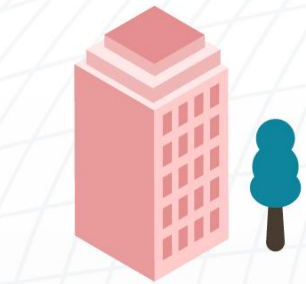
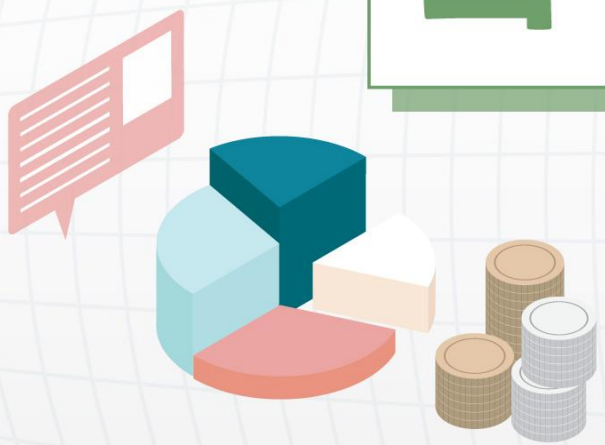
セキュリティは コストから 経営資源へ





DX&AI時代の事業を止めないサイバーレジリエンス戦略

AeyeSecurityLab

本資料の目的

DXの進展とAIの進化により、
サイバーセキュリティを取り巻く環境はこれまでにないスピードで変化しています。

ビジネスの多くがデジタル上で展開される今、サイバー攻撃はもはやIT部門だけの課題ではなく、
企業価値や事業継続に直結する経営リスクとなっています。

これからのセキュリティ対策には、「攻撃されることを前提」に、
迅速な復旧と継続的な強化を目指すサイバーレジリエンスの発想が欠かせません。
その実現の鍵となるのが、「CTEM（継続的な脅威エクスポージャー管理）」という考え方です。

本資料では、従来の対策から脱却し、
CTEMを取り入れてサイバーレジリエンスを強化するための道筋を解説。

特に、優先度が高いWebアプリケーションの脆弱性対策に焦点を当て、
AIを活用した自動化や、対策状況を一元的に可視化・最適化する方法もご紹介します。

単なる「考え方の解説」にとどまらず、実践的な進め方と運用管理のヒントまでを網羅。
経営層・セキュリティ部門・事業部門が共通の視点でセキュリティ強化を推進するために、ぜひご活用ください。

DX時代、サイバー攻撃は経営リスクに直結

事業とデジタルが一体化する中で、サイバー攻撃は企業全体を脅かす存在に

サービス停止が
事業停止に直結

コンプライアンス
違反リスク

ブランド価値
信頼の毀損

サプライチェーン
全体への波及

投資家・株主の
評価

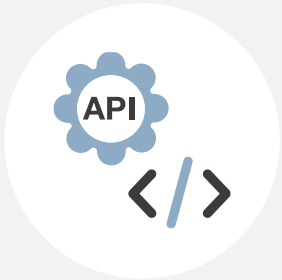
サイバー攻撃は増加の一途を辿り、顧客・社会からの信頼要求も高まっている

セキュリティは「コスト」ではなく、信頼獲得のための投資に

DXとAIの進化がもたらす脅威の拡大

DXの進展

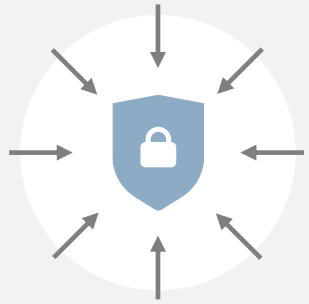
WebサービスやAPIの増加



攻撃対象や侵入口が急速に拡大

AIの進化

サイバー攻撃のコモディティ化



攻撃の自動化・高度化が進行

リスクが常態化する今、従来の“防御中心”の考え方では限界が…

攻撃を前提としたセキュリティ対策：サイバーレジリエンス

攻撃されても、業務やサービスを継続し、被害を最小化しながら素早く復旧できる体制が必要

NIST CSF 2.0のモデルと、対応する対策・ソリューション

ガバナンス（Govern）：経営層と戦略の統合

特定	防御	検知	対応	復旧
資産とリスクの 可視化	脅威の 侵入・拡散を阻止	脅威の早期発見 分析	インシデントの 迅速な封じ込め	事業継続の 確保
ASM、脆弱性管理 ID/アクセス管理	EPP/EDR、DLP ネットワーク セキュリティ	SIEM 脅威インテリジェンス	SOAR インシデント レスポンスサービス	

