平成 30 年 2 月 15 日

後期高齢者医療 広域連合電算処理システム

安全性設計書

目次

1 概要 1

2 アクセス制御 3

2.1 ファイルのアクセス制御 3

2.2 データベースのアクセス制御 7

2.3 ファイアウォールによる制御 9

3 ウィルス対策 11

3.1 ウィルス対策ソフトウェアの導入 11

4 暗号化 13

4.1 通信の暗号化 13

5 ユーザ認証 15

5.1 Windows ログイン 15

5.2 二要素認証 18

5.3 標準システム認証 22

5.4 標準システムにおけるパスワードの定期更新とアカウントロック 23

6 不正アクセス 25

6.1 不正端末機器の接続防止 25

1 概要

本書は「後期高齢者医療広域連合電算処理システム(以下、「標準システム」という)」の安全性設計について記載する。

安全性設計の方針は、情報セキュリティの阻害要因から情報資産を守るため、以下の 3 点を念頭に置いている。

・権限のないユーザに情報が漏洩しないこと
・不正アクセスやデータ改ざんによって情報が破壊されないようにすること
・許可された利用者が必要な情報にアクセスできること

本書で説明する内容の一覧を表 1-1 に示す。

表 1-1　本書での説明内容一覧

No.	項目	説明内容
1	アクセス制御	ファイル、ファイアウォールに関わるアクセス制御の方法について記載する。
2	ウィルス対策	システムファイルやデータファイルなどを破壊するコンピュータウィルスへの感染を防止する方法について記載する。
3	暗号化	第三者による通信中のデータの盗聴や改ざんを防止する方法について記載する。
4	ユーザ認証	OS、標準システムに関わるユーザ認証について記載する。
5	不正アクセス	不正端末接続によるデータ漏洩、職員または外部委託事業者などの不正接続による情報資産の流出を防ぐ方法について記載する。

本書では標準システムに関わる業務を実施するグループ/ユーザを以下のように定義する。

表 1-2　グループ/ユーザの定義

No.	グループ名	想定ユーザ
1	広域連合システム管理者	各広域連合のシステム管理者、運用責任者。
2	広域連合システム運用者	各広域連合のシステム運用者。
3	SI ベンダ	業者の保守担当者。
4	広域連合職員	各広域連合に属する職員。
5	市区町村職員	各市区町村に属する職員。

第 2 章以降では、表 1-1 のそれぞれの項目についての詳細を説明する。

【このページは白紙】

2 アクセス制御

本章では、ファイル、ファイアウォールに関わるアクセス制御の方法について記載する。

2.1 ファイルのアクセス制御

(1) 目的

Windows の標準機能を用いて、OS 上のファイルへのアクセスを制限することでサーバおよび端末上の重要な情報の誤操作による消失、改ざんなどのリスクを防ぐことを目的とする。

(2) 概要

各サーバ領域へのアクセス権をユーザ権限ごとに決定する。サーバおよび端末における各領域の定義を以下に示す。

(a) システム領域

OS の動作に関わるファイルが格納されている領域。アプリケーションのインストール/アンインストールなどの作業に関わる領域。

(b) データ領域

標準システムのデータを格納するために使用する領域。

(c) ログ領域

標準システムに関わるアプリケーションログが生成される領域。

(3) 対象範囲

ファイルのアクセス制御の対象範囲を示す。

(a) 広域連合側

広域連合に在籍するグループ/ユーザのアクセス制御の対象範囲を表 2-1 に示す。

表 2-1　グループ/ユーザのアクセス制御の対象範囲（広域連合）

No.	対象	サーバ・端末機器名	実施の有無
1	広域連合	Web サーバ	○
2		AP サーバ	○
3		DB サーバ	○
4		帳票サーバ	○
5		AD サーバ	○
6		運用管理サーバ	○
7		バックアップサーバ	○
8		運用管理端末	○
9		広域端末	○
10		広域端末(一括転送用)	○
11		(検証用)Web サーバ	○
12		(検証用)AP サーバ	○
13		(検証用)DB サーバ	○
14		(検証用)帳票サーバ	○
15		(検証用)端末	○

