
aws
SUMMIT
ONLINE
JAPAN

サーバ管理を楽にしよう！
AWS Systems Managerの基本ハンズオン

石橋 香代子

アマゾン ウェブサービス ジャパン
技術統括本部 エンタープライズソリューション本部
ソリューションアーキテクト

aws SUMMIT ONLINE

自己紹介

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

本セッションについて

➢ 目的

・AWS Systems Manager の基本機能をさわってみて、
どのようなことができるのかを体感いただくことを目的としています。

➢ 注意

・AWS Systems Managerをまだお使いでない方で、概要を掴みたい方を対象としています。アドバンストな使い方は取り上げておりません。

・本セッションの中では、各シナリオを実現する上で最低限抑えておくべきことのみをご説明します。各機能の詳細はお話ししませんので、AWS公式ドキュメントや、BlackBelt資料などをご参照ください。

AWS公式ドキュメント：AWS Systems Manager ユーザーガイド
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/what-is-systems-manager.html

BlackBelt Online Seminar (AWS Systems Manager) ：
SlideShare : https://www.slideshare.net/AmazonWebServicesJapan/20200212-aws-black-belt-online-seminar-aws-systems-manager
PDF : https://d1.awsstatic.com/webinars/jp/pdf/services/20200212_AWSBlackBelt_SystemsManager_0214.pdf
Youtube : https://www.youtube.com/watch?v=UXSbh4Wsp7c&feature=youtu.be

ハンズオン実施にあたっての注意点

- ハンズオンでは、AWSの各種サービスの利用、リソースの作成を行います。無料枠を超える場合、ご利用料金が発生することをあらかじめご認識ください。
- セッション終了後のリソース削除についても、お客様の責任でご実施いただくようお願いいたします。
- リソースの削除方法につきましては、ハンズオン資料に手順をつけておりますのでそちらもご参照ください。
- マネジメントコンソールは収録時点のものとなります。差異がある場合がございますのであらかじめご了承ください。
- お客様所有かつ自由に構成、検証などができる AWS アカウントにて実施をお願いいたします。可能であれば、ハンズオン用にAWSアカウントを取得いただくことをお勧めします。

アジェンダ

1. AWS Systems Manager概要
2. SSM利用にあたっての準備
3. セッションマネージャーによるサーバアクセス
4. Run Commandによるサーバ群へのコマンドの一括投入
5. インスタンスへのOSパッチの自動適用
6. ハンズオン環境のCleanup

AWS Systems Manager概要

aws SUMMIT ONLINE

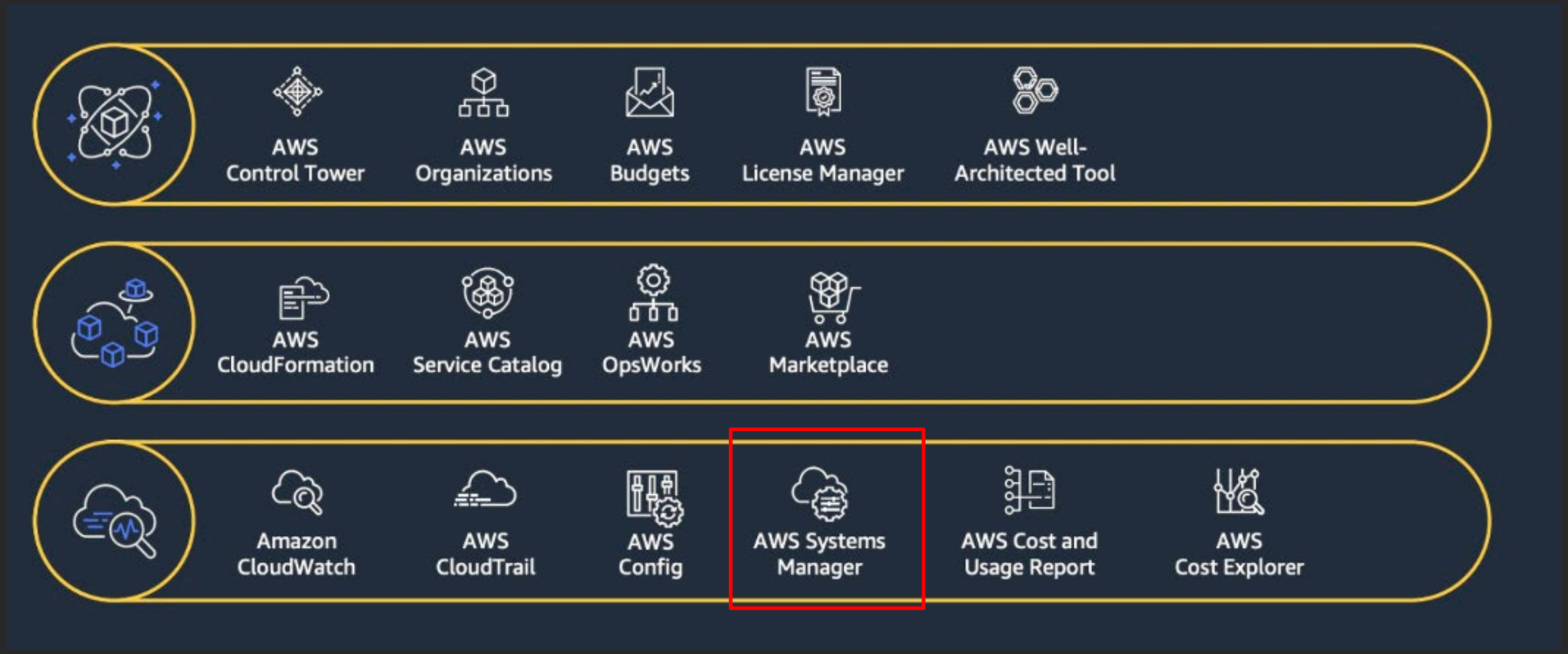
AWS マネジメント & ガバナンス サービス

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

ビジネスアジ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



ビジネスアジ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

高速セットアップ	インスタンスをSSMで管理するよう自動構成

➢ 運用管理

エクスプローラー	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
CloudWatch ダッシュボード	CloudWatchによるダッシュボードの表示
PHD	Trusted AdvisorとPersonal Health Dashboardの表示

*XRXA=CrossRegion CrossAccount

➢ アプリケーション管理

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

自動化（Automation）	AWS環境全体に対する自動化処理の実行
カレンダーの変更 （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 (1/2)

➢ 全体

高速セットアップ	インスタンスをSSMで管理するよう自動構成

➢ 運用管理

エクスプローラー	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
CloudWatch ダッシュボード	CloudWatchによるダッシュボードの表示
PHD	Trusted AdvisorとPersonal Health Dashboardの表示

