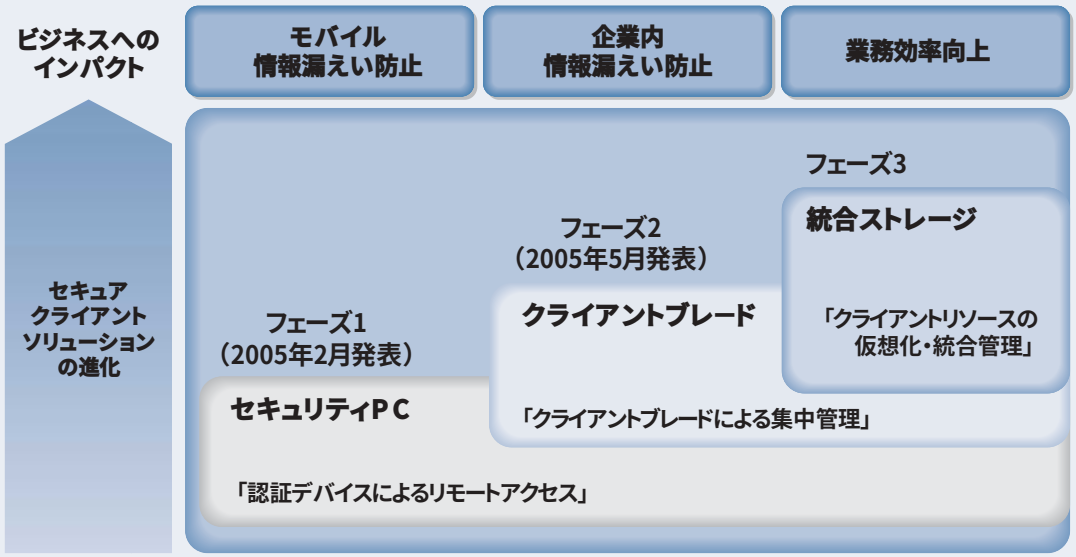
Vol.87 No.7 595

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

Secure Client Solutions for Providing Safety and Comfortable Work Style in Ubiquitous Era

■小檜山智久 *Tomohisa Kohiyama*　■丸 山 隆 史 *Takashi Maruyama*



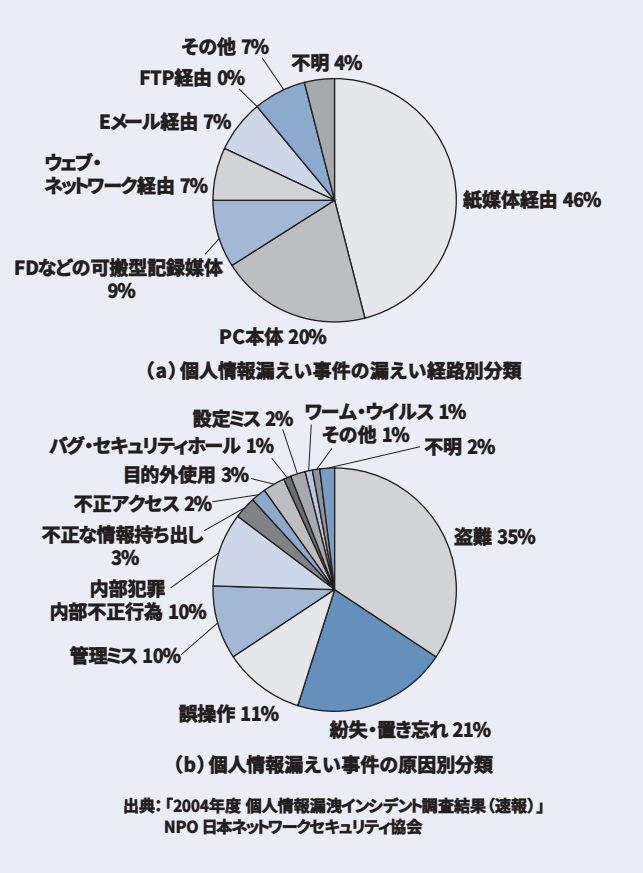
日立製作所が進めるセキュア クライアント ソリューションのロードマップ　セキュア クライアント ソリューションにより，情報漏えい対策と快適なビジネス環境を実現する。マイグレーションパスを設けることにより，いつでも最新のソリューションの利用が可能である。

