2026年 10大脅威から読み解く

AIで変わる！ 脆弱性診断 効率化のヒント

2026 2.13 (金)

LIVE リアルタイム配信 11:00-11:30

アーカイブ配信 2.24 (火) 8:00 - 2.25 (水) 22:00

AeyeSecurityLab

株式会社エーアイセキュリティラボ
執行役員 兼 CX本部長
関根 鉄平 CISSP

2026年10大脅威から読み解く
AIで変わる！
脆弱性診断 “効率化”のヒント

はじめに

本日は本ウェビナーにご参加いただきありがとうございます

Q&A

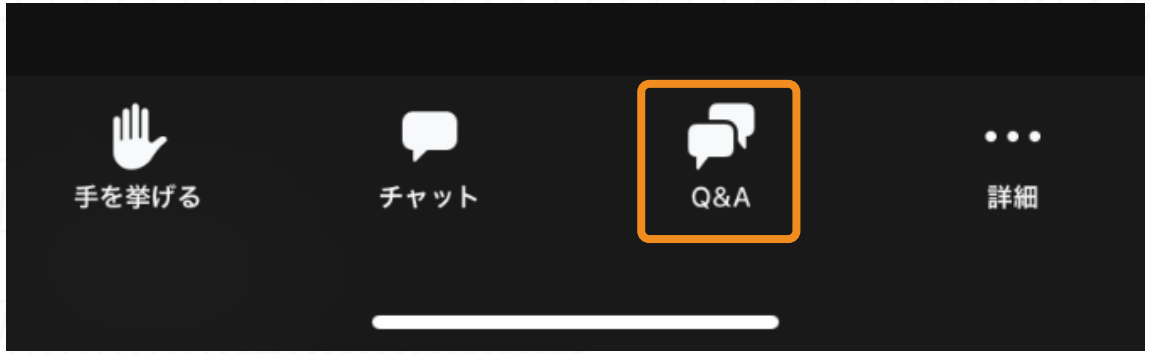
- ウェビナー中、お困り事がありましたらQ&Aにてご連絡ください。
- お客様のQ&A投稿、お名前、音声や画像が他の参加者様に届くことはございません。
- 質疑応答セッションは後に設けておりますが、ご質問はいつでもご投稿いただけます。

アンケート

- ウェビナー終了後、アンケート回答にご協力をお願いいたします。
- 本日の講演内容についてご質問のある方は、Zoom退出時に表示されるアンケート内にコメントをいただければ、後日回答させていただきます。

タイムテーブル

11:00	ご挨拶
11:05	本題
11:25	質疑応答
11:30	終了



登壇者紹介

株式会社エーアイセキュリティラボ

執行役員兼CX本部長 **関根 鉄平** CISSP

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をしつつ、CSIRTや開発現場でのセキュリティを推進。
2020年6月より現職。AeyeScanのカスタマーサクセスチームの責任者として脆弱性診断の内製化を支援。大規模イベントや大手企業での講演に多数登壇。
『セキュリティエンジニアの知識地図』を共著。

コミュニティ活動など

- 情報セキュリティ10大脅威 選考会メンバー
- OWASP/ISOGJ アジャイル開発におけるセキュリティ｜パターン・ランゲージ
- OWASP/ISOGJ Webシステム／Webアプリケーションセキュリティ要件書

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250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。

プレス発表「情報セキュリティ10大脅威 2026」を決定

独立行政法人情報処理推進機構
公開日：2026年1月29日

組織編の3位に「AIの利用をめぐるサイバーリスク」が初めてのランクイン

独立行政法人情報処理推進機構（IPA、理事長：齊藤裕）は、情報セキュリティの脅威において、2025年に社会的影響が大きかったトピックスを「情報セキュリティ10大脅威 2026」として発表しました。詳しい解説は、2月下旬以降、順次IPAのウェブサイトで公開する予定です。

・情報セキュリティ10大脅威 2026

IPAでは、国民の情報セキュリティにおける脅威への関心喚起、対策実施の促進を目的として2006年から、「情報セキュリティ10大脅威」を公表しています。前年に発生した情報セキュリティの事故や攻撃の状況などから、IPAが脅威候補を選定し、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250名のメンバーで構成する「10大脅威選考会」の投票を経て決定したものです。「組織」の立場と「個人」の立場での「10大脅威」はそれぞれ以下のとおりです。

