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
（Android）

Ver1.0（2023.07）

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、本製品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

利用するバージョンや機種により使用可能な機能や画面の表示、設定アプリのメニューが異なる可能性があります。**本資料は AQUOS sense3 Android バージョン 10 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
1-1 資産・構成管理 **テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。**	・端末と利用者の把握	P.6

表 2．チェックリスト項目と利用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
2-4 マルウェア対策 **スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。**	・提供元不明アプリのインストールを許可しない設定の確認	p.7
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・のぞき見の対策	P.9
5-1 脆弱性管理 **テレワーク端末にはメーカーサポートが終了した OS やアプリケーションを利用しないよう周知する。**	・メーカーサポートの確認	P.11
5-2 脆弱性管理 **テレワーク端末の OS やアプリケーションに対して最新のセキュリティアップデートを適用するよう周知する。**	・OS 及びアプリケーションの最新化	P.13
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.17
6-2 通信暗号化 **無線 LAN ルーターを利用する場合は、セキュリティ方式として「WPA2」又は「WPA3」を利用し、無線の暗号化パスワードは第三者に推測されにくいものにする。**	・無線 LAN のセキュリティ方式の確認	P.18
7-2 インシデント対応・ログ管理 **テレワーク端末と接続先の各システムの時刻を同期させる。**	・時刻同期設定	P.19
8-1 データ保護 **スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。**	・端末位置の把握	P. 21
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。**	・デバイスパスワードの設定	P.23

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 1-1 への対応

3-1-1　端末と利用者の把握

テレワーク用に従業員へ貸与する端末のシリアル番号を確認します。管理者は、利用者が使用している端末とその設置場所をあらかじめ把握し、**定期的な棚卸によって紛失を検知できるようにすることが重要です。**ここでは端末を識別するシリアル番号の確認手順を記載します。

端末のシリアル番号の確認

利用者に貸与するテレワーク端末のシリアル番号を確認します。

【手順①】

テレワーク端末背面に記載のシリアル番号（製造番号）を確認します。

参考　テレワーク端末背面のシリアル番号が見つけられない場合

設定アプリを開き、「デバイス情報」-「モデルとハードウェア」の順にタップするとシリアル番号の欄からシリアル番号を確認できます。

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 2-4 への対応

４-１-１　　提供元不明アプリのインストールを許可しない設定の確認

公式アプリケーションストア（Google Play ストアやキャリアサイト）以外のアプリである、「提供元不明アプリ」は、マルウェア感染のきっかけとなる恐れや情報漏洩のリスクがあります。そのため、端末が不明なアプリのインストールを許可しない設定であることを確認します。この設定はデフォルトで、許可しない設定になっていますが、以下の手順で設定の確認・有効化を行うことができます。

【手順①】

「設定」から「アプリと通知」をタップします。

【手順②】

「詳細設定」をタップし、「特別なアプリアクセス」をタップします。

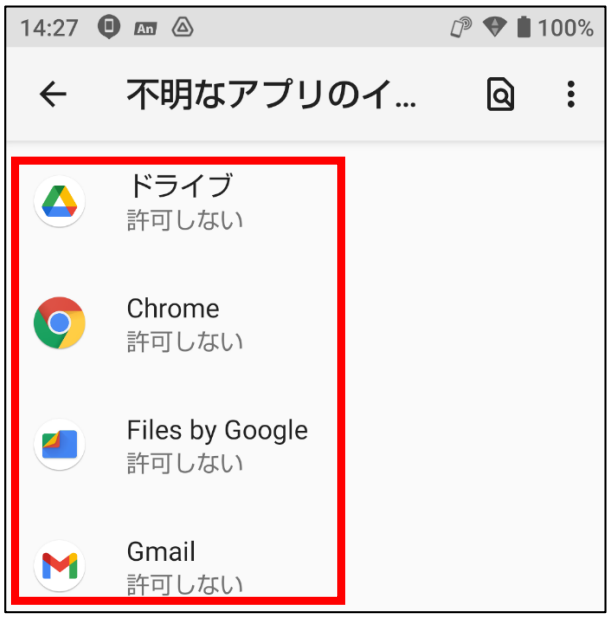
【手順③】

「不明なアプリのインストール」をタップします。

【手順④】

アプリの一覧が表示されます。この一覧は、端末にインストール済みのアプリ経由で、不明なアプリをインストールできるかどうかが表示されています。

アプリ毎に、不明なアプリのインストールが許可されていないか確認します。「許可する」設定になっているアプリがある場合は、必ず「許可しない」設定へ変更してください。



4-2　チェックリスト 4-1 への対応

4-2-1　　第三者からの盗聴・のぞき見の対策

テレワークはオフィスワークに比べ、第三者（家族を含む）に盗聴・のぞき見されるリスクが高くなります。そのため、**オフィス外で端末を利用する場合は第三者からの盗聴・のぞき見されないよう注意する必要があります。**端末上に投影されている情報がのぞき見されないように**のぞき見防止フィルム**を利用する、端末から離れる際は**画面ロックをかける**等の対策が必要です。

