[AWS Black Belt Online Seminar]
AWS Config Update

サービスカットシリーズ

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

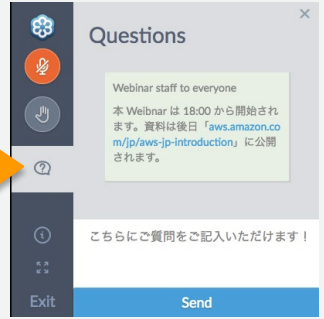
AWS Black Belt Online Seminar とは

「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、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.

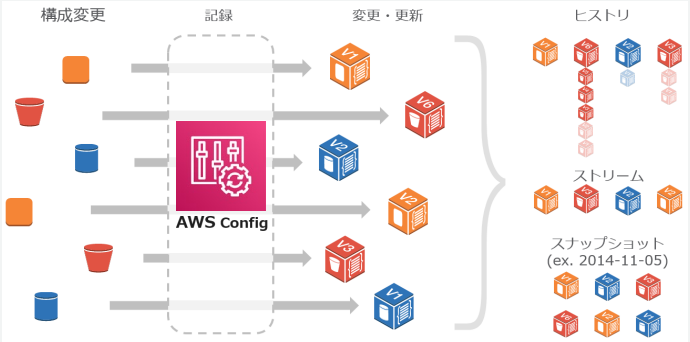
本日のアジェンダ

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

AWS Config

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/)

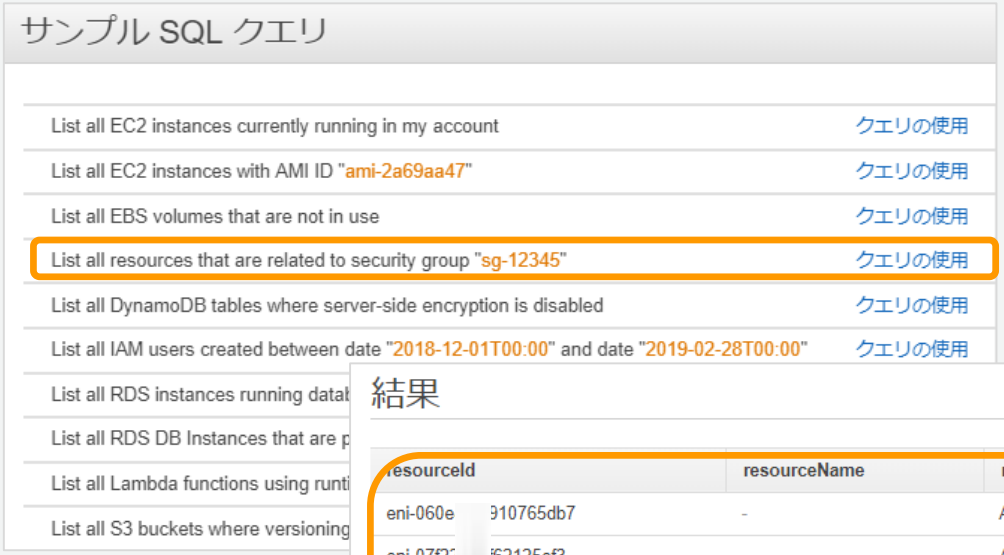
- AWS リソースの構成情報、変更履歴を記録
  - 構成情報を定期的にスナップショットとして保存
  - 必要に応じ SNS を使った通知も可能
- 構成情報を元に、現在のシステムがあるべき状態になっているか評価できる（Config Rules）

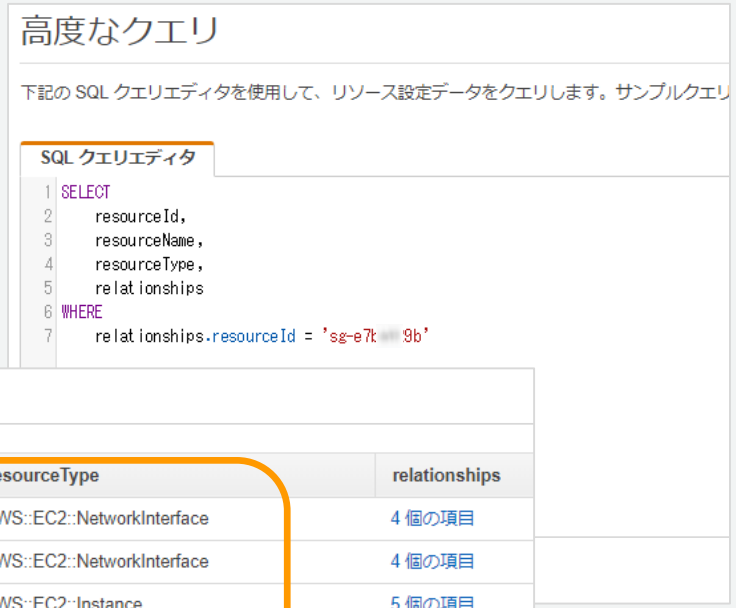
価格体系 (http://aws.amazon.com/jp/config/pricing/)

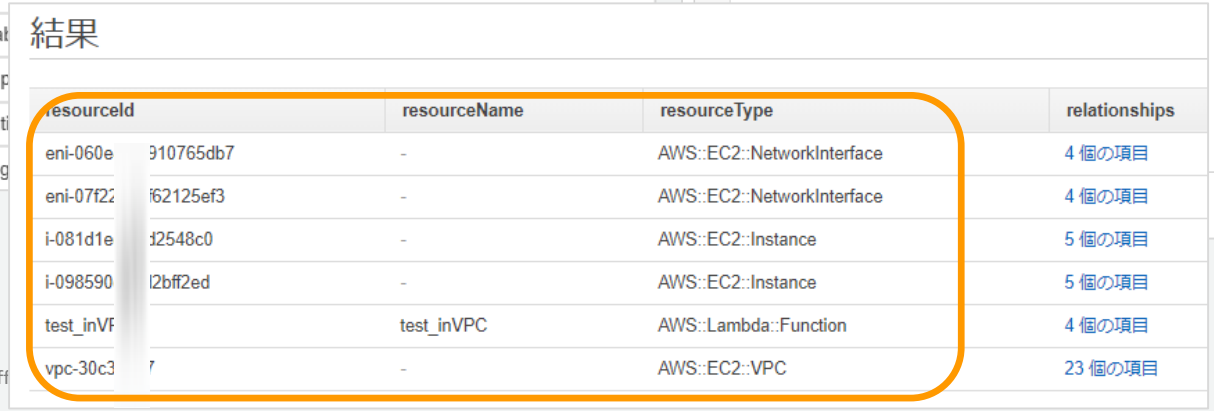
- 1 回の設定項目の記録につき 0.003 USD
- Config Rules ルール評価ごとに 0.001USD
- ログが保存される Amazon S3 の料金

AWS Config の利用例

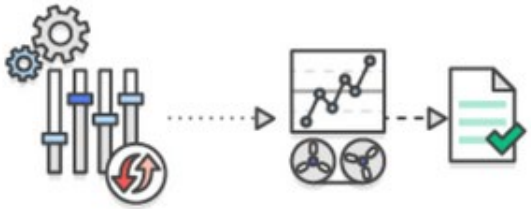
特定のセキュリティグループを利用しているリソースを検索
（ SSH/RDPがフルオープンのSGが発見された！ 影響は？）







