資料2-5

三重県公共事業情報統合データベース再構築･運用保守業務委託

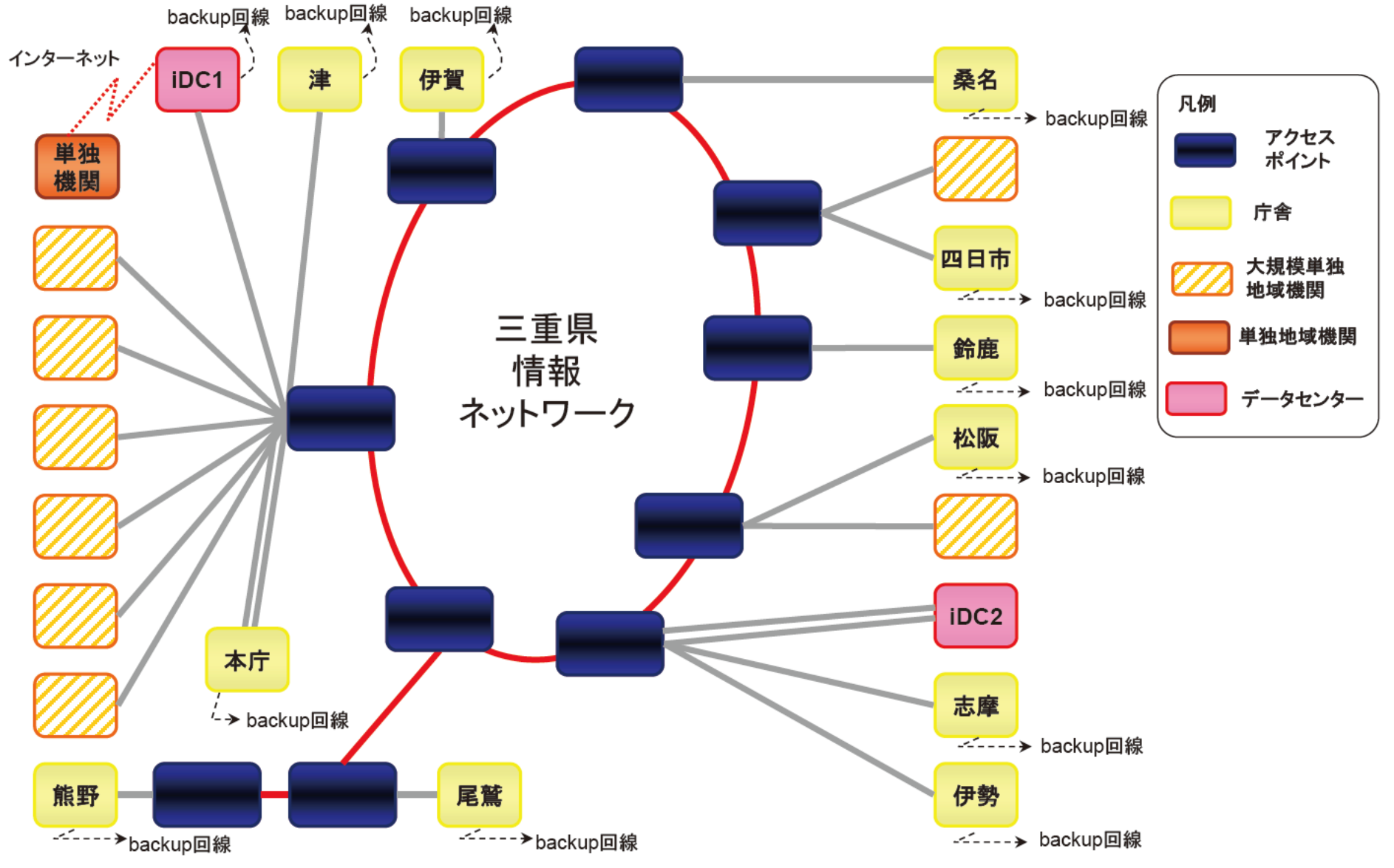
参　考　資　料

