＜データベース・セキュリティ・コンソーシアム主催＞

DBSC初冬セミナー 「クラウド環境下のデータ保全、フォレンジックについて」 2022/12/7

# クラウドフォレンジックを効率的に行うアーキテクチャ

ニューリジェンセキュリティ株式会社

大島 悠司

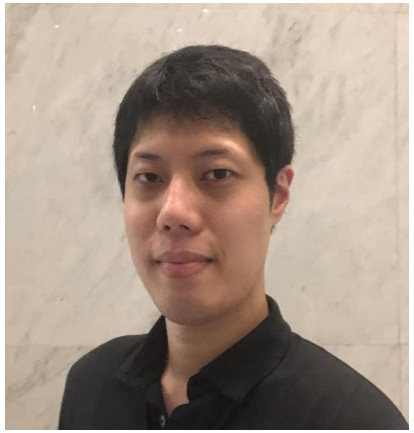
nuligen security

# 自己紹介

- 大島 悠司（おおしま ゆうじ）
  - ニューリジェンセキュリティ株式会社
  - クラウドセキュリティアーキテクト/基盤リーダー
  - 2022 APN ALL AWS Certifications Engineers

- 経歴
  - デジタルフォレンジック、マルウェア解析
  - スレットインテリジェンス、基盤運用
  - SOC、インシデントレスポンス
  - ニューリジェンの創業メンバーとして
    サービス開発/基盤構築運用/研究開発に従事

yuj1osm




野村総合研究所

# ニューリジェンセキュリティ 会社概要

nuligen security

nuage（仏：雲、くも）
＋
intelligence

クラウドネイティブセキュリティ分野において
intelligenceを提供する。

| | |
|---|---|
| 名称 | ニューリジェンセキュリティ 株式会社 |
| 所在地 | 東京都渋谷区神宮前六丁目12番18号 |
| 事業内容 | クラウドネイティブセキュリティサービス事業 |
| 資本金 | 2億円 |
| 設立年月日 | 2022年3月14日（事業開始：4月1日） |
| 出資比率 | 株式会社野村総合研究所：50%、株式会社ラック：50% |
| 役員構成 | 代表取締役社長　大野 祐一<br>代表取締役　小林 賢治<br>専務取締役　和田 博英<br>取締役　中間 俊英<br>取締役　佐藤 健 |

# 目次



nuligen security

# はじめに

# 世の中のクラウド事情

- 背景
  - 従来のオンプレミスのワークロードをクラウドへ移行する組織が増加

- クラウドのメリット
  - **初期費用がゼロ**
  - **柔軟性と俊敏性**により必要な分だけ即時に利用可能
  - マネージドサービスにより**運用負荷が軽減**

- 世の中のクラウド推進の流れ
  - 企業の**デジタルトランスフォーメーション（DX）**推進
  - 政府の**クラウド・バイ・デフォルト原則**

# クラウドフォレンジックの課題

- クラウドにおけるフォレンジックは従来のオンプレミスとは異なる

| | オンプレミス | クラウド |
|---|---|---|
| ワークロードの稼働時間 | 物理サーバや仮想マシン上で<br>**ワークロードが長時間稼働** | コンテナやサーバレスなどで<br>ワークロードが稼働するため、<br>**スケールにより短期間の稼働** |
| ログの保存期間 | 容量が許す限り**ログを長期間保存** | クラウドから提供される**ログは**<br>**種類が豊富**だが、**短期間で削除**される |
| フォレンジックの調査方法 | ディスク/メモリイメージや<br>ネットワークログなどと相関分析 | 監査ログやAPIコールログなどの<br>**多種多様なログを相関分析** |

クラウドの柔軟性とログの短期保存により**フォレンジックが困難**

↓

クラウドの**ログ特性をよく理解して、適切な設計**をしておくことが重要

# 本公演の概要

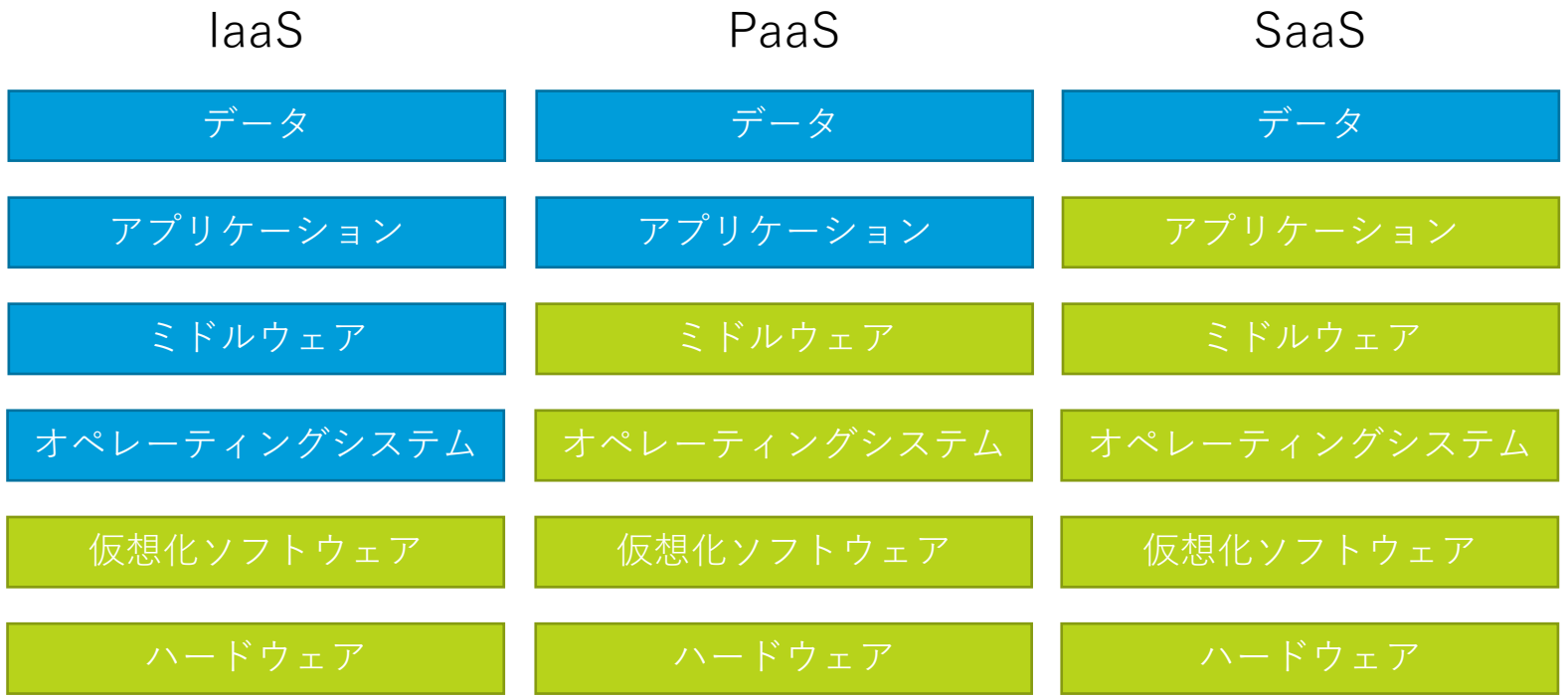
- **お話しすること**
  - クラウドの責任共有モデルから**利用者の責任**を説明
  - クラウドの**ログ特性**を説明
  - クラウドフォレンジックに効果的な**設計や運用**を説明

