セキュリティ管理者向け

2026年10大脅威から読み解く

本当に効果的な対策とは

AeyeSecurityLab

AeyeSecurityLab

「情報セキュリティ10大脅威2026」から考える コスト効果の高い対策とは？

- 情報セキュリティ10大脅威とは
- 2025年から2026年のランキング変遷
- 2026年ランキングの注目ポイント
- 従来のセキュリティ対策と現在の脅威のギャップ
- 人手前提から、AI前提の運用へのシフト
- AIによる脆弱性診断の自動化・効率化
- 事例紹介｜AIを活用した脆弱性診断の取り組み

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	→	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	→	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	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	↓	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	→	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	↑	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	↓	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）	↓	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	↓	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	↓	ビジネスメール詐欺

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

6年連続1位から見える「被害の深刻化・経営リスク」

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1位 →	ランサム攻撃による被害	2016年	11年連続11回目

従来の「データ復旧を人質に取る」手法から、バックアップの破壊や基幹システムの停止を狙い、事業継続そのものを不可能にする攻撃へと変質しています。
2025年には、大手企業における全国規模の「出荷停止・欠品」が発生するなど、社会インフラを揺るがす事態にまで発展しました。

多様化・巧妙化する多重脅迫

ランサムウェアはいまや一度の侵入が複合的な経営リスクに直結します。
窃取した情報の公開を示唆する**「多重脅迫」が高度化**しており、
事業停止・信用失墜・法的対応を同時に招くリスクが高まっています。

2年連続2位から見える「境界を超えて広がる攻撃面」

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

- 大手レコード会社：不正アクセスによるグループ会社への波及（2025年）
  同社サーバーを利用するグループ会社3社においても、不正アクセスを確認
- 都立私立大学：管理委託先への攻撃に起因する情報漏洩の疑い（2025年）
  情報ネットワーク事業の管理委託先が攻撃を受け、学内の個人情報の一部が流出した可能性

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の利用拡大に伴い、入力データの学習利用やガバナンスの欠如などが課題視されがちな中、
システムの脆弱性増加や攻撃力の向上といった「サイバーリスク」も同様に深刻化。
初登場で3位という結果は、現場が直面している新たな脅威に対する強い警鐘と言えます。

AI生成結果の“鵜呑み”による
セキュリティリスク

- ハルシネーション
- 脆弱なコードの生成
- データ削除・誤送信

AIの“悪用”による
サイバー攻撃の高度化

- 攻撃の容易化
- ディープフェイク
- 防御回避の探索

Veracode社の調査では、AI生成コードの45%にセキュリティ上の欠陥が含まれていたという実態が。

出典 Veracode「October 2025 Update: GenAI Code Security Report」

従来のセキュリティ対策と現在の脅威のギャップ

狙われる「脆弱な隙」は、攻撃面の広がりやAIによる攻撃力の向上により、かつてない経営リスクへと発展。
いま、従来の点検を超え、複雑化するリスクを常に「捉え続ける仕組み」への転換が求められています。

内部中心設計のセキュリティ運用		10大脅威が示す“現在のリスク構造”
管理下にある資産・システム中心に設計	⟷	管理／把握外の公開資産が起点となるリスク
静的な設定・構成に基づくリスク管理	⟷	サプライチェーンを含む連鎖的な侵害
定期的な点検・診断による安全性確認	⟷	自動化・高速化により“常時狙われる”環境
内部からの統制・管理を重視	⟷	侵入を前提とした攻撃シナリオ

問題は “やっていないこと” ではなく、“見えていないこと”

「やりたくても、手が回らない」現場

現在のサイバーリスクは、「見ようとすれば人手で把握できる範囲」をすでに超えています。
リスクが見えないのは、意識や体制の問題ではなく、リソースの制約と環境の複雑化によるものです。

資産（攻撃面）の広がり

DX推進に伴うWeb資産の増加
管理外の野良サイトの乱立

24時間365日の攻撃

AIによる絶え間ない攻撃に対し
点の対策では追い付かない

増え続ける業務

鳴りやまないアラートの精査で
本来の業務に手が回らない

従来のやり方では太刀打ちできない構造的な限界が原因

AeyeSecurityLab

人手前提のセキュリティ運用から、AI前提の運用へ

AIは攻撃の脅威であると同時に、防御を支える「最強の味方」にもなります。
人手による対応が限界を迎える今、 AIとの共存が、現場が本来の判断業務に専念できる強い守りを実現します。

