サプライチェーン攻撃の入口を塞ぐ、クライアント証明書によるなりすまし対策

～取引先・委託先を含めた安全なWebアクセス管理の実践ポイント～

2026/6/24

GMOグローバルサイン株式会社

電子証明書事業本部

アジェンダ

目次

会社紹介

会社概要

セキュリティ事業

- 1996年事業開始
- SSL発行実績
  累計3,800万枚
- SSLサーバ証明書
  国内シェア・認知度 No.1

- 電子印鑑ソリューション
- クライアント証明書
- IoT/IoMT セキュリティ
- マイナンバー/eKYC 本人確認
- SSO「GMOトラスト・ログイン」

会社名	GMOグローバルサイン株式会社
代表者	代表取締役　中條 勝夫
所在地	東京都渋谷区道玄坂1-2-3 渋谷フクラス（グループ第2本社）
設立	2003年4月
事業内容	情報セキュリティ及び電子認証業務事業
資本金	3億5,664万円
従業員数	568名 ※2025年8月時点
海外拠点	ベルギー、英国、米国、中国、シンガポール、 フィリピン、インド、ロシア、UAE、他

実績

日本国内で電子証明書ベンダーとして、20年以上の経験と実績

SSLサーバ証明書
国内シェア・認知度 **No.1**

クライアント証明書
導入企業数 **7,300社**

MARUHA NICHIRO
SHISEIDO
SOMPOケア
ALSOK
Benefit one
Dai-ichi Life Group
UCHIDA
NAVICOM AVIATION
NS Solutions
KeyPoint
Plenty 株式会社プレンティー
Marketing Applications

※2026年6月時点

脅威となり続けるサプライチェーン攻撃

サプライチェーン攻撃の脅威

サプライチェーン攻撃は8年連続ランクイン

特に2023年以降、1位と2位は順位変わらずランクインしており、大きな脅威として被害を及ぼしています。

1	ランサム攻撃による被害	11年連続
2	**サプライチェーンや委託先を狙った攻撃**	**8年連続**
3	AIの利用をめぐるサイバーリスク	初選出
4	システムの脆弱性を悪用した攻撃	6年連続
5	機密情報を狙った標的型攻撃	11年連続
6	地政学的リスクに起因するサイバー攻撃	2年連続
7	内部不正による情報漏えい等	11年連続
…	8位以下は省略	

自社のセキュリティだけでは不十分。
取引先・委託先までの対策が必要。

※引用元：IPA「情報セキュリティ10大脅威 2026」

サプライチェーン攻撃の主な要因

技術的要因

脆弱性・OSS/サードパーティ依存

- ライブラリの脆弱性
- 更新パッチ遅延

組織的要因

ガバナンス・委託先管理の欠如

- インシデント対応の不備
- セキュリティ基準の未統一

人的要因

従業員の教育・認証情報の運用

- 認証情報の不適切な管理
- サイバー攻撃への耐性

サプライチェーン攻撃の被害事例①

大阪急性期・総合医療センター（2023年）

調査・復旧費用

約数億円

逸失利益では十数億円以上と換算

復旧までの期間

約2カ月

通常診療の完全復旧まで

流出経路

VPN経由

脆弱性悪用→認証情報漏えいの可能性

― 何が起きたか

2022年10月、基幹災害拠点病院である大阪急性期・総合医療センターがランサムウェア攻撃を受け、電子カルテを含む基幹システムが暗号化されるインシデントが発生した。

⚠

業務委託先の給食事業者が設置・運営する給食システムに、情報基盤構築事業者が**リモート保守のために設置したVPN機器の脆弱性**を用いて侵入。
（漏洩され**公開されていたID・パスワード情報を用いて侵入された可能性**もある）

― 本件から読み取れること

- ✓ アクセス可能な全ユーザに管理者権限を与えないように、**適切な権限付与が必要**
- ✓ PC・サーバなど**共通のID・パスワードを設定しない、利用しないような認証設計**
- ✓ 自社の停止が取引先全体に与える影響まで含めた事業継続計画の組み立て
- ✓ ランサムウェアを想定した**オフライン/イミュータブルなバックアップが不可欠**

※引用元：大阪急性期・総合医療センター 情報セキュリティインシデント調査委員会「調査報告書」

サプライチェーン攻撃の被害事例②

アスクル株式会社（2025年）

流出件数

約74万件

問い合わせ内容・サプライヤーの情報

復旧までの期間

約1.5カ月

攻撃の検知から注文の再開まで

流出経路

業務委託先の認証情報

管理者アカウントのID・パスワード漏えい

― 何が起きたか

2025年10月、アスクル株式会社がランサムウェア攻撃を受け、物流システムや社内システムがサーバ暗号化・ファイル削除の被害に遭い、受注・出荷業務を全面停止する事態となった。

⚠

流出元は、例外的に**多要素認証を設定していなかった業務委託先の管理者アカウントの認証情報**。ランサムウェアの被害が**バックアップデータまでも暗号化されてしまった**ことで回復まで長期化してしまった。

― 本件から読み取れること

- ✓ **委託先まで含めた認証・権限管理**（ID管理のサプライチェーン）**の重要性**
- ✓ 「侵入を防ぐ」だけでなく**「気づける」ような監視体制**や**即時対応体制が必要**
- ✓ 自社の停止が取引先全体に与える影響まで含めた事業継続計画の組み立て
- ✓ ランサムウェアを想定した**オフライン/イミュータブルなバックアップが不可欠**

※引用元：アスクル株式会社「ランサムウェア攻撃の影響調査結果および安全性強化に向けた取り組みのご報告」

国の制度でも指摘

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

経産省・内閣官房国家サイバー統括室が策定し、2026年下半期から運用開始

LEVEL・自己評価	LEVEL・第三者評価	LEVEL・第三者評価
★3 **最低限の対策**	★4 **中核企業に求められる水準**	★5 **高度な対策(検討中)**
・**26項目**の要求事項 ・専門家確認付き**自己評価** ・有効期間：**1年** ・想定対象：**全サプライチェーン企業**	・**44項目**の要求事項 ・評価機関による**第三者評価+技術検証** ・有効期間：**3年** ・**多要素認証/ID管理**が必須要件	・国際規格ベースの**ベストプラクティス** ・ISO/IEC 27001等が基準 ・要求事項数は**今後検討** ・サプライチェーン全体の強靭化策
想定脅威: 広く認知された脆弱性を悪用する一般的なサイバー攻撃	想定脅威: 供給停止・機密情報漏えいで甚大な影響を及ぼす攻撃	想定脅威: 未知の攻撃を含む高度なサイバー攻撃

★4以上では"パスワード認証のみ"では合格不可能

サプライチェーン攻撃に必要な対策

取引先・委託先のシステム × 認証レベルの弱さ × 機器の脆弱性

=

侵入成立

認証面では、パスワード以外の認証運用が必須

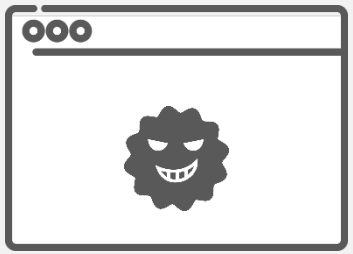
フィッシング耐性のある認証で
不正アクセス対策

多要素認証を突破するフィッシング攻撃

リアルタイムフィッシング

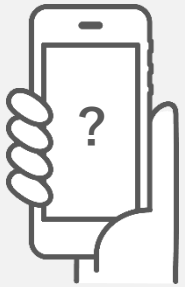
攻撃者は、ユーザを偽サイトへ誘導。
入力された認証情報をそのままリアルタイムで正規サイトへ入力して、不正アクセスする手法。

