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 Meet）

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
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 Meet 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（Google Meet）のライセンス形態には「Business starter（有償）」「Standard business（有償）」「Business Plus（有償）」「Enterprise（有償）」が存在します。（2023 年 11 月 7 日現在）利用するライセンス形態により使用できる機能が異なります。**本資料は小規模チーム向けの「Standard business（有償）」ライセンスの利用を前提としています。**

(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、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
3-3 アクセス制御・認可 **オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。**	・端末と利用者の把握	P.7
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.9
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.10
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.12
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.14
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.17
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	P.19
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は、必要な作業時のみ利用する。**	・管理者権限の管理	P. 19

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
3-3　アクセス制御・認可 **オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。**	・ミーティング時の本人確認	P.20
3-5　アクセス制御・認可 **オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。**	・不適切な参加者の強制退室	P.21
4-1　物理セキュリティ **テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。**	・第三者からの盗聴・覗き見の対策	P.22
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.22
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。**	・セキュリティ関連操作の確認方法	P.23
8-5　データ保護 **オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対してはパスワードの設定や期間指定の自動削除等を実施するよう周知する。また、上記ルールは可能な限り設定を強制する。**	・ミーティング情報の件名に機密情報の記載禁止 ・ミーティング録画ファイルの削除	P.25 P.26
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。**	・パスワード強度	P.27
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.27
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.29
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.30

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 3-3 への対応

3-1-1　端末と利用者の把握

この項目では主催者が参加者の入退室をコントロール及び認識するための設定を行います。会議の途中で**不正な参加者が参加したときに、情報漏洩するリスクを低減**することができます。

主催者より先の入室を禁止する

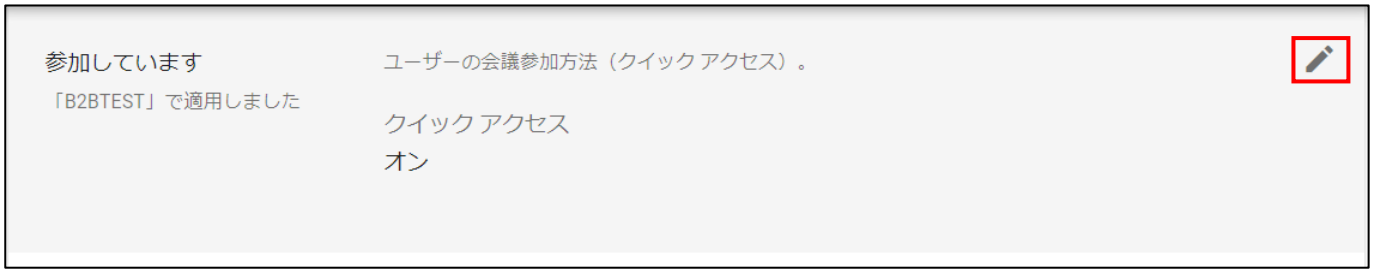
外部出席者が主催者の同意なしにスケジュール済みミーティングに加わり、ミーティングを自由に操作できてしまうことを防ぎます。

【手順①】

Google workspace　（https://admin.google.com/）にログインし、左上の「アプリ」-「Google Workspace」-「Google Meet」をクリックするとミーティングに関連する設定画面が表示されます。

