



# AWS Black Belt Online Seminar

# AWS Systems Manager

## Quick Setup 編

渡邊 良臣

Solutions Architect

2023/12

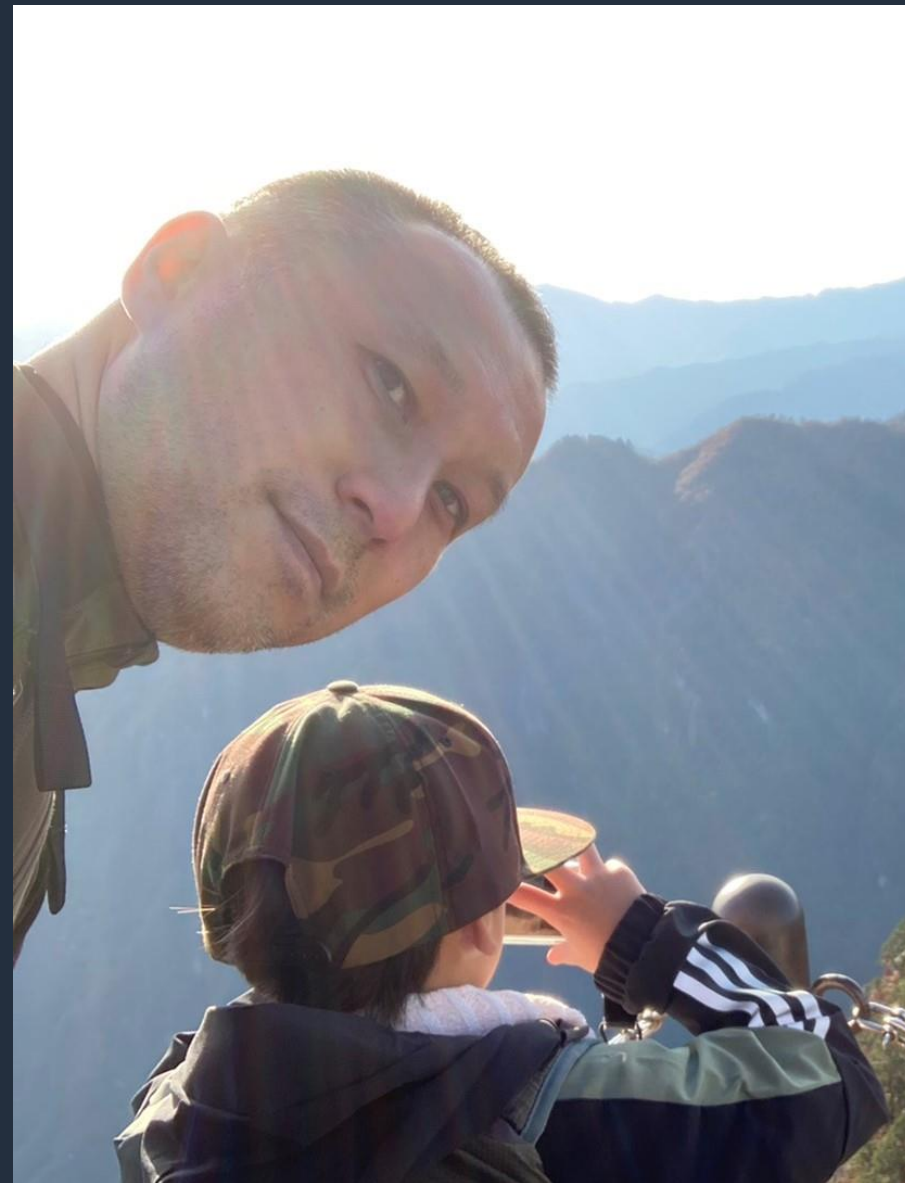
# 自己紹介

## 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



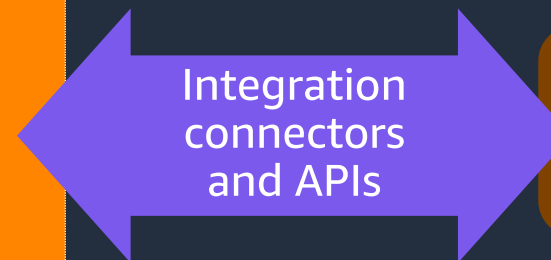
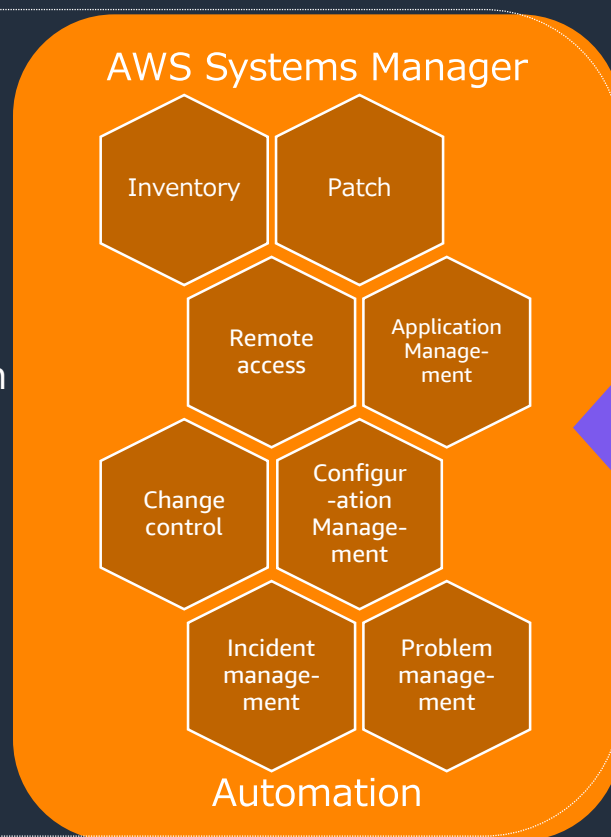
**Amazon EventBridge**  
Notification and remediation



**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

Cloud On-premises Edge

(\* ) 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

# 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

aws サービス [Alt+S] 東京

## AWS Systems Manager

管理とガバナンス

### 高速セットアップ ①

- ▼ 運用管理
  - エクスペローラー
  - OpsCenter
  - CloudWatch ダッシュボード
  - インシデントマネージャー
- ▼ アプリケーション管理
  - アプリケーションマネージャー
  - AppConfig
  - パラメータストア
- ▼ 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

## 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。

### 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。

ap-northeast-1

使用開始

### その他のリソース

- ドキュメント
- よくある質問
- サポートフォーラム

### 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。

© 2023, Amazon Web Services, Inc. またはその関連会社

## 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。

### ホームリージョンを選択 ②

ap-northeast-1

使用開始

③

# 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](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](https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_getting-started_concepts.html)

# Quick Setup の設定画面 (作成)

AWS Systems Manager

Systems Manager > Quick Setup

## Quick Setup

設定タイプ

以下の結果をフィルタリング

