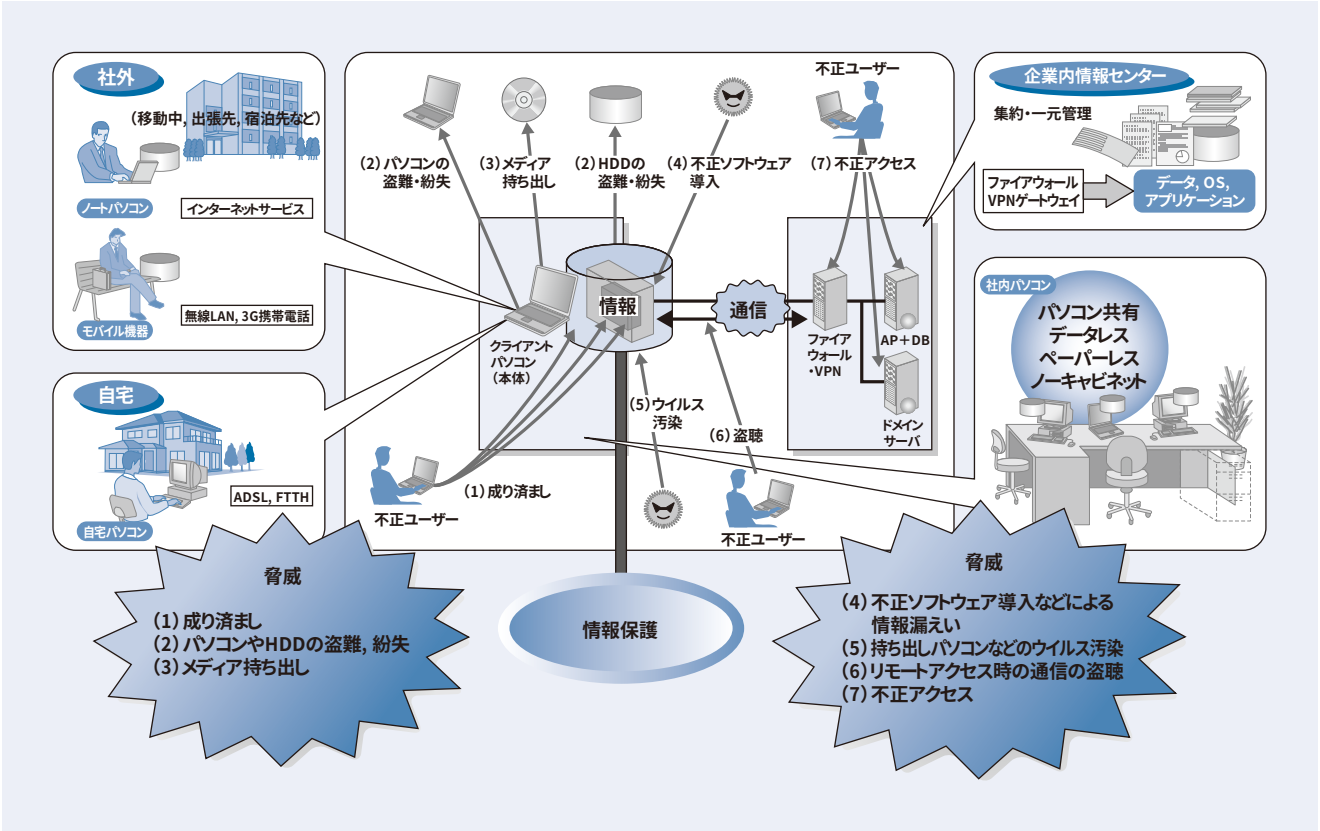
ユビキタス情報社会を支えるセキュリティソリューション

Security Solutions for Supporting Ubiquitous Information Society

北田賢司 *Kenji Kitada*　長谷川大造 *Daizô Hasegawa*　川飛達夫 *Tatsuo Kawatobi*
金野千里 *Chisato Konno*　富山朋哉 *Tomochika Tomiyama*



