サプライチェーンを揺るがす「DX推進の死角」とは？

AIを活用した

脆弱性対策の内製化 アプローチ

AeyeSecurityLab

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。

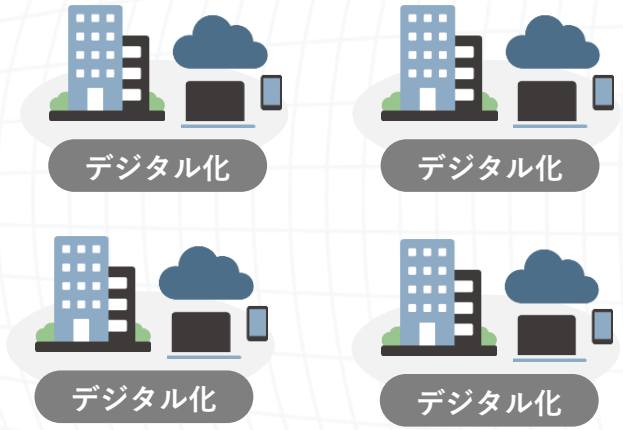
そして、サイバーセキュリティの進化を通して、
人は、人にしかできない、創造性を活かした仕事に注力できる、
社会の進化にも貢献していきます。

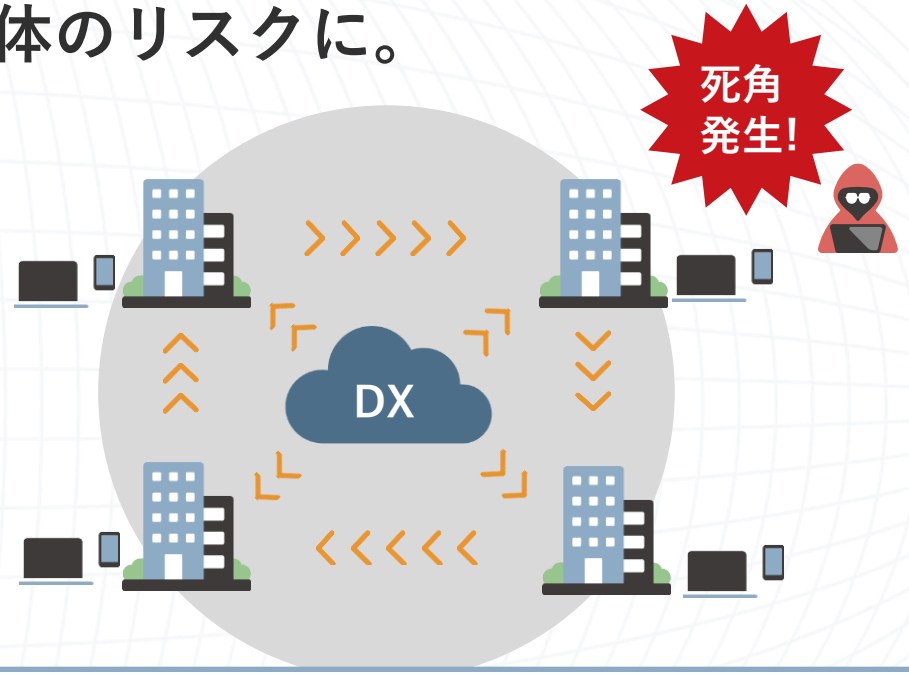
AeyeSecurityLab

「DX推進の死角」に気づいていますか？

DXの進展に伴い、サプライチェーンリスクが拡大

企業間連携が進み、脆弱性がサプライチェーン全体のリスクに。





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

昨年はサイバー攻撃、特にランサムウェアによる被害が話題に

大手飲料メーカー

2025年9月、ランサムウェア攻撃により、システム障害が発生。**国内グループ各社の受注・出荷業務が停止。**さらに個人情報が流出した可能性があると発表された。

大手通販業者

2025年10月、ランサムウェア攻撃によりシステム障害が発生し、受注・出荷業務が停止。**同社の子会社に配送の一部を委託する別会社のECサイトも停止に。**

業務停止・システム停止による事業影響、社会的信頼・株価への影響だけでなく

取引先やグループ会社、サプライチェーンを巻き込む被害に発展

AeyeSecurityLab

多様化するランサムウェアの「侵入経路」

