統合専用端末セットアップ手順書

第 2.0 版

令和５年３月６日

医療保険情報提供等実施機関

統合専用端末セットアップ手順書

目次

変更履歴

項番	版数	変更日	該当箇所	変更内容
1	1.0	2017/1/31		新規作成
2	2.0	2023/3/6		Internet Explorer サポート終了に伴う修正 Microsoft Edge 対応に関する追記 ※上記に伴う構成変更等を含む最新化
3	2.0	2023/3/6		医療扶助（福祉事務所）対応

統合専用端末セットアップ手順書

1．はじめに

1.1 本書の目的

（1）「統合専用端末セットアップ手順書」（以下「本書」という。）は、医療保険者、後期高齢者医療広域連合および、福祉事務所（以下、医療保険者等）において、医療保険者等向け中間サーバー等（以下、中間サーバー）へ接続するための統合専用端末のセットアップを行うための手順を示す。医療保険者等の環境において画面イメージが異なる、または、より強固なセキュリティポリシーがある場合は、それぞれ読み替えて作業を行うこと。

（2）セットアップ作業についてはWindows OSの基礎知識、および基本的な操作経験を有する者が行うことを前提として記述する。

1.2 利用環境

統合専用端末の OS および ブラウザーは以下とする。（医療保険者は令和 5 年 6 月以降、福祉事務所は令和 5 年 4 月以降）

（1）OS　　：Windows10 Pro または Windows11 Pro（各バージョンともに Home Edition は不可）

（2）ブラウザー：Microsoft Edge（Internet Explorer、Chrome 等は動作保証外）

1.3 設定単位

次章以降で説明する設定単位については以下の通り。

統合専用端末に Windows ログインユーザーアカウントを複数設定する場合、ログインユーザー単位の設定が必要になるものがあることに注意すること。 特に電子証明書はログインユーザー単位のインストールが必要ため、注意すること。

章節	章節名	設定単位
2	ホスト名（PC 名）の設定	端末単位
3	電子証明書の設定	ログインユーザー単位
4	ブラウザーの設定	ログインユーザー単位
5.1	不正プログラム対策	端末単位
5.2	証跡管理	端末単位
5.3	論理アクセス制限	端末単位
5.4	権限管理	端末単位
5.5	セキュリティーホール対策	端末単位
5.6	情報システムの利用制限	ログインユーザー単位
5.7	機器の要塞化	端末単位
5.8	信頼済みサイトの登録	端末単位
5.9	ポップアップブロックの設定	端末単位
6.1	全国国民保険協会、健康保険組合、福祉事務所における設定	端末単位
7.1	国民健康保険組合、後期高齢者医療広域連合における設定	端末単位

※　端末単位の設定は、Administrator ユーザー（管理者権限）のみ設定可能。

2．ホスト名（PC 名）の設定

統合専用端末のホスト名は、以下の命名規則に則り、重複しないように設定すること。

＜命名規則＞

保険者コード(半角英数字 8 桁)＋”-”(半角ハイフン 1 桁)＋※連番(半角数字 2 桁)

※統合専用端末を複数台設置する医療保険者等については 01 から昇順に振ること。

【例】A0000001-01

保険者コード　連番

① スタートメニューから「設定」をクリックする。

② 「システム」をクリックする。

③ 「バージョン情報」をクリックする。

④ 「PC 名の変更」をクリックする。

⑤ 命名規則に則り PC 名を入力し、「次へ」ボタンをクリックする。

⑥ 「今すぐ再起動をする」をクリックする。

3．電子証明書の設定

（１）電子証明書の設定手順については、「オンライン請求ネットワーク関連システム共通認証局ユーザーマニュアル」を参照すること。電子証明書のインストールは、必ずWindowsのログインユーザー毎に行うこと。

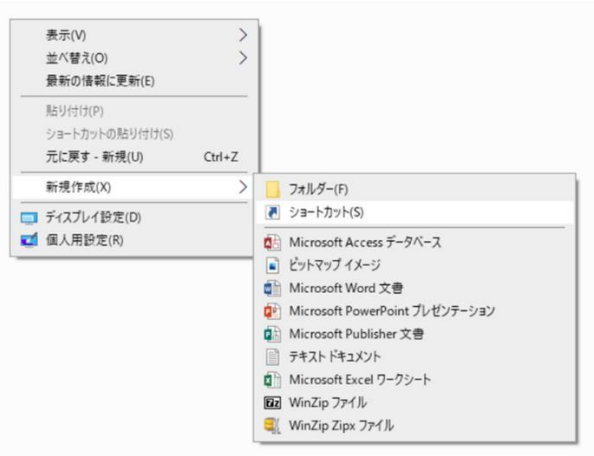
（２）電子証明書の設定は「6.ネットワークに係る設定」後に行うこと。

４．ブラウザーに係る設定

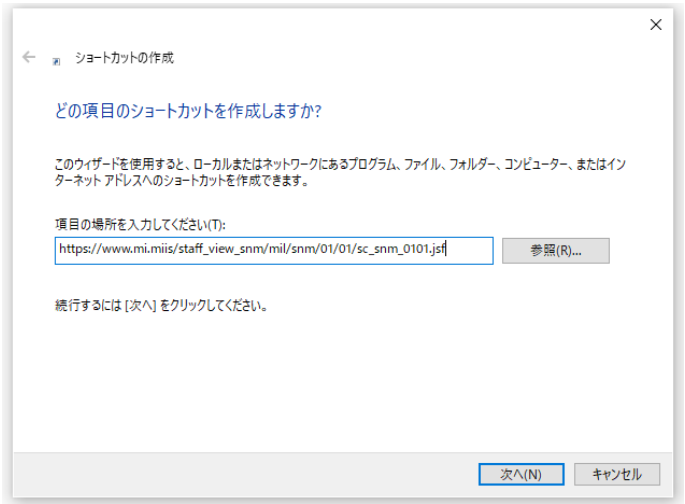
4.1 ショートカット アイコンの作成

デスクトップ上に本番環境、接続検証環境それぞれに接続可能な業務担当者、システム担当者のショートカットアイコンを設定する。

（１）デスクトップ上の何もないところで右クリックし、「新規作成」から「ショートカット(S)」を選択する



（２）「項目の場所を入力してください（T）」欄へ以下の該当する表から、業務担当者の URL またはシステム管理者の URL を入力し、「次へ」をクリックする。



＜医療保険者、後期高齢者医療広域連合　本番環境＞

利用者区分	URL＜本番環境＞
業務担当者	https://www.mi.miis/staff_view_snm/mil/snm/01/01/sc_snm_0101.jsf
システム管理者	https://www.mi.miis/system_view_snm/mil/snm/01/02/sc_snm_0102.jsf

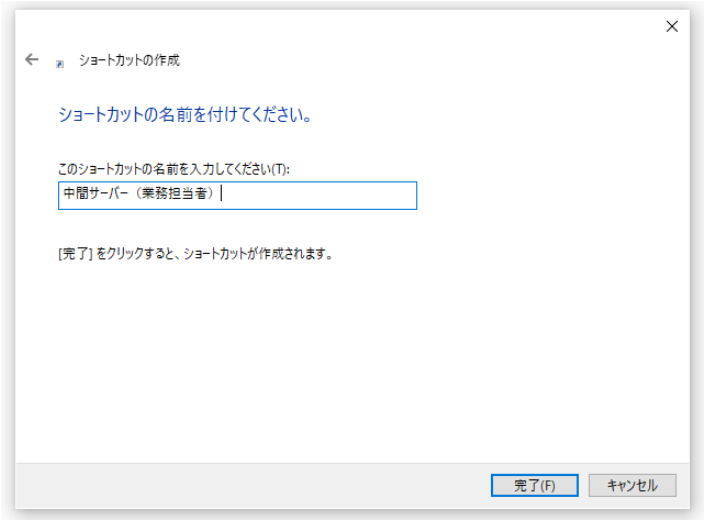
＜福祉事務所　本番環境＞ ※福祉事務所専用

利用者区分	URL＜本番環境＞
業務担当者	https://www.mi.miis/staff_view_fnm/mil/fnm/01/01/sc_fnm_0101.jsf
システム管理者	https://www.mi.miis/system_view_fnm/mil/fnm/01/02/sc_fnm_0102.jsf

（３）ショートカットの名前を入力してください(T)」欄へ任意の名前を入力し、完了を押下する。

例：業務担当者　　：中間サーバー（業務担当者）

システム管理者：中間サーバー（システム管理者）



（４）デスクトップ上に作成したアイコンが作成されていることを確認する

【参考】接続検証環境への接続用 URL

接続検証環境は本番環境ではできない運用保守事業者によるテストや、医療保険者等でのテストに利用することができる。ただし、原則利用申請が必要であり、システムメンテナンス等で閉局日となることがある。

＜医療保険者、後期高齢者医療広域連合　接続検証環境＞

利用者区分	URL＜接続検証環境境＞
業務担当者	https://www.mi-st.miis/staff_view_snm/mil/snm/01/01/sc_snm_0101.jsf
システム管理者	https://www.mi-st.miis/system_view_snm/mil/snm/01/02/sc_snm_0102.jsf

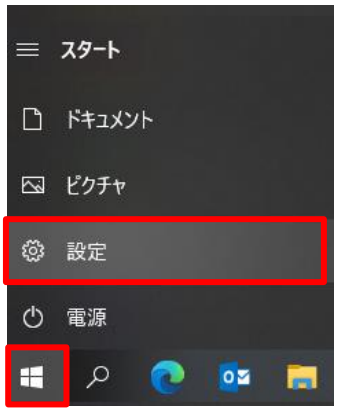
＜福祉事務所　接続検証環境＞ ※福祉事務所専用

利用者区分	URL＜接続検証環境境＞
業務担当者	https://www.mi-st.miis/staff_view_fnm/mil/fnm/01/01/sc_fnm_0101.jsf
システム管理者	https://www.mi-st.miis/system_view_fnm/mil/fnm/01/02/sc_fnm_0102.jsf

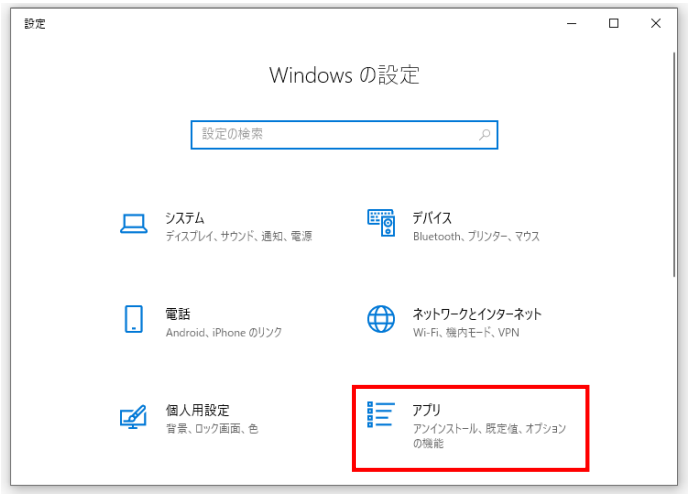
4.2 標準ブラウザーの設定

Microsoft Edgeを標準ブラウザーとして設定する方法について記載する。

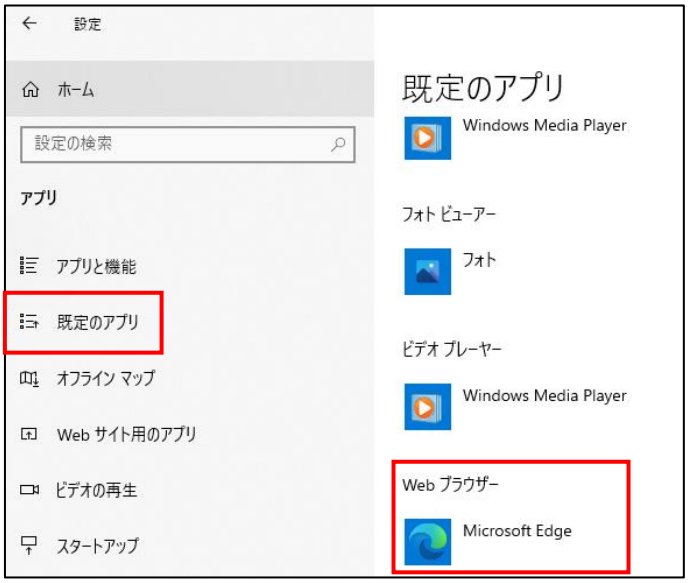
（１）スタートボタンを押下し、スタートメニューから「設定」をクリックする。



（２）「アプリ」をクリックする。



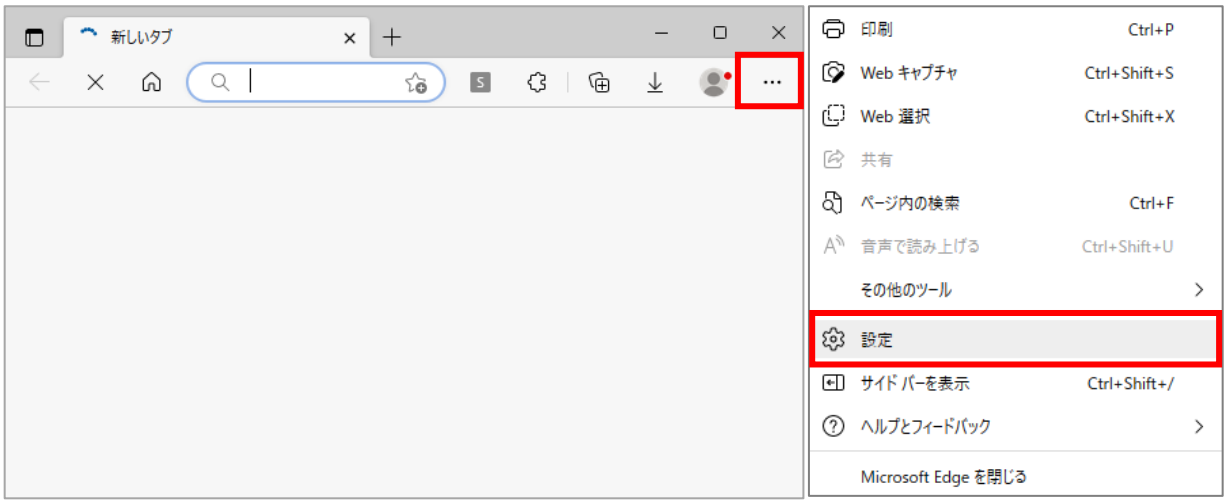
（３）「既定のアプリ」を選択し、Web ブラウザーに「Microsoft Edge」を選択する。



