
aws
SUMMIT
ONLINE
JAPAN | MAY 11-12, 2021

AWS-23

AWS Management and Governance サービスによるイノベーションの加速

アマゾン ウェブ サービス ジャパン 株式会社
ソリューションアーキテクト
柳　嘉起 (Yanagi, Yoshiki)

ソリューションアーキテクト

柳　嘉起（Yanagi Yoshiki）

経歴

- 前職ではSIerにて、公営競技システムの構築/運用を担当
  - 主な業務内容はシステムの移行計画策定/インフラ設計/構築/試験/運用
  - お客様先に常駐し、システム運用に関するコンサルティングなども経験

好きなサービス

- AWS Management and Governance Service
- AWS Support

想定聴講者と本セッションでお話しすること

■想定聴講者

・システム運用に携わっている方
・モダンアプリケーションの運用管理にお悩みの方
・AWSへの移行をご検討中の方

■本セッションでお話しすること

・AWS Management and Governance サービスを使って実現できること
・特に下記について詳しくご説明

・統制の自動化（ガードレール）と監査のしくみの実装（AWS Config ＋AWS Audit Manager）
・オブザーバビリティサービスのご紹介
・運用を効率化する AWS Systems Manager の新機能

アジェンダ

1．はじめに
2．AWS Management and Governance サービス
- Set up Governance
- Enable compliance
- Provision & orchestrate
- Monitor & observe
- Centralize operations

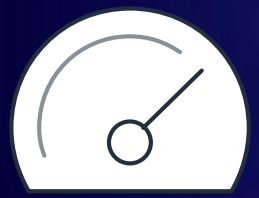
3．まとめ
4．NEXT STEPS

1. はじめに

ビルダーとIT管理部門の要求におけるバランス

ビルダー

開発速度の向上



AWSがもたらす
スピード

IT管理部門

ガバナンス確立

大規模な一元管理

アジリティとガバナンスのコントロール

アジリティ

セルフサービス

迅速な実験

修復の自働化

変化への迅速な対応

ガバナンス

セキュリティ

コンプライアンス

運用管理

AWS Management and Governance サービス

Set up governance

Enable compliance

Provision & orchestrate

Monitor & observe

Centralize operations

AWS CloudFormation

NEW! AWS Audit Manager

NEW! AWS Proton

NEW! AWS Distro for OpenTelemetry

NEW! Amazon Managed Service for Prometheus

NEW! Amazon Managed Service for Grafana

AWS Cost and Usage Report

AWS Systems Manager

AWS Service Catalog

AWS Control Tower

AWS Marketplace

Amazon CloudWatch

AWS X-Ray

AWS Cost Explorer

AWS CloudTrail

AWS Config

AWS License Manager

AWS Budgets

AWS Well-Architected Tool

AWS Organizations

AWS Managed Services

2. AWS Management and Governance サービス

- Set up Governance
- Enable compliance
- Provision & orchestrate
- Monitor & observe
- Centralize operations

Management and Governance サービス


Set up governance


Enable compliance


Provision & orchestrate


Monitor & observe


Centralize operations


AWS Control Tower


AWS Organizations


AWS Security Hub


Amazon GuardDuty

AWS Control Tower

セキュアで事前設定済みのAWSアカウントを提供する仕組み
・ガードレール設置、アカウント発行機能、ダッシュボード

AWS Organizations

AWS リソースの増加に合わせて、環境を一元的に管理し、統制
・権限制御　Service Control Policy(SCP)
・一括請求　コンソリデーティッドビリング

AWS Security Hub

セキュリティアラートの一元的な表示および管理を行い、セキュリティチェックを自動化

Amazon GuardDuty

インテリジェントな脅威検出と継続的なモニタリングで AWS のアカウント、ワークロード、データを保護

Management and Governance サービス


Set up governance


Enable compliance


Provision & orchestrate


Monitor & observe


Centralize operations


AWS Control Tower


AWS Organizations


AWS Security Hub


Amazon GuardDuty

ガードレール　大事な概念なのでもう一度・・・

- 実施してはいけない操作の禁止、危険な設定の監視を自動的に行うしくみ
- 審査プロセスにより立ち止まり検査するのではなく、ルールを逸脱する行為をリアルタイムでチェックする仕組みを設けることにより、セキュリティとアジリティを両立する考え方

Management and Governance サービス


Set up governance


Enable compliance


Provision & orchestrate


Monitor & observe


Centralize operations


AWS CloudTrail


AWS Config


AWS Audit Manager

AWS CloudTrail

アカウントアクティビティをログに記録し、継続的に監視

AWS Config

AWS リソースの構成情報や設定を継続的にモニタリングおよび記録し、評価を自動的に実行

AWS Audit Manager NEW!

