FireClover 脆弱性診断サービス

サービス仕様書

Ver1.0 2025年01月21日

日鉄日立システムソリューションズ株式会社

改訂履歴

版数	改訂日付	改訂内容及び理由
Ver 1.0	2025年01月21日	

目次

1. はじめに

1.1. 本書の位置づけ

このFireClover 脆弱性診断サービス サービス仕様書（以下「本書」といいます。）は、弊社が提供する FireClover 脆弱性診断サービス（以下「診断サービス」といいます。）のサービス内容について記述したものです。

2. 提供サービス概要

2.1. 診断サービス

診断サービスは、弊社のセキュリティエンジニアが診断ツールを使用して脆弱性診断等を行い、コンピュータ、サーバやネットワーク機器のセキュリティを評価し、潜在的な脆弱性の調査と分析します。そのうえで、診断結果報告書を成果物として納入することを目的としています。

2.1.1. サービスの流れ

サービスの流れは次のとおりです。

①ヒアリング
②脆弱性診断　（IP 数上限まで）
③診断結果報告

サービスの詳細については後述する「3.1 サービスの流れ」を参照ください。

2.1.2. オプションサービス

オプション契約に応じ、次のオプションサービスを提供します。

・脆弱性診断　（IP 数上限以上）

オプションサービスの詳細は「3.2 オプションサービス内容」を参照ください。

2.2. サービス提供条件

2.2.1. サービス提供地域

日本国内のみを対象とします。

2.2.2. 言語

日本語でのみ実施します。

3. 診断サービス内容

3.1.　サービスの流れ

3.1.1. 事前準備・ヒアリング

診断実施に先立ち、弊社指定の診断対象一覧シートを提供します。以下必要事項を記入の後、指定の日時までに返信してください。 診断対象数は原則 100IP を上限とします。

・診断対象ネットワーク機器の IP アドレス 、ホスト名、役割、OS、設置場所

※入館申請、持込み PC 申請等、診断に向けた注意事項も診断対象一覧シートと合わせて連絡してください。

※お客様から返信されたヒアリングシートは、弊社の作業責任者が内容を確認の後、記入いただいた内容についてご連絡差し上げます。

本診断サービスでは、より高レベルな診断を実現するために、管理者ユーザを利用することを推奨しています。利用する場合は、診断機器にリモートログイン可能な管理者ユーザをご用意ください。弊社診断機器設置時にお客様にてご入力いただき、弊社はこの情報を関知しません。

※管理者ユーザとは、一般的に Windows の場合はドメインやローカルの Administrator ユーザ、Linux の場合は root ユーザを指します。

※設定した管理者情報でログイン出来ない機器に関しては取得出来る情報に限りがあります。

3.1.2. 脆弱性診断

事前調整の内容に基づき、診断対象に対して脆弱性診断を実施します。

診断作業は機器持ち込みの上、お客様ネットワークに接続して実施します。

※診断対象に対して、診断ツールが接続できることを条件とします。

※診断は原則、弊社営業日の 9:00～17:30 での対応とします。施設又は設備利用の都合上、弊社営業時間外又は営業日以外で診断の実施が必要となる場合は、個別にご相談ください。

3.1.3. 診断項目

主な診断項目は下記の通りとなります。 診断ツールは Rapid7 社 Nexpose を利用します。

サーバへの疎通確認
デフォルトポートのスキャン
OS の識別
パッチ/ホットフィックスのチェック
アプリケーション層の監査
ネットワークベースの脆弱性
その他、既知の脆弱性

3.1.4. 診断基準

診断ツールの評価を元に、検出した脆弱性の深刻度を判定します。検出した深刻度の判定は、CVSS ベーススコアを参考に以下 3 段階に区分します。

高	CVSS ベーススコア 7.5 ～ 10.0
中	CVSS ベーススコア 3.5 ～ 7.4
低	CVSS ベーススコア 0.0 ～ 3.4

3.1.5.診断結果報告書の提出

診断結果報告書は日本語で作成し、PowerPoint 形式にて提供します。

診断結果報告書には、脆弱性数の多い機器、脆弱性の傾向や、特にリスクの高い脆弱性を抜粋し、脆弱性を悪用された場合の影響や対策提言などを記載します。

※弊社の作業責任者から、お客様に対し、対面又はリモート会議ツールを用いて、診断結果報告書についてご説明（想定される脅威、悪用された場合の影響、その他質疑応答）させていただきます。なお、ご説明は日本語で弊社営業日の 9:00-17:30 に実施させていただきます。

