

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 （Chrome リモート デスクトップ）

**Ver1.1**（2024.03）

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](mailto:telework-security@ml.soumu.go.jp)

URL [https://www.soumu.go.jp/main\\_sosiki/cybersecurity/telework/](https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/)

## 目次

<b>1</b>	<b>はじめに .....</b>	<b>3</b>
<b>2</b>	<b>チェックリスト項目に対応する設定作業一覧 .....</b>	<b>4</b>
<b>3</b>	<b>管理者向け設定作業 .....</b>	<b>6</b>
3-1	チェックリスト 8-4 への対応 .....	6
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.....	6
3-2	チェックリスト 9-4 への対応 .....	10
3-2-1	2 段階認証プロセスの設定.....	10
3-3	チェックリスト 10-2 への対応 .....	12
3-3-1	管理者アカウントのパスワード強度.....	12
3-4	チェックリスト 10-3 への対応 .....	12
3-4-1	管理者権限の管理.....	12
	注意事項.....	12
<b>4</b>	<b>利用者向け作業 .....</b>	<b>13</b>
4-1	チェックリスト 8-4 への対応 .....	13
4-1-1	クリップボードの同期機能の無効化.....	13
4-2	チェックリスト 5-4 への対応 .....	15
4-2-1	最新のセキュリティアップデート.....	15
4-3	チェックリスト 7-3 への対応 .....	18
4-3-1	リモートデスクトップ接続時のアクセスログ確認.....	18
4-4	チェックリスト 9-1 への対応 .....	23
4-4-1	パスワード強度.....	23
4-5	チェックリスト 9-2 への対応 .....	25
4-5-1	初期パスワード変更.....	25
4-6	チェックリスト 9-4 への対応 .....	27
4-6-1	2 段階認証プロセスの設定.....	27
	注意事項.....	39

## 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、Google Chrome の拡張機能「Chrome Remote Desktop」を利用する際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

本アプリケーションは無償で利用できますが、Google Workplace を利用している前提としております。Google Workplace のライセンス形態はすべて有償で「Business Starter」「Business Standard」「Business Plus」「Enterprise」が存在します。（2023 年 11 月 7 日現在）利用するライセンス種類により使用可能な機能が異なります。**本資料では「Business Standard」ライセンス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、2023 年 11 月 7 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
<b>8-4 データ保護</b> 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。	・ <a href="#">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</a>	P. 6
<b>9-4 アカウント・認証管理</b> テレワークで利用する各システムへのアクセスには、多要素認証を求めるよう設定する。	・ <a href="#">2 段階認証プロセスの設定</a>	P.10
<b>10-2 特権管理</b> テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用する。	・ <a href="#">管理者アカウントのパスワード強度</a>	P.12
<b>10-3 特権管理</b> テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用する。	・ <a href="#">管理者権限の管理</a>	P.12

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	対応する設定作業	ページ
<b>8-4 データ保護</b> 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。	・ <a href="#">クリップボードの同期機能の無効化</a>	P.13
<b>5-4 脆弱性管理</b> 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。	・ <a href="#">最新のセキュリティアップデート</a>	P.15
<b>7-3 インシデント対応・ログ管理</b> 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。	・ <a href="#">リモートデスクトップ接続時のアクセスログ</a>	P.18
<b>9-1 アカウント・認証管理</b> 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。	・ <a href="#">パスワード強度</a>	P.23
<b>9-2 アカウント・認証管理</b> 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。	・ <a href="#">初期パスワード変更</a>	P.25
<b>9-4 アカウント・認証管理</b> テレワークで利用する各システムへのアクセスには、多要素認証を求めるよう設定する。	・ <a href="#">2 段階認証プロセスの設定</a>	P.27

## 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ってしまうため、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で、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は設定を一括適用できるため、AD サーバーに下記記載のポリシーテンプレートを追加してグループポリシー（GPO）を作成することを推奨します。ポリシーテンプレートの追加先やグループポリシーの作成は、AD ドメイン環境を構築した担当者にご確認ください。

#### 【手順①】

以下のサイトから、「ポリシーテンプレート」をクリックし、Google Chrome の管理テンプレートをダウンロードします。

- 管理対象パソコンに Chrome ブラウザのポリシーを設定する

<https://support.google.com/chrome/a/answer/187202?hl=ja>

#### 管理対象パソコンに Chrome ブラウザのポリシーを設定する

管理対象の Chrome ブラウザ（Windows 版、Mac 版、Linux 版）が対象です。

このページは、オンプレミス ツールを使用して、企業が管理するパソコンに Chrome のポリシーを設定する IT 管理者を対象としています。

ユーザーの会社用パソコンに Chrome ブラウザをインストールしたら、好みのオンプレミス ツールを使用してユーザーのデバイスにポリシーを適用できます。Windows グループ ポリシーを使用したり、Mac や Linux 用の好みの設定ツールを使用したりできます。Google が提供するポリシー テンプレートを使用するとポリシーを容易に設定することができ、インストールとアップデートも簡単です。

管理者はデバイスレベルのポリシーや OS ユーザーレベルのポリシーを適用できます。デバイスレベルのポリシーは、ユーザーが Chrome ブラウザを使用しているかどうかや、アカウントにログインしているかどうかに関係なく適用されます。OS ユーザーレベルのポリシーは特定のユーザーがデバイスにログインしたときに適用されます。また、管理者はユーザーが変更できないポリシーを適用したり、ユーザーが変更可能なデフォルトの設定を適用したりできます。

注: Chrome ポリシーの全リストを確認するには、**ポリシー テンプレート** の zip ファイルに含まれている common/ フォルダ（サポート対象のすべての言語に対応）を参照してください。

## 【手順②】

ダウンロードしたファイル「policy\_templates.zip」を展開します。

デスクトップ > policy_templates			
名前	更新日時	種類	サイズ
chromeos	2021/02/02 14:08	ファイル フォルダー	
common	2021/02/02 14:08	ファイル フォルダー	
windows	2021/02/02 14:08	ファイル フォルダー	
VERSION	2001/01/01 0:00	ファイル	1 KB