4.3 ブラウザーの設定

（1）Microsoft Edge の設定内容

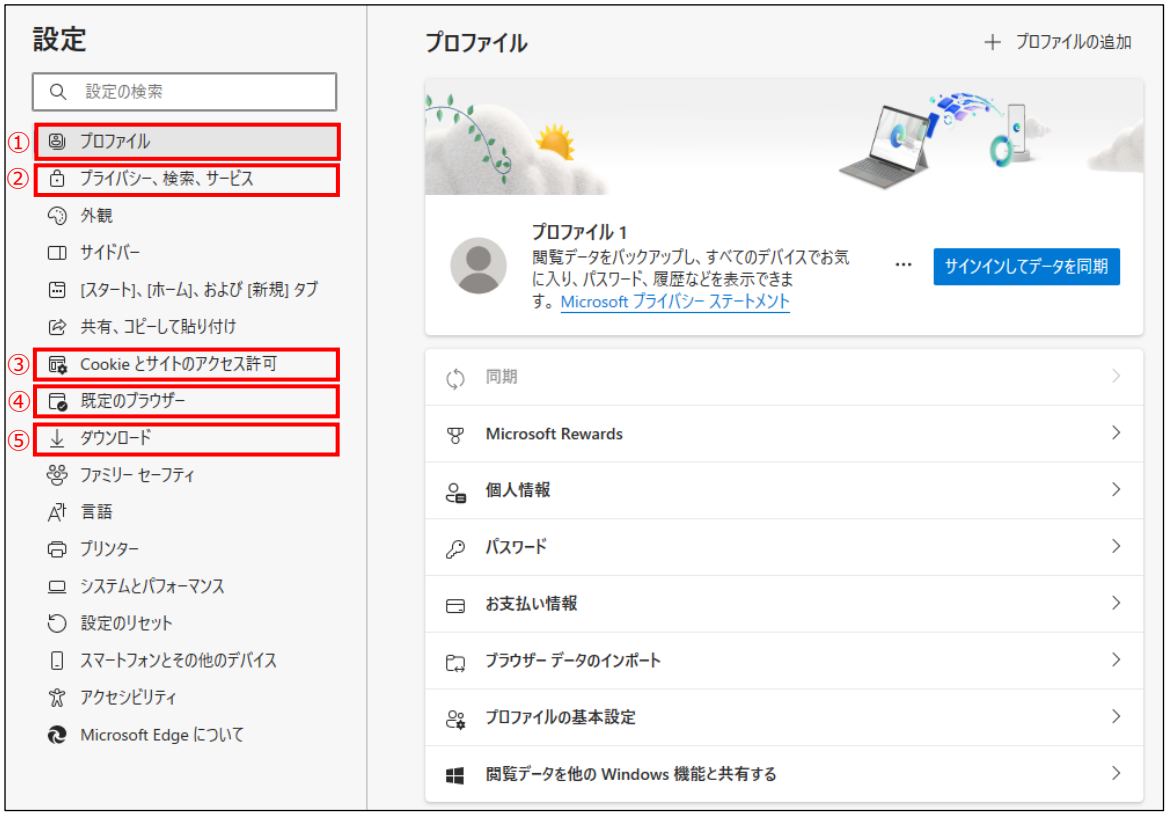
Microsoft Edge の「・・・」をクリックし設定を選択する。



＜Microsoft Edge の設定画面＞

以下の 5 項目の設定を行う。（特に指定のない設定値は初期設定のままとする）

5 項目以外は医療保険者等のポリシー等に従って任意に設定すること。



①プロファイルの設定

＜個人情報＞

・基本情報の保存と入力：OFF

・基本情報：何も設定しない

・ユーザー設定情報を保存して入力する：OFF

＜パスワード＞

・パスワードの保存を提案：OFF

・パスワードを自動的に保存する：OFF

・パスワードのオートフィル：OFF

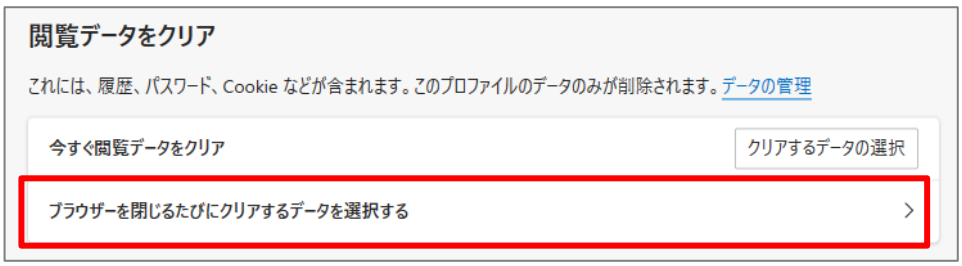
②プライバシー、検索、サービスの設定

トラッキングの防止：ON

追跡防止：基本

＜「閲覧データをクリア」の設定＞

「ブラウザーを閉じるためにクリアするデータを選択する」をクリックする



・閲覧の履歴：ON

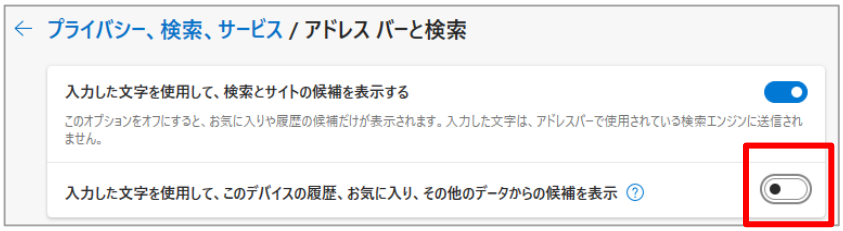
・ダウンロードの履歴：ON

・キャッシュされた画像とファイル：ON

＜サービスの設定＞

「アドレスバーと検索」をクリックする。

入力した文字を使用して、このデバイス上の履歴、お気に入り、その他のデータからの提案を表示：OFF



③Cookie とサイトのアクセス許可

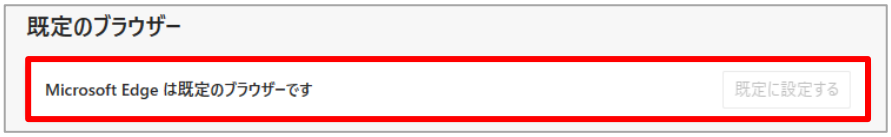
「JavaScript」をクリックする

・許可（推奨）：ON

④既定のブラウザー

規定のブラウザーが Microsoft Edge になっていることを確認する。

（「4.2 標準ブラウザーの設定」で設定済みであることの確認）



⑤ダウンロード

ダウンロードの動作を毎回確認する：ON

5．セキュリティ対策に係る設定

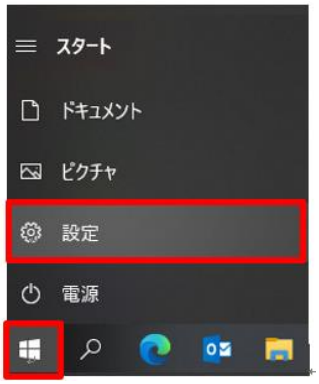
「統合専用端末の端末仕様等について」で示されている技術的対策を行う上での設定手順を記載する。
本章において、推奨設定例を示しているが、各医療保険者等のセキュリティポリシー等を踏まえ、設定内容を検討いただきたい。他のアンチウィルスソフトウェアや改ざん検知の仕組みを導入する必要がある場合は、医療保険者等の責任において導入すること。

5.1 不正プログラム対策

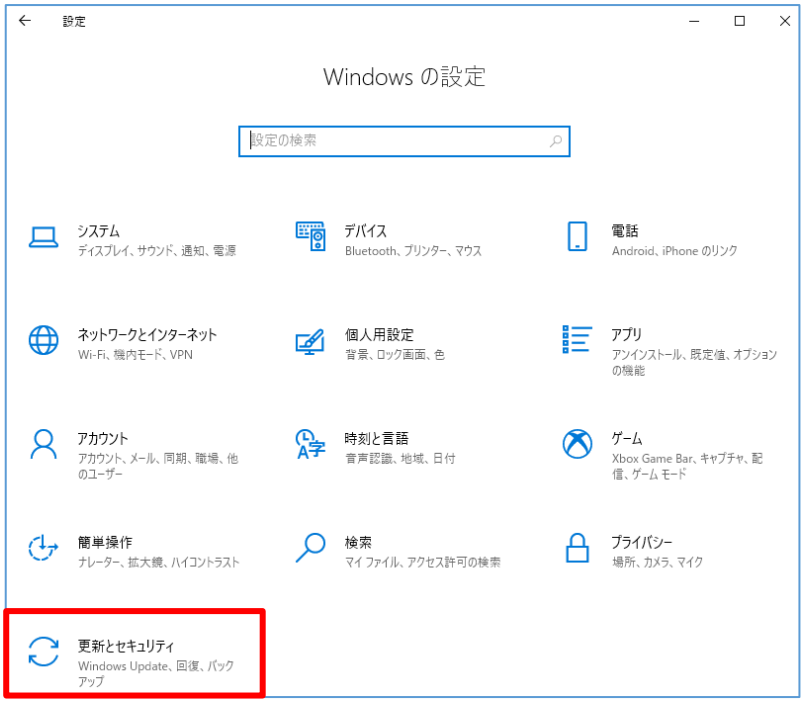
ウイルス対策ソフトウェア（Windows セキュリティ）を有効化し、リアルタイムスキャンを実施するための設定手順について記載する。

（１）セキュリティ保護状態の確認

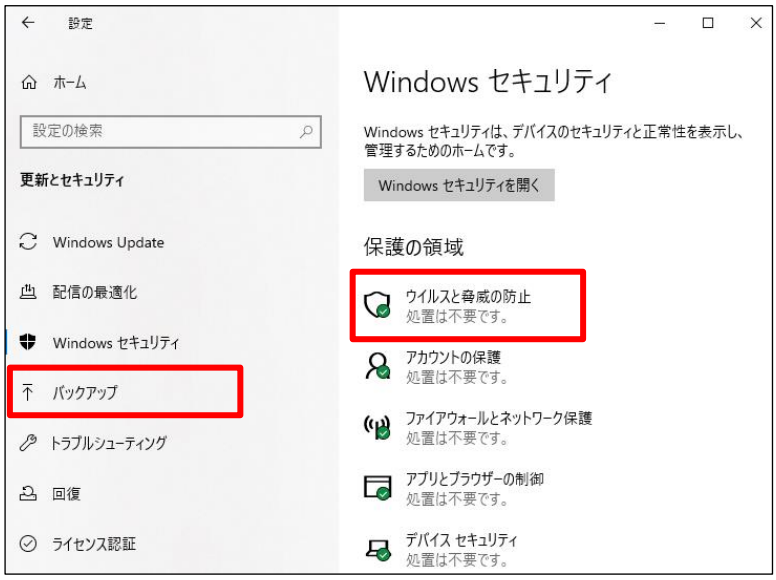
①スタートボタンを押下し、スタートメニューから「設定」をクリックする。



②「更新とセキュリティ」をクリックする。



③「Windows セキュリティ」タブから「ウイルスと驚異の防止」をクリックする。



④「ウイルスと脅威の防止の設定」にある「設定の管理」をクリックする。

（すでにアンチウィルスソフトウェアを導入済みの場合は表示が異なります）

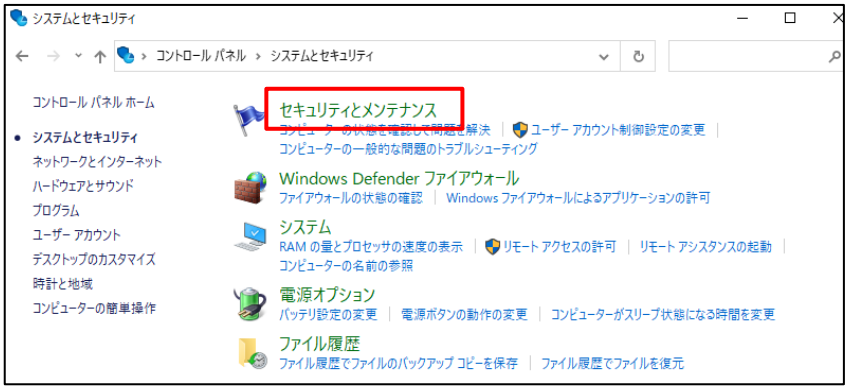
⑤「リアルタイム保護」にあるスイッチボタンをクリックし「オン」にする。

（２）定期的なフルスキャンの実施

医療保険者等のポリシーにより別のアンチウィルスソフトウェアを利用している場合は、その設定に準じること。

①スタートメニューを右クリックし「コントロールパネル」を表示する（以下、コントロールパネルの表示方法は割愛する）
「システムとセキュリティ」をクリックする。

②「セキュリティとメンテナンス」をクリックする。



③「メンテナンス」タブから「メンテナンス設定の変更」をクリックする。

④「メンテナンスタスクの実行時刻」についてはフルスキャンを実行可能な時刻を設定し、

「OK」ボタンをクリックする。 例では 12:00 にしている。

（３）定期的な最新パターンファイルの適用

医療保険者等のポリシーに沿って、原則として常に最新の定義ファイルを適用すること。

＜参考＞Windows セキュリティ の場合

①インターネットに接続されている端末より、以下サイトにアクセスし、Windows Defender 定義ファイル（Windows11,Windows10 用）の最新版（64bit）をダウンロードする。

https://www.microsoft.com/en-us/wdsi/defenderupdates

Antimalware solution	Definition version
Microsoft Defender Antivirus for Windows 11, Windows 10, Windows 8.1, and Windows Server	32-bit | 64-bit | ARM
Microsoft Security Essentials	32-bit | 64-bit
Windows Defender in Windows 7 and Windows Vista	32-bit | 64-bit
Microsoft Diagnostics and Recovery Toolset (DaRT)	32-bit | 64-bit
System Center 2012 Configuration Manager	32-bit | 64-bit
System Center 2012 Endpoint Protection	32-bit | 64-bit
Windows Intune	32-bit | 64-bit

②①にてダウンロードした実行ファイル（例：mpam-fe.exe）を USB メモリ等の媒体に格納する。

当該 USB メモリ等をインターネットに接続されている端末に接続する際、USB メモリに対して使用する前後に必ずウイルススキャンを実施すること。

③USB メモリ等から Windows Defender 定義ファイルを統合専用端末のデスクトップ等の任意の場所に移した後、実行してパターンファイルを適用（※）する。