中間者攻撃（AiTMなど）



攻撃者は、正規サイトとユーザの間で認証情報の受渡す偽サイトへ誘導。
認証後のCookie情報を窃取して、正規サイトへ不正アクセスする手法。

多要素認証疲労攻撃



攻撃者は、プッシュ通知認証を何度も発信。
ユーザが誤って認証を承認してしまうミスを誘うことで、不正アクセスを狙う手法。

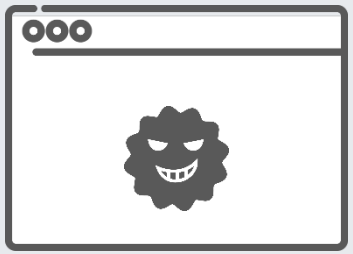
突破されてしまう認証方法

GlobalSign by GMO

リアルタイムフィッシング

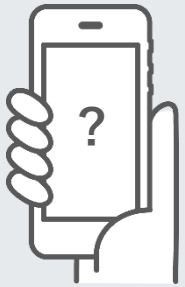
ワンタイムパスワード
などの入力を求める認証

中間者攻撃（AiTMなど）



ワンタイムパスワード
プッシュ通知認証 など

多要素認証疲労攻撃



プッシュ通知認証

「多要素認証を入れたら安心」はもう通用しない

不正アクセス対策として求められる認証

ID・パスワードのみの認証

- 攻撃手法の進化で、ID・パスワードの長さ・複雑さは効果が薄い。
- サプライチェーン攻撃の要因として、ID・パスワードの漏えいが多い。

多要素認証

- 旧来のパスワード攻撃は多要素認証で防ぐことが出来る。
- 攻撃手法の変化で、多要素認証の一部の認証方法を突破できる攻撃が増加。

フィッシング耐性のある（多要素）認証

フィッシング耐性のある認証とは

ユーザが誤っても、攻撃者から認証情報を守ることが可能な認証

3.2.5. フィッシング耐性

フィッシング攻撃は、SP 800-63Bでは以前は「検証者なりすまし」と呼ばれていましたが、不正な検証者やRPが、不注意な申請者を騙して認証器を偽者に提示させようとする試みです。SP 800-63の以前のバージョンでは、フィッシング攻撃に耐性のあるプロトコルは「強力な中間者攻撃耐性」とも呼ばれていました。

この文書では、フィッシング耐性とは、認証プロトコルが、認証要求者の警戒に頼ることなく、認証シークレットと有効な認証器出力が偽の検証者（つまり、検証者を装った攻撃者）に漏洩されるのを防ぐ能力を指します。認証要求者が偽の検証者に誘導される方法は関係ありません。例えば、認証要求者が検索エンジン最適化によって偽の検証者に誘導されたか、メールで誘導されたかに関わらず、フィッシング攻撃とみなされます。

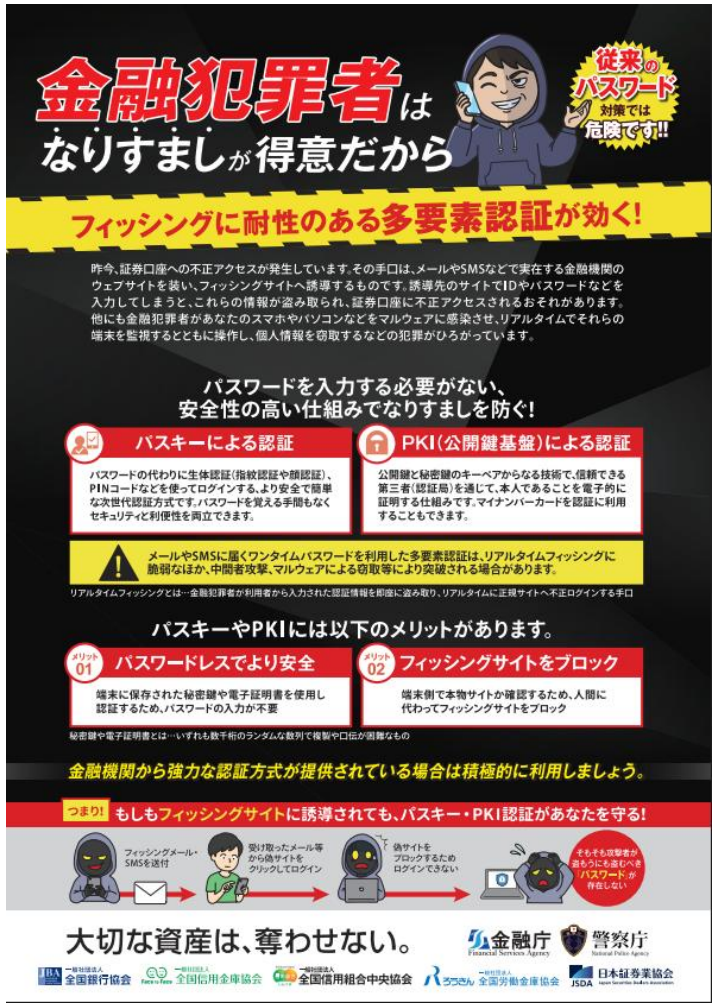
必要に応じて、承認された暗号化アルゴリズムを用いてフィッシング耐性を確立するものとする（**SHALL**）。**この目的で使用される鍵は**、[SP800-131A]の最新版で規定されている最低限のセキュリティ強度（すなわち、本書の発行時点で112ビット）以上を提供するものとする（**SHALL**）。

フィッシング耐性には、単要素または多要素暗号認証が必要です。認証器出力の手動入力を必要とする認証器（例：アウトオブバンド認証器やOTP認証器）は、手動入力によって認証器出力が認証対象の特定のセッションに紐付けられないため、フィッシング耐性があるとはみなさ**れません**。例えば、なりすましの検証器が認証器出力を検証器に中継することで、認証に成功する可能性があります。

※引用元：米国国立標準技術研究所（NIST）「SP 800-63B-4: Digital Identity Guidelines, 3.2.5Phishing Resistance」

各団体で推奨が進む

金融庁



引用元：金融庁「フィッシング耐性のある多要素認証編（詳細版）」

Microsoft

トークン保護の機能がトークン窃取攻撃を防ぐ決定的な方法であるのと同様に、新しい種類の資格情報を用いることでユーザーが AiTM フィッシング攻撃の餌食になることをほぼ防ぐことが可能です。フィッシングに耐性のある資格情報は、機密情報を公開しない暗号的な手法を使用しているため、攻撃者が認証プロセスを傍受したり複製したりすることができず、より安全です。Microsoft Entra ID がサポートする認証方法 のうち、パスキー、証明書ベース認証 (CBA)、および Windows Hello for Business はフィッシング耐性があります。最も強い保護を提供することで、米国のサイバーセキュリティ向上に関する大統領令 などの規制要件を満たしています。

引用元：Japan Azure Identity Support Blog「Adversary-in-the-Middle フィッシング攻撃への対策」

Salesforce

管理者を含む特権ユーザー向けに、フィッシング対策型の多要素認証（MFA）の導入準備を進めてください。

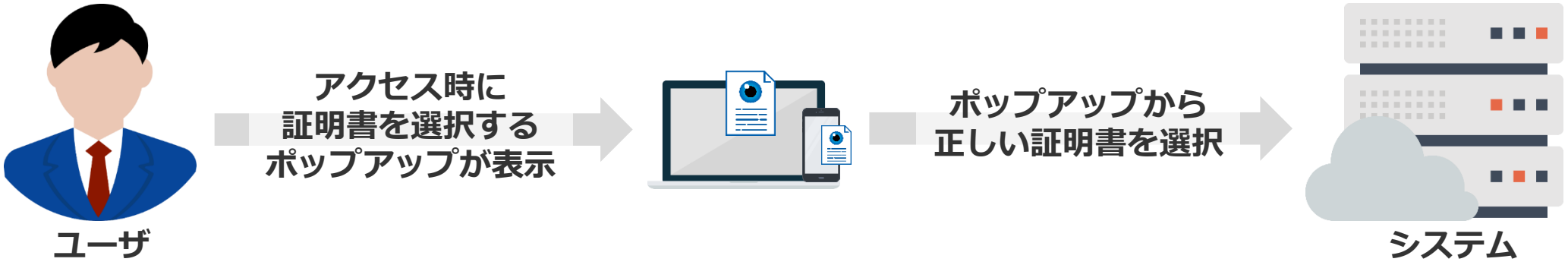
発行日：2026年6月16日

ティア	Salesforceへの直接ログイン（Salesforce MFA認証）	SSO認証方式参照（AMR）シグナル	SSO認証コンテキストクラス参照（ACR）シグナル	結果
フィッシング対策機能付き多要素認証	セキュリティキー（WebAuthn）、組み込み認証機能（Touch ID、Windows Hello）、*管理者生成の一時検証コード*	証明書、面、fido、fido2、fpt、hwk、虹彩、パスキー、phr、pki、ポップ、pwlesspasskey、網膜、sc、スマートカード、swk、tlsclient、wia、x509	fido、fido2、fpt、hwk、パスキー、phr、pki、pwlesspasskey、retina、スマートカード、swk、tlsclient、wia、x509	ログインに成功しました。

