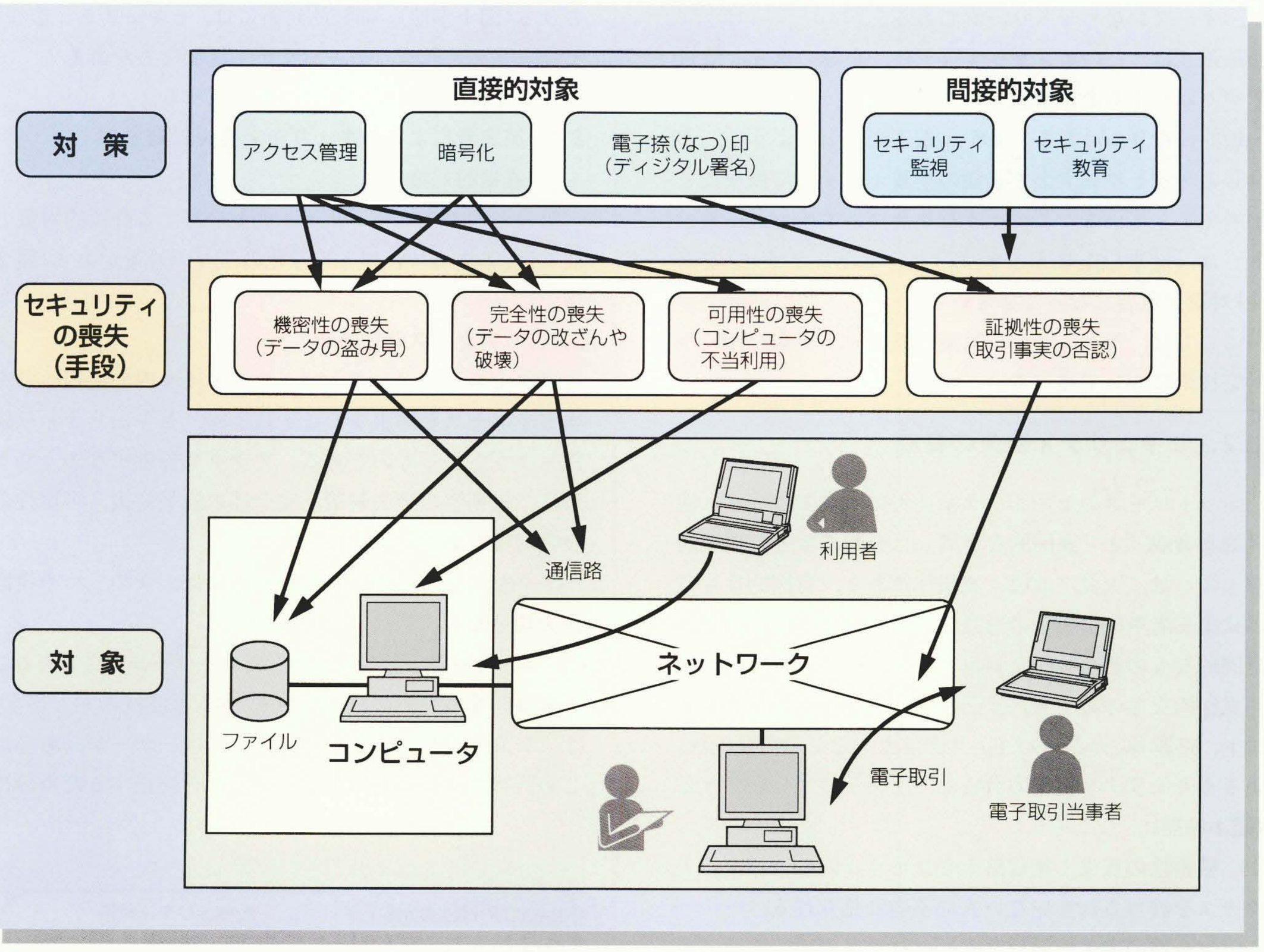
オープンネットワークにおけるセキュリティ技術

Security Technologies for Open Networks

佐々木良一 *Ryôichi Sasaki*　小林偉昭 *Hideaki Kobayashi*
櫻庭健年 *Taketoshi Sakuraba*　大谷 真 *Makoto Ôya*



セキュリティの喪失の脅威とその対策

オープンネットワークでのセキュリティ技術の重要性は増大しつつあり，セキュリティ喪失の脅威に対応する総合的な対策が求められている。

電子商取引の普及や，インターネットと企業情報ネットワークの接続の増加により，セキュリティ(安全性)対策の重要性が増大している。第三者によるセキュリティの喪失としては，(1)情報の不当な盗み見などによる「機密性の喪失」，(2)データの改ざんや破壊などによる「完全性の喪失」，(3)コンピュータパワーの不当な利用などによる「可用性の喪失」がある。

これらの第三者によるセキュリティの喪失に対する直接的対策には，アクセス管理と暗号化があり，間接的対策としてセキュリティ監視やセキュリティ教育などがあることが知られている。また，取引相手によるセキュリティ喪失には取引事実の不当な拒否などの証拠性の喪失があり，その対策としては電子捺印(ディジタル署名)がある。

