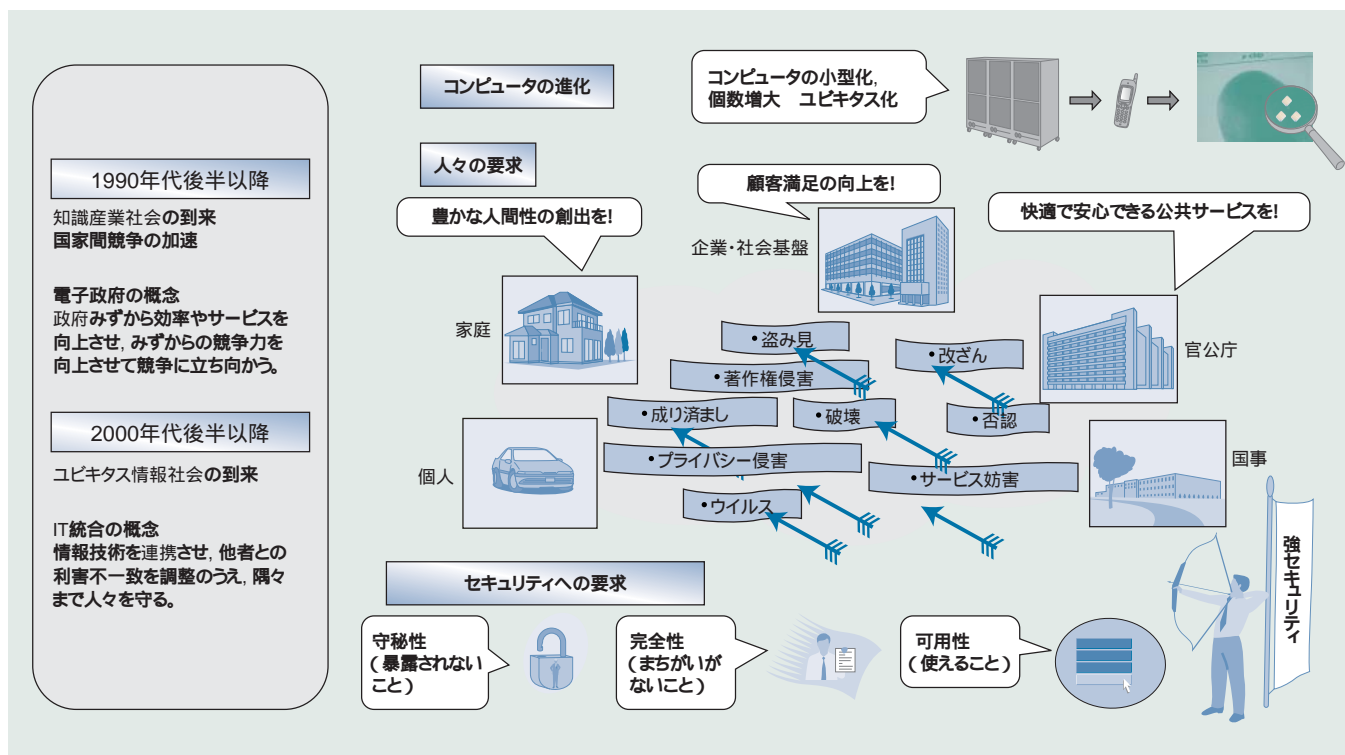


# 情報セキュリティ技術

## Information Security Technologies

宝木 和夫 Kazuo Takaragi



注:略語説明 IT(Information Technology)

**情報セキュリティの進展** 国家や企業のシステムでIT化が急速に進む一方で、盗聴、成り済ましなど、人為的な不正行為の危険性が增大している。これに対応して、守秘性など個別のセキュリティ機能が開発され、将来的には統合化され適用されていく。

現在、ITの最たるインターネットは、国内企業のほぼすべて、一般家庭でも10世帯のうち9世帯は利用しており、ITは水道や電気に匹敵する普及に近づいている。しかし、ITシステムは人為的な不当行為に対して弱いという問題があり、情報セキュリティへの要求が生じている。情報セキュリティは、「情報が許可なく読まれたり、書かれたりすることを防ぐこと」と定義され、情報の基本処理からサービスまで幅広く関係する技術である。

