

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 （iOS）

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	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 1-1 への対応	6
3-1-1 端末と利用者の把握	6
4 利用者向け作業	7
4-1 チェックリスト 4-1 への対応	7
4-1-1 第三者からののぞき見の対策	7
4-2 チェックリスト 5-1 への対応	8
4-2-1 メーカーサポートの確認	8
4-3 チェックリスト 5-2 への対応	9
4-3-1 OS 及びアプリケーションの最新化	9
4-4 チェックリスト 6-1 への対応	12
4-4-1 サービスへの接続確認	12
4-5 チェックリスト 6-2 への対応	13
4-5-1 無線 LAN のセキュリティ方式の確認	13
4-6 チェックリスト 7-2 への対応	14
4-6-1 時刻同期設定	14
4-7 チェックリスト 8-1 への対応	15
4-7-1 端末位置の把握	15
4-8 チェックリスト 8-2 への対応	18
4-8-1 保存データの暗号化	18
4-9 チェックリスト 9-2 への対応	18
4-9-1 初期パスコード設定変更	18

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、iOS 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により使用可能な機能が異なります。**本資料では iOS バージョン 17 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、ご利用様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 3. 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
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。	・ 第三者からののぞき見の対策	P.7
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.8
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.9
6-1 通信暗号化 セキュリティインシデントの発生時や、そのおそれがある状況に備えて、対応手順及び関係者への各種連絡体制を定め、従業員に緊急連絡先を周知する。	・ サービスへの接続確認	P.12
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.13
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.14
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.15
8-2 データ保護 テレワーク端末の盗難・紛失時に情報が漏えいしないよう、端末に内蔵されたハードディスクやフラッシュメモリ等の記録媒体の暗号化を実施する。ただし、端末に会社のデータを保管しない場合を除く。	・ 保存データの暗号化	P.18
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。	・ 初期パスコード設定変更	P.18

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

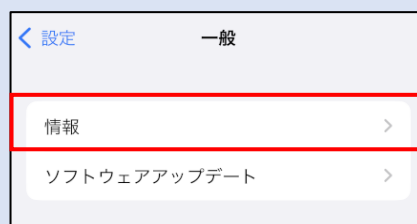
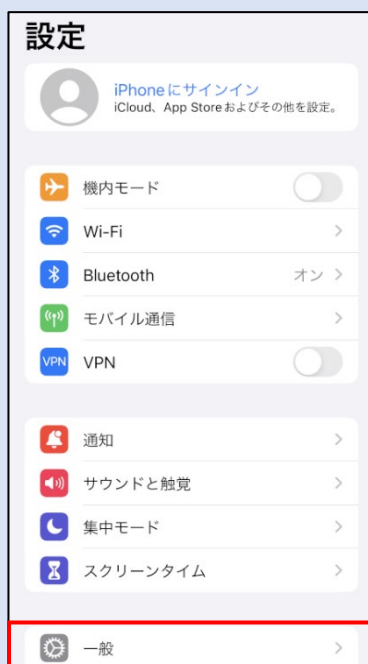
利用者に貸与するテレワーク端末のシリアル番号を確認します。

【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からない場合
設定アプリを開き、「一般」-「情報」の順番にタップすると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 4-1 への対応

4-1-1 第三者からののぞき見の対策

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**。端末に投影されている会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。

自動スクリーンロック設定

【手順①】

「設定」をタップし、「画面表示と明るさ」をタップします。



【手順②】

「自動ロック」をタップし、任意の自動ロック時間をタップします。



4-2 チェックリスト 5-1 への対応

4-2-1 メーカーサポートの確認

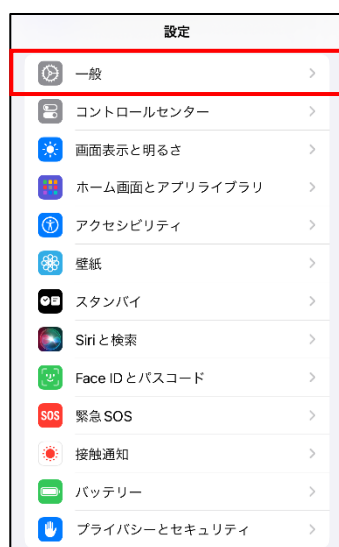
利用する端末の iOS は製品提供元からリリースされる最新の iOS バージョンを利用します。最新バージョンを利用することは、脆弱性をついたサイバー攻撃に対して有効な対策となりますので、定期的にアップデートがないか確認をすることを推奨します。利用している iOS バージョンのサポート期間や今後の更新予定などについては製品提供元である Apple 社のサイト（※）で確認してください。

