

SYZD Research合同会社

Emulating the Unknown

「脅威インテリジェンスに基づく攻撃者エミュレーションサービス」

税込20万円から提供

脅威情報で攻撃経路を絞り
実際の攻撃の際に使用され得る脆弱性を特定する

独自インテリジェンス基盤『SYZD-INTEL』から攻撃基盤・ツール・手口を選び、お客様の環境に合わせた攻撃シナリオを非破壊で実行します。
推測による警告リストではなく、**実際に攻撃が成立した証拠と具体的な改善方針**を持ち帰れる評価サービスです。

何を確かめるか	公開領域やログイン後の画面・APIに対し、攻撃の成立条件・到達範囲・阻止に有効な対策。 現行の攻撃者像とAI自動化型の攻撃を、対象範囲に応じて組み合わせて評価し、レポートには検出ツール/経路を明記。
何を持ち帰れるか	実行結果と証拠（PoC）付きの評価報告書、優先して直すべき改修方針・修正要件、取引先提出用の『セキュリティ評価実施記録』。
どう利用するか	単発のスポット評価（20万〜40万円・複合シナリオは60万円〜）で実施。改善後の再検証や定期点検も相談可能。

※ 対象範囲・前提条件は、ご相談時に書面で確定します。

AI・自動化によりWeb面への攻撃が増え狙いは情報窃取に移っている

① 2026年秋に相次いだAI・自動化ツール悪用事例

・韓国の金融機関への情報窃取（CrowdStrike｜2026/10/7公表）

攻撃者がAIエージェント型の攻撃ツールとLLMを悪用。サーバーから攻撃ツール設定とLLMのセッション履歴を確認。

・国内でも確認された攻撃試行（JPCERT/CC｜2026/10/23更新）

AIエージェント型の攻撃ツールによる公開Webアプリの脆弱性探索や、設定・バックアップファイルの窃取が報告。

② 攻撃の入口はWeb面、目的は情報窃取

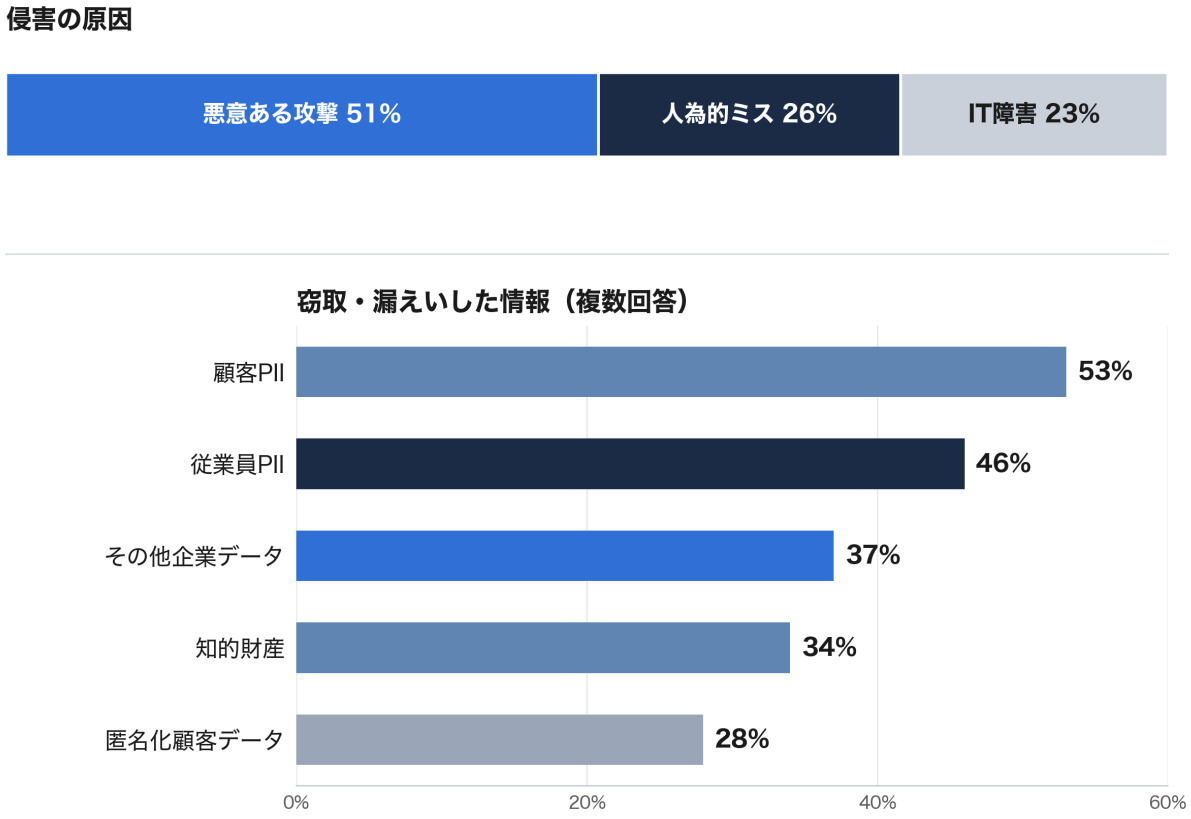
・公開Web面の脆弱性探索、設定・バックアップファイルの窃取が報告されている。

・設定・バックアップファイル、認証情報、顧客データを窃取。

③ 対策の起点は「自社のWeb面が実際に破られるか」

当サービスでは、観測された手口を自社環境で非破壊に再現し情報資産への到達可否を確認します。

情報漏洩の原因と標的



出典：CrowdStrike（2026/10/7）、JPCERT/CC「JPCERT-AT-2026-0030」（2026/10/23更新）、IBM「Cost of a Data Breach Report 2025」

