

# 社会現象としての 「サイバー攻撃」と 経営戦略

-”あたりまえ”に攻撃される時代にもつべき目線とは-

# 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や各地での講演・エバンジェリスト活動にも携わる。

# 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。

# DXとAIが変えた サイバーセキュリティの「前提」

# DXの進展で「デジタル」が競争力の源泉＝差別化要素に

## 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

情シス・セキュリティ部門が推進し  
デジタルは事業を「支える」

## 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



### 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

事業部門が推進し  
デジタルが事業を「左右する」



# サイバーセキュリティが経営リスクに直結する

事業とデジタルが密接に関わり合うようになり、サイバー攻撃は事業全体への脅威に

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



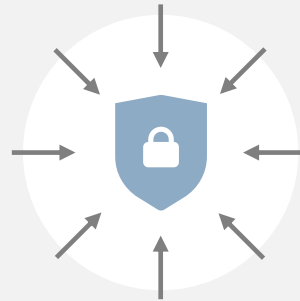
サイバー攻撃は増加の一途を辿り、顧客・社会からのセキュリティに対する信頼要求も強まっている。

**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**

# AIの進化により「攻撃される前提」でのリスク管理が重要に

## AIの進化

サイバー攻撃の  
コモディティ化



攻撃されるのが  
当たり前の世界へ



サイバー攻撃はもはや「**社会現象**」といえる

# 攻撃される前提のセキュリティ対策：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

資産とリスクの  
可視化

ASM、脆弱性管理  
ID/アクセス管理

防御

脅威の  
侵入・拡散を阻止

EPP/EDR、DLP  
ネットワーク  
セキュリティ

検知

脅威の早期発見  
分析

SIEM  
脅威インテリジェンス

対応

インシデントの  
迅速な封じ込め

SOAR  
インシデント  
レスポンスサービス

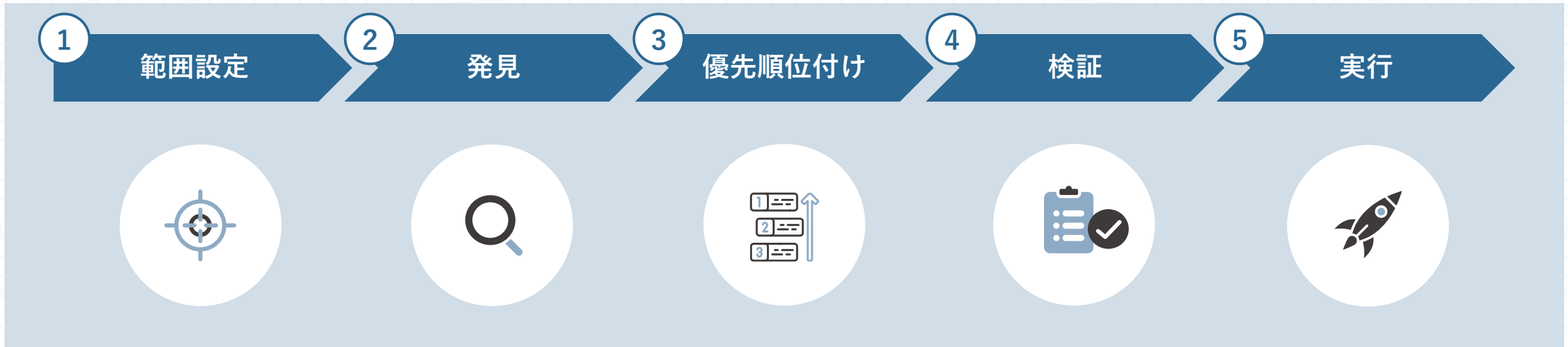
復旧

事業継続の  
確保



# 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。  
「**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。