人々のITへの依存度が高まるほど、情報が暴露されないこと(守秘性)、まちがいがいいこと(完全性)、使えること(可用性)といったセキュリティへの要求も高まっている。

日立製作所は、「セキュリティはいずれ破られる」との通念を覆す確固とした対策技術、すなわち、強セキュリティの技術を開発中である。これをいたるところに適用することによって、安心して安全な社会の実現に貢献することを目指す。

## 1 はじめに

1990年代の後半以降、世界中の先進国、新興国にIT(Information Technology)化の波が押し寄せる中、IT化が進むにつれて、内部犯罪の多発、情報の漏えい、手口が巧妙化するハッキング、被害スケールの拡大といった問題が次々と生じてきた。わが国は2003年に発表した「e-Japan戦略II」で、「世界最高水準の高信頼性社会の構築」を基本目標として戦略を進めた。また、これと同じアナロジーで、「業界最高水準の高信

頼性会社の構築」を目標とする企業が増えている。いずれにおいても、情報セキュリティの重要性は増すばかりである。日立製作所は、1980年代から情報セキュリティの研究開発を本格的に進め、今日に至るまでさまざまな技術を蓄積してきた。

従来、情報セキュリティの対象となるシステムの分類としては、関係者だけの閉じたネットワークと、不特定多数が参加するオープンなネットワークの二つに分類して議論されてきた。しかし、コンピュータが小型化し、個数も増大して、社会のあらゆる側面に影響を与える

ようなコピキタス情報社会には、さらに強固な情報セキュリティが必要になる。

ここでは、情報セキュリティが適用されるシステムを4タイプに分類し、それぞれのタイプで基盤となるべき技術、共通的に使われる暗号、認証技術の最新の開発状況、および今後進むべき方向性について述べる。

## 2 情報システムとセキュリティ技術の変遷

セキュリティを必要とするシステムの構造は、四つのタイプに大別して考えることができる(図1参照)。

タイプ1は、従来から銀行オンラインなどで使われているようなネットワークであり、大きな装置と多数の端末がつながり、かつ、身内どうしで通信を行うような閉じたシステムである。ここでは、データの盗聴や改ざんを防ぐために暗号が使われる。暗号の主な役割は、悪意を持つ人にデータの盗聴や改ざんをされないようにしたいという「守り」が主体のものである。

タイプ2は、最近までのインターネットのように、多数のコンピュータを主に有線ケーブルでつないで通信を行うようなオープンなシステムである。ここでは、上述したデータの盗聴や改ざんを防ぐ暗号のほか、電子商取引などで必要となる本人確認のために、デジタル署名やPKI(Public Key Infrastructure:公開鍵基盤)などの認証技術が使われる。認証技術の主な役割は、データのやり取りに信用性を導入することにより、新しいビジネスの創生を可能にするといった「攻め」の要素が入る。

タイプ3は、今、正に始まるようしているコピキタス情報時代のネットワークがこれに相当し、無線通信機能を持つ多くのコンピュータがインターネットにつながり、世界中のコンピュータと通信し合うシステムである。ここでは、上述した、データ盗聴と改ざんを防ぐ暗号や本人確認を行うデジタル的な認証技術に加え、生体認証が使

れるようになる。生体認証の主な役割は、コピキタス情報時代においては、デジタル的認証だけでは本人に成り済ますという不正行為を十分に防ぎきれないので、これを補って本人確認の安全性を増やすことである。

タイプ4は、将来(2010年以降)の新段階のネットワークがこれに相当する。無線通信機能を持つ機器がさらに小さくなり、場合によっては肉眼では見えにくい小さくなり、数も増大し、世界中のコンピュータと通信し合うシステムである。このタイプのシステムでは、機器間の認証が頻繁に行われる一方で、本人がいつ、どこで、何をしたかという個人情報が不用意に蓄積されるという危険性が増える。そのため、上述したような暗号や認証技術に加え、プライバシー保護対応ID(Identification:識別情報)管理が必要になる。プライバシー保護対応ID管理の役割は、本人確認のたびにさらけ出されるIDを適宜変更する(実名、別名間の切り替えなど)管理方法などにより、危険な形で個人情報が蓄積されることを防ぎ、プライバシー面でも安心して安全な社会を構築することである。

