別紙7

リモート保守環境の利用について

令和元年８月１日

地域連携部 情報システム課

初版　　令和元年　８月　１日

1．リモート保守環境システム概要

- 情報システム受託事業者からのリモート保守については、情報システムが接続されているネットワークの種類により、インターネットVPN経由またはIP-VPN経由のいずれかにより三重県行政WANに接続し、保守業務を実施します。
- リモート接続する際の通信は暗号化を実施し、インターネットVPN経由による接続については、事前登録された情報システム受託事業者の任意の端末のみ接続を許可します。IP-VPN経由による接続については、リモート保守環境管理担当職員が貸し出したリモート接続端末のみ接続を許可します。

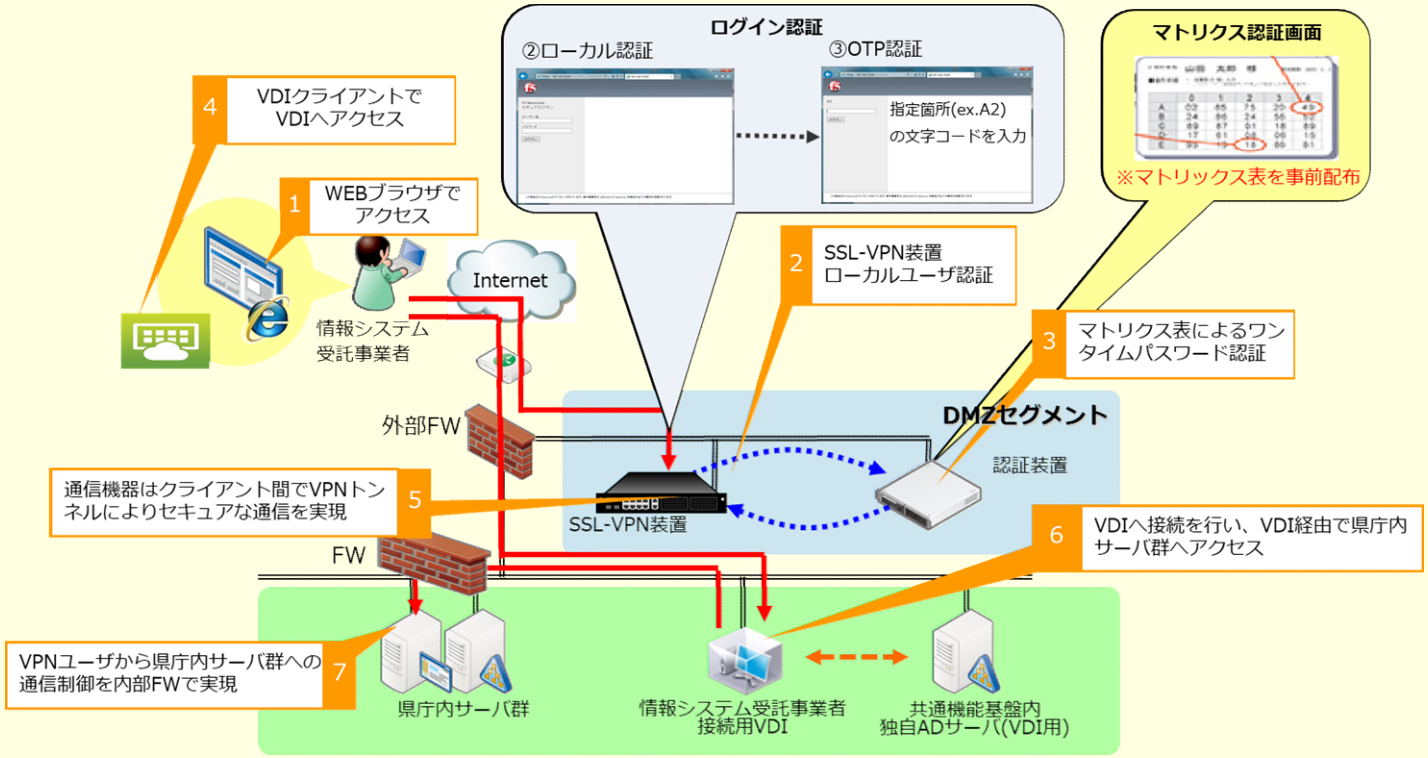
No.	システム種別	接続方式
1	業務系及びDMZ系ネットワークに接続されている情報システム	インターネットVPN経由で三重県行政WANに接続します
2	個人番号利用事務系ネットワークに接続されている情報システム	IP-VPN経由で三重県行政WANに接続します

