中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料

設定解説資料
（Windows リモートデスクトップ）

ver1.0（2023.07）

本書は、総務省の調査研究事業により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）
総務省 サイバーセキュリティ統括官室
Email telework-security@ml.soumu.go.jp
URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

1 はじめに

(ア) 本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目について、Windows リモートデスクトップを利用しての具体的な作業内容の解説をすることで、管理者が実施すべき設定作業や利用者が利用時に実施すべき作業の理解を助けることを目的としています。

(イ) 前提条件

利用するエディションやバージョンにより使用可能な機能が異なります。**本資料では Window 10 Pro（バージョン 1909）の利用を前提としております。**

(ウ) 本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者（これらに準ずる役割を担っている方を含みます）を対象として、その方々がチェックリスト項目の具体的な対策を把握できるよう、第 2 章ではチェックリスト項目に紐づけて解説内容と解説ページを記載しています。本書では第 3 章にて管理者向けに、第 4 章では利用者向けに設定手順や注意事項を記載しています。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責事項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および注意事項の解説が記載されたページを記載しています。
3 管理者向け設定作業	対象のチェックリスト項目に対する管理者向けの設定手順や注意事項を解説しています。
4 利用者向け作業	対象のチェックリスト項目に対する利用者向けの設定手順や注意事項を解説しています。

(エ) 免責事項

本資料は現状有姿でご利用者様に提供するものであり、明示であると黙示であるとを問わず、正確性、商品性、有用性、ご利用者様の特定の目的に対する適合性を含むその他の保証を一切行うものではありません。本資料に掲載されている情報は、2022 年 11 月 29 日時点の各製品の操作画面を基に作成しており、その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。本製品をご利用者様の業務環境で利用する際には、本資料に掲載している設定により業務環境システムに影響がないかをご利用者様の責任にて確認の上、実施するようにしてください。本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

2 チェックリスト項目に対応する設定作業一覧

本書で解説しているチェックリスト項目、対応する設定作業解説および注意事項が記載されているページは下記のとおりです。

表 2. チェックリスト項目と管理者向け設定作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
8-4 データ保護 **テレワーク端末には原則として重要情報を保管しないよう周知する。万一その必要性が生じた場合には、パスワードの設定やファイルの暗号化を実施し、一時的な保管のみを許可する。ただし、端末に会社のデータを保管しない場合を除く**	・リモートデスクトップ接続端末間でのファイル転送無効化	P.6
9-1 アカウント・認証管理 **テレワーク端末のログインアカウントや、テレワークで利用する各システムのパスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。**	・ログインパスワードポリシー設定	P.1010
9-3 アカウント・認証管理 **テレワーク端末やテレワークで利用する各システムに対して一定回数以上パスワードを誤入力した場合、それ以上のパスワード入力を受け付けないよう設定する。**	・ログインパスワードポリシー設定	P.1313

表 3. チェックリスト項目と利用者向け作業の紐づけ

チェックリスト項目番号	対応する設定作業	ページ
5-4 脆弱性管理 **テレワーク端末から社内にリモートアクセスするための VPN 機器等には、メーカーサポートが終了した製品を利用せず、最新のセキュリティアップデートを適用する。**	・最新のセキュリティアップデート	P.1515
7-3 インシデント対応・ログ管理 **テレワーク端末からオフィスネットワークに接続する際のアクセスログを収集する。**	・リモートデスクトップ接続のアクセスログ確認リモートデスクトップ接続のアクセスログ確認	P.1818
9-2 アカウント・認証管理 **テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。**	・初期パスワード設定変更	P.2525

3 管理者向け設定作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目のうち、本製品の管理者が実施すべき対策の設定手順や注意事項を記載します。

3-1　チェックリスト 8-4 への対応

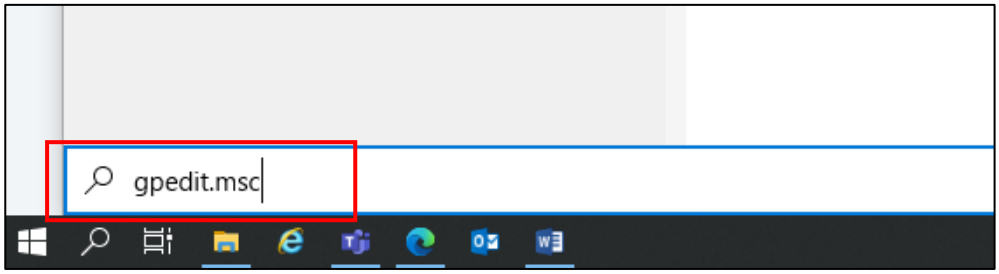
3-1-1　リモートデスクトップ接続端末間でのファイル転送無効化

リモート接続を行う端末間でファイルの転送が出来てしまうと、接続元端末へデータを持ち出すことができてしまうため、情報漏えいのリスクが高まります。**リモートデスクトップ接続における端末間のファイル転送を禁止することで情報漏えいのリスクを低減できます。**

リモートデスクトップ接続時の端末間のファイル転送の禁止設定

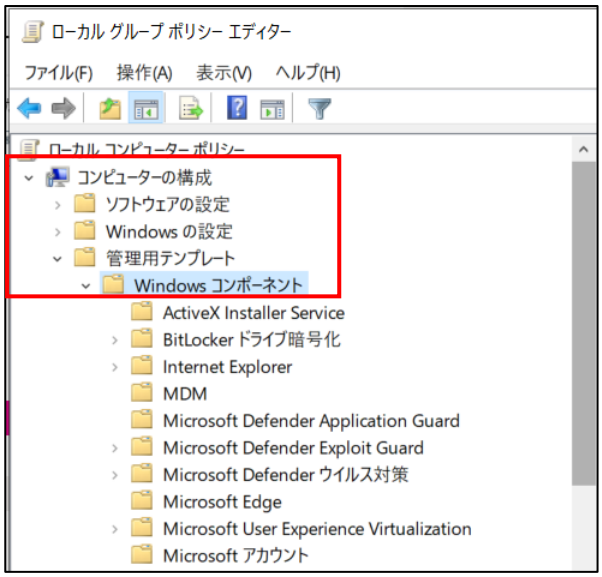
以下の手順は、AD（Active Directory）ドメイン環境ではない場合に、リモート接続先となる端末 1 台ずつに設定する手順です。
AD ドメイン環境の場合は、AD サーバーで管理されている対象端末に対し、設定を一括で適用することができます。
そのため、AD ドメイン環境の場合は、AD サーバーで以下に記載するポリシーを有効にしたグループポリシーオブジェクト（GPO）を作成することを推奨します。AD ドメイン環境下でのグループポリシーの作成については、AD ドメイン環境構築した担当者にご確認ください。

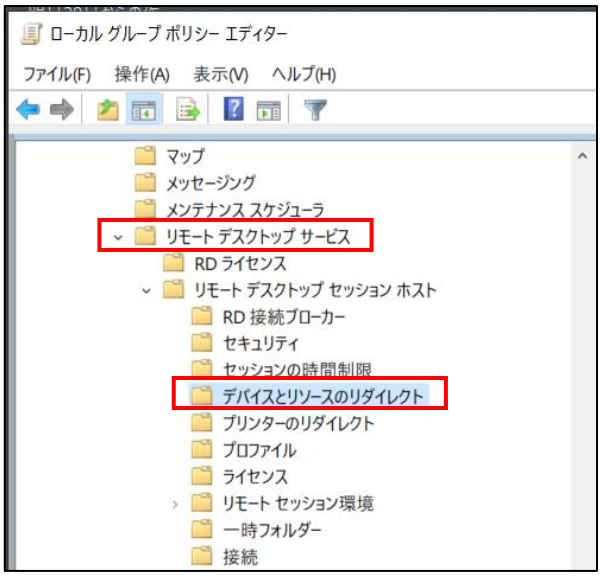
【手順①】
スタートメニュー右側の検索ボックスに「gpedit.msc」と入力し、Enter キーを押下します。



【手順②】

「ローカルグループポリシーエディター」から、左ペインで「ローカル コンピュータ ポリシー」-「コンピュータの構成」-「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」を順に選択します。