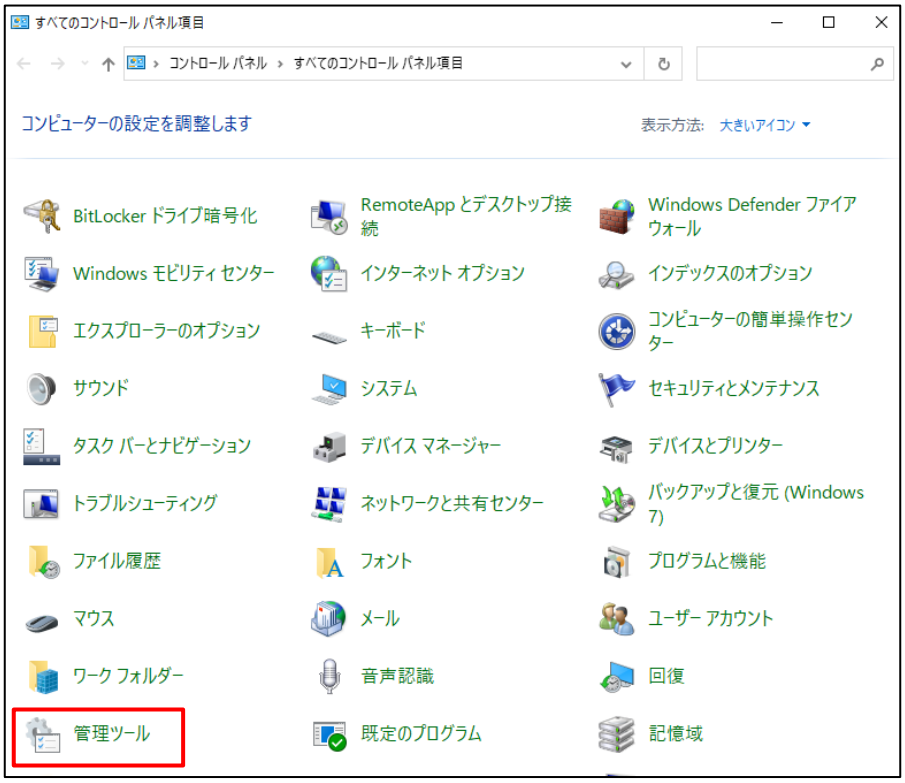
※ 最新のパターンファイルを適用しない場合、統合専用端末の脆弱性が高まるため、定期的に適用すること。

5.2 証跡管理

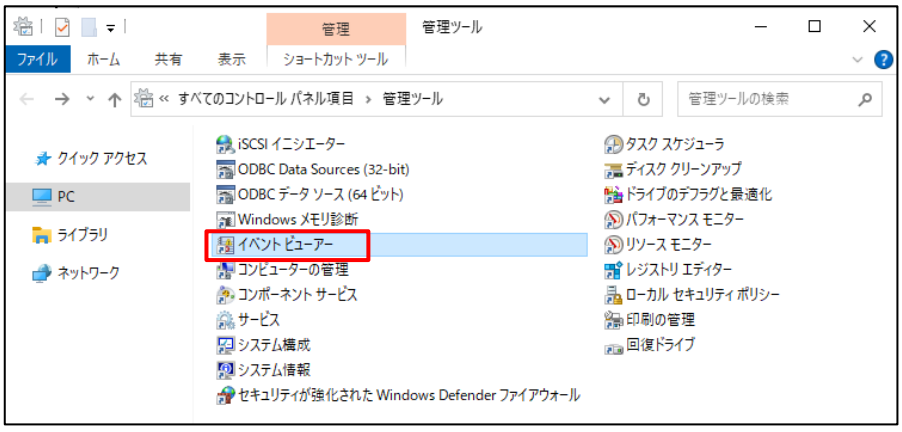
Windows の標準機能を利用し、端末の利用履歴等を記録した監査ログを取得するための設定手順について記載する。また、監査ログに正確な時刻が記録されるよう、OS の時刻を標準時刻に同期するための設定手順についても記載する。

（１）監査ログの取得設定

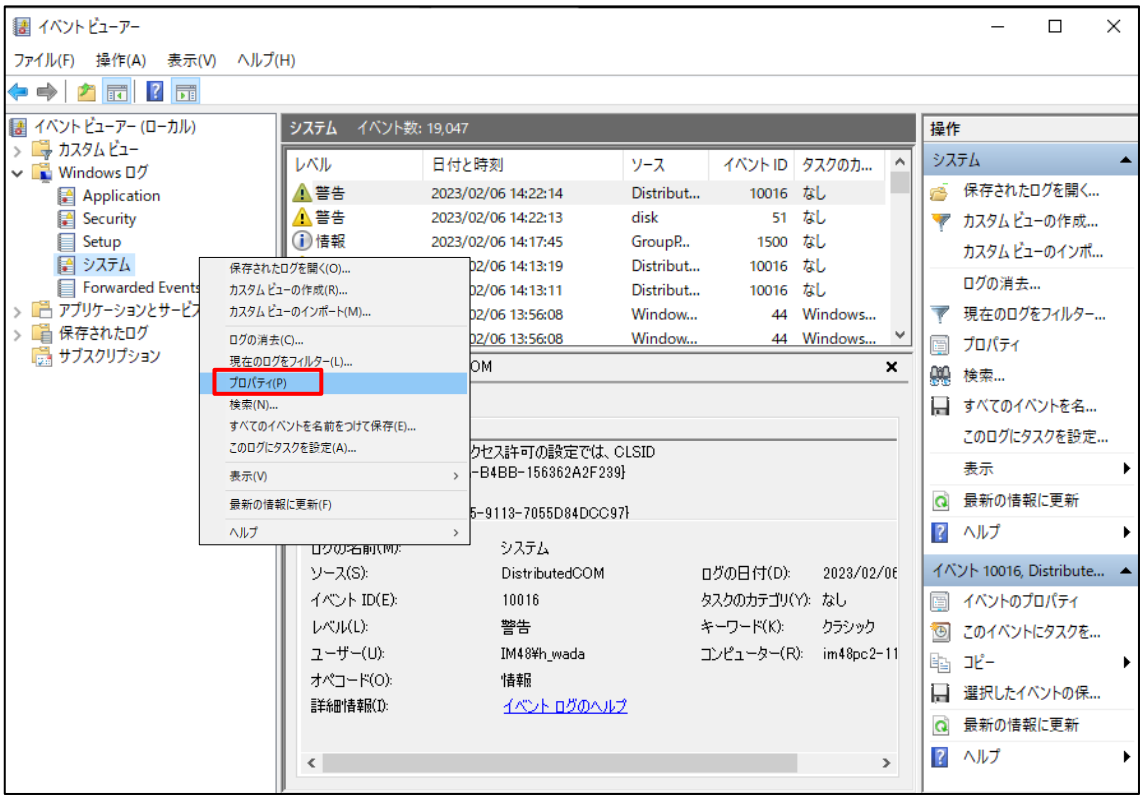
①コントロールパネルから「管理ツール」をクリックする



②「イベントビューアー」をクリックする。

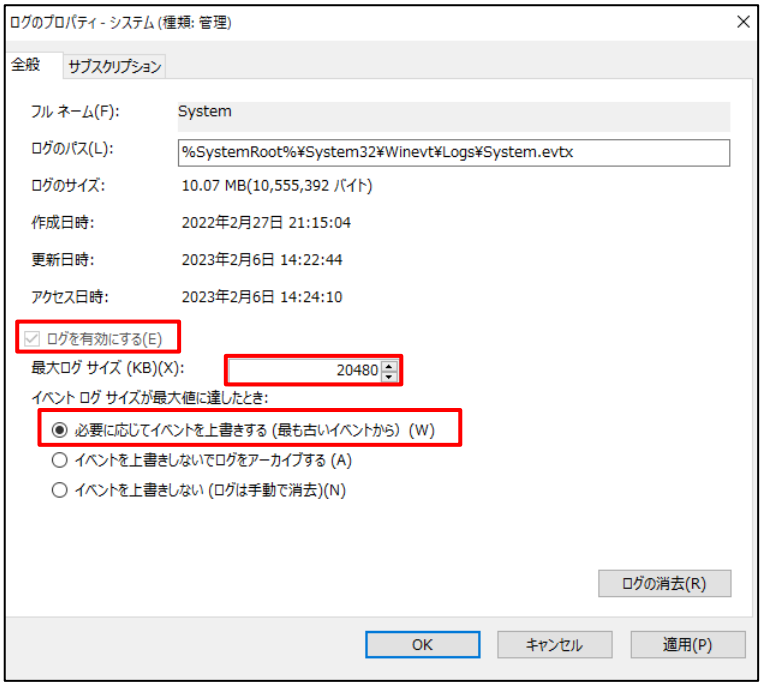


③「Windows ログ」-「システム」を開き、右クリックで「プロパティ」を選択する。



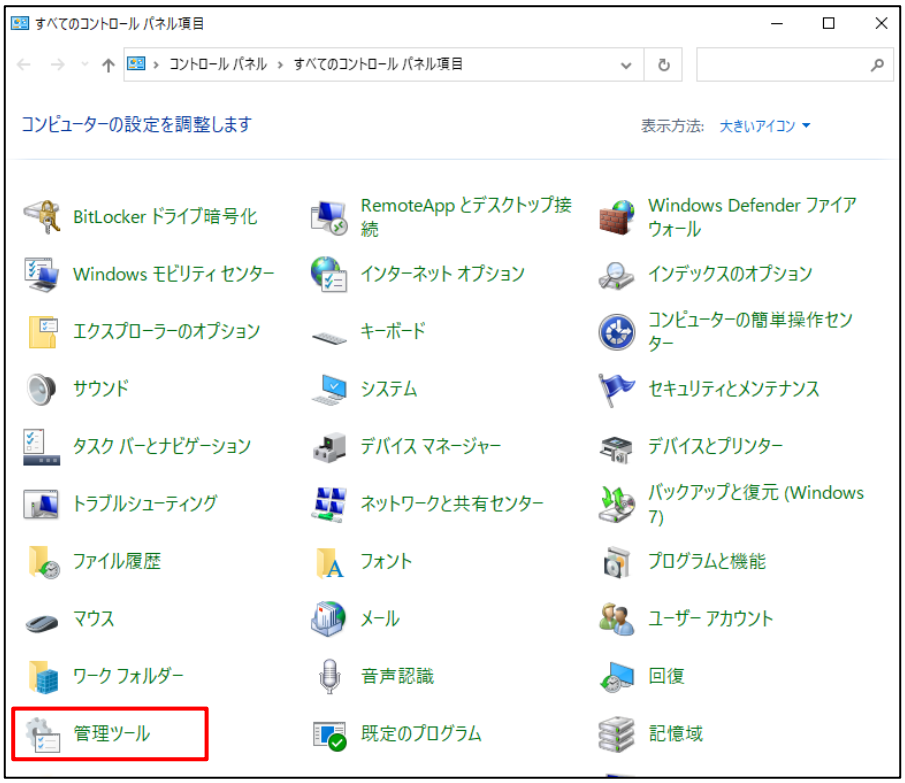
④各種設定を行う。

- 「ログを有効にする」：チェック☑が入っていることを確認する。
- 「最大ログサイズ」：20480
- 「イベントログサイズが最大値に達したとき」：必要に応じてイベントを上書きする（最も古いイベントから）（W）を選択する。