2. インターネットVPN経由による接続（1/3）

接続概要

事前登録された情報システム受託事業者の任意の端末から、インターネットを経由してSSL-VPN通信にてVDI※1にリモート接続し、リモート保守を実施します。リモート接続する際の通信は暗号化を実施し、県庁内に構築するVDIへログイン後、サーバ群への通信を行います。

※1　デスクトップ環境を仮想化してサーバ上に集約したもの



2. インターネットVPN経由による接続(2/3)

認証方法

- マトリクス認証は、サーバから指定されたチャレンジコードに対応する行列の数値を事前配布済みのマトリクス表より入力するワンタイムパスワード認証システム。
- クライアントに特別なソフトウエアをインストールする必要は無く、ブラウザがあれば利用可能。

＜マトリクス認証概要＞

1. 認証機器のログイン画面にアクセスし、ID及びパスワードを入力します。
2. サーバから指定されたチャレンジコードに対応する行列の数値を入力します。

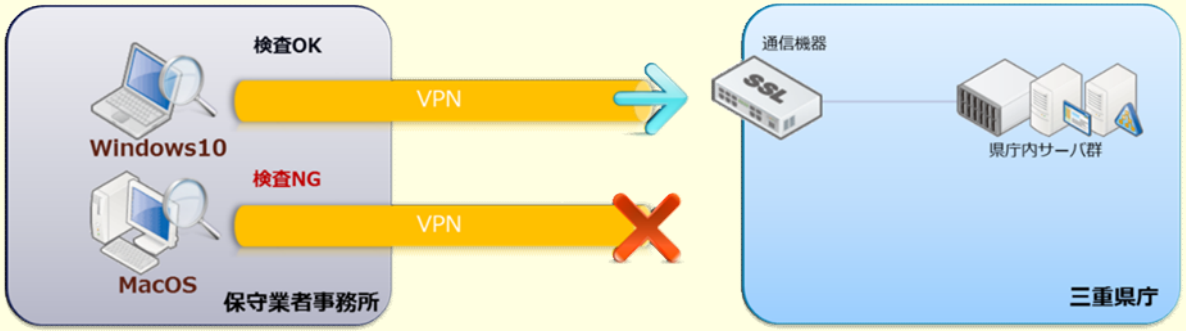
2. インターネットVPN経由による接続(3/3)

エンドポイントセキュリティ

- リモート接続時に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。

＜チェック項目＞

1. 端末固有情報
   端末固有情報を取得し、接続が許可された端末であるかチェックします。
2. Windows OS情報
   端末のWindows OS情報を取得し、接続が許可されたWindows OSであるかチェックします。
3. 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。