＜目次＞

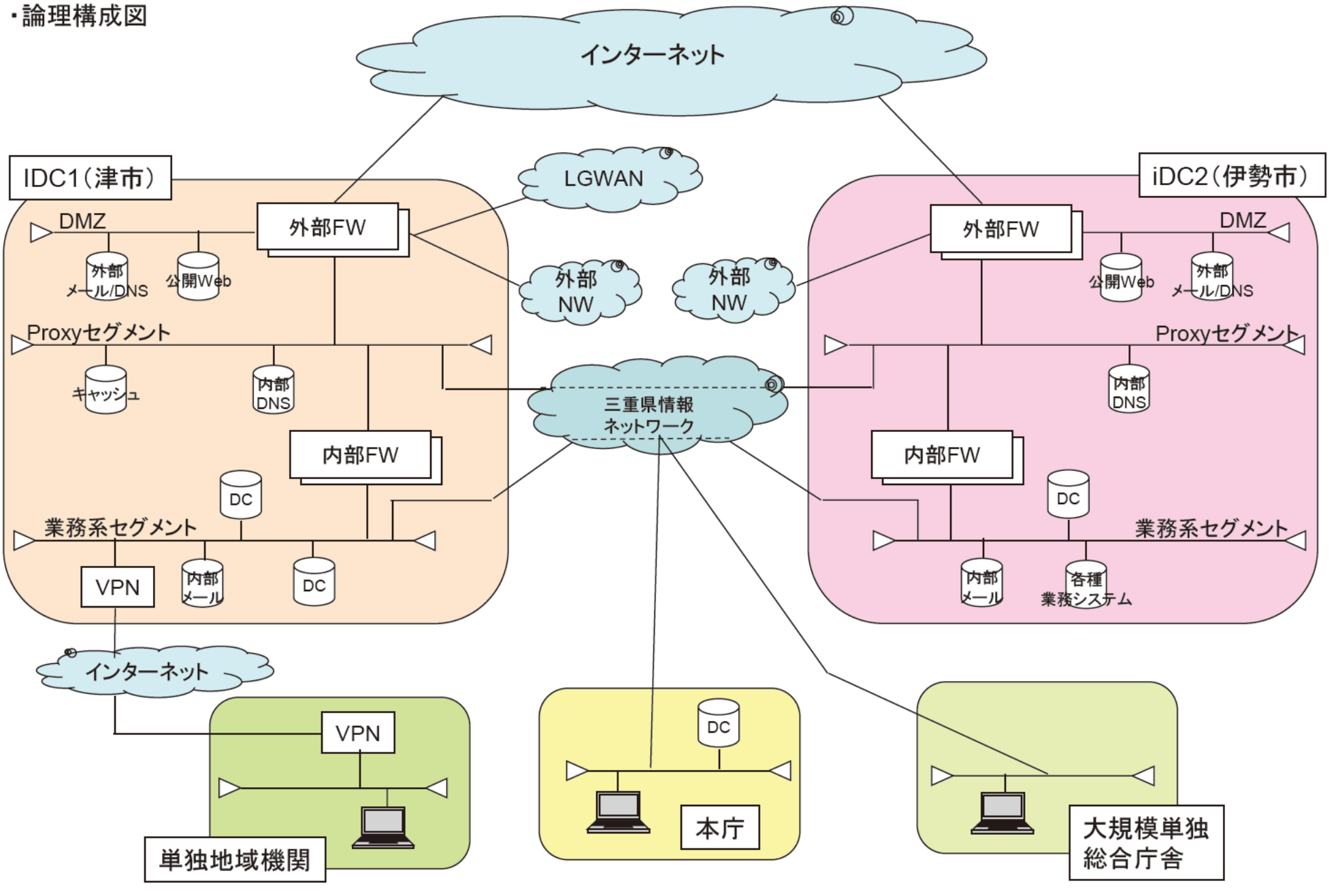
三重県行政WAN概要図（平成29年1月時点）及び外部接続セグメントの利用について

