



AWS
Black Belt
Online Seminar

【AWS Black Belt Online Seminar】 Amazon Macie

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 保里 善太

2018.04.04

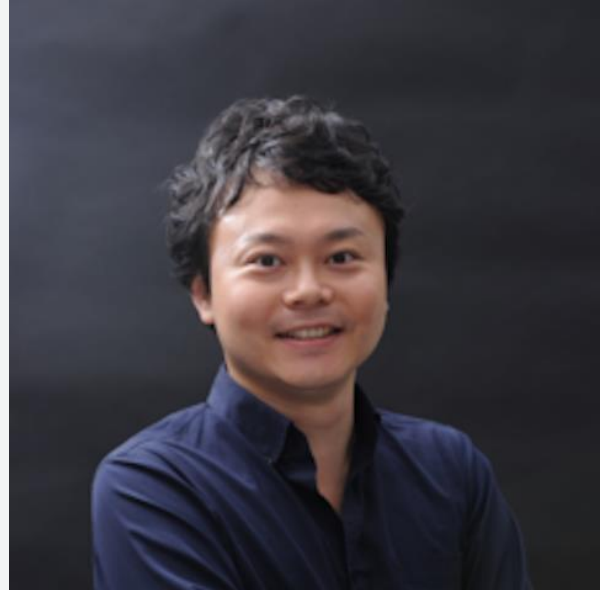


自己紹介

保里 善太(ほり ぜんた)

技術統括本部

ソリューションアーキテクト



中規模のスタートアップから大手まで、主にFinTech/ゲーム領域をご支援させていただいています。

好きなAWSのサービス:

Amazon Macie/Amazon GuardDuty/Amazon SageMaker

内容についての注意点

- 本資料では2018年4月4日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっております。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。

AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

Agenda

📦 クラウドでのデータ保護

📦 Amazon Macieとは

📦 使い始めるには

📦 機能・操作について

📦 ユースケース

📦 Macieの料金

Agenda

クラウドでのデータ保護

 Amazon Macieとは

 使い始めるには

 機能・操作について

 ユースケース

 Macieの料金

データの保護に関する課題

企業内の機密データにまつわるリスクを知りたい

どこにどのようなデータがあるのかわからない

個人情報(PII)や個人医療情報(PHI)が外部に晒される可能性はないか知りたい



どのような形でデータが保存され誰に共有されているのかわからない

機密データに関するインシデント発生時に対処したい

保存されているデータの分類をニアリアルタイムでできないだろうか

セキュリティやコンプライアンスの規制対象となるデータを特定したい

データ漏えいの脅威

内部の脅威

外部からの脅威

偶発的な脅威

社員によるアクセス権限の設定ミスや操作ミスによる機密データの漏えい

顧客や取引先のミスによる情報の漏えい

意図的な脅威

社員や元社員が金銭目的や怨恨による理由で社内の機密情報を持ち出す

セキュリティホールや不十分な権限管理を突かれての不正アクセスによる情報の漏えい

近年のセキュリティインシデント

内部の脅威

外部からの脅威

偶発的な脅威

オブジェクトストレージ
S3の設定ミスにより個人
情報を誤まって不特
定多数に公開

ある家具販売メーカー
で取引先の個人情報を
含むノートパソコンと携
帯電話が盗難された

意図的な脅威

大手教育教材会社でシ
ステム開発・運用をして
いた元社員が業務上入
手した個人情報を名簿業
者に売却した

大手決済会社への不正
アクセスによる個人情
報の大量流出が発生

データ保護に関する様々な規制

📦 GDPR

- 2018/5/25から施行されるEUの一般データ保護規則
- 企業の所在地には関わらずEU圏の住民のデータを取り扱う企業は全てが対象
- 違反した場合には高額な制裁金も
 - 企業の場合、年間売上の4%、または2000万ユーロ(約26億円)のいずれか高い方

📦 3省4ガイドライン

- 厚生労働省、経済産業省、総務省の3省が出している4つのガイドライン
- 電子化された医療情報(電子カルテ等)をクラウドなどの外部に保存する際に遵守する必要があるガイドライン

📦 PCI DSS

- クレジットカード会員情報の保護のための規制



📦 HIPAA

- 米国における医療保険の相互運用性と説明責任に関する法令



データ保護のために必要なこと



どこにどのような
データがあるのか
を知ること



データ保護のために必要なこと



どこにどのような
データがあるのか
を知ること



データがどのように
扱われているのか
を知ること



データ保護のために必要なこと



どこにどのような
データがあるのか
を知ること



いつでもデータを見
てリスクを把握
できること



データがどのように
扱われているのか
を知ること



データ保護のために必要なこと



どこにどのような
データがあるのか
を知ること



いつでもデータを見
てリスクを把握
できること



データがどのように
扱われているのか
を知ること



問題があった場合に
警告を発すること



機密データを検出・分類・リスク評価・警告

amazon
macie



Agenda

📦 クラウドでのデータ保護

📦 **Amazon Macieとは**

📦 使い始めるには

📦 機能・操作について

📦 ユースケース

📦 Macieの料金

Amazon Macieの4つのアプローチ



どこにどのような
データがあるのか
を知ること



いつでもデータを見
てリスクを把握
できること



データがどのように
扱われているのか
を知ること



問題があった場合に
警告を発すること



Amazon Macieの4つのアプローチ



データの検出と 分類



ストレージの
データを自動
分類

いつでもデータを見
てリスクを把握
できること



データがどのように
扱われているのか
を知ること



問題があった場合に
警告を発すること



Amazon Macieの4つのアプローチ



データの検出と 分類



ストレージの
データを自動
分類

いつでもデータを見
てリスクを把握
できること



イベント監視



CloudTrailデー
タを監視

問題があった場合に
警告を発すること



Amazon Macieの4つのアプローチ



データの検出と分類



ストレージの
データを自動
分類

データの可視化



分類したデータ
やアクセスを
ダッシュボード
に表示

イベント監視



CloudTrailデー
タを監視

問題があった場合に 警告を発すること



Amazon Macieの4つのアプローチ



データの検出と分類



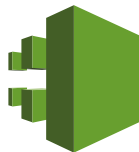
ストレージの
データを自動
分類

データの可視化



分類したデータ
やアクセスを
ダッシュボード
に表示

イベント監視



CloudTrailデー
タを監視

アラートによる警告



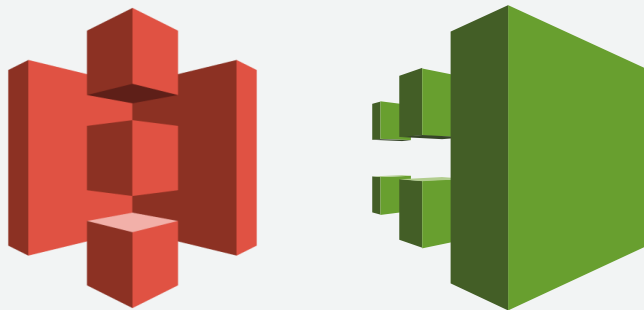
アラートレベル
に応じた警告
を行う

Amazon Macieとは



- ❏ 決められたルールや機械学習を利用してAWSに保存された機密データを自動的に検出、分類をしてそれぞれのデータに対してリスク評価する
- ❏ データへのユーザーアクセスや権限変更等のCloudTrailイベントを監視、リスク評価する
- ❏ 取得した情報をダッシュボードで可視化する
- ❏ 決められたルールや機械学習を利用して異常を検知し、アラートを発する
- ❏ Macie自体はインシデントレスポンスはしない
- ❏ CloudWatch Eventsと連携してインシデントレスポンスの仕組みを構築できる
- ❏ US East(バージニア)とUS West(オレゴン)の2リージョンで提供

監視対象のデータソース



- ❏ 現状ではAmazon S3とAWS CloudTrailのみが監視対象
- ❏ Macieと同一リージョンのS3バケットが監視対象
- ❏ 他のアカウントのS3バケットも監視できる



Amazon
EBS



Amazon
RDS



Amazon
DynamoDB



Amazon
EFS



AWS Glue

- ❏ その他の AWS のデータストアについては2018年の後半にサポートされる予定

<https://aws.amazon.com/jp/maciek/faq/>

Macieの動作イメージ



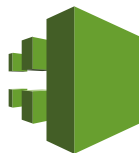
データの検出と分類



S3オブジェクト

S3バケットプロパティ

イベント監視



CloudTrail data

リスク評価

リスクレベル
(1-10)に応じた
リスク分類

データの可視化



アラートによる警告



Critical,
High,
Medium,
Low
Informational

匿名アクセス
不正アクセス



CloudWatch
Events

Agenda

📦 クラウドでのデータ保護

📦 Amazon Macieとは

📦 **使い始めるには**

📦 機能・操作について

📦 ユースケース

📦 Macieの料金

Macie を有効にする

📦 リージョンを選択

- 現状ではUS East(バージニア)かUS West(オレゴン)のみ

📦 AWS CloudTrailがアカウントで有効になっていること

📦 MacieにAWSアカウントへのアクセスを許可するIAM Roleを作成

- CloudFormationスタックテンプレートが用意されているので実行する

amazon Macie US West (Oregon) ▼

Enable Amazon Macie

Use this page to configure Amazon Macie. [Learn more](#)

Region
US West (Oregon) ▼ [Learn more](#)

Requirements

- ✓ IAM roles created [Learn how to create the required IAM roles](#)
- ✓ AWS CloudTrail enabled [Learn how to create AWS CloudTrail](#)
After you enable Macie, the service will process and analyze your CloudTrail data for the last 60 days starting today. For details about usage-related charges, see <https://aws.amazon.com/macie/pricing/>.