<b>Host Management</b> Systems Manager の使用 設定ステータス <input 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 機能を有効にします。 <input type="button" value="作成"/>	<b>Config Recording</b> AWS Config の使用 設定ステータス <input type="radio"/> 設定なし 説明 選択した AWS リソースタイプへの必要を強制し記録できるようにします。記録されたデータの配信オプションと通知オプションを設定します。 <input type="button" value="作成"/>	<b>Conformance Packs</b> AWS Config の使用 設定ステータス <input 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できる AWS Config ルールと修復アクションを集めたものです。 <input type="button" value="作成"/>
<b>Patch Manager</b> Systems Manager の使用 設定ステータス <input 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のパッチ適用を自動化します。 <input type="button" value="作成"/>	<b>Change Manager</b> Systems Manager の使用 設定ステータス <input type="radio"/> 設定なし 説明 Change Manager が組織全体で管理オペレーションを呼び出すために必要な IAM ロールを設定します。 <input type="button" value="作成"/>	<b>DevOps Guru</b> DevOps Guru の使用 設定ステータス <input 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役立つ、機械学習を活用した DevOps Guru サービスを有効にします。 <input type="button" value="作成"/>
<b>Distributor</b> Systems Manager の使用 設定ステータス <input 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。 <input type="button" value="作成"/>	<b>Resource Scheduler</b> AWS 予約インスタンスを利用 設定ステータス <input 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。 <input type="button" value="作成"/>	<b>OpsCenter</b> Powered by Systems Manager 設定ステータス <input type="radio"/> 設定なし 説明 Enables OpsCenter to centrally manage operational issues (OpsItems) across multiple AWS accounts. <input type="button" value="作成"/>
<b>Default Host Management Configuration</b> Systems Manager の利用 設定ステータス <input type="radio"/> 設定なし 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管理構成を有効にします。 <input type="button" value="作成"/>	<b>Resource Explorer</b> AWS Resource Explorer を利用 設定ステータス <input type="radio"/> 設定なし 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検出するために必要なリソースを設定します。 <input type="button" value="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

