TREND 情報セキュリティ技術の動向 ―コア技術，キーコンポーネント，応用システム

Information Security Technologies ―Core Technologies, Key Components, and Application Systems

川村　信一　KAWAMURA Shin-ichi
才所　敏明　SAISHO Toshiaki

情報セキュリティ技術は，守りの技術としてだけでなく攻めの技術としてさまざまな新サービスを実現可能にしている。ここでは，セキュリティ技術を要素技術，キーコンポーネント，応用システムに分けて説明する。要素技術では暗号，暗号プロトコル，電子透かし，本人認証，耐タンパーを，キーコンポーネントではLSIとICカードを取り上げる。応用システムではこの特集で論述している電子印紙，IEEE1394コピー防止，コンテンツ配信システム，有料モバイル音声放送，BSディジタル放送，EC／電子決済システム，プラント制御システムを概説する。

This paper describes the trends in information security technologies. First, it explains the core technologies, which include cryptography, cryptographic protocols, digital watermarking, biometrics, and tamper resistance. It then comments on key components, such as LSIs and smart cards, necessary for building secure systems. Finally, it describes the application systems Toshiba has been developing; namely, the electronic revenue stamp, the copy protection system for the IEEE1394 bus, electronic content distribution systems, the pay-mobile broadcasting system, digital broadcast satellite systems, electronic commerce systems, and plant control systems.

“守り”から“攻め”に

情報システムは社会システムの中枢を担い，私たちの生活にとってなくてはならないものとなっている。システムのわずかなそごや故障により生じた不具合が，私たちの生活に重大な損失をもたらす可能性が高まっている。したがってシステムは，“故障や災害”が発生しても所定の動作をできる限り維持し続け，その被害を最小限に抑えなければならない。これは情報システムの“信頼性”にかかわる問題であるが，広い意味ではこれも情報セキュリティに含めることがある。

しかし，システムに対する脅威は構成する機器・ソフトの故障や地震や台風などの災害だけではなく，“故意や過失”のように人間を要因としてもたらされることも多い。しかも故意の人間が相手の場合，信頼性対策とはまったく異なる対策が必要となる。相手は知力の限りを尽くすハッカーかもしれないからである。このような人間を要因とする情報システムに対する脅威への対策が狭義の情報セキュリティ技術である[1]。

しかし，セキュリティ技術を脅威に対する対策という，“守り”の側面だけで捕らえるのは不十分である。例えば，電子商取引システムのようにネットワーク上での情報のやり取りにより商取引を行うシステムは，セキュリティの保証なしには成り立たない。これは，ユーザーがセキュリティ機能を意識するようなシステムが必要だといっているのではない。むしろ，セキュリティ機能は見えないほうが良い。

それにもかかわらず，セキュリティの保証なしには商取引をネットワーク上で行うことなど考えられない。セキュリティ技術は既存のシステムを守るためだけでなく，セキュリティ技術なしでは成立し得なかった新サービスを実現可能にするという，“攻めの技術”としての意義をもつ。セキュリティ技術があって初めて実現できるサービスは，電子商取引だけにとどまらない。

暗号，透かし，個人識別，耐タンパーがコア技術

では，情報セキュリティを支えるコア技術とは何であろうか。それは暗号技術であり，電子透かし技術であり，本人認証，さらに耐タンパー技術である。また，キーコンポーネントとしてセキュリティ向けLSIやICカードがある(図1)。

暗号アルゴリズム

暗号は情報セキュリティのもっとも基本的なコア技術である。DES方式(注1)やRSA方式(注2)といった単独の暗号アルゴリズムの評価尺度は安全性と処理速度の二つに集約できる。

(注1) DES方式
77年に米国商務省が制定した標準の共通鍵(かぎ)暗号方式。金融分野を中心に米国外でも広く利用されてきた。

(注2) RSA方式
もっとも広く利用されている公開鍵暗号方式。

暗号方式の安全性

多数の暗号方式が提案されているが，それらは，共通鍵(秘密鍵)暗号方式，公開鍵暗号方式，のいずれかに分類される。

共通鍵方式の場合には，80年代半ば以降提案された差分攻撃や線形攻撃に対する耐性がどの程度あるかが安全性の目安となる。これらの攻撃法は，よく選ばれた多数の入力を暗号アルゴリズムに与え対応する出力を解析することにより，鍵を探索する強力な攻撃法である。

