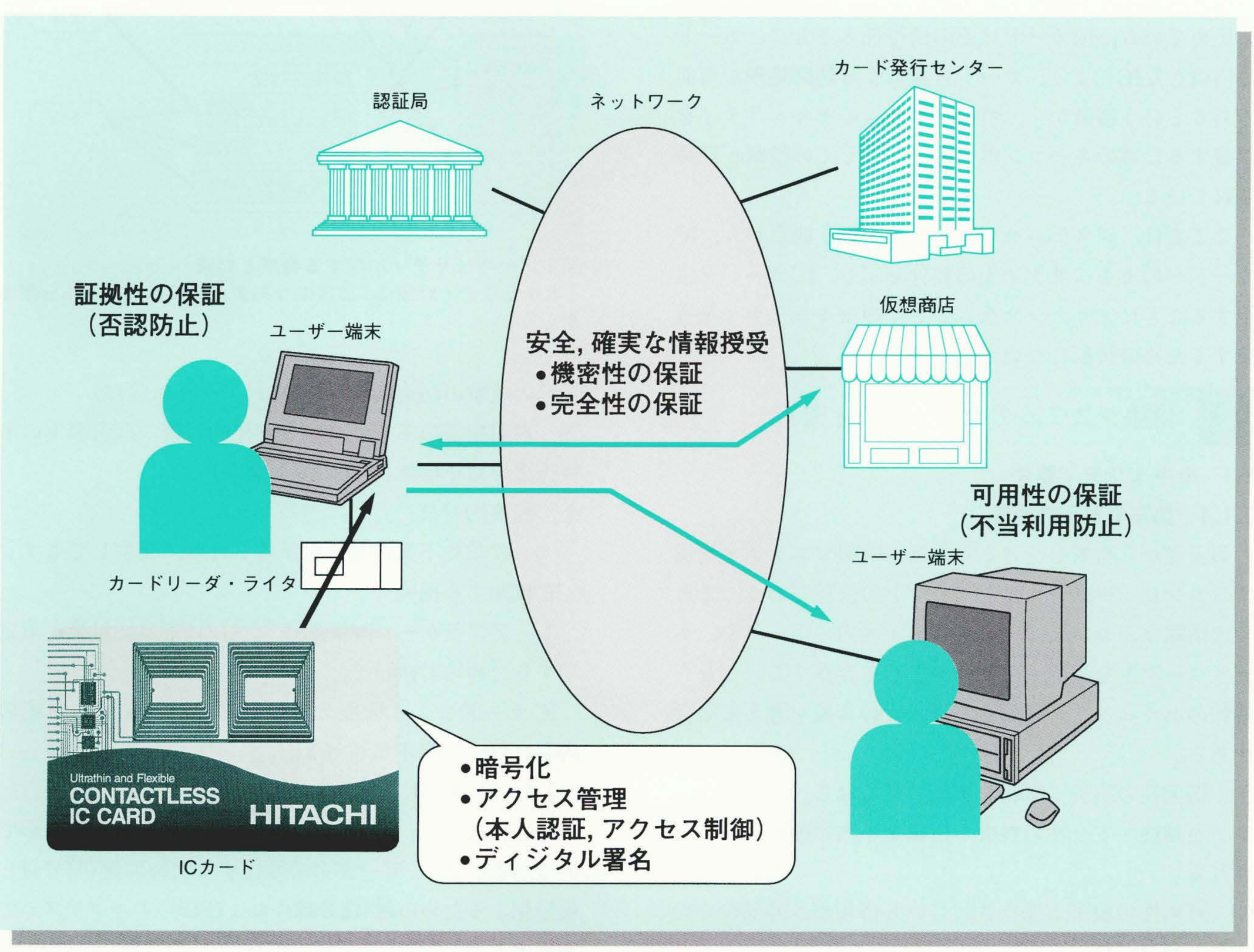
セキュリティシステムにおけるICカードの活用

Secure Information System with IC Card

織茂昌之 *Masayuki Orimo*　新舎隆夫 *Takao Shinsha*
瀬戸洋一 *Yôichi Seto*　菊地良知 *Yoshinori Kikuchi*



