

令和7年国勢調査 オンライン回答支援ブースの開設等に係る取扱いについて

令和7年2月
国勢統計課オンライン調査係

都道府県・市町村におけるオンライン回答啓発に係る取組として、「オンライン回答支援ブース」の開設や調査員等にタブレット端末を携帯させ、世帯訪問時にその場でオンライン回答を支援する仕組み（以下「タブレット調査員」という。）を実施する場合は、本資料の取扱いに沿って対応いただきますようお願いいたします。

1 「オンライン回答支援ブース」の開設・運用に係る取扱いについて

(1) 設置する端末の要件

オンライン回答支援ブースに設置する端末は、地方公共団体で既に所有している端末（公共施設等に設置されたパソコンも含む）又は委託費でレンタルした端末とします。（委託費による端末の購入は不可。）

なお、委託費でレンタルする場合の端末（タブレット端末又はパソコン）の要件は下表のとおりです。

※ QRコードから「国勢調査オンライン（電子調査票）」へのアクセス・ログインが簡単に行えるため、タブレット端末の使用を推奨。

また、当該端末の使用後、事業者が端末等の返却時又は廃棄時においては、蓄積された電磁的記録を復元できないように抹消してください。（事業者が抹消した旨の証明書を取得すること。）

① 「タブレット端末」の要件

項目	スペック等
画面	9.7型以上であること。
OS	iPadOS16以降 又は Android12以降であること。
無線LAN	IEEE802.11a/b/g/n/acに準拠していること。
ブラウザ	iPadの場合はSafari17以上、Androidの場合はGoogle Chrome123以上を搭載していること。
ソフトウェア	Androidの場合はウイルス対策ソフトを導入すること。 また、QRコードの読取りを可能とするための標準カメラ機能を搭載していること。
カメラ	QRコードの読取りを行うための内臓カメラを搭載していること。
その他	AC充電器等を用意すること。

② 「パソコン」の要件

項目	スペック等
形状・画面	指定なし。※ 例 ノート型の 15.6 インチ
OS	Windows11 であること。
CPU	Core i3 以上であること。
メモリ	4GB 以上であること。
HDD・SSD	200GB 以上であること。
無線 LAN	IEEE802.11a/b/g/n/ac に準拠していること。
有線 LAN	10/100/1000BASE-T の LAN ポートを有すること。
ブラウザ	Google Chrome123 以上、Microsoft Edge123 以上又は Firefox124 以上を搭載していること。
マウス	有すること。
ソフトウェア	ウイルス対策ソフトを導入すること。
その他	電源ケーブル等を用意すること。

(2) 端末への初期設定

公共施設等に設置されているパソコンを使用する場合も含め、端末に入力内容が残らないようにするため、「別紙1 端末のセキュリティ設定」を参照し、セキュリティ設定を必ず行ってください。

※契約者のみに交付する
(本文書には添付しない)

(3) 通信回線の要件

通信回線については、CATV、光ファイバー等のブロードバンド環境、4G LTE、5G 等のデータ通信サービスのインターネット接続が必要になります。

詳細については、「別紙2-1 オンライン回答支援ブースに設置する端末の通信回線について」を参照してください。

(4) 運用要件

ア セキュリティ上の監視要員として、また、オンライン回答支援ブースの利用者が端末の操作等で支援を必要とする場合がありますので、地方公共団体の職員や運用を委託する事業者等を原則常駐するようにしてください。

なお、オンライン回答支援ブースを開設した公共施設等の職員が兼務する場合など、常駐が困難な場合には、セキュリティ上の問題等が発生した（そのおそれを含む。）場合や利用者からの支援等の求めがあった場合に、速やかに対応できる体制等を整備した上で運用することが必須となります。

また、常駐する職員や運用を委託する事業者等には、事前に地方公共団体のセキュリティポリシー及び個人情報保護に関する規定についての教育を施すことが必須となります。

イ オンライン回答を行う場合は、『インターネット回答依頼書』に記載されているログインID・アクセスキー(再回答の場合は世帯が設定したパスワード)が必要となりますので、世帯が持参しているか確認してください。(持参していない場合は回答不可。)

