



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、 Amazon 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

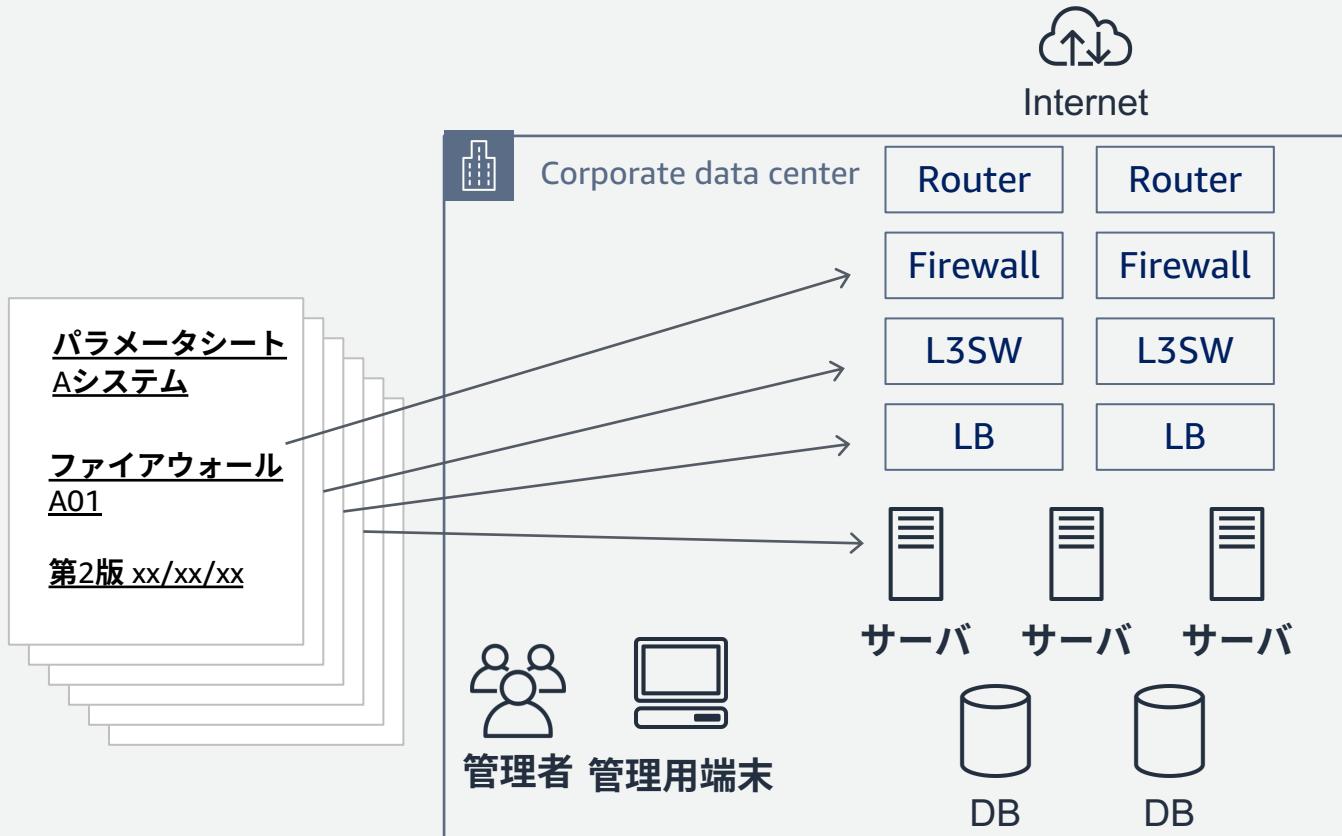
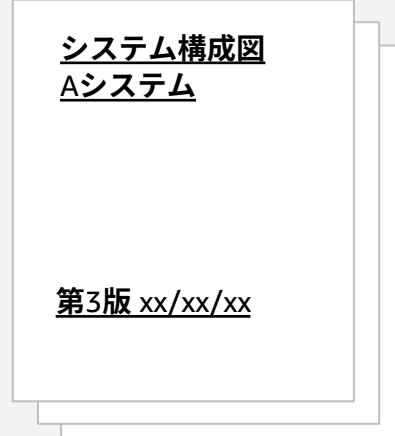
内容についての注意点

- 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.

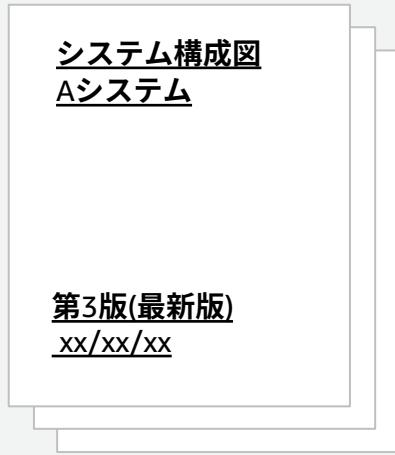
本日のアジェンダ

- 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

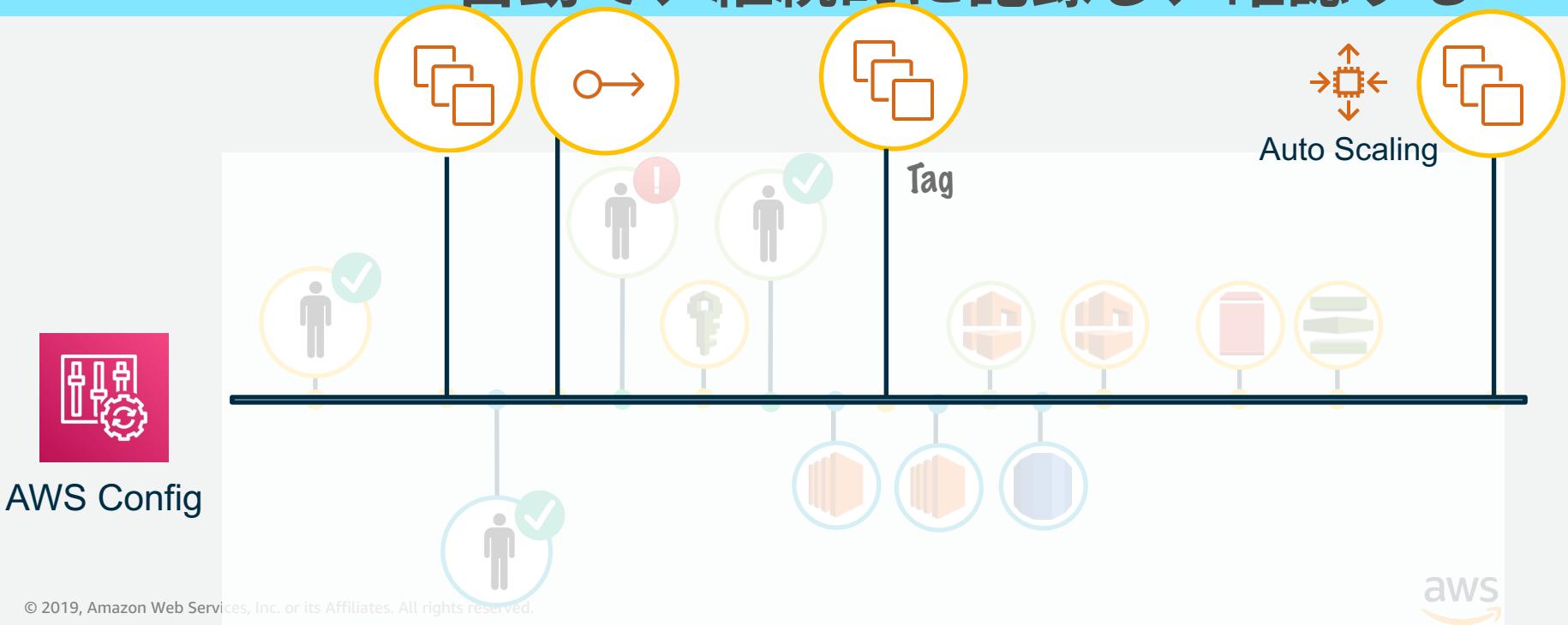


- ・構成ドキュメントと実設定の整合性
 - サービス修正による構成変更
 - バージョンアップに伴う設定見直し
 - トラブル時の緊急対処
 - 担当変更などによる引継ぎ

- ・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

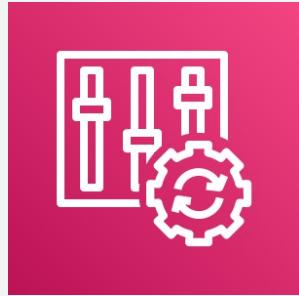
AWSに対する構成変更をどう管理するか

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

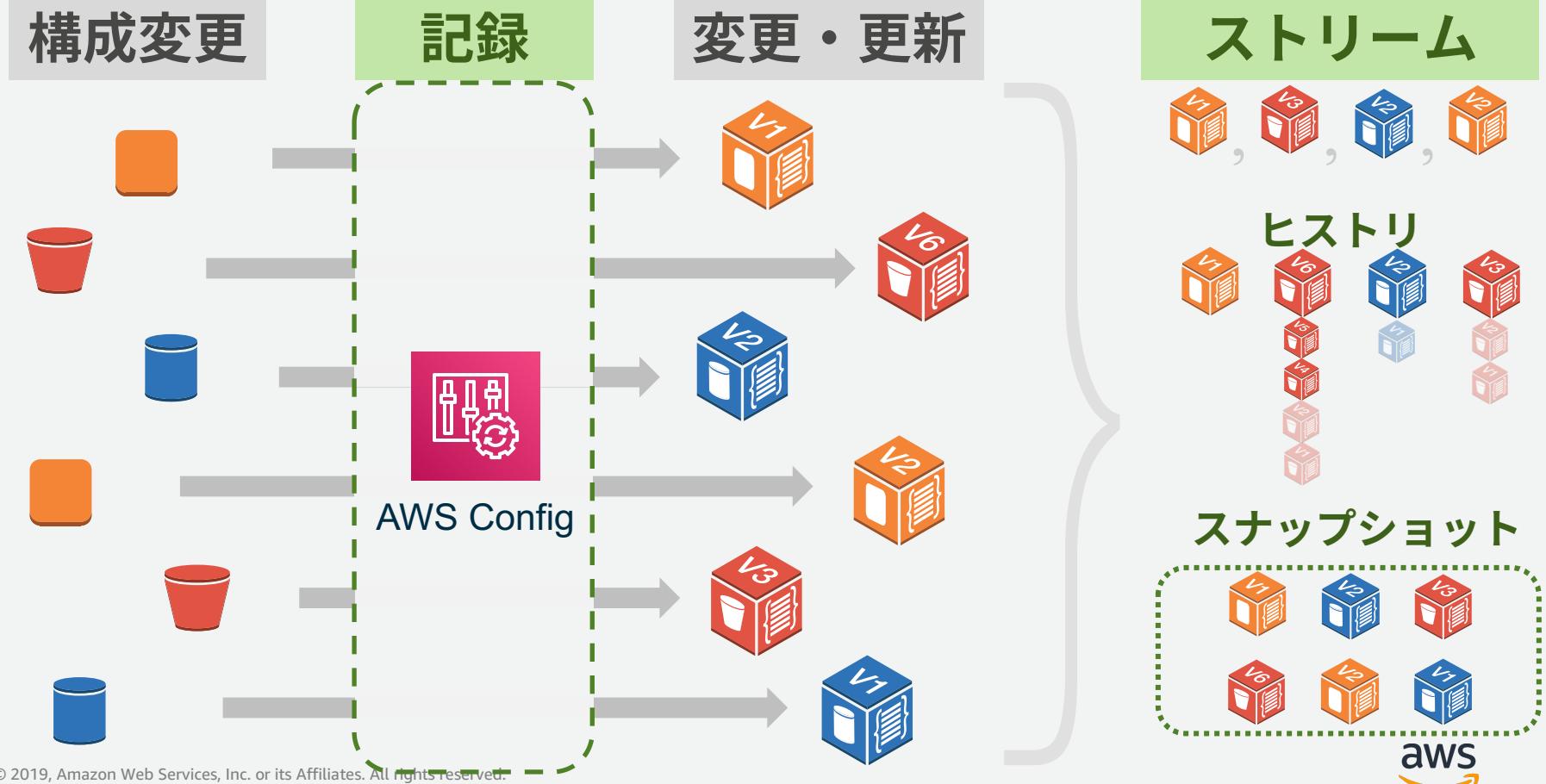
AWS Configとは



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

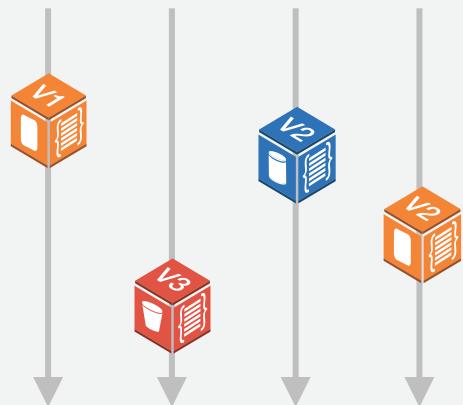
AWS Config の動作イメージ



AWS Config 各機能の役割

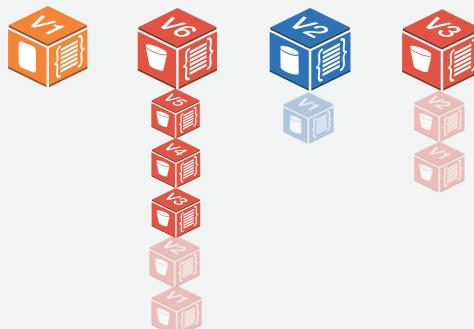
ストリーム (Configuration Stream)

- 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

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

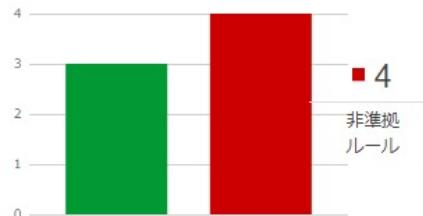
リソース

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

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

03 2019年6月月 3:45:43 午後

8 変更 1 イベント 7 変更 5 イベント

構成の詳細

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

Amazon Resource Name	arn:aws:ec2:ap-northeast-1:27...l724:instance/i-081...d2548c0	インスタンスタイプ	t2.micro
リソースタイプ	AWS::EC2::Instance	インスタンスの状態	running
リソース ID	i-081...d2548c0	プライベート DNS	ip-172...41.ap-northeast-1.com
リソース名	null	プライベート IP	172...41
アベイラビリティーゾーン	ap-northeast-1a	パブリック DNS	ec2-54...ap-northeast-1.c...
		AMI ID	ami-0f9...4075b

関係 5

EC2 NetworkInterface	EC2 SecurityGroup	EC2 Subnet	EC2 Volume	EC2 VPC
eni-060...10...	sg-e...9b	subnet-0e...6	vol-09c5...5...	vpc-30...7

© 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>	ボリュームの追加
Configuration.State.Name	"stopped"	"running"	インスタンス起動
Configuration.PublicIpAddress		"54.250 [REDACTED]"	
Configuration.InstanceType	"t2.micro"	"c4.large"	インスタンスタイプ変更(t2→c4)
Configuration.StateTransitionReason	"User initiated (2019-06-07 03:29:25 GMT)"	""	
Configuration.PublicDnsName	""	"ec2-54-250-[REDACTED].ap-northeast-1.compute.amazonaws.com"	

