WIN-4-5001-02

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

ユーザーズガイド

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

WIN-4-5001-02

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

ユーザーズガイド

マニュアルはよく読み、保管してください。
• 操作を行う前に、安全上の指示をよく読み、十分理解してください。 • このマニュアルは、いつでも参照できるよう、手近なところに保管してください。

２０２５年　５月　（第１版）　ＷＩＮ－４－５００１－０１
２０２５年　９月　（第２版）　ＷＩＮ－４－５００１－０２

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 シリーズのセキュリティ対策の設定内容とその変更方法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　装置出荷時のセキュリティ設定と変更方法

第３章　セキュリティ設定による影響と対処方法

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®、Windows Server®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

はじめに i

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　HF-Wシリーズ、HF-W/IoTシリーズのセキュリティ対策について 1-1

１．１．１　セキュリティ対策の概要 1-1

１．１．２　セキュリティ対策の方針 1-2

１．１．３　セキュリティ対策に対するユーザーの対応 1-3

１．１．４　セキュリティ対策の設定値 1-4

１．２　CIS Benchmarks™ 1-4

１．２．１　CIS Benchmarks™ のプロファイル 1-4

１．３　グループポリシー 1-5

１．３．１　ローカルグループポリシーエディター 1-5

第２章　装置出荷時のセキュリティ設定と変更方法 2-1

２．１　HF-Wのセキュリティ設定 2-1

２．１．１　装置出荷時のセキュリティ設定 2-1

２．２　ユーザーによるセキュリティ設定の変更 2-2

２．２．１　ローカルグループポリシーエディターによる設定変更 2-2

第３章　セキュリティ設定による影響と対処方法 3-1

３．１　セキュリティ設定による影響 3-1

３．２　セキュリティ設定への対処方法 3-3

３．２．１　リモートデスクトップを使用する 3-3

３．２．２　リモートデスクトップでファイルコピーを行う 3-7

３．２．３　共有フォルダへのアクセスを許可する 3-9

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　HF-W シリーズ、HF-W/IoT シリーズのセキュリティ対策について

近年、高度化・巧妙化するサイバー攻撃や、クラウドサービスにおけるユーザー設定の不備等を原因としたセキュリティの脅威が増加し続けており、情報システム全体を安全に維持管理しておく重要性が高まっています。

HF-Wシリーズ、およびHF-W/IoTシリーズにおいても、プロトコルに脆弱性が存在し、マルウェアへの感染等により機能停止に至る可能性があります。

HF-Wシリーズ、およびHF-W/IoTシリーズでは、ユーザーが安全に構築・使用いただくため、装置を工場から出荷する際にセキュリティ対策を行っています。

なお、これ以降、「HF-W」の表記は「HF-Wシリーズ」、「HF-W/IoTシリーズ」を含むものとします。

■ HF-Wのセキュリティ対策については、下記のホームページに記載があります。

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

１．１．１　セキュリティ対策の概要

HF-Wのセキュリティ対策は、Microsoft®社が標準で用意しているセキュリティ対策に加えて、Microsoft®社も自社製品のセキュリティ向上施策として推奨しているCIS Benchmarks™（*1）ガイドラインに記載のセキュリティ対策推奨値に対し、「HF-Wのセキュリティ対策方針」に従い、セキュリティ対策推奨値に変更する項目を判断しています。

セキュリティ設定値は、Windows®標準のセキュリティオプション設定ツールであるローカルグループポリシーエディター（gpedit.msc）を使用して、ユーザーによる変更が可能です。

（*1）：詳細については本書「１．２ CIS Benchmarks™」を参照してください。

１．１．２　セキュリティ対策の方針

CIS Benchmarks™ガイドラインのセキュリティ対策推奨値を全て適用すると、セキュリティの強化がユーザーの資産である従来機能や、運用の機能低下を招き、使い勝手に影響を与える可能性があります。そのため、HF-Wでは「HF-Wのセキュリティ対策方針」によりセキュリティ対策とユーザーの使い勝手のバランスを考慮した設定内容とします。

CIS Benchmarks™ガイドラインの推奨値に対して以下の方針により設定項目を判断します。

・HF-Wのセキュリティ対策方針
（1）当該機能の利用が、セキュリティ観点上、リスクを許容することが困難である。 （2）当該機能の利用に対して、攻撃者による攻撃の可能性が高い。 （3）当該機能の利用を制限することにより、ユーザーによる運用や利便性に支障がない。

・「HF-Wのセキュリティ対策方針」による設定項目判断の例

No	CIS Benchmarks™ セキュリティ項目	該当するセキュリティ対策方針	判断結果
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」に設定されていることを確認する。	（1）誰でも共有フォルダ内のファイルを読み取ることができてしまうため、セキュリティ観点上、リスクを許容することが困難である。	設定する
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。	（2）ユーザー権限を、正当なユーザーに制限しないと、権限のないユーザーが悪意のあるソフトウェアをダウンロードして実行し、権限を昇格させる可能性があります。	設定する
1.1.3	「パスワードの最低有効期間」 が 「1 日以上」に設定されていることを確認する。	（3）パスワードの更新が頻繁になり、利便性に支障をきたす。	設定しない

１．１．３　セキュリティ設定に対するユーザーの対応

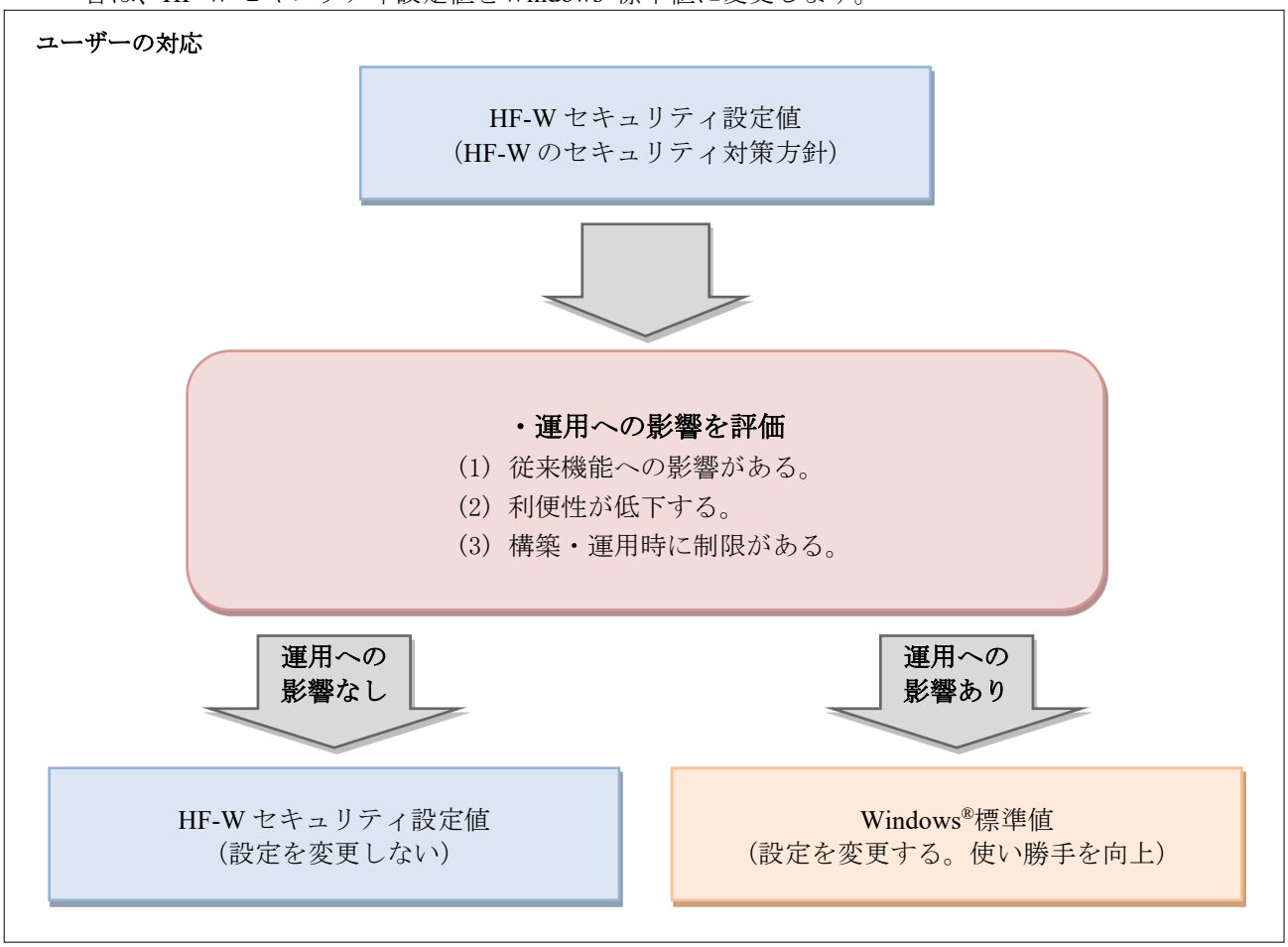
HF-Wのセキュリティ設定は、ローカルグループポリシーエディターを使用して変更が可能です。

HF-Wのセキュリティ対策が全てのユーザーにとって最善であるとは限らず、ユーザーの資産である従来機能の動作、システムの運用、操作の利便性などで機能低下を招き、構築・運用時の使い勝手に影響を与える可能性があります。この場合、セキュリティ設定をWindows®標準値に変更し、使い勝手を向上させてください。

また、外部からの攻撃に対して想定される被害の大きさ、攻撃の可能性など、ご使用環境に応じた“リスク評価”をユーザーが行い、セキュリティ対策の強化が必要と想定される場合、Windows®のセキュリティ設定を強化する必要があります。

