# AWS Systems Manager

## Hybrid Activations 編

## AWS Black Belt Online Seminar

村田　京介

Solutions Architect

2023/06

# AWS Black Belt Online Seminar とは

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

# 内容についての注意点

- 本資料では 2023 年 5 月時点のサービス内容および価格についてご説明しています。最新の情報は AWS 公式ウェブサイト(https://aws.amazon.com/)にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

# 本セミナーの対象者

AWS の運用をされている方、これから運用される予定の方

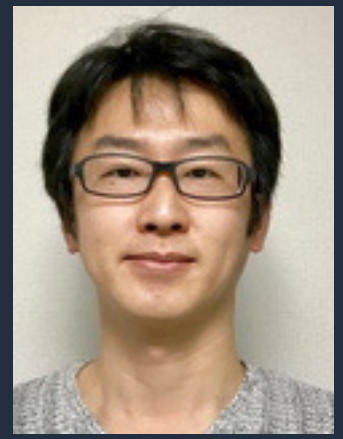
## 本セミナーの目的

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

## 本日お話ししないこと

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

# 自己紹介



名前：村田 京介（Kyosuke Murata）

所属：技術統括本部 エンタープライズ技術本部
　　サービスソリューション部

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

好きな AWS サービス： AWS Systems Manager

AWS Chatbot

# アジェンダ

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

# AWS Systems Manager (SSM) の概要

# AWS Systems Manager (SSM)

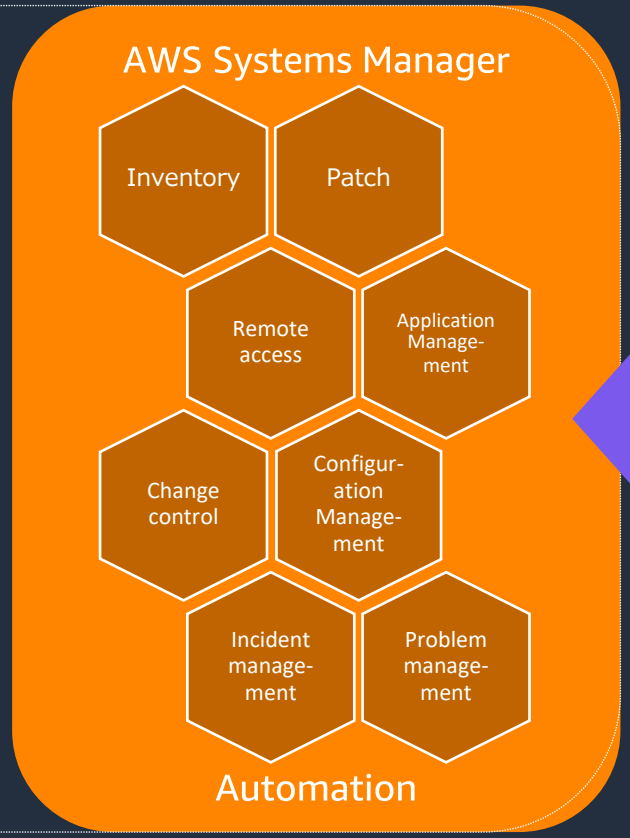
## ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション

