
aws
SUMMIT
ONLINE
JAPAN | MAY 11-12, 2021

AWS-51

情シス向け運用ユースケース

石橋 香代子

アマゾン ウェブ サービス株式会社　技術統括本部 エンタープライズソリューションアーキテクト本部 消費財&流通小売ビジネス部
シニア ソリューション アーキテクト

自己紹介

石橋 香代子 (いしばし かよこ)

シニア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

このセッションでお話しすること

✓ 話すこと：

・運用ユースケースに応じた AWS サービスの使い方

・AWS サービスを使って運用を楽にかつスケーラブルにする方法

✓ 話さないこと：

・各サービス、各機能の詳細
（ AWS 公式ドキュメントや Black Belt オンラインセミナー資料をご確認ください ）

Agenda

このセッションでは、ある情シスの１日を追っていきます。

- Case1　インベントリの可視化
- Case2　オンコール
- Case3　サーバーアクセス
- Case4　資産管理台帳の整備

ある情シスの一日

朝9時
さぁ今日も一日
頑張るぞ。

すると間も無く・・・

Javaで脆弱性！
全てのサーバーの Java の有無、バージョンを調査せよ

セキュリティチームから緊急指示が！

Case1 インベントリの可視化

インベントリの調査、あなたなら・・・？？

- ✓ まず、各システム担当者へサーバー一覧（Excel）の提出を依頼して・・・

IPアドレス、ログインID、パスワード

- ✓ サーバーにログインして、Java のバージョンを確認して・・・
- ✓ ログインできないサーバーがある、再度担当者へ確認だ。
- ✓ サーバー台数多いな、何台繰り返せばいいんだ。

