セキュリティ担当者のための

事業部門と進めるDXの教科書

― AIで人材不足を解消しよう ―

AeyeSecurityLab

本書の目的

昨今DXの推進は、多くの組織において取り組むべき重要課題とされています。

日本企業のDXが進まなかった場合、2025年以降には
最大年間12兆円の経済損失が生じる可能性があるとの報告もあり、
「2025年の崖」ともいわれています。

その一方で、DX推進に伴い「クラウド活用」が加速する中、
いかにスピード感を持ってセキュリティ対策に取り組んでいくかも
課題のひとつではないでしょうか。

本資料では、経営者やDXを推進する担当者に向けて、
DXとセキュリティを両輪で進める秘訣をまとめました。

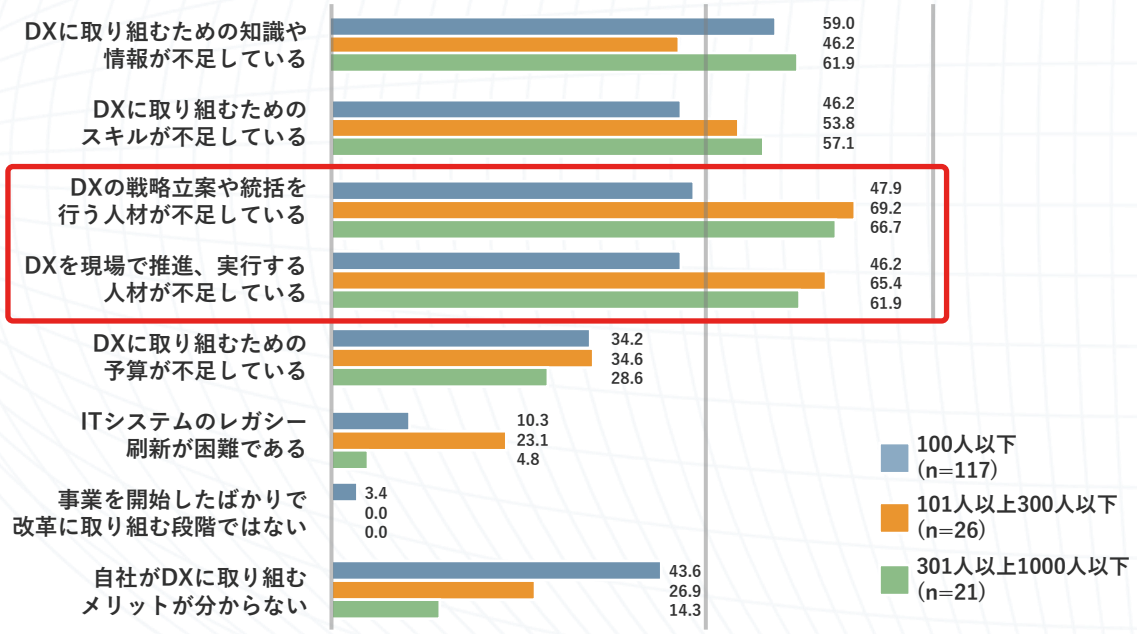
DX推進とセキュリティ対策の両立にお悩みの方は、ぜひご一読ください。

AeyeSecurityLab

DXを取り巻く状況

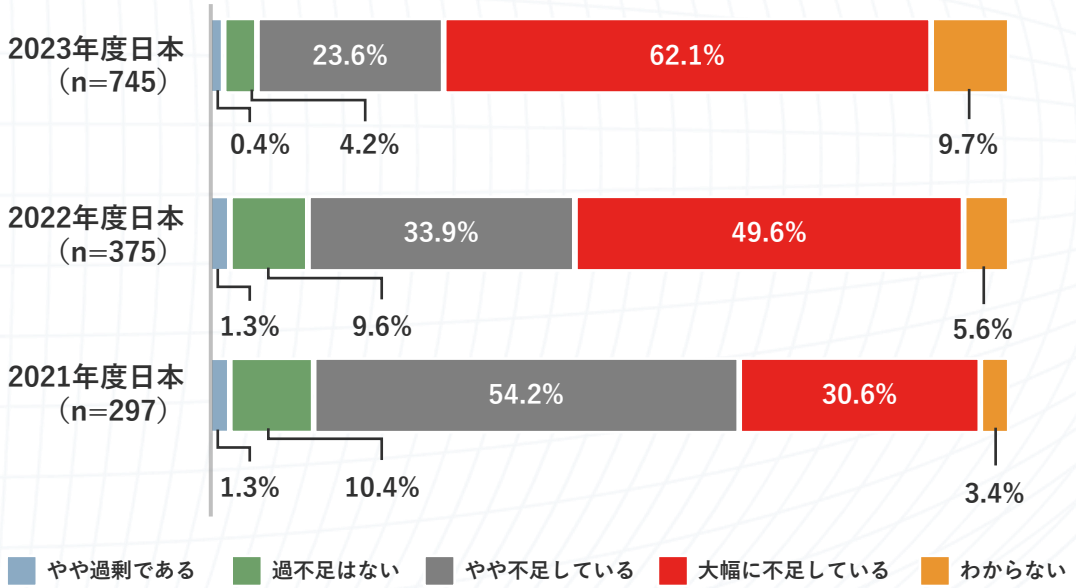
❶ DX人材の不足

日本のDXが遅れているのは、ナレッジやIT予算、取り組みに対する理解不足だけではない。
IPAの調査によると、多くの企業がDX人材の不足を感じている状況が明らかになっている。



【DXに取り組まない理由】

多くの企業が人材不足と回答



【DXを推進する人材の「量」の確保】

85%以上の企業がDX人材を確保できていない

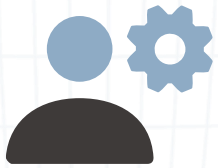
出展：DX 動向 2024 - 深刻化する DX を推進する人材不足と課題 https://www.ipa.go.jp/digital/chousa/discussion-paper/f55m8k00000039kf-att/dx-talent-shortage.pdf

DXを取り巻く状況

❷ 内製によるシステム開発の増加

IPAによる「DX白書動向2024」では、 DX 推進に必要な要素として以下が挙げられている。
これらを実現する手段として、生成AIの利活用やシステム開発の内製化などが推し進められつつある。