▼ 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-[REDACTED].local	StartInstances	CloudTrail	どのユーザーによる操作か？(CloudTrail)
2019年6月月17日の9:51:06午後	sk-[REDACTED].local	AttachVolume	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 リソース識別子 (オプション) 検索

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
i-01	279d	EC2 Instance 1 ルールに準拠していません
i-08	8c0	EC2 Instance 1 ルールに準拠していません
i-09	2ed	EC2 Instance
i-08	1068 (削除済み)	EC2 Instance
i-09	3246 (削除済み)	EC2 Instance

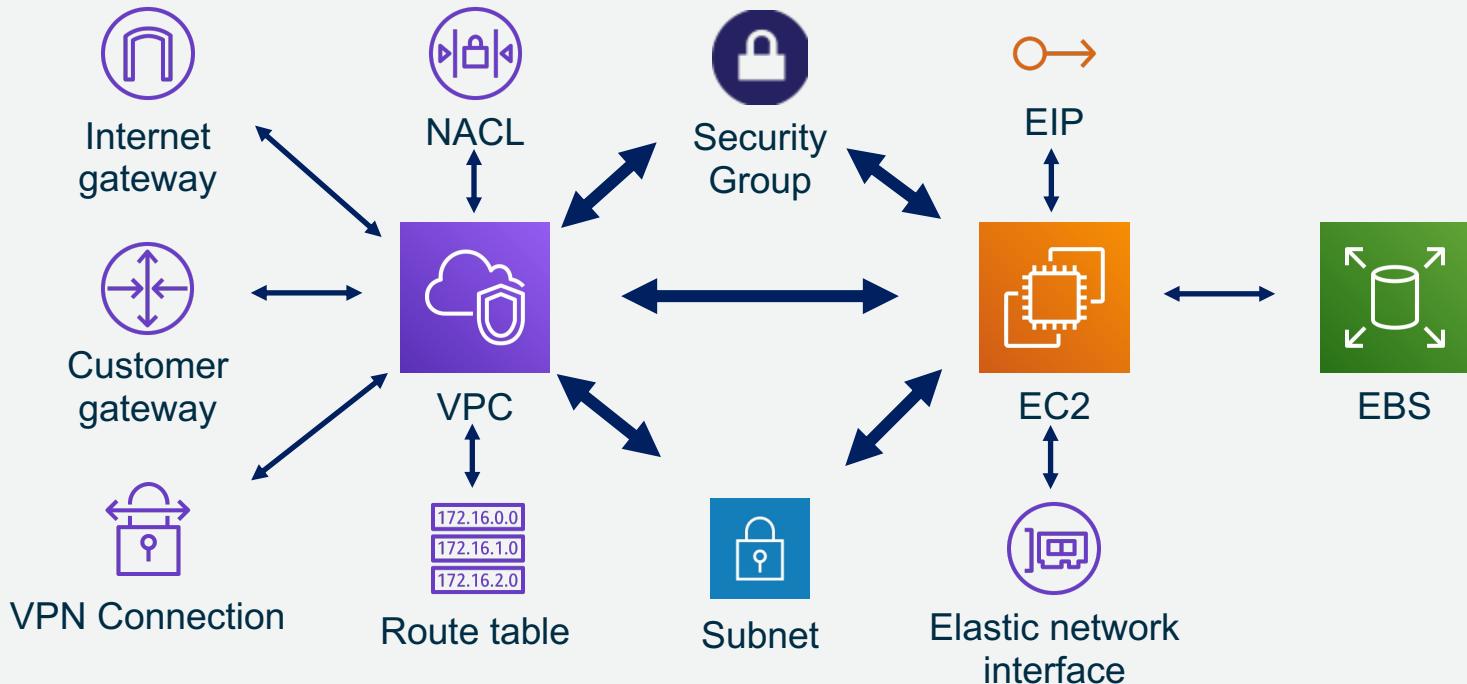
▼ CloudTrail イベント 5

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



リソースのイベントトリ：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...'
```

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

結果

resourceId	resourceName	resourceType	relationships
eni-060e...	310765db7	-	AWS::EC2::NetworkInterface 4 個の項目
eni-07f22...	62125ef3	-	AWS::EC2::NetworkInterface 4 個の項目
i-081d1e...	f2548c0	-	AWS::EC2::Instance 5 個の項目
i-098590...	b2ff2ed	-	AWS::EC2::Instance 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

クエリの実行 サンプル SQL クエリ

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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

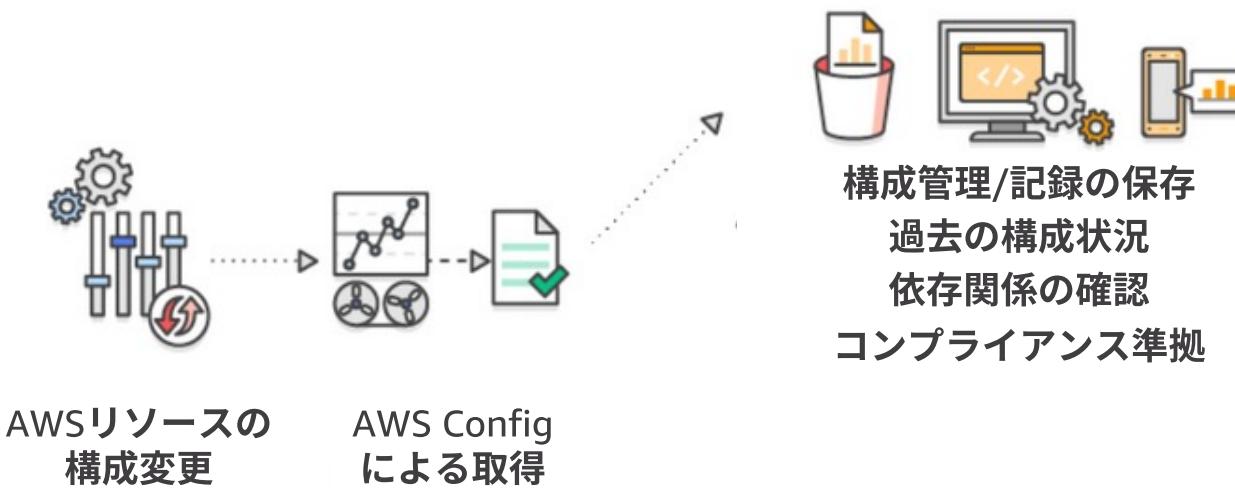
*1: グローバルサービスは米国東部（バージニア北部）リージョンでサポート

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

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

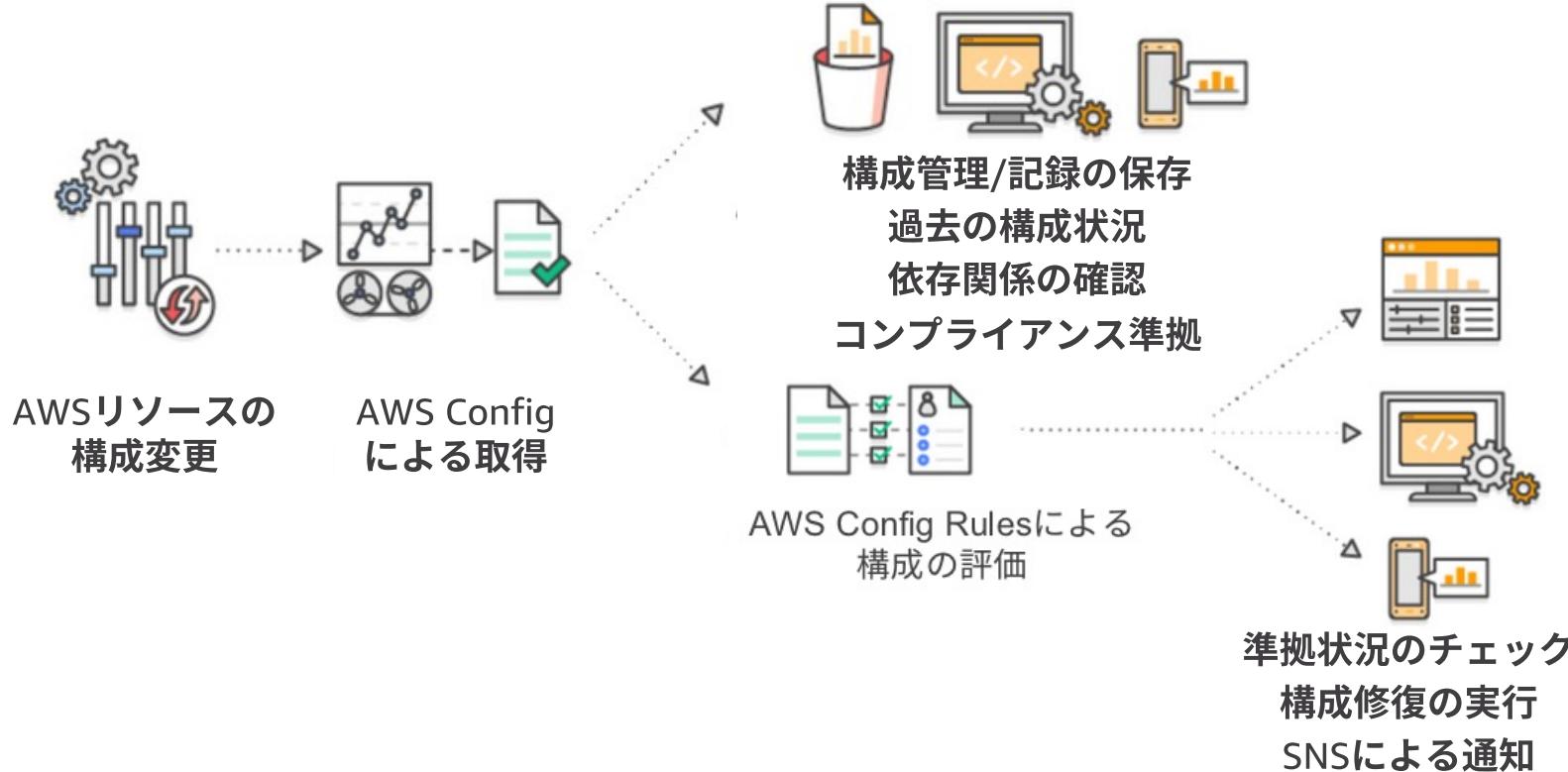


AWS Config のによる構成管理のメリット



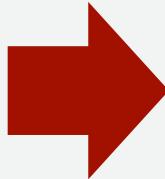
AWS Config Rules 概要

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

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

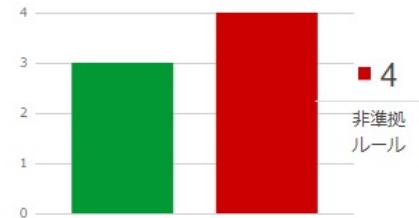
リソース

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
WAFFRegional 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

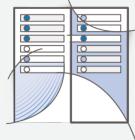
定期的

- 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



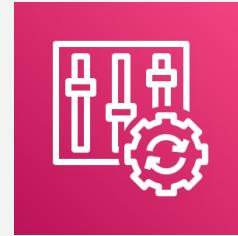
ストレージ

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

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



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](https://github.com/awslabs/aws-config-rdk)



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)

docs

Add support for Python 3.7 (#152)

policy

I107 (#142)

rdk

correct the import of module in test_code for the rdklib (#

testing

Add support for Python 3.7 (#152)

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

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Watch

25

Star

112

Fork

55

```
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
```

Latest commit 59aa408 13 days ago

