別紙1　庁内端末詳細

・一人一台パソコン

導入年度	2009	2011	2012	2013
メーカー	HP	NEC	富士通	富士通
型番	Probook 4515s	PC-VK21LXZCC	LIFEBOOK A572/E	LIFEBOOK A573/G
CPU	Turion Ⅱ Ultra Dual Core M600	Corei3-2310M	Corei3-2370M	Corei3-3120M
クロック	2.40GHz	2.10GHz	2.40GHz	2.50GHz
HD容量	160G	250G	250G	320G
メモリ	2GB	2GB	2GB	2GB
画面サイズ	15.6インチ	15.6インチ	15.6インチ	15.6インチ
画面標準解像度	HD（1,366×768）	HD（1,366×768）	HD（1,366×768）	HD（1,366×768）
OS	Windows 7 Professional SP1	Windows 7 Professional SP1	Windows 7 Professional SP1	Windows 7 Professional SP1
庁内メール クライアントソフト	Outlook2010	Outlook2010	Outlook2010	Outlook2010
ブラウザ	Internet Explorer 8.0	Internet Explorer 8.0	Internet Explorer 8.0	Internet Explorer 8.0
導入台数	1,617	1,612	1,426	491

・その他庁内端末

上記一覧の庁内端末以外に，以下の約2500台の庁内端末がある。

※　メーカー、機種、スペック等多種

なお、マイクロソフトのサポートが終了しているOSを搭載する端末は行政WAN接続禁止とする。

	その他庁内端末
OS	Windows Vista ，Windows Server 2008 Windows 7，Windows Server 2008R2 Windows8，Windows Server 2012
庁内メール クライアントソフト	Outlook（2007/2010/2013）
ブラウザ	Internet Explorer(7/8/9/10/11)
導入台数	約3,600

