WIN-4-5005-01

HITACHI

日立産業用コンピュータ HF-W シリーズ

セキュリティ設定一覧

（Windows Server® IoT 2025 Standard 編）

ユーザーズ
マニュアル

株式会社 日立インダストリアルプロダクツ

２０２５年　９月　（第１版）　ＷＩＮ－４－５００５－０１

はじめに

このマニュアルは、日立産業用コンピュータ HF-W（Windows®版）シリーズ、IoT 対応 産業用コントローラ HF-W/IoT シリーズにおける Windows®のセキュリティ設定内容について記述したものです。

＜マニュアル構成＞

このマニュアルは、次のような構成となっています。

はじめに

第１章　HF-W シリーズ、HF-W/IoT シリーズのセキュリティ対策

第２章　設定一覧

装置（ハードウェア）の操作や注意事項、日立産業用コンピュータとしての RAS 機能の使い方などについては、下記ホームページから電子マニュアルをダウンロードして参照してください。

ホームページアドレス：

https://www.hitachi-ip.co.jp/products/hfw/products/win/w/download/index.html

＜商標について＞

・Microsoft®、Windows®は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

・CIS Benchmarks™は、Center for Internet Security, Inc.の商標です。

目次

第1章　HF-W シリーズ、HF-W/IoT シリーズのセキュリティ対策

1.1　概要

HF-Wのセキュリティ対策の設定項目と設定値の一覧です。

1.1.1　対象機種

本書が対象とするプレインストール OS、CIS Benchmarks™のバージョンとその対象のHF-Wシリーズは次のとおりです。

- HF-W2000 モデル68

プレインストール OS	CIS Benchmarks™ガイドライン バージョン	製品型式	モデル
Windows Server® IoT 2025 Standard（64bit）	CIS Microsoft Windows Server 2025 Benchmark v1.0.0 - 03-19-2025	HJ-2068-SGMB	B モデル
		HJ-2068-SGMT	T モデル

1.1.2　設定値記載項目

CIS Benchmarks™ガイドラインに記載のセキュリティ設定項目と、本書の「第2章 設定一覧」に記載の項目との対応は次のとおりです。

CIS Benchmarks™	記載内容	設定一覧の記載有無	
Item No. Title	項番	記載あり	・No
	推奨するセキュリティ設定値の概要	記載あり	・セキュリティ項目
Profile Applicability	セキュリティ項目の重要度と適用範囲	記載なし	―
Description	セキュリティ項目の詳細説明	記載なし	―
Rationale	セキュリティ設定変更の根拠	記載なし	―
Impact	セキュリティ項目を変更しない場合の影響	記載なし	―
Audit	セキュリティ設定の確認方法	記載なし	―
Remediation	セキュリティ項目の設定方法	記載あり	・ローカルグループポリシーのパス ・推奨される設定値
Default Value	セキュリティ項目のデフォルト値	記載あり	・Windows® 標準設定値
References	関連する参照情報	記載なし	―
CIS Controls®	対応する CIS Controls®（*1）の項目	記載なし	―

（*1）CIS Controls®とは、CISの提供するサイバーセキュリティ対策のガイドラインです。

1.2　その他の設定値

HF-WはRAS機能を実現するために独自にローカルグループポリシーの設定を変更しています。

RAS機能の動作に影響を及ぼすため、以下のローカルグループポリシーの設定は変更しないでください。

（○：変更あり、×：変更なし）

設定項目	内容	ローカルグループポリシーのパス	Windows Server® IoT 2025 Standard
Windows Update時のドライバアップデートの無効化	Windows Update時のサードパーティ製ドライバーに対するアップデートを無効化する。	コンピューターの構成\管理用テンプレート\Windowsコンポーネント\Windows Update\Windows Updateから提供される更新プログラムの管理\Windows Update からドライバーを除外する	○
アクティビティの履歴のオフ	[アクティビティの履歴] の「このデバイスでのアクティビティの履歴を保存する」をオフにする。	コンピューターの構成\管理用テンプレート\システム\OSポリシー\ユーザーアクティビティの公開を許可する	○

