



このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar]

AWS Config

サービスカットシリーズ

Archived

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

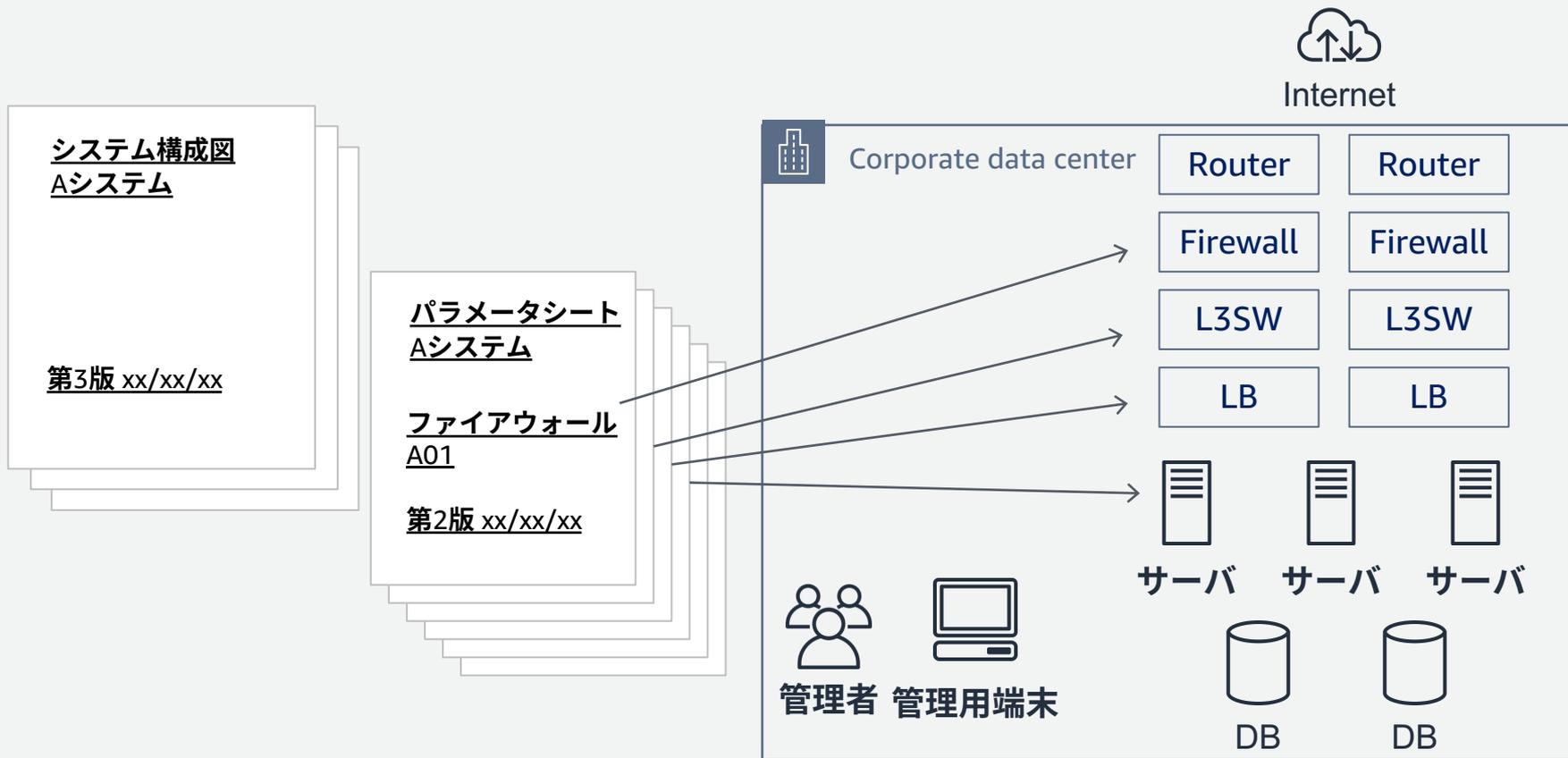
内容についての注意点

- 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おります。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



