「いつかやろう」が一番危ない

Webサイトの脆弱性対策を後回しにしてはいけない理由

AeyeSecurityLab

本資料の目的

「いつかやろう」と後回しにされがちなWebサイトの脆弱性対策。
しかし実際には、Webサイトは公開された瞬間からサイバー攻撃の対象となっており、
気づかないうちに被害が進行しているケースも少なくありません。

さらに、リリースや改修のたびに新たな脆弱性は発生し続けるため、
「一度診断したら終わり」「年1回やれば大丈夫」では安全を維持できない時代になっています。

本資料では、脆弱性対策を後回しにするリスクと、継続的な脆弱性診断が必要とされる理由、
そして継続運用を実現するための「内製化」という選択肢についてご紹介しています。

「脆弱性診断の必要性が理解しきれていない」「必要性は感じているが、具体的な行動に移せていない」
あるいは、「どう継続的な診断体制をつくればいいのかわからない」
といった方に役立つ内容となっていますので、ぜひご一読ください。

その「後回し」が、貴社を揺るがす。
脆弱性対策を怠った際の甚大なコスト

貴社のWebサイトも、すでに攻撃されているかもしれない

Webサイトは常にサイバー攻撃のリスクに晒されており、個人情報の窃取などを目的とした被害が後を絶ちません。攻撃が発生してから発覚するまでの平均期間は長く、今この瞬間も、気付かぬうちに攻撃されている可能性があります。

攻撃発生～発覚までの平均期間

参考： https://www.cscloud.co.jp/news/report/202402216761/（株式会社サイバーセキュリティクラウド）

インシデント発生時において生じる損害

各種事故対応についてアウトソーシング先への支払が発生

1	費用損害 （事故対応損害）	被害発生から収束に向けた**各種事故対応**に関してアウトソーシング先への支払を含め、自組織で直接費用を負担することにより被る損害（下記2～6に該当しないもの）

さらに、次のような損害の発生も起こりうる

2	賠償損害	情報漏えいなどにより、第三者から損害賠償請求がなされた場合の**損害賠償金**や弁護士報酬等を負担することにより被る損害
3	利益損害	ネットワークの停止などにより、事業が中断した場合の**利益喪失**や、事業中断時における人件費などの固定費支出による損害
4	金銭損害	ランサムウェア、ビジネスメール詐欺等による**直接的な金銭（自組織の資金）の支払い**による損害
5	行政損害	個人情報保護法における**罰金**、GDPRにおいて課される**課徴金**などの損害
6	無形損害	風評被害、ブランドイメージの低下、株価下落など、無形資産等の価値の下落による損害、**金銭の換算が困難な損害**

