医療保険者等向け中間サーバー等
統合専用端末に係る端末仕様について

第４.１版

令和４年１２月１２日

内容

変更履歴表

項番	版数	変更日	該当箇所	変更内容
1	1.0	2016/7/27	-	新規作成
2	2.0	2016/9/30	4. ソフトウェア	サポートOS について、医療保険者等からWindows10 への対応要望が多く寄せられていること、Windows10 のデスクトップOS シェアがWindows8.1 よりも高くなってきていること等を踏まえ、Windows8.1 からWindows10 へ変更
3	2.0	2016/9/30	4. ソフトウェア	ウイルス対策について、検討中の内容を追記
4	2.0	2016/9/30	5.セキュリティ対策	不正プログラム対策、セキュリティホール対策及び時刻同期について、検討中の内容を追記
5	3.0	2016/10/14	4. ソフトウェア	ウイルス対策に係る対応内容を追記
6	3.0	2016/10/14	5.セキュリティ対策	不正プログラム対策、セキュリティホール対策及び時刻同期に係る対応内容を追記
7	4.0	2022/ 5 /16	3.ハードウェア	「表 3-1 統合専用端末の最小システム要件」を最新化 （Windows11 Pro へアップグレード可能なスペックを表記）
8	4.0	2022/ 5 /16	4.ソフトウェア	中間サーバーにおける OS およびブラウザ対応のマイルストーンに基づく変更
9	4.0	2022/ 5 /16	5.セキュリティ対策	Windows Update およびウイルス対策ソフトのパターンファイルの扱いについて記載
１０	4.0	2022/ 5 /16	7. OS およびブラウザ対応のマイルストーン	中間サーバーにおける OS およびブラウザ対応のマイルストーンを記載
１１	4.1	2022/12/12		福祉事務所向け対応

１．はじめに

医療保険者等および福祉事務所（以下、医療保険者等）は、医療保険者等向け中間サーバー等（以下、中間サーバー）の業務運用・管理の実施にあたり、当該業務運用・管理のみで利用する統合専用端末を設置する必要がある。

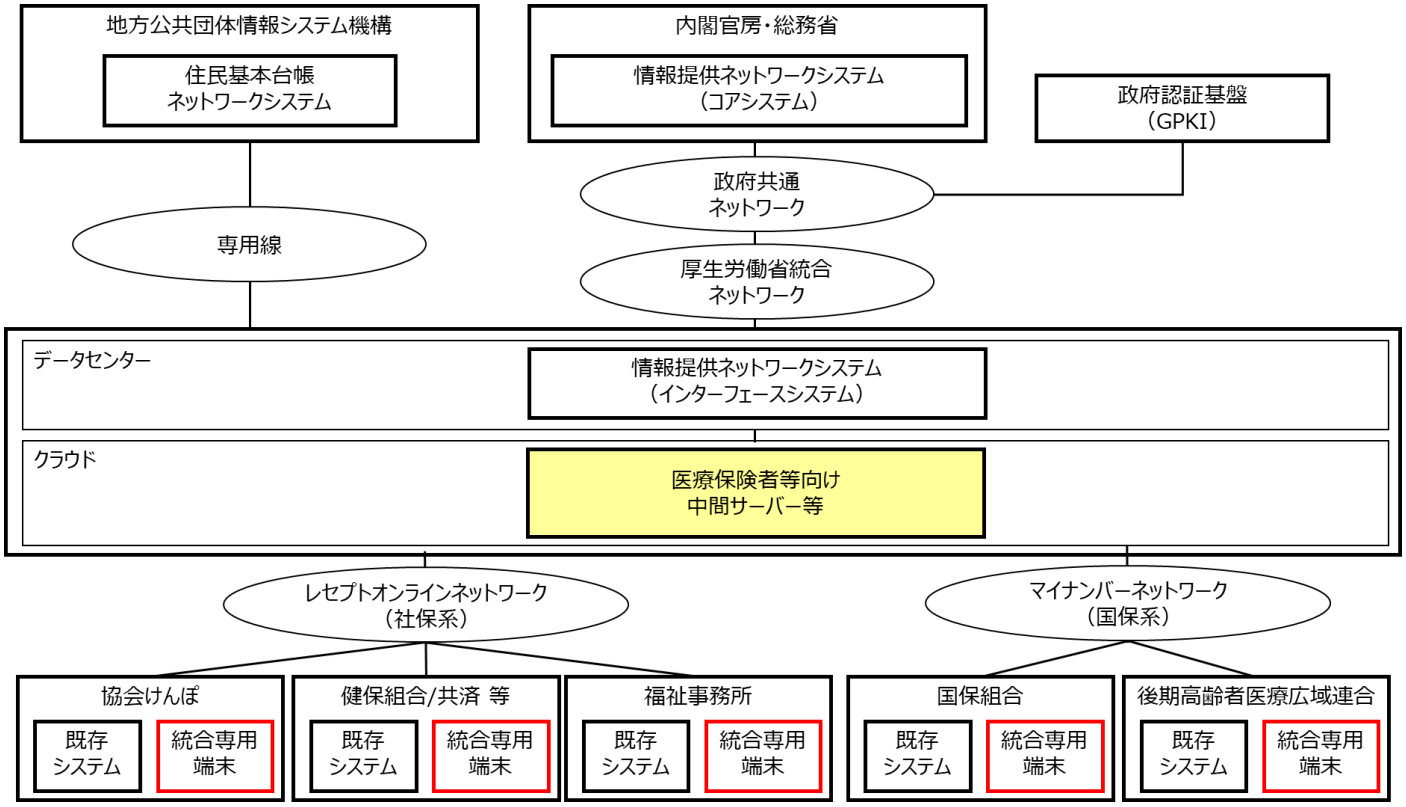
本書は、医療保険者等が利用する統合専用端末を構成するハードウェアの推奨スペック、必要なソフトウェア、セキュリティ対策及び利用するネットワークに係る情報を整理したものである。