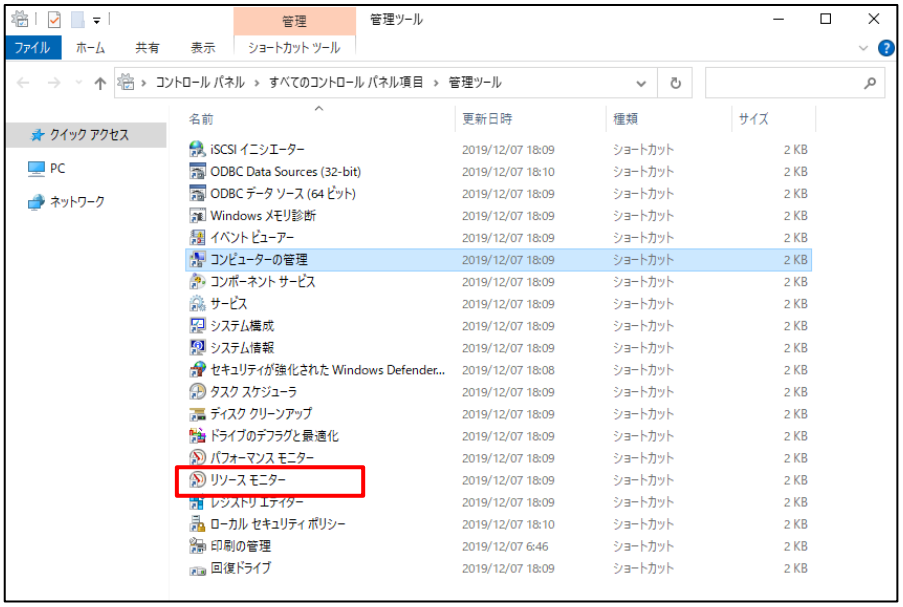


（２）端末へのログイン/ログアウトの監視設定

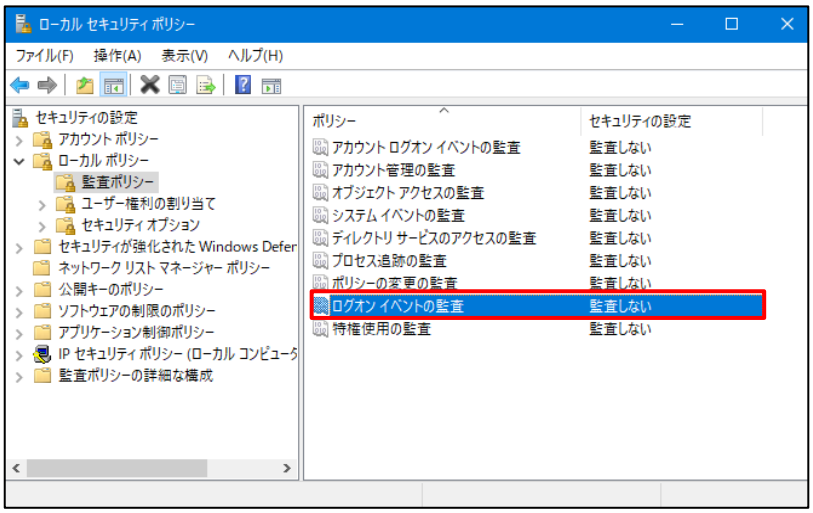
①コントロールパネルから「管理ツール」をクリックする



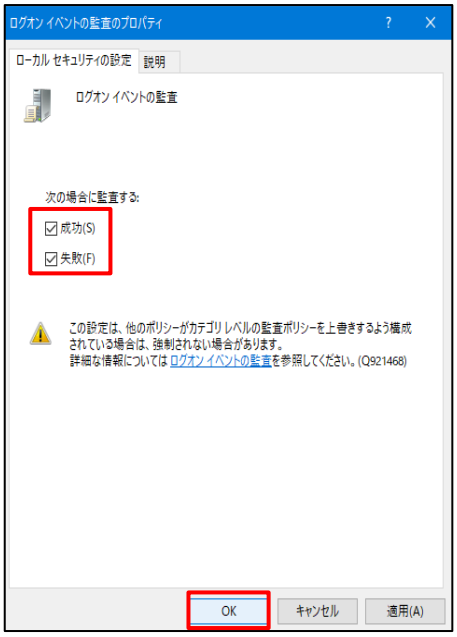
②「リソースモニター」を開く。



③「監査ポリシー」-「ログオンイベントの監査」を開く。



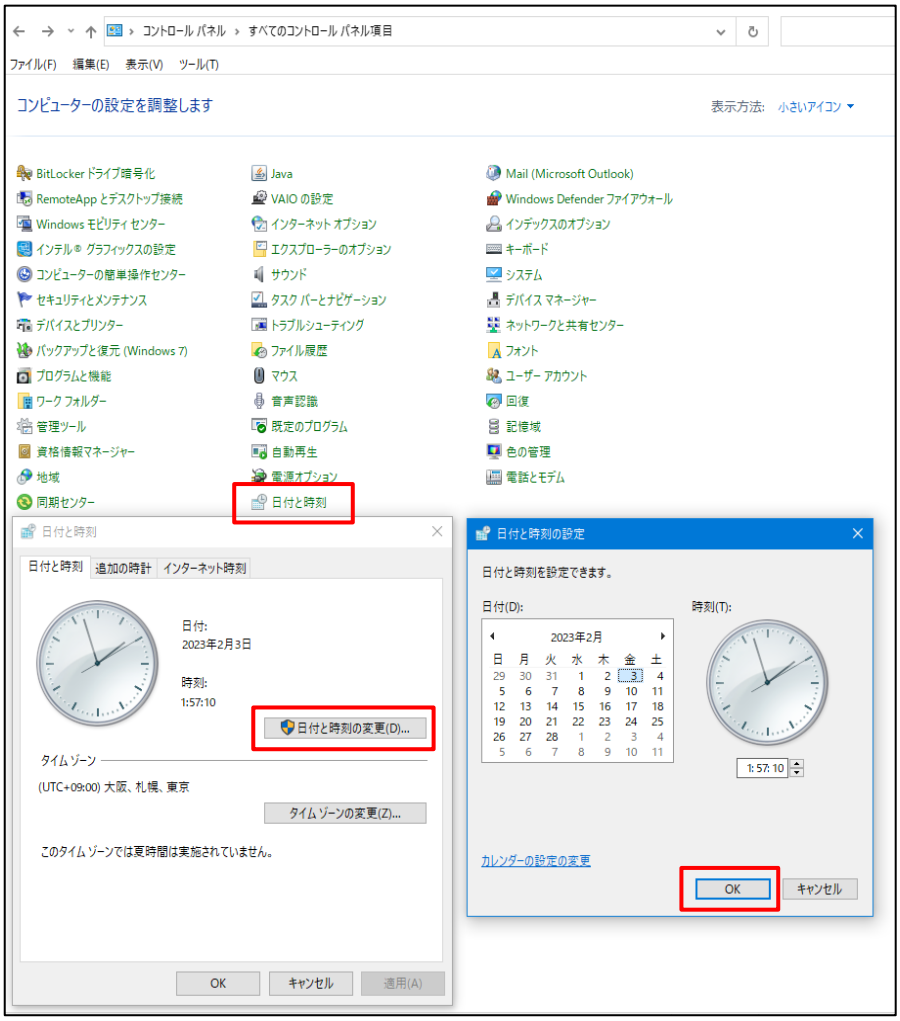
④監査の対象として「成功」「失敗」項目にチェックを入れ、「OK」ボタンをクリックする。



（３）時刻設定

①コントロールパネルから「日付と時刻」を選択し、「日付と時刻の変更」を選択して

現在の日付と時刻を入力し、「OK」ボタンをクリックする。



＜参考＞

正確な時刻を調べる方法

●ラジオ、テレビの時報

●インターネット：日本標準時（http://www.nict.go.jp/JST/JST5.html）

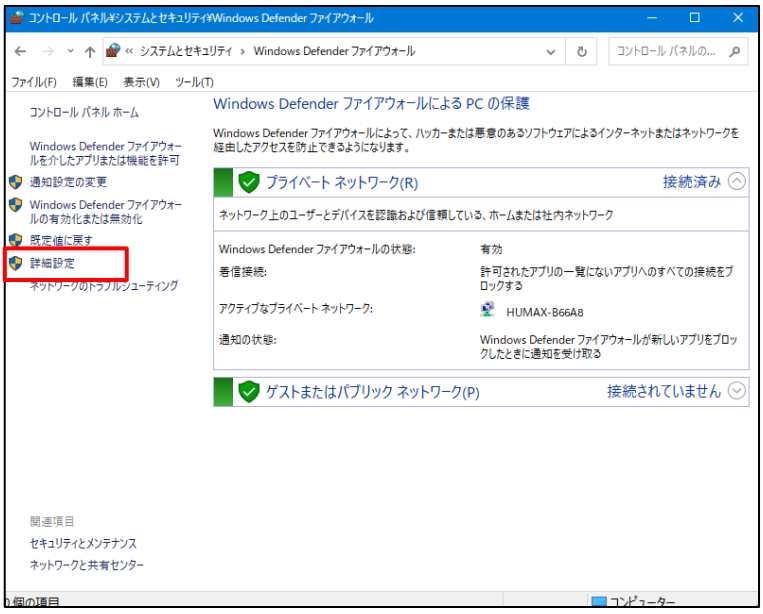
5.3 論理的アクセス制限

アクセス制限を実施するため、端末のファイアウォール機能の設定手順及び電子データへのアクセス制御の設定手順について記載する。医療保険者等において独自のファイアウォールを使用している場合、その設定に準拠すること。

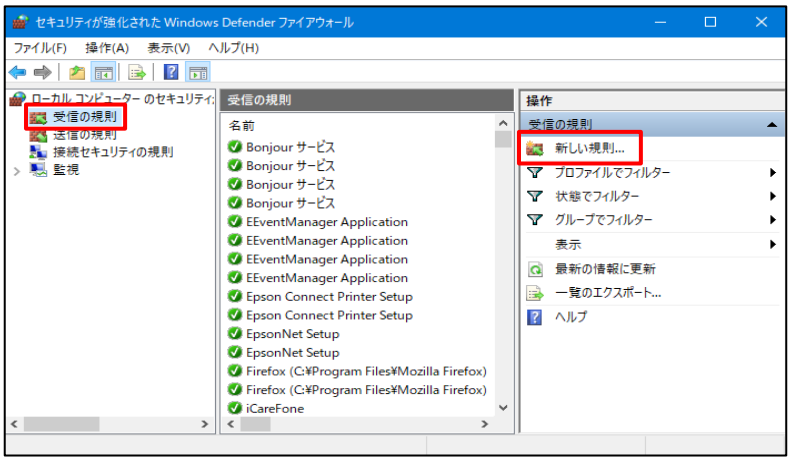
（１）端末のファイアウォール機能

①コントロールパネルから「Windows Defenderファイアウォール」を選択する。

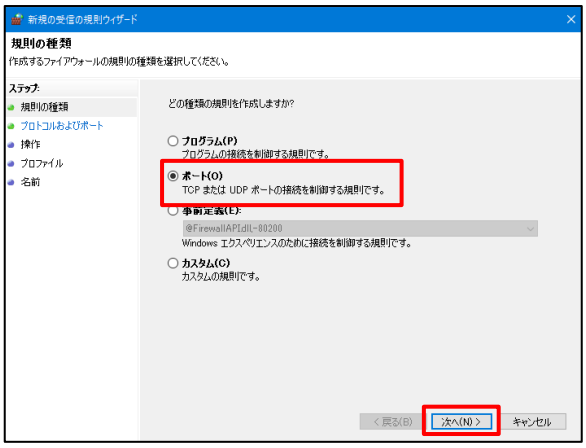
②「詳細設定」を選択する。



③「受信の規則」項目を選択し、「新しい規則」をクリックする。（送信の規則に関しても同様の設定を行う）

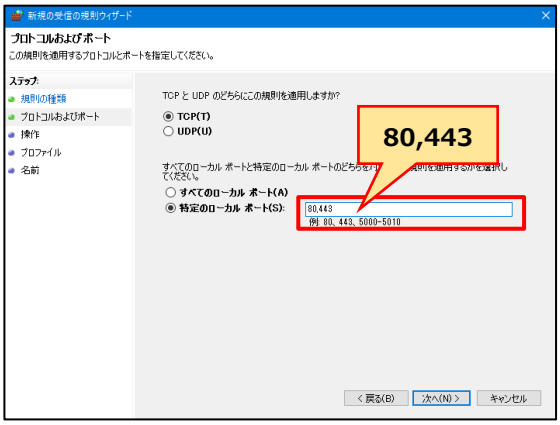


④「ポート」を選択し、「次へ」をクリックする。

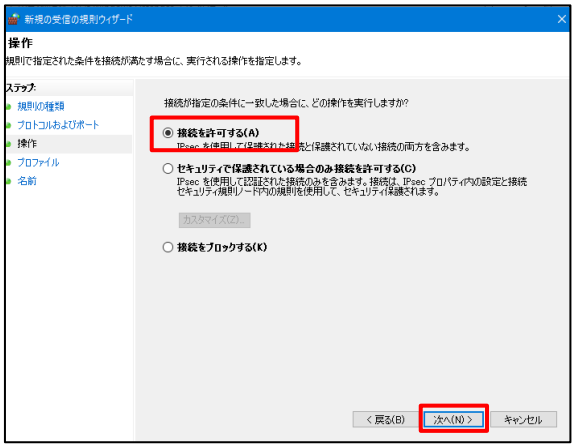


⑤「TCP（T）」にチェックを入れ、「特定のローカルポート（S）」に以下の値を入力する。

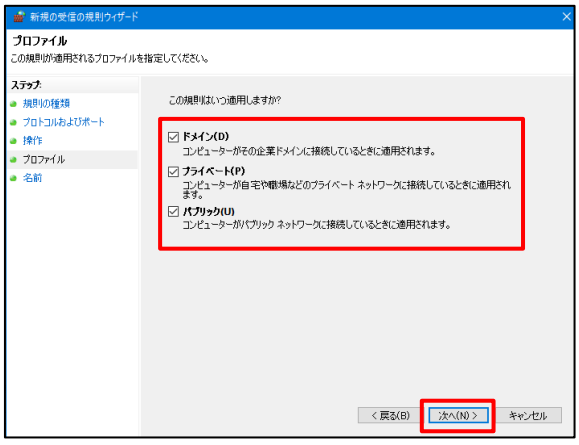
プロトコル名	プロトコル番号
HTTP	80
HTTPS	443



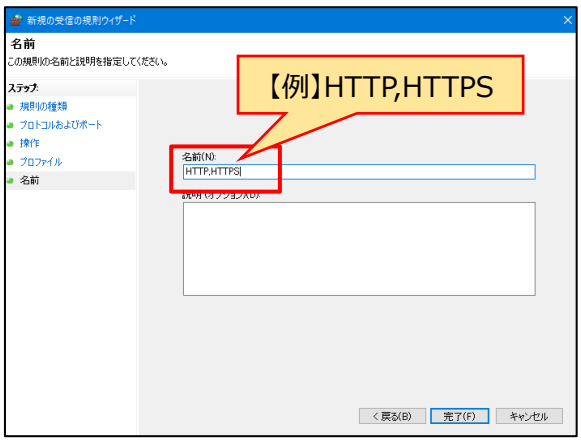
⑥「接続を許可する（A）を選択し、次へ　をクリックする。



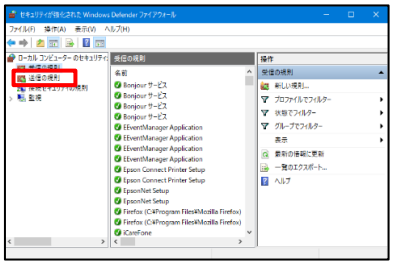
⑦下記の項目にチェックがついていることを確認し、「次へ」をクリックする。



⑧「名前」へ任意の名称を入力し、「完了」をクリックする。



⑨「送信の規則」においても、「受信の規則同様の設定を行う。



5.4 セキュリティーホール対策

ソフトウェアのセキュリティパッチを定期的に適用するための手順について記載する。

なお、統合専用端末のセキュリティパッチの状態はセットアップ時点で最新の状態とすること。

＜作業の流れ＞

①統合専用端末の更新プログラムの適用状態の確認（統合専用端末）

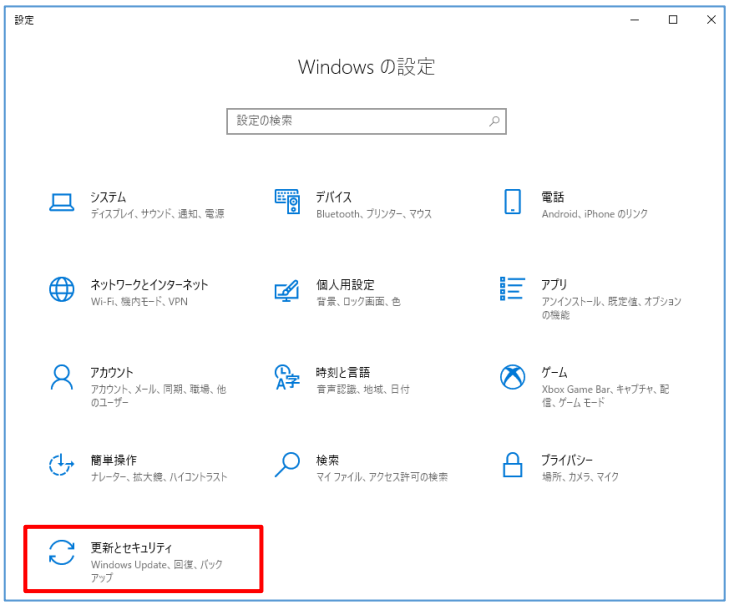
②インターネットに接続している業務端末等から必要な更新プログラムをダウンロード（業務端末等）

