2025年最新版

10大脅威から考える
今こそ変える時、
脆弱性診断へのAI活用

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

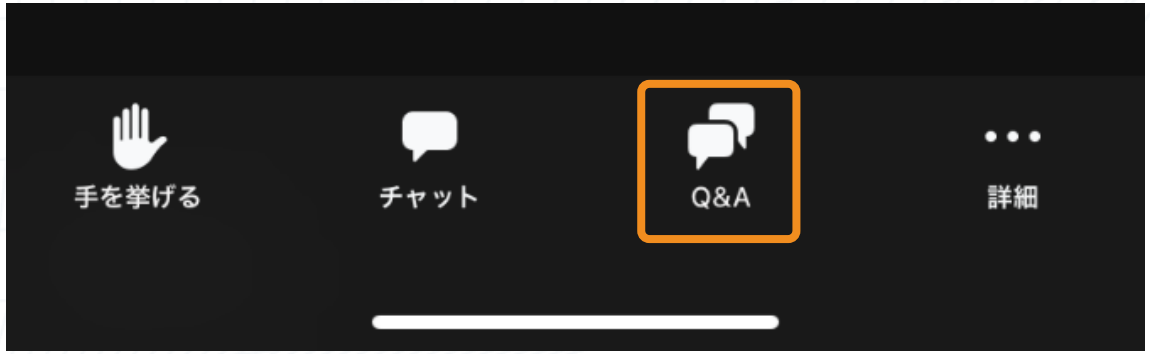
- ウェビナー中、お困り事がありましたらQ&Aにてご連絡ください。
- お客様のQ&A投稿、お名前、音声や画像が他の参加者様に届くことはございません。
- 質疑応答セッションは後に設けておりますが、ご質問はいつでもご投稿いただけます。

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

16:00	ご挨拶
16:05	本題
16:25	質疑応答
16:30	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。

情報セキュリティ
10大脅威 2025

- 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/10threats2025.html

AeyeSecurityLab

「2024」から「2025」のランキング変遷

2024年		2025年	
1位	ランサムウェアによる被害	1位 →	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃	2位 →	サプライチェーンの弱点を悪用した攻撃
3位	内部不正による情報漏えい等の被害	3位 ↑	システムの脆弱性を突いた攻撃
4位	標的型攻撃による機密情報の窃取	4位 ↓	内部不正による情報漏えい等の被害
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	5位 ↓	機密情報等を狙った標的型攻撃
6位	不注意による情報漏えい等の被害	6位 ↑	リモートワーク等の環境や仕組みを狙った攻撃
7位	脆弱性対策情報の公開に伴う悪用増加	7位 NEW	地政学的リスクに起因するサイバー攻撃
8位	ビジネスメール詐欺による金銭被害	8位 ↑	分散型サービス妨害攻撃（DDoS攻撃）
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	9位 ↓	ビジネスメール詐欺
10位	犯罪のビジネス化（アンダーグラウンドサービス）	10位 ↓	不注意による情報漏えい等

出典 https://www.ipa.go.jp/security/10threats/10threats2025.html

5年ぶりにランクインした「分散型サービス妨害攻撃（DDoS攻撃）」

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
8位 ↑	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目

年末年始に国内の航空会社や金融機関など、あわせて46の組織が攻撃の標的とされた（2025年1月9日時点）。
日本航空（JAL）や三菱UFJ銀行、NTTドコモなどで攻撃が相次ぎ、「一時的にシステムに不具合が起きる」「サイトが閲覧しづらくなる」などの影響が広がる。
特に日本航空においては攻撃被害により最大6時間の遅延が発生するなど、社会的な影響が大きいことから、再び10大脅威に選出された。

DDoS攻撃とは？

世界各地のルータやIoT機器などを乗っ取って大量の通信を発生させ、標的のサイトやシステムへ大量にアクセスするなどして、ダウンさせる。対策として攻撃元となりうるIPアドレスの制限や、組織で導入する機器やシステムの設定確認／ソフトウェアの更新などが求められる。

新設された「地政学的リスクに起因するサイバー攻撃」

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
7位 NEW	地政学的リスクに起因するサイバー攻撃	2025年	初選出

2025年1月8日、警察庁は「Mirror Face（別名「Earth Kasha（アース カシャ）」）」と呼ばれるサイバー攻撃グループに関する注意喚起を公開した。本グループは2019年より日本の安全保障や国際関係に関連した情報窃取を目的に、特定の国の関与により活動していると評価されている。
これまでシンクタンクや政府、政治家、メディア、あるいはそれらに属する個人が攻撃対象とされてきた。
今後はこれらとビジネス関係にある組織も対象となる恐れがあるとして、注意喚起されている。