ウ オンライン回答支援ブースにおけるオンライン回答に当たって、関係者が行えることは下表のとおりとなりますので、御留意ください。

関係者	行えること
地方公共団体職員	・入力・回答送信の支援 ・端末操作の支援
オンライン回答支援ブース 設置・運用の委託業者	・入力・回答送信の支援 ・端末操作の支援
調査員、指導員	・入力・回答送信の支援 ・代理入力、回答送信 ・端末操作の支援
世帯	・入力・回答送信

エ 端末を操作する世帯以外に、ログインID・アクセスキー・パスワードや入力内容を見られないよう、端末へのプライバシーフィルターの装着や^{しゅへいばん}遮蔽板等の設置などの措置を講じてください。

オ 世帯の端末使用が終了した際は、その都度、画面が回答途中の状態になっていないかなど確認してください。回答途中などの場合は、回答を終了させてください。

カ 次の世帯が端末の使用を開始する前に、以下の作業を行ってください。

タブレット端末：ブラウザを閉じ、画面をホーム画面に戻す。

パソコン：画面を「国勢調査オンライン（電子調査票）」のトップページに戻す。

キ 設置する端末には、セキュリティワイヤーで固定するなど、持ち出されないような措置を講じてください。

また、ルーター等のネットワーク機器については、職員等以外の者が触れないところに設置してください。

(5) オンライン回答支援ブースの開設・運用を委託する場合

オンライン回答支援ブースの開設・運用を委託する場合には、事業者との委託契約の中で地方公共団体のセキュリティポリシー及び個人情報保護に関する規定の遵守、情報セキュリティ上の問題（そのおそれを含む。）発生時における地方公共団体の職員への速やかな報告についての要件を明記することが必須となります。

2 「タブレット調査員」の実施に係る取扱いについて

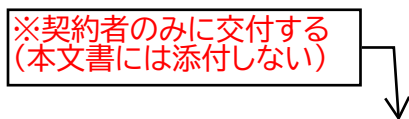
(1) 使用する端末の要件

タブレット調査員が使用するタブレット端末は、個人情報保護の観点から、地方公共団体で既に所有している端末又は委託費でレンタルした端末（委託費による端末の購入は不可。）とします。なお、個人が所有する端末は、個人情報の取扱いの観点から絶対に使用しないでください。

※ 委託費でレンタルする場合のタブレット端末の要件については、「1 「オンライン回答支援ブース」の開設に係る取扱いについて」－「(1) 設置する端末の要件」の「① 「タブレット端末」の要件」を参照。

また、当該端末の使用後、事業者への返却時又は廃棄時に、蓄積された電磁的記録を復元できないように抹消してください。(事業者が抹消した旨の証明書を取得すること。)

※契約者のみに交付する
(本文書には添付しない)



(2) 端末への初期設定

ア タブレット端末に入力内容が残らないようにするため、「別紙1 端末のセキュリティ設定」を参照し、セキュリティ設定を必ず行ってください。

イ タブレット端末を紛失した場合でも個人情報等が保護されるように、「別紙3 タブレットの遠隔ロック設定」を参照し、遠隔操作により端末にロックをかけることのできるサービス (iCloud 機能等) を必ず利用してください。

ウ タブレット端末自体の利用者認証機能を利用し、第三者が端末を使用できないようにしてください。

(3) 通信回線の要件

通信回線については、4G LTE、5G 等の高速データ通信サービスのインターネット接続が必要になります。インターネットに接続できない場合はアクセスできませんのでご注意ください。

詳細については、「別紙2-2 タブレット調査員が携帯するタブレット端末の通信回線について」を参照してください。

(4) 運用要件

ア オンライン回答を行う場合は、『インターネット回答依頼書』に記載されているログインID・アクセスキー(再回答の場合は世帯が設定したパスワード)が必要となりますので、世帯が所有しているか確認してください。(所有していない場合は回答不可。)

