# CSS MDRサービス
# SCS評価制度への対応機能

2026年10月
エヌアイシー・パートナーズ株式会社

# 目次


- 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（SCS評価制度）とは
- 本資料の目的
- 本資料の内容
- 本文の凡例
- 本文


Copyright © 2026 NIC PARTNERS Inc.

# 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（SCS評価制度）とは

- 経済産業省が検討を進め、IPA（情報処理推進機構）が制度運用を支援する、取引先を含めたサプライチェーン全体のサイバーセキュリティ対策を可視化するための制度です。

- 企業の対策状況を、事業規模や取り扱う情報・業務の重要度に応じて段階的に評価します。
  基本対策を評価する「★3（専門家確認付きの自己評価）」や、より厳格な「★4（第三者による評価）」などの評価水準を整備し、企業のセキュリティ水準を可視化します。

- 2026年度上期に評価用ガイド等、下期に評価機関等を公表し、2026年度末（2027年3月頃）の運用開始を目指しています。

  ○ https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html

Copyright © 2026 NIC PARTNERS Inc.

# 本資料の目的

- SCS評価制度への対応は、取引先からの要請に応えることや、評価結果の取得・提示を目的とするだけのものではありません。
- 本制度は、サプライチェーンを通じたサイバー攻撃のリスクを低減するため、企業の規模や役割、扱う情報・システムの重要性などに応じて求められるセキュリティ対策の考え方・水準を示し、各企業が自社の課題を把握して必要な防護体制を整備・強化することを促すものです。
- 制度が示す指針に基づき、自社の対策状況を適切に把握・改善するとともに、その状況を取引先と共有・可視化することで、サプライチェーン全体を含めた実効性のある安全対策につなげることが重要です。これが、本制度に対応する本質的な目的といえます。

**本資料は、その中で「CSS MDRサービスが『どの評価基準No.に対し、どのような対応ができるか」を整理したものです。**

**一朝一夕にすべてのSCS評価項目を満たすことはできません。しかし「今、セキュリティを守る対応ができていないところ」に、サービスを利用して即座に対応することは可能です。まずそこから始めましょう。**

Copyright © 2026 NIC PARTNERS Inc.

# 本資料の内容

- **左部分**
  - ○ CSS MDRサービスで提供している「機能名」「機能内容」を記載

- **右部分**
  - ○ そのCSS MDRサービスの機能を用いて対応できる評価基準Noとその内容を記載
  - ○ その下に、CSS MDRサービスでの「対応内容」を記載
  - ○ 「要求への充足提供」
    各評価基準No.で要求されている内容を**充足して提供**できる
  - ○ 「要求に対応するための情報提供」
    各評価基準No.で要求されている内容に**対応するための情報提供**ができる

Copyright © 2026 NIC PARTNERS Inc.

# 本文の凡例

## CSS MDR で提供している機能名

CSS MDRサービスでの機能

## 対応する評価基準No

### 要求への充足提供

「各評価基準No.で要求されていることを充足して提供できる」

評価基準No.

