セキュリティ担当者に読んでほしい

やさしいWebアプリ診断の進め方ガイド

AeyeSecurityLab

こんなお困りごとはありませんか？

脆弱性診断を
すぐに実施したい

リリース時期に合わせ、
任意のタイミングで脆弱性診断を
実施したいが
診断スケジュールを調整したり
外部委託するのも手間がかかる。

既存のセキュリティ対策を
効率化したい

日々の作業に追われて、
情報収集や分析にまで手が回らない。
セキュリティ対策状況を簡単に
可視化できれば、対応の優先度が
付けられるのに。

そもそも
セキュリティエンジニアが
足りない

セキュリティエンジニアは
既存業務に追われていて、
新しいことがさせられない。
新規採用も難しいし、育成は時間や
コストがかかりすぎる。

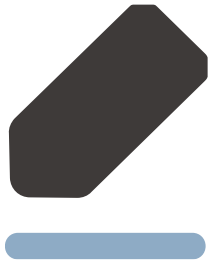
Webセキュリティのお困りごとはAIで解決

AIを活用すれば、誰でも簡単にコスト削減が可能！

誰でもできる

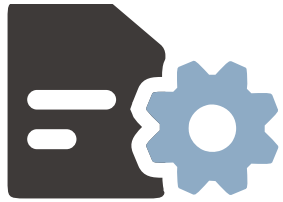
- CIツールなど自動化の仕組みを利用。
- 診断のテストシナリオも自動作成、セキュリティエンジニアを作業から解放。

自動でレポート



- 業界標準ガイドラインに沿ったレポート出力。
- リスクや自社システムへの影響が明確になり顧客や経営層への報告もスムーズ。

高度な管理



- 脆弱性検出時に自動でタスク化。
- 検出結果だけでなく、改修状況までフォローすることで、手間なく高度な管理を実現。

本資料は、Webアプリケーション診断の内製化に向けた推進ステップをわかりやすく解説します。

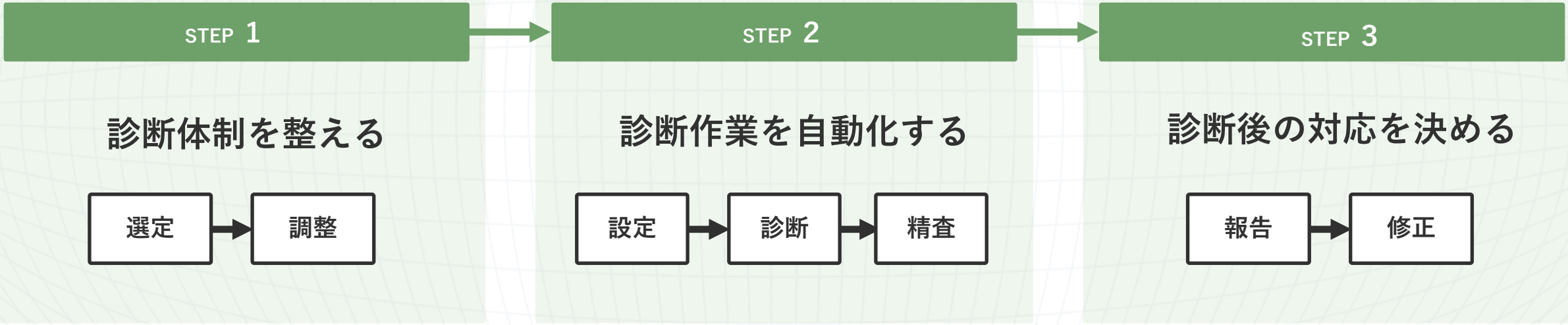
内製化を進める際の具体的な手順がわかる

内製化の際に考慮すべきポイントがわかる

セキュリティ人材がいなくても内製化する方法がわかる

内製化推進フロー

Webアプリケーション診断の流れ



Webアプリケーション診断は大きく３つのパートに分けられます。
一連の作業のなかで診断ばかりに目が行きがちですが、内製化成功のカギはその前後の作業である診断体制の整備・診断後の対応にあります。
以降のページで、各パートごとに解説していきます。

STEP 1 診断体制を整える

診断対象の選定

ネットワークに接続しているWebサイトは、提供しているサービスによらず全て診断対象に含めることを推奨します。
Webサイトの重要度や更新頻度などに応じて、診断の優先度や診断実施ルールを決めていきましょう。