Permissions

By choosing Enable Macie, you are providing the service with permissions to analyze AWS CloudTrail logs and events to classify and protect your data. You can disable Macie at any time and thus stop it from processing and analyzing AWS CloudTrail logs and events.

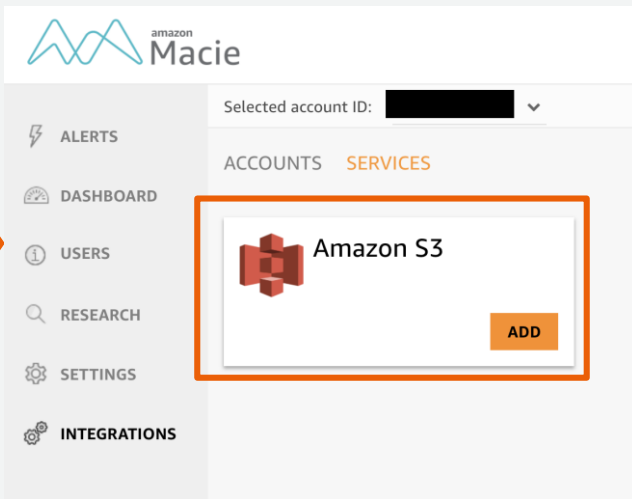
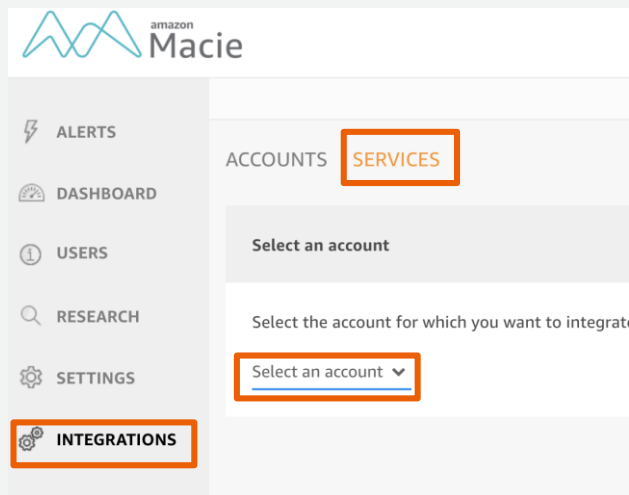
CANCEL ENABLE MACIE

Macieで保護するS3バケットの追加 (1/2)

Amazon Macieで保護対象に指定するS3バケットを選択します

1. INTEGRATIONS→SERVICESを選択してSelect an accountから連携するアカウントを選択

2. Amazon S3を選択してADDをクリック



Macieで保護するS3バケットの追加 (2/2)

Amazon Macieで保護対象に指定するS3バケットを選択します

3. 保護対象に指定するS3バケットを選択して
[REVIEW AND SAVE]をクリックして追加する

※ 他のアカウントのS3バケットを保護対象
に含める場合には
INTEGRATIONS→ACCOUNTを選択して
Member AWS accountsからアカウントIDを
入力する。

Total selected resources: 2

You can select up to 250 S3 buckets and prefixes.

When you specify an S3 bucket, by default, Macie only classifies objects that are added to the bucket after your bucket selection is complete. If you select "Classify all", Macie classifies all existing objects in the S3 bucket. Make sure you know the size of your S3 bucket before you select "Classify all" since this can significantly affect your content classification costs. For more information, see [Amazon Macie Pricing](#) and [Specify data for Macie to monitor](#).

All Buckets

<input type="checkbox"/>	Name	Total size	Total processed	Total cost estimate	Classify all
<input type="checkbox"/>	[REDACTED]	9.22 MB	9.23 MB	\$0.05	<input type="checkbox"/>
<input checked="" type="checkbox"/>	aws-athena-[REDACTED]	71.95 KB	164.17 KB	\$0.00	<input type="checkbox"/>
<input type="checkbox"/>	aws-athena-[REDACTED]	369.31 KB	443.30 KB	\$0.00	<input type="checkbox"/>
<input type="checkbox"/>	[REDACTED]	472.28 MB	497.33 MB	\$2.43	<input type="checkbox"/>
<input type="checkbox"/>	pinpointtest-[REDACTED]	Not available	Not available	Not available	<input type="checkbox"/>
<input checked="" type="checkbox"/>	zen-macie-test	1.11 MB	1.12 MB	\$0.01	<input type="checkbox"/>

The screenshot shows the Amazon Macie console interface. On the left is a navigation menu with options: ALERTS, DASHBOARD, USERS, RESEARCH, SETTINGS, and INTEGRATIONS. The 'INTEGRATIONS' option is selected. The main content area shows the 'ACCOUNTS' tab active. Under 'AWS accounts', there is a field for 'Master AWS account:' followed by a redacted ID. Below that is a section for 'Choose retention duration for S3 metadata' with 'Number of months: 1'. At the bottom, there is a button labeled 'Member AWS accounts' which is highlighted with an orange box.

Agenda

📦 クラウドでのデータ保護

📦 Amazon Macieとは

📦 使い始めるには

📦 **機能・操作について**

📦 ユースケース

📦 Macieの料金

データの検出と分類



データの検出と分類



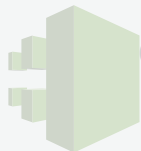
ストレージの
データを自動
分類

データの可視化



分類したデータ
やアクセスを
ダッシュボード
に表示

イベント監視



CloudTrailデー
タを監視

アラートによる警告

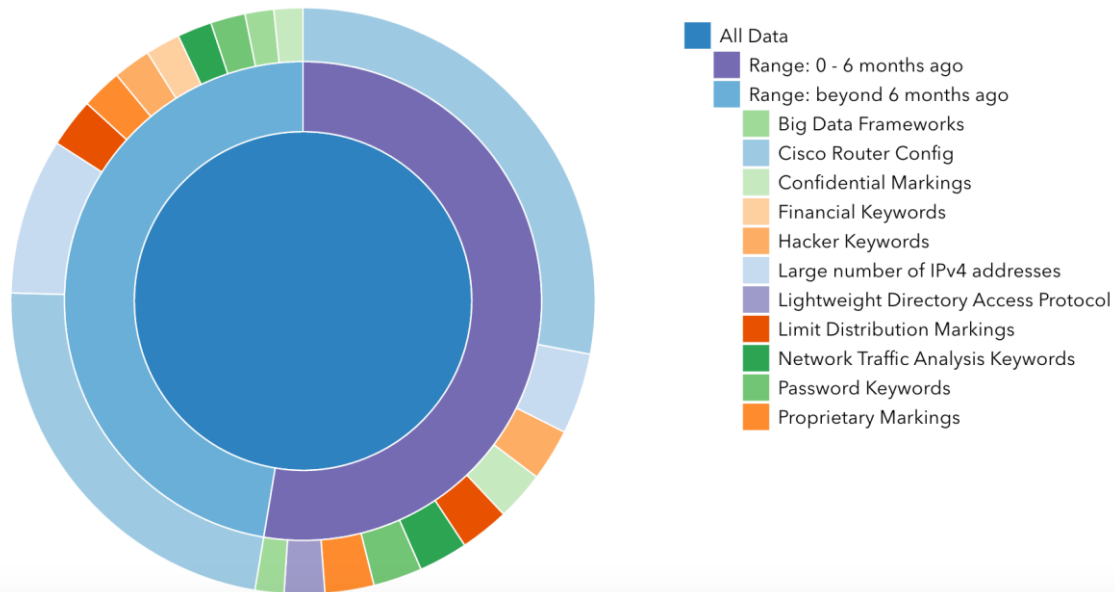


アラートレベル
に応じた警告
を行う

S3に保存された重要なデータの検出と分類

【データ分類例】

Amazon S3 Overview by DLP Theme - minRisk: (7)



- 📦 メールアドレスやクレジットカード番号などの個人情報
- 📦 SSL証明書、RSA秘密鍵
- 📦 iOSとAndroidの認証鍵
- 📦 OAuthとSaaSにアクセスするためのAPI Key
- 📦 データベースのバックアップ
- 📦 静的ウェブサイトコンテンツ
- 📦 ソースコード

データの検出と分類

📦 データ分類のタイミング

- Macieによりデータソースが初めて保護対象に指定されると分類が開始（最初はデータ量に依存して時間がかかる）
- データソースに新たなデータが追加されると分類を開始（非同期で実行）

📦 オブジェクトリスクレベル（1-10）

- 次に紹介する6つのデータ分類手法に基づいて割り当てられたさまざまなリスクレベルの中から最大のリスクレベルをそのオブジェクトのリスクレベルとして決定

📦 S3 メタデータの保持期間

- 分類されたS3オブジェクトのメタデータはデフォルト1ヶ月保存され、最大12ヶ月まで延長可能
- このメタデータに対して可視化したり、クエリを実行したり、カスタムでアラートを作成することが可能