AWS の使用状況を継続的に監査して、従来手動で行われていた証跡収集作業を削減

INTRODUCING

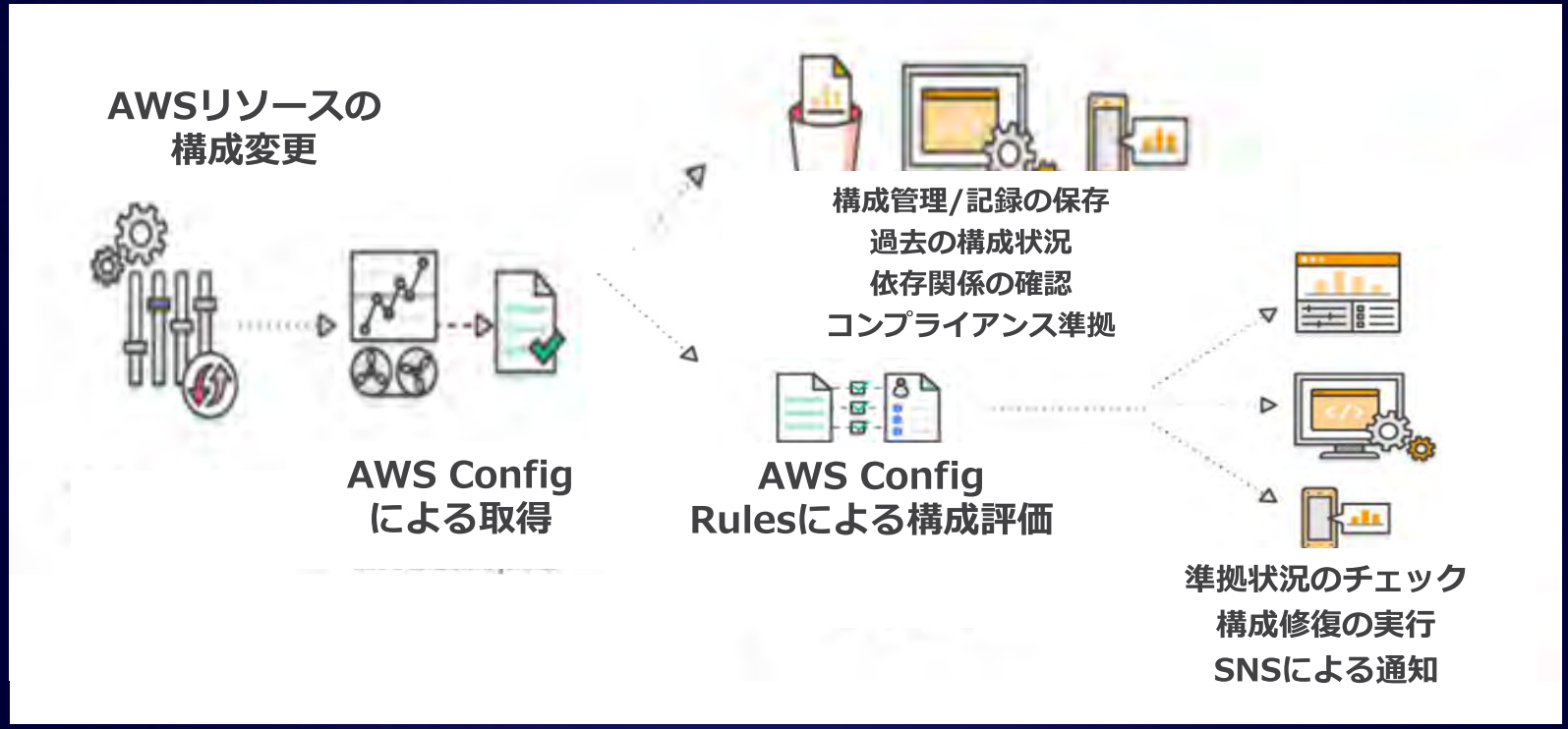
AWS Config

AWS リソースの構成情報や設定を継続的にモニタリングおよび記録し、評価を自動的に実行

・AWSリソースの構成情報、変更履歴を記録
・構成情報を定期的にスナップショットとして保存
・必要に応じAmazon SNS（Simple Notification Service）を使った通知も可能

【Config Rules】

・構成情報を元に、現在のシステムがあるべき状態になっているか評価できる



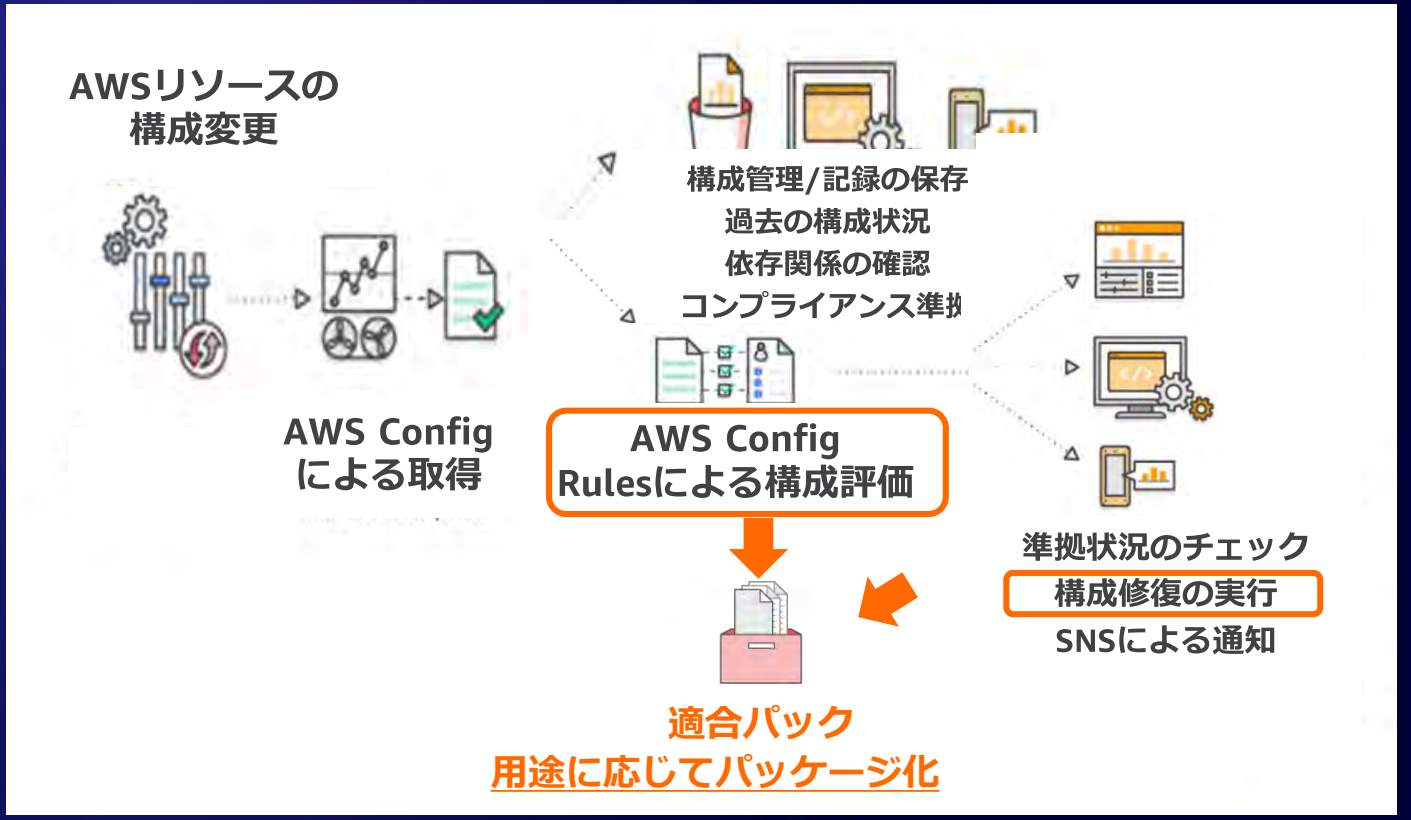
AWS Config 適合パック (Conformance Pack)

