緊急解説セミナー開催！ 世界を止めたPHP問題

「PHPの重大脆弱性の衝撃とは？」

今、何が起きている？企業はどう備える？



日時
2026年10月23日（金）
15:30〜16:00

会場
幕張メッセ 2ホール奥
セミナー会場

参加方法
来場登録で聴講可能

AeyeSecurityLab

株式会社 エーアイセキュリティラボ
執行役員　関根 鉄平 氏

AeyeScan

【緊急解説】世界を止めたPHP問題

重大脆弱性の衝撃と、企業が今取るべき備え

©AeyeSecurityLab Inc.

登壇者紹介



株式会社エーアイセキュリティラボ

執行役員　**関根 鉄平** CISSP



発売中

セキュリティエンジニアとして大手金融機関等の脆弱性診断に従事。その後、Webアプリケーション検査ツール・サポートチームの立ち上げ、CSIRTや開発現場でのセキュリティ推進を経て、2020年6月より現職。
AeyeScanカスタマーサクセス責任者として診断の内製化を支援し、2026年度より開発責任者に就任。顧客の声を反映したプロダクトの進化を牽引している。
大規模イベント等の講演多数。『セキュリティエンジニアの知識地図』共著。

コミュニティ活動など

- 日本セキュリティオペレーション事業者協議会（ISOG-J）、OWASP Japan 共同ワーキンググループ
- 公益社団法人日本通信販売協会（JADMA）Web・セキュリティ専門部会
- 情報セキュリティ10大脅威 選考会メンバー

©AeyeSecurityLab Inc.

ととのう、セキュリティ

私たちは、AIの力でセキュリティ対策が無理なく回り続ける
仕組みを提供し、専門部門だけに頼らず、チームで安全を
支えられる状態をつくります。
本来の業務に集中しながら、事業が前に進み続ける世界を
実現していきます。

「ととのう、セキュリティ」の
考え方を動画で紹介しています



AeyeSecurityLab

©AeyeSecurityLab Inc.

世界を緊張させた『PHP緊急リリース』までのカウントダウン

2026年10月21日　0時頃

何者かにより2件のCVE番号が、誤った公開時刻と誤った深刻度（10点満点、実際は9.2）と共にHackerNewsへ投稿され、SNSなどで拡散される。この時点では、欠陥の技術的な中身は漏れていない。

同日　4時頃

PHPのコアに存在する重大な脆弱性（CVSS v4.0 スコア 9.2、通称「php2shell」）に関するリークを受け、PHP Groupが2026年10月21日 23:00 に修正パッチ公開の緊急カウントダウン予告を発表。

同日　5時頃

欠陥を報告したセキュリティ企業のCalifが、攻撃の実演動画を誤って一時公開。削除後もコピーがSNSで拡散される。

同日　16時頃

PHPを組み込んだソフトを配布しているChainguardが、公開の6時間以上前に修正済コンテナイメージを配布。

同日　23時前

サポート対象の全バージョン（8.2.35 / 8.3.36 / 8.4.27 / 8.5.12）へ修正パッチが一斉公開。

©AeyeSecurityLab Inc.

なぜこれほどの大騒動に発展したのか？

異例の事前予告

情報漏洩（リーク）に伴い
パッチ公開が事前に通知される



「タイムリミット型のカウントダウン」という極めて高い緊迫感が生じた

迫られるゼロアワー対応

「修正パッチ公開＝攻撃コード生成」という共通認識



パッチを当てる前にやられる等の恐怖心を煽る予測が拡がった

圧倒的な影響範囲

Webサーバーの多くで稼働しており企業規模問わず対応が発生



2024年にも公表から24時間以内に攻撃された前例があり、対策不可避の状態であった

©AeyeSecurityLab Inc.

