セキュリティ端末としてのシンクライアントの導入要件

～ 要求が多様化するシンクライアント･ソリューションへの対応 ～

尾関　隆章

企業の情報セキュリティへの取り組みが本格化するとともに，情報漏洩リスクへの対策としてシンクライアント導入の動きが急速に高まっている。

企業・自治体などでシンクライアントを導入する場合，PCの利用環境の違いや利用しているアプリケーションの種類によりさまざまな要件が生じ，シンクライアントとサーバを連携させたシステムの構築形態は一様とはならないのが現状である。

このような種々の用件に対応するため，2005年に入ってからは，従来のシンクライアント端末売りから脱却し，サーバ側システムと連携した各種ソリューションの提案が，大手ITベンダにより続々と発表されている。

本稿では，セキュリティ端末としてのシンクライアントを導入する上での技術的要件について，当社が今まで行ってきたシンクライアントコンサルティングサービスでの経験を元に，シンクライアント端末の観点とSBC（Server Based Computing）のようなサーバ側の観点から紹介する。

シンクライアント端末とSBCのメリット

シンクライアントはネットワーク端末として機能し，それ自体スタンドアローンでPCと同じように使用することはできないため，必ずネットワークを介してサーバと接続しSBCの形態で使用される。

このため，企業においてシンクライアントシステムを導入する上でのメリットは，次の二つの観点から捉えられるべきである。

●端末をシンクライアントにするメリット
●SBCを適用するメリット

まず，端末を従来のPCからシンクライアントに置き換えることによるメリットとして；

① 端末からの情報漏洩を根本的に防止
（データ保持不可，外部メモリ接続不可）
② 端末からのウィルス感染を防止
（ハードディスクなし，サーバ上で動作）
③ 端末の管理負担を極小化
（ソフトウェア管理，ハードウェア管理，故障対応）
④ 端末の維持コストを極小化
（低故障率，低電力使用，リサイクルコスト低減）

などの点を挙げることができる。

次に，SBCを適用することによるメリットとしては；

⑤ サーバ集中アーキテクチャによる管理負荷の低減
（端末の環境設定・管理の集中化）
⑥ アプリケーションの一括管理
（インベントリ管理，バージョンアップ管理）
⑦ 端末のフリーロケーション化
（どの端末からも個人の仮想端末環境にログイン可）

が挙げられる。

ここで，SBCアーキテクチャを適用する場合には，必ずしも端末をシンクライアントに置き換える必要はないことに留意したい。

すなわち，SBCアーキテクチャの構築により上記 ⑤～⑦ のサーバ集中型システムのメリットだけを享受したいのであれば，端末をシンクライアントに置き換える必要はなく，端末として従来のPCを使用することができる。

一方，端末をシンクライアントに置き換える目的は，上記 ①～④ のメリットを獲得することであるが，必然的に⑤～⑦ のSBC適用によるメリットも享受できることになる。

すなわち，シンクライアントの導入は①～⑦ までのセキュリティ強化のメリットと管理・運用コスト（TCO）削減のメリットを同時に享受できるという，より効果の大きい対策といえる。

シンクライアントとSBCの種類と構成方法

シンクライアントシステムとは，一般的には『端末には最低限の機能しか持たせず，アプリケーションソフトやファイルなどの資源をサーバ側で管理するシステムの総称』と定義される。シンクライアントがPCと大きく異なるのは，『ハードディスクを持たない』ことと『スタン

ドアローンでは機能がほとんどない』という点である。

シンクライアント端末の種類を，それを提供するベンダの専門分野から大別すると（**図1**参照）；

a）レガシーシンクライアント

主にシンクライアント専業ベンダが提供するシンクライアント。

使用されるOSは，Windows CE，XPe，Linux，独自OS などがあり，シンクライアントの特徴である機能の軽さを重視した製品が多い。

b）ディスクレスPC

主にPCベンダが提供するシンクライアント。

OSはWindows XPeが主流であり，PCに近いフレキシビリティを特徴とする製品が多い。

c）ユビキタスシンクライアント

Linuxプレイヤー，セキュリティベンダが提供するアタッチメント型シンクライアント。

図1　シンクライアントの種類

PCにUSBキーなどをアタッチすることにより，シンクライアントとして動作する環境を提供する製品であるが，シンクライアントとしての完成度に課題を残す。

一方，SBCあるいはそれに類似したセンタ側システムの構成として以下の4種類を挙げることができる[1)]。

（1）画面転送型（図2参照）

本構成はSBCシステムのデファクトスタンダード的なシステムと言える。

センタのサーバにはWindowsサーバが適用されサーバOSの機能である『ターミナルサービス』を使用してサーバOS上でクライアントのアプリケーションが走行し，アプリケーションが使用するファイルも全てサーバ上に格納される。

