ランサムウェアの狙いはVPNだけじゃない！？

AIと実現する、Web資産の把握 & 脆弱性診断 の 内製化術

©AeyeSecurityLab Inc.

AeyeSecurityLab

登壇者紹介

主な著書

株式会社エーアイセキュリティラボ

事業企画部 ディレクター **阿部 一真**（あべ かずま）

新卒でNTTデータに入社し、Salesforceビジネス推進部門で
コンサルティングセールス・カスタマーサクセスを経験。
その後、AIベンチャー企業・SaaSスタートアップ企業にてCS責任者
およびプロダクトマネージャー・事業統括責任者を歴任し、エーアイ
セキュリティラボに入社。
現在は、新規プロダクト企画・事業開発をリードしながら、
各種セミナー・講演への登壇などエバンジェリストとしても活動。

©AeyeSecurityLab Inc.

あらたな答えを、つぎつぎと。

変化の激しいサイバーセキュリティの世界。

私たちは、未知の課題が生まれるたび、培った知見と経験・実績をもとに、
「あらたな答え」を世の中に提供し続けていきます。

世界も驚くような、技術の力で。

そして、サイバーセキュリティの進化を通して、
人は、人にしかできない、創造性を活かした仕事に注力できる、
社会の進化にも貢献していきます。

AeyeSecurityLab

©AeyeSecurityLab Inc.

2025年を振り返ると…

©AeyeSecurityLab Inc.

ランサムウェア被害が相次いでいる

大手保険代理店

およそ510万件にのぼる
個人情報漏洩の可能性

大手飲料メーカー

製造ライン・商品出荷が停止
個人情報漏洩の可能性も

大手オフィス用品ECサイト

業務停止・情報流出の可能性
提携他社への影響も

大手商社

クラウドシステム開発会社

クリニック

総合物流企業

大手小売業

私立大学

⋮

この他にも多くの事例が発表されており、被害は後を絶たない状況

©AeyeSecurityLab Inc.

