【 Amazon S3 の最新セキュリティ対策 】

～悪意あるオブジェクトの排除から設定不備対策まで～

2021年9月
トレンドマイクロ株式会社
AWSアライアンス担当：姜 貴日

姜 貴日 - Kwiil Kang

トレンドマイクロ株式会社
セールスエンジニアリング部
AWS Alliance Tech Lead

「Security Automation」、「DevSecOps」、 「Container」など
よりクラウドと親和性が高い領域に特化したソリューション提案を行う。

トレンドマイクロ Webinar 2020

トレンドマイクロ
& New Relic共催セミナー

JAWS DAYS 2021

AWS Summit Tokyo 2021

クラウドセキュリティ普及 のための 取り組み

トレンドマイクロはアマゾン ウェブ サービス ジャパン社（AWS）と ともに
クラウド環境のセキュリティ啓蒙活動に取り組んでいます。

★ クラウド環境の脅威に関する情報発信･学習機会の提供

★ クラウドセキュリティのベストプラクティス・考え方を発信

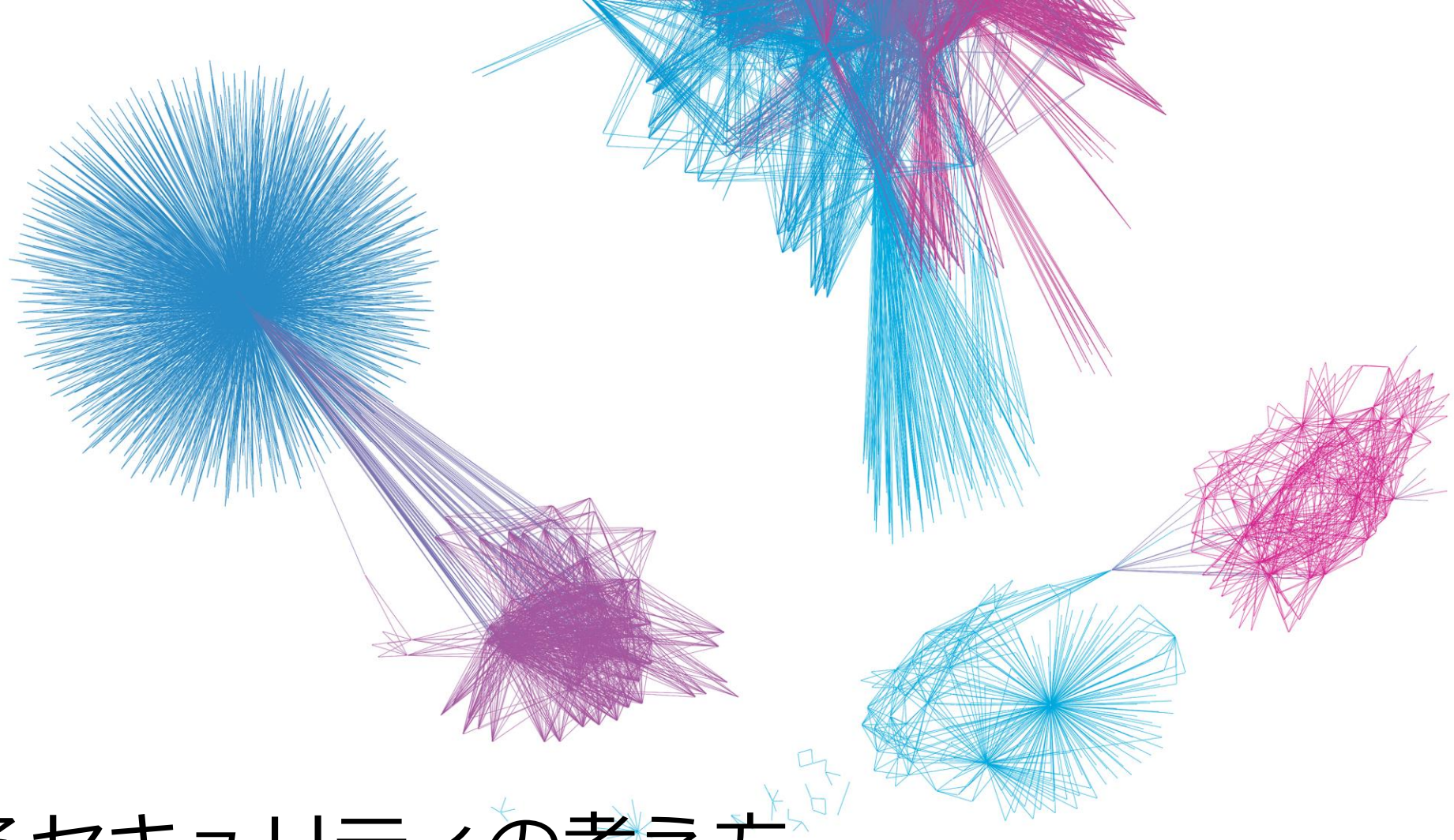
トレンドマイクロは法人組織のセキュリティイノベーション推進を支援する
組織を設立し、セキュリティの啓蒙に努めています。

★ サイバーセキュリティ・イノベーション研究所 設立

- トレンドマイクロ製品･サービスの安全性評価
- 役割に適したセキュリティ教育の提供
- 専門性の高い脅威分析と、その結果の公開

アジェンダ

1. AWSにおけるセキュリティの考え方
2. クラウドセキュリティの最新動向
3. Trend Micro Cloud Oneのご紹介
4. File Storage Securityのデモ
5. まとめ



AWSにおけるセキュリティの考え方

AWSのセキュリティの考え方:責任共有モデル

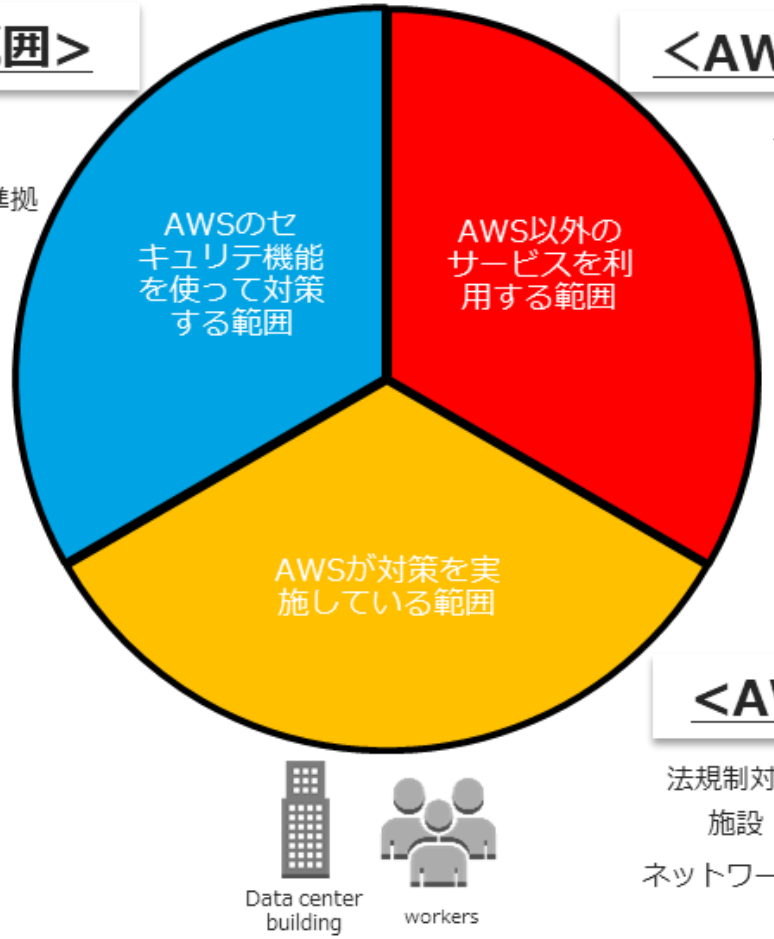
- お客様はクラウド内のセキュリティに責任を持ちます。
- お客様の責任は、選択した AWS クラウドのサービスに応じて異なります。

