昭和37年9月15日第三種郵便物認可　三菱電機技報　72巻5号(通巻804号)　1998年5月25日発行(毎月1回25日発行)

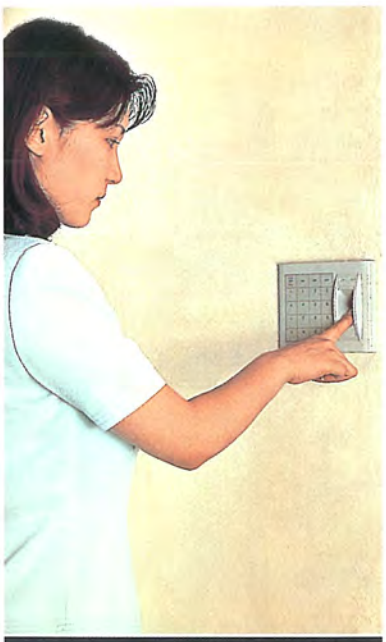
技術がつくる高度なふれあい SOCIO-TECH

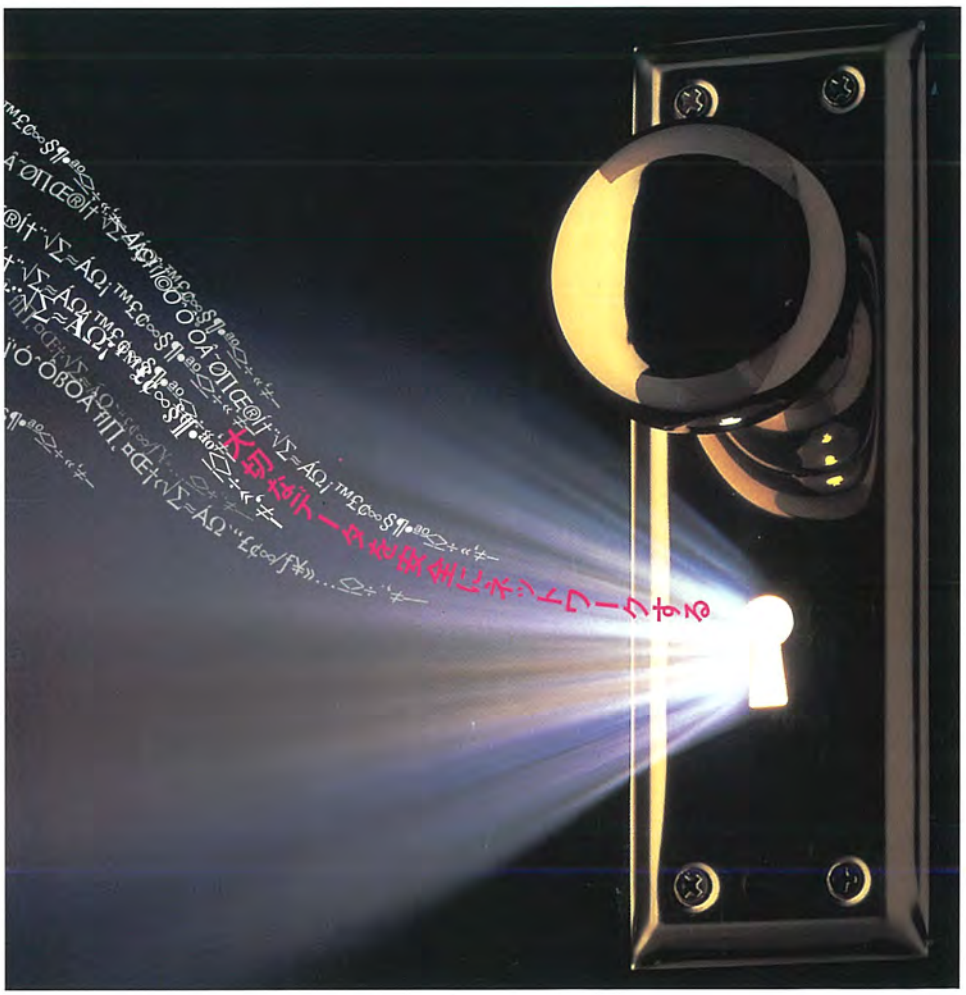
MITSUBISHI

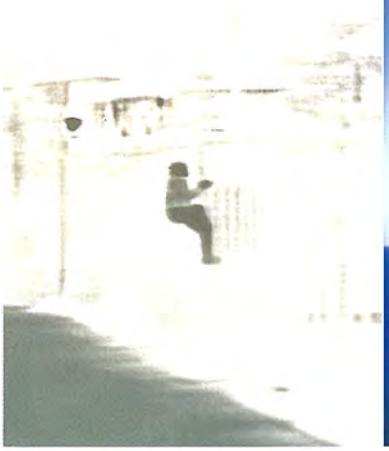
三菱電機技報 Vol.72 No.5

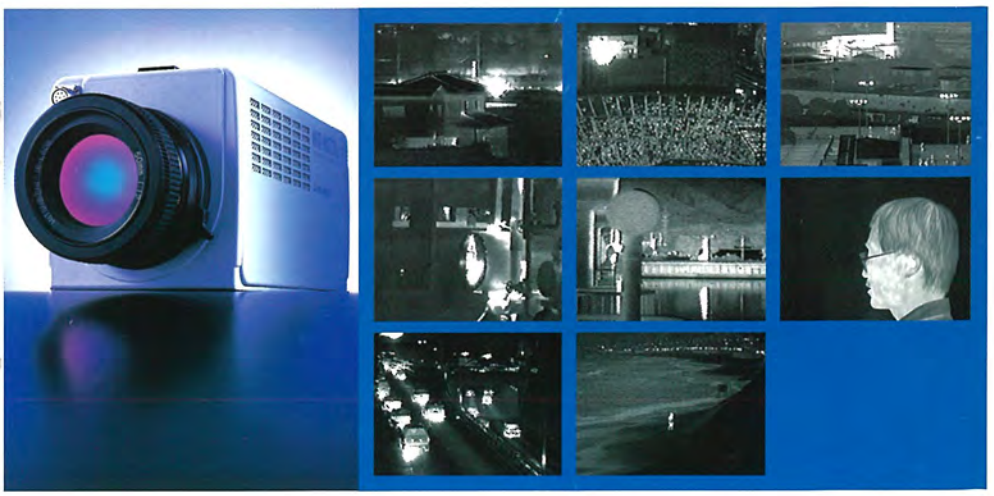
特集“暗号・セキュリティ技術及びその応用”

'98 5









ISSN　0369-2302／CODEN:MTDNAF

三菱電機技報 Vol. 72 No. 5 1998

特集“暗号・セキュリティ技術及びその応用”

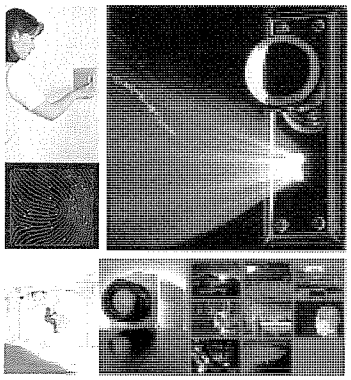
目　次

表紙

暗号・セキュリティ技術とその応用

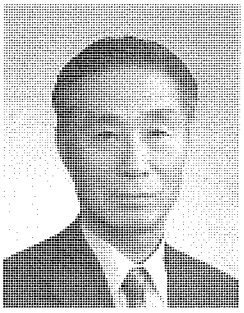
暗号と個人識別及び情景監視技術は，セキュリティ技術として最も利用範囲の広い基本技術である。三菱電機では，それぞれ優れた特長を持つこれらの技術を保有し，その応用によって様々なニーズに応じたセキュリティ関連製品を提供している。

右上は世界最高水準の暗号技術“MISTY”を核とした情報セキュリティシステムで情報の安全性を実現することを意味するイラスト，左上は高精度指紋判別装置の応用製品と判別画像，右下は41万画素の高画質を持つコンパクト赤外線カメラと映像，左下は侵入監視装置の映像例を示す。



巻　頭　言

情報社会の自由と安全



中央大学　理工学部
情報工学科
教授　辻井重男

青春の日にフランス革命に感激した哲学者ヘーゲルは，“歴史とは，人間の自由拡大の過程である”ととらえたが，現在，我々は工業社会から情報社会への変革の中で，人間の自由は拡大しつつあると見てよいのだろうか。自由が単調に増加していると楽観することはできないが，インターネットの普及に伴って，個性的に活動している人々を見ると，ヘーゲルの法則とでも言うべきものが成り立つ側面も否定できない。自由の拡大は結構なのだが，自由には自己規律・責任が伴わねばならない。しかし，複雑で深度の深い技術社会では，自己責任にも限界があるから，個人が自由に活動する舞台としての情報ネットワークは，安全で信頼感の高いものでなければならない。つまり，情報セキュリティは，情報社会のインフラストラクチャなのである。

企業レベルで考えれば，従来，情報セキュリティをローカルで付加価値的なものとみなしてきたのに対し，ここ数年，ネットワークのオープン化に伴って，情報セキュリティをインフラストラクチャとしてとらえるような意識もようやく高まりつつあるかに見受けられる。米国系の企業では，経営理念に直結する形でセキュリティポリシーを確立し，ガイドラインを策定し，リスク分析を行い，システム監査やモラル教育体制を整え，また，人事面では，従来のCIO(Chief Information Officer)と並んで，CISO(Chief Information Security Officer)を置くところも増えつつあるようだ。

また，国家社会のレベルで見れば，米国では，1997年10月，大統領の諮問委員会が，ライフラインへの情報ネットワークを介した攻撃を含む社会の安全を脅かす諸々の不安要素を分析し，社会的安全を向上させるための施策を大統領に勧告している。我が国でも内閣と諸省庁間の連携を強化し，こうした課題を検討する体制を確立すべきであろう。

情報セキュリティの向上に関しては，技術，法制度，倫理等の面から総合的に，かつ国際的視点に立って，対応を深めていかねばならない。日本は，不正アクセスが犯罪にならない珍しい国である。ネットワーク化の浸透や電子経済の普及に伴って，これでは困ると考える人も増えてきたようである。国際問題としては，日本人が，日本に居ながらA国のコンピュータに不正アクセスして日本政府に訴えられても，政府は，いわゆる双罰主義の原則によって罰しようがないのである。また，公開かぎ(鍵)証認等を業とする認証機関(Certification Authority：CA)が日本でも幾つか設立されているが，ネットワーク時代には，互いに他国のCAを利用するケースも考えられる。この場合，国際間で各々の認証を認め合うことが有効であり，そのためには，CAに課せられる要件が互いに同程度のものであることが望ましい。ドイツのディジタル署名法には，そのことが明記されている。ドイツに限らず欧米を中心にCAに関する法制度が整備する中にあって，我が国も，社会安全，産業振興，そして個人情報保護の間のバランスを図りつつ，国際整合性のある法制度を整えていくことが求められている。

次に，情報倫理について考えてみたい。倫理という言葉が固ければ，サイバースペースにおけるルールと言い換えてもよい。倫理を考える場合，カントの定言命令とベンサムやミルの功利主義という二つの異なった立場があると言われている。しかし，素人の私には，カントの言う普遍的立法の原理と最大多数の最大幸福という功利主義の立場は，底流でフィードバックグループをなしているように思われる。これからは，両者の立場を大いに連携させて，住みよいサイバー社会を築いていくべきではないだろうか。

最後になったが，情報セキュリティ技術について触れておきたい。情報セキュリティ技術も膨大な体系をなすことは，本誌からもうかが(窺)える。暗号については，例えば三菱電機からも共通鍵暗号に対する線形解読法やそれを踏まえたMISTY暗号のような国際水準を抜く成果が生まれており，日本の暗号技術も世界有数のレベルに達している。ここで暗号は，情報セキュリティという守りの技術の要素技術であると同時に“電子マネーなどをつくる”という社会変革力を秘めた攻めの技術であることを強調しておきたい。

いずれにしても，暗号は重要な要素技術であるが，単独に使われるというよりハードウェアあるいはソフトウェアとして情報セキュリティシステムや情報ネットワークに組み込まれることが多いから，日本の暗号技術が国際市場で伸びていくためには，システムコンセプト形成能力やソフトウェア産業力・情報産業力，更に言えば，貿易面での外交能力や，先に述べた法制度やモラルまで含めた情報文化力とでも呼ぶべき国力の向上を急がねばならない。

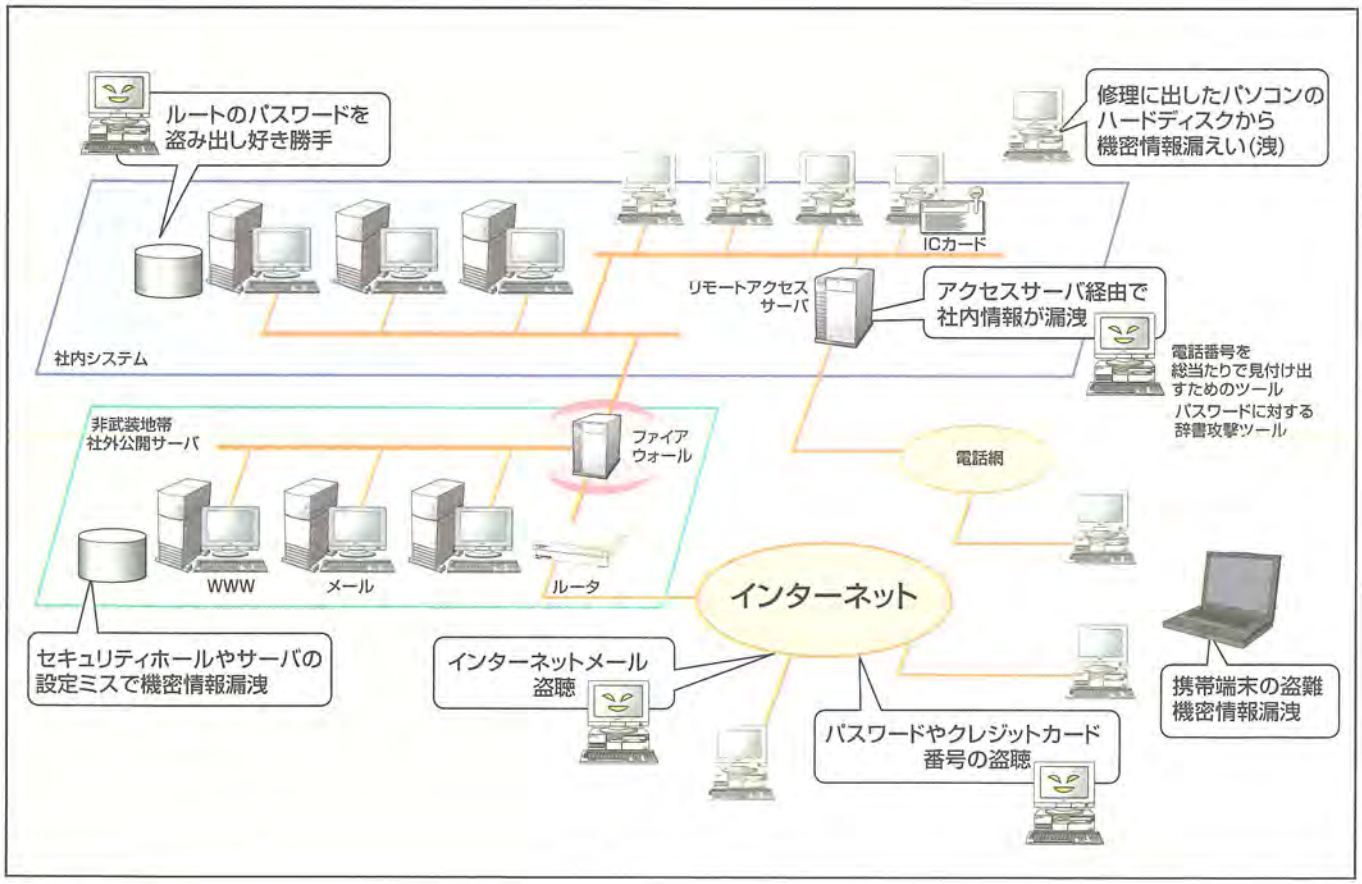
暗号・セキュリティ技術の現状と展望

片木孝至*
池端重樹**
竹田栄作***

要　旨

インターネットを始めコンピュータネットワークと通信の急速な発展により，情報セキュリティの重要性が注目されている。情報セキュリティ対策の基盤は技術的対策から始まる。暗号技術は，守秘と認証という基本機能を持ち，直接的に情報を守るとともに，他の情報セキュリティ技術の要素としても用いられる。暗号とともに使用されるセキュリティ技術として，人間の身体的特徴を活用した個人識別，公共空間や重要施設等の大規模なエリアに対する遠隔監視，そしてこれらを統合する応用システムがある。

本稿では，これらの技術の現状と動向を中心に，情報セキュリティの対策について述べる。



想定される脅威

情報セキュリティ対策を講じるためには，まず脅威／リスクの分析が求められる。個々のシステムの置かれた環境，周囲条件，運用によって，どの脅威が支配的か異なる。

*情報技術総合研究所長(工博)　***同研究所 情報セキュリティ技術部長　**産業システム研究所 技師長

1. まえがき

国内のコンピュータ及びネットワーク利用の犯罪で現在公に認知されたものは，1995年32件，'96年89件，'97年101件と増加している。これは欧米と比較して多いとは言えないが，犯罪には至らない不正アクセスは極めて深刻な状況にある。国境の意味はネットワーク上は失われており，国外からのアクセスを地理的に遮るようなものはない。'97年の米国国防総省へのハッカー侵入は年間16万件以上と推定された。カード犯罪は，既に日本市場において年間約200億円の損害が報道されていて，カードは近い将来ネットワークと人とのインタフェースとなるだけに，その急増は脅威である。電子決済や電子商取引も含め，今後の情報化ネットワーク社会の進展の上で，十全な情報セキュリティ対策とそのインフラの整備は不可欠である。

情報セキュリティ技術は**表1**のような総合的対策を必す(須)とする。攻撃者はシステムの最も弱いところを探しねらうという。特にシステムで問題なのは人に関する対策であろう。情報セキュリティも，技術的対策の上に人事・運用を含めた明確なセキュリティポリシーと管理を持つことが情報を守るかなめ(要)となる。つまり，組織として何をどれだけのコストをかけて守るべきかを明確にする。このポリシーに基づいて，管理運用規程等を定めていく。法・制度の整備，ネットワーク社会における倫理確立のための教育，啓もう(蒙)，さらに，欧米等に比べて決定的に不足していると指摘されるセキュリティ管理者の養成も求められる。

これら対策の前提としても，技術的対策が基本として求められる。

2. 情報セキュリティ

2.1 情報セキュリティとは

情報システムの正当なユーザーに"安全と信頼"を与えること，様々な脅威から情報を守ることである。天災・事故・故障・誤り等の非人為的及び過失的脅威と，盗聴・改ざん・偽造・不正行為等の人為的かつ意図的脅威の二つの脅威がある。現在大きな問題となっているのは後者であり，それに対する情報セキュリティに焦点を絞って以降に述べる。

2.2 国際的・政治的広がり

犯罪捜査等のためにアクセス権限を合法的に法執行機関へ与えることを合法的アクセスと言う。例えば，公的な大規模システムにおけるアクセス権限の付与として'94年米国連邦政府によって提案された通称クリッパーチップ方式と呼ばれる鍵供託システム(Key Escrow System：KES)が世界的に大きな議論を巻き起こした。ビジネス界や学会から，政府による情報の一元的管理につながるという危ぐ(惧)が示され，また，技術的な問題点もあり，米国連邦政府も推進を断念した。しかし，その後，'96年に，暗号鍵を紛失したときそれを回復するという形の鍵回復システム(Key Recovery System：KRS)として再び新たな提案を行い，強力に推進しようとしている。その公的採用については現在も議論が行われている。

情報セキュリティ，特に暗号には，情報の機密性保護を実現するという性格から，政治的な問題が絡んでくる。さらに，それが地球規模の情報ネットワークの広がりで使用されることから，その扱いに国際的な視点が求められる。このため，OECD(Organization for Economic Cooperation and Development：経済協力開発機構)等の国際機関で，情報セキュリティに関して検討が行われている。次に示す'97年3月策定のOECD暗号政策ガイドラインは，情報セキュリティを考える際のベースとなり得る。

2.3 OECD暗号政策ガイドライン

次のように要約される。

(1) 暗号の信頼性
　情報システムの利用者が十分信頼のおける暗号方式であること

(2) 暗号方式の自由選択
　法律の範囲内で，暗号方式を自由に選択できる権利

(3) 市場主導による暗号方式の開発
　各国政府のニーズ・需要・責任に応じた市場主導の開発

(4) 暗号方式の標準化
　暗号手法の技術的標準・基準・プロトコルは，国家又は国際レベルで開発／普及

(5) プライバシーと個人データの保護
　通信の秘密及び個人データの保護を含むプライバシーに関する個人の基本的権利の尊重

表1．情報セキュリティ対策

セキュリティポリシー				法・制度 倫理	教育・啓蒙
施設・設備 装置 ソフトウェア ネットワーク	監視・監査	管理・運用 保険	人事 組織		
情報セキュリティ技術					

(6) 合法的アクセス
各国の暗号政策において，暗号化されたデータの平文又は暗号鍵への合法的アクセスを容認

(7) 責任
暗号サービスを提供する又は暗号鍵を保有／利用する個人や機関の責任は，明確に記述

(8) 国際協力
各国政府は，暗号政策の国際的調和を図る。正当でない貿易障壁の取り除き

3. 情報セキュリティ技術

情報に対するアクセス権限の付与をどのように実現するかが，情報セキュリティ技術の中心的な課題である。ユーザー(人・組織及び設備のエンティティ，又はネットワークシステムの要素等)の認証と情報の保護とが基本となる。

3.1 ユーザーの認証

ユーザーの認証とは，情報にアクセスしようとするユーザーが何らかの形で身元保証されている存在であることを確認することを言う。相手が人である場合，これを個人認証と呼び，パスワードのような記憶，ICカードなどの携帯，その人の指紋，網膜，こう(虹)彩パターンなどバイオメトリックスによる方法がある。

人以外の認証も，その対象が持つ固有情報又は固有の能力を利用する。この場合，不正アクセスがあり得る環境では，暗号による認証が基本となる。これは，その対象がある秘密の暗号鍵を用い得る機能を持つことを確認することによって行われる。

3.2 情報の保護

情報の保護とは，あらかじめ定められた形(例えば読み出し，書き込みなど)のアクセスを定められた情報(鍵)を持つものにだけ許し，それ以外のアクセス(不正アクセスと呼ぶ。)を排除することを言う。防止と検知による抑止である。

防止は，施設・設備にかかわるものからセンサ及びソフトウェアによる方法等があり，それぞれ重要であるが，今後，オープン形のネットワークで特に重要となるのは暗号的手法である。

検知による抑止は，不正アクセスが生じたときに，それを検出し警告を発するか，その情報を無効にする。さらに，不正アクセスの証跡を保存し不正アクセス者に何らかの制裁を加える等により，不正アクセスの意欲をそ(削)ぎ，抑止することを言う。これには，認証技術，不正アクセスの特徴をとらえそれに基づいての検知・対処，コンピュータウイルス対策，ディジタル透かしと呼ばれる手法(対象となる情報に不正検知のための情報を埋め込み，不正使用時に埋め込んだ検知用情報から不正を暴露する。ときには不正使用者も特定する。)等がある。

3.3 アクセス制御方式の構成

ユーザーの認証と情報の保護とを基礎として，アクセス制御システムが構成される。ここでアクセス制御とは，定められたアクセス権限の付与を実現する方法のことである。ユーザーの数と守るべき情報の数，システムの一元的管理者の有無，各ユーザーや各情報に対しどのようなアクセスが許されるか，ユーザーや情報の増減に伴う更新の度合など，各システムのパラメータと形態に応じて，効率の良い方式を用いる必要がある。特に大規模システムにおけるアクセス制御の基本的課題である。例えばネットワークではVirtual Private Networkがある。三菱電機のMELWALLシリーズが該当する。

4. 暗号技術

暗号の機能には守秘と認証がある。

4.1 守　秘

図1に，暗号による守秘機構を示す。発信者が秘密に送りたい情報P(平文)を暗号化鍵K_1を用いて暗号文Eに変換することを暗号化，受信者が復号鍵K_2を用いてEを元のPに戻すことを復号と呼ぶ。ここで，暗号化／復号は効率良く実行できなければならない。復号鍵なしに暗号文から平文を求めるのは困難でなければならない。復号鍵は秘密にし，あらかじめ認められた当事者以外は入手できないようにしなければならない。他の入手可能な情報から推定することも不可能にしなければならない。

逆に，暗号文を何らかの手段で入手し復号鍵なしで平文に復元することを解読という。

4.2 認　証

図2に，代表的な認証の方法(Message Authentication Code：認証子)を示す。これは文書における署名やなつ(捺)印の機能に該当する。発信者は，伝達したい平文Pについて何らかのデータ圧縮を施し，圧縮文pを作る。次に，認証子生成鍵L_1でpを認証子aに変換し，これを平分Pに付けた(P，a)を送る。受信者は，受信した平文に対して同様に圧縮文を求めるとともに，認証子を認証子生成鍵L_2で復号し，認証子からも圧縮文を復元する。その圧縮文両者が一致すれば，受信した平文と認証子は正当であると判定

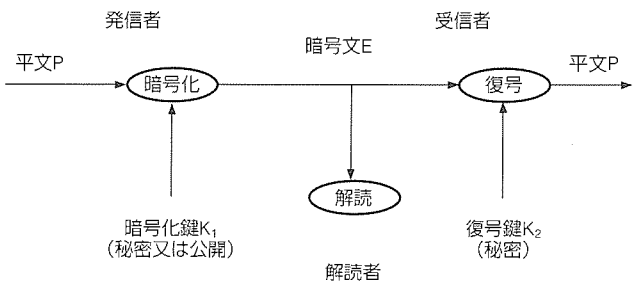


図1．暗号による守秘

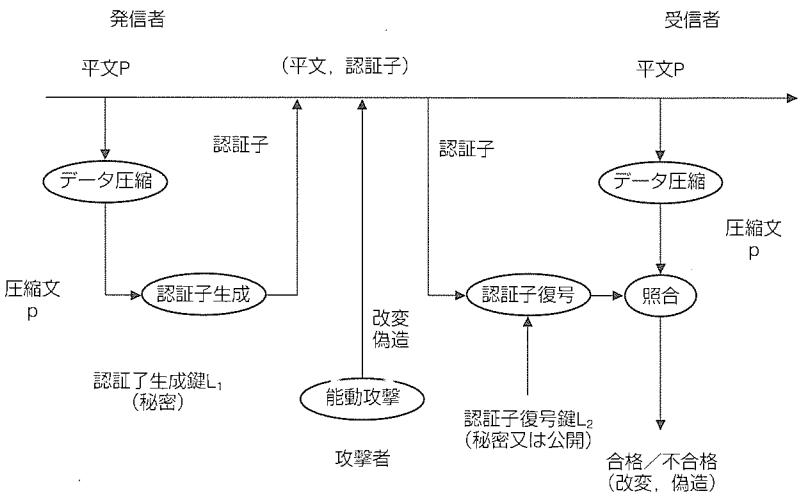


図2．暗号による認証

する。実行の効率，鍵の秘匿性の保持，鍵及び認証子の類推を困難とする必要性はいずれも守秘の場合と同様である。

4.3 共通鍵方式と公開鍵方式

発信者と受信者が同じ鍵を共有する暗号を，共通鍵暗号又は対称鍵暗号と言う。有名で代表的な共通鍵暗号は，'76年に米国連邦政府の標準暗号として採用されたDES(Data Encryption Standard)である。DESは，標準化のために，そのアルゴリズムを完全に公開されている。これは，暗号の安全性は鍵を秘密に保つことによって確保すべきであり，アルゴリズムは公開しても安全であるように設計すべきであるというコンセプトに基づいている。当社の暗号アルゴリズムMISTYも同じ設計思想によっている。事実，暗号アルゴリズムは秘密にしてもやがて知られてしまうことが多い。特にネットワーク上で多数の人に使われるものでソフトウェアで実装されたものは秘匿しておくことは不可能である。アルゴリズムの公開は，暗号の普及，研究・開発の活性化に大きく貢献している。

一方，発信者と受信者の鍵が異なり，片方から他方を推定するのが極めて難しい場合，これを公開鍵暗号又は非対称暗号という。鍵の一方を公開しても他方を秘密に保つことができる。公開する鍵を公開鍵(Public Key)，秘密に保つ鍵を秘密鍵（又は個人鍵，Private Key)と呼ぶ。守秘には，暗号化鍵K_1が公開鍵，復号鍵K_2が秘密鍵である。認証には，認証子生成鍵L_1が秘密鍵，認証子復号鍵L_2が公開鍵である。このような認証をディジタル署名と呼ぶ。公開鍵暗号では，秘密鍵を持つのは原則として一人，所有者個人のみとなるので，鍵管理が簡潔になると同時に発信と受信のセキュリティ上の区別を明確にすることが可能であり，通信上の犯罪・係争の解決に有用である。欠点としては，共通鍵暗号に比べて暗号化や復号が複雑であり処理速度が著しく遅く，およそ100倍から1,000倍も遅くなる。したがって，データの守秘には共通鍵暗号を使い，鍵そのものの配送やディジタル署名に公開鍵暗号を使うことが一般的である。代表的なものにRSA(Rivest- Shamir-Adelman)暗号，また最近では，RSA暗号よりも効率が良いと言われているだ(楕)円暗号がある。

4.4 暗号の安全性

暗号を守秘に用いる場合，解読ができるだけ難しくなるように設計しなければならない。暗号の安全性は，実用上ほとんどが計算量的安全性を尺度としている。計算量的に安全であるとは，原理的には解読可能であっても，膨大な計算量を解読に要するため実際上解読不可能であるというケースを指す。実用的な暗号については計算量的に安全であることを理論的に証明することは極めて難しく，経験や勘及び事例に基づいて判断されてきた。DESは，多くの研究者による様々な面からの安全性評価に耐え，開発から十年以上，最も信頼できる商用暗号としての地位を保ってきた。しかし，解読技術の急速な進歩により，またコンピュータの高速化，超並列計算技術等により，DES解読に要する計算量の壁が年々低められつつあり，DESも安全とは言えなくなってきた。その解読技術の代表的なものの一つに，当社の松井が発明した線形解読法とそれによる計算機を使ったDES解読実験による実証がある。米国では，Triple-DES(DESを3回かける)をこれに対応するものとして採用する動きにある。しかし，DESよりもどれぐらい安全であるかという指標・根拠に正確なものは未だない。また，速度が3倍遅くなるというトレードオフがある。

これらの問題を克服するものの一つとしてMISTYを位置付けることができる。代表的解読法に対して，計算量的に十分解読困難(すなわち安全)となるように設計されている。ハードウェア，ソフトウェアの両方のいずれの実装においても高速で，また，ICカード向けのスモールスケールから高速ネットワーク機器用のラージスケールまで幅広いプラットホームに適用できる。

4.5 公開鍵基盤

暗号の守秘機能・認証機能を大規模システム上で使うためには，鍵管理のインフラ整備が必要である。その基礎となるのは公開鍵方式による鍵管理方式である。認証局(Certificate Authority：CA)方式による公開鍵基盤(Public Key Infrastructure：PKI)と言われる。**図3**に示すように，ユーザーAは自分の名前N_Aと自分の公開鍵PU_Aを認証局に提出し，これに認証局の署名S_C(N_A，PU_A)を付けてもらう。すなわち，ユーザーAの公開鍵認証書として，名前と公開鍵と署名の組(N_A，PU_A，S_C(N_A，PU_A))を発行してもらう。言い換えると，認証局という権威者が，各

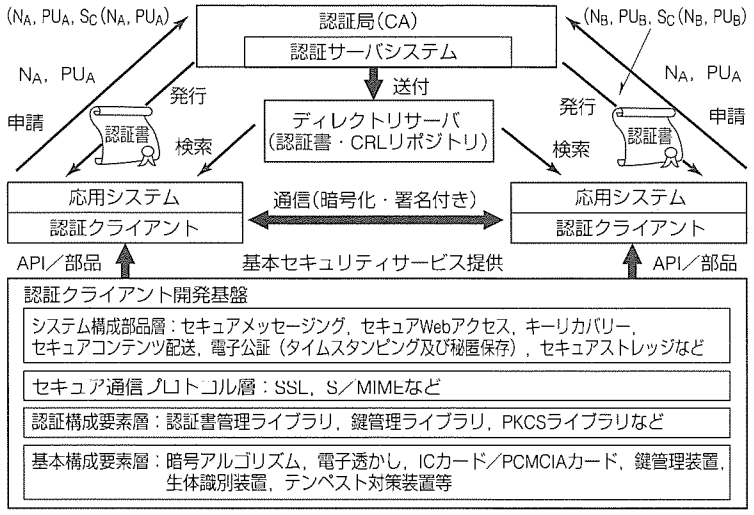


図3．公開鍵基盤(認証局方式)

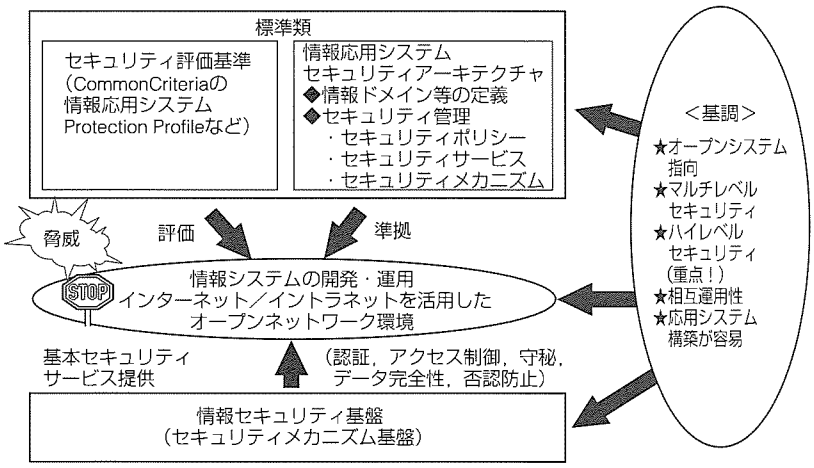


図4．情報セキュリティの枠組み

ユーザーの公開鍵であることを保証した認証局の署名付きの保証書を各ユーザーに提供するのである。ユーザーAとユーザーBが相互に各々の公開鍵認証書を交換し，相手の保証付きの公開鍵を入手し，それを用いて共通鍵暗号のための鍵を送ったり認証したりすることによって，AとBの間の通信の守秘・認証を実現することができる。将来，各企業集合体ごと又は業種ごとに複数のPKIのインフラが併存する形になると思われる。そのインフラ間の情報授受をいかに円滑に行うかが，今後の大きな課題となろう。