繰り返し

50台、、、平均3分でも２時間か。
ランチはコンビニ弁当でしのぐか・・・

- ✓ できた！Excel でグラフ作ったぞ！
- ✓ と思ったら別の依頼

PHPも調査して

＿|￣|○ ｶﾞｸｯ

スマートなチームなら、こんな風に

ダッシュボードで
楽々

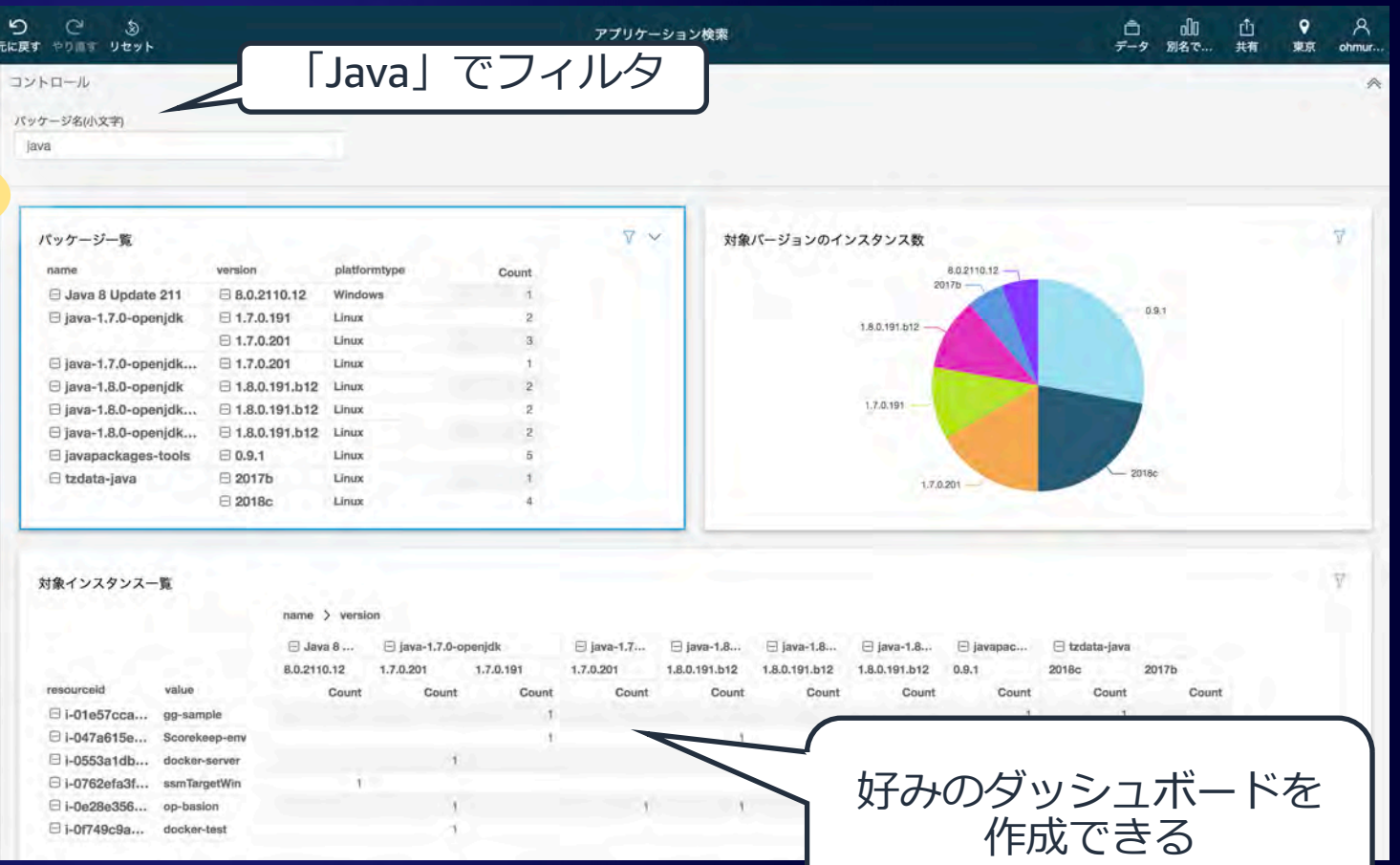
Point

・オンプレミスのサーバーを含む、全てのサーバーのインベントリ情報を含めることができる。

・常に最新の情報(*)を確認することができる。

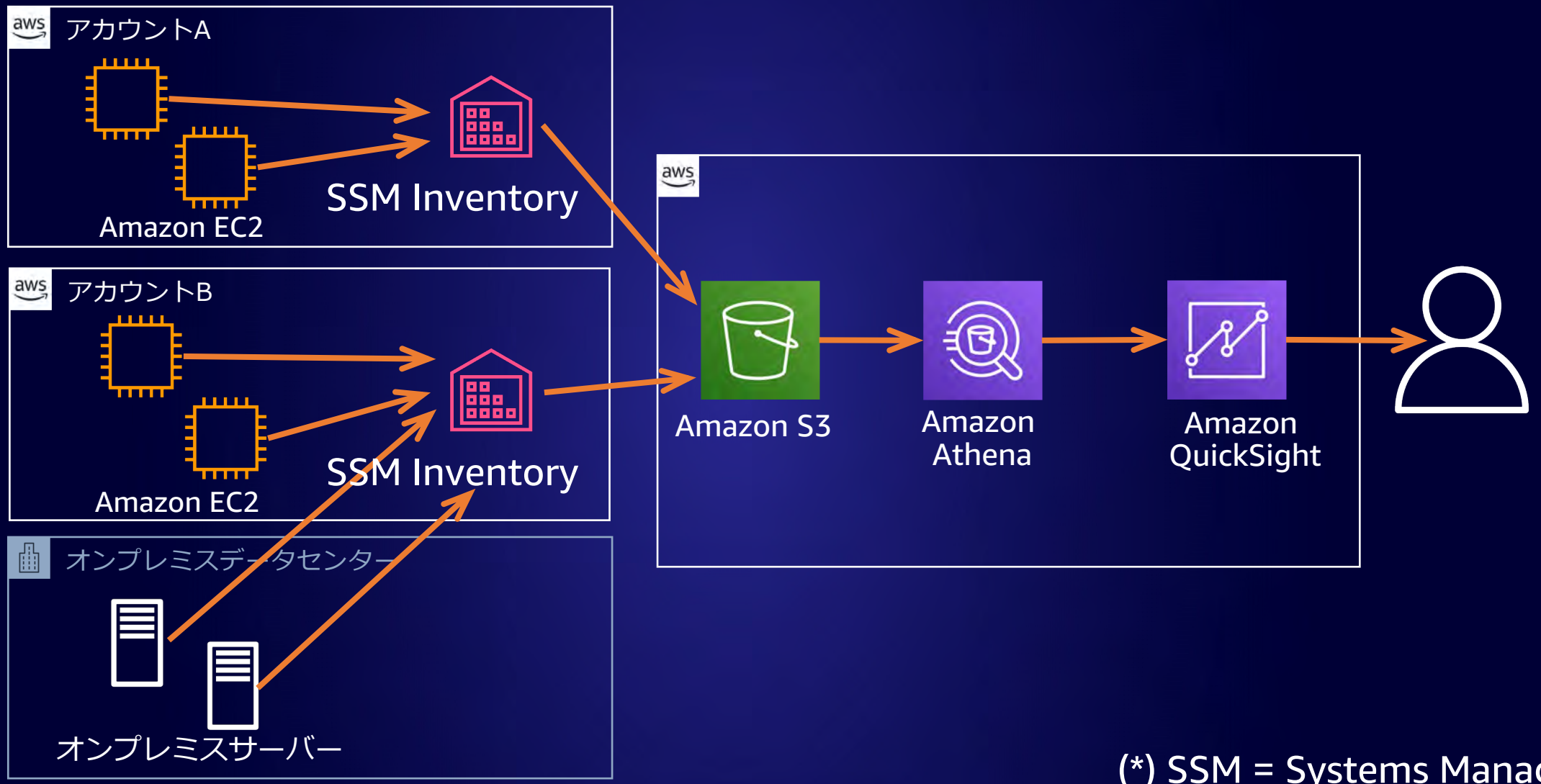
・台数が多くてもスケールする

楽々10分



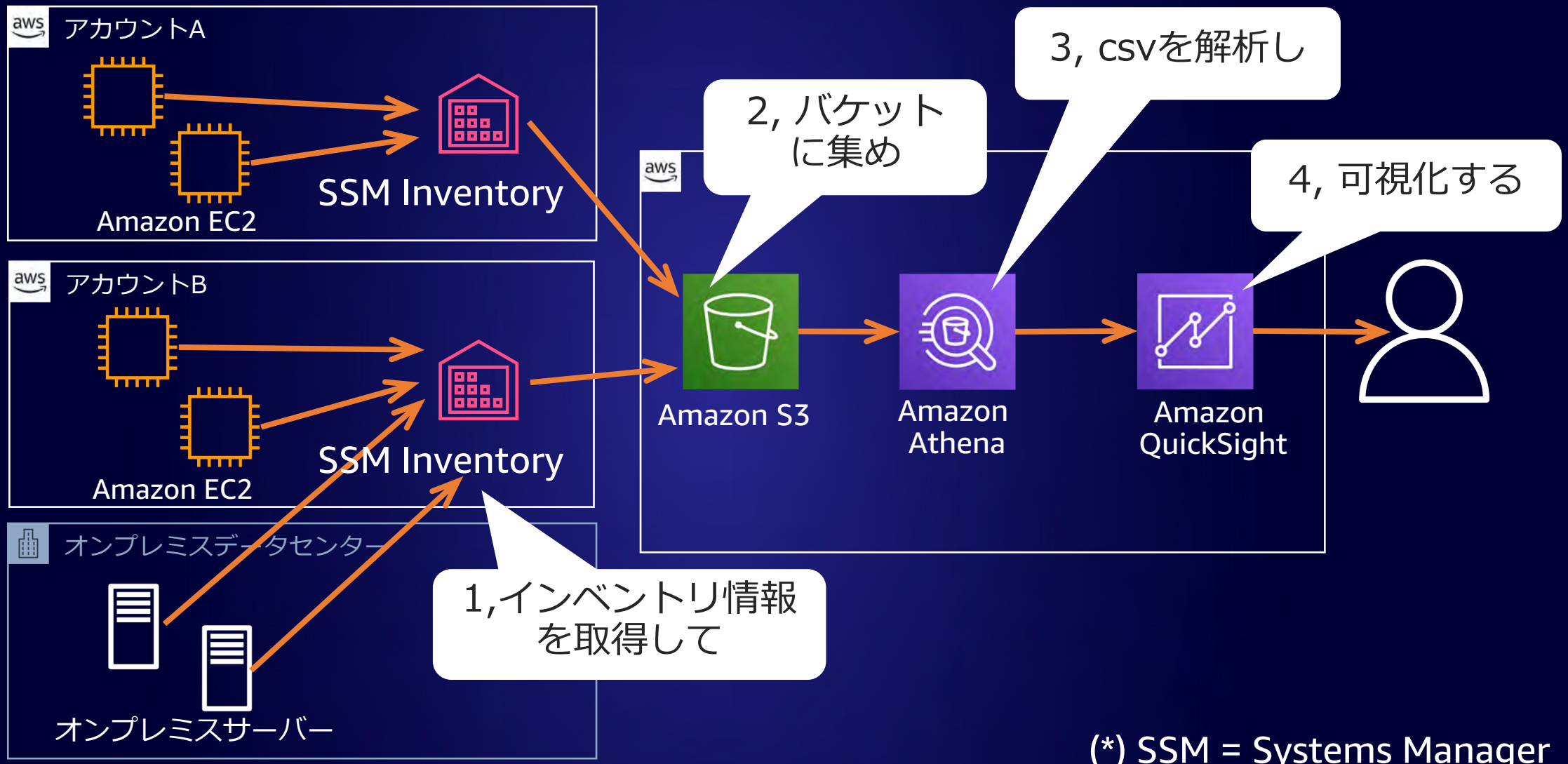
(*) 最短で30分毎にインベントリ情報が収集されます。

アーキテクチャ例



(*) SSM = Systems Manager

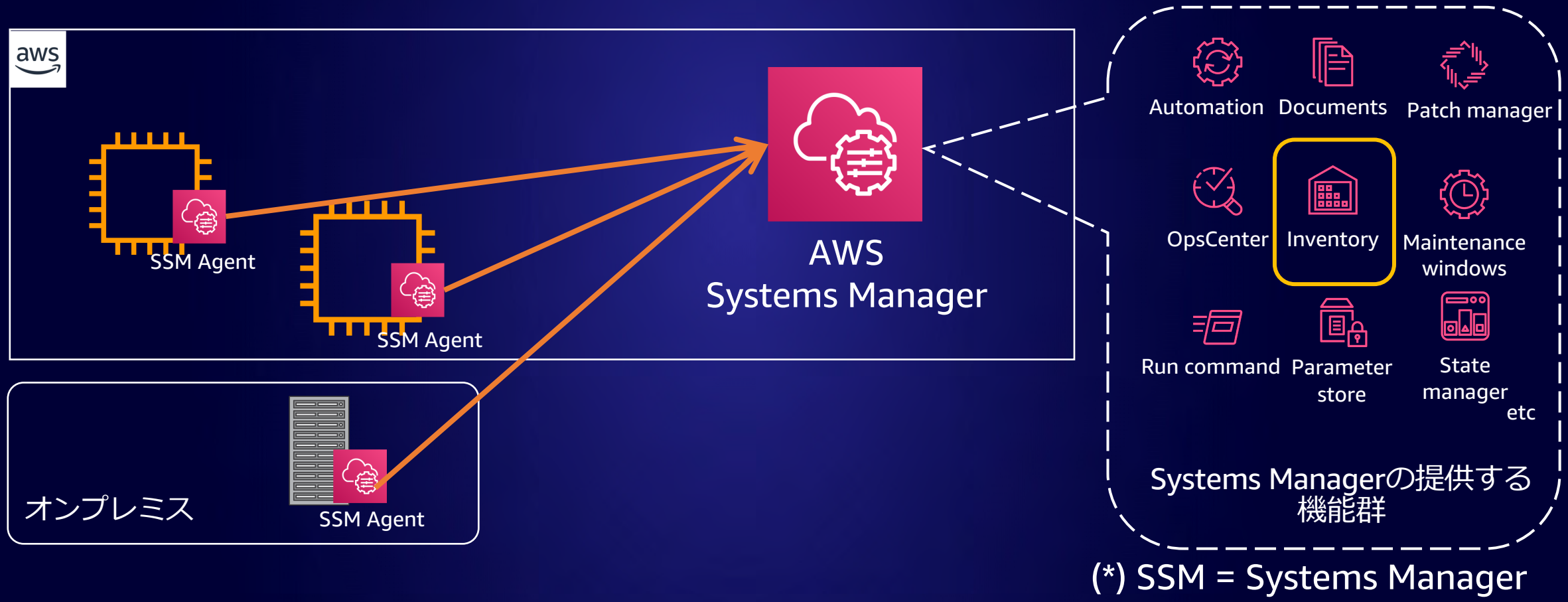
アーキテクチャ例



(*) SSM = Systems Manager

使用サービスのご紹介： **AWS Systems Manager**

AWS および オンプレミスのサーバー群を管理する多機能なツールセット



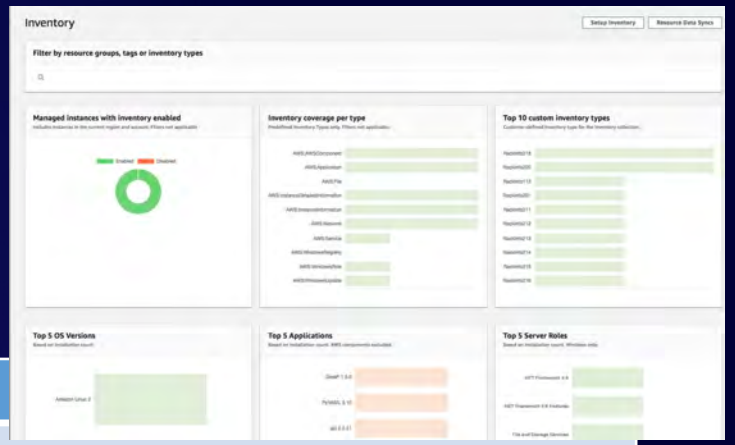
(*) SSM = Systems Manager

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

使用サービスのご紹介：SSM Inventory

- 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。
- 定期的に収集でき、データはS3バケットに保管される。

(*) 最短で30分毎にインベントリ情報が収集されます。



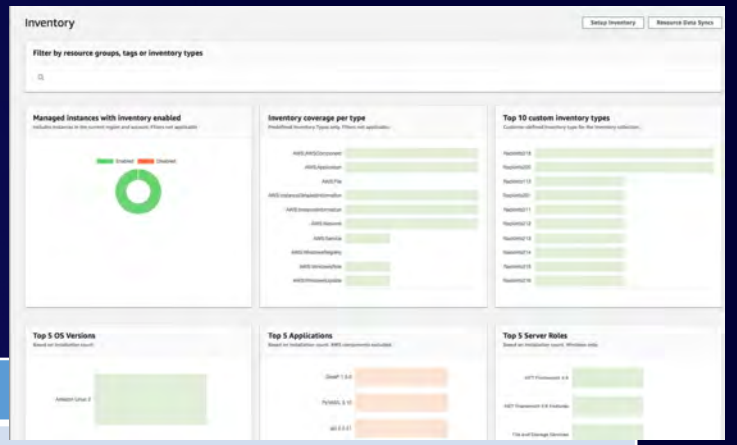
取得できる情報	詳細
アプリケーション	アプリケーション名、発行元、バージョンなど
AWS コンポーネント	EC2 ドライバ、エージェント、バージョンなど
ファイル	名前、サイズ、バージョン、インストール日、変更および最新アクセス時間など
ネットワーク構成情報	IP アドレス、MAC アドレス、DNS、ゲートウェイ、サブネットマスクなど
Windows アップデート (Winのみ)	Windows Updateに関する情報 (Hotfix ID、インストール者、インストール日など)
インスタンスの詳細	OS名、OSバージョン、最終起動、DNS、ドメイン、ワークグループ、OS アーキテクチャなど
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