ICカードを用いた情報システムのセキュリティ保証

ICカードは，情報システムのセキュリティを保証するための重要なコンポーネントとして位置づけられる。

近年のコンピュータネットワーク技術，特にインターネットの発達により，情報システムのネットワーク化の対象が，従来の大企業だけでなく，中小企業や個人までも含めた範囲に広がっている。また，その範囲も，金融，交通，物流などと多岐にわたっており，これに伴ってセキュリティ対策が重要視されている。ICカードは，その携帯性とともに，カードに内蔵したICによってシステムとして達成すべきセキュリティ対策をカード自身も分担できるという特徴を持ち，情報システムのセキュリティを保証するための重要なコンポーネントとして位置づけられる。

情報システムでのセキュリティ対策の基本として，暗号化，アクセス管理，ディジタル署名があげられる。これらの対策を，ICカードと上位システムとで適切に機能分担することにより，対象となるシステムのセキュリティを保証することが可能となる。日立製作所は，これらの対策それぞれの実現技術について開発を進めている。

1　はじめに

近年のコンピュータネットワーク技術，特にインターネットを利用したEC(Electronic Commerce：電子商取引)の発達により，コンピュータ ネットワーク システムのセキュリティを確保する手段として，ICカードが注目を集めている。ICカードはその携帯性とともに，カードに内蔵したICにより，カード自身による防御処理が可能であるという特徴から，情報システムのセキュリティを保証するためのキーコンポーネントとしての役割が期待されている。

ここでは，システムセキュリティという観点から，ICカードへのセキュリティ上の要件を示し，ICカードを活用することにより，システムとしてのセキュリティを達成するための技術について述べる。

2　情報システムのセキュリティ対策

2.1　セキュリティ要件

2.1.1　第三者からの脅威

第三者から脅威を受ける対象は，情報システムを構成するコンピュータやネットワーク上の情報である。これらの情報は，コンピュータのファイル内のデータや，ネットワーク上を通信中のデータとして存在する。これら情報のセキュリティに対しては，次の脅威を考える必要がある。

(1)　機密性の喪失：情報を不当に見られる。

(2)　正確性・安全性の喪失：情報を不当に改ざん，破壊される。

(3)　可用性の喪失：保存されている情報が，外部からの不当な利用で使えなくなる。

2.1.2　取引相手への脅威

パソコンを利用した株式売買の出現に見られるように，情報ネットワークを利用したECの実施範囲が拡大してくると，第三者対策だけでなく，取り引きの当事者間のトラブルの防止が大切となる。したがって，上記3項目の脅威に加えて，取引相手が契約書などの取引文書を偽造，改ざんし，取引内容や取引事実を不当に事後否認する，「証拠性の喪失：取引事実・内容の証拠性がなくなる。」という脅威を新たに考える必要がある。

2.2　セキュリティ対策

前節で示した脅威に対する対策は，次のように大別することができる[1](**図1**参照)。

(1)　第三者からの攻撃に対する直接的対策：セキュリティへの攻撃の防止機能(暗号化，アクセス管理)

(2)　取引相手の不正に対する直接的対策：取引事実の事後否認の防止機能(ディジタル署名)