設定管理のための共通コンプライアンスフレームワーク

- 複数の Config Rules 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
- 単一AWSアカウント、AWS Organizations の組織全体に対して適用可能
- 不変性（immutable）

サンプルテンプレート

- テンプレートを使用すると、FedRAMP、HIPAA、PCI DSS など、AWS のベストプラクティスおよび規制基準に適合した適合パックをすばやく使い始められる
- 2021年3月時点で50以上のサンプルテンプレートが利用可能

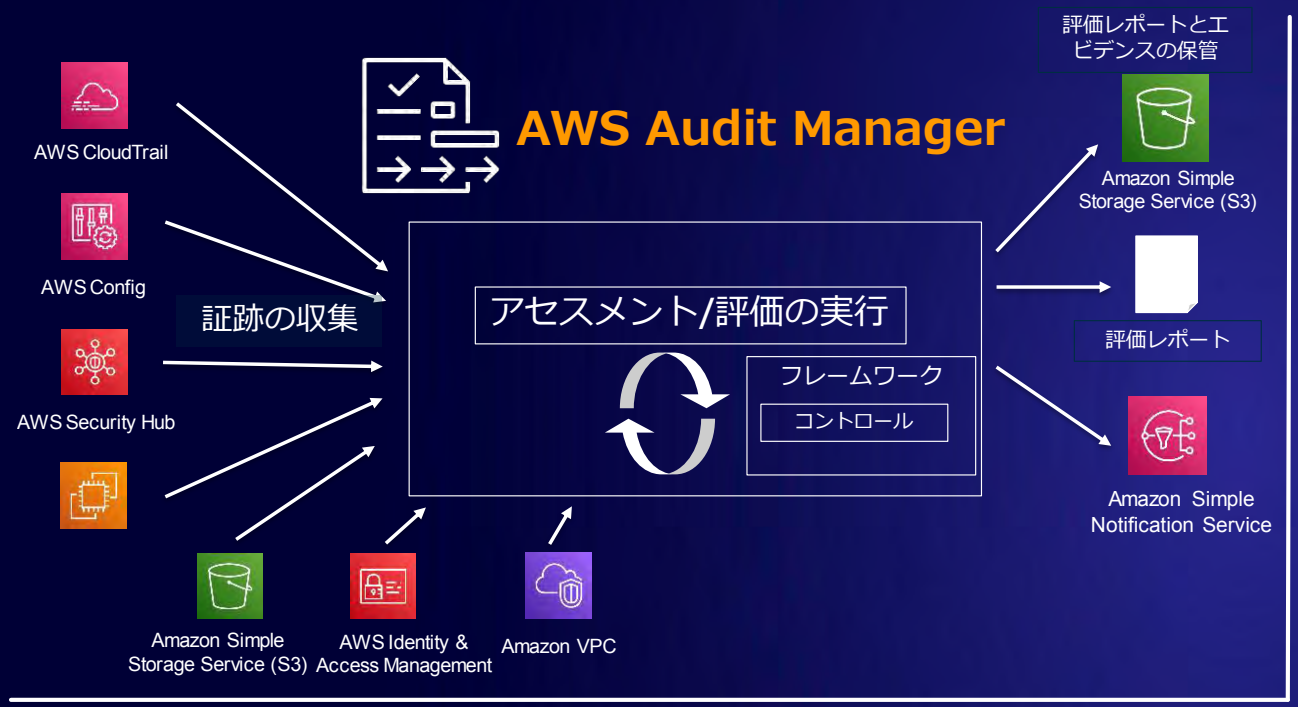


INTRODUCING

AVAILABLE

AWS Audit Manager

AWS の使用状況を継続的に監査して、従来手動で行われていた証跡収集作業を削減



- AWSの使用状況を継続的に監査することにより リスクアセスメントや規制、 業界標準への準拠確認をサポート
- CIS AWS Foundations BenchmarkやGDPR、 PCI DSSについて事前定義フレームワークを 提供し、AWS上の監査証跡を自動で収集