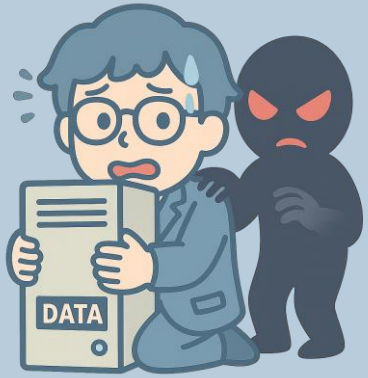
NW機器/VPN

クラウド

Webサイト

CMS/SaaS

PC/社用端末



メール/ファイル

「DX推進の死角」は、どうやって生まれ、どこにあるのか？

公開するWebサイトや提供するWebサービスが増えている

開発規模・サイト規模が大きくなっている（100画面以上ある）

機能改修・追加などリリース頻度が高く間隔も短くなっている

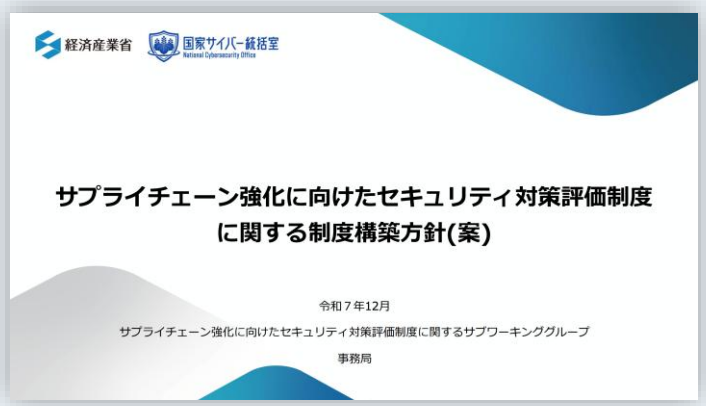
知らないうちに作られ公開されていたWebサイト

新規リリース時に診断したきり何もやっていないWebサイト

リリース前の診断が追い付かず脆弱性が残っているWebサイト

セキュリティ対策水準の向上を図る「サプライチェーン対策評価制度」

経済産業省は、サプライチェーン全体の強靭性の確保と、対策要求の共通化による対策適正化・確認の効率化を目的とした「サプライチェーン対策評価制度」を導入する方針を示している。



セキュリティ対策の
成熟度を3段階で評価

	★3	★4	★5
想定脅威	一般的な サイバー攻撃	供給停止・情報漏洩 など大きな影響を もたらす攻撃	未知の攻撃も含めた 高度なサイバー攻撃
対策の基本的な 考え方	全てのサプライ チェーン企業が 最低限 実装すべき対策	サプライチェーン 企業等が標準的に 目指すべき対策	サプライチェーン 企業等が到達点と して目指すべき対策
評価スキーム	専門家確認付き 自己評価	第三者評価	第三者評価

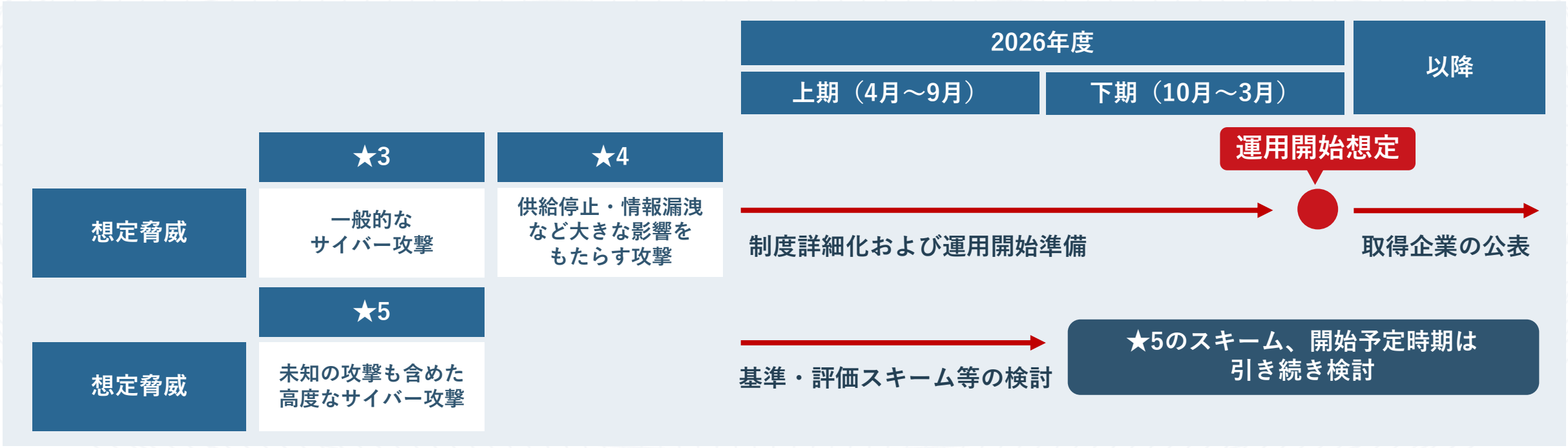
※★1、★2に関しては、先行する自己評価制度の仕組みである「SECURITY　ACTION」にて制度化