サーバとクライアントとの間では画面転送のための通信が行われ，クライアント側のディスプレイではPCと同様の画面と操作性を得ることができる。

このとき，サーバとクライアント端末との間で使用される通信プロトコルは Remote Desktop Protocol（RDP）と呼ばれる。また，画面転送型のシステム構成では，ターミナルサービスの機能を補足しシステムの管理を容易にする目的で，SBCツールを利用するケースも多い。

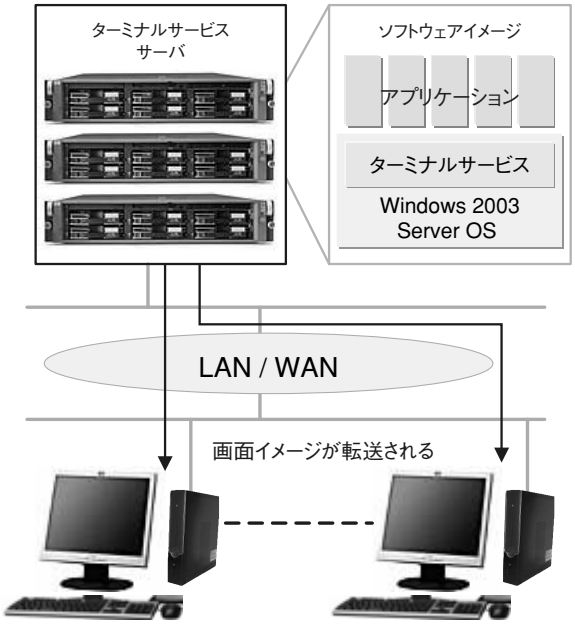

図2　画面転送型

SBCツール・ソフトウェアとして，MetaFrame*[1)]（旧称，現在は Citrix Presentation Serverと呼ばれる）が知られている。MetaFrameが使用される場合には，サーバ～端末間プロトコルはRDPではなく，Independent Computing Architecture （ICA）プロトコルが使用される。

*1）MetaFrameおよびCitrix Presentation ServerはCitrix Systems, Inc.の登録商標です。

(2) ブレードPC型（図3参照）

センタにサーバを設置する代わりに，PCのハードウェア（CPU，HDD，メモリなど）を独立したブレード型のユニットに搭載し，これをクラスタ状にラック内に収容し，センタ側に設置する方式がブレードPC型システムである。

この方式では，個別のPC機能がセンタに移行・集約された形となるため，従来PCで行っていた業務は全てブレードPC上で実行することができる。

ブレードPCとシンクライアント間の通信には前述のRDPプロトコルを使用することが可能であるが，独自のプロトコル（アナログインタフェース）を使用するブレードPCシステムもある。

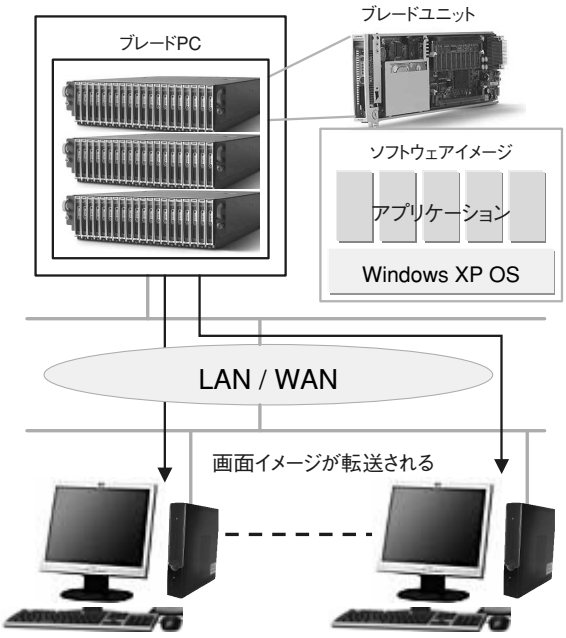

図3　ブレードPC型

(3) 仮想PC型（図4参照）

前述のブレードPC方式がハードウェア的に個別PCをセンタに集約した形態であったのに対し，サーバ上のソフトウェアで仮想的に個別PCを構築する方法がこの仮想PC型システムである。