◢ 情報セキュリティ10大脅威 2026［組織］

- 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/10threats2026.html

「2025」から「2026」のランキング変遷

2025年		2026年	
1位	ランサム攻撃による被害	→	1位 ランサム攻撃による被害
2位	サプライチェーンや委託先を狙った攻撃	→	2位 サプライチェーンや委託先を狙った攻撃
3位	システムの脆弱性を突いた攻撃	NEW	3位 AIの利用をめぐるサイバーリスク
4位	内部不正による情報漏えい等	↓	4位 システムの脆弱性を悪用した攻撃
5位	機密情報等を狙った標的型攻撃	→	5位 機密情報等を狙った標的型攻撃
6位	リモートワーク等の環境や仕組みを狙った攻撃	↑	6位 地政学的リスクに起因するサイバー攻撃（情報戦を含む）
7位	地政学的リスクに起因するサイバー攻撃	↓	7位 内部不正による情報漏えい等
8位	分散型サービス妨害攻撃（DDoS 攻撃）	↓	8位 リモートワーク等の環境や仕組みを狙った攻撃
9位	ビジネスメール詐欺	↓	9位 DDoS 攻撃（分散型サービス妨害攻撃）
10位	不注意による情報漏えい等	↓	10位 ビジネスメール詐欺

出典 https://www.ipa.go.jp/security/10threats/10threats2026.html

新設された「AIの利用をめぐるサイバーリスク」

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
3位 NEW	AIの利用をめぐるサイバーリスク	2026年	初選出

AI活用の拡大に伴い、入力データが学習に再利用されることによる情報漏えいや、AI生成物の商用利用・公開に起因する権利侵害が顕在化しつつある。さらに、生成結果を十分に検証せずに利用した場合、誤判断や脆弱なコード実装、ハルシネーションによる問題が発生するおそれがある。
加えて、攻撃者はAIを武器としてサイバー攻撃や詐欺を高度化・巧妙化させており、リスクは組織の内外で拡大している。

ガバナンス整備と、安全なAI活用の重要性が急速に高まっていることから選出

AIの利用をめぐるサイバーリスク①法的・経営上の課題

情報漏洩

AIに入力した機密情報が
学習に使用され
第三者の回答に出力される

権利侵害

権利関係の確認をせず
AIの生成物を
商用利用・公開してしまう

ガバナンス欠如

AI利用ルールが未整備で
リテラシーの差が
そのまま脆弱性となる

関連事故

Samsung電子：機密ソースコードの流出（2023年）
エンジニアがバグ修正のためにChatGPTへ機密コードを入力し、社外流出が発生

出典 https://forbesjapan.com/articles/detail/62905

OpenAI：チャット履歴と個人情報の露出（2023年）
システムのバグにより、他人のチャットタイトルや支払い情報が一部閲覧可能に

出典 https://www.itmedia.co.jp/news/articles/2303/25/news051.html

AIの利用をめぐるサイバーリスク②技術起因の落とし穴

ハルシネーション

AIが生成した
もっともらしい嘘を
信じて実行してしまう

脆弱なコードの生成

AIが生成したコードを
検証せず実装し
脆弱性を抱えてしまう

誤判断・誤送信

AIに権限を与えてしまい
誤判断によるデータ削除や
誤送信が発生

関連事故

AIパッケージ・ハルシネーション攻撃（2023年～）
AIが推奨した「実在しないライブラリ」を攻撃者が先回りして作成し、マルウェアを仕込む

出典 https://gigazine.net/news/20250415-slopsquatting-ai-hallucinated-code/

AI生成コードの約3割に脆弱性が混入（2025年 Veracodeの調査による報告）
AIが作成したコードの多くに重大なセキュリティ上の欠陥が含まれていることが判明

出典 https://www.itmedia.co.jp/enterprise/articles/2402/26/news045.html

AIの利用をめぐるサイバーリスク③サイバー攻撃の高度化

攻撃の容易化

AIの支援により
高度なマルウェアや
攻撃ツールが作成可能に

ディープフェイク

本人にそっくりな
音声や動画を作成し
詐欺などに悪用

防御回避

セキュリティソフトの
監視をすり抜ける手法を
AIに探索させる

関連事故

楽天モバイル：不正接続ツール作成（2025年）
プログラミング知識のない少年らがAIで攻撃プログラムを作成し、システムに不正接続

出典 https://www.nikkei.com/article/DGXZQOUE271BZ0X20C25A2000000/

著名人のフェイク動画による投資詐欺（2025年）
実業家や首相の偽動画がSNSで氾濫。AIによる高い信憑性で被害が拡大

出典 https://www.fsa.go.jp/receipt/toushisagi_koukoku/shuhou.html

初のAI駆動型ランサムウェア『PromptLock』がESETにより発見（2025年）
生成AIモデルを悪用することで、従来型の手法では考えられない高度な攻撃を実現