(3)　間接的対策

(a)　攻撃や不正の発生を予防したり，発生してもすぐに検知する機能

(b)　アプリケーション要求レベルに応じた対策を策定するための計画技法

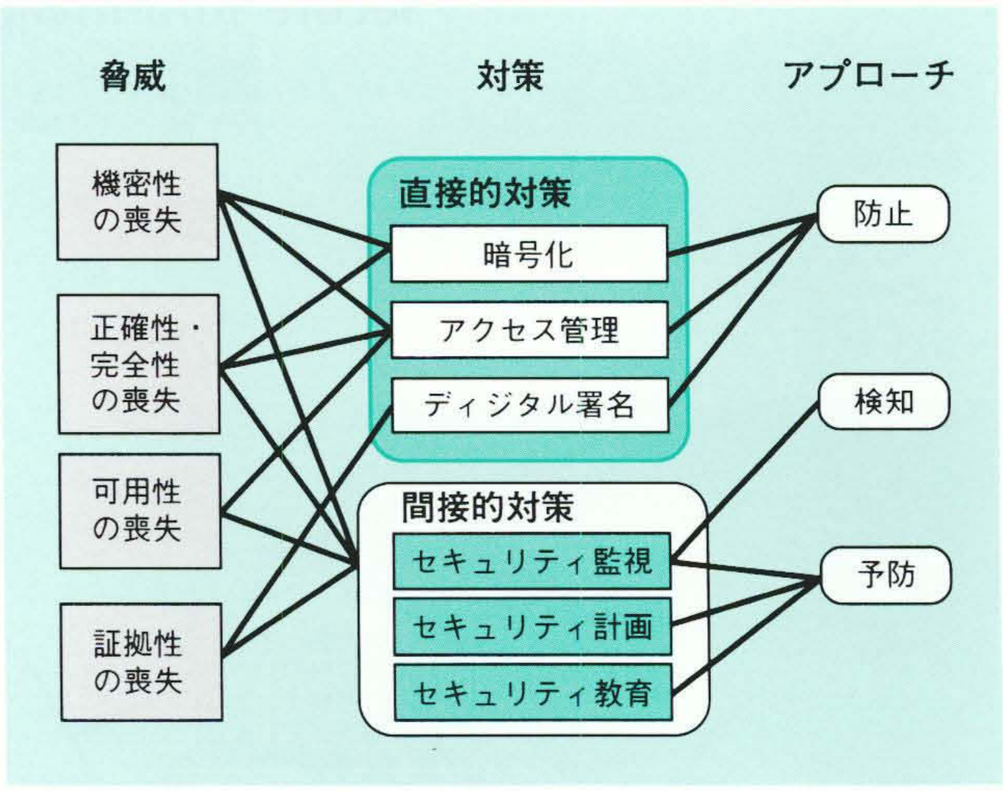


図1　セキュリティに関する脅威と対策
セキュリティ対策は，直接的な対策と間接的な対策に分類できる。

ICカードによる機能分担が有効となる直接的対策の内容について以下に述べる。

2.2.1　暗 号 化

暗号化技術は，セキュリティ対策の基本となるものである。暗号化は，データを暗号化するための鍵(暗号鍵)，復号化するための鍵(復号鍵)，および暗号アルゴリズムで実現する。暗号鍵と復号鍵とが同一であるか否かにより，暗号アルゴリズムは次の二つのタイプに大別できる。

(1)　共通鍵暗号：暗号鍵と復号鍵が同じである。この鍵は暗号化者・復号化者両方で秘匿しておく必要がある。

(2)　公開鍵暗号：暗号鍵と復号鍵が異なる。通常，暗号鍵を関係者に公開し，復号鍵だけを秘密に持つ。前者を公開鍵，後者を秘密鍵，またはプライベート鍵と呼ぶ。

2.2.2　アクセス管理

(1)　本人認証

アクセス管理の第一歩は，ユーザーが本人であるか否かをシステムが正しく認識することである。すなわち，他のユーザーに間違えたり，他のユーザーに成り済ましたアクセスを許さないことである。この本人認証のための手段としては，以下のものがある。

(a)　本人が持つ知識による認証

パスワードや暗証番号を用いた認証である。直接盗まれることがない，実装が容易であるという長所がある反面，本人が忘れる，パスワードが盗まれるなどの危険性がある。現状ではこの方法が最も広く利用されている。

(b)　本人の所有物による認証

銀行カードやICカードを用いた認証である。物理的な安全性がある反面，偽造や盗難の危険性がある。

(c)　本人の身体的特徴による認証(生体認証)

指紋，声紋，網膜パターン，署名などを用いた認証である。確実性が高く，本人の負担が軽いが，認証のための特別な装置や高度な処理ソフトウェアが必要である。

(2)　アクセス制御

「どのユーザーに，どの資源に対して，どのようなアクセスを許すか・許さないか」を，アクセス制御情報として管理し，この制御情報に基づいて，本人認証を完了した相手の資源へのアクセスを制御する。

2.2.3　ディジタル署名

電子的な商取引を行う当事者間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取り引きをほんとうに行ったことを証明する認証の機能が必要である。このための技術として，次に示すディジタル署名技術が開発されている(**図2**参照)。

(1)　署名生成(送信者)

送信者は，署名捺(なつ)印するメッセージと自分用の秘密鍵を用いてディジタル署名を生成する。具体的には，メッセージのハッシュ値を公開鍵暗号アルゴリズムを用いて秘密鍵によって暗号化する。ここでハッシュ値とは，元のメッセージを圧縮した値であり，実際上，一つのハッシュ値に対して一つのメッセージしか存在しないという性質のものである。送信者は，メッセージとこのディジタル署名を受信者に送る。

