脆弱性診断 内製化 の始めかた

差がつく運用設計の”5ステップ”とは？

AeyeSecurityLab

登壇者紹介

主な著書

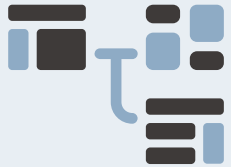
株式会社エーアイセキュリティラボ

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、新規プロダクト企画・事業開発をリードしながら、
各種セミナー・講演への登壇などエバンジェリストとしても活動。

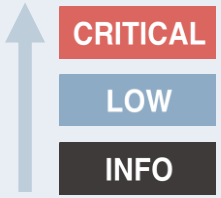
「脆弱性診断」と言われて
何を思い浮かべますか？

脆弱性診断と言われて思い浮かぶのは…？



Webサイトの診断

脆弱性の評価



優先度付け

脆弱性の修正

しかし、診断・修正だけでは

戦略的なセキュリティ対策ができているとは言えない…！

脆弱性診断を自動化・内製化するときに考えること

「内製化できればいいんだけどな…」

診断の**品質を維持**できるだろうか？

診断員を**育成・確保**できるだろうか？

コスト(費用・時間)を削減できるか？

脆弱性診断を自動化・内製化するときに考えること

診断の**品質を維持**できるだろうか？

診断員を**育成・確保**できるだろうか？

コスト(費用・時間)を削減できるか？

＋

内製化に向けた体制を組み、運用にのせられるか？

脆弱性診断を内製化できるかは、体制づくり・運用設計にかかっている

課題 1

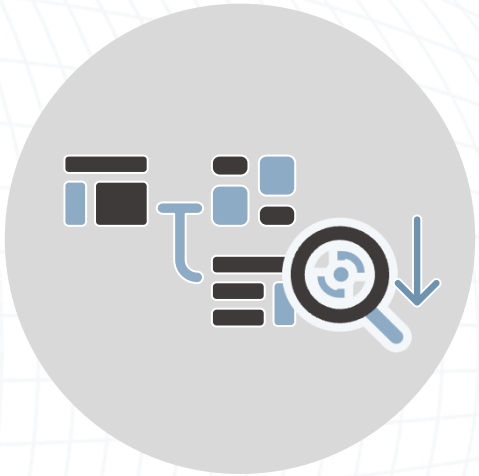
どういう体制を組めばいい？

今まで外部ベンダーに委託していたので
社内で診断業務を完結させようとしたとき
必要な業務・役割が分からない…

課題 2

どうやって運用ルールを作る？

運用ルールを作る、といっても…
非現実的なルールを作ってもしょうがないし
どんな観点で、何について決めればいい？



課題 3

ルール通りに診断してくれない

特に事業部門・開発部門で診断を行う場合
予め運用ルールを定め、周知徹底しても
なかなかその通りには運用されない…

脆弱性診断の内製化を進める
具体的なステップ

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

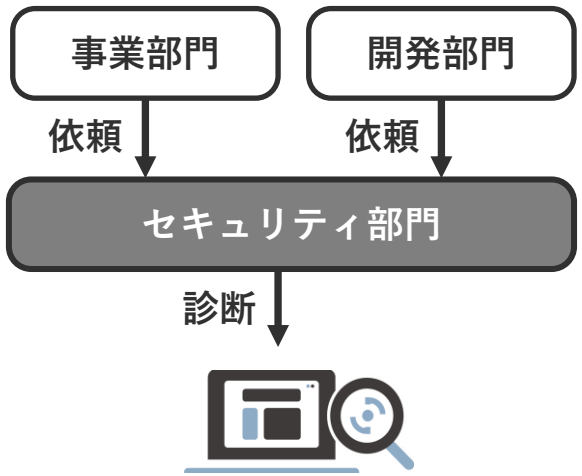
脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 0 運用体制の構築・役割分担