# Quick Setup の設定画面 (削除)

The screenshot displays the AWS Systems Manager Quick Setup console. The interface includes a left-hand navigation pane, a top navigation bar, and a main content area. Annotations 1 through 5 highlight specific elements:

- ①: 高速セットアップ (Quick Setup)
- ②: 設定 (Settings)
- ③: 設定タイプ (Setting Type)
- ④: アクション (Action)
- ⑤: 設定を削除 (Delete Setting)

The main content area shows a table of settings with the following columns: 設定タイプ (Setting Type), デプロイタイプ (Deploy Type), 組織単位 (Organization), リージョン (Region), デプロイのステータス (Deploy Status), 関連付けのステータス (Associated Status), and 最終更新日 (Last Updated). The table lists various settings such as Change Manager, Config Recording, Conformance Packs, Default Host Management Configuration, DevOps Guru, Distributor, and Host Management.

設定タイプ	デプロイタイプ	組織単位	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	ap-northeast-1, us-east-2	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, 3 Pending	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



AWS Identity and Access Management (IAM)

② IAM ロールの作成



ホームリージョン (※)



AWS CloudFormation

③ スタックセットの作成



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



(※) ホームリージョン : スタックセットが作成されるリージョン



# 処理概要

項番	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。



このスクリーンショットは、AWS Systems Managerの「設定」ページの詳細表示を示しています。左側のナビゲーションメニューには「設定タイプ」のリストがあります。中央には「設定」の検索ボックスと「詳細を表示」、「アクション」、「作成」のボタンがあります。下部には設定の詳細なテーブルが表示されています。

設定タイプ	デプロイタイプ	組織単位	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	QuickSetup	該当なし (グローバル)	SUCCEEDED	なし	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	該当なし	us-east-2, us-west-2	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 Failed 1 Pending 5 Success	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](#)

### 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 [こちら](#) 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 [こちら](#) が有効になります。

[CloudWatch エージェントの基本設定](#) と [Amazon CloudWatch の料金](#) 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://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](#)

### 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 [こちら](#) 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 [こちら](#) が有効になります。

[CloudWatch エージェントの基本設定](#) と [Amazon CloudWatch の料金](#) 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://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-inventory.html)

[https://www.youtube.com/watch?v=2\\_6YcNmNFcg](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](#)

### 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 [こちら](#) 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 [こちら](#) が有効になります。

[CloudWatch エージェントの基本設定](#) と [Amazon CloudWatch の料金](#) 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](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）

## 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](#)

### 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  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  が有効になります。

[CloudWatch エージェントの基本設定](#) と [Amazon CloudWatch の料金](#) に含まれるメトリクスの詳細をご覧ください。

CloudWatch エージェントをインストールして Basic レベルの設定を行う。

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](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](#)

### 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。

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。

### 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  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  が有効になります。

[CloudWatch エージェントの基本設定](#) と [Amazon CloudWatch の料金](#) に含まれるメトリクスの詳細をご覧ください。

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://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](#)

### 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 [こちら](#) 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](#) 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](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](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](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

**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か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。

非管理アカウントで「現在のリージョン」を選択した場合のターゲット選択は、リソースグループなどの 4 つから選択する事が可能。

**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か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。

**ターゲットリージョン**  
この設定をデプロイするリージョンを選択します。

非管理アカウントで「リージョンを選択」した場合のターゲット選択は、「すべてのインスタンス」か「タグ」による選択のみとなる。

# 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

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。

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。

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](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

