中小規模企業向けPC統合セキュリティシステム PC運用上手TM

“PC Unyo Jozu” Integrated Security Appliance

渡壁　健　■ WATAKABE Takeshi
藤原　勇治　■ FUJIWARA Yuji
山下　卓規　■ YAMASHITA Takumi

企業活動において，パソコン（PC）のセキュリティ対策がますます重要になっており，一般に，セキュリティ製品の導入には，セキュリティポリシーを設計するために高度な専門知識を有するIT（情報技術）管理者と導入のための工数が必要となる。

東芝は，情報漏えい対策に必要なセキュリティ機能と，システムやPCの運用管理に必要な様々な管理機能を備えた中小規模の企業向けPC統合セキュリティシステム　PC運用上手TMを開発した。PC運用上手TMは，詳細なセキュリティポリシーの設計や設定を不要にし，専任のIT管理者がいなくても，導入とその後の運用を効率的に行うことができる。

Security countermeasures for PCs have become an increasingly important issue in corporate activities in recent years.　Toshiba has developed the “PC Unyo Jozu” integrated security appliance, which provides security functions required for information leakage protection as well as various controlling functions required for system operation and PC management.

In the introduction of a security solution, generally an information technology（IT）administrator with expertise and experience as well as development expenditures for introduction of the system are essential in order to design its security policies.　“PC Unyo Jozu” facilitates the simple design and setup of security policies, and both the introduction and operation of the system can be performed efficiently even if there is no full-time IT administrator.

1　まえがき

企業活動において，パソコン（PC）は，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一方で，紛失や盗難，不正使用，及びウイルス感染などのセキュリティリスクの対象となりやすい。また，社会的にも個人情報保護法やJ-SOX法(注1)の施行があり，PCのセキュリティ対策の重要性はますます高まっている。個人情報漏えいによる損害賠償の可能性や企業イメージダウンは，企業の存続さえも危うくしかねない。また，企業の情報を守る観点では，情報漏えいだけでなく，ウイルスや災害などによる情報喪失も課題である。このようなセキュリティリスクは企業の規模や業種に関係なく存在し，どんな企業であってもセキュリティ対策が必須の状況である。

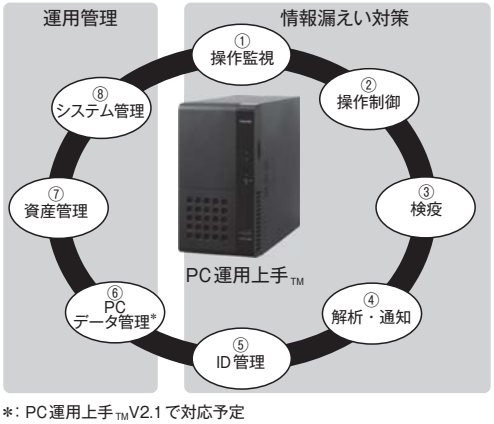
一方で，専門の部署や専任のIT管理者を持つ大規模企業に対し，中小規模の多くの企業では専任のIT管理者を置くことは困難である。

東芝は，これらの課題を解決し，PCを安全に活用するためのPC統合セキュリティシステム　PC運用上手TMを開発し，商品化した。ここでは，PC運用上手TMの八つの機能と，それを支えるセキュリティ技術について述べる。

（注1）　企業の内部統制強化を目的とした金融商品取引法の一部規定のこと。
（注2），（注3），（注4），（注5），（注6）　Windows Server, Active Directory, Microsoft, Outlook, Windowsは，米国Microsoft corporationの米国及びその他の国における登録商標。

2　PC運用上手TMの概要

PC運用上手TMは，従業員30～500人の中小規模の企業を対象としたPC統合セキュリティシステムである。OS（基本ソフトウエア）のWindows Server®(注2)2003をベースに，情報漏えい対策と運用管理を実現する次の八つの機能を持つ（**図1**）。



*：PC運用上手TMV2.1で対応予定

図1．PC統合セキュリティシステム　PC運用上手TM ― 情報漏えい対策とPC管理をオールインワンで提供する。
“PC Unyo Jozu” integrated security appliance