5. 個人識別と監視／アクセス管理技術

どういう人がどのようにアクセスし運用するかを知ることは，情報システムや重要施設のセキュリティを決定付ける重要な要素である。アクセスする人を認識・判定する個人識別，個人ごとに固有な人間の身体的特徴に基づく識別技術は，アクセス権限を決める尺度と関連付けて使用される。指紋による照合は，中でもその代表的なものである。コンピュータ室等への入退室，金融端末やパソコンを始め各種情報端末へのアクセスに対する個人確認に適用される。指紋画像を得るセンサ技術，画像照合を正確かつ高速に行うパターン照合アルゴリズム，これらを低コストでかつ高速に実行する装置と画像データを蓄積・検索するデータベース技術で構成される。

当社は廉価で高精度な指紋照合装置を提供している。指紋に加え，実際の署名操作から照合を行うオンライン筆者照合も提供している。ペン入力コンピュータや携帯情報端末のタブレット上に筆記した筆跡・筆順・筆速から個人を照合する。

このほかにも虹彩・網膜・顔など様々な認識手段があるが，用途・分野・環境，及び必要とされるセキュリティの度合いに応じて組み合わせて使用されるケースがある。

これらは人間の感覚・認識を代行する手段であるが，それ以外に，人間の感覚・認識をサポートし，その力の及ぶ範囲を空間的・時間的に拡大させる機能がある。特に安全・防犯セキュリティにおいて顕著に求められ，人的監視に勝るコスト効率，また，人的には従来不可能であった部分への監視をもたらす。

監視カメラシステムによる映像監視，センサ(光，赤外線，超音波，マイクロ波)による侵入検知，施設とモニタセンターをネットワークで結ぶ遠隔監視等がある。

事務所，ホテル，店舗，アメニティエリア，エレベーター，駐車場等を持つ高層化・大型化・複合化されたビル向けに大規模な総合ネットワーク化された集中監視システムの要求がある。今後はディジタル回線の普及によって他のOA設備と接続され相互にデータを共有しあうシステムへの展開，さらに情報セキュリティとのより一層の統合強化が必要となる。

高速道路の料金収集の無人化を含む広域の交通情報・制御システム等も同様の事情にある。

6. 応用システム

この特集では三つの応用システム事例を紹介しているが，今後の応用システム構築における情報セキュリティの動向は次に集約される。すなわち，オープンシステム指向，マルチレベルセキュリティ(異なる機密区分データが共存する，複数の情報ドメイン／複数のセキュリティポリシーをサポート)，ハイレベルセキュリティ，相互運用性(他のセキュリティシステムとの通信及び相互認証)，システム構

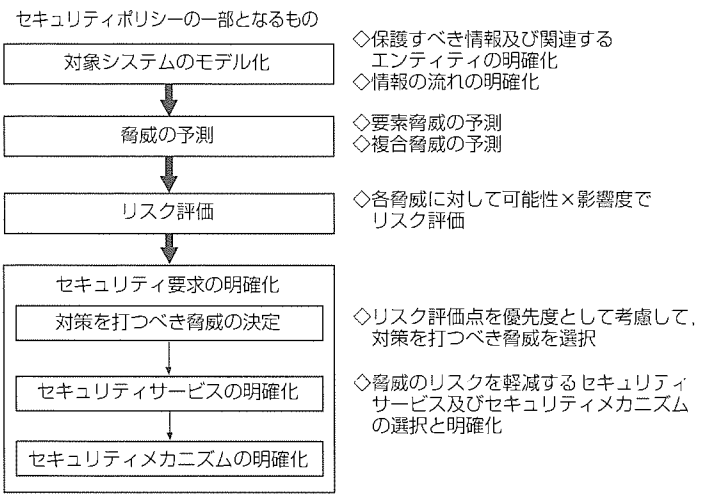


図5．リスク分析の手順

築とメンテナンスが容易であること等が求められる。そして，これらを実現するためには，**図4**に示すように，セキュリティ評価基準，セキュリティアーキテクチャ，システム構築手段である情報セキュリティの技術，製品の基盤が整備されることが前提として求められる。

また，対象となる業務，応用システムのリスク分析がシステム設計に先立って行われなければならない。**図5**にそのアプローチを示す。

7. むすび

暗号・セキュリティの技術／製品は，従来一部特定のユーザーマーケットに限定されたものであったが，最近のエレクトロニックコマース等の商用を意識した実験／試行段階を経て，今後は本格的に広く社会・公共のインフラへ浸透し実用化されていく段階に入ると思われる。

技術，製品の急速な進化・洗練，コスト低減，使い方と使う側を含めたシステムとしてのトータルなセキュリティの実現がより激しく求められるであろう。

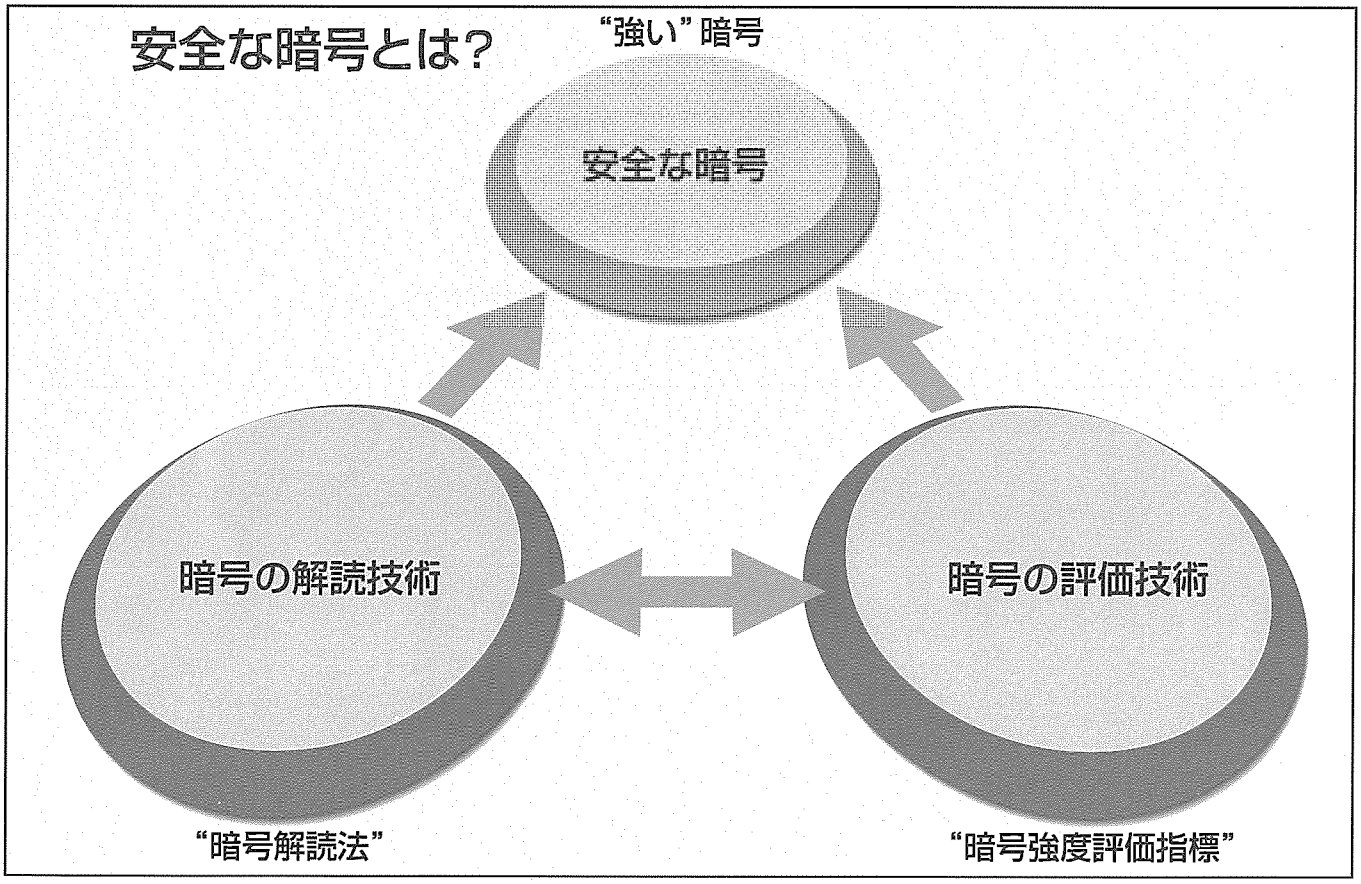
暗号解読・強度評価技術

時田俊雄*
松井　充*
反町　亨*

要　旨

かつて暗号技術が軍事目的を中心として用いられていた時代には，暗号アルゴリズムの詳細は機密であった。しかし，今日のように暗号がオープンネットワークでも利用されるようになると，暗号アルゴリズムは不特定多数の利用者によって共有されることが前提となるため，そのアルゴリズムの詳細は利用者には知られていると考えることが妥当である。このことを暗号強度の立場から見ると，“強い暗号”とは，第三者がそのアルゴリズムの詳細を知っていると仮定しても，暗号化に必要なかぎ(鍵)の情報を推定するのに必要な情報量又は計算量が十分大きいものでなければならない，ということを意味している。この情報量や計算量は実際にその暗号を“解読”すれば明らかとなるが，実際に解読できてしまう暗号は“弱い暗号”であり，私たちが必要とする“強い暗号”は解読できない暗号である。そこで，実際には解読を試みなくても，もし解読を試みるとどれくらいの情報量や計算量が必要となるかを評価できる指標，すなわち強度評価指標を得ることが重要となる。この意味で暗号強度評価技術と暗号解読技術とは表裏をなしていると言える。

また，このような暗号強度評価技術，暗号解読技術があって初めて暗号の性能評価ができるとともに，より強い暗号アルゴリズムの設計が可能となる。今後も暗号研究者にとって暗号解読技術，暗号評価技術の研究は不可欠である。



安全な暗号

安全な暗号とは，様々な暗号解読法に対して強い暗号のことである。したがって，暗号設計者はあらゆる暗号解読技術に精通している必要がある。また，設計した暗号の強度を評価するには，暗号強度評価技術は欠かすことができない。安全な暗号を設計するためには，暗号の解読技術と暗号の評価技術が必要不可欠である。

*情報技術総合研究所

1. まえがき

ディジタル時代の到来によって暗号技術はプライバシーの保護の観点から注目され，その技術内容や安全性に関する議論も公の場で活発に行われるようになってきた。この流れを決定付けたのは，1977年に米国で標準化された商用標準暗号DES(Data Encryption Standard[1])である。

DESは，政府によって仕様が完全に公開された点が画期的であった。当時，標準暗号制定の任にあった米国商務省標準局は，暗号機器の互換性を実現するために暗号アルゴリズムを公開とし，通信の安全性は送信者と受信者が秘密に共有する鍵のみによって実現することを目指した。

オープンネットワークで利用可能な暗号は，不特定多数によって共有されるため，DESのようにたとえ暗号アルゴリズムが公開されても，鍵の秘匿性によって通信の安全性が保たれなければならない。このような暗号方式は，近年の急激な通信網の広がりとともにますます必要とされている。

このことを暗号強度の立場から見ると，安全な暗号，すなわち強い暗号とは，第三者がそのアルゴリズムを知っていると仮定しても，通信路から得られた情報を基に鍵を推定するのに必要な情報量又は計算量が十分大きくなければならない。

'90年代に入って，DESを始めとするブロック暗号と呼ばれるタイプの暗号化方式に対する新しい解読法が幾つか発見され，大きな話題となった。これに伴い，解読法に対する暗号強度評価指標や，それに基づいた安全な暗号の設計指針が盛んに研究されている。

本稿では，まず暗号解読に対する一般的な考え方を解説し，特にブロック暗号の解読法を概観し，各解読法に対する暗号強度評価指標がいかに構築されるかを述べる。

2. 暗号攻撃の分類

暗号攻撃とは，解読者が暗号アルゴリズムを知っているとの条件で鍵を推定する試みである。その理論化のための前提条件として次の二つの仮定を置くのが普通である。

- 解読者は暗号文を自由に入手できる。
- 暗号文は一定の鍵で暗号化されている。

以下，上記の条件は満たされていると仮定する。また，暗号解読者は，暗号文だけではなく，平文に関する何らかの情報も知っていると想定するのが現実的である。そこで，この平文情報の種類によって暗号攻撃を次のように分類する。

2.1 暗号文単独攻撃

暗号文単独攻撃は，解読者は平文に関する何らかの統計的情報を持っているが具体的には平文は知らない，という条件での解読である。例えば日本語や英語などの自然言語は，統計的に偏りが大きい情報として知られている。したがって，平文が自然言語であれば，解読者がその言語に関する統計情報を持っていることは暗号解読の有力な手掛かりになる。

2.2 既知平文攻撃

既知平文攻撃とは，解読者は与えられた暗号文と対応する平文のペアを自由に入手可能との条件で鍵を求める解読条件である。ここで平文を得られるという条件は，例えば，暗号アルゴリズムを認証通信に用いたときには普通に起こり得る。**図1**は共通鍵暗号を用いた基本的な認証方法である。

ここで確認者と証明者は，あらかじめ同じ暗号アルゴリズムと同じ鍵を共有しているとする。認証の目的は，証明者が確認者に対して，この鍵を直接送信することなく，鍵を知っているという事実だけを相手に納得させることである。

認証のプロセスは以下のとおりである。まず，確認者は証明者に対して使い捨ての乱数Rを送付する。これに対して証明者は，この乱数を平文として，自分の持っている鍵Kで暗号化し，その結果得られた暗号文Cを確認者に送り返す。確認者は，自分で乱数を暗号化することができるので，これが証明者から送り返されてきたものと一致するかどうかで証明者の正当性を確認できる。

しかし，この認証方式の場合，第三者は通信路から平文Rと暗号文Cのペアを同時に得ることができる。したがって，通信の盗聴を続けていれば，Rが毎回変化するという正にその理由で，平文と暗号文のペアをたくさん手に入れることができ，既知平文攻撃の環境が成立する。

2.3 選択平文攻撃

選択平文攻撃は，既知平文攻撃という条件の上に，更に解読者が平文の内容を自由に指定できるという条件が加わる。したがって選択平文攻撃は解読者にとって極めて有利な条件と言えるが，これも実際の通信では起こり得ることである。例えば，**図1**の認証通信において，確認者に成り済ました第三者が自分で自由に生成したRを証明者に送った場合，偽の確認者は正しい証明者から対応する暗号文を自由に入手可能であり，選択平文攻撃の環境が成立する。

表1では，暗号文攻撃のための環境を，解読者が得られる又は操作できる平文に関する条件の点から分類した。

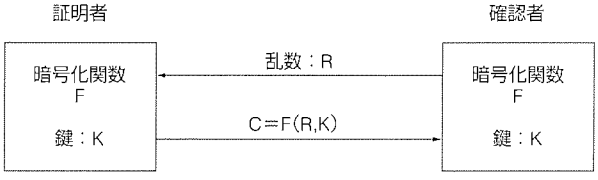


図1．共通鍵暗号を用いた認証

3. 暗号解読法と暗号強度指標

暗号解読の効率を表すパラメータとはすなわち暗号強度を示すパラメータであり，この意味で暗号解読と暗号強度評価はいわば表裏の関係にある。ここでは，共通鍵暗号，特にブロック暗号を対象に，現在有力とされる三つの代表的な暗号解読法を紹介し，その暗号強度指標を解説する。

3.1 全数探索法

(1) 全数探索法の概要

全数探索法とは，可能性のあるあらゆる鍵を一つ一つ総当たりでチェックする方法である。具体的には，与えられた平文を各鍵候補で暗号化し，これが与えられた暗号文と一致するかどうかで鍵を判別する。

したがって，全数探索法は基本的には既知平文攻撃であり，しかも平文と暗号文の組は一つしか必要でない。ただし，暗号文の数が多い場合には，暗号文単独攻撃にも用いることができる。この場合には，各鍵で復号した結果得られた情報の偏りがあらかじめ解読者の知っている平文の偏りと一致するかどうかで，正しい鍵を確率的に判別する。

以上から，全数探索法は，解読者が取得すべき情報量が少ないという点と，解読者は暗号アルゴリズムの詳細を知らなくても暗号装置さえあれば解読が実行できる点で，極めて現実的な解読法である。

(2) 全数探索法に関する暗号強度評価指標

全数探索法に対する暗号強度は，単純に鍵の長さで評価することができる。DESは56ビットの鍵が標準仕様であるが，前に述べたように，この長さは現在の技術水準から考えて，もはや安全であるとは言えないとされている。

また，幾つかの暗号で利用されている64ビットの鍵でも，暗号学的には不十分とされることが多い。さらに今後10～20年の予想される技術進歩を考慮すると，これから設計される暗号は100ビット程度以上の鍵の長さが必要というのが研究者の一般的な見方である。

3.2 差分解読法[2]

(1) 差分解読法の概要

差分解読法は，'90年にイスラエルのBihamとShamirによって発表された選択平文攻撃で，暗号アルゴリズムの内部構造を解析することによって実現する解読法であり，その原理は“平文の変化に対する暗号文の変化を統計的にとらえる”ものである。具体的には，解読者はあらかじめ平文Pの変化量$\Delta P(\neq 0)$と暗号文Cの変化量ΔCを固定し，次にランダムに与えた平文Pに対して次式(1)に示す定義で与えられる平均差分確率$DP(\Delta P \rightarrow \Delta C)$を調べる。

$$DP(\Delta P \rightarrow \Delta C) = Prob_P\{F(P+\Delta P) + F(P) = \Delta C\} \quad \cdots\cdots (1)$$

ここで，Fは暗号化関数を表し，＋はビットごとの排他的論理和演算を表すものとする。この式の意味は，入力平文をΔPだけ変化させたときに暗号文がΔCだけ変化する確率である。もしFが理想的にランダムであるならば，どんな$\Delta P(\neq 0)$やΔCに対しても$DP(\Delta P \rightarrow \Delta C)$は十分小さな値にならなければならない。

しかしながら，アルゴリズムによってはこの値が大きくなるようなΔPとΔCの組が見付かっており，このことが手掛かりとなって，それまで解読不可能であった幾つかの暗号が解読されたのである。一般に差分解読法の成功に必要な平文と暗号文のペアの数は，$DP(\Delta P \rightarrow \Delta C)$の逆数に比例することが知られている。

DESに対する全数探索法よりも高速な解読法は，差分解読法によって初めて与えられた。

(2) 差分解読法に関する暗号強度指標

暗号アルゴリズムの差分解読法に対する強度評価指標は，次式(2)で定義される最大平均差分確率で与えられることが知られる。

$$DP_{max} = \max_{\Delta P \neq 0, \Delta C} DP(\Delta P \rightarrow \Delta C) \quad \cdots\cdots (2)$$

ところが一般に，与えられた暗号アルゴリズムに対してDP_{max}の値を正確に求めるのは，膨大な計算量が必要なため，大変難しいとされている。このため，実用となっているほとんどの暗号アルゴリズムで，この値は知られていない。

そこで，これを求める代わりに暗号アルゴリズム$C = F(P)$を，より小さい部分関数F_1，F_2，F_3，…を用いて$C = Fn(\cdots(F_2(F_1(P))))$という形に分解し，$DP(\Delta P \rightarrow \Delta C)$や$DP_{max}$の代わりに次の式(3)，式(4)で定義される差分特性確率，最大差分特性確率を差分解読法に関する強度指標とするのが一般的である。

$$DP'(\Delta P_1 \rightarrow \Delta P_2 \rightarrow \cdots \Delta P_{n+1}) = \prod_{i=1}^{n} Prob_{Pi}\left\{F_i + (P_i + \Delta P_i) + (F_i(P_i) = \Delta P_{i+1})\right\} \quad \cdots\cdots (3)$$

$$DP'_{max} = \max DP'(\Delta P_1 \rightarrow \Delta P_2 \rightarrow \cdots \Delta P_{n+1}) \quad \cdots\cdots (4)$$

上式において，P_1は平文Pを，P_{i+1}（ただし，$1 \leqq i \leqq n-1$）は$F_i(P_i)$を，P_{n+1}は暗号文Cを表すものとする。また上記最大値は，$\Delta P_1 \neq 0$を満足するすべての$\Delta P_1, \Delta P_2, \cdots \Delta P_{n+1}$をわたるものとする（図2）。

BihamとShamirがDESに対して初めて差分解読法を与えたときも，正確には$DP'(\Delta P_1 \rightarrow \Delta P_2 \rightarrow \cdots \Delta P_{n+1})$の値が大きくなるような$\Delta P_i$の具体例を与えたのである。

一般にDP'_{max}の具体的な値を求めることも計算量的に容易ではないため，正確な値が知られていないブロック暗号が数多く存在している。

3.3 線形解読法[3]

(1) 線形解読法の概要

線形解読法は，'93年に当社が開発した解読法で，原理的

表1．解読者から見た暗号解読のための条件

	平文の入手	平文の生成
暗号文単独攻撃	×	×
既知平文攻撃	○	×
選択平文攻撃	○	○

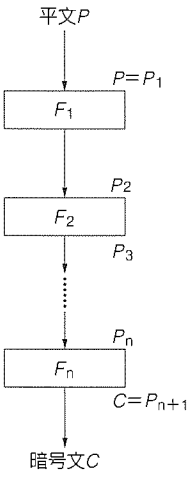


図2．n段ブロック暗号アルゴリズム

に既知平文攻撃法であるという特徴を持っている。これも暗号アルゴリズムの内部構造を解析することによって実現する解読法であり，その原理は“平文と暗号文のビット相関関係を統計的にとらえる”ものである。より具体的には，解読者はあらかじめ平文Pのマスク値ΓPと暗号文Cのマスク値$\Gamma C(\neq 0)$をそれぞれ固定し，次にランダムに与えた平文Pに対して次式(5)で定義される平均線形確率を調べる。

$$LP(\Gamma C \rightarrow \Gamma P) = |\ 2\mathrm{Prob}_P\{P\cdot\Gamma P = C\cdot\Gamma C\} - 1\ |^2 \quad \cdots\cdots (5)$$

ここで$(\cdot)$は，ビットごとの論理和をとった値のパリティ値（0又は1）を示している。式(5)の意味は，入力平文のうちΓPで指定されたビットのパリティが，暗号文のうちΓCの指定されたビットのパリティと一致する確率の1／2からの偏りの自乗ということである。

もし暗号化関数Fが理想的にランダムであるならば，どんなΓPや$\Gamma C(\neq 0)$に対しても，$LP(\Gamma C \rightarrow \Gamma P)$は小さな値にならなければならない。

しかしながら，アルゴリズムによってはこの値が大きくなるようなΓPとΓCの組が見付かっており，このことを手掛かりに，それまで解読不可能とされてきた幾つかの暗号が解読されたのである。一般に線形解読法の成功に必要な平文と暗号文のペアの数は，$LP(\Gamma C \rightarrow \Gamma P)$の逆数に比例することが知られている。

例えば，DESに対する初めての計算機による解読実験は，線形解読法によって与えられた。

(2) 線形解読法に関する暗号強度評価指標

暗号アルゴリズムの線形解読法に対する強度評価指標は次式(6)で定義される最大平均線形確率で与えられることが知られる。

$$LP_{max} = \max_{\Gamma C\neq 0,\Gamma P} LP(\Gamma C \rightarrow \Gamma P) \quad \cdots\cdots (6)$$

ところが一般に，与えられた暗号アルゴリズムに対して，LP_{max}の値を正確に求めるのは，膨大な計算量が必要なため，大変難しいとされている。このため，実用となっているほとんどの暗号アルゴリズムで，この値は知られていない。

そこで，LP_{max}を求める代わりに暗号アルゴリズム$C=F(P)$を，より小さい部分関数F_1，F_2，F_3，…を用いて$C=F_n(\cdots(F_2(F_1(P))))$という形に分解し，$LP(\Gamma C \rightarrow \Gamma P)$や$LP_{max}$の代わりに次の式(7)，式(8)で定義される線形特性確率，最大線形特性確率を線形解読法に関する強度指標とするのが一般的である。

$$LP'(\Gamma P_{n+1} \rightarrow \Gamma P_n \rightarrow \cdots \Gamma P_1) = \prod_{i=1}^{n} \left|2\mathrm{Prob}_{Pi}\left\{P_i\cdot\Gamma P_i = P_{i+1}\cdot\Gamma P_{i+1}\right\} - 1\right|^2 \quad \cdots\cdots (7)$$

$$LP'_{max} = \max LP'(\Gamma P_{n+1} \rightarrow \Gamma P_n \rightarrow \cdots \Gamma P_1) \quad \cdots\cdots (8)$$

ここで，P_1は平文Pを表し，P_{i+1}（ただし，$1\leqq i\leqq n-1$）は$F_i(P_i)$を，P_{n+1}は暗号文Cを表すものとする。また上記最大値は，$\Gamma P_{n+1}\neq 0$を満足するすべての$\Gamma P_1, \Gamma P_2, \cdots \Gamma P_{n+1}$をわたるものとする。

当社がDESに対して初めて線形解読法を与えたときも，正確には$LP'(\Gamma P_{n+1} \rightarrow \Gamma P_n \rightarrow \cdots \Gamma P_1)$の値が大きくなるような$\Gamma P_i$の具体例を与えたのであった。

一般にLP'_{max}の具体的な値を求めることも計算量的に容易ではないため，正確な値が知られていないブロック暗号が数多く存在している。

4. むすび

ブロック暗号の暗号解読技術や強度評価技術は，暗号学の中でも急速に発展している分野である。DESに代わる新しい標準となるべき暗号方式が望まれる中，新しい特徴を持ったブロック暗号の提案も盛んであり，暗号強度評価技術はこれらの性能評価のために重要な手段を与えている。

参考文献

(1) National Bureau of Standard：Data Encryption Standard, Federal Information Processing Standards, No.46, U.S.Department of Commerce (1987)

(2) Biham, E., Shamir,A.：Differential Crptanalysis of DES-like Cryptosystem, Proceeding of CRYPT'90-Advances in Cryptology, Lecture Notes in Computer Science, **537**, Springer Verlag (1990)

(3) Matsui, M.：Liner Cryptanalysis Method for DES, Proceeding of Eurocrypt'94-Advances in Cryptology, Lecture Notes in Computer Science, **765**, Springer Verlag (1993)

ブロック暗号アルゴリズム“MISTY”

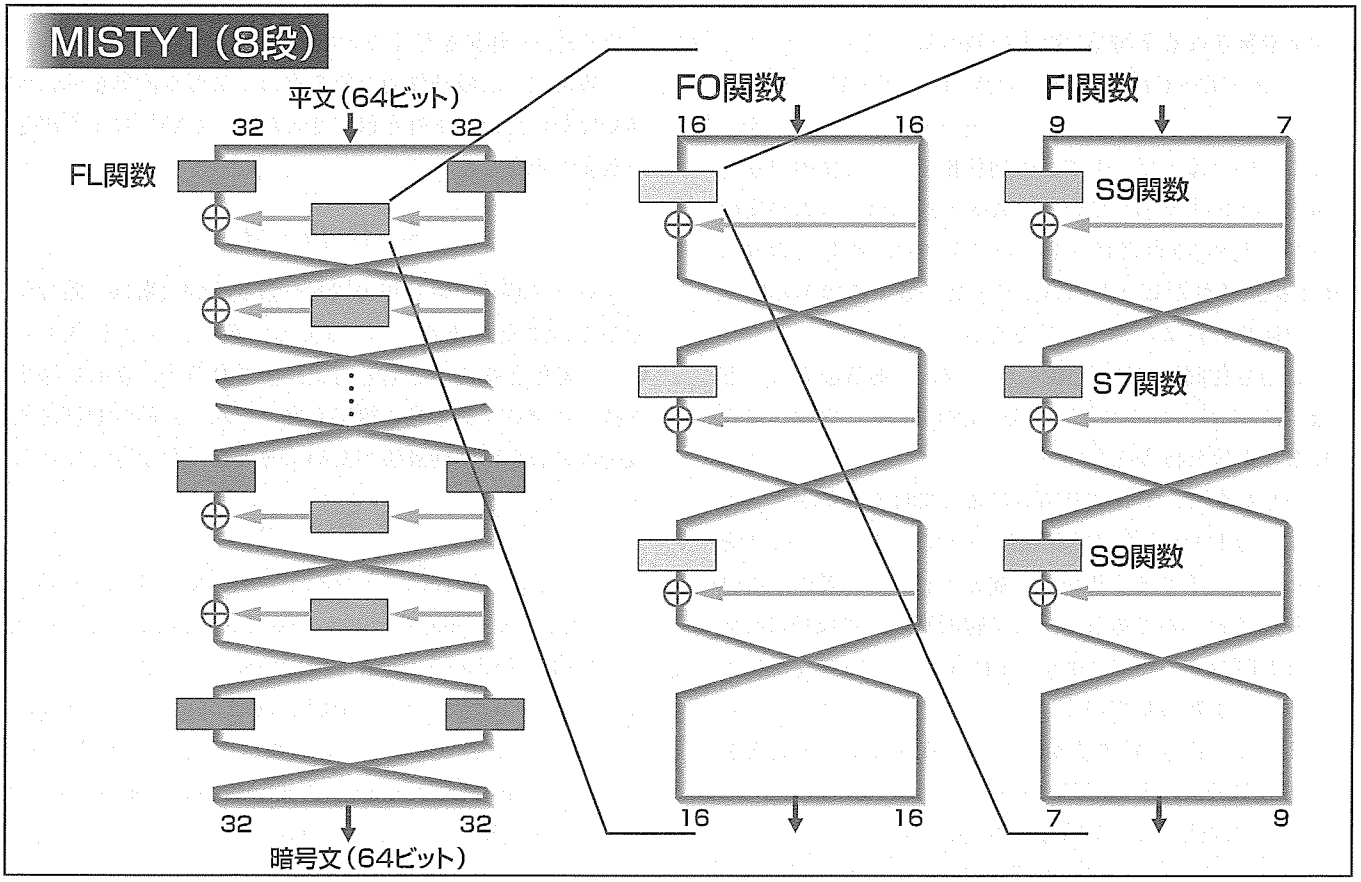
松井　充*
時田俊雄*
反町　亨*

要　旨

“MISTY”は三菱電機が開発した世界最高水準の安全性と実用性を兼ね備えた暗号アルゴリズムであり，その詳細仕様を公開することにより，オープンネットワークにおけるデータ通信やエレクトロニックコマースなどの分野で業界標準となることを目指している。アルゴリズムとしてはMISTY1とMISTY2の二つがあり，共に128ビットの暗号化かぎ(鍵)を持つ64ビットブロック暗号であり，MISTYはこれら二つのアルゴリズムの総称である。またMISTY1は，ISO(国際標準化機構)9979に13番目の暗号アルゴリズムとして登録済みである。

MISTYの特長は安全性と実用性が両立している点にある。安全性としては，ブロック暗号の各種の暗号解読法に対して十分な強度を持っている。特に差分解読法と線形解読法という二大解読法に対しては，その安全性が数学的に証明されている(これを“証明可能安全性”を持つという。)。次に実用性としては，暗号化処理の基本部であるデータランダム化部において，下のイメージ図のような構成とその構造を再帰的に採ることにより，暗号化関数の並列処理が可能となり(高速性)，また，最終的な暗号化関数(S7，S9)のサイズを小さくすることで，ソフトウェア及びハードウェアのテーブル(ロジック)サイズを小さくすること（小型化)が可能となる。例えば，0.8μmCMOSゲートアレーで512Mbpsの暗号化処理が可能であり，Pentium(注)100MHzで20Mbpsの処理速度を達成している。

(注) “Pentium”は，米国Intel Corp. の商標である。



MISTY1の暗号化処理部の基本構造

この図はMISTY1の暗号化処理部の全体構造（左図）とその主要部分であるFO関数の構造（中図），さらにFO関数に用いられるFI関数の構造（右図）を示している。

このようにMISTY1は，主要部分であるFO関数8段で構成され，さらにFO関数2段ごとにFL関数処理が行われ，64ビットの平文データを64ビットの暗号文データに暗号化する。

*情報技術総合研究所

1. まえがき

本稿では，当社が設計した暗号アルゴリズムMISTY1及びMISTY2について示す。MISTY1及びMISTY2はそれぞれ128ビットの暗号化鍵を持つ64ビットブロック暗号であり，その設計に当たって十分な安全性と，ハードウェア／ソフトウェアを問わずあらゆるプラットフォームでの高速性を両立させるように工夫を行った。これらの二つのアルゴリズムを総称してMISTYと呼ぶ。

以下では，MISTYを設計するに当たって設けた設計基準について述べる。なお本稿では，誌面の関係上，MISTY1を中心に述べる。MISTY1は，国際標準機関であるISO(ISO9979)に暗号アルゴリズムとして登録完了済みである。

また本稿では，読者自身による評価を助けるため，MISTY1のC言語によるサンプルプログラムを添付する。

2. MISTYの設計基準

MISTYを設計するに当たって，次の三つの基本設計基準(方針)を設定した。

2.1 安全性

方針1として，安全性に関して何らかの数値的根拠を持つこととした。

一般に実用的な暗号とは，固定長の暗号化鍵で多量のデータを暗号化しても現実的な意味で安全性が損なわれない方式であり，したがって，MISTYに無条件の安全性(情報理論的安全性)を求めることはもとより不可能である。しかしながら我々は，安全性に関して信頼性のある何らかの数値的根拠は必要と考えた。特にブロック暗号については，差分解読法と線形解読法に対する対策は暗号設計者にとって不可欠でありながら，現実にはほとんどすべてのブロック暗号で，これらの解読法に対する厳密な安全性は証明されていないのが現状である。そこで今回MISTYにおいて差分解読法と線形解読法に対する安全性を数値的に保証すること，すなわち証明可能安全性を実現させた。

具体的には，MISTYは，平均差分確率，平均線形確率が共に2^{-56}以下という十分な安全性を保証している。

2.2 高速性(ソフトウェア)

方針2として，プロセッサの種類によらず，ソフトウェアで実用的な性能を達成することとした。

最近提案される多くのブロック暗号アルゴリズムは，特定の仕様のプロセッサ(例えば32ビットALUを持つ等)上のソフトウェアで最高の速度を達成するように設計されているため，しばしばそれ以外の仕様のプロセッサでは性能が大きく低下する。

今回，特定の仕様のプロセッサで最高の性能を追求することよりも，あらゆるプロセッサで適度な高速性と小型化を実現することを重要視し，マルチプラットフォームに対応できることを選択した。

具体的には，例えば特定のプロセッサのみが高速な命令はMISTYには採用しない方針を採った。これにより，ソフトウェアでは，例えばIntel Pentium 100MHz上で20Mbps，またHP PA7200 120MHz上では40Mbpsの暗号化処理性能を実現することを確認した。