AeyeSecurityLab

未修正の脆弱性が侵入を許す

ランサムウェア攻撃を含む全データ漏洩において「脆弱性の悪用」が主な初期侵入原因に

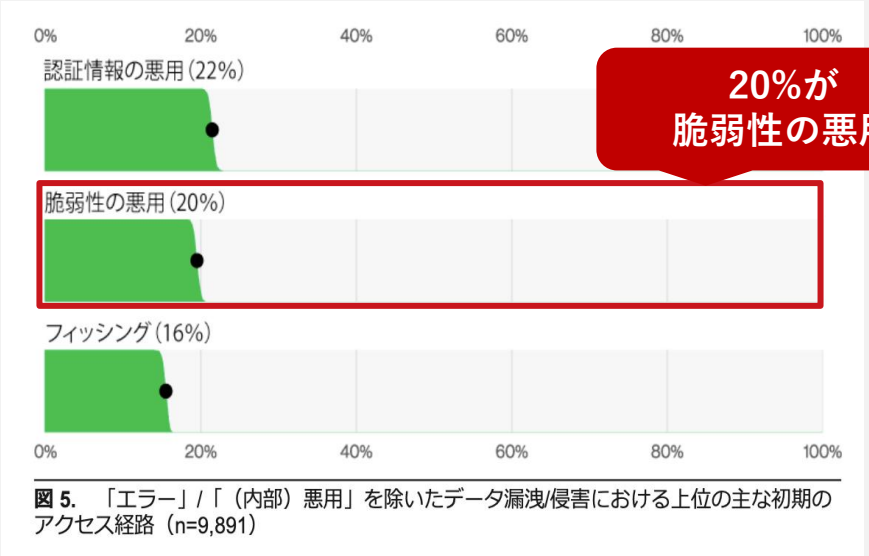


図 5. 「エラー」/「（内部）悪用」を除いたデータ漏洩/侵害における上位の主な初期のアクセス経路（n=9,891）

昨年と比べて34%の増加

ランサムウェア攻撃の75%を占めるシステム侵入でも「脆弱性の悪用」が最も一般的な初期侵入原因に

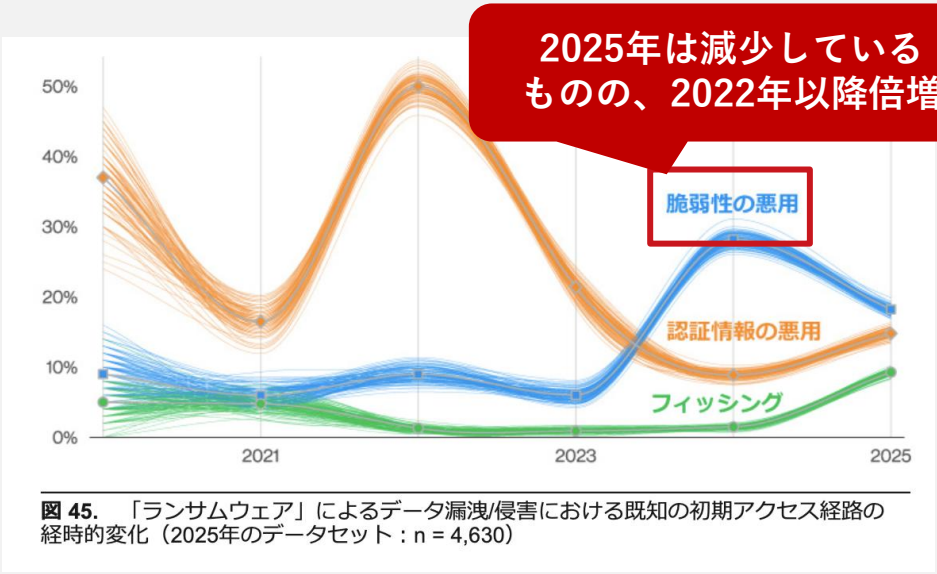


図 45. 「ランサムウェア」によるデータ漏洩/侵害における既知の初期アクセス経路の経時的変化（2025年のデータセット：n = 4,630）

ゼロデイ攻撃が脆弱性の悪用増加の一因に

出典：ベライゾン社 2025年度 データ漏洩/侵害調査報告書（DBIR）
https://www.verizon.com/business/ja-jp/resources/reports/dbir/

©AeyeSecurityLab Inc.

AeyeSecurityLab

多様化するランサムウェアの「侵入経路」

NW機器/VPN

クラウド

Webサイト

CMS/SaaS

PC/社用端末

メール/ファイル

©AeyeSecurityLab Inc.