③②を USB メモリ等に保存し、セキュリティスキャン実施（業務端末等）

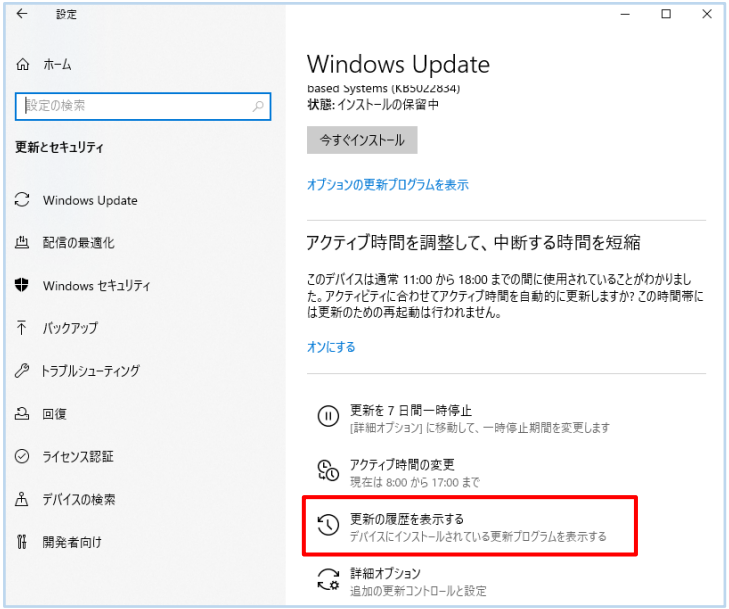
④統合専用端末に USB メモリを接続し、更新プログラムを適用（統合専用端末）

（１）統合専用端末に適用されている更新プログラムを確認する。

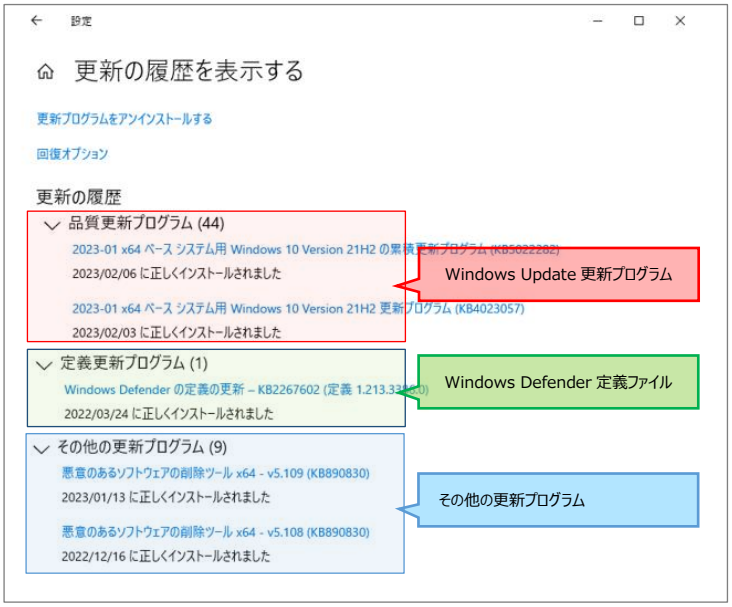
① スタートメニューから「設定」を表示し、「更新とセキュリティ」をクリックする。



② Windows Updateの「更新の履歴を表示する」をクリック



③ インストール済みの更新プログラムを確認



④統合専用端末のWindows バージョンを確認

スタートメニューから「設定」を表示し、「システム」をクリックする。

「詳細情報」を選択して、Windowsのエディション、バージョン、システムの種類を確認する。（以下で使用する）

⑤④で確認したOS、バージョンに該当する累積更新プログラムを以下のサイトからダウンロードする。

https://www.catalog.update.microsoft.com/home.aspx（Microsoft Updateカタログサイト）

⑥検索窓から「Windows␣10␣x64␣セキュリティ␣累積更新」と入力し、検索ボタンを押下する。

（Windows10、64ビットの場合）※環境によっては検索に少し時間がかかります

⑦必要な累積更新プログラムを選択し、ダウンロードボタンを押下する。

④で調べた Windows の詳細情報をもとにタイトル欄のバージョンと製品欄の該当製品を確認し、

- ●21H2（バージョンが 1903 以降用、LTSB 含む）を適用する場合は A
- ●20H2（バージョンが 1903 以降用、LTSB 以外）を適用する場合は B
- ●22H2（バージョンが 1903 以降用、LTSB 以外）を適用する場合は C

をダウンロードすること。（バージョンが 1903 以前の場合は該当する累積更新プログラムをダウンロードすること）

LTSB（※）を使用している医療保険者においては「LTSB」と記載があるものをダウンロードすること。

※LTSB（Long-Term Servicing Branch）は長期サービス チャネルのバージョンの一つで、2018 年に公開されたバージョン以降は LTSC（長期サービス チャネル）と名称変更されています。

⑧ダウンロードした更新プログラムを USB メモリ等の媒体に格納する。

当該 USB メモリ等をインターネットに接続されている端末に接続する際、必ず使用する前後にウイルススキャンを実施すること。

⑨USB メモリ等から更新プログラムを統合専用端末のデスクトップ等の任意の場所に移した後、実行して適用する。

＜注意＞

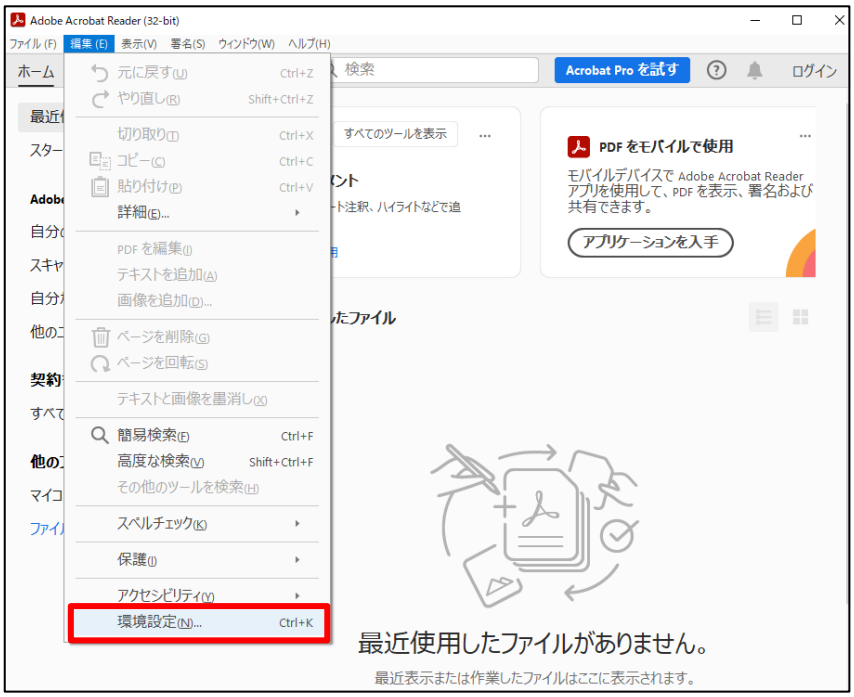
統合専用端末を中間サーバーネットワークから一時的に切り離し、インターネットに接続されている業務ネットワークに接続して、Microsoft の認証　もしくは、Windows Update を適用する運用をした場合は、必ず作業後にウイルススキャン（フルスキャン）を実施した上で中間サーバーのネットワークに接続すること。

5.6 情報システムの利用制限

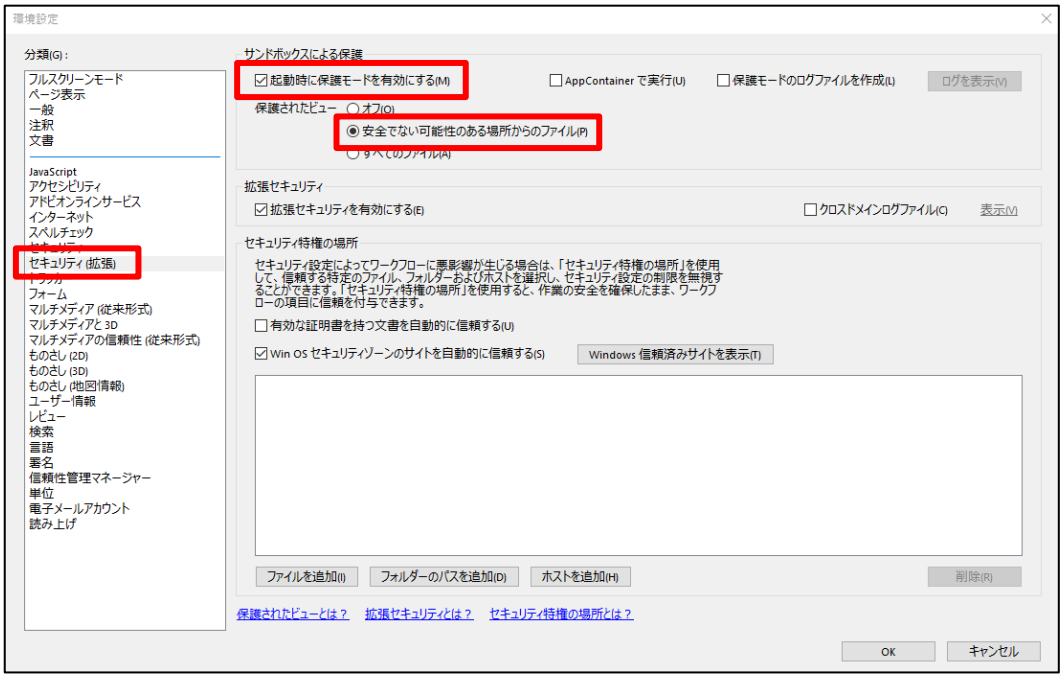
PDF リーダーのセキュリティ設定項目に対して制限を行い、業務用途以外での利用ができないようにするための設定手順について例を記載する。（Adobe Acrobat Readerを利用していない場合は対象外）

（１）Adobe Acrobat Reader「保護されたビュー」を有効にする。

①「編集」メニューから「環境設定」を選択し、環境設定画面を表示する。



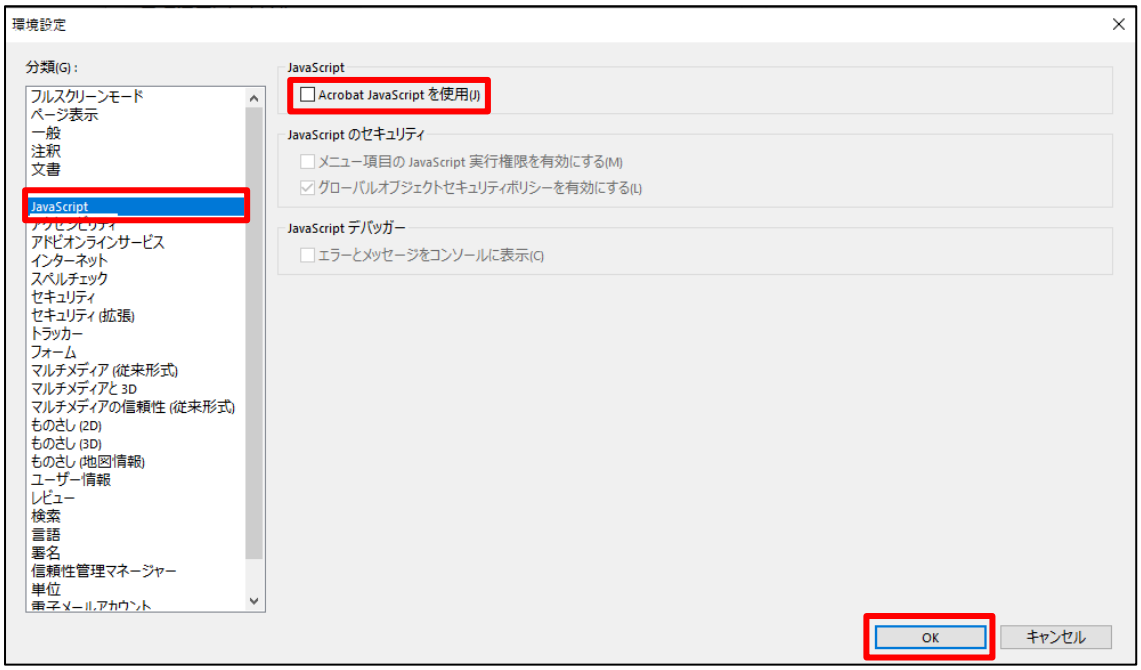
②分類から「セキュリティ（拡張）」を選択し、「起動時に保護モードを有効にする」と「安全でない可能性のある場所からのファイル」にチェックを入れ、「OK」ボタンをクリックする。



（２）Adobe Acrobat Reader「JavaScript」を無効にする。

①「編集」メニューから「環境設定」を選択する。

②分類から「JavaScript」を選択し、「Acrobat JavaScript を使用」のチェックを外し、「OK」ボタンをクリックする。



5.7 機器の要塞化

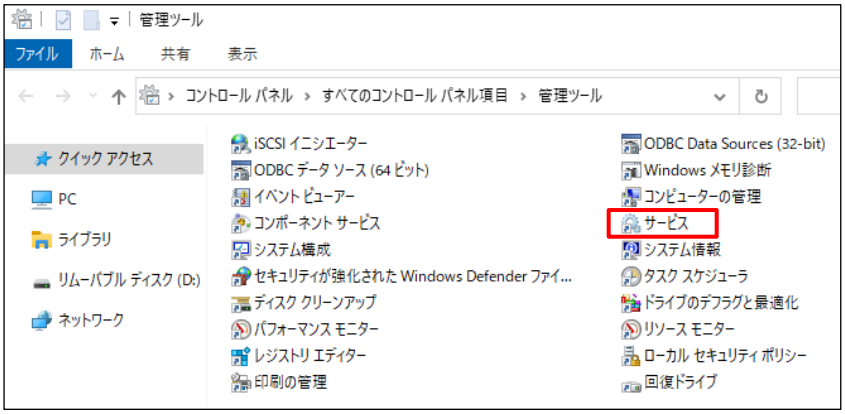
統合専用端末は不要なアプリケーションによって引き起こされるセキュリティの低下を防止する必要がある。そのリスクを可能な限り最小化するために、不要なOSの機能やサービスの停止及び不要なプログラムのアンインストール等を行う必要がある。

以下に「不要なサービスの停止」「不要なプログラムのアンインストール」について設定手順を記載する。

※個々のサービスやプログラムについては、端末のメーカーによって初期インストールされているアプリケーション等が異なるため、医療保険者等において個々のポリシーに沿って作業すること。