(1) ユーザー操作を監視し記録する操作監視機能
(2) Web閲覧などを制限する操作制御機能
(3) PCのセキュリティ状態をチェックする検疫機能
(4) ログの閲覧や保存をする解析・通知機能
(5) Active Directory®(注3)によるユーザーID（Identification）管理を容易にするためのID管理機能
(6) クライアントPCのデータをバックアップするPCデータ管理機能
(7) PCやほかの機器を管理する資産管理機能
(8) ポリシー設定などを行うシステム管理機能

PC運用上手TMのシステム構成は，エージェントと呼ぶソフトウェアをインストールしたクライアントPCと，PC運用上手TMサーバから成る（**図2**）。エージェントは，PC運用上手TMサーバから取得するセキュリティポリシーに従って，ユーザーの操作監視や操作制御を行い，これらの動作をログとして記録する。ログはPC運用上手TMサーバに転送され，サーバ上で一定期間保存される。ログはデジタルフォレンジック技術により保護されており，たとえ管理者であっても，ログを改変すると検出される。

PC運用上手TMサーバのユーザーインタフェースは，Webコンソールと呼ばれるWebベースのインタフェースである。ログインするユーザーによって，一般ユーザー向けメニューと管理者向けメニューの2種類がある。

高度な専門知識を有する専任のIT管理者がいなくても導入を容易にするため，サーバ環境設定ツールを用意しており，あらかじめ導入環境の情報を入力してそれを指定すれば，自動的にPC運用上手TMサーバの構築が完了する。また，複雑なセキュリティポリシーの設計をしなくても運用を開始できるように，あらかじめ5段階のポリシーテンプレートを用意している。これにより，セキュリティに関する知識に自信のないユーザーでも，テンプレートを選択するだけで簡単にセキュリティポリシーの設定ができる。また，項目は個別に設定可能であり，用意されたポリシーテンプレートを基に，ユーザー独自のセキュリティポリシーも簡単に設定することができる。

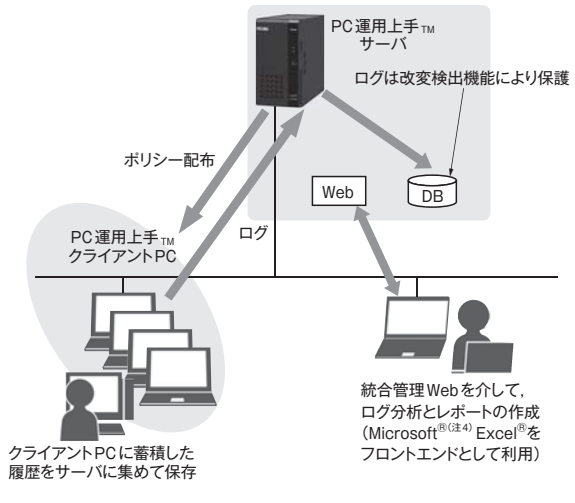


図2. システム構成 ― サーバからのポリシー配布によって監視，制御する。
Configuration of "PC Unyo Jozu"

3 特長

PC運用上手TMの各機能の特長となる技術を**表1**に示す。

表1. PC運用上手TMの特長
Main features of "PC Unyo Jozu"

区 分	技 術
操作監視	・ファイル操作監視 ・メール送信監視
操作制御	・登録USBだけ使用許可
検疫	・修正プログラムの適用検査 ・セキュリティ対策ソフトの検査
PC持出し申請ワークフロー	・内蔵ハードディスク装置（HDD）の暗号化確認 ・BIOSパスワード，HDDパスワードの有効確認

3.1 操作監視

情報漏えい対策の基本はユーザー操作の記録である。いつ，誰が，どの情報にアクセスしたかを記録して，内部犯罪や不正操作の抑止を図るとともに，漏えいが発生した場合には，ログを解析して情報漏えいルートを特定する。PC運用上手TMは，操作監視の対象として，ログオン，アプリケーション起動，ウィンドウタイトル，ファイル操作，Web閲覧，デバイス接続，印刷，及びメール送信の8項目のユーザー操作について監視と記録を行う。

