

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サイトの 把握 & 診断の **内製化術**

登壇者紹介



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CXチームでの活動に加え、新規プロダクト企画・海外事業展開など全社横断プロジェクトにも携わる。

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。

2025年を振り返ると…

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

クリニック

大手小売業

クラウドシステム開発会社

総合物流企業

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

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

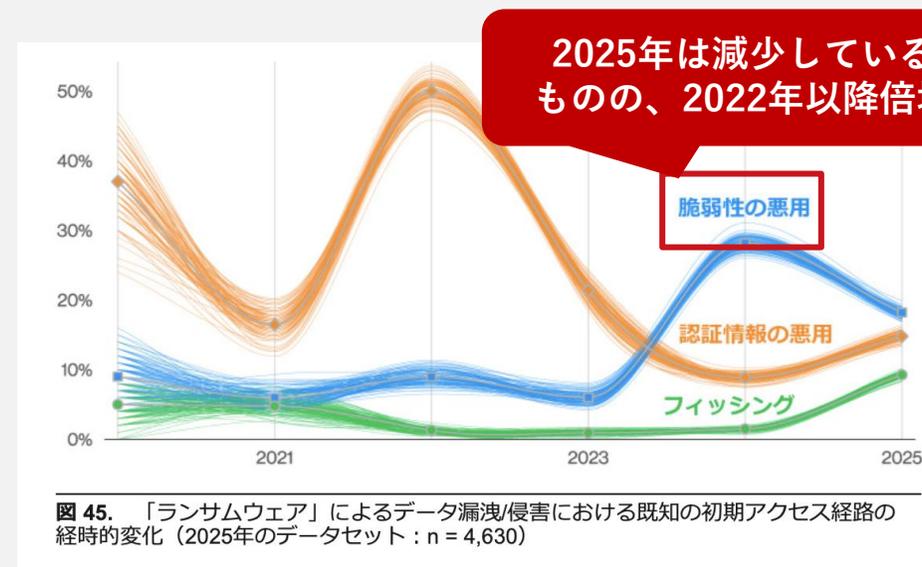
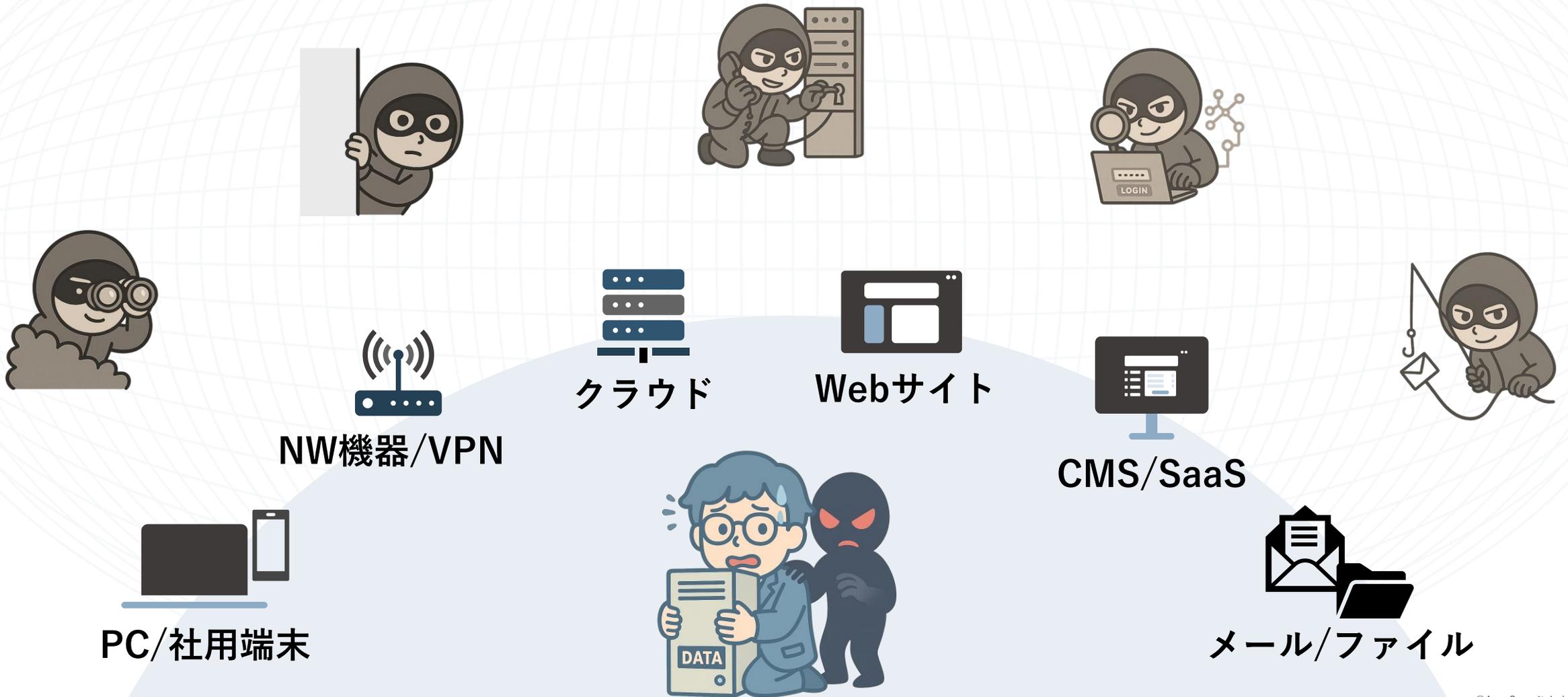