イ タブレット端末を使用してのオンライン回答に当たって、関係者が行えることは下表のとおりとなりますので、御留意ください。

関係者	行えること
調査員、指導員	<ul style="list-style-type: none"> ・入力・回答送信の支援 ・代理入力、回答送信 ・端末操作の支援
世帯	<ul style="list-style-type: none"> ・入力・回答送信

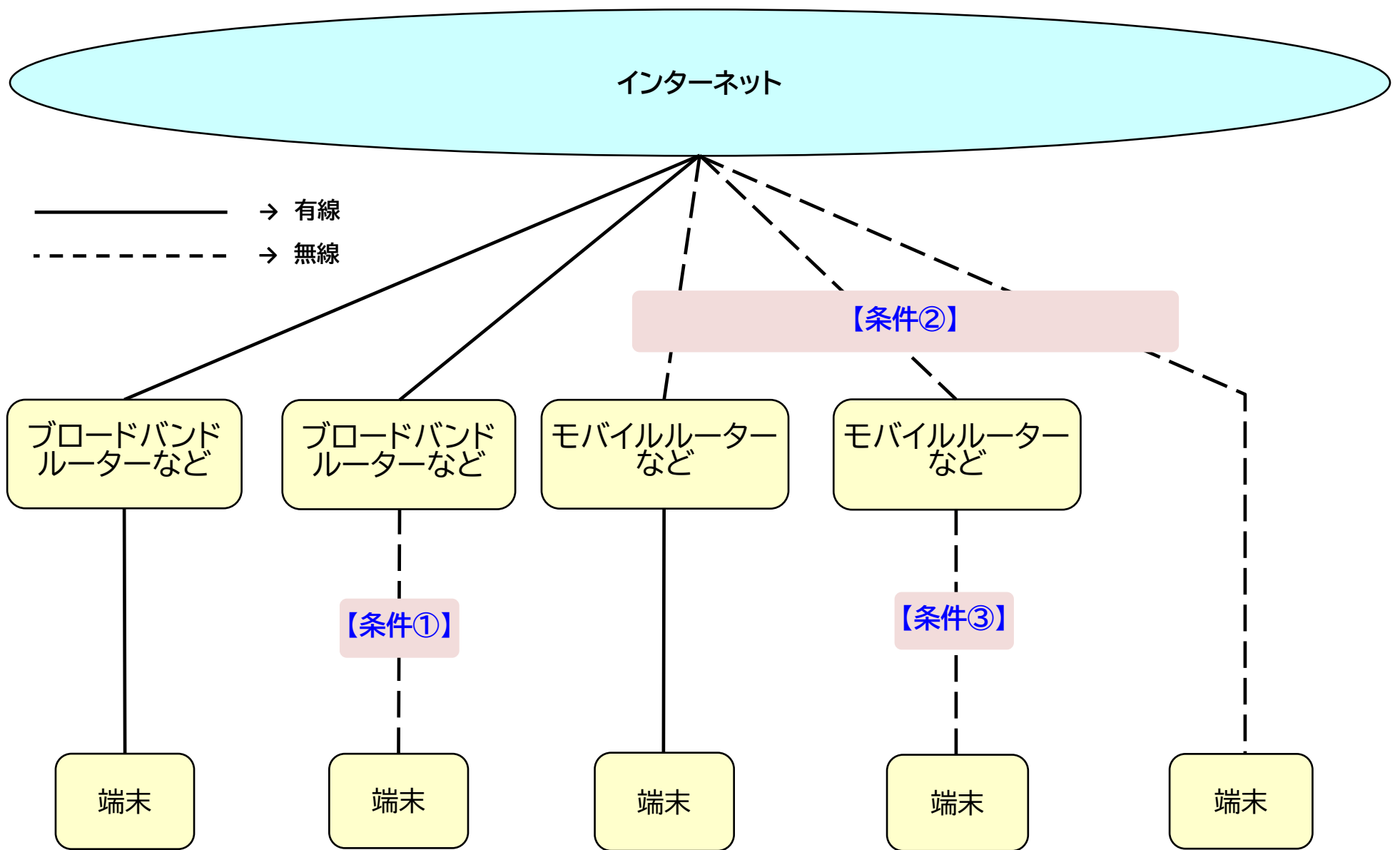
※ 世帯がタブレット端末を操作する際に、オンライン回答以外の操作が行われないよう注意してください。

