情報漏えいを阻止する「セキュアクライアントソリューション」

Secure Client Solution for Preventing Information Leakage

新井 利明 Toshiaki Arai　田中 輝雄 Teruo Tanaka　野田 文雄 Fumio Noda

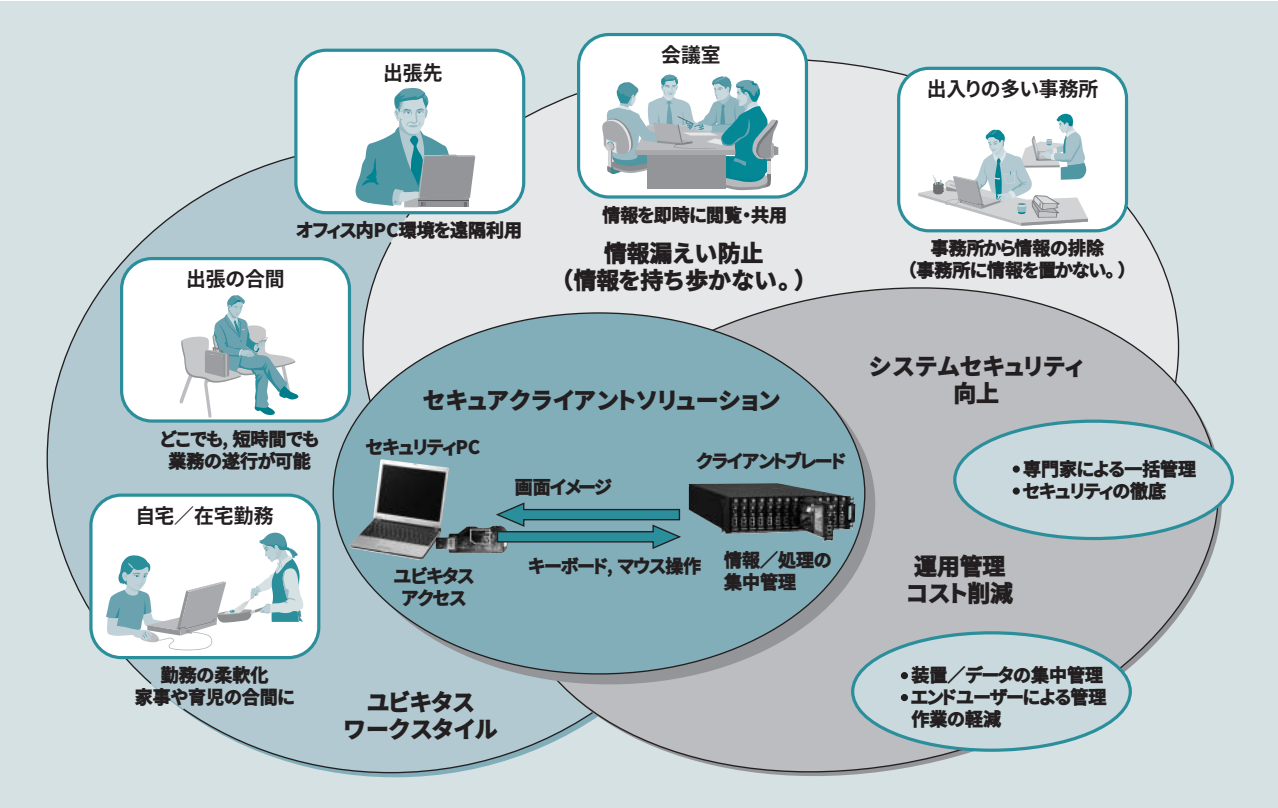


図1 「セキュアクライアントソリューション」が提供する価値
情報漏えいの防止やセキュリティ向上だけでなく，新たなワークスタイルの創生，運用管理コスト削減など，その価値は多面にわたる。

1. はじめに

情報漏えいの発生は，対策や流出情報への保障に多大な出費を要するだけでなく，漏えいを引き起こした企業に対する信頼性を大きく損なうため，影響は長期間にわたり，該当企業の存続をも危うくする危険性がある大きな問題である。情報漏えいの中でも，モバイルPC（Personal Computer）からの漏えいは対策が困難なものの一つである。情報を格納したPCを各人が持ち歩く場合には，事故の可能性を排除することができない。すなわち，電車やバスの中に置き忘れたなどのうっかり事故や盗難など，いたるところにPC紛失の危険性があるからである。そのため，モバイルPCのセキュリティを確保するには「事故は必ず起こる」という想定で施策する必要がある。