人手前提の運用

- 資産棚卸のたび現場が疲弊
- 脆弱性の見逃し・診断漏れ
- 対応の優先順付けが属人化

気付いた時には遅いケースが増える

AIを組み込んだ運用

- 公開資産を自動で継続把握
- 脆弱性を24時間自動で検知
- 定量的なリスク評価を可視化

人は判断 / 意思決定に集中できる

AIが人の代わりに守るのではなく

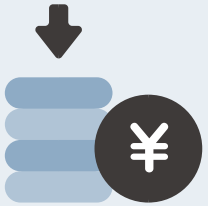
人が守れる状態を作るために、AIを活用しませんか？

脆弱性診断は、AIにより自動化しやすい分野

AI前提の運用へシフトする第一歩として、取り組みやすいのが「脆弱性診断」です。
サイト更新や新種の脆弱性に合わせて“繰り返し”行う必要がある診断業務は、セキュリティ対策の中でも特に継続的な負荷が高く、AIによる自動化・内製化が力を発揮する領域と言えます。

脆弱性診断にAIを取り入れる効果

対応スピードアップ



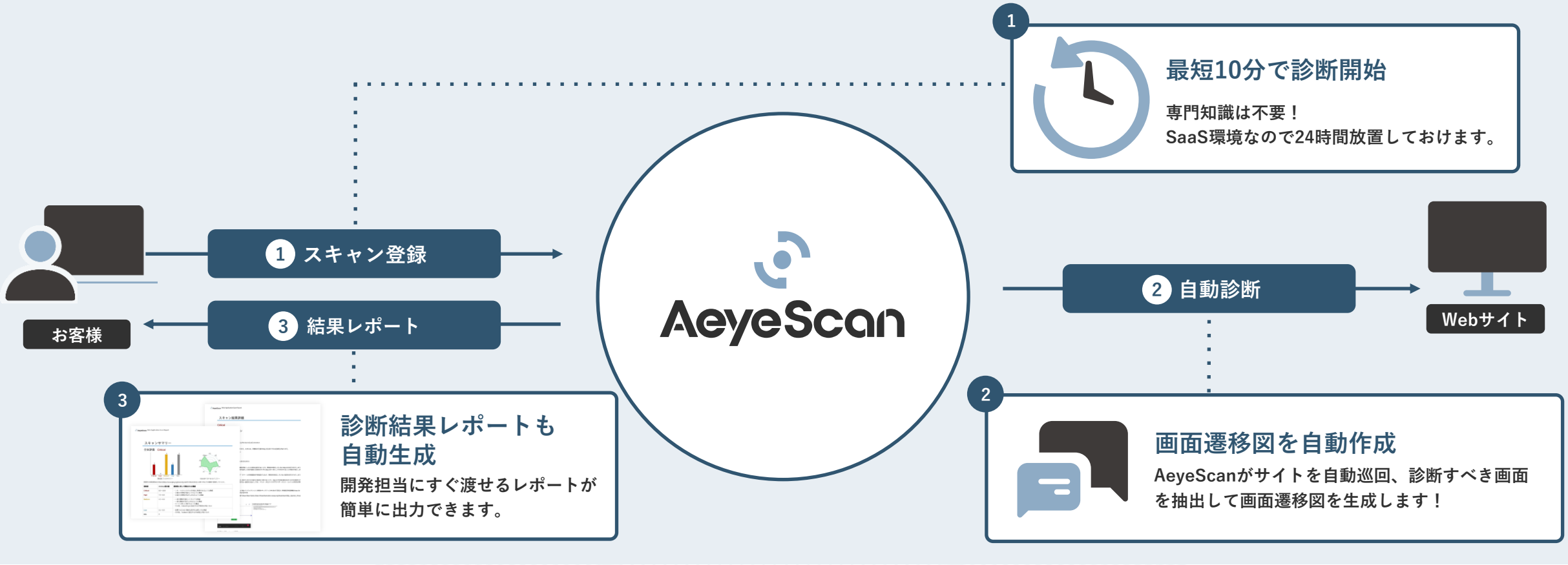
コストダウン

情報・ノウハウの社内蓄積

AeyeSecurityLab

AI前提の運用を具現化する、次世代の脆弱性診断プラットフォーム

AeyeScanは、未把握のWeb資産の可視化・リスク評価から脆弱性診断まで、各工程で自動化を実現。
人手に頼らない「網羅的・継続的なセキュリティ」を維持できる仕組みを提供します。