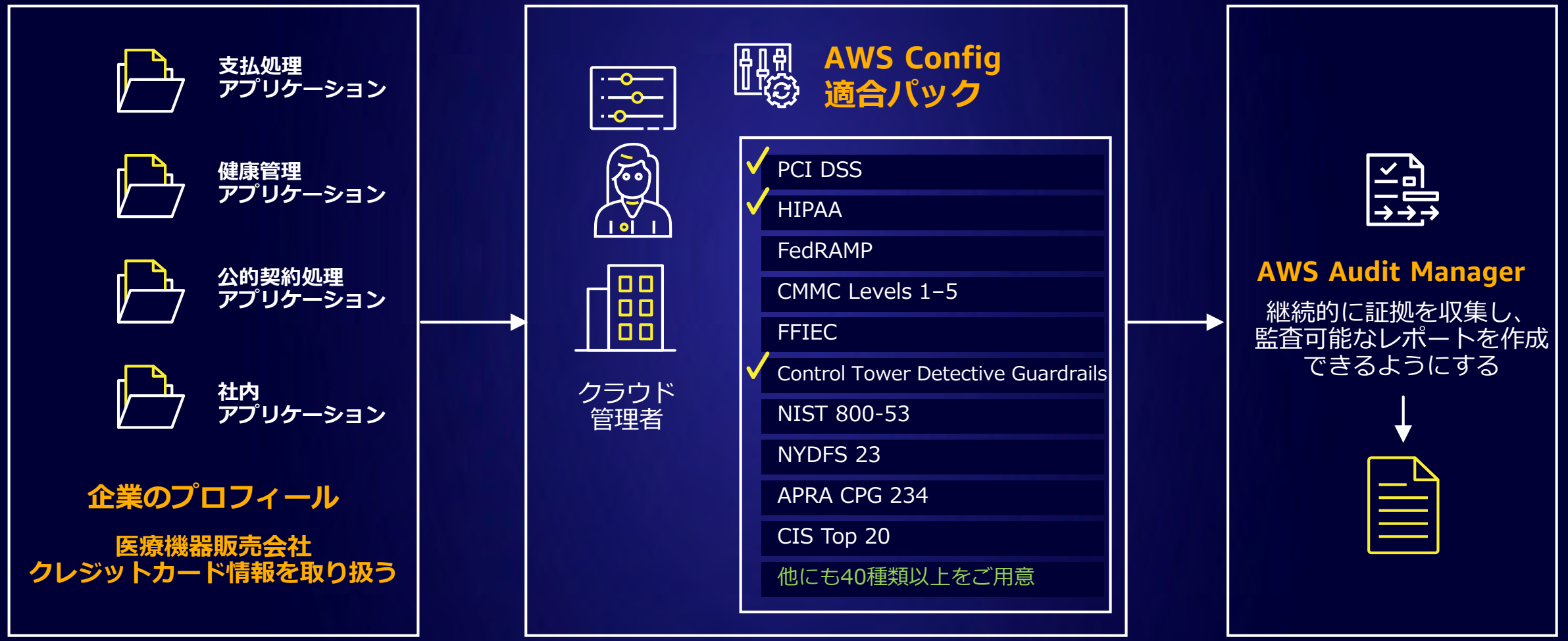
【お客様のメリット】

- 監査証跡の収集を手作業で行う手間を削減し、監査対応のレポートを短時間で生成できる

【監査人のメリット】

- 監査証跡の収集を手作業で行う手間を削減
- 監査証跡の真正性が Audit Manager により担保される
- リアルタイムに近い形で最新の証跡を取得できる

【デモ】 AWS Config 適合パック+AWS Audit manager



管理ツール

AWS Config
AWS リソースの設定を記録して評価する

AWS Config では、AWS アカウントに関連付けられたリソースの詳細ビューが表示されます。これには、リソースの設定方法、相互関係、時間の経過とともに設定や関係が変化した様相などが含まれます。

今すぐ始める

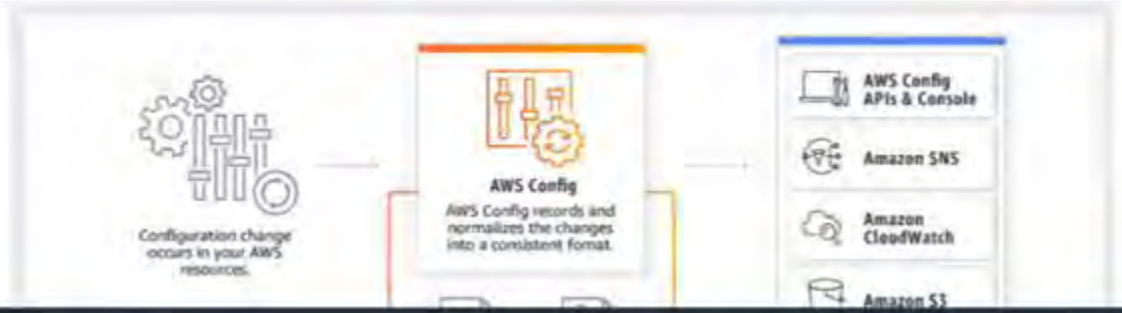
AWS リソースと AWS 以外のリソースの要約ビュー、および各 AWS リージョンのルールとリソースにおけるコンプライアンス状態。

ダッシュボードを表示する

料金表

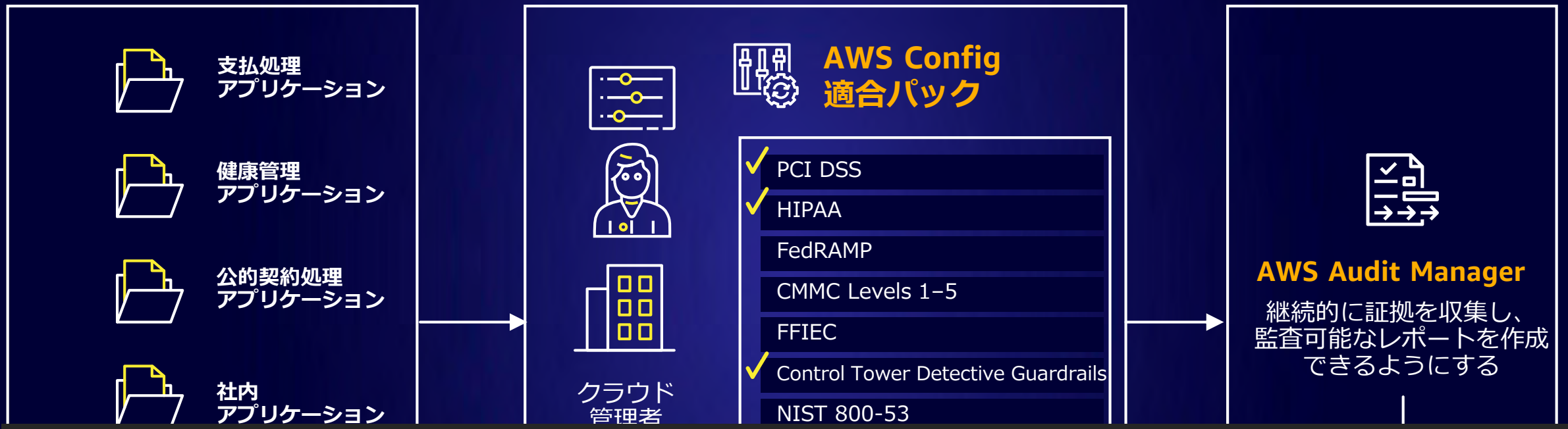
AWS Config	料金の詳細
AWS Config ルール	料金の詳細
AWS GovCloud (米国)	料金の詳細
TCO 計算ツール	AWS 料金計算ツール

