

三重県 デジタル社会推進局  
デジタル改革推進課様

個人番号利用事務系ネットワークにおける  
セキュリティ対策業務

サービス定義書

第初版

2022年10月11日  
ミツイワ株式会社

# 変更履歴

更新日	版	変更内容	承認	査閲	担当
2022/10/11	初版	新規作成			
2023/3/31	1版	ネットワーク構成図修正			

目 次	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	目 次	担当		更新日	版数
						初版

# 第1章 サービス定義

1.1 サービス定義	1
1.1.1 機能を提供するサービス構成	1
(1) パソコン管理機能	1
(2) パソコン認証機能	1
(3) 利用者認証機能	1
(4) パソコン操作ログ記録機能	2
(5) 外部媒体使用制限機能	2
(6) 外部媒体暗号化機能	2
(7) パソコン暗号化機能	3
(8) その他機能	3
(9) バックアップ	3
(10) 稼働監視	3
1.1.2 その他、本業務の提供するサービス	4
(1) アカウント設定	4
(2) セキュリティ対策	4
(3) パソコン及びプリンタの更新	4
(4) Windows OS及びMicrosoft Officeのバージョンアップ作業	4
1.1.3 運用保守	5
(1) 運用業務	5
(2) 保守業務	5
1.1.4 機器の撤去・設定情報及びログ情報等の抽出	5
1.1.5 サービスを提供する各システムのハード構成	6
(1) システム構成図概要	6
(2) システムを構成する機種、OS、サービス	7

目 次	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	目 次	担当		更新日	版数
						初版

1.2 サービス概要

1.2.1 機能

(1) パソコン管理機能

(2) パソコン認証機能

(3) 利用者認証機能

(4) パソコン操作ログ記録機能

(5) 外部媒体使用制限機能

(6) 外部媒体暗号化機能

(7) パソコン暗号化機能

(8) その他機能

(9) バックアップ

(10) 稼働監視

1.2.2 その他、本業務の提供するサービス

(1) アカウント設定

(2) セキュリティ対策

(3) パソコン及びプリンタの更新

(4) Windows OS及びMicrosoft Officeのバージョンアップ作業

1.2.3 運用保守

(1) 運用業務

(2) 保守業務

1.2.4 機器の撤去・設定情報及びログ情報等の抽出

8

8

8

9

10

11

12

12

13

13

14

17

20

20

20

20

21

22

22

24

24

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.1 サービス定義	担当		更新日	
					版数	初版

## 1.1 サービス定義

ここでは、本業務における、根幹となる基本方針を記す。

### 1.1.1 機能を提供するサービス構成

#### (1) パソコン管理機能

提供サービス		提供システム
セキュリティパッチの管理	自治体情報セキュリティ向上プラットフォームから連携サーバを経由し、Microsoftのセキュリティパッチ取得と本ネットワーク内への配信と管理	WSUSサーバ
	WSUSで配信しないMicrosoft製品やAdobe製品のセキュリティパッチの配信と管理	Asset Viewサーバ
ウイルス対策ソフトの管理	自治体情報セキュリティ向上プラットフォームから連携サーバを経由し、パターンファイル取得と本ネットワーク内のウイルス対策サーバやServer Protect for Linuxへの配信	ウイルス対策統合管理サーバ (Trend Micro Apex Central)
	本ネットワーク内のWindowsサーバ/パソコンのウイルス対策及びパターンファイル配信・管理	ウイルス対策サーバ(Apex One)
パソコン情報の取得・出力	本ネットワーク内に接続されるパソコンのインベントリ情報取得	Asset Viewサーバ
プログラム等の配信機能	本ネットワーク内に接続されるパソコンへのプログラムやファイルの配信	Asset Viewサーバ
パソコン設定管理機能	本ネットワーク内に接続されるサーバ/パソコンのグループポリシー設定	Active Directoryサーバ
	本ネットワーク内に接続されるパソコンの不正アプリケーションの禁止	Asset Viewサーバ
リモート操作機能	本ネットワーク内に接続されるパソコンのリモート操作	Asset Viewサーバ

#### (2) パソコン認証機能

提供サービス		提供システム
不正接続の検知	本ネットワーク内に許可されていないパソコンの接続検知	Asset Viewサーバ センサーサーバ/センサーPC
不正パソコン接続の禁止	本ネットワーク内に許可されていないパソコンの接続を拒否	Asset Viewサーバ センサーサーバ/センサーPC
許可パソコンの追加・削除	本ネットワーク内に新たなパソコンの接続許可及び登録削除	Asset Viewサーバ
ログの抽出・分析	本ネットワーク内に接続されるパソコンのウイルス検知や不正接続等の記録	ウイルス対策サーバ(Apex One) Asset Viewサーバ

#### (3) 利用者認証機能

提供サービス		提供システム
認証機能	別ネットワークのActive Directoryサーバとの信頼関係による既存アカウント認証	Active Directoryサーバ
生体認証機能	本ネットワーク内のパソコンを利用する個人の静脈情報を登録し、Windowsアカウントと紐付けたユーザ認証	静脈認証サーバ(AuthConductor) Active Directoryサーバ
	新規利用者の生体情報の収集・登録	静脈認証サーバ(AuthConductor) Active Directoryサーバ
ログの記録・抽出・分析	本ネットワーク内に接続されるパソコン利用時のログイン成功・失敗情報の記録と抽出	静脈認証サーバ(AuthConductor) Active Directoryサーバ

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.1 サービス定義	担当		更新日	
					版数	初版

#### (4) パソコン操作ログ記録機能

提供サービス		提供システム
パソコン操作の記録	本ネットワーク内のパソコンを操作(ログイン/ログオフ/ファイルアクセス)した履歴の記録	AssetViewサーバ
パソコンの不正操作に関する通報	本ネットワーク内のパソコンにて不正操作の恐れがあった場合の通報(運用管理端末への通知)	AssetViewサーバ
エージェント等未インストールパソコンの検出	本ネットワーク内のパソコンにて指定するエージェントの有無を検出	AssetViewサーバ
管理対象パソコンの追加・削除	本ネットワーク内での利用を追加・削除されたパソコン情報の追加・削除	AssetViewサーバ Active Directoryサーバ
ログの抽出・分析	本ネットワーク内に接続されるパソコンにて記録した操作ログの抽出とレポート作成	AssetViewサーバ

#### (5) 外部媒体使用制限機能

提供サービス		提供システム
対象とする外部媒体	本ネットワーク内のパソコンで利用するUSBメモリ及びUSB外付けハードディスクに対し媒体単位での使用許可・禁止等の利用制限	AssetViewサーバ
対象とする外部媒体読み取り書き込み装置	本ネットワーク内のパソコンで利用するCD/DVD/メモリーカード等の読み取り書き込み装置に対する装置単位での使用許可・禁止等の利用制限	AssetViewサーバ
使用可能な媒体の制限	本ネットワーク内のパソコンでの利用を許可された外部媒体、パソコン、利用者の組合せによる使用許可・禁止等の利用制限	AssetViewサーバ
使用可能なパソコンの制限	本ネットワーク内に接続されるパソコンでの外部媒体や外部媒体読み取り・書き込み装置の使用許可・禁止等の利用制限	AssetViewサーバ
使用可能な利用者の制限	本ネットワーク内のパソコンを利用する利用者での外部媒体や外部媒体読み取り・書き込み装置の使用許可・禁止等の利用制限	AssetViewサーバ
許可媒体の追加・削除アクセス権の変更	本ネットワーク内のパソコンにて外部媒体や外部媒体読み取り・書き込み装置の使用許可禁止等の利用申請及び管理者による承認	AssetViewサーバ
使用を拒否した外部媒体に対するログの記録・抽出・分析	本ネットワーク内のパソコンにて外部媒体や外部媒体読み取り・書き込み装置等の不正使用時のログを記録・抽出	AssetViewサーバ