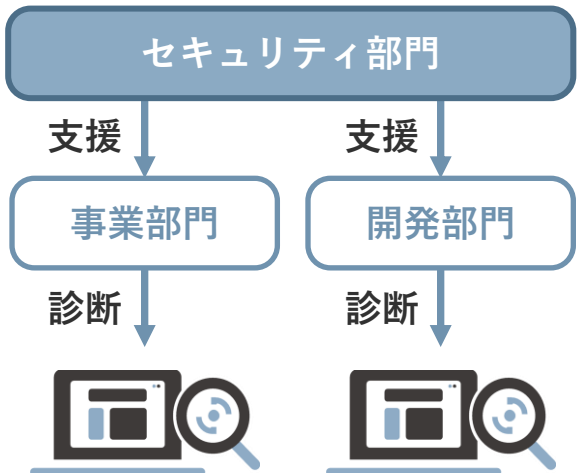
従来の運用体制

セキュリティ部門が
まとめて診断



これからの運用体制

**事業部門・開発部門が
脆弱性診断を実施できる
体制**を構築



メリット

- シフトレフトの実現
- 診断対象の的確な把握
- セキュリティ意識の醸成

AeyeSecurityLab

脆弱性診断内製化のポイント

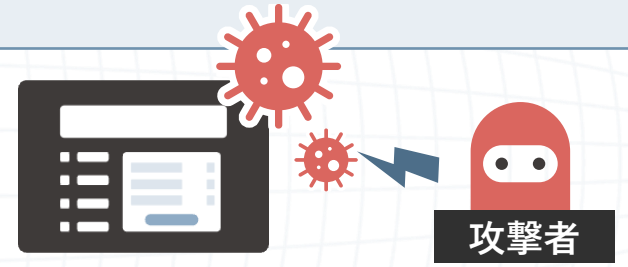
脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 1 情報収集・対象の把握

自社で管理すべきWebサイトの棚卸＆探索により、診断対象の全体把握が重要

某大手ハウスメーカー（A社）さまの事例

某日、A社が運営サイトのアクセスが急増し、高負荷状況に…
調査した結果、**過去に3年程度オープンしていたWebサイトの現在は運用していないページが攻撃を受けていた**ことが判明