ウ 世帯のタブレット端末使用が終了した際は、その都度、画面が回答途中の状態になっていないかなど確認してください。回答途中などの場合は、回答を終了させてください。

エ 次の世帯がタブレット端末の使用を開始する前に、ブラウザを閉じていただき、タブレット端末の画面をホーム画面に戻してください。

オ 調査活動中、タブレット端末の置き忘れ等がないか細心の注意を払ってください。

※ 世帯の記入済みの紙の調査票と同様に紛失することのないよう、厳重な管理に係る指導を徹底してください。



【パターン1】

有線のインターネット回線をルーターに接続し、そこから有線で端末を接続

【パターン2】

有線のインターネット回線をルーターに接続し、そこから無線で端末を接続
 (【条件①】を設定)

【パターン3】

モバイルルーターなどに、有線で端末を接続
 (【条件②】を設定)

【パターン4】

モバイルルーターなどに、無線で端末を接続
 (【条件②,③】を設定)

【パターン5】

端末から直接インターネットに接続
 (【条件②】を設定)

【注】接続に当たって暗号化方式等の設定条件

【条件①】

- (1) 暗号化方式をWPA2、WPA2-PSK又はWPA3のいずれかに固定可能なWi-Fiである場合のみ可能。
- (2) WPA2、WPA2-PSK又はWPA3が利用可能であっても、WEP、WPA又はWPA-PSKも選択できるものは使用不可。