※福祉事務所向けに関しては、令和５年度からの利用開始に向けて推奨環境を記載している。

2．統合専用端末の位置づけ

番号制度に係るシステム全体構成における統合専用端末の位置づけを以下に示す。

図 2-1 統合専用端末の位置づけ



３．ハードウェア

統合専用端末のハードウェアに係る推奨スペックを以下に示す。
現在の端末を使用し続ける場合は、そのまま使用可能。

新規に統合専用端末を購入する際は、下記を参考に Windows10 Pro、もしくは Windows11 Pro を購入すること。

表 3-1 統合専用端末の最小システム要件

項番	項目	推奨値	備考
1	プロセッサ（CPU）	1 ギガヘルツ（GHz）以上、2 コア以上の 64 ビット互換性プロセッサ、またはシステムオンチップ（SoC）	
2	メモリ	4GB 以上	8GB 以上を推奨
3	ストレージ	256GB 以上の記憶装置 （統合専用端末本体に内蔵された HDD、SSD ドライブに限る）	ネットワークドライブ（NAS）、および外付け HDD 等の外部記憶装置を常時接続した利用は不可。
4	システムファームウェア	UEFI（セキュアブート対応）	旧 BIOS
5	ネットワークインターフェイス	100Mbps 相当以上が 1 ポート以上	ネットワーク接続機器に適合した物理インターフェイスとすること。
6	ディスプレイ	12 インチ以上（WDDM2.0 ドライバ）対応	
7	グラフィックカード	DirectX 12 以上（WDDM 2.0 ドライバ）に対応	
8	セキュリティ対策	トラステッドプラットフォームモジュール（TPM）Ver.2.0 以上	
9	入力デバイス	日本語対応の標準キーボード、マウス等	
１０	その他	CD（DVD）ドライブ、USB インターフェイス等	外部データを持ち込む場合やログを持ち出す場合を考慮したインターフェイスを保有すること。

なお、統合専用端末からプリンタを利用して印刷を行うことは可能とする。ただし、ネットワークプリンタを利用する場合は、別ネットワークに存在するプリンタへの接続は禁止する。

