

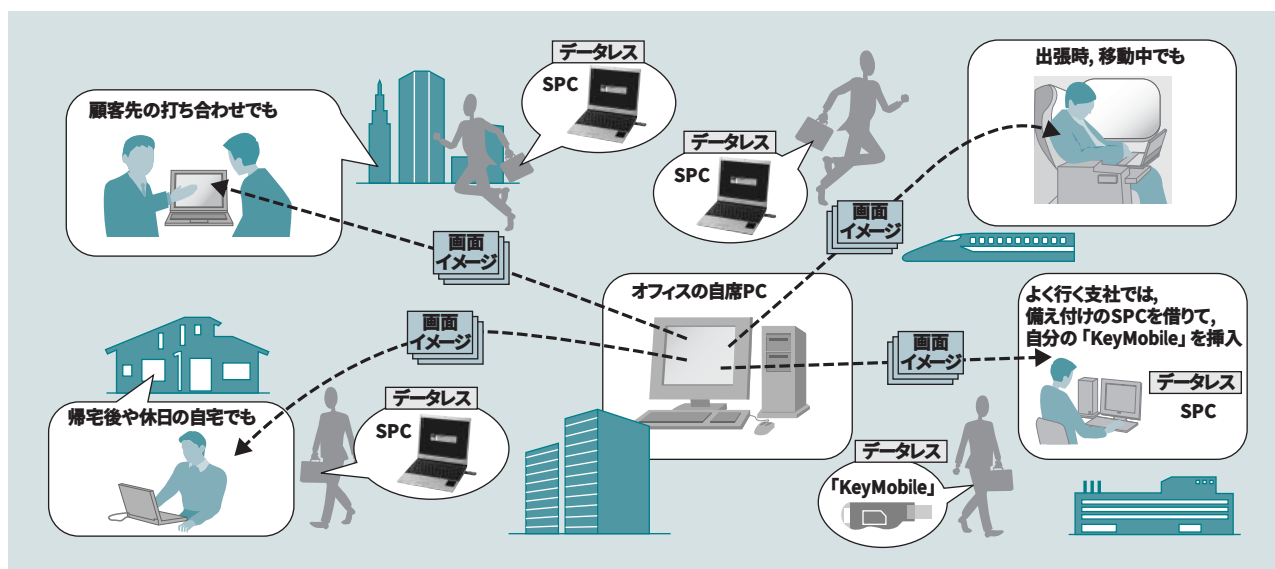
「セキュアクライアントソリューション」を支える「セキュリティPC」と周辺装置

Hitachi's Secure Thin Client, "Security PC" in the Ubiquitous Network Environment

中西 潤 Jun Nakanishi
杉山 卓也 Takuya Sugiyama

牧野 一郎 Ichirō Makino
石原 修 Osamu Ishihara

小高 浩 Hiroshi Kodaka



注:略語説明 SPC(Security Personal Computer)

図1 ユビキタス環境において利便性とセキュア性を両立する「セキュリティPC」

画面転送の仕組みによって、自宅や出張先など、あらゆる場所で自席のPC環境を安全に操作することができる。また、出張先の拠点にセキュリティPCを常設しておけば、ユーザーはKeyMobileを持参するだけで、自席のPC環境に安全にリモートアクセスすることができる。

1. はじめに

ビジネス分野において、多種多様な業務用端末として利用されてきたPC(Personal Computer)は、ユビキタス情報社会の進展に伴い、インターネットなどを通して、企業ユーザーが「いつでも」、「どこでも」企業システムにアクセスできるリモートアクセス機能により、業務効率の向上に貢献してきた。

一方、企業の機密情報や顧客の個人情報などの流出が新たな社会問題となってきている。日立製作所は、モバイルノートPCの社外での紛失・盗難による情報漏えいの防止策として、機密データを保存できないようにハードディスクをなくしたシンクライアント端末と、外部認証デバイス「KeyMobile(キーモバイル)」の組み合わせによるセキュリティPCを業界に先駆けて開発し、2005年初頭から社内を導入して、顧客企業へも提供してきた(図1参照)。