Quick Setup

設定タイプ

以下の結果をフィルタリング

- Host Management: Systems Manager の使用
- Config Recording: AWS Config の使用
- Conformance Packs: AWS Config の使用
- Patch Manager: Systems Manager の使用
- DevOps Guru: DevOps Guru の使用
- Distributor: Systems Manager の使用
- Resource Scheduler: AWS ソリューションを利用

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

Quick Setup

設定タイプ

以下の結果をフィルタリング

- Host Management: Systems Manager の使用
- Config Recording: AWS Config の使用
- Conformance Packs: AWS Config の使用
- Patch Manager: Systems Manager の使用
- Change Manager: Systems Manager の使用
- DevOps Guru: DevOps Guru の使用
- Distributor: Systems Manager の使用
- Resource Scheduler: AWS ソリューションを利用
- OpsCenter: Powered by Systems Manager
- Resource Explorer: AWS Resource Explorer を利用



# 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)

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。



### 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 [🔗](#)

# 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](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**

**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

**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 を使用して通知を送信します。

- 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 で記録する対象を選択する。**

**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。**

**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。**

**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) ▼

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。

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。

# Config Recording 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

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

④ 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。

「デフォルト」を選択すると、1回だけ実行される。

**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

スケジュール頻度

- 無効 ▲
- 毎日
- 7日ごと
- 30日ごと
- 無効 ▼ ✓

Quick Setup は、適用する設定に加えられた変更を修復できます。

「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

### 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。

管理アカウントにて設定する場合は、組織を  
対象としたターゲットが選択可能。

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。

## 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。

非管理アカウントにて設定する場合は、  
ターゲットとしてリージョンが選択可能。

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。

# 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](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 ✕



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

 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

**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。

<input checked="" type="radio"/> <b>組織全体</b> 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。	<input type="radio"/> <b>カスタム</b> この設定をデプロイするリージョンを選択します。	<input type="radio"/> <b>現在のアカウント</b> 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。
--	--	--

管理アカウントにて設定する場合のターゲット。「カスタム」は、すべての組織単位を対象として、リージョンを選択したい時に選択する。

## 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。

<input checked="" type="radio"/> <b>現在のリージョン</b> 現在のリージョンに設定をデプロイします。	<input type="radio"/> <b>リージョンを選択</b> この設定をデプロイするリージョンを選択します。
--	--

非管理アカウントにて設定する場合は、ターゲットとしてリージョンが選択可能。

# 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。

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](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](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)

設定名

パッチポリシーを識別するための名前を入力する。

設定名には最大 113 文字を使用できます。設定名では大文字と小文字が区別されます。

有効な文字: A~Z、a~z、0~9、\_、スペース、-(ハイフン)



# 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

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。

「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。

「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](#)

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

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。

最初の CRON 間隔までターゲットのスキャンを待ちます。

# 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る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

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。

**パッチインストール後の再起動を管理する。**

「スキャンとインストール」を選択すると「インストールスケジュール」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「カスタムスキャンスケジュール」と同様に「日単位」と「カスタム CRON 式」を選択可能。

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。

「カスタムインストールスケジュール」を選択した場合は「カスタムスキャンスケジュール」と同様に「日単位」と「カスタム CRON 式」を選択可能。

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。

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るため、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。

ホームリージョンで作成したパッチベースラインを選択可能。

**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るため、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 <a href="#">🔗</a>
Amazon Linux	AWS-AmazonLinuxDefaultPatchBa... ▼	pb-0221829c157d721d8
Amazon Linux 2	AWS-AmazonLinux2DefaultPatchB... ▲	pb-00fda5699d1ae3942
Amazon Linux 2022	Q	pb-067dab85430494167
CentOS	AWS-AmazonLinux2DefaultPatchBaseline ✓ Default Patch Baseline for Amazon Linux 2 Provided by AWS.	pb-0b4917141375bc4b5
Debian Server	カスタムベースライン	pb-0d5f3f8560fc606e3
Oracle Linux	Test-BlackBelt-Baseline	pb-04ed5d5c38572bb74
Raspberry Pi OS	Test-BlackBelt-Baseline	pb-04e6dbcacfd1dc4ef
Red Hat Enterprise Linux (RHEL)	AWS-RedHatDefaultPatchBaseline ▼	pb-0ad5cb7136a2984d