仕組み




AWS Audit Manager
Getting started
Assessments
Delegations
Assessment reports
Framework library
Control library
Settings
Notifications
Security, Identity, & Compliance, Management & Governance
AWS Audit Manager
Continuously audit your AWS usage to simplify how you assess risk and compliance
AWS Audit Manager helps you continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards. Audit Manager makes it easier to evaluate if your policies, procedures, and activities, also known as controls, are operating as intended. The service offers prebuilt frameworks with controls that are mapped to well-known industry standards and regulations, full customization of frameworks and controls, and automated collection and organization of evidence as defined by each control requirement. When it is time for an audit, AWS Audit Manager helps you manage stakeholder reviews of your controls and enables you to build audit-ready reports with much less manual effort.
Launch AWS Audit Manager
Start from a pre-built standard framework based on common compliance standards and developed with AWS best practices in mind.
Launch AWS Audit Manager
Pricing
Per resource assessments, per account, per
フィードバック
日本語
© 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転用禁止。
プライバシーポリシー
利用規約
Cookie の設定

【デモ】 AWS Config 適合パック+AWS Audit manager



AWS Config Rules（ルール）

AWSの環境が指定したルールに適合しているかどうかを「検知」する仕組み

適合パック

目的別に複数の Config Rules と修復アクションをパッケージ化して、まとめて適用できるように

AWS Audit Manager

Config Rules 等で収集した情報を元に、監査レポートの作成をサポートするサービス

Management and Governance サービス

AWS CloudFormation | **AWS Service Catalog** | **AWS Marketplace** | **AWS Proton**

AWS CloudFormation

Infrastructure as Code で AWS 及び サードパーティの
システムプロビジョニングを高速化

AWS Service Catalog

AWSサービスのカタログを作成および管理し、組織で利用できるようにする

AWS Marketplace

8,000 を超えるサードパーティーアプリケーションの実行

AWS Proton NEW!

コンテナおよびサーバーレスアプリケーション向けの
アプリケーションデプロイサービス

RECENT RELEASE

AWS CloudFormation Modules

Amazon CloudFormationにおいて再利用可能な部品を
Moduleとして定義し、再利用性を高めることができる

Management and Governance サービス

Set up governance

Enable compliance

Provision & orchestrate

Monitor & observe

Centralize operations

Amazon CloudWatch

AWS X-Ray

Amazon CloudWatch

AWS とオンプレミスにおける
モニタリング/オブザーバビリティサービス

AWS X-Ray

分散アプリケーションの分析およびデバッグ

RECENT RELEASE

Amazon CloudWatch Lambda Insights

- Lambda Functionのパフォーマンス監視やトラブルシュート、最適化を可能にする機能
- Functionに関するメトリクスを自動的にダッシュボードにとりまとめ、メモリリークや新バージョンのデプロイによる性能変化を可視化できる

AWS CloudWatchのビジュアライズ強化

Working with the open source community

Grafana

Prometheus

CLOUD NATIVE COMPUTING FOUNDATION

kubernetes

cortex

OpenTelemetry

splunk>

sumo logic

INTRODUCING

AVAILABLE

AWS Distro for OpenTelemetry

AWS によりサポートされるOpenTelemetryのオープンソースディストリビューション

- AWSによるセキュリティ、パフォーマンステストとサポート
- AWS コンテナと AWS Lambda コンソールから、ワンクリックでのデプロイと設定が可能
- CloudWatch、X-Ray、Elasticsearch サービス、パートナーソリューションを含む AWS モニタリングソリューションのExporterを用意

LEARN MORE | AWS re:Invent 2020 session OPN301 – Open-source observability at AWS

https://aws-otel.github.io/

INTRODUCING

IN PREVIEW

Amazon Managed Service for Prometheus（AMP）

コンテナ環境向けのモニタリングとアラーティングのマネージドサービス

- PromQLを利用して、インフラを管理することなく AWSまたはオンプレのコンテナワークロードを監視できる
- ワークロードの拡大縮小に応じて自動的にスケーリング AZをまたいだレプリケーションもサポート
- IAMによるアクセス権限制御や、PrivateLinkによるセキュアな アクセスを提供。API呼び出しはCloudTrailで記録される。
- サービス検出・メトリック収集にAWS Distro for OpenTelemetry が利用可能。また、Amazon Managed Service for Grafana との連携によるリッチなデータ可視化も

LEARN MORE | AWS re:Invent 2020 session EMB046 – Introducing Amazon Managed Service for Prometheus