2.3 高速性(ハードウェア)

方針3として，ハードウェア上で十分な高速性を実現することとした。

ハードウェアに関しては，最近提案されるほとんどの暗号アルゴリズムがソフトウェアでの実現を前提としており，暗号アルゴリズムによっては，ハードウェアでは極端に規模が大きくなったり，又はソフトウェアに比べて速度向上が余り期待できないことがあることに注目した。今回，MISTYのハードウェアでの性能目標を，ソフトウェアでは実現不可能な数百Mbpsクラスの通信路にも対応できることとした。

具体的には，例えばテーブル参照命令の場合，ソフトウェアでは一般にそのテーブル内容と速度の関係は少ないのに対し，ハードウェアでは，場合によってはテーブルの内容を直接論理回路で構成することによって速度を飛躍的に改善できる場合がある。そこでMISTYでは，テーブル内容をハードウェア向きに可能な限り最適化するなど，ハードウェアの特性をできる限り生かした構成を採ることにした。この結果，例えばMISTY1の暗号化処理速度は，評価用チップにおいて，512Mbpsと非常に高速な処理速度を達成することを確認した。

3. 評価用サンプルプログラム

MISTY1の8段版のサンプルプログラムを図1に示す。一つ目はメインプログラムであり，二つ目のプログラムを呼び出している。二つ目はMISTY1アルゴリズムのコアロジックであり，128ビットの鍵を使ってECBモードによる暗号化及び復号処理を行う。

4. むすび

本稿では，当社が開発した暗号アルゴリズム“MISTY”についてその設計基準を中心に述べた。MISTYは安全性と高速性を兼ね備えた実用的なブロック暗号であると言える。

参考文献

(1) 松井　充：ブロック暗号アルゴリズムMISTY，電子情報通信学会技術報告，ISEC96-11 (1996)

(2) Matsui, M.：New Block Encryption Algorithm MISTY, 4th International Workshop of Fast Software Encryption, Lecture Notes in Computer Science, **1267**, Springer Verlag (1997)

(3) Schneier, B.：Applied Cryptography：Protocols, Algorithms and Source Codes in C, John Wiley & Sons, Inc.

```
/*****************************************************
 *                                                   *
 *    A Sample Main C Program of MISTY1 Algorithm    *
 *                                                   *
 *    Language  : Highly Portable C Language         *
 *    Coding by : Mitsuru Matsui / 14 May 1997       *
 *    Copyright : Mitsubishi Electric Corporation    *
 *                                                   *
 *****************************************************/
typedef unsigned long uint; /* 'short' also works fine. */
typedef unsigned char uchar;
extern uint EXTKEY[4][8];

main()
{
        static uchar text[16] =
        {0x01,0x23,0x45,0x67,0x89,0xab,0xcd,0xef,
              0xfe,0xdc,0xba,0x98,0x76,0x54,0x32,0x10};
        static uchar key[16]  =
        {0x00,0x11,0x22,0x33,0x44,0x55,0x66,0x77,
              0x88,0x99,0xaa,0xbb,0xcc,0xdd,0xee,0xff};
        int  i;

        printf( "Secret Key   " );
        for( i=0; i<16; i++ ) printf( "%02x ", key[i] );
        printf( "¥n" );
        printf( "Plaintext    " );
        for( i=0; i<16; i++ ) printf( "%02x ", text[i] );
        printf( "¥n" );
        misty1( text, key, 2, 0 );
        printf( "Extended Key " );
        for( i=0; i<8; i++ )
        printf( "%02x %02x ", (uchar)(EXTKEY[1][i]>>8),
        (uchar)(EXTKEY[1][i]&0xff) );
        printf( "¥n" );
        printf( "Ciphertext   " );
        for( i=0; i<16; i++ ) printf( "%02x ", text[i] );
        printf( "¥n" );
        misty1( text, key, 2, 1 );
        printf( "Plaintext    " );
        for( i=0; i<16; i++ ) printf( "%02x ", text[i] );
        printf( "¥n" );
}

/*****************************************************
 *                                                   *
 *    MISTY1 Block Cipher Algorithm (8-round/ECB)    *
 *                                                   *
 *    Language  : Highly Portable C Language         *
 *    Coding by : Mitsuru Matsui / 14 May 1997       *
 *    Copyright : Mitsubishi Electric Coporation     *
 *                                                   *
 *****************************************************/
typedef unsigned long uint; /* 'short' also works fine. */
typedef unsigned char uchar;
uint EXTKEY[4][8];

static uchar S7[128] = {
27,50,51,90,  59,16,23,84,  91,26,114,115,  107,44,102,73,
31,36,19,108,  55,46,63,74,  93,15,64,86,  37,81,28,4,
11,70,32,13,  123,53,68,66,  43,30,65,20,  75,121,21,111,
14,85,9,54,  116,12,103,83,  40,10,126,56,  2,7,96,41,
25,18,101,47,  48,57,8,104,  95,120,42,76,  100,69,117,61,
89,72,3,87,  124,79,98,60,  29,33,94,39,  106,112,77,58,
1,109,110,99,  24,119,35,5,  38,118,0,49,  45,122,127,97,
80,34,17,6,  71,22,82,78,  113,62,105,67,  52,92,88,125 };

static uint S9[512] = { 451,203,339,415,483,233,251,  53,385,
185,279,491,307,  9,  45,211,199,330,  55,126,235,356,403,472,
163,286,  85,  44,  29,418,355,280,331,338,466,  15,  43,  48,314,
229,273,312,398,  99,227,200,500,  27,  1,157,248,416,365,499,
 28,326,125,209,130,490,387,301,244,414,467,221,482,296,480,
236,  89,145,  17,303,  38,220,176,396,271,503,231,364,182,249,
216,337,257,332,259,184,340,299,430,  23,113,  12,  71,  88,127,
420,308,297,132,349,413,434,419,  72,124,  81,458,  35,317,423,
357,  59,  66,218,402,206,193,107,159,497,300,388,250,406,481,
361,381,  49,384,266,148,474,390,318,284,  96,373,463,103,281,
101,104,153,336,  8,  7,380,183,  36,  25,222,295,219,228,425,
 82,265,144,412,449,  40,435,309,362,374,223,485,392,197,366,
478,433,195,479,  54,238,494,240,147,  73,154,438,105,129,293,
 11,  94,180,329,455,372,  62,315,439,142,454,174,  16,149,495,
 78,242,509,133,253,246,160,367,131,138,342,155,316,263,359,
152,464,489,  3,510,189,290,137,210,399,  18,51,106,322,237,
368,283,226,335,344,305,327,  93,275,461,121,353,421,377,158,
436,204,  34,306,  26,232,  4,391,493,407,  57,447,471,  39,395,
198,156,208,334,108,  52,498,110,202,  37,186,401,254,  19,262,
 47,429,370,475,192,267,470,245,492,269,118,276,427,117,268,
484,345,  84,287,  75,196,446,247,  41,164,  14,496,119,  77,378,
134,139,179,369,191,270,260,151,347,352,360,215,187,102,462,
252,146,453,111,  22,  74,161,313,175,241,400,  10,426,323,379,
 86,397,358,212,507,333,404,410,135,504,291,167,440,321,  60,
505,320,  42,341,282,417,408,213,294,431,  97,302,343,476,114,
394,170,150,277,239,  69,123,141,325,  83,  95,376,178,  46,  32,
469,  63,457,487,428,  68,  56,  20,177,363,171,181,  90,386,456,
468,  24,375,100,207,109,256,409,304,346,  5,288,443,445,224,
 79,214,319,452,298,  21,  6,255,411,166,  67,136,  80,351,488,
289,115,382,188,194,201,371,393,501,116,460,486,424,405,  31,
 65,  13,442,  50,  61,465,128,168,  87,441,354,328,217,261,98,
122,  33,511,274,264,448,169,285,432,422,205,243,  92,258,  91,
473,324,502,173,165,  58,459,310,383,  70,225,  30,477,230,311,
506,389,140,143,  64,437,190,120,  0,172,272,350,292,  2,444,
162,234,112,508,278,348,  76,450 };

#define FL_enc( k ){
r1 ^= r0 & EXTKEY[0][k];
r3 ^= r2 & EXTKEY[1][(k+2)&7];
r0 ^= r1 | EXTKEY[1][(k+6)&7];
r2 ^= r3 | EXTKEY[0][(k+4)&7];
}
#define FL_dec( k ){
r0 ^= r1 | EXTKEY[0][(k+4)&7];
r2 ^= r3 | EXTKEY[1][(k+6)&7];
r1 ^= r0 & EXTKEY[1][(k+2)&7];
r3 ^= r2 & EXTKEY[0][k];
}
#define FI_key( k ){
```

図1．サンプルプログラム(1)

```
        r0  = EXTKEY[0][k] >> 7;
        r1  = EXTKEY[0][k] & 0x7f;
        r0  = S9[r0] ^ r1;
        r1  = S7[r1] ^ ( r0 & 0x7f );
        r1 ^= EXTKEY[0][(k+1)&7] >> 9;
        r0 ^= EXTKEY[0][(k+1)&7] & 0x1ff;
        r0  = S9[r0] ^ r1;
        EXTKEY[3][k] = r1;
        EXTKEY[2][k] = r0;
        EXTKEY[1][k] = r1 << 9 ^ r0;
        }
        #define FI_txt( a0, a1, k ){
        a1  = a0 >> 7;
        a0 &= 0x7f;
        a1  = S9[a1] ^ a0;
        a0  = S7[a0] ^ a1;
        a1 ^= EXTKEY[2][k];
        a0 ^= EXTKEY[3][k];
        a0 &= 0x7f;
        a1  = S9[a1] ^ a0;
        a1 ^= a0 << 9;
        }
        #define FO_txt( a0, a1, a2, a3, k ){
        t0  = a0 ^ EXTKEY[0][k];
        FI_txt( t0, t1, (k+5)&7 );
        t1 ^= a1;
        t2  = a1 ^ EXTKEY[0][(k+2)&7];
        FI_txt( t2, t0, (k+1)&7 );
        t0 ^= t1;
        t1 ^= EXTKEY[0][(k+7)&7];
        FI_txt( t1, t2, (k+3)&7 );
        t2 ^= t0;
        t0 ^= EXTKEY[0][(k+4)&7];
        a2 ^= t0;
        a3 ^= t2;
        }

/*****************************************
 *                                       *
 *   Encryption/Decryption Subroutine Body   *
 *                                       *
 *      misty1( text, key, block, mode )     *
 *                                       *
 *   text  : plain/ciphertext address  I/O   *
 *   key   : secret-key address        I     *
 *   block : number of text blocks     I     *
 *   mode  : 0:encryption 1:decryption I     *
 *                                       *
 *****************************************/
misty1( text, key, block, mode )
uchar *text,*key;
int    block,mode;
{
    register uint t0, t1, t2;
    register uint r0, r1, r2, r3;

/*** Key Scheduling ***/
    EXTKEY[0][0] = (uint)key[0]<<8  ^ (uint)key[1];
    EXTKEY[0][1] = (uint)key[2]<<8  ^ (uint)key[3];
    EXTKEY[0][2] = (uint)key[4]<<8  ^ (uint)key[5];
    EXTKEY[0][3] = (uint)key[6]<<8  ^ (uint)key[7];
    EXTKEY[0][4] = (uint)key[8]<<8  ^ (uint)key[9];
    EXTKEY[0][5] = (uint)key[10]<<8 ^ (uint)key[11];
    EXTKEY[0][6] = (uint)key[12]<<8 ^ (uint)key[13];
    EXTKEY[0][7] = (uint)key[14]<<8 ^ (uint)key[15];
    FI_key( 0 ); FI_key( 1 ); FI_key( 2 ); FI_key( 3 );
    FI_key( 4 ); FI_key( 5 ); FI_key( 6 ); FI_key( 7 );

/*** Data Randomizing ***/
    if( !(mode & 1) ){
/*** Encryption ***/
        while( block-- > 0 ){
            r0 = (uint)text[0]<<8 ^ (uint)text[1];
            r1 = (uint)text[2]<<8 ^ (uint)text[3];
            r2 = (uint)text[4]<<8 ^ (uint)text[5];
            r3 = (uint)text[6]<<8 ^ (uint)text[7];
            FL_enc( 0 );  FO_txt( r0, r1, r2, r3, 0 );
            FO_txt( r2, r3, r0, r1, 1 );
            FL_enc( 1 );  FO_txt( r0, r1, r2, r3, 2 );
            FO_txt( r2, r3, r0, r1, 3 );
            FL_enc( 2 );  FO_txt( r0, r1, r2, r3, 4 );
            FO_txt( r2, r3, r0, r1, 5 );
            FL_enc( 3 );  FO_txt( r0, r1, r2, r3, 6 );
            FO_txt( r2, r3, r0, r1, 7 );
            FL_enc( 4 );
            text[0] = r2 >> 8; text[1] = r2 & 0xff;
            text[2] = r3 >> 8; text[3] = r3 & 0xff;
            text[4] = r0 >> 8; text[5] = r0 & 0xff;
            text[6] = r1 >> 8; text[7] = r1 & 0xff;
            text += 8;
        }
    }
    else{
/*** Decryption ***/
        while( block-- > 0 ){
            r0 = (uint)text[0]<<8 ^ (uint)text[1];
            r1 = (uint)text[2]<<8 ^ (uint)text[3];
            r2 = (uint)text[4]<<8 ^ (uint)text[5];
            r3 = (uint)text[6]<<8 ^ (uint)text[7];
            FL_dec( 4 );  FO_txt( r0, r1, r2, r3, 7 );
            FO_txt( r2, r3, r0, r1, 6 );
            FL_dec( 3 );  FO_txt( r0, r1, r2, r3, 5 );
            FO_txt( r2, r3, r0, r1, 4 );
            FL_dec( 2 );  FO_txt( r0, r1, r2, r3, 3 );
            FO_txt( r2, r3, r0, r1, 2 );
            FL_dec( 1 );  FO_txt( r0, r1, r2, r3, 1 );
            FO_txt( r2, r3, r0, r1, 0 );
            FL_dec( 0 );
            text[0] = r2 >> 8; text[1] = r2 & 0xff;
            text[2] = r3 >> 8; text[3] = r3 & 0xff;
            text[4] = r0 >> 8; text[5] = r0 & 0xff;
            text[6] = r1 >> 8; text[7] = r1 & 0xff;
            text += 8;
        }
    }
}
```

図1．サンプルプログラム(2)

公開鍵暗号

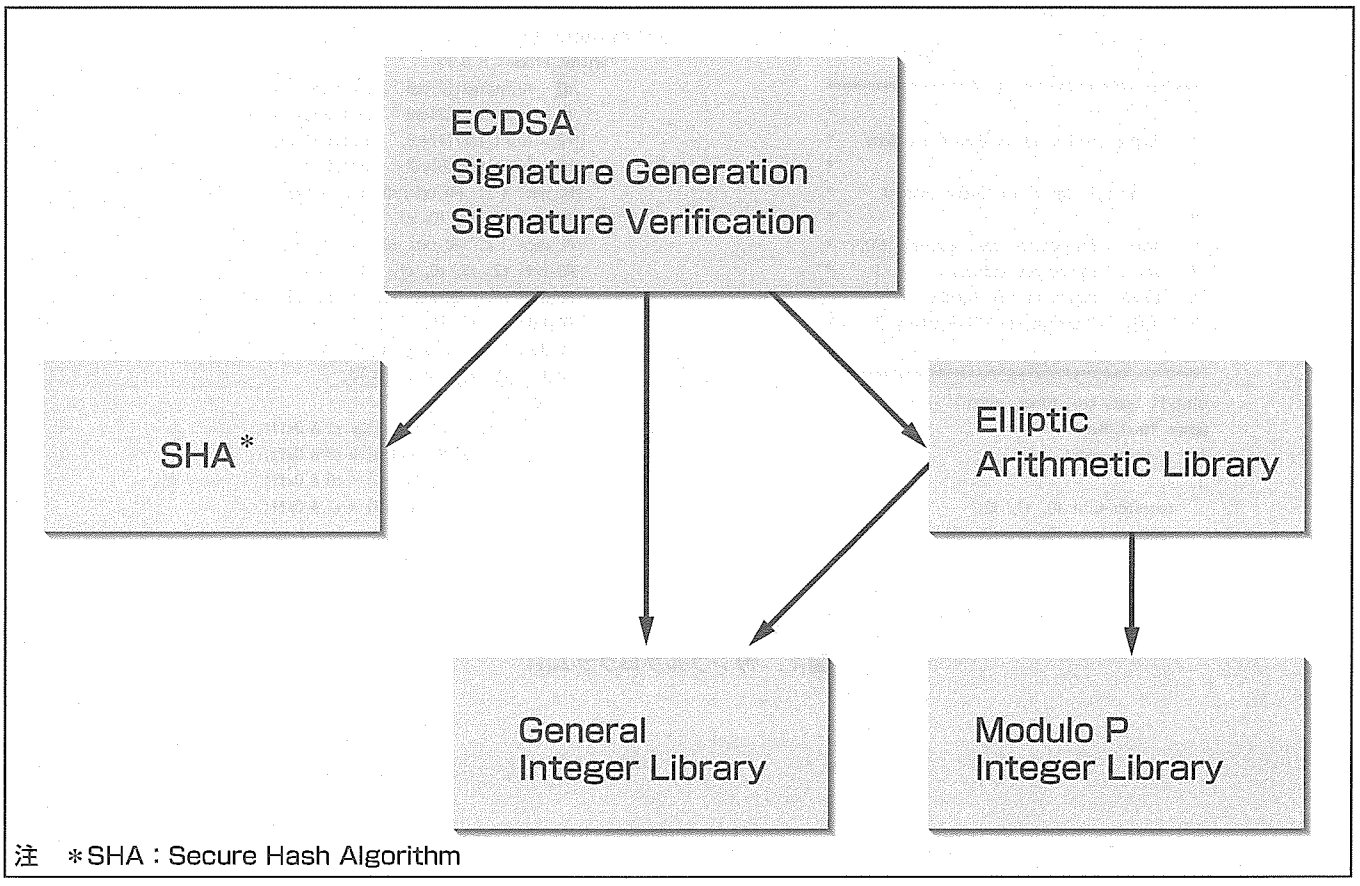
酒井康行*
長谷川俊夫*
中嶋純子**

要　旨

公開かぎ(鍵)暗号系の代表的アルゴリズムであるRSA暗号，だ(楕)円曲線暗号，及び超楕円曲線暗号の安全性と実装に関して考察する。RSA暗号の安全性の根拠は，素因数分解の困難さに置いているが，素因数分解対策を施さない鍵生成アルゴリズムによって生成された鍵は，512ビットの場合，パソコン1台で数十時間で解読される確率が低くないことを示した。また，最近その高速性から注目されている楕円曲線暗号において，標数Pの体上の曲線を用い，電子署名と検証を16ビットMPU上で世界で初めて実装した。ICカードは近年の情報セキュリティシステムにおいて重要な役割を果たしているが，実装に利用できるリソース(ROM／RAM)が少ないことから，プログラムサイズをいかに小さくするか，また速度とのトレードオフをいかにとるかが大きな問題となる。

本稿で述べる16ビットMPU上のソフトウェアは，小さいプログラムサイズで高速に電子署名や署名の検証を行えることから，ICカード上の実装に適したものである。また，楕円曲線暗号の拡張として，超楕円曲線暗号の基礎研究も近年活発である。超楕円曲線のヤコビ多様体上の離散対数問題を安全性の根拠とした，安全かつ実用的な暗号系を構成した。

これまで実用的速度が達成された超楕円曲線暗号はなかったが，本稿の公開鍵暗号は，スカラー倍算をAlpha 21164(250MHz)上のC言語で118msで実行でき，世界初の実用的超楕円曲線暗号である。



楕円曲線暗号ライブラリのソフトウェアアーキテクチャ

標数Pの体上の楕円曲線を用いた楕円曲線暗号ライブラリを作成した。楕円DSA署名，検証，ハッシュ関数の機能を搭載し，プログラムサイズ4Kバイトで高速に署名生成，検証が可能である。また，このライブラリは、RSA暗号にも利用可能である。

*情報技術総合研究所　**LSI事業推進センター

1. まえがき

秘密鍵暗号とともに現代暗号の中核をなす技術に公開鍵暗号がある。公開鍵暗号は，暗号化鍵と復号鍵が異なることが秘密鍵暗号との大きな違いである。公開鍵暗号の発明は，2000年以上の歴史を持つ暗号技術の中で，最も革命的な出来事の一つである。公開鍵暗号アルゴリズムによって，今日の情報セキュリティシステム構築に欠かすことのできないディジタル署名が実現され，また，秘密鍵暗号の使用において大きな問題となるデータの送受信者間での秘密鍵の共有という問題も解決された。

代表的な公開鍵暗号のアルゴリズムにRSA暗号，楕円曲線暗号，超楕円曲線暗号があるが，公開鍵暗号は一般に，大きな整数の演算を必要とするため，秘密鍵暗号と比べて処理速度が遅いという問題がある。また，公開鍵暗号アルゴリズムのパラメータ設定の際には，様々な解読法に耐えるための考慮が必要とされる。すなわち，速度と安全性が両立されるようなパラメータ設定が必要となる。

RSA暗号は，素因数分解を解く困難さに安全性の根拠を置いているが，素因数分解攻撃に十分な耐性を持つ鍵を生成しなければ，実際に解読される確率が低くないことが示されている[1]。楕円曲線暗号は，RSA暗号よりも高速に暗号化処理が行えることから最近注目され，IEEEやISOでも標準化作業が進められるなど，RSA暗号に代わるデファクトとなり得る暗号アルゴリズムである。しかし，最近の情報セキュリティシステムで重要な役割を演じているICカードへの実装のためには，プログラムサイズと速度との両立をいかに達成するかが問題となっている[2]。また，楕円曲線暗号を一般化した超楕円曲線暗号は，その演算量の多さから，演算効率が良く(速度が速く)かつ安全な暗号系の構成方法が課題となっている[3]。

そこで本稿では，①RSA暗号の素因数分解攻撃に対して安全な鍵生成法，②楕円曲線暗号の16ビットMPUへの効率的実装，③安全で速度効率の良い超楕円曲線暗号の構成，について検討した。その結果，RSA暗号の鍵生成法の検討に関しては，当社暗号ライブラリ“Power-MISTY”等に設計指針を与え，楕円曲線暗号の検討に関しては，16ビットMPU搭載ICカード等のセキュリティデバイスに実装可能なライブラリプログラムを開発することができた。

これらの結果は他の暗号応用製品への適用も可能であり，楕円曲線暗号はPower-MISTYへも搭載される予定である。また超楕円曲線暗号に関しては，これまで実用的速度が達成された例がなかったが，世界で初めて実用的超楕円曲線暗号の構成に成功した。

2. RSA暗号と素因数分解

この章では，安全なRSA暗号を設計するための鍵生成法を考察する。

2.1 素因数分解

公開鍵暗号技術では，数学的議論がしばしば行われる。暗号の安全性の根拠を数学的問題に帰着させて暗号が構成されるからである。整数論など，現代暗号の登場までは工学的応用の少なかった純粋数学が活躍する場でもある。RSA暗号はその安全性の根拠を素因数分解を解く困難さに置いており，RSA暗号を解読する一つの方法は，公開情報である法と呼ばれる大きな整数の素因数分解をすることである。一般に，大きな整数を素因数分解するためには，多大な計算が必要となる。素因数分解のアルゴリズムは，その計算量が，合成数の大きさで決まるもの(合成数依存型)と，素因数の性質で決まるもの(素因数依存型)の2種類に大別される。合成数依存型のアルゴリズムには，2次ふるい法，数体ふるい法，関数体ふるい法などがあり，素因数依存型のアルゴリズムには，楕円曲線法，P−1法，P+1法，ρ法などがある。

2.2 安全なRSA暗号鍵

RSA暗号の鍵生成に用いられる素数は，これらの素因数分解アルゴリズムに対して十分な耐性を持たなくてはならない。素因数分解は，たとえ合成数が大きくても，その素因数が小さかったり，ある種の性質を持つ場合は，素因数の発見が容易になる。RSA暗号に用いる素数Pは，次の性質を満たすことが必要と言われている。

(1) P−1は大きな素数tで割り切れる
(2) t−1は大きな素数rで割り切れる
(3) P+1は大きな素数sで割り切れる

RSA暗号は現在では公開鍵暗号のデファクトであり，様々なシステムに実装されている。その中には，上記の性質を満たしていない素数(鍵)を用いているものが少なくない。実際，条件(3)を考慮しない素数生成アルゴリズムによって生成された256ビットの素数Pを因数として持つ512ビット合成数N(512ビットRSA暗号鍵)を素因数分解実験したところ，パソコン1台で数十時間で分解できる確率が小さくないことが示された[1]。ただし，1,024ビット以上の鍵のRSA暗号の場合，上記の3条件を考慮せずにランダムに素数を生成しても，現在の素因数分解アルゴリズムや計算機能力では，容易に因数分解される確率は小さい。

3. 16ビットマイコンM16Cでの楕円曲線暗号の実装

公開鍵暗号は，秘密鍵暗号と比較して一般に演算量が多いため，処理時間がかかるという問題がある。最近のパソコンのような高性能な環境ではソフトウェアによる公開鍵暗号の処理時間やプログラムサイズは深刻な問題とはならない場合が多いが，計算能力やROM／RAMのサイズが限られているICカードのような環境では深刻さが増す。そのため，最近ではRSA暗号よりも処理速度の速い楕円曲

線暗号が注目されている。鍵長が160ビットで1,024ビット鍵長のRSA暗号と同じ安全性を達成でき，RSA暗号と比べて短い鍵長でよく，それによって小さなシステムパラメータ，バンド幅の節約，低消費電力につながる。我々は，当社の16ビットマイコンM16C(10MHz)上での標数P(Pは素数)の体上の楕円曲線暗号のソフトウェア実装を行い，暗号ライブラリを作成した[2]。M16Cは，移動体通信システムなどで幅広く使われている工業用マイコンである。

3.1 楕円曲線暗号実現方式

楕円曲線暗号は，速度効率の良さから，標数Pの体上の曲線又は標数2の体上の曲線が用いられる。ここで標数Pの体上の曲線上の楕円暗号は，標数2のものと比べて，CPUに搭載されている乗算器・除算器を有効に活用でき，また，既存のRSA用コプロセッサを流用でき，非常に優れた方式と考える。

3.2 楕円曲線暗号ライブラリの設計思想

次の4項目を設計の柱とした。

(1) 標数Pの楕円曲線を採用
(2) DSA署名生成，署名検証，ハッシュ関数の機能を提供
(3) プログラムサイズを4Kバイト程度以内に収める
(4) 楕円曲線暗号以外の暗号への適用可能性も重視

上記(1)は，標数Pの方式は既存の乗算剰余コプロセッサを使用することが可能であることと，CPUに搭載されている乗算器・除算器を有効活用できるという理由からである。(2)は，楕円DSA署名は現在最も標準化が進んでいるという理由による。(3)は，今回のターゲットであるM16C上のアプリケーションを考えた際に適切なサイズだからである。(4)は，RSAなどへの適用も重要と考えたからである。

3.3 ソフトウェアアーキテクチャ

作成した楕円暗号ライブラリは，次のようなソフトウェアアーキテクチャをとる。ライブラリは大きく分けて次の五つで構成される。

(1) Modulo Pによる演算ライブラリ
(2) 任意長の整数演算ライブラリ
(3) 楕円曲線上の演算ライブラリ
(4) 楕円曲線上のDSA署名作成，署名検証ライブラリ
(5) SHA演算ライブラリ

上記(1)は，楕円曲線の事前に固定されたパラメータに従って高速化のため最適化したライブラリである。(2)は，この楕円曲線暗号ライブラリをより汎用的に適用可能とするために任意長の整数演算が可能なライブラリである。

3.4 楕円曲線暗号ライブラリのパフォーマンス

実装したソフトウェア暗号ライブラリの詳細は**表1**及び次のとおりである。

標数Pの楕円曲線暗号をハードウェアに制約のある環境下で実際に十分高速に処理でき，小さなサイズの高速暗号ライブラリを提供できたことの意味は大きい。現在，ICカード上で実装された1,024ビット鍵RSA暗号の処理時間は，コプロセッサを搭載したもので署名生成に数百ms程度かかる。この値が専用ハードウェアを使用していることを考えれば，このライブラリはソフトウェアのみで実現しているので，十分に優位性がある。また，楕円曲線暗号では一般にDSA署名生成よりも署名検証の方が時間がかかるが，このライブラリでは処理の許容限度と考えられている1s以内で検証処理まで行える。さらに，このライブラリはRSA暗号の処理も可能である。

表1．楕円曲線暗号ライブラリ

動作環境	三菱電機工業用16ビットマイコンM16C(10MHz)
機能	(a) 160ビット鍵の楕円DSA署名生成，楕円DSA署名検証 (b) ハッシュ関数(SHA) (c) 一般的な多倍長整数演算機能
性能	(a) CODE／DATAサイズ　：約4Kバイト (b) 楕円曲線上のDSA署名生成：約150ms (c) 楕円曲線上のDSA署名検証：約630ms

3.5 プログラムサイズと速度とのトレードオフ

プログラムサイズと処理速度との間にはトレードオフがあるが，使用するシステムに応じて処理速度を多少犠牲にすることにより，プログラムサイズを更に小さくすることも可能である。また，プログラムサイズを増加させることによって処理速度を上げるという対応が可能である。

4. 超楕円曲線暗号の構成

楕円曲線暗号の拡張によって，超楕円曲線においても公開鍵暗号が構成できる[3]。有限体上の超楕円曲線Cのヤコビ多様体$J(C;F_q)$は有限可換群となり，離散対数問題が定義できる。この離散対数問題は，与えられたD_1，$D_2 \in J$に対して$D_1 = mD_2$を求める問題である。この離散対数問題を解くことの困難性を安全性の根拠にした公開鍵暗号が構成できる[3]。超楕円曲線暗号を特徴付けるパラメータに，曲線の種数g及び有限体F_qがある。なお，種数g＝1の曲線を楕円曲線と呼び，種数gが2以上の曲線を超楕円曲線と呼ぶ。この章では，曲線C：$v^2+v=u^{2g+1}$の場合に着目し，安全で速度効率の良い超楕円曲線暗号を構成し，実際に実装する。

4.1 安全な多様体の構成

次の条件を満たす多様体を構成する。

C1：多様体の位数$\#J(C;F_q)$が大きな素数で割り切れる
C2：多様体$J(C;F_q)$が小さな有限体F_q^kに写像されない
C3：種数gが定義体F_qに比べて大きすぎない($2g+1 < \log(q)$)

表2．安全な多様体

多様体	位数#J	#Jの最大素因数
$J(C;F_2^{59})$	178ビット	165ビット
$J(C;F_2^{89})$	267ビット	246ビット
$J(C;F_2^{113})$	339ビット	310ビット

条件C1は，離散対数問題の一般的解法であるPohlig-Hellman法に対する安全条件である。条件C2は，MOV-reductionを超楕円曲線の場合に一般化したFreyらの方法に対する安全条件である。楕円曲線又は超楕円曲線上の離散対数問題は，曲線を注意深く選べば，解くのに有限体(多様体)の大きさの指数時間かかる。しかし，有限体上の離散対数問題は，準指数時間で解けるアルゴリズムが知られている。したがって，小さな有限体に写像されない多様体を選ぶことが必要である。条件C3は，種数gが大きすぎる場合，準指数時間で解かれることがあり，その安全条件である。ただし，この条件C3は，種数gが小さい場合はほとんど問題にならない。

安全な多様体を構成するためには，まず多様体$J(C;F_q)$の位数#Jが計算できなければならない。与えられた多様体の位数を計算することは，楕円曲線の場合と同様，一般には計算量的に難しい問題である。しかし，ある種の曲線に関しては，容易に計算できる[3]。本稿では，Weil予想に基づいて多様体の位数を計算する方法を用いた。

探索の結果，種数g＝3でF_2上の曲線$C: v^2+v=u^7$の場合で，次のような多様体が得られた(表2)。

$J(C;F_2^{59})$は1,024ビット鍵のRSA暗号，$J(C;F_2^{89})$は2,048ビット鍵のRSA暗号，$J(C;F_2^{113})$は5,000ビット鍵のRSA暗号と同等の安全性がある。

4.2 超楕円曲線暗号の実装

実用的観点からは，暗号の安全性とともに，速度が重要な要素となる。一般のアーベル多様体$A(F_q)$の位数は，$(q^{1/2}-1)^{2g} \leqq \#A(F_q) \leqq (q^{1/2}+1)^{2g}$となることが知られている。したがって，多様体の位数が同じ場合は，種数gが大きいほど定義体の大きさは小さくなる。ヤコビ多様体の群演算は楕円曲線上の点の加算に比較して，一般に複雑であるが，定義体が小さくできることから，演算の複雑さの差ほどには速度差は生じない。

本稿で得られたg＝3の曲線の$J(C;F_2^{59})$は，暗号化演算がすべて59ビット以下の整数によって行われる。RSA暗号や楕円曲線暗号は大きな整数の多倍精度演算が必要であるのに対し，$J(C;F_2^{59})$は，64ビットCPU上では通常の大きさの整数で演算できるため，実用的な速度を達成できる。実際，実装して速度を計測したところ，Alpha 21164(250MHz)上のC言語で，スカラー倍算(暗号化の基礎となる演算)を118msで実行できた[4]。これまで超楕円曲線暗号の実用化研究はなされておらず，本稿で述べた暗号は，初の実用的超楕円曲線暗号である。

5. むすび

楕円曲線暗号は，曲線を注意深く選べば，解読にかかる計算量は鍵サイズの指数関数となる。したがって，RSA暗号よりも鍵サイズが小さくでき，その結果高速処理が可能となることから今後ますます普及していくことが予想され，実装上の観点からの研究は重要なテーマの一つである。また，超楕円曲線暗号は，より効率の良い群演算が行える曲線のクラスを見付け，32ビットCPUで実用的速度を得ることが今後の課題である。

参考文献

(1) Sakai, Y., Sakurai, K., Ishizuka, H.：On Weak RSA-keys produced from Pretty Good Privacy, Lecture Notes in Computer Science, 1334, (ICICS97), 314～324 (1997)

(2) Hasegawa, T., Nakajima, J., Matsui, M.：A Practical Implementation of Elliptic Curve Cryptosystems over GF(p) on a 16-bit Microcomputer, to be appeared at PKC98 (1998)

(3) Sakai, Y., Sakurai, K., Ishizuka, H.：Secure Hyperellitic Cryptosystems and Their Performance, to be appeared at PKC98 (1998)

(4) 酒井康行，石塚裕一，櫻井幸一：安全な超楕円曲線暗号の構成とその実装，暗号と情報セキュリティシンポジウム(SCIS98) (1998)

