



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

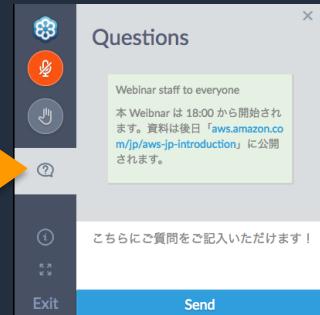
AWS Black Belt Online Seminar とは

「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



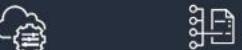
AWS
CloudTrail



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.

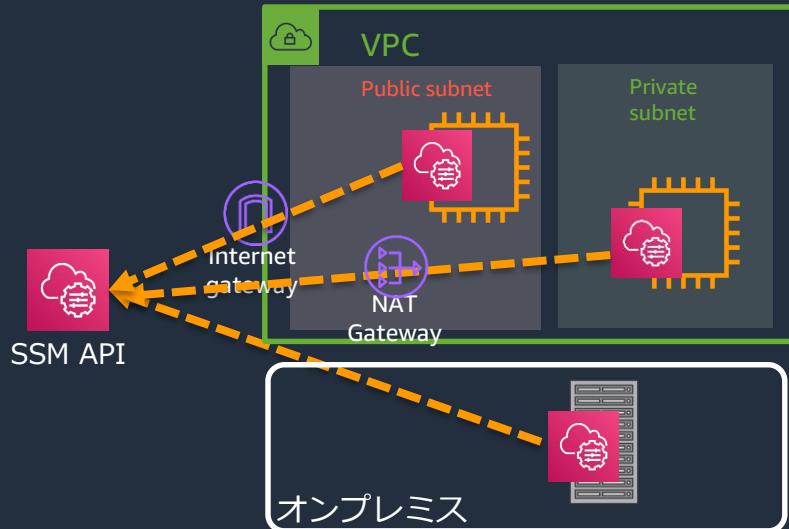


マネージドインスタンスにするために ②SSM APIへの経路確保

- 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。

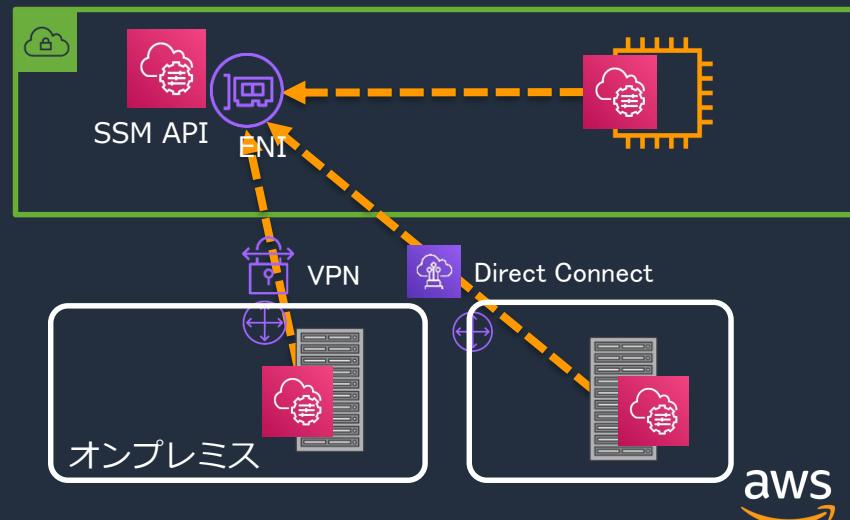
1. インターネット経由

- 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



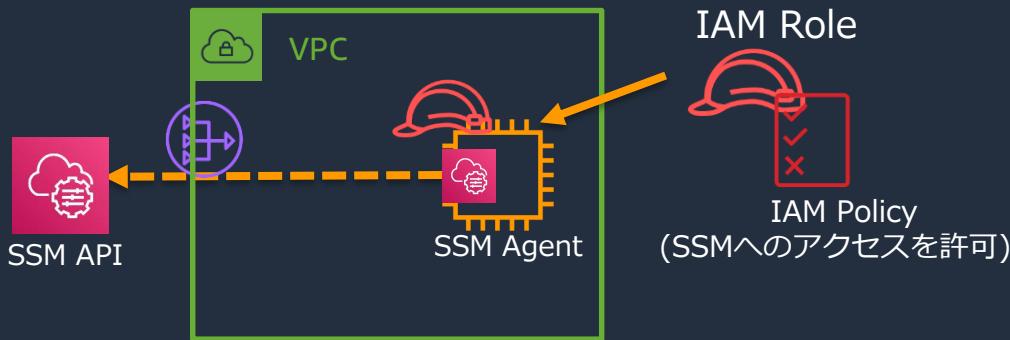
2. VPC エンドポイント経由

- 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ことを推奨



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 dashboard with "Quick Setup" highlighted.
- Middle Panel (Main View):** Titled "Systems Manager Quick Setup". It asks for permission roles and lists scheduled actions:
 - Permissions (Required):** Options to use the default role or choose an existing one.
 - Quick Setup options:** A list of scheduled actions:
 - Update Systems Manager (SSM) Agent every two weeks
 - Collect inventory from your instances every 30 minutes
 - Scan instances for missing patches daily
 - Install and configure the CloudWatch agent (unchecked)
 - Update the CloudWatch agent once every 30 days (unchecked)
- Right Panel (Targets):** Titled "Targets". It specifies the target selection method:
 - Choose all instances in the current AWS account and Region (selected)
 - Specify instance tags
 - Choose instances manually

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

- 付与するロールを選択し、
Select the roles to be assigned.
- 実施するジョブを選択し、
Select the jobs to be performed.
- ターゲットを指定する。
Specify the target.

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

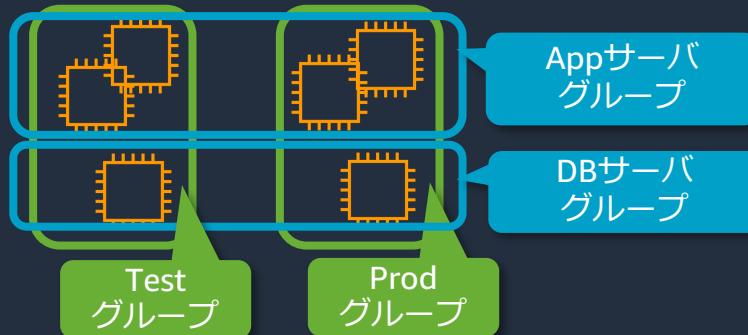
詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-quick-setup.html

© 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

ターゲット
ターゲットを選択する方法を選択します。

インスタンスタグの指定
1つ以上のタグのキーと値のペアを指定して、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する
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。