独自に作成したパッチベースラインを利用する場合。


# 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

ログストレージにパッチ適用

S3 バケットに出力を書き込む  
Simple Storage Service (Amazon S3) バケットにパッチ適用オペレーションログを保存します。コンソールでのパッチ適用オペレーションの出力は 48,000 文字後に切り捨てられます。

S3 URI  
パッチ適用ログを保存する S3 バケットを選択します。現在のリージョンのバケットのみ選択できます。

🔍  表示  S3 を参照

📘 管理アカウントには読み取りアクセス許可が必要で、ローカルアカウントには S3 バケットに対する書き込みアクセス許可が必要です。

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、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

ログストレージにパッチ適用

S3 バケットに出力を書き込む  
Simple Storage Service (Amazon S3) バケットにパッチ適用オペレーションログを保存します。コンソールでのパッチ適用オペレーションの出力は 48,000 文字後に切り捨てられます。

S3 URI  
パッチ適用ログを保存する S3 バケットを選択します。現在のリージョンのバケットのみ選択できます。

🔍  表示  S3 を参照

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**  
別のリージョンに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。
- リソースグループを指定**  
現在のアカウント内のリソースグループ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。

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。

# 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か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。

**ターゲットリージョン**  
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。

すべてのリージョン

- us-east-1 (N. Virginia)
- us-east-2 (Ohio)
- us-west-1 (N. California)
- us-west-2 (Oregon)
- sa-east-1 (Sao Paulo)
- eu-central-1 (Frankfurt)
- eu-west-1 (Ireland)
- eu-west-2 (London)
- eu-west-3 (Paris)
- eu-north-1 (Stockholm)
- ca-central-1 (Central)
- ap-south-1 (Mumbai)
- ap-northeast-2 (Seoul)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- ap-northeast-1 (Tokyo)

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。

「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。

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。

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-quicksetup-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](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](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

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

通知用に SNS トピックが作成される。

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、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。

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](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

Amazon DevOps Guru > インサイト: 事故的 > API Gateway ListRestApiMonitorOper 5xx errors caused by errors in Lambda function ScanFunctionMonitorOper affecting application availability

### API Gateway ListRestApiMonitorOper 5xx errors caused by errors in Lambda function ScanFunctionMonitorOper affecting application availability

インサイトの概要

説明  
At March 26, 2023 21:05 GMT, API Gateway ListRestApiMonitorOper had 5XX errors caused by errors in Lambda function ScanFunctionMonitorOper. Check the recommendations to see how to resolve the issue.

インサイトの重要度  
Severity  
ステータス  
△ 検知中  
影響を受けるアプリケーション

開始時刻  
3月 26, 2023 21:05 UTC  
終了時刻  
-  
Opitem ID  
-

最終更新時刻  
3月 26, 2023 21:07 UTC  
Opitem ID  
-

グラフ化された異常 (10) 3月 26, 21:05-今 検知  
Amazon DevOps Guru は、異常の発生を検出し、結果を視覚的に分かりやすく表示します。  
メトリクス名、アプリケーション、サービス名でメトリクスを検索

Anomalous metrics (10)

1H 3H 12H 1D 3D 1W 2W 1M 2M 3M 6M 1Y 2Y 3Y 5Y 10Y 20Y 30Y 40Y 50Y 60Y 70Y 80Y 90Y 100Y

AWS/Lambda:Invocations Count  
21:03 21:01 21:00 21:05 21:10 21:15

AWS/ApiGateway:Count Count  
21:03 21:01 21:00 21:05 21:10 21:15

AWS/DynamoDB:SuccessfulRequestLatency Milliseconds  
21:03 21:01 21:00 21:05 21:10 21:15

