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
（macOS）

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、Mac 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 macOS Sonoma（バージョン 14.3）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
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
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.7

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
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。**	・ファイル拡張子の表示設定	P.9
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.11
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.13
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.14
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.21
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.22
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.23
8-3 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。**	・FileVault による暗号化設定	P.30
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。**	・初期パスワード設定変更	P.33

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を確認する

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

デスクトップ左上にある Apple マークをクリック後、「この Mac について」をクリックし、下図の画面からシリアル番号を確認します。

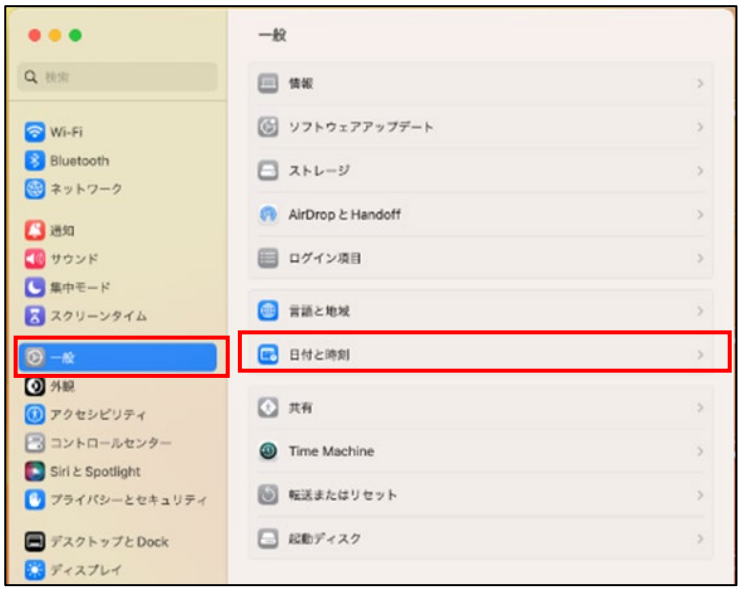
3-2　チェックリスト 7-2 への対応

3-2-1　　時刻同期設定

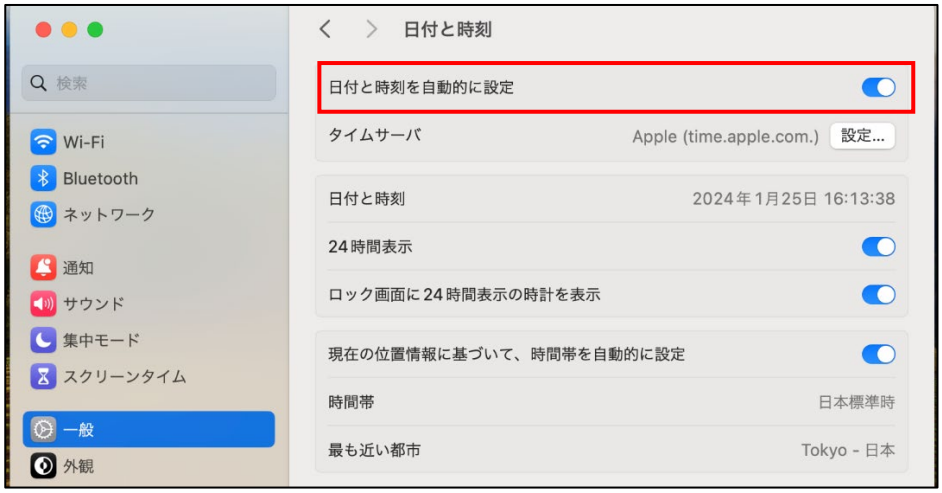
端末とアクセス先の各システムの時刻を同一のものにするため、端末の時刻同期設定を行います。各機器の時刻を一致させることで、**インシデント発生時のアクセスログ等の調査の際に、正確な調査を行う**ことができます。

【手順①】
デスクトップ左上にある Apple マークをクリック後「システム設定」をクリックします。

【手順②】
「一般」をクリック後「日付と時刻」をクリックします。

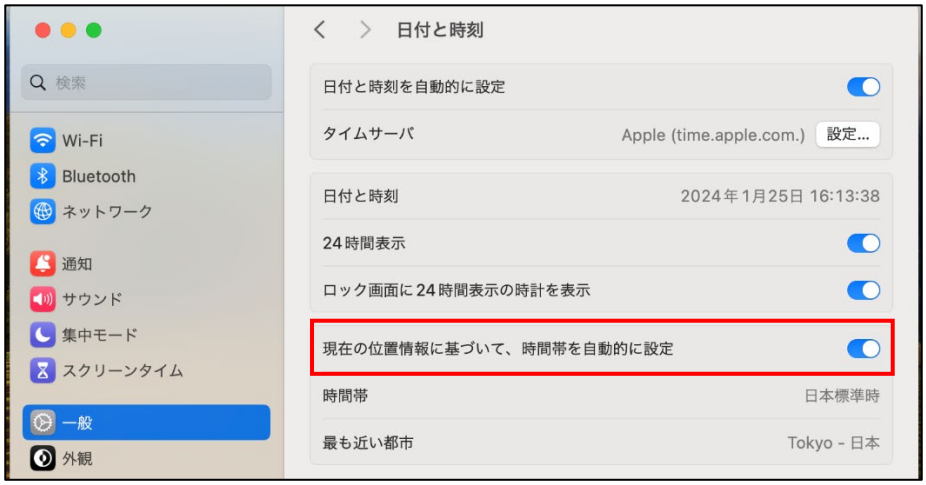


【手順③】
「日付と時刻を自動的に設定」をオンにします。
社内時刻同期サーバー（NTP サーバー）で一括時刻同期をさせている場合は、時刻同期サーバー名の欄に社内時刻同期サーバー名を指定してください。



【手順④】

「現在の位置情報に基づいて、時間帯を自動的に設定」をオンにします。



4　利用者向け作業

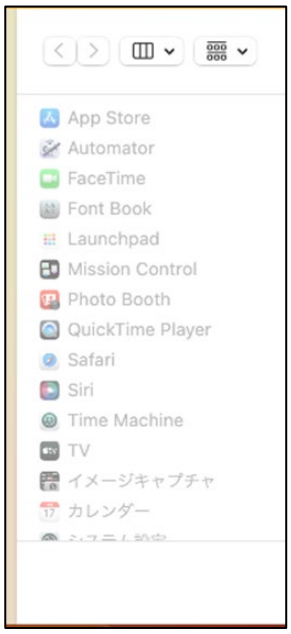
ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第２部に記載されているチェックリスト項目のうち、本製品の利用者が実施すべき対策の設定手順や注意事項を記載します。