凡例　○：必須

(b) 市区町村側

市区町村に在籍するグループ/ユーザのアクセス制御の対象範囲を表 2-2 に示す。

表 2-2　グループ/ユーザのアクセス制御の対象範囲（市区町村）

No.	対象	サーバ・端末機器名	実施の有無
1	市区町村	データ連携用機器	○
2		窓口端末	○

凡例　○：必須

(4) 方式

Windows の標準機能を用いて各サーバおよび各端末に、「(5)設定例」で示すような OS 上のファイルへのアクセス権を設定する。

(5) 設定例

(a) 広域連合側

広域連合に在籍するグループ/ユーザのアクセス権の設定例を表 2-3、表 2-4 に示す。

表 2-3　グループ/ユーザのアクセス権の設定例（広域連合/各サーバ）

No.	領域	グループ名	更新権限	参照権限
1	システム領域	広域連合システム管理者	○	○
2		広域連合システム運用者	○	○
3		SI ベンダ	○	○
4		広域連合職員	×	×
5	データ領域	広域連合システム管理者	○	○
6		広域連合システム運用者	○	○
7		SI ベンダ	○	○
8		広域連合職員	×	×
9	ログ領域	広域連合システム管理者	○	○
10		広域連合システム運用者	○	○
11		SI ベンダ	○	○
12		広域連合職員	×	×

凡例　○：必須
　　×：不要

表 2-4　グループ/ユーザのアクセス権の設定例（広域連合/各端末）

No.	領域	グループ名	更新権限	参照権限
1	システム領域	広域連合システム管理者	○	○
2		広域連合システム運用者	○	○
3		SI ベンダ	○	○
4		広域連合職員	○	○
5	データ領域	広域連合システム管理者	○	○
6		広域連合システム運用者	○	○
7		SI ベンダ	○	○
8		広域連合職員	○	○
9	ログ領域	広域連合システム管理者	○	○
10		広域連合システム運用者	○	○
11		SI ベンダ	○	○
12		広域連合職員	○	○

凡例　○：必須

(b) 市区町村側

市区町村に在籍するグループ/ユーザのアクセス権の設定例を表 2-5 に示す。

表 2-5　グループ/ユーザのアクセス権の設定例（市区町村/各端末）

No.	領域	グループ名	更新権限	参照権限
1	システム領域	市区町村職員	○	○
2	データ領域	市区町村職員	○	○
3	ログ領域	市区町村職員	○	○

凡例　○：必須

2.2 データベースのアクセス制御

(1) 目的

データベースにユーザ権限の設定を行う目的は、以下の 2 点が挙げられる。
・ユーザの誤操作※を防ぐ
・不正な操作を行ったユーザをある程度特定し、責任を明確化する

目的を実現するため、標準システムメンテナンス時のデータベース操作などを実行できるユーザ権限を適正に設計する。

※　実行すべきでない作業を誤って実行すること。

(2) 概要

Oracle の標準機能を用いてデータベースへのアクセス権をグループごとに決定し、実行できる作業を限定する。Oracle データベースにおける付与権限の例を表 2-6 に示す。

表 2-6　Oracle データベースにおける付与権限の例

No.	機器	領域	グループ名	更新権限	参照権限
1	DB サーバ	データベース	広域連合システム管理者	○	○
2			広域連合システム運用者	○	○
3			SI ベンダ	○	○
4			広域連合職員	×	×
5			市区町村職員	×	×
6	（検証用）DB サーバ	データベース	広域連合システム管理者	○	○
7			広域連合システム運用者	○	○
8			SI ベンダ	○	○
9			広域連合職員	×	×
10			市区町村職員	×	×

凡例　○：必須
　　×：不要

(3) 対象範囲

データベースのアクセス制御の対象範囲を表 2-7 に示す。

表 2-7　データベースのアクセス制御の対象範囲

No.	対象	サーバ・端末機器名	実施の有無
1	広域連合	Web サーバ	×
2		AP サーバ	×
3		DB サーバ	○
4		帳票サーバ	×
5		AD サーバ	×
6		運用管理サーバ	×
7		バックアップサーバ	×
8		運用管理端末	×
9		広域端末	×
10		広域端末(一括転送用)	×
11		(検証用)Web サーバ	×
12		(検証用)AP サーバ	×
13		(検証用)DB サーバ	○
14		(検証用)帳票サーバ	×
15		(検証用)端末	×
16	市区町村	データ連携用機器	×
17		窓口端末	×