端末の状態として、画面消灯（スリープ）と画面ロックの２つの状態があります。この２つの状態は、いずれも自動で実行されるように設定することができます。
記載する「自動スリープ設定」と「自動ロック設定」は、どちらも設定を行ってください。

自動スリープ設定

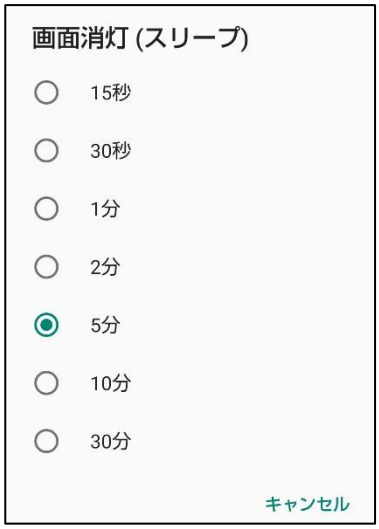
本項目は画面をスリープ状態にする設定です。後述の「自動ロック」の設定も、必ず行ってください。

【手順①】
「設定」から「ディスプレイ」をタップします。

【手順②】
「画面消灯（スリープ）」をタップします。

【手順③】

任意の画面スリープ時間を指定します。指定した時間が経過すると画面が消灯します。



自動ロック設定

本項目は画面スリープ状態になった後からの自動ロック時間を設定する項目です。

【手順①】

「設定」-「セキュリティ」をタップします。

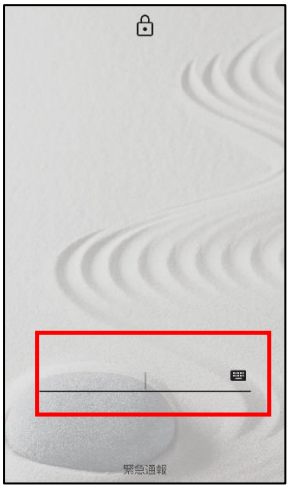
【手順②】

「画面ロック」右側の「⚙」アイコン（設定）をタップし、「自動ロック」をタップします。

【手順③】

任意の自動ロック時間を指定します。指定した時間が経過すると画面がロックされます。

画面がロックされると、解除するには、設定したパスワードを入力する必要があります。



4-3　チェックリスト 5-1 への対応

4-3-1　　メーカーサポートの確認

利用する端末の Android は製品提供元からリリースされる最新の Android バージョンを利用します。最新バージョンを利用することは、脆弱性をついたサイバー攻撃に対して有効な対策となりますので、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。利用している Android バージョンのサポート期間や今後の更新予定などについては製品提供元のサイト（※）で確認してください。