第2章　設定一覧

2.1　Windows Server® IoT 2025 Standard

Windows® OS の標準設定値から変更したセキュリティ項目の設定値を記載します。

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
2.2.3	「ネットワークからこのコンピュータにアクセスする」が「管理者、認証ユーザ」に設定されていることを確認する (MS のみ)	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\ユーザー権利の割り当て\ネットワーク経由でのアクセス	Administrators, Backup Operators,Everyone,Users	Administrators, Authenticated Users
2.2.8	「ローカルログオンを許可する」が「管理者」 に設定されていることを確認する (MS のみ)	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\ユーザー権利の割り当て\ローカル ログオンを許可	Administrators, Backup Operators,Everyone,Users	管理者
2.2.11	「ファイルとディレクトリのバックアップ」が「管理者」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\ユーザー権利の割り当て\ファイルとディレクトリのバックアップ	Administrators, Backup Operators	管理者
2.2.22	「ネットワークからこのコンピュータへのアクセスを拒否」に「ゲスト、ローカル アカウント、および管理者グループのメンバー」が含まれていることを確認します (MS のみ)	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\ユーザー権利の割り当て\ネットワーク経由のアクセスを拒否	未設定(空)	Guests, Local account and member of Administrators group.
2.2.23	「ゲスト」 を含めるには、「バッチジョブとしてログオンを拒否」を確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\ユーザー権利の割り当て\バッチ ジョブとしてのログオンを拒否	未設定(空)	Guests
2.2.24	「サービスとしてのログオンを拒否」に「ゲスト」が含まれていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\ユーザー権利の割り当て\サービスとしてのログオンを拒否	未設定(空)	Guests
2.2.25	「ゲスト」を含めるには、「ローカルログオンを拒否する」を確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\ユーザー権利の割り当て\ローカル ログオンを拒否	未設定(空)	Guests

