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
（Google ドライブ）

Ver1.2 (2025.03)

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
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、Google ドライブ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

本製品のライセンス形態は「Business Starter（有償）」「Business Standard（有償）」「Business Plus（有償）」「Enterprise（有償）」が存在します（2024 年 11 月 5 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様に提供するものであり、明示であることと黙示であることを問わず、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、2024 年 11 月 5 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
3-1　アクセス制御・認可 **許可された人のみが重要情報を利用できるよう、システムによるアクセス制御やファイルに対するパスワード設定等を行う。**	・ドライブとドキュメントの共有 ・アプリレベルでのアクセス制御	P.6 P.8
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。**	・監査ログの確認方法	P.14
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。**	・パスワードポリシーの設定	P.16
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。**	・パスワード変更要求設定	P.18
9-4　アカウント・認証管理 **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。**	・2 段階認証のポリシー設定	P.20
10-1　特権管理 **テレワーク端末やテレワークで利用する各システムの管理者権限は、業務上必要な最小限の人に付与する。**	・管理者権限の付与	P.22
10-2　特権管理 **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。**	・管理者アカウントのパスワード要件	P.24
10-3　特権管理 **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。**	・管理者権限の管理	P.24

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
3-1　アクセス制御・認可 **許可された人のみが重要情報を利用できるよう、システムによるアクセス制御やファイルに対するパスワード設定等を行う。**	・ファイルやフォルダーの共有設定	P.25
6-1　通信暗号化 **Web メール、チャット、オンライン会議、クラウドストレージ等のクラウドサービスを利用する場合（特に ID・パスワード等の入力を求められる場合）は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。**	・サービスへの接続確認	P.27
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。**	・Google アカウントへのログインデバイスの確認方法	P.28
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。**	・パスワード要件	P.30
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。**	・初期パスワード変更	P.30
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。**	・パスワード入力制限	P.32
9-4　アカウント・認証管理 **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。**	・2 段階認証プロセスの設定	P.33

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 3-1 への対応

3-1-1 ドライブとドキュメントの共有設定

ドライブとドキュメントの共有を制限することによって、関係者以外のアクセスによる情報漏洩のリスクを低減することができます。

【手順①】

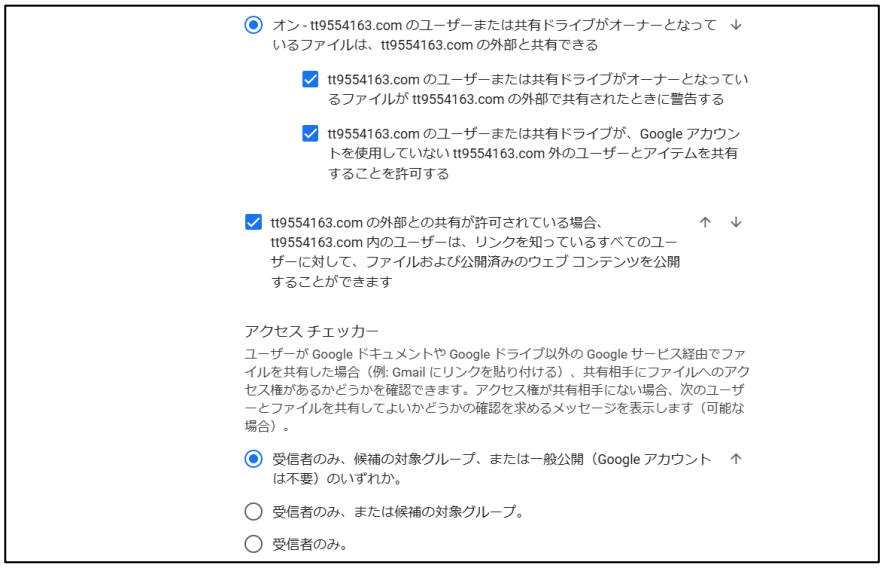
管理コンソールから「アプリ」-「Google Workspace」-「ドライブとドキュメント」をクリックし設定画面を開きます。

【手順②】

「共有設定」をクリックし、「組織部門」から組織を選択します。

【手順③】

「共有オプション」から組織の要件に従って共有先の範囲、共有時のアクション、共有元ユーザーの範囲を設定します。



3-1-2　アプリレベルでのアクセス制御

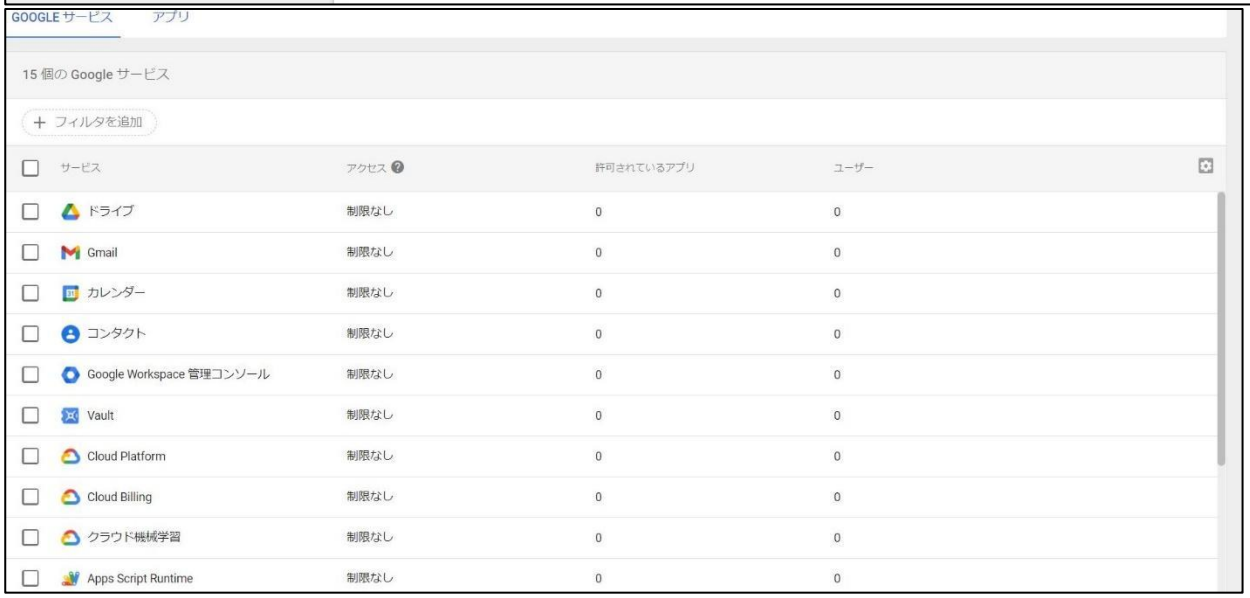
Google ドライブの API にアクセスできるサードパーティ製アプリを指定することによって、不審なアプリからのアクセスを防ぐことができます。