※　主要 3 キャリアの製品アップデート情報サイト

NTT ドコモ：https://www.nttdocomo.co.jp/support/product_update/

au：https://www.au.com/information/notice_mobile/update/

ソフトバンク：https://www.softbank.jp/mobile/info/personal/software/

Android バージョンの確認方法

【手順①】

「設定」から「デバイス情報」をタップします。

【手順②】

「Android バージョン」の下に製品のバージョンが記載されています。

4-4　チェックリスト 5-2 への対応

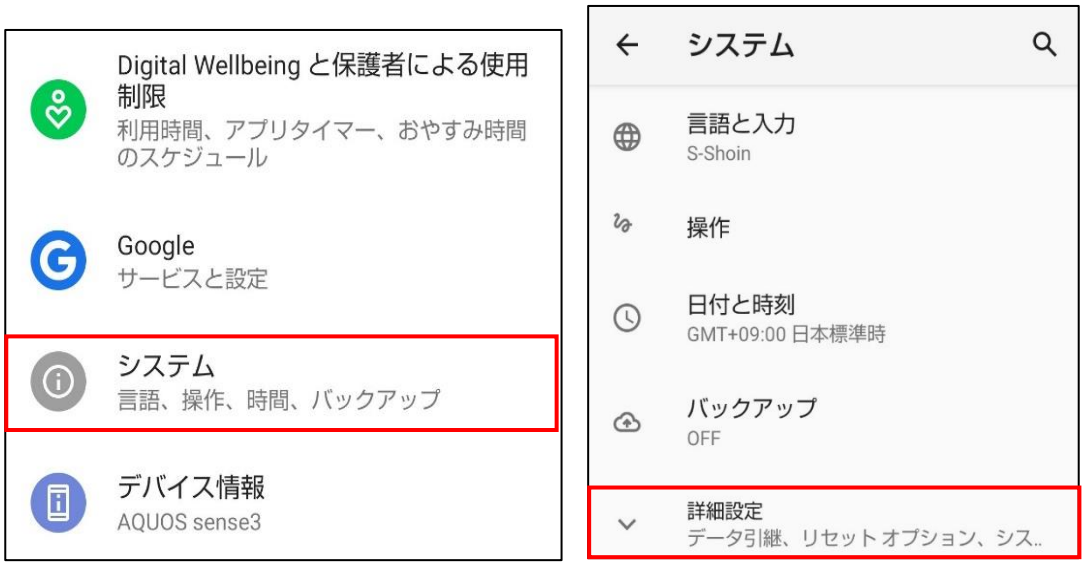
4-4-1　OS 及びアプリケーションの最新化

OS やアプリケーションを最新の状態にアップデートして利用します。アップデートをすることは、OS やアプリケーションの脆弱性が修正され、**脆弱性をついたサイバー攻撃に対して有効な対策です。**そのため、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。