なお，共通鍵方式でもっとも広く用いられてきたDES方式は，鍵長が56ビットと短く，現在では差分・線形攻撃を用いなくとも，専用ハードウェア(通称DES Cracker)で直接鍵を総当りすることにより数日以内で鍵の探索が完了する。これに代わる方式として，鍵長がDESの3倍までとれるトリプルDES方式，米国がDES方式の後継アルゴリズムとして公募し現在絞込みを行なっているAES(Advanced Encryption Standard)方式などが有望である。

一方，公開鍵方式の場合は，従来から知られている数学上の困難な問題に安全性の根拠を帰着させるような構成が理想的であり，すでにいくつかの方式の安全性がそのような形で証明されている。同様な手法は暗号プロトコルに対しても適用される。

ただ，もっとも有名で広く使われているRSA方式は，素因数分解問題がやさしければ解読できることは知られているものの，素因数分解問題と同程度に難しいか否かは示されていない。

しかし，RSA方式はすでに提案から20年以上にわたり多数の研究者が解読を試み成功していないため，RSA方式は安全であるということを前提としてそれ以外の方式の安全性を示すアプローチもある。

なお，暗号解読が新聞などでセンセーショナルに報道されることがあるが，その技術的意義を読み取るにはどのような条件の下で何ができたのかを注意深く調べてみる必要がある。暗号解読の懸賞問題についても同様の注意が必要である。

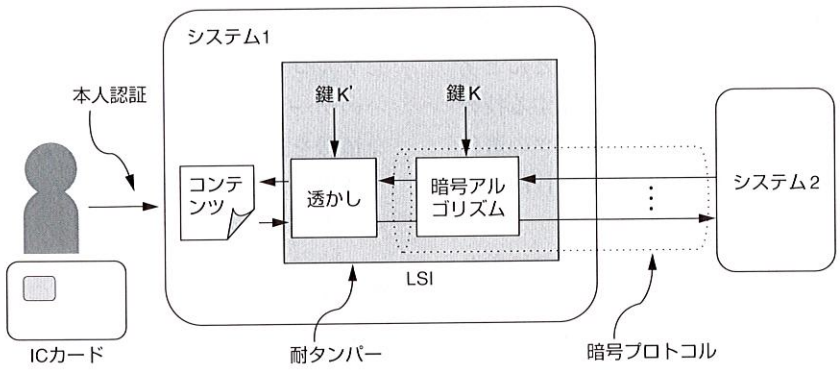

図1．情報システムのセキュリティコンポーネント　暗号，暗号プロトコル，透かし，本人認証，耐タンパーがコア技術である。
Security components for information systems

暗号方式の研究発表が，学会のような公の場で行われるようになったのは70年代半ばからであり，多くの研究者の努力により現在までに暗号方式の安全性を厳密に評価する理論体系がかなり整備されてきた(囲み記事参照)。

ここで暗号アルゴリズムの厳密な安全性がユーザーにとってどの程度の意味をもつのか，といった疑問をもたれる読者がいるかもしれない。しかし，冒頭に述べたように，情報システムが社会システムの中枢を構成する以上，その土台となるアルゴリズムの安全性評価があいまいでは，社会システムそのものが揺らぐことになる。

実際，ある規格書(注3)に採用されていた暗号方式に攻撃法が発見されたため，安全性の根拠が示されている別な方式に置き換えられた例もある。最先端の理論がほとんど時を経ずに標準的方式の選定に適用されるという活気が現在の暗号研究にはある。

暗号のもう一つの評価尺度である処理速度については，既存の方式をより高速に実装する計算アルゴリズムの研究と，従来方式と同じ安全性でありながら処理速度が速い新方式を構成する研究が活発に行われている(図2)。