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
2.2.27	「リモートデスクトップサービスによるログオンを拒否する」が「ゲスト、ローカルアカウント」に設定されていること(MS のみ)	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\ユーザー権利の割り当て\リモート デスクトップ サービスを使ったログオンを拒否	未設定(空)	Guests, Local account.
2.2.46	「ファイルとディレクトリの復元」が「管理者」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\ユーザー権利の割り当て\ファイルとディレクトリの復元	Administrators, Backup Operators	管理者
2.2.47	「システムのシャットダウン」が「管理者」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\ユーザー権利の割り当て\システムのシャットダウン	Administrators, Backup Operators	Administrators
2.3.2.1	「監査: 監査ポリシー サブカテゴリ設定(Windows Vista 以降)を強制的して、監査ポリシーカテゴリの設定を上書きする」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\Windows 設定\セキュリティ設定\ローカル ポリシー\セキュリティ オプション\監査: 監査ポリシー サブカテゴリの設定 (Windows Vista 以降) を強制して、監査ポリシー カテゴリの設定を上書きする	未定義	有効
2.3.8.1	「Microsoft ネットワーク クライアント: 常に通信にデジタル署名行う」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\Microsoft ネットワーク クライアント:常に通信にデジタル署名を行う	無効	有効
2.3.9.2	「Microsoft ネットワーク サーバー: 通信にデジタル署名(常に)」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\Microsoft ネットワーク サーバー: 常に通信にデジタル署名を行う	無効	有効
2.3.9.3	「Microsoft ネットワーク サーバー: 通信にデジタル署名を行う (クライアントが同意した場合)」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\Microsoft ネットワーク サーバー: クライアントが同意すれば、通信にデジタル署名を行う	無効	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
2.3.9.5	「Microsoft ネットワークサーバー: サーバー SPN ターゲット名検証レベル」が「クライアントによって提供されている場合は受け入れる」に設定されていることを確認する (MS のみ)	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\Microsoft ネットワーク サーバー: サーバー SPN ターゲット名検証レベル	未定義	クライアントによって提供される場合は受け入れる
2.3.10.3	「ネットワークアクセス: SAM アカウントの匿名の列挙を許可しない」が「有効」に設定されていることを確認する (MS のみ)	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ネットワーク アクセス: SAM アカウントおよび共有の匿名の列挙を許可しない	無効	有効
2.3.10.11	「ネットワークアクセス: SAM へのリモート呼び出しを許可するクライアントを制限する」が「管理者: リモートアクセス: 許可」に設定されていることを確認する (MS のみ)	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ネットワーク アクセス: SAM へのリモートの呼び出しを許可するクライアントを制限する	未定義	管理者: リモートアクセス: 許可 "O:BAG:BAD:(A;;RC;;;BA)
2.3.11.1	「ネットワークセキュリティ: NTLM で Local System によるコンピューターID の使用を許可する」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ネットワーク セキュリティ: NTLM で Local System によるコンピューター ID の使用を許可する	未定義	有効
2.3.11.2	「ネットワークセキュリティ: LocalSystem による NULL セッションフォールバックを許可する」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ネットワーク セキュリティ: LocalSystem による NULL セッション フォールバックを許可する	未定義	無効
2.3.11.3	「ネットワークセキュリティ: オンライン id を使用するためにこのコンピュータへの PKU2U 認証要求を許可する」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ネットワーク セキュリティ: オンライン ID を使用するためのこのコンピューターへの PKU2U 認証要求を許可する。	未定義	無効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
2.3.11.4	「ネットワークセキュリティ: Kerberos に許可される暗号化の種類を構成する」が「AES128_HMAC_SHA1、AES256_HMAC_SHA1、将来の暗号化の種類」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ネットワーク セキュリティ: Kerberos で許可する暗号化の種類を構成する	未定義	AES128_HMAC_SHA1, AES256_HMAC_SHA1, 将来使用する暗号化の種類
2.3.11.7	「ネットワークセキュリティ: LAN Manager 認証レベル」が「NTLMv2 応答のみ送信する」に設定されていることを確認する LM と NTLM を拒否する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ネットワーク セキュリティ: LAN Manager 認証レベル	未定義	NTLMv2 応答のみ送信（LM と NTLM を拒否する）
2.3.11.10	「ネットワークセキュリティ: NTLM SSP ベース (セキュア RPC を含む) のクライアント向け最小セッション セキュリティ」が「NTLMv2 セッションセキュリティが必要、128 ビット暗号化が必要」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ネットワーク セキュリティ: NTLM SSP ベース (セキュア RPC を含む) のクライアント向け最小セッション セキュリティ	128 ビット暗号化が必要	NTLMv2 セッション セキュリティが必要、128 ビット暗号化が必要
2.3.11.11	「ネットワークセキュリティ: NTLM SSP ベース (セキュア RPC を含む) のサーバー向け最小セッションセキュリティ」に「NTLMv2 セッションセキュリティが必要、128 ビット暗号化が必要」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ネットワーク セキュリティ: NTLM SSP ベース (セキュア RPC を含む) のサーバー向け最小セッション セキュリティ	128 ビット暗号化が必要	NTLMv2 セッション セキュリティが必要、128 ビット暗号化が必要