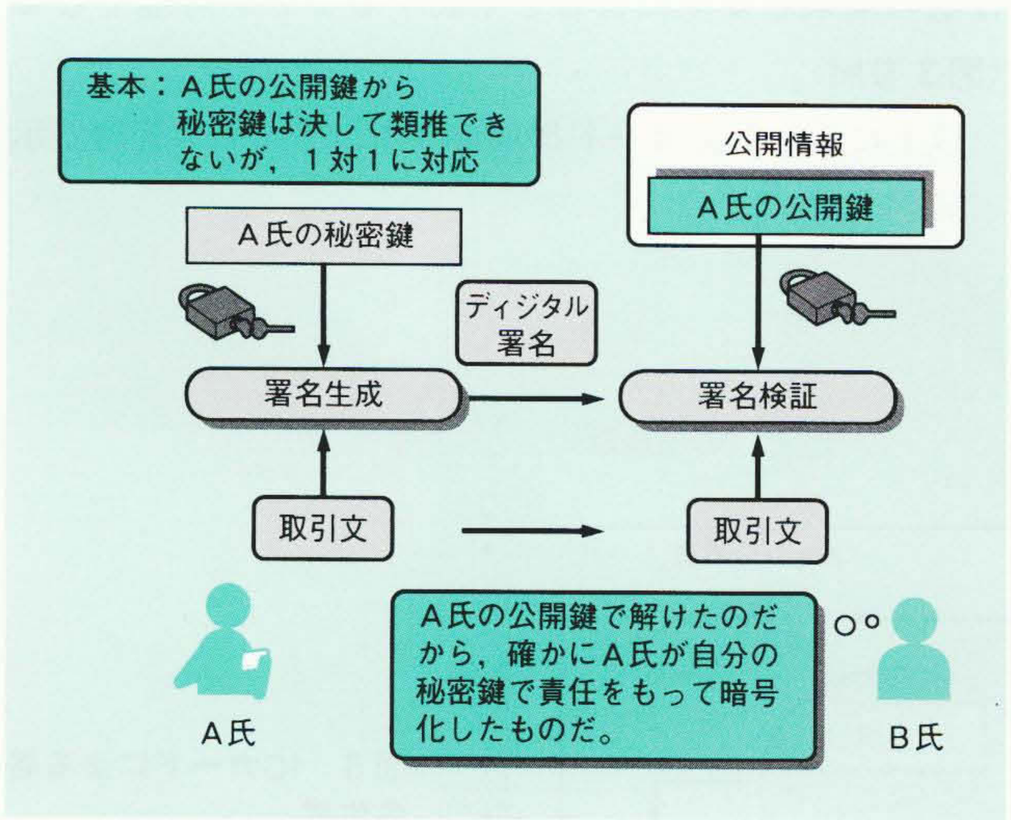


図2　ディジタル署名の仕組み
公開鍵暗号技術を用いることにより，電子文書への署名が実現できる。

(2)　署名検証(受信者)

受信者は，ディジタル署名を受信メッセージと送信者の公開鍵を用いて検証する。具体的には，メッセージのハッシュ値を生成し，ディジタル署名を公開鍵で復号化した値と比較照合する。これらの値が一致すれば，このメッセージは送信者自身が作成したものであることが保証される。

この署名生成・検証プロセスでは，署名を検証するための公開鍵と対になる秘密鍵を持っているのは署名生成者だけである。したがって，各ユーザーが自分の秘密鍵を安全に保管しているという前提さえ成り立てば，公開鍵で検証されたディジタル署名は，その公開鍵と対の秘密鍵を保持しているユーザー以外には生成できないことが保証される。

3　ICカードに要求されるセキュリティ機能

2章で述べたセキュリティ対策では，ICカードが分担すべきセキュリティ機能は以下のとおりである。

3.1　暗号化のための鍵保管機能

暗号化での鍵は，絶対に第三者に漏れてはいけないものである。ハードウェア的に耐タンパリング性に優れ，かつ，次項に示す内部データの保護機能を持つICカードに鍵を格納することにより，その安全な保管が実現できる。なお，この形態では暗号化処理はカード外部で行われるため，この際に鍵がカード外部に出ることになる。ICカード内に暗号処理機能を持たせ，カード内で暗号化・復号化処理を行うことにより，さらに安全な鍵の保管が可能となる。