参照：https://aws.amazon.com/jp/compliance/shared-responsibility-model/

責任共有モデルをもう少し詳しく

<AWS機能を使ってユーザが対策する範囲>

セキュリティ診断　鍵管理
ユーザー認証　コンプライアンス準拠
ファイヤウォール　WAF
データ暗号化　DDoS対策



<AWS以外のサービスを利用する範囲>

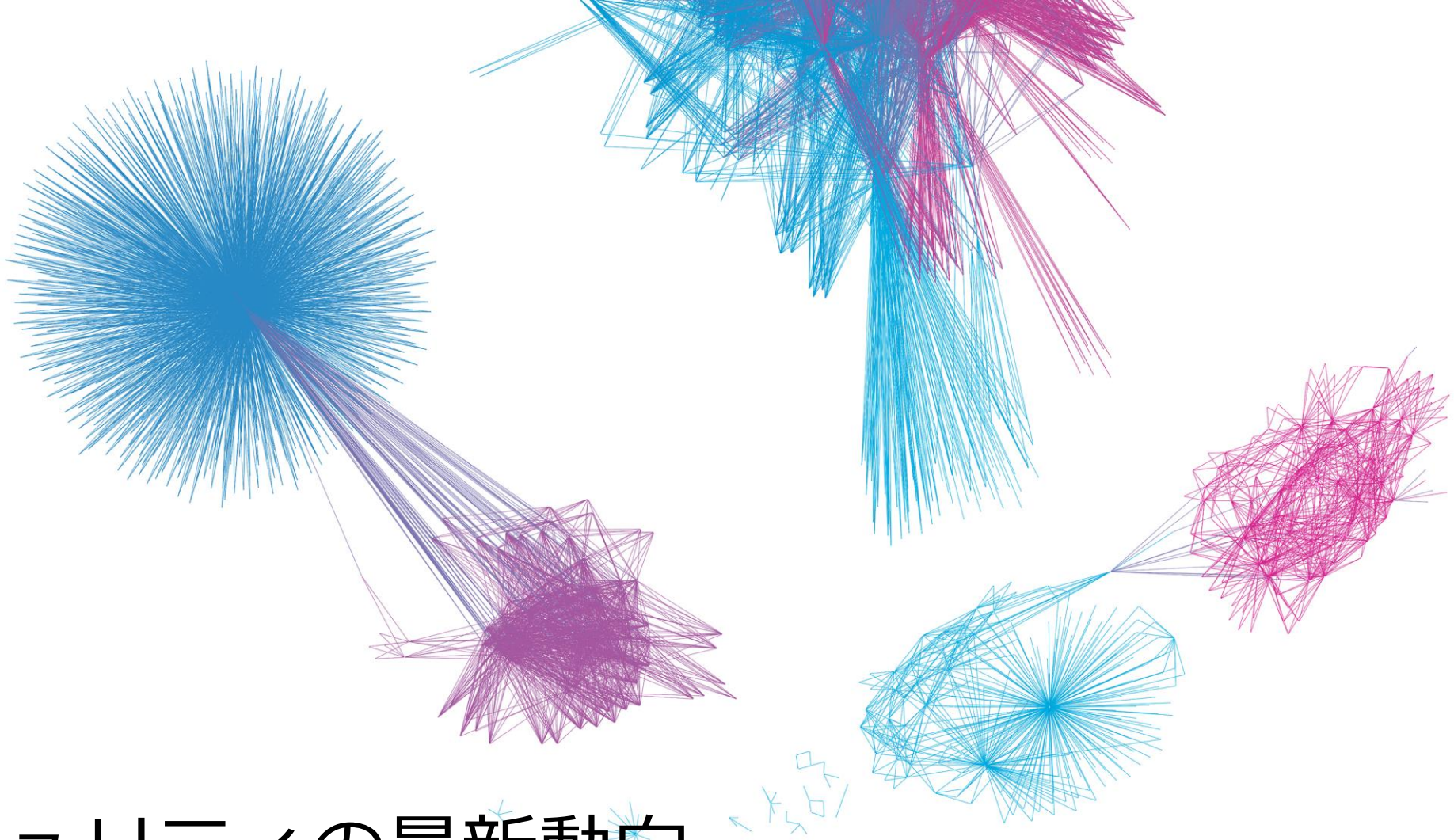
インシデントレスポンス　フォレンジック
セキュリティ診断　アンチマルウェア
IPS/IDS,WAF　改ざんの検出

TREND MICRO

<AWSが責任を持つ範囲>

法規制対応　ログ管理　ストレージ
施設　物理冗長性　サーバー
ネットワーク　ハイパーバイザー

AWSをさらにセキュアにするためにベンダーを活用

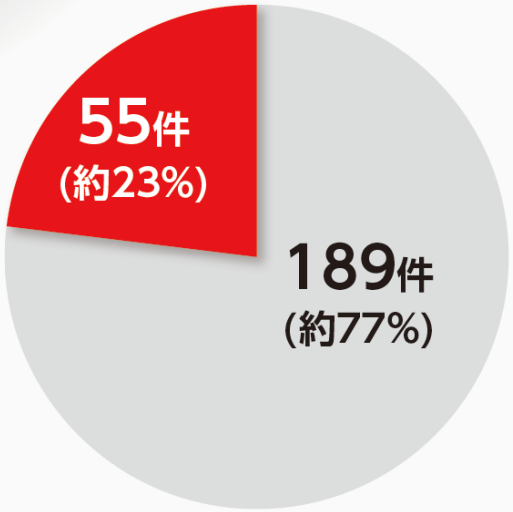


クラウドセキュリティの最新動向

クラウド環境で観測された攻撃例　①脆弱性を利用

アプリケーションの脆弱性に要注意

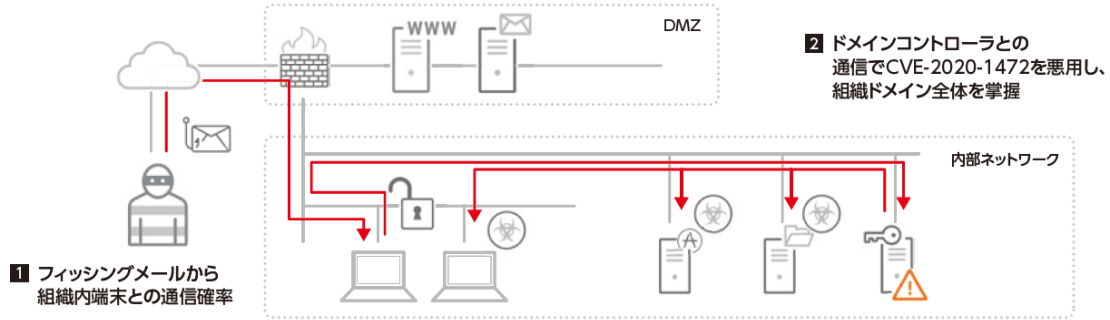
公表事例のうち、約4件に1件は脆弱性が原因でインシデント発生



脆弱性（OS・ミドルウェア）
脆弱性（Webアプリケーション）
脆弱性（詳細不明）
アカウントリスト攻撃
アカウント侵害
設定ミス
ブルートフォース/辞書攻撃
メール経由
持ち出し用PCの侵害
その他
不明

※ 2020年の1年間で被害を受けた法人/団体がインターネット上で情報公開した事例を、トレンドマイクロが独自に集計した数値に基づく

サーバ関連の脆弱性 ～ Zerologon（CVE-2020-1472）～



オンプレであっても、クラウドであっても、
アプリケーション、ミドルウェア、サーバ領域は
常に脆弱性を悪用した攻撃の脅威に直面している

クラウド環境で観測された攻撃例 ②ランサムウェア(IR)

当社インシデントレスポンス実例（ランサムウェア）

【AWS】情報サービス業

種類：CRYSIS
被害：業務用サーバの暗号化

AWS上の公開サーバに侵入、
最終的にランサムウェアによって
サービス提供サーバ群が暗号化。

原因 メンテナンス時に緩めた
RDPポートの閉め忘れ

【AWS】小売業

種類：CRYSIS, CRING
被害：業務用サーバの暗号化

AWS上のサーバに侵入、
最終的にランサムウェアによって
業務用サーバ群が暗号化。

原因 内部サーバに意図せず
外部IPを付与して公開

【Microsoft Azure】卸売業

種類：PYSA
被害：業務用サーバ・PCの暗号化

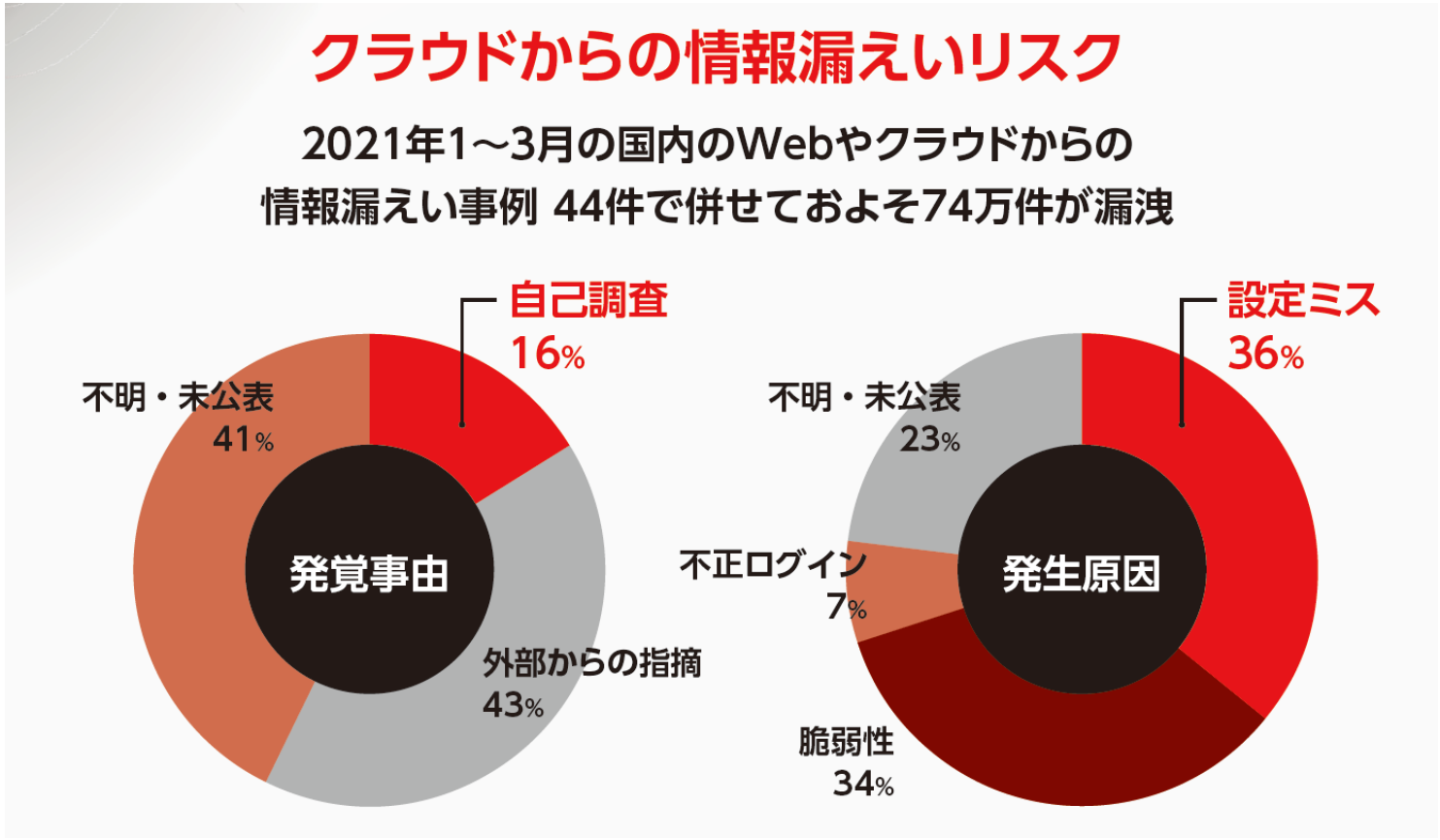
Azure上のサーバに侵入、
最終的にランサムウェアによって
サービス提供サーバ群が暗号化。

