリング	DynamoDB のコンソールか Scheduler CLI	Quick Setup のコンソール
実行タイミング	Lambda に設定した実行間隔による	Change Calendar の State 遷移を EventBridge にてルール設定
コスト	スケジュールされるインスタンス数による (下記ガイドの試算例では 4.10 USD/月)	ほぼ無料
用途	インスタンスの起動/停止を、きめ細かくコントロールしたい場合	EC2 インスタンスをスケジュールに基づいてシンプルに起動/停止させたい場合

Change Calendar については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-change-calendar.html

※ BlackBelt も別途公開予定となっております

EventBridge については、以下をご参照ください。

<https://www.youtube.com/watch?v=H7641kZMghg>

3. 個別機能のご紹介

OpsCenter

OpsCenter の概要

- アカウント全体で OpsItems を管理するように OpsCenter を構成する
- Systems Manager の委任管理者をセットアップし、メンバーアカウントで OpsItems を作成、編集、表示できる様にする
- 複数のアカウント間で OpsItems を管理するために必要な IAM ポリシーとロールを作成する

OpsCenter については、以下をご参照ください。

https://www.youtube.com/watch?v=XXG88mXS6_E

設定タイプの差違

非管理アカウントからの設定

The screenshot shows the 'Quick Setup' page of AWS Systems Manager. On the left, a sidebar lists various service categories like '運用管理', 'アプリケーション管理', and 'ノード管理'. The main area displays a grid of service cards:

- Host Management**: Systems Manager の使用 (選択済み) / IAM ロールを設定し、Amazon EC2 インスタンスを安全に管理するため一般的に使用されている Systems Manager 機能を有効にします。
- Config Recording**: AWS Config の使用 (選択済み) / 調査した AWS リソースタイプへの変更を追跡し記録できるようにします。記録されたデータの履歴オプションと通知オプションを設定します。
- Conformance Packs**: AWS Config の使用 (選択済み) / AWS Config が提供するコンフォーマンスパックをデプロイします。コンフォーマンスパックは、1つのエンティティとしてデプロイできる AWS Config ルールと修復アクションを集めたものです。
- Patch Manager**: Systems Manager の使用 (選択済み) / IAM ロールを設定し、Amazon EC2 インスタンスを安全に管理するため一般的に使用されている Systems Manager 機能を有効にします。
- DevOps Guru**: DevOps Guru の使用 (選択済み) / 1つのノードまたは組織全体で、アプリケーションとノードのパッチ適用を自動化します。
- Distributor**: Systems Manager の使用 (選択済み) / エージェントなどのソフトウェアパッケージを Amazon EC2 インスタンスに配布できるようにします。
- Resource Scheduler**: AWS フリューショーンを利用 (選択済み) / 設定した時間にインスタンスが停止および開始するようスケジュールします。

各カードには「作成」ボタンがあります。

管理アカウントからの設定

The screenshot shows the 'Quick Setup' page of AWS Systems Manager for a managing account. The sidebar and service cards are identical to the non-managing account setup. A red box highlights the **OpsCenter** card in the bottom right corner:

OpsCenter
Powered by Systems Manager
選択済み
Enables OpsCenter to centrally manage operational issues (Operations) across multiple AWS accounts.

A red arrow points from the text '管理アカウントで設定タイプを表示した時だけ OpsCenter が表示される' to this card.

OpsCenter の設定画面（委任された管理者アカウント）

Delegated administrator account

Choose a delegated administrator account which will be granted permissions to manage OpsItems across multiple AWS accounts.

委任された管理者として登録する AWS Organization メンバーアカウントのアカウント ID を入力します。

組織内の他のアカウントを管理する権限を付与されたアカウントを指定する。

OpsCenter の設定画面 (ターゲット)

Targets

Choose the accounts that the delegated administrator can manage.

Entire organization
All accounts in your AWS organization

Custom
A subset of organizational units (OUs)

組織内のすべてのアカウントを対象とする。

対象とする OU を選択する。

3. 個別機能のご紹介

Resource Explorer

Resource Explorer の概要

- AWS Resource Explorer はリソースの検索・発見サービスで、名前・タグ・ID などからリソースを検索する事ができる
- 検出されたリソースに関する情報がインデックスに入力される事で、リソースの検索が可能となる
- インデックスの情報は、ビューを通して表示させる事ができる
- アグリゲーターインデックスは Resource Explorer が有効になっている他のリージョンからインデックスをレプリケーションする
- Quick setup では、アグリゲータインデックスと、アカウントが使用するすべての AWS リージョンのすべてのリソースを含むフィルタを持つデフォルトビューを作成する

Resource Explorer については、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/resource-explorer/latest/userguide/welcome.html



設定タイプの差違

非管理アカウントからの設定

The screenshot shows the 'Quick Setup' page of AWS Systems Manager. On the left, a sidebar lists various services: '運用管理' (AWS Config, CloudWatch Metrics, OpsCenter), 'アプリケーション管理' (AWS Lambda, AppSync, AppSync API, AppSync GraphQL API, AppSync GraphQL API), '変更管理' (Change Manager, Change Calendar, Change Window), 'ノード管理' (Patch Manager, DevOps Guru, Distributor), 'Resource Scheduler', and '共有リソース' (CloudWatch Metrics). The main area displays six configuration types:

- Host Management**: Systems Manager の使用 (選択済み)。説明: IAM ロールを設定し、Amazon EC2 インスタンスを安全に管理するために一時的に使用されている Systems Manager 機能を有効にします。
- Config Recording**: AWS Config の使用 (選択済み)。説明: AWS Config が提供するコンフォーマンスパックをデプロイします。選択されたデータの履歴オプションと通知オプションを設定します。
- Conformance Packs**: AWS Config の使用 (選択済み)。説明: AWS Config が選択した AWS リソースタイプへの変更を追跡し記録できるようにします。選択されたデータの履歴オプションと通知オプションを設定します。
- Patch Manager**: Systems Manager の使用 (選択済み)。説明: 1 つのノードまたは組織全体で、アプリケーションとノードのパッチ適用を自動化します。
- DevOps Guru**: DevOps Guru の使用 (選択済み)。説明: エージェントなどのソフトウェアパッケージを Amazon EC2 インスタンスに配布できるようにします。
- Resource Scheduler**: AWS リソリューションを利用 (選択済み)。説明: 指定した時間にインスタンスが停止および開始するようスケジュールします。

Bottom navigation: CloudShell, フィードバック.

管理アカウントからの設定

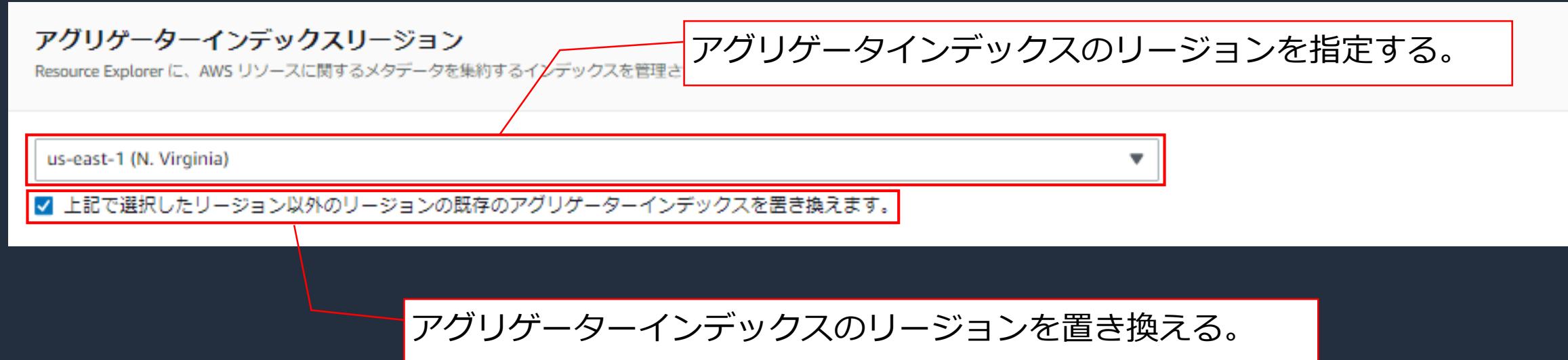
The screenshot shows the 'Quick Setup' page of AWS Systems Manager for managed accounts. The sidebar and configuration types are identical to the non-managed account view. A red box highlights the 'Resource Explorer' configuration type, which is only visible in the managed account view.

Resource Explorer: AWS Resource Explorer を利用 (選択済み)。説明: 組織内のすべてのアカウントとリージョンのデフォルトホスト構成を有効にします。

Bottom navigation: CloudShell, フィードバック.

管理アカウントで設定タイプを表示した
時だけ Resource Explorer が表示される

Resource Explorer の設定画面 (アグリゲーターインデックスリージョン)



Resource Explorer の設定画面（ターゲット）

ターゲット

検出を有効にするリソースを含むアカウントとリージョンを選択します。

組織全体

Organization 内のすべての組織単位のすべてのアカウントを含めます。

特定の組織単位

Organization に含める組織単位 (OU) を選択します。

組織内のすべてのアカウントを対象とする。

対象とする OU を選択する。

3. 個別機能のご紹介

補足

組織に AWS アカウントを追加/除外した際の挙動について

AWS アカウントを追加した場合

- 当該 AWS アカウントに、Quick Setup の設定がデプロイされる

AWS アカウントを除外した場合

- 当該 AWS アカウントの、Quick Setup の設定が削除される



使用されるスタックセットに自動デプロイの設定が施されている

- 自動デプロイ : 有効
- アカウント削除時にスタックを保持 : スタックを削除

スタックセットの自動デプロイについては、以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/AWSCloudFormation/latest/UserGuide/stacksets-orgs-manage-auto-deployment.html

組織に AWS アカウントを追加/除外した際の挙動について

既に Quick Setup を設定している AWS アカウントを追加した場合

- 管理アカウントから設定がデプロイされるため、重複して設定が行われる

Quick Setup

ライブラリ 設定

ファイル条件 フィルター条件

▼ 設定タイプ

- Conformance Packs (1)
- Config Recording (3)
- DevOps Guru (3)
- Distributor (3)
- Patch Manager (3)
- Host Management (3)
- Resource Scheduler (3)
- Change Manager (1)

▼ デプロイタイプ

- Local (7)
- Organizational (13)

設定

リージョンまたはデプロイステータスで検索

設定タイプ	デプロイタイプ	リージョン	デプロイのステータス	関連付けのステータス
Change Manager	組織	該当なし (グローバル)	SUCCEEDED	なし
Config Recording	ローカル	us-east-2	SUCCEEDED	2 Success
Config Recording	組織	us-east-2	SUCCEEDED	-
Config Recording	組織	us-west-2	SUCCEEDED	-
Conformance Packs	ローカル	us-east-2	SUCCEEDED	1 Success
DevOps Guru	ローカル	us-east-2	SUCCEEDED	1 Failed 1 Success
DevOps Guru	組織	us-east-2	SUCCEEDED	-
DevOps Guru	組織	us-west-2	SUCCEEDED	-
Distributor	ローカル	us-east-2	SUCCEEDED	5 Success
Distributor	組織	us-east-2	SUCCEEDED	-

注意事項

- 管理アカウント（組織）と非管理アカウント（ローカル）から重複して設定するケースも含めて、影響範囲の確認や事前の検証を入念に行う事を推奨

Quick Setup の利用可能リージョン

- 米国東部 (オハイオ)
- 米国東部(バージニア北部)
- 米国西部(北カリフォルニア)
- 米国西部 (オレゴン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- カナダ(中部)
- 欧州(フランクフルト)
- 欧州 (ストックホルム)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 南米 (サンパウロ)

Quick Setup から設定されるサービスや機能が利用可能なリージョンは、上記リージョンと一致いたしません。

各設定タイプが利用可能なリージョンにつきましては、個別のガイドをご確認願います。

Quick Setup が利用可能なリージョン：

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-quick-setup.html

Quick Setup の利用に関する注意点

- ・セットアップされるサービスや機能が多岐に渡るため、対象のサービスや機能についてある程度の知識と経験が必要
 - Quick Setup で設定する AWS サービスに馴染みがない場合は、それらのサービスについて事前に詳細をご確認頂く事を推奨
- ・Quick Setup の設定タイプから設定を削除しても、State Manager の関連付け（Association）から施された設定やリソースは削除されない
- ・ターゲットの AWS アカウントとリージョンを掛けた（乗じた）数が 10,000 を超えるとデプロイに失敗する
- ・設定タイプは管理アカウントにデプロイされない（ターゲットに組織全体を指定したとしても、管理アカウントは含まれない）

4. まとめ

まとめ

- 運用に役立つ機能を、マルチアカウント/マルチリージョンにセットアップする場合にとても便利です
- セットアップされる機能は推奨されるベストプラクティスに基づいて設定されるため、これから AWS をご利用になる運用担当者の方にもお勧めです
- 設定を削除しても作成されたリソースは削除されない点や、有効化された設定が無効化されない点などの注意事項についてはご留意ください

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

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
- ・ 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>



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

内容についての注意点

- ・ 本資料では資料作成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。AWS のサービスは常にアップデートを続けているため、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
- ・ 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
- ・ 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)



Thank you!



