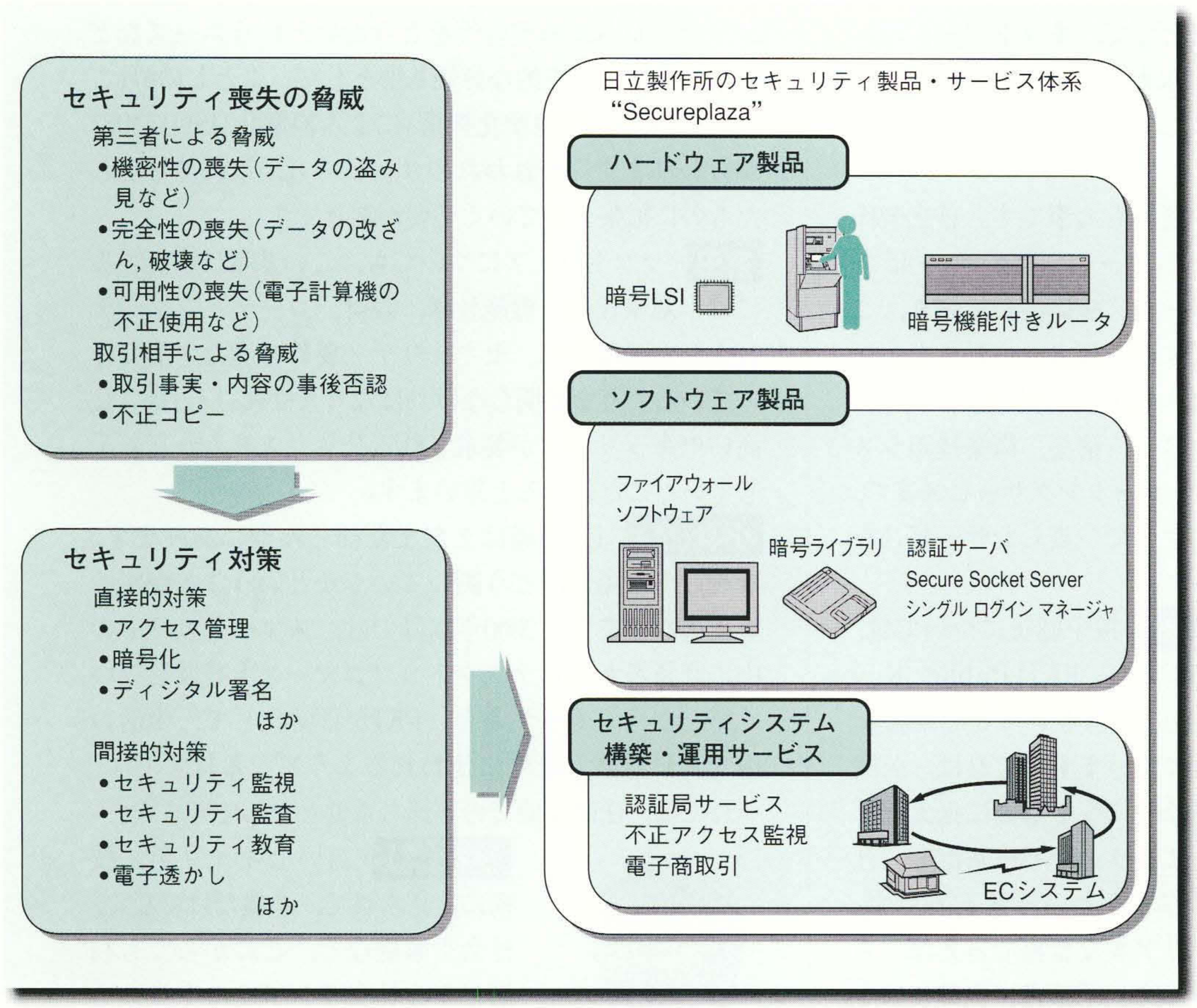
進歩する情報システムセキュリティ技術と日立製作所の取組み

Advancing Information System Security Technologies and Hitachi's Approach

佐々木良一 *Ryôichi Sasaki*　小林偉昭 *Hideaki Kobayashi*
水野 勉 *Tsutomu Mizuno*　畠山靖彦 *Yasuhiko Hatakeyama*