原因 内部サーバに意図せず
外部IPを付与して公開

いずれの場合も
クラウドの設定ミス・設定不備によって不正アクセスされたことが確認。

※この例は利用ユーザの設定不備に起因するものであり、AWSサービス自体に問題があるわけではございません。

クラウド環境で観測された攻撃例 ②ランサムウェア(IR)



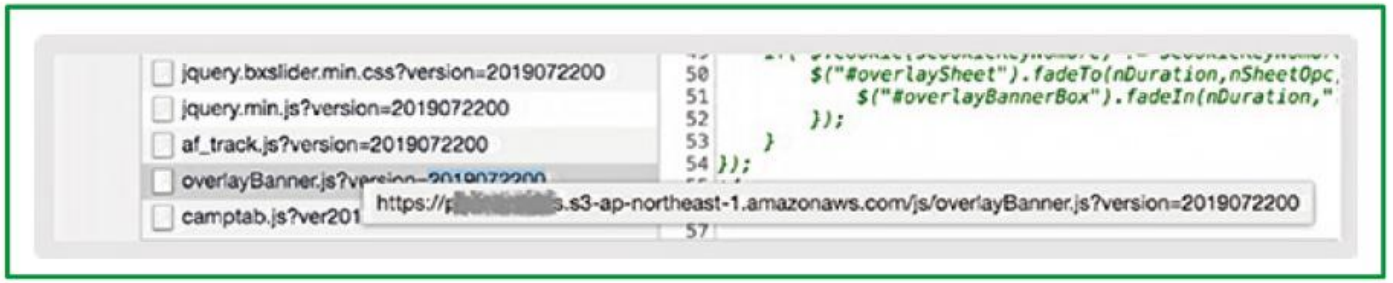
当社調べでは、情報漏えいインシデントの発生原因の多くを占めている。
脆弱性対策とあわせて設定ミスへの対策も重要

クラウド環境で観測された攻撃例 ③不正?ファイル設置

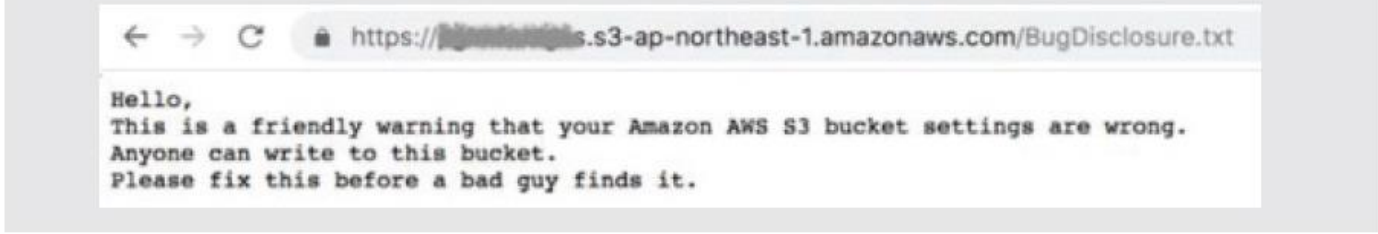
クラウドストレージに設置されたファイル

Webシステムとして
クラウド利用

Amazon Simple Storage Service
(Amazon S3)



Webシステム用に
Amazon S3を利用していて
読み取り権限だけではなく
書き込み権限も許可されていた
事例が国内外で確認。



内部利用のS3に誤って外部からの書き込み権限を付与していたため、
ブラウザ上でこれを確認され、第三者から警告文ファイルが設置されていました。
おそらく善意の警告文だと思われますが、当然不正なファイルの設置も可能な状況です。