- 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



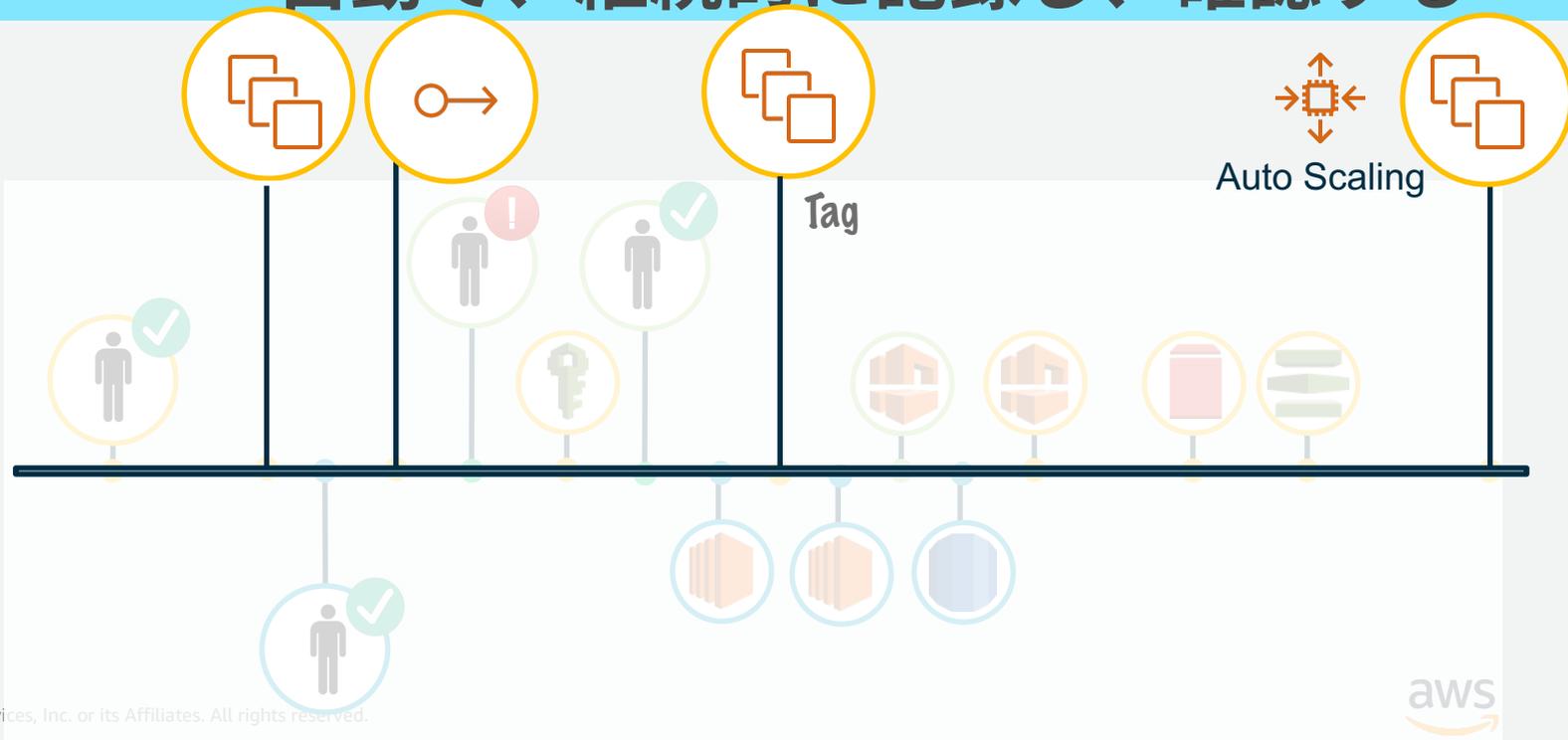
- システム数の増加にともなう管理コスト増
- 依存関係の誤認によるシステム影響
- システム障害や、セキュリティ調査での過去の設定内容の確認
- コンプライアンス準拠への負担増