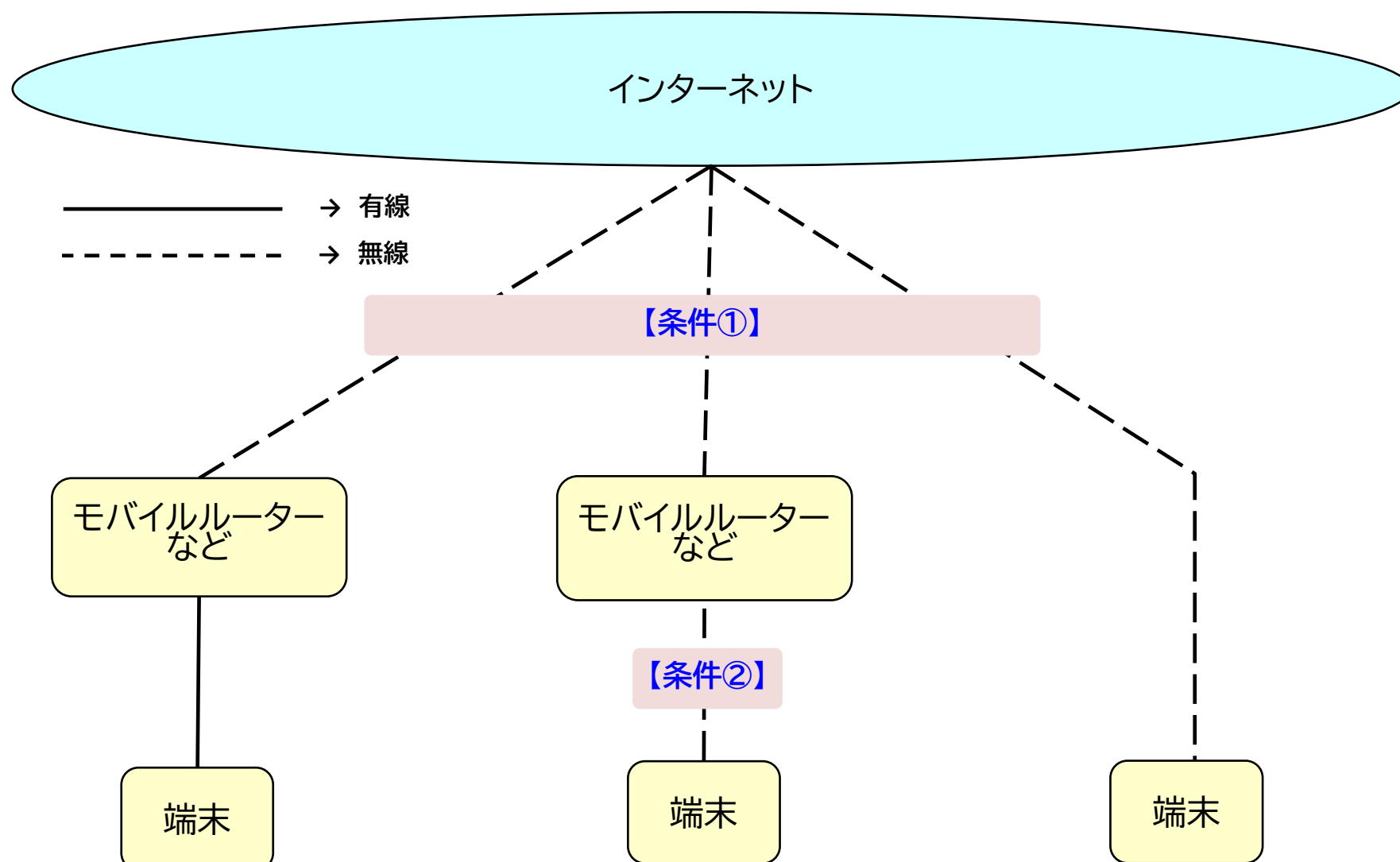
【条件②】

- (1) Wi-Fiの場合は、暗号化方式をWPA2、WPA2-PSK又はWPA3のいずれかに固定可能であること。
 ※ 暗号化方式がWEP、WPA又はWPA-PSKであるWi-Fiは使用不可。
- (2) Wi-Fiの場合は、パスワードが第三者に公開されていないこと。
 ※ 不特定多数の者が利用可能なフリーWi-Fiは禁止。

【条件③】

- (1) データ通信カードなど端末間の通信の暗号化方式がWPA2、WPA2-PSK又はWPA3のいずれかに固定可能なWi-Fiである場合のみ可能。
- (2) WPA2、WPA2-PSK又はWPA3が利用可能であっても、WEP、WPA又はWPA-PSKも選択できるものは使用不可。

タブレット調査員が携帯するタブレット端末の通信回線について



【パターン1】
モバイルルーターなどに、有線で
端末を接続
（【条件①】を設定）

【パターン2】
モバイルルーターなどに、無線で
端末を接続
（【条件①,②】を設定）

【パターン3】
端末から直接インターネット
に接続
（【条件①】を設定）

【注】接続に当たって暗号化方式等の設定条件**【条件①】**

- (1) Wi-Fiの場合は、暗号化方式がWPA2、WPA2-PSK又はWPA3のいずれかに固定可能であること。
※ 暗号化方式がWEP、WPA又はWPA-PSKであるWi-Fiは使用不可。
- (2) Wi-Fiの場合は、暗号化に際してはパスワードが第三者にオープンになっていないこと。
※ 不特定多数の者が利用可能なフリーWi-Fiは禁止。

【条件②】

- (1) データ通信カードなどと端末間の通信の暗号化方式がWPA2、WPA2-PSK又はWPA3に固定されているWi-Fiである場合のみ可能。
- (2) WPA2、WPA2-PSK又はWPA3が利用可能であっても、WEP、WPA又はWPA-PSKも選択できるものは使用不可。

