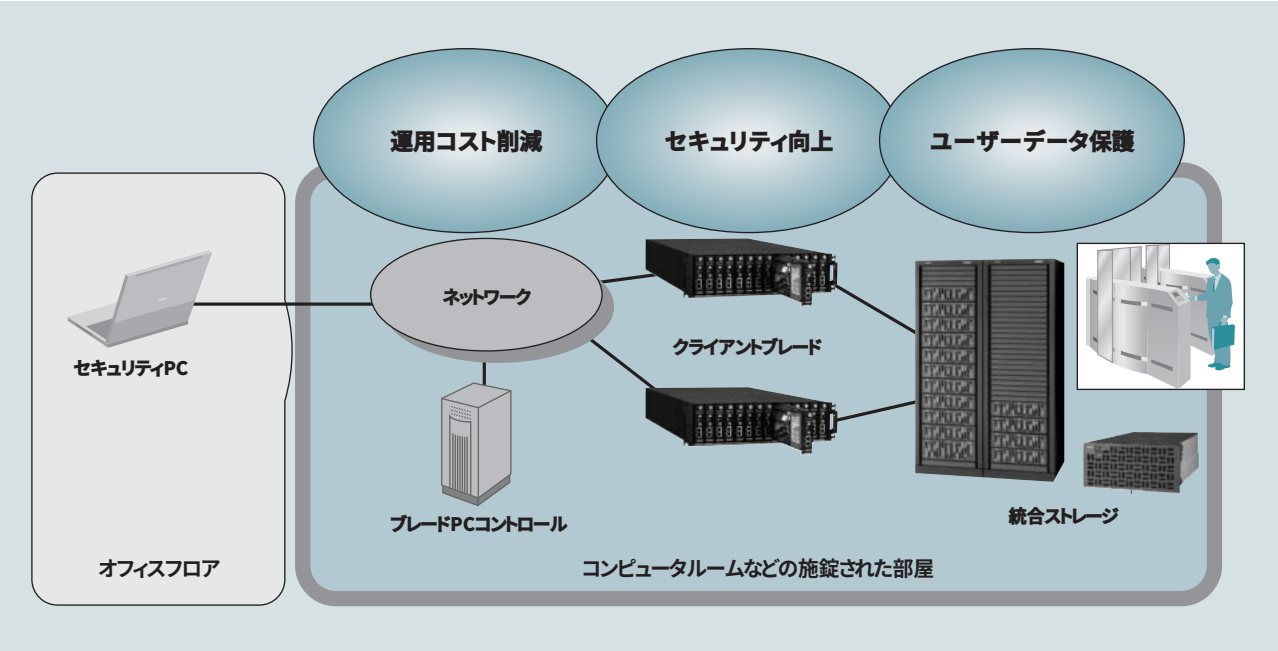
高度なセキュリティとTCO削減を両立する「ポイント・ブレード型セキュアクライアントソリューション」

Point to Blade Type Secure Client Solution with Higher Security and Lower TCO

八高 克志 Katsushi Yakô
中山 淳 Jun Nakayama
土谷 時博 Tokihiro Tsuchiya
白銀 哲也 Tetsuya Shirogane



注:略語説明 PC(Personal Computer)

図1 「ポイント・ブレード型セキュアクライアントソリューション」の概要

ポイント・ブレード型セキュアクライアントソリューションはオフィスのセキュリティを強化するとともに，ユーザーデータの保護，運用の合理化によるTCO(Total Cost of Ownership)の削減を可能にする。

1. はじめに

「セキュアクライアントソリューション」におけるセキュリティ確保の基本方針をひと言で表すと，情報を手もとに「持たない」，「出さない」ことである。

実際には，これに加えて本人認証による成り済まし防止とVPN(Virtual Private Network)による通信秘匿(とく)によって，画面出力や，キーボード，マウス操作をもセキュアに行うが，電子データの永続的方法での持ち出しにおける「持たない」，「出さない」は，HDD(Hard Disk Drive)などの記憶媒体を持たず，USB(Universal Serial Bus)メモリなどの外部媒体接続を制限したセキュリティPC(Personal Computer)によって実現されている。