ページが公開されていたこと、アクセス可能であることは認識されていたのか？

気付いたら「さくっと」
Webサイトができている…

開発後・リリース後も検証環境や
テスト環境がひっそり残っている…

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 2 診断の必要性や優先順位を評価、対応方針の検討

スコープを明確にし、**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

診断の優先順位 – 診断方法の考え方（例）

例：「取扱い情報」と「開発規模」の掛け算で、診断手法を分類

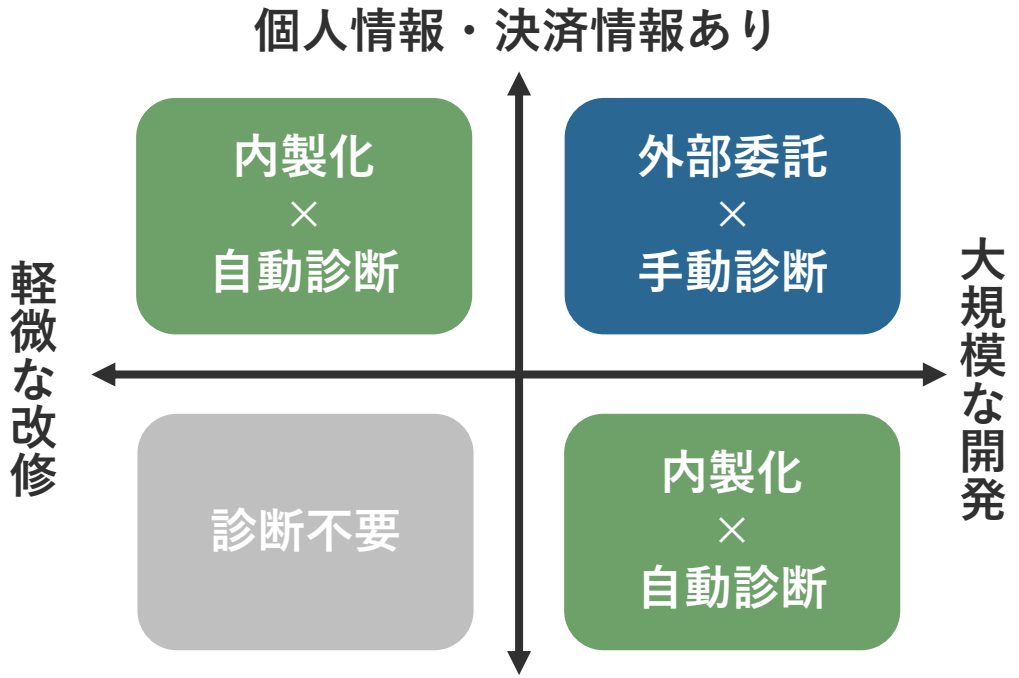
診断対象サイトの重要度

- 取り扱っている情報の重要度

×

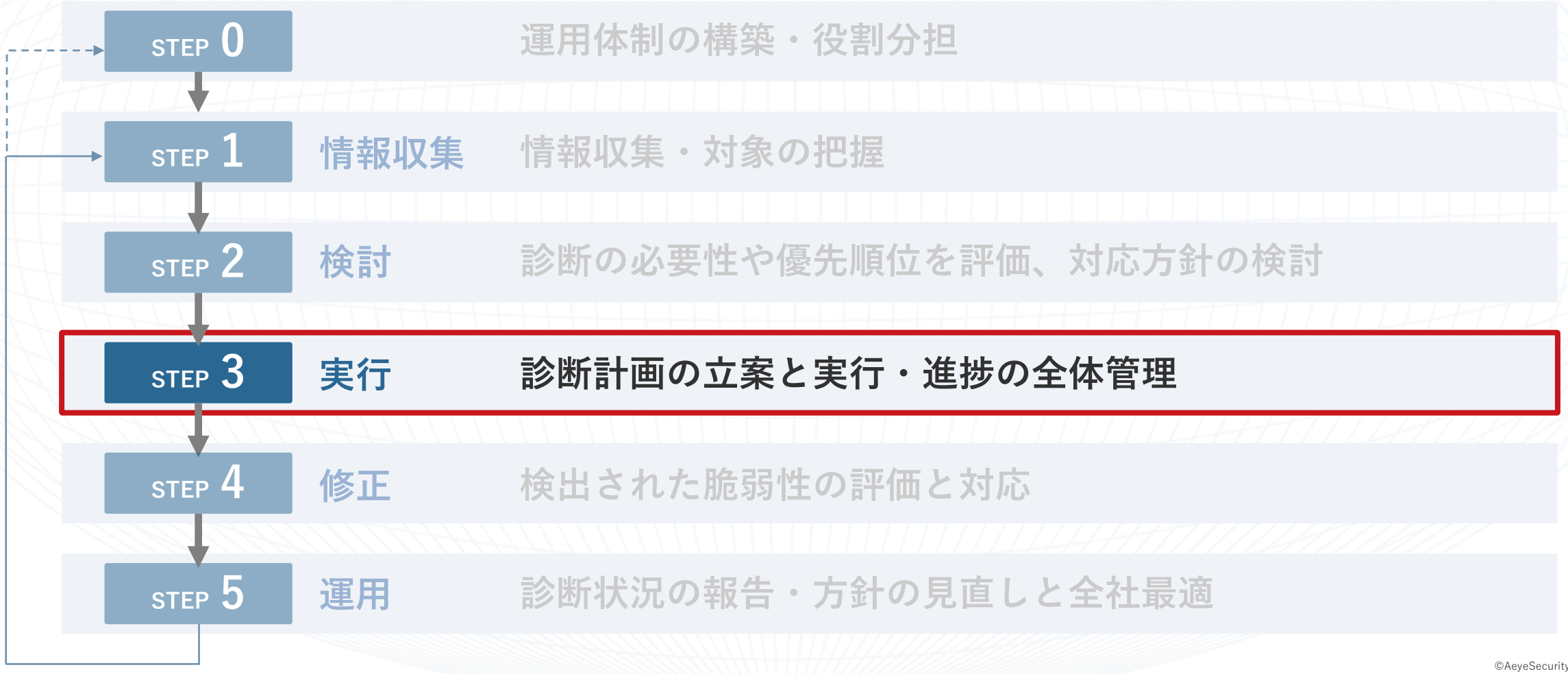
開発規模

- 軽微な改修 or 大規模な開発



脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。



STEP 3 診断計画の立案と実行・進捗の全体管理

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

脆弱性診断実施問診票

この問診票は、脆弱性診断を実施いただくにあたり、確認・調整がお要な項目を事前にご対応いただくことを目的にしております。
この問診票は、貴社内でご利用いただくもののため、エーアイセキュリティラボへの送付は不要です。