AWS/DynamoDB:ThrottledRequests Count  
21:03 21:01 21:00 21:05 21:10 21:15

→ Invocations 異常  
サービス名  
AWS/Lambda  
リソース名  
アプリケーション

ディメンション  
FunctionName:ScanFunctionMonitorOper  
リソース名  
アプリケーション

→ Count 異常  
サービス名  
AWS/ApiGateway  
リソース名  
アプリケーション

ディメンション  
ApiName:ListRestApiMonitorOper  
リソース名  
アプリケーション

→ SuccessfulRequestLatency 異常  
サービス名  
AWS/DynamoDB  
リソース名  
アプリケーション

ディメンション  
Operation:Scan  
統計  
Maximum

→ ThrottledRequests 異常  
サービス名  
AWS/DynamoDB  
リソース名  
アプリケーション

ディメンション  
Operation:Scan  
統計  
Sum

1H 3H 12H 1D 3D 1W 2W 1M 2M 3M 6M 1Y 2Y 3Y 5Y 10Y 20Y 30Y 40Y 50Y 60Y 70Y 80Y 90Y 100Y

AWS/DynamoDB:ReadThrottleEvents  
AWS/Lambda:Errors

特定された問題をインサイトとして表示。

インサイトに関する推奨事項。

### レコメンドーション (5)

このインサイトの発生に対処するために実施することが推奨される更新を表示します。

[Resolve errors in Lambda ScanFunctionMonitorOper](#)  
Investigate the errors by checking the logs of the Lambda function ScanFunctionMonitorOper.

DevOps Guru がこれを推奨しているのはなぜですか?  
Lambda の Errors メトリクスが高いしきい値を超えました。ApiGateway の 5XXError メトリクスが高いしきい値を超えました。

関連メトリクス (2)  
Errors  
Lambda ScanFunctionMonitorOper  
5XXError  
ApiGateway ListRestApiMonitorOper

[Amazon DynamoDB のスロットリングのトラブルシューティング](#)  
DynamoDB テーブルの読み取りオペレーション、書き込みオペレーション、またはその両方のスロットリングが行われています。スロットリングイベントの修正方法については、このリンクをご確認ください。

DevOps Guru がこれを推奨しているのはなぜですか?  
AWS::DynamoDB::TableName の ThrottledRequests メトリクスが高いしきい値を超えました。AWS::Lambda::FunctionName の Duration メトリクスが高いしきい値を超えました。

関連メトリクス (3)  
ReadThrottleEvents  
ThrottledRequests  
さらにリソースを表示  
Duration  
AWS::Lambda::FunctionName ScanFunctionMonitorOper

[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](#)  
DynamoDB リクエストの応答時間が長くなっています。リクエストのレイテンシーを減らす方法については、このリンクをご確認ください。

DevOps Guru がこれを推奨しているのはなぜですか?  
DynamoDB の SuccessfulRequestLatency メトリクスが高いしきい値を超えました。

関連メトリクス (1)  
SuccessfulRequestLatency

[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](#)  
Lambda 関数が多数のエラーをスローしています。一般的な Lambda エラー、その原因、および緩和戦略については、このリンクをご確認ください。

DevOps Guru がこれを推奨しているのはなぜですか?  
Lambda の Errors メトリクスが高いしきい値を超えました。

関連メトリクス (1)  
Errors  
Lambda ScanFunctionMonitorOper

[Amazon API Gateway の SXX エラーのトラブルシューティング](#)  
API Gateway で多数の SXX エラーがスローされています。一般的な API Gateway のエラーについては、[ゲートウェイレスポンスのタイプ] (https://docs.aws.amazon.com/apigateway/latest/developerguide/supported-gateway-response-types.html) を参照してください。SXX エラーをトラブルシューティングするには、[API Gateway で SXX エラーを見つける] (https://aws.amazon.com/premiumsupport/knowledge-center/api-gateway-find-5xx-errors-cloudwatch/) を参照してください。API Gateway のトラブルシューティングの詳細については、[AWS ナレッジセンター - Amazon API Gateway] (https://aws.amazon.com/premiumsupport/knowledge-center/#Amazon\_API\_Gateway) を参照してください。

DevOps Guru がこれを推奨しているのはなぜですか?  
ApiGateway の 5XXError メトリクスが高いしきい値を超えました。

関連メトリクス (1)  
5XXError  
ApiGateway ListRestApiMonitorOperprod



# 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 を利用することで、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](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](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 for a non-admin account. The 'Patch Manager' section is visible, but the 'Change Manager' option is not present. The 'Host Management', 'Config Recording', 'Conformance Packs', 'DevOps Guru', and 'Distributor' sections are visible and have '作成' (Create) buttons.

