Web資産管理を“定型業務”へ。

AIを活用したASMの仕組み化と脆弱性対策の効率化ガイド

AeyeSecurityLab

本資料の目的

DXが進み、事業のデジタル化が加速する中で、サービスそのものがデジタルで完結する時代となりました。
開発環境の進化により、誰でもスピーディーにデジタルサービスを立ち上げられるようになった一方、
事業部門主導で生まれた「セキュリティ担当部門が把握しきれないWeb資産」が急増しています。

こうした“見えていない資産”は、攻撃者にとって格好の侵入口となります。
しかし、サーバーやネットワーク機器の管理が「定型化」されているのに対し、
Web資産の管理は今なお多大な工数と専門知識を要する「非定型な業務」であり、
現場の重荷となっているのが実情です。

本資料では、注目の集まるASM（Attack Surface Management）の中でも、
特に管理が難しいとされる「Web領域のASM（Web-ASM）」に焦点を当てます。
属人的な評価プロセスをAIによって「定型化」し、現実的な運用へと落とし込むためのポイントを詳しく解説します。

貴社のWeb資産管理を「特別な苦労」から「当たり前の仕組み」へと変える一助となれば幸いです。

DXの進展が、セキュリティの前提を変えた

Phase 1

情報のデジタル化

＜主なリスク＞

- 人的リスク(漏洩・持出)
- ストレージの安全性
- 不適切な認証・権限設定

データそのものの
セキュリティリスクが中心

Phase 2

業務のデジタル化

＜主なリスク＞

- クラウド環境の設定不備
- ネットワークへの攻撃
- 不完全なエンドポイント管理

業務プロセス自体がデジタル化し
インフラ周りのセキュリティが重要に

Phase 3

事業のデジタル化

＜主なリスク＞

- 頻繁なサービスアップデート
- 把握しきれないWeb資産の増加
- サプライチェーンの拡大

サービスそのものがデジタルで
完結するようになると、
リスクはさらに多層化・継続化

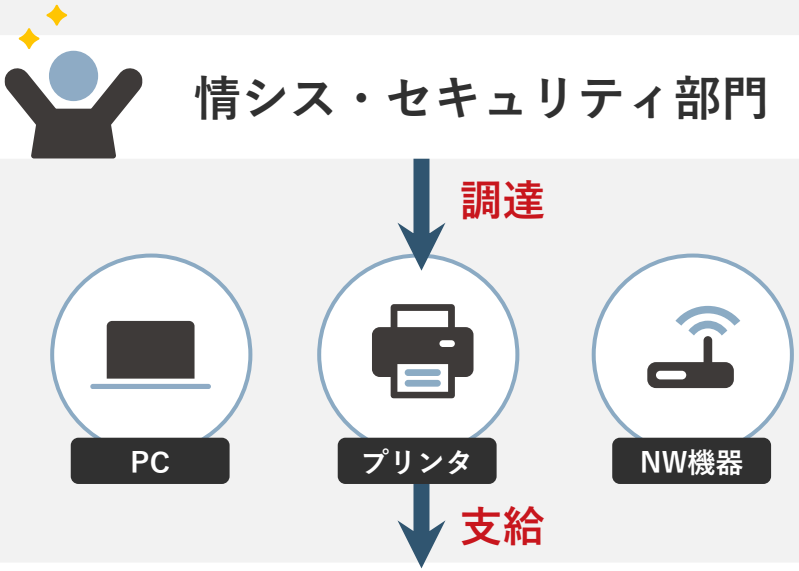
事業のデジタル化（Phase3）は進んでも、対策が追いついていない

もはや「すべての資産を把握すること」は構造的に難しい

DXにより、資産の管理主体が「情シス」から「事業部門」へシフト。情シスが資産をコントロールし、
台帳で網羅的に管理する従来の方法では、把握が不可能なフェーズに突入しています。