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

使用サービスのご紹介：SSM Inventory

- 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。
- 定期的に収集でき、データはS3バケットに保管される。

(*) 最短で30分毎にインベントリ情報が収集されます。



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… …バージョンなど
ファイル	名前、サ…
ネットワーク構成情報	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

このユースケースではこれを使用

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

使用サービスのご紹介：Amazon QuickSight

- クラウドスケールのビジネスインテリジェンス(BI)サービス
- インタラクティブな BI ダッシュボードを簡単に作成し、公開できる
- 多様なビジュアルから選択できる

今回のユースケースでは
「ピボットテーブル」「円グラフ」を使用

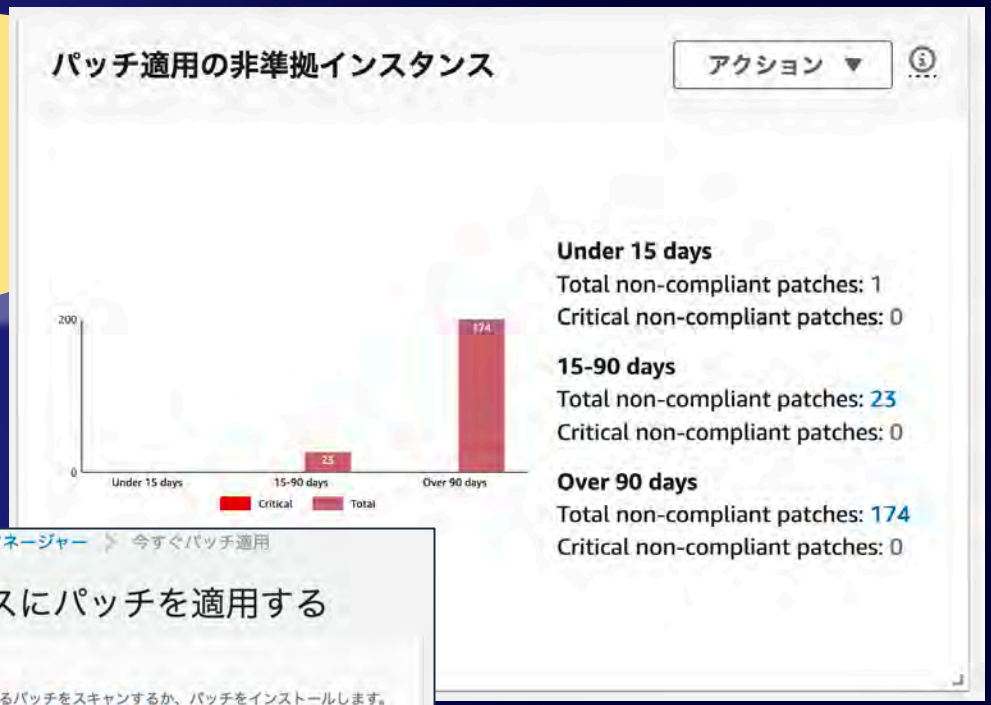
https://docs.aws.amazon.com/ja_jp/quicksight/latest/user/welcome.html

SSM があればこんなことも ①

パッチ適用状況確認して！

マネジメントコンソール
（マネコン）から確認だ

未適用のパッチがあるな、
適用までやってしまおう

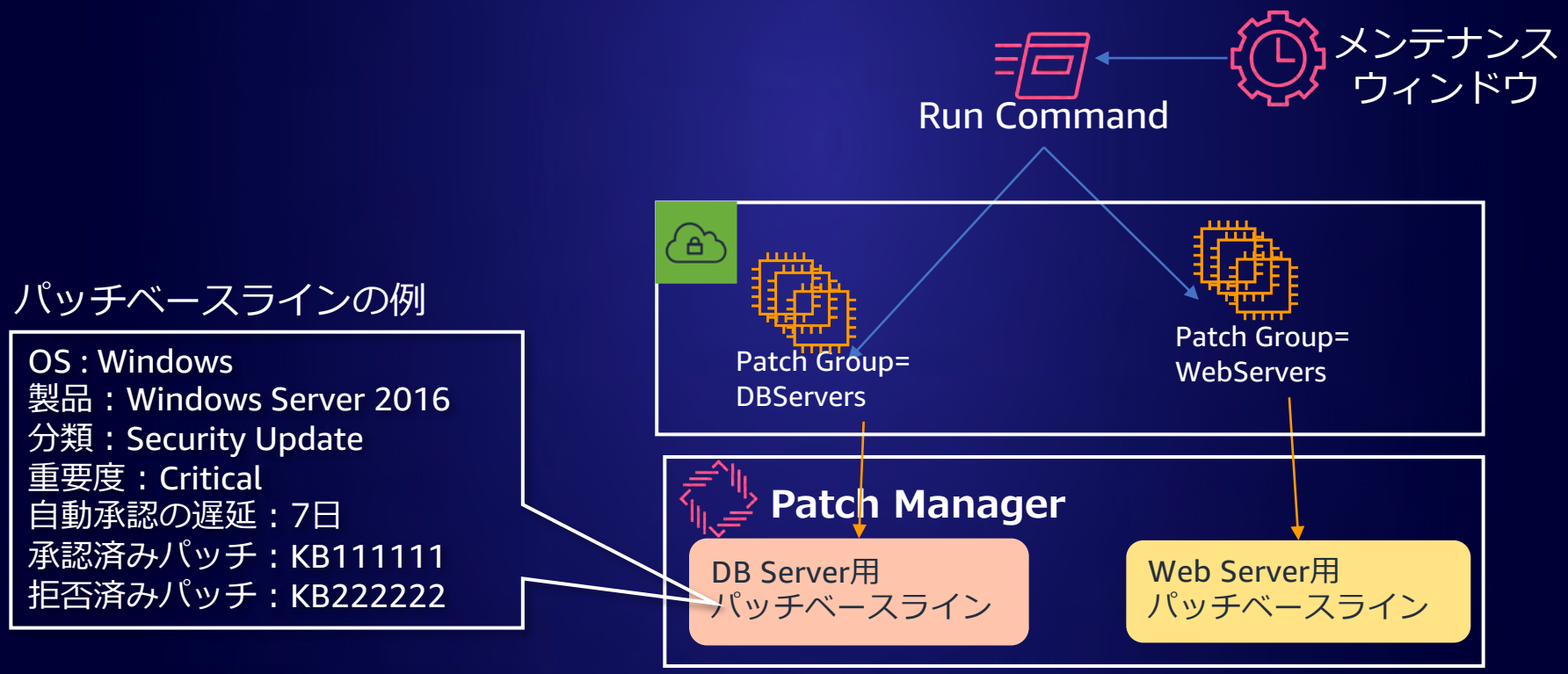


Point

サーバーログイン不要、
マネコンから解決！

使用サービスのご紹介：SSM Patch Manager

- パッチ適用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
- 事前定義したパッチベースラインに則って評価される

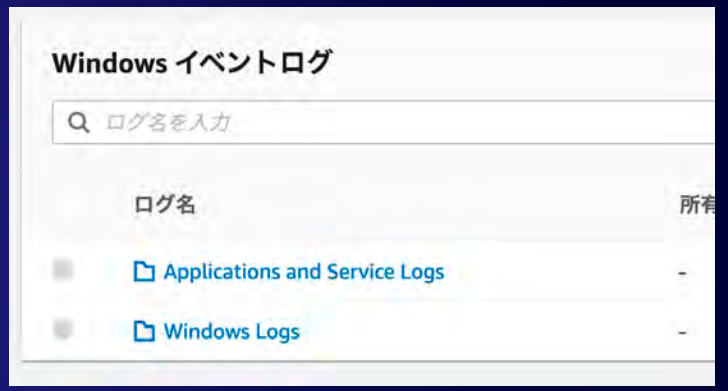


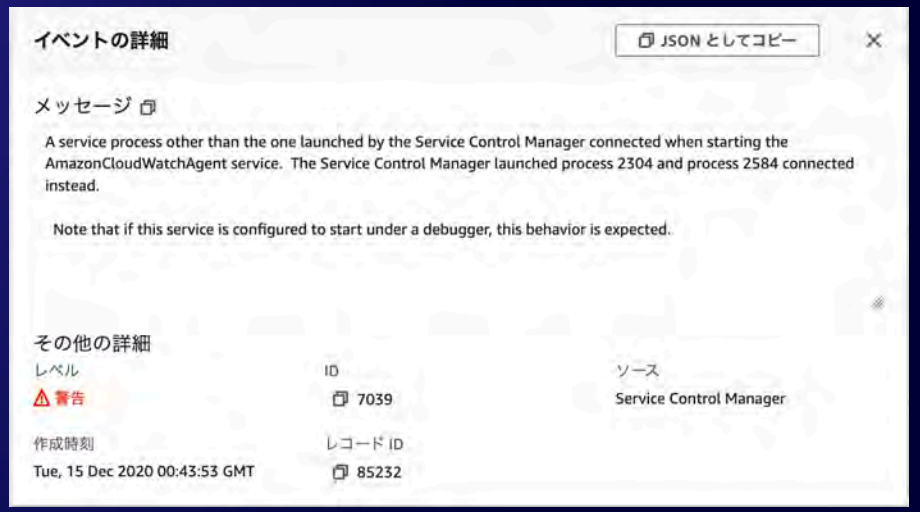
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-patch.html