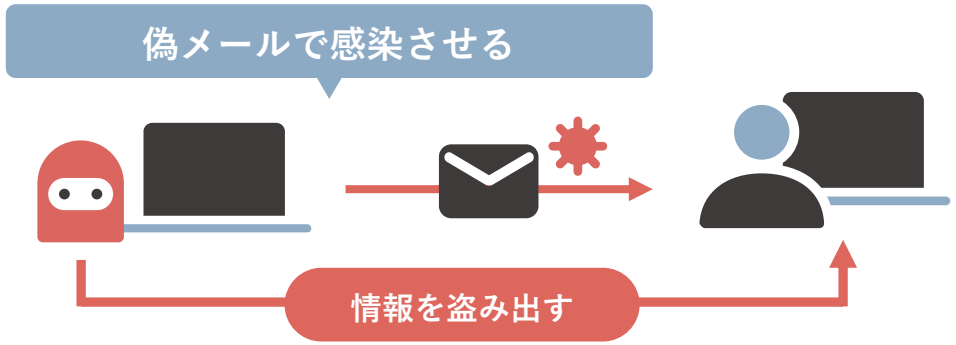
活動期間	2019年12月～
主な攻撃対象地域	日本、台湾、インド
主なターゲット	2019～2023年まで：　公共関連組織、国際関係の組織・個人、メディア関係組織・個人 2023年：　公共関連組織に加え、先端技術をもつ企業など 2024年：　政府、研究機関、シンクタンクに属する個人や、国際関係に関連する組織

Mirror Face（別名「Earth Kasha（アース カシャ）」）の攻撃手口は？

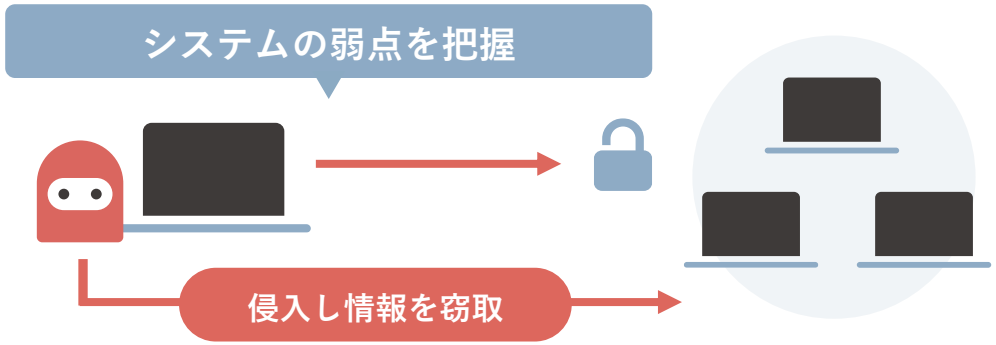
標的型メール攻撃やネットワークへの侵入など、攻撃フェーズごとに多様かつ高度な攻撃手法が用いられる。対策として基本的なセキュリティ対策を見直すとともに、侵入された場合に速やかに発見／対処できるよう多層防御を講じることが推奨される。

ミラーフェイスによる攻撃手法

❶ 標的型メール攻撃



❷ ネットワークへの侵入



昨年7位の「システムの脆弱性をついた攻撃」が3位にランクアップ

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
3位 ↑	システムの脆弱性をついた攻撃	2016年	5年連続8回目

以前より脅威とされている「ゼロデイ攻撃」や「Nデイ攻撃」など、システムの脆弱性をついた攻撃が引き続き注視されている。

また今年1月にはCISAが公開する脆弱性データベース「KEVカタログ」に、2020年に修正された既知の脆弱性「jQuery」が追加されるなど、既知の脆弱性が突然活発化するケースがある。

新たに発見される脆弱性に加え、既知の脆弱性においても継続的に対策していくことが求められる。

セキュリティ対策の対象範囲は広がり続け、対策の複雑性と実現難易度が一層高まっている

では、どうするべきか…？

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

セキュリティ領域におけるAI活用

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

「では、具体的になにをすればいいのか？」

まずは、

脆弱性診断から「AIをフル活用」し、

セキュリティ対策に濃淡をつけませんか？

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「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)

