Amazon EC2を使った公開サーバにおけるセキュリティベストプラクティス
～個人情報の漏洩と脆弱性～

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

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
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。

AWS Summit Tokyo 2019

JAWS DAYS 2020

トレンドマイクロ Webinar 2020

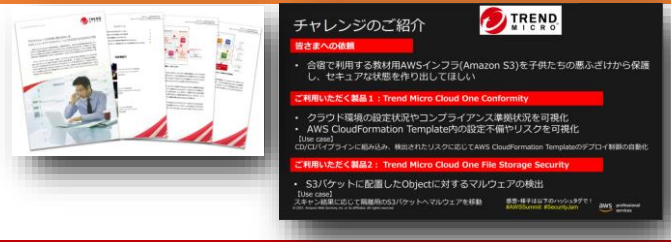
トレンドマイクロ
& New Relic共催セミナー

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

TREND MICRO | cybersecurity institute

本日お伝えしたい事

- 公開サーバへの攻撃傾向とその被害について
- Amazon EC2 における、最低限実施すべき
  セキュリティのベストプラクティスを理解頂く
- 各攻撃フェーズで必要な設計指針と
  AWSとトレンドマイクロで提供出来る対策

公開サーバへの攻撃傾向とその被害

サービス提供者様のセキュリティ悩み事

セキュリティインシデントの発生

Webサイトの停止・ブランド毀損・情報漏洩

→ 数億円から数百億円の損害

→ 情報資産を守りたい

セキュリティ対策

→ どんな「脅威」があるの？

→ どんな「対策」をすればいいの？

→ 今回はこちら**「公開サーバの対策」**

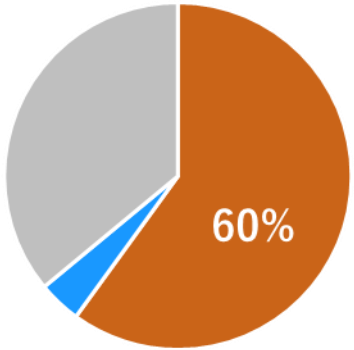
不正侵入のきっかけは？

発表日	会社名	対象サイト	原因	被害
2020/07	A社	オンラインショップ	脆弱性からの不正侵入	・顧客クレジットカード情報：数十件 ・顧客個人情報：数千件
2020/07	B社	オンラインショップ		・顧客クレジットカード情報：数百件
2020/07	C社	オンラインショップ		・顧客クレジットカード情報：数百件
2020/07	D社	オンラインショップ		・顧客クレジットカード情報：数百件
2020/06	E社	オンラインショップ		・顧客クレジットカード情報：数百件
2020/04	F社	オンラインショップ		・顧客クレジットカード情報：数百件
2020/03	G社	オンラインショップ		・顧客クレジットカード情報：数百件
2020/03	H社	オンラインショップ		・顧客クレジットカード情報：数百件
2020/02	I社	オンラインショップ		・顧客クレジットカード情報：数百件
2020/01	J社	オンラインショップ		・顧客個人情報：数百件

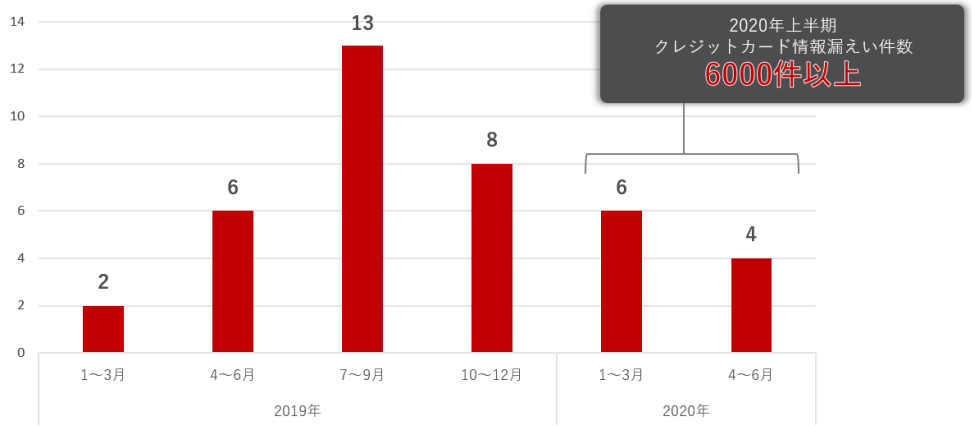
引用：https://cybersecurity-jp.com/

公開サーバへの攻撃：ECサイトへの攻撃が継続

- 公開サーバへの攻撃原因は例年に引き続き「脆弱性」を悪用した攻撃が大半を占める
- 昨年に引き続き、ECサイトを改ざんしてクレジットカード情報を窃取する「Eスキミング」の被害が継続して発生
- Eスキミングの公表事例のほとんどが外部からの指摘で発覚しており、既にカード情報が不正利用されている