SSM があればこんなことも ②

なんか**Windowsサーバーが突然再起動した**んだけど・・・

イベントログを
見てみよう





Point

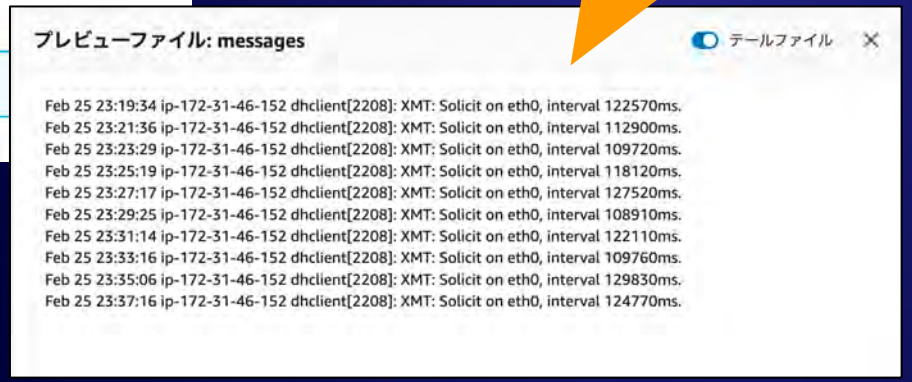
サーバーログイン不要、
マネコンからログ確認も！

使用サービスのご紹介：SSM Fleet Manager

new
2020/12

- AWS のマネコンからサーバー群の管理作業を可能とするビジュアルツール
- ファイルシステムの参照やユーザ管理、一般的なパフォーマンスカウンタのチェック、Windows のレジストリ操作などに対応

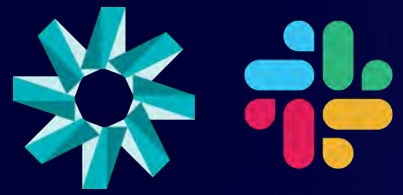
ログの Tail も便利



ユーザー/グループ作成も

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

Case1 インベントリの可視化 まとめ



Java で脆弱性！
全てのサーバーの Java の有無、バージョンを調査せよ

ご紹介した仕組みを使うと

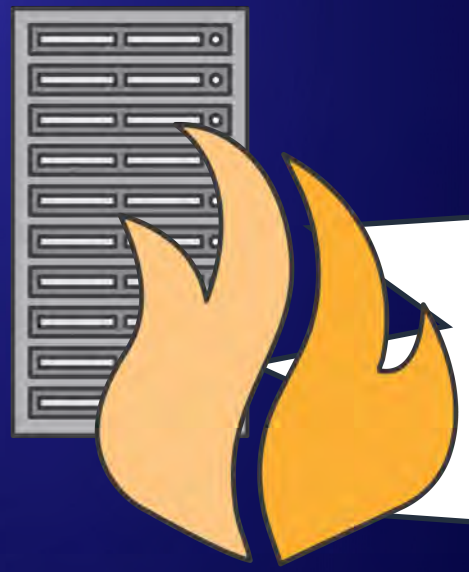
- ✓ １台ずつサーバーにログインしてコマンド発行
- ✓ 台数が多くなると時間も膨大にかかる
  - ✓ 急ぐとミスも誘発

- ✓ 事前に用意したダッシュボードで楽々調査
- ✓ 台数が多くなっても問題なし
- ✓ 使用する主なサービス
  - ✓ SSM Inventory, Amazon QuickSight

ある情シスの一日

さて、、、パッチ適用まで
したから疲れたな。
休憩しよう

と思ったら・・・



AbcServerで
障害発生

Case2 オンコール(*)

(*) ここでは、緊急時の担当者呼び出しをさしています

皆様の障害発生時のオンコールの仕組みは？

- ✓ オペレーターさんが24/365でアラート監視？
- ✓ オフショアで対応？

でも、、、

- ✓ 大きな障害が発生した場合には、監視コンソールが真っ赤！
- ✓ 対応マニュアルに則って 全関係先に電話連絡が終わるまでに数時間かかったりも。

え、もう発生から２時間経ってる。
もっと早く連絡くれないと・・・

スマートなシステムなら、こんな風に

障害が
検知されると・・・

自動で輪番コール
「対応できる場合には”1“を
押してください。」

“1”を押して
対応しよう。

チャット
ルームに
自動投稿

応答者もわかる

Point

・コール対応の
オペレーター要らず

・電話をかける作業が
スケールする

・チャットルームに応答者の記録が出て、
みんなが応答者を把握できる

アーキテクチャ例

アラート検知

Amazon CloudWatch Metrics

Amazon EventBridge (CloudWatch Events)

Amazon SNS

アラート&
担当者確認

Ops

輪番TEL

SQS

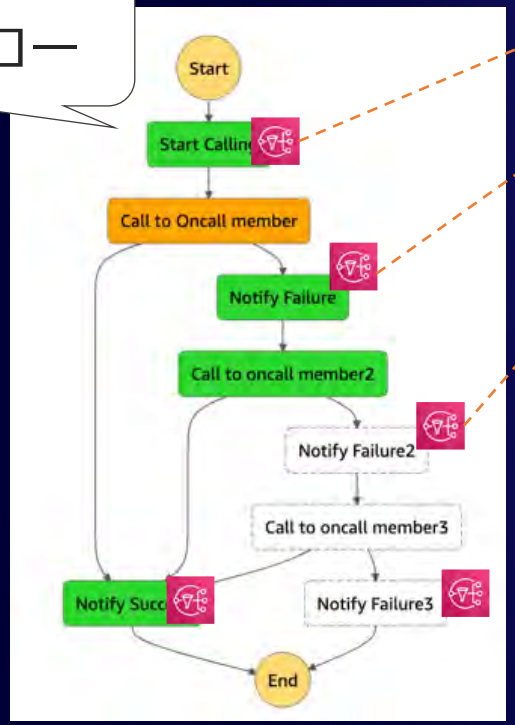
AWS Step Functions

Amazon Connect

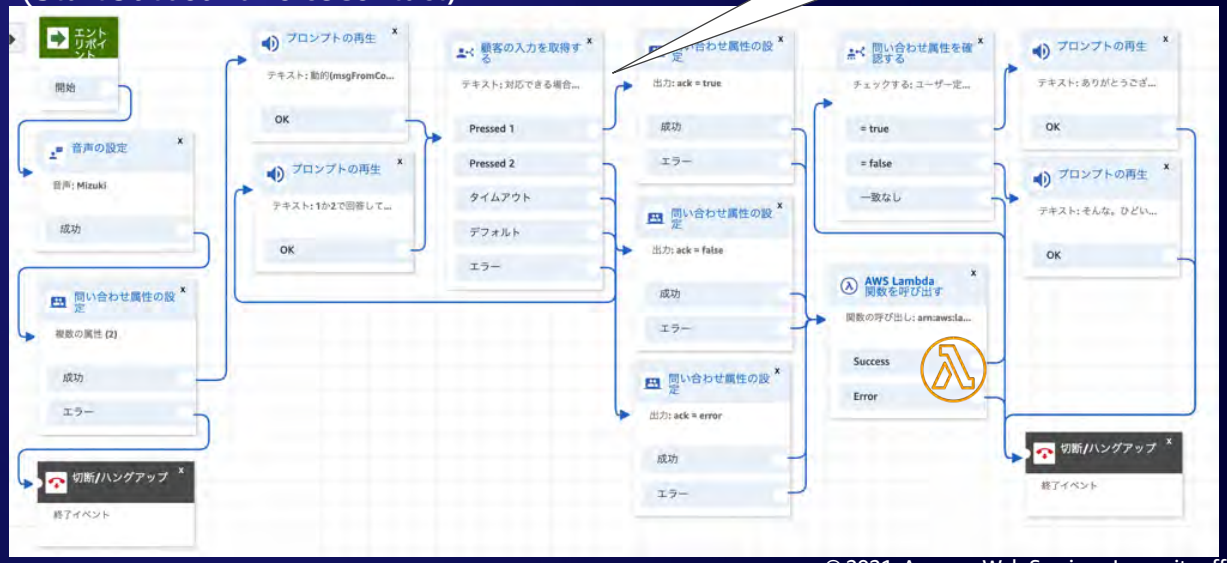
Kinesis Data Stream

アウトバウンド発信のAPIをコール
(StartOutboundVoiceContact)