AWS Config による構成管理



AWSリソースの
構成変更

AWS Config
による取得

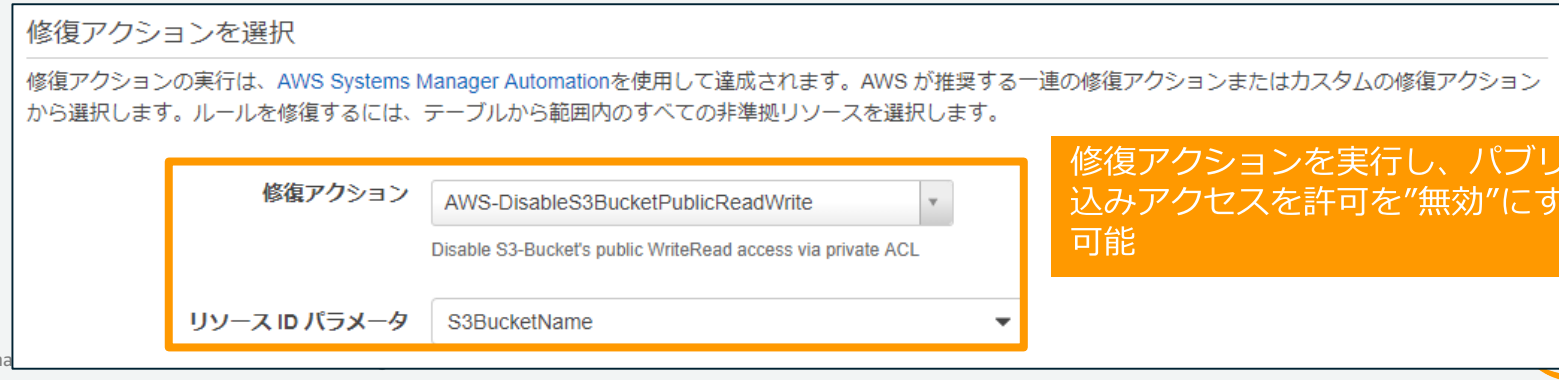
構成管理/記録の保存
過去の構成状況
依存関係の確認
コンプライアンス準拠

AWS Config Rules の利用例

パブリック読込みが許可されたS3バケットを把握

AWSが提供するマネー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

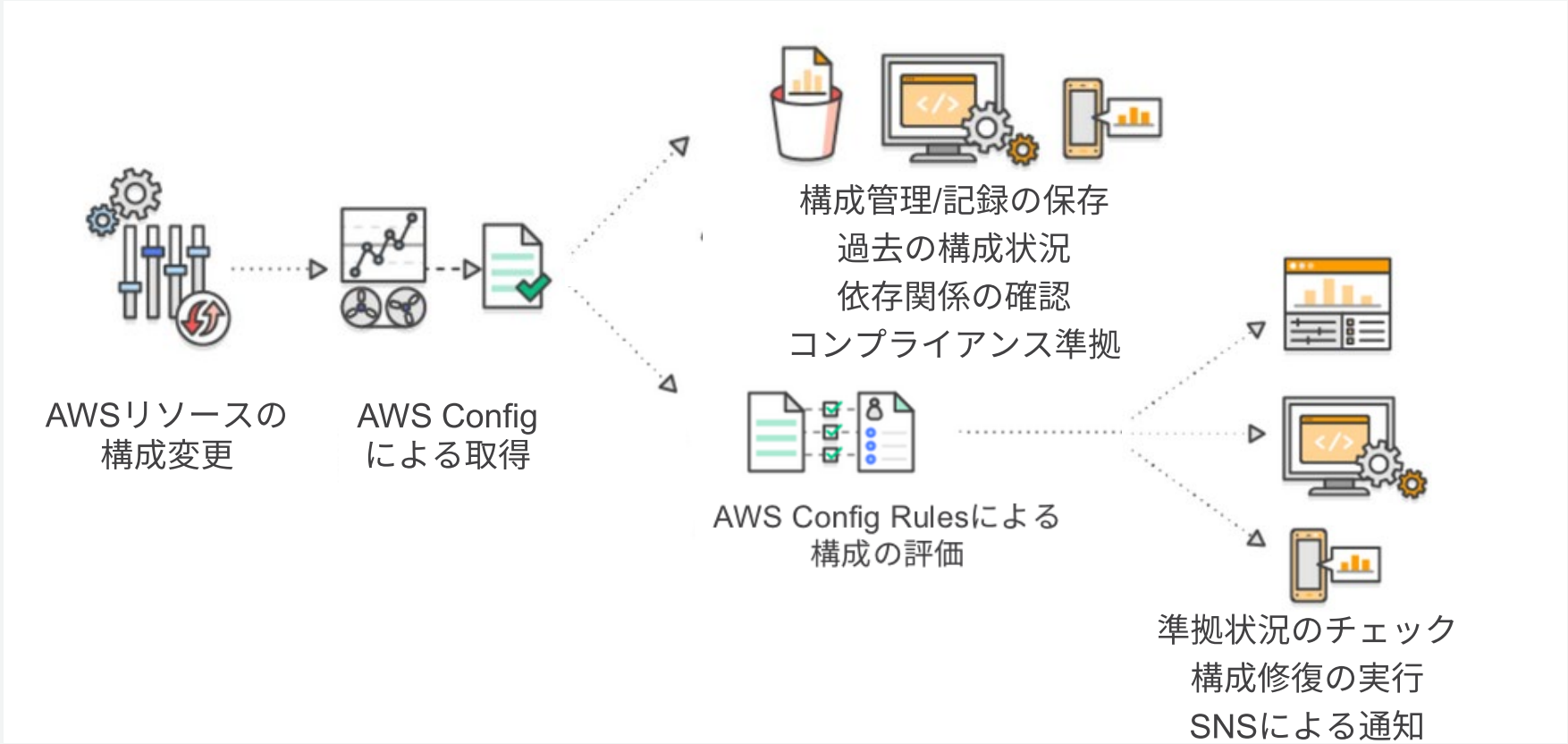
必要があれば修復アクションで1click/自動で対応



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

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

AWS Config Rules で構成情報を評価



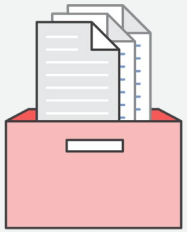
基本的な機能については、前回の BlackBelt をご確認ください

[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/

新機能のご紹介

AWS Config のアップデート

適合パック

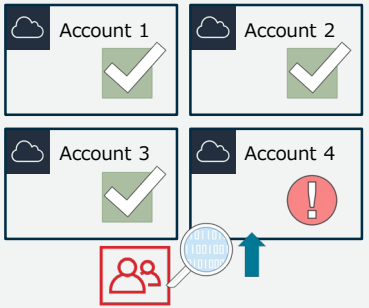


組織全体への展開と
コンプライアンスチェックを
より簡単に

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

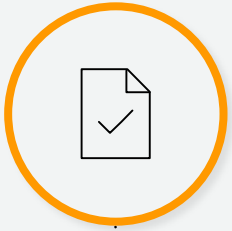
その他の
アップデート



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

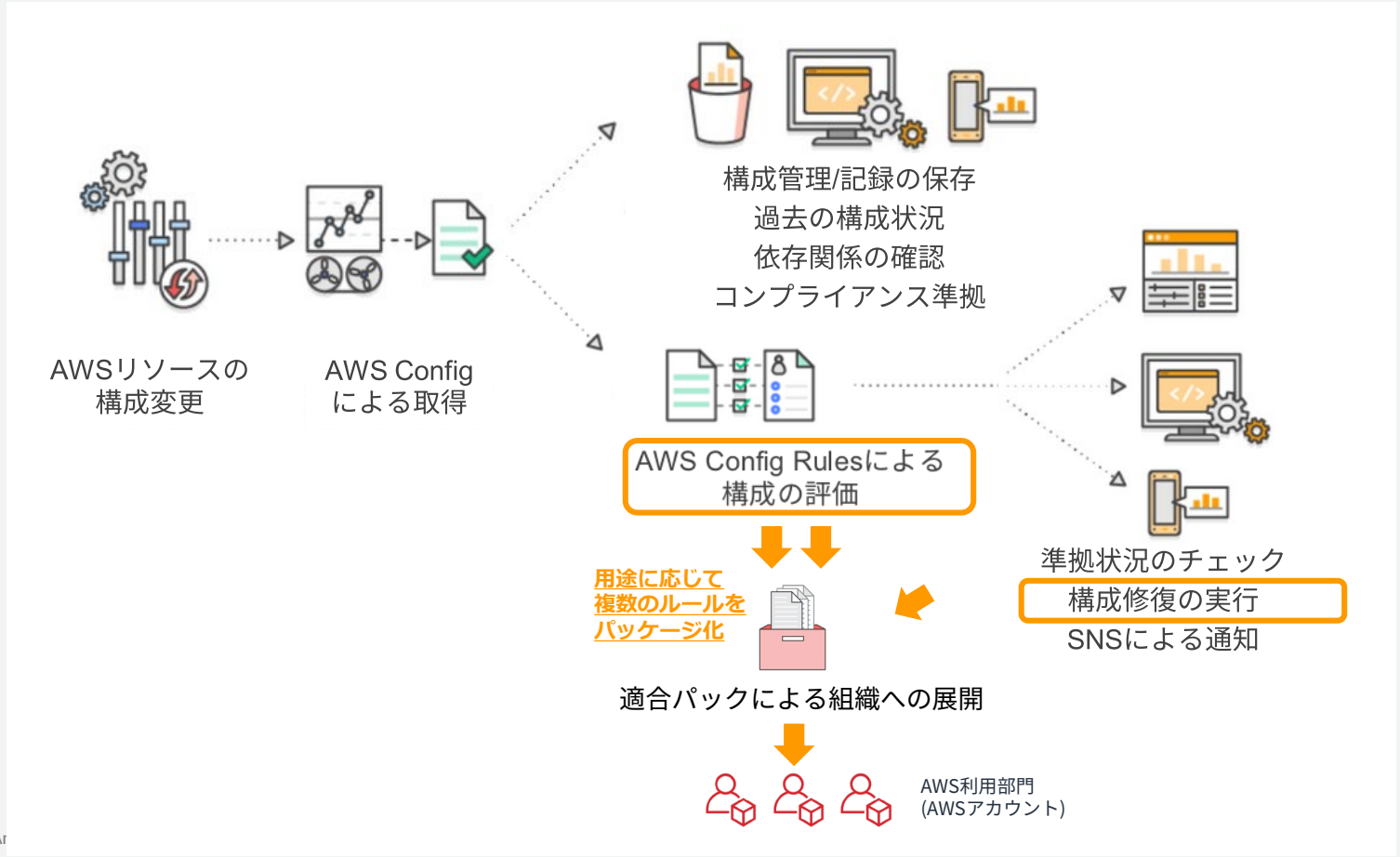
不変性(immutable)

- 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

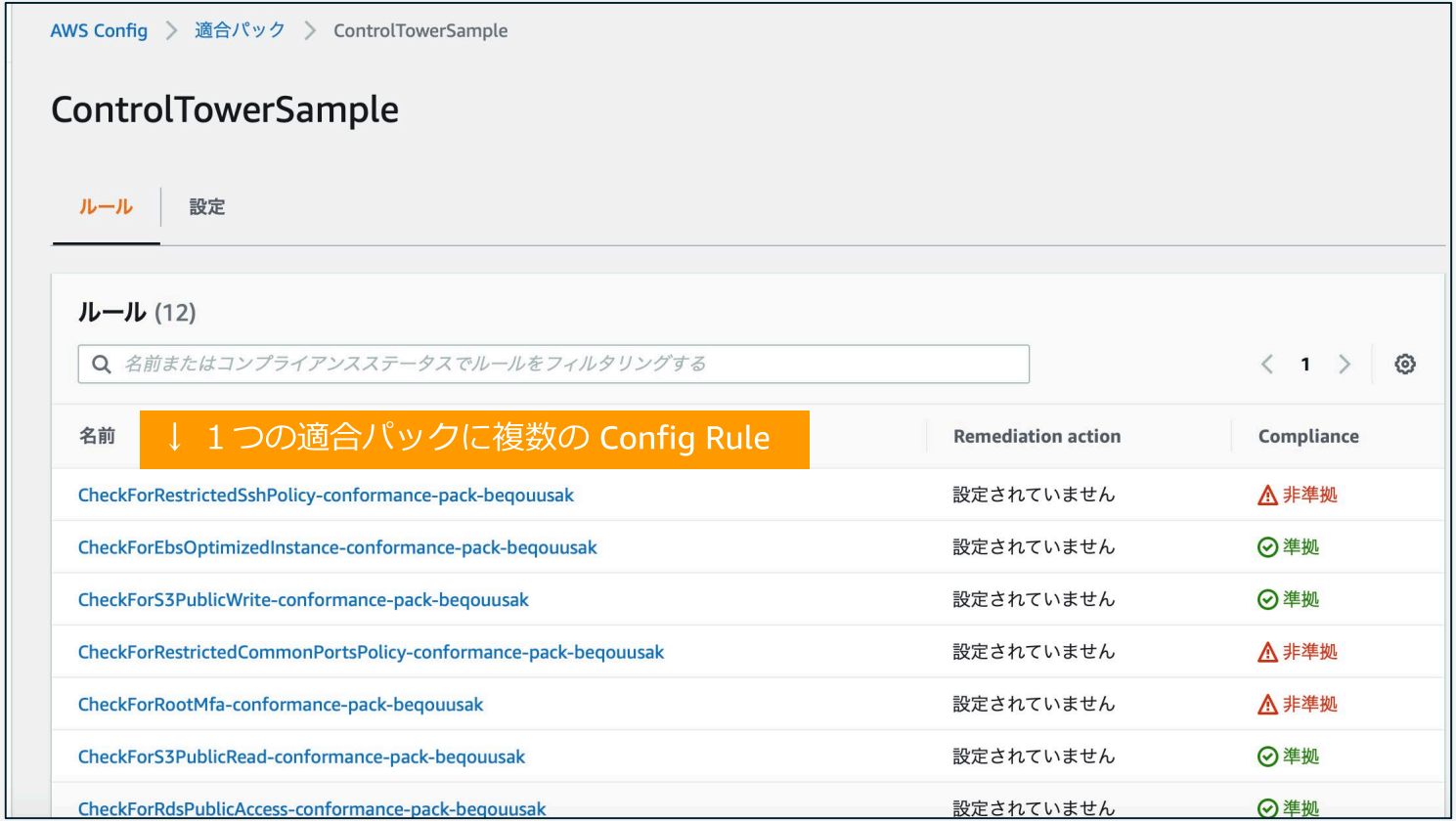
価格体系

- 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



↑ 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

Sign up

awslabs / aws-config-rules　Watch 100　Star 966　Fork 463

Code　Issues 36　Pull requests 23　Actions　Projects

master　aws-config-rules / aws-config-conformance-packs /　Go to file

tysodotcom Updated names of the CIS AWS Foundation benchmark y...　24 days ago　History

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

https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/conformancepack-sample-templates.html
https://github.com/awslabs/aws-config-rules/tree/master/aws-config-conformance-packs

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
ABS CCIG 2.0 マテリアルワ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
APRA CPG 234 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
CIS 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
CMMC レベル 2 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)
運用のベストプラクティス FedRAMP (中)
FFIEC の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

テンプレート名
K-ISMS 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
MAS TRMG 2013 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
NERC CIP 運用のベストプラクティス
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
NIST 800-53 リビジョン 4 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
NIST CIS 運用のベストプラクティス
NYDFS 23 運用のベストプラクティス
PCI DSS 3.2.1 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

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
AWS Control Tower 発見的ガードレールコンフォーマンスパック
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
EC2 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
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
データの耐障害性に関する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
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
暗号化とキー管理の運用のベストプラクティス