具体的には，WindowsサーバOS上にソフトウェアの仮想実行環境を提供するミドルウェア（VM Ware*2) など）を実装し，その上でWindows XP OSとアプリケーションを走行させる方式である。

（2）の方式をソフトウェアで実現した方式であるので，機能的特徴は（2）のシステムと類似している。

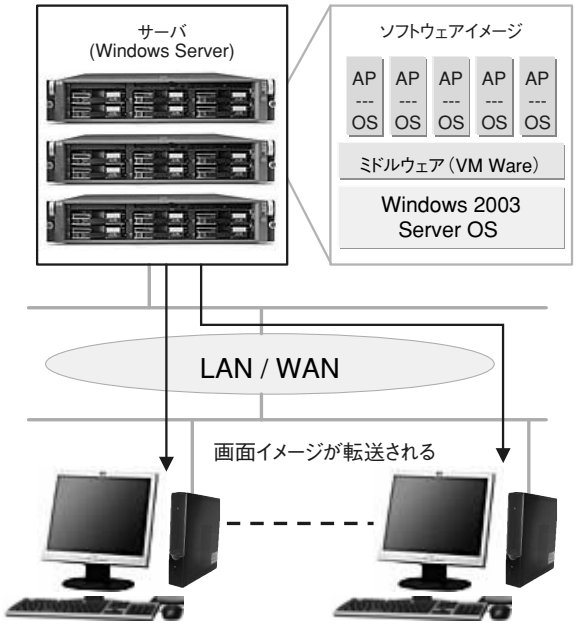

図4　仮想PC型

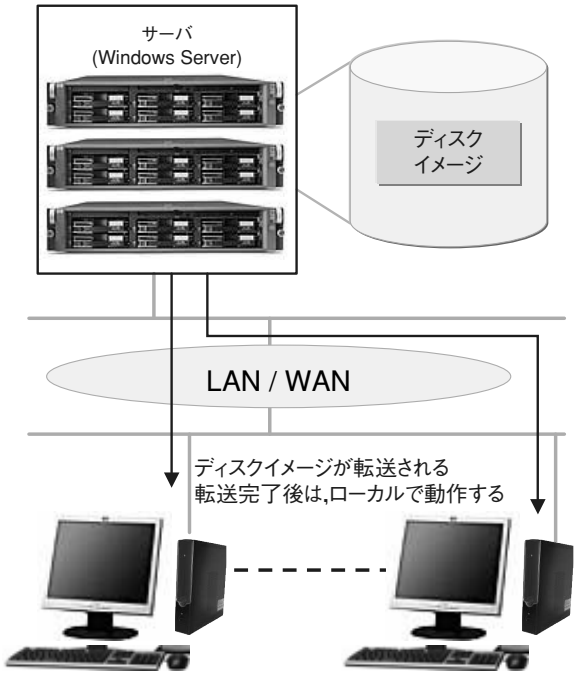

図5　ネットワークブート型

(4) ネットワークブート型（図5参照）

PCに内蔵されるハードディスク部分をセンタに移行し集約した形態が，このネットワークブート型システムである。

センタのサーバにはPCのディスクイメージを格納し，端末の電源が投入されるとこのディスクイメージがサーバ

*2)VM WareはVM Ware Inc.の登録商標です。

から端末に転送される。したがって，シンクライアントの電源投入時にPCとして動作するための全てのファイルがサーバから転送されるため，ファイルイメージの転送が完了した後は従来のPCと同様に使用することができる。