【手順①】

管理コンソールから「セキュリティ」-「API の制御」をクリックします。

【手順②】

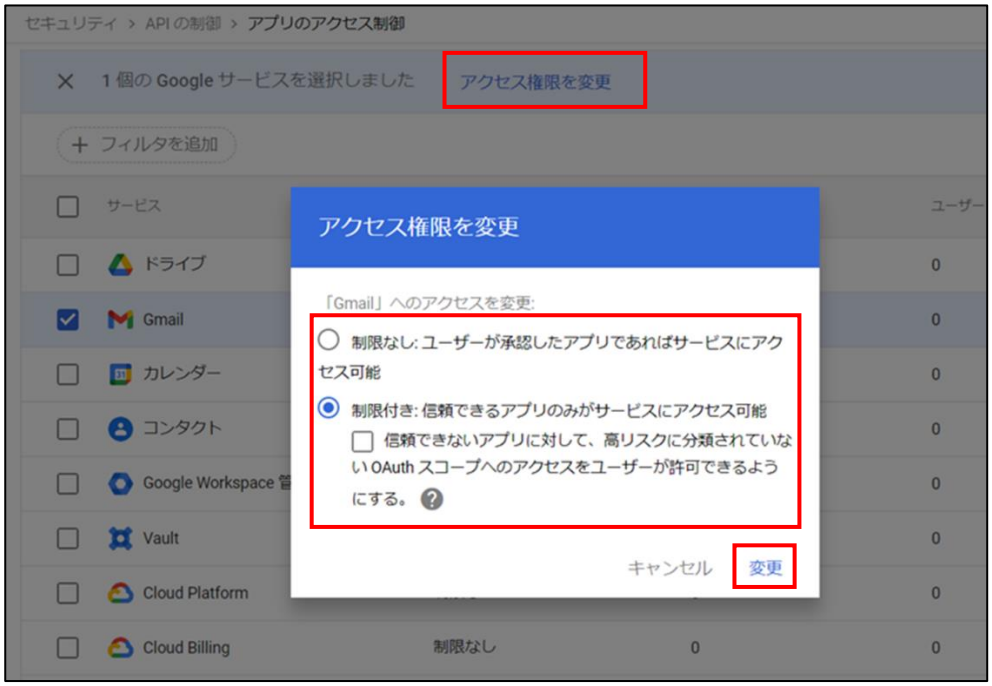
アプリのアクセス制御の「Google サービスを管理」をクリックし、サービスのリストを表示します。



【手順③】

GOOGLE サービスの一覧から「ドライブ」を選択後、「アクセス権限を変更」をクリックします。「アクセス権を変更」画面で、「制限付き」を選択し、「変更」をクリックします。

アクセス権を変更画面で、「制限付き」または「制限なし」を選択、「変更」をクリックしてアクセス制御を行います。「制限付き」を選択、かつアクセスを許可するサードパーティ製アプリがある場合は、次の手順に進みます。



【手順④】

以下の画面まで戻り、「サードパーティ製アプリのアクセスを管理」をクリックします。

【手順⑤】

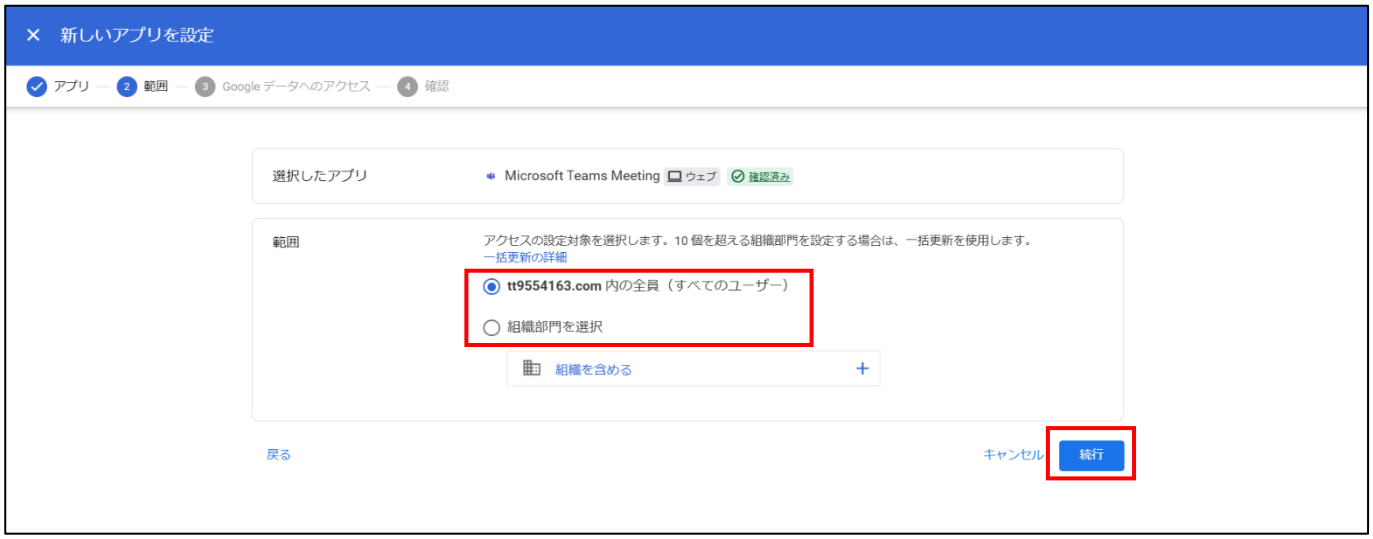
「新しいアプリを設定」を選択します。

【手順⑥】

検索欄に Google ドライブに API 接続を許可するアプリ名を入力し、「検索」をクリックします。表示されたアプリ一覧から対象のアプリにカーソルを当て「選択」をクリックします。