高いセキュリティを実現するために，日立製作所は，セキュリティ システム インテグレーション，セキュリティ運用などのサービスを行うとともに，暗号LSI，チャネル直結暗号装置などのハードウェア製品や，暗号ライブラリ，電子捺印ライブラリ，暗号機能付きファイアウォールなどのソフトウェア製品を開発している。

1. はじめに

インターネットの利用が急激に増大しつつあり，その利用者は全世界で1億人を超えるとも言われている。インターネットは，だれでも参加でき，その通信規約や応用ソフトウェアをだれもが容易に利用できるという意味で，オープンなネットワークである。

最近では，このインターネットに，企業の重要な情報をやり取りする企業情報ネットワークを接続することが一般的になりつつある。また，電子商取引のように，これらのネットワーク上で多額の金銭を電子的に扱うことが増えてきている。このような状況にあるインターネットでは，従来以上にネットワークのセキュリティ(安全性)対策が重要になってきている。

ここでは，セキュリティ対策の概要と，日立製作所の対応技術について述べる。

2. セキュリティ喪失の脅威

ネットワークのセキュリティ喪失に対する脅威は，「偶発的な脅威」と「意図的な脅威」に分類できる。偶発的なものには，天災，故障，誤操作があり，意図的なものには第三者や取引相手の悪意の行為がある。ここでは，意図的なものを直接的な対象とする。

意図的なもののうち，第三者(例えば，スパイ，テロリスト，犯罪者，産業スパイ，クラッカーなどの愉快犯)によるセキュリティ喪失の脅威は，次の三つに分類できる(**図1**参照)。

(1) 機密性の喪失：通信路上やファイル内の情報が，アクセスを許可されていない人に不当に見られる。

(2) 完全性の喪失：通信路上やファイル内の情報が，不当に改ざんされたり破壊される。

(3) 可用性の喪失：コンピュータの機能や保存されている情報が，外部の人間のコンピュータパワーの不当な利用によって使えなくなる。

第三者がこのような脅威を与える手段としては，コンピュータの直接的操作による場合と，不正なソフトウェアをコンピュータに流し込むことによる場合がある。後者がコンピュータウイルスと呼ばれるものである[1)]。

また，取引相手が脅威を与えるものとしては，証拠性の喪失を考えておく必要がある。すなわち，取引相手が契約書などの取引文書を偽造したり改ざんし，取引内容や取引事実を不当に事後否認することがありえる。例えば，「株を3,000株買ってくれと言ったのに30,000株も買わされてしまった。損害を賠償してくれ」といった不当な要求に対し，証拠を示し，自分の正当性を証明できるようにしておく必要がある。

3. セキュリティ対策技術

セキュリティ対策は，直接的対策と間接的対策に大別できる(**図1**参照)。間接的対策には，セキュリティ監視，セキュリティ教育，セキュリティ評価などがある[1)]。

ここでは，直接的対策について述べる。

3.1 第三者によるセキュリティ喪失に対する直接的対策

第三者によるセキュリティ喪失に対する直接的対策としては，アクセス管理と暗号化の二つの対策がある(**図2**参照)。

3.1.1 アクセス管理技術

アクセス管理は，通信路上やファイル内の情報への不当なアクセスを防止することにより，セキュリティを確保しようとするものである。アクセス管理がうまくできれば，機密性の喪失対策，完全性の喪失対策，可用性の喪失対策に効果がある。

