導入事例

厳しいセキュリティ基準への対応を求められる金融業が、脆弱性診断を内製化した理由

AeyeSecurityLab

はじめに

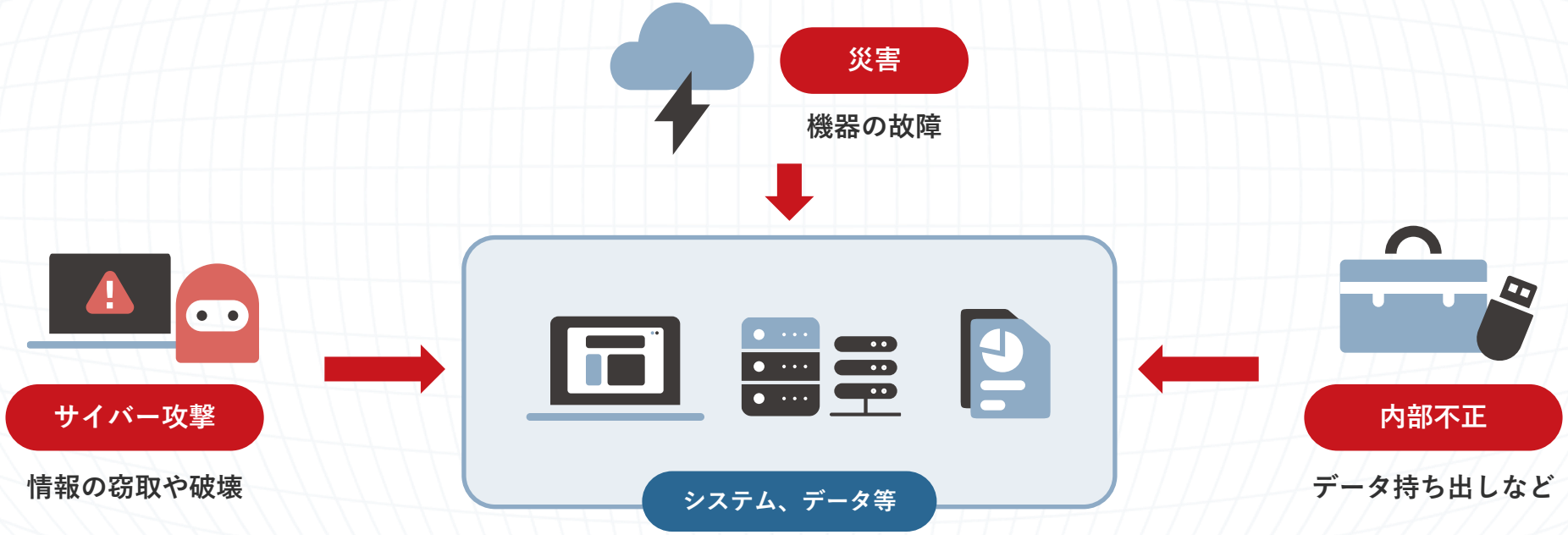
近年サイバー攻撃の手法が多様化し、被害件数も増加しています。
ひとたび攻撃を受けると、Webサービスの停止や情報漏洩はもちろん、
対応・調査にかかる費用の損失や信用失墜など、甚大な被害を被ることに。

特に資金移動を伴うシステムを取り扱う金融業のお客様は、
セキュリティを重視されているのではないでしょうか？

本資料では、あらためてセキュリティの基礎をおさらいした上で、
課題となりがちな**人手やコストなどのリソース不足**を解消すべく、
セキュリティ対策の効率化についてご紹介します。
ぜひ最後までご覧ください。

サイバーセキュリティとは

サイバーセキュリティとは、企業・組織が所持している情報やWebシステムをさまざまな脅威から守ることです。
ITを利活用する現代社会においてサイバー攻撃は身近な脅威であり、万一の事態に備えた適切な対策が必要です。

