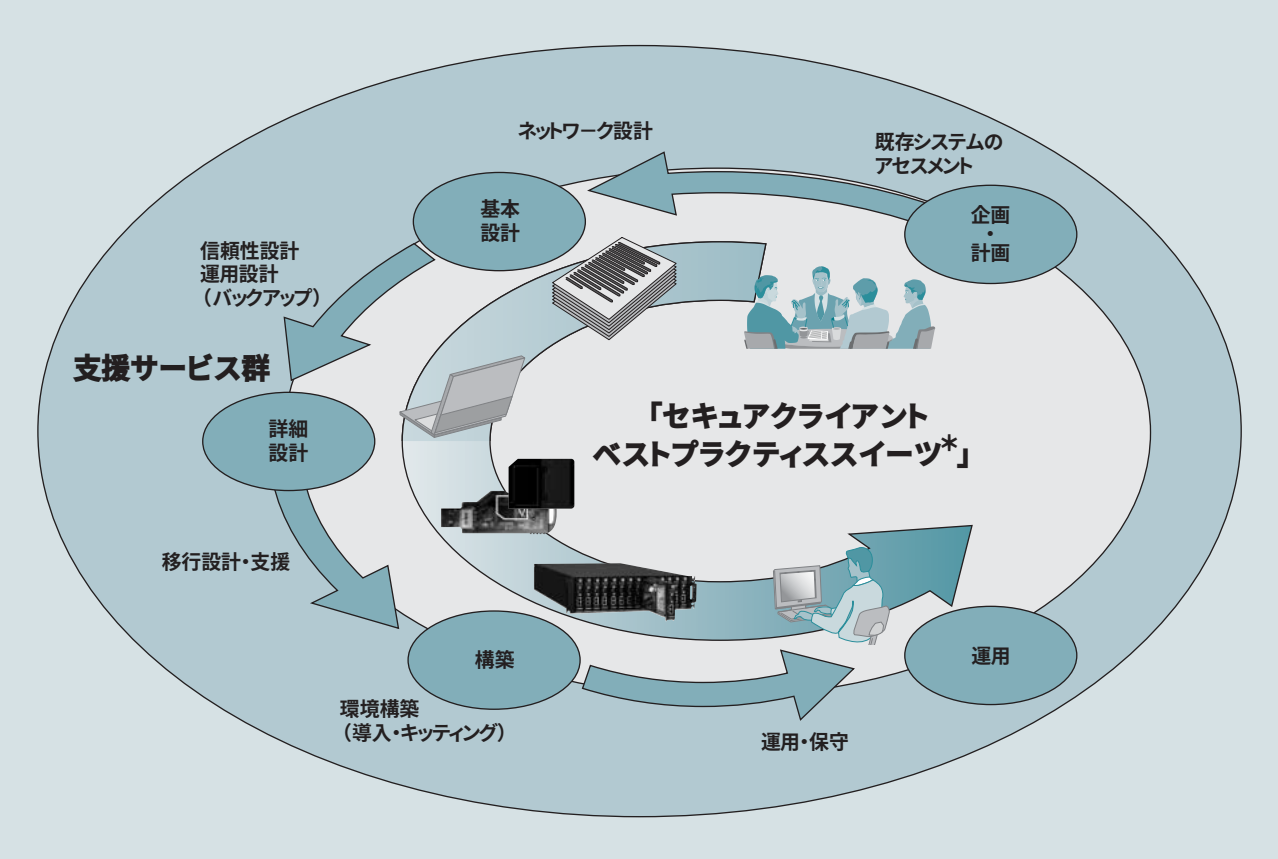
「セキュアクライアントソリューション」を取り巻く支援サービス群

Diverse Services in and around Secure Client Solution

高原 清 Kiyoshi Takahara
黒川 浩一 Kôichi Kurokawa
米山 英彦 Hidehiko Yoneyama
白勢 則之 Noriyuki Shirase