- **お話ししないこと**
  - 具体的なログの見方や調査方法

- 対象者
  - 企業やプロジェクトのクラウド管理者
  - セキュリティ担当者
  - セキュリティ責任者

# クラウドの責任共有モデル

# 代表的なXaaSにおける責任範囲



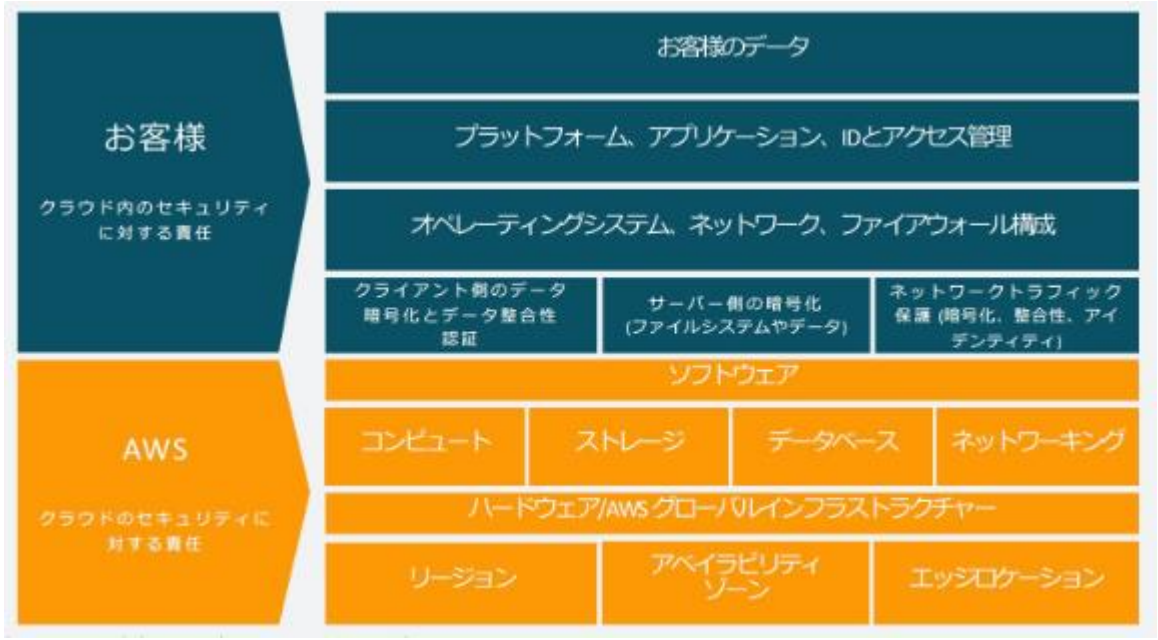

- クラウドサービスの提供形態によって責任範囲が異なる
- いずれの形態も**ユーザの責任がゼロになることはい**

# AWSのIaaSにおける責任共有モデル例（Amazon EC2の場合）

- AWS
  - ハードウェア/ソフトウェア/NWを含んだ
    インフラストラクチャすべての保護に責任を負う

- お客様
  - OS更新やセキュリティパッチ適用、
    AWSが提供するセキュリティ機能の設定など、
    セキュリティ構成と管理に責任を負う

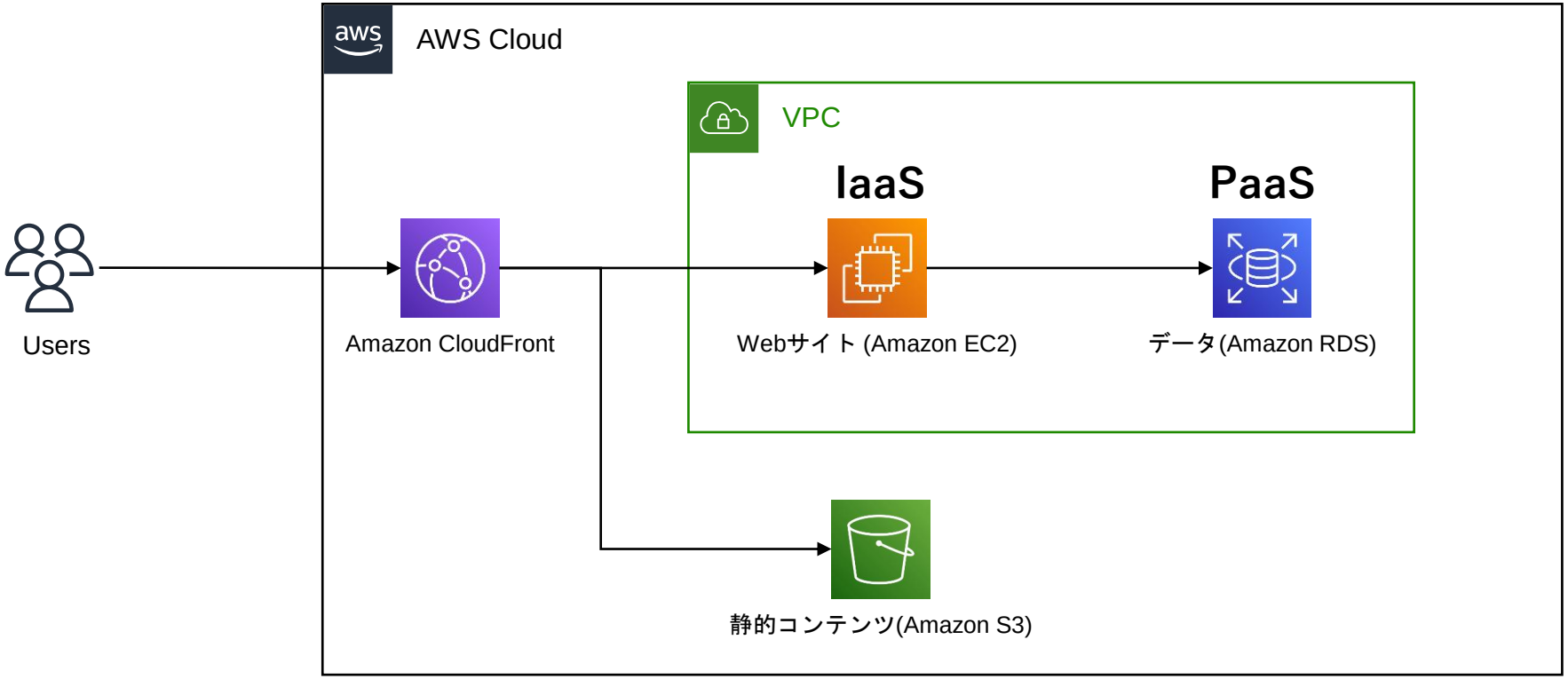
- **あくまでセキュリティ構成はユーザに委ねられる**




責任共有モデル｜AWS
https://aws.amazon.com/jp/compliance/shared-responsibility-model/

# ワークロード全体で考えるセキュリティ対策

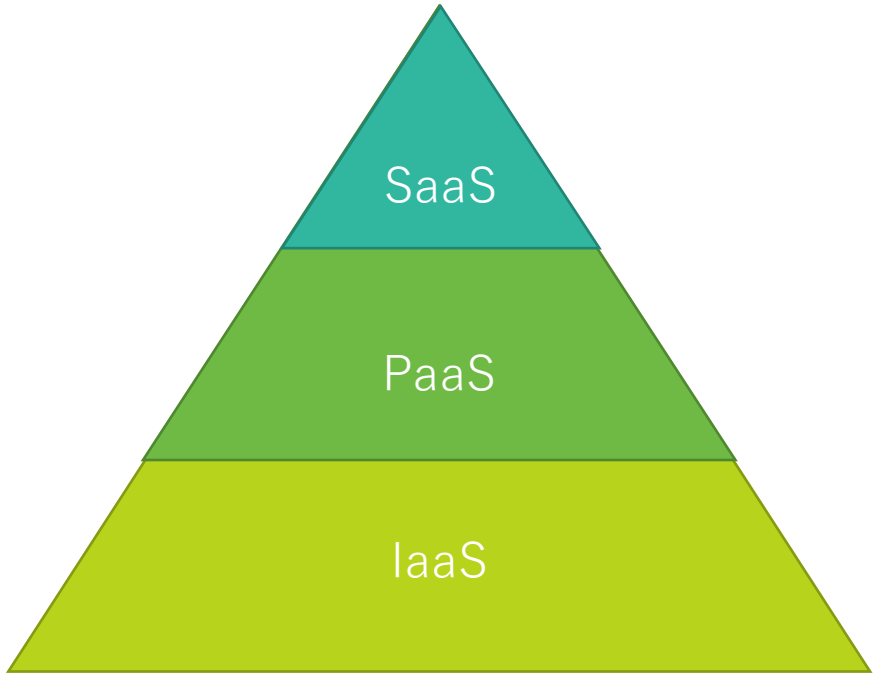
- 実際には、ワークロードは複数のサービスが組み合わさってできている
- **ワークロード全体として、責任境界をきれいに線引きできるわけではない**
- 重要なのは、**各サービスの機能を理解したうえで、ユーザがセキュリティ対策**を検討すること