輪番の
ワークフロー



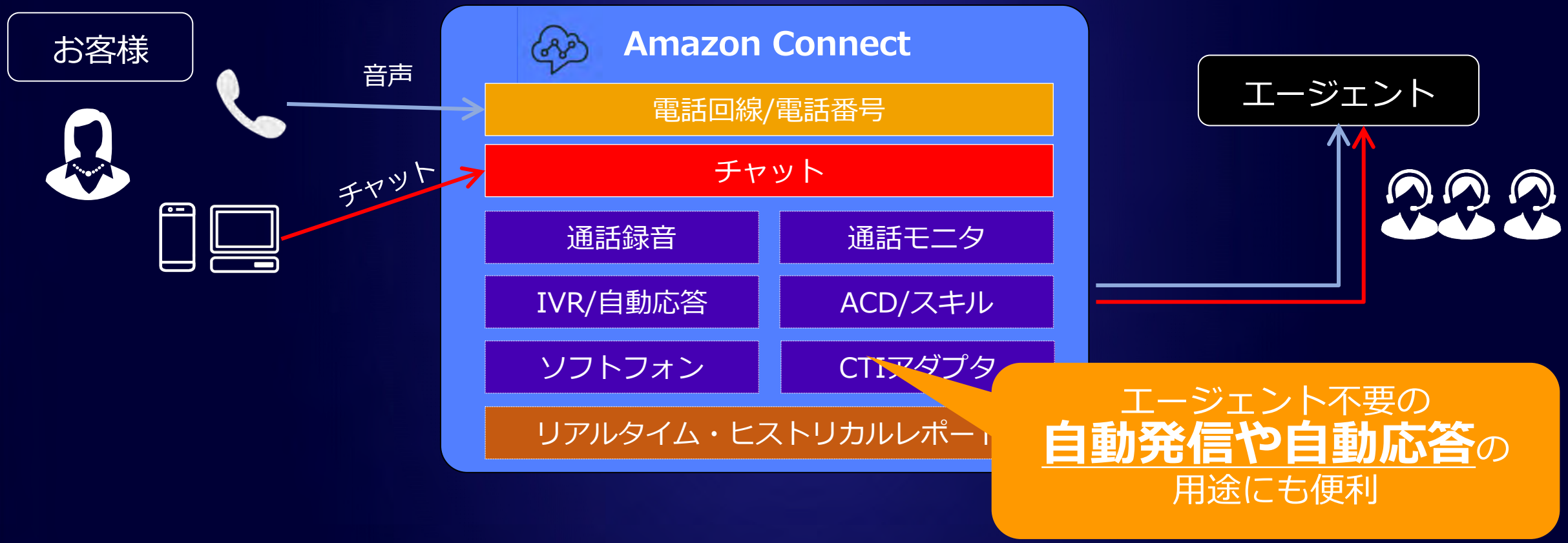
担当者にコール
「対応できる場合は
1を・・・」



使用サービスのご紹介：Amazon Connect

Amazon Connectは、あらゆる規模のビジネスに対応できる

オムニチャネルコンタクトセンターを All in One・従量課金で提供



エージェント不要の
自動発信や自動応答の
用途にも便利

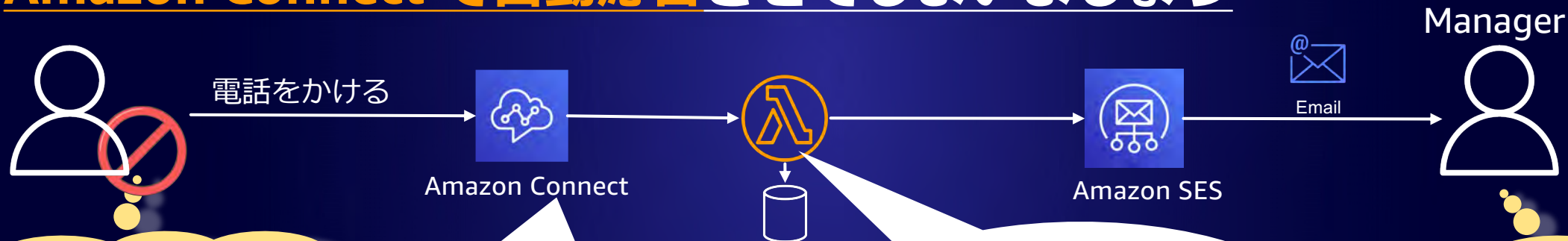
Amazon Connect があれば、こんなことも

情シスの定番**「アカウントロック対応依頼」**・・・

パスワードロック
しちゃいました

定型作業で、皆様の貴重な時間が奪われていませんか？

Amazon Connect で自動応答させてしまいましょう



Point

・自動化できるところは自動化して、楽をしましょう

Case2 オンコール まとめ

AbcServerで
障害発生

ご紹介した仕組みを使うと

- ✓ オペレータが 24/365 で有人監視
- ✓ インシデント数が多くなると電話連絡に時間がかかる

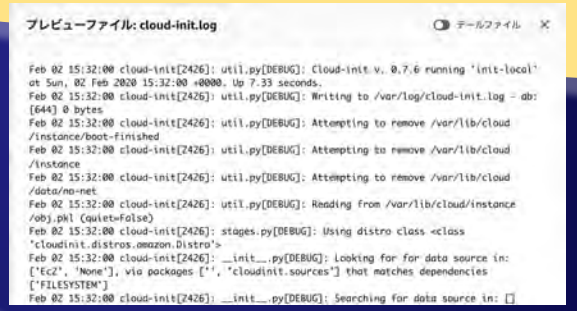
- ✓ AWS Step Functions, Amazon Connectで自動で輪番コール
- ✓ インシデント数が増えても自動でスケール
- ✓ コール対応のオペレータ要らず

ある情シスの一日

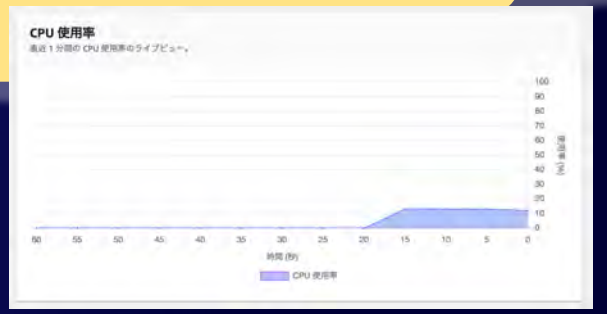
コールを受けた
よし、何が起きているか
確認だ

SSM Fleet Manager で・・

ログを確認



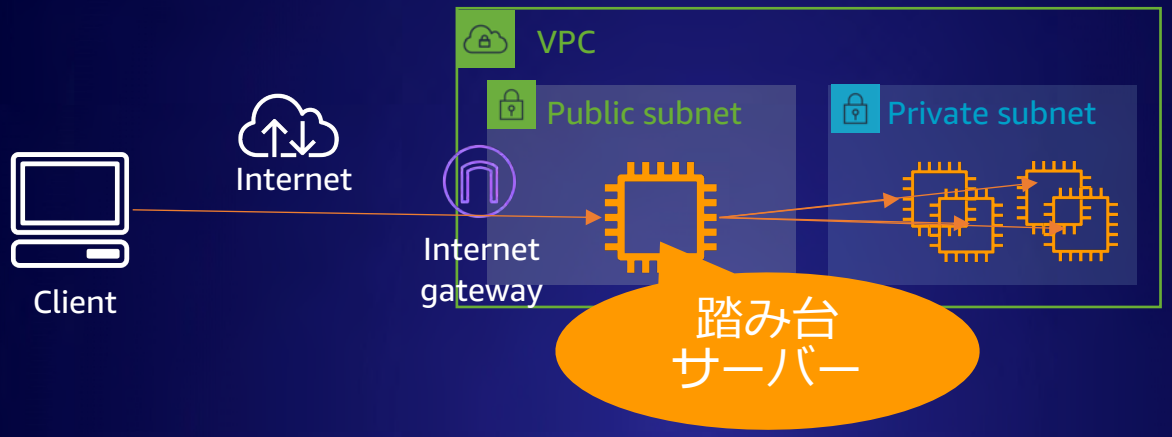
パフォーマンスカウンターを確認



だめだ、手強いぞ
サーバーに入って、本格調査が必要だ

Case3 サーバーアクセス

よくあるサーバーへのアクセス方法 – 踏み台



でも、、、

- ✓ 踏み台サーバーの管理、大変ですよね。
  - ✓ 踏み台が落ちたらどこにも入れないし。
  - ✓ 踏み台のユーザー ID 管理も、煩雑になりがち。

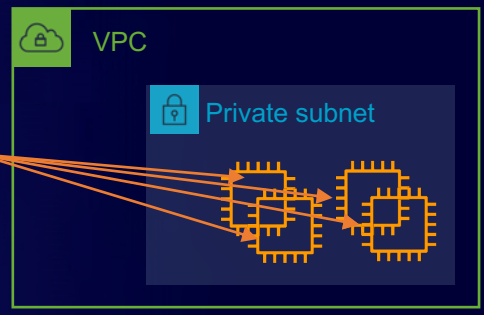
都度テンポラリー
ユーザー ID 発行？

作業後毎回
パスワード変更？

  - ✓ ssh ポートを解放するのも、セキュリティ上心配・・・

スマートなチームなら、こんな風に

マネコンから
シェルアクセスだ



ブラウザに
別タブ

Point

・マネコンから目的のサーバーに直接アクセス

・マネージドサービスなのでユーザー側で可用性の考慮不要

・IAM による認証
　・外部 IdPでのユーザー管理を利用できる（フェデレーション）

・セキュリティグループのインバウンドポート穴あけ不要

セッション ID: kayoko-096523a28157a99c1　　インスタンス ID: i-049

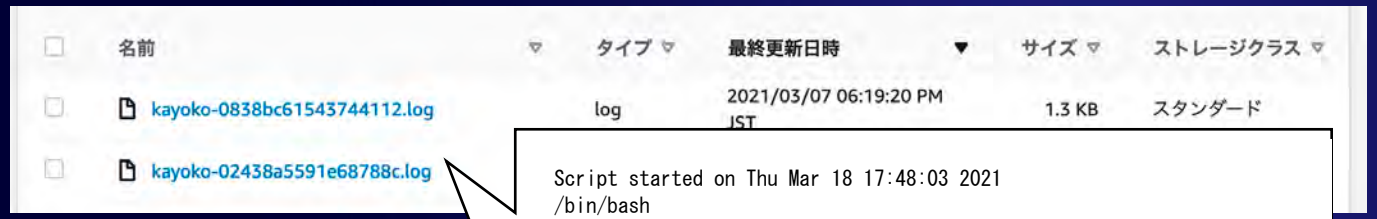
```
This session is encrypted using AWS KMS.
/bin/bash
cd /usr
sh-4.2$ /bin/bash
[kayoko@ip-172-31-46-152 /]$ cd /usr
[kayoko@ip-172-31-46-152 usr]$ whoami
kayoko
[kayoko@ip-172-31-46-152 usr]$
```