・サーバ機器

約550台のサーバが行政WANにて稼働している。

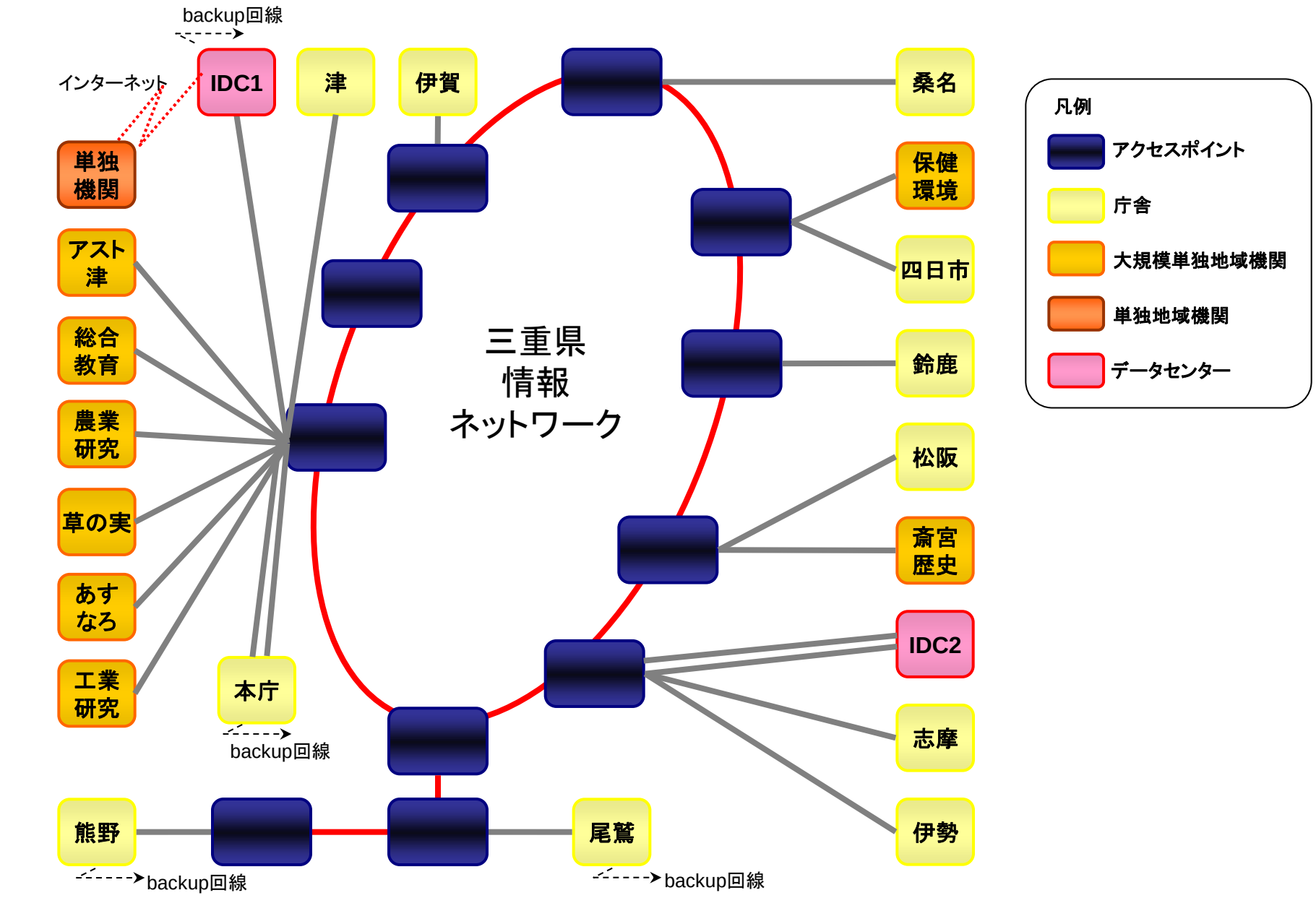
※　メーカー、機種、スペック等多種

なお、マイクロソフトのサポートが終了しているOSを搭載する端末は行政WAN接続禁止とする。

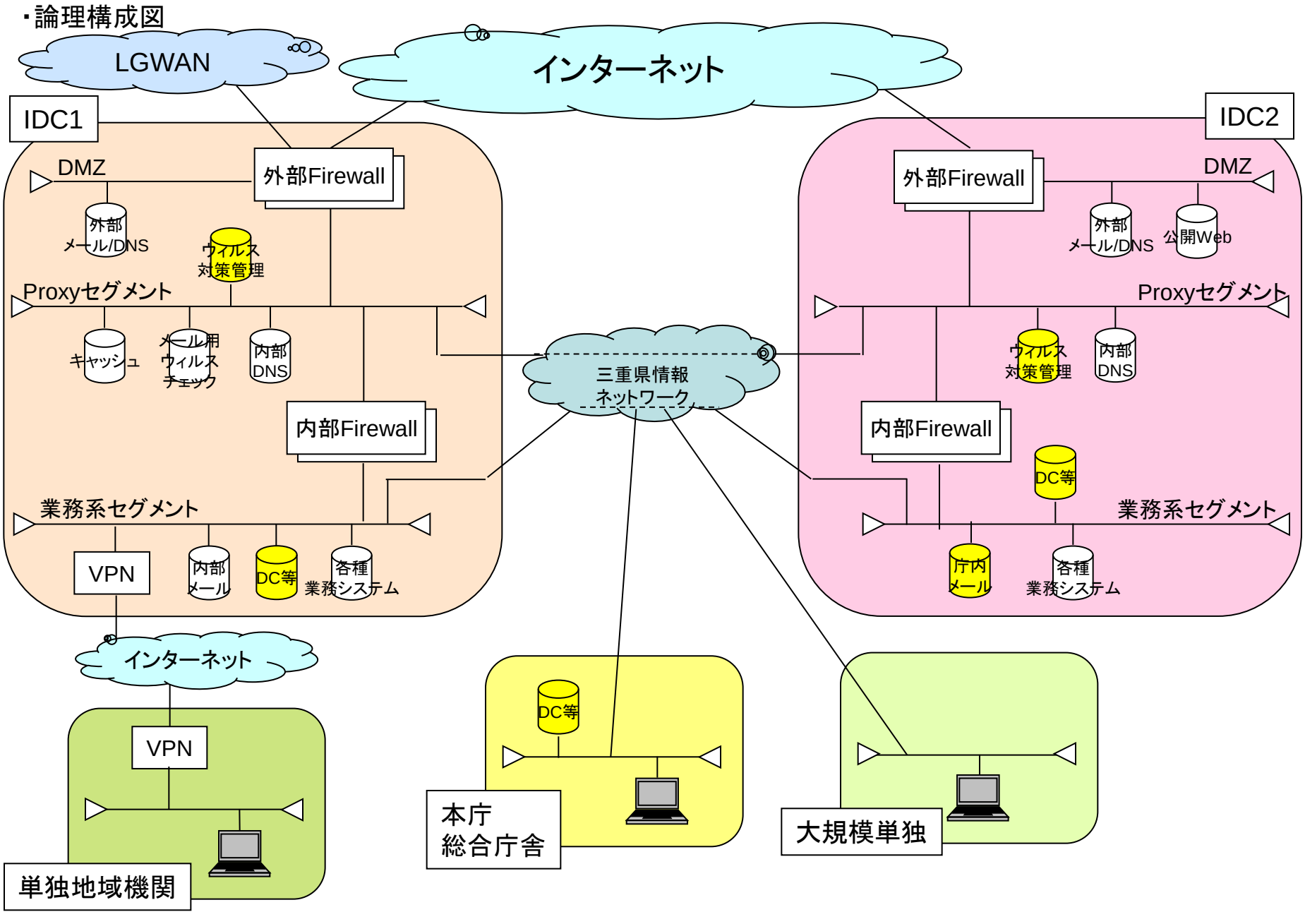
	サーバ
OS	Windows Server 2003、Windows Server 2008 Windows Server 2008R2、Windows Server 2012 Linux、UNIX等
導入台数	約600