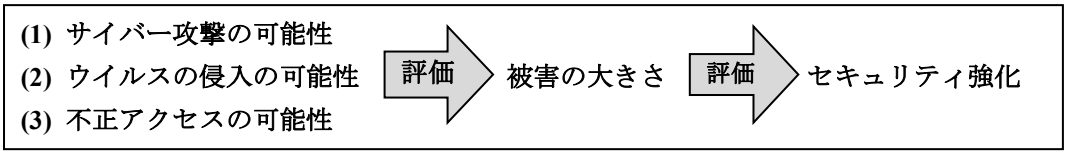
(1) ユーザーに対応していただく、セキュリティ設定変更の判断フロー

HF-W セキュリティ設定値が構築・運用時の使い勝手に影響を与えるか評価を行い、影響がある場合は、HF-W セキュリティ設定値をWindows®標準値に変更します。



(2) リスク評価

使用環境に応じた“リスク評価”を行い、セキュリティ対策の強化が必要な場合、セキュリティ設定値を変更します。



１．１．４　セキュリティ対策の設定値

HF-Wのセキュリティ対策で行う設定値は、プレインストールOSによって異なります。当該機種のプレインストールOSの設定一覧を参照してください。

プレインストール OS	HF-Wシリーズ	設定一覧	マニュアル番号
Windows® 10 IoT Enterprise 2021 LTSC（64bit）	HF-W2000 モデル 68/65	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® 10 IoT Enterprise 2021 LTSC 編）	WIN-4-5002-01
Windows Server® IoT 2022 Standard（64bit）	HF-W2000 モデル 68/65	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 2022 Standard 編）	WIN-4-5003-01
Windows® 11 IoT Enterprise LTSC 2024（64bit）	HF-W2000 モデル 68/65, HF-W200E	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）	WIN-4-5004-01
Windows Server® IoT 2025 Standard（64bit）	HF-W2000 モデル 68/65	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）	WIN-4-5005-01

「設定一覧」は、Windows® OSの標準設定値から変更したセキュリティ項目と、設定値を記載しています。

１．２　CIS Benchmarks™

Center for Internet Security（CIS）は米国の州、地方、政府機関のサイバー攻撃の防御、対応、回復を担うMulti-State Information Sharing and Analysis Center（MS-ISAC）と、選挙事務所や選挙インフラシステムのサーバーセキュリティを担うElections Infrastructure Information Sharing and Analysis Center（EI-ISAC）の運用を行っている2000年に設立された米国の非営利団体です。

CIS Benchmarks™ はCISが作成したサイバーセキュリティのベストプラクティスです。

ソリューションの開発、展開、評価、またはセキュリティ保護を計画しているユーザーを対象としており、安全なベースライン構成を確立するための規範的なガイダンスを提供します。

Microsoft®社製品およびサービスのベンチマークを公開しており、Microsoft®社は自社製品のセキュリティ向上施策として CIS Benchmarks™ を推奨しています。

１．２．１　CIS Benchmarks™ のプロファイル

CIS Benchmarks™ は、異なるレベルのセキュリティを提供するプロファイルレベルがあります。

・レベル１プロファイル（L1）

あらゆるシステムで構成でき、サービスの中断や機能の低下を引き起こさない、不可欠となる基本セキュリティ要件を推奨しています。

・レベル２プロファイル（L2）

機能の低下を引き起こす可能性のある、より高度なセキュリティを必要とする環境向けのセキュリティ設定を推奨しています。

HF-Wのセキュリティ対策設定値は、ユーザーの使い勝手やパフォーマンスへの影響が少ない レベル１プロファイル（L1）をベースに「１．１．２　セキュリティ対策の方針」に従いセキュリティ対策項目を選定しています。

１．３　グループポリシー

グループ ポリシーは、Microsoft®社の提供するユーザーやコンピュータに対する設定を管理するためのActive Directory ドメインサービスにおけるポリシー設定です。

ポリシー設定は、コンピュータに影響を与えるポリシー設定と、ユーザーに影響を与えるポリシー設定に分かれていて、システム設定やセキュリティ設定（グループポリシー）ができます。

１．３．１　ローカルグループポリシーエディター

Active Directory ドメインサービスは、ネットワーク内のコンピュータや利用者アカウントを一括して管理することができますが、同じ仕組みを個別のコンピュータや利用者アカウントに内部で利用できるようにしたのがローカルグループポリシーエディター（gpedit.msc）です。

HF-Wのセキュリティ設定は、ローカルグループポリシーエディター（gpedit.msc）を使用して変更可能です。変更方法は、「第２章　装置出荷時のセキュリティ設定と変更方法」を参照してください。

第２章　装置出荷時のセキュリティ設定と変更方法

２．１　HF-Wのセキュリティ設定

２．１．１　装置出荷時のセキュリティ設定

装置出荷時にWindows® OSの標準設定値から変更したセキュリティ設定内容については、「１．１．４　セキュリティ対策の設定値」に記載の当該機種のプレインストールOSの設定一覧を参照してください。

変更したセキュリティ項目に関する説明、設定変更の根拠は、CIS Benchmarks™ ガイドラインに記載があります。

CIS Benchmarks™ ガイドラインは次のサイトからユーザー登録を行うことで、無料でダウンロードすることができます。

https://www.cisecurity.org/cis-benchmarks/

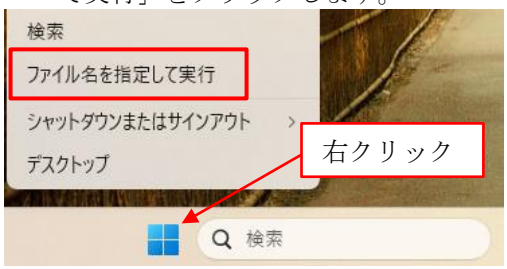
２．２　ユーザーによるセキュリティ設定の変更

HF-Wのセキュリティ設定は、ユーザーの運用の用途によりセキュリティ強化や使い勝手の向上を図るためにユーザーにより「ローカルグループポリシーエディター（gpedit.msc）」を使用して変更することが可能です。

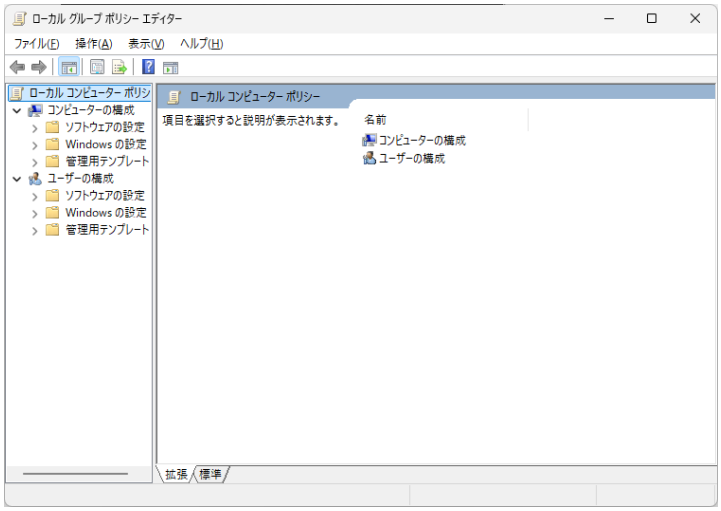
「ローカルグループポリシーエディター（gpedit.msc）」を使用してセキュリティ設定の変更方法を記載します。

２．２．１　ローカルグループポリシーエディターによる設定変更方法

（1）デスクトップ画面下に配置されているスタートボタンを右クリックし「ファイル名を指定して実行」をクリックします。

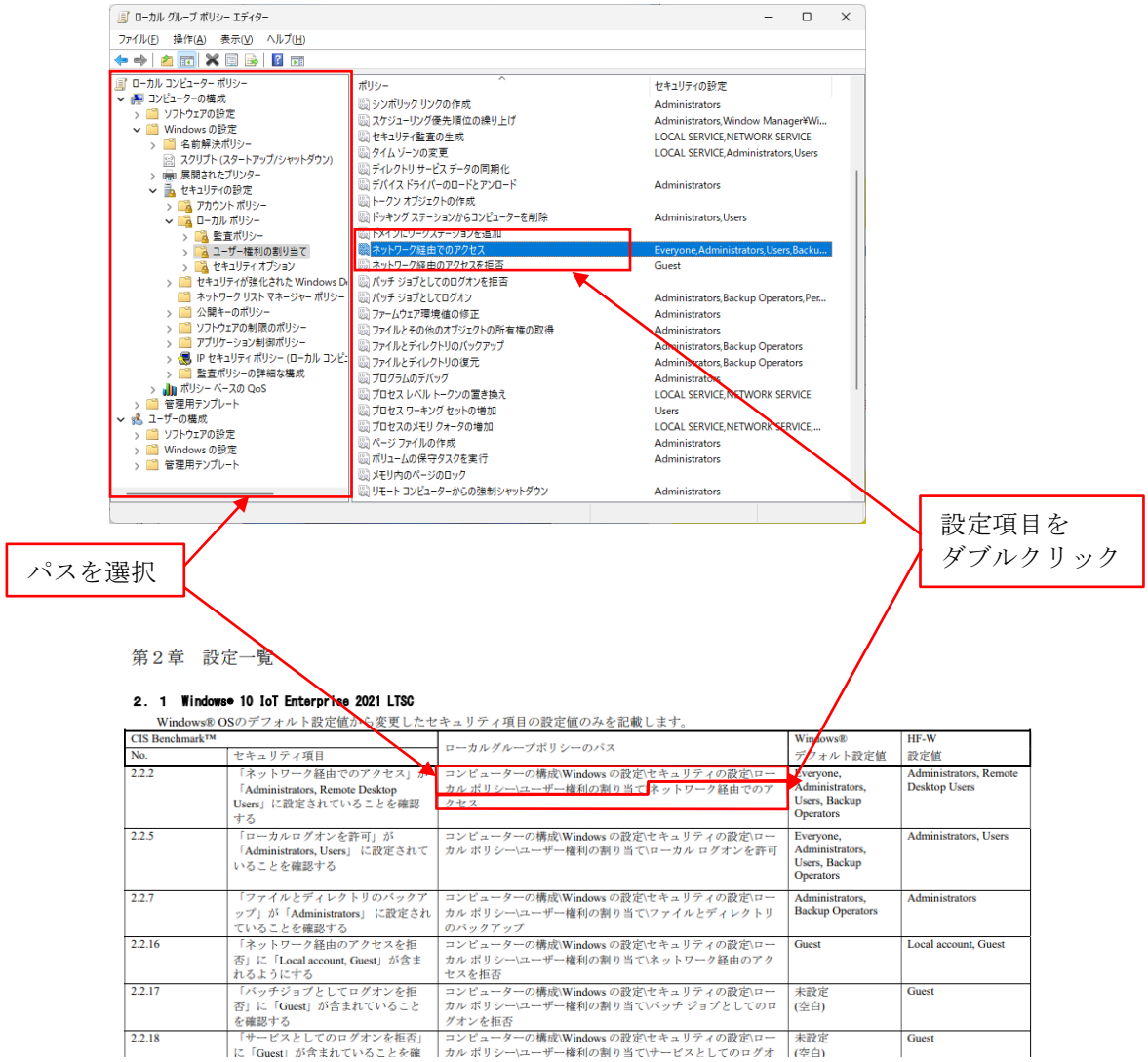


（2）「ファイル名を指定して実行」画面で「**gpedit.msc**」と入力してローカルグループポリシーエディターを起動します。



ユーザーアカウント制御（UAC）が有効な場合は、確認ダイアログが表示されます。確認メッセージで［はい］ボタンをクリックします。

（３）別冊「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」第２章 設定一覧の「ローカルグループポリシーのパス」欄に記載のパスがローカルグループポリシーエディターの項目ツリーと対応します。
変更する項目のパスをローカルグループポリシーエディター画面からたどり、設定項目を選択し、ダブルクリックします。