# クラウドログの特性

# クラウド提供形態ごとのログ特性

- **SaaS**はアプリ側で用意された**ログが限定的**
  - **必要なログが取得されて**おり、それらを利用者は**いつでも利用可能か**、**契約前に確認**する
- **IaaS**は**多種多様なログ**を簡単に取得可能
  - エージェントのインストールが必要など、**ログ取得方法の制約が無いか確認**する




（サービス例）

Microsoft365, GoogleWorkspace

Amazon RDS, Azure SQL Database

Amazon EC2, Compute Engine

# クラウドのログ種別

- クラウドを使うことで**多くの種類のログが簡単に取得可能**
- それぞれの**ログから分かることや、各ログがどこで、いつまで保存されているかを把握**すること

| 種別 | 説明 |
| --- | --- |
| IAMログ | 認証ログ<br>サインインログなど |
| プラットフォーム管理ログ | クラウドプラットフォームに対する変更 |
| リソース管理ログ | リソースに対する変更<br>VMの作成/変更/削除など |
| リソースログ | リソースが生成するログ<br>Network FlowログやFirewallログなど |
| アプリケーションログ | VM上のアプリケーションが生成するログ |

# クラウドログの例

- CSV、XML、JSONなどで構造化されていることが多い
- クラウドやサービス機能によって**フォーマットが異なる**

Azure AD（サインインログ）

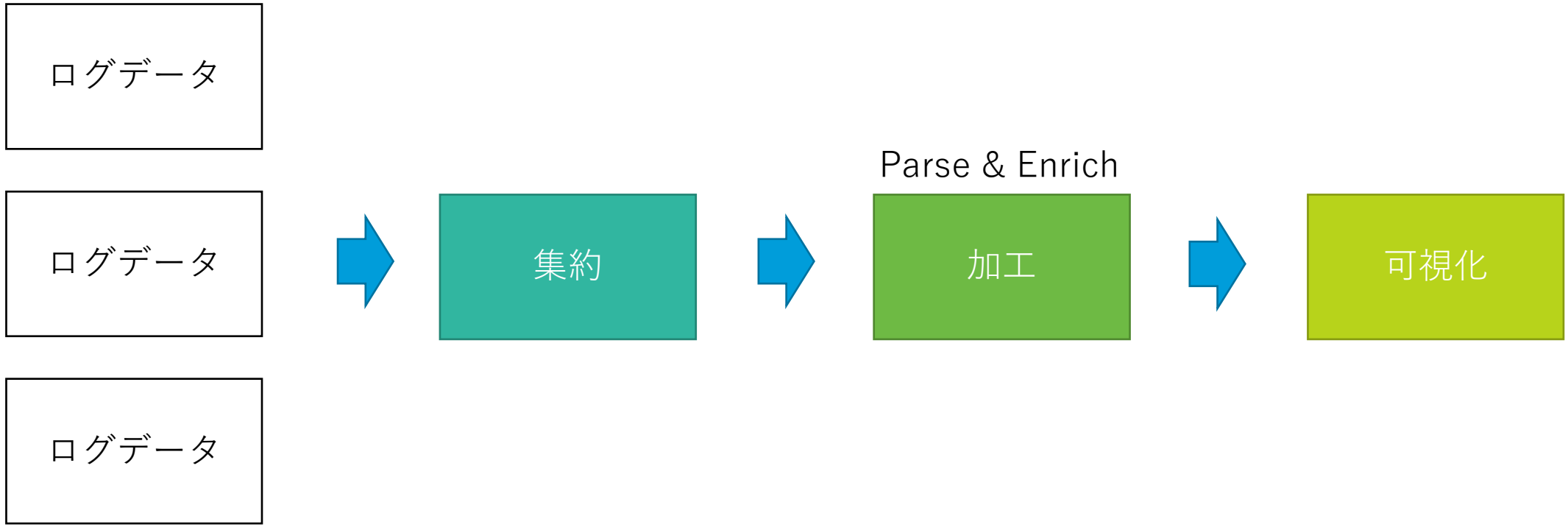

```
[
  {
    “id”: “9aaedfa6-7d22（省略）",
    "createdDateTime": "2022-11-26T07:46:00Z",
    “userDisplayName”: “ユーザゼロイチ",
    "userPrincipalName": “user01@sample.com",
    "userId": "75577223-289b （省略） ",
    "appId": "c44b4083-3bb0 （省略） ",
    "appDisplayName": "Azure Portal",
    "ipAddress": " 52.93. （省略） ",
    "ipAddressFromResourceProvider": null,
    "clientAppUsed": "Browser",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/ （省略） ",
    "correlationId": "1e8ba1b0-102f （省略） ",
                ~（省略）~
"status": {
        "errorCode": 0,
        "failureReason": "Other.",
        "additionalDetails": null
    },
                ~（省略）~
]
```