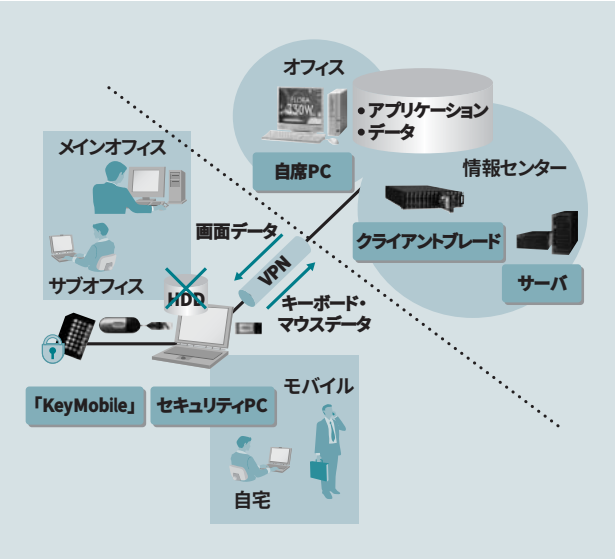
一方，ビジネスの拡大のためには，オフィスにとどまることなく，従来の範ちゅうを超えた場所や時間での業務が新たに必要となることが多い。新たな場所，新たな時間，新たな顧客を対象とすることが，ビジネスチャンスにつながるためである。また，ブロードバンドの進展にともない，ワークスタイルも大きく変化している。従来のオフィス時間に縛られることなく，自由な時間に自由な場所で業務をすることで，社員の士気も高まり，生産性向上や雇用の定常的な確保にもつながる。

ここでは，単なるオフィスセキュリティの確保だけでなく，オフィス作業者が活動する場としてのオフィスシステムの基盤となる「セキュアクライアントソリューション」の基本コンセプトと，その概要について述べる（図1参照）。

日立製作所は，PCからの情報漏えいを防止し，安全かつ快適な利用環境を実現する「セキュアクライアントソリューション」を開発した。情報を格納することも持ち出すこともできないセキュリティPCと，個人を認証するデバイス「KeyMobile」とを組み合わせることにより，紛失など不慮の事故の際にも情報漏えいを阻止することを可能とした。オフィスで使用するすべての情報を，情報センターに配置したクライアントブレードと高信頼ストレージに集約・配置し，安全・安心に利用できる環境を提供する。

2. セキュアクライアントソリューション（SCS）の概要

セキュアクライアントソリューション（以下，SCSと言う。）開発の基本となる考え方は「事故は必ず起こる」である。モバイル環境での業務遂行のためにPCを持ち歩くかぎり，盗難，置き忘れなどの事故を完全に回避することは不可能である。モバイルPCを紛失した場合，たとえデータが暗号化されていたとしても，情報が流出したことは事実であり，情報漏えいは回避されたと言うことはできない。このことから，「情報は持ち運ぶから漏えいする，持ち運ばなければ漏えいしない」が日立の考えるSCSの基本コンセプトである。すなわち，情報は持ち運ぶ必要がなく，利用できさえすればよい，という考えである。PCに情報を格納して持ち運ぶのではなく，情報は情報センターに安全に格納したままで，許可された人物だけがそれを参照したり，利用することができる仕組みを作ればよいという考えに従って，情報を持ち運ぶことができないセキュリティPCと個々の作業者を認証する「KeyMobile」を組み合わせて，情報をセンターに閉じ込めたまま，自由に利用できる環境を構築できるようにした。さらに，情報や機器を集約して一元管理することで，管理工数を削減できるクライアントブレードやIP（Internet Protocol）ストレージなどを導入し，オフィス環境からの情報および情報機器の撤廃を可能とした。これらの製品により，情報を持ち運ぶことなく安全に利用することが可能となる。