近年，パソコンやUSB接続メモリなどの可搬型記憶媒体の盗難や置き忘れにより，その中に格納されていた企業情報が漏えいするという事故が多発し，社会問題化している。日立製作所は，経営トップ主導のプロジェクト体制で情報セキュリティの抜本的対策の決め手となるセキュア クライアント ソリューションを開発，社内に適用してきた。認証デバイスと連携して動作し，HDDを搭載しないセキュリティPC，集約装置・管理可能なクライアントブレードなどの特徴的なコンポーネントにより，これまで情報の保護が十分でなかったクライアントPC環境の情報漏えい防止と，安全で快適なビジネス環境の実現を目指していく。

1 はじめに

1980年のOECD（経済協力開発機構）勧告「プライバシーの保護と個人データの国際流通についてのガイドラインに関する理事会勧告」を契機として，各国でプライバシー保護に関する法制化が進んできた。わが国でも2005年4月から個人情報保護法が完全施行され，企業の情報セキュリティ対策は待ったなしの状況にある。同法は2003年5月に成立し，国や自治体に対応した基本法の部分が即日施行された。今回はこれに加え，個人情報取り扱い事業者の義務や罰則を規定した一般法の部分が施行された。

社会的背景としては，企業情報漏えい事故の多発がある（**図1**参照）。原因として盗難，置き忘れ，内部犯罪，情報持ち出しの比率が増加している。PC（Personal Computer）内蔵のHDD（Hard Disk Drive）や，USB（Universal Serial Bus）接続メモリなどの可搬型記録媒体からの漏えいが全体の四分の一を占めていることから，悪意のない企業人が簡単に加害者になってしまう実態がわかる。このため，通常のPC利用形態が情報漏えい防止の観点では不十分で，普通に使っていても情報漏えいを起こさない新しい仕組みが求められている。この仕組みが確立していない現時点では，PC持ち出しや社外利用を禁止する企業も多く，本来はユーザーの利便性を向上させる目的で開発された情報機器のメリットを損なう結果となっている。このように，安全性と利便性を両立させるという課題に対し，多くの企業は決め手を欠いているのが現状である。また，経営者の観点では，たとえ不可抗力な原因によるものであっても，通常の業務を遂行中に従業員が情報漏えいの当事者にならない



注:略語説明　FTP(File Transfer Protocol)

図1　個人情報漏えい事例の経路別と原因別分類
盗難，置き忘れ，内部犯罪，情報持ち出しなどによりPC本体や可搬型記憶媒体経由で漏えいする事例が多いことに着目した。

ようにする仕組みを提供することは重要である。さらに，内部犯罪に関しても十分な抑止力となるソリューションが求められている。いったん情報が漏えいすると，会社の社会的信用の失墜や補償・対策費用の支出など，経営へのダメージは深刻なものとなる。実際，2004年度の情報漏えい事故366件の平均想定損害賠償額は13.9億円と報告されており[1]，加えて，会社が受けるであろう社会的な打撃の影響を考えると，原理的に情報漏えいしない抜本的な防止対策が切望されていると言える。

ここでは，このような情報漏えいを未然に防ぐ，日立製作所のセキュア クライアント ソリューションの考え方と，その取り組みについて述べる。

2 日立製作所の情報セキュリティ対策への取り組み

情報漏えいを防止するための各種のソリューションは，従来から実用に供されてきた。PC自体の盗難を防ぐワイヤによるロックといった物理的なものから，PCや可搬型記憶媒体に暗号化やアクセス制限をするためにパスワードロックをかけるもの，ICカードやUSBキーのようなハードウェアの鍵デバイスを併用するもの，ネットワークをモニタして非登録PCのネットワーク接続を排除するものなど，各種の方式がある。