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

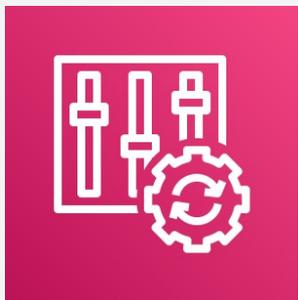


AWS Config



AWS Config概要

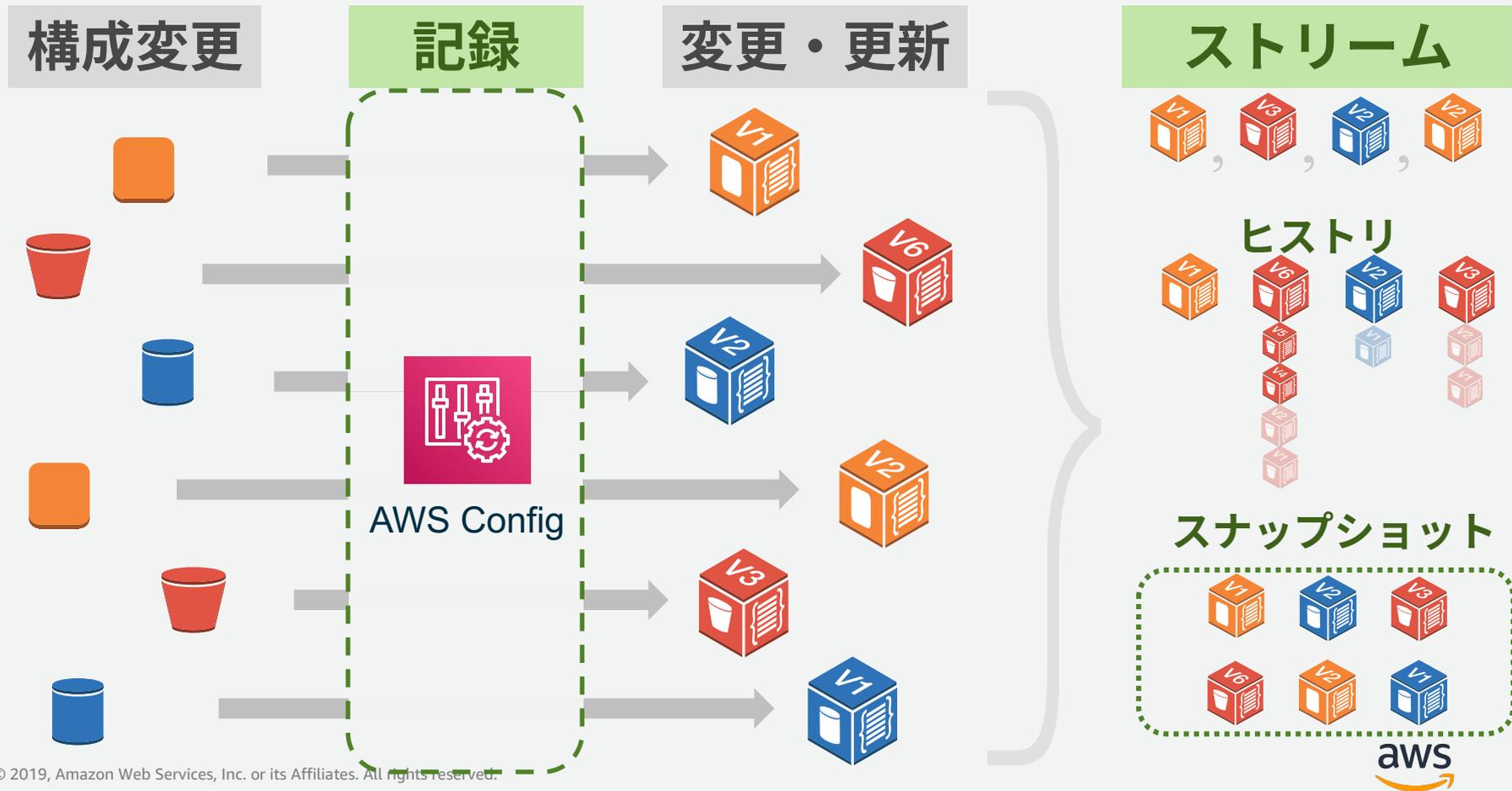
AWS Configとは



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

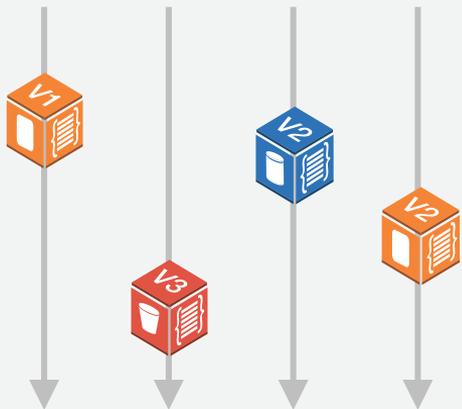


AWS Config 各機能の役割

ストリーム

(Configuration Stream)

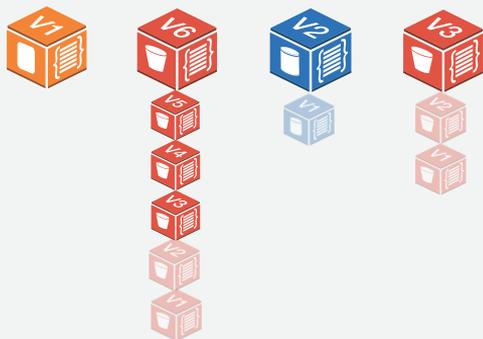
- リソースが作成/変更/削除されるたびに作成
- 構成ストリームに追加される
- SNSトピック連携可能



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ギュ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

AWS Config

Config ダッシュボード

ステータス ⓘ

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](#)

リソース

AWSリソースの情報

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

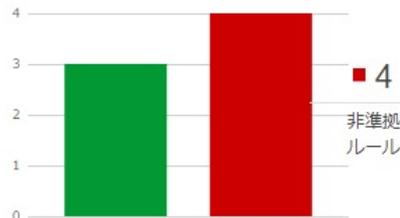
ElasticLoadBalancingV2 LoadBalancer 2

EC2 InternetGateway 1

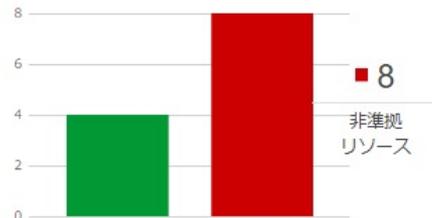
[合計 39 個のリソースを表示](#)

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。

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



非標準ルール ⓘ

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

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 コンプライアンスタイムライン

6月3日14:52に変更8個、イベント1個を記録

29 2019年5月月 10:21:58 午前

03 2019年6月月 2:52:48 午後 8 変更 1 イベント

03 2019年6月月 3:45:43 午後 7 変更 5 イベント

▼ 構成の詳細

Amazon Resource Name	am.aws.ec2:ap-northeast-1:27 1724:instance/i-081 2548c0
リソースタイプ	AWS::EC2::Instance
リソースID	i-08 d2548c0
リソース名	null
アベイラビリティゾーン	ap-northeast-1a

▼ 関係 5

EC2 NetworkInterface	eni-060 10... 6
EC2 SecurityGroup	sg-e 3b 6
EC2 Subnet	subnet-0e 6 6
EC2 Volume	vol-09c5 5... 6
EC2 VPC	vpc-30 7 6

その時点での構成の詳細情報とアタッチされていたAWSリソース

インスタンスタイプ	t2.micro
インスタンスの状態	running
プライベート DNS	ip-172 41.ap-northeast-1.com
プライベート IP	172. 41
パブリック DNS	ec2-54- .ap-northeast-1.c
AMI ID	ami-0f9 4075b

© 2019, 

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		<pre>Object deviceName: "/dev/sdf" ebs: Object attachTime: "2019-06-17T12:51:06.000Z" deleteOnTermination: false status: "attached" volumeId: "vol-02-1912fc"</pre>
Configuration.State.Name	"stopped"	"running"
Configuration.PublicIpAddress		"54.250-1912fc"
Configuration.InstanceType	"t2.micro"	"c4.large"
Configuration.StateTransitionReason	"User initiated (2019-06-07 03:29:25 GMT)"	""
Configuration.PublicDnsName	""	"ec2-54-250-1912fc.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17日の9:51:34午後	sk-1912fc.local	StartInstances	CloudTrail
2019年6月17日の9:51:06午後	sk-1912fc.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

リソースのインベントリ ステータス ⓘ

Search for existing or deleted resources recorded by AWS Config. For a specific resource, view the resource details, configuration timeline, or compliance timeline. The resource configuration timeline allows you to view all the configuration items captured over time for a specific resource. The resource compliance timeline allows you to view compliance status changes. To query your resource configurations, use the [advanced SQL query editor](#).