参考： NPO法人 日本ネットワークセキュリティ協会『インシデント損害額調査レポート 第2版（2024年）』より引用

AeyeSecurityLab

サイバー攻撃による金銭的損失は大きい

予想される金銭的損失だけでなく、ブランドイメージ低下や株価下落など無形損害による影響は甚大なものになります。

予想される金銭的損失（平均）

Webサイトからの情報漏洩による被害額

※クレジットカード情報を含む場合

3,843万円

一人当たりの損害賠償額

約3万円

事後調査
（フォレンジック調査など）

300~数千万円以上

＋

時価総額への影響

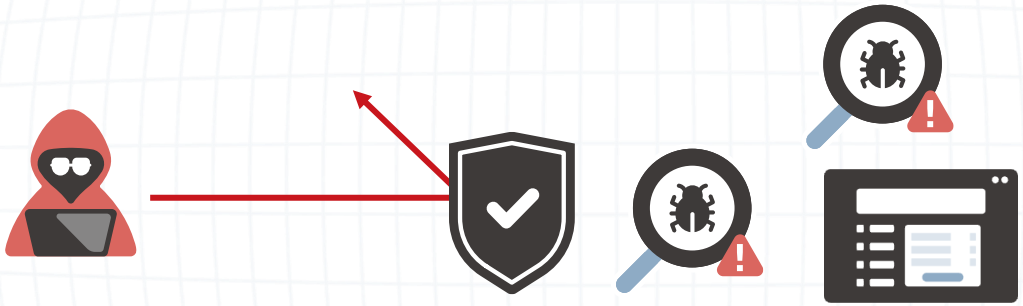
株価下落
ブラインドイメージ低下

株価平均 **6.3%下落**

参考：「JNSA『2018年 情報セキュリティインシデントに関する調査報告書』および『インシデント損害額調査レポート 第2版（2024年）』より引用・算出」

脆弱性診断は投資対効果の高い対策

Webサイトからの漏洩原因は「SQLインジェクション」や「設定不備」などの既知の脆弱性を突かれたものが多く、脆弱性診断で防げる可能性が高いです。
事後の「復旧費用」に対し、事前の「脆弱性診断」はその数分の一のコストですみます。



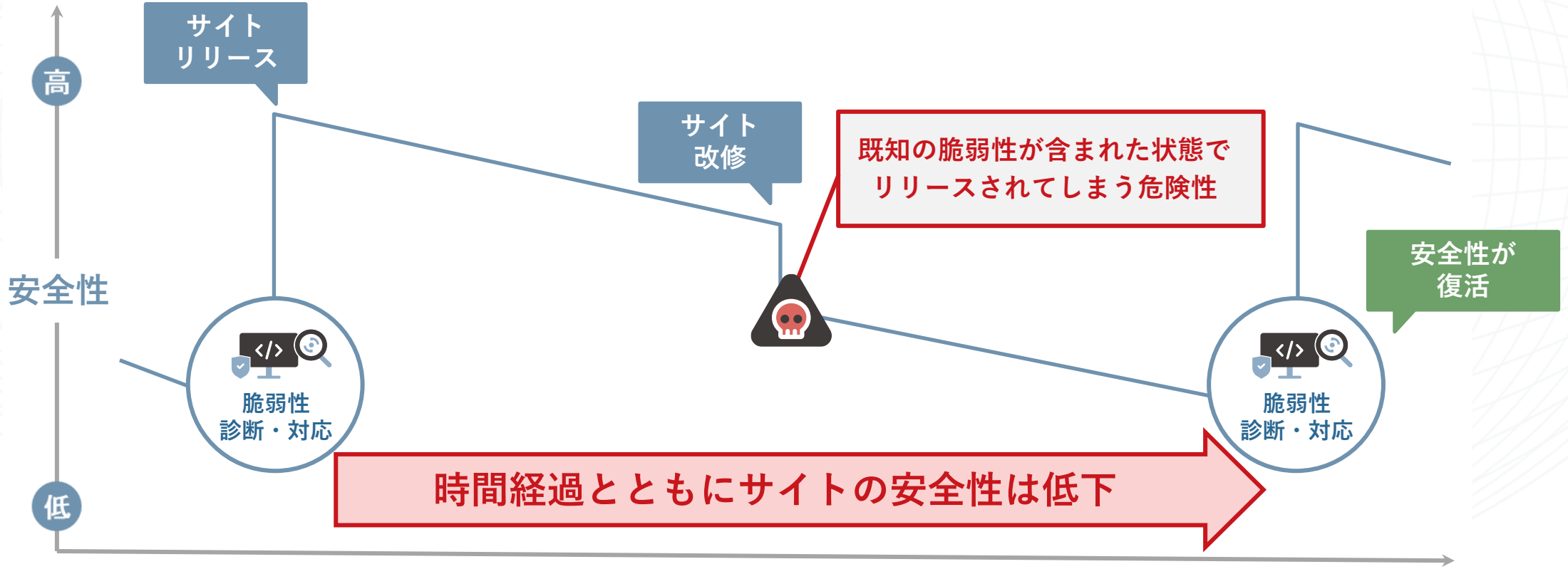
「脆弱性対策は後回し」という判断は、企業の存続に関わる重大リスク。
脆弱性診断は、これら数千万円規模のリスクを回避するために
極めて投資対効果の高い対策と言えます。

参考：「インシデント損害額調査レポート 別紙『被害組織調査』第2版（2024年）https://www.jnsa.org/result/incidentdamage/202402.html