No			回答記載欄	説明・対応
体制・基本情報				
1	必須	診断対象サイト名		スキャンを実施する対象サイトを選定してください。 一部Aeyescanで対応できないサイトがあります。は「No28.注意事項」をお読みください。
2	必須	サイト担当者①	部署名 氏名 メールアドレス	AeyeScanの利用中にサーバへ影響が発生した場合、サイト担当者へ連絡を行うために診断対象サイトの運用をご担当されている方もしくは窓口の方の連絡先を記載してください。
3		サイト担当者②	部署名 氏名 メールアドレス	サイト担当者①とご連絡がつかない場合のお問合せ先を記載してください。
4	必須	診断実施担当者①	部署名 氏名 メールアドレス	AeyeScanの設定を依頼する、診断の一時中断を依頼する等の連絡を行うために、診断を担当される方（AeyeScanを操作される方）の連絡先を記載してください。
5		診断実施担当者②	部署名 氏名 メールアドレス	診断実施担当者①とご連絡がつかない場合のお問合せ先を記載してください。
スケジュール				
6	必須	診断スケジュール	日程	XX月XX日～XX月XX日	診断スケジュールの目安は下記の通りです。 ・24時間アクセス可能な場合： 3～5日程度 ・8時間アクセス可能な場合： 5～15日程度 ※サイトの規模やサイトからの応答速度により増減する場合があります。
7			曜日	■平日・土日祝 □平日 □その他()	診断実施可能な曜日を記載してください。
8			時間	■24時間 □10:00-18:00	診断実施可能な時間帯を記載してください。 特定の時間にサーバ停止するなど、アクセス負荷の時間帯があれば、その他として詳

