

管理しきれていないWebサイトへの処方箋

「Web-ASM」で

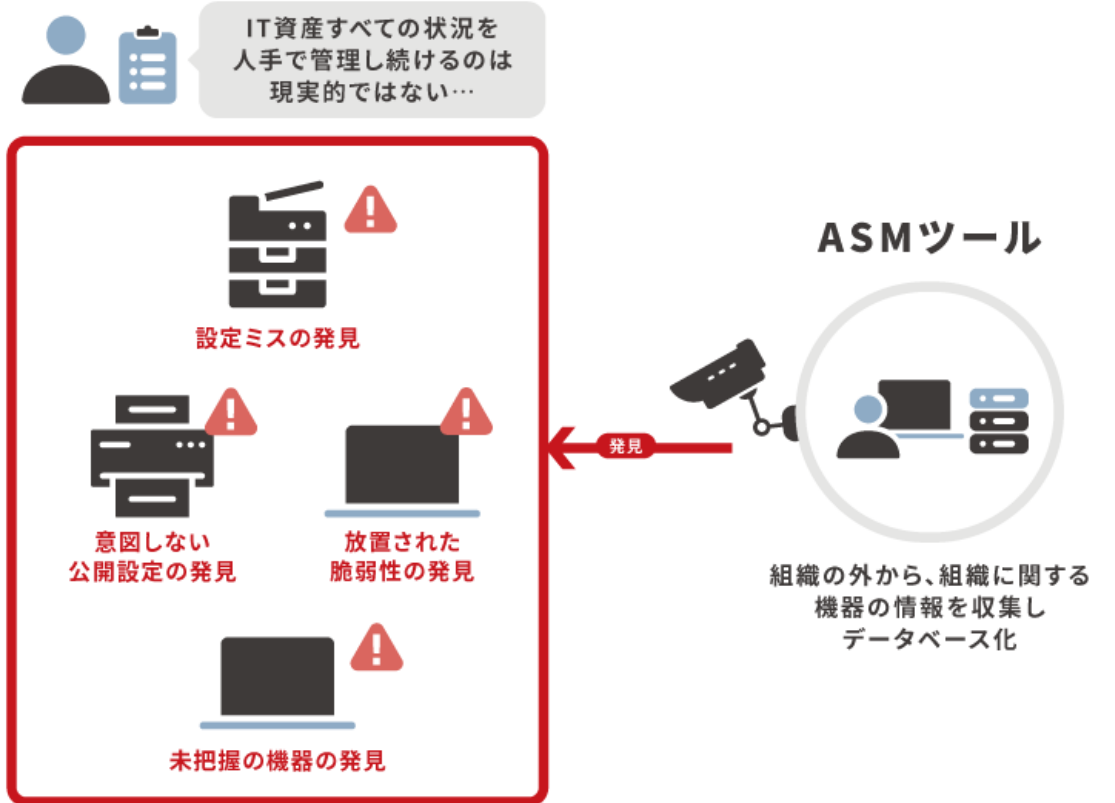
脆弱性対策を強化

AeyeSecurityLab



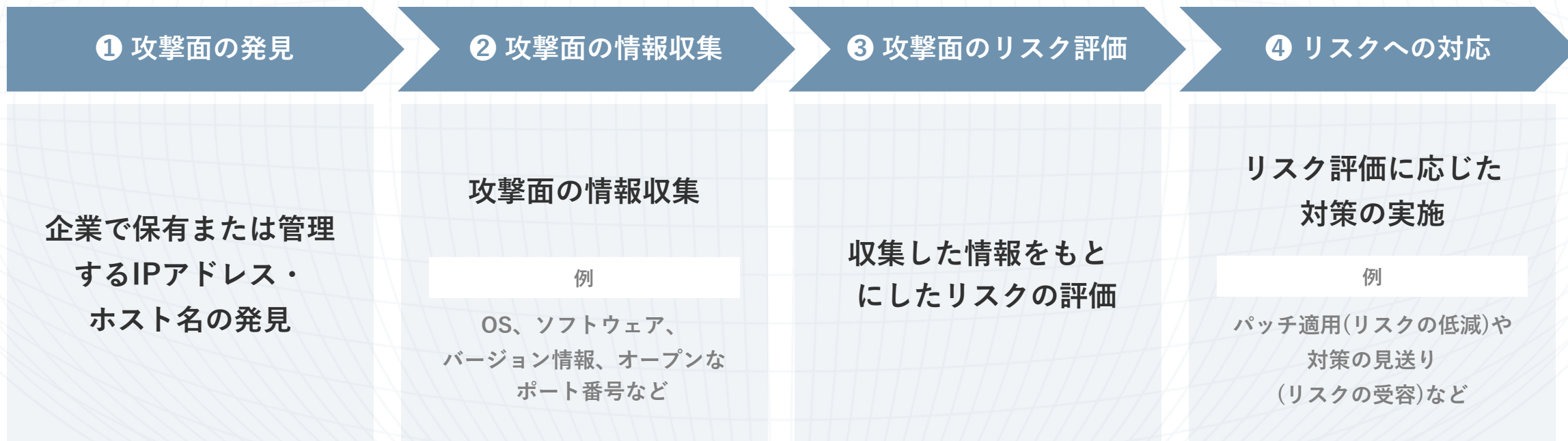
ASM (Attack Surface Management) とは

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



ASMのプロセス

ASMは、主に「攻撃面の発見」「攻撃面の情報収集」「攻撃面のリスク評価」「リスクへの対応」の4つのプロセスで構成される。



ASMと脆弱性診断との違い

ASMと脆弱性診断は、脆弱性管理ができるという共通点を除くと、以下のような違いがある。効果的なセキュリティ対策のためにも、目的に応じて使い分けることが大切。

| | ASM | 脆弱性診断 |
|----------|--------------------------------|---|
