

## 5.1 ターミナルサービスの概要

### 5.1.1 機能概要

ターミナルサービスは、複数クライアントのデスクトップ環境を、リモートベースで一元的に提供するサーバーサービスです。Windows Server 2008では役割サービスの「ターミナルサービス」として、サーバーマネージャからインストールできます。

クライアントがリモートデスクトップ接続やRemoteAppを使ってアクセスすると、サーバー側でデスクトップ環境やアプリケーションが起動し、クライアント側ではデスクトップ画面やキーボード、マウスの動作、あるいはアプリケーションの実行画面だけが送信されます。各セッションは別々に動作するため、ユーザー同士が干渉することはありません。

ターミナルサービスを使って、アプリケーションを1台のターミナルサーバーから提供することで、次のメリットがあります。

まず、アプリケーションを個々のクライアントコンピュータにインストールする必要がないため、システム管理者の管理コストを下げることができます。

また、アプリケーションは高スペックなサーバー側で実行されるため、クライアント側のOSやスペック上の制限を受けません。例えばLinuxからリモートデスクトップ接続(rdesktopプログラム)を利用することも、可能です。

ターミナルサービスとの通信は、効率的に画面情報を送信するRDP(Remote Desktop Protocol)が使われており、狭いネットワーク帯域向けにチューニングも可能なため、アプリケーションからWAN経由でアクセスするより、ターミナルサービスを利用する方がよいパフォーマンスを得られることがあります。

あわせて、ターミナルサービスでは、各ユーザーのドキュメント類は基本的にターミナルサーバー上で管理され、クライアントに保存されません。そのため、クライアントコンピュータごとファイルを紛失するといったこともありません。ただし、リダイレクト設定によって、クライアントのローカルリソースのドライブヘデータを保存することも可能です。

### 5.1.2 ターミナルサービスのアーキテクチャ

ターミナルサービスは、次のような主要五つのサービス役割から成り立っています。

## ■ ターミナルサーバー

リモートデスクトップ接続やRemoteAppを利用して接続するクライアントに対して、ターミナルサービスのコア機能を提供します。具体的にはマルチユーザーレベルでのデスクトップやアプリケーションウィンドウ環境と、それらの画面表示や入力デバイスからの入出力に関する機能一般を提供します。

ターミナルサーバーでは、RDPを利用して、3389/tcpポートで通信を行います(図5.1)。RDPでは画像データそのものを送受信するのではなく、画面やキーボード、マウスの操作をデータ化して送受信するため、操作レスポンスが下がりにくい、という特長があります。また、各ユーザーのセッションやデスクトップはそれぞれ個別に生成され、干渉し合うといったことはありません。

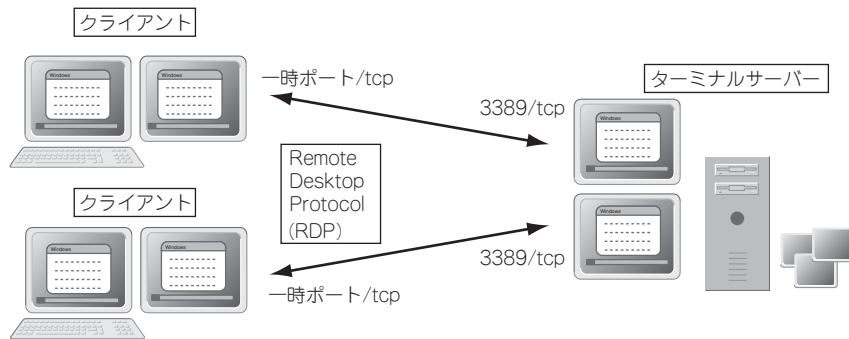


図5.1 リモートデスクトップ

また、ターミナルサーバーではデスクトップだけではなく、アプリケーション機能も提供します。ユーザーがファイルやショートカットを起動すると、3389/tcpでターミナルサーバーに接続し、必要なアプリケーションを呼び出して、RDPを透過的に利用してアプリケーションウィンドウを表示します。ユーザーはローカルアプリケーションを使用しているのと同じ操作環境で、ターミナルサーバー上のアプリケーションを使用することができます(図5.2)。呼び出されたウィンドウ内のみ、リモートデスクトップを利用しているというイメージです。これはRemoteAppと呼ばれます。

ターミナルサーバーはリモートデスクトップ接続クライアントプログラムを通して、クライアントにサービスを提供します。最新版は「リモートデスクトップ接続6.1」となり、RDP 6.1プロトコルが利用されます。それ以前のバージョンでも利用はできますが、一部の機能が利用できなくなります。

OSにより、初期インストールされているリモートデスクトップ接続は異なりますが、プログラムをアップグレードすることが可能です。

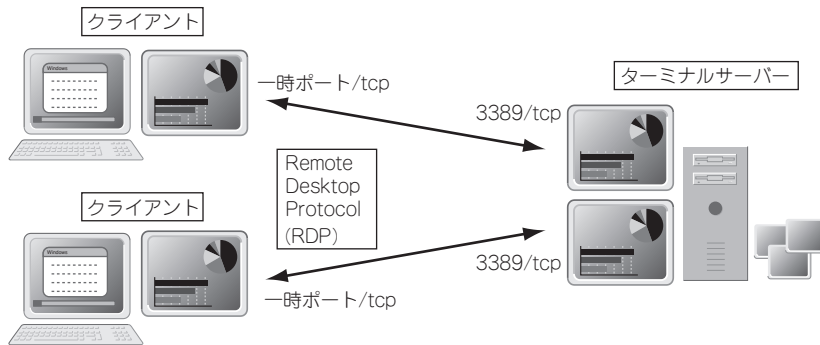


図5.2 RemoteApp

### ■ ターミナルサービスWebアクセス(TS Webアクセス)

TS Webアクセスの機能を使用すると、ユーザーはWebブラウザからRemoteAppプログラムを起動することができます(図5.3)。管理者はTS Webアクセスを使用することで、RemoteAppプログラムを、より容易に構成、展開できます。