出典 https://eset-info.canon-its.jp/malware_info/malware_index/251008.html

2年連続2位となった「サプライチェーンや委託先を狙った攻撃」

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
2位 →	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目

サプライチェーン攻撃とは、自社環境を直接狙うのではなく、接続された委託先やグループ会社のサーバー、VPN、認証基盤、運用アカウントなど、侵入しやすい経路を突破口に、信頼関係やネットワーク連携を悪用して横展開（ラテラルムーブメント）する手法。境界防御だけでなく、委託先を含むアクセス制御、最小権限、監視強化が重要となる。

関連事故

日本コロムビア：不正アクセス被害（2025年）
同社サーバーを利用しているグループ会社3社においても不正アクセス被害が発生

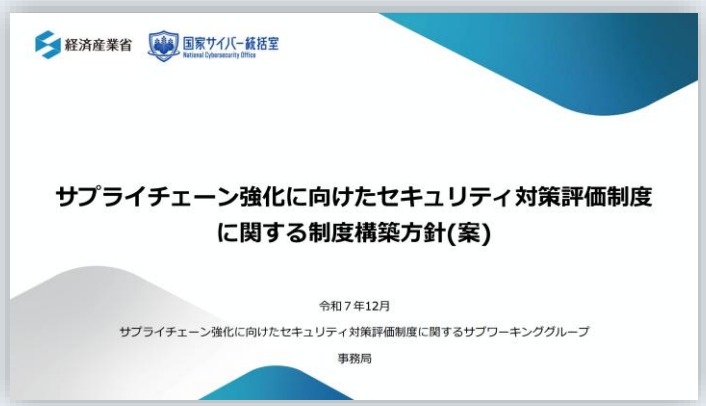
出典 https://columbia.jp/oshirase/info250808.html

法政大学：個人情報漏洩の可能性ありと発表（2025年）
情報ネットワーク事業の管理委託をしている会社が不正アクセスを受けたことに起因

出典 https://www.hosei.ac.jp/info/article-20250710091502/

2026年度中の制度開始予定「サプライチェーン対策評価制度」

経済産業省は、サプライチェーン全体の強靭性の確保と、対策要求の共通化による対策適正化・確認の効率化を目的とした「サプライチェーン対策評価制度」を導入する方針を示しました。



セキュリティ対策の
成熟度を3段階で評価

	★3	★4	★5
想定脅威	一般的なサイバー攻撃	供給停止・情報漏洩など大きな影響をもたらす攻撃	未知の攻撃も含めた高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が最低限実装すべき対策	サプライチェーン企業等が標準的に目指すべき対策	サプライチェーン企業等が到達点として目指すべき対策
評価スキーム	自己評価	第三者評価	第三者評価

※★1、★2に関しては、先行する自己評価制度の仕組みである「SECURITY　ACTION」にて制度化

★3、★4については2026年度下期の運用開始が想定されている

参考：サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)より抜粋および意訳

制度対応も始まり
セキュリティ対策はいよいよ
やることが多すぎる…

増え続けるセキュリティ対策において、これからの時代に必要なのは「AI活用」

人手やコスト・時間が限られる中でセキュリティを担保するためには、対応に濃淡をつけつつ、リソースを効率良く配分する方法を考える必要がある。その方法のひとつが、AI活用といえる。

手間と時間をかけて専門家が対応する	濃 ⟷ 淡	人的リソースを最小化しつつ対応する
専門人材は限られているが、技術的に人間が対応しなければいけない範囲が広い		継続的・網羅的に対応する必要があるが、割ける人的・金銭的リソースは限定的