**AWS Config**
Configuration history

**Amazon EventBridge**
Notification and remediation

**AWS CloudTrail**
Audited actions

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




Integration connectors and APIs

- Third-party tools
- ITSM
- Custom solutions

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

Cloud On-premises Edge

# SSM 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

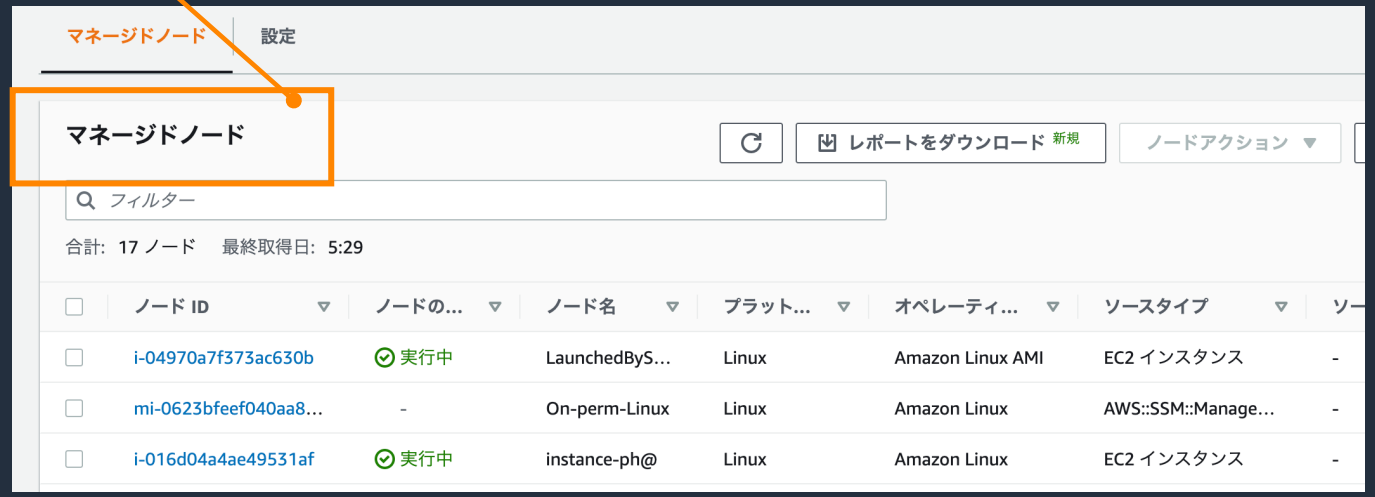
Quick Setup

# EC2 インスタンス以外を SSM で管理するには？

# SSM を使って管理を行うためには

## **”マネージドノード”**にする

**ここに一覧で出てくるようになります**




マネージドノード：

- SSM 管理下のインスタンス群
- EC2 インスタンスのほか、**オンプレミスのサーバ**も含められる。

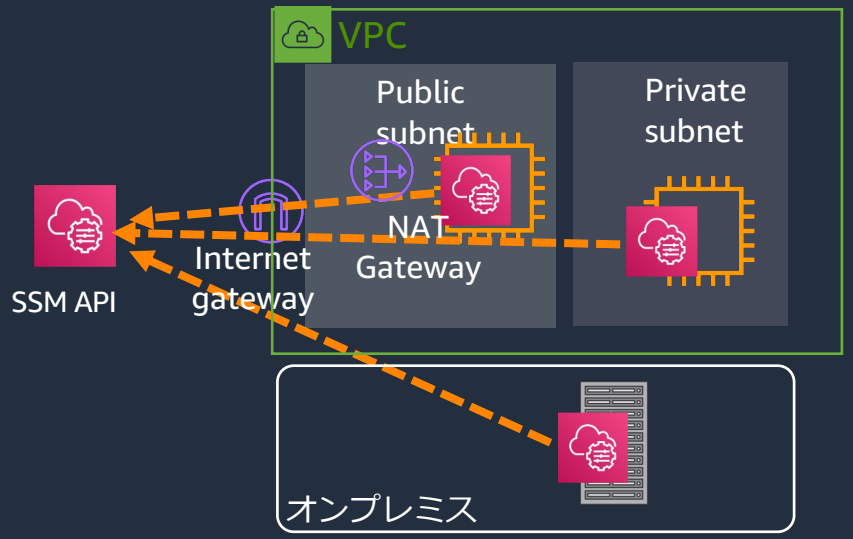
# SSM でサポートされている EC2 以外のマシンタイプ

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

# ① アウトバウンド経路の確保

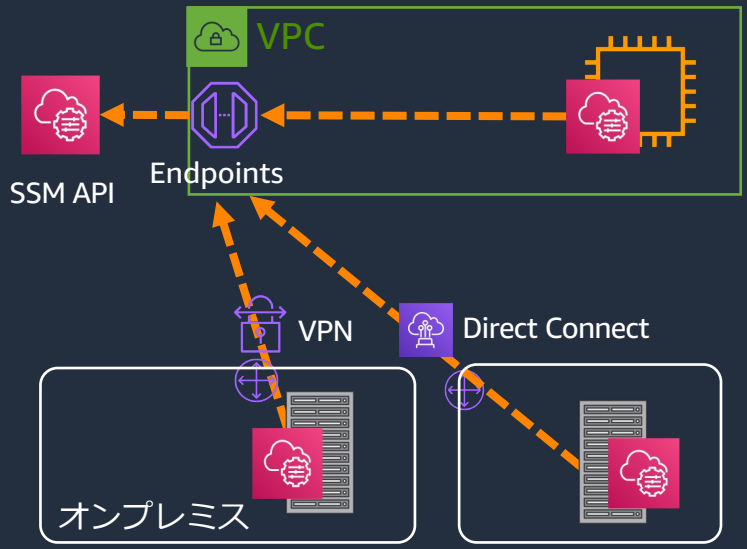
- 以下のいずれかのパターンで、SSM Agent からの HTTPS のアウトバウンド経路を確保
- インバウンドアクセスは不要

**1. インターネット経由**




**2. VPC エンドポイント経由**

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




SSM のセットアップ詳細はこちら

# ② IAM サービスロールの作成

- マネージドノードが SSM と通信するために IAM サービスロールを作成

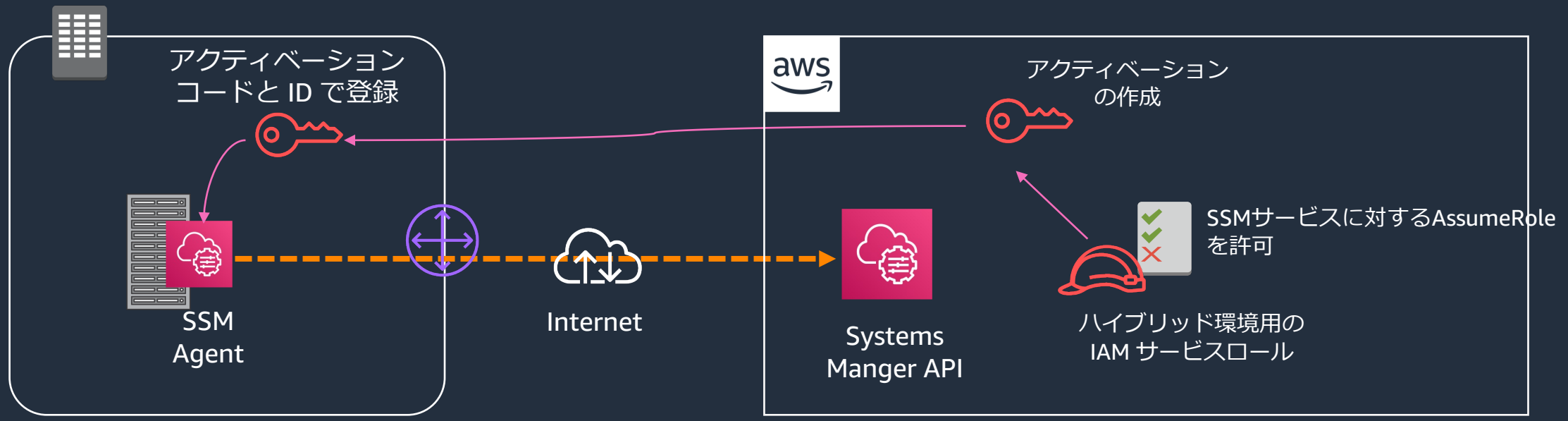
1. 信頼できるエンティティに「Systems Manager」 を選択 (必須)
2. IAM ポリシーについては、まず「AmazonSSMManagedInstanceCore」 でコア機能をアタッチ (必須)
3. S3 などのポリシーをアタッチ (オプション)

