

AWS

S U M M I T

AWSのガバナンス入門

(AWS CloudTrail, AWS Config)

アマゾン ウェブ サービス ジャパン株式会社
パートナーソリューションアーキテクト 市崎 洋平

2017年6月2日



本セッションのFeedbackをお願いします

受付でお配りしたアンケートに本セッションの満足度やご感想などをご記入ください
アンケートをご提出いただきました方には、もれなく**素敵なAWSオリジナルグッズ**を
プレゼントさせていただきます

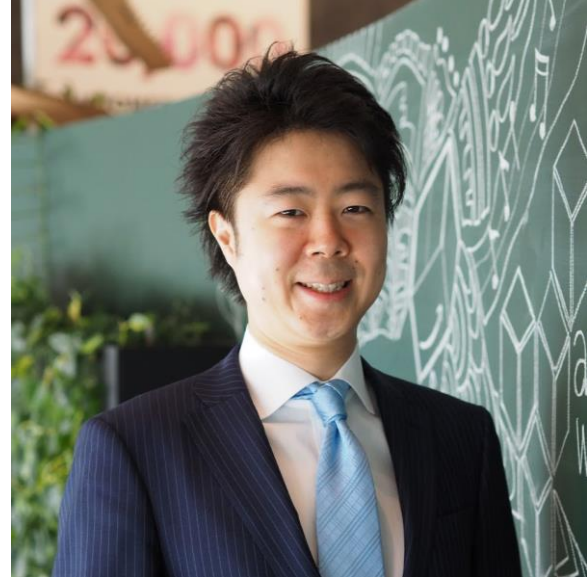


アンケートは受付、パミール3FのEXPO展示会場内にて回収させていただきます

自己紹介

市崎 洋平（いちざき ようへい）

アマゾン ウェブ サービス ジャパン株式会社
エコシステムソリューション部
パートナーソリューションアーキテクト



大手外資系ITベンダー

大手銀行業向けプリセールス

ITコンサルティング

大規模アプリSI

大規模インフラSI

本セッションの目的

AWSの「操作管理」の重要性

「操作管理」をどのように実現可能か

アジェンダ

- オンプレミス環境の“ガバナンス”課題
- AWSを利用した場合のメリット
- AWS CloudTrail とは
- AWS CloudConfig とは
- AWS CloudConfig Rules とは

はじめに

ITガバナンスとは・・・

組織構成

経営層の積極関与

投資対
効果

プロセス・
仕組みの充実

カルチャー
の醸成

内部統制

COBIT5

control objectives for
information and related technology

- 原則 1 ステークホルダーの要求を充足
- 原則 2 事業体全体の包含
- 原則 3 単一の統合されたフレームワークの適用
- 原則 4 包括的アプローチの実現
- 原則 5 ガバナンスとマネージメントの分離

