インフラ脆弱性診断サービス

インフラ脆弱性診断サービスは、ITシステムのサーバやネットワーク機器のOSおよびミドルウェアの脆弱性の検出を行うサービスです。診断は、リモート／オンサイトのいずれかの診断方法で実施します

■ 診断種別

リモート

- 弊社の診断用ネットワークからインターネット越しに診断を行います。
- 外部からの調査行為や侵入に対してファイアウォール等のセキュリティ機能が有効に機能しているかを評価する場合には、リモートでの診断が適しています。

オンサイト

- お客様のデーターセンターや事業場へ診断員が訪問し、お客様のネットワーク内部から診断を行います。
- 対象のシステムに脆弱性が潜在していないかを評価する場合には、オンサイトでの診断が適しています。

リモート／オンサイトいずれの場合も診断項目は変わりません。

■ 診断項目

診断項目	診断内容
オープンポート調査	すべてのIPに対してTCP/0-65535、UDP/0-65535、ICMPに対するポート待受状態を調査します。
バナー情報調査	待受状態のポートと通信を確立、または通信エラーを発生させることで稼働中のOSやミドルウェアの種類やバージョン等の情報を取得できるか調査します。
OS脆弱性調査	脆弱性が解消されていないOSおよびパッチ適用状況を調査するまた、脆弱性があるサービスやプログラムの稼働についても調査します。
主要ミドルウェア脆弱性調査	脆弱性が解消されていない主要なミドルウェア（HTTPサービス、SMTPサービス、DBサービス、DNSサービスなど）について調査します。
脆弱なアカウントの調査	デフォルトアカウントや脆弱なパスワード設定のOSアカウントが存在しないか調査します。
危殆化した暗号利用の調査	SSL/TSL通信に脆弱な暗号化方式が利用可能な状態にないか調査します。
その他脆弱性の調査	その他、DDoS攻撃の影響を大きく受ける状況にないか、脆弱性を誘発する設定不備の可能性などについて調査します。

診断の結果、脆弱性が検出できたかどうかを書面によりご報告します。

■ 診断内容

項目	備考
対象機器・システム名称	
IPアドレス	
発見した脆弱性の種類	CVEが付番されている場合はCVE番号を記載
脆弱性の深刻度	CVSS表記できる場合はCVSS値を記載
脆弱性を悪用された場合のリスク	
対処方法および緩和策	

深刻度が極めて高い脆弱性を発見した場合は、すべての診断作業の終了を待たずに、速報として概要をメールで報告します。

■ 診断項目

診断項目	診断内容
対象機器・システム名称	
（マスクしたIPアドレス）	「対象機器・システム名称」で対象が特定できない場合は、情報をマスクしたIPアドレスでお伝えします。
発見した脆弱性の種類	CVEが付番されている場合はCVE番号を記載
脆弱性の深刻度	CVSS表記できる場合はCVSS値を記載
対処方法および緩和策	早期に通知することを優先するため、不明の場合は「調査中」と記載

■ 診断実施の流れ

1. 受付

- お客様からのお問い合わせを受け、診断実施内容および診断実施の希望時期を確認いたします。

2. 見積

- 受付から3営業日以内に診断実施の可否と見積を提示いたします。

※ 要員がアサインできない等により実施できない場合があります

3. 契約

- 正式なお申し込みを頂いた後、契約手続きをさせていただきます。

4. 事前準備

- 診断ツールの最新化や診断場所の手配などの事前準備に3～5営業日のお時間をいただきます。

5. 診断実施

- お客様と合意した日程・時間帯で診断作業を実施します。

※ 実施期間は、対象とするサイトの規模により変動します

6. 報告

- 診断結果を報告書にまとめてご報告します。

◆ 注意事項

インフラ脆弱性診断サービスは、診断作業時点における既知の脆弱性を調査するサービスです。診断結果で脆弱性が見つからなかった場合でも脆弱性が無いことを保証するものでは有りません。

製品・サービスについてのお問い合わせは

株式会社ＦＦＲＩセキュリティ
〒100-0005
東京都千代田区丸の内3-3-1　新東京ビル2階
TEL：03-6277-1811　E-mail：sales@ffri.jp

本製品に関する情報はインターネットでもご覧いただけます。
https://www.ffri.jp/

2021年12月現在　Ver 1.00.00