■図：公表された公開サーバへの攻撃の被害原因内訳
（2020年上半期 n=25）



■図：国内で公表されたECサイト改ざんによるカード情報漏えい被害
事例件数の推移（2019年～2020年上半期）

※公表事例を元にトレンドマイクロが独自に整理

悪用される脆弱性とその「年齢」の関連性

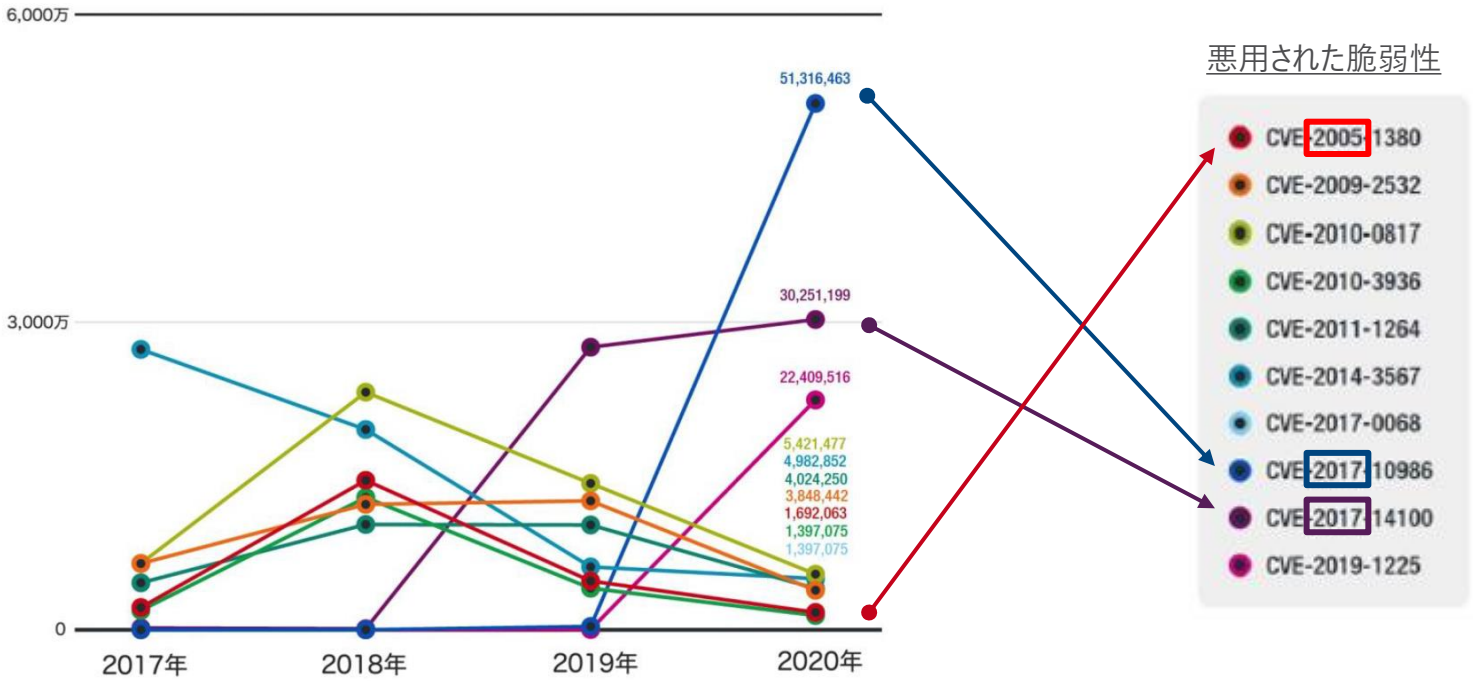


図 28：検出された脆弱性トップ 10 と検出数の年間推移

ここまでのまとめ

- 脆弱性を起因とした不正侵入が発生していて
  特にECサイトへの攻撃が継続している。

- 更に、脆弱性は最新ものだけでなく、既知のものが
  使われる事が多く、その対策が必要。

Trend Micro Cloud One™のご紹介

アンケートのお願い

AWS セキュリティのカギ ”責任共有モデル”