三菱電機情報セキュリティアーキテクチャ

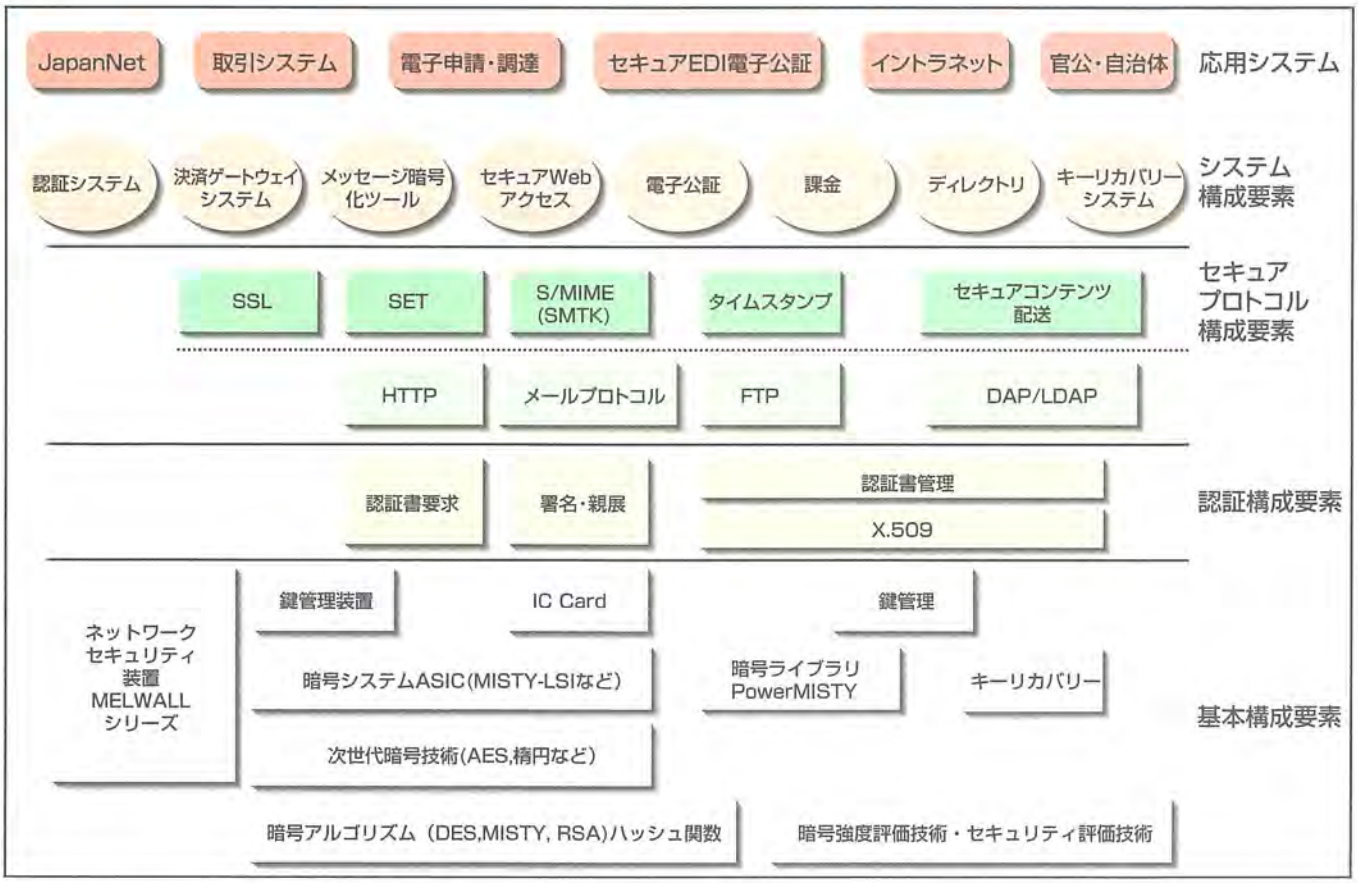
勝山光太郎*　米田　健*
藤井誠司**
鈴木　博***

要　旨

インターネットの爆発的普及により，盗聴，改ざん，成り済ましといった脅威から情報システムを安全に守ることが，これまで以上に大きな課題となっている。これまで，情報の秘匿に重点のあった情報セキュリティ技術も，公開かぎ(鍵)のインフラ構築により，認証や否認防止といった面での応用が展開されるようになってきた。

情報セキュリティの適用分野を特定秘匿型，協調交流型，参加閲覧型，大規模不特定認証型の四つに大別し，これらに適用するセキュリティソリューションとして，セキュア通信ソリューション，セキュアメールソリューション，セキュアWebアクセスソリューション，セキュア認証システムソリューション，セキュアEDIソリューション，セキュアECソリューションを実現する。

これらのソリューションを提供するための構成要素を定義したものが，情報セキュリティアーキテクチャである。基本構成要素，認証構成要素，セキュアプロトコル構成要素，システム構成要素の4階層からなる。基本構成要素は，暗号アルゴリズム，暗号強度評価技術を基盤とし，暗号ASICや暗号ライブラリで構成される。認証構成要素は，認証書を扱うライブラリ群からなる。セキュアプロトコル構成要素は，SSL(Secure Socket Layer)やS／MIME(Multimedia Internet Mail Extension)といったプロトコルの規格に準拠したライブラリ群からなる。システム構成要素は，認証システムや電子公証システムといった要素からなる。これらを利用して様々な応用システムが構築される。



三菱電機情報セキュリティアーキテクチャ

情報セキュリティアーキテクチャは階層構造をとり，基本構成要素，認証構成要素，セキュアプロトコル構成要素，システム構成要素からなる。これらを組み合わせて応用システムを構築する。

20(408)　*情報技術総合研究所(工博)　**同研究所　***情報システム製作所

1. まえがき

インターネットの爆発的な普及とともに，これまで企業において専用線や企業内LANを用いて構築されてきたシステムにインターネットが加わり，盗聴，改ざん，成り済まし，受信否認，送信否認といった脅威が現実のものとなってきている。こうした脅威から情報システムを安全に守るために，暗号技術を利用した情報セキュリティ技術の重要性に関する認識が高まってきている。これまで暗号技術は秘匿を主に対象としてきたが，公開鍵インフラの構築により，認証や否認防止といった面での応用が展開されるようになってきた。

本稿では，最初に情報セキュリティ適用分野とそれに対応するソリューションを述べる。さらに，それらのシステム構築に必要となる情報セキュリティアーキテクチャについて概観する。

2. 情報セキュリティ適用分野

ネットワークの規模や業務形態，そこでのセキュリティレベルを考えたときに，**図1**に示すような四つの形態に大きく分類できる。

(1) 特定秘匿型

役員情報OAシステム，官公庁で高い機密性が要求されるシステムなどで，閉じたグループでの秘匿通信や認証・アクセス制御を必要とする形態である。

(2) 協調交流型

グループウェア，ワークフロー，電子メールなどを利用したシステムにおいて，ディジタル署名による認証やセキュアにメールが送れることを必要とする形態である。

(3) 参加閲覧型

分散遠隔会議システム，衛星情報配信，地域公共サービスシステム，Webによる有料情報提供サービスに見られるような認証・アクセス制御を必要とする形態である。

(4) 大規模不特定認証型

エレクトロニックコマースやセキュアEDIといった不特定の人の認証，及びお金を扱うためにより高度なセキュリティを必要とする形態である。

3. セキュリティソリューション

上記で述べた適用分野に対して，システム構築と運用の面から以下で述べるソリューションの中の幾つかを組み合わせて顧客の要求を満足するセキュアなシステムを構築することが可能となる。**図1**に，適用するソリューションの例を併せて記述する。

(1) セキュア通信ソリューション

ネットワークレベルでの様々な脅威，すなわち，盗聴，成り済まし，改ざんに対してセキュリティを確保した通信機能を実現する。

(2) セキュアメールソリューション

盗聴，成り済まし，改ざんといった脅威に対して，安全なメールシステムを実現する。

(3) セキュアWebアクセスソリューション

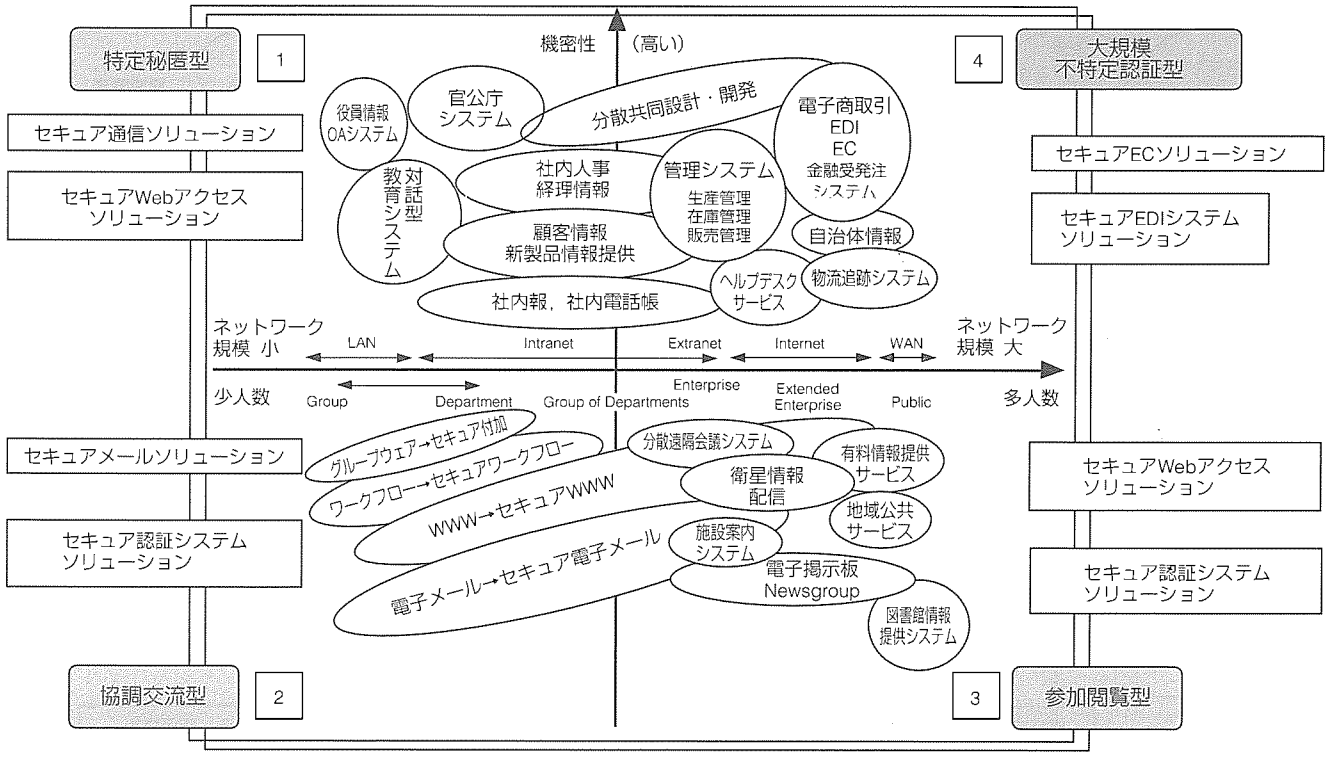


図1．セキュリティ利用システム分野と適用ソリューション

WWWサーバの種類に依存せず，セキュアWebアクセスを実現する。WWWブラウザからのWebアクセスに対し，MISTYによるネットワーク上のデータの暗号化，ディジタル証明書を利用した確実なユーザー認証によるWWWサーバへのアクセスを実現する。

(4) セキュア認証システムソリューション

セキュアメール／Webアクセスを利用する際に，“個人認証”“ディジタル署名”を行うための認証システムプラットフォームを実現する。

(5) セキュアEDIソリューション

企業間の電子商取引(EC)をインターネット環境で実現したい企業に対し，取引データの暗号化通信機能により，企業間コミュニケーションの安全性を実現する。

(6) セキュアECソリューション

通商産業省の電子商取引推進事業プロジェクト“JapanNet”で得られた成果を基に，最高水準の認証技術・暗号技術を利用したオープンネットワークでの安全で信頼性の高い商取引を実現する。

4. 情報セキュリティアーキテクチャ

以上述べてきたソリューションを実現するために必要となる情報セキュリティアーキテクチャを図2に示す。大きく四つの階層，すなわち，基本構成要素，認証構成要素，セキュアプロトコル構成要素，システム構成要素に分かれる。そして，これらを利用して応用システムが構築される。

以下，これらの構成要素について述べる。

4.1 基本構成要素

(1) 暗号アルゴリズム

MISTY，DES(Data Encryption Standard)，RSA(Rivest，Shamir，Adelman：開発者の名前の頭文字)といった暗号アルゴリズムの設計技術である。

(2) 次世代暗号技術

ブロック暗号の事実上の世界標準であるDESの次の世代のブロック暗号として標準化が進められているAES(Advanced Encryption Standard)，及び公開鍵方式の一つである楕円暗号のアルゴリズム設計技術である。

(3) 暗号強度評価技術，セキュリティ評価技術

線形解読法や差分解読法を始めとする暗号解読技術を利用した暗号の強度評価技術，及びシステムのセキュリティ脅威分析やリスク分析に基づくセキュリティ評価技術である。

(4) 暗号システムASIC

MISTYやDES，RSA及び楕円といった暗号アルゴリズムを実装したASICで，スマートカード，携帯端末，ディジタル放送機器への組込みが可能である。

(5) 鍵管理装置

鍵を耐タンパー性のあるハードウェアで保護する管理装置である。鍵生成を装置内で実施することで，鍵が一切装置外に出ることなく，高いセキュリティを保つことが可能となる。

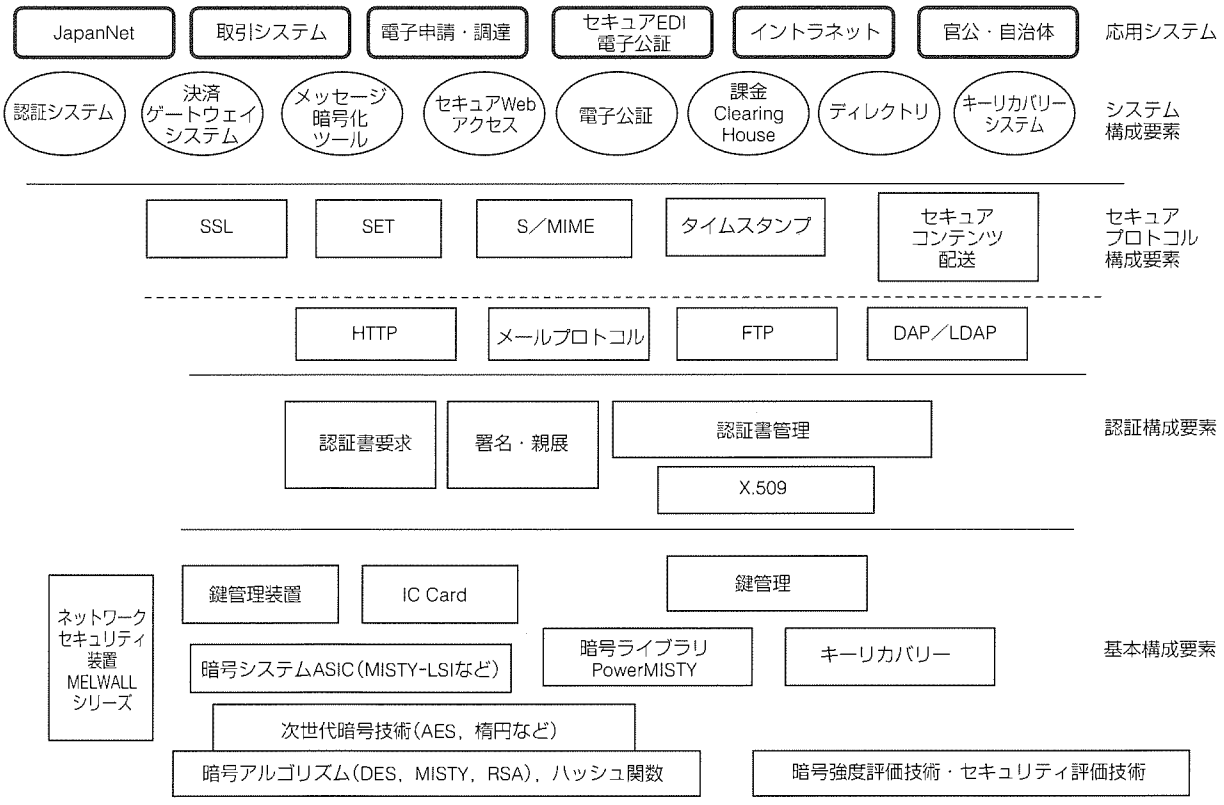


図2．三菱電機情報セキュリティアーキテクチャ

(6) ICカード

暗号アルゴリズム内蔵のICカードである。ICカードのセキュリティ機能と携帯性により，本人認証のためのカードとして利用可能である。

(7) 暗号ライブラリ“PowerMISTY”

MISTY，DES，RSAを始めとする各種暗号アルゴリズム，及びMD5，SHA1などのハッシュ関数を実装したライブラリである。

(8) キーリカバリー

輸出規制，鍵紛失時の対策を考慮し，鍵回復を実現するためのメカニズムを実装したライブラリである。

(9) 鍵管理

一つの計算機上で幾つもの鍵を操作する必要があり，公開鍵の秘密鍵を安全に効率良く管理するためのライブラリである。

(10) ネットワークセキュリティ装置

VPN(Virtual Private Network)を暗号を利用して構築するための，暗号ハブや暗号アダプタといった装置である。

4.2 認証構成要素

(1) 認証書要求ライブラリ

ディジタル認証書の認証局(Certification Authority：CA)に対する発行要求を実現するためのライブラリである。

(2) 署名・親展ライブラリ

ディジタル署名，親展を実現するためのライブラリである。

(3) X.509ライブラリ

ディジタル認証書の標準であるITU規格のX.509に準拠した形式を扱うためのライブラリである。

(4) 認証書管理ライブラリ

ディジタル認証書の格納，取出し，検証，及び保存といった機能を実現するライブラリである。

4.3 セキュアプロトコル構成要素

(1) SSL

TCP(Transmission Control Protocol)上にセキュアな通信路を確立するためのプロトコルである。

(2) SET(Secure Electronic Transaction)

Visaとマスターカードによって標準化が推進されているクレジットカード決済を実現するためのプロトコルである。

(3) S／MIME

メールをセキュアに送受信するためのプロトコルである。

(4) タイムスタンプ

時刻保証と改ざん防止を実現するタイムスタンプのプロトコルである。

(5) セキュアコンテンツ配送

ディジタルコンテンツをセキュアに配送するとともに，課金の仕組みを提供するプロトコルである。

4.4 システム構成要素

(1) 認証システム

ディジタル認証書を発行し，管理するシステムである。

(2) 決済ゲートウェイシステム

SETプロトコルを始めとする各種決済のためのゲートウェイ機能を実現するシステムである。

(3) メッセージ暗号化ツール

ファイルに対するディジタル署名，親展を行うツールで，メールソフトと連携してセキュアメール機能を実現する。

(4) セキュアWebアクセス

ディジタル認証書による認証と，それに基づくWebのアクセス制御及び暗号化通信を実現するシステムである。

(5) 電子公証

タイムスタンプ機能と秘密分散による秘匿保存機能を実現するシステムである。

(6) 課金

セキュアコンテンツ配送機能からの課金情報の収集と，それに基づく課金を実現するシステムである。

(7) ディレクトリ

ディジタル認証書の格納及び検索，ディジタル認証書の失効情報であるCRL(Certification Revocation List)の格納を行うシステムである。

(8) キーリカバリーシステム

鍵回復を行うためのセンター機能を実現するシステムである。

5. むすび

情報セキュリティの適用分野と，それに対するソリューション，そして，それらを実現するための情報セキュリティアーキテクチャについて概観した。現在，このアーキテクチャに基づいて開発された構成要素を利用して幾つかの応用システムが構築されており，実証が進んでいる。

今後は，更に多くの実証を通じてアーキテクチャの有効性の検証を進めるとともに，新しい暗号アルゴリズムの開発や，それに基づくインフラの提案を実施していく所存である。

共通鍵暗号“MISTY”評価用LSI

加藤潤二*　松井　充**
反町　亨**
市川哲也***

要　旨

近年，インターネットの普及，エレクトロニックコマースの実現に見られるように，オープンネットワークの利用が身近なものになってきている。しかしながら，オープンネットワークを利用して個人情報のやり取りや企業間の取引・決済などの電子商取引を行う場合，情報の盗聴，改ざん，成り済まし等が行われる可能性が高く，情報をいかに他者に漏らすことなく安全に送受信するかが最大の課題であり，安全な情報通信を実現するために，暗号技術をシステムに組み込むことが重要である。

その暗号技術を実現する方法として，ソフトウェア又はハードウェアで実装する方法がある。ところが，ソフトウェアでは数十Mbps程度のスループットしか実現できず，高速通信への対応のためには暗号アルゴリズムをハードウェアで実現することが必す(須)となってきている。

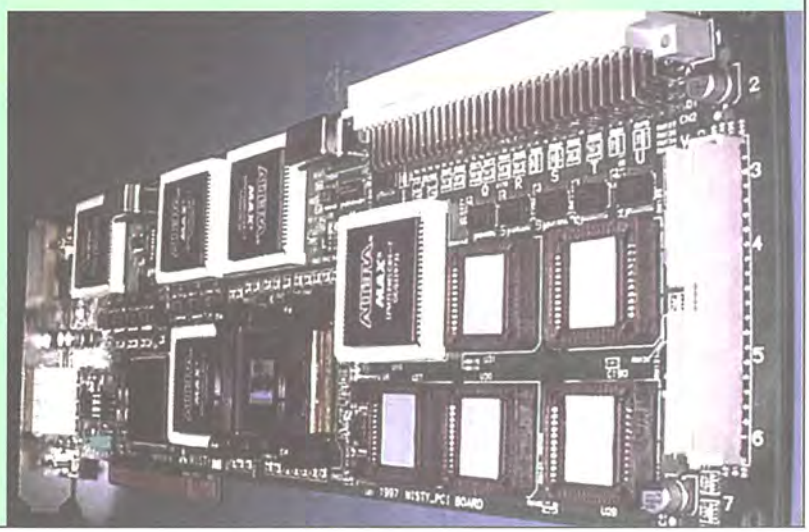
今回，三菱電機㈱が独自開発した秘密かぎ(鍵)暗号アルゴリズム“MISTY”の高速・高性能を，客先の評価によって実証し，情報通信システムにおいて暗号アルゴリズムMISTY及び当社暗号LSIを採用してもらうことを目的として，MISTY評価用LSI及びその評価システムの開発を行った。その結果，256Mbpsという世界最高速レベルのLSIを開発したので紹介する。

秘密鍵暗号アルゴリズム評価用LSI M64409FPの特長

- 三菱電機が開発した高速・高性能な秘密鍵暗号アルゴリズムMISTYを採用
  ブロック長:64ビット　鍵:128ビット
- 208QFP
- ISO規定暗号モード準拠(ECB,CBC,OFB-64,CFB-64)
- 処理速度　256Mbps
- 32ビットI／Oポート装備
- 消費電力　1.5W

M64409FP評価システム

- M64409FPを用い,MISTY高速演算性能の評価を実現
- 5V単一電源のPCI標準長カード
- ソフトウェア(PowerMISTY)とハードウェア(この評価基板)の演算結果の比較及び処理速度の表示が可能
- PCIバスマスタ方式を採用することによるDMA機能



評価用LSI及び評価システムの特長

M64409FPは，三菱電機が開発した高速・高性能秘密鍵暗号アルゴリズム“MISTY”をハードウェアで実現した。これを使用して評価システムを構築し，その高速演算性能の評価を実現できる。

*三菱電機㈱システムLSI事業化推進センター　**同情報技術総合研究所　***三菱電機エンジニアリング㈱

1. まえがき

近年，インターネットの普及とエレクトロニックコマースが実現する一方で，情報をいかに他者に漏らすことなく安全に送受信するかが最大の課題であり，暗号技術をシステムに組み込むことへの要求が高まりつつある。

暗号技術を実現する方法として，ソフトウェア又はハードウェアで実装する方法がある。ところが，ソフトウェアでは数十Mbps程度のスループットしか実現できず，高速通信への対応のためには暗号アルゴリズムをハードウェアで実現することが必須となってきている。

採用した秘密鍵暗号アルゴリズム“MISTY”[1]は，1996年に松井によって提案された128ビットの暗号鍵を持つ64ビットブロック暗号である。暗号アルゴリズムMISTYは，ブロック暗号の汎用的な解読法として最も強力なものとされている差分解読法[2]や線形解読法[3]に対する安全性が数値的に保証されるように設計が行われている。また，並列処理構造を強く意識して設計されており，ハードウェアや並列処理可能なプロセッサ上では高い処理能力を発揮することができる。

今回，秘密鍵暗号アルゴリズムMISTYを高速で実現する評価用LSI(M64409FP)の開発を行った。

本稿では，チップ設計開発及びこれを用いた評価システムについて述べる。

2. LSI設計

2.1 アーキテクチャ

図1にM64409FPのブロック図を示す。このLSI設計では，まず，評価用のLSIであることを考慮に入れ，暗号化モードをISOで規定されている暗号化モードであるECB(Electric Code Book)，CBC(Cipher Block Chaining)，OFB(Output FeedBack)，CFB(Cipher FeedBack)の4モードをすべてサポートした。また，評価システムとして，現在一番汎用的であると思われる32ビットバスに対応し，次に処理予定の鍵，IV(Initial Value)データをスムーズに更新可能なように，それぞれ32ビット幅のデータ用入力ポート，出力ポート，鍵，IV入力ポートを備えている。

これらの条件を満足し，暗号化処理性能及び汎用的なASICで実装可能なゲート規模を検討した結果，大きく分けて八つのブロック構成とした。以下に各ブロック機能を述べる。

(1) テキスト入力ブロック

32ビット単位で入力されるテキストを64ビット単位に整形し，データセレクタブロックへの受渡しを行う。

(2) テキスト出力ブロック

64ビット単位の暗号化結果をMISTYコアブロックから受け取り，32ビット単位に分割して出力する。また，使用される暗号化モード(OFB，CFB)によっては，このブロックで入力されたテキストデータと擬似乱数として生成されたMISTYの暗号化結果を排他的論理和とすることも行う。

(3) IVレジスタブロック

32ビット単位で入力されたIVデータを64ビット単位に整形し，データセレクタブロックへの受渡しを行う。

(4) 鍵レジスタブロック

32ビット単位で入力されたIVデータを，128ビット単位に整形する。また，拡大鍵生成関数を用いて新たに128ビットの拡大鍵データを生成し，元の鍵を合わせた256ビッ

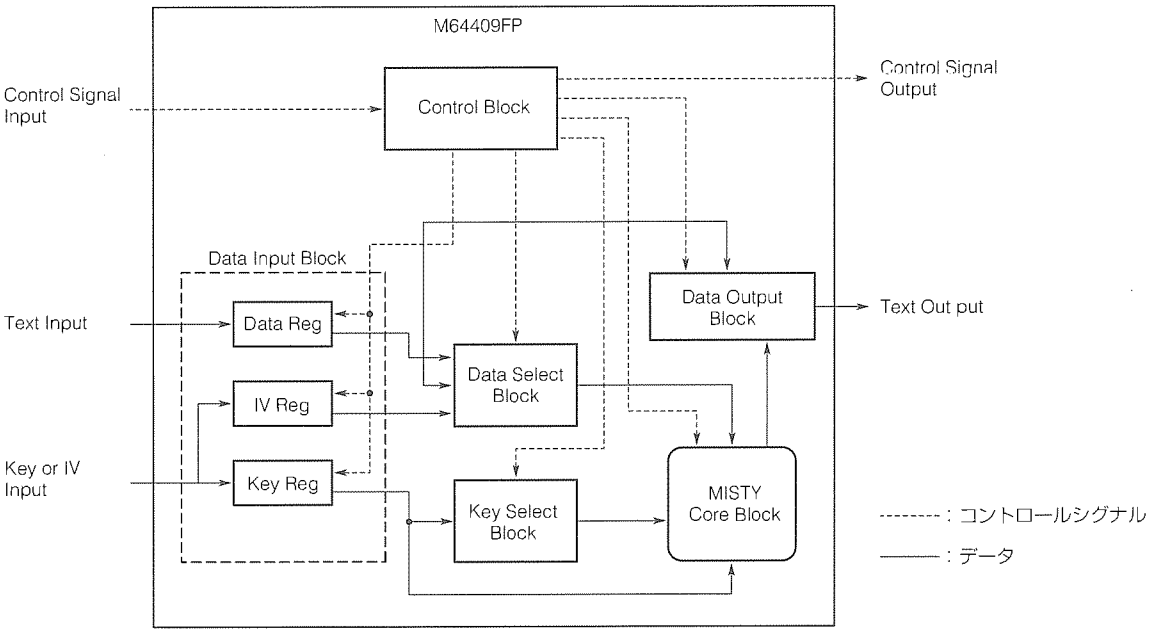


図1． M64409FPのブロック図

トの拡大鍵として，鍵セレクタブロックとMISTYコアブロックへの受渡しを行う。

(5) データセレクタブロック

各種サポートする暗号化モードにより，MISTYコアブロックやテキスト出力ブロックで処理するデータの選択を行う。

(6) 鍵セレクタブロック

鍵レジスタブロックから入力された拡大鍵を鍵スケジュールのとおりにMISTYコアブロックで利用可能なように選択を行う。

(7) MISTYコアブロック

MISTYアルゴリズムの演算を実現する部分である。処理性能を考慮し，データ入出力がそれぞれ2クロック要するので，8段構成であるMISTYアルゴリズムを1クロックで4段処理する。したがって，1ブロックの暗号化では，MISTYコアブロックを2回処理することとなる。

(8) 制御ブロック

各種入力制御信号を一括制御し，他の7ブロックの制御信号を発生する。

2.2 チップの仕様

表1にM64409FPのチップの仕様を示す。

M64409FPは0.8μmCMOS ASIC，208ピンQFP(Quad Flat Package)で作成し，データの入出力は32ビット幅で，データ入力端子，データ出力端子，鍵・IVデータ入力端子にそれぞれ32ピン，データの制御端子に13ピンを配置している。

電源電圧4.75～5.25V，動作周波数8MHzで動作し，256Mbpsの処理速度を実現する。消費電力は1.5Wである。

3. MISTY評価システム

M64409FPを用いてMISTY評価システムを開発した。**図2**に評価基板の概略ブロック図，**図3**に外観写真を示す。

今までの評価システムは，GPIBというインタフェースを用いていたため，余り汎用性がないものになっていた。そこで，今回開発したシステムでは，より汎用性のあるものにするため，評価基板にはパソコン(標準的なDOS／V)内の拡張PCI(Peripheral Component Interconnect)スロットルに接続可能なPCIアドインボードを採用し，評価プログラムはWindows95(注1)上で動作可能なものを採用した。

(注1)“Windows95”は，米国Microsoft corp.の商標である。

表1. M64409FPの仕様

項目		内容		
処理速度		256Mbps		
動作周波数		8 MHz		
データ入出力用端子	データパラレル入出力端子	入力	32ピン	
		出力	32ピン	
	鍵・IV入力端子	入力	32ピン	
プロセステクノロジー		0.8μm		
電気的特性	電源電圧	4.75～5.25V		
	消費電力	1.5W		
動作周囲温度		−20～75℃		
パッケージ形態		HQFP(パワーQFP)208ピン		

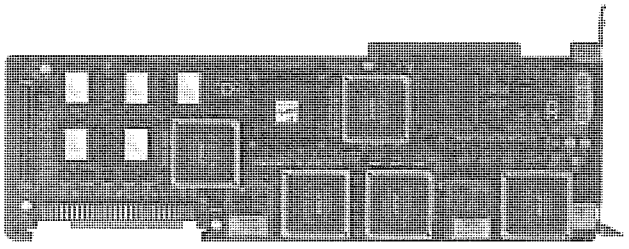


図3. 評価基板の外観写真

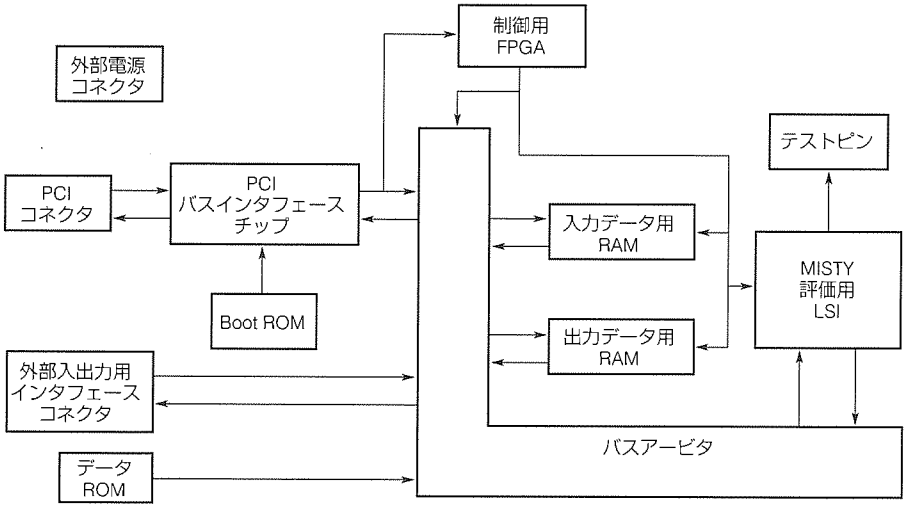


図2. 評価基板の概略ブロック図

以下に，この評価システムにおける基板及びプログラムの主な特長を示す。

3.1 評価基板

(1) パワーオンリセットを装備し，評価LSIは取り外し可能にするためICソケットを実装した。

(2) ロジアナ等でモニタ可能にするため，評価LSIの各ピンの特性をテストピンに出力した。

(3) 発振器をICソケット実装とし，評価LSI動作クロックを自由に設定できる。

(4) ボード単体でも評価可能である(外部入力が可能で，かつ外部電源装置から電源供給可能である。)。

(5) 外部入力には，評価基板上のROM(制御信号パターンを含めたすべてのデータをROMに書き込むことによって評価可能である。)，又は外部入力専用コネクタを用いることができる(基板上のDIP-Switchで選択可能である。)。

(6) 5V単一電源のPCI標準長カード(LONG CARD)である。

(7) PCIバスマスタ方式を採用することにより，DMA(Direct Memory Access)機能を実現した。

3.2 評価プログラム

(1) GUIによって操作が容易である。

(2) プログラム実行中にWindow上でECB，CBC，OFB，CFBそれぞれの暗号化／復号の選択が可能である。

(3) 処理データ入力は，評価プログラム実行中にWindow上でキーボード入力(Hexコード又は文章の両方に対応している。)又はファイル読み込み(Binary File)の選択が可能である。

