三重県　地域連携部
　　情報システム課様

個人番号利用事務系ネットワークにおける
セキュリティ業務

システム基本設計書

第初版

2016年7月29日
ミツイワ株式会社

CONFIDENTIAL MATERIAL /RESTRICTED ACCESS

All Rights Reserved, Copyright(C) ミツイワ株式会社 2016

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業務	確認		作成日	2016/07/25
					更新日	
	プロセス	目　次	担当	ミツイワ）大山	版数	初版

第1章 システム基本設計

1.1 基本設計 ---------- 1
1.1.1 機能を提供するサービス構成 ---------- 1
(1) 端末管理機能 ---------- 1
(2) 端末認証機能 ---------- 1
(3) 利用者認証機能 ---------- 1
(4) 端末操作ログ記録機能 ---------- 1
(5) 外部媒体使用制限及び暗号化機能 ---------- 1
(6) 端末暗号化機能 ---------- 2
(7) その他機能 ---------- 2
(8) バックアップ ---------- 2
(9) 稼働監視 ---------- 2
1.1.2 機能を提供するシステム構成と業務継続性 ---------- 3
(1) 端末管理機能 ---------- 3
(2) 端末認証機能 ---------- 3
(3) 利用者認証機能 ---------- 3
(4) 端末操作ログ記録機能 ---------- 3
(5) 外部媒体使用制限及び暗号化機能 ---------- 3
(6) 端末暗号化機能 ---------- 4
(7) その他機能 ---------- 4
(8) バックアップ ---------- 4
(9) 稼働監視 ---------- 4
1.1.3 各システムのハード構成 ---------- 5
(1) 機種、OS、サービス ---------- 5
(2) HDDドライブ構成 ---------- 6
(3) HDDパーティション構成 ---------- 6

1.2 信頼性 ---------- 7
(1) 基本方針 ---------- 7
(2) サーバ冗長化構成設計 ---------- 7
(3) 障害復旧方式 ---------- 7
(4) 故障検知 ---------- 8
1.3 サービス概要 ---------- 11
1.3.1 機能 ---------- 11
(1) 端末管理機能 ---------- 11
(2) 端末認証機能 ---------- 12
(3) 利用者認証機能 ---------- 13
(4) 端末操作ログ記録機能 ---------- 14
(5) 外部媒体使用制限及び暗号化機能 ---------- 15
(6) 端末暗号化機能 ---------- 16
1.4 バックアップ ---------- 17
1.4.1 機能 ---------- 17
1.4.2 性能 ---------- 17
1.4.3 運用 ---------- 18
1.5 ラック搭載図 ---------- 20

1.1 基本設計

ここでは、本業務における、根幹となる基本設計を記す。

1.1.1 機能を提供するサービス構成

(1) 端末管理機能

提供システム	提供サービス
Asset Viewサーバ	本ネットワーク内に接続される端末の情報収集及びアラートの検知
WSUSサーバ	業務セグメントからの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
ウイルス対策統合管理サーバ (Trend Micro Control Manager:TMCM)	業務セグメントからのパターンファイル取得と本ネットワーク内のVB Corpサーバや Server Protect for Linuxへの配信
ウイルス対策サーバ (ｳｲﾙｽﾊﾞｽﾀｰｺｰﾎﾟﾚｲﾄｴﾃﾞｨｼｮﾝ:VB Corp)	本ネットワーク内のWindowsサーバ／クライアントのウイルス対策及びパターンファイル提供

(2) 端末認証機能

提供システム	提供サービス
Asset Viewサーバ	本ネットワーク内に接続される端末の情報収集と不正端末の検知と管理者への通知
Asset Viewセンサーサーバ	本ネットワーク内の本庁セグメントに接続された不正端末の検知と接続の遮断
Asset ViewセンサーPC	本ネットワーク内の別セグメント(3セグメント)に接続された不正端末の検知と接続の遮断

(3) 利用者認証機能

提供システム	提供サービス
ADサーバ	既存ActiveDirectoryと信頼関係を持ち、既存Windowsアカウントでのユーザ認証
静脈認証サーバ	本ネットワーク内の端末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

