[AWS Black Belt Online Seminar]

AWS Config

サービスカットシリーズ

Security Solutions Architect
桐谷 彰一
2019/06/18

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

自己紹介

名前： 桐谷 彰一（きりたに しょういち）

所属： ソリューションアーキテクト　セキュリティスペシャリスト

経歴： セキュリティベンダー、ネットワークベンダーのプリセールスエンジニア
エンタープライズ、官公庁のお客様のセキュリティ対策のご支援

好きなAWSサービス：

Amazon GuardDuty

AWS Security Hub

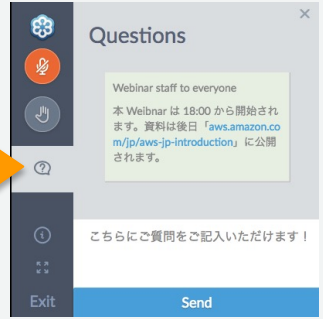
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
  お答えできませんのでご了承下さい

① 吹き出しをクリック
② 質問を入力
③ Sendをクリック



Twitter 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2019年6月18日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(http://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。

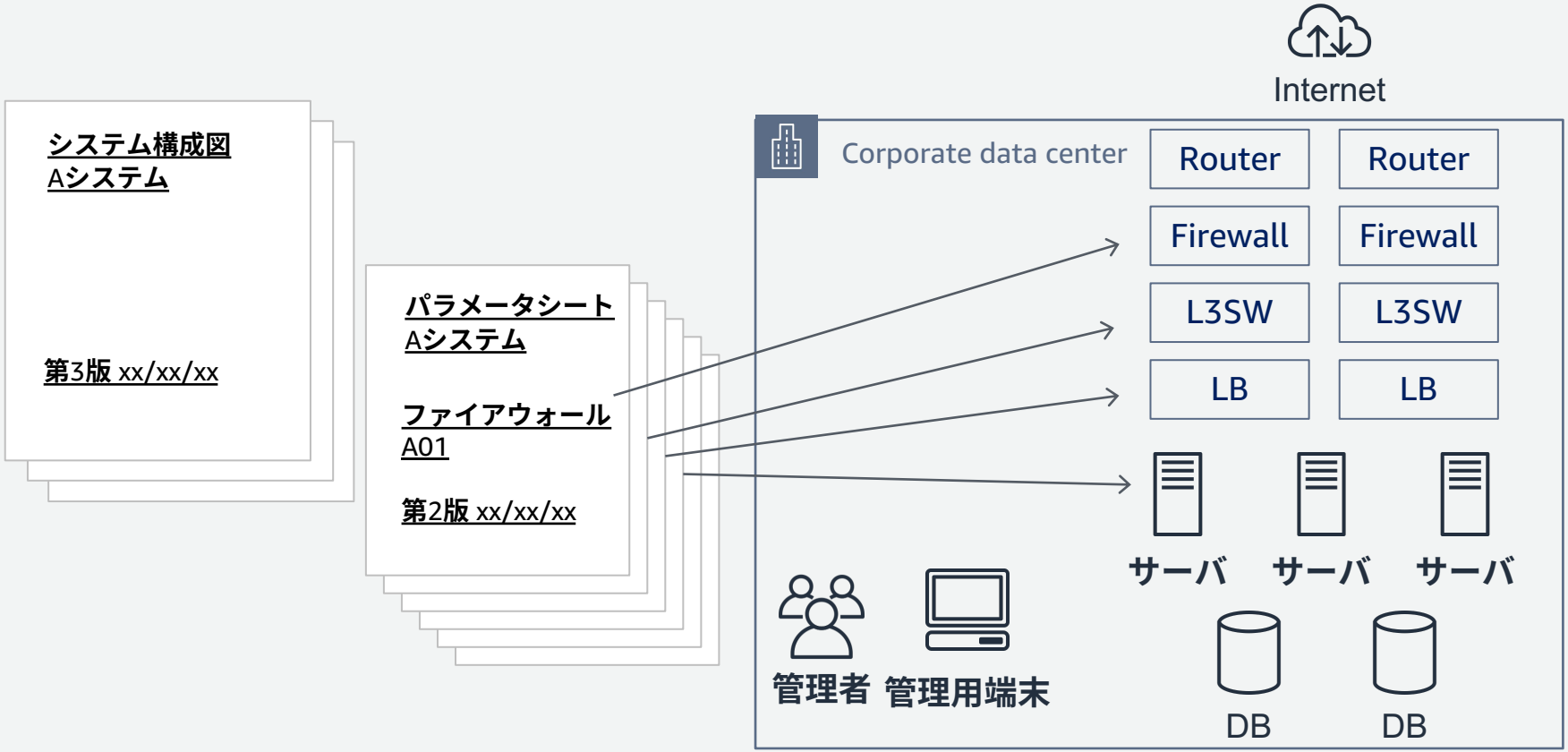
- 価格は税抜表記となっています。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

本日のアジェンダ

- 構成管理にまつわる課題
- AWS Config 概要
- AWS Config Rules 概要
- ユースケース、ベストプラクティス
- 料金について
- まとめ

構成管理の手法



構成管理にまつわる課題

管理者

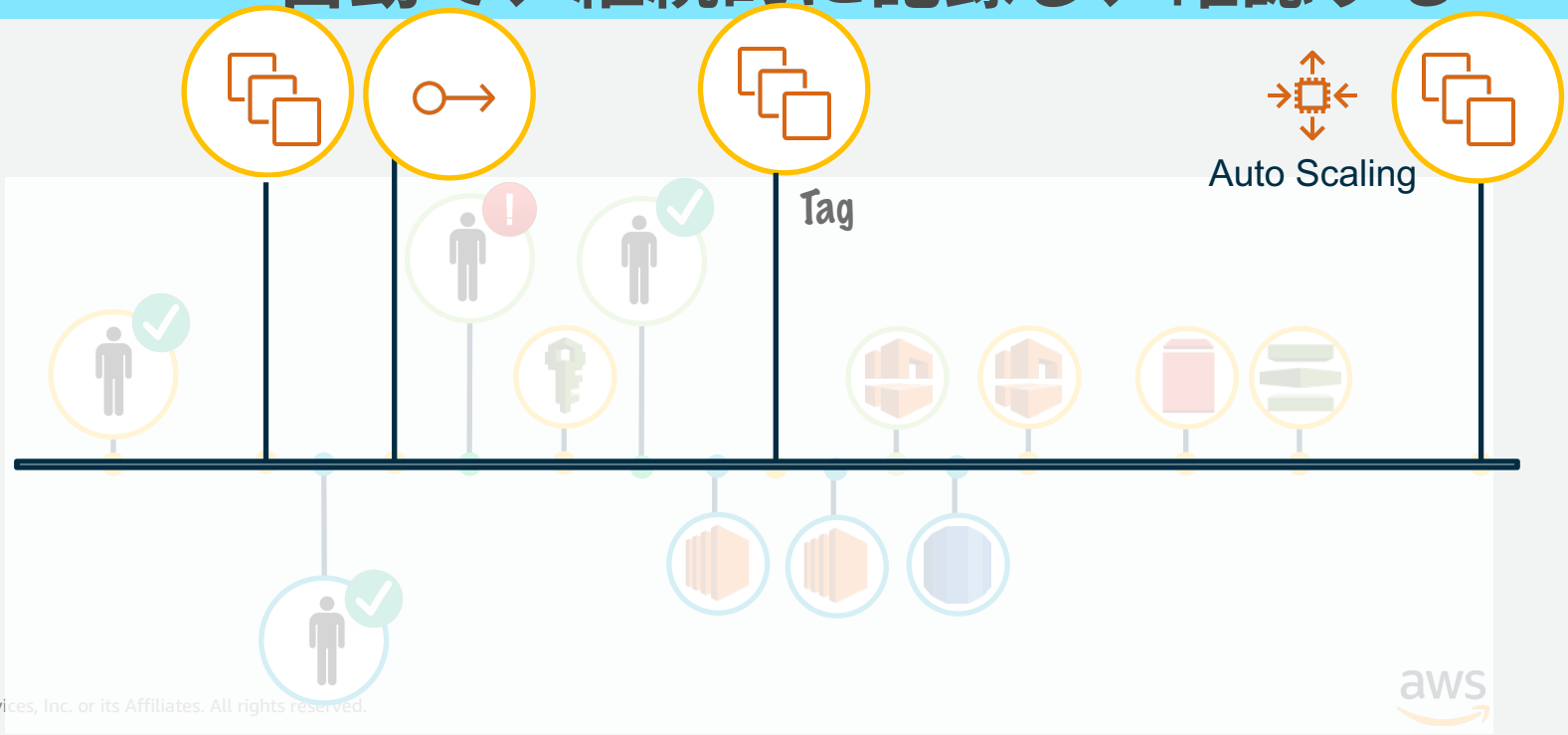
- 構成ドキュメントと実設定の整合性
  - サービス修正による構成変更
  - バージョンアップに伴う設定見直し
  - トラブル時の緊急対処
  - 担当変更などによる引継ぎ

管理者

- システム数の増加にともなう管理コスト増
- 依存関係の誤認によるシステム影響
- システム障害や、セキュリティ調査での過去の設定内容の確認
- コンプライアンス準拠への負担増