6つのデータ分類手法

分類手法	説明
コンテンツタイプ	<ul style="list-style-type: none">ファイルのヘッダに埋め込まれている識別子(Content-Type)にて分類Content-Typeによってリスクレベルを1-10に振り分け
ファイル拡張子	<ul style="list-style-type: none">ファイル拡張子によるオブジェクトの分類拡張子によってリスクレベルを1-10に振り分け
テーマ	<ul style="list-style-type: none">コンテンツ内に予め決められたテーマ(キーワード)が含まれるかによって分類テーマは英語のみに対応テーマによってリスクレベルを1-10に振り分け
正規表現	<ul style="list-style-type: none">オブジェクト内を正規表現により検索、分類リスクレベルを1-10に振り分け
個人情報 (PII)	<ul style="list-style-type: none">NIST-80-122 および FIPS 199 などの業界標準に基づいて個人情報を分類氏名 / 郵送先住所 / メールアドレス / クレジットカード番号 / IPアドレス(IPv4およびIPv6) / 運転免許証ID (米国) / 国識別番号 (米国) / 生年月日PIIの情報量に応じて高・中・低のPII影響度に分類
Support Vector Machine ベースの分類	<ul style="list-style-type: none">オブジェクト内のコンテンツを学習済みのSVMにより分類テキスト、トークン、n-grams、および文字 n-grams とそれらのメタデータ機能を分類する

6つのデータ分類手法

分類手法	説明
コンテンツタイプ	<ul style="list-style-type: none">ファイルのヘッダに埋め込まれている識別子(Content-Type)にて分類Content-Typeによってリスクレベルを1-10に振り分け
ファイル拡張子	<ul style="list-style-type: none">ファイル拡張子によるオブジェクトの分類拡張子
テーマ	<ul style="list-style-type: none">コンテンツテーマテーマ
正規表現	<ul style="list-style-type: none">オブジェクト内を正規表現により検索、分類リスクレベルを1-10に振り分け
個人情報 (PII)	<ul style="list-style-type: none">NIST-80-122 および FIPS 199 などの業界標準に基づいて個人情報を分類氏名 / 郵送先住所 / メールアドレス / クレジットカード番号 / IPアドレス(IPv4およびIPv6) / 運転免許証ID (当同) / 同識別番号 (当同) / 生年月日PIIの
Support Vector Machine ベースの分類	<ul style="list-style-type: none">オブジェクト内のコンテンツを字皆済みのSVMにより分類テキスト、トークン、n-grams、および文字 n-grams とそれらのメタデータ機能を分類する

各設定項目の有効/無効のみ変更できる

ルールの追加はできない

有効/無効含めて設定変更不可

データ分類項目の例とリスク評価の例

分類手法	分類項目例	リスクレベル
コンテンツタイプ	<ul style="list-style-type: none">▪ P12形式のファイルが保存されている▪ PGP keysが保存されている	<ul style="list-style-type: none">▪ 8▪ 8
ファイル拡張子	<ul style="list-style-type: none">▪ Microsoft Outlook形式のファイルが保存されている▪ .cer形式のファイルが保存されている	<ul style="list-style-type: none">▪ 8▪ 6
テーマ	<ul style="list-style-type: none">▪ restricted, classifiedという単語を2つ以上含むコンテンツが存在▪ proprietary, confidentialという単語を2つ以上含むコンテンツ存在	<ul style="list-style-type: none">▪ 5▪ 5
正規表現	<ul style="list-style-type: none">▪ AWS Secret Keyの1つ以上のマッチング▪ DSA Private Key1つ以上のマッチング	<ul style="list-style-type: none">▪ 10▪ 8
個人情報 (PII)	<ul style="list-style-type: none">▪ 1つ以上のフルネームとクレジットカードの組が存在▪ 5以上の名前またはEメールおよび他のPIIの組み合わせ	<ul style="list-style-type: none">▪ 高▪ 中

※分類項目とリスクレベルはあらかじめ設定がされており、**カスタマイズはできない**

https://docs.aws.amazon.com/ja_jp/macie/latest/userguide/macie-classify-data.html

イベント監視



データの検出・ 分類



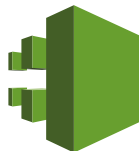
ストレージの
データを自動
分類

データの可視化



分類したデータ
やアクセスを
ダッシュボード
に表示

イベント監視



CloudTrailデー
タを監視

アラートによる警 告



アラートレベル
に応じた警告
を行う

イベント監視

- 📦 CloudTrail イベント及びCloudTrail イベント内のエラーの中からあらかじめ危険度の高いものとして定義されたアクティビティを抽出してリスク評価
- 📦 重要なイベントやエラーを分類、リスク評価、可視化する
- 📦 項目を有効/無効にすることはできるがカスタマイズはできない

データソース	説明
CloudTrail イベント	<ul style="list-style-type: none">▪ インフラストラクチャ内で発生する可能性がある CloudTrail がログを記録したデータおよび管理イベント (API 呼び出し) のサブセットを分析して処理▪ CloudTrail イベントをあらかじめ決められたリスクレベル(1-10)に振り分け
CloudTrail イベント内エラー	<ul style="list-style-type: none">▪ CloudTrail がログを記録したデータおよび管理イベント (API 呼び出し) の、Macie がサポートするサブセットがインフラストラクチャ内で発生したときに発生する可能性があるエラーを分析して処理▪ CloudTrail エラーをあらかじめ決められたリスクレベル(1-10)に振り分け

イベント監視によるリスク評価の項目例

データソース	イベント/エラーの内容	リスクレベル
CloudTrail イベント	▪ X.509証明書がアップロードされ特定のユーザーに関連付けられている (UploadSigningCertificate)	▪ 10
	▪ VPC Flow Logsが削除された (DeleteFlowLogs)	▪ 10
	▪ MFAデバイスが無効にされた (DeactivateMFADevice)	▪ 9
	▪ AWSアカウントのパスワードポリシーが変更された (UpdateAccountPasswordPolicy)	▪ 9
CloudTrail イベント内エラー	▪ アクセス拒否の例外が返された場合のエラー (AccessDeniedException)	▪ 10
	▪ アクセス拒否が返された場合のエラー (AccessDenied)	▪ 10
	▪ 不正なパラメータが入力された場合のエラー (Client.InvalidParameterValue)	▪ 8
	▪ 許可されていない権限を実行した場合のエラー (Client.UnauthorizedOperation)	▪ 8