リソースグループの選択
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。

→ 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

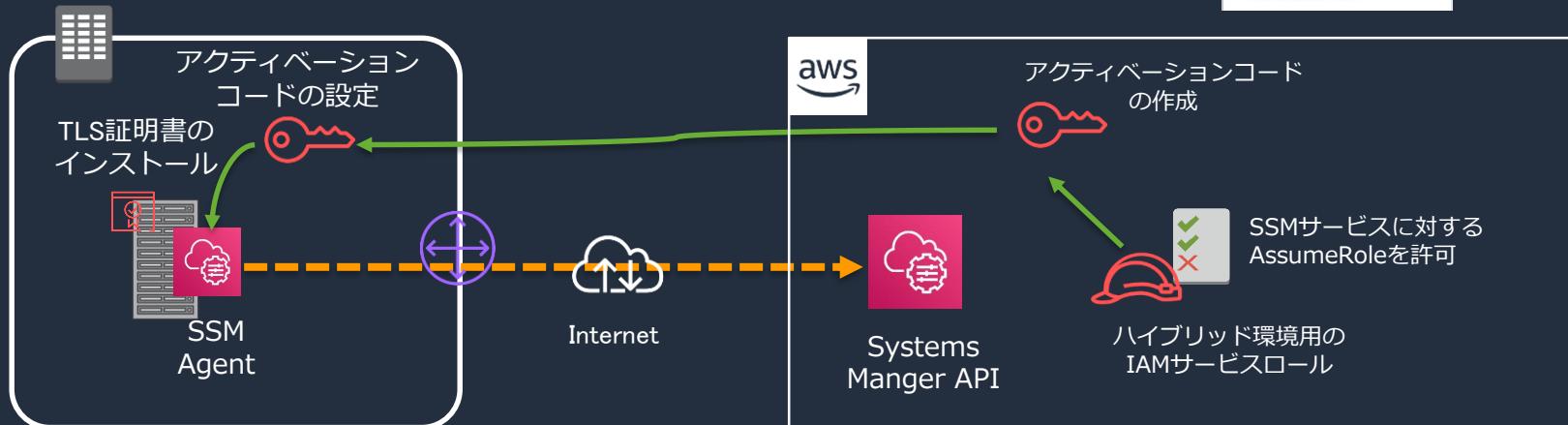
- タグエディターを使用することで、一度に複数のリソースのタグを追加・編集・削除が可能になる。

The screenshot illustrates the Tag Editor feature in the AWS Management Console. It is divided into three main sections:

- マネジメントコンソール 上部バー**: The top navigation bar of the AWS Management Console.
- 1, リソースを検索**: The search interface for finding resources. It includes fields for Regions (ap-northeast-1 selected), Resource Type (AWS::EC2::Instance selected), and Tag Options. A search button labeled "リソースを検索する" is present.
- 2, 結果からタグ管理したいリソースを選択**: The search results page titled "リソースの検索結果 (30 個の中から選択された 3 個)". It lists three EC2 instances with checkboxes next to their names. The first instance has its checkbox checked.
- 3, タグの一括編集が可能**: The Tag Editor interface. It shows the selected resource (the first EC2 instance) and allows editing its tags. Fields include "タグキー" (Environment), "タグ値 - オプション" (Prod), and "タグを削除". A "タグを追加" button is also visible.

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

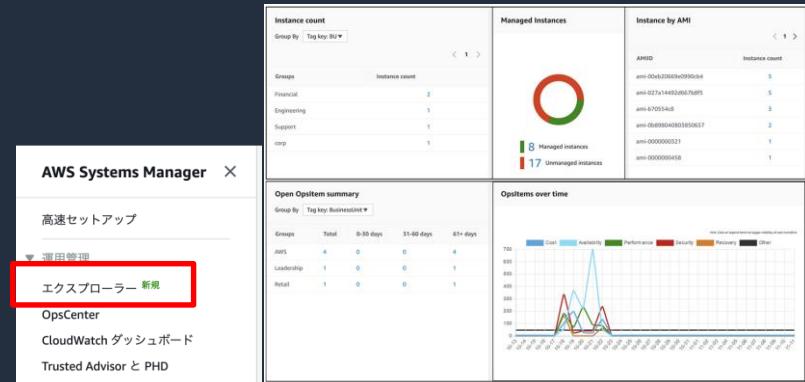
AWS SSM Explorer

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 navigation bar with the 'OpsCenter' link highlighted by a red box.

The dashboard displays the following data:

未解決	進行中	未解決	進行中
1128	0	1128	0
未解決	進行中	未解決	進行中

ソース	カウント	0~30日	31~90日	90日以上
SSM	1097	27	5	1065
EC2	30	0	18	12
RDS	1	0	1	0

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

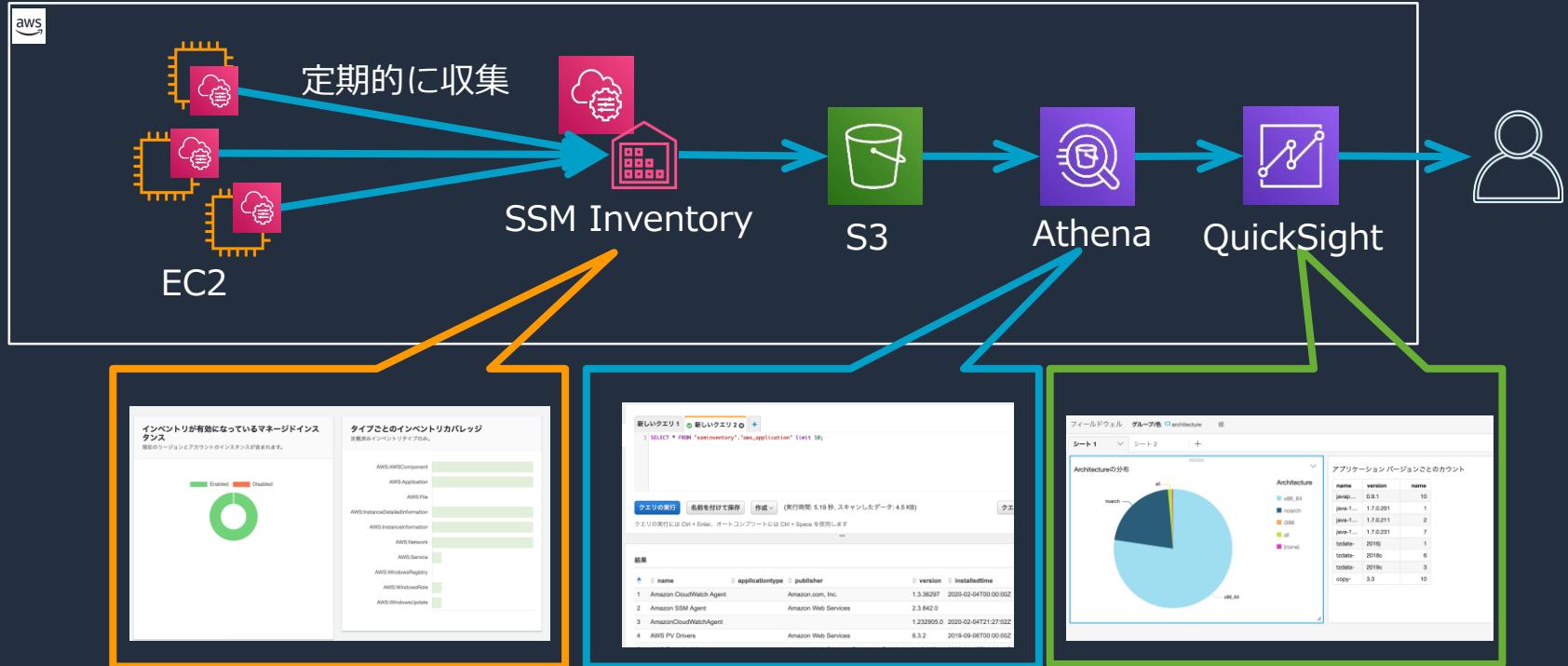
- SSM Explorer
- SSM OpsCenter
- コンプライアンス