| IT資産の範囲 | 外部からアクセス可能なIT資産 (未把握のものを含む) | 自社で把握済みのIT資産 |
| 情報の確度 | IT資産の潜在的な脆弱性を示唆するにとどまる | 調査対象のIT資産に模擬攻撃のパケットを送信し、応答を評価して脆弱性を特定する |
| IT資産への影響 | 対象のIT資産への影響はほとんどない | 模擬攻撃のパケットが、IT資産の動作に影響を与えることがある |

ASMを取り巻くガイドライン・ガイダンスの状況

サイバーセキュリティ 経営ガイドライン Ver 3.0

ASM(Attack Surface Management) 導入ガイダンス

サプライチェーン強化に向けた
セキュリティ対策評価制度の構築について

外部から把握出来る情報を用いて
自組織のIT資産を発見し管理する

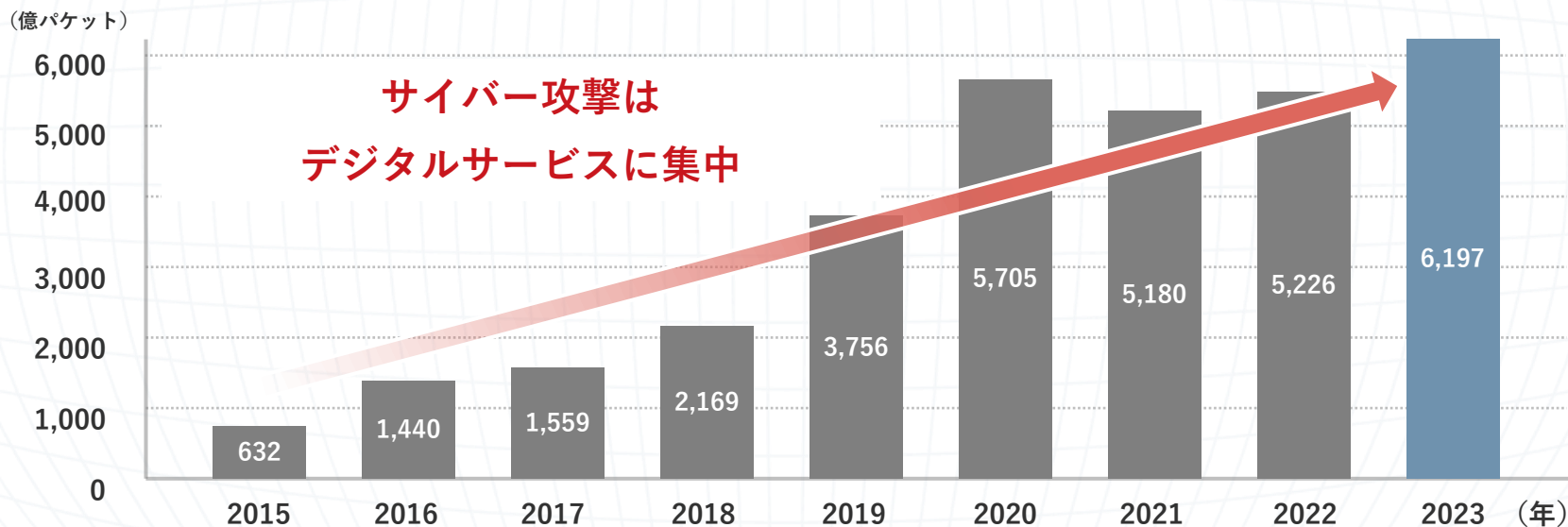
出展 [経済産業省 | サイバーセキュリティ経営ガイドライン Ver 3.0](#)