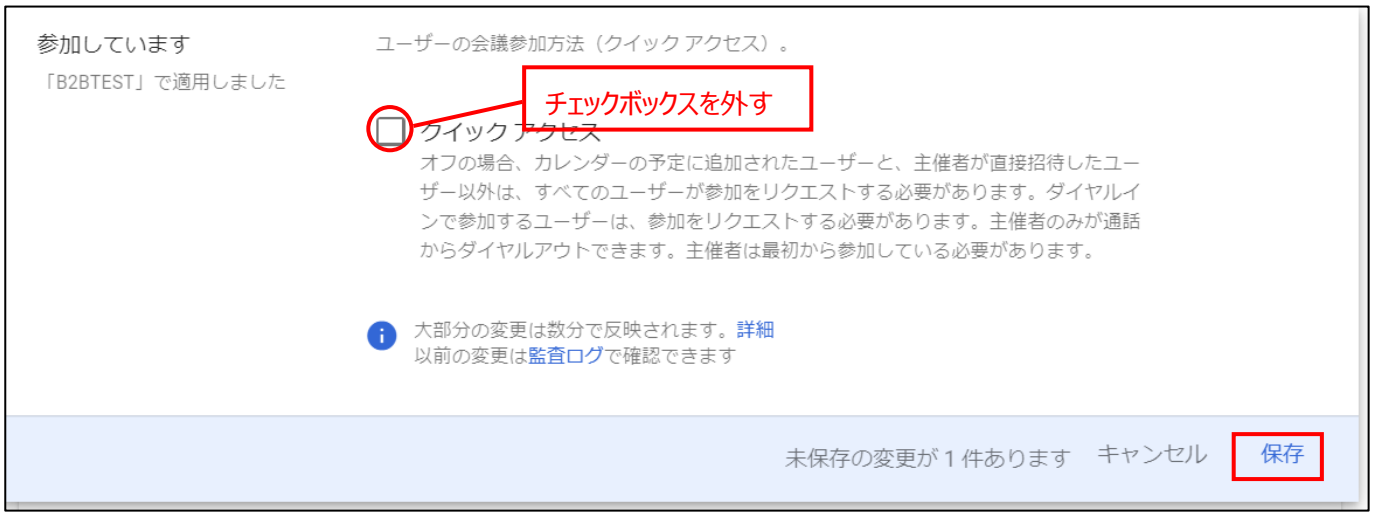
【手順②】

右側の「Meet の安全性設定」の項目内にある「参加しています」の「編集」ボタンをクリックします。



【手順③】

「クイックアクセス」のチェックボックスにチェックが入っていた場合は外し、「保存」ボタンをクリックします。



画面下部に「設定が更新されました」と表示されたら設定は完了です。

3-2　チェックリスト 7-3 への対応

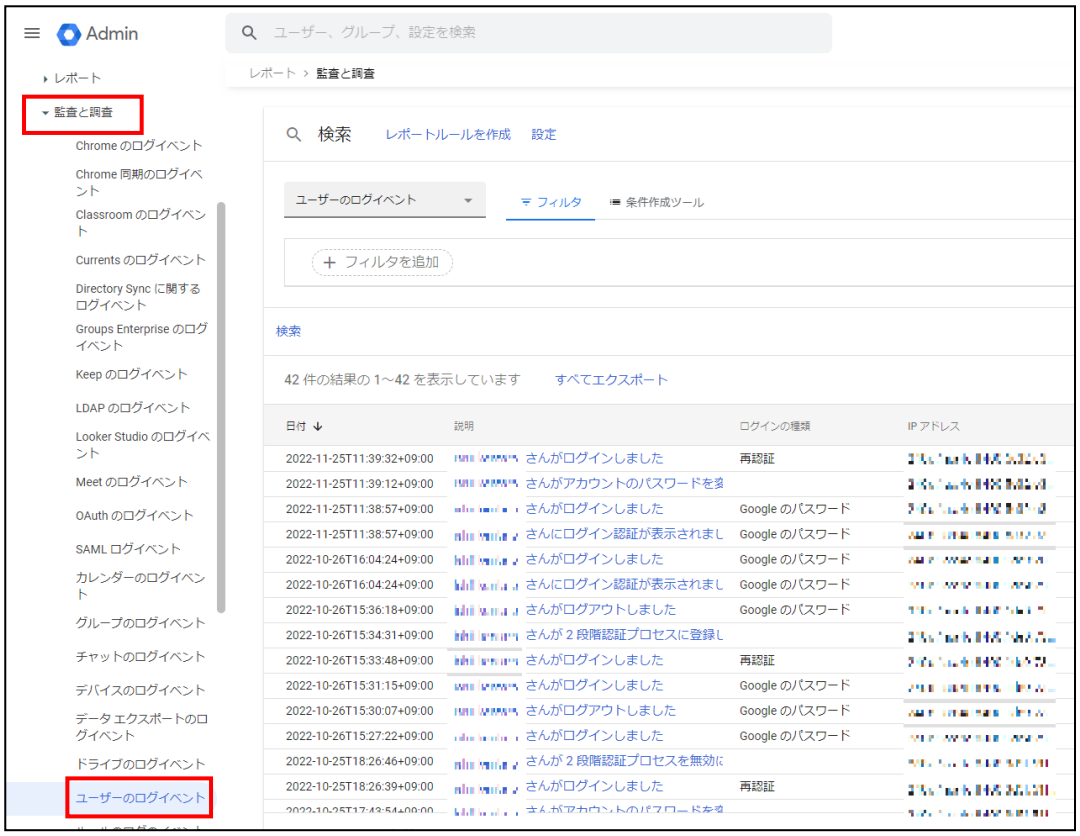
3-2-1　　監査ログの確認方法

監査ログより、ユーザーの Google Workspace へのログイン履歴を確認することができます。Google Meet 個別へのアクセスを判別することはできませんが、Workspace へのログイン履歴から**ユーザーの不正アクセスがないか定期的に確認することで、よりセキュアな運用を行うことができます。**

ユーザーのログイン履歴の確認

【手順①】

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。



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、強度の高いパスワード設定をユーザーに要求できます。**これにより、強度の低いパスワードが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】

「組織部門を検索」から、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」から「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」で、ユーザーが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」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すると、ユーザーが使用しているパスワードが脆弱なものである場合、次回ログイン時に、より強力なパスワードに変更するように強制することができます。

「パスワードの再利用を許可」のチェックボックスは**オフ**にします。これにより、ユーザーが過去に使用したパスワードを再利用できないようにします。次に、「有効期限」で、パスワードが期限切れになるまでの期間を選択します。