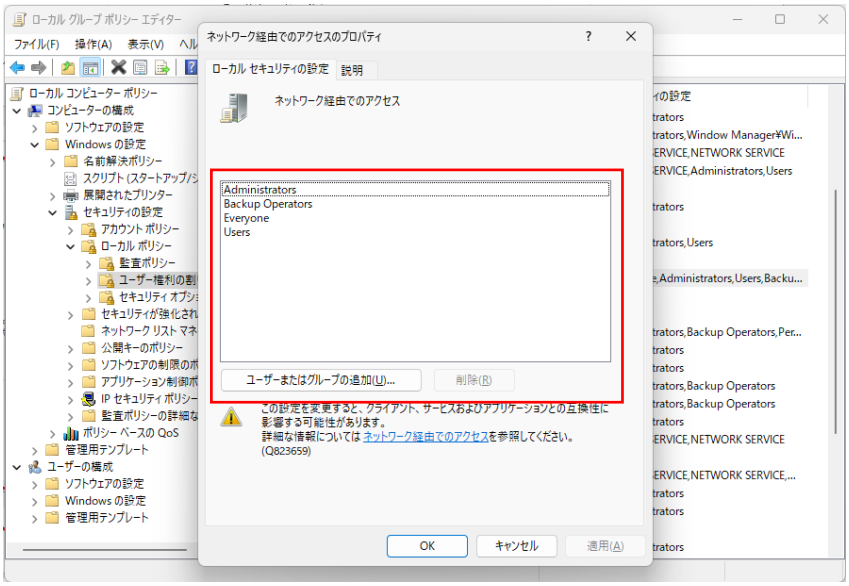
第２章　設定一覧

２．１　Windows® 10 IoT Enterprise 2021 LTSC

Windows® OSのデフォルト設定値から変更したセキュリティ項目の設定値のみを記載します。

CIS Benchmark™ No.	セキュリティ項目	ローカルグループポリシーのパス	Windows® デフォルト設定値	HF-W 設定値
2.2.2	「ネットワーク経由でのアクセス」が「Administrators, Remote Desktop Users」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\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」が「Administrators, Users」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\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「Administrators」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\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を拒否」に「Local account, Guest」が含まれるようにする	コンピューターの構成\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, Guest
2.2.17	「バッチジョブとしてログオンを拒否」に「Guest」が含まれていることを確認する	コンピューターの構成\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)	Guest
2.2.18	「サービスとしてのログオンを拒否」に「Guest」が含まれていることを確	コンピューターの構成\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	未設定 (空白)	Guest

（４）設定画面が表示されます。設定を変更し、「OK」をクリックします。



（５）設定を変更する項目分、（５）、（６）を繰り返します。

（６）設定変更が完了したら、ローカルグループポリシーエディターを閉じて、HF-Wを再起動してください。

（７）HF-Wを再起動後、ローカルグループポリシーエディターを再び起動して、設定変更が反映されていることを確認してください。

第３章　セキュリティ設定による影響と対処方法

３．１　セキュリティ設定による影響

HF-Wシリーズのセキュリティ設定により使用が制限されるWindows®機能があります。

本項では、使用が制限されるWindows®機能のなかで代表的なものについて、HF-Wシリーズのセキュリティ設定項目とその設定値を示します。

これらの機能は、セキュリティ設定をWindows®標準設定に変更することで使用可能になります。

・セキュリティ設定を変更する手順については、３．２項をご参照ください。

・セキュリティ設定の変更は、セキュリティリスクを考慮したうえで実施してください。

（1）リモートデスクトップを使用する

リモートデスクトップは接続先のコンピュータに操作の権限が与えられてしまい、サイバー攻撃の標的となりやすいため、HF-Wシリーズではリモートデスクトップが可能なユーザー権限を設定し、管理者以外の接続を許可しない設定にしています。

No	セキュリティ設定項目	OS（*1）		設定値	
		Win10, Win11	Srv2022, Srv2025	HF-Wセキュリティ設定	Windows®標準設定
1	ネットワーク経由のアクセスを拒否	●	－	Guests, ローカルアカウント	Guest
		－	●	Guests, ローカルアカウントと Administrators グループのメンバー	Administrator
2	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	●	●	Guests, ローカルアカウント	未設定

（2）リモートデスクトップでファイルコピーを行う

リモートデスクトップサービスセッションから、悪意のあるソフトウェア・データの転送や、ステルス的にディスクアクセスが行われる可能性があるため、HF-Wシリーズではドライブへのリダイレクトを許可しない設定にしています。

No	セキュリティ設定項目	OS（*1）		設定値	
		Win10, Win11	Srv2022, Srv2025	HF-Wセキュリティ設定	Windows®標準設定
1	ドライブのリダイレクトを許可しない	●	●	有効	未構成

（3）共有フォルダへのアクセスを許可する

共有フォルダには、意図しない相手に情報を共有してしまうリスクや、ウイルス感染による情報漏えいのリスクなどがあるため、HF-Wシリーズでは、ゲストログオンを許可しない設定にしています。

No	セキュリティ設定項目	OS（*1）		設定値	
		Win10, Win11	Srv2022, Srv2025	HF-Wセキュリティ設定	Windows®標準設定
1	安全でないゲストログオンを有効にする	●	●	無効	有効
2	ネットワーク経由のアクセスを拒否	●	－	Guests, ローカルアカウント	Guest
		－	●	Guests, ローカルアカウントと Administrators グループのメンバー	未設定
3	ネットワーク経由でのアクセス	●	●	Windows標準値	Everyone（*2）
4	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	●	●	有効	無効
5	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	●	●	有効	無効
6	リアルタイム保護を無効にする	－	●	無効	未構成