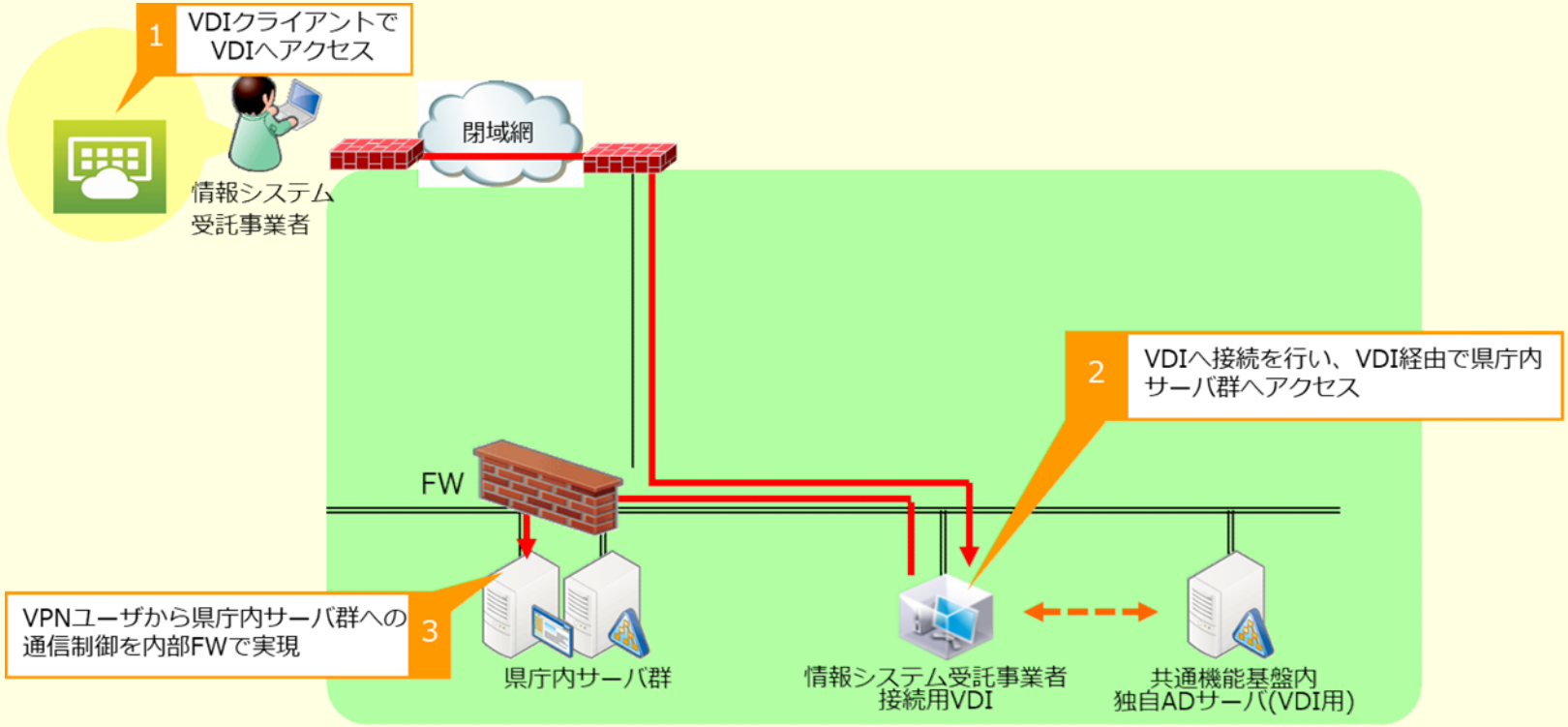


3. IP-VPN経由による接続

接続概要

リモート保守環境管理担当職員が貸し出したリモート接続端末から、閉域網を利用しIP-VPNにてVDI※1にリモート接続し、リモート保守を実施します。県庁内に構築するVDIへログイン後、サーバ群への通信を行います。