IAM サービスロール作成の詳細はこちら

# ③ アクティベーション作成

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

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

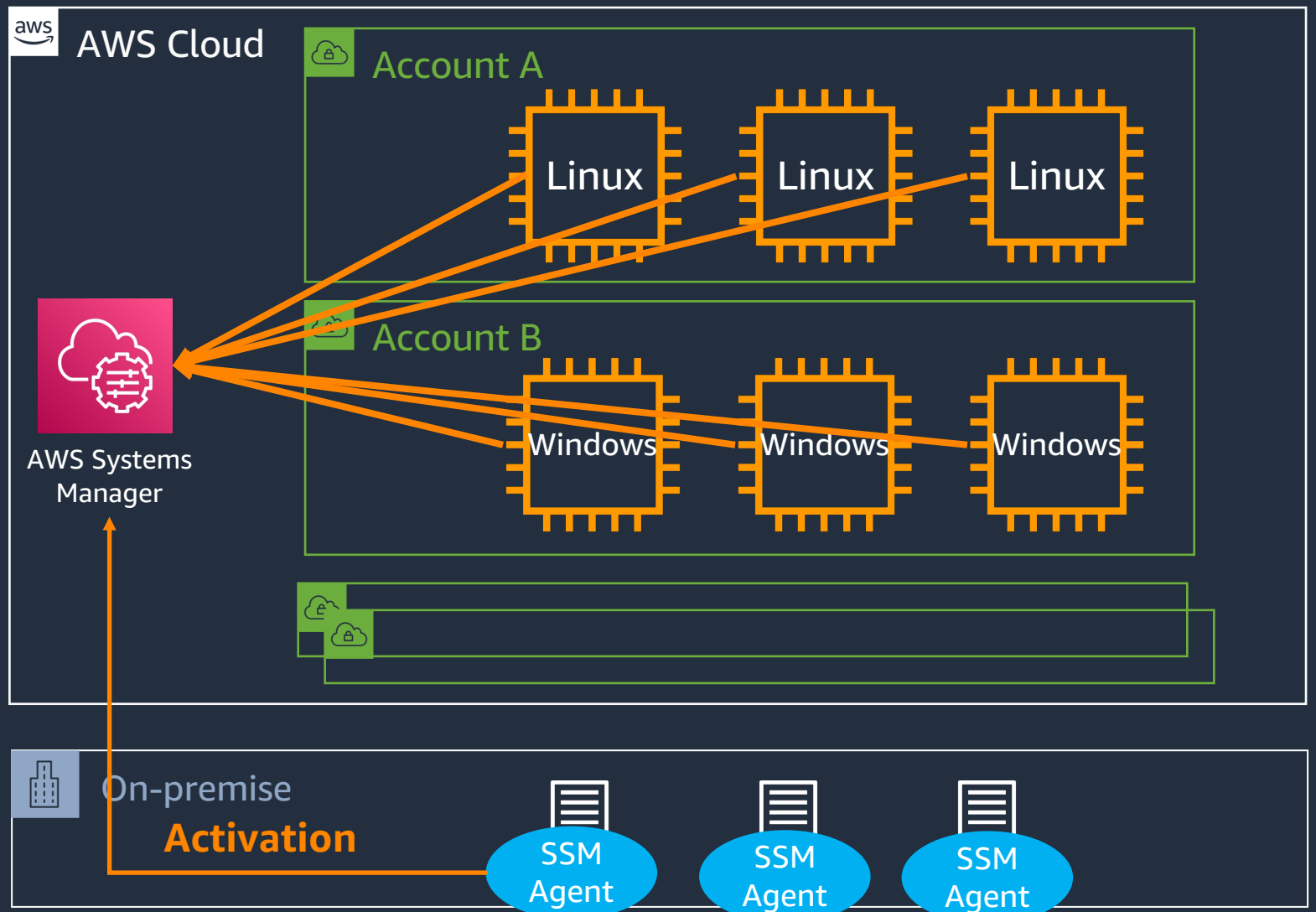


# ④ SSM Agent のインストールと登録

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

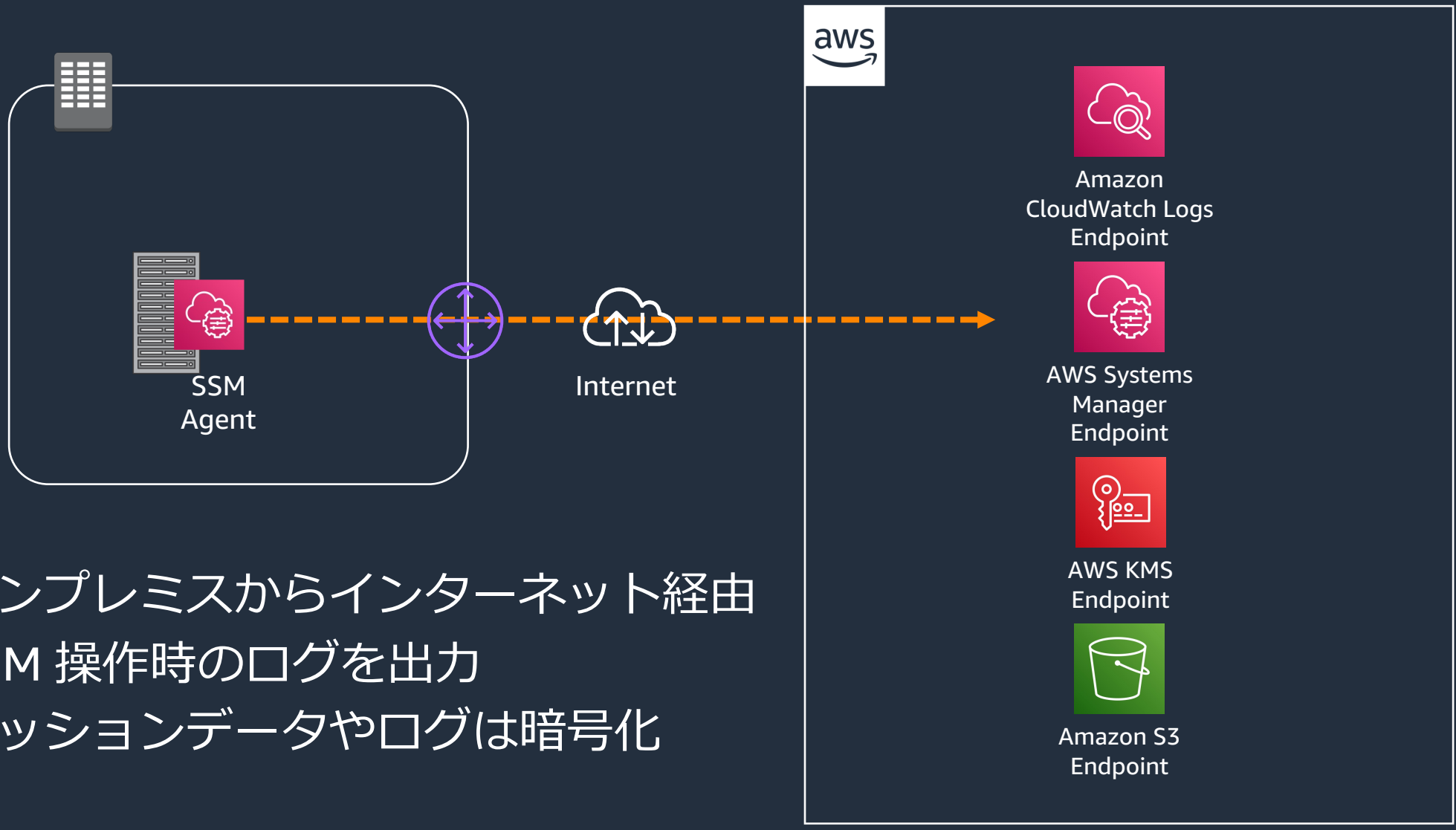
  Linux へのインストール手順はこちら、Windows のインストール手順はこちら

