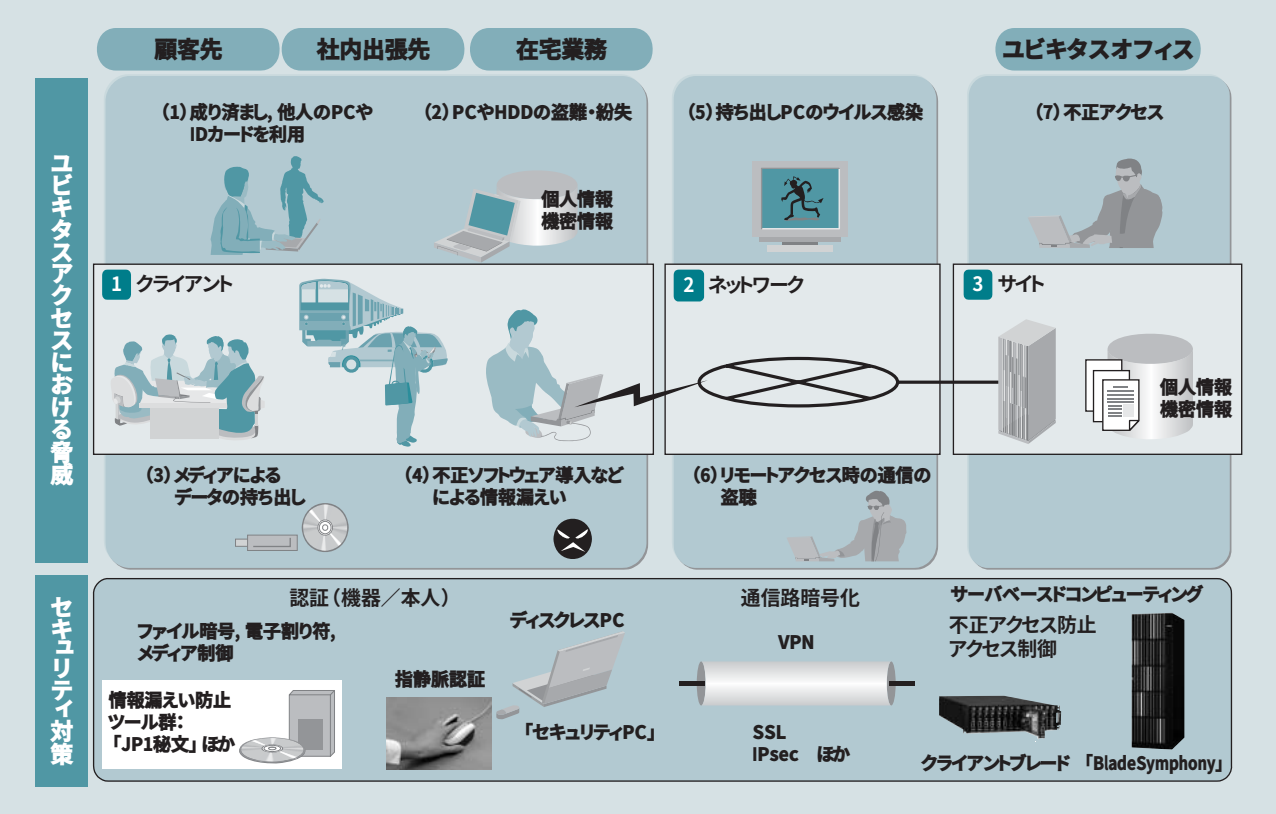
ユビキタスアクセスを実現するトータルセキュリティソリューション

Total Security Solution for Ubiquitous Access Systems Environment

金野 千里 Chisato Konno
田川 豊 Yutaka Tagawa
長谷川 大造 Daizô Hasegawa
永井 康彦 Yasuhiko Nagai



注:略語説明 PC(Personal Computer)，HDD(Hard Disk Drive)，VPN(Virtual Private Network)，SSL(Secure Socket Layer)
IPsec(Security Architecture for Internet Protocol)