## 【手順③】

解凍したフォルダの windows フォルダの「admx」フォルダを開き、以下 2 つのファイルをコピーします。

- google.admx
- chrome.admx

デスクトップ > policy_templates > windows > admx			
名前	更新日時	種類	サイズ
de-DE	2021/02/02 14:08	ファイル フォルダー	
en-US	2021/02/02 14:08	ファイル フォルダー	
es-419	2021/02/02 14:08	ファイル フォルダー	
es-ES	2021/02/02 14:08	ファイル フォルダー	
fr-FR	2021/02/02 14:08	ファイル フォルダー	
id-ID	2021/02/02 14:08	ファイル フォルダー	
it-IT	2021/02/02 14:08	ファイル フォルダー	
ja-JP	2021/02/02 14:08	ファイル フォルダー	
ko-KR	2021/02/02 14:08	ファイル フォルダー	
nl-NL	2021/02/02 14:08	ファイル フォルダー	
pt-BR	2021/02/02 14:08	ファイル フォルダー	
ru-RU	2021/02/02 14:08	ファイル フォルダー	
th-TH	2021/02/02 14:08	ファイル フォルダー	
tr-TR	2021/02/02 14:08	ファイル フォルダー	
uk-UA	2021/02/02 14:08	ファイル フォルダー	
vi-VN	2021/02/02 14:08	ファイル フォルダー	
zh-CN	2021/02/02 14:08	ファイル フォルダー	
zh-TW	2021/02/02 14:08	ファイル フォルダー	
chrome.admx	2001/01/01 0:00	ADMX ファイル	485 KB
google.admx	2001/01/01 0:00	ADMX ファイル	1 KB

コピー後、「C:\Windows\PolicyDefinitions」フォルダに上記 2 つのファイルをペーストします。

C:\Windows\PolicyDefinitions			
名前	更新日時	種類	サイズ
en-US	2020/11/03 3:29	ファイル フォルダー	
ja-JP	2021/02/02 12:52	ファイル フォルダー	
chrome.admx	2001/01/01 0:00	ADMX ファイル	485 KB
google.admx	2001/01/01 0:00	ADMX ファイル	1 KB

続いて、policy\_templates の「admx」フォルダの ja-JP フォルダを開き、以下 2 つのファイルをコピーします。

- google.adml
- chrome.adml

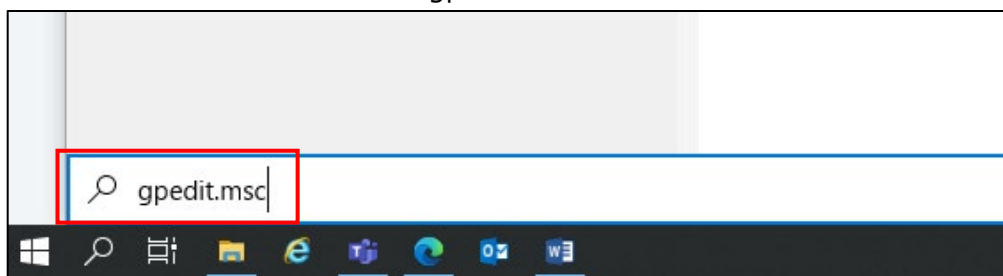
デスクトップ > policy_templates > windows > admx > ja-JP			
名前	更新日時	種類	サイズ
chrome.adml	2001/01/01 0:00	ADML ファイル	426 KB
google.adml	2001/01/01 0:00	ADML ファイル	1 KB

接続先端末毎の「C:¥Windows¥PolicyDefinitions¥ja-JP」フォルダにペーストします。



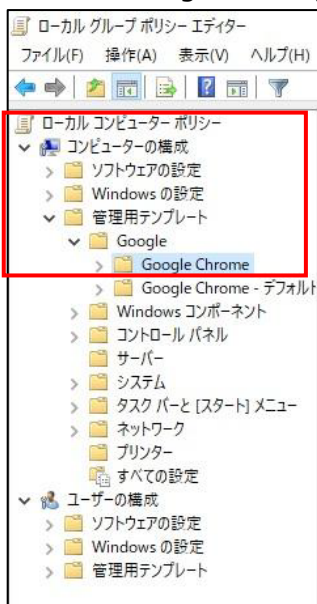
#### 【手順④】

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。



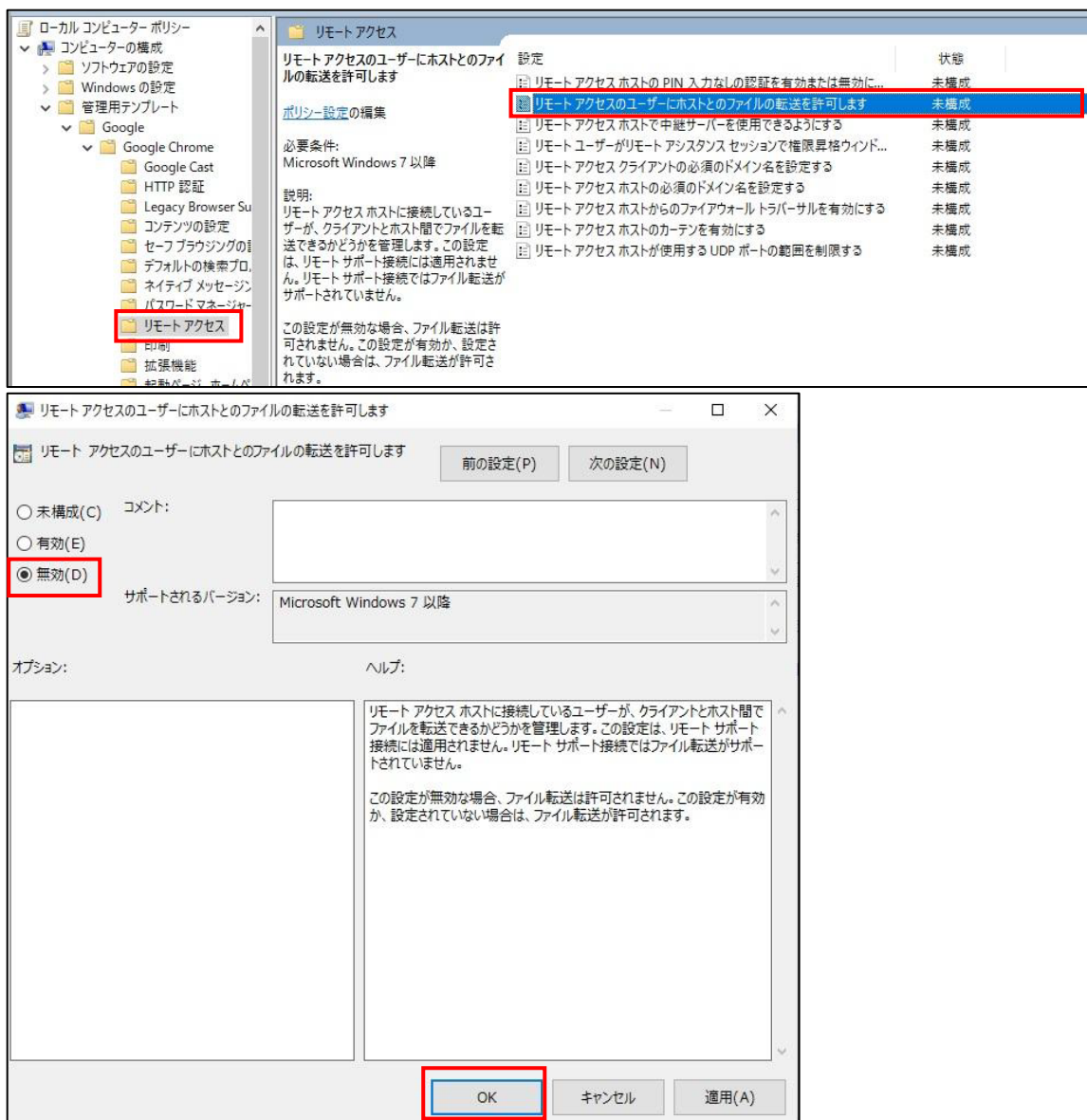
#### 【手順⑤】

「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」-「Google」-「Google Chrome」を順に選択します。

