

	パターン1	パターン2	パターン3	パターン4	パターン5	パターン6
	リモートデスクトップ方式	仮想デスクトップ方式	クラウド型アプリ方式	セキュアブラウザ方式	アプリケーションラッピング方式	会社PCの持ち帰り方式
概要	オフィスにある端末を遠隔操作	テレワーク用の仮想端末を遠隔操作	クラウド上のアプリケーションを社内外から利用	特別なブラウザを用いて端末へのデータ保存を制限	テレワーク端末内への保存を不可とする機能を提供	オフィスの端末を持ち帰りテレワーク端末として利用
テレワーク端末に電子データを保存するか？	保存しない	保存しない	どちらも可	保存しない	保存しない	保存する
オフィスの端末と同じ環境を利用するか？	同じ	テレワーク専用の環境	クラウド型アプリに関しては同じ	ブラウザ経由で利用するアプリに関しては同じ	テレワーク専用の環境	同じ
クラウドサービスを利用するか	しない	しない	する	する	する/しない どちらも可	する/しない どちらも可
高速インターネット回線の必要性	必須	必須	望ましい	望ましい	望ましい	不要

	IPSec-VPN	SSL-VPN
リモートアクセス端末への 専用ソフトインストール/環境設定	必要 環境設定も複雑 (専用ソフトは、IPSec-VPN装置と同一メーカー製品が原則)	不要 専用ソフトが必要な場合は自動インストール、自動環境設定
リモートアクセス端末機器	△ 専用ソフトが対応している装置 (パソコンが中心)	○ パソコン、 携帯電話 (WEBブラウザ使用)
コンテンツやサーバーに対する アクセス制御	△ 難しい	○ 容易
初期導入コスト	○ 低い	△ 高い
運用管理コスト	△ 高い	○ 低い
既存ネットワークへの適用性	△ NAT (アドレス変換)、ファイアウォール越えなどの考慮が必要	○ シームレスに導入可能
性能 (処理速度・アクセス速度)	○ SSL-VPNより高速	△ IPSec-VPNより低速

	リバースプロキシ方式	ポートフォワーディング方式	L2フォワーディング方式
リモートアクセス 端末側構成要素	WEBブラウザ	WEBブラウザ＋モジュール (WEBからダウンロード、自動インストール)	WEBブラウザ＋モジュール (WEBからダウンロード、自動インストール)
使用可能アプリケーション	△ WEBアプリケーション	○ 通信中ポート番号が変わるものは 使用できない場合あり	◎ ほとんどのアプリケーションで 使用可能
リモートアクセス 端末機器	○ WEBブラウザが動く端末	△ モジュールの仕様によって制限 利用時に管理者権限が必要	△ モジュールの仕様によって制限
用途	出張先の端末などから簡単に使いたい。 仕様アプリケーションはWEBメールやWEB型グループウェアなどWEBページ中心	クライアント端末のOSが様々である。 ある程度の種類のアプリケーションを使いたい	アプリケーションを制限なく使いたい。 使用されるクライアント端末の種類は限られている。

名前	概要	ログ能力	鍵交換	webUI	適用先	適用難易度	
sshportal	動的にユーザとホストを構成するBastionサーバーツール	あり	RSA	なし	Gateway Server	少し難しい	導入や使用法などがあまり詳細に記されていない。
sshuttle	擬似的な簡易VPN	あり	※VPN	なし	クライアント	易しい	専用のサイトが用意されている上に、導入手順が詳細に記されている。
sshpiper	プロキシのようなソフトウェア	あり	RSA	あり	クライアント	すこし難しい	導入や使用法などがあまり詳細に記されていない。

名前	概要	ログ能力	key exchange	webUI	適用先	適用難易度	
Aker	FreeIPAを利用したBastionサーバーツール	あり	Kerberos チケット	なし	Gateway Server, HostServer, クライアント	難しい	python2とpython3の依存関係の問題あり。 インストールまでの説明が少ない。
teleport	リモートアクセスするためのセキュリティゲートウェイ	あり	SSL証明書	あり	Gateway Server, HostServer, クライアント	すこし難しい	管理者専用のサイトが用意されており、導入まで丁寧に記載されている
SoftEther VPN	レイヤ2でカプセル化やトンネリングを行う、VPN構築ソフトウェア	あり	認証 RSA 暗号化 AES、DES など	なし	Gateway Server, HostServer, クライアント	すこし易しい	インストールまでのロードマップが用意されている コンピュータネットワークへの深い知識が必要