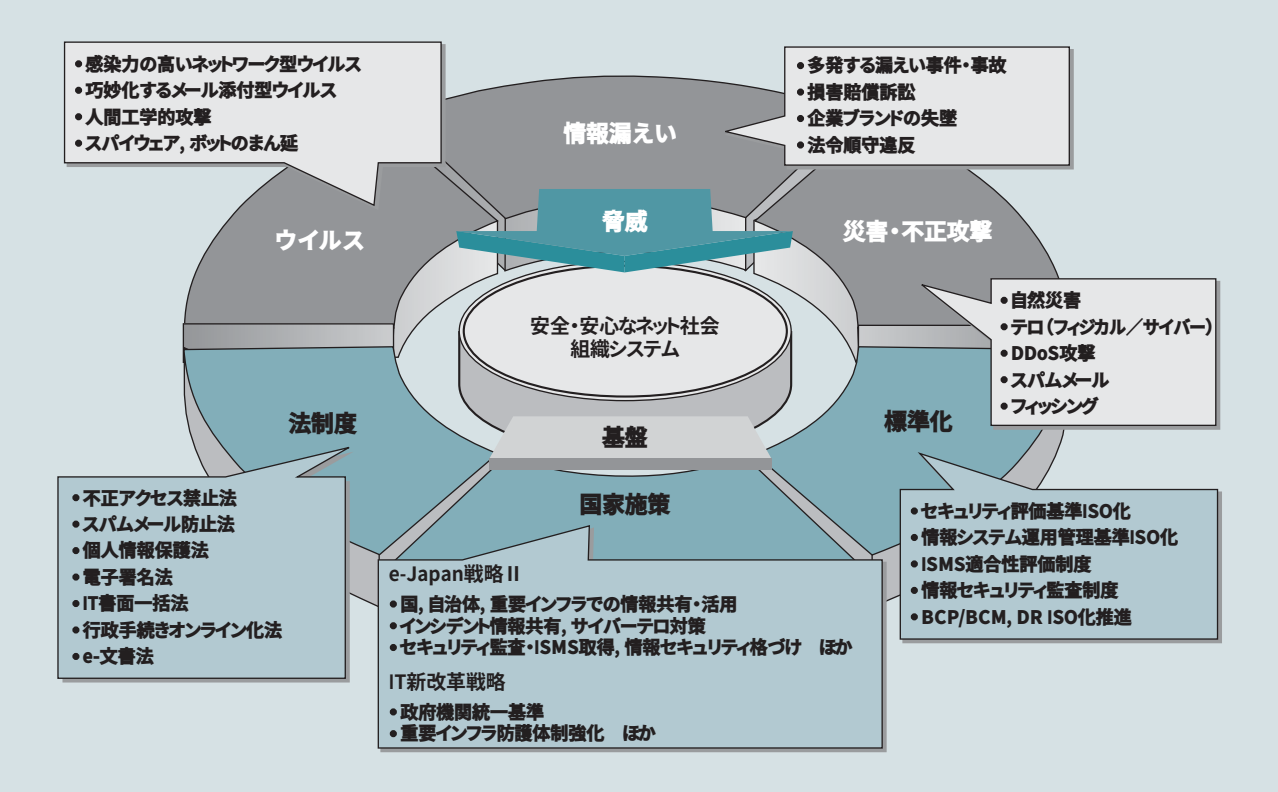
図1 ユビキタスアクセスにおける脅威とセキュリティ対策の全体像
ユビキタスアクセスにおいて，クライアント，ネットワーク，サイトのそれぞれを取り巻く脅威〔(1)～(7)〕と対策の全体像を示している。

ユビキタス化と安全・安心のはざまで

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，近年，オフィスでの業務形態の変化やワークプレイスのユビキタス化が進んでいる。いつでも，どこでも，タイムリーな処理や情報へのアクセスが可能となり，業務のスピードや効率は飛躍的に向上した。このような環境の下，固定の個人デスクを所有しないオフィスも出現している。

こうした急激な変化の一方で，パソコンの盗難・紛失，成り済まし，通信路の盗聴，情報漏えいなど，セキュリティ面での脅威がクローズアップされている(図1参照)。さらに，2005年4月に施行された個人情報保護法の順守をはじめとして，ネット社会における企業の社会的な責任は，ますます大きくなりつつある[1)]。

この両面を踏まえつつ，安全・安心な業務環境を整えて組織の活動を活性化していくことが，組織にとって重要な課題となっている。



注:略語説明　DDoS（Distributed Denial of Service），DR（Disaster Recovery），ISMS（Information Security Management System）
ISO（International Organization for Standardization），BCP/BCM（Business Continuity Plan/Business Continuity Management）