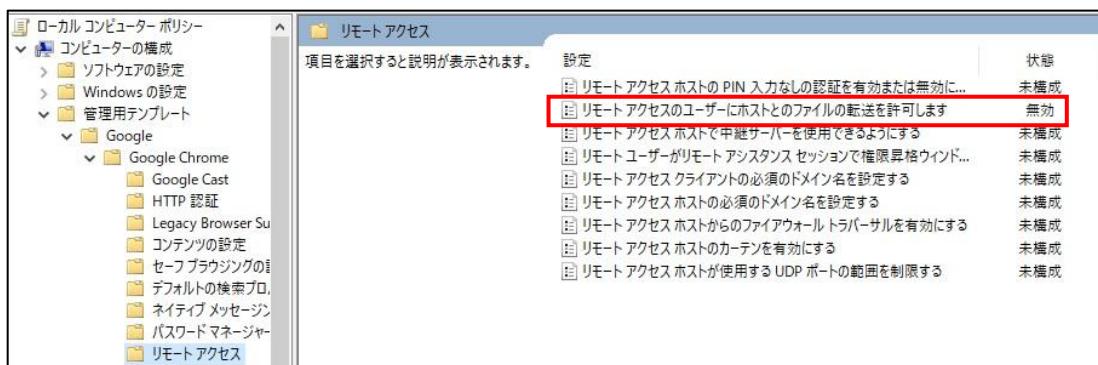


## 【手順⑥】

「Google Chrome」の「リモートアクセス」を選択し、右側の「リモートアクセスのユーザーにホストとのファイルの転送を許可します」を開き、「無効」を選択し、「OK」をクリックします。



設定が反映され、無効化されると、以下のように「リモートアクセスのユーザーにホストとのファイルの転送を許可します」の状態が「無効」となります。



### 【参考】設定反映前後の比較

下記左側：ポリシー未適用でファイルのダウンロードとアップロードが可能な状態になっています。

下記右側：ポリシーが適用されファイル転送ができなくなっています。



## 3-2 チェックリスト 9-4 への対応

### 3-2-1 2 段階認証プロセスの設定

2 段階認証を有効化することにより、ログインするためにパスワードだけでなく SMS で受け取った一時的なコードなど追加の認証情報が求められるようになります。**2 段階認証の設定によりパスワードが破られた場合でも、不正ログインを防ぐことができます。**

#### 【手順①】

Google 管理コンソール (<https://admin.google.com/>) から、「セキュリティ」-「2 段階認証プロセス」をクリックします。



## 【手順②】

2 段階認証プロセスのポリシーを設定することができます。デフォルトでは「ユーザーが 2 段階認証プロセスを有効にできるようにする」はオンであり、ユーザーへの適用は「強制しない」が選択されています。ユーザーへの適用の方法は、「強制しない」以外に、「今すぐ強制」と「指定日以降に強制」を選択できます。

### i) 「指定日以降に強制」を選択した場合

「新しいユーザーの登録期間」を設定することで、ユーザーに 2 段階認証が適用されるまでの猶予期間を設けることができます。登録期間を設定しなかった場合、2 段階認証未登録ユーザーはログインしようとするとき必ず下記画面となりログインできなくなるため、必ず登録期間を設定してください。

- ii) 「今すぐ強制」で「新しいユーザーの登録期間」を設定した場合や「指定日以降に強制」を選択した場合ユーザーがログインした際、下記画面に遷移し、2 段階認証の登録を促します。



### 3-3 チェックリスト 10-2 への対応

#### 3-3-1 管理者アカウントのパスワード強度

パスワード強度が弱いパスワードを使用した場合、パスワードが解読され、不正アクセスを受けるおそれがあります。そのため、適切なパスワードを設定することが重要です。設定するパスワードは「[中小企業等向けテレワークセキュリティの手引き](#)」の P.96 に記載の「パスワード強度」を参考に設定することを推奨します。

【参考】安全なパスワードを作成してアカウントのセキュリティを強化する

URL : <https://support.google.com/accounts/answer/32040?hl=ja>

### 3-4 チェックリスト 10-3 への対応

#### 3-4-1 管理者権限の管理

作業ミスによるシステムやデータへの悪影響を防ぐために、**一般ユーザーのアカウントを作成し、普段はそのアカウントを利用、管理者用アカウントの利用は最小限に留める**ことを推奨します。

### 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、Chrome 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 8-4 への対応

#### 4-1-1 クリップボードの同期機能の無効化

Chrome リモート デスクトップ接続には、クリップボードの同期の機能という機能がありますが、情報漏洩のリスクを低減するため、利用しないことを推奨します。

クリップボードの同期が有効な場合、ブラウザ画面右上アイコンにマウスのカーソルを置くと、「このサイトでは、クリップボードにコピーされているテキストや画像へのアクセスが許可されています。」と表示されます。



上図のように表示された場合、この機能を無効にする必要があります。

アイコンをクリックし、「<https://remotedesktop.google.com> によるクリップボードへのアクセスを常にブロックする」を選択し、「完了」をクリックします。



その後、Google からログアウトし、再度ログイン後 Chrome リモート デスクトップを利用して接続します。



初回接続時に、Chrome リモート デスクトップのメニュー画面が以下になっている場合は既にクリップボードの同期は無効になっています。



## 4-2 チェックリスト 5-4 への対応

### 4-2-1 最新のセキュリティアップデート

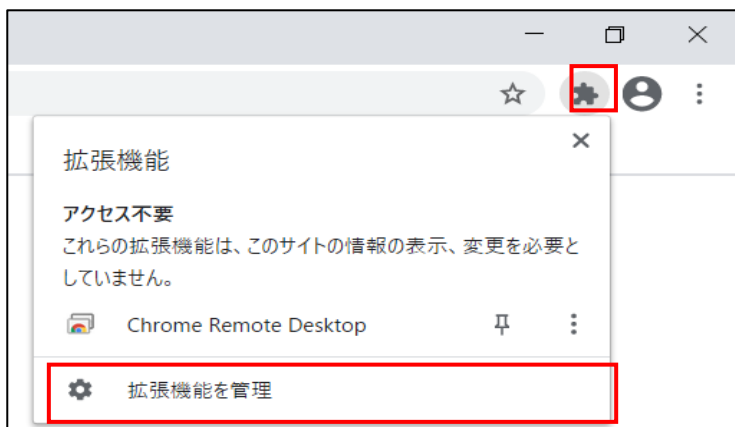
製品提供元からリリースされている最新バージョンのアプリケーションを利用します。最新バージョンを利用することは、アプリケーションの脆弱性をついたサイバー攻撃に対して有効な対策となるため、定期的にアップデートがないか確認をすることを推奨します。