AIを活用した「自動化」も必要

脆弱性診断は、AI活用と相性が良い

法令遵守

- デジタル関連法令対応
- コンプライアンス対応
- 業界のセキュリティガイドラインへの準拠

…etc

ミスができない領域

人が考えて対応すべき

ガバナンス強化

- 事業特性に応じたセキュリティポリシーやガイドライン作成
- セキュリティ対応マニュアルの整備と実行管理

…etc

関係者が多く影響範囲が広い

人の精緻な設計が必要

具体的な対策

- セキュリティ製品やサービスの導入
- システム面のサイバー攻撃対策
- **脆弱性診断**

…etc

目的と方法を決めれば
対策にAIを組み込める

脆弱性診断をAIで効率化することで
継続的な運用が可能に！

生成AI時代の脆弱性診断なら AeyeScan

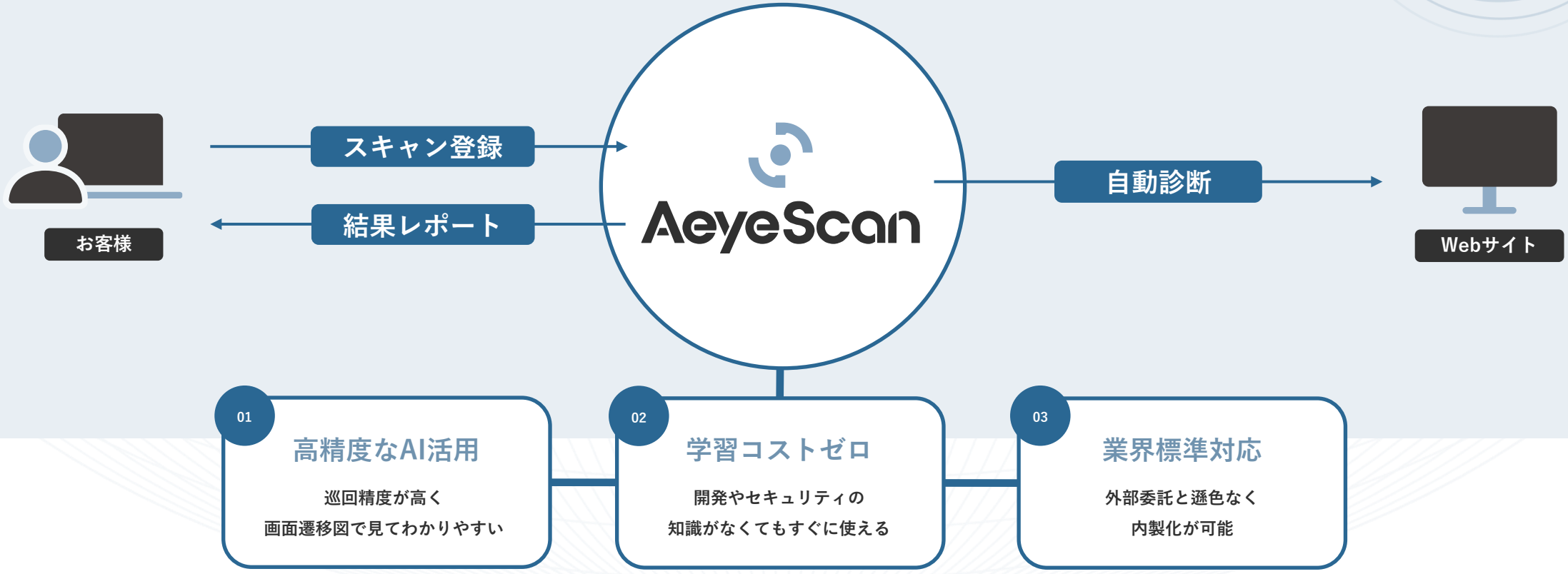
クラウド型Webアプリケーション
脆弱性検査ツール

国内市場シェア
No.1※

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（2024年度実績）



01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

02
学習コストゼロ
開発やセキュリティの
知識がなくてもすぐに使える

03
業界標準対応
外部委託と遜色なく
内製化が可能

Demonstration

デモ

内製と外注を併用する「ハイブリッド型」の運用がおすすめ

脆弱性診断のベストな頻度

1 Webサイト構築時

まず、Webサイトの設計・開発時に
可能な限り脆弱性を解消しておく。

2 Webサイト運用時

運用中に発生する問題に対応し、
Webサイトの安全性を維持する。

自社のセキュリティポリシーに適した運用を。推奨は…

年に1回の
定期診断

＋

リリースや
機能改修時

ツールだけで全てをまかなおうとせず、
大規模改修などの際は外注も視野に入れ、濃淡をつけた対応を！

AeyeSecurityLab

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

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

人材・教育

OHSAWA DRIVING SCHOOL / 河合塾 / EPARK / AIRE / HIS / H.I.S. RETAILING / アイフル / MS&AD MS&ADインターリスク総研
Junion / JINSOKEN / NTT EAST / odakyu / 近鉄情報システム株式会社 / GEO / 毎日を、給料日にする。JOBPAY / SOMPOひまわり生命
ZENKIGEN / Direct Sourcing / SymEnergy シン・エナジー / 水ing Swing Corporation / Suzuyo / NANKAI 南海システムソリューションズ / DMM FinTech / Tokyo Century
PERSOL / Leverages / 日本調剤 / HITOWA GROUP / ベルーナ / grow up together MEDIA / Net Protections
workport / Looop / Loyalty Marketing, Inc.