# ここまでやれば、晴れてマネージドノードに！



# 具体的な構成手順とデモ

# 前提




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

# 【ご参考】閉域網での構成例

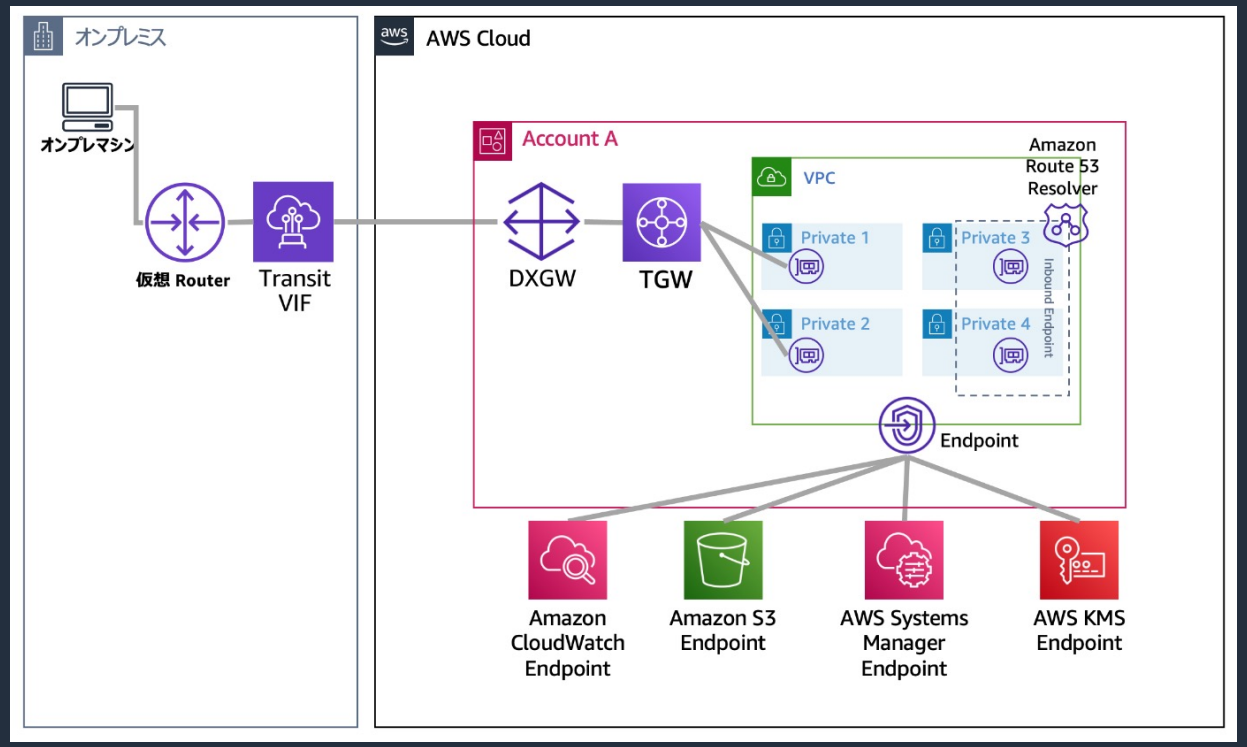
Amazon Web Services ブログ

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

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

こんにちは。ソリューションアーキテクトの村田と申します。

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




閉域網での構成例について記載したブログはこちら

# 手順 1. インターネットへの疎通確認

## Ubuntu Server 20.04 LTS の場合

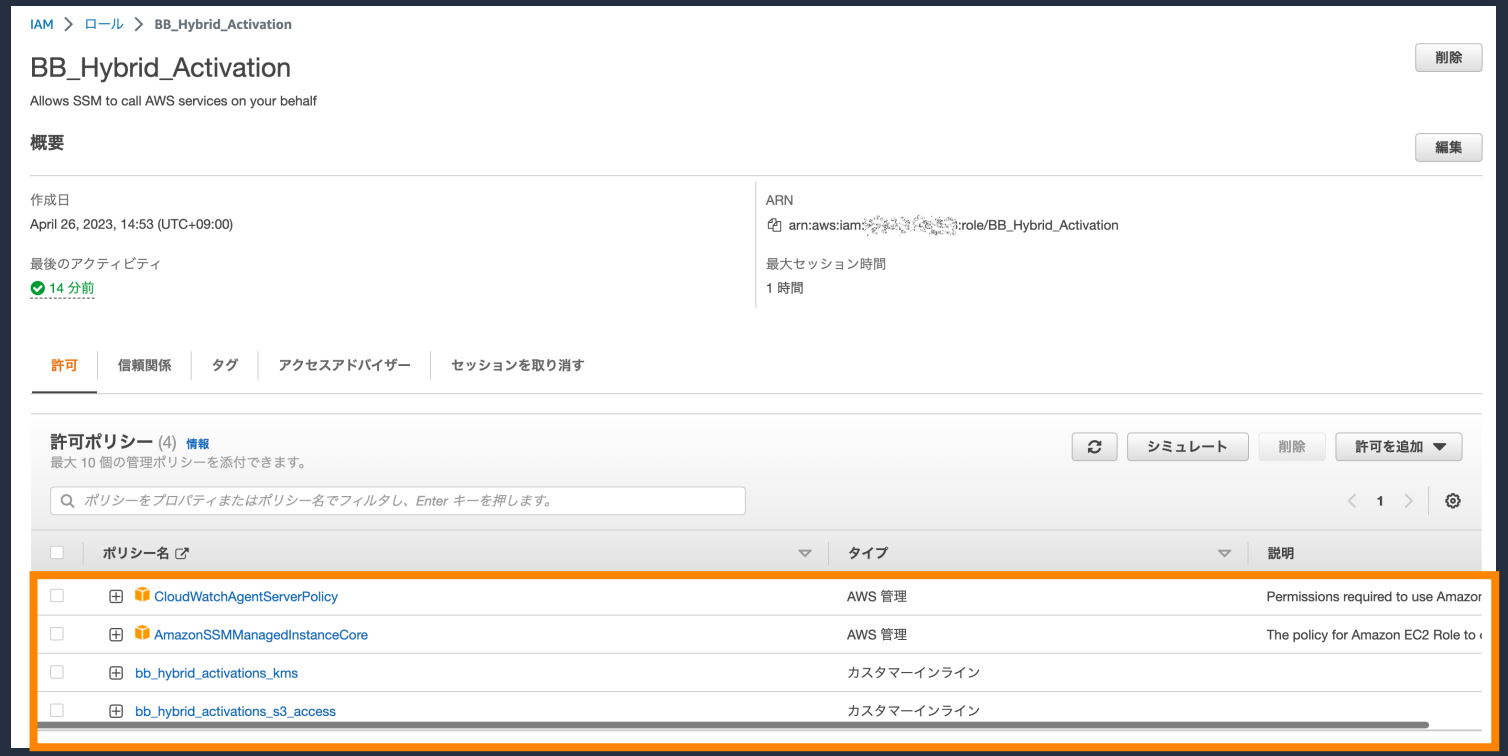
インターネット向けの HTTPS アクセスができることの確認

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

SSM の各種エンドポイントと通信プロトコルについてはこちら

# 手順 2-1. IAM サービスロールの作成

# 手順 2-2. IAM サービスロールの作成




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

今回の構成では、セッションデータやログの暗号化を行っています。

Amazon CloudWatch Logs へのセッションデータのログ記録と暗号化についてはこちら
Amazon S3 へのセッションデータをログ記録と暗号化についてはこちら
Session Manager のセッションデータ暗号化についてはこちら