アクセス管理を適切に行うためには，次の二つの技術が大切となる。

(1) ユーザー認証技術：名のったユーザーが本人であることを証明するための技術であり，本人確認技術とも言う。

(2) アクセス制御技術：それぞれのユーザーが，あらかじめ許可された権利以上のアクセスを防止するための技

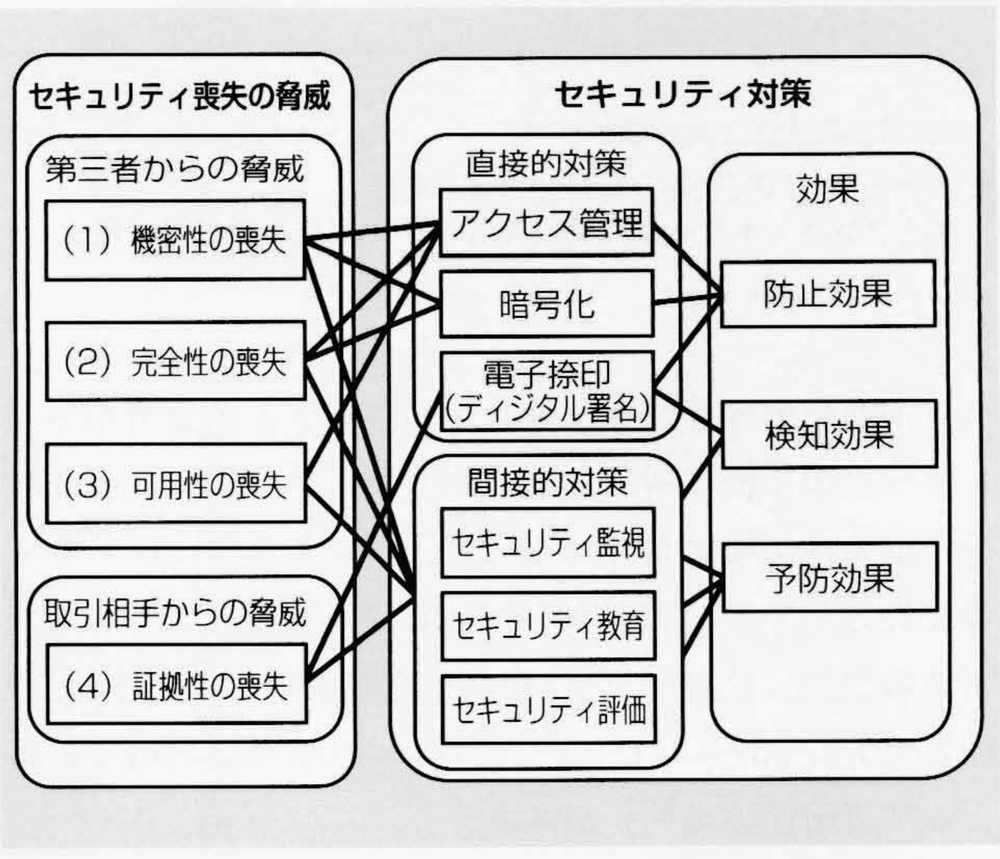


図1 セキュリティ喪失の脅威とセキュリティ対策

セキュリティ喪失を防ぐには，効果的なセキュリティ対策が必要である。防止効果のある直接的対策だけでなく，検知効果や予防効果のある間接的対策も大切である。

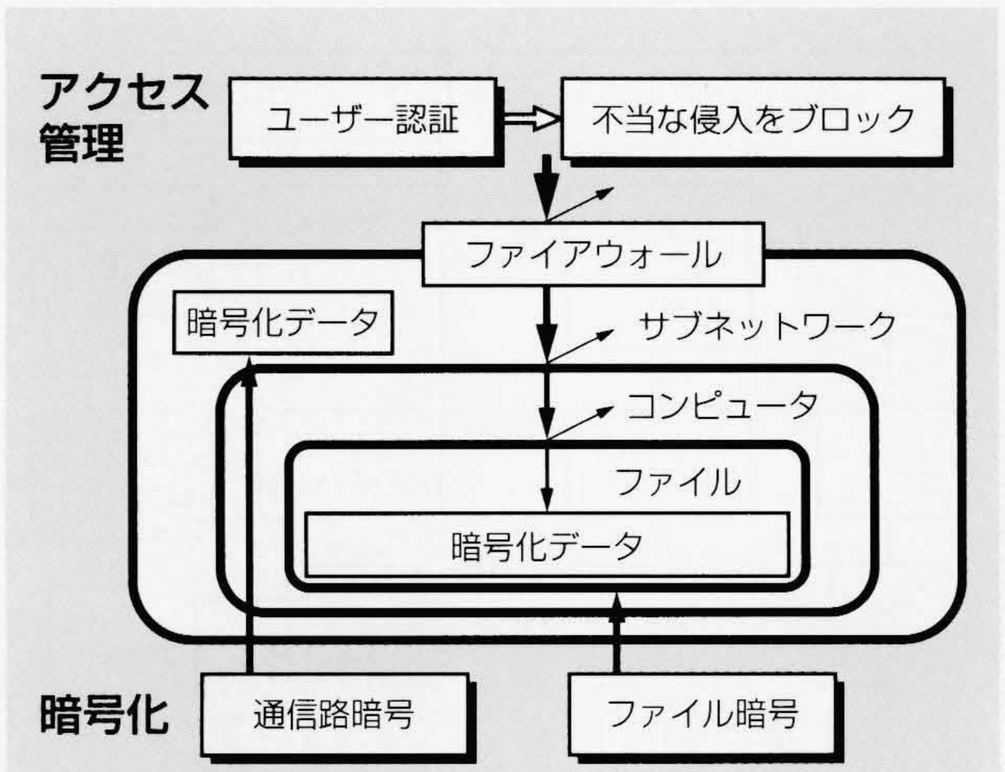


図2　アクセス管理と暗号化
直接的セキュリティ対策としてはアクセス管理と暗号化があり，これらを組み合わせて用いることが多い。

術である。

上述(1)のユーザー認証は，自分のパソコンやネットワークの端末へのアクセス時に実施される。このユーザー認証技術は，以下の三つに分類することができる。

(a)　本人の知識を利用するもの：ID(Identification)ナンバー，パスワード，パスフレーズなど

(b)　本人の持ち物を利用するもの：磁気カード，ICカード(スマートカードとも言う。)など

(c)　本人の身体的特徴を利用するもの：指紋，声紋，網膜パターン，DNA(遺伝子の本体)など

現状のコンピュータシステムではパスワードだけを用いるものが中心であるが，今後はより高信頼なセキュリティを確保するため，ICカードと組み合わせて用いられるようになっていくものと予想する。