*XRXA=CrossRegion CrossAccount

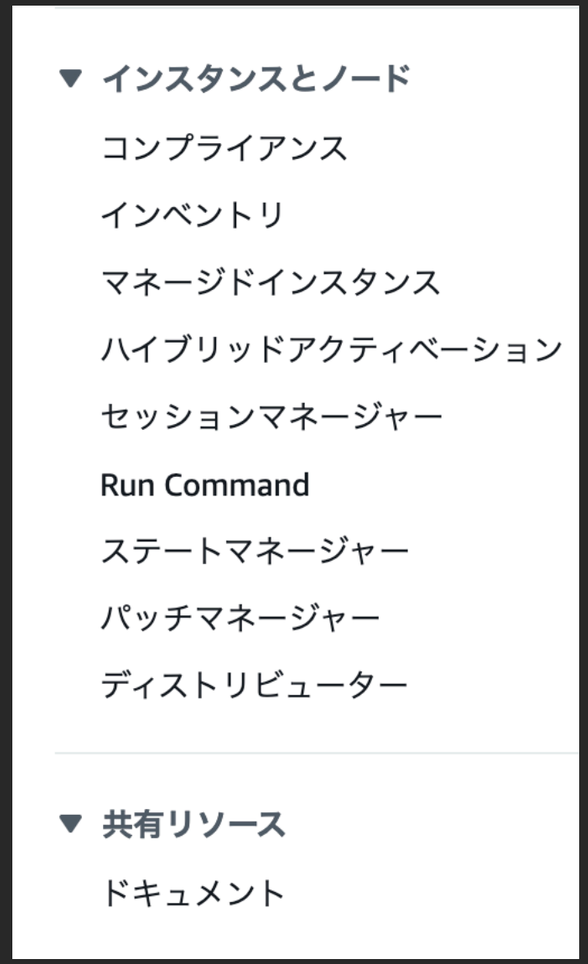
➢ アプリケーション管理

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

自動化（Automation）	AWS環境全体に対する自動化処理の実行
カレンダーの変更 （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)



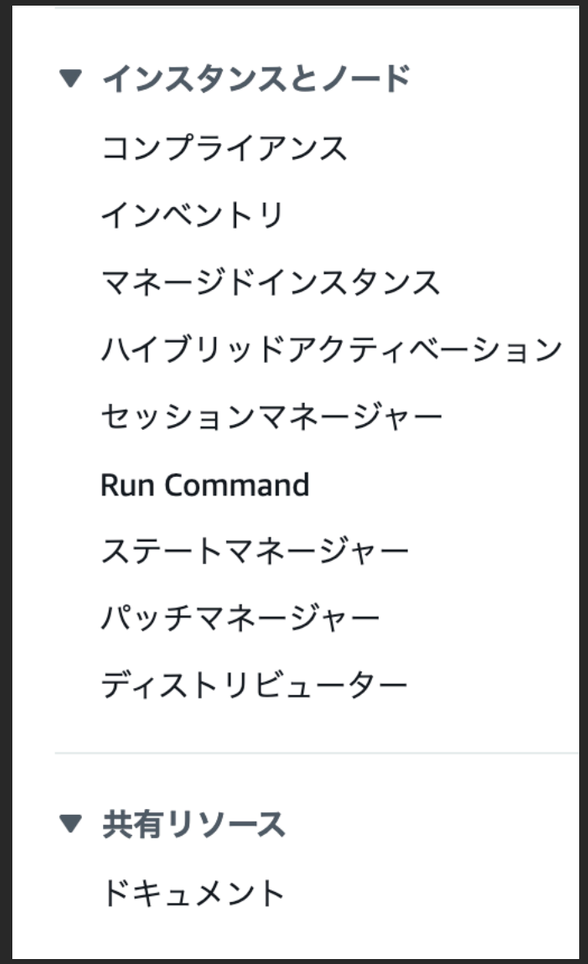
➢ インスタンスとノード

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	指定ルールに基づきサーバ群にパッチを適用する
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

AWS SSM：Features (2/2)



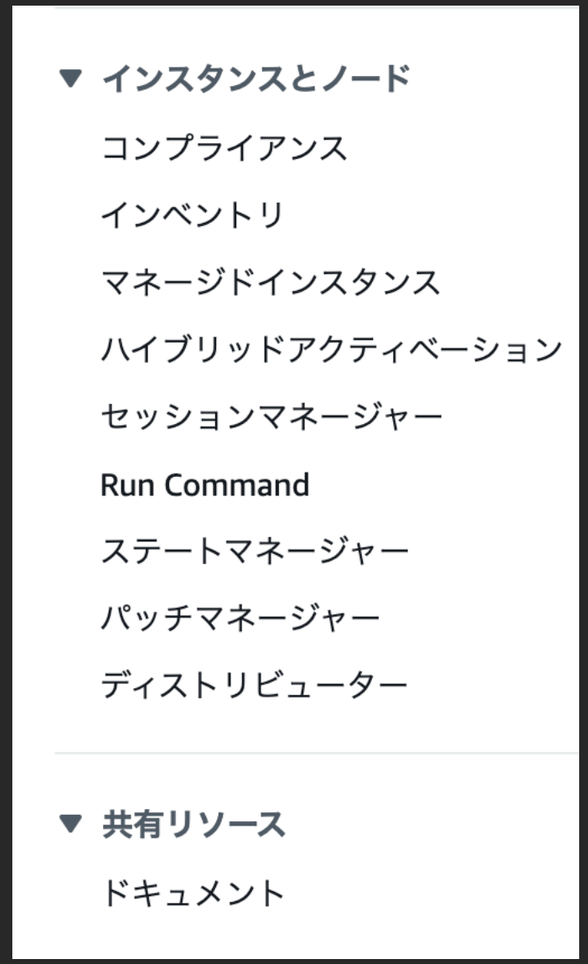
➢ インスタンスとノード

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	指定ルールに基づきサーバ群にパッチを適用する
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

AWS SSM：Features (2/2)



➢ インスタンスとノード

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[illegible]をSSM管理下に入れる
セッションマネージャー	[illegible]
Run Command	[illegible]
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	指定ルールに基づきサーバ群にパッチを適用する
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