スマートなチームなら、こんな風に

操作履歴 (ストリームログも)

S3 Bucket

CloudWatch Logs




```
Script started on Thu Mar 18 17:48:03 2021
/bin/bash
cd /usr
[?1034hsh-4.2$ /bin/bash
]0;@ip-172-31-46-152:/[?1034h[kayoko@ip-172-31-46-152 /]$ cd /usr
]0;@ip-172-31-46-152:/usr[kayoko@ip-172-31-46-152 usr]$
[K[kayoko@ip-172-31-46-152 usr]$ whoami
kayoko
]0;@ip-172-31-46-152:/usr[kayoko@ip-172-31-46-152 usr]$ exit
exit
sh-4.2$ exit
exit


Script done on Thu Mar 18 17:48:03 2021
```

接続履歴

AWS CloudTrail

```
"eventTime": "2021-03-07T09:29:54Z",
"eventSource": "ssm.amazonaws.com",
"eventName": "StartSession",
"awsRegion": "ap-northeast-1",
```

発見的統制も

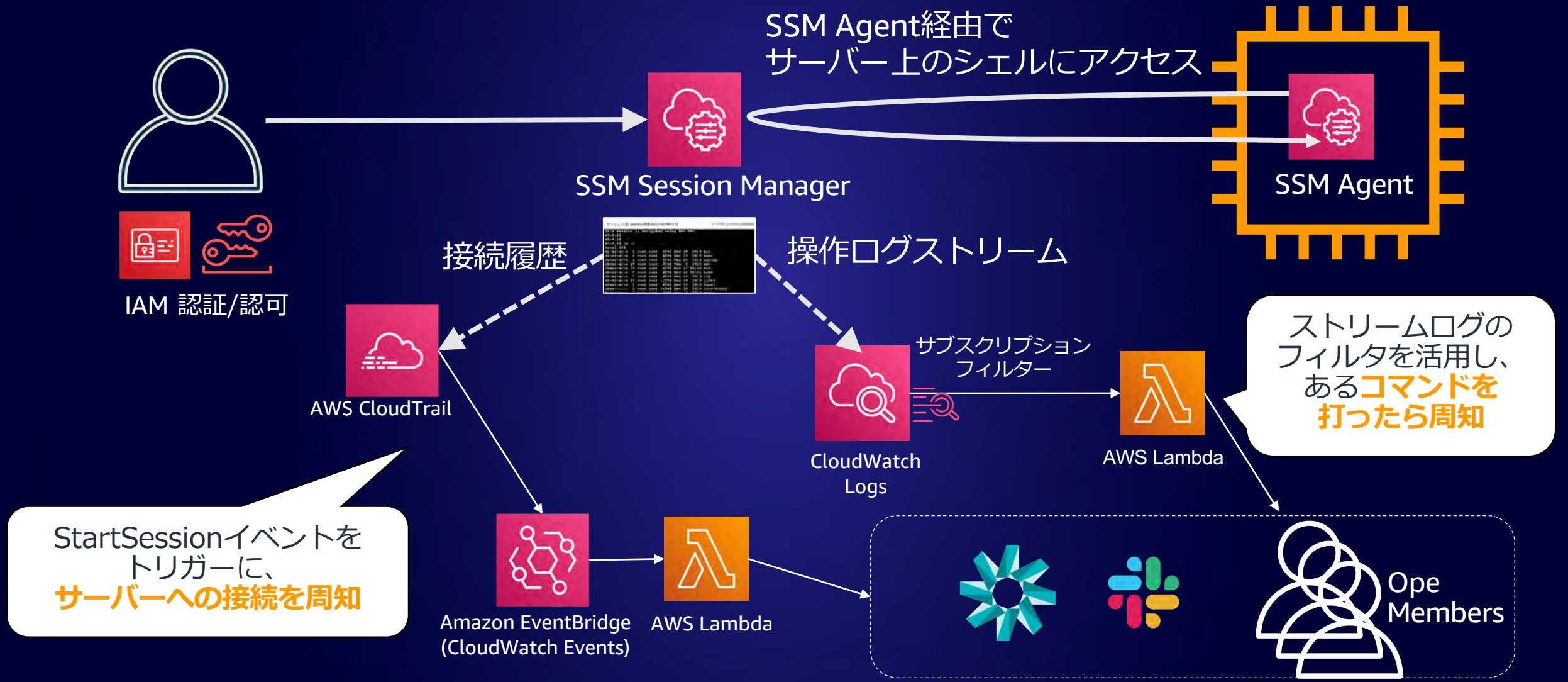
Aさんがサーバーに入ったんだな

Point

・作業ログは自動取得
操作履歴：S3 or CloudWatch Logs
接続履歴：CloudTrail

・工夫により発見的統制も

アーキテクチャ例



使用サービスのご紹介：SSM Session Manager

- 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
  - サーバーのログイン情報（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
  - ストリーミングログの取得、アイドルセッションタイムアウトの設定も可能に