<http://www.isaca.org/cobit/>

ここでは、“ガバナンス”を

対象

IT
システム

AWS
を使った
システム

手段

記録を
取る

振り返る

ルールを
適用する

狙い・実現できること

問題の
原因を
追跡可能

問題を
発生
させない

監査

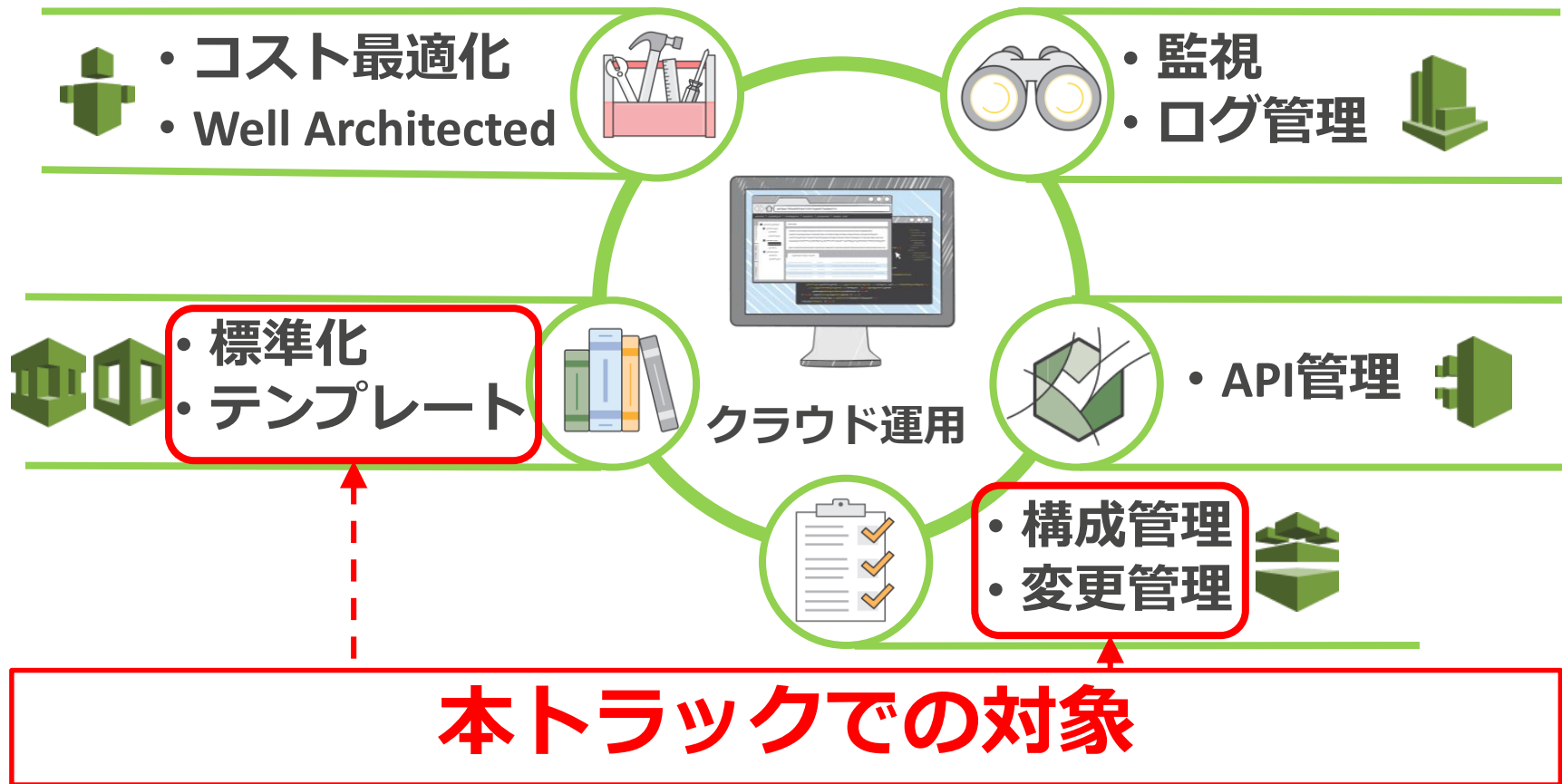
秩序

事故
防止

過去

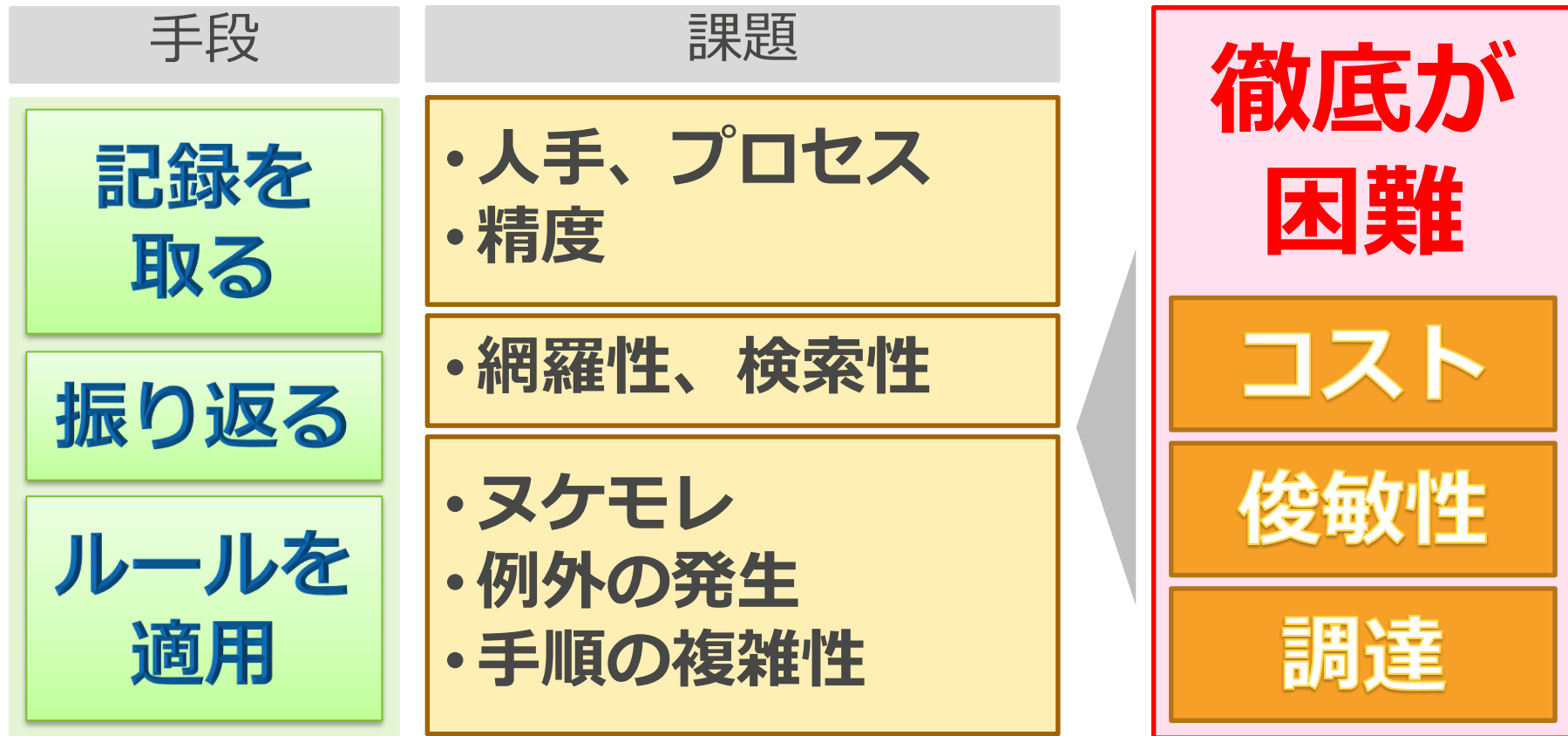
未来

AWSにおける、クラウド運用のOverview



オンプレミス環境の“ガバナンス”課題

オンプレ環境におけるガバナンスの課題（俯瞰）



オンプレ環境におけるガバナンスの課題（詳細）

	対象	どのように？
記録を取る	<ul style="list-style-type: none">・機器の設置場所、時期・接続配線・機器交換、廃棄・F/W, 固有の設定	<ul style="list-style-type: none">・目視・人手で記録・都度更新・複数の記録先
	ヒューマンエラー	機器ごとの項目
	俊敏性	
振り返る	低い記録精度・網羅性・検索性	
	問題を追跡できない	

オンプレ環境におけるガバナンスの課題（詳細）

対象・どのように？

- ・機種/スペックの統一・パターン化
- ・調達先の統一
- ・物理構成のパターン化
- ・非機能要件の項目共通化

ルール
を
適用
する

販売終了

調達先の変更

特殊な構成・要件

ルール非準拠の多発・継続

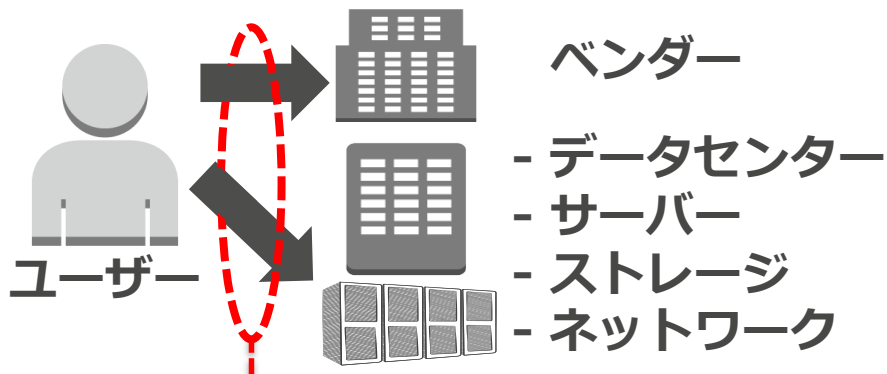
問題発生(セキュリティ、未知の問題、等)

