別紙１　医療情報システム要求仕様書

								要求仕様	必須
1	9							電子カルテシステム	
1	9							二要素認証システム	
1	9	1						全般	
1	9	1	1					端末利用時は、個人認証を実施後、デスクトップが解放され利用可能なこと。	○
1	9	1	2					当センターで稼働する電子カルテシステム端末で動作可能なこと。	○
1	9	2						ハードウェア	
1	9	2	3					ICカードリーダー	
1	9	2	3	1				非接触ICカード規格「FeliCa」の読み取りができること。	○
1	9	2	3	2				Windows 11 対応であること。	○
1	9	2	3	3				カード・デバイスに対する通信距離は、5mm以下であること。	○
1	9	2	3	4				端末との接続は、USB接続であること。	○
1	9	3						システム要件	
1	9	3	1					アカウント情報連携機能	
1	9	3	1	1				電子カルテシステムの利用者情報を取得し、認証システムサーバにアカウント情報を格納可能であること。	○
1	9	3	2					端末認証・個人認証機能	
1	9	3	2	1				ソフトウェアは、サーバ及びクライアントから構成されていること。	○
1	9	3	2	2				クライアントのOSは、Windows11に対応していること。	○
1	9	3	2	3				利用者認証の認証方式は、「ICカード+パスワード」の二要素認証であること。また、運用を考慮して端末により、「ID+パスワード」での認証も設定可能であること。また、本認証で使用するIDは電子カルテシステムの利用者IDとし、それに紐づいたICカードが利用可能であること。	○
1	9	3	2	4				将来的には、オプションを追加することにより、多様な生体認証やワンタイムパスワードを組合わせた二要素認証にも対応可能なパッケージであること。その際の費用は別途とする。	○
1	9	3	2	5				一人の利用者に対して、複数のアカウント情報（異なるＩＤとパスワード）を登録可能であること。また、各業務アプリケーションごとに、シングルサインオンで使用するＩＤとパスワードを定義可能であること。	○
1	9	3	2	6				上記機能は、当センター職員でメンテナンス可能であること。	○
1	9	3	2	7				利用者の有効期間については、開始日と終了日を設定できること。	○
1	9	3	2	8				端末のOSへのサインインは、共通アカウントを予定しており、当該環境においても、Windows認証同様にWindowsの認証画面を用いたセキュアな認証が可能であること。また、利用者認証後にデスクトップが解放され各システムが利用可能であること。（未認証状態ではデスクトップが利用不可能な状態であること）	○
1	9	3	2	9				将来的な用途も見据え、個人アカウントの端末でも本認証システムが動作可能であること。	○
1	9	3	2	10				利用者認証画面は、Credential Providerを採用し、一部にHTMLを表示することが可能であること。	○
1	9	3	2	11				利用者認証後、指定のスクリプト等の実行が可能であること。	○

別紙１　医療情報システム要求仕様書

								要求仕様	必須
1	9	3	2	12				ロックされている時は、再度、ログイン時と同様の認証を行いロックを解除可能であること。また、別の利用者がログインすることも可能なこと。その場合は、利用中のアプリケーションの終了処理を実行可能であること。	○
1	9	3	2	13				ICカードの情報を認証システムサーバに格納可能であること。当初、ICカードを使用しない場合でも将来的にICカードリーダを追加して運用可能なように標準構成にて機能提供可能であること。	○
1	9	3	2	14				ICカードと利用者の紐づけのための登録ツールが用意されており、登録は、ID+パスワードで本人確認実施後、ICカードをかざして登録可能であること。また、CSVファイルからの一括登録や差分登録可能なツールも提供されること。	○
1	9	3	2	15				ICカード忘れ及び紛失時の対応として仮カード発行（登録）が可能であること。	○
1	9	3	2	16				仮カードに関しては、返却期限の設定が可能であること。また、期限を過ぎた仮カードではログインできないように制御可能であること。	○
1	9	3	2	17				仮カードの貸出履歴が参照可能であること。また、一覧を画面出力及びCSVファイル出力可能であること。	○
1	9	3	2	18				認証システムサーバとクライアント端末間の認証情報の通信は暗号化などの方法によりセキュリティの高い方法を利用していること。	○
1	9	3	2	19				利用者が同時に複数の端末にログインすることができなような利用制限が可能であること。また、設定により複数端末の同時ログインも可能であること。	○
1	9	3	2	20				特定の利用者については上記制限なく、複数の端末に同時にログイン可能な設定が可能であること。	○
1	9	3	3					シングルサインオン機能	
1	9	3	3	1				端末・個人認証後、シングルサインオン機能を利用可能であること。	○
1	9	3	3	2				自動代行入力が可能であること。本機能は、各業務システムのログイン画面に対してＩＤ、パスワード及びログイン等の任意のボタン押下を自動処理可能であること。	○
1	9	3	3	3				自動代行入力用の設定ツールが用意されていること。	○
1	9	3	3	4				自動代行入力の設定は、簡単に設定可能な機能が用意されていること。	○
1	9	3	3	5				上記全てのシングルサインオン機能に関して、１人の利用者に対して複数のＩＤ及びパスワードの管理が可能で、各業務アプリケーションごとに使用するＩＤ及びパスワードを設定可能であること。	○
1	9	3	4					ファイルフォルダ機能	
1	9	3	4	1				アカウント情報連携機能にて新規のアカウント情報を取得した場合、ActiveDirectoryに権限設定し、同時に自動的にファイルサーバに個人用フォルダを作成可能であること。	○
1	9	3	4	2				電子カルテ端末にログインした後、ActiveDirectoryに設定された権限を確認し、個人用フォルダをネットワークドライブとしてマウント可能であること。また、ランチャのボタンやデスクトップのショートカットから参照が可能であること。	○
1	9	3	4	3				共有フォルダは手動でファイルサーバに作成し、ActiveDirectoryへの権限設定も手動で行うが、個人用フォルダ同様、ログイン後、ネットワークドライブとして自動でマウント可能であること。	○