日立製作所でも，これまで，万一に備えた情報漏えい防止策を実施してきた。上述のPCの盗難や紛失に対する対策を例にすれば，PCのモバイル利用時にはHDDにパスワードロックをかけ，さらに，ファイルを自動的に暗号化するソフトウェアの導入を義務付けるなどの施策の実施である。しかし，たとえパスワードや暗号化で保護されていても，盗難や紛失でデータの実体が流出すれば，情報漏れがないと断言できないことも事実である。そのため，日立製作所は，2004年7月に盗難，紛失・置き忘れ，不正な情報持ち出しの原因となるPC本体や可搬型記憶媒体からの情報漏えい防止に対する抜本的な対策の仕組みを作るため，経営トップ主導による社内プロジェクトを発足させた。そして，このプロジェクトで作り上げたシステムを直ちに社内に適用し，待ったなしの社内情報セキュリティ対策に取り組んだ。また，実際に運用することでノウハウと実績を蓄積し，これをソリューションとして提供することで，顧客の利に資すると考え，これを実現するシステムを「セキュア クライアント ソリューション」と呼んでいる。

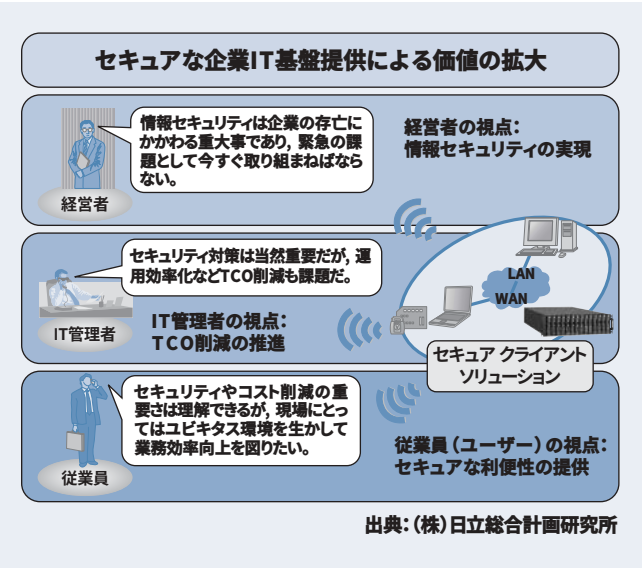
このプロジェクトでは，2004年12月に試行システムを完成させ，開発に直接関係した部署の従業員を中心に100人規模の試行を開始した。さらに，2004年度に情報・通信グループのモバイルユーザー2,000人に導入を済ませ，2005年度前半で，直ちに対策が必要なモバイルユーザーへの導入を完了させる。引き続きイントラネット内の低リスク部分についても年間8,000人以上のユーザーへの計画的な導入を進めていく。社内展開時の意見や要望は，逐次製品にフィードバックしている。通信カード利用時のレスポンス改善や，電波状態が悪いときの再接続機能の強化など，ユーザーになって初めてわかる改善項目を，開発チームみずからが体感して改良している。

このプロジェクトの目的は，抜本的な情報漏えい対策の実現である。しかし，単にそれだけにとどまらず，管理の集中化による運用・管理コストの削減も目指している。情報・通信グループの情報システム部門の計画では，運用人員に関しては3年後に30%削減を，その他の効果として，ユーザーの作業工数削減や，稼動状況の可視化によるPC台数削減も図る。

3 「どこでもMyDeskPC」コンセプトとセキュア クライアント ソリューション

3.1 ワークスタイルを変える

ここ数年で，われわれを取り巻くブロードバンド環境は



注：略語説明　TCO（Total Cost of Ownership），LAN（Local Area Network）
WAN（Wide Area Network）

図2　セキュア クライアント ソリューションが目指すもの
経営者，IT管理者，従業員，それぞれの立場のニーズに応えるのがセキュア クライアント ソリューションである。