ここでは Chrome リモート デスクトップだけでなく、Chrome の最新バージョンの確認とアップデートの手順についても記載します。

#### Chrome リモート デスクトップのバージョン確認

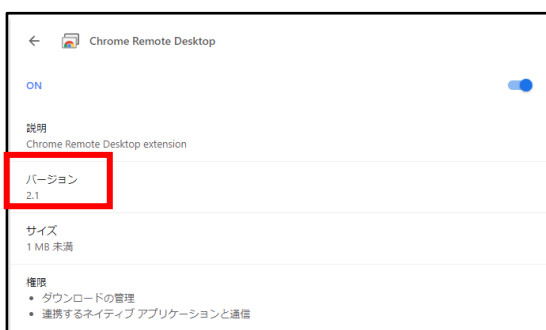
##### 【手順①】

接続元の PC の Chrome 画面右上にある「拡張機能」をクリックし、「拡張機能を管理」を開きます。



##### 【手順②】

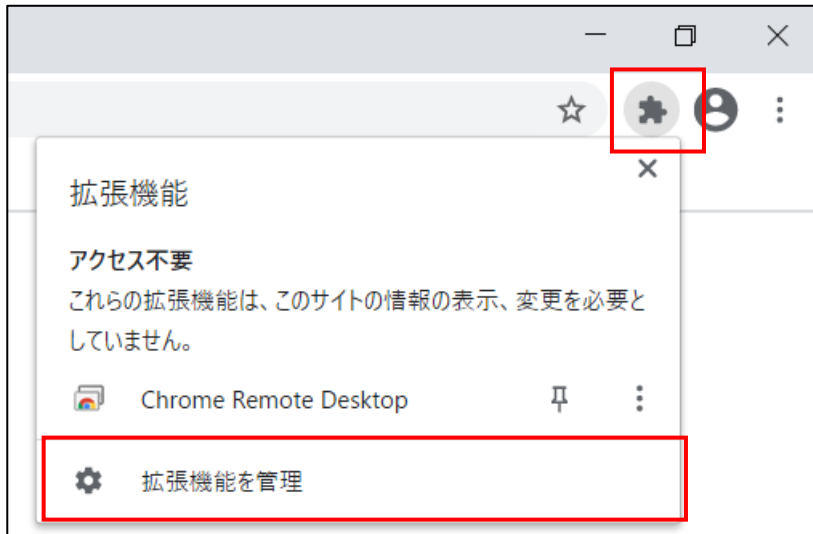
Chrome Remote Desktop の「詳細」-「バージョン」から利用中のバージョンを確認します。



## Chrome リモート デスクトップの手動アップデート方法

### 【手順①】

接続元の PC の Chrome 画面-右上にある「拡張機能」をクリックし、「拡張機能を管理」を開きます。



### 【手順②】

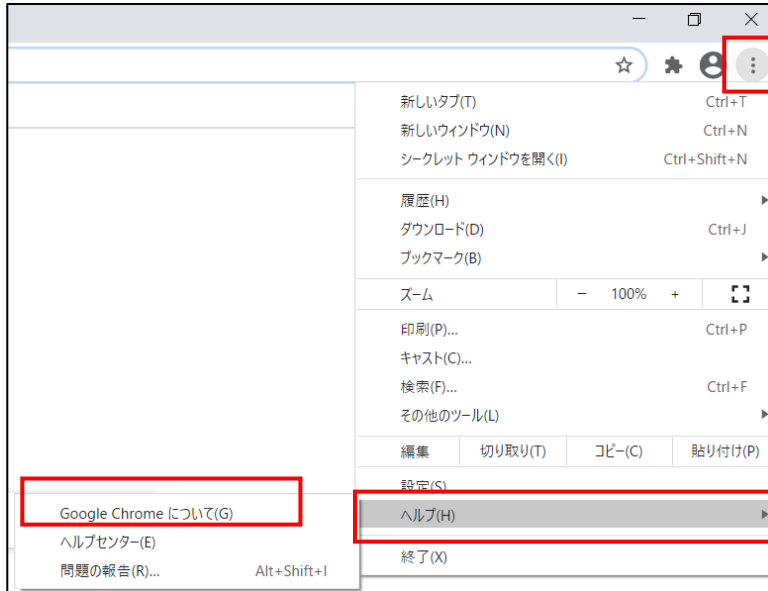
画面右上の「デベロッパーモード」をオンにし、「更新」をクリックすると拡張機能をアップデートすることができます。



## Chrome のバージョンの確認と更新

### 【手順①】

接続元の PC の Chrome 画面右上にある「Google Chrome の設定」の「ヘルプ」から「Google Chrome について」をクリックします。



### 【手順②】

「Google Chrome は最新版です」の表示が出ており、アプリケーションが最新であることを確認します。古いバージョンの場合は、「Google Chrome について」を開くと更新が始まります。



## 4-3 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時のアクセスログ確認

Google アカウントに不審なデバイスからのログインがなかったか確認します。加えて、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。

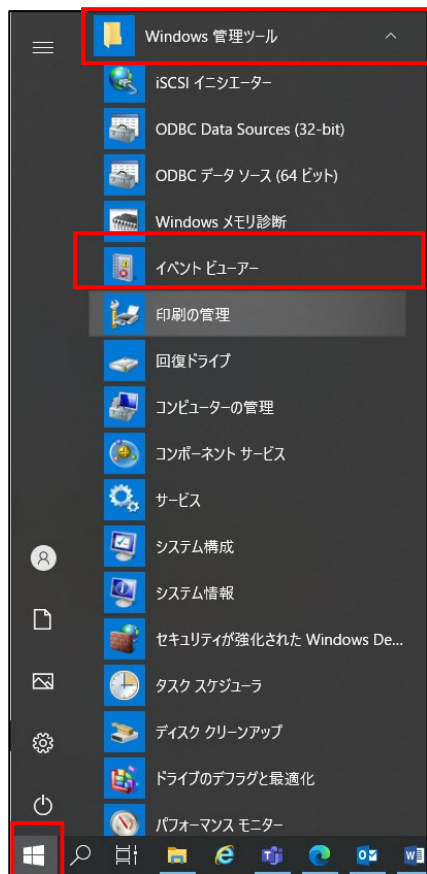
確認の結果、他の端末から接続先の端末へリモートデスクトップサービスによるログオンが疑われる場合、速やかにリモートデスクトップ先端末のパスワードを変更し、管理者に連絡してください。