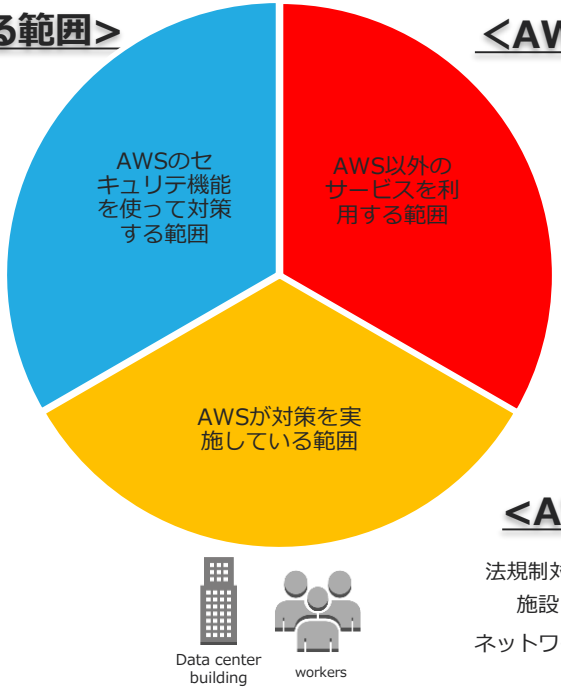
お客様は
クラウド**上**の
セキュリティに責任を持つ

AWSは
クラウド**自体**の
セキュリティに責任を持つ

クラウド“上”のセキュリティはどのように守るのか？

<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>

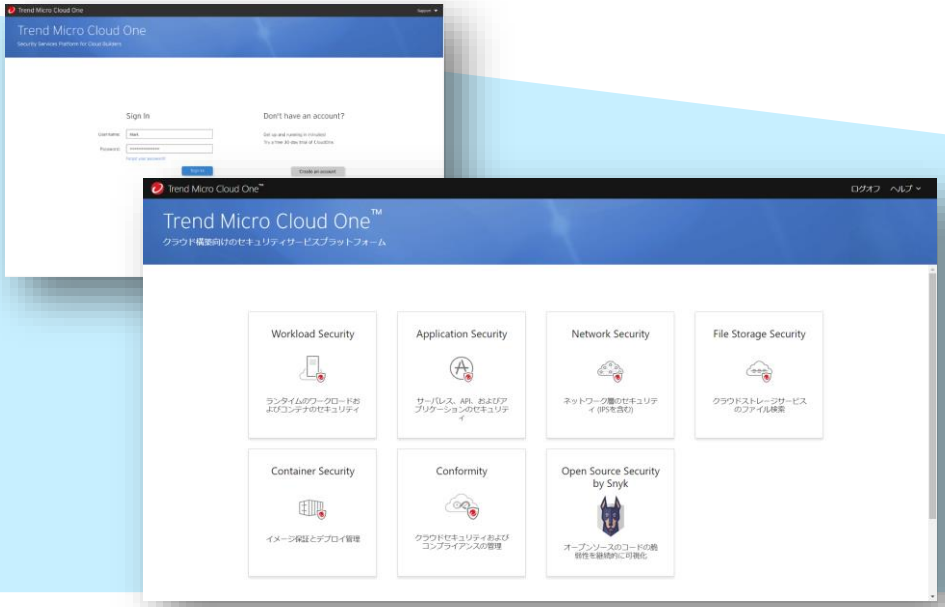
法規制対応　ログ管理　ストレージ
施設　物理冗長性　サーバー
ネットワーク　ハイパーバイザー

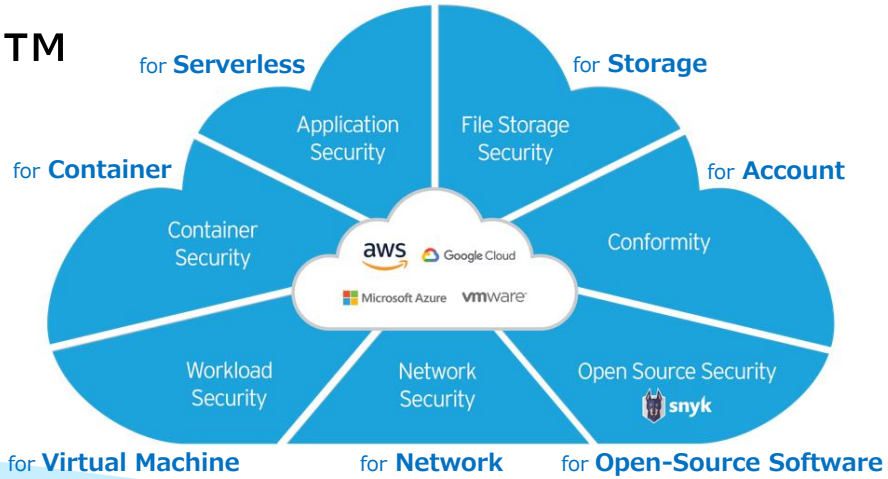
TREND MICRO

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――

Cloud One AWS対応製品群

Trend Micro
Cloud One™

Trend Micro Cloud One
- Workload Security
クラウドワークロードおよびコンテナの保護

Amazon EC2 | Amazon Elastic Container Service | Amazon Elastic Kubernetes Service | AWS Elastic Beanstalk

- Network Security
クラウド向けネットワークIPS

Amazon VPC

- Container Security
ビルドパイプラインでのコンテナイメージスキャン

Amazon Elastic Container Registry

- Application Security
サーバレスおよびアプリケーションの保護

AWS Fargate | Amazon Elastic Container Service | Amazon Elastic Kubernetes Service | AWS Lambda

Deep Security SE実践強化塾
https://www.youtube.com/playlist?list=PL5OUFC_NrEsbHqRoTJ7OZGkoFQq9vPWIm