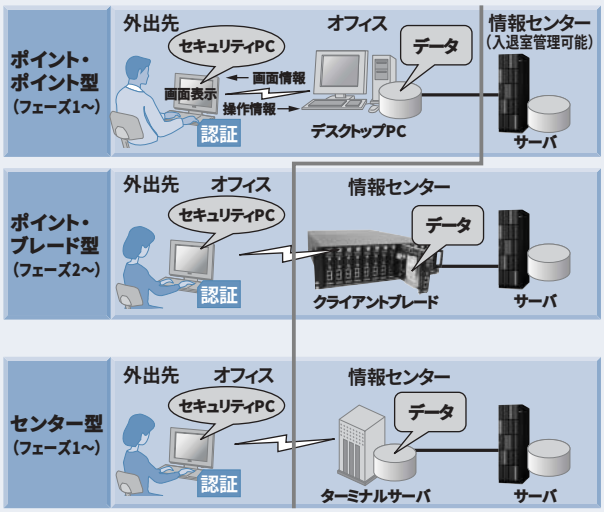


図3　セキュア クライアント ソリューションのシステム接続形態
ポイント・ポイント型では既設のPCにリモートアクセスする。ポイント・ブレード型は既設PCをクライアントブレードで集約したもの，センター型ではサーバによるターミナルサービスを行う。

大幅に進展した。ホテルや空港ではインターネット接続サービスが利用でき，駅や店舗をスポットとする無線LAN（Local Area Network）のアクセス拠点も増えつつある。第3世代の携帯電話インフラストラクチャーを使ったデータ通信も実用的なレベルで商用化されている。CATVやADSL（Asymmetric Digital Subscriber Line），光ファイバなどを使った高速通信を契約している家庭も増加している。このような環境を背景に，ノートPCや可搬型記憶媒体に情報を入れて持ち歩いていた情報携帯型に代わり，従来はLANを前提として発展してきたシンクライアント型の，情報を持ち歩かない利用形態がブロードバンド通信環境の発展に合わせて実用的になってきた。これがユビキタス時代のワークスタイルの主流になると考える。

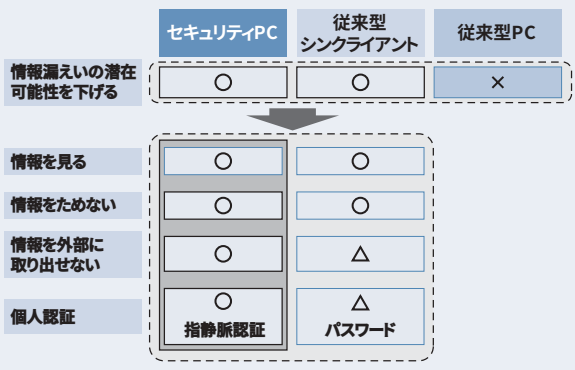
日立製作所が目指すシステムは，経営者の視点から考えた情報セキュリティ，IT管理者の視点から考えたTCO（Total Cost of Ownership）の削減，そしてユーザーである従業員の視点から考えたセキュアな利便性という3本柱を，さらによい形で実現しようとするものである（**図2**参照）。情報セキュリティは，情報を手もとにコピーして持ち歩けないようにすることと，認証デバイスによる成り済ましのリスク極小化で達成することができる。

情報を持ち歩かなければ失くすこともないというのが基本的な考え方である。TCOの削減では，従来分散していたクライアントPC環境を集中管理することで管理コストの削減を図る。また，オフィスだけでなくモバイル機器の利用も視野に入れた運用モデルを考え，そのために必要な特徴ある製品のラインアップを用意することで，どこでも支障なく通常業務が行え，かつ情報が手もとに残らない仕組みを構築してセキュアな利便性を達成する。

セキュア クライアント ソリューションには幾つかのシステム接続形態がある（**図3**参照）。いずれの形態でも，データやアプリケーションが動作する情報処理装置の実体はオフィスや情報センター側にある。セキュリティPCはHDDを内蔵していない端末で，キーボードやディスプレイとして機能する。

