サプライチェーンリスク拡大中！

それでも脆弱性対策が進まない3つの理由と解決法

AeyeSecurityLab

本資料の目的

企業・業種の垣根を超えたシステム・サービスの連携や、サプライチェーンの複雑化が進む昨今。

経済産業省から「サプライチェーン対策評価制度の基本構想(案)」が示されていることからもわかるように、
中小企業を含めたサプライチェーン全体のセキュリティ強化が急務となっています。

どの企業にとってもセキュリティ強化は緊急かつ重要な問題となっている中、

「具体的にどのような対策をすればよいか分からない」

「セキュリティ対策項目が増え、難易度が上がっている中での対策が困難」

「特に脆弱性診断は専門的な知識が必要なうえ、定期的な実施も必要でコスト・工数がかかる」

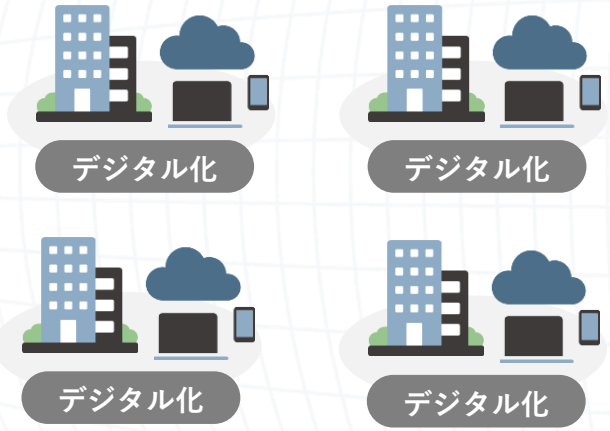
といった課題をお持ちの企業も多いのではないでしょうか。

本資料はそれらの課題に対する解決策をご紹介しますので、ぜひご一読ください。

AeyeSecurityLab

DXの進展に伴い、サプライチェーンリスクが拡大

DX初期は自社のセキュリティ対策に重点をおけば大きなリスクにならなかったことも、
企業間連携が進むと脆弱性がサプライチェーン全体のリスクになることがあります。



DX初期：社内業務のデジタル化

セキュリティ対策が不十分な
「即席デジタル」の乱立

DX中期：企業間連携のデジタル化

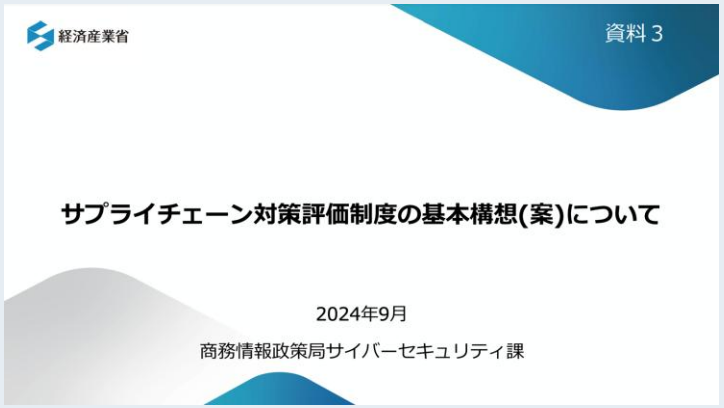
「即席デジタル」との連携で
サプライチェーン全体が脆弱化

サプライチェーン対策評価制度の基本構想(案)

企業の対策状況を可視化し、サプライチェーン全体のセキュリティ対策の強化が図れるよう、
経済産業省より「サプライチェーン対策評価制度の基本構想(案)」がまとめられました。

制度の目的

- サプライチェーン企業、ひいてはサプライチェーン全体の強靭性(事業継続性に加えてデータ保護を含む)の確保
- 対策要求の共通化を通じたサプライチェーン対策の重複排除、対策状況の可視化による確認の効率化



セキュリティ対策
を
３段階で評価

取引先の
セキュリティ対策
レベルを可視化

自社の
セキュリティ対策
水準と目標を
明確化

中小企業を含めたサプライチェーン全体のセキュリティ対策底上げが急務とされている

参考：サプライチェーン対策評価制度の基本構想(案)について

セキュリティ対策を全部やりきるのは難しい

セキュリティ対策項目は増え、難易度も上昇し、より深い技術知見が必要

Webアプリケーションのセキュリティ対策

① ファイルの公開設定
② Webページの公開設定
③ 脆弱性への対策
④ ソフトウェアの脆弱性対策
⑤ エラーメッセージの設定
⑥ ログ管理
⑦ 暗号化
⑧ 不正ログインへの対策