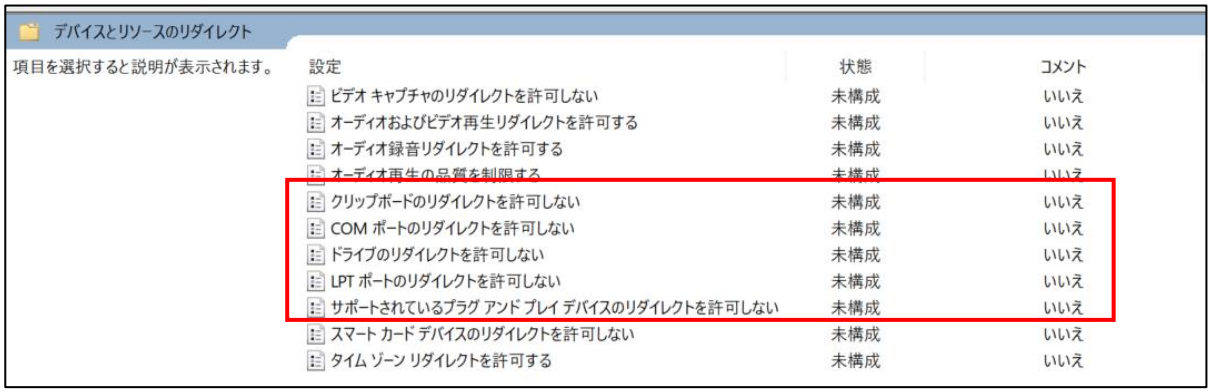


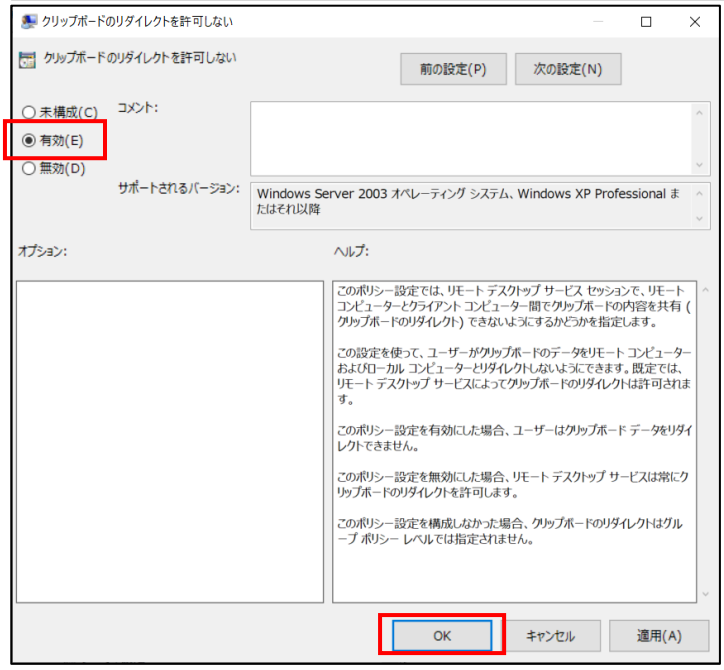


【手順③】

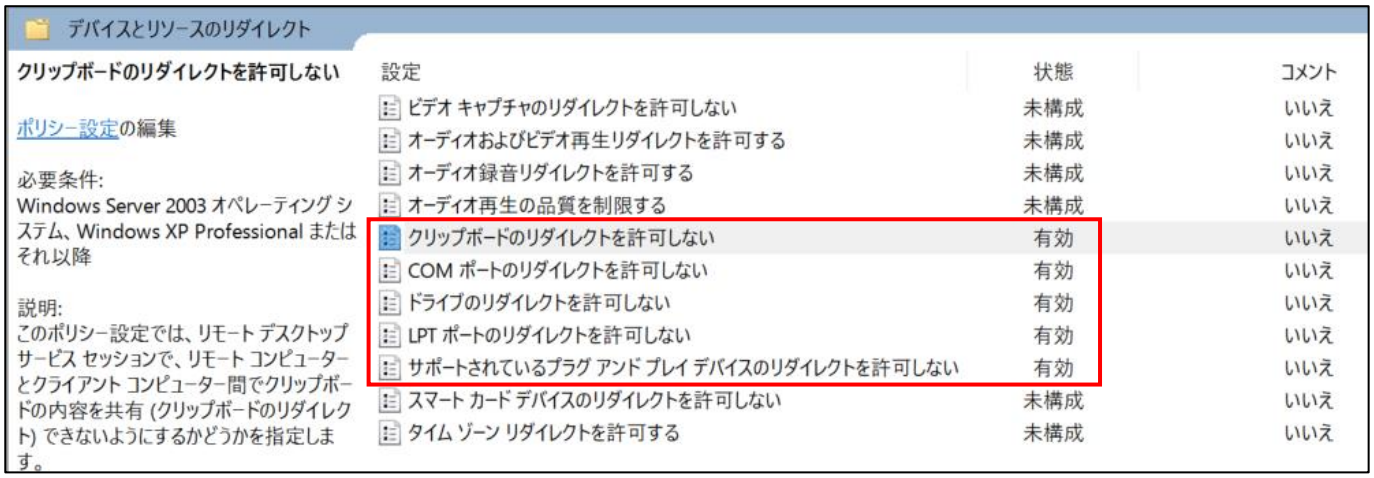
右側に表示される設定項目から、以下の項目をそれぞれ開き、「有効」を選択後、「OK」をクリックします。

- クリップボードのリダイレクトを許可しない
- COM ポートのリダイレクトを許可しない
- ドライブのリダイレクトを許可しない
- LPT ポートのリダイレクトを許可しない
- サポートされているプラグアンドプレイ デバイスのリダイレクトを許可しない



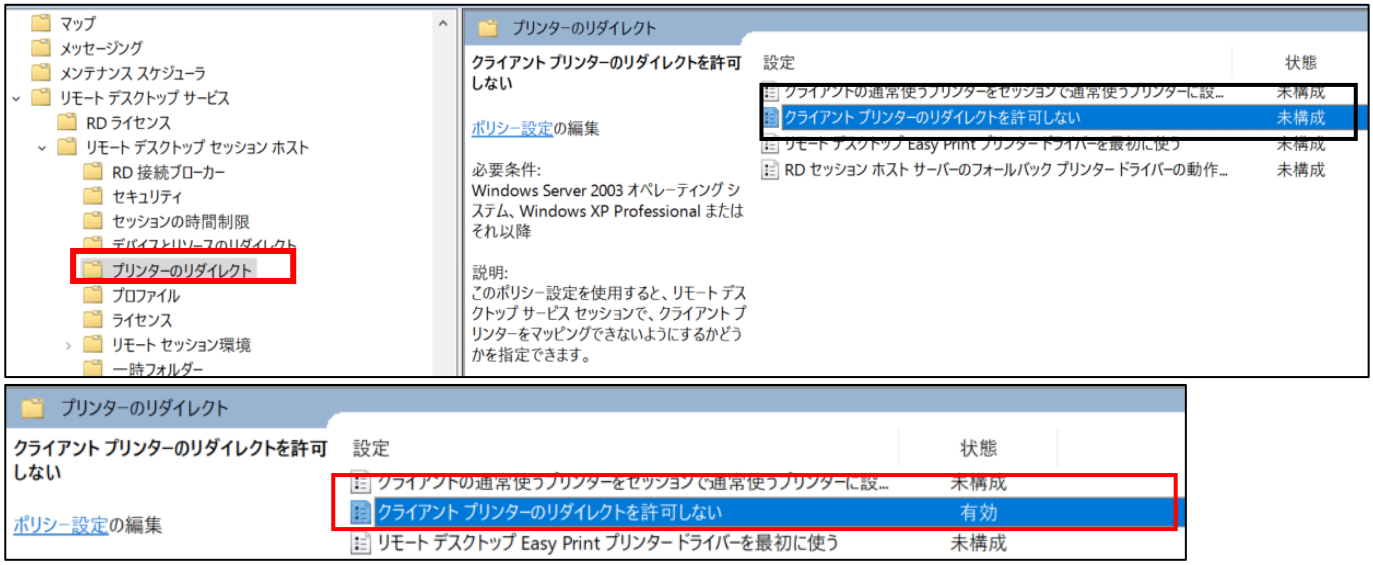


上記 5 項目を有効化すると、以下のように「状態」が「有効」になります。



【手順④】

「デバイスとリソースのリダイレクト」と同じ階層にある「プリンターのリダイレクト」を選択し、右側の「クライアントプリンターのリダイレクトを許可しない」をクリック後、「有効」にチェックを入れ、「OK」をクリックします。