※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が、これは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有効期限の設定が必要な場合は、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

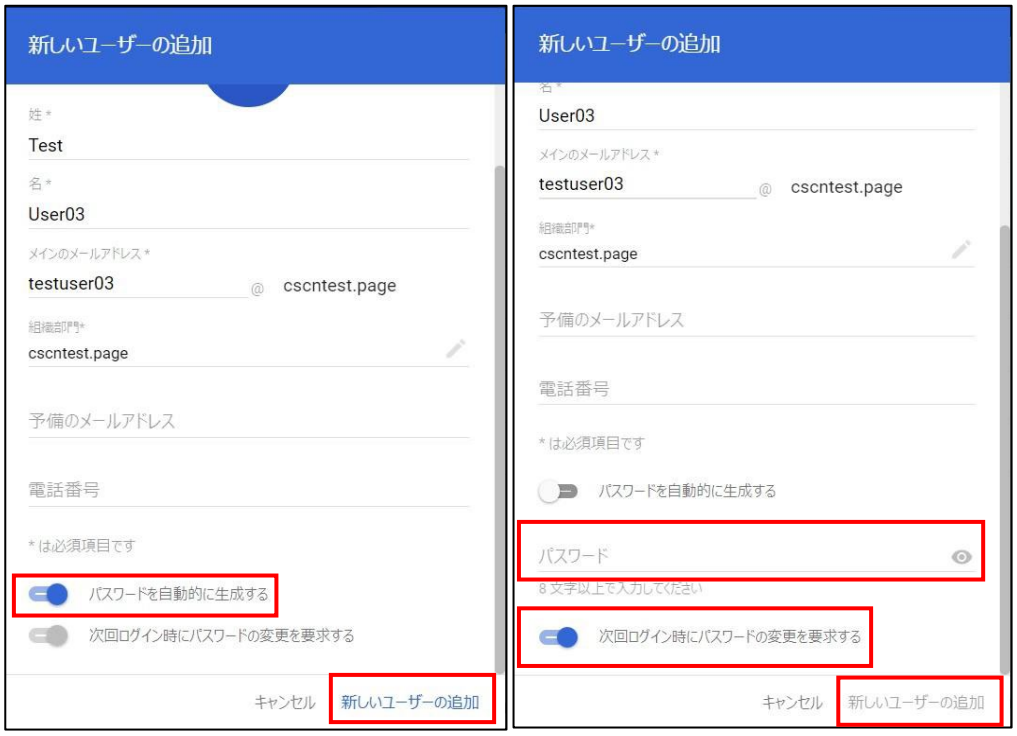
3-4　チェックリスト 9-2 への対応

3-4-1　パスワード変更要求設定

ユーザーアカウント発行時や、管理者により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通知されたパスワードでログイン後、パスワード変更を強制することができます。**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ドを変更せずに使い続けるのを防ぐことができます。**