以上の通り，シンクライアントを適用するためのSBCシステムにはそれぞれ特徴の異なった方式があり，業務への適合性に応じて適切なシステムが選択されることになる。

次に，（1）～（4）の方式の特徴を以下に述べる。

【(1) 画面転送型の特徴】

SBCの典型的な構成であり，シンクライアントとの組み合わせで最も実績のある方式である。

PC上で動作する一般的なアプリケーションの大部分は使用することができるが，一部のアプリケーションはサーバ上でのマルチユーザ環境で動作しない場合がある。このようなケースでは，アプリケーションの一部変更あるいは初期ファイルの修正といったチューニングが必要になる。

また，RDPあるいはICAプロトコルを使用してサーバからクライアント端末への画面転送を行っていることにより，クライアント上での動画再生ではプロトコルに起因する制約が生じ，動画で不自然な再生となる場合がある。

【(2) ブレードPC型の特徴】

上記（1）の方式での難点である『一部のアプリケーションはサーバ上でのマルチユーザ環境で動作しない』という制約を，このブレードPC型では解消することができる。

一方，本方式は個々のPCをハードウェア的に集約した形態であるため，ハードウェアコストがかさむ点が難点となる。

また，ブレードPCと端末との間の通信をRDPでなくアナログインタフェースで繋ぐ方式では，上記（1）の『動画表現への制約』を解消することができる。しかし，このアナログインタフェース方式の場合，サーバ～端末間の距離が200m程度までしか延ばせないという制約が課せられる。

【(3) 仮想PC型の特徴】

上記（2）と同様に『アプリケーションへの制約』は解消することができる。

本方式ではサーバ上のソフトウェアで仮想PCを走行させる構成となり，1クライアント当たりに必要となるサーバリソースが（1）の画面転送方式に比較して，かなり大きくなることが課題である。

【(4) ネットワークブート型の特徴】

本方式は厳密にはSBC式ではなく，シンクライアントを端末として使用したセンタ管理（ブート）型の方式である。

サーバからディスクイメージをブートしてPCと同等の機能を実現する方式であることから，同一の端末に必要に応じて種々のディスクイメージをブートすることにより，全く異なる端末として使用することができるため，PCの教育・研修などの用途には向いているといえる。

ただし，ディスクイメージ転送時には大容量のファイル転送が必要であり，複数の端末が同時に起動するケースも一般的であることから，サーバ～端末間のネットワークを大容量化する必要がある。

以上に示したそれぞれの構成が適用されるケースを例示する。

4方式のうちで実際に最も多く採用されている（1）の『画面転送型』を標準的な構成と仮定した場合；

- （1）の『画面転送型』方式の制約により正常に動作しないアプリケーションを業務上どうしても使用する必要がある場合，（2）の『ブレードPC型』あるいは（3）の『仮想PC型』を適用する。
- シンクライアントシステムを適用し，かつ動画の再生を正常に行う必要がある場合には，（2）のアナログインタフェース方式を適用する。
- 教育・研修現場のように，ある特定の『PC環境』を任意に提供・解除したい場合には，（4）の『ネットワークブート型』を適用する。

といった選択がある。

すなわち，一般的なアプリケーションソフトウェアを使用する業務環境では，（1）の『画面転送型』を適用することができるが，特定のアプリケーションへの制約を回避したい場合には（2）の『ブレードPC型』または（3）の『仮想PC型』の適用が必要となり，教育・研修現場のような特定の使用目的がある場合には（4）の『ネットワークブート型』を適用する，と考えることができる。

ターミナルサービスとSBCツールの使い分け

画面転送型システムを導入する場合には，Windowsサーバの基本機能であるターミナルサービスだけを使用する方法とSBCツールを併用する方法がある。

この二つの方法にどのような差異があるかについて以

下で説明する。

まず，ターミナルサービスは『サーバ上でSBCを実現するための基本的な環境を提供する機能』ということができる。

一方，MetaFrameなどのSBCツールは『ターミナルサービスの環境を更に使い易くする便利機能を提供するミドルウェア』[2] ということができる。

そこで，SBCツールによって提供される代表的な便利機能を列挙すると；

●アプリケーション分離環境；

マルチユーザ使用に未対応のアプリケーションが動作できる環境を提供する（最新のCitrix Presentation Server機能で提供する）

●ロードバランス機能，サーバ負荷管理機能；

サーバを複数台併用する場合，クライアントを負荷の軽いサーバに自動的に接続する（ただし，ターミナルサービスでもセッション数ベースでの負荷管理機能は提供される）

●インストレーション管理機能；

ターミナルサービスを実行するサーバファーム（複数サーバ群）の拡張を容易に行うことができる（APインストール，サーバ設定などに関して）

●クライアントに対するポリシー設定をさらにきめ細かく行うことができる

●イメージアクセラレーション；

動画パフォーマンス向上させる（Windows Media Player®*3)，RealOne Player®*4)，Macromedia Flash®*5) などに対し有効）