別紙2　三重県行政WAN概要図（平成26年11月末時点）

・物理構成図



・論理構成図



別紙3

統合サーバの利用について

仮想サーバの仕様

＜ハイパーバイザー＞

- VMware vSphere 5.5

＜提供される仮想サーバの性能、サーバ数＞

	庁内ドメイン ウィルス対策	運用管理 （収集）	運用管理 （パッチ配信）
CPU	1コア	1コア	1コア
メモリ	8GB	8GB	8GB
HDD実効容量	100GB	150GB	300GB
サーバ数(IDC1)	3	1	1
サーバ数(IDC2)	3	1	1

＜使用可能なOS＞

- Windows Server（統合サーバにてDatacenter Editionを導入しているため、個別のライセンス購入不要。
- Red Hat Enterprise Linux（個別のライセンス購入必要）

※ サポート期限内のOSに限る。

サービスレベル

提供時間	24時間365日の自動運転 ※追加環境機器設置場所の計画停電や更新プログラム適用等のメンテナンス作業により情報システムの停止が必要となる場合があります。
保守対応時間	開庁日(8:00～20:00) ※システムが停止する等の障害が発生した場合は24時間365日で対応します。
機器の障害対策	全ての機器は2重化しているので、片方の機器が故障してもサービスを自動的に継続することが可能です。
仮想マシンの障害対策	vSphere HAによる冗長化が可能です。
統合監視	Ping による仮想マシンの死活監視を行います。
バックアップ	システム全体のバックアップを毎日実行し、5日分保管します。バックアップデータは遠隔地にも保管します。
リストア	最新のバックアップデータからシステム単位またはファイル単位でリストアを行います。

統合サーバ管理者との役割分担

概要説明	統合サーバ管理者	本システム受託事業者
ゲストサーバをインストールする領域の作成	○	
ゲストサーバのOSインストール、環境構築		○
統合サーバにて提供される死活監視、バックアップの設定	○	
本システムの障害監視、バックアップ設定		○
ゲストサーバの動作確認		○
ゲストサーバの運用		○
統合サーバにて提供されるバックアップからのリストア	○	△（依頼）
スナップショットの作成、削除		○
統合サーバのハードウェア障害対応	○	
システム障害対応		○