ここでは、「セキュアクライアントソリューション」を支えるクライアント端末となる「セキュリティPC」、およびその周辺機器について述べる。

2. セキュリティPC(SPC)とは

2.1 SPCの特徴

セキュリティPC(以下、SPCと言う。)は、セキュリティ上の脅威について、さまざまな対策を施している(図2参照)。

(1)「データを持たない、出さない」を実現

SPCの基本コンセプトの一つ、「データを持たない」を実現するために、SPCでは画面転送型のリモートアクセスソフトウェアを採用し、オフィスやデータセンターなどに設置されたコンピュータの画面イメージ(画素情報)だけを取り扱い、漏えいさせてはならないデータをSPCには持たない仕組みである。SPCでは、ハードディスクの代わりにフラッシュメモリを搭載し、マイクロソフト社の組込みOS(Operating System)であるWindows^{※)} XP Embeddedを採用し、フラッシュメモリへの書き込みは禁止している。

もう一つの基本コンセプト、「データを出さない」を実現する

※) Windowsは、米国およびその他の国における米国Microsoft Corp.の登録商標である。

セキュリティPCは、「本体内部にデータを持たず、本体外部へデータを出さない」という情報漏えい防止対策を基本コンセプトとし、ユーザー固有の外部認証デバイス「KeyMobile」を鍵とすることで端末本体に依存しない運用を可能としている。社外での「モバイルユース」に加えて、ユーザー環境にリモートアクセスできる「サテライトオフィス」や、フリーアドレス型の「ノンテリトリアルオフィス」など、セキュアでユビキタスなワーキングスタイルを実現することができる。

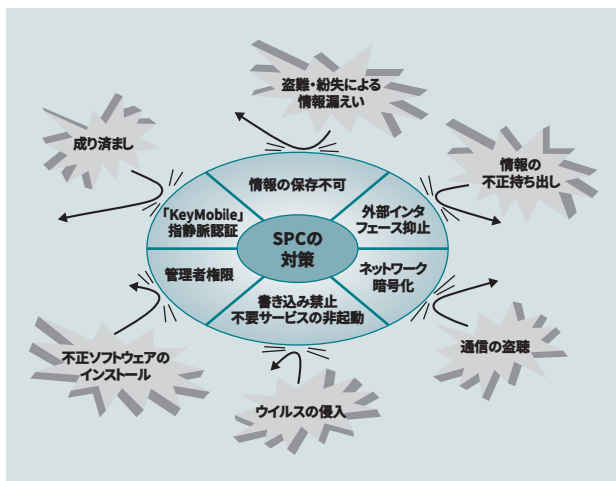


図2 PCへのセキュリティ上の脅威とSPCの対策

SPCは、セキュリティ上の脅威に対して、さまざまな工夫を施している。

ために、SPCでは外部インタフェースの抑止を行っている。デバイスドライバやアプリケーションソフトウェアを搭載しないことで、ローカルプリンタへの印刷や、USB(Universal Serial Bus)メモリなどの外部メディアへの書き込みを禁止している。また、インストールやファイルアクセスを制限し、ドライブの参照は禁止して、インタフェースの抑止は解除ができないようにしている。

(2) KeyMobileによるセキュアな利便性を確保

SPCでは、ユビキタス性を高めるために、外部認証デバイス「KeyMobile」を採用している。KeyMobileは、ICカードチップとフラッシュメモリを搭載したMMC(Multi Media Card)規格サイズの認証デバイスである。クレジットカードやキャッシュカードで使用されているICカードチップを搭載しており、高いセキュリティレベルを実現している。また、フラッシュメモリ部分は、SPCを利用する際の情報を格納することができる。

KeyMobileの最大の特長は、「必要な情報を安全に、いろいろな場所に持って行ける」ことである。SPCには一切の情報を持たないが、KeyMobileにはユーザー認証情報やネットワーク接続情報を格納することができ、これらの情報はユーザー認証を行わないと読み出すことができない仕組みとなっている。

