ASMの課題は 生成AI で解決

セキュリティエンジニアが教える
人手をかけずに脆弱性対策する方法

©AeyeSecurityLab Inc.

AeyeSecurityLab

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。

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

©AeyeSecurityLab Inc.

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

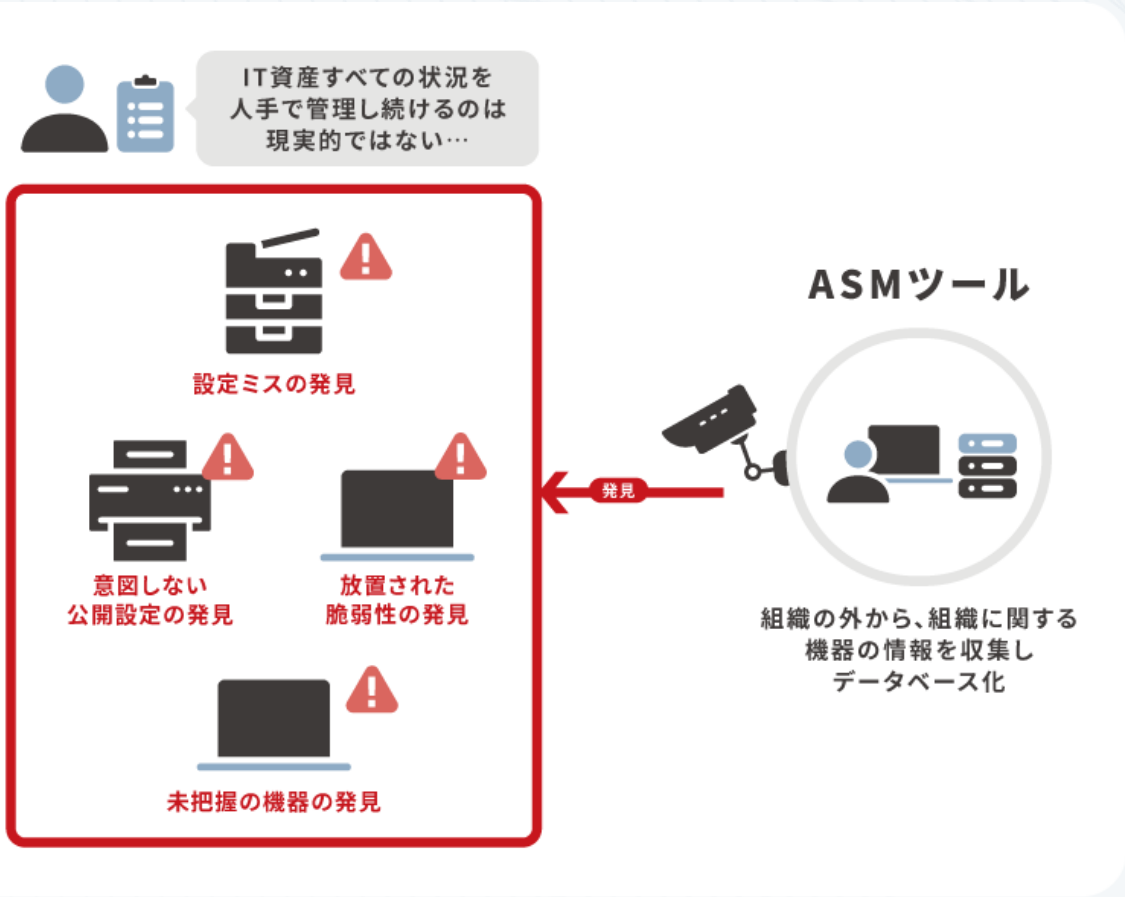
攻撃面の発見

↓

攻撃面の情報収集

↓

攻撃面のリスク評価



参考：経済産業省　「ASM（Attack Surface Management） 導入ガイダンス」https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

©AeyeSecurityLab Inc.