4-1　チェックリスト 2-2 への対応

4-1-1　ファイル拡張子の表示設定

メールに添付されているファイルやローカルディスク、ファイルサーバなどに保管されているファイルが、怪しいファイルか見分ける方法として、ファイル名拡張子（ファイルの種類を区別するためにファイル名の末尾につけられる文字列）を確認する方法があります。

しかし、デフォルトでは下記のように非表示となっており、ファイルの拡張子確認することができません。



下記手順により、ファイル名拡張子が表示され、ファイルの拡張子を確認することができるようになります。

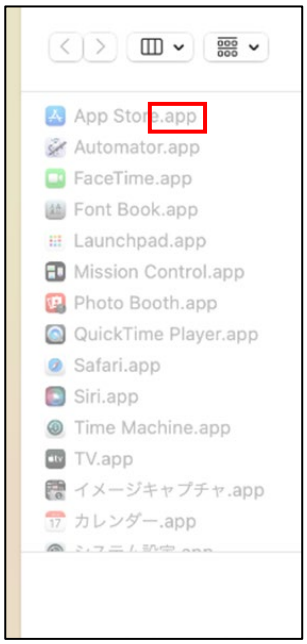
【手順①】

画面左上の Apple マーク隣の「Finder」をクリックし、「設定」を選択します。

【手順②】

「詳細」タブをクリックし、「全てのすべてのファイル名拡張子を表示」にチェックを入れます。

ファイル名拡張子が表示されるようになります。（例.アプリケーションの場合は、「.app」です。）



4-2　チェックリスト 4-1 への対応

4-2-1　　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。

手動スクリーンロックのかけ方

「Control」キーと「Command」キーを押しながら「Q」キーを入力することで使用している端末をロックすることが可能です。

自動スクリーンロック設定

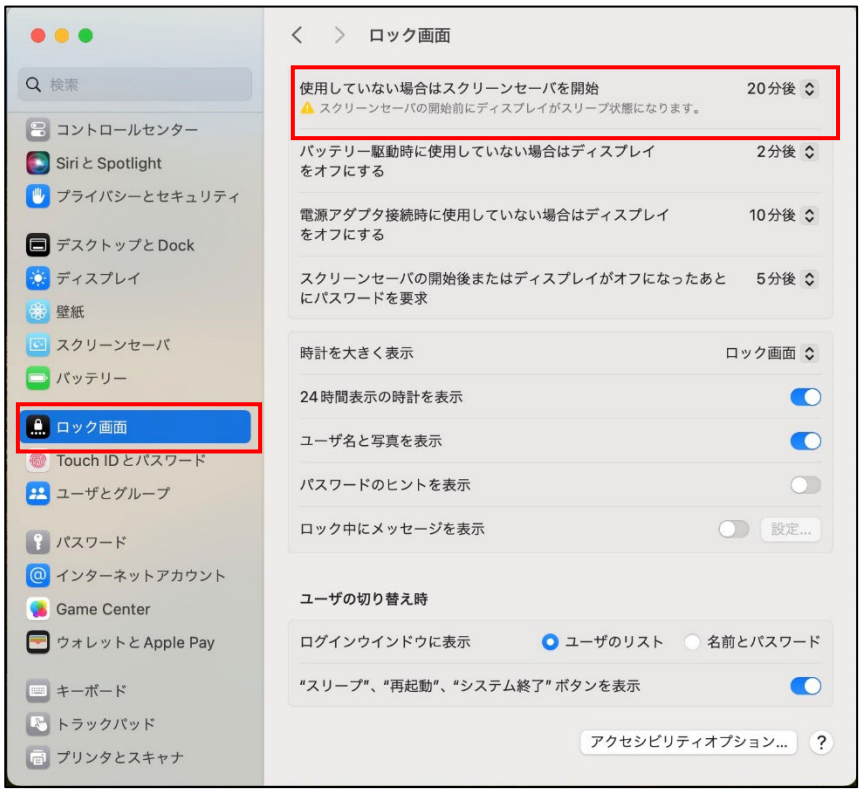
ロックをせずに端末から離れてしまう場合に備え、一定時間操作しない場合に自動的にロックする設定を行います。

【手順①】

デスクトップ左上にある Apple マークをクリック後「システム設定」をクリックします。

【手順②】

下図の画面の「ロック画面」をクリックし、「使用していない場合はスクリーンセーバを開始」に任意の待ち時間を設定します。



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 OS は製品提供元からサポートのあるバージョンを利用します。サポート切れの OS を使用していると不具合や脆弱性が修正されないため、不正アクセスの起点となってしまう恐れがあり、セキュリティ上のリスクとなります。OS のサポート期間については、Apple 社のサイト（※）を確認するか、macOS 端末の取引のある SI ベンダーや代理店に確認してください。

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

OS バージョンの確認方法

【手順①】

デスクトップ左上にある Apple マークをクリック後「この Mac について」をクリックします。

【手順②】

下図の画面から macOS の現在のバージョンを確認します。

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。macOS にインストールされている各アプリケーションのアップデートは、アプリケーションの更新機能、各製品の公式 HP 等で確認するか、対象製品の取引のある SI ベンダーや代理店に確認を行ってください。