#### (6) 外部媒体暗号化機能

提供サービス		提供システム
外部媒体の暗号化	本ネットワーク内のパソコンで利用するUSBメモリ及びUSB外付けハードディスクに対し情報記録時の暗号化	AssetViewサーバ
パソコンや利用者による制限の緩和	本ネットワーク内に接続されるパソコンや利用者に応じて暗号化機能の利用制限	AssetViewサーバ

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.1 サービス定義	担当		更新日	
					版数	初版

(7) パソコン暗号化機能

提供サービス		提供システム
パソコン暗号化	本ネットワーク内で利用するパソコンのハードディスク全体での暗号化と一元管理	Data Protectionサーバ
対象外フォルダやパソコンの設定	本ネットワーク内で利用するパソコンのハードディスク全体での暗号化の有効化/無効化	Data Protectionサーバ

(8) その他機能

提供サービス		提供システム
名前解決(DNS)	本ネットワーク内で利用するサーバ/パソコンの名前解決	DNSサーバ
時刻同期(NTP)	別ネットワークにて稼働する既存NTPサーバと時刻同期し、本ネットワーク内で利用するサーバ/パソコンの時刻同期	NTPサーバ

(9) バックアップ

提供サービス		提供システム
バックアップ	本ネットワーク内で利用する各サーバのシステム及びデータ(ログ含む)のバックアップを取得	バックアップサーバ
バックアップの取得頻度と世代管理	システムバックアップの日次取得 操作ログ等のバックアップは日次、週次、年次に分けてハードディスク内に取得	バックアップサーバ AssetViewサーバ

(10) 稼働監視

提供サービス		提供システム
稼働監視	本ネットワーク内で稼働する各サーバの死活監視及び故障予兆の検知及び通知	稼働監視中継サーバ
	本ネットワーク内で稼働する各サーバの重要サービスの稼働状況の監視及び通知	稼働監視ツール (System Defender Box: SDB)

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.1 サービス定義	担当		更新日	
					版数	初版

## 1.1.2 その他、本業務の提供するサービス

### (1) アカウント設定

提供サービス	
アカウント設定	三重県より提示される、本システムを利用する為の管理者アカウント及び利用者アカウントの登録

### (2) セキュリティ対策

提供サービス	
セキュリティ対策	本システムにて構成される各サーバ及び運用管理パソコンについても、本システムからセキュリティパッチ及びウイルス対策のパターンファイル等を配信する

### (3) パソコン及びプリンタの更新

提供サービス	
新規パソコンのキッティング	三重県より提供される、新規パソコンに対し本システムを利用可能とするソフトウェア一式を導入する
既存パソコンのデータ移行	現在利用している既存パソコンから三重県から指示されたデータを新規パソコンへコピーする
新規プリンタのキッティング	三重県より提供される、新規プリンタに対し本ネットワーク内で利用可能とする設定を行う
パソコン及びプリンタの交換	三重県より提供される設置情報に基づき、拠点での交換配布を行う
継続利用パソコンの移行	現在利用している既存パソコンに対し本システムを利用可能とするソフトウェア一式を導入する

### (4) Windows OS及びMicrosoft Officeのバージョンアップ作業

提供サービス	
Windows OS及びMicrosoft Officeのバージョンアップ	三重県より指定される、Windows OS及びMicrosoft Officeのバージョンに対し、本システムで利用する必須ソフトウェア全てを対応バージョンに変更を実施する
	本システムにて利用しているすべてのパソコンに対し、Windows OS及びMicrosoft Officeを三重県より指示されたバージョンでクリーンインストールを実施
パソコンのデータ移行	利用しているパソコンから三重県から指示されたデータをバックアップしバージョンアップ後のパソコンへコピーする



第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.1 サービス定義	担当		更新日	
					版数	初版

### 1.1.3 運用保守

#### (1) 運用業務

提供サービス	
各種設定変更見直し	導入後、三重県様からの要望により設定変更、見直しを行う
管理対象パソコン追加・削除時のサーバ設定作業	三重県様からの依頼があった、管理対象パソコンの追加・削除を行う(年度末に限る)
新規パソコンへの本システム利用ソフトウェアの導入支援	ヘルプデスクが実施する、新規パソコンへの本システム利用ソフトウェアの導入支援を行う
本システムの利用者追加・削除時のサーバ設定作業	三重県様からの依頼があった、本システムの新規利用者の追加・削除を行う(年度末に限る)
外部媒体追加・削除時のサーバ設定作業	三重県様からの依頼があった、外部媒体情報の追加・削除を行う(年度末に限る)
セキュリティパッチ情報の提供	本システムで利用するソフトウェアに関するバグフィックス、セキュリティ対応等のパッチリリースに伴う情報提供を行う
セキュリティパッチインストール	本システムで利用するサーバ、パソコンに対し、必要なパッチのインストールを行う
Windows OS大型アップデート対応	本システムで利用するパソコンに対し、年1回程度のWindows OSの大型アップデートを行う
稼働監視	本システムを提供するサーバ等に対し、監視を行う
障害一次切り分け	障害発生時の原因切り分けを行う
障害対応	必要に応じて障害発生拠点へ駆けつけ、不良部位の切り分け・修理・修正・交換を行う
障害後是正措置・予防措置	障害情報をもとに原因を分析し、是正措置・予防措置を行う
マニュアルの改訂	本システム稼働後、必要に応じてドキュメントの修正を行う
月次報告	本システムで提供する各機能の運用状況及び障害状況の報告を行う(定例会の開催・月1回)
操作研修	運用管理担当者及びヘルプデスク向けに本システムの操作研修を行う

#### (2) 保守業務

提供サービス	
電話による障害連絡の受付	三重県様と協議、決定した連絡先において電話による障害連絡の受付を行う
障害機器特定後の機器交換	本システムで利用するハードウェア機器にて障害特定時の機器交換を行う
消耗品等の補充	本システムが安定稼働するのに必要な消耗品の補充を行う