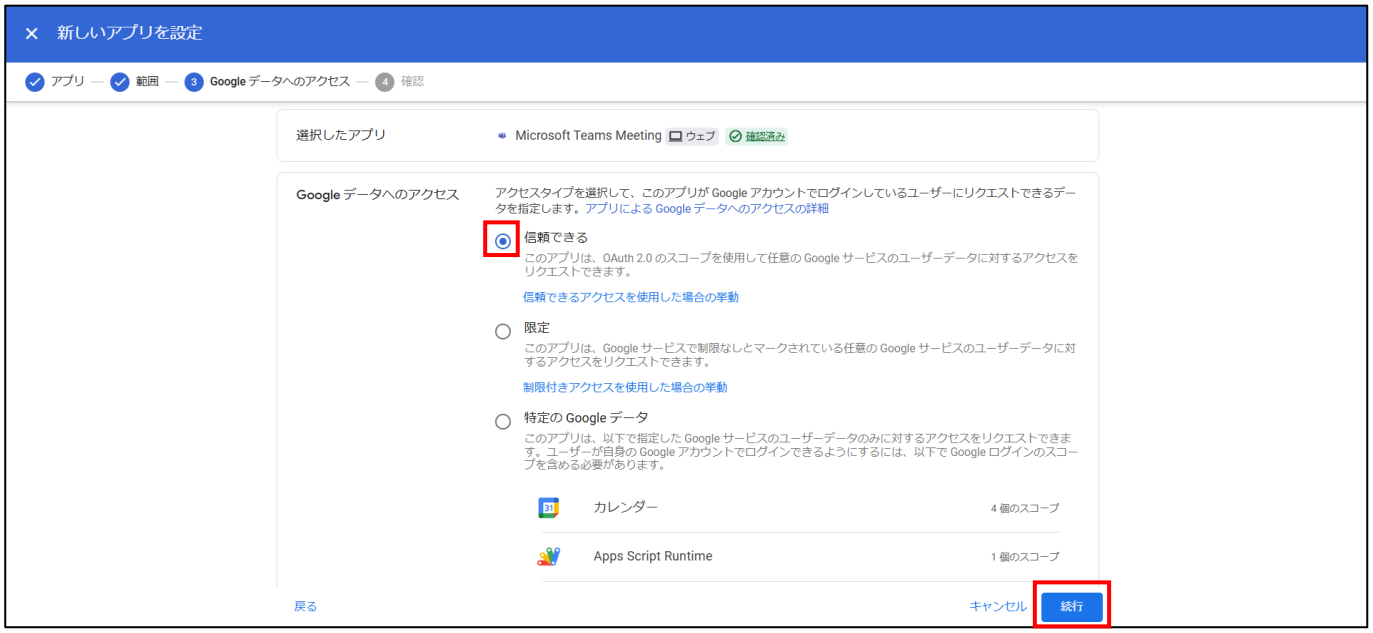
【手順⑦】

アクセスの設定範囲を選択し、「続行」をクリックします。



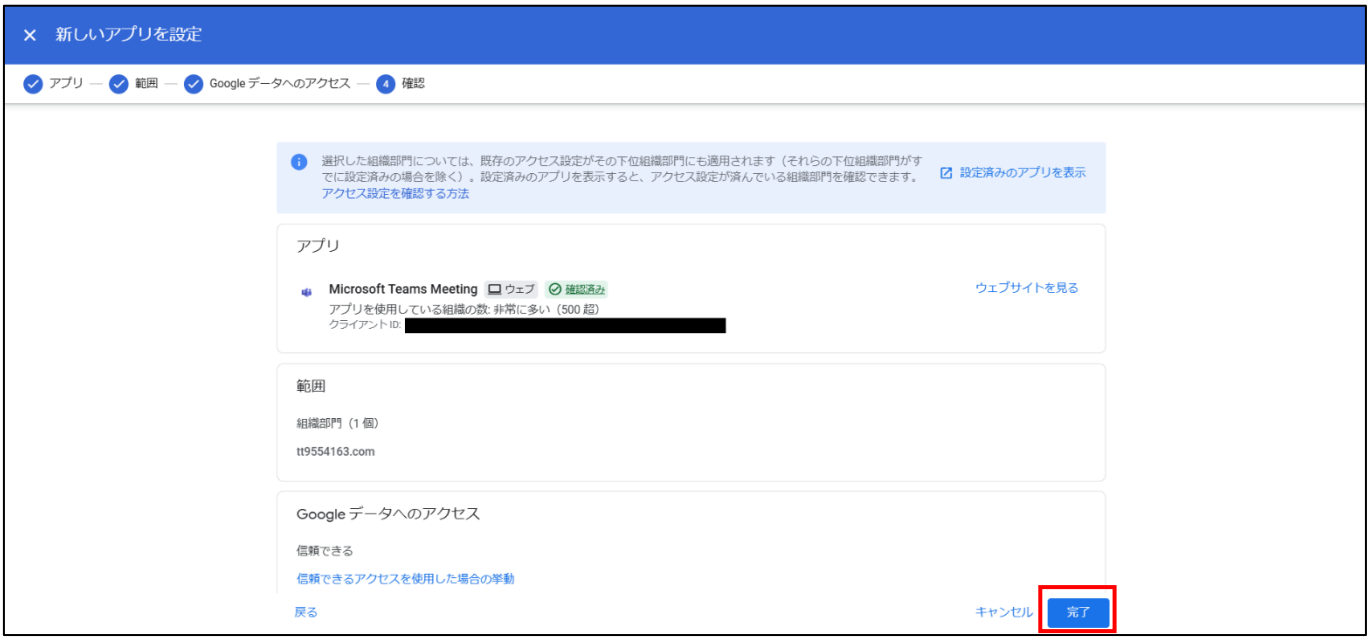
【手順⑧】

「信頼できる」にチェックし、「続行」をクリックします。



【手順⑨】

「完了」をクリックします。



【手順⑩】

追加が完了すると一覧に対象のアプリが追加されます。

3-2　チェックリスト 7-3 への対応

3-2-1 監査ログの確認方法

監査ログより、ユーザーのログイン履歴やドライブへのアクセスログを確認することができます。**ユーザーの不正アクセスがないか確認することにより Google ドライブのセキュアな運用を行うことができます。**

ここでは以下の確認方法を記載します。

- ユーザーのログイン履歴の確認
- ドライブへのアクセスログの確認

ユーザーのログイン履歴の確認

【手順】

管理コンソールから、「監査と調査」-「ユーザーのログイベント」をクリックします。

ドライブへのアクセスログの確認

【手順】

管理コンソールから、「レポート」-「監査と調査」-「ドライブのログイベント」をクリックします。

3-3　チェックリスト 9-1 への対応

3-3-1 パスワードポリシーの設定

管理者はパスワードポリシーを設定することにより強度の強いパスワード設定をユーザーに要求できます。**パスワードポリシーにより、強度の弱いパスワードを使用されるリスクを低減することができます。**