OS アップデート確認

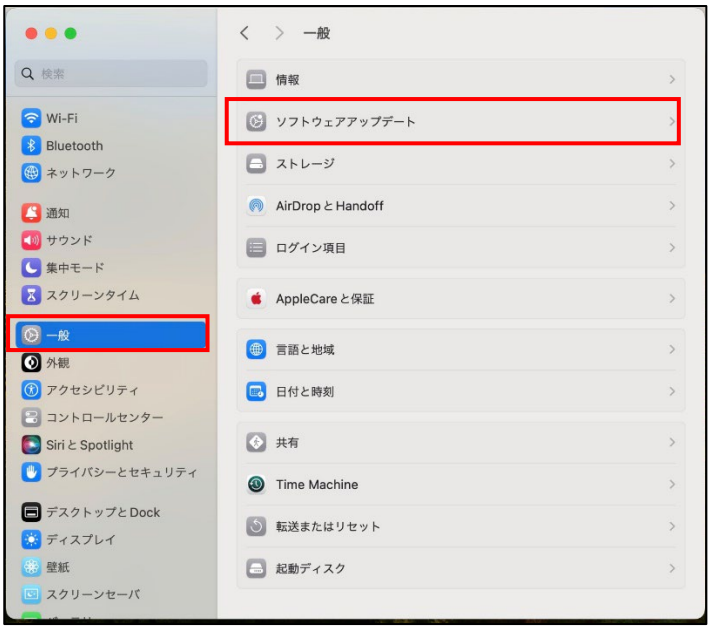
macOS が最新になっているかを確認します。

【手順①】

デスクトップ左上にある Apple マークをクリック後「システム設定」をクリックします。

【手順②】

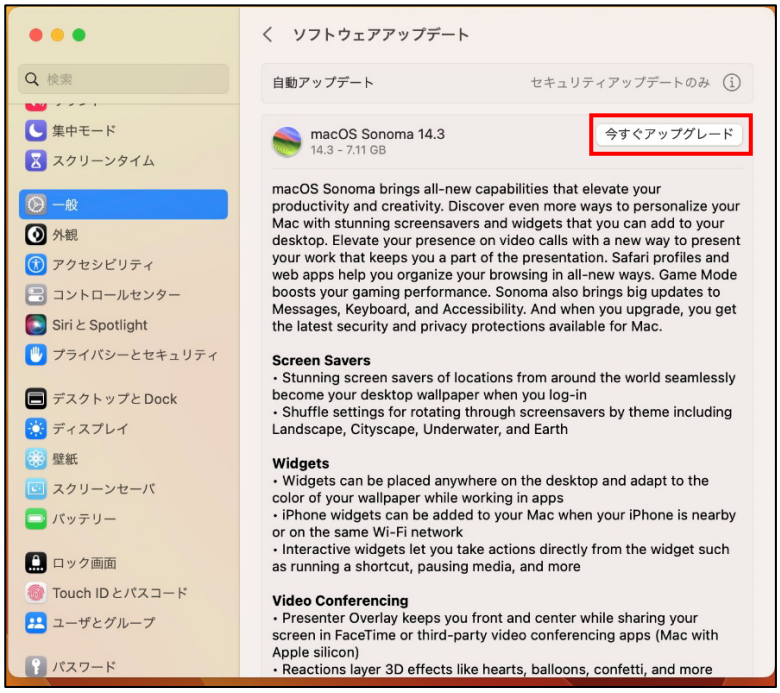
「一般」をクリック後、「ソフトウェア・アップデート」をクリックします。



【手順③】

画面（※）上部に「今すぐアップグレード」の表示がなければ最新バージョンの Sonoma となっています。

※　下記画面のみ、Sonoma ではなく、Ventura の画面です。Sonoma では表記や画面イメージが異なる可能性がありますが、基本的な手順は同じです。



macOS 手動アップデート

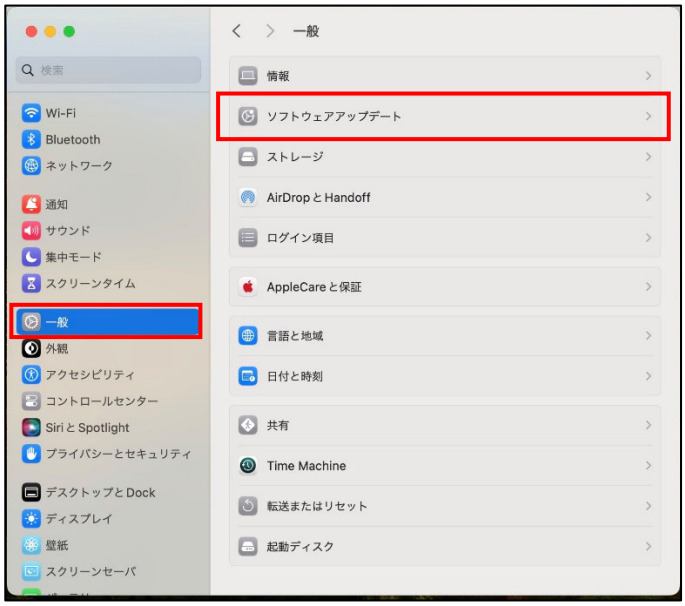
ソフトウェアが最新になっていない場合この手順にて手動アップデートを行います。

【手順①】

デスクトップ左上にある Apple マークをクリック後「システム設定」をクリックします。

【手順②】

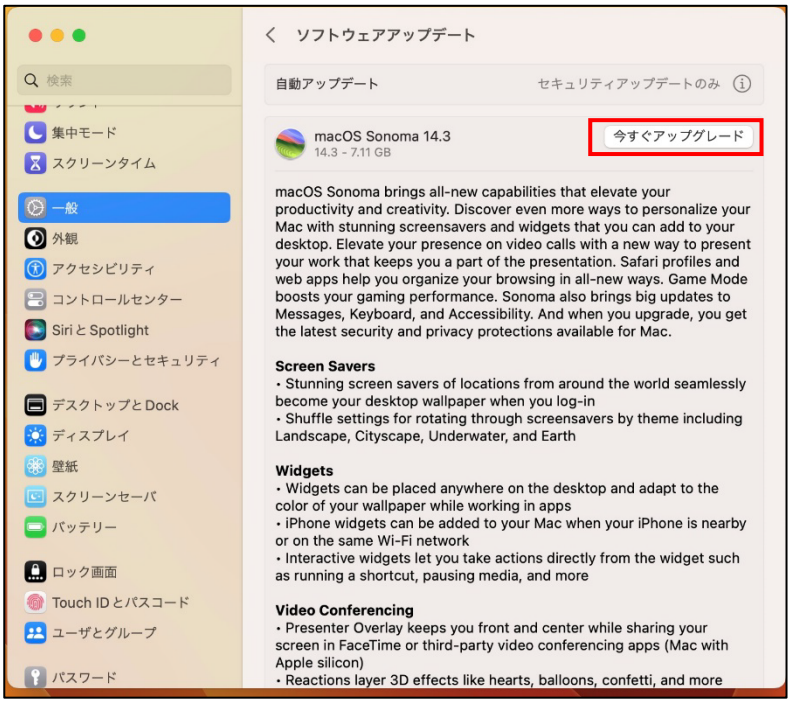
下図の画面が表示されたら「一般」をクリック後「ソフトウェア・アップデート」をクリックします。



【手順③】

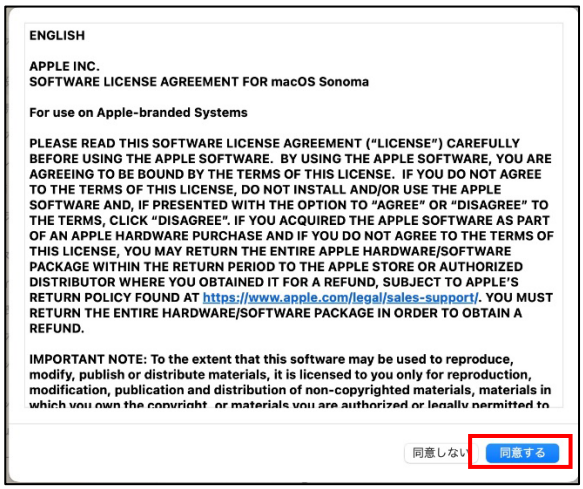
この手順と以降の手順「【手順④】」のみ、Sonoma ではなく、Ventura の画面です。Sonoma では表記や画面イメージが異なる可能性がありますが、基本的な手順は同じです。