参考資料1

・物理構成図



・論理構成図



外部ネットワークの接続制限（現況）

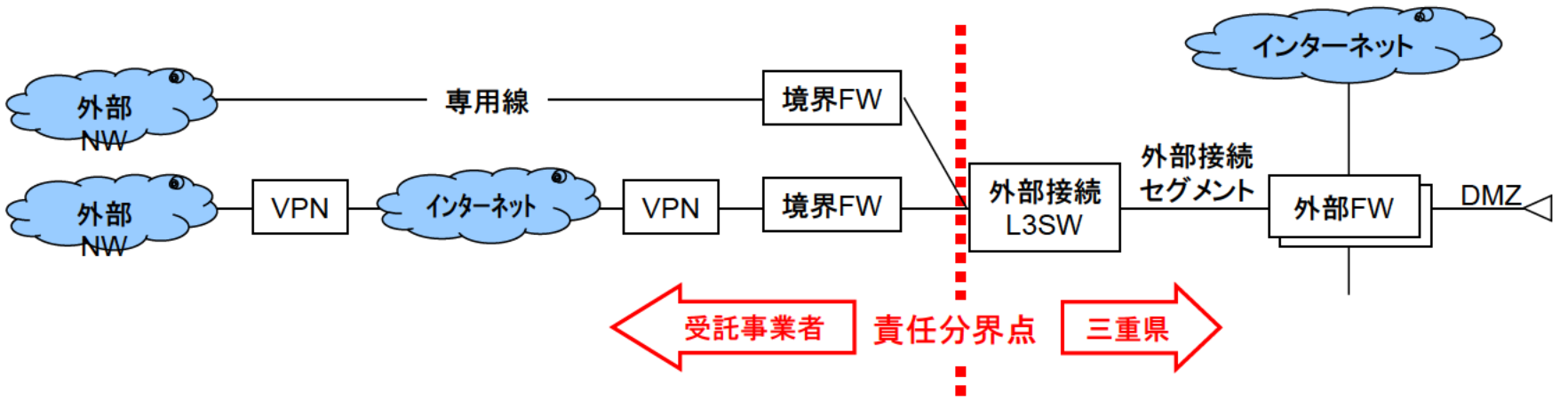
三重県行政WANと他の外部ネットワークを相互接続することは許可しない。
ただし、下記の範囲内で外部接続セグメントを経由すれば、接続は可能であるが、県と調整を必要とする。
外部接続セグメントとは、三重県行政WANと他の外部ネットワークとを中継する専用のセグメントのことを指す。

外部接続セグメントに関する許可プロトコル

インターネット	→	外部接続セグメント	通信不可（外部FW経由）
	←		通信不可（外部FW経由）
DMZ	→	外部接続セグメント	通信不可
	←		http、https
業務系	→	外部接続セグメント	最小限のプロトコルのみ
	←		通信不可

外部接続セグメント経由の想定接続構成例

現在の外部接続セグメント経由の想定接続構成例は以下の2通りあるが、三重県行政WANと他の外部ネットワークと接続することは原則許可していない。



なお、セグメント及び物理境界は上図の責任分界点を基準とし、受託事業者側の機器やその設置、設定にかかる費用を含む全ては受託事業者の責任範囲とする。
境界FWについては、NAT変換機能を有するルーターでもよいこととする。
三重県側の既存機器の設定作業は三重県で実施するが、設定に必要な情報等については、受託事業者が準備すること。
また、設定や作業にあたっては、三重県ネットワーク管理者と調整し、許可を得ること。

外部接続セグメントの必須条件

・割当IP
　外部接続セグメントへの割当IPは、原則、xxx.xxx.xxx.xxx/29 の8個（6個）となり、外部接続L3SW、境界FWにおいて、それぞれ1つずつ割り当てることになるため、事実上利用できるIPは4個である。
　ただし、不足する場合は、調整のうえ8個程度であれば、追加することができるものとする。
・NATの必要性
　双方のネットワークにおいて、内部アドレスの秘匿ため、外部FW、境界FWでそれぞれNATをかける必要がある。