AeyeSecurityLab

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 4 検出された脆弱性の評価と対応

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

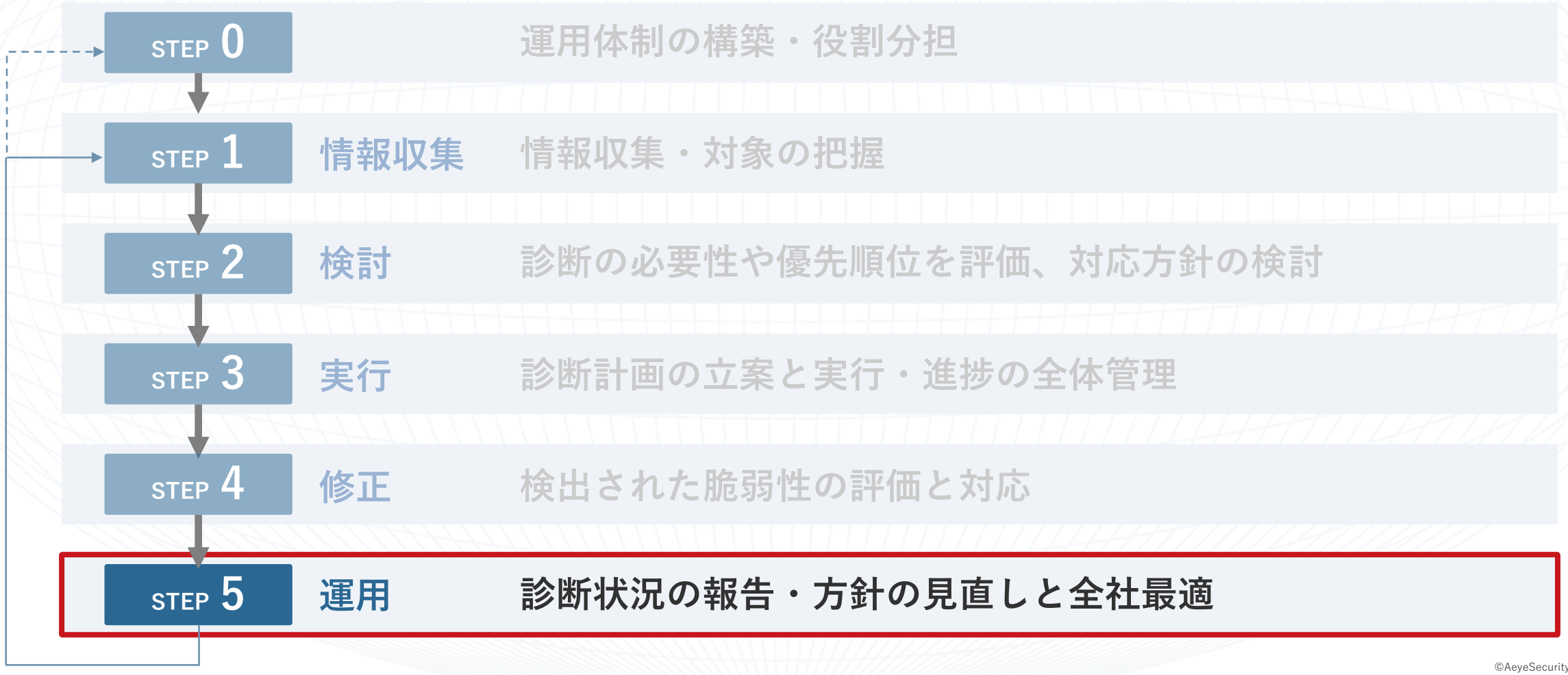
対策方針の検討

- 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

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。



STEP 5 診断状況の報告・方針の見直しと全社最適

診断の予実と診断結果をもとに、次年度以降の方針を見直し、最適化するのが大事

経営層		セキュリティ部門 情報システム部門		事業部門・開発部門 グループ会社
				
セキュリティ関連施策の 投資判断	→ 戦略目標の定義 リソース配分 →	具体的な施策の決定 ルール策定・運用設計	→ ルール周知 技術サポート 実行管理 →	全社ポリシーに則った セキュリティ対策
全社情報セキュリティの リスクマネジメント	← 定期報告 施策検討・上申 ←	セキュリティ対策関連の 情報収集・集約	← プロジェクトや 対策状況の共有 ←	セキュアな開発 セキュアなサービス提供