【手順⑤】

設定を反映させるために端末を再起動します。

3-2　チェックリスト 9-1 への対応

3-2-1　　ログインパスワードポリシー設定

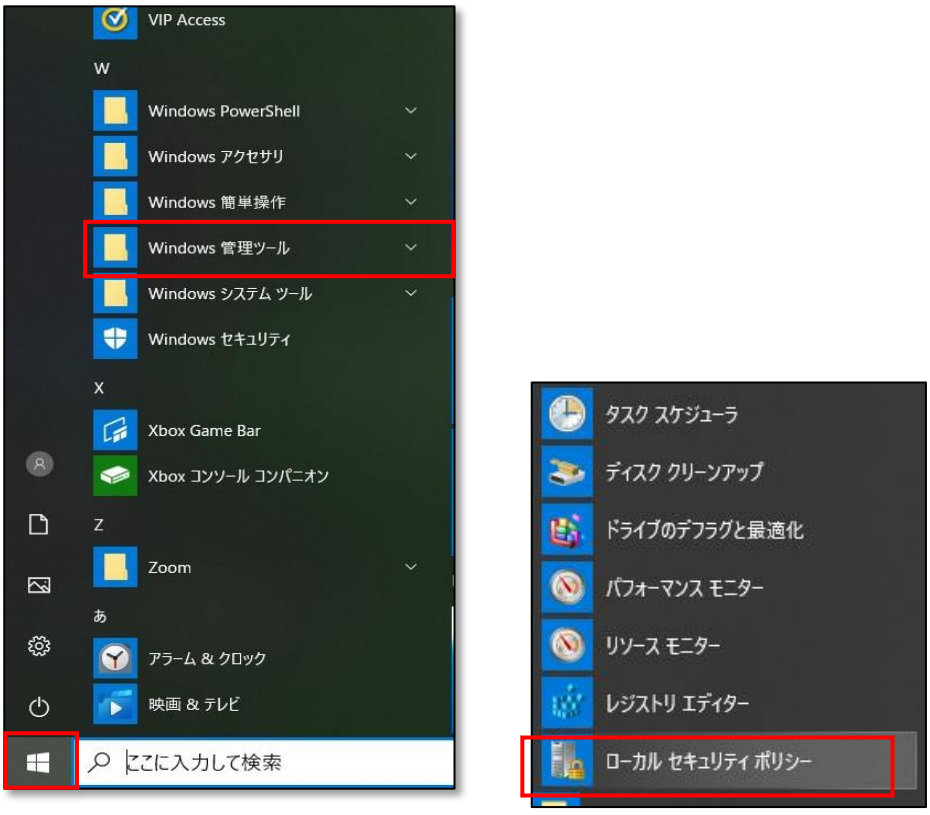
この項目では端末へログインするためのパスワード設定を行います。パスワードポリシーを設けることで推測されやすいパスワードを利用者が設定することを防ぎ、**悪意のある第三者から不正アクセスされるリスクを低減**します。

ログインパスワード設定

本手順は、外部認証ツールを使用していない場合のパスワードポリシーの設定手順です。Active Directory 等の外部認証ツールを利用している場合は、使用しているツールの設定方法をご参照ください。

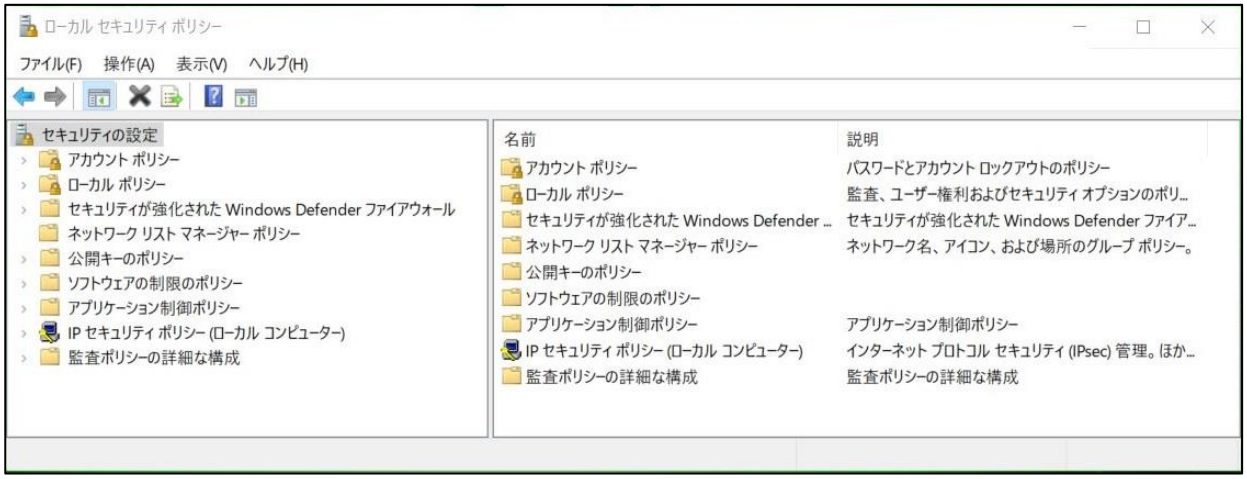
【手順①】

画面左下の Windows スタートメニューをクリックし、「Windows 管理ツール」-「ローカルセキュリティポリシー」-「ローカルセキュリティポリシー」をクリックします。