```
$ 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>
```

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 AWS-DisableS3BucketPublicReadWrite

Disable S3-Bucket's public WriteRead access via private ACL

リソース ID パラメータ 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口グ(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 development 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

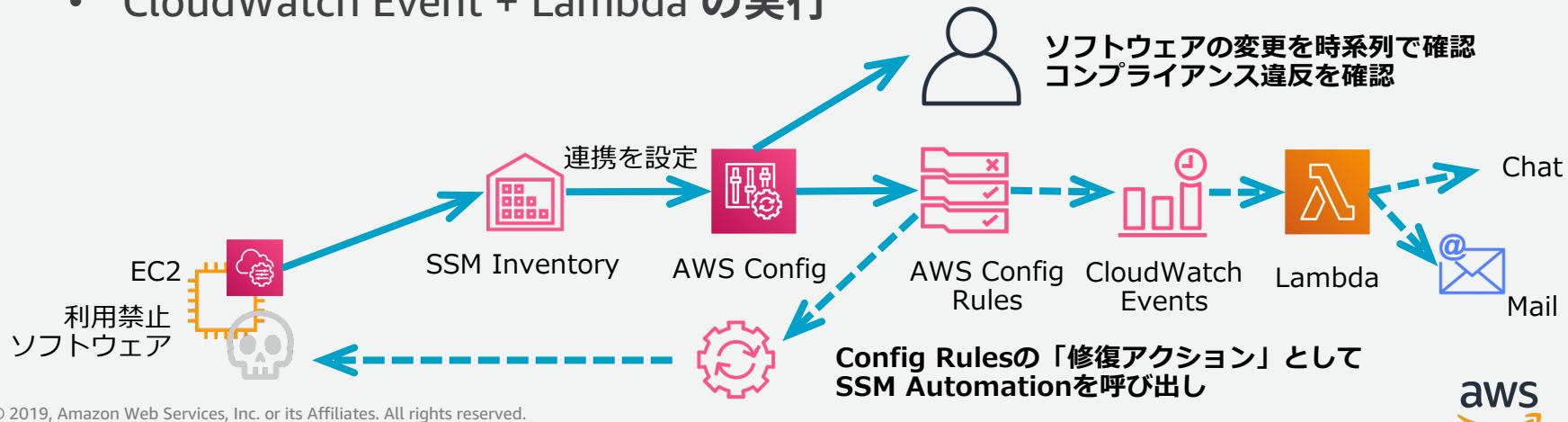
<https://github.com/awslabs/aws-config-rules>

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



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

The screenshot shows a blog post on the AWS Management Tools Blog. The header includes the AWS logo and navigation links for Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, Explore More, and a search icon. Below the header, there are links for Blog Home, Category, Edition, and Follow. The main content area has a title 'AWS Management Tools Blog' and a sub-title 'AWS Config best practices' by Sid Gupta on 27 JUL 2018. It includes a share button. The post content discusses AWS Config's role in maintaining configuration history and evaluating against best practices. It lists two best practices: 1. Enabling AWS Config in all accounts and Regions, and 2. Recording configuration changes to ALL resource types. The post concludes that AWS Config supports comprehensive audits.

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

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



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



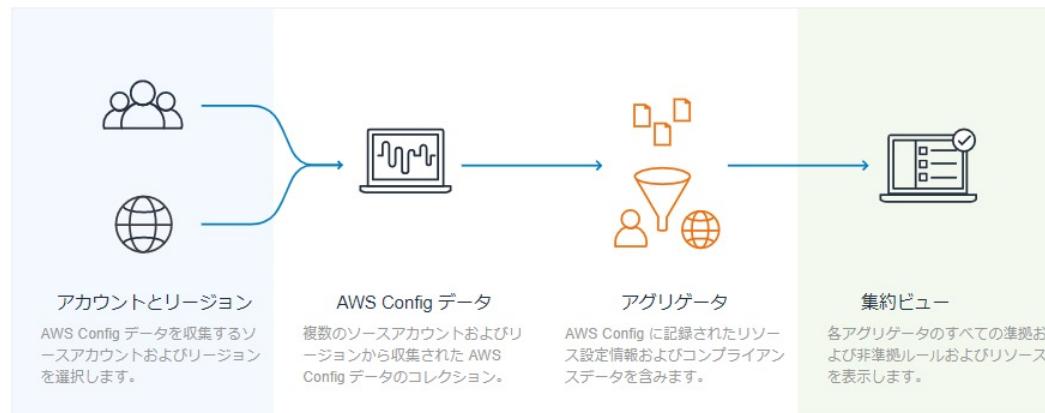
Available at no
additional charge

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
<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

❶ 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
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

❷ 4 非準拠ルール
❸ 3 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	❹ 準拠していないリソース
s3-bucket-logging-ena...	ap-northeast-1	276240001724	❹ 準拠していないリソース
ec2-instance-manage...	ap-northeast-1	276240001724	❺ 準拠していないリソース

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

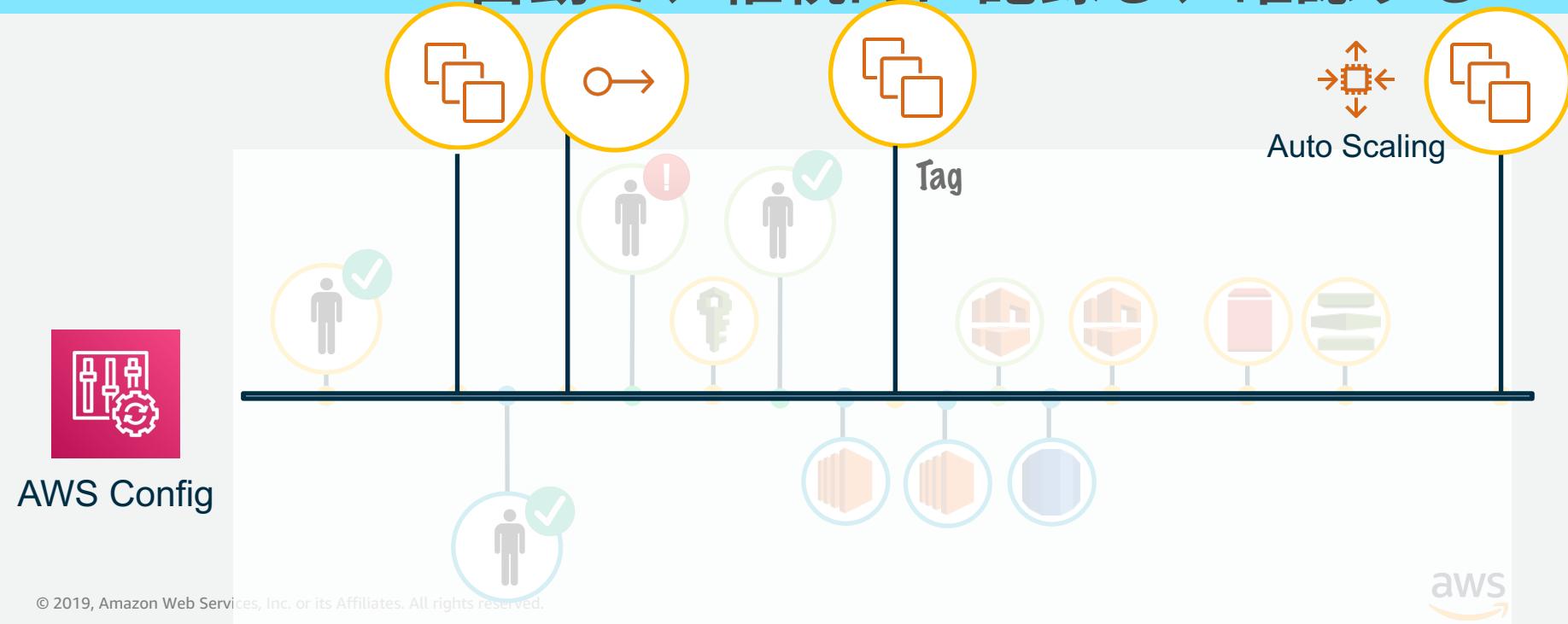
- 追加料金

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

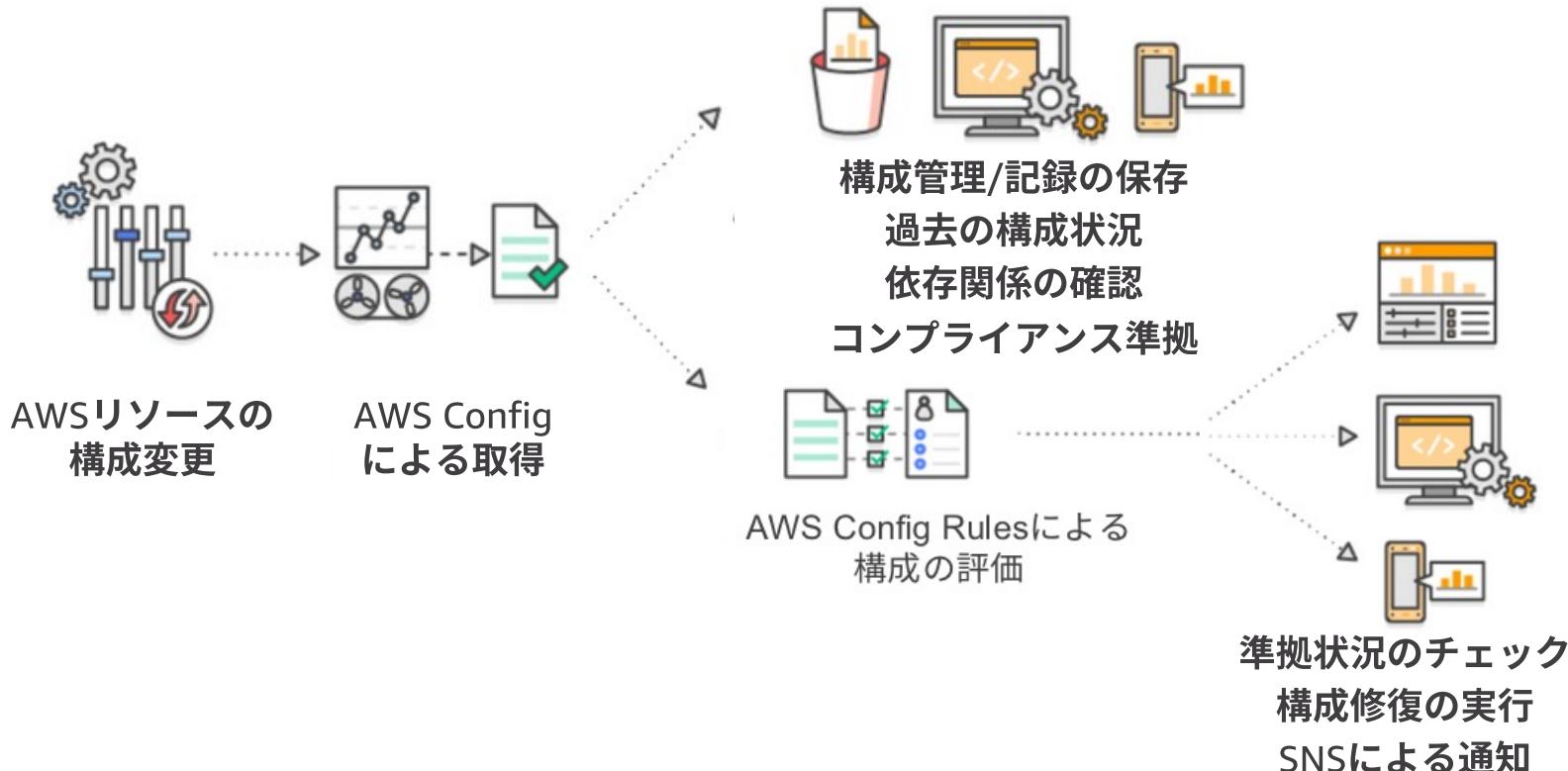
まとめ

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 / 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

The screenshot shows the AWS Japan website homepage. At the top, there is a navigation bar with the AWS logo, search bar, and links for "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", and "コンソールにサインイン". Below the navigation bar is a secondary navigation menu with links for "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", and a search icon. The main content area features a large title "AWS クラウドサービス活用資料集トップ" and a descriptive paragraph about AWS services. Below the paragraph are four call-to-action 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".

<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>





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 Update

サービスカットシリーズ

Archived

Security Solutions Architect 桐谷 彰一
2020/12/08

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

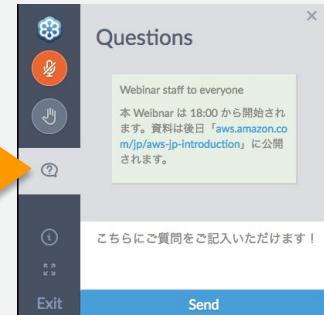
AWS Black Belt Online Seminar とは

「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、Amazon 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

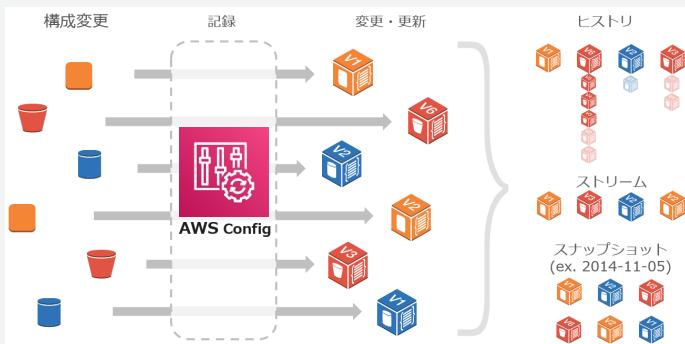
- 本資料では2020年12月8日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available 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

1. AWS Config のおさらい
2. 新機能：適合パックの概要
3. 新機能：サードパーティリソースサポートの概要
4. 組織のセキュリティ管理をより効率化するその他のアップデート
5. まとめ

AWS Config のおさらい

構成情報の記録、評価を行うマネージドサービス



特徴 (<http://aws.amazon.com/jp/config/>)

- 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 SNS を使った通知も可能
- 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 (Config Rules)

価格体系 (<http://aws.amazon.com/jp/config/pricing/>)

- 1 回の設定項目の記録につき 0.003 USD
- Config Rules ルール評価ごとに 0.001USD
- ログが保存される Amazon S3 の料金

AWS Config の利用例

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
(SSH/RDPがフルオープンのSGが発見された！ 影響は？)

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 DynamoDB tables where server-side encryption is disabled	クエリの使用
List all IAM users created between date "2018-12-01T00:00" and date "2019-02-28T00:00"	クエリの使用

高度なクエリ

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

SQL クエリエディタ