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。



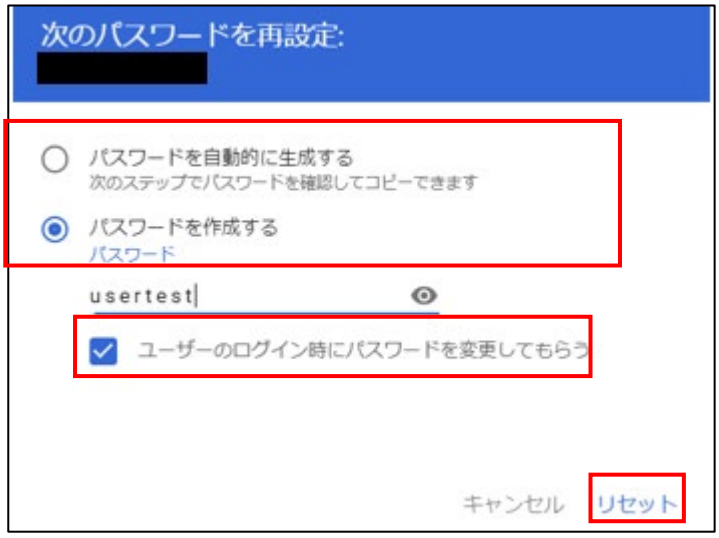
既存ユーザーのパスワード再設定時のパスワード変更要求設定

【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

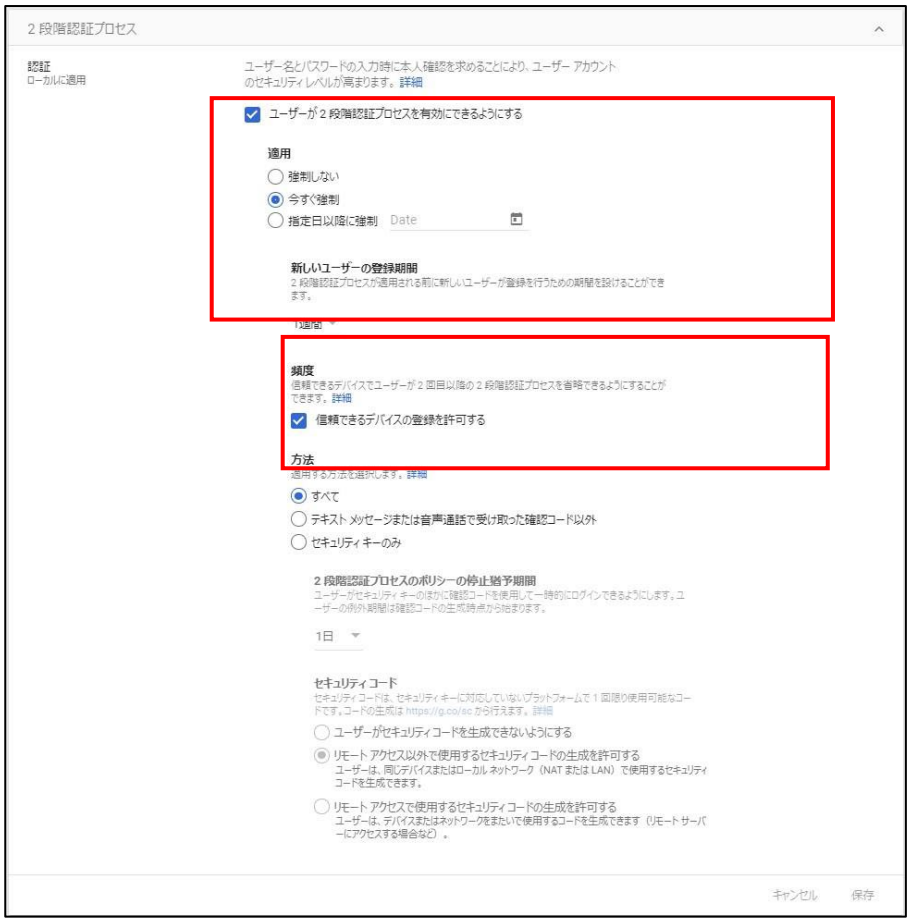
2 段階認証を有効化することにより、ログインするためにパスワードだけでなく SMS で受け取った一時的なコードなど追加の認証情報が求められるようになります。**2 段階認証の設定によりパスワードが破られた場合でも、不正ログインを防ぐことができます。**

【手順①】

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 Meet の設定変更を行え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。

管理者権限は、下記手順により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

3-8　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 3-3 への対応

４-１-１ ミーティング時の本人確認

ミーティングは、特別なアクセス制御を行わない限り**誰でも参加することができます**。また、ミーティング参加時の参加者としての表示名は、参加者側で自由に設定ができます。**なりすました不正ユーザー（※）が参加していないか確認するために、ミーティング開始時や途中参加者が入った場合はカメラの映像とマイクを有効化させ、映像と音声で本人確認することを推奨します**。