Amazon CloudTrailログ（コンソールログイン）


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDA（省略）",
    "arn": "arn:aws:iam::（省略）:user/user01",
    "accountId": "（省略）",
    "userName": "user01"
  },
  "eventTime": "2022-11-26T07:45:28Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "ap-northeast-1",
  "sourceIPAddress": "52.93. （省略） ",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/（省略）",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
            ~（省略）~
}
```

# ログの集約と処理

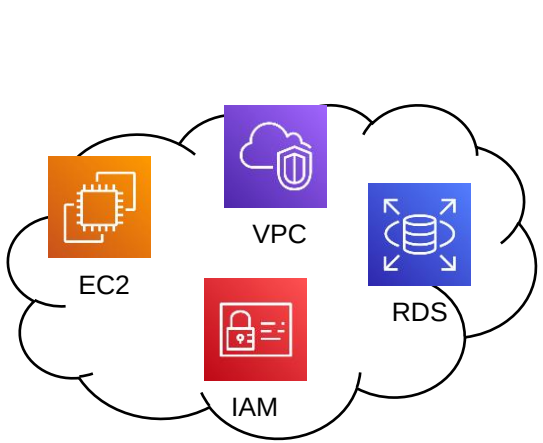
- **調査に必要なログを有効化**したうえで、**集約/加工し、可視化**できるようにする



# ログ収集と調査を考慮したアーキテクチャ

AWS
# AWS CloudTrail

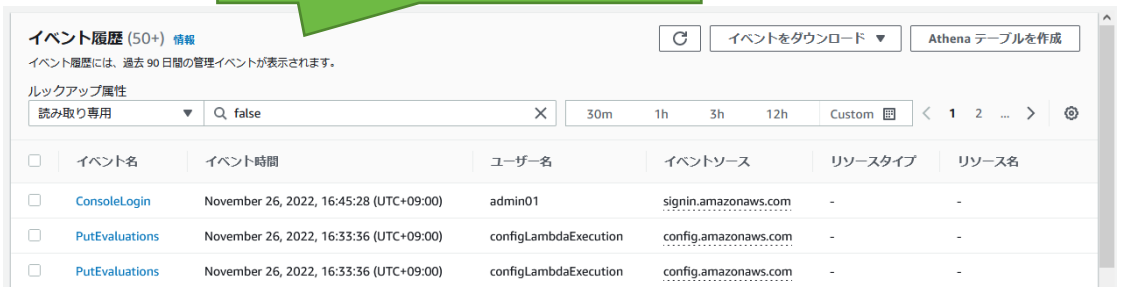
- 誰が、いつ、何に対して、何をしたか、全て記録
- ほぼ5分以内にログを確認可能
- ログ保持期間は90日 → 他サービスへ転送すること



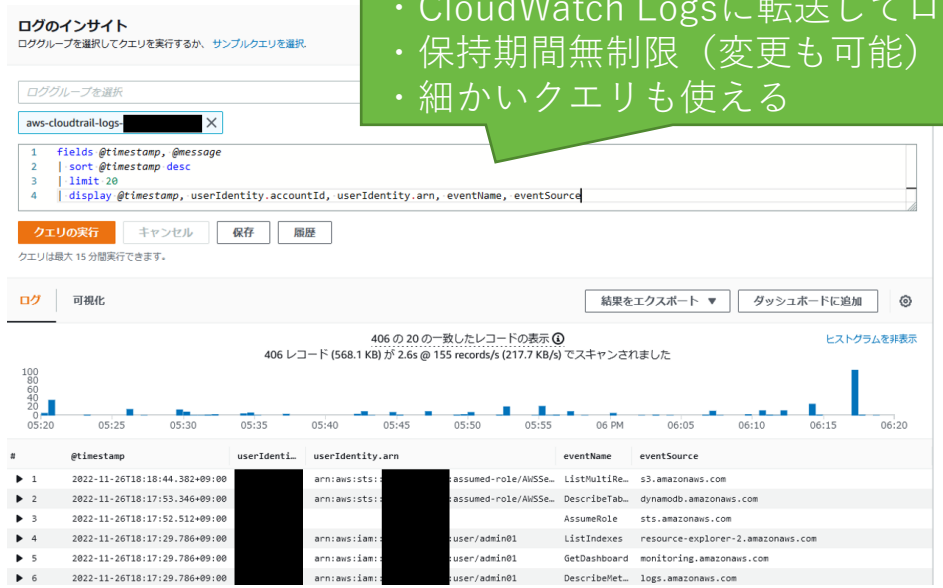

Users

AWS CloudTrail

・Trailの機能でログ調査
・保持期間90日




・CloudWatch Logsに転送してログ調査
・保持期間無制限（変更も可能）
・細かいクエリも使える

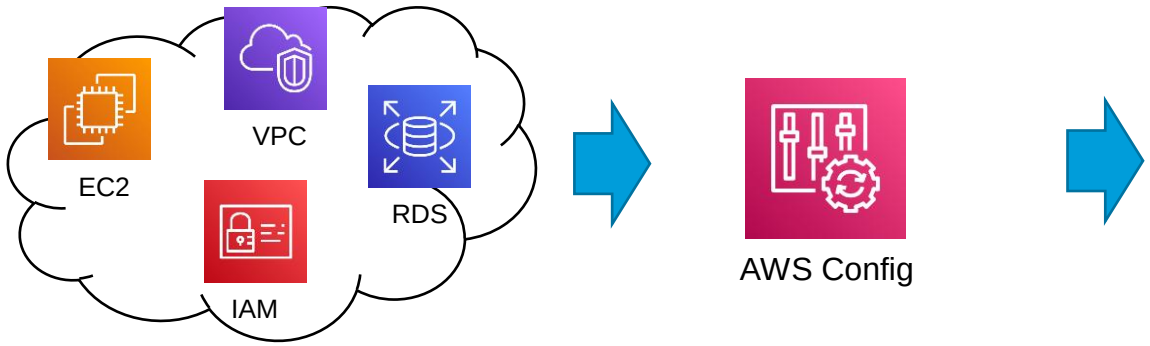



Amazon S3

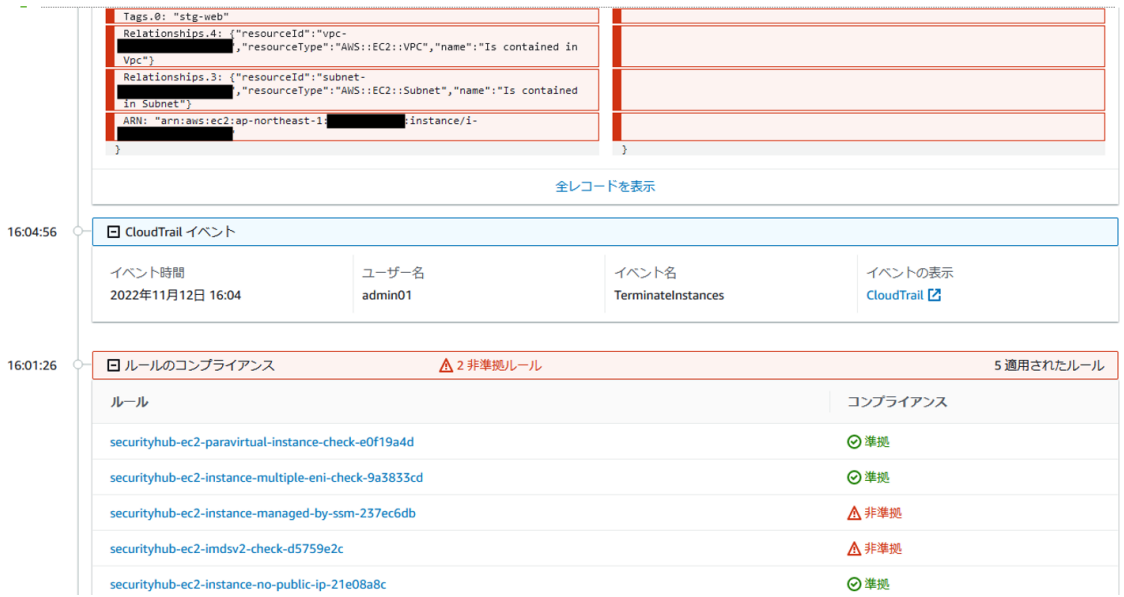
・S3に転送して長期保存
・生ログをExportして他のツールで調査も可能

AWS
# AWS Config

- **何に対して、いつ、何がされたか、全て記録**