AWS Systems Manager

State Manager 編

AWS Black Belt Online Seminar

小野 卓人

Solutions Architect
2023/06

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6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：小野 卓人 (Takuto Ono)

所属：技術統括本部 金融ソリューション本部
保険ソリューション部

経歴：

SIer で金融機関向けシステムの受託開発
インフラ設計・構築・運用保守

現在は、ソリューションアーキテクトとして主に保険業界のお客様を担当

好きなAWSサービス： AWS Systems Manager



本セミナーの対象者

AWS の運用をされている方、これから運用される予定の方

本セミナーの目的

- AWS Systems Manager State Manager の機能とユースケースをご理解いただく。

本日お話ししないこと

- AWS Systems Manager の全体的な説明
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager State Manager 以外の機能の詳細
→ 各機能にフォーカスしたセッションを参照ください（今後も続々と公開予定です！）

アジェンダ

1. State Manager の概要
2. State Manager の主要な構成要素
3. 関連付けの作成
4. 関連付けの実行結果
5. TIPS
6. まとめ

AWS Systems Manager State Manager の概要

AWS Systems Manager

ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション



AWS Config

Configuration history



Amazon EventBridge

Notification and remediation



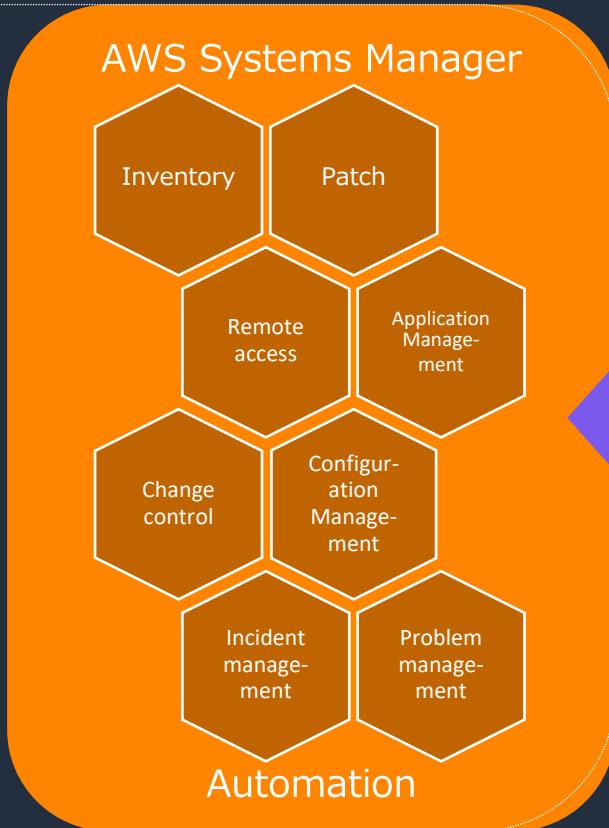
AWS CloudTrail

Audited actions



AWS Identity and Access Management (IAM)

Role-based access control



Cloud



On-premises



Edge

Integration
connectors
and APIs

- Third-party tools
- ITSM
- Custom solutions

AWS の他のサービスや
3rd Party のツールと統合された
管理ソリューションを提供

(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

運用管理

-  Explorer
-  OpsCenter
-  Incident Manager

アプリケーション管理

-  Application Manager
-  AppConfig
-  Parameter Store

変更管理

-  Change Manager
-  Automation
-  Maintenance Windows
-  Change Calendar

ノード管理

-  Fleet Manager
-  Session Manager
-  Inventory
-  Run Command
-  Patch Manager
-  Distributor
- State Manager

Quick Setup

AWS Systems Manager の機能

運用管理

-  Explorer
-  OpsCenter
-  Incident Manager

アプリケーション管理

-  Application Manager
-  AppConfig
-  Parameter Store

変更管理

-  Change Manager
-  Automation
-  Maintenance Windows
-  Change Calendar

ノード管理

-  Fleet Manager
-  Session Manager
-  Inventory
-  Run Command
-  Patch Manager
-  Distributor
- State Manager

Quick Setup

AWS Systems Manager State Manager とは



安全でスケーラブルな設定管理サービス

- マネージドノードやその他の AWS リソースを“定義された状態”に保つためのプロセスを自動化
- “定義された状態”への準拠状況をダッシュボードで可視化
- AWS リソースの管理とガバナンスを改善し、設定のズレを軽減するのに役立つ
- State Manager は追加料金なしでご利用可能

The screenshot shows the AWS Systems Manager State Manager console interface. The top section, titled 'Connections', displays a table of recent connections with columns for Connection ID, Name, Document Name, Last Run Date, Status, and Version. Most entries are successful (green), except for one entry which failed (red). The bottom section, titled 'Compliance Dashboard', includes a filtering section for compliance types (Association, Patch) and a summary table showing the count of rules for each type.

関連 ID	関連付けの名前	ドキュメント名	最終実行日	ステータス	関連付けのバージョン	リソースのステータス数
b288296a-52d1-46f0-b698-3d09f6d04d57	AWS-QuickSetup-SSMHostMgmt-UpdateCloudWatchAgent-tb53k	UpdateCloudWatchDocument-tb53k	Wed, 17 May 2023 15:01:39 GMT	成功	1	Success:1
ba084271-08de-4502-999b-6821bcccc490	AWS-QuickSetup-SSMHostMgmt-AttachIAMToInstance-tb53k	AWS-QuickSetup-CreateAndAttachIAMToInstance-tb53k	Tue, 25 Apr 2023 05:20:14 GMT	成功	1	Success:15
e8c0e024-6509-4b7e-81ce-dff0400f5dd	AWS-QuickSetup-SSMHostMgmt-UpdateSSMAgent-tb53k	AWS-UpdateSSMAgent	Tue, 23 May 2023 05:19:06 GMT	成功	1	Success:1
eb57b0c6-8519-4630-a05d-3a1142cd8883	AWS-QuickSetup-PatchPolicy-ScanForPatches-LA-tg57x	AWS-RunPatchBaseline	Wed, 24 May 2023 08:10:54 GMT	失敗	1	Failed:4
ff10e458-9f16-4729-b943-3ba9369a794		AWS-GatherSoftwareInventory	Wed, 01 Feb 2023 06:25:45	保留中	2	

コンプライアンスダッシュボードのフィルタリング

コンプライアンスルールの概要

コンプライアンスタイプ	準拠ルール	非準拠ルール	重要なルール	高ルール	中ルール	低ルール	情報ルール
Association	12	0	0	0	0	0	0
Patch	461	0	0	0	0	0	0

State Manager のユースケース例

マネージドノード上での OS コマンド実行

- ・ アンチウイルスソフトウェアのインストールと設定
- ・ SSM Agent などのエージェントソフトウェアを定期的にアップデート
- ・ ネットワーク設定
- ・ Microsoft Active Directory ドメインへのノード参加

AWS リソースの制御

- ・ EC2 インスタンスにロールをアタッチする
- ・ セキュリティグループに Ingress ルールと Egress ルールを適用する
- ・ AMI へのパッチ適用

リソースを **定義された状態** に維持する

Maintenance Windows との使い分け



State Manager

- SSM ドキュメントを定期実行し、「定義された状態」を維持するプロセスを自動化
- 「定義された状態」への準拠状況をレポート
- マネージドノードのブートストラップ (Auto Scaling シナリオにも有効)

リソースを定義された状態に維持する



Maintenance Windows

- 開始時刻と終了時刻を持つ「タイムウインドウ」内で複数のタスクを実行
- パッチ適用など、ノードの停止を伴うような変更をスケジュール実行
- SSM ドキュメント以外にも Lambda 関数と Step Functions の実行をサポート

時間的制約のあるタスクを
タイムウインドウ内に実行する



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/state-manager-vs-maintenance-windows.html

State Manager の 主要な構成要素

State Manager の主要な構成要素



State Manager Association (関連付け)

SSM ドキュメント



“定義された状態”を維持するためのアクションを定義したもの

スケジュール

アクションの実行タイミングに関する設定

ターゲット



“定義された状態”を維持する対象リソース



実行結果の可視化
(AWS Systems Manager Compliance)

※その他の設定項目については後述します

State Manager の主要な構成要素



State Manager Association (関連付け)

SSM ドキュメント



“定義された状態”を維持するためのアクションを定義したもの

スケジュール

アクションの実行タイミングに関する設定

ターゲット



“定義された状態”を維持する対象リソース

※その他の設定項目については後述します



実行結果の可視化
(AWS Systems Manager Compliance)



Systems Manager ドキュメントとは

- 実行するアクションを定義したもの
 - 一般的なタスクを自動化し、ヒューマンエラーを減らす
- 100以上の事前設定済みのドキュメント
 - カスタムドキュメントの作成も可能
- JSON or YAML 形式
- バージョニング、タグをサポート

The screenshot shows the AWS Systems Manager Documents interface. On the left, there's a sidebar with categories: Automation documents (12 categories), Command documents (9 categories), Policy documents (No categories for this document type), and Session documents (No categories for this document type). The main area displays two documents: 'AWS-ASGEnterStandby' and 'AWS-ASGExitStandby'. Both documents are of type Automation, owned by Amazon, and support Windows, Linux, and MacOS. They are the default version. At the top, there are tabs for 'Owned by Amazon', 'Owned by me', 'Shared with me', and 'All documents'. There are also buttons for 'Create document', 'Preferences', and 'Actions'.



ドキュメントについて詳細は[こちら](#)

```
{  
  "schemaVersion": "2.2",  
  "description": "Cross-platform demo document",  
  "mainSteps": [  
    {  
      "action": "aws:runPowerShellScript",  
      "precondition": {  
        "StringEquals": ["platformType", "Windows"]  
      },  
      "name": "WindowsOpenPorts",  
      "inputs": {  
        "runCommand": ["netstat -a"]  
      }  
    },  
    {  
      "action": "aws:runShellScript",  
      "precondition": {  
        "StringEquals": ["platformType", "Linux"]  
      },  
      "name": "LinuxOpenPorts",  
      "inputs": {  
        "runCommand": ["netstat -lntu"]  
      }  
    }  
  ]  
}
```

State Manager がサポートするドキュメントタイプ

以下の 3 つのドキュメントタイプをサポート

Type	Usage with	主な用途
Automation (Runbook)	✓ Automation	<ul style="list-style-type: none">AWS リソースのメンテナンス、デプロイ、修復に関する一般的なタスクを簡素化するためのワークフローを定義
Command	✓ Run Command	<ul style="list-style-type: none">マネージドノード上で実行するコマンドを定義
Policy	✓ Inventory	<ul style="list-style-type: none">AWS-GatherSoftwareInventory ポリシードキュメントと State Manager の関連付けを使って、マネージドノードからインベントリデータを収集

Automation、Run Command、Inventory の各機能については、公式ドキュメントまたは今後公開予定の Black Belt オンラインセミナーのセッションを参照ください。



State Manager の主要な構成要素



State Manager Association (関連付け)

SSM ドキュメント



“定義された状態”を維持するためのアクションを定義したもの

スケジュール

アクションの実行タイミングに関する設定

ターゲット



“定義された状態”を維持する対象リソース



※その他の設定項目については後述します



実行結果の可視化
(AWS Systems Manager Compliance)

ターゲットの指定方法

Command または Policy ドキュメントの場合



対象は マネージドノード

- タグ指定
- ノードを手動で選択
- リソースグループ指定
- すべてのマネージドノード

Automation Runbook の場合



対象は主に AWS リソース

- シンプルな実行
 - Runbook を単体で実行
- レートの制御
 - 複数のターゲットに対して Runbook を実行

ターゲットの指定方法

Command または Policy ドキュメントの場合



対象は マネージドノード

- タグ指定
- ノードを手動で選択
- リソースグループ指定
- すべてのマネージドノード

ターゲットの選択

ターゲットの選択
ターゲットを選択する方法を選択します。

インスタンスタグを指定
タグのキーと値のペアを 1 つ以上指定して、それらのタグを共有するインスタンスを選択します。

インスタンスを手動で選択
ターゲットとして登録するインスタンスを手動で選択します。

リソースグループを選択
ターゲットとするリソースを含むリソースグループを選択します。

すべてのインスタンスを選択
ターゲットとして登録するすべてのインスタンスを選択します。

インスタンスタグを指定
インスタンスタグのキーと値のペアを 1 つ以上指定して、タスクを実行するインスタンスを識別します。

タグキー タグの値(オプション) Add

ターゲットとするインスタンスに適用された、タグキーとオプションの値を入力した後、追加を選択します。

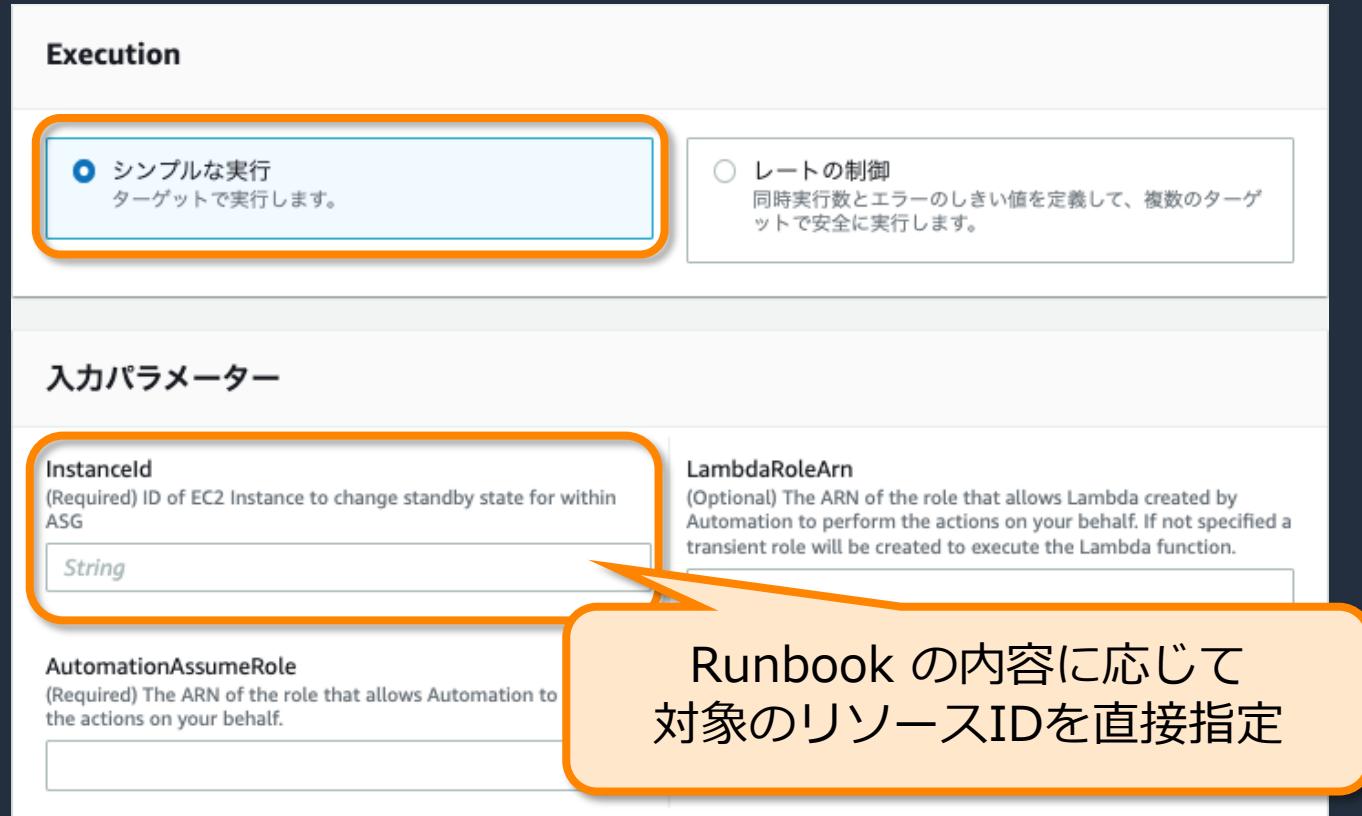
ターゲットの指定方法

Automation Runbook の場合



対象は主に AWS リソース

- ・ シンプルな実行
 - Runbook を単体で実行
- ・ レートの制御
 - 複数のターゲットに対して Runbook を実行



※入力パラメーターは一例です。実際は Runbook の内容によって変わります

ターゲットの指定方法

Automation Runbook の場合



対象は主に AWS リソース

- ・ シンプルな実行
 - Runbook を単体で実行
- ・ レートの制御
 - 複数のターゲットに対して Runbook を実行

Execution

シンプルな実行
ターゲットで実行します。

レートの制御
同時実行数とエラーのしきい値を定義して、複数のターゲットで安全に実行します。

- ・ 複数のリソースを対象に Automation Runbook を実行できる
※State Manager ではなく Automation の機能
- ・ State Manager が呼び出す 親 Automation は、ターゲットとなるリソースごとに子 Automation を起動する



Automation のドキュメントも参照ください。
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/running-automations-scale.html