CSS MDRでの対応内容

### 要求に対応するための情報提供

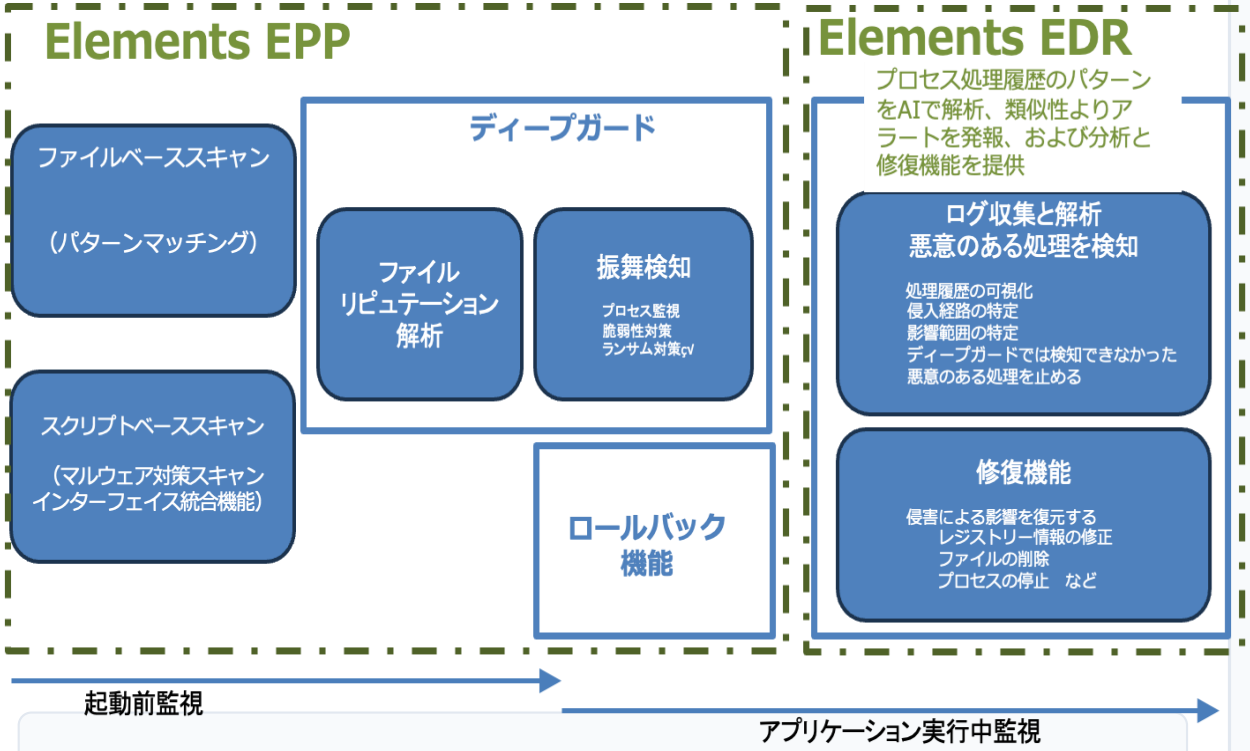
「各評価基準No.で要求されていることに対応するための情報提供ができる」

評価基準No.

CSS MDRでの対応内容

## CSS MDR で提供している機能名

### EDR機能（マルウエア対策）




従来のパターンマッチングによるウイルス検知機能にファイルのリピュテーション解析や振舞検知機能、ログの相関分析による悪意のある処理を検知します。

**✓ 発生したインシデントの処理停止、隔離、修復を行います。**

## 対応する評価基準No

### 要求への充足提供

**4-4-5-1**

ネットワークに接続しているすべてのパソコン及びサーバに、マルウェア対策ソフトウェアを導入すること。

**CSS MDR:** EPP/EDR機能の提供

### 要求に対応するための情報提供

**1-2-2-2**

入手した情報及びログの相関分析により、サイバー攻撃の予兆及びインシデントの発生の検知を可能とし、インシデントの防止及びインシデントが発生した場合の対応が導き出せる体制を整備すること。

**CSS MDR:** 対象とするログはサーバーおよびクライアントのログに基づいた分析でありネットワーク機器のログは対象外

**6-1-1-5**

セキュリティインシデントの報告フォーマットを整備すること。

**CSS MDR:** 重要インシデント発生時はチケット管理システムおよびメールにて、および月報で弊社提供フォーマットにて提供

| CSS MDR で提供している機能名 | 対応する評価基準No |
| --- | --- |
| **リアルタイムスキャンとマニュアルスキャン**<br><br>**リアルタイムスキャン**<br>・利用者がファイルを使用する直前に防御する常時監視機能<br><br>**マニュアルスキャン**<br>・**「毎日」「毎週」「4週毎」**の周期でディスク全体をスキャン<br>・**USBストレージ挿入時**に自動的にデバイス全体をスキャン<br>・メールボックス内の個別のメールをスキャン可能 | **要求への充足提供**<br><br>**4-4-5-2**<br>情報機器に応じたスキャン範囲及び頻度を定め、スキャンを実行すること。<br>**CSS MDR: 定期スキャン　オンデマンドスキャンの実行**<br><br>**5-1-2-3**<br>外部から受け取ったファイルについて安全性を確認するため、マルウェア対策ソフトのリアルタイムスキャンを実行する、又は仮想環境上で安全性を確認する仕組みを整備する。<br>**CSS MDR: リアルタイムスキャン機能提供**<br><br>**要求に対応するための情報提供**<br><br>**4-4-5-5**<br>メールによるマルウェア感染を防止するため、メールゲートウェイ、メールサーバ等でマルウェアチェックを実施すること。<br>**CSS MDR:** ローカルのメール受信ホルダーを定期チェック、悪意のあるコードを含むメールをリストアップする。 |

## CSS MDR で提供している機能名

### エージェントの自動更新

新バージョンのエージェントが自動で配信される




・**リブートレス**にて**自動バージョンアップ**（パターンファイルも自動更新）
・**製品のバージョン管理は不要**
・**15万台を超えるPCでのバージョンアップ実施の実績**