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
BookLive

エンタメ

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

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 / freee / vector / 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. / 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 / 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
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
YL

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）

AeyeSecurityLab

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

AeyeScanを実際に操作してみませんか？

期間限定アーカイブ配信

2026年 10大脅威から読み解く

AIで変わる！ 脆弱性診断 効率化のヒント

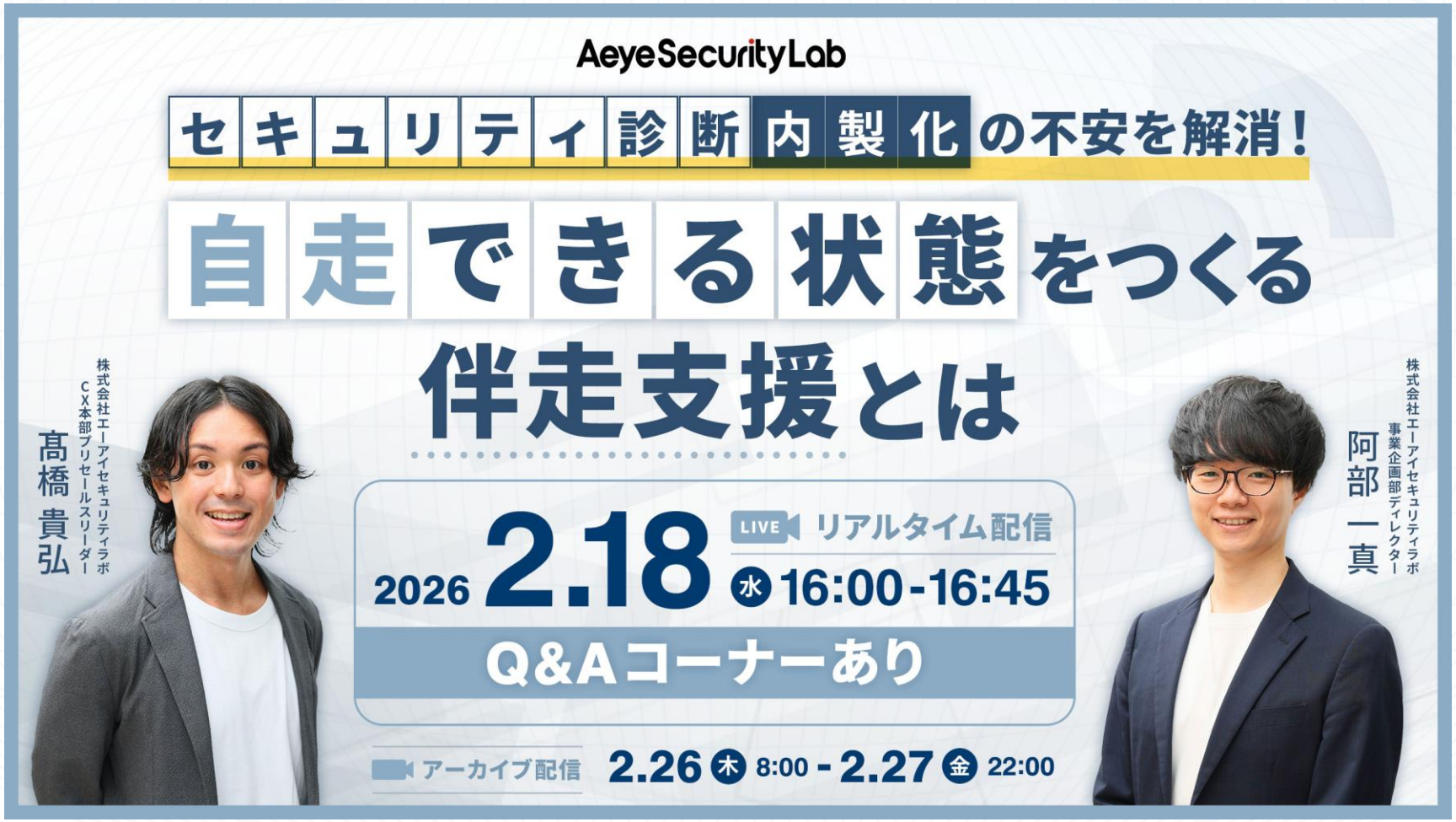
2026 2.13 (金) LIVE リアルタイム配信 11:00-11:30

アーカイブ配信 2.24 (火) 8:00 - 2.25 (水) 22:00

AeyeSecurityLab

株式会社エーアイセキュリティラボ
執行役員 兼 CX本部長 | 関根 鉄平 CISSP

次回予告



オフラインイベントも是非お申込みください！

アンケート

ご回答いただいた皆さまへ
本ウェビナーのPDFデータをプレゼント

セキュリティに、確かな答えを。