ターゲットの指定方法

Automation Runbook の場合

複数のターゲットの指定方法

- パラメータ値
- リソースグループ
- タグ
- すべてのインスタンス

1 の条件に合致するターゲットの
2 のパラメータ情報を
子 Automation の 3 に連携する



ターゲットの指定方法

Automation Runbook の場合

複数のターゲットの指定方法

- パラメータ値
- リソースグループ
- タグ
- すべてのインスタンス

カンマ区切りで複数の
リソースの情報を指定可能

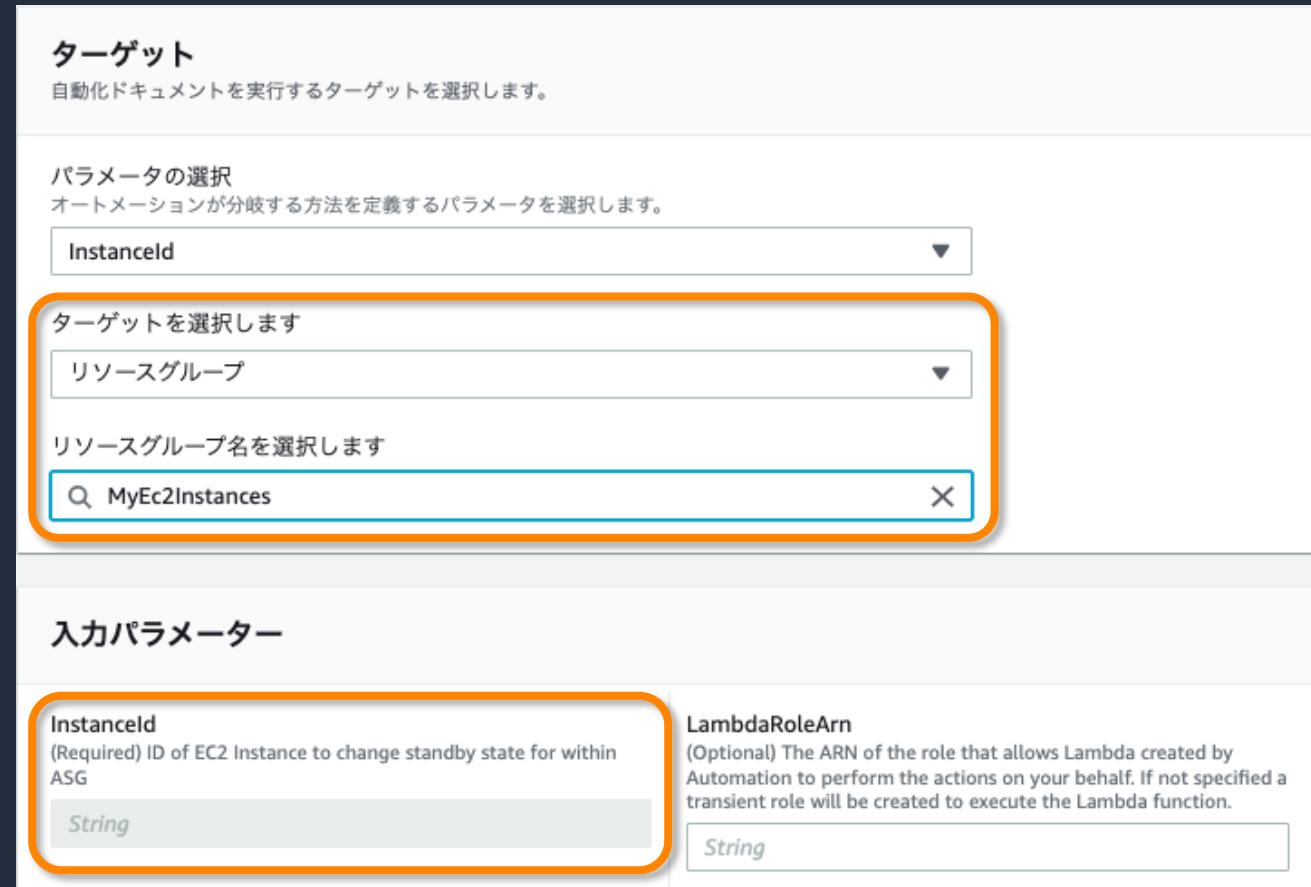


ターゲットの指定方法

Automation Runbook の場合

複数のターゲットの指定方法

- パラメータ値
- **リソースグループ**
- タグ
- すべてのインスタンス



ターゲットの指定方法

Automation Runbook の場合

複数のターゲットの指定方法

- パラメータ値
- リソースグループ
- タグ
- すべてのインスタンス



ターゲットの指定方法

Automation Runbook の場合

複数のターゲットの指定方法

- パラメータ値
- リソースグループ
- タグ
- すべてのインスタンス



同時実行数とエラーしきい値

(Command / Policy / Automation 共通)

▼ レートの制御

同時実行性
同時にタスクを実行するターゲットの数または割合(%)を指定

10 ターゲット

パーセンテージ

エラーのしきい値
指定した数または割合(%)のターゲットでタスクが失敗した後、タスクを停止

ターゲット

10 パーセンテージ

同時実行性

- 関連付けを同時に実行するターゲットの数、または割合を指定

エラーのしきい値

- この値を超えてタスクが失敗したら関連付けタスクの停止を指示したり、残りのターゲットに対する実行要求を停止する

State Manager の主要な構成要素



State Manager Association (関連付け)

SSM ドキュメント



“定義された状態”を維持するためのアクションを定義したもの

スケジュール

アクションの実行タイミングに関する設定

ターゲット



“定義された状態”を維持する対象リソース



※その他の設定項目については後述します



実行結果の可視化
(AWS Systems Manager Compliance)

スケジュールの指定方法



スケジュールなし

関連付けを1回のみ実行

→ 関連付けの作成直後に1回実行される

スケジュールあり

cron/rate 式で指定した スケジュールで関連付けを実行

→ cron式、rate式による柔軟なスケジュール設定

加えて、以下のタイミングでも実行される

- ✓ 関連付けやドキュメントの修正時
- ✓ ターゲットとなるマネージドノードが初めてオンラインになったタイミング
(Command / Inventory の場合)
- ✓ マネジメントコンソールや AWS CLI / AWS SDK から即時実行した場合
(詳細は次スライド)

関連付けの実行タイミング

指定したスケジュールで実行されるほか、以下のタイミングでも関連付けが実行される

- ✓ 関連付けを新規作成または編集したとき ※1
- ✓ SSM ドキュメントを更新したとき
- ✓ 手動で関連付けを起動したとき
- ✓ ターゲット（マネージドノード）の状態が変更になったとき ※2
 - 対象インスタンスが初めてオンラインになる
 - スケジュールを逃した後、インスタンスが初めてオンラインになる
 - 30日以上停止していたノードがオンラインになる

※1 即時実行を抑止するオプションも有り

※2 Command または Policy ドキュメントの場合

[関連付けはいつリソースに適用されますか？]

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-state-about.html#state-manager-about-scheduling

Cron 式 / Rate 式

State Manager / Maintenance Windows で使われるスケジュール表記法

- cron 式 … 時間を指定

例) 每月第3火曜日の午後11:30(UTC)

cron(30 23 ? * TUE#3 *)

※ 現在、State Manager では 関連付けの cron 式での月の指定はサポートされていません。

- rate 式 … 頻度を指定

例) 15分おき

rate(15 minutes)

- 1回限りのスケジュール実行

例) 2023年7月20日15時55分(UTC)

at(2023-07-20T15:55:00)

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/reference-cron-and-rate-expressions.html



© 2023, Amazon Web Services, Inc. or its affiliates.

Cron でスケジュール指定する場合のオプション

- ✓ ApplyOnlyAtCronInterval オプション
 - 関連付けの作成/修正直後の実行をSKIPする

- ✓ スケジュールオフセット
 - cron式で指定された日時から関連付けを実行するまでに待機する日数
 - 1日～6日まで指定可



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/reference-cron-and-rate-expressions.html

その他のオプション

関連付けの実行タイミングの制御に関する 2 つのオプション



Change Calendar (変更カレンダー)

- 対象のカレンダーが Close の場合、関連付けの実行をスキップ



Cloud Watch アラーム

- 対象のアラームが Active の場合、関連付けの実行をスキップ

The screenshot shows the AWS Lambda function configuration page. Under the 'Triggers' section, there is a 'CloudWatch alarm - オプション' (CloudWatch alarm - Options) section. It contains two main sections: '変更カレンダー' (Change calendar) and 'CloudWatch alarm - オプション' (CloudWatch alarm - Options).
変更カレンダー: A dropdown menu labeled 'Select change calendars'.
CloudWatch alarm - オプション:
- 'Alarm name': A dropdown menu labeled 'Choose alarm' with a 'Create CloudWatch alarm' button.
- A checkbox labeled 'Continue association if alarm status is unavailable': A note below it states, 'If State Manager is unable to retrieve information about the state of your CloudWatch alarm, the association continues to run.'

関連付けの作成

関連付けの設定項目

Command または Policy ドキュメント	Automation Runbook
名前	名前
ドキュメントおよびパラメーター	ドキュメントおよびパラメーター
ターゲット	Execution (ターゲットに関する設定)
スケジュール	スケジュール
コンプライアンスの重要度	-
変更カレンダー	変更カレンダー
レートの制御	レートの制御
S3出力	-
Cloud Watch アラーム	Cloud Watch アラーム

関連付けの設定項目

(Command / Policy ドキュメント固有の設定項目)

● コンプライアンスの重要度

- ✓ Compliance のダッシュボード上に、関連付けの状態(準拠 or 非準拠)とともにここで指定した重要度 (非常事態/高い/ミディアム/低い) を表示する



● S3 出力

- ✓ コマンド出力をS3上にファイルとして保存する



関連付けの実行結果の確認

実行結果の確認 - State Manager のコンソール画面



関連付け						
	関連 ID	関連付けの名前	ドキュメント名	最終実行日	ステータス	関連付けのバージョン
<input type="checkbox"/>	b288296a-52d1-46f0-b698-3d09f6d04d57	AWS-QuickSetup-SSMHostMgmt-UpdateCloudWatchAgent-tb53k	UpdateCloudWatchDocument-tb53k	Wed, 17 May 2023 15:01:39 GMT	成功	1 Success:1
<input type="checkbox"/>	ba084271-08de-4502-b99b-6821b4cc4900	AWS-QuickSetup-SSMHostMgmt-AttachIAMToInstance-tb53k	AWSQuickSetup-CreateAndAttachIAMToInstance-tb53k	Tue, 25 Apr 2023 05:20:14 GMT	成功	1 Success:15
<input type="checkbox"/>	e8ce0d24-65d9-4b7e-81ce-dff0f400f5dd	AWS-QuickSetup-SSMHostMgmt-UpdateSSMAgent-tb53k	AWS-UpdateSSMAgent	Wed, 17 May 2023 14:02:34 GMT	成功	1 Success:2
<input type="checkbox"/>	eb37b0c6-85f9-4630-a05d-3a1142cd8883	AWS-QuickSetup-PatchPolicy-ScanForPatches-LA-tg37x	AWS-RunPatchBaseline	Mon, 22 May 2023 08:11:17 GMT	失敗	1 Failed:4
<input type="checkbox"/>	ff10e458-9f16-4729-b943-3ba9369a7949		AWS-GatherSoftwareInventory	Wed, 01 Feb 2023 06:25:45 GMT	成功	1 Skipped:1

- State Manager のマネジメントコンソールで、関連付けごとの状況をリスト表示または詳細表示で確認できる
- 詳細表示画面では過去の実行履歴を確認したり、関連付けを即時実行することが可能

Association ID: b288296a-52d1-46f0-b698-3d09f6d04d57						
説明	リソース	パラメーター	ターゲット	バージョン	実行履歴	
関連付けの実行						
実行 ID	関連付けのバージョン	ステータス	状況の詳細	作成日	リソースのステータス	
34914338-e197-4a70-b7fb-061aa9f8bdca	1	成功	Success	Wed, 17 May 2023 14:31:36 GMT	Success:1	
24c4abba-5221-4b39-ac09-716517ae3ea1	1	成功	Success	Tue, 25 Apr 2023 05:18:45 GMT	Success:2	
477d9bb2-40d7-4718-a4f8-4313b3bfe00c	1	成功	Success	Sun, 26 Mar 2023 05:18:56 GMT	Success:1	

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-state-assoc-history.html

© 2023, Amazon Web Services, Inc. or its affiliates.

実行結果の確認 - Compliance のコンソール画面



- Compliance は AWS Systems Manager の一機能
- 以下の情報をコンプライアンスデータとして収集・表示することができる
 - Patch Manager によるパッチ適用のステータス
 - State Manager の関連付けに関するデータ
 - マネージドノードに対して指定したカスタムコンプライアンスタイル

The screenshot shows the AWS Systems Manager Compliance Dashboard. At the top, there's a filtering section with radio buttons for 'コンプライアンスタイプ' (selected), 'パッチグループ', and 'リソースグループ'. Below that is a search bar and filter buttons for 'リソース' and 'ルール'. The main area is titled 'コンプライアンスリソースの概要' and displays two rows of data:

コンプライアンスタイプ	準拠リソース	非準拠リソース	重要なリソース	高リソース	中リソース	低リソース	情報リソース	未指定リソース
Association	②	△ 0	△ 0	△ 0	△ 0	△ 0	△ 0	△ 0
Patch	②	△ 0	△ 0	△ 0	△ 0	△ 0	△ 0	△ 0

Compliance ダッシュボードでサマリーを確認

- ステータスが準拠／非準拠のマネージドノード数
- ステータスが準拠／非準拠の関連付けの数

TIPS



AWS Config で関連付けのコンプライアンス履歴を追跡

- AWS Config で State Manager の関連付けのコンプライアンス履歴と変更の追跡を表示可能
- AWS Config の記録対象として「SSM:AssociationCompliance」のリソースタイプを有効にしておく必要がある



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-compliance-about.html#sysman-compliance-history

© 2023, Amazon Web Services, Inc. or its affiliates.

マルチアカウント・マルチリージョン 実行

- ドキュメントタイプが Automation Runbook の場合、クロスアカウント・クロスリージョンでの関連付けの実行が可能
- マネジメントコンソールでは操作できないため、AWS CLI/AWS SDK から関連付けを作成する必要がある

```
aws ssm create-association \
--association-name association name \
--targets Key=ResourceGroup,Values=resource group name \
--name runbook name \
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/RunbookAssumeRole \
--automation-target-parameter-name target parameter \
--schedule "cron or rate expression" \
--target-locations Accounts=111122223333,444455556666,444455556666,Regions=region,region
```

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/scheduling-automations-state-manager-associations.html#create-automation-association-cli



構成管理ツールとの連携例

- **AWS-ApplyAnsiblePlaybooks SSM ドキュメント**

State Manager の関連付け経由で Ansible プレイブックを実行する

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-state-manager-ansible.html

- **AWS-ApplyChefRecipes SSM ドキュメント**

State Manager の関連付け経由で Chef recipe を実行する

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-state-manager-chef.html

- **AWS-ApplyDSCMofs SSM ドキュメント**

Windows PowerShell Desired State Configuration (PowerShell DSC) の Managed Object Format (MOF) ファイルを State Manager の関連付け経由で実行する

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-state-manager-using-mof-file.html

まとめ



まとめ

Systems Manager State Manager の特徴

- State Manager は安全でスケーラブルな設定管理サービス
- マネージドノードおよび他の AWS リソースを定義された状態に保つプロセスを自動化
- Systems Manager Inventory で利用されるほか、Command ドキュメントや Automation Runbook の定期実行も可能

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!

