AWS Black Belt Online Seminar

AWS Systems Manager Patch Manager 編

小野　卓人

Solutions Architect

2024/04

自己紹介

名前：小野 卓人（Takuto Ono）

所属：技術統括本部
フィナンシャルサービスインダストリ技術本部
保険ソリューション部

経歴：
SIer で金融機関向けシステムの受託開発
インフラ設計・構築・運用保守
現在は、ソリューションアーキテクトとして主に保険業界のお客様を担当

好きなAWSサービス： AWS Systems Manager

本セミナーの対象者

AWS の運用をされている方、これから運用される予定の方

本セミナーの目的

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

本日お話ししないこと

- AWS Systems Manager の全体的な説明
  → AWS Systems Manager Overview を参照ください
- AWS Systems Manager Patch Manager 以外の機能の詳細
  → 各機能にフォーカスしたセッションを参照ください

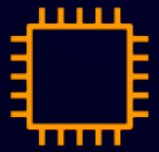
アジェンダ

1. パッチ管理の課題
2. Patch Manager の全体像
   - パッチオペレーションの流れ
   - パッチベースラインとパッチグループ、パッチポリシー
   - Patch Manager で使用する SSM ドキュメント
3. Patch Manager の開始方法
4. 実行結果の確認
5. TIPS
6. 料金
7. まとめ

パッチ管理の課題

パッチ管理における課題

パッチ適用の考慮事項



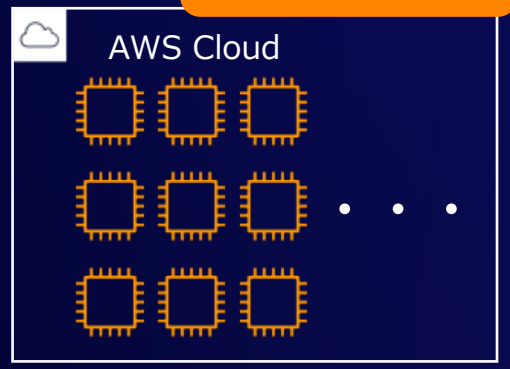
サーバごとに異なる
- **OS、バージョン**
- **インストール済みパッケージ**
- **セキュリティ要件**
- **適用タイミング etc**

パッチ管理作業は重労働

- パッチ適用状況の管理
- 適用が必要なパッチの洗い出し
- 定期的なパッチ適用の実施
- 緊急パッチへの例外的な対応

バリエーションが増えれば
増えるほど作業が大変！

大量のEC2
インスタンス

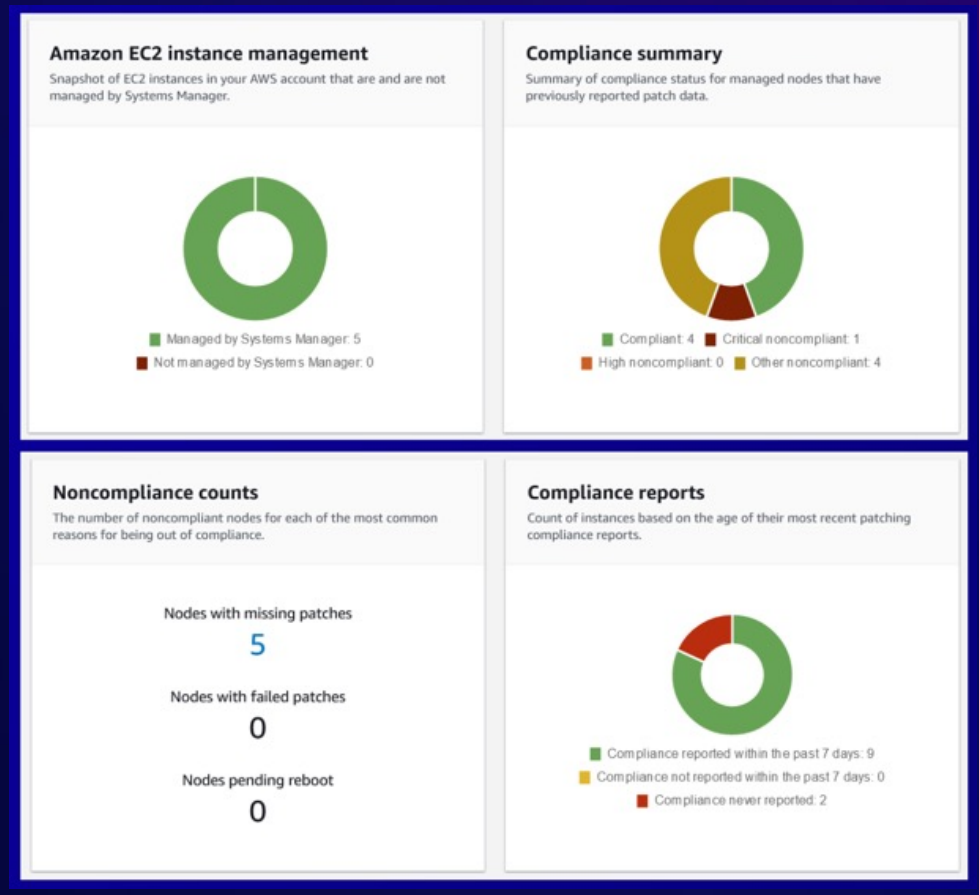


オンプレも・・・

Systems Manager Patch Manager とは

マネージドノードへのパッチ適用プロセスを自動化

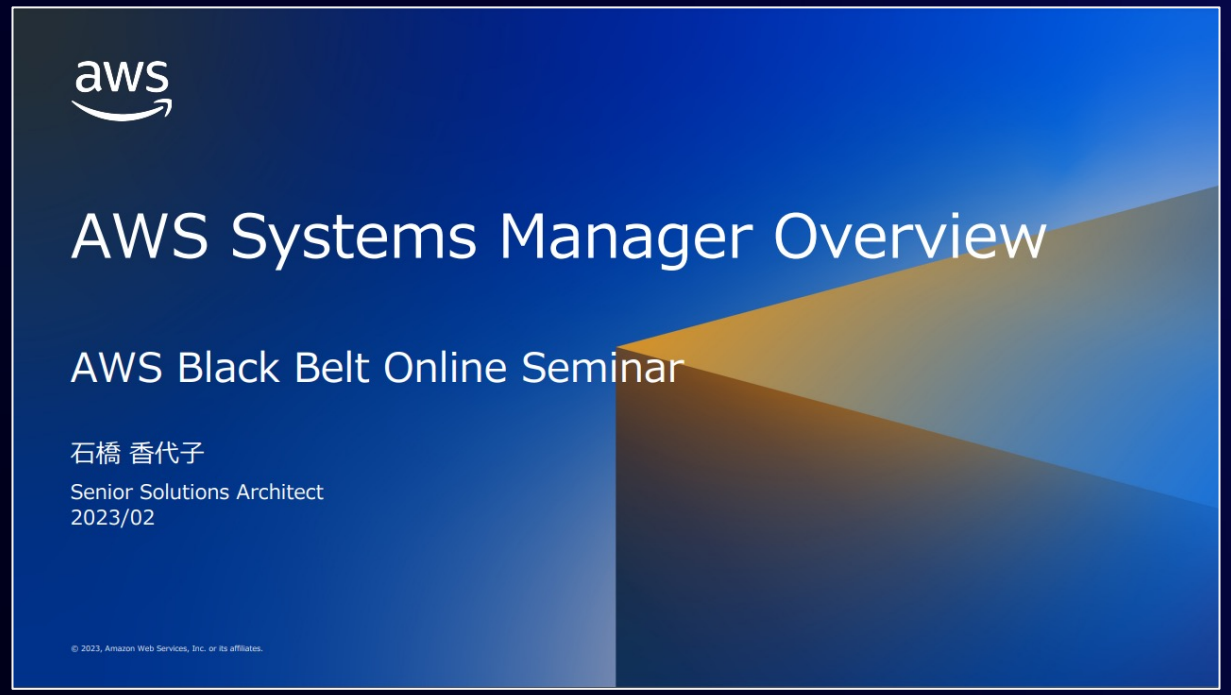
- 自動承認のルールを定義し、適用すべきパッチの選別を自動化
- 定期的にパッチをスキャン＆インストール
- ダッシュボードでパッチのコンプライアンス状況を可視化
- リソースデータ同期によりクロスアカウント、クロスリージョンでコンプライアンス情報を収集可能