HOL-08
「サーバのソフトウェア構成を可視化しよう！
SystemsManager & QuickSightハンズオン」

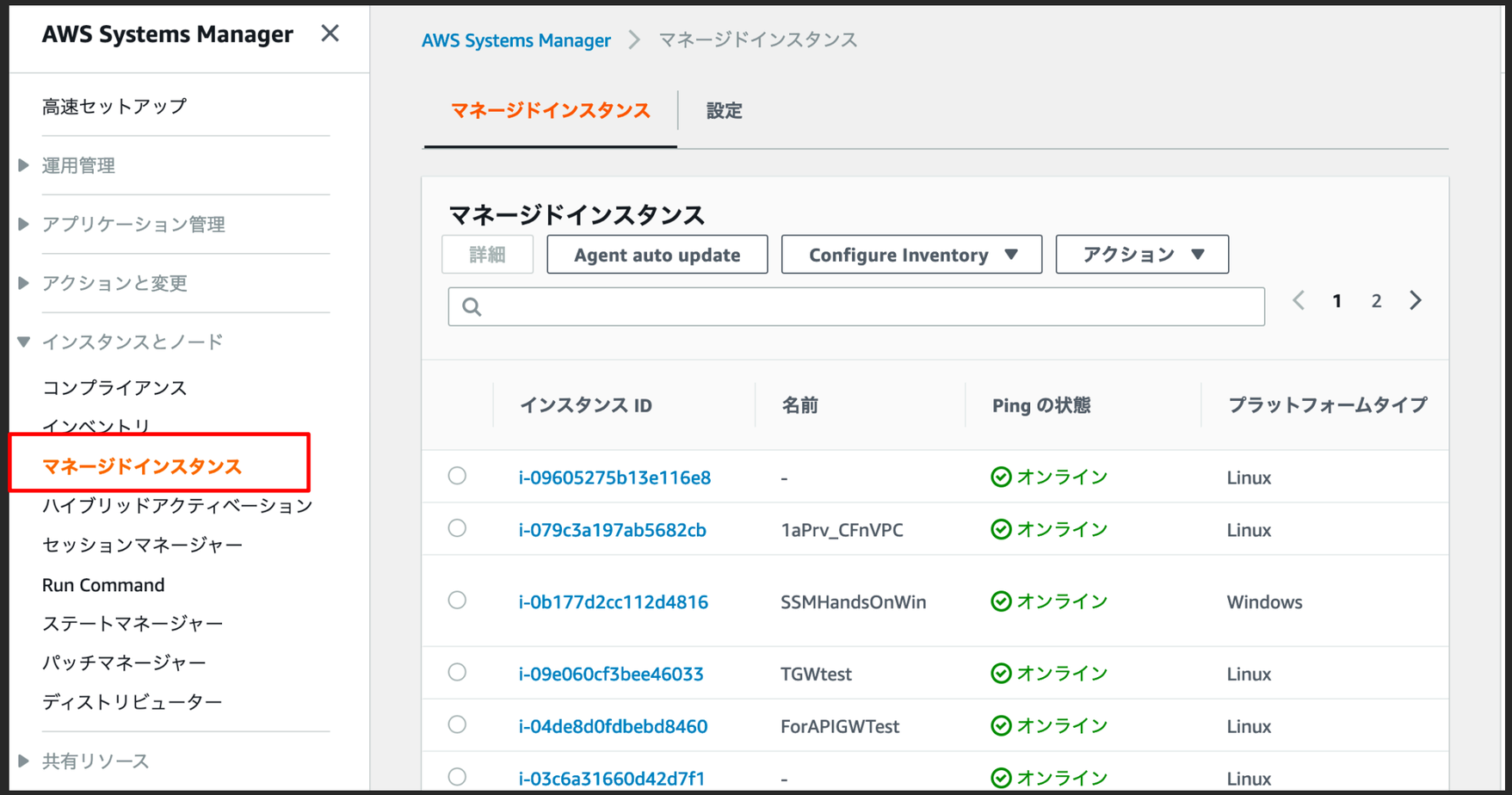
➢ 共有リソース

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

SSM利用にあたっての準備

aws SUMMIT ONLINE

まずは、マネージドインスタンスにしよう



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められる。

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

① SSM Agentの導入

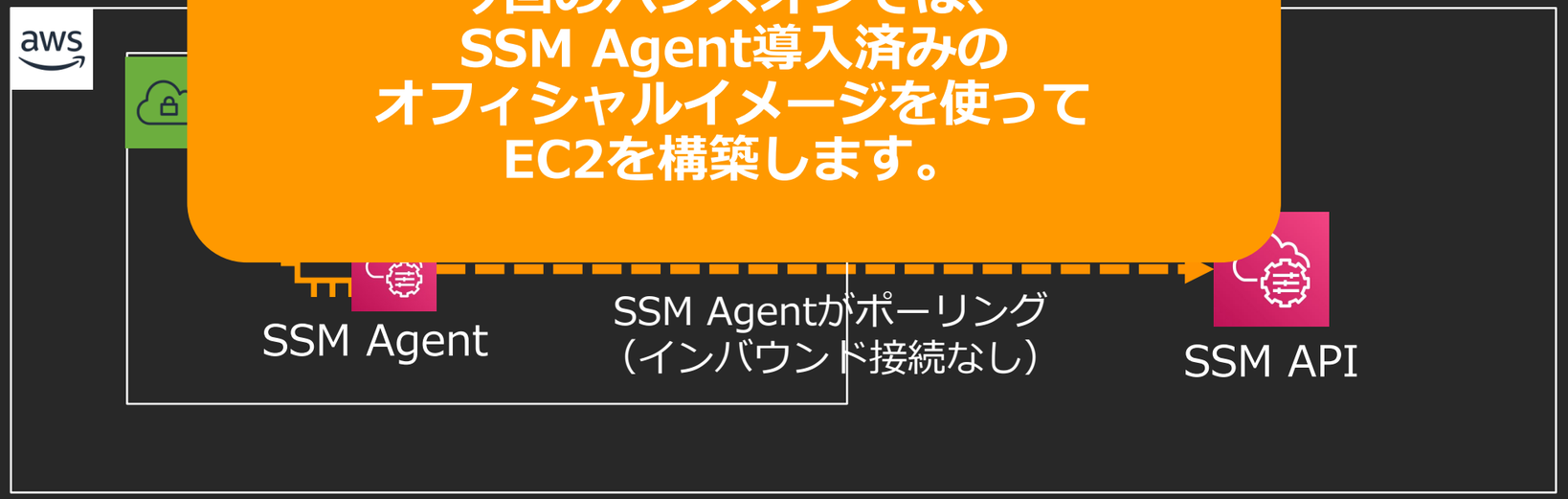
- SSM AgentがSSM APIと連携し各種操作、コントロールを行う。
- Amazon LinuxやWindows、Ubuntu Serverのオフィシャルイメージには導入済み
  - それ以外のAMI、及びオンプレミスサーバは、手動でインストール
- 幅広い対応OS
  - WindowsServer2003～、RHEL6.0～、Ubuntu12.04～、Raspbian(Raspberry Pi OS) 等）
    https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/prereqs-operating-systems.html

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

① SSM 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～、Ra spberry Pi OS) 等）
    https://docs.aws.amazon.co -operating-systems.html

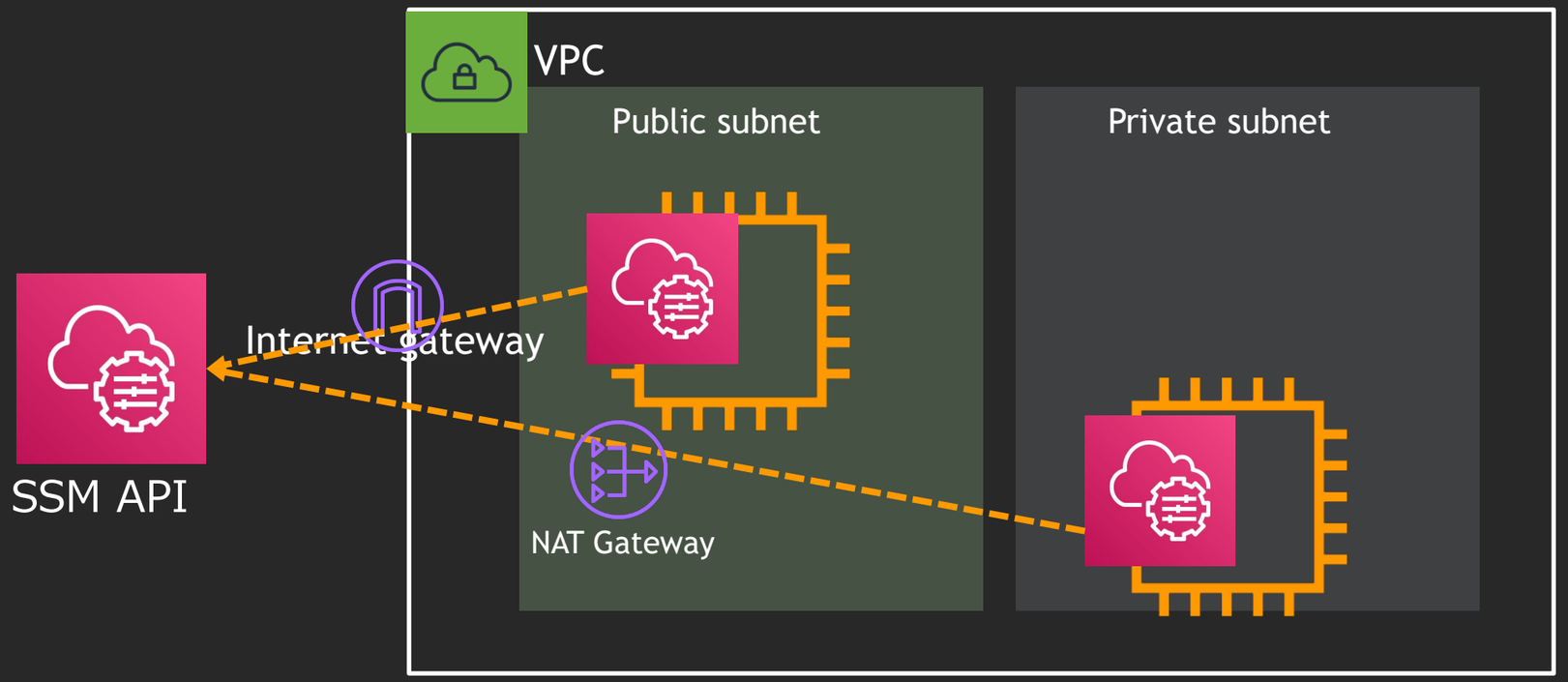
**今回のハンズオンでは、
SSM Agent導入済みの
オフィシャルイメージを使って
EC2を構築します。**