※この例は利用ユーザの設定不備に起因するものであり、AWSサービス自体に問題があるわけではございません。

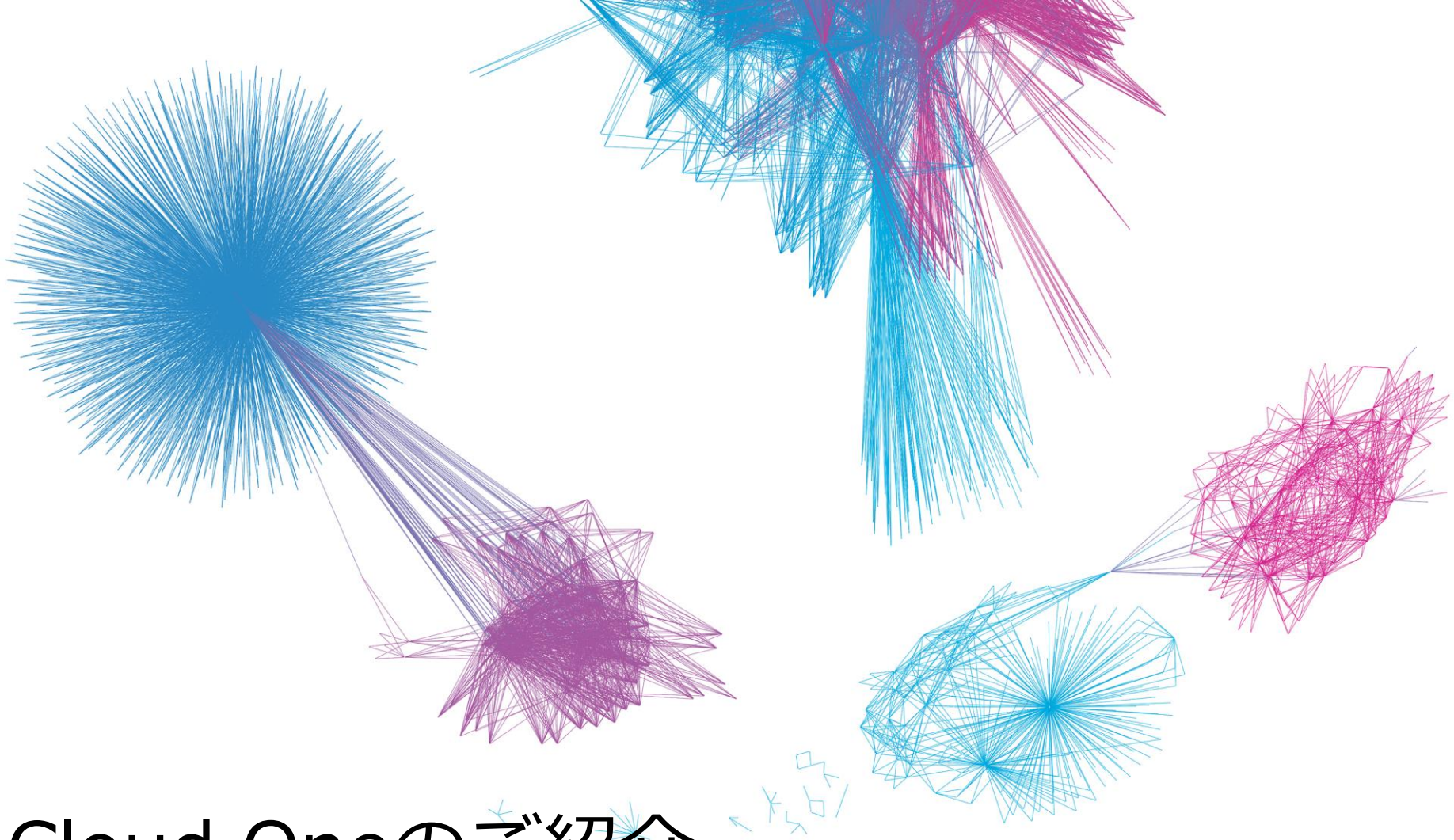
ここだけは押さえておきたいセキュリティのポイントは？

脆弱性対策

公開サーバ経由の情報漏えい・Web改ざんだけでなく、ランサムウェアの侵入・拡散経路としても利用。

設定ミス

クラウドは簡単に使い始められる、オンプレの環境とは設定項目が異なる。こうした理由から設定の見落としが発生しがち。

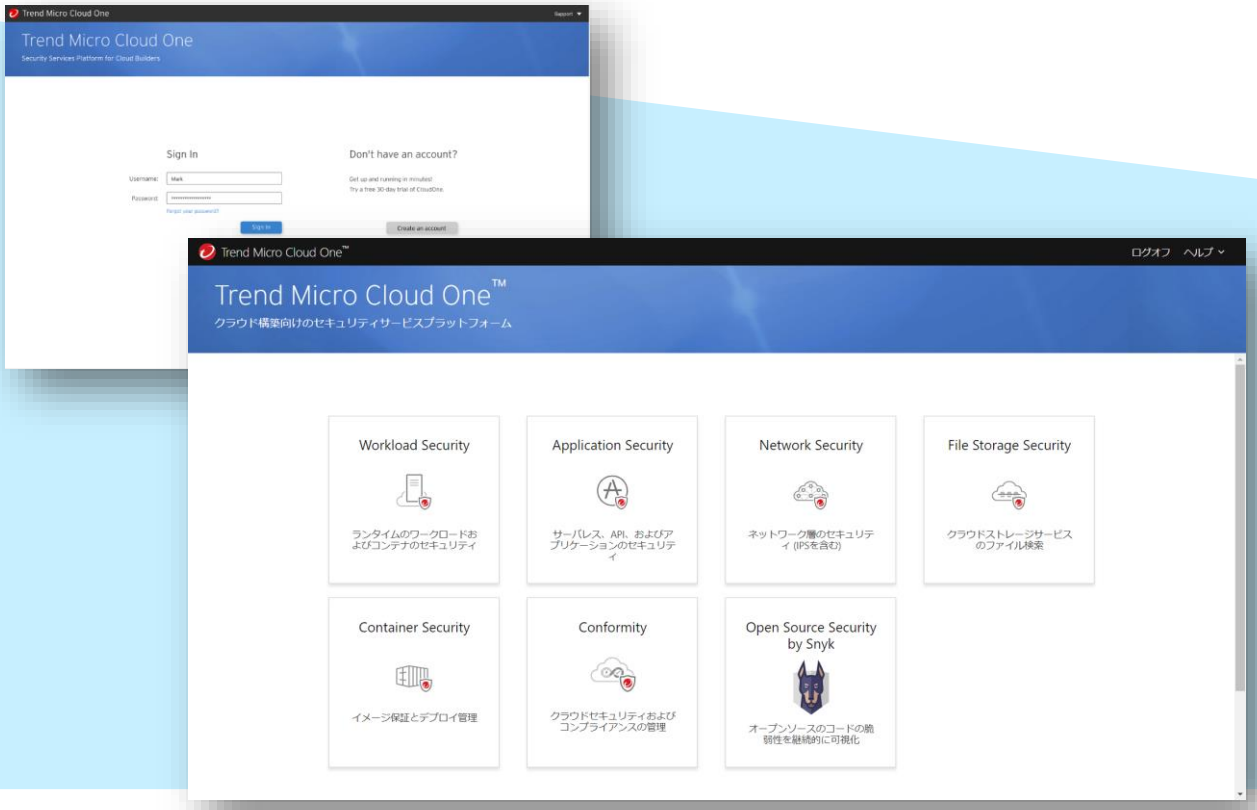


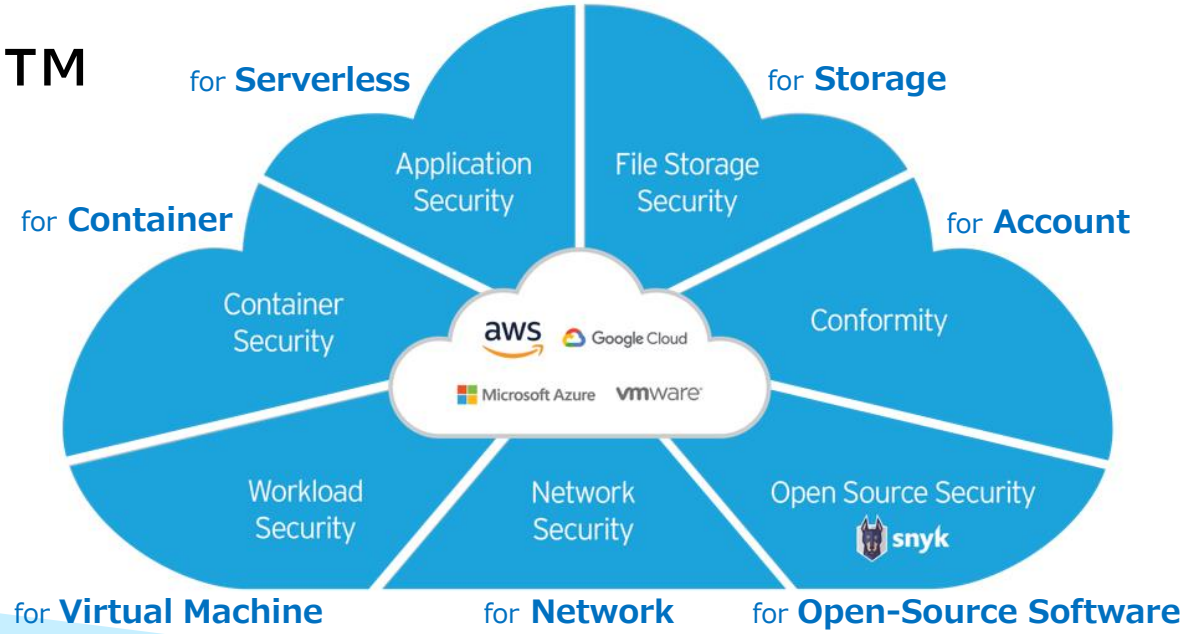
Trend Micro Cloud Oneのご紹介

Trend Micro Cloud One™

多様なサービスで構成されるクラウド環境を
まとめて保護するセキュリティサービス群

- クラウドセキュリティプラットフォーム -





単一コンソールから各製品にシングルサインオン
クラウドセキュリティを管理運用しやすく――

Trend Micro Cloud One 傘下の製品群

Workload Security

クラウド上の仮想マシン（インスタンス）にソフトウェアとしてインストールすることで脆弱性対策や多層防御を提供。

Application Security

セキュリティを「アプリケーション機能の一部」として組込む。
Webアプリケーションへの攻撃を検知・ブロック。

Network Security

クラウド環境上のネットワーク型IPS製品。
Amazon VPC内のリソースに対する脆弱性を利用する攻撃通信を検知・ブロック。

Container Security

レジストリに保存しているコンテナイメージに対して脆弱性やウイルススキャンを実施、これを検知。

File Storage Security

Amazon S3などのクラウドストレージにアップロードされるファイルに対してウイルススキャンを実施。

Conformity

情報漏えい・不正な遠隔操作等を引き起こす可能性がある設定の不備を検知し、リスクを可視化。

Open Source Security by Snyk

オープンソースに存在する脆弱性やライセンス問題などをスキャン・検知してリスクを可視化。

※ 2021年6月時点、日本商流では販売していません。

Cloud One - Conformity

AWS、Azure、Google Cloudなどのクラウドアカウントと連携させることで、情報漏えいなどのインシデントにつながる設定不備･設定ミスを検知して、リスクを可視化します。ユーザのコンプライアンス対応を支援します。

スキャン結果イメージ

実際のコンソールは英語表記のみです。

特徴

- AWS, Azure、Google Cloudが提供する60以上のサービスに対応（Google Cloudは2021年対応予定）
- 700を超えるルールでリスクを可視化
- AWS Well Architected Framework, PCI DSS, HIPAA, NIST, GDPR, CIS、FISC安全対策基準などに対応

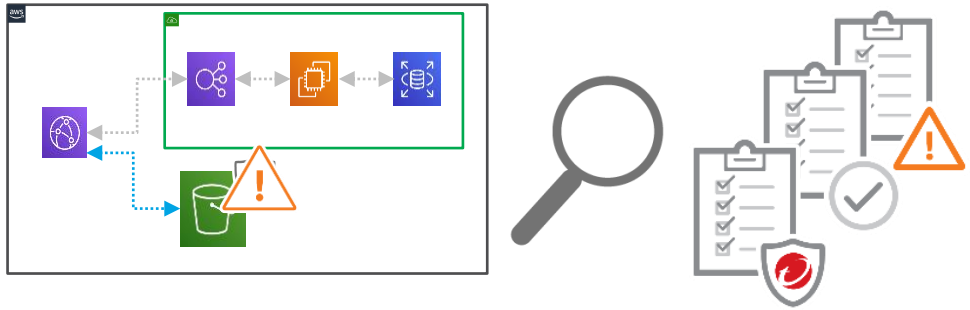
提供機能

- Security and Compliance
  - AWS Well-Architected Frameworkをベースとして、700個以上のルールで設定不備やコンプライアンス状況を可視化。
- Template Scanner
  - CloudFormation や TerraformのTemplatesをアップロードする事でテンプレート上のリスクを可視化・修復を支援。
- Real-Time Threat Monitoring
  - AWSアカウント上のリソースにルール違反がないかをリアルタイムに検出。
- Auto-Remediation
  - 修正方法を提示、AWS Lambdaと連携することで、簡易的なセキュリティやガバナンスの自動化を実現。※OSSにて提供