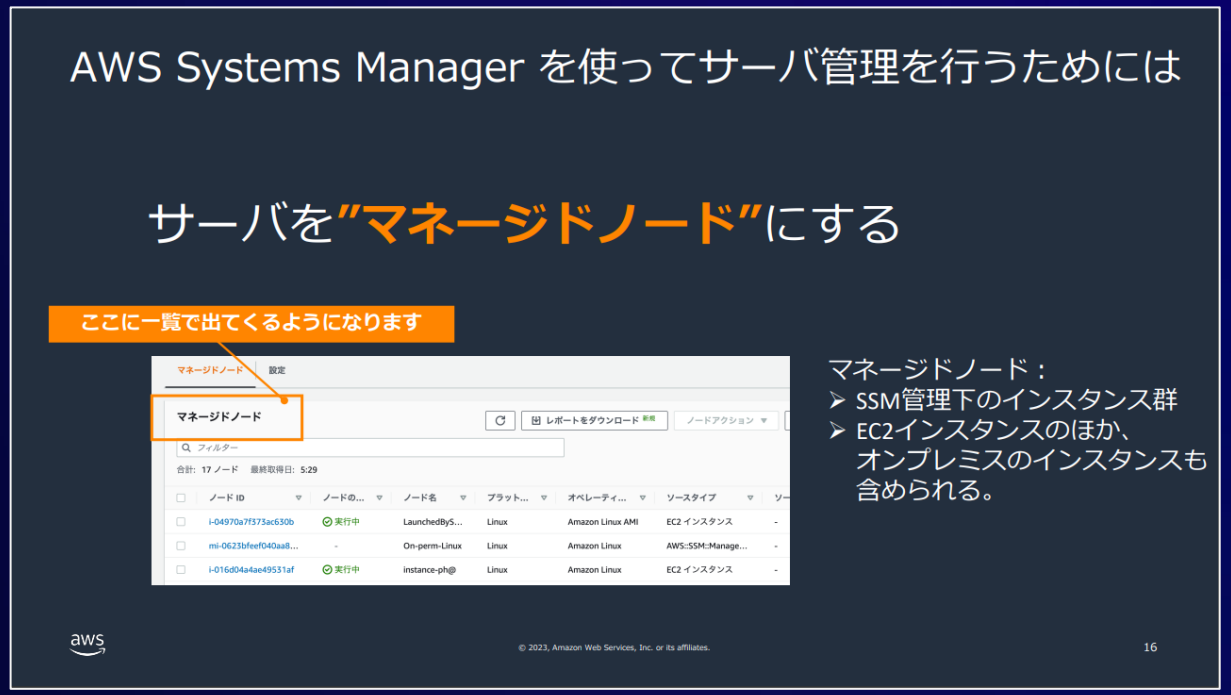


（補足）マネージドノードとは

Systems Manager で使用するように設定されたマシン

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





(*) AWS Systems Manager = SSM と略します。

Patch Manager の前提条件

最新のサポート情報はドキュメントを参照ください
https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-prerequisites.html

- Systems Manager のマネージドノードであること
- （Linux 、 macOS の場合）Python がインストールされていること
- パッチソースリポジトリへの接続が可能であること
- Systems Manager サービスのホストする S3 バケットへアクセスできること

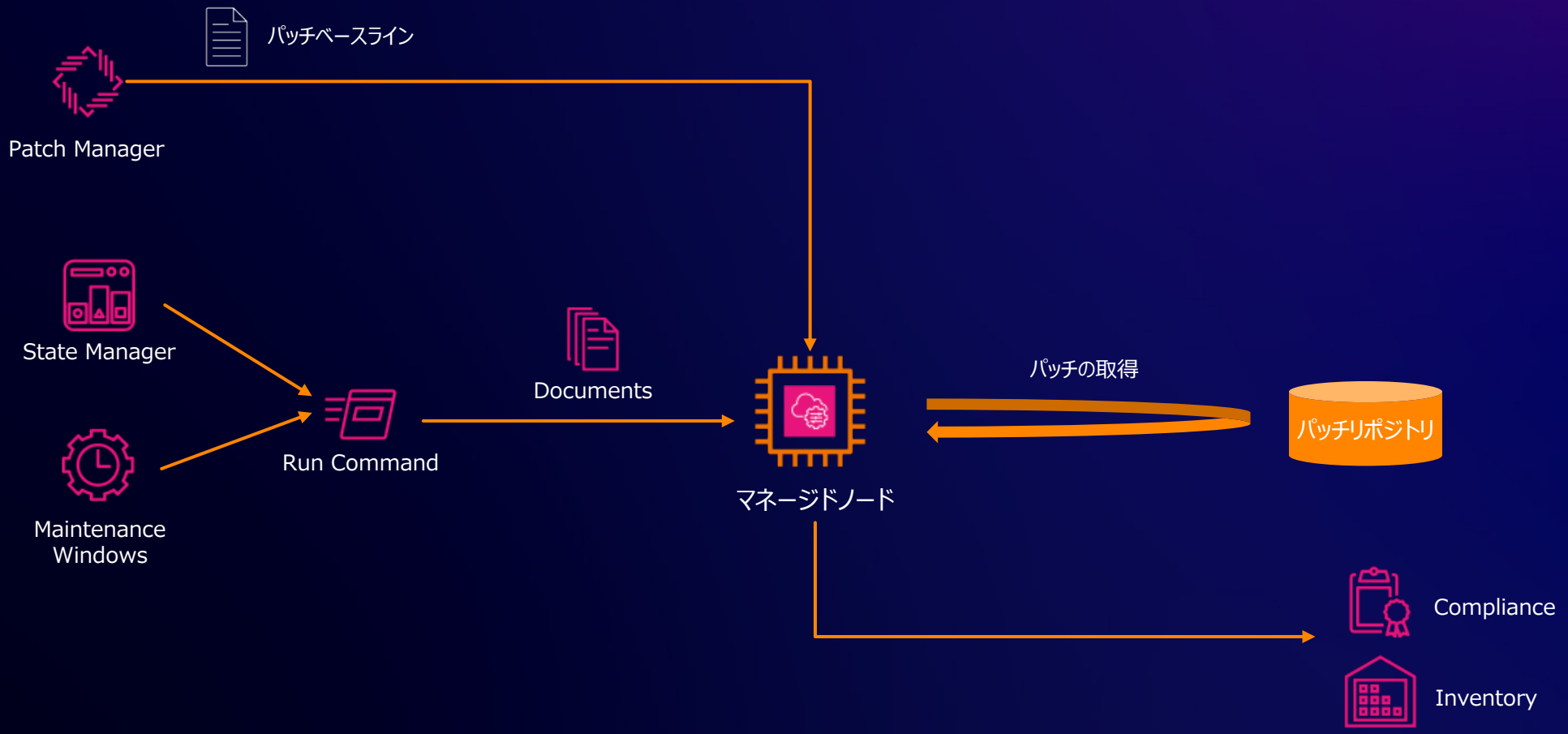
  詳細はこちらを参照
  https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/ssm-agent-minimum-s3-permissions.html

- Patch Manager でサポートされている OS および OS バージョンであること

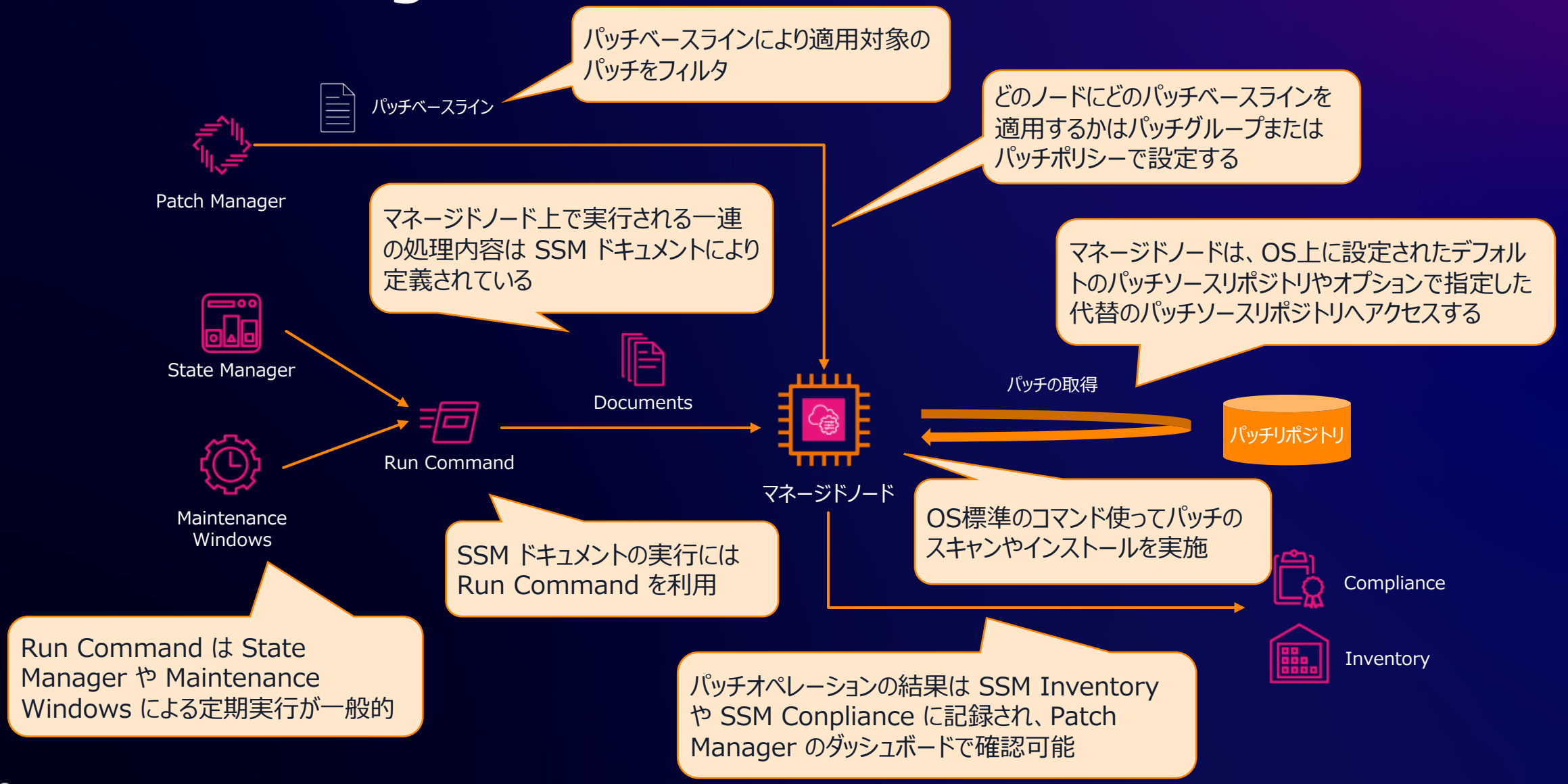
  ※ Systems Manager の他の機能でサポートされる OS のバージョンと必ずしも一致しない点に注意