VPNよりWebが狙われている

データ漏洩／侵害は、リモートアクセス（VPN）
だけで起きているわけではない。

Webアプリケーションの方が多く**42%**

ランサムウェアも、Web資産が初期侵入の足がかりとなり

未修正の脆弱性が悪用されるケースが増加

していると考えられる。

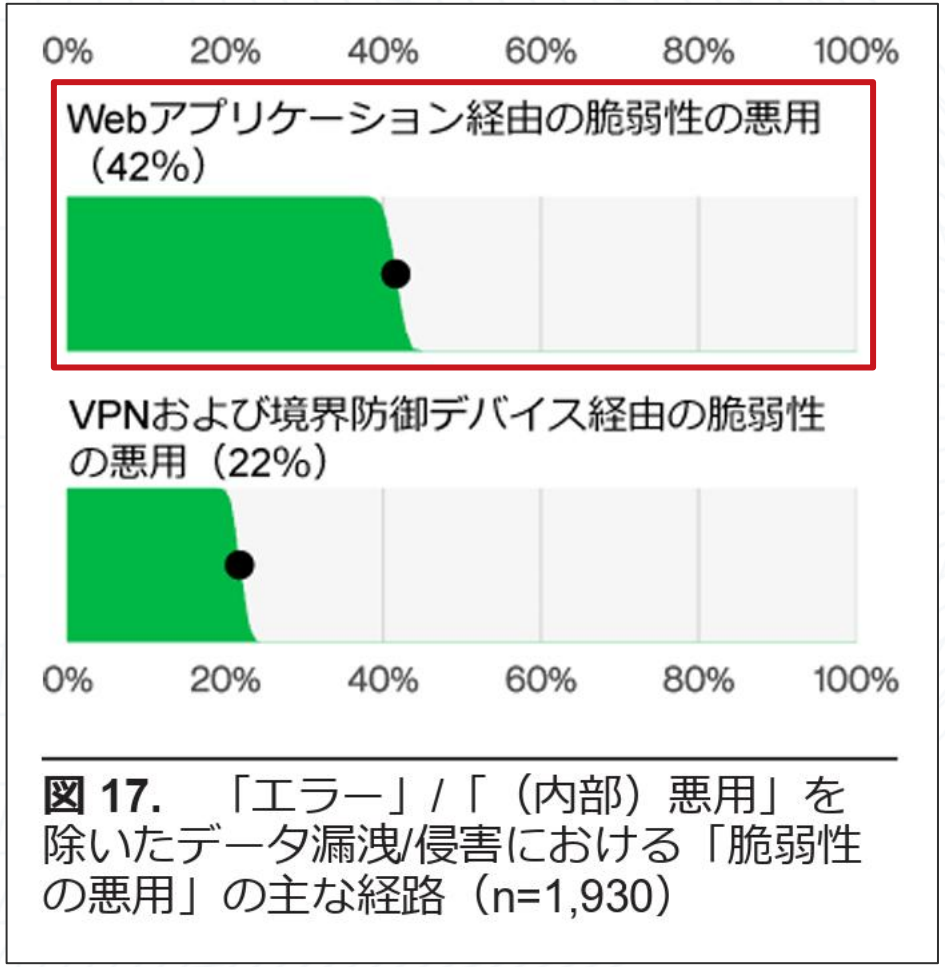


図 17. 「エラー」/「（内部）悪用」を除いたデータ漏洩/侵害における「脆弱性の悪用」の主な経路（n=1,930）

出典：ベライゾン社 2025年度 データ漏洩/侵害調査報告書（DBIR）
https://www.verizon.com/business/ja-jp/resources/reports/dbir/

©AeyeSecurityLab Inc.

AIで「効率化」されたサイバー攻撃にどう立ち向かう？

©AeyeSecurityLab Inc.

攻撃手法はAIにより高度化されている

攻撃者

365日24時間

AIがWebサイトの「未修正の脆弱性」を自動で探索

企業

年に1回

自社のWebサイトに脆弱性診断を実施

常に攻撃してくる相手に、年1回の脆弱性診断では太刀打ちできない

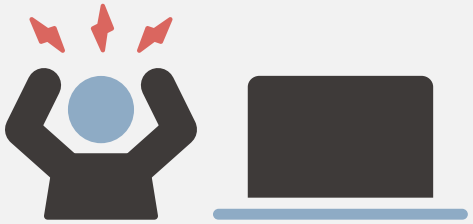
©AeyeSecurityLab Inc.

AeyeSecurityLab

従来の脆弱性対策のやり方を変えなければならない

年1回の
チェックのみ

診断は
外部委託中心



リードタイムが長く
攻撃のスピードに追従しづらい

攻撃者と同じ
スピード感

社内で
いつでも診断

脆弱性の有無を常時把握し
必要に応じて対応できる

24時間365日体制の脆弱性診断を、**内製化**で実現することが望ましい

©AeyeSecurityLab Inc.

脆弱性対策の成熟段階

成熟段階		把握済み資産	未把握の資産
Lv.1	既知のWeb資産に対する脆弱性の把握	ひと通り診断	ー
Lv.2	優先順位に基づく定常的な診断＆対応	定期的な診断	ー
Lv.3	未知の攻撃面を含む網羅的な資産管理	定期的な診断	探索・棚卸し
Lv.4	「探索→優先度付け→診断」サイクル	定期的な診断	定期的な探索

©AeyeSecurityLab Inc.

脆弱性対策の「内製化」に立ちはだかる壁

©AeyeSecurityLab Inc.

脆弱性診断を内製化するときに考えること

「内製化できればいいんだけどな…」

診断の**品質を維持**できるだろうか？

診断員を**育成・確保**できるだろうか？

コスト(費用・時間)を削減できるか？

©AeyeSecurityLab Inc.

脆弱性診断を内製化するときに考えること

診断の**品質を維持**できるだろうか？

診断員を**育成・確保**できるだろうか？

コスト(費用・時間)を削減できるか？

プロ級の機能・性能

誤検知・過検知が少なく
外部委託（手動診断）に近い性能

誰でも使える操作性

ツール習得コストがかからず
すぐに・簡単に利用できる

利用範囲・回数が無制限

画面数やサイト数に制限がなく
いつでも・いくらでも使える

©AeyeSecurityLab Inc.

でも、Web資産の把握って難しくない…？

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

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

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
- 潜在的なデジタル領域の攻撃面
- サプライチェーンの拡大

情シス・セキュリティ部門が認識しやすい
社内ITを中心とした「静的」IT資産がほとんど

どこで何やってるか
分からない…！

©AeyeSecurityLab Inc.