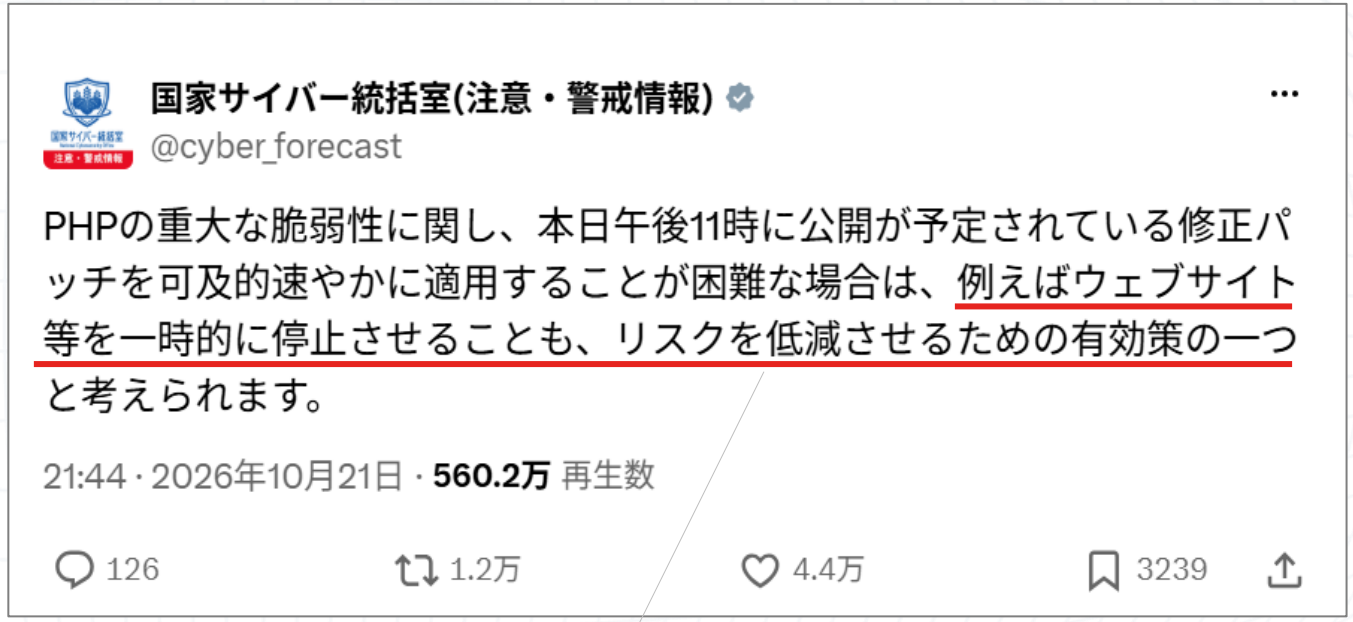
騒動のおかげで「サービスを止める」という選択肢が認められた

従来

サービス提供時間外
でのパッチ適用

今回

パッチ適用までの
時間稼ぎとして
「予防的停止」を推奨

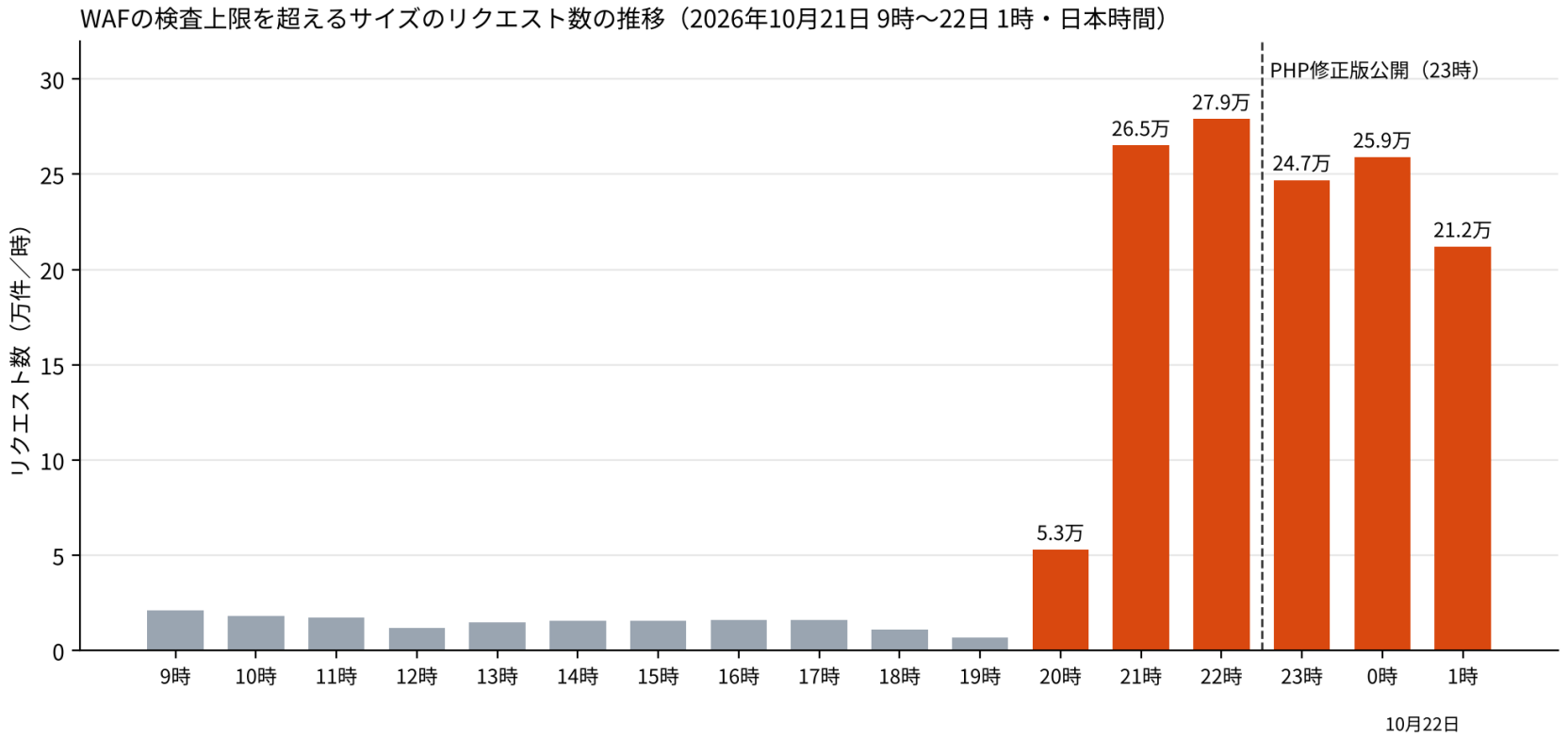


政府機関も『リスク低減のための有効策』と明言

©AeyeSecurityLab Inc.

10月21日夜、現場で実際に起きていたこと

パッチが公開される前から、脆弱性を狙ったとみられる通信・スキャン活動が観測された。



出典：株式会社サイバーセキュリティクラウド観測データ（1時間ごとの集計・概数）

©AeyeSecurityLab Inc.

技術的な観点からみた今回の状況

「大きな問題ではあるが、攻撃の成立条件が厳しく、容易に悪用できる攻撃手法が確認できていない」という状態

OSの防犯機能（ASLR等）

メモリ破壊をRCEにつなげるには、精密なメモリ操作やASLRなどの防御機能の回避が必要で、攻撃手法は実行環境に左右される。

参考：Red Hat Security Advisory (CVE-2026-109618) / GitHub 9bie PoC解析

攻撃の汎用化が難しい

稼働環境や、メモリ消費量のタイミング調整が必要となり、全自動で無差別攻撃を行う「汎用ワーム型ツール」の作成難易度が極めて高かった。

参考：Google Cloud Security Blog / Red Hat Vulnerability Statement

事前に懸念されたような「すべてのPHPサイトが直ちに侵害される」状況ではなかった

©AeyeSecurityLab Inc.