注：略語説明　VPN（Virtual Private Network），HDD（Hard Disk Drive）

図2　SCSの概要

情報とPC機器を情報センターに集約し，セキュリティPCと「KeyMobile」を用いて安全・安心に業務を遂行できる。

SCSの概要を図2に示す。SCSでは，業務遂行に必要な情報とそれを操作する情報処理装置は，情報センター内に隔離されている。作業者はKeyMobileだけを持ち歩くことで，いつでも，どこからでも，安全・安心に隔離された情報にアクセスすることが可能である。このとき，セキュリティPCは単なる表示装置あるいは入力装置として機能し，それ自体に情報を格納することはない。セキュリティPCは必要に応じて持ち歩くか，または共用の機器として各所に配置しておくことも可能である。

3. SCSの効果と利用シーン

3.1 SCSの効果

（1）情報漏えいの根絶

SCSの効果は，情報漏えいを確実に回避できることにある。セキュリティPCには何の情報も格納することができないため，万一セキュリティPCを紛失した場合にも「情報漏えいはない」と断言することができる。また，セキュリティPCを利用するためにはKeyMobileとパスワードの両方が必要であることから，紛失したセキュリティPCを利用して第三者が情報を取り出すことはできない。さらに，KeyMobileを紛失した場合には，そのKeyMobileに登録されている証明書を無効とすることにより，KeyMobile自体を無効とし，使用することを禁止できる。以上のように，KeyMobileとセキュリティPCの組み合わせによって，万一の場合にも情報漏えいを確実に回避することが可能である。

セキュリティPCは，情報を格納することができないばかりではなく，情報センターに集約された情報を取り出すことも不可能である。USB（Universal Serial Bus）メモリなどの記録媒体やプリンタなどをセキュリティPCに接続することができないため，セキュリティPCを介して情報を格納することはできない。このように，作業者がセキュリティPCだけを用いて作業しているか

ぎり，情報は情報センターだけに格納されており，外部に持ち出すことは不可能である。したがって，モバイル環境での情報漏えいを防止するだけでなく，内部犯行による情報漏えいも予防することが可能である。

（2）運用管理コスト削減，システムセキュリティ向上

SCSでは，個人のPCの処理装置やデータを情報センターに集約し，一括して管理するため，各個人がPC管理作業を行う必要がなくなり，運用管理コストを低減することが可能である。後述するポイント・ブレード型のシステムを導入した場合の運用管理コスト低減の試算結果を図3に示す。運用管理コストは，ほぼ半減できると予測している。

また，SCSでは，集約された情報や機器を専門のオペレータが一括して管理するため，ウイルスチェックやバックアップなどのミスをなくすことが可能であり，システム全体のセキュリティや信頼性の向上が見込まれる。

（3）本来業務への集中と業務効率の向上

SCSでは，個人のPC機器はデータとともにセンターに集約され，一元管理される。そのため，各ユーザーは個人でPCの管理作業を実施することなく，常に最新のバージョンのソフトウェアやセキュリティ環境で業務を遂行することができ，ユーザーの本来業務に集中することができる。また，ネットワークに接続できる環境であれば，セキュリティPCとKeyMobileだけを持ち運ぶことで，場所を問わず，同じ操作，同じ実行環境でPCを使用することができるため，多様なワークスタイルに対応することが可能であり，業務効率の向上を図ることができる。

3.2 利用シーン

SCSの特長を活用することにより，オフィス作業者の業務環境を大きく改善することが可能となる。これまで，情報漏えいの危険性があるため，PCを持ち出しての業務が禁止されていた部署においても，作業者がオフィスから外に出て，最も作業のしやすい環境で業務を遂行することが可能となる。