図2　組織システムを取り巻く情報セキュリティ動向の全体像
上半分が脅威群，下半分が基盤群を示している。組織システムはネット犯罪，内部不正，不正攻撃や自然災害などさまざまな脅威にさらされており，セキュリティ対策を支える基盤として法制度，国家施策，標準化などが進められている。

情報セキュリティの動向

安全・安心なネット社会や組織システムを実現するにあたっては，ネット犯罪，内部不正，自然災害などのさまざまな脅威がある。しかも，感染力の強いウイルスや潜在するボット，スパムメールのまん延，フィッシング，さらには，高まる大規模地震の発生確率など，そのレベルは増大している。

一方で，法制度や認証制度の整備，セキュリティ評価の標準化，ネット利用の高度化と安心なインフラ整備をけん引する国家施策などが進められている。これらを基盤として，安全・安心なネット社会と組織システムを実現するのが，情報セキュリティ対策である[1]。その全体像を図2に示す。

日立のトータルセキュリティソリューション「Secureplaza」

現在，そして今後において，求められる情報セキュリティ対策を実現するため，日立グループはセキュリティに対するトータルなソリューション体系「Secureplaza」を提供している。Secureplazaは二つの体系に分けられ，一つは，システムやサービスの広がりに応じて，顕在化する脅威への対策を行うステップ別のソリューションである。もう一つは，さまざまなセキュリティ対策の目的に合わせてパッケージ化した，目的別のソリューションである[2]。

ステップ別のソリューションの体系は，ポリシー，ファイアウォール，VPN（Virtual Private Network），認証システム，不正アクセス監視，コンテンツ監視，統合運用管理，監査・教育，保険などの9ステップから成る。一方の目的別ソリューションは，対策目的やシステム拡張目的に焦点を絞った九つのソリューションから成り，図3に示すように組織全体をカバーしている[2),3),4)]。また，現在のホットな対策や法令順守なども含んでいる。九つのソリューションの概要は，次のとおりである。