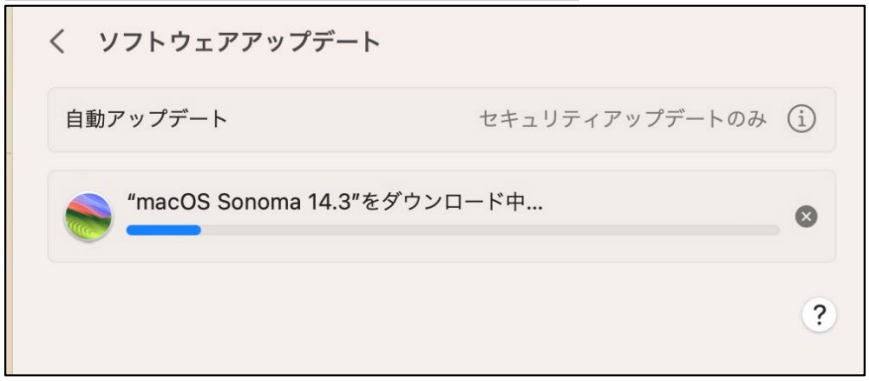
画面上部の「今すぐアップグレード」をクリックします。



【手順④】

アップデートの同意が求められるので、「同意する」をクリックすると、アップデートが開始します。





OS 自動アップデート設定

ソフトウェアを自動的に最新の状態に保つ設定を行います。

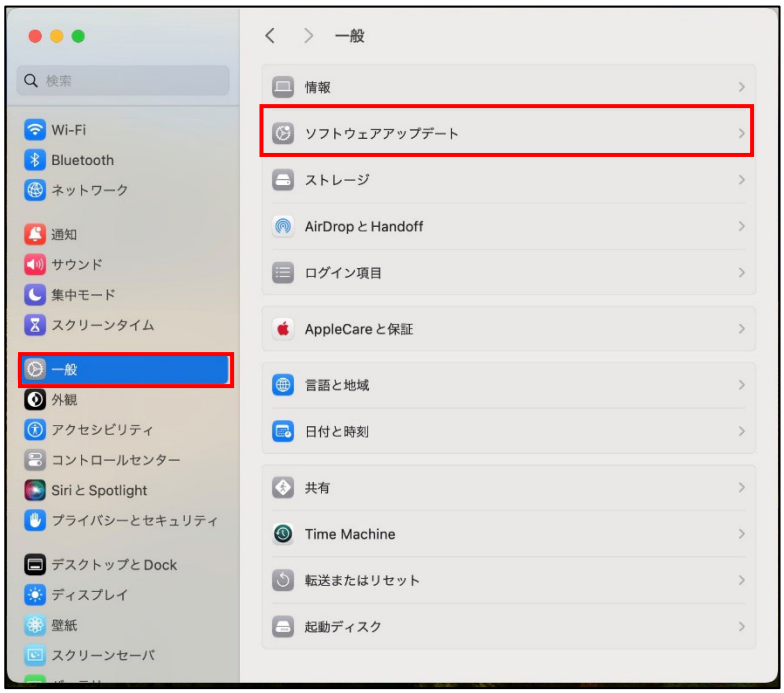
MacBook、MacBook Pro、および MacBook Air は、アップデートを自動的にダウンロードするには電源アダプタに接続されている必要があります。