※ Apple サポート公式サイト（<https://support.apple.com/ja-jp>）

iOS バージョンの確認方法

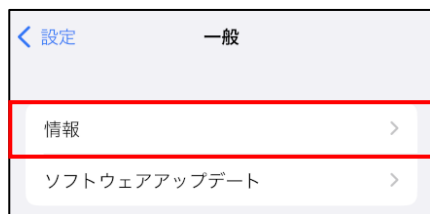
【手順①】

「設定」をタップし、「一般」をタップします。



【手順②】

「情報」をタップし、システムバージョンから iOS システムバージョンを確認します。



4-3 チェックリスト 5-2 への対応

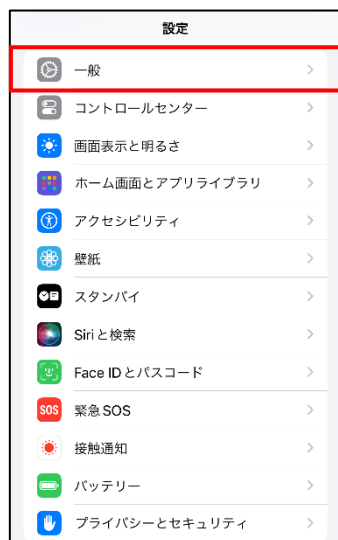
4-3-1 OS 及びアプリケーションの最新化

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、**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**。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。

iOS 手動アップデート方法

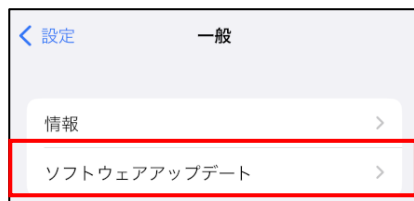
【手順①】

「設定」をタップし、「一般」をタップします。



【手順②】

「ソフトウェアアップデート」をタップします。「ダウンロードしてインストール」が表示された場合は、最新のアップデートが必要な状態です。「ダウンロードしてインストール」をタップし、アップデートを実行します。



iOS 自動アップデート設定

【手順①】

「設定」をタップし、「一般」をタップします。



【手順②】

「ソフトウェアアップデート」をタップし、「自動アップデート」をタップします。



【手順③】

自動インストールの「iOS アップデート」と自動ダウンロードの「iOS アップデート」をオンにします。

※ iOS をアップデートする際は、Wi-Fi 接続が必須となります。

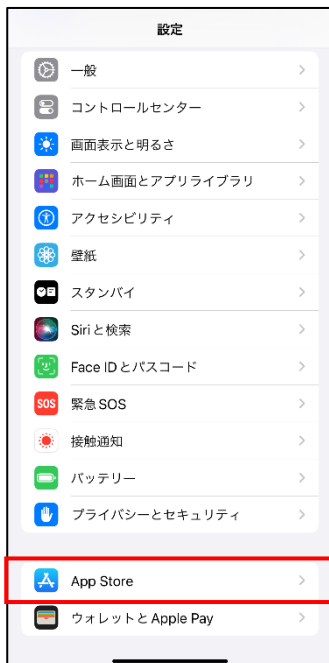


インストールしているアプリの自動更新設定

端末内にインストールしているアプリケーションが最新となっているかを確認します。

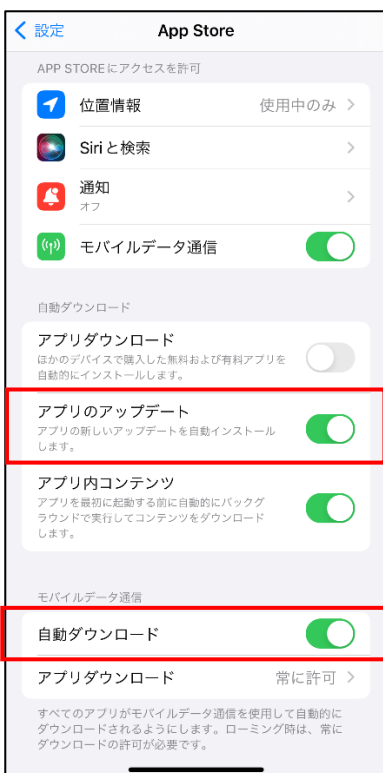
【手順①】

「設定」をタップし、「App Store」をタップします。



【手順②】

「アプリのアップデート」と「自動ダウンロード」をオンにします。



【手順③】

「アプリダウンロード」をタップし、「常に許可」にチェックを入れます。

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

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。

また、接続先のドメイン（「https://」から先の文字列）が接続しようとしているサイトのドメインと同一かを確認します。不安な場合は、普段使用するサイトをブックマークに登録しブックマークから開くことや、検索サイトで検索を行い検索結果から開くことなどをお勧めします。

＜参考情報－Safari 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、

4-5 チェックリスト 6-2 への対応

4-5-1 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」をタップし、「Wi-Fi」をタップします。