Android のシステムアップデート方法

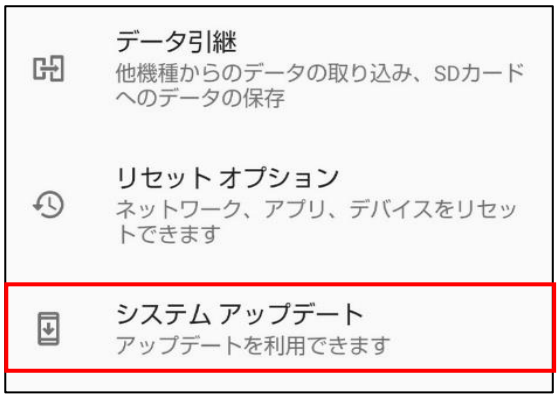
【手順①】

「設定」から「システム」をタップし、「詳細設定」をタップします。



【手順②】

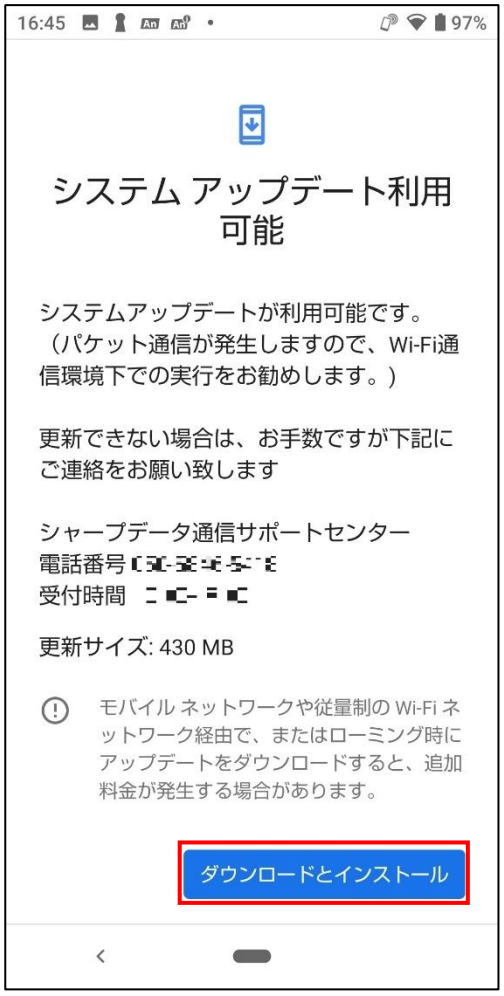
「システムアップデート」をタップします。



【手順③】

「ダウンロードとインストール」をタップします。

再起動を行う必要がある場合は画面に従い再起動してください。



インストールしているアプリの更新

【手順①】

「Play ストア」をタップします。

【手順②】

画面左上の「メニュー」をタップし、「マイアプリ＆ゲーム」をタップします。

【手順③】

アップデート利用可能なアプリを確認できます。アップデートがある場合は、「すべて更新」をタップして、アプリのアップデートを行います。

アプリの自動更新の設定

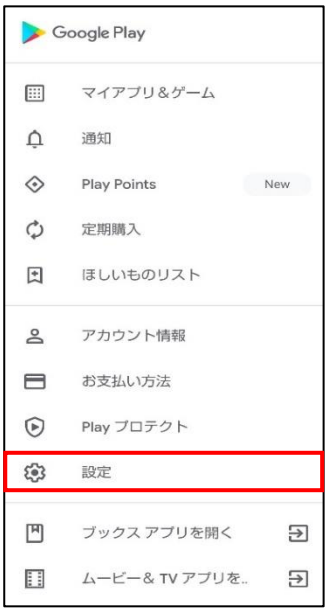
端末内にインストールしているアプリを自動更新する設定をします。

【手順①】

「Play ストア」をタップします。

【手順②】

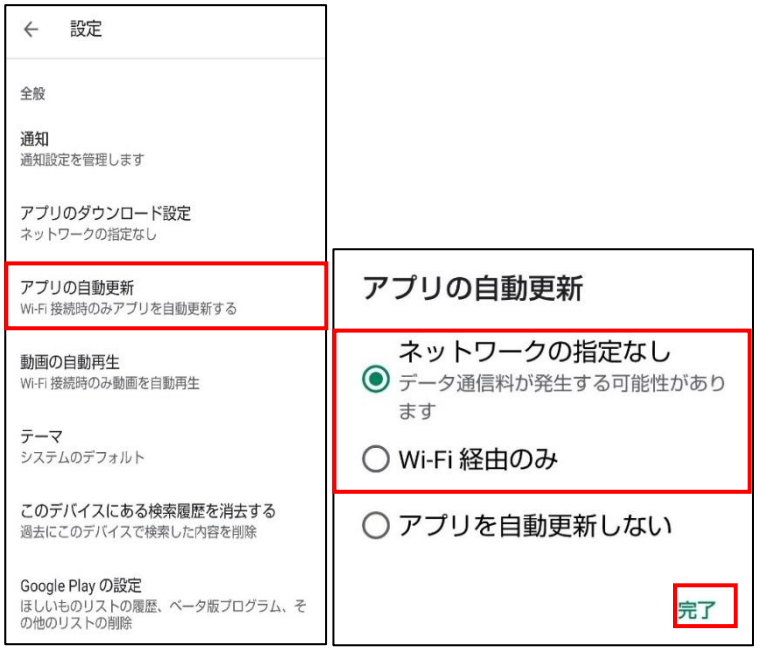
画面左上の「メニュー」をタップし、「設定」をタップします。



【手順③】

「アプリの自動更新」をタップし、アプリの自動更新を以下のどちらかに設定し、「完了」をタップします。

- 「ネットワークの指定なし」：モバイルネットワーク利用時と Wi-Fi 利用時の両方で自動更新されます。
- 「Wi-Fi 経由のみ」：Wi-Fi 接続時のみに自動更新されます。



4-5　チェックリスト 6-1 への対応

4-5-1　　サービスへの接続確認

インターネットの通信は、通信内容をどこかで盗み見られたり、改ざんされたりする可能性があります。そのため、通信内容が暗号化されている「HTTPS」通信で接続しているかを確認します。Web サイトにアクセスする場合は、ブラウザの接続先 URL 入力欄（アドレスバー）を確認し、接続先のサイトが「https://」から始まっているかどうかを確認します。

＜参考情報－Chrome ブラウザの URL 入力欄（アドレスバー）の確認場所＞

HTTPS 通信の場合、🔒マークのアイコンがつきます。URL の個所をタップすると、URL のアドレスを確認することができます。

4-6　チェックリスト 6-2 への対応

4-6-1　　無線 LAN のセキュリティ方式の確認

無線 LAN の暗号化方式**「WEP」や「WPA」は脆弱性があり、通信内容を盗み見られる危険性があります。**そのため、より安全な暗号化方式である「WPA2」や「WPA3」を用いて、無線 LAN を利用していることを確認します。

【手順①】

【設定」から、「ネットワークとインターネット」をタップします。

【手順②】

「Wi-Fi」をタップします。

【手順③】

接続済の Wi-Fi と接続可能な Wi-Fi の一覧が表示されます。「接続済み」の記載のある Wi-Fi の「⚙」をタップします。

【手順④】

接続している Wi-Fi の詳細が表示されます。「セキュリティ」に表示されている暗号化方式をチェックし「WPA」や「WEP」になっていないことを確認します。「WPA」や「WEP」になっていた場合は別の Wi-Fi に接続し直すことを推奨します。

4-7　チェックリスト 7-2 への対応

4-7-1　　時刻同期設定

端末とアクセス先の各システムの時刻を同一のものにするため、端末の時刻同期設定を行います。各機器の時刻を一致させることで、**インシデント発生時のアクセスログ等の調査の際に、正確な調査を行う**ことができます。