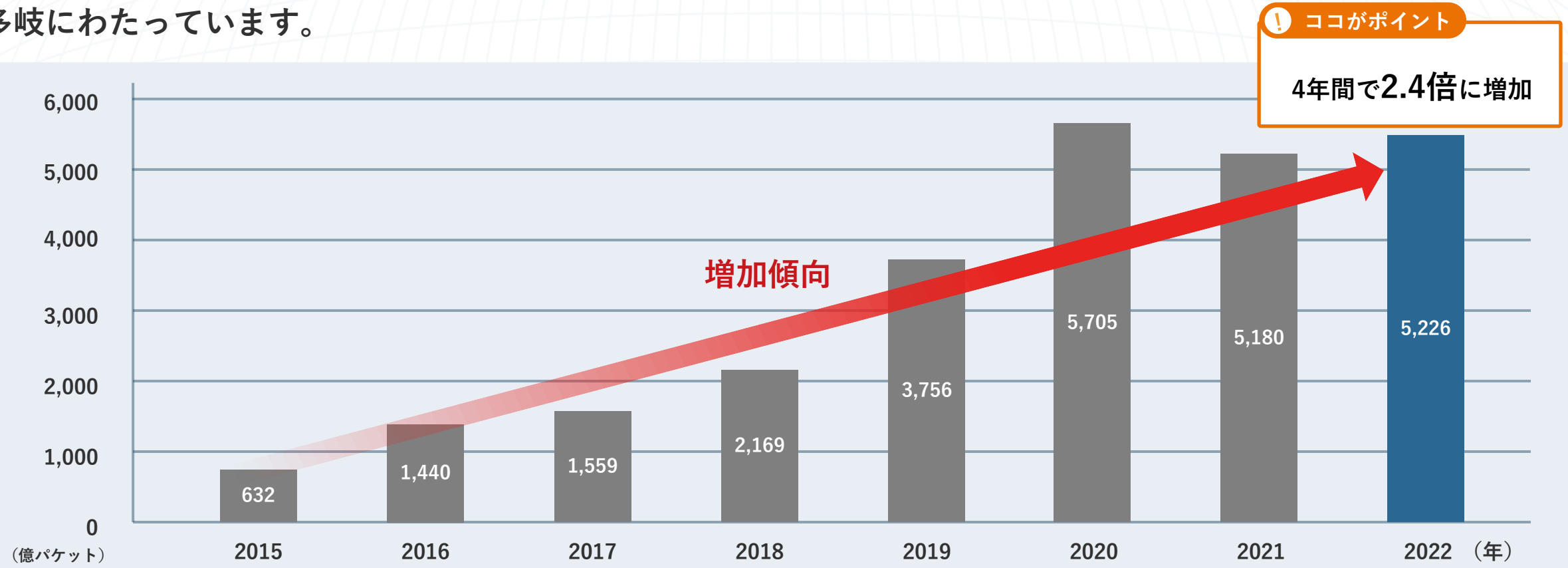


Check

攻撃を受けてしまった場合、情報漏えいによる信用の失墜、システム停止による経済的損失などの影響が考えられます。
保護対象や脅威となる原因ごとに対策を実施し、被害に遭うリスクを低減しましょう。

サイバー攻撃の推移

サイバー攻撃を観測・分析できるシステム「NICTER」によると、日本におけるサイバー攻撃は2018年度から2.4倍も増加。内容は、IoT機器を狙った通信が最多、「その他の通信」が占める割合も増えており、攻撃対象が多岐にわたっています。



出典　総務省｜令和5年度版 情報通信白書

情報セキュリティ脅威の動向

※2016年以降

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1位 →	ランサムウェアによる被害	2016年	9年連続9回目
2位 →	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3位 ↑	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4位 ↓	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5位 ↑	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6位 ↑	不注意による情報漏えい等の被害	2016年	6年連続7回目
7位 ↑	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8位 ↓	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9位 ↓	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10位 →	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

出典 IPA｜情報セキュリティ10大脅威2024

すべての脅威が2年連続でランクイン、対策は進むも手口が高度化・複雑化

サイバーセキュリティ経営ガイドラインの改訂

サイバー攻撃の多様化・巧妙化や、サプライチェーン全体を通じた推進の必要性の高まりなどを受け、経済産業省は2023年3月にサイバーセキュリティ経営ガイドラインを改訂。各項目の見直しや対策例の拡充などが行われました。

改訂ポイント

- 「攻撃の検知」に関する「サイバーセキュリティリスクに対応するための仕組みの構築」を追加
- 「復旧」に関する「サイバーセキュリティリスクに対応するための仕組みの構築」を追加
- 委託先におけるリスクマネーの確保や委託先の組織としての活用の把握等の留意点を追記
- インシデント発生時に組織として調査しておくべき事項をまとめた付録を追加　など