3.2　アクセス管理のための認証と内部データ保護機能

3.2.1　カード保有者がアクセス主体の場合

ICカードが，その保有者の代理としてアクセス対象に保有者の正当性とアクセス権限を提示するためには，ICカードは以下の機能を持つことが必要である。

(1)　本人認証

カードは，ユーザーが本人(正当な保有者)であるかどうかを認証する機能を持たなければならない。カード自

身が利用者を認証することによって紛失や，盗難カードを用いた第三者によるカードの不正利用を防御することができる。現状では，ICカードにパスワード(PIN：Personal Identification Number)を入力し，あらかじめカード内に格納されているパスワードとの一致判定を行う方式が一般的である。

(2)　アクセス制御

上記の本人認証が完了したICカードは，その保有者の代理として，カード内に格納された保有者の属性情報をアクセス対象に提示する。ここでICカードは，以下のセキュリティを保証する機能を持つことが必要である。

(a)　カード保有者による不正の防御

カード内属性情報では，カード保有者による変更ができないように，カード自身が防御する。

(b)　アクセス対象によるカード正当性の認証

アクセス対象とアクセス権を持つカードだけが共有する論理を規定し，カード内にその処理機構を入れておく。通常，この論理としては暗号論理が用いられる。アクセス対象が生成するデータ(チャレンジコード)に対し，カードが前記処理を施してその結果を提示することにより，カードが正当なものであることをアクセス対象に保証する。

3.2.2　カードがアクセス対象となる場合

ICカードは，外部からの自内データアクセス要求に対する制御機能を持つことが必要である。これについて以下に述べる。

(1)　アクセス要求元の認証

カードは，アクセス要求元に対してデータ(チャレンジコード)を送り，アクセス要求元の応答を判定することにより，その正当性を認証する機能を持つ。これは，**3.2.1**項(2)(b)でのカードとアクセス対象の関係を入れ替えた処理に相当する。

(2)　カード内部データ保護

カード内データエリアを複数の領域に分割し，各領域ごとのアクセス条件をカード内に設定する。アクセス要求を受けたカードは，認証した相手の権限をこの条件に基づいて判定し，そのアクセスを管理する。

3.3　ディジタル署名生成機能

前述したように，ディジタル署名処理では，公開鍵暗号アルゴリズム，署名を生成するための秘密鍵，署名を検証するための公開鍵がそれぞれ必要となる。通常，公開鍵は，署名生成するユーザーの属性を示す情報とともに管理され，これらを合わせて証明書と呼ぶ。ディジタル署名処理では，秘密鍵は絶対に第三者に漏れてはいけないものである。ICカードを用いることにより，この秘密鍵の管理を安全かつ容易に行うことができる。

(1)　秘密鍵と証明書のICカードへの格納

秘密鍵をICカードに格納することにより，安全な保管が可能となる。さらに，署名生成・検証に必要な証明書も同時にICカードに格納することにより，公開鍵暗号が搭載されている端末であれば，任意の端末でICカードの情報を用いて自分の署名を生成することができ，利便性が高まる。

(2)　署名生成処理のICカードでの実行

上記(1)の形態では署名生成処理はカード外部で行われるため，この際に秘密鍵がカード外部に出ることになる。ICカード内に署名生成アルゴリズムを持たせ，カード内で署名生成処理を行うことにより，秘密鍵がカード外に出ることがなくなるとともに，カード受け付けが可能な任意の端末で安全に署名を生成することが可能となる(**図3**参照)。