- **Trailログとの相関分析**で、誰が実施したかも調査可能
- さらに、**リソースのコンプライアンスチェックも可能**
- **ログ保持期間はデフォルトで7年間**




・Configの機能でログ調査
・保持期間7年
・Trailログと相関分析可能





Amazon S3

・S3に転送して長期保存
・生ログをExportして他のツールで調査も可能

AWS

# AWS Severity Hubに集約

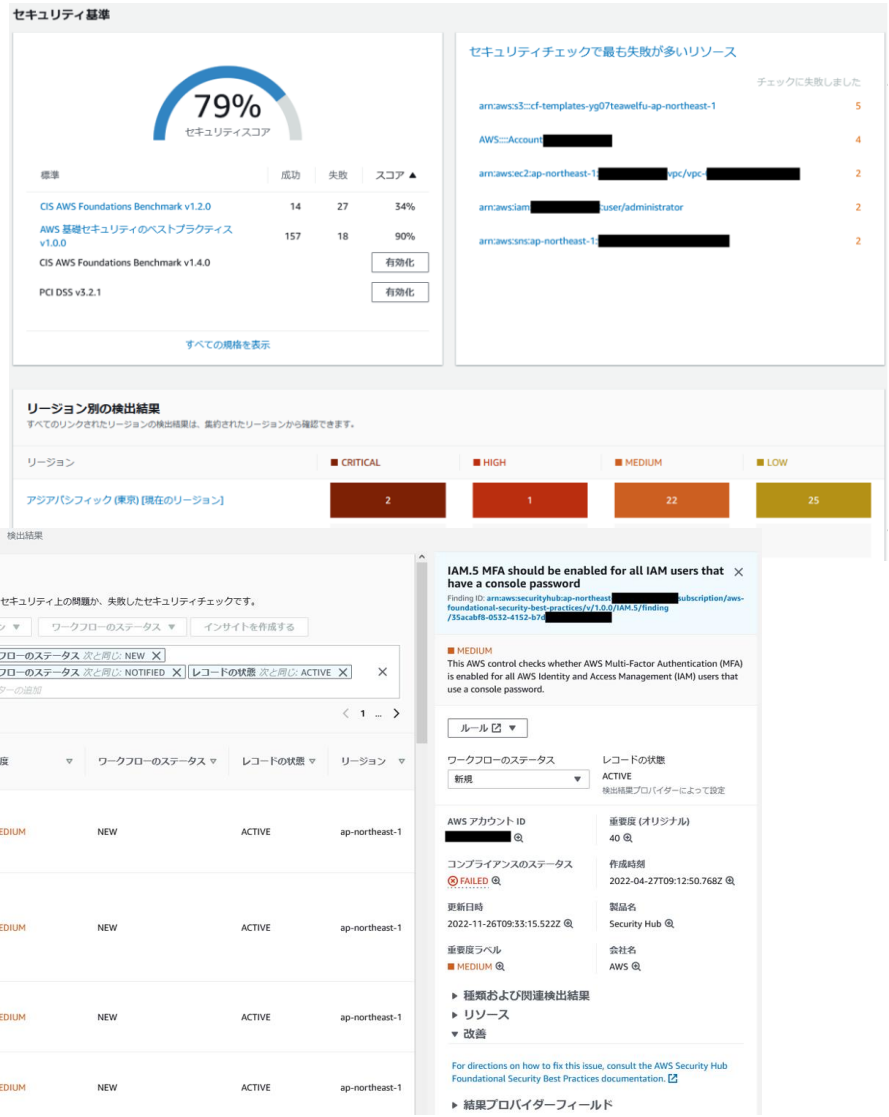
- 多くのセキュリティサービスはSecurity Hubに集約可能
- 検知の一元管理やスコア確認が可能

AWS Config
リソース構成管理

Amazon GuardDuty
Trailなどのログから脅威を検知

IAM Access Analyzer
IAMロールやS3の外部アクセスを検知

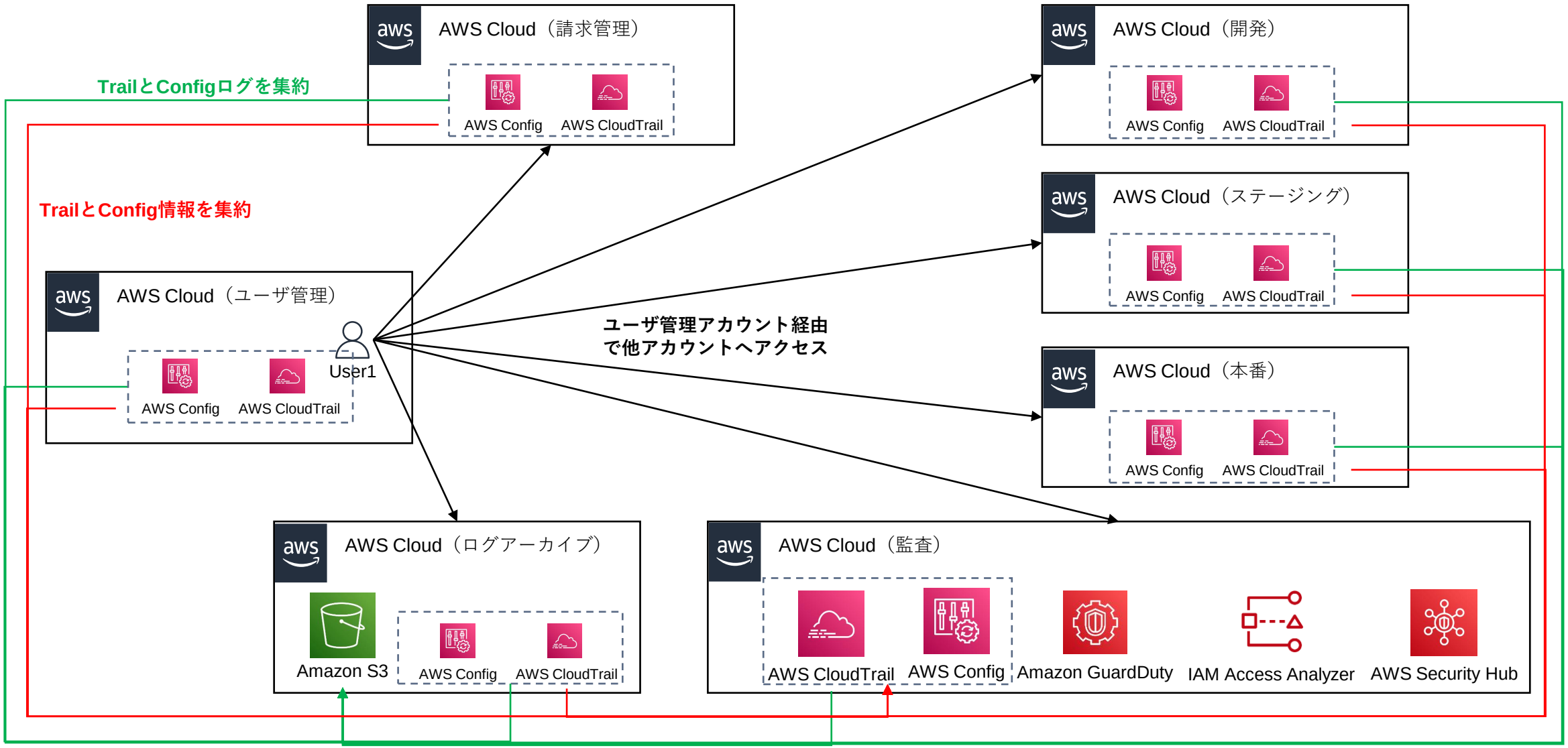
AWS Security Hub




・ドリルダウンで調査可能

AWS

# マルチアカウントの構成例



# Azureプラットフォームのログ

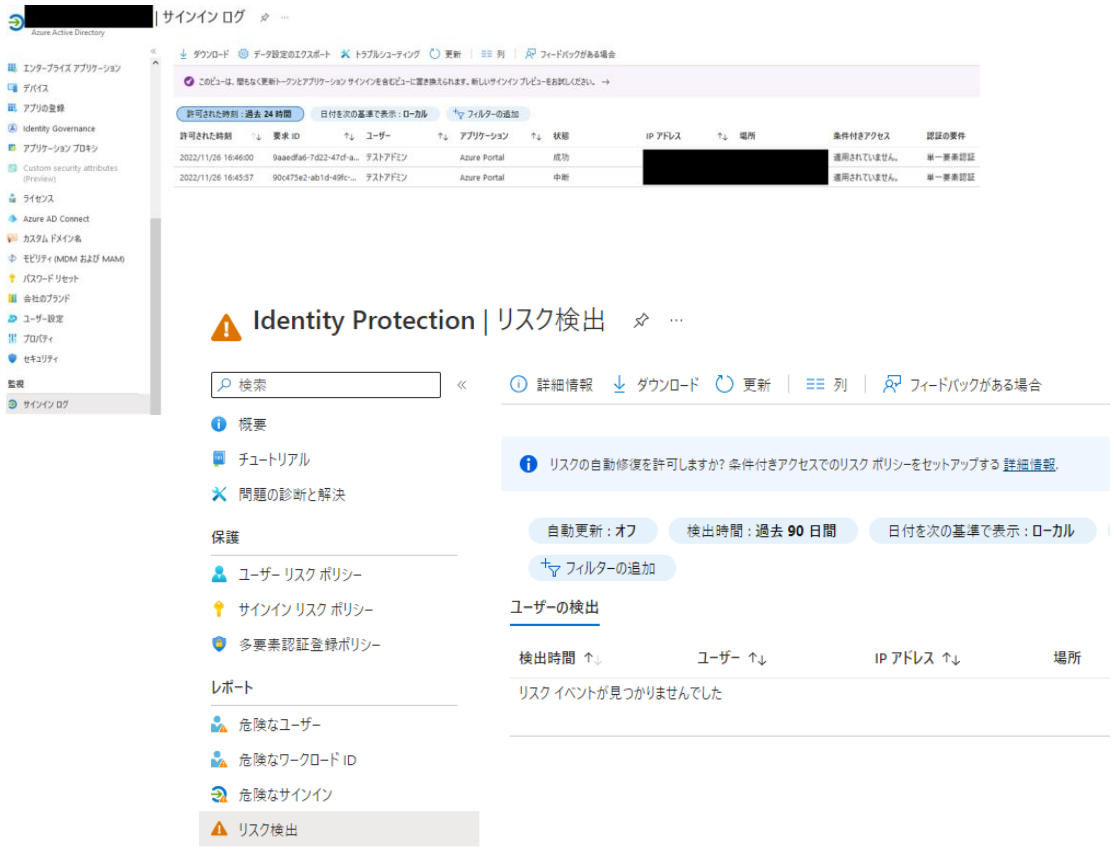
- Azureプラットフォームからは以下のような様々なレイヤーからログが取得できる

| 種別 | 説明 |
| --- | --- |
| テナントログ<br>（Azure ADログ） | Azure ADのようにユーザのテナント全体に関わるレイヤー<br>サインイン履歴やAzure ADで行われた変更の監査証跡 |
| サブスクリプションログ<br>（Azureアクティビティログ） | リソースの横断的なプラットフォームのレイヤー<br>リソースに対して行われた変更 |
| リソースログ | リソースの内部操作に関する情報<br>キーコンテナからのシークレット取得やデータベースへの要求 |
| OSログ | エージェントをインストールすることで収集できるログ<br>CPU/メモリなどのOSリソースに対するメトリック/ログ |
| アプリケーションログ | アプリケーションのパフォーマンスや操作に関するログ |

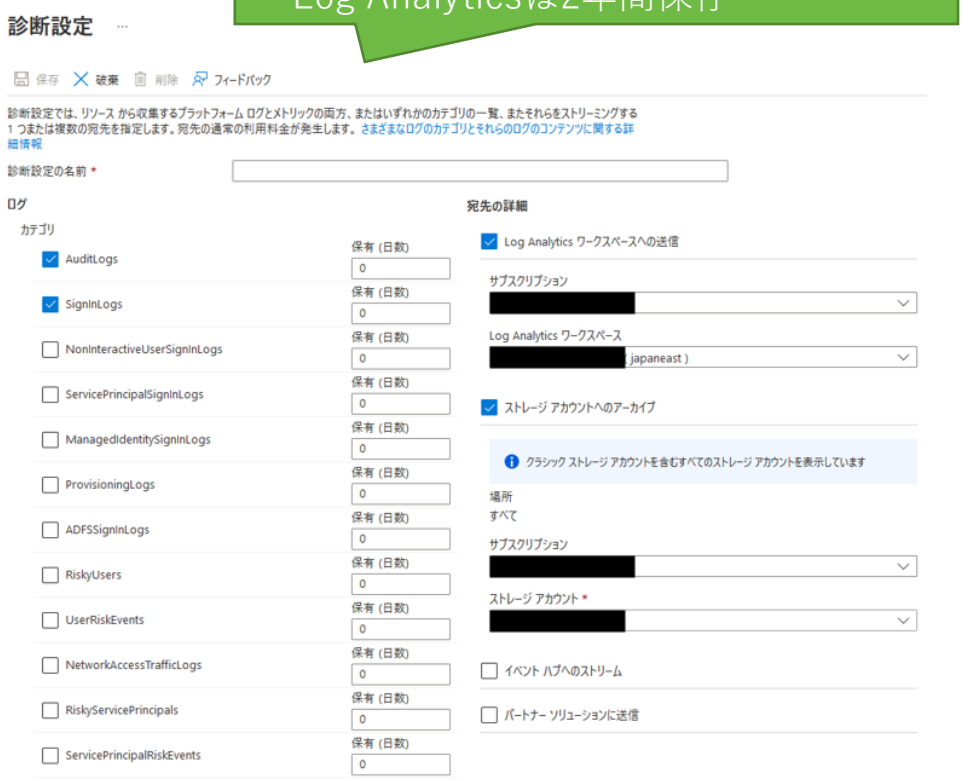
Azure

# Azure ADログ

- サインインログや監査ログは、**反映に5分**程度、**30日間保持**