タブレットの遠隔ロック設定

【はじめに】

本設定については、次のOSを対象に作成しています。これ以外のOSの場合は、個別にご相談下さい。

<対象OS>

・iOS ※ Apple IDが必要になります。

・Android ※ Googleアカウントが必要になります。

※バージョンや機種等によって手順などには違いがありますので、ご注意ください。

<iPad又はiPhoneの遠隔ロックの設定手順>

1 配布する端末に対して事前に必要な条件

・Apple IDでログインしていること。

「設定」>「iPad(iPhone)にサインイン」の順に進み、設定したApple IDとパスワードを入力する。

・iPad(iPhone)に「iPad(iPhone)を探す」設定がされていること。

「設定」>「(ユーザ名)」>「探す」の順に進み、

「iPad(iPhone)を探す」「探す」ネットワーク「最後の位置情報を送信」をオンにする。

・位置情報サービスがオンになっていること。

「設定」>「プライバシーとセキュリティ」>「位置情報サービス」をオンにする。

・4G LTEなどの通信サービス又はWi-Fiに接続されていること。

2 手元の端末から遠隔ロックをする方法

<iOS端末から遠隔ロックをする場合>

①「設定」から、検索するiPad(iPhone)で設定したApple IDでサインインする。

②「探す」アプリを開く。

③「デバイスを探す」をタップする。

④マップが開き、iPad(iPhone)の位置が示されたら、紛失したiPad(iPhone)を選択する。

⑤「紛失としてマーク」から、「有効にする」を選択する。

⑥パスコードを設定する。

※紛失端末の発見者に連絡をしてもらう場合は、適宜、電話番号・メッセージを入力します。

<PC(Web)から遠隔ロックをする場合>

①icloud.com/findへアクセスし、検索するiPad(iPhone)で設定したApple IDでサインインする。

②マップが開き、iPad(iPhone)の位置が示されたら、紛失したiPad(iPhone)を選択する。

③「紛失としてマーク」を選択する。

④パスコードを設定する。

※紛失端末の発見者に連絡をしてもらう場合は、適宜、電話番号・メッセージを入力します。

<Androidの遠隔ロックの設定手順>

1 配布する端末に対して事前に必要な条件

- ・Googleアカウントにログインしていること。

「設定」>「パスワードとアカウント」>「アカウント追加」>「Google」の順に進み、表示された画面でGoogleアカウントに設定したメールアドレスとパスワードを入力する。

- ・位置情報がオンになっていること。

「設定」>「位置情報」>「位置情報を使用」をオンにする。

- ・「デバイスを探す」設定がされていること。

「設定」>「セキュリティとプライバシー」>「デバイスを探す」をオンにする。

- ・デバイスが Google Play に表示されていること。

<https://play.google.com/library/devices/>にアクセスし、「メニューに表示する」チェックボックスがオンになっていることを確認します。

- ・電源が入っており、4G・LTEなどの通信サービスまたはWi-Fiに接続されていること。

2. 手元の端末から遠隔ロックをする方法

<Android端末から遠隔ロックをする場合>

- ①「デバイスを探す」アプリをダウンロードし、紛失した端末のGoogleアカウントとパスワードでログインする。
- ②「デバイスを探す」画面から、紛失した端末を選択する。
- ③マップが開き、端末の位置が示されたら、「デバイスを保護」を選択する。
- ④PIN、パターンまたはパスワードを入力し、ロックする。
※拾った方に連絡をしてもらう場合は、適宜、電話番号・メッセージを入力します。

<PC(Web)から遠隔ロックをする場合>

- ①android.com/find にアクセスし、Google アカウントにログインする。
- ②マップが開き、端末の位置が示されたら、紛失した端末を選択する。
- ③「デバイスを保護」を選択し、PIN、パターンまたはパスワードを入力し、ロックする。
※先に「ロックとデータ消去を有効にする」の選択が必要となる場合があります。
※拾った方に連絡をしてもらう場合は、適宜、電話番号・メッセージを入力します。