Patch Manager の全体像

Patch Manager 全体像



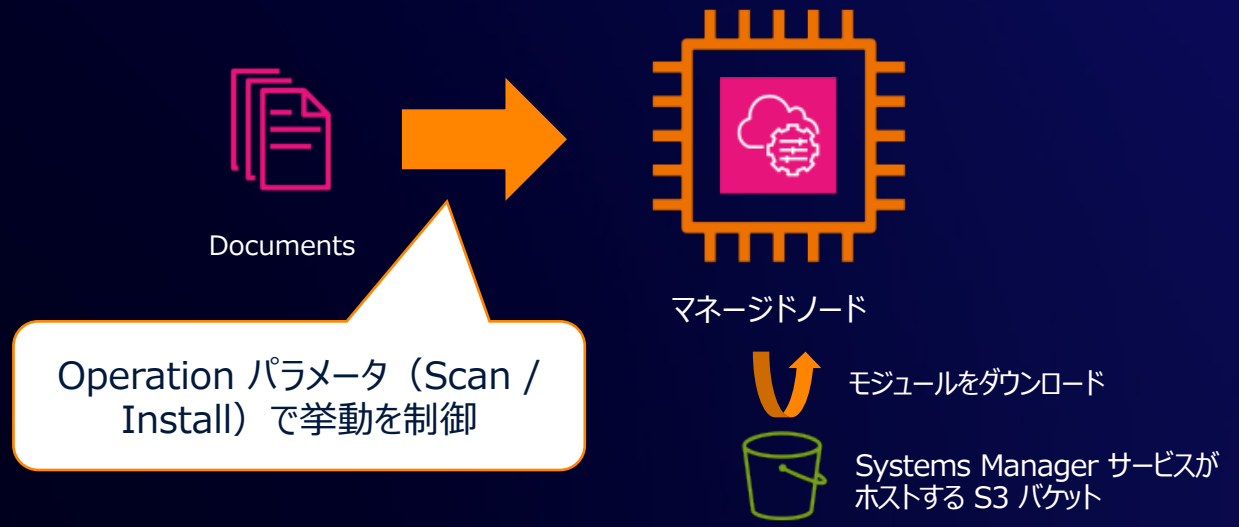
Patch Manager 全体像



パッチオペレーションの流れ

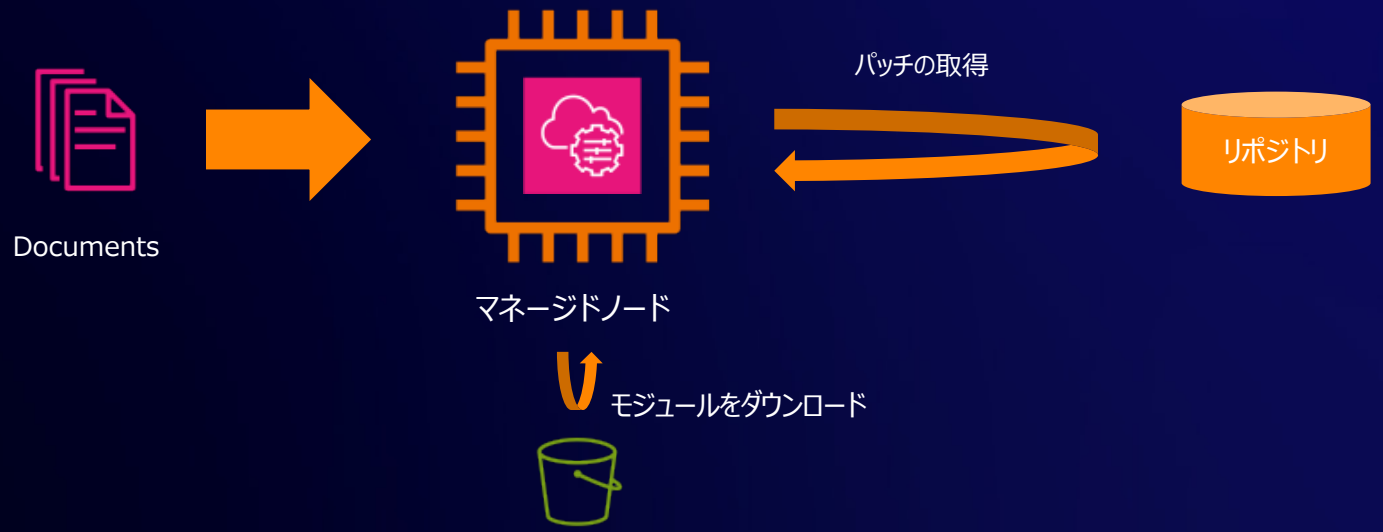
マネージドノード上で実行される処理

- 実行される処理の内容は SSM ドキュメントで定義されている
- マネージドノード上で実行される処理は、大きく２つのモードがある
  - **Scan オペレーション**：指定した基準（ベースライン）に対して不足しているパッチの報告のみを実施
  - **Scan and install オペレーション**：指定した基準（ベースライン）に対して不足しているパッチを自動的にインストールする
- SSM ドキュメントを実行する過程で Python モジュール（Linux/macOS）または PowerShell モジュール（Windows）を S3 からダウンロードして実行する



マネージドノード上で実行される処理

- Scan や Install の処理自体は OS 標準の仕組みを使用
  （例：Windows の場合は Windows Update API、RHEL の場合は yum / dnf）
- マネージドノードからパッチリポジトリへのネットワークアクセスが必要
  - Windows の場合、Windows Update カタログのサイトまたは Windows Server Update Services (WSUS) へのアクセスが必要
  - Linux の場合、マネージドノードに設定されているデフォルトのリポジトリ以外のソースリポジトリを代替リポジトリとして指定可能
    https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-alternative-source-repository.html

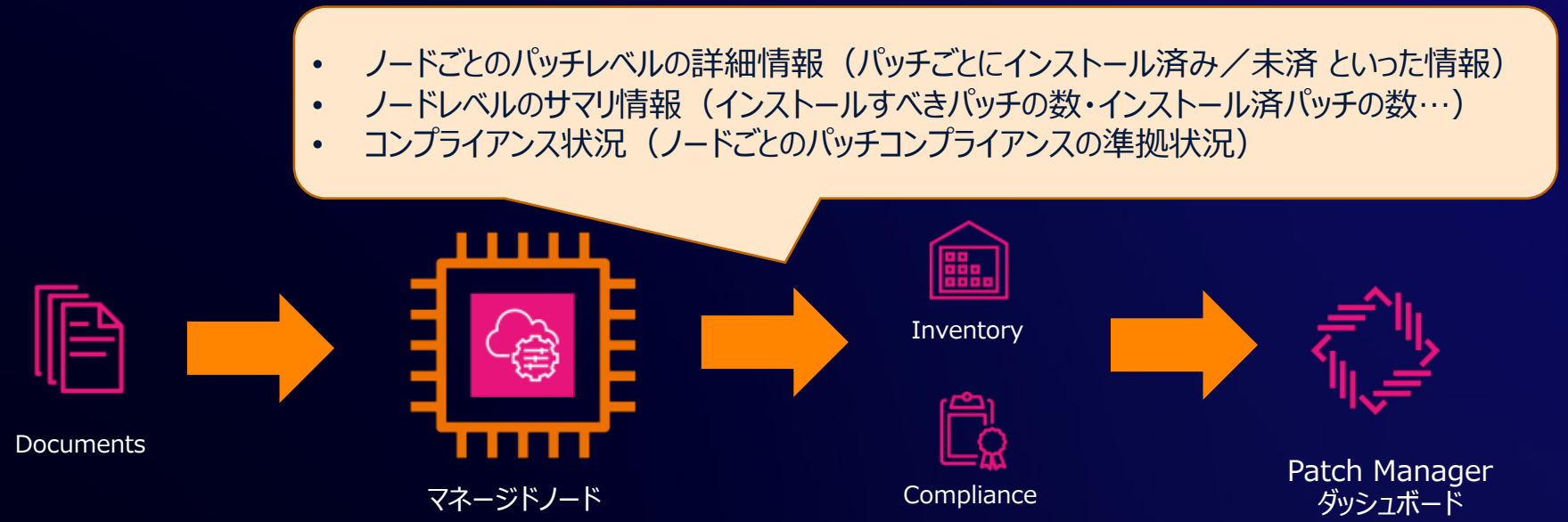


SSM ドキュメントの実行方法

- SSM ドキュメントは SSM Run Command によって起動される
- Maintenance Windows や State Manager によって Run Command をスケジュール実行することが一般的
  - 後述の「パッチポリシー」を使用する場合 State Manager が自動的にセットアップされる
  - EventBridge Scheduler によるシンプルなスケジュール実行も可能
- Patch Manager でオンデマンドに「今すぐパッチ適用」することも可能
  - 単発実行の State Manager が自動的にセットアップされる

パッチオペレーションの実行結果

- パッチの Scan/Install 結果は SSM Inventory や SSM Compliance の API を通じて記録される
- Patch Manager のダッシュボード画面でパッチ適用の状況や、 Inventory で各ノードのパッチ単位の適用状況を確認できる

