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



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

 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。

All Rights Reserved, Copyright $\ensuremath{\mathbb{C}}$ 2025, Hitachi Industrial Products, Ltd.

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。

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	3-8
3. 2. 3 共有フォルダへのアクセスを許可する	3-11

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 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。

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	(1)誰でも共有フォルダ内のフ	設定する
	タにアクセスする」 が 「管理者、リ	ァイルを読み取ることができて	
	モートデスクトップユーザ」に設定	しまうため、セキュリティ観点	
	されていることを確認する。	上、リスクを許容することが困	
		難である。	
2.2.5	「ローカルログオンを許可する」 が	(2)ユーザー権限を、正当なユ	設定する
	「管理者、ユーザー」 に設定されて	ーザーに制限しないと、権限の	
	いることを確認する。	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。	
1.1.3	「パスワードの最低有効期間」 が	(3) パスワードの更新が頻繁に	設定しない
	「1 日以上」に設定されていること	なり、利便性に支障をきたす。	
	を確認する。		

・「HF-Wのセキュリティ対策方針」による設定項目判断の例

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	WIN-4-5002-01
	00/05	(Windows [®] 10 IoT Enterprise 2021	
		LTSC 編)	
Windows Server [®] IoT 2022	HF-W2000 モデル	日立産業用コンピュータ HF-Wシ	WIN-4-5003-01
Standard (64bit)	68/65	リーズセキュリティ設定一覧	
		(Windows Server [®] IoT 2022	
		Standard 編)	

「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 BenchmarksTM $\mathcal{O}\mathcal{T}\mathcal{D}\mathcal{T}\mathcal{T}\mathcal{H}$

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「検索バー」をクリックします。



(2)検索画面が表示されます。検索バーに「gpedit.msc」と入力します。

すべて アプリ ドキュメント 設定 その他 ▼	X
最も一致する検索結果	
gpedit.msc Microsoft Common Console Document	
	gpedit.msc Microsoft Common Console Document
	端所 <u>C:#windows#system32</u>
	-0 管理者として実行(A)
	口 ファイルの場所を開く
	ראבסבצ-
	「gpedit.msc」を入力
K	
, 𝒫 gpedit.msc	ai



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。



■ ローカル グループ ポリシー エディター		<u></u>	×
ファイル(E) 操作(<u>A</u>) 表示(<u>V</u>) ヘルプ(<u>H</u>)			
🗢 🔿 🔲 🗟 🔒 🛛 🗊			
 □ ローカル コンピューター ポリシー ○ コンピュター ポリシー □ ローカル コンピューター ポリシー □ 副 Windows の設定 ○ ゴンドウェアの設定 ○ ゴンドウェアの設定 ○ ゴンドウェアの設定 ○ ゴンドウェアの設定 ○ Windows の設定 ○ 管理用テンプレート 	名前 第コンビューターの構成 過 ユーザーの構成		
< →			

(5) 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。



ローカル グループ ポリシー エディター イル(F) 操作(A) 表示(V) ヘル	ネットワーク経由でのアクセスのプロパティ	? ×	×
🔿 🖄 🔜 📉 🔀 📴	ローカル セキュリティの設定 説明		
ローカル コンピューター ポリシー ▲ コンピューターの模成 > 通 ソフトウンアの防定 > 通 名前解決ポリシー 図 名前解決ポリシー 図 スクリプト (スタートアップ)S > 職 展開されたプリンター > 通 セキュリティの設定 > 通 アカウント ポリシー	ネットワーク経由でのアクセス Administrators Backup Operators Everyone Users		rの設定 trators Erators Window Manager¥Wi ERVICE, NETWORK SERVICE ERVICE, Administrators, Users trators
	- ザーまたはグループの追加(LD		z, Administrators, Users, Backu rrators, Backup Operators, Per rrators rrators
 > ■ ドセキュリティボリシー > ■ 監査ボリシーの詳細な > → 加 ボリシーベースの QoS > ■ 管理用テンブレート ● ブーの構成 > ■ プーの構成 		リケーションとの互換性に 参照してください。	trators, Backup Operators trators, Backup Operators trators ERVICE, NETWORK SERVICE
> I OLYDEROUD > I Windowsの設定 > I 管理用テンプレート			trators trators

- (7) 設定を変更する項目分、(5)、(6)を繰り返します。
- (8) 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。
- (9) 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。

	セキュリティ設定項目	OS (*1)		設定値	
No		Win10	Srv2022	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	•	_	Guest,	Guest
	拒否			ローカルアカウント	
		—	•	Guest,	Administrator
				ローカルアカウントと	
				Administrators グループ	
				のメンバー	
2	リモート デスクトップサービ	•	•	Guest,	未設定
	スを使ったログオンを拒否			ローカルアカウント	

(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。

	セキュリティ設定項目	OS (*1)		設定値	
No		Win10	Srv2022	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	•	•	有効	未構成
	しない				

(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。

	セキュリティ設定項目	OS (*1)		設定値	
No		Win10	Srv2022	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	●	_	Guest, ローカルアカウント	Guest
		_	•	Guest, 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、一:非該当、

Win10 : Windows[®] 10 IoT Enterprise 2021 LTSC, Srv2022 : Windows Server[®] IoT 2022 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。

第3章 セキュリティ設定による影響と対処方法

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「検索バー」をクリックします。



②検索画面が表示されます。検索バーに「gpedit.msc」と入力します。

፼ <u>C</u> ©			
上位のアプリ			
同設定	ニ エクスプローラー	ראש זעד אעדב	5回 コントロール パネル
		「gpedit.ms	sc」を入力
🗄 🔎 検索するには、ここに入力し	it 🖾	2	

③検索結果に表示された	🛾 gnedit.msc 🗆	をクリック	します。
	Spearmise]		

	· · · ·
ita	も一致する検索結果 gpedit.msc Microsoft Common Console Document
# P	gpedit.msc 🗮 💽 🔚

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。

④ ローカルグループポリシーエディターが起動されます。

ファイル(上) 操作(点) 表示(少) ヘルブ(土) ● ● (二) 回 (金) (金) (金) (金) (金) (-2,0) ● ● (二) 回 (金) (金) (-2,0) ● ● (二) (-2,0) ● (-2,0) ● ●	🍠 ローカル グループ ポリシー エデ	19-		-	×
 ◆ ● □ □ □ □ □ □ □ □ □ □ □ □ □ □	ファイル(E) 操作(<u>A</u>) 表示()	の ヘルプ(日)			
□ ローカル コンピューター ボリシー ③ コンピューターの爆成 ○ ツバカウェアの設定 ○ Windows の設定 ○ 雪 管理用テンプレート ○ ゴーダーの爆成 ○ Windows の設定 ○ 雪 管理用テンプレート ○ Windows の設定 ○ 雪 管理用テンプレート ○ 「「「「」」」 ○ 「」」 ○ 「」	🗢 🏟 💼 📴 🗟 👔	DI			
		■ ローカル コンピューター ポリシー 項目を選択すると説明が表示されます。	名前 ■コンビューターの構成 ▲ ユーザーの構成		
		∖拡張√標準/			