### 1.1.4 機器の撤去・設定情報及びログ情報等の抽出

詳細はサービス概要に記載

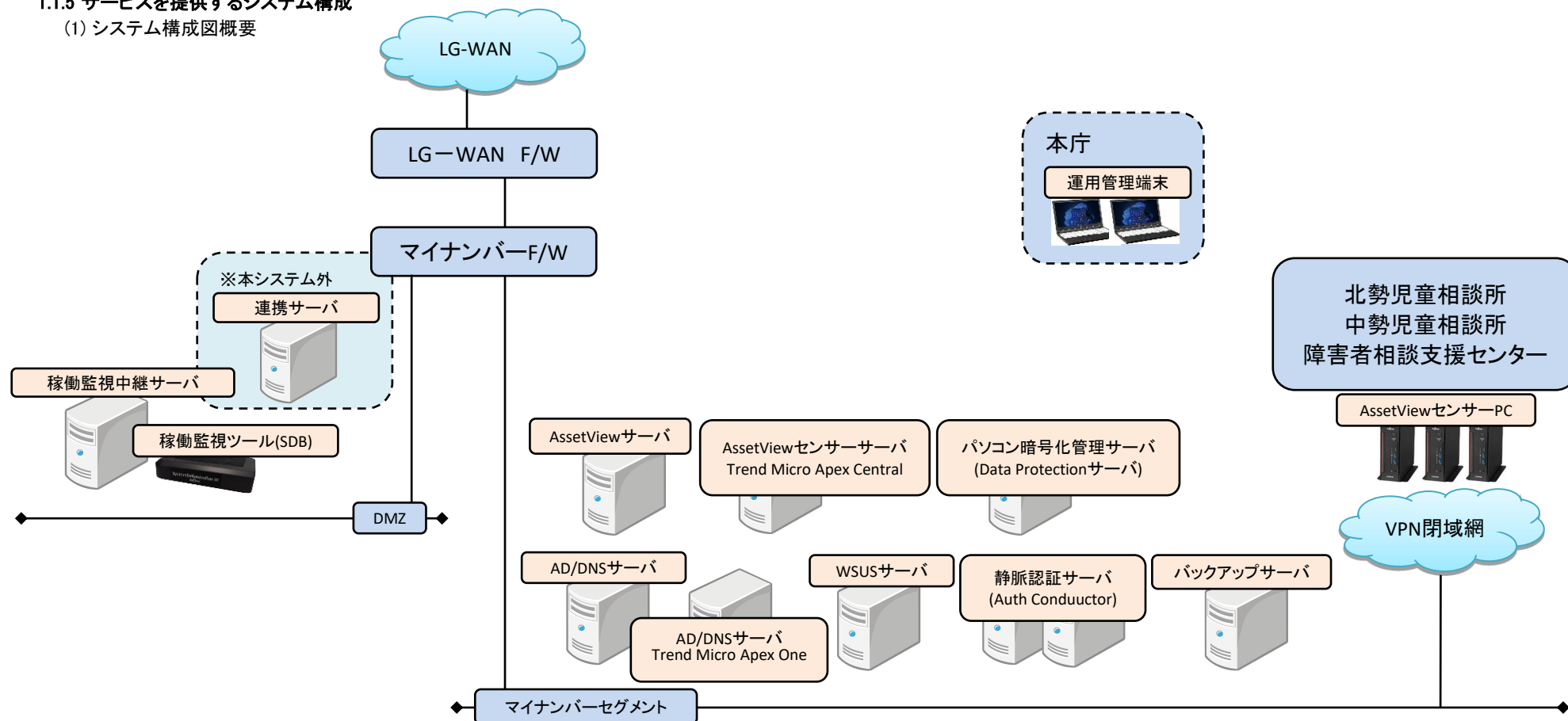
# 第1章 サービス定義

システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務
プロセス	1.1 サービス定義

確認		作成日	2022/10/11
担当		更新日	
		版数	初版

## 1.1.5 サービスを提供するシステム構成

### (1) システム構成図概要



第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.1 サービス定義	担当		更新日	
					版数	初版

(2) システムを構成する機種、OS、サービス

No.	名称	種別	機種	OS	サービスとソフトウェア
1	Active Directoryサーバ1	サーバ	PRIMERGY RX1330 M5	Windows Server 2019 Standard	Active Directory、DNS、NTP
2	Active Directoryサーバ2	サーバ	PRIMERGY RX1330 M5	Windows Server 2019 Standard	Active Directory、DNS、NTP ウイルス対策サーバ(Trend Micro Apex One)
3	WSUSサーバ	サーバ	PRIMERGY RX1330 M5	Windows Server 2019 Standard	WSUSサーバ
4	AssetViewサーバ	サーバ	PRIMERGY RX1330 M5	Windows Server 2019 Standard	端末管理、端末認証、操作ログ記録、外部媒体制御、外部媒体暗号化(Asset View)
5	AssetViewセンサーサーバ	サーバ	PRIMERGY RX1330 M5	Windows Server 2019 Standard	端末認証(Asset View)、ウイルス対策統合管理サーバ(Trend Micro Apex Central)
6	AssetViewセンサーPC1	クライアント	ESPRIMO Q7010/H	Windows10 Professional	端末認証(Asset View)
7	AssetViewセンサーPC2	クライアント	ESPRIMO Q7010/H	Windows10 Professional	端末認証(Asset View)
8	AssetViewセンサーPC3	クライアント	ESPRIMO Q7010/H	Windows10 Professional	端末認証(Asset View)
9	静脈認証サーバ1	サーバ	PRIMERGY RX1330 M5	Windows Server 2019 Standard	利用者認証(Auth Conductor)
10	静脈認証サーバ2	サーバ	PRIMERGY RX1330 M5	Windows Server 2019 Standard	利用者認証(Auth Conductor)
11	パソコン暗号化管理サーバ	サーバ	PRIMERGY RX1330 M5	Windows Server 2019 Standard	端末暗号化(Drive Protection)
12	バックアップサーバ	サーバ	PRIMERGY RX2530 M6	Windows Server 2019 Standard	システムバックアップ(ARCServe Backup)
13	稼働監視中継サーバ	サーバ	PRIMERGY RX1330 M5	Windows Server 2019 Standard	稼働監視(Server View Operation Manager)
14	稼働監視ツール	-	System Defender Box	ubinux Release 14.1相当	プロセス稼働監視
15	運用管理端末1	クライアント	LIFEBLOCK A5512/J	Windows10 Professional	運用管理
16	運用管理端末2	クライアント	LIFEBLOCK A5512/J	Windows10 Professional	運用管理
17	ネットワークスイッチ	スイッチ	SR-S324TL3	-	マイナンバーセグメントとの接続用

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

## 1.2 サービス概要

### 1.2.1 機能

#### (1) パソコン管理機能【AssetView、Windows Server Update Services、Trend Micro Apex Central、Trend Micro Apex One】

- 本機能では以下の機能を提供する。
  - 本ネットワークに接続された端末のソフトウェア情報等の管理
  - 端末へのプログラム、セキュリティパッチ、ウイルス対策ソフトのパターンファイル等の配信
  - リモート操作
- 運用要件を以下とする。
  - ハードウェア、ソフトウェア情報の取得

項目	スケジュール	備考
ハードウェア情報の取得	ログオン時	
ソフトウェア情報の取得	ログオン時	
アラート発生時の検知	インベントリ収集のタイミング	

#### 2)-1 セキュリティパッチの配信

本ネットワーク内にWSUSサーバを設置し、配下の端末にMicrosoftのセキュリティパッチを配信

本ネットワーク内のWSUSサーバは自治体情報セキュリティ向上プラットフォーム上の配信サーバよりセキュリティパッチデータを取得

※セキュリティパッチの取得タイミングは業務ネットワーク側のWSUSサーバの取得タイミングとは時間帯を分ける。

対象端末	取得サーバ	備考
WSUSサーバ	自治体情報セキュリティ向上プラットフォーム上の配信サーバ	
サーバ／パソコン	本ネットワーク内のWSUSサーバ	

#### 2)-2 ウイルス対策ソフトの管理

本ネットワーク内にウイルス対策サーバ(Trend Micro Apex One: Apex One)を設置し、配下の端末にパターンファイルを配信

本ネットワーク内にウイルス対策統合管理サーバ(Trend Micro Apex Central: Apex Central)を設置し、配下のApex Oneサーバ及びServer Protect for Linuxにパターンファイルを配信

本ネットワーク内のApex Centralサーバは自治体情報セキュリティ向上プラットフォーム上の配信サーバよりパターンファイルを取得

※パターンファイルの取得タイミングは業務ネットワーク側のApex Centralサーバの取得タイミングとは時間帯を分ける。

対象端末	取得サーバ	備考
Apex Centralサーバ	自治体情報セキュリティ向上プラットフォーム上の配信サーバ	
Apex Oneサーバ	本ネットワーク内のApex Centralサーバ	配置先: AssetViewセンサーサーバ
Linux系業務サーバ	本ネットワーク内のApex Centralサーバ	配置先: AssetViewセンサーサーバ
Windows系サーバ／クライアント	本ネットワーク内のApex Oneサーバ	配置先: ADサーバ2