自分のパソコンや端末を経由してサーバコンピュータにアクセスする場合にも，ユーザー認証が行われる場合がある。これをリモートユーザー認証と呼ぶ。リモートユーザー認証では，通信路上で盗聴して入手したパスワード情報を再利用する不正行為に対処するため，通常のパスワードを改良したワンタイムパスワードや，ゼロ知識証明などの方法が採用されることが多い。

上述(2)のアクセス制御はアクセスをブロックする部位により，以下のように分類することができる。

(a)　サブネットワークの入り口でのブロック：いわゆる，ファイアウォール技術と言われるもので，特定のネットワークへの不当な侵入を防止する。企業情報ネットワークとインターネットを接続し，その間で選択的にデータのやり取りを行うようにするための非常に重要な技術である。

(b)　コンピュータの入り口でのブロック：不当な相手をコンピュータに入れなくするためのもので，相手からかかってきた通信を一度切ってコールバックする方式などがある。

(c)　ファイルの入り口でのブロック：ユーザーにより，(i)見ることも書き込むこともできないファイル，(ii)見ることはできるが書き込めないファイル，(iii)見ることも書き込むこともできるファイルが設定でき，その設定によって権利の無い主体の不正アクセスを制御する機能である。

3.1.2　暗号化技術

暗号化技術は，アクセス管理に失敗して情報を不当に入手されても，その文字やデータを変形することにより，第三者に理解できなくするためのものである。第三者が情報を理解できないので機密性の喪失対策として有効であり，完全性の喪失対策のうち，第三者にとって都合の良い改ざんを防止するのに有効である。

暗号技術は紀元前から用いられている。ローマのジュリアス シーザが使ったと言われているシーザー暗号では，字をn字分ずらして使う方法が取られている。例えば，2字ずらす場合には，アルファベットであれば，aはc，bはdになる。したがって，「sasaki」が「ucucmk」と変換される。このように，字をずらすような方法を通常，アルゴリズムと言い，ずらす字が2文字であるときに，2を鍵と言う。暗号ではこのように，アルゴリズムと鍵を用いる。このようにして送信者が暗号化した暗号文を受け取った人が，同じアルゴリズムと対応する鍵を知っていれば元の文を求めることができる。

暗号アルゴリズムには，アルゴリズム公開型のものと，アルゴリズム秘匿型のものがある。近年，ビジネス環境で使われるものは，運用を容易にするために大部分がアルゴリズム公開型になっており，アルゴリズムを公開しても，鍵さえ秘密にしておけば安全なようなアルゴリズムとなっている。

アルゴリズム公開型の暗号方式には，「共通鍵暗号」と「公開鍵暗号」がある(**表1**参照)。共通鍵暗号は，暗号化のための鍵と復号のための鍵が同じか，容易に類推できるものである。米国で標準的に用いられている“DES”や日本電信電話株式会社が開発した“FEAL”，日立製作所が開発した“MULTI”などがよく知られている。これらの方式は，暗号処理時間が速いのが特徴である。これ

表1　共通鍵暗号と公開鍵暗号

暗号アルゴリズムには共通鍵暗号と公開鍵暗号がある。データの暗号化には前者が，鍵配送や電子捺印には後者がそれぞれ用いられる。

項　目	共通鍵暗号	公開鍵暗号
代表例	DES，FEAL，MULTI	RSA，だ円暗号
暗号鍵の関係	暗号鍵＝復号鍵	暗号鍵≠復号鍵
秘密鍵の配送	必要(×)	不要(○)
安全な認証(電子捺印)	困難(×)	容易(○)
暗号化速度	速い(○)	遅い(×)
主要な用途	データの暗号化	鍵配送，電子捺印

に対して公開鍵暗号は，暗号化のための鍵と復号のための鍵が1対1には対応するが，鍵の内容がまったく異なり，一方から他方への類推が確率的に不可能な方式である。公開鍵暗号としては，米国で開発された“RSA”が有名である。

暗号通信のためには，暗号化の鍵に対応する復号鍵を送信者に送っておく必要がある。公開鍵暗号では暗号鍵と復号鍵が異なるため，一方の鍵を公開鍵としてだれにでも公開でき，鍵の管理が容易であるという特徴がある。また，暗号鍵と復号鍵が異なるという特徴をうまく利用することにより，次節に述べる電子捺印(ディジタル署名とも呼ばれる。)の機能を実現することができる。