Serverのメーカー	Supermicro
Serverのモデル	SYS-5018D-FN4T
CPU	Intel(R) Xeon(R) CPU D-1541 @ 2.10GHz コア 8コ, スレッド 16コ, 物理CPU 1コ
マザーボード	メーカー：Supermicro 型番：X10SDV-8C-TLN4F
メモリ	128GB
ストレージ	モデル：ATA SAMSUNG MZ7LM240 (scsi) ハードディスク /dev/sda: 240GB セクタサイズ (論理/物理): 512B/512B ×2
ネットワーク	メーカー：Intel 2x Gigabit Ethernet LAN ports 2x 10GBase-T ports 1x Dedicated IPMI LAN port

メーカー	FXC株式会社
製品型番	FXC5210
データ転送速度	10/100/100Mbps(CSMA/CD)
イーサネットポート 10BASE-T / 100BASE-TX /1000BASE-T	8ポート 2SFP(Small Form Factor Pluggable)
総スループット	14.8Mpps(64byte)
総帯域幅	20Gbps
MACアドレス登録数	8,000個

求める機能	実現する技術	ソフトウェア
①踏み台数(段数)の削減	VPN トンネリング	sshuttle SoftEtherVPN
②トンネルの管理の容易化	特になし	該当なし
③ログイン時の入力作業の削減	シングルサインオン (Kerberos) 公開鍵、証明書認証 (SSH)	試用した全てのソフトウェア
④ユーザ情報の一括管理	LDAP Kerberos RADIUS	Active Directory sshportal Teleport SoftEtherVPN
⑤情報登録の自動化	特になし	該当なし
⑥GUI	特になし	Teleport SoftEtherVPN
⑦ログの取得	特になし	sshportal Teleport SoftEtherVPN
⑧E2Eのみのログイン情報による利用	VPN	sshuttle SoftEtherVPN Teleport

	sshuttle	sshportal	Teleport	SoftEtherVPN	Active Directory
①踏み台数(段数)の削減	✓ VPN	—	—	✓ VPN	—
②トンネルの管理の容易化	—	—	—	—	—
③ログイン時の入力作業の削減	✓	✓	✓	✓	✓
④ユーザ情報の一括管理	—	✓ LDAP	✓ RADIUS LDAP	✓ RADIUS LDAP	✓ LDAP Kerberos
⑤情報登録の自動化	—	—	—	—	—
⑥GUI	—	—	✓	✓	—
⑦ログの取得	—	✓	✓	✓	—
⑧E2Eのみのログイン情報による利用	✓ VPN	—	—	✓ VPN	—

求める機能	実現する技術	ソフトウェア
SSHの段数の削減	VPN トンネリング	sshuttle SoftEtherVPN
トンネルの管理の容易化	特になし	該当なし
ログイン時の入力作業の削減	シングルサインオン (Kerberos) 公開鍵、証明書認証 (SSH)	試用した全てのソフトウェア
ユーザ情報の一括管理	LDAP Kerberos RADIUS	Active Directory sshportal Teleport SoftEtherVPN
情報登録の自動化	特になし	該当なし
WebUI	特になし	Teleport SoftEtherVPN
ログの取得	特になし	sshportal Teleport SoftEtherVPN
E2Eのみのログイン情報による 利用	VPN	sshuttle SoftEtherVPN Teleport

Serverのメーカー	Supermicro
Serverのモデル	SYS-5018D-FN4T
CPU	Intel(R) Xeon(R) CPU D-1541 @ 2.10GHz コア 8コ, スレッド 16コ, 物理CPU 1コ
マザーボード	メーカー：Supermicro 型番：X10SDV-8C-TLN4F
メモリ	128GB
ストレージ	モデル：ATA SAMSUNG MZ7LM240 (scsi) ハードディスク /dev/sda: 240GB セクタサイズ (論理/物理): 512B/512B ×2
ネットワーク	Dual LAN メーカー：Intel Corporation 型番：X552/X557-AT 規格：10GBASE-T メーカー Intel Corporation 型番：I2500-Gigabit Network Controller