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

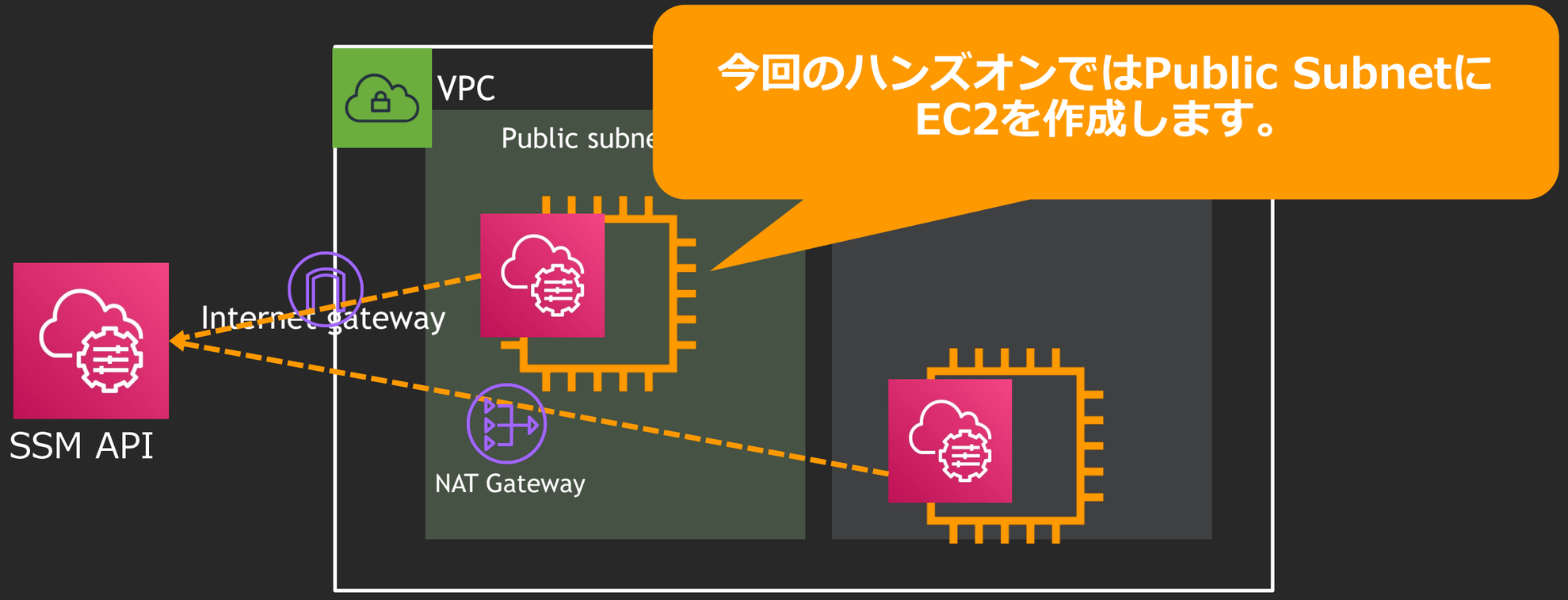
② SSM APIへの経路確保

・SSM Agentから SSM APIへの アウトバウンド経路を確保する。



② SSM APIへの経路確保

・SSM Agentから SSM APIへの アウトバウンド経路を確保する。

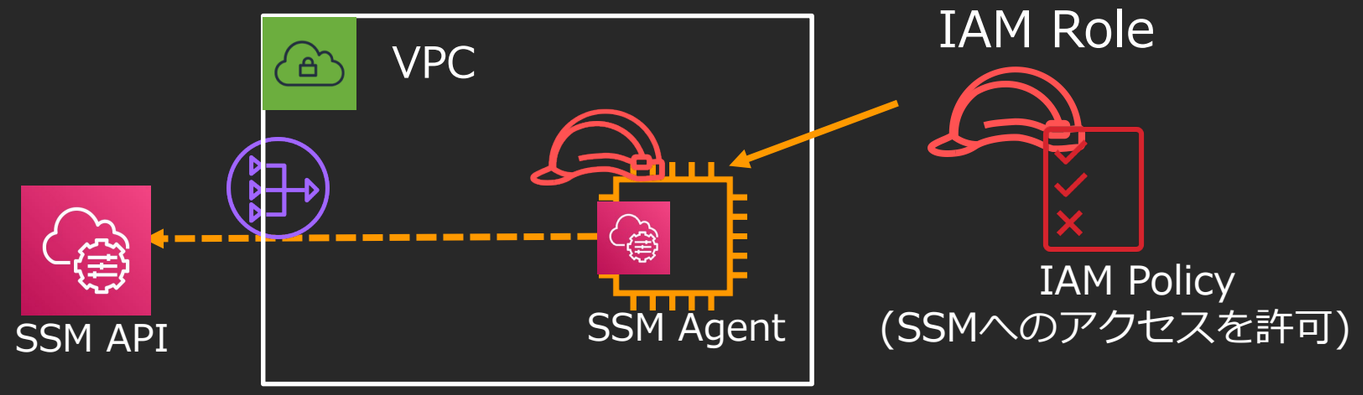


③ IAMロール付与

- 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)