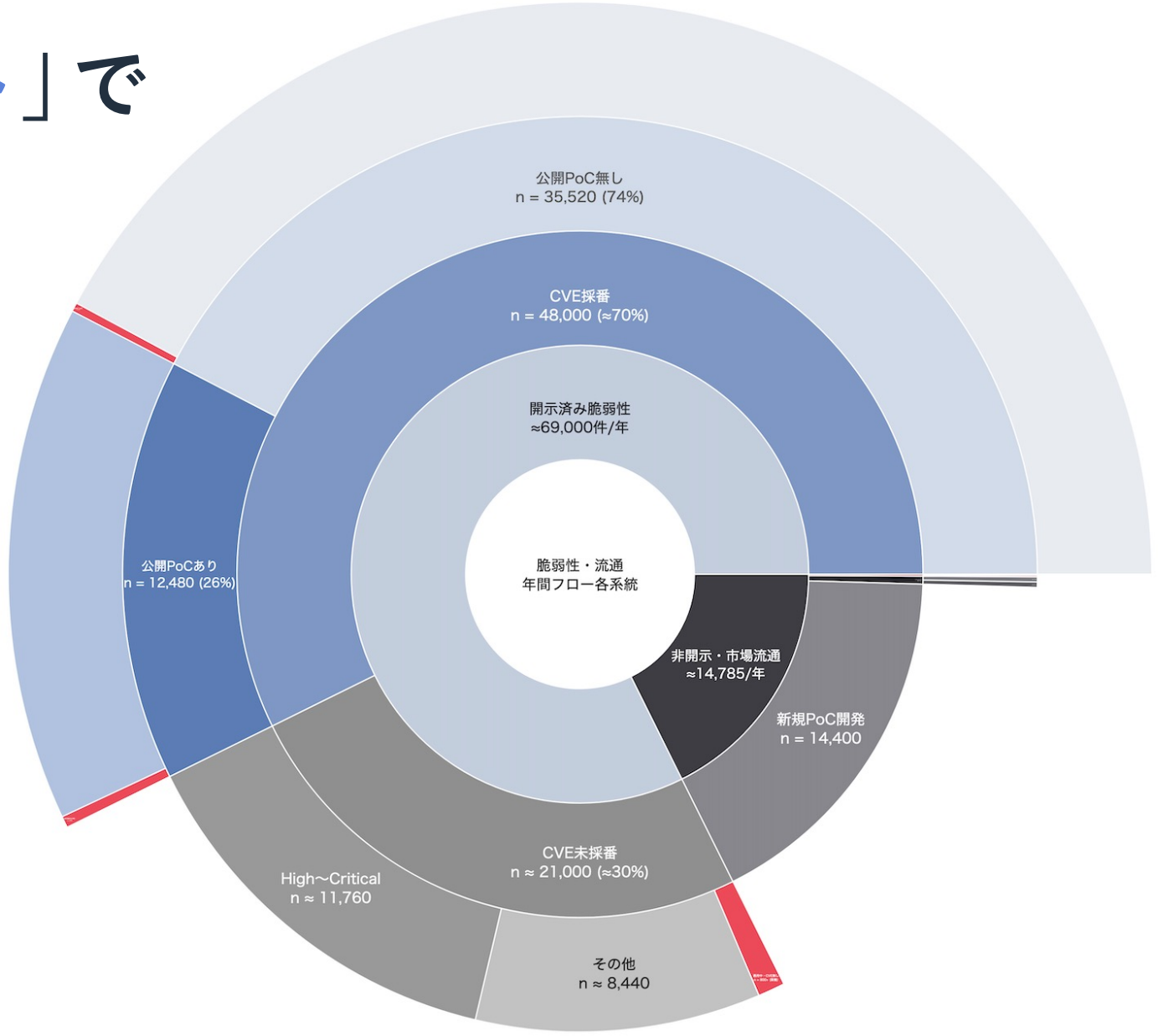
「脆弱性診断・ペンテスト」で満足していませんか

① 最も危険な領域がスコープから外れている

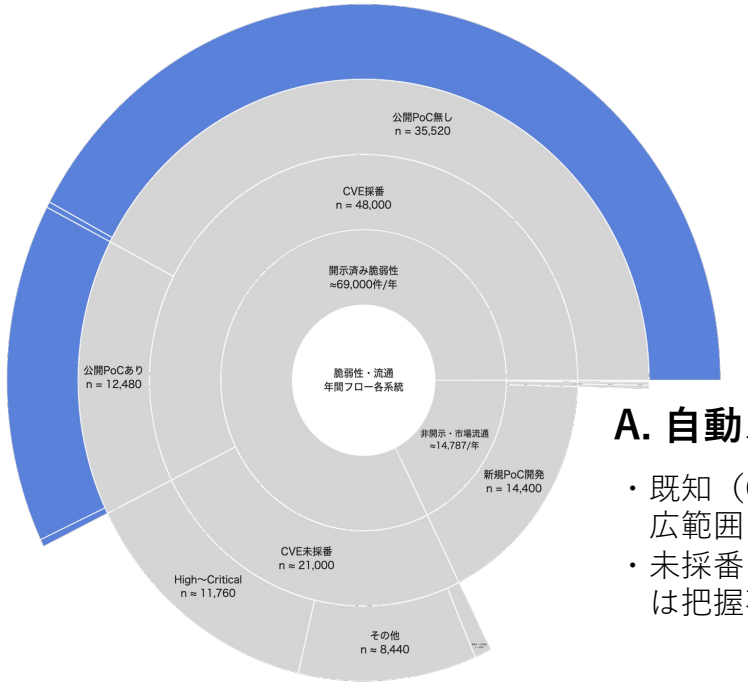
- 未採番リスク： 開示脆弱性の30%（約2.1万件）はCVEがなく、その半数以上が深刻（High〜Critical）
- 水面下リスク： 非開示・市場流通が年約1.5万件。CVEのない悪用事例も多数（累積800件超）
  - ↳ **「診断で検知ゼロ＝安全」ではない**

② 危険ではないアラートの対処に忙殺されている

- CVE採番（4.8万件）のうち、74%は攻撃コード（PoC）すら存在しない
- 実際に悪用実績がある脆弱性はわずか約480件（1%未満）
  - ↳ 攻撃されない脆弱性のパッチ当てに追われ、本来防ぐべき脅威に対処できていない