(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。

ココイル(の) 場合(な) まニハタ タルゴ(い)				
ファイル(E) 操作(A) 表示(Q) ヘルフ(E)				
副 ローカル コンピューター ポリシー	ポリシー	セキュリティの設定		
✓ ● コンピューターの構成	※ オブジェクト ラベルの変更			
> 🧾 ソフトウェアの設定	励オペレーティングシステムの一部として機能			
Windowsの設定	⑦ グローバルオブジェクトの作成	LOCAL SERVICE NETWO		
> 🧾 名前解決ボリシー	〇〇 フンドューターとフーザー アカウントに委任時の信頼を付与			
図 スクリフト (スタートアップ/シャットダウン)	いい リービスレーズのログオンを拒否	Guest		
> 時間 展開されたプリンター	(i) +	NT SERVICEYALL SERVICES		
◇ ▶ セキュリティの設定	いい システル パフォーマンスのプロファイル	Administrators NT SERVI		
> <u>A</u> PDD> mDD=		Administrators User		
▼ □ □−カル ホリシー	い、システム時刻の変革	LOCAL SERVICE Adminis		
	回いゴルクルリカのため	Administrator		
2.2 ユージー作用の目の目で	20. フケジュートバグ停告順位の通貨上げ	Administrators Window		
> A UTIDIT A DIDA	() オナリティシア () () () () () () () () () () () () ()	LOCAL SERVICE NETWO		
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	回してコンパーショウエル	LOCAL SERVICE Adminis		
● ホリーブ ブラスト モージャーパラブ	「「「ディークレステージの友史」	LOCAL SERVICE, Adminis		
> 二 ソフトウェアの制限のポリシー		Administration		
> 20 アブリケーション創催ポリシー		Administrators		
IP セキュリティ ポリシー (ローカル コンドューター)	「「「トークノオノンエクトのFFR」 「「「ドーナングフラーショント」」の「あまりた」	Addition and the second		
▶ ● 監査ボリシーの詳細な機成	回,ドラキノフ ステージョノからコノビューフーを削除	Administrators, Users		
> 1 ポリシー ベースの QoS	回、トメインにワークステーションを追加			
> 1 管理用テンプレート	200 イットワーク経由でのアクセス	Administrators, Remote		
・ 遇 ユーザーの構成	(ペットリーク)社田のアクセスを担当	ローカル アカウント,Guest		
> 🎬 ソフトウェアの設定		Guest		
> 🧮 Windows の設定	(1) パッナ ションとしてロクオン	Administrators, Backup		
> 🧰 管理用テンプレート	2017アームウェア環境値の修正	Administrators		
	図ファイルとその他のオフジェクトの所有権の取得	Administrators		
	同ファイルとティレクトリのバックアップ	Administrators		
	201 ファイルとティレクトリの復元	Administrators		
	い、フロクラムのデバック	Administrators		
	回 プロセス レベル トークンの置き換え	LOCAL SERVICE, NETWO		
	□ プロセス ワーキング セットの増加	Users		
	し プロセスのメモリクォータの増加	LOCAL SERVICE, NETWO		
	いい ページ ファイルの作成	Administrators		
	100 ボリュームの保守タスクを実行	Administrators		
	この メモリ内のページのロック			
	闘 リモート コンピューターからの強制シャットダウン	Administrators		
	闘 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	ローカル アカウント,Guest		
	😳 リモート デスクトップ サービスを使ったログオンを許可	Administrators, Remote		
	📖 ローカル ログオンを拒否	Guest		
	闘 ローカル ログオンを許可	Administrators, Users		
	📓 永続的共有オブジェクトの作成			
	闘 監査とセキュリティログの管理	Administrators		

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の場合>

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



				-			
ネットワーク組	産由のアクセスを打	目否のプロパラ	ŕ1			?	×
ローカル セキ	キュリティの設定	説明					
	ネットワーク経	由のアクセスを	E拒否				
Guest ローカル	アカウント						ו
1-	ザーまたはグルー	プの追加(<u>U</u>)		削除(<u>R</u>)		
		Г	OK		キャンセル	適用(<u>A</u>)

<Windows Server® IoT 2022 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(<u>R</u>)] ボタンを クリックレてください

クリックしてくたさい。		
ネットワーク経由のアクセスを拒否のプロパティ	?	×
ローカル セキュリティの設定 説明		
ネットワーク経由のアクセスを指否		
「Grund ローカル アカウントと Administrators グループのメンバー		
ユーザーまたはグループの:追加(<u>い</u>) 削除(<u>R</u>)		
OK キャンセル	適用	用(<u>A</u>)

・ [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。

ネットワーク経由のアクセスを拒否のプロパティ	?	×
ローカル セキュリティの設定 説明		
ネットワーク経由のアクセスを拒否		
Guest		
ユーザーまたはグルーブの追加(<u>U</u>)		1
OK キャンセル	適用	(<u>A</u>)

・[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。

ユーザー または グループ の 選択	×	
オブジェクトの種類の選択(<u>S</u>): コーザー または ビルトイン セキュリティ ブリンシパル	オブジェクトの種類(<u>O</u>)	Г. у
場所の指定(<u>F</u>): DESKTOP-OOPVEUT	場所(L)	「Administrator」を入刀
違訳するオブジェクト名を入力してください(日)TEI: Administrator	名前の確認(<u>C</u>)	
詳細設定(<u>A</u>)	ОК キャンセル	

「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。

⑦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

■ ローカル グループ ポリシー エディター			1221	×
ファイル(F) 操作(A) 表示(V) ヘルプ(H)				
• • 2 • 2 • 2				
Tローカル コンピューター ポリシー	#00-	セキュリティの設定		
💵 コンピューターの構成		2419940/B02		
> 1 ソフトウェアの設定	調オフジェクトラヘルの変更			
✓ [○] Windows の設定	回オペレーティング システムの一部として機能			
> ○ 名前解決ポリシー	図 クローバル オブジェクトの作成	LOCAL SERVICE, NETWO		
回 スクリプト (スタートアップ/シャットダウン)	③ コンビューターとユーザーアカウントに委任時の信頼を付与			
> 瞬 展開されたプリンター	間サービスとしてのログオンを拒否	Guest		
✓ → セキュリティの設定	いい サービスとしてログオン	NT SERVICE¥ALL SERVICES		
> 📸 アカウント ポリシー	闘 システム パフォーマンスのプロファイル	Administrators, NT SERVI		
✓ 100 ローカル ポリシー	()) システムのシャットダウン	Administrators, Users		
> 1 監査ボリシー	協 システム時刻の変更	LOCAL SERVICE, Adminis		
2 ユーザー権利の割り当て	闘 シンボリック リンクの作成	Administrators		
> 🙀 セキュリティ オプション	闘 スケジューリング優先順位の繰り上げ	Administrators, Window		
> 🧾 セキュリティが強化された Windows Defenc	🔤 セキュリティ監査の生成	LOCAL SERVICE, NETWO		
ネットワーク リスト マネージャー ポリシー	闘 タイムゾーンの変更	LOCAL SERVICE, Adminis		
> 🧰 公開キーのポリシー	闘 ディレクトリ サービス データの同期化			
> 🧾 ソフトウェアの制限のポリシー	副デバイス ドライバーのロードとアンロード	Administrators		
> 🧾 アプリケーション制御ポリシー	し、トークンオブジェクトの作成			
> 🔜 IP セキュリティ ポリシー (ローカル コンピューター	じし、ドッキングステーションからコンピューターを削除	Administrators, Users		
> > > > > <	圖 ドメインにワークステーションを追加			
> 🔐 ボリシー ベースの QoS	③ ネットワーク経由でのアクセス	Administrators, Remote		
> 🧰 管理用テンフレート	30 ネットワーク経由のアクセスを拒否	ローカル アカウント,Guest		
18. ユーサーの構成	100 パッチ ジョブとしてのログオンを拒否	Guest		
> 9 ソノトウェアの設定	🔤 パッチ ジョブとしてログオン	Administrators, Backup		
> Windows の設定	□ ファームウェア環境値の修正	Administrators		
>	ファイルとその他のオブジェクトの所有権の取得	Administrators		
	ファイルとディレクトリのパックアップ	Administrators		
	岡 ファイルとディレクトリの復元	Administrators		
	国 プログラムのデバッグ	Administrators		
	□ プロセス レベル トークンの置き換え	LOCAL SERVICE NETWO		
	100 プロセスワーキング セットの増加	Users		
	同プロセスのメモリクォータの博加	LOCAL SERVICE NETWO		
	国ページファイルの作成	Administrators		
	間ボリュームの保守なつなを実行	Administrators		
		Administrators		
_	CULTURE TO CONTRACTOR			
	ショックモードコンビューシーからの強制シャッドックソン 同じエート デフクトップ サービスを使ったりパナンを短不	Rently 7th20h Guert		
	(1) リエート デフクトップ サージフを使ったログオンを注意	Administrators Parato		
	いローカルログオンを拒否	Guest	-	
		Administrators Liters		
	回し カル ロノハノ こい つ 回 永靖的 土方オブジェクトの作成	Administrators, Oscis		
	(1) からいスライノノエンドのFRA	Administrators		
	の(重量ででイエリノイログの管理	Administrators		

