

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® 11 IoT Enterprise LTSC 2024 編)

ユーザーズ
マニュアル

2025年 9月 (第1版) W I N - 4 - 5 0 0 4 - 0 1

- このマニュアルの一部または全部を無断で転写したり複写したりすることは、固くお断りいたします。
- このマニュアルの内容を、改良のため予告なしに変更することがあります。

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
1.1 概要	1-1
1.1.1 対象機種	1-1
1.1.2 設定値記載項目	1-2
1.2 その他の設定値	1-3
第2章 設定一覧	2-1
2.1 Windows® 11 IoT Enterprise LTSC 2024	2-1

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68/65

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® 11 IoT Enterprise LTSC 2024 (64bit)	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0 – 02-22-2024	HJ-2065-WHMA	A モデル
		HJ-2065-WHMS	S モデル
		HJ-2065-WHMB	B モデル
		HJ-2065-WHMT	T モデル
		HJ-2068-WHMA	A モデル
		HJ-2068-WHMS	S モデル
		HJ-2068-WHMB	B モデル
		HJ-2068-WHMT	T モデル

- HF-W200E

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® 11 IoT Enterprise LTSC 2024 (64bit)	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0 – 02-22-2024	HJ-200E-WHMM	M 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	項目番号	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® 11 LTSC 2024
Adobe Flash Player の設定	Internet Explorer上での Adobe Flashをオフに設定する。	ユーザーの構成\管理用テンプレート\Windows コンポーネント\Internet Explorer\セキュリティ機能\アドオン管理\Internet ExplorerでAdobe Flashをオフにし、アプリケーションが Internet Explorerテクノロジを使用してFlashオブジェクトをインスタンス化できないようにする	○
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® 11 IoT Enterprise LTSC 2024

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® 標準設定値	HF-W 設定値
No.	セキュリティ項目			
2.2.2	「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、リモートデスクトップユーザー」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\ネットワーク経由でのアクセス	Everyone, Administrators, Users, Backup Operators	Administrators, Remote Desktop Users
2.2.5	「ローカルログオンを許可する」が「管理者」、「ユーザー」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\ローカルログオンを許可	Everyone, Administrators, Users, Backup Operators	Administrators, Users
2.2.7	「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	Administrators
2.2.16	「ネットワーク経由のアクセス拒否」に「ゲスト、ローカルアカウント」が含まれるようにする	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\ネットワーク経由のアクセスを拒否	Guest	Local account, Guests
2.2.17	「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(空白)	Guests
2.2.18	「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(空白)	Guests
2.2.19	「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	Guest	Guests
2.2.20	「ゲスト、ローカルアカウント」を含めるには、「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」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\リモートデスクトップサービスを介したログオンの拒否	未設定(空白)	Local account, Guests

CIS Benchmarks™		ローカルグループポリシーのパス	Windows® 標準設定値	HF-W 設定値
No.	セキュリティ項目			
2.2.37	「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	Administrators
2.2.38	「システムのシャットダウン」が「管理者」、「ユーザー」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, Users, Backup Operators	Administrators,Users
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を行う」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
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る場合は受け入れる」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\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

CIS Benchmarks™		ローカルグループポリシーのパス	Windows® 標準設定値	HF-W 設定値
No.	セキュリティ項目			
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	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
2.3.10.10	「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	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	値なし	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への PKU2U 認証要求を許可する。	未定義	無効
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)

CIS Benchmarks™		ローカルグループポリシーのパス	Windows® 標準設定値	HF-W 設定値
No.	セキュリティ項目			
2.3.11.9	「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) 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
2.3.11.10	「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) 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
2.3.11.11	「ネットワークセキュリティ: NTLM の制限: 受信 NTLM トランフィックの監査」が「すべてのアカウントの監査を有効にする」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\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 を制限する: 着信 NTLM トランフィックを監査する	未定義	すべてのアカウントに対して監査を有効にする
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」以上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	資格情報を要求する	昇格の要求を自動的に拒否する

CIS Benchmarks™		ローカルグループポリシーのパス	Windows® 標準設定値	HF-W 設定値
No.	セキュリティ項目			
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
18.6.8.1	「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
18.6.11.2	「DNS ドメインネットワーク上でのネットワークブリッジのインストールおよび構成を禁止する」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のネットワークブリッジのインストールおよび構成を禁止する	未構成	有効
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
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
18.6.23.2.1	「Windows が提案されたオープンホットスポットに自動的に接続できるようにする」、「連絡先が共有するネットワーク、有料サービスを提供するホットスポット」を「無効」に設定し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\WLAN サービス\WLAN 設定推奨されるオープンホットスポット、連絡先によって共有されたネットワーク、有料サービスを提供するホットスポットに Windows が自動的に接続することを許可する	未構成	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
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
18.9.19.2	「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」に設定し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」に設定し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)
18.9.19.4	「セキュリティポリシー処理の構成: 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」に設定し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\グループポリシー\セキュリティ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)