一方，公開鍵暗号は処理時間が共通鍵暗号に比べて2，3けた遅いため，大量データの暗号化には不適である。

3.2　取引相手の不正への直接対策

情報ネットワークを利用した取り引きでのトラブルを防止するためには，取引者がその内容についてほんとうに取り引きを行ったことを証明する認証の機能が必要である。このような機能は，従来の紙を用いた取り引きでは，契約書にインクなどで取引文を書き，それに捺印することによって実現されてきた。しかし，印影などの原情報を単にディジタル化して電子取引文書に付けただけでは，簡単に不正を行うことができる。コンピュータを用いれば，その取引文書を修正したり，印影を別の取引文書に移すことも容易であり，変更点が少しもわからなくなってしまうからである。

この解決策として考案されたのが，公開鍵暗号などを利用した次の二つの認証機能を持つ電子捺印技術である。

(1)　電子捺印を本人が押したものであることを証明できる「ユーザー認証機能」

(2)　対象とする取引文書に押したものであることが証明できる「メッセージ認証機能」

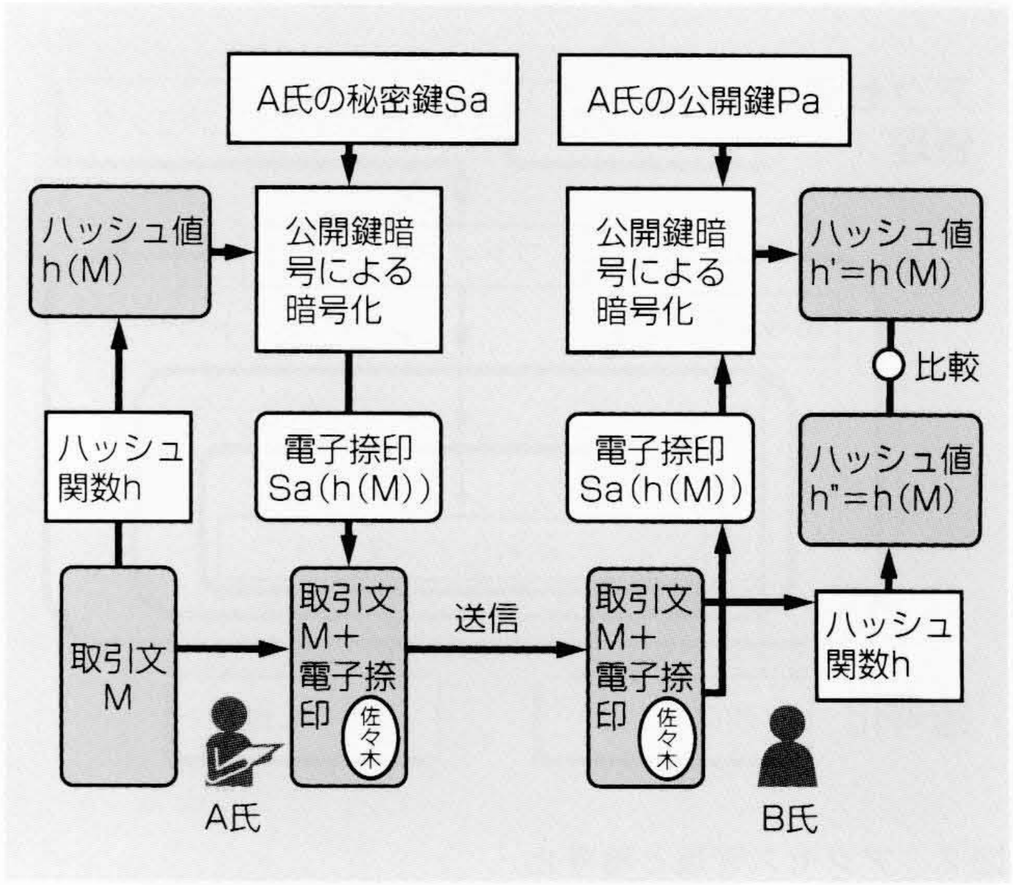


図3　電子捺印の方式

電子の世界で捺印の機能を実現するために，ハッシュ関数と公開鍵暗号が組み合わされて用いられる。

これらの具体的実現手段を**図3**に示す。同図で，ハッシュ関数というのは，長い取引文書から100ビット程度の圧縮文(ハッシュ値とも言う。)を作るためのものである。元の文が1ビットでも異なるとハッシュ値はまったく異なるものになり，改ざんの検知に用いることができる。短いハッシュ値を作ってから公開鍵暗号の秘密鍵Saを用いて暗号化をするのは，公開鍵暗号の処理速度が遅いという欠点に対処するためである。また，二つのハッシュ値(h'とh")が等しいということは，(1)取引文の改ざんが行われておらず，かつ(2)A氏の公開鍵Paに対応するSaでハッシュ値に暗号がかけられたことを意味している。したがって，メッセージ認証の機能と，ユーザー認証の機能を満足していることになり，電子の世界の捺印の機能を果たしていることになる。インターネットを利用して電子ショッピングや電子決済を行うようになることが予想されるが，このようなことを安全に実施するための基幹技術が，この電子捺印技術である。

