高セキュリティなシンクライアントソリューション“TZCS”の差異化技術

Differentiation Technologies for "TZCS" Thin Client Solution with High Security

松岡　義雄　■MATSUOKA Yoshio
和田　光悦　■WADA Koetsu
松田　恭平　■MATSUDA Kyohei

近年，高速無線ネットワークが社会インフラとして定着し，小型のデジタル端末でSNS（Social Networking Service）などのサーバとつながったサービスを，誰もが安価でかつほぼ無意識に享受できるようになった。端末にはデータを置かず，サーバ上で仮想マシンを動作させるシンクライアント製品は，これまでオペレーター用端末や非常に高いセキュリティが必要な特殊用途で使われていたが，基本ソフトウェア（OS）更新に伴うPC（パソコン）買替え需要や，スマートフォンなどの普及による業務形態の変化，機密情報漏えい問題の頻発などにより，企業が導入するセキュアなIT（情報技術）システムの有力な選択肢としてニーズが高まっている。

東芝は，B2B（Business to Business）向けノートPCと同等なモビリティや堅牢（けんろう）性とともに高セキュリティを求める顧客向けに，デスクトップ仮想化（VDI）に対応したシンクライアントソリューション“TZCS”を商品化した。TZCSは，独自のBIOS（Basic Input/Output System）・OS技術の融合によりストレージをいっさい持たない端末で利用でき，独自の端末管理サーバ技術との組合せにより遠隔から瞬時かつ完全なデータ消去と各種設定値の保護が可能なソリューションである。

With the widespread dissemination of high-speed wireless networks as a social infrastructure system in recent years, small digital devices are providing users with various services effortlessly and at low cost via the network through connections to social networking service (SNS) servers. Thin client products, which can remotely display desktop images transferred from a virtual machine via the network without storing the actual data files, have mainly been used as operator terminals and for specialized applications requiring high security. From the viewpoint of security, attention is being focused on thin client products as a potential candidate for the next information technology (IT) infrastructure for enterprise use due to the replacement demand for PCs caused by the expiration of support for operating system (OS) software, changes in business configuration as a result of the broad diffusion of mobile devices with high functionality, and frequent occurrences of information leakage.

Toshiba has developed the "TZCS" thin client solution for virtual desktop infrastructure (VDI), which ensures high security for users while providing high mobility and robustness comparable to its notebook PCs for the business-to-business (B2B) market. Taking advantage of the integration of our proprietary basic input/output system (BIOS) and OS technologies, the TZCS can be used without any storage devices and offers a quick remote data deletion function as well as protection functions for a variety of setting values by applying terminal management technology.

1　まえがき

東芝のB2B向けノートPCは，約30年の歴史を持つ独自BIOSを搭載し，高速起動や様々なB2B向けセキュリティ機能を特長としている。また当社は，“東芝スマートクライアントマネージャー（TSCM）”という端末管理ソフトウェアを商品化しており，セキュリティパッチの効率的配布や，サーバと有線LANで認証できなければBIOSが電源を切断するセキュリティ機能（起動認証）を提供している。

更に当社は，これらの技術を基に2013年にBIOSの無線LANサポート実験プロジェクトを立ち上げ，試行錯誤を重ねて技術試作品を2014年に完成させ，BIOSが無線アクセスポイントを介してIP（Internet Protocol）ネットワークに接続しサーバと通信できるようにした。無線LANをサポートするBIOS技術の特長を生かし，高セキュリティを求める企業関係者のニーズに応えて，VDI対応シンクライアントソリューション TZCSを商品化した。TZCSは，モバイル仕様でありながら確実に情報保護の実現が可能な企業向けソリューションである。

ここでは，TZCSのシステム構成と，高セキュリティを実現するうえで差異化技術となる独自のBIOS・OS技術，及びサーバによる管理機能について述べる。

2　システム構成

TZCSは専用のBIOS及びOSを使用することで，ハードディスクドライブ（HDD）やソリッドステートドライブ（SSD）などのストレージをいっさい持たないVDI用シンクライアント端末“TZCSクライアント”と，サーバ管理機能ソフトウェアから構成される。TZCSクライアントは，起動後はRAM上で動作することから，電源オフ時には端末にデータが残らず，盗難や紛