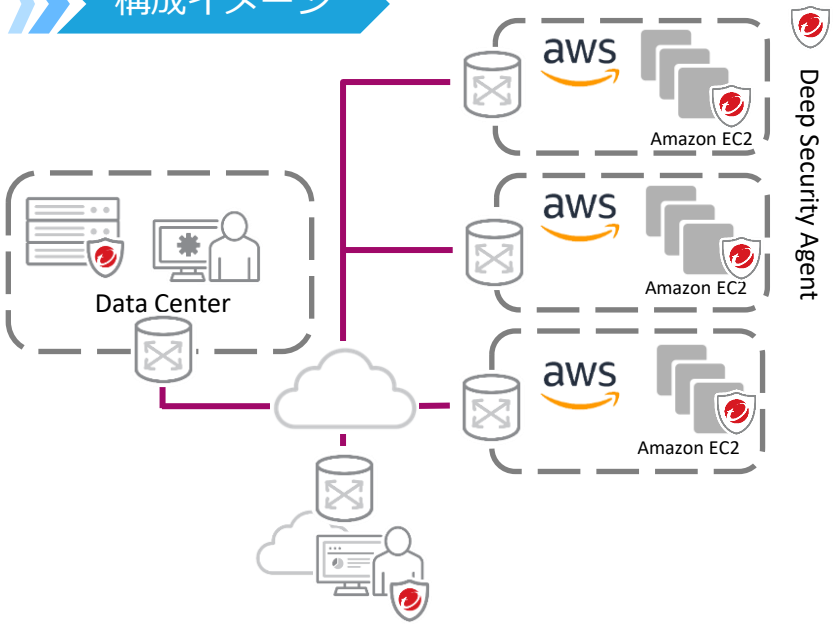
- Conformity
クラウドの設定不備を可視化、コンプライアンス対応支援

AWS Cloud

Cloud One - Workload Security (旧名称：Deep Security as a Service)

クラウド上のサーバにインストールすることで、脆弱性対策や多層防御を提供。トレンドマイクロが管理サーバをクラウド上で提供するため、導入にあたり管理サーバを構築する必要がありません。

構成イメージ



提供機能

- Agentをインストールしたサーバに対して下記の機能を提供。サーバの多層防御･脆弱性対策を実現。
  - 不正プログラム対策
  - IPS/IDS（侵入防御）
  - Webレピュテーション
  - ファイアウォール
  - アプリケーションコントロール
  - 変更監視
  - セキュリティログ監視