（1）Secureplaza/CS（Consultation Service）

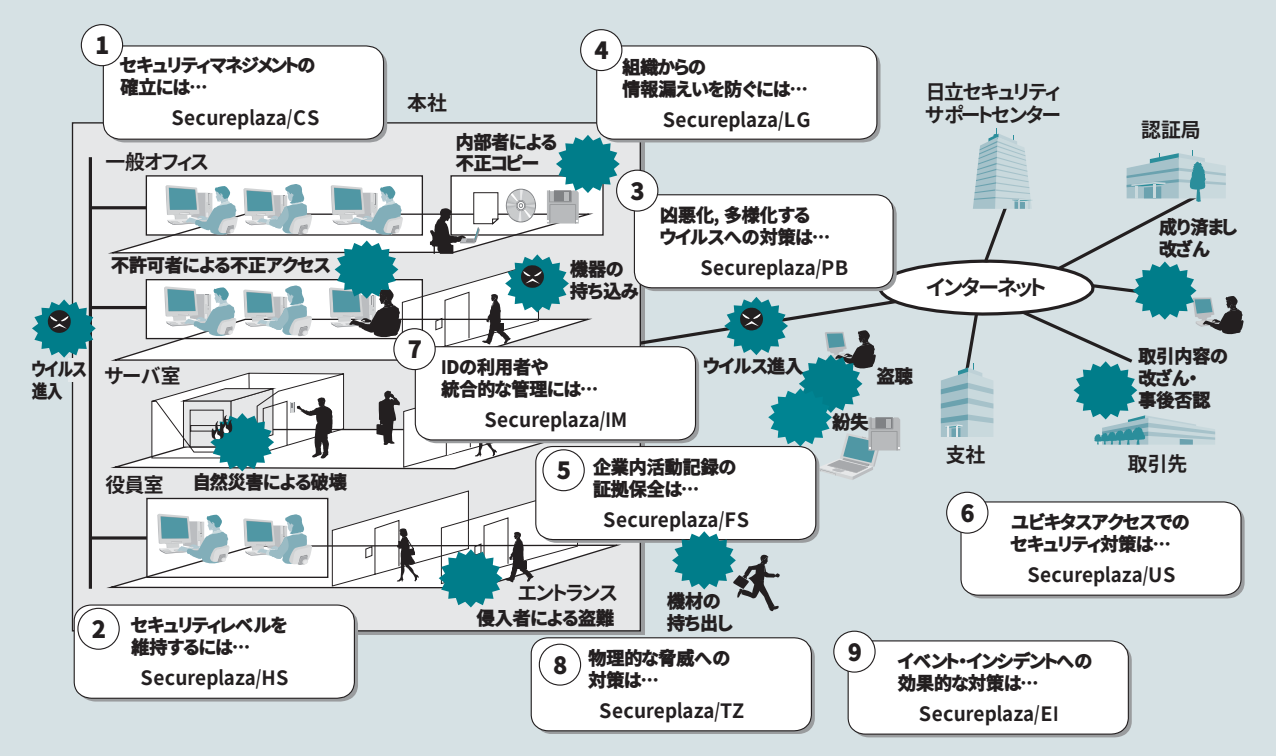


図3　Secureplazaの目的別ソリューションの全体像
組織では，ゲートから一般オフィス，サーバ室，役員室，さらにインターネットへ接続しているドメインなど，さらされている脅威や，有する情報資産価値もさまざまである。こうした組織全体の多様なリスクに対応するソリューション群がSecureplazaである。

セキュリティポリシー策定，**コンプライアンス**[(a)]プログラム策定，ISO15408準拠システム設計，認証取得支援，各種セキュリティ診断，セキュリティ監査など

（2）Secureplaza/HS（Healthcare Service）

セキュリティマネジメント，不正アクセス監視と対策，セキュリティ情報提供などから成るセキュリティレベルの維持・管理サービス群

（3）Secureplaza/PB（Pollution Block）

既知のウイルス対策,未知のウイルス対策，持ち込みPC（Personal Computer）からの感染防止，サイト内の感染拡大抑止などから成るトータルなウイルス汚染防止対策

（4）Secureplaza/LG（Leak Guard）

入退管理，認証，アクセス制御，PCメディア制御，コンテンツフィルタリング，出力紙への電子透かし付与などから成るトータルな情報漏えい防止対策

（5）Secureplaza/FS（Forensic Solution）

企業内活動の電磁的な記録（各種ログ，操作情報，処理内容，組織内映像など）を取得，保管，分析することにより，不正防止，監査対応，証拠保全を実現するソリューション

（6）Secureplaza/US
（Ubiquitous Access Security）

認証，通信路保護，持ち出し機器の保護，クライアント内情報保護などから成る，安全なモバイル業務，ユビキタスアクセスを実現するソリューション

（7）Secureplaza/IM（Identity Management）

PKI[(b)]（Public Key Infrastructure）や生体などによる認証，ディレクトリ管理，プロビジョニング，シングルサインオンによるアクセス制御などから成るトータルなID管理ソリューション

（8）Secureplaza/TZ（Trusted Zone）

確実な本人認証による入退管理，物品の搬入搬出管理，映像との連携，大規模分散拠点の統合運用管理・監視などから成るトータルな物理セキュリティ対策

（9）Secureplaza/EI（Event Incident & Action）

セキュリティオペレーションセンターで，物理，サイバー両面のイベント・インシデントを統合監視し，速やかな対策を打つソリューション

このレポートでは，特にこの中の（6）についてクローズアップしたい。

(a) コンプライアンス
法律・法令や社会的な倫理，規範を守って行動すること。主に企業の経営活動について言う。1960年代から米国企業を中心に発達してきた考え方だが，近年では，わが国でも企業不祥事の多発に伴って重視されるようになってきた。違法行為の防止といったリスクマネジメントの一環としてだけでなく，社会的信頼を高めるための活動として積極的に取り組む企業が増えている。

(b) PKI
暗号鍵と復号鍵が異なる公開鍵暗号技術を利用するネットワーク社会の基盤となる技術。認証や，通信路の暗号化，データの改ざん検知，ネットワーク取引の否認防止など，さまざまな用途を実現することができる。

ユビキタスアクセスセキュリティソリューション：Secureplaza/US

1. ユビキタスアクセスにおける脅威

利便性や効率性を追求したユビキタスアクセスは，反面，さまざまな脅威にもさらされる。**図4**は，JNSA（NPO日本ネットワークセキュリティ協会）の調査による，組織からの情報漏えいにおける原因別の割合を示している[5]。これを見ると，盗難，紛失・置き忘れなど，情報を搭載したもの自体を介しての漏えいが5割以上を占めていることがわかる。ユビキタスアクセスは，正にこの脅威に直面しているのである。しかも，社内の防御されたネットワークからのアクセスだけでなく，社外の一般のオープンなインターネットを介してのアクセスによって，ウイルス感染や不正アクセスのリスクも非常に高くなる。組織活動のスピードアップ，業務効率の向上を実現するユビキタスアクセスだが，その一方では，個人情報の漏えいや機密情報の盗難が一度発生すると，組織にとっては，ブランドイメージの失墜，損害賠償訴訟，競合力の低下など，計りしれないリスクと直面することになる。したがって，こうした脅威に備えることなくして，安心なユビキタスアクセスの実現はありえない。