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
18.9.19.5	「セキュリティ ポリシー処理の構成: グループ ポリシー オブジェクトが変更されていない場合でも処理する」が「有効: TRUE」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\グループ ポリシー\セキュリティ 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)
18.9.20.1.2	「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
18.9.20.1.6	「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
18.9.28.1	「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
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ー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	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

CIS Benchmarks™		ローカルグループポリシーのパス	Windows® 標準設定値	HF-W 設定値
No.	セキュリティ項目			
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
18.9.33.6.1	「接続-スタンバイ (バッテリ) 中にネットワーク接続を許可する」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\システム\電源の管理\スリープの設定\コネクトスタンバイ中にネットワーク接続を許可する (バッテリ使用時)	未構成	無効
18.9.33.6.2	「接続-スタンバイ中にネットワーク接続を許可する (接続中)」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\電源の管理\スリープの設定\コネクトスタンバイ中にネットワーク接続を許可する (電源接続時)	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	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
18.9.36.2	「認証されていない RPC クライアントを制限する」を「有効: 認証済み」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\システム\リモート プロシージャ コール\認証されていない RPC クライアントを制限する	未構成	有効: 認証済み
18.10.3.2	「管理者以外のユーザーによる パッケージ Windows アプリのインストールを禁止する」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\Windows コンポーネント\アプリ パッケージの展開\管理者以外のユーザーがパッケージ化された Windows アプリをインストールできないようにする	未構成	有効
18.10.4.1	「システムがロックされている間に音声で Windows アプリをアクティブにする」が「有効: 強制拒否」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\アプリのプライバシー\システムがロックされているときに音声で Windows アプリをアクティベートできるようにする	未構成	有効: 強制的に拒否

CIS Benchmarks™		ローカルグループポリシーのパス	Windows® 標準設定値	HF-W 設定値
No.	セキュリティ項目			
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
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
18.10.14.1	「[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
18.10.14.3	「ローカルアカウントのセキュリティの質問の使用を禁止する」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\Windows コンポーネント\資格情報ユーザーインターフェイス\ローカルアカウントに関するセキュリティの質問を使用できないようにする	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
18.10.15.8	「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コントロールの切り替え	未構成	無効
18.10.28.2	「エクスプローラー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

CIS Benchmarks™		ローカルグループポリシーのパス	Windows® 標準設定値	HF-W 設定値
No.	セキュリティ項目			
18.10.28.3	「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
18.10.28.4	「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
18.10.41.1	「すべてのコンシューマの Microsoft アカウントユーザー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
18.10.42.7.1	「ファイルハッシュ計算機能を有効にする」が「有効」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\Microsoft Defender ウイルス対策\MpEngine\ファイルハッシュ計算機能を有効にする	未構成	有効
18.10.56.2.3	「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
18.10.56.3.3.3	「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
18.10.56.3.9.1	「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
18.10.56.3.9.2	「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
18.10.56.3.9.3	「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

CIS Benchmarks™		ローカルグループポリシーのパス	Windows® 標準設定値	HF-W 設定値
No.	セキュリティ項目			
18.10.56.3.9.4	「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
18.10.56.3.9.5	「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
18.10.56.3.11.1	「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
18.10.58.3	「Cortana 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\検索\Cortana を許可する	未構成	無効
18.10.58.4	「ロック画面上の Cortana 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\検索\ロック画面で Cortana を許可する	未構成	無効
18.10.58.5	「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
18.10.58.6	「検索と Cortana の場所の使用を許可する」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\検索と Cortana による位置情報の使用を許可する	未構成	無効
18.10.65.2	「Microsoft Store 内のプライベートストアのみを表示する」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\ストア\Microsoft Store 内のプライベートストアのみを表示する	未構成	有効
18.10.65.4	「最新バージョンの Windows への更新のオファーを無効にする」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\ストア\最新バージョンの Windows への更新プログラム提供をオフにする	未構成	有効

CIS Benchmarks™		ローカルグループポリシーのパス	Windows® 標準設定値	HF-W 設定値
No.	セキュリティ項目			
18.10.75.2.1	「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
18.10.77.1	「Windows ゲームの録画と放送を有効または無効にする」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\Windows ゲームの録画とブロードキャスト\Windows のゲーム録画とブロードキャストを有効または無効にする	未構成	無効
18.10.80.1	「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
18.10.80.2	「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
18.10.81.2	「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
18.10.88.1.1	「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
18.10.88.1.2	「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
18.10.88.1.3	「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
18.10.88.2.1	「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

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
18.10.88.2.3	「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
18.10.88.2.4	「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
18.10.91.2.1	「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
19.7.42.1	「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