※リスクレベルはあらかじめ数値が設定されており、**カスタマイズはできない**

データの可視化



データの検出・ 分類



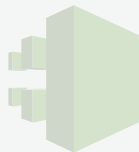
ストレージの
データを自動
分類

データの可視化



分類したデータ
やアクセスを
ダッシュボード
に表示

イベント監視



CloudTrailデー
タを監視

アラートによる警 告



アラートレベル
に応じた警告
を行う

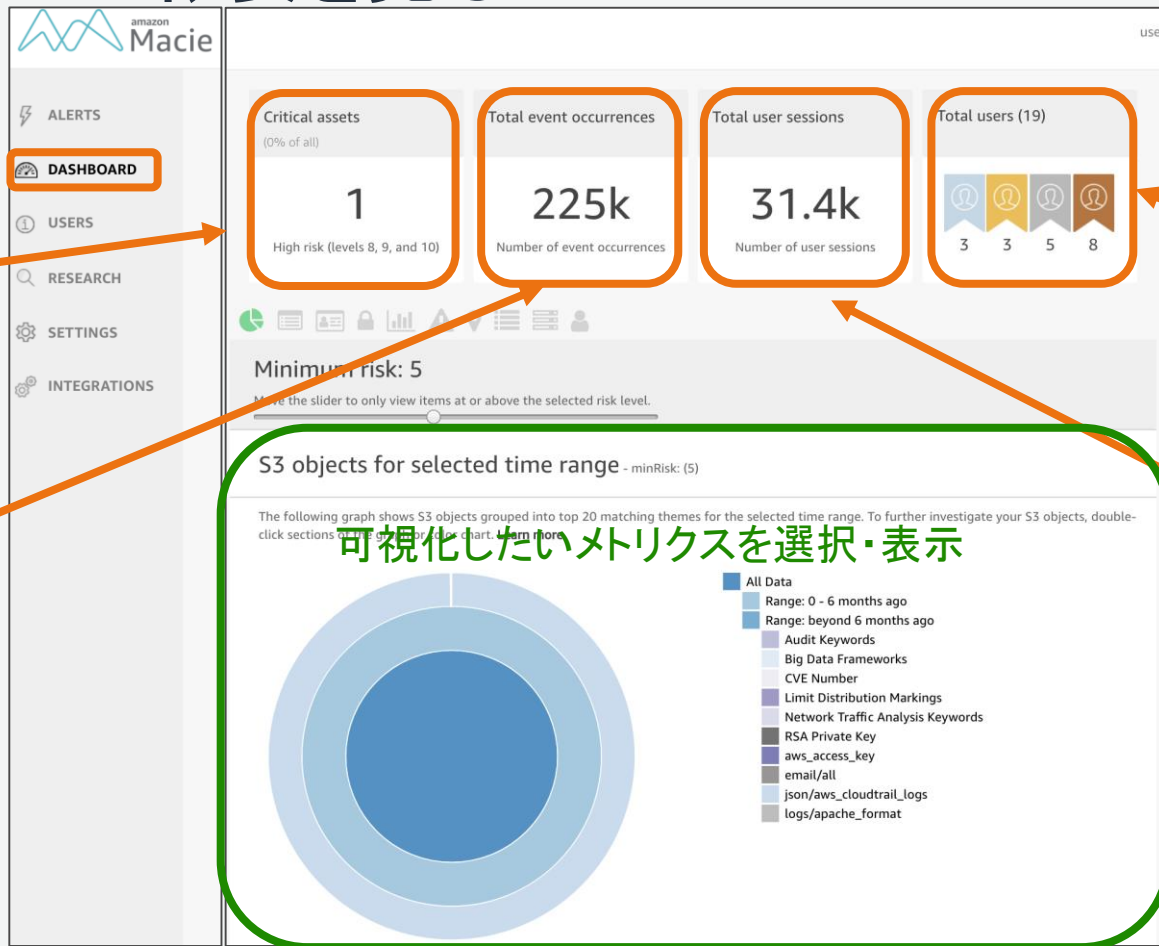
Dashboardで概要を見る



DASHBOARD

リスクレベルが
8~10に分類され
た高リスク
S3 オブジェクト

Macieが有効化
されてからの
CloudTrailイベ
ントの発生総数



IAMユーザーま
たはIAMロール
毎のアクセス頻
度による分類

可視化したいメトリクスを選択・表示

CloudTrailの
ユーザーセッ
ションの合計総
数

時間単位のS3オブジェクトの可視化

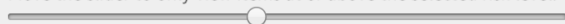


DASHBOARD



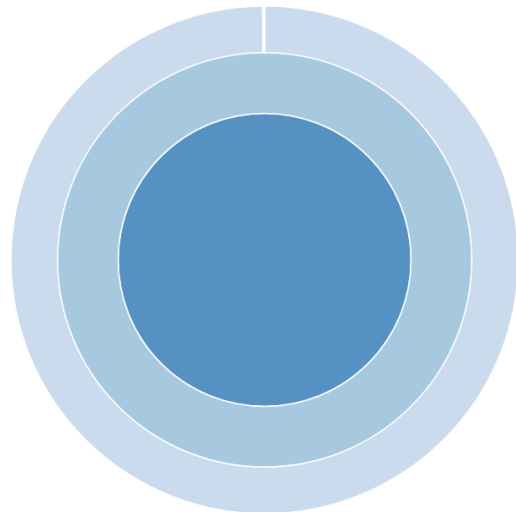
Minimum risk: 5

Move the slider to only view items at or above the selected risk level.



S3 objects for selected time range - minRisk: (5)

The following graph shows S3 objects grouped into top 20 matching themes for the selected time range. To further investigate your S3 objects, double-click sections of the graph or color chart. [Learn more](#)



- All Data
- Range: 0 - 6 months ago
- Range: beyond 6 months ago
- Audit Keywords
- Big Data Frameworks
- CVE Number
- Limit Distribution Markings
- Network Traffic Analysis Keywords
- RSA Private Key
- aws_access_key
- email/all
- json/aws_cloudtrail_logs
- logs/apache_format

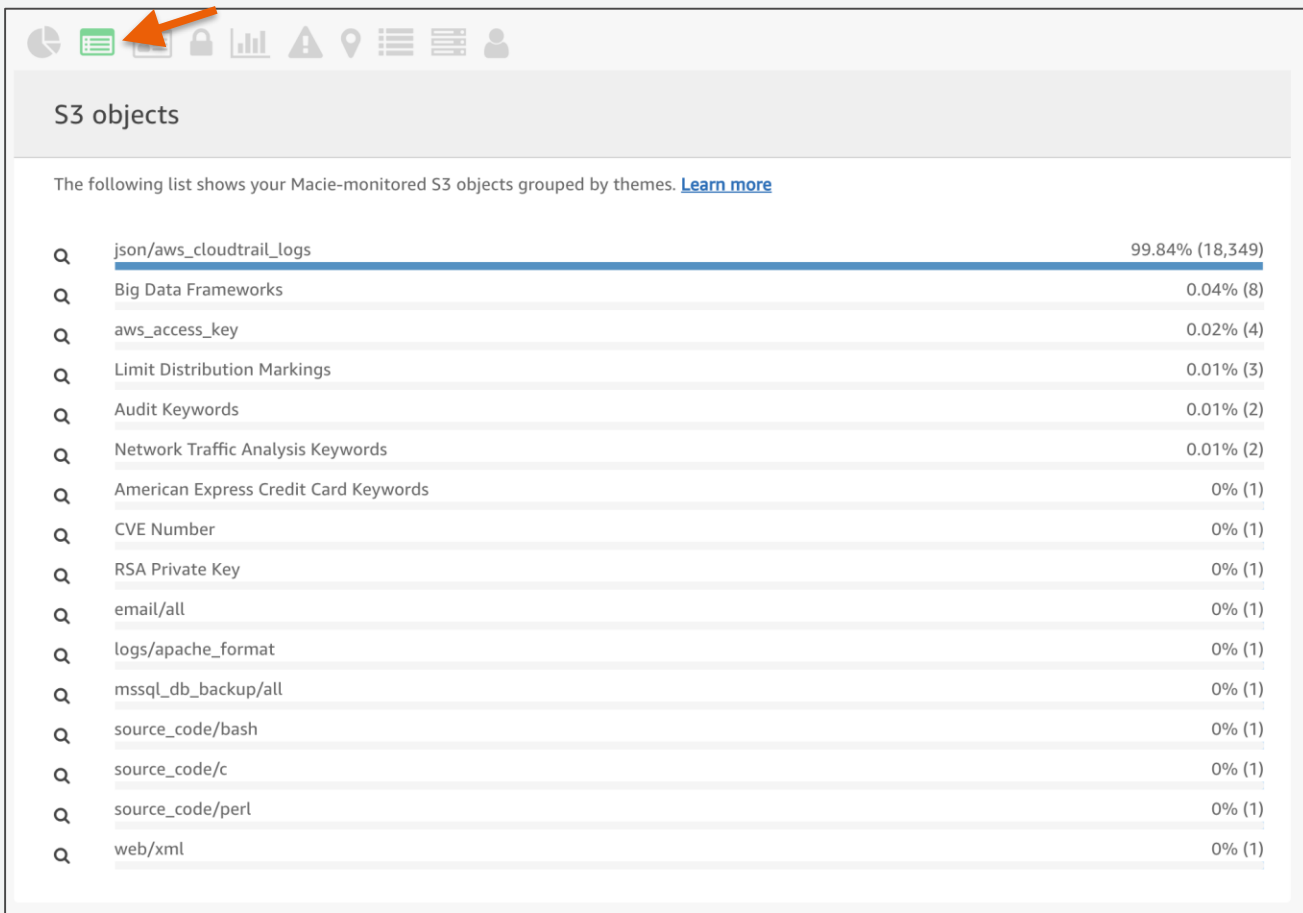
選択した値以上の割り当てリスクレベルを持つ項目のみを絞り込み表示

最も頻繁に割り当てられる上位20のテーマにマッチするS3オブジェクトを6ヶ月前後の時間範囲で分類

S3オブジェクトの分類一覧



DASHBOARD



S3 objects

The following list shows your Macie-monitored S3 objects grouped by themes. [Learn more](#)

Q	json/aws_cloudtrail_logs	99.84% (18,349)
Q	Big Data Frameworks	0.04% (8)
Q	aws_access_key	0.02% (4)
Q	Limit Distribution Markings	0.01% (3)
Q	Audit Keywords	0.01% (2)
Q	Network Traffic Analysis Keywords	0.01% (2)
Q	American Express Credit Card Keywords	0% (1)
Q	CVE Number	0% (1)
Q	RSA Private Key	0% (1)
Q	email/all	0% (1)
Q	logs/apache_format	0% (1)
Q	mssql_db_backup/all	0% (1)
Q	source_code/bash	0% (1)
Q	source_code/c	0% (1)
Q	source_code/perl	0% (1)
Q	web/xml	0% (1)

Macieの監視対象にあるS3オブジェクトのテーマ別の分類一覧

右にはそれぞれのテーマに分類されたオブジェクトの総数と全体に対する割合を表示

個人情報(PII)別 S3 オブジェクト

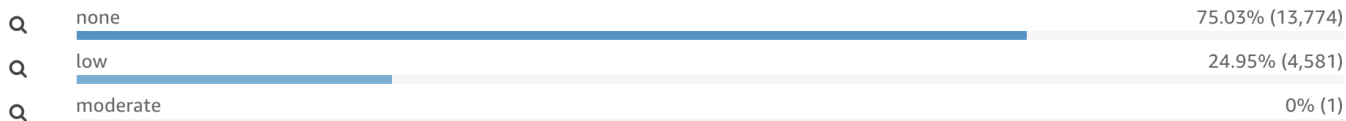


DASHBOARD



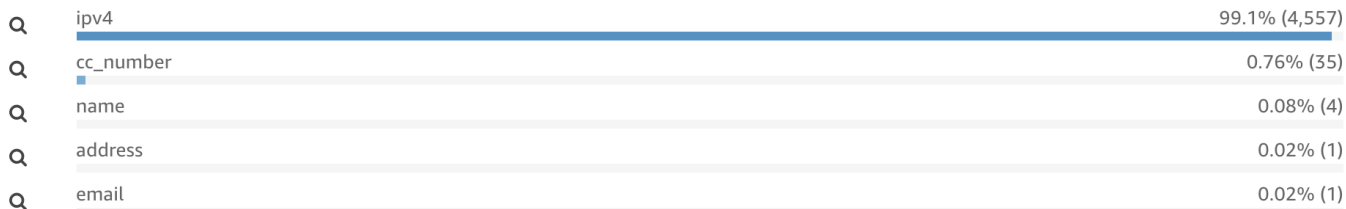
S3 objects by PII priority

The following list shows your Macie-monitored S3 objects grouped by the PII priority. [Learn more](#)