引用元：Salesforce「Prepare for Phishing-Resistant MFA Enforcement for Privileged Users including Admins」

クライアント証明書とは

ユーザが正規の利用者であることを認証する電子証明書



1. ID・パスワードと併用することで **多要素認証**
2. インストールされている端末のみアクセス可能な **アクセスコントロール**
3. 公開鍵暗号方式を用いた **パスワードレス認証**

クライアント証明書が選ばれる理由

理由①

端末制御

クライアント証明書がインストールされている端末のみアクセス可能。
証明書を正しい端末へ配布することで、**アクセス端末の制御**が可能に。

理由②

フィッシング耐性

公開鍵暗号方式によって、端末に保存されている鍵を用いた**パスワードレス認証**のため、フィッシング耐性のある認証を実現。

理由③

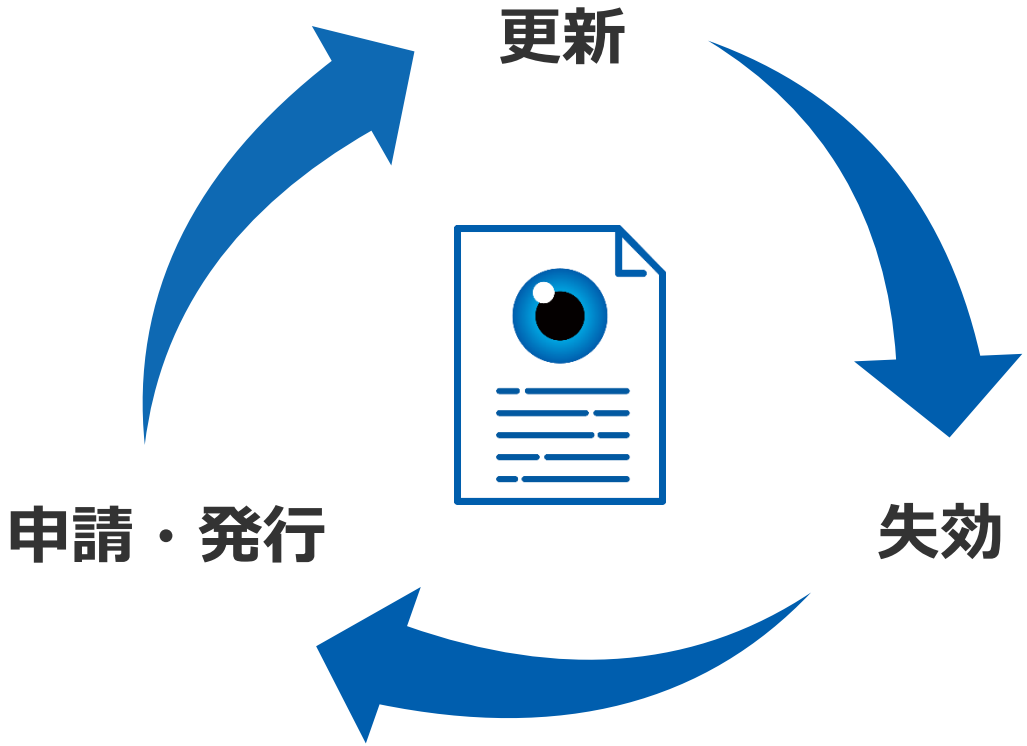
利便性の高さ

ユーザは認証する時、ポップアップから正しい証明書を選択するのみでシステムへアクセス可能なため、**ユーザの認証時の負担が少ない。**

グローバルサインのクライアント証明書

グローバルサインのクライアント証明書

マネージドPKI Lite byGMO



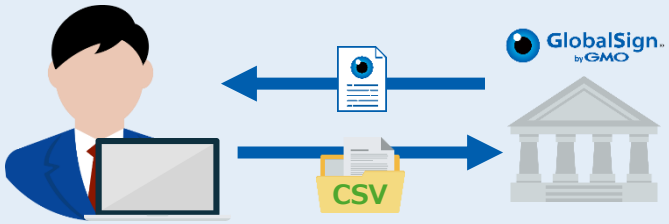
- ✓ 最短1営業日で証明書発行可能
- ✓ 初期費用・保守費用 不要
- ✓ 認証局の管理は全てGS
- ✓ 専用の管理画面で一括管理

認証局運用のコストがなくなり、証明書管理の負荷を低減

証明書配布方法

ユーザの負担軽減

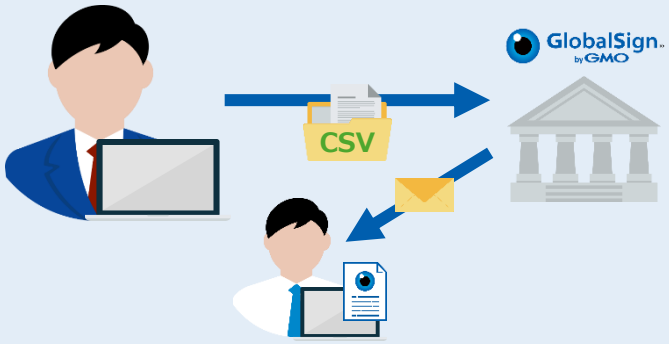
管理者一括申請/一括取得



管理者が管理画面上からcsvで情報を一括で入力し、その情報を基に発行された証明書を管理者がダウンロードします。

利用ケースNo.1

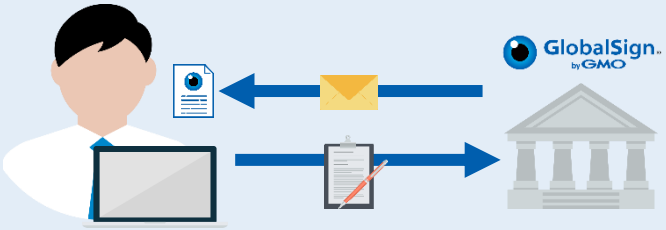
管理者(一括)申請/ユーザ取得



管理者がcsvで入力したメールアドレス宛に、証明書取得用のURLが記載されたメールが届きます。メールを受信したユーザが証明書をダウンロードします。

管理者の負担軽減

ユーザ申請/ユーザ取得



専用のポータルページから、ユーザ自身が申請し、その申請したユーザ宛に証明書取得用URLが記載されたメールが届きます。

※その他にAPIによる連携も提供しております。

価格

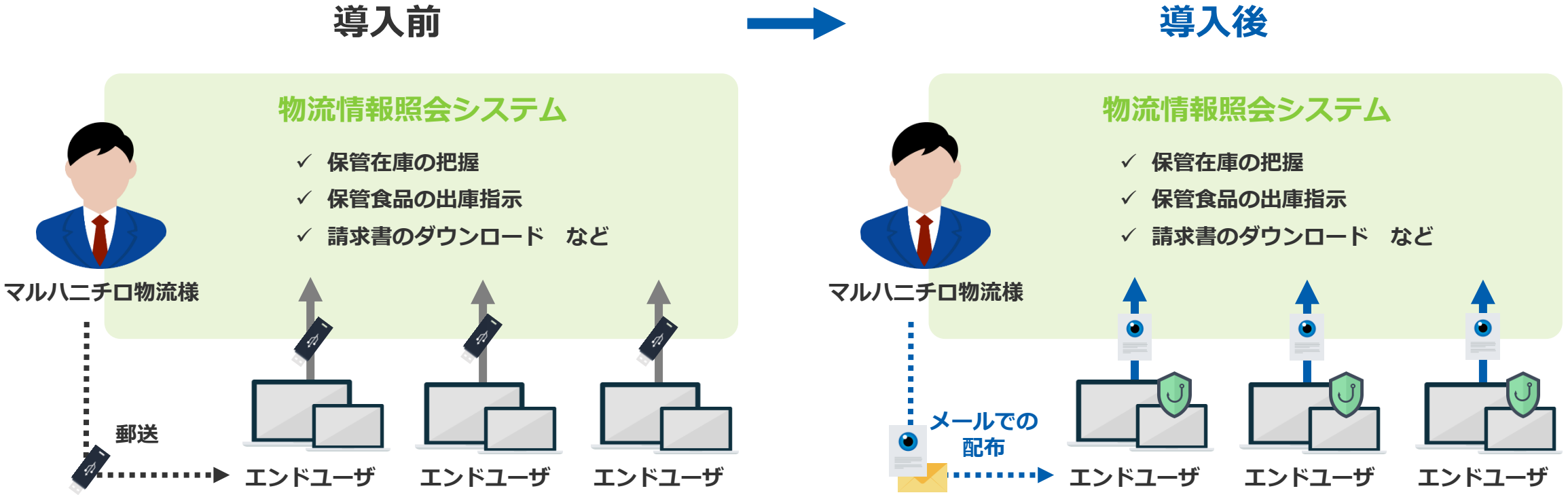
	グローバルサイン	A社
100ライセンス価格 ※証明書有効期間1年	770,000円 ※購入ライセンス数の10%を追加提供	1,380,000円
初期費用/保守費用	無料	有償
提供ライセンス	1ライセンス～	100ライセンス～
無料トライアル	有 ※アクセス認証用途のみ提供可能	不明