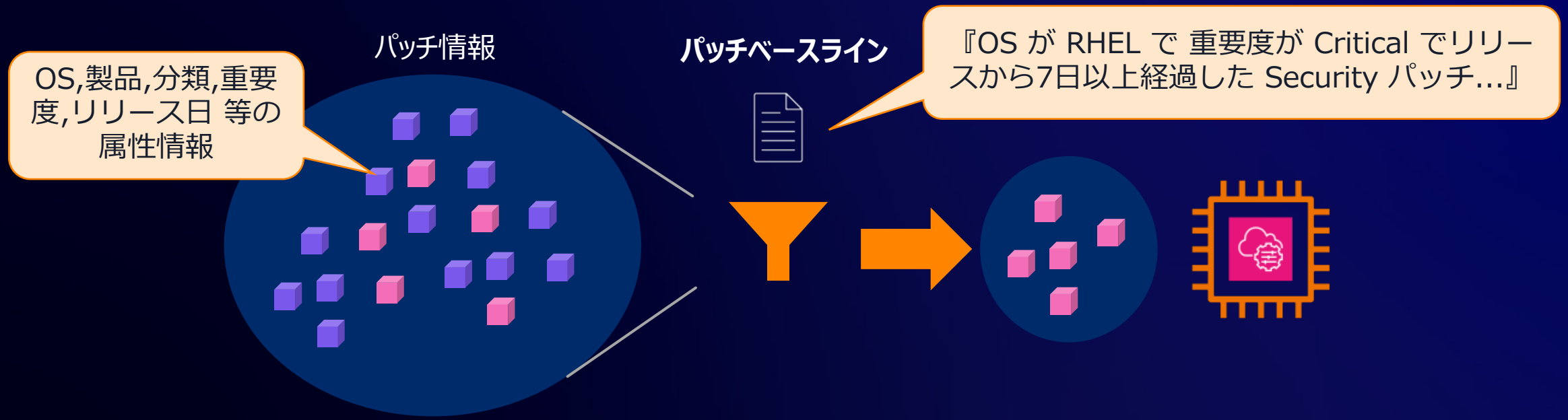


https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-find-noncompliant-nodes.html
https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-compliance-states.html

パッチベースラインと
パッチグループ、パッチポリシー

パッチベースライン

- オペレーティングシステムごとに用意された、適用対象のパッチをフィルタするルール
- AWSが提供する事前定義のパッチベースラインのほか、カスタムで作成することが可能



パッチベースライン - 主要な設定項目

Windows Server の場合の設定画面例

Red Hat Enterprise Linux の場合の設定画面例

- OS（Windows / Ubuntu / SUSE / RHEL など）
- 製品：対象となる OS のバージョンやエディション
- 分類（Security や BugFix など）
- 重要度（Critical や Low など）
- 自動承認の遅延または期限※　※Debian や Ubuntu では設定不可
- コンプライアンスレポートの重要度（重大/高/中/低/情報/未指定）
- 承認済みパッチ/拒否済みパッチ
- 代替パッチソースリポジトリ（Linux の場合）

- ➢ 対象の OS によって設定可能項目が若干異なる
- ➢ Windows の場合、OS のパッチだけでなく Microsoft の提供するアプリケーション（SQLServer や Exchange など）のパッチに関するルールも作成可能

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

パッチベースラインとマネージドノードの関連付け

パッチグループ

パッチポリシーを使用しない従来の方式

- マネージドノードに「**Patch Group**」または「**PatchGroup**」タグを設定
- タグの値に応じてパッチベースラインを紐付ける

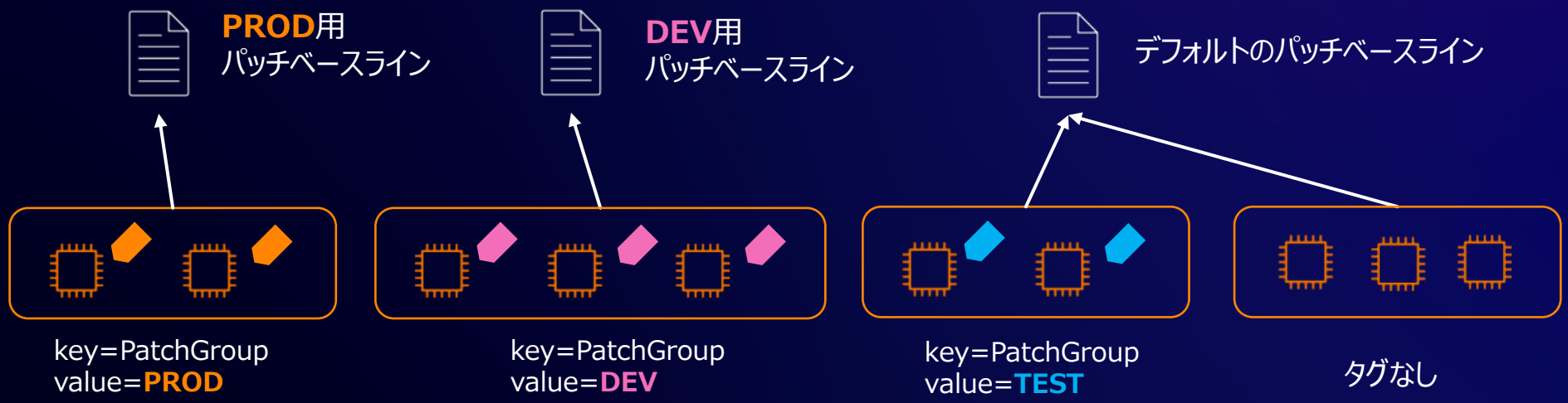
パッチポリシー

広範囲なパッチ適用オペレーションを
簡易かつ一元的に制御できる新しい方式

- パッチポリシーの適用範囲を指定する
  - 組織全体
  - OU/リージョン指定
  - 現在のアカウント
- ターゲットの OS の種類ごとにパッチベースラインを指定する

パッチグループ

- マネージドノードを特定のパッチベースラインへ関連付ける従来からの仕組み
- マネージドノードに「**Patch Group**」または「**PatchGroup**」タグを設定する
  ※スペースあり　※スペース無し

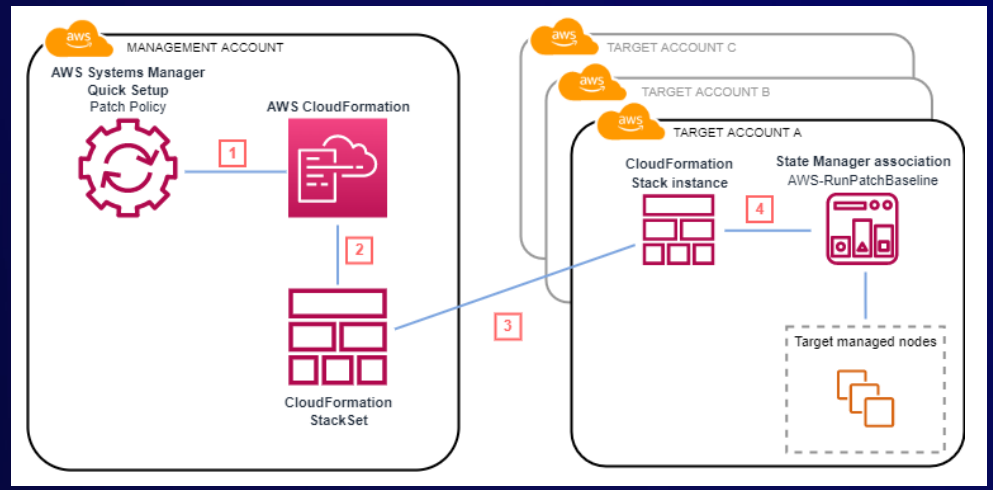


- ✓ マネージドノードごとに 1 つのパッチグループに所属できる
- ✓ 各パッチグループは OS ごとに1つのパッチベースラインへ紐づけできる
- ✓ パッチグループに所属しないマネージドノードはデフォルトのパッチベースラインが適用される

パッチポリシー

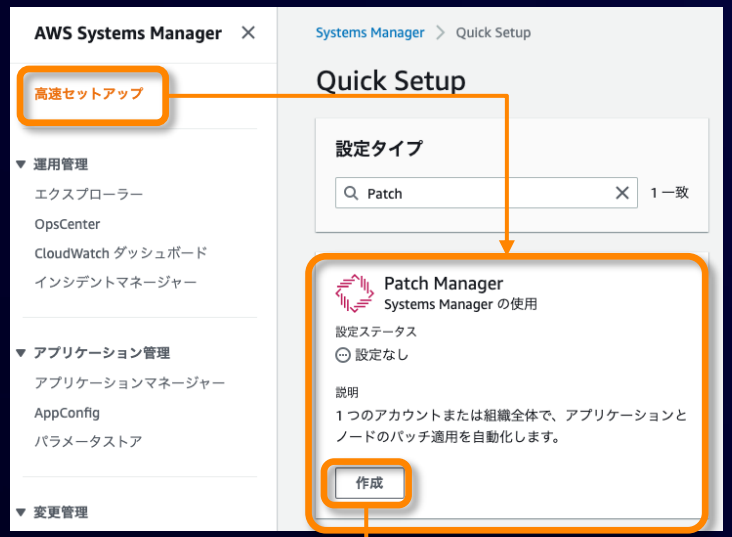
- 2022年12月にリリースされた、マルチアカウント/マルチリージョン環境でのパッチ適用オペレーションを一元的に制御できる機能
- Systems Manager の Quick Setup を使用してセットアップ
- パッチグループの設定は不要で、 OS の種類ごとに AWS マネージドベースラインまたはカスタムベースラインを指定する
- スケジュールに従って AWS-RunPatchBaseline SSM ドキュメントを実行する State Manager 関連付けが対象のアカウント/リージョンに対して自動的にセットアップされる

- 現状、パッチポリシーは一部のリージョンでサポートされていない点に注意



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

パッチポリシーの設定方法 (1/3)