■暗号プロトコル

通信において，ある目的を達成するためにあらかじめ定められたルールに従って，送信者と受信者がメッセージをやり取りすることをプロトコルと呼ぶ。特に，送信者または受信者の処理に暗号アルゴリズムを含むようなプロトコルを，ここでは暗

(注3) 規格書
RSA社のPKCS#1第1版。修正版の第2版が公開されている。

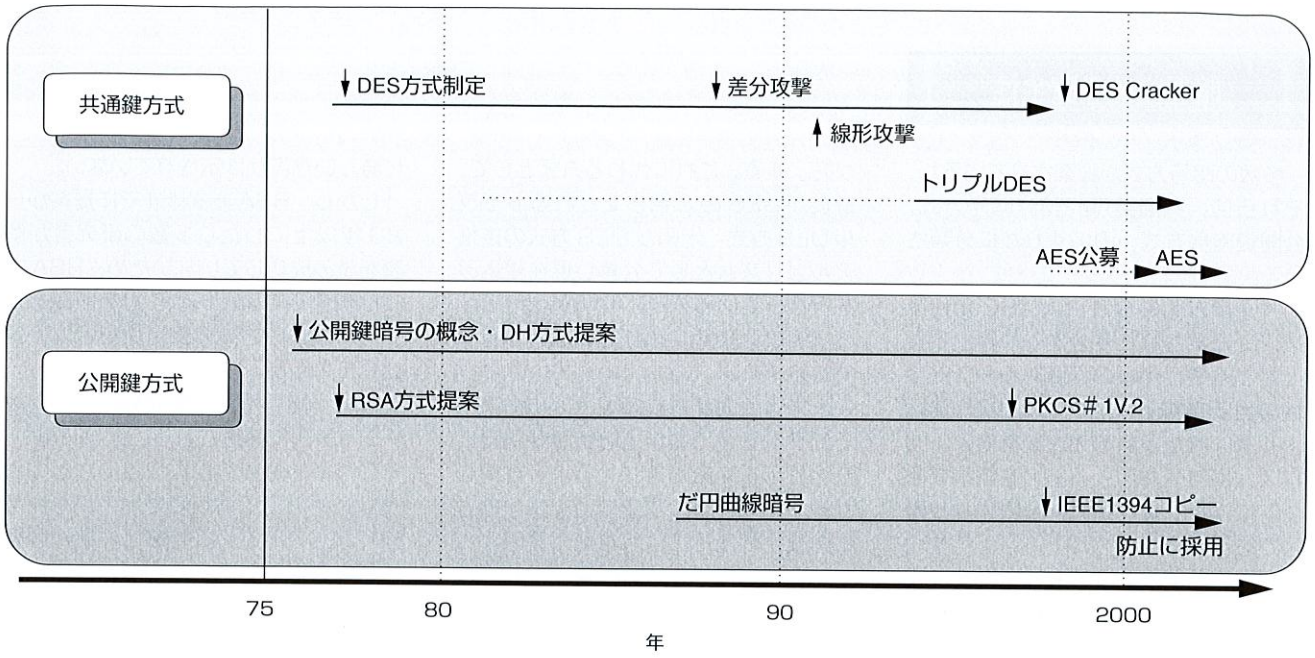

図2．現代暗号アルゴリズムの略年表　暗号の研究発表は70年代半ばから本格化し，近年一層活発となっている。
Brief history of contemporary cryptography

号プロトコル(注4)と呼ぶ。

どのような暗号アルゴリズムもプロトコルのなかで使われる。また，アルゴリズム単体では安全な方式も，プロトコルのなかでの使い方を誤ればアタックされてしまうことがある。暗号プロトコルの研究では実現する機能の有用性とプロトコルの安全性が重要な課題となる。

近年注目を集めている電子マネーは暗号プロトコルの集大成と位置付けられる。電子マネーが満たすべき偽造や二重使用の防止といった複数の要件を整理し，それらの要件が(できれば証明可能な形で)保証されるようプロトコルを設計することで，いくつかの代表的な電子マネーのプロトコルが実現されてきた。