認定取得の有無が取引基準となる可能性もあり、どの企業も無関係ではいられない

参考：サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)より抜粋および意訳

2026年度下期から運用開始想定

2025年12月下旬（昨年末）に制度構築方針（案）が更新され、★3、★4については2026年度下期の運用開始を想定していると記載された。



運用開始に向けて、自社のセキュリティ対策状況の見直しが急務となっている

参考：サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)より抜粋および意訳

Web領域のセキュリティ対策だけでも、広範に及ぶ

Webアプリケーションのセキュリティ対策項目

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

参考：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～

ただでさえやることがいっぱいなのに、
制度対応もしないといけないのか…

IT部門・セキュリティ部門の皆様から伺う「お悩み」

予算が限られている

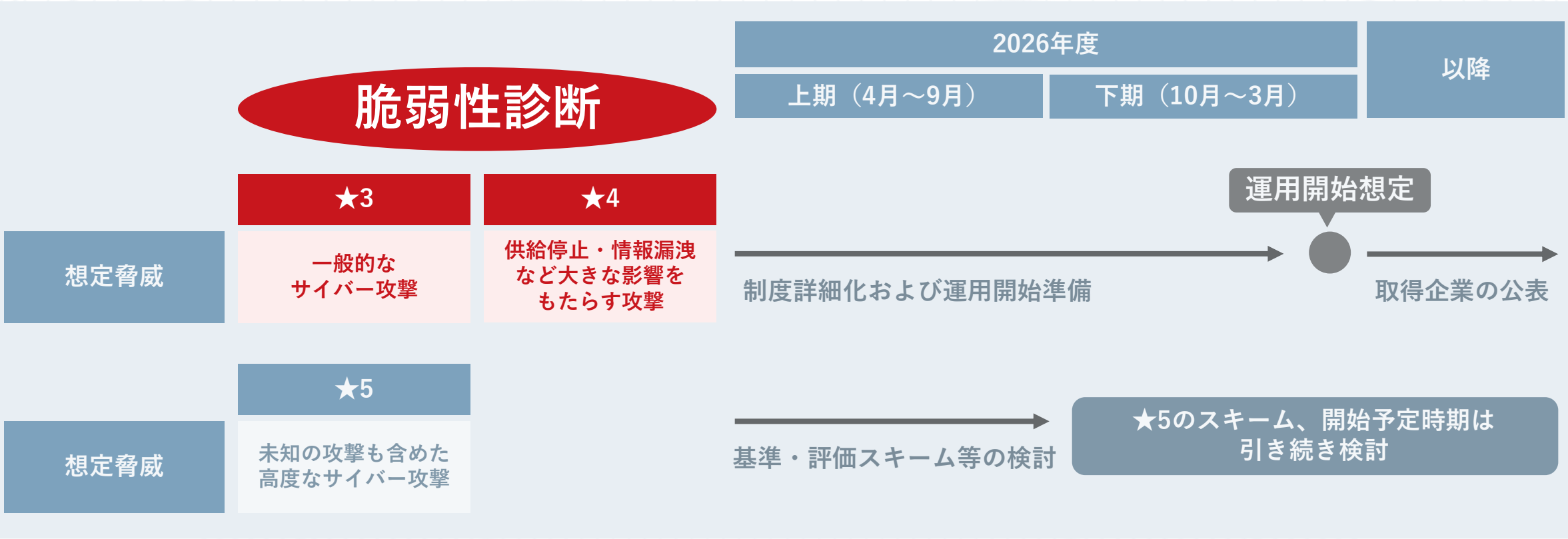
人員も限られている

対策すべき範囲 増

必要な対策の幅 増

まずは「攻撃手法・対策方法が分かっている」部分から対策

★3、★4で想定されている“既知の脆弱性”から対策する＝穴を塞ぐことが最優先。
未知の攻撃への防護策を考えるのは、その次でOK。



参考：サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)より抜粋および意訳

脆弱性対策の「内製化」に立ちはだかる壁

脆弱性診断を網羅的・継続的に実施するために「内製化」を考える

「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？

？

コスト（費用・時間）を抑えられるか？

？

社内メンバーで対応できるだろうか？

＋

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のポイントは、体制づくり・運用設計

課題 1

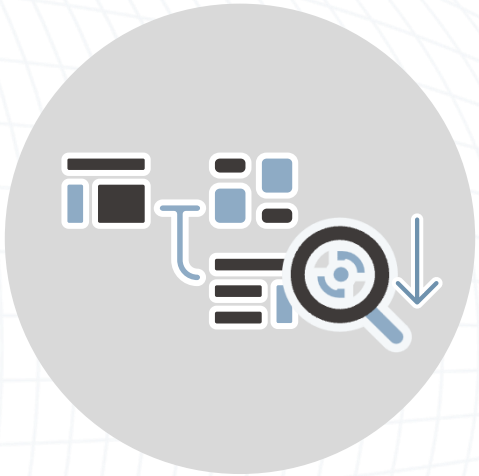
どういう体制を組めばいい？

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？

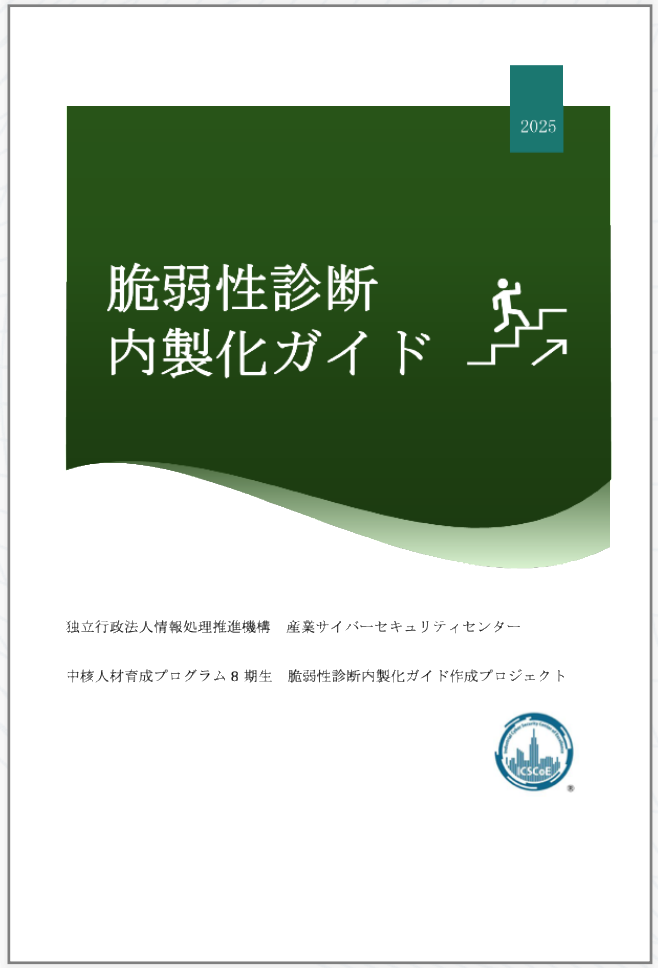


課題 3

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…

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

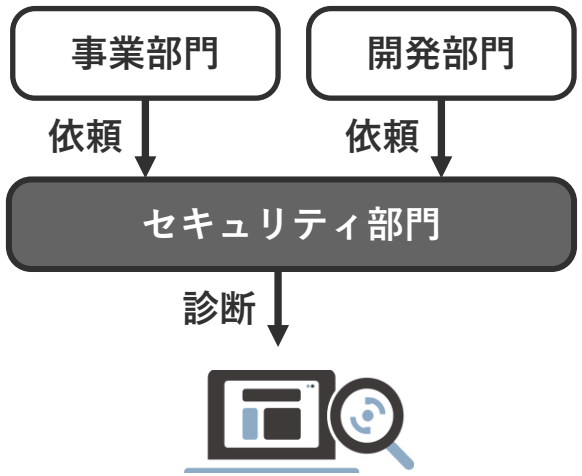
脆弱性診断内製化のポイント