(4) 鍵・IV入力は，プログラム実行中にWindow上でデフォルトパターン又はキーボード入力の選択が可能である。

(5) ソフトウェア(PowerMISTY)とハードウェア(この評価基板)の演算結果の比較及び処理速度の表示が可能である。

(6) 評価基板がなくても評価プログラムは実行可能であり，ソフトウェアでの演算結果を表示する(ハードウェア未検出を表示する。)。

この評価システムを用いて評価した結果，M64409FPが256Mbpsという高速演算性を実現したことを確認した。また，この評価装置は，CPUがMMX(注2) Pentium(注2) 233MHz，主記憶が64Mバイトのパソコンでソフトウェアを用いて演算したときの処理速度と比較すると，約2.5倍演算性能が優れていることを計測した(CPUの動作速度が下がれば2.5倍以上の差が出てくると思われる。)。

(注2) "MMX""Pentium"は，米国Intel corp.の商標である。

4. むすび

秘密鍵暗号アルゴリズム"MISTY"を採用し高速な演算を実現するLSI(M64409FP)，及びこれを用いた評価システムについて述べた。

今後の展開として，高速・高機能版から小型版など，用途に合わせた開発を行っていく。用途としては，ネットワーク機器，セットトップボックス，携帯端末等に加えて特にICカードへの暗号技術の搭載が重要になっていくと思われる。ICカードはエレクトロニックコマースに用いられるのはもちろん，パスポートや免許証などID (Identity)カードとして個人の情報を記録しておく用途として用いられることが予想され，その情報を外部に漏らさないように高いセキュリティ技術が求められる。三菱電機ではICカード搭載用に暗号アルゴリズムMISTYを実現する数kゲート規模のマクロセルの開発を行っており，それの評価，デモボードを作成する予定である。

参考文献

(1) 松井 充：ブロック暗号アルゴリズムMISTY，信学技報，ISEC96-11 (1996-7)

(2) Biham, E., Shamir, A.：Differential Criptanalysis of Data Encryption Standard, Springer-Verlag (1993)

(3) Matsui, M.：Linear Cryptanalysis Method for DES Cipher, Eurocrypt '93 (1993)

ネットワークセキュリティ“MELWALL”

時庭康久*　泉　祐市**
後沢　忍*　渡辺　晃*
稲田　徹*

要　旨

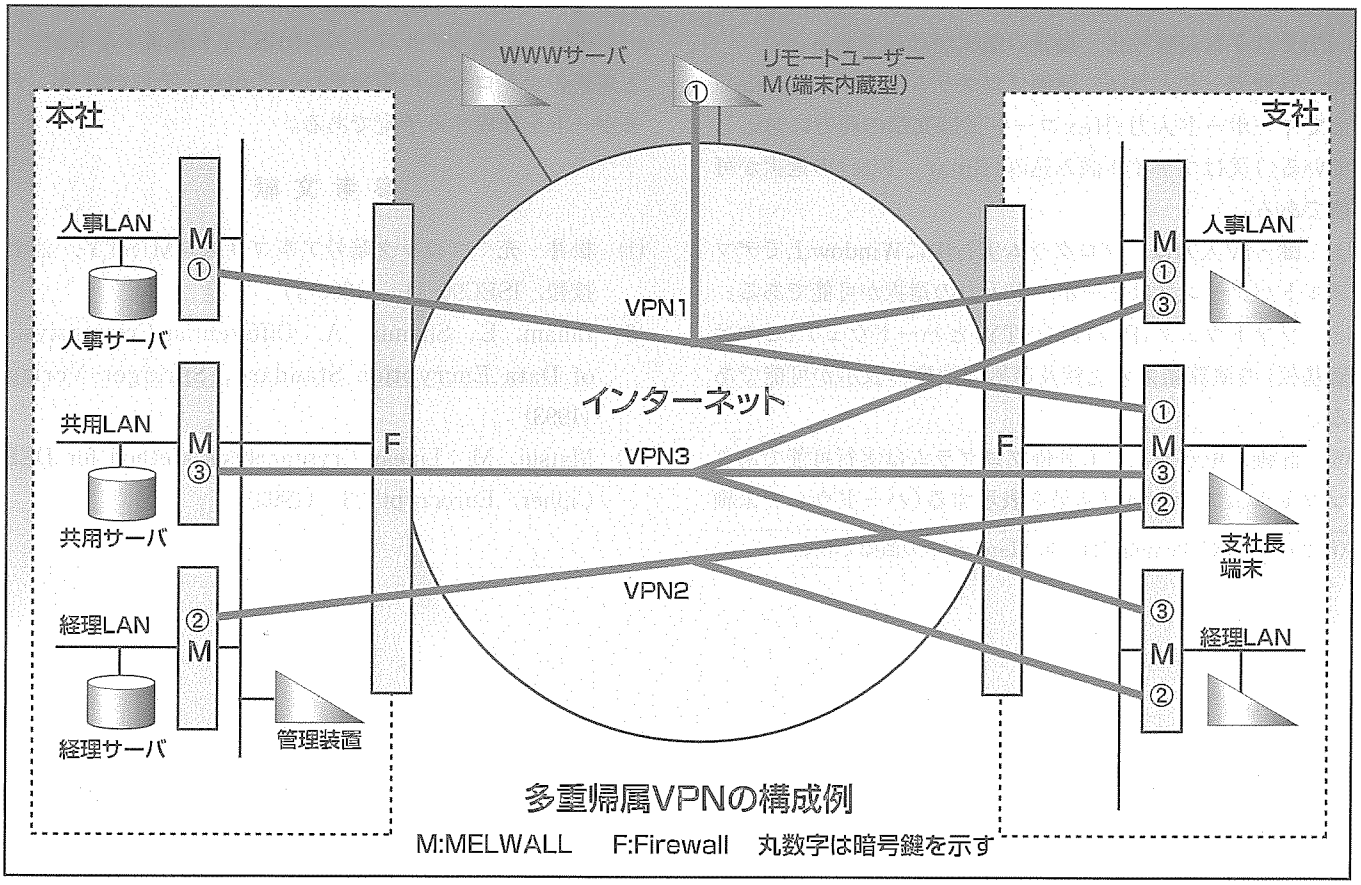
インターネットをビジネス目的で使用する場合には，通信の安全性についての保証はなにもないので，データの盗聴／改ざん，不正アクセスなどのネットワークセキュリティへの配慮が必す(須)となっている。インターネット上で通信データに暗号を用いることにより，専用線等による私設網と同等の安全性を持つVPN(Virtual Private Network：仮想私設網)と呼ばれるシステムが普及し始めている。

三菱電機では，暗号によってVPNを構築するネットワークセキュリティシリーズ“MELWALL”を製品化している。この製品は，既存ネットワークシステムへのアドオンによってVPNを構築するものである。

本稿では，VPNの構築という観点に的を絞り，暗号によるVPNの運用形態の分析とビジネスへの最適な適用の模索によって“VPNの属性と暗号かぎ(鍵)をリンクさせる”というコンセプトを述べる。

管理手法として暗号鍵の事前共有方式を採用するとともに，一局集中型のリモート管理方式を採用し，VPN構築の最適化と運用負荷の軽減を実現した。また，リモートアクセスにもこのコンセプト及び管理手法の適用を図り，リモートユーザーが任意のタイミングで自己の属するVPNの最新の暗号鍵を取得する機構を設けた。

これらの機能の実現により，VPNの適用範囲が広がるとともに，VPNの多重化を含む柔軟なシステム構築が可能となった。



VPNの構成例

ネットワークセキュリティシリーズ“MELWALL”によって，本社と支社及びリモートユーザーが重なった三つのVPN(多重帰属VPN)を構成している。VPN外からの不正侵入や盗聴はできない。VPN内からはインターネット上のWWW等にアクセスすることができる。管理装置によって暗号鍵の配送等のリモート管理が可能である。

*情報技術総合研究所　**情報システム製作所

1. まえがき

インターネットの出現によって全世界のコンピュータネットワークは確実に成長を続けている。インターネットは必要不可欠な要素になりつつあるが，その実体は多様な組織にわたるオープンなネットワークであり，通信の安全性についての保証はなく，ビジネス目的で使用する場合には，データの盗聴／改ざん，不正アクセスの防止などのネットワークセキュリティが必須となっている。

インターネット上の通信データを暗号化することによって専用線等による私設網と同等の安全性を持つVPNと呼ばれるシステムが普及し始めている。

今回，ネットワークセキュリティシリーズ“MELWALL”を既存ネットワークシステムにアドオンするというアプローチにより，VPNを構築する技術を実現した。MELWALLは，図1に示すようなネットワーク上を流れるデータを暗号化する専用ハードウェア(又はソフトウェア)である。

本稿では，暗号によるVPNの運用形態を分析するとともに，今回MELWALLを用いて実現したシステムの特長について述べる。さらに，このシステムの管理方式とリモートユーザーに適用する場合の方式についても言及する。

2. 暗号によるVPN

2.1 VPNの概念

初期のVPNの発想は，従来企業ネットワークの幹線として利用していた専用線を安価なインターネットに置き換えることによるコストの削減である。VPNの概念としては，一つの企業を一つのVPNとみなし，社外ネットワークにおけるセキュリティの確保を目的とするものである。

一方，LANで構成される社内ネットワークに着目した場合，一般的にはLAN上をあらゆる性質の情報が混在して流れており，この中には社内においても秘匿すべき性質のもの(人事情報等)が含まれている。こうした背景から，情報の性質を考慮してVPNを構築したいというニーズが生まれた。VPNの概念としては，ある情報を共有するグループを一つのVPNとみなし，グループ外部のネットワークにおけるセキュリティの確保を目的とするものである。例えば，複数事業所に存在する人事部門を一つのVPNとして定義し，他部門から情報を隔離するといった運用が可能になる。この実現には，図1の暗号装置を各人事部門の境界に設置し，外部を流れるデータを暗号化すればよい。

そして暗号化の鍵については，VPN内部での複数事業所間のメッシュ状の暗号通信を想定し，VPN内の暗号装置で同一の暗号鍵を共有する方式を採用した。

これは，VPNが扱う情報の性質に暗号鍵を対応付けるという概念であり，鍵を持つことがVPNへの帰属を意味するため，鍵の持つ身近な概念とマッチしており，ユーザーに受け入れられやすい。

2.2 VPNの構成と多重化

上記の概念に基づき，VPN定義の最適化とそれに伴う管理の簡易化を図った。

図2に示す実運用形態モデルへの適用を考えてみる。図は本社と支社のシステムに着目したものであり，本社側には社員全員がアクセスする共用サーバが設置され，本社と支社は人事LANと経理LANを持っている。また，プロキシサーバが設置され，社外のWWWサーバ等にアクセスする場合にはプロキシサーバを経由する(支社側のみ図示)。

各社員には共用サーバと自部門のサーバ及びプロキシサーバへのアクセス権限が与えられている。支社長には人事と経理へのアクセス特権も与えられている。つまり各社員は複数のVPNに帰属していることになり，これを多重帰属と呼ぶ。多重帰属の関係を表1に示す。

多重帰属を実現するためには，暗号装置内に帰属するVPNの暗号鍵が設定され，あて(宛)先アドレスとの対応テーブルを持つ必要があり，通信相手端末のアドレスとアプリケーションの種別の比較によって暗号化(復号)／透過中継／廃棄を実行する。中継処理では，設定された条件に

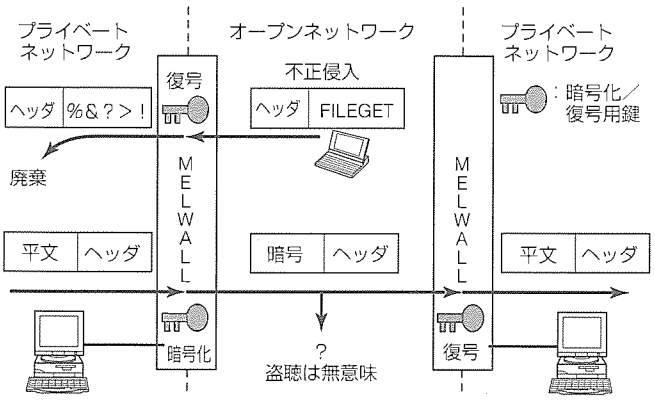


図1．暗号装置の動作原理

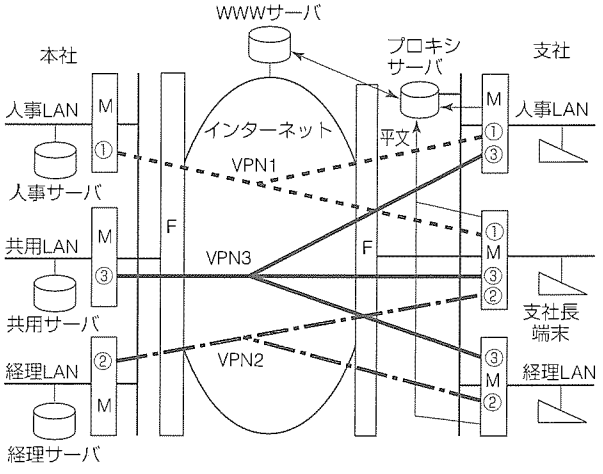


図2．VPNの実運用形態モデル

表1．支社の多重帰属関係

	VPN1	VPN2	VPN3	VPN外
人事課員	○	—	○	○
経理課員	—	○	○	○
支社長	○	○	○	○

表2．通信パス概念による設定内容

通信パス	宛先	暗号鍵
基本パス	—	鍵①
特例パス1	共用サーバ	鍵③
特例パス2	プロキシサーバ	平文：鍵なし

よって処理を決定する特例パスの概念と，デフォルトの処理を行う基本パスの概念がある。

特例パスとは，宛先アドレスに合致した通信データの暗号化(復号)／透過中継／廃棄を実行する処理である。また基本パスとは，特例パスの宛先アドレスに合致しない通信データを宛先アドレスに依らずに実行する処理である。

支社の人事LANを収容する暗号装置の設定内容を**表2**に示す。

これにより，共用サーバとプロキシサーバ以外との通信には基本パスが適用され，**図2**の鍵①によって外向きは暗号化され，内向きは復号が行われる。

以上で述べたように，採用したVPNシステムの特長は次のとおりである。

(1) VPNの最適化

VPN構成単位は情報の性質に依存する。

(2) VPN管理の容易化

VPNと暗号鍵は1対1に対応し，暗号鍵を保持(グループ共有)していれば同一のVPNに帰属する。

(3) VPNの多重化

基本パス，特例パスという暗号装置内の処理方法の概念によって多重帰属を実現する。

3. 管理方式

3.1 管理コンセプト

多数の暗号装置や多重帰属しているVPNの構成管理のためには，管理に膨大な作業量が発生する。この作業負荷を軽減するため，このシステムでは，専用管理装置による一局集中型のリモート管理方式を採用した。さらに，暗号鍵のグループ共有というシステムの性質上，暗号鍵の事前共有方式を採用した。

現在，鍵共有方式としては，通信のセッション確立時に暗号鍵をネゴシエーションするというダイナミック共有方式が主流であるが，以下の理由により，このシステムでは適用しなかった。

(1) 複数の装置が同一の鍵をグループ共有する場合，ダイナミック共有方式はなじまない。

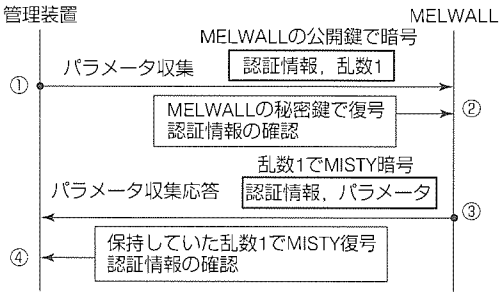


図3．管理通信例

(2) 鍵のネゴシエーションにかかわる遅延が大きい。

後者については，インターネットでは問題にならないが，将来的に100M-LANやATM(Asynchronous Transfer Mode)上のバースト的なマルチメディアトラヒックに適用する場合も想定して判断した。

3.2 管理装置の機能

管理装置の機能を以下に示す。

(1) 暗号鍵の管理

暗号鍵の生成を行い，管理対象であるすべての暗号装置に対して，オンラインによる一括鍵配送を行う。

(2) VPN構成パラメータの管理

端末とVPNとの帰属関係を，基本パスや特例パスによってオンラインで設定する。暗号装置からオンラインでパラメータを収集して編集することも可能である。

(3) 各種補助機能

GUIによる管理下の暗号装置の登録や削除，暗号鍵やパラメータ情報のファイル管理，オペレータ操作や通信の履歴(ログ)の保存なども可能である。

鍵配送やパラメータ送付などの管理通信のため，独自のプロトコルを定義する。管理通信はオープンネットワークを経由する可能性が高く，管理通信データの盗聴や改ざん，お互いの成り済ましを防止するため，認証及び暗号化が必要である。管理通信フレームに対しては公開鍵暗号と共通鍵暗号を併用する。

管理通信プロトコルは，**図3**(例，パラメータ収集)に示すように単純である。

暗号装置導入時に，管理装置で各暗号装置ごとの公開鍵と秘密鍵のペアを生成し，秘密鍵の方を暗号装置にあらかじめ設定しておき，公開鍵は管理装置側で保持しておく。

このシステムでは，各暗号装置が公開鍵を公開する相手は管理装置のみであることから，管理装置側で一括生成・管理を行う。これにより，公開鍵をCA(Certificate Authority)機関に登録し運用する作業が不要になるとともに，運用手順の簡易化が可能となる。

4. リモートアクセスへの適用

携帯端末やリモートアクセスソフトウェアの普及によっ

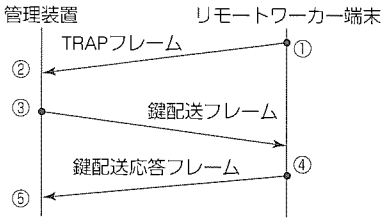


図4．鍵配送シーケンス

て，社外から社内ネットワークにアクセスするリモートユーザーが急増している。この章では，リモートアクセスを実現する際の方式について述べる。

4.1 運用形態の相違による課題

MELWALLでは，既存のネットワークに暗号装置をアドオンすることによってデータを暗号化し，一般のユーザーに暗号装置の存在や暗号通信を意識させない構造とした。つまり，暗号装置の管理やシステムの運営は，ごく一部の管理者が行うことを前提にしている。

一方，リモートユーザーのワーキング形態は公衆網に接続されたパソコンによるものがほとんどであり，この形態に外付けのハードウェアである暗号装置をアドオンするのは，利便性上，現実的ではない。したがって，暗号装置の機能を暗号ドライバソフトウェアという形で端末に内蔵する。サーバ側には暗号装置を接続し，リモート側とサーバ側で同じ暗号鍵をあらかじめ共有し運用する。

リモートユーザー端末(端末内蔵型)を管理体系に収容するために，運用上の相違から以下のような新たな課題が生まれる。

すなわち，セキュリティ維持の観点から鍵更新が必要であり，管理者は管理装置を操作し，暗号装置に対する鍵配送を実施している。しかし，リモート側は，通常，電源が入っておらず，またIP(Internet Protocol)アドレスも確定していないため，管理装置主導による鍵配送の対象とすることはできない。したがって，リモート側には，電源投入時等のタイミングで自発的に鍵を取得する機構が必要である。

4.2 解 決 策

リモートユーザー側主導による鍵の取得手順は次のとおりである。

(1) リモートユーザーは，端末起動等のタイミングで，管理装置に対して鍵配送シーケンスを用いて鍵を入手する。

(2) 社内サーバへのアクセス時，上記(1)で入手した鍵によって通信データは暗号化され，暗号通信が成立する。

図4にリモートユーザー端末主導による鍵配送シーケンスを示す。

① リモートユーザー端末はTRAPフレームを管理装置に送信する。TRAPには端末を識別する情報等が格納されており，管理装置の公開鍵で暗号化されている。

② 管理装置は，TRAPを自己の秘密鍵で復号して端末識別情報等を得る。この情報を基に，端末に許可された鍵のみを格納した鍵配送フレームを作成する。このフレームは端末側の公開鍵で暗号化されている。

③ 鍵配送フレームを送信する。このときの宛先IPアドレスは，TRAPフレーム内の送信元アドレスを用いる。

④ リモートユーザー端末は，自己の秘密鍵で復号して暗号鍵を得るとともに，鍵配送応答フレームを送信する。

⑤ 管理装置は，配送結果を保存し，履歴を残す。

5. むすび

MELWALLでは，VPNの属性と暗号鍵をリンクさせるという方式により，VPN構築の最適化と運用負荷の軽減を実現し，暗号によるVPNのビジネス利用の運用形態に最適な方式を採用した。これにより，VPNの多重化を含む自在なシステム構築が可能となった。

さらに，このシステムの管理方式とリモートアクセスに適用する場合もシステムに最適な方式とした。

今後は，大規模化に対応した管理装置の階層化を実現し，Firewallとの共存のためのトンネル装置や，セキュリティ産業の国際的な流れや次世代のインターネットワーキング技術への対応に備えて，IPSEC等の技術の取り込みについて検討していく予定である。

参考文献

(1) 渡邊 晃，厚井裕司，井手口哲夫，横山幸雄，妹尾尚一郎：暗号技術を用いたセキュア通信グループの構築方式とその実現，情報処理学会論文誌，**38**，No.4 (1997)

(2) 時庭康久，後沢 忍，稲田 徹，田口卓哉，永島規充：暗号による仮想私設網の構築方式，情報処理学会第55回(平成9年後期)全国大会講演論文集(3)，651～652 (1997)

(3) 田口卓哉，後沢 忍，時庭康久，稲田 徹，永島規充：暗号システムの管理方式，情報処理学会第55回(平成9年後期)全国大会講演論文集(3)，655～656 (1997)

(4) 後沢 忍，渡邊 晃，田口卓哉，永島規充：暗号によって構成されるVPNとその管理方式，電子情報通信学会技術報告[情報ネットワーク]，IN97-113，信学技報，**97**，No.326，9～16 (1997)

(5) 横山幸雄，青木 尚，後沢 忍，大越丈弘：三菱ネットワークセキュリティ暗号装置"MELWALL3000シリーズ"，三菱電機技報，**70**，No.10，1044～1048 (1996)

(6) 後沢 忍，馬場義昌，松井 充，板垣寛二：ネットワークセキュリティ技術，三菱電機技報，**71**，No.2，156～159 (1997)

公開鍵インフラストラクチャ構築技術

佐伯正夫*　坂上　勉**
吉武　淳*
辻　宏郷*

要　旨

公開かぎ(鍵)インフラストラクチャ(Public Key Infrastructure：PKI)は，盗聴，改ざん，成り済まし等の脅威を防ぐための，“公開鍵暗号技術に基づくセキュリティサービスを提供する，鍵及び認証書の管理を行う構成要素・機能・手続きの集合”であり，多様な情報システムにわたって，認証，アクセス制御，改ざん防止，秘匿及び否認防止を効率的に実現するための共通基盤技術である。業界標準に基づき，三菱電機情報セキュリティアーキテクチャに沿って三菱電機PKIを構築した。

その構築技術を，主要構成要素と主な特長を中心にして紹介する。

(1)　各種業界標準に準拠し多様な応用システムに適用可能

WWW(World Wide Web)で使用するSSL(Secure Socket Layer)対応認証書，S／MIME(Secure／Multipurpose Internet Mail Extensions)メーラ対応認証書など，用途に応じた認証書を選択・定義できる認証サーバシステムと，移行性・相互運用性・拡張性を付与する応用システム構築用ライブラリを提供する。

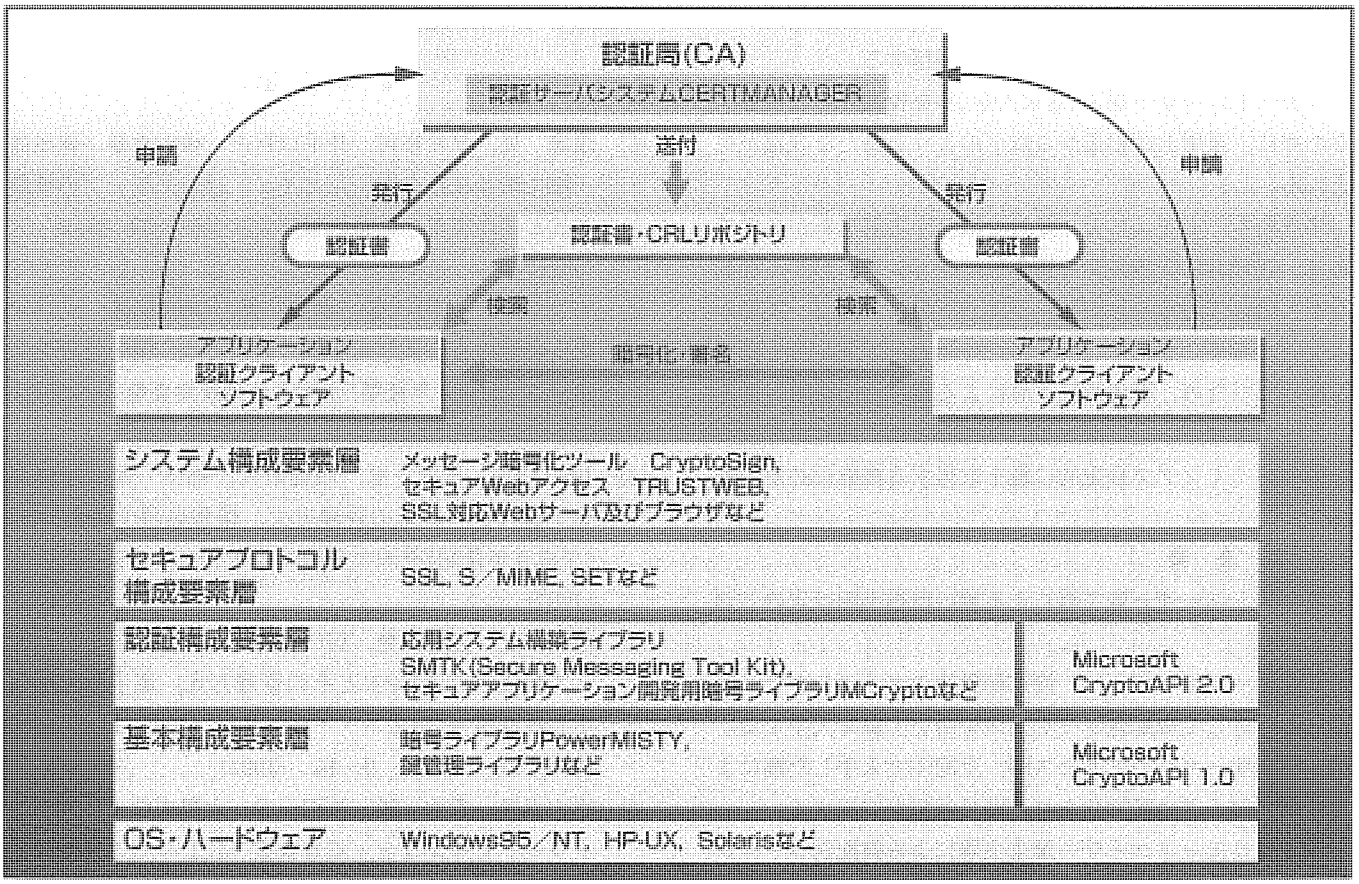
(2)　企業向け機能を豊富に用意

社員の手間をかけずに管理部門が一括代行して鍵と認証書を発行・管理するための一括代行申請機能，社員の鍵紛失，パスワード忘れ，退職等に対してリカバリーを可能とするキーアーカイブ・認証書再発行機能等を提供する。

(3)　世界最高水準の強度を誇るMISTY鍵による暗号化

(4)　応用システム構築を簡便化するメッセージ暗号化ツール，Webサーバアクセス等のシステム構成要素群を提供

最後に，PKIの新しい構成要素である“キーリカバリーシステム”を紹介する。



PKI構成概念図

PKIは，多様な応用システムにわたって，“公開鍵暗号技術に基づくセキュリティサービスを提供する，鍵及び認証書の管理を行う構成要素・機能・手続きの集合”であり，認証局(Certification Authority：CA)，認証書及び認証取消リスト(Certification Revocation List：CRL)のリポジトリ，認証クライアントソフトウェア，及びそれらを構築するための各種構成要素からなる共通基盤システムである。

*情報技術総合研究所　**情報システム製作所

1. まえがき

PKIは，盗聴，改ざん，成り済ましといった脅威を防ぐための，“公開鍵暗号技術に基づくセキュリティサービスを実現する，鍵及び認証書の管理を行う構成要素・機能・手続きの集合”であり，多様な情報システムにわたって，認証，アクセス制御，改ざん防止，秘匿及び否認防止を効率的に実現するための共通基盤技術である。このたび，業界標準に基づき，“三菱電機情報セキュリティアーキテクチャ”に沿って“三菱電機PKI”を構築した。

本稿では，まずPKIの一般的要件を概観し，次に三菱電機PKIの構築技術を，主要な構成要素と主な特長を中心にして紹介する。また最後に，PKIの新しい構成要素である“キーリカバリーシステム”を紹介する。

2. PKIの一般的要件の概観

2.1 PKIの必要性

多様な応用システムにまたがって認証やアクセス制御などを実現するためには，鍵の生成と配布，認証書の発行と配布，認証書の検証，鍵及び認証書の失効と更新などに関して，応用システム間で相互運用性が必要となる。

その相互運用性を実現するため，また，応用システム構築の負担を軽減するために，“鍵及び認証書を管理する共通基盤”が必要である。その共通基盤として，PKIの必要性が高まっている。したがって，PKI処理系を構築するには，他の処理系との相互運用性や，（理想的には利用者が意識しなくて済むほどの）応用システムから見た簡便性が特に重要となる。

2.2 公開鍵による認証技術

公開鍵暗号は，だれもがアクセスできる所に公開する鍵（公開鍵：Public Key）と利用者各人が秘密に保管して使用する鍵（秘密鍵：Private Key）との一対の鍵として生成し使用する。送信者Aの秘密鍵で暗号化したメッセージは公開鍵暗号の数学的特性によって送信者Aの公開鍵でしか復号できないので，受信者Bは，送信者Aの公開鍵を入手し，それで受信メッセージを復号できたら，“送信者はAに違いない”と確信できる。なお，実際には，メッセージそのものを公開鍵で暗号化すると時間がかかるなどの理由から，送信メッセージをメッセージ縮約アルゴリズムによってメッセージダイジェストというハッシュ値に変換し，それを送信者Aの秘密鍵で暗号化してメッセージに付けて送信する。この暗号化したメッセージダイジェストを“署名”と言う。受信者Bは，送信者Aの公開鍵によって署名を復号して得たメッセージダイジェストと，受信メッセージから直接に計算して得たメッセージダイジェストとを比較して，両者が一致したら“送信者はAである”と確信することができる。同時に，“メッセージが改ざんされていない”ことも確認できる。これを“署名の検証”と言う。

以上が，公開鍵暗号を用いた相手認証（成り済まし防止）及びメッセージ認証（改ざんチェック）の原理である。

ただし，このとき，入手した公開鍵が本当にAのものであることを確認する必要がある。そこで，信用できるCAが，公開鍵とその所有者の結び付きを証明する“認証書”を発行するという仕組みを導入する。認証書には，公開鍵，公開鍵の所有者を示す識別名，有効期限などの情報を載せ，CAの署名を付加する（言わば，鍵と認証書は，電子的な実印と印鑑証明書のようなものである。）。受信者Bは，署名の検証時に，送信者Aの認証書を入手し，それに載っているAの公開鍵でAの署名を検証するとともに，Aの認証書の有効性を検証する。認証書の検証では，認証書の署名（CAによる署名）が本物か，認証書の有効期限が切れていないか，認証書が失効していないかなどの検証を行う。

2.3 PKI処理系の主要構成要素と主な要件

公開鍵・秘密鍵及び認証書の，生成，更新，配布，バックアップ／リカバリー，失効，有効期限切れといった運用ライフサイクルを実現するために，PKI処理系は，主に次の構成要素と機能要件を満たす必要がある。

2.3.1 CA

(1) RA（Registration Authority）機能

認証書の申請に対して，申請内容などから認証書発行対象を識別（本人確認）して，認証書を発行してよいか否かを判断する。CAと分離した構成要素とする場合もある。

(2) 認証書の発行機能

(3) 認証書の失効管理機能

鍵漏えい（洩），利用者の退職など，有効期限内であっても認証書をもはや信用できない種々の事象が生じたら，CAが認証書を失効させなければならない。CAは，失効した認証書のシリアル番号をCRLに記載して速やかに配布するなどの方法によって，利用者が認証書を検証する時点での失効チェックを可能とする必要がある。

(4) 鍵のバックアップ／リカバリー機能

利用者が保管している鍵の格納装置が破損したり，鍵を使用するために必要なパスワードを利用者が忘れたりする場合に対しても暗号化したデータを復号可能とするために，鍵対をバックアップ／リカバリーする機能が必要である。

2.3.2 リポジトリ

通信相手の認証書とそのCAの認証書，そのCAが生成したCRLなどを，利用者がネットワークを通じて入手可能とする必要がある。リポジトリは，そのための認証書やCRLの貯蔵庫であり，LDAP（Lightweight Directory Access Protocol）準拠のディレクトリシステムやデータベース管理システムを採用する動向にある。

2.3.3 認証クライアントソフトウェア

認証クライアント（認証書発行対象）側のソフトウェアに

も，CA及びリポジトリと連携した種々の機能が必要である。その主な機能要件を次に示す。

(1) 鍵の生成と認証書の申請・取得機能
(2) 鍵と認証書を利用する機能
　暗号化，署名，署名の検証(及び認証書の検証)など
(3) 鍵の更新と世代管理機能
(4) 鍵のバックアップ／リカバリーシステムを利用する機能
(5) リポジトリから認証書及びCRLを検索する機能

3. 三菱電機PKI構築技術

2.3節で述べたPKI処理系の主要構成要素と主な要件を実現しながら，三菱電機情報セキュリティアーキテクチャに沿って三菱電機PKIを構築した。その構築技術を，主要な構成要素とその主な特長とを中心にして紹介する。

3.1 認証サーバシステム

CAの要件を実現しながら，特に企業向けに開発した認証書発行・管理システムである。この認証サーバシステムはMistyGuard“CERTMANAGER”として製品化されている。

(1) 各種業界標準に準拠し，多様な応用システムに適用可能

ITU-T勧告X.509及びPKCS(Public Key Cryptography Standards)に準拠し，セキュアWeb通信の業界標準SSLやセキュアメールの業界標準S／MIMEに準拠したブラウザ及びメーラ対応認証書など，用途に応じた認証書を選択発行可能であるとともに，認証書及び申請書の内容やCA階層構成の外部定義が可能である。また，LDAP準拠のディレクトリシステムに認証書及びCRLを送信することも可能である。

