

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 （Gmail）

Ver1.0 (2023.XX.XX)

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	3
2	チェックリスト項目に対応する設定作業一覧	4
3	管理者向け設定作業	6
3-1	チェックリスト 2-2 への対応	6
3-1-1	迷惑メール対応と保護設定	6
3-2	チェックリスト 3-1 への対応	9
3-2-1	アプリレベルでのアクセス制御	9
3-3	チェックリスト 7-3 への対応	15
3-3-1	監査ログの確認方法	15
3-4	チェックリスト 9-1 への対応	16
3-4-1	パスワードポリシーの設定	16
3-5	チェックリスト 9-2 への対応	18
3-5-1	パスワード変更要求設定	18
3-6	チェックリスト 9-4 への対応	20
3-6-1	2 段階認証のポリシー設定	20
3-7	チェックリスト 10-1 への対応	22
3-7-1	管理者権限の付与	22
3-8	チェックリスト 10-2 への対応	23
3-8-1	管理者アカウントのパスワード強度	23
3-9	チェックリスト 10-3 への対応	23
3-9-1	管理者権限の管理	23
4	利用者向け作業	24
4-1	チェックリスト 6-1 への対応	24
4-1-1	HTTPS 通信の確認	24
4-1-2	サービス接続先の確認	24
4-2	チェックリスト 7-3 への対応	24
4-2-1	Google アカウントへのログインデバイスの確認方法	24
4-3	チェックリスト 9-1 への対応	26
4-3-1	パスワード強度	26
4-4	チェックリスト 9-2 への対応	27
4-4-1	初期パスワード変更	27
4-5	チェックリスト 9-3 への対応	29
4-5-1	パスワード入力制限	29
4-6	チェックリスト 9-4 への対応	29
4-6-1	2 段階認証プロセスの設定	29

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、Gmail 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

本製品を含む 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。（2022 年 11 月 1 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、2022 年 11 月 1 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
2-2 マルウェア対策 不審なメールを開封し、メールに記載されている URL をクリックしたり、添付ファイルを開いたりしないよう周知する。	<ul style="list-style-type: none"> ・ 迷惑メール対応と保護設定 	P.6
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。	<ul style="list-style-type: none"> ・ アプリレベルでのアクセス制御 	P.9
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。	<ul style="list-style-type: none"> ・ 監査ログの確認方法 	P.15
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。	<ul style="list-style-type: none"> ・ 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。	<ul style="list-style-type: none"> ・ 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。	<ul style="list-style-type: none"> ・ 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。	<ul style="list-style-type: none"> ・ 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。	<ul style="list-style-type: none"> ・ 管理者アカウントのパスワード 	P.23
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。	<ul style="list-style-type: none"> ・ 管理者権限の管理 	P.23

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
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。	<ul style="list-style-type: none"> ・ HTTPS 通信の確認 ・ サービス接続先の確認 	P.24 P.24
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。	<ul style="list-style-type: none"> ・ Google アカウントへのログインデバイスの確認方法 	P.24
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。	<ul style="list-style-type: none"> ・ パスワード 	P.26
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。	<ul style="list-style-type: none"> ・ 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。	<ul style="list-style-type: none"> ・ 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。	<ul style="list-style-type: none"> ・ 2 段階認証プロセスの設定 	P.29

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 2-2 への対応

3-1-1 迷惑メール対応と保護設定

メールの保護機能の設定や迷惑メールフィルタを設定することで、**ユーザーが受信する迷惑メールを抑制することができ、メールからのマルウェア感染リスクを低減させることができます**。また、不審メールを開封しない、不審メール内記載の URL をクリックしない、不審メールの添付ファイルを開かない、などをユーザーへ継続的に注意喚起することで、**ユーザーの不審メールに対する意識を高めマルウェア感染の被害のリスクを低減する**ことが見込めます。