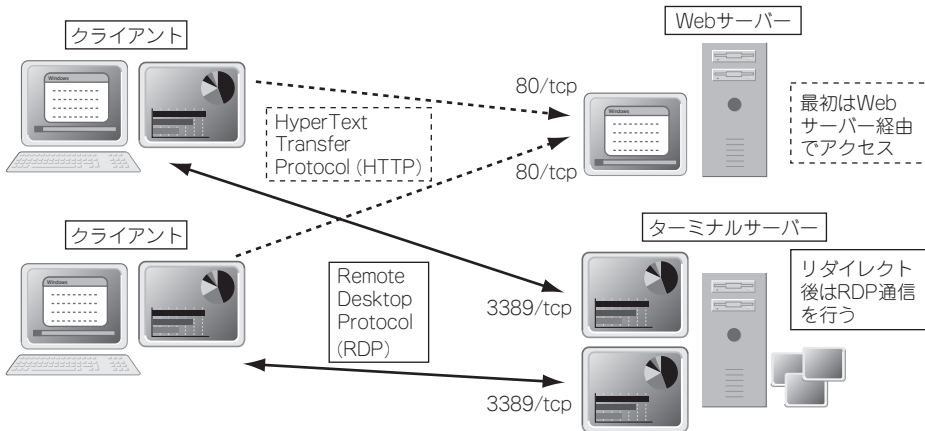


図5.3 TS Webアクセス

### ■ ターミナルサービスライセンス(TSライセンス)

クライアントがターミナルサーバーと接続する際に必要な、ターミナルサービスクライアントアクセスライセンス(TS CAL)を管理し、TS CALの発行や確認を行います。

ターミナルサービスでは、利用するクライアントやユーザーに対して、TS CALを割り当てなければ、サービスを利用できません。そのため、TS CALのアクティブ化や割り当てを、TSライセンスサーバーが実行します。

また、クライアントにTS CALが割り当てられているか、TS CALが不正な状態でないかを、ターミナルサービス接続時にTSライセンスに自動的に確認を行うようになっ

ています。TSライセンスについては「5.2.2 ターミナルサービスライセンスの概要」を参照してください。

### ■ ターミナルサービスゲートウェイ(TSゲートウェイ)

インターネットを含む、ネットワーク外部から、内部のターミナルサーバーに、認証されたユーザーのみを接続するためのゲートウェイサービスを提供します。

ターミナルサービスは、イントラネットで利用される前提で実装されているため、インターネットから直接利用したい場合、セキュリティ上不安な部分があります。このような場合、外部からの接続に対して、セキュリティを高める実装が必要です。

TSゲートウェイは、HTTPS(443/tcp)プロトコルを使って外部から接続を受け付け、内部のターミナルサーバーにはRDP(3389/tcp)でリダイレクトを行います(図5.4)。

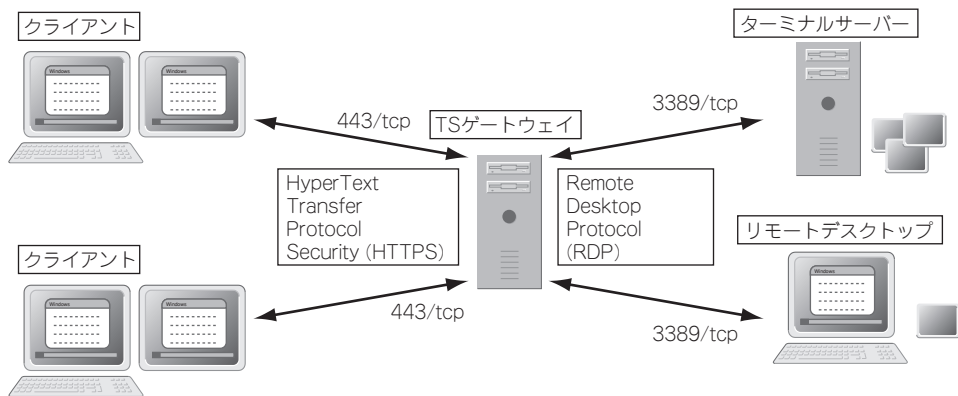


図5.4 TSゲートウェイ

### ■ ターミナルサービスセッションブローカ (TSセッションブローカ)

負荷分散されたターミナルサーバー群に対して、ユーザーが適切なターミナルサーバーに接続するためのソリューションを提供します。

多数のユーザーに対して、安定したターミナルサービスを提供したい場合、複数のターミナルサーバーを配置した上、負荷分散を使ってユーザーを分散配置する方法が採られます。

TSセッションブローカは、ターミナルサーバーへのセッション状況を確認し、負荷分散をとおして新規のログオンセッションが発生したとき、もっともセッション数の少ないターミナルサーバーへリダイレクトします(図5.5)。

また、各ターミナルサーバーのセッション状況を記録して、いったん切断されたセッションについて、同じクライアントが再接続を要求したときに、切断されたセッションに再接続させることができます。