注:略語説明　HDD(Hard Disc Drive), VPN(Virtual Private Network), AP(Access Point), DB(Database), OS(Operating System), LAN(Local Area Network), 3G(3rd Generation), ADSL(Asymmetric Digital Subscriber Line), FTTH(Fiber to the Home)

ユビキタスアクセスにおける脅威の全体イメージ

モバイルパソコンの普及を背景としたブロードバンドインターネットの高度利用により，ユビキタス情報社会に向けて社会基盤の整備が進んできている。一方，ユビキタスアクセスがいっそう一般的になるにしたがい，データの漏えいの経路も複雑かつ多岐に広がりつつある。

近年，パソコンの利用形態の多様化やネットワーク環境の充実に伴い，業務のユビキタス化が進んでいる。また，それとともにパソコンの盗難・紛失，成り済まし，通信路での盗聴，情報漏えいなど，さまざまな脅威が大きくなってきている。一方，個人情報保護法の施行により，企業の個人情報の取り扱いでは，入手方法や管理義務，利用制限，開示要求への対応などの義務が生じている。組織にとって業務効率を向上する目的で進められてきたIT化で，個人情報をはじめとする情報漏えいは，組織の存続自体に脅威を及ぼす時代となってきている。

日立グループは，このような脅威に対処しつつ，安全なユビキタスアクセス環境を実現するためのソリューションを提案する。

1 はじめに

ブロードバンドの普及，パソコンの性能向上，大容量の二次記憶媒体の出現など，IT(Information Technology)環境の発展に伴い，インターネットサービスの高度化や業務形態のモバイル化などが進展してきた。この急激な変化の一方で，パソコンの盗難・紛失，成り済まし，通信路での盗聴，情報漏え

いなど，セキュリティ面での脅威が大きくクローズアップされてきている。

ユビキタスアクセスを組織で実現するためには，業務フロー，およびそこに内在する脅威の明確化，現有システム資産との親和性，要求されるセキュリティレベル，構築期間・稼動開始期限，費用といったさまざまな要件を考慮した適切なソリューションが求められる。

ここでは，ユビキタス情報社会を支える日立グループのセキュリティソリューションと，ネットワーク・ITシステムの先にあるユビキタス情報社会に対応するセキュリティパソコンをはじめとする次期システムへの取り組みについて述べる。

2 企業情報システムを取り巻く状況

2.1 ブロードバンド，モバイル時代のセキュリティの課題

1950年代に始まった企業のITシステムは，時代とともに，TSS（Time Sharing System），CSS（Client-Server System），さらにパソコンサーバへとネットワークの形態を変えてきた。しかし，1990年代の後半，インターネットの民間利用が急速に普及するに至り，企業のネットワークもこの影響を受けることになった。これらオープンネットワークやモバイル機器の利用形態が，以下のようなセキュリティ上のさまざまな問題を引き起こす要因となってきた。

（1）セキュリティホール（セキュリティ上の欠陥）による侵入，改ざんの脅威
（2）ウイルス汚染の脅威
（3）従業員によるデータの持ち出しなどの脅威
（4）モバイルパソコン，メディアの紛失や盗難などの事故

今後，ブロードバンド，モバイルがさらに進化し，新たなユビキタスワークスタイルの普及が進むと考えられる。そして，今，新たなユビキタス時代に即したセキュリティが求められている。

2.2 法制度と標準化の動向

政府は，社会基盤としてITシステムとインターネットの重要性が増大してきたことや，インターネットなどの普及による事件・事故が多数発生している状況を受け，不正アクセス禁止法，個人情報保護法，e-文書法など，法律面の整備を着実に進めている。また，情報システムの全般を運用管理する基準であるISMS（Information Security Management System）とその適合性評価制度や，個人情報保護に関するコンプライアンスプログラムの要求事項とその認定制度などが整えられ，認定を取得する企業も増加している。特に，企業にとっては，個人情報保護法の遵守が緊急の課題となっている。

3 トータル セキュリティ ソリューション“Secureplaza”[1)]

3.1 日立製作所のセキュリティソリューション“Secureplaza”