AWSに対する構成変更をどう管理するか

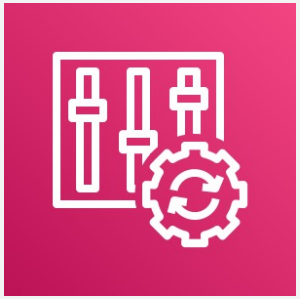
何に対して、 誰が、いつ、何をしたかを
自動で、継続的に記録し、確認する



AWS Config

AWS Config概要

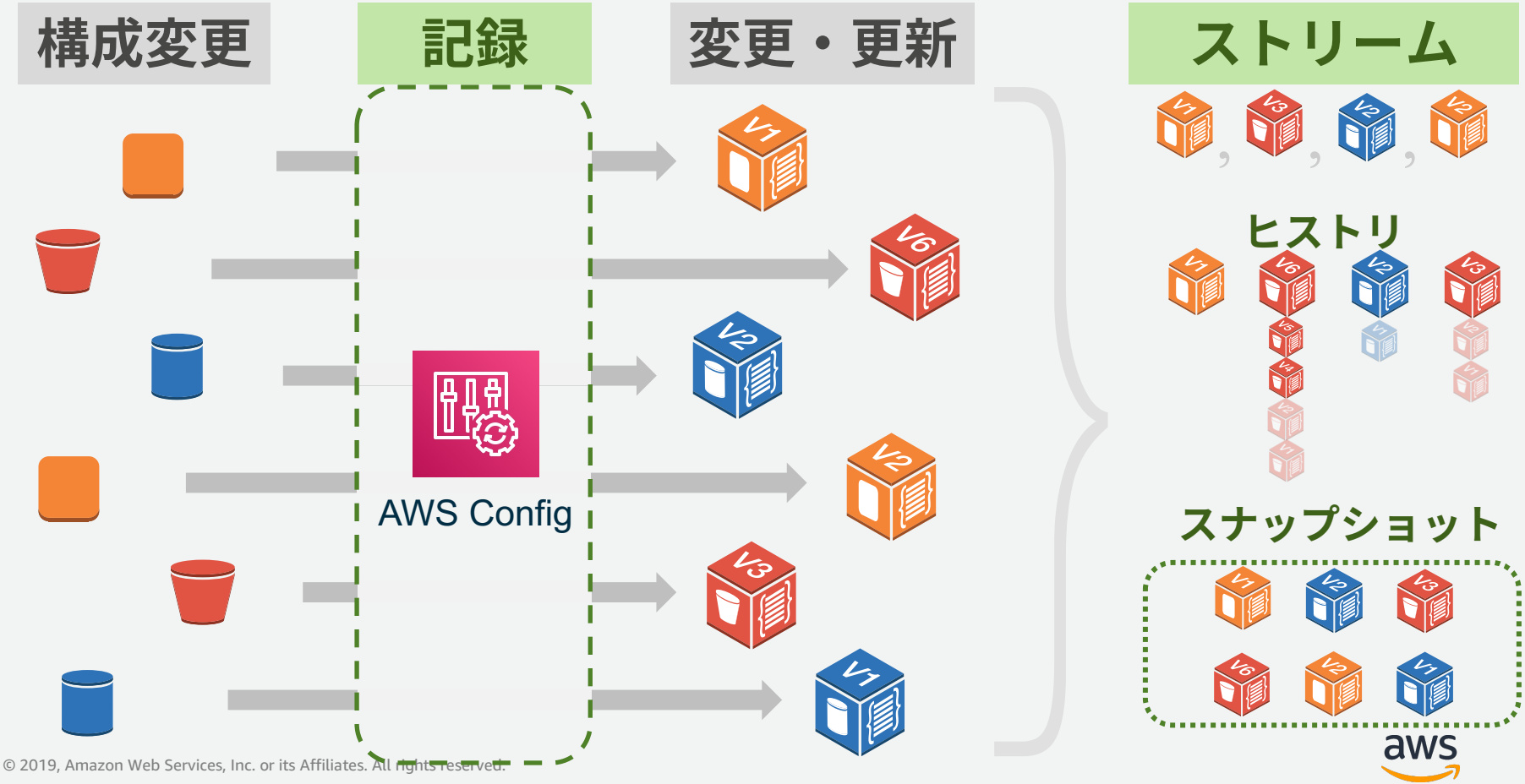
AWS Configとは



AWS Config

- AWSリソースのインベントリ管理、構成変更管理のための、フルマネージド型サービス
- AWSリソースの構成変更をロギング
  - 保持期間はデフォルト７年間 （30日間～７年間で設定可）
- 履歴も保存
  - 構成情報は定期的にスナップショットとしてS3に保存
  - 必要に応じSNSを使った通知も可能
- ログはS3に保存
- 構成変更の追跡、セキュリティ分析、トラブルシューティング、コンプライアンス準拠を容易に

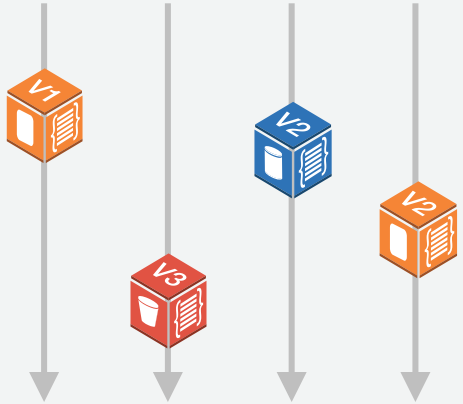
AWS Config の動作イメージ



AWS Config 各機能の役割

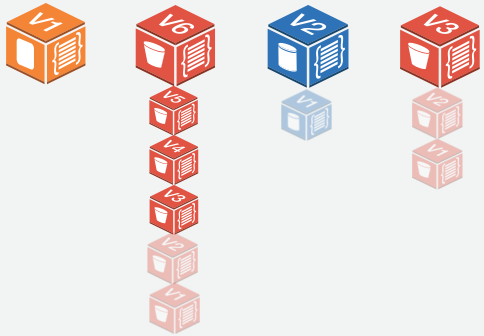
ストリーム
(Configuration Stream)

- リソースが作成/変更/削除されるたびに作成
- 構成ストリームに追加される
- SNSトピック連携可能



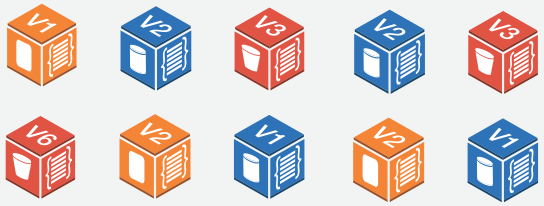
ヒストリー
(Configuration History)

- 任意の期間における各リソースタイプの構成要素の集合
- リソースの設定履歴を、指定したS3バケットに保存



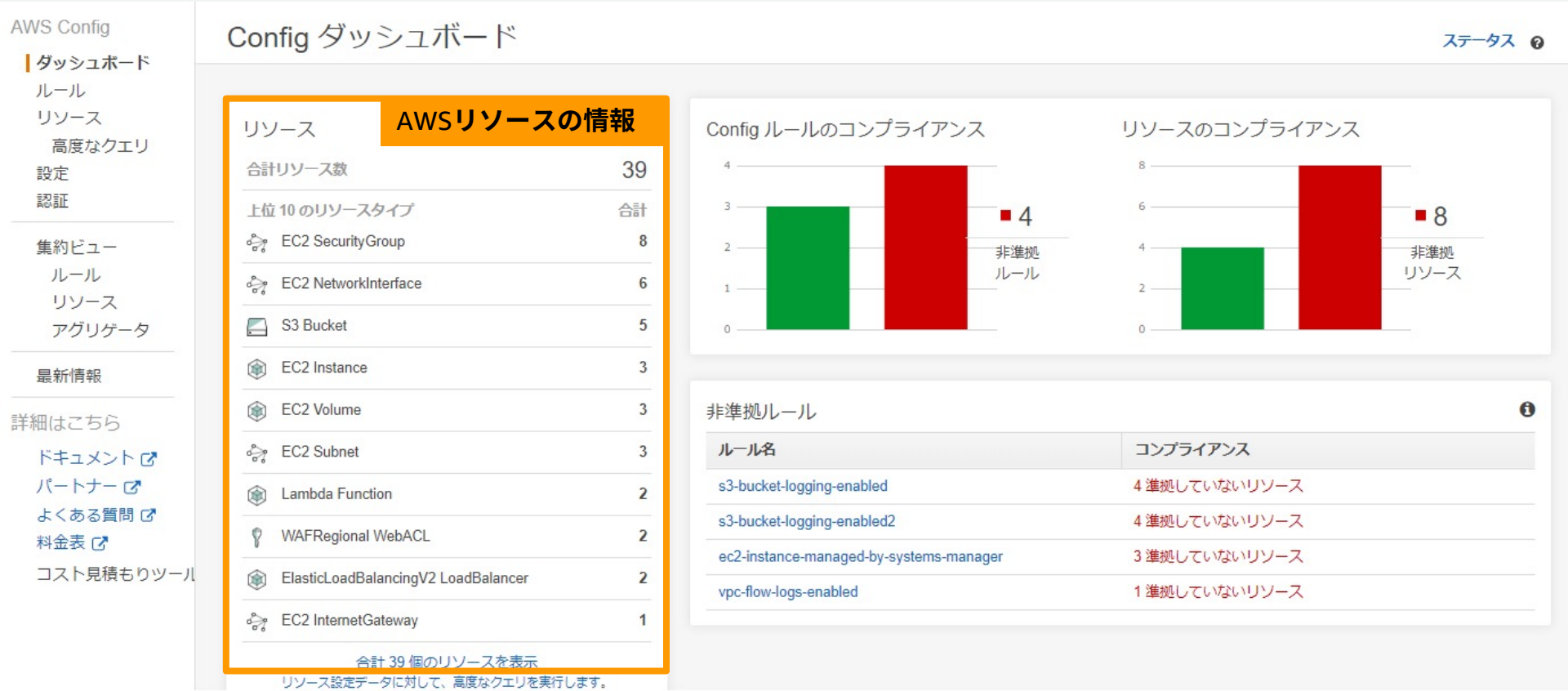
スナップショット
(Configuration Snapshot)