## 対応する評価基準No

### 要求への充足提供

**4-4-5-3**

マルウェア対策ソフトウェアのパターンファイルを、ベンダーの推奨に従ってアップデートすること。

**CSS MDR**
自動更新されます

### 要求に対応するための情報提供

## CSS MDR で提供している機能名

MicrosoftのOS, Office,その他ベンダーのアプリケーションのセキュリティパッチの確認が可能。
必要に応じて週次/月次でのパッチ適用も可能。

パッチのカテゴリー（セキュリティ関連かどうか）

| デバイス名 | ベンダ名 | ソフトウェア名 | パッチ名 | 現行バージョン | アップデートバージョン | カテゴリ | 重大度 |
|---|---|---|---|---|---|---|---|
| PC1 | Microsoft Corporation | Microsoft Teams classic | Microsoft Teams 1.7.00.33761 | 1.5.00.17656 | 1.7.00.33761 | security | important |
| PC1 | Google Inc. | Google Chrome | Google Chrome 132.0.6834.84 | 131.0.6778.265 | 132.0.6834.84 | security | important |
| PC1 | Zoom Video Communications, Inc. | Zoom | Zoom 6.3.6 | 6.2.7 | 6.3.6 | nonSecurity | unclassified |
| PC1 | Microsoft Corporation | Microsoft Visual C++ Redistributable 2012 (x86) | Microsoft Visual C++ Redistributable 2012 11.0.61030.0 | 11.0.60610.1 | 11.0.61030.0 | nonSecurity | unclassified |
| PC1 | Microsoft Corporation | Microsoft Visual C++ Redistributable 2012 (x64) | Microsoft Visual C++ Redistributable 2012 11.0.61030.0 | 11.0.60610.1 | 11.0.61030.0 | nonSecurity | unclassified |
| PC1 | Microsoft Corporation | Microsoft Visual C++ 2015-2019 Redistributable (x86) | Microsoft Visual C++ Redistributable 14.42.34433.0 | 14.27.29112.0 | 14.42.34433.0 | nonSecurity | unclassified |
| PC1 | Microsoft Corporation | Microsoft Visual C++ 2015-2019 Redistributable (x64) | Microsoft Visual C++ Redistributable 14.42.34433.0 | 14.27.29112.0 | 14.42.34433.0 | nonSecurity | unclassified |
| PC1 | Microsoft Corporation | Microsoft Teams (work or school) | Microsoft Teams 24335.208.3315.1951 | 24295.605.3225.8804 | 24335.208.3315.1951 | nonSecurity | unclassified |
| PC2 | Google Inc. | Google Chrome | Google Chrome 132.0.6834.84 | 131.0.6778.265 | 132.0.6834.84 | security | important |
| PC2 | Zoom Video Communications, Inc. | Zoom | Zoom 6.3.6 | 6.2.7 | 6.3.6 | nonSecurity | unclassified |
| PC2 | Microsoft Corporation | Microsoft Visual C++ Redistributable 2012 (x86) | Microsoft Visual C++ Redistributable 2012 11.0.61030.0 | 11.0.60610.1 | 11.0.61030.0 | nonSecurity | unclassified |
| PC2 | Microsoft Corporation | Microsoft Visual C++ Redistributable 2012 (x64) | Microsoft Visual C++ Redistributable 2012 11.0.61030.0 | 11.0.60610.1 | 11.0.61030.0 | nonSecurity | unclassified |
| PC2 | Microsoft Corporation | Microsoft Visual C++ 2015-2019 Redistributable (x86) | Microsoft Visual C++ Redistributable 14.42.34433.0 | 14.27.29112.0 | 14.42.34433.0 | nonSecurity | unclassified |
| PC2 | Microsoft Corporation | Microsoft Visual C++ 2015-2019 Redistributable (x64) | Microsoft Visual C++ Redistributable 14.42.34433.0 | 14.27.29112.0 | 14.42.34433.0 | nonSecurity | unclassified |
| PC2 | Microsoft Corporation | Microsoft Teams (work or school) | Microsoft Teams 24335.208.3315.1951 | 24295.605.3225.8804 | 24335.208.3315.1951 | nonSecurity | unclassified |
| PC3 | Microsoft Corporation | Windows Update Agent | 2024-10 .NET 6.0.35 Security Update for x64 Client (KB5045998) | 1309.2410.30012.0 | 10.0.26100 | security | important |
| PC3 | Google Inc. | Google Chrome | Google Chrome 132.0.6834.84 | 131.0.6778.265 | 132.0.6834.84 | security | important |
| PC3 | Igor Pavlov | 7-Zip exe (x64) | 7-Zip 24.09 | 22 | 24.09 | security | moderate |
| PC3 | Zoom Video Communications, Inc. | Zoom | Zoom 6.3.6 | 6.2.7 | 6.3.6 | nonSecurity | unclassified |
| PC3 | Microsoft Corporation | Microsoft Visual C++ 2015-2022 Redistributable (x86) | Microsoft Visual C++ 2015-2022 Redistributable 14.42.34433.0 | 14.30.30708.0 | 14.42.34433.0 | nonSecurity | unclassified |