Cloud One – Conformity ユースケース

1、S3の閲覧権限のPublic設定を検出し、情報漏えいを抑止

2、コンプライアンスに違反する設定不備を検出



3、意図しない権限昇格がされていないか AdministratorAccess Policyの付与の監視

4、許可していないリージョンでのリソース利用を検出

5、CloudFormation やTerraform Templateをスキャンすることによるセキュリティ課題の早期発見

6、複数部署で利用されているマルチクラウド環境の可視化

Conformity – 動作イメージ①

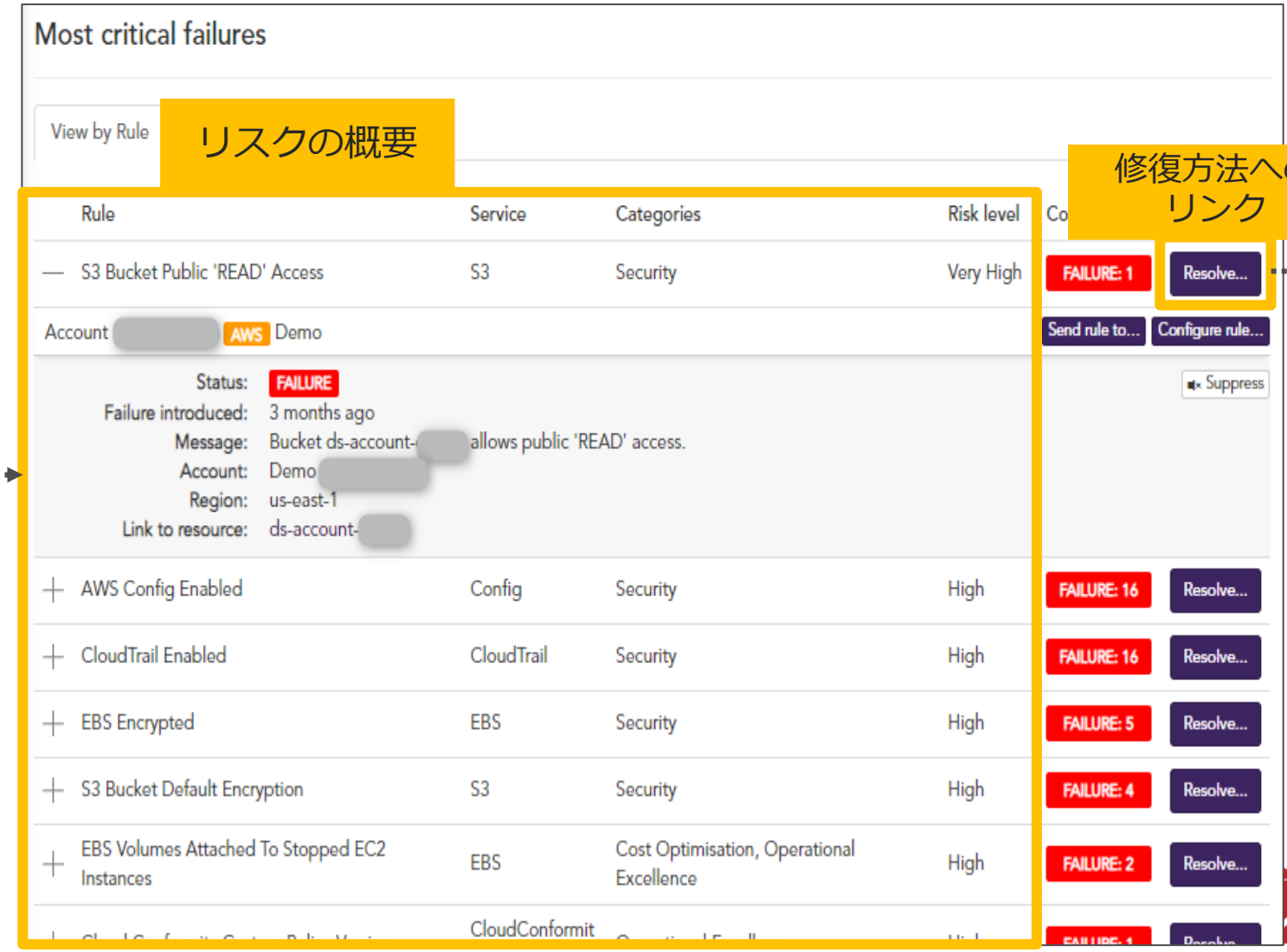
AWS Cloud

①アカウント配下の
リソース情報を
定期取得
(Conformity bot)