次に、すべてのタイプで基盤となる共通鍵暗号と公開鍵暗号について述べる。





## 3 共通鍵暗号、公開鍵暗号

1970年代末に、米国で開発された共通鍵暗号“DES(Data Encryption Standard)”と公開鍵暗号“RSA”(Rivest, Shamir, Adelman)は、その後しばらくデファクトスタンダード(実質的世界標準)として使われた。わが国では、日立製作所が独自に開発した共通鍵暗号“MULTI2(Multimedia Encryption 2)”が、唯一のデジタル衛星放送用の標準的暗号となった。最近では、性能や安全性を向上させた米国暗号標準“AES(Advanced Encryption Standard)”や、だ円曲線暗号も使われ始めている。さらに今後は、コピキタス情報時代にふさわしい小規模で高速なストリーム暗号や、高い安全性を持つ耐タンパ(耐侵入)暗号実装技術が求められるようになると思われる。

### 3.1 小規模、高速性を実現するストリーム暗号

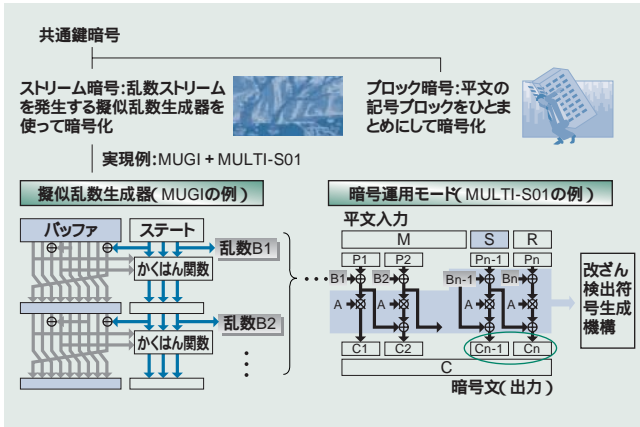
データ通信装置やハードディスク装置の小型化が急速に進む中で、それらデバイスで扱われるデータサイズは飛躍的に大きくなっている。このような情報技術で支

) RSAは、RSA Security, Inc.の商標である。

	1990年	2000年	2010年	
情報セキュリティシステムの変遷	メインフレームの時代 (特定システムセキュリティ)	インターネットの時代 インターネットセキュリティ	コピキタスの時代 (第1期) セキュア情報ライブライン (第2期) 高度セキュリティとプライバシー	
セキュリティを必要とするシステム	タイプ1 •銀行端末セキュリティ •防衛システム 	タイプ2 •コミュニケーション手段 •電子商取引 	タイプ3 •社会基盤(モバイル機器、情報家電、情報ライブライン) 	タイプ4 •個々の生活の隅々(ウェアラブル) 
対策を実現する技術	共通鍵暗号・公開鍵暗号 デジタル署名・PKI バイオメトリクス プライバシー保護対応ID管理			

注:略語説明 PKI(Public Key Infrastructure), ID(Identification)

図1 システムのセキュリティを支えるさまざまな暗号・認証・管理技術  
情報セキュリティを必要とするシステムの構造が急速に変化するとともに、新たなセキュリティ技術が求められている。



注:略語説明 MUGI( Multi Giga Cipher ), MULTI-S01( Multimedia Encryption Stream 01 )

**図2 ストリーム暗号の概要**  
 ストリーム暗号は、擬似乱数生成器と暗号運用モードの二つの部分から構成される。前者は、平文とは独立に処理が行われる点が特徴である。

えられる社会においては、取り扱う情報の高速な暗号化が重要な技術課題となる。

ストリーム暗号は、ランダムなデータストリームを発生する擬似乱数生成器を使って暗号化を行う共通鍵暗号の一種である(図2参照)。ストリーム暗号には、上述のDESやAESのようなブロック暗号と比べ、小規模での実装が可能であることなどのメリットがある。