セキュリティPCとその他のクライアントの機能を比較したものを**図4**に示す。セキュリティPCの特徴は，PC本体には情報を蓄積したり，外部に取り出したりできないようにしたことと，ユーザー認証機能を強化したことである。

手もとの端末にHDDなどストレージ機能が備わっている場合，盗難や紛失などの事故にあったときに，ストレージ内に大事な情報がなかったことを証明するのは困難である。現在ではソフトウェアでHDDやUSB接続メモリなど



注：記号説明　○（適合），△（やや適合），×（不適合）

図4　セキュリティPCと一般PCの機能比較
セキュリティPCでは，装置の基本機能として，情報をデータとして取り出せないようにした。

の入出力デバイスの機能を制限する方法もあるものの，使用者がそのソフトウェアを導入して確実に運用していたかどうかを証明する手段が確立していなかったからである。

この課題を解決するため，セキュリティPCではHDDのような書き込めるストレージを排除した。装置の基本仕様として，装置内部に情報が蓄積されることはなく，一般の可搬型記憶媒体を接続してもデータを書き込めないようにしてあるので，データを外部に取り出すこともできない。これにより、たとえ盗難・紛失事故が起きても，セキュリティPCからの情報漏えいは起こらなかったと言えるようにしている。

図3でセキュリティPCの横にあるのがユーザー認証に使う認証デバイスで，接続情報や電子証明書など，情報アクセスに必要な鍵情報が安全に格納されている。つまり，この認証デバイスは鍵束の安全な格納容器と言える。鍵束を使えるようにするためには，パスワード照合を行う。例えば，不正利用者が規定回数連続してパスワード入力をまちがえると，認証デバイスは銀行のICカードのようにみずから閉そくして使えなくしてしまう。管理者の許可を得ない限り，ユーザーはこの閉そくを解除できない仕組みである。このため，万が一，認証デバイスを紛失したときも，銀行のICカード並みに成り済まし防止の安全性が確保できる。なお，現在のパスワード照合による方式では，まだ成り済ましの可能性を完全に排除できないので，バイオメトリクス（生体認証）とのコンビネーションを実現し，ユーザーの確認から本人の確認へと，認証の確からしさを強化していく予定である。

公衆のインターネット環境を使って通信しても，当事者以外から傍受されないようにする仕組みがVPN（Virtual Private Network）による暗号通信である。一般に，社外からのアクセスはVPNによる暗号通信で行う。暗号通信路を確立するための電子証明書は，認証デバイスに格納してある。暗号通信路を流れるのはキーボードやマウスの操作情報，オフィスや情報センターのPCで作られた画面の画像情報であって，ファイルのデータ自体は移動しない。このようにして今いる場所が自分のデスクになり，いつでも安心・安全・快適に自分のPC環境を使えるようになる。

以上がセキュア クライアント ソリューションの上位のコンセプト，「どこでもMyDeskPC」である。数年前から，この利便性に主眼を置いたコンセプトに基づくシステムを研究所で試作，実運用し，今回のセキュリティに主眼を置いたセキュア クライアント ソリューションシステムの礎とした。

セキュア クライアント ソリューションの類型について以下に述べる。

3.2 ポイント・ポイント型

オフィスや情報センターに設置してあるPCに，ネットワーク経由でキーボードやマウスなどの入力情報を送り，PCで処理した後の表示画面を画像情報として手もとの端末に表示するものをポイント・ポイント型のリモートアクセスと呼ぶ。この型の代表的なものにマイクロソフト社のWindows XP Professional※1)に同梱（こん）されている“Remote Desktop”がある。これには，手軽にリモートアクセスを実現できるという特徴があるものの，特定のOS（Operating System）上だけのサポートに限られているという課題がある。この課題を解決するために，日立製作所は，独自のリモートアクセス通信制御ソフトウェアを開発した。オフィスや情報センターにあるPCとユーザーの手もとにあるセキュリティPCとのやり取りは，安全性を高めるために非公開の通信プロトコルによって行う。さらに，VPNソフトウェアも独自開発のものを用意し，日立製作所として保証できるシステムを構築している。