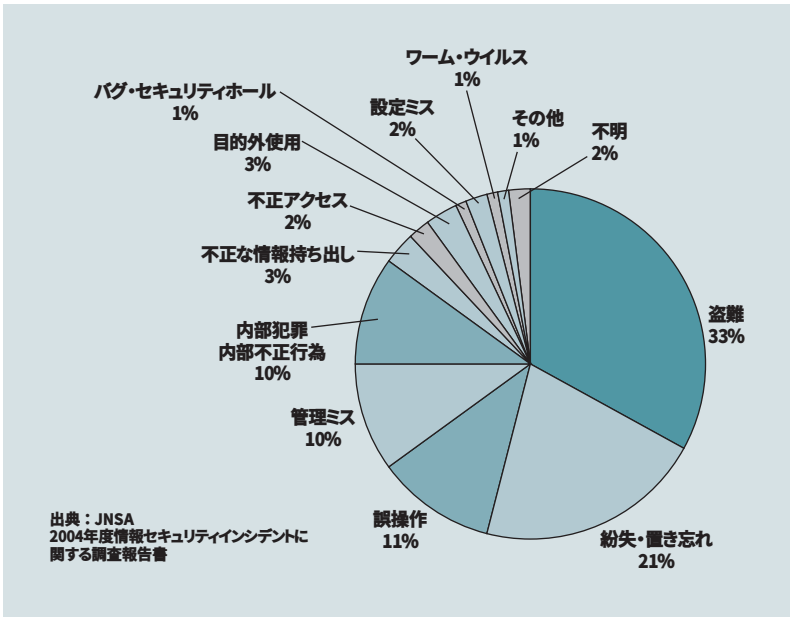


図4　個人情報漏えい事件・事故の原因別件数割合
2004年度に発生した情報漏えい事件，事故における漏えい原因別の割合を示している。

2. ユビキタスアクセスにおけるセキュリティ対策の全体像

ユビキタスアクセスでは，社外に持ち出されるクライアントPCやメディア，ネットワーク上でやり取りされる情報，オープンなネットワークを介した接続を許容するサイト側のそれぞれに対して，さまざまな脅威が存在する。その全体像を**図5**に示す。縦軸に保護対象として，クライアント，ネットワーク，サイトをとり，それぞれに対して想定される脅威を示している。