電子マネーのほかに，電子投票，オークションなど，やはり厳密な形で安全性を保証できる方式が研究され実用化もされている。

■電子透かし

電子透かしとは，動画や音声，静止画といったいわゆるコンテンツ情報に対して，その品質をほとんど劣化させずに付加情報を添加する技術である。現在は，コンテンツの著作権保護や不正コピー抑止を目的とする利用法が検討されている。

暗号は重要な情報を守るのにきわめて効果的であるが，いったん復号された情報はそれ以後，保護の施しようがない。例えば，ディジタル化された動画を衛星で配信するシステムを考えよう。通信路上での傍受は暗号化して送受信することで防止することができる。しかし，受信端末でいったん復号してディジタル情報になってしまうとそれ以後のコピーや加工は容易である。

そこで，コンテンツそのものにその著作権者名や受信者名を埋め込んでおき，著作権を守ろうというのが電子透かしの考え方である。

電子透かしの研究では，コンテンツの劣化が十分小さく付加情報の埋込みや検出が効率よく行えて，かつ埋込み情報が無効化されにくい透かしアルゴリズムを研究することが第一のテーマである。また，どのような情報を透かしとして埋め込み，どう運用するかといったシステム設計も，重要な研究課題である。

■本人認証

本人認証は個人識別とも呼ばれ，人物を特定する技術である。情報システムにおいて利用される本人認証の手段は，(a)記憶，(b)所有物，(c)バイオメトリクスの三つに大別される。記憶による認証ではパスワードや暗証番号が，所有物では磁気カードやICカードが代表例であり，すでに広く用いられている。

これに対してバイオメトリクス，すなわち指紋や声など生体情報に基づく本人認証技術は，これから本格的に普及する技術である。

従来バイオメトリクスを用いた本

(注4) 暗号プロトコル
公開鍵方式による暗号プロトコルの代表例として通信相手との間で秘密の鍵を共有するためのDiffie-Hellmanの鍵配送法(DH方式)がある。

人認証技術は装置の小型化やコストの面で，(a)や(b)の方法に比べ不利であったが，素子や部品の小型化，LSI化により普及の素地が整い始めた。

バイオメトリクスとしては指紋，指照合，手形，顔，網膜，虹彩，声，手書きサインなどさまざまな方法が考案されているが，認証の精度，装置規模，コスト，適した利用環境などに違いがあり，どの方式をどういう場面で利用するかの見極めが成功の鍵となる。

当社は従来から手がけている指照合と顔認識のほかに，音声による識別と手書きサインによる識別を新たに開発した。

バイオメトリクス特有の課題は，パスワードやカードと違い認証の過程で本質的に誤りが入り込む余地があることである。他人を本人と誤認する率を他人受入率，本人を他人と誤認する率を本人拒否率と言う。これら二つの誤りをいかに小さくするかが課題であるが，複数方式を組合せるのであれば個々の方式の誤り率はある程度大きくても実用に耐える。

■耐タンパー

耐タンパーとはtamper(いじること)できないという意味で，情報セキュリティの分野では装置やLSI，あるいはソフトウェアを不正目的で解析したり改造することが難しいことを指す。

暗号アルゴリズムを実装する場合，鍵や処理の途中結果を装置から読み取ることができると，どのように強い暗号アルゴリズムを用いても解読できてしまう。そのため少なくとも鍵とアルゴリズム全体を耐タンパーな形で実現しなければならない。暗号プロトコルや電子透かし，本人認証の実装においても耐タンパーが必要な部分が存在する。

耐タンパーについて，いくつか注意すべき点がある。一つは100％タンパリングを排除する手段はないという点である。英語で言えばtamper-registanceは適当な言葉と言えるがtamper-proofは実現し得ないと思ったほうが良い。

二つ目は，ハードウェア的な強度は同じであっても，そこに収める情報の重要性や装置の管理運用方法に依存して要求される耐タンパー性は変わるという点である。これは100％の耐タンパーは実現できないということと無関係ではない。

例えば，耐タンパー性があるといわれるICカードであるが，1枚のICカードが解析された場合に，システム全体に影響を及ぼすような重要な秘密情報を記憶させることは避けるべきである。