【手順①】

デスクトップ左上にある Apple マークをクリック後、「システム設定」をクリックします。

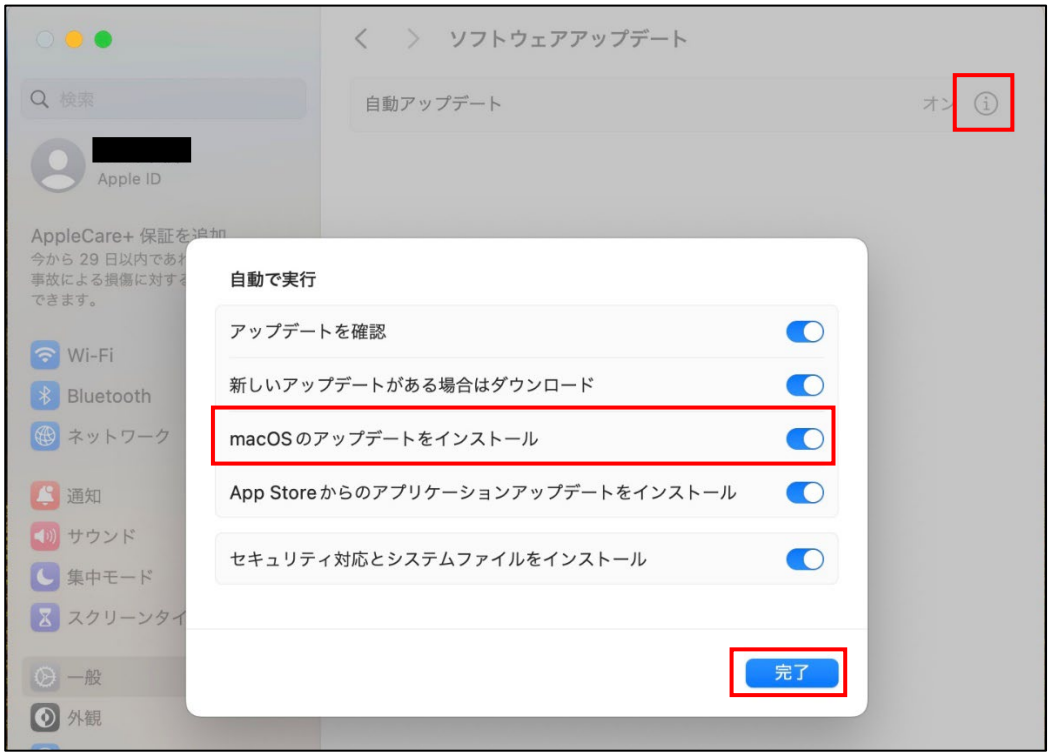
【手順②】

下図の画面が表示されたら「一般」をクリック後、「ソフトウェア・アップデート」をクリックします。



【手順③】

自動アップデートの右にあるインフォメーションボタンをクリックし、「macOS のアップデートをインストール」をオンにして、完了をクリックします。



インストールしているアプリケーションバージョンの最新化

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。

＜参考情報－Safari ブラウザの場合＞

macOS 更新時に一緒にアップデートされます。

【手順①】

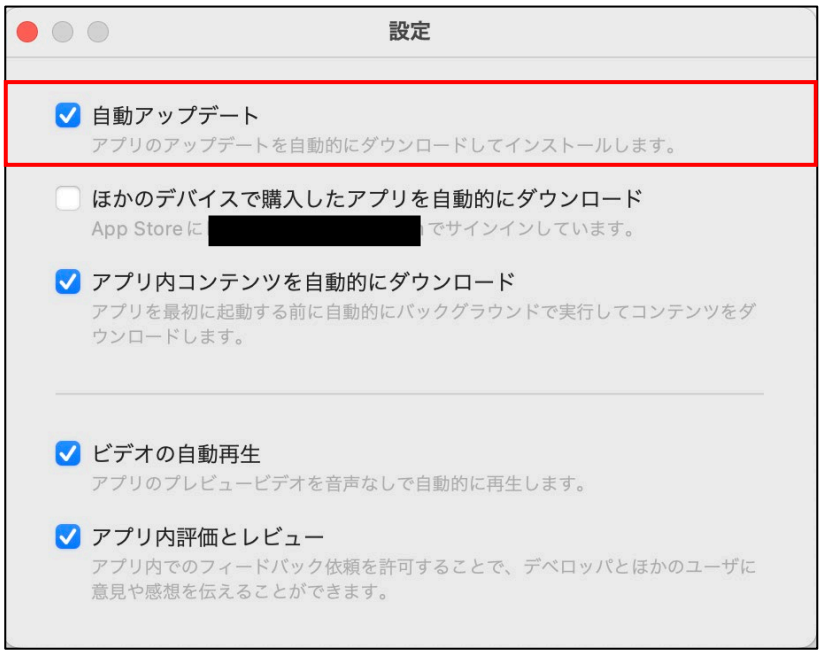
デスクトップ左上にある Apple マークをクリック後「App Store」をクリックします。

【手順②】

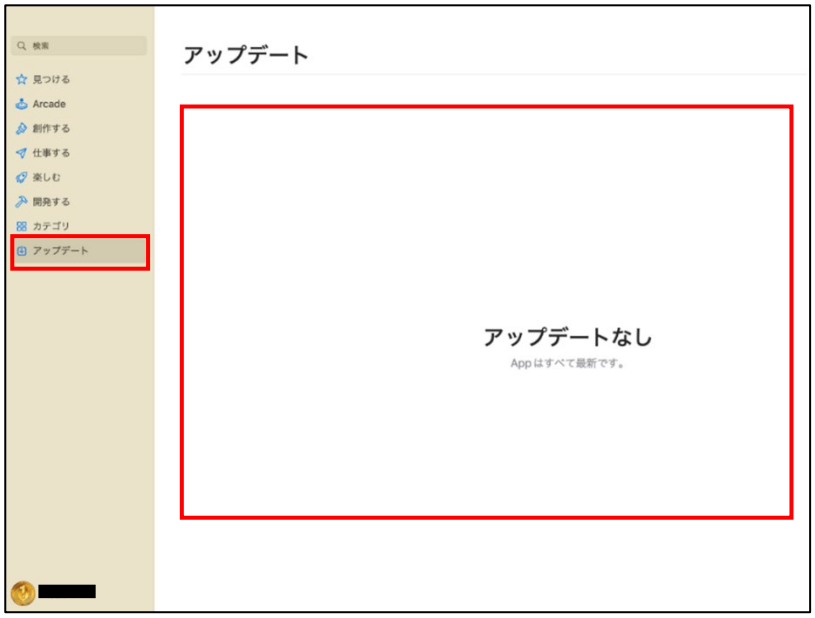
画面左上にある「Apple Store」をクリック後、「設定」をクリックします。

【手順③】

画面上部の「自動アップデート」の項目にチェックを入れます。その後、各アプリケーションのアップデートが始まります。



個々のアプリケーションの最新バージョンを確認するには下記の画面左側の「アップデート」をクリックし、任意のアプリ欄にある「さらに表示」をクリックすることで確認することが可能です。



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。
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＞
通信が暗号化されている場合、鍵のマークが表示されます。

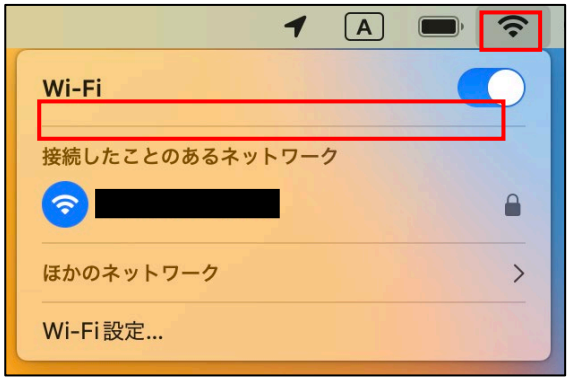
アドレスバー内を直接確認することも可能です。

4-6　チェックリスト 6-2 への対応

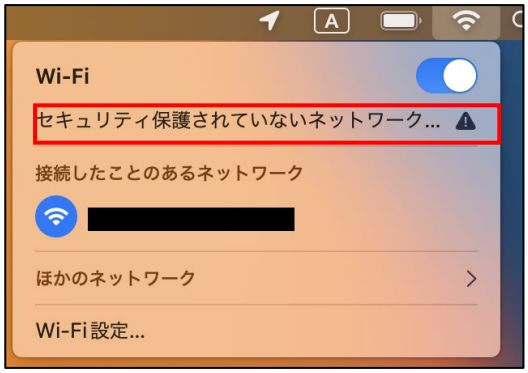
4-6-1　　無線 LAN のセキュリティ方式の確認

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。

画面右上にある「  」マークをクリックし、「Wi-Fi」の下になにも表示されていないことを確認します。
もし、**「セキュリティ保護されていないネットワーク」または「安全性の低いセキュリティ」を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。**



＜参考＞安全でない無線 LAN の場合の表示



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・盗難があった場合に備えて位置情報を検出できるように設定することを推奨します。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、**端末紛失・盗難時に端末の位置を特定できる可能性を高めることができます。**

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。

- 位置情報サービスの有効化：端末の場所を調べられるようにする機能の有効化
- Mac を探す設定の有効化：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。**