出典 サイバーセキュリティ経営ガイドライン

サイバーセキュリティを強化する5つの対策

以下の対策はすべて継続的な実施や運用が求められるため、ツールを使った自動化 / 効率化がおすすめです。

1 OS・ソフトウェアを最新状態に保つ

ツール活用可

OSやソフトウェアに存在する脆弱性を狙った攻撃を防ぐために、定期的にアップデートを行う。

2 安全なパスワードを使う

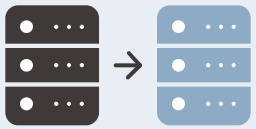
ツール活用可

意味を持たない長めのパスワードを設定することに加え、複数のサービスで使いまわさない。特にプライベートと仕事で使うパスワードを共通にしない。

3 データをバックアップする

ツール活用可

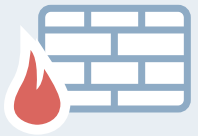
データが改ざん / 削除される被害を想定し、復旧できるようにしておく。



4 セキュリティ対策製品を導入する

ツール活用可

ファイアウォール、IPS / IDS、WAFなど、脅威を防げるソリューションを守備範囲に応じて導入する。



5 脆弱性診断を実施する

ツール活用可

サイバー攻撃の対象となる欠陥がないか検証し、設定の不備や脆弱性を早期に発見する。

ココがポイント

中でも、「5.脆弱性診断を実施する」は、インフラとして24時間365日安定稼働が求められる金融システムにとって重要な対策。
新たな脆弱性に対応するためにも、定期的な診断を継続していくことが必要です。

脆弱性診断の効率化はツールの選定がカギ

脆弱性診断の実施にあたり、金融業のお客様からは下記のような課題をお聞きしています。

金融業のお客様の声

CASE 1：外部のサービスに脆弱性診断を委託

- 1つのサイトを診断するのに数百万円単位のコストがかかる
- リニューアル時はスケジュールがギリギリで調整が大変
- 診断実施に至るまでの調整コストが膨らんでいる
- 自分たちの都合で実施したいが、知識・ノウハウがない

CASE 2：手動で脆弱性診断を実施しながらも、一部作業で診断ツールを利用

- 人手が必要な作業に多くの工数を取られる
- ツールの精度が悪いため、使いこなせず結局手作業
- エンジニアのリソースに限りがあるため診断だけに人やコストを割けない

ココがポイント

高精度な診断を人手をかけずに自動化できるツールの選定・導入が、
脆弱性診断効率化の成功ポイントです。

AeyeSecurityLab

脆弱性診断は「AeyeScan」にお任せください

クラウド型Webアプリケーション脆弱性診断ツール「AeyeScan」 なら、AIやRPAの活用により診断工程を大幅に自動化。
セキュリティに厳しい金融業のお客様にも選ばれています。

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

導入事例紹介

アイフル 様

企業名　アイフル株式会社

事業内容　リテール金融サービス

従業員数　連結 2,470名／単体 1,229名(2024年3月31日現在)

課題

診断の外部委託ではコストがかさむ上
調整に手間がかかり
開発スタイルにそぐわなかった

具体的な課題

1. セキュリティの深い知識までは持っていない
2. 外注では全体で数百万単位のコストがかかる
3. 外注だと日程調整などに手間がかかる

高いセキュリティが求められるため診断を外部委託していたが、コストと手間がかかる状態だった。日程も融通がきかず、アジャイル方式の開発スタイルとは相性がよくなかった。

導入

レポートの分かりやすさ、
診断項目・精度、コストなど
総合的に見て導入を決定

導入の背景

1. エンジニアにとって分かりやすく、使い勝手がよい
2. スキャンが高精度で、どう修正すべきかも分かる
3. サポート体制がしっかりしている

エンジニアにとっての分かりやすさ、使いやすさを重視。画面遷移図が自動生成される点や、『問診票』が用意されていて事前の準備が容易な点も評価。

効果

コスト・工数削減を実現し、
スピーディな開発と
セキュリティの担保を両立

具体的な効果

1. 診断会社との調整の手間がなくなった
2. 好きなタイミングで何回でも診断が可能に
3. クライアントやユーザー部門にも安心材料を提示できる

スタートガイドを参照することで、予想以上にスムーズに導入できた。画面遷移で詰まるところが出てきた際も、サポートに連絡し、スピーディーに更新対応がなされたことが好印象。