(4) 端末操作ログ記録機能

提供システム	提供サービス
Asset Viewサーバ	本ネットワーク内の端末を操作した履歴の収集と管理

(5) 外部媒体使用制限及び暗号化機能

提供システム	提供サービス
Asset Viewサーバ	本ネットワーク内の端末における外部媒体の利用制限の管理及び情報持出し時の暗号化の管理

(6) 端末暗号化機能

提供システム	提供サービス
端末暗号化管理サーバ	本ネットワーク内の端末の暗号化及び管理

(7) その他機能

提供システム	提供サービス
DNSサーバ	本ネットワーク内の端末の名前解決
NTPサーバ	本ネットワーク内の端末の時刻同期

(8) バックアップ

提供端末	提供サービス
バックアップサーバ	本業務を構成してい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

(9) 稼働監視

提供端末	提供サービス
稼働監視中継サーバ	本業務を構成している各サーバのハードウェア稼働状況の監視及び管理者への通知
稼働監視ツール(System Defender Box:SDB)	本業務を構成している各サーバの重要サービス稼働状況の監視及び管理者への通知

1.1.2 機能を提供するシステム構成と業務継続性

(1) 端末管理機能

提供システム	システム構成	業務継続性
Asset Viewサーバ	サーバ1台(Asset Viewサーバ)	停止時は資産情報の収集とアラート検知が停止(端末は利用可能) 端末上の資産情報収集は稼働、一時的に端末側で保持
WSUSサーバ	サーバ1台(WSUSサーバ)	停止時はセキュリティパッチの配信が停止(端末は利用可能)
TMCMサーバ	サーバ1台(Assetiewセンサーサーバ)	停止時はパターンファイルの配信が停止(端末は利用可能)
VB Corpサーバ	サーバ1台(ADサーバ2)	停止時はWindows端末へのパターンファイルの配信が停止(端末は利用可能)

(2) 端末認証機能

提供システム	システム構成	業務継続性
Asset Viewサーバ	サーバ1台(Asset Viewサーバ)	本ネットワークに接続される不正端末の検知と遮断が停止(端末は利用可能)
Asset Viewセンサーサーバ	サーバ1台(Asset Viewセンサーサーバ)	本庁セグメントに接続される不正端末の検知と遮断が停止(端末は利用可能)
Asset Viewセンサー PC	パソコン3台(Asset Viewセンサー PC1～3)	停止したセンサーPCが設置されている本庁外のセグメントに接続される 不正端末の検知と遮断が停止(端末は利用可能)

(3) 利用者認証機能

提供システム	システム構成	業務継続性
ADサーバ	サーバ2台(ADサーバ1, 2)	サーバ1台の停止時は、Windows認証機能を継続利用可能
静脈認証サーバ	サーバ2台(静脈認証サーバ1, 2)	サーバ1台の停止時は、生体認証機能を継続利用可能

(4) 端末操作ログ記録機能

提供システム	システム構成	業務継続性
Asset Viewサーバ	サーバ1台(Asset Viewサーバ)	停止時は端末操作ログの収集が停止(端末は利用可能) 操作ログは一時的に端末側で保持

(5) 外部媒体使用制限及び暗号化機能

提供システム	システム構成	業務継続性
Asset Viewサーバ	サーバ1台(Asset Viewサーバ)	停止時は外部媒体の使用制限機能を継続利用可能。 暗号化機能は利用不可。許可された権限があっても外部媒体への書込みは 不可。但し、暗号化機能を無効化していた端末では書込みが可能

(6) 端末暗号化機能

提供システム	システム構成	業務継続性
端末暗号化管理サーバ	サーバ1台(端末暗号化管理サーバ)	停止時は端末暗号化認証のパスワードリセット機能が停止(端末は利用可能) 端末暗号化機能は継続利用可。

(7) その他機能

提供システム	システム構成	業務継続性
DNSサーバ	サーバ2台(ADサーバ1，2)	サーバ1台の停止時は、名前解決機能を継続利用可能
NTPサーバ	サーバ2台(ADサーバ1，2)	サーバ1台の停止時は、時刻同期機能を継続利用可能

(8) バックアップ

提供端末	システム構成	業務継続性
バックアップサーバ	サーバ1台(バックアップサーバ)	停止時は本業務システムのバックアップ取得が停止

(9) 稼働監視

提供端末	システム構成	業務継続性
稼働監視中継サーバ	サーバ1台(稼働監視中継サーバ)	停止時は本業務を構成している各サーバの故障検知及び管理者への通知 機能が停止(本業務システムは継続稼働可能)
稼働監視ツール	装置1台(SDB)	停止時は本業務を構成している各サーバのサービス停止検知及び管理者 への通知機能が停止(本業務システムは継続稼働可能)