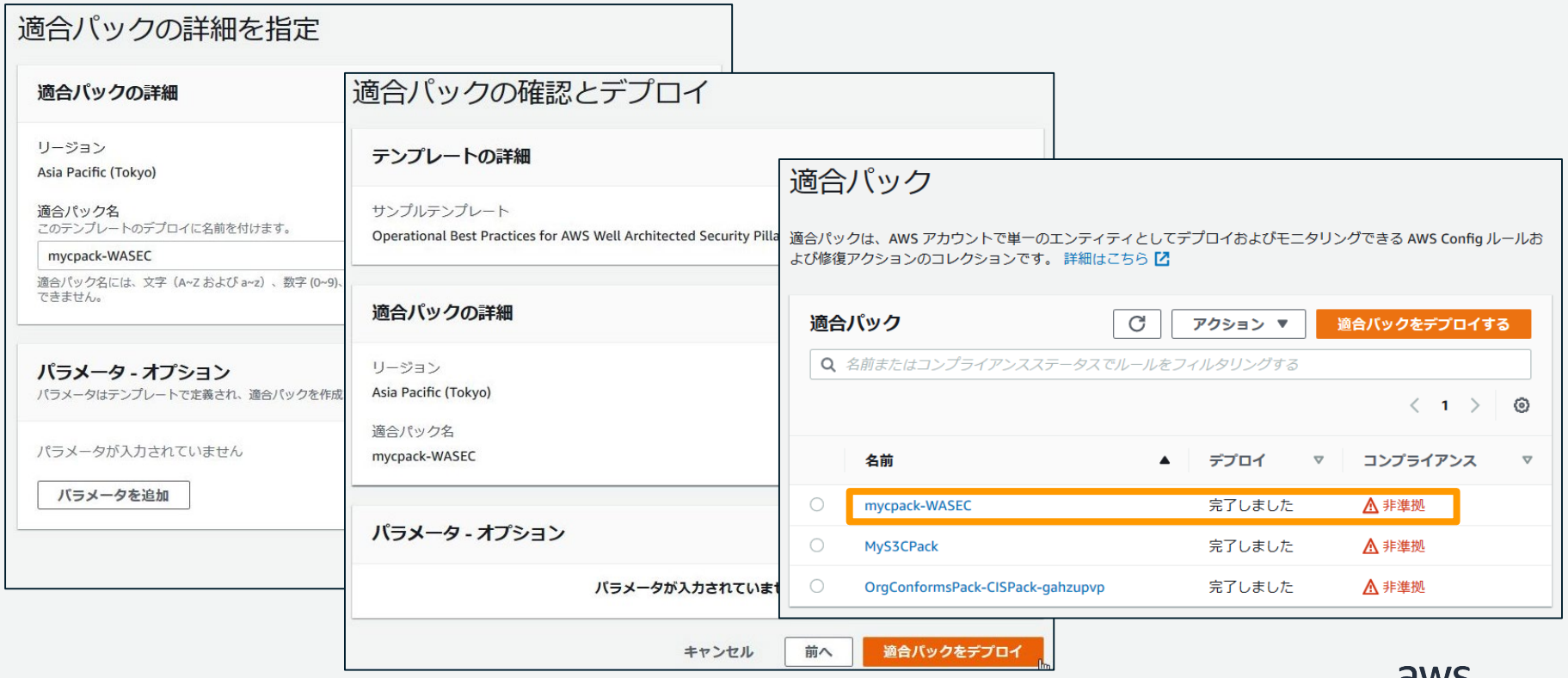
テンプレート名
クエリに関する運用のベストプラクティス – コーディングのベストプラクティス
アセット管理の運用のベストプラクティス
ロードバランシング運用のベストプラクティス
ログ記録運用のベストプラクティス
管理とガバナンスサービスの運用のベストプラクティス
モニタリング運用のベストプラクティス
ネットワーキングとコンテンツ配信サービスの運用のベストプラクティス
パブリックにアクセス可能なリソース運用のベストプラクティス
セキュリティ、アイデンティティ、およびコンプライアンスサービスの運用のベストプラクティス
サーバーレス運用のベストプラクティス
ストレージサービス運用のベストプラクティス
修正アクションを含むテンプレートの例
カスタムコンフォーマンスパック

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

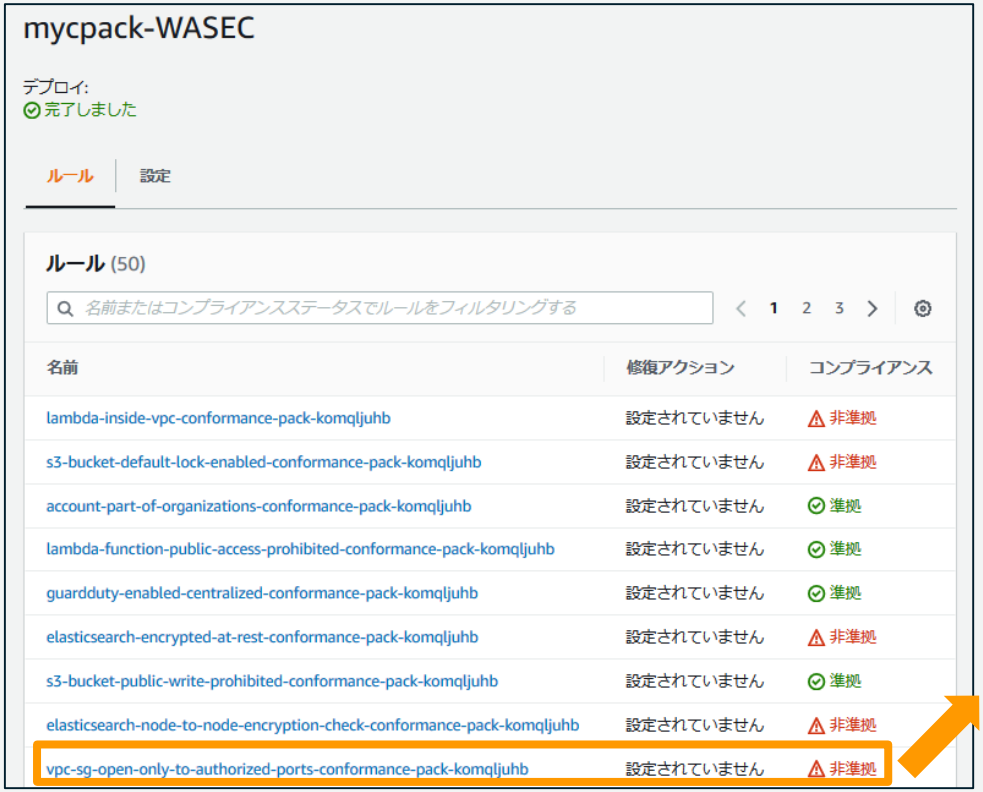
適合パックの設定イメージ (2/3)

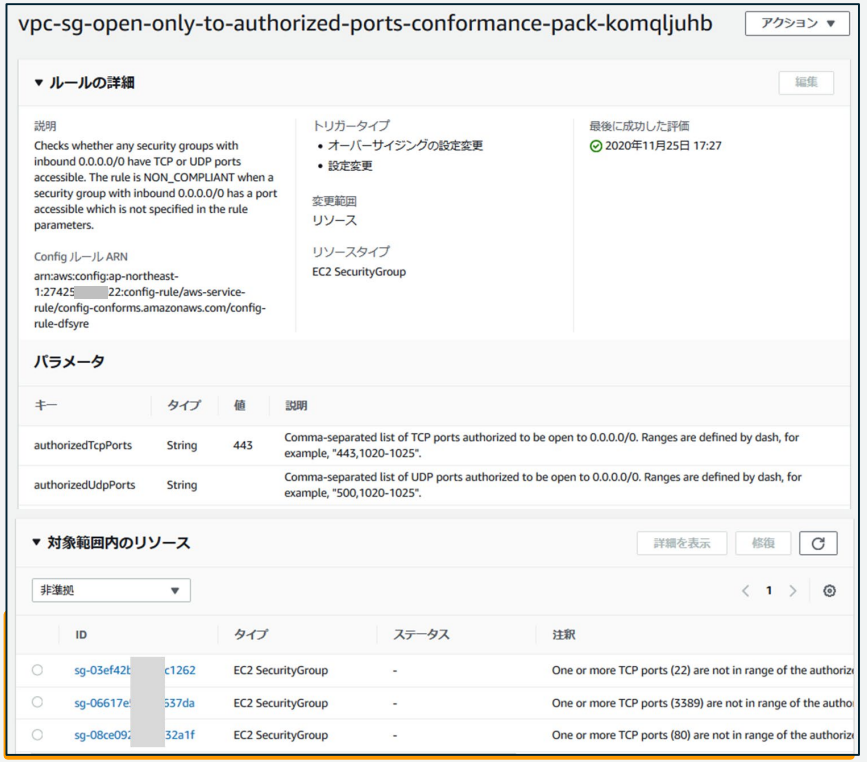
AWS Well-Architected フレームワークセキュリティ柱の運用のベストプラクティス