※　なりすましたユーザーによる機密情報の取得イメージ

4-2　チェックリスト 3-5 への対応

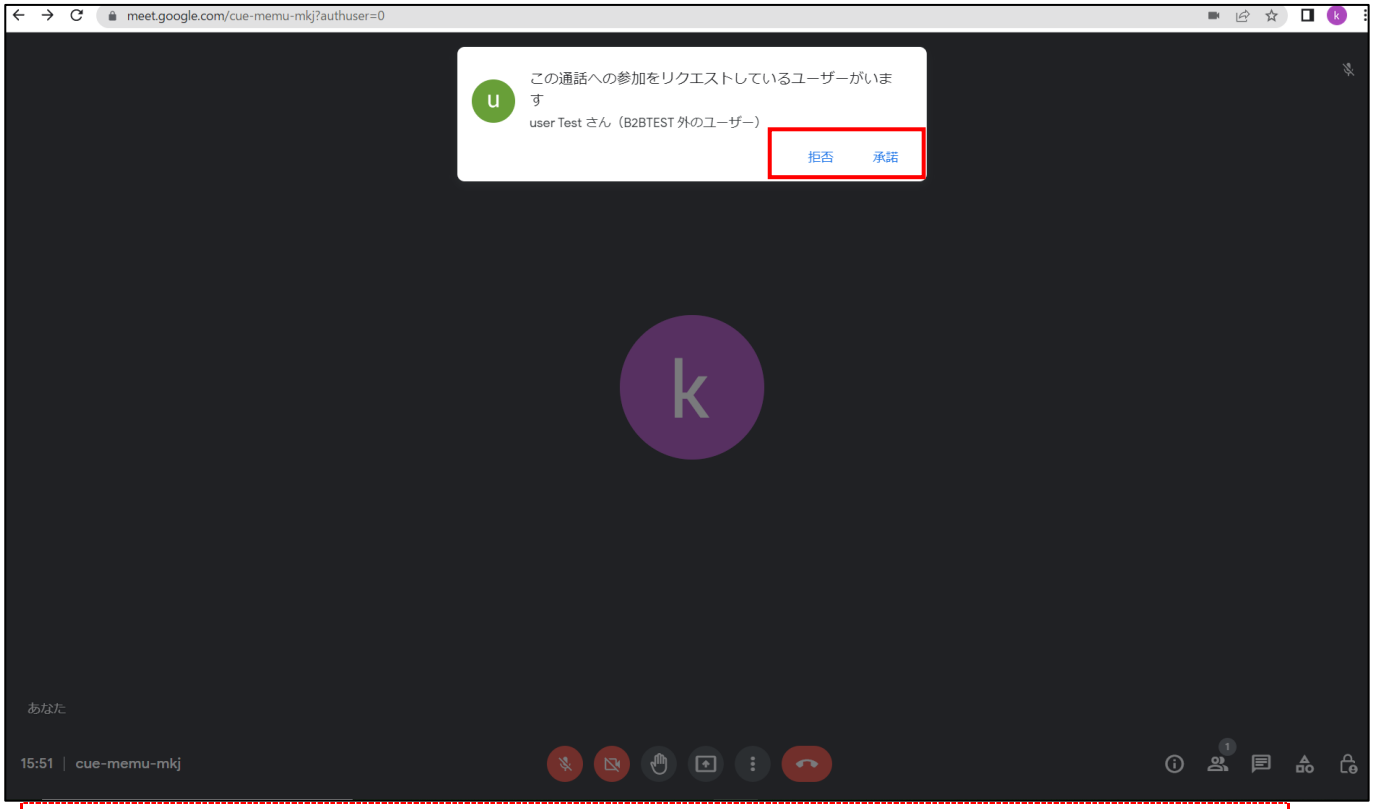
4-2-1 不適切な参加者の強制退室

Google Meet の待機室には、URL を知っていれば、**誰でも入室できてしまいます。**そのため主催者は、待機室内の参加者名を確認し、予め招待している参加者のみを許可します。

【参加メンバーの入室許可/拒否】

待機中の参加者を許可するにはミーティング画面の上部にポップアップされたリクエスト通知から選択します。

表示されたユーザーが正規の場合は「承認」、招待していない外部メンバーの場合は「拒否」をクリックします。



- **注意事項**

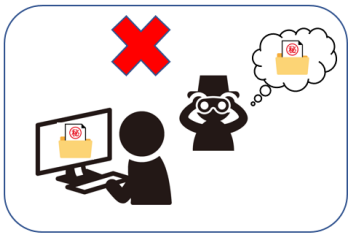
悪意のあるユーザーは、名前をなりすまして参加する可能性があります。

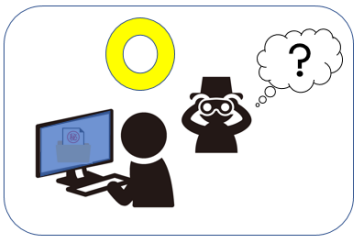
可能であればミーティング冒頭で参加者のカメラ機能を有効化して顔や音声で本人確認を実施することを推奨します。

4-3　チェックリスト 4-1 への対応

4-3-1 第三者からの盗聴・覗き見の対策

オフィス外で利用する場合は、第三者から盗聴・盗み見されないように注意する必要があります。端末上に投影されている会議資料などがのぞき見されないように**のぞき見防止フィルタを利用する**、会議音声が外部に漏れないようにイヤホンを利用する、など利用シーンにおいた対策が必要です。





4-4　チェックリスト 6-1 への対応

4-4-1 サービスへの接続確認

HTTPS 通信の確認

Google Meet でユーザーがアクセスする URL への通信は基本的に HTTPS で暗号化されていますが、**第三者から共有された URL 等については、不正なアクセス先（HTTP 通信となっているケース、Google のドメインではないケース等）でないことを確認する**ようにします。不正なアクセス先へのアクセスを回避することにより、情報を抜き取られたり、マルウェアに感染したりするリスクを低減することができます。

使用するアカウントの確認

誤って個人アカウントを利用してしまうと、業務データが個人アカウント内に連携されてしまう恐れがあります。**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 Meet にアクセスします。**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、アカウントのメールアドレスが業務利用のものであることを確認します。

4-5　チェックリスト 7-3 への対応

4-5-1 セキュリティ関連操作の確認方法

ユーザー自身が、最近行われたセキュリティ関連の操作を確認することにより、**不正アクセスや不正操作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**。心当たりのないログイン履歴が確認できた際は、速やかにパスワードを変更することで、不正アクセス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。