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

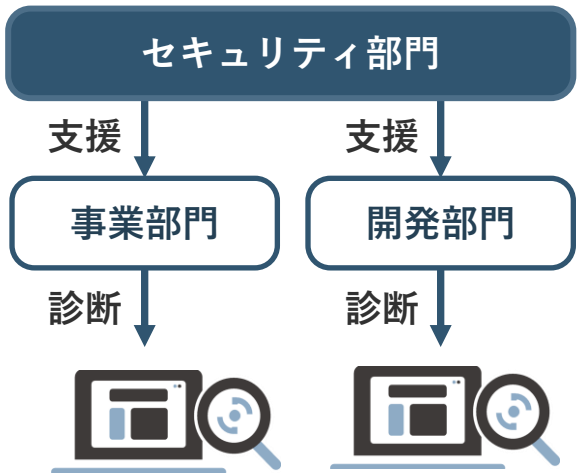
従来の運用体制

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

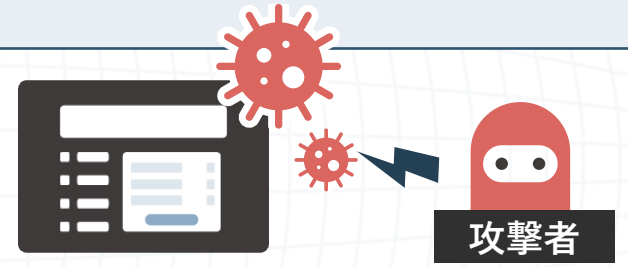
- シフトレフトの実現
- 診断対象の的確な把握
- セキュリティ意識の醸成

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…

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

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

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

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

「死角」になっている
Webサイト・Webアプリはどうする？

DXの進展：Web資産の把握が難しくなっている

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認識しやすい
社内ITを中心とした「静的」IT資産がほとんど

どこで何やってるか
分からない…！

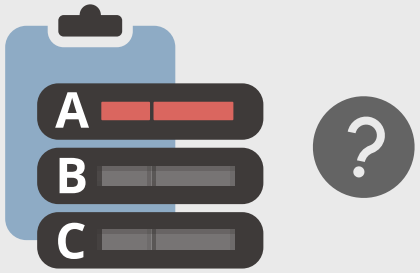
Web資産を把握する難しさはどこにある？

人力で探索・精査が必要

広範囲から検出することはできるが、
不要なものも多く紛れ込んでおり、
人手による精査が必要。

リスク評価が困難

リスクをどう評価するか悩ましい。
システム観点からだけでなく、
事業観点での優先順位付けが必要。



高度な生成AI活用により、効率的かつ信頼性の高い探索が可能

生成AIをASMに活用することで…！

会社名だけ
で攻撃面を探索

検索結果に上がってきた
組織名(文字列)を解読

膨大な情報源
から総合的に判定

- SSL証明書の情報
- IR情報(Web公開済み)　など

発見経路/理由
が分かる

生成AIが攻撃面を見つけるまでに
辿ったルートを説明

AeyeSecurityLab

リスク対応の優先順位付けに必要な情報を自動判別

Web資産の重要度

各Web資産の属性

（サイト用途、保持データなど）

リスクの深刻度 NEW

ミドルウェアやライブラリの悪用観測脆弱性※

※既にサイバー攻撃で悪用が確認された脆弱性

製品情報サイト	重要度：中	2件	ミドルウェアA	CVE-xx	深刻度：高
			ミドルウェアA	CVE-xx	深刻度：中
ECサイト クレジットカード情報保持	重要度：高	1件	ライブラリB	CVE-xx	深刻度：低
ヘルプサイト WordPress使用	重要度：低	10件	ミドルウェアC	CVE-xx	深刻度：高
			ライブラリD	CVE-xx	深刻度：高
			：		