リソース タグ コンプライアンス状況

EC2: Instance ▼

削除されたリソースを含める

リソースのアクション ▼

リソース識別子	リソースタイプ	コンプライアンス
<input type="radio"/> i-0i-279d	EC2 Instance	1ルールに準拠していません
<input type="radio"/> i-0f-8c0	EC2 Instance	1ルールに準拠していません
<input type="radio"/> i-0f-2ed	EC2 Instance	
<input checked="" type="radio"/> i-0f-1068 (削除済み)	EC2 Instance	
<input type="radio"/> i-0f-5246 (削除済み)	EC2 Instance	

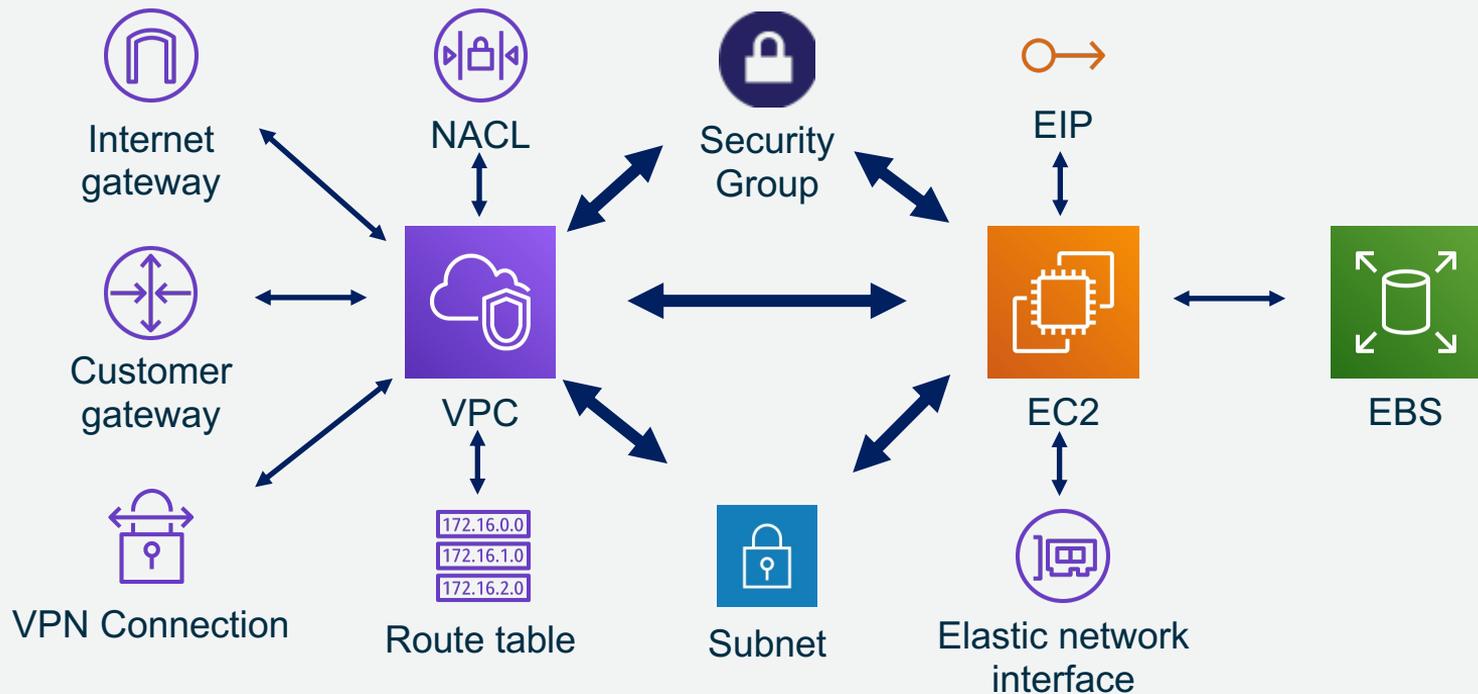
▼ CloudTrail イベント 5

どのユーザーによってターミネートされたか？

イベント時間	ユーザー名	イベント名
2019年6月3日の3:43:13午後	sk- local	StopInstances
2019年6月3日の3:43:12午後	sk- local	StopInstances

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

高度なクエリ

ステータス ⓘ

下記の SQL クエリエディタを使用して、リソース設定データをクエリします。サンプルクエリの1つを使用するか、リソースの構成スキーマを参照して独自のクエリを作成します。

SQL クエリエディタ

```
1 SELECT
2   resourceId,
3   resourceName,
4   resourceType,
5   relationships
6 WHERE
7   relationships.resourceId = 'sg-e7b6...
```

クエリの実行

サンプル SQL クエリ

サンプル SQL クエリ

List all EC2 instances currently running in my account

クエリの使用

List all EC2 instances with AMI ID "ami-2a69aa47"

