「伝わらない」から「巻き込む」へ

全社で進める

セキュリティ対策講座

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。

AeyeSecurityLab

AeyeSecurityLab

誰でも簡単に

プロさながらの高度な

脆弱性診断を

AeyeScan

「伝わらない」から「巻き込む」へ

全社で進める

セキュリティ対策講座

AeyeSecurityLab

質問受付中!!

DXの進展によって変わる
セキュリティ対策の「常識」

AeyeSecurityLab

質問受付中!!

IT部門が頑張る「今までのセキュリティ対策」が限界にきている

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

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

情シス・セキュリティ部門が主導するため
IT資産やセキュリティ対策をコントロールしやすい

**事業部門が主導するため
対策が難しい！**

AeyeSecurityLab

質問受付中!!

全社一丸でのセキュリティ対策が求められるが…

事業部門

セキュリティ…?
自分の仕事で精一杯

セキュリティ部門

セキュリティ対策を進めて
自社サービスを守らねば！

経営層

費用対効果あるの？
DXが優先じゃない？

事業部門からは理解が得られず、
経営層からは人員・予算を引き出せず…

AeyeSecurityLab

質問受付中!!

「巻き込む」ために、改めて考えたいこと

何のためにセキュリティをやるのか

AeyeSecurityLab

質問受付中!!

企業は、何のためにセキュリティに取り組むのか

ビジネス(Business)のため

ビジネスの観点で

- セキュリティリスクを想定・評価すること
- セキュリティ対策・運用を検討すること
- (投資)効果を測定し、改善すること

AeyeSecurityLab

質問受付中!!

ビジネス視点で会話する＝「共通言語」を持つことが大切

技術視点での会話

データベースに対して不正な操作を行う「SQLインジェクション」の脆弱性が検出されました。

ビジネス視点での会話

顧客情報が窃取・漏洩する可能性があり、顧客離反だけでなく数千万円単位の損害賠償請求につながる可能性があります。

AeyeSecurityLab

質問受付中!!