AWS Black Belt Online Seminar

AWS Systems Manager Patch Manager 編

小野 卓人

Solutions Architect

2024/04



自己紹介

名前：小野 卓人（Takuto Ono）

所属：技術統括本部
　　フィナンシャルサービスインダストリ技術本部
　　保険ソリューション部



経歴：

Sler で金融機関向けシステムの受託開発

インフラ設計・構築・運用保守

現在は、ソリューションアーキテクトとして主に保険業界のお客様を担当

好きなAWSサービス： AWS Systems Manager



本セミナーの対象者

AWS の運用をされている方、これから運用される予定の方

本セミナーの目的

- AWS Systems Manager Patch Manager の機能とユースケースをご理解いただく。

本日お話ししないこと

- AWS Systems Manager の全体的な説明
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager Patch Manager 以外の機能の詳細
→ 各機能にフォーカスしたセッションを参照ください

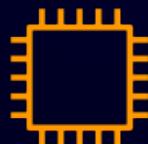
アジェンダ

1. パッチ管理の課題
2. Patch Manager の全体像
 - パッチオペレーションの流れ
 - パッチベースラインとパッチグループ、パッチポリシー
 - Patch Manager で使用する SSM ドキュメント
3. Patch Manager の開始方法
4. 実行結果の確認
5. TIPS
6. 料金
7. まとめ

パッチ管理の課題

パッチ管理における課題

パッチ適用の考慮事項



- サーバごとに異なる
 - OS、バージョン
 - インストール済みパッケージ
 - セキュリティ要件
 - 適用タイミング etc

バリエーションが増えれば
増えるほど作業が大変！

パッチ管理作業は重労働

- パッチ適用状況の管理
- 適用が必要なパッチの洗い出し
- 定期的なパッチ適用の実施
- 緊急パッチへの例外的な対応

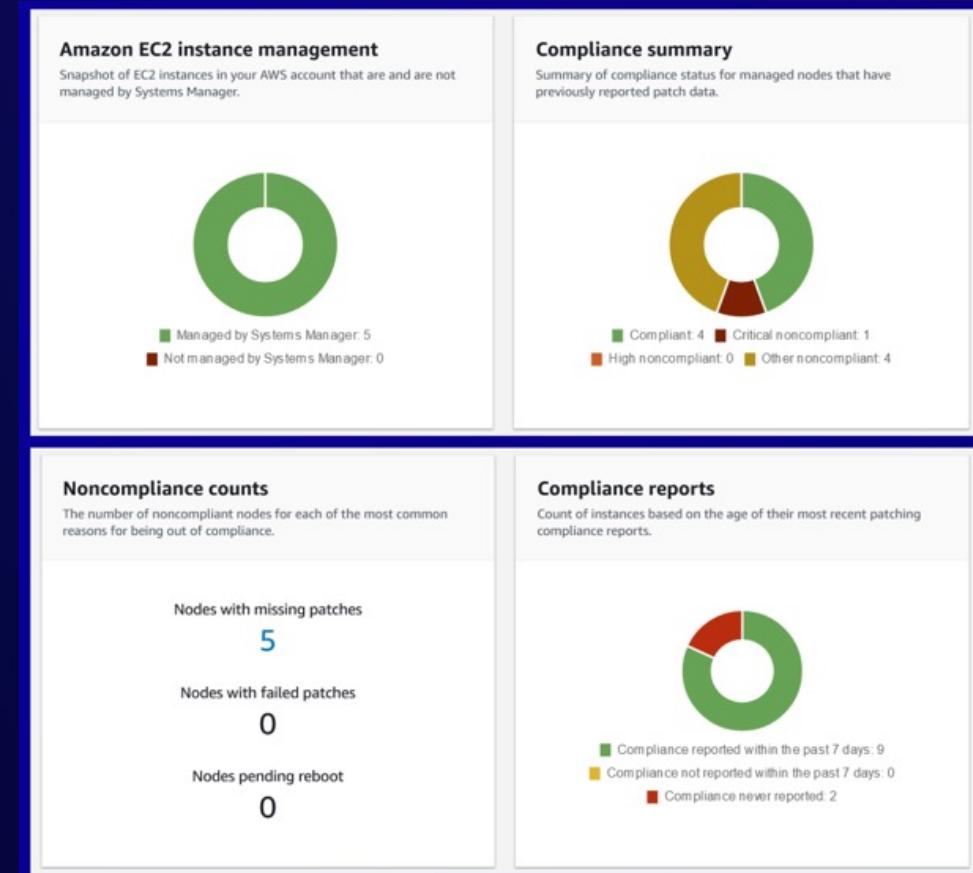




Systems Manager Patch Manager とは

マネージドノードへのパッチ適用プロセスを自動化

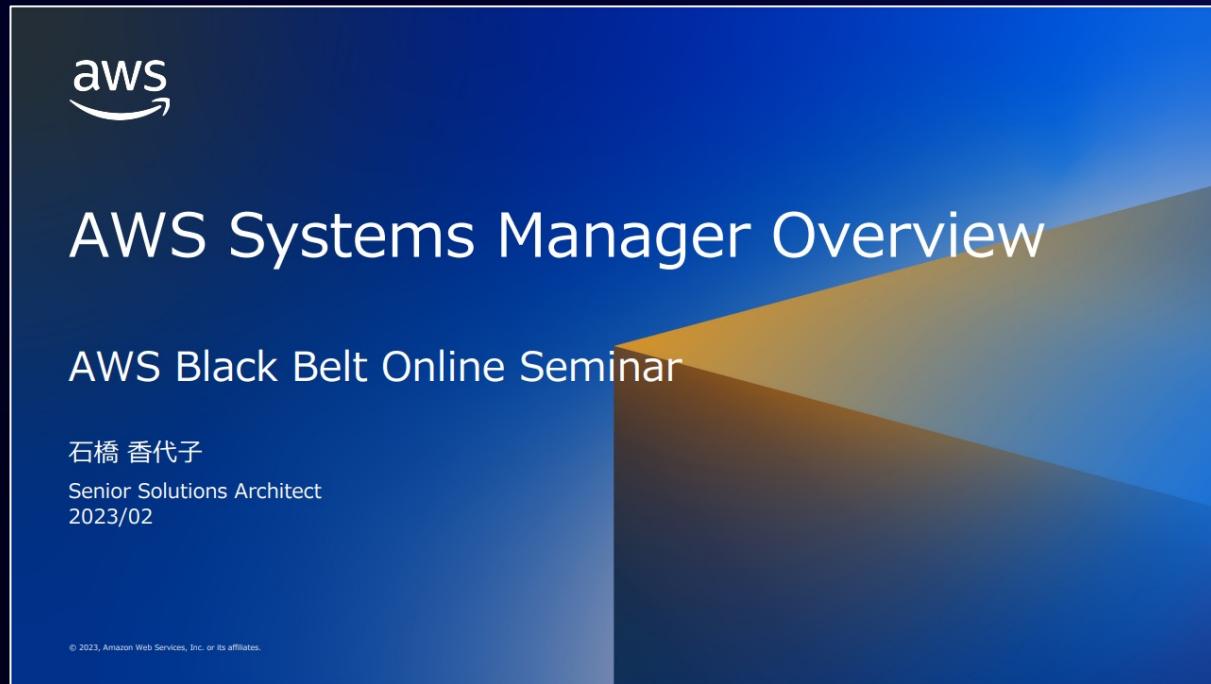
- 自動承認のルールを定義し、適用すべきパッチの選別を自動化
- 定期的にパッチをスキャン＆インストール
- ダッシュボードでパッチのコンプライアンス状況を可視化
- リソースデータ同期によりクロスアカウント、クロスリージョンでコンプライアンス情報を収集可能



(補足) マネージドノードとは

Systems Manager で使用するように設定されたマシン

Maintenance Windows の一部の機能では処理対象のサーバーをマネージドノードにする必要があります。
詳細は、AWS Black Belt Online Seminar の「[AWS Systems Manager Overview](#)」をご覧ください



AWS Systems Manager を使ってサーバ管理を行うためには

サーバを“マネージドノード”にする

ここに一覧で出てくるようになります

The screenshot shows the AWS Systems Manager Managed Nodes list. The title bar includes "マネージドノード" and "設定" buttons, a search bar, and download/report and node action buttons. A callout arrow points to the "マネージドノード" button in the title bar. The main area displays a table of managed nodes with columns: ノード ID, ノードの状態, ノード名, プラットフォーム, オペレーティングシステム, サービスタイプ, and ソース。The table shows three entries: i-04970a7f373ac630b (実行中, LaunchedBySSM, Linux, Amazon Linux AMI, EC2インスタンス), mi-0623bfeef040aa8... (On-prem-Linux, Linux, Amazon Linux, AWS-SSM-Managed), and i-016d04a4ae49531af (実行中, instance-ph@, Linux, Amazon Linux, EC2インスタンス).

マネージドノード：
➢ SSM管理下のインスタンス群
➢ EC2インスタンスのほか、
オンプレミスのインスタンスも
含められる。

(*) AWS Systems Manager = SSM と略します。

Patch Manager の前提条件

最新のサポート情報はドキュメントを参照ください

<https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-prerequisites.html>

- Systems Manager のマネージドノードであること
- (Linux 、 macOS の場合) Python がインストールされていること
- パッチソースリポジトリへの接続が可能であること
- Systems Manager サービスのホストする S3 バケットへアクセスできること

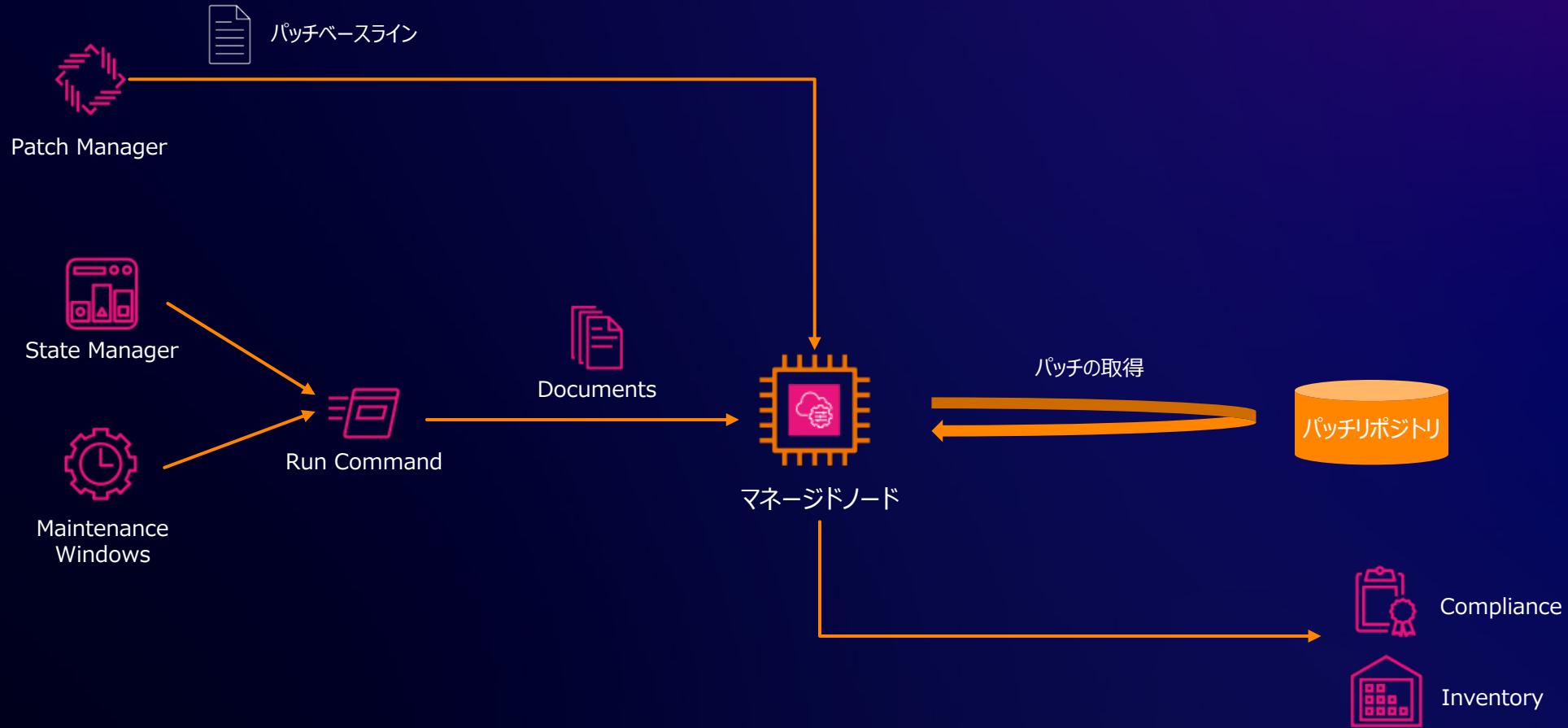
詳細はこちらを参照

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/ssm-agent-minimum-s3-permissions.html

- Patch Manager でサポートされている OS および OS バージョンであること
※ Systems Manager の他の機能でサポートされる OS のバージョンと必ずしも一致しない点に注意

Patch Manager の全体像

Patch Manager 全体像



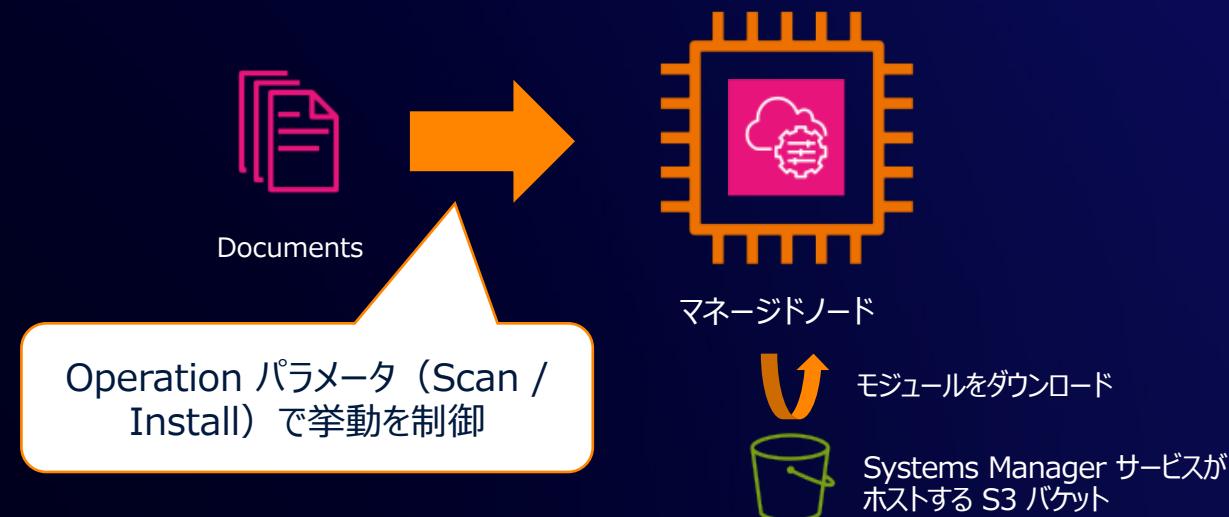
Patch Manager 全体像



パッチオペレーションの流れ

マネージドノード上で実行される処理

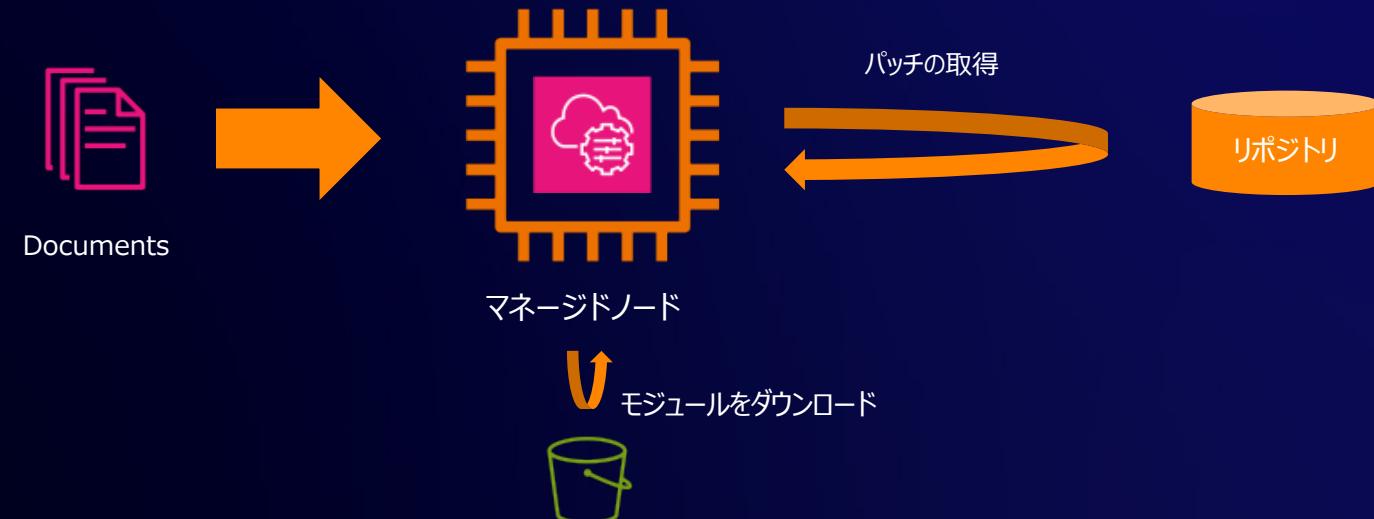
- 実行される処理の内容は **SSM ドキュメント**で定義されている
- マネージドノード上で実行される処理は、大きく2つのモードがある
 - Scan オペレーション**：指定した基準（ベースライン）に対して不足しているパッチの報告のみを実施
 - Scan and install オペレーション**：指定した基準（ベースライン）に対して不足しているパッチを自動的にインストールする
- SSM ドキュメントを実行する過程で Python モジュール（Linux/macOS）または PowerShell モジュール（Windows）を S3 からダウンロードして実行する