# 手順 3-1. アクティベーションの作成

# 手順 3-2. アクティベーションの作成


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

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

**Activation Code** [redacted]

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

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

# 手順 4. SSM Agent インストール

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

$ mkdir /tmp/ssm

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

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

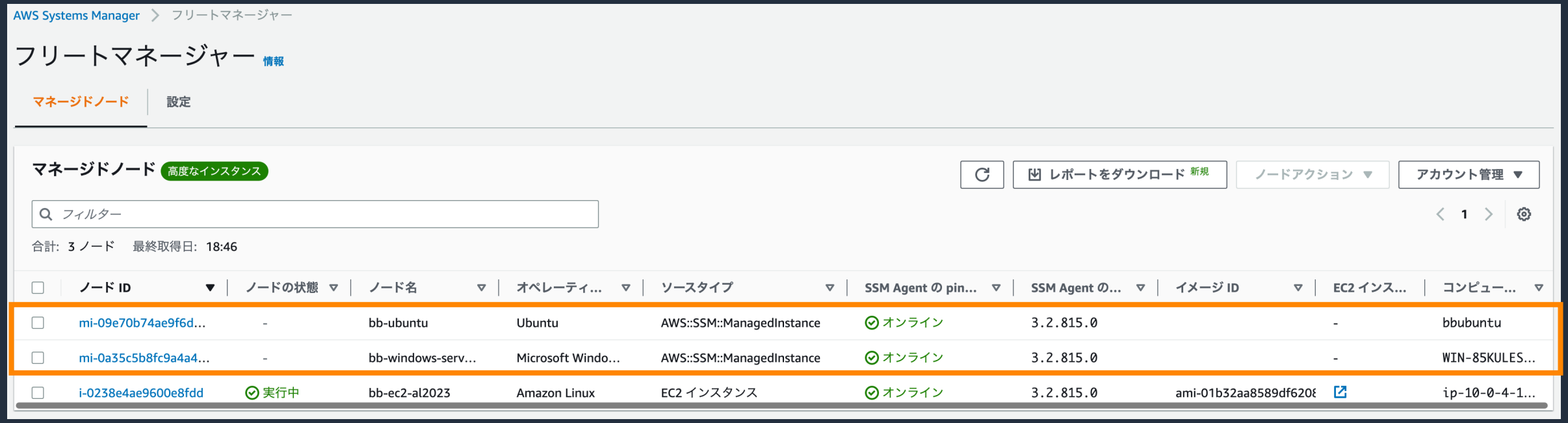
$ sudo service amazon-ssm-agent stop

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