重要度：WithSecure社の評価（Critical/Important）

## 対応する評価基準No

### 要求への充足提供

### 要求に対応するための情報提供

**4-4-4-2**
以下のいずれかに該当する場合、アップデートプログラムがリリースされてから14日以内に、アップデートすること。
- 当該アップデートが、ベンダーにより「重大」(Critical)又は 「高リスク」(High Risk)と説明される脆弱性を修正するものである。
- 当該アップデートが、CVSS v3 の基本スコアが7以上の脆弱性を修正するものである。
- 当該アップデートが修正する脆弱性のレベルの詳細がベンダーから提供されていない。

[対象]
-会社支給のパソコンの OS、ブラウザ及びOffice ソフト
-サーバの OS及びミドルウェア
-会社支給のスマートデバイスのOS及びアプリ
-インターネットとの境界に設置されているネットワーク機器の OS及びファームウェア

**CSS MDR:**
セキュリティーパッチの未適用PC一覧およびクライテリア情報の提供。必要であれば定期的なパッチの適用（FUを除く）。スマートデバイスを除く。

## CSS MDR で提供している機能名

### セキュリティー関連情報の収集

- Windowsの自動更新の状況
- パスワードの最小文字数
- アカウントロックアウトの閾値
- システムドライブの空き容量
- ディスクの暗号化ステータス
- BitLocker回復キーの収集
- リモートデスクトップの利用状況
- ローカルディスクの共有状況