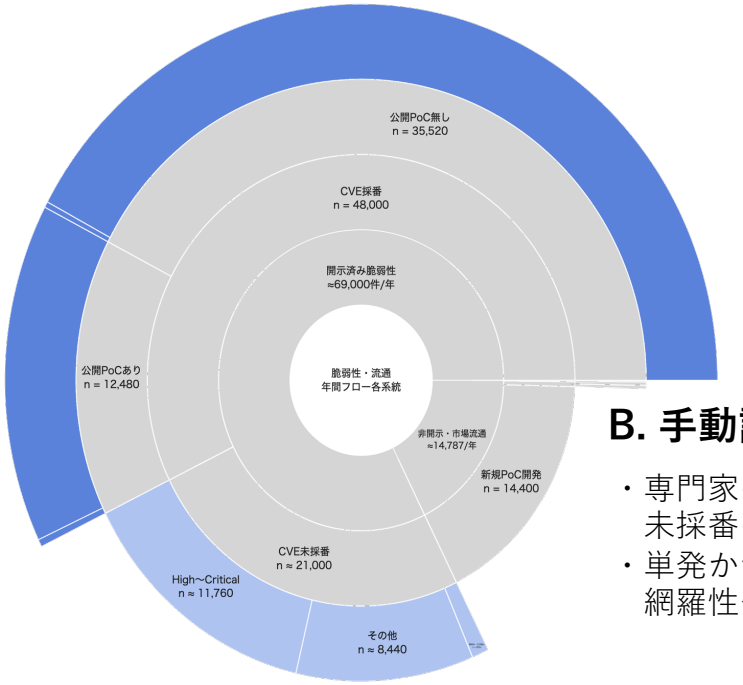


出典: VulnCheck EIR 2025 / State of Exploitation・Flashpoint VulnDB/KEV (2026-02時点)・CISA KEV (rxerium集計)・Google GTIG 0-day Report 2024・Kaspersky出品調査 (2023.1–2024.9) の公表値を基に当社作成。
注: 角度は件数に比例し、外縁の段差は階層深度差。総数≈83,787は測定系の異なる年次フローの形式的和。開示計≈69,000は非CVE比率28–33%による区間推定[66,667–71,642]の中央値。悪用≈480は公表1%推定とKEV追加884件×47.7%(≈422)の二経路で検証済み。「≈」は母集団の異なる公表比率を当年へ適用した輸送推計。市場出品≈312は実績547件/21ヶ月の年率換算。悪用中・CVE無し800+は累積値(年次内訳未公表)。