#### 3) リモート操作

対象端末	操作端末	備考
Windows系クライアント	運用管理端末によりAssetViewサーバにアクセスしてリモート操作	

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

(2) パソコン認証機能【AssetView】

- 本機能では以下の機能を提供する。
  - 本ネットワークへの接続を許可されていない端末の検知及び接続の拒否
  - 新規接続端末の登録
- 運用要件を以下とする。
  - セグメント毎にセンサーを配置し、不正端末を検知または接続の遮断

対象ネットワーク	制御端末	備考
個人番号利用事務系基幹	AssetViewセンサーサーバ	
北勢児童相談所	AssetViewセンサーPC1	
児童相談センター／中勢児童相談所	AssetViewセンサーPC2	
障害者相談支援センター	AssetViewセンサーPC3	

※本稼働前までは検知モードとし、稼働後は遮断モードにする

2) 新規接続端末の登録

本ネットワーク内に新しく機器を接続するもしくは廃棄する場合は、事前にMACアドレスの登録または削除を実施(管理者への申請)

対象操作	操作端末	備考
端末の登録／削除	運用管理端末1／2	

【管理者への新規端末登録申請の流れ】 ※AssetViewがインストールできない機器を含む

- ①利用者が本ネットワークに接続する機器のMACアドレスを確認
- ②機器情報及び利用理由等を記載した申請書を管理者宛に送付
- ③管理コンソールにて申請内容に基づきIPアドレス、MACアドレスを登録し、許可設定を行う
- ④利用可能となる

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

(3) 利用者認証機能 【Active Directory、Auth Conductor】

- 本機能では以下の機能を提供する。
  - 本ネットワークを利用する際の、Active Directory及び生体（静脈）での認証
  - 利用者情報の管理
- 運用要件を以下とする。
  - 本ネットワーク内の端末を利用する為の認証

項目	認証サーバ	備考
Active Directoryによる利用者認証	Active Directoryサーバ1	
	Active Directoryサーバ2	
生体（静脈）による利用者認証	静脈認証サーバ（仮想ホスト）	ロードバランサーによる代表サーバ
	静脈認証サーバ1	富士通 Auth Conductor
	静脈認証サーバ2	富士通 Auth Conductor

※業務系Active Directoryとは信頼関係のみ

2) 認証情報の登録

Windows認証のIDはADサーバ内の本業務利用者のアカウントを使用  
 静脈認証のIDは個別に登録し、個人の静脈情報とADアカウントとの紐付を行う  
 運用管理者は静脈登録可能な権限が与えられ、静脈登録を行う  
 ACパスワードは静脈認証に不具合がある場合に使用し、都度パスワードを管理者にて登録する。  
 静脈認証システムに未登録のユーザが本業務の端末を利用する場合の一時回避キーは無効化とする。

認証サーバ	認証情報の登録	備考
Active Directoryサーバ1	本業務利用者専用のアカウントを登録	
Active Directoryサーバ2	本業務利用者専用のアカウントを登録	
静脈認証サーバ1	個別IDと静脈の登録	実際の登録は各端末のツールにて行う
静脈認証サーバ2	個別IDと静脈の登録	実際の登録は各端末のツールにて行う

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

(4) パソコン操作ログ記録機能 【AssetView】

- 本機能では以下の機能を提供する。
  - 本ネットワーク内における端末の操作（ログイン、ファイルのコピー、印刷等）の記録
  - アラート情報の検知
- 運用要件を以下とする。
  - 端末の操作内容を記録

項目	ログ収集内容	備考
端末へのログオン／ログオフ	日時、操作端末、利用者情報	
ファイル操作（作成、移動、コピー、印刷等）	日時、操作端末、利用者情報	
外部媒体の接続	日時、操作端末、利用者情報	
通信デバイスの接続	日時、操作端末、利用者情報	
クリップボードの利用	日時、操作端末、利用者情報	

2) アラート情報の検知

特定操作時のアラートを画面上のメッセージ通知と管理者宛て通知（管理画面でのアラート通知）を行う

アラート通知可能項目	アラート設定	アラート通知可能項目	アラート設定
システムドライブの空き容量不足	—	リアルタイムモニター	—
IP アドレス重複	—	ウイルススキャン	—
MAC アドレス重複	—	業務時間外のログイン	—
ドライブの追加	—	ログイン回数超過	—
ハードウェアのネットワーク検知	—	業務対象グループ以外のログイン	—
ハードウェアのネットワーク遮断	—	特定個人情報ファイルの検知	○
使用禁止デバイスの接続	—	個人情報ファイルの検知	○
読み込専用USB デバイスへの書込み	—	機密情報ファイルの検知	○
読み込専用デバイスへの書込み	—	指定ドキュメントファイルの検知	—
ファイル配布/プログラム実行タスクの失敗	—	ファイル操作警告	—
アラートアプリケーションのインストール	—	ファイル操作禁止	—
警告プロセスの起動	—	指定実行ファイルの検知	—
禁止プロセスの起動	—	VPN 接続の未確認機器の遮断	—
停止監視プロセスの停止	—		
ウィンドウタイトル警告	—		

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

(5) 外部媒体使用制限機能 【AssetView】

- 本機能では以下の機能を提供する。
  - 本ネットワーク内における外部媒体の使用可能端末及び使用可能職員を制限
- 運用要件を以下とする。
  - 本ネットワーク内の端末において使用制限される外部媒体

対象となる外部媒体	制限の種類	対象となる外部媒体	制限の種類
CD/DVD/Blu-ray ドライブ	読み専用	ポータブルデバイス	使用禁止
FD/SDカード	使用禁止	MO	使用禁止
USBデバイス等	使用禁止（許可されたUSBメモリを除く）	Wi-Fi	使用禁止
共有フォルダ	書き込み許可	Bluetooth	使用禁止

2) 許可端末及び外部媒体の登録

本ネットワーク内で外部媒体を使用する場合の登録または削除を実施（管理者への申請）

対象操作	操作端末	備考
外部媒体の登録／削除	運用管理端末1／2	

【管理者への外部媒体利用申請の流れ】

- ①利用者が端末に外部媒体を接続
- ②申請画面を表示させ理由記載して申請及び管理者へ連絡
- ③管理コンソールにて申請内容を確認して承認
- ④利用可能となる

(6) 外部媒体暗号化機能 【AssetView】

- 本機能では以下の機能を提供する。
  - 許可された外部媒体への情報記録時の暗号化を実施
- 運用要件を以下とする。
  - 許可された外部媒体への情報書き出し時の暗号化  
本ネットワーク内から外部媒体へ情報をコピーする場合に暗号化を行う  
暗号化時は利用者にてパスワードを設定する



第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

(7) パソコン暗号化機能 【Data Protection(Drive Encryption)】

- 本機能では以下の機能を提供する。
  - 本ネットワーク内における端末への記録情報の暗号化
- 運用要件を以下とする。
  - 端末のハードディスクを暗号化

暗号化対象	暗号化の範囲	備考
各クライアント	端末のハードディスク全体	

2) 起動時の認証

静脈とADアカウント／パスワードによる二要素認証とする為、起動時の認証は不要とする

対象操作	操作内容	備考
起動時の認証画面	無効	

(8) その他機能 【Domain Name System、Network Time Protocol】

- 本機能では以下の機能を提供する。
  - 本ネットワーク内におけるサーバ/パソコンの名前解決
  - 本ネットワーク内におけるサーバ/パソコンの時刻同期
    - 本ネットワーク内にDNSサーバを設置し、配下の端末に本ネットワーク内の名前解決を行う
    - 本ネットワーク内のADサーバはマイナンバーファイアウォールDMZ設置の中継サーバと名前解決を行う
    - 本ネットワーク内にNTPサーバを設置し、配下の端末との時刻同期を行う
    - 本ネットワーク内のADサーバはマイナンバーファイアウォールDMZ設置の中継サーバと時刻同期を行う