1.1.3 各システムのハード構成

(1) 機種、OS、サービス

No.	名称	種別	機種	OS	サービス
1	ADサーバ1	サーバ	PRIMERGY RX1330 M2	Windows Server 2012 R2 Standard	Active Directory、DNS、NTP
2	ADサーバ2	サーバ	PRIMERGY RX1330 M2	Windows Server 2012 R2 Standard	Active Directory、DNS、NTP ウイルス対策サーバ(ｳｲﾙｽﾊﾞｽﾀｰ Corp)
3	WSUSサーバ	サーバ	PRIMERGY RX1330 M2	Windows Server 2012 R2 Standard	WSUSサーバ
4	AssetViewサーバ	サーバ	PRIMERGY RX1330 M2	Windows Server 2012 R2 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 M2	Windows Server 2012 R2 Standard	端末認証(Asset View)、ウイルス対策統合管理サーバ(Trend Micro Control Manager)
6	AssetViewセンサーPC1	クライアント	ESPRIMO　Q556M	Windows10 Professional	端末認証(Asset View)
7	AssetViewセンサーPC2	クライアント	ESPRIMO　Q556M	Windows10 Professional	端末認証(Asset View)
8	AssetViewセンサーPC3	クライアント	ESPRIMO　Q556M	Windows10 Professional	端末認証(Asset View)
9	静脈認証サーバ1	サーバ	PRIMERGY RX1330 M2	Windows Server 2012 R2 Standard	利用者認証(PalmSecure LoginDirector)
10	静脈認証サーバ2	サーバ	PRIMERGY RX1330 M2	Windows Server 2012 R2 Standard	利用者認証(PalmSecure LoginDirector)
11	端末暗号化管理サーバ	サーバ	PRIMERGY RX1330 M2	Windows Server 2012 R2 Standard	端末暗号化(Drive Encryption)
12	バックアップサーバ	サーバ	PRIMERGY RX2530 M2	Windows Server 2012 R2 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 M2	Windows Server 2012 R2 Standard	稼働監視(Server View Operation Manager)
14	稼働監視ツール	-	System Defender Box	Cent OS 6.2 相当	プロセス稼働監視
15	運用管理端末	クライアント	LIFEBOOK A574/M	Windows8.1 Professional	運用管理

(2) HDDドライブ構成

No.	名称	HDD1	RAID	容量	HDD2	RAID	容量	HDD3	RAID	容量
1	ADサーバ1	300GB×2	RAID1	300GB	–	–	–	–	–	–
2	ADサーバ2	300GB×2	RAID1	300GB	–	–	–	–	–	–
3	WSUSサーバ	600GB×2	RAID1	600GB	–	–	–	–	–	–
4	AssetViewサーバ	300GB×3	RAID5	600GB	600GB×3	RAID5	1.2TB	1.8TB×4	RAID5	5.4TB
5	AssetViewセンサーサーバ	300GB×2	RAID1	300GB	–	–	–	–	–	–
6	AssetViewセンサーPC1	320GB×1	–	320GB	–	–	–	–	–	–
7	AssetViewセンサーPC2	320GB×1	–	320GB	–	–	–	–	–	–
8	AssetViewセンサーPC3	320GB×1	–	320GB	–	–	–	–	–	–
9	静脈認証サーバ1	300GB×3	RAID5	600GB	–	–	–	–	–	–
10	静脈認証サーバ2	300GB×3	RAID5	600GB	–	–	–	–	–	–
11	端末暗号化管理サーバ	300GB×2	RAID1	300GB	–	–	–	–	–	–
12	バックアップサーバ	300GB×2	RAID1	300GB	1.2TB×8	RAID5	8.4TB	–	–	–
13	稼働監視中継サーバ	300GB×2	RAID1	300GB	–	–	–	–	–	–
14	稼働監視ツール	16GB×1	–	16GB	–	–	–	–	–	–
15	運用管理端末	320GB×1	–	320GB	–	–	–	–	–	–