モバイル環境においてはセキュリティPCを導入することで十分なセキュリティを確保することができるが，クライアントPCをこれまでどおりオフィスに設置していたのではオフィスフロアのセキュリティを確保したことにはならない。オフィスフロアにも高度なセキュリティを確保するためには，オフィスフロアでも「持たない」，「出さない」を実現する必要がある。

オフィスフロアにおける「持たない」，「出さない」を，クライアントPCの本来の目的である利便性を極力損なうことなく実現するのが「ポイント・ブレード型セキュアクライアントソリューション」である(図1参照)。

セキュリティ確保のためであってもコストを抑えることは重要であり，ポイント・ブレード型は運用コストを削減する効果がある。また，これまで見過ごされがちであったクライアントPC内に残されたユーザーデータをストレージメディア障害から保護することもできる。

ここでは，高度なセキュリティと運用コストの削減を両立する「ポイント・ブレード型セキュアクライアントソリューション」について述べる。

**「ポイント・ブレード型セキュアクライアントソリューション」は，クライアントPCの機能を
クライアントブレードという形で厳格な入退室管理を行っている
コンピュータルームなどの空間に集約することにより，オフィスフロアにおいても
情報を手もとに「持たない」，「出さない」を実現し，オフィスフロアからの情報漏えいを根本的に対策するソリューションである。
また，これまで見過ごされていたクライアントPCの内部ストレージ内に格納されていたユーザーデータを
ストレージメディア障害から保護し，保守・運用の合理化によってコスト削減を可能にした。**

2．オフィスフロアのセキュリティ

セキュリティPCによる「持たない」，「出さない」を実現すれば情報セキュリティは万全であると言うためには，「HDDなどの記憶メディアを持つクライアントPC本体の設置されている場所は安全である」という前提を設ける必要がある。例えば，モバイル環境のセキュリティを向上する目的でセキュリティPCを導入し，オフィスフロアにクライアントPC本体を設置していた場合は，オフィスが安全であると言えなければならない。これは，モバイル利用の有無にかかわらず，「オフィスフロアのセキュリティが万全であるか」という問題に帰着する（**図2**参照）。

オフィスフロアはカードキーなどで施錠されていたとしても，訪問客や取引先業者などの出入りなどがあるため，部外者の職場フロアへの侵入を十分に抑止できているとは言いがたい。つまり，オフィスフロアは侵入者に対して，それほど安全な空間ではないということになる。

問題点は侵入者によるもの以外にもある。オフィスフロアにクライアントPCの本体が設置されているということは，組織内の人間であれば本人でも，他人でもクライアントPCに物理的にアクセスできる。このため，クライアントPC本体の持ち出しやUSBメモリ，DVD-Rなどの可搬媒体などを介して情報が漏えいする危険性は残される。情報セキュリティ保全の内部教育を徹底したとしても，たった一人のモラルを欠いた職員がいただけでセキュリティシステム全体が崩壊してしまうというやっかいな問題である。組織内の人間の不正行為による情報漏えい事件があとを絶たないことからも，オフィスフロアにクライアントPCを設置することはセキュリティ上の重大な問題である。

また，USBメモリなどの大容量の可搬電子媒体が容易に利用できてしまうことは特に注意しなければならない。モラルを欠いた職員だけでなく，侵入者によってでも情報を簡単に，しかも大量に持ち出されてしまうのである。その情報量は個人情報であれば全顧客情報に匹敵し，営業情報，製品技術情報であれば企業の状況を完全に把握できるものとなる。