対象端末	取得サーバ	備考
DNSサーバ	マイナンバーファイアウォールDMZのDNSサーバ	配置先:ADサーバ1／2
NTPサーバ	マイナンバーファイアウォールDMZのNTPサーバ	配置先:ADサーバ1／2

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

(9) バックアップ 【Windows Server Backup、ARCServe Backup、Asset View】

- ・ 本機能では以下の機能を提供する。
  - 1) 本ネットワーク内で利用する各サーバのシステム及びデータ(ログ含む)のバックアップ
- 1) 基本要件
  - ・ バックアップに関する要件
  - a) バックアップ範囲
 

本業務を構築するシステムの各サーバのバックアップを取得する。
  - b) バックアップの種類
 

システムバックアップ: Windows OSのリカバリ用にWindows Server Backupにてシステム全体のバックアップを取得する。  
 データバックアップ: 各システムのデータリカバリ用にARCServe Backupにて各システムデータのバックアップを取得する。
  - c) バックアップデータの管理
 

バックアップはバックアップサーバのHDDに取得。システム全体のバックアップは原則1世代、データは原則2世代とする。

2) バックアップ容量

サーバ	システム領域	データ領域	備考
ADサーバ1	最大30GB想定	-	
ADサーバ2	最大30GB想定	最大:15GB想定	
WSUSサーバ	最大30GB想定	最大:500GB想定	
AssetViewサーバ	最大30GB想定	最大:300GB想定	
AssetViewセンサーサーバ	最大30GB想定	最大:30GB想定	
静脈認証サーバ1	最大30GB想定	最大:200GB想定	
静脈認証サーバ2	最大30GB想定	最大:20GB想定	
端末暗号化管理サーバ	最大40GB想定	最大:50GB想定	
バックアップサーバ	最大30GB想定	-	
稼働監視中継サーバ	最大30GB想定	-	

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

### 3) バックアップポリシー

- ・OSを含むシステム全体のバックアップはWindows Server Backupにてバックアップサーバの個別フォルダへ週一回バックアップを取得。
  - ・システムに重要な機能を持つサーバについては、別途ARCServeにてバックアップサーバの個別フォルダへ週一回のフルバックアップと毎日の差分バックアップを取得。
  - ・インベントリ情報や操作ログについては、AssetViewの機能でDBバックアップを取得する。(5世代保存)
- また、DBは約1年間(370日)毎に削除するが、1年毎にバックアップデータを別ドライブにコピーバックアップを取得する。

サーバ	種類	ソフトウェア	取得周期	取得先	世代	備考
ADサーバ1	システムバックアップ	Windows Server Backup	週1回(土曜 4:00)	バックアップサーバ	1	リカバリ用
ADサーバ1	ADデータフルバックアップ	ARCServe Backup	週1回(土曜 23:00)	バックアップサーバ	2	リカバリ用
ADサーバ1	ADデータバックアップ	ARCServe Backup	毎日差分( 1:00)	バックアップサーバ	2	リカバリ用
ADサーバ2	システムバックアップ	Windows Server Backup	週1回(土曜 6:00)	バックアップサーバ	1	リカバリ用
ADサーバ2	AD/Corpデータフルバックアップ	ARCServe Backup	週1回(土曜 0:00)	バックアップサーバ	2	リカバリ用
ADサーバ2	AD/Corpデータバックアップ	ARCServe Backup	毎日差分( 1:30)	バックアップサーバ	2	リカバリ用
WSUSサーバ	システムバックアップ	Windows Server Backup	週1回(土曜 8:00)	バックアップサーバ	1	リカバリ用
WSUSサーバ	WSUSデータフルバックアップ	ARCServe Backup	週1回(日曜 23:00)	バックアップサーバ	2	リカバリ用
WSUSサーバ	WSUSデータバックアップ	ARCServe Backup	毎日差分( 2:00)	バックアップサーバ	2	リカバリ用
AssetViewサーバ	システムバックアップ	Windows Server Backup	週1回(土曜 10:00)	バックアップサーバ	1	リカバリ用
AssetViewサーバ	AssetViewデータバックアップ	AssetView DB Backup	週1回(月曜 23:00)	ローカルドライブ	5	保管/過去閲覧用
AssetViewサーバ	AssetViewデータバックアップ	データコピー	年1回(1月2日 2:00)	ローカルドライブ	5	保管/過去閲覧用
AssetViewサーバ	AssetViewデータフルバックアップ	ARCServe Backup	週1回(月曜 0:00)	バックアップサーバ	2	リカバリ用
AssetViewサーバ	AssetViewデータバックアップ	ARCServe Backup	毎日差分( 2:30)	バックアップサーバ	2	リカバリ用
AssetViewセンサーサーバ	システムバックアップ	Windows Server Backup	週1回(土曜 12:00)	バックアップサーバ	1	リカバリ用
AssetViewセンサーサーバ	Apex Centralデータフルバックアップ	ARCServe Backup	週1回(火曜 23:00)	バックアップサーバ	2	リカバリ用
AssetViewセンサーサーバ	Apex Centralデータバックアップ	ARCServe Backup	毎日差分( 3:00)	バックアップサーバ	2	リカバリ用
静脈認証サーバ1	システムバックアップ	Windows Server Backup	週1回(土曜 14:00)	バックアップサーバ	1	リカバリ用
静脈認証サーバ1	静脈認証データフルバックアップ	ARCServe Backup	週1回(水曜 23:00)	バックアップサーバ	2	リカバリ用
静脈認証サーバ1	静脈認証データバックアップ	ARCServe Backup	毎日差分( 3:30)	バックアップサーバ	2	リカバリ用
静脈認証サーバ2	システムバックアップ	Windows Server Backup	週1回(土曜 16:00)	バックアップサーバ	1	リカバリ用
静脈認証サーバ2	静脈認証データフルバックアップ	ARCServe Backup	週1回(木曜 23:00)	バックアップサーバ	2	リカバリ用
静脈認証サーバ2	静脈認証データバックアップ	ARCServe Backup	毎日差分( 4:00)	バックアップサーバ	2	リカバリ用
端末暗号化管理サーバ	システムバックアップ	Windows Server Backup	週1回(土曜 18:00)	バックアップサーバ	1	リカバリ用
端末暗号化管理サーバ	暗号化情報データフルバックアップ	ARCServe Backup	週1回(金曜 23:00)	バックアップサーバ	2	リカバリ用
端末暗号化管理サーバ	暗号化情報データバックアップ	ARCServe Backup	毎日差分( 4:30)	バックアップサーバ	2	リカバリ用
バックアップサーバ	システムバックアップ	Windows Server Backup	週1回(日曜 23:00)	ローカルドライブ	1	リカバリ用
稼働監視中継サーバ	システムバックアップ	Windows Server Backup	週1回(日曜 23:00)	ローカルドライブ	1	リカバリ用