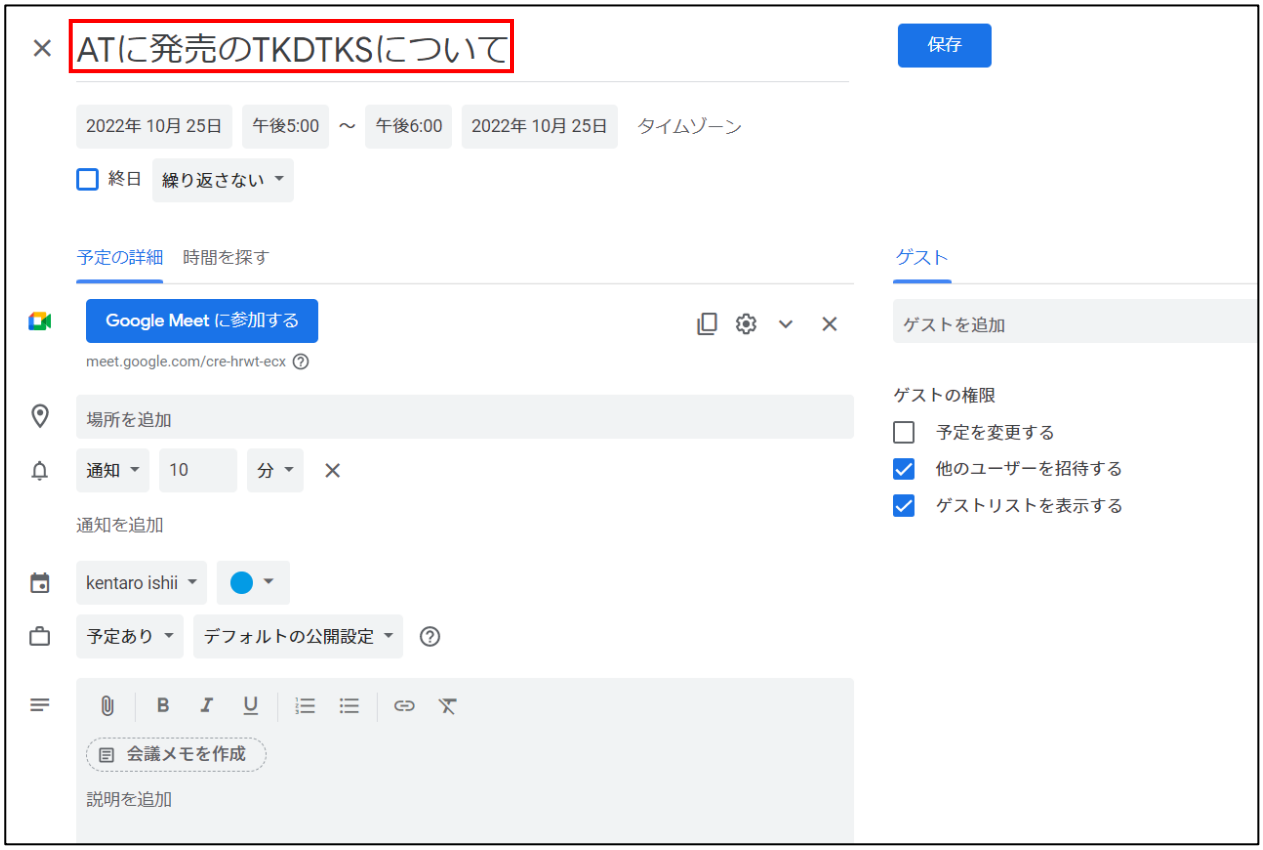
使用した心当たりのないがない端末が表示されている場合は、当該端末をクリックし、「心当たりがない場合」-「デバイスでログアウトする」をクリックします。また、その後速やかにパスワードを変更します。

4-6　チェックリスト 8-5 への対応

ここでは、**ミーティング利用時に利用者（主催者）が注意すべき事項と設定**について記載します。

4-6-1　ミーティング情報の件名に機密情報の記載禁止

会議名に**機密情報が含まれている場合、間違った相手に招待メールを送信してしまうと情報が漏洩してしまいます**。Google Meet（※Google カレンダー）ではミーティングをスケジュールする際に件名と議題を記載する項目がありますが、ここには機密情報を記載せずに参加者同士が分かる内容で記載することを推奨します。