⑧一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(<u>R</u>)] 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。

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のプロパティ	?	×
ローカル セキュリティの設定 説明		
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		
Gust ローカルテカウント]
ユーザーまたはグループの追加(U) 削除(B)		
OK ++>>セル	適用(<u>A</u>	0

⑨ 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 「検索バー」 をクリックします。



②検索画面が表示されます。検索バーに「gpedit.msc」と入力します。

上位のアプリ			
記録	□ 1/270-7-	ריי אלעם <i>ל</i> אעקב	▶回 コントロール パネル
		「gpedit.ms	ic」を入力
● 検索するには、ここに入力します	t Hi	2 🗖	

③検	索結果に表示された「 gpedit.msc 」 をクリックします。
	፼ <u></u> <u>0</u> ∅ …
	最も一致する検索結果
	gpedit.msc Microsoft Common Console Dacument
4	🔎 gpedit.msc 🛛 🛱 💽 🚍

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。

④ ローカルグループポリシーエディターが起動されます。

■ ローカル グループ ポリシー エディター		-	×
ファイル(E) 操作(A) 表示(V) ヘルプ(H)			
← ⇒ □ □ ≥ 2 □			
	はす。 名前 ■コンピューターの構成 ■ ユーザーの構成		
─────────────────────────────────────			

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]-[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。

I make through the state I was				
🛄 デバイスの検索	↑ □ デバイスとリソースのリダイレクト			
デバイスの登録	ドライブの川ダイレクトを許可したい	10 T	17.95	7426
📄 ニュースと関心事項	171707710712:1-3080	シン ビデナナップチッカリガノリカレキをす コートリン	+ 10 +	1111
□ ファイル 艰歴	ポリシー設定の編集	E ビデオ ギャノテャのリティレットを計与しない E) ナービュナカ にのジェナ軍 キリガノ りょうか マナス	木偶成	007
フッシュしてインストール		ビスーディオのよびビデス研生リジイレジトを計引する	未確成	1117
ノレセンテーションの設定 ポータゴル まかし、ニテハ(ガン・フニ)	必要条件: Windows Senier 2002 オパレーティングシ	ビーバーディルボロッティレットを計つする	木偶成	1117
二 ホーングル イベレーティング システム	ステム、Windows XP Professional または	ビカリップボードの川ダイレクトを許可したい	未構成	11117
- L/W-/	それ以降		木偶成	0.072
メッヤージング	8m 80.	「「ドライブのリダイレクトを注意」ない	10.25	LALA Z
メンデナンス スケジューラ	ポッサ: このポリシー設定は、リモート デスクトップ	F LPT ポートのリダイレクトを許可しない	去模式	11117
✓ 🧰 リモート デスクトップ サービス	サービス セッションで、クライアント ドライブの	日 サポートされているブラグ アンドブレイ デバイスのリダイレクトを許可し	未構成	いいえ
📫 RD ライセンス	マッピングをしないようにするかどうかを指定	〒 スマートカードデバイスのリダイレクトを許可しない	未構成	いいえ
✓ 2 リモート デスクトップ セッション ホスト	689 (F71) 971 VVF).	三 タイム ゾーン リダイレクトを許可する	未構成	いいえ
RD 接続ブローカー	既定では、RD セッション ホスト サーバーは	WebAuthn リダイレクトを許可しない	未構成	いいえ
セキュリティ	接続時に自動的にクライアントドライブを			
セッションの時間制度	イッノします。イッノされたトライノは、エクス プローラーまたは「コンピューター」のセッション			
	フォルダー ツリーに、<コンピューター名>の <			
1077-007107F	ドライブ文字>という形式で表示されます。			
= JUJ/1//	このボリシー設定を使ってこの動作を上書き			
> 三 リモート ヤッション環境	CCA9:			
□□ -時フォルダー	このポリシー設定を有効にすると、クライアン			
🧾 接続	トドライブのリダイレクトはリモート テスクトッ			
> 🧾 リモート デスクトップ接続のクライアント	また、クリップボードでのファイル コピーのリダ			
音声認識	イレクトは、Windows Server 2003、			
imit 画面の端の UI imit 回 imit imit imit 回 imit imit	Windows 8、および Windows XP を実行			
· 検索	していシュノビューフーでは新刊されません。			
一 資格情報のユーザーインターフェイス 一 たたまたのプリン・	このポリシー設定を無効にすると、クライアン			
 	トドライブのリダイレクトは常に許可されま			
	す。さらに、クリッノホートのリタイレクトを許 可すると クリップボードでのファイル コピーの			
	リダイレクトは常に許可されます。			
2				
配信の最適化	このボリシー設定を構成しなかった場合、ク			
> 🛄 コントロール パネル	ブポードでのファイル コピーのリダイレクトはグ			
	ループポリシーレベルでけ指定されません。			

⑥ [未構成(C)]を選択し、[OK]ボタンをクリックしてください。

●未構成(C) →	>h:	
○ 有効(E) ○ 無効(D)		
9 7	ポートされるバージョン:	vs Server 2003 オペレーティング システム、Windows XP Professional ま 以降
オプション:		へいば:
		ビディブなやどうなしないまたでもなどかな考慮をします(ドラインダ しか)、 しか)、 したし、 したし、 したし、 したし、 したし、 したし、 したし、 した
		このポリシー設定を未効にすると、クライアントトライブのリタイレクトされに 許可されます。さらに、クルプボードのリダイレクトを許可すると、クルプボー ドでのファイル コピーのリタイレクトは第に許可されます。