（*1）●：該当、－：非該当、

Win10：Windows® 10 IoT Enterprise 2021 LTSC、

Win11：Windows® 11 IoT Enterprise LTSC 2024、

Srv2022：Windows Server® IoT 2022 Standard、

Srv2025：Windows Server® IoT 2025 Standard

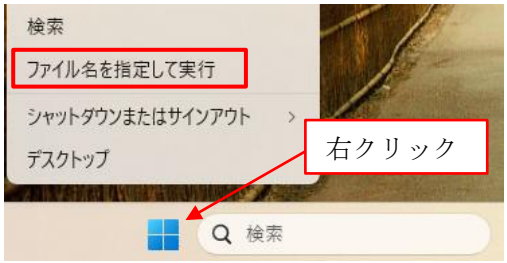
（*2）追加するユーザー/グループは必要に応じて変更してください。

３．２　セキュリティ設定への対処方法

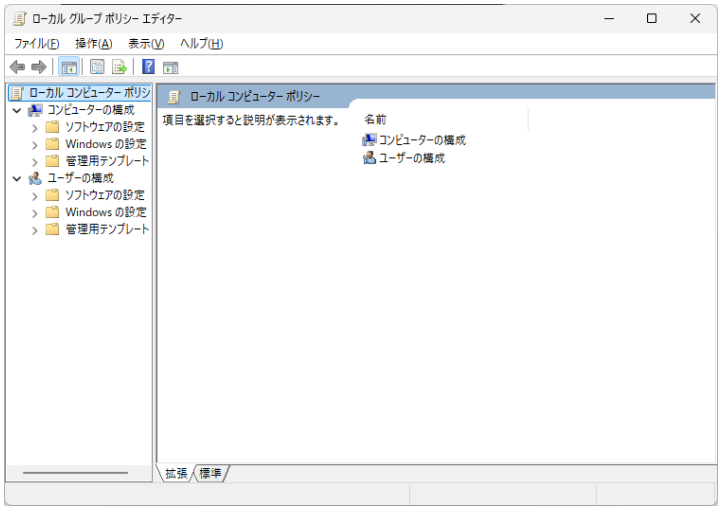
３．２．１　リモートデスクトップを使用する

（１）リモートデスクトップを使用するためのセキュリティ設定手順

① デスクトップ画面下に配置されているスタートボタンを右クリックし「ファイル名を指定して実行」をクリックします。

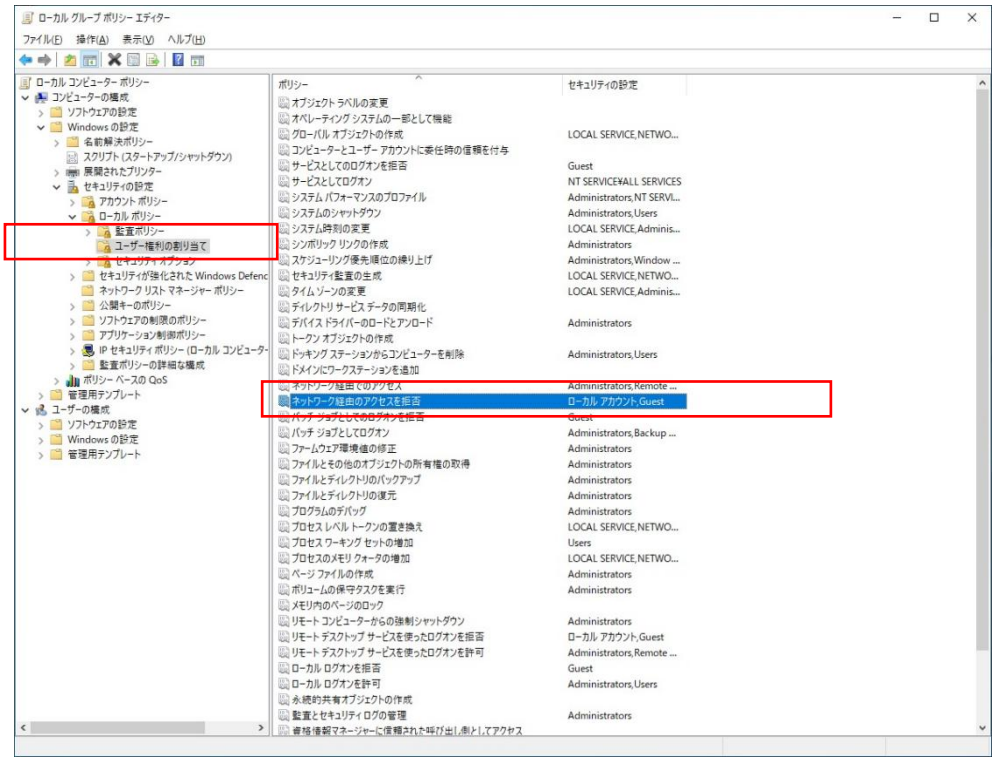


②「ファイル名を指定して実行」画面で「**gpedit.msc**」と入力してローカルグループポリシーエディターを起動します。



ユーザーアカウント制御（UAC）が有効な場合は、確認ダイアログが表示されます。確認メッセージで［はい］ボタンをクリックします。

③ 左側の項目ツリーから[コンピューターの構成]-[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] を選択し、右側の項目の「ネットワーク経由のアクセスを拒否」をダブルクリックしてください。

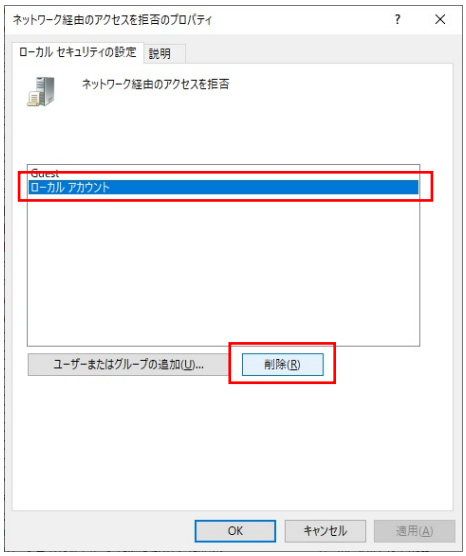


④ 設定に対して以下の操作を行ってください。

<Windows® 10 IoT 2021 LTSC, Windows® 11 IoT LTSC 2024 の場合>

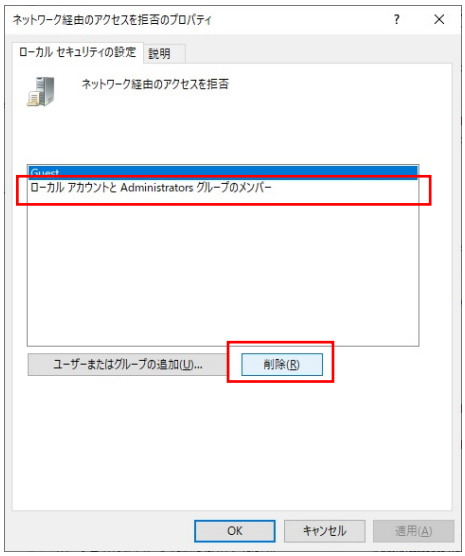
・"ローカルアカウント"を選択し、[削除(R)] ボタンをクリックしてください。

・"ローカルアカウント"を削除後に、[OK]ボタンをクリックしてください。

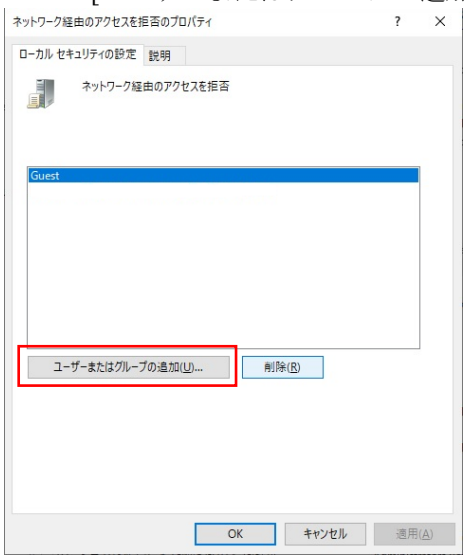


<Windows Server® IoT 2022, Windows Server® IoT 2025 の場合>

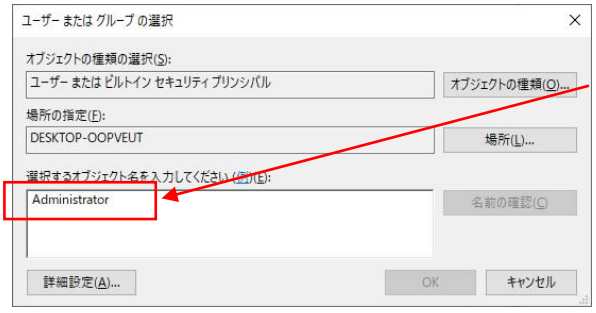
・"ローカルアカウントと Administrators グループのメンバー"を選択し、[削除(R)] ボタンをクリックしてください。



・[ユーザーまたはグループの追加(U)…]ボタンをクリックしてください。



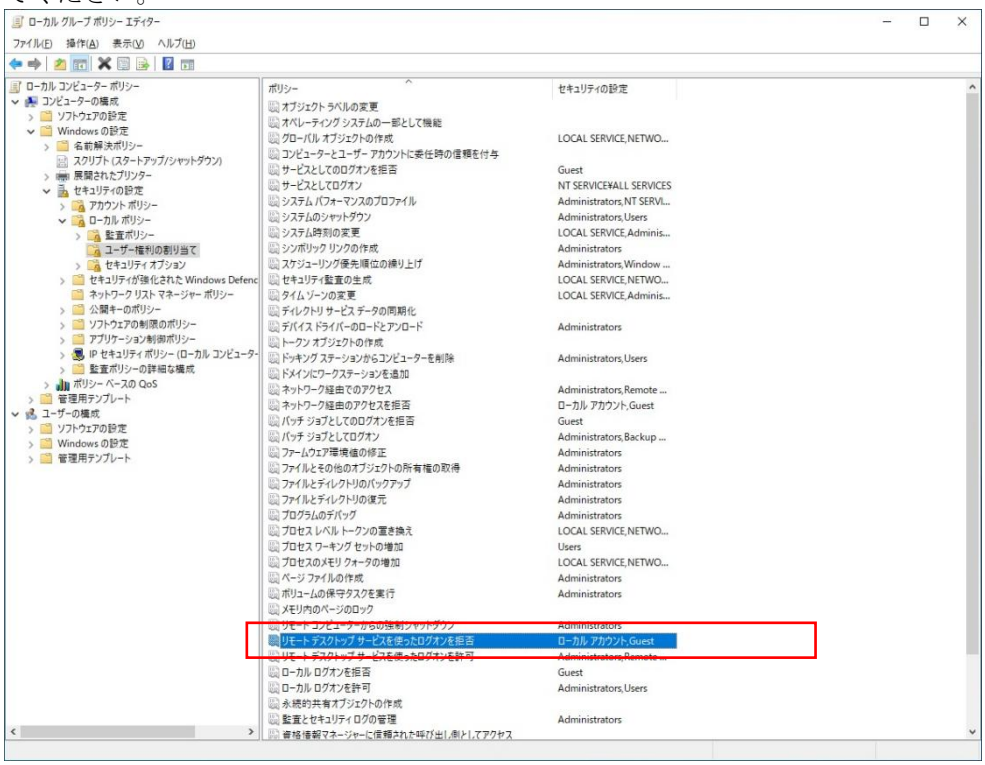
・[選択するオブジェクト名を入力してください(例)(E):]に"Administrator "を入力し、[OK]ボタンをクリックしてください。



「Administrator」を入力

・「ネットワーク経由のアクセスを拒否プロパティ」で"Administrator"を追加後に、[OK]ボタンをクリックしてください。

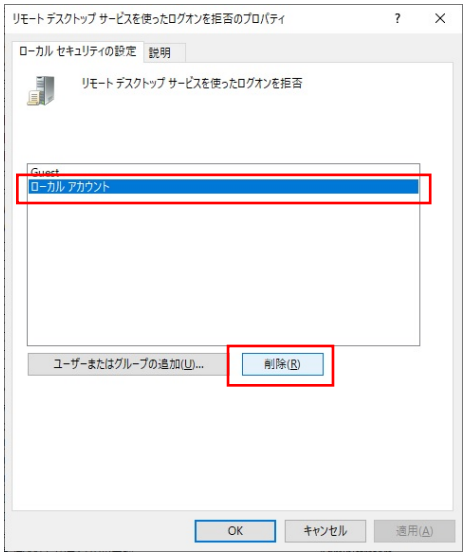
⑤ 右側の項目の「リモートデスクトップサービスを使ったログオンを拒否」をダブルクリックしてください。