診断対象例

STEP 1 診断体制を整える

診断実施ルールの整備

選定した診断対象ごとに、診断実施ルールを決めます。
最低限決めておくべきルールとして以下の３つが挙げられます。

診断の頻度	：	リリースの都度／定期（年１回など）
診断の範囲	：	新規・改修画面／一部画面のサンプリング（※1）／全画面
診断手法	：	ツール／手動（※2）

※1　ログインや決済など一部機能を選ぶ方法。どの画面にも同等に攻撃されるリスクはあるので、選定の手間を考えると全画面の診断がお勧めです。
　　高度な自動巡回機能を保有するツールを利用すると、人手をかけることなく簡単に全画面の洗い出しが可能です。
※2　二要素認証を必要とするログイン機能などは、ツール診断が難しいため手動診断をお勧めします。

STEP 1 診断体制を整える

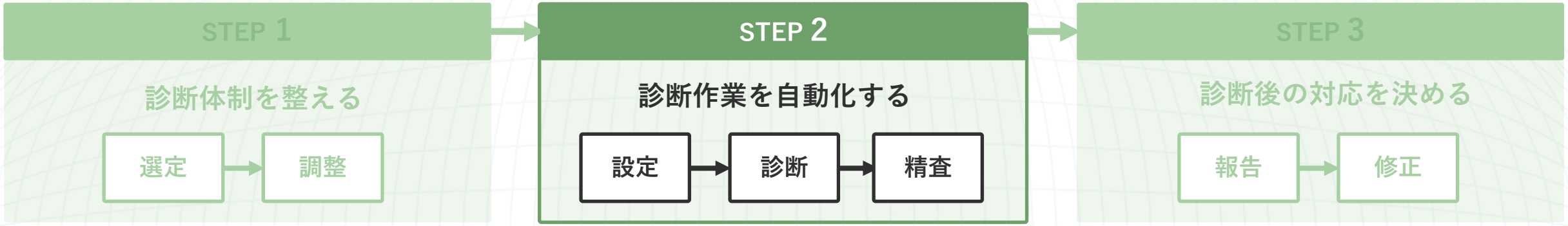
診断実施ルールの整備

診断実施時はWebサイトへの大量アクセスが発生するため、関係者に周知や確認を行います。
特に運用中の本番サイトでは、業務影響が出ないよう事前の確認や調整が必要です。

診断実施環境	：	本番サイト（運用中）／本番サイト（公開前）／開発環境
データ削除機能	：	無／有（※1）
メール送信箇所	：	無／有（※2）

※1　診断により、データ削除の可能性があります。ツール診断対象から除外し、手動診断など他の方法での脆弱性チェックをお勧めします。
※2　大量にメールが送信される場合があります。診断によるメールと分かるよう、テストなど特定の文言を含める・メール受信担当やサーバ管理者に連絡しておくなどの調整が必要です。

STEP 2 診断作業を自動化する



診断の設定

ツール選定ポイント：ツール設定のしやすさ、自動巡回してくれるか

診断対象画面をツールに設定します。必要最低限のデータを登録すれば自動で巡回・診断でき、人手による作業を減らしてくれるツールを選定すると良いでしょう。

診断実施

ツール選定ポイント：診断項目の網羅性、CIツール連携の可否

ツールによる診断を実施します。診断の設定が正しくできていれば、ツール任せにすることが可能です。ただし、ツールにより診断項目が異なるため、
診断すべき項目が適切に含まれているか確認しておきましょう。また、診断の頻度が高い場合、CIツールから自動実行できるかなど、活用のしやすさも重要です。

診断結果の精査

ツール選定ポイント：検知性能、判定方法のわかりやすさ

ツールが検出した脆弱性を確認します。専門家によるチェックを前提としたプロ向けツールでは過検知（※）の傾向があり、脆弱性かどうか判断できるセキュリティエンジニアが必要です。内製時の負荷を下げるためにも、ツールの検知精度や判定のわかりやすさを重視すると良いでしょう。

※脆弱性を攻撃する操作はできないものの、脆弱性が存在するときに似た挙動を示した場合に、可能性の示唆として報告されることを指します。

STEP 3 診断後の対応を決める

対応ルールの整備

脆弱性が検出された場合の対応ルールを決めます。すべての脆弱性を直ちに修正することは難しいため、想定される脅威をもとにコストや影響度などを考慮して判断します。

	脆弱性の深刻度	対応方法の例	脆弱性に対して想定される脅威
対応例	Critical	即時修正	• 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	1ヶ月以内に修正	
	Medium	• 利用頻度が高い機能　3ヶ月以内に修正 • 上記以外、または再現性が低い場合　次回リリースまでに修正	• 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	• 再現性ありと判断できる場合　次回リリースまでに修正 • 再現性が低い場合　リスク保有(次回診断まで様子見)	• 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	リスク保有（次回診断まで様子見）	