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

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
Junion
JINSOKEN
ZENKIGEN
Direct Sourcing
PERSOL
Leverages
workport

インフラ

EPARK
AIRE
HIS
H.I.S. RETAILING
NTT EAST
odakyu
近鉄情報システム株式会社
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
ベルーナ
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
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
MITSUBISHI ELECTRIC 三菱電機デジタルイノベーション株式会社
YONA
リピスト

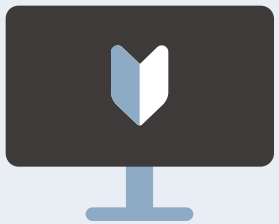
セキュリティ企業

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）

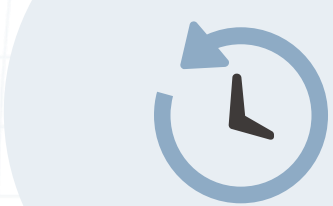
AeyeSecurityLab

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。

AeyeSecurityLab

導入事例紹介

エイチ・アイ・エス 様

企業名　株式会社エイチ・アイ・エス

事業内容　総合旅行会社

従業員数　10,849名（2023年6月時点）

課題

セキュリティの内製化が困難。
診断の外注コストを削減したい

具体的な課題

1. 社内からの診断依頼が増え続けていた
2. 診断対象が多く外部委託せざるを得ない
3. 外注による診断コスト増

内製・外製含め100を超えるWebアプリケーションがあり、内部の体制だけでは全ての診断実施に対応できず、一部を外部に委託。コスト削減と体制整備が課題だった。

導入

情報処理推進機構（IPA）の検証結果と
「7割以上自動化」という点が決め手

導入の背景

1. 手動の診断では対応が追い付かず自動化を検討していた
2. 自動化できても性能が落ちない製品を探していた

手動作業を伴う診断では対応が困難になり、診断の自動化を検討。AeyeScanは、IPAの検証結果が高評価だったことと、「7割以上の自動化が可能」という点が決め手で導入。

効果

診断・レポート作成工数を大幅に削減。
さらなる内製化比率の向上を目指す

具体的な効果

1. 診断の大部分を自動化し工数を削減
2. レポート機能により大幅に時間を短縮
3. リリース前に診断と脆弱性改修が完了

「脆弱性が発覚しても、リリースまでに修正が間に合わない」という悩みも解消され、脆弱性を潰してからアプリをリリースできるように。

導入事例紹介

マネーフォワード 様

企業名　株式会社マネーフォワード

事業内容　PFMサービスおよびクラウドサービスの開発・提供

従業員数　2,400名（2024年5月末日現在）

課題

事業が拡大しプロダクトが増えるにつれ、
脆弱性診断の間隔が空いてしまうことが
懸念材料だった

具体的な課題

1. 外注だとナレッジが蓄積されない
2. 外注だと画面数に応じた料金体系で網羅的な診断を受けづらい
3. 開発が遅れた場合、ベンダーとのスケジュール調整が困難

新機能の追加や大規模な改修の際には脆弱性診断を実施していたが、それ以外はプロダクト側の判断に委ねていた。小さな改修のたびに診断を外注するのではなく、内部で迅速に診断する選択肢も持ちたかった。

導入

診断ツールを導入し
継続できなかった経験から、
使いやすさを重視

導入の背景

1. 自動巡回のカバー率が高く、主要な脆弱性を確実に検出できる
2. グループ会社のプロダクトも診断できるライセンス体系
3. API診断が可能

外国籍エンジニアも多く在籍するため、英語にも対応していること、Slackをはじめとする外部サービスとの連携性も要件だった。複数のツールの比較検討を進め、いくつかのプロダクトを対象に検証を実施した上で選定。

効果

約60プロダクトに診断を実施できた
今後、最低年1回の診断を計画

具体的な効果

1. 画面遷移図により、CISO室がプロダクトの画面を把握できるように
2. 開発者のセキュリティ意識が高まった
3. グループ統一のセキュリティスタンダード適用にも活用予定

ほぼすべてのサービスを内製で開発する中、「セキュリティスペシャリストの活動をAeyeScanがサポートしてくれている」とCISOも評価。セキュリティエンジニア以外に、QAチームでも使用を開始している。

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

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） クラウド型Web診断サービス「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	
社員数	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

セキュリティに、確かな答えを。