＼脆弱性診断で考えてみよう／

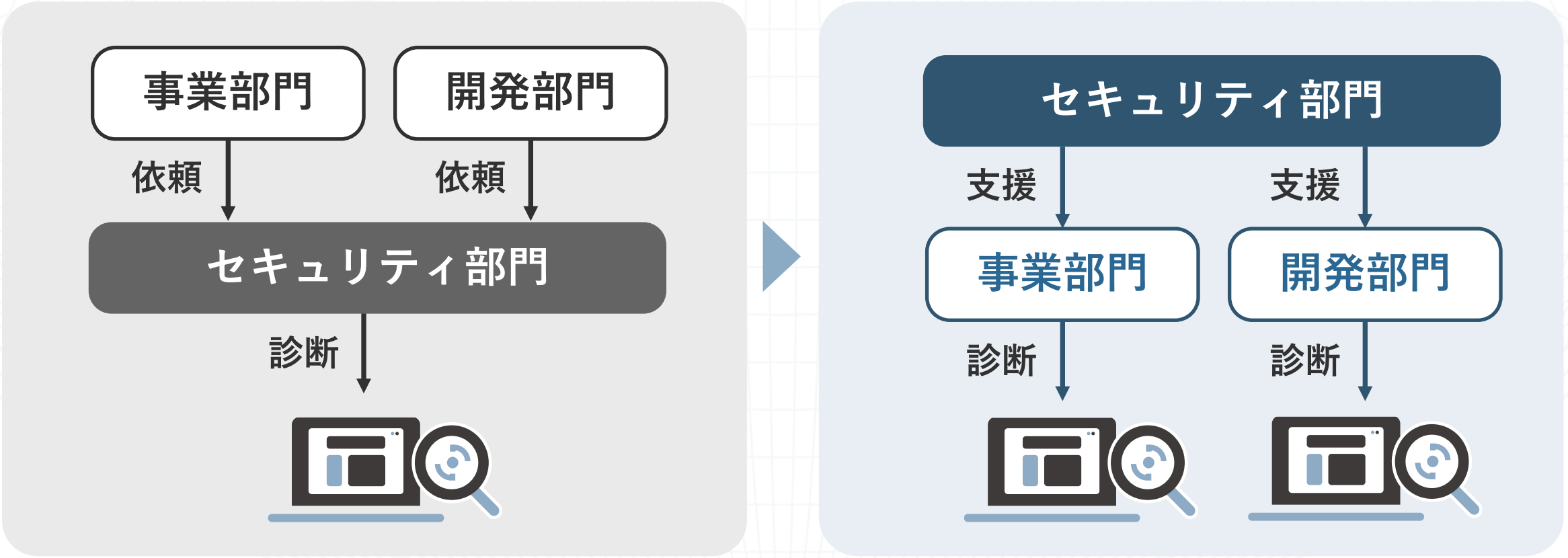
「全社で進める」セキュリティ対策

AeyeSecurityLab

質問受付中!!

「全社で進める」セキュリティ対策　① 体制検討

セキュリティ部門が一括請負する体制から、**事業部門が脆弱性診断を実施する体制へ**



AeyeSecurityLab

質問受付中!!

「全社で進める」セキュリティ対策　② 方針検討

スコープを明確にし、ビジネス上の優先順位・必要を評価して対策の濃淡をつけることが重要

診断対象の棚卸し

診断の必要性を評価

- 取り扱っている情報の重要度
- ビジネス上の重要度
- 監督官庁・業界団体のガイドライン
- リリース・アップデート頻度(開発体制)

対策方針の検討

診断方法

- 外部委託
- 社内診断(内製化)

診断タイミング

- 新規リリース
- 改修・追加開発
- 定期診断

AeyeSecurityLab

質問受付中!!

「全社で進める」セキュリティ対策　③ 情報連携

Webサイト・Webアプリを開発している部門との情報連携・協業が「ミソ」

診断計画を立てる

リリース前の診断

開発プロジェクトのキックオフ等に参加し、スケジュールを事前に確認しておく

定期診断

実施時期を各プロジェクトと事前に調整しておく

診断の実施準備をする

開発部門と情報連携し、診断要件を確認する

例

診断対象の基本情報

対象システム、対象 IP アドレス、対象 URL・診断用アカウント、保有するデータ 資産分類（個人情報、クレジットカード情報など）等

技術仕様に関する情報

システム仕様や構成図、フレームワーク、外部連携サービス 等

診断実施にあたっての確認事項

診断アクセスによるメール等の外部通知の有無 等

AeyeSecurityLab

質問受付中!!