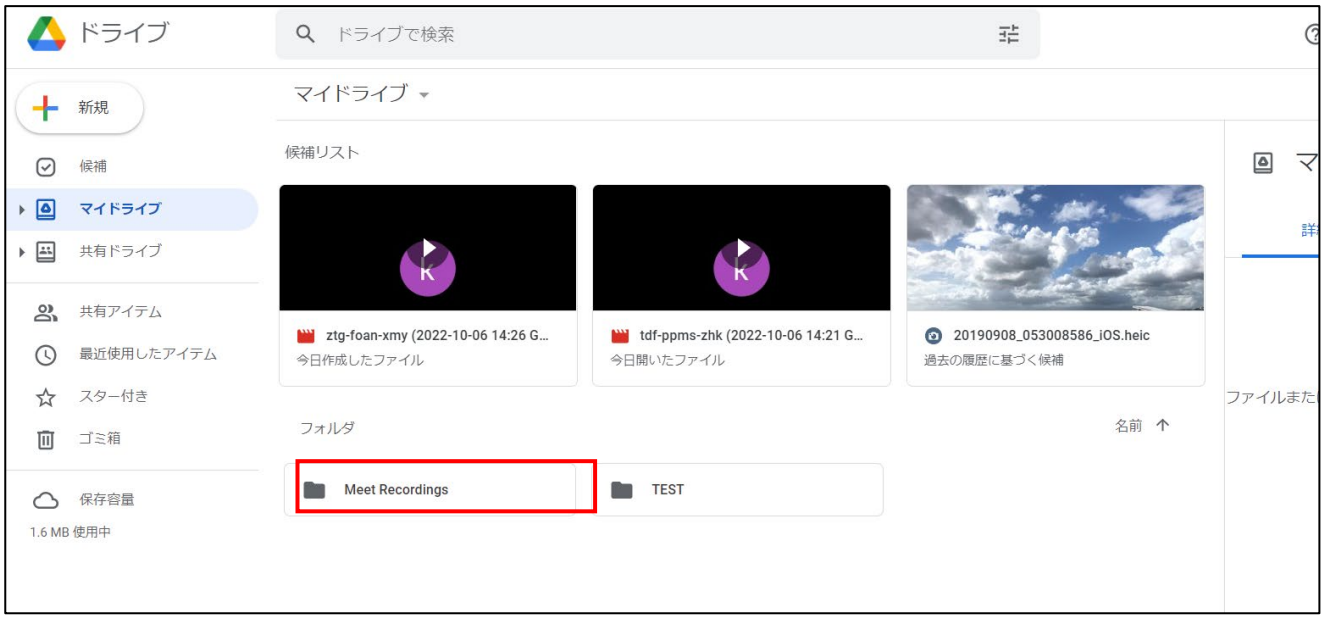


4-6-2　ミーティング録画ファイルの削除

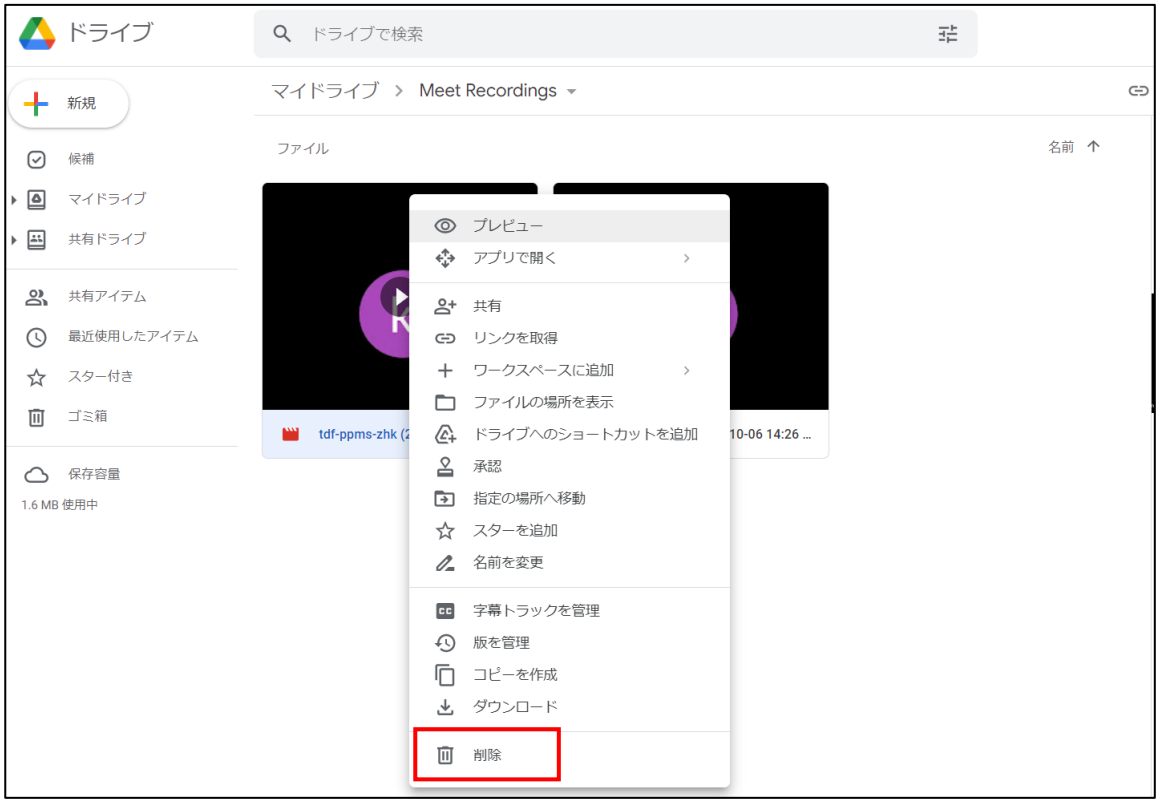
不要になった録画ファイルを適宜削除することを推奨します。Google Meet で録画した動画ファイルは主催者の Google ドライブ上のマイドライブ配下にある「Meet Recording」に保管されます。削除することにより、**悪意のあるユーザーによる持ち出しやサイバー攻撃を受けた際の機密情報漏洩のリスク低減になります**。