SPC本体からユーザー独自の情報を分離したことにより、ユーザーは、SPC本体にかかわらず、KeyMobileを使って、オフィスやデータセンターなどに設置された自身のコンピュータへ接続することができる。

また、SPCには、利用中にKeyMobileを取り外すと、自動的にSPCをログオフする機能がある。接続先のコンピュータの状態は変化しないので、KeyMobileをSPCに入れて再接続すると、ログオフ前の画面から操作を継続することができる。ユーザーが一時的にSPCを放置したまま席を外す場合などに便利な機能である。

2.2 SPCの機種

社外への持ち出しによる情報漏えい防止対策とリモートアクセス用の各種通信接続に配慮したB5サイズのモバイルノートPC「FLORA Se210」、および有線LAN(Local Area Network)接続を前提としたデスクトップPC「FLORA Se330」が、SPCの代表的な2機種である(図3参照)。

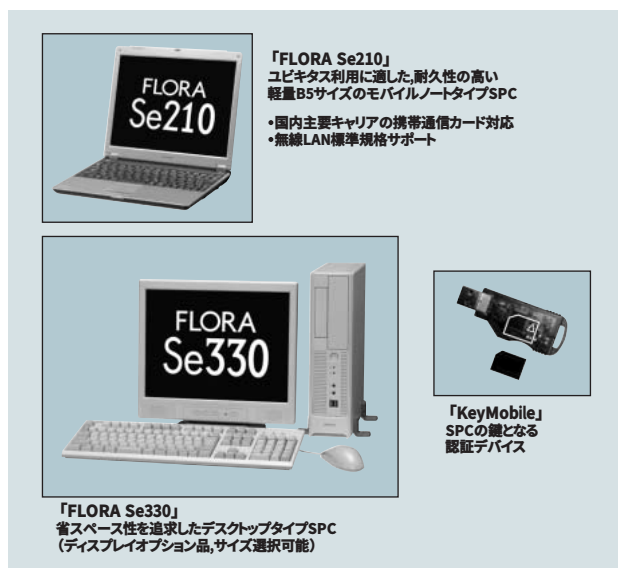
3. SPCの利用形態

3.1 モバイルユースとサテライトオフィス

モバイルSPC「FLORA Se210」は、各種通信形態に対応し、さまざまなビジネスシーンでセキュアな利便性を発揮する。自宅からでもVPN(Virtual Private Network)接続して利用することができるので、例えば、月末の各種業務処理を行うために出張先から自社オフィスにわざわざ戻らずに直接帰宅しても、自宅でセキュアにオフィス業務をこなすことができ、業務効率が向上する。

また、部署の業務形態によっては、FLORA Se210は社員の人数分を導入しなくても、KeyMobileだけを全社員に配布し、1日当たりの出張者の最大数だけ導入しておけば、出張者用モバイル端末として社員間で共有することができ、出張者用モバイル端末の導入コストを低減できる。

KeyMobileの有効利用方法はさまざまあるが、例えば、企業内の本社・支社などの各拠点にFLORA Se330を配備することで、SPCやPCを持ち運ばなくても、KeyMobileさえ持ってい



注:略語説明 LAN(Local Area Network)

図3 SPCと「KeyMobile」の外観

モバイルノートタイプのSPC「FLORA Se210」、デスクトップタイプのSPC「FLORA Se330」、および「KeyMobile」の外観をそれぞれ示す。

れば、自社内の出張先をサテライトオフィスにすることも可能となる。

3.2 ノンテリトリアルオフィスの実現

オフィス内において、固定された自席にとらわれず、社員が業務内容などに応じて最適な仕事環境を自由に選択できるフリーアドレス型の「ノンテリトリアルオフィス」を実現する手段の一つとしても、SPCの活用は有効である。