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。

- 3.2.3 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「検索バー」をクリックします。





③ 検索結果に表示された「gpedit.msc」 をクリックします。

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。

① ローカルグループポリシーエディターが起動されます。



⑤ 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。

■ ローカル グループ ポリシー エディター				- 🗆 ×
ファイル(E) 操作(A) 表示(Y) ヘルプ(E)				
🕨 🧇 🙍 📰 🔒 📓 📷 🛛 🍸				
1 ローカル コンピューター ポリシー	Lanman ワークステーション			
∨ 🛃 コンピューターの構成		10.0	44.09	TANK
> 🧾 ソフトウェアの設定	安全でないケストロクオンを有効にする	設定	权思	JVYL
> 🛄 Windows の設定	ポリシー時定の標準	目間号の順位	未構成	いいえ
✓ ■ 管理用テンプレート		11 経過的目出性共常でのまれいションの処理します	288	11112
> Mindows コンボーネント	必要条件:	図 安全でないケストロクオンを有効にする	無効	いいえ
> 2 コントロール バネル サーバー	Windows Server 2016 以降または Windows 10 以降	回避緩防可用性共有上のオフラインファイルの可用性	未確成	いいえ
> 📫 システム	29 8 8 :			
> 📫 920 /(-2 [29-h] X==-	このポリシー設定では、SMB クライアントが			
ネットワーク	SMB サーバーへの安全でないゲストログオ			
BranchCache	ノを計可するかとうかを決定します。			
DirectAccess クライアント エクスペリエンスの	このポリシー設定を有効にした場合、または			
0NS 221721	このポリシー設定を構成しなかった場合、			
LAN Manager 9-7-	SMB クライアントは安全でないゲスト ログオ			
Lanman 9-927-939	ンを許可します。			
Microsoft VII W- VII Store - 7 #-VI	このポリシー設定を毎効にした場合、SMB			
> One ((truck 7 truck - ==	クライアントは安全でないゲストログオンを			
SNMD	拒否します。			
2011年1月11日 121 121 121 121 121 121 121 121 121	中央スキレゲストログキンがファイルサー			
↓ CPIP 設定	パーによって使用されるのは、共有フォルダー			
Windows Connect Now	に対する認証されていないアクセスを許可す	r		
Mindows 接続マネージャー	ることが目的です。エンタープライズ環境では	t		
> 🧮 WLAN #-ピス	一般的ではありませんが、ファイルサーバー			
> 📔 WWAN #-ピス	としく動作しているコンシューマー NAS (イツ) トワーク接続ストレージ) アプライアンスでは			
オフライン ファイル	安全でないゲストログオンが頻繁に使用さ			
ネットワーク プロバイダー	れています。Windows ファイル サーバーでは	t		
> 🏹 ネットワーク接続	認証を要求し、既定では安全でないゲスト			
ネットワーク接続状態インジケーター	ログオンビア 日しません。安全でないケスト			
🎽 ネットワーク分離	名、SMB 暗号化などの重要なセキュリティ			
バックグラウンドインテリジェント転送サービス	機能が無効になります。結果として、安全			
フォント	でないゲストログオンを許可するクライアント			
🧰 ホットスポット認証	は、さまさまな man-in-the-middle 火撃			
ワイヤレスディスプレイ	1 初指、マルウェアに対するリスクにつながる可	t i i i i i i i i i i i i i i i i i i i		
ゴリンター	能性があります。また、安全でないゲストロ			
🖏 すべての設定	グオンを使用してファイル サーバーに書き込ま			
✔ 🕵 ユーザーの構成	れたデータには、ネットワーク上のすべての			
> 🧾 ソフトウェアの設定	す。Microsoftでは、安全でないゲストログ	1		
> 🛄 Windows の設定	オンを無効にして、認証されたアクセスが要			
> 🧰 管理用テンブレート	求されるようにファイル サーバーを構成するこ とをお勧めします。			
()	│ │			
	Ann and Come a			

⑥ [有効(<u>E</u>)]を選択し、[OK]ボタンをクリックしてください。

🌉 安全でないゲストロクオンを有効にする				
🔜 安全でないゲスト ログオンを有効にする		前の設定(<u>P</u>)	次の設定(<u>N</u>)	
○ 未構成(<u>C</u>) →×>ト:				~
 有劝(E) (○ 無効(D) 				
サポートされるパージョン:	Windows Server 2016 [以降または Windows	10 以降	^
オプション:	ヘルプ:			
	このポリシー いゲストログ このポリシー った場合、S このポリシー ログオンを拒 安全でない 有フォルダー	設定では、SMB クライ オンを許可するかどうか 設定を有効にした場合 MB クライアントは安全 設定を無効にした場合 否します。 デスト ログオンがファイル こ対する装証されていれ	アントが SMB サーバー を決定します。 、またはこのポリシー設定 でないゲスト ログオンを 、SMB クライアントはま 、サーバーによって使用 おいアクセスを許可する。	-への安全でな ^ 定を構成しなか 許可します。 安全でないゲスト されるのは、共 ことが目的です
	・エンタープラ て動作してし アシスでは、 いため、SMM になります。4 は、さまざまれ 失、データの ま、カークの	イズ環境では一般的 るコンシューマー NAS 安全でないゲスト ログフ ファイル サーバーでは載 を使用しません。安全 3 署名、SMB 暗号化 素果として、安全でない 2 man-in-the-midd 破損、マルクエアに対す ションをごと ロガースを	ではありませんが、ファイ (ネットワーク接続ストし たが頻繁に使用されて 短を要求し、既定では でないゲストログオンは などの重要なセキュリう ゲストログオンを許可 追。攻撃に対して脱弱 るリスクにつながる可能 ミロ・マン・サード	レサーバーとし ノージ) アプライ います。 均安全でないゲ 想証されていな マイ権能が無効 するクライアント になり、データ損 生力物のます。 レーーサージェック
	[ок	キャンセル	通用(<u>A</u>)

⑦ 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。

■ ローカル グループ ポリシー エディター					×
ファイル(E) 操作(A) 表示(V) ヘルプ(日)					
🗢 🔿 🙍 📰 🗙 🗊 🗟 📓					
■ ローカル コンピューター ポリシー	ポリシー ^	セキュリティの設定			^
✓ № コンビューターの構成	🔝 オブジェクト ラベルの変更				
> 🛄 ソフトウェアの設定	副 オペレーティングシステムの一部として機能				
Windows の設定	◎ グローバル オブジェクトの作成	LOCAL SERVICE NETWO			
> 🧾 名前解決ボリシー	副コンドューターとコーザー アカウントに委任時の信頼を付与				
言 スクリフト (スタートアッフ/シャットタウン)	10 サービスとしてのログオンを拒否	Guest			
> 時に長期されたノリンター	副 サービスとしてログオン	NT SERVICE¥ALL SERVICES			
◇ 画 セキュリティの設定	◎ システムパフォーマンスのプロファイル	Administrators NT SERVI			
	100 システムのシャットダウン	Administrators Users			
	13 システム時刻の変更	LOCAL SERVICE Adminis			
> 14 当日ボッジー 、 12 コーザー推利の割り当て	い シンボリック リンクの作成	Administrators			
シーム セキュリティオブション	は スケジューリング優先 順位の繰り上げ	Administrators Window			
> 🤗 セキュリティが強化された Windows Defend	い ヤキュリティ 駐吉の牛成	LOCAL SERVICE NETWO			
ネットワークリストマネージャーボリシー	副タイトゾーンの変更	LOCAL SERVICE Adminis			
> 🦳 公開キーのボリシー	◎ ディレクトリサービスデータの同期化				
> 🎽 ソフトウェアの制限のポリシー	三 デバイス ドライバーのロードと アンロード	Administrators			
> 🧾 アプリケーション制御ポリシー	10 トークンオブジェクトの作成				
» 👼 IP セキュリティ ポリシー (ローカル コンピュータ-	ドッキング ステーションから コンドューターを 創除	Administrators Users			
> 🧰 監査ボリシーの詳細な構成	同ドメインにワークステーションを追加				
> 🏭 ポリシー ベースの QoS	1 x 10-7 2 m n n n n n n n n n n n n n n n n n n	Administrators Remote	_		
> 📫 管理用テンプレート	副ネットワーク経由のアクセスを拒否	ローカル アカウント Guest			
∨ 🔒 ユーザーの構成	目 パッチ ジョブトレアのログナンを招示	Guart			
> 🧰 ソフトウェアの設定	10 パッチ ジョブとしてログオン	Administrators Backup			
> Windows の設定	10 ファームウェア環境値の修正	Administrators			
> 🧰 宮垣用テンノレート	10 ファイルとその他のオブジェクトの所有権の取得	Administrators			
	同 ファイルとディレクトリのバックアップ	Administrators			
	100 ファイルとディレクトリの復元	Administrators			
	110 プログラムのデバッグ	Administrators			
	□ プロセスレベルトークンの置き換え	LOCAL SERVICE NETWO			
	100 プロヤス ワーキング ヤットの増加	Users			
	プロセスのメモリ クォータの増加	LOCAL SERVICE NETWO			
	副 ページ ファイルの作成	Administrators			
	10 ボリュームの保守タスクを実行	Administrators			
	※ メモリ内のページのロック				
	副リモート コンピューターからの強制シャットダウン	Administrators			
	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	ローカル アカウント Guest			
	110 リモート デスクトップ サービスを使ったログオンを許可	Administrators Remote			
	ローカル ログオンを拒否	Guest			
	ローカル ログオンを許可	Administrators.Users			
	副永徳的共有オブジェクトの作成				
	● 動産とおもうは長く口グの管理	Administration			
	100 新聞とビイエリナイ ロンの 新練	Administrators			