⑥ 一覧に対して以下の操作を行ってください。

・"ローカルアカウント"を選択し、[削除(R)] ボタンをクリックしてください。

・"ローカルアカウント"を削除後に、[OK]ボタンをクリックしてください。



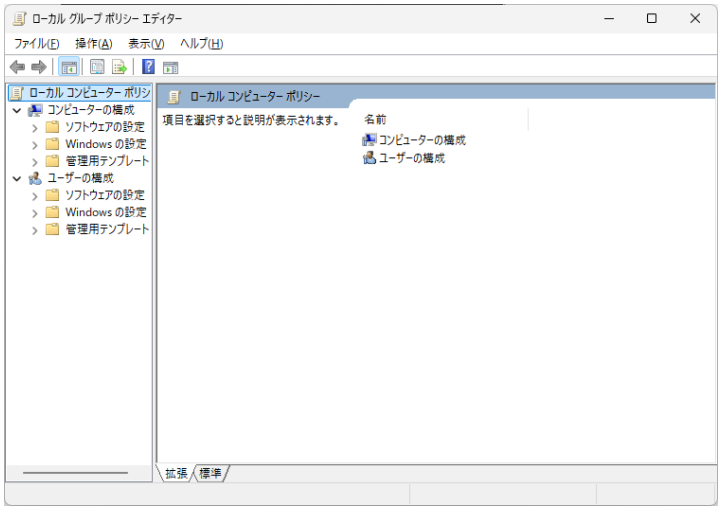
⑦ ローカルグループポリシーエディターを終了し、HF-Wを再起動してください。

３．２．２　リモートデスクトップでファイルコピーを行う

（１）リモートデスクトップでファイルコピーを行うための設定手順

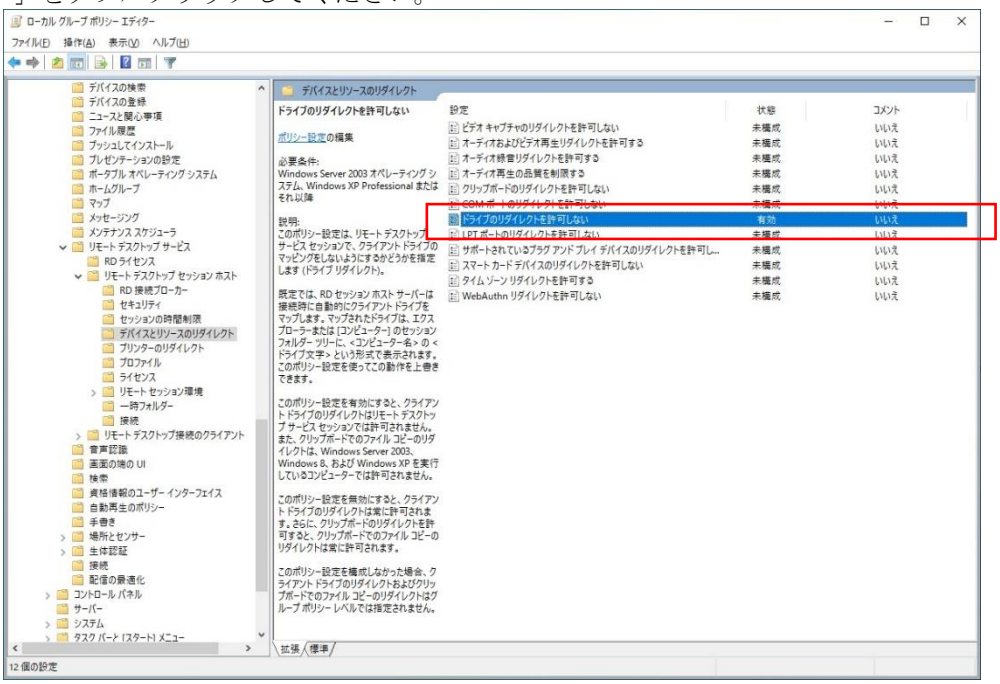
①デスクトップ画面下に配置されているスタートボタンを右クリックし「ファイル名を指定して実行」をクリックします。

②「ファイル名を指定して実行」画面で「**gpedit.msc**」と入力してローカルグループポリシーエディターを起動します。

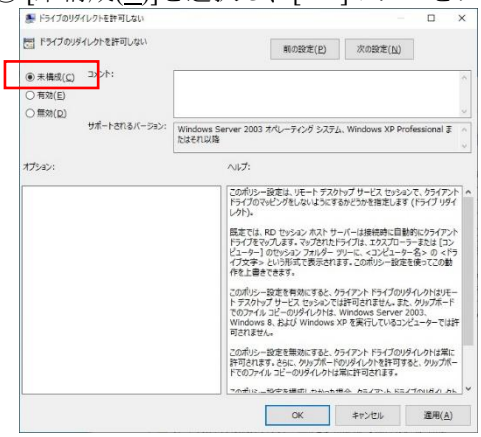


ユーザーアカウント制御（UAC）が有効な場合は、確認ダイアログが表示されます。確認メッセージで［はい］ボタンをクリックします。

③ 左側の項目ツリーから[コンピューターの構成]-[Windowsの設定]-[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]を選択し、右側の項目の「ドライブのリダイレクトを許可しない」をダブルクリックしてください。



④ [未構成(C)]を選択し、[OK]ボタンをクリックしてください。



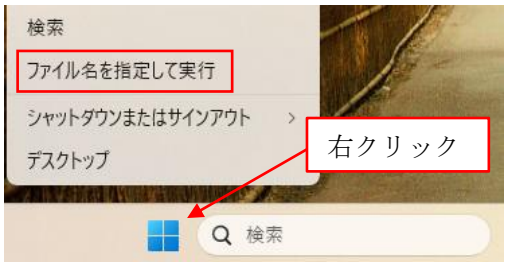
⑤ ローカルグループポリシーエディターを終了し、HF-W を再起動してください。