図 45. 「ランサムウェア」によるデータ漏洩/侵害における既知の初期アクセス経路の経時的変化 (2025年のデータセット: n = 4,630)

ゼロデイ攻撃が脆弱性の悪用増加の一因に

多様化するランサムウェアの「侵入経路」



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。

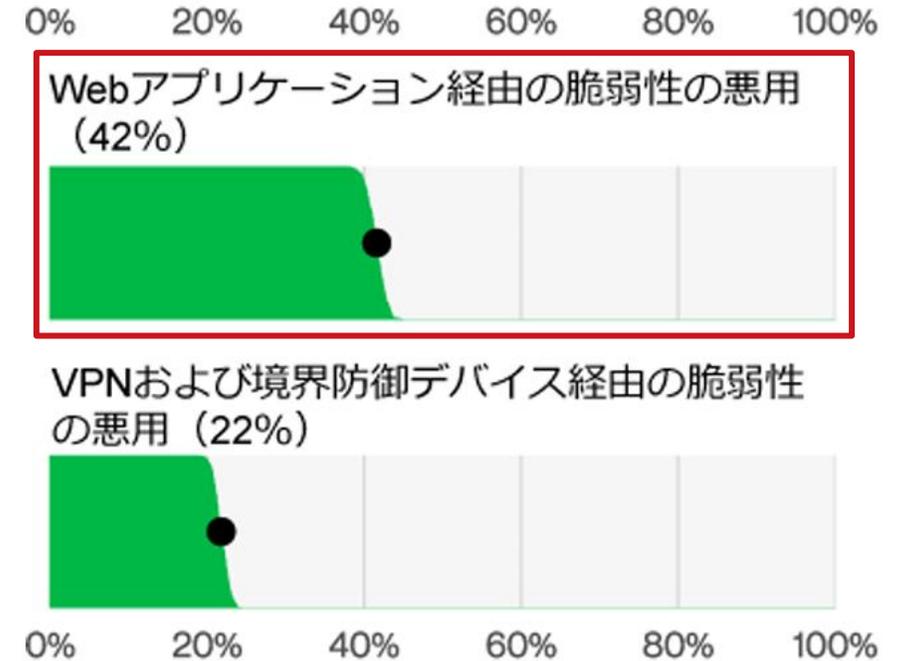
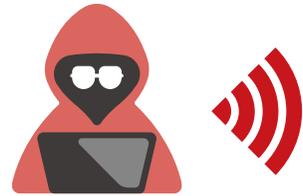


