Windows11 24H2 にアップデートしたら 共有フォルダが開けない時の修正方法 (測量プログラムが起動出来ない時も該当します。)

1. Windows マークを右クリックして ファイル名を指定して実行 をクリックします



2. 名前のところに gpedit.msc と入力してOKをクリックします。



 コーカルグループポリシーエディターが開くので、左側ペインの コンピューターの構成→管理用テンプレート→ネットワークを展開して Lanman ワークステーションをクリックします。

(ル(F) 操作(A) 表示(V) ヘルプ(H)			
* 2 🗊 🔒 🛛 🗊 🖓			
ーカルコンピューター ポリシー	ワークステーション		
コンビューダーの構成 項目を選択する	と説明が表示されます。	設定	状態
Windows の設定		目 代替ポートマッピング	未構成
管理用テンプレート			未構成
> Mindows コンポーネント		ーー	未構成
> 🗂 コントロール パネル		■ 監査サーバーが署名をサポートしていない	未構成
🚰 サーバー		E NTLM (LM、NTLM、NTLMv2) をブロックする	未構成
> 📫 システム			未構成
> 🦳 タスク バーと [スタート] メニュー		🗈 暗号の順位	未構成
iii デスクトップ		E SMB 圧縮を無効にする	未構成
✓ ²⁰ ネットワーク		E SMB over QUIC サーバー例外リストを無効にしました	未構成
BranchCache		ご 代替ポートを有効にする	未構成
DirectAccess クライアント エク		🗈 既定で SMB 圧縮を使用する	未構成
DNS 757 72F		🗈 継続的可用性共有でのキャッシュを処理します	未構成
		🔄 安全でないゲスト ログオンを有効にする	未構成
Lanman ()-()()-()()		リモートメールスロットを有効にする	未構成
	圧クリツク	🗈 継続的可用性共有上のオフライン ファイルの可用性	未構成
SNMP		E QUIC 経由で SMB を有効にする	未構成
SSL 權成設定		E SMB の最大バージョンを義務付ける	未構成
> ☐ TCPIP 設定		FI CMD の早小げ_パーパーンは主教分ける	± ## ##

4. 右側ペインにある

安全でないゲスト ログオンを監査する をダブルクリックします。

項目を選択すると説明が表示されます。	。 設定	状態
	三 代替ポート マッピング	未構成
	田 安全でないゲストログオンを監査する	未構成
	□目 監査リーバーは項号化をリバートしていません ■ 監査サーバーが署名をサポートしていない	未構成
	 E NTLM (LM、NTLM、NTLMv2)をブロックする E NTLM サーバー禁止例外一覧 	② ダブルクリッ
	 : 暗号の順位	未構成
	 E SMB 圧縮を無効にする	未構成
	🗈 SMB over QUIC サーバー例外リストを無効にしました	未構成
		未構成
	🔝 既定で SMB 圧縮を使用する	未構成
	🗈 継続的可用性共有でのキャッシュを処理します	未構成
	🗉 安全でないゲスト ログオンを有効にする	未構成
	🗉 リモート メールスロットを有効にする	未構成
	🗈 継続的可用性共有上のオフライン ファイルの可用性	未構成
	📄 QUIC 経由で SMB を有効にする	未構成
	EI SMB の最大バージョンを義務付ける	未構成
	■ CMD の早示パージョンを主教付ける	土堆帚

5. 無効を選択してOKをクリックします。

🕵 安全でないゲスト ログオンを監査する		×
〒 安全でないゲスト ログオンを監査する	前の設定(P) 次の設定(N)	
○ _{未構成(C)} コメント:		A
○ 有効(E)		
● 無効(D)		Ŧ
トされるバージョン: Windows	s Server 2025 以降または Windows 11 以降	*
③ 無効を選択 —		Ψ.
オプション:	ヘルプ:	
	このボリシーでは、SMB クライアントがケスト アカウントとしてログオンにとき に、SMB クライアントが監査イベントを有効にするかどうかを制御します。 このポリシー設定を有効にした場合、SMB クライアントはクライアントがゲス ト アカウントとしてログオンしたときにイベントをログに記録します。 このポリシー設定を無効にするか、未構成にした場合、SMB クライアントは イベントをログに記録しません。	~
	OK キャンセル 適用(A)	
	④ OKをク	IJ