【手順①】

Google 管理コンソールを開き、「セキュリティ」-「概要」-「パスワードの管理」をクリックします。

【手順②】

左側で、パスワード ポリシーを設定する組織部門を選択します。

安全度：「安全なパスワードを適用する」チェックボックスをオンにします。

長さ：ユーザーのパスワードに設定する最小文字数と最大文字数を入力します。文字数は 8～100 文字の間で指定できます。

次回ログイン時にパスワード ポリシーを適用する：ユーザーに強制的にパスワードを変更させたい場合は、チェックボックスをオンにします。このチェックボックスをオンにしない場合、使用しているパスワードが脆弱であっても、現在のパスワードを使い続ける間は組織の Google サービスにアクセスできます。

パスワードの再利用を許可：ユーザーが過去に使用したパスワードを再利用できるようにするには、チェックボックスをオンにします。再利用できないパスワードとして Google が確認するパスワードの履歴を指定することはできません。

有効期限：パスワードが期限切れになるまでの期間を選択することができます。パスワードの有効期限はデフォルトで無効になっています。パスワードの定期変更によるセキュリティ上の効果は薄いという調査結果があるためです。コンプライアンス上の理由で必要な場合は、ユーザーのパスワードの有効期限を設定できます。

【参考】ユーザーのパスワード要件を適用、監視する

URL：https://support.google.com/a/answer/139399?hl=ja

3-4　チェックリスト 9-2 への対応

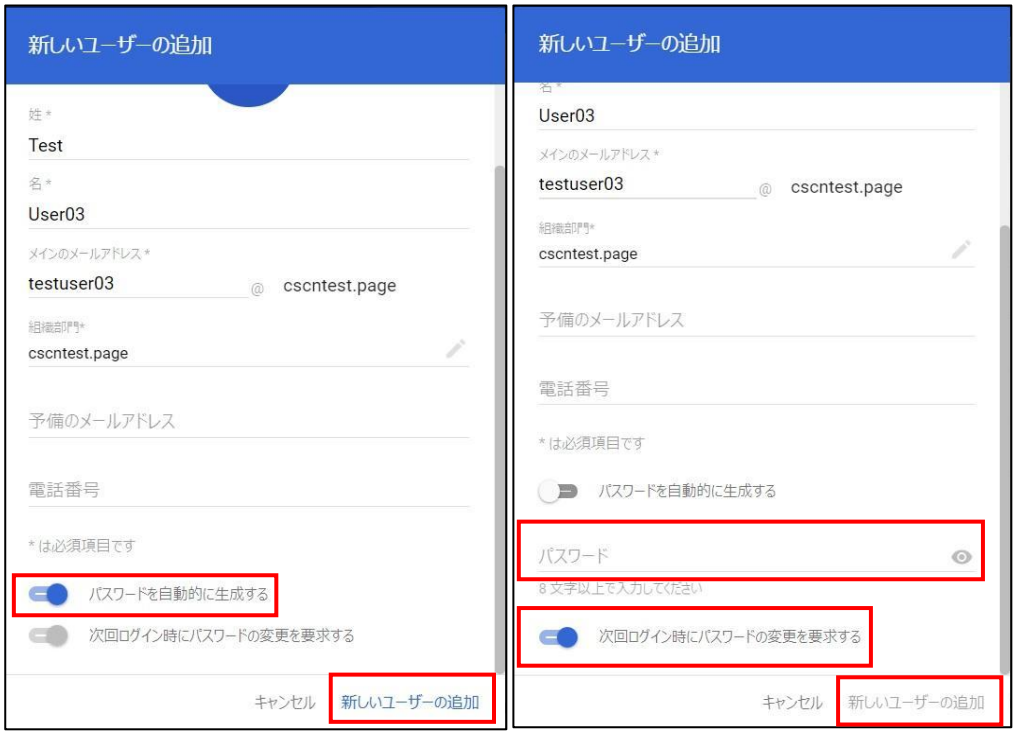
3-4-1 パスワード変更要求設定

管理者により、ユーザーアカウント発行時やパスワードを再設定する際に、**「次回ログイン時にパスワードの変更を要求する」をオンにしておく**ことで、ユーザーがログイン時に管理者から知らされたパスワードでログイン後、パスワード変更を促されることになります。

これにより、ユーザーが初期パスワードや再設定したパスワーを変更せずに使い続けることを防げます。

新しいユーザー追加時のパスワード変更要求設定

ランダムなパスワードを初期設定したい場合は、「パスワードを自動的に生成する」をオンにします。または、任意のパスワードで初期設定したい場合は、「パスワードを作成する」を選択し、初期設定するパスワードを入力、「次回ログイン時にパスワードの変更を要求する」をオンにします。最後に「新しいユーザーの追加」をクリックします。



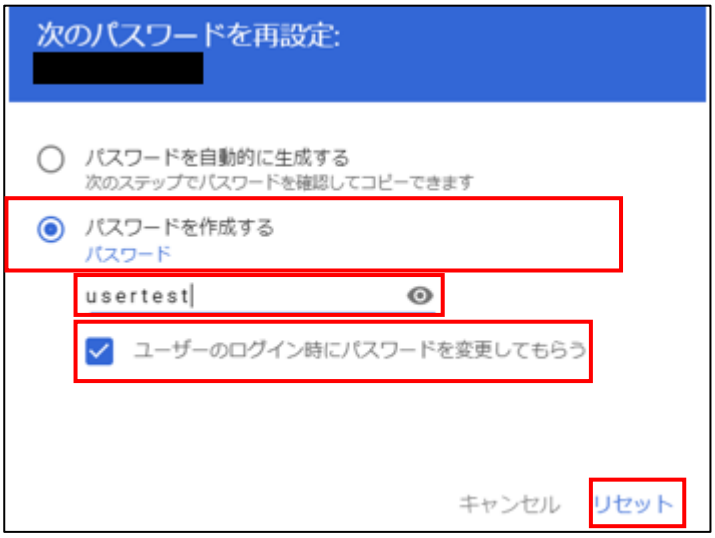
既存ユーザーのパスワード再設定時のパスワード変更要求設定

【手順①】

管理コンソールから「ディレクトリ」-「ユーザー」でユーザー情報が表示された後、パスワードを再設定するユーザーの「パスワードを再設定」をクリックします。

【手順②】

ランダムなパスワードを初期設定したい場合は、「パスワードを自動的に生成する」を選択します。または、任意のパスワードで初期設定したい場合、「パスワードを作成する」を選択し、初期設定するパスワードを入力、「ユーザーのログイン時にパスワードの変更を要求する」をチェックします。最後に「リセット」をクリックします。