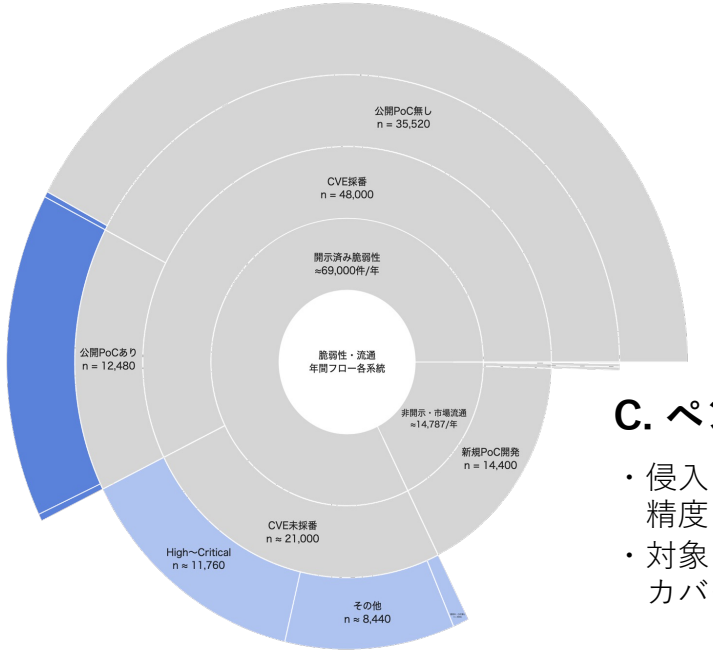
A. 自動スキャン

- 既知（CVE採番済み）の脆弱性を広範囲にリストアップ
- 未採番の欠陥や実際の悪用リスクは把握不可



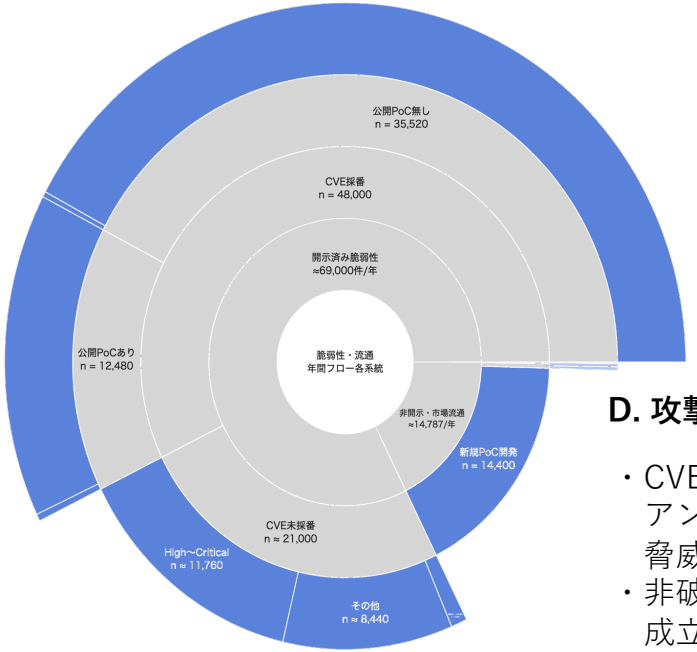
B. 手動診断

- 専門家の手動検証により、未採番の欠陥も深掘り可能
- 単発かつ限定スコープのため、網羅性や最新脅威への追従に限界



C. ペンテスト

- 侵入・侵害の成立可否を実証する精度は最高峰
- 対象は侵入ルートとなる一部に絞られ、カバー範囲は極小



D. 攻撃者エミュレーションサービス

- CVE有無の全域に加え、PoCやアンダーグラウンド市場流通の脅威を常時監視
- 非破壊検証により「実際に攻撃が成立する証拠」を可視化

既存サービスとの位置づけと目的・守備範囲の違い

比較項目	A. 自動スキャン	B. 脆弱性診断（手動）	C. ペネトレ・TLPT	D. 攻撃者エミュレーションサービス
主な目的	既知の弱点を 幅広く一覧化する	仕様書に基づき対象内の 弱点を洗い出す	特定の攻撃目標への 到達可能性を検証する	**現実に使われる攻撃手口への 耐性と優先対策を確かめる**
設計の起点	機械クローラーと 既知CVEリスト	事前定義された検査項目と アプリケーション仕様	合意した侵入目標と 組織固有の演習シナリオ	**脅威情報（SYZD-INTEL）に 基づく攻撃基盤・手法の再現**
主な成果物	ツール出力レポート （推測アラートが混在）	指摘事項一覧と 一般的な修正方針	侵入経路の演習報告書と 防御・運用の改善提案	**成立・阻止の証拠（PoC）と 優先改修方針・セキュリティ評価実施記録**
費用・期間の目安	月額 数千円〜数万円	50万〜200万円 （1〜2ヶ月）	200万〜1,000万円 （2〜3ヶ月）	**20万〜40万円（複合 60万円〜） （最短2営業日〜1ヶ月）**