Quick Setup からパッチポリシーの設定を行う

- Scan / Install それぞれの実行スケジュール
- パッチインストール後の再起動の有無
- OS の種類ごとに使用するパッチベースライン
- ログの出力先
- レート制御
- IAM ポリシーの追加
- ターゲット（後述）

パッチポリシーを作成すると、対象のアカウント/リージョンで CloudFormation Stack インスタンスが作成される

Quick Setup パッチポリシーの使用
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-policies.html

パッチポリシーの設定方法 (2/3)

OS の種類ごとに使用するパッチベースラインを指定可能

AWS から提供されるデフォルトのパッチベースラインのほか、カスタムのパッチベースラインも指定可

オペレーティングシステム	ベースラインを選択	ベースライン ID
Alma Linux	AWS-AlmaLinuxDefaultPatchBaseline	pb-0aca46f9a9d062454
Amazon Linux	AWS-AmazonLinuxDefaultPatchBaseline	pb-0221829c157d721d8
Amazon Linux 2	AWS-AmazonLinux2DefaultPatchBaseline	pb-00fda5699d1ae3942
Amazon Linux 2022	AWS-AmazonLinux2022DefaultPatchBaseline	pb-067dab85430494167
Amazon Linux 2023	AWS-AmazonLinux2023DefaultPatchBaseline	pb-0be4fdf9cb953577d
CentOS	AWS-CentOSDefaultPatchBaseline	pb-0b4917141375bc4b5
Debian Server	AWS-DebianDefaultPatchBaseline	pb-0d5f3f8560fc606e3
macOS	AWS-MacOSDefaultPatchBaseline	pb-0ff8843fd26c9bc63
Oracle Linux	AWS-OracleLinuxDefaultPatchBaseline	pb-04ed5d5c38572bb74
Raspberry Pi OS	AWS-RaspbianDefaultPatchBaseline	pb-04e6dbcacfd1dc4ef
Red Hat Enterprise Linux (RHEL)	AWS-RedHatDefaultPatchBaseline	pb-0adf5cb7136a2984d
Rocky Linux	AWS-RockyLinuxDefaultPatchBaseline	pb-05b8b04891f902733
SUSE Linux Enterprise Server (SLES)	AWS-SuseDefaultPatchBaseline	pb-045f39f1765049417
Ubuntu Server	AWS-UbuntuDefaultPatchBaseline	pb-0ec96a11368349171
Windows Server	AWS-DefaultPatchBaseline	pb-04ba050f612fba3a6

パッチポリシーの設定方法 (3/3)

ターゲット：パッチポリシーをデプロイする対象ノード

組織全体

- 組織内のOUおよびリージョン内の全てのマネージドノードを対象とする

OUとリージョンを選択

- 選択した OU とリージョン内の全てのマネージドノードを対象とする
- 選択した OU とリージョン内で、特定のタグの key または key-value を持つマネージドノードを対象とする

現在のアカウント

リージョンを指定

- 選択したリージョン内の全てのマネージドノードを対象とする
- 選択したリージョン内で、特定のタグの key または key-value を持つマネージドノードを対象とする

現在のリージョン

- 全てのマネージドノード
- リソースグループ指定
- ノードタグ指定
- 手動（インスタンスID指定）

Patch Manager で使用する SSM ドキュメント

Patch Manager で使用される SSM ドキュメント

現在、使用が推奨されているのは以下の SSM ドキュメント

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-ssm-documents.html

ドキュメント名	説明	対象OS
AWS-ConfigureWindowsUpdate	Windows Update 機能を設定し、自動アップデートをオンまたはオフにする。パッチベースラインによる制御やパッチのコンプライアンス情報の収集は実施しない	Windows
AWS-InstallWindowsUpdates	Windows Server のマネージドノードにアップデートをインストールする。パッチベースラインによる制御やパッチのコンプライアンス情報の収集は実施しない	Windows
AWS-RunPatchBaseline	ノードをスキャンしてパッチの適用状況を調査したり、ノードにパッチをインストールすることができる。パッチベースラインによる制御やパッチのコンプライアンス情報の収集を行う	Windows/Linux/macOS
AWS-RunPatchBaselineAssociation	AWS-RunPatchBaselineドキュメントと似ているが、BaselineTags と呼ばれるパラメータを使用することで特定のパッチベースラインを選択することができる。EC2インスタンス以外の、ハイブリッド環境のノードは未サポート	Windows/Linux/macOS
AWS-RunPatchBaselineWithHooks	AWS-RunPatchBaseline ドキュメントをラップしている。パッチサイクル中の3つのポイント（パッチのインストール前、インストール後、再起動後）で他のSSMドキュメントを実行することができる	Windows/Linux/macOS

上記以外の SSM ドキュメント（レガシーSSMドキュメント）については以下のドキュメント参照
https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-ssm-documents.html#patch-manager-ssm-documents-legacy

Patch Manager で使用される SSM ドキュメント

現在、使用が推奨されているのは以下の SSM ドキュメント

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-ssm-documents.html

ドキュメント名	説明	対象OS
AWS-ConfigureWindowsUpdate	Windows Server への基本的なパッチ適用または Windows Update の設定のみを実施したい場合に使用する	
AWS-InstallWindowsUpdates		
AWS-RunPatchBaseline	**通常はこのドキュメントを使用すると良い** （パッチポリシーを設定する場合、このドキュメントが使用される）	
AWS-RunPatchBaselineAssociation	主に Quick Setup ホスト管理設定 機能（後述）によって使用されることを想定している	
AWS-RunPatchBaselineWithHooks	ライフサイクルフック処理をカスタマイズしたい場合に使用する	

上記以外の SSM ドキュメント（レガシーSSMドキュメント）については以下のドキュメント参照

https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-ssm-documents.html#patch-manager-ssm-documents-legacy

Patch Manager の開始方法

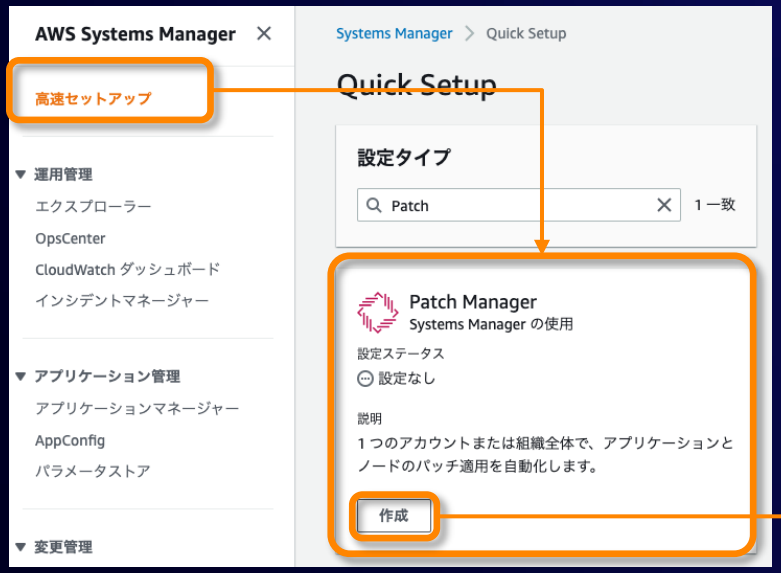
Patch Manager の一般的な開始方法

- Quick Setup でパッチポリシーを設定する
- Quick Setup でホスト管理オプションを設定する
- パッチ適用向けのメンテナンスウィンドウを作成する
- Patch Manager の「今すぐパッチ適用」からオンデマンドのパッチオペレーションを実行する

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

Quick Setup でパッチポリシーを設定する

- Scan / Install のスケジュール、ターゲット、パッチベースライン 等の設定を行う
- 一度の操作で複数のアカウント、複数のリージョンに対して設定内容を展開できるのが特徴



Quick Setup パッチポリシーの使用
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-policies.html

Quick Setup でホスト管理オプションを設定する

- SSM Agent のアップデートやインベントリ収集の設定に加え、パッチのスキャンのスケジュールを簡単に設定できる
- インストールのオペレーションは実行できない

Amazon EC2 ホスト管理
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/quick-setup-host-management.html

パッチ適用向けのメンテナンスウィンドウの作成

- パッチポリシーが登場する以前の一般的なシナリオ
- 所定のタイムウィンドウ内で複数のターゲットに対して SSM ドキュメントを実行
  - SSM ドキュメントを直接実行するほか、Automation ランブックや State Manager の実行も可能
- セットアップの手間はかかるがカスタマイズしやすい方法

Maintenance Windows※

Run Command

※要件に応じてその他の
スケジューラーを使用することも可能

チュートリアル: パッチ適用向けのメンテナンスウィンドウの作成 (コンソール)
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-patch-mw-console.html

「今すぐパッチ適用」からオンデマンドのパッチオペレーションを実行

- パッチオペレーションをオンデマンドで即時実行したい場合に有用

マネージドノードへのオンデマンド パッチ適用
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-patch-now-on-demand.html