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





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、適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プラインワー (CCSFP)、およびさまざまな業界フレームワークのガイダンス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)

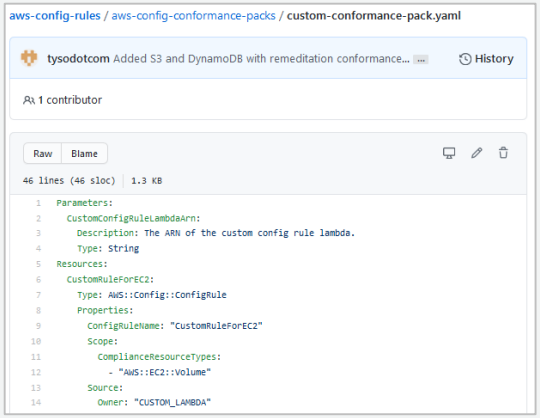
コントロール ID	コントロールの説明	AWS Config ルール	ガイダンス
SEC-1	ワークロードはどのように安全に運用しますか? ワークロードを安全に運用するには、セキュリティのすべての領域に対してベストプラクティスの上書きを適用する必要があります。組織レベルとワークロードレベルで運用上の優秀性において定義した要件とプロセスを取得し、すべての領域に適用します。AWS や業界の推奨事項、脅威インテリジェンスに関する最新情報を入手して、脅威モデルとコントロール目的の進化に役立てることができます。セキュリティプロセス、テスト、検証を自動化することで、セキュリティオペレーションをスケールすることが可能になります。	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	ワークロードはどのように安全に運用しますか? ワークロ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。組織レベルとワークロ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 や業界の推奨事項、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可能になります。	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	ワークロードはどのように安全に運用しますか? ワークロ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。組織レベルとワークロ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。

https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/operational-best-practices-for-wa-Security-Pillar.html