$ sudo service amazon-ssm-agent start

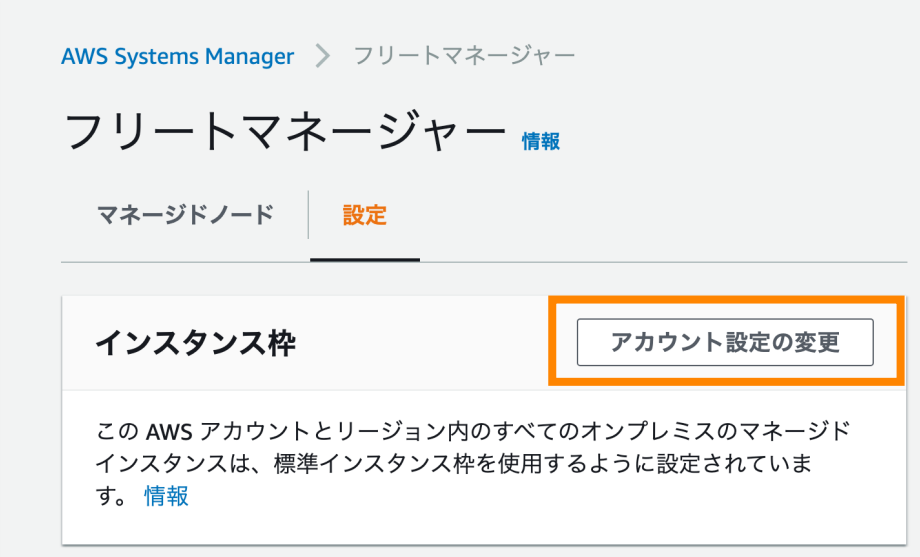
※ Linux へのインストール手順はこちら、Windows のインストール手順はこちら

# 晴れてマネージドノードに



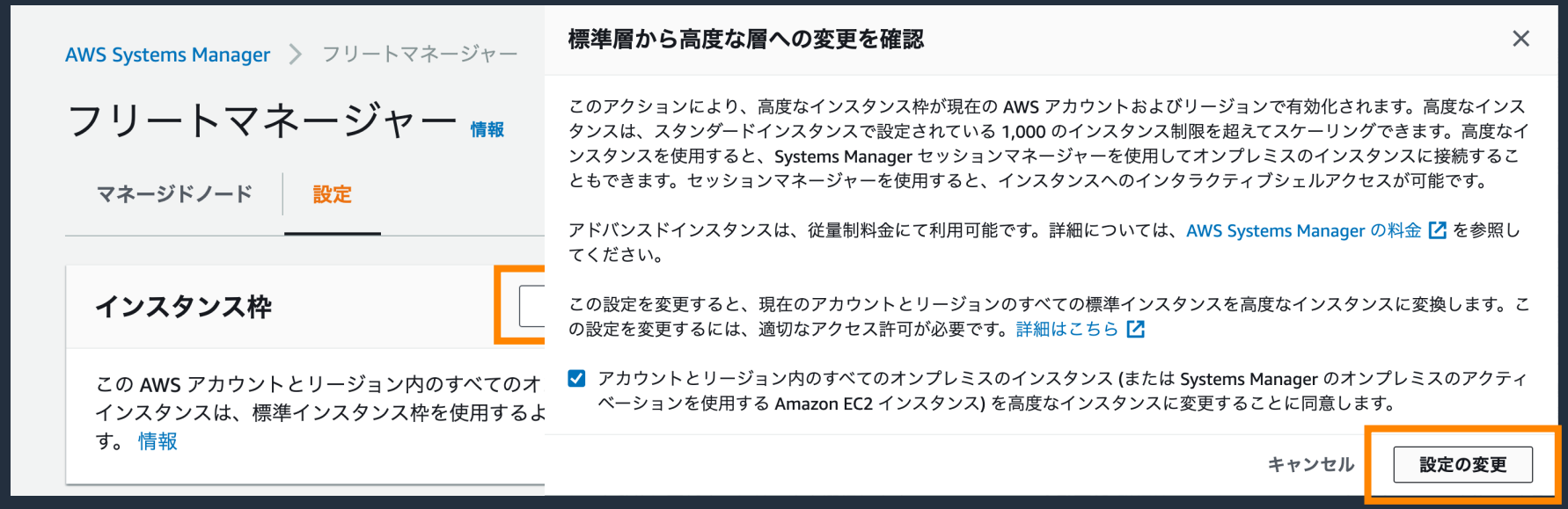

- ハイブリッドノードの Fleet Manager への表示のされ方
  - ノード ID は “mi-” から始まる
  - ソースタイプは ”AWS::SSM::ManagedInstance”
  - ノード名の列は ”アクティベーション時の入力値”（ホスト名はコンピュータ名の列）

# 手順 5. インスタンス枠を変更（オプション）



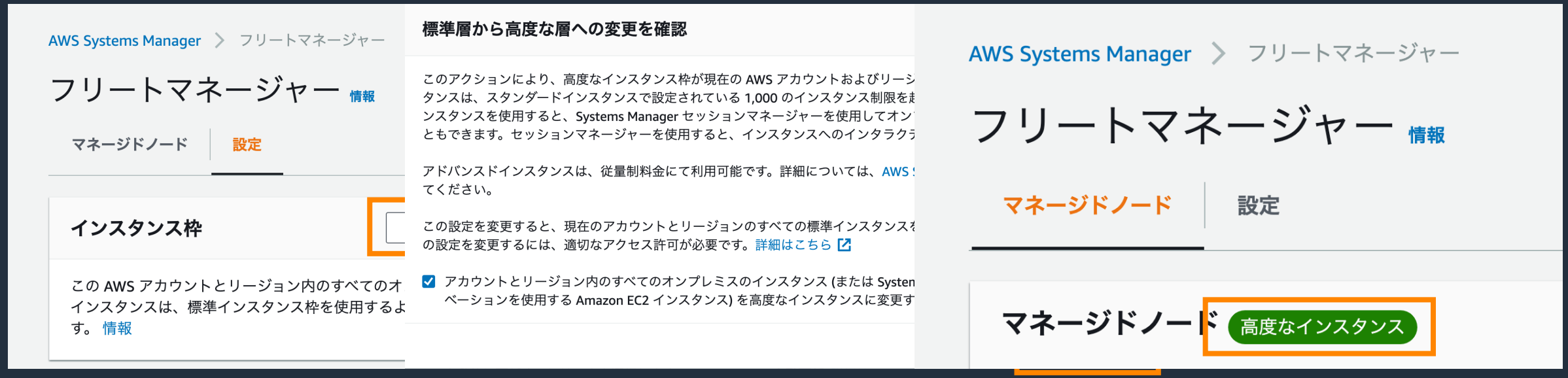

- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
  - アカウント毎にリージョンあたり 1,000 を越えるハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を登録
  - ハイブリッドノードに接続するために Session Manager を使用
  - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