Webサーバのセキュリティ対策

⑨バージョンアップを行う
⑩ 不要なサービス・アプリケーションの停止
⑪ 不要なアカウントの削除
⑫ 安全なパスワードの設定
⑬ アクセス制御
⑭ ログ管理

ネットワークのセキュリティ対策

⑮ 不要な通信の遮断
⑯ 通信のフィルタリング
⑰ 不正な通信の検知・遮断
⑱ ログ管理

その他のセキュリティ対策

⑲ クラウドサービスへのセキュリティ対策
⑳ Webアプリケーション・Webサーバ・ネットワークへの定期的な脆弱性診断

引用元：安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～

セキュリティ対策の中でも、脆弱性対策は課題が山積み

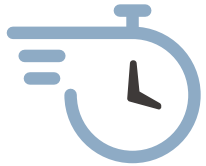
脆弱性対策が進まない3つの理由

専門知識と技術の不足

社内に専門家が不足していることから効果的な対策ができず、リスクを見落とす可能性も

予算や対応する人材不足

脆弱性対策は定期的な実施が求められるものの、リソース不足から十分な頻度で実施できない



事業スピードに追いつかない

デジタルサービスそのものの増加・リリースサイクルの高速化により、対策が追いつかない

脆弱性診断の「自動化」が課題解決に欠かせない

課題が山積みの脆弱性対策。中でも脆弱性診断(セキュリティ診断)は…

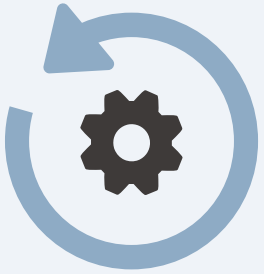
継続的・永続的に対策が必要	⟷	人力では**生産性が上がらない**
網羅的に診断することが望ましい	⟷	網羅性を高めると**費用も増える**

ツールを使って自動化・内製化ができれば

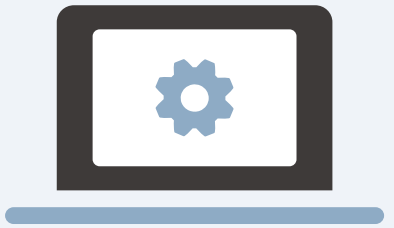
業務の効率化・費用の最適化につながりやすい

脆弱性診断の自動化・内製化に必要な要素とは？

脆弱性診断のプロセスに事業部門を巻き込む



AIを活用した脆弱性診断ツールの導入



脆弱性診断の自動化・内製化に必要な要素とは①

脆弱性診断のプロセスに事業部門を巻き込む

事業部門とセキュリティ部門で
一緒に脆弱性診断を行うことのメリットを訴求

シフトレフト

早期に脆弱性を発見することで
開発終盤での手戻りを最小化できる

診断の精度・網羅性UP

業務やサービス仕様に詳しいチームが
診断に参加することで
診断の精度・網羅性が上がりやすい

脆弱性診断の自動化・内製化に必要な要素とは②

脆弱性診断ツールの導入

事業部門を巻き込む前提で考えた場合、ツール選定に必要なポイントは…

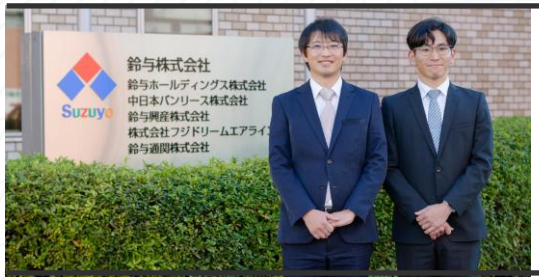
1. 誰でも使える操作性
2. 利用範囲に制限がない
3. 結果がわかりやすい

AIを活用した脆弱性診断ツール

AeyeScanをご紹介させてください！

導入事例紹介

鈴与 様



企業名	鈴与株式会社
事業内容	総合物流事業
従業員数	1,146人（2024年8月31日時点）

課題

外部ベンダーに診断を依頼していたが、
対象となるWebシステムが増えるほど
コストと時間がボトルネックに

具体的な課題

1. 社外向けWebシステムの開発が増え、診断にかかるコストが膨らんでいた
2. 外部ベンダーに依頼すると、見積もりや契約だけで1か月かかるなど、時間を要してしまう
3. コスト・時間の制約から頻度高く診断を行うことができない

これまで社内向け業務システムの開発が中心だったが、物流データを活用した新たな価値提供を推進するため、社外向けWebシステムを積極的に開発する方針へ転換。しかし、診断にかかるコストと時間がボトルネックになっていた。

導入

セキュリティ専門家でなくても扱える上、
外部ベンダーの診断と同等の品質も評価

導入の背景

1. 診断開始までの工数が少なく、UI含めて誰でも使いやすい
2. OWASPなど業界標準の脆弱性をカバーしており、外注と同等の診断ができる
3. 専門家でなくても、レポートを見れば問題点と必要な対策が理解できる

診断の内製化にあたり、複数ツールをトライアル導入して比較検討。セキュリティの専門家でなくても扱えることや診断品質、レポートのわかりやすさや、画面遷移図で巡回が抜け漏れなく行われているか見えることなどが決め手となり導入。