なお，公開鍵PaをA氏以外が作成してA氏の公開鍵であるという「成りすまし」を防止するためのものが認証局と言われるものであり，印鑑登録や印鑑証明の機能を持つものである[1)]。

4．日立製作所のセキュリティ技術

日立製作所は，総合力を発揮して安全なインターネット・イントラネットを実現するため，“FOREFRONT with Cyberspace”構想に基づく日立セキュリティフレ

ームワーク“Secured Cyberspace”として，(1)システムインテグレーション〔消費者EC(Electronic Commerce)システム，企業間ECシステムなど〕，(2)セキュリティ運用サービス(認証局サービス，ファイア ウォール アウトソーシング サービスなど)，(3)ハードウェア製品(暗号LSI，チャネル直結型暗号装置，暗号化機能付きルータなど)の提供，(4)ソフトウェア製品の提供といった統合的アプローチを行っている(**図4**参照)。

セキュリテイ用のソフトウェアアーキテクチャと対応製品の概要を**図5**に示す。これらの製品の一つが，日立製作所が開発した共通鍵暗号“MULTI”をパソコンやワークステーション向けにライブラリ化した“Keymate/MULTI”である。MULTI暗号は，DESなどに比べて暗号処理速度が1けた近く速く，また，安全性の一つの尺度である鍵長が長い(DESの56ビットに対し，64ビット標準，256ビットまで拡張が可能)という特徴を持ち，PerfecTVなどのディジタル衛星放送の暗号化のわが国での標準としても採用されている。

また，圧縮と暗号を融合することにより，安全性を保ちつつ全体の処理時間を約60%に短縮することができる「圧縮/暗号統合化方式」[2]を製品化している。さらに，新公開鍵暗号や高速ハッシュ関数の研究開発も行っている。

電子捺印機能についても，“Keymate/Sign”としてソフトウェアライブラリの形で製品として提供している。この機能は，日立製作所のグループウェア製品である“GroupMax”の構成要素である“GroupOASQUARE”に組み込まれている。

また，ファイアウォール“Gauntlet”※)を米国TIS社から導入して提供するとともに，ファイアウォール間，ファイアウォールとパソコン間で暗号通信を行うVPNの機能を独自に開発し追加した[3](**図6**参照)。この機能は，(1)独自開発であるため，米国の暗号製品の輸入規制に触れず，長い鍵長の強い暗号を自由に使える，(2)上記の圧縮と暗号を融合して行う機能を世界で最初に製品として実現したため，効率的な圧縮処理と暗号化が可能，(3)応用プログラム間の通信を安全に行うためのソフトウェアである“SecureSocket”[4]を開発し導入することにより，Socketインタフェース対応に開発した応用プログラムであれば，それを変更することなく暗号通信が可能などの特徴を持つ。また最近，ファイアウォールが多段に存在する場合にもエンド ツー エンドで暗号通信が行える機能を追加した[3]。