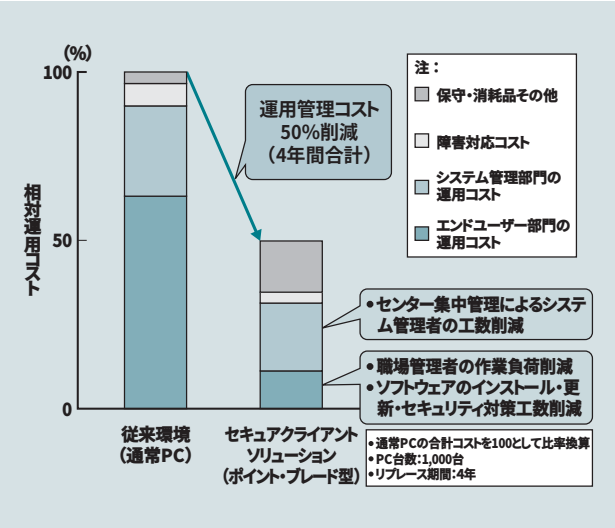


図3　SCSの運用管理コストの試算
従来の通常のPCを用いた場合に比べ，運用管理コストが半減すると予測される。

（1）出 張 先

出張先で，顧客と直接商談したり，プレゼンテーションを実施する際には，詳細な顧客情報や営業機密情報が必要となる。これまで，情報漏えいの危険性があるため持ち出すことができなかった機密性の高い情報も，セキュリティPCを利用することで，安全・安心にどこからでも閲覧することができる。その際，セキュリティPCを用いての業務処理環境はオフィス内の自分の机上の業務環境と同一であることから，出張のために特別な準備をするなど不要な付帯作業は発生しない。また，出張から帰った場合にも，収集したデータを出張用のPCからオフィスのPCへダウンロードするという作業は発生しない。

（2）出張の合間

出張の合間や，出張中の急用に対しても，どこでも，安全に業務を遂行することが可能である。駅や空港のビジネススポットや近年整備されつつあるファストフード店などの無線LAN（Local Area Network）環境を利用して自由に業務を遂行できる。また，データ通信カードを用いた場合にも，高速リモートアクセスソフトウェアにより，ストレスを感じることなく，快適に業務を遂行することが可能である。

（3）自　　宅

忙しいビジネスマンでも，自宅に早く帰ることができる。出張先から，報告書の作成や業務連絡のために帰社する必要はなく，直接帰宅して自宅でゆっくりと業務を継続することが可能である。業務環境はオフィスと自宅でまったく同一であり，従来のように，自宅での仕事のために，データを自宅用PCにコピーしたり，自宅で取得したメールを会社に転送するなどの余分な手間がなく，かつセキュリティ上，問題の多い作業をする必要もない。

（4）在宅勤務

在宅勤務で，家事や育児と掛け持ちの場合も，セキュリティPCがあれば，いつでも，どこでも仕事をすることができる。セキュリティPCにKeyMobileを挿入するだけで，即座に業務環境を利用できるため，手の空いた時間に自由に仕事をすることができる。

（5）会 議 室

会議室に共用のセキュリティPCを配置しておくことで，出席者が情報を自由に共用することができる。議論の流れに応じて，各人のPCに所有している情報にセキュリティPCを用いてアクセスし，閲覧，回覧することができる。すべての資料を持ち歩いて会議に参加するのではなく，KeyMobileだけを持参して参加すればよい。

（6）出入りの多い事務所

PC装置を集約するクライアントブレードを利用することで，オ

フィス内のセキュリティを確保することが可能である。貴重な情報とPC機器をセンターに集約することで，事務所からは一切の情報を排除することができるため，特に，出入りの多い事務所のセキュリティ確保に有効である。

SCSの効果は次のとおりである。

（a）いつでも，どこでも，安全・安心に仕事ができる。

（b）オフィスとモバイルで同一の作業環境を構築できるため，仕事をシームレスに遂行することができる。

（c）オフィス用，モバイル用，自宅用など個別のPCを持つ必要がなく，複数のPCの管理やデータ整合性の維持などの業務に直接関係のない作業を省き，本来業務に集中することができる。

このような効果を持つSCSを導入することにより，業務効率の向上とPC管理コストの低減を図ることが可能である。

4. SCSを支える構成要素

SCSを構成する主な要素は以下の五つである。

（1）セキュリティPC

HDD（Hard Disk Drive）を持たず，情報を格納することのできない新しいタイプのクライアントPCである。本体内部に情報を格納することができないだけでなく，情報漏えいの要因となる危険性のあるUSBポートやプリンタポートなど，すべての情報転送のインタフェースを利用不可能としている。これにより，セキュリティPCを介してのいかなる情報漏えいをも排除することができる。また，いっそう高度なセキュリティを実現する，指静脈認証機能付きのセキュリティPCも製品化している。

（2）KeyMobile

KeyMobileは，ICチップとフラッシュメモリを備えたMMC（Mobile Multimedia Card）規格サイズの認証デバイスである。ICチップには認証・証明書基盤が発行する証明書を格納し，フラッシュ領域にはユーザーの利用環境を格納する。この組み合わせにより，ユーザーはKeyMobileを持ち歩くだけで，いつでも，どこからでも安全・安心に自分独自の作業環境を利用することが可能となる。