3-5　チェックリスト 9-4 への対応

3-5-1 2 段階認証のポリシー設定

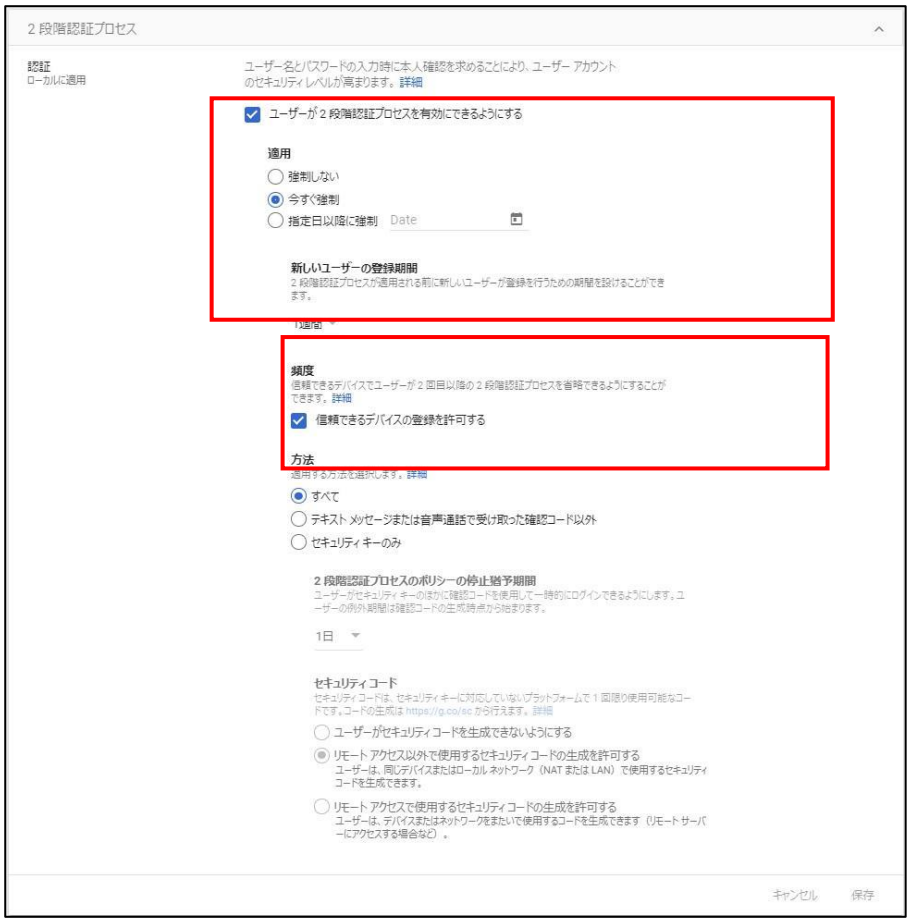
2 段階認証を有効化することにより、ログインするためにパスワードだけでなく SMS で受け取った一時的なコードなど追加の認証情報が求められるようになります。**2 段階認証の設定によりパスワードが破られた場合でも、不正ログインを防ぐことができます。**

【手順①】

管理コンソールから、「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。



「指定日以降に強制」を選択した場合は、**「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。**

「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」を選択した場合は、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。

3-6　チェックリスト 10-1 への対応

3-6-1 管理者権限の付与

管理者権限を付与するユーザーを限定することで、Google ドライブの設定変更できるユーザーを必要最小限に抑え、**悪意のあるユーザーにより、意図しない設定変更が行われるリスクを低減**することができます。

下記手順により、管理者権限をユーザーに付与することができます。

【手順①】

管理コンソールから「ディレクトリ」-「ユーザー」-設定対象のユーザーをクリックします。

【手順②】

管理者にしたいユーザーをクリックして開き、「管理者ロールと権限」から「ロールを割り当ててください」をクリックします。

【手順③】

割り当てたいロールの割り当てをオンにします。ただし、すべての権限を持つ「特権管理者」というロールを割り当てるユーザーは必要最小限とし、各ユーザーにはそれぞれの管理業務に合わせたロールを割り当てるようにします。