「全社で進める」セキュリティ対策　④ 修正対応

評価の理由・根拠(特に“対応不要”とした場合)と、**対応履歴を残しておく**のが大事

診断結果の確認

修正対応の必要性を評価

- CVSS等の深刻度
- **発生しうる被害・リスクの大きさ**
- **修正にかかるコスト(工数・費用)**
- **リリースまでに残された時間**

など

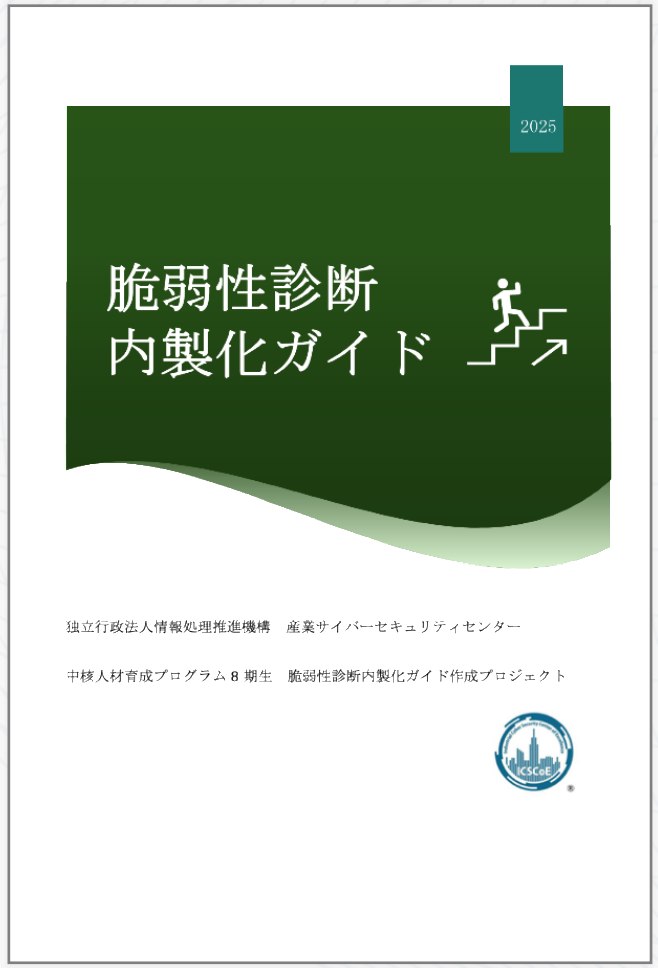
対策方針の検討

- リリース前に必ず修正する
- 次回リリースまでに必ず修正する
- 大規模修正で修正
- 現時点では対応不要

AeyeSecurityLab

質問受付中!!

IPA（独立行政法人情報処理推進機構）から脆弱性診断内製化ガイドが公開



公開の背景

脆弱性の早期発見がますます重要に

- 事業継続
- 信頼性維持の観点

内製化への関心が高まっている

- 新たな脆弱性の増加
- リリースサイクルの高速化

主な内容

- 外部発注と内製の違い
- 内製化に必要な組織体制と人材
- 内製化の進め方と継続的改善プロセス
- 関係組織との連携とセキュリティ意識の醸成
- ツール選定におけるポイント

参照：IPA「脆弱性診断内製化ガイド」 https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2025/Vulnerability-assessment.html

AeyeSecurityLab

質問受付中!!

本日のまとめ

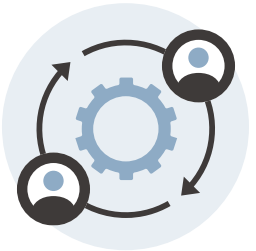
全社を巻き込んで進めるセキュリティ対策の「新常識」

事業部主導のデジタル化
⇩
IT部門だけでは
追いつかない
セキュリティ対策

これで
解決！

ビジネスの視点＝事業部門との
「共通言語」で会話する

全社を巻き込んだセキュリティ対策



AeyeSecurityLab

質問受付中!!

「全社で進める」セキュリティ対策を実現する

脆弱性対策の“新常識”

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「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）

有償契約
300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

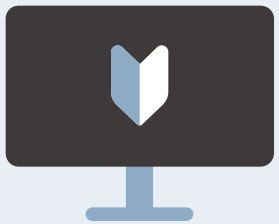
02
学習コストゼロ
開発やセキュリティの
知識がなくてもすぐに使える

03
業界標準対応
外部委託と遜色なく
内製化が可能

AeyeSecurityLab

質問受付中!!