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

#### 4)リストアポリシー

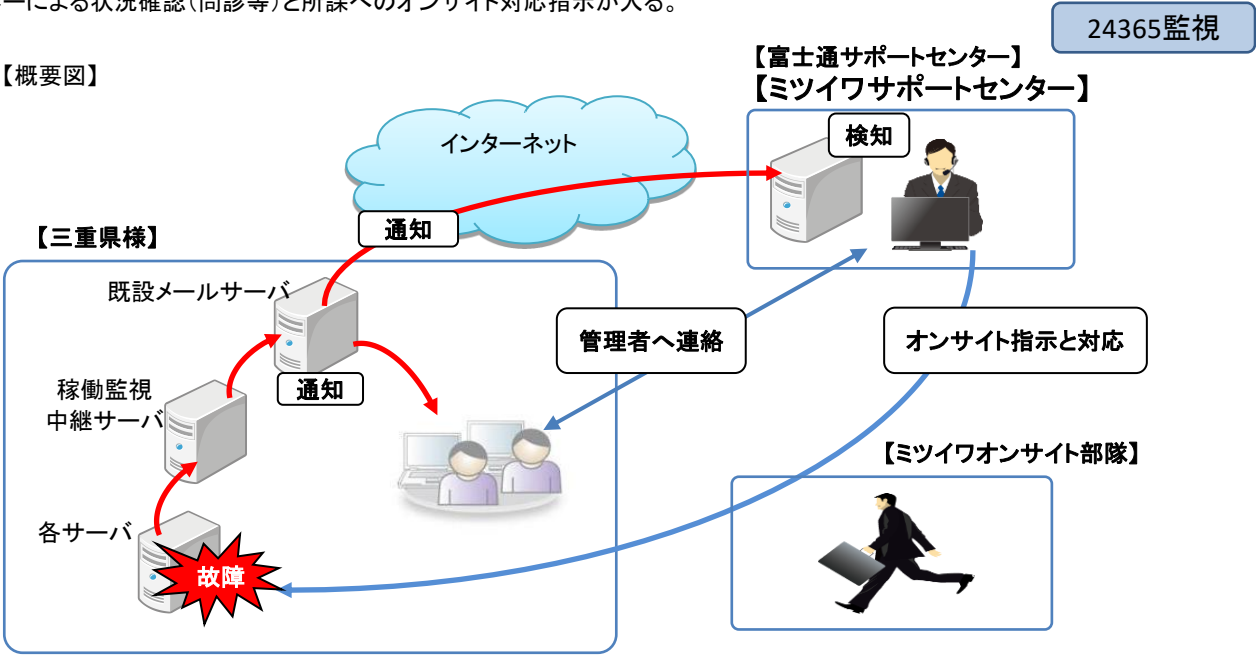
- 全てのデータはバックアップデータから復旧を行う。
- システムの復旧については、OSのメディアから起動し回復コンソールにて復旧を行う。
- データの復旧については、ARCServeにてリストアを行う。

サーバ	種類	ソフトウェア	利用シーン	いつまで戻るか	備考
ADサーバ1	システムバックアップ	Windows Server Backup	OS障害時	1週間前	
ADサーバ1	ADデータフルバックアップ	ARCServe Backup	全HDD故障時	1週間前	
ADサーバ1	ADデータバックアップ	ARCServe Backup	一部データ消去	1日前	
ADサーバ2	システムバックアップ	Windows Server Backup	OS障害時	1週間前	
ADサーバ2	AD/Corpデータフルバックアップ	ARCServe Backup	全HDD故障時	1週間前	
ADサーバ2	AD/Corpデータバックアップ	ARCServe Backup	一部データ消去	1日前	
WSUSサーバ	システムバックアップ	Windows Server Backup	OS障害時	1週間前	
WSUSサーバ	WSUSデータフルバックアップ	ARCServe Backup	全HDD故障時	1週間前	
WSUSサーバ	WSUSデータバックアップ	ARCServe Backup	一部データ消去	1日前	
AssetViewサーバ	システムバックアップ	Windows Server Backup	OS障害時	1週間前	
AssetViewサーバ	AssetViewデータバックアップ	AssetView DB Backup	過去データ閲覧(直近)	1週間前	
AssetViewサーバ	AssetViewデータバックアップ	データコピー	過去データ閲覧	1年前	
AssetViewサーバ	AssetViewデータフルバックアップ	ARCServe Backup	全HDD故障時	1週間前	
AssetViewサーバ	AssetViewデータバックアップ	ARCServe Backup	一部データ消去	1日前	
AssetViewセンサーサーバ	システムバックアップ	Windows Server Backup	OS障害時	1週間前	
AssetViewセンサーサーバ	Apex Centralデータフルバックアップ	ARCServe Backup	全HDD故障時	1週間前	
AssetViewセンサーサーバ	Apex Centralデータバックアップ	ARCServe Backup	一部データ消去	1日前	
静脈認証サーバ1	システムバックアップ	Windows Server Backup	OS障害時	1週間前	
静脈認証サーバ1	静脈認証データフルバックアップ	ARCServe Backup	全HDD故障時	1週間前	
静脈認証サーバ1	静脈認証データバックアップ	ARCServe Backup	一部データ消去	1日前	
静脈認証サーバ2	システムバックアップ	Windows Server Backup	OS障害時	1週間前	
静脈認証サーバ2	静脈認証データフルバックアップ	ARCServe Backup	全HDD故障時	1週間前	
静脈認証サーバ2	静脈認証データバックアップ	ARCServe Backup	一部データ消去	1日前	
端末暗号化管理サーバ	システムバックアップ	Windows Server Backup	OS障害時	1週間前	
端末暗号化管理サーバ	暗号化情報データフルバックアップ	ARCServe Backup	全HDD故障時	1週間前	
端末暗号化管理サーバ	暗号化情報データバックアップ	ARCServe Backup	一部データ消去	1日前	
バックアップサーバ	システムバックアップ	Windows Server Backup	OS障害/一部データ消去	1週間前	
バックアップサーバ	リカバリディスク	ServerViewSuite	全HDD故障時	新規構築	
稼働監視中継サーバ	システムバックアップ	Windows Server Backup	OS障害/一部データ消去	1週間前	
稼働監視中継サーバ	リカバリディスク	ServerViewSuite	全HDD故障時	新規構築	

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

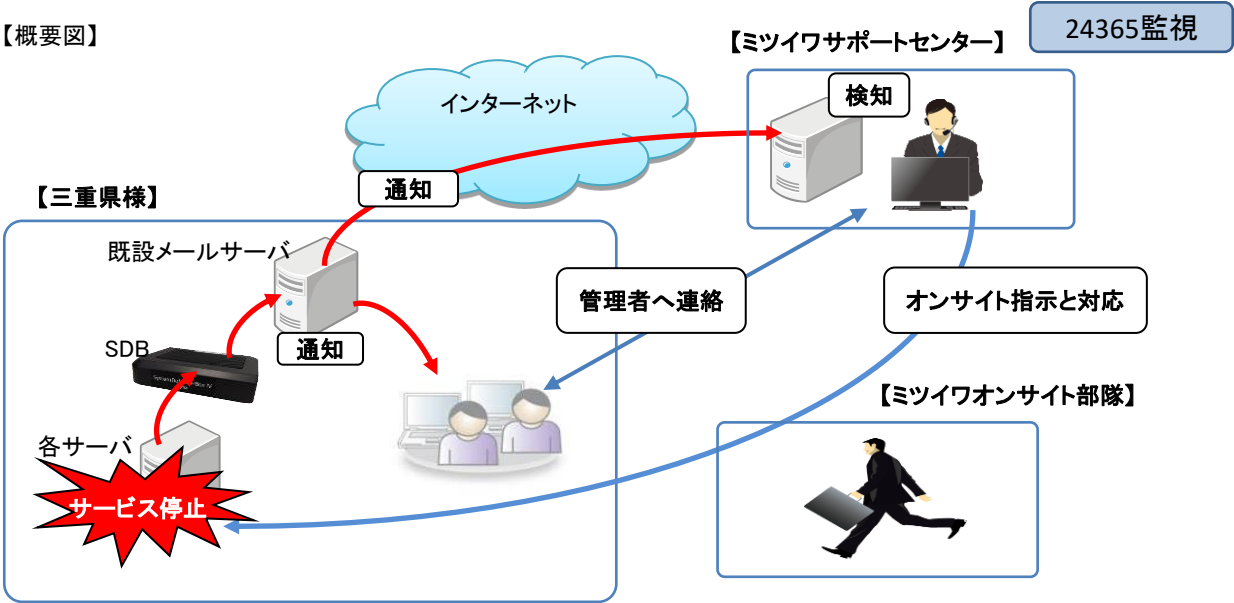
(10) 稼働監視 【Server View Operation Manager、System Defender Box】