資料 リ－２

リモート保守環境の利用について

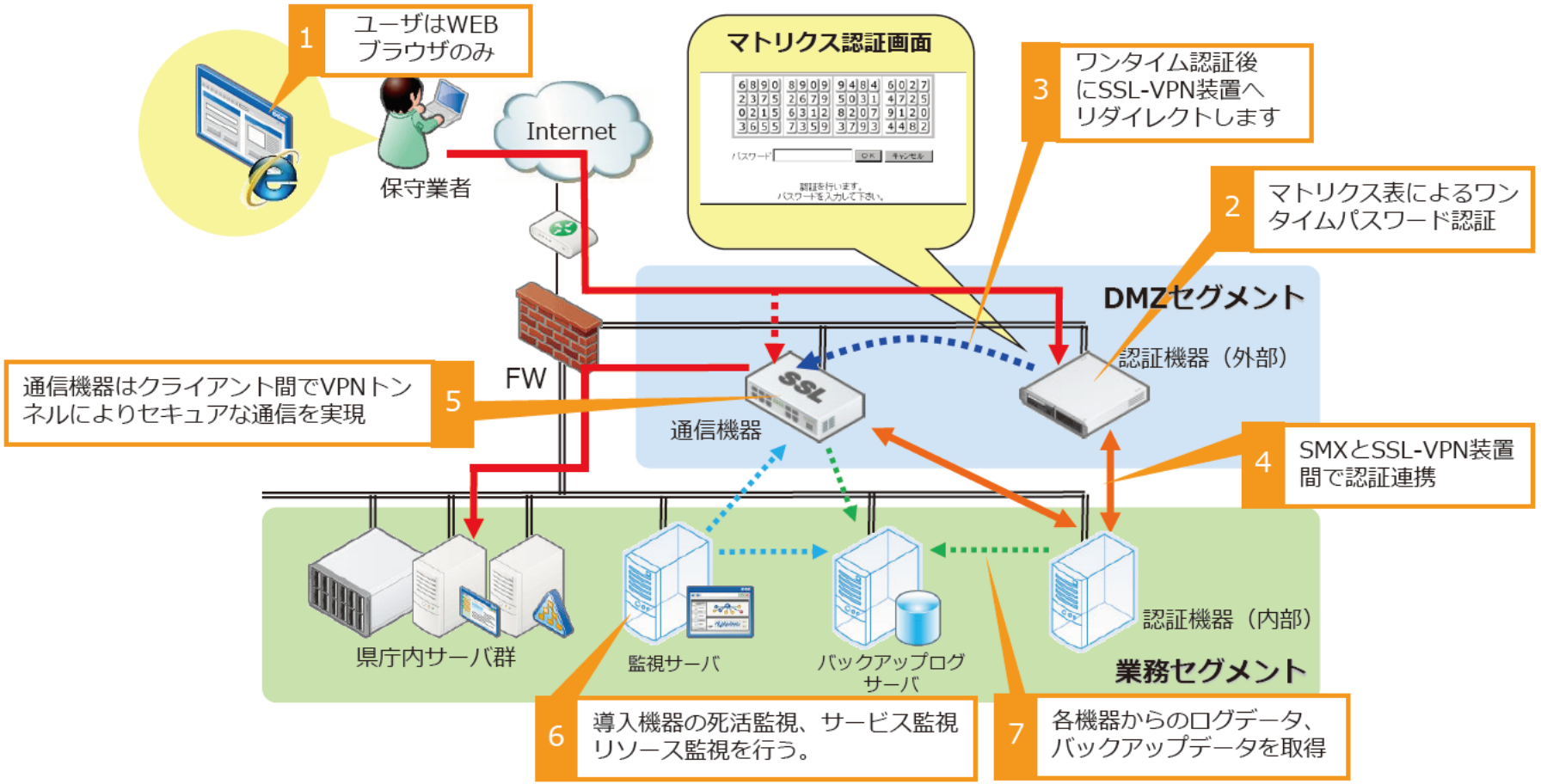
文書番号：MPRC-012
REV.1.02

2015年4月

三重県地域連携部
情報システム課システム企画班

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

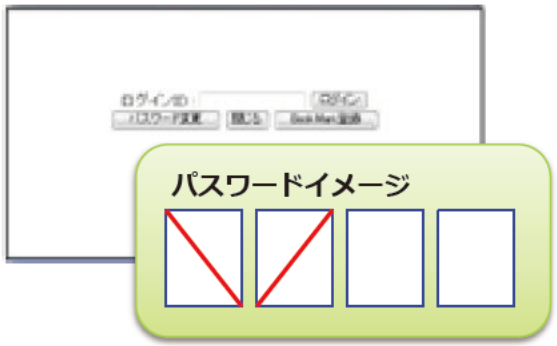
ワンタイムパスワード認証は、ブラウザにランダムに生成される64個の数列（マトリクス表）から、自分が覚え易いイメージ(形)をパスワードとして利用するワンタイム･パスワード認証システム。