統合サーバにて提供される死活監視

- 統合サーバでは、別途構築している統合監視サーバからPingによる各ゲストサーバの死活監視を行っており、本システムでも利用可能です。
- 本システムにおけるリソース監視については、詳細仕様書2.6の障害監視システムを利用するものとします。

＜監視方法＞
統合監視サーバから各仮想マシンに対して1分に1回「Ping監視」を行う。
3回連続で応答がない場合は障害が発生していると判断する。

＜障害を検知した場合の動作＞
指定のメールアドレスにメールを送信する。
なお、メール送信のタイミングは障害発生時及び障害復旧時。

＜監視時間＞
24時間365日

統合サーバにて提供されるバックアップ

- 統合サーバではバックアップサービスを提供しており、本システムでも利用可能です。
- 統合サーバのバックアップサービスを利用する場合においても、詳細仕様書2.7に示すバックアップは別途行うものとします。

＜バックアップの種類＞

1. イメージバックアップ
   - 統合サーバのバックアップ環境を利用して、夜間にスナップショットを取得した後、統合サーバのバックアップストレージにバックアップデータを保存する。
   - 5世代分のバックアップデータを保存。
   - サーバ単位もしくはファイル単位でのリストアが可能。
2. ファイルバックアップ
   - 5世代分のバックアップデータを保存。
   - ファイル単位のリストアが可能。

■別紙4_現行システム機器一覧

No.	セグメント	設置場所	利用用途						想定機器			
			庁内ドメイン			庁内メール	ウィルス対策	運用管理	機種	CPU	メモリ	HDD実効容量
			DNS	DHCP	WINS							
1	業務系	本庁	○	1-2階			○		HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
2			○	3-4階					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
3			○	5-6階					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
4			○	7-8階					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
5			○	吉田山					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
6		桑名	○	桑名					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
7		四日市	○	四日市					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
8		鈴鹿	○	鈴鹿					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
9		津	○	津					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
10		松阪	○	松阪					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
11		伊勢	○	伊勢					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
12		志摩	○	志摩					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
13		伊賀	○	伊賀					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
14		尾鷲	○	尾鷲					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
15		熊野	○	熊野					HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
16		IDC2	○		Secondary		○		HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
17			○				○	Slave	HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
18						MBX（クラスタ）			HP Prolient DL380 G6	Xeon X5560 2.80GHz × 2	24GB	146GB(RAID1)
19									HP Prolient DL380 G6	Xeon X5560 2.80GHz × 2	24GB	146GB(RAID1)
20									HP Prolient DL380 G6	Xeon X5560 2.80GHz × 2	24GB	146GB(RAID1)
21						HUB/CAS			HP Prolient DL380 G6	Xeon X5540 2.53GHz × 2	12GB	146GB(RAID1)
22						HUB/CAS			HP Prolient DL380 G6	Xeon X5540 2.53GHz × 2	12GB	146GB(RAID1)
23						Backup			HP Prolient DL360 G6	Xeon E5530 2.40GHz	6GB	146GB(RAID1)
24						共有Disk			HP StrageWorks EVA4400	ー	ー	1.35TB(RAID1+0)
25		IDC1	◎		Primary		○		HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
26			○				○	Slave	HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
27								Master	HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
28								WSUS	HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
29	Proxy	IDC2					○		HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)
30		IDC1					○		HP Prolient DL360 G6	Xeon L5520 2.26GHz	4GB	146GB(RAID1)