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。

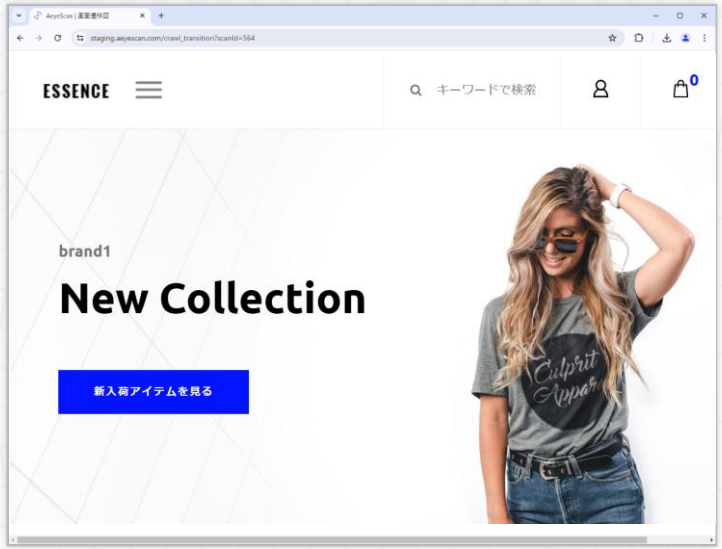
わかりやすいレポート

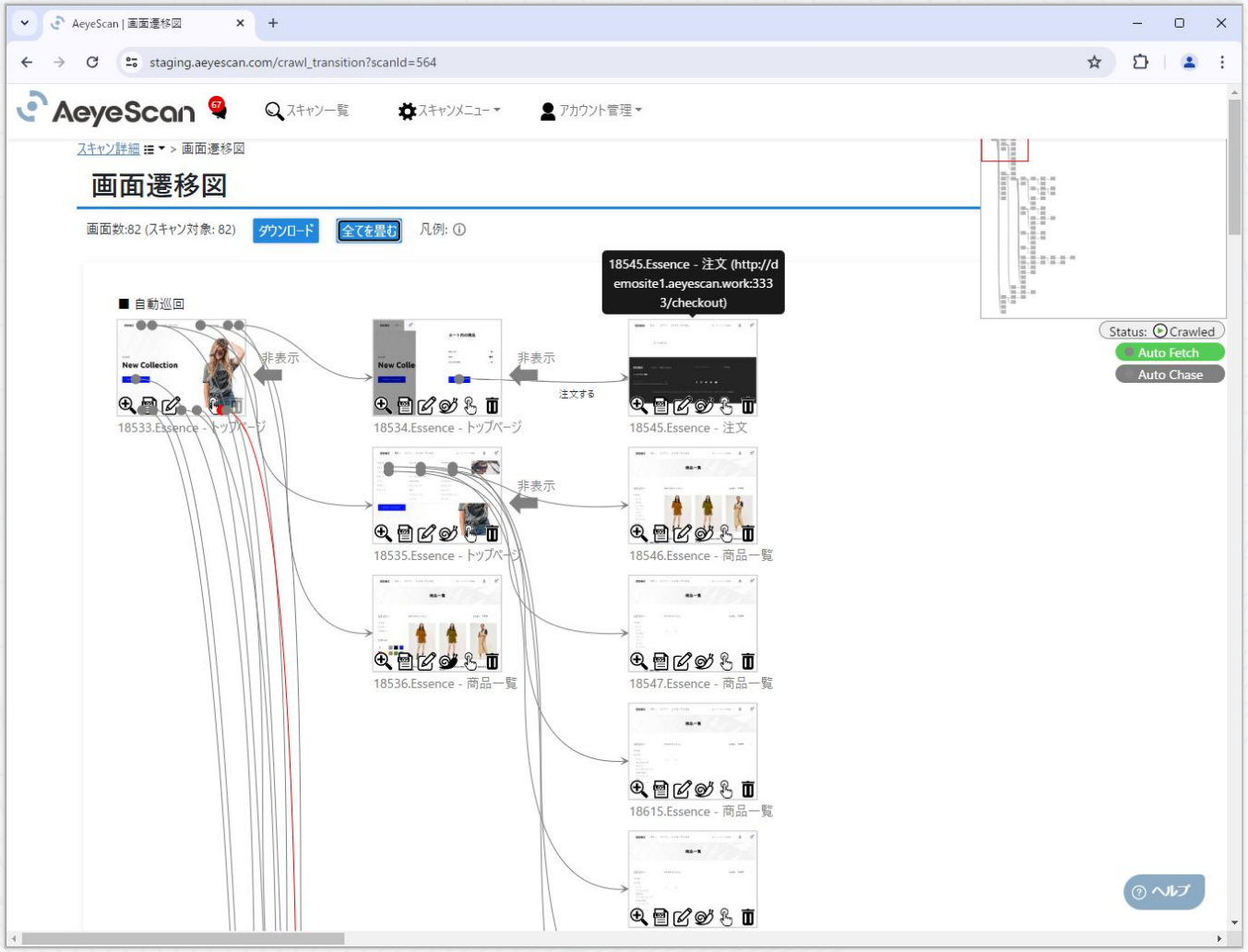
各種ガイドラインに準拠した
プロ仕様のレポート出力、
日本語と英語に対応。

AeyeSecurityLab

質問受付中!!