メール安全性の設定

【手順①】

管理コンソールの「アプリ」-「Google Workspace」-「Gmail」-「安全性」をクリックします。



【手順②】

添付ファイル：メールに含まれる不正なソフトウェアによる被害を防ぐ追加ポリシーです。

IMAP での閲覧時の保護：IMAP ユーザーを保護するための追加設定です。

リンクと外部画像：リンクや外部画像を使ったメールフィッシングを防ぐための追加設定です。

なりすましと認証：なりすましや未認証メールによるフィッシング攻撃を抑えるための追加設定です。

安全性	
添付ファイル 「cscntest.page」で適用しました	<p>メールに含まれる不正なソフトウェアによる被害を防ぐ追加のポリシーです。 詳細</p> <p>影響を受けるメールを表示します（グラフへのアクセスには Google Workspace Enterprise Plus エディションが必要です）。</p> <p>信頼できない送信者から送られる暗号化された添付ファイルに対する保護機能: オン</p> <p>信頼できない送信者から送られるスクリプトを含む添付ファイルに対する保護機能: オン</p> <p>異常な種類のメール添付ファイルに対する保護: オフ</p> <p>今後のおすすめの設定を自動的に適用: オン</p>
IMAP での閲覧時の保護 「cscntest.page」で適用しました	<p>メールの利用時に IMAP ユーザーを保護するための追加設定です。 詳細</p> <p>IMAP のリンク保護を有効にする: オフ</p>
リンクと外部画像 「cscntest.page」で適用しました	<p>リンクや外部画像を使ったメールフィッシングを防ぐための追加設定です。 詳細</p> <p>短縮 URL により隠されたリンクを特定: オン</p> <p>リンク先の画像をスキャン: オン</p> <p>信頼できないドメインへのリンクをクリックした場合に警告メッセージを表示: オン</p> <p>今後のおすすめの設定を自動的に適用: オン</p>
なりすましと認証 「cscntest.page」で適用しました	<p>なりすましや未認証メールによるフィッシング攻撃を抑えるための追加設定です。 詳細</p> <p>なりすましに関する設定の影響を受けるメールを表示</p> <p>未認証メールを表示</p> <p>グラフへのアクセスには Google Workspace Enterprise Plus エディションが必要です。</p> <p>類似したドメイン名に基づくドメインのなりすましに対する保護機能: オン</p> <p>従業員名のなりすましに対する保護機能: オン</p> <p>受信メールによるドメインのなりすましに対する保護機能: オン</p> <p>未認証メールに対する保護機能: オフ</p> <p>受信メールによるドメインのなりすましから Google グループを保護: オフ</p> <p>今後のおすすめの設定を自動的に適用: オン</p>

迷惑メール等のフィルタリング設定

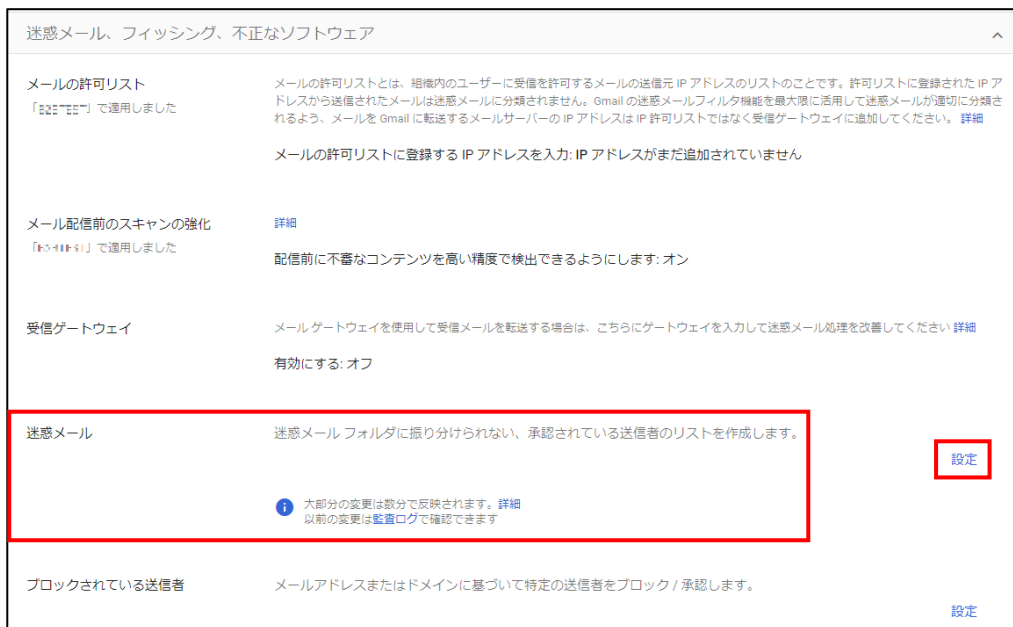
【手順①】

管理コンソールの「アプリ」-「Google Workspace」-「Gmail」-「迷惑メール、フィッシング、不正なソフトウェア」をクリックします。



【手順②】

「迷惑メール、フィッシング、不正なソフトウェア」の「迷惑メール」の「設定」をクリックします。



【手順③】

デフォルトの動作を設定/変更することにより迷惑メールフィルタを適用することができます。

設定を追加

迷惑メール [詳細](#)