出展 [経済産業省 | ASM \(Attack Surface Management\) 導入ガイダンス](#)

サプライチェーン強化に向けて、ASMへの取組みが求められている

ASMを取り巻くサイバー攻撃の状況

DXの推進に伴いデジタルサービスが不可欠となる一方、サイバー攻撃のリスクも増大している。未把握のWebサイト・Webサービスへの対策が、デジタルサービス領域を守る第一歩。



サイバー攻撃を観測・分析できるシステム「NICTER」によると、2023年は過去最高の観測数を記録しており、サイバー攻撃がますます活発化している状況。そのうち約3割が、HTTP・HTTPSで使用されるポートへの攻撃である。



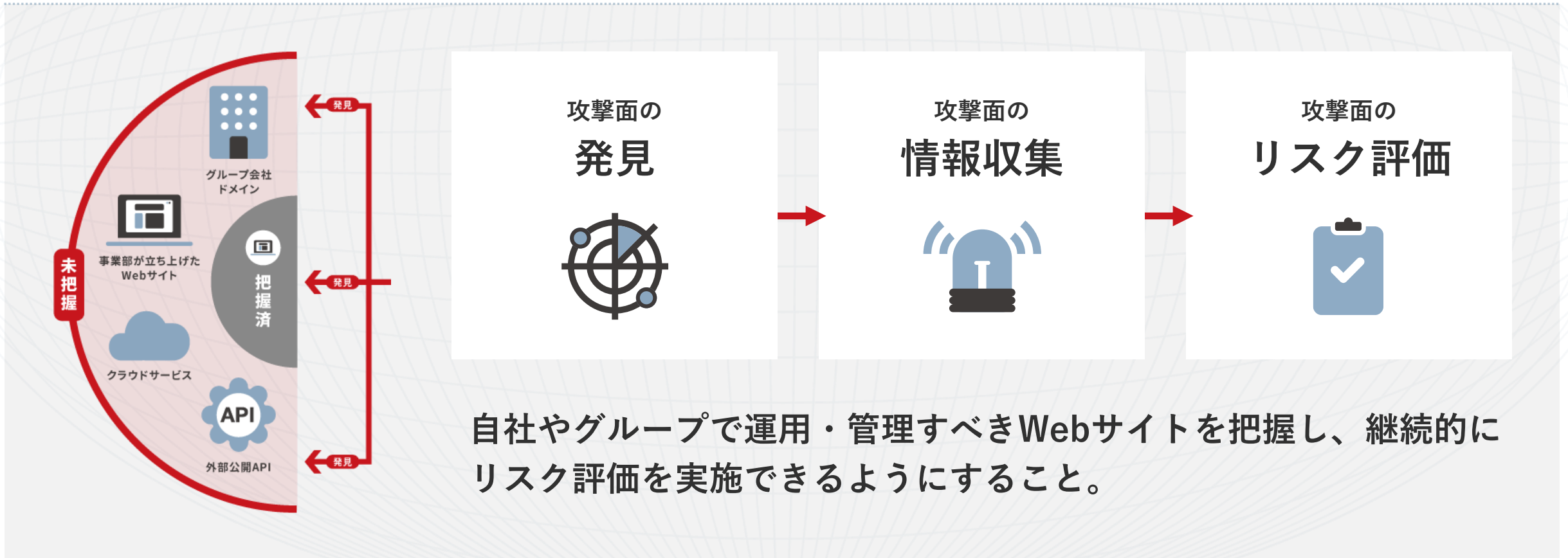
DX推進に伴い、
デジタルサービスが主流となっている

必要なのは **Web-ASM** という考え方

社内IT資産だけでなく、社外向けWebシステム・アプリのASMのこと

Web-ASMとは

未把握のWebサイトの継続的な発見・リスク評価

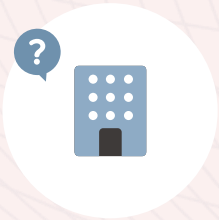


Web-ASMにおける課題

一般的なASMと同様、Web-ASMの実現には「人手がかかる」といった課題も。ただでさえセキュリティ対策においては人材不足が叫ばれている中、なかなか手が回っていない企業も多い。