パスワードの基となるパターンはユーザが記憶するものなので紛失の危険性がありません。

<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。

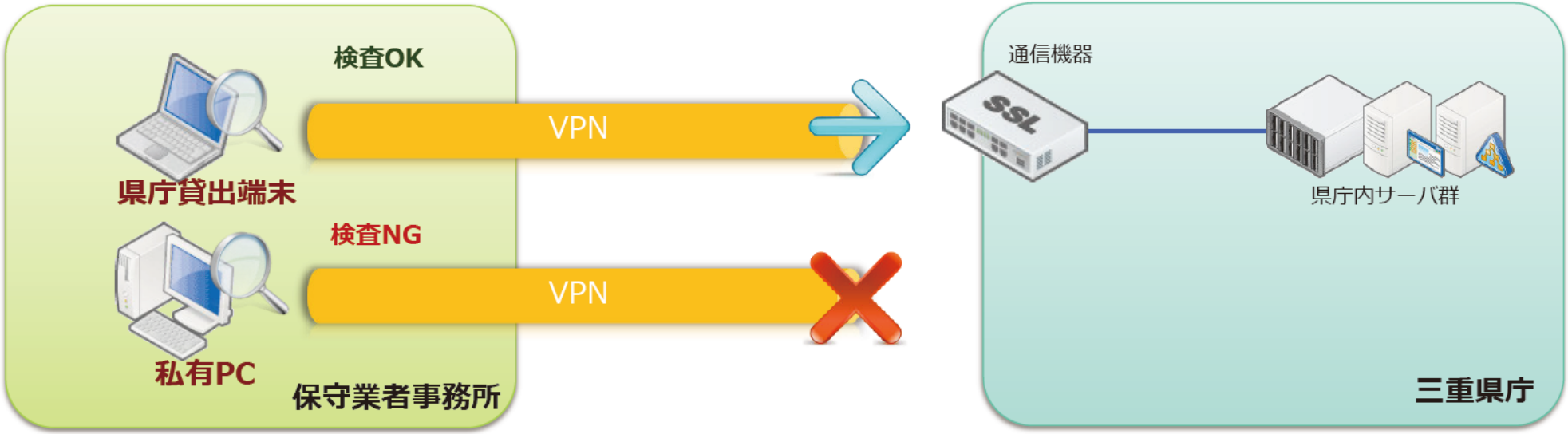
3. エンドポイントセキュリティ

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>

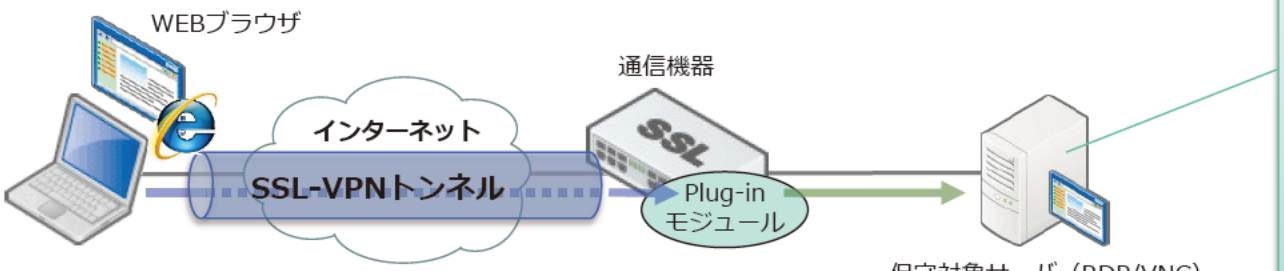
1．端末固有情報
　機器の固有情報を取得し、県庁の貸出した端末をチェックします。