導入事例紹介

JOBPAY 様

企業名　株式会社JOBPAY

事業内容　給与前払いサービス

課題

人手や予算が限られる中
いかに少ない工数で
高頻度の診断を実施するかを模索

具体的な課題

1. 診断サイクルが年1回にとどまっていた
2. 診断をより短いサイクルで回したい
3. エンジニアのリソースに限りがあった

資金移動を伴うサービスを提供している以上、セキュリティに関しても一層厳しく取り組む必要があると考えていた。年1回の診断では少なすぎると判断し、より短いサイクルで回すことを検討。

導入

エンジニアの作業工数がかからず、
問い合わせへの対応も迅速なことから選定

導入の背景

1. 1回診断を実施するたびに費用がかさまない
2. エンジニアのコストを減らせると判断
3. サポートの対応に安心感を抱いた

半自動ツールを用いた診断内製化も検討したが、シナリオ作成や登録作業に多くの工数が取られることがネックに。AeyeScanのPoCを行い、診断サイクルを短くしていける手応えがつかめたことから導入を決定。

効果

API連携も駆使し、工数をかけずに
資金移動業者としてのセキュリティを確保

具体的な効果

1. 四半期に1回のペースで診断する体制を確立
2. APIを活用したSlack連携など、さらなる自動化を実現
3. やや複雑なログイン画面の巡回も自動化

以前の工数を100とすると、10以下かゼロくらいの工数削減を実感。レポートが日本語で誰が見ても分かりやすい点も高評価。万が一問題が発生した際の「証跡」としても活用できると考える。

導入事例紹介

マネーフォワード 様

企業名	株式会社マネーフォワード
事業内容	PFMサービスおよびクラウドサービスの開発・提供
従業員数	2,400名（2024年5月末日現在）

課題

事業が拡大しプロダクトが増えるにつれ、
脆弱性診断の間隔が空いてしまうことが
懸念材料だった

具体的な課題

1. 外注だとナレッジが蓄積されない
2. 外注だと画面数に応じた料金体系で網羅的な診断を受けづらい
3. 開発が遅れた場合、ベンダーとのスケジュール調整が困難

新機能の追加や大規模な改修の際には脆弱性診断を実施していたが、それ以外はプロダクト側の判断に委ねていた。小さな改修のたびに診断を外注するのではなく、内部で迅速に診断する選択肢も持ちたかった。

導入

診断ツールを導入し
継続できなかった経験から、
使いやすさを重視

導入の背景

1. 自動巡回のカバー率が高く、主要な脆弱性を確実に検出できる
2. グループ会社のプロダクトも診断できるライセンス体系
3. API診断が可能

外国籍エンジニアも多く在籍するため、英語にも対応していること、Slackをはじめとする外部サービスとの連携性も要件だった。複数のツールの比較検討を進め、いくつかのプロダクトを対象に検証を実施した上で選定。

効果

約60プロダクトに診断を実施できた
今後、最低年1回の診断を計画

具体的な効果

1. 画面遷移図により、CISO室がプロダクトの画面を把握できるように
2. 開発者のセキュリティ意識が高まった
3. グループ統一のセキュリティスタンダード適用にも活用予定

ほぼすべてのサービスを内製で開発する中、「セキュリティスペシャリストの活動をAeyeScanがサポートしてくれている」とCISOも評価。セキュリティエンジニア以外に、QAチームでも使用を開始している。

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 DRIVING SCHOOL / 河合塾 / Junion / JINSOKEN / ZENKIGEN / Direct Sourcing / PERSOL / Leverages / workport

インフラ

EPARK / AIRE / HIS / H.O RETAILING / NTT EAST / odakyu / 近鉄情報システム株式会社 / G-gO / SymEnergy / 水ing Swing Corporation / Suzuyo / NANKAI 南海システムソリューションズ / 日本調剤 / HITOWA GROUP / 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 株式会社キッツ / KOSÉ / SAKI / TIGER / TEIJIN / Denkei / House / Mizuno / ユーグレナ

エンタメ

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

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア / Lexica E-Retailing Platform / estie / エアアドエムマット株式会社 / 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 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 KDDI Agile Development Center / circlace / さくら情報システム / SUNDAY SYSTEMS / 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 / JAST / PCNET 株式会社パシフィックネット / 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

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

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	55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

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

セキュリティに、確かな答えを。