このほか日立製作所は，電子商取引用の認証局機能，セキュア コマース プロトコル“SECE”などに対応するソフトウェア製品を開発している。

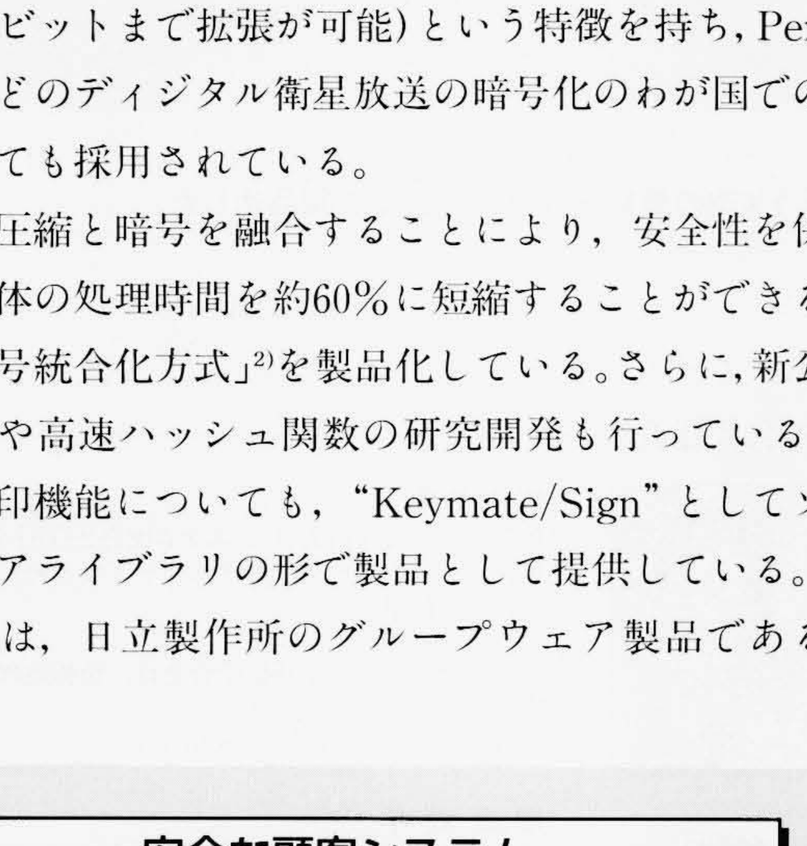
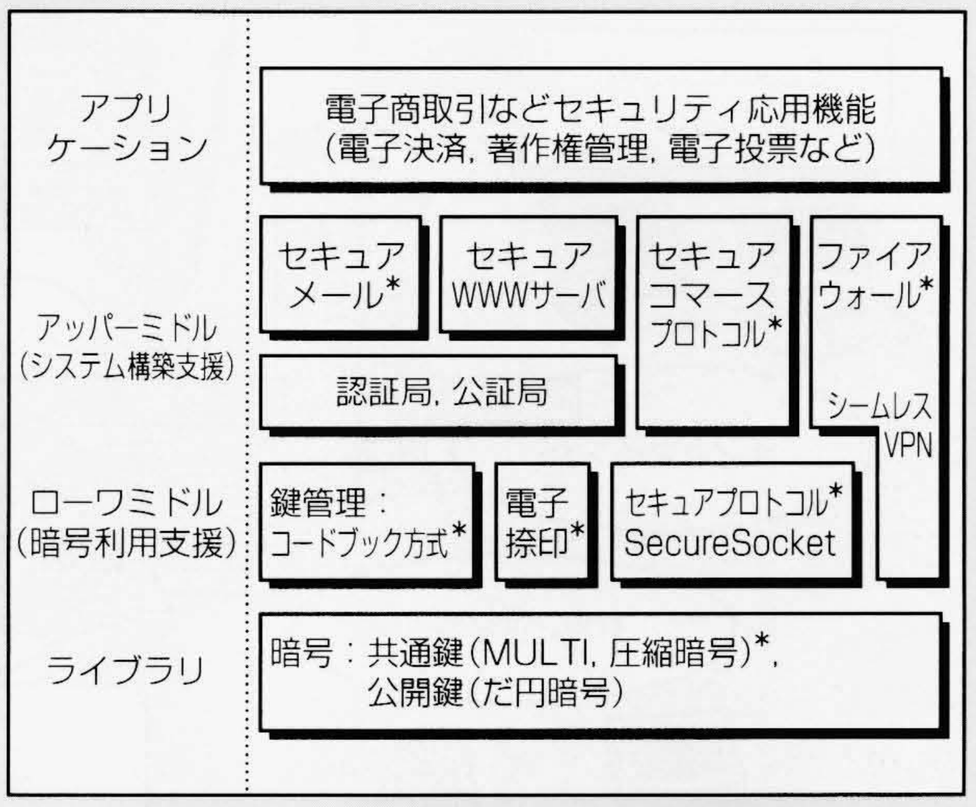


図4　日立製作所のセキュリティサービスと製品群
日立製作所は，顧客システムのセキュリティを確保するため，ハードウェアとソフトウェア製品だけでなく，システム インテグレーション サービスやセキュリティ運用サービスも提供している。



注：略語説明ほか　WWW(World Wide Web)
VPN(Virtual Private Network)
＊は製品化済みのものを示す。

図5　セキュリティ ソフトウェア アーキテクチャ
日立製作所のセキュリティ ソフトウェア アーキテクチャは，アプリケーションレベル，アッパーミドルレベル，ローワミドルレベル，およびライブラリレベルから成り，種々の製品を提供している。