ビジネス環境の変化に 迅速に対応できる **ITシステムの整備**	競争領域を 強化するための **社内外システムの連携**	ビジネス上の ニーズに合致する **データ活用と分析**



DX推進に伴い、誰でもサービスを作れるツールも増加している

参考：IPA「DX動向2024： https://www.ipa.go.jp/digital/chousa/dx-trend/eid2eo0000002cs5-att/dx-trend-2024.pdf 」

DXを取り巻く状況

❸ 内製化傾向がさらに強まる

IPAが、事業戦略や IT システムに適用しているソーシング手段を調査した結果によると、あらゆるシステムにおいて**「内製による自社開発」**が増加傾向となっており、アジリティ（機敏性）を重視するシステム・低コストであることを重視して導入するシステムにおいては、その傾向が顕著に表れている。

2022年度と2023年度の比較

アジリティ(機敏性)を重視するシステム			低コストであることを重視して導入するシステム		
2022年度	→	2023年度	2022年度	→	2023年度
12.1%		23.0%	13.5%		23.5%

システム開発を内製化しやすい環境が整っている一方で、
セキュリティをどう担保するかも課題になりやすい。

参考：IPA「DX動向2024： https://www.ipa.go.jp/digital/chousa/dx-trend/eid2eo0000002cs5-att/dx-trend-2024.pdf」

至上命題となったDXを支えるセキュリティ

DXに伴い、セキュリティ対策の実施対象は拡大しており、難易度も増している。

DX		セキュリティ
デジタルサービスの開発・提供 自社で管理すべきデジタル資産 × 急速な技術の進化	増 =	必要なセキュリティ対策の **対応範囲も広く…** **難易度も高く…**

DXとセキュリティは**両輪**で進める必要があるものの、そこには**課題**も…

DX推進に伴う課題

❶ 時間・予算・人材の不足

予算が潤沢なコア事業と比べると、新規サービスはセキュリティ対策が不十分な傾向にある。脆弱性診断を行う予算が足りなかったり、スケジュールが調整できないなど、事業スピードとの両立が難しいことがその理由。