利用ケース

MARUHA NICHIRO

課題

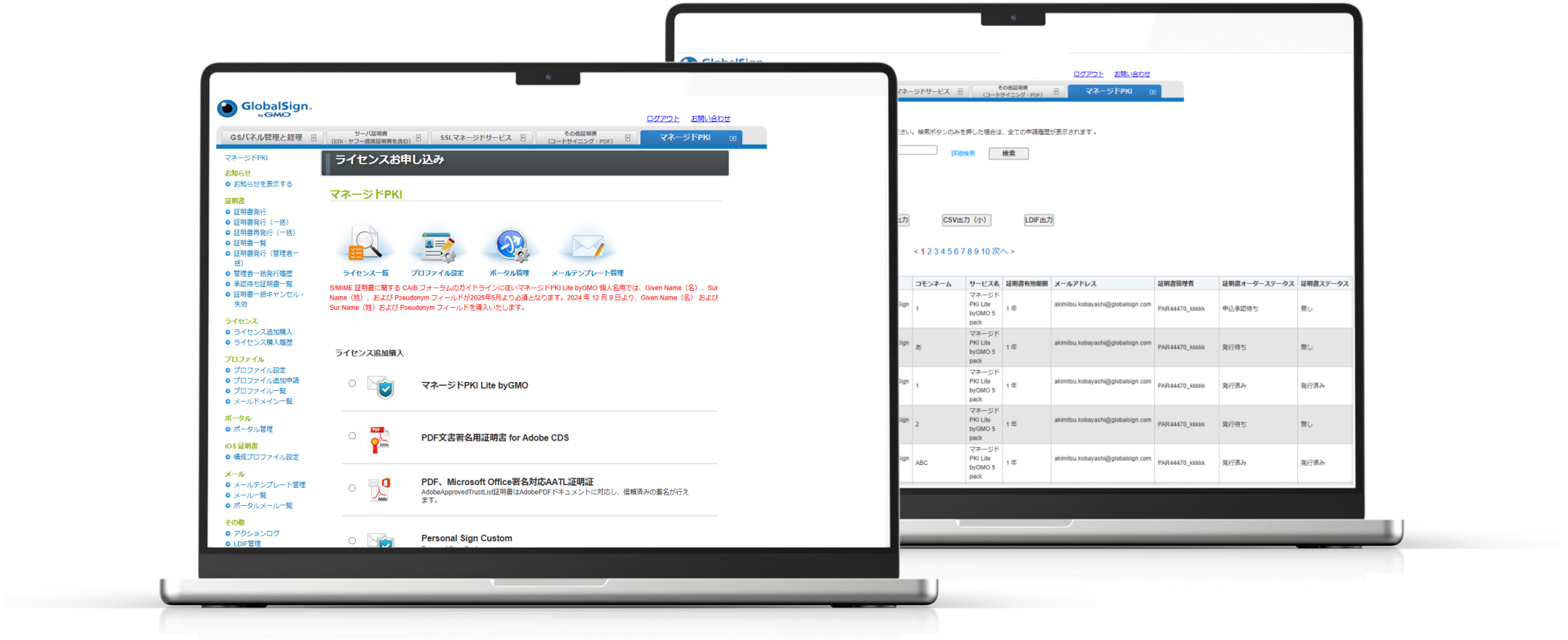
- 利用中の認証方法の安全性の低下や利便性の問題など、エンドユーザへのデメリットがあった。
- システム内の情報が認証情報の漏えいした場合の被害が大きい。



引用元：GMOグローバルサイン株式会社「マネージドPKI Lite byGMO 導入事例　株式会社マルハニチロ物流様」

無料トライアル

お客様のご利用用途に合わせたテスト証明書を提供
管理画面の操作もテスト環境でお試し可能



まとめ

サプライチェーンで必要な不正アクセス対策

アクセス権限とアカウントの適切な管理

- 管理権限は一部ユーザのみに付与
- 適切なユーザに正しい認証方法の割当
- 不要となったアカウントは
  アクセスできないように対応

×

一部の認証方法の限界

- パスワード認証は複雑さや長さ関係なく
  突破されてしまう
- パスワード認証の以外の一部の認証方法も
  突破される可能性が高まっている

▼

クライアント証明書で不正アクセス対策を実現

お問い合わせ

GMOグローバルサイン株式会社

〒150-0043

東京都渋谷区道玄坂1-2-3 渋谷フクラス

https://jp.globalsign.com/

電子証明書事業本部

TEL： 03-4545-2300

MAIL：sales-jp@globalsign.com

"回らない"脆弱性対策を、AI活用で「自走する運用」へ

サプライチェーンリスクに備えるための

「自動化」アプローチ

登壇者紹介

株式会社エーアイセキュリティラボ

CX本部プリセールスリーダー　**髙橋 貴弘**

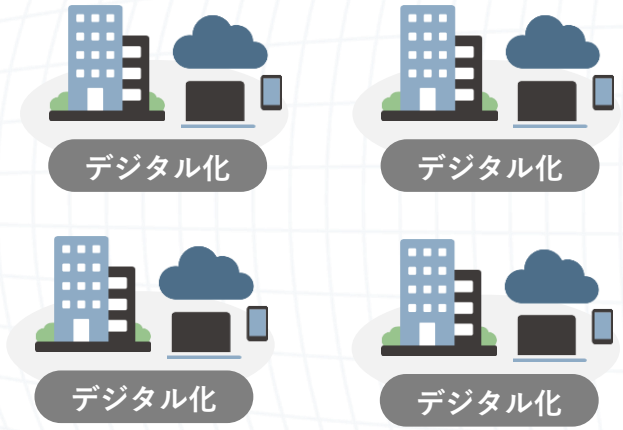
小売店向けPOSレジサービス等のセールスとして約3年間従事したのち、定期通販向けカートシステム業界にてカスタマーサクセスリーダーを担当。
ECサイトにおけるDX推進を100社以上支援し、業務フロー改善やKPI設計にも深く関わる。
2023年より現職。プリセールスリーダーとしてAeyeScanの導入支援に多数携わり、エンタープライズからSaaSスタートアップまで、さまざまな企業の課題解決を支援している。