②設定不備を測定

③リスクの
可視化

スキャン結果

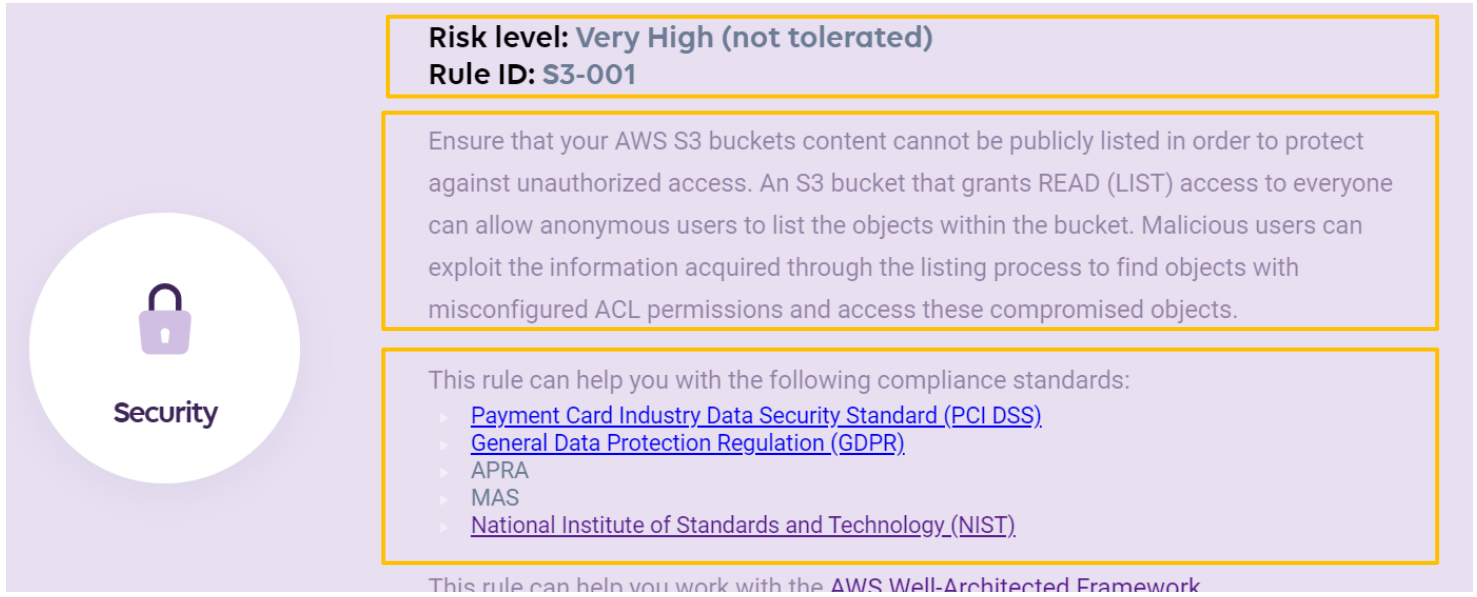


④Resolve
をクリック

Conformity – 動作イメージ②

(ルール解説) バケットがPublic状態でどのようなリスクがあるのか

④Resolve
をクリック



リスクレベル

リスクの説明

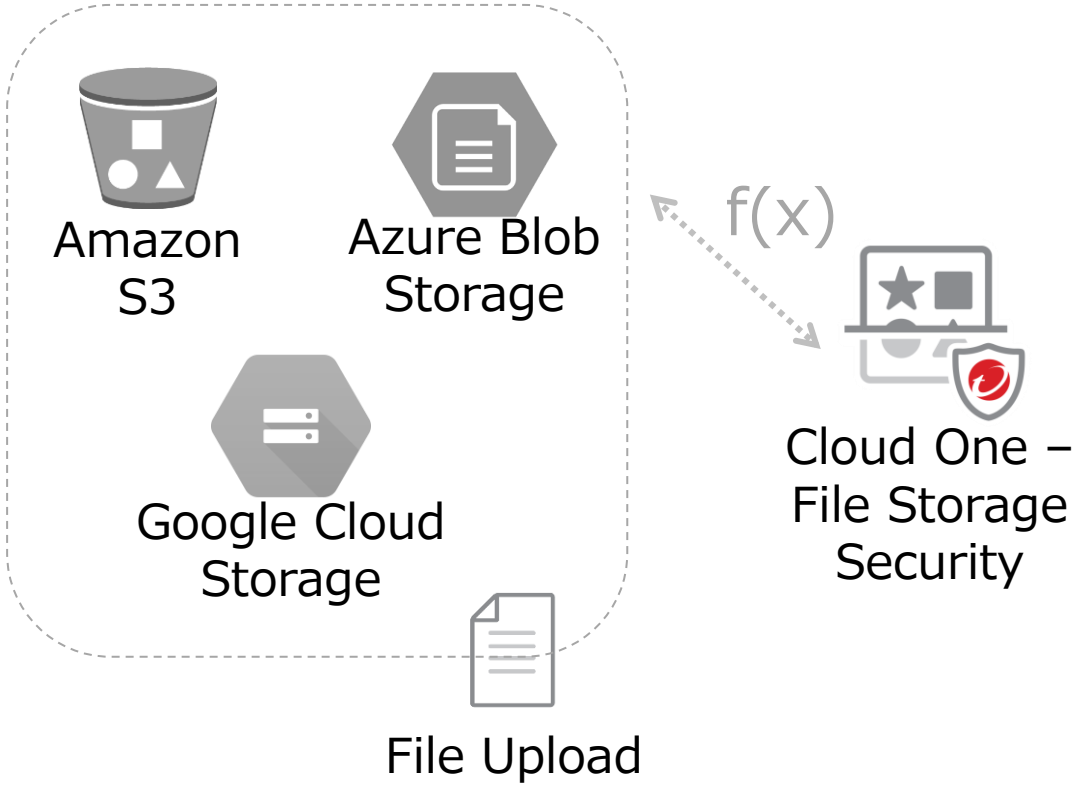
関連するコンプライアンス

2種類の修復方法を提示

Cloud One – File Storage Security

パブリッククラウドベンダーが提供するクラウドストレージを保護するセキュリティ機能を提供します。
これらに対してアップロード、保管されるファイルをスキャンします。

構成イメージ



※Google Cloud Storageは対応予定となります。
※構成の詳細については弊社担当へご相談ください。

提供機能

- Amazon S3, Azure Blob Storage、Google Cloud Storage 内のファイルをスキャン

特徴

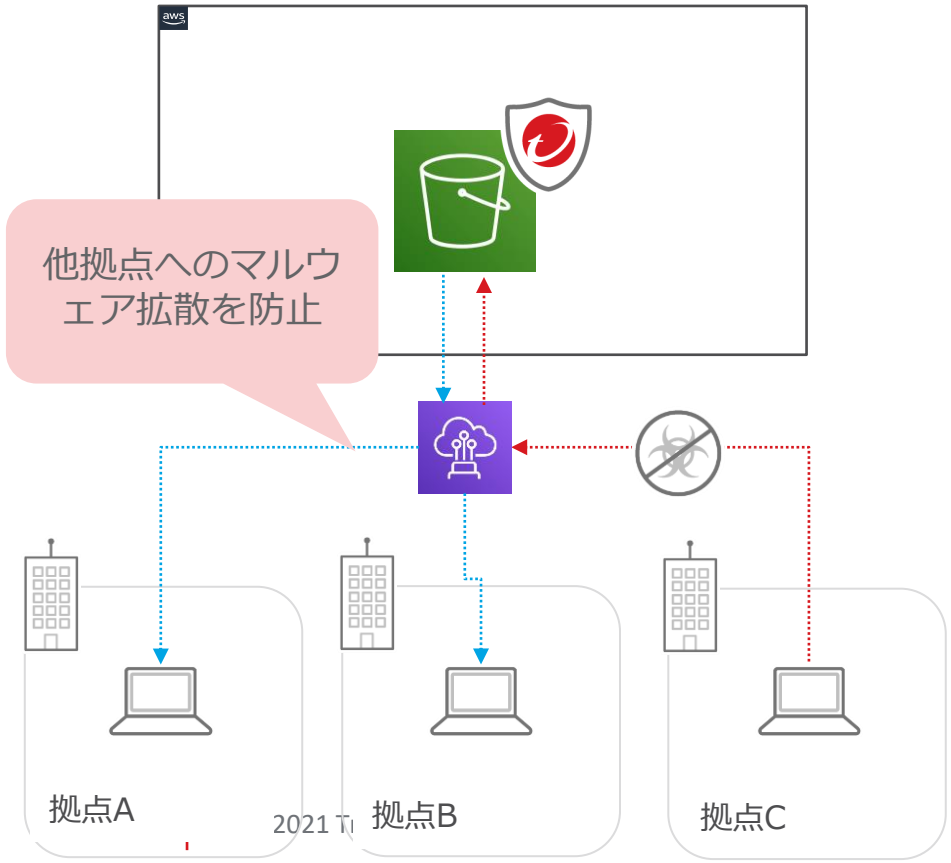
- AWS CloudFormation Templateとして提供
  サーバレスで機能実装のため、スキャンサーバの用意が不要
- ファイルの新規アップロード/ダウンロードの際には自動的にファイルをスキャン
- 不正プログラム検出後の自動隔離も実装可能
  ※OSSとして提供

TREND MICRO

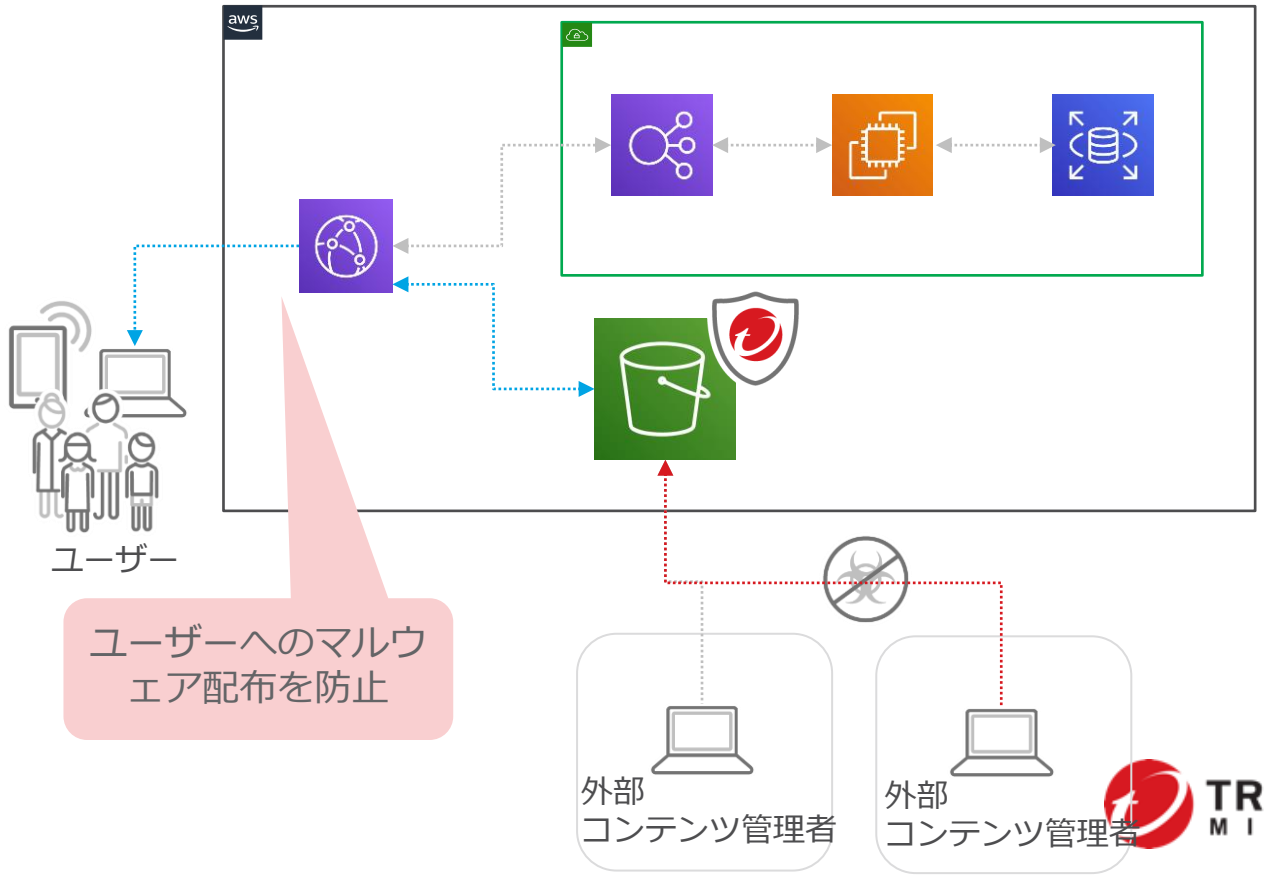
File Storage Security ユースケース

S3起点のマルウェア混入・拡散防止

**1、社内における複数拠点間のファイル共有先として
S3を利用している場合、
マルウェアの混入および拡散を防止**



**2、外部からデータを取り込んでS3へ保存する公開系システムの場合、マルウェアが混入および配信されることを防止
（例） ECサイト、投稿サイト、データクローリング　etc.**

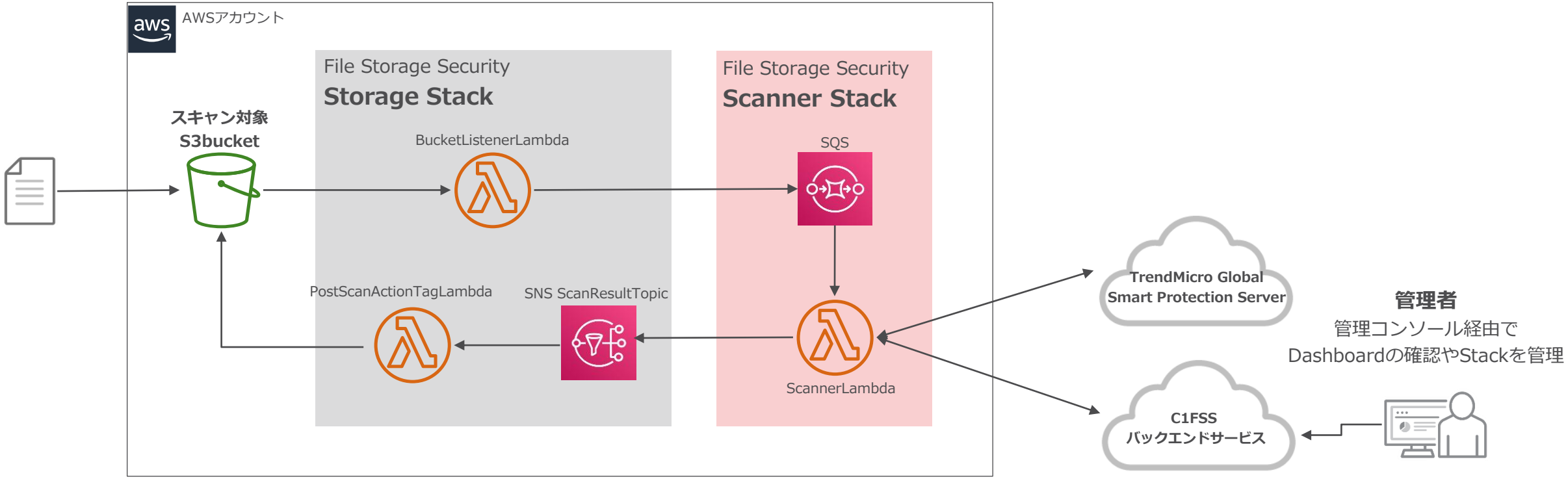


主な構成要素

File Storage Security はAWS CloudFormation Templateを用いてデプロイをします。最少2つのStackで構成されます。