(3) HDDパーティション構成

No.	名称	Cドライブ	用途	Dドライブ	用途	Eドライブ	用途	Eドライブ	用途
1	ADサーバ1	100GB	システム領域	200GB	未使用	–	–	–	–
2	ADサーバ2	100GB	システム領域	200GB	Corp等データ	–	–	–	–
3	WSUSサーバ	100GB	システム領域	500GB	コンテンツ領域	–	–	–	–
4	AssetViewサーバ	100GB	システム領域	500GB	AssetViewデータ領域	1.2TB	週次バックアップ	5.4TB	年次バックアップ領域
5	AssetViewセンサーサーバ	100GB	システム領域	200GB	TMCM等データ	–	–	–	–
6	AssetViewセンサーPC1	160GB	システム領域	160GB	未使用	–	–	–	–
7	AssetViewセンサーPC2	160GB	システム領域	160GB	未使用	–	–	–	–
8	AssetViewセンサーPC3	160GB	システム領域	160GB	未使用	–	–	–	–
9	静脈認証サーバ1	100GB	システム領域	500GB	静脈データ/ログ領域	–	–	–	–
10	静脈認証サーバ2	100GB	システム領域	500GB	静脈データ/ログ領域	–	–	–	–
11	端末暗号化管理サーバ	100GB	システム領域	200GB	暗号化管理データ	–	–	–	–
12	バックアップサーバ	200GB	システム領域	100GB	自身のバックアップ領域	8.4TB	バックアップ領域	–	–
13	稼働監視中継サーバ	200GB	システム領域	100GB	自身のバックアップ領域	–	–	–	–
14	稼働監視ツール	16GB	システム領域	–	–	–	–	–	–
15	運用管理端末	160GB	システム領域	160GB	未使用	–	–	–	–

1.2 信頼性

(1) 基本方針

「本業務にて利用する各サーバ」のうち職員様利用においてトラブル時の影響が大きいサーバは各部品を冗長化しサービスの継続性を高める。

(2) サーバ冗長化構成設計

システム名称	内蔵Disk冗長化方式	電源ユニット冗長化方式	冷却ファン冗長化方式
ADサーバ1	RAID1	内蔵電源ユニット冗長化	内蔵冷却ファン冗長化
ADサーバ2	RAID1	内蔵電源ユニット冗長化	内蔵冷却ファン冗長化
WSUSサーバ	RAID1	内蔵電源ユニット冗長化	内蔵冷却ファン冗長化
AssetViewサーバ	RAID5	内蔵電源ユニット冗長化	内蔵冷却ファン冗長化
AssetViewセンサーサーバ	RAID1	内蔵電源ユニット冗長化	内蔵冷却ファン冗長化
静脈認証サーバ1	RAID5	内蔵電源ユニット冗長化	内蔵冷却ファン冗長化
静脈認証サーバ2	RAID5	内蔵電源ユニット冗長化	内蔵冷却ファン冗長化
端末暗号化管理サーバ	RAID1	内蔵電源ユニット冗長化	内蔵冷却ファン冗長化
バックアップサーバ	RAID1+RAID5	–	–
稼働監視中継サーバ	RAID1	–	–
センサーPC1	–	–	–
センサーPC2	–	–	–
センサーPC3	–	–	–
稼働監視ツール(SDB)	–	–	–