今回の騒動が残した「教訓」

今回の経験から見えたことは、パッチ適用までの時間を稼ぐ『多層防御』と『当たり前の脆弱性対応』という王道の対策の重要性と言える。

Good

サービスを一時停止して安全を確保する「予防的停止」という選択肢が認められた



Bad

パッチ公開前の「情報リーク段階」で、高度な意思決定と判断が現場に要求された



©AeyeSecurityLab Inc.

今後同様のことが発生した場合の確認ポイント

1. 体制（Who）
   対応の主管部門・責任者は明確だったか？
2. 検知（When/Where）
   いつ、どこから脆弱性の開示予告を入手したか？
3. 特定（What）
   対象システム（PHP利用状況・公開範囲など）の棚卸しは迅速に行えたか？
4. 防御（How）
   パッチ公開までの時間をどう凌いだか？（アクセス遮断・緩和策の判断と実行）
5. 収束（Result）
   いつ恒久対応（パッチ適用・検証）が完了したか？

©AeyeSecurityLab Inc.

今後のセキュリティ対策

©AeyeSecurityLab Inc.

現場を襲う、終わりのない「判断」と「対応」

アラート対応

どこまで無視していい？

脆弱性対応

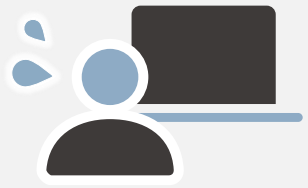
自社環境で本当に危ない？

優先順位づけ

どこまでやれば合格？

説明責任

「安全です」と言えるか？



事業継続

サービス止めてまで直す？

次から次へと「正解のない」判断を迫られ「無理して」対応している

©AeyeSecurityLab Inc.

守り手が疲弊する、終わりのない苦行

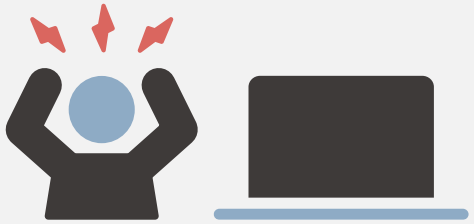
攻撃者は「AI」で武装し、低コストで攻撃を続けるが、我々は限られた「人手」で、増え続ける穴を塞ぎ続けるしかない。もはや、従来型の防御は限界を迎えている。

攻撃者



AIによる攻撃の
「自動化・高度化」

企業



リソース不足と
「対応範囲の肥大化」

脆弱性対策の継続的な運用はますます困難な状況に
しかし、人手・予算はなかなか増えない

AeyeSecurityLab

だからこそ、『無理のない脆弱性対応』を仕組み化する時代へ

例）脆弱性管理のプロセスを仕組み化する場合

判断を「分解」する

リスクを3つの構成要素に分解

- 悪用可能性（Exploit）
- 到達可能性（Exposure）
- 事業影響（Impact）



判断を「形式知化」する

CVSSのほか、業務文脈をルール化

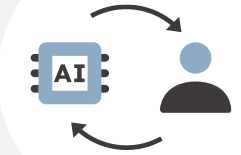
- ビジネス観点の重要度は？
- システム停止時の影響範囲は？
- 業務継続の代替手段はある？



判断を「仕組み化」する

AIと役割分担し、人は戦略に注力

AI	人間
• 情報収集 • 情報整理 • 反復作業	• 例外処理 • 経営判断 • 仕組みの設計



©AeyeSecurityLab Inc.

「無理なく」脆弱性対策を強化するなら！

©AeyeSecurityLab Inc.

AeyeSecurityLab

AIとの協働を実装する
クラウド型Webアプリケーション脆弱性診断ツール「AeyeScan」

属人的な「作業」をAIが担う「仕組み」へ。
持続可能なセキュリティ運用の仕組みをご提供します。

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！

©AeyeSecurityLab Inc.