```
1 SELECT
2     resourceId,
3     resourceName,
4     resourceType,
5     relationships
6 WHERE
7     relationships.resourceId = 'sg-e7k...8b'
```

List all RDS instances running data

結果

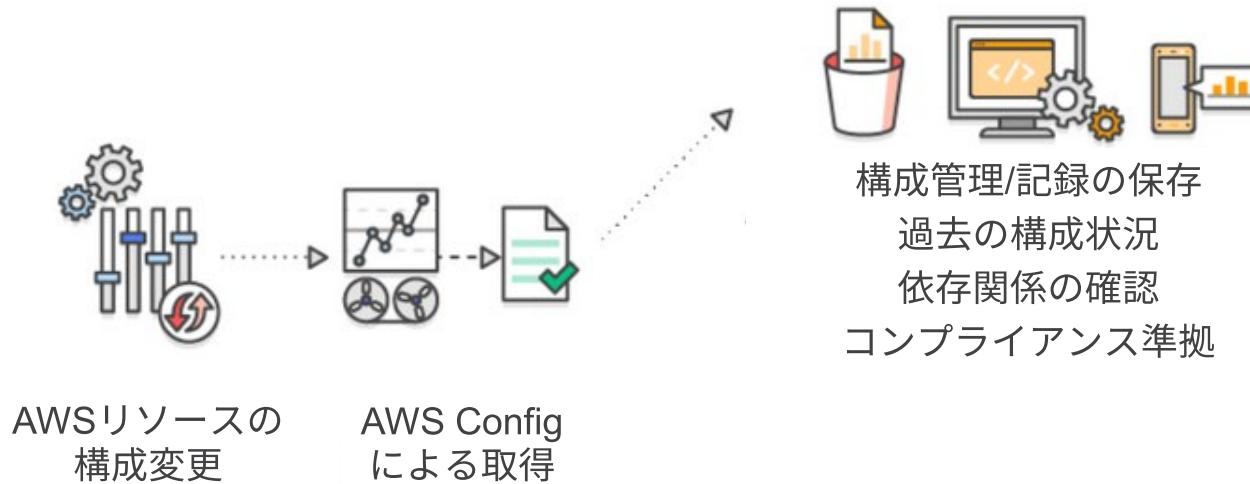
List all RDS DB Instances that are p

List all Lambda functions using runti

List all S3 buckets where versioning

resourceId	resourceName	resourceType	relationships
eni-060e	910765db7	AWS::EC2::NetworkInterface	4 個の項目
eni-07f22	f62125ef3	AWS::EC2::NetworkInterface	4 個の項目
i-081d1e	f2548c0	AWS::EC2::Instance	5 個の項目
i-098590	f2bff2ed	AWS::EC2::Instance	5 個の項目
test_inVF	test_inVPC	AWS::Lambda::Function	4 個の項目
vpc-30c3	7	AWS::EC2::VPC	23 個の項目

AWS Config による構成管理



AWS Config Rules の利用例

パブリック読み込みが許可されたS3バケットを把握

s3-bucket-public-read-prohibited

説明 S3 バケットが読み取りパブリックアクセスを許可していないことを確認します。S3 バケットポリシーまたはバケット ACL で読み取りパブリックアクセスを許可している場合、そのバケットは準拠していません。

コンプライアンス状況

非準拠

リソース ID リソースタイプ リソースのコンプライアンス状況 アクション

リソース ID	リソースタイプ	リソースのコンプライアンス状況	アクション
sk-test	S3 Bucket	非準拠	該当なし

再評価 結果の削除 編集

AWSが提供するマネジドルールを利用して、リスクがある設定を簡単に把握
(160以上のルールを提供) ※2020/12/08現在
+カスタムルールで特定の評価にも対応

必要があれば修復アクションで1click/自動で対応

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。

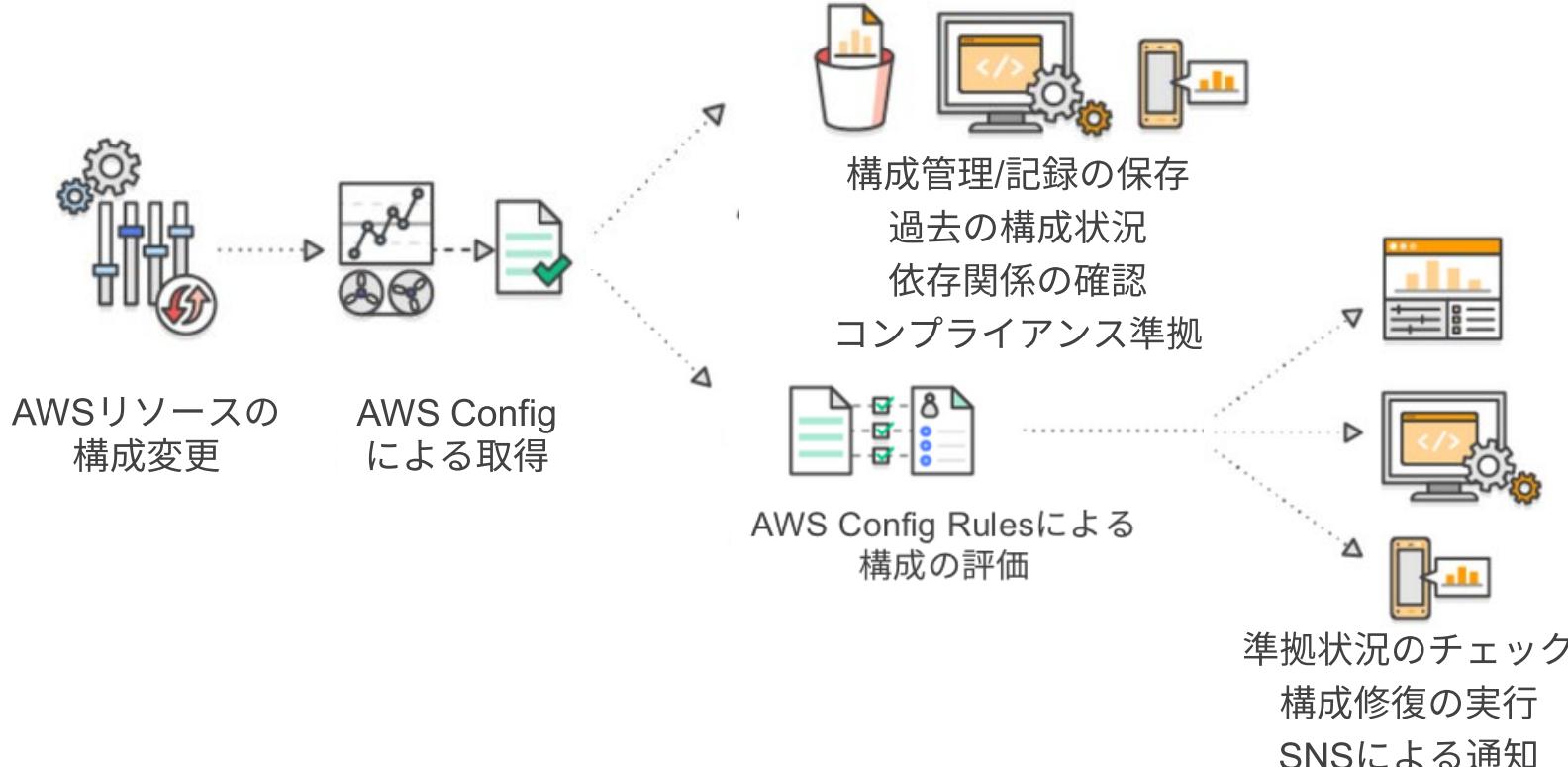
修復アクション AWS-DisableS3BucketPublicReadWrite

Disable S3-Bucket's public WriteRead access via private ACL

リソース ID パラメータ S3BucketName

修復アクションを実行し、パブリック読み込みアクセスを許可を"無効"にすることも可能

AWS Config Rules で構成情報を評価



基本的な機能については、前回の BlackBelt をご確認ください

[AWS Black Belt Online Seminar] AWS Config 資料及び QA 公開

<https://aws.amazon.com/jp/blogs/news/webinar-bb-aws-config-2019/>



ブログホーム カテゴリ ▾ エディション ▾ Search B

Amazon Web Services ブログ

[AWS Black Belt Online Seminar] AWS Config 資料及び QA 公開

by AWS Japan Staff | on 30 JUN 2019 | in AWS Config, General, Webinars |
[Permalink](#) | [Share](#)

先日(2019/6/18) 開催しました AWS Black Belt Online Seminar 「AWS Config」の資料を公開しました。当日、参加者の皆様から頂いた QA の一部についても共有しております。



© 2020, Amazon



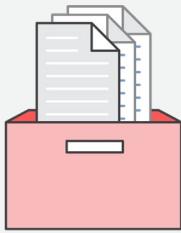
20190618 AWS Black Belt Online Seminar AWS Config from
Amazon Web Services Japan



新機能のご紹介

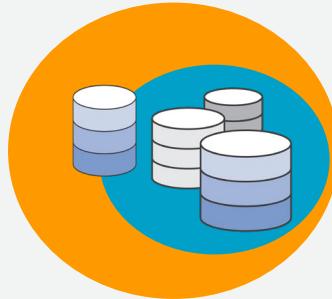
AWS Config のアップデート

適合パック



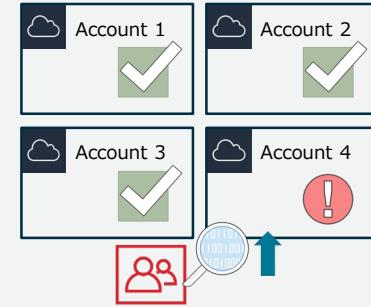
組織全体への展開と
コンプライアンスチェックを
より簡単に

サードパーティ リソースへの対応



AWS リソース以外の
設定変更や
追跡が可能に

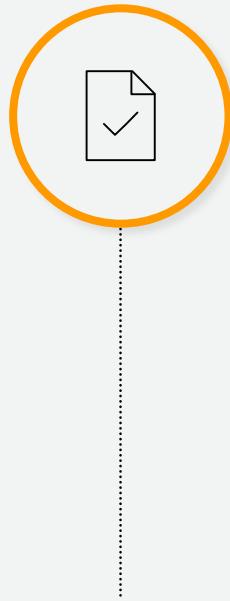
その他の アップデート



組織のセキュリティ管理を
より効率的に

適合パックの概要

AWS Config 適合パック (Conformance Pack)



構成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 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
- 単一AWSアカウント、AWS Organizations の組織全体に対して適用可能

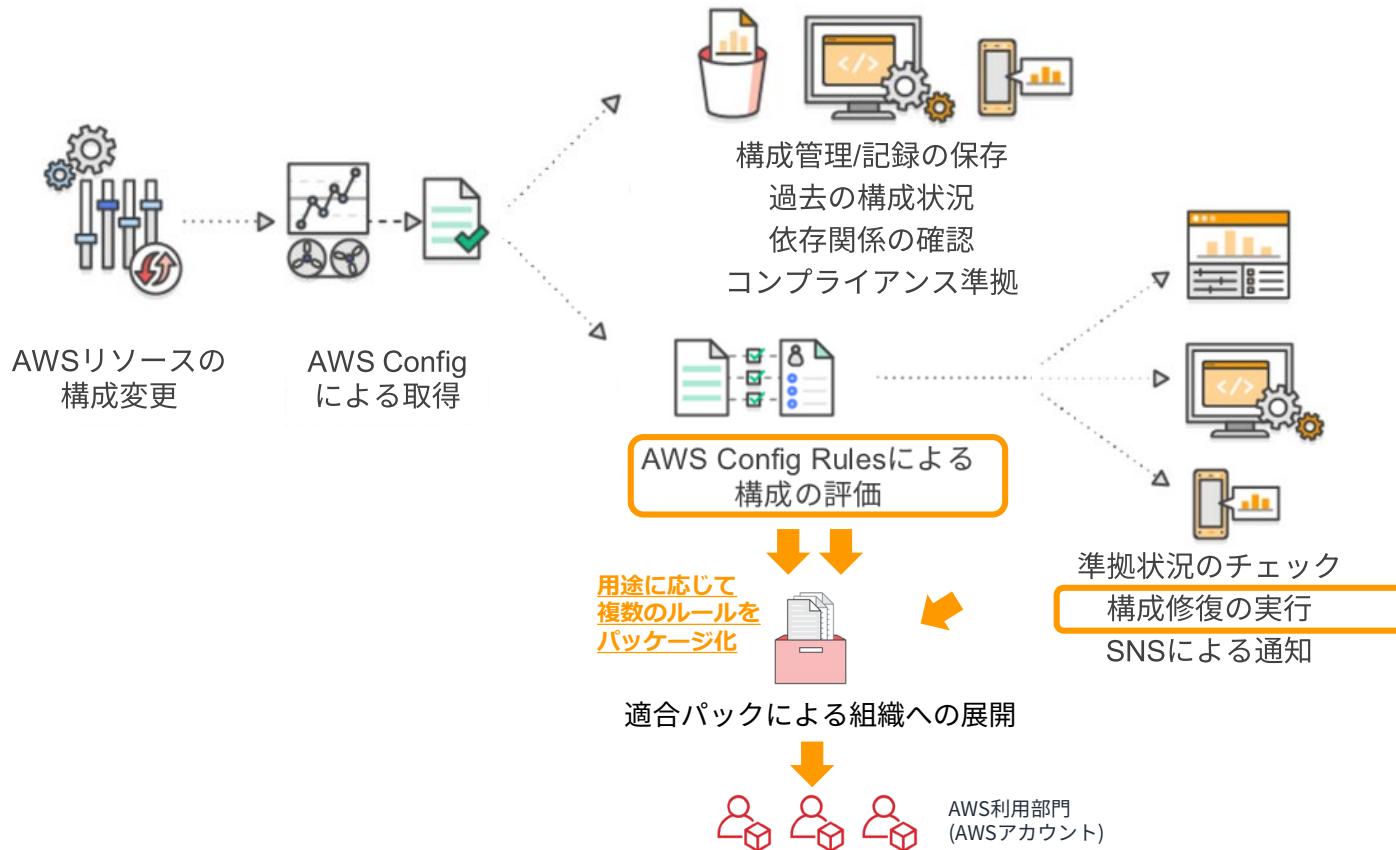
不变性(immutable)

- 個々のルールは、アクセス権限やアカウントの権限に関わらず、デプロイされた適合パックの外部から変更不可
- 組織のマスター アカウントから展開した適合パックは、メンバーアカウントから変更不可

価格体系

- 適合パックによるルール評価ごとに 0.0012USD

AWS Config 適合パック



適合パックの詳細

AWS Config > 適合パック > ControlTowerSample

ControlTowerSample

ルール 設定

ルール (12)

名前	↓ 1つの適合パックに複数の Config Rule	Remediation action	Compliance
CheckForRestrictedSshPolicy-conformance-pack-beqouusak		設定されていません	⚠ 非準拠
CheckForEbsOptimizedInstance-conformance-pack-beqouusak		設定されていません	✓ 準拠
CheckForS3PublicWrite-conformance-pack-beqouusak		設定されていません	✓ 準拠
CheckForRestrictedCommonPortsPolicy-conformance-pack-beqouusak		設定されていません	⚠ 非準拠
CheckForRootMfa-conformance-pack-beqouusak		設定されていません	⚠ 非準拠
CheckForS3PublicRead-conformance-pack-beqouusak		設定されていません	✓ 準拠
CheckForRdsPublicAccess-conformance-pack-beqouusak		設定されていません	✓ 準拠

↑ 各Config Rule の評価結果

適合パックのサンプルテンプレート

「運用のベストプラクティス」など、様々なサンプルを提供
50個を超えるテンプレートを用意（2020/12/08現在）

ドキュメント > AWS Config > 開発者ガイド フィードバック

コンフォーマンスパックのサンプルテンプレート

PDF

AWS Config コンソールに表示されるコンフォーマンスパックの YAML テンプレートを次に示します。コンフォーマンスパックテンプレート内では、1つ以上の AWS Config ルールと修正アクションを使用できます。コンフォーマンスパックに一覧表示されている AWS Config ルールは、AWS Config 管理ルールまたは AWS Config カスタムルールにすることができます。すべてのコンフォーマンスパックテンプレートは、からダウンロードできます[GitHub](#)。

トピック

- AWS Control Tower 発券的ガードレールコンフォーマンスパック
- ABS CCIG 2.0 マテリアルワーカークロードの運用のベストプラクティス
- ABS CCIG 2.0 標準ワーカークロードの運用のベストプラクティス
- ACSC 基本的な 8 運用のベストプラクティス
- ACSC ISM 運用のベストプラクティス
- AI と ML 運用のベストプラクティス
- Amazon の運用上のベスト プラクティス DynamoDB
- Amazon S3 の運用に関するベストプラクティス
- APRA CPG 234 運用のベストプラクティス
- アセット管理の運用のベストプラクティス
- AWS ID とアクセス管理の運用に関するベストプラクティス
- AWS Well-Architected フレームワークの信頼性の柱運用のベストプラクティス
- AWS Well-Architected フレームワークセキュリティ柱の運用のベストプラクティス
- BCP と DR 運用のベストプラクティス

GitHub にて公開 + 日々追加中

The screenshot shows the GitHub repository page for `aws-labs / aws-config-rules`. The master branch is selected. Recent commits are listed:

- tysodotcom Updated names of the CIS AWS Foundation benchmark y... 24 days ago
- AWS-Control-Tower-Dete... Added Control Tower Conformance Pack 2 months ago
- Operational-Best-Practice... Additional conformance packs 2 months ago
- Operational-Best-Practice... Additional conformance packs 2 months ago
- Operational-Best-Practice... Updated ACSC Related Conformance Packs last month
- Operational-Best-Practice... Updated ACSC Related Conformance Packs last month

適合パックのサンプルテンプレート (1/2)

各国や業界のセキュリティ要件、ガイドライン、レギュレーションなどに対するテンプレート

テンプレート名	テンプレート名
ABS CCIG 2.0 マテリアルワークコードの運用のベストプラクティス	K-ISMS 運用のベストプラクティス
ABS CCIG 2.0 標準ワークコードの運用のベストプラクティス	MAS 通知 655 運用のベストプラクティス
ACSC 基本的な 8 運用のベストプラクティス	MAS TRMG 2013 運用のベストプラクティス
ACSC ISM 運用のベストプラクティス	NC TRMG の運用のベストプラクティス
APRA CPG 234 運用のベストプラクティス	NERC CIP 運用のベストプラクティス
BNM 運用のベストプラクティスRMiT	NCSC クラウドセキュリティ原則の運用のベストプラクティス
CIS 運用のベストプラクティス	NIST 800-53 リビジョン 4 運用のベストプラクティス
CMMC レベル 1 運用のベストプラクティス	NIST 800 171 運用のベストプラクティス
CMMC レベル 2 運用のベストプラクティス	NIST CIS 運用のベストプラクティス
運用のベストプラクティス FedRAMP (低)	NYDFS 23 運用のベストプラクティス
運用のベストプラクティス FedRAMP (中)	PCI DSS 3.2.1 運用のベストプラクティス
FFIEC の運用のベストプラクティス	RBI MD-ITF 運用のベストプラクティス
HIPAA セキュリティ運用のベストプラクティス	

適合パックのサンプルテンプレート (2/2)

各AWSサービスのベストプラクティスや、Well-Architected フレームワークの視点で用意されたテンプレート

テンプレート名	テンプレート名
AWS Control Tower 発見的ガードレールコンフォーマンスパック	クエリに関する運用のベストプラクティス - コーディングのベストプラクティス
AI と ML 運用のベストプラクティス	アセット管理の運用のベストプラクティス
Amazon の運用上のベスト プラクティス DynamoDB	ロードバランシング運用のベストプラクティス
Amazon S3の運用に関するベストプラクティス	ログ記録運用のベストプラクティス
EC2 運用のベストプラクティス	管理とガバナンスサービスの運用のベストプラクティス
AWS IDとアクセス管理の運用に関するベストプラクティス	モニタリング運用のベストプラクティス
AWS Well-Architected フレームワークの信頼性の柱運用のベストプラクティス	ネットワーキングとコンテンツ配信サービスの運用のベストプラクティス
AWS Well-Architected フレームワーク セキュリティ柱の運用のベストプラクティス	パブリックにアクセス可能なリソース運用のベストプラクティス
BCP と DR 運用のベストプラクティス	セキュリティ、アイデンティティ、およびコンプライアンスサービスの運用のベストプラクティス
コンピューティングサービス運用のベストプラクティス	サーバーレス運用のベストプラクティス
データの耐障害性に関する運用のベストプラクティス	ストレージサービス運用のベストプラクティス
データベースサービス運用のベストプラクティス	修正アクションを含むテンプレートの例
データレイクおよび分析サービスの運用のベストプラクティス	カスタムコンフォーマンスパック
暗号化とキー管理の運用のベストプラクティス	

適合パックの設定イメージ (1/3)

AWS Well-Architected フレームワークセキュリティ柱の運用のベストプラクティス

AWS Config ×

AWS Config > 適合パック

適合パック

適合パックは、AWS アカウントで単一のエンティティとしてデプロイおよびモニタリングできる AWS Config ルールおよび修復アクションのコレクションです。 [詳細はこちら](#)

適合パック

名前またはコンプライアンスステータスでルールをフィルタリングする

名前	デプロイ	コンプライアンス
MyS3CPack	完了しました	⚠ 非準拠
OrgConformsPack-CISPack-gahzupvp	完了しました	⚠ 非準拠

ルール
リソース
▼ アグリゲータ
ルール
リソース
認証
高度なクエリ
設定

最新情報 □
ドキュメント □
パートナー □
よくある質問 □
料金表 □

テンプレートを指定

テンプレートの詳細

適合パックテンプレート
すべての適合パックはテンプレートに基づいています。テンプレートは、AWS Config ルールと修復アクションをデプロイする AWS アカウントとリージョンに関する設定情報を含む YAML ファイルです。

サンプルテンプレートを使用 テンプレートをアップロード

サンプルテンプレート

well

Operational Best Practices for AWS Well Architected Reliability Pillar
Operational Best Practices for AWS Well Architected Security Pillar
サンプルテンプレートを選択

サンプルテンプレートを表示するには、次を参照してください [適合パックのサンプルテンプレート](#)です。 □

キャンセル 次へ

適合パックの設定イメージ (2/3)

AWS Well-Architected フレームワークセキュリティ柱の運用のベストプラクティス

The screenshot shows three panels from the AWS CloudFormation console:

- 適合パックの詳細を指定**:
 - 適合パックの詳細**
 - リージョン: Asia Pacific (Tokyo)
 - 適合パック名: mycpack-WASEC
 - 適合パック名には、文字 (A~Z および a~z) 、数字 (0~9)、できません。
 - パラメータ - オプション**: パラメータが入力されていません。ボタン: パラメータを追加
- 適合パックの確認とデプロイ**:
 - テンプレートの詳細**
 - サンプルテンプレート: Operational Best Practices for AWS Well Architected Security Pillar
 - 適合パック**
 - 適合パックは、AWS アカウントで単一のエンティティとしてデプロイおよびモニタリングできる AWS Config ルールおよび修復アクションのコレクションです。 詳細は[こちら](#)
 - 検索バー: 名前またはコンプライアンスステータスでルールをフィルタリングする
 - リスト:

名前	デプロイ	コンプライアンス
mycpack-WASEC	完了しました	△ 非準拠
MyS3CPack	完了しました	△ 非準拠
OrgConformsPack-CISPack-gahzupvp	完了しました	△ 非準拠

適合パックの設定イメージ (3/3)

AWS Well-Architected フレームワークセキュリティ柱の運用のベストプラクティス

mycpack-WASEC

デプロイ:
④完了しました

ルール 設定

ルール (50)

名前 修復アクション コンプライアンス

lambda-inside-vpc-conformance-pack-komqljuhb	設定されていません	△ 非準拠
s3-bucket-default-lock-enabled-conformance-pack-komqljuhb	設定されていません	△ 非準拠
account-part-of-organizations-conformance-pack-komqljuhb	設定されていません	○ 準拠
lambda-function-public-access-prohibited-conformance-pack-komqljuhb	設定されていません	○ 準拠
guardduty-enabled-centralized-conformance-pack-komqljuhb	設定されていません	○ 準拠
elasticsearch-encrypted-at-rest-conformance-pack-komqljuhb	設定されていません	△ 非準拠
s3-bucket-public-write-prohibited-conformance-pack-komqljuhb	設定されていません	○ 準拠
elasticsearch-node-to-node-encryption-check-conformance-pack-komqljuhb	設定されていません	△ 非準拠
vpc-sg-open-only-to-authorized-ports-conformance-pack-komqljuhb	設定されていません	△ 非準拠

vpc-sg-open-only-to-authorized-ports-conformance-pack-komqljuhb アクション ▾

ルールの詳細

説明 Checks whether any security groups with inbound 0.0.0.0/0 have TCP or UDP ports accessible. The rule is NON_COMPLIANT when a security group with inbound 0.0.0.0/0 has a port accessible which is not specified in the rule parameters.

トリガータイプ オーバーサイジングの設定変更
設定変更

変更範囲 リソース

Config ルール ARN arn:aws:config:northeast-1:27425...:22:config-rule/aws-service-rule/config-conforms.amazonaws.com/config-rule-dfsyre

リソースタイプ EC2 SecurityGroup

パラメータ

キー	タイプ	値	説明
authorizedTcpPorts	String	443	Comma-separated list of TCP ports authorized to be open to 0.0.0.0/0. Ranges are defined by dash, for example, "443,1020-1025".
authorizedUdpPorts	String		Comma-separated list of UDP ports authorized to be open to 0.0.0.0/0. Ranges are defined by dash, for example, "500,1020-1025".

対象範囲内のリソース

非準拠	ID	タイプ	ステータス	注釈
sg-03ef42b	c1262	EC2 SecurityGroup	-	One or more TCP ports (22) are not in range of the authorized ports.
sg-06617e	337da	EC2 SecurityGroup	-	One or more TCP ports (3389) are not in range of the authorized ports.
sg-08ce092	32a1f	EC2 SecurityGroup	-	One or more TCP ports (80) are not in range of the authorized ports.

適合パック : AWS Well-Architected フレームワークセキュリティ柱の運用のベストプラクティス

各質問に関連した Config Rule がまとめられている

質問	含まれる Config Rule
SEC 1. ワークロードを安全に運用するには、どうすればよいですか?	account-part-of-organizations, codebuild-project-envvar-awscred-check, iam-root-access-key-check, root-account-hardware-mfa-enabled, root-account-mfa-enabled,
SEC 2. ユーザー ID とマシン ID はどのように管理したらよいでしょうか?	access-keys-rotated, emr-kerberos-enabled, iam-password-policy, iam-user-group-membership-check, iam-user-mfa-enabled, iam-root-access-key-check, root-account-hardware-mfa-enabled, root-account-mfa-enabled, iam-user-unused-credentials-check, mfa-enabled-for-iam-console-access, secretsmanager-rotation-enabled-check, secretsmanager-scheduled-rotation-success-check,
SEC 3. 人とマシンのアクセス許可はどのように管理すればよいでしょうか?	elb-deletion-protection-enabled, emr-kerberos-enabled, iam-group-has-users-check, iam-no-inline-policy-check, iam-policy-no-statements-with-admin-access, iam-user-no-policies-check, rds-instance-deletion-protection-enabled,
SEC 4. セキュリティイベントをどのように検出し、調査していますか?	api-gw-execution-logging-enabled, cloud-trail-cloud-watch-logs-enabled, cloudtrail-enabled cloud-trail-encryption-enabled, cloud-trail-log-file-validation-enabled, cloudtrail-s3-dataevents-enabled, cloudtrail-security-trail-enabled, cloudwatch-alarm-action-check, cw-loggroup-retention-period-check, elb-logging-enabled, guardduty-enabled-centralized, multi-region-cloudtrail-enabled, rds-logging-enabled, redshift-cluster-configuration-check, s3-bucket-logging-enabled, securityhub-enabled, vpc-flow-logs-enabled, wafv2-logging-enabled
SEC 5. ネットワークリソースをどのように保護しますか?	alb-waf-enabled, dms-replication-not-public, ebs-snapshot-public-restorable-check, ec2-instance-no-public-ip, ec2-security-group-attached-to-eni, elasticsearch-in-vpc-only, emr-master-no-public-ip, restricted-ssh, ec2-instances-in-vpc, internet-gateway-authorized-vpc-only, lambda-function-public-access-prohibited, lambda-inside-vpc, rds-instance-public-access-check, rds-snapshots-public-prohibited, redshift-cluster-public-access-check, restricted-common-ports, s3-account-level-public-access-blocks, sagemaker-notebook-no-direct-internet-access, vpc-default-security-group-closed, vpc-sg-open-only-to-authorized-ports

適合パック : AWS Well-Architected フレームワークセキュリティ柱の運用のベストプラクティス

質問	含まれる Config Rule
SEC 6. コンピューティングリソースをどのように保護していますか?	ec2-imdsv2-check, ec2-instance-managed-by-systems-manager, ec2-managedinstance-association-compliance-status-check, ec2-managedinstance-patch-compliance-status-check
SEC 7. どのようにデータを分類していますか?	cw-loggroup-retention-period-check, guardduty-non-archived-findings
SEC 8. 保管時のデータをどのように保護していますか?	api-gw-cache-enabled-and-encrypted, cloud-trail-encryption-enabled, cloudwatch-log-group-encrypted, cmk-backing-key-rotation-enabled, dms-replication-not-public, dynamodb-table-encrypted-kms, ebs-snapshot-public-restorable-check, ec2-ebs-encryption-by-default, ec2-instance-no-public-ip, efs-encrypted-check, elasticsearch-encrypted-at-rest, elasticsearch-in-vpc-only, emr-master-no-public-ip, encrypted-volumes, ec2-instances-in-vpc, kms-cmk-not-scheduled-for-deletion, lambda-function-public-access-prohibited, lambda-inside-vpc, rds-instance-public-access-check, rds-snapshot-encrypted, rds-snapshots-public-prohibited, rds-storage-encrypted, redshift-cluster-configuration-check, redshift-cluster-public-access-check, s3-account-level-public-access-blocks, s3-bucket-default-lock-enabled, s3-bucket-public-read-prohibited, s3-bucket-public-write-prohibited, s3-bucket-server-side-encryption-enabled, s3-bucket-versioning-enabled, s3-default-encryption-kms, sagemaker-endpoint-configuration-kms-key-configured, sagemaker-notebook-instance-kms-key-configured, sagemaker-notebook-no-direct-internet-access, sns-encrypted-kms
SEC 9. 転送時のデータをどのように保護していますか?	acm-certificate-expiration-check, ulb-http-drop-invalid-header-enabled, alb-http-to-https-redirection-check, elasticsearch-node-to-node-encryption-check, elb-acm-certificate-required, elb-tls-https-listeners-only, redshift-require-tls-ssl, s3-bucket-ssl-requests-only
SEC 10. インシデントの予測、対応、復旧はどのように行いますか?	-

存在する AWS リソース「のみ」 「自動で」評価 = 利用状況に即した準拠状況を確認

各サンプルテンプレートの詳細説明

AWS Well-Architected フレームワークセキュリティ柱の運用のベストプラクティス

PDF

コンフォーマンスパックは、マネージド型またはカスタムの AWS Config ルールと AWS Config 修復アクションを使用して、セキュリティ、運用中、またはコスト最適化ガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。コンフォーマンスパックは、サンプルテンプレートとして、特定のガバナンスまたはコンプライアンス標準への準拠を完全に保証するようには設計されていません。サービスの使用が、運用可能な法的および規制の要件を満たしているかどうかは、お客様が評価してください。

以下は、アマゾンウェブサービスの Well-Architected フレームワークセキュリティ柱と AWS マネージド Config ルール間のマッピングのサンプルです。各 Config ルールは、特定の AWS リソースに適用され、柱の設計原則の 1 つ以上に関連しています。Well-Architected フレームワークカテゴリーは、複数の Config ルールに関連している場合があります。これらのマッピングに関する詳細およびガイダンスについては、以下の表を参照してください。

このコンフォーマンスパックは、AWS Security Assurance Services LLC (AWS SAS) によって検証されました。AWS SAS は、Payment Card Industry Qualified Security Assessors (QSA)、HITRUST 認定 共通セキュリティフレームワークプロブライナー (CCSFP)、およびさまざまな業界フレームワークのガイドラインと評価を提供することを認定されたコンプライアンスプロフェッショナルのチームです。AWS SAS プロフェッショナルはこのコンフォーマンスパックを設計し、お客様が Well-Architected フレームワークセキュリティの柱設計原則のサブセットにアクセスできるようにしました。

AWS リージョン: を除く、サポートされているすべての AWS リージョン中東 (バーレーン)

コントロール ID	コントロールの説明	AWS Config ルール	ガイダンス
SEC-1	ワーカーはどのように安全に運用しますか? ワーカードを安全に運用するには、セキュリティのすべての領域に対してベストプラクティスの上書きを適用する必要があります。組織レベルとワーカードレベルで運用上の優秀性において定義した要件とプロセスを取得し、すべての領域に適用します。AWS や業界の推薦事項、脅威インテリジェンスに関する最新情報を入手して、脅威モデルとコントロール目的の進化に役立てることができます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティオペレーションをスケールすることができます。	アカウント-パート of-organizations	AWS Organizations 内の AWS アカウントの一元管理は、アカウントが準拠していることを確認するのに役立ちます。一元化されたアカウントガバナンスがないと、アカウント設定が不整合になり、リソースと機密データが公開される可能性があります。
SEC-1	ワーカーはどのように安全に運用しますか? ワーカードを安全に運用するには、セキュリティのすべての領域に対してベストプラクティスの上書きを適用する必要があります。組織レベルとワーカードレベルで運用上の優秀性において定義した要件とプロセスを取得し、すべての領域に適用します。AWS や業界の推薦事項、脅威インテリジェンスに関する最新情報を入手して、脅威モデルとコントロール目的の進化に役立てることができます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティオペレーションをスケールすることができます。	codebuild-project-envvar-awscred-check	認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY が AWS Codebuild プロジェクト環境に存在しないことを確認します。これらの変数はクリアテキストで保存しないでください。これらの変数をクリアテキストに保存すると、意図しないデータ漏えいや不正アクセスの原因になります。
SEC-1	ワーカーはどのように安全に運用しますか? ワーカードを安全に運用するには、セキュリティのすべての領域に対してベストプラクティスの上書きを適用する必要があります。組織レベルとワーカードレベルで運用上の	iam-root-access-key-check	ルートユーザーに AWS Identity and Access Management (IAM) ロールにアタッチされたアクセスキーがないことを確認することにより、システムとアセットへのアクセスを制御できます。ルートアクセスキーが削除されていることを確認します。代わりに、ロールベースの AWS アカウントを作成して使用し、最小機能の原則を組み込みます。

適合パック：カスタムテンプレート

ユーザー独自の評価内容をカスタムテンプレートとして作成可能

- GitHubからテンプレートをダウンロード
(yaml形式)

The screenshot shows a GitHub repository page for 'aws-config-rules / aws-config-conformance-packs / custom-conformance-pack.yaml'. The code listing contains several AWS CloudFormation resources, specifically AWS::Config::ConfigRule definitions, which are highlighted by a yellow box.