Android の時刻設定

【手順①】

「設定」の「システム」をタップし、「日付と時刻」をタップします。

【手順②】

「ネットワークの時刻を使用する」と「ネットワークから提供されたタイムゾーンを使用する」を有効にします。

4-8　チェックリスト 8-1 への対応

4-8-1　　端末位置の把握

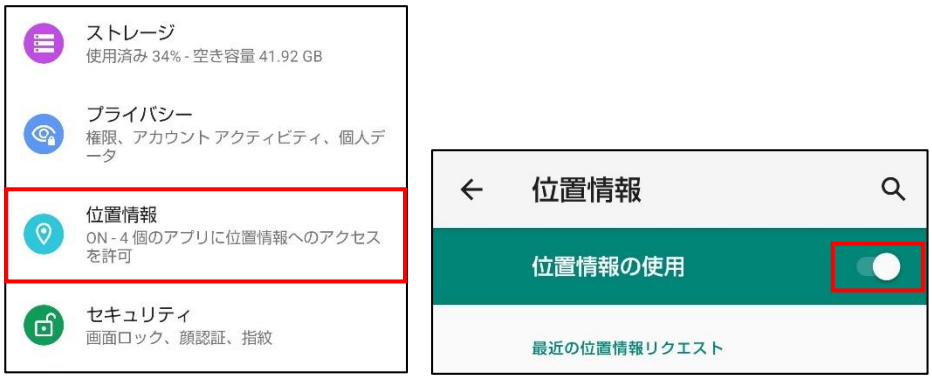
端末の紛失・盗難に備えて位置情報を検出できるように設定します。端末の位置情報を検出できるように設定することにより、**紛失・盗難時に端末の位置を特定できる可能性が高まり、情報漏洩のリスクを低減することができます。**
端末の位置情報を検出するには、下記の端末の位置情報の設定を有効しておくことに加え、端末に Google アカウント（下部に解説あり）でログインし、連携しておく必要があります。対象端末の位置情報は、連携している Google アカウント保有者のみが確認することができます

この手順は、利用者が自身のテレワーク端末の位置を確認できるようにする方法です。**管理者側で一律に管理を行いたい場合は、別途 MDM 製品の導入を検討してください。**

位置情報の取得設定

この設定を行うことで、端末の場所を調べられるようにする機能を有効化します。

【手順①】
「設定」から「位置情報」をタップし、「位置情報の使用」をオンにします。



【手順②】
「設定」から「セキュリティ」から、「デバイスを探す」をタップし、「ON」にします。

端末位置の確認方法

【手順①】

下記 URL にアクセスし、Android 端末に登録している Google アカウントでログインします。

https://www.google.com/android/find

【手順②】

画面左ペインから、端末を選択します。ここでは、以下の 3 つの操作を実行することができます。

- 「音を鳴らす」：端末から音を出すことができます。音は、端末がマナーモードになっていても発生します。
- 「デバイスを保護」：端末をロックし Google アカウントからログアウトします。この際、ロック画面にメッセージを表示することができます。
- 「デバイスデータを消去」：端末内のデータ全てを消去します。消去後はデバイスの位置の特定も出来なくなります。

【参考】紛失した Android デバイスの位置の特定、ロック、データ消去を行う

URL：https://support.google.com/accounts/answer/6160491?hl=ja

4-9　チェックリスト 9-2 への対応

4-9-1　デバイスパスワードの設定

Android は、初期状態ではパスワードによるロックが適用されていないため、利用者自身で設定を行う必要があります。また、貸与された端末で初期パスワードが設定されている場合、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。**

初期パスワードの設定変更

【手順①】

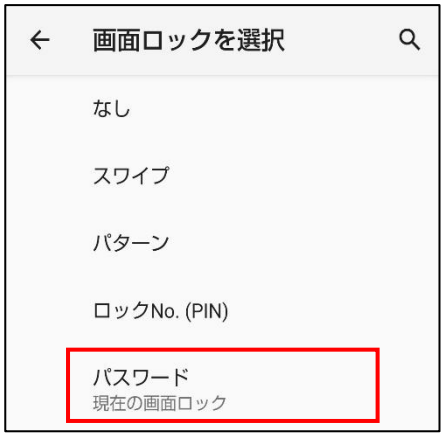
「設定」から「セキュリティ」をタップします。

【手順②】

「画面ロック」をタップします。既にパスワードが設定されている場合は、パスワードを入力してください。

【手順③】

「パスワード」をタップします。



【手順④】

新しいパスワードを入力し、「次へ」をタップします。次に、新しいパスワードをもう一度入力し、「確認」をタップします。