2、インスタンスの“中身”を把握するための機能

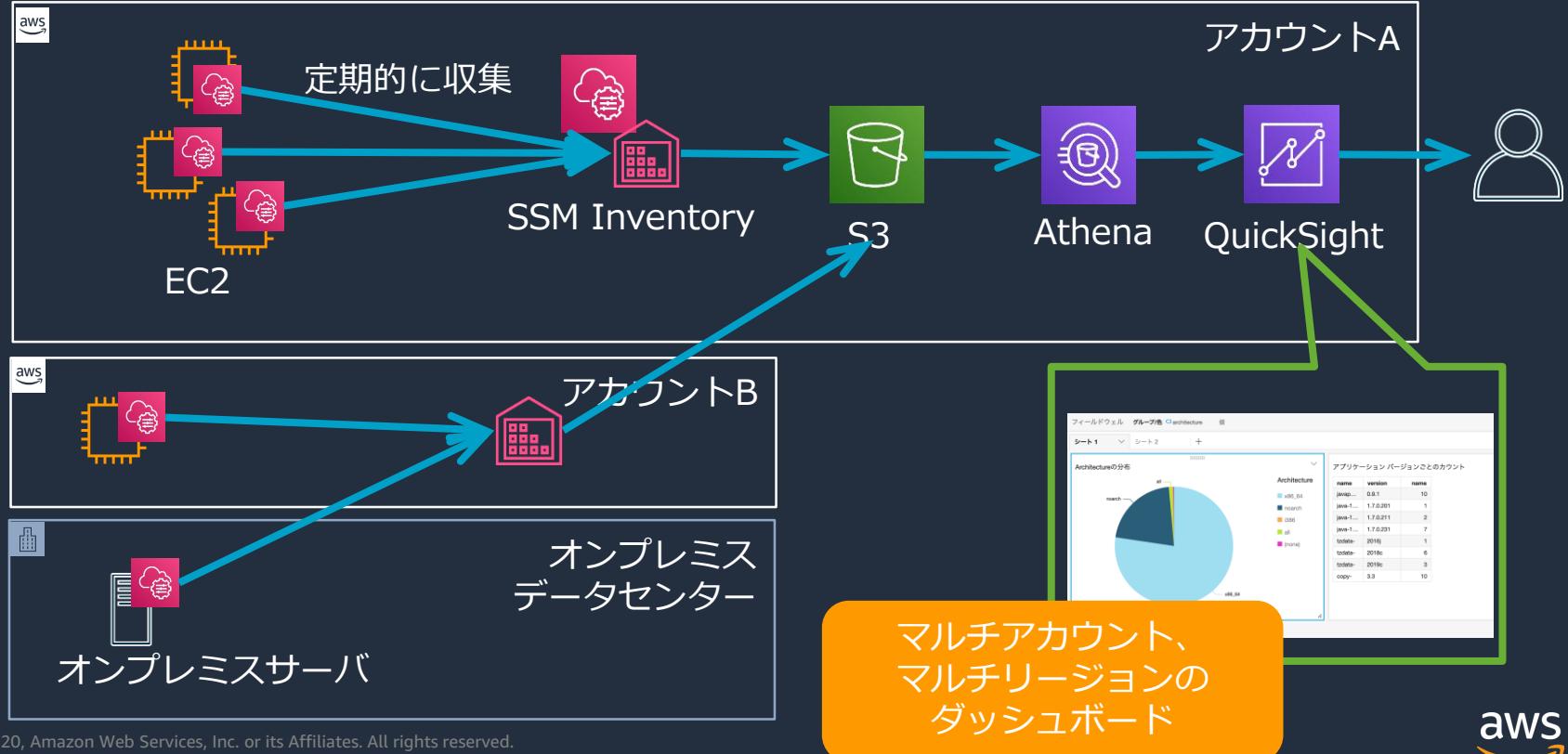
ご紹介する機能

- 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

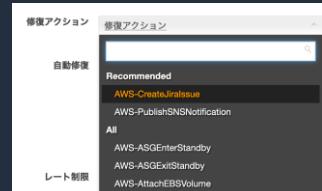
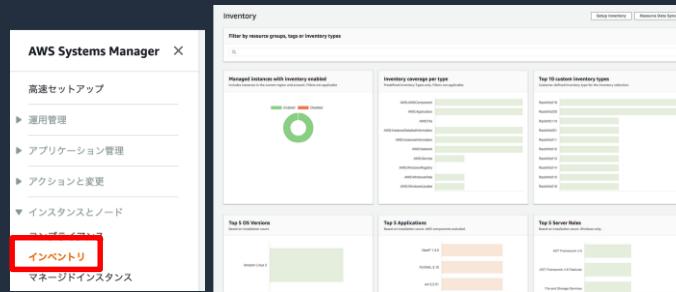


AWS SSM インベントリ



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

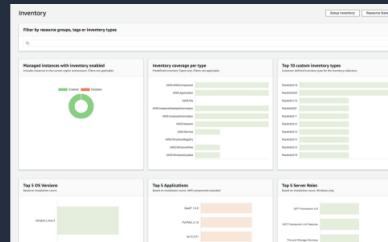
詳細は、**SSM OpsCenter**へ

- ・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 'ドキュメント' (Documents) page. It has three tabs at the top: 'Amazon が所有' (Owned by Amazon), '自己所有' (Own), and 'Shared with me'. Below these are three colored callout boxes: '事前定義ドキュメント' (Pre-defined Document) pointing to the 'Amazon が所有' tab; '自作ドキュメント' (Custom Document) pointing to the '自己所有' tab; and '共有されたドキュメント' (Shared Document) pointing to the 'Shared with me' tab. To the right, a large green callout box labeled '実体は JSON or YAML' points to a sample document content window titled 'AWS Systems Manager' which displays JSON code. A red box highlights the 'ドキュメント' tab in the navigation bar.