INTRODUCING

IN PREVIEW

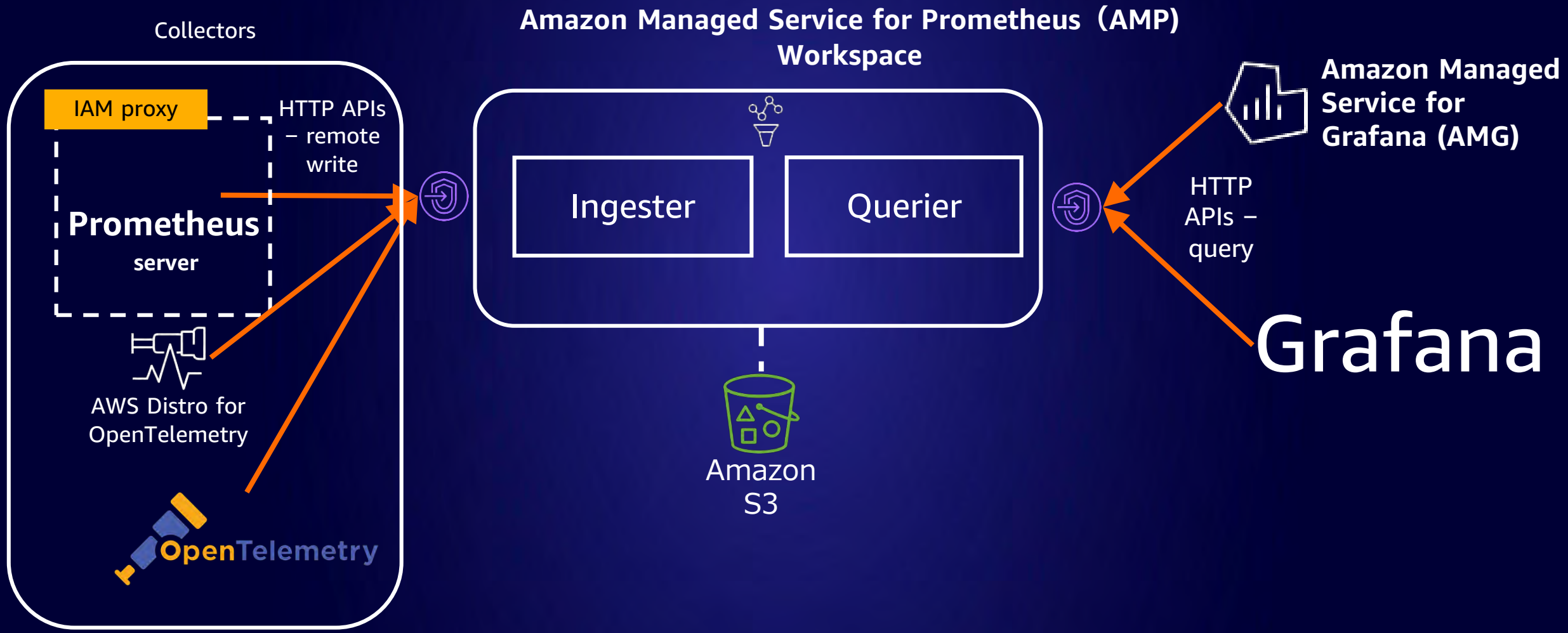
Amazon Managed Service for Grafana（AMG）

Grafana Labsと連携して開発された、フルマネージドなデータ可視化サービス

- 複数のデータソースからのメトリックやログを視覚化できる
- Grafanaサーバの構築、スケーリング、パッチ適用などのメンテナンスはAWSが実施。サーバ運用の手間をオフロードできる
- AWS SSOと統合されており、ユーザ毎にアクセスできるダッシュボードとデータソースにシームレスなアクセスが可能
- AWSアカウントとリソースの検出機能
- APIを利用して既存のGrafana環境からクエリとダッシュボードをインポート可能

LEARN MORE | AWS re:Invent 2020 session EMB048 – Introducing Amazon Managed Service for Grafana

AMP & AMG セットアップ例



Management and Governance サービス

Set up governance

Enable compliance

Provision & orchestrate

Monitor & observe

Centralize operations

AWS Systems Manager

運用を効率化するコックピット

運用管理

運用に必要なデータを
ダッシュボードとして提供

可視化

アプリケーション管理

アプリケーションリソースを
グループ化し、一元管理を実現

アプリケーション指向

変更管理

メンテナンス/デプロイ
タスクを自動化

自動化

ノード管理

AWSリソース、オンプレミス
Windows & Linuxの管理

スケーラブル

AWS Systems Manager の機能(1/2)

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

運用管理

Explorer	運用アイテム情報のダッシュボード
OpsCenter	運用アイテム（対応が必要なイベント）の管理

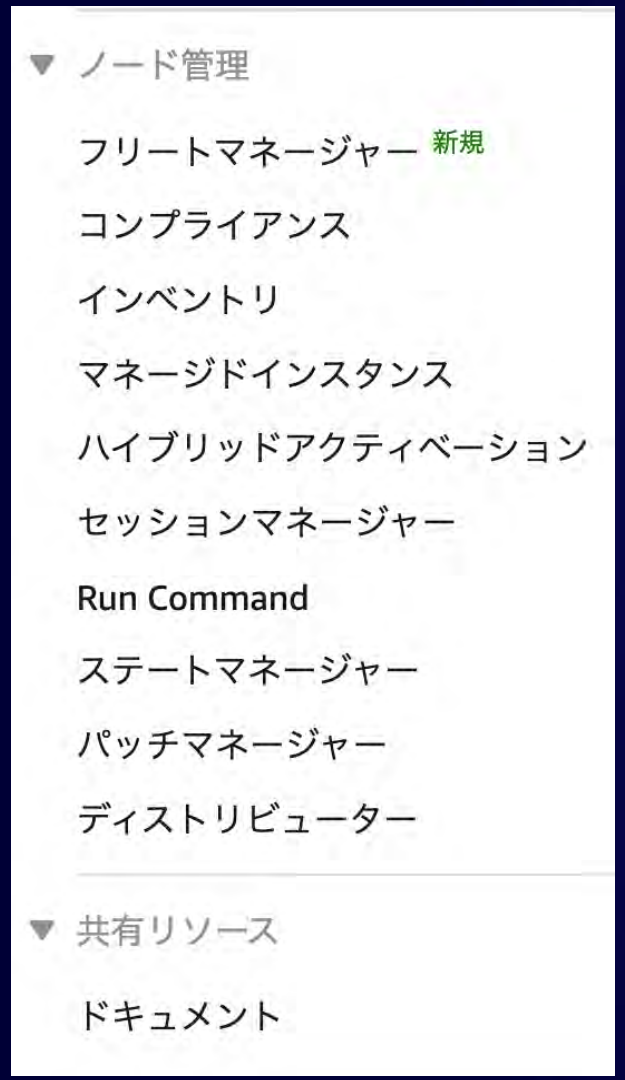
アプリケーション管理

アプリケーションマネージャー	アプリケーションを構成するAWS上のリソースを一元的に管理
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

変更管理

変更マネージャー	システムの構成変更管理に必要な、申請、承認、実装、結果というワークフローを簡素化
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 Systems Manager の機能(2/2)



ノード管理

フリートマネージャー	ビジュアルUIでLinux、Windows、macOSのサーバ群を管理する
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

INTRODUCING

AVAILABLE

AWS Systems Manager 変更マネージャー

クラウドとオンプレミスの変更管理

・システムの構成変更管理に必要な、申請や承認のワークフローをベストプラクティスに基づき効率化する

・事前に定義されたワークフローに基づきプロセスを回すことで意図しない変更が適用されることを防止

・CloudWatchのアラームと連携し異常時のロールバックにも対応

・SSM Change Calenderに基づき、ビジネス上の重要イベントなど変更を加えるべきではない時間帯の変更を避ける制御もできる

・AWS OrganizationsとAWS SSOと統合されており、システムに対する変更を記録・監査し可視性を高めることができる

LEARN MORE | AWS re:Invent 2020 session MGT401 – Automate anything with AWS Systems Manager