マネージドノード上で実行される処理

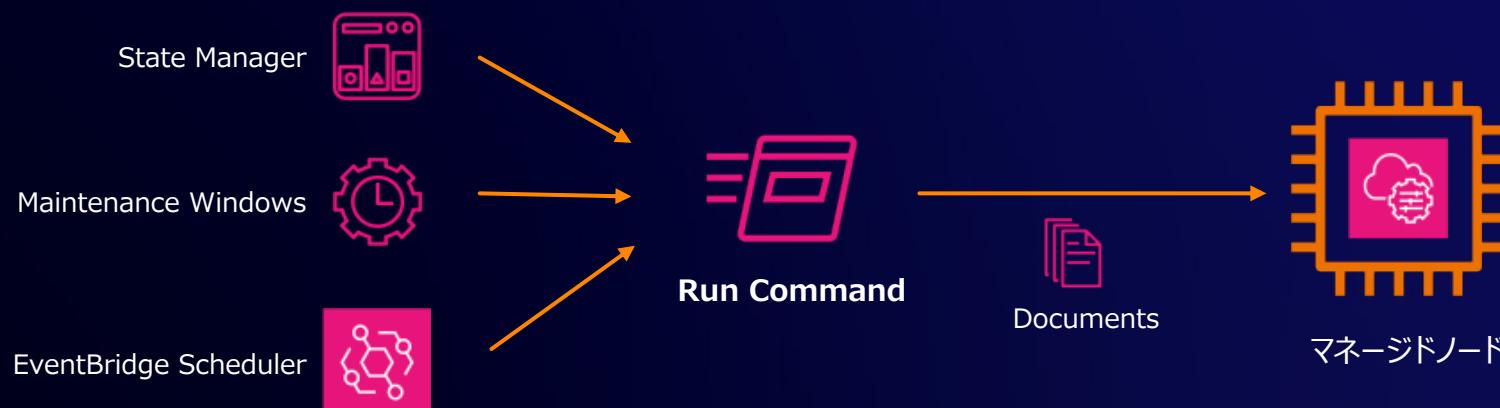
- Scan や Install の処理自体は OS 標準の仕組みを使用
(例 : Windows の場合は Windows Update API、RHEL の場合は yum / dnf)
- マネージドノードからパッチリポジトリへのネットワークアクセスが必要
 - Windows の場合、Windows Update カタログのサイトまたは Windows Server Update Services (WSUS) へのアクセスが必要
 - Linux の場合、マネージドノードに設定されているデフォルトのリポジトリ以外のソースリポジトリを代替リポジトリとして指定可能

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-alternative-source-repository.html



SSM ドキュメントの実行方法

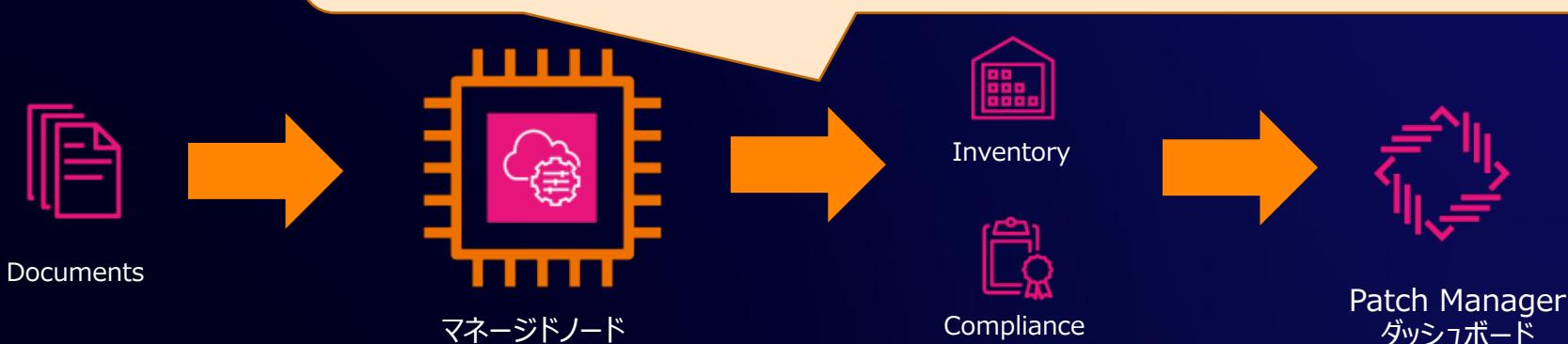
- SSM ドキュメントは SSM Run Command によって起動される
- Maintenance Windows や State Manager によって Run Command をスケジュール実行することが一般的
 - 後述の「パッチポリシー」を使用する場合 State Manager が自動的にセットアップされる
 - EventBridge Scheduler によるシンプルなスケジュール実行も可能
- Patch Manager でオンデマンドに「今すぐパッチ適用」することも可能
 - 単発実行の State Manager が自動的にセットアップされる



パッチオペレーションの実行結果

- パッチの Scan/Install 結果は SSM Inventory や SSM Compliance の API を通じて記録される
- Patch Manager のダッシュボード画面でパッチ適用の状況や、Inventory で各ノードのパッチ単位の適用状況を確認できる

- ノードごとのパッチレベルの詳細情報（パッチごとにインストール済み／未済 といった情報）
- ノードレベルのサマリ情報（インストールすべきパッチの数・インストール済パッチの数…）
- コンプライアンス状況（ノードごとのパッチコンプライアンスの準拠状況）



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-find-noncompliant-nodes.html
<https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-compliance-states.html>

パッチベースラインと パッチグループ、パッチポリシー

パッチベースライン

- オペレーティングシステムごとに用意された、適用対象のパッチをフィルタするルール
- AWSが提供する事前定義のパッチベースラインのほか、カスタムで作成することが可能

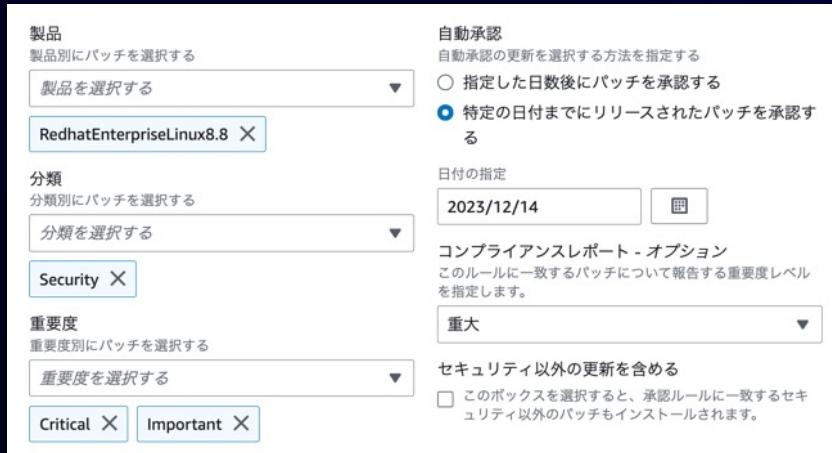


パッチベースライン - 主要な設定項目

Windows Server の場合の設定画面例



Red Hat Enterprise Linux の場合の設定画面例



- OS (Windows / Ubuntu / SUSE / RHEL など)
- 製品 : 対象となる OS のバージョンやエディション
- 分類 (Security や BugFix など)
- 重要度 (Critical や Low など)
- 自動承認の遅延または期限※ ※Debian や Ubuntu では設定不可
- コンプライアンスレポートの重要度 (重大/高/中/低/情報/未指定)
- 承認済みパッチ/拒否済みパッチ
- 代替パッチソースリポジトリ (Linux の場合)

- 対象の OS によって設定可能項目が若干異なる
- Windows の場合、OS のパッチだけでなく Microsoft の提供するアプリケーション (SQLServer や Exchange など) のパッチに関するルールも作成可能

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-patch-baselines.html

パッチベースラインとマネージドノードの関連付け

パッチグループ

パッチポリシーを使用しない従来の方式

- マネージドノードに「**Patch Group**」または「**PatchGroup**」タグを設定
- タグの値に応じてパッチベースラインを紐付ける

パッチポリシー

広範囲なパッチ適用オペレーションを
簡易かつ一元的に制御できる新しい方式

- パッチポリシーの適用範囲を指定する
 - 組織全体
 - OU/リージョン指定
 - 現在のアカウント
- ターゲットの OS の種類ごとにパッチベースラインを指定する

パッチグループ

- マネージドノードを特定のパッチベースラインへ関連付ける従来からの仕組み
- マネージドノードに「**Patch Group**」または「**PatchGroup**」タグを設定する

※スペースあり

※スペース無し

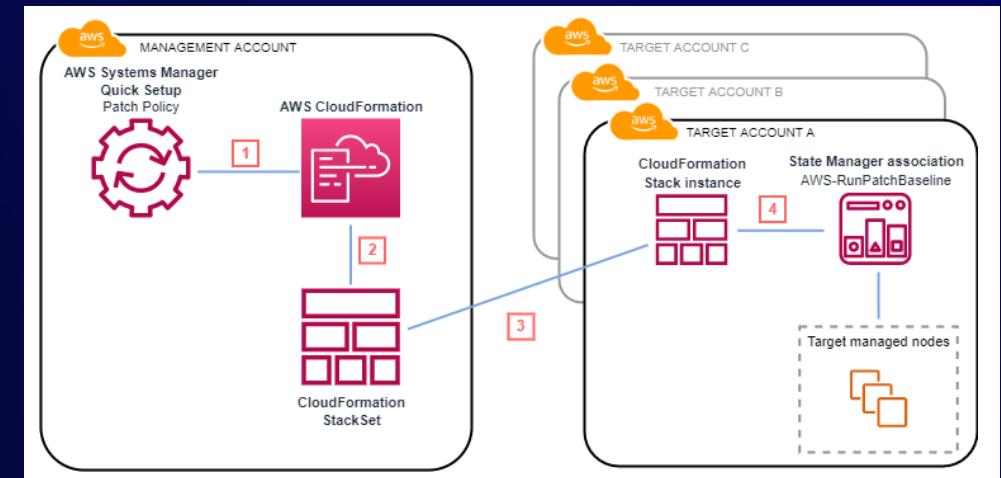


- ✓ マネージドノードごとに 1 つのパッチグループに所属できる
- ✓ 各パッチグループは OS ごとに1つのパッチベースラインへ紐づけできる
- ✓ パッチグループに所属しないマネージドノードはデフォルトのパッチベースラインが適用される

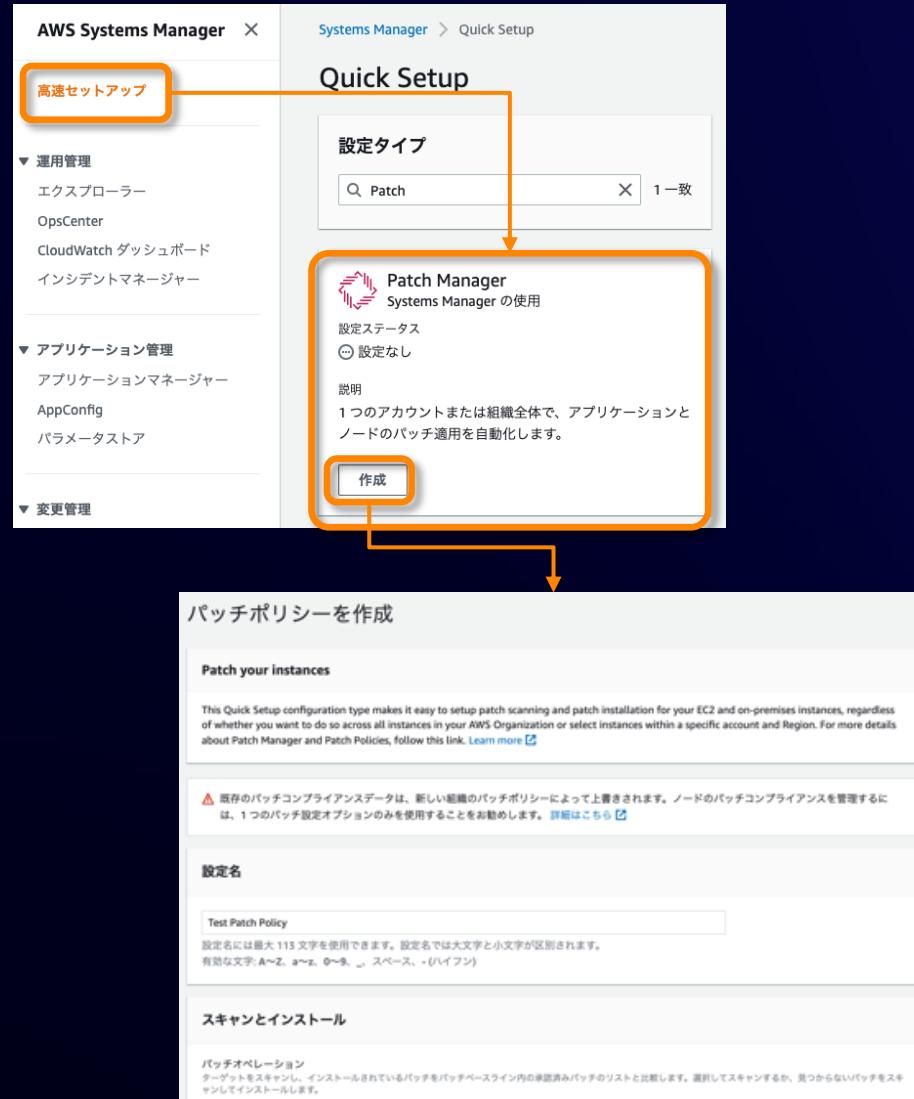
パッチポリシー

- 2022年12月にリリースされた、マルチアカウント/マルチリージョン環境でのパッチ適用オペレーションを一元的に制御できる機能
- Systems Manager の Quick Setup を使用してセットアップ
- パッチグループの設定は不要で、OS の種類ごとに AWS マネージドベースラインまたはカスタムベースラインを指定する
- スケジュールに従って AWS-RunPatchBaseline SSM ドキュメントを実行する State Manager 関連付けが対象のアカウント/リージョンに対して自動的にセットアップされる
- 現状、パッチポリシーは一部のリージョンでサポートされていない点に注意