S3 objects by PII types

The following list shows your Macie-monitored S3 objects grouped by the PII types. [Learn more](#)



PII 影響度別 S3
オブジェクト:

PII影響度(高、中、
低、なし)に応じた
S3オブジェクト数と
割合の一覧

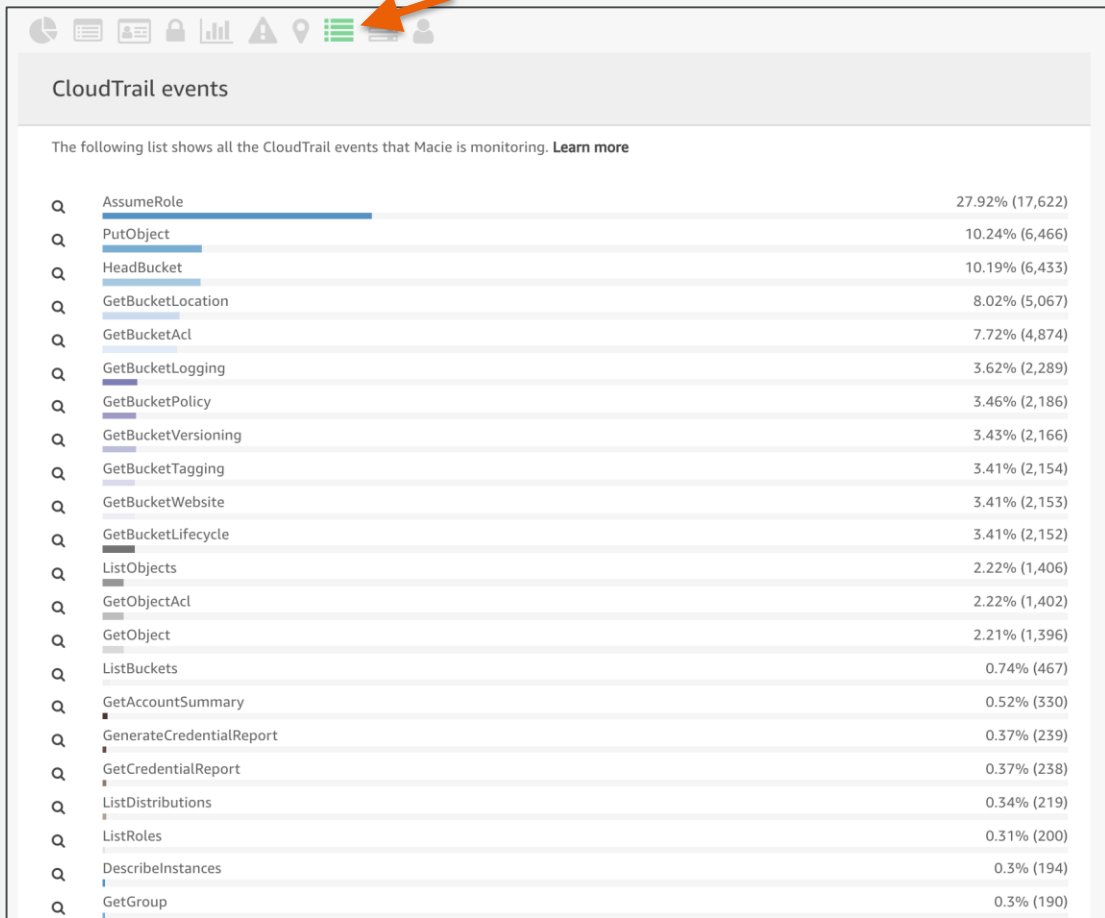
PII タイプ別 S3 オ
ブジェクト:

PIIの分類タイプに
応じたS3オブジェ
クト数と割合の一
覧

CloudTrail イベントの一覧



DASHBOARD



Macieの監視対象にあるCloudTrailのデータおよび発生イベントの全一覧

右にはそれぞれのイベントのユーザーセッションの合計数と全体に対する割合を表示

CloudTrail イベント時系列グラフ



Minimum risk: 5

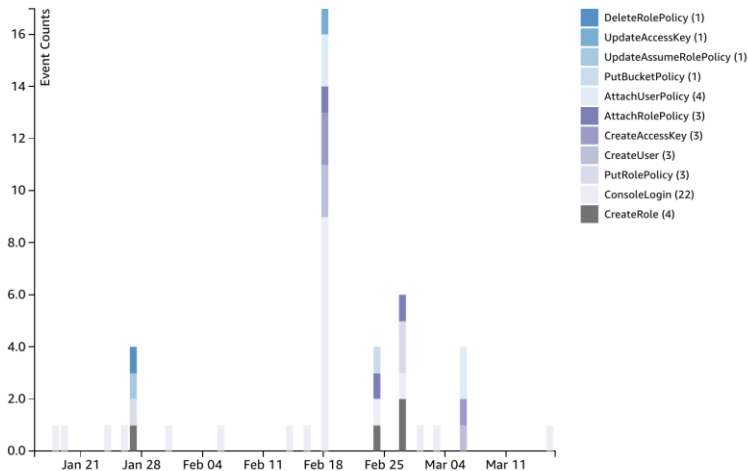
Move the slider to only view items at or above the selected risk level.

リスクレベルでの絞り込み

High-risk CloudTrail events - minRisk: (5)

To further investigate the top 20 high-risk CloudTrail events for the last 60 days, double-click sections of the graph or the color chart. [Learn more](#)

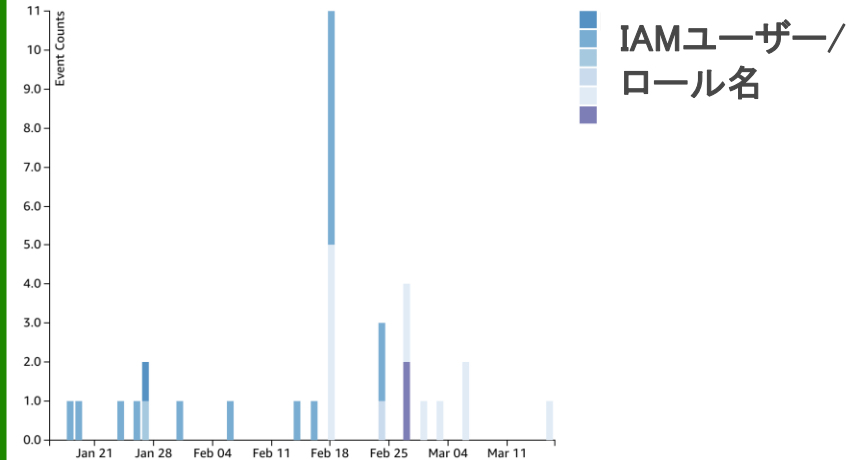
Daily Weekly



CloudTrail users - minRisk: (5)

To further investigate the users associated with the top 20 high-risk CloudTrail events for the last 60 days, double-click sections of the graph or the color chart. [Learn more](#)

Daily Weekly



最近 60 日間で発生した上位20件の CloudTrail データおよび管理イベントの時系列表示

実行ユーザー別のイベントの時系列表示



CloudTrail エラー時系列グラフ



DASHBOARD



Minimum risk: 5

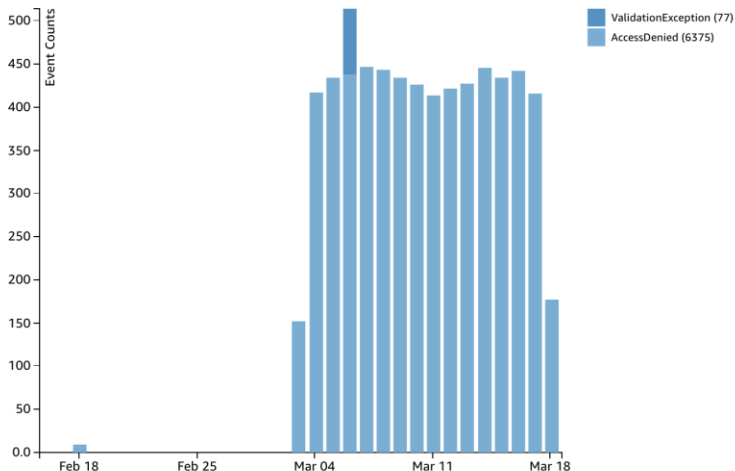
Move the slider to only view items at or above the selected risk level.