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 \"Ingesting dependencies and updating required tools: ${AWS_SSM_DOCUMENT_DEPENDENCIES}\""
            ]
        }
    }
]
```

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

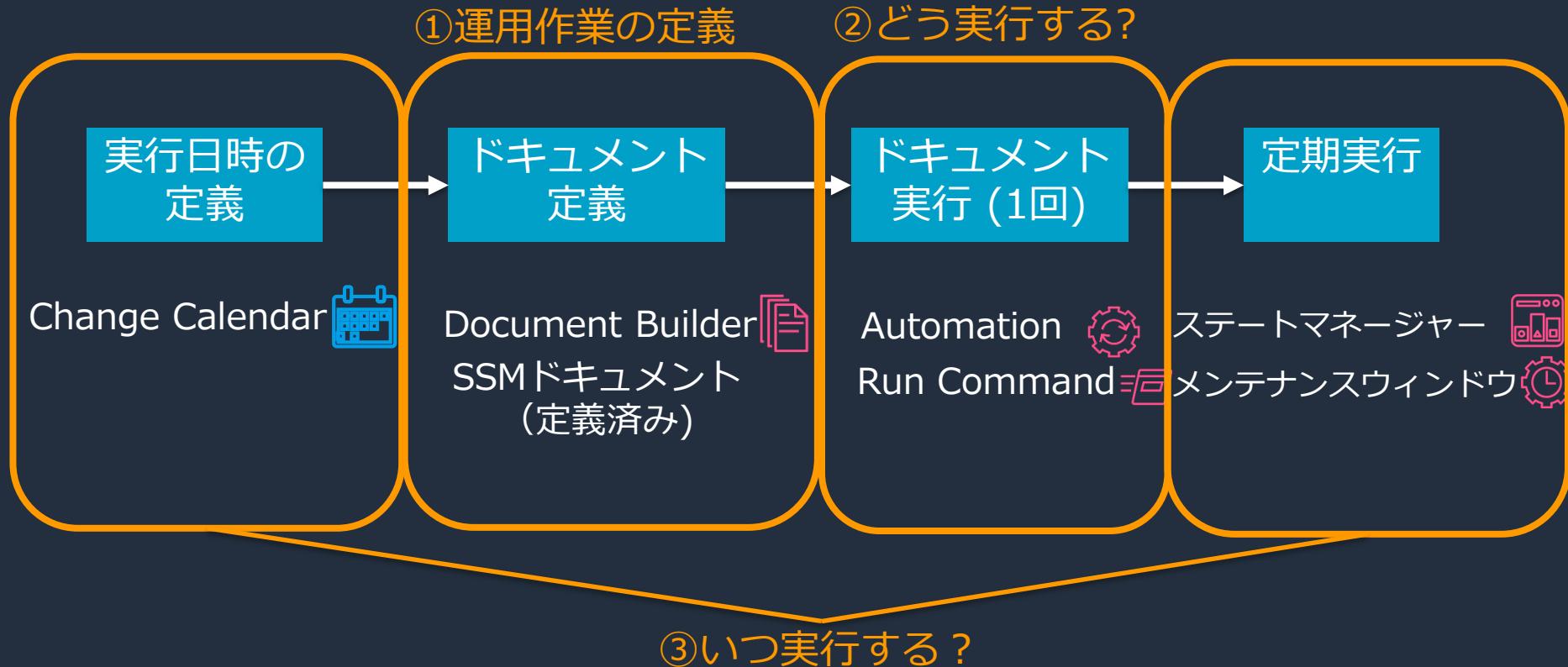


Change Calendar

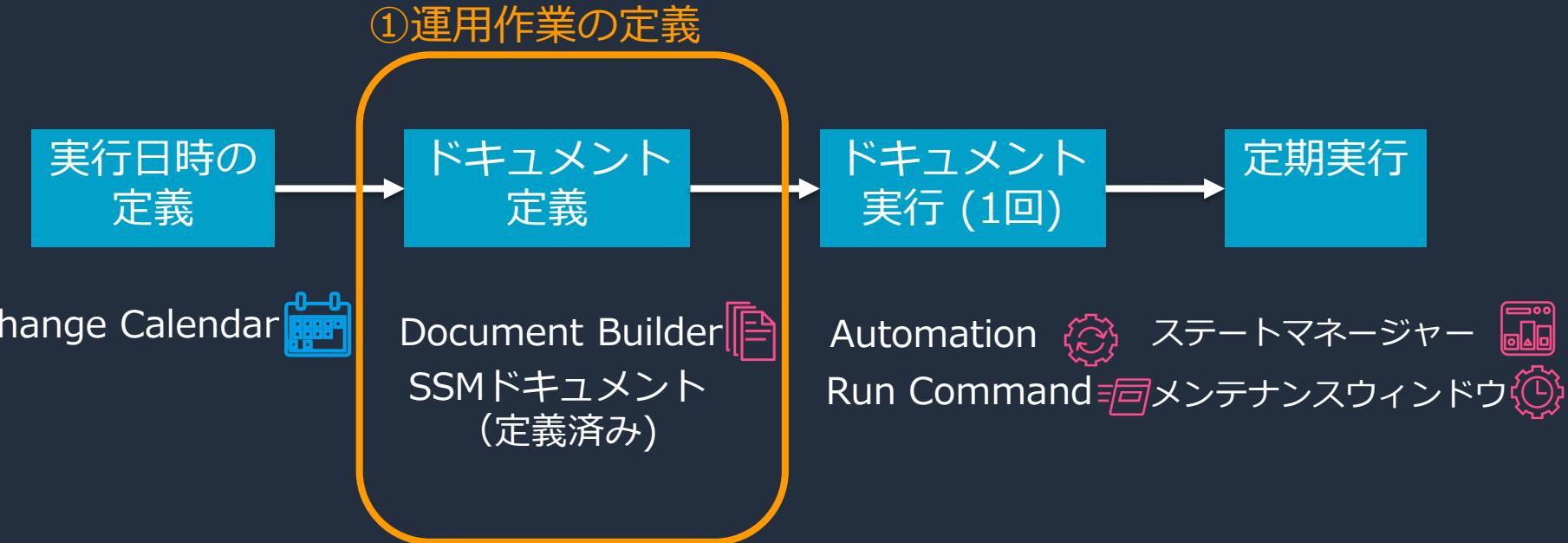
Document Builder
SSM ドキュメント
(定義済み)

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

The image contains three screenshots of the AWS Systems Manager Document Builder interface:

- Screenshot 1: Step 1: LaunchEc2Instance**

This screenshot shows the configuration for the first step of an automation document. It includes fields for Step name (LaunchEc2Instance), Action type (Run a script), and Description (This step launches an EC2 instance). It also includes sections for "What does the step do?" and "What is the Output of the step?".
- Screenshot 2: Inputs and Runtime**

This screenshot shows the "Inputs" section where you can define input variables for the action type selected. It also shows the "Runtime" section, which specifies the type of runtime function for the execution (Python3.6) and the name of the method in your code for running the function (Launch_Instance).
- Screenshot 3: Script Editor**

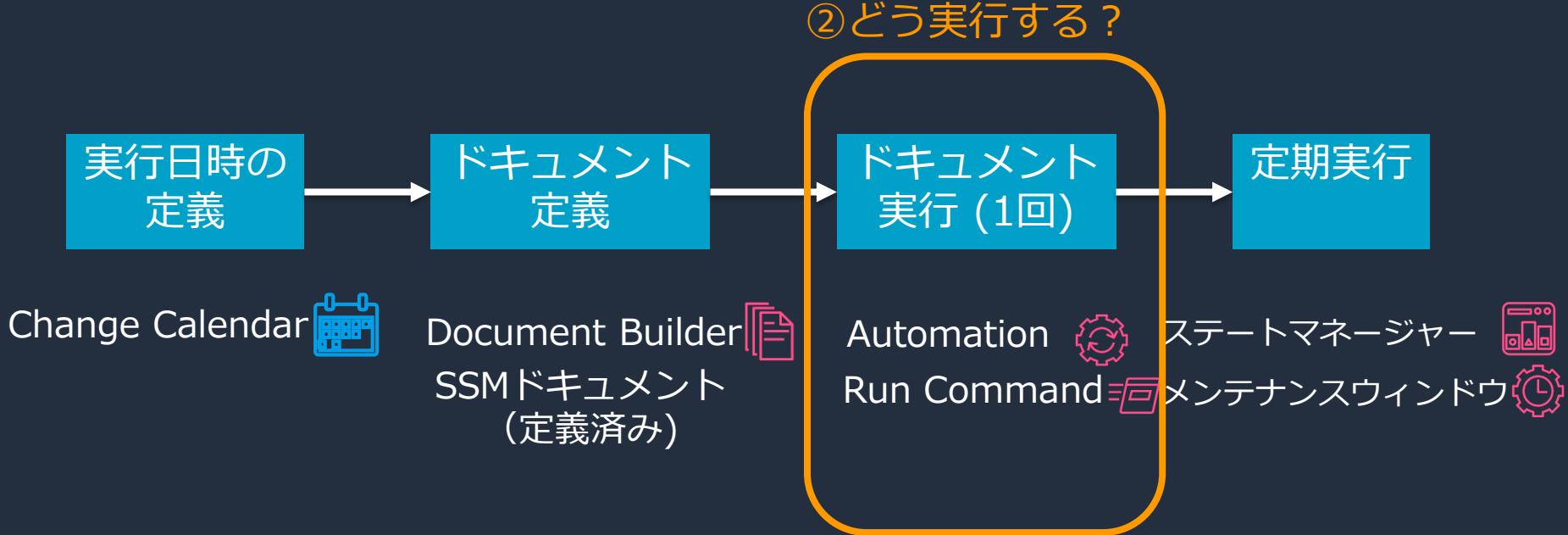
This screenshot shows the "Script" editor where the Python script for launching an EC2 instance is pasted. The script uses the Boto3 library to interact with the AWS SDK.