AWSを利用した場合のメリット

AWSを“操作”すること

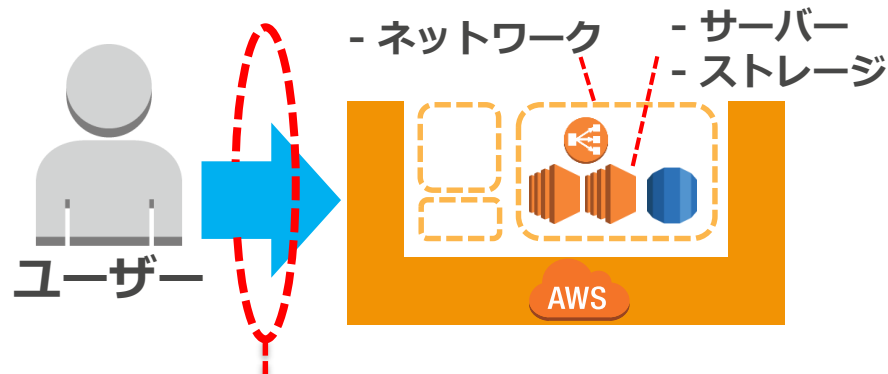
ITシステム環境を手に入れる

オンプレミス



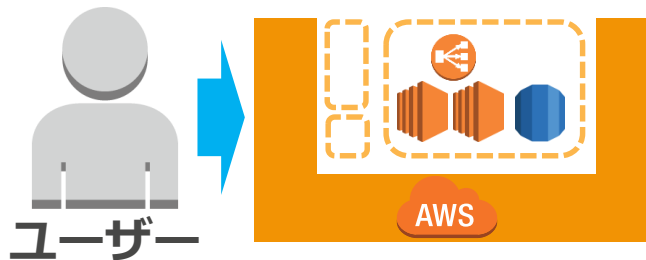
- ・ベンダーと会話
- ・DC立ち入り
- ・人手の作業、依頼

AWS

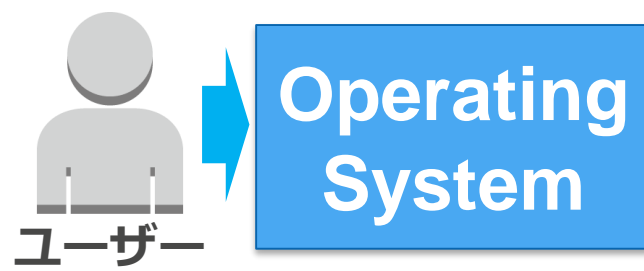


- ・AWSアカウント
- ・認証
- ・コマンド(API)実行

AWSを“操作”すること



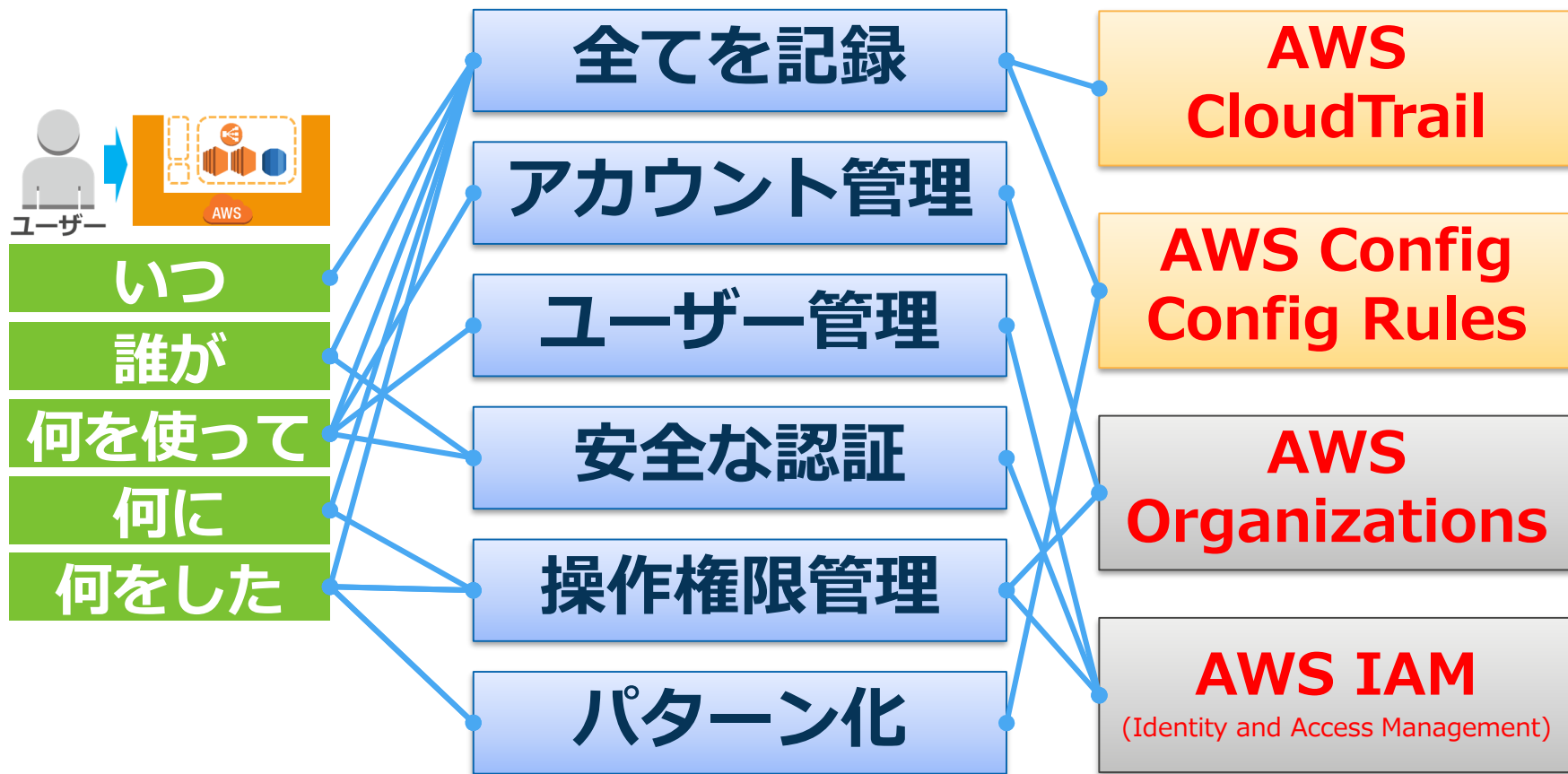
いつ	17:40
誰が	開発者A
何を使って	admin010
何に	i-XXXXXX
何をした	起動