リスクレベルでの絞り込み

High-risk CloudTrail errors - minRisk: (5)

To further investigate the top 20 high-risk CloudTrail errors for the last 60 days, double-click sections of the graph or the color chart. [Learn more](#)

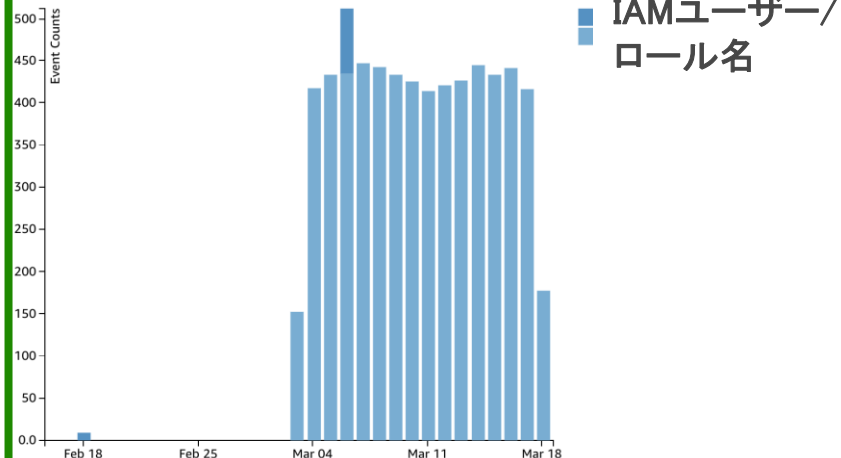
Daily Weekly



CloudTrail users - minRisk: (5)

To further investigate the users associated with the top 20 high-risk CloudTrail events for the last 60 days, double-click sections of the graph or the color chart. [Learn more](#)

Daily Weekly



最近 60 日間で発生した上位20件の CloudTrail エラーの時系列表示

実行ユーザー別の発生エラーの時系列表示





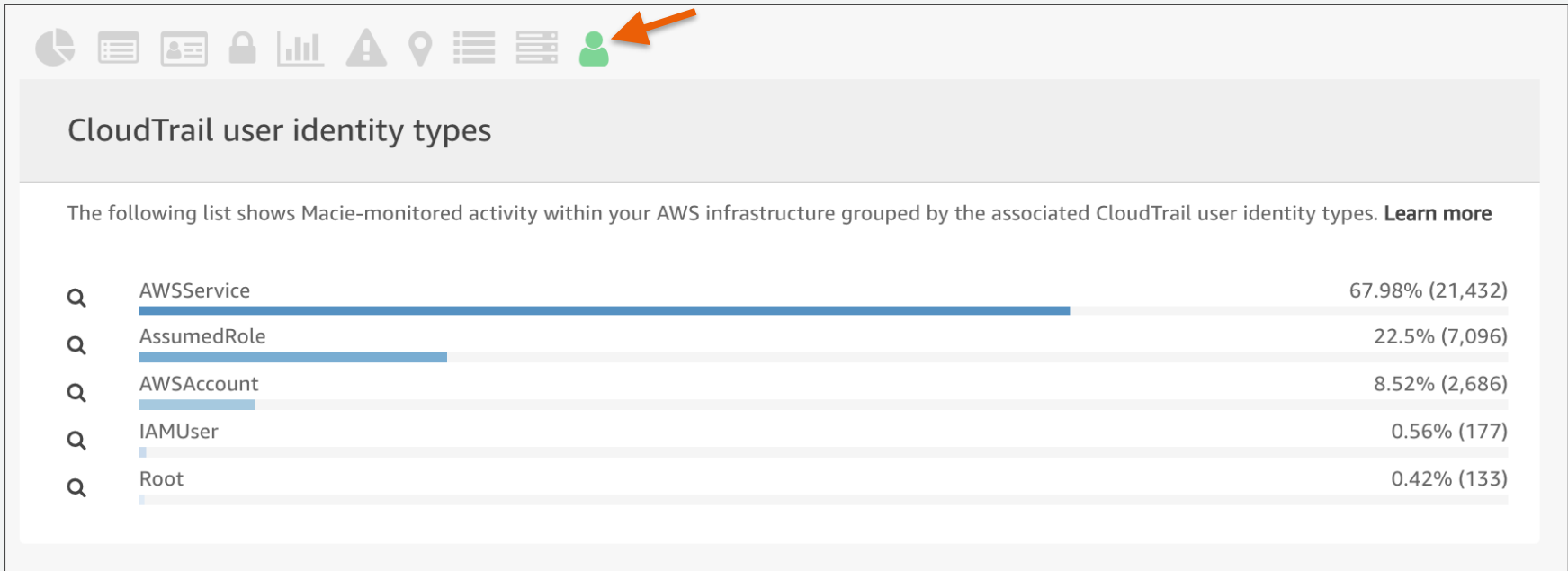
Activity ISPs

The following list shows Macie-monitored activity within your AWS infrastructure grouped by the associated ISPs. [Learn more](#)

Q	Amazon	99.19% (6,262)
Q	So-net Entertainment Corporation	0.6% (38)
Q	Softbank BB	0.09% (6)
Q	AT&T Wireless	0.04% (3)
Q	Sony Network Communications	0.03% (2)
Q	Wire and Wireless Co.,Ltd.	0.03% (2)

- 📦 CloudTrailに記録されている実行されたイベントがどのインターネットサービスプロバイダー (ISP) を介して実行されたかを分類

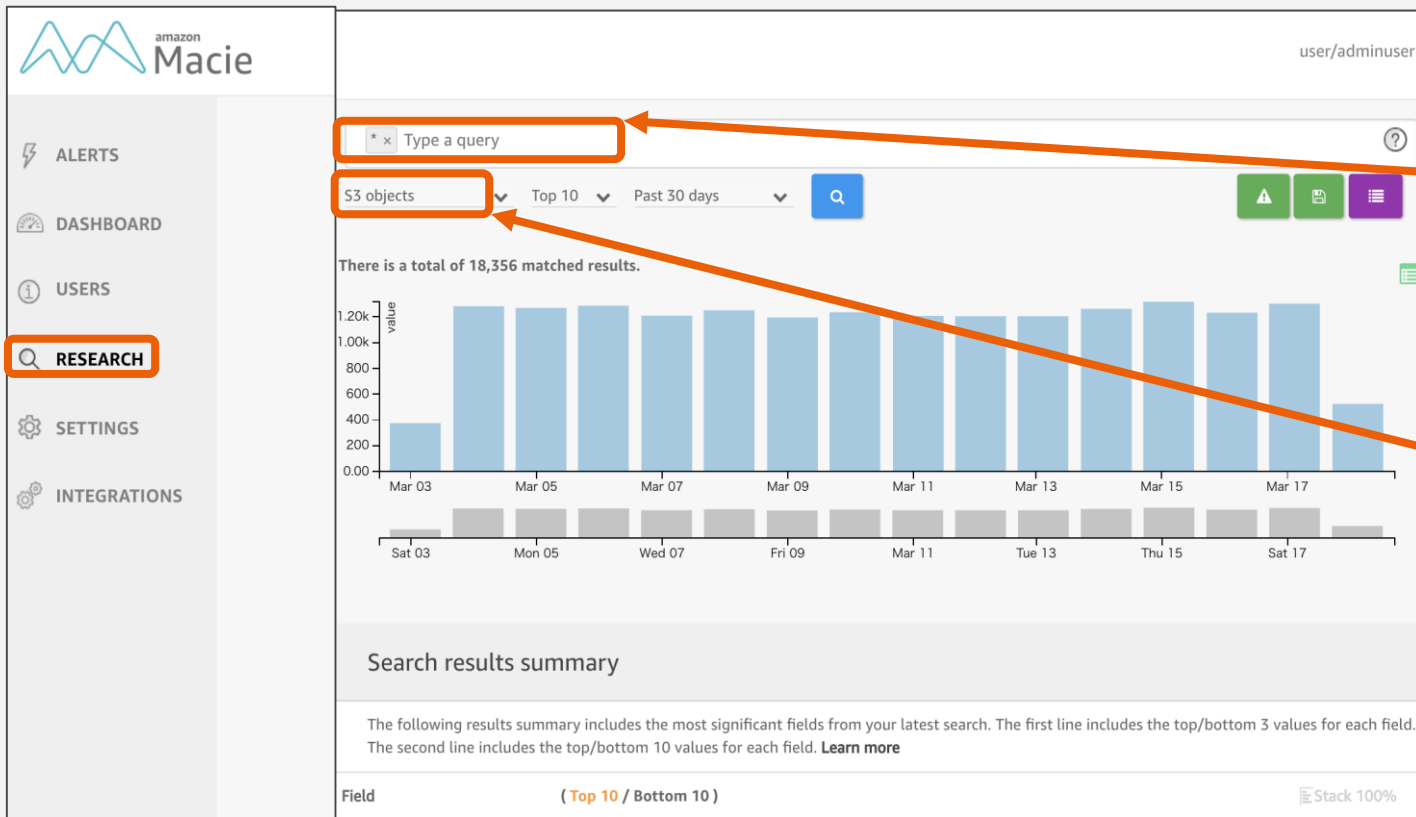
AWS CloudTrail User Identity Type



- CloudTrailに記録されている実行されたイベントがどのIAM User Identityによって実行されているかを分類・表示

Researchタブで検索する

RESEARCH



クエリパーサーでクエリを実行し、Macie が監視するデータおよびアクティビティを検索可能

検索可能なIndexはデータソースに応じてCloudTrail データ、S3 バケットプロパティ、S3 オブジェクトの3種類

Researchタブで検索する



- ❏ クエリ構文は、Apache Luceneのクエリパーサー構文に基づいている
 - https://lucene.apache.org/core/2_9_4/queryparsersyntax.html
- ❏ これらのクエリを用いてマッチング条件に適合した場合に警告する独自のアラートを設定できる (カスタムの基本アラート)

Data Index(データソース)の説明

Data Index	説明
CloudTrail データ	raw Cloudtrail データの 5 分ごとの集計の集合体
S3 バケットプロパティ	Macie が監視する S3 バケットに関するメタデータの集合体
S3 オブジェクト	Macie が監視するバケットに保存されている S3 オブジェクトに関するメタデータの集合体

Researchタブで検索する: 検索例



検索条件	Data Index	クエリ例
Amazon が所有している IP アドレスから実行されたものではないコンソールログインを検索	CloudTrail データ	<code>eventName!sp.compound:/ConsoleLogin:~(Amazon.*)/</code>
特定のテーマに分類されたオブジェクト (例えばaws_access_key)について検索	S3 オブジェクト	<code>themes:"aws_access_key"</code>
パブリック S3 バケット内の個人情報 (PII)を検索	S3 オブジェクト	<code>filesystem_metadata.bucket:"my-public-bucket" AND (pii_impact:"moderate" OR pii_impact:"high")</code>
リスクレベルが7よりも大きいか又はPII 影響度が中以上のものを検索	S3オブジェクト	<code>dlp_risk:>7 OR pii_impact:"moderate" OR pii_impact:"high"</code>

アラートによる警告



データの検出・ 分類



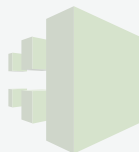
ストレージの
データを自動
分類

データの可視化



分類したデータ
やアクセスを
ダッシュボード
に表示

イベント監視



CloudTrailデー
タを監視

アラートによる警 告



アラートレベル
に応じた警告
を行う

アラートによる警告



root ▾

ALERTS

DASHBOARD

USERS

RESEARCH

SETTINGS

INTEGRATIONS

Categories

All (1)

Basic Alert (1)

Predictive (0)

Anonymized Access (0)

Config Compliance (0)

Credential Loss (0)

Data Compliance (1)

File Hosting (0)

Identity Enumeration (0)

Information Loss (0)

Location Anomaly (0)

Open Permissions (0)

Privilege Escalation (0)

Ransomware (0)

Service Disruption (0)

Suspicious Access (0)

Active (1) Archived (0) All (1)

Group archive Sort by: Time: newest ▾

Amazon Macie is monitoring 17.5k new S3 objects since the last alert generated a month ago. [Learn more](#)

MED

RSA Private Key uploaded to AWS S3

DATA COMPLIANCE BASIC ALERT

a month ago

1 Results

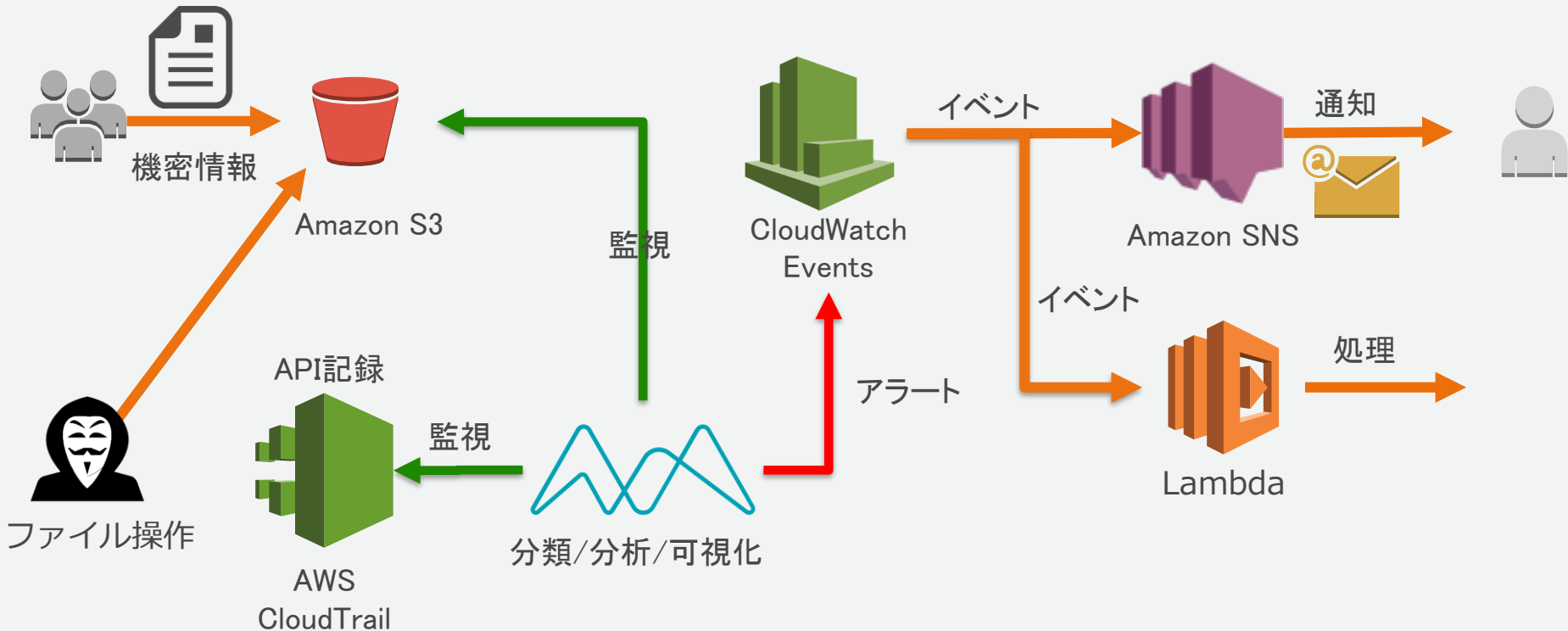
12 Views

zen-macie-test

📦 アラートはアラート画面に表示される

📦 CloudWatch Eventsへイベント通知できる

CloudWatch Eventsとアラートの連携



Critical, High, Medium, Low, Informationalのレベルに応じたアラートが通知される

Macieのアラートの重大度

📦 Critical

- 多数のリソースまたはシステムのセキュリティ侵害が発生
- このセキュリティ上の問題は緊急事態として対応し、**直ちに改善を実施すること**

📦 High

- 1つまたは複数のリソースまたはシステムのセキュリティ侵害を通知
- このセキュリティ上の問題は緊急事態として対応し、**直ちに改善を実施すること**

📦 Medium

- インフラストラクチャ内での情報の機密性、完全性、および可用性を侵害する可能性のあるセキュリティ上の問題
- 次の可能な機会（たとえば、次のサービスの更新中）にこの問題を修正すること

📦 Low

- インフラストラクチャ内での情報の機密性、完全性、および可用性を侵害する可能性のあるセキュリティ上の問題
- 将来のサービスの更新の一部として、この問題を修正すること

📦 Informational

- インフラストラクチャの特定のセキュリティ設定の詳細
- ビジネスおよび組織の目標に基づいて、単にこの情報に留意するか、これを使用してシステムおよびリソースのセキュリティを改善が可能

Macieのアラートの種類

📦 基本アラート (Basic Alerts)

- 事前にクエリで定義されたルールベースのアラート
- デフォルトで事前設定されている**マネージド型アラート**とユーザーがカスタム設定で追加できる**カスタムアラート**がある
 - ルールベースの各項目の設定を**有効/無効**にすることが可能
- カスタムアラートはResearchタブのところで説明したクエリでルール設定できる

📦 予測アラート (Predictive Alerts)

- 機械学習により学習された通常のアクティビティのパターンから逸脱したアクティビティに対して自動的にアラートを発生する
- **カスタマイズは不可**

S3をデータソースとするマネージド型アラート(例)

リスク

大

アラート内容	Category	警告のSeverity
不特定多数へS3バケットへの書き込み権限が許可されている	オープン権限	Critical
AWS Access Key IDとSecret Access KeyがS3へアップロードされた	データコンプライアンス	Critical
不特定多数のユーザーへS3のRead権限を許可している	オープン権限	Critical
AWS, Slack, SSH, 公開鍵証明書等の秘密鍵を含む認証情報がS3に保存されている	データコンプライアンス	High
リスクレベルの高いドキュメント(リスクレベル7以上)のS3 ACLの設定がグローバルアクセス可能になっている	オープン権限	High
AWS Access Key IDとSecret Access Keyがソースコード内に埋め込まれている	データコンプライアンス	High
PCI DSSの要件対象となるクレジットカード情報を含むデータがS3に存在している	データコンプライアンス	Medium

※マネージド型アラートの一部の例。これ以外にも多数項目があるほか、クエリを用いて独自のカスタムアラートも作成できる。

小

CloudTrailをデータソースとするマネージド型アラート

大

アラート内容	Category	警告のSeverity
Tor(The Onion Router)を経由しての匿名ユーザーからのアクセス	匿名アクセス	Critical
匿名のプロキシサーバーからのアクセス	匿名アクセス	High
信頼できないOS (Kali Linux等)からのAPIリクエスト	不審なアクセス	Medium
不特定多数のユーザーがS3のACL設定を書き換えられるようになっている	オープン権限	Medium
5分間で30回以上のS3バケットへのアクセスを匿名ユーザーが試みようとしている	情報損失	Medium
不特定多数のユーザーへS3のオブジェクトとメタデータへのread権限が付与されている	オープン権限	Medium
S3バケットの削除がAWS外部のIPアドレスからRootユーザーで実行されている	情報損失	Medium

※マネージド型アラートの一部の例。これ以外にも多数項目があるほか、クエリを用いて独自のカスタムアラートも作成できる。

小

Agenda

📦 クラウドでのデータ保護

📦 Amazon Macieとは

📦 使い始めるには

📦 機能・操作について

📦 **ユースケース**

📦 Macieの料金

Macieのユースケース

📦 機密データの検出（データコンプライアンス）

- ソースコード内に埋め込まれた認証情報の検出
- 知的財産データが保存されていないか監視する
- 現在のS3バケット内の情報を整理・可視化する

📦 企業内での不正アップロードの検出

- Credential情報、個人情報、知的財産が不正に保存されないように監視する

📦 不正アクセス・攻撃の検知（不審なアクセス/匿名アクセス）

- 通常とは異なるユーザー/IPアドレスからのS3への操作の検知

📦 不注意な操作への警告（オープン権限）

- 機密データに誤って設定されたアクセス権限の検出
- 不注意によるデータ公開への警告

📦 監査

- 格納された機密データが適切に保存・アクセスされているか監査

データ漏えいの脅威に対するMacieの対処の一例

内部の脅威

外部からの脅威

偶発的な脅威

社員によるアクセス権限の設定ミスや操作ミスによる機密データの漏えい

顧客や取引先のミスによる情報の漏えい

意図的な脅威

社員や元社員が金銭目的や怨恨による理由で社内の機密情報を持ち出す

セキュリティホールや不十分な権限管理を突かれての不正アクセスによる情報の漏えい

データ漏えいの脅威に対するMacieの対処の一例

内部の脅威

外部からの脅威

偶発的な脅威

- ❏ アクセス権限の変更の検出
- ❏ PublicなバケットにアップロードされたPIIの警告
- ❏ ユーザーの通常とは異なるアクセスパターンの検知
- ❏ 他社の保持するデータはクロスアカウントでの監視

意図的な脅威

社員や元社員が金銭目的や怨恨による理由で社内の機密情報を持ち出す

セキュリティホールや不十分な権限管理を突かれての不正アクセスによる情報の漏えい

データ漏えいの脅威に対するMacieの対処の一例

内部の脅威

外部からの脅威

偶発的な脅威

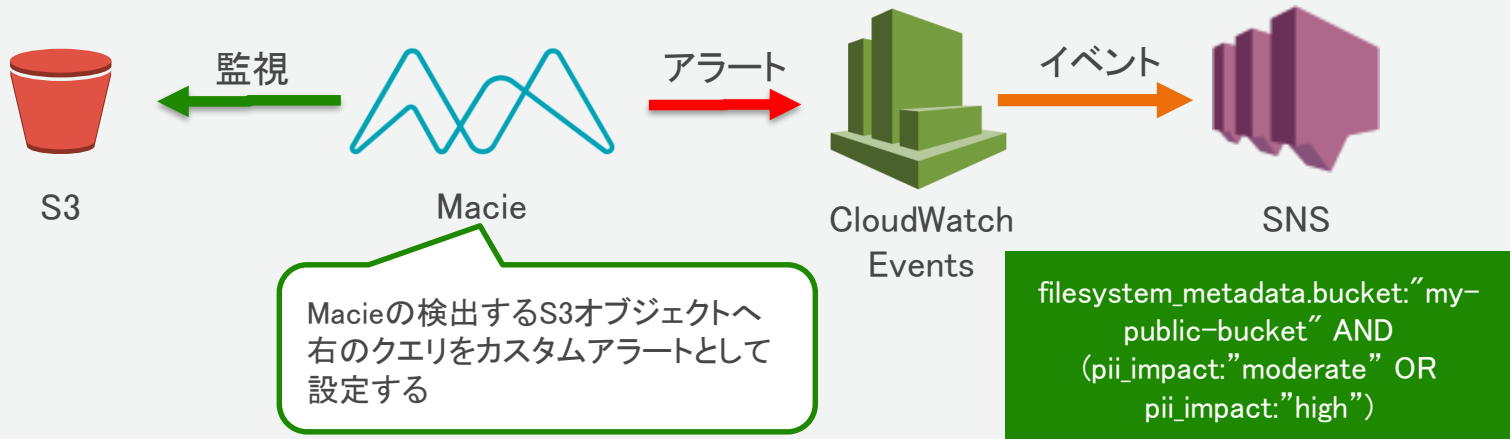
- ❏ アクセス権限の変更の検出
- ❏ PublicなバケットにアップロードされたPIIの警告
- ❏ ユーザーの通常とは異なるアクセスパターンの検知
- ❏ 他社の保持するデータはクロスアカウントでの監視

意図的な脅威

- ❏ 通常とは異なるユーザー/IPアドレスからのS3への操作の検知
- ❏ ユーザーの操作に対するアラートを管理者が受け取る

例) PublicなS3バケットにアップロードされたPIIの警告

- ❏ 個人情報が多数のユーザーへ公開されたことを検知
- ❏ 通常のWebサーバーとして公開しているオブジェクトは検出したくない
- ❏ 個人情報を持つオブジェクトのみを限定的に検出
 - Config Rulesは情報を考慮せずに全てのPublicバケットを検出してしまふ



Agenda

📦 クラウドでのデータ保護

📦 Amazon Macieとは

📦 使い始めるには

📦 機能・操作について

📦 ユースケース

📦 **Macieの料金**

Macieの料金

$$= \text{コンテンツ分類 (GB)} + \text{CloudTrail イベント処理(件数)} + \text{メタデータ保存期間の延長 (GB/月)}$$

無料枠

最初の 1 GB
までは無料

最初の 10 万件の
イベントは無料

生成された分類済
みS3オブジェクトメ
タデータは最初の
30 日間無料保存

基本料金

コンテンツ分類エ
ンジンでの処理1
GB あたり 5 USD

イベント 100 万件
ごとに 4 USD

処理データ 1 GB あ
たり 0.05 USD を毎
月課金 (最大 12 か
月まで延長可)

まとめ

Macieを用いるとPCI/HIPAA/GDPRなどのコンプライアンスや規制の対象となる機密データを特定できる。

Macieを用いると企業内の機密データにまつわるリスクの可視化とリスク管理ができるようになる。

Macieを用いるとデータの漏えいや不正アクセスなどをアラートにより検知しデータを保護できる。

参考資料

- Amazon Macieメインページ
 - <https://aws.amazon.com/jp/macie/>
- Amazon Macieの詳細
 - <https://aws.amazon.com/jp/macie/details/>
- Amazon Macieドキュメント
 - <https://aws.amazon.com/jp/documentation/macie/>
- Amazon Macie 料金
 - <https://aws.amazon.com/jp/macie/pricing/>
- Amazon Macie FAQ
 - <https://aws.amazon.com/jp/macie/faq/>
- Amazon Macie Blog
 - <https://aws.amazon.com/jp/blogs/news/launch-amazon-macie-securing-your-s3-buckets/>

FAQ

📦 日本語で書かれた名前や住所はPIIとして識別されるのか？

- 現状、Macieの自然言語処理は英語に最適化されているため、日本語のPIIの検出は未対応。今後多言語にも対応していく予定です。

📦 S3のオブジェクトが暗号化されている場合には検出・分類は可能か？

- Amazon S3 オブジェクトが Amazon S3 で管理された暗号化キー (SSE-S3) を使用して暗号化されている場合、セットアップ時に作成されたロールを使用してオブジェクトの読み取りと分類が可能。
- Amazon S3 オブジェクトが AWS KMS で管理されたキー (SSE-KMS) を使用して暗号化されている場合、特定のIAMロール(AWSMacieServiceCustomerServiceRole)をKMS カスタマーマスターキー (CMK) にキーユーザーとして追加した場合のみ読み取りと分類が可能。
- Amazon S3 オブジェクトがクライアント側の暗号機能を使って暗号化されている場合は読み取りと分類不可。

📦 Macie自体は機密データを保持するのか？

- データ分類時に一時的にS3のオブジェクトをメモリ上にロードして解析を行うが、解析後はのちの分析に必要なメタデータのみを保持するだけで、解析により一時的に保存されたコンテンツはMacieから完全に削除されます。

オンラインセミナー資料の配置場所

AWS クラウドサービス活用資料集

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

			
サービス別資料	ソリューション別資料	業種別資料	その他の資料
無料オンラインセミナー「Black Belt Online Seminar」のサービスカット資料他、AWSのTechメンバーによる各サービスの解説資料がご覧いただけます。	無料オンラインセミナー「Black Belt Online Seminar」のソリューションカット資料他、特定のソリューションについてのAWS活用方法がご覧いただけます。	無料オンラインセミナー「Black Belt Online Seminar」のインダストリーカット資料他、特定の業界のユースケースがご覧いただけます。	イベントに関する資料やアップデート情報などがご覧いただけます。

Amazon Web Services ブログ

- 最新の情報、セミナー中のQ&A等が掲載されています。
- <https://aws.amazon.com/jp/blogs/news/>

公式Twitter/Facebook AWSの最新情報をお届けします



@awscloud_jp



検索

もしくは

<http://on.fb.me/1vR8yWm>

最新技術情報、イベント情報、お役立ち情報、
お得なキャンペーン情報などを日々更新しています！

AWSの導入、お問い合わせのご相談

AWSクラウド導入に関するご質問、お見積、資料請求をご希望のお客様は以下のリンクよりお気軽にご相談下さい。

<https://aws.amazon.com/jp/contact-us/aws-sales/>

<p>お問い合わせ</p> <hr/> <p>日本担当チームへのお問い合わせ ></p> <hr/> <p>関連リンク</p> <p>フォーラム</p> <hr/>	<h2>日本担当チームへのお問い合わせ</h2> <p>AWS クラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のフォームよりお気軽にご相談ください。平日営業時間内に日本オフィス担当者よりご連絡させていただきます。</p> <p>※ご請求金額またはアカウントに関する質問はこちらからお問い合わせください。</p> <p>※Amazon.com または Kindle のサポートにお問い合わせはこちらからお問い合わせください。</p> <p>アスタリスク (*) は必須情報となります。</p> <p>姓*</p> <input type="text"/> 名* <input type="text"/>
---	--

※「AWS お問い合わせ」で検索して下さい。

aws