- ある時点でのコンフィグレーションアイテムの集合
- 自動で定期的、あるいは変更トリガで作成され、指定したS3バケットに保存



Snapshot @ 2019-06-18, 11:00am

AWS Config ダッシュボード



設定タイムライン

時系列で構成情報を確認

設定タイムライン

構成情報の変更部分（変更前→変更後）を確認

▼ 変更 13

設定変更 12

フィールド	開始	終了
Configuration.BlockDeviceMappings.0		▼ Object deviceName: "/dev/sdf" ▼ ebs: Object attachTime: "2019-06-17T12:51:06.000Z" deleteOnTermination: false status: "attached" volumeId: "vol-02 1912fc"
Configuration.State.Name	"stopped"	"running"
Configuration.PublicIpAddress		"54.250 ,"
Configuration.InstanceType	"t2.micro"	"c4.large"
Configuration.StateTransitionReason	"User initiated (2019-06-07 03:29:25 GMT)"	""
Configuration.PublicDnsName	""	"ec2-54-250 .ap-northeast-1.compute.amazonaws.com"

ボリュームの追加

インスタンス起動

インスタンス
タイプ変更(t2→c4)

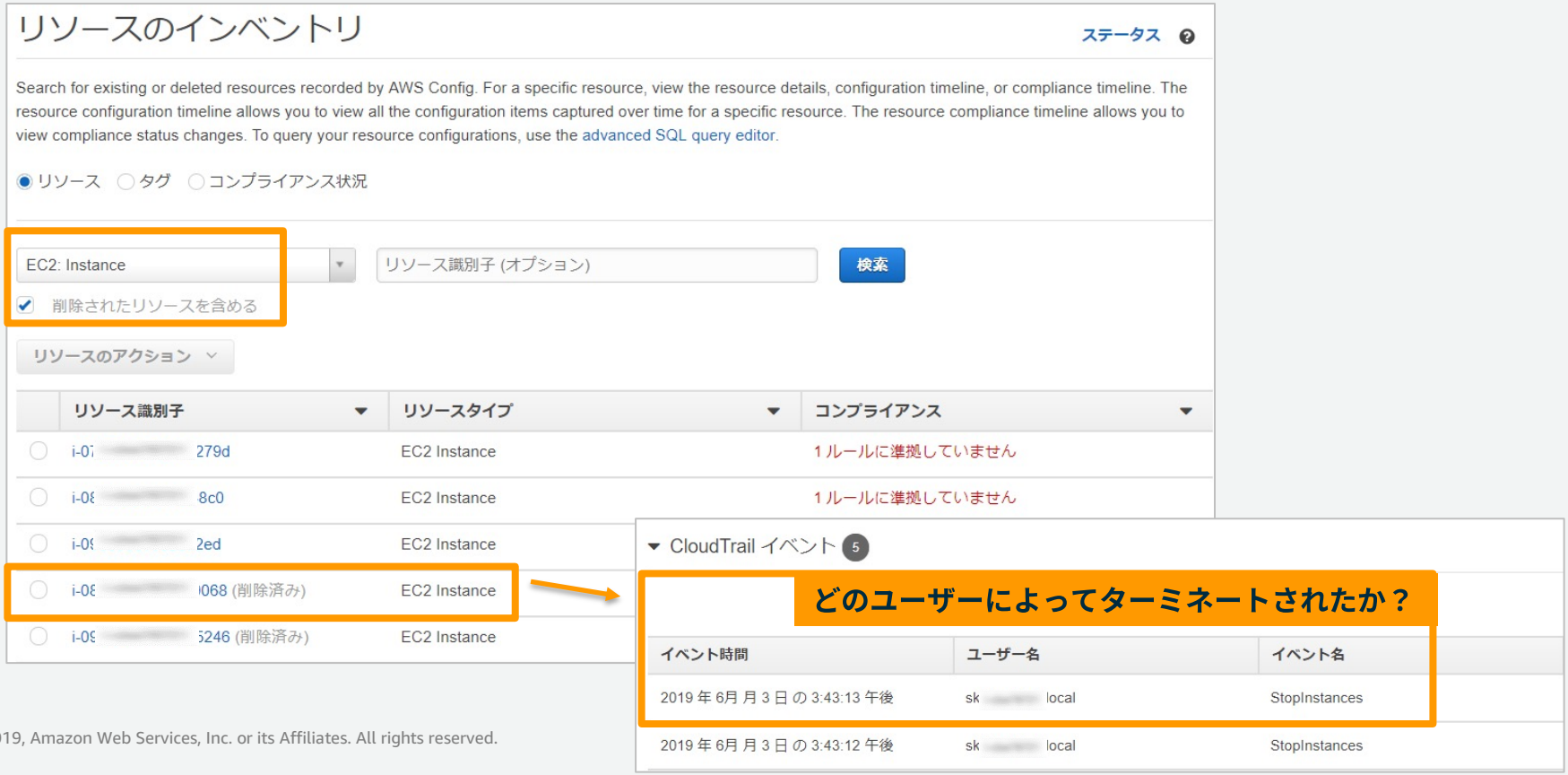
▼ CloudTrail イベント 4

イベント時間	ユーザー名	イベント名	イベントの表示
2019 年 6月 月 17 日 の 9:51:34 午後	sk .local	StartInstances	CloudTrail
2019 年 6月 月 17 日 の 9:51:06 午後	sk .local	AttachVolume	CloudTrail

どのユーザーによる
操作か？(CloudTrail)