特徴

- 管理サーバの構築・運用が不要
- サーバ保護に必要な複数の機能を単一Agentに搭載

Cloud One - Workload Security ユースケース

侵入防御機能（仮想パッチ）

仮想パッチとは

脆弱性を修正するセキュリティパッチをインストールする代わりに、脆弱性を突く攻撃をブロックし、仮想的にパッチの役目を提供します。

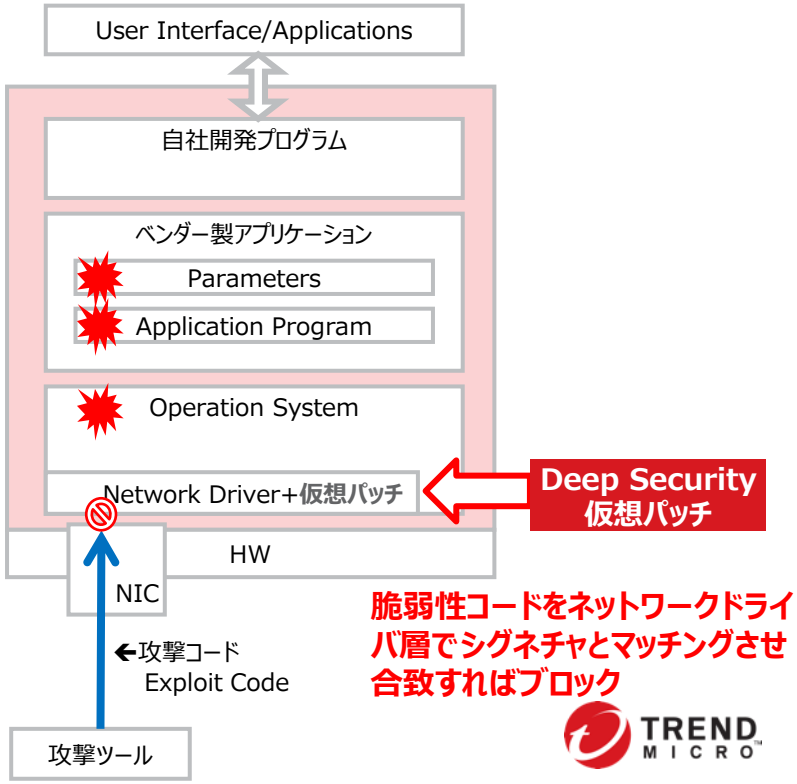
脆弱性を突いた攻撃をブロックする機能

OSやアプリケーションの脆弱性を突いた攻撃をネットワークレベルでブロック

ポイント１：
ソフトウェアのコードレベルでの修正を行わないので、動作中のシステムへ影響が少ない

ポイント２：
WindowsやLinuxのようなOSだけでなく、様々なアプリケーションの仮想パッチがトレンドマイクロから提供される

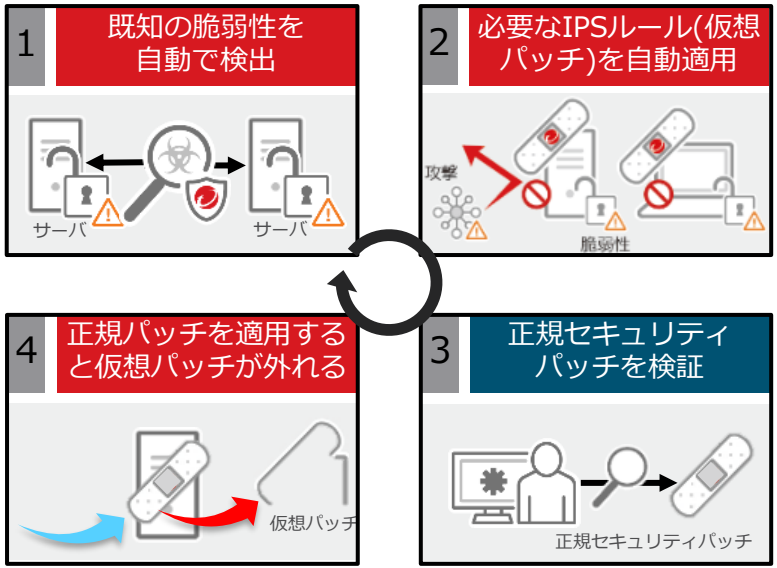
※トレンドマイクロから提供される侵入防御ルールの他にも、独自のルールを作成することも可能です。



Cloud One - Workload Security ユースケース

システム運用者の運用負荷を軽減 ～推奨設定～

「推奨設定」とはDeep Security Agentが自動でサーバ内のシステム情報をスキャンし、
サーバ上にある脆弱性を見つけて、そこに対する必要なIPS/IDSルール”仮想パッチ”を自動で適用する機能です。結果的にサーバは、必要な保護だけを適切に自動で受けることが可能となります。



解決可能なペインポイント

- サーバ管理者の脆弱性管理や、脆弱性を狙った攻撃への対処負荷を低減。
- 管理者自身でIPSルールの適用を行う必要がない。

なぜ仮想パッチをリリースできるのか

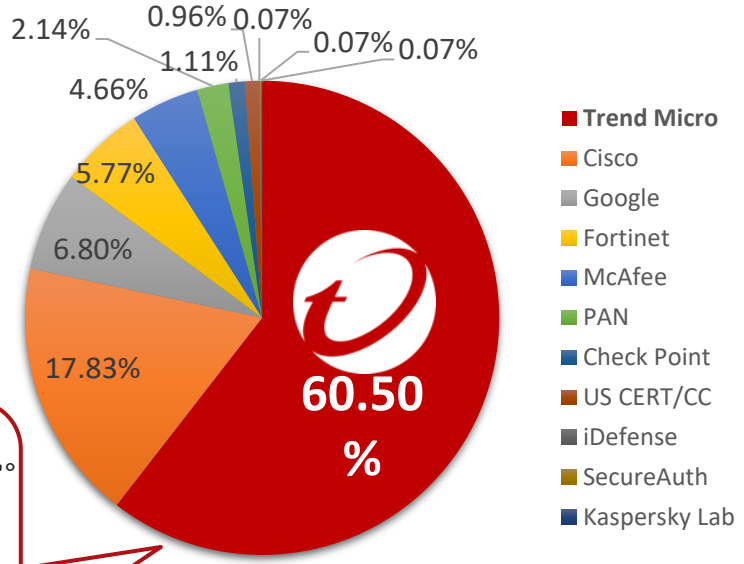
トレンドマイクロが運営する**ZERO DAY INITIATIVE(ZDI)**から脆弱性情報を取得しているため