これらの問題を抜本的に解決するのがポイント・ブレード型セキュアクライアントソリューションである。ポイント・ブレード型は，クライアントPCの機能を持つクライアントブレードを厳格な入退室管理しているコンピュータルームなどの施錠した空間に集約し，これをモバイル環境の場合と同様にセキュリティPCを用いてオフィスフロアからアクセスする。これによって，オフィスフロアにおいても「持たない」，「出さない」を実現するのである。

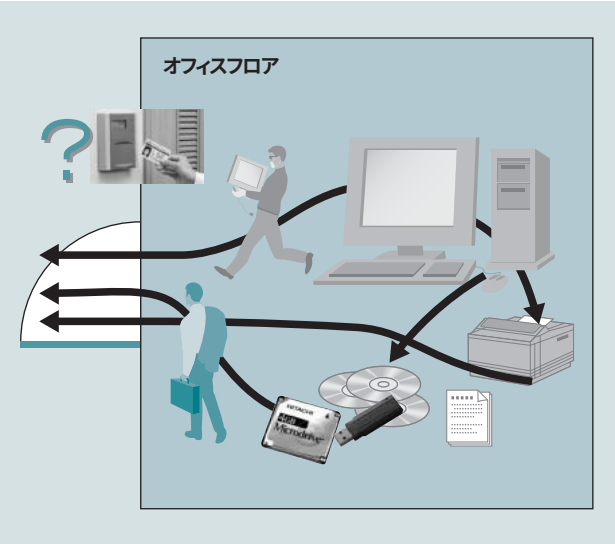


図2　オフィスフロアからの情報漏えいの形態イメージ
クライアントPCの本体が設置されたオフィスフロアからは，さまざまな形態で情報の持ち出しが可能である。

3．メディア障害からのユーザーデータ保護

情報漏えい防止ではないが，広い意味でのセキュリティ対策であるユーザーデータの保護も重要である。

クライアントPCのローカルストレージには受信メール，作成途中や非公式な業務データ，オフィススイートのカスタマイズやウェブブラウザのブックマークに代表されるユーザー個別の設定情報など，さまざまなデータが保存されている。

これらはすべて業務データであり，ローカルストレージのメディア障害でこれらを消失した場合には，データ再作成の人件費，データを再作成するまでのビジネス機会の喪失，および再作成できなかったデータ価値の損失による重大な損害を被ることは明らかである。米国Survey.comの調査によると，HDD故障による損失額は1回のHDD故障あたり15,000ドルにもなるという。

しかし，業務データをファイルサーバに格納していないことを理由に，責任を被害者に転嫁しやすく，システム管理部門の投資動機になりにくいことから，ローカルストレージ内のユーザーデータの保護はこれまで見過ごされてきた。また，エンドユーザーがそれぞれバックアップ運用を行おうとしても事情はそれほど簡単ではない。DVD-Rなどの可搬ディスク媒体の容量拡大が目覚ましいとはいえ，HDDとの容量格差は一向に縮まる様子はない。また，テープドライブもオフィスフロアで普及していないことから，クライアントPCにおけるバックアップ運用は一般化していない。

一般に，ストレージのメディア障害に対する冗長化手法としてはRAID（Redundant Array of Independent Disks）が知られている。RAIDストレージは複数のHDDを利用するため，大容量ストレージに適している。また，サーバ系OS（Operating System）や，専用のRAIDコントローラを必要とすることから高価になる傾向にある。このため，主にサーバ向けのストレージとして普及してきたが，クライアントPC1台のローカルストレージの代替えとしてはオーバースペックでかつ高価であり，ほとんど利用されてこなかった。