また，契約書などにより装置の所有者や管理者が特定されていて有効期限がある場合に比べ，売りきり商品は解析される恐れが大きい。また，装置の無効化の処理もできないため，相対的に耐タンパー性は低いと考えるべきである。

装置に実装された暗号アルゴリズムの解析手法として，近年フォールトベース解析，タイミング解析，消費電力解析が注目されている。これらは，1チップLSIに作り込めば耐タンパーは十分という安易な考え方が，必ずしも通用しないことを示しており対策が必要である。

ハードウェアによる耐タンパー技術に加え，難読化などの手法によりソフトウェアを耐タンパー化する技術も注目されている。

■キーとなるLSIとICカード

以上のようなコア技術を耐タンパー実装するために，LSIは重要なキーコンポーネントである。また，LSI化により比較的低コストで処理速度を向上させることもできる。

近年0.5μm以下のプロセスを用いれば公開鍵方式を含め暗号方式は，1チップ内にコンパクトに収めることができる。公開鍵方式，共通鍵方式混載の1チップLSIも提供可能であり，従来利用を考えなかった低価格の機器にも容易に導入することができるようになっている。

情報セキュリティのもう一つのキーコンポーネントとして，ICカードがある。ICカードは，電子マネーに利用されているコンタクト型，次期テレフォンカードに予定されている接点のないコンタクトレス型，両方のインタフェースをもつコンビカードなどに分かれる。

コンタクト型ICカードでは近年，RSA方式，トリプルDES方式，さらにだ円暗号方式も実装されている。これらの方式は現在考えられる最高レベルの暗号方式である。

現在はICカードの各種共通仕様の整備，JavaCard(注5)による多機能化対応，さらにCPUの高機能化が精力的に進められている。

■多岐にわたる応用システム

セキュリティ技術はユーザーが直接目にしたり，意識することは少ないが，多岐にわたるシステムに適用されている。今後は家電も含め，セキュリティ技術の入っていないシステムの方が珍しくなるであろう。