●プリンタドライバ管理；

プリンタドライバの設定を細かくかつ簡便に行うことができる

●セキュリティ管理・ネットワーク管理に関する能を拡充し，より柔軟な管理を可能とする

などが挙げられる。

ターミナルサービスだけの使用とするか，SBCツールを併用するかの判断基準は，ターミナルサービスが提供する機能以外に，SBCツールで提供される上述の機能がどこまで必要かということに尽きるが，これはシステム管理のコスト軽減と初期コスト・ランニングコストの軽減とのトレードオフによって決めることになる。

シンクライアントに要求される機能要件とは

シンクライアントの機能要件は何か？

シンクライアントの『あるべき姿』から言えば，一般的なOSすら持たず，あるいは最小限のOS機能だけを持ち，画面とキーボード・マウスの制御だけを行う機能を提供すればよいということができる。

しかし，実際にはサーバ側との通信プロトコルをサポートするためにOSとしてWindows XPe®*3)，Windows CE®*3)，Linux*6) などを搭載し， RDP・ICAクライアント，インターネットブラウザを実装する方法が現実的である。

また，セキュリティ端末という観点から，USBデバイス（USBトークン）やICカードによる認証機能が要求される場合も多い。

実際にシンクライアントに要求される機能要件を列挙すると；

① セキュリティ確保のため，OS機能は最小限
② 必要なSBCクライアントを搭載すること
③ 電源投入後の迅速な立ち上がり
④ 小型，省電力，ファンレス
⑤ 認証（ネットワーク認証，個人認証）のためのUSBトークンやICカードなどに対応
⑥ 端末の設定，設定変更，交換などが容易

などである。

これらの要件を満足するシンクライアント端末の一例を**表1**に示す。

端末に関する要件①～④は端末側の仕様により満足される。⑤の認証への対応については，端末側でトークン/カードに対応していることと，サーバ側での認証機能対応の双方が必要となる。⑥の端末管理のための機能は，端末に適用される『保守・管理ツール』の機能次第であるが，表に示したシンクライアントの場合には，これらの要件を満足している。

業務環境からの要件 - アプリケーションの可用性

PCシステムをベースとしたオフィス環境では，業務で共通的に使用されるアプリケーションの他に，特定の業務でのみ使用するアプリケーション，あれば便利というアプリケーションなど，さまざまなアプリケーション・ソフトウェアがPC上にインストールされている。

シンクライアントを導入する場合，現行のアプリケーションを全て使用できるようにしたいと考えるのはもっともであるが，前述の通り一部のアプリケーションはサーバ側のターミナルサービス機能だけでは正常に動作しない場合もある。

シンクライアント導入の目的であるセキュリティ確保と管理の集中化によるTCO削減を実現するためには，ま

*3）Windows Media Player，Windows XPe，Windows CEはMicrosoft Corporationの登録商標です。 *4）RealOne PlayerはRealNetworksの登録商標です。
*5）Macromedia FlashはMacromedia, Inc.の登録商標です。 *6）LinuxはLunus Torvalds氏の米国およびその他の国における登録商標または商標です。

表1　シンクライアント端末の一例 （ネクストネット社 HTC-3110）

ソフトウェア 仕様

ファームウェア	·Microsoft Windows CE 5.0（Windows Based Terminal規格準拠） ·Microsoft Internet Explorer 6.0 （HTML, JavaScript, XML対応）·Media Player9.0 ·RDP 5.5　·Citrix ICA 8.33　·VNCサーバー
サーバOS	·Microsoft Windows 2000/2003 Server ·Microsoft Windows NT Server 4.0, Terminal Server Edition ·Citrix®WinFrame®、MetaFrame®　およびPresentation Server
ユーザインタフェース	·WBTモードまたはWindows デスクトップモードを切り替え可能
管理ソフトウェア	·RxM　管理ソフトウェアによるリモート管理、設定および更新 ·ICA/RDP接続の管理　·ファームウェア更新　·端末のリモート起動(Wake-on-LAN) ·端末の設定(IP情報, ホスト名等) ·レポーティング　·デスクトップ画面のリモートによる画面シャドウィング(VNC)