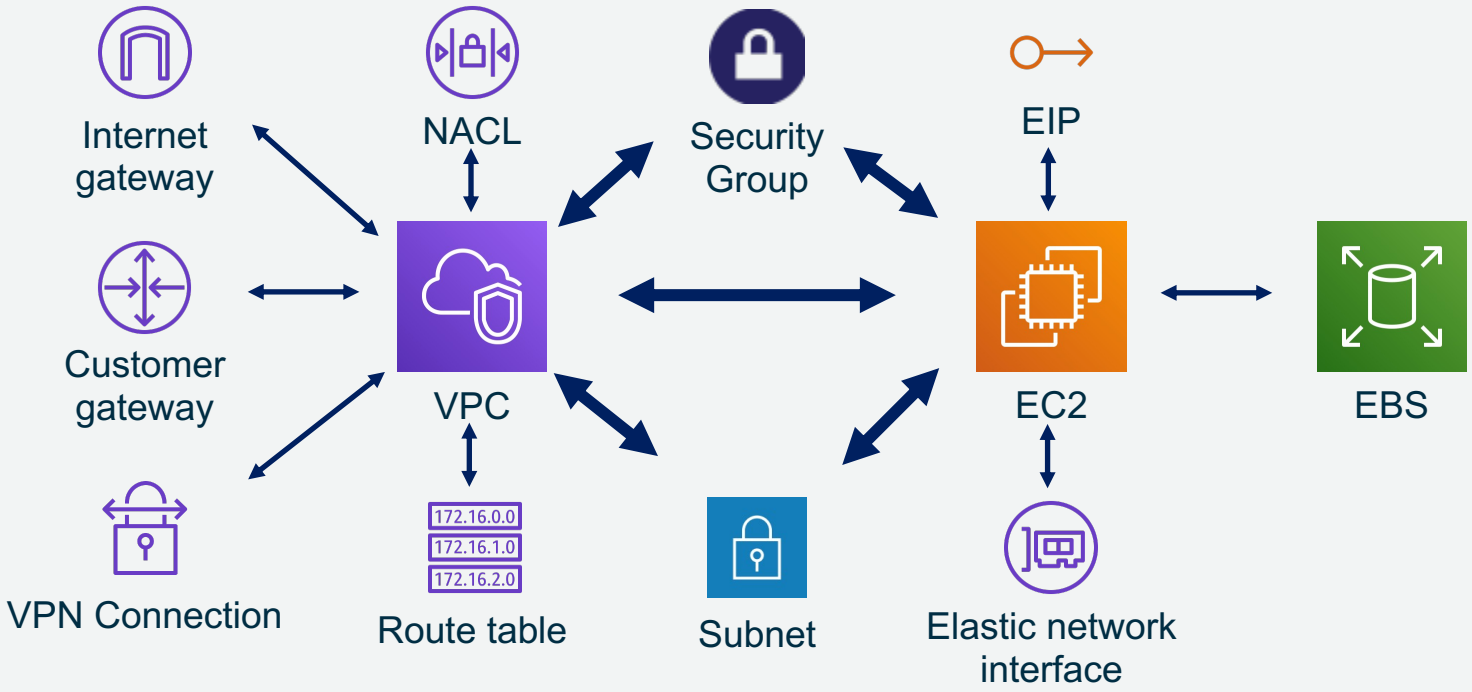
リソースのインベントリ

利用例： ターミネート済みのEC2インスタンスの情報を確認



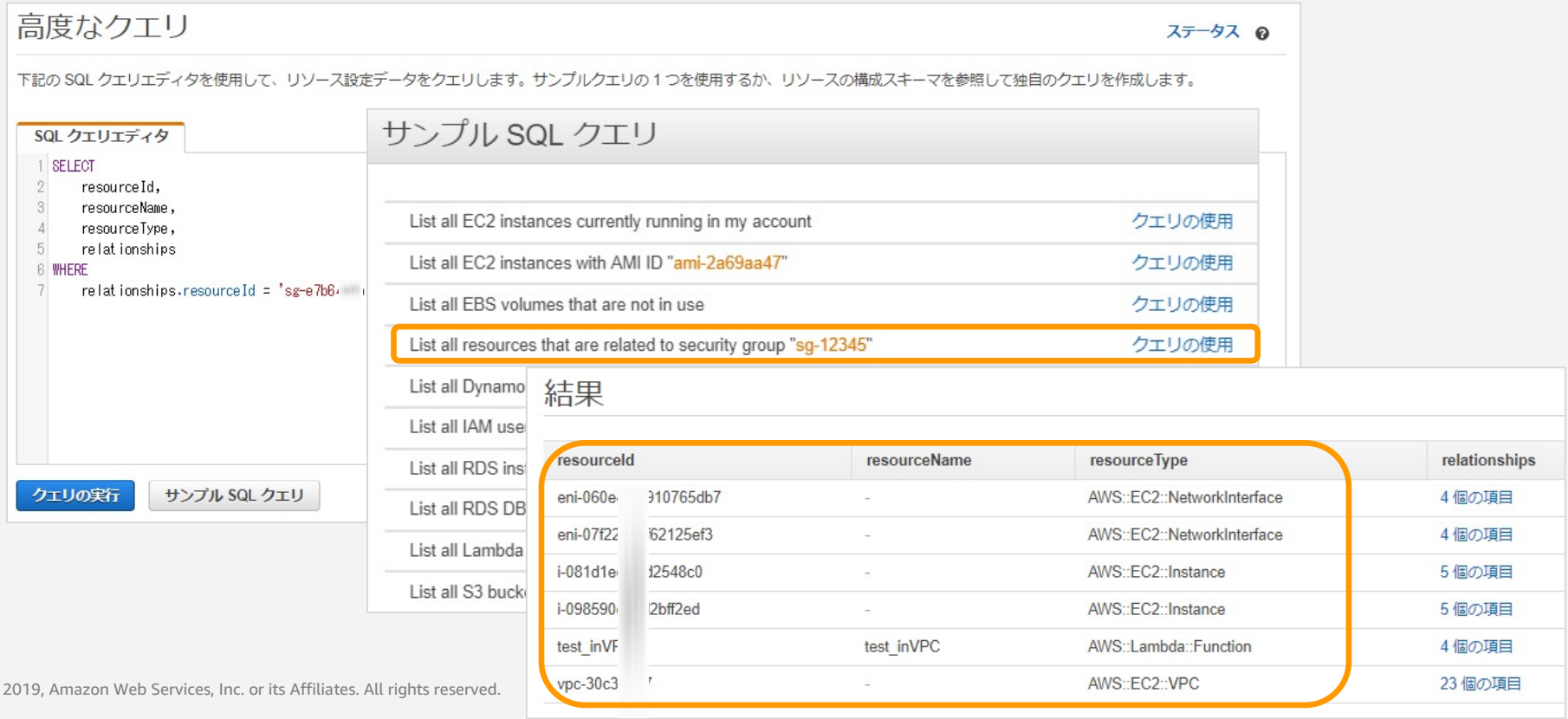
リソース間の関係（リレーションシップ）

- アカウント内のAWSリソース間の関係を管理
- 双方向の依存関係が自動的に割り当てられる



リソースのインベントリ：高度なクエリ

利用例： 特定のセキュリティグループを利用しているリソースを検索



AWS Config が対応しているAWSリソース

New!!


Amazon VPC


Amazon EC2


Amazon S3


Classic Load Balancers


Application Load Balancers


Amazon EBS volumes


AWS Service Catalog


AWS CloudTrail


AWS IAM


Amazon Redshift


Amazon RDS


AWS Systems Manager


AWS Certificate Manager


Amazon API Gateway


Amazon CloudWatch alarms


AWS CloudFormation stacks


Amazon DynamoDB tables


AWS Auto Scaling groups


AWS CodeBuild


AWS CodePipeline


AWS WAF *1


Amazon CloudFront *1


AWS Elastic Beanstalk


AWS Lambda


AWS X-Ray


AWS Shield *1

*1: **グローバルサービスは米国東部（バージニア北部）リージョンでサポート**

https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/resource-config-reference.html