Secureplazaでは，セキュリティ対策のさまざまな要求に応えるため，二つの体系を用意している。その一つが，顧客のシステムやサービスの広がりに即して対策するステップ別ソリューションであり，もう一つが顧客のセキュリティ対策の目的に合わせてパッケージ化した目的別ソリューションである。

ステップ別ソリューションの体系は九つのステップに分類されている。一方，既存の目的別ソリューションは，以下の六つのソリューションから成る。

（1）コンサルテーションサービズ“Secureplaza/CS”
（2）ヘルスケアサービズ“Secureplaza/HS”
（3）アイデンティティマネジメント“Secureplaza/IM”
（4）トラステッドゾーン“Secureplaza/TZ”
（5）リークガード“Secureplaza/LG”
（6）ポリューションブロッグ“Secureplaza/PB”

現在は，最近の法制度の整備と，ユビキタスワークスタイルに対応する新たなセキュリティの実現への要求が高まっている。日立グループは，新たな目的別ソリューション，ユビキタスセキュリティ“Secureplaza/US”によって，これらのニーズに応えていく考えである。

3.2 ユビキタスセキュリティ“Secureplaza/US”

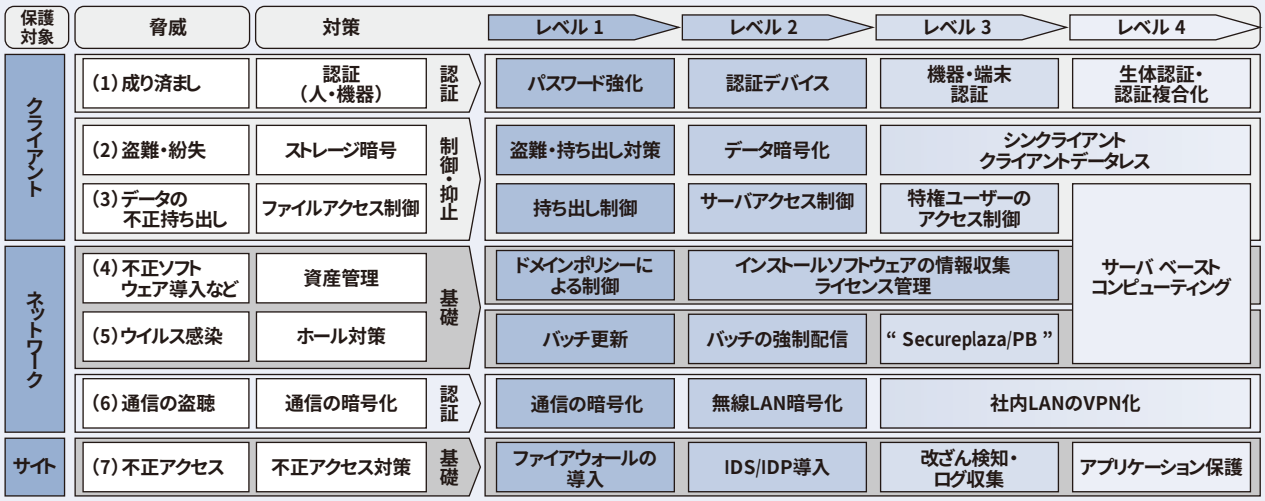
ユビキタスアクセスでは，社外へ持ち出されるクライアントパソコンやネットワークを介して接続されるサイトに，（1）成り済まし，（2）盗難・紛失，（3）データの不正持ち出し，（4）不正ソフトウェア導入，（5）ウイルス感染，（6）通信の盗聴，（7）不正アクセスなどのさまざまな脅威が存在する。これらについての対策の全体像を**図1**に示す。

脅威への対策の要点は，以下の3点である。

（1）認証：アクセス者個人とアクセス端末の確実な認証
（2）通信路保護：安全な（暗号化）通信環境の実現
（3）アクセス制御：データやドキュメントなど，コンテンツへのアクセス制御の実現