注：略語説明
EC(Electronic Commerce;
電子商取引)

セキュリティ喪失の脅威と日立製作所の対応

情報ネットワークの急速な発展に伴って増加しているセキュリティ喪失の脅威に対処するため，日立製作所はさまざまな製品・サービスを提案している。

EC(Electronic Commerce：電子商取引)の普及などにより，情報のセキュリティ(安全性)対策の必要性が増大している。第三者によるデータの盗み見や改ざん，破壊などの脅威に対しては，アクセス管理，暗号化，セキュリティ監視，セキュリティ評価などの対策があることが知られている。また，取引相手からの取引事実の不当な否認やディジタルコンテンツ(ディジタル形式の情報内容)の不正コピーなどの脅威への対策としては，電子捺(なつ)印(ディジタル署名)や電子透かしがある。

日立製作所は，高い情報セキュリティの実現のために，暗号や電子透かしなどの技術開発を先行的に行ってきた。また，これらの技術を生かして，情報システムに対する総合的なセキュリティ製品・サービス体系である“Secureplaza”の下に，暗号ライブラリ，電子透かしライブラリ，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や，セキュリティ システム インテグレーション，セキュリティ評価のサービスなどを総合的に提案している。

1 はじめに

インターネットの利用が引き続き増大してきており，その利用者は全世界で2億人を超えるとも言われている。世界中で，インターネット情報のセキュリティ(安全性)上の欠点を利用した不正アクセス，ネットワーク犯罪なども増加の傾向にある。

一方，最近では，そのインターネットに企業情報ネットワークを接続するとともに，EC(Electronic Commerce：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。したがって，ネットワークと接続された情報システムが攻撃を受けると，その被害は甚大なものとなる。

このような状況下にあって，情報システムのセキュリティ対策が従来以上に重要になってきている。

ここでは，情報システムセキュリティ対策の概要と，

日立製作所の対応について述べる。

2 セキュリティ喪失の脅威

情報システムのセキュリティ喪失に対する脅威は，(1) 偶発的な脅威と，(2) 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，第三者の悪意の行為と取引相手の悪意の行為がある。以下では，意図的な脅威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，海外のスパイ，テロリスト，犯罪者，産業スパイ，クラッカーなどの愉快犯) による脅威は，次の三つに分類できる[1), 2)]。

(1) 機密性の喪失：通信路上やファイル内の情報を，アクセスが許可されていない人が不当に見る。

(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。

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んで作用させることによる場合があり，後者がコンピュータウイルスと呼ばれるものである。

また，取引相手からの第一の脅威としては，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や改ざんし，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。

取引相手からの第二の脅威は，入手したマルチメディアデータやプログラムが不正にコピーされるという問題である。これらのコピーの取得は，特別な対策を取っていないと簡単に実行されてしまう。

3 セキュリティ対策技術

3.1 第三者の不正への対策

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。間接的対策としては，セキュリティ監視やセキュリティ教育，セキュリティ評価などがあり，これらは，セキュリティ対策を正しく行うために不可欠なものである。

直接的対策として，アクセス管理と暗号技術がある。この二つの技術について以下に述べる。

3.1.1 アクセス管理技術

アクセス管理は，攻撃対象である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，対象である情報に攻撃を加えることができないので，機密性，完全性，可用性の喪失対策などに効果がある。

