PCクライアントのセキュアな環境を実現するFlexClient™

FlexClient™ Enabling Secure Environment for Client PCs

内野　雅司　　舟城　亮一　　遠藤　隆久
■ UCHINO Masashi　■ FUNAKI Ryoichi　■ ENDO Takahisa

近年，パソコン（PC）は，ビジネスをはじめ様々な領域で活用されている。その一方で，PCの資産やそこで処理・蓄積される情報の管理は，セキュリティの観点からより重要になっており，安全なクライアントシステムの構築が求められている。

東芝ソリューション（株）は，この要求に応えるため，オフィスのLAN環境では“ネットワークブート機能とiSCSI（internet Small Computer System Interface）ストレージ”により，PCのローカルディスクに情報を蓄積しない環境を実現し，かつモバイルなどのLANがない環境では“PCのローカルディスクをセキュアに利用できる機能”を組み合わせた，新しいタイプのシステムを開発した。当社では，このシステムを適用して，ISMS（Information Security Management System）などのセキュリティの実践で大きな成果を挙げている。

With the remarkable progress of their performance and functionality, PCs are now used in various situations including the business world. However, there are numerous security risks in terms of managing the hardware, software, and data on PCs. Thin client systems for mobile computing have a limitation in that the mobility of the client devices degrades performance and functionality. There is a need to create a safe client environment without compromising the capabilities of the PCs.

Toshiba Solutions Corporation has developed FlexClient™, a new client security system that makes best use of standard PCs in and out of the office. When the PCs are connected to a LAN in the office, FlexClient™ makes them boot from the network using a centralized, Internet Small Computer System Interface (iSCSI)-based storage and prevents the PCs from storing data on the internal disk drive. When the PCs are offline in a mobile environment, it provides a secure way of using the internal disk drive. Data on the disk are managed from the server. We have deployed FlexClient™ in our systems, allowing us to manage security risks in an Information Security Management System (ISMS)-compliant business environment.

1　まえがき

企業活動において，セキュリティ対策はますます重要になっている。PCは，企業の情報システムのクライアントとして幅広く利用されている反面，紛失や盗難，不正使用，ウィルスなどのセキュリティ脅威の対象となり，対策が必須の状況である。市場では，一般にシンクライアントと呼ばれるシステムがセキュリティ対策として注目されているが，既存のシステム環境との親和性や拡張性，管理面，投資コストなどで課題が多い。

東芝ソリューション（株）は，これらの課題を解決し，PCを安全で効率的に活用できるシステムFlexClient™を開発した。ここでは，FlexClient™の方式，動作，及び活用例を述べる。

2　シンクライアント方式

一般にシンクライアントとは，クライアント側にローカルディスクなどの記憶装置を持たない端末を指し，“端末側にデータを持たない”，“情報やシステム環境をサーバセンター側に集中”などの環境を実現している。実際のシステムは，サーバ，ストレージ，及びネットワークで構成され，主なシンクライアント方式として次の3方式がある。

(1)　サーバ方式　　シンクライアントとして広く知られているもので，アプリケーションをサーバ上で実行し，その画面情報だけを送受信する。

(2)　ブレードPC方式　　PC本体をブレードPCとし，これをサーバセンターのラックなどに集約して収容する。アプリケーションは各ブレードPC上で実行し，その画面情報だけを送受信する。

(3)　ネットワークブート方式　　基本ソフトウェア（OS），データ，アプリケーションを格納したサーバセンター側のストレージをPCのローカルディスクとみなして実行する。OSとアプリケーションはPC上で実行し，データは直接サーバセンター側のストレージと入出力を行う。

しかし，いずれの方式も，実際のシステム構築や運用においては次のような課題がある。

(1)　サーバ方式は，アプリケーションをサーバ上で実行するため，サーバの性能設計やPCアプリケーションのサーバ上への移行などが課題となる。また，サーバ購入や専用端末へのリプレースなどの投資も必要である。