(3) 障害復旧方式

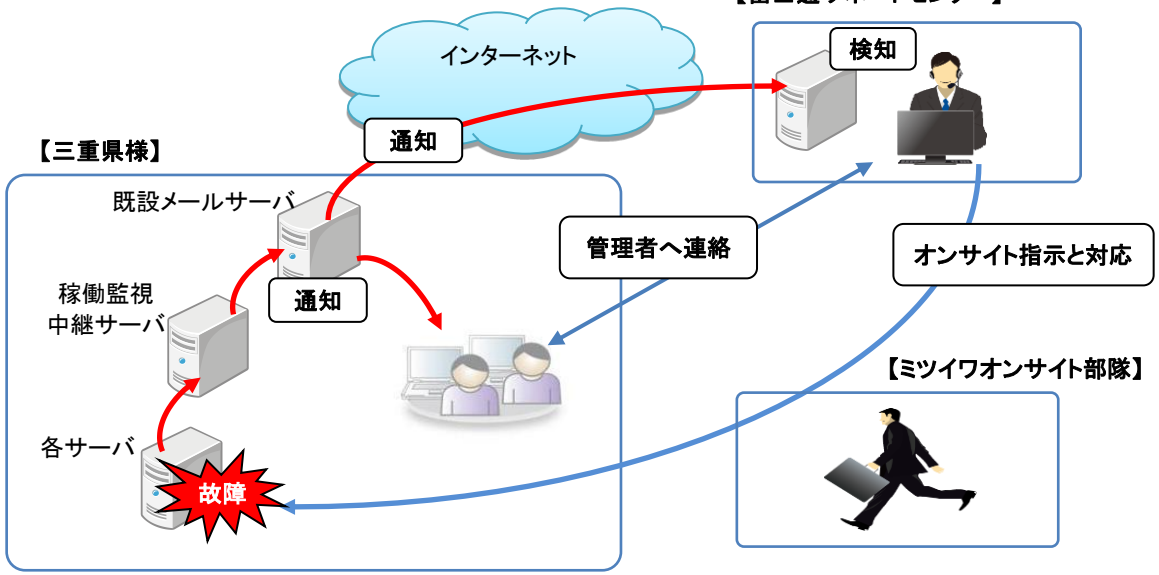
障害発生時、冗長化されているものについてはサービスを停止することなく(一時的な中断はあり)業務を継続可能。
活性交換部品は業務を停止することなく、完全復旧可能。それ以外はシステムを停止し、復旧を行う。

障害内容	障害範囲	障害時機器状態	障害時の対応方法	備考
CPU障害	全障害	停止	ハードウェア交換	
メモリ障害	全障害	停止	ハードウェア交換	
システムボード異常	全障害	停止	ハードウェア交換	
ネットワークカード異常	全障害	停止	ハードウェア交換	
電源障害	一部障害	運用継続	ハードウェア交換	ホットプラグ対応
	全障害	停止	ハードウェア交換	
ディスク障害	一部障害	運用継続	ハードウェア交換	ホットプラグ対応
	全障害	停止	ハードウェア交換 バックアップより復旧	
OSシステムダウン	ー	停止	障害原因調査、OS再起動、バックアップより復旧	障害要因により対応は異なる

(4) 故障検知

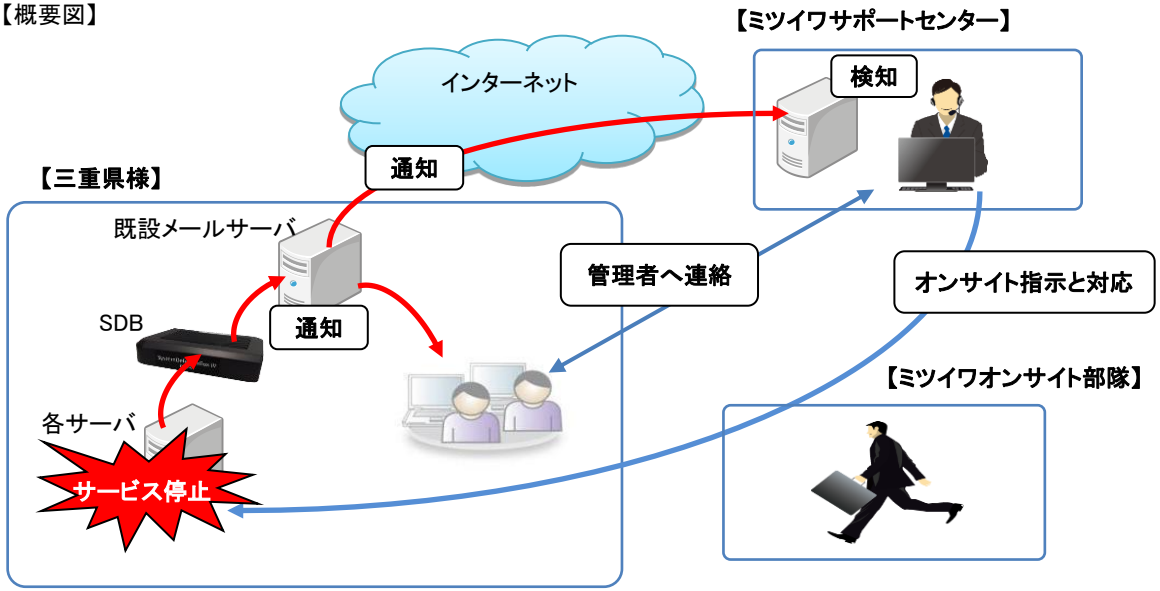
1) ハードウェアの故障発生(予兆を含む)時には、装置前面の故障ランプが点灯し、Serverviewにて管理者様と富士通サポートセンターへ自動通知される。
その後、富士通サポートセンターによる状況確認(問診等)と所課へのオンサイト対応指示が入る。