ユーザーのオフィスPC環境を、PC仮想化サーバやクライアントブレードに集約し、データセンターなどで集中管理することにより、ユーザーは固定デスクを持たずに、SPCとKeyMobileだけでPC業務を遂行することができる。

ノンテリトリアルオフィスは、従来型の内線電話機やIP(Internet Protocol)固定電話機を使用する場合は設置場所に自由度を欠いてしまい、内線PHSを導入するには基地局の設置コストなど、初期投資が大きくなってしまふ。

SPCは、これに対応する拡張機能として、内線電話に対応するソフトフォンを利用することが可能である。社内サーバで社員名簿のディレクトリサービスを提供していれば、SPCを通じた検索結果から直接電話発信ができ、時間とコストの削減に効果が期待できる。社員の個人アドレスなどの情報は、電話機やSPCには残らず、安全なオフィスやデータセンター内にあるコンピュータに保持しているため、社外からでも安心して利用することができる。

3.3 コールセンターへの適用

SPCは、モバイルユースやオフィスユースでの利用だけでなく、コールセンター用端末としても活用できる。

現在のコールセンター運用は、顧客サービス向上のため、PCを利用して顧客の問い合わせ履歴などを参照しながら対応する方式で、コールセンター業務をアウトソーシングしたり、オペレータを社外から起用するケースが多い。企業側は、このような運用形態の中で、顧客の個人情報漏えいの防止策として、入退出管理や記憶装置の持ち込み品チェックなどに多大なコストをかけているのが実情だと推測される。しかし、通常のPCに替わり、「データを持たない、出さない」SPCをコールセンターとして利用すれば、顧客の個人情報流出のリスクが軽減される。

また、コールセンターに必須の通話録音機能でも、オペレータが利用するSPCには通話データを残さないで、音声パケット情報を、SPCとつながっているデータセンターのコンピュータ側に保存することで、セキュアな運用が可能となる。

4. セキュリティPCへの指静脈認証技術の適用

SPCでは、KeyMobileにより、成り済ましを防ぐ仕組みを提供しているが、第三者の成り済ましを防ぐ、さらに強固なセキュリティを実現するために、生体内部データである「指の静脈パターン」で本人を識別する「指静脈認証装置」を拡張機能として採用している。SPC用の指静脈認証装置には、FLORA Se210用の内蔵タイプと、FLORA Se330用のUSBインタフェースに接続する外付けタイプがある(図4参照)。

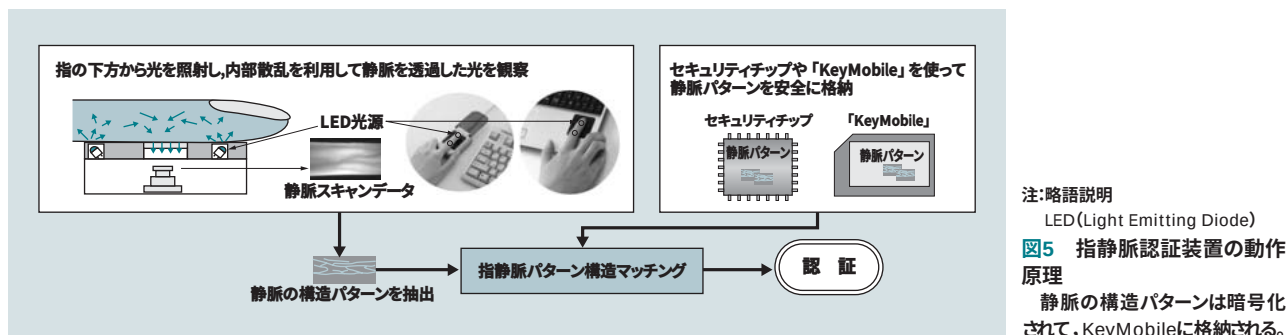
指静脈認証装置は、指内部の静脈パターンを照合するため、肌表面の状態(湿気、乾燥、汚れなど)の影響を受けず、高い認証精度を実現する(図5参照)。