3-7　チェックリスト 10-2 への対応

3-7-1 管理者アカウントのパスワード要件

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

3-8　チェックリスト 10-3 への対応

3-8-1 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。

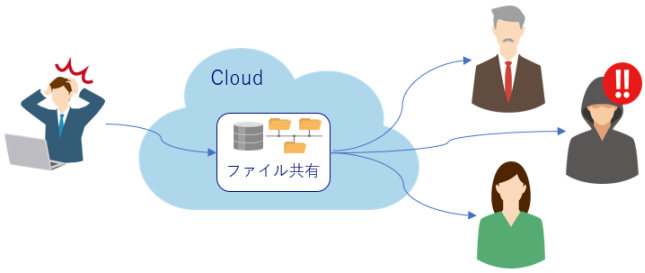
4　利用者向け作業

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 3-1 への対応

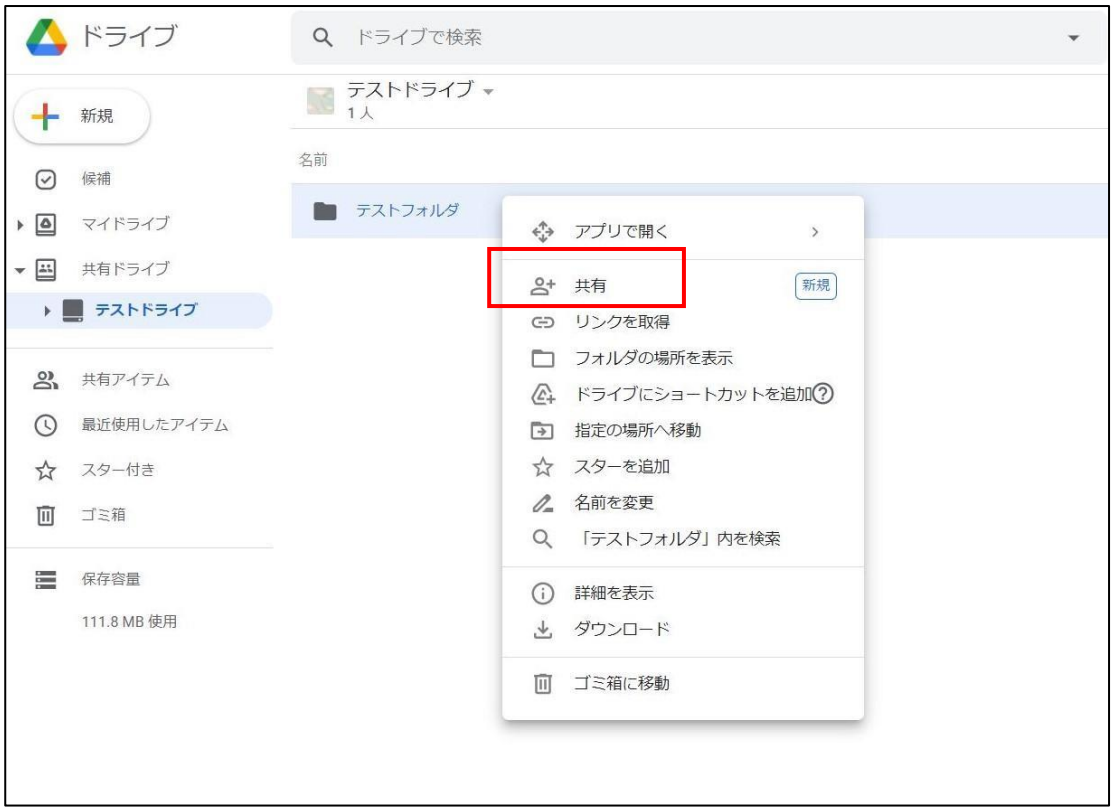
4-1-1 ファイルやフォルダーの共有設定

ユーザーの作成したフォルダーやファイルを組織の外部のユーザーに共有することができます。**関係者以外に共有しないよう、十分に注意して共有設定を行ってください。**



【手順①】

Google ドライブを開き、左側メニュー「共有ドライブ」をクリックし、任意のドライブを選択後、右クリックし、「共有」をクリックします。



【手順②】

「ユーザーやグループと共有」画面に任意のユーザーを入力、「閲覧者」「閲覧者（コメント可） 」「投稿者」「コンテンツ管理者」のいずれかを選択し、「送信」をクリックします。

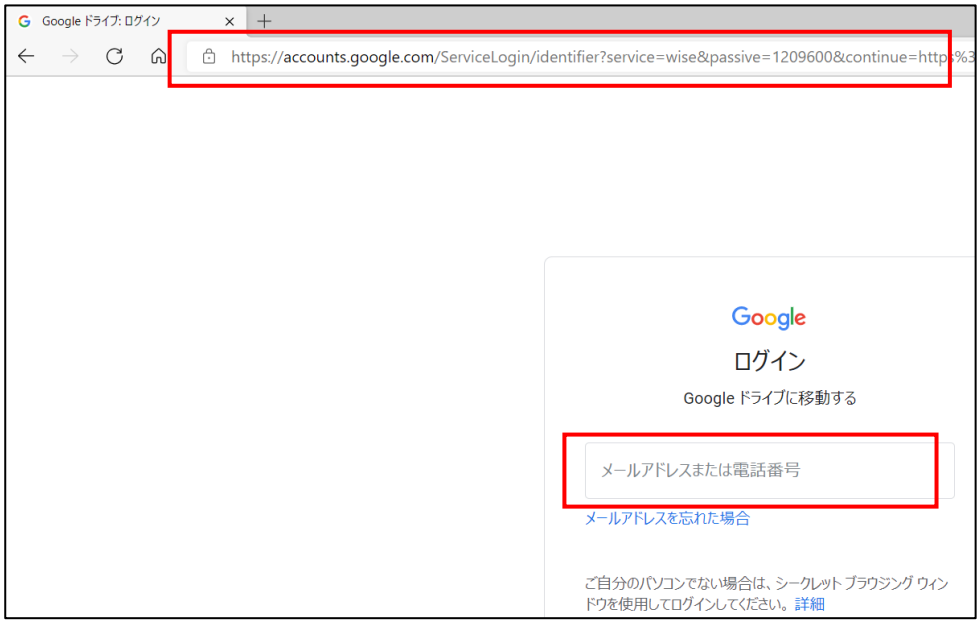
リンクを取得してリンクを共有したユーザーへの共有もできます。リンクを知っているユーザーは誰でもアクセスできてしまうため、一時的な共有の場合に限定してこの共有方法を使用することを推奨します。

4-2　チェックリスト 6-1 への対応

4-2-1 サービスへの接続確認

Google ドライブの URL として、第三者から共有されたものについては、**不正なアクセス先（Google ドライブのドメインではない等）でないことを確認する**ようにします。

また、**使用するアカウントが、個人アカウントではなく、業務利用アカウントを使用していることを確認し、Google ドライブにアクセスします。**

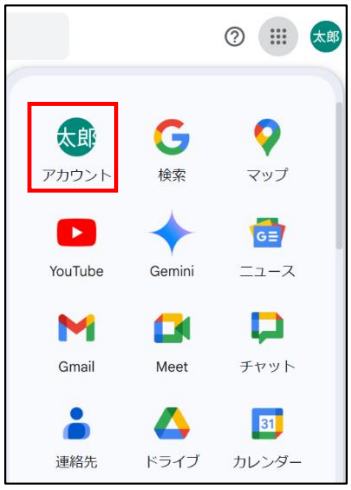


4-3　チェックリスト 7-3 への対応

4-3-1 Google アカウントへのログインデバイスの確認方法

最近ログインが行われたデバイスを確認することにより、**不正ログインがなかったかをユーザー自身で認知することができます**。
心当たりのないデバイスが確認できた際は、速やかにパスワードを変更することで、不正ログインをブロックすることができます。

【手順】①】
左上 Google アプリ-「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。

【手順④】

使用した心当たりのない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。その後、次の手順で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 パスワード要件

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

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ため、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「パスワードの変更」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。