（3）クライアントブレード

高密度に実装したPCであり，シャーシやラックに集約して格納することができる。これにより，従来はオフィスや外出先に散在していたPCとそこに格納されていた情報（データ）を，まとめて情報センターに集約することが可能である。一括運用向けに設計されているので，ユーザーはPCの管理作業を行う必要がない。1ラックに100台以上搭載することが可能であり，スペースの有効利用も図ることができる。

（4）高速リモートアクセスソフトウェア

接続ソフトウェアは，セキュリティPCと接続元のPCとの間の通信を可能とする。PCからセキュリティPCへは画面イメージを転送し，セキュリティPCからPCへはキーボード入力イメージを転送する。ネットワーク帯域に応じて，通信プロトコルを変化させる機能により，低品質なネットワーク環境においても，実用的な応答性を実現している。

（5）通信カード，VPN（Virtual Private Network）

リモート環境からPC機器にアクセスするものである。SCSでは，多様な要求に応えるため，主要な製品に対応している。

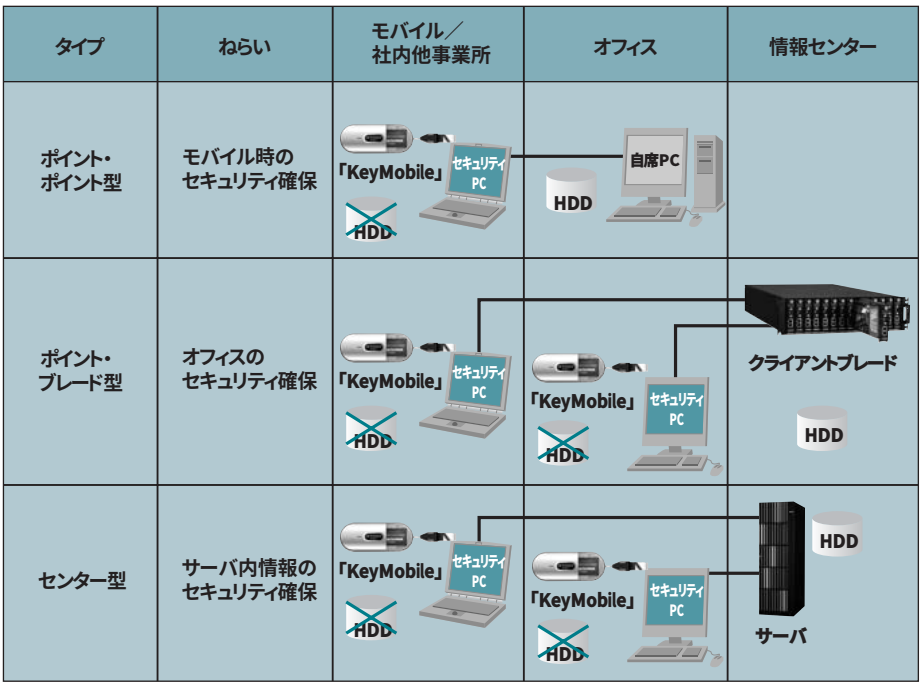


図4　SCSの標準パターン
目的に応じた3種類の基本パターンを用意している。

5. システム導入パターン

SCSは，多様なユーザーのニーズに応えるため，前述したさまざまな構成要素を自由に組み合わせてソリューションを構築することが可能であるが，標準的な3パターンを用意している（図4参照）。

5.1 ポイント・ポイント型

（1）概要と特徴

これまでオフィスで使用していたデスクトップPCに，セキュリティPCとKeyMobileを用いてリモート環境から接続して使用する形態である。従来利用していたオフィスのPC利用環境をそのまま，リモート環境から安

全・安心に使用することができる。モバイル環境での情報漏えい防止と移行性を重視したソリューションである(図5参照)。

(2) 想定用途

出張先や自宅など，オフィス外へノートPCを持ち出す機会の多い，営業・企画部門者の情報漏えい対策に最適である。デスクトップ上のPCをそのまま利用できるため，ノートPCとのデータの一貫性を考慮せずに利用することができ，ユーザーのPC運用管理の手間が大幅に削減できる。また，これまでセキュリティ上の理由により，ノートPCの持ち出しが禁止されていた部門でも，このソリューションにより，業務環境が大きく広がり，ビジネスの拡大が望める。

(3) 移 行 性

セキュリティPCとKeyMobileを導入するだけで，既存のシステムをそのまま利用できる。外部からのアクセスに対応できるネットワーク環境が構築されていない場合には，VPNの導入・設定やデータ通信カードが必要となる。