⑧設定に対して以下の操作を行ってください。

<Windows[®] 10 IoT 2021 LTSCの場合>

- ・"ローカルアカウント"を選択し、[削除(<u>R</u>)] 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。

ネットワーク経由のアクセスを打	巨否のプロパティ			?	×
ローカル セキュリティの設定	説明				
ネットワーク経	由のアクセスを拒否				
Guest ローカル アカウント					
	fa-4-1-1-1	#16(p)	_		
ユーリーまたはクルー	/の追加(<u>U</u>)	<u>則</u> 陈(<u>K</u>)			
		OK ŧ	ャンセル	適用	(<u>A</u>)

<Windows Server® IoT 2022 の場合>

- ・"Guest"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(<u>R</u>)] ボタンを クリックしてください。
- ・"Guest"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。

ネットワーク経由のアクセス	を拒否のプロパティ		?	×
ローカル セキュリティの設力	12 説明			
ネットワーク	経由のアクセスを拒否	ία.		
				1
Guest ローカル アカウントと A	dministrators グルー:	プのメンバー		
ユーザーまたはグル	-プの追加(U)	削除(R)		
		OK twitt	() () () () () () () () () () () () () (
		Tr/E/	(四/四)	

- ⑨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

ネットワーク経由でのアクセスのブロバティ	?	>
ローカル セキュリティの設定 説明		
ネットワーク極由でのアクセス		
Administrators Remote Desktop Users		
ユーザーまたはグループの追加(山) 利除(民)		
ユーザーまたはグループの追加(Ú) ○の設定を変更すると、クライアント、サービスおよびアプリケー 影響する可能性があります。 詳細な情報についてはネットワーク短曲でのアクセスを参照 (Q823659)	ションとの互換性に してください。	

⑩ [選択するオブジェクト名を入力してください(<u>例)(E)</u>:]に"Everyone"を入力し、[OK]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 選択	×	
オブジェクトの種類の選択(<u>S</u>):		
ユーザー または ビルトイン セキュリティ プリンシパル	オブジェクトの種類(<u>O</u>)	
場所の指定(<u>F</u>):		「Everyone」を入力
DESKTOP-OOPVEUT	場所(<u>L</u>)	
躍択するオブジェクト名を入力してください (例)(E)+		
Everyone	名前の確認(<u>C</u>)	

① [OK]ボタンをクリックしてください。

AP		
dministrators		
lemote Desktop Users		
□_ff_また/けグⅢ	ブル28-truin allBarrain	21
ユーザーまたはグルー この設定を変更	ブの追加(1) 削除(1)	3 アブリケーションとの互換性(
ユーザーまたはグルー この設定を変更 影響する可能性 詳細な情報につ	プの通加(U) すると、クライアント、サービスおよび があります。 いては ネット・ワーク理由でのアクセン	3) アブリケーションとの互換性() 2を参照してください。

② 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。



³[無効(<u>S)</u>]を選択し、[OK]ボタンをクリックしてください。



- ④ 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(<u>S</u>)] を選択し、[OK]ボタンをクリックしてください。



- ※ Windows Server[®] IoT 2022の場合は追加で⑮~圀を実施してください。
- ⑤ 左側の項目ツリーから[コンピューターの構成]-[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 護を無効にする」をダブルクリックしてください。

イル(E) 操作(A) 表示(V) ヘルプ(H)					
🔶 📶 🔒 🖬 🗊 🔻					
コーカル コンピューター ポリシー	📋 リアルタイム保護	2			
■ コンビューターの構成	リアルタイム保護を無効にする	107	0.00	_	_
) 「ソノトウェノの設定		同日アルタイム保護を長めにする	#125		-
Windows OBJE	ポリシー設定の編集	1 動作の数据を有効にする	有加		-
/ ● 管理用テノノレート		1 オバアのダウンロード ファイル と汚付ファイルをフキャンオス	市た		_
Active Vincteller Service	必要条件: Windows Vista 以降	12 3 パイロックション アンドイルビルパイング かどく マンタン	本語成		
Bitl ocker ドライブ度号化	WINDOWS VISIO (C)4	1 キ加丁ポリューム書き込み運知を変効にする	主体成		
Event Logging	說明:	1111月14日になったいになったりで	土垣式		
> internet Explorer	このポリシー設定は、既知のマルウェアを検	1 フクリプトのフォッンを有効にします	# 2h		
MDM	出身のリアルライム体護ノロノアドを無効に	三 ステリアトロスイモノビリカルにします。	主接成		
> 🧾 Microsoft Defender Exploit Guard		1)動作動現を有効にする場合のローカル設定の優先を構成する	未模式		
✓ I Microsoft Defender ウイルス対策	マルウェアまたは望ましくない可能性のあ	E 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場合のロー	未構成		
MAPS	ロンフトウェアかコンピューター上でインストー しまたは実行されようとすると、Microsoft	11 コンピューターでファイルとプログラムの動作を監視する場合のローカル	未構成		
> iii Microsoft Defender Exploit Guar	Defenderウイルス対策から警告が表示さ	1: リアルタイム保護を有効にする場合のローカル設定の優先を構成する	未構成		
MpEngine	れます。	1 受信ファイルと送信ファイルの動作を監視する場合のローカル設定の	未構成		
クライアントインターフェイス	このポリシージャをおかにオテレ	ご 受信ファイル、送信ファイルおよびプログラムの動作の監視を構成する	未構成		
2++v	Microsoft Defender ウイルス対策は、マ				
セキュリティインテリジェンスの更新	サウェアの検出に対する処置の実行をユー				
ネットリーク検査システム	1-に要求しなくなります。				
リアルダイム保護	このポルシージウエモかにした場合 また				
1 	にした場合、Microsoft				
一 市市、	Defender ウイルス対策は、マルウェアの検				
○ (#復)	出に対する処置の実行を要求します。				
(1) 除外					
> 📫 Microsoft User Experience Virtualiza					
Microsoft アカウント					
Microsoft セカンダリ認証要素					
NetMeeting					
OneDrive					
OOBE					
PC 設定の同期					
RSS 74-15					
Windows 10 への機能の道加					
Windows Defender SmartScreen					
Windows nello for Business					
Windows Media Player					
Windows Media デジタル業件推算得					
Windows Messenger					
Windows PowerShell					
> 💙 Windows Update					
Windows インストーラー					
> 🧾 Windows エラー報告					
Windows カスタマー エクスペリエンス向」					
📔 Windows カラー システム			_		
I Windows カレンダー	1 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	< .			_
>	\ 拓張人標準/				