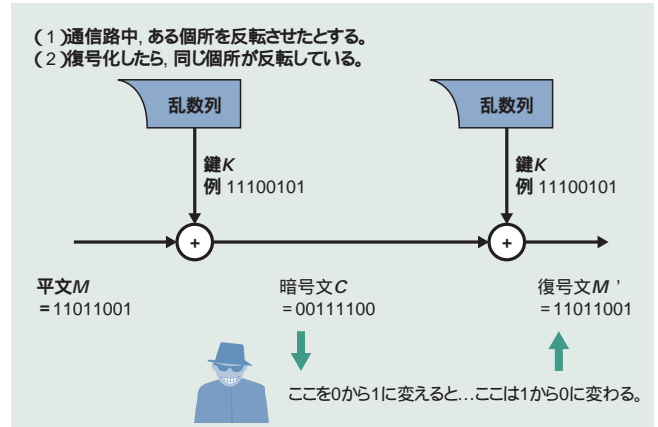
日立製作所のストリーム暗号“MUGI( Multi Giga Cipher )”は、それまでの研究成果の多くが凝縮されたブロック暗号AESの優れた部分を取り入れつつ、ストリーム暗号特有の事前処理が可能という性質を生かす設計となっている。その結果、高い安全性を保ちながらも小規模、高速な処理を達成した<sup>1),2)</sup>(表1参照)。

さらに、日立製作所は、新しいストリーム暗号運用モード“MULTI-S01( Multimedia Encryption Stream 01 )”という技術も開発した<sup>3)</sup>。従来のストリーム暗号運用モード(排他的論理和型)では、守秘性は実現されたものの、完全性は実現されなかった。MULTI-S01では、改ざん検出符号生成機構を内部に持たせることにより、守秘性と完全性の両方を実現した(図3参照)。これにより、例えば、電子商取引などで重要データを送る場合に、伝送路上で、盗み見を防ぐばかりでなく、データが

**表1 実装結果の比較**  
 ストリーム暗号‘MUGI’とブロック暗号‘AES’の研究レベルでの実装結果の比較を示す。ストリーム暗号は、入力メッセージとは独立にLSI内でストリームの処理が可能のため、比較的小規模の回路で高速処理ができる。

	設計条件	論理規模 (Kゲート)	暗号加速度 (Gビット/s)
MUGI	速度優先	52.4	14.4
	規模優先	14.2	3.61
AES	速度優先	57.5	2.28
	規模優先	6.9	0.12

注:略語説明 AES( Advanced Encryption Standard )



**図3 排他的論理和運用モードの問題点**  
 通信路中で、ある個所を反転させたとして、復号化した場合には、同じ個所が反転している。

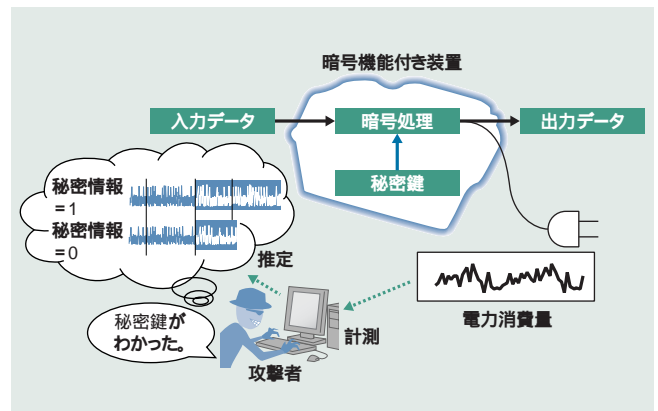
改ざんされた場合には、それを突き止めることもできるようになった。

MUGIとMULTI-S01は、ストリーム暗号としては初めてISO International Organization for Standardization)の国際標準になることが確定した。また、この技術の一部は、日立製作所の暗号ライブラリ‘Keymate/ Crypto’として提供されている。

今後、映像監視システムの暗号化などに適用するとともに、普及に向けた取り組みをさらに強化していく。

### 3.2 高い安全性を持つ耐タンパ暗号実装技術

現在、磁気カードは簡単に不正コピー(スキミング)がされ、本人が知らない間に使われるという被害があとを絶たない。しかし、磁気カードをICカードに置き換えても不正コピーを防ぐことはできない。不正コピーを防ぐには、ICカードに耐タンパ性を新たに持たせることが必要である。耐タンパ性とは、ICカード処理中に外部から電力消費量や電磁波形の計測を試みられても、中身