サイバーレジリエンス実現には
“防御中心”から“動的適応”への転換が必要

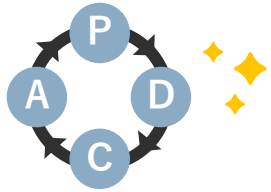
従来のセキュリティ対策

「守る」前提の防御中心の発想

定期更新や一時的な対策に依存

これからのセキュリティ対策

「攻撃を受ける」前提の継続的な見直し

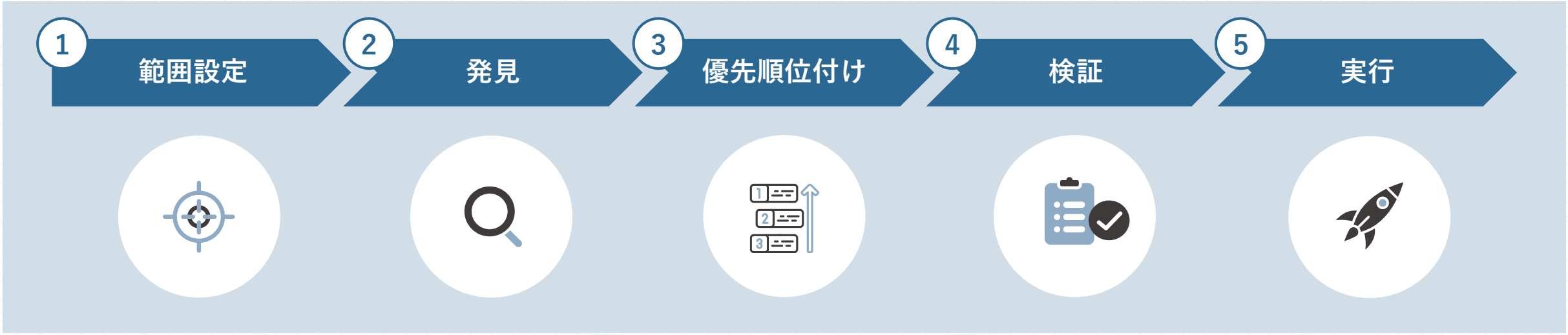


状況に応じて動的に最適化

この“動的適応”を実現するための具体的な仕組み＝CTEM

CTEM（Continuous Threat Exposure Management）とは？

Gartnerが2022年に提唱した「継続的な脅威エクスポージャー管理」の考え方で、
「どのリスクを、どの順番で、どの程度まで許容するか」を常に見直す仕組みを指す



ココがポイント

1. “継続的”な取り組みであること
2. “ビジネス観点”での評価・対応を行うこと

CTEMの発想に進化したセキュリティ対策とは？

従来型のセキュリティ対策	CTEM型のセキュリティ対策
1~3年に1回の診断に依存	継続的な通院・検査と日常的なチェック
技術観点でのリスク評価と優先順位づけ	ビジネス観点でのリスク評価と優先順位づけ
資産を守るために「閉じる」という発想	外に「開かれている」前提、攻撃される前提
IT部門がデジタル資産を一括管理できる	クラウド・Web・AIを誰でも使える(管理できない)
守るべき場所を絞って人手・予算を集中	全体をカバーするための自動化・内製化・分散化