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-policies.html



パッチポリシーの設定方法 (1/3)



Quick Setup からパッチポリシーの設定を行う

- Scan / Install それぞれの実行スケジュール
- パッチインストール後の再起動の有無
- OS の種類ごとに使用するパッチベースライン
- ログの出力先
- レート制御
- IAM ポリシーの追加
- ターゲット (後述)

パッチポリシーを作成すると、対象のアカウント/リージョンで CloudFormation Stack インスタンスが作成される

Quick Setup パッチポリシーの使用

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-policies.html

パッチポリシーの設定方法 (2/3)

OS の種類ごとに使用するパッチベースラインを指定可能

AWS から提供されるデフォルトのパッチベースラインのほか、カスタムのパッチベースラインも指定可

オペレーティングシステム	ベースラインを選択	ベースライン ID
Alma Linux	AWS-AlmaLinuxDefaultPatchBaseline	pb-0aca46f9a9d062454
Amazon Linux	AWS-AmazonLinuxDefaultPatchBaseline	pb-0221829c157d721d8
Amazon Linux 2	AWS-AmazonLinux2DefaultPatchBaseline	pb-00fda5699d1ae3942
Amazon Linux 2022	AWS-AmazonLinux2022DefaultPatchBaseline	pb-067dab85430494167
Amazon Linux 2023	AWS-AmazonLinux2023DefaultPatchBaseline	pb-0be4fdf9cb953577d
CentOS	AWS-CentOSDefaultPatchBaseline	pb-0b4917141375bc4b5
Debian Server	AWS-DebianDefaultPatchBaseline	pb-0d5f3f8560fc606e3
macOS	AWS-MacOSDefaultPatchBaseline	pb-0ff8843fd26c9bc63
Oracle Linux	AWS-OracleLinuxDefaultPatchBaseline	pb-04ed5d5c38572bb74
Raspberry Pi OS	AWS-RaspbianDefaultPatchBaseline	pb-04e6dbcacf1dc4ef
Red Hat Enterprise Linux (RHEL)	AWS-RedHatDefaultPatchBaseline	pb-0adf5cb7136a2984d
Rocky Linux	AWS-RockyLinuxDefaultPatchBaseline	pb-05b8b04891f902733
SUSE Linux Enterprise Server (SLES)	AWS-SuseDefaultPatchBaseline	pb-045f39f1765049417
Ubuntu Server	AWS-UbuntuDefaultPatchBaseline	pb-0ec96a11368349171
Windows Server	AWS-DefaultPatchBaseline	pb-04ba050f612fba3a6

パッチポリシーの設定方法 (3/3)

ターゲット：パッチポリシーをデプロイする対象ノード

組織全体

- 組織内のOUおよびリージョン内の全てのマネージドノードを対象とする



OUとリージョンを選択

- 選択した OU とリージョン内の全てのマネージドノードを対象とする
- 選択した OU とリージョン内で、特定のタグの key または key-value を持つマネージドノードを対象とする

現在のアカウント

リージョンを指定

- 選択したリージョン内の全てのマネージドノードを対象とする
- 選択したリージョン内で、特定のタグの key または key-value を持つマネージドノードを対象とする

現在のリージョン

- 全てのマネージドノード
- リソースグループ指定
- ノードタグ指定
- 手動 (インスタンスID指定)

Patch Manager で使用する SSM ドキュメント

Patch Manager で使用される SSM ドキュメント



現在、使用が推奨されているのは以下の SSM ドキュメント

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-ssm-documents.html

ドキュメント名	説明	対象OS
AWS-ConfigureWindowsUpdate	Windows Update 機能を設定し、自動アップデートをオンまたはオフにする。パッチベースラインによる制御やパッチのコンプライアンス情報の収集は実施しない	Windows
AWS-InstallWindowsUpdates	Windows Server のマネージドノードにアップデートをインストールする。パッチベースラインによる制御やパッチのコンプライアンス情報の収集は実施しない	Windows
AWS-RunPatchBaseline	ノードをスキャンしてパッチの適用状況を調査したり、ノードにパッチをインストールすることができる。パッチベースラインによる制御やパッチのコンプライアンス情報の収集を行う	Windows/Linux/macOS
AWS-RunPatchBaselineAssociation	AWS-RunPatchBaseline ドキュメントと似ているが、BaselineTags と呼ばれるパラメータを使用することで特定のパッチベースラインを選択することができる。EC2インスタンス以外の、ハイブリッド環境のノードは未サポート	Windows/Linux/macOS
AWS-RunPatchBaselineWithHooks	AWS-RunPatchBaseline ドキュメントをラップしている。パッチサイクル中の3つのポイント（パッチのインストール前、インストール後、再起動後）で他のSSMドキュメントを実行することができる	Windows/Linux/macOS

上記以外の SSM ドキュメント（レガシーSSMドキュメント）については以下のドキュメント参照

<https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-ssm-documents.html#patch-manager-ssm-documents-legacy>

Patch Manager で使用される SSM ドキュメント



現在、使用が推奨されているのは以下の SSM ドキュメント

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-ssm-documents.html

ドキュメント名	説明	対象OS
AWS-ConfigureWindowsUpdate	Windows Server への基本的なパッチ適用または Windows Update の設定のみを実施したい場合に使用する	
AWS-InstallWindowsUpdates		
AWS-RunPatchBaseline	通常はこのドキュメントを使用すると良い (パッチポリシーを設定する場合、このドキュメントが使用される)	
AWS-RunPatchBaselineAssociation	主に Quick Setup ホスト管理設定 機能（後述）によって使用されることを想定している	
AWS-RunPatchBaselineWithHooks	ライフサイクルフック処理をカスタマイズしたい場合に使用する	

上記以外の SSM ドキュメント（レガシ-SSMドキュメント）については以下のドキュメント参照

<https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-ssm-documents.html#patch-manager-ssm-documents-legacy>

Patch Manager の開始方法

Patch Manager の一般的な開始方法

- Quick Setup でパッチポリシーを設定する
- Quick Setup でホスト管理オプションを設定する
- パッチ適用向けのメンテナンスウィンドウを作成する
- Patch Manager の「今すぐパッチ適用」からオンデマンドのパッチオペレーションを実行する

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager.html



Quick Setup でパッチポリシーを設定する

- Scan / Install のスケジュール、ターゲット、パッチベースライン 等の設定を行う
- 一度の操作で複数のアカウント、複数のリージョンに対して設定内容を展開できるのが特徴

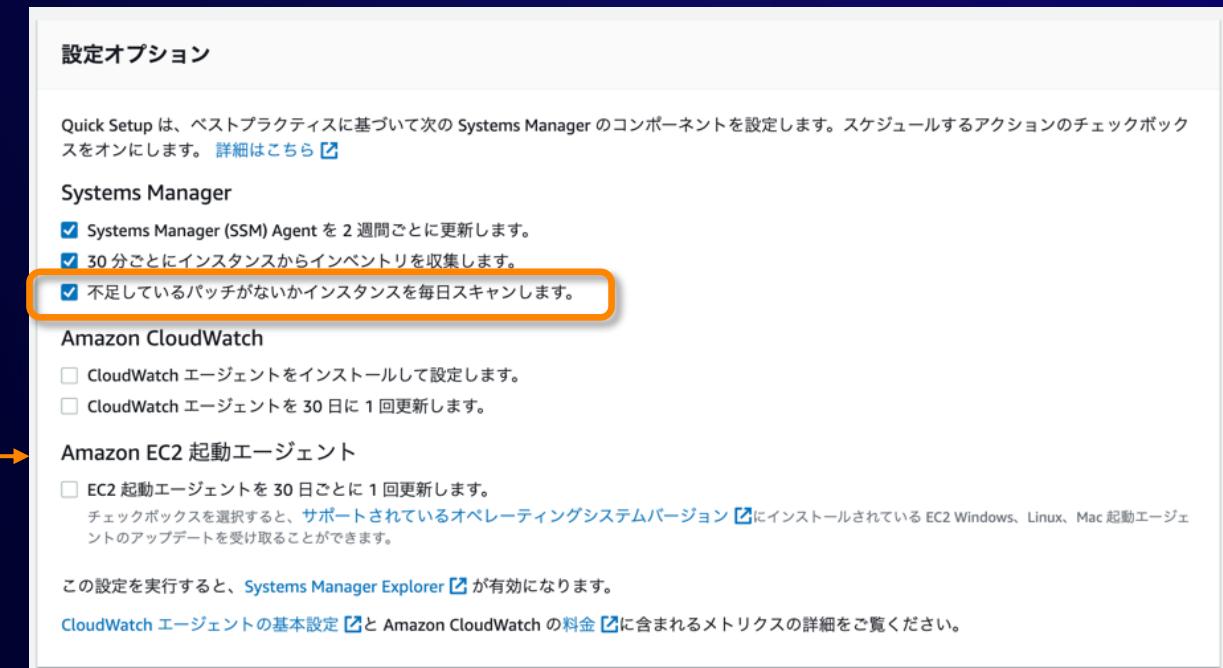
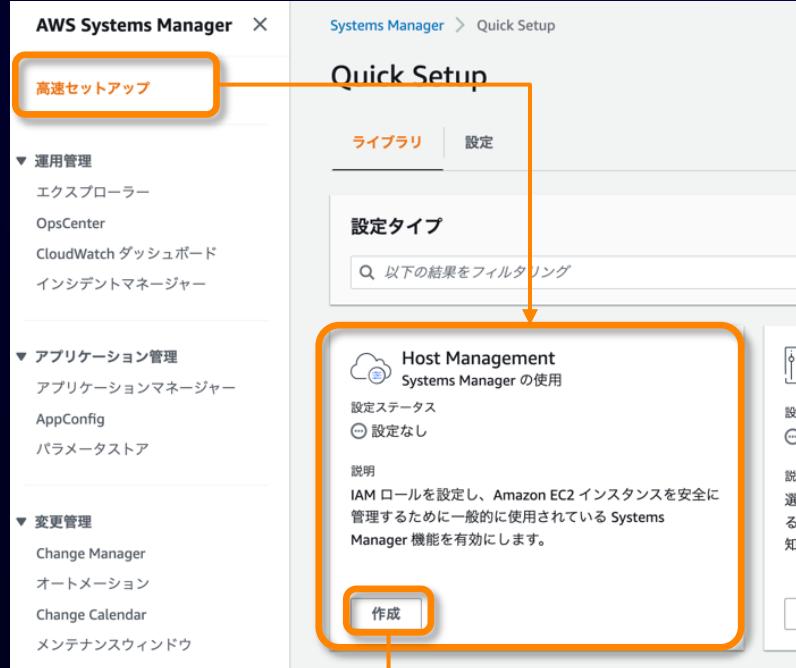
The screenshot shows the AWS Systems Manager Quick Setup interface. On the left, the navigation pane includes 'AWS Systems Manager' with a highlighted 'Quick Setup' button, '運用管理' (Operations Management) with 'エクスプローラー', 'OpsCenter', 'CloudWatch ダッシュボード', and 'インシデントマネージャー'; 'アプリケーション管理' with 'アプリケーションマネージャー', 'AppConfig', and 'パラメータストア'; and '変更管理'. The main 'Quick Setup' page has a search bar for 'Patch' and a list item 'Patch Manager Systems Manager の使用' with a '設定なし' status and a note about applying patches to accounts or organizations. A large orange box highlights this section, and an arrow points from it to the right panel. The right panel is titled 'パッチポリシーを作成' (Create Patch Policy) and contains sections for 'Patch your instances' (warning about overwriting existing patch compliance data), '設定名' (Setting Name) with a 'Test Patch Policy' input field, 'スキャンとインストール' (Scan and Install) with options for 'スキャナ' (Scanner) and 'スキャナとインストール' (Scanner and Install), 'スキャンのスケジュール' (Scan Schedule) with '推奨される既定値を使用' (Use recommended default) and 'カスタムスキャンスケジュール' (Custom scan schedule) options, 'インストールスケジュール' (Install Schedule) with '推奨される既定値を使用' (Use recommended default) and 'カスタムインストールスケジュール' (Custom install schedule) options, and 'パッチベースライン' (Patch Baseline) with a note about accepting or rejecting patches. Another arrow points from the 'Patch Manager' section in the center to the 'Patch Policies' section on the right.

Quick Setup パッチポリシーの使用

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-policies.html

Quick Setup でホスト管理オプションを設定する

- SSM Agent のアップデートやインベントリ収集の設定に加え、パッチのスキャンのスケジュールを簡単に設定できる
 - インストールのオペレーションは実行できない



Amazon EC2 ホスト管理

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/quick-setup-host-management.html

パッチ適用向けのメンテナンスウィンドウの作成

- ・ パッチポリシーが登場する以前の一般的なシナリオ
- ・ 所定のタイムウインドウ内で複数のターゲットに対して SSM ドキュメントを実行
 - ・ SSM ドキュメントを直接実行するほか、Automation ランブックや State Manager の実行も可能
- ・ セットアップの手間はかかるがカスタマイズしやすい方法



Maintenance Windows*



Run Command

※要件に応じてその他の
スケジューラーを使用することも可能

チュートリアル: パッチ適用向けのメンテナンスウィンドウの作成 (コンソール)
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-patch-mw-console.html

「今すぐパッチ適用」からオンデマンドのパッチオペレーションを実行

- ・ パッチオペレーションをオンデマンドで即時実行したい場合に有用

The screenshot shows the AWS Systems Manager interface with the 'Patch Manager' tab selected. The main content area displays various metrics and reports related to patch management, such as 'Amazon EC2 インスタンス管理' (EC2 Instance Management) and 'コンプライアンス違反数' (Compliance Violation Count). The 'Patch Manager' button is highlighted with an orange box.

This screenshot shows the 'Patch Manager' configuration page. It includes sections for '基本設定' (Basic Settings), 'パッチ適用操作' (Patch Application Operation), '再起動オプション' (Reboot Options), 'パッチを適用するインスタンス' (Instances to Apply Patch To), and 'ログストレージのパッチ適用中' (Patch Application Log Storage). The 'Patch Manager' button is highlighted with an orange box at the bottom right.