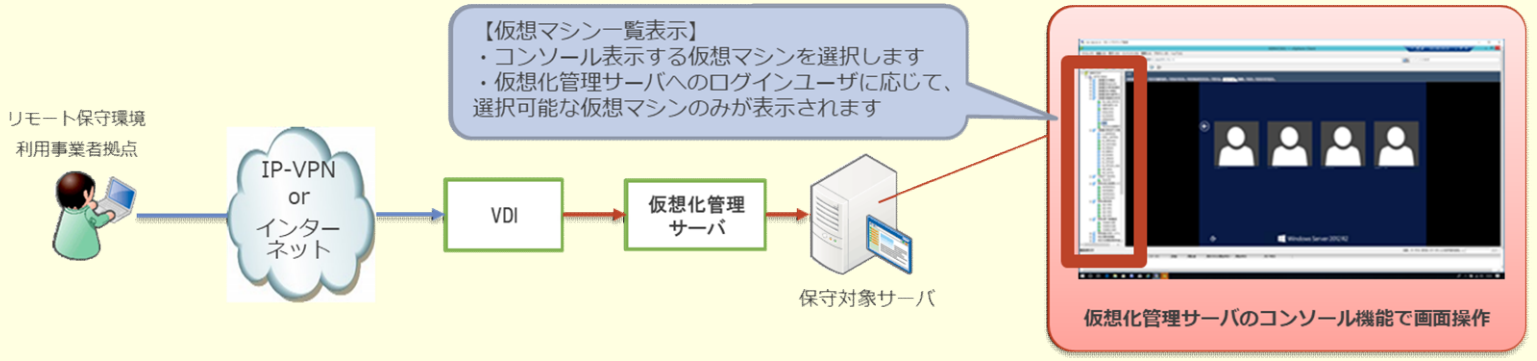
※1　デスクトップ環境を仮想化してサーバ上に集約したもの



4. ターミナル接続

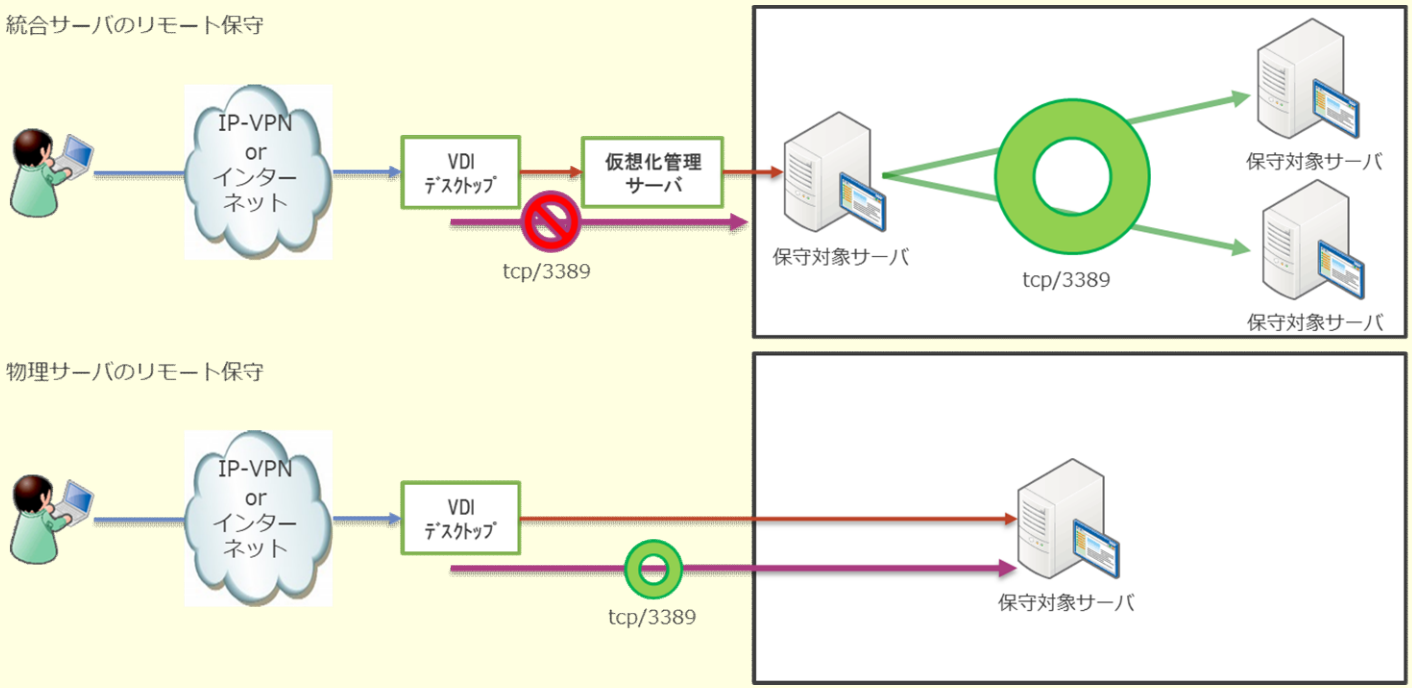
- リモート保守環境は、インターネットVPN経由の場合は、事前登録された情報システム受託事業者の任意の端末から、IP-VPN経由の場合はリモート保守環境管理担当職員が貸し出したリモート接続端末から、VDIにログインして仮想化管理サーバのコンソール機能※1を利用して県庁内サーバ群に接続します。

※1　仮想マシンへのアクセスを提供する機能



5. RDP（リモートデスクトップ）接続

- リモート保守環境は、セキュリティの観点から、原則としてVDIから県庁内サーバ群へのRDP接続（tcp/3389）を禁止とします。
  ただし、以下の条件下においてはRDP接続が可能です。
  - ✓コンソール機能で接続した保守対象サーバから、別の保守対象サーバへ接続する場合。
  - ✓物理サーバに対してリモート保守を実施する場合。



6. 接続仕様(1/2)