⑩ "未構成"を選択し、[OK]ボタンをクリックしてください。

🌉 リアルタイム保護を無効にする	- 🗆 X
リアルタイム保護を無効にする	前の設定(E) 次の設定(N)
●未構成(<u>C</u>) → ×>ト: () 有効(F)	×
○ 無効(D)	~
サポートされるパージョン:	Windows Vista 以緣
オプション:	
	このポリシー設定は、既知のマルクエアを快出するリアルタイム保護プロンプ トを無効にします。 マルクエアまたは第三しくない可能性のあなソフトウエアがコンピューター上 マインストールまたは実行されようとすると、Microsoft Defender ウイル ス対策から警告が表示されます。 このポリシー設定を有効にすると、Microsoft Defender ウイルス対 第は、マルクエアの検出に対する処置の実行をユーザーに要求しなくなりま す。 このポリシー設定を無効にした場合、または構成しなかった場合、 Microsoft Defender ウイルス対策は、マルクエアの検出に対する処置 の実行を要求します。
	OK キャンセル 週用(<u>ム</u>)

<サービスの設定変更>

① 検索画面の検索バーに「サービス」と入力し、検索結果に表示された「サービス」をクリックします。

	፼ C ©
	最も一致する検索結果
	ジービス アプリ
	דלי
	コンポーネント サービス
	🍳 Microsoft Azure サービス
	設定 (2)
	「廿ービス」を入力
-	ר א א א א א א א א א א א א א א א א א א א

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。

18 サービス画面が起動されます。

🔍 サービス							-	×
ファイル(E) 操作(A)	表示(⊻) ヘルプ(∐)							
4 e 📄 🗖 🗖								
🤐 サーヒス (ローカル)	〇, サービス (ローカル)	-						
	項目を選択すると説明が表示されます。	名前 ^	説明	状態	スタートアップの種類	ログオン		
		ActiveX Installer (AxInstSV)	インタ		手動	Local S		- 1
		Agent Activation Runtime_9	Runti		手動	Local S		- 1
		🏟 AllJoyn Router Service	口一力		手動 (トリガー開始)	Local S		1
		🏟 App Readiness	ユーザ		手動	Local S		
		Application Identity	アプリ	実行中	自動 (トリガー開始)	Local S		
		Application Information	追加	実行中	手動 (トリガー開始)	Local S		
		🎑 Application Layer Gateway	インタ		手動	Local S		
		🏟 Application Management	グルー		手動	Local S		
		AppProtection Service	App		手動	Local S		
		🎑 AppX Deployment Service (Micr	実行中	手動 (トリガー開始)	Local S		
		🖏 AssignedAccessManager サ	Assig		手動 (トリガー開始)	Local S		
		🖏 AVCTP サービス	オーデ	実行中	手動 (トリガー開始)	Local S		
		🖳 Background Intelligent Tran	アイド	実行中	自動 (遅延開始)	Local S		
		Background Tasks Infrastruc	システ	実行中	自動	Local S		
		🧠 Base Filtering Engine	ベース	実行中	自動	Local S		
		SitLocker Drive Encryption	BDES	実行中	手動 (トリガー開始)	Local S		
		🖳 Block Level Backup Engine	WBE		手動	Local S		
		🧠 Bluetooth オーディオ ゲートウェ	Bluet	実行中	手動 (トリガー開始)	Local S		
		🔍 Bluetooth サポート サービス	Bluet	実行中	手動 (トリガー開始)	Local S		
		🧠 Bluetooth ユーザー サポート サ	Bluet	実行中	手動 (トリガー開始)	Local S		
		🍓 BranchCache	このサ		手動	Networ		
		CaptureService_96b7d78	Wind		手動	Local S		
		Certificate Propagation	ユーザ		手動 (トリガー開始)	Local S		
		🖏 Citrix Workspace Advanced	Keep	実行中	自動	Local S		
		Client License Service (ClipS	Micr	実行中	手動 (トリガー開始)	Local S		
		CNG Key Isolation	CNG	実行中	手動 (トリガー開始)	Local S		
		🔍 COM+ Event System	サポー	実行中	自動	Local S		
		COM+ System Application	コンポ		手動	Local S		
		🔍 ConfigMgr タスク シーケンス エ	タスク		手動	Local S		
		Q Configuration Manager リモ	許可		無効	Local S		
	1 1/2E (100/0E /	M Commented Designed Directory	7.0.44	专行手	는 문서 사람 2018년 AAN L	110		 _
	\144.0K/\194.0F/							

ノア1ル(E) 操TF(A)	表示(型) ヘルノ(日)								
♦ ♦ □ □	🗟 📑 🛛 🖬 👘 🕨 🖬 🖬 🕪								
🔍 サービス (ローカル)	サービス (ローカル) カ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・								
	DNS Client	名前	説明	状態	スタートアップの種類	ログオン			^
		🖏 Credential Manager	セキュ		手動	Local S			
	説明:	CredentialEnrollmentManag	資格		手動	Local S			
	り、このコンピューターのドメイン ネーム システ	Cryptographic Services	提供	実行中	自動	Networ			
	ム (DNS) 名がキャッシュされ、フル コンピュー	🖏 Data Sharing Service	アプリ		手動 (トリガー開始)	Local S			
	ター名が登録されます。サービスが停止され	DCOM Server Process Laun	DCO	実行中	自動	Local S			
	ると、DNS 名は引き続き解決されます。し	🖏 dcsvc	Decl		手動 (トリガー開始)	Local S			
	れず、コンピューター名は登録されません。	Q Delivery Optimization	コンテ		手動 (トリガー開始)	Networ			
	サービスが使用不可にされた場合、このサー	Device Association Service	システ		手動 (トリガー開始)	Local S			
	ビスに明示的に依存するサービスはすべて起	🏟 Device Install Service	ユーザ		手動 (トリガー開始)	Local S			
	一朝できなくなります。	🖏 Device Setup Manager	デバイ	実行中	手動 (トリガー開始)	Local S			
		DeviceAssociationBroker_46	Enab		手動	Local S			
		Applied the second seco	このユ		無効	Local S			
		DevQuery Background Disc	アプリ		手動 (トリガー開始)	Local S			
		A DHCP Client	このコ	実行中	自動	Local S			
		🖏 Diagnostic Policy Service	診断		自動 (遅延開始)	Local S			
		🏟 Diagnostic Service Host	Diag		手動	Local S			
		🏟 Diagnostic System Host	Diag		手動	Local S			
		🖏 Distributed Link Tracking Cli	ネット	実行中	自動	Local S			
		Distributed Transaction Coo	テータ		白動 (遅延開始)	Networ	1		
		DNS Client	DNS	実行中	自動 (トリガー開始)	Networ			
		Downloaded Maps Manager	ダウン	to da da da da da d	無効	Networ			
		🎑 Encrypting File System (EFS)	暗号		手動 (トリガー開始)	Local S			
		🖏 Enterprise App Managemen	エンタ		手動	Local S			
		🖏 Extensible Authentication P	拡張		手動	Local S			
		Runction Discovery Provider	FDP		手動	Local S			
		Sunction Discovery Resourc	このコ		手動 (トリガー開始)	Local S			
		Ceolocation Service	このサ		無効	Local S			
		🖏 GraphicsPerfSvc	Grap		無効	Local S			
		🖏 Group Policy Client	管理	実行中	自動 (トリガー開始)	Local S			
		Altachi Software RAID Service	Hitac	実行中	自動	Local S			~