3.1.6.QA 対応

診断結果報告書の納品後 1 ヶ月以内に生じたご質問については、「5. お問い合わせ対応」記載の連絡先までご連絡ください。

※上記連絡先において承ることができるご質問の内容は、診断結果報告書の見方、記載内容の確認等の簡便なものに限ります。

※別途作業が必要となる場合（追加診断の実施、脆弱性対策の実施等）は、別途お見積もりが必要となりますので予めご了承ください。

3.2.　オプションサービス内容

3.2.1.IP 上限以上の対応

診断対象数は原則、100IP を上限とします。上限を超える診断対象数についてはオプションサービスとして個別に対応します。

※診断対象数が上限を大幅に超える場合、複数回に分けたお申込として承ります。

4. ご注意事項

4.1. 作業前

本項に記載する注意事項について、ヒアリングシート記入前に必ず確認ください。不明な点がありましたら、弊社の担当エンジニアへ問い合わせください。

診断対象がクラウドサービスやホスティングサービスを利用している場合は、サービス事業者への確認と、必要に応じた事前連絡を、お客様自身で行ってください。一部のサービス事業者では、 脆弱性診断を実施する際の事前連絡と許可が必要な場合があります。

リモート診断において、診断対象として指定いただいた IP アドレスに対し、弊社診断元 IP アドレスからの通信許可を事前に設定してください。

診断作業時には対象ホストの状態を確認いただくため、診断当日は、ご担当者様に連絡が取れるようお願いします。オンサイト診断作業時には、ご担当者様に立ち合いをお願いします。

オンサイト診断の場合、事前に「弊社持ち込み機器に付与する IP アドレス」「弊社持ち込み機器設置場所」 「御社診断対象機器と弊社持ち込み機器が疎通可能な御社ネットワーク機器の空ポート」「診断対象機器の管理者ユーザとパスワード」「入館手続き」「PC 持込み手続き」を準備していただく必要があります。作業当日までに準備が不足していた場合、診断作業を延期することがあります。

運用環境において、侵入検知システム（IPS/IDS）や、その他監視装置が設置されている場合、脆弱性診断実施中当該システムから大量のアラートメールが運用・保守業者様に配信されることがあります。監視を行っている場合は、事前に監視対象から外す、除外対象として設定する等の対応を行ってください。

必要に応じて診断対象のデータベースやシステムの設定情報のバックアップを取得してください。万が一システムに不具合が生じた場合、事前に取得したデータベースのバックアップをリストアする等の対応を実施してください。

4.2. 作業中

診断対象からのレスポンスが遅いなど状況によっては、診断作業を延期することがあります。

診断時間帯、継続的に疑似攻撃を含んだ多くの通信が発生するため、診断対象システムの CPU 使用率の上昇やネットワークトラフィックが大きくなることにより、サーバにアクセスできなくなることや、サーバからのレスポンスに時間がかかることがあります。

診断作業には、サービス不能(DoS)攻撃に関する項目は含まれていませんが、多数のリクエストを同時に送信することで、一時的にサービス不能となる状態が発生する可能性があります。

診断対象の動作や診断作業の遅延など、影響が発生した場合は弊社診断機器の LAN ケーブルを抜き、弊社の担当エンジニアまでご連絡ください。

4.3. その他

診断サービスは、対象に潜むすべての脆弱性を発見することを保証するものではありません。

脆弱性診断結果の報告は、助言型の報告であり、診断対象が安全である旨を伝達するものではありません。

新しい脆弱性や攻撃手法の発見、セキュリティの動向に伴い、指摘項目や脆弱性の検出方法や判定方法を定期的に見直しているため、継続的な診断を実施した場合に診断結果に差異が生じる場合があることをご承知おきください。

5. お問い合わせ対応

対応方法	原則電子メールにて対応
対応内容	診断結果報告書に関するご質問 ※お客様の仕様に関わる内容および報告書記載以上の対策方法詳細についてはお答えしかねます。
対応窓口	fireclover-support@nhs.co.jp
対応時間	メール受付は 24 時間 365 日。弊社からの電子メールの返信は、弊社営業日の 9:00-17:30。
対応言語	日本語

※ FireClover は日鉄日立システムソリューションズの登録商標です。
※ Nexpose、Metasploit は、Rapid7 LLC の米国及びその他の国における商標または登録商標です。
※ その他本書記載の会社名・製品名は、各社の商標または登録商標です。