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
2.3.17.1	「ユーザーアカウント制御: ビルトイン Administrator アカウントの管理者承認モード」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ユーザー アカウント制御: ビルトイン Administrator アカウントのための管理者承認モード	未定義	有効
2.3.17.2	「ユーザー アカウント制御: 管理者承認モードでの管理者の昇格プロンプトの動作」が「安全なデスクトップで同意を求める」に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ユーザー アカウント制御: 管理者承認モードでの管理者に対する昇格時のプロンプトの動作	Windows 以外のバイナリに対する同意を要求する	セキュリティで保護されたデスクトップで同意を要求する
2.3.17.3	「ユーザーアカウント制御: 標準ユーザーの昇格プロンプトの動作」が「昇格要求を自動的に拒否する」に設定されていることを確認する	コンピューターの構成\ポリシー\Windows の設定\セキュリティの設定\ローカル ポリシー\セキュリティ オプション\ユーザー アカウント制御: 標準ユーザーに対する昇格時のプロンプトの動作	資格情報の入力を求めるプロンプトが表示される	昇格の要求を自動的に拒否する
18.1.2.2	「ユーザーがオンライン音声認識サービスを有効にできるようにする」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\コントロール パネル\地域と言語のオプション\ユーザーがオンライン音声認識サービスを有効にできるようにする	未構成	無効
18.6.8.5	「安全でないゲストログオンを有効にする」が「無効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\ネットワーク\Lanman ワークステーション\安全でないゲスト ログオンを有効にする	未構成	無効
18.6.11.3	「DNS ドメインネットワーク上でのインターネット接続の共有の使用を禁止する」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\ネットワーク\ネットワーク接続\DNS ドメイン ネットワーク上でインターネット接続の共有の使用を禁止する	未構成	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
18.6.11.4	「ネットワークの場所を設定するときにドメインユーザーに昇格を要求する」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\ネットワーク\ネットワーク接続\ネットワークの場所を設定するときにドメイン ユーザーに昇格を要求する	未構成	有効
18.6.14.1	「強化された UNC パス」が「有効」に設定され、すべての NETLOGON および SYSVOL 共有に「相互認証が必要」と「整合性が必要」と「プライバシーが必要」が設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\ネットワーク\ネットワーク プロバイダー\強化された UNC パス	未構成	有効：すべての NETLOGON および SYSVOL 共有に「相互認証が必要」と「整合性が必要」と「プライバシーが必要」が設定
18.7.1	「印刷スプーラーにクライアント接続の受け入れを許可する」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\プリンター\印刷スプーラーにクライアント接続の受け入れを許可する	未構成	無効
18.9.3.1	「プロセス作成イベントにコマンドラインを含める」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\プロセス作成の監査\プロセス作成イベントにコマンド ラインを含める	未構成	有効
18.9.4.1	「暗号化 Oracle 修復」が「有効: 強制的に更新されたクライアント」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\資格情報の委任\暗号化 オラクルの修復	未構成	有効：更新済みクライアントの強制
18.9.4.2	「リモートホストがエクスポートできない資格情報の委任を許可する」を「有効」に設定します (自動化されています)	コンピューターの構成\ポリシー\管理用テンプレート\システム\資格情報の委任\リモート ホストでエクスポート不可の資格情報の委任を許可する	未構成	有効
18.9.7.2	「インターネットからのデバイスメタ情報の取得を禁止する」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\デバイスのインストール\デバイス メタデータに関連付けられているアプリケーションの自動ダウンロードを禁止する	未構成	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
18.9.13.1	「ブート開始ドライバーの初期化ポリシー」が「有効: 良好、不明、および不良(ブートに不可欠)」に設定されていることを確認します。	コンピューターの構成\ポリシー\管理用テンプレート\システム\起動時マルウェア対策\ブート開始ドライバーの初期化ポリシー	未構成	有効
18.9.19.2	「レジストリポリシー処理を構成する:定期的なバックグラウンド処理中に適用しない」が「有効: FALSE」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\グループ ポリシー\レジストリ ポリシーの処理を構成する	未構成	有効: FALSE (unchecked：バックグラウンドで定期的に処理しているときは適用しない)
18.9.19.3	「レジストリポリシーの処理を構成する: グループポリシーオブジェクトが変更されていなくても処理する」が「有効: TRUE」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\グループ ポリシー\レジストリ ポリシーの処理を構成する	未構成	有効: TRUE (checked：グループ ポリシー オブジェクトが変更されていなくても処理する)
18.9.20.1.1	「プリントドライバの HTTP 経由のダウンロードをオフにする」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\インターネット通信の管理\インターネット通信の設定\プリンター ドライバーの HTTP 経由でのダウンロードをオフにする	未構成	有効