1）Storage Stack
- スキャン対象のS3 bucketを監視
- スキャン結果を受け取る

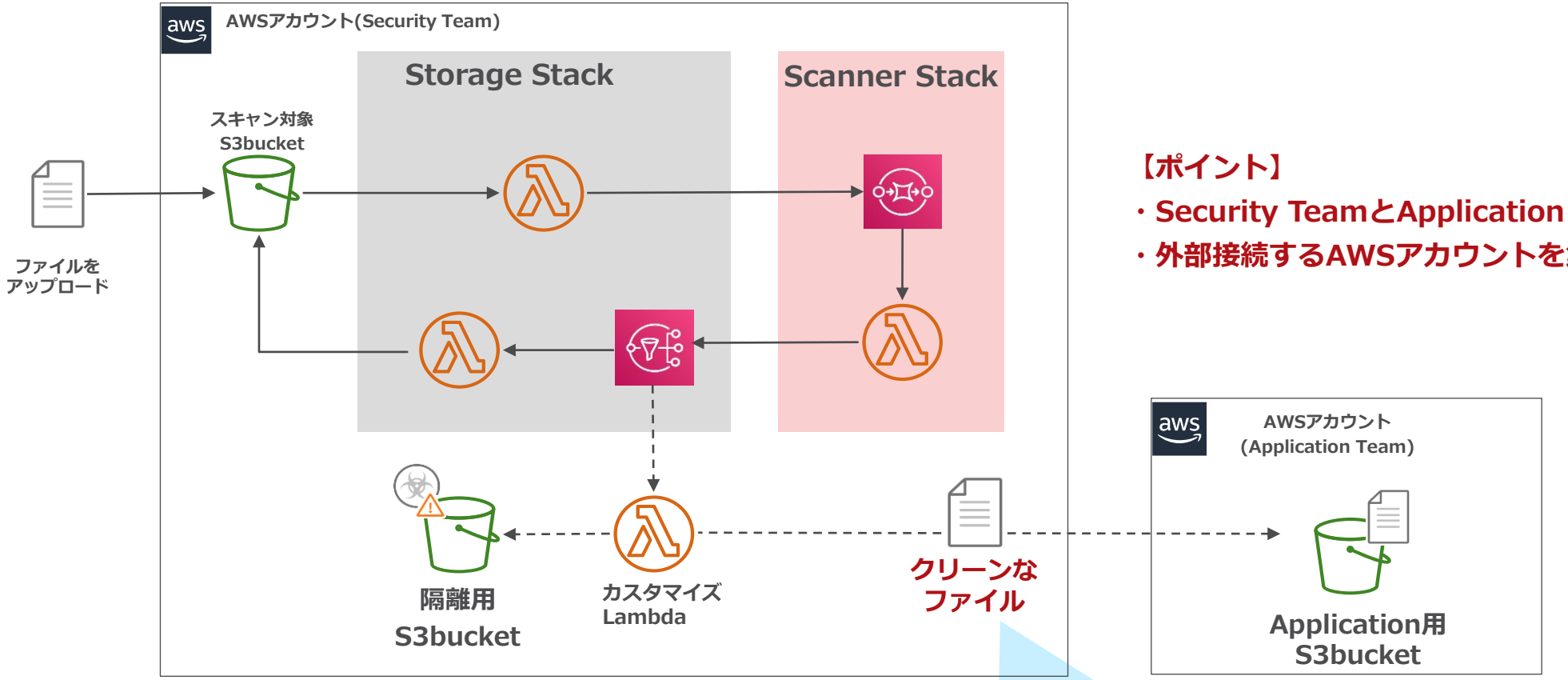
2）Scanner Stack
- ファイル識別情報をTrend Micro Global Smart Protection Serverに送信
- スキャン結果をStorage Stackに連携



※これらのStackはお客様のクラウド環境へデプロイいただきます。AWSリソース利用料はお客様のご負担となります。

デプロイパターン①：1つのAWSアカウント配下にデプロイ

スキャン後のアクションをカスタマイズすることで、お客様のご要望の構成やワークフローに柔軟に組み込むことができます。



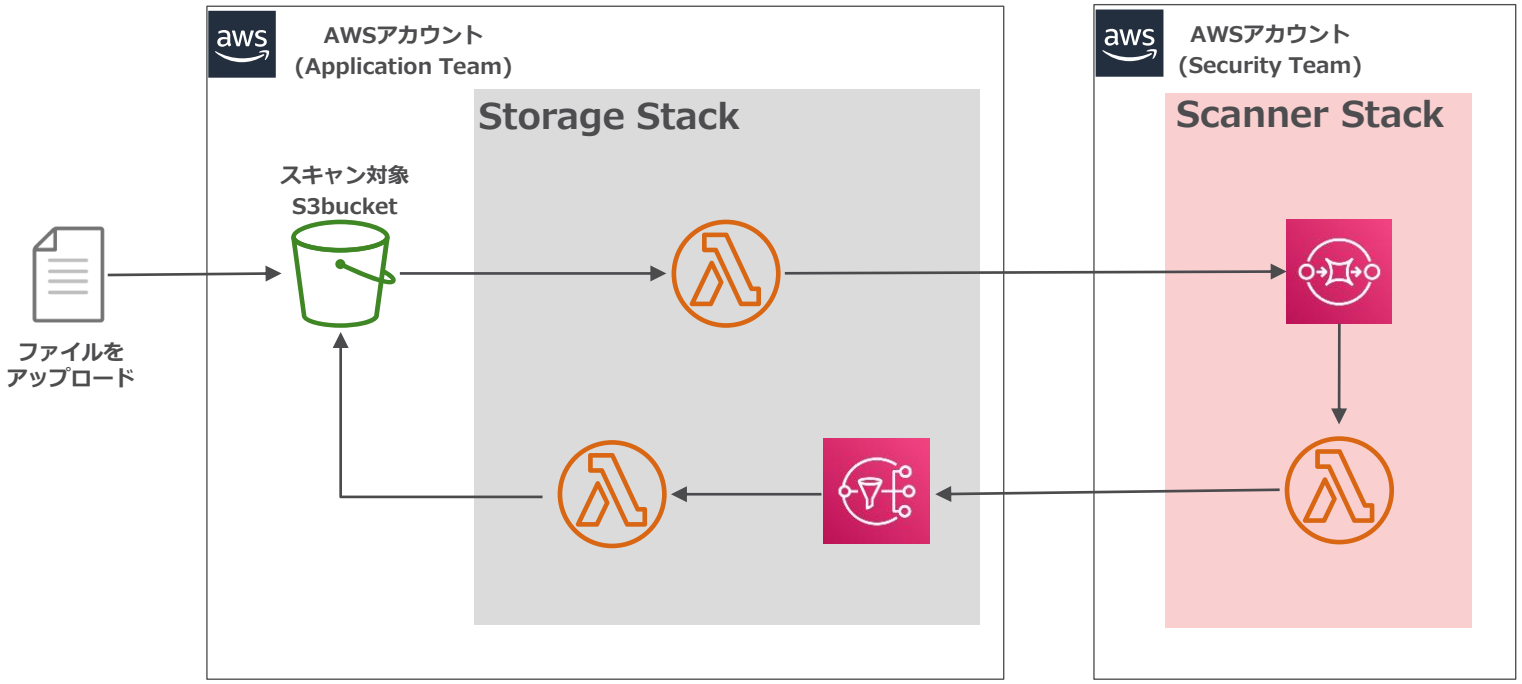
【ポイント】
- Security TeamとApplication Teamとで環境を分離
- 外部接続するAWSアカウントを集約

マルウェアではないファイルのみを
別アカウントのS3バケットへ転送

※スキャン対象のS3バケットとStorage Stackは同じリージョンを選択する必要があります。
※カスタマイズLambdaはお客様にて開発いただく必要がございます。

デプロイパターン②：ScannerとStorageを別々のAWSアカウントへデプロイ

Scanner StackとStorage Stackをそれぞれ別のAWSアカウント配下にデプロイする構成です。
AWS CloudFormation Templateを活用してそれぞれ簡単にデプロイすることができます。

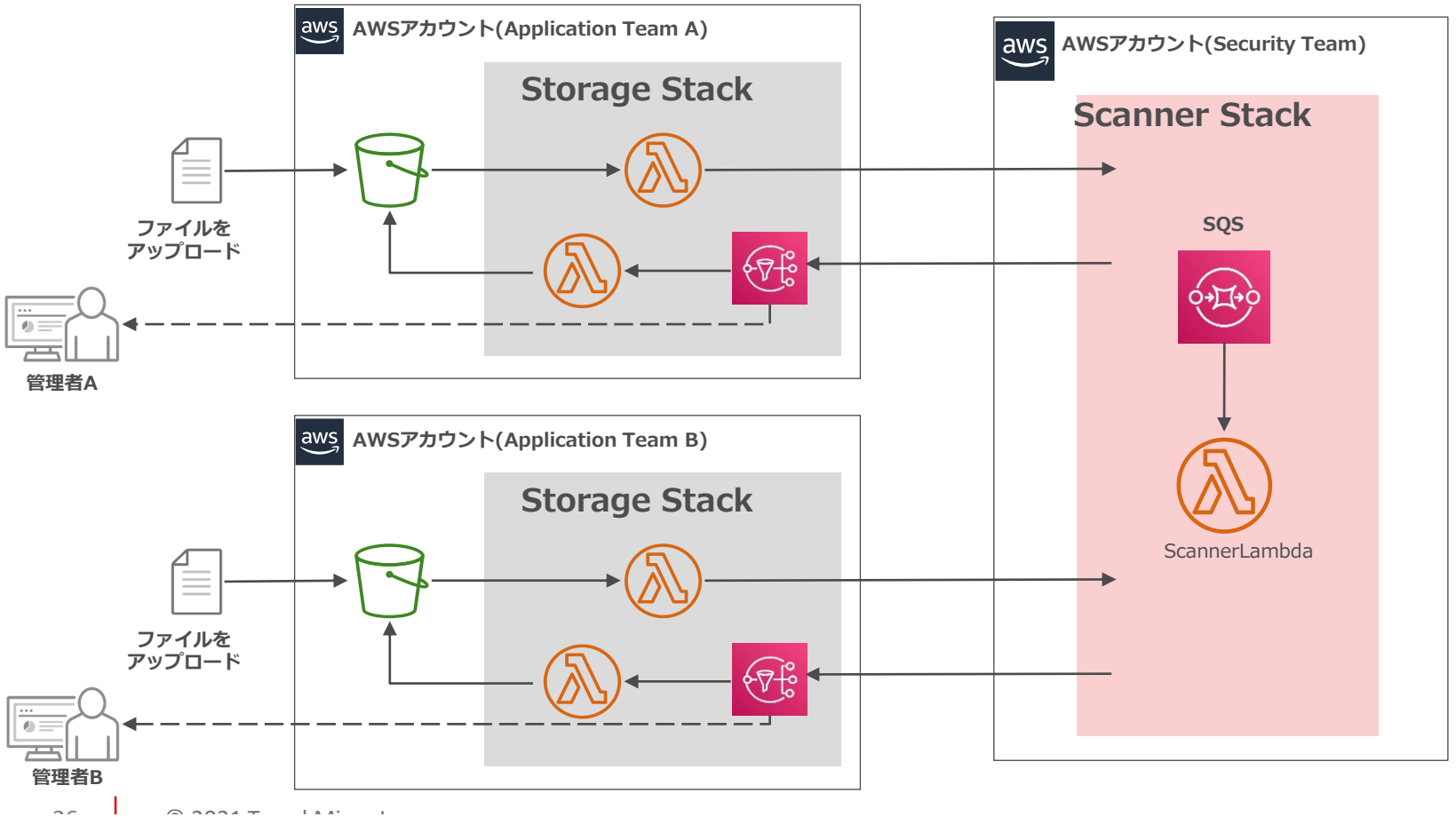


【ポイント】
・将来的にStorageを拡張する予定がある場合
・外部接続するAWSアカウントを集約
・AWS Lambdaの同時実行上限を分散させる必要がある場合