**図4 実装(サイドチャネル)攻撃の手口の例**  
 暗号機能付き装置の電力消費波形を観測することで、秘密鍵の数値を推定することが可能である。



表2 ICカードでの処理速度の比較

だ円曲線暗号「ECDSA」では、鍵長160ビットで測定し、株式会社ルネサステクノロジ製のICチップ「AE-4」での実装値で、毎秒20回の署名が可能である。一方、同等の安全性を持つRSAの1,024ビットでは署名生成に約1秒を必要とする。

	従来方式	日立製作所の新技術
暗号方式	RSA	ECDSA wNAF
処理	署名生成	署名生成
速度(毎秒署名回数)	1回	20回

注:略語説明 RSA(Rivest, Shamir, Adelman), ECDSA(Elliptic Curve Digital Signature Algorithm), wNAF(Width w Non-Adjacent Form:非隣接形態方法)

のデータがどのような数値であるかを知られないように保護策がとられていることである。

現在、ICカードに暗号機能を単純に実装しただけでは、耐タンパ性は得られない(図4参照)。日立製作所は、この課題に対応し、ICカード用にさまざまな耐タンパ技術を開発している。電力解析と呼ばれる最も基本的な実装攻撃を例にして、耐タンパ技術について以下に述べる。

実装する暗号の例として、電子認証で用いられる公開鍵暗号の一つであるだ円曲線暗号を取り上げる。だ円曲線暗号は、電子署名法で使用が認められた公開鍵暗号である。同じく電子署名法で認められたRSA暗号と比べて、ICカード実装時のコストパフォーマンスがよいなどの特徴があるだ円曲線暗号を安全に実装することができれば、ユビキタス情報時代の機器に向けた方式となる(表2参照)。

仮に、単純に、ICカード内でだ円曲線暗号を実行させようとすると、まず、ICカード内メモリに、0または1のビットが160個ほど並んだデータが格納される。これは、秘密鍵と呼ばれるもので、第三者に知られてはならない数値である。だ円曲線暗号では、単純な処理の場合に、秘密鍵を1ビットずつ読みながら処理する。しかし、対応するビットが1か0かによって、電力消費波形が大いに異なる(図4参照)。そのため、単純な実装では、外部に露出している入力端子にセンサを当てて観測されると、秘密鍵を知られてしまうおそれがある。

日立製作所は、この課題を解決するために、秘密鍵の数値の表現形態を0,1の2値ではなく、0,1,-1の3つの値で表現し、かつ、ビット幅 $w$ ごとに電力処理を同様化する方法、すなわち、幅 $w$ のwNAF(Width w Non-Adjacent Form:非隣接形態方法)を開発した。これにより、電力消費量の波形に秘密鍵の値を推定される手がかりはほとんど与えないようにすることで、だ円曲線暗号の処理を安全に行うことを可能にした。

今後、機器間の認証がさまざまな状況下で行われるようになると、wNAFのような特徴を持つ耐タンパ暗号

実装技術がいろいろな局面で使われるようになると予測されることから、早期の製品化を推進中である。

## 4 デジタル署名,PKI,生体認証

われわれは以前の日常生活で、「自分が自分であることをどのように証明すればよいか」などと思い悩むことはあまりなかった。しかし、タイプ2のインターネット以降では、状況は異なる。例えば、今、自分が、パスポートもなくいきなり外国に放り出され、しかも、周りを見知らぬ人しかいないとしたら、自分が自分であることを証明するのは容易でないことに気づくことになる。インターネット以降のバーチャル空間では、そういうことがいたるところで生じる。

一般に自分が自分であることを証明するのは、次のいずれかの方法による。

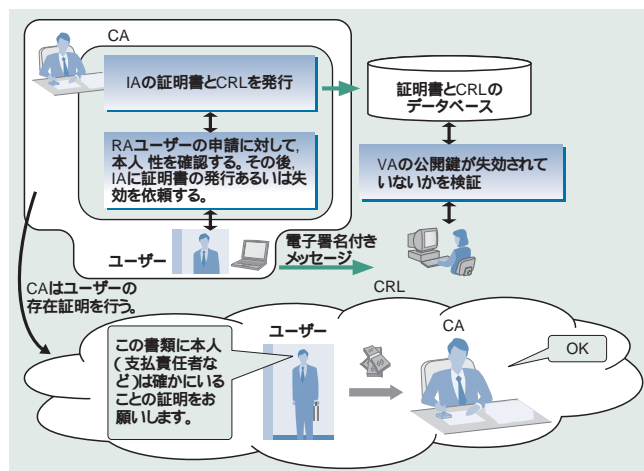
- (1)自分以外の人を作成した証明書を利用する。
- (2)相手の記憶を利用して証明してもらう。