共通

- 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。
- 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。

インターネットVPN経由

- リモート保守環境への接続には、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おける接続要件は以下のとおりです。

№	項目	要件
1	OS	Windows 8.1以降
2	Webブラウザ	Internet Explorer 11
3	ウイルス対策	➢ トレンドマイクロ(ウイルスバスター) ➢ シマンテック(ノートン) ➢ マカフィー ➢ ESET ➢ カスペルスキー

- リモート接続端末のセキュリティアップデート(Windows Update)は、一定の条件で適用されている必要があります。
- リモート接続端末の固有情報の事前登録が必須となります。

６．接続仕様（2/2）

IP-VPN経由

- リモート保守環境への接続には、情報システム受託事業者ごとにIP-VPN回線が必要となります。
- リモート保守環境への接続には、リモート保守環境管理担当職員が貸し出したリモート接続端末が必須となります。

7. 制限事項

共通

- 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利用に際し、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。）
- リモート保守作業以外の構築・導入テスト等の作業に関しては、原則現地での作業となります。

インターネットVPN経由

- リモート接続端末のセキュリティ対策が不十分な場合は、リモート保守環境に接続できません。

IP-VPN経由

- IP-VPN回線の調達から利用開始までに最大で3カ月程度要するため、申請にあたっては当該期間を考慮して申請を行ってください。

8. 構築の流れと役割分担(インターネットVPN経由)

凡例　○:担当　△支援　ー:担当なし

№	作業項目	リモート保守環境管理担当		情報システム担当		作業内容
		受託事業者	担当職員	担当所属	受託事業者	
1	インターネット接続環境準備	ー	ー	ー	○	インターネット接続環境を準備する。(ただし、インターネット接続環境がある場合には、新たに準備する必要はありません。)
2	VDI環境作成	○	ー	ー	ー	VDI環境はリモート保守環境受託事業者が作成する。
3	VDI環境設定	ー	ー	ー	○	情報システム受託事業者にて、VDI環境に独自の設定が必要な場合は設定を行う。
4	リモート接続端末準備	ー	ー	ー	○	リモート接続端末を準備する。(ただし、前述の「6. 接続仕様」を満たす端末がある場合には、新たに準備する必要はありません。)
5	リモート接続端末設定	ー	ー	ー	○	リモート接続端末を設定する。 リモート保守環境受託事業者は、VDI環境に接続するためのソフトウェアと設定手順書を提供する。
6	リモート保守環境動作確認	△	ー	ー	○	情報システム受託事業者は、以下の動作確認を行う。 ➢ リモート接続端末から三重県行政WANへのインターネットVPN接続(SSL-VPN、マトリクス認証) ➢ リモート接続端末からVDI環境への接続 ➢ VDI環境から仮想化管理サーバへの接続 ➢ 仮想化管理サーバから情報システムの仮想マシンへの接続 リモート保守環境受託事業者は、情報システム受託事業者の動作確認に対して問合わせ対応を行う。

9. 構築の流れと役割分担(IP-VPN経由)