## 対応する評価基準No

### 要求への充足提供

### 要求に対応するための情報提供

**3-1-1-6**
重要なシステムを構成する情報機器について、設定情報を把握するための仕組みを整備すること。

**CSS MDR**:
セキュリティに関する設定情報を収集（ただし、サーバーおよびPCについての収集となる）

## CSS MDR で提供している機能名

### 以下のデバイス情報の取得

- ホスト名
- OS名・バージョン
- BIOSメーカー
- MACアドレス
- IPアドレスVMの脆弱性

など

＊ 取得情報は次ページより３ページ記載

## 対応する評価基準No

### 要求への充足提供

**4-4-5-2**

パソコン及びサーバごとにマルウェア対策ソフトのスキャン範囲及び頻度を定め、スキャンを実行すること。

**CSS MDR:** 定期スキャン　オンデマンドスキャンの実行

### 要求に対応するための情報提供

**3-1-1-1**

適用範囲内のパソコン及びシンクライアントの製造元、OS及び台数を把握するための仕組みを整備すること。

**CSS MDR:** 脆弱性診断/ASM対応/セキュリティーパッチ未適用情報

＊CSS MDRではシンクライアントは対象外です

**4-4-5-5**

メールによるマルウェア感染を防止するため、メールゲートウェイ、メールサーバ等でマルウェアチェックを実施すること。

**CSS MDR:**
ローカルのメール受信ホルダーを定期チェック、悪意のあるコードを含むメールをリストアップする

次の時間が経過したらアカウントのロックアウトカウンターをリセットする

システム保全性保護

フルディスクアクセス

システム拡張

ネットワークコンテンツフィルタリング

ホットフィックスID

ホットフィックスの説明

ホットフィックスのインストール時間

ホットフィックスされたクライアント バージョン

ホットフィックスのステータス

ライセンス キーコード

有効期限

サブスクリプションタイプ

WithSecure MDR for Endpoints

デバイスUUID

前回のユーザー

UPN

OS 製品

IP アドレス

IPv6 アドレス

パブリックIP

発生状況

MAC アドレス

ホスト名

DNSアドレス

プラットフォームのバージョン

プラットフォームのビルド

管理者としてログインしています

ログインしているユーザー

最近ログインしたユーザー

実行中のすべてのセッションにパスワードが必要です

エージェントのインストール時刻

ユーザーに製品のアンインストールを許可する

ユーザーがセキュリティ機能を無効にすることを許可

アンインストールパスワードが空です

改ざん防止

インストーラーパッケージの作成時間

現在のファイアウォール プロファイル

共有事項の匿名な列挙は制限されています。

プラットフォーム アーキテクチャ

CPU名

CPUベンダー

CPU識別子

WithSecure製品のアンインストールはユーザーに許可されています

アンインストール パスワードは設定されています

改ざん防止

ディープガード

リアルタイム スキャン

リアルタイムスキャンがロックされています

UUIDソース

プロファイルから除外されたパス

除外されたローカルのパス

マルウェア定義ファイルの最新更新

マルウェア定義ファイルのバージョン

前回のEPPスキャンタイプ

前回のEPPスキャン開始

前回のEPPスキャン完了

前回のEPPスキャンタスクのステータス

前回のEPPスキャン済みファイルの数

検出した感染の数

登録日

OS名前

マルウェア保護

Windows自動更新

パスワードの最小文字数

アカウントロックアウトのしきい値

アカウントのロックアウト期間

ステータスの更新日時

ソフトウェアアップデートのステータス

クライアント バージョン

システムドライブの空き容量

ディスク暗号化ステータス

ドライブの暗号化

BitLocker回復キーの収集が成功しました

スクリーンセーバーを有効にしました

スクリーンセーバーのパスワード保護

共有フォルダーには誰でもアクセスできます

共有フォルダー

ローカルドライブはネットワークに共有されています

リモート デスクトップ プロトコル（RDP）は有効です

企業名

ラベル

コメント

アセットグループ

デバイスの重要度

保護ステータスの概要

全体保護

指定プロファイル

プロファイルの指定ステータス

OS バージョン

ファイアウォール

デバイス制御

アプリケーション制御 (Premium)

DataGuard (Premium)