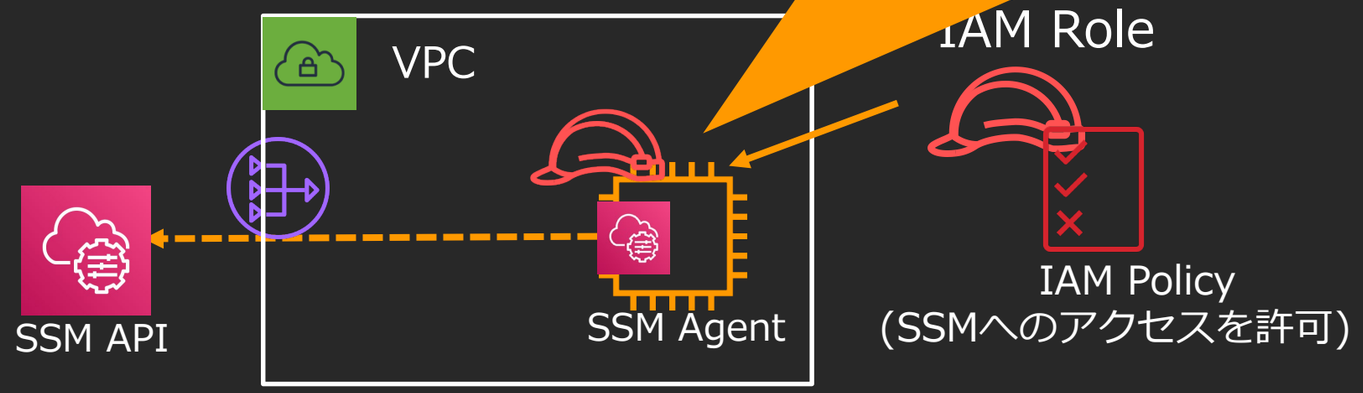
③ IAMロール付与

- IAMロールを作成し、EC2にアタッチ
- IAMポリシー

  1, 「AmazonSSMManagedInstanceCore」 で

  2, 必要に応じて、S3などのポリシーをアタッチ

今回のハンズオンでは、コア機能をアタッチしたロールを作成します。



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

→ 導入済みのオフィシャルイメージを使います。

2, SSM APIへの経路確保

→ パブリックサブネットに配置し、インターネットにてアクセスします。

3, IAMロール付与

→ コア機能をアタッチしたロールを付与します。

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

→ 導入済みのオフィシャルイメージを使います。

2, SSM APIへの経路確保

→ パブリックサブネットに配置し、インターネットにてアクセスします。

3, IAMロール付与

→ コア機能をアタッチしたロールを付与します。

早速やってみましょう

セッションマネージャーによる
サーバアクセス

aws SUMMIT ONLINE

SSM セッションマネージャー

- インバウンドの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
  1、SSM Agent 経由で直接アクセス
  2、SSM Agent でトンネルを作成してSSHなどでアクセス

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

SSM Agent 経由で直接アクセス

トンネリングアクセス (SSH/SCP接続)

Linuxを
選んだ方

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

SSH設定ファイルにてAWS CLIコマンドを設定

IAM認証/認可

OS認証

```
$ ssh -i TokyoKey.pem ec2-user@i-079c3a197ab5682cb
Last login: Tue Feb  4 20:54:19 2020 from localhost

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|¥___|___|

https://aws.amazon.com/amazon-linux-2/
6 package(s) needed for security, out of 28 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-2-214 ~]$
```

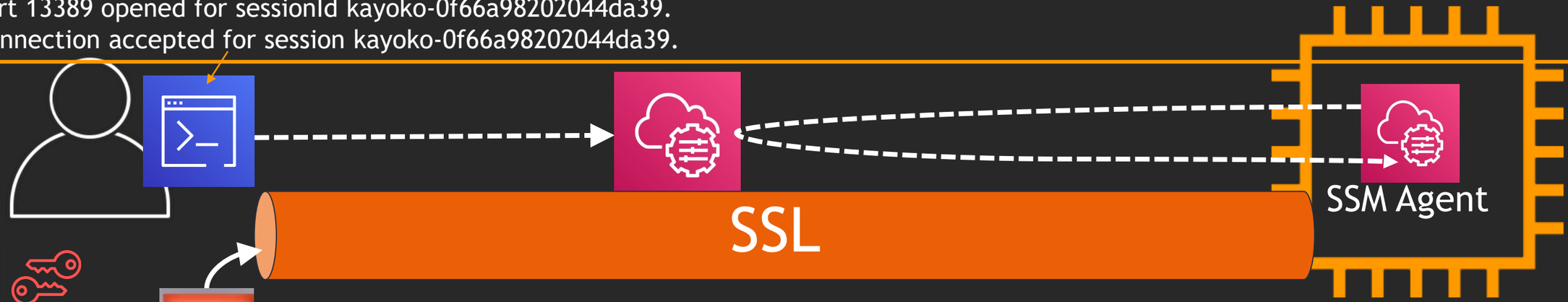
端末のターミナルから
インスタンスにアクセス

トンネリングアクセス (RDP接続)

Windowsを
選んだ方

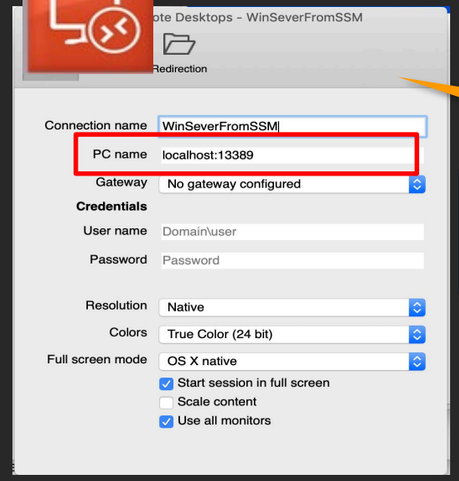
```
$ aws ssm start-session --target i-04f43c284532fbc32 --document-name AWS-StartPortForwardingSession --parameters "portNumber=3389, localPortNumber=13389"

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

AWS CLI にてトンネリングを確立する



IAM認証/認可

OS認証



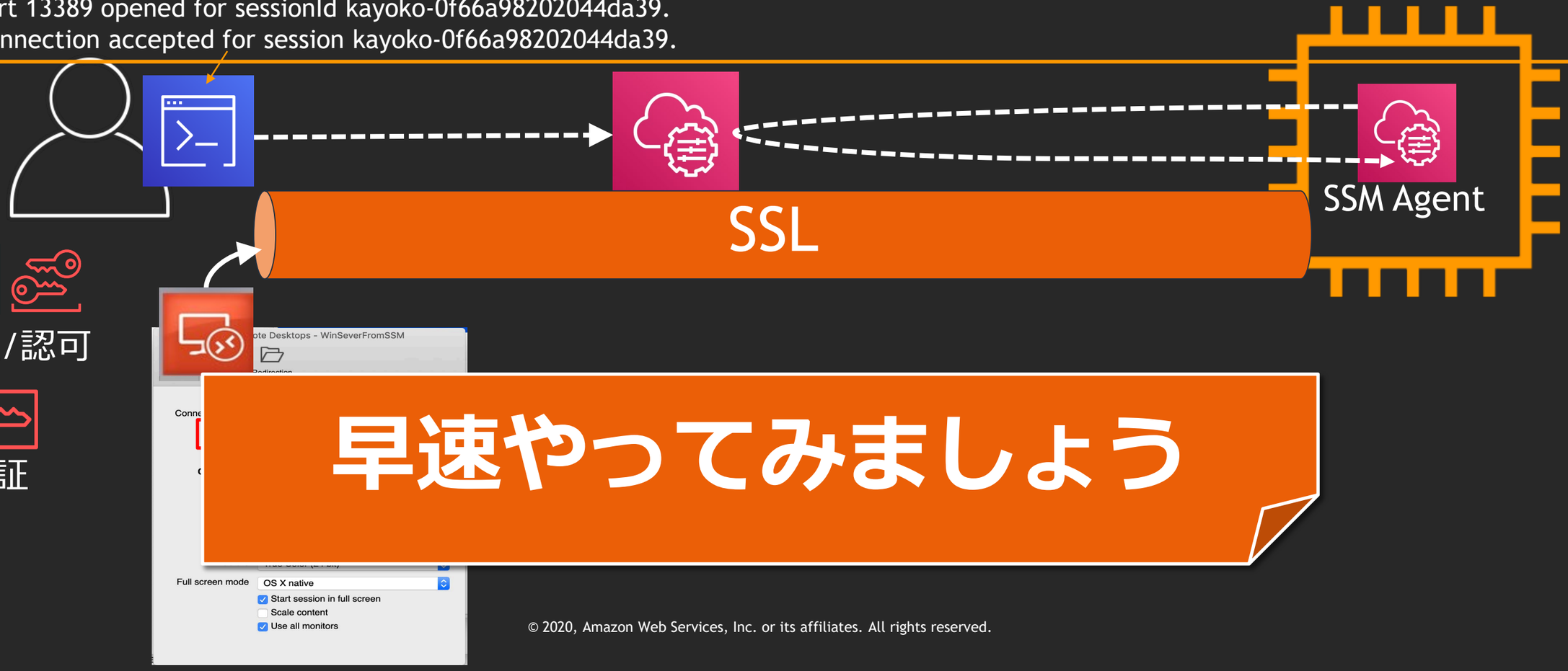
リモートデスクトップクライアントから
アクセス

トンネリングアクセス (RDP接続)

Windowsを
選んだ方