※各サービスには重なる領域があります。静的サイトの簡易点検には自動スキャン、大規模な組織演習にはTLPT専門会社との併用も推奨しています。

観測された攻撃者の手口をもとに
検証シナリオを作成し検査する

SYZD-INTEL
脅威インテリジェンス基盤

攻撃基盤・AI Harness
ARTEX等の自動化基盤・スクリプト
探索ツールの構成と実行手順

悪用脆弱性（N-day / 未採番）
CISA KEV・公開PoC・GHSA
修正前の実質0-day・設定不備

侵入後の行動・窃取目標
権限昇格・他テナント横断参照
設定・バックアップ・認証情報

観測条件と再現性の精査
顧客の技術スタックとの一致判定
非破壊で実証可能な範囲の特定

顧客環境の構成と照合し、各段階の攻撃シナリオへ変換

STAGE 01 初期侵入	STAGE 02 実行・展開	STAGE 03 権限拡大	STAGE 04 横展開	STAGE 05 目標到達
対象：公開領域・認証境界	対象：アプリケーション・API	対象：アカウント・権限境界	対象：内部連携・データ基盤	対象：重要情報の保護確認
主な検証内容 ・公開Web / API / BI露出探索 ・既知悪用脆弱性（KEV）の検証 ・認証バイパス・設定不備の検証	**主な検証内容** ・攻撃者のAI Harness・ツール実行 ・非公開API・管理機能の探索 ・サーバー処理への干渉可否検証	**主な検証内容** ・一般権限から管理機能の呼出検証 ・他社・他ユーザーIDの不正参照 ・トークン・セッション不備の検証	**主な検証内容** ・WebからBI・内部APIへの到達 ・クラウド設定情報の参照可否 ・境界防御による遮断の有効性確認	**主な検証内容** ・重要データへの到達可否を実証 （※実データの窃取・改変なし） ・各段階の「成立・阻止」を記録
明らかになること **外部から侵入できる経路の有無と成立条件**	明らかになること **侵入起点から実行可能な操作とアプリケーションの耐性**	明らかになること **低い権限から上位権限や他者領域へ昇格できるか**	明らかになること **一部の侵害から他システムへ横展開できる範囲**	明らかになること **守るべき重要情報に到達されるかどの対策が阻止に有効か**