Patch Manager の開始方法の比較

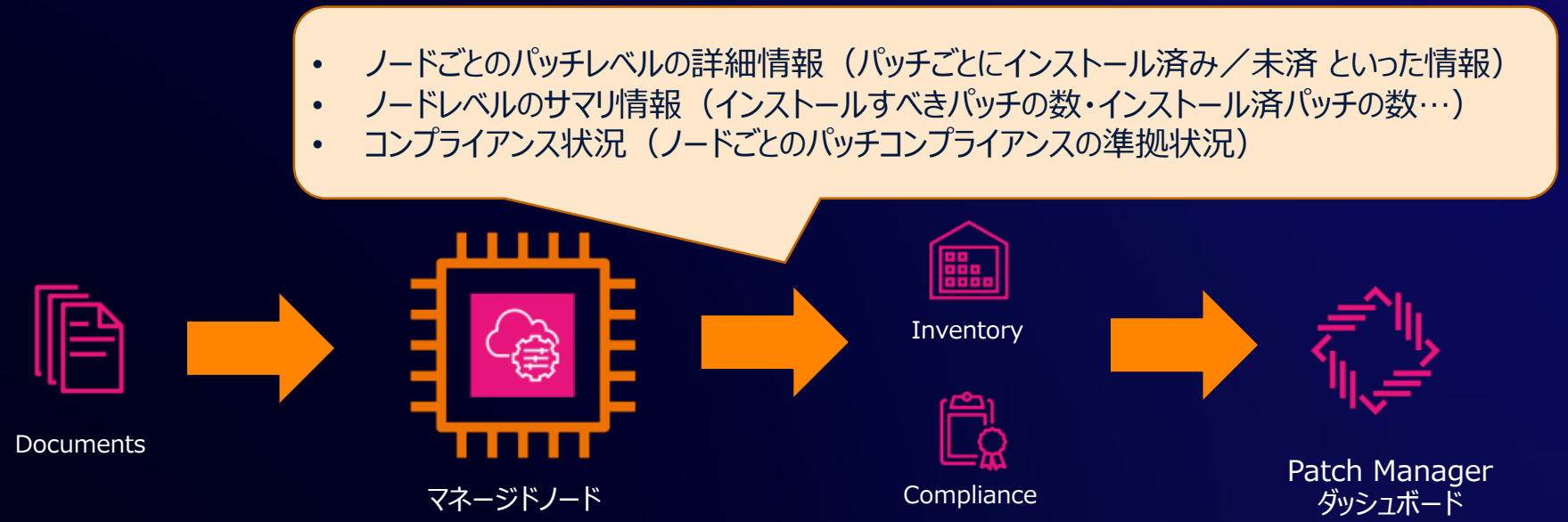
比較項目	パッチポリシー	ホスト管理オプション	メンテナンスウィンドウ	今すぐパッチ適用
Scan/Install	どちらも可	**Scan のみ**	どちらも可	どちらも可
スケジュール	設定可（State Manager 関連付けが自動でセットアップされる）	設定可（State Manager 関連付けが自動でセットアップされる）	設定可（**自分でメンテナンスウィンドウ等を作成する必要がある**）	**即時実行のみ**（即時実行用の State Manager 関連付けが自動でセットアップされる）
パッチベースライン	OSごとに指定したパッチベースラインを使用する	所属するパッチグループに応じたパッチベースラインが使用される	所属するパッチグループに応じたパッチベースラインが使用される。BaselineOverride パラメータ(後述)で上書きすることも可能	所属するパッチグループに応じたパッチベースラインが使用される
SSM ドキュメント	AWS-RunPatchBaseline	AWS-RunPatchBaselineAssociation	任意のSSMドキュメントを指定可	AWS-RunPatchBaseline または AWS-RunPatchBaselineWithHooks
対象ノード	マネージドノード	EC2のマネージドノード**（ハイブリッド環境のノードは対象外）**	マネージドノード	マネージドノード
マルチアカウント／マルチリージョン	**管理アカウント**から一元的に設定可能	**管理アカウント**から一元的に設定可能	アカウントやリージョンごとに設定が必要	アカウントやリージョンごとに実行が必要

実行結果の確認

パッチオペレーションの実行結果

再掲

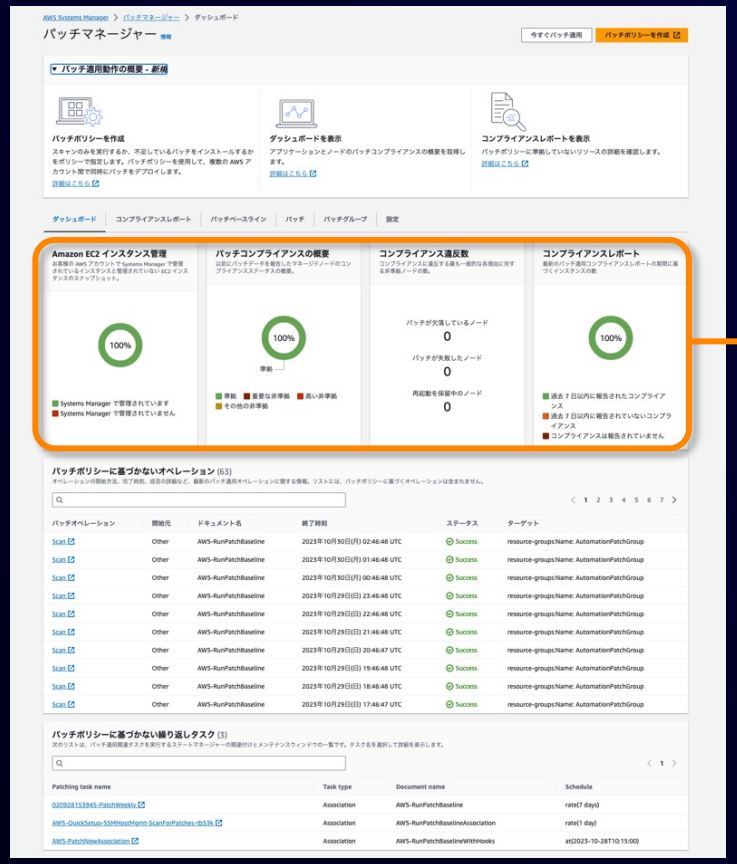
- パッチの Scan/Install 結果は SSM Inventory や SSM Compliance の API を通じて記録される
- Patch Manager のダッシュボード画面でパッチ適用の状況や、 Inventory で各ノードのパッチ単位の適用状況を確認できる

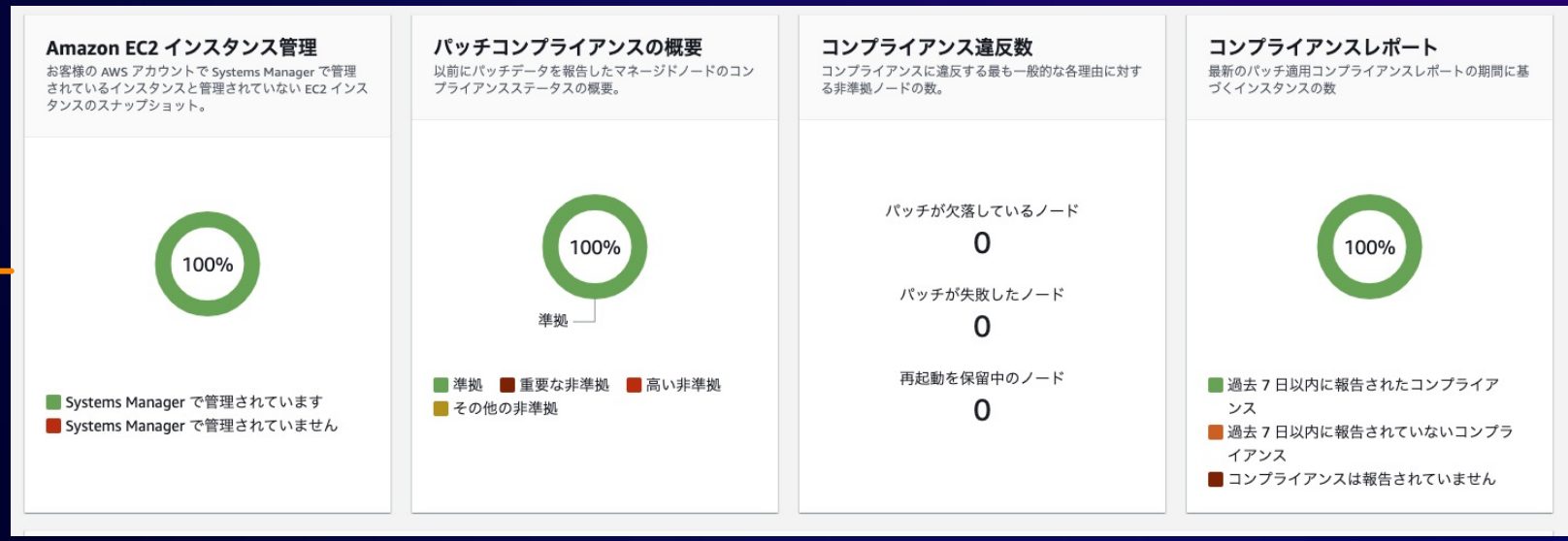


https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-find-noncompliant-nodes.html
https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-compliance-states.html

パッチダッシュボード (1/3)