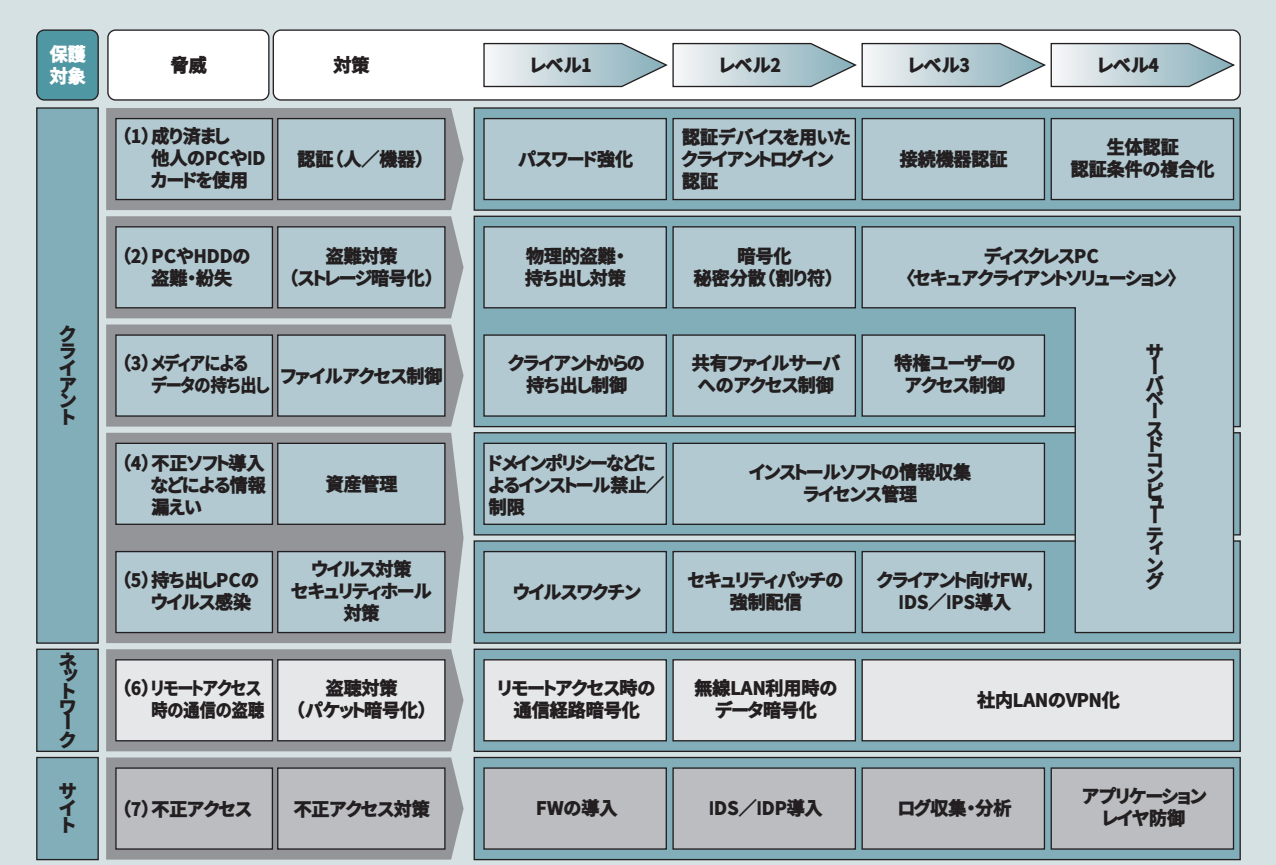
想定される脅威として，クライアントでは(1)成り済まし，(2)PCやHDD（Hard Disk Drive）の盗難や紛失，(3)付属メディアなどによるデータの不正持ち出し，(4)不正ソフトウェアのインストールに起因する情報漏えい，(5)ウイルス感染があり，ネットワークでは(6)通信の盗聴，サイトでは(7)不正アクセスなどがあげられる。横軸に，それぞれの脅威に対する，セキュリティレベルに応じたさまざまな対策を，4段階のレベルで示している。

(1)に対しては，記憶情報による認証としてパスワードの強化，次のレベルでは，USB（Universal Serial Bus）キーやICカードなどのデバイスによる認証，さらにセキュリティレベルを高めるには，接続される機器認証や使用者の生体認証があげられる。

(2)や(3)に対しては，クライアント情報の暗号化ツールや付属メディアのアクセス制御を実現するツールの適用があげられる。さらにセキュリティレベルの高い対策としては，ディスクレスのPCやメディア接続不可のPCと，アプリケーションやデータをすべてサーバ上で管理するサーバベースドコンピューティングのシステム形態があげられる。

現在のハードディスクやメディアドライブを持ったリッチなクライアントPCによるシステム環境下で対策を打つとすれば，それぞれのツールを活用することになるが，今後の組織システムにおける抜本的な対策として，上記のディスクレスPCを指向する動きが始まっている。

セキュリティ対策フローの観点から，ユビキタスアクセスでのセキュリティ対策をあげると，(1)通信路の保護（盗聴の防止），(2)



注:略語説明 FW(Firewall), IDS/IPS(Intrusion Detection System:侵入検知システム/Intrusion Prevention System:侵入防止システム)

図5 ユビキタスアクセスにおける脅威と対策の全体像

モバイルアクセスにおいて，保護対象であるクライアント，ネットワーク，サイトのそれぞれに対する脅威群と，セキュリティレベルに応じた対策の全体像を示している。

認証(成り済ましの防止)，(3)クライアントデータの保護(情報漏えいの抑止)の3ステップになる。このうち，(1)と(2)はクライアントの形態に依存することなく共通に実施される。(3)は，リッチなクライアントに対しては暗号化ツールやメディア利用制御ツールの利用があげられるが，究極はクライアントにデータを搭載しない上述の形態となる。