セキュリティ＝コスト ←認識→ セキュリティ＝経営資源の最適配分

CTEMの実現を阻む、3つの壁

課題 1

リソースが不足し 継続的な可視化ができない

診断が年1回・四半期ごとなど断続的で
常に“最新状態”を把握できていない

課題 2

情報がバラバラで 優先順位付けが難しい

手段・部門ごとにデータが分断され、
本当にリスクが高い箇所が見えない

課題 3

対応が属人的かつ 手作業に依存している

対応の質が担当者の経験に左右され
進捗や対応ステータスが把握しづらい

要因は“人”に依存した断続的な運用

継続的かつ自動的にリスクを把握できる体制への転換が必要

AIを活用し、“人に依存しない”脆弱性対策へ

AI活用の脆弱性対策トータルソリューション

効率的・網羅的にリスクを発見し
脆弱性診断を自動化

AeyeScan

継続的な攻撃面の管理
脆弱性対策

×

人依存の課題が多い
脆弱性管理を仕組みで解決

AeyeCopilot

対策プロセスの可視化
一元管理

AeyeSecurityLab

AeyeScanとは？

AI・RPAの活用により、脆弱性診断を自動化するクラウド型Webアプリケーション診断ツール
自動巡回に優れており、人手をかけずに診断が可能

1
最短10分で診断開始
専門知識は不要！
SaaS環境なので24時間放置しておけます。

お客様

1 スキャン登録

3 結果レポート

AeyeScan

2 自動診断

Webサイト

3

診断結果レポートも自動生成
開発担当にすぐ渡せるレポートが簡単に出力できます。

2
画面遷移図を自動作成
AeyeScanがサイトを自動巡回、診断すべき画面を抽出して画面遷移図を生成します！

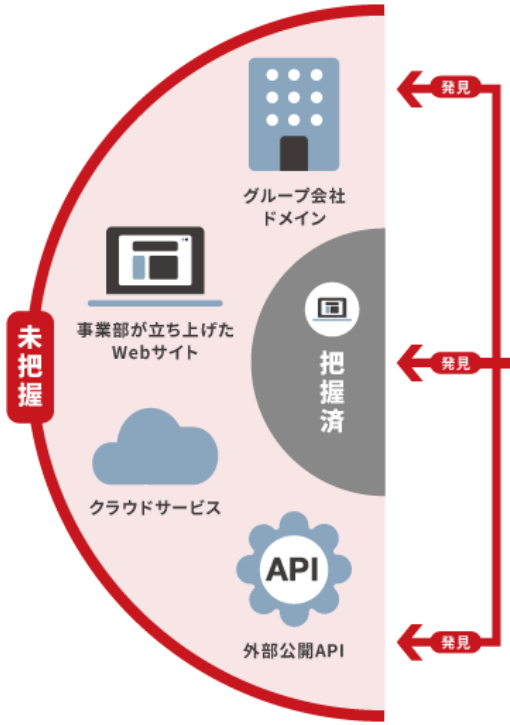
網羅的・継続的なリスクの見える化も支援

オプション機能

Web-ASMとは？

未把握な攻撃面の継続的な発見・リスク評価※

※リスク評価：AeyeScanのスキャンによる



特許取得実績のある
生成AI活用の技術により、
効率的・網羅的に攻撃面を発見。

生成AI

Web-ASMの実施ステップ

1 攻撃面の発見

Web-ASM機能

自社が保有している
ドメイン一覧を抽出

2 攻撃面の情報収集

自動巡回

未把握のドメインを
巡回対象に追加

3 攻撃面のリスク評価

脆弱性診断

管理対象の全ドメインに
脆弱性診断を実施

AeyeScan ひとつで、
より網羅的な脆弱性診断とリスクマネジメントが可能に！

AeyeCopilot

2025.11 RELEACE

脆弱性管理において陥りがちな課題を解決するセキュリティマネジメントプラットフォーム

経営層（CTO／CISO）

セキュリティ対策の最適化に
必要な情報が**把握できていない**

セキュリティ部門

個別案件やインシデント対応に追われ、
全体像の把握や情報収集まで**手が回らない**

事業／開発部門

コスト・納期を守ることが最優先で、
セキュリティは**後回し or 出来ていない**

人に依存する課題をシステムで “仕組み化”

全社のセキュリティリスクを把握
施策の投資判断ができる

セキュリティ情報を集約
先手を打った検討・支援へ

全社ポリシー・ガバナンスに準拠
セキュアなサービス開発を

確かな実績と技術力

すでに多くの企業で導入・実績を重ねてきたAeyeScanの技術・知見がソリューションの根底に

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「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）

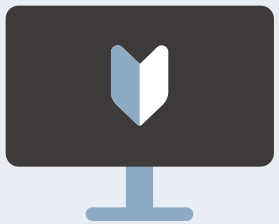
プロが認める品質・精度 × ブラウザ上での直感的な操作

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

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。

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
H.O RETAILING
NTT EAST
odakyu
近鉄情報システム株式会社
G-gio
SymEnergy
水ing Swing Corporation
Suzuyo
NANKAI 南海システムソリューションズ
日本調剤
HITOWA GROUP
grow up together MEDIA
Looop
Loyalty Marketing, Inc.