【手順①】

Google Meet の録画ファイルは、Google Drive に保管されます。Google Drive の「Meet Recordings」をクリックします。



下記のように対象のファイル上で右クリックし、「削除」を選択すると削除することができます。



4-7　チェックリスト 9-1 への対応

4-7-1　　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。

【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

4-8　チェックチェックリスト 9-2 への対応

4-8-1 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「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。

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】

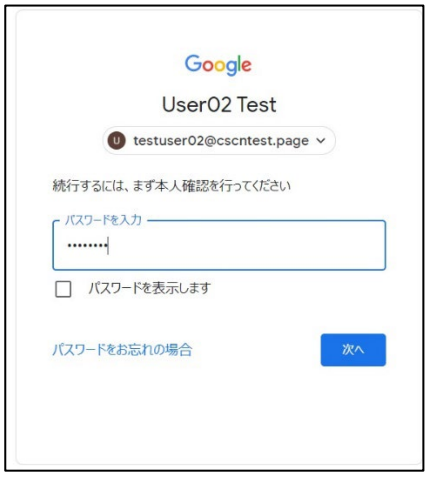
右上 Google アカウントアイコンの「Google アカウントを管理」をクリックします。

【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。

4-9　チェックリスト 9-3 への対応

4-9-1 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。

4-10 チェックリスト 9-4 への対応

4-10-1　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】

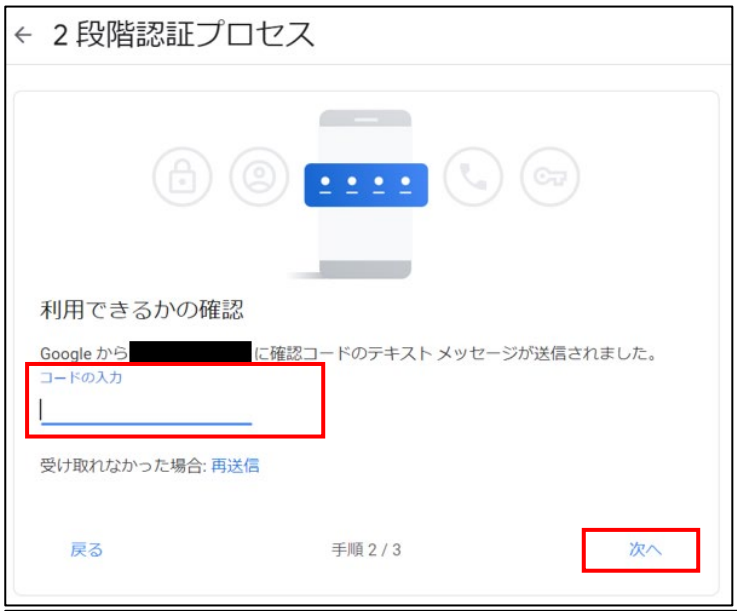
2 段階認証のプロセス画面において、「使ってみる」をクリックします。

【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。

【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。



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。

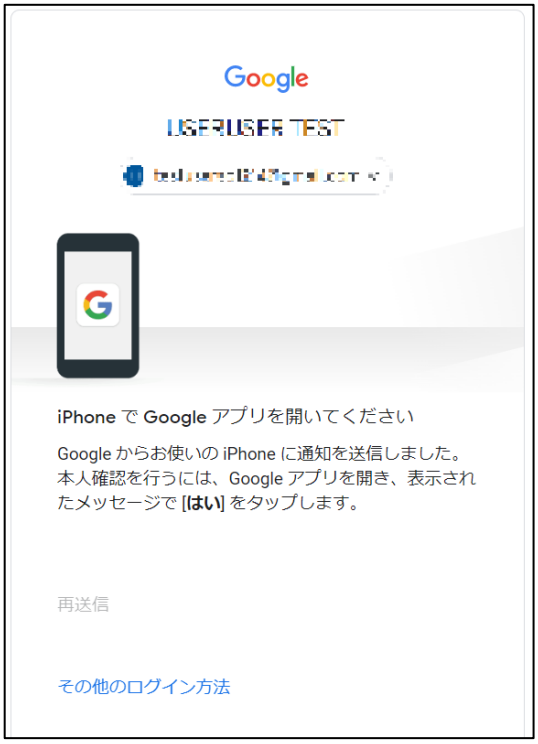
【手順⑧】

下記画面に切り替わったら設定完了です。

【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。