「年1回の診断」はもはや機能しない。
現代の攻撃スピードに追いつくには

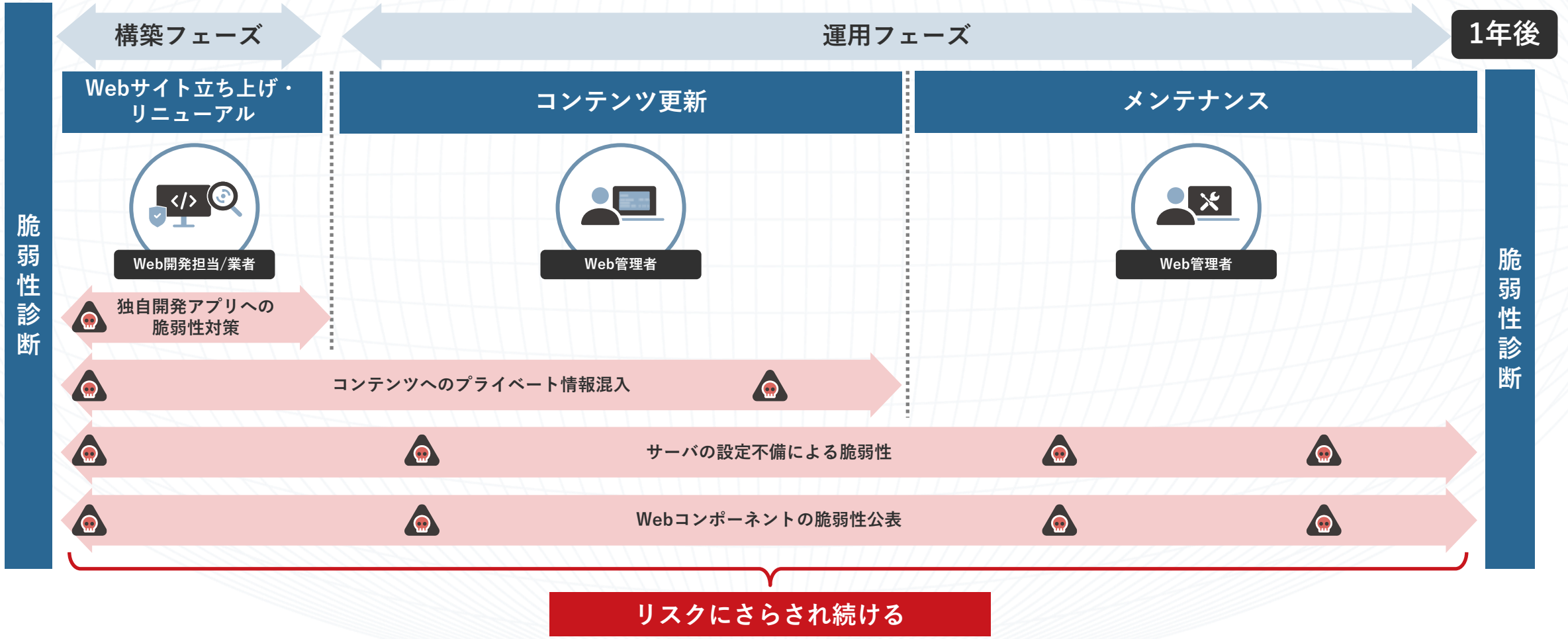
Webサイトリリース時の安全は維持されない

サイト改修時に安全性の下げ幅が大きく、何もしないとそのまま低下し続けてしまいます。



年1回の脆弱性診断では追いつかない

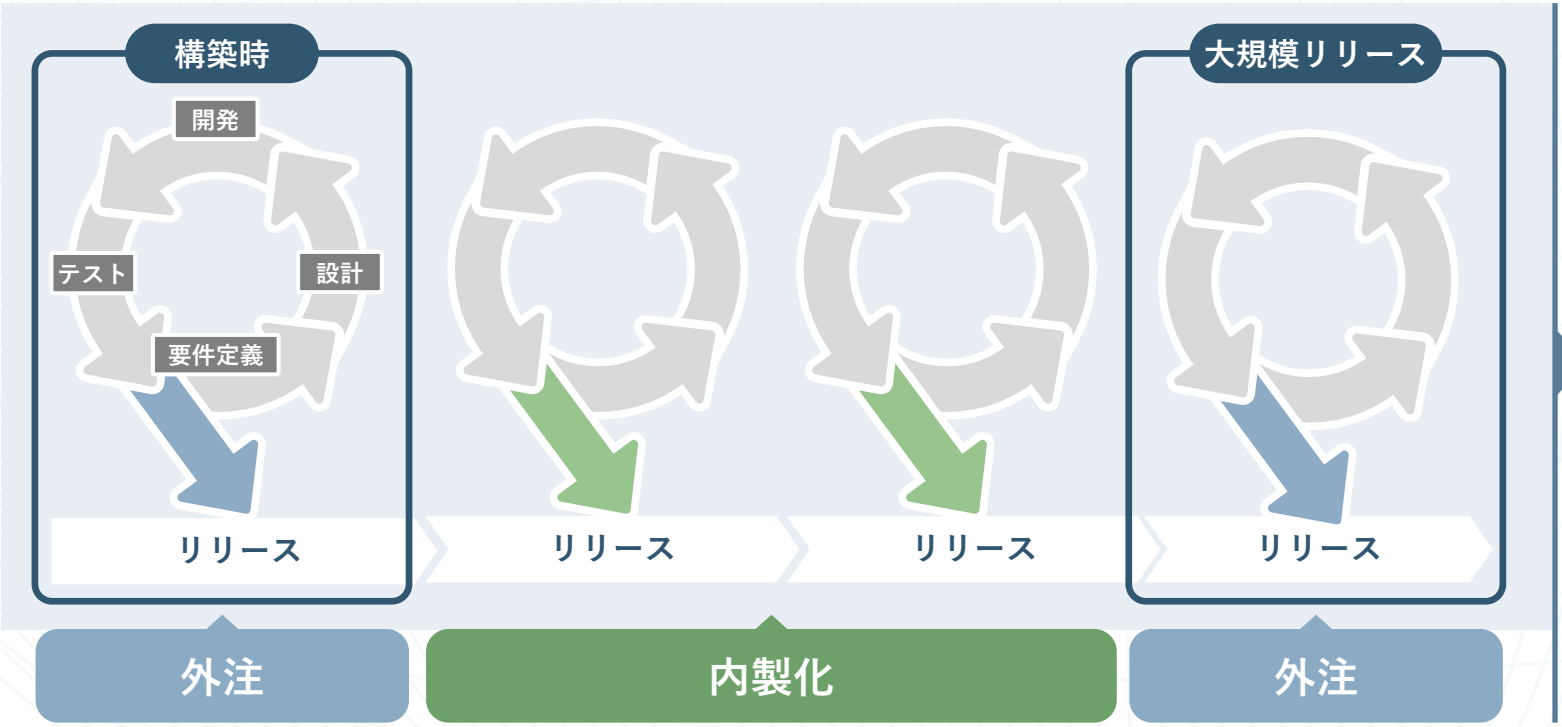
脆弱性は新しく生まれ続けているため、次回診断までリスクに晒され続けることに。



AeyeSecurityLab

今、「外部委託」と「内製化」を使い分ける企業が増えている

外注と内製を使い分けることで、費用と時間を削減しつつ、定期的な診断サイクルを実現できます。



大規模リリースは
外部に任せ、日々の
小さな更新は社内で。

状況に応じた柔軟な
診断体制で、継続的な
脆弱性対策を実現。

リリース頻度が高まる中、継続的な脆弱性診断を実施し、
新たな攻撃に対して「常に」備えておくことが不可欠です。

なぜAeyeScanが
継続的な脆弱性診断に有効なのか

AeyeSecurityLab

時間・工数の圧倒的削減とROIを実現

従来の脆弱性診断（外部ベンダによる手動診断）

ベンダ選定	見積・契約	手動診断	レポート作成	脆弱性対応
30日		7日	3日	

約40日

AeyeScanによる自動診断

診断設定	自動診断 自動レポート	脆弱性対応
10分	2日	

時間・工数の圧倒的削減！

約2日

出荷前診断の工数75%削減、約3割のコスト削減を実現した企業例も

セキュアな体制の確立とガバナンス強化を実現

セキュリティリスクの可視化

自動的に診断が実施され、
結果が共有される

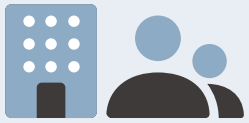
最新の脆弱性に対応

新たな脆弱性の情報を
随時反映

AeyeScan
による内製化

セキュリティ
ガバナンス強化

他部門やグループ企業にも
対応を拡大



セキュアな
開発サイクルの実現

リリースの度に診断を実施

AeyeSecurityLab

内製化を成功に導く手厚いサポート体制

貴社に合わせた柔軟なメニューをご提供し、内製化が軌道に乗るまでサポート。
持続可能な体制が迅速に整います。

脆弱性診断に特化した業務フロー作成支援

提供内容の一例

