脆弱性診断サービス

2025年 v 3.5

PSC SECURITY
すべてのオンラインビジネスに安心を

01

Web脆弱性診断サービス・ネットワーク脆弱性診断サービス

５年連続年間100件以上の実績！

【Web脆弱性診断】

脆弱性診断とは

▼脆弱性診断とは

脆弱性診断とは、システムやソフトウェアに「セキュリティ上の弱点（脆弱性）」が存在しないかを検査することです。例えるなら、泥棒に狙われないように、家の鍵や窓がしっかり閉まっているか、壊れていないかを確認する作業に似ています。
どんなに注意深く設計・開発しても、設計ミスやプログラムの不備などにより、意図しない「弱点」が生じることがあります。この弱点を放置すると、攻撃者に悪用され、情報漏洩やシステム停止などの深刻な被害につながる可能性があります。

▼脆弱性を放っておくと

脆弱性を放置することは、家の窓やドアに鍵をかけずに外出するようなもので、攻撃者の侵入を許す危険があります。侵入されると、不正アクセスや情報流出、改ざん、マルウェア感染など、被害が拡大する恐れがあります。
その結果、調査・復旧費用や賠償金など、多額の経済的損失が発生するだけでなく、顧客や取引先からの信頼を失い、ブランド価値や株価の下落につながる可能性もあります。脆弱性への対応は、企業の存続に直結するリスク管理の一環であり、速やかな修正と定期的な診断が不可欠です。

【Web脆弱性診断】

ピーエスシー脆弱性診断サービスの特徴

▼シェアNo.1 信頼性のある国産ツール「Vex」を使用した自動診断

ピーエスシーのWeb脆弱性診断サービスは、診断ツール「Vex」を用いた自動診断です。
「Vex」は国内シェアナンバーワンの実績を持ち、セキュリティ専門技術者に認められるツールです。また開発元が国内であることから、日本国内での使用に対し、サポートが充実しています。

▼専門家による手動シナリオ作成

自動診断ツールではWebアプリケーションのリクエストを再現するための**診断シナリオを適切に作成することが、診断結果の精度に大きく影響**します。ピーエスシーでは診断処理を**社内専門チーム**で行うことにより、診断ノウハウを蓄積し、より正確な診断シナリオを作成します。

▼スピード・価格メリットを重視したサービスを提供

昨今のサイバーセキュリティ被害を考えると、Webサイトのセキュリティ品質は重要だが、予算・納品日程を考慮して柔軟に対応してほしい、との要望を多くの企業様から頂いています。
ピーエスシーの脆弱性診断サービスでは、その要望を実現します。

【Web脆弱性診断】

ピーエスシー脆弱性診断サービスの特徴

▼診断結果に対するサポート

ピーエスシーの脆弱性診断サービスでは、診断結果に対する質問サポートに期限を設けず対応します。報告書ご提出後１か月以上経った場合でも、報告内容の不明な点や、診断結果が検知された要因についての問合せに回答します。(※「**エクスプレスプラン**」では１か月以内の受付)

▼充実したオプションサービス

対象のWebアプリケーションがインターネットに公開されていない場合に、現地ローカルネットワークに接続して診断を行う「オンサイト診断」や、診断結果報告をオンライン会議上で行う「報告会」、診断を行った結果、検出した問題を修正した後での「再診断実施」など、様々なオプションを用意しております。
またWebアプリケーションだけでなく、ネットワーク上に接続された機器の診断を行う「ネットワーク診断」のご用意もございます。

PSC SECURITY
事前・事後の統合セキュリティ

【診断サービス実績】
1,069 社

【SOC 運用実績】
229 社・312PJ （東京・大阪合計）

【Web脆弱性診断】

4つの診断プラン＋個別問題診断

▼4プラン基本料金

スピード重視 最短2日間	手動シナリオ 再現性を重視	手動シナリオ 再現性を重視 再診断付き	WEB-API対応 再診断付き レポート充実	診断実施後の 「緊急」「高」 問題への対応に
エクスプレスプラン	ベーシックプラン	バリュープラン	アドバンスドプラン	ピンポイントプラン
~~200,000円~~	~~300,000円~~	~~400,000円~~	~~600,000円~~	100,000円～ （1問題につき）
2026/3月まで 150,000円	2026/3月まで 250,000円	2026/3月まで 350,000円	2026/3月まで 450,000円	
詳細はP9>>	詳細はP11>>	詳細はP12>>	詳細はP13>>	詳細はP15>>

Option

①オンサイト診断（+200,000円、遠距離・宿泊は別途実費。※「**エクスプレスプラン**」は対象外）
②オンライン報告会（＋50,000円 ※「**エクスプレスプラン**」は対象外）
③追加再診断（＋150,000円～ ※100URLまでの場合）
④WEBペネトレーションテスト（別途お見積りとなります）