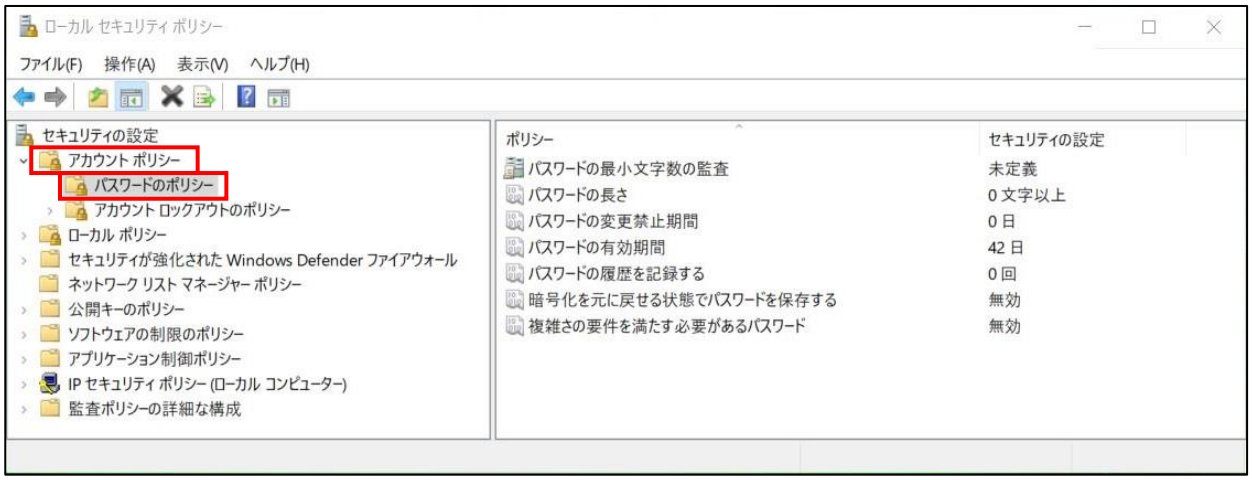
【手順②】

「ローカルセキュリティポリシー」をクリックすると、Windows のセキュリティ設定を行える「ローカルセキュリティポリシー」の画面が表示されます。



【手順③】

左ペインにある「アカウントポリシー」をダブルクリックし、「パスワードのポリシー」を選択後、右ペインにパスワードに関するポリシー設定画面が表示されます。



【手順④】

パスワードのポリシー画面は各項目をダブルクリックすることで設定することができます。パスワードの長さと複雑性に焦点を当てた項目の設定方法を記載します。

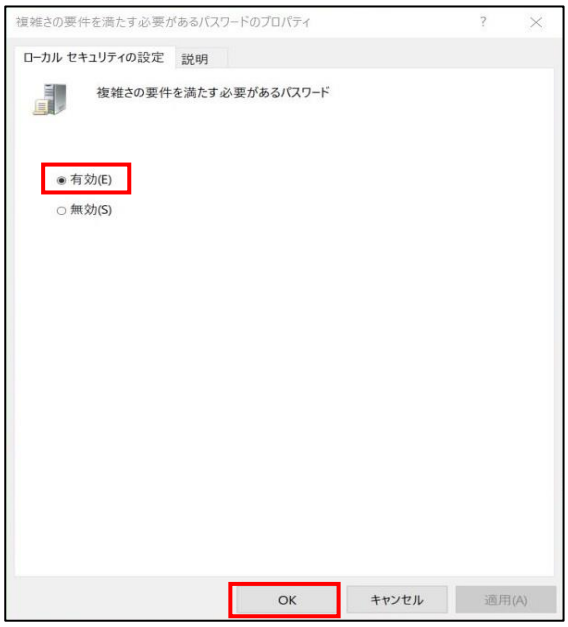
- パスワードの長さ

この設定ではユーザーカウントのパスワードに使用できる最小文字数を決定できます。設定後、「OK」をクリックします。

- 複雑さの要件を満たす必要があるパスワード

この設定を有効にすることで Windows の既定ポリシーとして次の 4 種類のうち 3 種類を組み合わせてパスワードを設定することを強制できます。

- 英大文字（A から Z）
- 英子文字（a から z）
- 10 進数の数字（0 から 9）
- アルファベット以外の文字（!、$、#、%など）



3-3　チェックリスト 9-3 への対応

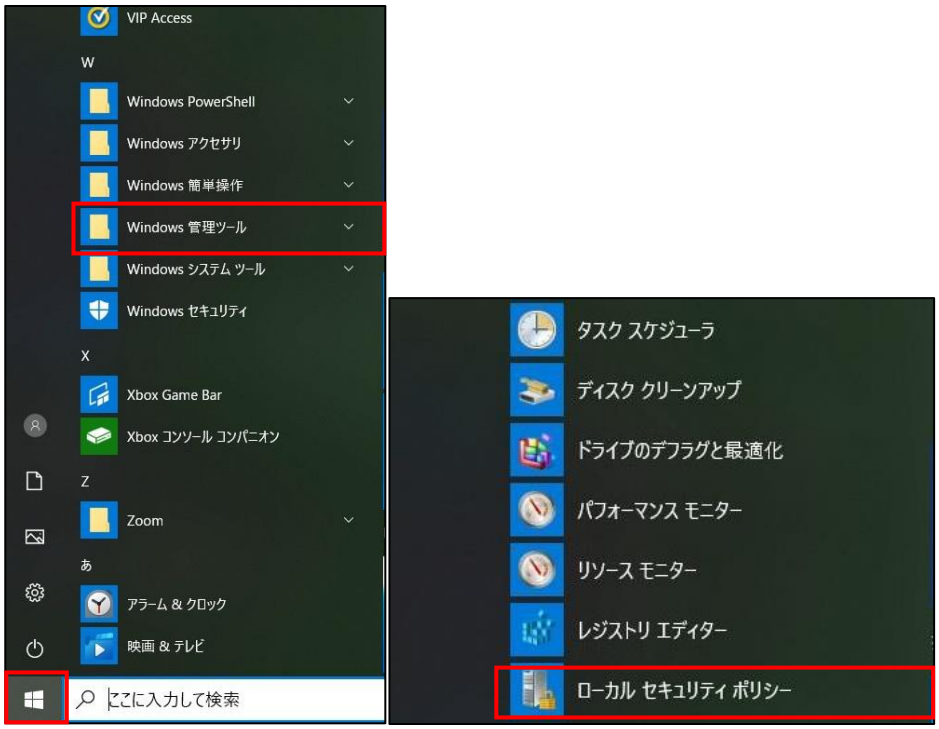
3-3-1　　アカウントロックアウト設定

パスワード入力を一定回数以上間違えるとパスワードを入力できない状態にする、ロックアウト設定を行います。ロックアウト設定を行うことで、**悪意のある第三者にパスワード解除されるリスクを低減**することができます。

以下の手順は、外部認証ツールを使用していない場合のパスワードポリシー設定手順です。Active Directory 等の外部認証ツールを利用している場合は、使用しているツールの設設定方法をご参照ください。

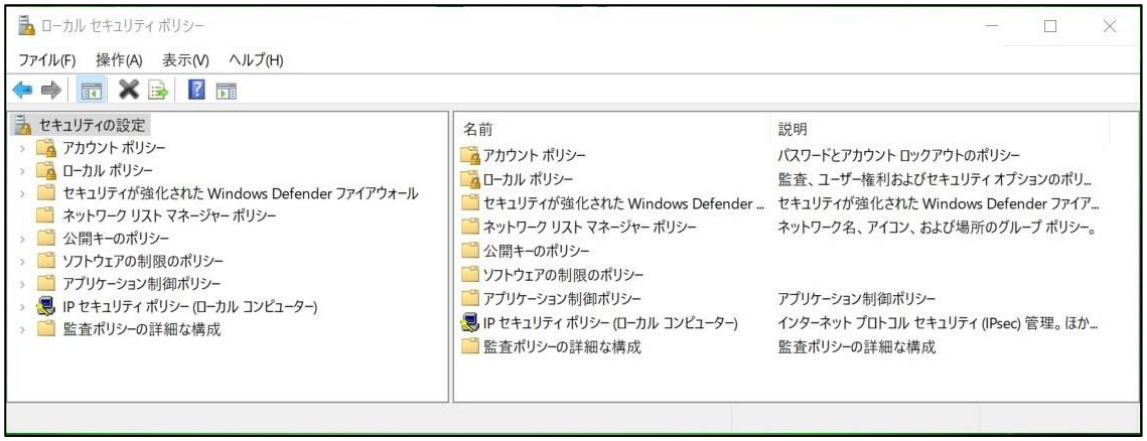
【手順①】

画面左下の Windows スタートメニューをクリック-「Windows　管理ツール」をクリック-「ローカルセキュリティポリシー」をクリックします。



【手順②】

「ローカルセキュリティポリシー」をクリックすると Windows のセキュリティ設定を行えるローカルセキュリティポリシー画面が表示されます。

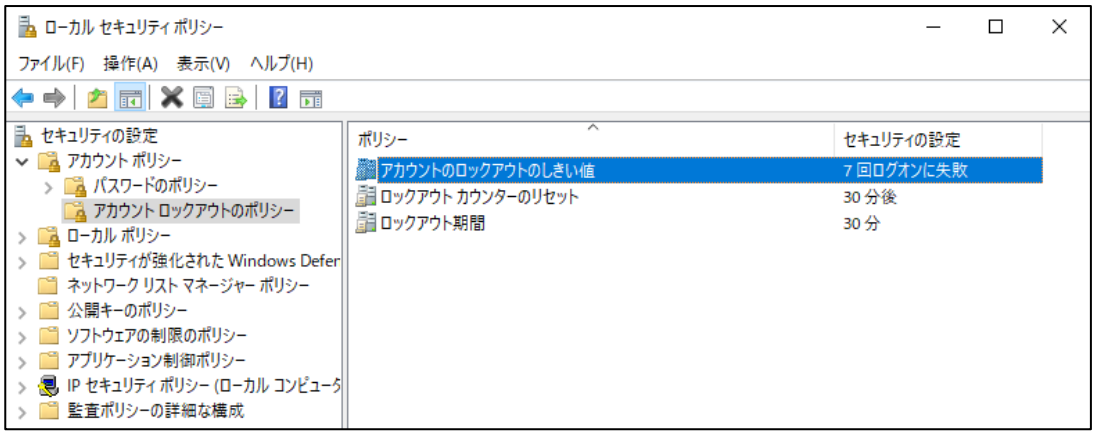


【手順③】

左ペインにある「アカウントポリシー」をダブルクリックし、「アカウントロックアウトのポリシー」を選択するとアカウントロックアウトに関するポリシーの設定画面が表示されます。

【手順④】

アカウントのロックアウトしきい値やロックアウト期間を設定します。以下は、「アカウントのロックのしきい値」を 7 回、「ロックアウトカウンターのリセット」を 30 分、「ロックアウト期間」を 30 分にした場合です。



注意事項

オフィスにある端末の管理に関して

テレワーク時に、Windows リモートデスクトップを利用してオフィスにある端末に接続する場合、意図しない当該端末の移動や持出し等が発生しないよう、端末管理を徹底してください。

４利用者向け作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第２部に記載されているチェックリスト項目のうち、本製品の利用者が実施すべき対策の設定手順や注意事項を記載します。