クエリの使用

List all EBS volumes that are not in use

クエリの使用

List all resources that are related to security group "sg-12345"

クエリの使用

List all Dynamo

List all IAM use

List all RDS ins

List all RDS DB

List all Lambda

List all S3 buck

結果

resourceId	resourceName	resourceType	relationships
eni-060e...	310765db7	-	4 個の項目
eni-07f22...	62125ef3	-	4 個の項目
i-081d1e...	12548c0	-	5 個の項目
i-098590...	2bff2ed	-	5 個の項目
test_inVF	test_inVPC	AWS::Lambda::Function	4 個の項目
vpc-30c3	-	AWS::EC2::VPC	23 個の項目

AWS Config が対応しているAWSリソース



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

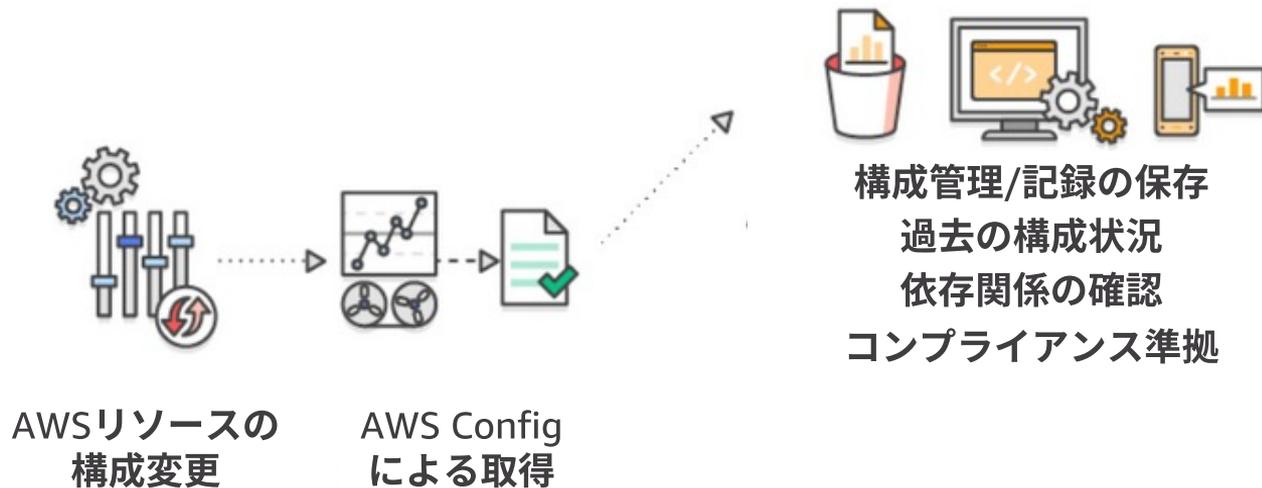


AWS Shield *1

*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

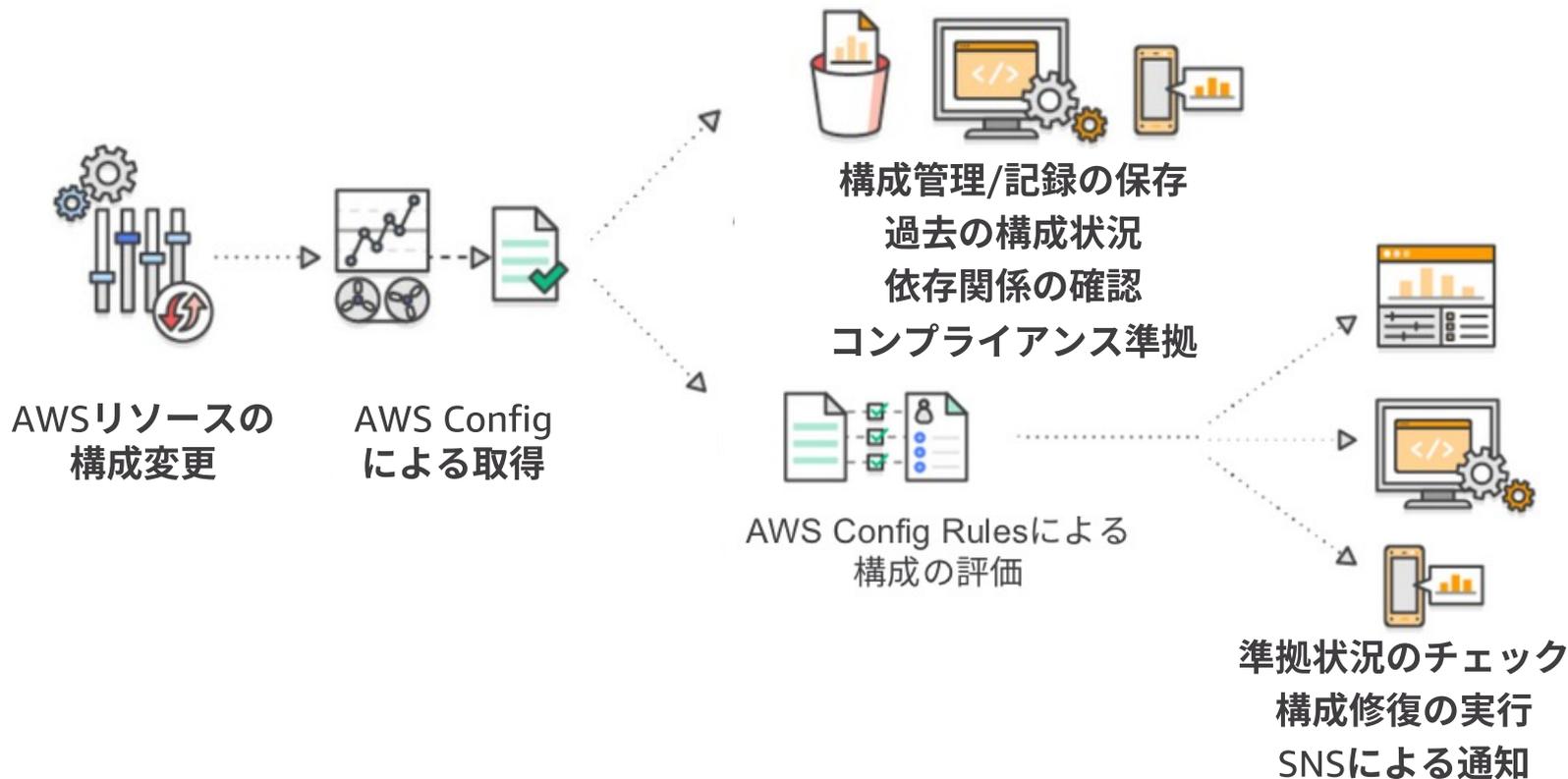
https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/resource-config-reference.html