(2) 企業向け機能を豊富に提供

社員の手間をかけずに管理部門が一括代行して鍵と認証書を発行・管理するための一括代行申請機能，社員の鍵紛失，パスワード忘れ，退職などに対してリカバリーを可能とするキーアーカイブ機能及び認証書再発行機能を提供する。また，秘密鍵格納媒体として，固定ディスク，フレキシブルディスク又はICカードを選択可能である。

(3) 運用支援機能

リモート管理端末による運用，プログラム及びログの署名検証機能による認証サーバシステム自身の改ざん防止，トランザクションログとデータベースによる稼働記録及び運用監視などを可能としている。

(4) 相互認証

他のCAドメインから発行された認証書を持っているビジネスパートナーと認証し合うには，あらかじめ認証ポリシーが合致するCA間で相互認証書対を作成しておき，利用者間で相手の認証書を検証するときに，相互認証書対によって両CA間で相互認証が許可されていることを検証する。その相互認証書対を生成可能である。

3.2 認証書・CRLのリポジトリ

LDAP準拠のディレクトリシステムを採用可能である。

3.3 認証クライアントソフトウェア

3.3.1 アプリケーション構築用ライブラリ

移行性・相互運用性・拡張性を付与するセキュアアプリケーション開発用の汎用ライブラリ群“MCrypto”及びセキュアなメッセージ通信を行うアプリケーションを容易に実現するための“SMTK(Secure Messaging Tool Kit)”を開発した。これらを用いて，次のことが可能となる。

(1) 世界最高水準の強度を誇るMISTYによる暗号化が可能
(2) CSP(Cryptographic Service Provider)を入れ替えることによってMicrosoft CryptoAPIなど他社の暗号ライブラリに簡単に移行可能
(3) 鍵や認証書の格納媒体に依存しない透過性を実現可能
(4) 検証ロジックを拡張でき，アプリケーションや認証ポリシーに応じて，認証書の検証仕様を変更可能

3.3.2 システム構成要素群

市販のWWWサーバ及びブラウザを使用可能とする一方で，それらでは実現できない応用システムを簡便に構築するために，システム構成要素群を提供している。

(1) メッセージ暗号化ツール

ファイルに対する署名・親展を実現するツールであり，メールソフトウェアと連携したセキュアメール機能を実現している。認証書を用いた相手認証と，MISTYを用いた堅固な親展が可能である。また，CERTMANAGERの一括代行申請機能，キーアーカイブと認証書再発行機能などを利用可能である。さらに，認証書やアドレス帳の一括管理機能や，ウィザード，アドレス帳に基づくグループ向け暗号化機能によって，簡単操作を実現している。このツールは，MistyGuard“CryptoSign”として製品化されている。

(2) セキュアWebアクセス

WWWサーバ及びそのコンテンツを変更することなく既存WWWサーバにアドオン可能な，Webアクセス制御及び暗号化通信を提供するシステムである。

認証書に基づいた利用者の認証とアクセス制御を実現するとともに，MISTYを用いたコンテンツの堅固な暗号化通信を実現している。また，CERTMANAGERの一括代行申請機能，キーアーカイブと認証書再発行機能などの利用が可能である。さらに，コンテンツ(ページ)単位，ディレクトリ単位，グループ単位などでのアクセス制御を可能とするとともに，GUIによるアクセス制御設定によって管理負荷を軽減している。このツールは，MistyGuard“TRUSTWEB”として製品化されている。このシステムイメージを図1に示す。

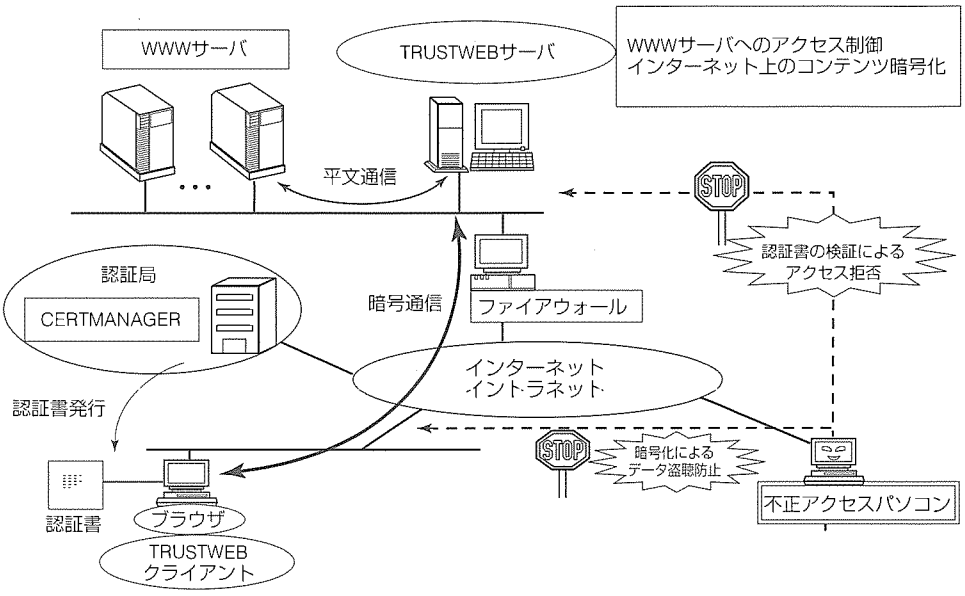


図1．MistyGuard“TRUSTWEB”のシステムイメージ

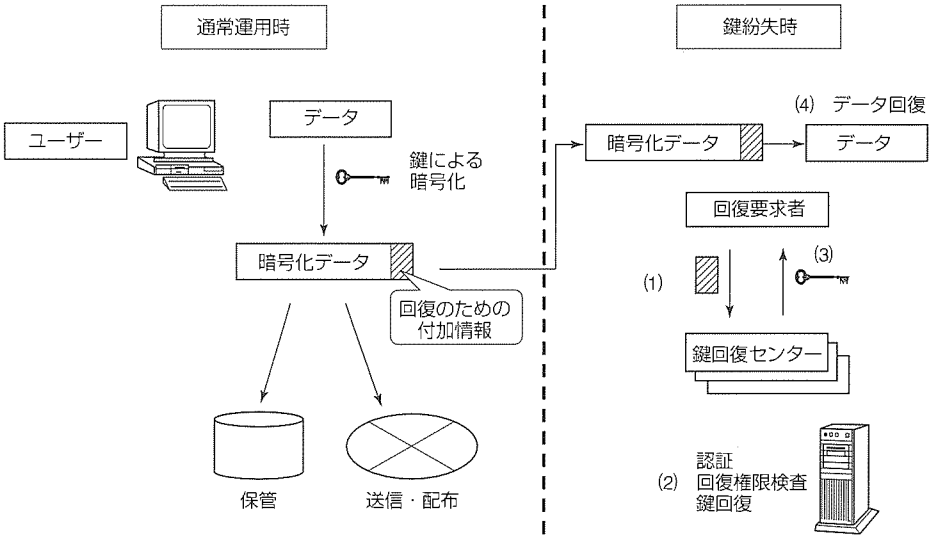


図2．DataAidのシステムイメージ

4. キーリカバリーシステム

鍵回復技術(キーリカバリー)は，暗号を利用した通信やデータ蓄積を行うシステムにおいて，鍵紛失などの緊急時に，認められた第三者が鍵及びデータを復元する技術である。これによって，情報が失われることを未然に防ぐことができる。当社が研究開発中の“DataAid”(仮称)は，鍵回復を実現したシステムであり，電子金庫，電子倉庫，暗号化コンテンツ配布などに適用可能である。

DataAidは次の特長を持っている。

(1) 回復要求者の認証や，複数の鍵回復センター間での危険分散によって，この機能の付加による安全性の低下はない。

(2) 組織の階層構成やデータ作成時刻による権限など，様々な回復権限を設定可能である。

(3) 鍵の回復要求は電子メールによって行うため，モバイル端末などでもデータ回復を行うことができる。

DataAidのシステムイメージを図2に示す。

5. むすび

最新の業界標準をキャッチアップしながら応用システムでの使用経験をフィードバックすることによって，今後とも企業向け機能を充実するとともに，より簡便に使えて相互運用性の高いPKIを追求していく所存である。

ディジタルコンテンツ流通技術

中川路哲男*　石塚裕一**
宮崎一哉**
中嶋春光**

要　旨

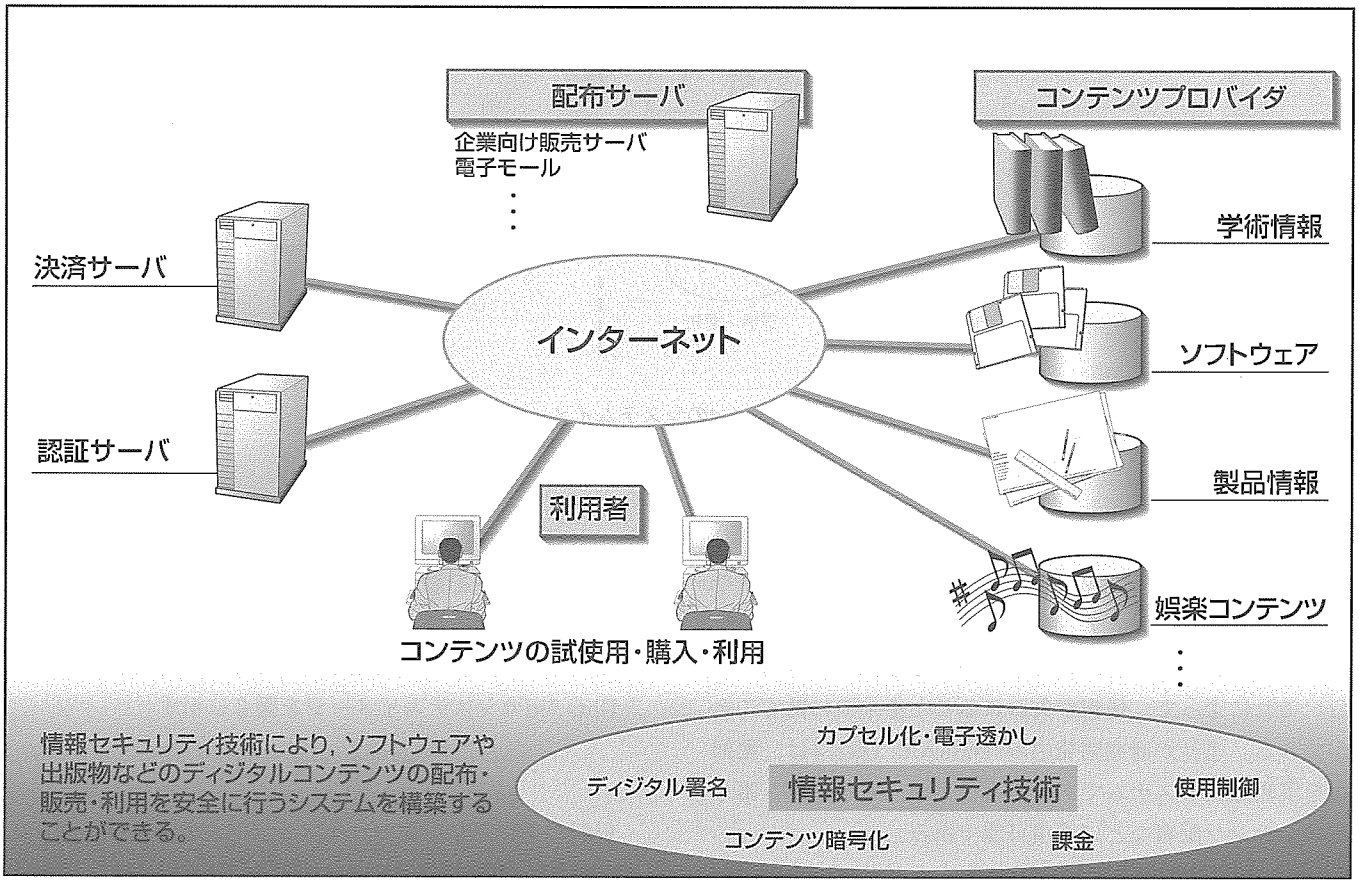
ソフトウェアや出版物などのディジタルコンテンツのインターネット上での流通・販売は，その流通コストの安さとカバーする範囲の広さから，エレクトロニックコマース(EC)の効果を最大限に引き出す形態として期待が高い。

一方，ディジタルコンテンツは複製や改ざんが容易であるため，不正利用の防止や適切な課金を行うことなどが困難であり，その普及を阻む課題となっていた。ここでは，ディジタルコンテンツ流通実現のための技術課題を紹介した上で，その核となる要素技術である“電子透かし”と，それをベースとしたセキュアコンテンツ配布システムである“DIGITEX”(仮称)について述べる。

電子透かしは，著作権情報をディジタルデータに判別・除去不能な形式で埋め込む技術である。周波数変換に基づく方式により，従来よりも計算量を削減し，かつ画質を劣化させることなくデータを埋め込むことができる。

DIGITEXは，上記電子透かしを含む情報セキュリティ技術により，ディジタルコンテンツの著作権管理と課金管理を実現したセキュアコンテンツ配布システムである。コンテンツの盗聴や改ざん，不正コピーなどの不正利用を防ぐ機能を持っている。

今後は，各種応用システム(ソフトウェア販売，製品情報提供，学術情報提供，娯楽コンテンツ販売など)へ適用していき，その有効性を検証していく。



セキュアコンテンツ配布システム“DIGITEX”

DIGITEXの著作権管理と課金管理により，コンテンツの盗聴や改ざん，不正コピーなどの不正利用を防いで，安全なコンテンツ流通・販売を実現することができる。

*情報技術総合研究所(工博)　**同研究所

1. まえがき

ECは，オープンなネットワークであるインターネット上で現行の商取引の一部を代行するものとして期待され注目されている。商取引は，一般に，契約の締結，決済，商品の受渡しという行為から成り立っている。契約の締結は意思表示の合致，決済は金銭(価値)の受渡しという抽象的な行為であり，比較的電子化しやすい。これに対して商品の受渡しは，商品が有形の物の場合，交通機関を利用した輸送という，ネットワーク外での行為が必ず要求される。

ところが，ソフトウェアやマルチメディア文書など，商品がディジタル化されたデータ(ディジタルコンテンツ)の場合，店舗の開設や在庫の保管，商品の受渡しなどを，すべてネットワークを介して行うことが可能となる。特にインターネットは流通コストが低く，しかもカバーする範囲が広域であるため，インターネット上のディジタルコンテンツ流通ビジネスは，ECの効果を最大限に引き出す優良な形態として期待が高い。また，近年のパソコンの高度化やオーサリングツールの高機能化，インターネットによる情報発信チャネルの一般人への開放により，ディジタルコンテンツの制作者のすそ(裾)野は，専業者から非専業者へ，計算機の熟練者から非熟練者へと拡大傾向にある。

一方，ディジタルコンテンツには“完全な複製が極めて容易である”という特性があり，その購入・利用に対して適正に課金することや，改ざん・不正コピーなどの不正利用を防止することが困難であるという課題がある。この課題が解決されない限りディジタルコンテンツ流通への良質なコンテンツの投入は望めず，逆に言うと，これらの課題を解決する情報セキュリティ技術がディジタルコンテンツ流通の普及のかぎ(鍵)を握っている。

本稿では，ディジタルコンテンツ流通のための技術について述べるとともに，当社で開発した著作権管理技術と，それを応用したセキュアコンテンツ配布システム“DIGITEX”(仮称)について紹介する。

2. ディジタルコンテンツ流通を実現する技術

ディジタルコンテンツ流通を実現する技術としては以下のものがある。

(1) コンテンツ作成技術

音声符号化・画像符号化などのデータ圧縮技術や，コンテンツ作成の手間を省力化するオーサリングツールなどにより，素材の収集・編集を行って商品としてのコンテンツを作成する技術である。

(2) 著作権管理技術

コンテンツの著作権，すわち著作者情報，利用者情報，利用条件，再配布条件，コンテンツ完全性のための情報(改ざんされていないことを保証する情報)，不正コピーを防止する情報などを管理し，不法な複製や改ざん，部分利用などを防止・抑止する技術である。

(3) コンテンツ配送技術

コンテンツを改ざんされることなく，その購入者に配送することを保証する技術である。オンラインでこれを実現するには，認証による通信相手の特定，ディジタル署名による改ざん防止，暗号化による秘匿通信の各技術が用いられる。しかし，現状ではいまだインターネットの帯域は狭く，マルチメディアデータのような大容量のコンテンツを配送する能力はない。そのために，まだCD-ROMのようなオフラインでの配送が用いられることも多い。また，将来的にはディジタル放送のような広帯域のメディアの利用が期待されている。

(4) 課金

課金は，購入者と販売者の間で合意されたコンテンツの購入条件に応じて，コンテンツ販売料金を決定する技術である。購入条件には，コンテンツの利用者，利用量，利用環境などに関する条件が含まれる。利用量とは利用回数や利用期間などのことで，これをあらかじめ購入時に決めておいて金額を決定し，その範囲内での利用を制御する事前課金と，利用した量に応じて金額を決定する事後課金とがある。

(5) 決済

決済は，課金で決定された金額を実際に利用者から徴収する技術である。SET(Secure Electronic Transaction)によるクレジット決済などの技術のほか，少額物品のための決済技術として，電子マネーやプリペイドカード方式などの少額決済技術が用いられることもある。

3. 著作権管理と電子透かし技術

複製や改ざんが容易なディジタルコンテンツの著作権管理・保護を実現するのが“カプセル化技術”である。カプセル化技術とは，コンテンツの本体であるディジタルデータと，その著作権情報である著作者情報，利用者情報，利用条件，再配布条件，コンテンツ完全性のための情報，不正コピーを防止する情報などを一体化する技術である。コンテンツを常にこのカプセルの形で流通させることにより，その著作権を保護することが可能になる。

当社は，このカプセル化技術を支える技術として，著作権情報をディジタルデータに判別・除去不能な形式で埋め込む電子透かし技術を開発した。そのコンテンツがネットワーク流通を経て利用され，又は一部分のみだけ抜き出されて利用されたとしても，電子透かしによって埋め込まれた著作権情報を基に，そのコンテンツが正しく利用されているかどうかを検証することが可能となる。

3.1 周波数変換に基づいた電子透かし

当社では，コンテンツの中でも最もニーズが高いと思わ

れる静止画像に焦点を当てた電子透かし技術を開発した[1]。電子透かしの方式には，画像の輝度値などの標本値を利用した方式，画像データを周波数成分に変換し特定の周波数成分に情報を埋め込む方式など様々な方式があり，処理の計算量や強度(透かし情報の除去のしにくさ)に一長一短がある。当社では，埋込み場所と人間の視覚特性との関係と，画像圧縮におけるひずみや雑音の少なさから，ウェーブレット変換による圧縮技術を利用した周波数変換に基づく方式を選択した。

3.2 実現方式

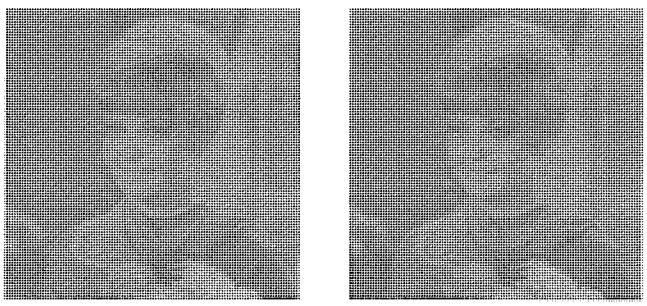
今回開発した電子透かしを実現する方式は，既存の方式であるウェーブレット変換を用いた画像の任意箇所へのテキストデータの埋込みに関する方式を発展させ，透かしの埋込み箇所に関する新しい考え方を用いている。既存の方式は，ウェーブレット変換によって得られる多重解像度表現(MRR)ベクトルの中で，高周波成分を表すMRRベクトルをクラス分けし，その大きさが0でない部分及び指定クラスに対して選択的に透かしを埋め込むという方法であった。

しかしこの方法は，ノイズのような画像情報にも情報を隠ぺい(蔽)し，ノイズを目立たせてしまう可能性がある。また，指定クラスも画像ごとに考える必要がある。そこで，この問題を解決ししかも計算量的に軽い方法として，対象画素とその近傍まで広げた画素群の変換係数によって埋込み箇所を決定することとした。処理の手順としては，原画像からウェーブレットフィルタによってMRRベクトルを求め，各画素ごとに近傍の値を含めた和があるしきい値以上であれば，透かしデータを埋め込み，透かし挿入後のベクトルとして出力するというものである。

3.3 適用例

今回開発した周波数変換による電子透かしの適用例を図1に示す。図において，原画像(左側)に対して，約4kバイトのデータを埋め込んだ結果として，埋込み画像(右側)が得られている。この方式では，たとえ原画像に初めからノイズが付着していたとしても，そこに情報が隠蔽されることがなくなり，そのノイズ箇所を広げ目立たせてしまうことを避けることができる。

このように，今回開発した電子透かし技術は，従来に比べて計算量を削減し，かつ画質を劣化させることなくデータを埋め込むことができるものである。



(a) 原画像　　(b) 透かし埋込み後の画像

図1．電子透かしによる画像例

4. セキュアコンテンツ配布システムDIGITEX

4.1 ねらいと特長

DIGITEXは，当社が開発したインターネット上でディジタルコンテンツの流通・販売を可能とするセキュアコンテンツ配布システムである[2]。前節で述べた電子透かし及びカプセル化技術を始めとする各種の情報セキュリティ技術を応用して，コンテンツの著作権管理と課金管理を実現している。DIGITEXの主な特長は以下のとおりである。

(1) コンテンツのカプセル化

ソフトウェアや出版物などのコンテンツ本体と制作者情報や購入情報はセキュアカプセルとして一体化され，流通する。セキュアカプセルは，ディジタル署名と暗号化によって正規の制作者が制作したこと，またその制作以降第三者によって改ざんされていないこと，購入した利用者のみが情報にアクセスできることを保証する。コンテンツが静止画像の場合は，前節で述べた電子透かしを用いてカプセル化を行う。セキュアカプセルは，プラットフォーム独立で動作可能であるよう，Javaによるオブジェクトとして実現した。

コンテンツタイプとしては，ソフトウェア，PDF文書(注1)，静止画，音楽，MPEG動画などを利用可能である。

コンテンツの暗号化のアルゴリズムとしては“MISTY”を用いた。MISTYの高速性により，大量のコンテンツ利用時にも，高速復号を実現している。

(2) 購入条件に応じた使用制御

コンテンツ購入時に指定した購入条件に基づいてコンテンツの使用が制御され，利用者や期間など使用環境を限定

(注1) PDF(Portable Document Format)とは，米国Adobe Systems, Inc.がディジタル化されたマルチメディア文書の交換を実現するために開発したファイル形式である。

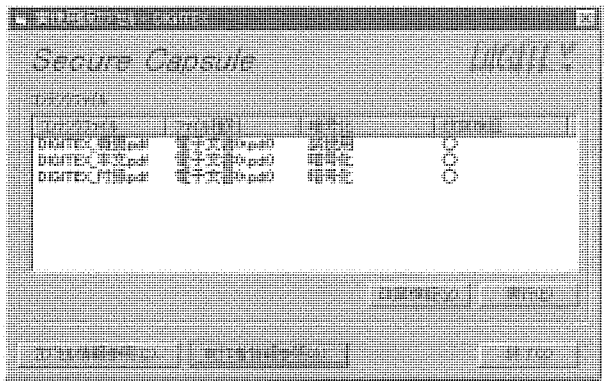


図2．セキュアカプセル利用の画面例

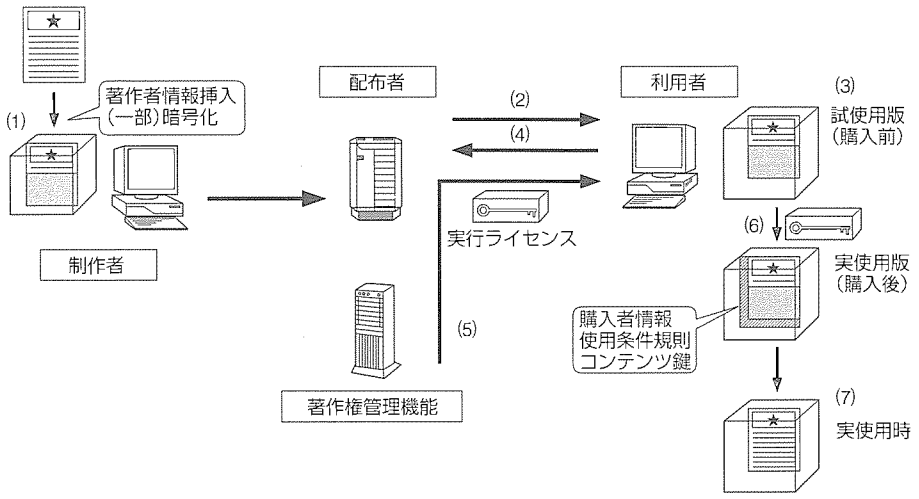


図3．DIGITEXの構成

することが可能となる。これにより，不正コピーなどの購入条件を越えたコンテンツ利用を防止・抑止することが可能となり，課金とコンテンツ使用の対応が保たれる。

(3) コンテンツの試使用が可能

利用者がコンテンツを購入する前にコンテンツの一部を利用・閲覧することのできる，試使用版のセキュアカプセルを作ることが可能である。試使用版のセキュアカプセルでは，購入した利用者のみがアクセス可能な暗号化された情報以外に，平文としてだれでもアクセス可能な情報を含んでいる。逆に，暗号化された情報は，復号する鍵がセキュアカプセル内に含まれていないため，利用・閲覧することができない。

セキュアカプセル利用の画面例を図2に示す。この例では，試使用のために暗号化されていないファイル一つと，暗号化されたファイル二つでカプセルが構成されている。

試使用後に利用者が購入する場合は，新たにコンテンツが送られるのではなく，試使用版のセキュアカプセルを実使用版のセキュアカプセルに変換する実行ライセンスが送られる。実行ライセンスには，暗号化されたコンテンツを復号する鍵のほか購入条件に応じた使用制御を行う制御情報が含まれており，変換後の実試用版セキュアカプセルでは，正規の購入利用者がコンテンツを利用・閲覧するたびに，動的に復号と使用制御が行われる。

このように試使用版を実使用版に変換するという新たな方式を用いることにより，データ量の大きい試使用版をCD-ROM又はディジタル放送などの大容量チャネルで配布し，購入のみをインターネットで行うことが可能になる。また，試使用版を再配布し，別の利用者がそれを購入することも可能になる。

(4) 著作権管理と課金管理の分離

著作権管理機能と課金管理機能を分離し独立の機能として実現することにより，コンテンツの配布と課金を行うサーバとは独立に，コンテンツの著作権を管理するサーバを配置することを可能とした。今後コンテンツ流通が普及すれば，その著作権管理を制作者に代わって行う機関が登場することも想定されるからである。

課金方式としては，会員制課金，事前課金，事後課金の3形態をサポートしている。

4.2 DIGITEXの構成

DIGITEXの構成を図3に示す。著作権管理機能は，上述したように，コンテンツ配布者の一部の機能として実装することも，独立したサーバとして実装することも可能である。代表的な処理の流れを以下に述べる。

(1) カプセル化ツールにより，制作者がコンテンツをカプセル化する。試使用以外の部分は暗号化される。

(2) 配布者のWebページで，試使用版コンテンツを配布する。

(3) 利用者がコンテンツを試使用する。

(4) 利用者からコンテンツの購入要求を配布者に発行する。

(5) 著作権管理機能で，利用者情報と購入条件から，コンテンツの復号鍵と使用制御ロジックを含む実行ライセンスを生成し，配布者経由で利用者に配布する。事前課金の場合は課金を実施する。

(6) コンテンツ利用者が，受信した実行ライセンスによって試使用版を実使用版へ変換する。

(7) コンテンツ利用者がコンテンツを使用する。使用時ごとにコンテンツは復号され，利用者限定・期間限定などの使用制御が行われる。事後課金の場合は，計測・課金を実施する。

5. むすび

インターネットの普及により，ディジタルコンテンツの流通はますます盛んになるものと考えられる。

今後は，ここで述べた技術を各種応用システムに適用し，その有効性を検証していく予定である。

参考文献

(1) 石塚裕一，酒井康行，櫻井幸一：周波数変換に基いた電子透かし技術の画質評価に関して，信学技報，87～96，ISEC97-22 (1997-7)

(2) 中嶋春光，宮崎一哉，中川路哲男：セキュアデジタルコンテンツ配布システム—DIGITEX—の開発，信学会全国大会シンポジウム，SD-3-7，(1998-3)

指紋判別装置

藤原秀人*
鷲見和彦**
大森　正***

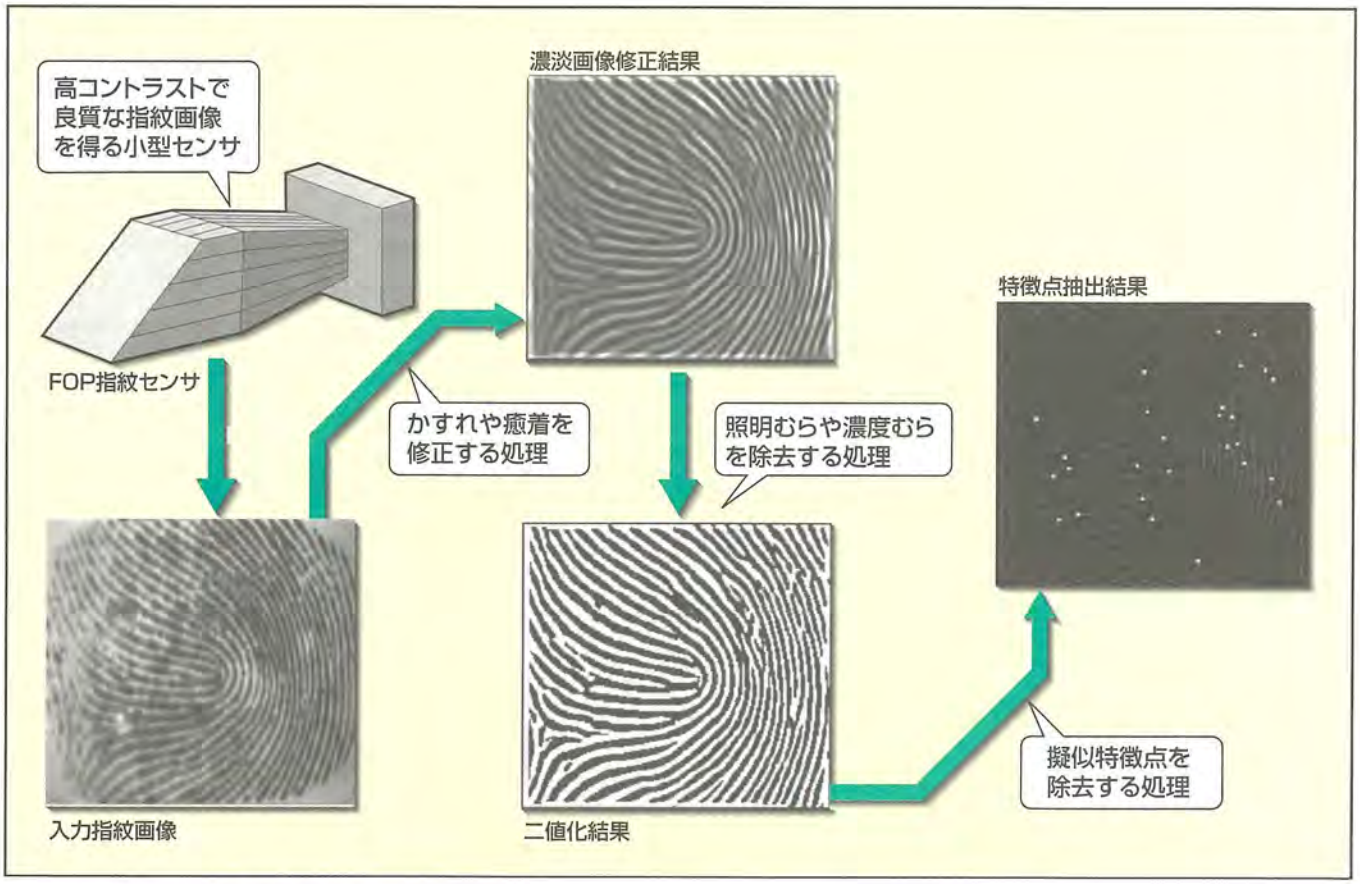
要　旨

入退室管理や情報セキュリティにおいてより高いセキュリティを実現するために，人間の身体的特徴を利用した個人識別技術の研究が盛んに行われている。中でも指紋は，万人不同，終生不変の性質を持ち，個人識別を実現する重要な特徴として利用されている。

指紋を用いた高精度な個人識別を実現するために，我々は独自の方式による指紋センサと，低品質な指紋に対してもロバストな照合を行える照合方式を開発した。

開発した指紋センサはFOP(Fiber Optic Plate)を利用したもので，得られる画像に台形ひずみがなく，小型化が可能という特長を持っている。一方，照合方式としては，指紋隆線の大局的な流れの方向を表す方向角データと，指紋の詳細な特徴を表す特徴点データを組み合わせた方式をベースとしている。指紋の濃度むらに関係なく良質な二値画像が得られる局所しきい値法や，指紋のかすれや癒着を修正する濃淡画像修正法等の前処理手法を盛り込むことでロバストを実現している。そしてこの方式の照合性能を評価した結果，他人受入れ率，本人拒否率ともに0.1%という結果を得た。

また，指紋照合装置FPR-1000HGは，30指程度を一つのグループして登録し，照合時にはグループID(Identification)と指紋画像から該当グループ内の人物を特定する検索照合機能を備えており，高いスループット(単位時間当たりの利用可能者数)を実現している。



指紋判別装置におけるセンサと処理

指紋を用いた個人識別を実現するための指紋センサと処理アルゴリズムを開発した。高精度かつコンパクトな指紋判別装置を実現するために，指紋センサの光学系にFOPを採用し，処理アルゴリズムには，指紋のかすれや癒着，照明むらや濃度むらを除去修正する各種前処理方式を開発し，実装している。

*産業システム研究所　**同研究所(工博)　***稲沢製作所

1. まえがき

指紋は個人識別の有効な手段として古くから利用されてきており，指紋照合の自動化に関する研究開発も数多く行われている。犯罪捜査の分野では，犯罪現場に残された遺留指紋の照合をも可能にするシステムが既に実用化されている。このシステムは，多数の登録指紋の中から一つの指紋を高速に選び出すので，大容量のデータベースと大規模なコンピュータシステムを必要とする。