#### 接続先端末の Windows のログの確認

接続先の端末上で、下記手順により、Chrome 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。

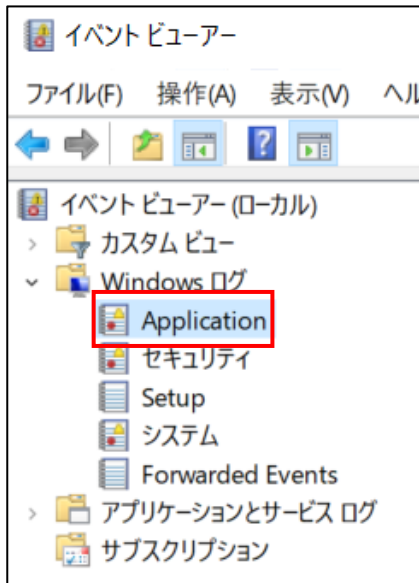
##### 【手順①】

「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。



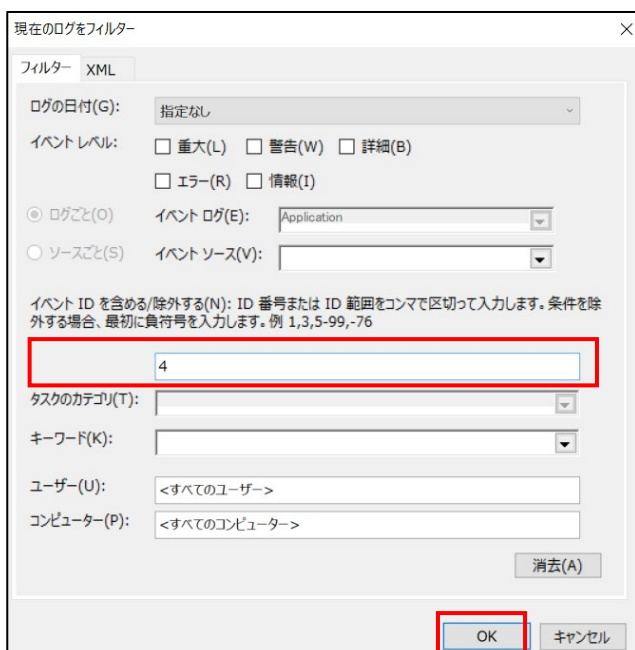
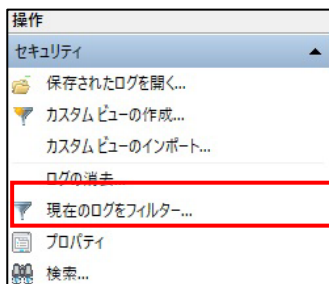
## 【手順②】

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



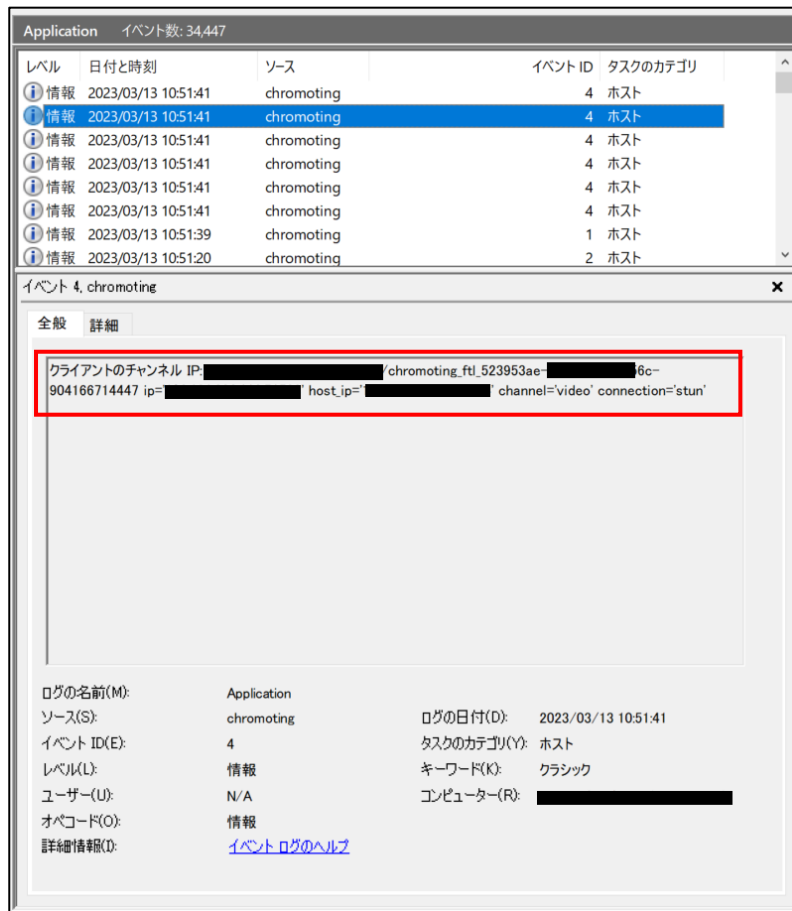
## 【手順③】

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「4」と入力し、「OK」をクリックします。



#### 【手順④】

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、自身が利用しているものかを確認します。



The screenshot shows the Chrome Remote Desktop application interface. At the top, it says 'Application イベント数: 34,447'. Below this is a table of events. The table has columns: 'レベル' (Level), '日付と時刻' (Date and Time), 'ソース' (Source), 'イベント ID' (Event ID), and 'タスクのカテゴリ' (Task Category). The first six rows show events from 2023/03/13 10:51:41, all with source 'chromoting' and category 'ホスト'. The seventh row shows an event from 2023/03/13 10:51:39 with source 'chromoting' and category 'ホスト'. The eighth row shows an event from 2023/03/13 10:51:20 with source 'chromoting' and category 'ホスト'.