```
aws-config-rules / aws-config-conformance-packs / custom-conformance-pack.yaml
tysodotcom Added S3 and DynamoDB with remediation conformance... History
1 contributor
Raw Blame
46 lines (46 sloc) 1.3 KB
Parameters:
  CustomConfigRuleLambdaArn:
    Type: String
    Description: The ARN of the custom config rule lambda.
Resources:
  CustomRuleForEC2:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: "CustomRuleForEC2"
      Scope:
        ComplianceResourceTypes:
          - AWS::EC2::Volume
      Source:
        Owner: AWS
        SourceIdentifier: EC2_VOLUME_INUSE_CHECK
      InputParameters:
        deleteOnTermination: true
      Description: Disallow EBS volumes that are unattached
      Type: AWS::Config::ConfigRule
      Properties:
        ConfigRuleName: CheckForEc2VolumesInUse
        Description: Disallow launch of EC2 instance types that are unattached
        Source:
          Owner: AWS
          SourceIdentifier: EBS_OPTIMIZED_INSTANCE
        Scope:
          ComplianceResourceTypes:
            - AWS::EC2::Instance
        Type: AWS::Config::ConfigRule
        Properties:
          ConfigRuleName: CheckForEbsOptimizedInstance
          Description: Disallow launch of EC2 instance types that are unattached
          Source:
            Owner: AWS
            SourceIdentifier: EBS_OPTIMIZED_INSTANCE
          Scope:
            ComplianceResourceTypes:
              - AWS::EC2::Instance
          Type: AWS::Config::ConfigRule
          Properties:
            ConfigRuleName: CheckForEncryptedVolume
            Description: Disallow launch of EC2 instance types that are unattached
            Source:
              Owner: AWS
              SourceIdentifier: EC2_VOLUME_INUSE_CHECK
            Scope:
              ComplianceResourceTypes:
                - AWS::EC2::Volume
```

- 修正してカスタムテンプレート化

The screenshot shows a CloudFormation YAML template with three AWS::Config::ConfigRule resources. The first two resources are highlighted by a yellow box. A callout box points to these resources with the text: 'Resources 配下に Config Rule を記載' and 'CloudFormation フォーマットの Config Rules 定義'.