※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
200社以上

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

AI活用のレベルが高いので、自動巡回が高精度で範囲が広い

例：AIによるフォーム入力値の判断処理

課題

フォーム入力は正しい値を入力する必要がある。
間違えると、**入力エラーとなり遷移できず診断が進まない…**

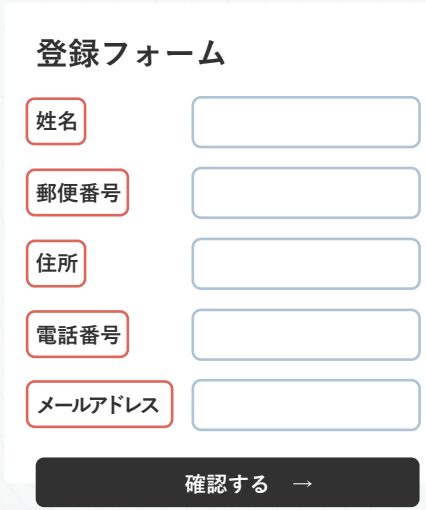
AeyeScanなら、
正確に入力値を推測して巡回！

ココがポイント

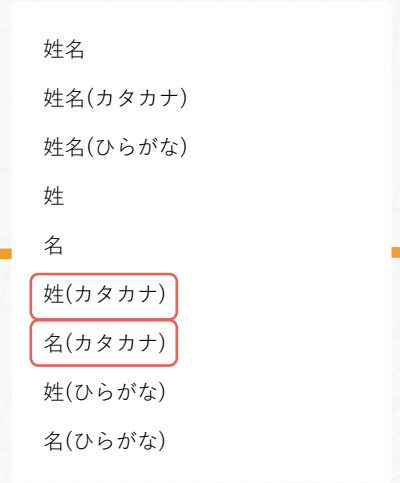
名前や住所など決まった項目だけでなく、
どんな項目にも対応！

例えば
- クレジットカード
- 画像アップロード

フォームを自動認識しラベル化



自動認識したラベル(赤枠)に応じ
適切な入力値を設定



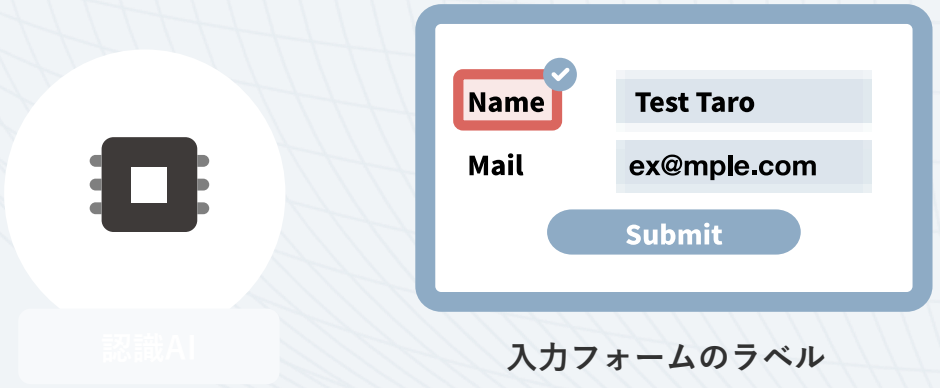
正常遷移

適切な値を入力

生成AIを使えば、巡回はここまで進化できる

認識AIができること

画面上の入力フォームのラベル（氏名など）を
認識AIが判断することでフォームに入力する



生成AIができること

生成AIを使うことで、人が画面を見るように
「これは商品画面」「これはお知らせ画面」と
判断できる！

生成AIの活用による高度な自動化を実現

生成AI機能

1 診断設定がさらにカンタンに

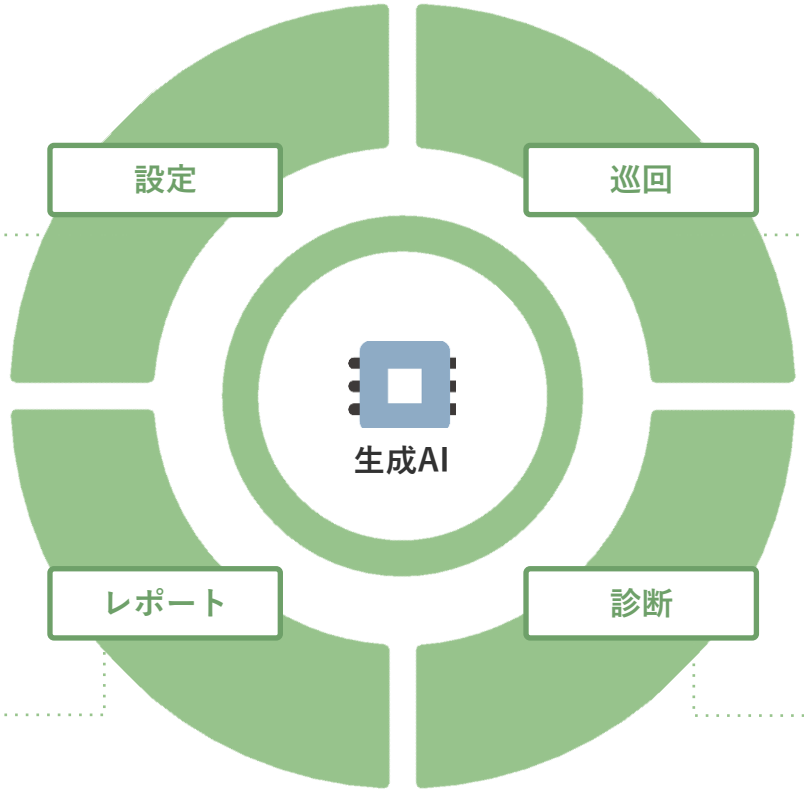
- フリーフォーマットでの指示

特許 第7320211号

2 巡回がより柔軟に進化

- 多言語対応
- フリーフォーマットでの指示
- 画面の自動類似判定

特許 第7348698号



3 手動で診断していた項目にも対応

- パラメータの用途を推測
- セッションIDの規則性を解析

特許 第7344614号

4 高度なレポート出力も可能に

- 診断結果を元に総評を生成

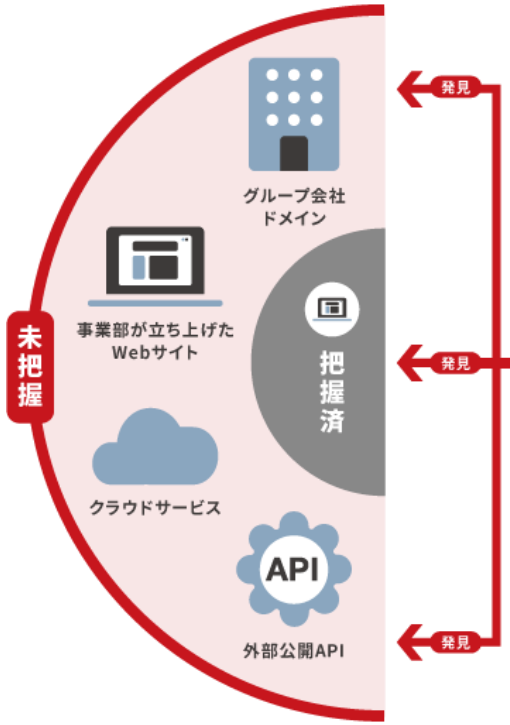
生成AI活用で、工数をかけずにWeb-ASMを実現

Web-ASM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！

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
200社以上

※ 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）

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

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
H.I.S. RETAILING
odakyu
近鉄情報システム株式会社
Junion
水ing Swing Corporation
Suzuyo
NTT東日本
HITOWA GROUP
grow up together MEDIA
Looop

金融

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

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! TORANOANA LABORATORY