(2)　ブレードPC方式は，従来のPCをブレードPCに置き換えるため，新規ブレードPCの購入費やリプレース作業への投資が必要である。

(3) ネットワークブート方式は，サーバセンター側へのストレージの設置と，この装置からのOSやアプリケーションのブートを行うための高帯域LAN環境が必要である。

また，それぞれの方式に共通して，画面送受信やブートのためにネットワークの常時接続が必要になる。

今回開発したFlexClient$_{TM}$は，オフィスのLAN環境ではPCをデータを持たない端末として利用でき，かつモバイル環境では常時ネットワーク接続を必要としないセキュアなPCとして利用できる，という新しい発想から生まれたシステムである。

3 FlexClient$_{TM}$の方式と特長

オフィス環境及びモバイル環境でのFlexClient$_{TM}$の方式と特長を述べる。

3.1 オフィス環境

社内などLANのあるオフィス環境では，FlexClient$_{TM}$はネットワークブート方式で動作する（**図1**）。この方式により，既存のWindows®(注1)環境がそのまま実行でき，既存アプリケーションもPC上で実行できるため，システムの移行は容易となる。

更に，iSCSIストレージ装置を活用することでネットワークへの容易な接続を実現し，各PCのローカルディスクの環境（OS／アプリケーション／データ）をiSCSIストレージ装置に集中することができる。これにより，PCの紛失や盗難に備えるだけでなく，各PCのアプリケーション環境の整備など運用管理を効率化できる。また，iSCSIストレージ装置の機能により，信頼性の向上とデータの一括バックアップなどが可能になる。FlexClient$_{TM}$は，運用管理コスト（TCO）の削減も同時に実現する。

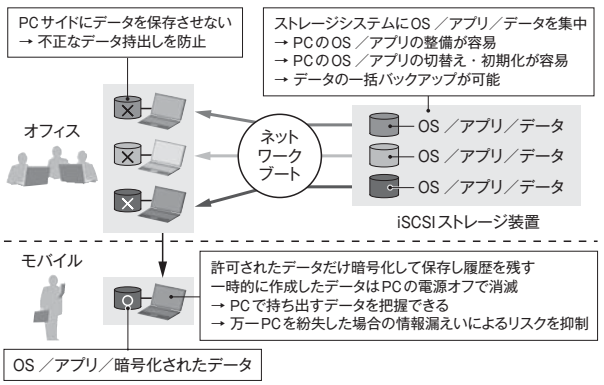


図1. FlexClient$_{TM}$のオフィス環境とモバイル環境 — オフィス環境ではクライアント側にデータを残さないが，モバイル環境では許可されたデータだけを暗号化して保存できる。

FlexClient$_{TM}$ used in office and mobile environments

(注1) Windowsは，米国Microsoft Corporationの米国及びその他の国における登録商標。

ネットワークブート方式での動作時はローカルディスクを使用しないため，このローカルディスク内容を消去し，セキュアなPCとして利用可能なモバイル環境を，このローカルディスクに構築できる。

3.2 モバイル環境

PCをオフィス外に持ち出すなどのモバイル環境では，広帯域ネットワーク環境が常時使用できるとは限らない。

モバイル環境では，FlexClient$_{TM}$は暗号化されたPCのローカルディスクからOSやアプリケーションを起動する（図1）。ローカルディスクは読取り専用として機能するため，モバイルで一時的に作成したデータは電源オフで無効になる。モバイル環境で利用するデータをPCに入れて持ち出したい場合は，“承認者ツール”と“SecureFileManager”を使って管理者が持出しを許可した情報に限り，管理サーバに履歴を残したうえで，ローカルディスクの特殊な領域に保存できる。