```
Resources:
  CheckForEbsOptimizedInstance:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: CheckForEbsOptimizedInstance
      Description: Disallow launch of EC2 instance types that are unattached
      Source:
        Owner: AWS
        SourceIdentifier: EBS_OPTIMIZED_INSTANCE
      Scope:
        ComplianceResourceTypes:
          - AWS::EC2::Instance
      Type: AWS::Config::ConfigRule
      Properties:
        ConfigRuleName: CheckForEc2VolumesInUse
        Description: Disallow EBS volumes that are unattached
        Source:
          Owner: AWS
          SourceIdentifier: EC2_VOLUME_INUSE_CHECK
        Scope:
          ComplianceResourceTypes:
            - AWS::EC2::Volume
        Type: AWS::Config::ConfigRule
        Properties:
          ConfigRuleName: CheckForEncryptedVolume
          Description: Disallow launch of EC2 instance types that are unattached
          Source:
            Owner: AWS
            SourceIdentifier: EC2_VOLUME_INUSE_CHECK
          Scope:
            ComplianceResourceTypes:
              - AWS::EC2::Volume
```

- 適合パックのデプロイ時にアップロードして利用

The screenshot shows the 'Template to Specify' step of the CloudFormation wizard. It includes sections for specifying the template source (Amazon S3 Bucket or Template File), selecting parameters, and previewing the template. A callout box points to the 'Template File' section with the text: 'テンプレートファイルをアップロード'.

テンプレートを指定

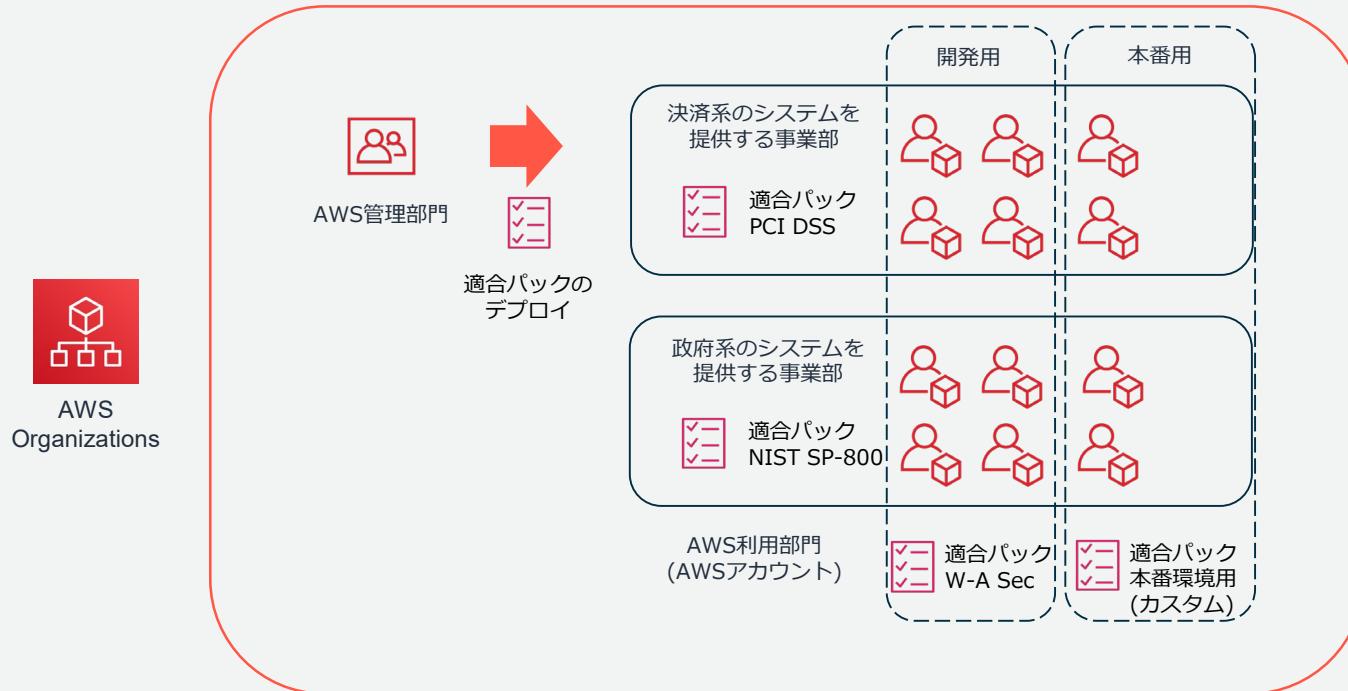
テンプレートの詳細

適合パックテンプレート

テンプレートソースを指定

テンプレートファイルをアップロード

適合パックによるアカウント特性や組織特性に応じた評価



サードパーティリソースへの対応

AWS Config が対応しているリソース



Amazon VPC



Amazon EC2



Amazon S3

Classic Load
BalancersApplication Load
BalancersAmazon EBS
volumesAWS Service
CatalogAWS Key Management
Service

AWS CloudTrail



AWS IAM



Amazon Redshift



Amazon RDS

AWS Systems
ManagerAWS Certificate
ManagerAmazon API
GatewayAmazon Simple
Notification ServiceAmazon CloudWatch
alarmsAWS CloudFormation
stacksAmazon DynamoDB
tablesAWS Auto Scaling
groups

AWS CodeBuild



AWS CodePipeline

Amazon Quantum
Ledger DatabaseAmazon Simple
Queue Service

AWS WAF *1



Amazon CloudFront *1

AWS Elastic
Beanstalk

AWS Lambda



AWS X-Ray



AWS Shield *1

Amazon Elasticsearch
Service3rd Party
Resources

*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

サードパーティリソース例： WordPress の構成情報を Config で管理

AWS Config

- ダッシュボード
- 適合パック
- ルール
- リソース**
- ▼ アグリゲータ
 - ルール
 - リソース
 - 認証
 - 高度なクエリ
 - 設定
- 最新情報
- ドキュメント
- パートナー
- よくある質問
- 料金表

AWS Config > リソース

リソースのインベントリ

AWS Config が記録した既存または削除されたリソースを検索します。特定のリソースについては、リソースの詳細と設定タイムライン、またはコンプライアンスマイルを確認してください。リソース設定タイムラインを使用すると、特定のリソースについて長期間にわたってキャプチャされたすべての設定項目を表示できます。リソースコンプライアンスマイルを使用すると、コンプライアンスステータスの変更を確認できます。リソース設定をクエリするには、次を使用します [高度な SQL クエリエディタ](#)。

リソース (85)	詳細を表示	リソースタイムライン
リソースカテゴリ	リソースタイプ	コンプライアンス
すべてのリソース	すべてのリソースタイプ	コンプライアンスのステータス
リソース識別子 - オプション	<input type="checkbox"/> 削除されたリソースを含める	
<input type="text"/> リソース識別子を入力		
< 1 2 3 ... > ①		
リソース識別子	タイプ	コンプライアンス
mywordpress-01	Testing WordPress	-
resource-001	Testing WordPress	-
i-03b7...7bcd	EC2 Instance	-
arn:aws:acm:ap-northeast-1:...	ACM Certificate	-
subnet-0f...17	EC2 Subnet	-

サードパーティリソースの設定や履歴を Config で管理

AWS Config > リソース > mywordpress-01

mywordpress-01

▶ 詳細

▼ 設定項目 (JSON) の表示

```
{  
    "version": "1.3",  
    "accountId": "274251360022",  
    "configurationItemCaptureTime": "2020-11-23T13:37:54.624Z",  
    "configurationItemStatus": "OK",  
    "configurationItemId": "1606138674624",  
    "configurationItemMD5Hash": "",  
    "resourceType": "MyCustomNamespace::Testing::WordPress",  
    "resourceId": "mywordpress-01",  
    "awsRegion": "ap-northeast-1",  
    "tags": {},  
    "relatedEvents": [],  
    "relationships": [],  
    "configuration": {  
        "InstanceId": "i-03b67bcd",  
        "PublicIp": "3.14.57",  
        "SubnetId": "subnet-843df",  
        "Name": "MyCustomResourceWordPress"  
    },  
    "supplementaryConfiguration": {},  
    "resourceTransitionStatus": "None"  
}
```

設定の詳細情報

リソースタイムライン

設定タイムライン コンプライアンスタイムライン

23 11月 2020 10:16:17 午後

23 11月 2020 10:37:54 午後 3 変更

▶ 構成の詳細

設定タイムラインで、設定状態の履歴も確認可能

▼ 変更 3

設定変更 3

フィールド	開始	終了
Configuration.SubnetId	"subnet-ala1a"	"subnet-83df"
Configuration.PublicIp		"3.14.57"
Configuration.InstanceId		"i-03b79daf67bcd"

仕組み：CloudFormation リソースプロバイダ

CloudFormation レジストリにサードパーティリソースのスキーマを登録
(スキーマをJSON定義して、cloudformation-cli で submit)

The screenshot shows the AWS CloudFormation console interface. On the left, the navigation pane includes 'CloudFormation' (selected), 'Stacks', 'StackSets', 'Exports', 'Designer', and 'CloudFormation レジストリ' (expanded) with 'Resource Types' selected. At the bottom left is a 'Feedback' link. The main content area shows the 'Resource Types' page under 'CloudFormation レジストリ: リソースタイプ'. A specific resource type, 'MyCustomNamespace::Testing::WordPress', is highlighted with an orange border and an orange arrow points from its definition in the JSON schema on the right to its listing in the console.

CloudFormation > CloudFormation レジストリ: リソースタイプ

リソースタイプ

AWS が新しくなりました。新しい協力会社も登場。お客様の組織向け(リソースを含む)もスタックテンプレートで利用可能になりました。 詳細

リソースタイプ (1)

プライベート ▾

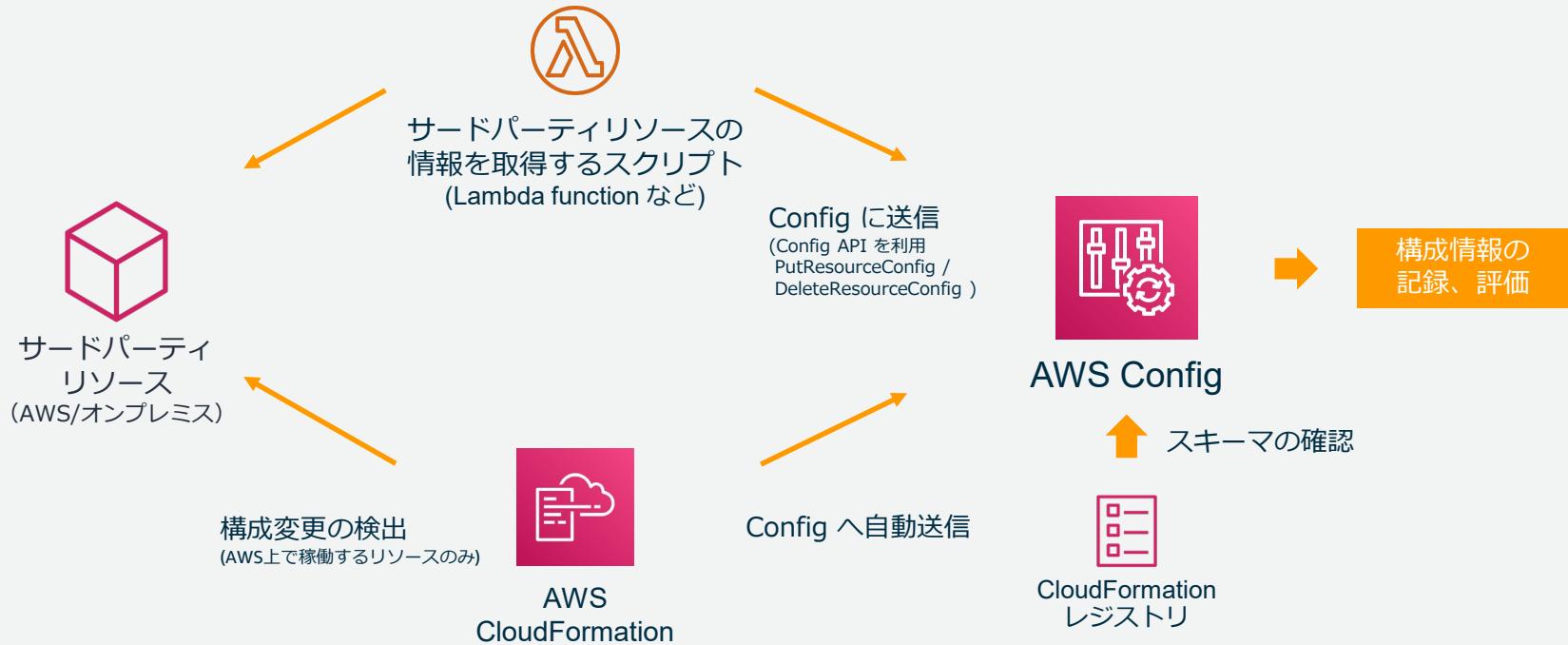
MyCustomNamespace::Testing::WordPress

An example resource that creates a website based on WordPress 5.2.2.

スキーマ