- Identity Protectionのリスク検出ログは、**反映に最大8時間**、**90日間保持**
- **いずれのログも他サービスへ転送**すること

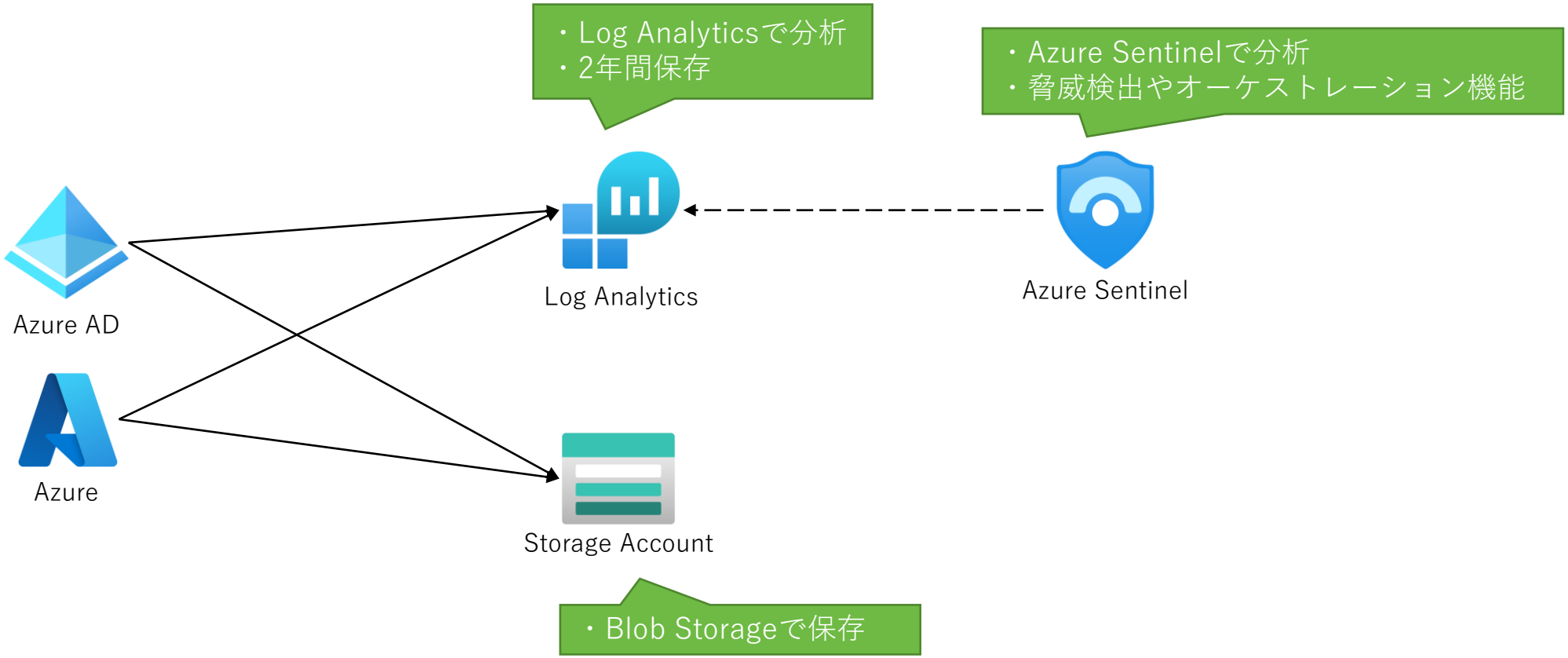



・Azure ADの診断設定で、任意のログを複数のサービスに転送可能
・Log Analyticsは2年間保存



# Azureのログ集約例

- Azure ADログとAzureのアクティビティログを分析、保存それぞれに転送
- Azure Sentinelを通した分析も可能



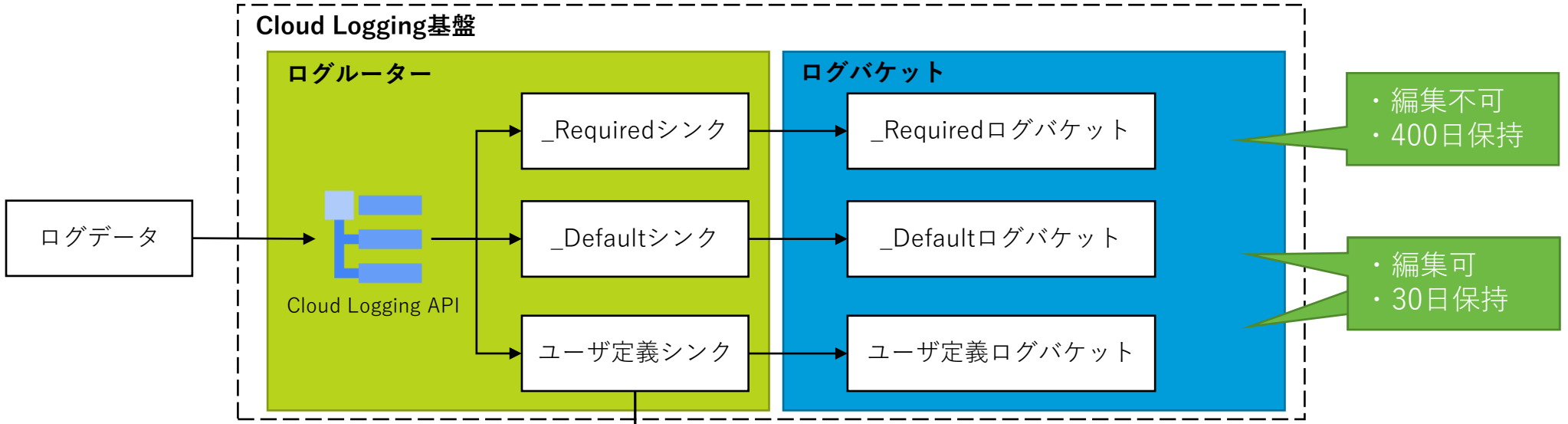
GCP
# Cloud Loggingが扱うログ

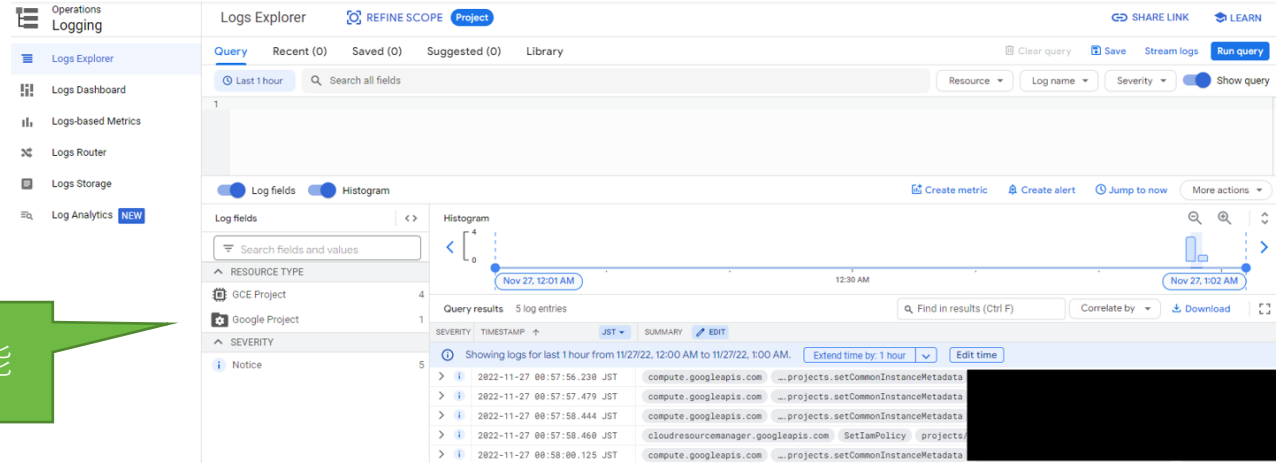
- Cloud Loggingは以下のログを扱う
- 特に注意が必要なのは、**セキュリティログは対象によってデフォルト設定や保存先が異なる**

| 種別 | 説明 |
|---|---|
| Google Cloudが生成するログ | Google Cloudの様々なサービスから転送 |
| ユーザが生成するログ | APIやVMのエージェントから転送 |
| セキュリティログ | Cloud Audit Logsのログ<br>Google CloudのAPIコールログであり、以下の種類がある<br>・管理アクティビティ監査ログ [デフォルトで**有効**、**_Required**バケット]<br>・データアクセス監査ログ [デフォルトで**無効**]<br>・システムイベント監査ログ [デフォルトで**有効**、**_Required**バケット]<br>・ポリシー拒否監査ログ [デフォルトで**無効**]<br>アクセスの透過性ログ<br>Googleサポートがアクセスした際のログ [デフォルトで**有効**、**_Required**バケット] |
| マルチクラウドとハイブリッドクラウドのログ | アプリケーションのパフォーマンスや操作に関するログ<br>AzureやAWS、オンプレミスから取り込んだログ |

GCP
# Cloud Logging概要

- Cloud Logging APIにログを送信、ログルーターのシンク設定で**ログバケット、他サービスに転送**