一方，近年，社会の情報化の進展に伴って，コンピュータ室等への入退室や各種情報端末・金融端末へのアクセスに対する安全性・信頼性の高い個人確認の手段として，指紋を用いたシステムの研究開発が各所で活発に行われており，数多く実用化されている。このようなシステムでは，高コントラストで良質な指紋画像を得られるセンサと，低品質な指紋画像に対しても正確でロバストな照合を行うアルゴリズムと，これらを低コストでかつ高速に実行する装置の開発がポイントである。

本稿では，高コントラストでひずみの少ない指紋画像をリアルタイムで入力するためのセンサと，低品質な指紋画像にも対応可能な照合方式及び照合装置について述べる。

2. 指紋センサ

個人確認の用途には，利用者の抵抗が少なく，高コントラストな指紋画像をリアルタイムで入力できる指紋センサが不可欠である。センシングの方式としては，プリズムとCCD(Charge-Coupled Device)を組み合わせ，全反射法の原理を用いるものが一般的である。しかしながらこの方法では，

- 撮像素子までの光路長が異なるため台形ひずみが発生する。
- CCDに結像させるための光路長が長くなるため小型化しにくい。光路長を短くすると，画像にひずみが生じる。

という欠点がある。

そこで我々は，光ファイバを束状に接着したFOPと呼ばれる光学部品を採用することで，これらの問題を解決した[1]。

図1にFOPセンサの構成を示す。FOPセンサは，光源の発光ダイオード(Light Emitting Diode：LED)，FOP，固体撮像素子(CCD)で構成される。FOPは両端部に指を接触させる入力面と，CCDを直接接続した出力面を持っており，入力面は光源からの反射光がファイバ内を導波するようにファイバ軸に対して傾斜している。全反射法の原理で入力面に指紋パターンを生成し，そのパターンをFOPによってCCDに直接伝送する。FOPを用いることで結像光学系(レンズ)をなくし，小型の指紋センサを実現できる。また，指紋パターンをFOPで直接CCDに伝送するので，ひずみのない指紋画像が得られる。

3. 照合方式

個人確認用システムにおいて，記憶されている登録指紋とセンサから入力された照合指紋が同一かどうかを判定するための照合方式として，例えば，①図2に示すような端点(隆線が途切れる点)や分岐点(枝分かれする点)を特徴点として，その座標と特徴点から伸びる隆線方向を用いる特徴点マッチング[2][3]，②図3に示すような指紋隆線の大局的な流れの方向を用いる方向コードマッチング[3][4]，③指紋画像を二値化した二値画像のテンプレートマッチングによって照合する二値画像パターンマッチング[5]，④指全体の画像を対象とした射影マッチング[4]等が提案されている。

今回の開発では，方向コードマッチングと特徴点マッチングを組み合わせた照合方式をベースとして，かすれ，癒着，濃度むらが存在するような低品質な指紋でも精度良く照合できるような工夫を前処理に盛り込んでいる。以下に処理の概要を記す。

3.1 隆線の方向角算出

まず二値化処理を行うが，センサで入力した画像は，照明むらや指の表面状態の影響で濃度むらがある。特に乾燥した指等では低コントラストな画像しか得られないため，より一層濃度むらが顕著になる。したがって，良質な二値画像を得るには，画面内の各部分に応じてしきい値を変える局所しきい値法が必要である。今回，指紋の濃淡画像が隆線部と谷線部が交互に繰り返す周期パターンである点に

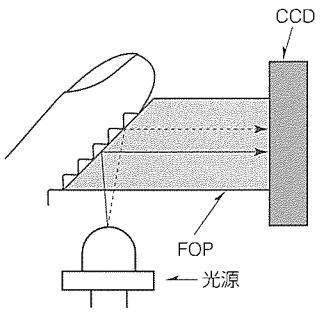


図1．FOPセンサの構成

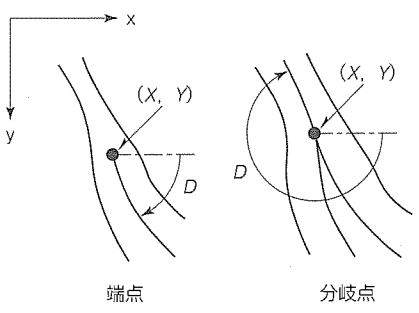


図2．特徴点

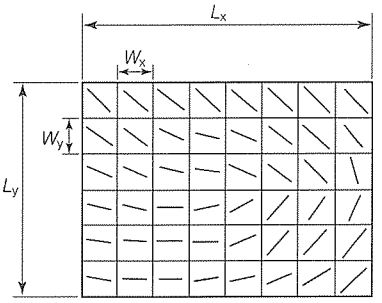


図3．隆線の方向コード

着目し，１画素ごとにその点を中心とする$N \times N$近傍の平均濃度からしきい値を決定するようにしている。

そして，二値画像を図３に示すように幾つかの小領域に分割し，各小領域内で図４に示すような４方向に対応したマスクパターンを計数し，この計数値から隆線の方向（-90°～90°）を算出する。ただし，この段階で得られた隆線方向は，雑音が顕著な小領域においてその信頼性が損なわれているので，確率的し（弛）緩法によって周囲とのつじつまが合うように修正される。結果として得られた小領域ごとの隆線の方向を方向角データと呼ぶ。

3.2　特徴点抽出

指紋の濃淡画像において癒着や途切れ等の雑音が多くなると，その影響で，本来は特徴点でない点（擬似特徴点）が増加する。このような擬似特徴点は，細線化後にも隆線構造の復元処理によってある程度除去可能であるが，復元処理にかかる負担や特徴点の抽出精度から考えて，癒着や途切れ等の雑音は二値化の前にできるだけ取り除いておくことが望ましい。

そこで，まず，3.1節で算出された隆線の方向角データを８方向に量子化した方向コードを用いて濃淡画像を修正する。具体的には，１画素ごとにその点を中心として，隆線の方向コードに応じた$M \times 1$近傍領域の平均値を計算し，結果をその中心点の新しい濃度値とするものである。

次に，上記処理で修正された濃淡画像を3.1節で説明した局所しきい値法で再度二値化し，更に細線化処理を施す。

最後に，細線化画像から特徴点を抽出し，途切れ，ひげ，癒着といった擬似特徴点を除去する。また，特徴点の位置を始点とし，線を所定の画素数だけ追跡したときの最終位置を終点とするベクトルから特徴点の方向を算出する。ここで，特徴点の座標と特徴点から伸びる隆線の方向（ベクトル角）を併せて特徴点データと呼ぶ。

図５から図８に処理結果の一例を示す。図５は原画像，図６は濃淡画像修正後の結果，図７は二値画像，図８は細線化画像と特徴点（白点）の抽出結果である。

次に，登録された指紋（登録指紋）の方向角・特徴点データと，利用時に入力された指紋（照合指紋）から抽出された方向角・特徴点データを照合して，本人のものか否かを判断する照合処理について説明する。

3.3　方向角データによる粗照合

まず，3.1節で述べた処理によって得られた，隆線の大局的な流れの方向を表す方向角データを用い，粗照合を行う。粗照合においては，照合指紋と登録指紋の方向角データを図９のように上下左右にそれぞれ±数領域ずつずらしながら各ずらし量における方向角の差の二乗平均を計算し，その最小値を方向角一致度として本人と他人の粗判別を行う。なお，最小値を示すずらし量が登録指紋と照合指紋の粗い位置ずれ量である。

3.4　特徴点データによる精照合

3.3節で述べた粗照合で方向角一致度がしきい値よりも小さい場合，すな

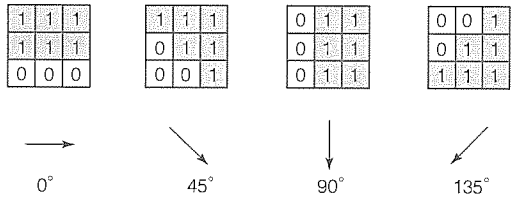


図４．方向別マスクパターンの例

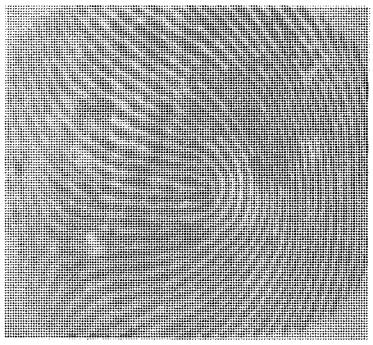


図５．原画像

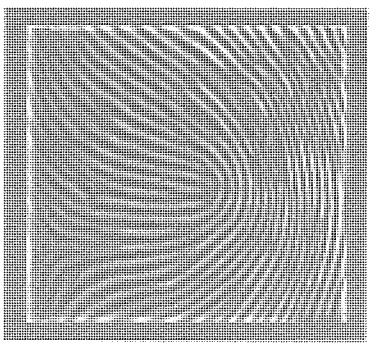


図６．濃淡画像修正結果

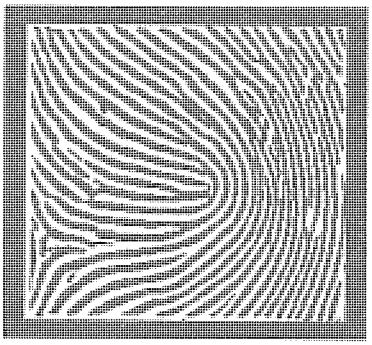


図７．二値化結果

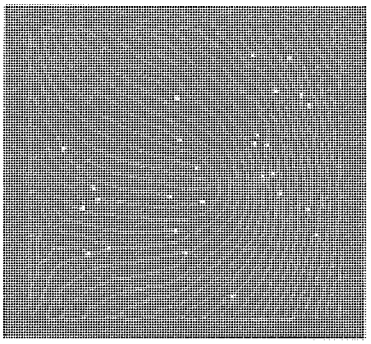


図８．特徴点抽出結果

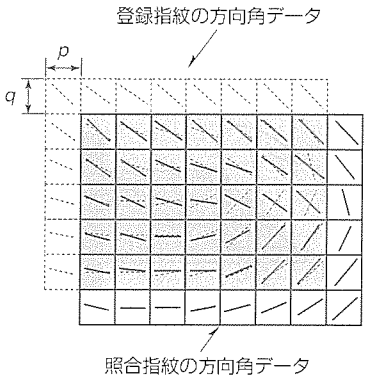


図９．方向角データによる粗照合

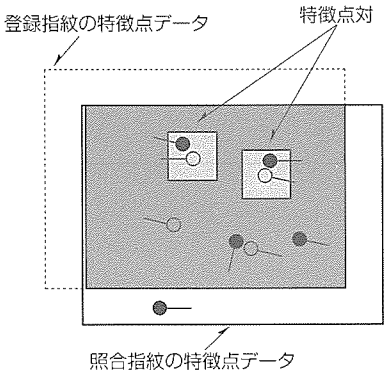


図10. 特徴点データによる精照合

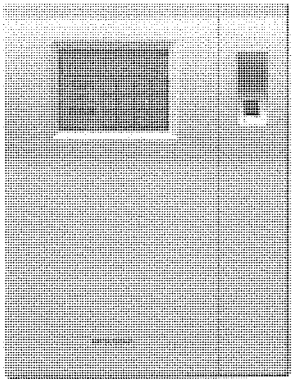


図11. 小型指紋照合装置FPR-1000HG

わち本人の可能性が高いと判断された場合には，3.2節の処理によって得られた特徴点データを使って精照合を行う。精照合においては，まず，照合指紋と登録指紋の特徴点を上下左右に数～十数画素の範囲で位置合わせしながら比較し，座標とベクトル角の差が小さい特徴点の組を特徴点対として選出する(図10)。そして，全特徴点数と特徴点対の数の比率を特徴点一致度として計算し，この特徴点一致度がしきい値よりも大きい場合に本人であると判定する。

3.5 照合性能

上記に説明した照合方式の性能を検証するために，今回，非常にかすれた指紋やしわの多い指紋など低品質な指紋を含めた200指程度のデータを採取し，本人拒否率及び他人受入れ率を検証した。照合性能は指紋のかすれ具合や凹凸の大小によって照合性能は左右されるため一概には述べられないが，前記したデータを用いた評価では，他人受入れ率が0.1%のとき本人拒否率0.1%以下という高い照合性能を持つことを確認した。

4. 指紋照合装置

ここでは，以上述べてきた照合技術を基に製品化した指紋照合装置を紹介する。図11に当社製指紋照合装置FPR-1000HGの外観を示す。この装置は，前記照合方式を1秒以下の時間で実現するための専用ハードウェアを内蔵している。

また，この照合装置は，液晶タッチパネルによる簡単操作や複数端末の遠隔集中管理による大規模システムへの対応等の特長に加え，通常のパーソナルID入力による1対1照合機能のほかに部署番号等のグループIDによる検索照合機能(1対N照合)の装備といった特長を持っており，出退勤管理システム等で利用しやすい構成になっている。また，複数の端末から得られた情報を遠隔地にある管理パソコンで集中管理でき，大規模なシステムへの適用も考慮されている。

5. むすび

以上，指紋照合におけるセンサと処理方式，及び検索照合機能を持った照合装置について概説した。今後，セキュリティに対する関心が高まるにつれて，より信頼性の高い個人識別技術の重要性はますます増加するであろう。その意味で，指紋センサ及び処理アルゴリズムの両面から更に改善・改良が加えられ，高精度でありながら，より使いやすく，より低コストなシステムを実現していくことが必要である。

参考文献

(1) 鹿井正博，宇佐見照夫：ファイバーオプティックプレートを用いた指紋センサ，電気学会研究会資料，IM-95-43，1～8 (1995)
(2) 森田孝一郎，浅井　紘：個人識別用指紋照合端末，信学技報，AL85-56，97～104 (1985)
(3) 笹川耕一，磯貝文彦，池端重樹：低品質画像への対応能力を高めた個人確認用指紋照合装置，信学論(D)，J72-D-Ⅱ，5，707～714 (1989)
(4) 南　敏，重光嶺男，津崎美樹：指紋照合のための新しいセキュリティシステムの開発，エレクトロニクス，No.9，38～43 (1988)
(5) 井垣誠吾，矢作裕紀，江口　伸，池田弘之，稲垣雄史：ホログラフィック指紋センサを用いた個人照合装置，信学技報，PRU87-31，27～33 (1987)

オンライン筆者照合技術

依田文夫*
小川　勇*
川又武典*

要　旨

近年，コンピュータネットワーク上での電子商取引，コンピュータに保存した機密文書へのアクセス，重要施設への入退場などにおけるセキュリティ機能を高めるために，個人認証技術が重要になってきた。この要求にこたえるため，モバイルコンピュータ“AMITY”等の携帯情報端末上に筆記した筆跡から本人であるか否かを判定するオンライン筆者照合技術を開発した。

本稿では，このオンライン筆者照合方式の概要について述べる。

この技術は以下の特長を持っている。

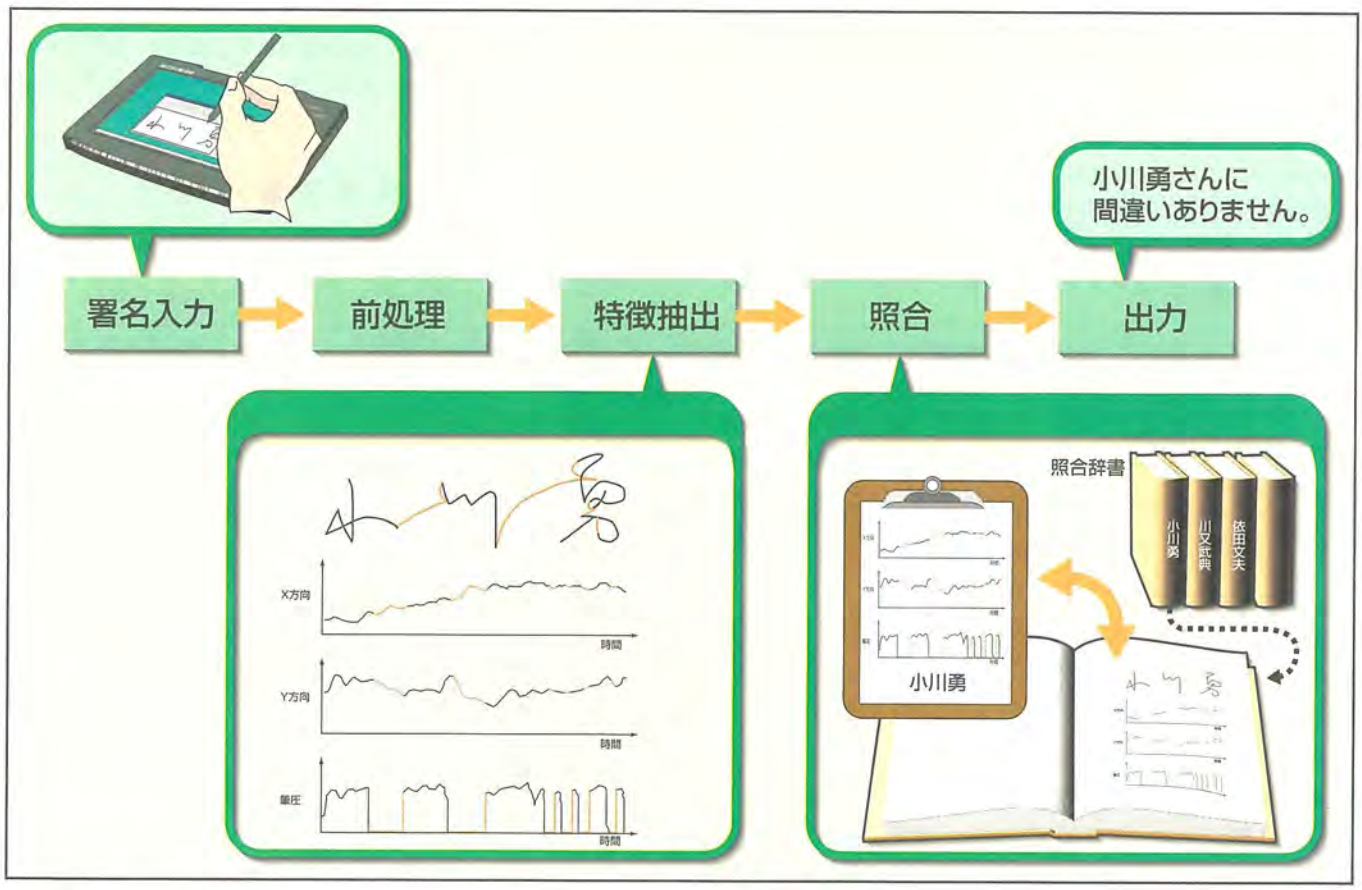
(1)　筆跡・筆順・筆速・筆圧の情報を個人固有の登録パターンと対応付けることにより，高い信頼度で個人を確認できる。

(2)　判別に使用する特徴を選択できるようにしたため，電磁誘導，感圧等のハードウェア(座標入力装置)の種類に依存しない柔軟なシステムを実現できる。

(3)　Windows(注1)の標準プラットフォームで動作するDLL(Dynamic Link Library)形式で実現したため，既存のアプリケーションとの連携を容易に行うことができる。

(4)　一人当たりの情報量を約1kバイトとコンパクトに抑え，高いポータビリティを実現した。

(注1)“Windows”は，米国Microsoft Corp.の商標である。



筆者照合処理のフロー

モバイルコンピュータ“AMITY”を用いて入力した署名の位置と大きさの正規化を前処理で行った後，個人を判定するために必要な特徴を抽出する。次に，メモリの中にあらかじめ格納してある登録署名の特徴と前記抽出した特徴とを比較して得た距離値をしきい値と比較することにより，本人であるか否かを判定する。

*情報技術総合研究所

1. まえがき

電子化が進み，コンピュータネットワークを介した買物や受発注を行う電子商取引がこれからますます盛んになる。また，入退場の管理，パソコン上の機密情報の管理など，セキュリティ確保への要求は強い。このような種々の応用においてセキュリティ機能を高める必要があるが，このためには，対象者が正当に承認された本人であるか否かを調べる必要がある。しかし，現状の本人確認はパスワードや暗証番号による方法が一般的であり，一般ユーザーは，番号を忘れたり他人に盗用されるという危険な状態にさらされている。このような問題を回避するために，最近では指紋やこう(虹)彩による本人照合装置が製品化されている。しかし，これらの装置は精度が高い反面，コストが高く，一般ユーザーがパソコン等で手軽に利用できないという課題がある。

そこで今回，低コストで手軽に利用できる本人照合技術を提供するため，当社のモバイルコンピュータ“AMITY”などの携帯情報端末上に筆記した署名によって本人を確認できるオンライン筆者照合技術を開発した。

本稿では，個人認証における筆者照合技術の位置付けを概観した後，今回開発した筆者照合方式について述べる。さらに，この方式を当社のモバイルコンピュータAMITY上に適用して評価した結果を紹介する。

2. 個人認証と筆者照合技術

個人を認証するには，①指紋・手形・虹彩など人間の肉体的な特徴を用いる方法，②パスワードや暗証番号など個人の記憶情報を用いる方法，③かぎ(鍵)や印鑑など所有物を用いる方法，などがある。筆者照合技術は，上記手法と異なり，個人の習慣化した特徴を用いて個人を同定する手法に位置付けられる。具体的には，個性の現われる筆跡や筆記を手掛かりに本人か否かを判定する。

この筆者照合方式は，さらに，オフライン方式とオンライン方式に大別される。オフライン方式は，データ入力装置として画像入力装置を用い，小切手など紙の上に書かれた署名の形状，線の太さなどの特徴を抽出して個人を同定する。一方，オンライン方式は，データ入力装置としてタブレットという座標検出装置を用い，筆記した署名の情報を用いて個人を同定する。この場合，署名の形状だけでなく筆の運び具合や筆圧を時間関数として計測できるため，署名の動的な情報を照合に利用できる。署名の動的な情報は，筆記者の個性を含んでいるだけでなく，目視で確認できないために他者にまねされにくいという特長を持っている。そのため，オンライン方式は，オフライン方式に比べて高精度な照合を実現できる。またオンライン方式は，データ入力装置を小型にできる利点がある。

以上の観点から，今回，オンライン方式の筆者照合技術を開発した。なお，この技術を広く個人ベースで普及させるためには，できるだけシンプルで安価な構成で実現する必要がある。すなわち，できるだけ既存の装置(ハードウェア)を流用できる方式を考えることが，実用上重要である。このため，電磁誘導，感圧等のタブレットの種類に依存しない，柔軟な方式を開発した。以下，この方式について説明する。

3. オンライン筆者照合方式

筆者照合技術は，パターン認識の一つの応用例である。具体的には，メモリの中に格納した個人の登録データと未知の入力データとを比較して得た距離値を事前に定めたしきい値と比較することにより，本人であるか否かを判定する。**図1**に当社が開発したオンライン筆者照合方式の処理の流れを示す。この方式では，座標入力装置を用いて入力した署名(以下“入力署名”という。)に対して，位置や大きさ等の正規化を行った後，個人を判定するために必要な特徴を抽出する。そして，抽出した特徴を使用してあらかじめ登録した本人署名(以下“登録署名”という。)の特徴と照合を行い，照合結果を出力する。以下，図に示す各処理についての詳細を述べる。

3.1 署名の入力

タブレットなどの座標入力装置を用いて署名を筆記することにより，ペンがタブレットに接触している点(以下“座標点”という。)の位置と筆圧の情報を一定の時間間隔でサンプリングする。この方式では，この時系列の座標点列情報を入力署名情報として使用する。

図2に入力署名の例を示す。図において，(a)は画面に筆記した署名の筆跡，(b)は(a)の署名を筆記したときのペンの動作と筆圧を一定時間間隔でサンプリングした結果である。

3.2 前処理

3.1節の方法で得た入力署名は，座標点数と座標値に冗長な情報が含まれている。同一人物でも常に同じ位置に同じ大きさの署名を書くとは限らないため，このような個人内変動を除去する必要がある。そこで，個人特有の特徴抽出を行う前に，入力署名に対して位置，大きさ，座標点数

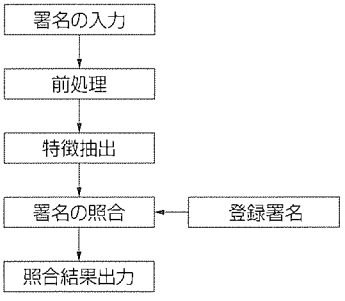
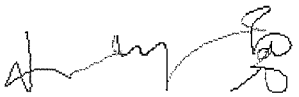
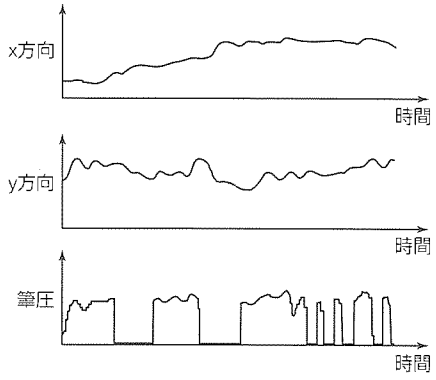


図1. 処理フロー



(a) 入力署名の筆跡



(b) 入力署名のサンプリング情報

図2． 入力署名の例

の正規化を行う。具体的には，位置の正規化として，入力署名の外接く(矩)形を求め，外接矩形のx座標成分，y座標成分の最小値がそれぞれ値“0”となるように入力署名を平行移動する。また，大きさの正規化として，外接矩形が一定の値になるように縮小する。また，座標点数の正規化として，入力署名の座標点数を所定の値Nに間引く。なお，入力署名の時間情報を保存するため，間引きは等時間間隔で行う。

3.3 特徴抽出

前処理で正規化した入力署名から，署名を照合するための特徴を抽出する。従来の署名照合方式には，ストローク(ペンが面に接触してから離れるまでの軌跡)単位又は座標点単位で特徴を抽出するものがある。しかし，ストローク単位で特徴を抽出する方式では，個々のストロークが複雑な形状をしている(例えば英語署名)場合，照合に十分な特徴を抽出することができない。また，座標点単位で特徴を抽出する方式では，抽出した特徴が署名の局所的な変動に対して影響を受けやすい。そこで，上記の問題点を解決するため，ストロークをセグメントと呼ぶ単純な線素に分割して特徴を抽出する方式を採用した。

3.3.1 座標点間の対応付けとセグメント情報の作成

セグメント情報を作成するために，まず，正規化した入力署名と登録署名との間で座標点間の対応付けを行う。座標点間の対応付けにはDP(Dynamic Programming)マッチングの手法を使用する。次に，対応付けた座標点間の情報からセグメント情報を作成する。ここで，セグメントとは，同じ座標点間に対応する一つ以上の座標点間の集まりを指す。例えば**図3**に示す入力署名($N=4$)と登録署名が存在する場合，入力署名の座標点間のaとbが共に登録署名の

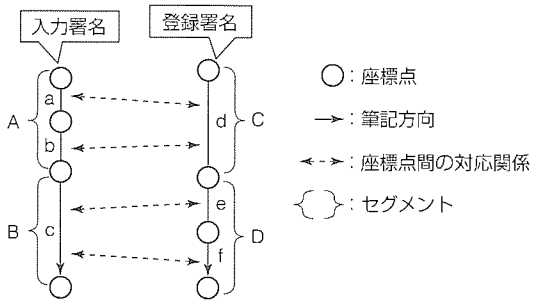


図3． セグメント情報の作成例

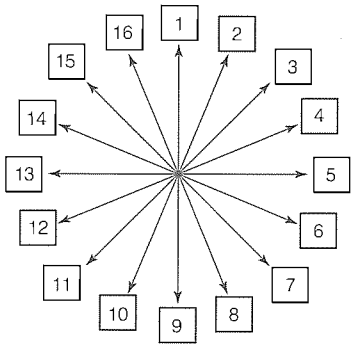


図4． 筆記方向

座標点間dに対応付いているため，入力署名の座標点間aとbを一つのセグメントAとする。また，入力署名の座標点間cは，同じ座標点間に対応する他の入力署名の座標点間が存在しないため，座標点間cのみを一つのセグメントBとする。同様にして登録署名のセグメント情報C，Dをダイナミックに作成する。

3.3.2 セグメント特徴の抽出

次に，セグメント情報を使用して，入力署名と登録署名とのそれぞれに対して特徴抽出を行う。この方式では，各セグメントに対して①長さ，②筆記方向(360°を16方向に量子化して表現したもの，**図4**参照)，③筆記時間(セグメントに属するサンプル点間数で表現)，④筆記速度，⑤平均筆圧，⑥筆圧変化を抽出する。

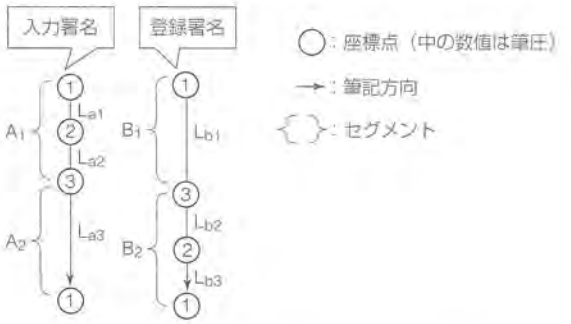
図5に$N=4$の入力署名のセグメントA_1，A_2，及び登録署名のセグメントB_1，B_2に対する特徴抽出例を示す。以下，各セグメントに対して抽出した特徴を“セグメント特徴”と呼ぶ。

3.4 照　合

特徴抽出処理で得た入力署名のセグメント特徴と登録署名のセグメント特徴とを使用して署名の照合を行う。具体的には，全セグメント数をSとした場合，入力署名の特徴kのセグメント特徴f_{ki}と登録署名の特徴kのセグメント特徴A_{ki}との距離D_kを式(1)で求める。

$$D_k=\frac{1}{S}\sum_{i=1}^{S}\left|f_{ki}-A_{ki}\right| \quad \cdots\cdots (1)$$

次に，求めた各特徴の距離D_kと特徴ごとにあらかじめ



セグメント	長さ	筆記方向	筆記時間	筆記速度	平均筆圧	筆圧変化
A_1	$L_{a1}+L_{a2}$	9	2	$(L_{a1}+L_{a2})/2$	2	2
A_2	L_{a3}	9	1	L_{a3}	2	−2
B_1	L_{b1}	9	1	L_{b1}	2	2
B_2	$L_{b2}+L_{b3}$	9	2	$(L_{b2}+L_{b3})/2$	2	−2

図5．セグメント特徴の抽出例

設定したしきい値T_kとを比較する。各特徴の距離D_kが一つでもしきい値T_kを超える場合は，入力署名を本人の署名ではないと判定する。特徴ごとに求めた距離D_kがすべてしきい値T_k以内になる場合は，入力署名を本人の署名であると判定する。同一人物であっても，署名は入力ごとに変動するため，変動を考慮したしきい値を設定する必要がある。そのため，しきい値は，登録署名の作成時に求めた各特徴の平均値及び標準偏差を利用して決定する。

また，この方式では，各特徴ごとに独立に距離値の評価を行うため，入力装置や使用条件に応じて照合に使用する特徴を自由に変更することが可能である。例えば，本稿の説明では筆圧の特徴を使用しているが，筆圧情報が取得できない入力装置を使用する場合は筆圧の特徴を使用しない照合が可能である。

3.5 登録署名の作成

署名の照合を行うためには，筆記者があらかじめ自分の署名を登録する必要がある。この方式では，登録用の署名として5個の署名から平均的な座標点列情報と各特徴の平均値・標準偏差を求め，これらの情報を登録署名として保存する。

4. モバイルコンピュータAMITYへの適用と性能評価

当社のモバイルコンピュータAMITY VPにこの方式を適用して性能の評価を行った。

4.1 筆者照合ソフトウェア

筆者照合ソフトウェアを，Windowsの標準プラットフォーム上で動作する汎用性の高いDLL形式で作成した。このため，既存のアプリケーションソフトウェアとの連携を容易に行うことができる。またこの方式は，1人分のデータに必要なメモリ容量は約1kバイトと小さく，ローカルで動作させる携帯端末やネットワークサーバのいずれに対しても簡単に実装できる。このソフトウェアを当社のモバイルコンピュータ"AMITY VP"上で動作させた例を図6に示す。

図6．AMITY VPへの適用例

4.2 性能評価

10名の筆記者が入力した本人の署名と，3名の筆記者が入力した10名分の偽筆署名とを使用して，この方式の照合性能を評価した。ここで，偽筆署名は，①筆跡を見せないで筆記させる，②筆跡を一度見せた後に筆記させる，③筆記中も筆跡を見せる，の3種類の条件で評価した。この結果，1回の試行による本人受理率（本人が本人と正しく判定される率）は平均で95%，他人拒否率（他人を正しく排除する率）は筆記中も他人の筆跡を見せる厳しい条件でも99%以上の性能が得られた。2回の試行を行う場合，本人受理率は，更に高い精度が得られる。なお，この方式は要求性能に応じて最適なしきい値を設定できる構成になっており，用途に応じて本人受理率，他人拒否率を変更することが可能である。

5. むすび

タブレット上に筆記した筆跡・筆順・筆速度・筆圧等から個人を特定する筆者照合方式を開発し，モバイルコンピュータ"AMITY"等の携帯情報端末上で高信頼，低コストのセキュリティを実現できることを述べた。

今後は，ネットワークをベースとした認証システムへの組み込みや，指紋照合方式と組み合わせたシステム等を検討する予定である。

参考文献

(1) 小川　勇，川又武典，南部　元，依田文夫：大局的特徴と局所的特徴とを併用したオンライン筆者識別方式，情報処理学会第53回全国大会講演論文集分冊2，271～272（1996）

(2) 小川　勇，川又武典，依田文夫：セグメント特徴を使用したオンライン署名照合方式，情報処理学会第56回全国大会講演論文集分冊2，（125～126）（1998）