巡回時に、自動で画面遷移図を生成





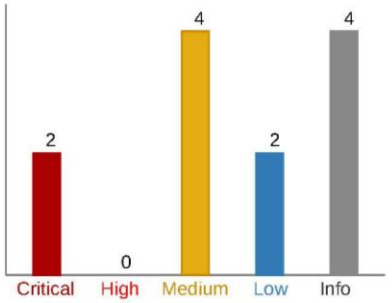
AeyeSecurityLab

質問受付中!!

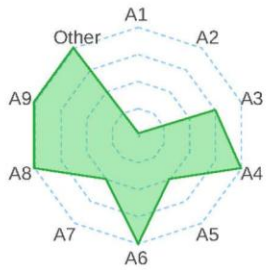
結果がわかりやすく、すぐさま修正作業に取り組めるレポート

スキャンサマリー

全体評価　Critical



深刻度ごとのサマリー



OWASP TOP 10 カテゴリー

脆弱性の深刻度はCVSSv3 (https://www.ipa.go.jp/security/vuln/CVSSv3.html) に基づき以下の基準で設定しています。

深刻度	CVSSv3基本値	脆弱性に対して想定される脅威
Critical	9.0～10.0	・リモートからシステムを完全に制御されるような脅威 ・大部分の情報が漏えいするような脅威 ・大部分の情報が改ざんされるような脅威
High	7.0～8.9	
Medium	4.0～6.9	・一部の情報が漏えいするような脅威 ・一部の情報が改ざんされるような脅威 ・サービス停止に繋がるような脅威 ・その他、Critical/Highに該当するが再現性が低いもの
Low	0.1～3.9	・攻撃するために複雑な条件を必要とする脅威 ・その他、Mediumに該当するが再現性が低いもの
Info	0	

クロスサイトスクリプティング

スキャン情報

948. スキャン結果 ブランドECサイト (http://demosite2.aeyescan.work:3333/)

対象ページ

36846.Essence - 登録情報編集（確認） (http://demosite2.aeyescan.work:3333/my-page/user-edit)

画面遷移図で表示

深刻度

Medium

CVSS: 6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

スクリーンショット

AeyeSecurityLab

質問受付中!!

AeyeScanが選ばれている理由

プロが認める機能・性能 × 誰でも使える操作性

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
KITZ 株式会社キッツ
KOSÉ
SAKI
TIGER
TEIJIN
Denkei
House
Mizuno
ユーグレナ

インフラ

EPARK
ARE
HIS
H2O RETAILING
NTT EAST
odakyu
近鉄情報システム株式会社
GEO
SymEnergy シン・エナジー
水ing Swing Corporation
Suzuyo
NANKAI 南海システムソリューションズ
HITOWA GROUP
grow up together MEDIA
Looop
Loyalty Marketing, Inc.

金融

ファイナル
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

人材・教育

Junion
JINSOKEN
ZENKIGEN
Direct Sourcing
PERSOL
Leverages
workport

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
estie
エアアドエムネット株式会社
M-aid
MTエムティーアイ
OZ INTERNATIONAL
Classi
COACH A Co.,Ltd.
cybozu
Speee
SecureNavi
DMM Boost
TAL
Digital Garage
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 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
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 TAKACHIHO KOHEKI CO.,LTD.
電通総研
TOPPAN
JOPS
JAST
NHC
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

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

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！

デミセミナーの日程を確認

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