2020/11

- AWS CLI からアクセスすることも可能
  - 開発チームなどマネコンにアクセスする習慣のない方にも

```
$ 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：https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/session-manager.html
ストリーミングログ取得：https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/session-manager-logging.html
アイドルセッションタイムアウト：https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/session-preferences-timeout.html

SSM Session Manager があればこんなことも

- AWS CLI を用いてポートフォワーディングが可能

Windows への **RDP 接続**や、
開発端末から **RDS に接続**する用途にも

RDP 接続の例

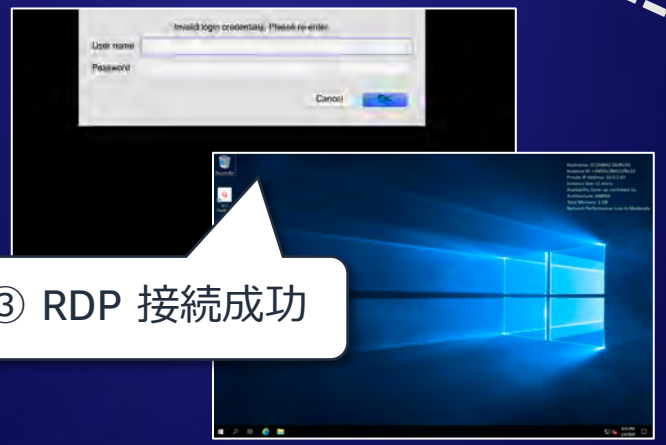
```
$ aws ssm start-session --target i-04f43c284532fbc32 --document-name AWS-
StartPortForwardingSession --parameters "portNumber=3389, localPortNumber=13389"
```

① AWS CLI でトンネリングを確立しておく

IAM 認証/認可

OS 認証

② ローカルの13389に接続



③ RDP 接続成功

接続履歴

AWS CloudTrail

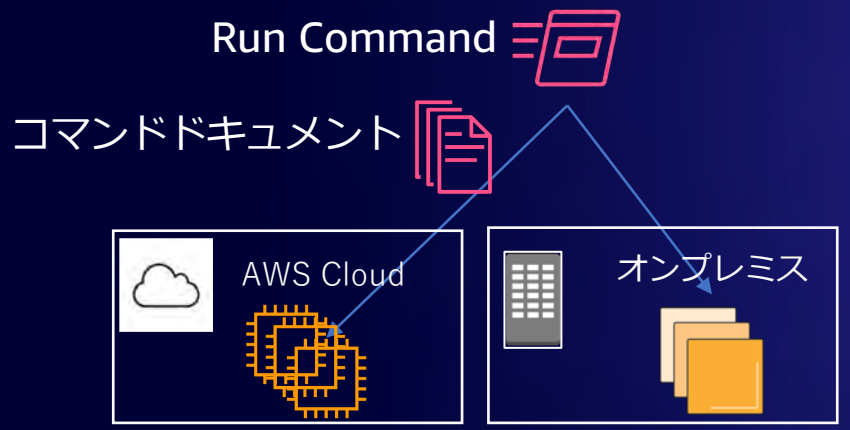
※操作履歴は取得できない

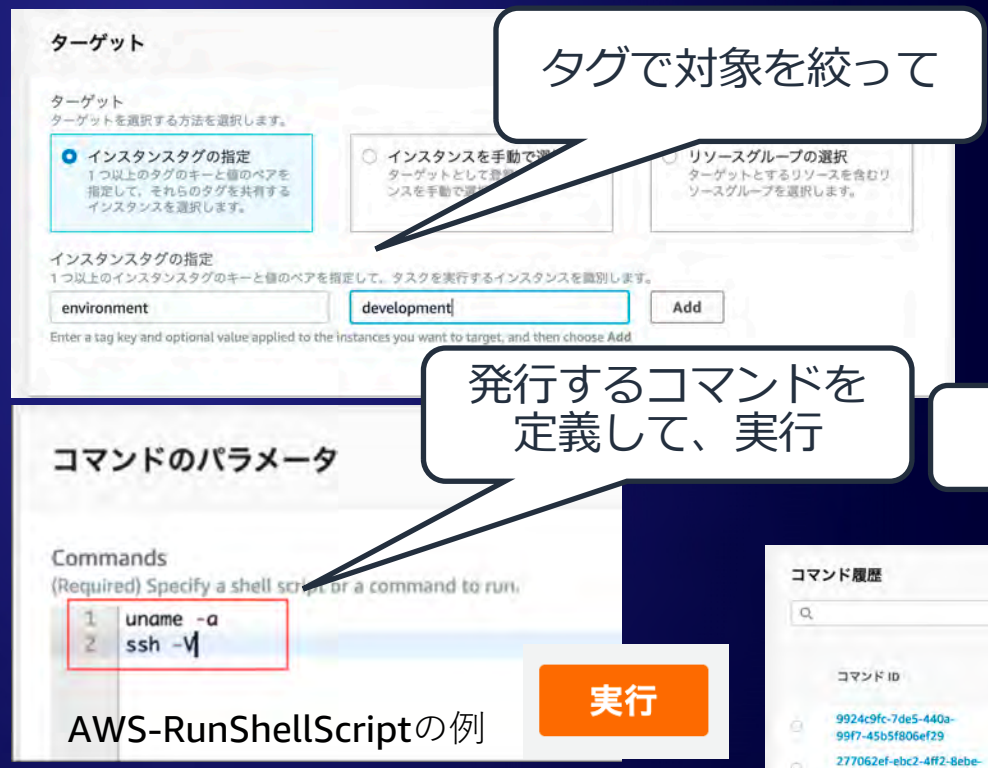
SSM があればこんなことも - 一括操作

- インタラクティブ操作の Session Manager に対して、
  一括操作には RunCommand が便利

全開発サーバーに**このコマンド（スクリプト）を実行**したい

OS 上でコマンドを実行できる





Point

サーバーログイン不要
マネコンから一括操作

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

Case3 サーバーアクセスまとめ

だめだ、手強いぞ
サーバーに入って、本格調査が必要だ

ご紹介した仕組みを使うと

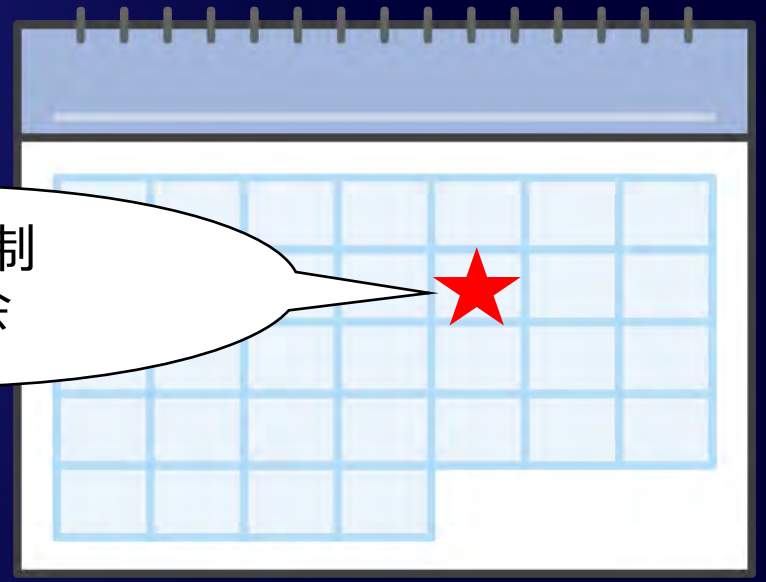
- ✓ 踏み台サーバー経由でのアクセス
- ✓ 踏み台サーバーの管理が必要
- ✓ セキュリティグループでの通信ポートの穴あけが必要

- ✓ SSM Session Manager でアクセス
- ✓ 踏み台サーバーの管理不要、可用性の考慮不要
- ✓ 通信ポートの穴あけ不要のため、インスタンスをセキュアに維持

ある情シスの一日

無事消火できた。
ふう

しかし、息つく暇なく・・・



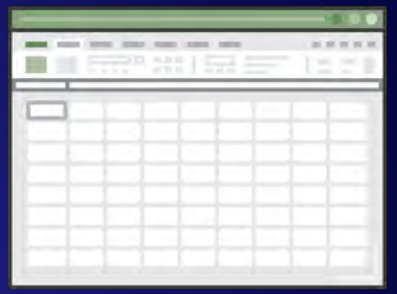
内部統制
委員会

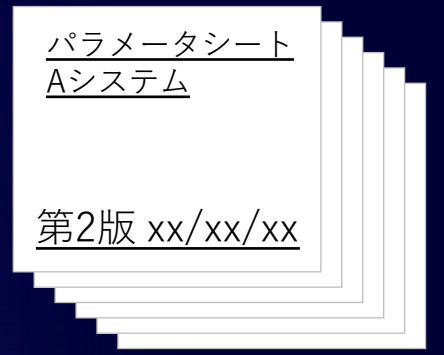
資産棚卸の
準備がぁぁ(+_+)

Case4 資産管理台帳の整備

資産管理台帳の管理は、とても大変・・・

・スプレッドシートでの管理？





最新に Update
されているか心配

やっぱり実機
見ないと不安

・設定がルールに則っているか、チェックはどうしていますか？

構築時にチェックした
ままだな・・・

ポリシー文書

チェックリスト

スマートなチームなら、こんな風に

AWS Config
「高度なクエリ」で
現在の情報をクエリ

直近で作られたインスタンス群を見たい

```
SELECT
  resourceId,
  resourceType,
  resourceCreationTime,
  accountId,
  awsRegion
WHERE
  resourceType = 'AWS::EC2::Instance'
  AND resourceCreationTime BETWEEN '2020-12-01T00:00'
  AND '2021-02-28T00:00'
```

実行

3ヶ月の間に新規に
作られたEC2一覧

resourceId	resourceType	resourceCreationTime	accountId	awsRegion
i-00c32bd2f8ba45ca3	AWS::EC2::Instance	2021-01-18T23:20:26.000Z	[redacted]	ap-northeast-1
i-01d20fc69e19abe48	AWS::EC2::Instance	2020-12-22T23:41:36.000Z	[redacted]	ap-northeast-1
i-05fb3fc5780941541	AWS::EC2::Instance	2020-12-15T00:40:03.000Z	[redacted]	ap-northeast-1

SSH/RDP がフルオープンの SG が発見された！
影響は？