【手順②】

接続している Wi-Fi を確認します。何も表示がなければ、安全な無線 LAN に接続されています。

下図のように、「セキュリティ保護されていないネットワーク」や「安全性の低いセキュリティ」と表示されている場合は、無線 LAN の設定を変更するか、別の無線 LAN に接続するようにしてください。



4-6 チェックリスト 7-2 への対応

4-6-1 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。

iOS の時刻設定

【手順①】

「設定」をタップし、「一般」をタップします。



【手順②】

「日付と時刻」をタップし、自動設定がオンになっていれば、時刻設定ができている状態です。



4-7 チェックリスト 8-1 への対応

4-7-1 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 Apple ID（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 Apple ID 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。ここでは、以下の 2 点についての手順を記載しています。

- ・ 端末の位置情報の取得設定：端末の場所を調べられるようにする機能の有効化
- ・ 端末の位置情報の確認：端末の現在位置の確認方法

なお、**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。**

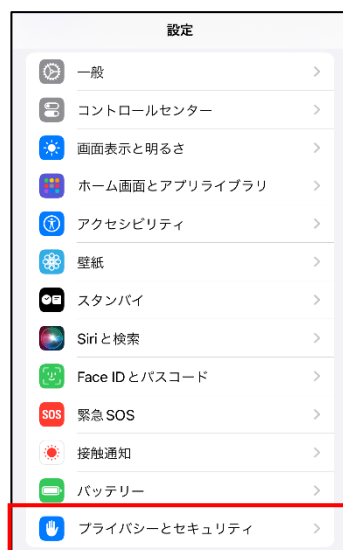
端末の位置情報の取得設定

端末の位置情報を取得するため次の 3 つの設定を行います

- ・ 位置情報サービスを ON にする
- ・ 「iPhone を探す」を ON にする
- ・ iCloud アカウントを端末と連携する

【手順①】

「設定」をタップし「プライバシーとセキュリティ」をタップします。



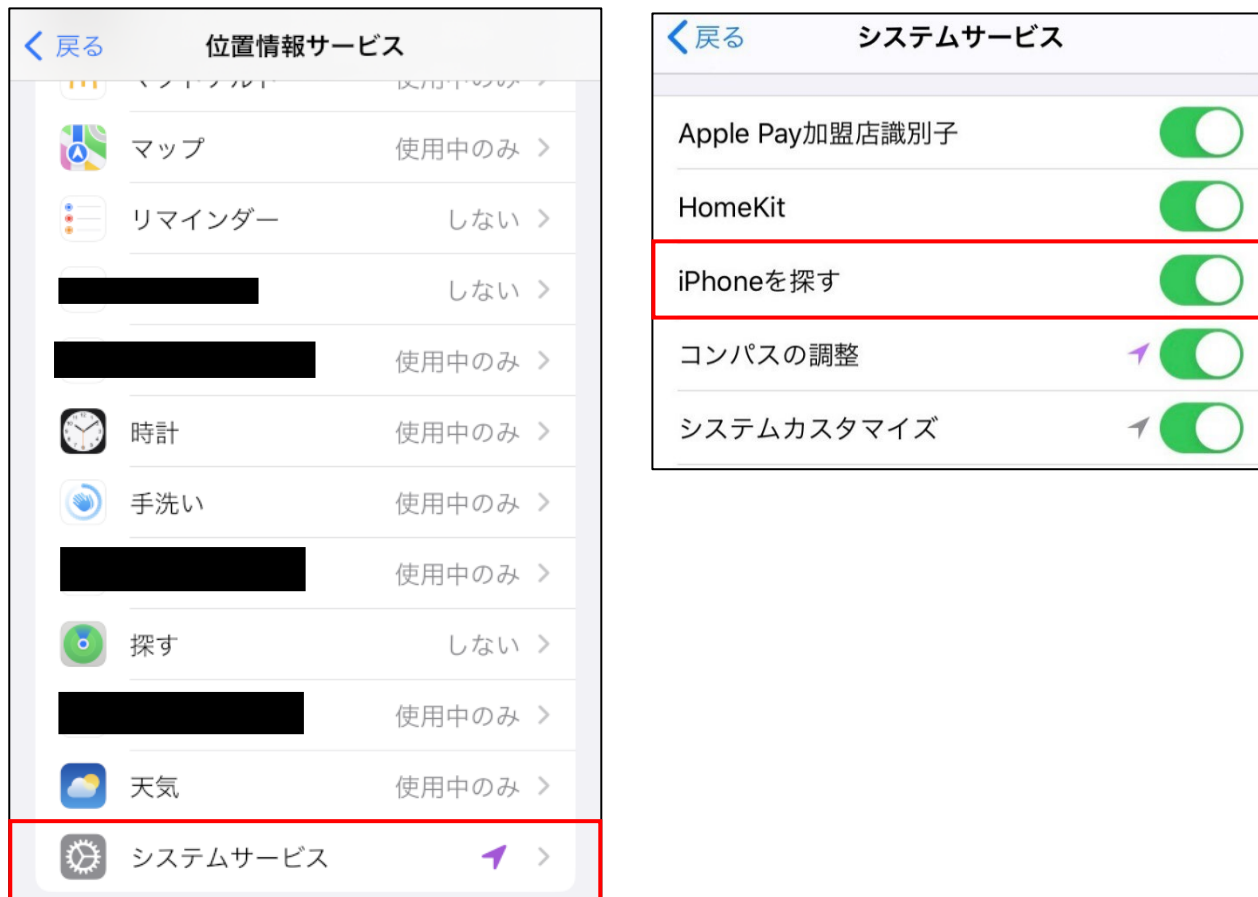
【手順②】

「位置情報サービス」をタップし、「位置情報サービス」が「オン」になっていることを確認します。「オフ」になっていた場合は「オン」にします。



【手順③】

「システムサービス」をタップし、「iPhoneを探す」をオンにします。



【手順④】

「設定」-「iPhone にサインイン」から、Apple ID でサインインします。

Apple ID を持っていない場合は、上記画面の「Apple ID をお持ちでないか忘れた場合」から Apple ID を作成するか、パソコンから下記 URL にアクセスして、「Apple ID を作成」から Apple ID を作成します。