AWS Config のよる構成管理のメリット

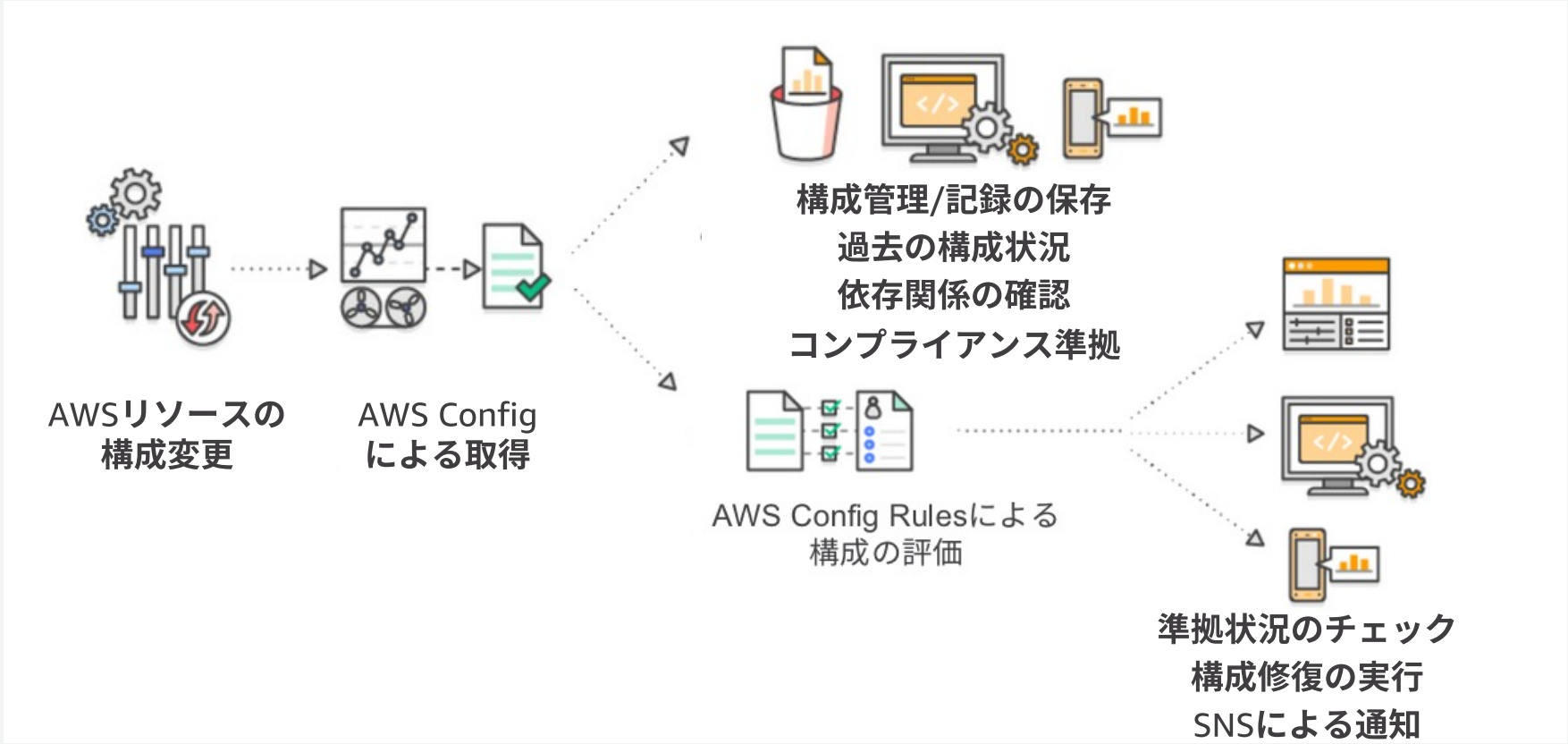
AWSリソースの
構成変更

AWS Config
による取得

構成管理/記録の保存
過去の構成状況
依存関係の確認
コンプライアンス準拠

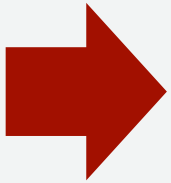
AWS Config Rules 概要

AWS Config で管理する構成情報を評価する



AWS Config Rulesによるポリシー準拠の評価

準拠すべきルールを
事前に設定



ルールに沿った
構成変更が行われて
いるかを評価

- 全てのEBCボリュームが暗号化されているか
- EC2インスタンスが適切にタグ付されているか等

マネージドルール

- AWSにより定義・提供される
- 汎用性の高いベーシック・ルール

カスタムルール

- 自分でAWS Lambdaをベースにルールを作成可能
- 管理自体は作成者 (自分) で実施

ダッシュボード

AWS Config
- ダッシュボード
- ルール
- リソース
  - 高度なクエリ
- 設定
- 認証

集約ビュー
- ルール
- リソース
- アグリゲータ

最新情報

詳細はこちら
- ドキュメント
- パートナー
- よくある質問
- 料金表
- コスト見積もりツール

Config ダッシュボード

ステータス

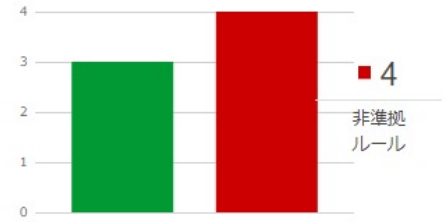
リソース

合計リソース数	39
上位 10 のリソースタイプ	合計
EC2 SecurityGroup	8
EC2 NetworkInterface	6
S3 Bucket	5
EC2 Instance	3
EC2 Volume	3
EC2 Subnet	3
Lambda Function	2
WAFRegional WebACL	2
ElasticLoadBalancingV2 LoadBalancer	2
EC2 InternetGateway	1

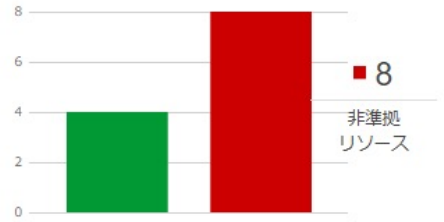
合計 39 個のリソースを表示
リソース設定データに対して、高度なクエリを実行します。

ルールの準拠状況

Config ルールのコンプライアンス



リソースのコンプライアンス



非準拠ルール

ルール名	コンプライアンス
s3-bucket-logging-enabled	4 準拠していないリソース
s3-bucket-logging-enabled2	4 準拠していないリソース
ec2-instance-managed-by-systems-manager	3 準拠していないリソース
vpc-flow-logs-enabled	1 準拠していないリソース

トリガータイプ：ルール評価実行のタイミング

設定変更

- 関連リソースが作成、変更された際
  - Scoped by changes to:
  - Tag Key/Value
  - Resource types
  - Specific resource ID

  例) 新規で作成するEC2に、必ずTagが付けれられいるかの評価

定期的

- 任意の定期的なタイミング
  - 1時間毎 ～ 24時間毎
- AWS Config がスナップショットを取る際

  例) CloudTrailが有効になっているかどうかの評価

マネージドルールのカテゴリ

コンピューティング

データベース

マネジメントと
ガバナンス

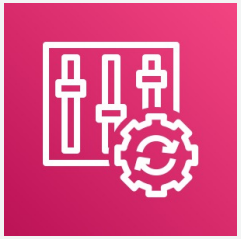
ネットワークと
コンテンツ配信

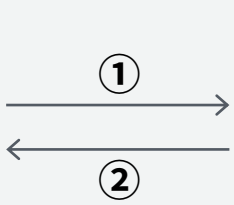
セキュリティ
アイデンティティ
コンプライアンス

ストレージ

https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/managed-rules-by-aws-config.html

カスタムルール





AWS Config Rules

Lambda function

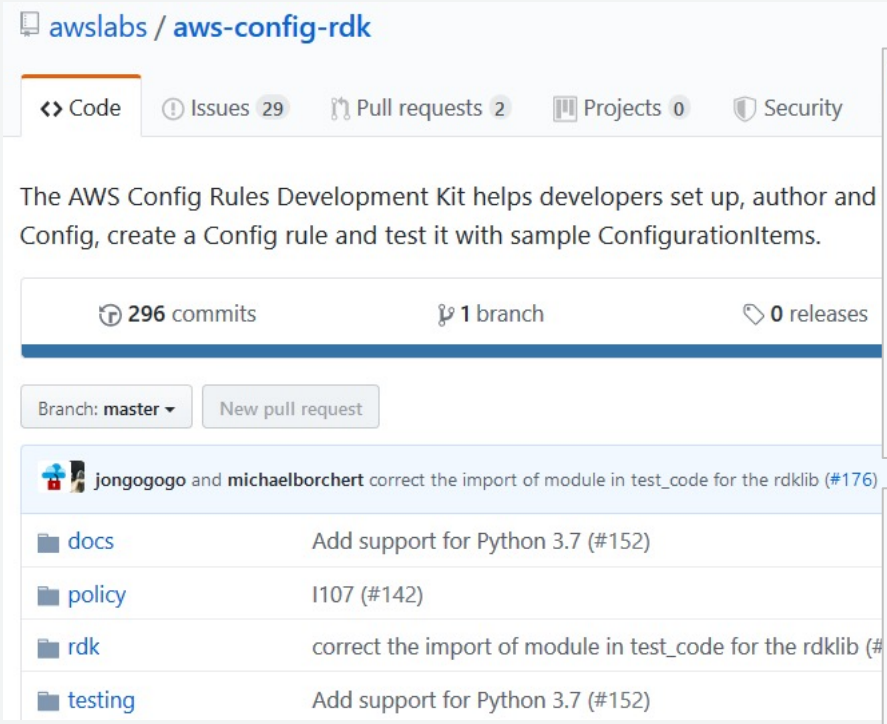
事前にLambda関数 を作成
- 自由にルールを設定することが可能
- 作成したLambda関数のARNを ルールに紐付ける
- トリガータイプを選択 (設定変更 or 定期的)

① ルールの評価実行
- AWS Configによって、ルールに紐づいた Lambda関数が実行される
- その際に、Lambda 関数に対しイベント パラメータがセットされる

② 評価結果の通知
- Lambda関数の実行結果をAWS Configに 引き渡す

AWS Config Rule Development Kit (RDK)

カスタムルールの作成を支援する開発キット



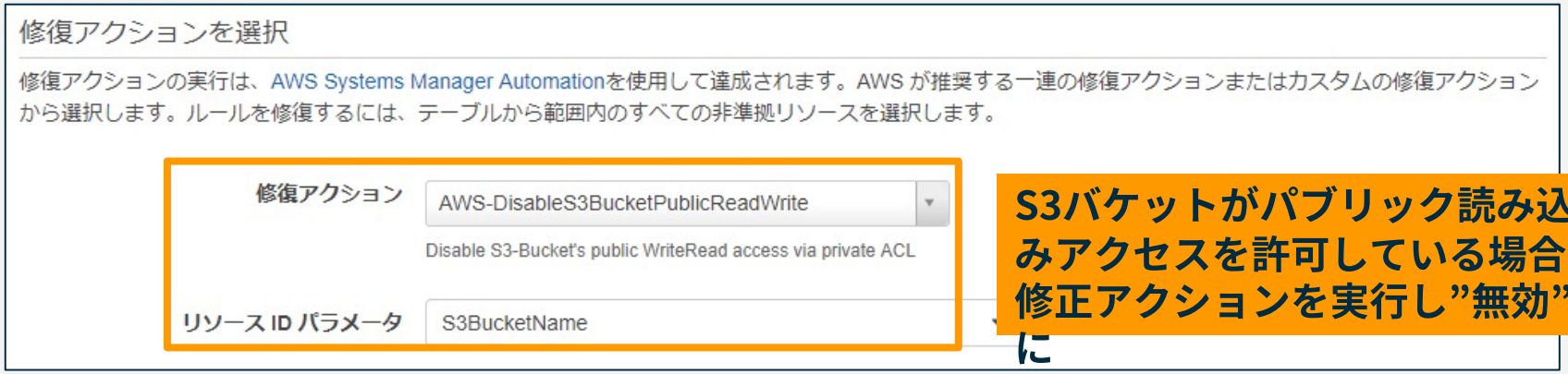

```
for sg in response['SecurityGroups']:
      evaluations.append(
      {
              'ComplianceResourceType': 'AWS::EC2::SecurityGroup',
              'ComplianceResourceId': sg['GroupId'],
              'ComplianceType': 'COMPLIANT',
              'Annotation': 'This is an important note.',
              'OrderingTimestamp': str(datetime.datetime.now())
      })


 return evaluations
```

```
$ rdk test-local MyTestRule
Running local test!
Testing MyTestRule
Looking for tests in /Users/mborch/Code/rdk-dev/MyTestRule

----------------------------------------------------------------------

Ran 0 tests in 0.000s

OK
<unittest.runner.TextTestResult run=0 errors=0 failures=0>
```

https://github.com/awslabs/aws-config-rdk

修復アクション

コンプライアンス違反のリソースに対して、ルールに関連付けられた修正アクションを実行



S3バケットがパブリック読み込みアクセスを許可している場合、修正アクションを実行し”無効”に

- 事前入力されたリストから修正アクションを選択
- AWS Systems Manager Automation ドキュメントを使用したカスタムの修正アクションを設定