いきなり全部やるのは難しい
➡４段階に分けて、一歩ずつ！

脆弱性対策の成熟段階

成熟段階		把握済み資産	未把握の資産
Lv.1	既知のWeb資産に対する脆弱性の把握	ひと通り診断	ー
Lv.2	優先順位に基づく定常的な診断＆対応	定期的な診断	ー
Lv.3	未知の攻撃面を含む網羅的な資産管理	定期的な診断	探索・棚卸し
Lv.4	「探索→優先度付け→診断」サイクル	定期的な診断	定期的な探索

脆弱性対策の成熟段階 Lv.1

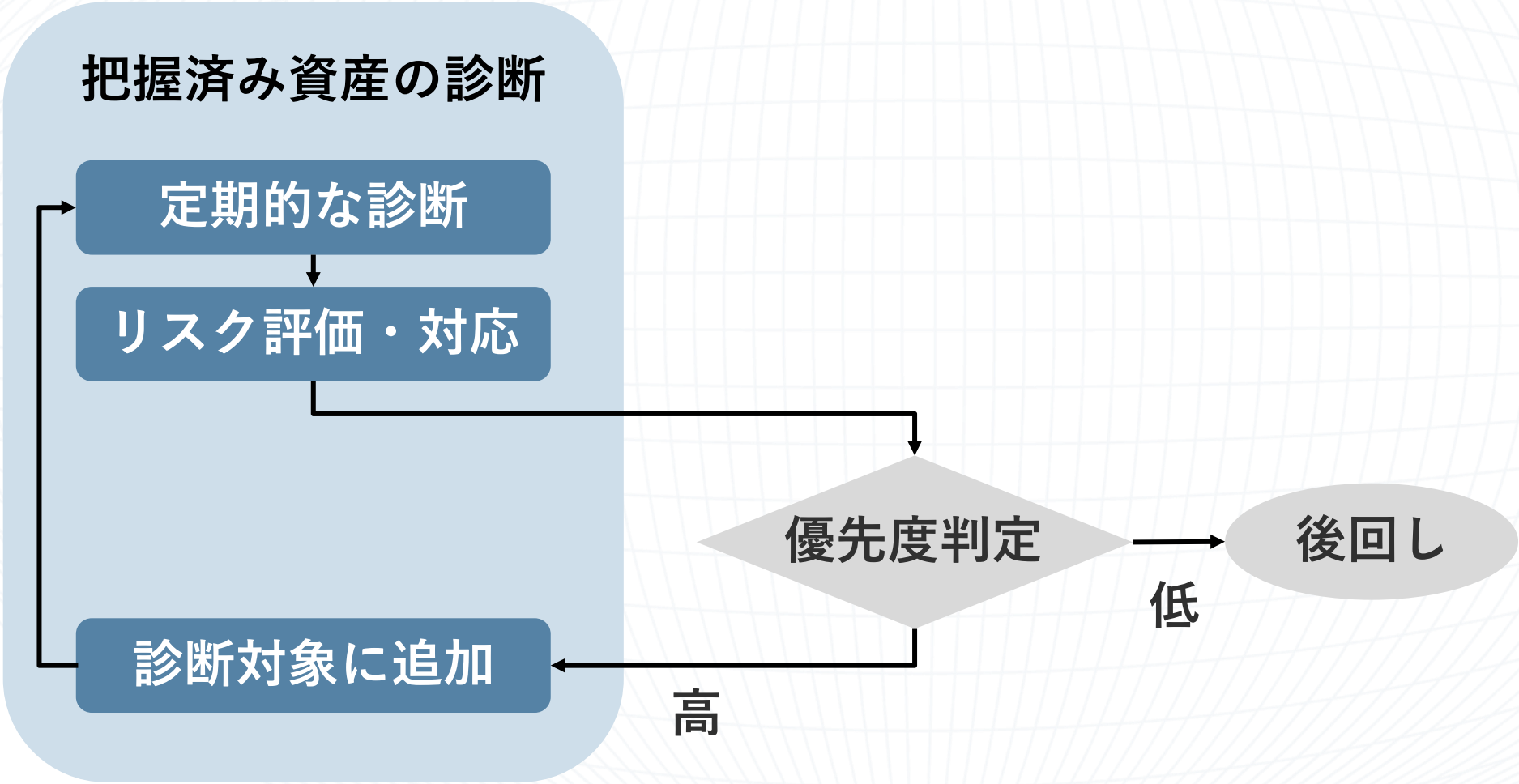
把握済み資産の診断

ひと通りの診断

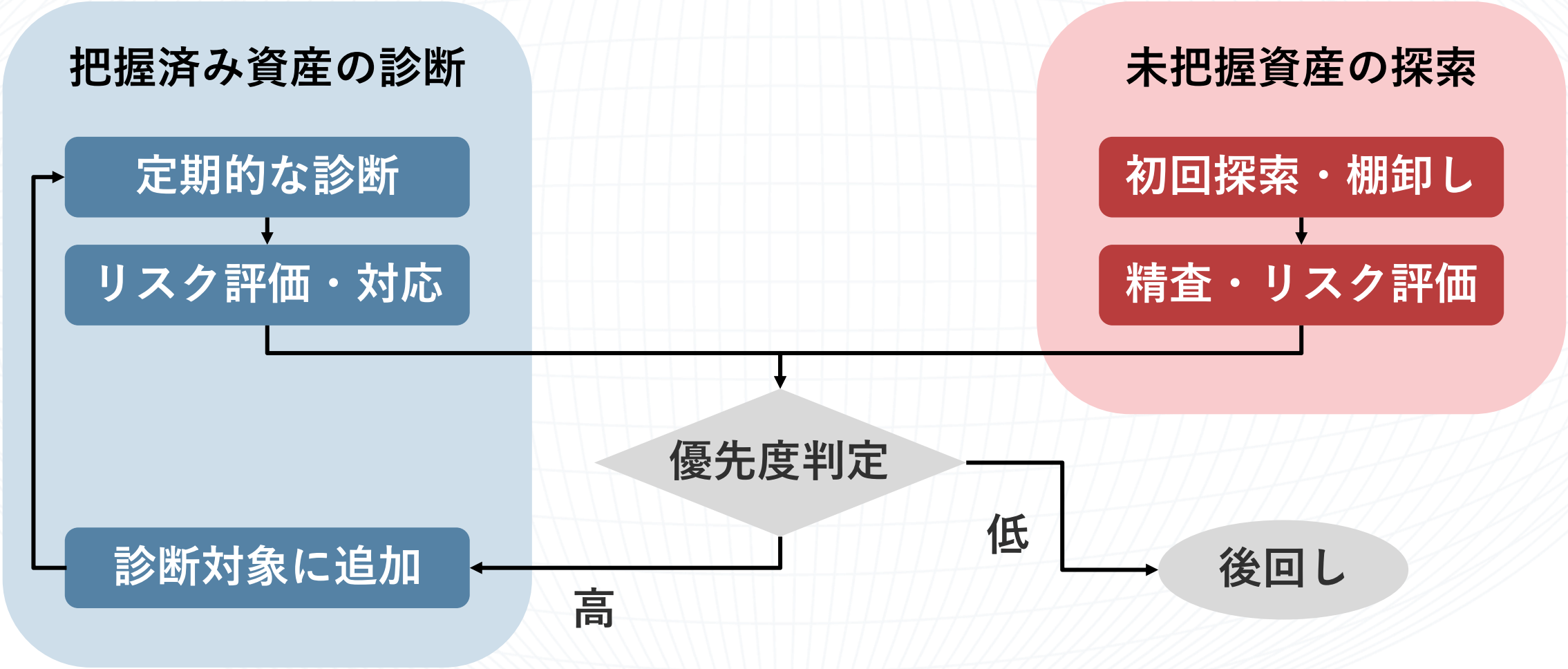
↓

リスク評価・対応

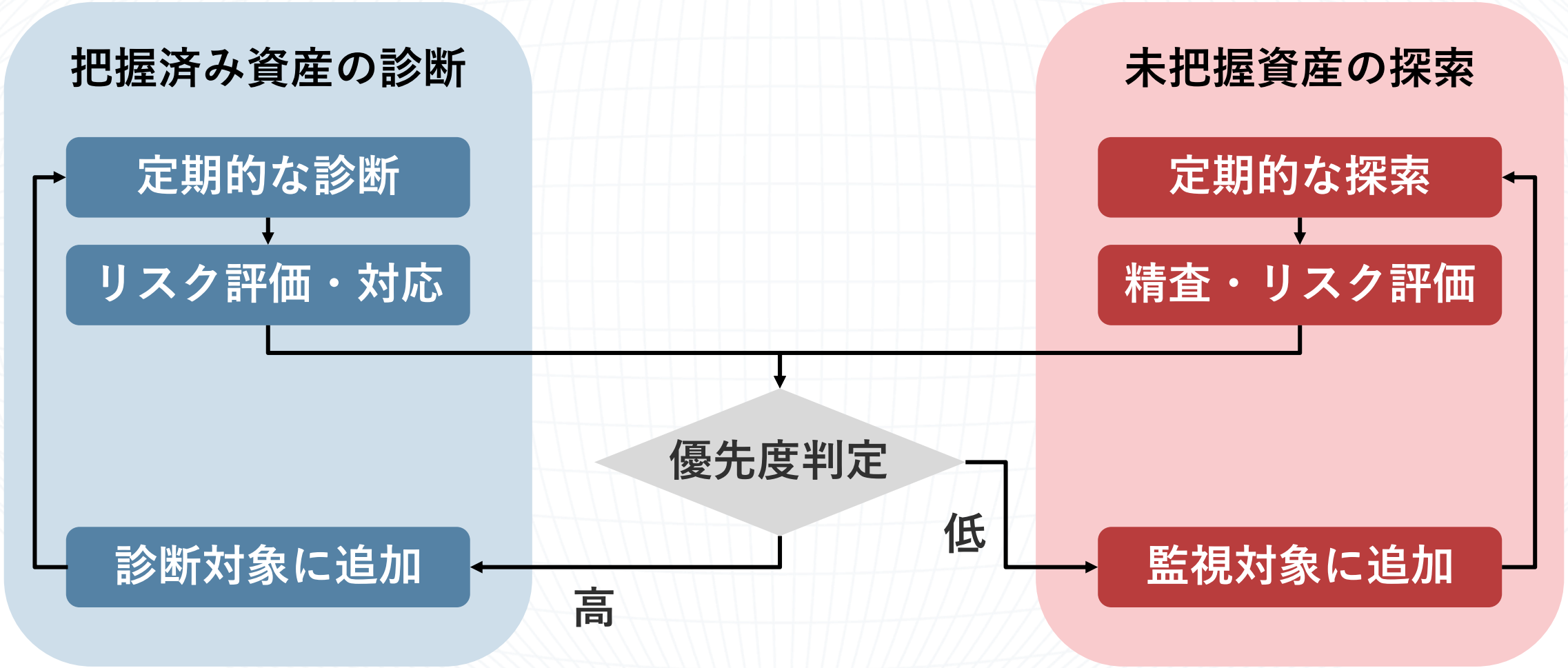
脆弱性対策の成熟段階 Lv.2



脆弱性対策の成熟段階 Lv.3



脆弱性対策の成熟段階 Lv.4



本日のまとめ

1 「DX推進の死角」はWebアプリ・Webサイトにあり

2 自社のWeb資産とその現状を把握し
効率的・網羅的な脆弱性対策を始めるべし

脆弱性対策の強化は、AeyeScanがご支援します！

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）