ASMツールの発見結果が正しいか判断するために
人手がかかる

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

正しくリスク評価して、対策要否を判断するにも
人手がかかる

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

Web-ASMは「AeyeScan」にお任せください

クラウド型Web診断ツール「AeyeScan」のオプションである「Web-ASM機能」を使えば、未把握の攻撃面の発見から、脆弱性診断によるリスク評価までシームレスに実施可能。

Web-ASM機能には生成AIを、脆弱性診断にはAI・RPAを活用し※、大幅な効率化を実現

※脆弱性診断にもオプションで生成AIがご利用可能です

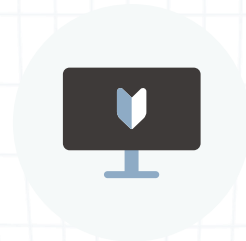


選ばれる理由



効率的に攻撃面を発見

管理しきれていない
Webサイトの未把握攻撃面まで
生成AIで効率的・網羅的に発見



誰でもかんたん操作

開発やセキュリティの
知識がなくても、
トレーニングなしで診断可能。



AIによる自動診断

圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。

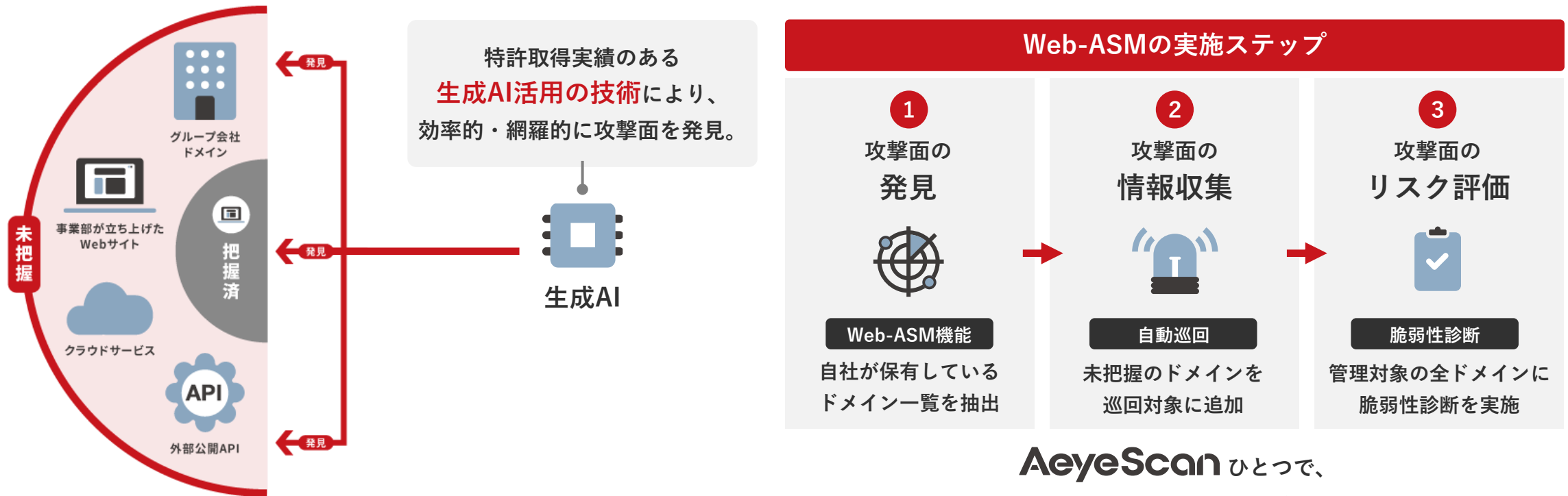


わかりやすいレポート

各種ガイドラインに準拠した
プロ仕様のレポート出力、日本語と英
語に対応。

生成AI活用で、工数をかけずにWeb-ASMを実現しませんか？

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。



AeyeScan ひとつで、

より網羅的な脆弱性診断とリスクマネジメントが可能に！

 **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



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

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



エンタメ



SaaS



SI・IT企業



セキュリティ企業



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 | 田中 大介 |
| 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） クラウド型Web診断サービス「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 | | |
| 従業員数 | 37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

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。