必須: 設定の概要に表示される短い説明を入力します。

すべての受信メールに Google の迷惑メールフィルタが適用されます。迷惑メールとして検出されたメールは自動的に迷惑メールフォルダに振り分けられます。
次の方法でこのデフォルトの動作を変更します

- ☒ 積極的に迷惑メールに分類する。
- ☒ 内部の送信者から受信したメールには迷惑メールフィルタを適用しない。
- ☒ これらの承認済み送信者リストにあるアドレスまたはドメインから受信したメールには迷惑メールフィルタを適用しない。
リストはまだ使用されていません。
[既存のリストを使用する](#) [リストを作成または編集](#)
- ☒ 迷惑メールを管理検索に移動する

Default ▾

キャンセル **保存**

3-2 チェックリスト 3-1 への対応

3-2-1 アプリレベルでのアクセス制御

Gmail 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。

API の制御

この設定により、自社およびサードパーティ製のアプリケーションとサービス アカウントに対して、Google Workspace API へのアクセスを許可または制限することができます。信頼するアプリケーションにのみアクセスを許可することにより、サードパーティ製アプリケーションが Google Workspace API にアクセスすることに伴うリスクを軽減できます。

アプリのアクセス制御

アプリからの Google サービスへのアクセスを管理します。組織が信頼できると判断したアプリに限り、ユーザーがアクセスを許可できるようにします。[詳細](#)

概要

0 個の制限付きの Google サービス
15 個の無制限の Google サービス
[GOOGLE サービスを管理](#)

0 種類のサードパーティ製アプリを設定しました
[サードパーティ製アプリのアクセスを管理](#)

設定

制限付きの Google サービスにアクセスできないアプリをユーザーが使おうとした場合に、このメッセージが表示されます

メッセージ（上限 300 文字）
☒ ドメインで所有する内部アプリを信頼する
Google Workspace Marketplace、Android、iOS のホワイトリストに登録したアプリは、アプリのアクセス制御リストで自動的に信頼されます。

[キャンセル](#)
[保存](#)

GOOGLE サービス

アプリ

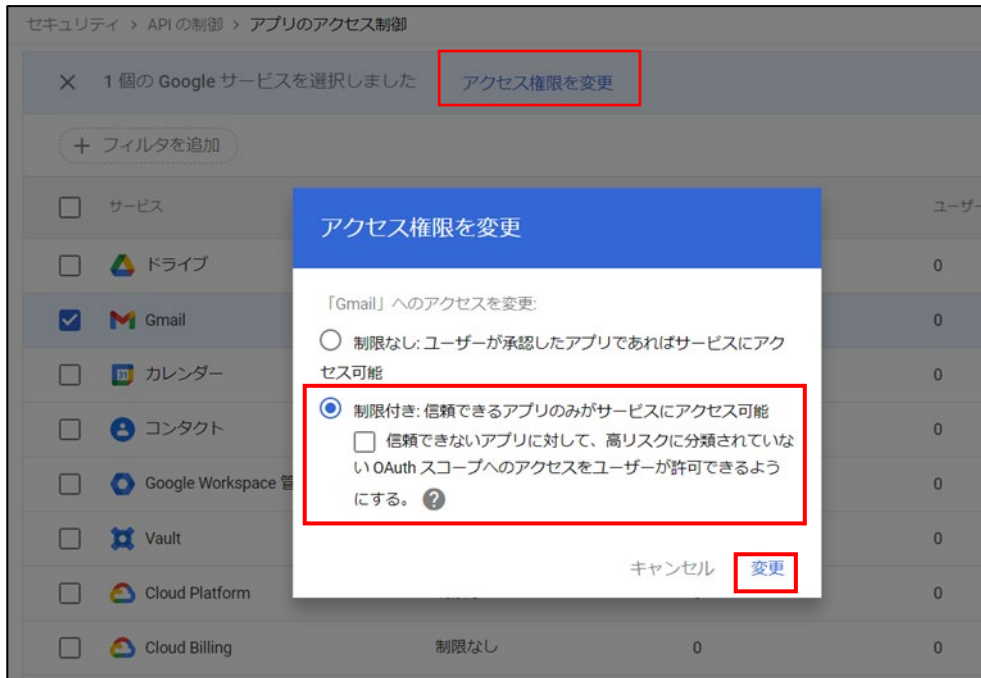
15 個の Google サービス

+ フィルタを追加

<input type="checkbox"/> サービス	アクセス	許可されているアプリ	ユーザー
<input type="checkbox"/> ドライブ	制限なし	0	0
<input type="checkbox"/> Gmail	制限なし	0	0
<input type="checkbox"/> カレンダー	制限なし	0	0
<input type="checkbox"/> コンタクト	制限なし	0	0
<input type="checkbox"/> Google Workspace 管理コンソール	制限なし	0	0
<input type="checkbox"/> Vault	制限なし	0	0
<input type="checkbox"/> Cloud Platform	制限なし	0	0
<input type="checkbox"/> Cloud Billing	制限なし	0	0
<input type="checkbox"/> クラウド機械学習	制限なし	0	0
<input type="checkbox"/> Apps Script Runtime	制限なし	0	0