（１）不要なサービスの停止方法

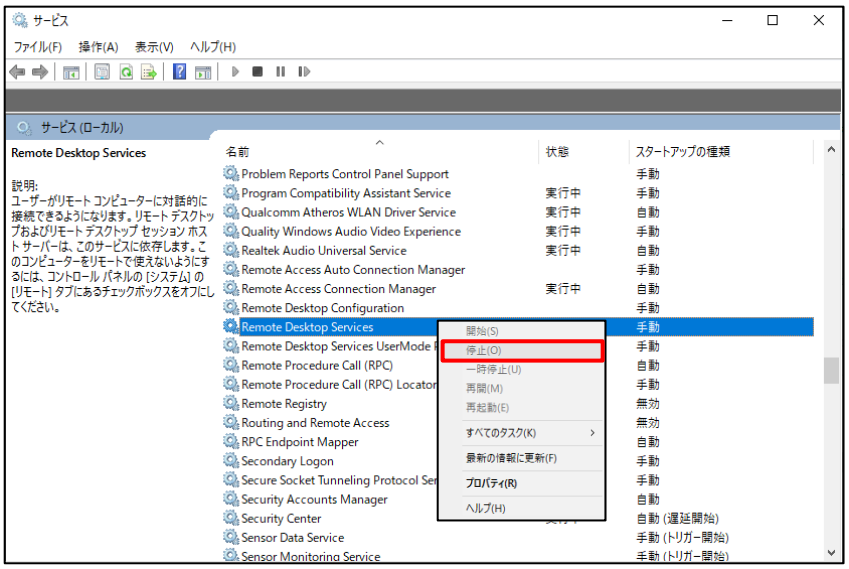
①コントロールパネルから管理ツールを開き、「サービス」をクリックする。



②停止したいサービスを選択し、右クリックする。

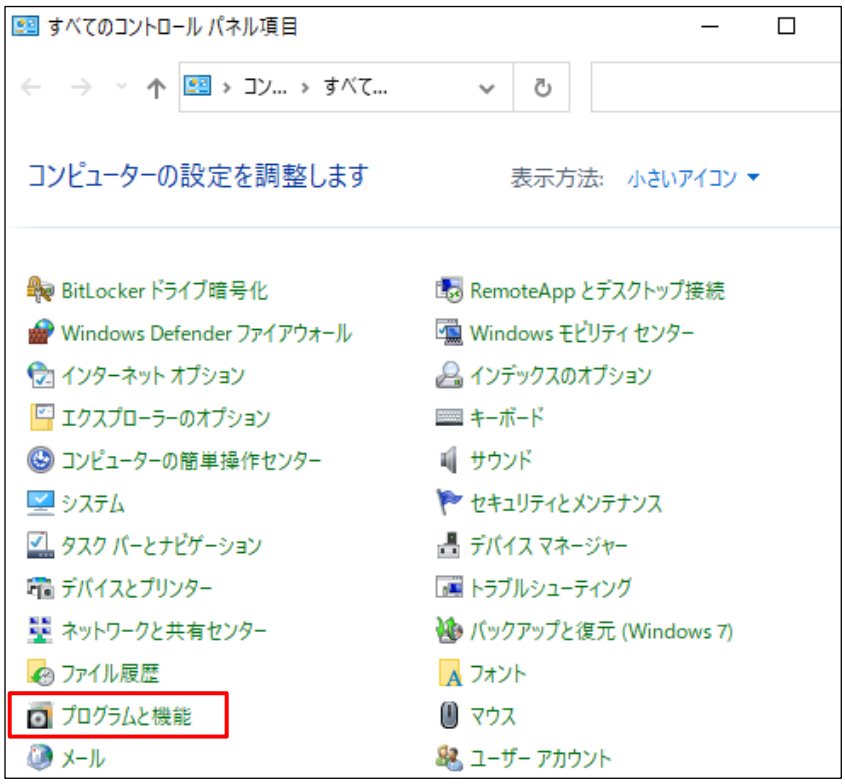
停止（O）を選択する。

（例）「リモートデスクトップ」サービスの停止



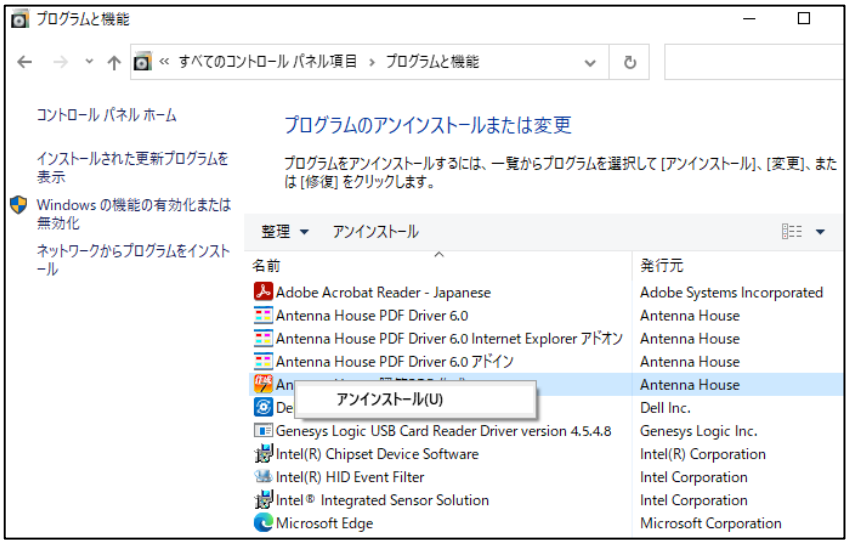
（２）不要なプログラムのアンインストール

①コントロールパネルから「プログラムと機能」をクリックする。



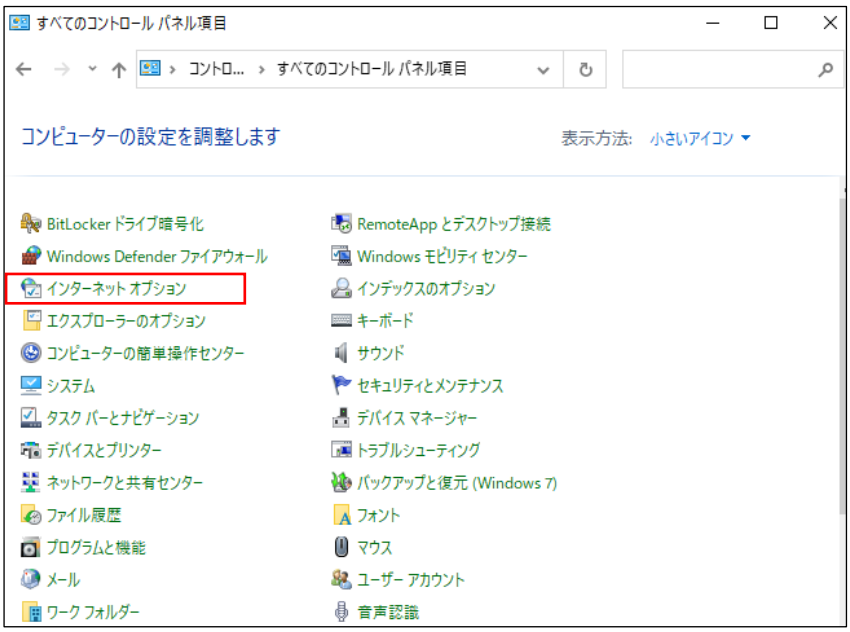
②不要なプログラム（※）の上で右クリックし「アンインストール（U）」を選択する。