INTRODUCING

AVAILABLE

AWS Systems Manager フリートマネージャー

AWS Systems ManagerのUIから、Linux、Windows、macOSのサーバ群を管理するビジュアルツールを提供

- SSHやRDPで個別にサーバに接続することなく、AWSのコンソールからサーバ群の管理作業を実行可能
- ファイルシステムの参照やユーザ管理、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
- 管理対象サーバはEC2に限らず、Systems Managerエージェントが導入されていれば、オンプレにあるサーバも管理可能

LEARN MORE | AWS re:Invent 2020 session MGT401 – Automate anything with AWS Systems Manager

高速セットアップ

▼ 運用管理
エクスプローラー
OpsCenter
CloudWatch ダッシュボード
PHD

▼ アプリケーション管理
アプリケーションマネージャー 新規
AppConfig
パラメータストア

▼ 変更管理
変更マネージャー 新規
自動化
カレンダーの変更
メンテナンスウィンドウ

▼ ノード管理
フリートマネージャー 新規

MANAGEMENT TOOLS

AWS Systems Manager
Gain Operational Insight and Take Action on AWS Resources.

Get Started with Systems Manager

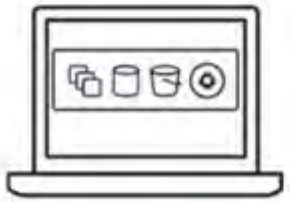
View operational data for groups of resources, so you can quickly identify and act on any issues that might impact applications that use those resources.

How it works

Group your resources

View insights

See relevant



Take action

Mitigate issues by

More resources

Documentation

API reference

FAQs

INTRODUCING

AVAILABLE

AWS Systems Manager アプリケーションマネージャー

アプリケーションを構成するAWS上のリソースを一元的に管理する

- タグやリソースグループ、CloudFormationスタックを選択してアプリケーションの構成要素を定義
- アプリケーションの視点でアラーム、運用上の問題、ログなどをダッシュボードに一括表示できる
- 問題に対処するための操作一式を定義したAutomation Runbookを作成しておけば、画面上でRunbookを呼び出すことで調査・修復を容易に実行可能

LEARN MORE | AWS re:Invent 2020 session MGT401 – Automate anything with AWS Systems Manager

高速セットアップ

▼ 運用管理
エクスプローラー
OpsCenter
CloudWatch ダッシュボード
PHD

▼ アプリケーション管理
アプリケーションマネージャー 新規
AppConfig
パラメータストア

▼ 変更管理
変更マネージャー 新規
自動化
カレンダーの変更
メンテナンスウィンドウ

▼ ノード管理
フリートマネージャー 新規

MANAGEMENT TOOLS

AWS Systems Manager
Gain Operational Insight and Take Action on AWS Resources.

Get Started with Systems Manager

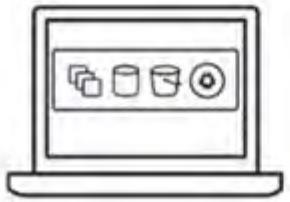
View operational data for groups of resources, so you can quickly identify and act on any issues that might impact applications that use those resources.

How it works

Group your resources

View insights

See relevant



Take action

Mitigate issues by

More resources

Documentation

API reference

FAQs

テクノロジーパートナーソリューション

Note that this grouping is not comprehensive but is meant to represent only a selection of these AWS Partners

3. まとめ

まとめ

Set up governance

AWSアカウントの構成、ガバナンスをどのように確立していくかの枠組み

禁止すべき行為は予防的ガードレール（AWS Organizations SCP）で防ぐ

Enable compliance

コンプライアンスを実装

・発見的ガードレール（AWS Config Rules）/ 適合パックで素早く導入

ビルダーの自由を意識し、ガバナンスコントロールと開発のスピードを両立

・AWS Audit Manager で監査対応を支援

Provision & orchestrate

環境のプロビジョニング、オーケストレーション

・Infrastracture as Code、テンプレートというクラウドならではのリソース管理手段

Monitor & observe

モニタリング、オブザーバビリティ

・アプリケーションの正常性、またサービスに影響が出ていないことの観測が重要に

・オブザーバビリティを実現する CloudWatch に加えて新マネジメントサービスの追加

Centralize operations

運用を効率化するコックピット

・AWS Systems Manager

・可視化 / アプリケーション指向 / 自動化 / スケーラブル

4. NEXT STEPS

NEXT STEPS

・関連セッションから、詳細な解説をご確認ください！
・ハンズオンでAWS Management and Governance サービスをぜひご体験下さい！

AWS Summit Online 2021

AWS-51　情シス向け運用ユースケース
・運用ケースに応じたAWSサービスの使い方がわかる！運用を楽にスケーラブルに！

AWS-35　Open-source observability at AWS　可観測性を支える OSS と AWS の『いま』を知る
・AWS上での可観測性を支えるOSSの「いま」を本セッションでクイックに学べる！