【手順③】

表示リストから管理するサービスを選択後、「アクセス権限を変更」をクリックし、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】

「アプリを追加」をクリックし「OAuth アプリ名またはクライアント ID」を選択します。



【手順⑥】

「OAuth アプリ名またはクライアント ID を検索」に対象のアプリ名を入力し、「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。

× OAuth アプリを設定する

1 アプリを検索する — 2 OAuth クライアント ID の選択 — 3 アプリの設定

OAuth アプリの名前またはクライアント ID を入力して、[検索] をクリックします。アプリの選択後、アプリのアクセスを信頼するかブロックするかを設定できます。

OAuth アプリ名またはクライアント ID を検索

teams

検索

アプリ名

- Webex Teams
- Zapier-Microsoft Teams
- Sisense for Cloud Data Teams
- Easy Teams
- Microsoft Teams Meeting
- Teams Mail

選択

【手順⑦】

「OAuth クライアント ID」のチェックボックスにチェックし、「選択」をクリックします。

× OAuth アプリを設定する

1 アプリを検索する — 2 OAuth クライアント ID の選択 — 3 アプリの設定

Microsoft Teams Meeting

クライアント ID

アプリのアクセスを設定するには、設定するクライアント ID のチェックボックスをオンにして [選択] をクリックします。

種類	クライアント ID
OAuth クライアント ID	
ウェブアプリケーション	
ウェブアプリケーション	

戻る

選択

【手順⑧】

「信頼されている:すべての Google サービスにアクセス可能」にチェックし、「設定」をクリックします。

× OAuth アプリを設定する

アプリを検索する — OAuth クライアント ID の選択 — 3 アプリの設定

Microsoft Teams Meeting

アプリのアクセス
このアプリ用に選択したクライアント ID に適用するアクセスタイプを選んでください。以前これらのクライアント ID に適用したアクセスタイプは、今回選んだアクセスタイプに変更されます。

☒ 信頼されている: すべての Google サービスにアクセス可能

☐ 限定: アクセス制限のない Google サービスにのみアクセスできます

☐ ブロック中: Google サービスにアクセスできません

戻る

設定

【手順⑨】

追加が完了すると一覧に対象のアプリが追加されます。

ユーザー、グループ、設定を検索

セキュリティ > API の制御 > アプリのアクセス制御

Google サービス

Google サービス API のアクセス設定を選択して、これらのサービスへのアクセスをリクエストできるサードパーティ アプリの種類を管理します。詳細

リストを表示

15 個の設定済みアプリ

アクセスを構成したサードパーティ製アプリとクライアント ID を管理します。詳細

リストを表示

アクセスしたアプリ

デフォルトの設定を使用して Google データにアクセスしたサードパーティ製アプリとクライアント ID を表示します。設定が完了しているアプリを含みます。詳細

リストを表示

設定済みアプリ アプリを追加 リストをダウンロード リストを一括更新

+ フィルタを追加

<input type="checkbox"/>	アプリ名	種類	ID	確認済みのステータス	アクセス
<input type="checkbox"/>					信頼できる
<input type="checkbox"/>	Microsoft Teams	ウェブ アプリケ...		Google により確認済み	信頼できる
<input type="checkbox"/>	Microsoft Teams	ウェブ アプリケ...		Google により確認済み	信頼できる

3-3 チェックリスト 7-3 への対応

3-3-1 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 Gmail の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」-「ユーザーのログインイベント」をクリックします。

The screenshot shows the Google Admin console interface. On the left sidebar, under 'Reports', the 'Audit & Investigation' option is highlighted. The main content area displays the 'User login events' page. At the top, there's a search bar and a filter dropdown set to 'User login events'. Below this, a table lists login events for a specific user. The table has columns for 'Date', 'Description', 'Login type', and 'IP address'.