ネットワークの隔離

EDRセンサー

アドバンスド・レスポンス

Active Directory組織単位

オンライン

OSのサポート終了

Windows セキュアブート証明書

Windows セキュアブート証明書が有効です

Windows ライセンスステータス

最終再開時間

再起動が必要です

再起動リクエストの理由

オフロードスキャンの状態

オフロードスキャンが切断されました

オフロードスキャンの平均アップロード速度

オフロードスキャンが実行したスキャン

オフロードスキャンが失敗したスキャン

オフロードスキャンのトラフィック

オフロードスキャンの開始時間

BIOSメーカー

コンピュータモデル

プロセッサコア

システムドライブの容量

物理メモリサイズ

空き物理メモリ

シリアル番号

BIOSバージョン

BIOSリリース日

コンピューターの説明

ディスクタイプ

ボリューム情報

RAM情報

管理者がログインしています

ディスク暗号化ポリシー

BitLocker リカバリキーの収集が有効です

BitLocke全体の保護ステータス

ゲスト アカウント

広告IDのステータス

アプリに位置情報へのアクセスを許可する

起動時に追加認証を要求する

起動時の拡張PINを許可する

トラステッドプラットフォームモジュール（TPM）を使用する
起動PINでトラステッドプラットフォームモジュール（TPM）を使用する

TPMはこのデバイスで使用できます

TPM仕様バージョン

リモート デスクトップ プロトコル (RDP) はアクティブです

リモートデスクトップサービスを介したログオンを許可する

リモートデスクトップサービスを介したログオンを拒否する
アカウント：ローカルアカウントでの空のパスワードの使用をコンソールログオンのみに制限する

最後に月次カウンターをリセットした日

毎月のリアルタイムファイルスキャン数

毎月のリアルタイム スキャンで検出された感染数

毎月の手動/スケジュールファイルスキャン数

毎月の手動/スケジュールスキャンで検出された感染数

Google Chromeプラグインのステータス

Mozilla Firefoxプラグインのステータス

Microsoft Edgeプラグインのステータス

Safari プラグインのステータス

デフォルトブラウザ

デフォルトのブラウザのプラグインステータス

接続ステータス

接続が常に失敗する

接続が時々失敗する

最新のソフトウェアアップデートのステータスアップデート日時。

最新のソフトウェアアップデート日時

最新のソフトウェアアップデートのインストール日時。

EDRオープンインシデント（重大リスク）

未解決の高リスク EDR インシデント

EDRオープンインシデント（中リスク）

EDR 未解決のインシデント

EDRオープンインシデント（中リスク）

EDR 未解決のインシデント

XM エージェントステータス

VM リスクスコア

エクスポージャリスク

XM ライセンス キーコード

ビジネスコンテキスト

公開エクスプロイト

フラグ

VM 脆弱性

VMの「重大」な脆弱性

VMの「高」脆弱性

VMの「中」脆弱性

VMの「低」脆弱性

VM 情報レベルの脆弱性

パブリックインターネットに公開済み

制御されたアップデート採用モード

制御対象アップデート：割り当て済みリリースグループ

制御対象アップデート：割り当て済みリリースグループの有効期限

制御対象アップデート：有効なリリースグループ

制御対象アップデート：有効なリリースグループの有効期限

定義更新ソース

Software Updater で使用されている現在の Elements Connector アドレス

アップデートをダウンロードするための現在のプロキシ

アップデートをダウンロードするためのプロキシの種類

Ultralight Coreのバージョン

Ultralight Coreのステータス

SMBIOS GUID

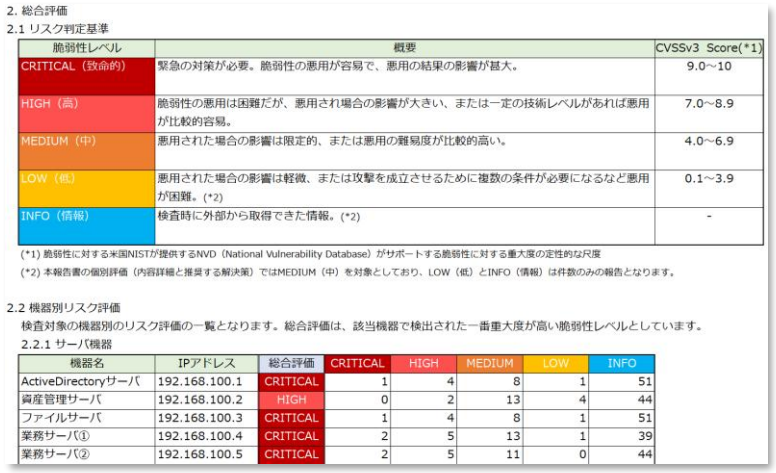
Active Directory GUID

最終 XM スキャン

## CSS MDR で提供している機能名

# 脆弱性診断の実施（年2回）

＜診断対象＞
サーバ、ネットワーク機器、NAS装置などアプライアンス機器
＜診断内容＞
デバイスおよびアプリケーションにおけるソフトウェアの弱点、パッチの不足、構成ミスを網羅的に診断
＜診断方法＞
インターネット側からの診断
内部からの診断
＜診断レポート＞
総合評価
機器別評価
機器別脆弱性詳細
重大な脆弱性に対する推奨対応策の提示



2. 総合評価

2.1 リスク判定基準

| 脆弱性レベル | 概要 | CVSSv3 Score(*1) |
|---|---|---|
| CRITICAL（致命的） | 緊急の対策が必要。脆弱性の悪用が容易で、悪用の結果の影響が甚大。 | 9.0～10 |
| HIGH（高） | 脆弱性の悪用は困難だが、悪用され場合の影響が大きい、または一定の技術レベルがあれば悪用が比較的容易。 | 7.0～8.9 |
| MEDIUM（中） | 悪用された場合の影響は限定的、または悪用の難易度が比較的高い。 | 4.0～6.9 |
| LOW（低） | 悪用された場合の影響は軽微、または攻撃を成立させるために複数の条件が必要になるなど悪用が困難。(*2) | 0.1～3.9 |
| INFO（情報） | 検査時に外部から取得できた情報。(*2) | - |

(*1) 脆弱性に対する米国NISTが提供するNVD（National Vulnerability Database）がサポートする脆弱性に対する重大度の定性的な尺度

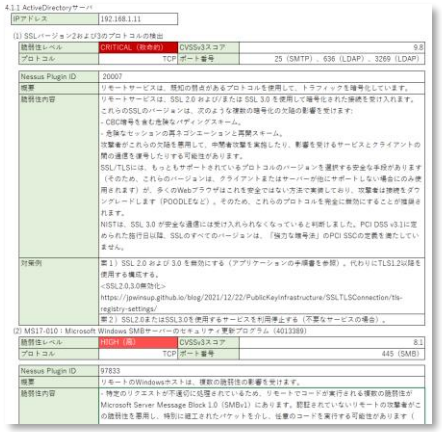
(*2) 本報告書の個別評価（内容詳細と推奨する解決策）ではMEDIUM（中）を対象としており、LOW（低）とINFO（情報）は件数のみの報告となります。

2.2 機器別リスク評価

検査対象の機器別のリスク評価の一覧となります。総合評価は、該当機器で検出された一番重大度が高い脆弱性レベルとしています。

2.2.1 サーバ機器

| 機器名 | IPアドレス | 総合評価 | CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|---|---|---|
| ActiveDirectoryサーバ | 192.168.100.1 | CRITICAL | 1 | 4 | 8 | 1 | 51 |
| 資産管理サーバ | 192.168.100.2 | HIGH | 0 | 2 | 13 | 4 | 44 |
| ファイルサーバ | 192.168.100.3 | CRITICAL | 1 | 4 | 8 | 1 | 51 |
| 業務サーバ① | 192.168.100.4 | CRITICAL | 2 | 5 | 13 | 1 | 39 |
| 業務サーバ② | 192.168.100.5 | CRITICAL | 2 | 5 | 11 | 0 | 44 |