18.9.20.1.5	「Web 発行およびオンライン注文ウィザードのインターネットダウンロードをオフにする」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\インターネット通信の管理\インターネット通信の設定\Web 発行およびオンライン注文ウィザードのインターネット ダウンロードをオフにする	未構成	有効
18.9.26.1	[カスタム SSP および AP の LSASS へのロードを許可する] が [無効] に設定されていることを確認します。	コンピューターの構成\ポリシー\管理用テンプレート\システム\ローカルセキュリティ機関\カスタム SSP と AP を LSASS に読み込むことを許可する	有効	無効
18.9.28.1	「ユーザーがサインイン時にアカウントの詳細を表示できないようにブロックする」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\ログオン\ユーザーがサインイン時にアカウントの詳細を表示できないようにブロックする	未構成	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
18.9.28.2	「ネットワーク選択 UI を表示しない」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\ログオン\ネットワークの選択の UI を表示しない	未構成	有効
18.9.28.3	「ドメインに参加しているコンピューターに接続しているユーザーを列挙しない」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\ログオン\ドメインに参加しているコンピュータに接続している ユーザーを列挙しない	未構成	有効
18.9.28.4	「ドメインに参加しているコンピュータのローカルユーザーを列挙する」が「無効」に設定されていることを確認する (MS のみ)	コンピューターの構成\ポリシー\管理用テンプレート\システム\ログオン\ドメインに参加しているコンピューターのローカル ユーザーを列挙する	未構成	無効
18.9.28.5	「ロック画面でアプリの通知をオフにする」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\ログオン\ロック画面のアプリ通知をオフにする	未構成	有効
18.9.28.6	「画像のパスワードサインインをオフにする」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\ログオン\ピクチャ パスワードを使用したサインインをオフにする	未構成	有効
18.9.28.7	「便利な PIN サインインをオンにする」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\システム\ログオン\便利な PIN を使用したサインインをオンにする	未構成	無効
18.9.36.1	「RPC エンドポイントマッパークライアント認証を有効にする」が「有効」に設定されていることを確認する (MS のみ)	コンピューターの構成\ポリシー\管理用テンプレート\システム\リモート プロシージャ コール\RPC エンドポイント マッパー クライアント認証を有効にする	未構成	有効
18.10.5.1	「Microsoft アカウントの省略可能を許可する」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\アプリ実行時 \Microsoft アカウントの省略可能を許可する	未構成	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
18.10.7.1	「ボリューム以外のデバイスの自動再生を許可しない」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\自動再生のポリシー\ボリューム以外のデバイスの自動再生を許可しない	未構成	有効
18.10.7.3	「自動再生機能をオフにする」が「有効: すべてのドライブ」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\自動再生のポリシー\自動再生機能をオフにする	未構成	有効: すべてのドライブ
18.10.8.1.1	「拡張スプーフィング対策を構成する」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\生体認証\顔特徴\拡張スプーフィング対策を構成する	未構成	有効
18.10.12.3	「Microsoft コンシューマー エクスペリエンスを無効にする」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\クラウド コンテンツ\Microsoft コンシューマー エクスペリエンスを無効にする	未構成	有効
18.10.14.1	「[パスワードの表示]ボタンを非表示にする」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\資格情報のユーザー インターフェイス\[パスワードの表示]ボタンを非表示にする	未構成	有効
18.10.15.3	「OneSettings ダウンロードを無効にする」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\データの収集とプレビュー ビルド\OneSettings ダウンロードを無効にする	未構成	有効
18.10.15.4	「フィードバック通知を表示しない」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\データの収集とプレビュー ビルド\フィードバックの通知を表示しない	未構成	有効
18.10.15.5	「OneSettings 監査を有効にする」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\データの収集とプレビュー ビルド\OneSettings 監査を有効にする	未構成	有効
18.10.15.6	「診断ログ収集の制限」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\データの収集とプレビュー ビルド\診断ログの収集を制限する	未構成	有効