URL : <https://appleid.apple.com/>



端末の位置情報の確認

【手順①】

紛失・盗難した端末とは別の端末で Web ブラウザから下記サイトへアクセスし、iCloud アカウントでログインを行います。

<https://icloud.com/find>

【手順②】

アクセス後に表示される画面上部の、「すべてのデバイス」から、検索する該当の端末名を選択し、端末の位置を地図上で確認します。なお、端末の電源がオフの場合、オフになる前に取得した位置情報のため、最新ではない可能性があります。



4-8 チェックリスト 8-2 への対応

4-8-1 保存データの暗号化

パスコードを設定することにより、データ保護機能が有効化され、保存されているデータが暗号化されます。パスコード設定手順は「4-9-1 初期パスコード設定変更」を参照してください。

【参考】[iPhone でパスコードを設定する - Apple サポート \(日本\)](#)

4-9 チェックリスト 9-2 への対応

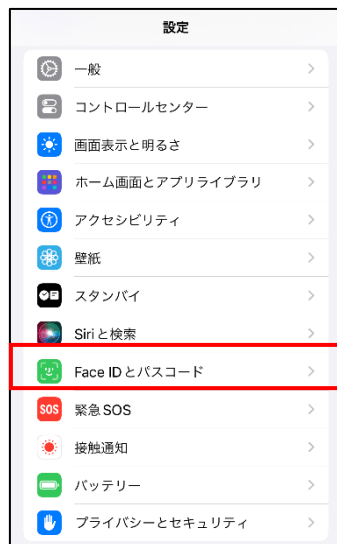
4-9-1 初期パスコード設定変更

初期パスコードは、誰が把握しているかわからないので、貸与された端末の初期パスコードは速やか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します。

初期パスワードの設定変更

【手順①】

「設定」をタップし、「Face ID とパスコード」をタップします。



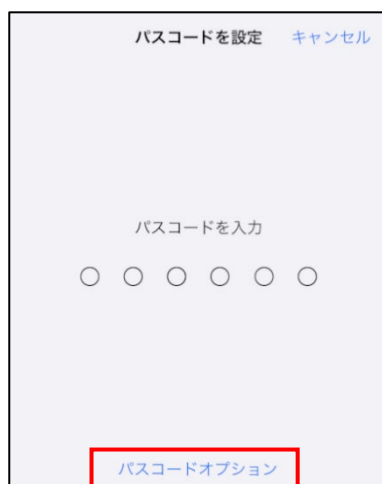
【手順②】

「パスコードをオンにする」をタップします。パスコードが元々オンになっている場合は「パスコードを変更」をタップします。



【手順③】

「パスコードオプション」をタップします。



【手順④】

ここでは、パスコードの種類（※）を選択できます。

本手順では「カスタムの英数字コード」を指定しています。この場合、英語と数字を組み合わせでの入力が必要で



【手順⑤】

新しいパスコード（※）を入力し、「次へ」をタップします。



パスコードの強度が十分でない場合、以下のように「このパスコードは簡単に推測できてしまいます」と表示されます。この表示が出た場合、「パスワードを変更」をタップし、以前入力したパスワードよりも、より複雑なパスコードをしてください。



【手順⑥】

新しいパスコードをもう一度入力し、「完了」をタップします。



【謝辞】

本設定解説資料の策定及び更新を行うにあたっては、Apple Inc.の関係各所の方々に多大なるご協力をいただきました。この場をお借りして深く御礼申し上げます。