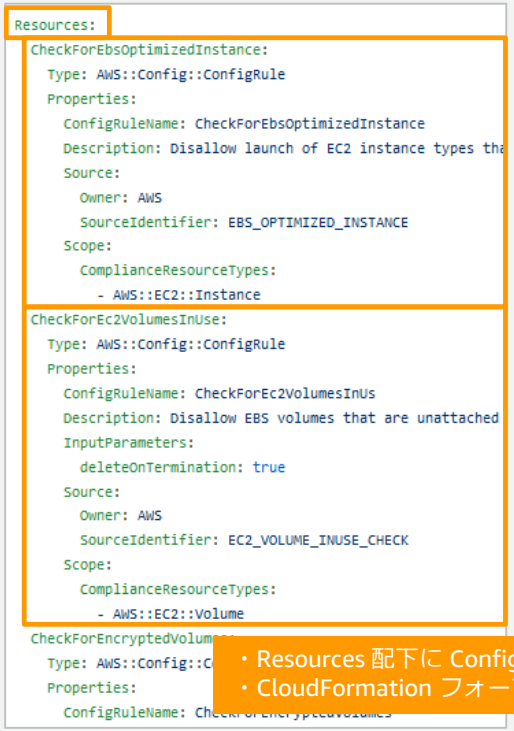
適合パック：カスタムテンプレート

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

1. GitHubからテンプレートをダウンロード (yaml形式)



2. 修正してカスタムテンプレート化

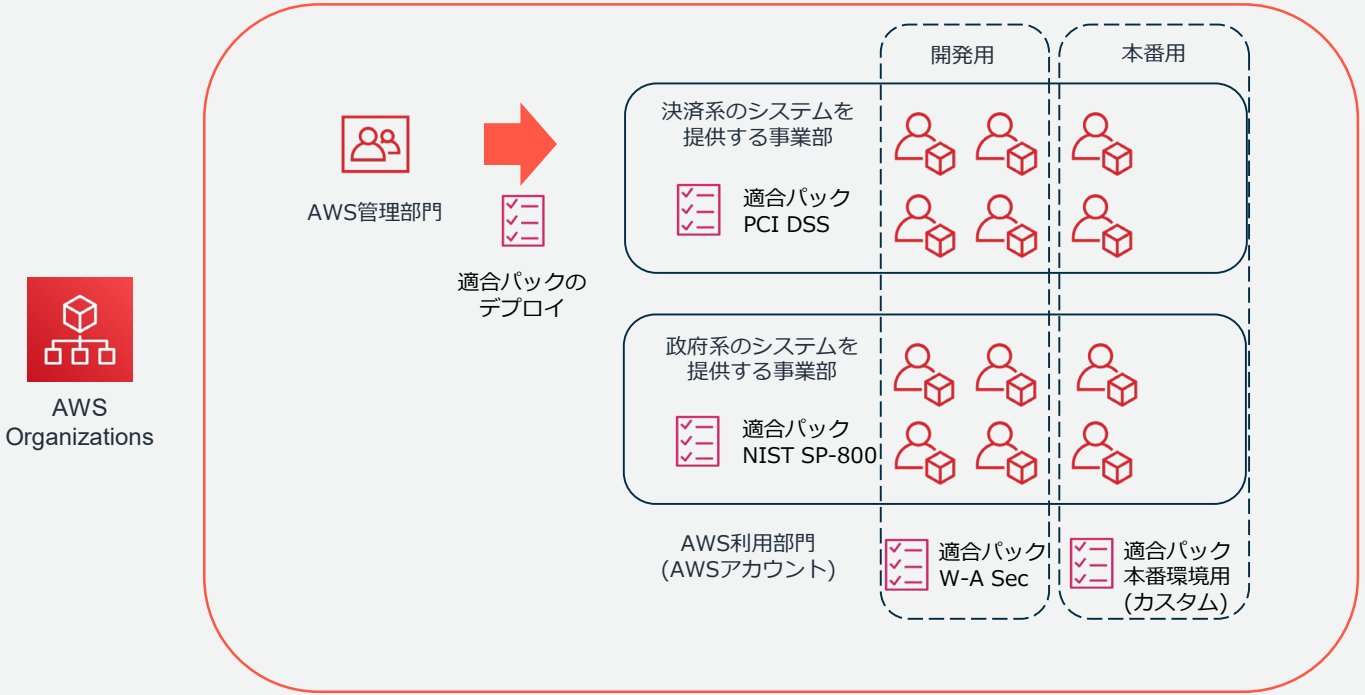


3. 適合パックのデプロイ時にアップロードして利用

- Resources 配下に Config Rule を記載
- CloudFormation フォーマットの Config Rules 定義

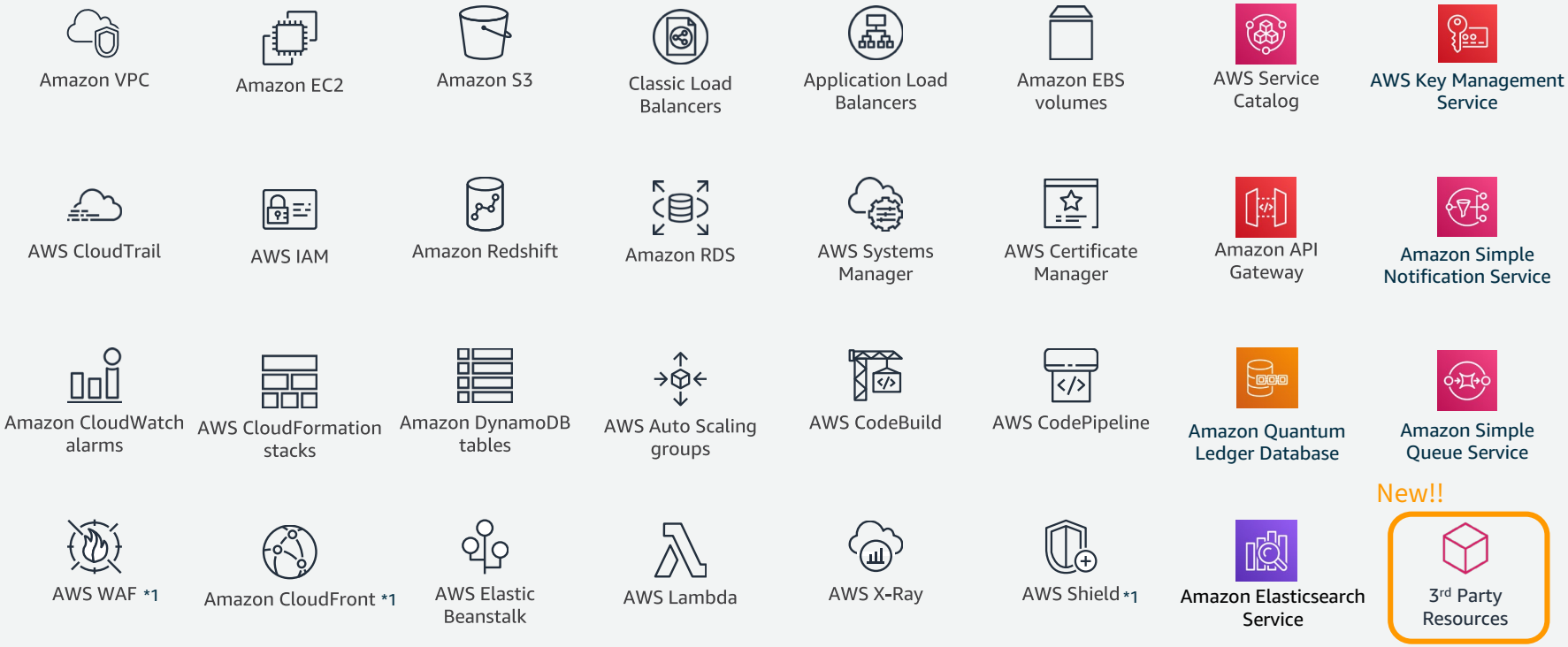
https://github.com/awslabs/aws-config-rules/blob/master/aws-config-conformance-packs/custom-conformance-pack.yaml
https://docs.aws.amazon.com/ja_jp/AWSCloudFormation/latest/UserGuide/aws-resource-config-configrule.html

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

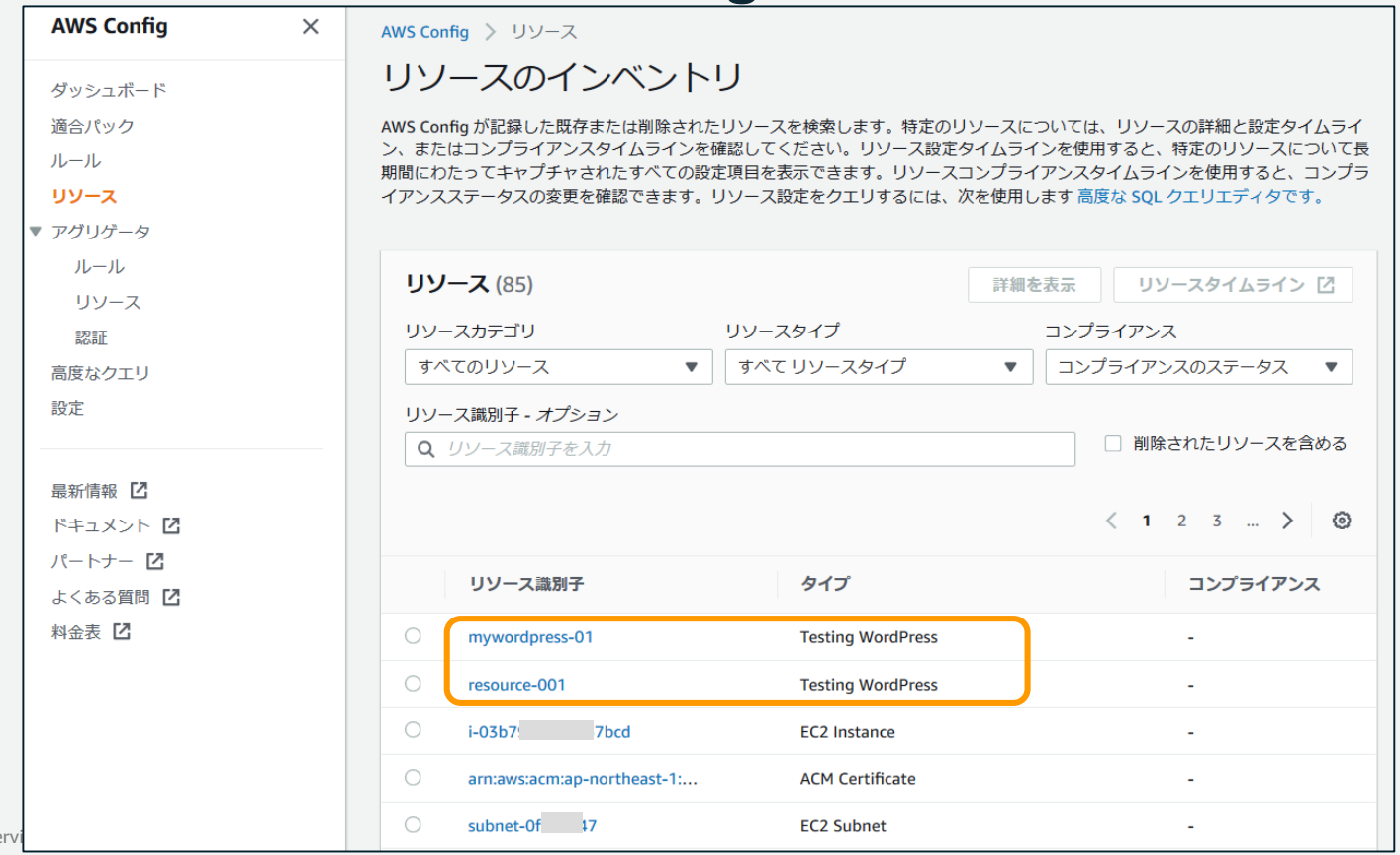
AWS Config が対応しているリソース



*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



https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/customresources.html

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

リソースタイムライン

▶ 詳細

▼ 設定項目 (JSON) の表示


```
{
  "version": "1.3",
  "accountId": "274251360022",
  "configurationItemCaptureTime": "2020-11-23T13:37:54.624Z",
  "configurationItemStatus": "OK",
  "configurationStateId": "1606138674624",
  "configurationItemMD5Hash": "",
  "resourceType": "MyCustomNamespace::Testing::WordPress",
  "resourceId": "mywordpress-01",
  "awsRegion": "ap-northeast-1",
  "tags": {},
  "relatedEvents": [],
  "relationships": [],
  "configuration": {
    "InstanceId": "i-03b[redacted]67bcd",
    "PublicIp": "3.[redacted].14.57",
    "SubnetId": "subnet-84[redacted]3df",
    "Name": "MyCustomResourceWordPress"
  },
  "supplementaryConfiguration": {},
  "resourceTransitionStatus": "None"
```