日付	説明	ログインの種類	IP アドレス
2022-11-25T11:39:32+09:00	山田 太郎さんがログインしました	再認証	192.168.1.100
2022-11-25T11:39:12+09:00	山田 太郎さんがアカウントのパスワードを変更しました		192.168.1.100
2022-11-25T11:38:57+09:00	山田 太郎さんがログインしました	Google のパスワード	192.168.1.100
2022-11-25T11:38:57+09:00	山田 太郎さんにログイン認証が表示されました	Google のパスワード	192.168.1.100
2022-10-26T16:04:24+09:00	山田 太郎さんがログインしました	Google のパスワード	192.168.1.100
2022-10-26T16:04:24+09:00	山田 太郎さんにログイン認証が表示されました	Google のパスワード	192.168.1.100
2022-10-26T15:36:18+09:00	山田 太郎さんがログアウトしました	Google のパスワード	192.168.1.100
2022-10-26T15:34:31+09:00	山田 太郎さんが 2 段階認証プロセスに登録しました		192.168.1.100
2022-10-26T15:33:48+09:00	山田 太郎さんがログインしました	再認証	192.168.1.100
2022-10-26T15:31:15+09:00	山田 太郎さんがログインしました	Google のパスワード	192.168.1.100
2022-10-26T15:30:07+09:00	山田 太郎さんがログアウトしました	Google のパスワード	192.168.1.100
2022-10-26T15:27:22+09:00	山田 太郎さんがログインしました	Google のパスワード	192.168.1.100
2022-10-25T18:26:46+09:00	山田 太郎さんが 2 段階認証プロセスを無効にしました		192.168.1.100
2022-10-25T18:26:39+09:00	山田 太郎さんがログインしました	再認証	192.168.1.100
2022-10-25T17:43:54+09:00	山田 太郎さんがアカウントのパスワードを変更しました		192.168.1.100

3-4 チェックリスト 9-1 への対応

3-4-1 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>

セキュリティの設定

cscntest.page のユーザーの設定を表示しています

パスワードの管理

パスワードの管理
ローカルに適用

組織向けにパスワードのポリシーを設定します

これらのポリシーは適用されない場合もあります (例: ユーザーがサードパーティの ID プロバイダで認証された場合)。詳細

安全度
ユーザーは強力なパスワードを使用する必要があります。詳細
☒ 安全なパスワードを適用する

長さ
8~100 文字で指定してください
最小の長さ: 8 最大の長さ: 100

長さや安全度の適用
長さや安全度の要件の変更は、該当するユーザーが次回パスワードを変更するときに適用されます。変更を直ちに適用するには、ユーザーの次回ログイン時に適用が開始されるように設定してください。
☐ 次回ログイン時にパスワードポリシーを適用する

再利用
☐ パスワードの再利用を許可

有効期限
パスワードの再設定の頻度
有効期限なし

キャンセル 保存

3-5 チェックリスト 9-2 への対応

3-5-1 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こと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。

The image displays two versions of the 'Add New User' form. The left form shows the 'Generate password automatically' toggle set to 'On' (blue), which is highlighted with a red box. The right form shows the 'Require password change on next login' toggle set to 'On' (blue), also highlighted with a red box. In both forms, the 'Add new user' button at the bottom right is highlighted with a red box. The forms include fields for name, email address, and phone number, as well as a password field in the right version.

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。

次のパスワードを再設定:

☐ パスワードを自動的に生成する
 次のステップでパスワードを確認してコピーできます

☒ パスワードを作成する
 パスワード

☒ ユーザーのログイン時にパスワードを変更してもらう

キャンセル
 リセット

3-6 チェックリスト 9-4 への対応

3-6-1 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】

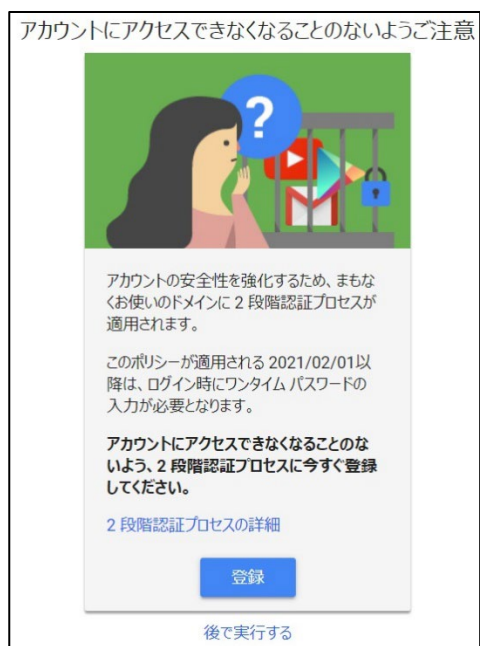
2段階認証プロセスのポリシーを設定することができます。デフォルトでは「ユーザーが2段階認証プロセスを有効にできるようにする」はオンであり、ユーザーへの適用は「強制しない」が選択されています。ユーザーへの適用の方法は、「強制しない」以外に、「今すぐ強制」と「指定日以降に強制」を選択できます。