17:40
管理者B
root
/etc/xxx
編集

OSの運用管理の概念を流用可能

AWSの「操作管理」を支援する機能



オンプレミスとAWSの差

操作の自由度

オンプレミス

- 物理機器、構成を、
 - 自由に変更できない
 - 即座に変更できない

AWS

- リソース、構成を、
 - 自由に変更可能
 - 即座に変更可能

AWSリソースの「操作管理」が重要

AWSにおける、変更記録の重要性

AWSリソースの「操作管理」

記録・振り返り

履歴から過去を調査

ルールを適用

操作権限の管理
構成パターンの強制

人間+
アカウント

AWS CloudTrail

AWS Organizations

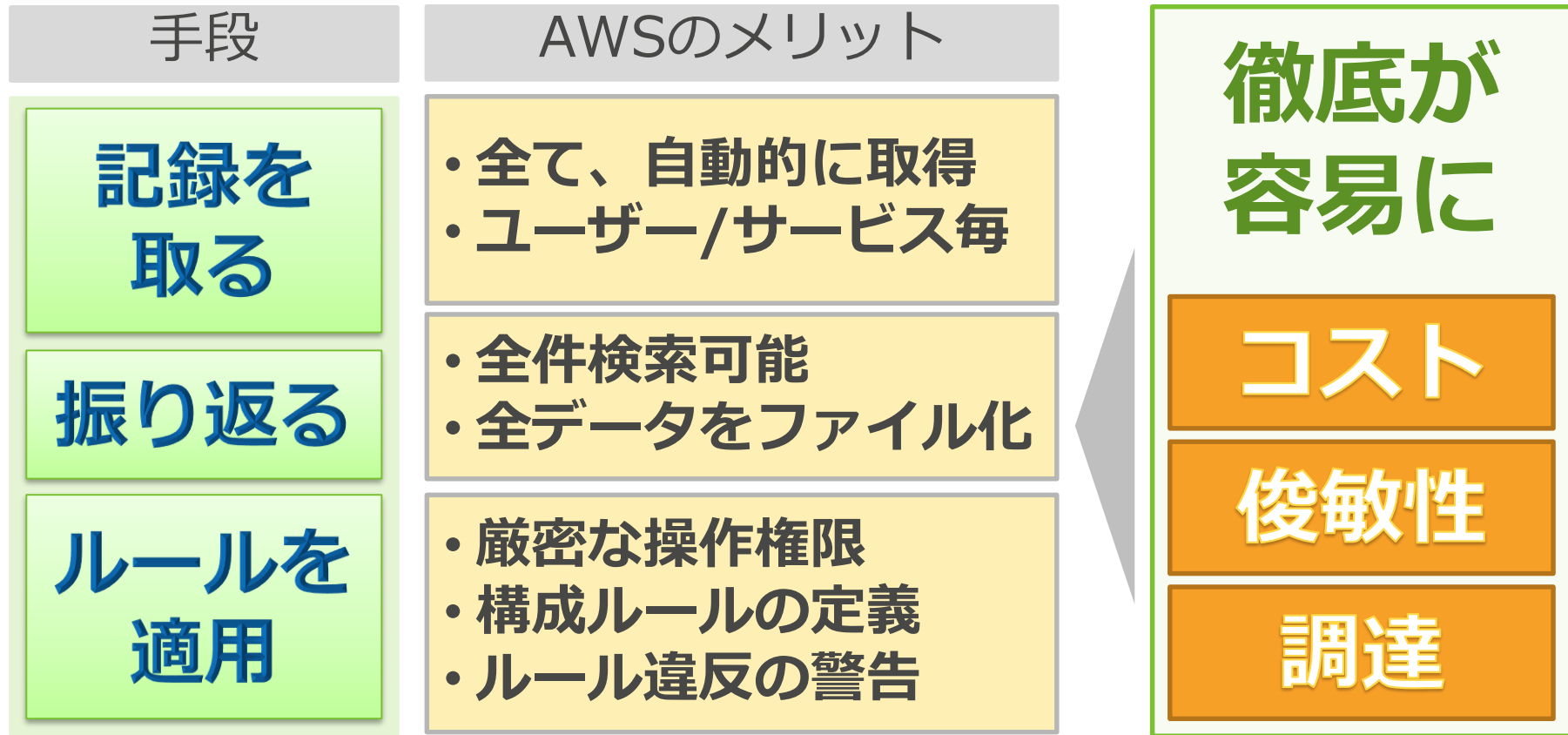
AWS IAM

システム
観点

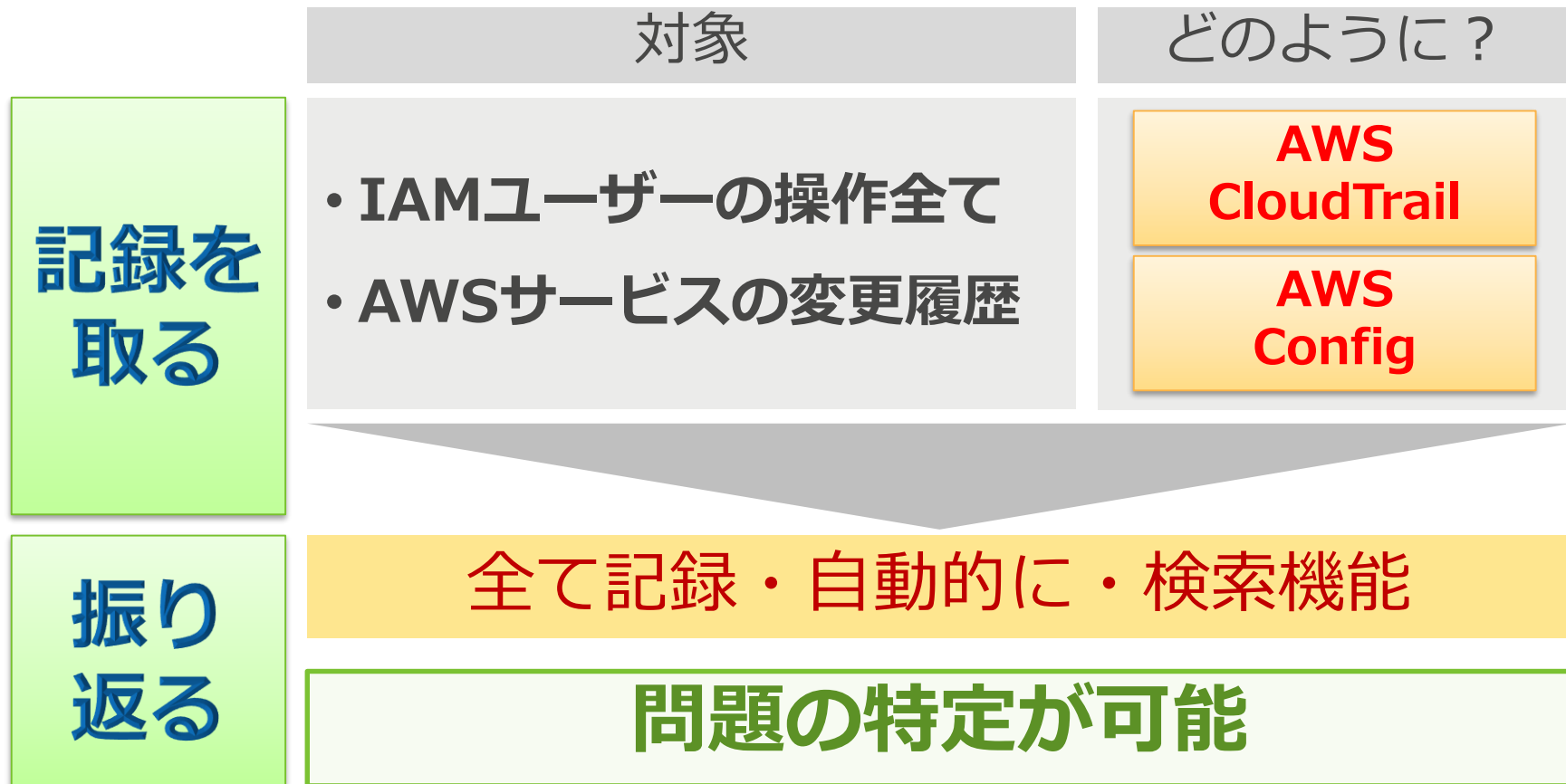
AWS Config

AWS Config Rules

AWSにおけるガバナンスの容易性（俯瞰）



AWSにおけるガバナンスの容易性（詳細）



AWSにおけるガバナンスの容易性（詳細）

対象・どのように？

ルール
を
適用