18.10.15.7	「ダンプコレクションの制限」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\データ収集とプレビュー ビルド\ダンプの収集を制限する	未構成	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
18.10.15.8	「インサイダービルドに関するユーザコントロールの切り替え」が「無効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\データ収集とプレビュー ビルド\Insider ビルドに関するユーザーコントロールの切り替え	未構成	無効
18.10.29.3	「エクスプローラのデータ実行防止をオフにする」が「無効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\エクスプローラー\エクスプローラーのデータ実行防止をオフにする	未構成	無効
18.10.29.4	「破損時にヒープ終了をオフにする」が「無効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\エクスプローラー\破損後のヒープ終了をオフにする	未構成	無効
18.10.29.5	「シェルプロトコルの保護モードをオフにする」が「無効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\エクスプローラー\シェル プロトコルの保護モードをオフにする	未構成	無効
18.10.42.1	「すべてのコンシューマの Microsoft アカウントユーザ認証をブロックする」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Microsoft アカウント\すべてのコンシューマー Microsoft アカウント ユーザーの認証をブロックする	未構成	有効
18.10.43.5.1	「Microsoft MAPS へのレポートに対してローカル設定の優先を構成する」が「無効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Microsoft Defender ウイルス対策\MAPS\Microsoft MAPS へのレポートに対してローカル設定の優先を構成する	未構成	無効
18.10.43.6.3.1	「ユーザーとアプリが危険な web サイトにアクセスするのを防ぎます」が「有効: ブロック」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Microsoft Defender ウイルス対策\Windows Defender Exploit Guard\ネットワーク保護\ユーザーとアプリが危険な Web サイトにアクセスするのを防ぎます	未構成	有効: ブロック
18.10.43.10.2	「すべてのダウンロードファイルと添付ファイルをスキャンする」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Microsoft Defender ウイルス対策\リアルタイム保護\すべてのダウンロードファイルと添付ファイルをスキャンする	未構成	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
18.10.43.10.3	「リアルタイム保護を無効にする」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Microsoft Defender ウイルス対策\リアルタイム保護\リアルタイム保護を無効にする	未構成	無効
18.10.43.10.4	「動作の監視を有効にする」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Microsoft Defender ウイルス対策\リアルタイム保護\動作の監視を有効にする	未構成	有効
18.10.43.10.5	「スクリプトのスキャンを有効にする」が「使用可能」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Microsoft Defender ウイルス対策\リアルタイム保護\スクリプトのスキャンを有効にします。	未構成	有効
18.10.43.13.3	「リムーバブルドライブのスキャン」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Microsoft Defender ウイルス対策\スキャン\リムーバブル ドライブをスキャンする	未構成	有効
18.10.43.13.5	「電子メールスキャンを有効にする」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Microsoft Defender ウイルス対策\スキャン\電子メールのスキャンを有効にする	未構成	有効
18.10.43.16	「望ましくない可能性のあるアプリケーションの検出を構成する」が「有効: ブロック」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Microsoft Defender ウイルス対策\望ましくない可能性のあるアプリケーションの検出を構成する	未構成	有効: ブロック
18.10.57.2.2	「パスワードの保存を許可しない」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\リモート デスクトップ サービス\リモート デスクトップ接続のクライアント\パスワードの保存を許可しない	未構成	有効
18.10.57.3.3.3	「ドライブのリダイレクトを許可しない」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\リモート デスクトップ サービス\リモート デスクトップ セッション ホスト\デバイスとリソースのリダイレクト\ドライブのリダイレクトを許可しない	未構成	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
18.10.57.3.9.1	「接続するたびにパスワードを要求する」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\リモート デスクトップ サービス\リモート デスクトップ セッション ホスト\セキュリティ\接続するたびにパスワードを要求する	未構成	有効
18.10.57.3.9.2	「セキュリティで保護された RPC 通信を要求する」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\リモート デスクトップ サービス\リモート デスクトップ セッション ホスト\セキュリティ\セキュリティで保護された RPC 通信を要求する	未構成	有効