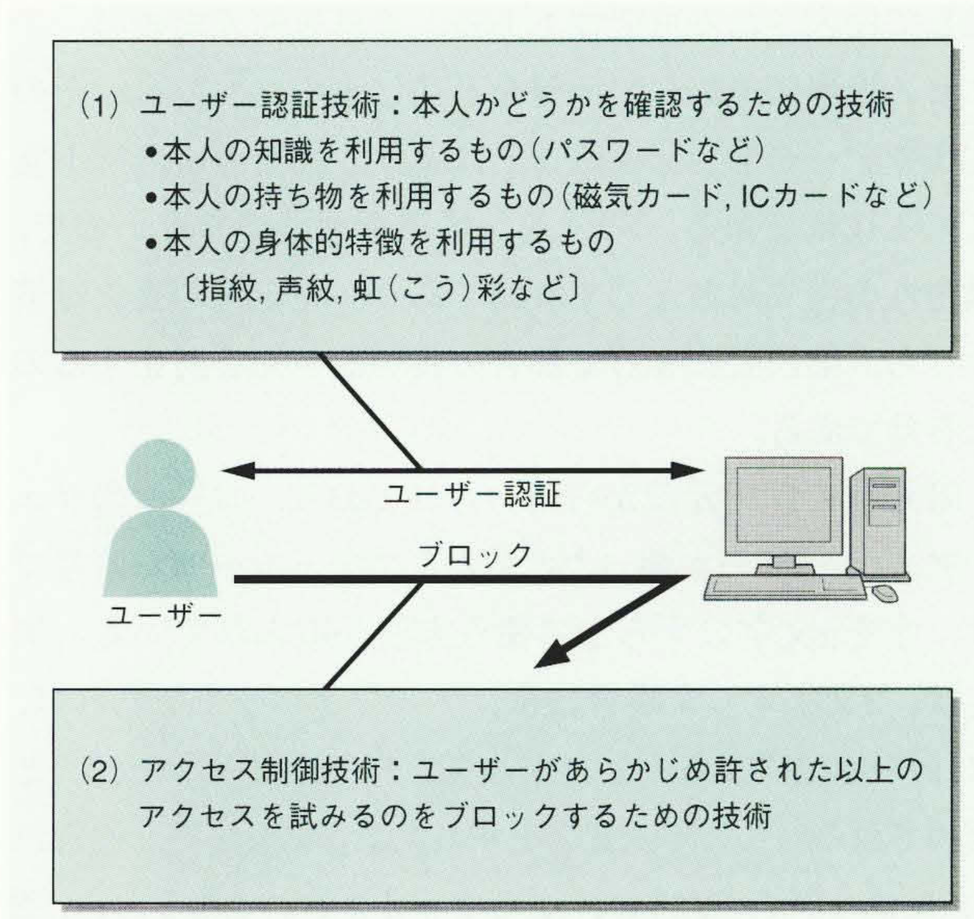


図1 アクセス管理のための二つの技術
アクセス管理を適切に行うには，ユーザー認証技術とアクセス制御技術が大切である。

アクセス管理を適切に行うためには，ユーザー認証技術とアクセス制御技術の二つが必要となる(**図1**参照)。

現状のコンピュータシステムでのユーザー認証は，パスワードだけを用いるものが中心である。今後は，より高いセキュリティを確保するために，ICカードや指紋照合との組合せが用いられるようになっていくものと予想する。

不正な侵入をブロックするためのアクセス制御は，さまざまな部位で実施できる。サブネットワークの入口でブロックする技術が「ファイアウォール」と言われるもので，企業情報ネットワークなど特定のネットワークへの不当な侵入を防止する[3)]。計算機内部でのアクセス制御としては，OS(Operating System)の機能を用いることにより，ユーザーが，(1) 見ることも書き込むこともできないファイル，(2) 見ることはできるが，書き込めないファイル，(3) 見ることも書き込むこともできるファイルなどを設定でき，ファイルの入口で，権利の無い主体の不正アクセスを制御することができる。

3.1.2 暗号技術

アクセス管理対策を行っていても，他人に成り済ましたり，セキュリティホール(セキュリティ上の欠陥)を利

用して侵入される可能性もある。これを防ぐために，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，第三者に理解不能にする技術である。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おり，ローマのジュリアス シーザーが使ったと言われているシーザー暗号では，字をn文字分ずらして使う方法が取られている。例えば，2文字ずらす場合には，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，「hitachi→jkvcejk」と変換される。ここで，文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，2を「かぎ」と言う。

このように，暗号では，アルゴリズムとかぎを用いる。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かぎを知っていれば，元の文を求めることができる。

現代の暗号アルゴリズムには，共通かぎ暗号と公開かぎ暗号がある(**表1**参照)。共通かぎ暗号は，暗号化のためのかぎと復号のためのかぎが同じか，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おり，前述のシーザー暗号も共通かぎ暗号の一つと言える。これらは，暗号処理時間が速いのが特徴である。