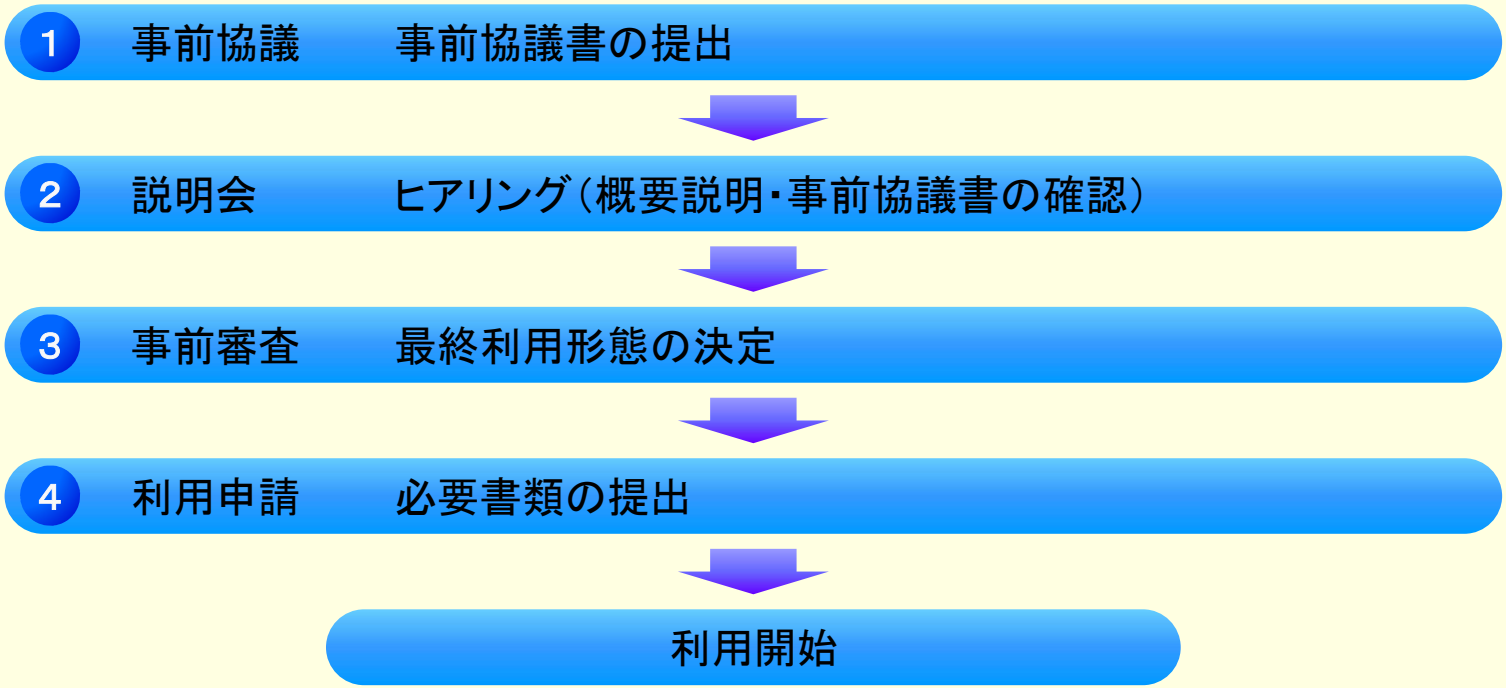
凡例　〇:担当　△支援　ー:担当なし

№	作業項目	リモート保守環境管理担当		情報システム担当		作業内容
		受託事業者	担当職員	担当所属	受託事業者	
1	拠点※1側IP-VPNサービス・回線調達	〇	ー	ー	ー	拠点側IP-VPNサービス・回線を調達する。
2	拠点側VPN装置調達	〇	ー	ー	ー	拠点側VPN装置を調達する。
3	拠点側VPN装置設定	〇	ー	ー	ー	拠点側VPN装置を設定する。
4	拠点側VPN装置設置	〇	ー	ー	ー	拠点側VPN装置を設置する。
5	VDI環境作成	〇	ー	ー	ー	VDI環境は、リモート保守環境受託事業者が作成する。
6	VDI環境設定	ー	ー	ー	〇	情報システム受託事業者にて、VDI環境に独自の設定が必要な場合は、情報システム受託事業者が必要な設定を行う。
7	拠点側リモート接続端末調達	ー	〇	ー	ー	リモート接続端末は、リモート保守環境管理担当職員が調達する。
8	拠点側リモート接続端末設定	〇	ー	ー	ー	リモート接続端末は、リモート保守環境受託事業者が設定する。
9	拠点側リモート接続端末設置	〇	ー	ー	ー	リモート接続端末は、リモート保守環境受託事業者が設置する。
10	リモート保守環境動作確認	△	ー	ー	〇	情報システム受託事業者は、以下の動作確認を行う。 ➢ リモート接続端末からVDI環境への接続 ➢ VDI環境から仮想化管理サーバへの接続 ➢ 仮想化管理サーバから情報システムの仮想マシンへの接続 リモート保守環境受託事業者は、リモート保守環境の動作確認に対して問合わせ対応を行う。

※1　情報システム受託事業者の保守拠点

10. 利用・申請の流れ（インターネットVPN経由）

- インターネットVPN経由によるリモート保守環境の利用開始までの流れは以下のとおりです。



11. 利用・申請の流れ（IP-VPN経由）

- IP-VPN経由によるリモート保守環境の利用開始までの流れは以下のとおりです。