セキュリティ管理者向け

2024年10大脅威から読み解く

本当に効果的な対策とは

AeyeSecurityLab

AeyeSecurityLab

「情報セキュリティ10大脅威2024」から考える コスト効果の高い対策とは？

- 情報セキュリティ10大脅威とは
- 2024年の10大脅威と特徴
- とどまることを知らないクレジットカード情報の漏洩
- クレジットカード情報漏洩の事例とダメージ
- 高度化・複雑化したサイバー攻撃への対策
- 脆弱性診断の内製化ができる「AeyeScan」のご紹介・デモ
- 「AeyeScan」による脆弱性診断の内製化の成功事例

情報セキュリティ10大脅威とは

IPA(情報処理推進機構)が、前年度に発生した「社会的影響が大きかったと考えられる脅威候補」を選出。情報セキュリティ分野の研究者、企業の実務担当者など約200名からなる「10大脅威選考会」の審議・投票を経て決定した脅威ランキングのこと。

- 専門家だけでなく「現場の声」も反映されている
- セキュリティ対策方針の検討や見直しに活用できる

出典 https://www.ipa.go.jp/security/10threats/10threats2024.html

昨年に続き、2024年版も1位はランサムウェア

※2016年以降

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1位 →	ランサムウェアによる被害	2016年	9年連続9回目
2位 →	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3位 ↑	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4位 ↓	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
! 5位 ↑	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6位 ↑	不注意による情報漏えい等の被害	2016年	6年連続7回目
! 7位 ↑	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8位 ↓	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9位 ↓	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
! 10位 →	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

出典 https://www.ipa.go.jp/security/10threats/10threats2024.html

すべての脅威が2年連続でランクイン、対策は進むも手口が高度化・複雑化

2024年の10大脅威と特徴

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
5位 ↑	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目

3年連続で順位が上がっている。2023年には過去最大のDDoS攻撃が行われた。

ゼロデイ攻撃とは？

OSやソフトウェアに脆弱性が発見・公開されてから、それに対応する修正プログラムが提供されるまでの間に、公開された脆弱性を悪用して行われるサイバー攻撃。

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
7位 ↑	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目

一時圏外に落ちるも4年連続ランクイン。2023年は断続的/継続的な攻撃が見受けられた。

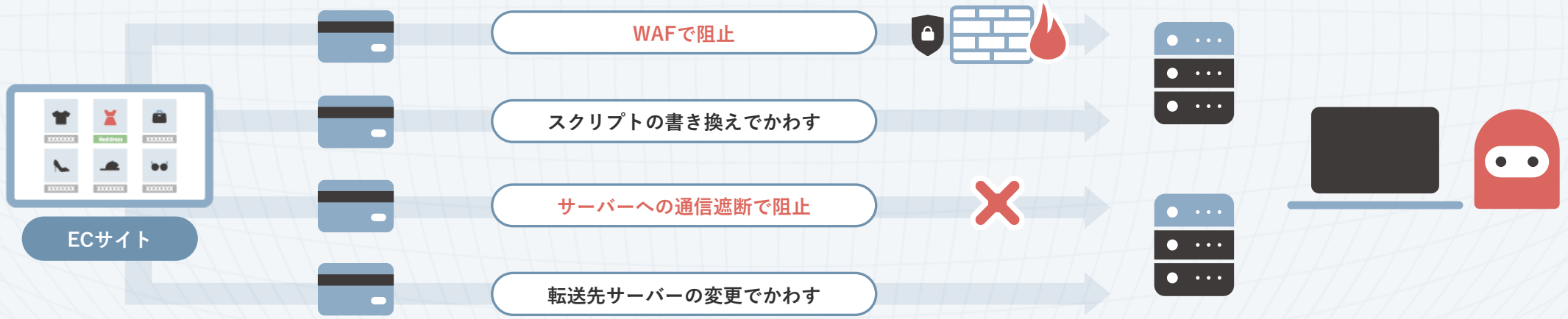
Nデイ攻撃とは？

OSやソフトウェアの脆弱性発見・公開後、それに対応する修正プログラムが発表されてから、適用されるまでの間に行われるサイバー攻撃。

とどまることを知らないクレジットカード情報の漏洩

第10位にランクインした「犯罪のビジネス化」の一例として、EC-CUBEの脆弱性を突いた攻撃が挙げられる。随時、セキュリティ対策をかわす方策が組織的に企てられている。

購入時に「利用者のクレジットカード情報を含む個人情報」を外部の攻撃者のサーバーへ転送する不正スクリプトの利用



簡単に攻撃できるツールや個人情報が、アンダーグラウンド市場で取引されている。

クレジットカード情報漏洩の事例

オープンソースのコンテンツ管理システムを用いて構築されたECサイトは、
個人情報を窃取する不正プログラムを埋め込む「Webスキミング」の被害に遭いやすい傾向にある。
脆弱性を放置したままの運用などは危険が大きい。