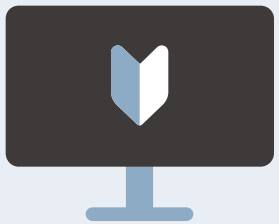
有償契約
300社以上

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

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

誰でも使える操作性 × プロが認める機能・性能

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

Junion
JINSOKEN
ZENKIGEN
Direct Sourcing
PERSOL
Leverages
workport

インフラ

EPARK
AIRE
HIS
NTT EAST
odakyu
近鉄情報システム株式会社
SymEnergy
水ing
Suzuyo
NANKAI
日本調剤
HITOWA GROUP
grow up together MEDIA
Looop
Loyalty Marketing, Inc.

金融

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
KOSÉ
SAKI
TIGER
TEIJIN
Denkei
House
Mizuno
ユーグレナ

エンタメ

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

SaaS

Advanced Media, Inc.
Lexica
estie
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
Finovo
freee
porters
hokan
Money Forward
RUN.EDGE
RVSTA
rescuenow

SI・IT企業

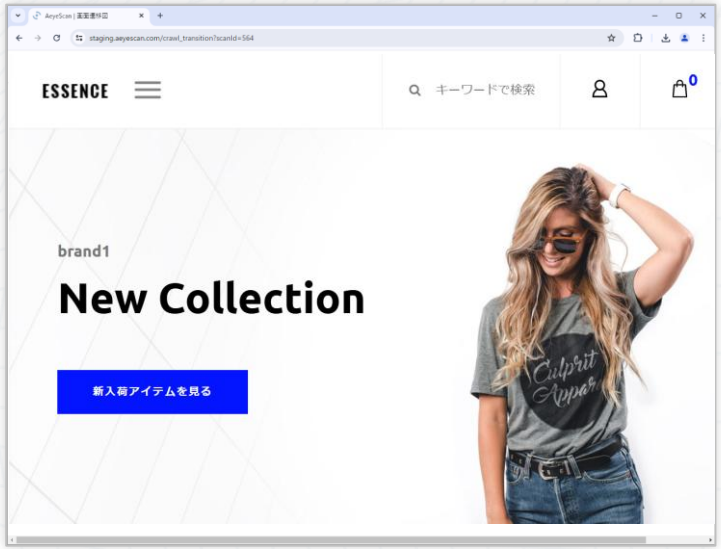
Rworks
アクモス株式会社
AVANT GROUP
Insight Edge
Infcurion
80&Co.
SB Technology
SBWorks
NTT DATA
NTTビジネスソリューションズ
OMRON
Globalway
circlace
さくら情報システム
SUNDAY SYSTEMS
CEC
GA TECHNOLOGIES
tdi 情報技術開発株式会社
Simplex Inc.
777WORKS
SOFT CREATE
SOLTEC
高千穂交易株式会社
電通総研
TOPPAN
JOPS
JAST
NHC
PCNET
Human Interactive Technology inc.
FUJISOFT
FUJITSU
MACROMILL
YONA
リピスト