マネジドノードへのオンデマンド パッチ適用

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-patch-now-on-demand.html

Patch Manager の開始方法の比較

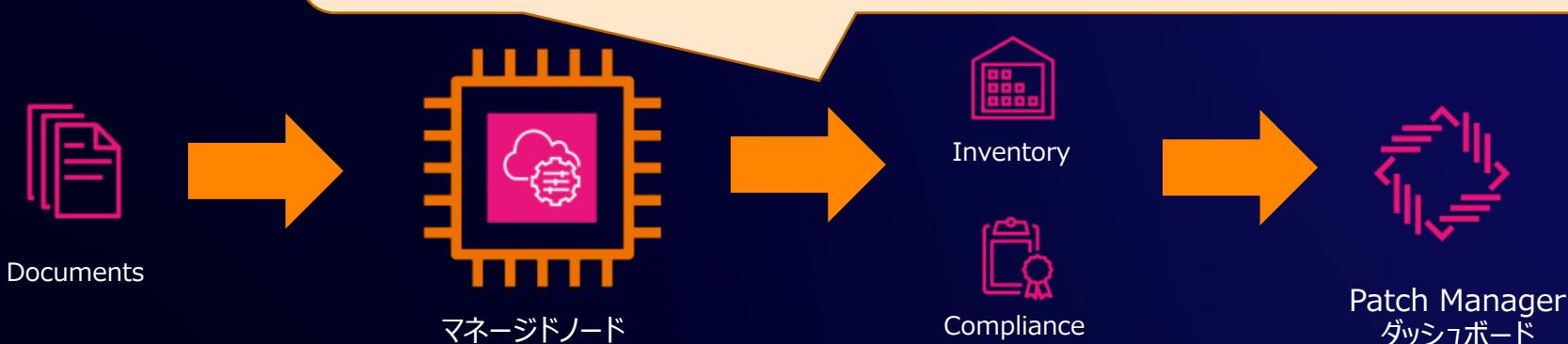
比較項目	パッチポリシー	ホスト管理オプション	メンテナンスウィンドウ	今すぐパッチ適用
Scan/Install	どちらも可	Scanのみ	どちらも可	どちらも可
スケジュール	設定可 (State Manager 関連付けが自動でセットアップされる)	設定可 (State Manager 関連付けが自動でセットアップされる)	設定可 (自分でメンテナンス ウィンドウ等を作成する必要がある)	即時実行のみ (即時実行用の State Manager 関連付けが自動でセットアップされる)
パッチベースライン	OSごとに指定したパッチベースラインを使用する	所属するパッチグループに応じたパッチベースラインが使用される	所属するパッチグループに応じたパッチベースラインが使用される。 BaselineOverride パラメータ (後述)で上書きすることも可能	所属するパッチグループに応じたパッチベースラインが使用される
SSM ドキュメント	AWS-RunPatchBaseline	AWS-RunPatchBaselineAssociation	任意のSSMドキュメントを指定可	AWS-RunPatchBaseline または AWS-RunPatchBaselineWithHooks
対象ノード	マネージドノード	EC2のマネージドノード (ハイブリッド環境のノードは対象外)	マネージドノード	マネージドノード
マルチアカウント / マルチリージョン	管理アカウントから一元的に設定可能	管理アカウントから一元的に設定可能	アカウントやリージョンごとに設定が必要	アカウントやリージョンごとに実行が必要

実行結果の確認

パッチオペレーションの実行結果

- パッチの Scan/Install 結果は SSM Inventory や SSM Compliance の API を通じて記録される
- Patch Manager のダッシュボード画面でパッチ適用の状況や、Inventory で各ノードのパッチ単位の適用状況を確認できる

- ノードごとのパッチレベルの詳細情報（パッチごとにインストール済み／未済 といった情報）
- ノードレベルのサマリ情報（インストールすべきパッチの数・インストール済パッチの数…）
- コンプライアンス状況（ノードごとのパッチコンプライアンスの準拠状況）



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-find-noncompliant-nodes.html
<https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-compliance-states.html>

パッチダッシュボード (1/3)

Patch Manager のパッチダッシュボード画面でパッチオペレーションのサマリを確認可能

The screenshot displays the AWS Patch Manager Dashboard, which includes the following sections:

- パッチマネージャー概要**: A summary section with links to "パッチポリシーを作成", "ダッシュボードを表示", and "コンプライアンスレポートを表示". It shows a green circle with 100% status.
- Amazon EC2 インスタンス管理**: A section titled "お客様の AWS アカウントで Systems Manager で管理されているインスタンスと管理されていない EC2 インスタンスのスナップショット". It shows a green circle with 100% status.
- パッチコンプライアンスの概要**: A section titled "以前にパッチデータを報告したマネージドノードのコンプライアンスステータスの概要". It shows a green circle with 100% status, indicating "準拠".
- コンプライアンス違反数**: A section titled "コンプライアンス違反数". It shows 0 violations.
- コンプライアンスレポート**: A section titled "コンプライアンスレポート". It shows a green circle with 100% status.
- パッチが欠落しているノード**: A section showing 0 nodes.
- パッチが失敗したノード**: A section showing 0 nodes.
- 再起動を保留中のノード**: A section showing 0 nodes.
- 過去 7 日以内に報告されたコンプライアンス**: A section showing 100% status.
- 過去 7 日以内に報告されていないコンプライアンス**: A section showing 0 status.
- コンプライアンスは報告されていません**: A section showing 0 status.

The dashboard also includes a table for "パッチポリシーに基づかないオペレーション" and a table for "パッチタスク".

- マネージドノード/非マネージドノード である EC2インスタンスの台数
- パッチコンプライアンスのステータス概要
- コンプライアンス非準拠のノード数
- 最新のパッチ適用コンプライアンス報告状況

パッチダッシュボード (2/3)

パッチポリシーに基づかないオペレーション

The screenshot shows the AWS Systems Manager Patch Manager Dashboard. It includes sections for patch compliance (Amazon EC2 Instances Management), patch baseline status, and a list of non-policy-based operations. A red box highlights the list of non-policy-based operations at the bottom.

パッチポリシーに基づかないオペレーション (63)

操作	開始日	ドキュメント名	終了時刻	ステータス	ターゲット
Scan	2023年10月30日(月)	AWS-RunPatchBaseline	02:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月30日(月)	AWS-RunPatchBaseline	01:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月30日(月)	AWS-RunPatchBaseline	00:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	23:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	22:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	21:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	20:46:47 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	19:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	18:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	17:46:47 UTC	Success	resource-groups:Name: AutomationPatchGroup

The screenshot shows the AWS Systems Manager Patch Manager Details page for non-policy-based operations. It lists 63 operations, all of which were successful. A red box highlights the list of operations.

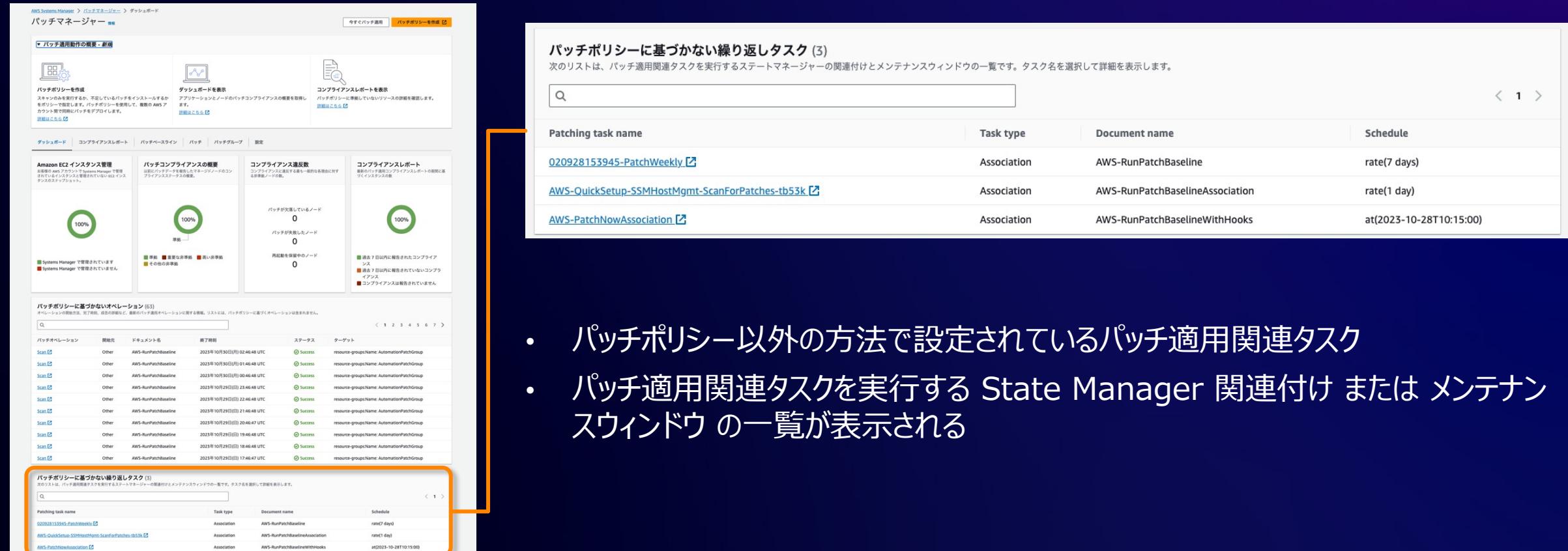
パッチポリシーに基づかないオペレーション (63)

操作	開始日	ドキュメント名	終了時刻	ステータス	ターゲット
Scan	2023年10月30日(月)	AWS-RunPatchBaseline	02:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月30日(月)	AWS-RunPatchBaseline	01:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月30日(月)	AWS-RunPatchBaseline	00:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	23:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	22:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	21:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	20:46:47 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	19:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	18:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	2023年10月29日(日)	AWS-RunPatchBaseline	17:46:47 UTC	Success	resource-groups:Name: AutomationPatchGroup

- パッチポリシー以外の方法で実行されたパッチ適用オペレーションの履歴

パッチダッシュボード (3/3)

パッチポリシーに基づかない繰り返しタスク



The screenshot shows the AWS Systems Manager Patch Manager Dashboard. On the left, there's a sidebar with links like 'Patch Policy-based Task' (selected), 'Dashboard', 'Patch Compliance Report', 'Patch Baseline', 'Patch Group', and 'Schedule'. The main area has three cards: 'Patch Policy-based Task' (100% success), 'Patch Compliance Report' (100% success), and 'Patch Compliance Countermeasures' (0 successful nodes). Below these is a section titled 'Patch Policy-based Recurring Task (3)' which lists three tasks:

Patching task name	Task type	Document name	Schedule
020928153945-PatchWeekly	Association	AWS-RunPatchBaseline	rate(7 days)
AWS-QuickSetup-SSMHostMgmt-ScanForPatches-tb53k	Association	AWS-RunPatchBaselineAssociation	rate(1 day)
AWS-PatchNowAssociation	Association	AWS-RunPatchBaselineWithHooks	at(2023-10-28T10:15:00)

An orange bracket on the left side groups the 'Patch Policy-based Task' card and the 'Patch Policy-based Recurring Task' section. Another orange bracket on the right side groups the 'Patch Policy-based Task' card and the 'Patch Compliance Report' card.

- パッチポリシー以外の方法で設定されているパッチ適用関連タスク
- パッチ適用関連タスクを実行する State Manager 関連付け または メンテナンスウィンドウ の一覧が表示される

コンプライアンスレポート (1/2)

Patch Manager のコンプライアンスレポート画面

AWS Systems Manager > パッチマネージャー > コンプライアンスレポート

パッチマネージャー - 情報

▶ パッチ適用動作の概要 - 新規

ダッシュボード | コンプライアンスレポート | パッチベースライン | パッチ | パッチグループ | 設定

ノードのパッチ適用の詳細 (1)

名前 ノード ID パッチ設定名 パッチ設定タイプ コンプライアンス状況 重要な非準拠の数 セキュリティの非準拠の数 その他の非準拠の数

target-1c-2	i-033594a67a0cf464d	test-policy,patch-policy	Patch group	準拠	0	0	0
-------------	---------------------	--------------------------	-------------	----	---	---	---

今すぐパッチ適用 パッチポリシーを作成

ログを表示 詳細を表示 S3へエクスポート すべてのS3エクスポートを表示

< 1 >

AWS Systems Manager > Run Command > コマンドID: i-033594a67a0cf464d > 出力先: i-033594a67a0cf464d

出力先: i-033594a67a0cf464d

ステップ 1 - コマンドの説明とステータス

ステータス	詳細なステータス	レスポンスコード	ステップ名	開始時間	終了時間
成功	成功	0	PreInstallScan	Sat, 28 Oct 2023 10:15:21 GMT	Sat, 28 Oct 2023 10:15:50 GMT

▼ Output

The command output displays a maximum of 48,000 characters. You can view the complete command output in Amazon S3.

/usr/bin/python3
/usr/bin/python2.7
/usr/bin/python2
/usr/bin/python
/usr/bin/yum

▶ Error

AWS Systems Manager > パッチマネージャー > コンプライアンスレポート > インスタンス i-033594a67a0cf464d のパッチを表示

パッチマネージャー - 情報

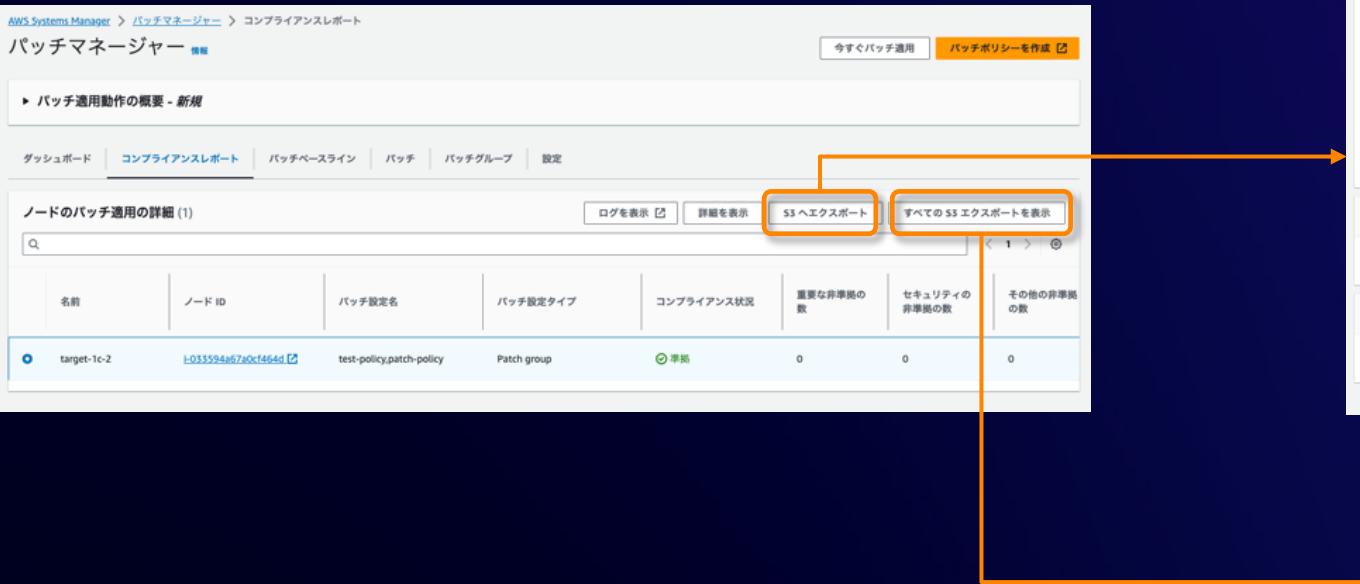
パッチの概要 (534)