※コンプライアンス違反の検出ログ(Cloud Watch Events)からLambdaをトリガーし、より細かい修正アクションも実行可能

ユースケース・ベストプラクティス

マネージドルールのユースケース #1

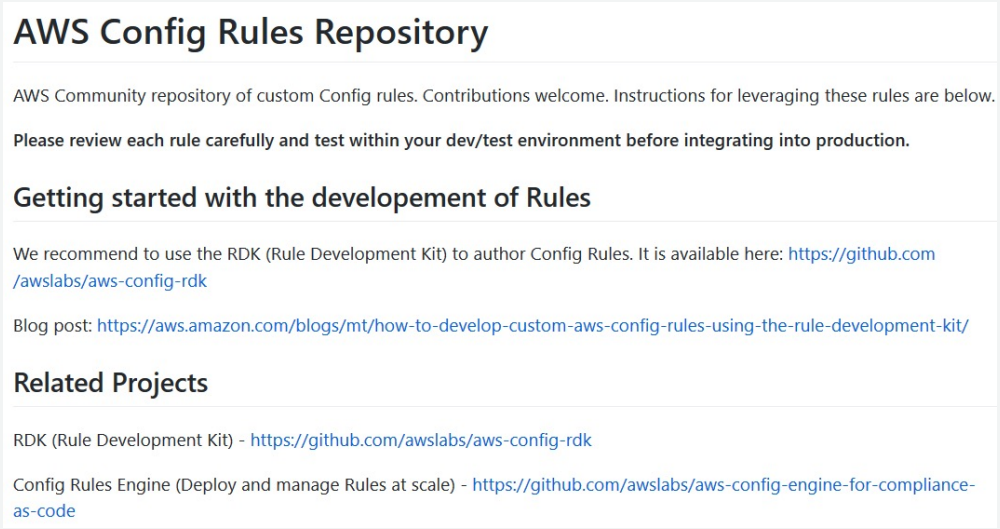
- approved-amis-by-id
  - 実行中のインスタンスで使用されている AMIが指定したもの(承認済のもの)かを確認
- required-tags
  - リソースに指定したタグがあるかどうかを確認
    （たとえば、EC2 インスタンスに ‘CostCenter’ タグがあるかどうか）
- encrypted-volumes
  - アタッチ済みの EBS ボリュームが暗号化されているかどうかを確認
- ec2-instance-managed-by-ssm
  - EC2 インスタンスが AWS Systems Manager で管理されているか確認
- vpc-flow-logs-enabled
  - VPCのパケット取得(Flow Logs)が有効になっているか確認

マネージドルールのユースケース #2

- s3-bucket-public-read-prohibited
  - Amazon S3 バケットでパブリック読み取りアクセスが許可されないことを確認
- s3-bucket-public-write-prohibited
  - Amazon S3 バケットでパブリック書き込みアクセスが許可されないことを確認
- rds-snapshots-public-prohibited
  - Amazon RDS スナップショットが公開禁止されているかを確認
- s3-bucket-server-side-encryption-enabled
  - Amazon S3 バケットで Amazon S3 のデフォルト暗号化が有効か確認
- access-keys-rotated
  - 有効なアクセスキーが、指定日数内にローテーションされるかどうかを確認

AWS Config Rules Repository

コミュニティベースでカスタマイズされたAWS Config Rules GitHub上で公開



AWS Config Rules Repository

AWS Community repository of custom Config rules. Contributions welcome. Instructions for leveraging these rules are below.

Please review each rule carefully and test within your dev/test environment before integrating into production.

Getting started with the developement of Rules

We recommend to use the RDK (Rule Development Kit) to author Config Rules. It is available here: https://github.com/awslabs/aws-config-rdk

Blog post: https://aws.amazon.com/blogs/mt/how-to-develop-custom-aws-config-rules-using-the-rule-development-kit/

Related Projects

RDK (Rule Development Kit) - https://github.com/awslabs/aws-config-rdk

Config Rules Engine (Deploy and manage Rules at scale) - https://github.com/awslabs/aws-config-engine-for-compliance-as-code

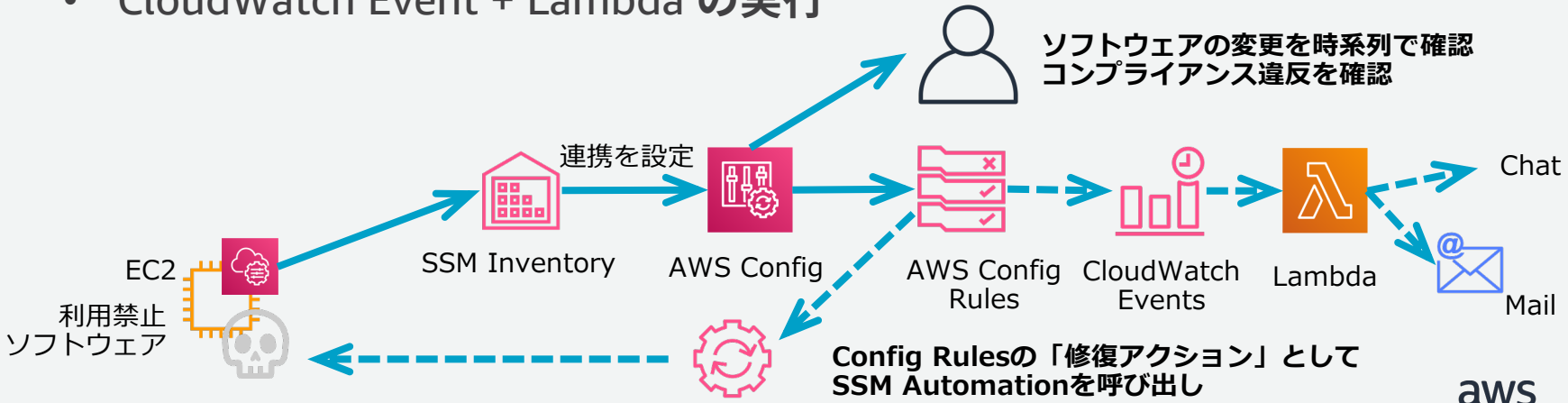
公開されているルールの例

- **Lambda**
  関数がVPCに紐づいているか
- **ALB**
  HTTPSリダイレクトが有効か
- **API Gateway**
  IPアドレスで接続制限しているか
- **S3**
  VPC Endpointが各VPCで有効か

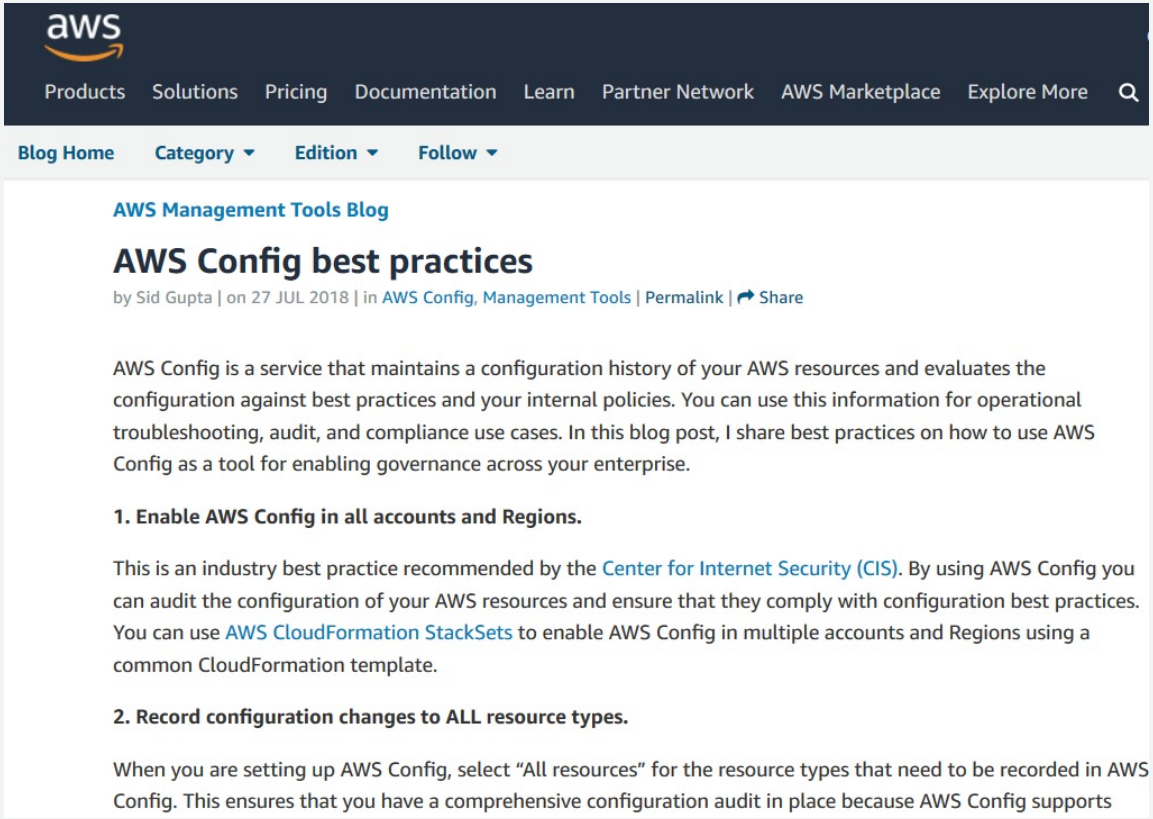
https://github.com/awslabs/aws-config-rules