```
1 def launch_instance(events, context):
2     client = boto3.client('ec2')
3     ec2 = client.describe_instances()
4     image_id = events['image_id']
5     instance_type = events['instance_type']
6     min_count = 1
7     max_count = 1
8     tag_config = {'ResourceType': 'instance', 'Tags': [{"Key": "tag1", "Value": tag_value}]}
9     resp = ec2.run_instances(ImageId=image_id, InstanceType=instance_type, MinCount=min_count, MaxCount=max_count, TagSpecifications=[tag_config])
10    instance_id = resp['Instances'][0]['InstanceId']
11    print(f'[INFO] 1 EC2 instance successfully launched: {instance_id}')
12    return f'InstanceID : {instance_id}'
```

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.



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

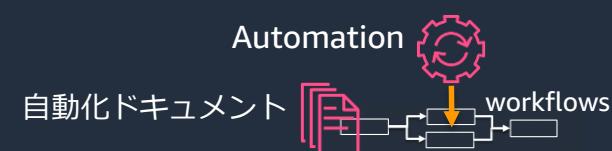
- 自動化ドキュメントを実行する
- AWSの操作もOS上での操作も



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

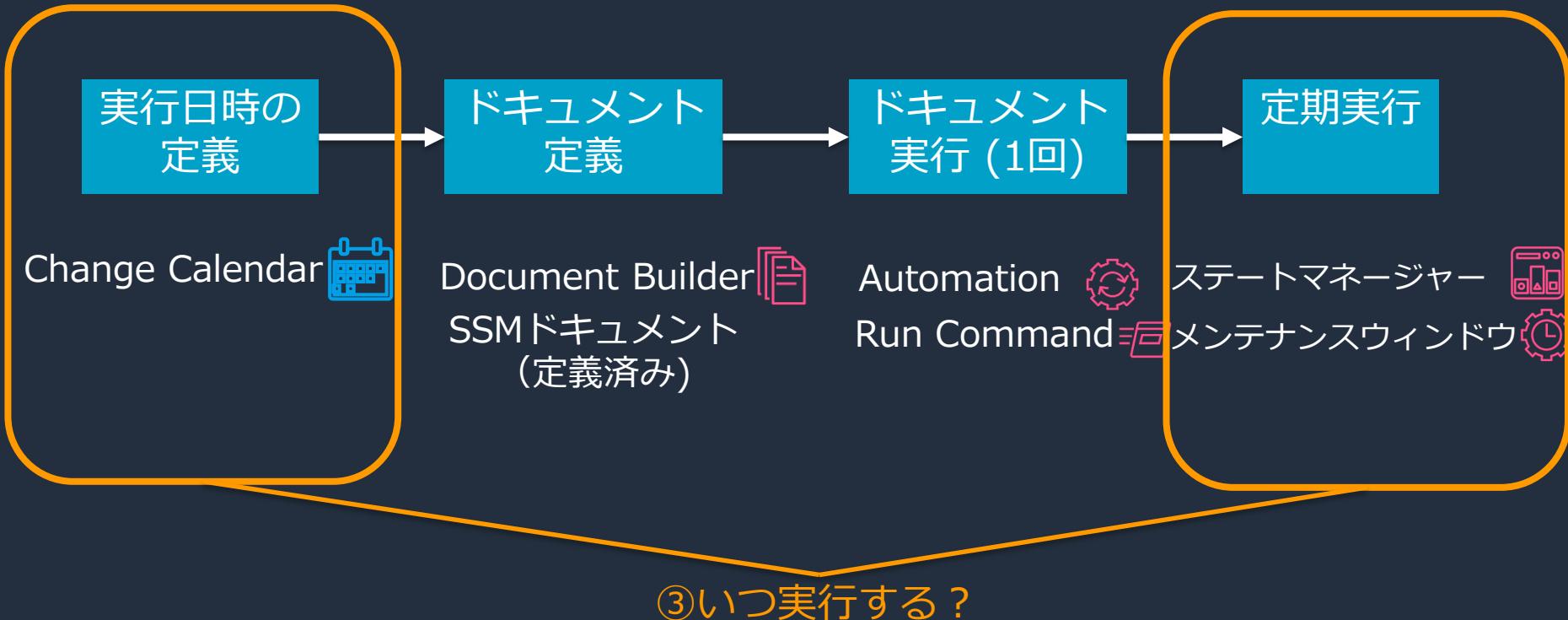
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



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

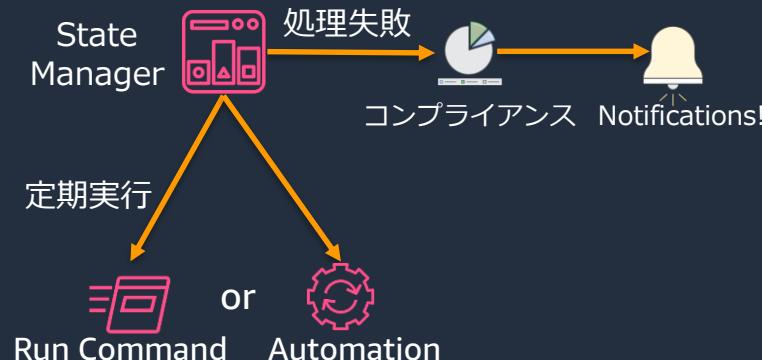
定義された状態に保つプロセスを自動化



- 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



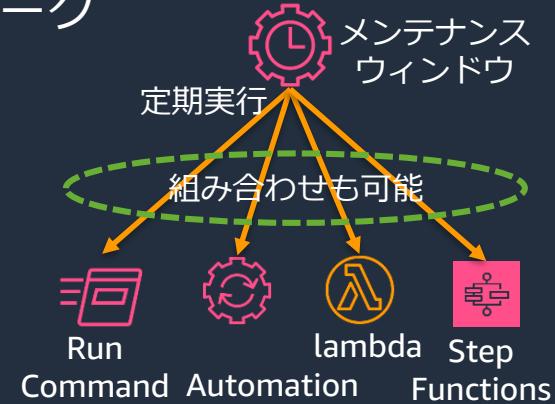
詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-state.html