これらの仕組みにより，セキュアなモバイル環境を提供する。

4 FlexClient$_{TM}$のシステム構成

FlexClient$_{TM}$のシステム構成を**図2**に示す。

FlexClient$_{TM}$は，既存システムにFlexClient$_{TM}$用iSCSIストレージ装置を追加し，PCのローカルディスクの環境をiSCSIストレージ装置上に構築することで，システム移行が実現できる。このため，他のシンクライアント方式のように，性能に絡んだサーバ拡張や，専用クライアントへの置換え，システム再設計，アプリケーションの動作評価などを行うことなく，容易に移行が可能となる。

システム構成の概要を以下に述べる。

(1) FlexClient$_{TM}$用iSCSIストレージ装置は，iSCSIプロトコルに対応し，IP（Internet Protocol）ネットワークとGigabit Ethernetで接続する。コントローラ部（ネット

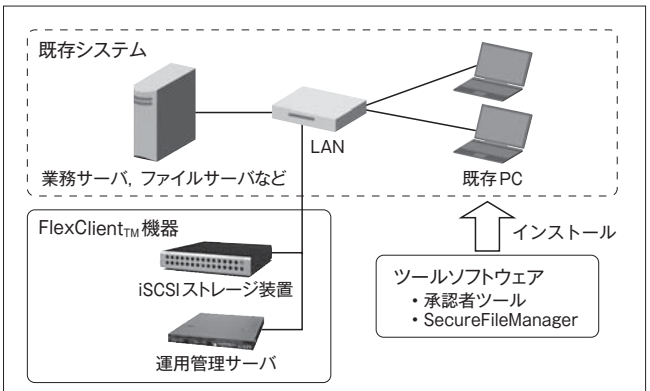


図2. FlexClient$_{TM}$のシステム構成 — FlexClient$_{TM}$は，既存システムにiSCSIストレージ装置と運用管理サーバを追加して構築できる。

Configuration of FlexClient$_{TM}$

一般論文

ワークインタフェース含む）と電源部は二重化しており，また，格納するハードディスクに対しては，RAID（Redundant Array of Independent（Inexpensive） Disks）5と冗長構成で高い信頼性を実現している。

（2） 運用管理サーバは，ネットワークブート時にブートに必要なファイルをPCにTFTP（Trivial File Transfer Protocol：ユーザー名やパスワード検証を必要としないファイル転送プロトコル）で転送する。また，モバイル運用時には，持出し情報の履歴管理などを行う。

（3） PCは，Windows®XP（SP2）を搭載しているPCが活用できる。ただし，FlexClient™では，データをメモリ上に一時的な格納を行うため，十分なメモリ容量（768 Mバイト以上を推奨）が必要である。

（4） 承認者ツールは，部門内などの承認権限者が使用するツールで，ファイル持出し（PCのローカルディスクへ格納）を許可する証明書を生成する。

（5） SecureFileManagerは，持出し申請者が使用するツールで，（4）で生成された証明書に基づいて許可された持出しデータを暗号化し，ローカルディスクの特別な領域に独自ファイルシステムにより格納する。同時に，持出し履歴と持ち出したファイルのコピーを運用管理サーバに記録する。

5 FlexClient™の動作概要

オフィス環境とモバイル環境時のFlexClient™の動作について述べる。

5.1 オフィス環境での動作

FlexClient™は，オフィス環境で次のように動作する（**図3**）。

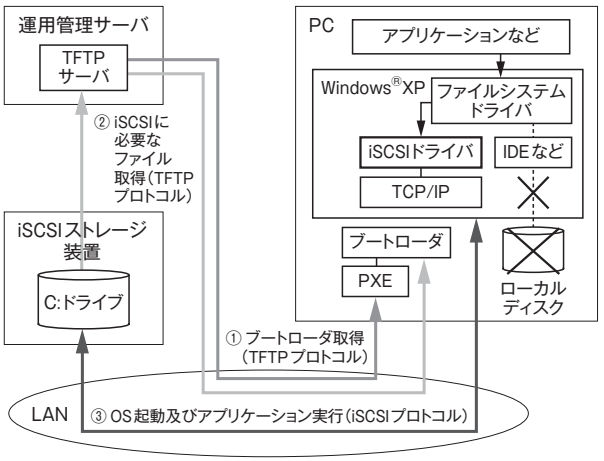
（1） ブートローダ取得　　PCは，電源が投入されるとPXE（Preboot eXecution Environment）(注2)によりOSが起動し，運用管理サーバからネットワークブート用のブートローダをTFTPで取得して実行する。