STEP 3 診断後の対応を決める

上位層向け（管理部門、委託元企業など）

○ 脆弱性のリスク

ツール選定ポイント： リスク評価にCVSSが用いられているか

まずは脆弱性のリスクを明確にしておく必要があります。脆弱性の深刻度を評価するためのCVSSという指標を利用すれば、誰でも簡単に脆弱性の一般的なリスクを把握することが可能です。

○ 自社システムへの影響

ツール選定ポイント： 脆弱性や攻撃リスク説明のわかりやすさ

自社システムにどのような影響があるか判断できる情報も必要です。
ツールを選ぶ際は、脆弱性の詳細な内容や攻撃された場合のリスクがわかりやすく説明されているかを確認しておきましょう。

開発向け（開発部門、外部委託先など）

○ 脆弱性のリスク

ツール選定ポイント： 診断ログなどの詳細情報が閲覧可能

脆弱性を修正するためには、どの画面でどのような操作により脆弱性を検出したか確認できる仕組みや、詳細な診断ログが開示されていることが重要です。

STEP 3 診断後の対応を決める

修正結果の確認

○ 脆弱性検出箇所のみ再診断を実施

ツール選定ポイント： 脆弱性を検出した箇所だけ再診断できるか

脆弱性が適切に修正されているか、再診断を実施して確認します。
診断を最初からやり直す方法だと、検出時と診断方法が異なる可能性があるので、検出した箇所のみ再診断できることが望ましいです。

脆弱性の管理

○ 脆弱性のリスク

ツール選定ポイント： タスク管理機能が提供されているか

脆弱性診断は、診断の実施・脆弱性の報告・修正依頼や結果確認と複数のフェーズに渡る作業であり、ステークホルダーも多岐にわたります。特に開発を外部に委託している場合は社外とのやり取りも発生するので、コミュニケーションコストの増大や、対応の属人化といった問題に繋がりかねません。
人手による作業を軽減するためにも、脆弱性の対応状況を把握できるようなタスク管理機能を利用すると良いでしょう。

最後に

作業はAIに任せて、
セキュリティ対策を高度化しよう

- Webセキュリティの知識や、Webアプリの開発経験がなくても、
  Webアプリケーション診断の内製化は可能です。

- AeyeScanでは、手間のかかる巡回作業やツール設定を自動化することで、
  いつでも誰でも簡単に、高精度なWebアプリケーション診断ができる
  サービスを提供しています。

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
100社以上

※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）

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
近鉄情報システム株式会社
ドリームインキュベータグループ
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
エムティーアイ
OZINTERNATIONAL
COACH A Co.,Ltd.
cybozu
JINSOKEN
Schoo
Speee
ZENKIGEN
Direct Sourcing
TAL
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
hokan
Money Forward
RUN.EDGE
RVSTA
Rescuenow

SI・IT企業

Rworks
アクモス株式会社
AVANT GROUP
CTC
Insight Edge
Infcurion
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
SOFT CREATE
SOLTEC
電通総研
TOPPAN
JOPS
NHC
Human Interactive Technology inc.
FUJISOFT
FUJITSU
MITSUBISHI ELECTRIC
YONA
リピスト

セキュリティ企業

NEC NECセキュリティ
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

導入事例紹介

エイチ・アイ・エス 様

企業名　株式会社エイチ・アイ・エス

事業内容　総合旅行会社

従業員数　10,849人（2023年6月時点）

課題

セキュリティの内製化が困難。
診断の外注コストを削減したい

具体的な課題

1. 社内からの診断依頼が増え続けていた
2. 診断対象が多く外部委託せざるを得ない
3. 外注による診断コスト増

内製・外製含め100を超えるWebアプリケーションがあり、内部の体制だけでは全ての診断実施に対応できず、一部を外部に委託。コスト削減と体制整備が課題だった。

導入

情報処理推進機構（IPA）の検証結果と
「7割以上自動化」という点が決め手

導入の背景

1. 手動の診断では対応が追い付かず自動化を検討していた
2. 自動化できても性能が落ちない製品を探していた

手動作業を伴う診断では対応が困難になり、診断の自動化を検討。AeyeScanは、IPAの検証結果が高評価だったことと、「7割以上の自動化が可能」という点が決め手で導入。

効果

診断・レポート作成工数を大幅に削減。
さらなる内製化比率の向上を目指す

具体的な効果

1. 診断の大部分を自動化し工数を削減
2. レポート機能により大幅に時間を短縮
3. リリース前に診断と脆弱性改修が完了

「脆弱性が発覚しても、リリースまでに修正が間に合わない」という悩みも解消され、脆弱性を潰してからアプリをリリースできるように。

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人（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） セキュリティ診断クラウドサービス「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	36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。