```
{ "typeName": "MyCustomNamespace::Testing::WordPress", "description": "An example resource that creates a website based on WordPress 5.2.2.", "sourceUrl": "https://github.com/aws-cloudformation/aws-cloudformation-rpdk.git", "properties": { "Name": { "description": "A name associated with the website.", "type": "string", "pattern": "^[a-zA-Z0-9]{1,219}\\Z", "minLength": 1, "maxLength": 219 }, "SubnetId": { "description": "A subnet in which to host the website.", "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z", "type": "string" }, "InstanceId": { "description": "The ID of the instance that backs the WordPress site.", "type": "string" }, "PublicIp": { "description": "The public IP for the WordPress site.", "type": "string" } }, "required": [ "Name", "SubnetId" ], "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ], "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ], "additionalProperties": false }
```

サードパーティリソースの構成情報の流れ



ご参考：
CloudFormation レジストリ、リソースプロバイダの詳細情報

[AWS Black Belt Online Seminar] AWS CloudFormation deep dive 資料及び QA 公開

<https://aws.amazon.com/jp/blogs/news/webinar-bb-aws-cloudformation-deep-dive-2020/>

aws

ブログホーム カテゴリ ▾ エディション ▾ Search Blogs

Amazon Web Services ブログ

[AWS Black Belt Online Seminar] AWS CloudFormation deep dive 資料及び QA 公開

by AWS Japan Staff | on 13 OCT 2020 | in AWS CloudFormation, Webinars | Permalink | Share

先日(2020/10/06)開催しました AWS Black Belt Online Seminar 「AWS CloudFormation deep dive」の資料を公開しました。当日、参加者の皆様から頂いた QA の一部についても共有しております。

The thumbnail image shows the AWS logo and the title '[AWS Black Belt Online Seminar] AWS CloudFormation deep dive'. Below the title is the subtitle 'サービスカットシリーズ'. The background has a dark teal geometric pattern.

Senior Solutions Architect
大村 幸敏
2020/10/06

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

過去資料
<https://amzn.to/JPArchive>

aws

CloudFormationレジストリ

- 独自に作成したCfnリソース定義を登録する
 - 3rd PartyリソースがCfnで管理できる
 - パブリック（AWSのネイティブ）リソースも移行中
 - 既存のテンプレートやタスクは変更不要
 - 現在519（東京リージョン）
- リソースプロバイダスキーマ
 - リソースの設計書に相当するスキーマ
 - 設定可能なプロパティなどを定義する
 - マネジメント
- CFnレジストリ
 - Drift Detector
 - Resource
 - AWS Config

リソースプロバイダ実装の流れ

実装の流れ

1. スキーマを定義する
2. ハンドラを実装する
3. ビルドする
4. テストする
5. レジストリに登録する
6. CFnで利用する

Pythonによる実装例 1

- 事前準備
 - Cloud9環境(Ubuntu)
 - Python 3.7 (RPD版と合わせる)
 - AWS CLI
 - AWS SAM CLI
- コード、CFn CLIとプラグイン
 - unicorn-makerのclone
 - venvの設定
 - cloudformation-cli*の導入
(バージョン整合注意)

```
$ sudo apt install python3
$ sudo update-alternatives --install /usr/bin/python python /usr/bin/python3.7 0
$ sudo update-alternatives --config python - (3:7を選択)
$ python --version
python 3.7.3
$ sudo apt install python3.7-venv
$ brew upgrade aws-sam-cl
$ sam --version
SAM CLI 1.18.149
$ aws --version
awscli 1.18.149 Python/3.6.9 Linux/5.4.0-182-aws botocore/1.18.8

$ git clone https://github.com/kuromukarni21/unicorn-maker.git
$ cd unicorn-maker/python
$ curl https://raw.githubusercontent.com/kuromukarni21/unicorn-maker/main/.venv/bin/activate
$ pip install --upgrade pip
$ pip install cloudformation-cli-python-plugin
$ vi requirements.txt - (cloudformation-cli-python-libのバージョンを2.1.2へ)
$ pip install -r requirements.txt
$ cd ..
$ pip install -r requirements.txt
$ cfn --version
cfn 0.1.1
$ pip list | grep form
cloudformation-cli                0.1.11
cloudformation-cli-python-lib      2.1.2
cloudformation-cli-python-plugin   2.1.1
```

その他のアップデート

組織のセキュリティ管理をより効率化する機能拡張

アドバンスドクエリ： マルチアカウント、マルチリージョンの検索に対応

AWS Config > 高度なクエリ > クエリエディタ

クエリエディタ

次の SQL クエリエディタを使用して、AWS リソースの設定を照会します。プロパティとそのデータ型のリストは [GitHub](#) にあります。クエリスコープを選択して、この AWS アカウントまたは複数のアカウントとリージョンに対してデータをクエリします。 詳細はこちら ↗

クエリスコープ	Count EC2 Instances
アグリゲータを選択して、このアカウントとリージョン、または複数のアカウントとリージョンに対してクエリを実行するクエリ範囲を定義します。 skorg-config-aggregator ▲ このアカウントとリージョンのみ skorg-config-aggregator	クエリスコープ: skorg-config-aggregator 1 SELECT 2 configuration.instanceType, 3 COUNT(*) 4 WHERE 5 resourceType = 'AWS::EC2::Instance' 6 GROUP BY 7 configuration.instanceType 実行 クリア 実行 (Ctrl+Enter)

出力

configuration.instanceType	COUNT(*)
t2.micro	3
t3.small	2
c4.xlarge	1
c5.2xlarge	1
c5.large	

名前を付けてエクスポート ▾

複数のアカウント、リージョンを横ぐしで検索して状況を確認

AWS Organizations 連携 :

AWS Organizations で委任管理者のサポートと
Config Rule/ 適合パックの一括配布



評価結果をまとめて確認



```
$aws organizations enable-aws-service-access --service-principal=config-multiaccountsetup.amazonaws.com
```

```
$aws configservice put-organization-config-rule ¥
--organization-config-rule-name my-cloudtrail-enabled ¥
--organization-managed-rule-metadata ¥
(snip) RuleIdentifier="CLOUD_TRAIL_ENABLED"
```

```
$aws configservice put-organization-conformance-pack ¥
--organization-conformance-pack-name="CISPack" ¥
--template-body="file://CISConformancePack.yaml" ¥
--delivery-s3-bucket="{awsconfigconforms-your-bucket}"
```

集約ビュー > ルール

ルール

ルールは、必要な構成設定を表します。AWS Config は、リソース設定が該当するルールに準拠しているかどうかを評価し、結果の概要を次のテ

アグリゲータ	コンプライアンス状況	リージョン	アカウント
skorg-config-aggregator	すべて	すべてのリージョン	すべてのアカウント
ルール名	コンプライアンス	リージョン	アカウント
OrgConfigRule-org-cloudtrail-en...	1 非準拠リソース	ap-northeast-1	27-022
OrgConfigRule-org-s3-bucket-s...	4 非準拠リソース	ap-northeast-1	27-022

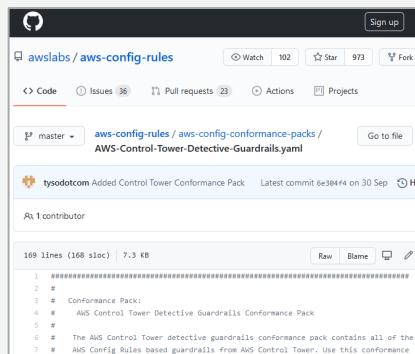
マルチアカウント環境へのガードレールの適用

適合パック : AWS Control Tower Detective Guardrails

- AWS Control Tower のガードレールに含まれる、Config Rule のパッケージ

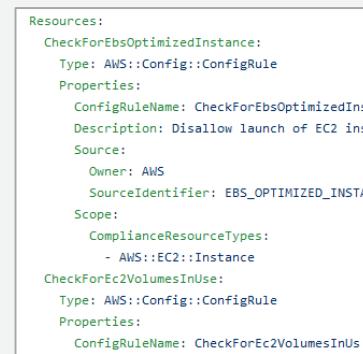
- AWS Control Tower の機能を切り出して利用
 - Control Tower の発見的ガードレールを既存 AWS アカウントに適用
 - Control Tower がサポートしていない AWS リージョンのセキュリティ統制
 - 組織のセキュリティポリシーに沿って、ガードレールをカスタマイズして利用

1. GitHubからテンプレートをダウンロード



```
awslabs / aws-config-rules
Issues 36 Pull requests 23 Actions Projects
master → aws-config-rules / aws-config-conformance-packs / AWS-Control-Tower-Detective-Guardrails.yaml
tysdotcom Added Control Tower Conformance Pack · Latest commit 6e304f4 on 30 Sep · History
1 contributor
169 lines (168 sloc) 7.3 KB Raw Blame
1 #####
2 #
3 # Conformance Pack
4 # AWS Control Tower Detective Guardrails Conformance Pack
5 #
6 # The AWS Control Tower detective guardrails conformance pack contains all of the
7 # AWS Config Rules based guardrails from AWS Control Tower. Use this conformance
```

2. 修正してカスタムテンプレート化



```
Resources:
  CheckForEbsOptimizedInstance:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: CheckForEbsOptimizedInst
      Description: Disallow launch of EC2 inst
      Source:
        Owner: AWS
        SourceIdentifier: EBS_OPTIMIZED_INST
      Scope:
        ComplianceResourceTypes:
          - AWS::EC2::Instance
  CheckForEc2VolumesInUse:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: CheckForEc2VolumesInUs
```

3. 組織にセキュリティポリシーに沿った評価

名前	修復アクション	コンプライアンス
CheckForEc2VolumesInUs-conformance-pack-bty6nzqs2	設定されていません	準拠
CheckForS3VersioningEnabled-conformance-pack-bty6nzqs2	設定されていません	非準拠
CheckForRootMfa-conformance-pack-bty6nzqs2	設定されていません	非準拠
CheckForRestrictedSshPolicy-conformance-pack-bty6nzqs2	設定されていません	非準拠
CheckForRdsStorageEncryption-conformance-pack-bty6nzqs2	設定されていません	準拠
CheckForRestrictedCommonPortsPolicy-conformance-pack-bty6nzqs2	設定されていません	非準拠
CheckForEncryptedVolumes-conformance-pack-bty6nzqs2	設定されていません	非準拠
CheckForRdsPublicAccess-conformance-pack-bty6nzqs2	設定されていません	準拠
CheckForS3PublicWrite-conformance-pack-bty6nzqs2	設定されていません	準拠
CheckForS3PublicRead-conformance-pack-bty6nzqs2	設定されていません	準拠

Landing Zone の手動適用がより簡単に

適合パック : AWS Control Tower Detective Guardrails

推奨/選択的	Config Rule	内容
強く推奨	ebs-optimized-instance	Amazon EBS 最適化以外のタイプの Amazon EC2 インスタンスを禁止
強く推奨	ec2-volume-inuse-check	Amazon EC2 インスタンスにアタッチされていない Amazon EBS ボリュームを禁止
強く推奨	encrypted-volumes	Amazon EC2 インスタンスにアタッチされた Amazon EBS ボリュームの暗号化を有効
強く推奨	rds-instance-public-access-check	Amazon RDS データベースインスタンスへのパブリックアクセスを禁止
強く推奨	rds-snapshots-public-prohibited	Amazon RDS データベーススナップショットへのパブリックアクセスを禁止
強く推奨	rds-storage-encrypted	ストレージが暗号化されていない Amazon RDS データベースインスタンスを禁止
強く推奨	restricted-common-ports	RDP を介したインターネット接続を禁止
強く推奨	restricted-ssh	SSH を介したインターネット接続を禁止
強く推奨	root-account-mfa-enabled	root ユーザーに対して MFA を有効
強く推奨	s3-bucket-public-read-prohibited	Amazon S3 バケットへのパブリック読み取りアクセスを禁止
強く推奨	s3-bucket-public-write-prohibited	Amazon S3 バケットへのパブリック書き込みアクセスを禁止
選択的	s3-bucket-versioning-enabled	バージョニングが有効になっていない Amazon S3 バケットを禁止
選択的	iam-user-mfa-enabled	MFA なしの IAM ユーザーへのアクセスを禁止
選択的	mfa-enabled-for-iam-console-access	MFA なしの IAM ユーザーへのコンソールアクセスを禁止

本日のまとめ

1. AWS Config のおさらい

- AWSリソースの構成管理、評価を行うマネージドサービス
- Config でリソースの構成記録、Config Rules で構成評価

2. 新機能：適合パックの概要

- Config Rules を用途に応じてパッケージ化
- 組織のセキュリティ管理やコンプライアンス準拠がより簡単に！

3. 新機能：サードパーティリソースサポートの概要

- AWSリソース以外にも対象に (WordPressなど)

4. 組織のセキュリティ管理をより効率化するその他のアップデート

- マルチアカウント環境での展開、ルール管理、評価、レポーティング
- 組織へのガードレールの適用、カスタマイズ性の向上

**利用シーンが広がった AWS Config を有効活用して
AWS の利用をより安全・快適に！**

Q&A

ご質問については

AWS Japan Blog 「<https://aws.amazon.com/jp/blogs/news/>」にて
後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索



The screenshot shows the AWS Japan Language Resources page. At the top, there's a navigation bar with the AWS logo, search bar, and links for "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", and "コンソールにサインイン". Below the navigation is a horizontal menu with links for "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", and a search icon. The main content area features a large title "AWS クラウドサービス活用資料集トップ" and a descriptive paragraph about the service. 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 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>





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

Configuration & Secret Management入門

AWS Black Belt Online Seminar

Amazon Web Services Japan K.K.

Solutions Architect

成尾 文秀

2021-September

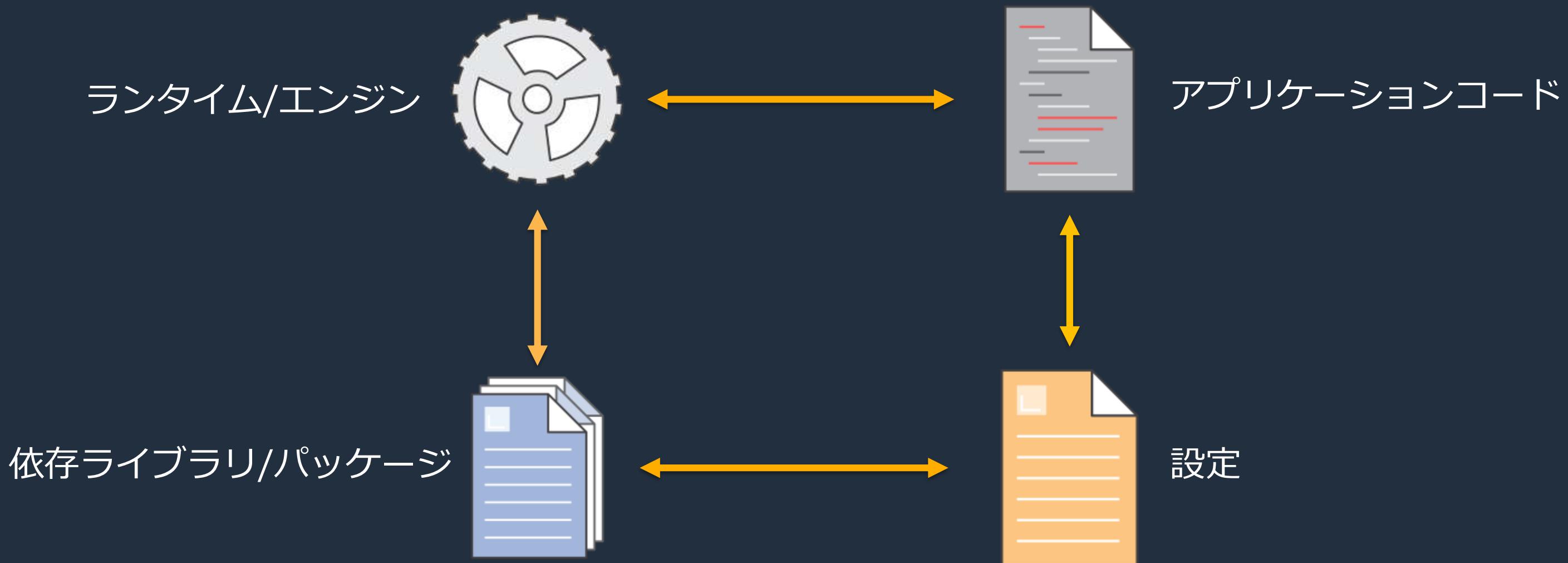


このセッションで扱うこと・学べること

- コンテナにおいてConfiguration (設定) をどのように扱うか
- AWSサービスを利用した変数の取り扱い

環境変数 – アプリケーション

- アプリケーションを構成するコンポーネント



環境変数 – 設定（アプリケーション）

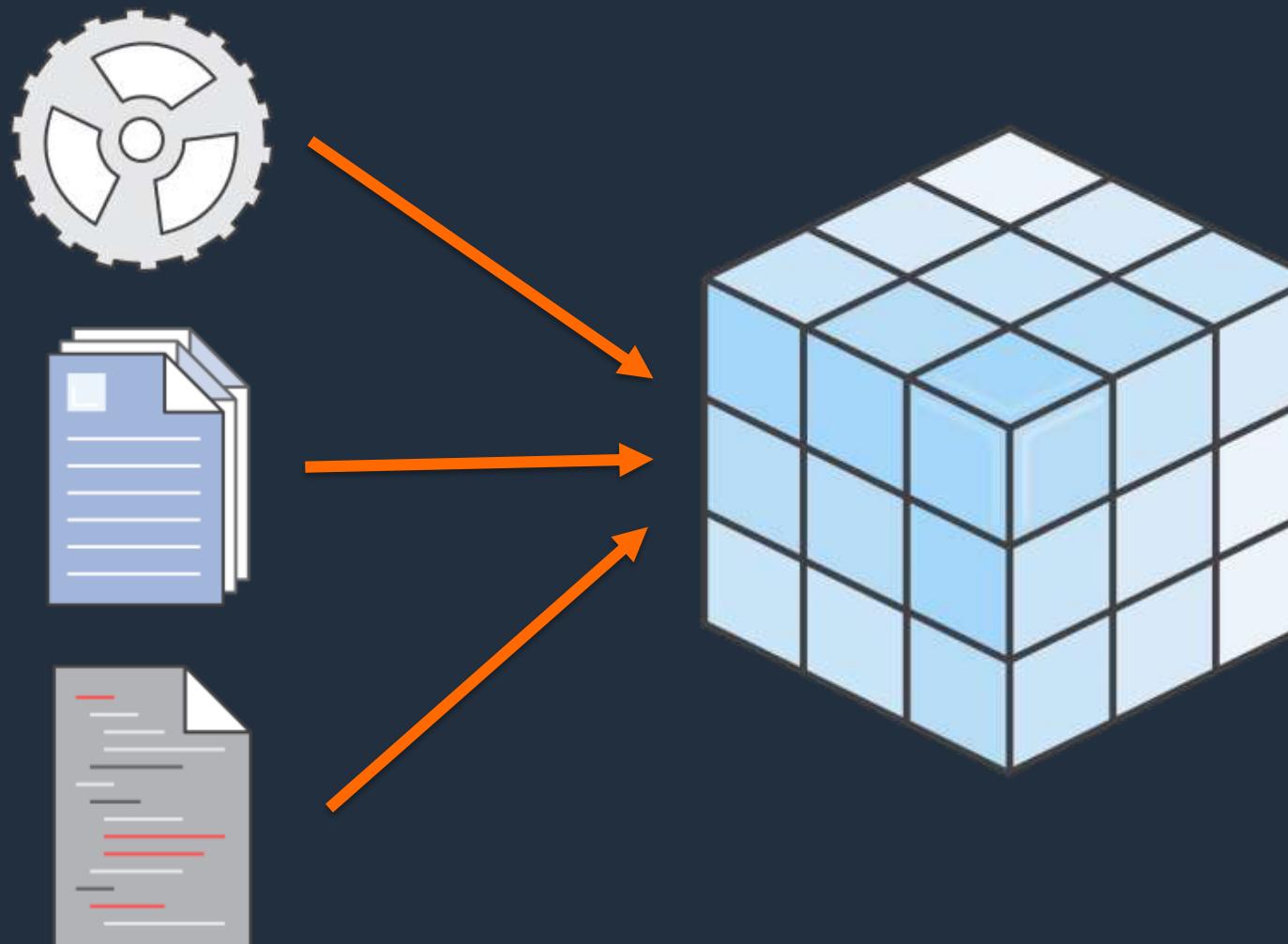
- 設定
 - アプリケーションが稼働する上で必要となる動作環境ごとに異なる情報
 - 変更頻度が高い情報
- 設定例
 - RDBの接続先
 - 外部APIのエンドポイント
 - デバッグフラグ
 - 同時処理数、タイムアウト秒数
- 設定をソースコードに含めた場合の影響
 - 変更の都度ビルド、テスト、デプロイ必要
 - ソースコード、コンテナイメージの流出といったセキュリティリスク



環境変数 - コンテナ

- コンテナ

ランタイム/エンジン
依存ライブラリ/パッケージ
アプリケーションコード



環境変数 – 設定（コンテナ）

- コンテナにおける設定
 - 環境変数として外部から渡す
- 読み込み例
 - 起動時にまとめて取得
 - アプリケーションから必要な時に都度取得
- AWSサービス
 - AWS Systems Manager - Parameter Store
 - AWS Secrets Manager
 - Amazon S3

環境変数 – Parameter Store

- Amazon ECSでのParameter Store利用方法
 - タスク定義内のコンテナ定義 (containerDefinitions) の secrets で指定