もちろん日立製作所製VPNの代わりに，他のVPNを使用することも可能である。

3.3 ポイント・ブレード型

従来の情報システムのセキュリティレベルを向上させるときは，現在使用しているクライアントPC環境を，段階的にリフォームできることが望ましい。

現在使っているPCをセキュリティPCによって安全にリモートアクセスするポイント・ポイント型を第1段階とすれば，第2段階は，クライアントPCの情報処理・保管機能を集約して，厳格な入退室管理が可能な情報センターでデータベースサーバなどと同等のセキュリティレベルで集中管理する形態になると考える。これをポイント・ブレード型と呼ぶ。

このソリューション開発のフェーズ1では，モバイル環境における手もとのユーザー端末からの情報漏えい防止に焦点を合わせた（25ページの図参照）。フェーズ2では，企業内情報セキュリティへの対応強化に主眼を置いている。これは**図1**における内部犯罪のポテンシャルを下げるものである。このモデルでは，ポイント・ポイント型モデルにおける社内のPCをブレード型のPCで置き換え，情報センターのマシン室のような管理された場所で集中管理を行うことで，いっそう高いレベルで企業内の情報漏えい防止を図る。このためのキーコンポーネントがクライアントブレードである（**図5**参照）。これはPCの情報処理・保管機能を1枚のブレード（刃）状のパッケージに実装したもので，今回のものは3 U（U=44.45 mm）というサイズのシャシに14台分を実装することができる。これを19型ラッ

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

クに収めることで，100台以上のPCをフルラックに集約することが可能である。また，通常のPCと同様に，ユーザーは電源のオンオフや再起動をリモートで行うことができる。これまでオフィスや出先に散在していたPCを情報センターのマシン室などに集約することによって，メンテナンス性や管理性を向上させることができる。また，信頼性の高いストレージにより，クライアントのデータを守る，ストレージ統合というフェーズ3へのマイグレーションを考慮したハードウェアアーキテクチャとしている。

フェーズ2では，併せてユーザー端末側のセキュリティPCのラインアップを拡充し，社内利用形態に合わせた最適なセキュリティPCの利用ができるようにする考えである。

3.4 センター型

ポイント・ポイント型のリモートアクセスのほかに，マイクロソフト社のWindows Server 2003などのターミナルサービスや，シトリックス社のMetaFrame※2)などのいわゆるSBC(Server Based Computing)によるリモートアクセスがある。この形式のものを「センター型」のリモートアクセスと呼ぶ。センター型でも，セキュリティPCと認証デバイスによって，いっそうの情報漏えい防止強化を図ることができる。

3.5 アウトソーシングサービス

その他，セキュア クライアント ソリューションでは，指静脈認証によるセキュリティの強化，IP(Internet Protocol)電話機能のサポート，そしてアウトソーシング サービスの提供を行っていく。

セキュア クライアント アウトソーシング サービスの概要を**図6**に示す。導入や運用にかかる顧客の費用を平準化し，煩わしい運用管理を効率化できるようにすることが目的である。セキュア クライアント ライフサイクル サポート，すなわち導入・保守・移設・破棄にかかるプロセスのサポートから，情報センターの運用管理などをアウトソーシングでサービスしていく(**図6**参照)。