しかし，それぞれの脅威に，どのレベルの対策を実施するかは，（1）業務フロー，およびそこに内在する脅威の大きさ，（2）現有システム資産との親和性，（3）要求されるセキュリティレベル，（4）構築期間・実現期限，（5）トータルコストなど，顧客のさまざまな条件によって異なってくる。Secureplaza/USでは，対策のレベルをセキュリティの強度に応じて，レベル1からレベル4までの4段階に分類している。このため，顧客の要件に適切なソリューションを提案することできる。

Secureplaza/USでは，認証技術を支えるIC付きメモリカード“KeyMobile”や，通信路暗号化を実現するVPN（Virtual



注：略語説明　LAN(Local Area Network)，VPN(Virtual Private Network)，IDS(Intrusion Detection System)，IDP(Intrusion Detection and Prevention System)

図1 ユビキタスアクセスにおけるさまざまな脅威と対策

縦軸にユビキタスアクセスにおける保護対象，横軸に想定される脅威とセキュリティレベル分けした対策の一覧を示す。

Private Network)，ファイル暗号，シンクライアントを実現するセキュリティパソコン，ブレードパソコン，サーバ ベースト コンピューティング(サーバ集中管理型)を実現する“Meta Frame”など，それぞれのレベルを実現する商品体系をそろえている。

3.3 ユビキタスセキュリティの実現

ユビキタスアクセスに対する脅威への対策ステップを図2に示す。

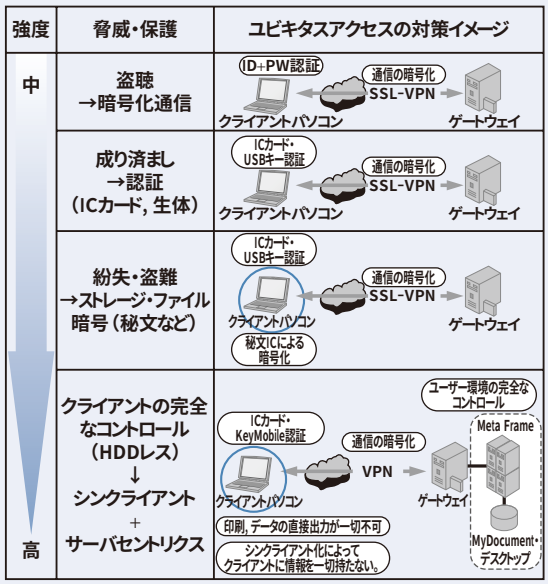
ユビキタスアクセスでは，まず，通信路でやり取りされるデータの盗聴を抑止する必要があり，それを実現するのがVPNである。次いで，外部からのアクセス者の成り済ましを抑止するために，確実な認証を実現するのが，ICカードや生体認証などである。また，外部に持ち出されたクライアントパソコンの紛失や盗難時に，その中のデータを保護するのがファイルの暗号化である。さらに，クライアントパソコン上のデータを保護する究極の形態として，サーバ ベースト コンピューティングの構成がある。これは，クライアントパソコンにはデータをダウンロードせず，処理やデータ管理はすべてサーバサイドで行い，クライアントパソコンを表示とキー入力デバイスとしてだけ利用する形態である。ただし，この形態の実現には，クライアントパソコンだけでなく，アプリケーションシステムの移行などが必要となる。

4 “Secureplaza/US”を構成する最新の商品群

今後のユビキタスセキュリティを実現していく先行的な商品群について以下に述べる。

4.1 “KeyMobile”

日立製作所は，ユビキタス情報社会におけるITシステムで重要となる認証デバイスとして，KeyMobileを提供している〔図3(a)参照〕。KeyMobileは，内蔵するICチップにより，ICカードと同様のレベルで安全に証明書と暗号鍵を格納することができる。また，フラッシュメモリを内蔵していることから，メモリにVPNクライアントやメタフレームクライアントなどを格納できるので，KeyMobileを持ち運ぶだけで認証とクライアントソフトウェ



注：略語説明　ID(Identification)，PW(Password)，SSL(Secure Socket Layer)，USB(Universal Serial Bus)，HDD(Hard Disc Drive)