```
SELECT
  resourceId,
  resourceName,
  resourceType,
  relationships,
  accountId,
  awsRegion
WHERE
  relationships.resourceId = 'sg-020eaa6b717c31941'
```

実行

特定のセキュリティ
グループを利用している
リソース一覧

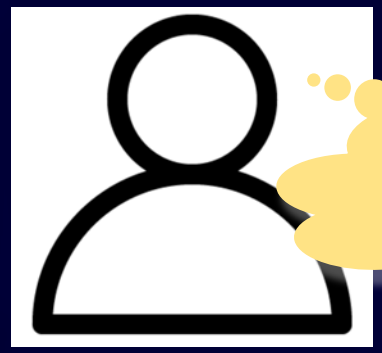
resourceId	resourceName	resourceType	relation
AWS::EC2::SecurityGroup/sg-020eaa6b717c31941	-	AWS::Config::ResourceCompliance	1 項目
arn:aws:elasticloadbalancing:ap-northeast-1:477772(	php-sample-20210118	AWS::ElasticLoadBalancingV2::LoadBal	5 項目
cluster-FXJAURKYY4QHFPO5B4QYQ5WKM4	database-1	AWS::RDS::DBCluster	4 項目

Point

・現在の構成情報をクエリで
確認できる

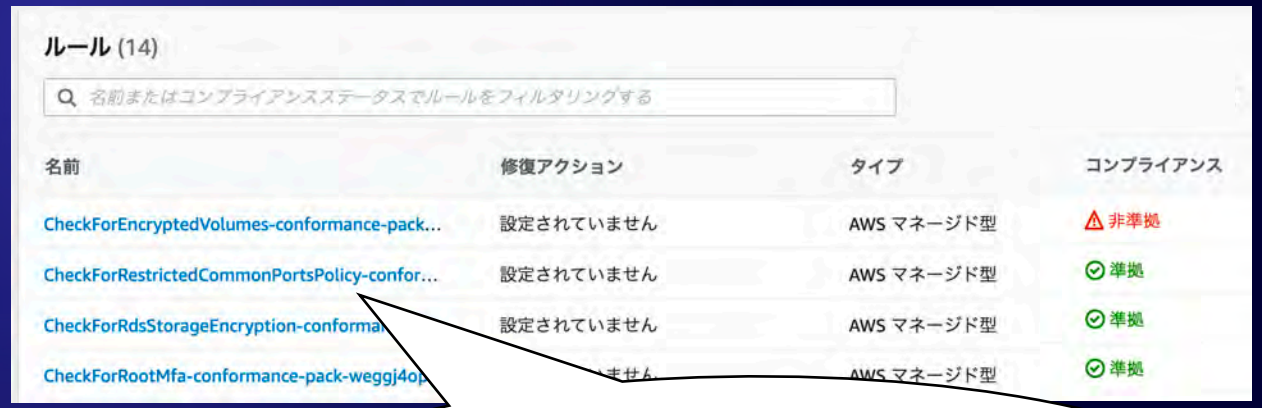
・アグリゲータを用いて、
マルチアカウント、
マルチリージョンでクエリ可能

スマートなチームなら、こんな風に



AWS Config
「適合パック」で、
ルールへの適合確認

事前定義された
ガードレール集
(ConfigRules集) をデプロイ



・それぞれのガードレールの
準拠状況をチェック
・修復アクションの定義も可能

Point

・ガードレール集 (Config Rules 集) を使い、簡単にガバナンスを確保

・必要なガードレールのみピックアップ、カスタムルールの追加など、カスタマイズ可能

・Organizations の組織全体にデプロイ可能

使用サービスのご紹介：AWS Config

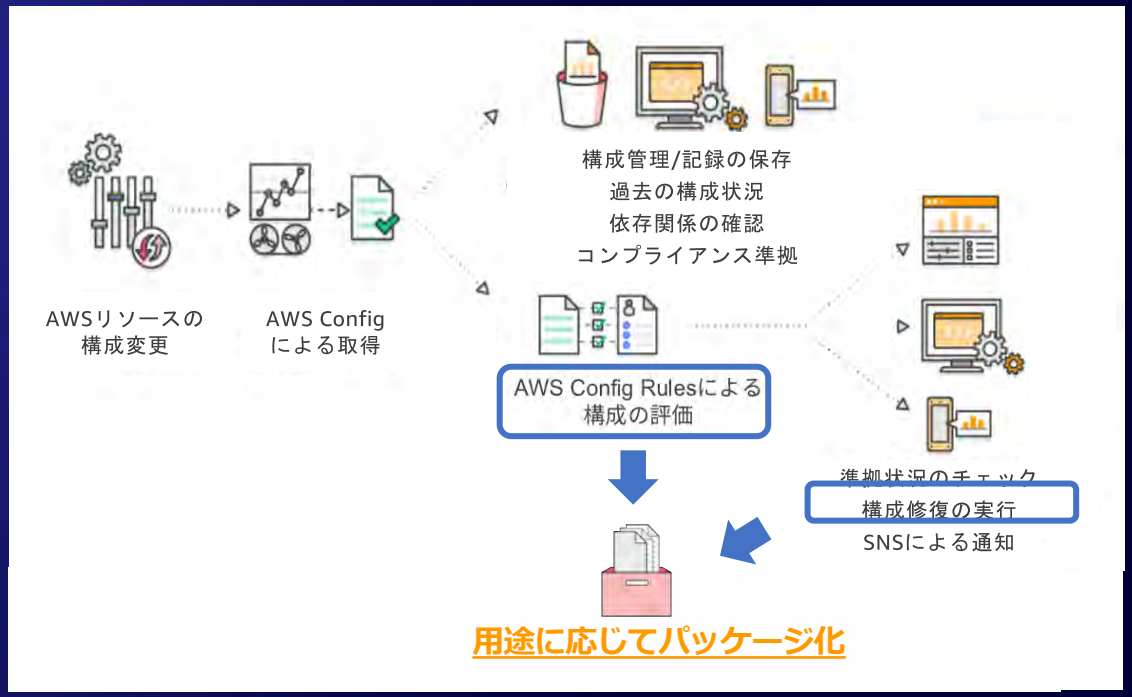
構成情報の記録、評価

高度なクエリ： ためている”今”の情報をクエリ

- AWS リソースの現在の設定状態をクエリできる
- 複数のサンプルが提供されているので、それをカスタマイズしてクエリを作るのが良い。
- アグリゲータの設定をすることで、マルチリージョン・マルチアカウントでの検索が可能

適合パック：構成にルールを設け、ルールに準拠しているかをチェック

- 複数の Config Rule と修復アクションをまとめて用途に応じてパッケージ化したもの
- 単一 AWS アカウントもしくは AWS Organizations の組織全体に対して適用可能



https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/querying-AWS-resources.html
https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/conformance-packs.html

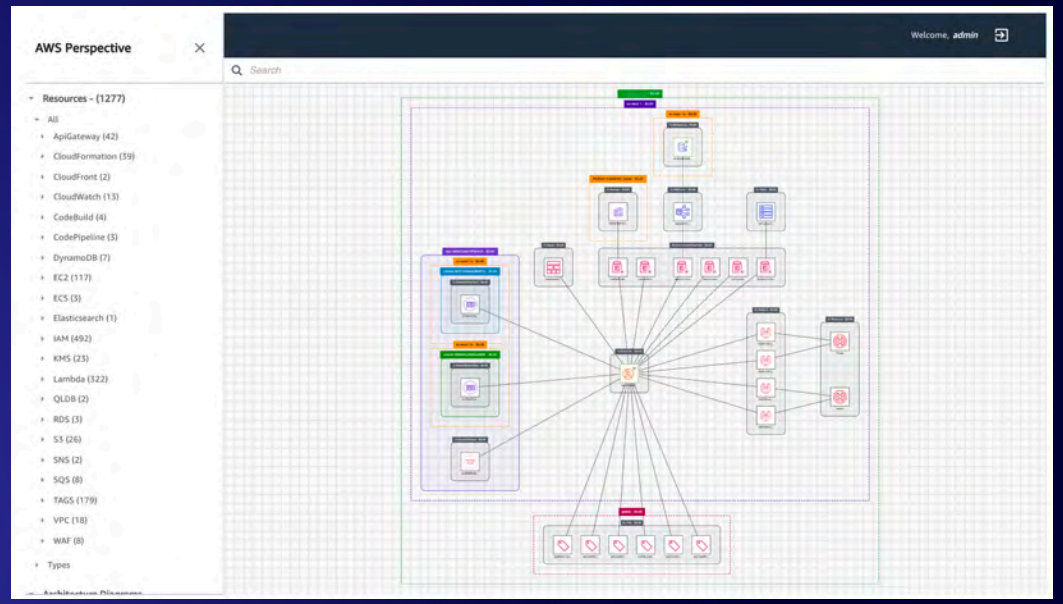
こんなソリューションも：AWS Perspective

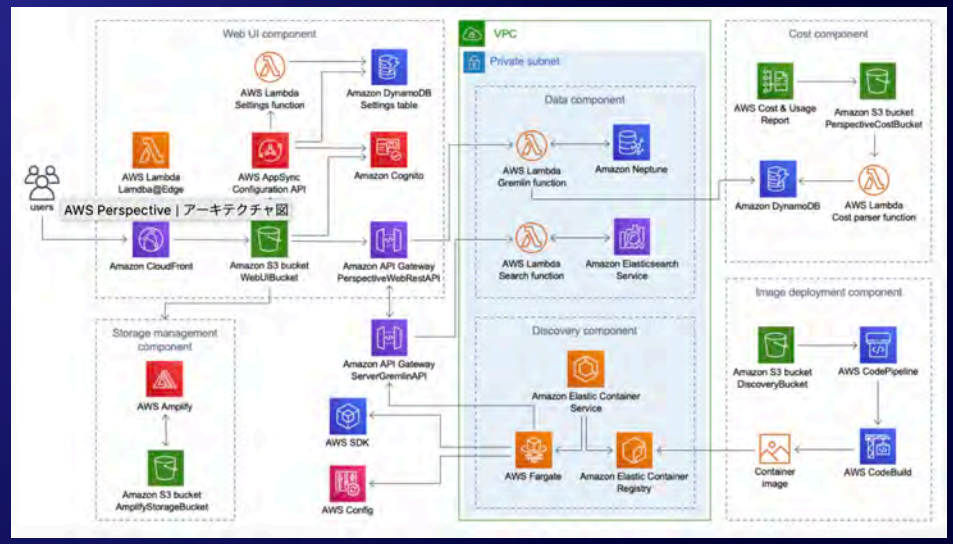
・AWS クラウドのワークロードを
アーキテクチャ図としてすばやく
視覚化するツール

・マルチアカウント、マルチリージョン

・AWS Solutions の一つ
公開されている CloudFormation テンプレートを、自分でデプロイして構成

・複数のコンポーネントが稼働するため、
利用料金に注意

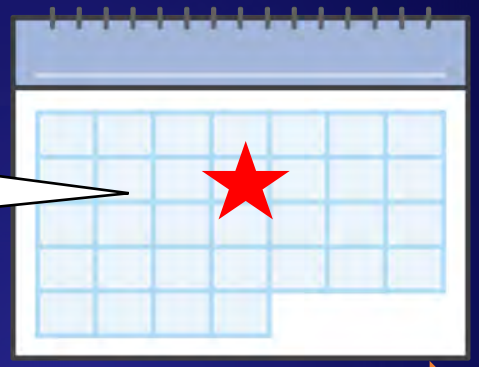




https://aws.amazon.com/jp/solutions/implementations/aws-perspective/

Case4 資産管理台帳の整備 まとめ

内部統制委員会
資産の棚卸しないと



ご紹介した仕組みを使うと

- ✓ スプレッドシートでの管理。最新情報が反映されているか懸念
- ✓ 社内ポリシーに準拠していることの確認がチェックリストベース

- ✓ AWS Config 高度なクエリで、最新情報に常にアクセス
- ✓ AWS Config 適合パックを用いて、ポリシー準拠を確認

(参考) 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10,000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課金)
  - Change Manager (作成した変更リクエストの数とリクエストされた API の数に基づいて請求)
  - 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

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

まとめ

このセッションでは、ある情シスの１日を追っていきました。

- Case1　インベントリの可視化
  - SSM Inventory & Amazon QuickSight で楽々インベントリ管理
- Case2　オンコール
  - Amazon Connect で自動発信で、自動輪番コール
- Case3　サーバーアクセス
  - SSM Session Manager で、踏み台サーバーいらず
- Case4　資産管理台帳の整備
  - AWS Config 高度なクエリで、現在の構成情報にアクセス
  - AWS Config 適合パックを用いてポリシー準拠を確認

まとめ

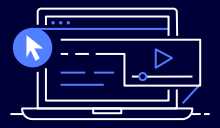
どれか一つのユースケースからでも、
はじめてみるのはいかがでしょうか。

運用を**楽**に、かつ**スケーラブル**に

Thank you!

AWS トレーニングと認定

AWS クラウドをキャリアに活用してください



デジタルトレーニング

クラウドのスキルを構築する無料のオンデマンドコースを探索する

クラスルームトレーニング

エキスパートインストラクターによるトレーニングに参加する

AWS 認定の取得

業界で認められている認定を取得する

教育プログラム

AWS のスキルと経験を持つ人材に出会える

エンタープライズリソース

学習ニーズ分析とAWSランプアップガイドを活用する

詳細はこちら　https://aws.amazon.com/jp/training/