「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。



3-7 チェックリスト 10-1 への対応

3-7-1 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。

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。

ロール		
test さんの管理者ロールを管理します。既定のロールを割り当てるか、特定の権限を持つカスタムロールを作成します。		
0 個のロールが割り当てられています		
ロール名	ロールの範囲	割り当て状況 ↑
ヘルプデスク管理者 Help Desk Administrator	すべての組織部門	<input checked="" type="checkbox"/> 割り当て済み
ユーザー管理者 User Management Administrator	-	<input type="checkbox"/> 未割り当て
サービス管理者 Services Administrator	-	<input type="checkbox"/> 未割り当て
グループ管理者 Groups Administrator	-	<input type="checkbox"/> 未割り当て
特権管理者 G Suite Administrator Seed Role	-	<input type="checkbox"/> 未割り当て
モバイル管理者 Mobile Administrator	-	<input type="checkbox"/> 未割り当て
グループの閲覧者 Groups Reader	-	<input type="checkbox"/> 未割り当て
グループエディタ Groups Editor	-	<input type="checkbox"/> 未割り当て
Storage 管理者 Storage Admin Role	-	<input type="checkbox"/> 未割り当て

3-8 チェックリスト 10-2 への対応

3-8-1 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>

3-9 チェックリスト 10-3 への対応

3-9-1 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 6-1 への対応

4-1-1 HTTPS 通信の確認

ユーザーがアクセスする Gmail への通信は基本的に HTTPS で暗号化されています。

4-1-2 サービス接続先の確認

Gmail 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（Gmail 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。