する

AWS Organizations

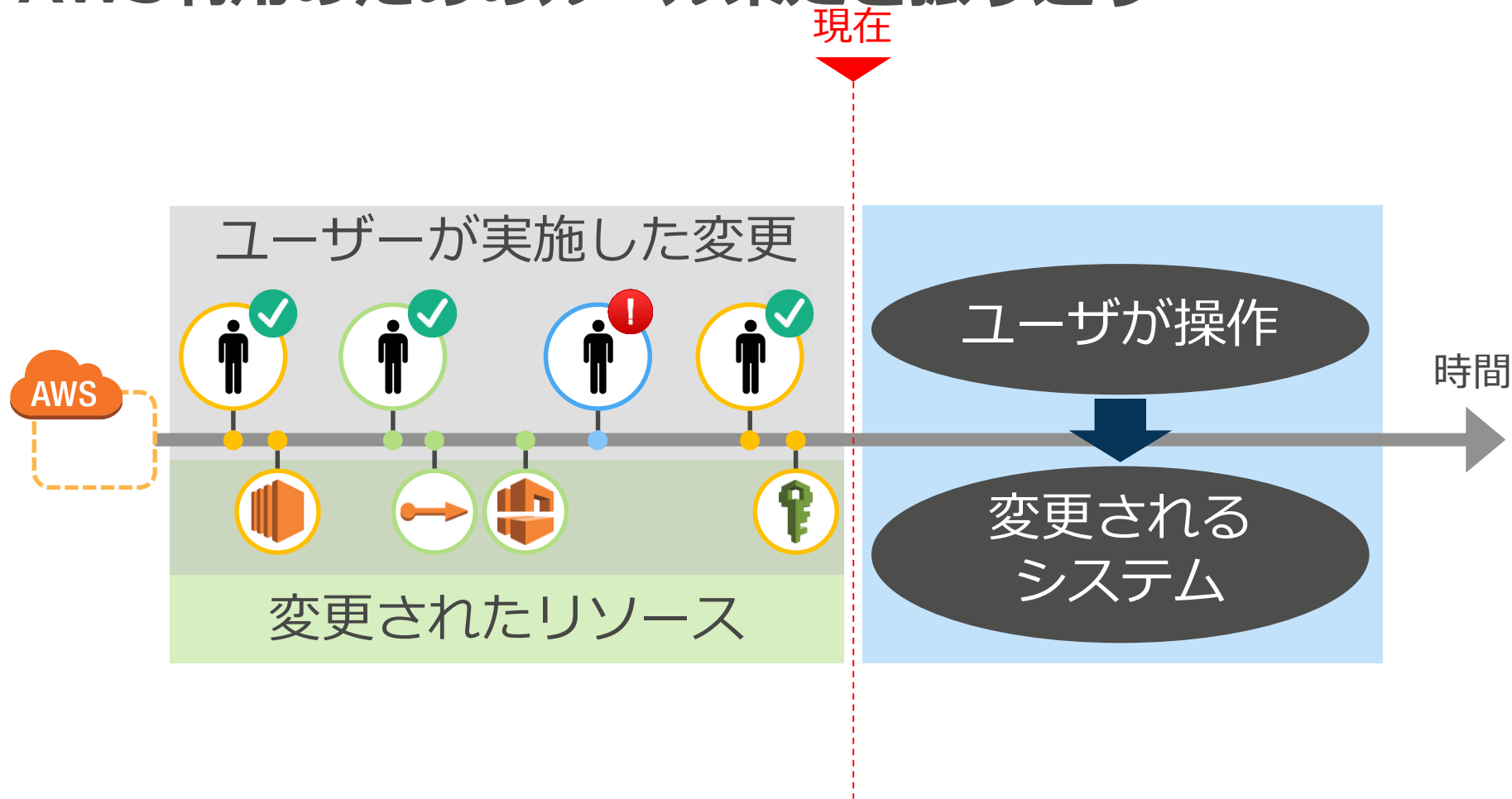
AWS IAM

AWS Config Rules

適切な権限・ルール外の警告

ルールを徹底したシステム

AWS利用のためのルール策定と振り返り



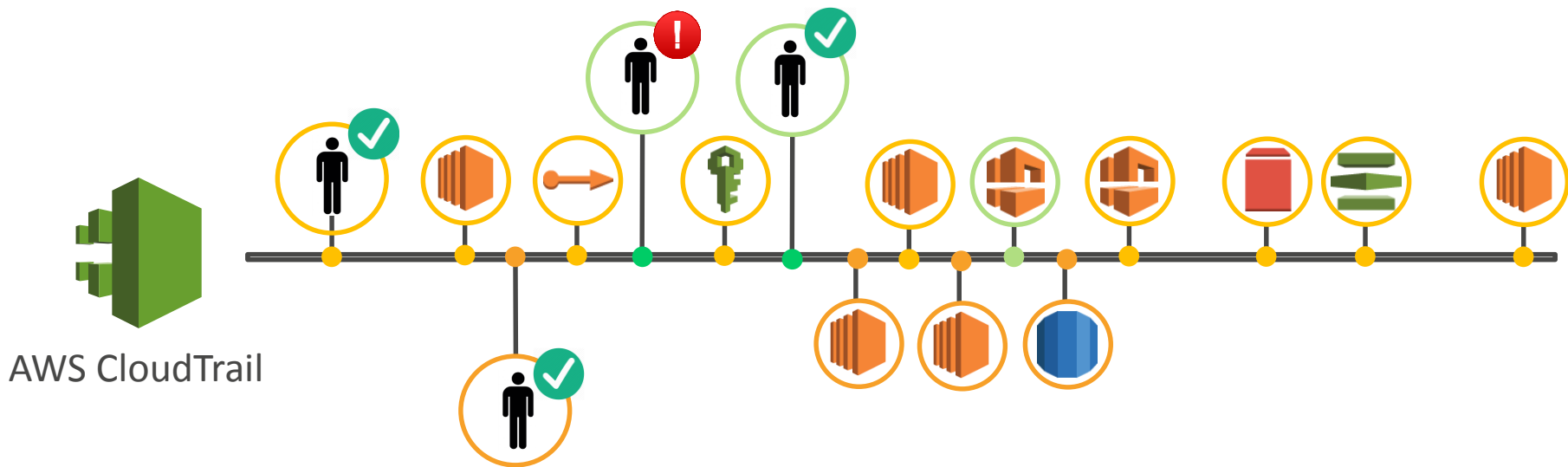
AWS利用のためのルール策定と振り返り



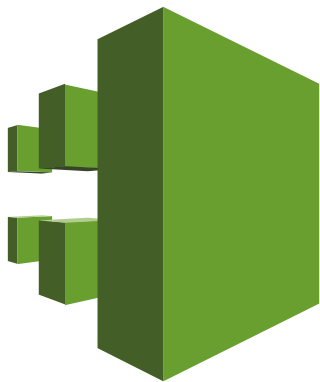
AWS CloudTrail とは

AWSに対する活動をどうとらえるか

誰が、何に対して、いつ、何をしたか、を**全て記録**



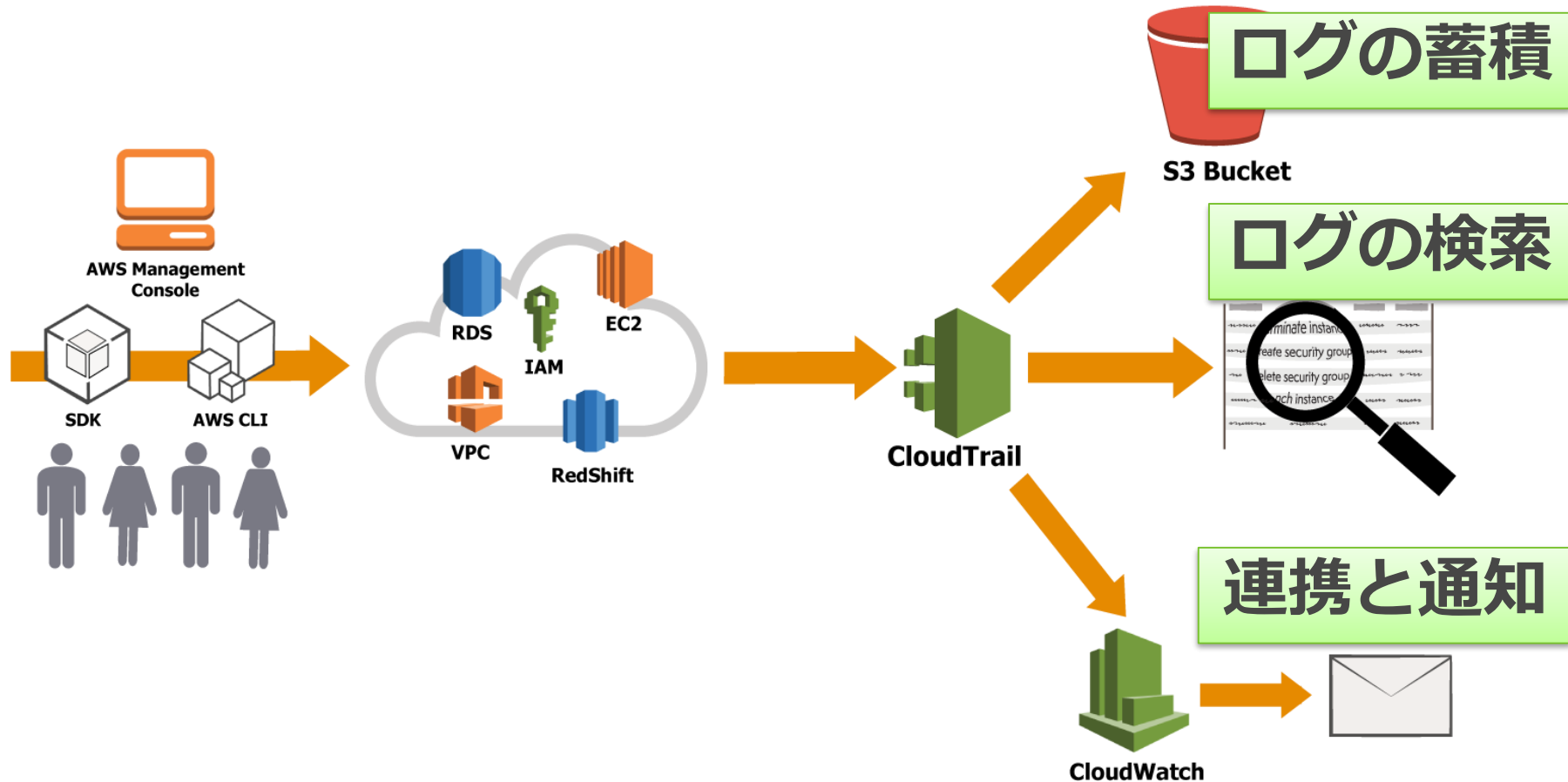
AWS CloudTrail とは



CloudTrail

- **AWSユーザの操作(API)をロギング**
 - IAMユーザのオペレーションをトラッキング
- **ログはS3に保存**
 - **暗号化**可能
 - **改ざん防止**機能
- **コスト : CloudTrail 利用は無料**
 - Amazon S3/SNSの使用料金が必要