【Web脆弱性診断】

4つの診断プラン ―こんな方にオススメ―

- 納期まで時間がない
- 念のため脆弱性を確認したい
- 社内ポリシー上、脆弱性診断実施の必要がある
- 初めてWeb脆弱性診断を実施したい

スピード重視 最短2日間

エクスプレスプラン

- 自動探査では取得できないサイトを診断したい
- 診断対象を事前に確認して、選択・追加をしたい
- 診断結果の詳細資料が欲しい

手動シナリオ 再現性を重視

ベーシックプラン

- 診断後に再診断を実施したい

手動シナリオ 再現性を重視 再診断付き

バリュープラン

- 101URL以上のサイトを診断したい
- Web-APIの診断をしたい
- SPAサイトの診断をしたい
- 他形式のレポートが必要

WEB-API対応 再診断付き レポート充実

アドバンスドプラン

- 診断後に検出した特定の問題・URLに対して個別の診断を行いたい
- 個別のパラメータを操作した診断を行いたい
- 問題が解消するまで何度も診断を行いたい

診断実施後の「緊急」「高」問題への対応に

ピンポイントプラン

【Web脆弱性診断】

4つの診断プラン比較

プラン比較	エクスプレスプラン	ベーシックプラン	バリュープラン	アドバンスドプラン	ピンポイントプラン
Webアプリケーション脆弱性検査報告書	○	○	○	○	○
診断時ログを含む診断サマリシート		○	○	○	○
診断後サポート	○(1月間)	○	○	○	○
再診断	再依頼	オプション	○	○	5回まで
101ページ以上のWEBサイト				○	ー
SPAサイトへの対応		△	△	○	○
WebAPIの診断対応				○	○
オプション報告書・チェックリスト				○	ー
報告書の英語対応				○	ー
自動診断＋手動診断による精細な診断					○

【Web脆弱性診断】

エクスプレスプラン ―スピード重視 お試しに最適―

Point① サイト自動探査・自動診断処理を続けて実施
診断処理完了後、最短２日で報告書を提出

Point② 高機能診断ツール「Vex」を使用

Point③ 診断URL数に関わらず定額(条件があります)

一般的なご対応の流れ

【Web脆弱性診断】

エクスプレスプラン診断内容について

▼診断対象

- ヒアリングシートに記載頂いたサイトの自動探査により診断対象を取得し、連続して診断処理を実施します。（取得した対象のお客様確認は行いません）
- ヒアリングシートにトップページと同じドメイン内のサブドメインを２件まで追加頂けます。（IPアドレスでの指定の場合はトップページ分のアドレスのみ）
- 自動探査にて検出する診断対象は500リンクまでとなります。
- １ページ内から検出する診断対象は100リンクまでとなります。
- トップページから検出するリンクの深さは20階層までとなります。
- 重複するページの除外、拡張子による除外、ファイル名による除外などで対象を絞ることができます。

▼診断結果報告

- 診断処理完了後、最短２日（３営業日以内）で報告書を提出します。
- 報告書の内容に対するお問い合わせは、報告書送付後１か月以内での受付となります。
- 報告会の実施については対応しておりません。
- 再診断をご希望の場合は、再度お申し込みを頂く必要がございます。

【Web脆弱性診断】

ベーシックプラン ―手動シナリオ作成 再現性を重視―

Point① 画面遷移の再現性が高い手動シナリオを作成

Point② プレスキャン後のURLリストを確認することにより診断対象の除外・追加に対応

Point③ Webアプリケーション脆弱性検査報告書以外に診断サマリシートを提出

Point④ 高機能診断ツール「Vex」を使用

Point⑤ OWASP TOP10・PCIDSS対応

一般的なご対応の流れ

ヒアリングシート記入 → プレスキャン実施 → URLリスト確認 → お見積り・お申込み → 診断実施 → 報告書送付

【Web脆弱性診断】

バリュープラン ―手動シナリオ作成 再現性を重視・再診断付き―

※ベーシックプランの対応Point(①～⑤)に加えて

Point⑥　診断後１回の再診断(初回診断報告後30日以内)

ベーシックプラン

Point①　画面遷移の再現性が高い手動シナリオを作成

Point②　プレスキャン後のURLリストを確認することにより診断対象の除外・追加に対応

Point③　Webアプリケーション脆弱性検査報告書以外に診断サマリシートを提出

Point④　高機能診断ツール「Vex」を使用

Point⑤　OWASP TOP10・PCIDSS対応

一般的なご対応の流れ

ヒアリングシート記入 → プレスキャン実施 → URLリスト確認 → お見積り・お申込み → 診断実施 → 報告書送付 → 再診断依頼 → 再診断実施 → 報告書送付

【Web脆弱性診断】

アドバンスドプラン ―再診断対応&Web-API対応―

※ベーシックプランの対応Point(①～⑤)に加えて

Point⑥ 診断後１回の再診断(初回診断報告後30日以内)

Point⑦ 101URL以上のサイト診断に対応

Point⑧ Web-API診断対応

Point⑨ 他形式でのレポート・チェックリスト

英語での報告書に対応

一般的なご対応の流れ

【Web脆弱性診断】

オプション

▼URL追加料金（診断対象が1診断100URLを超える場合）

20 URL 追加につき
¥50,000 /20 URL

- １診断につき100URLまでを基本料金とします。
- 100URLを越える場合、**20URL毎に¥50,000が加算されます。**
  （※ベーシックプラン・バリュープランは100URLを越える診断に対応していません）

▼Web-API診断対象URL（手動でHTTP(s)リクエストを作成するAPIの場合）

1 APIにつき 5 URLで計算

- 後記「診断の制限事項」の「Web-APIの診断について」を参照ください。
  （※自動診断プラン・ベーシックプラン・バリュープランはWeb-APIの診断に対応していません）
- 通常のWebページとWeb-APIとが混在する場合、後記の「脆弱性診断数の考え方について」により１診断にまとめるかを判定します