AWS Config のよる構成管理のメリット



AWS 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

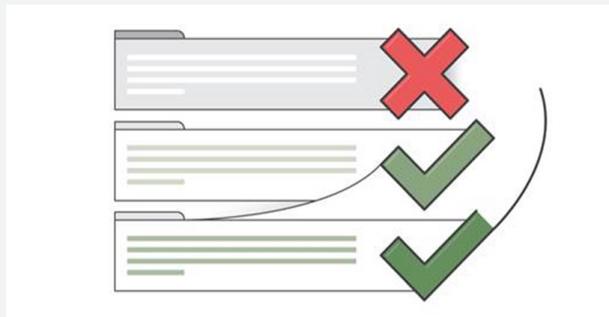
- 全てのEBCボリュームが暗号化されているか
- EC2インスタンスが適切にタグ付されているか等

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

Config ダッシュボード

ステータス ⓘ

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](#)

リソース

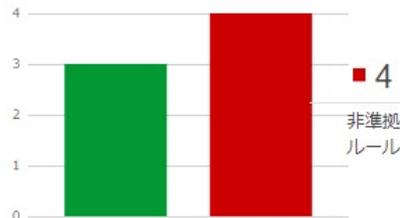
合計リソース数	39
上位 10 のリソースタイプ	合計
EC2 SecurityGroup	8
EC2 NetworkInterface	6
S3 Bucket	5
EC2 Instance	3
EC2 Volume	3
EC2 Subnet	3
Lambda Function	2
WAFRegional WebACL	2
ElasticLoadBalancingV2 LoadBalancer	2
EC2 InternetGateway	1

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が付けられているかの評価

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



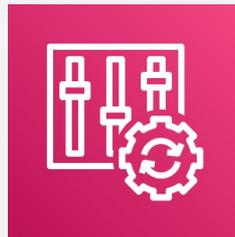
セキュリティ
アイデンティティ
コンプライアンス



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

awslabs / aws-config-rdk

Watch 25 Star 112 Fork 55

Code Issues 29 Pull requests 2 Projects 0 Security

The AWS Config Rules Development Kit helps developers set up, author and Config, create a Config rule and test it with sample ConfigurationItems.

296 commits 1 branch 0 releases

Branch: master New pull request

jongogogo and michaelborchert correct the import of module in test_code for the rdklib (#176) Latest commit 59aa408 13 days ago