図2 リモートアクセスにおける対策のステップ

図1の対策を，典型的なリモートアクセス環境を想定し，セキュリティの強度に応じて行う対策の例を示す。

アの実行が利用できる環境を実現している。

4.2 指静脈認証装置

本人認証の究極のレベルは生体認証である。

日立製作所は，生体認証技術として指静脈認証装置を開発し，製品化している〔**図3**(b)参照〕。指静脈認証は，目に見えない指静脈を使うため偽造が困難であり，認証精度の高さに加え，本人拒否率が低いという特徴を持っている。また，一指のみであるので装置の小型化が可能で，パソコンのログインだけでなく，入退室管理システム，金融ATMなど広範な応用が実現されている。

4.3 セキュリティパソコン

外部に持ち出されるクライアントパソコンやメディアの紛失，盗難による情報漏えいの対策として，暗号化ツールが一般的には使われている。

これに対して，その抜本的な解決策として，セキュリティパソコンを開発した(**図4**参照)。セキュリティパソコンは，HDD(Hard Disc Drive)を搭載せず，付属のKeyMobileからパソコン リモコン ソフトウェアを起動して，インターネット経由で企業内にあるデスクトップパソコンまたはサーバを利用することができるようにしたものである。これにより，パソコンの利用が避けられない外出先での業務でも，紛失や盗難による情報漏えいのリスクをゼロに近づけることをねらっており，個人情報保護法対応に有効な対策となる。

5 おわりに

ここでは，「いつでも」，「どこでも」，「誰でも」アクセスできるユビキタス情報社会で想定される脅威に対するトータルな対策を実現するユビキタス セキュリティ ソリューション“Secureplaza/US”について述べた。

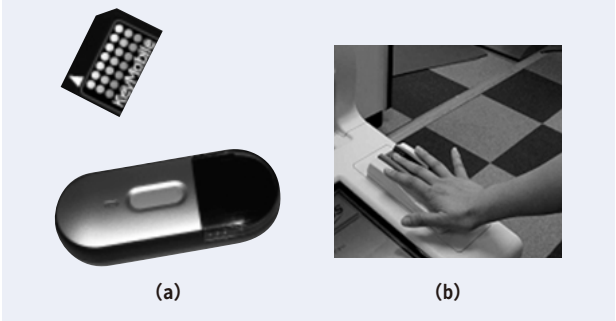


図3 KeyMobileとKeyMobile読み取り装置(a)，指静脈認証装置の外観(b)
認証デバイスであるKeyMobileと生体認証を実現する指静脈認証装置の外観を示す。

図4 HDDレスのセキュリティパソコンの外観
日立製作所のHDDレスパソコンの外観を示す。KeyMobileを認証デバイス兼リモコンソフト格納用のメモリとして使用する。

日立グループは，今後も，「安心・安全」なインターネット社会の発展に寄与するセキュリティソリューションの充実を図っていく考えである。

参考文献など

1) 日立セキュリティソリューション Secureplaza,
http://www.hitachi.co.jp/Prod/comp/Secureplaza/

執筆者紹介

北田賢司
1993年株式会社日立システムアンドサービス入社，ネットワークビジネス本部 ネットワークソリューション部 所属
現在，日立製作所セキュリティソリューション推進本部においてソリューションの企画・拡販などの業務に従事
E-mail：kkitada @ itg. hitachi. co. jp

金野千里
1977年日立製作所入社，情報・通信グループ セキュリティソリューション推進本部 所属
現在，セキュリティソリューションの企画と事業展開に従事
理学博士
情報処理学会会員，日本応用数理学会会員
E-mail：c-konno @ itg. hitachi. co. jp

長谷川大造
1989年日立製作所入社，情報・通信グループ セキュリティソリューション推進本部 所属
現在，セキュリティソリューションの企画と事業展開に従事
E-mail：d-hasegawa @ itg. hitachi. co. jp

富山朋哉
1994年日立製作所入社，情報・通信グループ セキュリティソリューション推進本部 所属
現在，セキュリティソリューションの企画・開発などの業務に従事
E-mail：ttomiya @ itg. hitachi. co. jp

川飛達夫
1970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 ネットワークシステム本部 所属
現在，ネットワークシステムのソリューション開発に従事
E-mail：tkawato @ itg. hitachi. co. jp