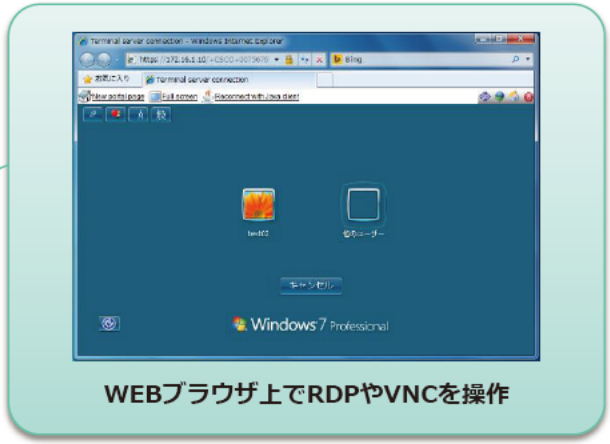
2．ウイルス対策ソフトウェア
　プログラムの実行、リアルタイム保護の有効、パターンファイルの更新などをチェックします。



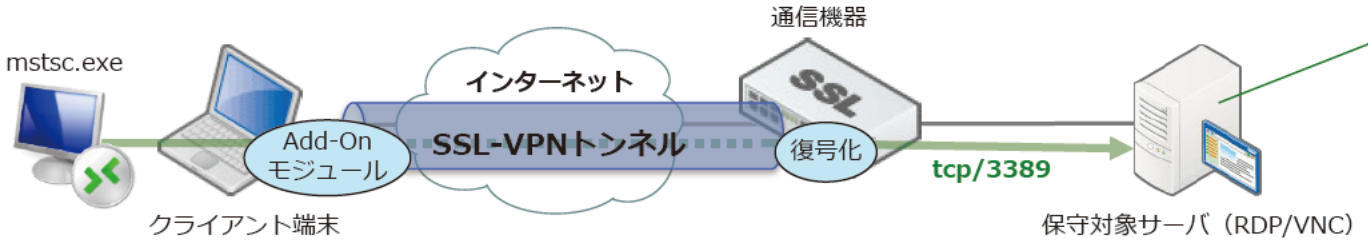
4. ターミナル接続

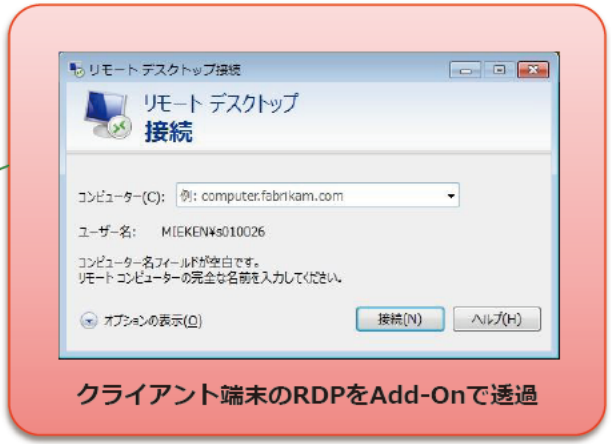
専用のプラグインを使うことで、クライアント端末にソフトウェアをインストールすることなく、Webブラウザからのリモートデスクトップや、VNC接続が可能となります。





※ クライアント端末がプロキシ経由の場合のみ、リモートデスクトップアプリケーション
からの接続方式となります。





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対策が不十分な場合は、リモート保守環境の利用を許可し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。

1. 事前準備　ヒアリングシートの記入
2. 説明会　ヒアリング（概要説明、記入シートの確認）
3. デモ利用　デモユーザにて接続動作確認
   （利用予定のアプリが正常に表示・動作するかを確認）
4. 審査　最終利用形態の決定
5. 本申請　必要書類の記載
6. 機器貸出し　県庁専用端末の貸出し

→ 利用開始