# 手順 5. インスタンス枠を変更（オプション）



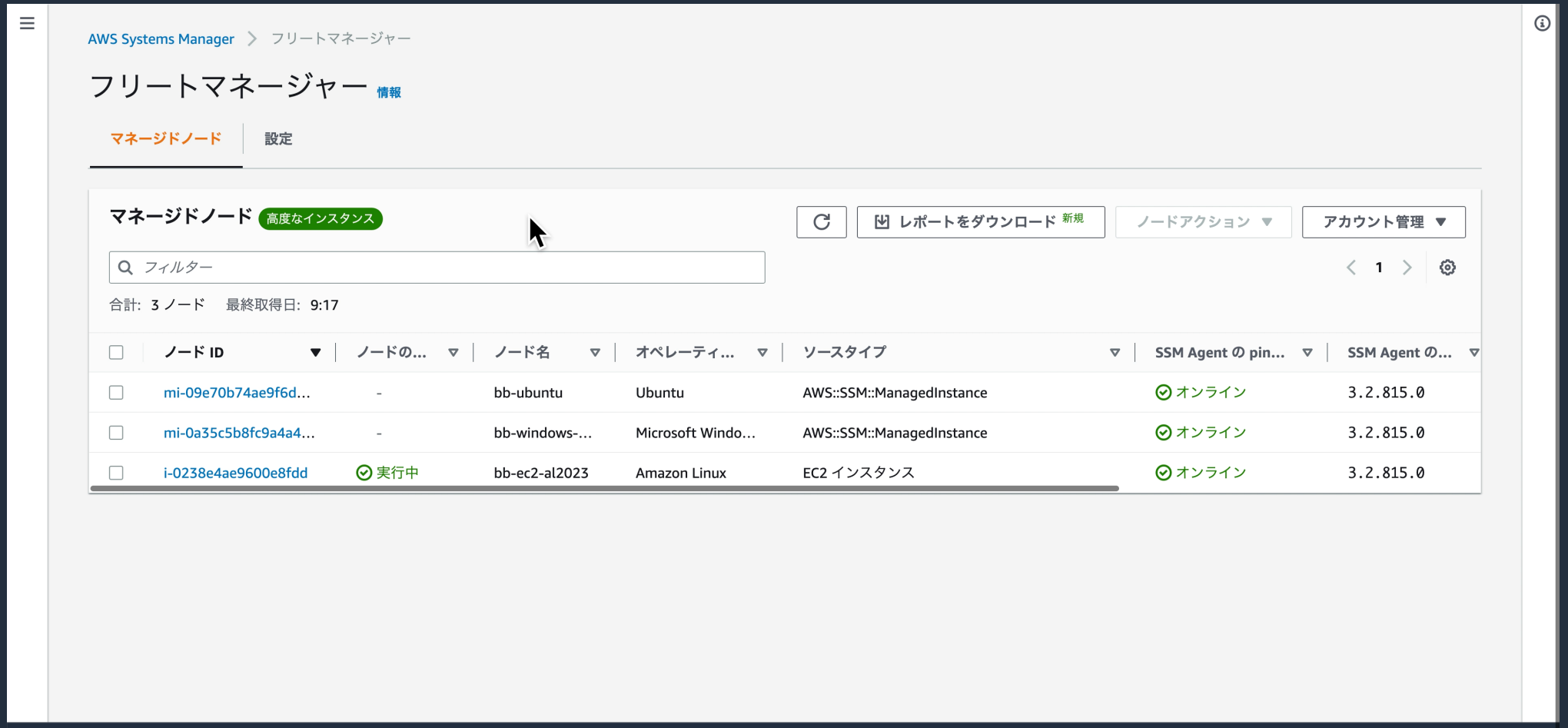

- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
  - アカウント毎にリージョンあたり 1,000 を越えるハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を登録
  - ハイブリッドノードに接続するために Session Manager を使用
  - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