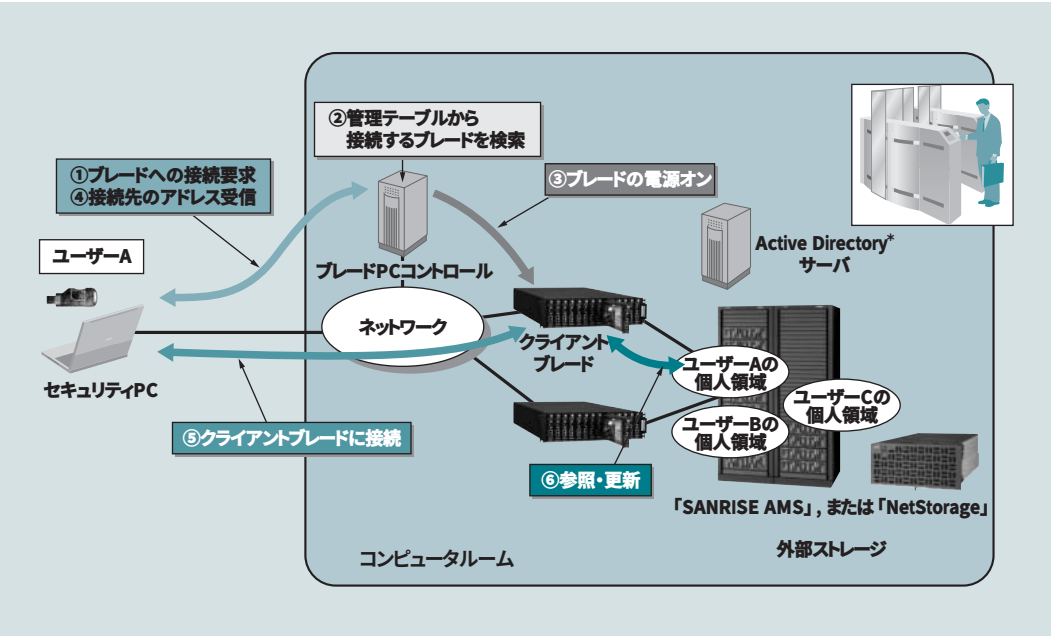
3.1 統合ストレージソリューション

ポイント・ブレード型ではオプションとして統合ストレージソリューションを提供している（**図3**参照）。これは大規模なRAIDストレージを複数の小規模な仮想ストレージに分割し，それぞれを各ユーザー専用のストレージとして割り当てるという形態で共有するものである。それぞれの仮想ストレージには「マイドキュメント」や「デスクトップ」といったフォルダ内のユーザーデータやアプリケーションのカスタマイズ情報および，ウェブブラウザのブックマークといったユーザー個別の設定情報が自動的に格納され，保護される。これによって，従来は事実上サーバ用途に限定されていたRAIDストレージのメリットをクライアント環境で享受することが可能になった。なお，ポイント・ブレード型ではクライアントブレードをコンピュータルームに集約できるため，ストレージアクセスによるトラフィックをコンピュータルーム内のネットワークに局所化し，オフィス内LAN（Local Area Network）のトラフィック増加を防ぐことができる。この点でも，統合ストレージソリューションはポイント・ブレード型ならではのソリューションといえる。

この統合ストレージソリューションには，コストパフォーマンスに優れる「SANRISE Adaptable Modular Storage（AMS）」が最適であり，普及化したIP（Internet Protocol）技術のうえに成り立つIP-SAN（Storage Area Network）プロトコルの一つであるiSCSIを実装している。これによってRAID5や，対メディア障害性を強化したRAID6，予備ディスクを用いた自動再冗長化機能のほか，「SANRISEシリーズ」が持つ高度な機能を高速かつ低コストで利用できるのが特徴である。

同じように普及化したNAS（Network Attached Storage）技術を用いたアプライアンスファイルサーバ「HA8000-ie/NetStorage」を外部ストレージとすることで，いっそう手軽に統合ストレージソリューションを実現することもできる。

なお，いずれのストレージも，IP技術のうえに構築されている。クライアントブレードにはギガビットLANインタフェースを二つ実装しているので，統合ストレージソリューションに有利である。一方のLANインタフェースをセキュアクライアントソリューションにおいて安定したレスポンスを要求する画面出力や，キーボード・マウス入力を担う「JP1/NETM/DM」や，ウェブ，メールなどといった従来からあるLANのトラフィックに用い，他方を統合ストレージソリューションにおけるストレージアクセスのトラ