Patch Manager のパッチダッシュボード画面でパッチオペレーションのサマリを確認可能

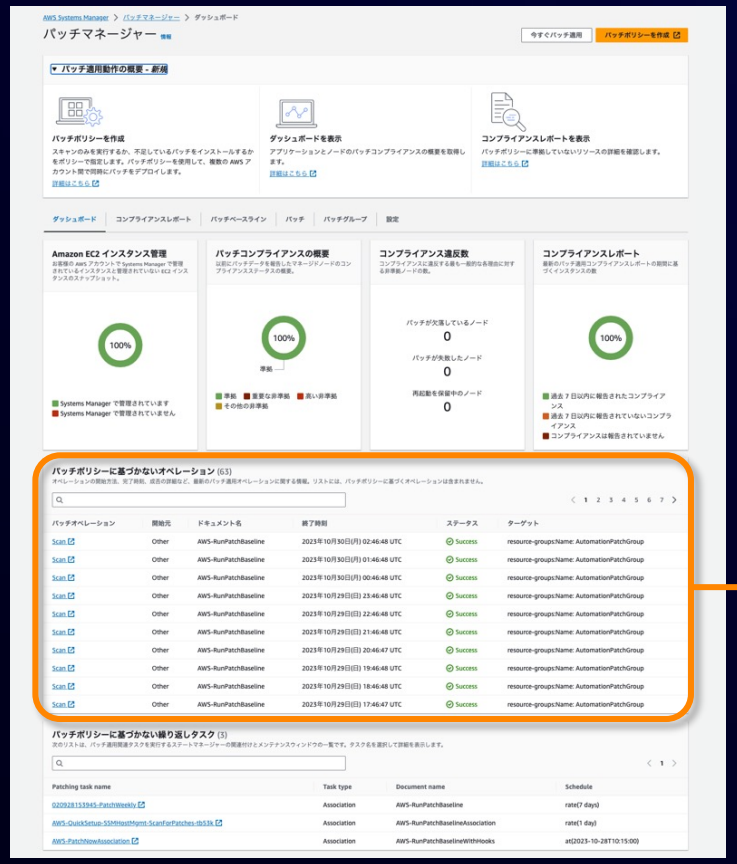




- マネージドノード/非マネージドノード である EC2インスタンスの台数
- パッチコンプライアンスのステータス概要
- コンプライアンス非準拠のノード数
- 最新のパッチ適用コンプライアンス報告状況

パッチダッシュボード (2/3)

パッチポリシーに基づかないオペレーション



パッチポリシーに基づかないオペレーション (63)

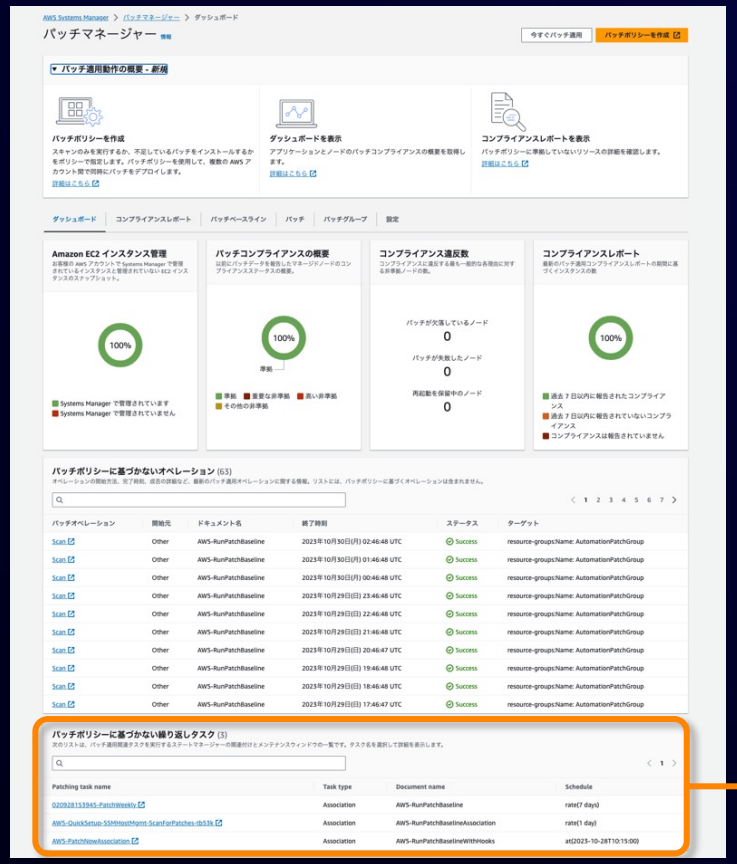
オペレーションの開始方法、完了時刻、成否の詳細など、最新のパッチ適用オペレーションに関する情報。リストには、パッチポリシーに基づくオペレーションは含まれません。

パッチオペレーション	開始元	ドキュメント名	終了時刻	ステータス	ターゲット
Scan	Other	AWS-RunPatchBaseline	2023年10月30日(月) 02:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	Other	AWS-RunPatchBaseline	2023年10月30日(月) 01:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	Other	AWS-RunPatchBaseline	2023年10月30日(月) 00:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	Other	AWS-RunPatchBaseline	2023年10月29日(日) 23:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup
Scan	Other	AWS-RunPatchBaseline	2023年10月29日(日) 22:46:48 UTC	Success	resource-groups:Name: AutomationPatchGroup

- パッチポリシー以外の方法で実行されたパッチ適用オペレーションの履歴

パッチダッシュボード (3/3)

パッチポリシーに基づかない繰り返しタスク



パッチポリシーに基づかない繰り返しタスク (3)

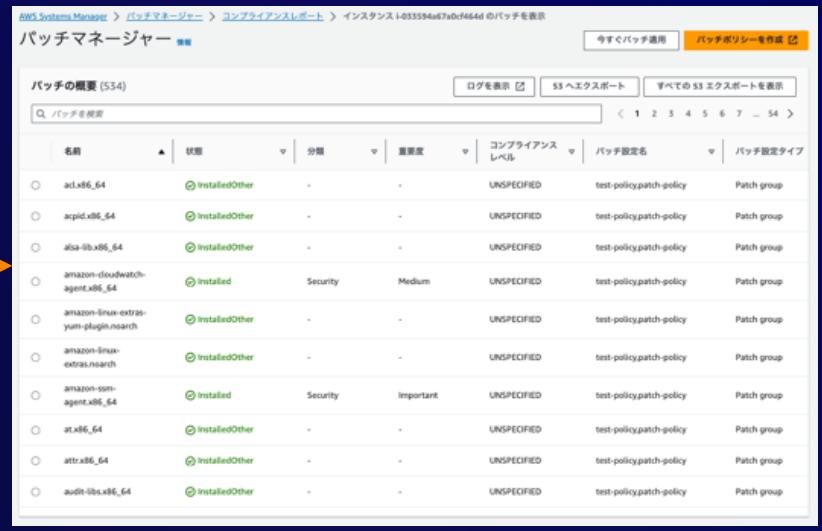
次のリストは、パッチ適用関連タスクを実行するステートマネージャーの関連付けとメンテナンスウィンドウの一覧です。タスク名を選択して詳細を表示します。

Patching task name	Task type	Document name	Schedule
020928153945-PatchWeekly	Association	AWS-RunPatchBaseline	rate(7 days)
AWS-QuickSetup-SSMHostMgmt-ScanForPatches-tb53k	Association	AWS-RunPatchBaselineAssociation	rate(1 day)
AWS-PatchNowAssociation	Association	AWS-RunPatchBaselineWithHooks	at(2023-10-28T10:15:00)

- パッチポリシー以外の方法で設定されているパッチ適用関連タスク
- パッチ適用関連タスクを実行する State Manager 関連付け または メンテナンスウィンドウ の一覧が表示される

コンプライアンスレポート (1/2)

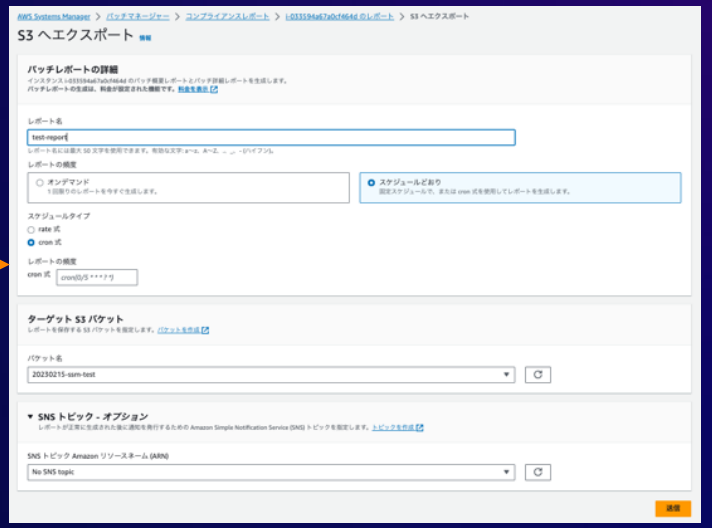
Patch Manager のコンプライアンスレポート画面

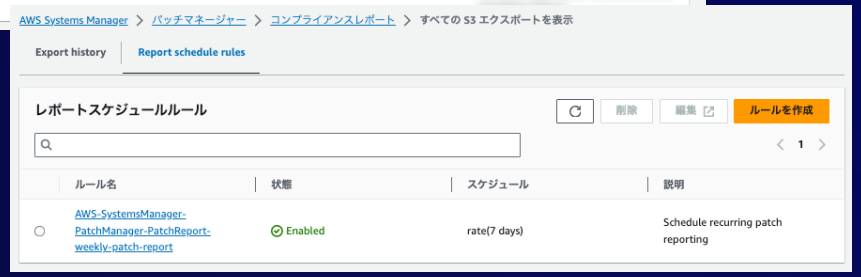


- Run Command の実行結果や、ノードごとにパッチの明細レベルでの適用状況を確認可能

コンプライアンスレポート (2/2)