暗号化のためのかぎと復号のためのかぎが１対１には対応するが，互いにまったく異なり，一方から一方への類推が確率的に不可能な方式が「公開かぎ暗号」である。公開かぎ暗号としては，“RSA”や「だ円曲線暗号」がある。暗号通信のためには，暗号化のかぎに対応する復号かぎを送信者に送っておく必要がある。公開かぎ暗号では，暗号かぎと復号かぎが異なるため，一方のかぎを公開かぎとしてだれにでも公開できることから，かぎの管理が容易であるという特徴がある。また，暗号かぎと復号かぎが異なるという特徴を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，公開かぎ暗号は，処理時間が共通かぎ暗号に比べて2，3けた遅いので，大量データの暗号化には不適である。公開かぎ暗号としては，従来，RSAが主に使われてきたが，最近では，だ円曲線暗号が，処理時間の速さと暗号強度の両面から注目されている。

表1　共通かぎ暗号と公開かぎ暗号

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

項目	共通かぎ暗号	公開かぎ暗号
代表例	DES，FEAL，MULTI	RSA，だ円曲線暗号
暗号かぎの関係	暗号かぎ＝復号かぎ	暗号かぎ≠復号かぎ
秘密かぎの配送	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	かぎ配送，電子捺印

注：記号説明　×(難点)，○(長所)

3.2　取引相手の不正への対策

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実際に取り引きを行ったことを証明する機能が必要である。このような機能は，紙を用いた従来の取り引きでは，契約書にインキなどで取引文を書き，それに署名や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，不正が簡単に行われる可能性がある。コンピュータを用いて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，変更点が判別できないからである。

この解決策として考案されたのが，公開かぎ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) ユーザー認証機能：電子捺印を，本人が行ったものであると証明できる。

(2) メッセージ認証機能：対象とする取引文書に電子捺印されたものであることが証明できる。

なお，電子捺印が普及すると，印鑑登録や印鑑証明に相当する機能が必要になる。これを実施するのが，「認証局」と呼ばれるシステムである。また，取引内容にまで立ち入って正当な取り引きかどうかを証明するのが，「公証局」と呼ばれるものである。

次に，ディジタルコンテンツのコピー防止のための「電子透かし技術」について述べる。

インターネットの世界では，絵画や写真などの情報をディジタル化し，配布するコンテンツビジネスが普及しつつある。ディジタルコンテンツは不正なコピーが容易で，著作権が侵されやすいことから，優良なコンテンツ

が出回らない，事業者の利益が圧迫されるなどの問題がある。そこで，配布先情報などを，コンテンツに見えないように埋め込むことにより，不正コピーを抑止し，著作権を守るのが「電子透かし(Digital Watermark)」である[4]。不正コピーから検出された配布先の相手とは，以後，取り引きしないなどの対応により，不正コピーの増加を防ぐことができる。

4 日立製作所のセキュリティ技術

日立製作所は，高いセキュリティの実現のために，10年以上前から暗号や電子捺印などの技術開発を先行的に行ってきた(**図2**参照)。これらの技術のうち，主なものについて以下に述べる。

4.1 暗号技術

日立製作所は，共通かぎ暗号として「MULTIシリーズ」を開発してきた(**表2**参照)。MULTIシリーズの一つが「MULTI2暗号」であり，アルゴリズムを公開した，レディメイドの方式である。DESなどに比べて暗号処理速度が5倍程度速く，また，安全性の重要な尺度であるかぎ長が長い(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)という特徴を持つ。各種のソフトウェア製品に組み込まれるとともに，ディジタル衛星放送の暗号化の日本標準として採用され，“SKY PerfecTV！”や“DIRECTV”などの受信機のLSIに組み込まれ，利用されている。

また，アルゴリズムを秘匿し，ユーザー向けにイージオーダーの形で開発したものに，“MULTI4”や“M6”などがある。M6暗号は，情報家電製品などでも利用できるように，小さなハードウェアで高速な処理を可能としたものである。日立製作所を含む企業などが参加した“CPTWG(Copy Protection Technological Working Group)”という国際的な団体が，IEEE1394ホームバス用のベースライン暗号として採用している。