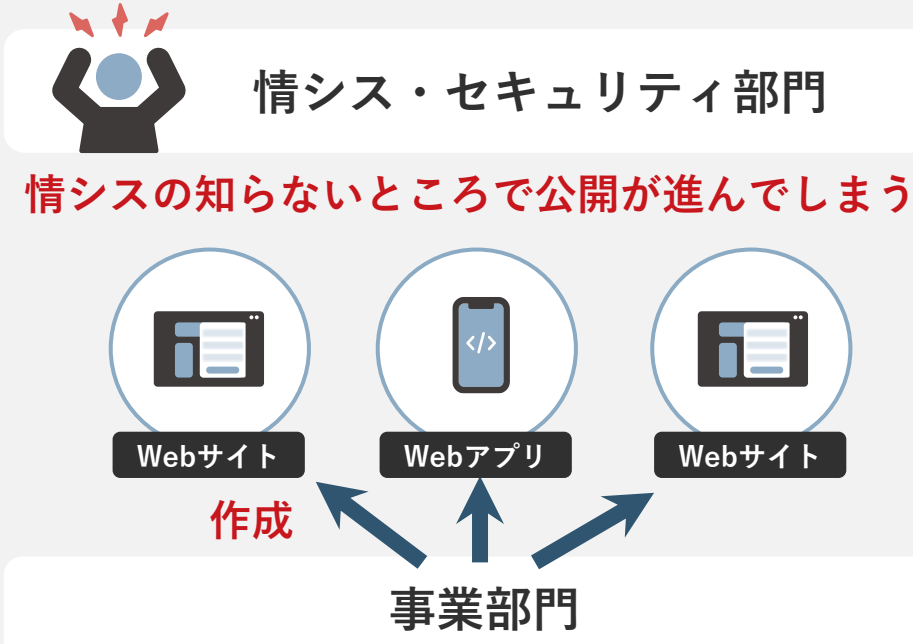
物理的なIT資産

台帳管理が可能な資産



デジタル資産

情シスの台帳に載らない資産



気づかないうちに増えている「未把握のデジタル資産」

公開するWebサイトや
提供するWebサービスが
増える

開発規模・サイト規模が
大きくなる
（100画面以上）

機能改修・追加など
リリース頻度が高く
間隔も短くなる

知らないうちに作られ
管理対象から漏れている

公開当初の構成から大きく乖離
最新状態をだれも把握していない

管理情報の修正が間に合わず
実態との齟齬が発生

攻撃者は、未把握の資産を狙っている

攻撃者は、公開されている情報（ドメイン・サブドメイン・証明書情報など）をもとに探索し、
管理されていない資産を足がかりに侵入を試みます。

「見えないものは守れない」

攻撃対象を可視化することが、サイバーセキュリティ強化の第一歩

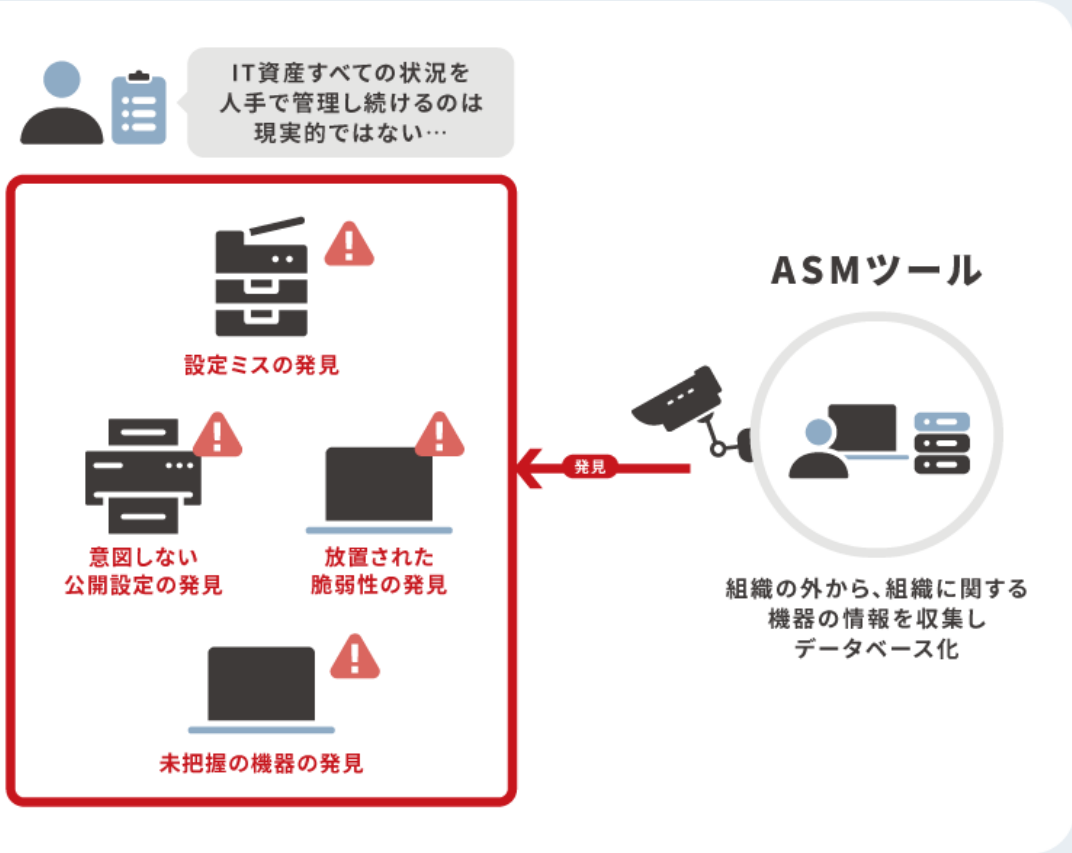
未把握の資産を可視化し、防御の網を広げる「ASM」

見えない攻撃対象を特定して管理の死角を排除する、ASMの必要性が高まっています。

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

資産ごとに異なる、リスク評価の難易度と運用負荷

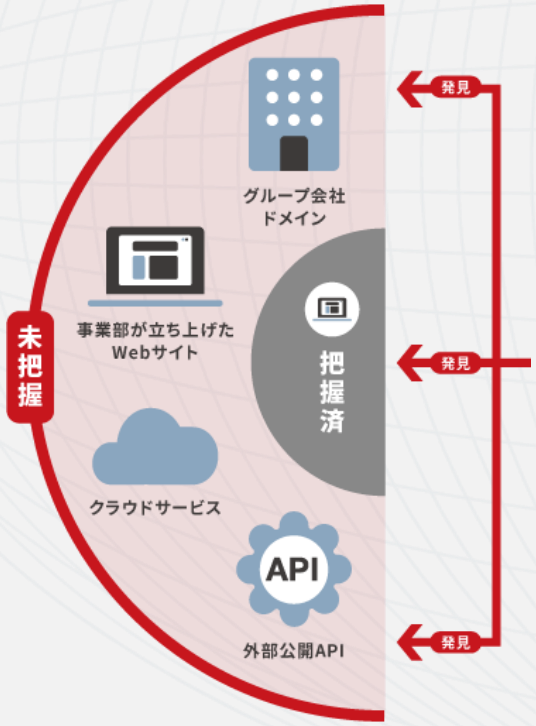
ASMで見つかった資産によって、その後の評価手法が大きく異なります。「定型管理」が可能なサーバー類に対し、Web資産の評価は今なお多大なコストと工数を要する「非定型な業務」のままになっていることも…。

	サーバー・NW機器	Web資産（サイト・アプリ）
主なリスク評価	パッチ適用状況・Ver.確認	脆弱性診断
手段	資産管理ツール・OS標準機能	外部委託・ツール活用
対策	自動更新・一括適用	個別の改修・コード修正
運用負荷	低い（仕組み化しやすい）	高い（コスト・工数）
頻度	リアルタイム	年1回に留まりがち

AeyeSecurityLab

