

生成AI でWeb脆弱性診断の抜け漏れゼロへ！

セキュリティを進化させる

ASMのスゴい精度とは

## 登壇者紹介



株式会社エーアイセキュリティラボ

執行役員兼CX本部長 **関根 鉄平** CISSP

セキュリティエンジニアとして大手金融機関等の脆弱性診断に従事。その後、Webアプリケーション検査ツール・サポートチームの立ち上げをしつつ、CSIRTや開発現場でのセキュリティを推進。

2020年6月より現職。AeyeScanのカスタマーサクセスチームの責任者として脆弱性診断の内製化を支援。大規模イベントや大手企業での講演に多数登壇している。

『セキュリティエンジニアの知識地図』を共著。



発売中

### コミュニティ 活動など

- 情報セキュリティ10大脅威 選考会メンバー
- OWASP/ISOGJ アジャイル開発におけるセキュリティ | パターン・ランゲージ
- OWASP/ISOGJ Webシステム/Webアプリケーションセキュリティ要件書

# ASM(Attack Surface Management)とは？

外部からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスのこと

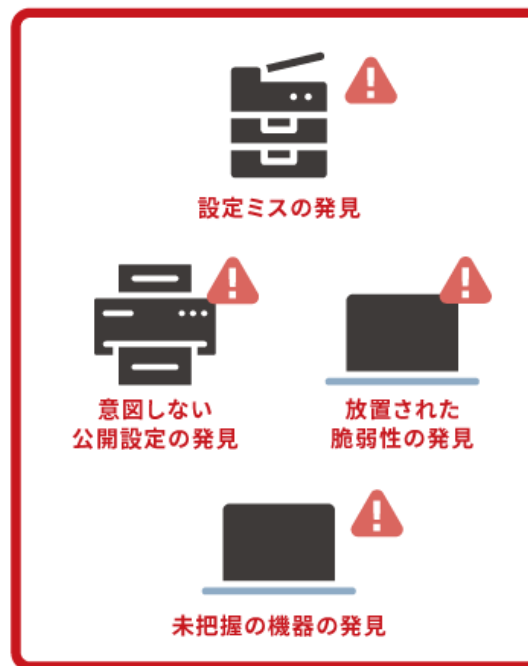
攻撃面の発見

攻撃面の情報収集

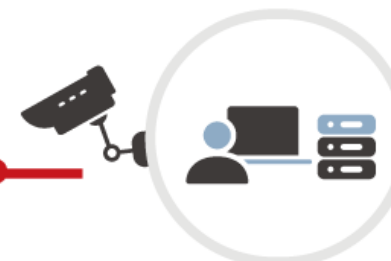
攻撃面のリスク評価



IT資産すべての状況を  
人手で管理し続けるのは  
現実的ではない…



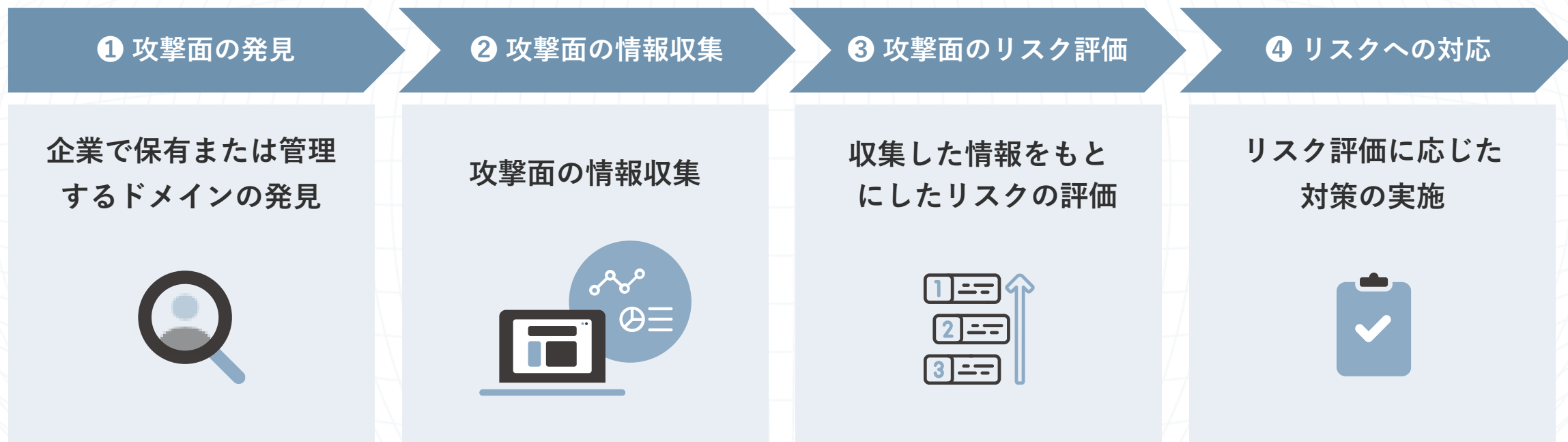
ASMツール



発見

組織の外から、組織に関する  
機器の情報を収集し  
データベース化

# ASMのプロセスの例



# ASMによる攻撃面の発見方法や評価プロセスはさまざま

ASMには具体的な定義がなく、攻撃面の発見方法も複数のアプローチがあるため、自組織に適したツールやサービスを採用する必要がある。

| 運用形態                                          | 特徴                                          |
|-----------------------------------------------|---------------------------------------------|
| EASM (External Attack Surface Management)     | インターネットからアクセス可能なIT資産の探索（未知の資産の発見も含む）、脆弱性の調査 |
| CAASM (Cyber Asset Attack Surface Management) | IT資産の脆弱性や設定管理                               |
| DRPS (Digital Risk Protection Service)        | 外部からの脅威を検知・分析し、デジタルリスクを管理                   |
| TPRM (Third Party Risk Management)            | ビジネス関係にある組織から生じるリスクの特定・評価、対応・管理             |
| セキュリティリスクレーティング,<br>セキュリティスコアリング              | 組織のセキュリティ態勢を客観的にスコアリングし、リスクの高い領域の特定         |



?

では、どうやって  
ASMツールを選べば  
よいのでしょうか？