凡例　○：必須
　　×：不要

(4) 方式

Oracle の標準機能を用いて各データベースに、表 2-6 に示すようなアクセス権限を設定する。

2.3 ファイアウォールによる制御

(1) 目的

ファイアウォールによる制御は、外部ネットワークからの不正なアクセスを防ぐことを目的とする。

(2) 概要

ファイアウォールのフィルタリングルールを設定して、許可された IP アドレスおよび必要なプロトコルだけ、外部からアクセスできるようにする。

基本的には、広域連合のシステムにアクセスのある市区町村および広域連合（事務所）の IP アドレスのみ許可する。また、セキュリティを高める上でも、必要とするプロトコル以外のアクセスは拒否する。

中間サーバへの通信は、広域端末および統合専用端末からの接続に対してファイアウォールによる制御を行う。

(a) 広域連合の通信

・標準システムへの通信

広域連合（事務所）の広域端末から広域連合（事務所）のファイアウォール（FW①）および広域連合のファイアウォールを経由して、DMZ の Web サーバへアクセスを行う。

・中間サーバへの通信

広域連合（事務所）の広域端末から広域連合（事務所）のファイアウォール（FW②）および取りまとめ機関のファイアウォールを経由して中間サーバへアクセスを行う。

(b) 市区町村の通信

市区町村の窓口端末およびデータ連携用機器から市区町村のファイアウォールおよび広域連合のファイアウォールを経由して、DMZ の Web サーバへアクセスを行う。

ファイアウォールの通信を図 2-1 に示す。

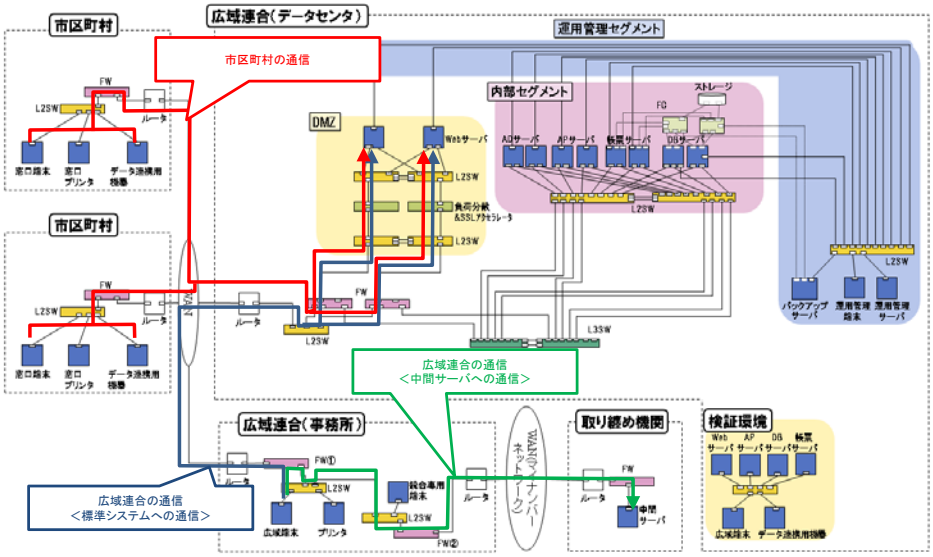

図 2-1　ファイアウォールの通信

(3) 方式

ファイアウォール製品を用いる。ファイアウォールで許可するプロトコル例を表 2-8 に示す。

表 2-8　ファイアウォールで許可するプロトコル例

No.	対象	プロトコル/ポート	説明
1	広域連合の通信 〈標準システムへの通信〉	HTTPS	標準システム接続で使用する。
2		DNS	名前解決で使用する。
3		NTP	時刻同期で使用する。
4		※	資源管理ソフトウェア (資源配布機能)で使用する。
5		※	資源管理ソフトウェア (クライアント制御)で使用する。
6		※	外字管理ソフトウェアで使用する。
7		※	ウィルス対策ソフトウェアで使用する。
8	広域連合の通信 〈中間サーバへの通信〉	HTTP	中間サーバへの接続で使用する。
9		HTTPS	
10	市区町村の通信	HTTPS	標準システム接続で使用する。
11		DNS	名前解決で使用する。
12		NTP	時刻同期で使用する。
13		※	資源管理ソフトウェア (資源配布機能)で使用する。
14		※	資源管理ソフトウェア (クライアント制御)で使用する。
15		※	外字管理ソフトウェアで使用する。