SSMと連携したOS構成情報の管理例：不正ソフトウェア導入に対する自動アクション

- SSM Inventory でソフトウェアの導入状況を確認
- AWS Config / Config Rules でソフトウェアの導入状況を記録・監視
- 違反を検知したら、通知やサーバを止めるなどの対処を実施
  - Config Rulesの 修復アクションとして SSM Automation の実行
  - CloudWatch Event + Lambda の実行



AWS Config のベストプラクティス



aws

Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Explore More

Blog Home Category Edition Follow

AWS Management Tools Blog

AWS Config best practices

by Sid Gupta | on 27 JUL 2018 | in AWS Config, Management Tools | Permalink | Share

AWS Config is a service that maintains a configuration history of your AWS resources and evaluates the configuration against best practices and your internal policies. You can use this information for operational troubleshooting, audit, and compliance use cases. In this blog post, I share best practices on how to use AWS Config as a tool for enabling governance across your enterprise.

1. Enable AWS Config in all accounts and Regions.

This is an industry best practice recommended by the Center for Internet Security (CIS). By using AWS Config you can audit the configuration of your AWS resources and ensure that they comply with configuration best practices. You can use AWS CloudFormation StackSets to enable AWS Config in multiple accounts and Regions using a common CloudFormation template.

2. Record configuration changes to ALL resource types.

When you are setting up AWS Config, select “All resources” for the resource types that need to be recorded in AWS Config. This ensures that you have a comprehensive configuration audit in place because AWS Config supports

https://aws.amazon.com/jp/blogs/mt/aws-config-best-practices

AWS Config のベストプラクティス

記録対象について

#1. 全てのアカウントとリージョンでAWS Configを有効に
→ すべての操作を記録する
→ ミスがあったら気付ける仕組みを整えておく

#2. すべてのリソースタイプについて、設定変更を記録する
→ 新しく追加されたリソースタイプも自動で記録対象となる

#3. グローバルリソースは１リージョンで記録を有効にする
→ 重複して記録されるのを防ぐ

AWS Config のベストプラクティス

保存先について

#5. 安全なS3バケットにヒストリーとスナップショットを保存する
→ AWSリソースの詳細情報も記録される
→ 特定の人しかアクセスできず、改竄ができない場所へ保存

S3バケットの公開設定をチェックするAWS Managed Ruleも活用可能

- s3-bucket-public-write-prohibited
- s3-bucket-public-read-prohibited

AWS Config のベストプラクティス

マルチアカウント環境での利用について

#19. Data aggregation機能を使って、管理アカウントから集中管理する
#20. Organizationsベースのaggregatorを使う

→ マルチアカウント環境では統制がとりにくい
→ 構成管理用アカウントから、集中管理を行う

集約ビュー：
マルチアカウント、マルチリージョンのデータを集約

Central dashboard that provides an aggregated view

Multi-account, multi-region

Integrates with AWS Organizations

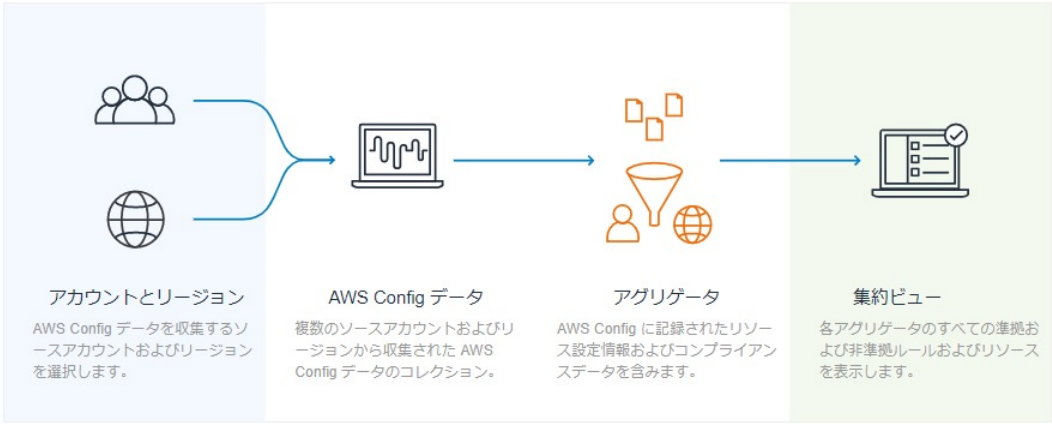
Available at no additional charge

集約ビュー：アグリゲータの作成

アグリゲータ

アグリゲータは、複数のアカウントおよびリージョンから AWS Config データを収集する AWS Config リソースタイプです。アグリゲータを使用して、複数のアカウントおよびリージョンについて AWS Config に記録されたリソース設定とコンプライアンスデータを表示します。

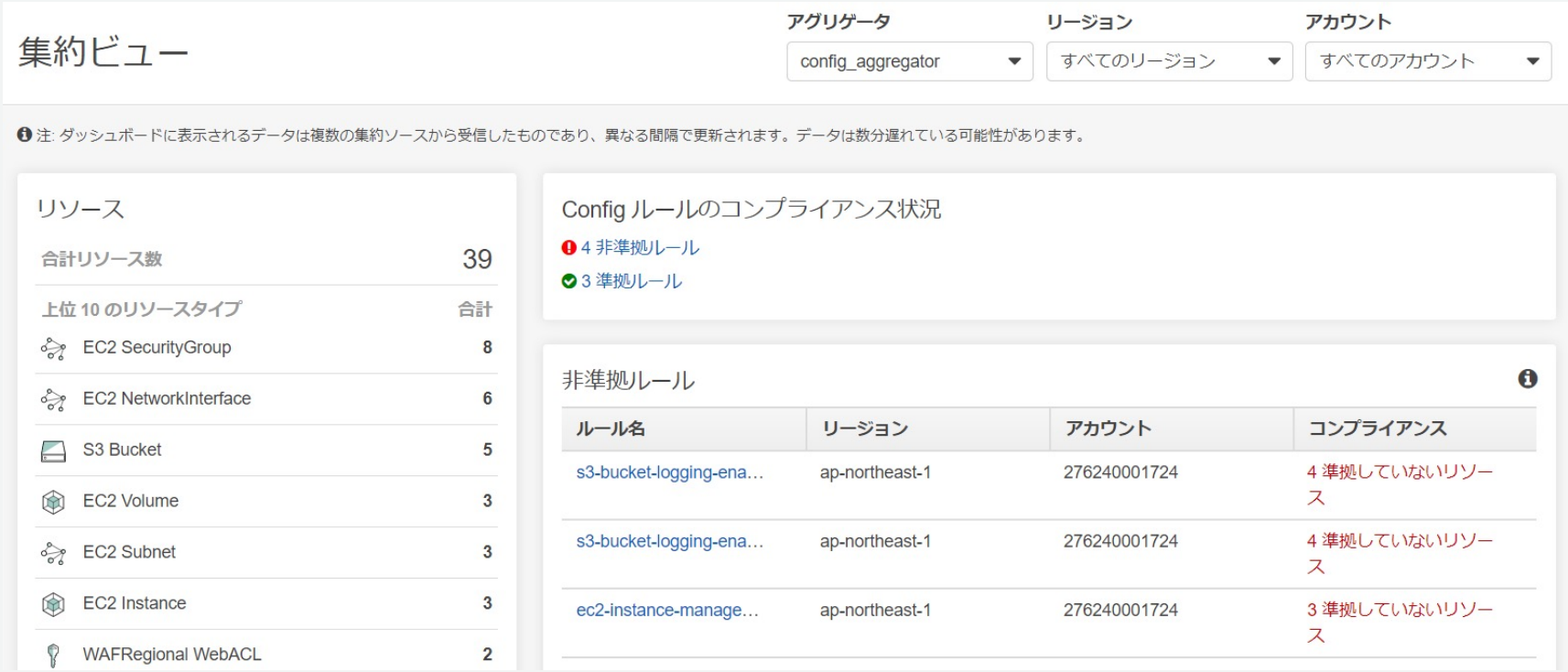
図を非表示



アグリゲータの追加　アクション

	アグリゲータ名	ソースアカウント	ソースタイプ
○	config_aggregator	1 個のアカウント	個々のアカウント

集約ビュー：マルチアカウント、マルチリージョンのデータを集約して表示



料金について

料金 (2019/06/18 時点)