- 本機能では以下の機能を提供する。
  - 【24時間365日での監視対応とする】
  - 1) 本ネットワーク内で稼働する各サーバの死活監視及び故障予兆の検知及び通知
  - 2) 本ネットワーク内で稼働する各サーバの重要サービスの稼働状況の監視及び通知
- 1) ハードウェアの故障発生(予兆を含む)時には、装置前面の故障ランプが点灯し、Serverviewにて管理者様と富士通サポートセンターへ自動通知される。その後、富士通サポートセンターによる状況確認(問診等)と所課へのオンサイト対応指示が入る。



第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

- 2) ソフトウェアの故障発生時には、プロセス監視しているSDBにて管理者様とミツイワサポートセンターへ自動通知される。  
 その後、ミツイワサポートセンターによる状況確認(問診等)と所課へのオンサイト対応指示が入る。



第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

### 3) ServerView 監視項目

システム名称	死活監視	部品故障 CPU/MEM/FAN等	HDD故障予兆	備考
ADサーバ1	○	○	○	
ADサーバ2	○	○	○	
WSUSサーバ	○	○	○	
AssetViewサーバ	○	○	○	
AssetViewセンサーサーバ	○	○	○	
静脈認証サーバ1	○	○	○	
静脈認証サーバ2	○	○	○	
端末暗号化管理サーバ	○	○	○	
バックアップサーバ	○	○	○	
稼働監視中継サーバ	-	○	○	
センサーPC1	-	-	-	
センサーPC2	-	-	-	
センサーPC3	-	-	-	
稼働監視ツール(SDB)	-	-	-	

### 4) SDB 監視項目

システム名称	死活監視	プロセス監視 (特定プログラム)	イベントログ監視 (エラーメッセージ)
ADサーバ1	○	○	○
ADサーバ2	○	○	○
WSUSサーバ	○	○	○
AssetViewサーバ	○	○	○
AssetViewセンサーサーバ	○	○	○
静脈認証サーバ1	○	○	○
静脈認証サーバ2	○	○	○
端末暗号化管理サーバ	○	○	○
バックアップサーバ	○	○	○
稼働監視中継サーバ	○	○	○
センサーPC1	○	-	-
センサーPC2	○	-	-
センサーPC3	○	-	-
稼働監視ツール(SDB)	○	-	-
本システム用スイッチ	○	-	-
マイナンバーファイアウォール	○	-	-
拠点VPNルータ(DC及び3拠点)	○	-	-
DMZ中継サーバ	○	-	-

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

5) メール通報情報

メール通知先	送信元アドレス	メールサーバ	備考
富士通サポートセンター	外部発信可能なメールアドレス	業務系メールサーバ	
ミツイワサポートセンター	外部発信可能なメールアドレス	業務系メールサーバ	
三重県デジタル改革推進課	外部発信可能なメールアドレス	業務系メールサーバ	

1.2.2 その他、本業務の提供するサービス

(1) アカウント設定

アカウント種別	登録先ドメイン	登録対象サーバ	備考
個人番号ドメインアカウント	個人番号ドメイン	個人番号NW用ADサーバ1/2	パスワード初回変更必須

(2) セキュリティ対策

種別	配信サーバ	対象システム
セキュリティパッチの配信	WSUSサーバ	本システムにて構成する以下のサーバ及びパソコン ADサーバ1/2、WSUSサーバ、AssetViewサーバ、AssetViewセンサーサーバ、静脈認証サーバ1/2 端末暗号化管理サーバ、バックアップサーバ、センサーPC1/2/3、運用管理端末1/2 稼働監視中継サーバ
ウイルス対策パターンファイルの配信	ApexOneサーバ	本システムにて構成する以下のサーバ及びパソコン ADサーバ1/2、WSUSサーバ、AssetViewサーバ、AssetViewセンサーサーバ、静脈認証サーバ1/2 端末暗号化管理サーバ、バックアップサーバ、センサーPC1/2/3、運用管理端末1/2 稼働監視中継サーバ

(3) パソコン及びプリンタの更新

項目	対象機器	作業内容	留意事項
新規パソコンのキッティング	新規購入パソコン	Windows10 Proのインストール	OSの初期設定内容、プロダクトキーの準備
		Microsoft Office 2016 Std/Proのインストール	Proの選定、プロダクトキーの準備
		イメージ展開	個別設定の準備(ホスト名、IPアドレス)
		本システム利用必須ソフトウェアのインストール (ApexOne、AssetView、DriveEncryption、PalmSecure)	検証用パソコンの準備
既存パソコンのデータ移行	更新対象のパソコン	原則利用者によるバックアップと復元を実施 (利用者にて対応時の支援実施)	三重県が指定するデータ、複数利用者の有無 利用者アカウント、個人データ保存の有無
新規プリンタのキッティング	新規購入プリンタ	ネットワーク設定	個別設定の準備(IPアドレス)



第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

(3) パソコン及びプリンタの更新(つづき)

項目	対象機器	作業内容	留意事項
パソコン及びプリンタの交換	新規購入パソコン	県庁にて搭載した新規購入機器の運搬	各設置場所での作業場所の確保
	更新対象のパソコン	作業場所で更新対象の機器を受け取りデータ移行	
	新規購入プリンタ	設定完了した新規購入機器の引き渡し	
	更新対象のプリンタ	更新完了した対象機器の県庁への運搬	開庁時間内に引き上げてくる
継続利用パソコンの移行	継続利用するパソコン	本システム利用必須ソフトウェアのインストール (ApexOne、AssetView、DriveEncryption、PalmSecure)	Windows10の機能アップデートが必要

【履行場所】

本庁、吉田山会館、桑名庁舎、四日市庁舎、鈴鹿庁舎、津庁舎、松阪庁舎、伊勢庁舎、伊賀庁舎、尾鷲庁舎、熊野庁舎、北勢児童相談所、中勢児童相談所、障害者相談支援センター

(4) Windows OS及びMicrosoft Officeのバージョンアップ作業(令和7年度を想定)

項目	対象機器	作業内容	留意事項
Windows OS及びMicrosoft Officeのバージョンアップ及びパソコンのデータ移行	本システムを利用する全パソコン	三重県が指定するWindowsOSのバージョンに対し本システムの各ソフトウェアの対応状況を確認 (ApexOne、AssetView、DriveEncryption、PalmSecure)	
		上記で確認した結果をもとに各ソフトウェアの対応実施 (ApexOne、AssetView、DriveEncryption、PalmSecure)	
		三重県が用意する検証パソコンにWindowsOS及びMS-Officeをインストール	
		本システム利用必須ソフトウェアのインストール (ApexOne、AssetView、DriveEncryption、PalmSecure)	
		動作検証	
		新規にWindowsOS及びMS-Officeのインストール	プロダクトキーの準備
		イメージ取得(MS-Officeによって分ける想定)	
		各設置場所を対象パソコンの受け取り	各設置場所での作業場所の確保
		三重県の指定するユーザデータの取得 (デスクトップ、ドキュメント、MS-Edge、お気に入り等を想定)	
		各設置場所でのイメージ展開	
		本システム利用必須ソフトウェアのインストール (ApexOne、AssetView、DriveEncryption、PalmSecure)	
		取得したユーザデータをコピー	
		設定完了したパソコンの引き渡し	