また、認証デバイス、KeyMobileのPIN(Personal Identification Number)コード入力を、指静脈による本人認証に置き換えることができるため、ユーザーはPINコードを記憶する手間が省け、操作の利便性が向上する。



図4 SPCへの指静脈認証装置の適用

「FLORA Se210」に内蔵した指静脈認証装置と、外付けタイプの指静脈認証装置の外観をそれぞれ示す。



5. モバイルSPCの簡易導入サービス

セキュアクライアントソリューションにおけるSPCの導入にあたっては、ユーザー認証のためのサーバ構築が必要であり、さらにモバイルユースの場合では、VPNサーバの構築も必要となる。

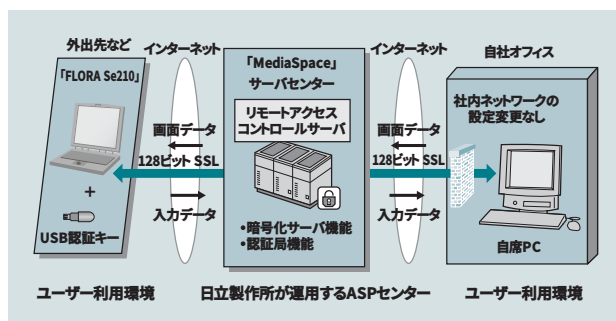
業務上、モバイルノートPCの利用が必須であるが、個人情報漏えいリスクのために社外への持ち出しを禁じている企業も少なくない。そこで、日立製作所は、SPCを容易に導入できるように、ユーザー認証やVPNなどをASP(Application Service Provider)運用するサービス「FLORA Se210 リモートアクセスパック」を提供している(図6参照)。

このサービスでは、SSL(Secure Socket Layer)-VPN方式の利用により、自社オフィス側のネットワーク環境やイントラネットの設定を変更することなく、セキュアにリモートアクセスをすることが可能である。また、サーバセンターへのユーザー登録後、自席PC用のソフトウェアをユーザー自身がダウンロードかつインストールすることで自席PC側の準備は完了するので、SPC利用開始までのリードタイムを大幅に短縮できる。

6. おわりに

ここでは、「セキュアクライアントソリューション」を支えるクライアント端末「セキュリティPC」、およびその周辺機器について述べた。

個人情報ははじめとした機密情報の漏えい防止対策とし



注:略語説明 SSL(Secure Socket Layer), ASP(Application Service Provider)
USB(Universal Serial Bus)

図6 「FLORA Se210」リモートアクセスパックの仕組み

日立製作所が提供するASPセンター「MediaSpace」によって、サービスの運営がされている。

て、セキュリティに注目して開発されたSPCは、拡張オプションや運用システムによってセキュリティ強度を向上するとともに、ユーザー業務における利便性をいっそう向上することが可能となっている。

日立製作所は、今後ますます発展していくユビキタス情報社会において、セキュアかつ便利なツールとして、SPCの機能をさらに向上させていく考えである。

執筆者紹介



中西 潤
1991年日立製作所入社、情報・通信グループ セキュリティ事業部 事業企画室 所属
現在、指静脈認証を使ったセキュリティ関連商品の事業化に従事



杉山 卓也
1991年日立製作所入社、情報・通信グループ エンタープライズサーバ事業部 クライアント本部 ビジネス統括部 所属
現在、FLORAおよびセキュリティPCの商品企画に従事



牧野 一郎
1992年日立製作所入社、情報・通信グループ エンタープライズサーバ事業部 クライアント本部 ビジネス統括部 所属
現在、セキュリティPCの商品企画に従事



石原 修
1991年日立製作所入社、情報・通信グループ トレーサビリティ・RFID事業部 ミュー・RFID事業推進本部 商品開発部 所属
現在、ミュー/RFID製品開発に従事



小高 浩
1987年日立製作所入社、情報・通信グループ ネットワークソリューション事業部 ネットワーク統括戦略本部 ネットワーク事業推進センタ 所属
現在、IPテレフォニーの事業推進に従事