# まず、自組織の課題を把握する

## 既知のIT資産管理

- ✓ 企業や組織構造により、一元管理が難しい
- ✓ サービスやIT資産数が多く、台帳管理が難しい
- ✓ 台帳の鮮度を保つことが難しい

## 未知のIT資産管理

- ✓ 各部門で取得しているドメインがあり、管理できていない
- ✓ 頻繁にテストサイトが構築されており、管理できていない

## 平時の脆弱性管理・対応

- ✓ サービスやIT資産数が多く、全てに脆弱性診断ができない
- ✓ 現場に任せていて、客観的にチェックできていない

# 解決したい課題や目的から、ASMに求める要件を明確にする

ASMに求める要件の例

| 大項目         | 内容                                                                                             |
|-------------|------------------------------------------------------------------------------------------------|
| 攻撃面の発見      | <ul style="list-style-type: none"><li>組織名からドメインを発見すること</li><li>FQDNと紐付くIPアドレスを発見すること</li></ul> |
| 攻撃面の付加情報の収集 | <ul style="list-style-type: none"><li>アクセス可能なポートや利用製品から用途を推測できること</li></ul>                    |
| 攻撃面のリスク評価   | <ul style="list-style-type: none"><li>リスクが提示されていること</li></ul>                                  |
| 運用面         | <ul style="list-style-type: none"><li>検出結果への対応ステータスを設定できること</li></ul>                          |

ASMはツールやサービス導入がゴールではなく、運用してこそ価値を発揮する。  
運用がイメージできるか、対策につながる情報が得られるかなど、運用面の考慮がポイント。



**早速、ASMに取り組みたい！  
その前に、ASMで気を付ける  
ポイントを押さえておきましょう。**

## ｜ASMのよくある課題

ASMはリスク低減効果が期待される一方で、収集・分析する情報の不確実性などの実施にあたっての留意点が存在する（経産省「ASM導入ガイダンス」より引用）

### 例：不正確な情報の検知



自社で管理していない  
サイトが発見される



偽陽性または偽陰性の  
情報が報告される

## ASMの検出アルゴリズムが関係している

# ASMの検出アルゴリズムの例

保有している可能性がありそうなドメインを  
列挙してくる



aeyescan.jpを発見！



aeyescan.net  
aeyescan.org  
⋮

保有している可能性がある  
ネットワーク帯の  
IPアドレスを列挙してくる



192.0.3.1を発見！



192.0.3.2  
192.0.3.3  
192.0.3.4  
⋮

よく使われる  
サブドメインを  
総当たりで列挙してくる

aeyescan.jp  
api.aeyescan.jp  
c.aeyescan.jp  
mail.aeyescan.jp  
stg.aeyescan.jp  
⋮