ZERO DAY INITIATIVE

ZERO DAY INITIATIVE(ZDI)は、**10,000名以上**のセキュリティ研究者と連携したコミュニティです。

2020年に全体の**60.5%**となる半数以上の脆弱性を発見した実績があります。

脆弱性を調査しているベンダから2020年に報告されたゼロデイ脆弱性のベンダ別割合



Microsoft

マイクロソフトの公開脆弱性の約**1/4**がZDIが発見。
社外として一番バグ情報を提供しています。

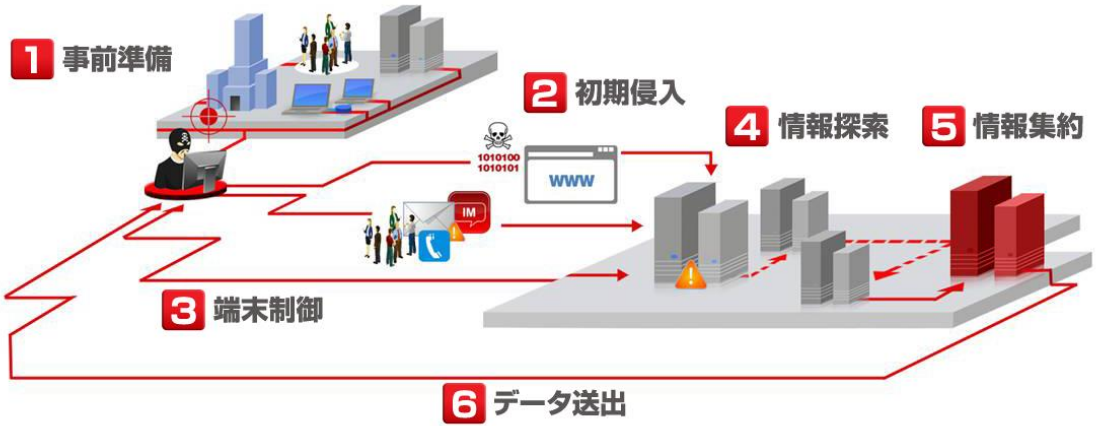
Adobe

Adobeの公開脆弱性の約**1/3**はZDIが発見。
社外として一番バグ情報を提供しています。

Public

各攻撃フェーズで必要な設計指針と AWSとトレンドマイクロで提供出来る対策

攻撃の各フェーズについて



攻撃フェーズ	攻撃内容
①事前準備	攻撃標的の決定、標的とその周辺への偵察による情報入手、初期潜入用不正プログラムやC&Cサーバの準備
②初期潜入	標的型メールの送信、受信者による添付不正プログラム実行 、公開サーバへの脆弱性攻撃による侵入
③端末制御	感染環境と所属するネットワーク情報の確認、バックドア型不正プログラムによる標的内端末への感染
④情報探索	内部活動ツールのダウンロード、ネットワーク内の情報探索
⑤情報集約	重要情報の収集
⑥情報送出	収集した重要情報の外部入手

各攻撃フェーズに対する対策例

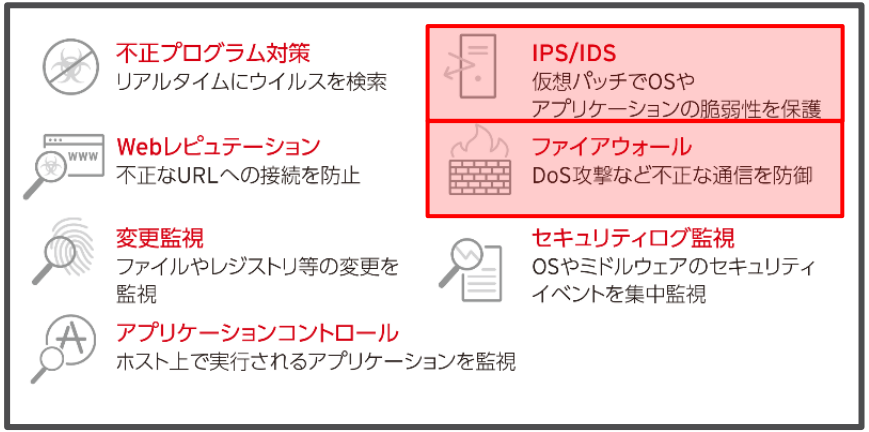
※各機能とも、攻撃から100%保護できるものではございません

入口対策の設計指針

【基本指針】

- **脅威の侵入を防御**する
  - 必要最低限のサービス提供する
  - 予兆検知・不正通信を遮断できる仕組みを活用する

Workload Securityでの対応



【設計指針】

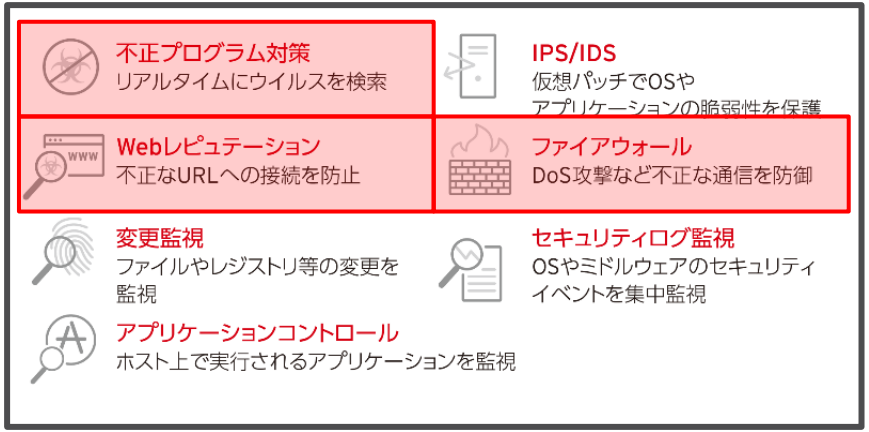
- ファイアウォール
  - ✓ ネットワーク型 もしくは ホスト型 のいずれかを必ず活用する
  - ✓ ネットワーク型で共通的対策が取れない場合、ホスト型を採用する
    機能重複があれば、必ずしも両方使用する必要は無い
- IPS/IDS
  - ✓ ネットワーク型 もしくは ホスト型 のいずれかを必ず活用する
  - ✓ 業務影響への低さを考慮し、ホスト型を優先的に利用する
    もし併用可能であれば併用する

