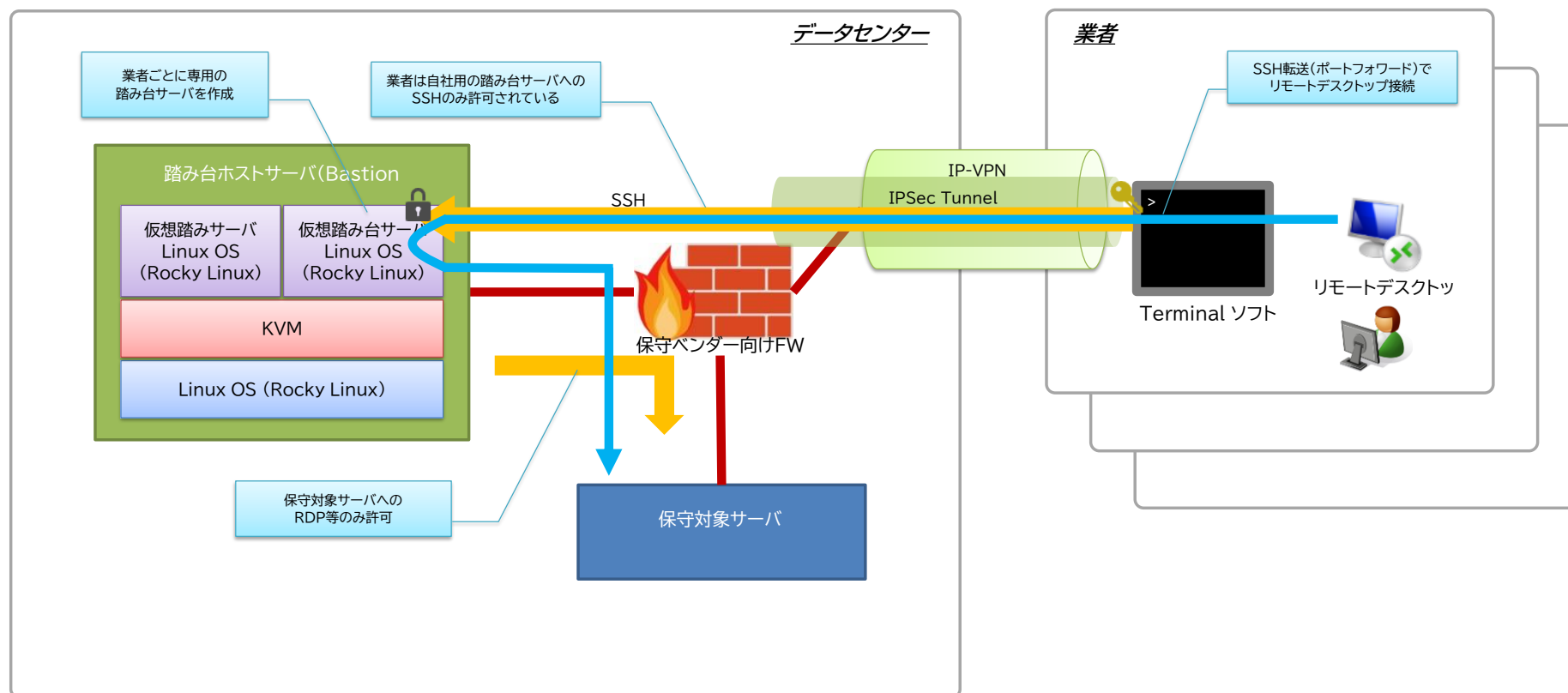


リモート保守等ネットワーク概要図



- ・データセンターと保守業者間で、VPN回線等を敷設
- ・データセンターと保守業者ルータ(FW)間でトンネル(IPSec)接続
- ・ファイアウォールと踏み台用のホストサーバを準備し、サーバをDMZに配置
- ・原則、外部→DMZはSSHのみ、DMZ→内部はRDPのみを許可(遠隔ベンダー向けFWでまとめて管理)
- ・仮想踏み台サーバは業者ごとに作成し、接続用のユーザ、SSH秘密鍵、パスフレーズと合わせて払い出し
- ・仮想踏み台サーバは普段は停止状態とし、申請を受けて起動する

【主なセキュリティ対策】

IP-VPN … 通信事業者による仮想ネットワーク → インターネットからの秘匿
 IPsec Tunnel … 通信機器間の暗号化 → 同一IP-VPNグループ内の拠点間の隔離(拠点限定)
 SSH … 端末間(クライアント→サーバ)通信の暗号化 → 同一ネットワーク内からの通信秘匿
 鍵認証 … パスワードではなく鍵ファイルで認証 → OSユーザパスワードの秘匿
 パスフレーズ … 鍵ファイル使用にパスワード(OSユーザとは別)が必要 → 二要素認証
 踏み台サーバ … 業者からの入り口を限定 → 接続時間や接続元の限定
 業者毎踏み台サーバ … 業者毎に許可された保守対象サーバにのみアクセスを限定