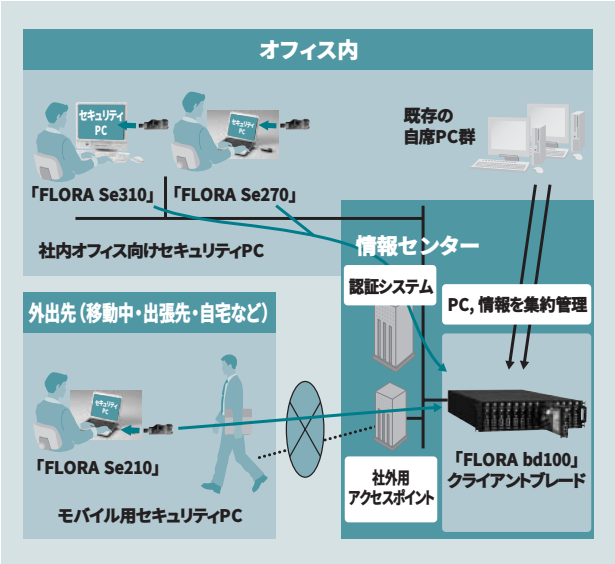


図6 ポイント・ブレード型の概要
1枚のブレードを個人に割り当てて，リソースを占有し，安定した環境で業務を遂行する。既存パソコンの集約を図り，情報漏えい防止をさらに強化できる。

5.2 ポイント・ブレード型

(1) 概要と特徴

オフィス内に散在しているPCを，データとともに情報センターに集約して，セキュリティPCから利用する形態である。既存PC上のソフトウェア資産はそのまま活用し，PCハードウェアと情報を集約することにより，オフィス内からの情報漏えいリスクを低減し，オフィスのセキュリティを向上する。また，IT資産を集約することによって管理負荷を低減し，セキュリティレベルを統一することが可能である。さらに，データ(情報)を集約する統合ストレージ機能との組み合わせにより，データ管理の容易化および信頼性向上が可能となる(図6参照)。

(2) 想定用途

比較的大規模な一般オフィスや顧客情報を扱う営業拠点(金融，流通，コールセンターなど)に最適であり，集約によるセキュリティの向上と運用管理コストの低減が見込まれる。また，複数の小規模な営業拠点が分散されている保険・証券業務などでは拠点集約により，運用者が削減でき，コストを抑えることが可能である。

(3) 移 行 性

クライアントブレードを情報センターに導入し，既存のデスクトップPC上のプログラムおよびデータをクライアントブレードに移行する。オフィス内およびモバイル環境からセキュリティPCとKeyMobileを用いてクライアントブレードにアクセスする。また，ポイント・ポイント型から，クライアントブレードを導入して移行することも可能である。

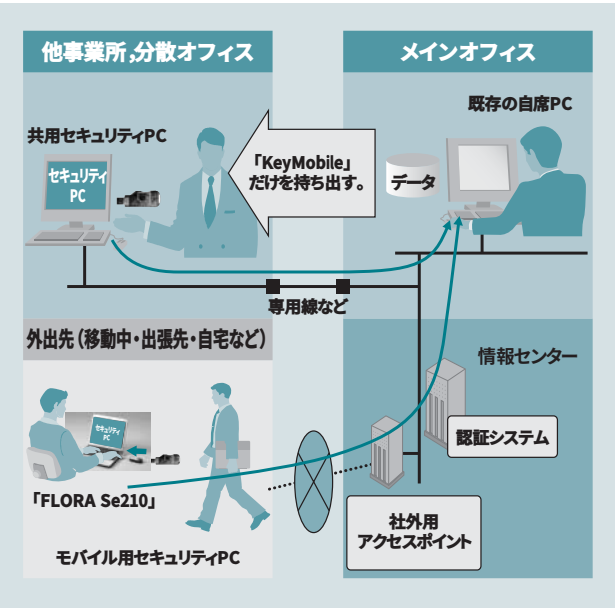


図5 ポイント・ポイント型の概要
社内ではKeyMobileだけで，共用セキュリティPCがそのまま自席PCとして利用可能であり，外出先ではKeyMobileとセキュリティPCで，自席PC環境をそのまま利用できる。