４-１　チェックリスト 5-4 への対応

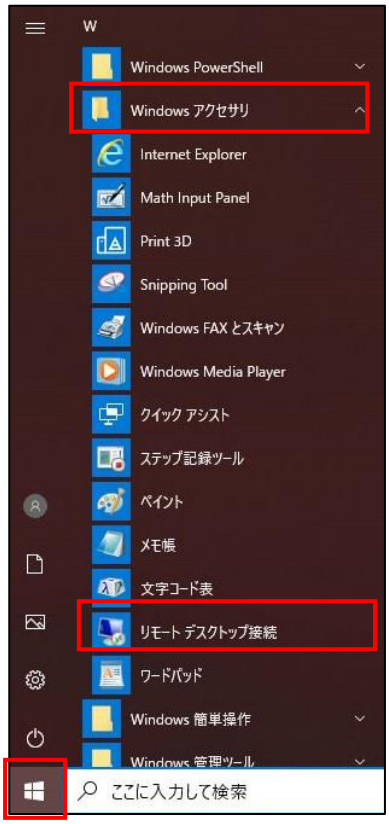
４-１-１　　最新のセキュリティアップデート

製品提供元からリリースされている最新バージョンのアプリケーションを利用します。最新バージョンを利用することは、アプリケーションの**脆弱性をついたサイバー攻撃に対して有効な対策となる**ため、定期的にアップデートがないか確認をすることを推奨します。
Windows Update により、Windows リモートデスクトップのセキュリティアップデートも適用されるため、Windows Update を自動でインストールする設定にしておくことを推奨します。
Windows リモートデスクトップや Windows のアップデートは、アプリケーションの更新機能、各製品の公式 HP 等で確認するか、対象製品の取引のある SI ベンダーや代理店に確認を行ってください。

ここでは、現在のリモートデスクトップのバージョンを確認する方法及び、Windows Update の自動インストールの設定方法について記載します。

貸与端末のリモートデスクトップ接続バージョン確認

【手順①】
左下 Windows アイコンの「スタート」をクリック後、「Windows アクセサリ」の「リモートデスクトップ接続」をクリックします。



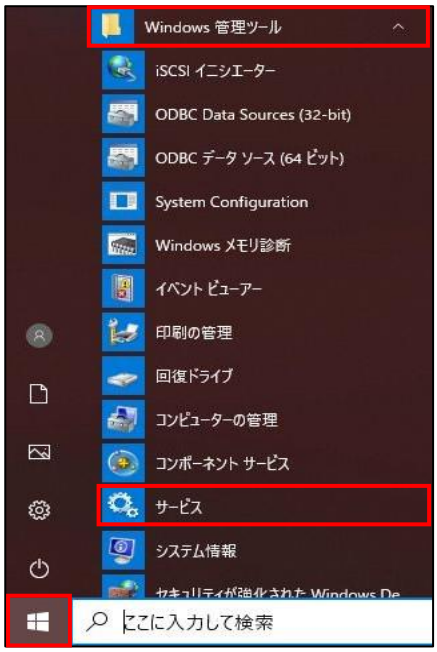
【手順②】

リモートデスクトップ接続画面左上のアイコンを右クリックし、「バージョン情報」をクリックします。

Windows Update の自動インストール設定

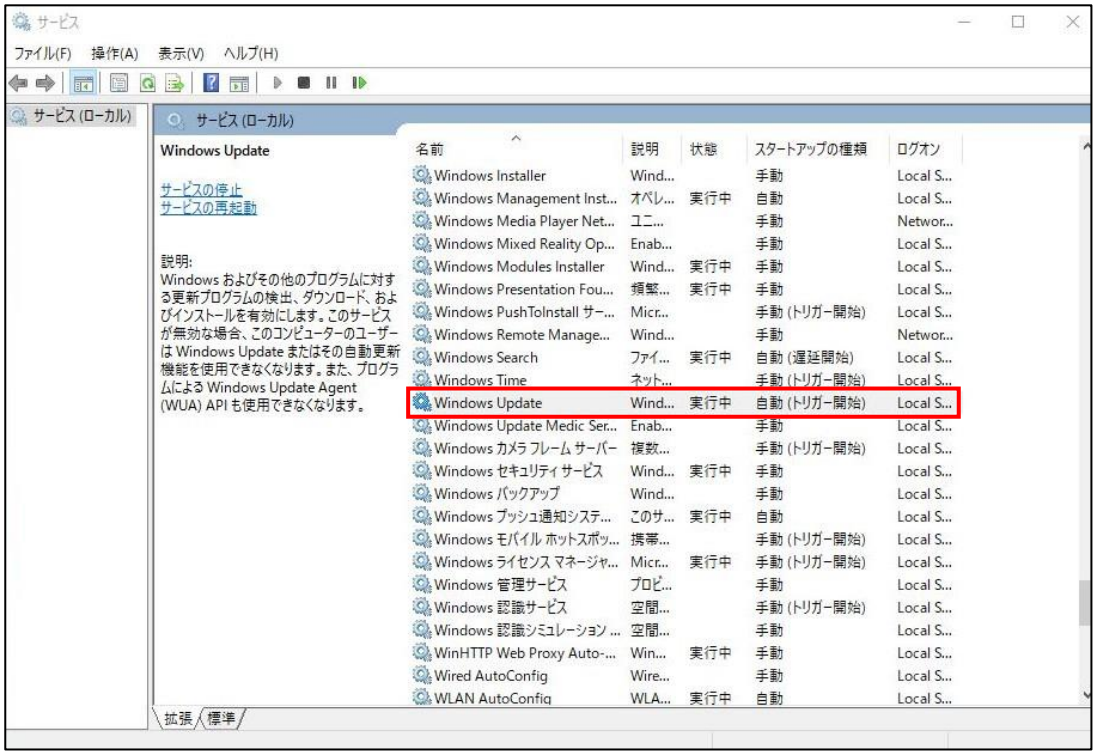
【手順①】

Windows 画面左下のスタートをクリック後、「Windows 管理ツール」-「サービス」をクリックします。



【手順②】

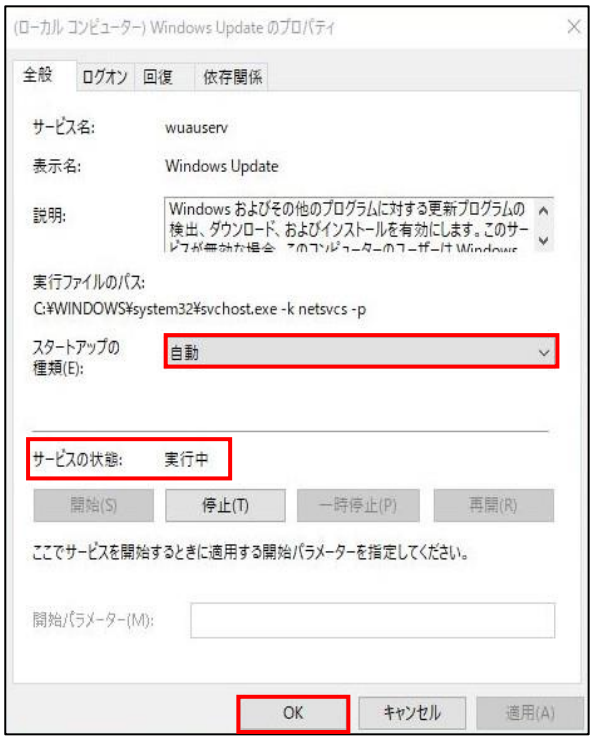
サービス（ローカル）一覧の中にある「Windows Update」をダブルクリックします。



【手順③】

「全般タブ」にあるスタートアップの種類が「自動」になっており、サービスの状態が「実行中」となっていることを確認します。
自動になっていない場合は、「スタートアップの種類」を「自動」に変更します。また「サービスの状態」が「停止中」の場合は、「開始」をクリックします。

「OK」をクリックして設定終了です。



4-2　チェックリスト 7-3 への対応

4-3-1　　リモートデスクトップ接続のアクセスログ確認

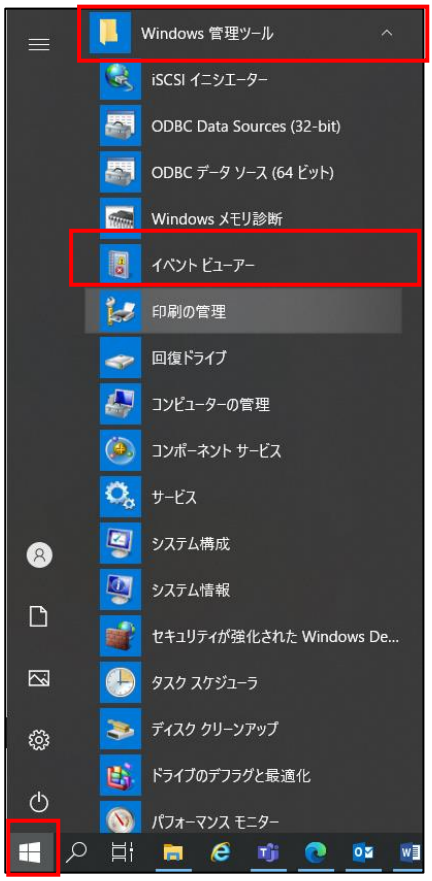
リモートデスクトップ接続先の端末に、身に覚えのないリモートからのログオンがないか確認します。リモートデスクトップ接続時には Window にログが出力されます。自身が行ったアクセスかどうか確認するため、接続先端末と接続元端末両方のログを確認し、自身の操作によって出力されたログであることを確認します。確認の結果、他の端末から接続先の端末へリモートデスクトップサービスによるログオンが疑われる場合、速やかにリモートデスクトップ先端末のパスワードを変更し、管理者に連絡してください。