※不要なプログラムについては、システム管理者およびベンダー等に確認すること。

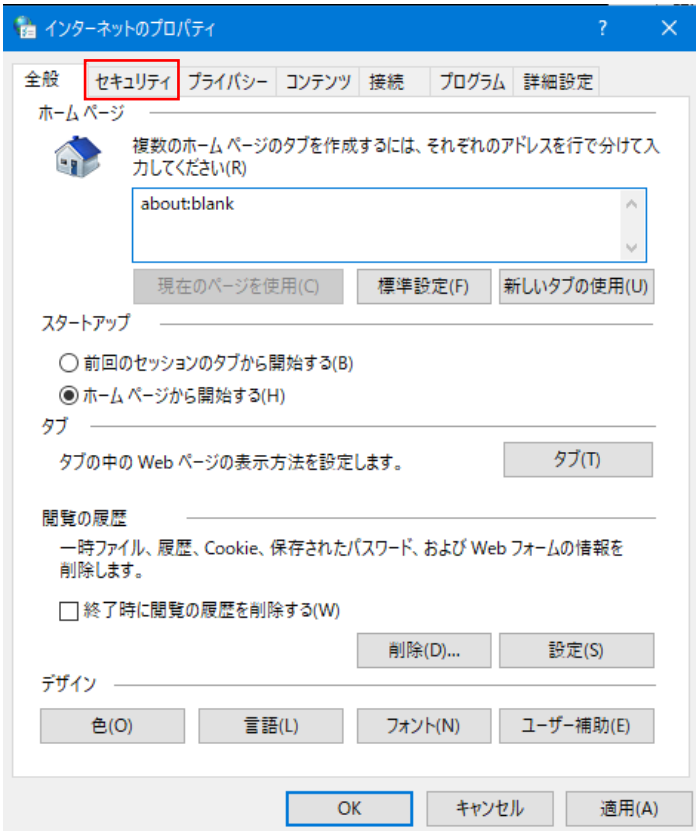


5.8 信頼済みサイトの登録

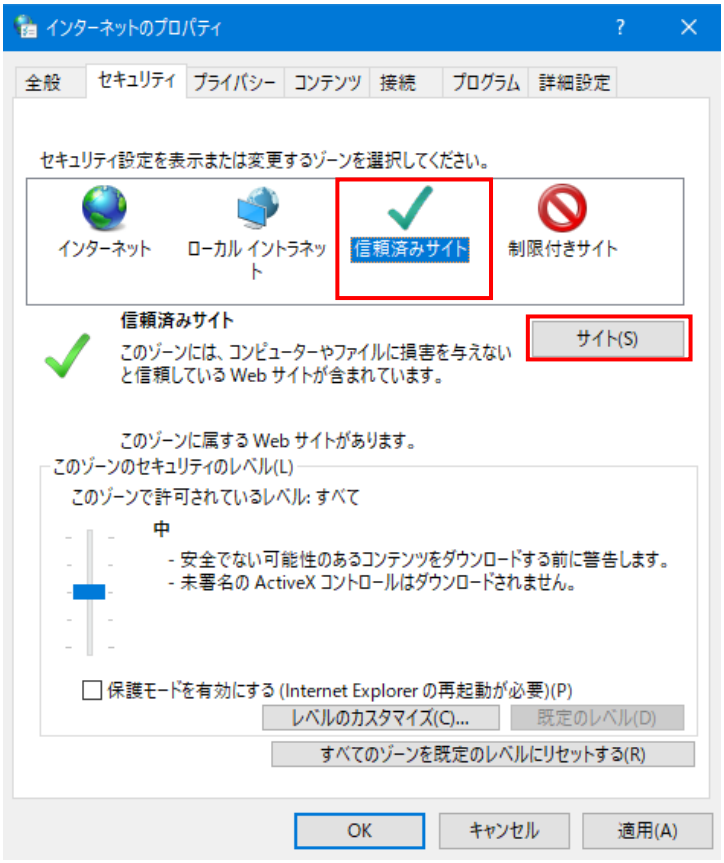
（１）コントロールパネルから「インターネットオプション」をクリックする。



（２）「インターネットのプロパティ」から「セキュリティ」タブを選択する。



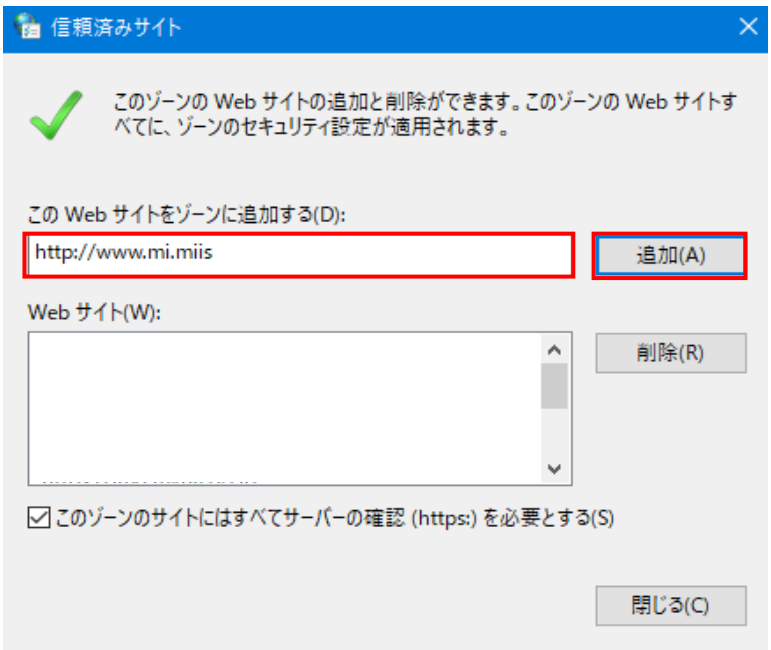
（３）「信頼済みサイト」を選択し、サイト（S）をクリックする。



（４）「このWebサイトをゾーンに追加する(D)」に、以下をひとつずつ入力し追加（A）をクリックする。

https://www.mi.miis

https://www.mi-st.miis

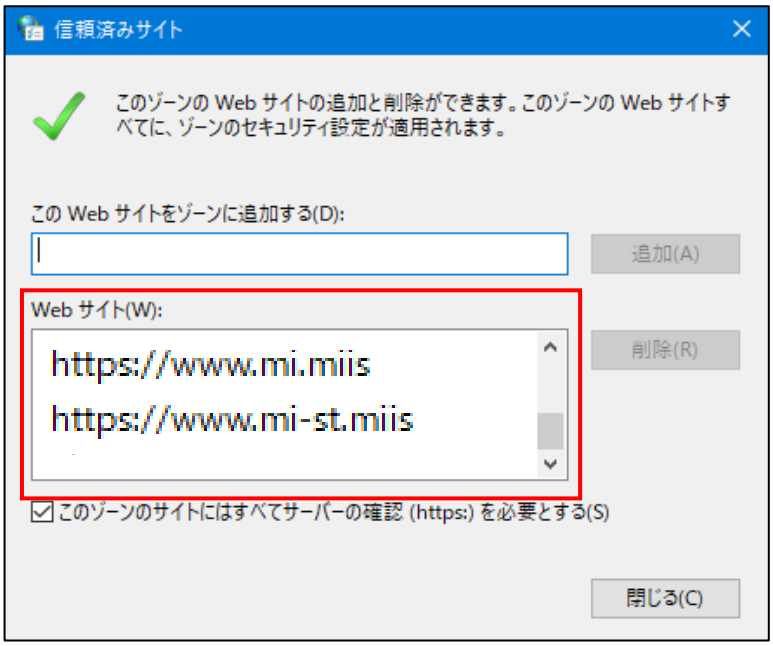


（５）「Web サイト(W)」の部分に、以下の二つが表示されている（信頼されている）ことを確認してください。

・https://www.mi.miis

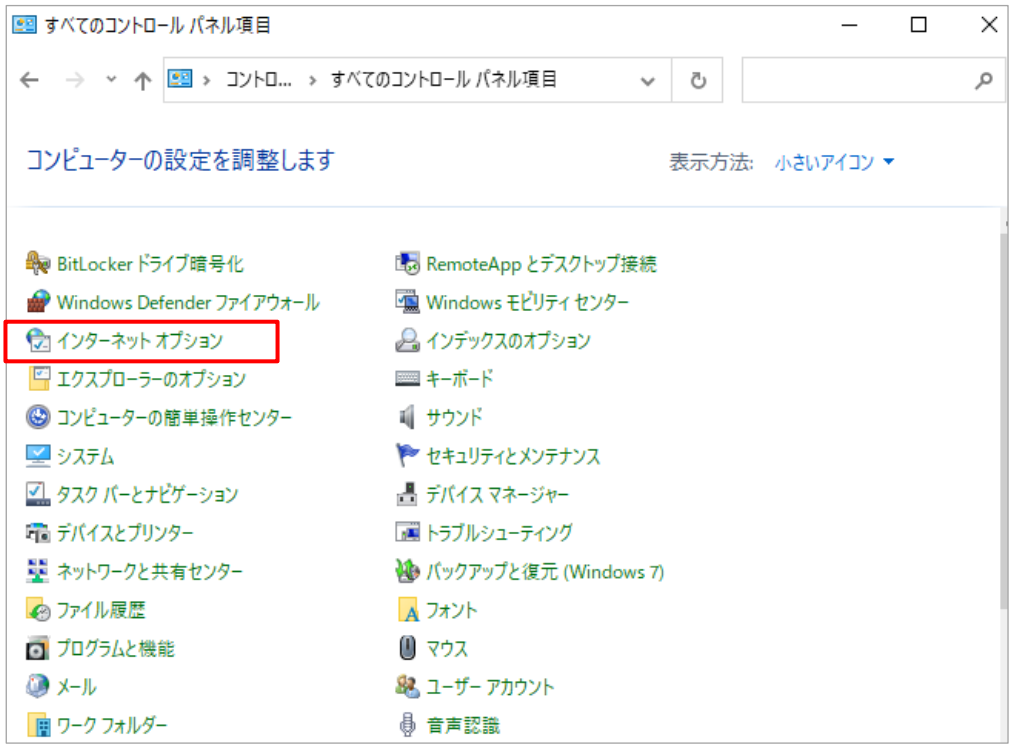
・https://www.mi-st.miis

「閉じる(C)」をクリックしてください。

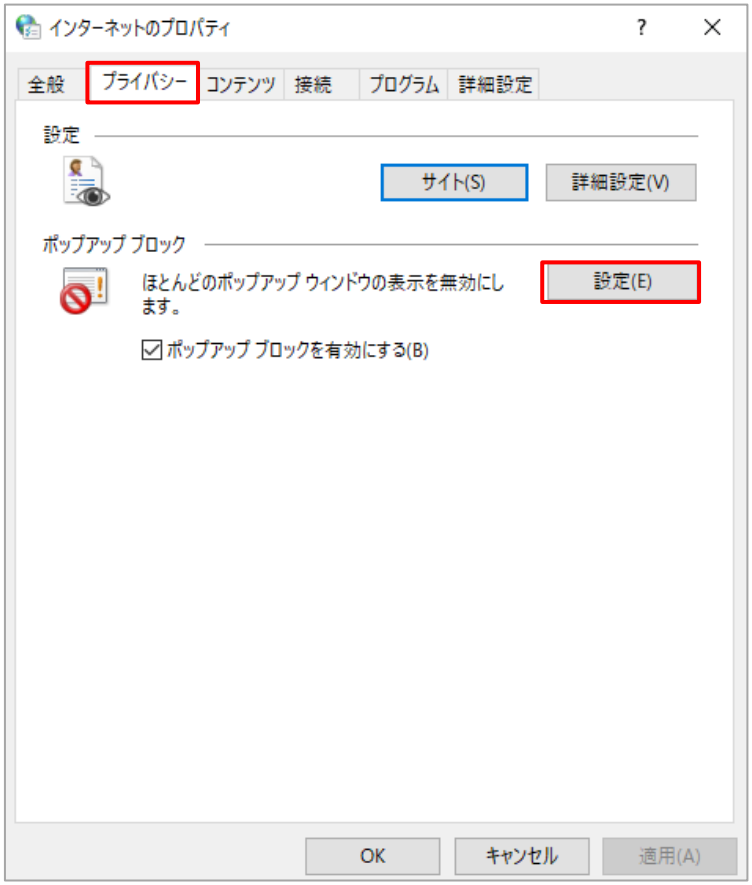


5.9 ポップアップブロックの設定

（１）コントロールパネルから「インターネットオプション」をクリックする



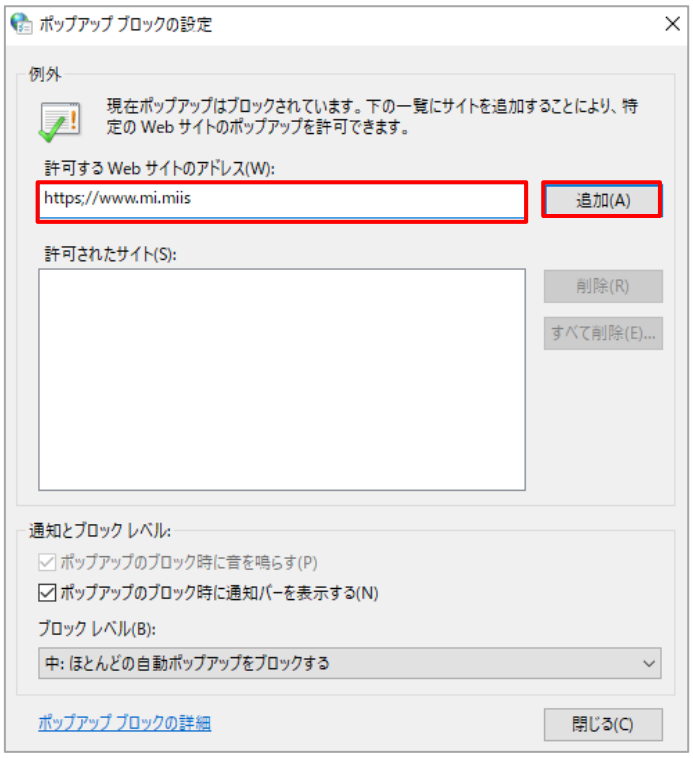
（２）プライバシーを選択し、設定をクリックする。



（３）「許可するWebサイトのアドレス（W）」に、以下をひとつずつ入力し追加（A）をクリックする。

https://www.mi.miis

https://www.mi-st.miis



（４）「許可されたサイト(W)」の部分に、以下の二つが表示されている（許可されている）ことを確認してください。

https://www.mi.miis

https://www.mi-st.miis

「閉じる(C)」をクリックしてください。

6 .ネットワークに係る設定

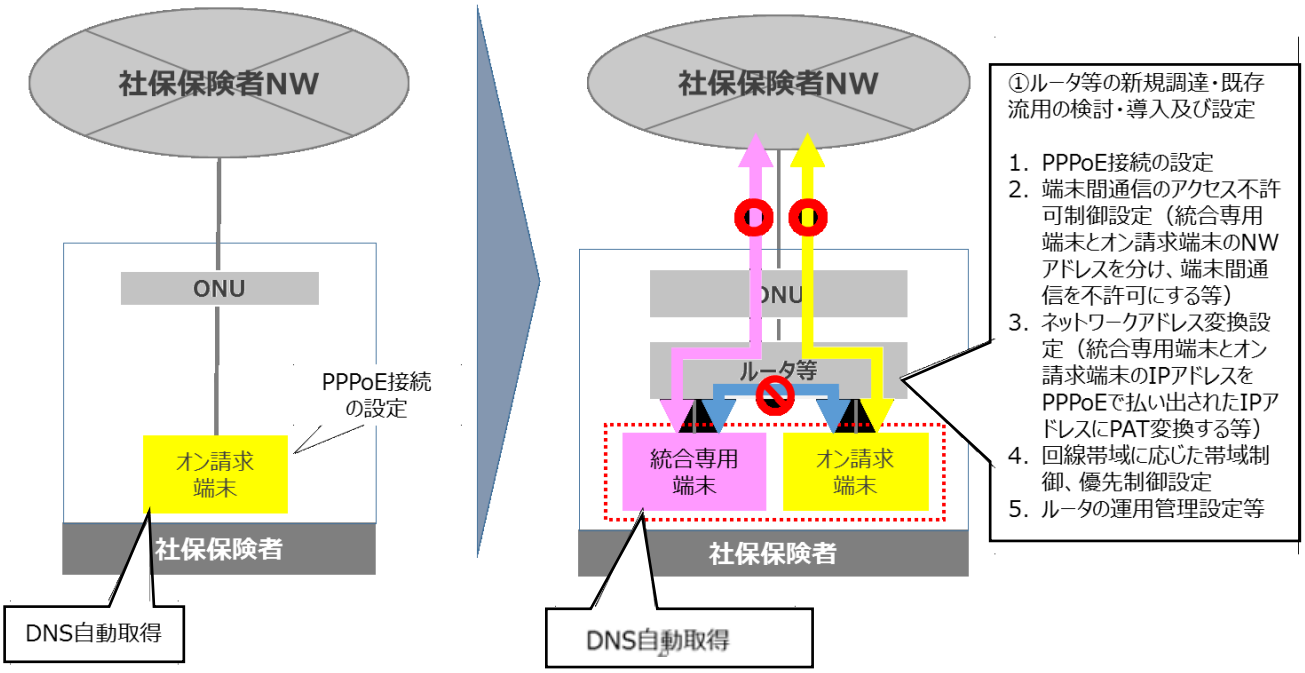
6.1 全国健康保険協会・健康保険組合・共済、福祉事務所における設定例

被用者保険
福祉事務所

※この章は医療保険者（被用者保険）および福祉事務所に関するものです

○ 全国健康保険協会・健康保険組合・共済等の医療保険者においては、既存のレセプトオンライン回線に統合専用端末を接続することとなるが、その接続設定については回線事業者においてその取扱いが異なるため、当該事業者と調整し適切に設定を行うこと。（福祉事務所に関しては厚労省から発出されている「ネットワーク接続方式について」を参照すること） 以下にその一例を示すので参考とされたい。

➢ **統合専用端末とオンライン請求端末を同時に利用する**には、①ルータ等の新規調達・既存流用の検討・導入及び設定 ②各端末の設定作業が必要になります。



※上記の図はIP-VPN 接続に関する社保系保険者を想定した図であり、IPsec+IKE 接続に関してはこの限りではない。IPsec+IKE に関する詳細な設定は契約しているIPsec+IKE サービス提供事業者へ問い合わせること。

6.2 国民健康保険組合、後期高齢者医療広域連合における設定方法

国保組合
広域連合

※この章は医療保険者等（国民健康保険・後期高齢者医療）に関するものです

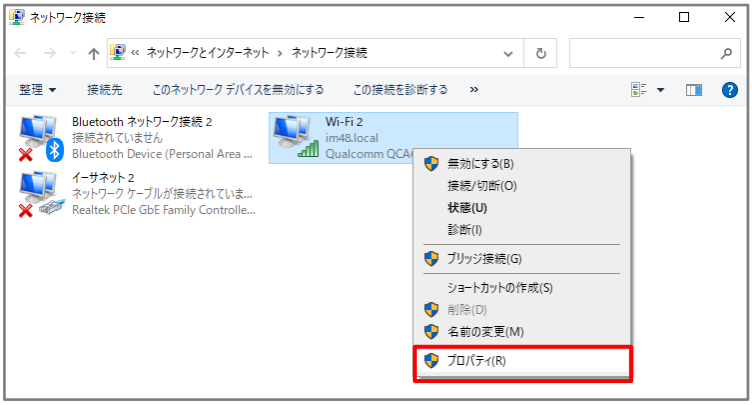
国保系（国民健康保険組合・後期高齢者医療広域連合）の医療保険者等において、マイナンバーネットワークに設定すべき内容はマイナンバーネットワーク事業者（ソフトバンク）から指定される構成管理表をもとに設定をすること。
統合専用端末に設定する IP アドレスは構成管理表に医療保険者ごとに指定されている IP アドレスの範囲から昇順に付与すること。

（１）IP アドレスの設定

①コントロールパネルから「ネットワークと共有センター」をクリックする。

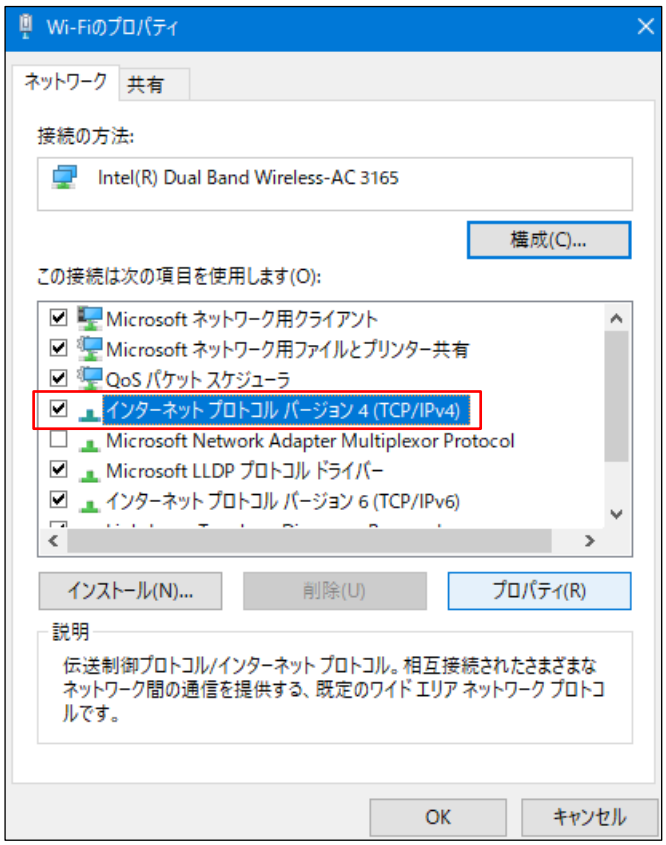
②「アダプターの設定の変更」をクリックする。

③統合専用端末が接続するネットワーク名（下記は例）を選択し、プロパティを開く

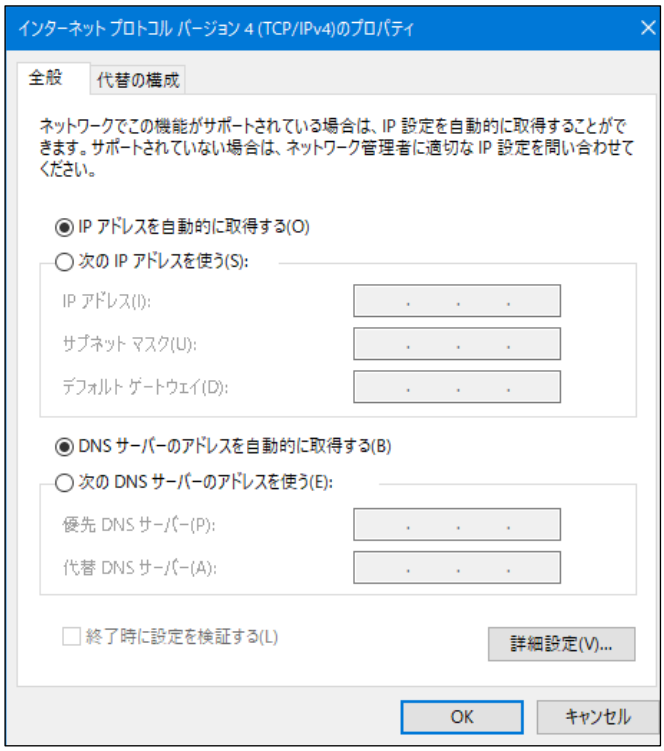


国保組合
広域連合

④「インターネット プロトコル バージョン 4(TCP/IPv4)」を選択し、「プロパティ」をクリックする。



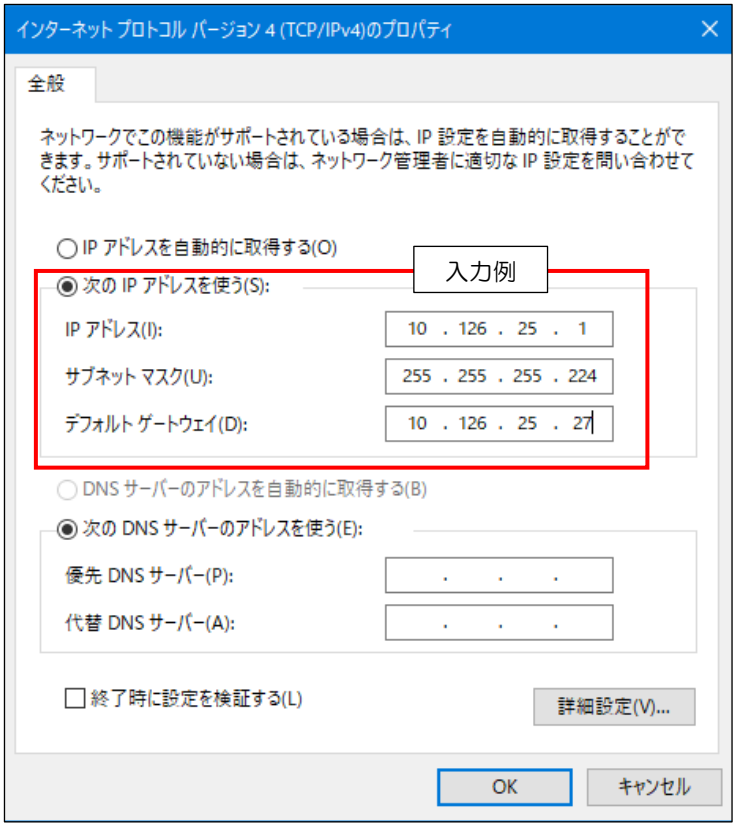
④「インターネット プロトコル バージョン 4(TCP/IPv4)」のプロパティ画面が表示されたことを確認する。