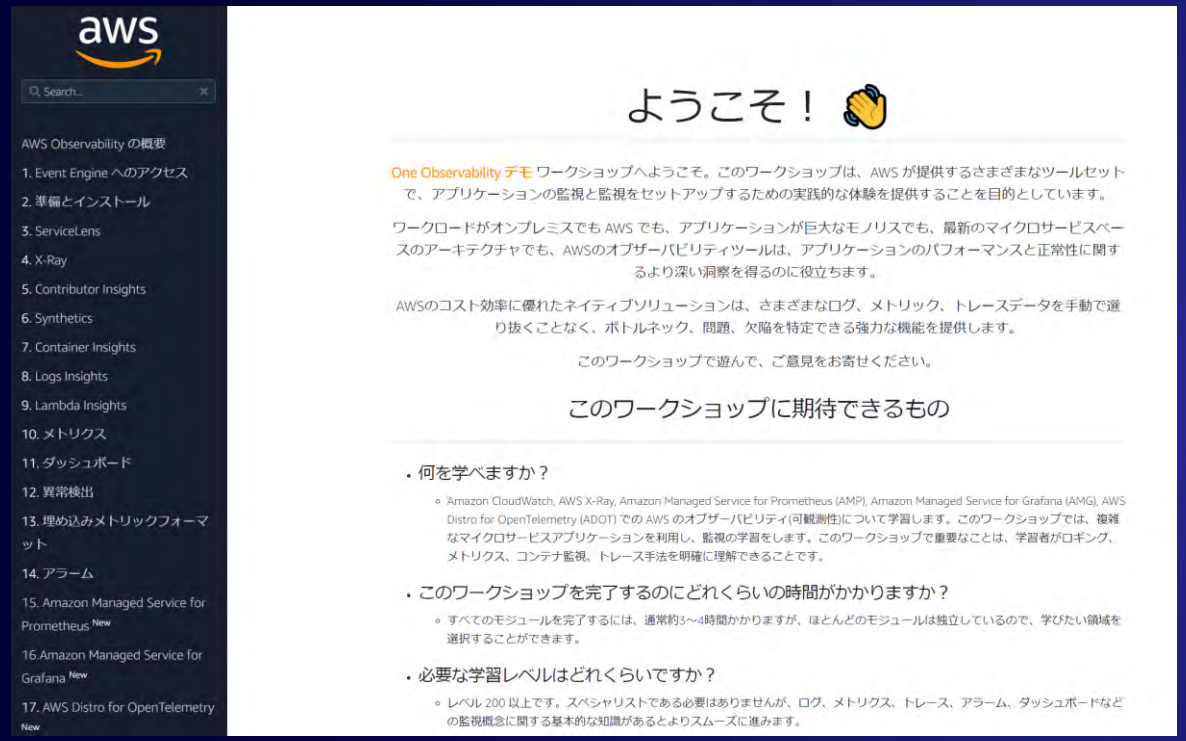
AWS-31　AWSで始める Infrastructure as Code
・インフラストラクチャのコード管理（Infrastructure as Code）のベストプラクティスを紹介！

AWS re:Invent 2020 session

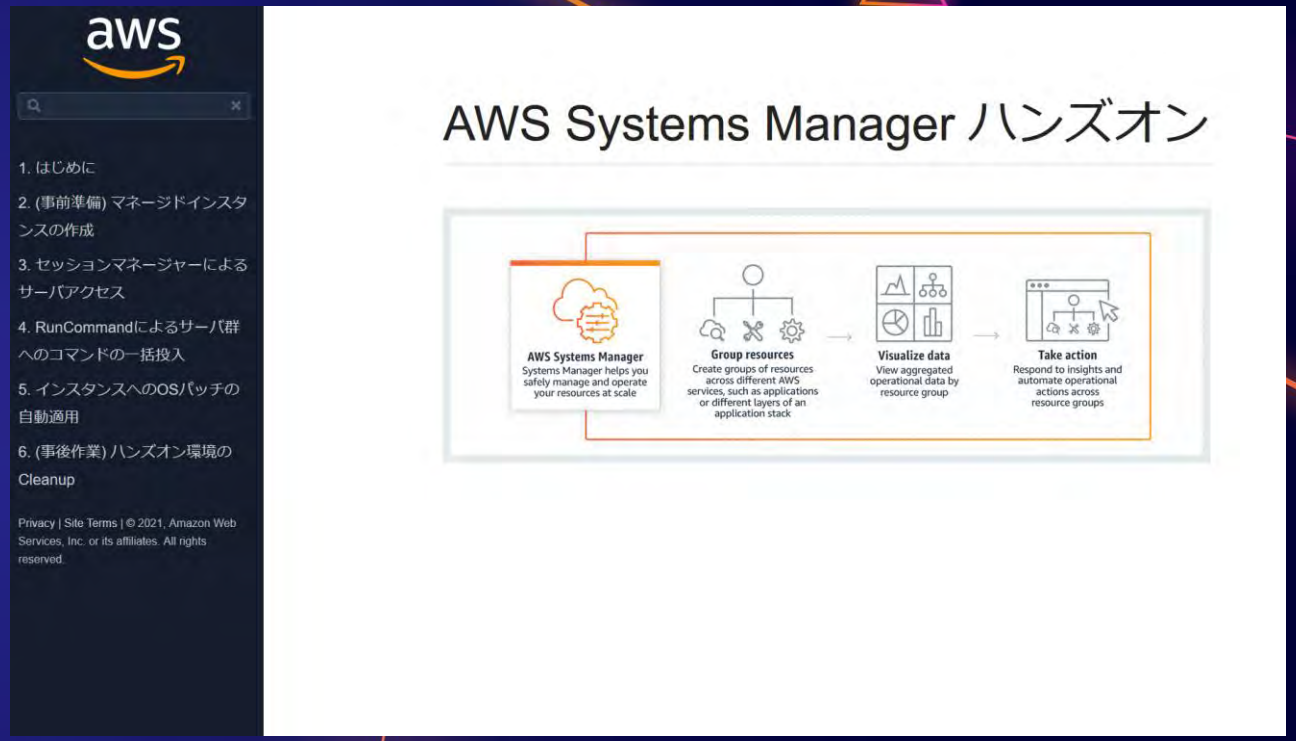
AWS re:Invent 2020 session OPN301 – Open-source observability at AWS
AWS re:Invent 2020 session EMB046 – Introducing Amazon Managed Service for Prometheus
AWS re:Invent 2020 session EMB048 – Introducing Amazon Managed Service for Grafana
AWS re:Invent 2020 session MGT401 – Automate anything with AWS Systems Manager

NEXT STEPS

・紹介ページに記載したリンク（LEARN MORE）から、詳細な解説をご確認ください！
・**ハンズオンでAWS Management and Governance サービスをぜひご体験下さい！**



https://observability.workshop.aws/ja/



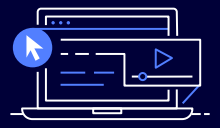
https://ssm-basic-handson.workshop.aws/
https://ssm-inventory-visualize.workshop.aws/

Thank you!

アマゾン ウェブ サービス ジャパン 株式会社
ソリューションアーキテクト
柳　嘉起 (Yanagi, Yoshiki)

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/