※　資源管理ソフトウェア、外字管理ソフトウェアおよびウィルス対策ソフトウェアで使用するポートについては各広域連合で協議の上設計し、必要であれば LGWAN にポート許可申請を行うこと。

3 ウィルス対策

本章では、システムファイルやデータファイルなどを破壊するコンピュータウィルスへの感染を防止する方法を記載する。

3.1 ウィルス対策ソフトウェアの導入

(1) 目的

ウィルス感染の被害は、ファイルの破壊、個人情報の漏洩、HTML ファイルの改ざんなどが挙げられる。ウィルス対策は、こうした被害を未然に防ぐこと、あるいはウィルス感染してしまった場合に早急にウィルスを削除し被害の拡大を防ぐことを目的とする。

(2) 概要

各サーバおよび各端末にウィルス対策ソフトウェアを導入する。

(3) 対象範囲

ウィルス対策の対象範囲を表 3-1 に示す。

表 3-1　ウィルス対策の対象範囲

No.	対象	サーバ・端末機器名	実施の有無
1	広域連合	Web サーバ	○
2		AP サーバ	○
3		DB サーバ	○
4		帳票サーバ	○
5		AD サーバ	○
6		運用管理サーバ	○
7		バックアップサーバ	○
8		運用管理端末	○
9		広域端末	○
10		広域端末(一括転送用)	○
11		(検証用)Web サーバ	○
12		(検証用)AP サーバ	○
13		(検証用)DB サーバ	○
14		(検証用)帳票サーバ	○
15		(検証用)端末	○
16	市区町村	データ連携用機器	○
17		窓口端末	○

凡例　○：必須

(4) 方式

ウィルス対策ソフトウェアを用いる。

(a) ウィルス定義ファイルの配布

ウィルス定義ファイルは、運用担当者がインターネットに接続可能な端末を使って、次のどちらかの方法で入手し、配布する。

・ウィルス対策ソフトウェアベンダのサイトからダウンロードする
・ベンダから媒体で入手する

i. 広域連合側

①運用管理サーバに、媒体などから最新のウィルス定義ファイルを導入する
②ウィルス定義ファイルを運用管理サーバから広域連合内の各サーバおよび運用管理端末に配布する
③ウィルス定義ファイルを Web サーバから広域端末へ配布する

ii. 市区町村側

①媒体などから窓口端末、データ連携用機器へ配布する

(b) ウィルス検知・削除時の対応

i. 広域連合側

①端末、サーバでウィルスを検知・削除する
②広域端末から Web サーバへ、ウィルス感染情報と処置状況を通知する
③Web サーバ、その他の広域連合内のサーバおよび運用管理端末から運用管理サーバへ、ウィルス感染情報と処置状況を通知する
④ウィルス感染情報と処置状況を運用管理端末で確認する

ii. 市区町村側

①窓口端末、データ連携用機器でウィルスを検知・削除する
②ウィルス感染情報と処置状況を広域連合にメールなどで報告する

4 暗号化

本章では、第三者による通信中のデータの盗聴や改ざんを防止する方法を記載する。

4.1 通信の暗号化

(1) 目的

通信経路上での、盗聴による情報漏洩や通信データの改ざんを防ぐことを目的とする。

(2) 概要

広域連合と市区町村間の通信を SSL により暗号化する。（それ以外の通信に関しては各広域連合のセキュリティポリシーに従うこと）

(3) 対象範囲

広域連合と市区町村間の HTTP プロトコルを用いた通信とする。

(4) 方式

広域連合と市区町村間で行う HTTP プロトコルを用いた通信を、SSL を用いて暗号化する。サーバ証明書は、各広域連合で認証局から購入する必要がある。
また、SSL 暗号化はサーバ負荷軽減のためにアクセラレータを導入する。

【このページは白紙】

5 ユーザ認証

本章では、OS、標準システムに関わるユーザ認証について記載する。

5.1 Windows ログイン

(1) 目的

Windows のユーザの設定を行うことで、許可されていないユーザのログインを防ぐことを目的とする。

(2) 概要

Windows の標準機能を用いて、用途や利用者ごとにユーザを作成し、必要な権限が付与されたユーザでのみログイン可能とする。

(3) 対象範囲

(a) 広域連合側

広域連合に在籍するユーザ設定の対象範囲を表 5-1 に示す。

表 5-1　ユーザ設定の対象範囲（広域連合）

No.	対象	サーバ・端末機器名	設定の有無
1	広域連合	Web サーバ	○
2		AP サーバ	○
3		DB サーバ	○
4		帳票サーバ	○
5		AD サーバ	○
6		運用管理サーバ	○
7		バックアップサーバ	○
8		運用管理端末	○
9		広域端末	○
10		広域端末(一括転送用)	○
11		(検証用)Web サーバ	○
12		(検証用)AP サーバ	○
13		(検証用)DB サーバ	○
14		(検証用)帳票サーバ	○
15		(検証用)端末	○