6. 同様に右側ペインにある

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ます。



7. 有効を選択してOKをクリックします。

ヨ 安全でないゲスト ログオンを有効にす	13
	前の設定(P) 次の設定(N)
○ 未構成(C) コメント:	*
● 有 %J(E) ○ 無効(D)	
6 有効を	 送訳 Server 2016 以降または Windows 10 以降
オプション:	ヘルプ:
	このポリシー設定では、SMB クライアントが SMB サーバーへの安全でない ゲスト ログオンを許可するかどうかを決定します。 このポリシー設定を有効にした場合、またはこのポリシー設定を構成しなか
	った場合、SMB クライアントは安全でないケストロクオンを許可します。
	った場合、SMB クライアントは安全でないケストロクオンを許可します。 このポリシー設定を無効にした場合、SMB クライアントは安全でないゲスト ログオンを拒否します。
	った場合、SMB クライアントは安全でないゲストロクオンを許可します。 このポリシー設定を無効にした場合、SMB クライアントは安全でないゲスト ログオンを拒否します。 署名を有効にした場合、SMB クライアントは安全でないゲストログオンを 拒否します。
	った場合、SMB クライアクトは安全でないケストロクオンを許可します。 このポリシー設定を無効にした場合、SMB クライアントは安全でないゲスト ログオンを拒否します。 署名を有効にした場合、SMB クライアントは安全でないゲストログオンを 拒否します。 安全でないゲストログオンがファイル サーバーによって使用されるのは、共有 フォルダーに対する認証されていないアクセスを許可することが目的です。エ ンタープライズ環境では一般的ではありませんが、ファイル サーバーとして動 作しているコンシューマー NAS (ネットワーク接続ストレージ) アプライアンスで は、安全でないゲストログオンが頻繁に使用されています。Windows ファ イル サーバーでは認証を要求し、既定では安全でないゲストログオンを使 用しません。安全でないゲストログオンは認証されていないため、SMB 署 名、SMB 暗号化などの重要なセキュリティ機能が無効になります。結果と

8. 設定ができましたら×をクリックしてローカルグループポリシーエディターを閉じます。

ローカル グループ ポリシー エディター			—		×
rイル(F) 操作(A) 表示(V) ヘルプ(H)					
🔶 🖄 📷 🔒 👔 🖬 🝸					
 ◇ 「 ネットワーク BranchCache DirectAccess クライアント I: DNS クライアント LAN Manager サーパー LAN Manager サーパー Link-Layer Topology Discc > ○ QoS パケット スケジューラ SNMP SSL 構成設定 > ○ TCPIP 設定 Windows 接続マネージャー > ○ Windows 接続マネージャー > ○ WWAN サービス WUAN サービス WWAN サービス WWAN サービス ネットワーク プロパイダー ネットワーク 分離 パックグラウンドインテリジェン マオント 	.anman ワークステーション 選択すると説明が表示されます。	 設定 E: 代替ボートマッピング E: 安全でないゲストログオンを監査する E: 監査サーバーは暗号化をサポートしていません E: 監査サーバーは暗号化をサポートしていない E: NTLM (LM、NTLM、2)をブロックする E: NTLM サーバー禁止例外一覧 E: 暗号の順位 E: SMB 圧縮を無効にする E: SMB cmaを無効にする E: SMB cmaを使用する E: 継続的可用性共有でのキャッシュを処理します E: 安全でないゲストログオンを有効にする E: WHEの用を有効にする E: WHEの用 E: UFL+トメールスロットを有効にする E: WHEの用性共有でのキャッシュを処理します E: 安全でないゲストログオンを有効にする E: WHEの用 E: UFL+レスロットを有効にする E: WHEの目用性共有とのオフラインファイルの可用性 E: QUIC 経由で SMB を有効にする E: SMB の最大パージョンを義務付ける E: SMB の最大パージョンを義務付ける E: SMB の最大パージョンを美務(ける) 		状 未 無未未未未未未未未未有未未未未生 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	

続いてローカルセキュリティーポリシーの設定を行います。

9. Windows マーク右クリックで ファイル名を指定して実行を開く をクリックします。



10. 名前のところに secpol.msc と入力してOKをクリックします。

💷 771)	し名を指定して実行	×	
	実行するブログラム名、または開くフォルダーやドキュメ ネットリソース名を入力してください。	ント名、インター	
名前(0):	secpol.msc	~	
			③ secpol.msc と入力
	OK ++>>セル	参照(B)	
•		。 OK を左ク	リック