コア事業

万全の
セキュリティ

主要
サービス

ノンコア事業

新
サービス

新
サービス

新
サービス

ベンダーのスケジュールが
リリースまでにおさえられない

予算が潤沢ではないため
**セキュリティ対策にコストを
かけられない**

セキュリティ部門の
人手が足りない

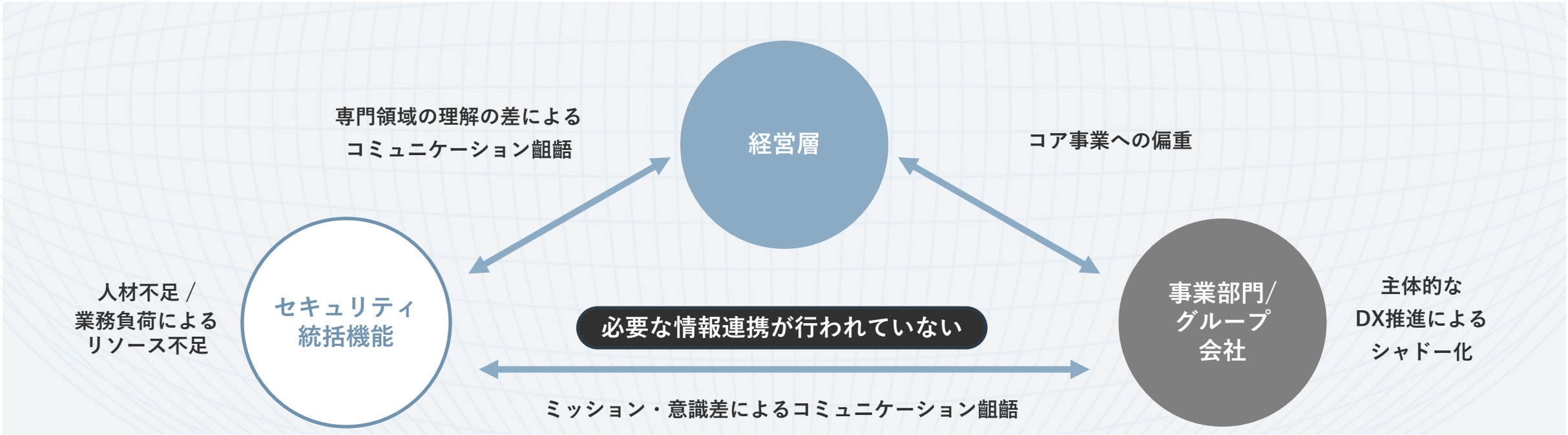
セキュリティを確保しつつ事業展開

DX推進のスピードを優先し**セキュリティが後まわし**に

DX推進に伴う課題

❷ コミュニケーション不足

DXによってセキュリティ対策の対象が増え続ける中、組織全体でセキュリティガバナンスを効かせるために部門や役割を超えたコミュニケーションが求められる。セキュリティ人材が果たすべき役割は増える一方。



セキュリティガバナンス強化に向けリソースを効率良く配分する必要がある

DXとセキュリティを両輪で進めるために必要な「AI活用」

人手やコスト・時間が限られる中でセキュリティを担保するためには、対応に濃淡をつけつつ、
リソースを効率良く配分する方法を考える必要がある。その方法のひとつが、AI活用といえる。

手間と時間をかけて
専門家が対応する

濃 ⟷ 淡

人的リソースを最小化
しつつ対応する

専門人材は限られているが、技術的に
人間が対応しなければいけない範囲が広い

継続的・網羅的に対応する必要があるが、
割ける人的・金銭的リソースは限定的

AIを活用した「自動化」も必要

今後、より重視される「デジタルサービス」のセキュリティ対策

中でも、DXに伴い今後も増加が見込まれるデジタルサービスへのセキュリティ対策は、運営する部門が多岐に渡り管理も難しいことから、AIを積極的に活用しながら優先度を上げていくべき。

業務のデジタル化

▼

社内IT資産 増

今までセキュリティ部門が管理していたので

攻撃面を把握しやすい

DX

AI活用がおすすめ

デジタルサービスの増加

▼

Web接点 増

事業部が独自に構築・運用するので

攻撃面を把握しにくい

AeyeSecurityLab

デジタルサービスのセキュリティ対策において重要な「脆弱性診断」

Webサイトのセキュリティ対策は、IPA「安全なウェブサイトの運用管理に向けての20ヶ条」の参照がお勧め。

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

※ ⑥⑦⑭⑱以外の全てを脆弱性診断で問題発見が可能。

脆弱性診断を実施することで、Webサイトに潜む脆弱性を発見・改修することはもちろん、20ヶ条のほとんどの問題を発見できる。

参考：IPA「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～」：https://www.ipa.go.jp/security/vuln/websecurity/sitecheck.html

AI活用と相性のよい、デジタルサービス領域の脆弱性診断

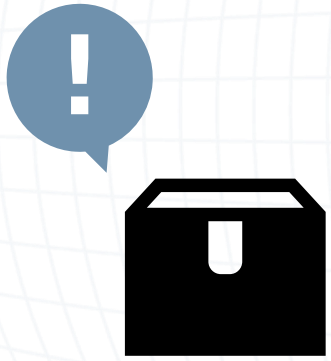
Webサイトを狙うサイバー攻撃が増加する中、日々新たな脆弱性が明らかになっており、対策もアップデートし続けなければならない。