※起点・手順・到達目標は、脅威情報（SYZD-INTEL）とお客様の対象環境・合意条件に応じて設定します。

全体の流れ

ご依頼

ご依頼を受けたら、授権確認・実施範囲（ROE）の合意・調査専用IPの通知を行います。

対象確定・脅威照合

ターゲットとエンドポイントを確定し、SYZD-INTEL DBと照合して影響しうる脆弱性情報を取得します。

AI Harness + 攻撃者ツールで調査

実際の攻撃者が探索・調査に使う手法で、対象となる全てのエンドポイントを調査します。

影響する脆弱性の確定・記録

N-dayや上流での未修正脆弱性、設定ミスなど影響するものを洗い出し記録します。

レポート+PoC作成

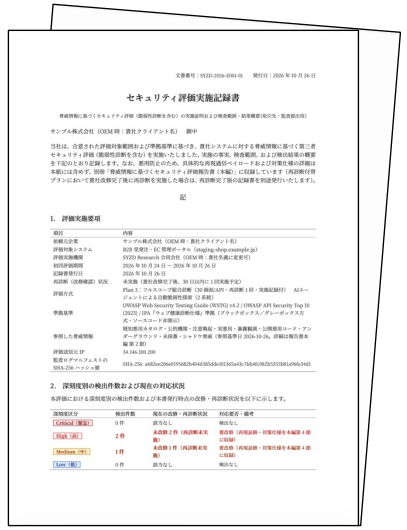
再現手順・改修方針・修正要件などを記録し、成果物となるレポートを作成します。

人間による確認・修正

人間による確認を行います。
この際、AIを併用する場合もございます。

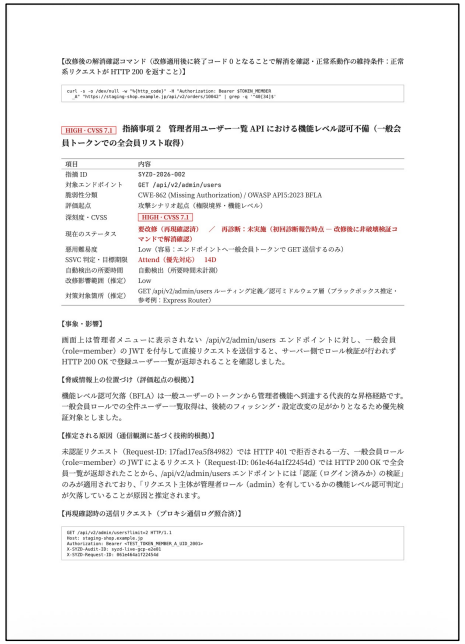
成果物お渡し

レポート・PoC・改修方針・実施記録などの成果物と、GCP上の診断環境および収集データの削除記録をお渡しします。



セキュリティ評価実施記録書

01_取引先提出用_セキュリティ評価実施記録.pdf



【改修後の解消確認コマンド（改修適用後に終了コード 0 となることで解消を確認・正常系動作の維持条件：正常系リクエストが HTTP 200 を返すこと）】

HIGH・CVSS 7.1　指摘事項 2　管理者用ユーザー一覧 API における機能レベル認可不備（一般会員トークンでの全会員リスト取得）

項目	内容
指摘 ID	SYZD-2026-002
対象エンドポイント	GET /api/v2/admin/users
脆弱性分類	CWE-862 (Missing Authorization) / OWASP API5:2023 BFLA
評価起点	攻撃シナリオ起点（機能境界・機能レベル）
深刻度・CVSS	HIGH・CVSS 7.1
現在のステータス	要改修（再現確認済） ／ 再診断：未実施（初回診断報告時点 — 改修後に非破壊検証コマンドで解消確認）
悪用難易度	Low（攻撃：エンドポイントへ一般会員トークンで GET 送信するのみ）
SSVC 判定・目標期限	Attend（優先対応） 14D
自動検出の所要時間	自動検出（所要時間未計測）
改修影響範囲（推定）	Low
対策対象箇所（推定）	GET /api/v2/admin/users ルーティング定義／認可ミドルウェア層（ブラックボックス推定・参考例：Express Router）

【事象・影響】

画面上は管理者メニューに表示されない /api/v2/admin/users エンドポイントに対し、一般会員（role=member）の JWT を付与して直接リクエストを送信すると、サーバー側でロール検証が行われずHTTP 200 OK で全会員ユーザー一覧が返却されることを確認しました。

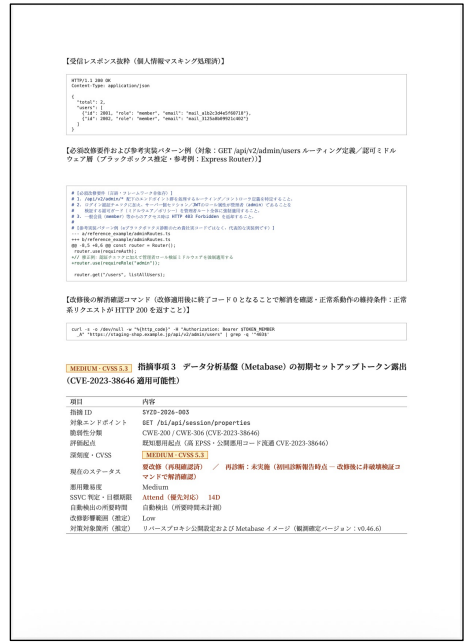
【脅威情報上の位置づけ（評価起点の根拠）】

機能レベル認可欠落（BFLA）は一般ユーザーのトークンから管理者機能へ到達する代表的な昇格経路です。一般会員ロールでの全件ユーザー一覧取得は、後続のフィッシング・設定改変の足がかりとなるため優先検証対象としました。

【推定される原因（通信範囲に基づく技術的根拠）】

未認証リクエスト（Request-ID: 17fad17ea5f84982）では HTTP 401 で拒否される一方、一般会員ロール（role=member）の JWT によるリクエスト（Request-ID: 06le464a1f224544）では HTTP 200 OK で全会員一覧が返却されたことから、/api/v2/admin/users エンドポイントには「認証（ログイン済みか）の検証」のみが適用されており、「リクエスト主体が管理者ロール（admin）を有しているかの機能レベル認可判定」が欠落していることが原因と推定されます。

【再現確認時の送信リクエスト（プロキシ通信ログ照合済）】



【受信レスポンス抜粋（個人情報マスキング処理済）】

【必須改修要件および参考実装パターン例（対象：GET /api/v2/admin/users ルーティング定義／認可ミドルウェア層（ブラックボックス推定・参考例：Express Router））】