AWS CloudTrail の利用方法 Overview

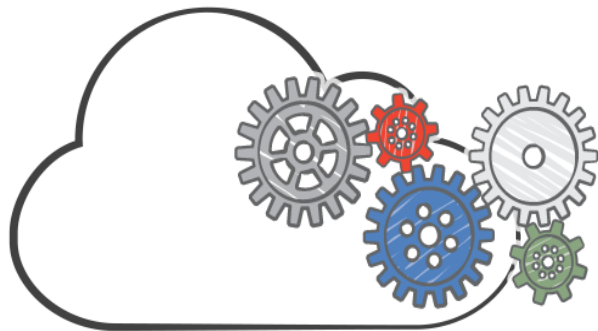


AWS CloudTrail により取得できるイベント

API イベント

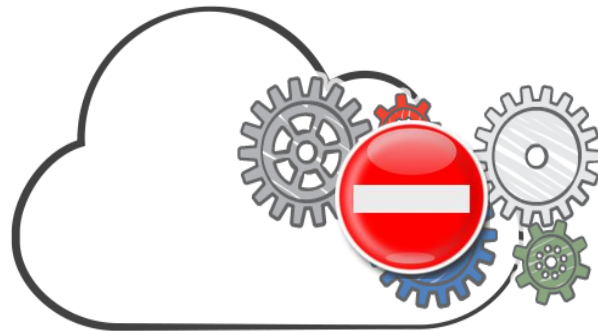


APIでないイベント



- サポートから発行されるAPI

- StartInstances
- CreateKeyPair



- ユーザのサインイン

- AWS マネジメント コンソール
- AWS ディスカッション フォーラム

ログファイルの保存先 = Amazon S3



The screenshot shows the Amazon S3 console interface. At the top, there's a navigation bar with 'Services' and 'Edit' dropdowns, and a user name 'Sivakar'. Below the navigation bar, there are buttons for 'Upload', 'Create Folder', and 'Actions'. To the right, there are tabs for 'None' and 'Properties'. The breadcrumb path is: 'All Buckets / fmrinc-cloudtrail-bucket / AWSLogs / 123456789012 / CloudTrail / us-west-2 / 2013 / 11 / 03'. Below the breadcrumb, there's a table with columns 'Name', 'Storage Class', and 'Size'. The table contains four rows of log files, all with 'Standard' storage class. The second row is highlighted in blue.

	Name	Storage Class	Size
<input type="checkbox"/>	123456789012_CloudTrail_us-west-2_2013-11-03T21:40Z_63QlcV3Qp2609sCL.json.gz	Standard	1 KB
<input checked="" type="checkbox"/>	123456789012_CloudTrail_us-west-2_2013-11-03T21:45Z_EseusVU7TNiEe8jS.json.gz	Standard	1.2 KB
<input type="checkbox"/>	123456789012_CloudTrail_us-west-2_2013-11-03T21:50Z_7CC05rQjf5YDGf78.json.gz	Standard	1.1 KB
<input type="checkbox"/>	123456789012_CloudTrail_us-west-2_2013-11-03T23:00Z_sGNVF0FjbKFip0rh.json.gz	Standard	1.1 KB

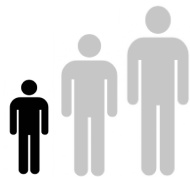
- ある特定のパスで保存（独自命名規則）
- SSE-KMSを使用して暗号化（デフォルト）

ログファイルの活用方法

短期的視点



通知



中期的視点



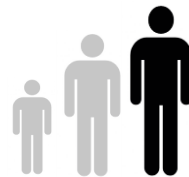
文字列検索



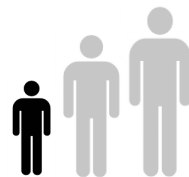
長期的視点



可視化



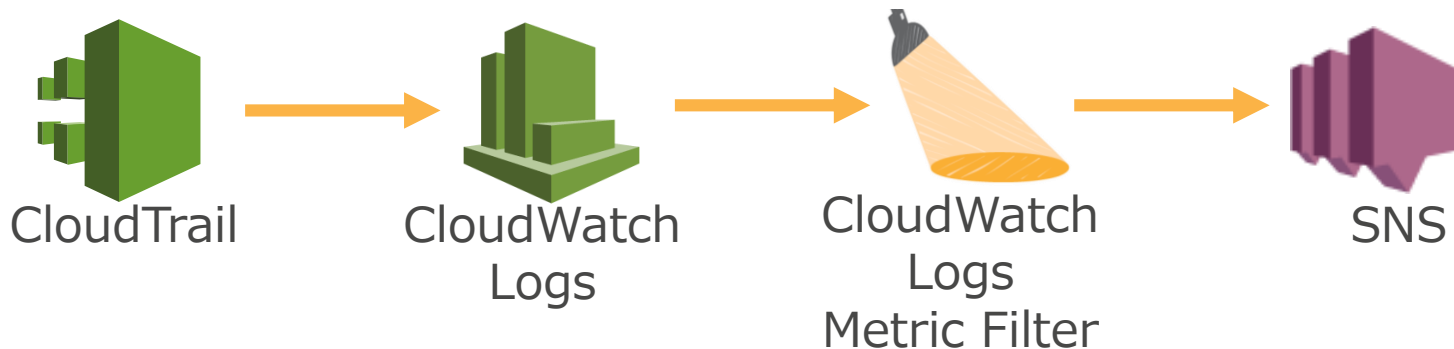
特定のアクションが起きたら通知される



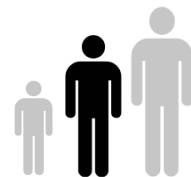
短期的

CloudTrailとCloudWatch Logsの連携

- CloudTrailのログをJSON形式でCloudWatch Logsに転送
- 特定のAPIを監視し、呼ばれたときに通知を受けることが可能
- CloudWatch Logへの転送はSSLで暗号化される



CloudTrail API lookup



中期的

AWSマネジメントコンソールから確認・検索可能

API activity history

Look up API activity related to creation, modification and deletion of resources in your AWS account in the last 7 days. Filter using one of the attributes to troubleshoot operational issues or security incidents.