別紙5

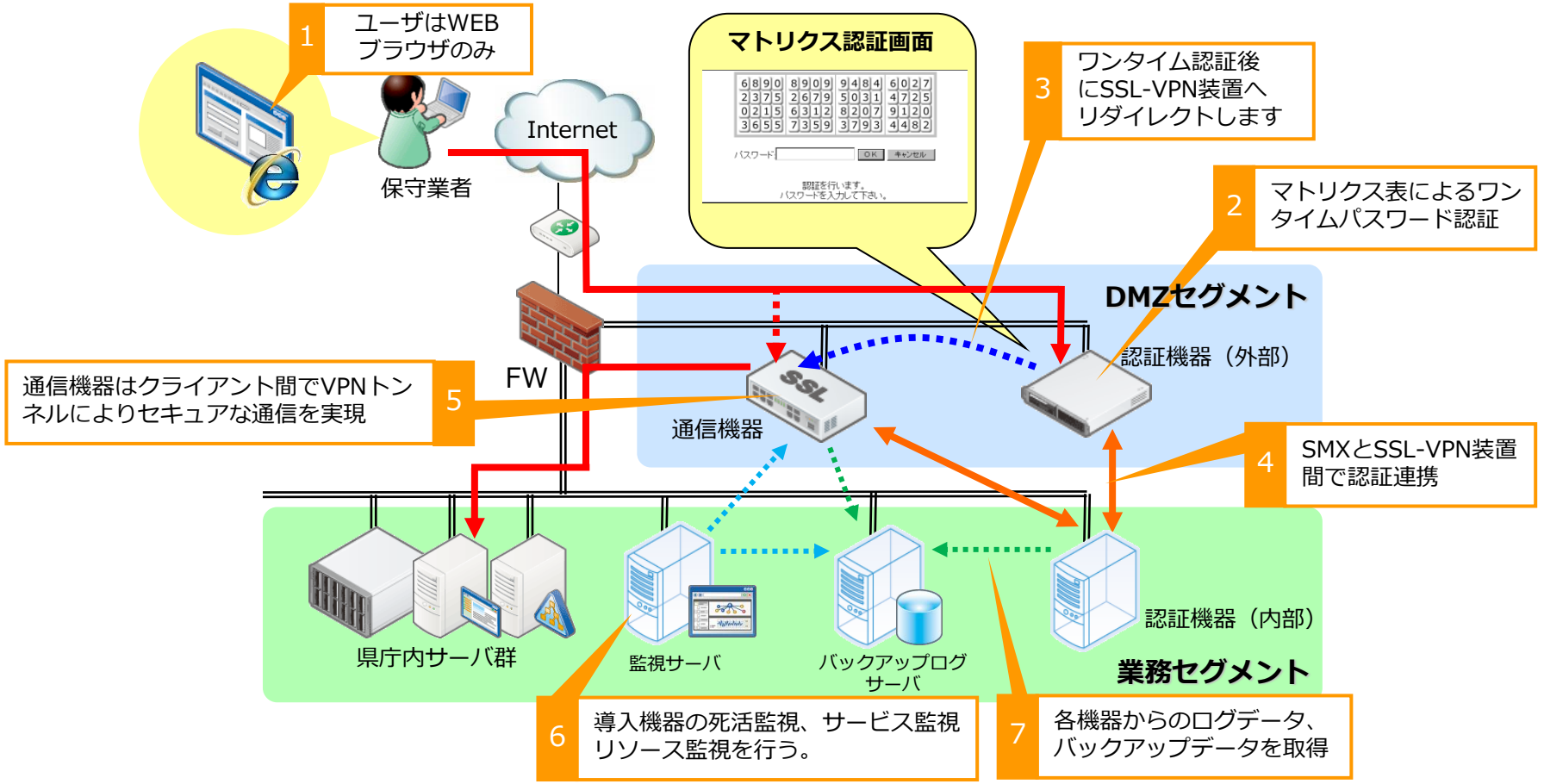
リモート保守環境の利用について

文書番号：MPRC-012
REV.1.00

2014年9月　IT推進課

1. リモート保守環境システム概要

システム関連業者の保守専用端末から、インターネットを経由してSSL-VPN通信でリモート接続し、保守業務を実施する。
リモート接続する際の通信は暗号化を実施し、特定の端末及びユーザからのアクセス制限を実施する。