¹⁹ 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。

② 「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。

全般 ログオン	回復 依存關係	
サービス名:	Dnscache	
表示名:	DNS Client	
説明:	DNS クライアント サービス (dnscache) により、このコンビ ーのドメイン ネーム システム (DNS) 名がキャッシュされ、フ ッピューター 名 が祭 録 され キオ・サービフ が 広 ル され スレ	コータ へ ルコ v
実行ファイルのパス:		
C:¥windows¥syst	em32¥svchost.exe -k NetworkService -p	
スタートアップの 種類(E):	自動	\sim
サービスの状態:	実行中	
	(高止(T)) (百) 面积	哥(<u>R</u>)
開始(<u>S</u>)	13-TT (T) 14-16-TT (E) 14-164	
開始(S) ここでサービスを開始	はするときに適用する開始パラメーターを指定してください。	
開始(<u>S</u>) ここでサービスを開始	きするときに適用する開始パラメーターを指定してください。	
開始(S) ここでサービスを開始 開始/「ラメーター(M	マエムロ マリテムビ マネ おするときに適用する開始パラメーターを指定してください。):	
開始(5) ここでサービスを開始 開始/(ラメーター(M	マエムロ マリテムビ マネ	

🔍 サービス							77 <u>.</u>	 ×
	まーへの ムルブ(山)							
🔕 サービス (ローカル)	〇 サービス (ローカル)							
	Function Discovery Resource	名前	説明	状態	スタートアップの種類	ログオン		^
	Publication	🧠 Credential Manager	セキユ		手動	Local S		
	サービスの開始	CredentialEnrollmentManagerUserSvc_46840	資格		手動	Local S		
	2 CAUBINE	Cryptographic Services	提供	実行中	自動	Networ		
		🖏 Data Sharing Service	アプリ		手動 (トリガー開始)	Local S		
		COM Server Process Launcher	DCO	実行中	自動	Local S		
	このコンビューダーおよびこのコンビューダーに 接続されている!!!!	🖏 desve	Decl		手動 (トリガー開始)	Local S		
	ワーク上で検出できるようにします。このサー	A Delivery Optimization	コンテ		手動 (トリガー開始)	Networ		
	ビスを停止するとネットワークリソースは公開	Device Association Service	システ		手動 (トリガー開始)	Local S		
	されなくなり、ネットワーク上の他のコンビュー	🖏 Device Install Service	ユーザ		手動 (トリガー開始)	Local S		
	ダーかこれらのリゾースを使出されなくなりま	🥋 Device Setup Manager	デバイ	実行中	手動 (トリガー開始)	Local S		
	5.	DeviceAssociationBroker_46840	Enab		手動	Local S		
		🖏 DevicePicker_46840	このユ		無効	Local S		
		🧟 DevQuery Background Discovery Broker	アプリ		手動 (トリガー開始)	Local S		
		🖏 DHCP Client	このコ	実行中	自動	Local S		
		🖏 Diagnostic Policy Service	診断		自動 (遅延開始)	Local S		
		🦓 Diagnostic Service Host	Diag		手動	Local S		
		🥘 Diagnostic System Host	Diag		手動	Local S		
		Client Distributed Link Tracking Client	ネット	実行中	自動	Local S		
		Contraction Coordinator	データ		自動 (遅延開始)	Networ		
		🖏 DNS Client	DNS	実行中	自動 (トリガー開始)	Networ		
		🖏 Downloaded Maps Manager	ダウン		無効	Networ		
		Carl Encrypting File System (EFS)	暗号		手動 (トリガー開始)	Local S		
		Characterise App Management Service	エンタ		手動	Local S		
		ktensible Authentication Protocol	拡張		手動	Local S		
		Kinction Discovery Provider Host	FDP		手動	Local S		
		Function Discovery Resource Publication	このコ		手動(トリガー開始)	Local S		
		Geolocation Service	201		無効	Local S		
		CraphicsPerfSvc	Grap		無効	Local S		
		🖏 Group Policy Client	管理	実行中	自動 (トリガー開始)	Local S		
		Altachi Software RAID Service	Hitac	実行中	自動	Local S		~

② 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。

22 「スタートアップの種類(<u>E</u>):」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。

サービス名: FDResPub 表示名: Function Discovery Resource Publication 説明: このコンビューターおよびこのコンビューターに接続されているジリン スを公開して、キットワーク上で特徴できるようにします。このた	
表示名: Function Discovery Resource Publication 説明: このコンピューターおよびこのコンピューターに接続されているリン スを公開して、ネットワーク上で検出できるようにします。このた	
説明: このコンピューターおよびこのコンピューターに接続されているリソ スを公開して、ネットワーク上で検出できるようにします。この5	
_ビフを広止オスレネットローク IN 1-7け小胆さわたくたり さ	Ŷ
実行ファイルのパス: C:¥windows¥system32¥svchost.exe -k LocalServiceAndNoImpersonation -	р
スタートアップの 自動 種類(E):	~
サービスの状態: 停止	
開始(<u>S</u>) 停止(<u>D</u>) 一時停止(<u>P</u>) 再開(<u>R</u>)	
ここでサービスを開始するときに適用する開始パラメーターを指定してください。	
間始/(ラメーター(M):	