10. ローカルセキュリティーポリシーが開くので、左側ペインの

ローカルポリシーを展開してセキュリティーオプションをクリックします。



11. 右側ペインにある

Microsoft ネットワーク クライアント: サードパーティ SMB サーバーへの接続に、 暗号化されていないパスワードを送信する をダブルクリックします。

12. 有効を選択してOKをクリックします。

-カル セ	キュリティの設定 Missacath ネ	説明	L. +- L' 1 [*] -= /4	NO CMP #_ If.	0.017			
	ワードを、暗号	パリーク クライアラ 化しないで送信す	5	EU SIND 9-71-	NUNX			
0	有効(E)	J						
0	無効(S)	⑧ 有	ī効を選	択				
						$O U \neq .$	БЛ Б	

同様に右側ペインにある以下のポリシーを設定します。

- 13. Microsoft ネットワーク クライアント: サーバーが同意すれば、通信にデジタル署名を行 う をダブルクリックして無効を選択してOKをクリックます。
- 14. **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 して無効を選択してOKをクリックします。
- 15. 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 をダブルクリックして無効を選択してOKをクリックします。

	ポリシー ^	セキュリティの設定
	闘 DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ	未定義
		未定義
47	🌉 Microsoft ネットワーク クライアント: サード パーティ製の SMB サーバ	有効
	🔤 Microsoft ネットワーク クライアント: サーバーが同意すれば、通信に	無効
Windows Defer	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
ジャー ポリシー	📖 Microsoft ネットワーク サーバー: S4U2Self を試行して要求情報を	未定義
	📓 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	無効
<u>シ</u> ー	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
ý−	📖 Microsoft ネットワーク サーバー: セッションを中断する前に、ある―	未定義
ローカル コンピュータ	□ □ Microsoft ネットワーク サーバー: ログオン時間を超過するととクライア	有効
凱成	闘 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
	- 🔤 アカウント: Administrator アカウントの状態	無効
	闘 アカウント: Administrator アカウント名の変更	Administrator
	📓 アカウント: Guest アカウントの状態	無効
	闘 アカウント: Guest アカウント名の変更	Guest
	│ アカウント: ローカル アカウントの空のパスワードの使用をコンソール ログ	無効
	闘 アカウント:Microsoft アカウントをブロックする	未定義
	闘 システム オブジェクト: Windows システムではないサブシステムのため	有効
	🖏 システム オブジェクト: 内部のシステム オブジェクトの既定のアクセス許	有効
	🖏 システム暗号化: コンピューターに保存されているユーザー キーに強力な	未定義
	🖏 システム暗号化: 暗号化、ハッシュ、署名のための FIPS 準拠アルゴリ	無効
	📖 システム設定: オプション サブシステム	
_	IIII シフテル設定・ソフトウェア創成のポリシーのために Windows 宇行可	毎劫

*機種によっては既に有効や無効に設定されている場合もあります。

16. 設定ができましたら×をクリックしてローカルセキュリティーポリシーを閉じます。

🖥 ローカル セキュリティ ポリシー		_	\times
ファイル(F) 操作(A) 表示(V) ヘルプ(H)			
🗢 🔿 🙍 📰 🗙 🗟 🔢 🖬			
セキュリティの設定 アカウント ポリシー ローカル ポリシー 国ーカル ポリシー 国生 コーザー権利の割り当て セキュリティオブション セキュリティオブション セキュリティオブション マガレーク リスト マネージャー ポリシー 公開キーのポリシー ソフトウェアの制限のポリシー アブリケーション制御ポリシー アブリケーション制御ポリシー 目や セキュリティ ポリシー (ローカル コンピュータ) 監査ポリシーの詳細な構成	 ポリシー DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ Microsoft ネットワーク クライアント: サード パーティ製の SMB サーパ Microsoft ネットワーク クライアント: サーバーが同意すれば、通信に 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 Microsoft ネットワーク サーバー: S4U2Self を試行して要求 情報を 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 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 Microsoft ネットワーク サーバー: ウーバー: SPN ターゲット名検証レベル Microsoft ネットワーク サーバー: セッションを中断する前に、あるー Microsoft ネットワーク サーバー: ログオン時間を超過するととクライア 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 アカウント: Administrator アカウントの状態 アカウント: Guest アカウントへの変更 アカウント: ローカル アカウントの空のパスワードの使用をコンソール ログ アカウント: Dーカル アカウントをブロックする システム オブジェクト: 時部のシステム オブジェクトの既定のアクセス許 システム暗号化: コンピューターに保存されているユーザーキーに強力な ジステム時号化: 暗号化、バッシュ、署名のための FIPS 準拠アルゴリ 	セキュリテイの設定 未未有無奈 気効効 素 気効 気力 た 定 効 効 定 効 の 定 定 効 効 の 定 定 定 効 の の 定 定 定 効 の の 定 定 定 効 の の 定 定 定 効 の の 定 の の の 定 定 定 の 効 の の 定 定 定 効 の の の 定 定 定 効 の の の 定 定 定 効 の の 定 の の 定 の の の 定 定 定 の の の の	
	IIII シフテム設定・ソフトウェア制限のポリシーのために Windows 実行可	無効	