▼再診断追加料金

再診断１回追加につき
¥150,000 /100 URL

- 100URLを越える場合、**20URL毎に¥20,000が加算されます。**

【Web脆弱性診断】

ピンポイントプラン ―診断実施後の 緊急・高 問題への対応に―

※当社脆弱性診断を実施後の課題対応

※「エクスプレスプラン」の診断は対応外となります

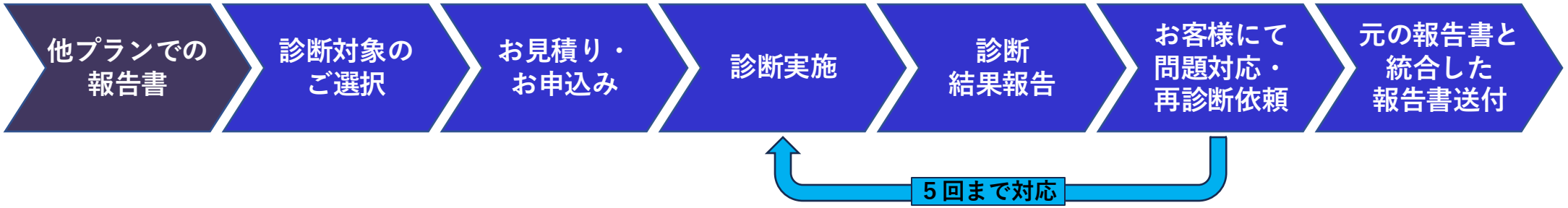
Point① 選択頂いた問題・対象URLに対する個別診断

Point② 問題への対応が完了するまで何度も再診断(5回まで)

Point③ 自動診断+手動操作による精細な診断

Point④ 問題への対応完了後に元の診断と統合した報告書を作成

一般的なご対応の流れ



【Web脆弱性診断】

ピンポイントプラン ―緊急・高 問題の例―

エクスプレスプラン以外の各プランで診断を実施した結果、下記の重要度[緊急]・[高]の問題が検出された場合に、問題と対象を限定して診断処理を実施します。

・[緊急]問題の例

リモートコード実行
安全でないデシリアライゼーション
脆弱性を含む製品の使用
LDAPインジェクション
NoSQLインジェクション
SSIインジェクション
サーバーサイドテンプレートインジェクション
XML外部実体参照
XPathインジェクション
SQLインジェクション
OSコマンドインジェクション