```
$ aws ssm start-session --target i-04f43c284532fbc32 --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.
```

AWS CLI にてトンネリングを確立する



早速やってみましょう

Run Commandによるサーバ群へのコマンドの一括投入

aws SUMMIT ONLINE

Run Command 

- Run Command
  - OS上でコマンドを実行
    - 例) ShellScriptの実行、AnsiblePlaybookの実行
  - 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
  - ターゲットとして、インスタンスタグ指定やリソースグループでの指定、および手動選択が可能。

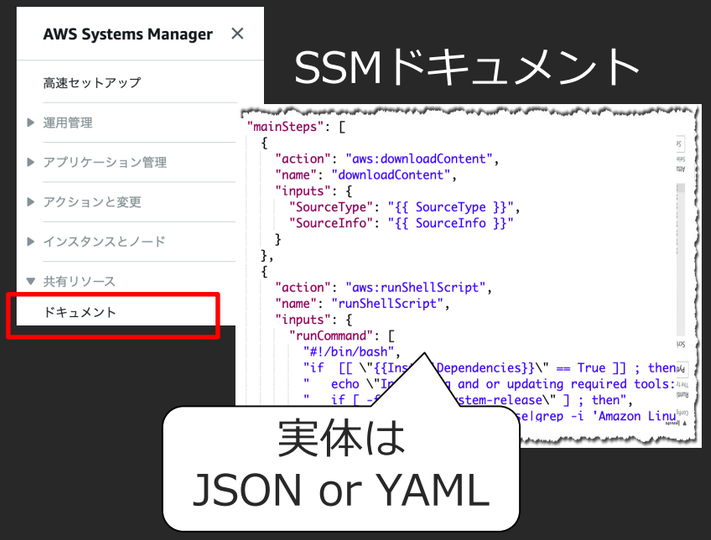
  - Run Commandは、コマンドドキュメントを実行する。

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

コマンドドキュメントって？

・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。

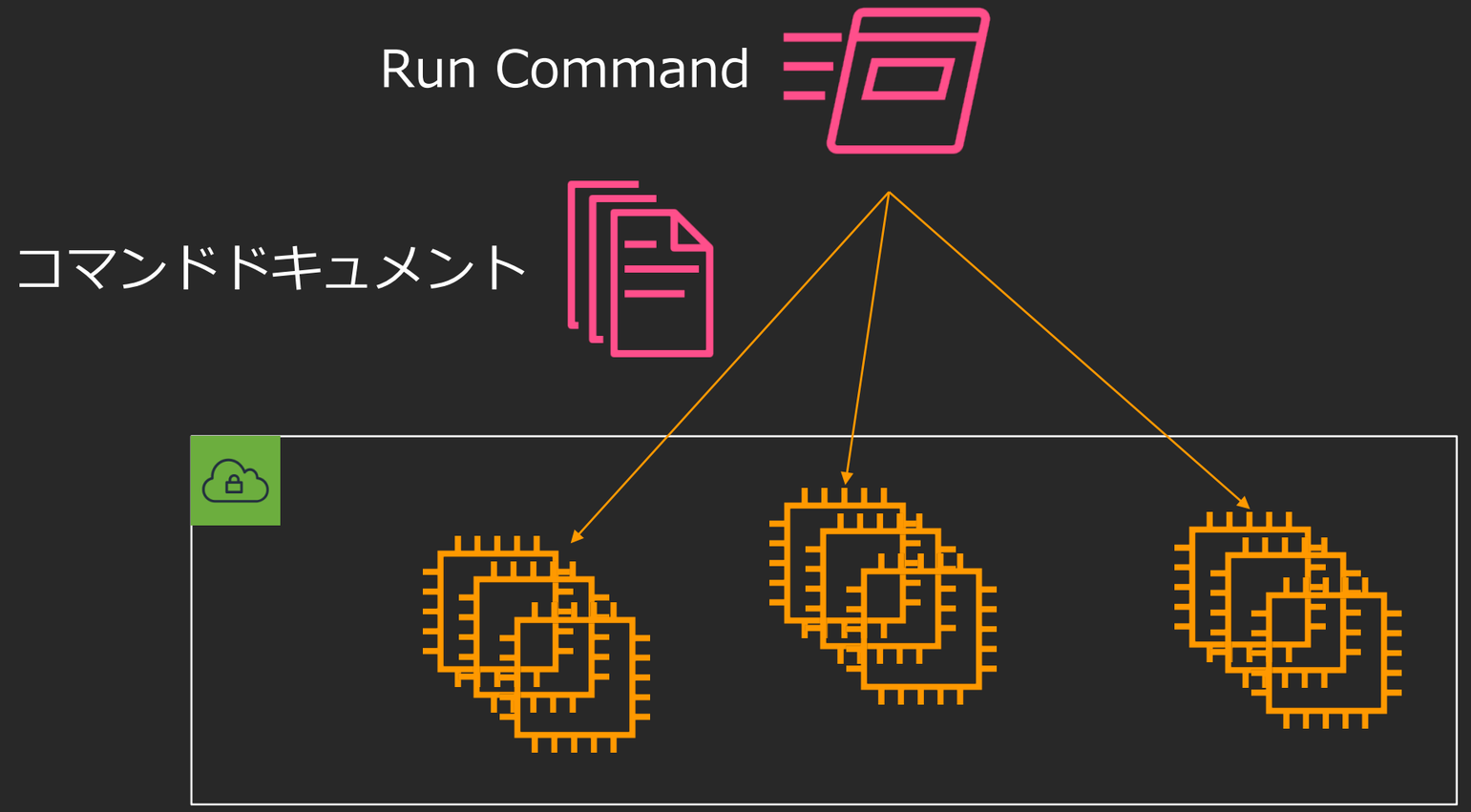
SSMドキュメント



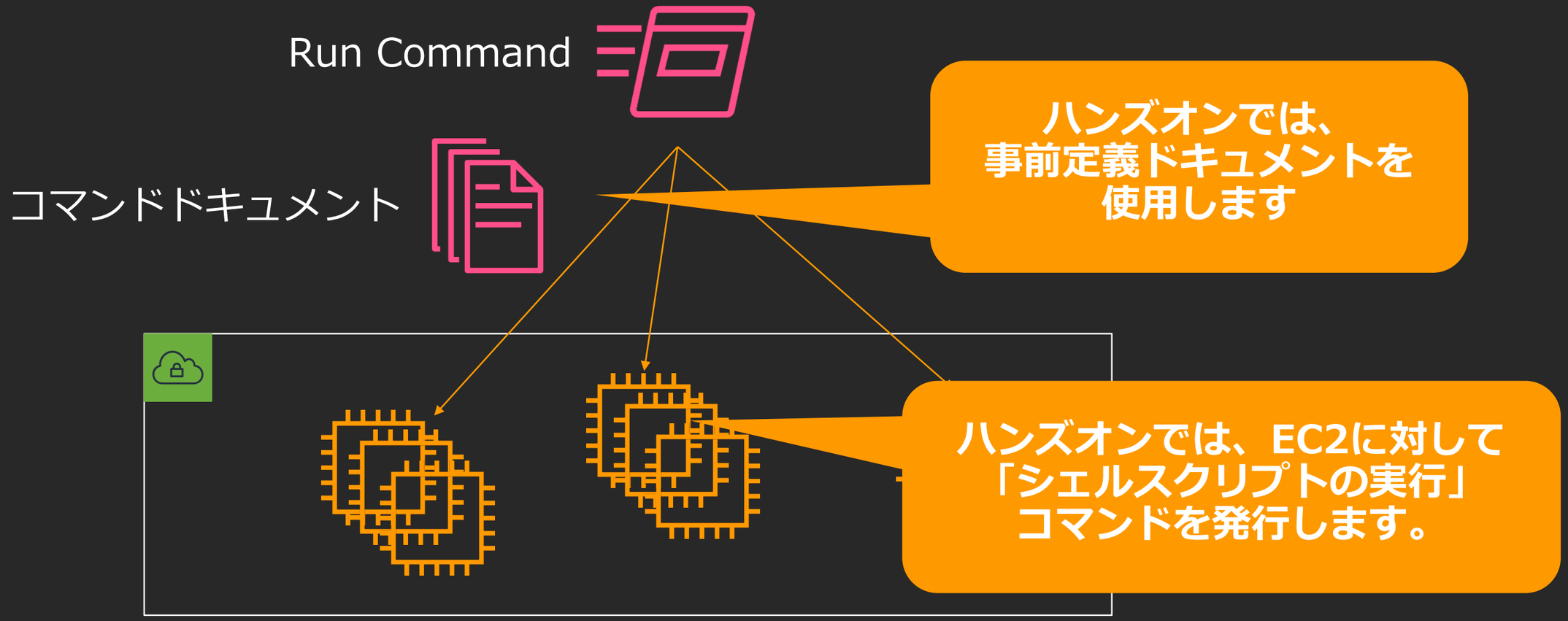
・Run Commandで実行するドキュメントをコマンドドキュメントと呼ぶ。