```
"secrets": [{}  
  "name": "environment_variable_name",  
  "valueFrom": "arn:aws:ssm:region:aws_account_id:parameter/parameter_name"  
}]
```

- タスク定義内のログ設定 (logConfiguration) の secretOptions で指定

```
"secretOptions": [{}  
  "name": "fluentd-address",  
  "valueFrom": "arn:aws:ssm:region:aws_account_id:parameter:parameter_name"  
}]
```

- 注意点
 - タスク起動時に環境変数として読み込む、更新した値を読む時は新しいタスクを起動
 - 大量取得がある際はスループットに注意（デフォルト：40 TPS、上限：1,000 TPS）

環境変数 – Secrets Manager

- Amazon ECSでのSecrets Manager利用方法
 - タスク定義内のコンテナ定義 (containerDefinitions) の secrets で指定
 - タスク定義内のログ設定 (logConfiguration) の secretOptions で指定
 - 特定の JSON キーなど柔軟な指定が可能 (EC2 or Fargate PV 1.40以降)

```
arn:aws:secretsmanager:region:aws_account_id:secret:secret-name:json-key:version-stage:version-id
```

- json-key : 指定すると特定のKeyのみ取得、指定がないとシークレットの内容全体を取得
- version-stage : AWSCURRENT (現在の値) AWSVIOUS (1つ前の値) を指定し取得
- version-id : 自動付与されるバージョンIDを指定して特定のデータを取得

- 注意点
 - タスク起動時に環境変数として読み込む、更新した値を読む時は新しいタスクを起動
 - 大量取得がある際は秒間取得上限に注意 (GetSecretValue : 5,000 per second 固定)

環境変数 – Amazon S3

- Amazon ECSでのAmazon S3ファイルからの利用方法 (EC2 起動タイプのみ)
 - タスク定義内の environment で個別にパラメータをセット
 - タスク定義内の environmentFiles の secrets で **S3** を指定可能 (EC2 or Fargate PV 1.40以降)

```
"environmentFiles": [  
    {  
        "value": "arn:aws:s3:::s3_bucket_name/envfile_object_name.env",  
        "type": "s3"  
    }  
]
```

- 注意点
 - タスク起動時に環境変数として読み込む、更新した値を読む時は新しいタスクを起動
 - タスク定義ごとに最大 10 個のファイルが指定可能

環境変数 – Secrets Manager & Parameter Store

- Amazon EKSでのSecrets Manager利用方法

- AWS Secrets and Configuration Provider (ASCP) for Kubernetes Secrets Store CSI Driver
 - 指定のmountPathにシークレットを取得して配置
 - Kubernetes Secretと同期

```
volumeMounts:  
- name: mysecret2  
  mountPath: "/mnt/secrets-store"  
  readOnly: true  
volumes:  
- name: mysecret2  
  csi:  
    driver: secrets-store.csi.k8s.io  
    readOnly: true  
    volumeAttributes:  
      secretProviderClass: "aws-secrets"
```

```
apiVersion: secrets-store.csi.x-k8s.io/v1alpha1  
kind: SecretProviderClass  
metadata:  
  name: aws-secrets  
spec:  
  provider: aws  
  secretObjects:  
  - data:  
    - key: username  
      objectName: ACSPEKSSecrets  
      secretName: ACSPEKSSecret  
      type: Opaque  
  parameters:  
    objects: |  
      array:  
      - |  
        objectName: "arn:aws:ssm:us-east-1:[ACCOUNT]:parameter/MyConfigValue"  
        objectVersion: "1"# [オプション] オブジェクトバージョン、空の場合は最新がデフォルト  
      - |  
        objectName: "arn:aws:secretsmanager:us-east-1:[ACCOUNT]:secret:MySecret-00AABB"  
        objectVersion: "00112233AABB00112233445566778899"  
      - |  
        objectName: "MyConfigValue2"  
        objectType: "ssmparparameter"# オブジェクトタイプ、シークレットには secretsmanager、コン  
        objectVersion: "1"  
      - |  
        objectName: "MySecret2"  
        objectType: "secretsmanager"  
        objectVersion: "00112233AABB00112233445566778899"
```

このセッションで扱ったこと

- コンテナにおいてConfiguration (設定) をどのように扱うか
- AWSサービスを利用した変数の取り扱い

Link

- Systems Manager パラメータストアを使用した機密データの指定 - Amazon ECS
https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/userguide/specifying-sensitive-data-parameters.html
- Parameter Store のスループットを引き上げる - AWS Systems Manager
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/parameter-store-throughput.html
- Secrets Manager を使用した機密データの指定 - Amazon Elastic Container Service
https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/developerguide/specifying-sensitive-data-secrets.html
- AWS Secrets Manager のクオータ - AWS Secrets Manager
https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/reference_limits.html
- 環境変数の指定 - Amazon Elastic Container Service
https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/developerguide/taskdef-envfiles.html
- Using Secrets Manager secrets in Amazon Elastic Kubernetes Service
https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/integrating_csi_driver.html
- AWS Secrets & Configuration Provider を Kubernetes Secrets Store CSI Driver で使用する方法 | Amazon Web Services ブログ
<https://aws.amazon.com/jp/blogs/news/how-to-use-aws-secrets-configuration-provider-with-kubernetes-secrets-store-csi-driver/>

本セッションの担当： 成尾 文秀

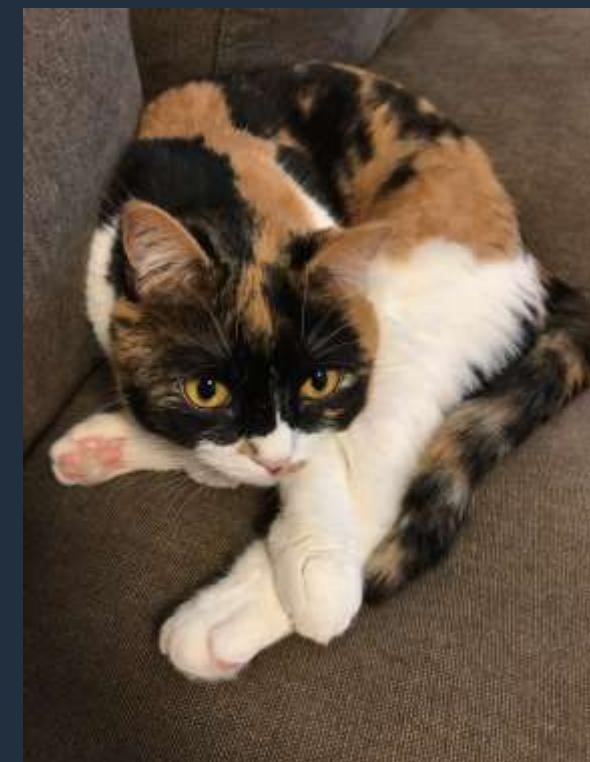
- 所属：
アマゾン ウェブ サービスジャパン株式会社
ソリューションアーキテクト



- 好きなAWSサービス：
 - Amazon ECS, Amazon EKS, Amazon S3



- 趣味：
 - ねこ、旅行



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け、Amazon Web Services 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。

- AWSの技術担当者が、AWSの各サービスについてテーマごとに動画を公開します
- お好きな時間、お好きな場所でご受講いただけるオンデマンド形式です
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます

内容についての注意点

- 本資料では2021年6月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には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.

本資料に関するお問い合わせ・ご感想

- 技術的な内容に関しては、有料のAWSサポート窓口へお問い合わせください
- <https://aws.amazon.com/jp/premiumsupport/>
- 料金面でのお問い合わせに関しては、カスタマーサポート窓口へお問い合わせください（マネジメントコンソールへのログインが必要です）
- <https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>
- 具体的な案件に対する構成相談は、後述する個別技術相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

AWS の日本語資料の場所「AWS 資料」で検索



The screenshot shows the AWS Japan Language Resources page. At the top, there's a navigation bar with the AWS logo, search bar, and links for Contact, Support, Japanese, Account, and Sign Up. Below the navigation is a main heading 'AWS クラウドサービス活用資料集トップ' (Top of the AWS Cloud Service Utilization Document Collection). A descriptive paragraph explains that AWS is a secure cloud services platform supporting business scale and growth with various services like databases and storage. Below the paragraph are four buttons: 'AWS Webinar お申込 »' (Apply for AWS Webinar), 'AWS 初心者向け »' (For AWS beginners), 'サービス別資料 »' (Service-specific documents), and 'ハンズオン資料 »' (Hands-on documents).

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 »](#) [サービス別資料 »](#) [ハンズオン資料 »](#)

<https://amzn.to/JPArchive>

AWS のハンズオン資料の場所 「AWS ハンズオン」で検索

The screenshot shows the AWS Hands-on landing page. At the top, there's a navigation bar with links for 'お問い合わせ' (Contact), 'サポート' (Support), '日本語' (Japanese), 'アカウント' (Account), and a prominent orange button '今すぐ無料サインアップ' (Sign up now). Below the navigation is a search bar and a menu with links like '製品' (Products), 'ソリューション' (Solutions), '料金' (Pricing), 'ドキュメント' (Documentation), '学ぶ' (Learn), 'パートナーネットワーク' (Partnership Network), 'AWS Marketplace', 'イベント' (Events), and 'さらに詳しく見る' (View more details) with a magnifying glass icon.

AWS ハンズオン資料

AWS をステップバイステップでお試しいただくのに役立つ動画および資料を掲載しています。

その他の資料は以下をご覧ください。

[初心者向けの資料 »](#)

[サービス別の資料 »](#)

[AWS オンラインセミナースケジュール »](#)

[AWS クラウドサービス活用資料集トップ »](#)

AWS 初心者向けハンズオン

AWS 初心者向けに「AWS Hands-on for Beginners」と題し、初めて AWS を利用する方や、初めて対象のサービスを触る方向けに、操作手順の解説動画を見ながら自分のペースで進められるハンズオンをテーマごとにご用意しています。

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に
対策などを相談することも可能

- 申込みはイベント告知サイトから

(<https://aws.amazon.com/jp/about-aws/events/>)

AWS イベント で[検索]



ご視聴ありがとうございました