17. ネットワークに接続できるか確認します。

接続できない時はパソコンを再起動して再度接続できるか確認します。 念のためネットワーク接続したいパソコン(サーバー側)のパソコンも再起動します。

それでもネットワークに接続出来なかったり、ネットワークの資格情報の入力画面が表示される 場合は「資格情報の登録」が必要になります。

これにはユーザー様の環境によって対処が異なりますので、次ページに様々な対処を記載しますので該当する対処を行って下さい。

資格情報を入力する際に<u>ネットワーク接続したいパソコン(サーバー側)</u>のログインユーザー名、 パスワード、場合によってはパソコン名が必要になりますので先に確認しておきます。

注意:ネットワーク接続したいパソコン(サーバー側)での作業になります。

ログインユーザー名の確認(Windows11)

Windows ボタンをクリックして表示されたメニューの下側に記載してあるのが ユーザー名です。



ログインユーザー名の確認(Windows10)

スタートボタンをクリックして表示されたメニューの左側にある小さいマークの一番上にある 人のマークにマウスを移動させるとユーザー名が表示されます。



パスワードの確認

パスワードは接続したいパソコン(サーバー)の起動時に入力しているパスワードです。 パスワードを入力しないで起動できている場合はパスワードが空欄になります。

プライバシーの関係でパスワードが分からない場合は接続先パソコンの管理者(使用者)に 後で資格情報入力時にパスワードを入力して頂きます。

パソコン名の確認

Windows マーク右クリックで システムをクリックします。



表示されたメニューのデバイス名欄がパソコン名になります。

	10.00 M			
设定の検索 Q.	All Dis Diff and Differen	e%.	この PC の名前を	変更
A-4	 デバイスの仕様 		כאל-	^
システム				
Bluetooth とデバイス	テハイス名	12th Cap late//D) Cape/TMJ i7 12700 210 CHz		
Judetobar C//T/X	アロビフタ 実装 RAM	32.0 GB (31.7 GB 使用可能)		
▼ ネットワークとインターネット	デバイス ID	14E89B3C-C00F-45E3-93EE-3DD2E85963E0		
/ 個人用設定	プロダクト ID	00355-61585-85617-AAOEM		
	システムの種類	64 ビット オペレーティング システム、x64 ペース プロセッサ		
1 アプリ	ベンとタッチ	このディスプレイでは、ベン入力とタッチ入力は利用できません		
アカウント				
3 時刻と言語	関連リンク ドメインまた	はワークグループ システムの保護 システムの詳細設定		
ブーム	Windows の仕様		コピー	1
🗴 アクセシビリティ				
· · · · · · · · · · · · · · · · · · ·	エディション	Windows 11 Pro		
ノフィハシーとセキュリティ	バージョン	24H2		
Windows Update	インストール日	2025/02/15		
	OS EILF	26100.3194		
	シリアル番号	JPH420216J		

ネットワーク接続したいパソコン(サーバー側)のユーザー名、パスワード、パソコン名が 確認できましたら資格情報の設定を行います。 デスクトップに共有フォルダへのショートカットがありショートカットをクリックすると Windows セキュリティーが表示される時

- 1. 共有フォルダへのショートカットをダブルクリックします。
- ネットワークの資格情報の入力画面が表示された場合は 接続先のパソコンにログインしているユーザー名とパスワードを入力して 資格情報を記憶するに

Windows セキュリティ ネットワーク資格情報の入力	×
次に接続するための資格情報を入力してください:	192.168.0.200
1-ザー名	① ユーザー名を入力
パスワード	
資格情報を記憶する	2) パスリードを人力 設定していない時は空欄
アクセスが拒否される	
ОК	<u>キャンヤル</u> ④ 左クリック

接続側のパソコンでパスワードを設定していない場合は入力しない(空欄)で大丈夫です。

3. OKをクリックした後に共有フォルダが開ければ設定完了です。

共有フォルダへのショートカットが無い場合

1. Windows マークを右クリックして ファイル名を指定して実行をクリックします



 ¥¥の後に接続したいPC名(サーバー名)を全て半角で入力してOKをクリックします。 (画像では server というパソコンに接続したい時です。)

💷 ファイ)	レ名を指定して実行 ×
	実行するプログラム名、または開くフォルダーやドキュメント名、インター ネットリソース名を入力してください。
名前(O):	¥#server ③ ¥¥パソコン名
	OK キャンセル 参照(B)
	④ 左クリック