Webスキミングによる被害事例

2022年6月7日
洋菓子製造・飲食店経営企業

スイーツを主に販売するオンラインショップにて、
7,645件のクレジットカード情報が漏洩。

クレジットカード情報を保有していなかったが、ECサイト上のシステムの一部の脆弱性をついたことによる第三者の不正アクセスにより、ペイメントアプリケーションの改ざんが行われた。

ココがポイント

クレジットカード番号の保持・非保持にかかわらず対策は必須。

AeyeSecurityLab

クレジットカード情報が漏洩した場合のダメージ

どのようなリスクがあるのか

ECサイトの停止に伴う売上損失

- 長期間の閉鎖
  (平均8.6ヶ月※1)
- 多額の売上損失
  (最大1億円以上※1)

事故対応費用

- 事故対応費用の平均額
  (平均2,400万円※2)
- 賠償リスク
  (クレジットカードの再発行手数料含む)

ECサイト閉鎖やSaaSサービスへの移行による事業縮退

- 52%が自社構築を断念しSaaSへ移行
- 14%がECサイトの運営を停止

被害企業のうち34%が、追加予算をかけてセキュリティ対策を実施。

※1 ： 被害にあったECサイト47社を対象とした調査によると、1社あたりのECサイトの平均閉鎖期間は、8.6か月間（個人情報保護委員会が実施した「ECサイトへの不正アクセスに関する実態調査」より
https://www.ppc.go.jp/files/pdf/ecsite_report.pdf）
※2 ：事故対応費用の平均額は、IPA が実施した「EC サイトのセキュリティ対策のための調査業務」による、最近被害を受けた19 社を対象とした場合の集計結果（IPA「ECサイト構築・運用セキュリティガイドライン」より）

高度化・複雑化したサイバー攻撃への対策

IPAが提示する「情報セキュリティ対策の基本」

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導(罠にはめる)	脅威・手口を知る	手口から重要視すべき対策を理解する

ココがポイント

「攻撃の糸口」は似通っており、「情報セキュリティ対策の基本」を
継続的に実施することで、被害に遭うリスクを低減できる。

高度化・複雑化したサイバー攻撃への対策

さらにIPAは、「情報セキュリティ対策の基本」の中で、複数の脅威に対して同時に効率的に行える対策として「共通対策」を提示している。

IPAが提示する「共通対策」

- パスワードを適切に運用する
- 情報リテラシー、モラルを向上させる
- インシデント体制を整備し、対応を行う
- 適切なバックアップ運用を行う
- メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
- 適切な報告/連絡/相談を行う
- サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

ココがポイント

脆弱性診断と脆弱性の解消は、WEBサイトを通してサービスを提供する以上、継続的に行わなくてはならない。

情報セキュリティ対策へのAI活用

AIの発展により、業務で活用できる幅は広がっている。

ChatGPTをはじめ、
0→1を生み出せる生成AIの台頭

RPAと組み合わせることで、
非定型業務も自動化が可能に

例えば、WEBサイトの
脆弱性診断の場合…

従来人手をかけて行っていた作業を、
AI＋RPAに処理させることができる

継続が求められる業務へのAI活用は、セキュリティ組織の成長にも寄与！

セキュリティ組織の
要因確保ができる

より高度で人間にしか
できない業務に集中できる

育成に、より一層
時間も費用も投資できる

脆弱性診断は、AIにより自動化しやすい分野

セキュリティ対策の中でも、特に「脆弱性診断」は、
WEBサイトを通じてサービスを提供する限り永続的に必要となるため、
AI活用による自動化・効率化（＝内製化）がおすすめ。

対応スピードアップ

コストダウン

情報や
ノウハウの社内蓄積

脆弱性診断の内製化を

成功 に導くAeyeScan

- いつでも誰でも診断できる環境をご提供 -

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）

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 / すかいらーグループ / Suzuyo / NTT東日本 / Looop

金融

アイフル / JOBPAY / SOMPOひまわり生命 / DMM FinTech / Tokyo Century

出版メディア

集英社 / 中日新聞 / NIKKEI

エンタメ

e+ 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 株式会社リバスタ

SI・IT企業

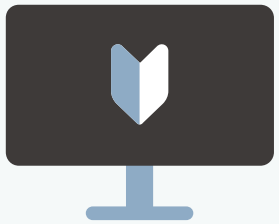
Rworks / アクモス 株式会社 / AVANT GROUP / CTC / Insight Edge / Infcurion / SB Technology / SBWorks / NTT DATA NTTデータ先端技術株式会社 / NTTビジネスソリューションズ / Globalway / circlace / さくら情報システム / CEC / tdi 情報技術開発株式会社 / Simplex Inc. / 777WORKS 株式会社スリーセブンワークス / SOFT CREATE / SOLTEC / 電通総研 / TOPPAN / JOPS / NI+C 日本情報通信株式会社 / Human Interactive Technology inc. / FUJISOFT / FUJITSU / 三菱電機インフォメーションネットワーク株式会社 / YONA / リピスト

セキュリティ企業

NEC NECセキュリティ / 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

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	33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。