パッチレポート



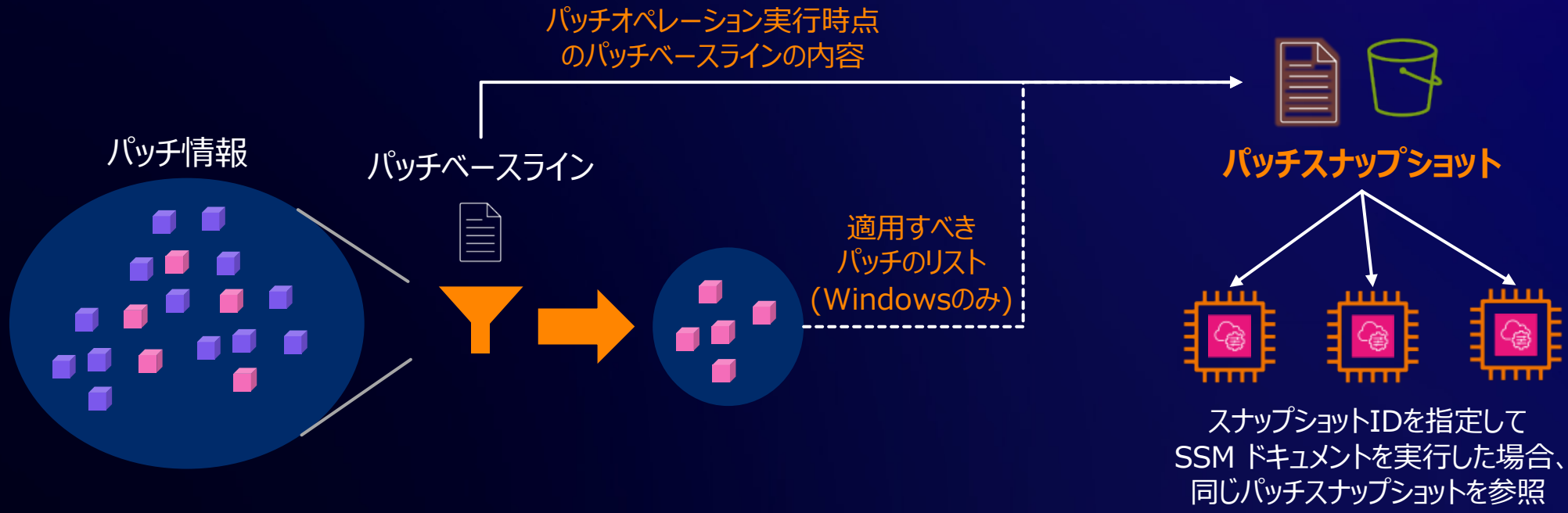


- オンデマンドまたはスケジュールでのレポート出力（S3へのCSVファイル出力）が可能
- レポート出力は Automation ランブック（AWS-ExportPatchReportToS3）が実行される

TIPS

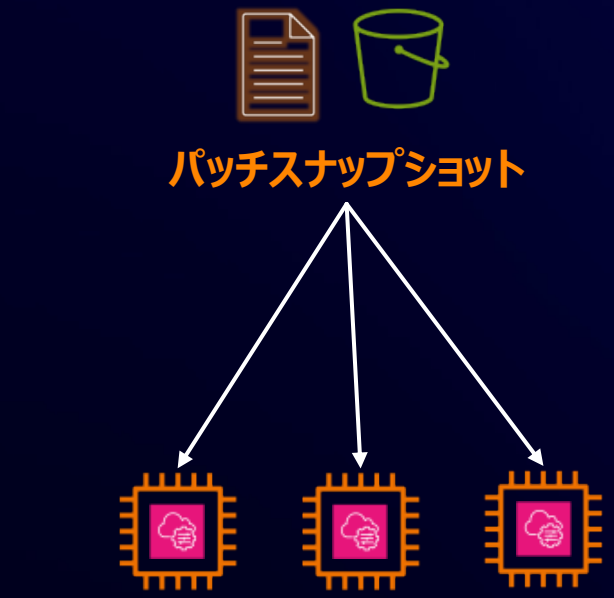
パッチスナップショット (1/2)

- パッチオペレーション実行時点のパッチベースラインのスナップショット
- 一時的に Systems Manager サービスが管理する S3 バケットへ保存される
- 同じスナップショット ID を指定して SSM ドキュメントを実行すると、同じパッチスナップショットを使用する



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-aws-runpatchbaseline.html#patch-manager-aws-runpatchbaseline-parameters-snapshot-id

パッチスナップショット (2/2)



GetDeployablePatchSnapshotForInstance API
& 署名付きURLによるS3アクセス

- AWS-RunPatchBaseline や AWS-RunPatchBaselineWithHooks SSM ドキュメントがスナップショット ID パラメータをサポート
- Maintenance Windows から SSM ドキュメントを実行する場合は自動的にスナップショット ID が設定されるため考慮不要
- パッチスナップショットの取得には S3 署名付きURLが使用される（長期間のスナップショットの保存は不向き）

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-aws-runpatchbaseline.html
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-aws-runpatchbaselinewithhooks.html

InstallOverrideList

- パッチベースラインでフィルタされたパッチのリストを上書きできる YAML 形式のリスト
- S3 に YAML ファイルを保存しておき、ファイルのパスをパラメータとして指定する
- インストールするパッチを詳細に指定することができるが、Scan オペレーションでは使用できない

＜ InstallOverrideList のサンプル書式>

```
patches:
    -
        id: 'kernel.x86_64'
    -
        id: 'bind*.x86_64'
        title: '32:9.8.2-0.62.rc1.57.amzn1'
    -
        id: 'glibc*'
    -
        id: 'dhclient*'
        title: '*12:4.1.1-53.P1.28.amzn1'
    -
        id: 'dhcp*'
        title: '*10:3.1.1-50.P1.26.amzn1'
```

InstallOverrideList のサンプル書式はドキュメントも参照
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-aws-runpatchbaseline.html#patch-manager-aws-runpatchbaseline-parameters-installoverridelist

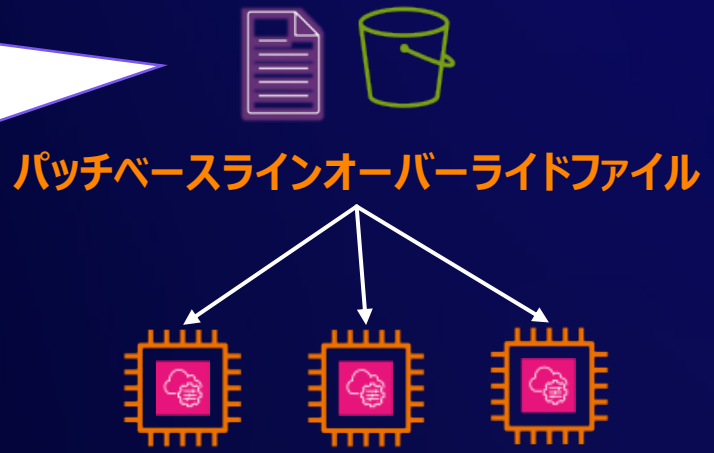
BaselineOverride

- パッチベースラインの設定を上書きすることができる
- S3 に JSON ファイルとして格納しておき、ファイルのパスをパラメータとして指定する
- パッチポリシーをセットアップした環境ではこのパラメータが使用されている。これにより、クロスアカウント/クロスリージョンで同じ設定のパッチベースラインを適用できる
- パッチベースラインオーバーライドファイルのサンプルや生成方法はドキュメント参照

＜パッチベースラインオーバーライドファイル＞

```
[
    {
        "ApprovalRules": {
            "PatchRules": [
                {
                    "ApproveAfterDays": 0,
                    "ComplianceLevel": "UNSPECIFIED",
                    "EnableNonSecurity": false,
                    "PatchFilterGroup": {
                        "PatchFilters": [
                            {
                                "Key": "PRODUCT",
                                "Values": [
                                    "*"
                                ]
                            },
```

:



https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-baselineoverride-parameter.html

Security Hub との連携

- Patch Manager は Security Hub との統合をサポート
- Patch Manager は、マネージドノードが非準拠であることを検出した場合に Security Hub へ検出結果を転送
- 検出結果にはパッチのサマリー結果が含まれる

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-security-hub-integration.html

異なる環境間で同じパッチを適用したい場合

開発環境と本番環境など、複数の環境に対して異なるタイミングで同じパッチを適用する場合、以下の方法がある

パッチベースラインの「自動承認」を使用

自動承認の遅延日数や期限日を指定し、パッチがリリースまたは最後に更新されてから待機する日数や期限日を指定できる

- Ubuntu や Debian は自動承認オプションは未サポート
- Amazon Linux のパッケージのリリース日と更新日の計算方法ついては以下のドキュメントも参照
  https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-release-dates.html
- Windows Server の場合、更新プログラムの置き換えや更新日時を指定しないアプリケーションパッチの提供が発生する場合がある
  https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-selecting-patches.html （Windows Server タブの内容を参照）

InstallOverrideList オプションを使用

適用したいパッチのリストを明示的に指定する

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/patch-manager-override-lists.html

料金

Patch Manager の料金

- パッチオペレーション

タスク	Amazon EC2 インスタンス	ハイブリッド環境のインスタンス
OSのパッチング	追加料金なし	追加料金なし
Linux アプリケーションのパッチング	追加料金なし	追加料金なし
Microsoft アプリケーションのパッチング	追加料金なし	アドバンスドオンプレミスインスタンスティアが必要。（アドバンスドオンプレミスインスタンスごとに時間あたり 0.00695 USD）

- パッチレポート

  レポート作成時は Systems Manager Automation が実行されるため、Systems Manager Automation の料金が発生する

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

まとめ

まとめ

Systems Manager Patch Manager は、マネージドノードにパッチを適用するプロセスを自動化

- 自動承認のルールを「パッチベースライン」として定義
  - 承認済みおよび拒否済みパッチの選択可能なリストのほか、リリースからの経過日数や特定日以前のパッチを自動承認することができる
- 定期的なパッチのスキャンとインストール
  - Maintenance Windows , State Manager , EventBridge Scheduler を使用してスケジュール実行が可能
- 緊急度の高いパッチへの迅速な対応も可能
- パッチのレポートによりコンプライアンス状況を一元的に把握

AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
  - https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/
  - https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

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

内容についての注意点

- 本資料では資料作成時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (https://aws.amazon.com/) にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- 技術的な内容に関しましては、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!