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



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

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

ウィンドウ ID: mw-0000d5625bf5315d0

説明:

Cron/Rate 式: cron(0 */30 * * ? *)

下次実行時間: 2020年2月9日(日) 16:30:00 UTC

期間: 3時間

ウィンドウの開始日:

名前	優先度	名前	タスク ARN
test-patchApply	1	patch-apply	AWS-RunPatchBaseline
	2	lambda-task	arn:aws:lambda:ap-northeast-1:123456789012:lambda-task

何を :

タスクを複数定義でき
優先順位も指定可能

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

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.



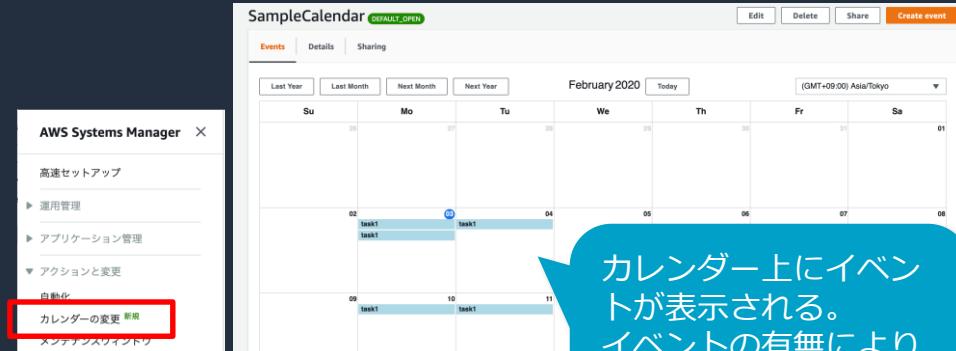
SSM Change Calendar

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



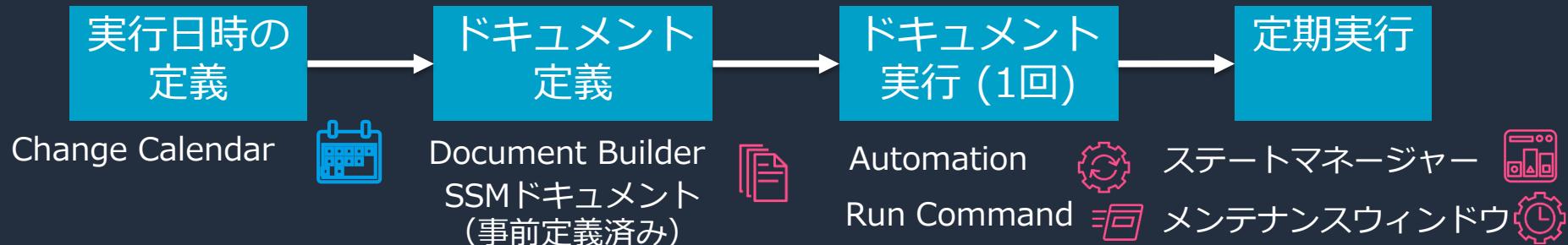
詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-change-calendar.html

© 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

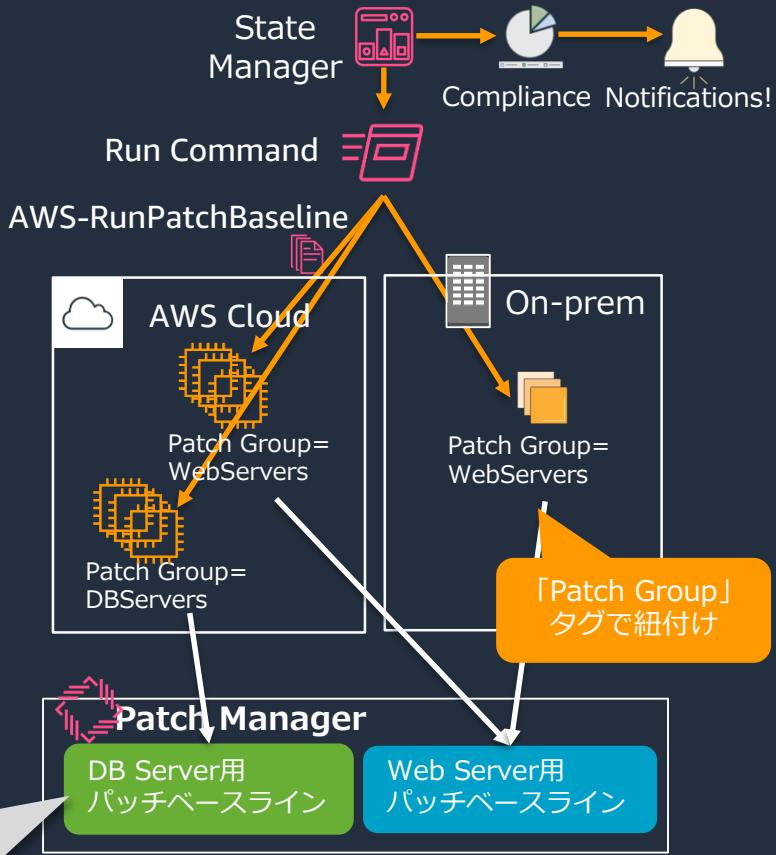


マネージドインスタンスにパッチを適用するプロセスを自動化

- ・ 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.



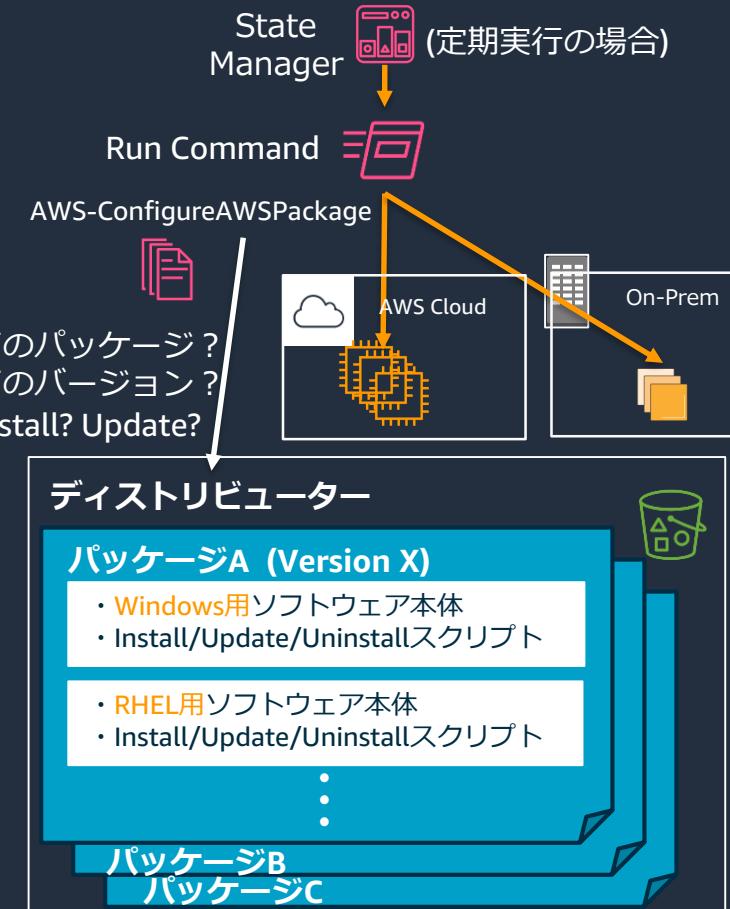
AWS SSM ディストリビューター

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.



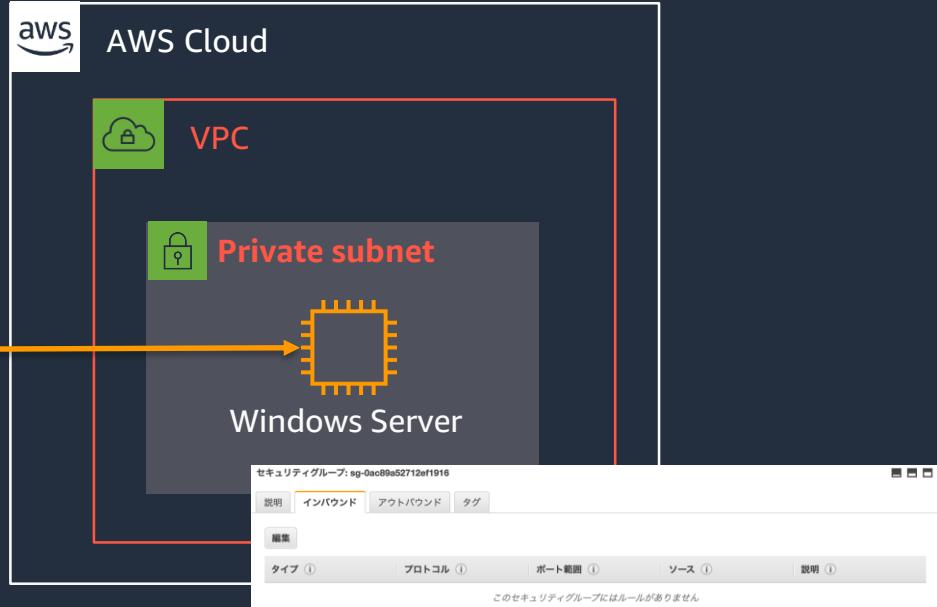
アジェンダ

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



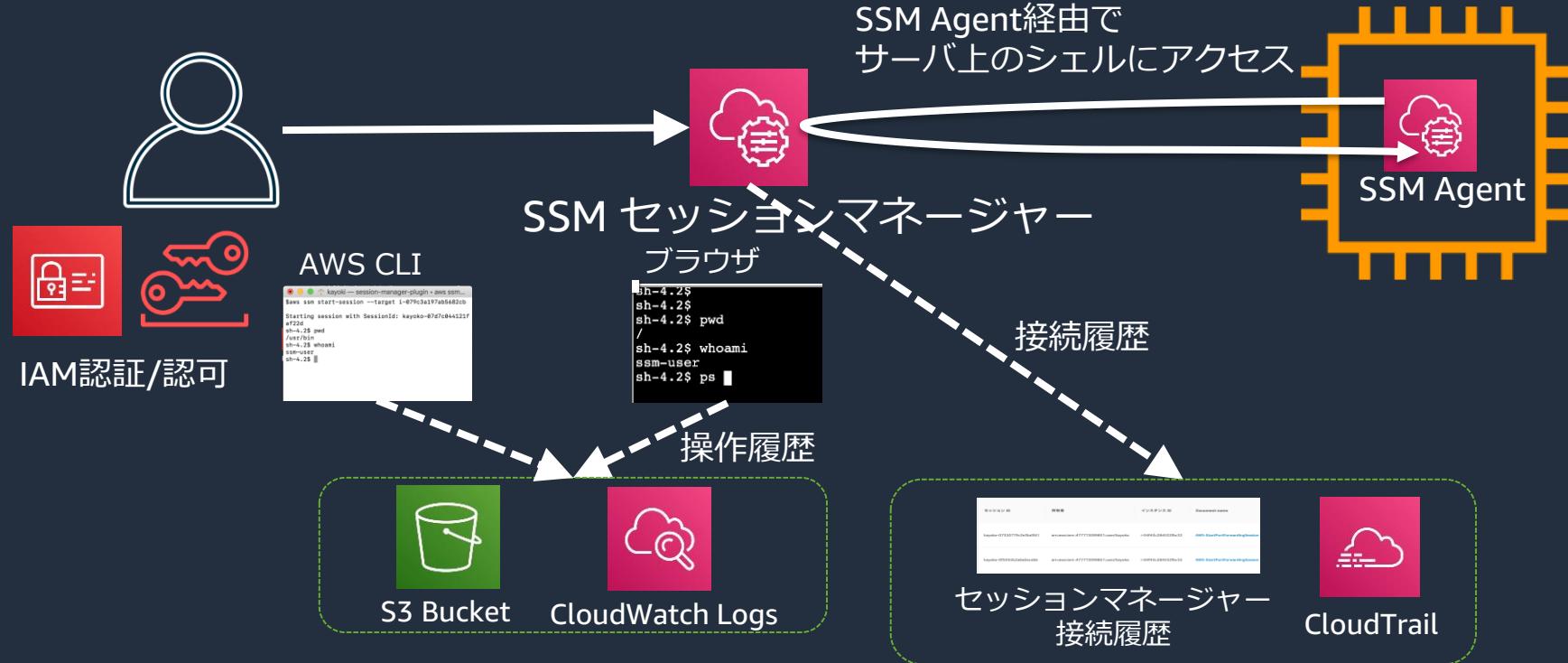
2019/7

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
```