設定の詳細情報

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

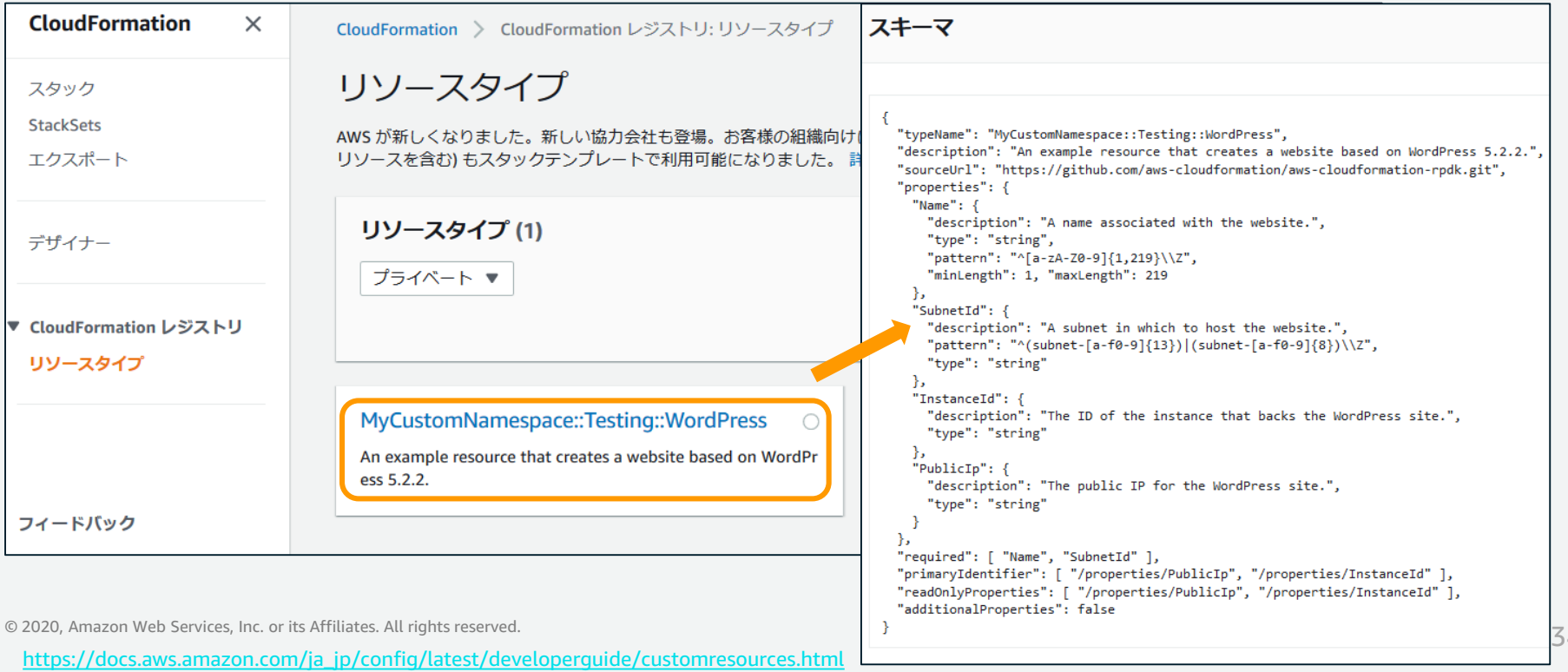
▼ 変更 3

設定変更 3

フィールド	開始	終了
Configuration.SubnetId	"subnet-ala[redacted]ala"	"subnet-8[redacted]3df"
Configuration.PublicIp		"3[redacted].14.57"
Configuration.InstanceId		"i-03b79daf[redacted]67bcd"

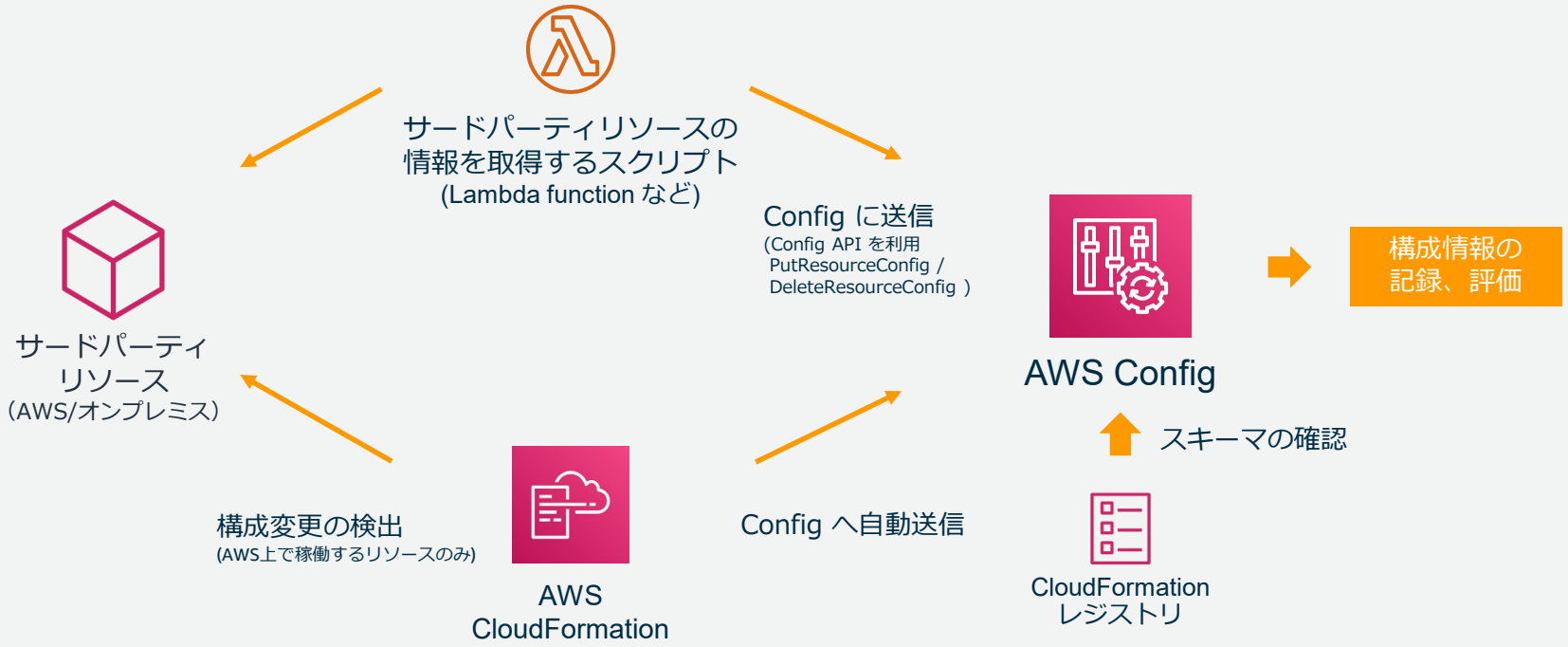
仕組み：CloudFormation リソースプロバイダ

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)