失時にも機密情報が漏れることがないため，安全である。またサーバ側の管理機能と組み合わせることで，様々なVDI環境や機能に柔軟に対応できる。

ここでは，TZCSのソフトウェア構成と動作概要について述べる。

2.1 ソフトウェア構成

TZCSのソフトウェアは，次の三つに分類される。

⑴ BIOS

⑵ OS：Small OS及びBig OS

⑶ 管理用ソフトウェア

TZCSクライアントにはSmall OSを包含したBIOSがあらかじめ組み込まれている点が，一般のPCと大きく異なる。ウィンドウシステムやVDIクライアントソフトウェアを含むBig OSは管理サーバ上に保存され，TZCSクライアントからつどダウンロードされ実行される。管理サーバはBig OS管理の他，起動認証や，ポリシー制御，端末情報制御，ログ収集などTZCSクライアントを管理するための機能を持つ。

2.2 動作概要

TZCSクライアントの電源をオンすると，**図1**に示すように，BIOSがSmall OSを実行してネットワークに接続後，Small OSが管理サーバに接続し個体識別情報を元に認証される(①)。次に，管理サーバにあらかじめ保存されたBig OSのダウンロードを要求する(②)。Big OSのダウンロード完了後(③)，TZCSクライアントはBig OSへ制御を切り替え，VDIクライアントソフトウェアを実行し，顧客のVDI環境へ接続する(④)。起動からVDI環境への接続後の仮想デスクトップ表示まで全てRAM上だけで動作するため，電源をオフすればストレージにデータが残るようなことはなく非常に安全である。

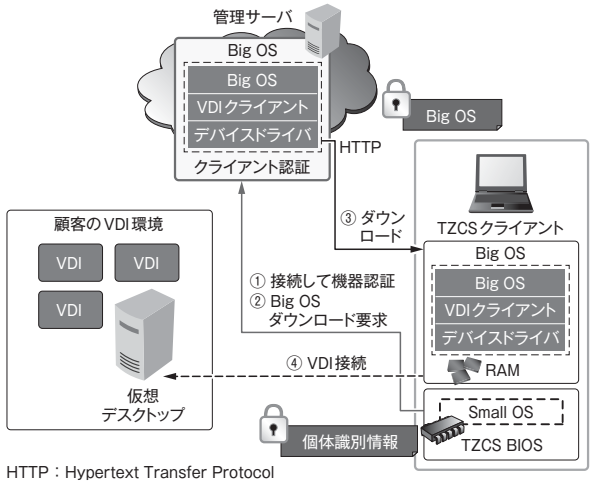

図1．TZCSの動作概要 ― TZCSクライアントの電源オンからVDI接続までの，BIOS，OS，及び管理サーバの動作を示し，全ての作業はRAM上で行われるため電源をオフすれば端末にデータはいっさい残らない。

Summary of TZCS operation sequence

3 高セキュリティを実現するTZCSの差異化技術

3.1 TZCS専用BIOS

一般的なノートPCのBIOSは，OSを起動するためのファームウェアとして，CPU，チップセット，及び各種入出力デバイスの初期化機能や，ハードウェア状態の情報取得，設定変更，及び設定保存のための機能，パスワード認証や改ざん検知などのセキュリティ処理機能，高速起動やスタンバイ復帰処理のための機能，DOS（Disk Operating System）から最新OSまでのソフトウェアとハードウェアとのインタフェース機能，ビデオ初期化や有線LANブートのためのオプションROMの起動機能など，様々な役割を持つ。

BIOSはBIOS ROMと呼ばれる小容量のフラッシュメモリに保存されるため，容量的な制約（4～6Mバイト）を受ける。また，無線LANなどの特定デバイスのドライバソフトウェアはデバイスベンダーから提供されないため，それらのデバイスを利用した機能をユーザーに提供できないという制約もあった。

そこで，次に示す二つの対策を実施した結果，BIOS，TZCSのOS，及び無線LANドライバを4MバイトのBIOS ROM容量に収めることに成功した。

⑴ BIOSの徹底した小型化　数万ファイルに及ぶ全ソースコードの中から，TZCSでは不要なコードやデータを削除した。特に，一般のOSや過去のDOSに対するサポートの削除，設定画面の簡素化，及びサポートデバイスの集中と選択によるオプションROMの削減を実施し小型化した。

⑵ 極小OSの内蔵と無線LANドライバの起動　無線LANドライバは自社製作できないことから，ベンダー提供の既存のオープンソースOSを選択し，その中でも当社がコード管理するエンベデッドOSを活用することで，更なる小型化を図った。

更に，BIOSのセキュリティ部分の強化を実施した。TZCSではBig OSをダウンロードして起動するが，それに先立ち，そのネットワーク接続先URL（Uniform Resource Locator）やダウンロードプロトコルなどの情報をTZCSクライアント側に保存しておく必要がある。例えば無線LANでサーバと接続する場合には，無線アクセスポイントのSSID（Service Set Identifier）などの情報をTZCSクライアントに設定しておく必要がある。一般のシンクライアントでは，HDDなどのストレージ上にこの設定値が保管されている。TZCSでは設定値の保存を安全に行うために，従来のBIOSパスワードの保管技術を応用して，BIOS管理下の不揮発メモリに保管することで高い安全性を確保している。