＊「ベストプラクティススイーツ」は，事前検証済みの推奨システム構成・製品の組み合わせをパターン化し，高品質な設計・構築サービスを迅速に提供するものである。

図1 「セキュアクライアントソリューション」を取り巻く多様な支援サービス

セキュリティPC，クライアントブレードを用いたシステムの構築はもとより，構築前の既存システムのアセスメント，ネットワークの設計，クライアントブレードのバックアップなど，ライフサイクル全般にわたり，関連するさまざまな構築・設計・運用についてのサービスが提供されている。

1. はじめに

「セキュアクライアントソリューション」では，すべての情報の保持と処理がクライアントブレード（もしくはサーバ）側で行われる。セキュリティPC（Personal Computer）には，クライアントブレードを操作するために必要な画面イメージとマウスのクリックなどの操作指示だけが授受される。

この仕組みにより，セキュリティPCには一切の業務情報を保持しないことから，情報の漏えいが防止されている。すなわち，「情報を持たないので，漏らすこともない」のである。

他方，このような画面転送方式を行い，円滑な操作環境を提供するためには，従来のクライアント環境とは異なるネットワーク設計が必要となる。

また，利用者の手もとにあるセキュリティPCには一切の情報が保持されず，従来のPCに相当するクライアントブレードは利用者の手の届かないセンターに設置されることから，これまでは利用者自身の手で可能だったプログラムのインストールやアップデート，データのバックアップなどを直接行うことができなくなる。

実際に導入するには，利用環境の構築や，従来のクライアントサーバシステム型のネットワーク構成から画面転送を想定したネットワーク構成への変更，既存PC上のデータの移行，ユーザーの手もとにあったPCがセンターで一括管理されること

日立製作所は，ITプラットフォームの設計から構築について，事前に検証した推奨システムの構成，製品の組み合わせをパターン化し，設計や構築に必要なサービスをセットとした「ベストプラクティススイーツ」を提供するとともに，「セキュアクライアントソリューション」の導入についても，基本設計から構築までを一貫してサポートする「セキュアクライアントベストプラクティススイーツ」サービスを提供している。また，導入においても，セキュリティPC，クライアントブレードを中心としたシステム構築だけでなく，その周辺分野についても多様なソリューションを用意し，円滑な導入と運用を支援している。

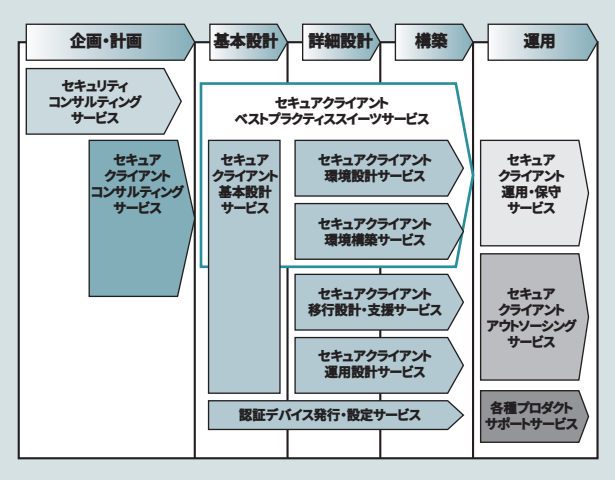


図2　セキュアクライアントソリューションを構成するサービス
システム導入から運用までライフサイクルをカバーしたサービスを提供している。

によるバックアップやウイルス感染時の対策といった運用方法など，システム環境の変更や，運用手順の変更などが不可欠となる。

日立製作所は，従来のPCを利用したシステムから，セキュリティPCとクライアントブレードを利用するセキュアクライアント環境への移行や運用については，そのライフサイクルに沿って多様なサービスを用意し，円滑な導入と運用を支援している（**図1**，**図2**参照）。