【改修後の解消確認コマンド（改修適用後に終了コード 0 となることで解消を確認・正常系動作の維持条件：正常系リクエストが HTTP 200 を返すこと）】

MEDIUM・CVSS 5.3　指摘事項 3　データ分析基盤（Metabase）の初期セットアップトークン露出（CVE-2023-38646 適用可能性）

項目	内容
指摘 ID	SYZD-2026-003
対象エンドポイント	GET /bi/api/session/properties
脆弱性分類	CWE-200 / CWE-306 (CVE-2023-38646)
評価起点	既知悪用起点（高 EPSS・公開悪用コード流通 CVE-2023-38646）
深刻度・CVSS	MEDIUM・CVSS 5.3
現在のステータス	要改修（再現確認済） ／ 再診断：未実施（初回診断報告時点 — 改修後に非破壊検証コマンドで解消確認）
悪用難易度	Medium
SSVC 判定・目標期限	Attend（優先対応） 14D
自動検出の所要時間	自動検出（所要時間未計測）
改修影響範囲（推定）	Low
対策対象箇所（推定）	リバースプロキシ公開設定および Metabase イメージ（脆弱確定バージョン：v0.46.6）

02_セキュリティ評価報告書_本編.pdf

第三者評価の実施記録が取引継続や検収の条件に

① 客観的な証明が受注・信用に直結

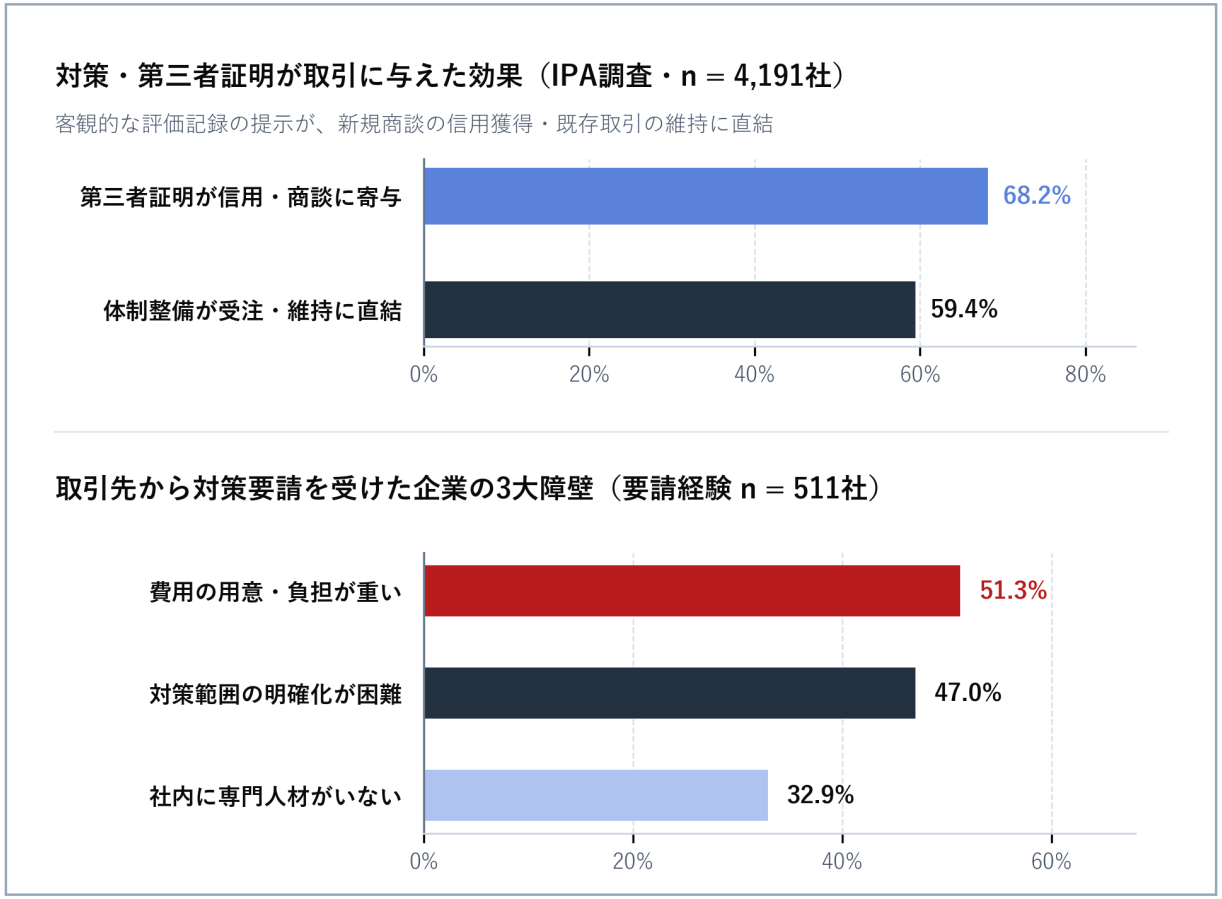
・第三者証明の提示で **68.2%が信用獲得・商談成立**

・対外提出専用の『セキュリティ評価実施記録』（A4・2頁/脆弱性の詳細は非記載）を納品し、取引先への説明にそのまま利用可能

② 現場の3大障壁（費用・範囲・人材）への対応

・まず公開面（20万円）から始められ、差額でログイン後評価へ広げられるパッケージ

・社内担当者や委託先の開発会社と優先順位を共有しやすいよう、成立条件と改修方針を具体的に記述



出典：IPA「2024年度 中小企業における情報セキュリティ対策に関する実態調査」（n=4,191）を基に当社作成

実施前/中/後の条件合意で
業務の継続性とデータを保護

案件ごとに独立した検証環境を立ち上げ、実施前・実施中・終了後の3段階で安全管理を徹底します。

01　実施前

対象と条件の合意

・DNSや確認ファイル等で対象システムの管理権限（所有者）を事前確認し、合意書（ROE）を締結

・検証する範囲・時間帯・禁止操作を定義し、貴社WAF等で識別できる調査専用の固定送信元IPを事前通知

02　実施中

低負荷・非破壊と停止権

・監査プロキシで通信量を秒間1〜5リクエスト以下に制限し、データの改変・削除を伴わない非破壊通信で検証

・万が一業務影響の懸念が生じた場合は、緊急停止窓口からいつでも即時に検証を中断可能

03　終了後

AI学習禁止と14日以内破棄