SaaS

estie
M-aid
エムティーアイ
OZ INTERNATIONAL
COACH A Co., Ltd.
cybozu
JINSOKEN
Schoo
Speee
SecureNavi
ZENKIGEN
Direct Sourcing
TAL
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
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
CTC
Insight Edge
Infcurion
80&Co.
SB Technology
SBWorks
NTT AT
NTT DATA
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
SOFT CREATE
SOLTEC
電通総研
TOPPAN
JOPS
NHC
Human Interactive Technology inc.
FUJISOFT
FUJITSU
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 NTTデータ先端技術株式会社
GSX
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

まとめ

増え続けるセキュリティ脅威への対策において

AIに任せられる業務は積極的に任せ、

安全と効率を両立しましょう！

AeyeSecurityLab

期間限定

Web-ASM機能オプション 利用料金50%OFFキャンペーン

内容	Web-ASM機能オプション利用料金を初回契約分50%OFFでご提供いたします。
適用対象	○ 2025年3月31日(月)までに株式会社エーアイセキュリティラボにご発注いただいたものが対象です。 ○ AeyeScan Businessライセンスをご契約中または2025年3月31日（月）までに新規で利用開始いただいていることが前提となります。
申込方法	「Web-ASM機能」お問い合わせフォームまたは弊社担当までご相談ください。

▶ お問い合わせフォームはこちら　https://www.aeyescan.jp/form/web-asm/

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

Q&A

お気軽にご質問ください

こちらから質問をお送りください

期間限定アーカイブ配信

2025年最新版 10大脅威から考える

今こそ変える時 脆弱性診断への AI活用

2025 3.5 [水]

リアルタイム配信
16:00-16:30

アーカイブ配信 3.13 [木] - 14 [金]

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 CISSP

次回予告

なぜ脆弱性診断の内製は運用でつまずくのか？

失敗しない5つのステップからガバナンス強化まで詳しく解説

2025 3.25 [火] リアルタイム配信 16:00-16:30

3.28 [金] アーカイブ配信

阿部 一真 | 株式会社エーアイセキュリティラボ 事業企画ディレクター

AeyeSecurityLab

アンケート

アンケートにご回答いただくと、
講演資料をダウンロードいただけます。
ぜひ、ご協力よろしくお願いいたします！

セキュリティに、確かな答えを。