位置情報サービスの有効化

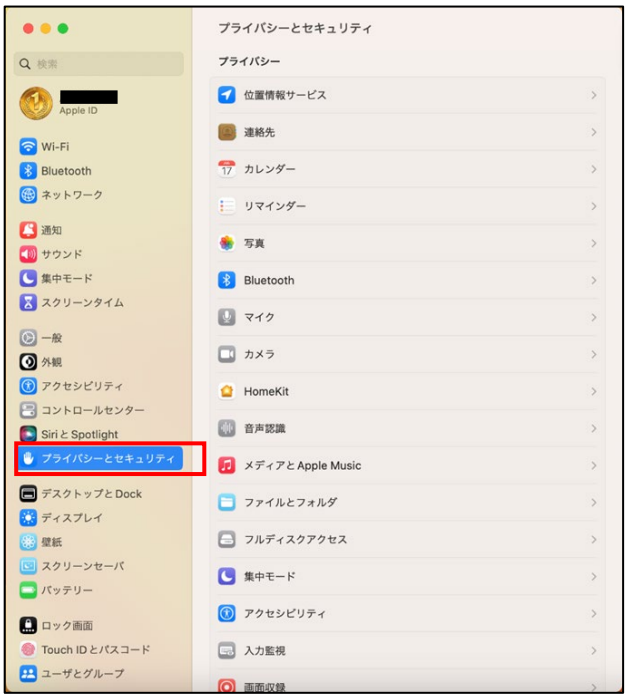
端末の位置情報サービスを有効にする設定を行います。

【手順①】

デスクトップ左上にある Apple マークをクリック後「システム設定」をクリックします。

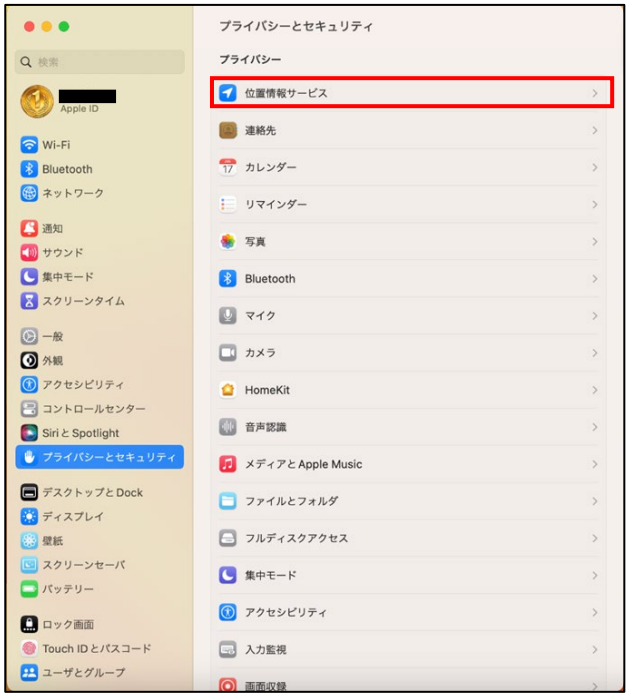
【手順②】

下図の画面から「プライバシーとセキュリティ」をクリックします。



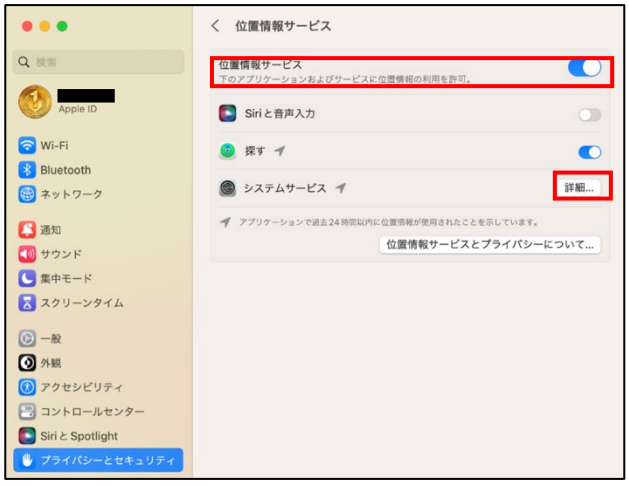
【手順③】

「位置情報サービス」をクリックします。パスワードの入力を求められた場合は、パスワードを入力してください。

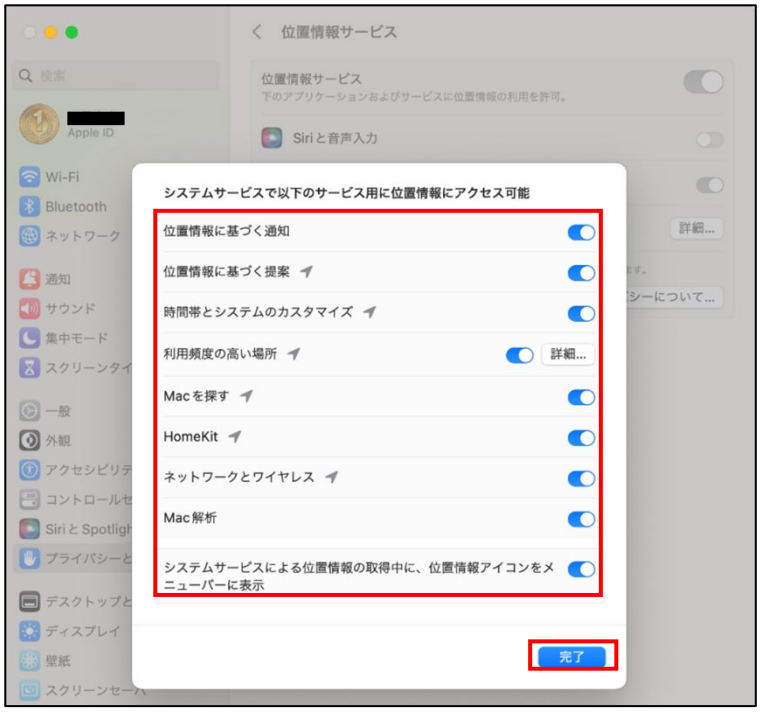


【手順④】

「位置情報サービス」をオンにし、システムサービスの「詳細」をクリックします。



下図のような項目が出てくるので、すべてチェックを入れた後「完了」をクリックします。



Mac を探す設定の有効化

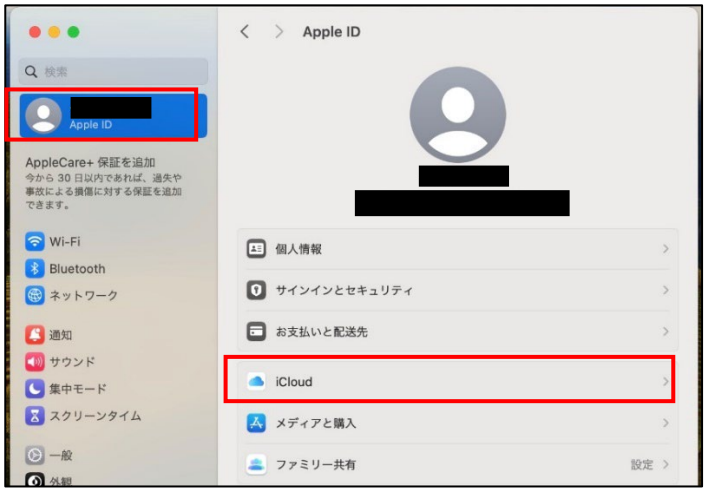
この設定を行うことで端末を紛失・盗難してしまった場合に、端末が現在どこにあるのかを検索することができます。ただし、この手順は紛失・盗難した端末が iCloud アカウントと連携していることが前提です。