金融

アイフル
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

メディア

集英社
中日新聞
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

エンタメ

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

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア
Lexica E-Retailing Platform
estie
エアアンドエムマット株式会社
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 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.
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 株式会社スリーセブンワークス
SOFT CREATE
SOLTEC
高千穂交易株式会社
電通総研
TOPPAN
JOPS
JAST
NHC
PCNET 株式会社パシフィックネット
Human Interactive Technology inc.
FUJISOFT
FUJITSU
MACROMILL
三菱電機デジタルイノベーション株式会社
YONA
リピスト

セキュリティ企業

NEC NECセキュリティ
NTT DATA 株式会社NTTデータ先端技術
GSX GLOBAL SECURITY EXPERTS
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

AeyeSecurityLab

導入事例紹介

バトンズ 様

企業名　株式会社バトンズ

事業内容　M&A総合プラットフォームの企画・開発・運用

従業員数　122名（2025年2月時点）

課題

M&A・事業承継に関わる機密情報を
万全のセキュリティで守るため、
診断の高頻度化が必要に

具体的な課題

1. 外部ベンダーによる脆弱性診断はコストがかかる
2. 診断範囲の調整も入ることから、準備にかなりの工数を要する

プラットフォームの企画・開発・運用を行う中で、企業の極めて重要な機密事項を取り扱うことから、診断頻度を見直すことに。限られた予算やリソースの中で高頻度化を目指すべく、内製化を検討。

導入

外部の専門家に依頼するときと
同レベルの診断クオリティを評価

導入の背景

1. 業界標準のセキュリティ基準に準拠している
2. 自動巡回の精度が他社ツールより高い
3. 自動で画面遷移図が生成され、非エンジニアでもわかりやすい

経産省が示すセキュリティ基準や、OWASPアプリケーションセキュリティ検証標準を満たしている上、自動巡回の精度が高いことからAeyeScanを採用。効率的に診断が実施できるわかりやすさも評価。

効果

週1の定期診断と
新機能リリース時の即日診断を実現し、
サービスへの信頼度も向上

具体的な効果

1. 診断の高頻度化を実現
2. 脆弱性を検知した場合も即座に対応できるようになった
3. お客さまにサービスの安全性を客観的に示せるようになった

外注時は年に1回の診断だったが、毎週土日の定期診断と、新機能リリース時の即日診断が可能に。金融機関などのお客様にセキュリティ対策の実施状況も説明しやすくなり、サービスへの信頼度向上を実感。

AeyeSecurityLab

導入事例紹介

ミズノ 様

企業名　ミズノ株式会社

事業内容　スポーツ用品の開発・販売ほか

従業員数　3,584名（2024年3月31日現在）

課題

国内だけでも約20 Webサイトを運営する中、
定期的な脆弱性診断ができていなかった

具体的な課題

1. サイト立ち上げ時や大規模改修時だけしか診断ができていない
2. 外部ベンダーによる脆弱性診断だと多額のコストがかかる
3. 内部の人材のスキル不足・業務負荷が高くなる

グローバル全体でセキュリティポリシーを見直し、その中に定期的な脆弱性対策を含めたものの、外部ベンダーによる脆弱性診断だとコストがかかる。内製化を検討するもスキル不足や業務過多といった課題があることから、自分たちでも使える診断ツールの導入を検討。

導入

定額で複数サイトに外部ベンダーによる
脆弱性診断と変わらないクオリティの診断が
できると評価

導入の背景

1. 専門知識を持たなくても簡単に操作できる
2. サイト数に比例して費用が増加しない
3. 外部ベンダーによる脆弱性診断と同等の品質で診断できる

AeyeScanのトライアルを行い、簡単に操作できることを実感。また、同一サイトに対して、外部ベンダーによる脆弱性診断による診断とAeyeScanによるスキャンを並行して行いレポートを比較。AeyeScanの方が同レベル以上・検知項目が多かったことから、導入を決めた。

効果

定期的な診断が可能な体制が整った。
時間短縮により、
診断後の対策、チェックもスムーズに

具体的な効果

1. 内製化により、診断にかかる時間が数ヶ月単位から数週間に短縮
2. 診断、対策、チェックの運用がきれいに回せている
3. 開発ベンダーとのコミュニケーションもスムーズになった

外部ベンダーによる脆弱性診断では脆弱性への対応も含めて数ヶ月単位の時間がかかっていたが、数週間で診断を終えてすばやく対策できるようになった。レポートに具体的な修正方針も示されるため、開発ベンダーとのコミュニケーションもとれ、対策もスムーズになった。

AeyeScan / AeyeCopilot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

各ソリューションの 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
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	55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

AeyeScan

セキュリティに、確かな答えを。