



セキュリティ担当者に読んでほしい

やさしいWebサイトの
セキュリティ基礎ガイド

AeyeSecurityLab

はじめに

Webサイトは今や企業活動に欠かせないツールですが、
セキュリティ対策が不足しているケースも少なくありません。
セキュリティを強固にするため、また効率よくセキュリティ対策するためにも、
Webサイトの運営形態に適したセキュリティ対策を検討する必要があります。

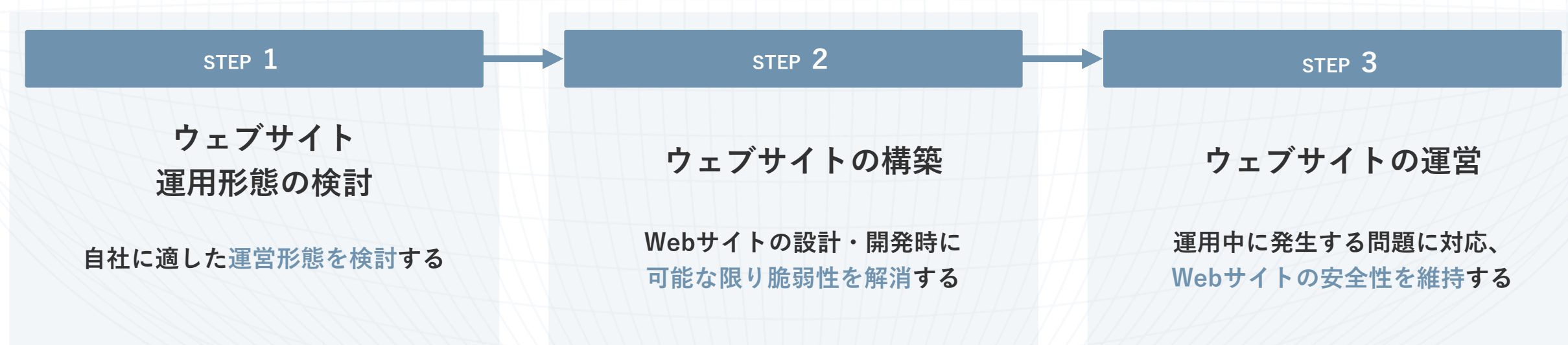
本資料では、誰もが簡単にWebサイトのセキュリティ対策に取り組めるように
セキュリティのプロがポイントを絞ってご説明しています。

ぜひ本資料のもと、**自社に必要なセキュリティ対策を実施**してください。

Webサイトのセキュリティ対策は3つの段階で考える

世界中の誰でも簡単にアクセスできるWebサイトは、攻撃の対象となりやすく、個人情報の漏えいや不正サイトに誘導するなどの改ざんにより、自社だけではなく利用者にも被害が発生することが想定されます。

そのため、**IPAでは以下3つの段階に分けてセキュリティ対策を検討することを推奨**しています。



Webサイト運営形態の検討

まず最初の段階として、運用形態を決めます。Webサイトを稼働させるサーバなども検討対象です。自社で行うのか外部委託するのかにより、どのようなセキュリティ対策をするのかが変わってきます。

運用形態	特徴
オンプレミス	Webサーバやネットワークの用意、Webサイトの構築・運用まで自社で行う
SaaS	Webサーバやネットワークは外部サービスを利用し、Webサイトの構築・運用は自社で行う
ASP	Webサイトの開設から運用に至るまで外部サービスを利用する

！ ココがポイント

セキュリティ対策を実行する人が異なるだけで、Webサイトの安全性を高める上で押さえるべきポイントは全て同じ。

Webサイトの構築

「安全なウェブサイトの作り方」を参考にすることで、自社開発でも外部委託でも同じ観点でセキュリティ対策が可能です。



IPA 安全なWebサイトの作り方

PDFは[こちら](#)