- 診断～修正までの貴社体制図
- 体制図に則した実業務フロー図
- 脆弱性診断関連の必要タスク

成功事例

- 持続可能なリスク低減体制を構築
- コミュニケーションコストの削減

脆弱性診断のルール作成支援

提供内容の一例

- 診断範囲の選定基準
- 診断タイミング / 頻度の目安
- 検出された脆弱性の対応指標

成功事例

- ガバナンスの強化
- Webセキュリティレベルの向上
- 情報安全意識の底上げ

脆弱性診断のスケジュール作成支援

提供内容の一例

- ツール診断計画の妥当性評価
- 全ドメイン毎の優先順位付け

成功事例

- 年次定期診断の実現
- 診断範囲、頻度の拡充
- 脆弱性診断マネジメントの実現

※ Businessプランご契約のお客様向けの内容です。※ 現時点の最新情報です。今後変更となる可能性がありますのでご了承ください。

AeyeSecurityLab

AeyeScanのポイント

専門知識・トレーニング不要で導入できる

1

最短10分で診断開始

専門知識は不要！
SaaS環境なので24時間放置しておけます。

お客様

1 スキャン登録

3 結果レポート

AeyeScan

2 自動診断

Webサイト

3

診断結果レポートも自動生成

開発担当にすぐ渡せるレポートが簡単に出力できます。

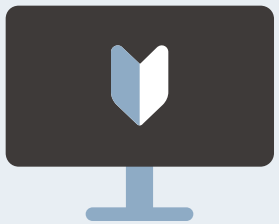
2

画面遷移図を自動作成

AeyeScanがサイトを自動巡回、診断すべき画面を抽出して画面遷移図を生成します！

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

全社で推進するための高度なマネジメント機能も搭載

オプション

運用は楽に、セキュリティは強く。ルールが自然に機能する脆弱性対策を実現します。

Webアプリケーション脆弱性診断ツール

AeyeScan

×

セキュリティマネジメントプラットフォーム

AeyeCopilot

脆弱性管理プロセスをシステムで自動化・仕組み化

- 診断対象となる自社資産の把握

部門間の連携強化

診断プロセス効率化

- 各種レポート生成
- 全体進捗の可視化

- 診断要否・優先順位の判断

脆弱性管理の実現

診断の運用標準化

- 判断に基づく診断の実施
- 修正状況の把握／支援

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
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（2023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

人材・教育

HSAWA EDUCATION GROUP　河合塾　Junion　JINSOKEN　ZENKIGEN　Direct Sourcing　PERSOL　立教大学　Leverages　workport

インフラ

EPARK　AIRE　H.I.S　H.O RETAILING　NTT EAST　odakyu　近鉄情報システム株式会社　G-GEO　SymEnergy　水ing Swing Corporation　Suzuyo　NANKAI　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　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!　BookLive

SaaS

Advanced Media, Inc.　Lexica E-Retailing Platform　エニアンドエムマッド株式会社　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　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　Human Interactive Technology Inc.　FUJISOFT　FUJITSU　MACROMILL　MITSUBISHI ELECTRIC　YONA　リピスト

セキュリティ企業

NEC NECセキュリティ　NTT DATA　GSX　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

まずは「現状把握」から 始めましょう

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） 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	
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。