ここでは，クライアントブレード型セキュアクライアントソリューション（以下，SCSと言う。），およびその周辺ソリューションについて述べる。

2．導入前設計ソリューション

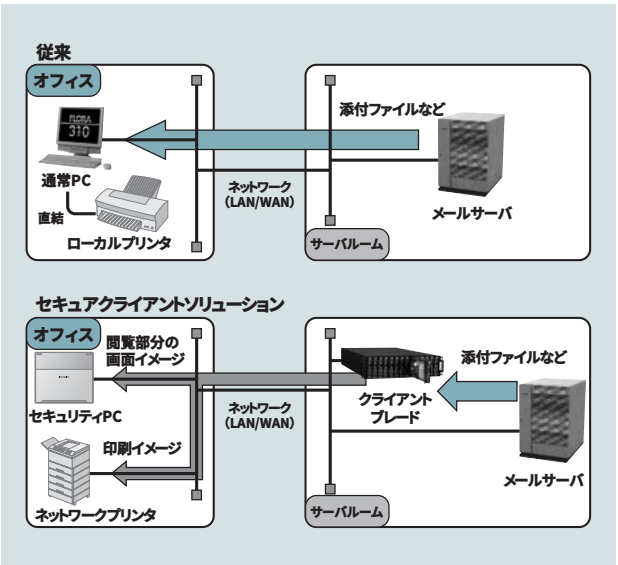
2.1 ネットワーク設計ソリューション

クライアントサーバシステムでは，画面レイアウトなどのユーザーインタフェースはクライアントのPCで動作するプログラムに内包され，業務データだけが送受されていた。これに対し，セキュアクライアントソリューションでは，セキュリティPCとクライアントブレードの間は，画面イメージと操作指示（マウスクリック，キー操作などのデータ）が送受される。一般的に画面データは業務データよりも大きくなることから，セキュリティPCを利用するためには，セキュリティPCとクライアントブレードの間は広い帯域を確保することが必要となる。

また，SCSの「情報を出力しない」という基本コンセプトに基づき，セキュリティPCへのプリンタの接続と印刷が禁止されている。このため，印刷はサーバルームに設置されるクライアントブレードから，オフィスに置かれるネットワークプリンタに直接出力することになり，サーバルームとオフィスの間のネットワーク流量を増加させることになる。

しかし，従来はサーバとPCの間で授受されていた大容量ファイル（メールシステムにおける添付ファイルなど）は，サーバとクライアントブレードの間のネットワークにとどまることになる。両者が同じサーバルームに配置されている場合には，オフィスのセキュリティPCには閲覧する部分の画面イメージだけが送られるため，ネットワークのトラフィックは低減される（**図3**参照）。

以上のように，セキュリティPC，クライアントブレードを導入する場合には，ネットワークの構成の見直しが不可欠である。各種サーバ，クライアントブレード，セキュリティPCの間で，どのよ



注：略語説明　PC（Personal Computer），LAN（Local Area Network）
WAN（Wide Area Network）

図3　ネットワーク設計の例
業務やシステムの特性に配慮し，従来とは異なる設計が必要になる。

うな通信が，どの程度発生するかは，業務やシステムの特性に依存することから，既存システムのアセスメントと，その結果を反映してネットワーク設計することがSCSの環境設計サービスの一つとして提供されている。

3. 導入・移行ソリューション

3.1 クライアントブレードのキッティング

ここでのキッティングとは，クライアントブレードに標準的なOS（Operating System），ソフトウェアなどを組み込み，個々のクライアントブレードについて，IP（Internet Protocol）アドレス，コンピュータ名など固有の情報を設定することを言う。

これまで，企業でのPCの運用では，企業ごとに必要な市販ソフトウェアや業務アプリケーションを組み込んだプレインストールPCを配付し，IPアドレスの設定などは配布されたユーザーの職場の管理者が担当してきた。しかし，SCSでは，利用者はネットワークを介してセキュリティPCからクライアントブレードに接続するため，事前にクライアントブレードのネットワーク設定などが済まされていなければならない。さらに，Windows※）では，各マシン単位にSID（System Identifier）と呼ばれる内部的な識別子が付与される。SIDは，グローバルに一意であることが求められる。