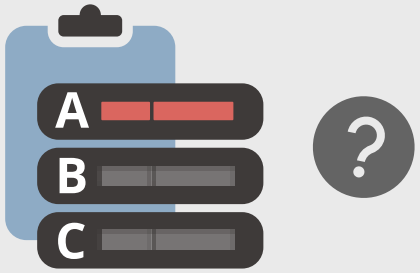
Web資産を把握する難しさ

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。



©AeyeSecurityLab Inc.

待てよ、攻撃者もAIを使ってるんだから
こっちも生成AIとか使えないかな…？

©AeyeSecurityLab Inc.

生成AI時代の脆弱性診断なら AeyeScan

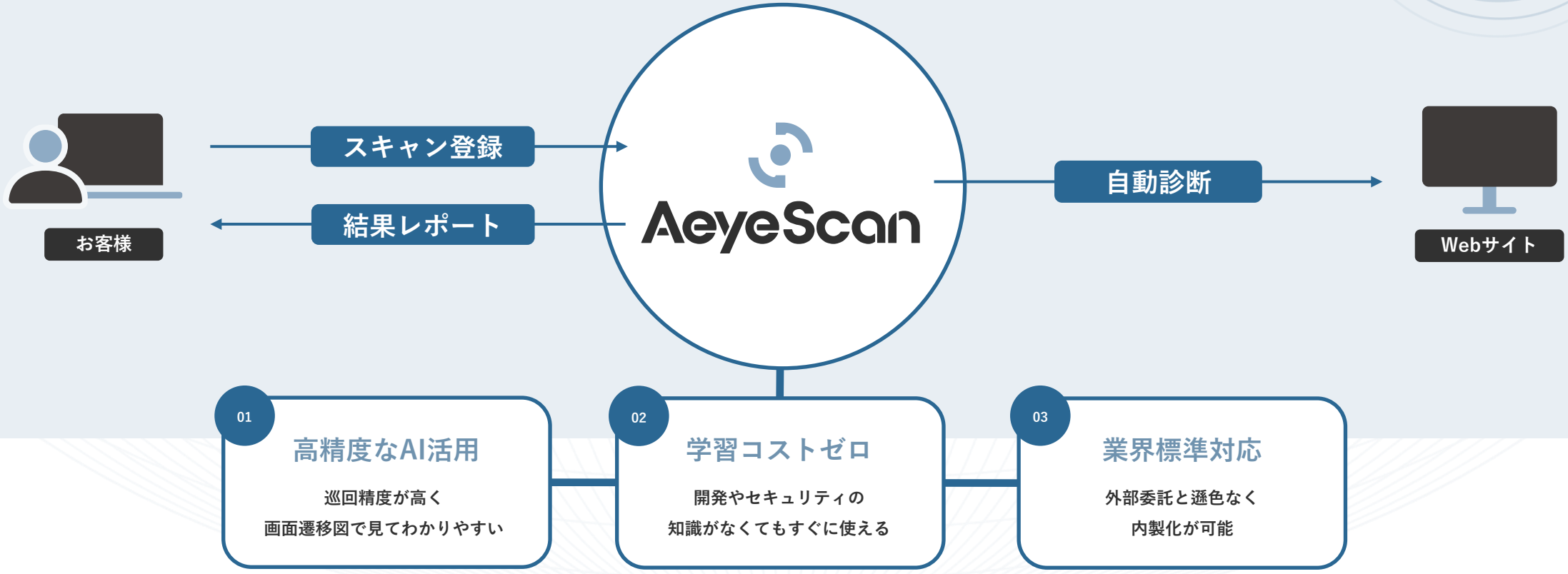
クラウド型Webアプリケーション
脆弱性検査ツール

国内市場シェア
No.1※