https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/customresources.html

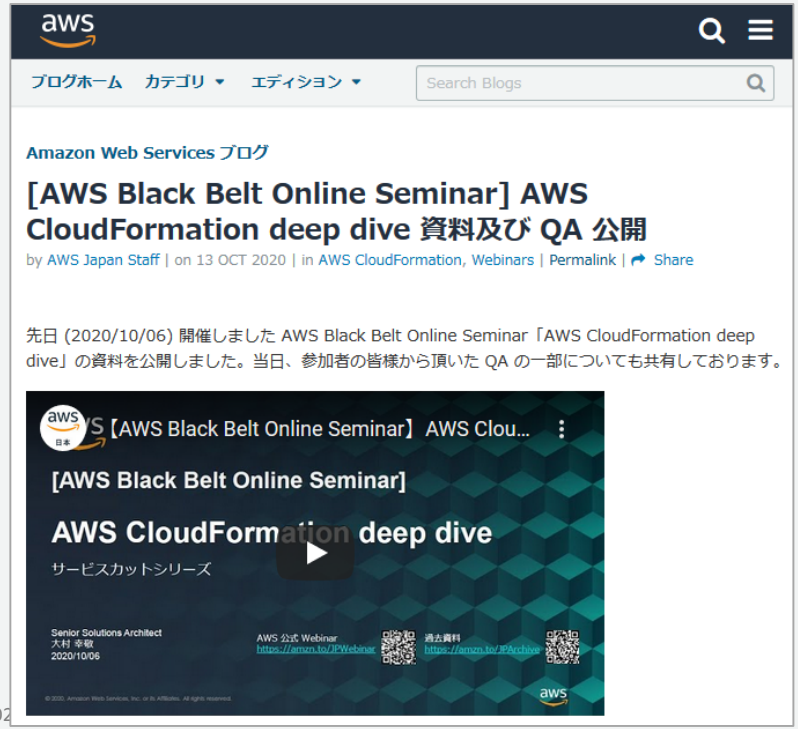
サードパーティリソースの構成情報の流れ

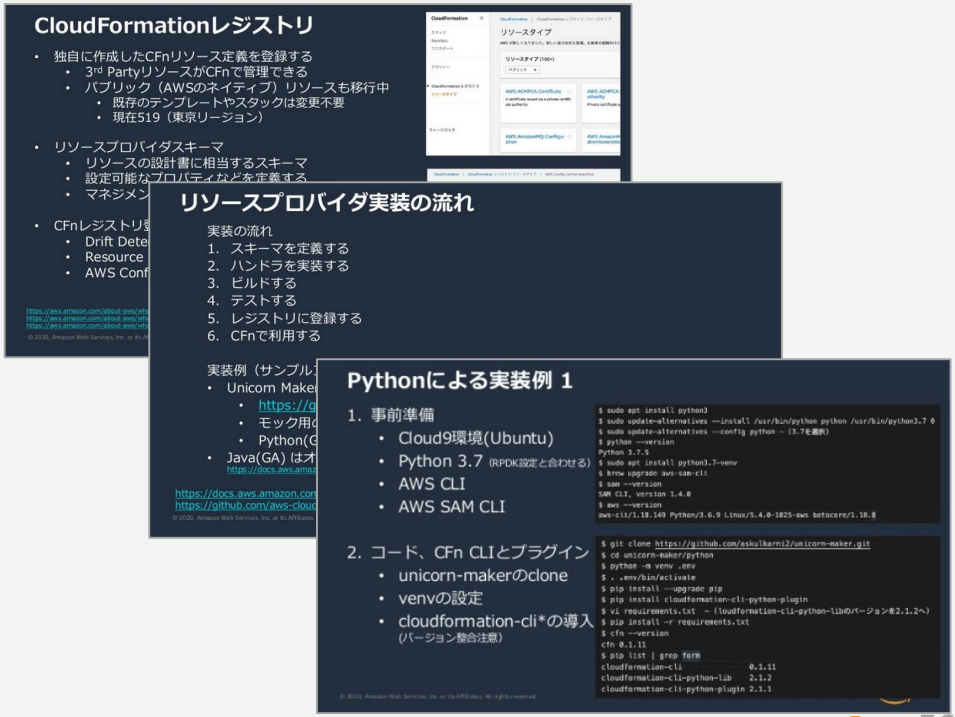


https://aws.amazon.com/jp/about-aws/whats-new/2020/06/aws-config-integrates-aws-cloudformation-registry/

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/

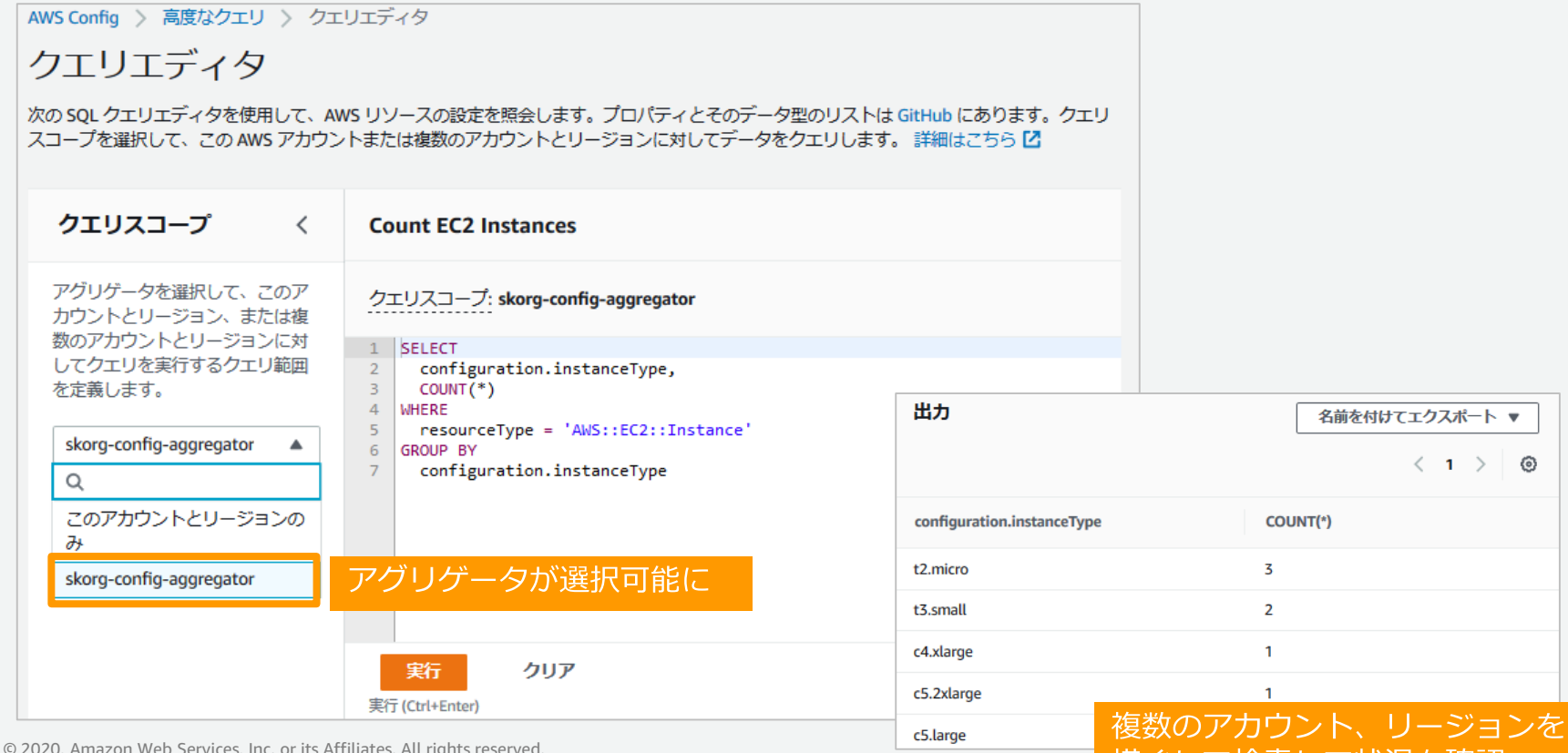




その他のアップデート

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



https://aws.amazon.com/jp/about-aws/whats-new/2020/03/introducing-aws-config-multi-account-multi-region-support-for-advanced-query/

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


```
$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}"
```

評価結果をまとめて確認

https://aws.amazon.com/jp/about-aws/whats-new/2019/07/aws-config-now-enables-you-to-provision-config-rules-across-all-aws-accounts-in-your-organization/
https://aws.amazon.com/jp/blogs/mt/deploy-aws-config-rules-and-conformance-packs-using-a-delegated-admin/

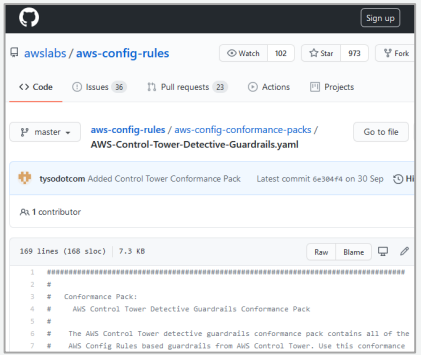
マルチアカウント環境へのガードレールの適用

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



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_INSTAN
      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

https://aws.amazon.com/jp/blogs/news/aws-control-tower-detective-guardrails-as-an-aws-config-conformance-pack/

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

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/strongly-recommended-guardrails.html
https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/elective-guardrails.html

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

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