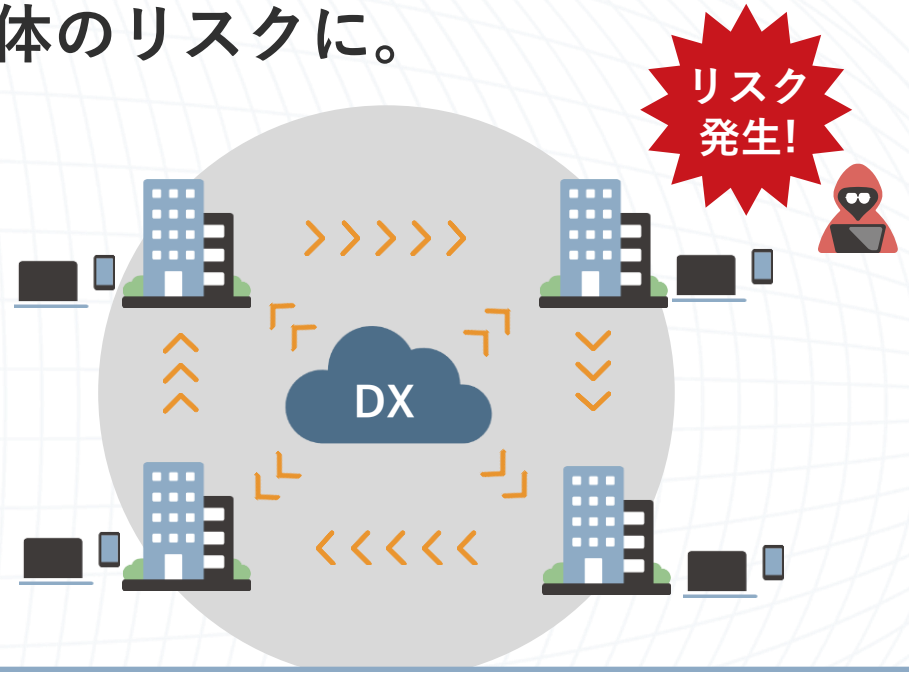
デジタル資産に潜む「見えないリスク」に気づいていますか？

AeyeSecurityLab

DXの進展に伴い、サプライチェーンリスクが拡大

企業間連携が進み、脆弱性がサプライチェーン全体のリスクに。





DX初期：社内業務のデジタル化

セキュリティ対策が不十分な
「即席デジタル」の乱立

DX中期：企業間連携のデジタル化

「即席デジタル」との連携で
サプライチェーン全体が脆弱化

昨年はサイバー攻撃、特にランサムウェアによる被害が話題に

大手飲料メーカー

2025年9月、ランサムウェア攻撃により、システム障害が発生。**国内グループ各社の受注・出荷業務が停止。**さらに個人情報が流出した可能性があると発表された。

大手通販業者

2025年10月、ランサムウェア攻撃によりシステム障害が発生し、受注・出荷業務が停止。**同社の子会社に配送の一部を委託する別会社のECサイトも停止に。**

業務停止・システム停止による事業影響、社会的信頼・株価への影響だけでなく

取引先やグループ会社、サプライチェーンを巻き込む被害に発展

AeyeSecurityLab

多様化するランサムウェアの「侵入経路」

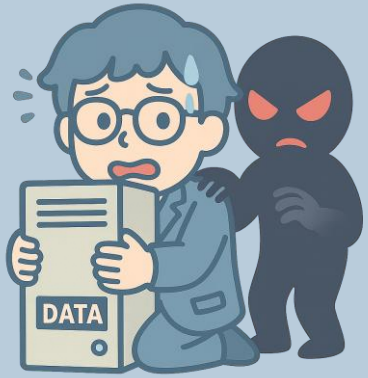
NW機器/VPN

クラウド

Webサイト

CMS/SaaS

PC/社用端末



メール/ファイル

「見えないリスク」は、どうやって生まれ、どこにあるのか？

公開するWebサイトや提供するWebサービスが増えている

開発規模・サイト規模が大きくなっている（100画面以上ある）

機能改修・追加などリリース頻度が高く間隔も短くなっている

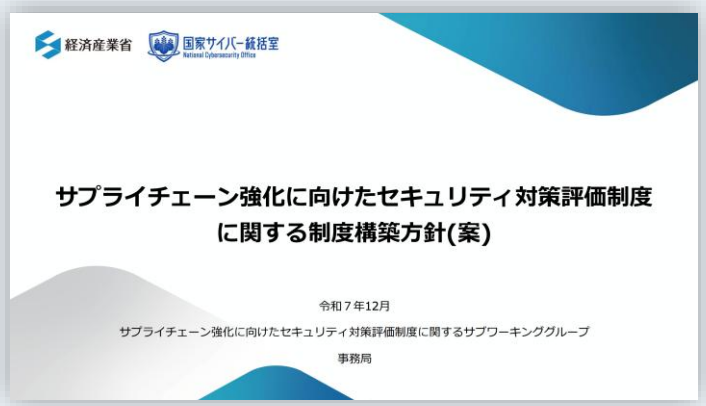
知らないうちに作られ公開されていたWebサイト

新規リリース時に診断したきり何もやっていないWebサイト

リリース前の診断が追い付かず脆弱性が残っているWebサイト

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

Web領域のセキュリティ対策だけでも、広範に及ぶ

Webアプリケーションのセキュリティ対策項目

Webアプリケーションのセキュリティ対策

① ファイルの公開設定
② Webページの公開設定
③ 脆弱性への対策
④ ソフトウェアの脆弱性対策
⑤ エラーメッセージの設定
⑥ ログ管理
⑦ 暗号化
⑧ 不正ログインへの対策

Webサーバのセキュリティ対策

⑨バージョンアップを行う
⑩ 不要なサービス・アプリケーションの停止
⑪ 不要なアカウントの削除
⑫ 安全なパスワードの設定
⑬ アクセス制御
⑭ ログ管理

ネットワークのセキュリティ対策

⑮ 不要な通信の遮断
⑯ 通信のフィルタリング
⑰ 不正な通信の検知・遮断
⑱ ログ管理

その他のセキュリティ対策

⑲ クラウドサービスへのセキュリティ対策
⑳ Webアプリケーション・Webサーバ・ネットワークへの定期的な脆弱性診断

参考：安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～

ただでさえやることがいっぱいなのに、
制度対応もしないといけないのか…

IT部門・セキュリティ部門の皆様から伺う「お悩み」

予算が限られている

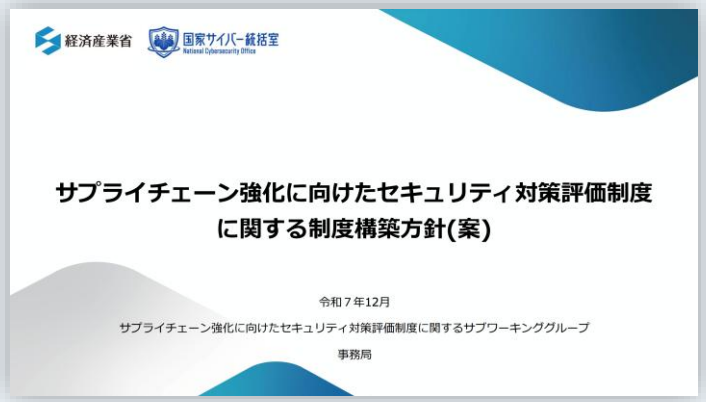
人員も限られている

対策すべき範囲 増

必要な対策の幅 増

まずは「攻撃手法・対策方法が分かっている」部分から対策

★3、★4で想定されている“既知の脆弱性”から対策する＝穴を塞ぐことが最優先。
未知の攻撃への防護策を考えるのは、その次でOK。



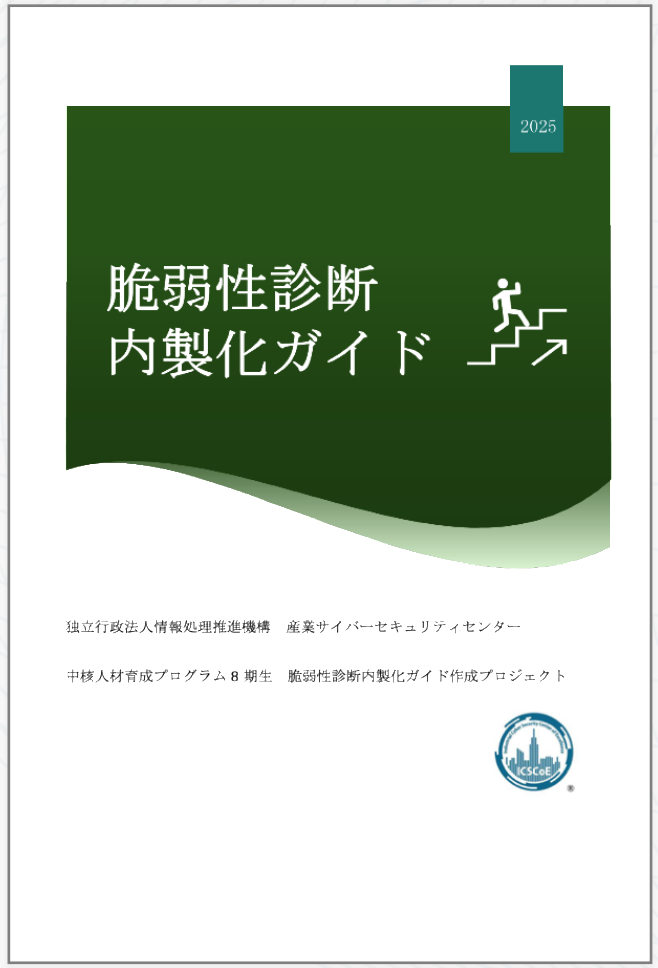
セキュリティ対策の
成熟度を3段階で評価

	脆弱性診断		
	★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

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

IPA（独立行政法人情報処理推進機構）から脆弱性診断内製化ガイドが公開



公開の背景

脆弱性の早期発見がますます重要に

- 事業継続
- 信頼性維持の観点

内製化への関心が高まっている

- 新たな脆弱性の増加
- リリースサイクルの高速化

主な内容

- 外部発注と内製の違い
- 内製化に必要な組織体制と人材
- 内製化の進め方と継続的改善プロセス
- 関係組織との連携とセキュリティ意識の醸成
- ツール選定におけるポイント