図 17. 「エラー」/「(内部) 悪用」を除いたデータ漏洩/侵害における「脆弱性の悪用」の主な経路 (n=1,930)

AIで「効率化」されたサイバー攻撃に どう立ち向かう？

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

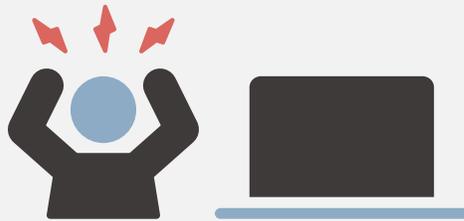
自社のWebサイトに脆弱性診断を実施

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

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

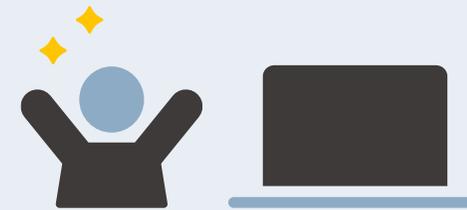


リードタイムが長く
攻撃のスピードに追従しづらい



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

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	—
Lv.2	優先順位に基づく定常的な診断&対応	定期的な診断	—
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

脆弱性対策の「内製化」に 立ちはだかる壁

脆弱性診断を内製化するときを考えること

「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？

脆弱性診断を内製化するときを考えること

診断の品質を維持
できるだろうか？

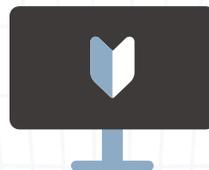
プロ級の機能・性能



誤検知・過検知が少なく
外部委託（手動診断）に近い性能

診断員を育成・確保
できるだろうか？

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

コスト（費用・時間）
を削減できるか？

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

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



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

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



どこで何やってるか
分からない…！

| 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。





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…？



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※



※富士ケメラ総研調べ「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



スキャン登録

結果レポート

AeyeScan

自動診断

Webサイト

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

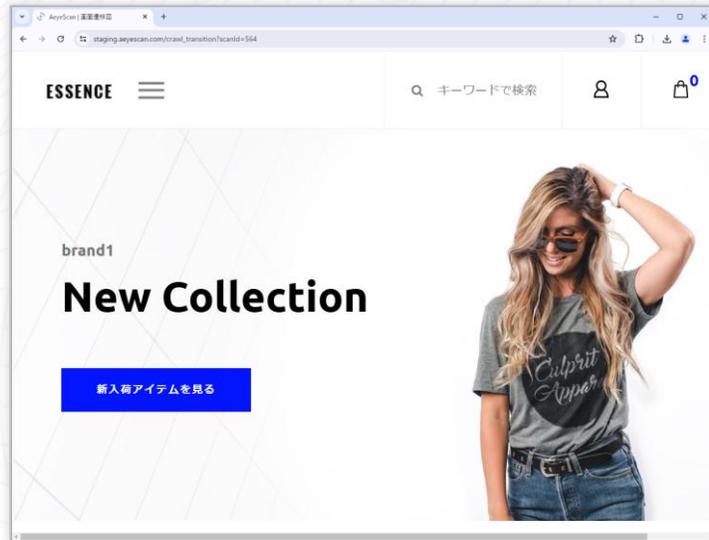
開発やセキュリティの
知識がなくてもすぐに使える

03

業界標準対応

外部委託と遜色なく
内製化が可能

巡回時に、自動で画面遷移図を生成



画面遷移図

画面数:82 (スキャン対象: 82) [ダウンロード](#) [全てを豊む](#) 凡例: ①

自動巡回

18533.Essence - トップページ

18534.Essence - トップページ

18535.Essence - トップページ

18536.Essence - 商品一覧

18545.Essence - 注文 (http://d.emosite1.aeyescan.work:333/3/checkout)

18546.Essence - 商品一覧

18547.Essence - 商品一覧

18615.Essence - 商品一覧

Status: Crawled

[Auto Fetch](#)

[Auto Chase](#)