3. ユビキタスアクセスに必要なセキュリティソリューション

Secureplaza/USは，図5に示すさまざまな対策から，システム要件に適したセキュリティを提案するソリューション体系である。

その要件を構成する項目は，(1)実現したいユビキタスアクセスの業務フロー，(2)現有システム資産の更新の可否，(3)必要なセキュリティレベル，(4)構築までの期限，(5)予算・費用など，いずれも本質的な要件である。

例えば，(1)では，営業社員の顧客訪問，研究開発者の出張，業務の持ち帰り，在宅勤務など，さまざまな業務が考えられ，それに対する要件として，通信帯域を保証できる環境での利用か，データを直接持参する必要があるのかなどがあげられる。(2)はすでに資産となっているPCの利用を前提とするのか，クライアント自体の更新も選択肢に入るのかがあげられる。同様に，(3)，(4)，(5)も顧客固有の条件が存在する。また，(5)においては構築の初期コストだけではなく，通信費を含む運用コストの検討が重要となる。

これらの中で，(2)のシステム構成とアプリケーション構成において，セキュアモバイルシステムの実現形態を分類すると，大きく三つに分けられる。

(a) 現有資産の活用:パターン1

クライアント，アプリケーションとも，現有システム資産をそのまま活用する。対策としては，クライアントのファイル暗号やメディア利用制御などの各種の情報漏えい防止ツール類を活用する。

(c) 新会社法

商法・商法特例法・有限会社法など，これまで幾つにも分かれていた会社に関する法律を一本化するとともに，時代に合わせた新たな制度も設けた商法の大改正によって施行される。有限会社制度が廃止されるが，最低資本金規制の撤廃や株式会社の取締役数削減により，起業が容易になる。また，M&Aが柔軟になるほか，LLC(合同会社)，LLP(有限責任事業組合)，会計参与の新設なども大きな特徴である。

(d) 日本版SOX法

2002年に成立した米国の企業改革法，Sarbanes-Oxley(サーベンス・オクスリー)法の日本版。2008年3月決算期から施行される予定で，上場企業とその関連会社に，内部統制の整備や公認会計士による監査が義務づけられる。米国版と比べ，ITによる内部統制の重要性が強調されているのが特徴。内部統制とは，不正防止を目的とした意思決定や業務のプロセスを確立，順守する体制を意味する。

(b) 現有資産の活用:パターン2

クライアントを含め，システム構成は利用するが，クライアントであるPCを画面とキーボードの機能だけの利用に限定する仮想的なシンクライアント化を行い，アプリケーションはサーバ側で実行する形態に移行する。

(c) クライアントシステムの入れ替え

クライアントをディスクレスPCに置き替え，アプリケーションはセンターやサーバで実行する形態に移行する。ただ，このケースも，システム構成としては，ソフトウェア資産をそのまま移行するクライアントブレード型と，サーバにソフトウェア資産を移植するサーバ型の選択肢がある。

Secureplaza/USでは，(a)においては，「JP1/秘文」をはじめとした多くの情報漏えい防止ツール類をそろえており，(b)，(c)においては，アプリケーションをサーバで実行するフレームワークを実現する製品類をそろえている。さらに(c)については，ディスクレスで強固な認証や通信路暗号化などをセットとしたセキュリティPCを開発し，**図5**における最上位レベルのセキュリティを実現するソリューションを用意している。

4. 次世代の企業情報システム「セキュアクライアントソリューション」

前述したユビキタスアクセスにおけるセキュリティ対策の最上位レベルに位置づけられるのが，セキュアクライアントソリューションである。このセキュリティPCによるシステムは，単にセキュアモバイルにとどまらず，今後の組織内のシステムアーキテクチャの方向性を示唆する存在でもある。

ITシステムは，1970年代のバッチ，TSS(Time Sharing System)などの中央集中処理の時代から，1990年代にかけては，システムコストや性能・操作性を追求して，分散処理，CSS(Client Server System)の時代へと急速に進んだ。その後，PCの高性能化と多機能化にけん引されて，オープンなネットワーク処理の時代へと移行してきた。IT化の進展は，業務効率向上や高い利便性を実現してきたが，一方で，セキュリティ上の問題，運用管理コストの問題，さらには個人情報保護法などのコンプライアンスの課題に組織は直面している。また，2006年5月施行の**新会社法**[c]や，現在議論されている**日本版SOX法**[d](内部統制)を受け，いかに組織の中のITを使った業務や処理の情報を統制していくかも火急の課題となっている。しかし，処理プログラムの分散化，情報やデータベースの散在，さらには組織内情報への多数の出入り口の存在は，その対策を非常に困難にしている。