３．２．３　共有フォルダへのアクセスを許可する

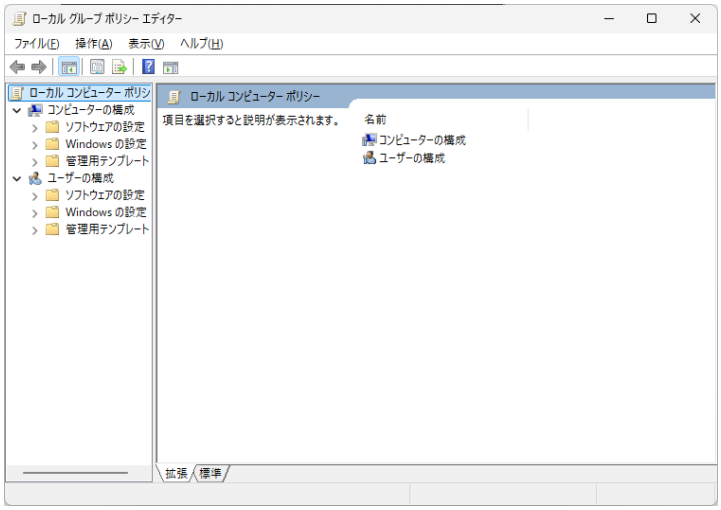
（1）共有フォルダへのアクセスを許可するための設定手順

＜ローカルグループポリシーの設定変更＞

① デスクトップ画面下に配置されているスタートボタンを右クリックし「ファイル名を指定して実行」をクリックします。

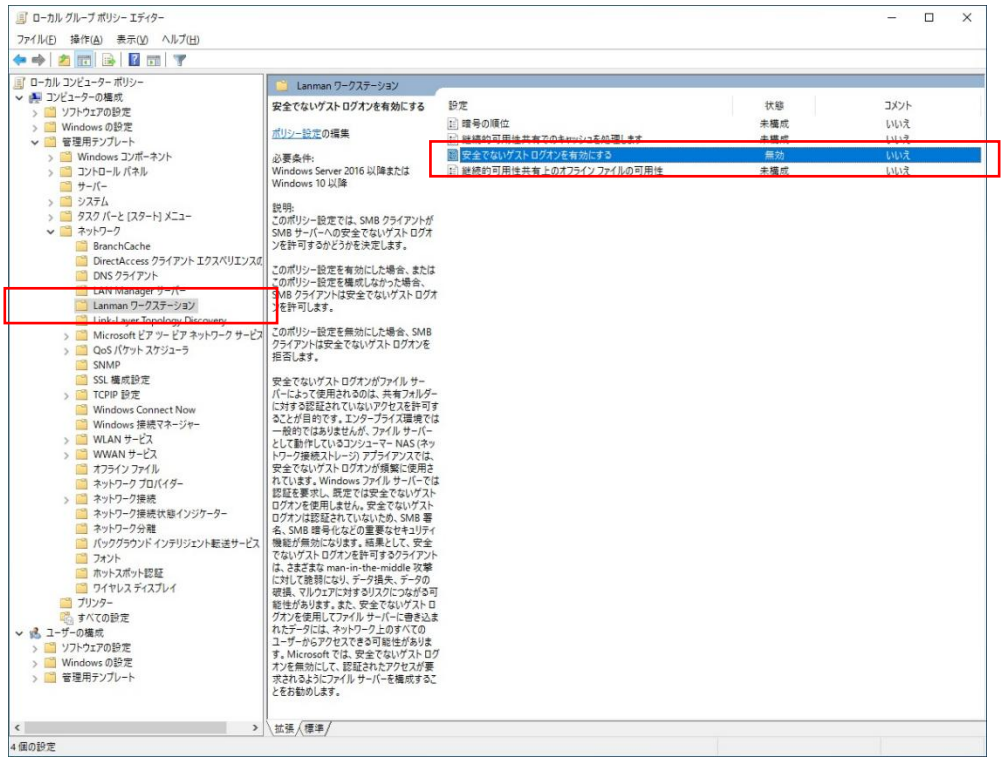


②「ファイル名を指定して実行」画面で「**gpedit.msc**」と入力してローカルグループポリシーエディターを起動します。

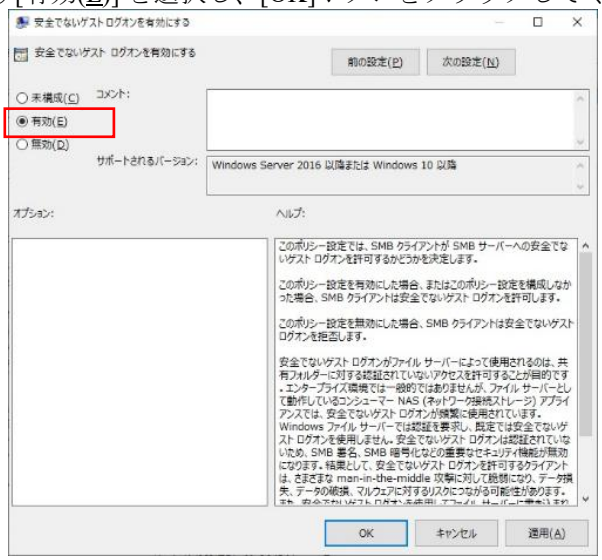


ユーザーアカウント制御（UAC）が有効な場合は、確認ダイアログが表示されます。確認メッセージで［はい］ボタンをクリックします。

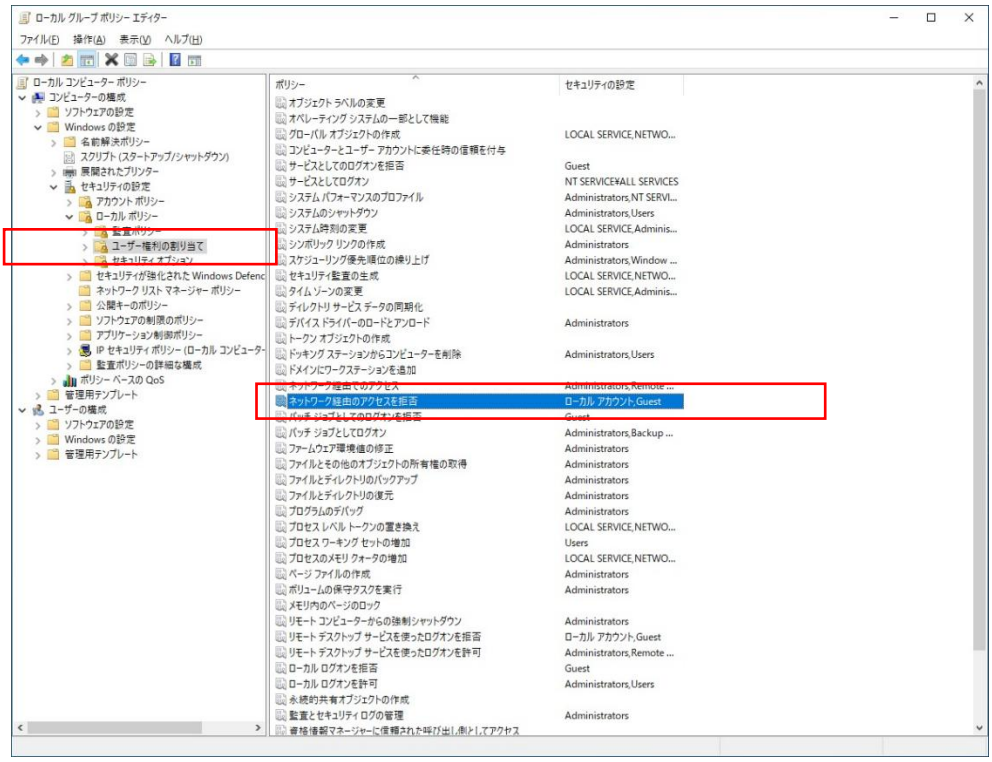
③ 左側の項目ツリーから[コンピューターの管理]-[管理用テンプレート]-[ネットワーク]-[Lanmanワークステーション] を選択し、右側の項目の「安全でないゲストログオンを有効にする」をダブルクリックしてください。



④ [有効(E)] を選択し、[OK]ボタンをクリックしてください。



⑤ 左側の項目ツリーから[コンピューターの構成]-[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] を選択し、右側の項目の「ネットワーク経由のアクセスを拒否」をダブルクリックしてください。

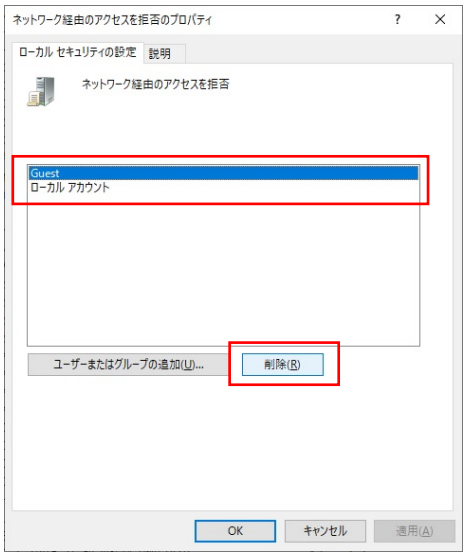


⑥ 設定に対して以下の操作を行ってください。

<Windows® 10 IoT 2021 LTSC, Windows® 11 IoT LTSC 2024の場合>

・"ローカルアカウント"を選択し、[削除(R)] ボタンをクリックしてください。

・"ローカルアカウント"を削除後に、[OK]ボタンをクリックしてください。

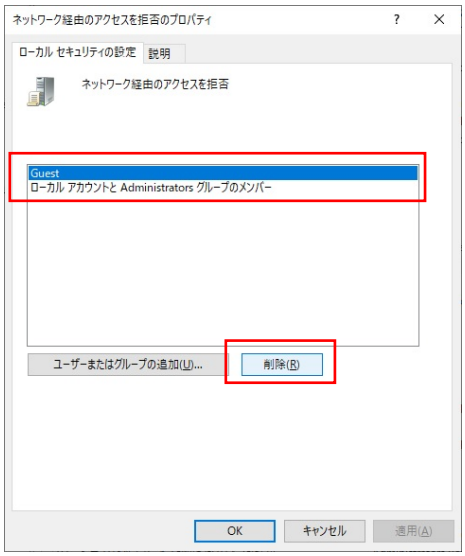


<Windows Server® IoT 2022, Windows Server® IoT 2025 の場合>

・"Guests"を選択し、[削除(R)] ボタンをクリックしてください。

・"ローカルアカウントとAdministrators グループのメンバー"を選択し、[削除(R)] ボタンをクリックしてください。

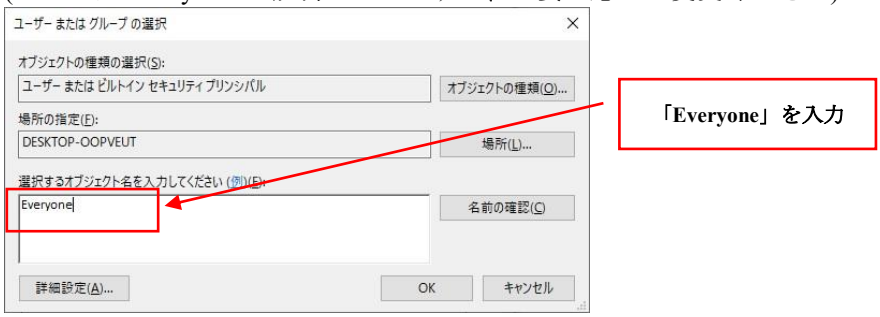
・"Guests"と"ローカルアカウントと Administrators グループのメンバー"を削除後に、[OK]ボタンをクリックしてください。



⑦ 右側の項目の「ネットワーク経由でのアクセス」をダブルクリックしてください。

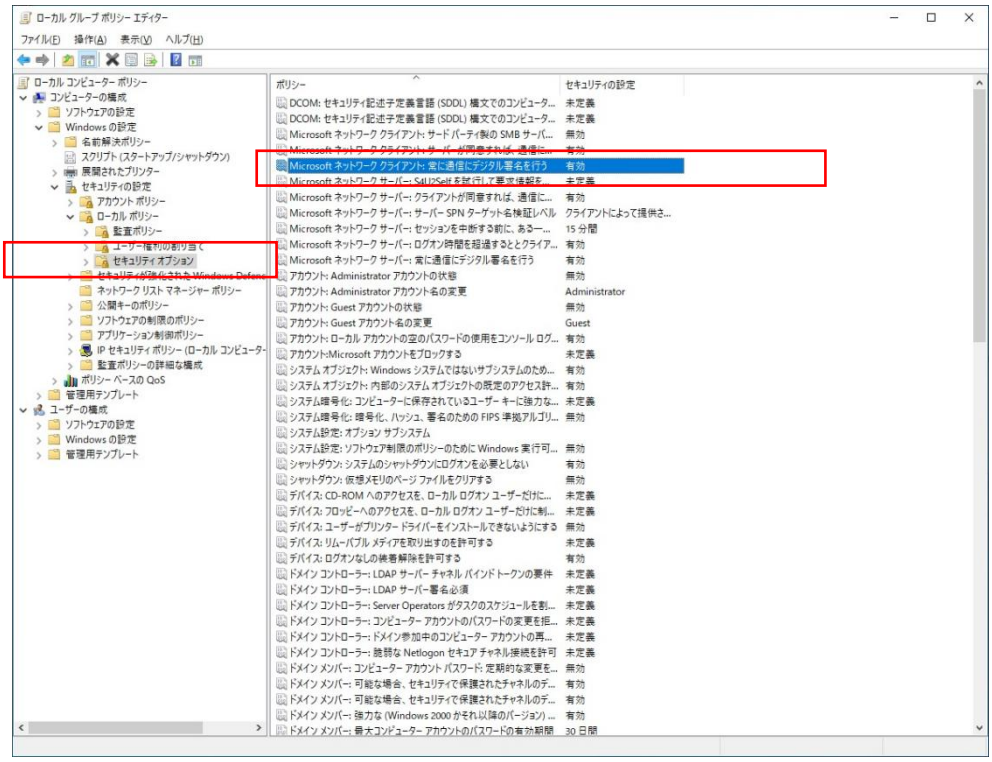
「ネットワーク経由でのアクセスのプロパティ」の、[ユーザーまたはグループの追加(U)...]ボタンをクリックしてください。

⑧ [選択するオブジェクト名を入力してください(例)(E):]に"Everyone"を入力し、[OK]ボタンをクリックしてください。
(ここでは"Everyone"で説明していますが、必要に応じて変更ください)