Filter: **Select attribute**

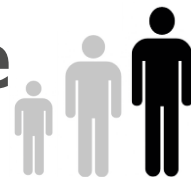
Enter lookup value

Time range: Select time range

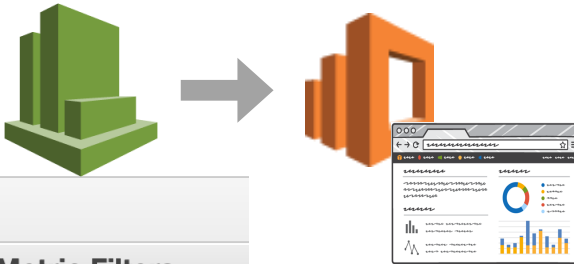


	Event time	User name	Event name	Resource type	Resource name
▶	2015-12-21, 01:18:28 PM		CreateTags		
▶	2015-12-21, 01:18:27 PM		RunInstances		
▶	2015-12-21, 01:17:03 PM		TerminateInstances		
▶	2015-12-21, 01:16:23 PM		ConsoleLogin		
▶	2015-12-20, 01:26:07 AM		RunInstances		
▶	2015-12-20, 01:26:07 AM		CreateTags		
▶	2015-12-20, 12:50:43 AM		DetachUserPolicy		
▶	2015-12-20, 12:46:34 AM		PutRolePolicy		
▶	2015-12-20, 12:40:39 AM		AttachUserPolicy		

CloudWatch Logs と Elasticsearch Service の連携による検索



長期的



Create Metric Filter **Actions**

Filter: Log Group Name

Log Groups	Expire Events After	Metric Filters
<input type="checkbox"/> /aws/lambda/HelloWorld	Never Expire	0 filters
<input type="checkbox"/> /aws/lambda/Logs	Never Expire	0 filters
<input type="checkbox"/> /aws/lambda/Shutdown	1 month (30 days)	0 filters
<input type="checkbox"/> /aws/lambda/s3access	Never Expire	0 filters
<input type="checkbox"/> CloudTrail-JSON-	Never Expire	10 filters
<input checked="" type="checkbox"/> Linux_Appache_Accesslogs	1 year (365 days)	0 filters
<input type="checkbox"/> Linux_Syslogs	1 year (365 days)	0 filters
<input type="checkbox"/> RDSOSMetrics	1 month (30 days)	0 filters
<input type="checkbox"/> defaultvpc-flowlogs	1 year (365 days)	0 filters

Actions menu options:

- Create log group
- Delete log group
- Export
- Export data to Amazon S3
- View all exports to Amazon S3
- Subscriptions
- Stream to Amazon Elasticsearch Service**
- Stream to AWS Lambda

AWS CloudTrail 有効化のベストプラクティス

すべてのリージョンで**有効**にすることがベストプラクティス

- 新リージョンが追加された際の自動登録
- 複数リージョンのログファイルを一元管理
- 複数リージョンの設定の統一
- 1つのリージョンに5つまでTrailを作成可能
 - ✓ ディベロッパー用
 - ✓ セキュリティ用
 - ✓ オーディット用

Create Trail

Trail name* CloudTrail-All-Regions

Apply trail to all regions ☒ Yes ☐ No ⓘ

Create a new S3 bucket ☒ Yes ☐ No

S3 bucket* cloudtrail-all-region-bucket ⓘ

Log file prefix ⓘ

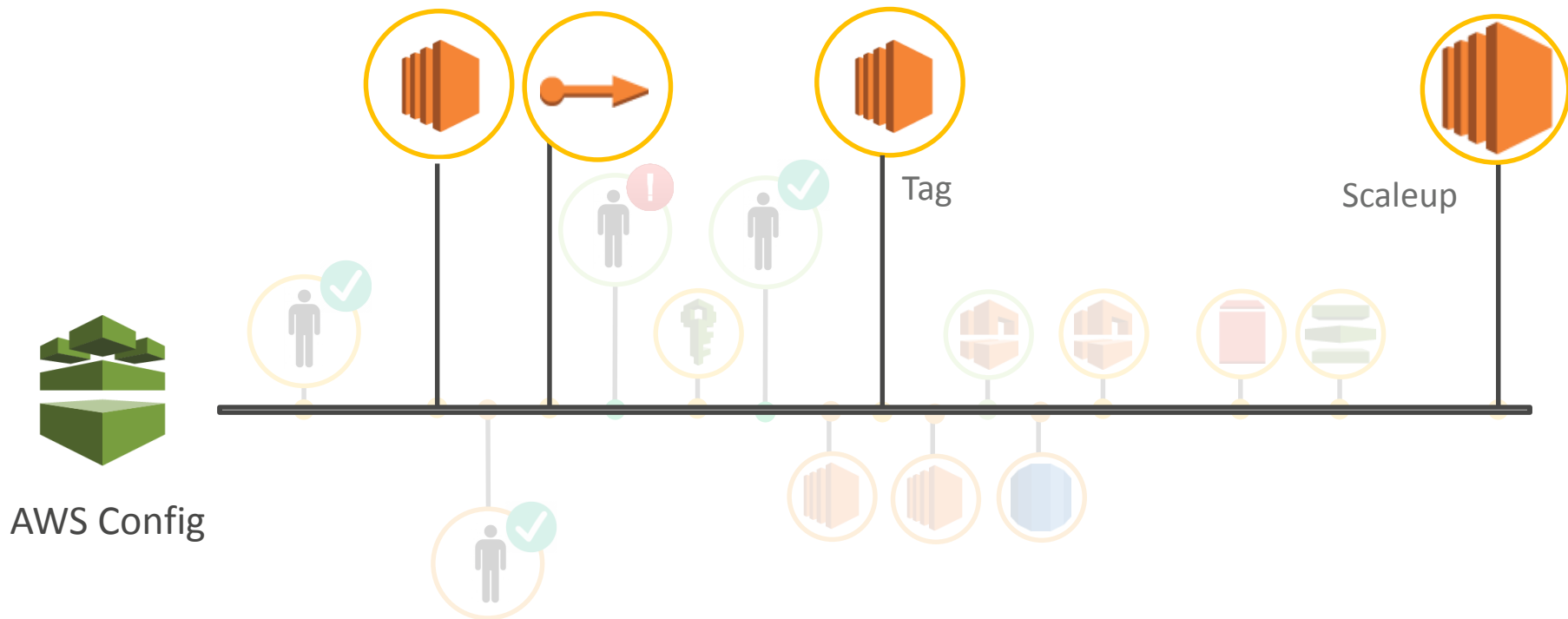
Location: /AWSLogs/675897846150/CloudTrail/us-west-2



AWS Config とは

AWSに対する活動をどうとらえるか

何に対して、誰が、いつ、何をしたか、を全て記録



AWS Configとは



AWS Config
AWS Config Rules

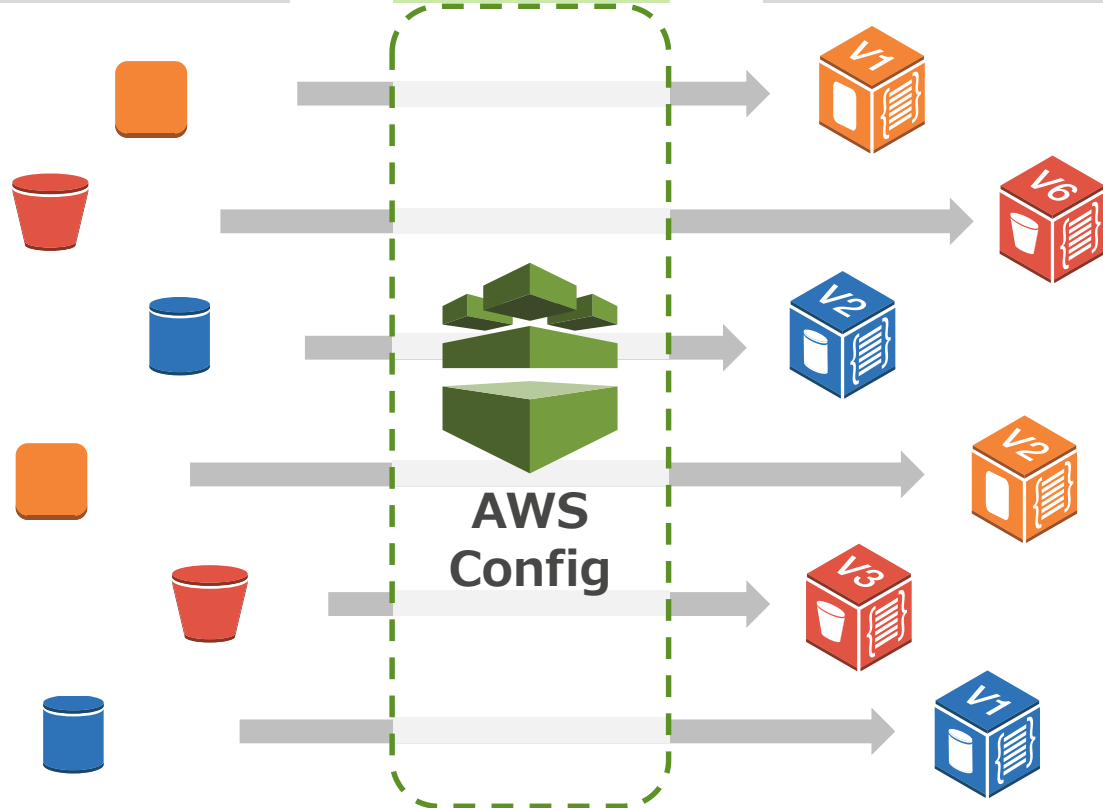
- **AWSリソースの構成変更をロギング**
- **履歴も保存**
 - 構成情報は定期的にスナップショットとしてS3に保存
 - 必要に応じSNSを使った通知も可能
- **ログはS3に保存**
- **あるべき状態の評価 (Rules)**
 - AWSが適用するルール
 - 独自のルールを適用
- **コスト**
 - 記録される設定項目につき 0.003 USD (1回の設定として前払いのみ)