【概要図】



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。

【概要図】



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	○(SDB)	○	○	
センサーPC1	○(SDB)	–	–	
センサーPC2	○(SDB)	–	–	
センサーPC3	○(SDB)	–	–	
稼働監視ツール(SDB)	○(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	○(SV)	○	○
ADサーバ2	○(SV)	○	○
WSUSサーバ	○(SV)	○	○
AssetViewサーバ	○(SV)	○	○
AssetViewセンサーサーバ	○(SV)	○	○
静脈認証サーバ1	○(SV)	○	○
静脈認証サーバ2	○(SV)	○	○
端末暗号化管理サーバ	○(SV)	○	○
バックアップサーバ	○(SV)	○	○
稼働監視中継サーバ	○(SV)	○	○
センサーPC1	○	–	–
センサーPC2	○	–	–
センサーPC3	○	–	–
稼働監視ツール(SDB)	○	–	–

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(ポート)	備考
		-	三重県様
server00@remcsworld.ne.jp	mynumber-svom@pref.mie.jp	10.1.124.30 (25)	富士通サポートセンター
mie-mynumber@ny.mitsuiwa.co.jp	mynumber-svom@pref.mie.jp	10.1.124.30 (25)	ミツイワサポートセンター

1.3 サービス概要

1.3.1 機能

(1) 端末管理機能

・ 本機能では以下の機能を提供する。

1) 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
2) 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
3) リモート操作

・ 運用要件を以下とする。

1) 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	
アラート発生時の管理者宛て通知	インベントリ収集のタイミング	

2) 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サーバは業務系ネットワークに設置のWSUSサーバよりセキュリティパッチデータを取得

対象端末	取得サーバ(接続ポート)	備考
WSUSサーバ	10.15.9.16:80	同期のタイミング:1日1回
サーバ／クライアント	ms16000:80	WSUSサーバ

3) 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(ウイルスバスターコーポレイトエディション:VB Corp)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 Control Manager:TMCM)を設置し、業務系ネットワークに設置のTMCMサーバよりパターンファイルを取得
本ネットワーク内のTMCMサーバから配下のVB Corpサーバ及びLinuxサーバ向けウイルス対策ソフト(Server Protect for Linux)にパターンファイルを配信
※パターンファイルの取得(配信)タイミングは既存上位側TMCMのアップデートに同期させる。

対象端末	取得サーバ(接続ポート)	備考
TMCMサーバ	10.15.9.12:80	
VB Corpサーバ	ms160005:80	AssetViewセンサーサーバ
Linux系業務サーバ	ms160005:80	AssetViewセンサーサーバ
Windows系サーバ／クライアント	ms160002:80	ADサーバ2

・ ソフトウェア構成

機能	配置先	ソフトウェア	備考
ハードウェア／ソフトウェア情報の取得	AssetViewサーバ	AssetView	
セキュリティパッチの配信	WSUSサーバ	Windows Server Update Services	
ウイルス対策ソフトの管理	TMCMサーバ	Trend Micro Control Manager	
	VB Corpサーバ	ウイルスバスターコーポレイトエディション	

(2) 端末認証機能

・ 本機能では以下の機能を提供する。

1) 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

・ 運用要件を以下とする。

1) 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	センサーサーバ	備考
個人番号利用事務系基幹	ms160005.mynumber.local	AssetViewセンサーサーバ
北勢児童相談所	ms160006.mynumber.local	AssetViewセンサーPC1
児童相談センター／中勢児童相談所	ms160007.mynumber.local	AssetViewセンサーPC2
障害者相談支援センター	ms160008.mynumber.local	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	ms160014.mynumber.local	運用管理端末

・ ソフトウェア構成

機能	配置先	ソフトウェア	備考
不正端末の検知／遮断	AssetViewセンサーサーバ	AssetView	
	AssetViewセンサーPC1	AssetView	
	AssetViewセンサーPC2	AssetView	
	AssetViewセンサーPC3	AssetView	