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②】

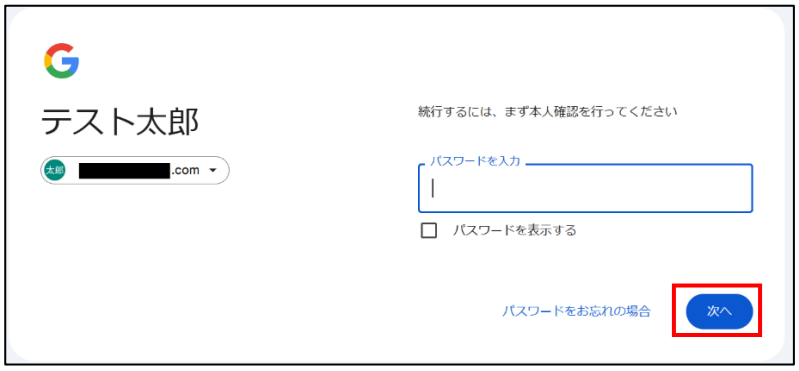
右上 Google アカウントアイコンの「Google アカウントを管理」をクリックします。

【手順③】

「個人情報」-「その他の情報と Google サービスの設定」-「パスワード」をクリックします。

【手順④】

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⑤】

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 9-3 への対応

4-6-1 パスワード入力制限

パスワードの入力を複数回誤ると、パスワードの入力に加えて画面に表示されたテキスト入力を求める画面が表示される場合があります。

4-7　チェックリスト 9-4 への対応

4-7-1 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。**

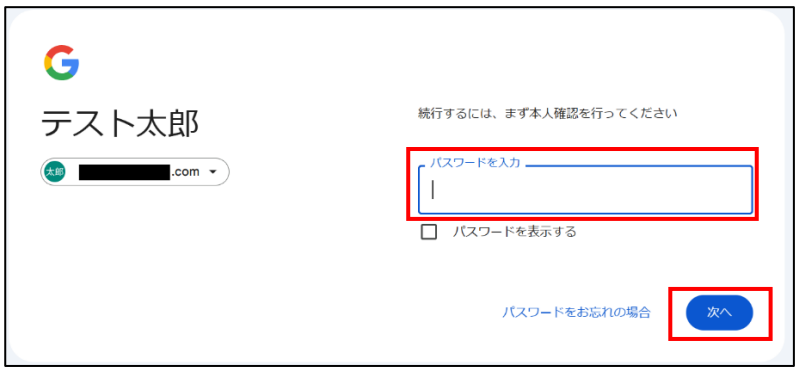
2 段階認証の登録が強制される場合

【手順①】

ログイン時に、下記画面に遷移した場合、「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。

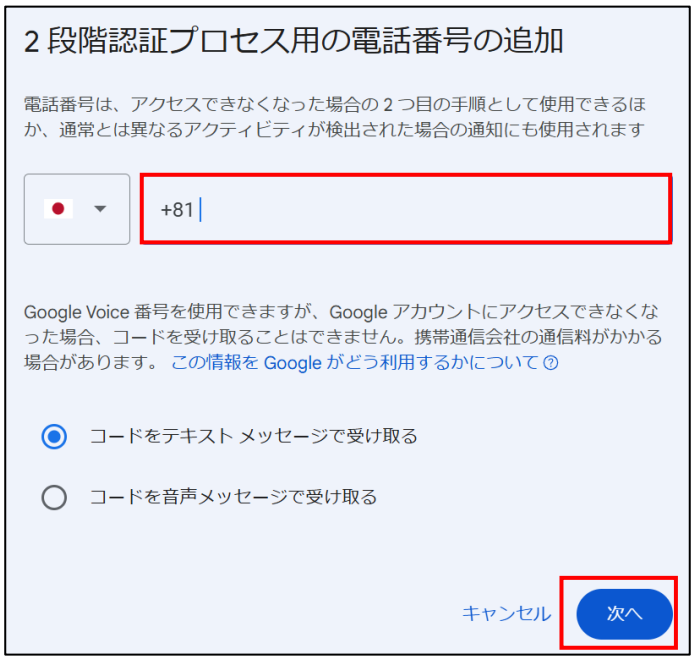


【手順③】

2 段階認証のプロセス画面の表示し、「2 段階認証プロセスを有効にする」をクリックします。

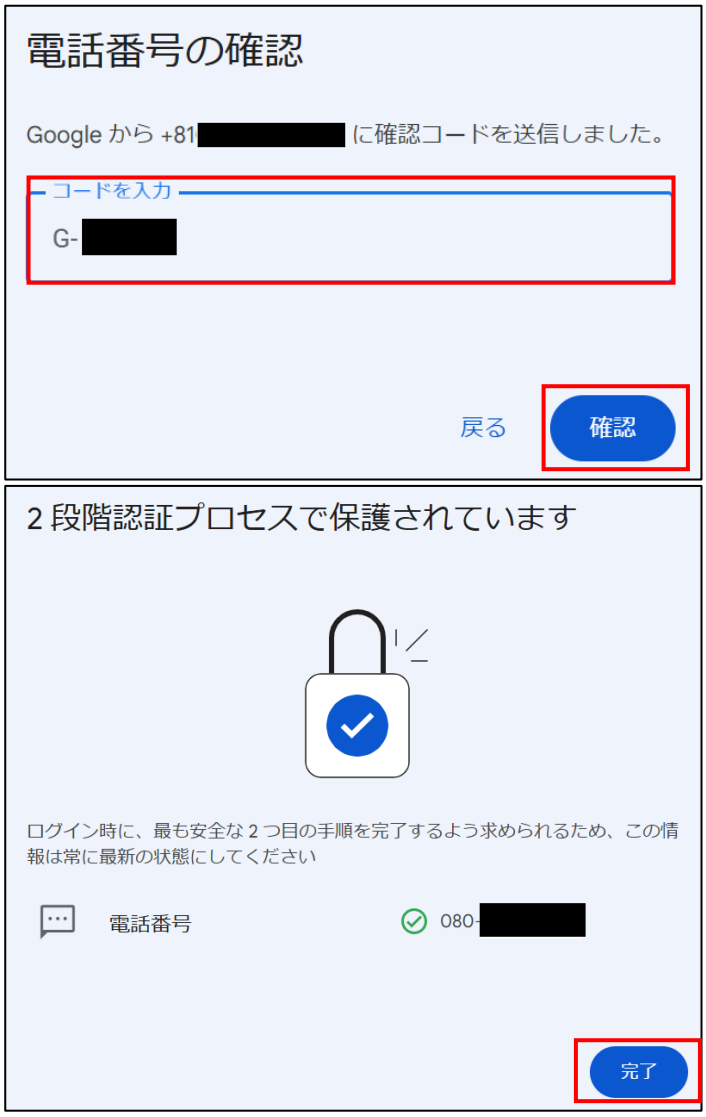