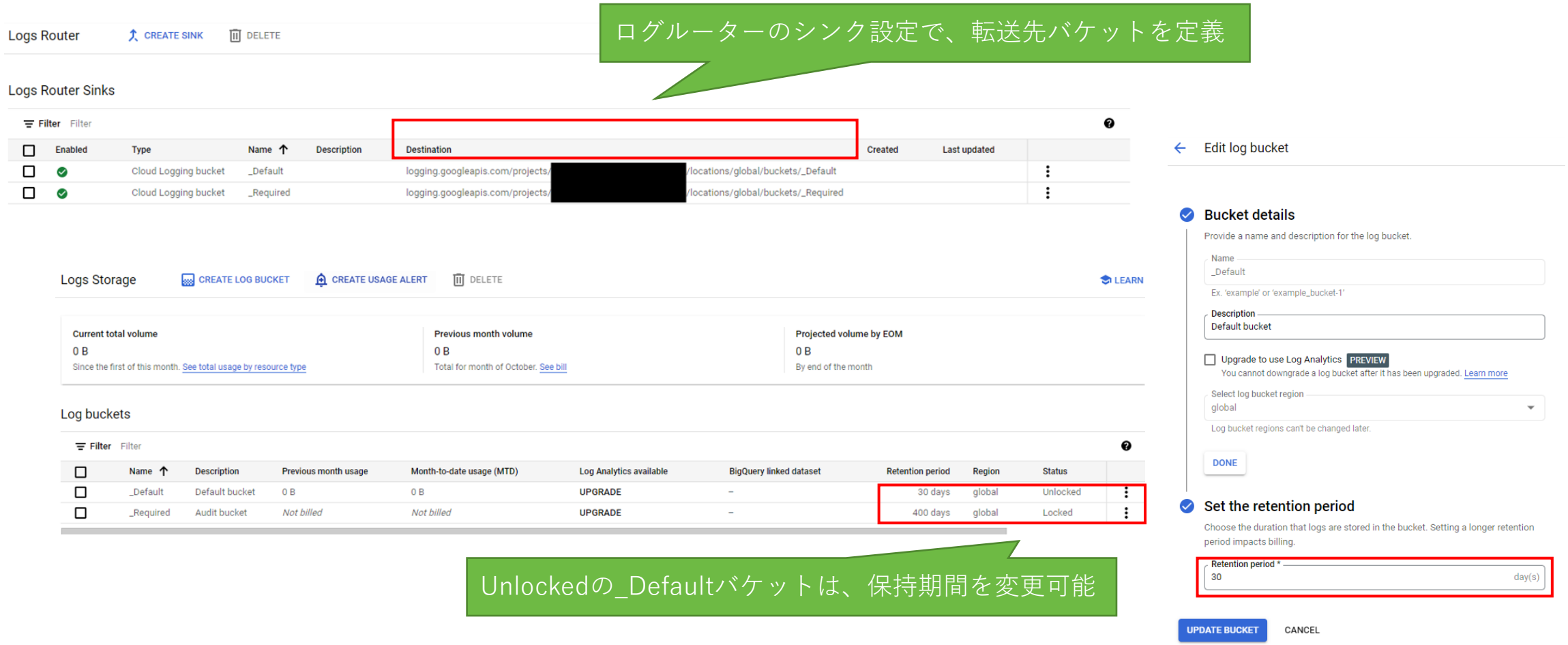



・Log Explorerで検索可能

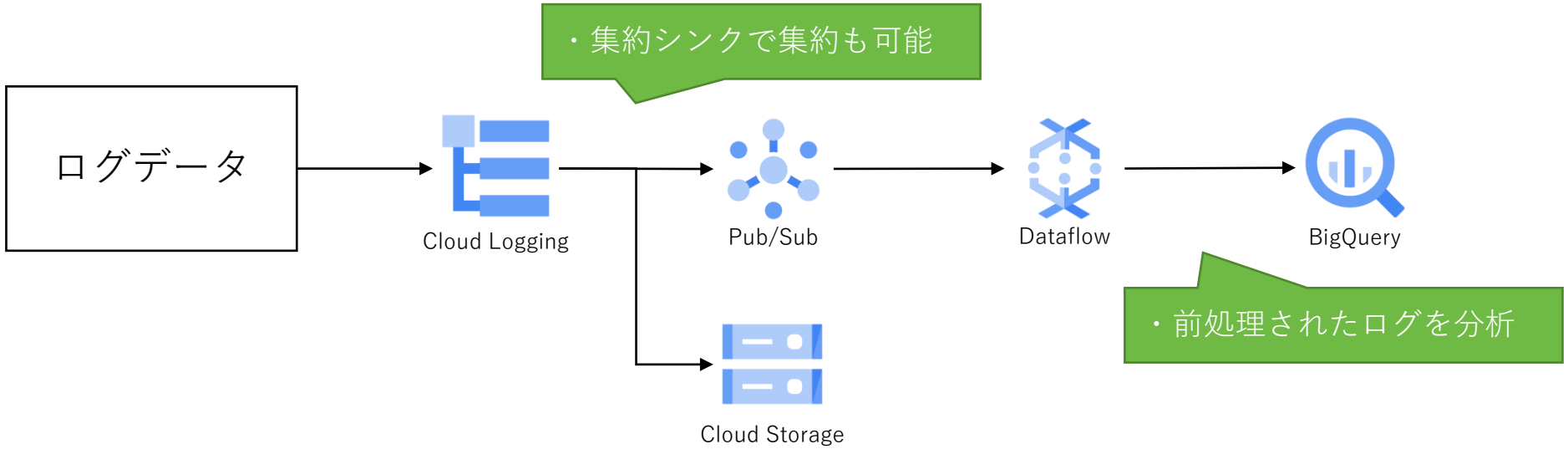
GCP
# ログルーターとログバケット

- 各種設定は以下の通り



GCP
# GCPのログ集約例

- ログデータをCloud LoggingからPub/Subトピックに送信し、Dataflowで前処理
- 前処理されたデータをBigQueryで調査
- 長期保存用にCloud Storageにも保存
- 複数プロジェクトのログを集約シンクで、1つのプロジェクトに集約も可能



# クラウドログの特徴まとめ

- どういう**シナリオに対して、どのログが使える**か
- その**ログは有効化**されていて、**保持期限**はいつまでか

| シナリオ | AWS | Azure | GCP |
|---|---|---|---|
| ログイン<br>パスワードスプレー<br>ありえない移動 | CloudTrailログ<br>90日 | Signinログ<br>30日 | Login Auditログ<br>400日 |
| ログイン後の挙動<br>横展開<br>キーの漏洩 | CloudTrailログ<br>90日 | Activityログ<br>90日 | System Eventログ<br>400日 |

# CSPM製品を使う

- 自社のクラウドセキュリティ対策に心配があれば、CSPMで設定チェックをすることも可能
- CloudscortでCSPMやVM（脆弱性管理）で求められるタスクを支援

## AWS運用ご担当者のセキュリティに関するお困りごとを解決します！

1 新しい脅威への対処が大変


2 大量に来る脆弱性通知


3 どう対応するかわからない


クラウドセキュリティに関するお悩みを解決

AWSセキュリティ機能強化&セキュリティ運用支援

cloudscort

① **AIおよび高度脅威インテリジェンスによる攻撃検知・対応**
AIによる攻撃検知とNRIセキュア・ラックのインテリジェンス利活用により、常に新しい脅威へ対処します。

② **セキュリティ専門家の知見に基づいた検知の絞り込み**
対応優先度の高い内容への絞り込みや検知内容の集約を行い、無駄のない運用を支援します。

③ **AWSセキュリティに関する運用のサポート**