以上のように，クライアントブレードのキッティングでは，単純に内蔵ハードディスクを複製するのでは不十分であり，各種の設定を必要とする。また，一度利用されたブレードを他の利用者に割り当てる場合，前の利用者の設定，資産を消去して初期状態に戻す必要があるため，環境構築サービスのオプションとしてキッティングサービスを提供している。

3.2 従来環境からの移行

移行設計・支援サービスでは，利用者が使用していた通常PCから，クライアントブレードにアプリケーションプログラムの設定，ファイルなどのデータの移行を円滑に行うことを支援する（図4参照）。

データだけの移行については，ネットワーク上に共用フォルダを置き，それを介して必要なデータを手作業で，それまで利用していたPCからクライアントブレードにコピーするなどの方法で簡便に行うことができる。

これに対し，デスクトップなどのユーザー環境，各種アプリケーションの設定を移行するには，マイクロソフト社や他のソフトウェアベンダーが提供するユーティリティプログラムを利用するなどの対応が必要である。また，移行する対象（設定ファイル，レジストリ情報など）を特定し，ユーティリティプログラムに指定することも必要となる。移行設計・支援サービスは，これらのユーティリティプログラムの利用方法に関するコンサルテーション，ガイダンスを行い，利用者の従来の環境設定とデータの移行を円滑に行えるように支援するものである。

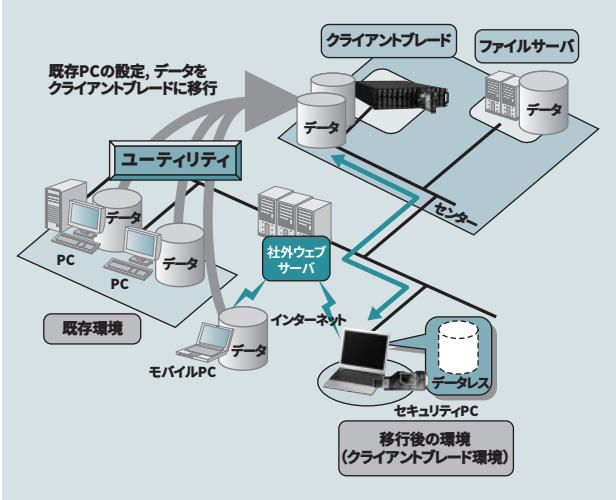


図4 移行設計・支援サービス
利用者が，従来の環境設定とデータの移行を円滑に行えるように支援する。

4. 運用・保守ソリューション

4.1 アプリケーションの配布とアップグレード

クライアントブレードに搭載するアプリケーションの管理に関しては，通常のオフィスに分散されているファットクライアントと同様である。すなわち，個々のクライアントブレードに「JP1/NETM/DM Client」を導入することで，同ソフトウェアによるアプリケーション配布や管理が可能となる。このソリューションでは，JP1/NETM/DM以外にマイクロソフト社が提供するWindowsアップデート環境などに対応している。

セキュリティPCに組み込まれているプログラムについても，同様にJP1/NETM/DMによるプログラムの修正が可能である。ただし，セキュリティPCについてはセキュリティ維持の観点から，内蔵プログラムをみだりに修正することができてはならない。このため，日立製作所が作成したアップデート以外は配布・適用が排除されるようになっている。

4.2 バックアップ

クライアントブレードは，センターに集中配置されることが一般的であり，利用者が直接触れることはできない。また，セキュリティPCはCD-Rドライブ，USB（Universal Serial Bus）メモリなどの接続を抑止している。このため，手もとに置いたPCのように利用者自身でクライアント上のデータをバックアップすることが難しくなる。そこで，クライアントブレード内蔵のハードディスクの障害に備えて，ディスク全体もしくは指定したフォルダ，ファイル単位でのバックアップをセンターで取得する仕組みを実装し，運用を設計するサービスを提供している。また，