さらに，日立製作所は，21世紀の共通かぎ暗号として，“M2000”などの開発も進めている。

一方，公開かぎ暗号としては，だ円曲線暗号方式の一つである“ELCURVE”を開発し，わが国初の暗号ソフトウェア製品を実現した。この製品は，ディジタル署名(電子捺印)やかぎ配送などの従来の公開かぎ暗号の機能だけでなく，一度の処理で長文のデータを暗号化できる機能を持っている。また，ICカードの中で，ディジタル署名を高速で作成する機能も実現している。

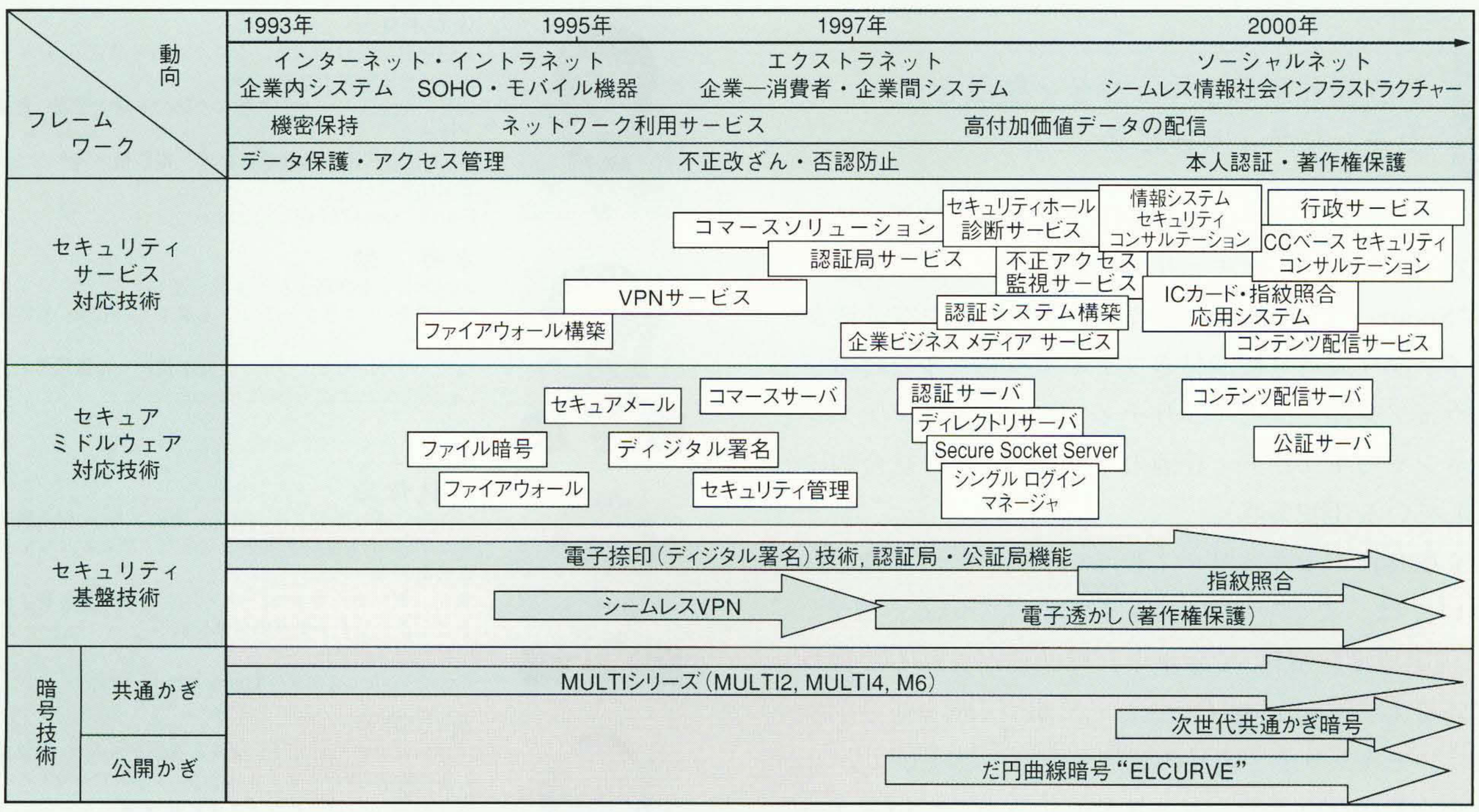


図2　セキュリティ技術の研究開発のロードマップ

日立製作所は，暗号技術，セキュリティ基盤技術，セキュアミドルウェア対応技術，セキュリティサービス技術の研究開発を先行的に実施してきた。

表2 日立製作所の共通かぎ暗号（MULTIシリーズ）
MULTIシリーズには，MULTI2やMULTI4，M6，M2000などがあり，さまざまな目的に合致するものを用意している。