AeyeScanで実現する、AIと人の協働

AIをセキュリティ運用に生かすには、専門知識や適切な運用設計が必要です。
AeyeScanは、専門家の知見を取り入れた診断プロセスを、使いやすい仕組みとして提供します。

“素(す)”のAIを使う



- とりあえず使う
- 判断基準が曖昧
- 業務文脈が不足

高度な専門性が必要で
判断品質がばらつく

AeyeScanによる仕組み化

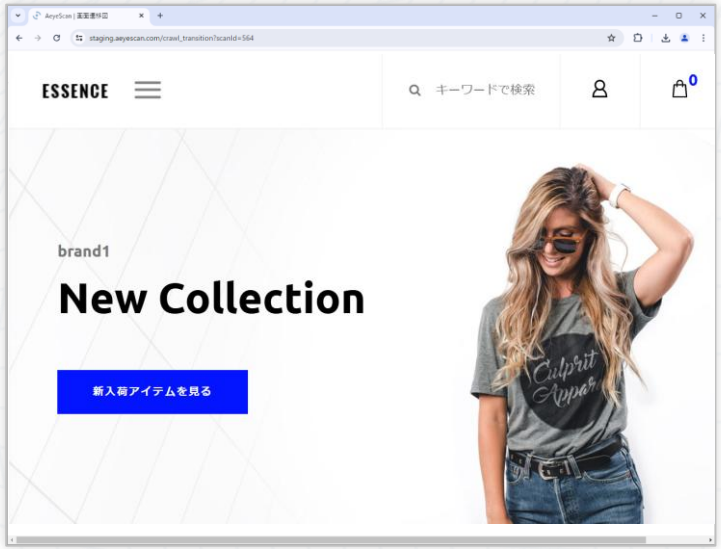
AeyeScan

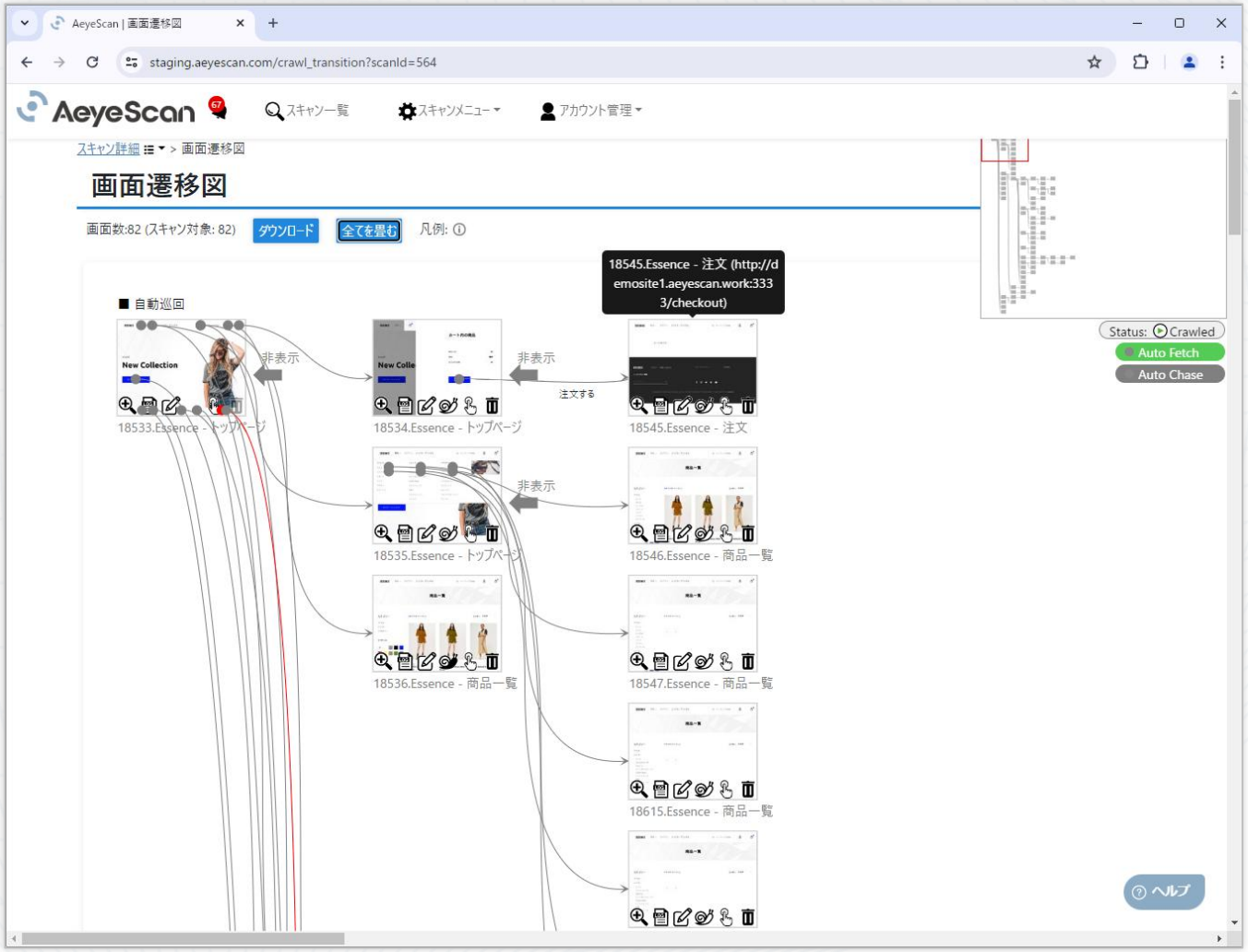
- 画面遷移図でサイト構造を可視化
- AIが診断作業を自動化
- 専門家の知見を診断プロセスに反映