- **AWS Config**

  リソースに対して記録された設定項目　１記録あたり：0.003USD

- **AWS Config Rules**

  月ごとにアクティブだったAWS Config ルール数

  最初の10ルール：2.00USD　次の40ルール：1.50USD　51ルール以上：1.00USD

  ※2019年8月1日からの料金

  記録されたAWS Config ルールの評価数（リージョンごと）

最初の10万ルールの評価につき：	0.001USD
次の40万ルール(100,001 – 500,000)の評価につき：	0.0008USD
次の500,001以上のルールの評価につき：	0.0005USD

- **追加料金**

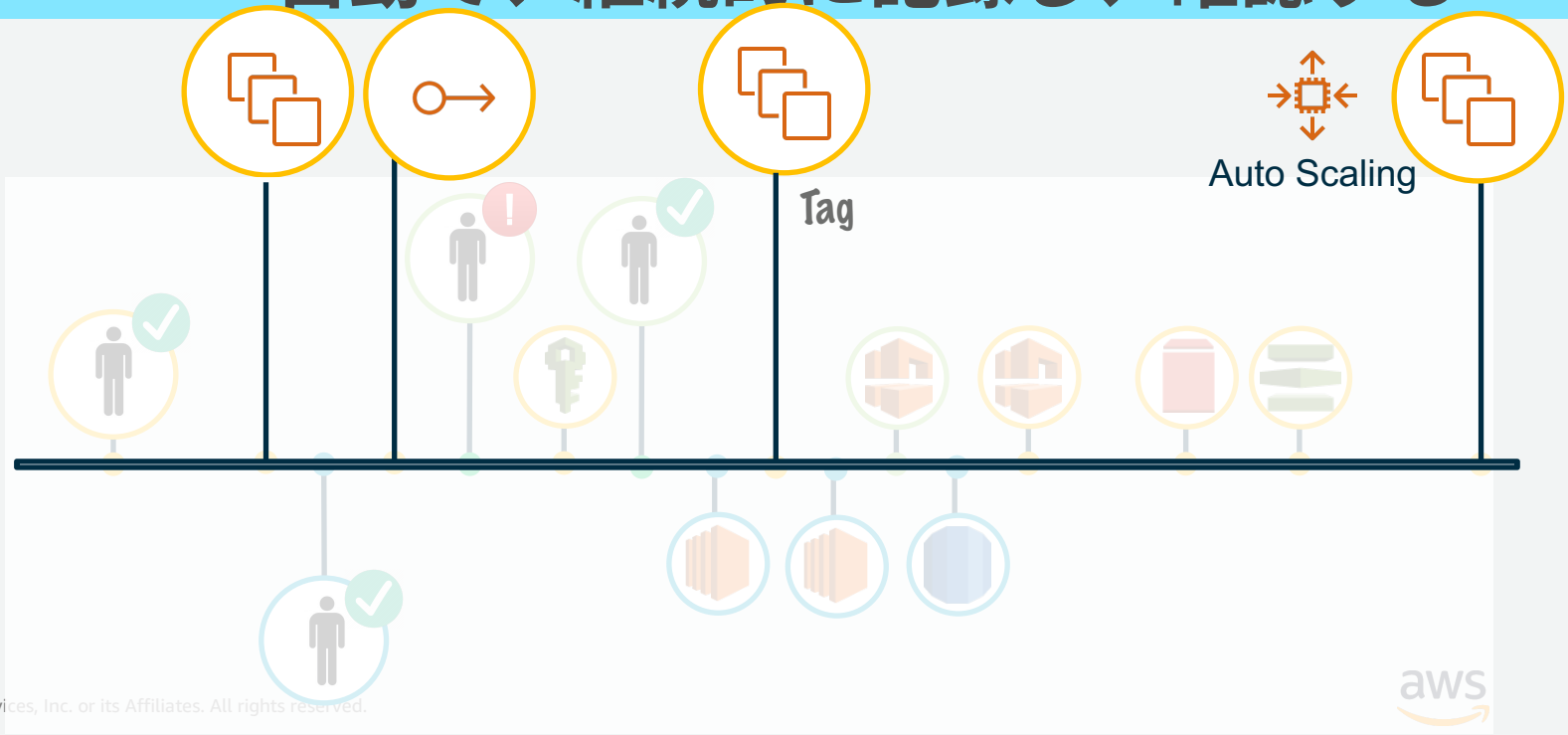
  S3(ログ保存)、SNS(通知)、 Lambda(カスタムルール)、SSM Automation(修復)

https://aws.amazon.com/jp/config/pricing/

まとめ

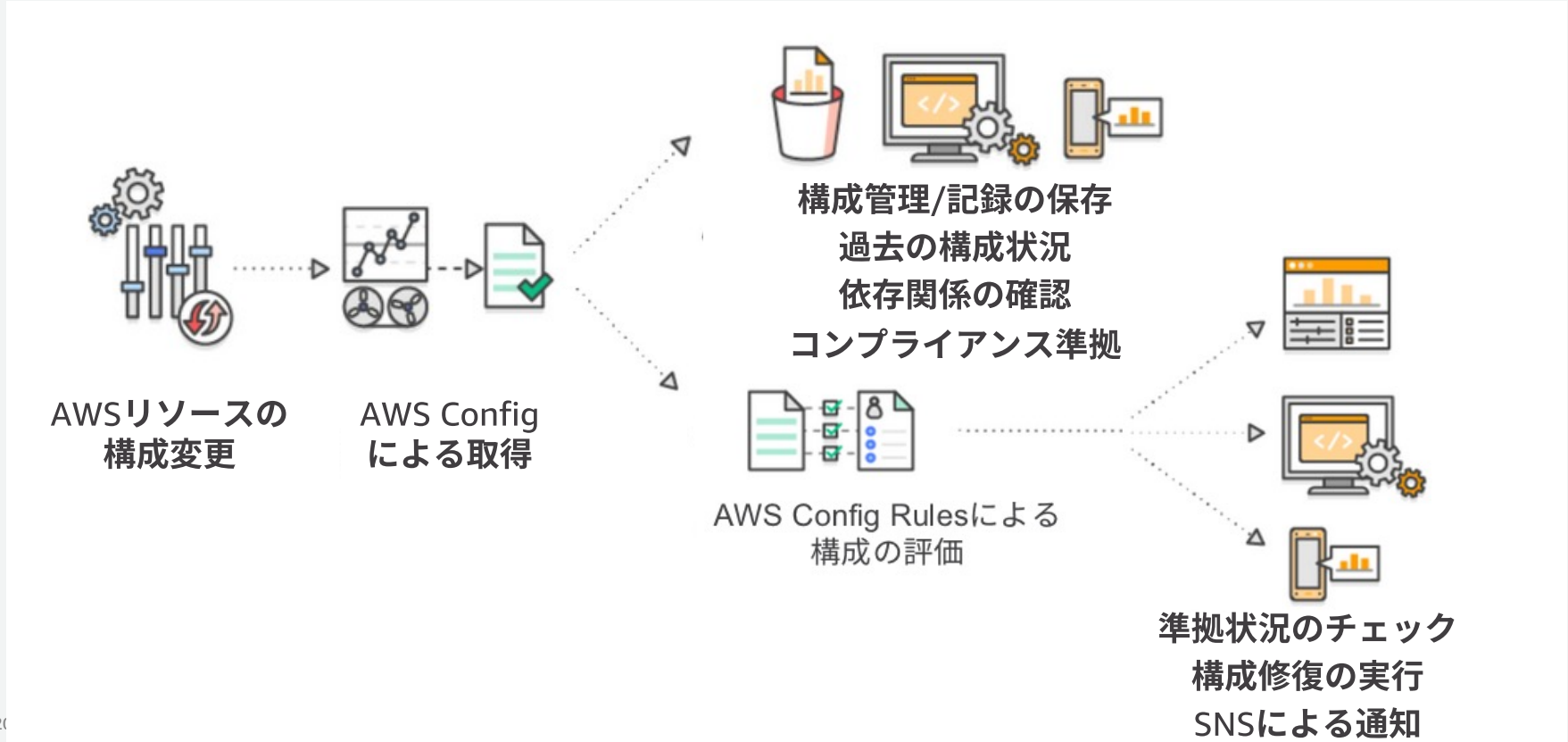
AWSに対する構成変更をどう管理するか（再掲）

何に対して、 誰が、いつ、何をしたかを
自動で、継続的に記録し、確認する



AWS Config

AWS Config / Config Rules による 構成管理、評価のメリット



参考資料

AWS Config のベストプラクティス
https://aws.amazon.com/jp/blogs/mt/aws-config-best-practices/

AWS Config マネージドルールのリスト
https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/managed-rules-by-aws-config.html

AWS Config で記録するリソースの選択
https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/select-resources.html

AWS Configに関するよくある質問
https://aws.amazon.com/jp/config/faq/

Q&A

お答えできなかったご質問については
AWS Japan Blog 「https://aws.amazon.com/jp/blogs/news/」にて
資料公開と併せて、後日掲載します。

6 月の Black Belt Online Seminar 配信予定

https://amzn.to/JPWebinar

6/4 (火) 12:00-13:00 Amazon Simple Notification Service (SNS)

6/18 (火) 12:00-13:00 AWS Config

6/19 (水) 18:00-19:00 Dive deep into AWS Chalice

6/25 (火) 12:00-13:00 Amazon DocumentDB (with MongoDB Compatibility)




AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

ご視聴ありがとうございました

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive