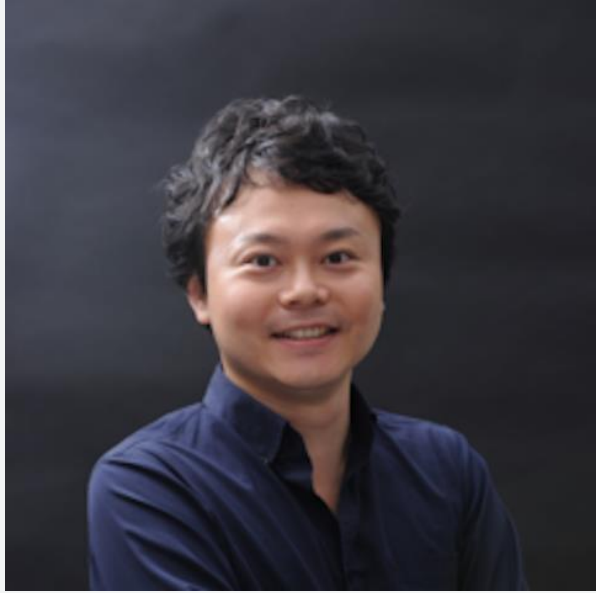
AWS
Black Belt
Online Seminar

【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

aws

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.

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

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

企業内の機密データにまつわるリスクを知りたい

機密データに関するインシデント発生時に対処したい

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

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

aws

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

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

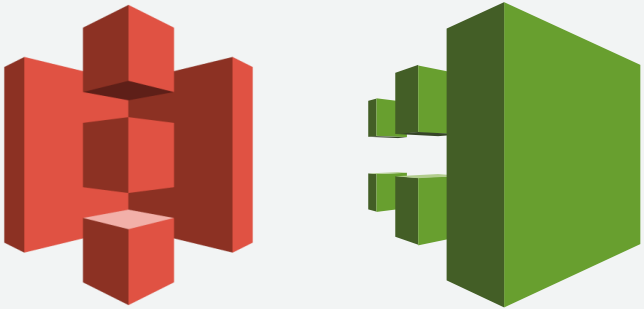
アラートによる警告

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

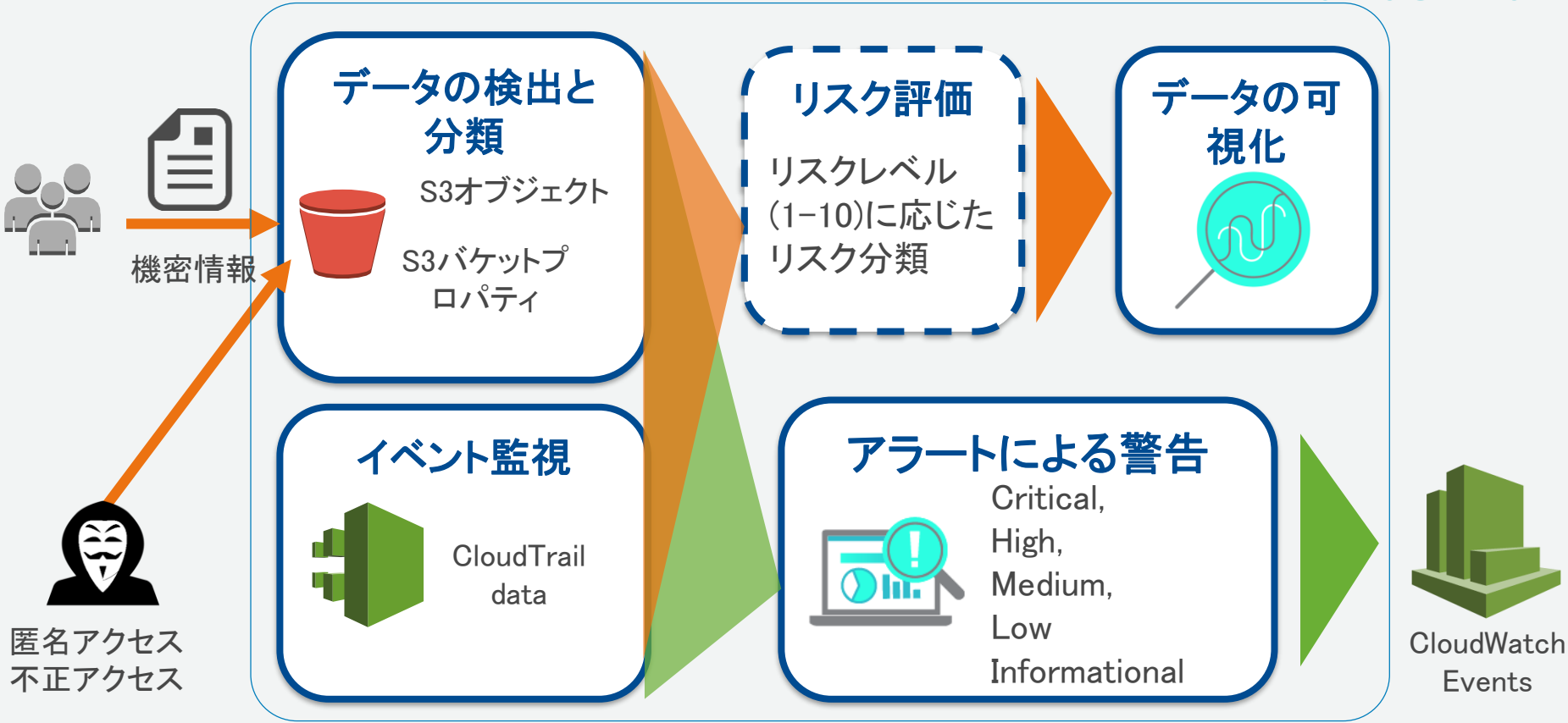


- 現状ではAmazon S3とAWS CloudTrailのみが監視対象
- Macieと同一リージョンのS3バケットが監視対象
- 他のアカウントのS3バケットも監視できる

- 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/macie/faq/

Macieの動作イメージ

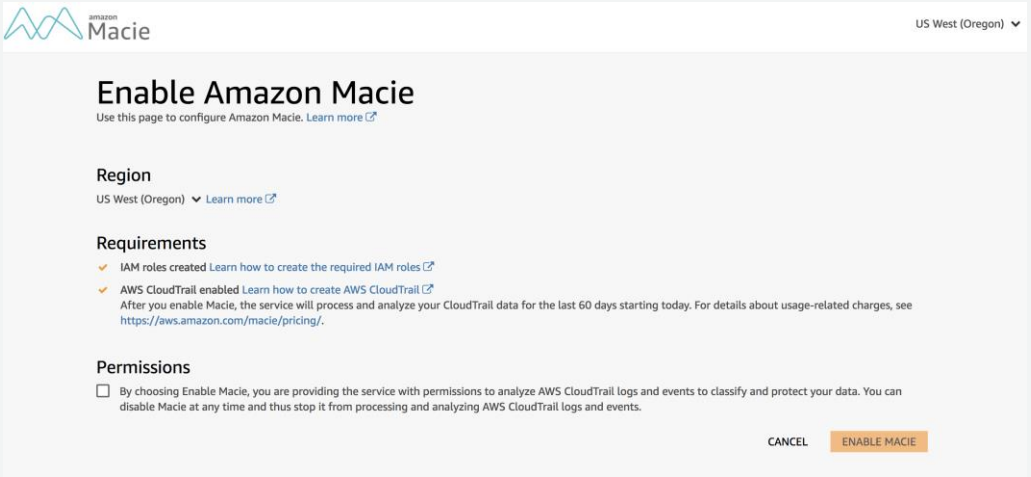


Agenda

- 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



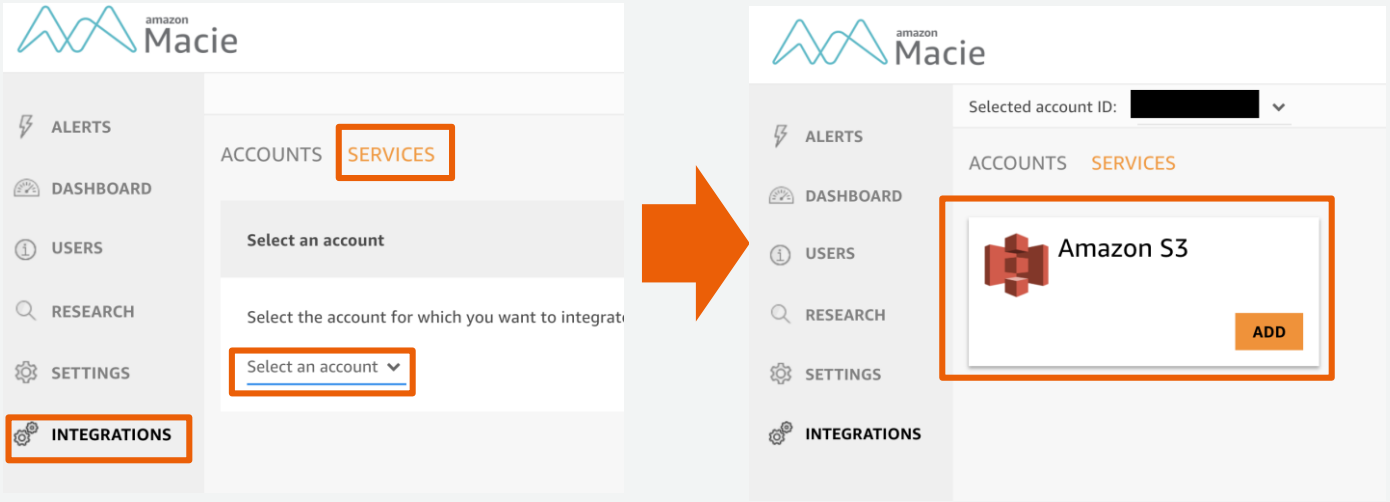
https://docs.aws.amazon.com/ja_jp/macie/latest/userguide/macie-setting-up.html

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

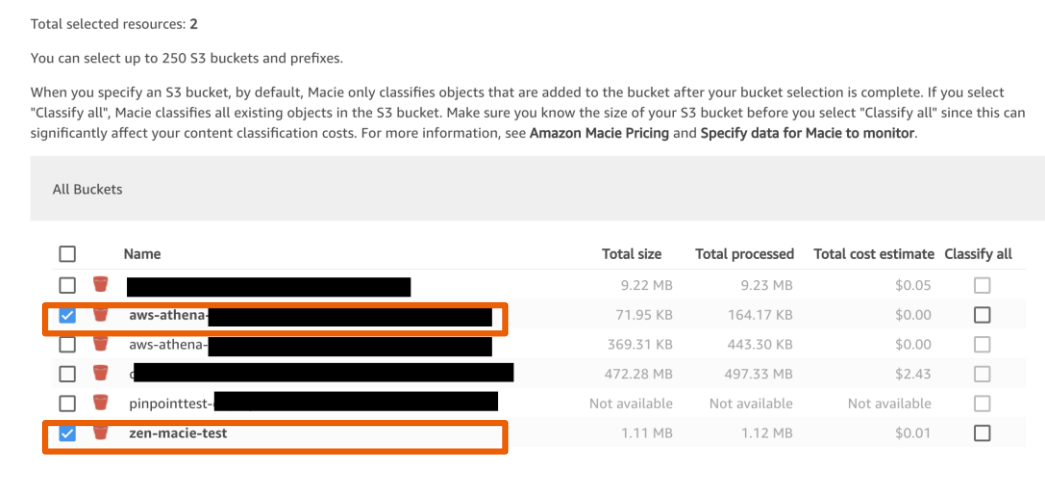
2. Amazon S3を選択してADDをクリック



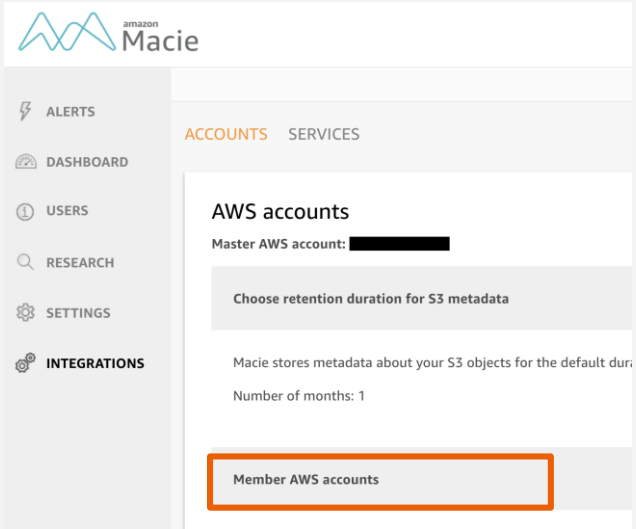
Macieで保護するS3バケットの追加 (2/2)

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。



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

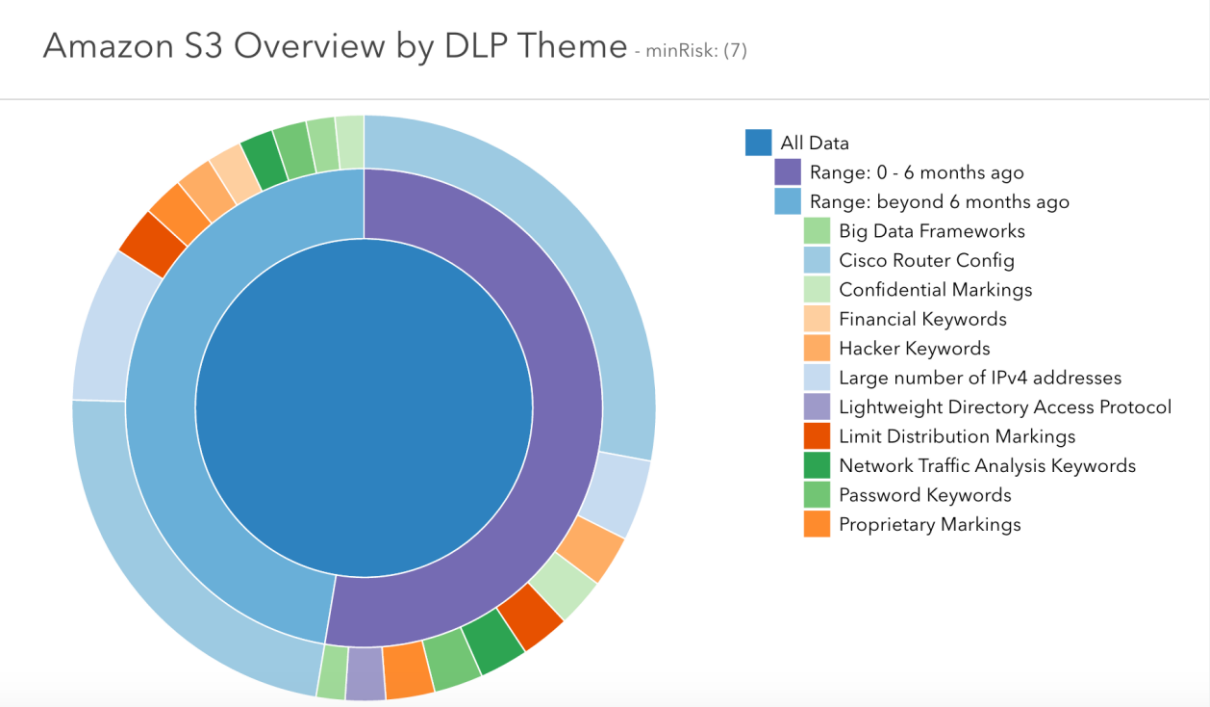
イベント監視

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】

- 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	▪ 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	▪ 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	▪ 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	▪ 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)	▪ 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	▪ 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	▪ 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	▪ ファイル拡張子によるオブジェクトの分類 ▪ 拡張
テーマ	▪ コンテ ▪ テー ▪ テー
正規表現	▪ 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)	▪ 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IPv
Support Vector Machine ベースの分類	▪ 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

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	▪ 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	▪ 8 ▪ 8
ファイル拡張子	▪ 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	▪ 8 ▪ 6
テーマ	▪ 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	▪ 5 ▪ 5
正規表現	▪ 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	▪ 10 ▪ 8
個人情報 (PII)	▪ 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	▪ 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	▪ 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	▪ 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) ▪ VPC Flow Logsが削除された (DeleteFlowLogs) ▪ MFAデバイスが無効にされた (DeactivateMFADevice) ▪ AWSアカウントのパスワードポリシーが変更された (UpdateAccountPasswordPolicy)	▪ 10 ▪ 10 ▪ 9 ▪ 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) ▪ アクセス拒否が返された場合のエラー (AccessDenied) ▪ 不正なパラーメータが入力された場合のエラー (Client.InvalidParameterValue) ▪ 許可されていない権限を実行した場合のエラー (Client.UnauthorizedOperation)	▪ 10 ▪ 10 ▪ 8 ▪ 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

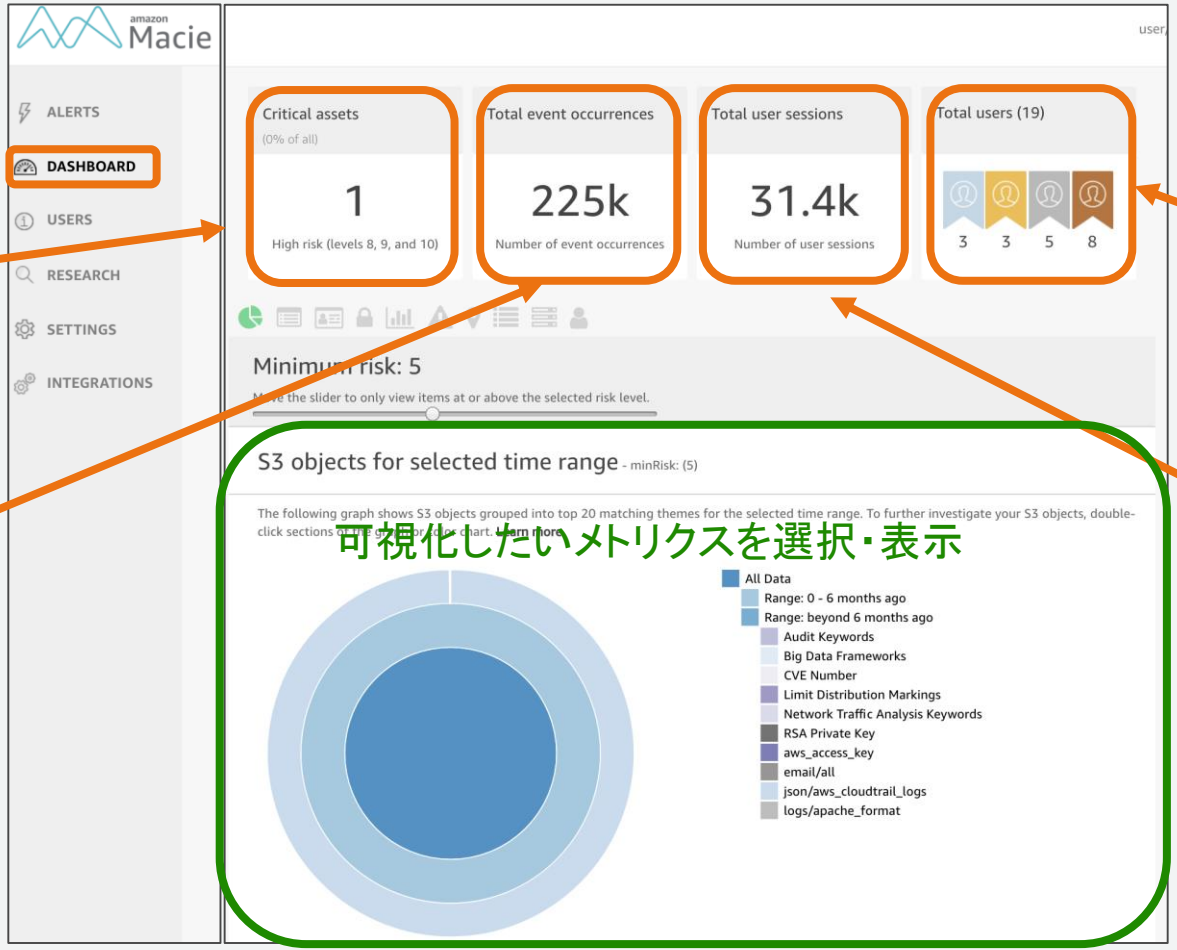
DASHBOARD

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

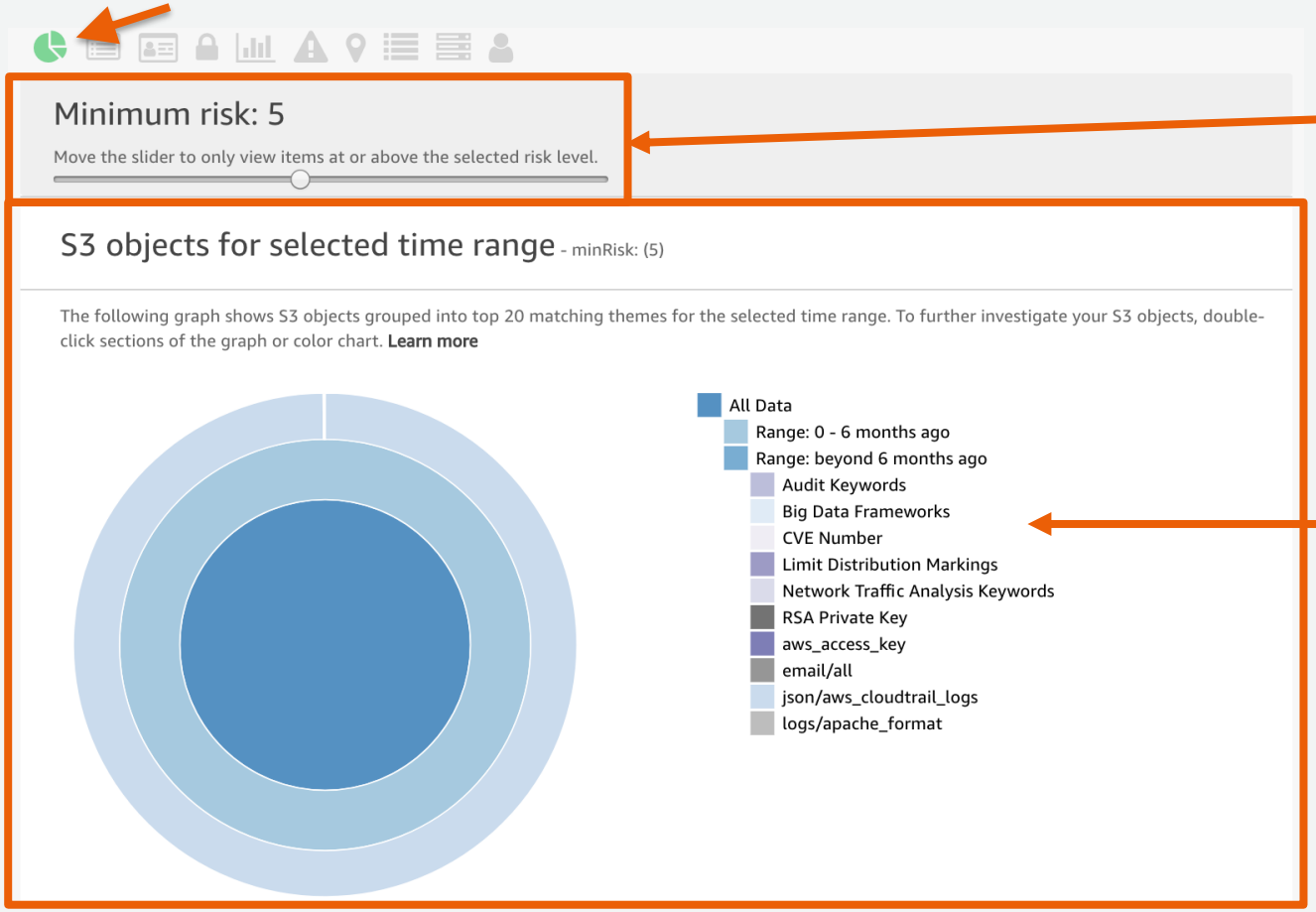
IAMユーザーまたはIAMロール毎のアクセス頻度による分類

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



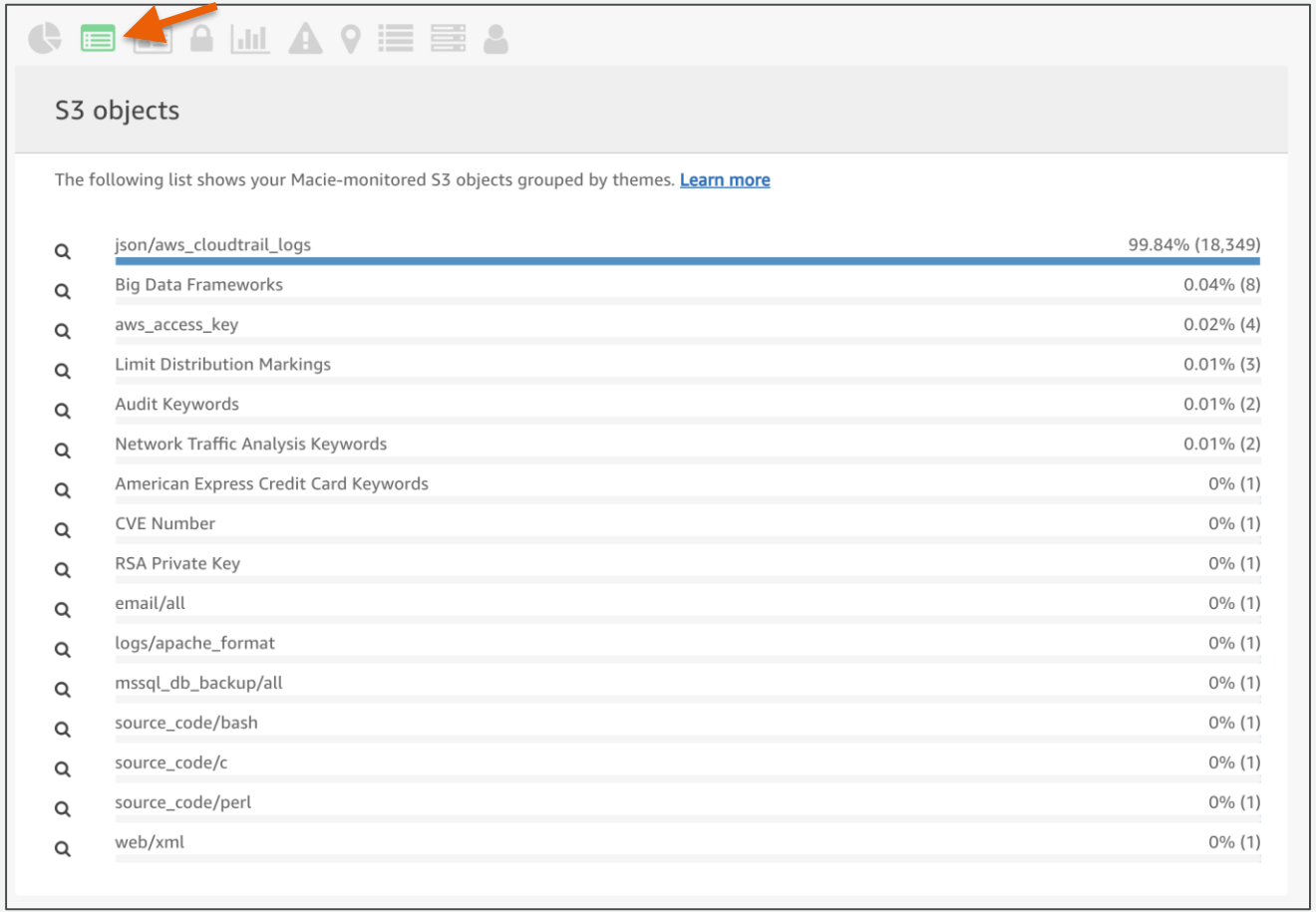
選択した値以上の割り当てリスクレベルを持つ項目のみを絞り込み表示

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

aws

S3オブジェクトの分類一覧

DASHBOARD

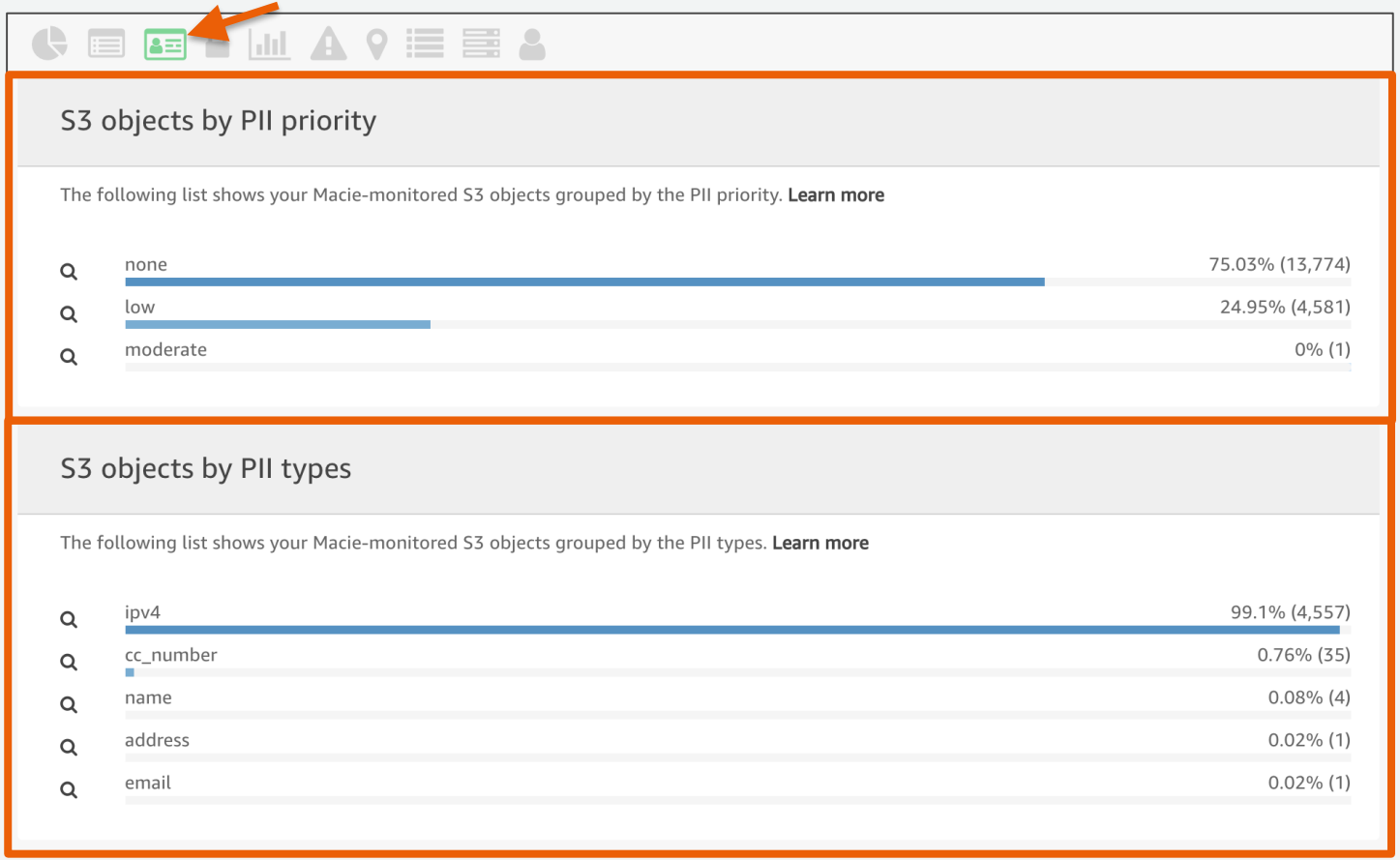


- Macieの監視対象にあるS3オブジェクトのテーマ別の分類一覧
- 右にはそれぞれのテーマに分類されたオブジェクトの総数と全体に対する割合を表示

aws

個人情報(PII)別 S3 オブジェクト

DASHBOARD



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

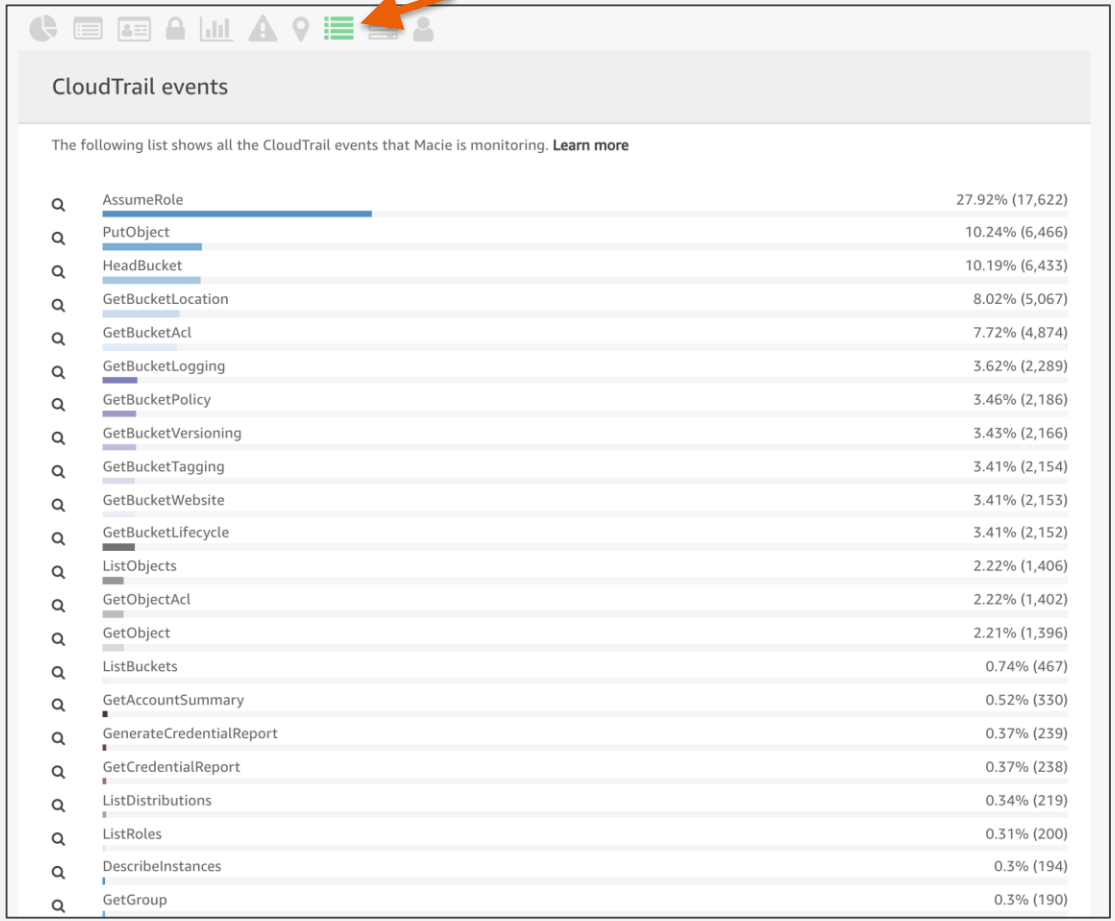
PII タイプ別 S3 オブジェクト:

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

aws

CloudTrail イベントの一覧

DASHBOARD

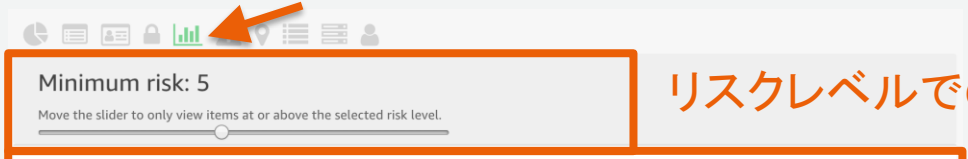


- Macieの監視対象にあるCloudTrailのデータおよび発生イベントの全一覧
- 右にはそれぞれのイベントのユーザーセッションの合計数と全体に対する割合を表示

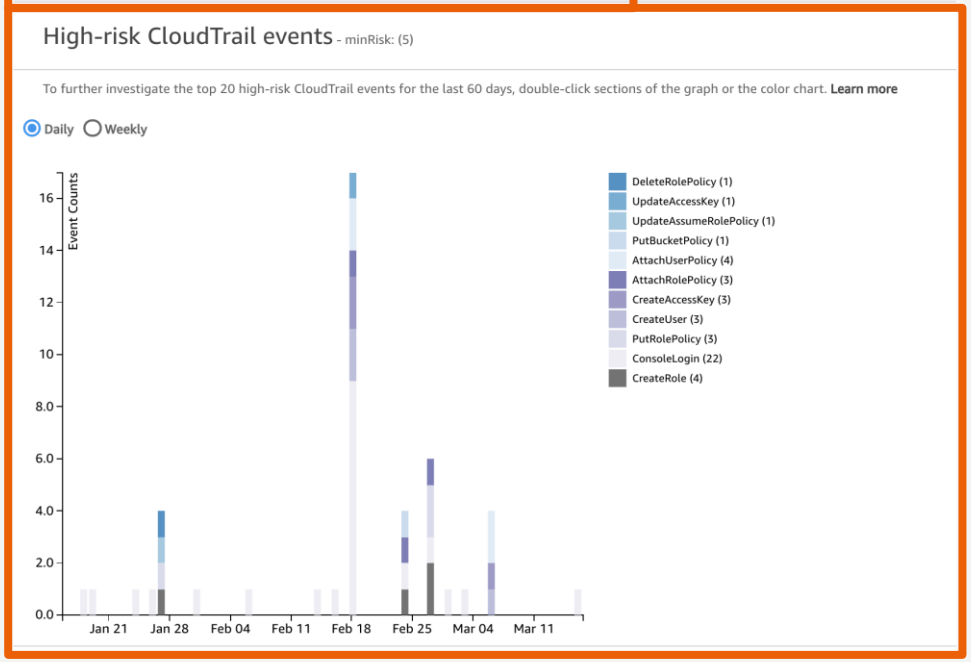
aws

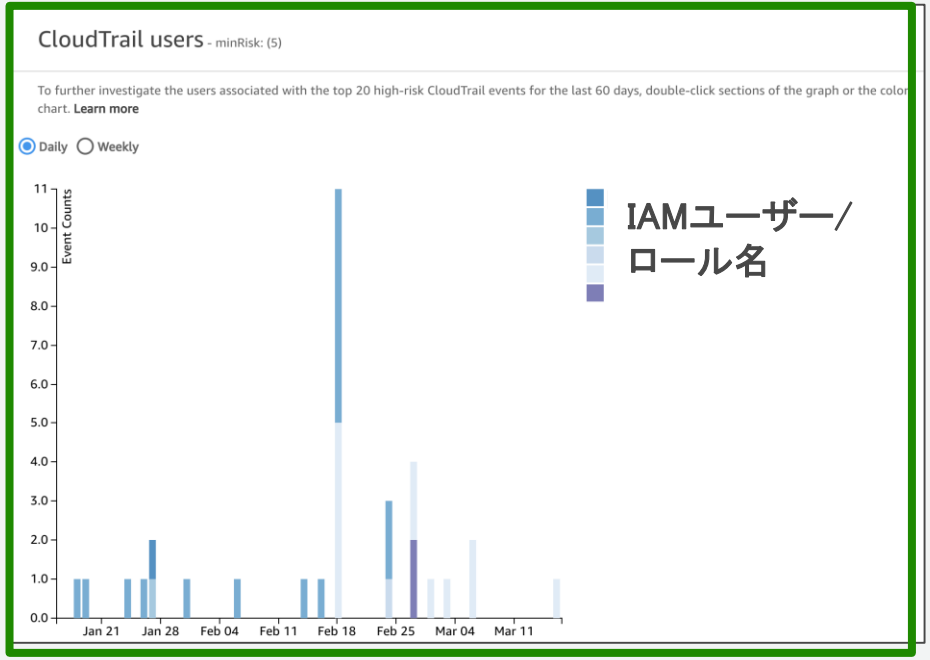
CloudTrail イベント時系列グラフ

DASHBOARD



リスクレベルでの絞り込み





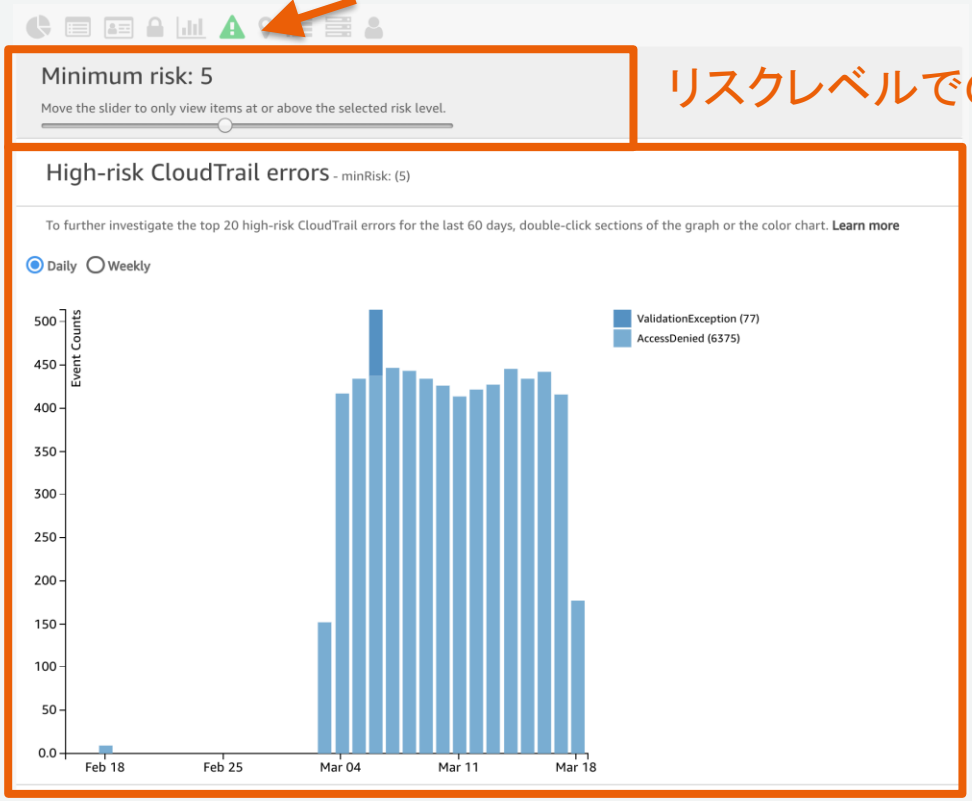
最近 60 日間で発生した上位20件の CloudTrail データおよび管理イベントの時系列表示

実行ユーザー別のイベントの時系列表示

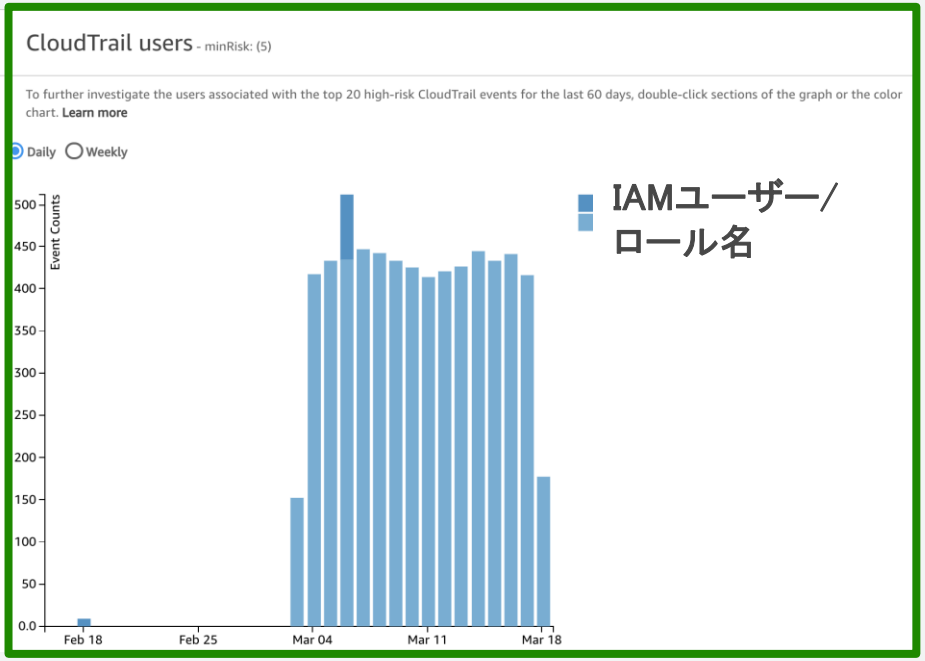
aws

CloudTrail エラー時系列グラフ

DASHBOARD



リスクレベルでの絞り込み

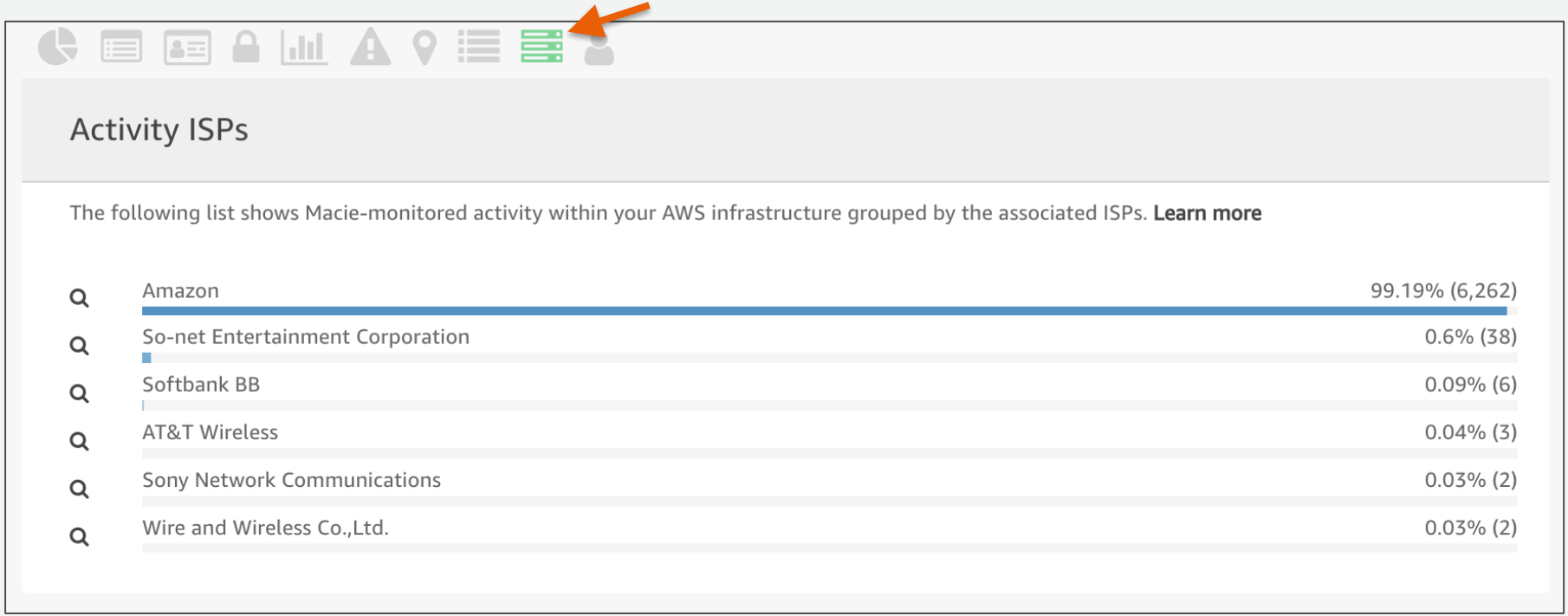


最近 60 日間で発生した上位20件の CloudTrail エラーの時系列表示

実行ユーザー別の発生エラーの時系列表示

アクティビティ ISP

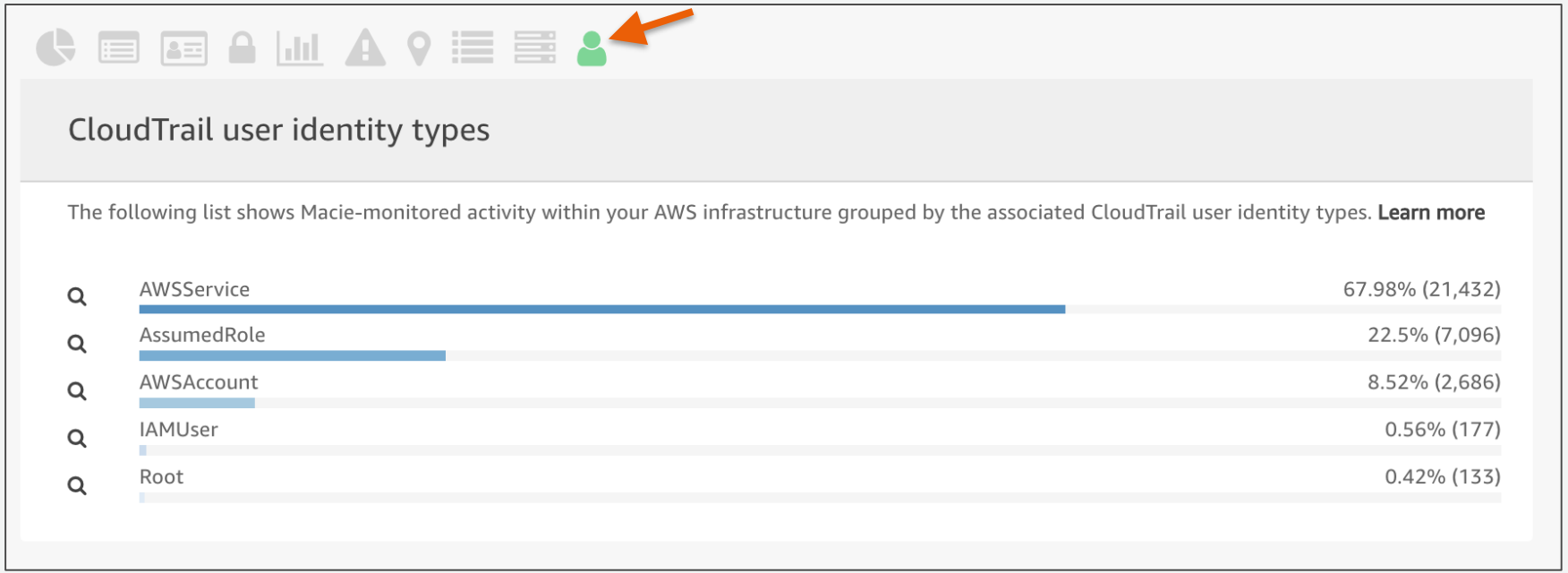
DASHBOARD



- CloudTrailに記録されている実行されたイベントがどのこ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

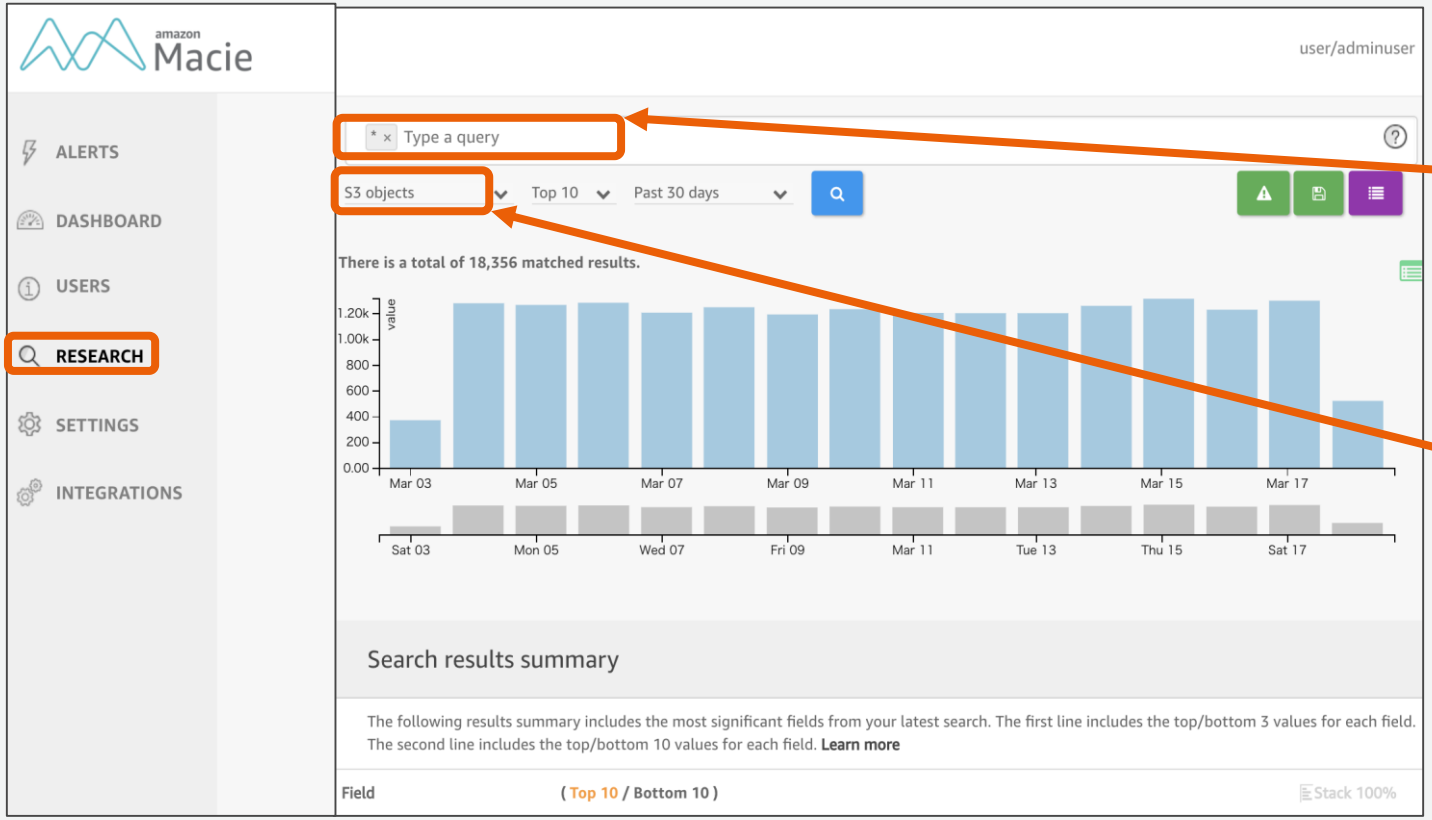
DASHBOARD



- 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

aws

Researchタブで検索する

RESEARCH

- 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

aws

Researchタブで検索する：検索例

RESEARCH

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	eventNameIsp.compound:/ConsoleLogin:~(Amazon.*)/
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	themes:"aws_access_key"
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	filesystem_metadata.bucket:"my-public-bucket" AND (pii_impact:"moderate" OR pii_impact:"high")
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	dlp_risk:>7 OR pii_impact:"moderate" OR pii_impact:"high"

aws

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

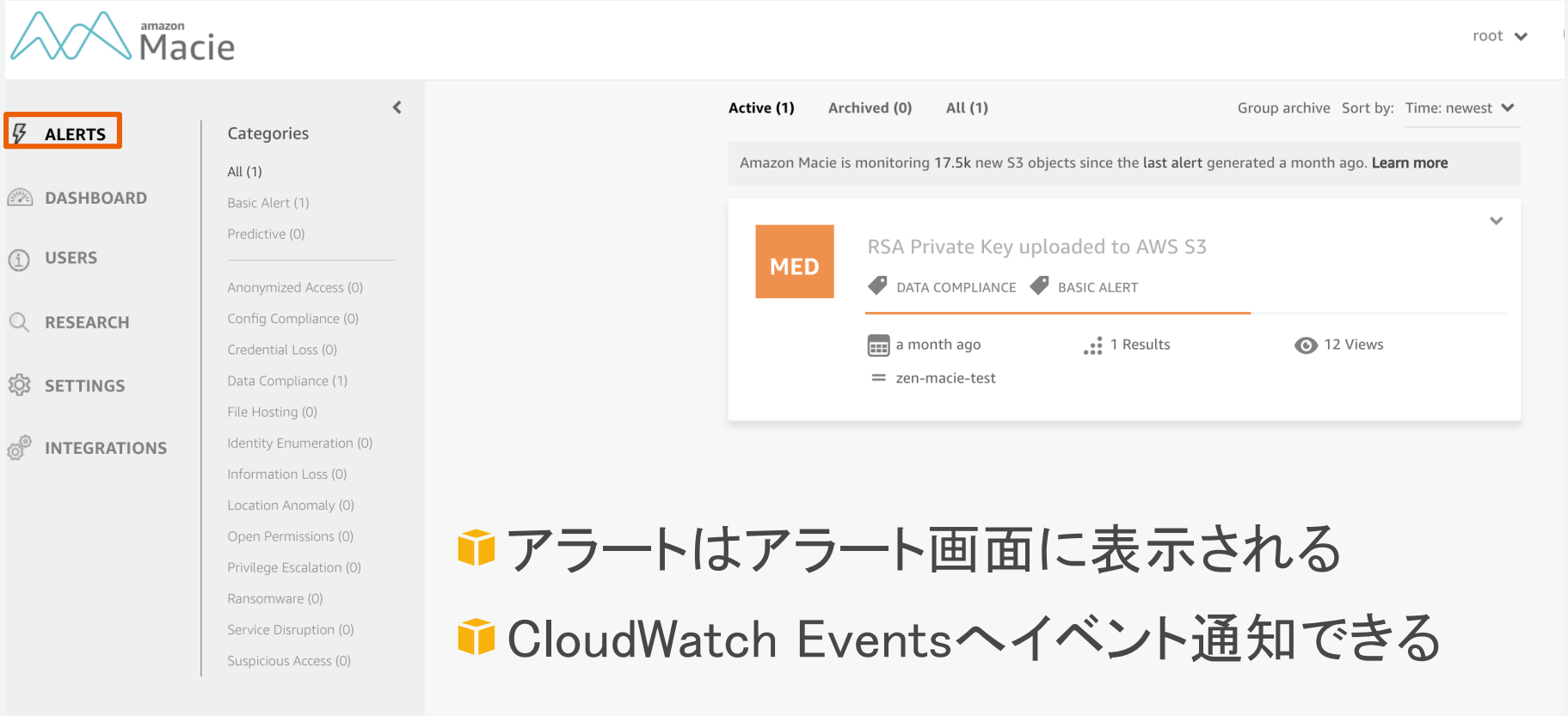
CloudTrailデータを監視

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

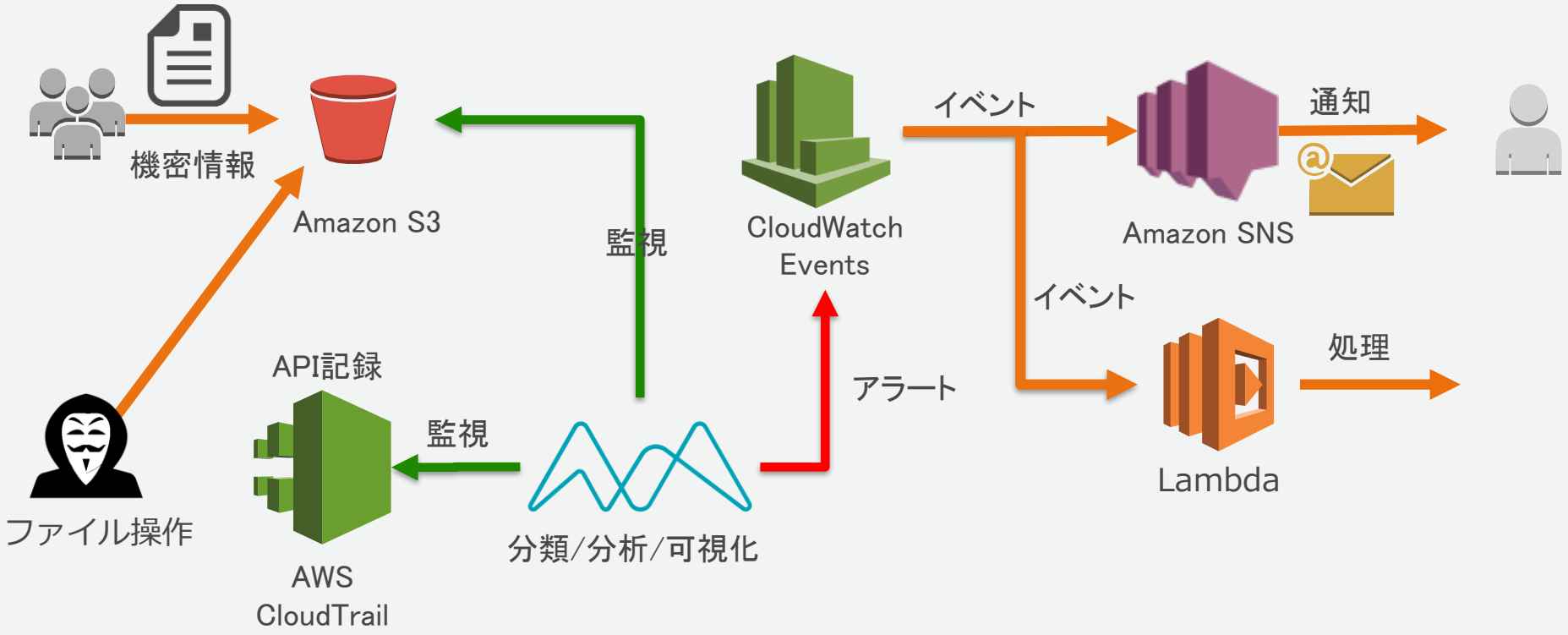
アラートによる警告

ALERTS



- 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

小

※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。

CloudTrailをデータソースとするマネージド型アラート

リスク 大 小

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
匿名のプロキシー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。

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

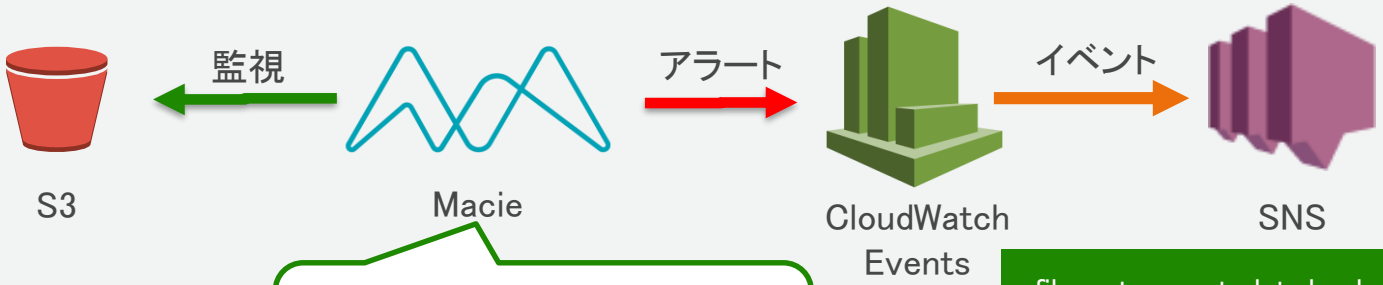
	内部の脅威	外部からの脅威
偶発的な脅威	アクセス権限の変更の検出 Publicなバケットにアップロードされた PIIの警告 ユーザーの通常とは異なるアクセスパターンの検知 他社の保持するデータはクロスアカウントでの監視	
意図的な脅威	社員や元社員が金銭目的や怨恨による理由で社内の機密情報を持ち出す	セキュリティホールや不十分な権限管理を突かれての不正アクセスによる情報の漏えい

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

- 個人情報が不特定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う



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**

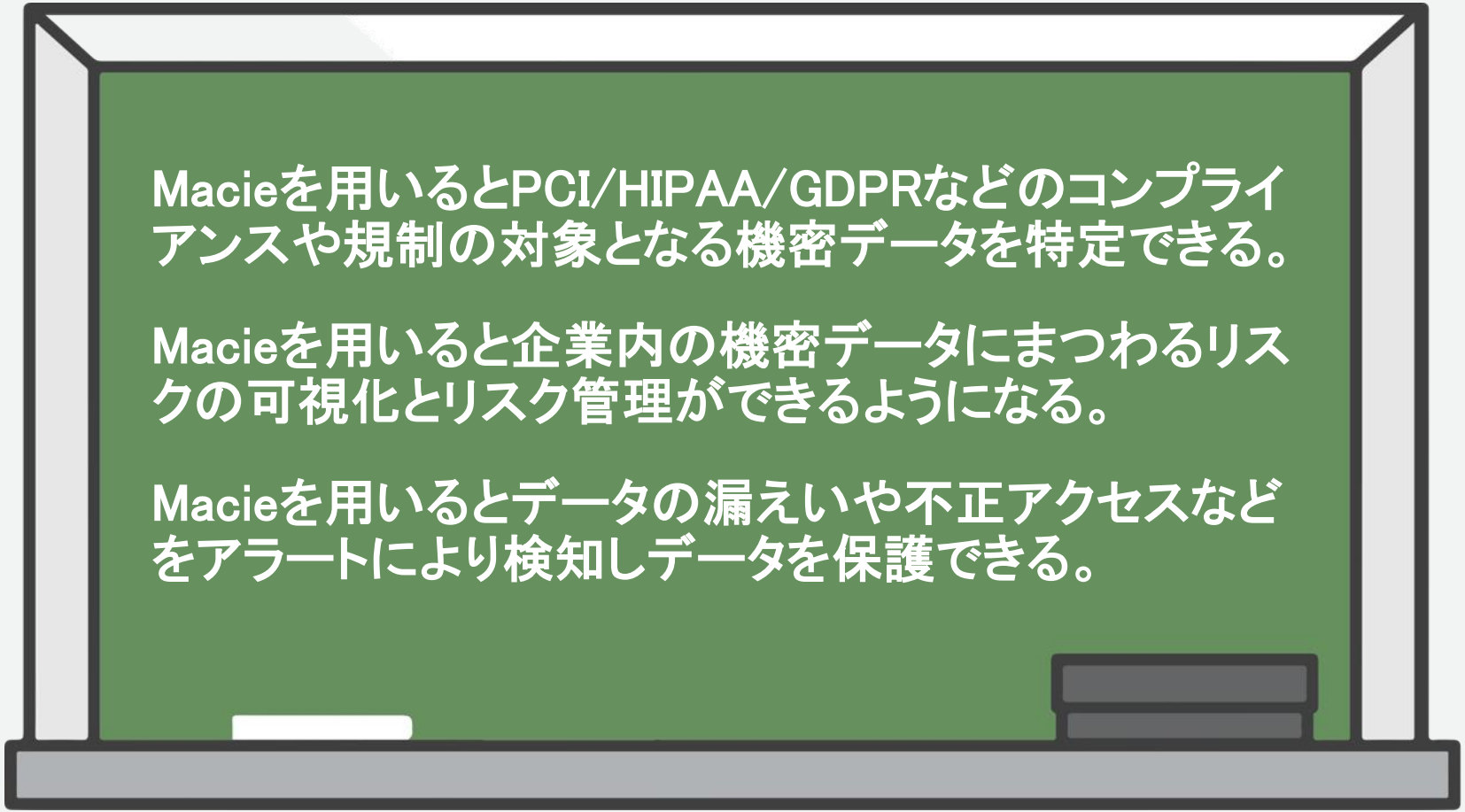
Macieの料金

＝ コンテンツ分類（GB） ＋ CloudTrail イベント処理(件数) ＋ 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）

https://aws.amazon.com/jp/macie/pricing

まとめ


Macieを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/

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

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/

※「AWS 問い合わせ」で検索して下さい。


aws