参照：IPA「脆弱性診断内製化ガイド」 https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2025/Vulnerability-assessment.html

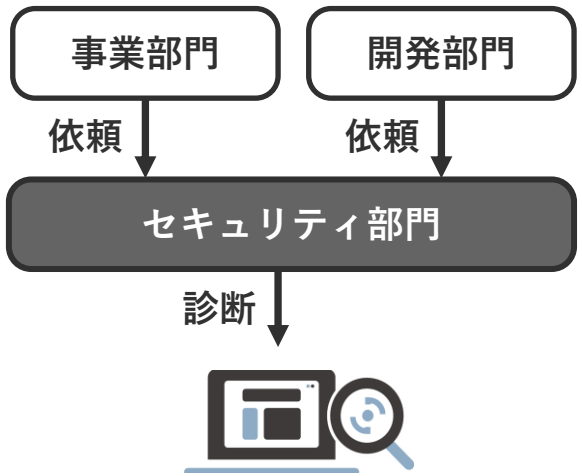
脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 0 運用体制の構築・役割分担

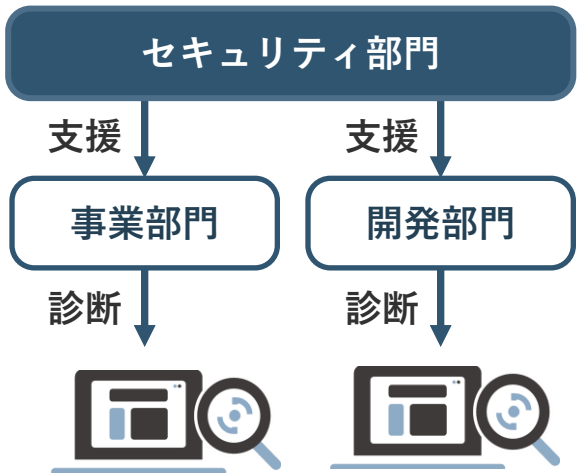
従来の運用体制

セキュリティ部門が
まとめて診断



これからの運用体制

**事業部門・開発部門が
脆弱性診断を実施できる
体制**を構築



メリット

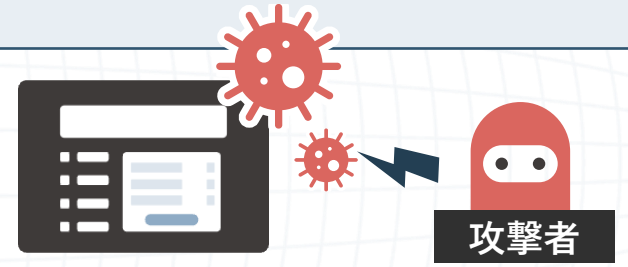
- シフトレフトの実現
- 診断対象の的確な把握
- セキュリティ意識の醸成

STEP 1 情報収集・対象の把握

自社で管理すべきWebサイトの棚卸＆探索により、診断対象の全体把握が重要

某大手ハウスメーカー（A社）さまの事例

某日、A社が運営サイトのアクセスが急増し、高負荷状況に…
調査した結果、**過去に3年程度オープンしていたWebサイトの現在は運用していないページが攻撃を受けていた**ことが判明



ページが公開されていたこと、アクセス可能であることは認識されていたのか？

気付いたら「さくっと」
Webサイトができている…

開発後・リリース後も検証環境や
テスト環境がひっそり残っている…

STEP 2 診断の必要性や優先順位を評価、対応方針の検討

スコープを明確にし、**優先順位・必要を評価して対策の濃淡をつける**ことが重要

診断対象の棚卸し

診断の必要性を評価

- 取り扱っている情報の重要度
- ビジネス上の重要度
- 監督官庁・業界団体のガイドライン
- リリース・アップデート頻度(開発体制)

対策方針の検討

診断方法

- 外部委託
- 社内診断(内製化)