Web資産の特定からリスク評価までを仕組み化する「Web-ASM」

仕組み化しづらいWeb資産に対し、ASMのアプローチを最適化させた「Web-ASM」が、いま解決策として注目されています。これまで非定型だった評価プロセスを定型化し、継続的な運用を可能にします。



攻撃面の
発見

攻撃面の
情報収集

攻撃面の
リスク評価

自社やグループで運用・管理すべきWebサイトを把握し、
継続的にリスク評価を実施できるようにすること。

Web-ASMを実用レベルに乗せるための最後のハードル

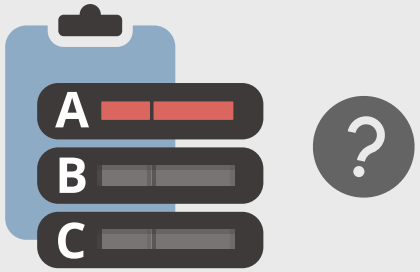
Web資産の特定には高度な判断が伴うため、従来のASMツールでは依然として「人の手による精査」がボトルネックとなっていました。

人力で探索・精査が必要

広範囲から検出することはできるが、
不要なものも多く紛れ込んでおり、
人手による精査が必要。

リスク評価が困難

リスクをどう評価するか悩ましい。
システム観点からだけでなく、
事業観点での優先順位付けが必要。



生成AIがWeb-ASMを「自動の定型業務」へ昇華させる

生成AIを活用することで、これまで人手に頼っていた「文脈の理解」や「リスク判定」が自動化され、
Web-ASMは真に現実的な運用フェーズへと進化します。

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

（エーアイスキャン）

AeyeScan でWeb資産管理の非定型を定型へ

AIが「発見」から「評価」までを仕組み化

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
300社以上

※ 富士キメラ総研調べ「2025 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 ベンダーシェア（2024年度実績）
※ITR調べ「ITR Market View：サイバー・セキュリティ対策市場2025」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