電子的な契約締結システムや決済システムでは、利用者が正当な権限を持つ者であることを証明することが必要になる。しかし、(2)の相手の記憶による証明では、本人性の証明度が低いため、(1)の第三者認証によらざるをえない場合がよく生じる。

第三者認証の要になるのが、デジタル署名を用いたPKIである。

PKIでは、「そのユーザーは確かにうちの組織にいる」というような、デジタル署名付き証明書を発行するCA(Certification Authority:認証局)が設けられる。

ユーザーはその組織内で、その証明書を提示すれ



注:略語説明 CA(Certification Authority), IA(Issuing Authority), CRL(Certification Revocation List:証明書失効リスト), RA(Registration Authority), VA(Validation Authority)

図5 PKIの基本構造

PKIでは、「そのユーザーは確かに当組織に所属している」というような、デジタル署名付き証明書を発行するCA(認証局)が設けられる。

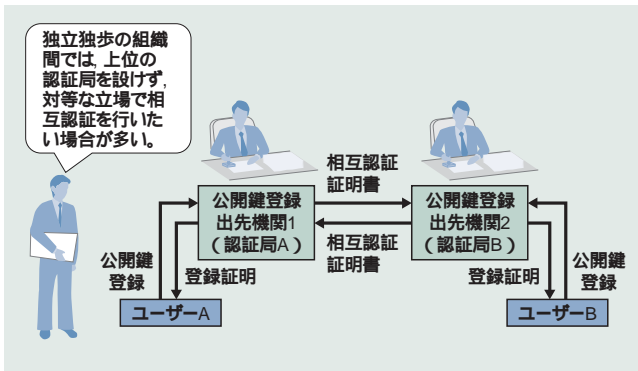


図6 認証局間の相互認証の仕組み  
異なる認証局が事前に相互認証を行い、その後、それぞれの認証局に属するユーザー間で相手認証を行う。

ば本人証明(自分が自分であることの証明)ができ、支障なく電子商取引を行える。ただし、認証局は何らかの理由により、その証明書は無効であるという失効証も発行しなければならない場合が生じる。確実に本人確認を必要とするような電子商取引においては、相手の証明書と失効証の有無のどちらも確認する必要が生じる(図5参照)。

さらに、電子商取引の範囲を広げ、異なる組織に所属するユーザー間で、電子商取引を行いたい場合は、組織間で事前に相互認証をしておくことになる。このようにすると、「友達の友達は友達」の論理で、例えば、連鎖した三つの認証パスを経由して、ユーザーAとユーザーBが認証(存在を確認)し合うことができる(図6参照)。

組織が三つ以上存在した場合も、同様の論理で、連鎖した四つ以上のパスが生じうる。

一つの認証局は、時には生じたり消えたりし、二つの認証局どうしは相互認証し合ったりしなかったりする、という動的変化のある環境になる。このような環境下で、あるユーザーが他のユーザーの存在を確認するためには、そのユーザーにたどりつくための、友達の手帳、すなわち、認証パスが存在するかどうかを確認しなければならない。この作業は、個人としてのユーザーにとっては煩雑な手間である。そのため、日立製作所は、個人に代わって認証パスの存在を探索し、証明書が有効であることの確認を行うCVS(Certificate Validation Server:証明書検証サーバ)をいち早く実用化し、PKIの発展に貢献している。

公開鍵暗号技術を利用して構築されるPKIは個人を認証する方式として有用であり、すでに住民基本台帳システムなどで用いられている。PKIでは、処理の最初に、ICカードの持ち主を確認するという、いわば、人と機械(ICカード)の間の本人確認が行われる。その後、