効果

約3割の診断コスト削減を実現。
診断頻度も増やすことができ、
セキュリティレベルがアップ。

具体的な効果

1. シナリオ作成も1日かからず終えられ、1週間以内には診断開始まで実行できる
2. コスト・時間が削減できただけでなく、開発サイドのセキュリティ意識も向上
3. 従量課金ではないので、今後診断対象の増加に伴いコストメリットも増えると実感

以前までは診断開始までに長いと1か月ほど時間を要していたが、コストを削減しながらスピード感のある診断が実現できるようになった。緊急度の高い脆弱性が見つかった際にはすぐ改修を依頼できるなど、セキュリティレベルの向上につながっている。

導入事例紹介

ミズノ 様

企業名　ミズノ株式会社

事業内容　スポーツ用品の開発・販売ほか

従業員数　3,584人（2024年3月31日現在）

課題

国内だけでも約20 Webサイトを運営する中、
定期的な脆弱性診断ができていなかった

具体的な課題

1. サイト立ち上げ時や大規模改修時だけしか診断ができていない
2. 外部ベンダーによる脆弱性診断だと多額のコストがかかる
3. 内部の人材のスキル不足・業務負荷が高くなる

グローバル全体でセキュリティポリシーを見直し、その中に定期的な脆弱性対策を含めたものの、外部ベンダーによる脆弱性診断だとコストがかかる。内製化を検討するもスキル不足や業務過多といった課題があることから、自分たちでも使える診断ツールの導入を検討。

導入

定額で複数サイトに外部ベンダーによる
脆弱性診断と変わらないクオリティの診断が
できると評価

導入の背景

1. 専門知識を持たなくても簡単に操作できる
2. サイト数に比例して費用が増加しない
3. 外部ベンダーによる脆弱性診断と同等の品質で診断できる

AeyeScanのトライアルを行い、簡単に操作できることを実感。また、同一サイトに対して、外部ベンダーによる脆弱性診断による診断とAeyeScanによるスキャンを並行して行いレポートを比較。AeyeScanの方が同レベル以上・検知項目が多かったことから、導入を決めた。

効果

定期的な診断が可能な体制が整った。
時間短縮により、
診断後の対策、チェックもスムーズに

具体的な効果

1. 内製化により、診断にかかる時間が数ヶ月単位から数週間に短縮
2. 診断、対策、チェックの運用がきれいに回せている
3. 開発ベンダーとのコミュニケーションもスムーズになった

外部ベンダーによる脆弱性診断では脆弱性への対応も含めて数ヶ月単位の時間がかかっていたが、数週間で診断を終えてすばやく対策できるようになった。レポートに具体的な修正方針も示されるため、開発ベンダーとのコミュニケーションもとれ、対策もスムーズになった。

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「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）

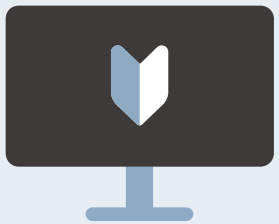
プロが認める品質・精度 ＋ ブラウザ上での直感的な操作

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

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

そもそもAeyeScanとは？

AI・RPAの活用により、脆弱性診断を自動化するクラウド型Webアプリケーション診断ツール。
自動巡回に優れており、人手をかけずに診断が可能。

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！

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

AISIN
KOSÉ
SAKI
TIGER
TEIJIN
Mizuno
ユーグレナ

インフラ

HIS
H.O RETAILING
odakyu
近鉄情報システム株式会社
水ing Swing Corporation
Suzuyo
NTT東日本
HITOWA GROUP
grow up together MEDIA
Looop

金融

アイフル
JOBPAY
SOMPOひまわり生命
DMM FinTech
Tokyo Century

メディア

集英社
中日新聞
NIKKEI

人材・教育

Junion
JINSOKEN
Schoo
ZENKIGEN
Direct Sourcing
PERSOL
Leverages

エンタメ

イープラス
CAPCOM
とらラボ!

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア
estie
M-aid
エムティーアイ
OZ INTERNATIONAL
COACH A Co.,Ltd.
cybozu
Speee
SecureNavi
TAL
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
Finovo
freee
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.
SB Technology
SBWorks
NTT AT
NTT DATA
NTTビジネスソリューションズ
OMRON
Globalway
circlace
さくら情報システム
CEC
GA TECHNOLOGIES
tdi 情報技術開発株式会社
Simplex Inc.
777WORKS 株式会社スリーセブンワークス
SOFT CREATE
SOLTEC
高千穂交易株式会社
電通総研
TOPPAN
JOPS
NHC
Human Interactive Technology Inc.
FUJISOFT
FUJITSU
MACROMILL
三菱電機インフォメーションネットワーク株式会社
YONA
リピスト

セキュリティ企業

NEC NECセキュリティ
NTT DATA NTTデータ先端技術株式会社
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

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	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） 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		
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

セキュリティに、確かな答えを。