出口対策の設計指針

【基本指針】

- サーバもしくはネットワークに侵入した**脅威が外部と通信することを防ぐ**
  - 不正プログラムを早期発見・隔離する
  - 外部への通信を早期発見・隔離する

Workload Securityでの対応



【設計指針】

- 不正プログラム対策
  - ✓ 不正プログラム（主にハッキングツールやバックドア）の検出を目的とし、積極的に隔離する
- Webレピュテーション
  - ✓ 通常、サーバが不特定多数のページへのアクセスは考えにくいため、基本的には高いセキュリティレベルで積極的に遮断する
- ファイアウォール
  - ✓ 必要の無い外部通信は全て遮断する

内部対策の設計指針

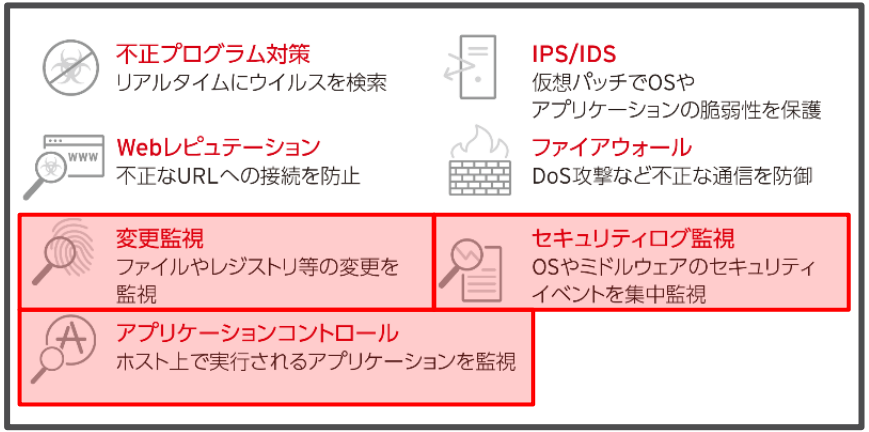
【基本指針】

- 予め想定ができなかった**未知の脅威の侵入**を前提とした対策を施す

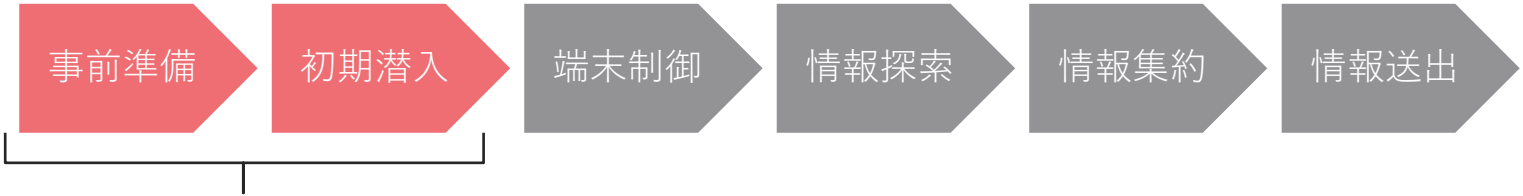
【設計指針】

- アプリケーションコントロール
  - ✓ サーバもしくはネットワークに侵入した未知の脅威の活動を阻止する
  - ✓ 実績の無い疑わしいプログラムの実行阻止
- 変更監視、セキュリティログ監視
  - ✓ プログラムやデータの改ざんなど阻止できなかった未知の脅威の活動を記録・早期検知することで被害の最小化を図る
  - ✓ ファイルやプロセスなど意図しない変更を検出・通知
  - ✓ 各種ログによる痕跡から怪しい動作の検出・通知

Workload Securityでの対応



各フェーズにおけるAWS環境での対策



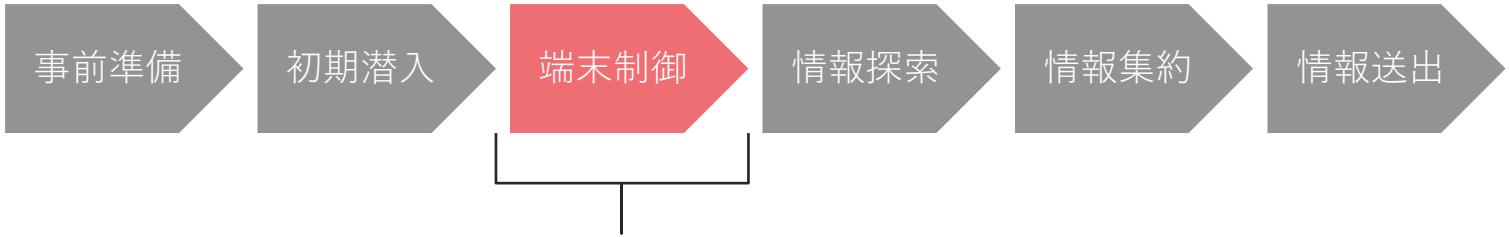
1. 事前準備フェーズ

- ✓ 偵察（例：ポートスキャン）、脆弱性探索に備えて、**Amazon GuardDuty(脅威の検出)**
  Amazon Inspector(セキュリティの分析や評価)などを導入する。
  Amazon Inspectorで脆弱性を可視化し、**AWS Systems Manager(運用データの可視化と自動化)**を
  利用して正規のパッチを適用できる運用を考慮する。
- ✓ 正規パッチの適用が難しい場合は、Workload Securityの**推奨設定の検索と仮想パッチ**の導入を検討する
- ✓ システムが社内ポリシーやガイドラインに準拠しているか、**AWS Config(継続的モニタリング)**を用いて評価を行う。
- ✓ **Amazon SNS(メッセージングサービス)**等を利用しそれらがアラートとして通知されるような仕組みも取り入れる