4.1.1 ActiveDirectoryサーバ

| IPアドレス | 192.168.1.11 | | |
|---|---|---|---|
| (1) SSLバージョン2および3のプロトコルの検出 | | | |
| 脆弱性レベル | CRITICAL（致命的） | CVSSv3スコア | 9.8 |
| プロトコル | TCP | ポート番号 | 25（SMTP）、636（LDAP）、3269（LDAP） |
| Nessus Plugin ID | 20007 | | |
| 概要 | リモートサービスは、暗号化の弱点があるプロトコルを使用して、トラフィックを暗号化しています。 | | |
| 脆弱性内容 | リモートサービスは、SSL 2.0 および/または SSL 3.0 を使用して暗号化された接続を受け入れます。これらのSSLのバージョンは、次のような複数の暗号化の欠陥の影響を受けます：<br>- CBC暗号を含む危険なパディングスキーム。<br>- 危険なセッションの再ネゴシエーションと再開スキーム。<br>攻撃者がこれらの欠陥を悪用して、中間者攻撃を実施したり、影響を受けるサービスとクライアントの間の通信を復号したりする可能性があります。<br>SSL/TLSには、もっともサポートされているプロトコルのバージョンを選択する安全な手段があります（そのため、これらのバージョンは、クライアントまたはサーバーが他にサポートしない場合にのみ使用されます）が、多くのWebブラウザはこれを安全ではない方法で実装しており、攻撃者は接続をダウングレードします（POODLEなど）。そのため、これらのプロトコルを完全に無効にすることが推奨されます。<br>NISTは、SSL 3.0 が安全な通信には受け入れられなくなっていると判断しました。PCI DSS v3.1に定められた期日以降、SSLのすべてのバージョンは、「強力な暗号法」のPCI SSCの定義を満たしていません。 | | |
| 対策例 | 要1）SSL 2.0 および 3.0 を無効にする（アプリケーションの手順書を参照）。代わりにTLS1.2以降を使用する構成する。<br><SSL2.0,3.0無効化><br>https://jpwinsup.github.io/blog/2021/12/22/PublicKeyInfrastructure/SSLTLSConnection/tls-registry-settings/<br>要2）SSL2.0またはSSL3.0を使用するサービスを利用停止する（不要なサービスの場合）。 | | |
| (2) MS17-010：Microsoft Windows SMBサーバーのセキュリティ更新プログラム（4013389） | | | |
| 脆弱性レベル | HIGH（高） | CVSSv3スコア | 8.1 |
| プロトコル | TCP | ポート番号 | 445（SMB） |
| Nessus Plugin ID | 97833 | | |
| 概要 | リモートのWindowsホストは、複数の脆弱性の影響を受けます。 | | |
| 脆弱性内容 | - 特定のリクエストが不適切に処理されているため、リモートでコードが実行される複数の脆弱性がMicrosoft Server Message Block 1.0（SMBv1）にあります。認証されていないリモートの攻撃者がこの脆弱性を悪用し、特別に細工されたパケットを介し、任意のコードを実行する可能性があります（ | | |

## 対応する評価基準No

### 要求への充足提供

**1-2-2-1**
サイバー攻撃及び脆弱性に関する公開情報・非公開情報を活用する体制を整備すること。
**CSS MDR**: 脆弱性診断/ASM対応/セキュリティーパッチ未適用情報を提供

**3-2-1-2**
脆弱性情報/脅威情報を収集する情報源、ツール及び頻度を定めること
**CSS MDR:** Nessus Professionalを利用して年2回の実行が可能

**3-2-1-3**
収集した脆弱性情報/脅威情報の対応要否判断基準・対応手順を定めること。
**CSS MDR**:脆弱性診断によりCritical /High/Mid/infoのクライテリアで重要度を分類

**3-2-1-4**
管理対象の情報機器における脆弱性の残存状況を把握するための仕組みを整備すること。
**CSS MDR:**
年2回の継続実施により対応状況を管理可能

### 要求に対応するための情報提供

**3-2-1-5**
収集した脆弱性情報/脅威情報に対する対応履歴を記録し、対応漏れがないかどうかについて月次で点検すること。

**CSS MDR:**
前提となる情報を提供

## CSS MDR で提供している機能名

### 脆弱性診断の実施（外部:日次/月次）

＜診断対象＞
グローバルIPを持つ機器の脆弱性を日次もしくは月次に実施いたします

＜診断内容＞
デバイスおよびアプリケーションにおけるソフトウェアの弱点、パッチの不足、構成ミスを網羅的に診断

＜診断方法＞
インターネット側からの診断

＜診断レポート＞
速報としてメールにてお知らせいたします

**対象機器**

**・ネットワーク機器**

Fortigate, Ivanti, Sonicwall, Cisco, F5, Juniper, Palo Alto, Checkpoint, FireEye, Sophos