名 称	アルゴリズム	位置付け	備 考
MULTI2	完全公開	規格量産品（レディメイド）	ディジタル衛星放送暗号化日本標準
MULTI4	非公開	半規格注文生産品（イージーオーダー）	——
M6	一部非公開	MULTI4の一具体例（ただし，軽量版）	IEEE1394バス業界ベースライン暗号
M2000	完全公開	規格量産品（レディメイド）	次世代暗号

4.2 その他の技術

ICカードと指紋照合技術を組み合わせることにより，確実で効率的な個人認証を行う技術を開発してきた[5]。また，コピー防止のために，静止画や動画などに電子透かしを挿入する技術を開発中である[6]。さらに，ファイアウォールが多重に設置された環境下で，一度ログインすれば，多重のファイアウォールを経由してエンド－エンドで暗号通信を行う「シームレスVPN(Virtual Private Network)」の機能を開発した[7]。

上記のほか，**図2**に示すように各種のセキュリティサービス対応技術や，セキュアミドルウェア対応技術の研究開発も行ってきた。

5 日立製作所のセキュリティ製品とセキュリティサービス

日立製作所は，開発した技術を生かして，情報システムに対する総合的なセキュリティ製品・サービス体系である“Secureplaza”の下に，暗号ライブラリや電子透かしライブラリ，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と，セキュリティ システム インテグレーションやセキュリティ評価のサービスなどを総合的に提案している(**図2**参照)。

日立製作所のセキュリティ製品やサービスのそれぞれについては，この特集の別論文で述べている。また，ISO(国際標準化機構)で今年中に標準化がされると言われている“CC(Common Criteria)”に基づくセキュリティ評価は，セキュリティ製品の製造メーカーだけではなく，国外の企業のネットワークと接続しようとしているユーザーにも影響が非常に大きいと考えられる。詳細はこの特集の「情報システムに対するセキュリティ国際評価基準の動向と日立製作所の対応」で述べる。

6 おわりに

ここでは，情報システムセキュリティ対策の概要と，日立製作所の情報セキュリティに対する取組みについて述べた。

日立製作所は，Secureplazaをさらに充実することにより，今後も高いセキュリティを確保するための手段を提案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) 佐々木：インターネットセキュリティ入門，岩波新書(1999)
3) 宝木，外：ファイアウォール，インターネット関連技術について，昭晃堂(1998)
4) 池田監修：デジタルサービス革命，日刊工業新聞社(1998)
5) 織茂，外：セキュリティシステムにおけるICカードの活用，日立評論，**80**，4，363～368(平10-4)
6) 吉浦，外：電子透かしとその応用，日立評論，**80**，7，511～516(平10-7)
7) 萱島，外：多段ファイア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(1997-3)

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 セキュリティシステム研究センタ 所属
現在，セキュリティシステムの研究と研究管理に従事
工学博士
IEEE会員，情報処理学会会員，電子情報通信学会会員，電気学会会員
E-mail：sasaki @ sdl. hitachi. co. jp

水野 勉
1978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 アプリケーション基盤本部 言語・図形設計部 所属
現在，暗号，セキュリティ，電子透かしの製品開発に従事
E-mail：mizun_ts @ soft. hitachi. co. jp

小林偉昭
1972年日立製作所入社，情報・通信グループ 新事業推進センタ ネットワーク事業推進室およびセキュリティ事業推進室 所属
現在，インターネットプロトコル主体のネットワーク事業とセキュリティ事業の推進に従事
情報処理学会会員
E-mail：h-kobayashi @ comp. hitachi. co. jp

畠山靖彦
1978年日立製作所入社，情報・通信グループ 情報システム事業本部 情報システム事業部 ネットワーク&サービス本部 ネットワークビジネス企画部 所属
現在，ネットワーク事業の企画に従事
E-mail：yhatake @ system. hitachi. co. jp