接続先端末のログ確認：Windows セキュリティログによるリモートデスクトップ接続時のログオンログの確認

接続先の端末上で、下記手順により、リモートデスクトップ接続経由での「ログイン」のログを確認します。

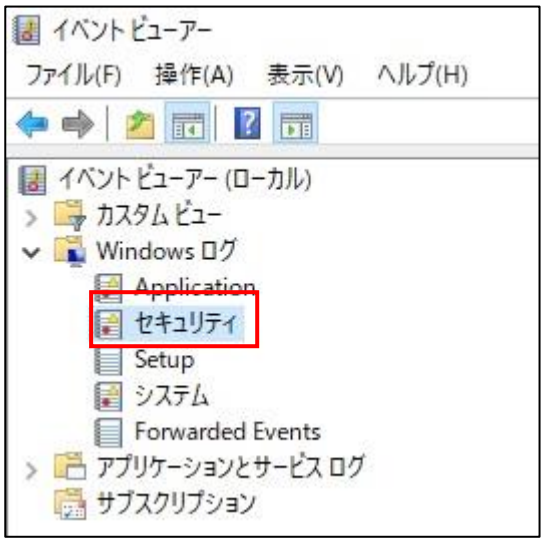
【手順①】

「スタート」をクリックし、「管理ツール」を開き、「イベントビューアー」をクリックします。



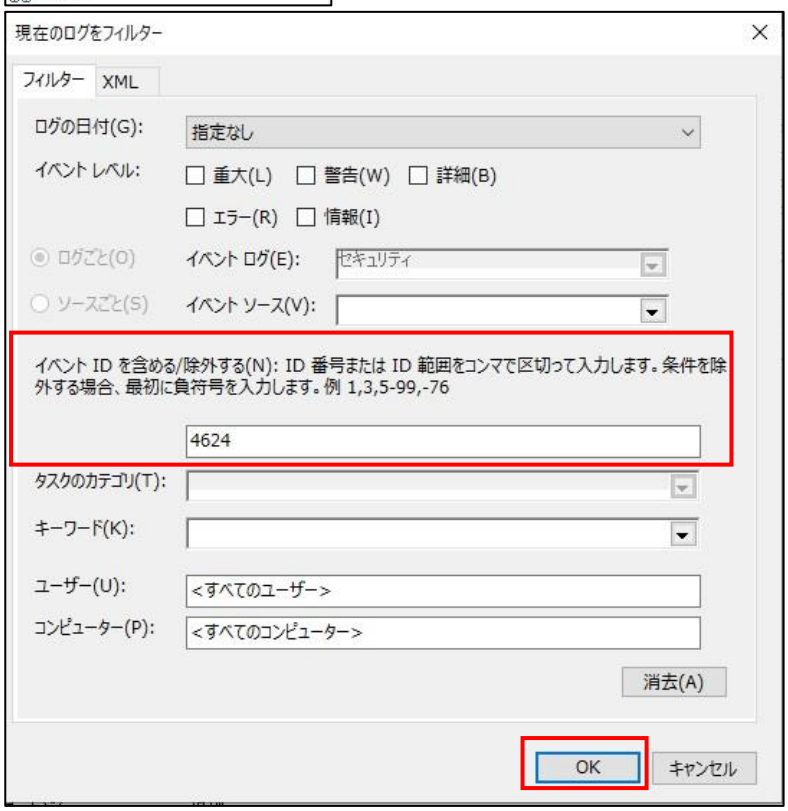
【手順②】

左ペインより「イベントビューアー（ローカル）」-「Windows ログ」-「セキュリティ」を選択します。



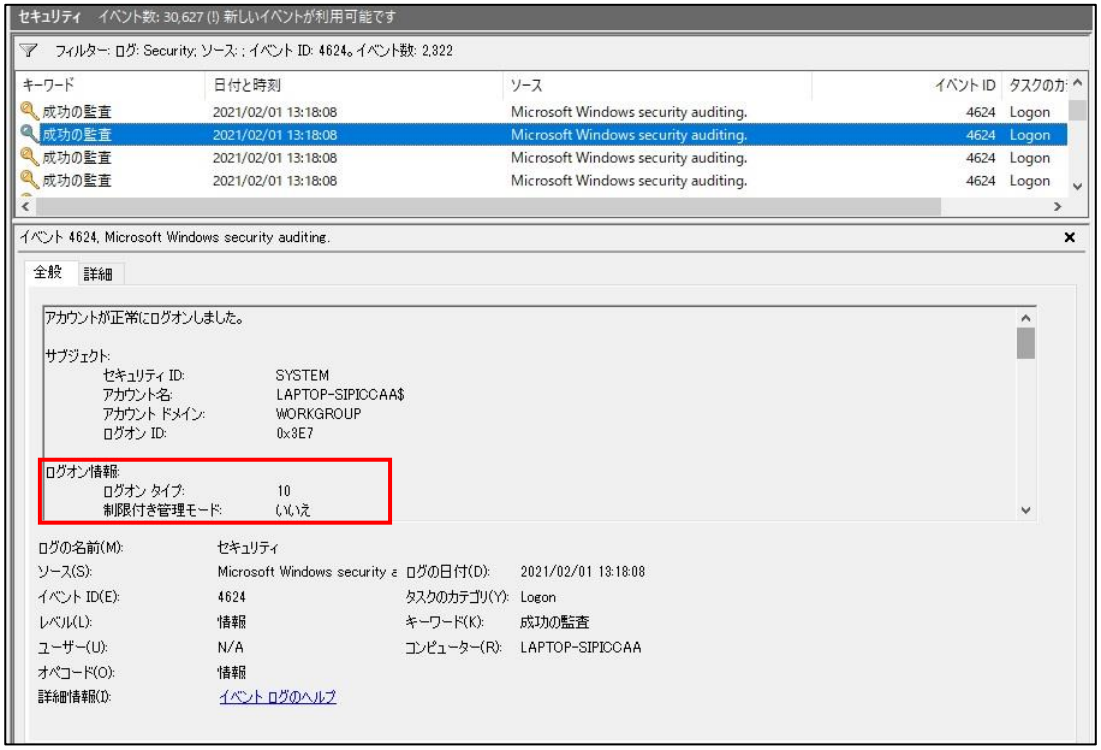
【手順③】

右ペインより「セキュリティ」-「現在のログをフィルター…」をクリックし、「フィルター」の「イベント ID を含める/除外する（N）」に「4624」と入力し、「OK」をクリックします。イベント ID「4624」はログオン成功時に出力されるログです。