脆弱性の内容だけでなく対策方法なども添えて通知することで、円滑なセキュリティ運用を実現します。
さらに、問い合わせ窓口やプロフェッショナルサポートによる支援も可能です。



CSPM、VM、WAF、NFWなどの運用を楽にする

## Cloudscort サービス概要

- Cloudscortは、クラウドネイティブ機能を強化する(使いやすくする)サービスです
- 機能群はSaaS型でご提供します。また、プロフェッショナルサービスは部分的なMSSとしてご提供します

| | クラウド機能 | Cloudscortのサービス | |
|---|---|---|---|
| 検知・対応 | Web Application Firewall<br>Webファイアウォール | WAFやNWFWの運用で求められるタスクを支援<br>• 最新攻撃パターンの自動適用<br>• 検知した攻撃通信の自動分析<br>• 被害拡大防止のための通信先遮断<br>• ユーザ要望によるカスタムルールの設定 | --- 共通機能 ---<br>• 高度脅威インテリジェンス（NRIセキュア、ラック）<br>• CISOダッシュボード<br>• プロフェッショナルサービス（MSS:セキュリティ運用支援） |
| | Network Firewall<br>Networkファイアウォール | | |
| 未然防御 | CSPM<br>クラウド設定管理 | CSPMやVMの運用で求められるタスクを支援<br>• 検知した脆弱性の解説・対策情報付与<br>• クラウド資産価値×脆弱度に応じた対応優先順位の判定<br>• セキュリティサービスの自動最適化 | |
| | VM<br>脆弱性管理 | | |



※ 実装見込みの情報を一部含みます。

# まとめ

# まとめ

- 世の中のクラウド移行が進む中、**フォレンジックのアプローチも変化**している
- 責任共有モデルであっても、最終的な**セキュリティ対策はユーザで検討**する必要がある
- **クラウドログは多種多様**であり、調査にあたって非常に役に立つ
- クラウドログを扱うときは以下に気をつける必要がある
  - **デフォルトで有効/無効**か
  - **保持期間はいつまで**か
  - どういった**サービスに連携できる**か
  - **フォーマットは分析で扱える**ものか
- 各ログの特性を考慮し、**収集・分析しやすいような基盤設計**をする


nuligen
security