４．ソフトウェア

統合専用端末に必要となるソフトウェアを以下に示す。導入するソフトウェアについては、以下に示す OS で動作保証されているバージョンを利用すること。

なお、統合専用端末には、中間サーバーを利用する業務及びセキュリティ対策に必要なソフトウェア以外のソフトウェアをインストールしないこと。

表 4-1 統合専用端末のソフトウェア

項番	項目	ソフトウェア	備考
1	OS	・Windows10 Pro ・Windows11 Pro	これから購入する際は、サポート期限の観点から Windows11 を推奨
2	ブラウザ	・Microsoft Edge	Microsoft Edge 以外は動作保証外
3	ウイルス対策	・Windows Defender	必須 他のウイルス対策ソフト、改ざん検知ソフト等を独自に使用する場合は、想定外の通信ブロック等が起きないよう保険者責任において使用すること。
4	暗号化 圧縮/解凍	・Lhaplus ・Winzip 等	ZIP 圧縮/展開の際にパスワードによる保護、および解除を行うことができるもの
5	PDF リーダー	・Adobe Acrobat Reader	必須
6	CSV ファイル編集	・Microsoft Excel ・CSV エディタ 等	任意 中間サーバー等からダウンロードした CSV ファイルを確認できるもの

５.セキュリティ対策

5.1. 実施すべき技術的対策

統合専用端末に実施すべきセキュリティに関する技術的対策を以下に示す。
統合専用端末はインターネットに接続可能なネットワーク上に配置することを禁止する。

下記、表５－１に記載した Windows Update やウイルス対策ソフトのパターンファイル等は、別のインターネットに接続可能な端末から取得し、セキュリティスキャンを行った USB メモリなどを介して、統合専用端末に適用すること。

表 5-1 技術的対策一覧

項番	分類	対策の内容
1	不正プログラム対策	・ウイルス対策ソフトウェアを導入し、以下のすべてを実施すること。 ● リアルタイムスキャンを実施 ● 定期的にフルスキャンを実施 ● 定期的に最新パターンファイルを適用 ● ウイルス検知時の通知
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こと。（独自の証跡管理ソフト等を導入する場合は保険者責任において実施すること） ・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こと。同期サーバーが存在しない環境の場合は、定期的に時刻を調整すること。
3	機器認証	・中間サーバー等側での機器認証に対応できるよう、共通認証局から発行された電子証明書を導入すること。
4	論理アクセス制御	・端末のファイアウォール機能による制御を行うこと。 ・電子データへのアクセス制御を行うこと。
5	権限管理	・特権アカウントの管理を適切に行い、発行や利用は必要最小限に留めるよう制限すること。
6	セキュリティホール対策	・OS およびウイルス対策ソフトのセキュリティパッチを定期的に適用すること。
7	利用制限	・OS、ブラウザ、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こと。 ＜想定される対策例＞ ・Windows ファイアウォールにより、ブラウザから中間サーバー等以外の通信を禁止 ・端末のブラウザに対し、スクリプトの許可を最小限のサイトに制限 ・Adobe Acrobat Reader の JavaScript 機能を無効化
8	機器の要塞化	・不要なOS 機能やサービスは、停止／アンインストールすること。 ＜想定される対策例＞ Windows リモートデスクトップ、Hyper-V 等の業務に使用しないサービスの停止又はアンインストール ・不要なアカウントは無効化、もしくは削除すること。

5.2 外部記録媒体の運用について

外部記録媒体の運用で留意すべき点を以下に示す

（１） 管理体制の整備

・外部記録媒体の管理者を設置する。

・外部記録媒体の利用状況、データ削除・廃棄状況等を定期的に確認する責任者を設置する。

（２） 運用準備

・統合専用端末との情報授受のみで利用する外部記録媒体を用意する。

・統合専用端末では、認められた外部記録媒体のみを利用するよう、措置を講じる。

（３） 利用

・外部記録媒体の利用は、管理者の承認に基づき利用する。

・利用者や管理者の承認実績など、外部記録媒体の利用状況等を確認できる媒体管理簿を用意し、必要事項を記入する。

・外部記録媒体へデータを保存する場合、暗号化処理又はパスワードによる保護等を行う。

・外部記録媒体の管理区域外への持ち出し、送付は禁止する。

（４） 保管

・外部記録媒体は施錠可能な場所に保管し、鍵の管理を適切に行う。

（５）データ削除・廃棄

・外部記録媒体の利用を終了する際、利用者は保存したデータをデータ復旧不可能な状態に削除し、管理者へ返却を行う。

・外部記録媒体を廃棄する際、物理破壊を実施する。

・外部記録媒体の削除・廃棄状況等を確認できるよう、媒体管理簿を用意し必要事項を記入する。

６．統合専用端末が接続するネットワーク及び統合専用端末の共用について

6.1. 接続するネットワークについて

統合専用端末が接続するネットワークは、医療保険者等の既存システムとのネットワークとは物理的又は論理的に分離すること。また、当然にインターネット回線と分離すること。