- ✓ IPAへの届出件数が多い脆弱性を取り上げている
→ 攻撃されやすい脆弱性とその対策方法がわかる！
- ✓ 脆弱性の原因そのものをなくす根本的な解決策だけでなく、
攻撃による影響の低減を期待できる保険的対策も紹介されている
→ リスクレベルに応じた適切な対策が選べる！
- ✓ セキュリティ実装の実施状況を確認するためのチェックリストなども付属している
→ Webサイト開発現場ですぐに使える！

！ ココがポイント

「安全なウェブサイトの作り方」およびチェックリストを活用することで、自社での開発だけでなく外部サービスを利用する場合も、
同じ観点で確認可能。

Webサイトの運営

IPAは「**安全なウェブサイトの運用管理に向けての20ヶ条**」を発表し、Webサイトを安全に運用するための指針を掲げています。

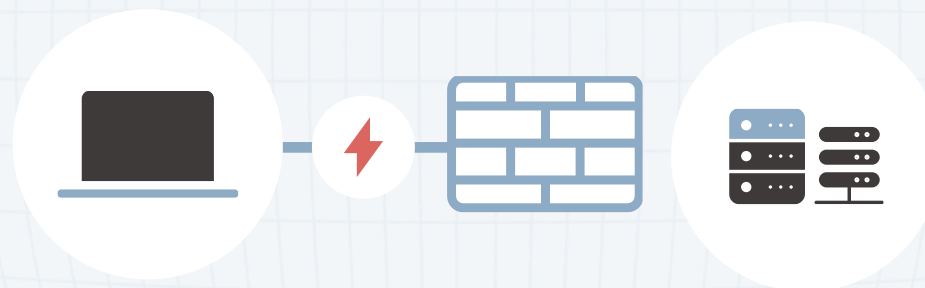
ウェブサイトのセキュリティ対策のチェックポイント

CHECK 01

ウェブアプリケーションのセキュリティ対策

CHECK 02

ウェブアプリケーションが稼働しているウェブサーバのセキュリティ対策



CHECK 03

ウェブサーバが設置されているネットワーク(ルータやファイアウォール)のセキュリティ対策

CHECK 04

その他のセキュリティ対策

！ ココがポイント

Webアプリケーション、Webサーバ、ネットワーク、その他と**4つのカテゴリで20ヶ条の項目を満たさなければならない**。対策がとられていない項目があった場合、早急な対策が必要。

20ヶ条は脆弱性診断一つで達成が目指せる

一つひとつの対応は大変そうに見えるけれど、押さえるべきポイントは同じ。

脆弱性診断で主要な項目は対策できます。

ウェブサイト
運用形態の検討

ウェブサイトの
構築

セキュリティ対策を自社で行うのか外部委託なのかで、
Webサイトの安全性を高める上で押さえるべきポイントは全て同じ

ウェブサイトの
運営

セキュリティ対策の
チェックポイント20ヶ条を
満たす必要がある。

脆弱性診断で対応可

Webアプリケーションのセキュリティ対策

運用形態	特徴	脆弱性診断での 問題発見
① ファイルの公開設定	一般に公開すべきでないファイルは非公開・削除する	☐
② Webページの公開設定	不要になったWebページは閉鎖する	☐
③ 脆弱性への対策	IPAの「安全なウェブサイトの作り方」に取り上げられている対策を実施する	☐
④ ソフトウェアの脆弱性対策	バージョンアップを始めとした脆弱性対策を実施する	☐
⑤ エラーメッセージ	エラーメッセージから設定情報が漏れる可能性があるため、メッセージ内容は必要最低限にする	☐
⑥ ログ管理	不審な動きにいち早く気付くためにログ管理を行う	
⑦ 暗号化	盗聴を防ぐために通信内容を暗号化する	
⑧ 不正ログインへの対策	安全なパスワードの設定など、不正ログインの防止対策をする	☐