凡例　○：必須

(b) 市区町村側

市区町村に在籍するユーザ設定の対象範囲を表 5-2 に示す。

表 5-2　ユーザ設定の対象範囲（市区町村）

No.	対象	サーバ・端末機器名	設定の有無
1	市区町村	データ連携用機器	○
2		窓口端末	○

凡例　○：必須

(4) 方式

Windows の標準機能を用いて各サーバおよび各端末に、「(5)設定例」で示すようなユーザを設定する。

(5) 設定例

(a) 広域連合側

広域連合の、各サーバ・端末に登録するユーザ名の例を表 5-3 に示す。

表 5-3　各サーバ・端末に登録するユーザ名の例

No.	グループ名（例）	登録ユーザ名（例）
1	広域連合システム管理者	kkouki01～kkouki03
2	広域連合システム運用者	kunyo01～kunyo03
3	SI ベンダ	kgyosya01～kgyosya03
4	広域連合職員	ukouki01～ukouki03

(b) 市区町村側

市区町村おける各端末に登録するユーザ名の例を表 5-4 に示す。

表 5-4　各端末に登録するユーザ名の例

No.	グループ名（例）	登録ユーザ名（例）
1	市区町村職員	usicho01～usicho03

5.2 二要素認証

(1) 目的

二要素認証を導入することで、なりすましによる不正利用および情報漏洩を防止する。また、利用者のログを正確に残し、不正アクセス監査の精度を高めることを目的とする。

(2) 概要

生体認証、記憶認証、物理認証のうち、二種類の認証方式を組み合わせることで、セキュリティを高める。

(3) 対象範囲

標準システムのシステム構成を図 5-1 に示す。

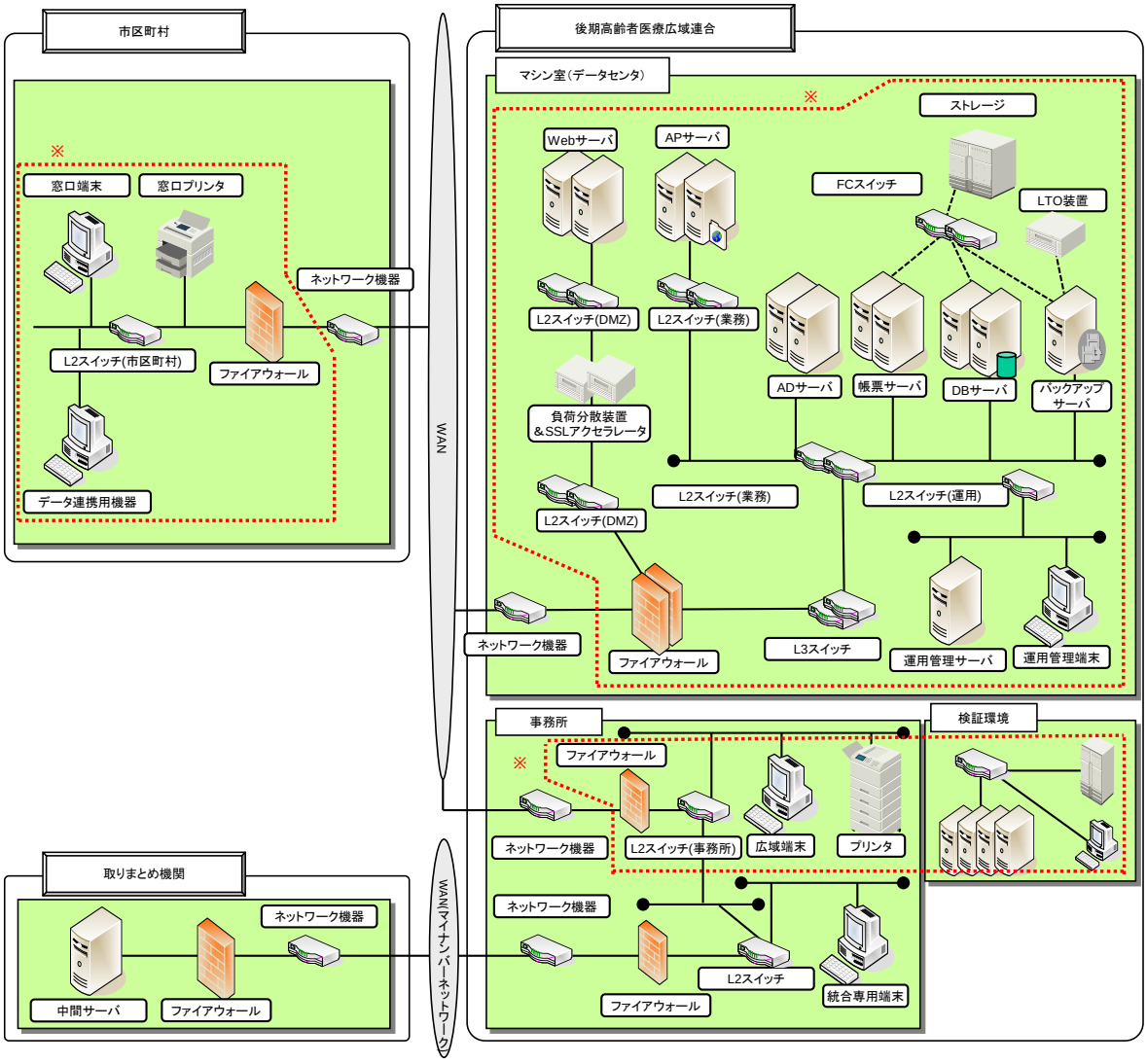

図 5-1　標準システムのシステム構成

※　標準システムの対象範囲を示す。

設置場所も含め、図 5-1 の構成とした場合に、二要素認証を利用する機器の対象範囲を表 5-5 に示す。

表 5-5　二要素認証を利用する機器の対象範囲

No.	対象	サーバ・端末機器名	実施の有無
1	広域連合	Web サーバ	×
2		AP サーバ	×
3		DB サーバ	×