（2） iSCSIに必要なファイル取得　　ブートローダは，iSCSIドライバの起動に必要なファイルを運用管理サーバ経由でiSCSIストレージ装置から取得する。

（3） OS起動及びアプリケーション実行　　OSの起動が開始し，iSCSIドライバが有効になった後，iSCSIストレージ装置とiSCSIで直接データのやり取りを行う。iSCSIストレージ装置内のドライブがPCのC:ドライブとして機能する。

この動作フローでOSが起動した後，アプリケーションからのデータ書込みと読込みは，すべてLANを介してiSCSIストレージ装置内のドライブに対して行われるため，PC側にデータを残さない。更に，PCのUSB（Universal Serial Bus）ポートや内蔵フロッピーディスクなどへのデータ書込み制限もできるため，不正なデータ持出しを抑制できる。

（注2） Intel社が作成したネットワークブートの規格で，サーバ及びクライアントが従うべきプロトコルなどが規定されている。



IDE　：Integrated Drive Electronics
TCP/IP　：Transmission Control Protocol/Internet Protocol

図3. オフィス環境時の動作フロー ― PCは電源投入後，運用管理サーバと連携する。OSが起動すると，アプリケーションはiSCSIストレージ装置と直接データをやり取りするため，ローカルディスクにはデータを残さない。

Sequence of FlexClient™ in office environment

5.2 モバイル環境での動作

モバイル時は，ローカルディスクに格納されたOSやアプリケーションを実行する。ただし，ローカルディスクに情報を残さないように，ローカルディスクへのWindows® API（Application Programming Interface）による書込みにFlexClient™が介入し，データはメモリ上のバッファ領域へ書き込まれ，ローカルディスクには書き込みが行われない。これにより，PCのシャットダウンや電源断を行うとメモリ上のデータはすべて消え，ローカルディスクにはデータが残らない環境となる。

また，オフィス環境から情報を持ち出す場合には，次のことが重要である。

（1） 許可された情報だけを持ち出す

（2） 許可された人だけが利用できる

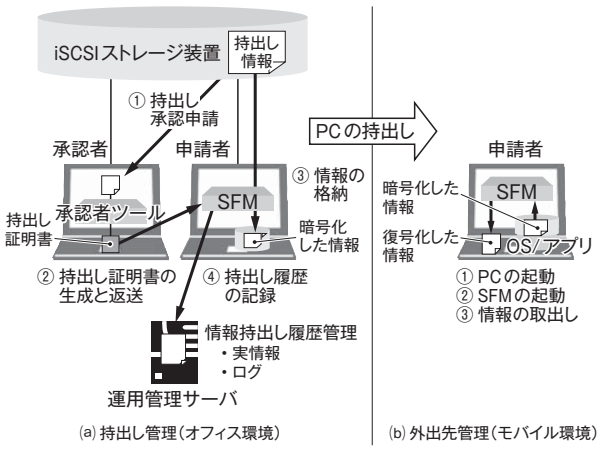
（3） 何が持ち出されたか記録に残す

FlexClient™は，安全な情報の持出しと万一の紛失などに対する事後対策を可能にする機能として，以下に述べる持出し管理と外出先管理のプロセスを提供している（**図4**）。