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、Gmail にアクセスします。

4-2 チェックリスト 7-3 への対応

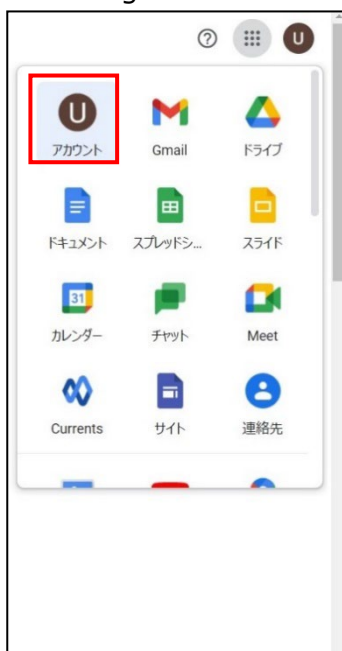
4-2-1 Google アカウントへのログインデバイスの確認方法

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。

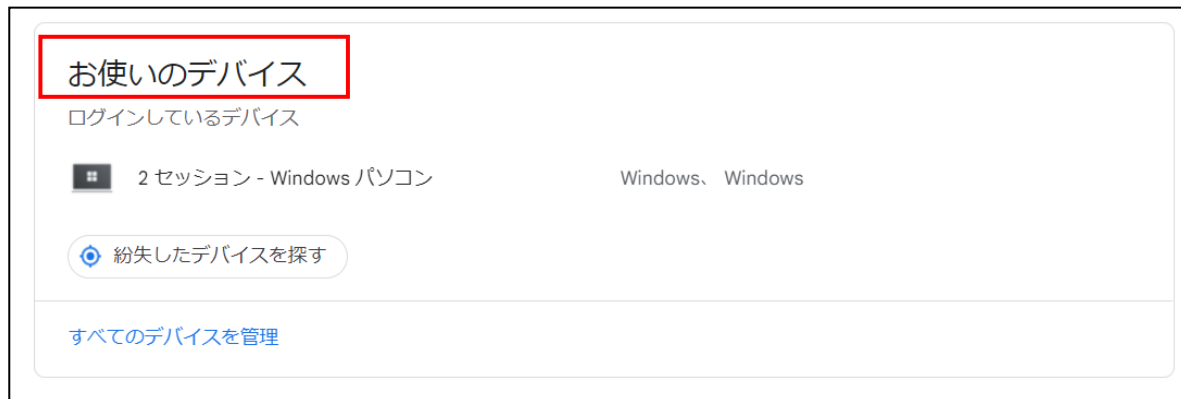
【手順】①

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。



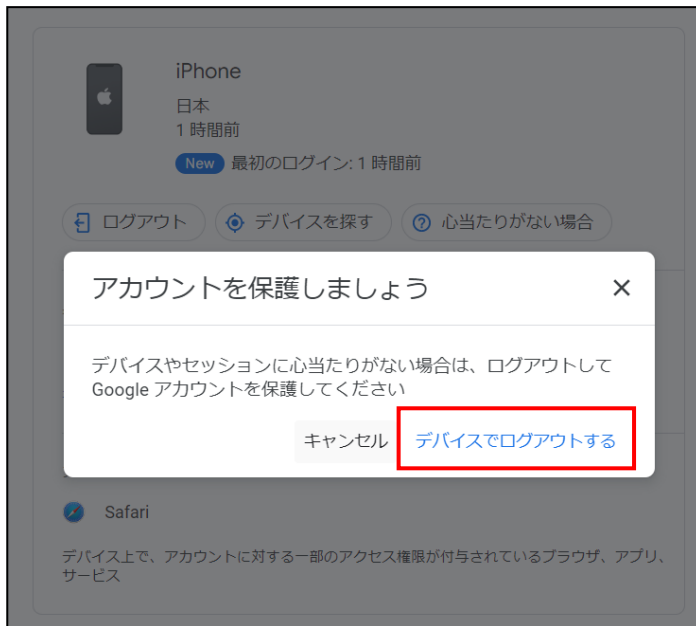
【手順③】

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。





4-3 チェックリスト 9-1 への対応

4-3-1 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>

4-4 チェックリスト 9-2 への対応

4-4-1 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「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。

Google アカウント

Google アカウントの検索

ホーム

個人情報

データとカスタマイズ

セキュリティ

情報共有と連絡先

お支払いと定期購入

Google アカウントについて

個人情報

Google サービスで使用する、名前、写真などの基本情報

基本情報

一部の情報は、Google サービスを利用する他のユーザーに表示される場合があります。詳細

写真 このアカウントの写真は変更できません

名前 Test User02

生年月日 生年月日を追加

パスワード *****
前回の変更: 11:58

【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。

Google

User02 Test

testuser02@cscntest.page

続行するには、まず本人確認を行ってください

パスワードを入力

パスワードを表示します

パスワードをお忘れの場合

次へ

【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

← パスワード

安全なパスワードを選択し、他のアカウントでは再利用しないでください。詳細

パスワードを変更すると、スマートフォンを含むお使いのデバイスすべてからログアウトされるため、すべてのデバイスで新しいパスワードを入力する必要があります。

新しいパスワード

パスワードの安全度:
8文字以上にしてください。別のサイトで使用しているパスワードや、すぐに推測できる単語（たとえばペットの名前）は使用しないでください。理由

新しいパスワードを確認

パスワードを変更

4-5 チェックリスト 9-3 への対応

4-5-1 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。

4-6 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、「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。



The image shows the Google login interface for a user named 'Tesr User01'. The email address 'testuser01@cscntest.page' is displayed. A message states: '続行するには、まず本人確認を行ってください' (To continue, please first verify your identity). Below this, there is a password input field labeled 'パスワードを入力' (Enter password) with a red rectangular highlight. Underneath the password field is a checkbox labeled 'パスワードを表示します' (Show password). To the right of the password field is a blue button labeled '次へ' (Next) with a red rectangular highlight. At the bottom left, there is a link 'パスワードをお忘れの場合' (If you forgot your password). At the bottom of the page, there are links for '日本語' (Japanese), 'ヘルプ' (Help), 'プライバシー' (Privacy), and '規約' (Terms).

【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。



The image shows the '2-step verification' process screen. At the top, there are three icons: a smartphone with a key icon, a blue shield with a 'G' logo, and a globe with a lock icon. The main heading is '2段階認証プロセスでアカウントを保護しましょう' (Protect your account with 2-step verification). Below this, there is a paragraph explaining that security is enhanced and account access is prevented. Two steps are listed: 1. '簡単にセキュリティを強化' (Easily enhance security) with a checkmark icon, explaining that a 2-step verification process is added to the login process. 2. 'すべてのオンライン アカウントに2段階認証プロセスを使用' (Use 2-step verification for all online accounts) with a lock icon, explaining that this process helps prevent cyberattacks and is a recommended method. At the bottom, there is a 'Safer with Google' logo and a blue button labeled '使ってみる' (Try it) with a red rectangular highlight.