# 手順 5. インスタンス枠を変更（オプション）

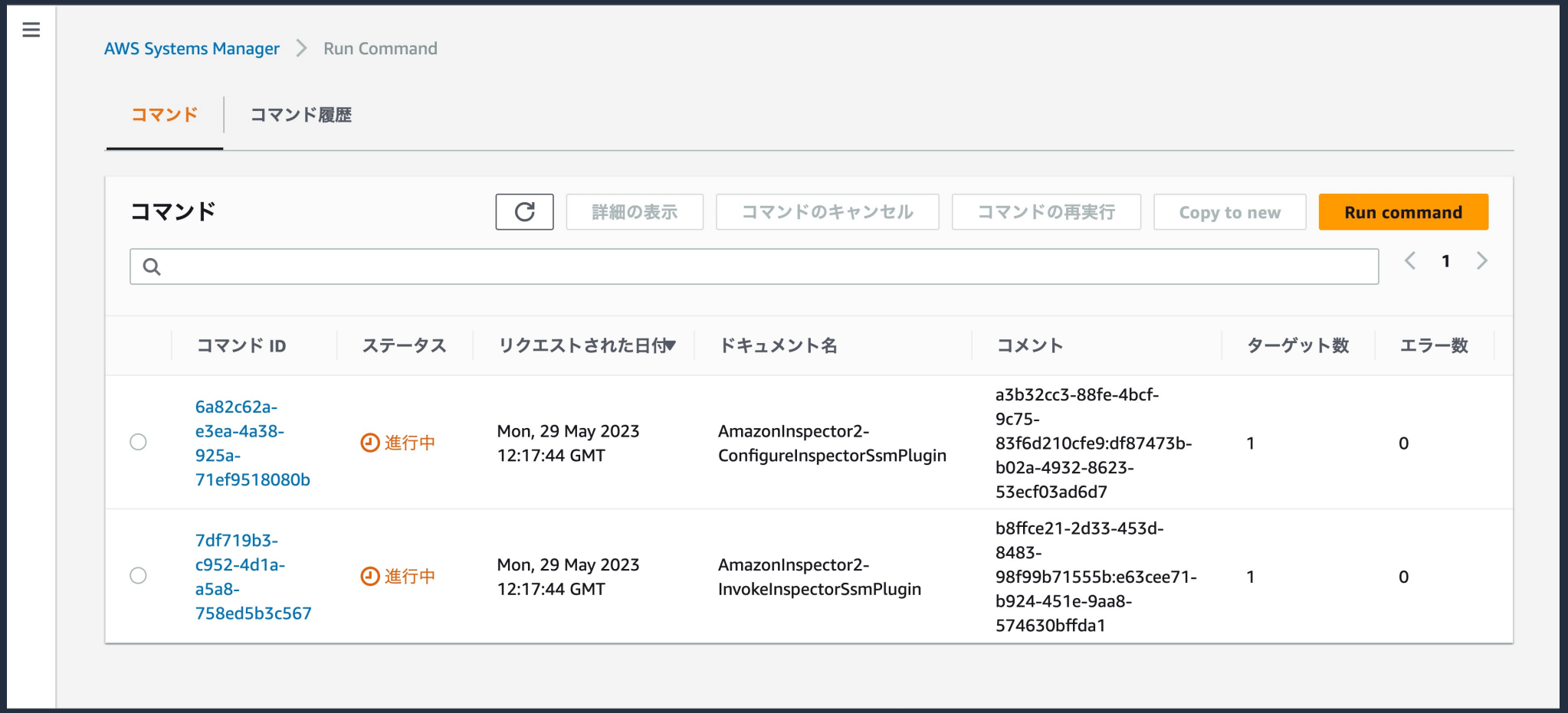



- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
  - アカウント毎にリージョンあたり 1,000 を越えるハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を登録
  - ハイブリッドノードに接続するために Session Manager を使用
  - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

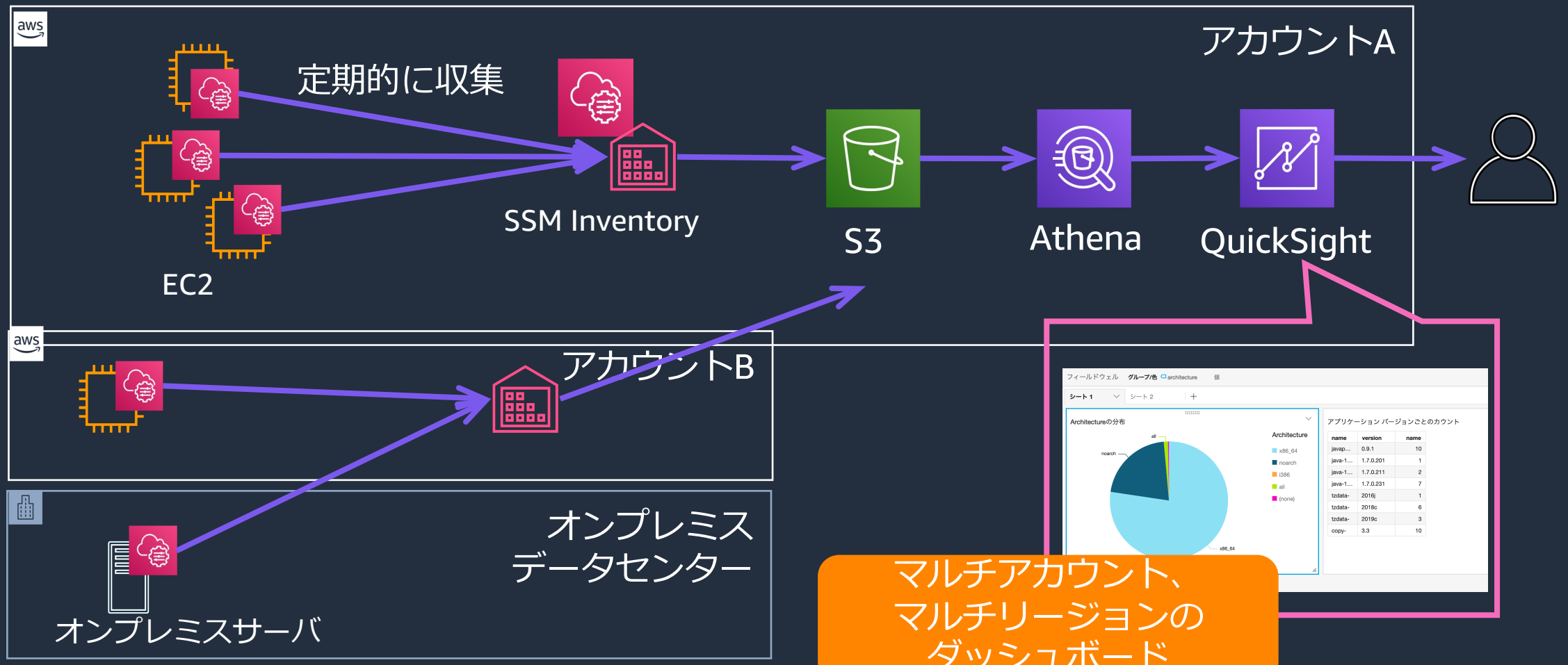
# デモ 1



# デモ 2



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




詳細はこちらのチュートリアル参照
「チュートリアル: リソースデータの同期を使用してインベントリデータを集約する」

# SSM Hybrid Activations の料金

# Hybrid Activations の料金

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

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

【参考】
インスタンス層の設定
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-managed-instances-tiers.html
AWS Systems Manager の料金
https://aws.amazon.com/jp/systems-manager/pricing/

# 計算例

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

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

【参考】
AWS Systems Manager の料金
https://aws.amazon.com/jp/systems-manager/pricing/

# まとめ

# まとめ

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

# 本資料に関するお問い合わせ・ご感想

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

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

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

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

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください

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

# その他コンテンツのご紹介

ウェビナーなど、AWS のイベントスケジュールをご参照いただけます

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

ハンズオンコンテンツ

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

AWS 個別相談会

AWS のソリューションアーキテクトと直接会話いただけます

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

# Thank you!