ヘルプ

結果がわかりやすく、すぐさま修正作業に取り組めるレポート

AeyeScan

Web-ASM | スキャン一覧 | スキャンメニュー | 組織設定

スキャン一覧 > スキャン詳細 > スキャン結果(カテゴリ)

スキャン結果(カテゴリ)

● 会社概要アップデート (<http://demosite1.aeyescan.work:3333/>)

レポートダウンロード

Severity	Count
Critical	11
High	0
Medium	23
Low	1
Info	17

● OWASP TOP 10の結果

- > A1:2017-インジェクション: 11件
- > A2:2017-認証の不備: 1件
- > A3:2017-機微な情報の露出: 1件
- > A4:2017-XML 外部エンティティ参照(XXE): 1件
- > A5:2017-アクセス制御の不備: 0件
- > A6:2017-不適切なセキュリティ設定: 17件
- > A7:2017-クロスサイトスクリプティング(XSS): 18件
- > A8:2017-安全でないデシリアライゼーション: 1件
- > A9:2017-既知の脆弱性のあるコンポーネントの使用: 1件

ヘルプ

概要 | 脆弱性情報 | 詳細ログ | 再スキャン実行

クロスサイトスクリプティング

スキャン情報

81. 会社概要アップデート (<http://demosite1.aeyescan.work:3333/>)

対象ページ

1777.Essence - 新規登録 (確認) (<http://demosite1.aeyescan.work:3333/register>)

画面遷移図で表示

深刻度

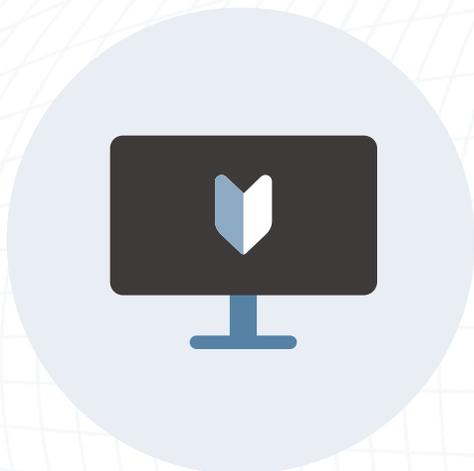
Medium

CVSS: 5.1 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N)

スクリーンショット

The left screenshot shows a login page with fields for 'メールアドレス' (Email Address) and 'パスワード' (Password). The right screenshot shows a registration form with fields for '氏名' (Name), '性別' (Gender), '年齢' (Age), 'パスワード' (Password), '確認パスワード' (Confirm Password), 'メールアドレス' (Email Address), and '電話番号' (Phone Number). A blue arrow points from the 'パスワード' field in the login page to the 'パスワード' field in the registration form.

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。

| 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

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



メディア



インフラ



製造



SaaS



金融



エンタメ



SI・IT企業



セキュリティ企業



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

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

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！

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
辿ったルートの説明



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



 <p>製品情報サイト</p> <p>重要度：中</p>	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
 <p>ECサイト クレジットカード 情報保持</p> <p>重要度：高</p>	1件	ライブラリB CVE-xx 深刻度：低
 <p>ヘルプサイト WordPress使用</p> <p>重要度：低</p>	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 :

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



定期開催中！

AeyeScanがよく分かるデモ動画・セミナー

AeyeScanを
検討してみたい方へ

AeyeScanがどんなものか知りたい方向けに、
デモを交えてわかりやすくご紹介。
まずは気軽に使い勝手をチェック！

AeyeScanデモ動画を視聴

AeyeScanの操作を
体験してみたい方へ

実際の操作を通して、一連の機能を体感。
導入前の不安や疑問をまるごと解消。
“わからないまま”をなくすセミナーです。

ハンズオンセミナーの日程を確認

セキュリティ対策に
お悩みの方へ

最新の事例や対策ノウハウをテーマ別に紹介。
月替わりで学べる無料ウェビナーを開催中。
お気軽にご視聴いただけます！

ウェビナーの日程を確認





AeyeScan

セキュリティに、確かな答えを。