診断タイミング

- 新規リリース
- 改修・追加開発
- 定期診断

STEP 3 診断計画の立案と実行・進捗の全体管理

Webサイト・Webアプリを開発している部門との情報連携・協業が「ミソ」

診断計画を立てる

リリース前の診断

開発プロジェクトのキックオフ等に参加し、スケジュールを事前に確認しておく

定期診断

実施時期を各プロジェクトと事前に調整しておく

診断の実施準備をする

開発部門と情報連携し、診断要件を確認する

例

診断対象の基本情報

対象システム、対象 IP アドレス、対象 URL・診断用アカウント、保有するデータ 資産分類（個人情報、クレジットカード情報など）等

技術仕様に関する情報

システム仕様や構成図、フレームワーク、外部連携サービス 等

診断実施にあたっての確認事項

診断アクセスによるメール等の外部通知の有無 等

STEP 4 検出された脆弱性の評価と対応

評価の理由・根拠(特に対応不要とした場合)と、**対応履歴を残しておく**のが大事

診断結果の確認

→

修正対応の必要性を評価

- CVSS等の深刻度
- 発生しうる被害・リスクの大きさ
- 修正にかかるコスト(工数・費用)
- リリースまでに残された時間

など

→

対策方針の検討

- リリース前に必ず修正する
- 次回リリースまでに必ず修正する
- 大規模修正で修正
- 現時点では対応不要

進め方はわかったけど
うちの会社でもできる…？

脆弱性診断を内製化するときに考えること

「内製化できればいいんだけどな…」

診断の**品質を維持**できるだろうか？

診断員を**育成・確保**できるだろうか？

コスト(費用・時間)を削減できるか？

脆弱性診断を内製化するときに考えること

診断の**品質を維持**できるだろうか？

診断員を**育成・確保**できるだろうか？

コスト(費用・時間)を削減できるか？

プロ級の機能・性能

誤検知・過検知が少なく
外部委託（手動診断）に近い性能

誰でも使える操作性

ツール習得コストがかからず
すぐに・簡単に利用できる

利用範囲・回数が無制限

画面数やサイト数に制限がなく
いつでも・いくらでも使える

AeyeSecurityLab

生成AI時代の脆弱性診断なら AeyeScan

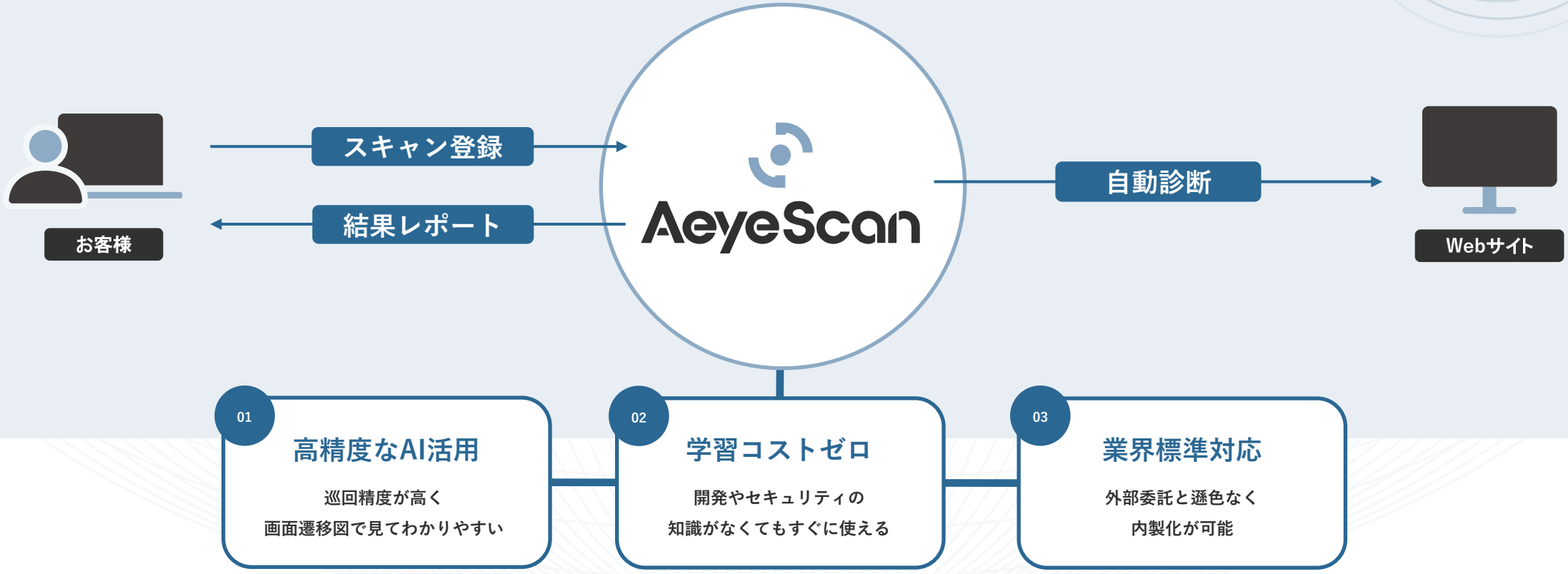
クラウド型Webアプリケーション
脆弱性検査ツール

国内市場シェア
No.1※

※富士キメラ総研調べ「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）

有償契約
300社以上

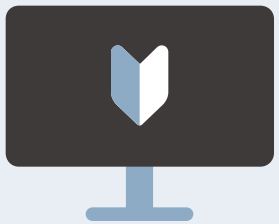


01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

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

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。

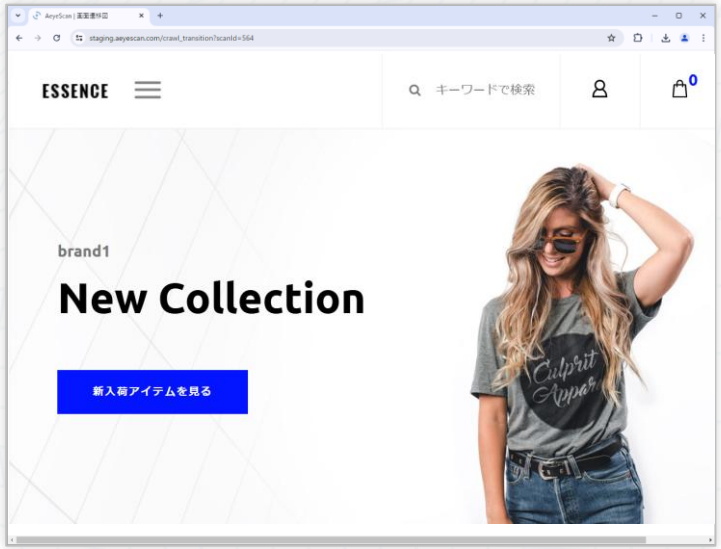
AIによる自動診断

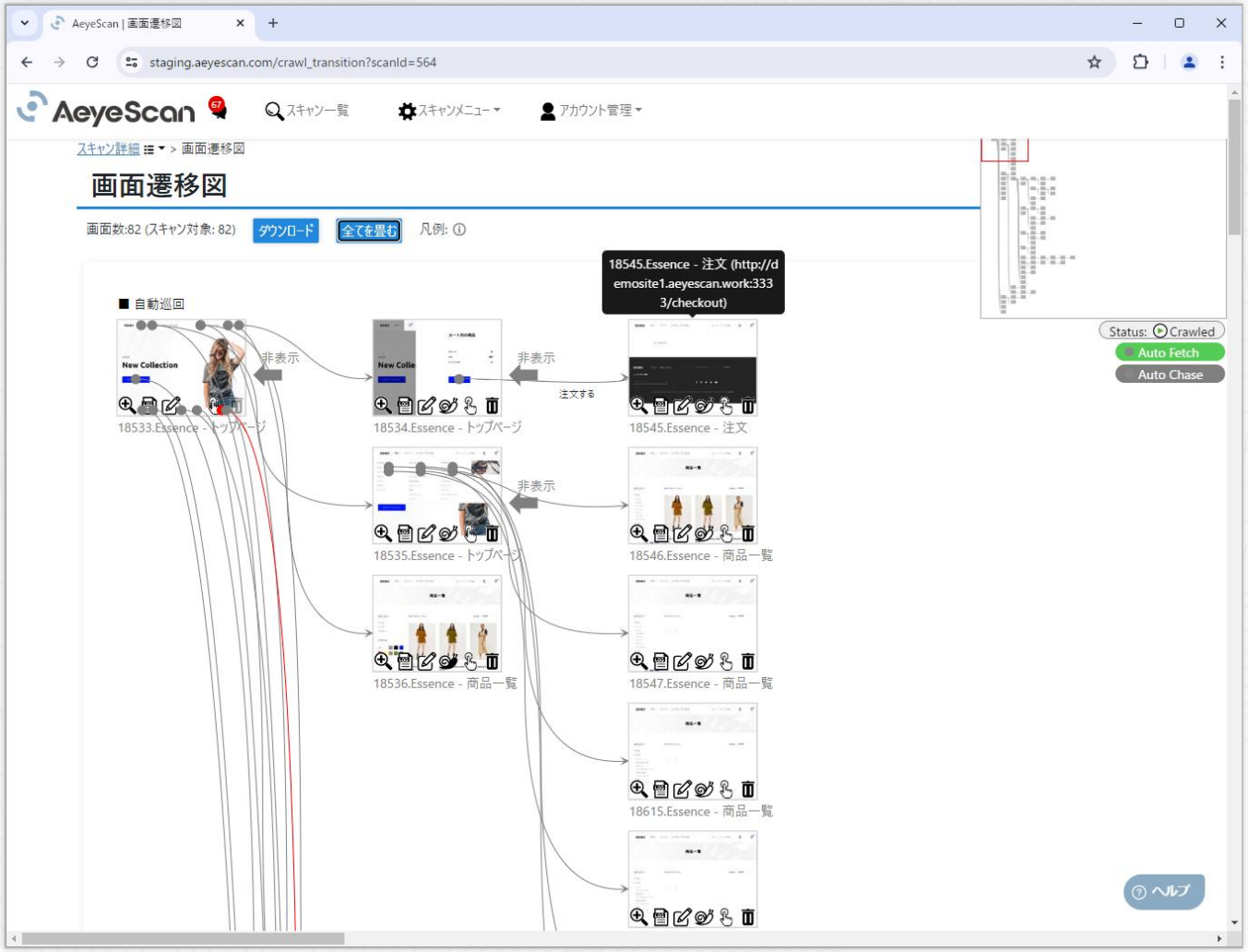
圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。

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。

巡回時に、自動で画面遷移図を生成



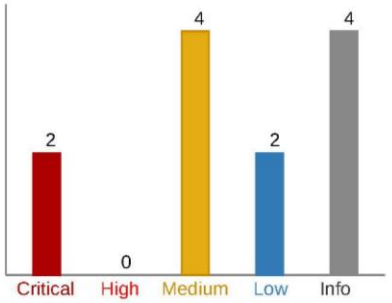


AeyeSecurityLab

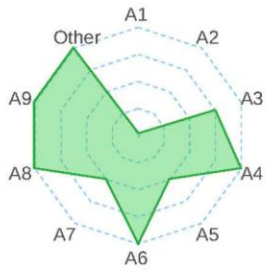
結果がわかりやすく、すぐさま修正作業に取り組めるレポート

スキャンサマリー

全体評価　Critical



深刻度ごとのサマリー



OWASP TOP 10 カテゴリー

脆弱性の深刻度はCVSSv3 (https://www.ipa.go.jp/security/vuln/CVSSv3.html) に基づき以下の基準で設定しています。

深刻度	CVSSv3基本値	脆弱性に対して想定される脅威
Critical	9.0～10.0	・リモートからシステムを完全に制御されるような脅威 ・大部分の情報が漏えいするような脅威 ・大部分の情報が改ざんされるような脅威
High	7.0～8.9	
Medium	4.0～6.9	・一部の情報が漏えいするような脅威 ・一部の情報が改ざんされるような脅威 ・サービス停止に繋がるような脅威 ・その他、Critical/Highに該当するが再現性が低いもの
Low	0.1～3.9	・攻撃するために複雑な条件を必要とする脅威 ・その他、Mediumに該当するが再現性が低いもの
Info	0	