以上に示したICカード機能のうち，アクセス管理で示

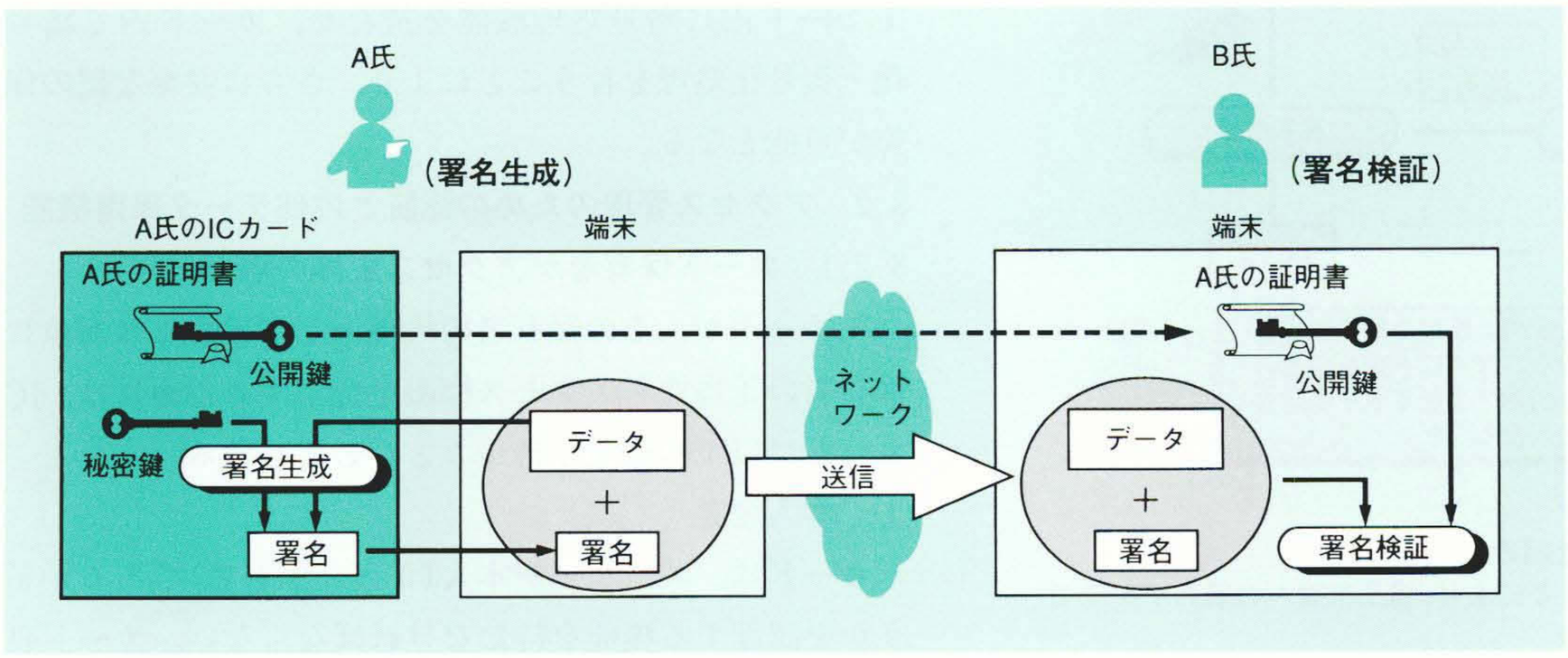


図3　ICカードによる署名生成

ICカード内で署名生成することにより，秘密鍵の安全な管理が実現できる。

した，PINによる本人認証とアクセス制御の方式については，ISO(国際標準化機構)で，ICカード標準として規定されている。

4 ICカード活用によるセキュリティシステム実現のための技術

前章で示したICカードセキュリティ機能を実現するとともに，より高セキュアで柔軟なシステムを構築するための基本技術として開発を進めているものについて，以下に述べる。

4.1 要素技術

4.1.1 次世代公開鍵暗号技術

日立製作所は，すでに，高速な共通鍵暗号として“MULTI 2”暗号を提供しており，MULTI 2暗号を搭載したICカードは既に実用化されている。さらに，1997年，だ円曲線上の演算規則を利用した，新しい公開鍵暗号技術であるだ円曲線暗号[2)]を開発し，「日立暗号ライブラリ“Keymate/Crypto”」として国内で初めて製品化した。だ円曲線暗号は，公開鍵暗号として現在広く用いられている“RSA”暗号に比較して，短い鍵長でより高い安全性を達成する。160ビット鍵長だ円曲線暗号は1,024ビット鍵長RSA暗号と，また，224ビット鍵長だ円曲線暗号は2,048ビット鍵長RSA暗号とそれぞれ同レベルの安全性を提供するものと評価されており，高い安全性を保証し，かつ高速に暗号処理を行うことを可能とする。RSA暗号の次世代公開鍵暗号であるだ円曲線暗号をICカード上で利用できるようにして，高い安全性のディジタル署名機構を提供していく考えである。

4.1.2 生体認証技術[3)]