一方で，サーバ，ネットワーク，ストレージの処理能力と技術の向上は目覚ましく，その課題に対応するITシステムとしての包括的な解決策としては，中央集中型の処理システム，サーバベースドコンピューティングが非常に有力であり，それがセキュアクライアントソリューションである。その詳細については，本号の各論文を参照いただきたい。

セキュリティ対策の投資効果をどう考えるか

1. セキュリティ対策の位置づけ

現在の組織は多種多様な情報を抱え，それを活用していくことが組織活動には不可欠な時代となっている。セキュリティ対策についてはすでに触れたが，組織の活動を活性化していくために，システムやサービスを広げていくにしたがって顕在化する脅威への対策である。さらに，企業の社会的責任として，制定されるさまざまな法制度や基準に準拠していくための対策の一つでもあり，セキュリティ対策は，経営投資の一部としてとらえるべき時代となっている。

2. セキュリティ対策の投資効果

セキュリティ対策の投資効果を定量的に評価することは，現状ではかなり難しい課題である。

情報漏えい事故を例にとると，JNSAの試算では，2004年度で1件当たりの被害額が平均13億円強となっている[5]。これは，被害者への謝罪と情報開示，損害賠償訴訟，ブランドの失墜，顧客離れや株価への影響

などを含んだ数値である。例えば，これに想定発生頻度（何年／回）を掛ければ仮想被害額を算出することは可能だが，組織の規模や置かれている状況で大きな差異が生じてくると考えられる。セキュリティ対策で，この仮想被害額がいかに低減できるかによって，投資効果があったと見る報告がある。

一方，セキュリティ対策の投資効果は，単にリスクの低減だけでなく，運用管理コストの低減にもつながる。例えば，セキュリティパッチの管理やウイルスパターンファイルの管理など，セキュリティ維持のために費やされている運用コストなどをトータルに考慮した投資効果の評価が重要である。

前述のセキュアクライアントソリューションは，クライアントからの情報漏えいリスクを大幅に低減するだけでなく，クライアント資産の運用管理コスト削減を含めて，大きな投資効果が期待できる。

ITシステムの新たな潮流

オフィスの業務形態変化やワークプレイスのユビキタス化が進展している反面，情報セキュリティの脅威やコンプライアンスへの備えがますます重要となってきている。その対策には，ここで報告したような，必要とされるセキュリティレベル，時間軸，コストなどの全体像を把握し，取り組むことが必要である。

ITシステムでは，これまでのリッチなパソコンを用いた環境から，サーバベースの新しい組織プラットフォームの構築が始まりつつある。日立グループは，その流れの中で，現システムでの対策から次期システムを視野に入れた対応までを提案するとともに，よりいっそう高い利便性と高度なセキュリティを兼ね備えたソリューションの開発に取り組んでいく。

参考文献など

1）**小林，外：よくわかる企業セキュリティ入門　事業継続とSOX法，日刊工業新聞社**（2006.2）
2）**日立セキュリティソリューション**　Secureplaza, http://www.hitachi.co.jp/Secureplaza
3）**金野千里：情報セキュリティの動向とトータルセキュリティソリューション，情報処理学会誌**（2002.10）
4）**金野，外：セキュアなサービスプラットフォームを実現するセキュリティソリューション“** Secureplaza **”，日立評論，86，** 6，437〜442（2004.6）
5）NPO**日本ネットワークセキュリティ協会，** http://www.jnsa.org/

執筆者紹介

金野 千里
1977**年日立製作所入社，情報・通信グループ　セキュリティ事業部　セキュリティソリューション推進本部　セキュリティマーケット開発部　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
日本応用数理学会会員，情報処理学会会員

長谷川 大造
1989**年日立製作所入社，情報・通信グループ　セキュリティ事業部　セキュリティソリューション推進本部　セキュリティマーケット開発部　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

田川 豊
1984**年日立製作所入社，情報・通信グループ　セキュリティ事業部　セキュリティソリューション推進本部　セキュリティシステムソリューション部　所属**
現在，セキュリティソリューションの開発と事業展開に従事

永井 康彦
1985**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　開発本部　セキュリティソリューション部　所属**
現在，セキュリティソリューションビジネスの推進に従事
工学博士
電子情報通信学会会員，電気学会会員，情報処理学会会員，日本航空宇宙学会会員