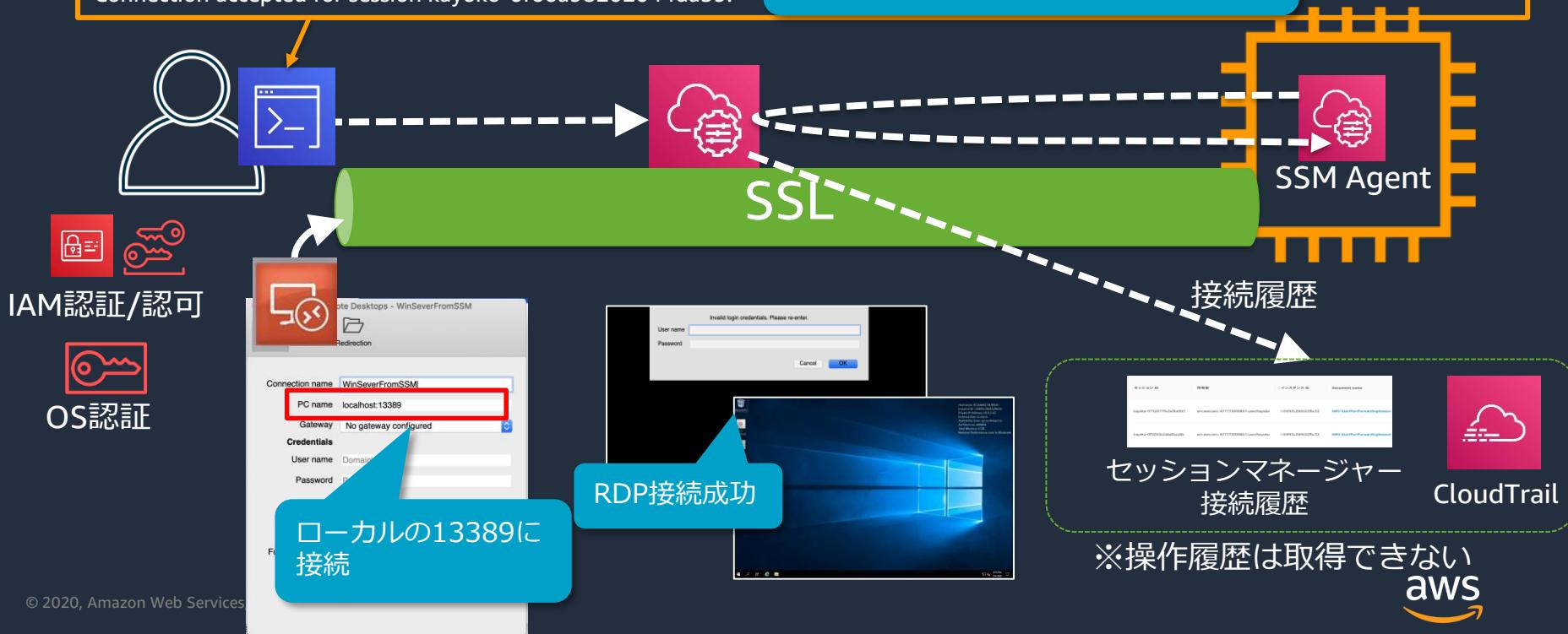
```
Starting session with SessionId: kayoko-024e90a532f59ad5e  
sh-4.2$
```