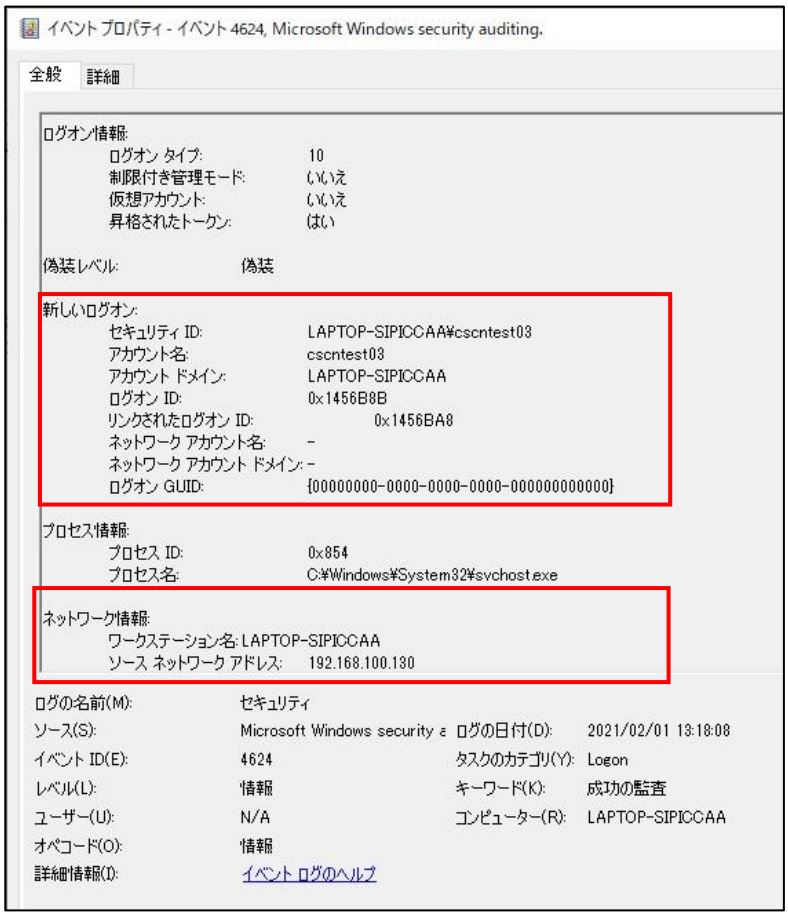


【手順④】

イベント欄から「ログオン情報」にログオンタイプが「10」のログを探します。ログオンタイプが「10」のログがリモートデスクトップ接続経由でのログオンのログになります。



このイベントログから「ログインされたアカウント名」や「ソースネットワークアドレス（接続元の IP アドレス）」が確認できます。

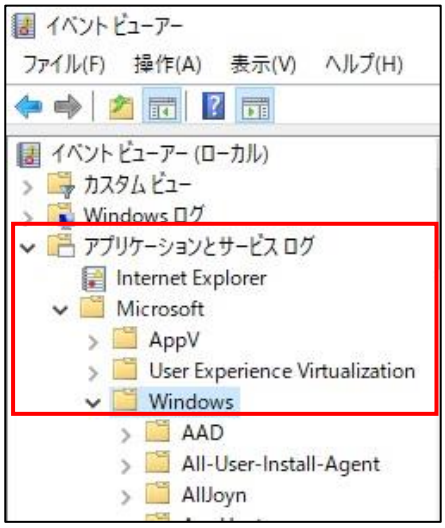


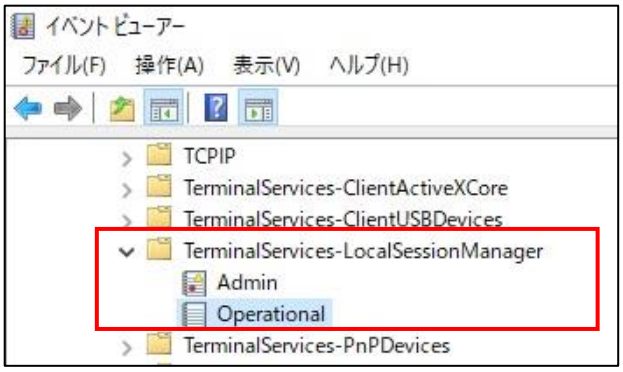
接続先端末のログ確認：アプリケーションとサービスのログによるリモートデスクトップ接続時のログオンログの確認

以下のイベントログからもリモートデスクトップ接続のログオンの履歴が確認できます。

【手順①】

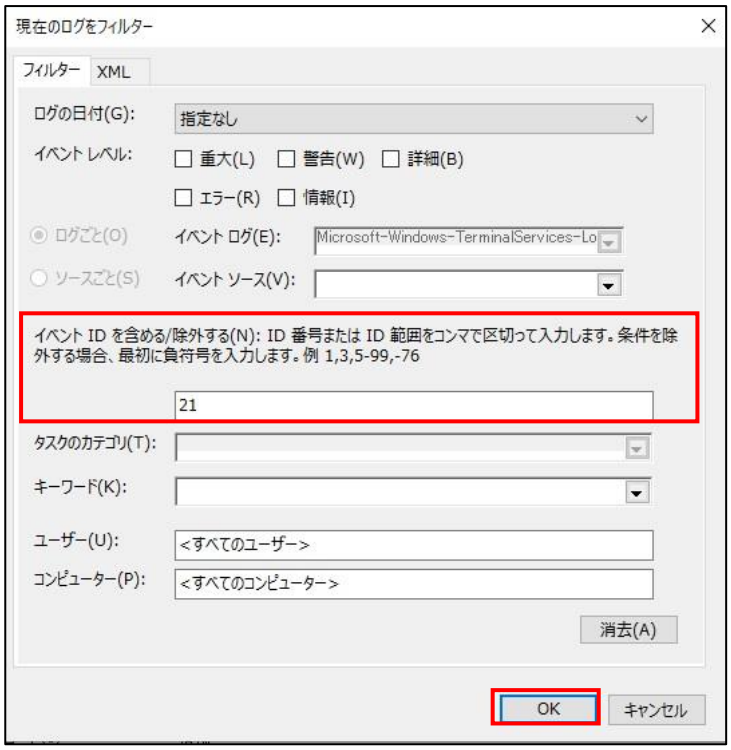
「イベントビューアー」の左ペインで「アプリケーションとサービスログ」-「Microsoft」-「Windows」-「TerminalServices-LocalSessionManager」-「Operational」を選択します。



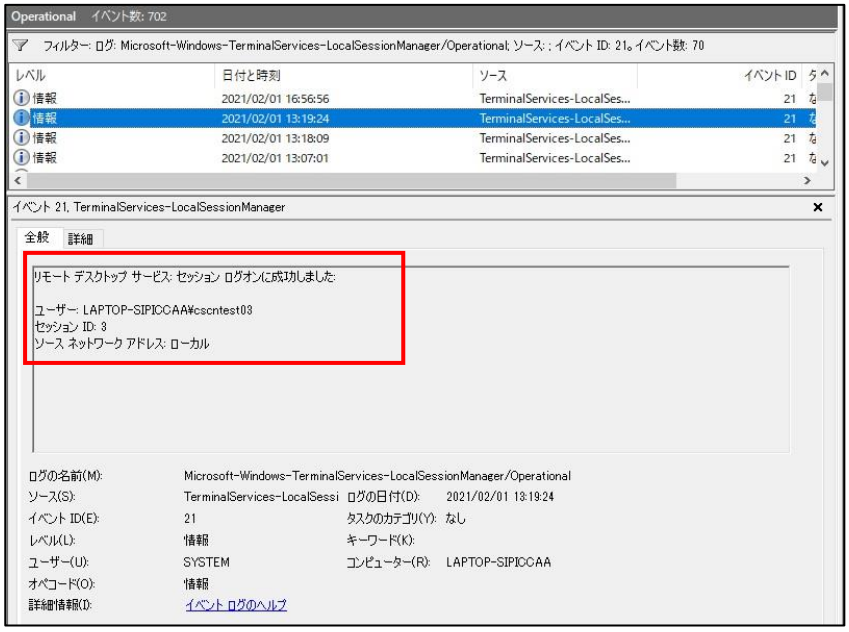


【手順②】

右ペインより「セキュリティ」-「現在のログをフィルター…」をクリックして、「フィルター」の「イベント ID を含める/除外する（N）」に「21」と入力して、「OK」をクリックします。イベント ID：21 は、リモートデスクトップセッションログオン成功時に出力されるログです。