インターネットを利用したECなどのオープンで大規模なシステムが実用化されつつある中で，より安全な本人認証を実現するため，本人の身体的特徴を用いる生体認証技術への要求が高まっている。身体的特徴としては，**表1**に示すものが利用される。例えば，指紋には「マニューシャ」と呼ばれる特徴を用いる(**図4**参照)。マニューシャの位置は，万人不同，終生不変であることが実証されている。生体認証の適用にあたっては，精度(本人拒否，他人受け入れ)だけではなく，テンプレートサイズ(登録データ量)，利用者の受容性，利便性などの検討が必要である。

このような特徴を持つ生体認証技術の，ICカード本人認証への適用を進めている。生体情報としては，小型化や精度の観点から指紋を用いている。生体認証の実現方法として，次の二方式がある(**図4**参照)。

(1) 認証サーバ方式：生体情報をサービスシステム側で一括管理する方式

(2) ICカードホルダ認証方式：サービスを要求するクライアント側でICカードの生体情報を管理する方式

これら二つの方式のうち，以下の理由により，ICカードホルダ認証方式の開発を行っている。

(1) ユーザー受容性：生体情報は，個人管理するほうが心理的抵抗感が少ない。

(2) 脅威対抗性：ディジタル化された情報は，サービス側でコピーかオリジナルかの識別が困難である。

(3) システム構築：認証サーバ方式は，サービスシステムごとにデータベースの構築が必要である。

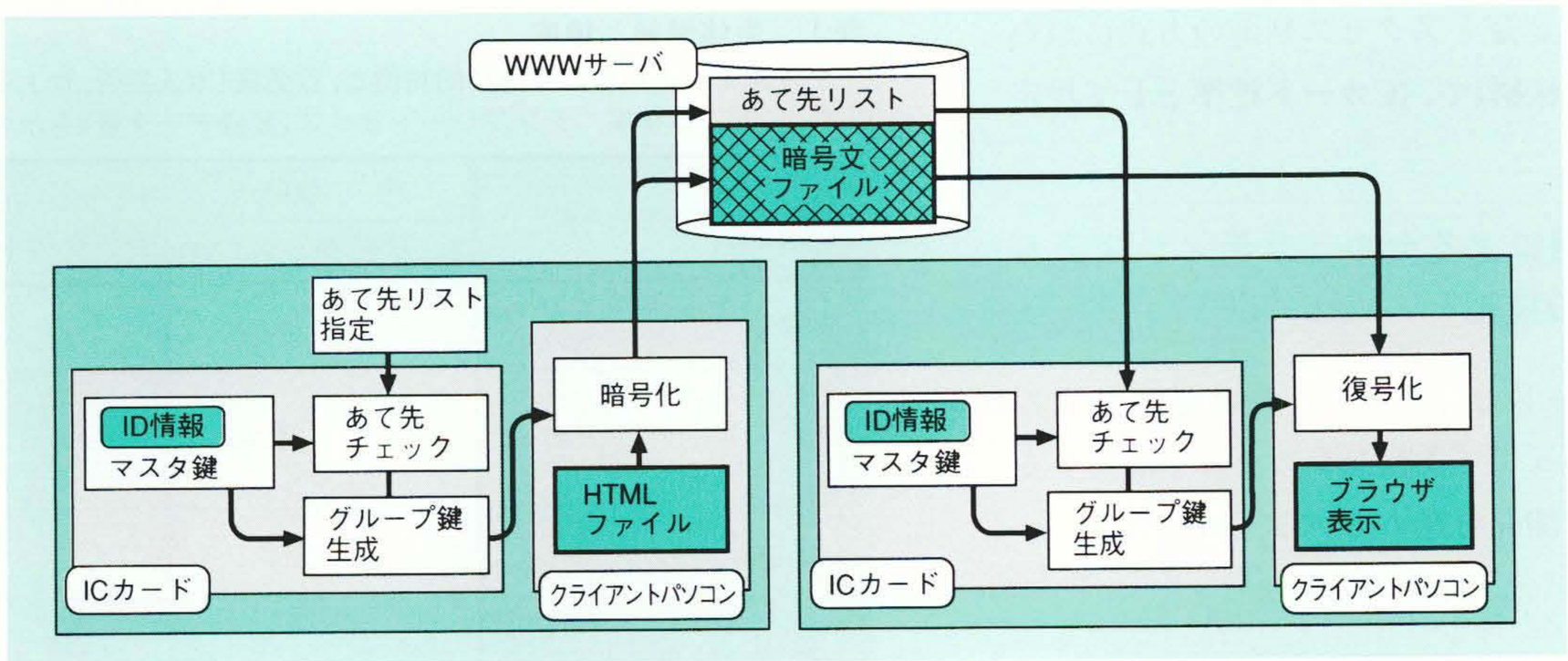
表1 生体情報と精度

生体認証に用いられる身体的特徴と，誤認識(本人拒否，他人受け入れ)に対する精度，テンプレートサイズ(登録データ量)を示す。

生体情報	内　容	精　度(%)		テンプレートサイズ(バイト)
		本人拒否	他人受け入れ	
指紋	手の指の指紋の特徴(マニューシャ)	0.5	0.001	1k
掌形	手の大きさ，長さ，厚さまたはそれらの比率	0.15	0.15	10
顔	顔の輪郭，目や鼻の形およびそれらの配置	1	1	1k
虹(こう)彩	虹彩(アイリス)の放射上の紋様パターン	2.8	0	256
声紋	話者の特徴を認識	1	0.1	1k
動的署名	署名の字体や署名時の書き順など	0.2	0.6	100
その他	耳，キーストローク，手の甲の静脈パターン，においなど	—	—	—

図4 指紋の特徴

マニューシャの位置は，万人不同，終生不変である。



注：略語説明
WWW(World Wide Web)
HTML(Hypertext Markup Language)
ID(Identification)

図5　WWWサーバ上情報のアクセス制御
グループ暗号方式を適用することにより，WWWサーバ上で情報の指定グループのメンバー以外への穏ぺいが実現できる。

4.2　応用技術：グループアクセス制御技術

前節で述べたアクセス管理は1対1間での相互のアクセスを対象とするものであるが，各ユーザーが携帯するICカードを用いて，m：n間でのアクセスの柔軟な管理を実現するグループ暗号方式を開発した[4]。この方式を適用して，WWWサーバ上で情報のアクセス制御を実現している(**図5**参照)。