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

### 1.2.3 運用保守

#### (1) 運用業務

項目	作業内容
各種設定変更見直し	本システム稼働後に発生した課題に対して設定変更の可否を三重県と検討 検討した結果にもとづき、各システムの設定変更を行う 設定変更した内容をドキュメントに修正反映する
管理対象パソコン追加・削除時のサーバ設定作業 (年度末作業)	三重県から提示される、管理対象パソコンの追加・削除情報を取得 運用管理端末にてAssetView管理コンソールを起動する 追加・削除情報からMACアドレスとIPアドレス、ホスト名をAssetViewに登録・削除を行う
新規パソコンへの本システム 利用ソフトウェアの導入支援	ヘルプデスクが実施する、新規パソコンへの本システム利用ソフトウェアの導入支援を行う
本システムの利用者追加・削除時のサーバ設定作業 (年度末作業)	三重県から提示される、本システム利用者の追加・削除情報を取得 運用管理端末にてAssetView管理コンソールを起動する 利用者の拠点のパソコンにリモート接続して静脈登録用ツールを起動 新規利用者による静脈登録を行っていただく 運用管理端末にて静脈登録ツールを起動 削除情報にもとづき、不要な静脈情報を削除
外部媒体追加・削除時のサーバ 設定作業 (年度末作業)	三重県から提示される、外部媒体の追加・削除情報を取得 運用管理端末にてAssetView管理コンソールを起動する 追加・削除情報から外部媒体情報をAssetViewに登録・削除を行う
セキュリティパッチ情報の提供	定期的に提供されるMicrosoftのセキュリティパッチ情報を取得 不定期に提供される本システムを構成するソフトウェアのセキュリティパッチ情報を取得 (ApexOne、AssetView、DriveEncryption、PalmSecure) 取得した情報は定例会(月1回)で三重県に提供する(重要な緊急パッチ等は都度提供)
セキュリティパッチインストール	提供したセキュリティパッチ情報にもとづき、三重県と適用可否を検討する 検討結果にもとづき、必要なパッチを入手する パッチ適用にあたり改修有無を確認し、三重県と検討する 検討結果にもとづき、パッチを適用する
Windows OS大型アップデート対応	本システムで利用するパソコンのWindows OS大型アップデート情報を取得 WindowsOS大型アップデートプログラムを入手し、三重県に提供する 三重県が用意する検証パソコンに大型アップデートプログラムを適用し、動作検証を行う AssetViewの配布機能を利用し、大型アップデートプログラムを本システムを利用するパソコンに配布する 三重県及びヘルプデスクが行うアップデート及び利用者からの問い合わせ対応の支援を行う

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

(1) 運用業務(つづき)

項目	作業内容	
稼働監視	本システムを構成するサーバ等に対し、24時間365日の死活監視と故障予兆監視を行う	
	監視対象機器は、本資料1.2.1(10) 稼働監視に記載のシステム	
	故障予兆は富士通サポートセンター、死活監視はミツイワサポートセンターにて受付	
	上記にて受け付け後、本プロジェクト担当者に連絡が入り、緊急対応の可否を判断	
	本プロジェクト担当者より三重県に連絡し、緊急対応の検討	
	本プロジェクト担当者よりオンサイトサポート要員へ出動要請を行う	
障害一次切り分け	発生した障害内容を確認し、障害切り分けを行う	
	必要に応じて障害発生拠点へ駆けつけ、調査資料を収集する	
	切り分けた障害原因を三重県に報告する	
障害対応	障害対応時間は原則、開庁日の9:00～17:00とするが、重要システムの障害の場合はこの限りではない	
	必要に応じて障害発生拠点へ駆けつけ、不良部位の切り分け・修理・修正・交換を行う	
	ソフトウェアやデータが破損した場合には、バックアップより復旧を行う	
	対応完了後に三重県に報告する	
障害後是正措置・予防措置	発生した障害内容から是正・予防措置を検討し三重県に報告する	
	三重県と検討した結果にもとづき、必要となる是正・予防措置を行う	
マニュアルの改訂	本システム稼働後、運用に変更があった場合、三重県に報告しドキュメントの修正を行う	
	ドキュメントの修正にあたっては、履歴管理を行う	
月次報告	本システムで提供する各機能の運用状況及び障害状況の報告を行う(定例会の開催・月1回)	
	暫定として前月末までのサービス状況を取りまとめ、当月の第三火曜日に報告を行う	
	運用状況の報告内容について ※レポート出力可能なものに限る	
	パソコン管理機能	セキュリティパッチ未適用PC一覧、ApexOne/パターンファイル未適用PC一覧
	パソコン認証機能	不許可接続となった検知PC一覧、ウイルス検知状況一覧
	利用者認証機能	パソコンのログイン成功・失敗状況一覧
	パソコン操作ログ記録機能	不正操作検知状況一覧
	外部媒体使用制限機能	外部媒体不正利用状況一覧、外部媒体登録状況一覧
	パソコン暗号化機能	HDD未暗号化PC一覧
	バックアップ	バックアップ取得成功・失敗状況一覧
	稼働監視	死活監視・故障予兆の検知状況一覧
	障害対応	対応した障害の原因・対処・是正措置・予防措置状況一覧
	課題管理	各機能の課題に対する進捗管理の状況一覧

第1章 サービス定義	システム	個人番号利用事務系ネットワークにおけるセキュリティ対策業務	確認		作成日	2022/10/11
	プロセス	1.2 サービス概要	担当		更新日	2023/03/31
					版数	初版

(1) 運用業務(つづき)

項目	作業内容	
操作研修	年2回を上限とし、運用管理担当者及びヘルプデスク向けに本システムの操作研修を行う	
	操作研修内容について	
	パソコン管理機能	新規パソコンへの本システム利用ソフトウェアのインストール手順
	パソコン認証機能	新規パソコンの本ネットワークへの接続手順
	利用者認証機能	新規利用者の静脈登録手順
	パソコン操作ログ記録機能	AssetViewサーバ管理コンソールにてアラート確認手順
	外部媒体使用制限機能	外部媒体利用制限設定手順、外部媒体登録手順
	パソコン暗号化機能	暗号化パスワード初期化手順

(2) 保守業務

項目	作業内容
電話による障害連絡の受付	三重県様と協議、決定した連絡先において電話による障害連絡の受付を行う
障害機器特定後の機器交換	本システムで利用するハードウェア機器にて障害特定時の機器交換を行う
消耗品等の補充	本システムが安定稼働するのに必要な消耗品の補充を行う
SSD/HDDの取り扱い	交換したサーバ機器等のSSD/HDDは現地にてメーカーツールによる読み取り不可処置を実施し、三重県に引き渡し 物理破壊を行っていただく

1.2.4 機器の撤去・設定情報及びログ情報の抽出

項目	作業内容
機器の撤去	本システムの運用終了後、本システム内のデータを消去し、解体撤去を行う
SSD/HDDの取り扱い	本システムで利用するサーバ等に搭載されている全てのSSD/HDDは三重県にて物理破壊を行う
設定情報の抽出	三重県と協議した内容にもとづき、各機能の設定情報及び登録情報を汎用的な形式で抽出する
ログ情報の抽出	三重県と協議した内容にもとづき、各機能のログ情報を汎用的な形式で抽出する