ネットワークを挟んで、機械(ICカード)と機械(サーバ)の間の相手認証が行われる。このどちらが欠けても認証の信用性はあやふやなものとなる。

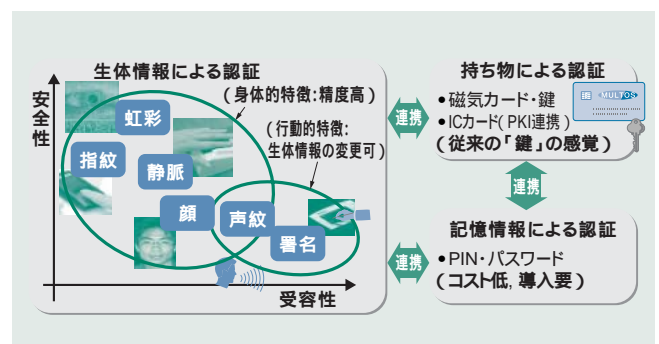
しかし、一般に、本人確認の手段として単に磁気カードやICカードのような持ち物、および暗証番号だけに頼る場合は、両方とも他人に比較的簡単に盗まれやすいというおそれがある。このため、本人確認技術の一つとして、生体認証が注目されている。生体認証は、本人確認に使われる情報と、本人そのものとの結び付きの強さに特徴がある。生体認証では、本人確認に使われる情報は利用者の体や動きの特徴であり、基本的に他人が持つことはできない。また、生体情報は「忘れない、無くさない」といった特徴があり、一定の安全性を保ちながら利便性向上に役立つと考えられている<sup>5)</sup>(図7参照)。

日立製作所は、銀行のATM(Automated Teller Machine:現金自動預け入れ払い機)での預金者の本人確認に適した指静脈認証の技術を開発した。これは、指の皮膚付近にある静脈のパターンを利用して本人確認を行うもので、利用できない人の割合が指紋などに比べて少ないことや、使用に際しての心理的抵抗感が少ないといった特徴があり、万人が利用する銀行などでの利用に適している<sup>6)</sup>。

## 5 プライバシー保護対応のID管理

「自分が自分であること(ID)を人に認めさせるのは簡単ではない」ということを前述した。しかし、タイプ4のユビキタス第2期に入ると、むしろ、個人のIDが頻繁に参照されるあまり、行動履歴をはじめとしたさまざまな個人情報ネットワークに蓄積されるというプライバシー侵害の危険性が増大する。

つまり、個人が自分の周りにあるコンピュータに自分



注:略語説明 PIN(Personal Identification Number)

図7 生体認証と他の本人確認法  
「忘れない、無くさない」などの特徴を持つ生体情報による認証は、他の特徴がある持ち物や、記憶情報による認証と連携して用いることができる。

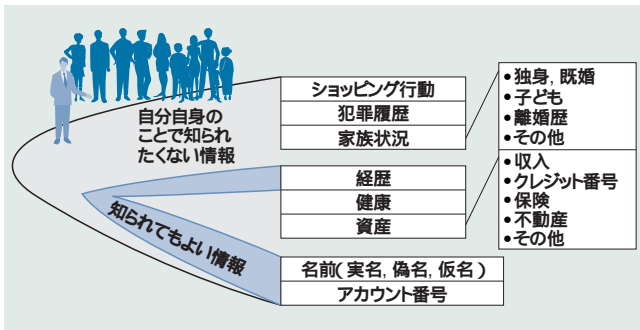


図8 IDに付随するプライバシー情報例  
本人が本人であることを知らせるIDには、名前だけでなく、経歴、健康、資産などさまざまな個人情報が付随する。

の名前(狭義のID、すなわち、実名、別名など)を伝えるときに、そのIDは、その個人に関するプライバシー情報がつながっている(図8参照)。

コンピュータと会話をするたびに、少なくともその名前の人がいつ、どこにいて、どういうサービスを頼んだかが知られることになる。このコンピュータが悪意の第三者に操られている場合、蓄積された情報を総合されて何らかの推論処理を行われると、その個人に関するプライベートな情報が知られてしまうおそれがある。