AWS Config の動作イメージ

構成変更

記録

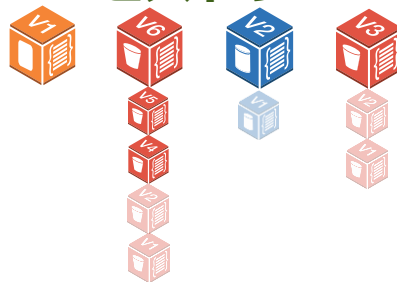
変更・更新



ストリーム



ヒストリ



スナップショット
(ex. 2017-06-02)

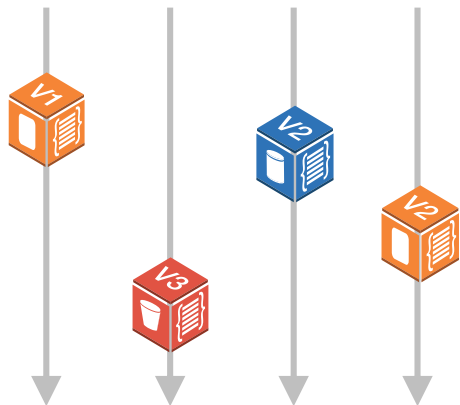


AWS Config 各機能の役割

ストリーム

(Configuration Stream)

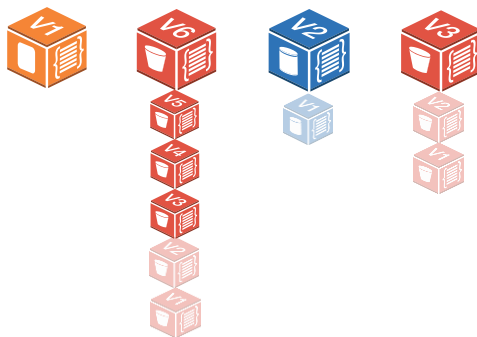
- リソースが作成/変更/削除されるたびに作成
- 構成ストリームに追加される
- SNSトピック連携可能



ヒストリー

(Configuration History)

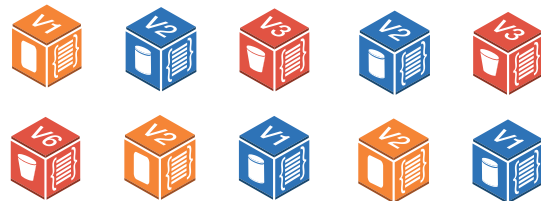
- 任意の期間における各リソースタイプの構成要素の集合
- リソースの設定履歴を、指定したS3バケットに保存



スナップショット

(Configuration Snapshot)

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



Snapshot @ 2017-06-02,
5:40pm

AWS Config が対応しているAWSリソース



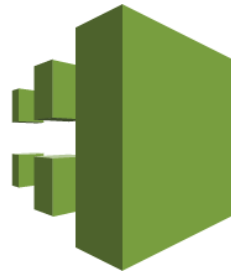
Amazon EC2
Instance, ENI...



Amazon VPC
VPC, Subnet...



Amazon EBS
Volumes



AWS CloudTrail



Amazon IAM



Amazon RDS



AWS Certificate
Manager



Amazon S3

TerminateしたEC2インスタンスも確認可能

Resource inventory

Status ?

Look up existing and deleted resources recorded by AWS Config. View compliance details for each resource or choose the Config timeline icon to see how a particular resource's configuration has changed over time.

Resources ☒

EC2: Instance

Resource identifier (optional)



Include deleted resources

Tag ☐

Tag key

Tag value (optional)

Look up

Choose the ⏮ icon to see Config timeline for a resource.

	Resource type	Resource identifier	Compliance	Config timeline
▶	EC2 Instance	i-██████████	Noncompliant with 1 rule	⏮
▶	EC2 Instance	i-██████████	Compliant	⏮
▶	EC2 Instance	i-██████████	Noncompliant with 1 rule	⏮
▼	EC2 Instance	i-02b0cff2 (deleted)	--	⏮



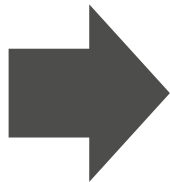
i-02b0cff2 Deleted

Resource i-02b0cff2 was deleted on March 21, 2015 at 11:58PM

AWS Config Rulesとは

AWS Config Rulesによるポリシー適合の評価

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

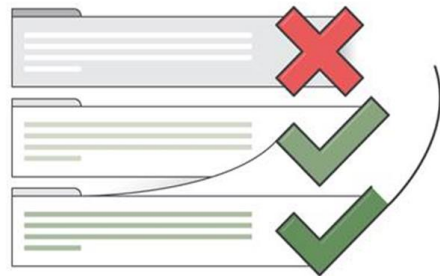
- 全てのEBCボリュームが暗号化されているか
- EC2インスタンスが適切にタグ付されているか等

AWS Managed Rules

- AWSにより定義・提供される
- AWSにより運用される
- 必要最低限のベーシック・ルール

Customer Managed Rules

- 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



AWS Managed Rules



AMIの確認



ルートアカウントの
MFA



ボリュームの
暗号化



CloudTrailの有効化



EIPのアタッチ



SSHの制限



EC2 in VPC



タグの付与



ポート設定

ルール評価実行のタイミング

Event-Based Evaluations

- 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

Periodic Evaluations

- 任意のタイミング
- 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

まとめ

AWS利用のためのルール策定と振り返り（再掲）



本セッションの目的（再掲）

AWSの「操作管理」の重要性

「操作管理」をどのように実現可能か

発展的内容

パートナー様のソリューション

システム
統合管理

資産管理

規則準拠・
コンプライアンス・
セキュリティ

暗号化

統合
ログ管理

AWS CloudWatch

AWS Trusted Advisor

AWS Service Catalog

AWS Inspector

AWS Key Management Service

AWSの「集中ロギング」

<https://aws.amazon.com/jp/answers/logging/centralized-logging/>

本セッションのFeedbackをお願いします

受付でお配りしたアンケートに本セッションの満足度やご感想などをご記入ください
アンケートをご提出いただきました方には、もれなく**素敵なAWSオリジナルグッズ**を
プレゼントさせていただきます



アンケートは受付、パミール3FのEXPO展示会場内にて回収させていただきます

AWS

S U M M I T

Thank you!