いつでも・だれでも・すきなだけ
診断できる安定した運用を支援

©AeyeSecurityLab Inc.

巡回時に、自動で画面遷移図を生成





©AeyeSecurityLab Inc.

AeyeSecurityLab

結果がわかりやすく、すぐさま修正作業に取り組めるレポート





©AeyeSecurityLab Inc.

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 Inc.

AeyeScanが選ばれている理由

誰でも使える操作性 × プロが認める機能・性能

©AeyeSecurityLab Inc.

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

インフラ※

EPARK / AIRE / HIS / NTT EAST / odakyu / 近鉄情報システム株式会社 / GEO / SymEnergy / 水ing / Suzuyo / TOYOTA HOME / NANKAI / 日本調剤 / JARMeC / HITOWA GROUP / BOOK-OFF / ベルーナ / MEDIA / Looop / Loyalty Marketing, Inc.

エンタメ

イープラス / CAPCOM / GungHo / とらラボ! / BookLive

メディア

集英社 / 中日新聞 / 東海テレビ / NIKKEI / Media Do

製造

AICA / AISIN / KITZ / KOSÉ / SAKI / TIGER / TEIJIN / Denkei / House / Mizuno / ユーグレナ

金融

アイフル / UPSIDER / MS&AD / JOBPAY / SOMPOひまわり生命 / DMM FinTech / Tokyo Century / Net Protections

人材・教育

OHSAWA DRIVING SCHOOL / 河合塾 / Junion / JINSOKEN / ZENKIGEN / Direct Sourcing / PERSOL / 立教大学 / Leverages / workport

SaaS

Advanced Media, Inc. / Lexica / M-aid / エムティーアイ / OZ INTERNATIONAL / giftee* / Classi / COACH A Co.,Ltd. / cybozu / Speee / SecureNavi / Diamond head / DMM Boost / TAL / Digital Garage / TEMONA / NAVITIME / KNOCK ON THE DOOR / BATONZ / VALUE HR / freee / vector / porters / hokan / Money Forward / RUN.EDGE / RVSTA / rescuenow