日立製作所は、ユビキタス情報時代の象徴となる「ムーチップ」のような小さなRFID(Radio-Frequency Identification)チップを世界に先駆けて開発してきた<sup>7)</sup>。それとともに、これらのハードウェアが普及した場合に、安全で安心な社会を築くためのシステムやソフトウェア方式もあわせて開発している。

例えば、本人確認のたびに露出されるID(実名、別名など)を適切に変更するなどの管理方法の開発や、きたるべきユビキタス未来社会の検討などを進めている<sup>8)</sup>(図9参照)。新たに、次々と生じ、悪質化する不正

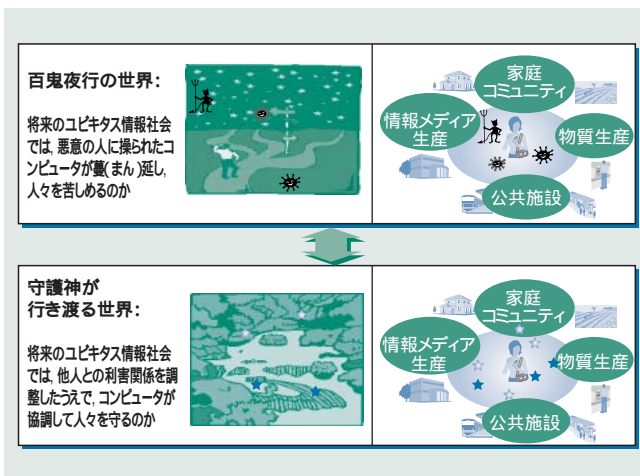


図9 将来のユビキタス情報社会の課題  
人々は、はるか古代において、やおよぶ神々と共存した思いがある。この潜在的希求イメージを参考に、新しいコンセプト、システムアーキテクチャを創造することが今後の課題となる。

行為の手口に対処するためには、守る側もそれに負けない対策技術の開発や、適切なセキュリティ技術を統合して臨機応変、かつ効果的に対抗できるようなシステムズアプローチが必要になると考えられる。

## 6 おわりに

ここでは、情報セキュリティが適用されるシステムを4タイプに分け、それぞれで基盤となるべき技術とともに、共通的に使われる暗号、認証技術の最新の開発状況について述べた。

これらに関連して重要と思われるコンピュータウイルス対策や、ISMS(Information Security Management System)、ファイアウォール、量子暗号などについては機会を改めて述べることにしたい。また、ストレージ、オペレーティングシステム、家電、電子文書、コンテンツ配信、有価証券関連など個別のシステムのセキュリティを確保するための応用技術も重要な課題であることを付け加えておく<sup>9)</sup>。

日立製作所は、今後も先進的な研究開発を続け、安全で安心できる社会の実現に貢献していく考えである。

おわりに、これらの研究の成果は、国内外の多くの方々から頂いたご指導、ご支援の賜物である。ここに深く感謝申し上げます。

### 参考文献ほか

- 1) D. Watanabe, et al.: A New Key Stream Generator MUGI, Fast Software Encryption( Feb. 2002 )
- 2) 大和田, 外: MUGIのハードウェア実装および評価, SCIS2005, 1E3-5 (2005.1)
- 3) S. Furuya, et al.: Integrity-Aware Mode of Stream Cipher, IECIE Transactions, Vol. E85-A No. 1 pp. 58-65( Jan. 2002 )
- 4) K. Okeya, et al.: The Width-w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks, RSA Conference Cryptographer's Track, LNCS 2612, pp. 327-341( Apr. 2003 )
- 5) 瀬戸: バイオメトリックセキュリティ入門, ソフト・リサーチ・センタ 2004.8 )
- 6) 宮武: 静脈パターンを用いた個人認証, 光学, 33巻, 8号, pp. 23 ~ 27 (2004.8)
- 7) K. Takaragi, et al.: An Ultra Small Individual Recognition Security Chip, IEEE MICRO, November - December 2001, pp. 43-49
- 8) やおよぶプロジェクトホームページ, <http://www.8mg.jp/>
- 9) 日立製作所システム開発研究所ホームページ <http://www.sdl.hitachi.co.jp>



宝木 和夫

1977年日立製作所入社, システム開発研究所セキュリティ基盤技術研究センタ センタ長  
現在, 情報セキュリティの研究開発に従事  
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: takara@sdl.hitachi.co.jp