以下では，この特集で取り上げた各種応用システムのポイントを紹介する(図3)。

■電子印紙

行政サービスのオンライン化や情報化に対応して，その手数料支払いも電子化しようというのが電子印紙

(注5) Javaならびにその他のJavaを含む商標は，米国SunMicrosystems社の商標。

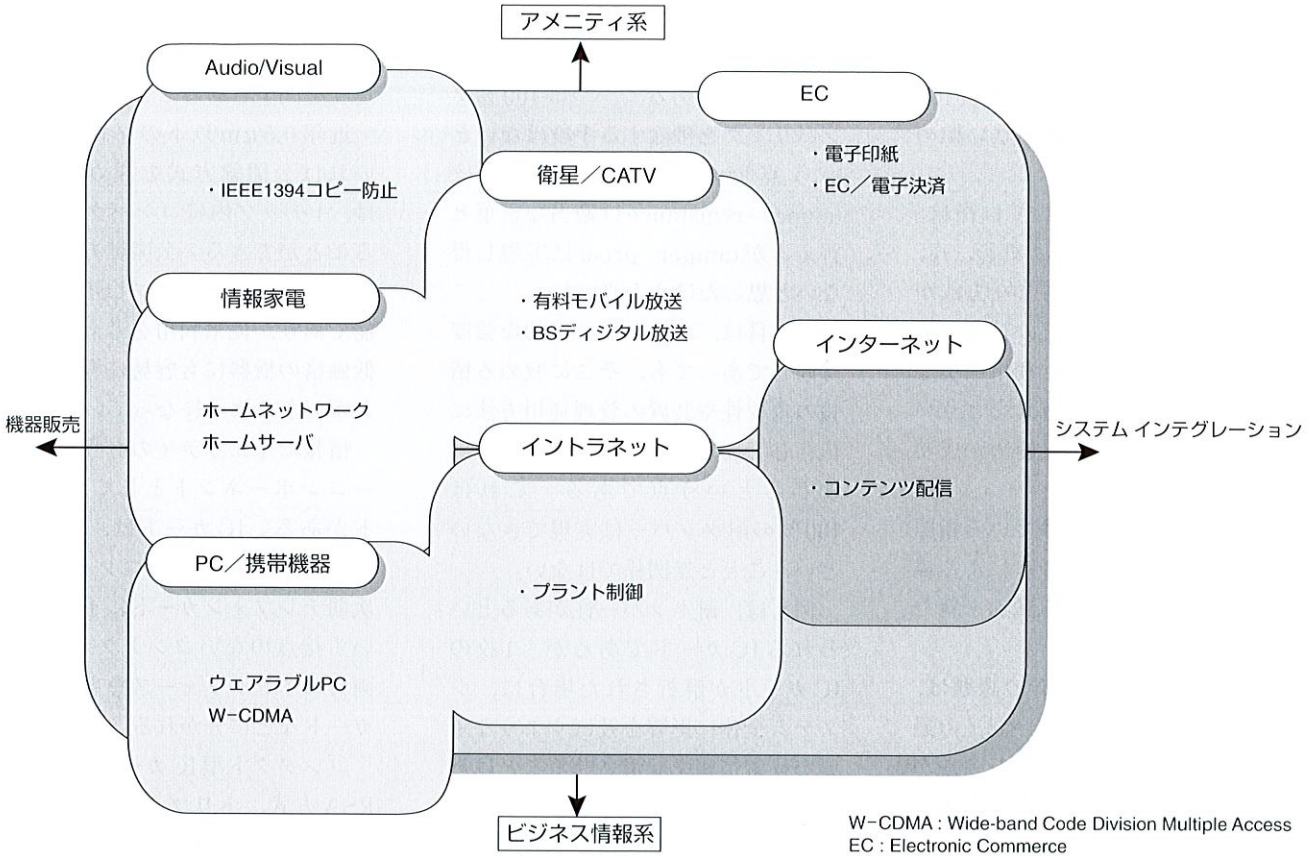

図３．ビジネス領域と対応するセキュリティシステム　横軸は当社が提供するソリューションの形態，縦軸は適用領域の性格を表している。・印はこの特集で掲載のシステム。
Business areas and corresponding security systems

のコンセプトである。

電子マネーは，買い物の対価の支払いをディジタル情報のやり取りにより実現しようというしくみであり，電子印紙も一種の電子マネーである。ただし，汎(はん)用の支払手段の実現をねらうのではなく，行政サービスの手数料支払いに場面を限定することにより，電子マネーで考慮されている転々流通性や匿名性といった要件が不要となり，よりシンプルで低コストなシステムが構成できる。

電子印紙の技術課題は克服されつつあり，法制度面の早急な見直しが望まれる。

■IEEE1394コピー防止システム

IEEE1394は，ホームネットワークの担い手として急速に普及し始めている次世代ディジタル通信路の伝送規格である。

今後，このIEEE1394がDVDプレーヤ，ディジタルVTR，ディジタル放送受信機などに装備され，機器間でディジタル化されたコンテンツをやり取りする可能性が高い。

ディジタル化されたコンテンツはコピーや加工が容易であるため，コピー制御情報や暗号を用いてコンテンツ提供者の権利を守る必要がある。その結果，価値あるコンテンツを適正なコストでユーザーに提供することが可能となる。

当社を含むメーカー５社が共同で設立したDTLA(Digital Transmission Licensing Administrator)では，98年９月よりIEEE1394のコピー防止技術のライセンス供与を開始している。

■コンテンツ配信システム

インターネットを利用して音楽や映像，テキスト，プログラムなど各種コンテンツを配信するビジネスが発展していくのは確実である。すでに音楽についてはコンテンツ提供者，システムオペレータ，メーカーが参加するSDMI(Secure Digital Music Initiative)において配信システムの要件と実現手段の議論が進められている。

このような状況を踏まえ，この特集では一般のコンテンツ配信システムがもつべき要件を整理している。また，将来セキュリティ機能が陳腐化した場合に機器の機能更新をソフトウェア的に安全に行うという，“リニューアル可能なセキュリティ機能”のコンセプトを提案し，その重要性を述べる。