5.2.1 持出し管理　　安全な情報の持出しのために，次のようなプロセスを提供する。

（1） 持出し承認申請　　情報を持ち出す場合，申請者は承認権限者に持ち出したい情報をメールなどで送付する。

（2） 持出し証明書の生成と申請者への返送　　承認権限者は，その情報の持出しを許可する場合に承認者ツールを使用して，持出し証明書を生成し，申請者に返送する。



SFM：SecureFileManager

図4. モバイル使用のための管理プロセス ― 情報を安全に持ち出すため，持出し承認や情報の暗号化，履歴の管理を行う。

Management process in mobile environment

(3) 情報の格納　　申請者は，この持出し証明書とSecureFileManagerを使って，持出し情報を暗号化し，ローカルディスクに格納する。

(4) 履歴の記録　　SecureFileManagerは，情報の格納と同時に，この情報と持出し履歴を運用管理サーバに残す。

この操作を，オフィスなどのネットワークブート環境で動作しているときに行うことで，ローカルディスク内に持ち出したい情報を格納できる。この格納領域は，SecureFileManagerだけが認識できる独自ファイルシステム領域を利用し，情報の暗号化も同時に行っている。このため，万一ローカルディスクを取り出して別のPCなどに実装して読出しを試みても，読出しが困難な仕組みとなっている。

5.2.2 外出先管理　　外出先などのモバイル環境では，次の操作により，ローカルディスクに格納した情報を取り出して利用することができる。

(1) PCの起動　　PCのローカルディスクからPCを起動する。

(2) SecureFileManagerの起動　　ID (IDentification) 及びパスワードで認証を行い，SecureFileManagerを起動する。

(3) 情報の取出し　　SecureFileManagerは，格納された情報を復号化して取り出す。

また，SecureFileManagerでは，格納した情報の保存期間を設定することができる。設定期間を経過後に暗号化キーを消去することにより，情報の解読が困難になる。

6 FlexClient$_{TM}$の活用例

FlexClient$_{TM}$は，次のような用途での活用を想定している。

(1) PCクライアントにデータを持たせない用途　　オフィスのLAN環境で，PCのローカルディスクにデータを持たせず運用できるため，総務・人事部門などの重要な情報を扱う部門で活用できる。

(2) PCの紛失・盗難時のリスクを低減したい用途　　モバイル環境で，営業部門が顧客へのプレゼンテーションなどに活用できる。また，ネットワークの利用で，ローカルディスクに情報を残さないメールやWebブラウジング用端末としても活用できる。万一，PCを紛失した場合でも紛失した情報を特定でき，リスクを抑制することができる。

(3) PC環境を効率的に整備したい用途　　コールセンターや窓口業務，学校の教室などで複数のPC環境を効率的に整備できる。これは，iSCSIストレージ装置内でPC環境をコピーすることで複数のPC環境の整備が簡単にでき，また，ブートする環境を切り替えることで，PCは複数の環境を利用することができる。

これらは活用例の一端であり，PCを使う情報システムの様々なシーンで応用できる。当社でも，ISMSなどのセキュリティを実現するうえで成果を上げている。

7 あとがき

FlexClient$_{TM}$は，当社が培ってきたセキュリティ技術やストレージ技術，プラットフォーム技術などを活用し，みずからISMSなどのセキュリティを実践するなかで開発し，商品化したものである。FlexClient$_{TM}$が，PCからの情報漏えいリスクの抑制や管理コスト低減に効果的なソリューションとして多くのユーザーに活用され，セキュリティ環境の実現に貢献することを期待している。

内野　雅司　UCHINO Masashi
東芝ソリューション（株）プラットフォームソリューション事業部
プラットフォームソリューション第三部主査。
ネットワークとセキュリティのシステム開発に従事。
Toshiba Solutions Corp.

舟城　亮一　FUNAKI Ryoichi
東芝ソリューション（株）プラットフォームソリューション事業部
商品企画部。
FlexClient$_{TM}$の商品化に従事。
Toshiba Solutions Corp.

遠藤　隆久　ENDO Takahisa
東芝ソリューション（株）プラットフォームソリューション事業部
ハードウェア開発第二部。
FlexClient$_{TM}$製品とストレージ製品の開発に従事。
Toshiba Solutions Corp.