発見から評価までをひとつの「定型フロー」に統合

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

AeyeSecurityLab

専門知識が必要な「対応の優先順位」もAIがサポート

Web資産の重要度とリスクの深刻度をAIが判定。属人的になりがちな「判断」の工程まで定型化します。

Web資産の重要度			リスクの深刻度 NEW		
各Web資産の属性 （サイト用途、保持データなど）			ミドルウェアやライブラリの悪用観測脆弱性※ ※既にサイバー攻撃で悪用が確認された脆弱性		
	製品情報サイト	重要度：中	2件	ミドルウェアA CVE-xx 深刻度：高 ミドルウェアA CVE-xx 深刻度：中	
	ECサイト クレジットカード情報保持	重要度：高	1件	ライブラリB CVE-xx 深刻度：低	
	ヘルプサイト WordPress使用	重要度：低	10件	ミドルウェアC CVE-xx 深刻度：高 ライブラリD CVE-xx 深刻度：高 ：	

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

人材・教育

大川自動車教習所 / 河合塾 / Junion / JINSOKEN / ZENKIGEN / Direct Sourcing / PERSOL / Leverages / 立教大学 / workport

インフラ

EPARK / AIRE / HIS / H2O RETAILING / NTT EAST / odakyu / 近鉄情報システム株式会社 / 東急 / SymEnergy / 水ing Swing Corporation / Suzuyo / NANKAI 南海システムソリューションズ / 日本調剤 / JARMeC 日本動物高度医療センター / HITOWA GROUP / BOOK・OFF / ベルーナ / grow up together MEDIA / Looop / Loyalty Marketing, Inc.

金融

アイフル / MS&AD MS&ADインターリスク総研 / JOBPAY / SOMPOひまわり生命 / DMM FinTech / Tokyo Century / Net Protections

メディア

集英社 / 中日新聞 / NIKKEI / Media Do

製造

AICA / AISIN / KITZ 株式会社キッツ / KOSÉ / SAKI / TIGER / TEIJIN / Denkei / House / Mizuno / ユーグレナ

エンタメ

イープラス / CAPCOM / GungHo Online Entertainment, Inc. / とらラボ! TORANOANA LABORATORY / BookLive

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア / Lexica E-Retailing Platform / エアアドエムネット株式会社 / M-aid / エムティーアイ / OZ INTERNATIONAL / Classi / COACH A Co.,Ltd. / cybozu / Speee / SecureNavi / Diamond head / DMM Boost / TAL / Digital Garage / TEMONA / NAVITIME / KNOCK ON THE DOOR / BATONZ / VALUE HR / freee / vector / porters / 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 / Insight Edge / Infcurion / 80&Co. / SBWorks / NTT Integration / NTT DATA / NTT ビジネスソリューションズ / OMRON / Globalway / KDDI KDDI Agile Development Center / circlace / さくら情報システム / SUNDAY SYSTEMS / CEC / GA TECHNOLOGIES / Simplex Inc. / 777WORKS / SOFT CREATE / SOLTEC / 高千穂交易株式会社 / TDI / 電通総研 / TOPPAN / JOPS / JAST / PCNET 株式会社パシフィックネット / Human Interactive Technology inc. / FUJISOFT / FUJITSU / MACROMILL / MITSUBISHI ELECTRIC 三菱電機デジタルイノベーション株式会社 / YONA / リピスト / YL

セキュリティ企業

NEC NECセキュリティ / NTT DATA 株式会社NTTデータ先端技術 / GSX GLOBAL SECURITY EXPERTS / 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

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

会社概要

商号	株式会社 エーアイセキュリティラボ	
役員	代表取締役社長	青木 歩
	取締役副社長	安西 真人
	取締役	杉山 俊春　角田 茜
	執行役員 CTO	浅井 健
	執行役員	関根 鉄平
事業内容	情報セキュリティ関連事業（調査・コンサルティング） セキュリティ診断クラウドサービス「AeyeScan」提供	
設立	2019年4月	
拠点	東京都千代田区神田錦町2-2-1 KANDA SQUARE 11F WeWork内	
資本金	1億円	
社員数	61名	
Webサイト	https://www.aeyesec.jp/	
取得認証	情報セキュリティマネジメントシステム（ISMS） ISMSクラウドセキュリティ認証（ISO27017） 情報セキュリティサービス基準適合サービスリスト	

AeyeSecurityLab

セキュリティに
「あらたな答え」を提供し続ける
プロ集団

IS 752963 / ISO 27001

CLOUD 790050 / ISO 27017

023-0026-20

セキュリティに、確かな答えを。