＊Active Directoryは，米国Microsoft Corporationの米国およびその他の国における登録商標または商標である。

図3　統合ストレージソリューションの概要
「マイドキュメント」，「デスクトップ」などのユーザーデータ用フォルダ，アプリケーションのカスタマイズ情報，ウェブブラウザのブックマークなどの個人別設定情報を自動的に外部ストレージに格納して統合する。

フィックに用いることで，ストレスなくセキュリティPCを利用することが可能である。

4. 保守・運用コストの削減

セキュリティレベルの向上のためであっても，保守・運用コストが上昇することは避けなければならないが，ポイント・ブレード型はクライアントPCの保守・運用コストを削減することが可能になる。

4.1 運用シーン別の保守・運用コスト削減効果

運用シーン別にした，ポイント・ブレード型の保守・運用コスト削減効果は以下のとおりである。

(1) ユーザーによるクライアントの日常運用

ユーザーの日常運用に関しては，クライアントブレードと通常のクライアントPCとではほとんど差異がない。クライアントブレードはオフィスの自席からネットワーク経由で利用するが，電源投入・遮断，OSハングアップ時のリセットも自席から行う機能を備えている。退勤時などにユーザーから個別に電源を切ることができるため，環境にもやさしいシステムと言える。

(2) ユーザーへのクライアントの初期割当運用

ユーザーにクライアントを新たに割り当てる場合，資産管理情報を作成したうえでユーザーに引き渡すこととなる。

ポイント・ブレード型では，ブレードPCコントロールサーバのGUI(Graphical User Interface)などからユーザーにクライアントブレードを割り当てることができる(**図4**参照)。

各セキュリティPCはユーザー認証情報を元にブレードPCコントロールサーバに問い合わせを行い，割り当てられたクライアントブレードのIPアドレスを取得して自動的に接続する(**図5**参照)。

ブレードPCコントロールサーバはデータベース管理システムを内蔵し，資産管理機能を備えているので，ユーザーへのクライアントブレード割当で入力したデータはそのまま資産管理情報の一部として一元管理される。

(3) クライアント環境の共有運用

出張の多い部署や，交代勤務を実施している職場では，クライアント環境の稼動率が低く，投資効果が低いことが問題となる。利用するアプリケーションがユーザー間で共通の場合には，原理的にはクライアント環境を共有化し，時間貸しで利用することにより，同時利用ユーザー数分にコストを適正化できる。ただし，この場合もセキュリティについての考慮は必要である。

ポイント・ブレード型では動的割当機能でこの問題に対処している。動的割当機能では，利用要求のあるユーザーに未使用中の任意のクライアントブレードを1台割り当て，利用が終了した時点で開放する。ここで，ユーザーに対するクライアントブレードの割り当てを制御しているのもブレードPCコントロールサーバである。

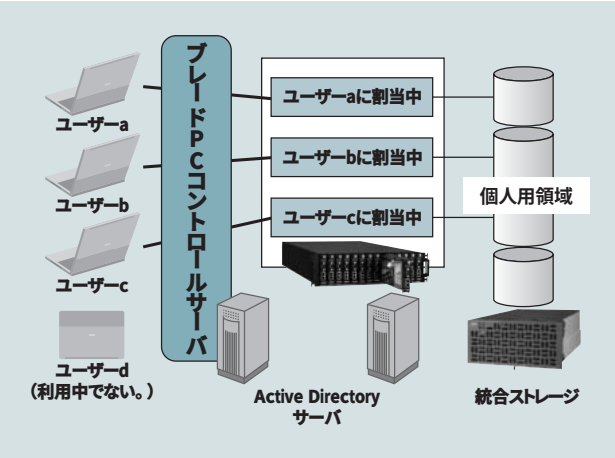


図4　クライアントブレードの動的割当機能
動的割当機能により，クライアントブレードの数を同時利用ユーザー数に適正化することができる。

注:略語説明　GUI(Graphical User Interface)