・[高]問題の例

不適切なアクセス制御
セキュリティ設定の不備
脆弱性を含む製品の使用
ディレクトリトラバーサル
クロスサイトリクエストフォージェリ

【Web脆弱性診断】

診断後の恒久対策ご提案例

脆弱性への攻撃を常に監視する

常に最新の脆弱性に対処する

■ 「Microsoft Defender XDR」
WEBサイトの緊急パッチ適用漏れによる
脆弱性を狙った攻撃の検知が可能。

導入 + 販売 + 保守
+
SOC運用

攻撃される前に防御する

新しい攻撃から
WEBサイトを守る

■Azure上のWEBサイト保護「Azure WAF」
■クラウド型WAF「攻撃遮断くん」
危険な通信からWEBサイトを保護。

導入 + 販売 + 保守
+
SOC運用

もし攻撃されても即時復旧する

データが盗まれる
可能性に備える

■ 改ざん検知・瞬間復旧「WebARGUS」
コンテンツ書換えや危険な実行ファイルを
サーバーに置かれても1秒以内に元の状態に。

導入 + 販売 + 保守
+
SOC運用

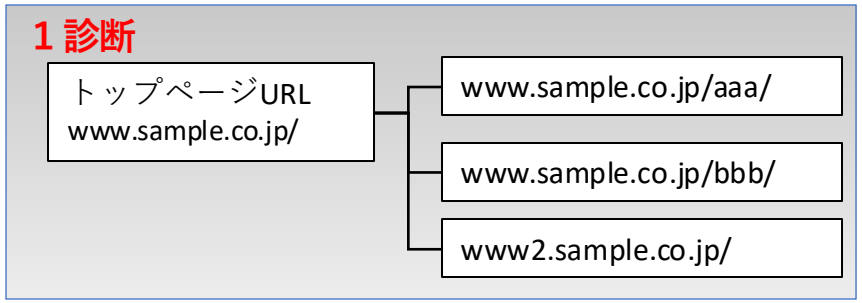
※SOCの詳細は、P30以降をご参照ください

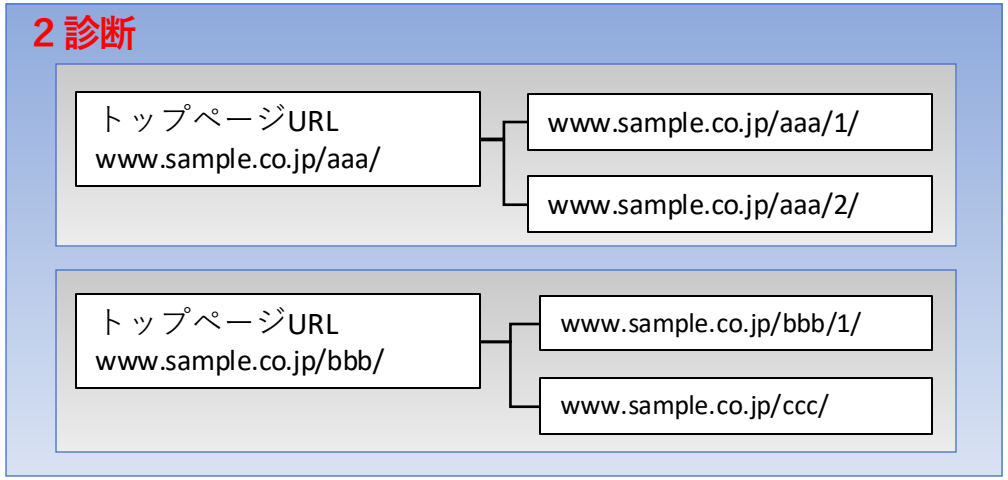
【Web脆弱性診断】

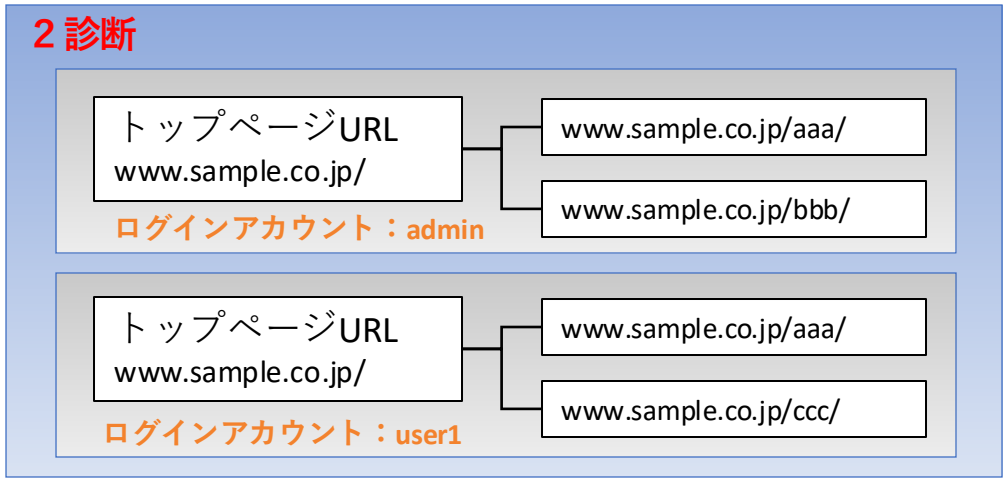
脆弱性診断数の考え方について（１）

▼１診断の範囲

・１診断は指定のトップページURLから、ページ内リンクにより到達できるサイト内の診断を１診断とします。複数のドメインに渡るサイトの場合、ヒアリングシートで指定されたドメイン内の範囲となります。
・ログインが必要なサイトは、１ユーザーアカウントでのログインで到達できるサイト内とします。同一サイトであっても、ログインユーザーアカウントが別になるものは、別の診断となります。
・１診断につき、１通の報告書となります。お客様の指定により報告書を分けて作成する場合、作成する報告書の数の診断数となります。