このようなサービスには，日立製作所社内のIT部門の運用ノウハウが生かされている。例えば認証デバイスを用いて運用する場合，従業員のデータベースなどとリンクした，その企業の認証システムと連携した発行運用管理が必要になる。初期の発行処理，発行済み証明書の失効処理，認証デバイスを自宅などに忘れて出社したときの一時認証デバイスの発行処理，紛失に伴う再発行処理，現在の使用状態の棚卸し処理といった発行運用管理などが必要である。これまでは，このような発行運用管理システムを構築しようとすると，認証デバイスのベンダーから開発キットを購入して自分で構築する必要があった。一方，実用的な認証デバイスの発行運用管理には長年の運用ノウハウが必要なことが多く，開発キットだけの提供では不十分であるといった課題があった。日立製作所は，社員証として5年間以上のICカード運用実績があり，今回の認証デバイスの発行運用管理システムは，そのようなノウハウをベースに構築したものである。

4 おわりに

ここでは，日立製作所のセキュア クライアント ソリューションについて述べた。

※2) 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または商標である。

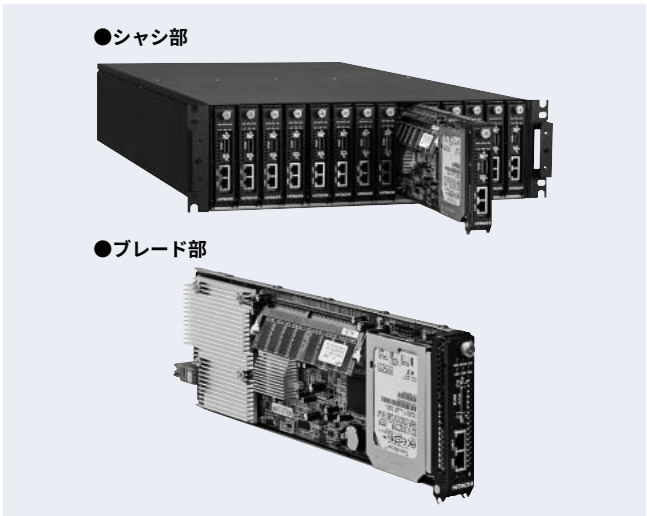
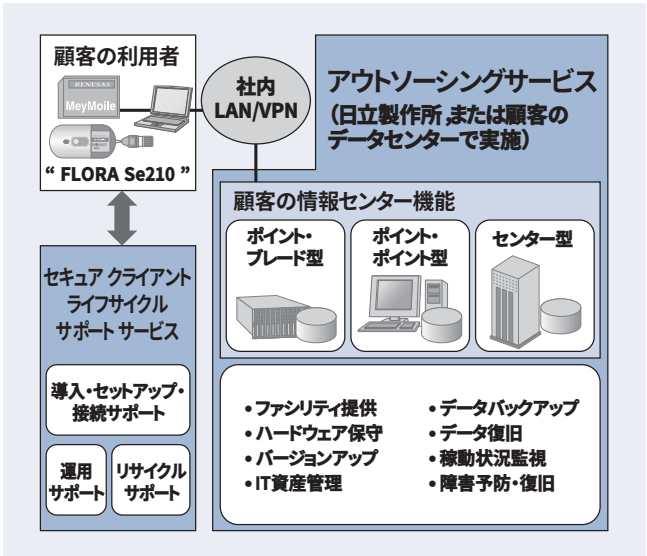
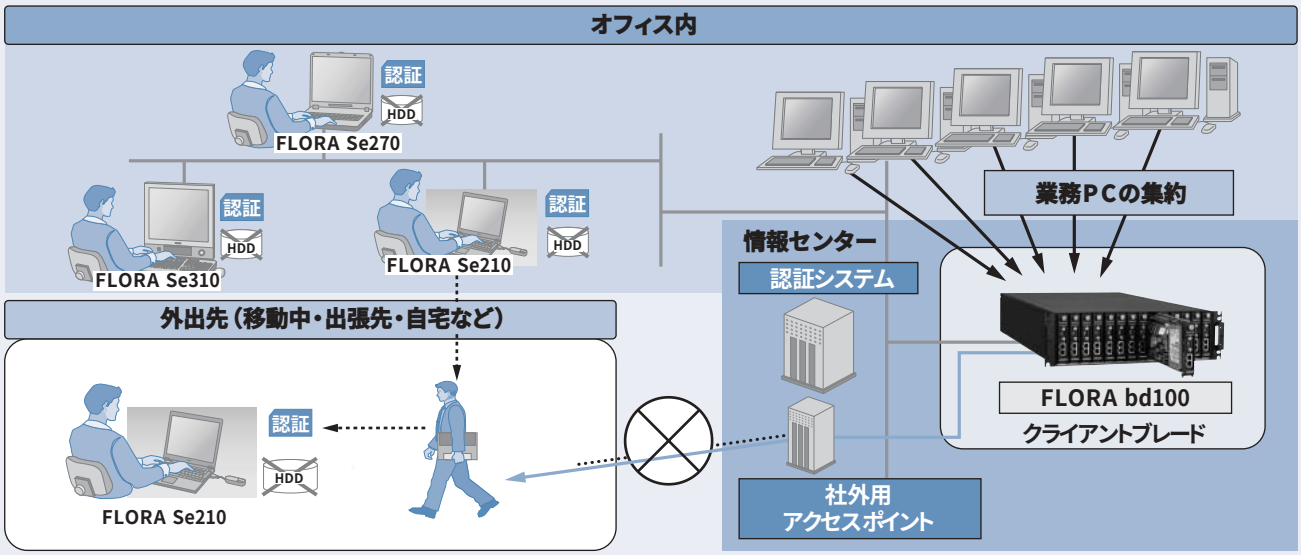