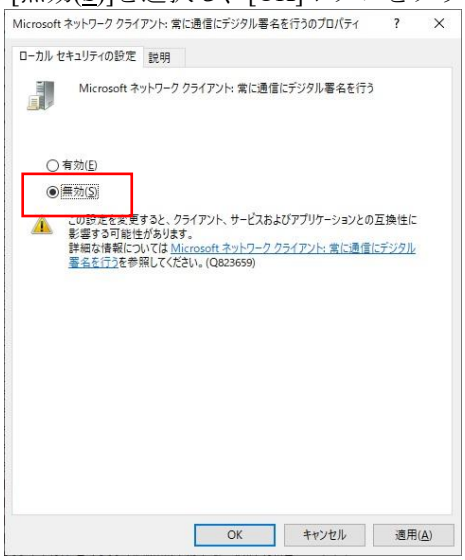


⑨ [OK]ボタンをクリックしてください。

⑩ 左側の項目ツリーから[コンピューターの構成]-[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] を選択し、右側の項目の「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」をダブルクリックしてください。



⑪ [無効(S)]を選択し、[OK]ボタンをクリックしてください。

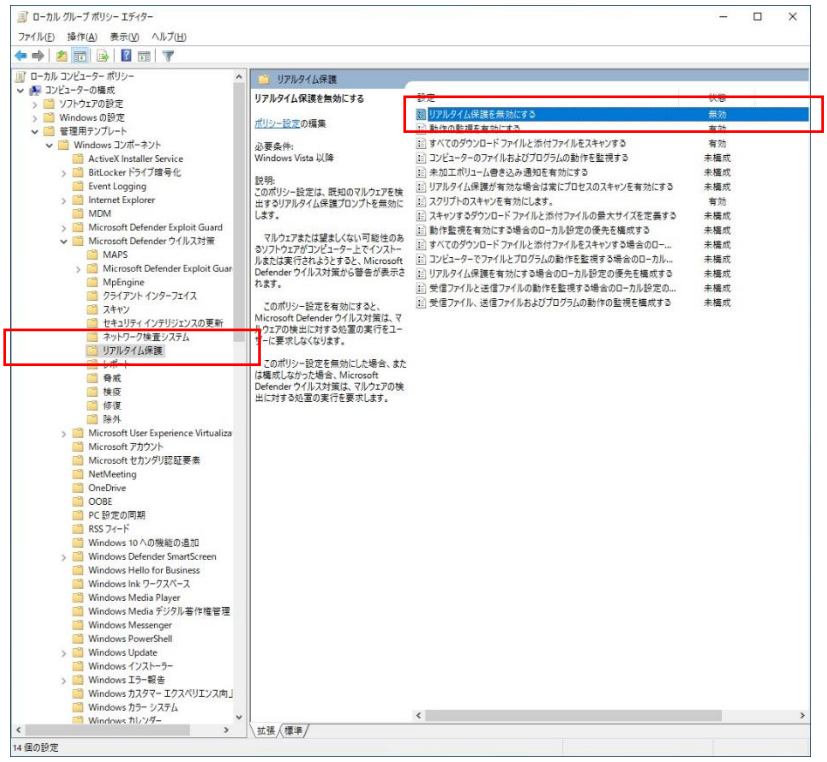


⑫ 右側の項目の「Microsoft ネットワーク サーバー：常に通信にデジタル署名を行う」をダブルクリックしてください。

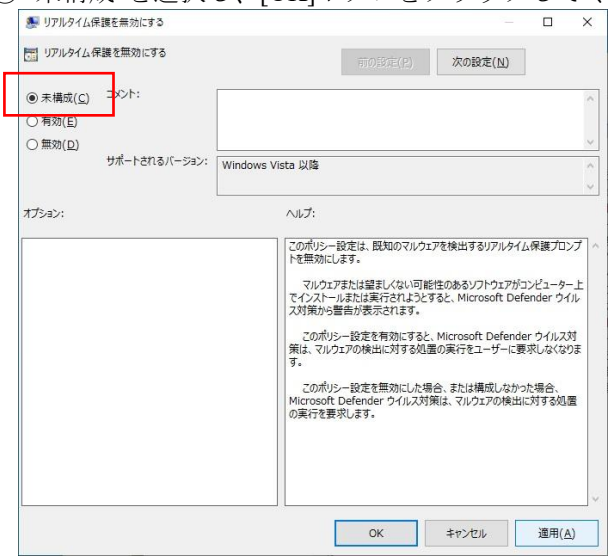
「Microsoft ネットワーク サーバー：常に通信にデジタル署名を行うのプロパティ」の、[無効(S)]を選択し、[OK]ボタンをクリックしてください。

※　Windows Server® IoT 2022, Windows Server® IoT 2025の場合は追加で⑬～㉔を実施してください。

⑬ 左側の項目ツリーから[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]-[Microsoft Defender ウイルス対策]-[リアルタイム保護] を選択し、右側の項目の「リアルタイム保護を無効にする」をダブルクリックしてください。



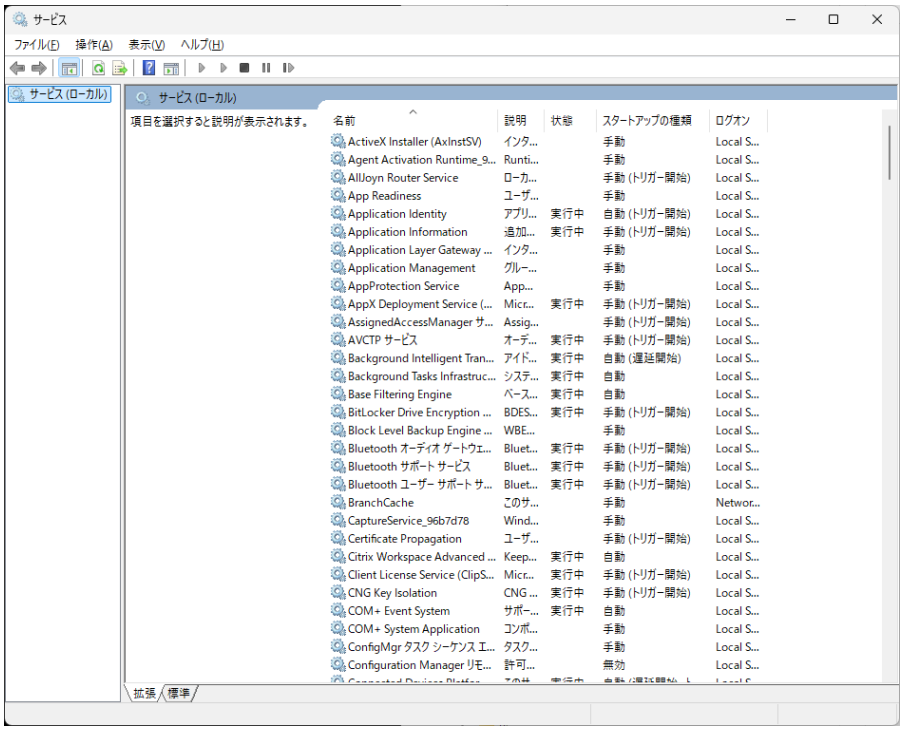
⑭ "未構成"を選択し、[OK]ボタンをクリックしてください。



＜サービスの設定変更＞

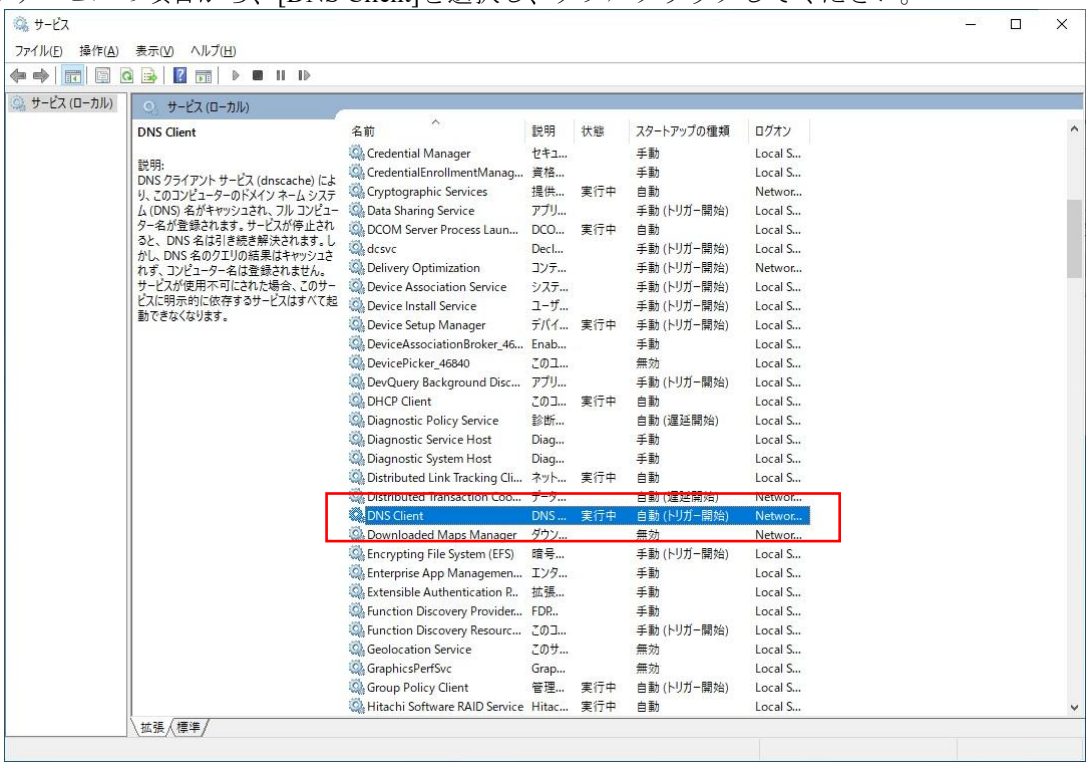
⑮デスクトップ画面下に配置されているスタートボタンを右クリックし「ファイル名を指定して実行」をクリックします。