4		帳票サーバ	×
5		AD サーバ	×
6		運用管理サーバ	×
7		バックアップサーバ	×
8		運用管理端末	×
9		広域端末	○
10		広域端末(一括転送用)	○
11		(検証用)Web サーバ	×
12		(検証用)AP サーバ	×
13		(検証用)DB サーバ	×
14		(検証用)帳票サーバ	×
15		(検証用)端末	○
16	市区町村	データ連携用機器	○
16		窓口端末	○

凡例　○：必須
　　×：不要

データ連携用機器については、執務室など不特定多数の利用者がアクセス可能な場所ではなく、データセンタなどセキュリティ対策が施されている場所に設置する場合、この限りではない。

(4) 方式

二要素認証方式については、各広域連合で協議のうえ、決定すること。なお、標準システムのテスト環境における二要素認証方式を以下に示す。

(a) 二要素認証方式

標準システムのテスト環境では、Windows ログイン時に指静脈認証（生体認証）および Windows アカウントでの認証（記憶認証）を用いて二要素認証を行う。

指静脈認証は、指静脈認証管理システム、Web サーバソフトウェアおよび認証に関するデータの格納先としてデータベースを導入することで実現する。

二要素認証を実施するために、標準システムのテスト環境へ導入する製品および理由を表 5-6 に示す。

表 5-6　標準システムのテスト環境へ導入する製品および理由

No.	サーバ	製品	理由
1	Web サーバ	・指静脈認証管理システム ・Web サーバソフトウェア(IIS)	・外部ネットワークからのアクセスとなるため、ファイアウォールによる制御がされている DMZ 内のサーバとする。 ・製品仕様として、Web サーバソフトウェアが必須となることから IIS を導入しているサーバとする。
2	帳票サーバ#2	データベース(SQL Server Express)	・他の SQL Server と競合しないサーバとする。 ・Active Directory 機能との共存が推奨されていないため、AD サーバ以外とする。 ・Active-Standby 構成のため通常時に業務処理が発生しない待機系サーバとする。