2. 認証方法

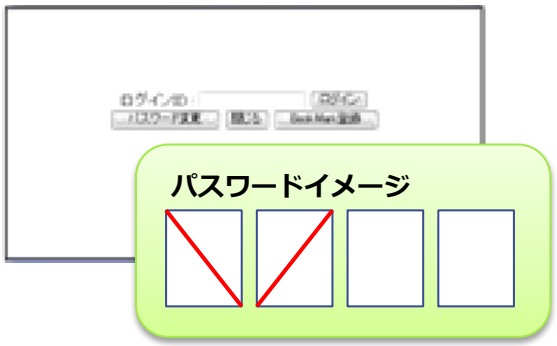
ワンタイムパスワード認証は、ブラウザにランダムに生成される64個の数列（マトリクス表）から、自分が覚え易いイメージ(形)をパスワードとして利用するワンタイム･パスワード認証システム。パスワードの基となるパターンはユーザが記憶するものなので紛失の危険性がありません。

<ワンタイムパスワード概要>

1．ユーザーはWEBブラウザから、認証機器のログイン画面にアクセスし、ログインIDを入力。
2．マトリクス表（乱数表）が生成されるので、予め指定した固定文字と、指定した「形」の位置の数字をパスワードとして入力。

■ パスワードイメージ

あらかじめ自分の好きなパスワードイメージを登録しておく。



■ 認証イメージ

マトリクス認証は、毎回マトリクス表に表示される数字がランダムに変更されるので、二度と同じパスワードを入力することが無い。

入力するパスワード

abcd85425679（一度だけ）

固定文字＋ワンタイムパスワード

高い認証強度を支える4要素認証

1．マトリクス表内のイメージの位置
2．数字を抜き出す順番
3．固定パスワードの併用
4．固定パスワードを挿入する位置

位置情報の組み合わせ数
4桁の場合：約1600万通り　（64の4乗）
6桁の場合：約687億1900万通り　（64の6乗）
8桁の場合：約281兆4749億通り　（64の8乗）
※固定パスワードを併用するとより多くの組み合わせ数になる。