SI・IT企業

Rworks / アクモス株式会社 / AVANT GROUP / Insight Edge / Infcurion / 80&Co. / SBWorks / NTT Integration / NTT DATA / NTTビジネスソリューションズ / OMRON / Globalway / KDDI Agile Development Center / circlace / さくら情報システム / SUNDAY SYSTEMS / CEC / GA TECHNOLOGIES / Simplex Inc. / 777WORKS / SOFT CREATE / SOLTEC / 高千穂交易株式会社 / TDI / 電通総研 / TOPPAN / JOPS / AST / PCNET / Human Interactive Technology Inc. / FUJISOFT / FUJITSU / MACROMILL / MITSUBISHI ELECTRIC / YONA / リピスト

セキュリティ企業

NEC NECセキュリティ / NTT DATA / GSX / cybertrust / LAC

※公共および社会・生活基盤までを包含

社名五十音順（導入いただいた企業様の一部です）

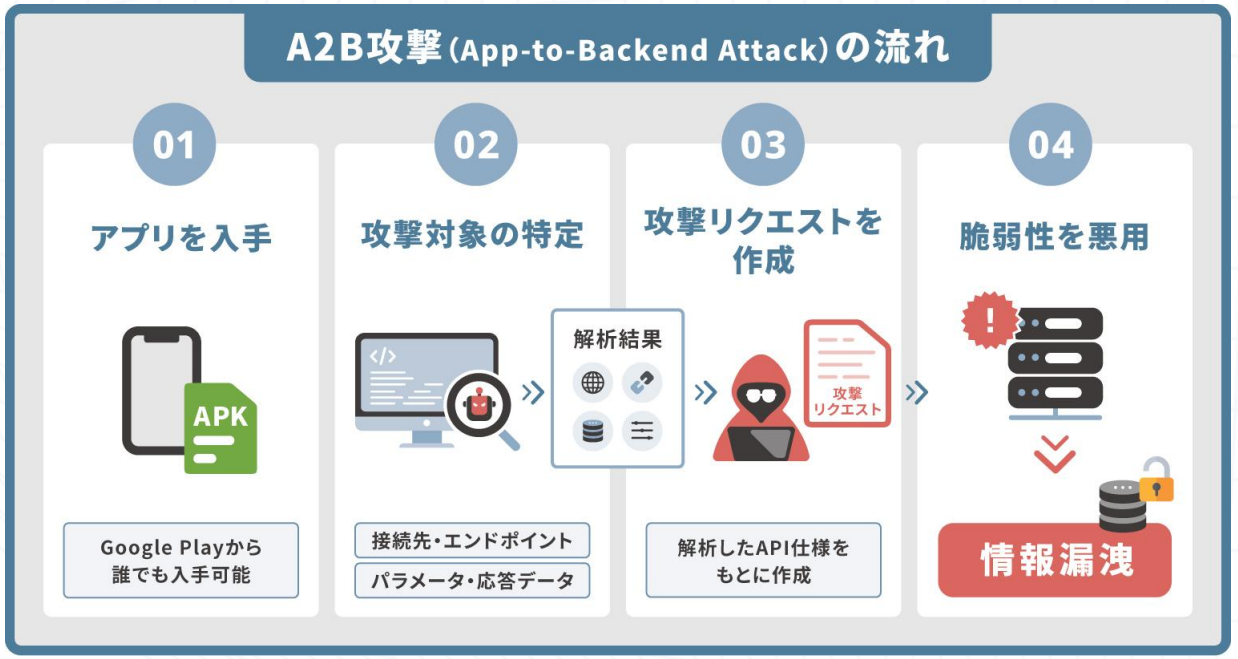
会社名及びロゴは各社の商標または登録商標です

©AeyeSecurityLab Inc.

AeyeSecurityLab

期間限定

「A2B攻撃」対策！診断ツールリリース予定！



APKファイルを用意するだけ！

攻撃者のAPI解析手法を

自動で診断



10万円／アプリ（初回のみ）

詳細はAeyeScanブースにて！

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

©AeyeSecurityLab Inc.

AeyeSecurityLab

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向けに、
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！

AeyeScanデモ動画を視聴

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

©AeyeSecurityLab Inc.



セキュリティに、確かな答えを。

©AeyeSecurityLab Inc.