AeyeSecurityLab

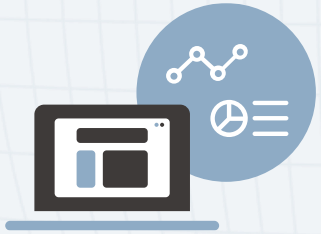
ASMのプロセスの例

❶ 攻撃面の発見

企業で保有または管理するドメインの発見

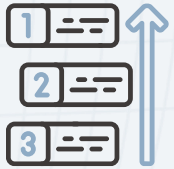
❷ 攻撃面の情報収集

攻撃面の情報収集



❸ 攻撃面のリスク評価

収集した情報をもとにしたリスクの評価



❹ リスクへの対応

リスク評価に応じた対策の実施

参考：経済産業省　「ASM（Attack Surface Management） 導入ガイダンス」https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

©AeyeSecurityLab Inc.

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， 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

参考：ISOG-J「ASM導入検討を進めるためのガイダンス（基礎編）」https://webapppentestguidelines.github.io/ASMGuidance/docs/chapter2/section3/

©AeyeSecurityLab Inc.

では、どうやって
ASMツールを選べば
よいのでしょうか？

©AeyeSecurityLab Inc.

AeyeSecurityLab

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

参考：ISOG-J「ASM導入検討を進めるためのガイダンス（基礎編）」https://webapppentestguidelines.github.io/ASMGuidance/docs/chapter3/section1/

©AeyeSecurityLab Inc.

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	• ドメインからFQDN一覧を発見すること • FQDNと紐付くIPアドレスを発見すること
攻撃面の付加情報の収集	• 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
攻撃面のリスク評価	• リスクが提示されていること
運用面	• 検出結果への対応ステータスを設定できること

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。

参考：ISOG-J「ASM導入検討を進めるためのガイダンス（基礎編）」https://webapppentestguidelines.github.io/ASMGuidance/docs/chapter3/section2/

©AeyeSecurityLab Inc.

早速、ASMに取組みたい！
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。

©AeyeSecurityLab Inc.

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

©AeyeSecurityLab Inc.

ASMの検出アルゴリズムの例

使用の可能性がある サブドメインを 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
⋮

©AeyeSecurityLab Inc.