⑯「ファイル名を指定して実行」画面で「**services.msc**」と入力してサービス画面を起動します。



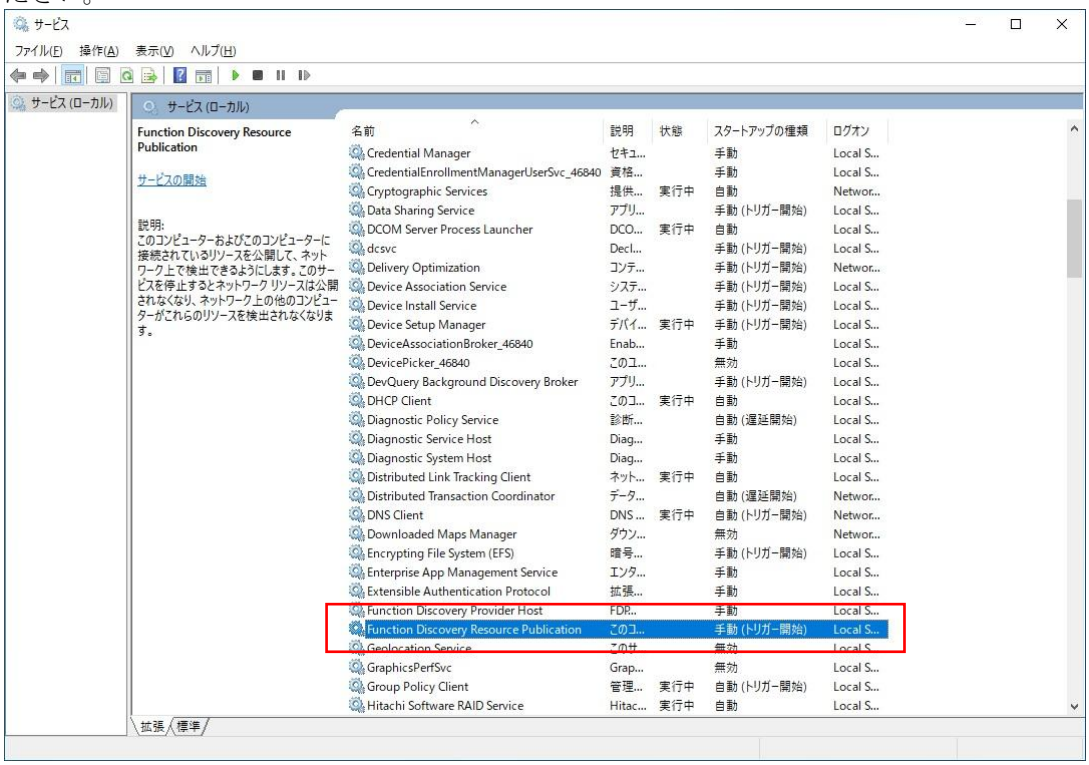
ユーザーアカウント制御（UAC）が有効な場合は、確認ダイアログが表示されます。確認メッセージで［はい］ボタンをクリックします。

⑰ サービスの項目から、[DNS Client]を選択し、ダブルクリックしてください。

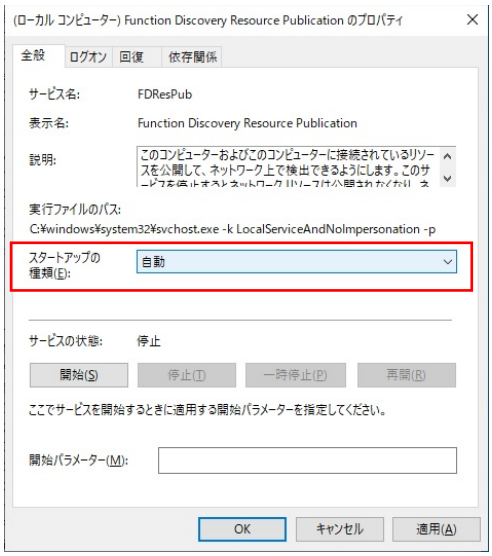


⑱ 「スタートアップの種類(E) :」が"自動"以外の場合は、"自動"を選択して、[OK]ボタンをクリックしてください。

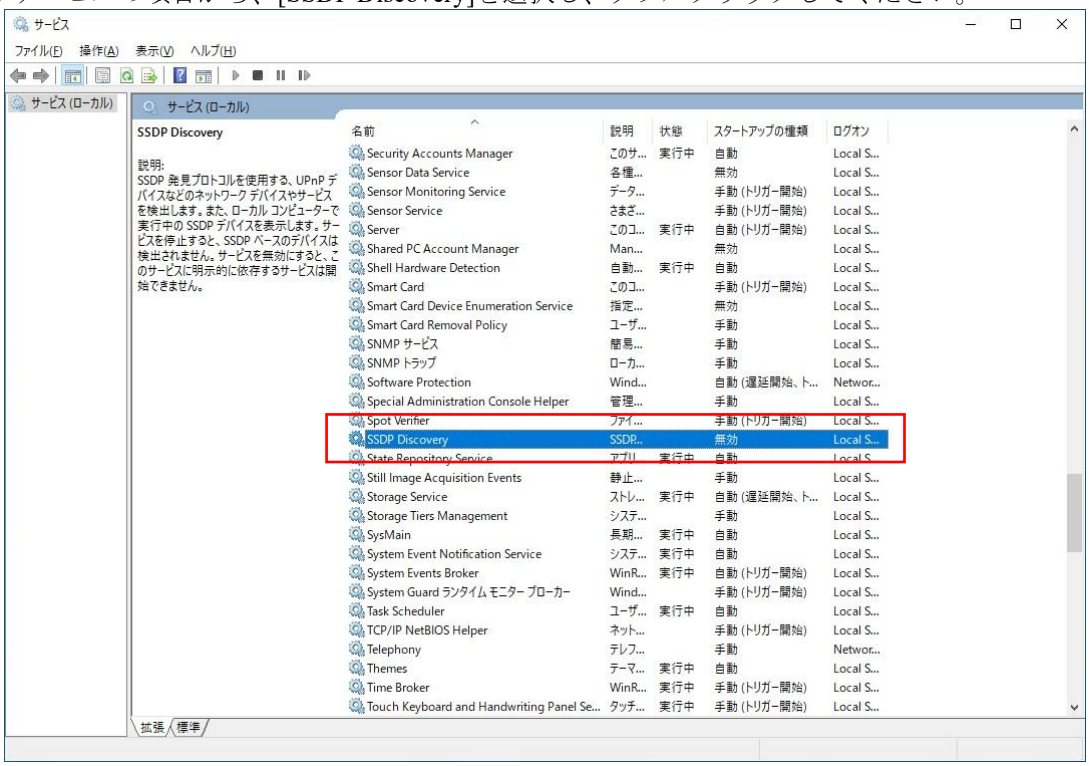
⑲ サービスの項目から、[Function Discovery Resource Publication]を選択し、ダブルクリックしてください。



⑳ 「スタートアップの種類(E):」が"自動"以外の場合は、"自動"を選択して、[OK]ボタンをクリックしてください。

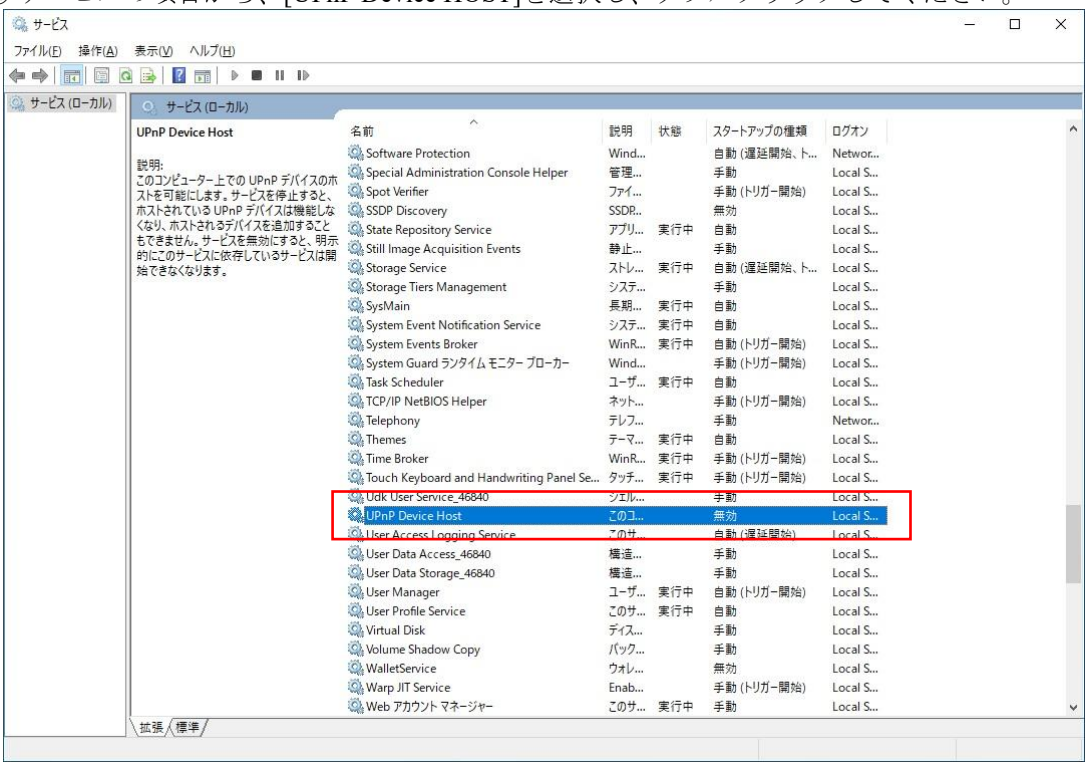


㉑ サービスの項目から、[SSDP Discovery]を選択し、ダブルクリックしてください。



㉒ 「スタートアップの種類(E):」が"自動"以外の場合は、"自動"を選択して、[OK]ボタンをクリックしてください。

㉓ サービスの項目から、[UPnP Device HOST]を選択し、ダブルクリックしてください。



㉔ 「スタートアップの種類(E):」が"自動"以外の場合は、"自動"を選択して、[OK]ボタンをクリックしてください。

㉕ ローカルグループポリシーエディターとサービス画面を終了し、HF-Wを再起動してください。