【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。

← 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。
データ通信料金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 [makiyama@yagmail.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。



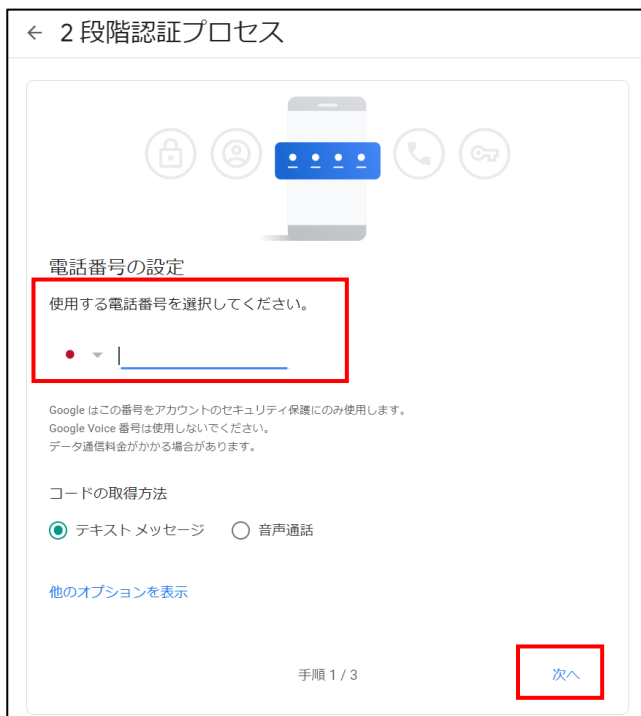
【手順③】

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。



【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](#)



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
[redacted] 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](#)

パスワードを必要としないログイン設定

Google Chrome（バージョン M108 より利用可）にてパスワードレス認証が利用可能です。利用する場合は iPhone5s 以降または Android スマートフォンが必要となります（本手順は iPhone13 で作成しています）

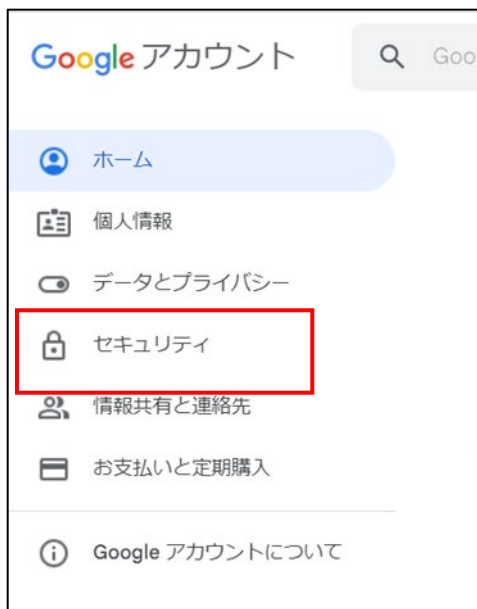
【手順①】

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】

「スマートフォンを使用してログイン」をクリックします。

Google へのログイン



パスワード 前回の変更: 2019/05/04 >

スマートフォンを使用してログイン	● オフ	>
2段階認証プロセス	● オフ	>

【手順④】

下記画面が表示されたら「次へ」をクリックします。

← スマートフォンを使用してログイン

仕組み

パスワードを入力する代わりに、スマートフォンに届いた Google からのメッセージをタップしてログインできます。
必要なのは、画面ロックで保護されたスマートフォンだけです。スマートフォンを使用できないときは、引き続きパスワードでログインできます。 [詳細](#)

次へ

1

メールアドレスを入力します



【手順⑤】

Android または iPhone の Google アプリに、対象のアカウントでログインし「次へ」をクリックします。

以下は iPhone の Google アプリでログインした場合です。

← スマートフォンを使用してログイン

スマートフォンの設定

Google からのメッセージを使ってログインするには、画面ロックを有効にしたスマートフォンが必要です。

 **スマートフォン**

パスワードが最近変更されたため、お使いのスマートフォンにもう一度ログインしていただく必要があります。

Android スマートフォンのセットアップ 

iPhone (5S 以降) のセットアップ 

戻る 手順 1 / 2 

【手順⑥】

以下画面への切り替わり後、「次へ」をクリックします。

← スマートフォンを使用してログイン

スマートフォンの設定

Google からのメッセージを使ってログインするには、画面ロックを有効にしたスマートフォンが必要です。

 **スマートフォン**

 iPhone 

 **Touch ID**

お使いの iPhone では Touch ID が有効になっているので、アカウントへのログインにスマートフォンを使用できます。

戻る 手順 1 / 2 

【手順⑦】

「有効にする」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。