PC運用上手TMのファイル操作監視の特長は，"標準監視"と"高度な監視"の2種類のモードを持つことである。標準監視は，エクスプローラを使ってユーザーが実行したファイル操作を記録するもので，ログ量も抑えられてわかりやすく，解析も容易である。コマンドプロンプトでの操作が記録されないなどの機能的な制約があるが，初期導入時の利用に適している。一方，高度な監視は，アプリケーションが実行するファイル操作も監視するもので，よりち密な監視に適している。これらのモードは，エクスプローラに特化したファイル監視機能と，PC全体を対象としたファイル監視機能の2種類を装備することで実現した。

ファイル操作ログには，PC内のファイル操作の場合"内部"，USBメモリなど外付けデバイスのファイル操作の場合"外付"，サーバなどの共有フォルダのファイル操作の場合"共有"というキーワードを付加する。不特定多数のPCによる外付けデバイスへのファイル書出しの有無を知りたい場合，PCのドライブ構成が異なっていてもドライブ名に頼ることなく

キーワード検索が可能である。

メール監視は，ユーザーからのメール送信の内容を監視する機能である。Outlook®(注5)2003，Outlook®2007，Outlook® Express6，Windows®(注6)Mailなどの主要なメールソフトウェアに対応し（2008年2月現在），送信メールのあて先，件名，本文，及び添付ファイルを保存する。また，監視対象は，社外あてメールだけ，又は全メールのいずれかを選択できる。PC運用上手TMの監視方式の特長は，メールソフトウェアの通信プロトコルに依存しないことである。また，メールには機密情報なども含まれる可能性があるため，システム管理者とは別に，送信メールの閲覧が可能なセキュリティ管理者を設定する仕組みとした。

PCが社外に持ち出されている間もエージェントは操作ログを蓄積し，社内LANに接続された際にログをサーバに転送するため，PC持出し中の操作ももれなく記録できる。

3.2 操作制御

操作制御は，指定アプリケーションの実行禁止，指定サイトのWeb閲覧禁止，フロッピーディスク装置（FDD），光ディスク装置（ODD），USB（Universal Serial Bus）などのデバイス使用制限，及び印刷制限の四つから成る。そのなかでPC運用上手TMの特長は，登録したUSBデバイスだけを使用可能とする機能である（**図3**）。USBメモリやUSB-HDDは同じメーカーの製品でも一つずつ異なる個体識別用のIDを持っている。資産管理システムにそのIDを登録することで，PCにUSBデバイスが接続されたとき，資産管理情報と照合して接続の許可又は不許可を制御する。それにより，利便性を損なわずに適切なUSBデバイスを使用することができる。更に，暗号化機能を有するUSBメモリと組み合わせることで，私物のUSBメモリの勝手な使用を防止するとともに，USBメモリの盗難や紛失，置忘れによる情報漏えい事故を防止することができる。

一方，マウスやキーボードなど情報漏えいの危険性がないUSBデバイスまで登録が必要になると，煩雑で使いにくいシステムになる。そこで，USBデバイスが接続されたときにまず種別を示す情報を読み取り，情報格納用のUSBデバイスだけを使用制限の対象とした。

3.3 検疫

検疫とは，社内LANに接続しようとするPCが，あらかじめ定められた基準を満たしているか検査する仕組みである。基準を満たしていれば社内LANへの接続を許可し，基準を満たさない場合は接続を制限する（**図4**）。Windows®の修正プログラムを適用していなかったり，セキュリティ対策ソフトウェアをインストールしていない無防備なPCが原因でウイルスやワームに感染し，一気に広がる危険を防止するため，日常的にPCをセキュアな状態に保つことを目的とする。

PC運用上手TMは，“Windows®の修正プログラムをきちんと適用しているか”，“セキュリティ対策ソフトウェアを導入しているか”，“パターンファイルを更新しているか”などを検査し，不合格のPCは限られた接続先との通信だけに制限する。検疫を実現する方式には一般的に，認証スイッチ方式，DHCP（Dynamic Host Configuration Protocol）認証方式，パーソナルファイアウォール方式の3種類がある。PC運用上手TMでは，既存のハードウェアやネットワーク構成の変更が不要で導入が容易である点を重視し，パーソナルファイアウォール方式を採用した。