このように，実行コードや設定値がOSから変更できないROM上にあることでセキュリティ性が高い製品となっている。またBIOSがOSの一部の機能を取り込めるため，将来的に新しいシステムやソリューションを構築することが可能になる。

一般論文

3.2 TZCS専用OS

TZCSのOSは，当社がソースを管理するエンベデッドOSをベースとし，TZCSに必要な機能を追加した専用品である。一つのOSモジュールとしてBIOS ROMに格納できればシンプルな設計となるが，BIOS ROMの容量的な制約から，前述したように動作及びファイル構成がSmall OSとBig OSの二つに分かれた構造とした。

3.2.1 Small OS　主な動作は，OS起動，ネットワーク接続，起動認証，及びBig OSのダウンロードである。Small OSのファイル構成は，OSカーネル部の起動と，ネットワーク接続に最低限必要なファイル類から成る。

(1) ネットワーク接続　TZCSクライアントを起動させると，Small OSは最初にネットワークへの接続を行う。Small OSにはハードウェアに搭載されている有線／無線LANデバイスを動作させるためのドライバが含まれており，まずそれらをロードし実行する。次に有線／無線LANがそれぞれ使用可能かどうかを確認する。TZCSクライアントに有線LANケーブルが接続されている場合はそれを使用し，そうでない場合は無線LANを使用する。

(2) 起動認証　TZCSクライアントは，TZCSシステムとして起動してよいかどうかを判別するため，起動認証を行う。その詳細は3.3節の管理機能で述べる。

(3) Big OSのダウンロード　TZCSクライアントは管理サーバからBig OSをダウンロードする。Big OSにはVDIクライアントソフトウェア及びそれらを動作させるために必要なライブラリファイルやドライバ類が含まれ，暗号化されている。Big OSはBIOS ROMの容量的な制約からサーバ側に置かれているが，この構造により一括アップデートを簡単にできるとともに，顧客ごとのソフトウェアカスタマイズも比較的容易になる。

Big OSをダウンロードして起動するため，ネットワーク速度が遅い場合は起動時間が長くなる。そこで，TZCSクライアントにSDメモリカードを装着しておけば，ダウンロードしたBig OSを機器固有の鍵で暗号化してカードに保存し，次回起動時はそのカードからBig OSを読み込んで起動する高速起動オプションも用意した。

(4) Big OSへの制御切替え　Big OSのダウンロードが完了すると，それを復号してRAMへ展開した後，これまでTZCSクライアントを制御していたSmall OSからBig OSへ制御を切り替える。Small OSの設定を引き継ぎながら，Big OSに含まれるドライバやライブラリを実行して制御を切り替えるようにした。

3.2.2 Big OS　主な動作は，VDI接続，端末の主要デバイスサポート，及びインジケータ機能である。

(1) VDI接続　Big OSへ制御が切り替わった後，ウィンドウシステムを有効にし，VDIクライアントソフトウェアを起動する。TZCSシステムではVDIクライアントとしてCitrix社のXenDesktop®とVMware社のVMware® Horizon™をサポートしており，顧客のVDI環境に応じた柔軟な対応が可能である。

(2) 端末の主要デバイスサポート　Big OSは，TZCSクライアントのモニタやサウンドなど種々のデバイスをサポートするドライバを含み，実行できる。なかでもタッチパッドは，誤動作防止のためのオン／オフ機能やパームリジェクション機能により，当社のB2Bノート PCと同等の使いやすさを実現した。

(3) インジケータ機能　TZCSシステムでは，インジケータと呼ばれるTZCSクライアントの設定変更を行うためのGUI（グラフィカルユーザーインタフェース）を持つ（**図2**）。画面の輝度変更や複数モニタの設定変更を行う。またバッテリー残量や無線強度の確認もできる。一般のシンクライアントでは仮想デスクトップを全画面表示すると，その端末のバッテリー残量などが確認できなくなるが，TZCSクライアントではファンクションキーを押すことで容易に視認できるようにした。

図2．インジケータの表示例 — インジケータは，TZCSクライアントの画面輝度などの設定変更やバッテリー残量などの確認を行うためのGUIである。
Example of indicator display

3.3 管理機能

TZCSの管理サーバ側の主な機能を次に述べる。

3.3.1 起動認証　TZCSクライアントの電源をオンすると，Small OSがHTTP（Hypertext Transfer Protocol）プロトコルを使用して管理サーバと通信し，起動認証を行う。起動認証はTZCSクライアントの個体識別情報をユニークなキーとして使用し，その端末が登録されているか，起動が許可されているかを確認する。起動が許可されている場合は，TZCSクライアントのふるまいを設定したポリシーの内容が端末に送信され，設定に従って動作する。