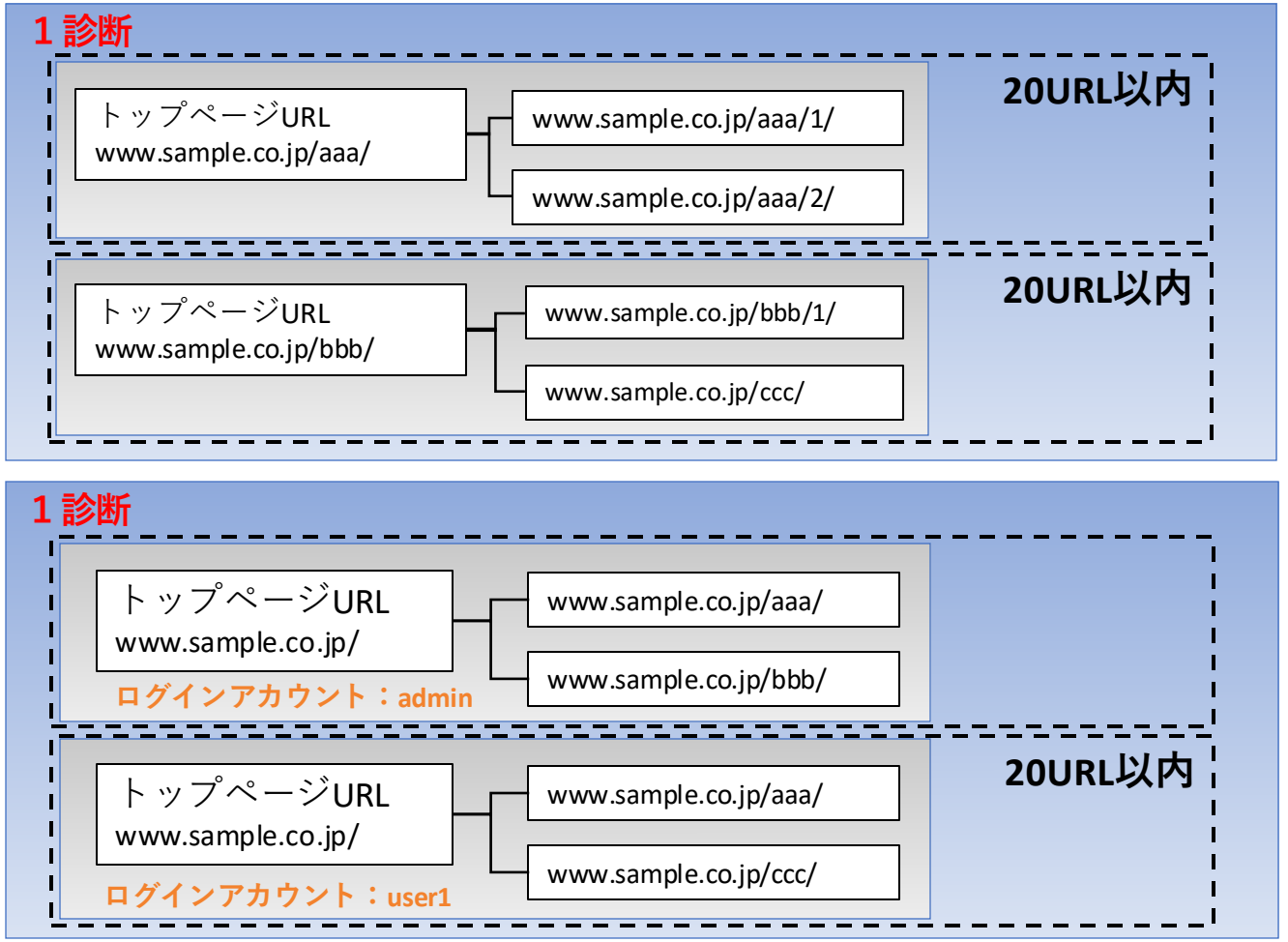


【Web脆弱性診断】

脆弱性診断数の考え方について（２）

▼診断の範囲の例外

・トップページが分かれているサイトで、それぞれのサイトのプレスキャン結果が20URL以内の場合は、まとめて１診断とすることができます。３サイト以上の場合や、20URLを越えるサイトはまとめの対象とはなりません。
・ログインが必要なサイトで、ユーザーアカウントでのプレスキャン結果が20URL以内の場合は、他のユーザーアカウントの診断とまとめて１診断とすることができます。
・まとめて１診断とした場合、報告書もまとめて１通となります。報告書を分ける場合は、それぞれ個別の診断となります。



【Web脆弱性診断】

診断の制限事項

▼診断が行えないサイト・URLについて

- 多要素認証には対応しておりません。診断をご希望の場合、パスワード認証での代替などの回避方法をご用意ください。
- ページの遷移にWebsocketなどのhttp(s)以外の通信が必要となるページは診断できません。
- 外部ドメインの認証によるシングルサインオンのサイトでは、リクエストに必要なパラメーターが再現できないため、診断することができない場合があります。
- IPS/WAF等により通信がブロックされるサイトは、診断時に除外設定を行うなど、通信のブロックがされないように設定してください。診断処理が失敗する場合があります。
- 同じパラメーターでのリクエストが１回しか正常に行えないURLは診断することができません。（登録済みのデータを削除するリクエスト・フォームの入力にユニーク値(電話番号・メールアドレス等)を必須とするリクエスト・等）

▼Web-APIの診断について

- 診断対象となるWeb-APIはプレスキャン時に取得したリクエストを再現して正常応答(レスポンスコード200)が取得できるものとなります。
- プレスキャンの際に、**ページ内の操作によりリクエスト・レスポンスが取得**できて、取得したリクエストを再現して正常応答(レスポンスコード200)が取得できるWeb-APIは、１リクエスト１URLとして、通常のWebページと同様の診断となります。
- Webアプリケーションより実行されるWeb-APIで、診断を行うには**手動でリクエストの設定を行う必要があるWeb-API**は**１リクエストに付き５URL相当**としてお見積もりを算出致します。
- Web-APIのリクエストに必要なパラメーターとして、スクリプトの実行結果が必要となるリクエストは診断対象とすることができません。

【Web脆弱性診断】

診断ツール：Vex　国内シェアNo.1のWebアプリケーション脆弱性検査ツール

Vex（Vulnerability Explorer）とは？

優れた脆弱性検出率を有する、純国産のWebアプリケーション脆弱性検査ツールです。DAST(Dynamic Application Security Testing)と呼ばれる手法を採用してWebサーバの外部から疑似攻撃リクエストを送信し、レスポンスを解析して脆弱性の有無を確認するため、現実的に起こり得る脅威を効率的に見つけ出すことが可能です。

経済産業省：情報セキュリティサービス基準「情報セキュリティサービスにおける技術及び品質確保に資する取組の例示」にてWebアプリケーション脆弱性診断の基準ツールにも選定

Point

①強力なシナリオ作成支援
- 自動と手動設定を組み合わせた**シナリオマップ機能**
- パラメータを手動で設定する**Handler機能**
- **自動巡回**によるシナリオ作成

②豊富な脆弱性検査項目（次ページにて説明）

③最新の脆弱性への対応や定期的な新機能の追加
- **約３ヵ月に１度の定期的な追加/更新**
- **危険度の高い新しい脆弱性には数日以内に緊急リリース**

④充実のレポート機能（次々ページにて説明）

【Web脆弱性診断】

脆弱性診断項目

Vexでは、以下のカテゴリに分類される診断シグネチャによる診断を実施します。
ベンダー推奨の、検出頻度の高い代表的な検査パターンや、利用頻度の高い製品に起因する
脆弱性を検出するシグネチャを含んだシグネチャセットを採用しております。。

SQLインジェクション
OSコマンドインジェクション
リモートコード実行
オープンリダイレクト
HTTPヘッダインジェクション
SSIインジェクション
XPathインジェクション
LDAPインジェクション
XML外部実体参照
安全でないデシリアライゼーション
ディレクトリトラバーサル
クロスサイトスクリプティング
クロスサイトリクエストフォージェリ
平文通信
セッションフィクセーション
セッション管理不備
過度な情報漏えい
不適切なエラー処理
サービス運用妨害
セキュリティ設定の不備
脆弱性を含む製品の使用
不適切なアクセス制御
NoSQLインジェクション
サーバサイドリクエストフォージェリ

【Web脆弱性診断】

目的や利用者に合わせたレポート・チェックリスト

①Web脆弱性診断報告書

検査結果概要：Webアプリケーションのセキュリティ強度を５段階で評価します。
検査結果サマリ：脆弱性別・検査対象リクエスト別の検出結果の一覧です。
脆弱性別検出結果詳細：検出された脆弱性毎の結果が出力されます。
検査対象リクエスト別検出結果詳細：検査対象リクエスト毎の結果が出力されます。
検査対象ホスト別検出結果詳細：サイト全体に対する脆弱性検出結果がホスト別に出力されます。
検出された脆弱性の詳細：脆弱性の概要、改修方法、想定される被害等が出力されます。