イベントログからログオンしたユーザ名が確認できます。

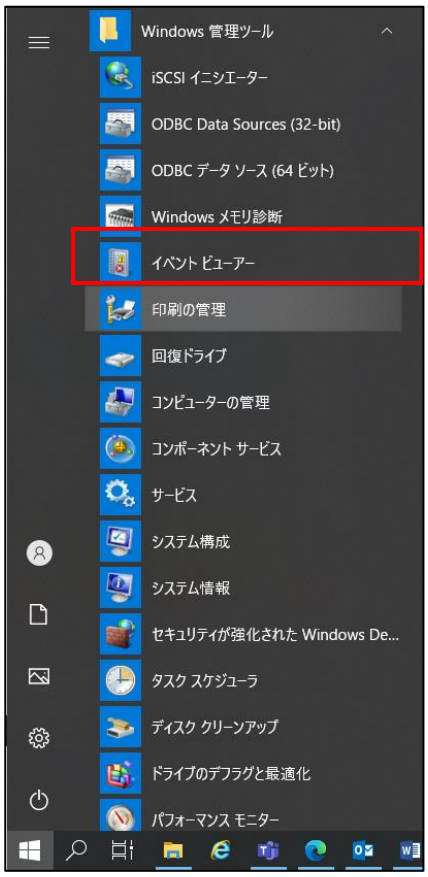


接続元端末でのリモートデスクトップ接続イベントログの確認

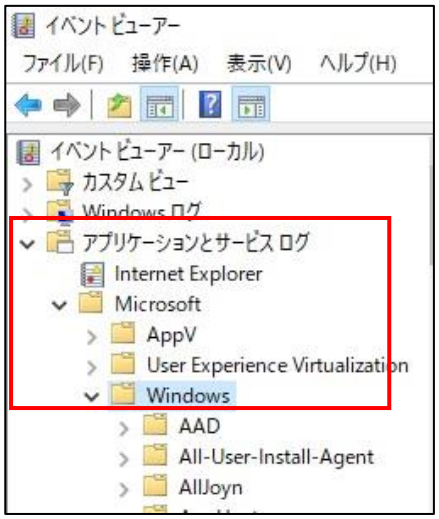
リモートデスクトップ接続先と接続元のログを比較し、接続先端末でのログが自身の操作によるものか確認することで、不正なアクセスがなかったか、確認することができます。本手順では、接続元の端末のログを確認する方法を記載します。

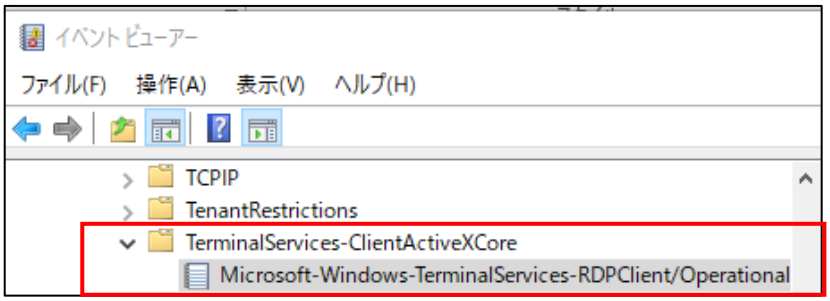
【手順①】

「スタート」-「管理ツール」-「イベントビューアー」をクリックします。



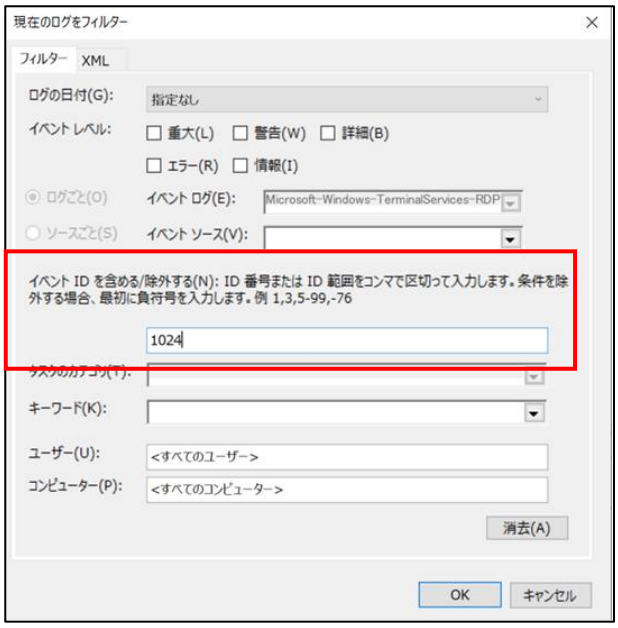
左ペインより「イベントビューアー（ローカル）」-「アプリケーションとサービスログ」-「Microsoft」-「Windows」-「TerminalServices-ClientActiveXCore」-「Microsoft-Windows-TerminalServices-RDPClient/Operational」-「Operational」を選択します。



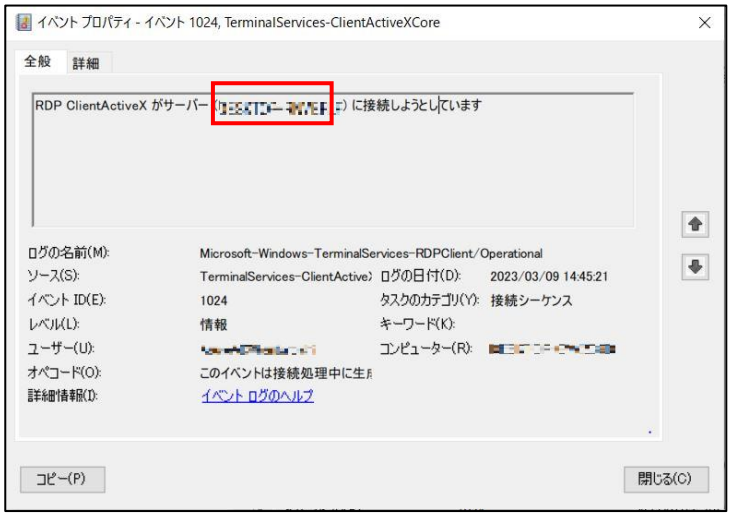


【手順②】

右ペインより[セキュリティ]-[現在のログをフィルター…]をクリック後、[フィルター]の[イベント ID を含める/除外する（N）]に「1024」と入力し、[OK]をクリックします。



イベントログから接続先の IP アドレスまたはデバイス名が確認できます。



4-3　チェックリスト 9-2 への対応

4-4-1　　初期パスワード設定変更

初期パスワードは、誰が把握しているかわからないので、貸与された端末の初期パスワードは速やかに変更することで**悪意のある第三者から不正アクセスされるリスクを低減**します。

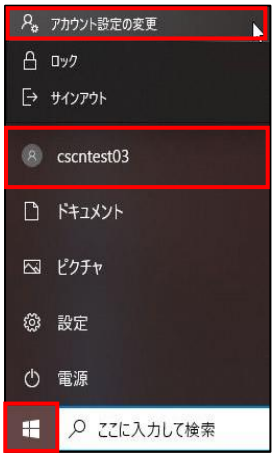
初期パスワードの設定変更

職場環境によっては、以下の手順では変更できない場合があります。その場合は、職場のパスワード変更手順に従ってパスワードを変更してください。

【手順①】

画面左下の Windows スタートメニューをクリックし、「cscntest03」（※）をクリック後、「アカウント設定の変更をクリック」し、アカウントの設定変更画面を表示させます。

※　本手順ではアカウント名を「cscntest03」としています。

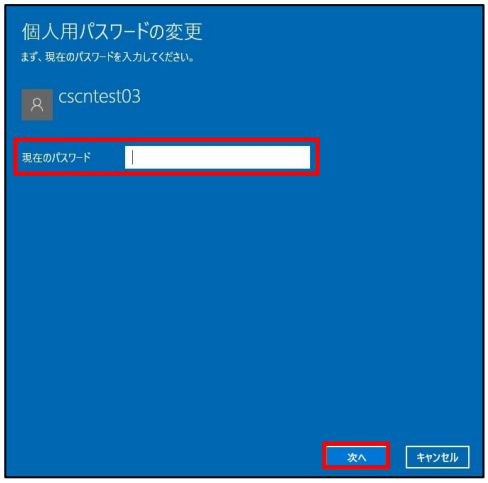


【手順②】

左ペインの「サインインオプション」を選択し、デバイスへのサインイン方法の管理から「パスワード」-「変更」をクリックします。

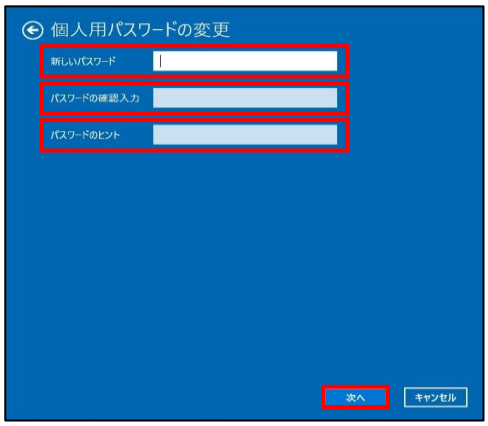
【手順③】

画面に従って「現在のパスワード」を入力し、「次へ」をクリックします。



【手順④】

「新しいパスワード」「パスワードの確認入力」「パスワードのヒント」を入力し、「次へ」をクリックします。



【手順⑤】

現在ログインしているアカウント名が表示されるので、「完了」をクリックするとパスワードの変更が完了します。