Below the table, there is a detailed view of 'イベント 4, chromoting'. It has tabs for '全般' (General) and '詳細' (Details). The '全般' tab is selected. It shows the following information:

- クライアントのチャンネル IP: [redacted] / chromoting\_ftl\_523953ae-[redacted]6c-
- 904166714447 ip=[redacted] host\_ip=[redacted] channel='video' connection='stun'

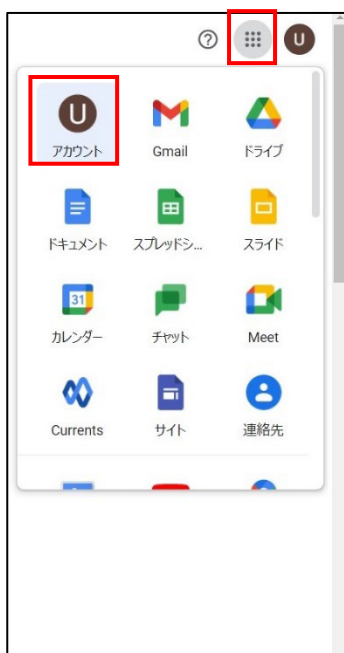
At the bottom, there is a summary section with the following information:

- ログの名前(M): Application
- ソース(S): chromoting
- イベント ID(E): 4
- レベル(L): 情報
- ユーザー(U): N/A
- オペコード(O): 情報
- 詳細情報(D): [イベント ログのヘルプ](#)
- ログの日付(D): 2023/03/13 10:51:41
- タスクのカテゴリ(Y): ホスト
- キーワード(K): クラシック
- コンピューター(R): [redacted]

### Google アカウントのログの確認

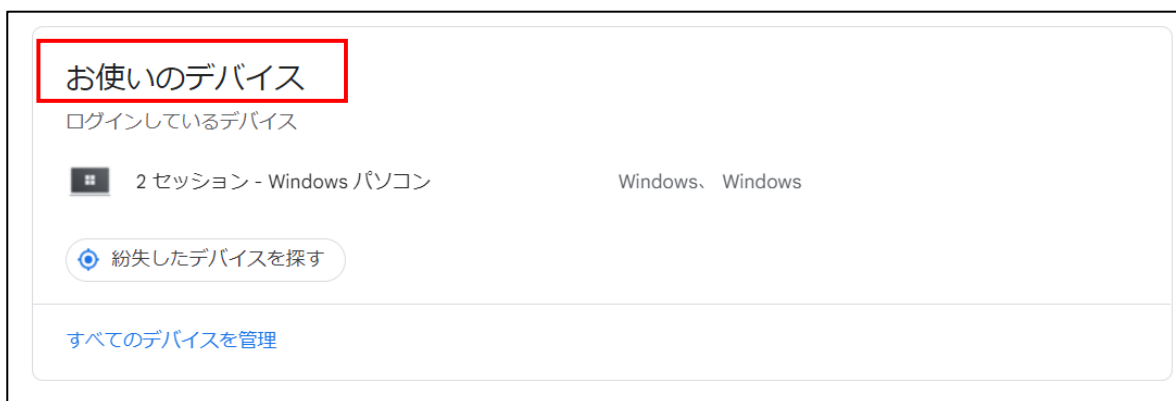
#### 【手順①】

画面右上の Google アプリ の「アカウント」を開きます。



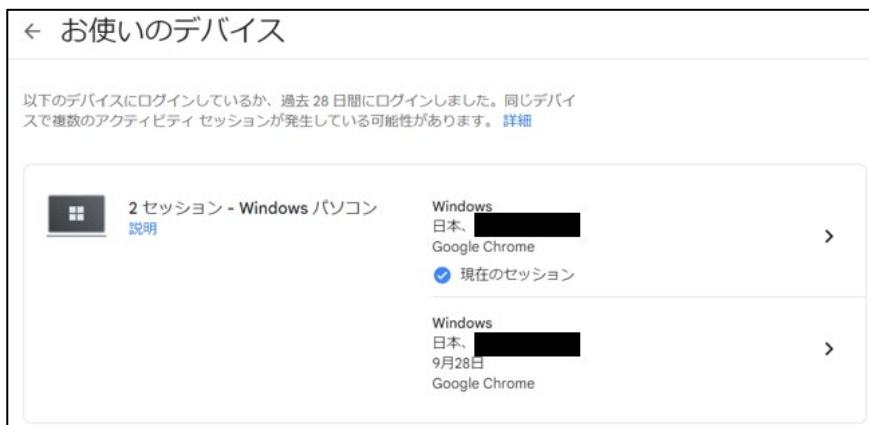
### 【手順②】

「セキュリティ」-「お使いのデバイス」をクリックします。



### 【手順③】

現在ログインしている端末と過去 28 日間にログインしていた端末が表示されます。「お使いのデバイス」に自身が利用している端末のみが表示されていることを確認します。



使用した心当たりがない端末が表示されている場合は、当該端末をクリックし、「心当たりがない場合」-「デバイスでログアウトする」をクリックします。また、その後速やかにパスワードを変更します。



## 4-4 チェックリスト 9-1 への対応

### 4-4-1 パスワード強度

パスワード強度が弱いパスワードを使用した場合、パスワードが解読され、不正アクセスを受けるおそれがあります。そのため、適切なパスワードを設定することが重要です。設定するパスワードは「[中小企業等向けテレワークセキュリティの手引き](#)」の P.96 に記載の「パスワード強度」を参考に設定することを推奨します。

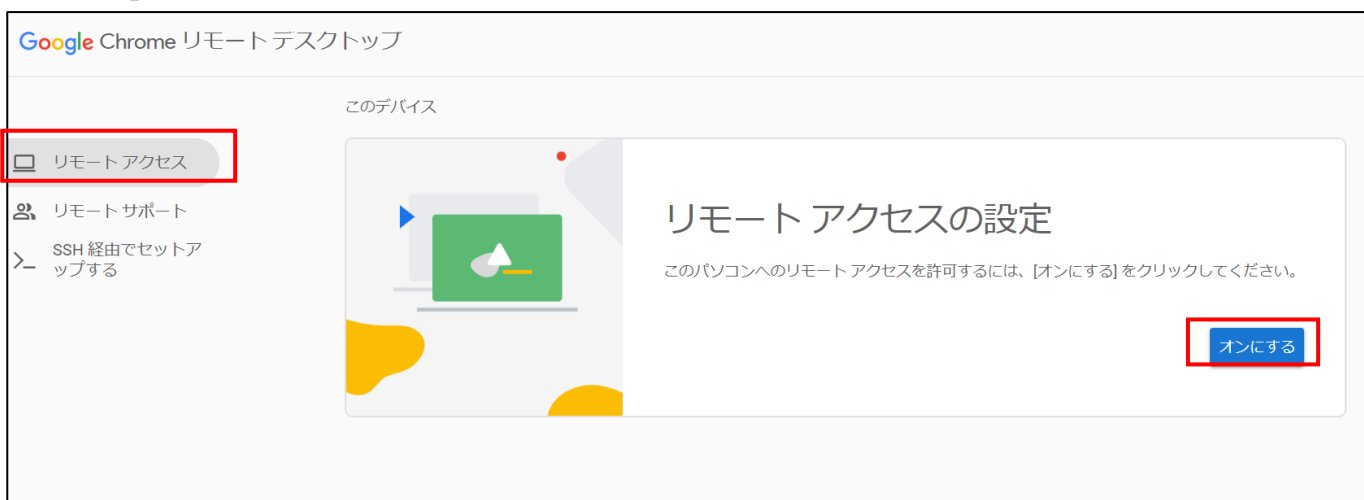
ベンダーの参考先情報：安全なパスワードを作成してアカウントのセキュリティを強化する