攻撃面を高精度で発見できる！

生成AIをWeb-ASMと組み合わせて…

会社名だけ
で攻撃面を探索

検索結果に上がってきた
組織名(文字列)を解読

膨大な情報源
から総合的に判定

- SSL証明書の情報
- IR情報(Web公開済み)　など

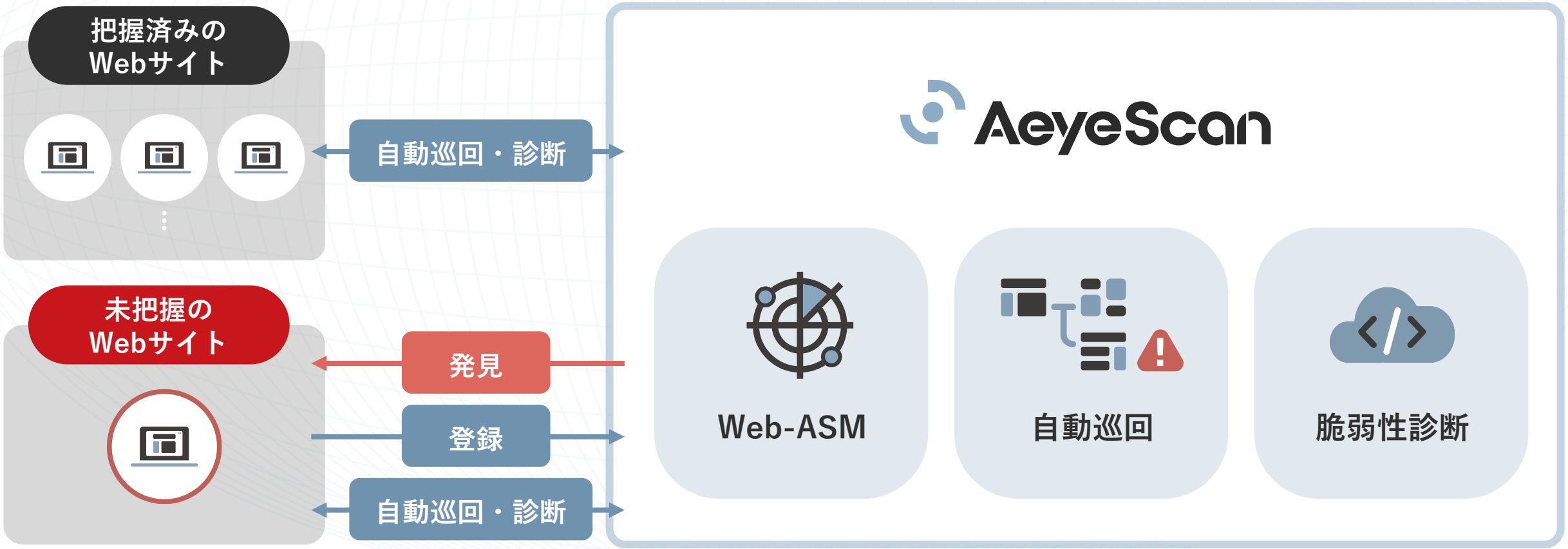
発見経路/理由
が分かる

生成AIが攻撃面を見つけるまでに
辿ったルートを説明

©AeyeSecurityLab Inc.

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



©AeyeSecurityLab Inc.

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※

有償契約
200社以上

※富士キメラ総研調べ「2023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)2022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 × ブラウザ上での直感的な操作

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

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

©AeyeSecurityLab Inc.

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

AISIN
KOSÉ
SAKI
TIGER
Mizuno
ユーグレナ

インフラ

HIS
H2O RETAILING
近鉄情報システム株式会社
J.union
ドリームインキュベータグループ
Suzuyo
NTT東日本
HITOWA GROUP
Looop

金融

アイフル
JOBPAY
SOMPOひまわり生命
DMM FinTech
Tokyo Century

メディア

集英社
中日新聞
NIKKEI

エンタメ

イープラス
CAPCOM
とらラボ!

SaaS

estie
M-aid
エムティーアイ
OZ INTERNATIONAL
COACH A Co., Ltd.
cybozu
JINSOKEN
Schoo
Speee
ZENKIGEN
Direct Sourcing
TAL
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
freee
hokan
Money Forward
RUN.EDGE
RVSTA 株式会社リバスタ
rescuenow

SI・IT企業

Rworks
アクモス 株式会社
AVANT GROUP
CTC
Insight Edge
Infcurion
80&Co.
SB Technology
SBWorks
NTT DATA
NTTビジネスソリューションズ
Globalway
circlace
さくら情報システム
CEC
tdi 情報技術開発株式会社
Simplex Inc.
777WORKS 株式会社スリーセブンワークス
SOFT CREATE
SOLTEC
電通総研
TOPPAN
JOPS
NI+C 日本情報通信株式会社
Human Interactive Technology inc.
FUJISOFT
FUJITSU
三菱電機インフォメーションネットワーク株式会社
YONA
リピスト

セキュリティ企業

NEC NECセキュリティ
NTT DATA NTTデータ先端技術株式会社
cybertrust
LAC

社名五十音順（導入いただいた企業様の一部です）会社名及びロゴは各社の商標または登録商標です

©AeyeSecurityLab Inc.

AeyeSecurityLab

期間限定

Web-ASM機能オプション 利用料金50%OFFキャンペーン

内容	Web-ASM機能オプション利用料金を初回契約分50%OFFでご提供いたします。
適用対象	○ 2025年3月31日(月)までに株式会社エーアイセキュリティラボにご発注いただいたものが対象です。 ○ AeyeScan Businessライセンスをご契約中または2025年3月31日（月）までに新規で利用開始いただいていることが前提となります。
申込方法	「Web-ASM機能」お問い合わせフォームまたは弊社担当までご相談ください。

▶ お問い合わせフォームはこちら　https://www.aeyescan.jp/form/web-asm/

©AeyeSecurityLab Inc.

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なの？
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

©AeyeSecurityLab Inc.

セキュリティに、確かな答えを。

©AeyeSecurityLab Inc.