## 管理アカウントからの設定

The screenshot shows the 'Quick Setup' page for an admin account. The 'Change Manager' option is visible in the 'Patch Manager' section and is highlighted with a red box. The 'Host Management', 'Config Recording', 'Conformance Packs', 'DevOps Guru', and 'Distributor' sections are visible and have '作成' (Create) buttons.

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。

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ブ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。 [詳細はこちら](#)

**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  
ランブ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

ロールとその権限を識別するための名前を入力する。

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://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](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

デプロイするパッケージを選択する。

更新頻度 ⓘ

- 30 日ごと ▲
- 2 日ごと
- 14 日ごと
- 30 日ごと ✓
- 無効

更新頻度を指定する。

更新頻度を決定します。

# 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か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（インスタスタグ）

## インスタスタグ

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。

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 × 火曜日 × 水曜日 ×

木曜日 × 金曜日 ×

**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

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。



# Resource Scheduler 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。

「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

デプロイする OU とリージョンの指定が可能。

## 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](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](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 in the AWS Systems Manager console. The '設定タイプ' (Setup Type) search bar is empty. The grid of services includes Host Management, Config Recording, Conformance Packs, Patch Manager, DevOps Guru, and Distributor. The 'OpsCenter' option is not visible in the grid.

## 管理アカウントからの設定

The screenshot shows the 'Quick Setup' page in the AWS Systems Manager console. The '設定タイプ' (Setup Type) search bar contains the text 'OpsCenter'. The 'OpsCenter' option is highlighted with a red box and a callout. The callout contains the following 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

# 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。

123456789321

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、アグリゲーターインデックスと、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](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

AWS Systems Manager > Quick Setup

設定タイプ

Host Management  
Systems Manager の使用

Config Recording  
AWS Config の使用

Conformance Packs  
AWS Config の使用

Patch Manager  
Systems Manager の使用

DevOps Guru  
DevOps Guru の使用

Distributor  
Systems Manager の使用

Resource Scheduler  
AWS ソリューションを利用

## 管理アカウントからの設定

AWS Systems Manager > Quick Setup

設定タイプ

Host Management  
Systems Manager の使用

Config Recording  
AWS Config の使用

Conformance Packs  
AWS Config の使用

Patch Manager  
Systems Manager の使用

Change Manager  
Systems Manager の使用

DevOps Guru  
DevOps Guru の使用

Distributor  
Systems Manager の使用

Resource Scheduler  
AWS ソリューションを利用

OpsCenter  
Powered by Systems Manager

Resource Explorer  
AWS Resource Explorer を利用

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)

**アグリゲーターインデックスリージョン**  
Resource Explorer に、AWS リソースに関するメタデータを集約するインデックスを管理する

us-east-1 (N. Virginia)

上記で選択したリージョン以外のリージョンの既存のアグリゲーターインデックスを置き換えます。

アグリゲーターインデックスのリージョンを指定する。

アグリゲーターインデックスのリージョンを置き換える。

# 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](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

検索 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
<input type="radio"/> Change Manager	組織	該当なし (グローバル)	✔ SUCCEEDED	なし
<input type="radio"/> Config Recording	ローカル	us-east-2	✔ SUCCEEDED	✔ 2 Success
<input type="radio"/> Config Recording	組織	us-east-2	✔ SUCCEEDED	-
<input type="radio"/> Config Recording	組織	us-west-2	✔ SUCCEEDED	-
<input type="radio"/> Conformance Packs	ローカル	us-east-2	✔ SUCCEEDED	✔ 1 Success
<input type="radio"/> DevOps Guru	ローカル	us-east-2	✔ SUCCEEDED	❌ 1 Failed ✔ 1 Success
<input type="radio"/> DevOps Guru	組織	us-east-2	✔ SUCCEEDED	-
<input type="radio"/> DevOps Guru	組織	us-west-2	✔ SUCCEEDED	-
<input type="radio"/> Distributor	ローカル	us-east-2	✔ SUCCEEDED	✔ 5 Success
<input type="radio"/> 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](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っても便利です
- 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

# 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=PLzWGOASvSx6FlwIC2X1nObr1KcMCBBlqY>



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おります。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!**