- docs Add support for Python 3.7 (#152)
- policy I107 (#142)
- rdk correct the import of module in test_code for the rdklib (#176)
- testing Add support for Python 3.7 (#152)

```
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

修復アクションを選択

修復アクションの実行は、[AWS Systems Manager Automation](#)を使用して達成されます。AWS が推奨する一連の修復アクションまたはカスタムの修復アクションから選択します。ルールを修復するには、テーブルから範囲内のすべての非準拠リソースを選択します。

修復アクション	<input type="text" value="AWS-DisableS3BucketPublicReadWrite"/>
	<small>Disable S3-Bucket's public WriteRead access via private ACL</small>
リソース ID パラメータ	<input type="text" value="S3BucketName"/>

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一ユースケース #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一ユースケース #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 development of Rules

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

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

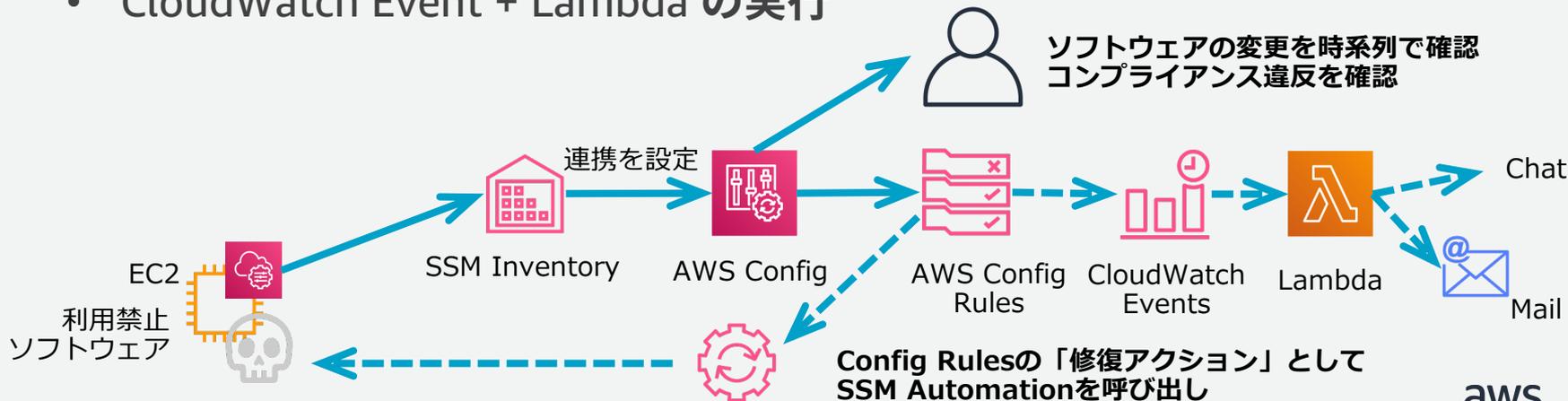
公開されているルールの例

- **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/aws-labs/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



[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

記録するリソースタイプ

AWS Config に設定の変更を記録させる AWS リソースの種類を選択します。デフォルトでは、AWS Config

すべてのリソース



このリージョンでサポートされているすべてのリソースを記録します ⓘ



グローバルリソース (AWS IAM リソースなど) を含める ⓘ

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
<input type="radio"/>	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