図5　ブレードPCコントロールサーバのGUIの画面例
この画面からクライアントブレードの割り当てや，電源の集中管理，コールランプの制御，状態の取得などを行う。

ユーザーは毎回異なるクライアントブレードを利用することになり，各クライアントブレードからセキュリティを保ったままでユーザーデータにアクセスするために，前述した統合ストレージソリューションを利用する。なお，動的割当によるコスト削減効果は統合ストレージソリューションの導入コストを考慮する必要がある。

(4) クライアントブレード集中電源制御

電源設備メンテナンスや年末年始などの電源停止時には，クライアント環境の安全のため，事前にクライアントPCをシャットダウンしておく必要がある。また，緊急セキュリティアップデー

トの適用のために夜間に一斉に電源を投入するという利用シーンも考えられる。

ポイント・ブレード型ではブレードPCコントロールサーバのGUIから複数台のクライアントブレードのシャットダウン,電源の投入,強制遮断または,リセットが可能である。

(5) クライアントブレード障害運用

クライアントブレードに障害が発生した場合,まず,ユーザーの業務を再開することが重要となる。ポイント・ブレード型では,代替機割当機能により,システム管理部門のオペレータの介在なしに,代替となるクライアントブレードを割り当てることが可能となる。そのため,エンドユーザーは迅速に業務を再開することが可能となり,ビジネス機会の喪失を最小限にできる。また,情報システム部門では,障害発生ごとにコンピュータルームに駆けつけてメンテナンスを行う必要がなくなることから,計画的にメンテナンス作業を行うことができるというメリットもある。これによってオペレータは生産的な仕事にいっそう長く時間を割くことが可能となり,また,常駐するオペレータの人数を削減することができれば保守・運用費の大幅な削減にもつながる。

次に行うことは,障害クライアントブレードの状態確認である。クライアントブレードは自らの状態を監視しており,障害を検知すると状態ランプを点灯する。

また,このランプの状態は,ネットワークを介してリモートで確認することができるため,システム管理担当者はこの時点で自席から離れる必要はない。

クライアントブレードに障害が確定した場合,または詳細な調査が必要な場合には,ユーザー名などの情報からクライアントブレードを特定して現場で直接保守作業を行うことになる。この際,リモートで該当クライアントブレードのコールランプを点灯または点滅することができるため,高度に集約したクライアントブレードにおいて,現場での対象個体の特定が容易である。

代替機割当機能はブレードPCコントロールサーバの機能であり,セキュリティPCから操作する。また,状態ランプの確認,コールランプの制御はブレードPCコントロールのGUIから行うことができる。

(6) ユーザーデータのバックアップ運用

統合ストレージソリューションにより,RAIDを適用したストレージメディア障害の対応が可能になった。しかし,ユーザー操作ミスやOS障害からのユーザーデータの保護を目的に,別途バックアップ運用を考えることも推測される。バックアップ運用をストレージ側で一括して行えることも統合ストレージソリューションのメリットである。