URL：<https://support.google.com/accounts/answer/32040?hl=ja>

## Chrome リモート デスクトップ接続時の PIN 設定

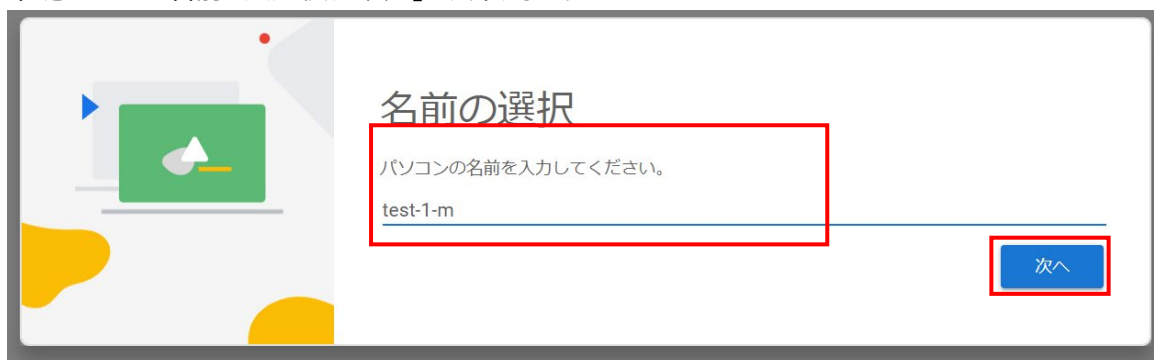
### 【手順①】

<https://remotedesktop.google.com/access/>へアクセスし、Google アカウントでログイン後、「リモートアクセス」の「オンにする」をクリックします。



### 【手順②】

任意の PC の名前を入力後、「次へ」をクリックします。



### 【手順③】

PIN の入力画面で、6 桁以上の PIN コードを入力し、「起動」をクリックします。

### Chrome リモート デスクトップ接続時の PIN 変更

Chrome リモート デスクトップ画面の、「このデバイス」に表示されている機器名横の「このデバイスの設定を編集」を開きます。その後、「PIN の変更」で 6 桁以上の PIN を入力して、「保存」すれば変更することができます。

## 4-5 チェックリスト 9-2 への対応

### 4-5-1 初期パスワード変更

初期パスワードは、誰が把握しているかわからないので、速やかにパスワード要件を満たすものに変更することで、**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することができます。**

#### 【手順①】

初回ログインした時に「安全なパスワードの作成」画面に遷移した場合は、指示に従いパスワードを変更します。



The screenshot shows the Google account setup screen for 'testuser02@cscntest.page'. It prompts the user to 'Create a secure password' by entering a new password in the 'パスワードの作成' field and confirming it in the '確認' field. A note states: '安全なパスワードの作成 他のウェブサイトで使用していない安全なパスワードを新たに作成してください'. There is a checkbox for 'パスワードを表示します' and a blue '次へ' button at the bottom right.

初回ログイン時に「安全なパスワードの作成」画面に遷移しない場合は、下記手順に従ってパスワードを変更します。

#### 【手順①】

右上 Google アカウントアイコンの「Google アカウントを管理」をクリックします。



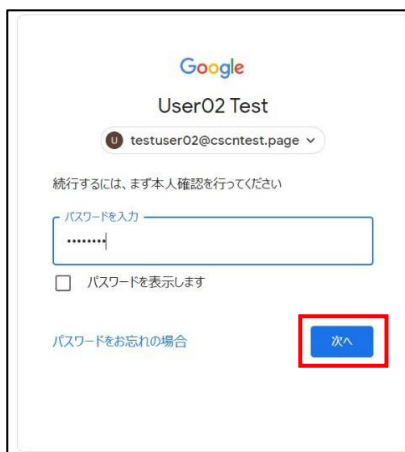
### 【手順②】

「個人情報」-「パスワード」をクリックします。



### 【手順③】

本人確認のための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】

新しいパスワードを入力し、「パスワードを変更」をクリックします。



## 4-6 チェックリスト 9-4 への対応

### 4-6-1 2 段階認証プロセスの設定

2 段階認証を有効化することにより、ログインするためにパスワードだけでなく SMS で受け取った一時的なコードなど追加の認証情報が求められるようになります。**2 段階認証の設定によりパスワードが破られた場合でも、不正ログインを防ぐことができます。**

#### 2 段階認証の登録が強制される場合

##### 【手順①】

ログイン時に、下記画面に遷移した場合は「登録」をクリックします。



##### 【手順②】

本人確認を行う画面への遷移後、パスワードを入力し、次へをクリックします。



### 【手順③】

2 段階認証のプロセス画面の表示後、画面内の「使ってみる」をクリックします。



### 【手順④】

2 段階認証に使用する電話番号を入力し、コードの取得方法を選択し、「次へ」をクリックします。



【手順⑤】

確認コードを入力し、「次へ」をクリックし、「有効にする」をクリックします。

← 2 段階認証プロセス



利用できるかの確認

Google から [redacted] に確認コードのテキストメッセージが送信されました。

コードの入力

受け取れなかった場合: [再送信](#)

戻る

手順 2 / 3

次へ



確認が完了しました。2 段階認証プロセスを有効にしますか？

2 段階認証プロセスの仕組みは以上です。お使いの Google アカウント [work@idm.google.com](#) で 2 段階認証プロセスを有効にしますか？

手順 3 / 3

有効にする

## 2 段階認証の登録を強制されない場合

### 【手順①】

右上 Google アカウントアイコン-「Google アカウントを管理」をクリックします。



### 【手順②】

「セキュリティ」をクリックし、Google へのログインの「2 段階認証プロセス」をクリックします。



### 【手順③】

2 段階認証のプロセス画面において、「使ってみる」をクリックします。



#### 【手順④】

使用する電話番号を入力し、コードの取得方法を選択し、「次へ」をクリックします。

← 2 段階認証プロセス



電話番号の設定

使用する電話番号を選択してください。

● ▼ |

Google はこの番号をアカウントのセキュリティ保護にのみ使用します。  
Google Voice 番号は使用しないでください。  
データ通信料がかかる場合があります。