富士キメラ総研調べ「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（2024年度実績）

有償契約
300社以上



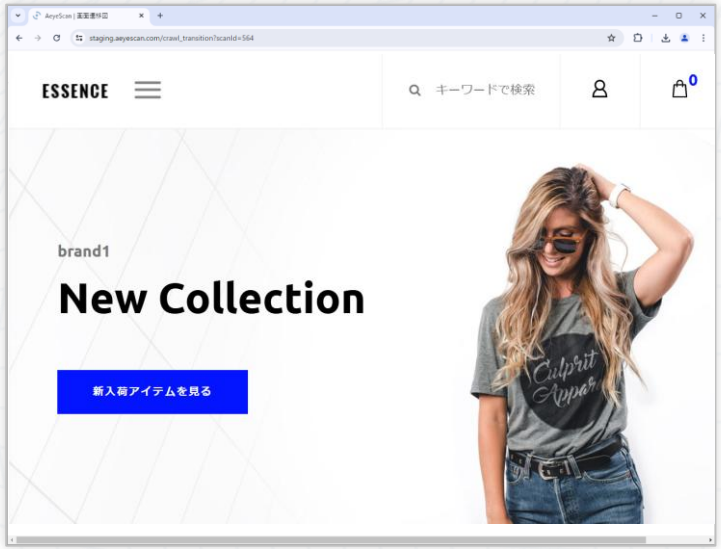
01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

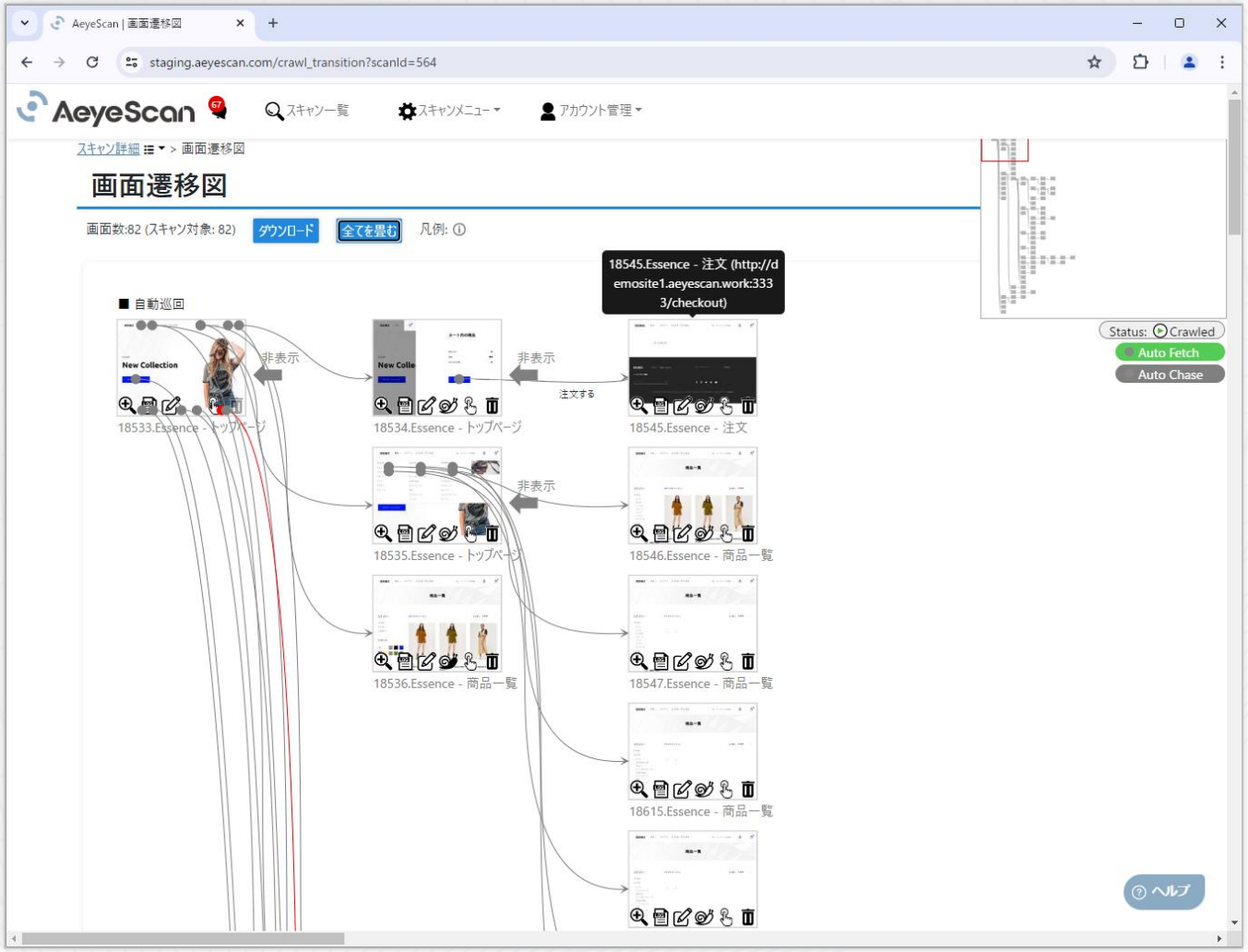
02
学習コストゼロ
開発やセキュリティの
知識がなくてもすぐに使える

03
業界標準対応
外部委託と遜色なく
内製化が可能

©AeyeSecurityLab Inc.