国保組合
広域連合

⑤ソフトバンク社から送付されている構成管理表に記載されたIPアドレス／サブネットマスク／デフォルトゲートウェイを入力し、「OK」をクリックする。

設定の詳細な説明については、次ページの「表6-2-1．IP アドレスの設定」参照。



国保組合
広域連合

表 6-2-1.　IP アドレスの設定

ソフトバンクから提示されている構成管理表（※）を参照すること。

設定値は医療保険者ごとに異なる。

＜注意事項＞

統合専用端末が複数台ある場合、設定する IP アドレスの値は重複させないこと。

②、③（④）のサブネットマスク、デフォルトゲートウェイは同一のものを設定する。

	ネットワーク機器					
	サブネットマスク (WAN)	IPアドレス ③ (LAN)	サブネットマスク ② (LAN)	ネットワークセグメント ① (LAN)	サブネットマスク ② (LAN)	VIPアドレス ④ (LAN)
例	30	10.126.25.27	27	10.126.25.0	27	10.126.9.1

※１　構成管理表：ソフトバンクとの契約の際に設定情報として配布されている。不明の場合はソフトバンクへ問い合わせること。

＜構成管理表の項目説明＞

該当箇所	名称	使用方法
①	ネットワークセグメント（LAN）	統合専用端末のIPアドレス設定可能範囲。 構成管理表に記載された値は使用不可のアドレスであり、右端の数字に1を加えた数値からアドレス設定可能範囲内で昇順にて割り当てること。また、ネットワーク機器等に既に割り当て済のアドレスがあるため、設定可能アドレスは各拠点のサブネットマスク(②)に応じて異なる。 【例】 サブネットマスク数26の場合：使用可能アドレス数57 サブネットマスク数27の場合：使用可能アドレス数25 【割り当て例】 構成管理表に記載されたアドレスが10.126.25.0であり、サブネットマスク数27の場合、統合専用端末には10.126.25.1から10.126.25.25までを昇順で割り当てる。 （１台目10.126.25.1、２台目10.126.25.2 ･･･25台目10.126.25.25と昇順で割り当てる。）
②	サブネットマスク（LAN）	統合専用端末のサブネットマスクには以下を設定すること。 【例】 サブネットマスク数 26：255.255.255.192 サブネットマスク数 27：255.255.255.224
③	IP アドレス（LAN）	統合専用端末のデフォルトゲートウェイのIPアドレス。 シングル構成：構成管理表中の③に記載された値を入力すること。 冗長構成　　：構成管理表中の④に記載された値を入力すること。
④	VIP アドレス（LAN）	

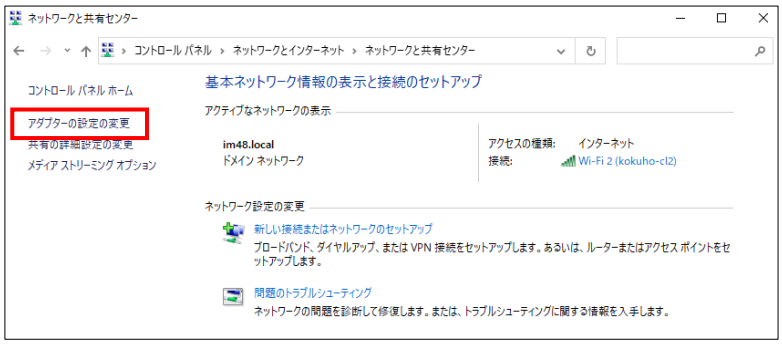
国保組合
広域連合

（２）DNS設定

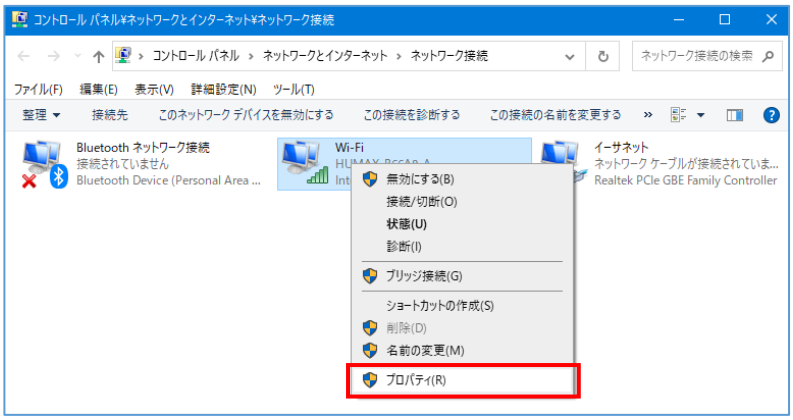
国民健康保険組合・後期高齢者医療後期連合の DNS 設定について記載する。

①コントロールパネルから「ネットワークと共有センター」をクリックする。

②画面左側の「アダプターの設定の変更」をクリックする。

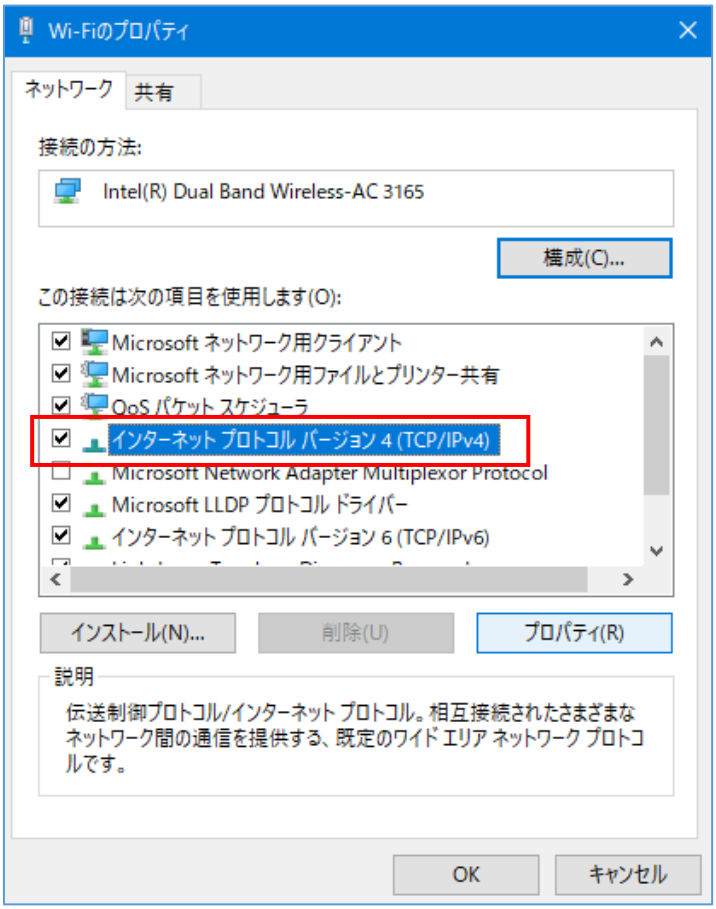


③LANアダプター名が表示されている接続アイコンを右クリックし、「プロパティ（R）」をクリックする。

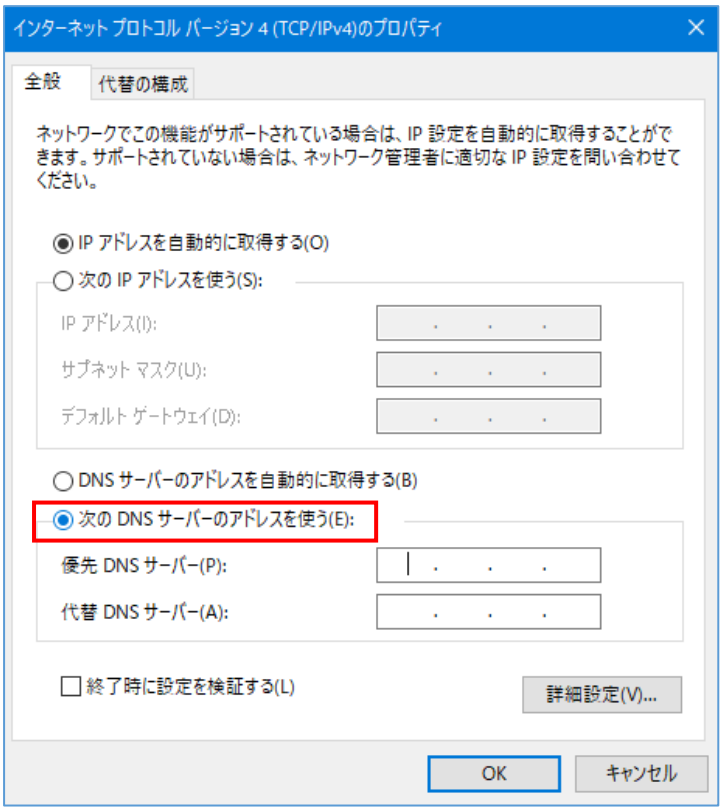


国保組合
広域連合

④「インターネット プロトコル バージョン4（TCP/IPv4）」を選択し、「プロパティ（R）」をクリックする。



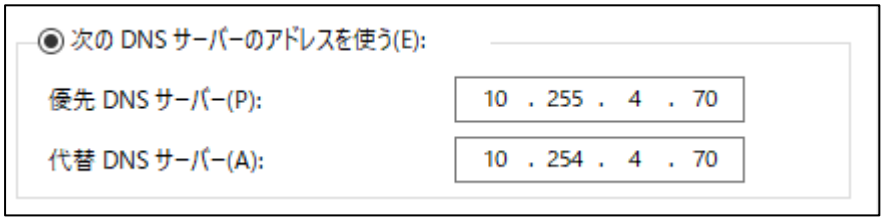
⑤「次のDNSサーバーのアドレスを使う（E）」をクリックする。



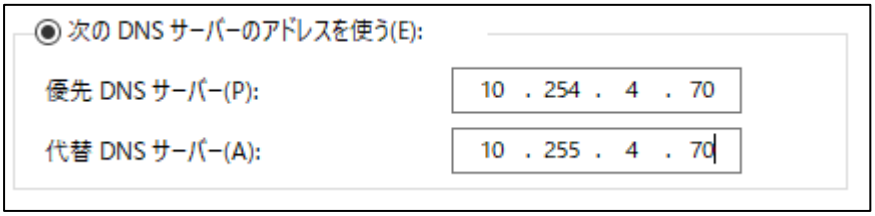
国保組合
広域連合

⑥「優先DNサーバー（P）」及び「代替DNSサーバー（A）を以下のとおり入力する。
※所在が東日本/西日本により設定値が異なるので注意すること。
（別紙「医療保険者_東西」参照）

＜東日本に所在する医療保険者等＞
「優先DNSサーバー(P)」に「10.254.4.70」と入力。
「代替DNSサーバー(A)」に「10.255.4.70」と入力。



＜西日本に所在する医療保険者等＞
「優先DNSサーバー(P)」に「10.255.4.70」と入力。
「代替DNSサーバー(A)」に「10.254.4.70」と入力。



⑦「優先DNSサーバー（P）」及び「代替DNSサーバー（A）」にDNSサーバーのIPアドレスが入力できていることを確認し、「OK」をクリックする。

6.3 ネットワーク接続要件

＜参考＞

（１） 本番環境接続要件

通信要件	ホスト名		IP アドレス	ポート番号
業務通信	統合専用端末	www.mi.miis	—	443（HTTPS）/TCP
	基幹システム	www.exs.miis		
	ASP 事業者	www.exs.miis		
名前解決	—		10.254.4.70 10.255.4.70	53（DNS）/TCP,UDP

（２）接続検証環境接続要件

通信要件	ホスト名		IP アドレス	ポート番号
業務通信	統合専用端末	www.mi-st.miis		443（HTTPS）/TCP
	基幹システム	www.exs-st.miis	—	
	ASP 事業者	www.exs-st.miis		
名前解決	—		10.254.4.70 10.255.4.70	53（DNS）/TCP,UDP

7 .インターネット接続に関する注意事項

○「統合専用端末の端末仕様等について」において、統合専用端末を接続するネットワークはインターネット回線と分離する必要があると規定されている。

ただし、統合専用端末のセットアップ時にMicrosoft 社の認証を受ける際や、Windows Updateの適用やウイルス対策ソフトの定義ファイルの最新化等のためにインターネットに一時的に接続、もしくはUSBメモリ等の媒体を通じて間接的にインターネットへの接続が必要となる場合がある。

○ このような場合のインターネット接続にあたっては以下の点に注意すること。

・インターネット回線を経由したウイルス感染のセキュリティリスクが生じるため、統合専用端末でインターネット接続を行った場合は、中間サーバーネットワークのLANに接続する前に最新パターンファイルを適用した上で必ずウイルススキャン（フルスキャン）を実施すること。

・USBメモリ等は利用前後にウイルススキャン（フルスキャン）をした上で使用すること。

○医療保険者等によるポリシーに基づき、Windowsセキュリティ以外のアンチウィルスソフトウェアを使用している場合は、その使用方法に準じてウイルススキャンを実施すること。