集約ビュー

アグリゲータ

config_aggregator

リージョン

すべてのリージョン

アカウント

すべてのアカウント

注: ダッシュボードに表示されるデータは複数の集約ソースから受信したものであり、異なる間隔で更新されます。データは数分遅れている可能性があります。

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 Volume 3

EC2 Subnet 3

EC2 Instance 3

WAFRegional WebACL 2

Config ルールのコンプライアンス状況

4 非準拠ルール

3 準拠ルール

非準拠ルール

ルール名	リージョン	アカウント	コンプライアンス
s3-bucket-logging-ena...	ap-northeast-1	276240001724	4 準拠していないリソース
s3-bucket-logging-ena...	ap-northeast-1	276240001724	4 準拠していないリソース
ec2-instance-manage...	ap-northeast-1	276240001724	3 準拠していないリソース

料金について

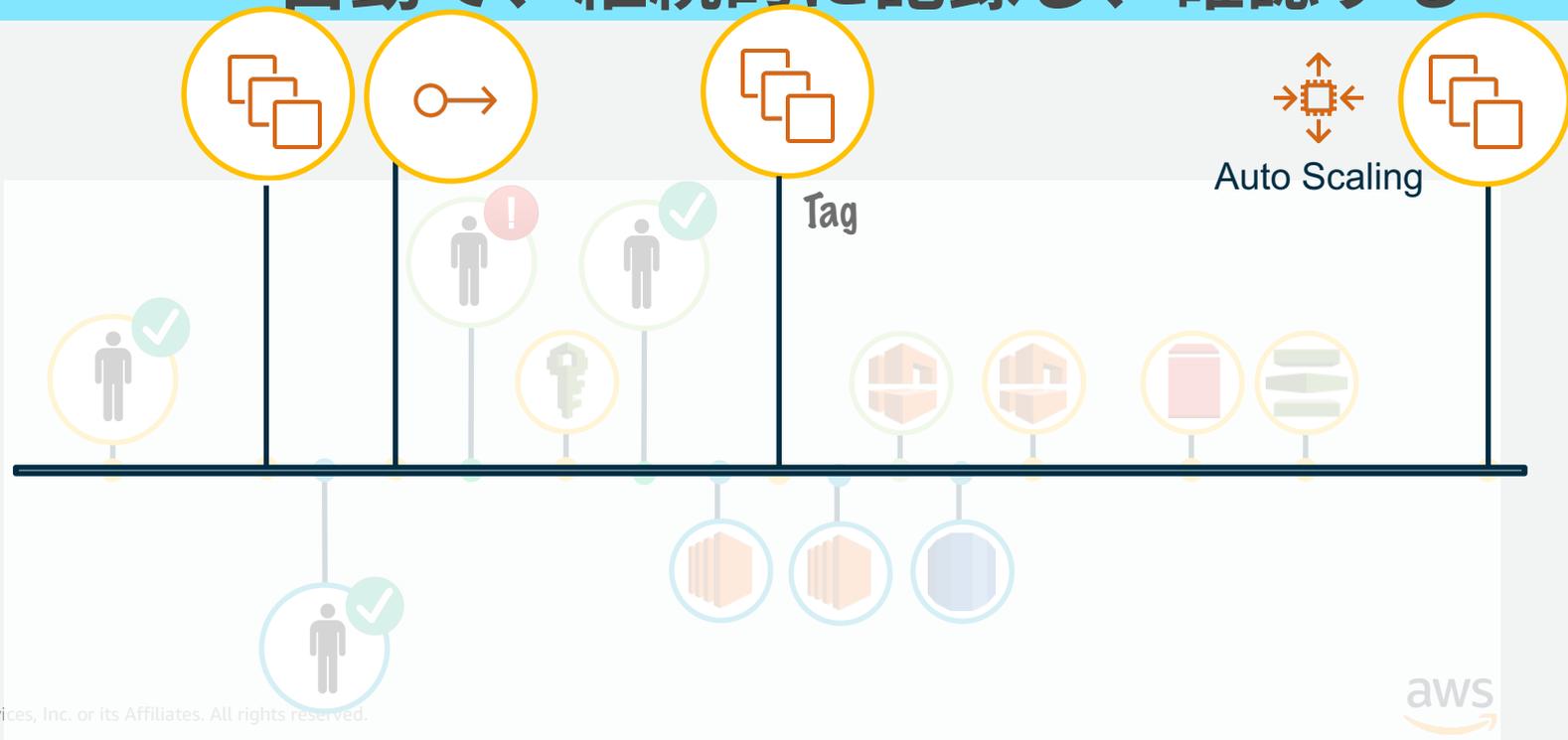
まとめ

AWSに対する構成変更をどう管理するか（再掲）

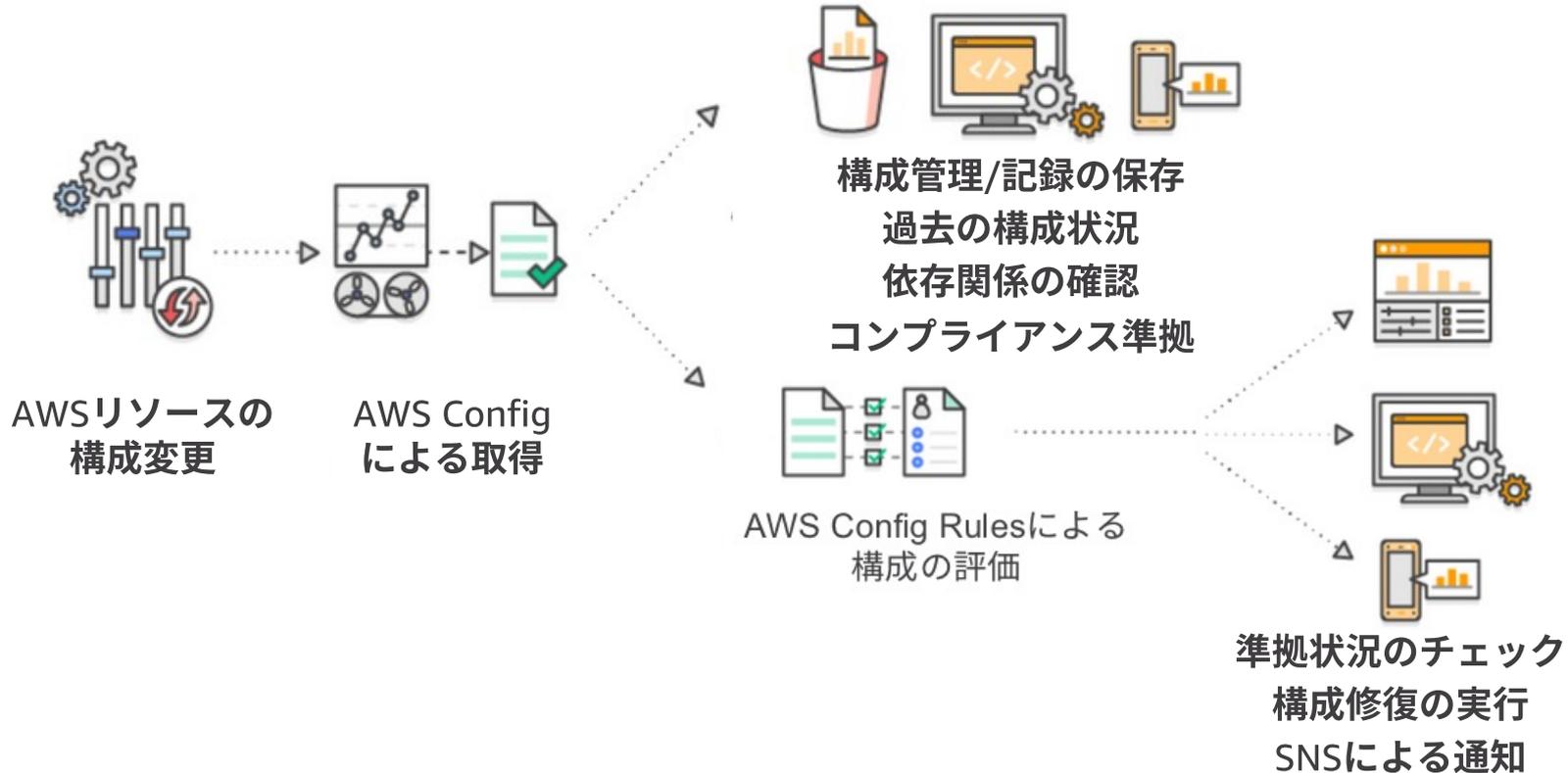
何に対して、誰が、いつ、何をしたかを
自動で、継続的に記録し、確認する



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一覧

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



The screenshot shows the AWS Japanese website header with the AWS logo, navigation links for '日本語', 'アカウント', and 'サポート', and a 'サインイン' button. The main heading is 'AWS クラウドサービス活用資料集トップ'. Below it is a paragraph of text in Japanese. At the bottom, there are four buttons: 'AWS Webinar お申込', 'AWS 初心者向け', '業種・ソリューション別資料', and 'サービス別資料'.

aws

日本担当チームへお問い合わせ サポート 日本語 アカウント [コンソールにサインイン](#)

製品 ソリューション 料金 ドキュメント 学習 パートナー AWS Marketplace その他

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

[AWS Webinar お申込](#) [AWS 初心者向け](#) [業種・ソリューション別資料](#) [サービス別資料](#)

<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>