| Webサーバのセキュリティ対策

運用形態	特徴	脆弱性診断での 問題発見
⑨ バージョンアップ	OS・ソフトウェア・ミドルウェアは最新状態に保つためにバージョンアップする	☐
⑩ 不要なサービス・アプリケーションの停止	悪用されるのを防ぐため、使っていないサービス・アプリケーションがあれば停止・削除する	☐
⑪ 不要なアカウントの削除	攻撃のきっかけとなるリスクがあるため、不要なアカウントは削除する	☐
⑫ 安全なパスワードの設定	安易なパスワードは解析されやすいため、推測されにくいパスワードを設定する	☐
⑬ アクセス制御	非公開のファイルを第三者に見られないように、適切なアクセス制御を行う	☐
⑭ ログ管理	Webサーバの故障や事故にいち早く気付くために、ログ管理を行う	

ネットワークのセキュリティ対策

運用形態	特徴	脆弱性診断での 問題発見
⑮ 不要な通信の遮断	ルータなどのネットワーク機器を使って、外部・内部の不要な通信を遮断する	☐
⑯ 通信のフィルタリング	ファイアウォールを使用し、通信のフィルタリングを適切に行う	☐
⑰ 不正な通信の検知・遮断	IDS／IPS・WAFを使用し、不正な通信を検知・遮断する	☐
⑱ ログ管理	ネットワーク機器のログを保管し、不審な動きがないか定期的に確認する	

| その他のセキュリティ対策

運用形態	特徴	脆弱性診断での 問題発見
①⑨ クラウドサービスの セキュリティ対策	クラウドサービスを利用する場合、サービス事業者が行っているセキュリティ対策を把握し、不足する対策は自社で対応する	○
②⑩ 脆弱性診断	対策漏れを防ぐために、webアプリケーション・Webサーバ・ネットワークに対して定期的な検査を行う	○

脆弱性対策

✔ セキュリティ対策のうち、脆弱性対策は継続が求められる

→ 継続できる仕組みや、コストを抑えるための方法を検討する必要がある

構築時

運用時

設計

構築中／完成

運用開始時

運用開始時／定期対応

- 安全なウェブサイトの作り方
- セキュリティ実装チェックリスト



必須条件

継続対応がマスト！

サーバ及び管理端末等で利用しているソフトウェアを最新の状態に

脆弱性診断の実施と、見つかった脆弱性に対する対策

脆弱性診断の実施は自動化・内製化がおすすめ

Webサイトの安全な運用に役立つ「脆弱性診断」は、
AIを活用すれば自動化・内製化できる。

メリット 01

継続的な診断による
セキュリティレベルの向上

メリット 02

Webサイトの
スピーディーな診断

メリット 03

脆弱性の早期発見

メリット 04

内製化による
コスト削減

メリット 05

対策に必要な
人材不足の解消

AeyeScan で効率的に Webサイトのセキュリティを強化しよう

Webサイトの安全性を高めるには、脆弱性診断を実施し、
IPAの「**セキュリティ対策のチェックポイント20ヶ条**」で
不足している対策を見直すと効率的にセキュリティを強化できる。

安全性を維持するには脆弱性診断を継続的に実施する必要があるため、
コストを抑えつつスピーディーに診断できる
「**AeyeScan**」で自動化・内製化するのがおすすめ。

 **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「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

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

×

ブラウザ上での直感的な操作

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

製造



インフラ



金融



メディア



人材・教育



エンタメ



Leverages

SaaS



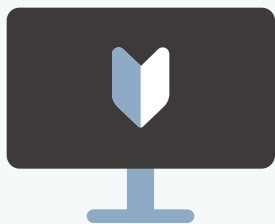
SI・IT企業



セキュリティ企業



| 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。

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つ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か？
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

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

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	43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		



IS 752963 /
ISO 27001



CLOUD 790050 /
ISO 27017





AeyeScan

セキュリティに、確かな答えを。