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

自分たちだけで内製化するのは大変

でも AeyeScan なら…！

生成AI時代の脆弱性診断なら AeyeScan

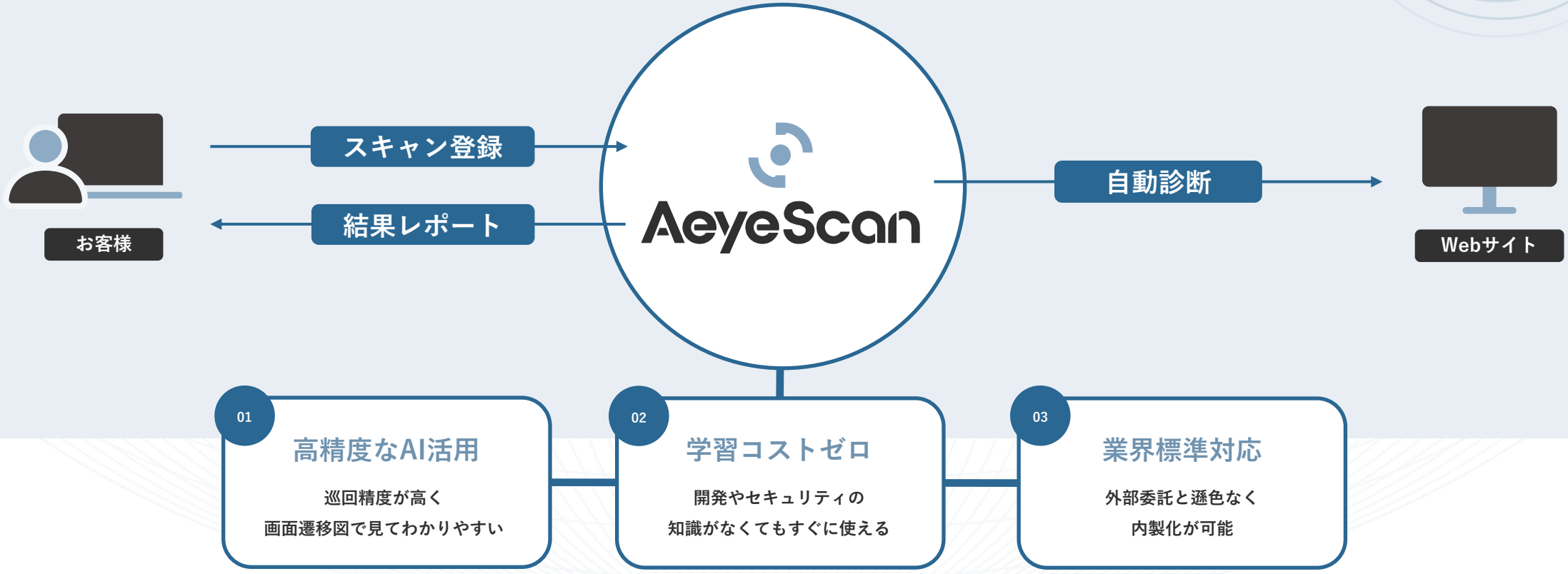
クラウド型Webアプリケーション
脆弱性検査ツール

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2026」SaaS型Webアプリケーション脆弱性診断・管理市場：ベンダー別売上金額シェア（2024年度実績）