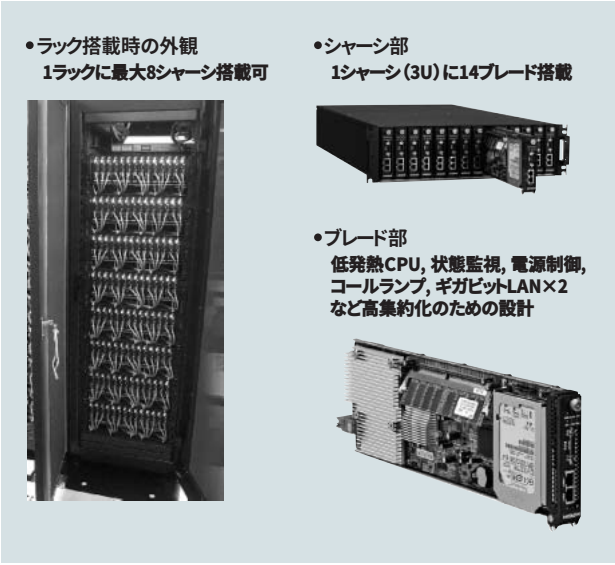
4.2 クライアントブレードの設置形態

クライアントブレードの運用形態として,各オフィスにラックを設置する方法,拠点ごとのコンピュータルームに集約する方法,複数拠点で統一のコンピュータセンターに集約する方法などが考えられる。

コンピュータルームに拠点ごとのクライアントブレードを集約する運用形態では,ハードウェアのメンテナンスにおいて,システム管理部門の担当者がエンドユーザーのオフィスを訪問する必要はない。ファームウェアのアップデートが必要となる場合などで多数のクライアントに対して一律に作業を行う場合などは効果が顕著な例である。また,空調管理されたコンピュータルームに集約することで,クライアントPCの故障率の低下も期待できる。

サテライトオフィスに代表される小さな拠点を多数持つ企業の場合は一つの拠点のコンピュータルームに複数拠点のクライアントブレードを集約し,各拠点から広域LANを介してセキュリティPCからアクセスする方法がある。これにより,システム管理部門の保守・運用のための出張や,障害が発生したクライアントブレードの運搬費が不要になるため,保守・運用コストを大幅に削減できる。

ここで述べたクライアントブレードのコンピュータルームへの集約は,クライアントブレードの高密度実装によるものである。高さ3 Uサイズ(約133.5 mm)のシャーシに最大14台,1ラックでは最大112台の「FLORA bd100」を搭載することができる(図6参照)。また,モバイル用のCPU(Central Processing Unit)を採用することで,OA(Office Automation)利用におけるパフォーマンスを維持しながら集約することにより,発生する熱の問題を解決した。



注:略語説明 CPU(Central Processing Unit),LAN(Local Area Network)

図6 クライアントブレード「FLORA bd100」
ポイント・ブレード型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ブレードはさまざまな特徴を持っている。

5. おわりに

ここでは，オフィスフロアのセキュリティ向上，ユーザーデータの保護，保守・運用コストの削減を実現する「ポイント・ブレード型セキュアクライアントソリューション」について述べた。

セキュリティの観点から，クライアント環境における記憶媒体と計算リソースはコンピュータルームに集約する形態が，将来的にも理想形であると推測されている。

日立製作所は，今後も，コンピュータルームにクライアントPCが集約しているというポイント・ブレード型の特徴を生かした付加価値のあるソリューションのバリエーションを充実させていく考えである。

参考文献など

1）BUSINESS WIRE，
http://www.businesswire.com/webbox/bw.031201/210710133.htm

2）**小槍山，外：ユビキタス時代の安心・安全・快適を実現するセキュアクライアントソリューション，日立評論，87，**5，595〜600（2005.7）

執筆者紹介

八高 克志
1995年日立製作所入社，情報・通信グループ ソフトウェア事業部 先端ミドルウェア開発部 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
情報処理学会会員

中山 淳
1989年日立製作所入社，情報・通信グループ ソフトウェア事業部 第2プラットフォームソフトウェア設計部 所属
現在，ブレードPCコントロール for FLORA bd100の開発に従事

土谷 時博
1989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 第3サーバ開発本部 第1部 所属
現在，NASおよび関連ソリューション開発に従事

白銀 哲也
1997年日立製作所入社，情報・通信グループ RAIDシステム事業部 開発本部 システム第3設計部 所属
現在，SANRISEのiSCSIエンハンス機能開発に従事
博士（工学）
情報処理学会会員