【手順④】

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、「確認」をクリックし、「完了」をクリックします。



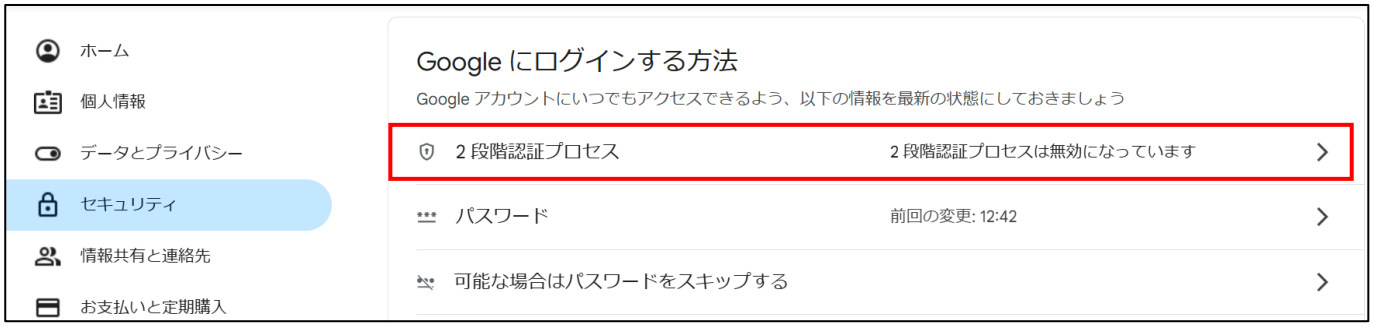
2 段階認証の登録を強制されない場合

【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。

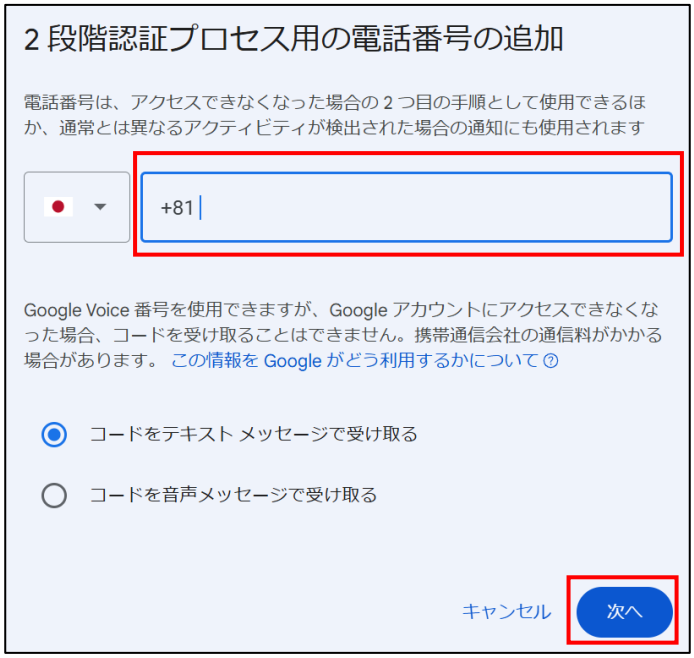


【手順③】

2 段階認証のプロセス画面において、「2 段階認証プロセスを有効にする」をクリックします。

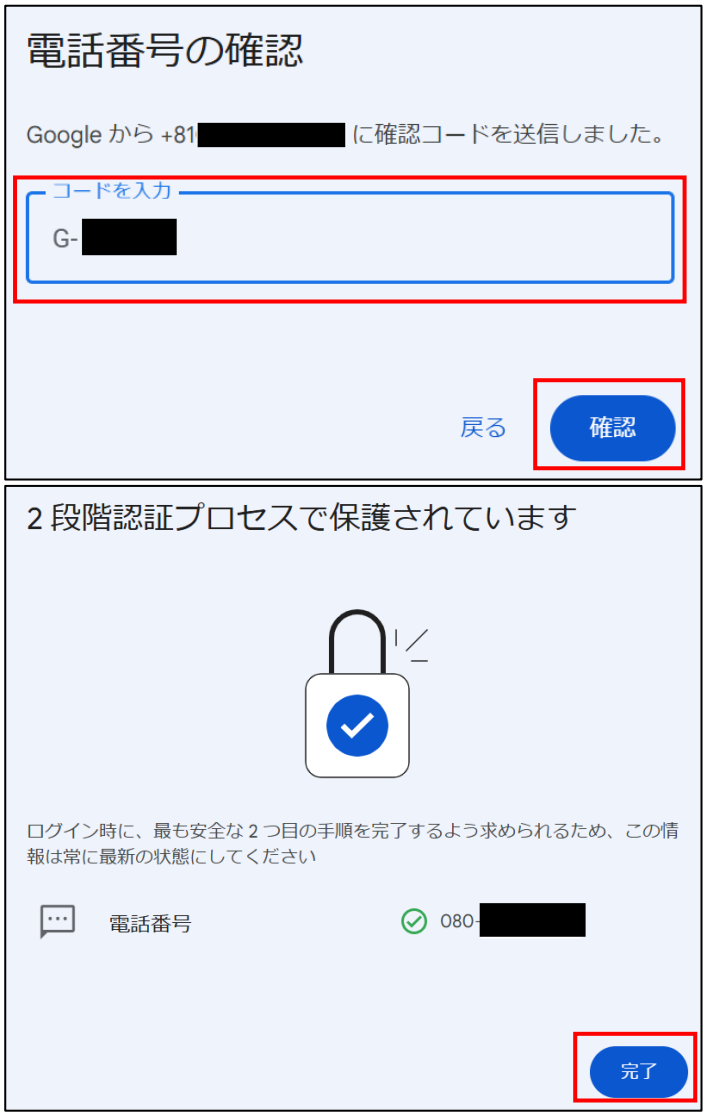
【手順④】

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。



【手順⑤】

確認コードを入力し、「確認」をクリック後、「完了」をクリックします。



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】

「パスキーとセキュリティキー」をクリックします。

【手順④】

下記画面が表示されたら「パスキーを作成する」をクリックします。

【手順⑤】

「パスキーを作成」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。

【参考】設定後のログイン方法

【手順①】

Google Chrome にログインをしようとすると下記表示になります。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。