## ！ ココがポイント

従来型の「守る」ことを主眼に置いた対策ではなく  
変化に対応し「**備え続ける**」ことが大切

# セキュリティ対策の“新”常識は「継続性」と「ビジネス観点」

## 継続的な管理・対策

恒常的な探索/発見・リスク診断・対応



## ビジネス観点の評価・対応

事業継続リスク・ビジネスインパクトと  
工数や予算の兼ね合いで優先順位づけ



IT部門だけで  
やるのは無理…



事業部門との  
**連携が必要！**



“全社体制” “経営視点で” セキュリティ対策を推進する必要

## | 全社で進めるセキュリティ対策の“目線”

### 対策実行

- 知識がなくても対策ができる自動化
- 継続的な診断と改善のサイクル
- 属人化しないナレッジ共有と環境

仕組み化・自走化

### 管理運用

- 全社のリスク・対策進捗の可視化
- コミュニケーションの自動集約
- 投資対効果（ROI）を意識した意思決定

可視化・最適化



# サイバーセキュリティの “新”常識に対応する第一歩



# | CTEMの実現と、サイバーレジリエンス強化を支援

エーアイセキュリティラボが提供するトータルソリューション

高度なAI活用により  
脆弱性対策の内製化を成功へ導く

**AeyeScan**

×

部門や役割、業務の違いを超えて  
情報・コミュニケーションをつなぐ

**AeyeCopilot**

継続的な攻撃面の管理・脆弱性対策

対策のプロセスを可視化・一元管理

# 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

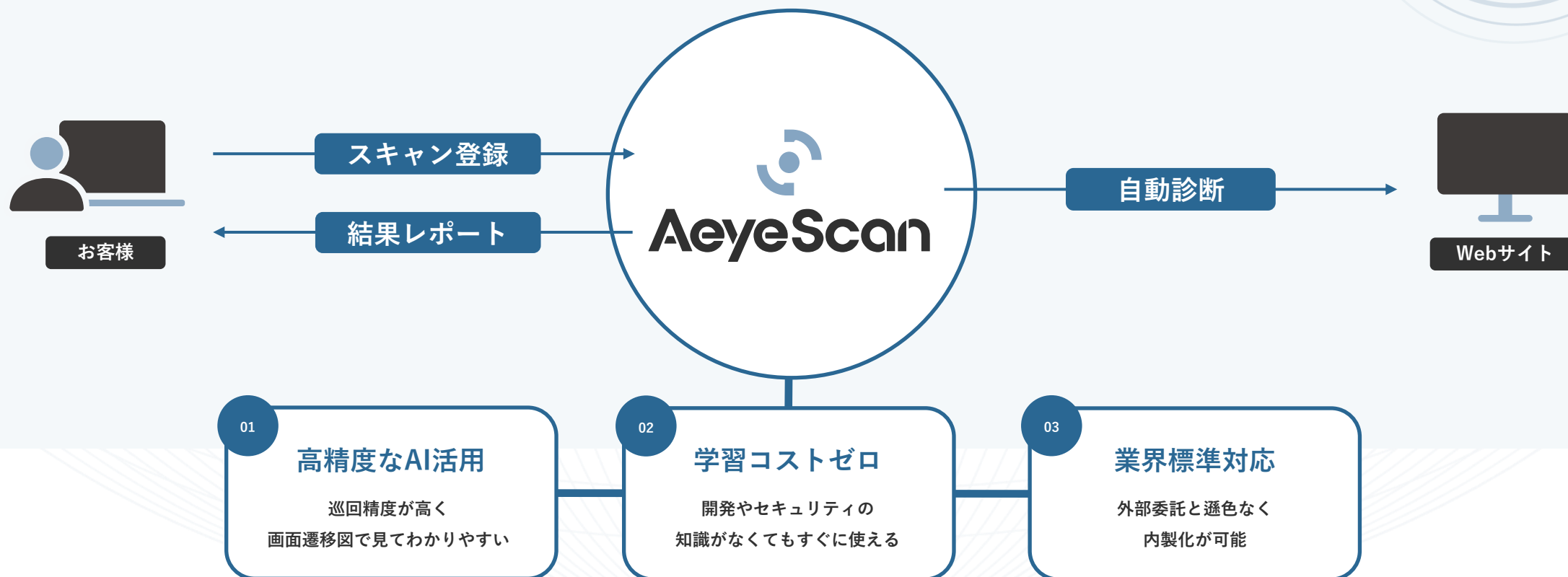
国内市場シェア

**No.1**※

※ 富士キメラ総研調べ「2024 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〉2023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）

有償契約  
300社以上



# | 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

### 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



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！

デモセミナーの日程を確認

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





# AeyeScan

セキュリティに、確かな答えを。