5.3 センター型

(1) 概要と特徴

1台のサーバを複数のユーザーが共用して利用する形態である。セキュリティPCとKeyMobileを利用してサーバにアクセスすることにより，セキュリティの向上が可能となる。すべてのユーザーが同一の環境で動作するため，一元管理による管理負荷の低減が可能である(図7参照)。

(2) 想定用途

定型業務の多いオフィスや顧客情報を扱う営業拠点への導入が最適である。

(3) 移 行 性

現在，サーバを利用しての業務を遂行中であれば，セキュ

リティPCとKeyMobileだけの導入で利用可能となる。個別PCを利用している場合には，ソフトウェアの移行性を検証する必要がある。

以上の三つのケースは，ユーザーの業務特性に応じて，一つのシステム中に混在させることも可能である。

6. SCSの将来像

SCSは，「情報漏えい撲滅」を目標に，モバイル環境のセキュリティ強化を出発点として，クライアントブレード導入によるオフィス内のセキュリティ強化や，指静脈認証によるさらなる強化へと進化してきた。

今後は，PCからの漏えいを防止するだけでなく，システムとしてのセキュリティ強化を目指す。また，近年注目を浴びているSOX（Sarbanes-Oxley）法対応や内部統制に向けた取り組みを推進する。

7. おわりに

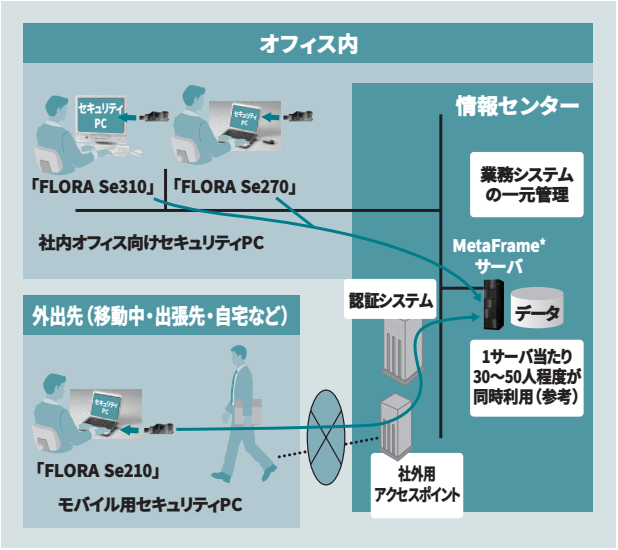
ここでは，PCからの情報漏えいを防止するセキュアクライアントソリューションについて述べた。

この特集では，以降，SCSを支える製品として，セキュリティPC，リモートアクセス技術，クライアントブレードと運用管理，ブレードサーバなどの基本技術を説明したうえで，続いて，SCSの導入と運用を簡便化するサポートサービスおよびアウトソーシングについて解説し，最後に日立での社内適用事例について述べる。

情報システムが社会に浸透するにつれて，情報が漏えいすることのリスクを回避することがますます困難となりつつある。ここに示したソリューションは情報システムの一部からの漏えいの防止であるが，これを基盤として，システム全体のセキュリティ確保のため，研究開発を推進していく。

参考文献ほか

1）柴田英寿：オフィスからパソコンがなくなる日，東洋経済新聞社
2）小林，外：よくわかる企業セキュリティ入門，日刊工業新聞社
3）セキュアクライアントソリューション，
http://www.hitachi.co.jp/products/secure_client_solution/



＊MetaFrameは，Citrix Systems, Inc. の米国あるいはその他の国における登録商標である。

図7　センター型の概要
1台のサーバを複数ユーザーで利用し，リソースの効率的な利用が可能である。多数の利用者が専用・定期業務を中心に利用するシステムに最適である。

執筆者紹介

新井 利明
1978年日立製作所入社，システム開発研究所 所属
現在，セキュアオフィスシステムの研究開発に従事
工学博士
情報処理学会会員

田中 輝雄
1983年日立製作所入社，情報・通信グループ プラットフォームソリューション事業部 事業戦略部 所属
現在，プラットフォームソリューション事業企画に従事
情報処理学会会員，日本応用数理学会会員

野田 文雄
1983年日立製作所入社，情報・通信グループ プラットフォームソリューション事業部 事業戦略部 所属
現在，セキュアクライアントソリューションの開発に従事
映像情報メディア学会会員，IEEE会員