※スキャン対象のS3バケットとStorage Stackは同じリージョンを選択する必要があります。
※パフォーマンス観点よりStorage StackとScanner Stackは同じ大陸のリージョンへデプロイすることを推奨します。

デプロイパターン③：Multi-Stack構成

1つのScanner Stackへ複数のStorage Stackを紐づけて利用する構成です。
AWS CloudFormation Templateを活用してそれぞれ簡単にデプロイすることができます。

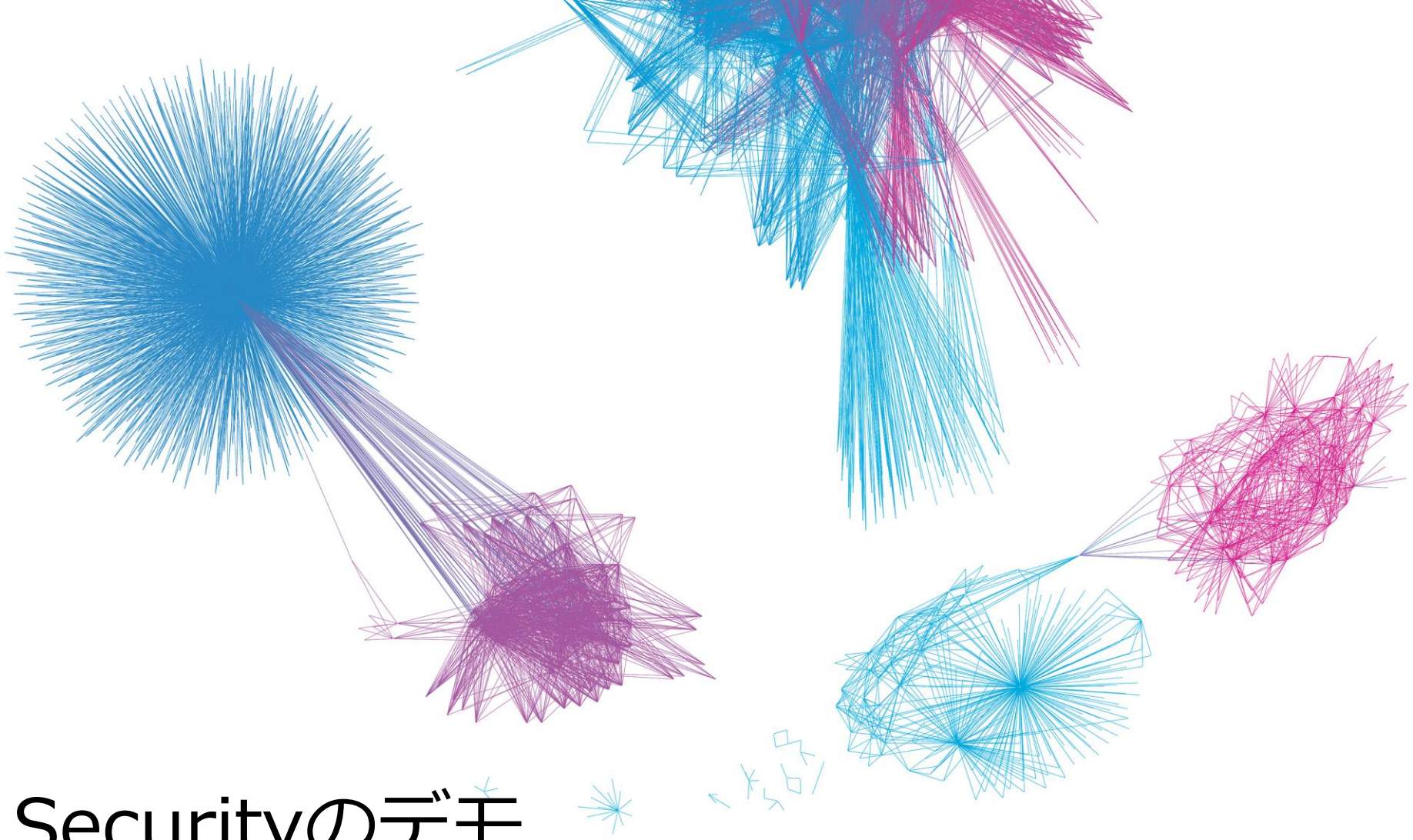


※スキャン対象のBucketごとにStorage Stackが必要です。

【ポイント】

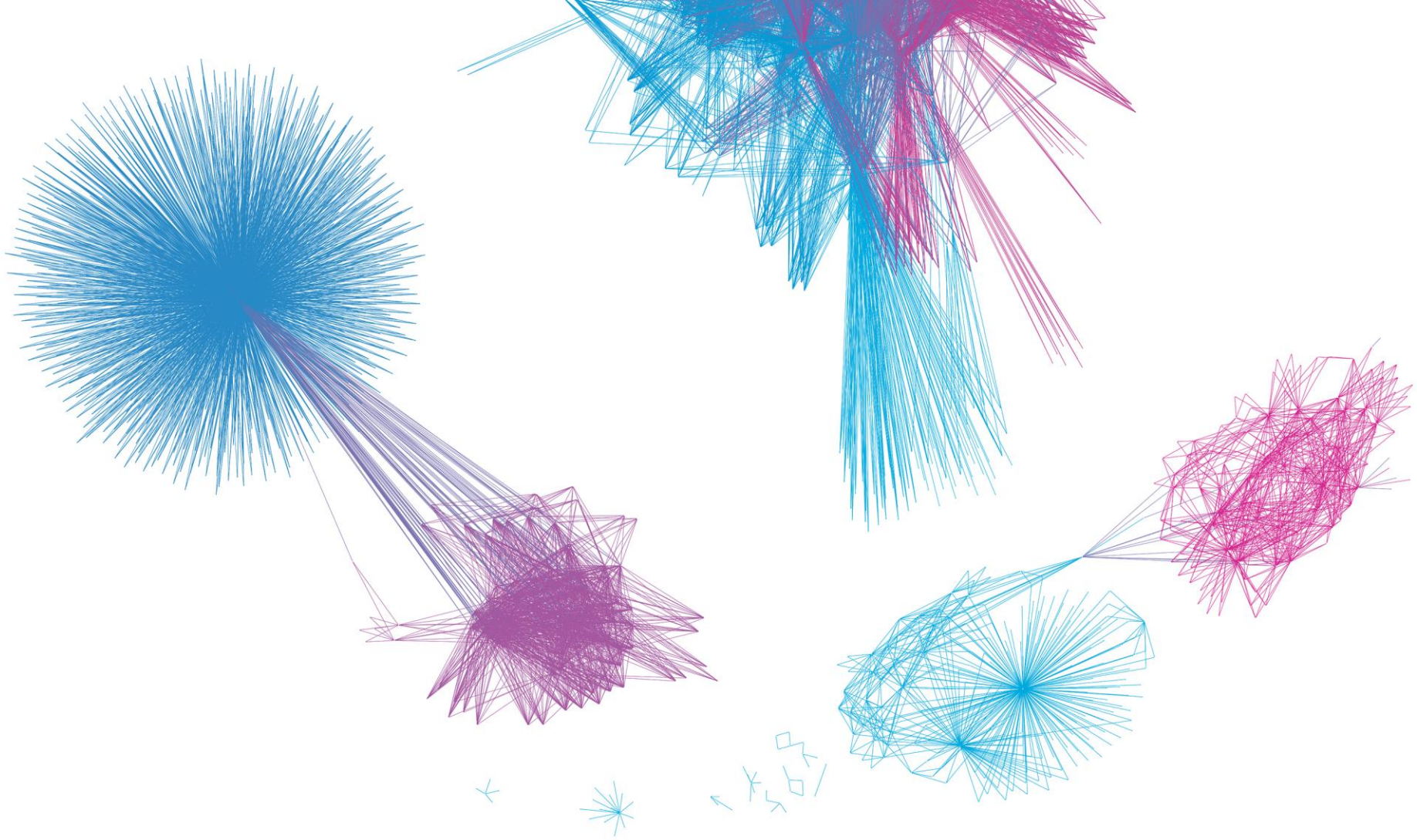
- **Scanner Stackのリソースを重複せずに集約**
- **Storage Stackの拡張が容易**
- Application TeamとSecurity Teamで管理を分離
- 外部接続するAWSアカウントを集約
- AWS Lambdaの同時実行上限を分散させる必要がある場合

※1つのScanner Stackに紐づけられるStorage Stackは50個までです。



File Storage Securityのデモ

デモシナリオ



まとめ

本日のまとめ

1. AWSにおけるセキュリティの考え方
   - AWSの責任共有モデルを理解し、ユーザ責任範囲を正しく認識する

2. クラウドセキュリティの最新動向
   - ここだけは押さえておきたいポイントは「脆弱性対策」「設定ミスの対策」

3. 設定ミスの対策と悪意あるオブジェクトの排除はどうすればいい？
   - Cloud One Conformity
   - Cloud One File Storage Security

TREND MICRO

THE ART OF CYBERSECURITY

An Innovative Approach to Cybersecurity

Automated hybrid cloud workload protection in Japan via API calls to Trend Micro's cloud security platform. **Created with real data by Trend Micro threat researcher and artist Jindrich Karasek**.