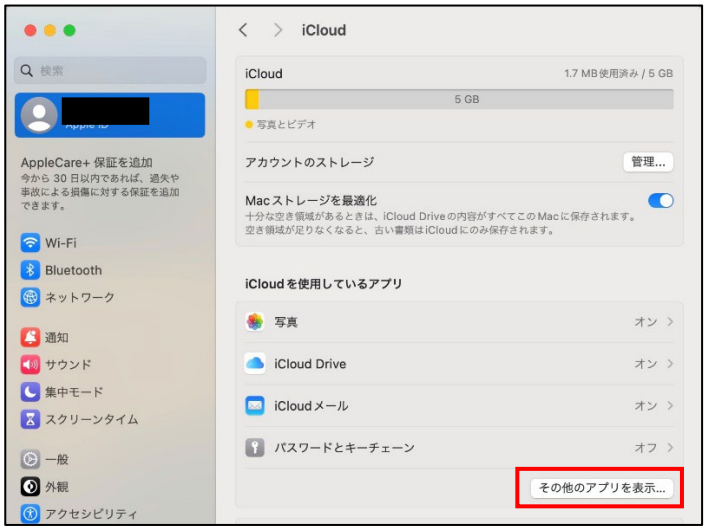
【手順①】

デスクトップ左上にある Apple マークをクリック後「システム設定」をクリックします。

【手順②】

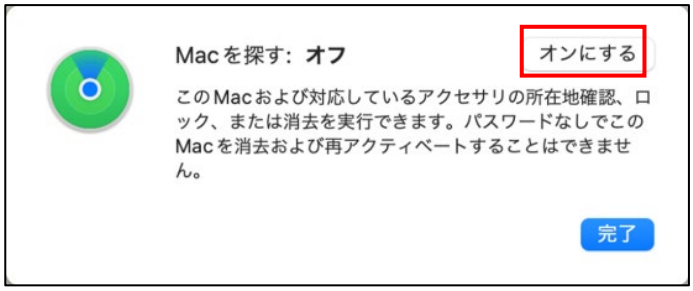
iCloud アカウントへログイン後、下図の「その他のアプリを表示」をクリックし、「Mac を探す」をクリックします。





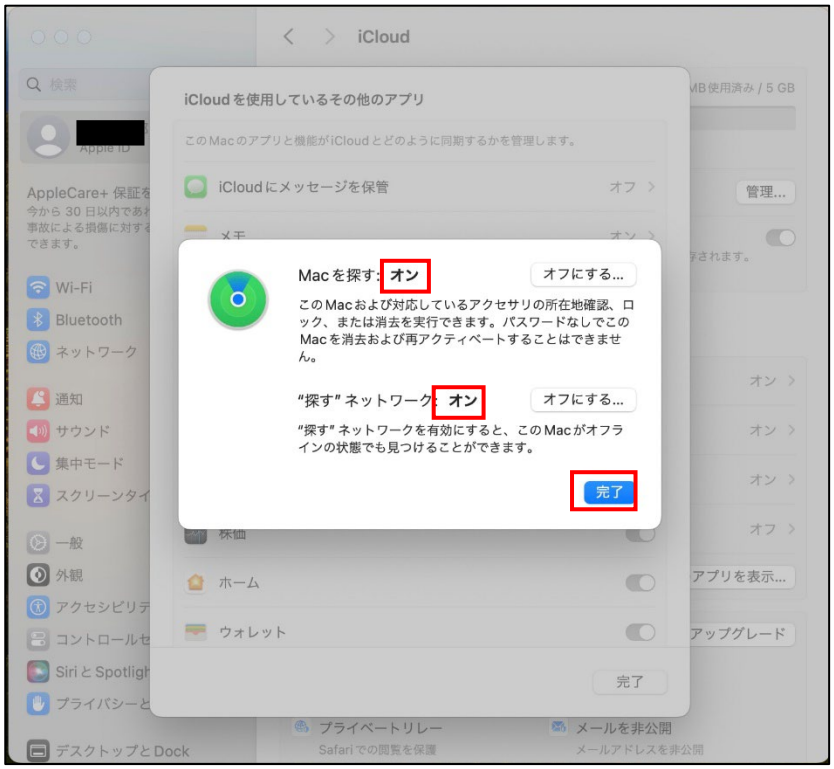
【手順③】

Mac を探すの「オンにする」をクリックすると、下図のような画面が表示されるので、「許可」をクリックします。



【手順④】

再度「Mac を探す」をクリックすると下図のように「Mac を探す」が「オン」になっていることを確認できます。



端末位置の確認方法

【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します。

https://icloud.com/find

【手順②】

アクセス後、画面上部で「すべてのデバイス」内の該当の端末名を選択します。

【手順③】

端末名をクリックすると端末の現在地が表示されます。端末の情報をクリックすると、下図の画面が表示されるのでこの画面からリモートロック等行うことも可能です。

4-8　チェックリスト 8-3 への対応

4-8-1　FileVault による暗号化設定

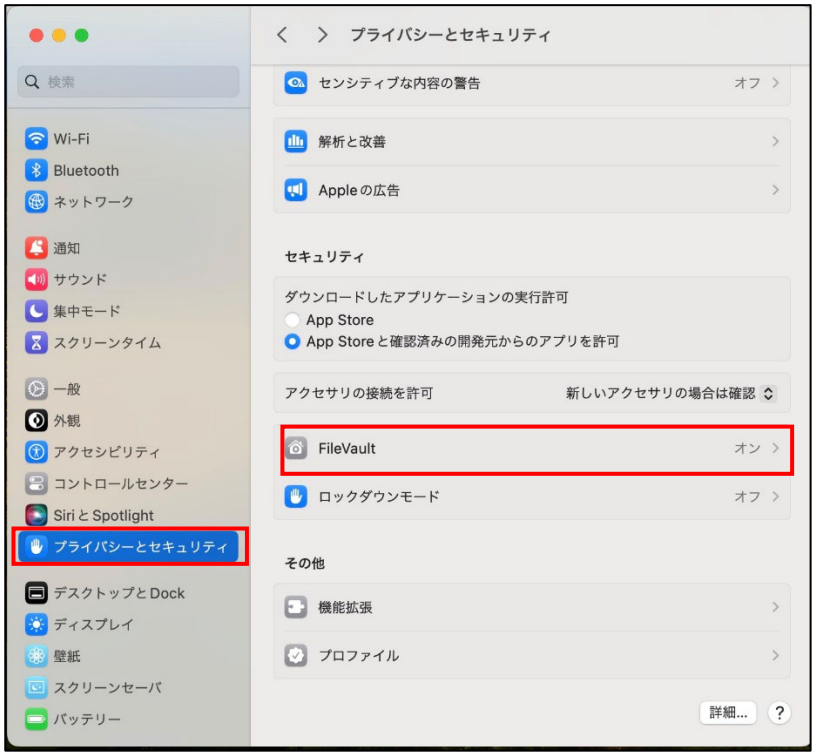
端末が、紛失・盗難によって悪意のある第三者にわたってしまった場合、端末からデータを盗まれ、悪用される恐れがあります。画面にロックがかかっている場合でも HDD を抜き出してデータが盗まれる可能性があるため、macOS に導入されている、HDD の保護を目的とした暗号化ソフトウェア「FileVault」を有効化します。**FileVault を有効にすることで HDD 内のデータを暗号化することができ、紛失時や盗難時に端末からデータを盗まれるリスクを低減することができます。**
す。