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.

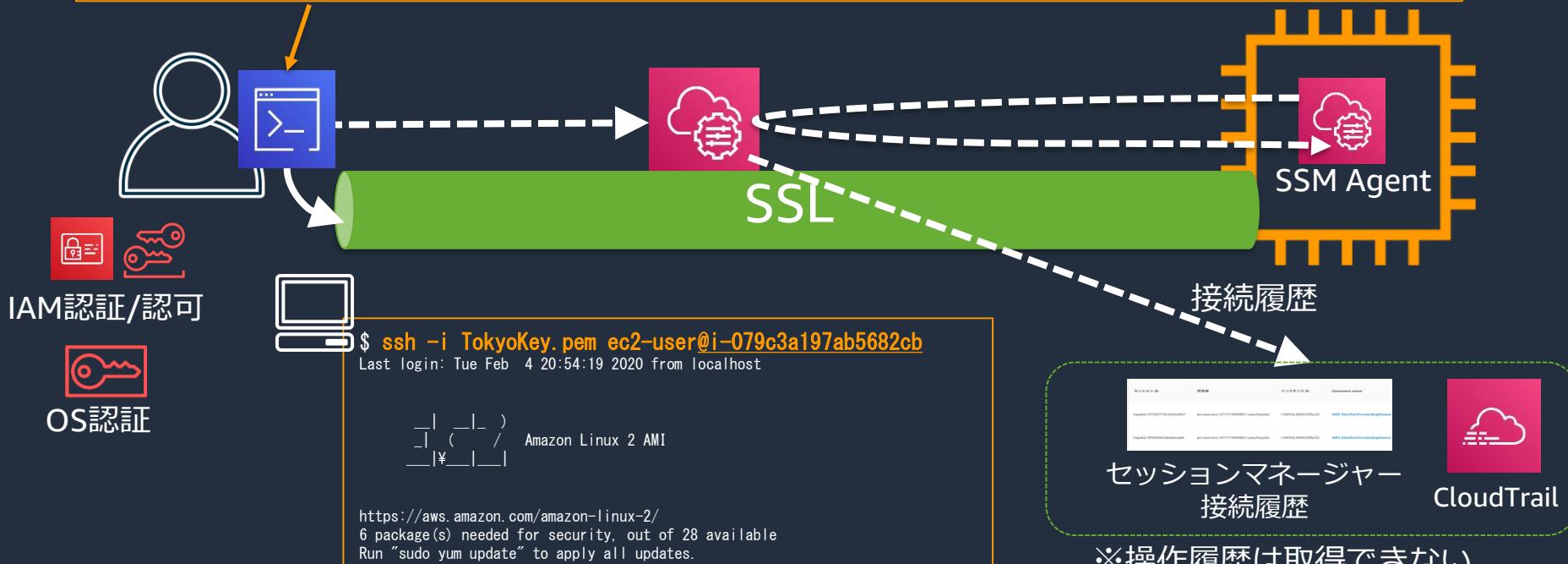
ローカル側の tcp13389 へのアクセスが
リモート側の tcp3389 に転送される



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 j-* mi-*  
ProxyCommand sh -c "aws ssm start-session --target %h --document-name AWS-StartSSHSession --parameters 'portNumber=%p'"  
$
```

SSHクライアントにProxy設定を追加



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

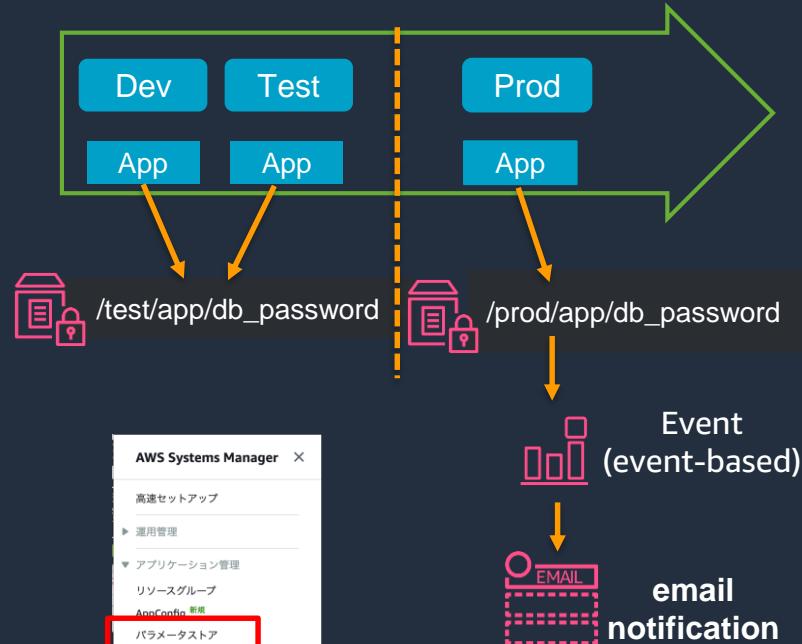
アジェンダ

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.



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 bar 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 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>