**・Web Server**

## 対応する評価基準No

### 要求への充足提供

### 要求に対応するための情報提供

**4-4-4-3**

日次もしくは月次にグローバルIPに対して脆弱性を調査し問題があれば報告をあげる

**CSS MDR:**

日次はアラートメールとして通報。
月次は　月次レポートとして情報を提供。

## CSS MDR で提供している機能名

# ブラウザー保護機能

HTTP/HTTPSのURLサイトの安全性評価を**「安全」「危険」「不審」「禁止」**の４つ段階で振り分ける。

各WEBブラウザソフトの検索結果でもアイコンで表示可能。

**＊HTTPSのWEBサーバとの通信は暗号化されている為、**
**URLフィルタリングはWEBブラウザを用いた対策が有効**




## 対応する評価基準No

### 要求への充足提供

### 要求に対応するための情報提供

**4-4-5-4**
パソコン/Web ゲートウェイを対象に、不正な Web サイトへのアクセスを制限すること。

**CSS MDR:**
エージェント導入機器（サーバー/クライアント）に対してブラウザー保護機能を提供
*CSS MDRではWebゲートウェイは対象外

## CSS MDR で提供している機能名

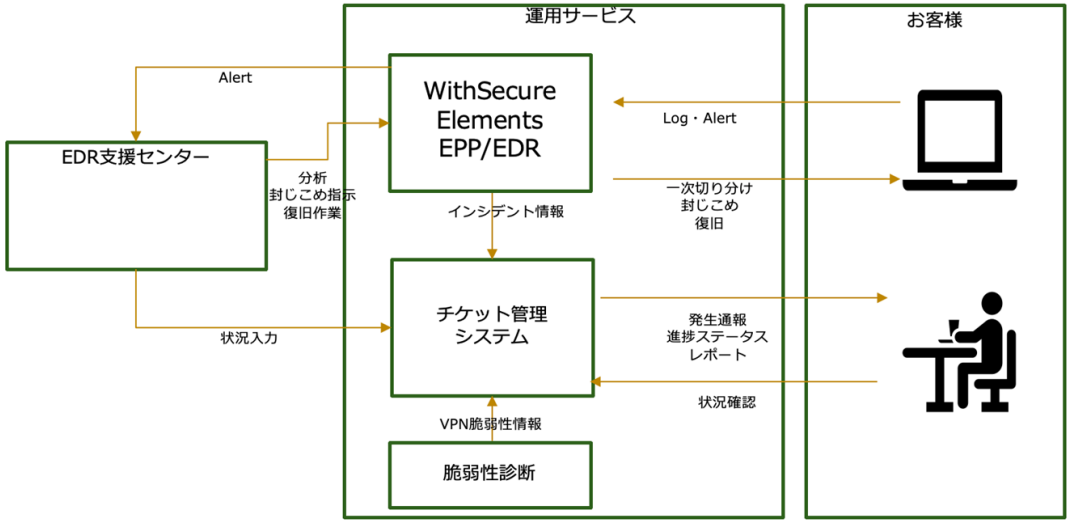
# CSS MDRサービスの運用全体像

■ 基本的なサービス内容

- アラート一次受付
- 一次切り分け（トリアージ）
- お客様への連絡
- ネットワーク隔離
- 端末復旧処置
- 対応報告

■ 重大度別／端末種別による対応（例）

<Highの場合>
ネットワーク隔離後、お客様（情報システム課）へメールで連絡し、その後、復旧作業を行う
<Middleの場合>
お客様へ連絡（情報システム課）へ電話し、承認を得たうえでネットワーク隔離し、その後、復旧作業を行う
<Lowの場合>
基本的に対応しない。上記対応時に必要に応じて参考情報として確認する




## 対応する評価基準No

### 要求への充足提供

### 要求に対応するための情報提供

**6-1-1-1**
以下の手順を含んだセキュリティインシデントへの対応手順を定めること。
①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告
**CSS MDR**:
WithSecure Elements EPP/EDRで提供される機能の範囲で対応

**6-1-1-5**
セキュリティインシデントの報告フォーマットを整備すること。
**CSS MDR:**
重要インシデント発生時はチケット管理システムおよびメールにて　および月報で弊社提供フォーマットにて提供


NHC
PARTNERS