②Web脆弱性診断サマリ （次ページ参照）

検査結果の診断サマリ(Excel形式一覧・操作内容・脆弱性詳細)をZipファイルにて提供します。

③検査対象情報／テスト結果チェックリスト （「アドバンスドプラン」で対応）

要望に応じて検査対象としてチェックされたメッセージ情報と、検査実施結果のリストを提供します。

④その他のレポート・チェックリスト （「アドバンスドプラン」で対応）

要望に応じて「安全なウェブサイトの作り方」チェックリスト・「ASVS:アプリケーションセキュリティ検証標準」チェックリスト・OWASP TOP10レポート・PCIDSSレポートを提供します。

【Web脆弱性診断】

Web脆弱性診断サマリ

診断完了後、検出した脆弱性とその内容をまとめたファイルを送付します。
診断の途中でもご要望があれば中間結果を送付いたします。

No.	ID	危険度	カテゴリ	シグネチャID	脆弱性の概要	機能名	URL	パラメータ名
1	350-54-G110	低	クロスサイトスクリプティング	015481_NoCharsetOptionInTheContentTypeHeaderField-header_check	Content-Typeヘッダに対するcharsetパラメータの不備	BadStore.net - Redirect to Home Page	http://10.0.0.7:8528/	-
2	350-54-G202	低	セキュリティ設定の不備	205626_Clickjacking-checker	クリックジャッキング攻撃への対策不備	BadStore.net - Redirect to Home Page	http://10.0.0.7:8528/	-
3	350-57-G440	低	クロスサイトスクリプティング	015481_NoCharsetOptionInTheContentTypeHeaderField-header_check	Content-Typeヘッダに対するcharsetパラメータの不備	BadStore.net	http://10.0.0.7:8528/cgi-bin/badstore.cgi	-
4	350-57-G528	低	不適切なエラー処理	205691_NullCharacterReplaceAllParams-checker	全てのパラメータに対するNull文字を利用したエラーメッセージの出力	BadStore.net	http://10.0.0.7:8528/cgi-bin/badstore.cgi	-

【ネットワーク脆弱性診断】

ネットワーク脆弱性診断

ネットワーク診断とは？

ネットワーク脆弱性診断ツール「Nessus」により、サーバーやネットワーク機器など、IPアドレスを持つ機器のセキュリティ脆弱性を診断します。

Nessusとは？

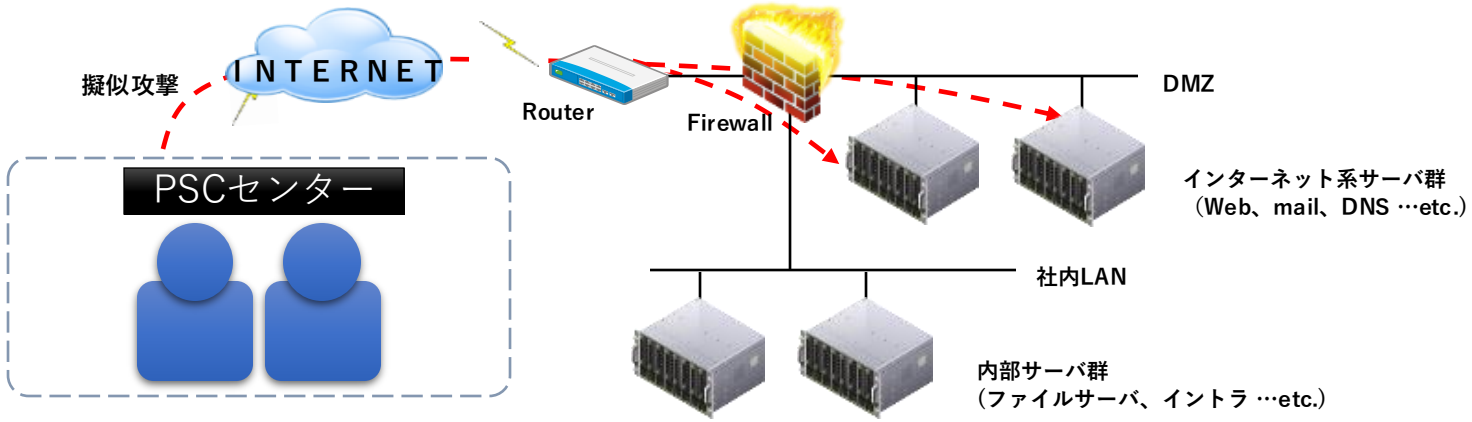
ネットワーク内のサーバー、デバイス、アプリケーションなど、広範囲なシステムに対する脆弱性を検出する脆弱性検査ツールです。世界中で多くの組織に利用され、信頼されている脆弱性評価のデファクトスタンダードです。

経済産業省：情報セキュリティサービス基準「情報セキュリティサービスにおける技術及び品質確保に資する取組の例示」にてプラットフォーム脆弱性診断の基準ツールにも選定

Point

ツールを使った自動診断+専門家による分析

①迅速な結果報告
②低価格で利用
③高い信頼性



【ネットワーク脆弱性診断】

ネットワーク脆弱性診断 ―検査項目例―

最も標準的な検査項目は「各アプリケーションの設定」「パッチ適用状況の確認」、
またインターネットからの「疑似攻撃テスト」を行います。

▼アプリケーションの脆弱性チェック

各種主要 OS、アプリケーション、アプライアンス製品等に関する脆弱性検査	
診断項目	パッチ適用状況チェック
	既知の脆弱性攻撃試行チェック
	不適切な設定のチェック (不必要な共有設定、デフォルト設定のままの問題点など)
	アカウントチェック (脆弱な状態にあるビルトインアカウントの存在など)