Windows®の修正プログラムは定期的に新規配信されるうえ，OSの種類やインストールされているソフトウェアによって適用すべきプログラムが異なる。PC運用上手TMは，Windows®の修正プログラムの一覧情報をインターネット経由で自動的に取得し，常に最新の状態に保つので，どの修正プログラムが適用されるべきかを管理者は気にする必要がない。また，社内に配信する修正プログラムをWSUS（Windows Server Update Services）で取捨選択している場合にはWSUSサー

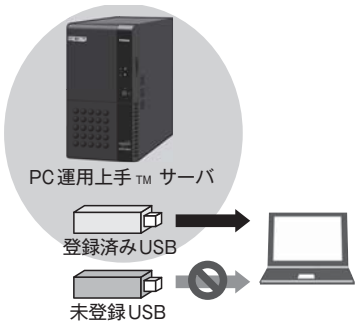


図3. 操作制御機能 — 資産管理システムに登録したUSBデバイスだけ使用できる。
User restriction function

図4. 検疫機能 — PCがセキュアな状態を維持しているかを検査する。
Network quarantine function

バと連携できるので，社内ポリシーに従ったWindows®修正プログラムの適用を検査できる。

セキュリティ対策ソフトウェアはPCに添付される場合も多く，毎年更新されるソフトウェアも多数ある。PC運用上手TMは，代表的な12製品，17バージョンのセキュリティ対策ソフトウェアに対応し（2008年2月現在），社内で複数種類のソフトウェアが混在している環境でもサポートすることが可能である。また，セキュリティ対策ソフトウェアのパターンファイル更新を検出し，一定期間内に更新されたことを検査条件とすることで，管理者が社内のセキュリティ対策ソフトウェアの種類や，最新パターンファイルのバージョンを把握する必要性をなくした。

また，PCが社外に持ち出されたことを自動的に検出し，社外環境での利便性に配慮して通信制限しない仕組みを持たせた。これにより，支店への出張などでセキュリティ対策ソフトウェアが更新できない場合でも，ネットワークに接続できなくなるのを防ぐことができる。

3.4　PC持出し申請ワークフロー

PC持出し申請ワークフローは資産管理システムの一部で，PCの持出しと返却の申請システムである。情報漏えい対策では，PCの盗難や紛失が発生した際，PC内のデータが安全かどうかを客観的に証明できることが重要である。PC運用上手TMは，対象PCのインベントリ情報としてHDDが暗号化されているかを検査し，申請時にチェックできる（**図5**）。PCの情報漏えい対策に有用な技術として，BIOS（Basic Input/Output System）パスワードやHDDパスワードを設定する機能があるが，BIOS機能として独自に実現されるため，ソフトウェアから設定の有効又は無効を確認するのは困難である。PC運用上手TMは，当社製PCのBIOSと連携することで，BIOSパスワードやHDDパスワードの設定状態を取得し，持出し申請時にチェックできる。これは，持ち出されるPCのデータの安全性をより高めた，他社製品にはないPC運用上手TMの特長である。

図5．PC持出し申請ワークフロー ― PCが暗号化されていないと注意を促す。

Example of PC takeout approval display

4　あとがき

PC運用上手TMは，当社のサーバ事業で培った技術を活用し，中小規模の企業をターゲットとして導入しやすさを追求したPC統合セキュリティシステムであり，セキュリティ対策に対するユーザーニーズに応えていけるものと期待している。

今後は更に，企業環境のセキュリティ全体をとらえて，Active Directory®が導入できない環境への対応，よりユーザー数の多い環境への対応，紙媒体に対するセキュリティ対策の強化，及び当社製PCとの連携強化などにタイムリーに応えられる製品を開発していく。

渡壁　　健　WATAKABE Takeshi
PC&ネットワーク社　PC開発センター　サーバ・ネットワーク設計部主務。サーバのハードウェア開発に従事。
PC Development Center

藤原　勇治　FUJIWARA Yuji
PC&ネットワーク社　PC開発センター　サーバ・ネットワーク設計部主務。サーバのハードウェア開発に従事。
PC Development Center

山下　卓規　YAMASHITA Takumi
PC&ネットワーク社　PC開発センター　サーバ・ネットワーク設計部主務。サーバのハードウェア開発に従事。
PC Development Center