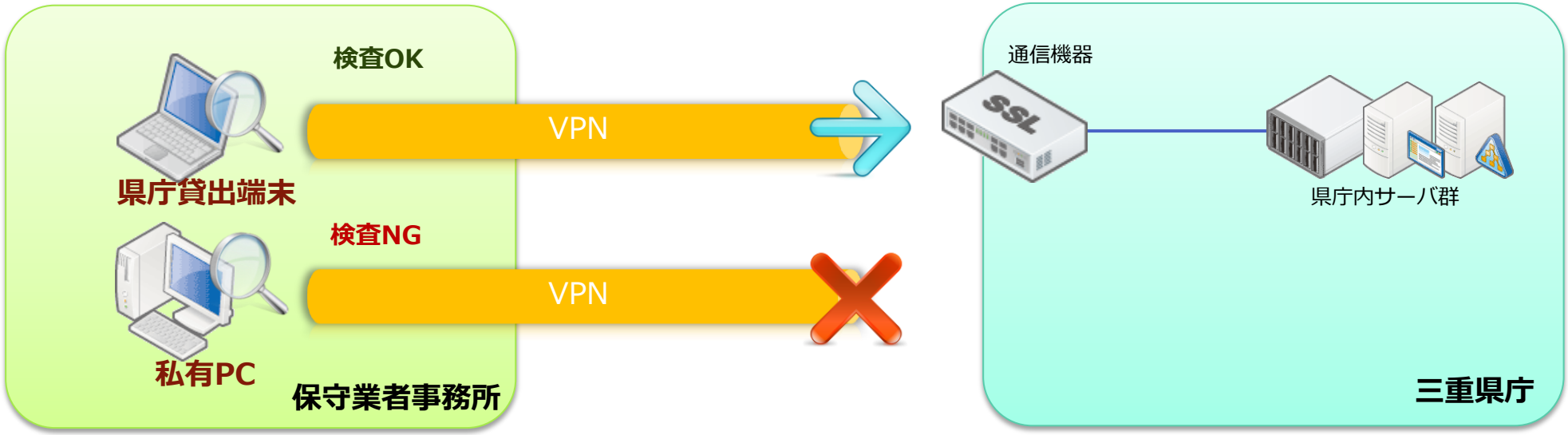
3. エンドポイントセキュリティ

エンドポイントセキュリティは、リモート接続時にクライアント端末の情報を収集し、特定のセキュリティを満たす端末のみ接続を許可する機能です。

<チェック項目>

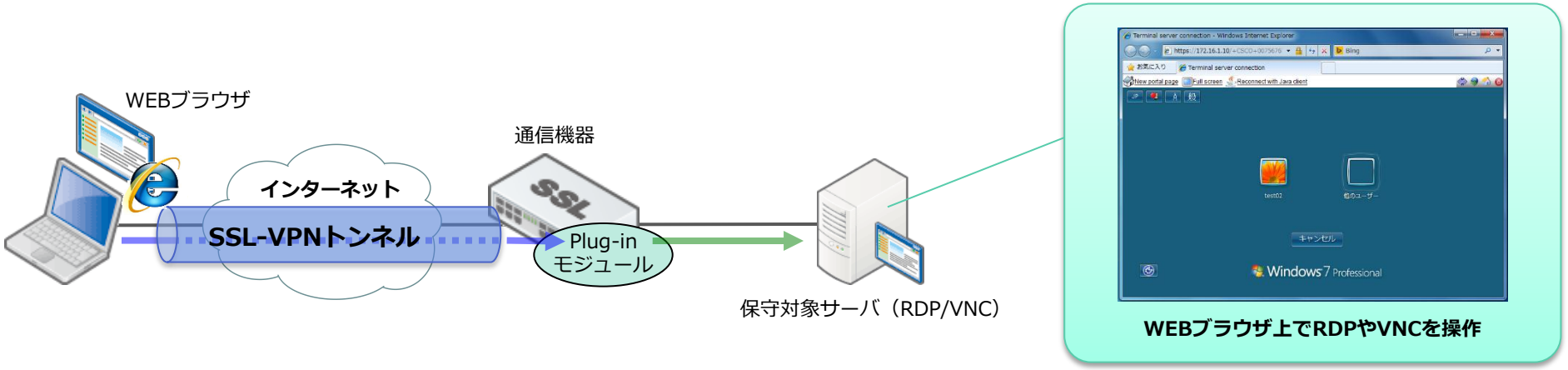
1．端末固有情報
　機器の固有情報を取得し、県庁の貸出した端末をチェックします。

2．ウイルス対策ソフトウェア
　プログラムの実行、リアルタイム保護の有効、パターンファイルの更新などをチェックします。



4. ターミナル接続

専用のプラグインを使うことで、クライアント端末にソフトウェアをインストールすることなく、Webブラウザからのリモートデスクトップや、VNC接続が可能となります。



5. 接続仕様・制限事項

■ 接続仕様

・ リモート保守環境への接続には保守業者ごとにインターネットへの接続回線が必要となります。
・ リモート保守環境への接続には県庁貸出専用端末が必須となります。
・ 接続回線の帯域には、ISDN回線以上（ADSL以上が推奨）の通信速度が必要となります。
・ 保守対象となる機器との通信はTCP/IPでのリモート接続可能な機器が対象となります。
・ 保守用ツール（ソフトウェア）の仕様などにより、リモート保守環境では利用出来ない場合があります。
・ 保守対象となる機器のセキュリティ・県庁様の判断により、利用出来ない場合があります。
・ システムの運用状況によっては緊急停止する場合があります。

■ 制限事項

・ 接続を行う際には必ず県庁貸出専用端末が必要となります。
・ 対象となる機器への保守契約が締結されていることが条件となります。
・ リモート保守環境の貸出しには各種申請書類の提出が必要となります。
・ リモート接続にて参照したデータの外部への保存やプリンタへの印刷は出来ません。
・ リモート接続中の操作に関しては、ログ保存されます。
（リモート保守環境内でログ内容を確認していただきます。）
・ リモート保守接続以外の作業（構築・導入テストなど）に関しては、従来通り現地での作業となります。

6. 利用・申請の流れ

リモート保守環境の申請から利用開始までの流れは以下となります。