▼攻撃パターンの試行

その他攻撃パターンの試行	
診断項目	ポートスキャン (TCP ポート、UDP ポートは Wellknown ポート対象)
	サービス検知
	バックドア攻撃
	リモートシェル攻撃（遠隔操作試行攻撃）
	※DoS 攻撃 (実機に対する影響があるため、対象外としています)

【ネットワーク脆弱性診断】

ネットワーク脆弱性診断 ―ご利用料金―

サーバー・ネットワークの脆弱性を短時間で診断

基本料金

~~400,000円~~

2026/3月まで
350,000円

不要サービスポートの有無、サーバーの脆弱性に関する診断結果をレポートします。
更に、WEBアプリケーション診断と組み合わせることでより深いリスクチェックが可能になります。

Option

① オンサイト診断（+200,000円～、遠距離・宿泊は別途実費）
② オンライン報告会（+50,000円）
③ 定期診断プラン（月額制）※ご相談下さい

※10 IPアドレスまでの料金となります。
リモート診断で10 IPを越える場合、2 IPごとに 50,000円追加となります。
※オンサイト診断にてプライベートIPアドレスが対象の場合、10 IPを越える場合には
100 IP 80万円 または クラスC 1 セグメント当たり 150万円（最大254IP）にて対応します。

▼ペネトレーションテスト

ターゲットにつき　¥3,500,000～

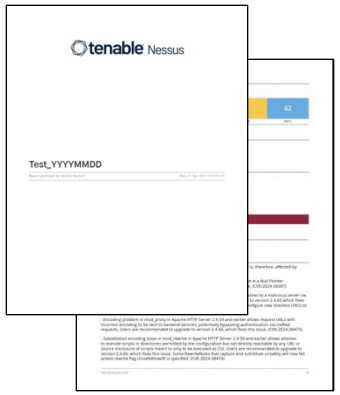
※ご相談下さい。

【ネットワーク脆弱性診断】

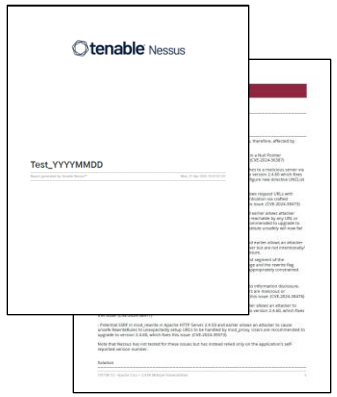
ネットワーク脆弱性診断 ―報告書・速報レポート内容―

報告書では「脅威度判定」「詳細情報」「診断情報」「結果サマリ」「検出ホスト」をご報告します。脅威度判定にて危険度の高い脆弱性が見つかった場合は、内容の詳細のご報告に加え推奨する「解決策」もご提案いたします。

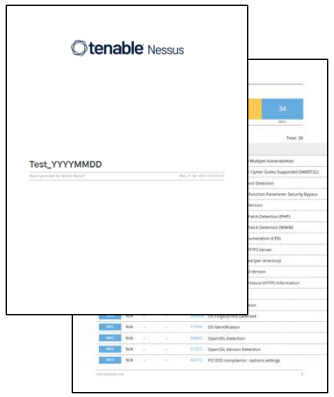
速報レポートは「ホスト別結果」「プラグイン詳細」「結果サマリ」の３つのレポートを作成します。
脆弱性診断ツール「Nessus」から出力したレポートを検査実施の翌営業日までにご提出いたします。



【ホスト別結果】



【プラグイン詳細】



【結果サマリ】

▼脅威度判定例

※報告書サンプルより抜粋

重大度	概要	検出数
緊急	即座に対策が必要で、特に致命的な脆弱性。	1
高	即座に対策が必要な脆弱性。	1
中	対策の検討が必要な脆弱性。	1
低	現時点でのリスクは低いが、今後を見越して対策の検討が必要なもの。	1
情報	脆弱性ではないが、診断実施の情報提示など。	42

▼詳細情報例

SSL Medium Strength Cipher Suites Supported (SWEET32)

NessusPlugin ID	42873	CVE 共通番号	CVE-2016-2183
プロトコル	TCP	サービスポート	443
名称	中程度の強度の SSL 暗号化パッケージがサポートされています (SWEET32)		
概要	リモートサービスは、中程度の強度の SSL 暗号化をサポートします。		
説明	リモートホストは、中程度の強度の暗号化を提供する SSL 暗号の使用をサポートします。Nessus では、64 ビット以上 112 ビット未満の鍵長を使用する暗号化、または 3DES 暗号化スイートを使用する暗号化を中程度の強度とみなしています。 注: 攻撃者が同じ物理ネットワークにいる場合、かなり簡単に中程度の強度の暗号化を回避できるようになります。		
問題解決方法	可能であれば、影響を受けているアプリケーションの構成を変更し、中程度の強度の暗号の使用を避けてください。		
PSC コメントなど	ご使用されている暗号化パッケージは中程度の強度の暗号化をサポートしており、SWEET32 として知られる脆弱性による影響を受けます。構成を変更し、64 ビットブロック暗号は使用を避けて下さい。		

※参考：CVSS v3スコア

CVSSスコアとは、脆弱性の深刻度を理解するための指標です。
スコアが高いほど、脆弱性の潜在的な影響が大きいことを示し、迅速な対応が求められます。
逆に、スコアが低い場合は、脆弱性の影響が限定的であることを示します。