■有料モバイル音声放送

“有料モバイル音声放送”の論文では，車など移動体に衛星から有料のコンテンツを供給するシステムの視聴制御と，課金部のセキュリティについて考察している。

視聴者が，ある番組やチャンネルを視聴する契約を結んでいるか否か，また視聴料を支払っているか否かによって視聴をコントロールする。そのために視聴を制御する情報を契約者端末に送らなければならない。

想定するモバイル放送では，契約者が多数であること，端末が常時受信状態とは限らないことから，従来の衛星放送とは異なる制御方法の提案が必要である。

■BSディジタル放送

放送衛星(BS)によるディジタル放送の開始が2000年に予定されている。BS放送では，一部有料放送が予定されており，その方式の標準化が(社)電波産業会(ARIB)で行われている。そこで考慮されている項目としては，加入者への契約情報を伝送する帯域の削減，受信機の低消費電力化の実現，受信機能とセキュリティ機能の分離などがある。

ディジタル放送では，セキュリティ技術の裏づけの下で，従来型の番組放送だけでなくデータ放送など新サービスが提供され発展していくと予想される。

■EC／電子決済

インターネットを用いた電子的取引情報を保護する簡便なしくみとして，SSL(Secure Socket Layer)の機能を用いて消費者と商店との間の通信を一括暗号化する方法がある。しかし，これは通信路上のデータを保護しているだけであり，消費者や商店が相互に相手を信用してよいかを確認するしくみは含まれていない。

通信路での安全性に加え，このような相互認証に十分配慮した決済プロトコルとしてSET(注6)がある。SSLベースの方式と異なり，SETは消費者・商店に加え金融機関も含むしくみである。

当社は，今後SETがインターネットを用いた電子決済方式の主流になるとの判断から，97年度の電子決済実験プロジェクトSCJ(スマートコマースジャパン)に続き，今年度のSCJパート2において，SETプロコトルの実装とICカードへの機能拡張を推進している。今後，そこでの経験を生かし電子決済システムの使い勝手と安全性の向上を実現して行く考えである。

■プラント制御システム

発電監視制御システムをはじめとする各種プラント制御システムは，従来メーカ固有のシステムアーキテクチャと，物理的隔離・保護によって守られてきたため，情報セキュリティ的配慮はあまりされてこなかった。しかし，ネットワーク化と機器のオープン化，マルチベンダー化に伴ない，セキュリティ上の脅威にさらされる機会が増大している。プラントシステムは，社会的にも重要な役割をすることが多く十分な対策を施す必要がある。

プラントセキュリティの導入にあたっては，性能の劣化，保守員の負担増，コストアップ，マルチベンダー化への逆行などが発生しないように十分配慮した設計が必要である。

■家庭とモバイルでさらなる展開

以上，この特集全体を通した技術背景を説明し，個々の記事に対応した技術動向を述べた。この特集の構成に見るように，情報セキュリティ技術は要素技術の研究開発とシステム開発が両輪となって進展している。

今後はこの特集で取り上げなかった，情報家電やモバイルインターネットの分野における情報セキュリティ技術の研究・開発，さらにシステムインテグレーションがますます重要となっていく。

文　献

(1) 才所敏明，他. 情報犯罪防止に向け技術開発加速. 東芝レビュー，52，2，1997，p.4-8.

川村　信一
KAWAMURA Shin-ichi,D.Eng.
研究開発センター コンピュータ・ネットワークラボラトリー主任研究員，工博。暗号・セキュリティ技術の研究・開発に従事。電子情報通信学会，情報処理学会，IEEE，IACR，SITA会員。
Computer & Network Systems Lab.

才所　敏明
SAISHO Toshiaki
情報・社会システム社 SI技術開発センター 戦略企画担当参事。
情報セキュリティの研究・開発に従事。情報処理学会，CSI，ACM，IEEE会員。
System Integration Technology Center

(注6) SETはSecure Electronic Transaction LLCの商標。