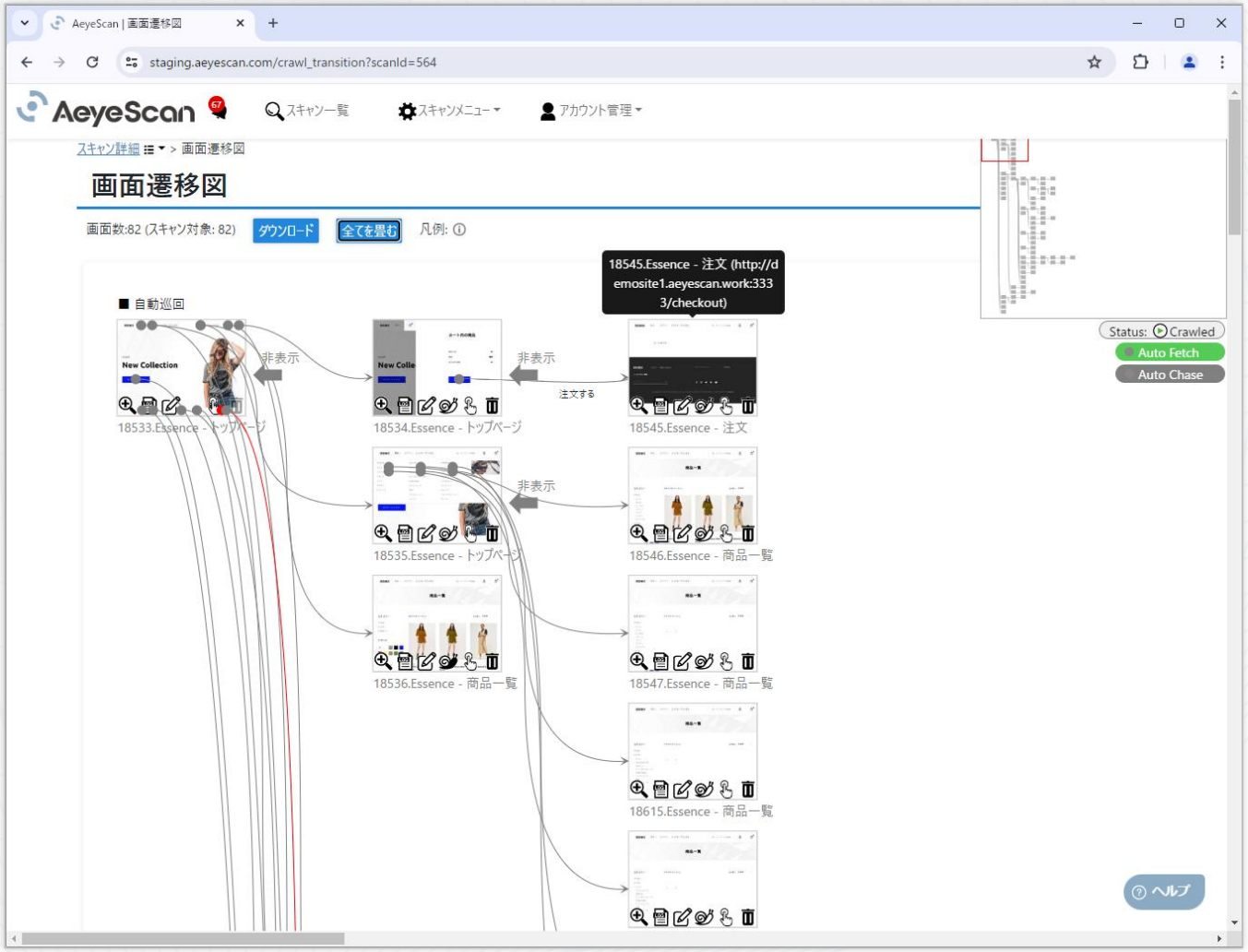
セキュリティ企業

NEC
NECセキュリティ
NTT DATA
GSX
cybertrust
LAC

社名五十音順（導入いただいた企業様の一部です）

巡回時に、自動で画面遷移図を生成



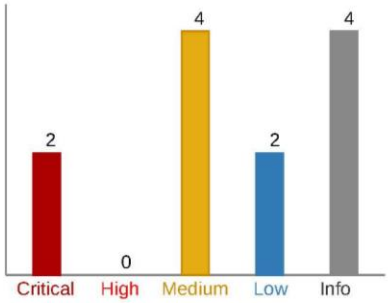


AeyeSecurityLab

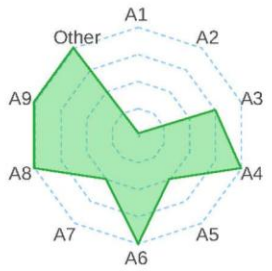
結果がわかりやすく、すぐさま修正作業に取り組めるレポート

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	

スキャン結果詳細

Critical

SQLインジェクション

深刻度

Critical

CVSS Score: 9.8
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

概要

危険な文字列をSQL文に挿入できます。そのため、攻撃者が任意のSQL文を実行できる危険性があります。

OWASP TOP 10 カテゴリー

A1:2017-インジェクション

ASVS4.0 カテゴリー

5.1.2,5.1.3,5.1.4,5.3.1,5.3.4,5.3.5,13.2.2,13.3.1

解説・対策方法

SQLインジェクションとは、攻撃者が細工した入力値を送信することで、開発者の想定していないSQL文を実行できてしまう脆弱性です。この脆弱性は、利用者の送信した値が適切に前処理されずにSQL文の一部として利用されることが原因で発生します。

この脆弱性を悪用することで、データベースの情報漏洩や情報改ざんなど、開発者の想定していない処理を実行されてしまう危険性があります。

対策方法としては、想定していない値が入力された場合に処理を中断することや、SQL文で特殊な意味を持つ文字を無害化することが挙げられます。後者を実現する一般的な方法としては、パラメータ化クエリやプリペアードステートメントの利用が挙げられます。

参考情報

安全なウェブサイトの作り方 - 1.1 SQLインジェクション | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 (https://w

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

AeyeSecurityLab

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向けに、
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！

AeyeScanデモ動画を視聴

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

セキュリティに、確かな答えを。