標準システムのテスト環境での二要素認証方式を図 5-2 に示す。

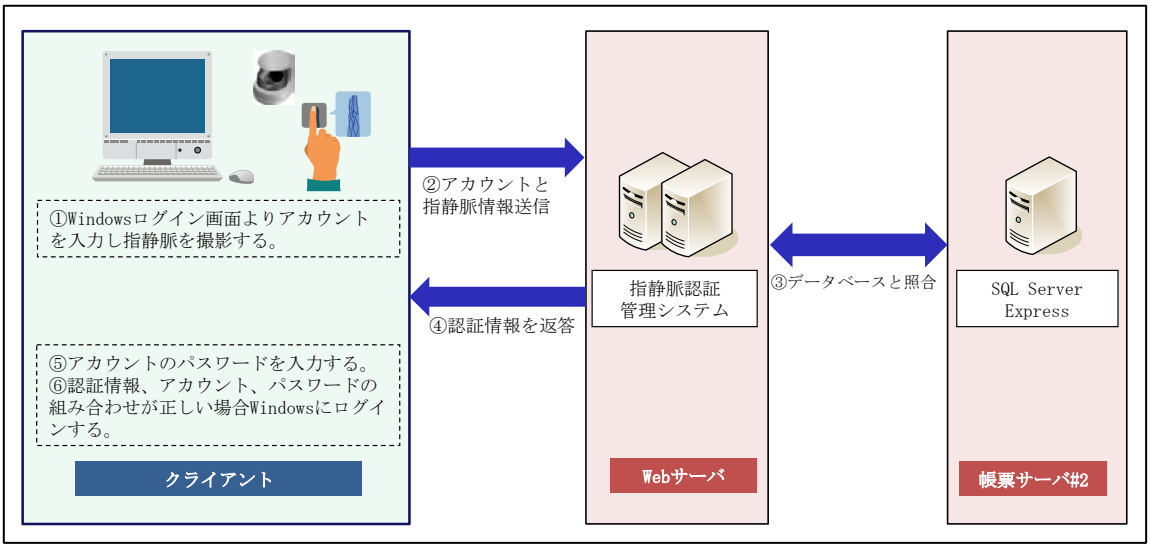

図 5-2　二要素認証方式（標準システムのテスト環境）

(b) 指静脈認証管理システム用データベースアクセス制御

標準システムのテスト環境において、指静脈認証管理システム用のデータベースは、直接ユーザがアクセスして処理を行うことはない。そのため、ユーザグループ種別によるデータベースアクセス制御は管理者ユーザグループのみ許可する。

5.3 標準システム認証

(1) 目的

ユーザ ID/パスワードによる認証機能を実装し、許可されていないユーザの標準システムへのログインを防止することを目的とする。

(2) 概要

標準システムで提供するユーザ認証機能を用いて許可されていないユーザのログインを防止する。

(3) 方式

標準システムで提供するユーザ登録機能を用いて標準システム用のユーザ ID/パスワードを登録する。

5.4 標準システムにおけるパスワードの定期更新とアカウントロック

(1) 目的

パスワードの定期更新促進、連続してパスワードを間違った場合にアカウント停止を行うことにより、不正な利用による情報漏洩などの被害防止を目的とする。

(2) 概要

パスワード情報に対する不正アクセスの対策として、パスワードの定期更新を通知する。また、パスワードを一定回数連続して間違った場合、不正ユーザとみなし、アカウントを停止する。これにより、悪意を持った第三者の不正アクセスに対するセキュリティを高める。

(3) 方式

標準システムに以下の 2 点を実装する。

・パスワードの定期更新を通知する機能
・一定回数連続でパスワードを間違った場合にアカウントを停止する機能

【このページは白紙】

6 不正アクセス

本章では、不正端末接続によるデータ漏洩、職員または外部委託事業者などの不正接続による情報資産の流出を防ぐ方法について記載する。

6.1 不正端末機器の接続防止

(1) 目的

不正持込み端末のネットワーク接続を排除することで、ウィルス被害や情報漏洩などの被害を防止することを目的とする。

(2) 概要

端末機器のネットワークへの接続を防止する。

(3) 対象範囲

市区町村ネットワークおよび広域連合ネットワーク（窓口端末が配置されているセグメント）とする。

(4) 方式

L2 スイッチの未使用ポートをシャットダウンなどにより、不正端末機器の接続を防止する。なお、L2 スイッチの未使用ポートシャットダウン設定については、市区町村側では市区町村で、広域連合（事務所）側では広域連合で行う。

【このページは白紙】