緊急：**9.0～10.0**
[例]SQLインジェクション、OSコマンドインジェクション

高：**7.0～8.9**
[例]ディレクトリトラバーサル、リモートファイルインクルード

中：**4.0～6.9**
[例]CSRF、XSS

低：**0.1～3.9**
[例]セッション管理不備、不適切なエラー処理

情報：**0.0**
[例]オートコンプリート機能が有効な重要情報入力フォーム

02

PSC SECURITYサービス

SOC（セキュリティオペレーションセンター）

オペレーションチーム

■役割

•24時間365日セキュリティ監視、運用

•ログアラート検出時15分以内に連絡

■業務

•ログ監視

•Firewall運用サービス

•死活監視サービス

•脆弱性診断自動スキャンサービス

•セキュリティパッチ定期通知サービス

•改ざん検知運用サービス

•障害切り分け

ＳＥ/アナリストチーム

■役割

•お客様毎にコンサルティング、SI、分析/報告を対応

•Security Management Centerの品質向上、体制強化

•Webサイトセキュリティ強化コンサルティング

■業務

•ログ分析

•Web/NW脆弱性診断レポート

•セキュリティ機器導入

•顧客別サポート(日次/月次)

•障害対応

セキュリティサービス体制

経験豊富な技術者と蓄積されたナレッジ

ネット環境に潜むあらゆる危険を防御

SOC提供サービス

PSC マネージドセキュリティサービス

SOC セキュリティオペレーションセンター業務

検知 → 切り分け → 報告 → 遮断・隔離

- 切り分け：・重要度判定 ・過検知/誤検知の切り分け
- 報告：・一次報告
- 遮断・隔離：・端末隔離 ・ユーザ利用停止依頼

PSCインシデントレスポンスサービス

情報システム部門業務

経路調査 → 影響調査 → 最終報告

- 経路調査：・情報漏洩確認

PSC セキュリティコンサルティング

アフターフォロー業務

情報システム暫定対処 → 恒久対処

- 情報システム暫定対処：・マルウェア抽出、調査 ・重要データ復旧 ・端末リプレース ・ユーザーアカウント再発行
- 恒久対処：・社内ルールの見直し ・セキュリティポリシーの更新、改訂 ・全社通知 ・セキュリティ教育

緊急度に応じて、一次報告・二次報告を実施し、推奨対応方法を連絡します。

危険度の把握から対応策の実施までに要する時間を最小限にすることで、被害の最小化をトータルでサポートします。

沿革

～2013
・Web脆弱性診断

2014
・ネットワークセキュリティ
・IBM/MSS（不正侵入検知）
・ファイヤーウォールログ分析

2015
・改ざん検知/防御
・WAF運用サービス
・サンドボックス（FireEye）

2016
・ログ統合＆相関分析サービス
・TrendMicro/F5Networks MSP

2017
・セキュリティ対策チーム支援サービス（オンサイト）
・クラウドセキュリティサービス

2018
・エンドポイントセキュリティ
・AWS WAF
・NDR

2019
・データベースセキュリティ

2020
・Microsoft Sentinel
・Microsoft Defender for Endpoint

2021
・Microsoft E5 Security

2022
・西日本SOC開設「西日本SMC」開設

2023
・アセスメントサービス
・グローバルSOC

プロから頼られる技術力
PSCのセキュリティソリューション

対応拠点

東京と大阪に拠点を置き、東西でサービスを提供できる体制をとっています。
また、PSC琉球（PSC子会社）が沖縄でDR 拠点として、万一の際のお客様窓口となります。

セキュリティサービス@東京

- コンサルティング
- SOC業務
- 分析、調査

セキュリティサービス@大阪

- ユーザサポート
- SOC業務
- 分析、調査

ピーエスシー琉球

- お客様窓口

設備

セキュリティ監視ルーム

- 24 時間 365 日運用を行う監視ルーム
- カード認証、指紋認証等マルチ認証が必要な入館作業
- 金融機関にフォーカスした世界水準の設備
- 冗長化された電源、空調
- 3段階のセンサー、充実の消火設備
- 人口用水路による洪水対策
- 震度6弱に耐えうる、堅牢な建物構造
- 高速な光ファイバーネットワークに直結した快適なブロードバンド環境
- 大手町から15分以内の好立地

認証登録・資格

- プライバシーマーク
- 品質マネージメントシステム認証
- 情報セキュリティマネージメントシステム認証
- 日本カード情報セキュリティ協議会 会員
- 日本セキュリティ監査協会 セキュリティ監視運用サービス部門認定
- ＳＳＳマーク（サービス登録番号：019-0019-40）

10820219(06)

登録番号：019-0019-40

日本カード情報セキュリティ協議会
安全なカード社会の実現を目指して

設備（西日本）

セキュリティ監視ルーム（西日本）

- 24 時間 365 日運用を行う監視ルーム
- エントランスフラッパーゲート、セキュリティゾーン毎のICカード認証等 複数の認証が必要な入館作業
- 24時間365日の有人警備
- 冗長化された電源、空調
- 「官庁施設の総合耐震基準」「建築構造設計基準」Ⅰ類を満たす地震対策
- 大規模水害時の想定浸水高をカバーする水防設備
- 燃料無補給で48時間以上連続稼働可能な非常用発電設備
- 大阪駅から15分以内の好立地

セキュリティサービスの東西連携

サービス詳細

PSC SECURITY

【診断サービス実績】

1,069社

【SOC運用実績】

229社・312PJ　（東京・大阪合計）