別紙１　医療情報システム要求仕様書

要求仕様									必須
1	9	3	4	4				共有フォルダは手動でファイルサーバに作成し、ActiveDirectoryへの権限設定は職種及び所属をもとに自動で可能であること。個人用フォルダ同様、ログイン後、ネットワークドライブとして自動でマウント可能であること。	○
1	9	3	5					ログ管理機能	
1	9	3	5	1				次のログの取得が可能なこと。 ・端末起動、シャットダウン時刻 ・サービス起動、終了時刻 ・端末利用開始（ログイン）時刻、終了（ログアウト）時刻 ・離席、ロック時刻、ロック解除時刻 ・シングルサインオン対象システムの起動時刻 ・利用者認証時の認証方法（二要素認証か一要素認証か判別可能なこと）	○
1	9	3	5	2				上記ログは、画面で検索し、絞り込みが可能なこと。また、CSV形式のファイルに出力可能なこと。 絞り込みは下記の項目の組み合わせで可能であること。 ・日時指定、範囲指定 ・職員指定 ・端末指定 ・上記の取得可能ログ項目での絞り込み	○
1	9	3	5	3				ログの保存期間は、180日とし、それより古いログはアーカイブし保存可能であり、必要に応じて参照可能であること。	○
1	9	4						マスタ管理機能	
1	9	4	1					利用者マスタ	
1	9	4	1	1				利用者マスタ（利用者ID、パスワード、ICカード情報、職種、権限）が登録可能であること。	○
1	9	4	1	2				一人の利用者に対して、複数のＩＤ、パスワードが異なるアカウント情報を登録可能であること。また、登録可能なアカウント情報は上限が無いこと。	○
1	9	4	1	3				利用者の有効期間については、開始日と終了日を設定できること。	○
1	9	4	1	4				利用者情報が有効か無効かをフラグ管理可能であること。	○
1	9	4	2					動作ポリシー設定	
1	9	4	2	1				端末の動作ポリシーの設定が以下の項目で可能であること。また、本設定は上限無く複数設定可能であること。 ・認証方法（例：一要素、二要素または生体認証の有無等） ・ログイン・ログアウト時に実行するスクリプト及び外部プログラムの指定	○

別紙１　医療情報システム要求仕様書

								要求仕様	必須
1	9	4	2	2				端末の動作ポリシーは以下の指定及び組み合わせで設定可能であること。また、本設定は上限無く複数設定可能であること。 ・端末指定 ・端末グループ ・利用者指定 ・利用者グループ ・端末指定　及び　利用者指定 ・端末指定　及び　利用者グループ ・端末グループ　及び　利用者指定 ・端末グループ　及び　利用者グループ	○
1	9	5						障害対応	
1	9	5	1					障害対応	
1	9	5	1	1				利用者認証において、何らかの理由で利用できない場合に、緊急的に、利用者ID、パスワード入力のみでログインする方法が提供されていること。	○
1	9	5	1	2				上記において、緊急パスワードログイン方法にて認証されてログインした場合には、当センターの指定する警告メッセージが表示されること。	○
1	9	5	1	3				認証サーバに障害が発生した場合は、自動的に本機能を切り替える事によりログインが可能なこと。	○
1	9	5	1	4				利用者を管理するActiveDirectoryが存在する場合は、認証先をActiveDirectoryに自動的に切り替えて継続運用可能であること。また、この場合は、ID＋パスワード認証で可能であること。	○
1	9	6						その他の機能	
1	9	6	1					電子カルテシステム連携機能	
1	9	6	1	1				認証実施後、電子カルテシステムへシングルサインオンが可能であること。	○
1	9	6	1	2				電子カルテシステムからログアウトした場合、ログイン画面に遷移可能であること。	○
1	9	6	1	3				電子カルテシステムの離席操作後、認証システムのロック画面に遷移可能であること。	○
1	9	6	1	4				電子カルテシステムの利用者切替ボタンを押下した場合、認証システムの認証画面に遷移し次の利用者が認証を実施後、次の利用者のログイン済み電子カルテに遷移可能であること。	○
1	9	6	2					その他の機能	
1	9	6	2	1				ログイン時およびログアウト時に任意のスクリプト（バッチやVBScript等）やEXEが実行できる機能を有すること。	○
1	9	6	2	2				端末に導入する認証モジュールについては、自動配信機能などにより更新が可能なこと。	○
1	9	6	2	3				端末で動作する認証機能の動作設定は、認証サーバで集約管理されており端末での作業を実施することなく、認証サーバで設定変更ができること。	○