【手順①】

デスクトップ左上にある Apple マークをクリック後、「システム設定」をクリックします。

【手順②】

表示された画面から「プライバシーとセキュリティ」内の「FileVault」をクリックします。



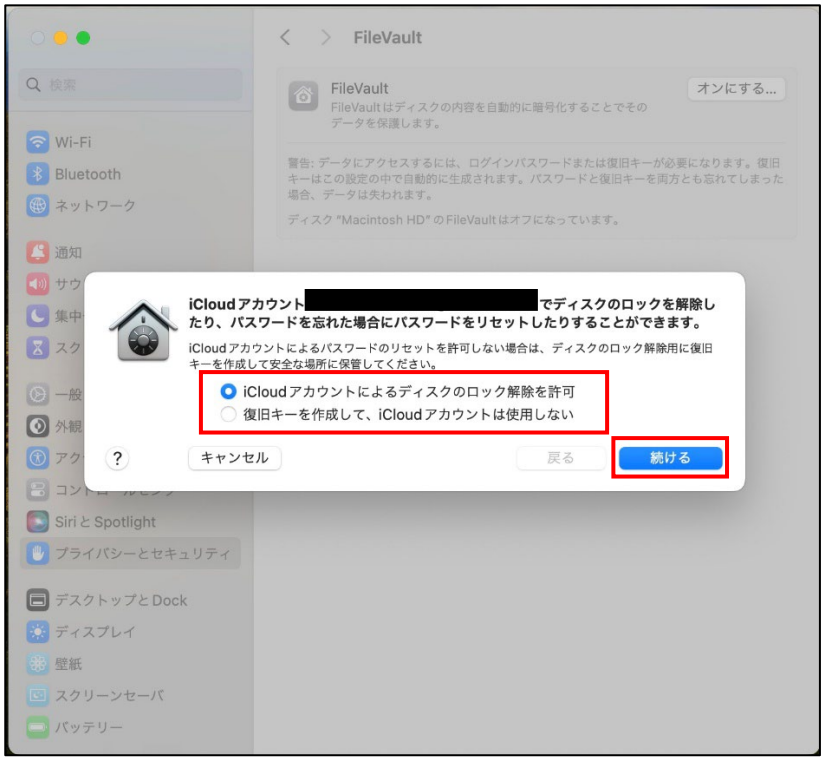
【手順③】

「FileVault」の「オンにする」をクリックします。

「ディスク"******"の File Vault はオンになっています。」と表示があれば File Vault は有効化されているので以降の手順は実施する必要はありません。

【手順④】

「iCloud アカウントによるディスクのロック解除を許可」もしくは「復旧キーを作成して、iCloud アカウントは使用しない」のどちらかを選択し「続ける」をクリックします。



【手順⑤】

「ディスク"******"の FileVault はオンになっています。」と表示があれば FileVault は有効化されています。

4-9　チェックリスト 9-2 への対応

4-9-1　　初期パスワード設定変更

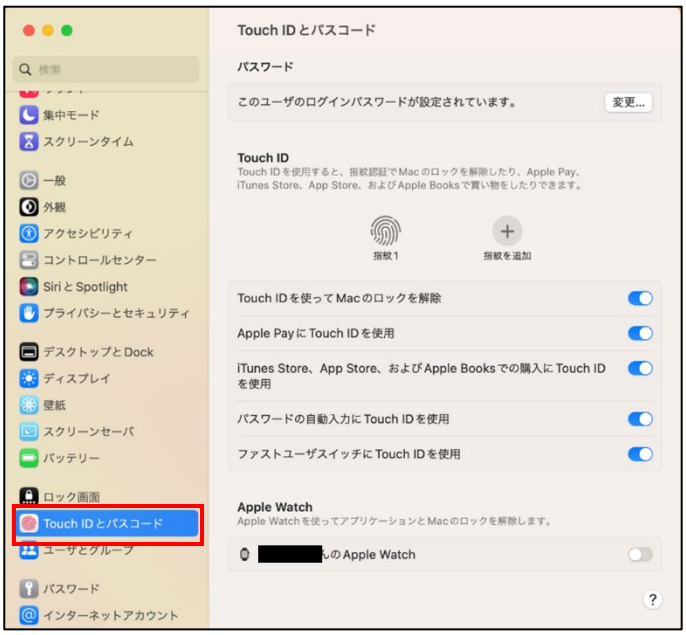
初期パスワードは、誰が把握しているかわからないので、速やかにパスワード要件を満たすものに変更することで、**悪意のある第三者から不正アクセスされるリスクを低減することができます。**

【手順①】

デスクトップ左上にある Apple マークをクリック後、「システム設定」をクリックします。

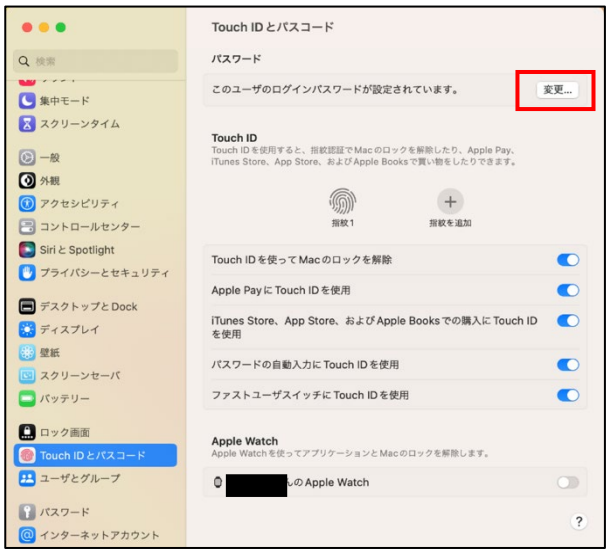
【手順②】

下図の画面が表示されたら「Touch ID とパスコード」をクリックします。



【手順③】

パスワードの「変更」をクリックします。



【手順④】

「古いパスワード」「新しいパスワード」「確認」を入力し、「パスワードを変更」をクリックします。

【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。