この方法は，現行のインターネットWWWサーバに何ら特別な機構を加える必要がないという特徴を持つ。情報の登録者は，情報を見せてもよいグループとの間で共有する鍵(グループ鍵)で情報を暗号化し，WWWサーバに登録する。この情報は鍵を共有しているグループのメンバ以外では復号化できないため，WWWサーバ上で情報のアクセス管理が実現できる。ここで，ICカードは情報を共有したい対象のグループ識別名(あて先リスト)を入力すると，そのグループ内で共有されている鍵を生成して出力する機能を持つ。この際，ICカードは，対象となるグループに対するカード保有者のアクセス権限をチェックした後に鍵生成を行うため，グループ鍵が権限者以外に漏洩(えい)することはない。

5　おわりに

ここでは，ICカードへのセキュリティ上の要件を示し，ICカードを核としたシステムセキュリティ実現のための技術について述べた。

ICカードは，今後の情報システムのセキュリティを保証するための重要なコンポーネントとして位置づけられる。今後も，ICカードを活用したセキュリティを実現するための基盤技術の開発をさらに進めていく考えである。

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) 宝木，外：楕円曲線を利用した高速暗号化方法，電子情報通信学会技報　ISEC97-15，7～15(1997-7)
3) Biometric Consortium http：//www. vitro. blomington. in. us：8080/～BC/
4) 洲崎，外：企業情報向けグループ暗号システム　(1)　暗号管理法式，情報処理学会第52回全国大会講演論文集(4)，355～356(1996)

執筆者紹介

織茂昌之
1981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，ICカードシステムセキュリティの研究開発に従事
IEEE会員，情報処理学会会員，計測自動制御学会会員
E-mail：orimo@sdl. hitachi. co. jp

瀬戸洋一
1979年日立製作所入社，システム開発研究所 第1部 所属
現在，医療情報システム，本人認証システムの研究開発に従事
工学博士，技術士(情報工学部門)
IEEE会員，電子情報通信学会会員，情報処理学会会員
E-mail：seto@sdl. hitachi. co. jp

新舎隆夫
1973年日立製作所入社，汎用コンピュータ事業部，CARDシステム開発センタ 所属
現在，ICカードシステムの開発に従事
情報処理学会会員，IEEE Computer Society会員
E-mail：tshinsha@kanagawa. hitachi. co. jp

菊地良知
1980年日立製作所入社，システム開発本部 ニュービジネス開発室 所属
現在，ICカード関連システムの開発に従事
情報処理学会会員
E-mail：kikuchi@iabs. hitachi. co. jp