(3) 利用者認証機能

・ 本機能では以下の機能を提供する。

1) 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

・ 運用要件を以下とする。

1) 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 Diretoryによる利用者認証	ms160001.mynumber.local	ADサーバ1
	ms160002.mynumber.local	ADサーバ2
生体(静脈)による利用者認証	ms160009.mynumber.local	静脈認証サーバ(仮想ホスト)
	ms160010.mynumber.local	静脈認証サーバ1
	ms160011.mynumber.local	静脈認証サーバ2

※既存Active Directoryとは信頼関係のみ

2) 認証情報の管理

Windows認証のIDは既存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
拠点管理者は静脈登録可能な権限が与えられ、拠点での静脈登録を行う
バイオ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
ADサーバ1	既存ADサーバとの信頼関係のみ	
ADサーバ2	既存ADサーバとの信頼関係のみ	
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

・ ソフトウェア構成

機能	配置先	ソフトウェア	備考
Active Directoryの利用者認証	ADサーバ1／2	Active Directory	
生体(静脈)の利用者認証	静脈認証サーバ1／2	Plam Secure Login Director	

(4) 端末操作ログ記録機能

・ 本機能では以下の機能を提供する。

1) 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

・ 運用要件を以下とする。

1) 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) 通知するアラート情報

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を行う

対象操作	アラート項目	備考
個人／機密情報が含まれるファイルの操作	人名、住所、特定文字列	
特定個人情報が含まれるファイルの操作	12桁数字、人名、住所、特定文字列	

3) 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	ms160014.mynumber.local	運用管理端末

【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

①利用者が本ネットワークに機器を接続

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と未許可機器と比較して許可設定を行う

④利用可能となる

・ ソフトウェア構成

機能	配置先	ソフトウェア	備考
端末操作の記録	AssetViewセンサーサーバ	AssetView	
	各クライアント	AssetView エージェント	

(5) 外部媒体使用制限及び暗号化機能

・ 本機能では以下の機能を提供する。

1) 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

2) 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。

1) 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	備考
CD/DVD/Blu-ray ドライブ	使用禁止	
FD/SDカード	使用禁止	
USBデバイス等	許可されたUSBメモリ以外使用禁止	
共有フォルダ	使用禁止	
ポータブルデバイス	使用禁止	
MO	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	ms160014.mynumber.local	運用管理端末

【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

3) 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

・ ソフトウェア構成

機能	配置先	ソフトウェア	備考
外部媒体の使用制限及び暗号化	AssetViewセンサーサーバ	AssetView	
	各クライアント	AssetView エージェント	

(6) 端末暗号化機能

・ 本機能では以下の機能を提供する。

1) 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。

1) 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

共有端末を利用する場合には、利用者分の認証コードを登録する

対象操作	操作内容	備考
起動時の認証画面	認証コード(パスワード)入力	

・ ソフトウェア構成

機能	配置先	ソフトウェア	備考
端末暗号化	端末暗号化管理サーバ	McAfee Drive Encryption	
	各クライアント	McAfee Drive Encryption	

1.4 バックアップ

1.4.1 機能

(1) 基本要件

・ バックアップに関する要件

1) 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。

2) 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。

3) 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。

1.4.2 性能

(1)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	初期：18.5GB（最大30GB想定）	–	
ADサーバ2	初期：18.2GB（最大30GB想定）	初期：4.87GB（最大：15GB想定）	
WSUSサーバ	初期：20.8GB（最大30GB想定）	初期：329MB（最大：50GB想定）	
AssetViewサーバ	初期：20GB（最大30GB想定）	初期：5.97GB（最大：300GB想定）	
AssetViewセンサーサーバ	初期：17.3GB（最大30GB想定）	初期：9.72GB（最大：30GB想定）	
静脈認証サーバ1	初期：17.2GB（最大30GB想定）	初期：1.49GB（最大：200GB想定）	
静脈認証サーバ2	初期：17.2GB（最大30GB想定）	初期：509MB（最大：20GB想定）	
端末暗号化管理サーバ	初期：22.5GB（最大40GB想定）	初期：4.33GB（最大：50GB想定）	
バックアップサーバ	初期：19.5GB（最大30GB想定）	–	
稼働監視中継サーバ	初期：19.8GB（最大30GB想定）	–	

1.4.3 運用

(1) 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 Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	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	TMCMデータフルバックアップ	ARCServe Bakup	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	TMCMデータバックアップ	ARCServe Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	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