SCS導入を機に，ファイルサーバなどのファイル共用の仕組みを構築し，バックアップすべき業務情報はサーバ上で管理する運用に切り替えることができる。そのためのファイルサーバや情報ポータルの設計・構築のサービスも関連ソリューションとして提供している。

4.3 ウイルス感染対策

セキュリティPCは，組込み専用のWindows XP Embeddedを使用していること，OSのファイアウォール機能を有効としてあるなど，ウイルス感染に対しても対策が講じられている。また，仮にウイルスに感染した場合でも，電源をオフすることで出荷状態に初期化されるため，感染した状態が継続することはない。

クライアントブレードに関しては，一般のPC同様にワクチンソフトのインストールなどにより，対策を行うことになる。

PCがウイルスに感染した場合に「LAN（Local Area Network）からの接続を絶ち隔離する。」といったセキュリティポリシーを運用する場合は，さらに進んだ対応が必要となる。この水準に対応するソリューションとして，汚染拡大防止機能を持ったソフトウェアや，そのソフトウェアがサポートするネットワーク機器を用いたソリューションが用意されている。このソリューションにより，ウイルスに感染したクライアントブレードをネットワークから自動的に切断することが可能となる（図5参照）。

5．おわりに

ここでは，クライアントブレード型セキュアクライアントソリューション，およびその周辺ソリューションについて述べた。

ここで述べたサービスは，従来のPCでは利用者が直接行っていたことを，利用者が触れることのできないサーバルームの集中管理環境の下で実現するため，その代替策が中心となっている。

他方，SCSは，従来のファットクライアントではなかった，端末の無個性性（個々のセキュリティPCには利用者に依存する情報が格納されないことによる，利用者とセキュリティPCとの関係の解消），ユビキタス性（「KeyMobile」を挿入すればどのセキュリティPCからでも自分の環境が利用可能），証明書を格納した認証デバイスによる成り済ましの防止など，さまざまな特長を持っている。

日立グループは，SCSの特長を応用してクライアントブレード上で動作するアプリケーションとの連携を図ることにより，セキュリティの高さと利便性を両立させたソリューションの開発・提供に取り組んでいく考えである。

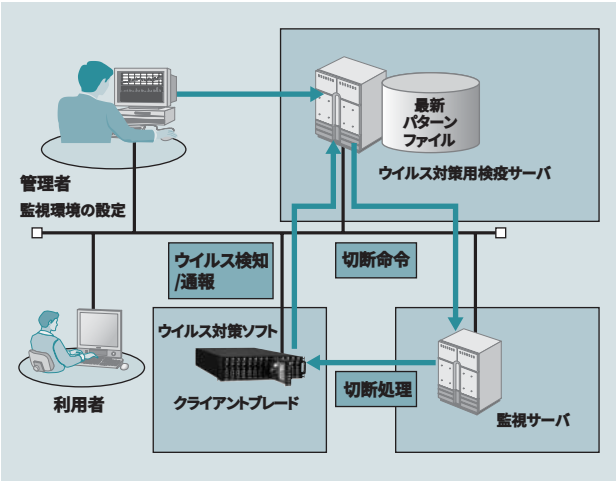


図5　ウイルス感染対策
ウイルス感染を検知し，感染したクライアントブレードを自動的にネットワークから切断する。

執筆者紹介

高原 清
1991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，プラットフォームを中心としたソリューションの事業企画に従事
情報処理学会会員

黒川 浩一
2002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　BPS開発部　所属
現在，ベストプラクティススイーツ・サービスの企画，開発に従事

米山 英彦
1999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の企画に従事

白勢 則之
1988年株式会社日立情報システムズ入社，産業情報サービス事業部　産業インフラサービス本部　所属
現在，ベストプラクティススイーツ・サービスの開発に従事