※コマンドドキュメントの他に、オートメーションで使用する自動化ドキュメントなどがある。

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

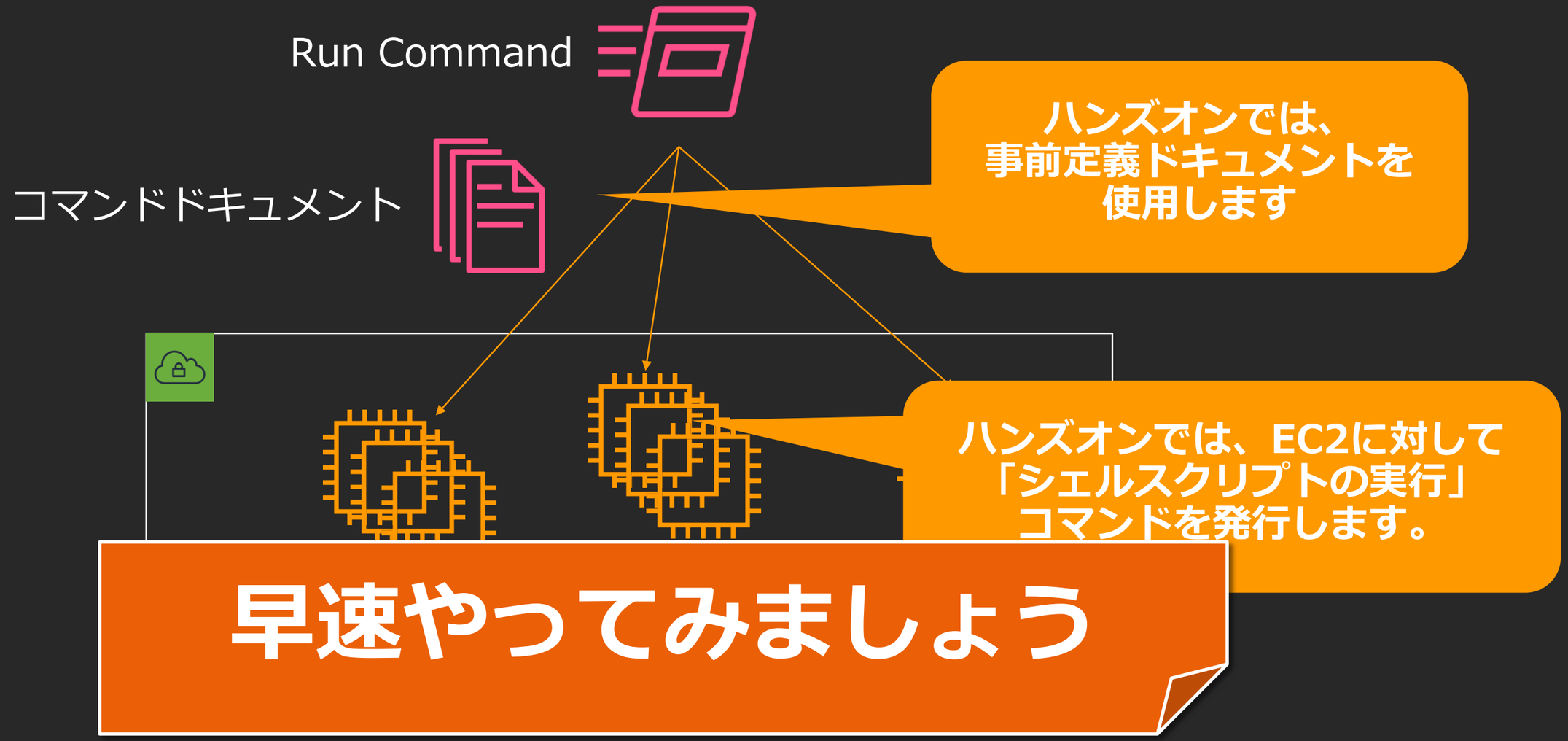
Run Commandの実行



Run Commandの実行



Run Commandの実行

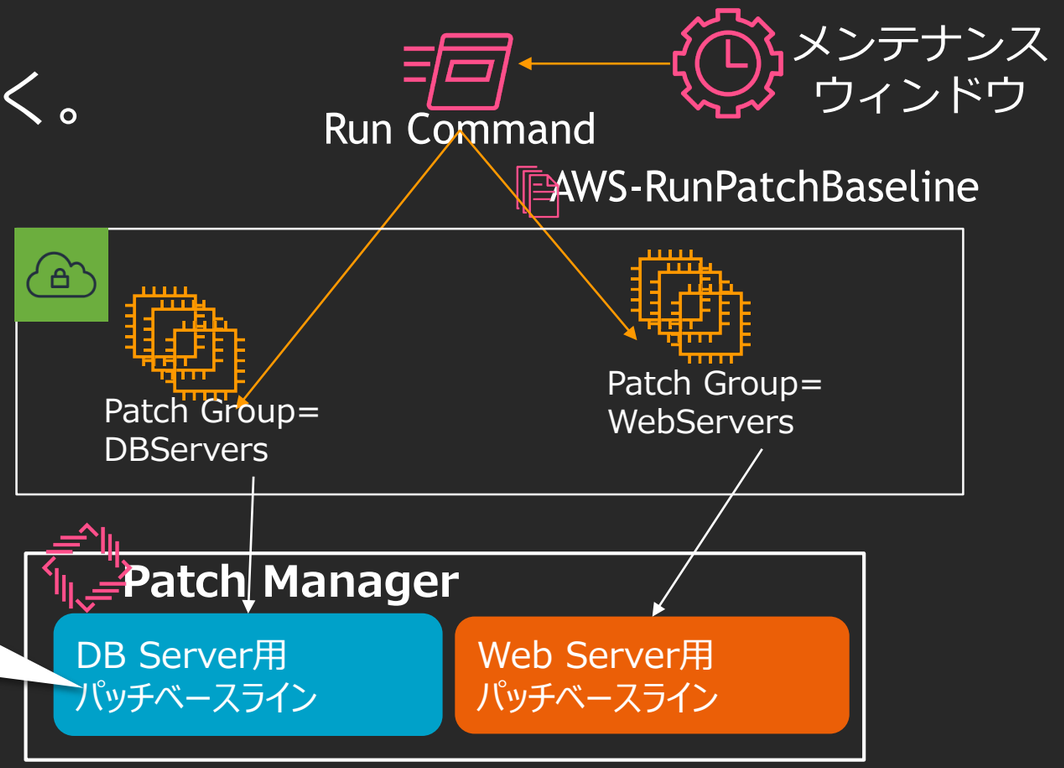


インスタンスへのOSパッチの自動適用

aws SUMMIT ONLINE

AWS SSM パッチマネージャー

- パッチルール準拠状況の確認、パッチ適用の自動化を可能とするフレームワーク
- フレームワークの実体は、メンテナンスウィンドウでのRun Command (AWS-RunPatchBaseline)の定期実行
- 事前にパッチベースラインを定義しておく。
  事前定義されたベースラインあり



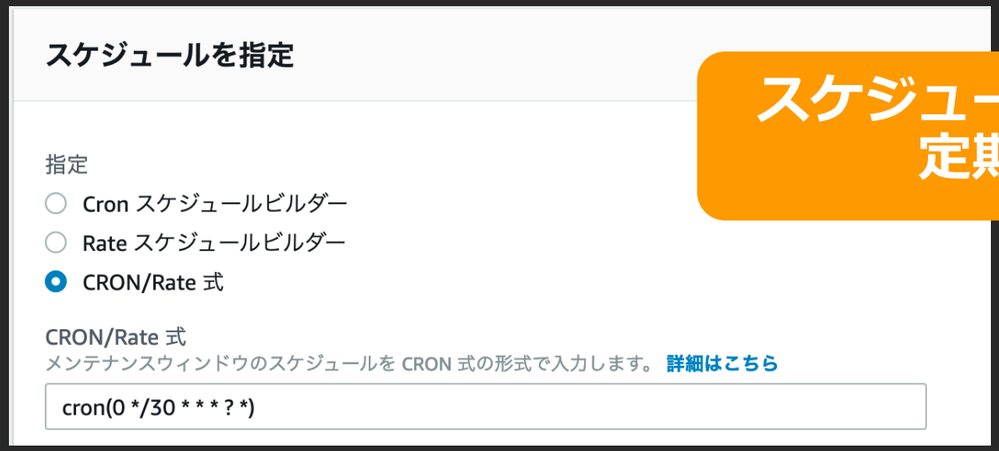
パッチベースラインの例

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

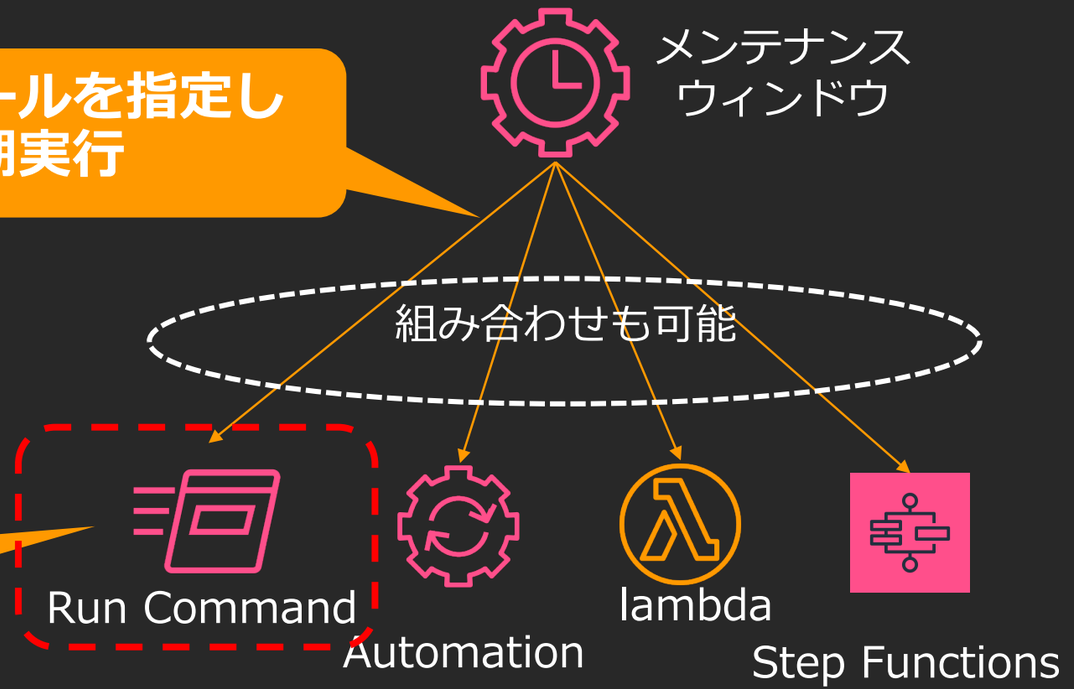
詳細は、https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-patch.html

AWS SSM メンテナンスウィンドウ

- 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
- Run CommandやLambda、Step Functionsなども実行可能



スケジュールを指定し定期実行



パッチマネージャーでは、Run Commandを実行

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

AWS SSM メンテナンスウィンドウ

- 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
- Run CommandやLambda、Step Functionsなども実行可能

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

しばし休憩

aws SUMMIT ONLINE

まとめ

aws SUMMIT ONLINE

まとめ

・本セッションは、AWS Systems Managerの以下の機能を
実際に体感していただきました。

- セッションマネージャーを利用したサーバアクセス
- Run Commandによるサーバ群へのコマンドの一括投入
- パッチマネージャーを用いた、インスタンスへのOSパッチの自動適用

・本セッションでは、EC2インスタンスを対象にハンズオンを進めましたが、オンプレミスのサーバもSSMの管理下にすることができます。

・SSMには、上記以外の機能もございます。ぜひ一つの機能から、導入してみてはいかがでしょうか。

環境のクリーンナップ

aws SUMMIT ONLINE

Thank you!

aws SUMMIT ONLINE