18.10.57.3.9.3	「リモート (RDP) 接続に特定のセキュリティレイヤーの使用を必要とする」が「有効: SSL」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\リモート デスクトップ サービス\リモート デスクトップ セッション ホスト\セキュリティ\リモート (RDP) 接続に特定のセキュリティレイヤーの使用を必要とする	未構成	有効：SSL
18.10.57.3.9.4	「リモート接続にネットワーク レベル認証を使用したユーザー認証を必要とする」を「有効」 に設定する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\リモート デスクトップ サービス\リモート デスクトップ セッション ホスト\セキュリティ\リモート接続にネットワーク レベル認証を使用したユーザー認証を必要とする	未構成	有効
18.10.57.3.9.5	「クライアント接続の暗号化レベルを設定する」が「有効: 高レベル」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\リモート デスクトップ サービス\リモート デスクトップ セッション ホスト\セキュリティ\クライアント接続の暗号化レベルを設定する	未構成	有効: 高レベル
18.10.57.3.11.1	「終了時に一時フォルダを削除しない」が「無効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\リモート デスクトップ サービス\リモート デスクトップ セッション ホスト\一時フォルダー\終了時に一時フォルダーを削除しない	未構成	無効
18.10.58.1	「エンクロージャのダウンロードを防止」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\RSS フィード\添付ファイルのダウンロードを禁止する	未構成	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
18.10.59.3	「暗号化されたファイルのインデックス作成を許可する」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\検索\暗号化されたファイルのインデックス作成を許可する	未構成	無効
18.10.76.2.1	「Windows Defender SmartScreen を構成します」が「有効: 警告してバイパスを回避」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows Defender SmartScreen\エクスプローラー\Windows Defender SmartScreen を構成します	未構成	有効：警告してバイパスを回避
18.10.81.1	「ユーザーによるインストール制御を有効にする」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows インストーラー\ユーザーによるインストール制御を有効にする	未構成	無効
18.10.81.2	「常にシステム特権でインストールする」が「無効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows インストーラー\常にシステム特権でインストールする	未構成	無効
18.10.82.2	「再起動後に自動的に前回の対話ユーザーでサインインしてロックする」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows ログオンのオプション\再起動後に自動的に前回の対話ユーザーでサインインしてロックする	未構成	無効
18.10.89.1.1	「基本認証を許可する」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows リモート管理 (WinRM)\WinRM クライアント\基本認証を許可する	未構成	無効
18.10.89.1.2	「暗号化されていないトラフィックを許可する」が「無効」に設定されていることを確認します	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows リモート管理 (WinRM)\WinRM クライアント\暗号化されていないトラフィックを許可する	未構成	無効
18.10.89.1.3	「ダイジェスト認証を許可しない」が「有効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows リモート管理 (WinRM)\WinRM クライアント\ダイジェスト認証を許可しない	未構成	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows®	HF-W
No.	セキュリティ項目		標準設定値	設定値
18.10.89.2.1	「基本認証を許可する」が「無効」 に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows リモート管理 (WinRM)\WinRM サービス\基本認証を許可する	未構成	無効
18.10.89.2.3	「暗号化されていないトラフィックを許可する」が「無効」に設定されていることを確認します	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows リモート管理 (WinRM)\WinRM サービス\暗号化されていないトラフィックを許可する	未構成	無効
18.10.89.2.4	「WinRM で RunAs 資格情報の保存を許可しない」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows リモート管理 (WinRM)\WinRM サービス\WinRM で RunAs 資格情報の保存を許可しない	未構成	有効
18.10.92.2.1	「ユーザーが設定を変更できないようにする」が「有効」に設定されていることを確認する	コンピューターの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows セキュリティ\アプリとブラウザーの保護\ユーザーが設定を変更できないようにする	未構成	有効
19.7.40.1	「常にシステム特権でインストールする」が「無効」に設定されていることを確認する	ユーザーの構成\ポリシー\管理用テンプレート\Windows コンポーネント\Windows インストーラー\常にシステム特権でインストールする	未構成	無効