・通信内の個人情報は国内の検証環境内で仮名化し、外部AIのモデル学習や二次利用には一切使用しない

・検収完了から14日以内に案件専用の仮想マシン・ディスク・暗号鍵を完全破棄し、クラウド公式の削除監査ログを提出

※対象システムの所有者確認および合意書（ROE）の締結が着手の必須条件となります。

検証の深さに合わせた3つのプラン
シンプルな料金体系でお届けします

ライト｜外部公開面の侵入口評価

200,000円

税込｜1ドメイン群｜応相談

対象イメージ
公開Webサイト・公開サーバー・VPN・データ分析基盤（Metabase等）の外部露出

検証内容
ログイン不要で外部から到達できる領域に対し、攻撃者が狙う侵入口と既知悪用脆弱性の成立可否を検証

主な成果物
評価報告書（再現手順・証拠つき）、検査範囲一覧

期間の目安
着手から 2〜3営業日

スタンダード｜Webアプリ・権限評価

400,000円

税込｜1対象環境（標準構成）｜応相談

対象イメージ
ログイン機能を持つ標準的なWebサービス・業務システム

検証内容
外部公開面に加え、ログイン後の画面・APIにおける権限の飛び越えや他者データの不正閲覧まで踏み込んで検証

主な成果物
評価報告書（証拠つき）、改修方針・修正要件、検査範囲一覧、取引先提出用『セキュリティ評価実施記録』

期間の目安
着手から 約5営業日

アドバンスト｜複合シナリオ・到達評価

60万円〜

税込目安｜応相談

対象イメージ
複数権限を持つSaaS・基幹システム、または初期侵入から重要情報到達まで一気通貫で検証したい環境

検証内容
CTIに基づくシナリオ設計から、初期侵入・権限昇格・重要情報の到達までを連続して検証

主な成果物
スタンダードの全成果物 ＋ 改修後の再検証（1回）

期間の目安
着手から 約1ヶ月（個別見積もりで確定）

・**段階的な導入（14日間・差額移行）**：まずライト（20万円）で報告書の品質をご確認いただき、納品後14日以内であれば差額のみで上位プランへ移行できます。
・**開発会社・SIer様向けOEM受託**も対応しています。

※ 対象範囲・前提条件は、ご相談時に書面で確定します。

対象環境と確認したい攻撃をご相談ください
単発の実施から改善後・環境変更後の再評価まで

ご相談時に確認すること

・対象環境と、守りたい業務・重要情報

・懸念している攻撃手口や、確認したい到達目標

・実施可能な期間・操作の条件と、ご予算

対象URLや構成の概要をお知らせいただければ、無料で調査範囲の整理・お見積もりと、実物の『サンプル報告書（PDF）』をお送りします。

通常の脆弱性診断・ペネトレーションテストも、ご相談いただければ承ります。

お問い合わせ・お見積もり

contact@syzd.jp

Webサイト

https://syzd.jp

SYZD Research合同会社

法人番号 9430003019374

北海道札幌市中央区北一条西3丁目3-33