コードの取得方法

☒ テキスト メッセージ    ☐ 音声通話

[他のオプションを表示](#)

手順 1 / 3

[次へ](#)

#### 【手順⑤】

確認コードを入力し、「次へ」をクリック後、「有効にする」をクリックします。

← 2 段階認証プロセス



利用できるかの確認

Google から [REDACTED] に確認コードのテキスト メッセージが送信されました。

コードの入力

|

受け取れなかった場合: [再送信](#)

[戻る](#)    手順 2 / 3    [次へ](#)



## パスワードを必要としないログイン設定

Windows10、macOS Ventura、ChromeOS 109 以降を搭載したノートパソコンまたは iOS 16、Android 9 以降を搭載したモバイルデバイスにてパスワードレス認証が利用可能です。（本手順は Windows10 で作成しています）

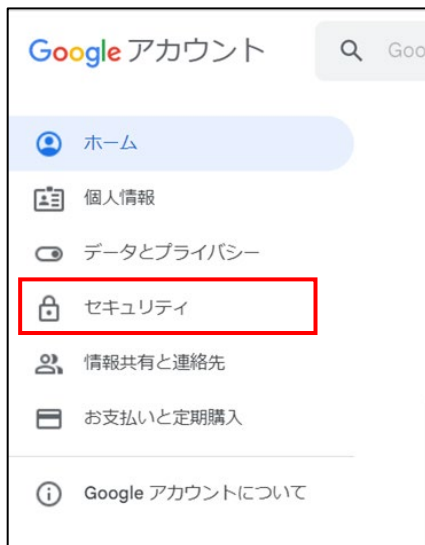
### 【手順①】

ブラウザ右上部のアカウントアイコンをクリックし以下画面の「Google アカウントを管理」をクリックします。



## 【手順②】

左ペインのメニューから「セキュリティ」をクリックします。



## 【手順③】

「パスキー」をクリックします。



【手順④】

下記画面が表示されたら「パスキーを作成」をクリックします。



【手順⑤】

現在ログインしている Google アカウントが表示されるので、「続行」をクリックします。



【手順⑥】

以下画面への切り替わり後、「パスワードを使用」をクリックします。

※パスワードではなく、Touch ID を求められたら Touch ID にて本人確認するようにしてください。



【手順⑦】

「完了」をクリックします。



【手順⑧】

下記画面に切り替わったら設定完了です。



## 2 段階認証設定後のログイン方法

### 【手順①】

Google Chrome にログインを試み下图の画面が表示されてから、Android または iPhone 上の Google アプリを立ち上げます。



### 【手順②】

アプリを立ち上げると下記画面が表示されます。デバイスとログインしている場所が正しければ「はい、私です」をクリックします。覚えのない不審なアクセスの場合は「いいえ、ログインしません」をクリックします。



【手順③】

FaceID を利用している場合は下記のように使用を許可の確認が出るため「OK」をタップします。FaceID の認証が完了すると Google にログインが完了します。



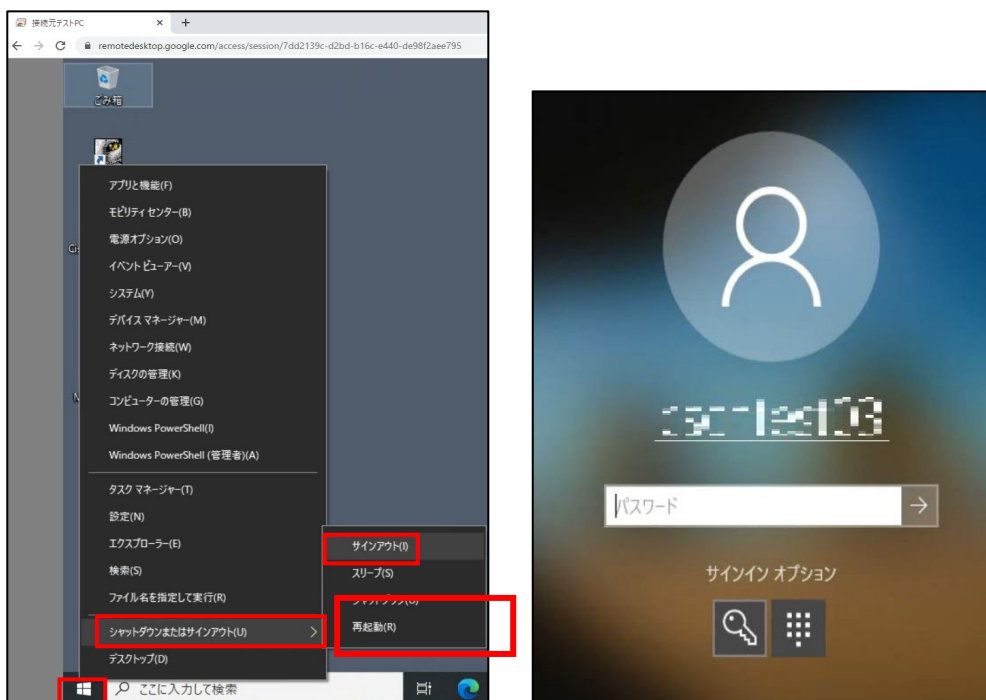
## 注意事項

### Chrome リモート デスクトップ接続を終了する際の注意事項

Chrome リモート デスクトップ接続で以下の手順を実施しない場合、正確にログが記録されず、管理者が不正利用に気が付きにくくなります。そのため、必ず下記手順で終了してください。

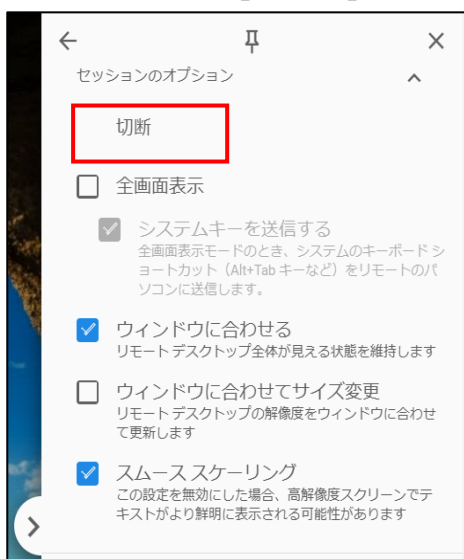
#### 【手順①】

接続先端末で、スタートメニューを右クリックし、「シャットダウンまたはサインアウト」から「サインアウト」をクリック後、サインイン画面になるのを確認します。シャットダウンやスリープを選択すると、次回以降リモート接続できなくなってしまうため、誤って選択しないように注意してください。



#### 【手順②】

「セッションのオプション」の「切断」をクリックし、Chrome リモート デスクトップを切断します。



【手順③】

Google からログアウトします。