 ネットワークの資格情報の入力画面が表示された場合は 接続先のパソコンにログインしているユーザー名とパスワードを入力して 資格情報を記憶するに☑をいれてOKをクリックします。

Windows セキュリティ	×
ネットワーク資格情報の入力	
次に接続するための資格情報を入力してください: 1	92.168.0.200
1-ザー名	
パスワード	
資格情報を記憶する	6 パスワードを入力 設定していない時は空欄
アクセスが拒否さ ⑦ 日を入れる	
ОК	キャンセル
	⑧ 左クリック

OKをクリックした後に共有フォルダが開ければ設定完了です。

資格情報を入力してOKをクリックしてもエラーが表示される場合

接続しようとしているパソコン(サーバー側)がパスワード設定を行っていない場合が多いです。

注意:ネットワーク接続したいパソコン(サーバー側)での作業になります。

1. デスクトップにネットワークアイコンがある時はネットワークアイコンを右クリックします。



2. プロパティーをクリックします。



3. ネットワークを共有センターの画面が表示されますので

左側にある 共有の詳細設定の変更 をクリックします。



4. 共有の詳細設定画面が表示されたら すべてのネットワーク をクリックします。

← 設定		- 0 ×		
Tsukahara ローカル アカウント	… > ネットワークの詳細設定 > 共有の詳細設定			
設定の検索 Q	ブライベート ネットワーク	\checkmark		
↑ ホ-ム	パブリック ネットワーク	現在のプロファイル へ		
■ システム ⑧ Bluetooth とデバイス	ネットワーク探索 お使いの PC はネットワーク上の他のデバイスを検出したり、他のデバイスで検出されたりします	オン 💽		
┃ 💎 ネットワークとインターネット	ファイルとブリンターの共有 ネットワーク上の他のユーザーがこのデバイスの共有ファイルやブリンターにアクセスすることを許可す	する オン 💽		
🥖 個人用設定				
🖹 アプリ	すべてのネットワーク			
💄 アカウント				
🕥 時刻と言語	@ ヘルガを表示 ④ 左ク	フリック		
● プーム	▶ フィードバックの送信			
🏋 アクセシビリティ				
🖤 プライバシーとセキュリティ				
O Windows Update				

5. 下にメニューが展開されてきますので、一番下のパスワード保護共有をオフにします。

(Windows10の時は無効にするの方を選択します。)

ネットワーク上の他のユーザーがこのデバイスの共有ファイルやプリンター	にアクセスすることを許可する オン 👥
すべてのネットワーク	^
パブリック フォルダーの共有 ネットワーク上の他のユーザーにバブリック フォルダー内のファイルの読み	*取りと書き込みを許可する オフ ●
ファイル共有の接続 128 ビット暗号化をサポートするデバイスに使用する	128 ビット暗号化 (推奨) 🗸
<mark>パスワード保護共有</mark> この PC のユーザー アカウントとパスワードを持つユーザーのみが、共有 ルダーにアクセスできます	ファイル、プリンター、パブリック フォ オフ 💽
	⑤ オフに変更する

6. 設定が出来ましたら×ボタンをクリックしてメニューを閉じます。

	… > ネットワークの詳細設定 > 共有の詳細設定		
設定の検索 Q	ブライベート ネットワーク		~
☆ ホーム	パブリック ネットワーク	現在のプロファイル	^
■ システム ⑧ Bluetooth とデバイス	ネットワーク探索 お使いの PC はネットワーク上の他のデバイスを検出したり、他のデバイスで検出されたりします	לא 🌑	
▼ ネットワークとインターネット	ファイルとフリンターの共有 ネットワーク上の他のユーザーがこのデバイスの共有ファイルやプリンターにアクセスすることを許可する	לא 🔿	
🥖 個人用設定 👔 アブリ	すべてのネットワーク		^
 アカウント 	パブリック フォルダーの共有 ネットワーク上の他のユーザーにパブリック フォルダー内のファイルの読み取りと巻き込みを許可する	オフ ()	
 時刻と言語 ゲーム 	ファイル共有の接続 128 ビット暗号のをサポートするデバイスに使用する 128 ビット暗号	号化 (推奨) 🏻 🗸	
★ アクセシビリティ	パスワード保護共有 このPC のユーザーアカウントとバスワードを持つユーザーのみが、共有ファイル、プリンター、バブリック フォ	7 7 💽	
ブライバシーとセキュリティ	ルターにアクセスできます		

接続出来なかったパソコンから共有フォルダが開けるか確認をします。