図5 クライアントブレード“FLORA bd100”の外観
社内のPCをクライアントブレードに集約し，厳格な入退室管理が行える情報センターなどで集中管理できるようにする。



注:略語説明 VPN(Virtual Private Network)

図6 セキュア クライアント アウトソーシング サービスの概要
顧客の導入・運用費用の平準化と，煩わしい運用管理の効率化を図る。



注：略語説明　HDD（Hard Disk Drive）

図7｜**「ポイント・ブレード型」の利用モデル**
ブレードPC“FLORA bd100”に業務PCの機能を集約し，さまざまなセキュリティPCによって企業内情報セキュリティを確保する。

このソリューションの開発プロジェクトを進めるにあたり，「安心を簡単に」というスローガンを掲げた。セキュリティレベルを上げる一方，そのために使い勝手が損なわれてはならないという意識で取り組むためである。

企業情報システムを情報漏えいから守っていくためには，策定したセキュリティポリシーに従った総合的な対策が必要である。コンポーネントの一つであるセキュリティPCを導入しても，安全になるわけではない。総合的なセキュアな企業情報システムを構築するために，日立製作所は，セキュリティコンサルティングをはじめとしたソリューション群を提供している。今回は，手もとで使用する端末から情報が漏れないクライアント環境の仕組みをセキュアクライアント ソリューションとして構築した（**図7**参照）。それは，従来のものを組み合わせただけでは情報が漏えいしないことの証拠を残す仕組みを構築できないと考えたからである。

日立製作所は，セキュア クライアント ソリューションにより，今後も，セキュアかつ利便性の高いワーキングスタイルの普及を目指していく考えである。

参考文献

1）NPO 日本ネットワークセキュリティ協会「2004年度個人情報漏洩インシデント調査結果（速報）」
2）NPO 日本ネットワークセキュリティ協会「2003年度情報セキュリティインシデントに関する調査報告書」
3）総務省「情報通信白書」平成16年版

執筆者紹介

小檜山智久

1984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 セキュア ユビキタス ソリューションセンタ 所属
現在，セキュア クライアント ソリューションの事業・製品企画に従事
電気学会会員，電子情報通信学会会員，情報処理学会会員，映像情報メディア学会会員
E-mail:tomohisa.kohiyama.ma@hitachi.com

丸 山 隆 史

1975年日立製作所入社，情報・通信グループ 情報システム本部 情報セキュリティ部 所属
現在，セキュリティPC，クライアントブレードなど，各種セキュリティ施策の社内展開に従事
E-mail:takashi.maruyama.qt@hitachi.com