※) Gauntletは，米国Trusted Information Systems, Inc.の商品名称である。

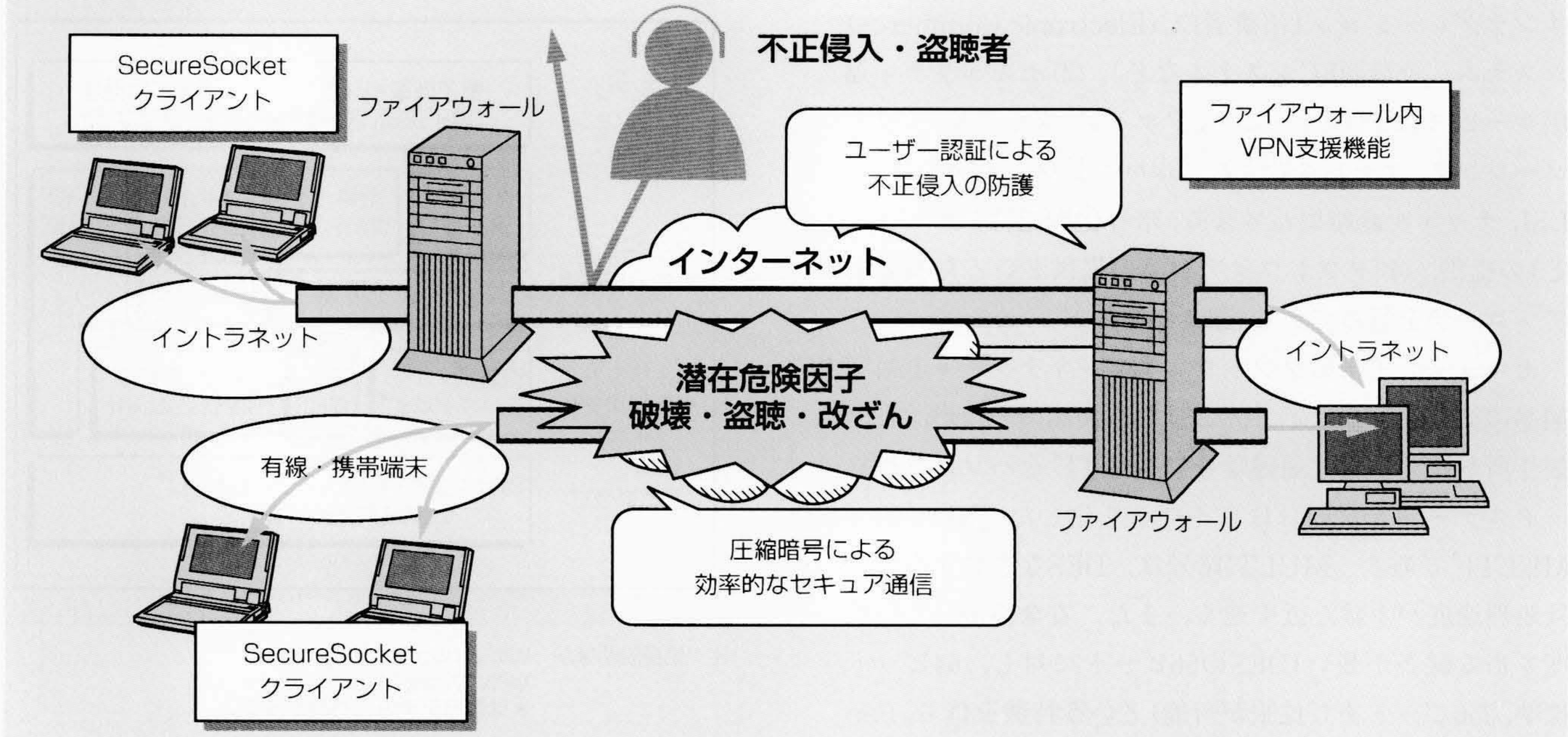


図6　ファイアウォールのVPN機能の製品化
ファイアウォール間，ファイアウォールとパソコン間で暗号通信を自由に行うVPNの機能を独自に開発して製品化した。

5. おわりに

ここでは，オープンネットワークでのセキュリティ対策の概要と，日立製作所の対応技術について述べた。

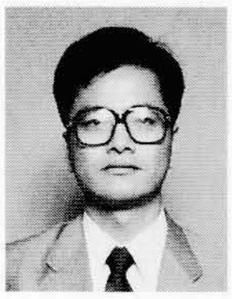
ネットワークの大規模化，モバイルコンピュータの普及，電子商取引の範囲拡大などによって今後，セキュリティ対策がますます重要になると考える。また，電子捺印などの暗号関連機能を高度に利用することにより，電子投票，著作権管理などのネットワークの利用範囲をさらに拡大することができると考える。

今後も，高信頼なセキュリティを確保するための技術を開発するとともに，新しいネットワークサービスの実現に貢献していく考えである。

参考文献

1) 佐々木，外：インターネットセキュリティ 基礎と対策技術，オーム社(1996)
2) 吉浦，外：モーバイル環境に適した圧縮/暗号化方式(その1)圧縮/暗号同時実行アルゴリズム，情報処理学会全国大会(1996年3月)
3) 萱島，外：多段ファイアーウォールに対応したVPN構築方式の提案，情報処理学会全国大会(1997年3月)
4) 高橋，外：モーバイル環境に適した圧縮/暗号化方式(その2)パケット圧縮/暗号化通信法式，情報処理学会全国大会(1996年3月)

執筆者紹介



佐々木良一
1971年日立製作所入社，システム開発研究所 第4部 所属
現在，ネットワーク，セキュリティなどの研究および研究管理に従事
工学博士
電気学会会員，電子通信学会会員，情報処理学会会員，IEEE会員
E-mail：sasaki@sdl. hitachi. co.jp

櫻庭健年
1983年日立製作所入社，システム開発研究所
第4部 所属
現在，セキュリティシステムの研究開発に従事
情報処理学会会員，IEEE会員，日本数学会会員
E-mail：sakuraba@sdl. hitachi. co.jp

小林偉昭
1972年日立製作所入社，情報事業本部
事業企画本部 所属
現在，ネットワーク関連製品の事業企画・製品企画に従事
情報処理学会会員
E-mail：h-kobayashi@comp. hitachi. co.jp

大谷　真
1972年日立製作所入社，ソフトウェア開発本部 所属
現在，インターネット・イントラネット関連ソフトウェアの開発に従事
情報処理学会会員，ACM会員
E-mail：ooyamako@soft. hitachi. co.jp