巡回時に、自動で画面遷移図を生成





©AeyeSecurityLab Inc.

AeyeSecurityLab

結果がわかりすく、すぐさま修正作業に取り組めるレポート

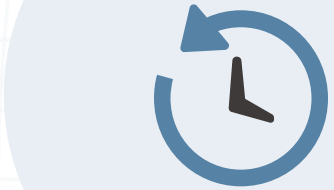
©AeyeSecurityLab Inc.

AeyeSecurityLab

AeyeScanが選ばれている理由

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。

©AeyeSecurityLab Inc.

AeyeScanが選ばれている理由

誰でも使える操作性 × プロが認める機能・性能

©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

インフラ※

EPARK / AIRE / HIS / HO RETAILING / NTT EAST / odakyu / 近鉄情報システム株式会社 / GEO / SymEnergy / 水ing Swing Corporation / Suzuyo / TOYOTA HOME / 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.

エンタメ

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

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

金融

7&i / 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

人材・教育

OHSAWA DRIVING SCHOOL / 河合塾 / Junion / JINSOKEN / ZENKIGEN / Direct Sourcing / PERSOL / 立教大学 / Leverages / workport

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア / Lexica E-Retailing Platform / エフアンドエムネット株式会社 / M-aid / MTエムティーアイ / OZ INTERNATIONAL / giftee* / 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 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 株式会社パソフィックネット / Human Interactive Technology Inc. / FUJISOFT / FUJITSU / MACROMILL / 三菱電機デジタルイノベーション株式会社 / YONA / リピスト

セキュリティ企業

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

※公共および社会・生活基盤までを包含

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

生成AIを活用したWeb-ASM機能で Web資産の把握・定期監視を実現

Web-ASMの実施ステップ

1 攻撃面の **発見**

Web-ASM機能

自社が保有している
ドメイン一覧を抽出

2 攻撃面の **情報収集**

自動巡回

未把握のドメインを
巡回対象に追加

3 攻撃面の **リスク評価**

脆弱性診断

管理対象の全ドメインに
脆弱性診断を実施

AeyeScan とあわせて
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！

ビジネス観点＆技術観点でリスクを評価

サイト用途

Medium

- ECサイト
- 製品情報サイト
- サービスサイト

など

Low

- ブログ系サイト
- 外部SaaSサイト
- テストサイト

など

保持データ

High

- 個人情報
- クレジット情報

など

簡易スキャン

Low

- TLS暗号スイートの不備
- HTTPSが強制されていません
- Cache-Controlヘッダの不備

など

Info

- 期限切れ間近のサーバ証明書
- Referrer-Policyヘッダの不備

など

©AeyeSecurityLab Inc.

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

生成AIをASMに活用することで…！

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.

AeyeSecurityLab

リスク対応の優先順位付けに必要な情報を自動判別

Web資産の重要度

各Web資産の属性

（サイト用途、保持データなど）

リスクの深刻度 NEW

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 ：

©AeyeSecurityLab Inc.

セキュリティ診断のお悩み・お困りごとをお聞かせください！

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 に関する 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.

本日の内容を受けて・・・

AeyeScanをもっと知りたい方向け

＼診断ツールの違いを知り、AeyeScanを体験／

6/09 火 オンライン@Zoom

6/17 水 オンライン@Zoom

6/26 金 神田スクエア

詳細・お申し込みはこちら

色々な角度から情報収集したい方向け

＼市場のトレンドを軸に様々な情報をお届け／

6/18 木 Web資産管理の実践知を解説

6/30 火 OWASP Top 10×実例を学ぶ

自席で視聴可能！お気軽にご参加ください

詳細・お申し込みはこちら

©AeyeSecurityLab Inc.

セキュリティに、確かな答えを。

©AeyeSecurityLab Inc.