# Demonstration

デモ

# 高度な生成AI活用により、効率的かつ信頼性の高い探索が可能

オプション機能

特許取得実績のある「**生成AI活用の技術**」を使って、未把握の攻撃面を**効率的・網羅的**に発見。



生成AI

検索結果に上がってきた組織名（文字列）を解読。  
SSL証明書の情報やIR情報など、複数の情報源をつなぎ合わせて総合的に判定。

従来のASMが抱える以下のような課題も、**生成AI活用**で解決可能。

## 1 発見した攻撃面は本当に自社のものなのか？



名称が類似している  
企業の情報が混じる



自社と関係がないと思われる  
組織の情報が混じる

## 2 リスク評価はどこまで信用できるのか？



大量の脆弱性を検知して  
報告する



該当しない脆弱性の検知や  
リスク評価が実際より高い場合も

# AIがWebサイトの属性を自動判定し、重要度をランク付け

2025.6  
リリース

## ① Webサイトの属性を判定し…

### サイト用途

Medium

- ECサイト
- VPN管理サイト

Low

- 外部SaaSサイト
- テストサイト

### 保持データ

High

- 個人情報
- クレジットカード情報

### 利用技術

Low

- WordPress
- EC-CUBE
- 旧式技術  
(JSP/PHP/CGIなど)

## ② 重要度をランク付け（判定理由も提示！）

セキュリティ対策の優先順位付けを効率的に行えるようになり、  
効率的なリソース配分・コンプライアンス強化・包括的なWeb資産管理を実現

# | AeyeScanひとつで、デジタル領域のセキュリティをトータルサポート

公開Webサイトの検出

Webサイト全体の把握

脆弱性診断によるリスク評価

把握済みの  
Webサイト



⋮

自動巡回・診断

未把握の  
Webサイト



発見

登録

自動巡回・診断

 **AeyeScan**



Web-ASM



自動巡回



脆弱性診断

 **AeyeScan** (エーアイスキャン) により  
セキュリティ対策にかかる **コストを削減!**



クラウド型Webアプリケーション  
脆弱性検査ツール

国内市場シェア  
**No.1**※



※ 富士キメラ総研調べ「2024 ネットワークセキュリティビジネス調査総覧 市場編」Webアプリケーション脆弱性検査ツール〈クラウド〉2023年度実績  
※ ITR調べ「ITR Market View : サイバー・セキュリティ対策市場2024」SaaS型Webアプリケーション脆弱性管理市場：ベンダー別売上金額シェア（2022年度実績）

プロが認める品質・精度

セキュリティベンダーやSIerでも  
顧客向けサービスとして活用



ブラウザ上での直感的な操作

専任エンジニア不要、情シスや開発部門でも  
安定した運用が可能

# さまざまな企業さまに導入いただいております

## ユーザー企業

### 製造



### インフラ



### 金融



### メディア



### 人材・教育



### エンタメ



## Leverages

### SaaS



## SI・IT企業



## セキュリティ企業



# AeyeScanの導入を検討してみませんか？

操作性の確認、実際に利用してみたい方へ

## AeyeScan の 無料トライアル

トライアルにかかる費用は不要。実際の操作性はどうか？  
またどのように脆弱性が発見されるのか？  
などの疑問は無料トライアルで解消しましょう。

無料トライアルの申し込み



お見積りの希望・導入をご検討している方へ

## AeyeScan への お問い合わせ

お見積りの希望・導入をご検討してくださっている方は  
お問い合わせフォームよりご連絡ください。  
当日もしくは遅くとも翌営業日にはご連絡を差し上げます。

お問い合わせフォーム





**AeyeScan**

セキュリティに、確かな答えを。