また起動認証は，TZCSクライアントが動作中にも定期的に実行され，動作中に起動非許可に設定されると，仮想デスクトップの接続を切りシャットダウンする。仮にTZCSクライアントを紛失してしまった場合でも，起動を非許可にすることで企業のリソースへのアクセスはいっさいできなくなり，端末上にもデータは保持されていないため，セキュリティを担保できる。シャットダウン時に作業中であったアプリケーションは仮想デスクトップ上で動き続けているため，データの喪失は発生しない。

仮想デスクトップに再接続すれば作業を再開できる。

3.3.2　ポリシー　TZCSクライアントの各接続先（起動認証サーバ，VDIサーバ，及びダウンロードサーバ）のURLと使用するTZCSモジュール（Big OS）の名前，及びTZCSクライアント側の動作設定（通信のリトライ回数と間隔や，起動認証のポーリング間隔，通信切断時のアクションなど）をまとめたものである。ポリシーは，管理者がWebユーザーインタフェース（UI）と呼ぶ管理コンソール（**図3**）で設定し，各TZCSクライアントには必ず一つのポリシーが設定されている。管理者は，ポリシーの設定を変えることで，使用するTZCSソフトウェアの更新や，TZCSクライアントの挙動を設定したり調整したりできる。管理コンソールには，ユーザー名とパスワードによるユーザー認証を得てログインする必要がある。

3.3.3　端末情報　機器登録時に指定した個体識別情報の他，TZCSクライアントの型番，シリアル番号，CPU名，メモリ容量，BIOSバージョン，TZCSモジュールのバージョン，最後のアクセス日時などがTZCSクライアントから管理サーバに送られてくる。管理者は管理コンソール上でこれらの情報を確認でき，例えば，最後のアクセス日時を使って，しばらく使用していない端末の廃棄や，期末の棚卸しで端末の存在確認を行うといった使い方も可能である。

3.3.4　ログ　管理コンソールでは，管理サーバのログを確認できる。ログには，TZCSクライアントの登録／削除，起動認証の実施結果，アカウントの登録／削除，管理コンソールへのログイン／ログアウト，及び管理コンソールでの操作（アカウント名と操作内容）が記録される。ログには情報，エラー，及び警告という三つの種類があり，成功した通常処理は情報，失敗した通常処理はエラーとなる。一方，TZCSクライアントやポリシーの削除，認証拒否，及び未登録端末からの接続要求など，セキュリティリスクとなりうる事象は警告となる。

図3．管理コンソールの表示例 ― 管理コンソールは，TZCSクライアントの各種設定や情報をWeb UIでリモート表示できる管理用ソフトウェアである。

Example of management console display

警告のログが出力された場合，管理者は内容を確認して問題があれば必要な対応を行う。

4　あとがき

当社独自のBIOS・OS技術の融合により，高セキュリティを求める顧客ニーズに応えるVDI対応シンクライアントソリューション TZCSを商品化した。

一般のシンクライアント製品はWindows(†) Embeddedベースで設計されているものが多く，また安価なHTML 5（Hypertext Markup Language 5）対応の端末も競合製品として存在する。それらは周辺機器のサポートや設定のしやすさなどの使い勝手では優っている点もある。また，オープンソースOSによる開発ではプログラムの小型化やデバイスドライバに問題が生じた場合の解決の難易度が高くなることが多い。当社は，これらの課題を克服することで，外出時に持ち出せる高セキュリティのモバイルシンクライアントとして，今後もTZCSの機能の充実を図っていく。

- XenDesktopは，Citrix Systems, Inc. 及びその子会社の商標であり，米国特許商標局及び他国で登録されている場合がある。
- Windowsは，米国Microsoft Corporationの米国及びその他の国における登録商標又は商標。

松岡　義雄　MATSUOKA Yoshio
パーソナル＆クライアントソリューション社 ビジネスソリューション事業部 設計第四部参事。TZCSソフトウェアの設計・開発に従事。
Business Solutions Div.

和田　光悦　WADA Koetsu
パーソナル＆クライアントソリューション社 ビジネスソリューション事業部 設計第四部主務。B2Bソリューション及びTZCSソフトウェアの設計・開発に従事。
Business Solutions Div.

松田　恭平　MATSUDA Kyohei
パーソナル＆クライアントソリューション社 ビジネスソリューション事業部 設計第四部主務。TZCSソフトウェアの設計・開発に従事。
Business Solutions Div.