継続的・永続的に対策が必要となる	人間が対応していると継続的・永続的に工数を取られて生産性が上がらない
自社Webサイト・Webサービスを網羅的に診断することが望ましい	Webサイト・Webサービスが増える度に、必要な費用も増えてしまう

AIによる自動化・内製化ができれば、
業務の効率化・費用の最適化に**つながりやすいと言える**

脆弱性診断の自動化・内製化に必要な要素とは？

AIを活用した脆弱性診断ツールの導入



加えて、事業部が独自に構築・運用した
Webサイトの攻撃面を把握できる機能があると、
ブラックボックス化を防げる。

情報集約・管理が円滑になることで
戦略策定や人材育成などの業務に人手を割ける

AIを活用した脆弱性診断ツールの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

結果が初心者でも分かる

専門知識がなくても診断できるツールを選ぶことで、
事業部門を巻き込んだ脆弱性対策も可能になる。

開発終盤での手戻りを最小化できる

診断の精度/網羅性が上がりやすい

まとめ

DXとセキュリティを両輪で進めるために、

AIに任せられる業務は任せて
人手不足を解消しよう！

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「2023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）2022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）

有償契約 200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

導入事例紹介

SOMPOひまわり
生命保険 様

企業名	SOMPOひまわり生命保険株式会社
事業内容	国内生保事業
従業員数	2,650人（2023年度末時点）

課題

外注だと手間と時間がかかり、
2週間の開発サイクルに合わせた診断が困難

具体的な課題

1. アジャイル開発のため外部委託だと契約や調整の手間、時間がかかる
2. 開発の早い段階で脆弱性対策をする「シフトレフト」を目指したい
3. 家族情報や病歴などを含む個人情報を扱うため、セキュリティ意識の底上げが必要

「健康応援企業」を目指し、アジャイル開発によりアプリ・サービスをスピーディーに提供する中、脆弱性対策が課題になっていた。外部診断ではコストや時間がかかる一方、人材育成も非現実的なため、診断ツール導入を検討することになった。

導入

他社ツールと比較検証した上で、
検知能力、操作性などを評価し選定

導入の背景

1. 他ツールと比較し、高い検知能力があると判断
2. 操作性がよく、開発チーム自ら診断できる
3. レポート内容がわかりやすい

最初にピックアップした11製品の中から、まずはDAST製品である3製品に絞ってPoCを実施。脆弱性のあるサイトを用意して検証した検知能力、操作性、機能・運用性、パフォーマンスの点でAeyeScanが優れていると判断し、導入を決定。

効果

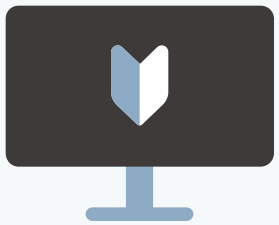
開発者が自分たちで手軽に診断できるようになり、ガイドや勉強会と組み合わせることで
シフトレフトの考え方も浸透

具体的な効果

1. 改修などのタイミングに合わせた、月に1本程度の診断が実現
2. ボタンを押すだけで手軽に診断できると、開発者側から感謝の声が上がっている
3. シフトレフトの考え方が理解され、開発者のセキュリティ意識が向上

AeyeScanの導入とともに開発者向けのガイドを作成し、開発プロセスに無理なく取り入れていった。コストや工数・時間といった課題が解決されたことに加え、開発者のセキュリティ意識も向上。グループ会社からも導入に興味を示されている。

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（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
200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

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
Mizuno
ユーグレナ

インフラ

HIS
H2O RETAILING
近鉄情報システム株式会社
Junion
水ing Swing Corporation
Suzuyo
NTT東日本
HITOWA GROUP
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

エンタメ

イープラス
CAPCOM
とらラボ!

SaaS

estie
M-aid
エムティーアイ
OZ INTERNATIONAL
COACH A Co., Ltd.
cybozu
JINSOKEN
Schoo
Speee
ZENKIGEN
Direct Sourcing
TAL
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
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
CTC
Insight Edge
Infcurion
80&Co.
SB Technology
SBWorks
NTT DATA
NTTビジネスソリューションズ
Globalway
circlace
さくら情報システム
CEC
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
電通総研
TOPPAN
JOPS
NHC 日本情報通信株式会社
Human Interactive Technology Inc.
FUJISOFT
FUJITSU
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） 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

セキュリティに、確かな答えを。