ハードウェア 仕様

プロセッサ	·VIA 1GHz 低電力CPU
入力·出力、周辺機器サポート	·シリアルポート×1; パラレルポート×1·USB 2.0 ポート×6（前面×2、背面×4） ·キーボード: PS/2　·マウス: PS/2 マウス ·ローカルプリンターにUSB, パラレル, シリアルによる接続，ネットワークプリンター ·VGA ビデオ出力(DB-15)
ネットワーク	·10/100Base-T ファーストイーサ(RJ-45)·USBWi-Fi®アダプタ802.11b（オプション）
内蔵ICカードリーダ	·PC/SC 1.0 準拠·適合カード　ISO7816-3　T=0及びT=1
ディスプレイ	·最大解像度、リフレシュレート(Hz)　1280×1024 @ 32bit @ Hyper
オーディオ	·出力: 1/8-インチミニジャック, フル16-ビットステレオ，　48 KHzサンプリングレート ·入力: 1/8-インチ8-ビットミニジャックマイクロフォン
サイズ·重量	·205mm（高さ）×43mm（幅）×210mm（奥行）　出荷重量:　2.5kg
動作環境	·温度　動作時: 0°～40°C　保管時:-10°～60°C　対流冷却, ファンレス設計 ·湿度　20% ～80%　結露なし　動作高度　0～3,050 メータ
電源	·100-240 VAC, 47-63 Hz （世界各国自動対応）
対応規制	·安全　cULus60950　TÜV-GS　EN 60950 ·電波障害　FCC Class B、CCC、C-Tick、CE、BSMI、VCCI、MIC
保証期間	·3年保証

ず，不要なアプリケーションを排除し，必要なアプリケーションだけを選定することが肝要である。それがクリアされた後に初めて，コストメリットの大きいシンクライアントシステムを構築することができるといえる。

業務環境を混乱させないという視点から，シンクライアントシステムを導入する際の要件はただひとつである。すなわち，『業務に必要なアプリケーションは従来どおり支障なく使用できること』であり，換言すればアプリケーションの種別に関係なく，従来の業務システム（C/Sシステム，Webアプリケーション，グループウェアなど）が使用できることである。

通常，Windows OS内蔵のPC上で動作するアプリケーションはサーバ上でも動作可能であることから，『画面転送型』のターミナルサービス機能を使用すれば最小限の要求条件は満足することができるといえる。

しかし，前述のように一部マルチユーザ環境に対応していないアプリケーションを従来通り使用するためには，SBCツールの利用，ブレードPC型あるいは仮想PC型システムの適用を検討する必要がある。

また，サーバ管理をより簡便・柔軟にするためにはSBCツールの併用を検討するべきであるが，この場合にも『コストに対する効果』の多寡を判断する必要がある。

ま と め

シンクライアントシステムを導入し，そのメリットを充分に享受するためには，業務に適したシステムの導入が必要である。本稿では，シンクライアントシステムのメリットと，導入するシステム構成の特徴を，端末とサーバ側システムの双方から紹介した。

最小限のシンクライアント導入要件を前提とすれば，『画面転送型』の基本的な構成と最小機能のシンクライアントを適用することがコスト的にも得策であると考えられる。

読者諸氏が実際にシンクライアントを導入するにあたって，個々の導入要件により『画面転送型』，『ブレードPC型』，『仮想PC型』，『ネットワークブート型』などの構成のいずれを選択すべきか，SBCツールは併用すべきか，またシンクライアント端末にはどのような種類を選定すべきかを考える上で，本稿の解説が多少とも参考になれば，幸甚である。 ◆◆

■参考文献

1）『次世代クライアント実力比較』，日経コンピュータ，2005.6.13号，2005年
2）『Citrix Access Suiteガイド』，シトリックスシステムズ・ジャパン（株），2005年

●筆者紹介

尾関隆章：Takaaki Ozeki. 沖コンサルティングソリューションズ株式会社