有償契約
300社以上

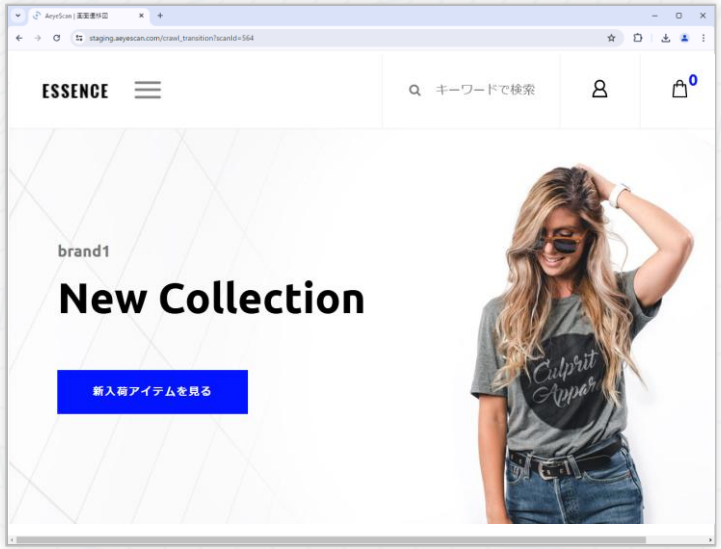


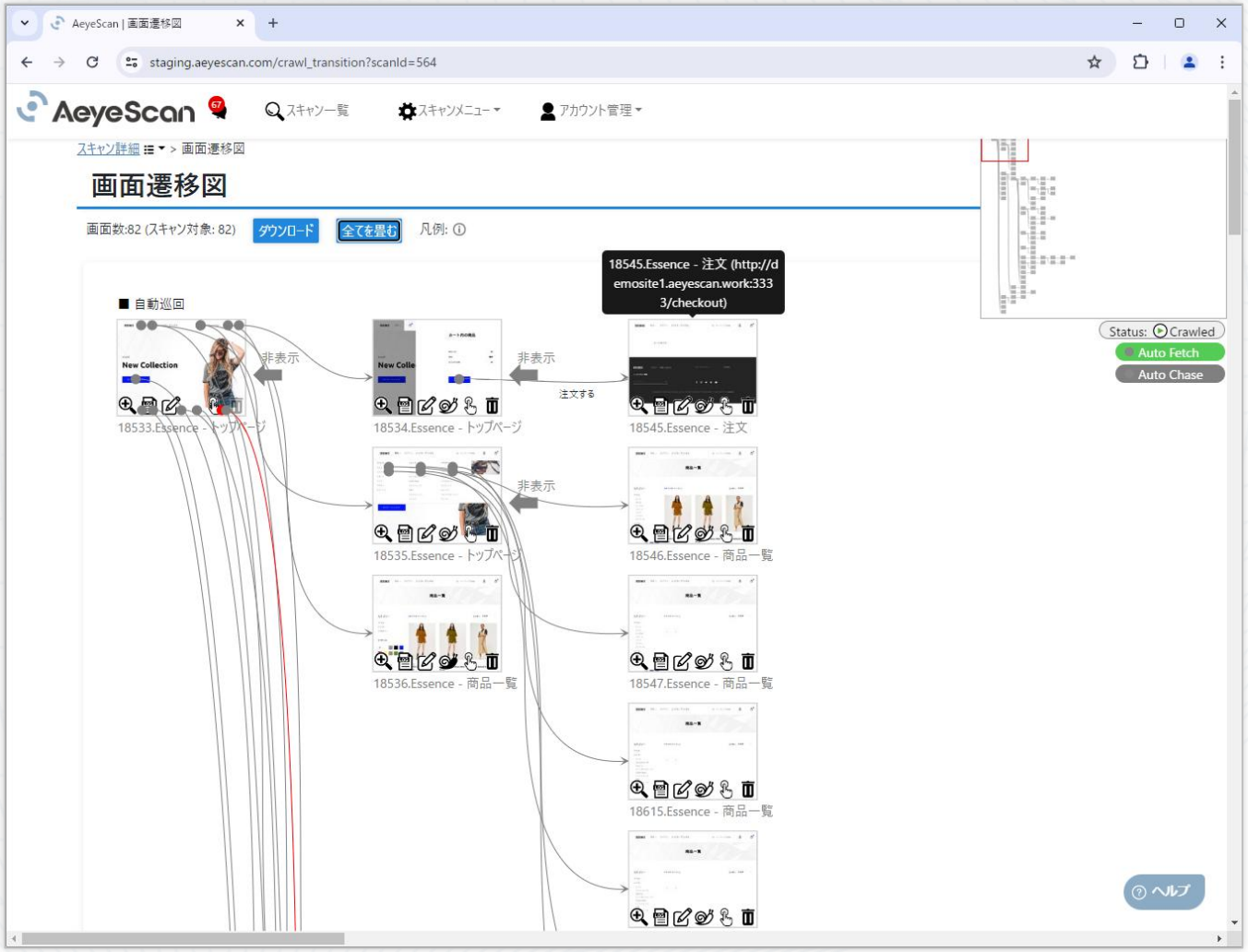
01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

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

巡回時に、自動で画面遷移図を生成





AeyeSecurityLab

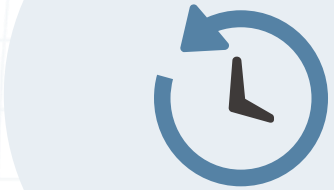
結果がわかりやすく、すぐさま修正作業に取り組めるレポート

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。

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

インフラ※

EPARK / AIRE / HIS / H2O RETAILING / NTT EAST / イープラス / CAPCOM / GungHo Online Entertainment, Inc. / odakyu / 近鉄情報システム株式会社 / GEO / SymEnergy シン・エナジー / とらラボ! TORANOANA LABORATORY / BookLive / 水ing Swing Corporation / Suzuyo / TOYOTA HOME / NANKAI 南海システムソリューションズ / 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.

エンタメ

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

メディア

集英社 / 中日新聞 / 東海テレビ / 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

金融

セブン-イレブン / UPSIDER / 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

人材・教育

OHSAWA DRIVING SCHOOL / 河合塾 / Junion / JINSOKEN / ZENKIGEN / Direct Sourcing / PERSOL / 立教大学 / Leverages / workport

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア / Lexica E-Retailing Platform / エフアンドエムネット株式会社 / M-aid / MTエムティーアイ / OZ INTERNATIONAL / giftee* / 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 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 株式会社パソフィックネット / Human Interactive Technology Inc. / FUJISOFT / FUJITSU / MACROMILL / MITSUBISHI ELECTRIC Changes for the Better / 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

※公共および社会・生活基盤までを包含

社名五十音順（導入いただいた企業様の一部です）

＼最終週もぜひご参加ください／

詳細はこちらから

セキュリティ診断のお悩み・お困りごとをお聞かせください！

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。