2．初期潜入フェーズ

- ✓ 脆弱性を利用した攻撃に備えて、Workload Securityの**推奨設定の検索と仮想パッチ**を利用して
  脆弱性への攻撃を未然に防ぐ運用を取り入れる。

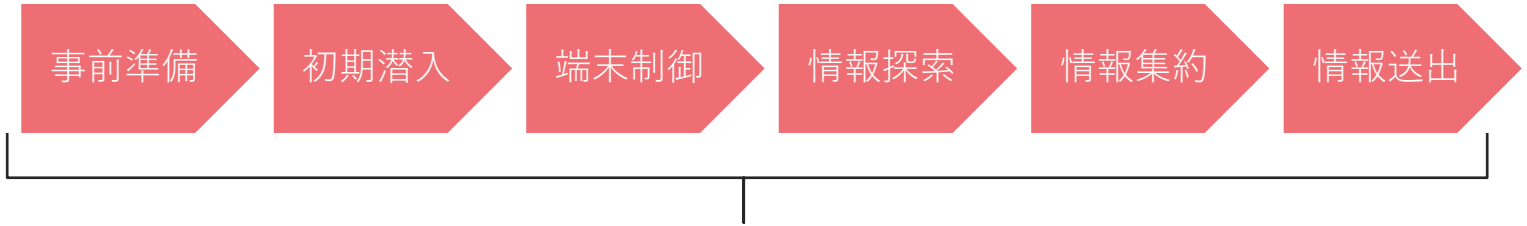
各フェーズにおけるAWS環境での対策



3．端末制御フェーズ

- ✓ 攻撃者によるシステムへの変更（例：hosts書き換え）を検出するために、Workload Securityの**変更監視**を導入し、気付ける仕組みを取り入れる。
- ✓ Workload Securityの**不正プログラム対策**のパターンを常に最新状態に保ち、リアルタイム検索やスケジュール検索を有効にし、既知のマルウェアに対応出来るようにしておく。
- ✓ Workload Securityの**アプリケーションコントロール**を有効化し、未知のマルウェアにも対応出来る用にしておく。
- ✓ 感染サーバとC&Cの通信を防御（又は検出）するために、Workload Securityの**Webレピュテーション**や**Amazon GuardDuty**を有効化しておく。

各フェーズにおけるAWS環境での対策



全体の運用効率化

1．ログの集中管理を検討する

✓　大量のログを管理するために、SIEMなどの導入を検討する。
Amazon GuardDuty、Amazon Inspector、Workload Security等から
出力される大量のログを**集中管理する仕組みを取り入れる**。
その次に、それらログから多角的に脅威を観測し、脅威の兆候を可視化する事で、様々な攻撃に備えます。

2．初動を迅速化する対策を検討する

✓　**Workload Securityのオートメーション(OSSで提供)**導入を検討する。
・感染サーバの特定⇒N.Wからの隔離⇒保全
・Workload Securityで検出した攻撃元IPアドレスをAWS WAFでブロック
等を自動で行う事が可能となり、インシデント発生時の初動対応を迅速かつ安全、確実に行う事が可能となる。

AWSサービスの詳細

- Amazon GuardDuty
  https://aws.amazon.com/jp/guardduty/
- Amazon Inspector
  https://aws.amazon.com/jp/inspector/
- AWS Systems Manager
  https://aws.amazon.com/jp/systems-manager/
- AWS Config
  https://aws.amazon.com/jp/config/
- Amazon SNS
  https://aws.amazon.com/jp/sns/

まとめ

- 公開サーバへの攻撃傾向とその被害
  - ✓ ECサイトへの攻撃が継続している
  - ✓ 脆弱性起因の不正侵入が多い
  - ✓ 攻撃に既知の脆弱性が利用されている
- AWSとトレンドマイクロで出来る公開サーバへの対策
  - ✓ 入口、出口、内部等、各攻撃フェーズを考慮した対策が重要

今までの AWSとトレンドマイクロの共催Webinar
https://www.trendmicro.com/ja_jp/business/campaigns/aws/cloud-one-on-aws.html


TREND MICRO
THE ART OF CYBERSECURITY
An Innovative Approach to Cybersecurity
トレンドマイクロのクラウドセキュリティプラットフォームによる、日本におけるハイブリッドクラウドワークロードの自動保護。**実際のデータを使用し、トレンドマイクロの脅威リサーチャーでアーティストでもあるJindrich Karasekによって作成されました。**

Q and A
セッション