サービス								
ワイル(<u>F</u>) 操作(<u>A</u>)	表示(<u>V</u>) ヘルプ(<u>H</u>)							
→ □ □ □ □	🗟 📓 🔝 🕨 💷 💷 🕪							
サービス (ローカル)	○ サービス (ローカル)							
	SSDP Discovery	名前	説明	状態	スタートアップの種類	ログオン		
	22	Security Accounts Manager	このサ	実行中	自動	Local S		
	説明:	Sensor Data Service	各種		無効	Local S		
	SSDP 発見ノロトコルを使用する、UPnP テ パイフたどのネットローク デパイフやサービフ	Sensor Monitoring Service	データ		手動 (トリガー開始)	Local S		
	を検出します。また、ローカル コンピューターで	Sensor Service	さまざ…		手動 (トリガー開始)	Local S		
	実行中の SSDP デバイスを表示します。サー	Server	207	実行中	自動 (トリガー開始)	Local S		
	ビスを停止すると、SSDP ベースのデバイスは	Shared PC Account Manager	Man	201	ab (1775 1871) 無効	Local S		
	横出されません。サービスを無効にすると、このサービスにあった。	Shell Hardware Detection	自動	実行中	白動	Local S		
	始できません。	Smart Card	207		手動 (トリガー開始)	Local S		
		Smart Card Device Enumeration Service	指定		無効	Local S		
		Smart Card Removal Policy	ユーザ		手動	Local S		
		SNMP #-PZ	簡易		手動	Local S		
		SNMP トラップ	口-力		手動	Local S		
		Software Protection	Wind		自動(遅延開始、ト	Networ		
		Special Administration Console Helper	管理		手動	Local S		
		Spot Verifier	771		手動(トリカー開始)	Local S		
		SSDP Discovery	SSDP		無効	Local S		
		State Repository Service	ולק	宝行中	自動	LocalS		
		Still Image Acquisition Events	静止		手動	Local S		
		Storage Service	ストレ	実行中	自動 (遅延開始、ト	Local S		
		Storage Tiers Management	システ		手動	Local S		
		🖏 SysMain	長期	実行中	自動	Local S		
		System Event Notification Service	システ	実行中	自動	Local S		
		A System Events Broker	WinR	実行中	自動 (トリガー開始)	Local S		
		🥋 System Guard ランタイム モニター ブローカー	Wind		手動 (トリガー開始)	Local S		
		🖏 Task Scheduler	ユーザ	実行中	自動	Local S		
		CP/IP NetBIOS Helper	ネット		手動 (トリガー開始)	Local S		
		A Telephony	テレフ		手動	Networ		
		🖏 Themes	テーマ	実行中	自動	Local S		
		🖏 Time Broker	WinR	実行中	手動 (トリガー開始)	Local S		
		Keyboard and Handwriting Panel Se	タッチ	実行中	手動 (トリガー開始)	Local S		

23 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。

(2) 「スタートアップの種類(<u>E</u>):」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。

	,,.,.,.,	
全般 ログオン	回復 依存關係	
サービス名:	SSDPSRV	
表示名:	SSDP Discovery	
説明:	SSDP 発見プロトコルを使用する、UPnP デバイスなどのネット ワーク デバイスやサービスを検出します。また、ローカル コンビュー ターで書行曲の SSDD デバイフを専デドキオ サービフを体止	Ŷ
実行ファイルのパ C:¥windows¥sy	것: stem32¥svchost.exe -k LocalServiceAndNoImpersonation -	р
スタートアップの	白動	
種類(<u>E</u>):		*
種類(E): サービスの状態:	停止	
種類(E): サービスの状態: 開始(S)	停止 停止① 一時停止(2) 再關(B)	-
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	停止 停止(T) 一時停止(P) 再開(B) 1953ときに適用する開始パラメーターを指定してください。	-
建填(E): サービスの状態: 開始(S) ここでサービスを開 開始/(ラメーター(停止 停止(① 一時停止(₽) 再開(<u>β</u>) 約453ときに適用する開始パラメ−タ−を指定してください。 M):	

🔍 サービス							21 <u>_</u> 25	×
ファイル(<u>F</u>) 操作(<u>A</u>)	表示(V) ヘルプ(H)							
🗢 🏟 📰 🖾 🧔) 🛃 🛛 📷 🛛 🕨 💷 🖬 🕩							
サービス (ローカル)	○ サービス (ローカル)							
	UPnP Device Host	名前	説明	状態	スタートアップの種類	ログオン		
		Software Protection	Wind		自動(遅延開始、ト	Networ		
	説明:	Special Administration Console Helper	管理		手動	Local S		
	このコンヒューダー上での UPnP ナハイスの不 フトを可能にします。サービフを停止すると	Spot Verifier	771		手動 (トリガー開始)	Local S		
	ホストされている UPnP デバイスは機能しな	SSDP Discovery	SSDR		無効	Local S		
	くなり、ホストされるデバイスを追加すること	State Repository Service	アプリ	実行中	自動	Local S		
	もできません。サービスを無効にすると、明示	Still Image Acquisition Events	静止	201	手動	Local S		
	旳にこのサービスに依存しているサービスは開 やぶきか/かります	Storage Service	ストレー	実行中	自動 (遅延開始, ト	Local S		
	28 C C & V & 7 & 9 &	Storage Tiers Management	*ZT		≤ in (22200/4(100) ≤ 動	Local S.,		
		SvsMain	長期	実行中	自動	Local S		
		System Event Notification Service	システ	実行中	自動	Local S		
		System Events Broker	WinR	実行中	自動 (トリガー開始)	Local S		
		System Guard ランタイム モニター ブローカー	Wind		手動 (トリガー開始)	Local S		
		Task Scheduler	ユーザ	事行中	自動	Local S		
		CP/IP NetBIOS Helper	ネット		手動 (トリガー開始)	Local S		
		A Telephony	テレフ		手動	Networ		
		🖏 Themes	₹-₹	実行中	自動	Local S		
		Time Broker	WinR	室 行中	手動 (トリガー開始)	Local S		
		Touch Keyboard and Handwriting Panel Se	タッチ	実行中	手動 (トリガー開始)	Local S		
	L F	Udk User Service_46840	シェル		手動	Local S	1	
		UPnP Device Host	このコ		無効	Local S		
		User Access Logging Service			自動 (遅延閉始)	Local S		
		🖏 User Data Access_46840	構造		手動	Local S		
		🖏 User Data Storage_46840	構造		手動	Local S		
		🔅 User Manager	ユーザ	実行中	自動 (トリガー開始)	Local S		- 17
		Q User Profile Service	このサ	実行中	自動	Local S		
		🖏 Virtual Disk	ディス		手動	Local S		
		Wolume Shadow Copy	パック		手動	Local S		
		WalletService	ウォレ		無効	Local S		
		Warp JIT Service	Enab		手動 (トリガー開始)	Local S		
		Web アカウント マネージャー	このサ	実行中	手動	Local S		~
	↓ 壮建 √ 槽榫 /			1999 (00/71/MI/75)	anaasiii			130

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。

²⁰ 「スタートアップの種類(<u>E</u>):」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。

AL -	Hater.	-	(+ + 99 m)	
L MR	1079	凹復	依仔閣係	
サービス名	i:	upr	nphost	
表示名:		UPr	nP Device Host	
説明:		この 。サ 19月1)コンピューター上での UPnP デバイスのホストを可能にします トービスを停止すると、ホストされている UPnP デバイスは機 」かくかり ホフトされろデバイフを追加するフンキできキサム	< >
実行7ァ1	ามดกว	ζ :		
C:¥winde	ows¥sv	stem32¥	evchost eve -k Local Service And Nolmpersonation -n	
	,		sectosace reconstruction personation p	_
スタートア: 種類(E):	ップの	自調	b	~
スタートア [・] 種類(<u>E</u>):	ップの	b i	かいのsieler k exemperationingerationation p 動	~
スタートア [・] 種類(E): サービスの	ップの 状態:	自調	b	~
スタートア [・] 種類(E): サービスの 開	ップの 状態: 始(<u>S</u>)	停止	BD BD 停止(① 一時停止(2) 再關(R)	~
スタートア・ 種類(E): サービスの 開ジ ここでサー	ップの 状態: 哈(S) ビスを開	自調停止	b	~
スタートア・ 種類(E): サービスの 開設 ここでサー 開始/(ラ;	ップの 状態: 始(S) ビスを開 メーター(J)	自 停止 始すると? √):	b b b 使止(I) 一時停止(P) 再開(B) きに適用する開始パラメーターを指定してください。	~

20 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。