スキャン結果詳細

Critical

SQLインジェクション

深刻度

Critical

CVSS Score: 9.8
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

概要

危険な文字列をSQL文に挿入できます。そのため、攻撃者が任意のSQL文を実行できる危険性があります。

OWASP TOP 10 カテゴリー

A1:2017-インジェクション

ASVS4.0 カテゴリー

5.1.2,5.1.3,5.1.4,5.3.1,5.3.4,5.3.5,13.2.2,13.3.1

解説・対策方法

SQLインジェクションとは、攻撃者が細工した入力値を送信することで、開発者の想定していないSQL文を実行できてしまう脆弱性です。この脆弱性は、利用者の送信した値が適切に前処理されずにSQL文の一部として利用されることが原因で発生します。

この脆弱性を悪用することで、データベースの情報漏洩や情報改ざんなど、開発者の想定していない処理を実行されてしまう危険性があります。

対策方法としては、想定していない値が入力された場合に処理を中断することや、SQL文で特殊な意味を持つ文字を無害化することが挙げられます。後者を実現する一般的な方法としては、パラメータ化クエリやプリペアードステートメントの利用が挙げられます。

参考情報

安全なウェブサイトの作り方 - 1.1 SQLインジェクション | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 (https://w

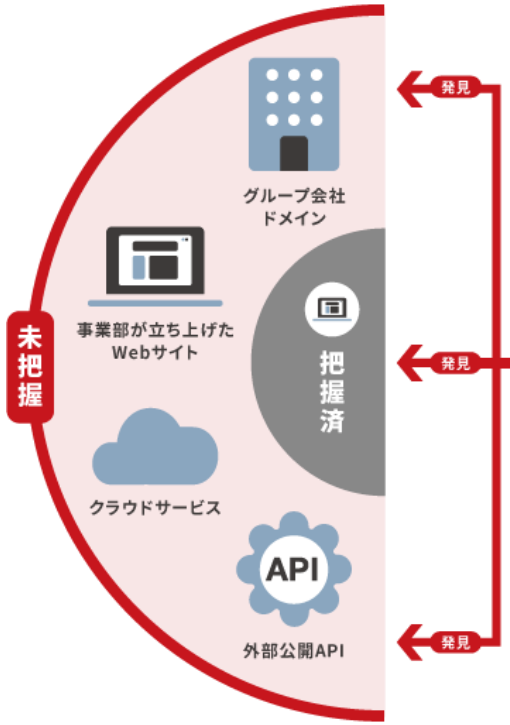
AeyeSecurityLab

生成AI活用で、工数をかけずにWeb-ASMを実現

オプション機能

Web-ASMとは？

把握していないWeb資産（攻撃面）の継続的な発見・リスク評価



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

判定理由やリスクの深刻度も
日本語でわかりやすく解説

Web-ASMの実施ステップ

1 攻撃面の **発見**

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**

属性やミドルウェア・
ライブラリの情報を収集

3 攻撃面の **リスク評価**

資産の重要度と
リスクの深刻度を提示

AeyeScan Web-ASM機能が、これらの作業を自動化

AeyeSecurityLab

【新機能】資産の探索からプラットフォーム診断までワンストップ！

NEW

探索・発見

自社に紐づくと思われる
Web資産を、生成AIが探索

ドメイン・Webサイト等の
発見経路／判定理由も説明

➡ブラックボックス化を防止

精査・評価

資産情報の収集、資産の精査
リスク評価・優先度付を支援

CVSS/EPSS/KEV等の指標
＋ビジネス観点の重要度

➡多角的な精査・評価を楽に

検査・監視

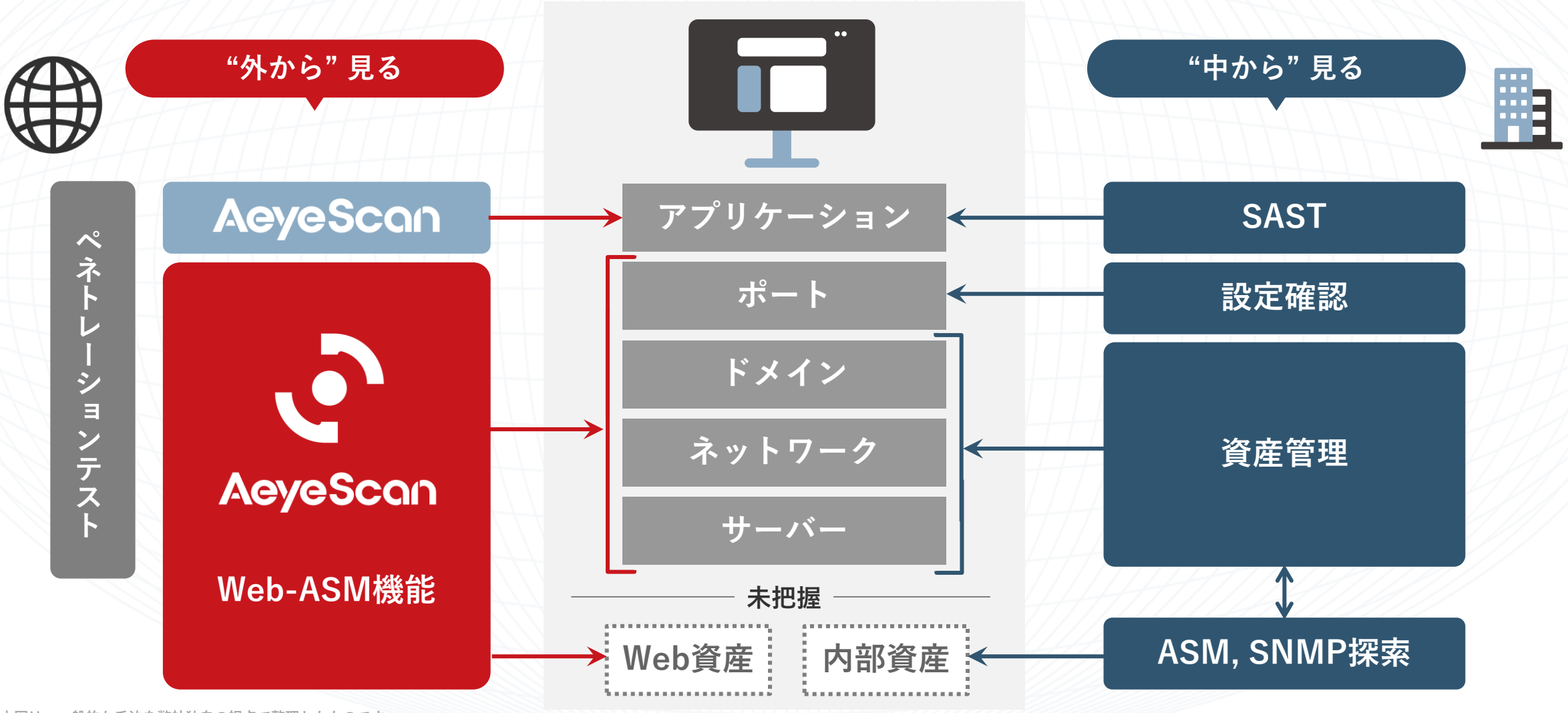
プラットフォーム　ネットワーク

PF診断やNW診断を含む
自社資産の定期的なスキャン

ポートスキャン/NWスキャン
での潜在的リスクチェック

➡全資産のモニタリングも

AeyeScanは、外から見る「セキュリティ診断」を網羅します



※本図は、一般的な手法を弊社独自の視点で整理したものです

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

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 / HOUSE RETAILING / NTT EAST / odakyu / 近鉄情報システム株式会社 / G-FAS / SymEnergy / 水ing Swing Corporation / Suzuyo / TOYOTA HOME / NANKAI / 日本調剤 / JARMeC 日本動物高度医療センター / HITOWA GROUP / BOOK-OFF / ベルーナ / grow up together MEDIA / Looop / Loyalty Marketing, Inc.

エンタメ

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

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

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

人材・教育

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

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア / Lexica E-Retailing Platform / エフアンドエムネット株式会社 / 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 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 / Simplex Inc. / 777WORKS / SOFT CREATE / SOLTEC / 高千穂交易株式会社 / TDI / 電通総研 / TOPPAN / JOPS / JAST / PCNET / Human Interactive Technology Inc. / FUJISOFT / FUJITSU / MACROMILL / 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

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

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