名前	状態	分類	重要度	コンプライアンスレベル	パッチ設定名	パッチ設定タイプ
alx86_64	InstalledOther	-	-	UNSPECIFIED	test-policy,patch-policy	Patch group
apcid.x86_64	InstalledOther	-	-	UNSPECIFIED	test-policy,patch-policy	Patch group
alsa-lib.x86_64	InstalledOther	-	-	UNSPECIFIED	test-policy,patch-policy	Patch group
amazon-cloudwatch-agent.x86_64	Installed	Security	Medium	UNSPECIFIED	test-policy,patch-policy	Patch group
amazon-linux-extras-yum-plugin.noarch	InstalledOther	-	-	UNSPECIFIED	test-policy,patch-policy	Patch group
amazon-linux-extras-search	InstalledOther	-	-	UNSPECIFIED	test-policy,patch-policy	Patch group
amazon-ssm-agent.x86_64	Installed	Security	Important	UNSPECIFIED	test-policy,patch-policy	Patch group
at.x86_64	InstalledOther	-	-	UNSPECIFIED	test-policy,patch-policy	Patch group
attr.x86_64	InstalledOther	-	-	UNSPECIFIED	test-policy,patch-policy	Patch group
audit-libs.x86_64	InstalledOther	-	-	UNSPECIFIED	test-policy,patch-policy	Patch group

- Run Command の実行結果や、ノードごとにパッチの明細レベルでの適用状況を確認可能

コンプライアンスレポート (2/2)

パッチレポート



AWS Systems Manager > パッチマネージャー > コンプライアンスレポート

パッチマネージャー 情報

パッチ適用動作の概要 - 新規

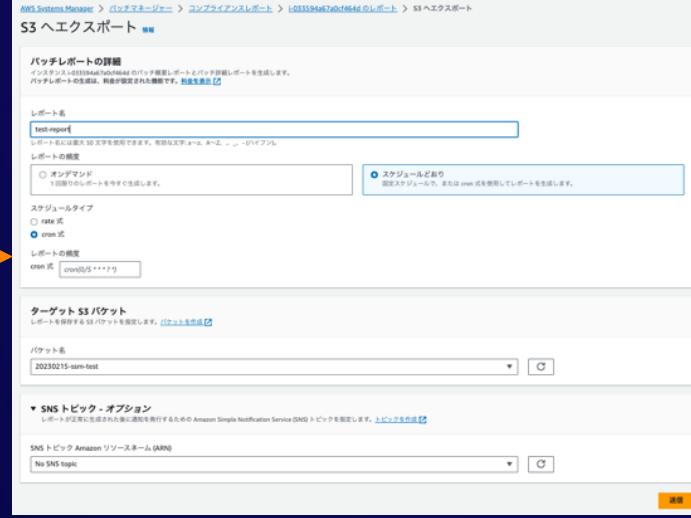
ダッシュボード | コンプライアンスレポート | パッチベースライン | パッチ | パッチグループ | 設定

ログを表示 [] | 詳細を表示 [] | S3へエクスポート | すべてのS3エクスポートを表示 []

ノードのパッチ適用の詳細 (1)

名前	ノード ID	パッチ設定名	パッチ設定タイプ	コンプライアンス状況	重要な非準拠の数	セキュリティの非準拠の数	その他の非準拠の数
target-1c-2	i-033594a67a0cf1f6ed	test-policy.patch-policy	Patch group	準拠	0	0	0

今すぐパッチ適用 | パッチポリシーを作成 []



AWS Systems Manager > パッチマネージャー > コンプライアンスレポート > S3へエクスポート

パッチレポートの詳細

パッチマネージャー (i-033594a67a0cf1f6ed) のパッチ履歴レポートとパッチ詳細レポートを生成します。

パッチレポートの名前は、料金が課せられる項目です。[編集] [削除]

レポート名: test-export

レポート名に最大 50 文字を使用できます。英数字、_、-、_、-、!、@、#、\$、%、^、&、`

レポートの範囲: オンデマンド | 1回限りのレポートを今すぐ生成します。 | スケジュールどおり: 毎日スケジュール。またはcron式を使用してレポートを生成します。

スケジュールタイプ: cron 式

レポートの範囲: cron [cron(0 0 * * *)]

ターゲット S3 バケット: レポートを保存する S3 バケットを指定します。[編集] [削除]

バケット名: 20230215-scm-test

SNS トピック - オプション: レポートが定期的に生成された際に通知を行なうための Amazon Simple Notification Service (SNS) トピックを指定します。[トピックを追加]

SNS トピック Amazon リソース名 (ARN): No SNS topic

確認 []



AWS Systems Manager > パッチマネージャー > コンプライアンスレポート > すべてのS3エクスポートを表示

Export history | Report schedule rules

パッチレポート履歴 (1)

レポート生成 ID	ドキュメント名	ステータス	開始時刻	終了時刻	ユーザー
e13fd53-f0b3-465c-91c2-2985dc2a6bb	AWS-ExportPatchReportToS3	Success	2023-10-30 1:24:20 pm	2023-10-30 1:25:01 pm	[]



AWS Systems Manager > パッチマネージャー > コンプライアンスレポート > すべてのS3エクスポートを表示

Export history | Report schedule rules

レポートスケジュールルール

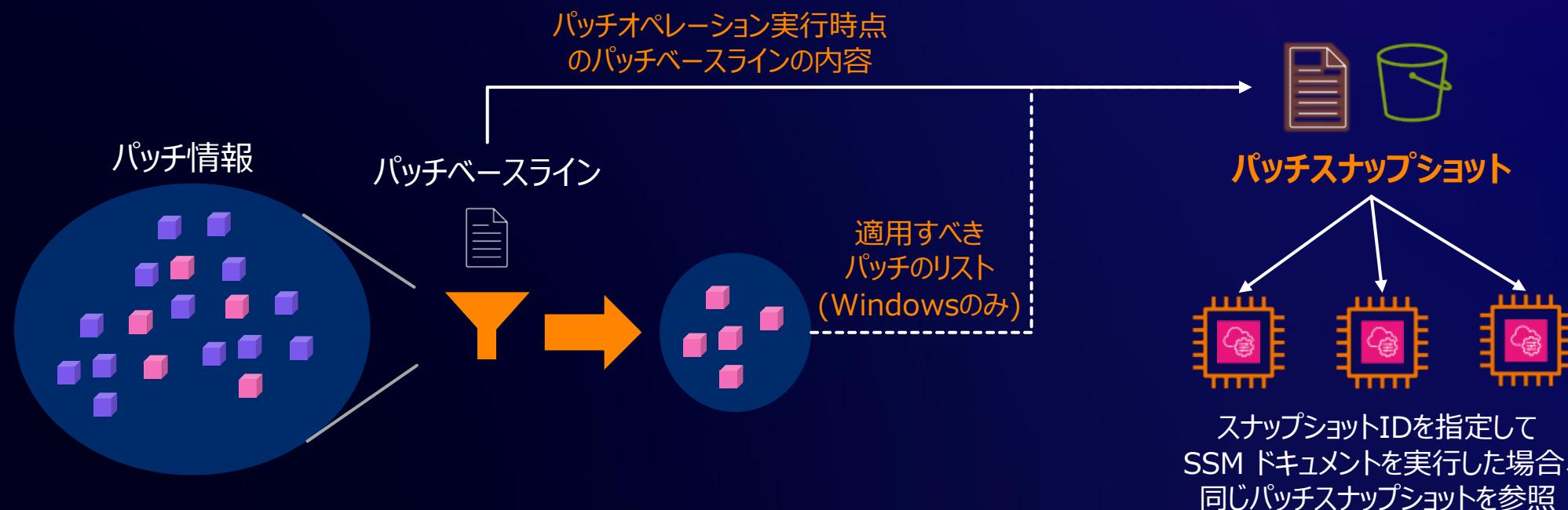
ルール名	状態	スケジュール	説明
AWS-SystemManager-PatchManager-PatchReport-weekly-patch-report	Enabled	rate(7 days)	Schedule recurring patch reporting

- オンデマンドまたはスケジュールでのレポート出力 (S3への CSVファイル出力) が可能
- レポート出力は Automation ランブック (AWS-ExportPatchReportToS3) が実行される

TIPS

パッチスナップショット (1/2)

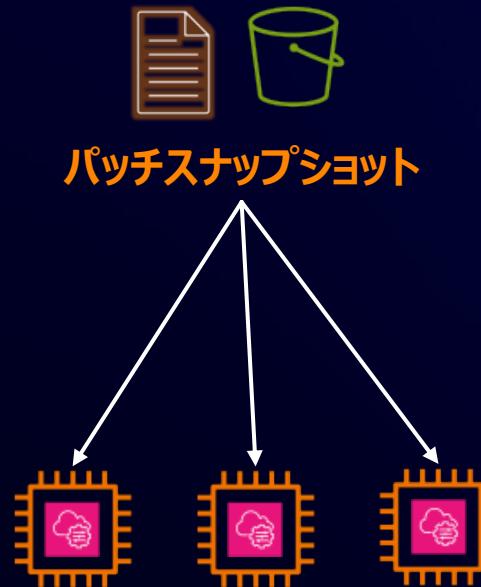
- ・ パッチオペレーション実行時点のパッチベースラインのスナップショット
- ・ 一時的に Systems Manager サービスが管理する S3 バケットへ保存される
- ・ 同じスナップショット ID を指定して SSM ドキュメントを実行すると、同じパッチスナップショットを使用する



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-aws-runpatchbaseline.html#patch-manager-aws-runpatchbaseline-parameters-snapshot-id

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

パッチスナップショット (2/2)



GetDeployablePatchSnapshotForInstance API
& 署名付きURLによるS3アクセス

- AWS-RunPatchBaseline や AWS-RunPatchBaselineWithHooks SSM ドキュメントがスナップショット ID パラメータをサポート
- Maintenance Windows から SSM ドキュメントを実行する場合は自動的にスナップショット ID が設定されるため考慮不要
- パッチスナップショットの取得には S3 署名付きURLが使用される（長期間のスナップショットの保存は不向き）

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-aws-runpatchbaseline.html

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-aws-runpatchbaselinewithhooks.html

InstallOverrideList

- ・ パッチベースラインでfiltrタされたパッチのリストを上書きできる YAML 形式のリスト
- ・ S3 に YAML ファイルを保存しておき、ファイルのパスをパラメータとして指定する
- ・ インストールするパッチを詳細に指定することができるが、Scan オペレーションでは使用できない

< InstallOverrideList のサンプル書式 >

```
patches:  
  -  
    id: 'kernel.x86_64'  
  -  
    id: 'bind*.x86_64'  
    title: '32:9.8.2-0.62.rc1.57.amzn1'  
  -  
    id: 'glibc*'  
  -  
    id: 'dhclient*'  
    title: '*12:4.1.1-53.P1.28.amzn1'  
  -  
    id: 'dhcp*'  
    title: '*10:3.1.1-50.P1.26.amzn1'
```



InstallOverrideList のサンプル書式はドキュメントも参照

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-aws-runpatchbaseline.html#patch-manager-aws-runpatchbaseline-parameters-installoverridelist

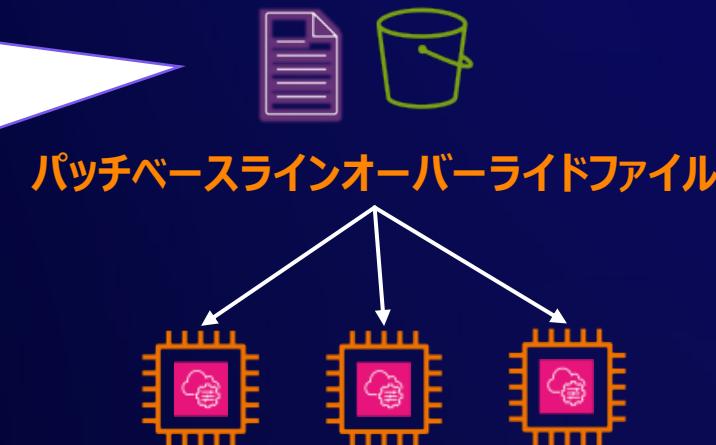
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

BaselineOverride

- ・ パッチベースラインの設定を上書きすることができる
- ・ S3 に JSON ファイルとして格納しておき、ファイルのパスをパラメータとして指定する
- ・ パッチポリシーをセットアップした環境ではこのパラメータが使用されている。これにより、クロスアカウント/クロスリージョンで同じ設定のパッチベースラインを適用できる
- ・ パッチベースラインオーバーライドファイルのサンプルや生成方法はドキュメント参照

<パッチベースラインオーバーライドファイル>

```
[  
  {  
    "ApprovalRules": {  
      "PatchRules": [  
        {  
          "ApproveAfterDays": 0,  
          "ComplianceLevel": "UNSPECIFIED",  
          "EnableNonSecurity": false,  
          "PatchFilterGroup": {  
            "PatchFilters": [  
              {  
                "Key": "PRODUCT",  
                "Values": [  
                  "*"  
                ]  
              },  
              :  
            ]  
          }  
        }  
      ]  
    }  
  }  
]
```



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-baselineoverride-parameter.html

Security Hub との連携

- Patch Manager は Security Hub との統合をサポート
- Patch Manager は、マネージドノードが非準拠であることを検出した場合に Security Hub へ検出結果を転送
- 検出結果にはパッチのサマリー結果が含まれる



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-security-hub-integration.html

異なる環境間で同じパッチを適用したい場合

開発環境と本番環境など、複数の環境に対して異なるタイミングで同じパッチを適用する場合、以下の方法がある

パッチベースラインの「自動承認」を使用

自動承認の遅延日数や期限日を指定し、パッチがリリースまたは最後に更新されてから待機する日数や期限日を指定できる

- Ubuntu や Debian は自動承認オプションは未サポート
- Amazon Linux のパッケージのリリース日と更新日の計算方法については以下のドキュメントも参照
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-release-dates.html
- Windows Server の場合、更新プログラムの置き換えや更新日時を指定しないアプリケーションパッチの提供が発生する場合がある
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-selecting-patches.html (Windows Server タブの内容を参照)

InstallOverrideList オプションを使用

適用したいパッチのリストを明示的に指定する

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-override-lists.html

料金

Patch Manager の料金

- ・ パッチオペレーション

タスク	Amazon EC2 インスタンス	ハイブリッド環境のインスタンス
OSのパッチング	追加料金なし	追加料金なし
Linux アプリケーションのパッチング	追加料金なし	追加料金なし
Microsoft アプリケーションのパッチング	追加料金なし	アドバンスドオンプレミスインスタンスティアが必要。 (アドバンスドオンプレミスインスタンスごとに時間あたり 0.00695 USD)

- ・ パッチレポート

レポート作成時は Systems Manager Automation が実行されるため、Systems Manager Automation の料金が発生する

<https://aws.amazon.com/jp/systems-manager/pricing/>

まとめ

まとめ

Systems Manager Patch Manager は、マネージドノードにパッチを適用するプロセスを自動化

- 自動承認のルールを「パッチベースライン」として定義
 - 承認済みおよび拒否済みパッチの選択可能なリストのほか、リリースからの経過日数や特定日以前のパッチを自動承認することができる
- 定期的なパッチのスキャンとインストール
 - Maintenance Windows , State Manager , EventBridge Scheduler を使用してスケジュール実行が可能
- 緊急度の高いパッチへの迅速な対応も可能
- パッチのレポートによりコンプライアンス状況を一元的に把握

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
- ・ 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>



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

内容についての注意点

- ・ 本資料では資料作成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。AWS のサービスは常にアップデートを続けているため、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
- ・ 技術的な内容に関しては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しては、[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)

Thank you!