(2)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 Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	全HDD故障時	1週間前	
WSUSサーバ	WSUSデータバックアップ	ARCServe Bakup	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 Bakup	全HDD故障時	1週間前	
AssetViewサーバ	AssetViewデータバックアップ	ARCServe Bakup	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	TMCMデータフルバックアップ	ARCServe Bakup	全HDD故障時	1週間前	
AssetViewセンサーサーバ	TMCMデータバックアップ	ARCServe Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	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 Bakup	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	

ARCServe Backup D 差 AssetView DB Backup データコピー（年1回：1月2日　2:00）

WindowsBackup システム（BK） システム（Local）

土曜日

	23:00	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
ADサーバ1		D					システム（BK）																		
ADサーバ2			D						システム（BK）																
WSUSサーバ				差							システム（BK）														
AssetViewサーバ					差							システム（BK）													
AssetViewセンサーサーバ						差								システム（BK）											
静脈認証サーバ1							差									システム（BK）									
静脈認証サーバ2								差										システム（BK）							
端末暗号化管理サーバ									差											システム（BK）					
バックアップサーバ																									
稼働監視中継サーバ																									

日曜日

	23:00	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
ADサーバ1		差																							
ADサーバ2			差																						
WSUSサーバ		D																							
AssetViewサーバ			差																						
AssetViewセンサーサーバ				差																					
静脈認証サーバ1					差																				
静脈認証サーバ2						差																			
端末暗号化管理サーバ							差																		
バックアップサーバ				システム（Local）																					
稼働監視中継サーバ			システム（Local）																						

月曜日

	23:00	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
ADサーバ1		差																							
ADサーバ2			差																						
WSUSサーバ				差																					
AssetViewサーバ		D	AssetView DB Backupローカル																						
AssetViewセンサーサーバ					差																				
静脈認証サーバ1						差																			
静脈認証サーバ2							差																		
端末暗号化管理サーバ								差																	
バックアップサーバ																									
稼働監視中継サーバ																									

火曜日

	23:00	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
ADサーバ1		差																							
ADサーバ2			差																						
WSUSサーバ				差																					
AssetViewサーバ					差																				
AssetViewセンサーサーバ		D																							
静脈認証サーバ1						差																			
静脈認証サーバ2							差																		
端末暗号化管理サーバ								差																	
バックアップサーバ																									
稼働監視中継サーバ																									

水曜日

	23:00	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
ADサーバ1		差																							
ADサーバ2			差																						
WSUSサーバ				差																					
AssetViewサーバ					差																				
AssetViewセンサーサーバ						差																			
静脈認証サーバ1		D																							
静脈認証サーバ2							差																		
端末暗号化管理サーバ								差																	
バックアップサーバ																									
稼働監視中継サーバ																									

木曜日

	23:00	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
ADサーバ1		差																							
ADサーバ2			差																						
WSUSサーバ				差																					
AssetViewサーバ					差																				
AssetViewセンサーサーバ						差																			
静脈認証サーバ1							差																		
静脈認証サーバ2		D																							
端末暗号化管理サーバ								差																	
バックアップサーバ																									
稼働監視中継サーバ																									

金曜日

	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	0:00
ADサーバ1		差																							
ADサーバ2			差																						
WSUSサーバ				差																					
AssetViewサーバ					差																				
AssetViewセンサーサーバ						差																			
静脈認証サーバ1							差																		
静脈認証サーバ2								差																	
端末暗号化管理サーバ		D																							
バックアップサーバ																									
稼働監視中継サーバ																									

1.5 ラック搭載図

42	
41	光パッチパネル
40	
39	UTPパッチパネル
38	
37	
36	
35	
34	
33	
32	
31	
30	
29	
28	
27	
26	
25	コンソールスイッチ
24	
23	モニタ/キーボード/マウス
22	コンソール／KVMスイッチ
21	Gigaスイッチ／SDB
20	ADサーバ2
19	ADサーバ1
18	WSUSサーバ
17	端末暗号化管理サーバ
16	
15	静脈認証サーバ2
14	静脈認証サーバ1
13	AssetViewサーバ
12	他システム機器
11	
10	他システム機器
9	
8	AssetViewセンサーサーバ
7	稼働監視中継サーバ
6	バックアップサーバ
5	
4	
3	電源ユニット
2	
1	