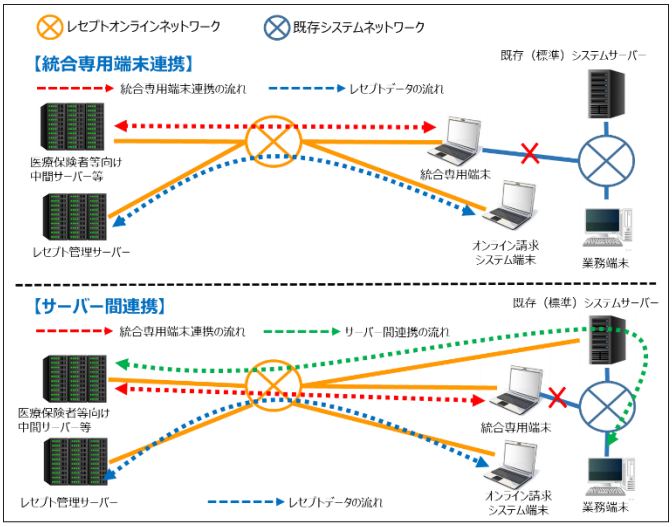
サーバー間連携を実施する医療保険者等においては、既存システムのサーバーが中間サーバーへ接続するネットワーク（レセプトオンラインネットワーク又はマイナンバーネットワーク）及び既存システムとのネットワークの双方に接続する場合がある。その場合は、前述「5.1 実施すべき技術的対策」の論理的アクセス制御について特に留意し、統合専用端末と既存システムの業務端末間で直接的なファイル共有が不可となるよう、措置を講じること。

6.2. 統合専用端末の共用について

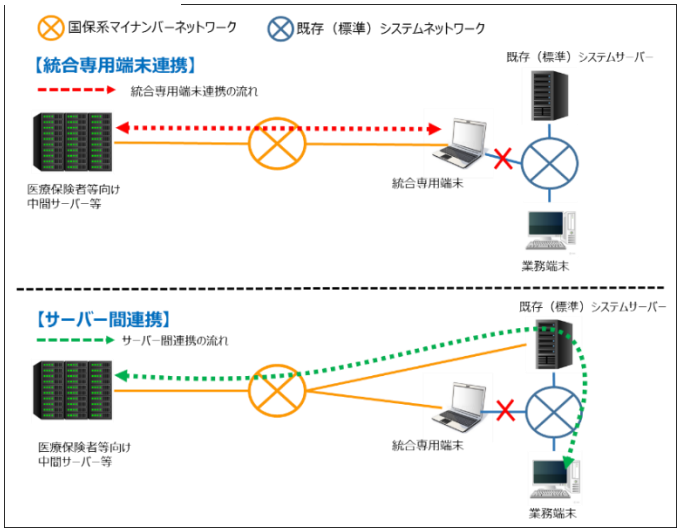
統合専用端末は、住民基本台帳ネットワークシステムへ本人確認情報の照会等を行う住基連携機能の操作が可能であることから、住民基本台帳ネットワークシステムにおけるセキュリティポリシーに照らし、既存システムの業務端末との共用を不可とする。また、同様にオンライン請求システム端末との共用も不可とする。

図 6-1 システム構成全体イメージ

＜社保系、福祉事務所＞



＜国保系＞



7．OS およびブラウザ対応のマイルストーン

2022 年 4 月 1 日現在、Windows OS および、ブラウザの更改期であるため、中間サーバーでは下記のマイルストーンにて対応を実施している。

統合専用端末はインターネットと分離したネットワーク内に存在するため、サポート終了後の 2022 年 6 月 16 日以降も Internet Explorer11 の利用が可能である。原則、中間サーバーでは Microsoft Edge に対応するまでの間（2023 年 6 月予定）は、Internet Explorer11 を継続して使用することを想定している。

2022 年 6 月 16 日以降、医療保険者都合等、および医療保険者等の環境によって Internet Explorer11 の利用を継続できない場合、Microsoft Edge の IE モード（Microsoft Edge は動作保証外）を使用すること。

※2023 年 6 月以降は、Microsoft Edge のみが利用可能となる。

以下に中間サーバーにおける OS、およびブラウザ対応のマイルストーンを示す。