アクセスマネジメントシステム

野沢俊治*
笹川耕一**

要　旨

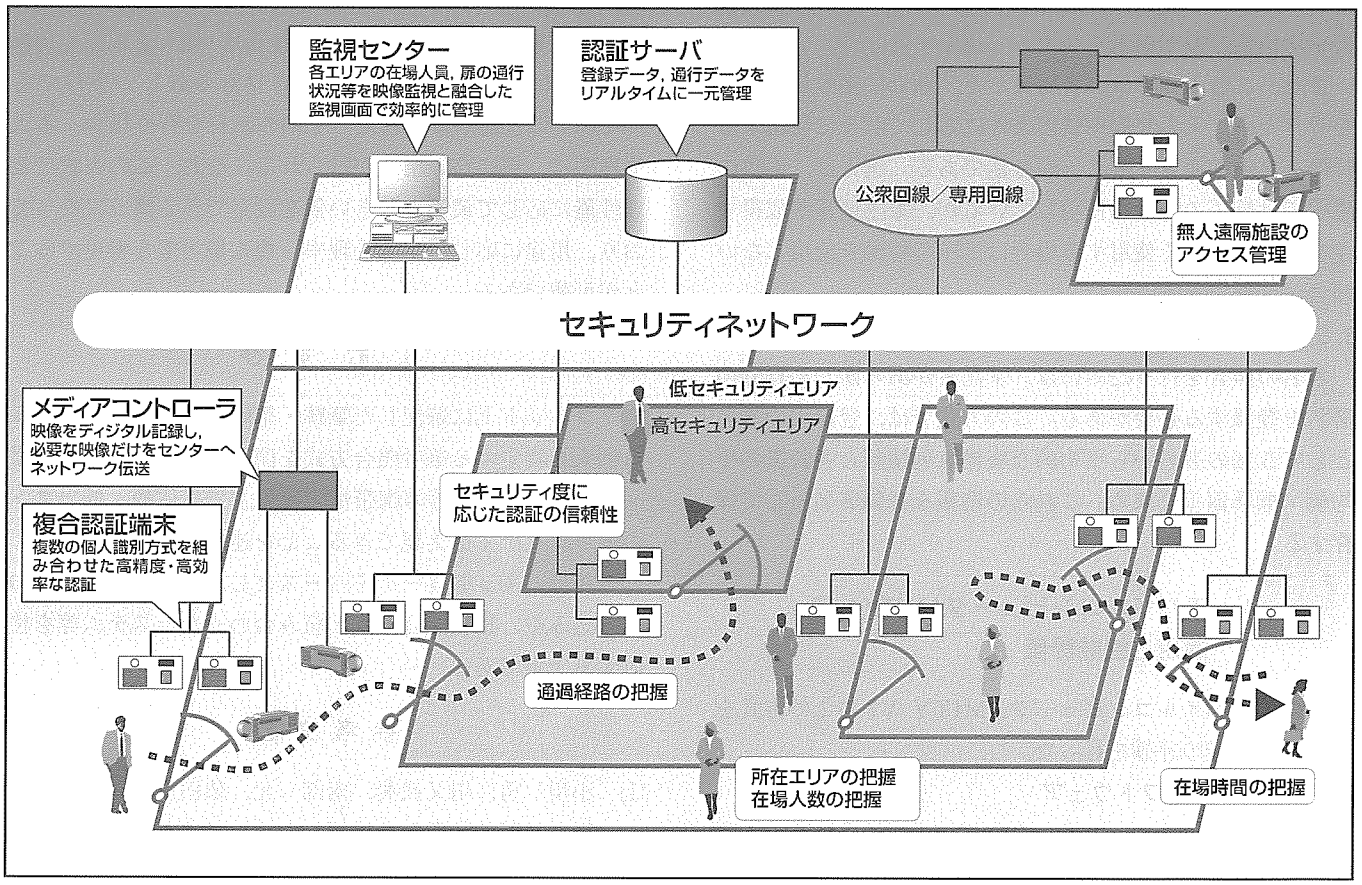
近年，我が国においても社会情勢の変化などからセキュリティシステムに対する関心が高まってきているが，普及拡大のためには，人的警備に勝るコスト効率が要求される。特に公共空間や重要施設などでは，大規模なエリアを遠隔で効率良く確実に監視する必要がある。このようなニーズに対応するため，現状のセキュリティシステムに加え，以下のような機能拡充・強化を図ったアクセスマネジメントシステムの検討を行っている。

(1)　エリア管理
- 個人の在場エリアや在場時間，通行経路の把握。エリアの在場人員の把握
- エリアのセキュリティレベル，時間帯，在場人員等に対応した認証信頼度の動的変更

(2)　個人識別の高度化
- 複数のバイオメトリック方式を組み合わせ，利便性と信頼性の両方を向上
- 個人の照合特性に適応し，動的に照合パラメータを変更

(3)　マルチメディア監視技術の適用
- 照合時に自動的に通過する人を記録
- 照合失敗時や照合度が低い場合には自動的にアラームを出し，監視センターに映像表示
- 侵入等のアラーム発生前後の映像を自動記録

本稿では，これらの機能の概要について紹介する。



アクセスマネジメントシステムの概念

エリア全体での人の所在を管理する面的なセキュリティを少人数で効率的に実現することを目指す。このために，遠隔で多数の扉やエリアの状態を確実に管理できるよう，①複合認証端末による高度な個人認証，②メディアコントローラを利用した映像監視，③エリア全体の認証端末の状態をリアルタイムで一元管理する認証サーバ，等の技術開発を進める。

*産業システム研究所　**同研究所（工博）

1. まえがき

セキュリティという概念は幅広く，いわゆる防犯と言われる分野以外にも，近年関心が高まっている情報セキュリティや個人の身体状況をモニタするパーソナルセキュリティ，さらに広義に解釈すれば，国防や防災まで含まれることもある。したがって，これを一概に定義することは困難であるが，一般的に言ってセキュリティとは，“特定の資産を想定される脅威から防護すること。そのために，脅威の発生又はその前兆を発見し，特定し，資産に脅威が及ぶことを抑止し，脅威が発生した場合はこれを排除すること。”と言える。ここで言う資産には人命，金銭，物品，設備，情報，環境，エネルギー等が含まれ，脅威とは資産に対する破壊・殺傷，消費・不正使用，窃取，改変・改ざん等を指す。脅威発生の原因としては，故意(人間の意志)，過失(人間のエラー)，故障(装置のエラー)，自然現象(災害，経時変化)が考えられる(図1)。

このうち，人の故意による脅威を専ら資産に対する物理的アクセス(接近)を管理制御することで抑止するのが防犯セキュリティである。

本稿では，防犯セキュリティシステムの今後の展開として，我々が検討しているアクセスマネジメントシステムの概要について述べる。

2. 防犯セキュリティシステムの現状

現状の防犯セキュリティには図2に示すように四つの主要な機能があり，これらが単独のシステム又は統合されたシステムとして提供されている。当社も，これらの機能を統合したビルセキュリティシステム“MELSAFETY-C”シリーズを製品化している。

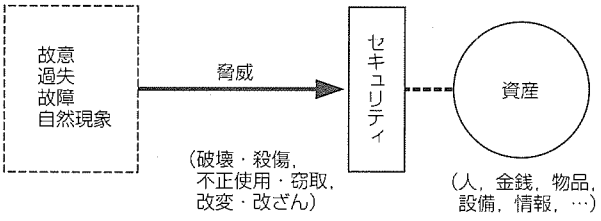


図1．セキュリティの概念

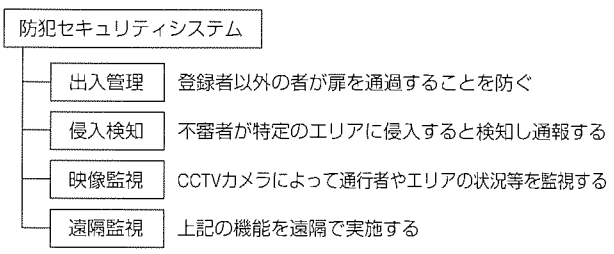


図2．防犯セキュリティシステムの機能

出入管理機能は，アクセスコントロールとも呼ばれ，暗証番号やカード等によって本人認証を行い，あらかじめ登録された人間であることが確認されると，電気錠等を制御して扉の通行を許可するものである。

侵入検知機能は，赤外線，超音波，マイクロ波等のセンサによって人間の接近を検知し，通報する。常時無人のエリアや夜間等の時間帯に無人になるエリアでの不審者検知に威力を発揮する。

映像監視機能は，主要地点に配置した監視カメラの映像を監視センター等でモニタし，不審者の発見や状況の把握を行う。

遠隔監視は，無人施設や保安要員がいない施設と警備会社や遠隔の監視センターとを公衆回線等で接続し，上記機能を実現するものである。

今まで我が国では，セキュリティシステムの導入は一部のビルや施設に限られていたが，昨今の社会情勢などから，今後，欧米並みに普及が進むものと思われる。また，勤怠管理や刑務所の管理など，新たな用途への展開も行われ始めている。

3. アクセスマネジメントシステム

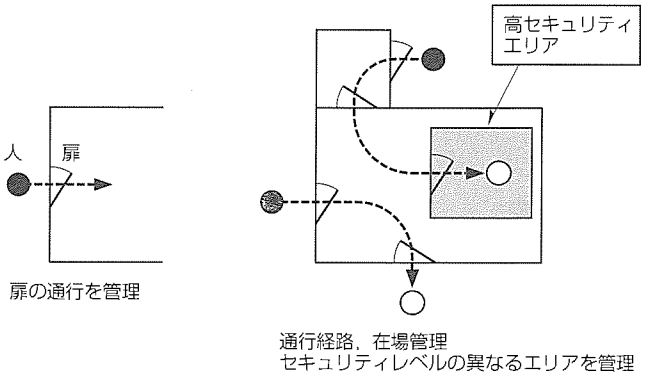
前章で記したような新たな分野や対象への展開を視野に入れながら，以下に挙げる点で現状の機能を拡充・強化させたシステムの検討を行っている。このような概念のシステムをアクセスマネジメントシステムと呼ぶ。

3.1 エリア管理

現状の出入り管理では基本的に特定の扉の通行を管理制御する“点”のセキュリティであるが，ビル全体でのセキュリティや空港，公共施設などの大規模空間でのセキュリティを考えると，以下のような“面”的なエリア管理の概念が必要になる(図3)。

(1) エリアでの在場管理

大規模な施設では，複数のエリアで構成され，出入りの扉や通行経路も複数あることが一般的である。このような



(a) 従来の出入り管理　(b) アクセスマネジメントシステム

図3．エリア管理の概念

施設で扉の通行管理データを一元管理し，特定の人がどのエリアにいるか，逆に特定のエリアにだれがいるかを把握できるようにする。また，これに基づいて在場時間や通行経路の管理も行え，詐称等の不正アクセスの発見にも利用できる。

(2) セキュリティ度に応じたアクセス管理

セキュリティレベルの異なるエリアで構成される施設では，セキュリティレベルに応じたアクセスマネジメントが必要となる。低セキュリティレベルのエリアへの出入りには利便性が阻害されない認証手段が，高セキュリティのエリアでは高信頼性が要求される。このようなセキュリティ度の違いに対しては，後述するように，認証方式のパラメータを変えたり，複数の認証方式の組合せにより，利用者に異なる操作を要求せずに実現できる。また，高セキュリティエリアでは，単独の在場を認めないなど，在場管理と絡めたセキュリティ手法を採る。エリアのセキュリティ度は，時間帯や使用状態等によって動的に変更する。

3.2 個人識別の高度化

今後，比較的高セキュリティが要求される場合の個人識別は，指紋など身体特徴情報を使うバイオメトリック方式が主流になっていくと思われる。バイオメトリック方式は，現在でも十分に実用に耐え得る精度を持っているものの，原理的にはわずかな確率で識別誤りが発生する。これについては，個々の識別方式の精度向上と同時に，システムとして対応することも重要である。例えば，以下に示すように，識別のパラメータを変更したり複数のバイオメトリック方式を組み合わせて識別を行うことで利便性と信頼性のバランスをとったり，両方を向上させたりすることができる。

バイオメトリック方式の認証誤りには，他人を登録された人間と誤る他人受許(False Acceptance：FA)と，登録された人間を他人と誤る本人拒絶(False Reject：FR)の二種類がある。本人かどうかの判断は，登録データと認証データの一致度がしきい値を超えるかどうかによって行われる。FAとFRの発生確率はこのしきい値に依存し，**図4**に示すように，しきい値を下げればFR率は減るがFA率が増加し，しきい値を上げればFA率は減少するがFR率が増加する。したがって，このしきい値をセキュリティ度に応じて変化させることにより，利便性と信頼性のバランスを調整できる。また，FR率は個人に依存するため，FRが起きやすい人に対してはしきい値を下げるなど，個人に適応して動的にしきい値を変動させる方式も考えられる。

一方，FA率とFR率を同時に改善することは，しきい値の変化だけでは困難である。そこで，例えば指紋と顔画像のような独立した二種類の認証方式を組み合わせることを考える。認証は，例えば，**表1**に示すように，二方式とも照合成功した場合のみ本人とみなすAND方式とする。

各方式のFA率をfa_1，fa_2，FR率をfr_1，fr_2とすると，二方式を組み合わせた場合のFA率(FAR)とFR率(FRR)は，$FAR=fa_1 \cdot fa_2$，$FRR=fr_1+fr_2$となる。したがって，通常の状態で組み合わせれば，FA率は極めて良くなるが，FR率が増加してしまうことになる。例えば$fa_1=fa_2=0.1\%$，$fr_1=fr_2=1\%$とすると，FAR=0.0001%，FRR=2%となる。ここで各方式のしきい値を下げて$fa_1=fa_2=1\%$，$fr_1=fr_2=0.4\%$に設定できるとすると，FAR=0.01%，FRR=0.8%となり，FA率，FR率とも改善することができる。組合せは，単純なAND方式以外にも，組み合わせる識別方式の特性に合わせて重み付けを行ったりOR方式にするなどの手法が考えられる。

二方式を組み合わせる場合，利用者に二度認証動作を行わせるのでは利便性が著しく阻害されるが，指紋と顔画像又は音声のように同時に識別ができて利用者に余計な操作を強いることがないように工夫すれば，システムとしての精度を上げる有効な手法となる。

3.3 マルチメディア監視技術の適用

3.3.1 メディアコントローラの機能

現状でもCCTVによる映像監視は行われているが，大規模なエリアを効率的に監視するためには，各種センサと連動したマルチメディア監視技術の適用が欠かせない。我々は，産業用の各種映像監視システム向けに，以下のような機能を持つメディアコントローラ[1]を開発している(**図5**)。

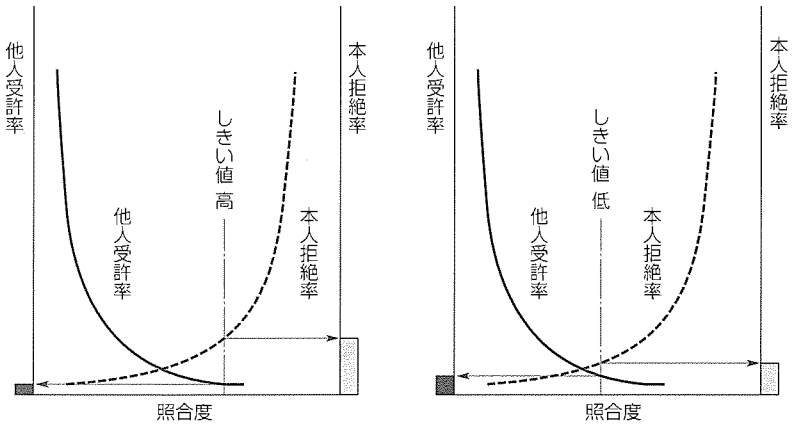


図4．バイオメトリック方式の識別誤り

表1．二方式の組合せによる照合の一例

		方式1	
		OK	NG
方式2	OK	OK	NG
	NG	NG	NG

OK：照合成功　NG：照合不成功

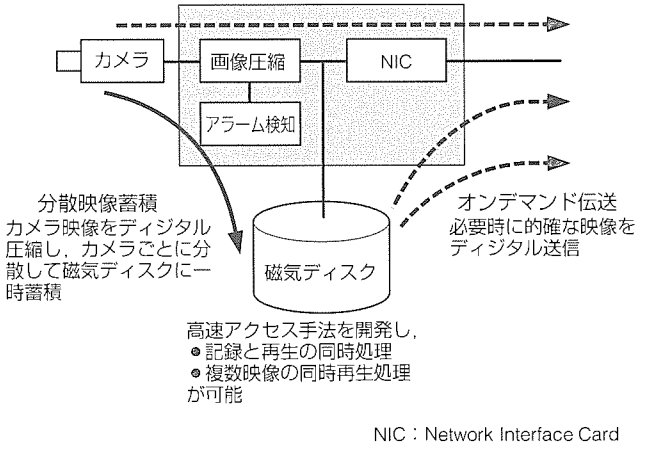


図5．メディアコントローラの機能

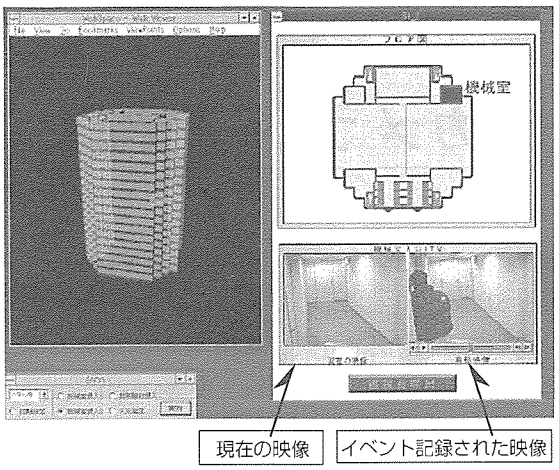


図6．イベント記録の表示例

(1)　監視カメラの映像をリアルタイムでディジタル化し，圧縮して，連続的に磁気ディスクにエンドレス記録する。必要に応じてネットワークを通して配信する。記録された映像は任意の時点から瞬時に再生・配信できる。再生中も記録は継続できる(エンドレス記録機能)。

(2)　エンドレス記録の時間はディスクの容量に制約されるため，長期保存するものは，こま落としや高圧縮率にして記録し直す(タイムラプス記録)。

(3)　各種センサと連動してイベント発生時前後の映像を自動的に残し，確認再生・配信できる(イベント記録)。

3.3.2　セキュリティシステムの構築

このメディアコントローラを用いた映像監視をアクセスコントロールや侵入検知と融合させることで，以下のような機能を持った信頼性が高く効率的なセキュリティシステムを構築することができる。

(1)　通行記録と映像アラーム

出入管理を行う扉周辺又は認証端末内にカメラとメディアコントローラを設置する。認証端末からのトリガーによって通行者を自動記録し，認証端末の通行履歴や時間と連動して通行者の映像を検索表示する。認証不成功時や照合率が低い場合のみ自動的に監視センターに映像を伝送・表示するため，常時映像をモニタする必要がなくなる。無論，必要に応じて現在の状況をリアルタイムでモニタすることも可能である。

(2)　アラーム発生前後の状況確認

侵入検知センサや人感センサと連動してアラーム発生前後の映像をイベント記録することで，侵入者や不審者の状況を逃すことなくとらえ，確認することができる(図6)。

(3)　簡易画像センシング

画像符号化の際フレーム間の動きベクトル情報を算出するが，この情報を利用して簡易な侵入検知や不審物検出等の画像センシングを低コストで実現する。

4. むすび

ビルや施設を対象としたセキュリティシステムの今後の展開の方向として，当社産業システム研究所において検討を行っているアクセスマネジメントシステムの概念の一端を紹介した。今後，ここで述べたような内容を基に更に検討を重ね，当社のセキュリティシステムに反映させていく所存である。

参考文献

(1)　尾崎　稔，亀山正俊，黒田伸一，塩谷景一，浅野光雄：産業用マルチメディア技術，三菱電機技報，71，No.2，180～183　(1997)

監視カメラシステム

布野健二*
佐藤正弘*

要　旨

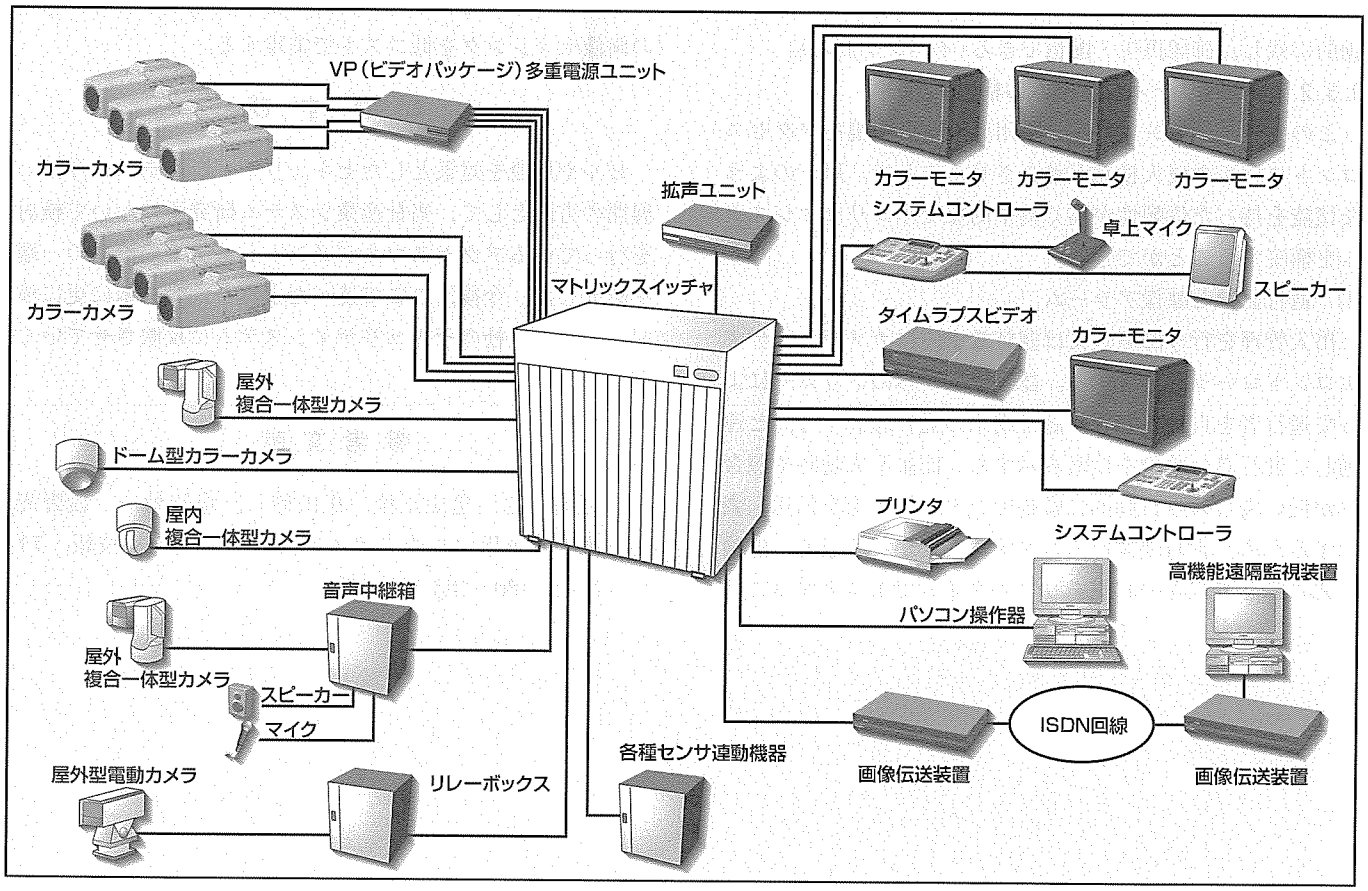
社会的環境の変化により，防犯・防災が強く求められるようになってきた。その中で，監視カメラシステムは，正確な状況判断と迅速な対応によって安全の確保を支援するものとして，重要な役割を果たすようになった。

事務所，ホテル，店舗，アメニティエリア，エレベーター内，駐車場等を持つ，高層化・大型化・複合化されたビル向けの監視カメラシステム市場では，大規模な集中監視システムの要求がある。集中管理センターでの24時間集中監視のほか，サブ管理センター，駐車場管理センターなど目的別・用途別にサブセンターでの監視要求(階層化)があり，監視カメラの増加対応だけでなく，監視箇所(モニタ，システムコントローラ)の複数箇所対応，監視コーデックを使用した遠隔地監視対応(広域化)が必要になってきた。

また，運用者(オペレータ)への負担を軽減するため，マンマシンインタフェース向上，各種警報に連動したセンサ連動機能や監視目的にマッチした映像監視とカメラ制御ができるシーケンス機能などでの監視の省力化が要求されている。

さらに，施工費用の削減要求から，監視カメラの小型・軽量化，ケーブルの省線化，制御装置の小型化が要求されている。特に大規模なシステムでは，監視カメラ-コントローラ間，コントローラ-モニタ間などのケーブル敷設の簡素化が求められている。

これらの多くの要求を満足する監視カメラシステムの核となるマルチポイントCCTVシステムを開発した。



監視カメラシステムの全体イメージ

今後ディジタル回線の普及によって広域化・集約監視化が進むと考えられる監視カメラシステムの全体イメージとして，マルチポイントCCTVシステムを核とし，遠隔での監視も可能としたシステム構成である。

*郡山製作所

1. まえがき

社会的環境の変化により，防犯・防災が強く求められるようになってきた。その中で，セキュリティに対する人手不足及び経費削減の要求による省力化・合理化の要求も増加傾向にあり，監視カメラシステムは，正確な状況判断と迅速な対応によって安全の確保を支援するものとして，重要な役割を果たすようになった。

この監視カメラシステムの最新機種であるマルチポイントCCTVシステムと，システム拡張機器である特殊カメラ，画像伝送装置について紹介する。

2. マルチポイントCCTVシステム

マルチポイントCCTVシステムは，監視用途と規模に応じて柔軟なシステム構築が行え，複数箇所での監視や運用者への負担を軽減するため，各種警報に連動するセンサ連動機能，監視目的に適したカメラ選択・制御を自動で行うシーケンス機能を備えている。

以下に，主な機能と各構成機器の概要を，**図1**に主な構成機器の外観を示す。

2.1 主な機能

(1) 大規模化への対応

増設拡張を容易にするため，システム制御機能を集約したマトリックススイッチャをカード形式のユニット形式としており，最大64台のカメラ入力，16台のモニタ出力を，複数箇所(最大8か所)から操作できる。

(2) 監視の省力化への対応

監視の目的別・用途別に，システムコントローラから画面メニュー設定，監視運用ができる。また，運用者(オペレータ)の負担を軽くするため，複数モニタで同時に複数映像を自動切換え監視するマルチシーケンス機能，単独モニタで自動切換え監視するシングルシーケンス機能を装備し，外部センサ(最大128点)によるセンサ連動機能や，毎日・毎週・毎月・特定日で監視パターンを変えられるスケジュール連動機能などを装備している。

(3) 施工の簡素化への対応

施工性を向上し設置工事費用の削減を目的に，映像・音声・制御・電源を同軸ケーブル1本に重畳したワンライン化により，ケーブルの省線化が図られている。

(4) 高機能化への対応

現場の音による状況確認及び警告放送が可能な集音／拡声(個別，グループ，一斉)機能がある。そのほか，より大規模なシステム(例えば，カメラ128台のシステム)に拡張できるように，RS-232Cの外部制御端子を装備している。

2.2 マトリックススイッチャ

マトリックススイッチャは，前項で説明した機能を実現するため，各機能別のカード形式の構成としている。以下に各カードの機能を，**表1**に主な仕様を示す。

(1) CPUカード

CPUカードは，システム全体の制御を行っており，プリンタ端子からアラームの履歴やシステムのログを出力可

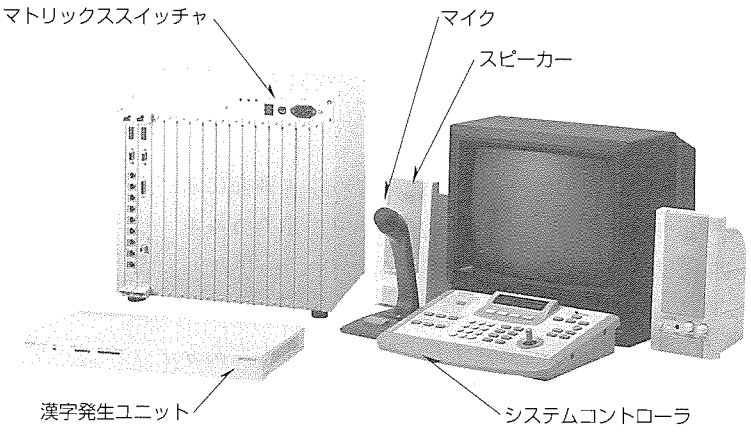


図1．マルチポイントCCTVシステムの主要機器

表1．マトリックススイッチャの仕様

品名／型名	マトリックススイッチャ U-9064	マトリックススイッチャ U-9016
入力カード数	標準装備なし　最大8枚 (合計64入力，8入力／カード)	標準装備なし　最大2枚 (合計16入力，8入力／カード)
出力／4画面カード数	標準装備なし　最大4枚 (4出力／出力カード，1出力／4画面カード)	標準装備なし　最大2枚 (4出力／出力カード，1出力／4画面カード)
センサカード	標準装備なし　1枚実装可能(オプション)	
システムコントローラ	標準装備なし　8台まで接続可能(オプション)	
外部制御	RS-232Cポートによって可能	
時計機能	2010年までのカレンダ内蔵，VTRの時刻補正機能あり	
操作の短縮キー	900件まで登録可能	
シーケンス動作	最大64ステップ×最大64件まで登録可能	
時計による シーケンス動作	48件／曜日のほかに48件／年	
センサによる シーケンス動作	最大128件	
周囲温度	−10〜50℃　20〜80%RH	
電源	AC100V　275VA (270W)	AC100V　140VA (100W)
外形寸法	(W) 480×(H) 399×(D) 300 (mm)	(W) 480×(H) 177×(D) 300 (mm)
質量	約16kg	約11kg

能としている。また，接続するカメラに供給する同期信号を生成している。

(2) 通信カード

システムコントローラと通信し，操作・表示情報をCPUカードに提供している。また，漢字発生ユニットや拡声ユニットのオプション機器と制御情報の通信を行っている。そのほか，パソコンやシーケンサ等と制御情報の通信を行うRS-232C端子がある。

(3) 入力カード

入力カードは，1カード当たり8台のカメラを接続でき，8カードまでの装備が可能で，CPUカードとカメラ間の制御信号を映像信号に重畳・分離する機能と，入力された8チャネルの映像信号を選択し，16チャネルの映像バスに出力する機能がある。

(4) 出力カード

出力カードは，映像バスからの16チャネルの映像信号を選択し，カメラ番号等の文字を映像信号に重畳し，4台のモニタに出力する機能がある。

(5) 4画面カード

4画面カードは，出力カードの機能に含め，1画面に4チャネルの映像を4分割合成する機能があり，出力カードと合わせて4カードまで装備可能である。

(6) センサカード

センサカードは，64点のセンサ入力と32点の出力があり，アラーム入力で指定したモニタに映像を表示する機能，指定したモニタから順番にアラーム映像を表示する機能，外部装置に通知するのみの機能の3モードが選択可能である。

2.3 システムコントローラ

システムコントローラは，マトリックススイッチャの通信カードと接続し，テンキーやジョイスティックで，映像の切換えやカメラの操作を行う操作器である。

操作性の向上のため，通信カードと19.2kbpsの高速で通信を行うとともに，LCD(Liquid Crystal Display)に操作入力状態を表示している。カメラ選択はテンキーを，カメラ回転台操作はジョイスティックを，ズームレンズ操作は押しボタンスイッチを採用し，手軽に素早く操作ができる。プリセット制御もテンキーによって128ポイントまで制御可能である。

そのほか，簡単キーにカメラ番号，モニタ番号，プリセット番号をあらかじめ登録(最大900件まで)しておき，簡単キー＋登録番号(テンキー)の操作で指定の映像が呼び出せる。**表2**に主な仕様を示す。

2.4 カメラ

屋内及び屋外複合一体型カメラ，高感度カラーカメラ，ドーム型カメラ，標準カラーカメラ等の豊富なラインアップがある。**図2**に各カメラの外観を示す。

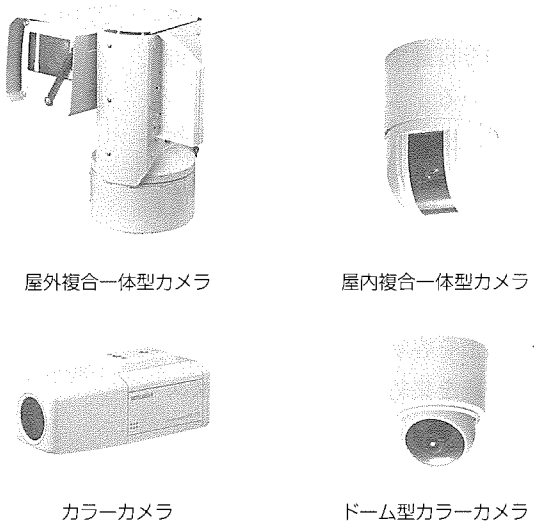


図2．マルチポイントCCTVシステム用カメラ

表2．システムコントローラの仕様

品名／型名	システムコントローラ　R-2300
主な機能	カメラ選択1～64 モニタ選択1～16 カメラ操作：パン，チルト，ズーム，フォーカス，プリセット，ワイパ，デフロスタ シーケンス動作：シングルモニタ，マルチモニタの開始，停止順送り，逆送り 4分割：入／切 (オプションの4画面カードが必要) 拡声：一斉／グループ／個別 (オプションの拡声ユニットが必要) 文字タイトル：英数カナ(標準) プリセット：128件／カメラまで操作可能 短縮(簡単)キー：900件まで登録可能 外部機器制御：2系統のON／OFF可能
音声機能	標準装備なし　オプション音声基板が必要
周囲温度	－10～50℃　20～80%RH
電源	AC100V　10VA(5W)
外形寸法	(W)336×(H)77×(D)240(mm)
質量	約3.0kg

表3．複合一体型カメラの仕様

品名／型名	複合一体型　CIT-701 (屋外，据置用)	複合一体型　CIT-751 (屋内用)
レンズ	f：8～80mm(F1.2)	f：5.8～58mm(F1.8)
撮像素子	1／2インチCCD	1／3インチCCD
解像度	水平：460本，垂直：350本	
最低被写体照度	2 lx(1／60秒)， 0.06 lx(電子増感32倍時)	3 lx(1／60秒)， 0.1 lx(電子増感32倍時)
旋回角度	水平：±175° 垂直：+20°～－60°	水平：±175° 垂直：0°～－90°
プリセット 最大旋回速度	水平：180°／秒， 垂直：60°／秒	水平：90°／秒， 垂直：45°／秒
動作周囲温度， 防水性，湿度	－20～40℃ (連続通電)	0～40℃ ただし，結露しないこと
電源	AC100V	
外形寸法	約(W)378×(H)402 ×(D)310(mm)	φ180×(H)250(mm)
質量	約16kg	約3kg

表4．カラーカメラの仕様

品名／型名	カラーカメラ CIT-731	カラーカメラ CIT-733	カラーカメラ CIT-761	カラーカメラ CIT-763	ドーム型カラーカメラ CIT-781	ドーム型カラーカメラ CIT-781
レンズ	別売り（固定焦点，f：8.4，2.8mm）				焦点距離2.6～5.6mm バリフォーカル 下値 F2～2.7	
撮像素子	1／3インチCCD					
解像度	水平：480本，垂直：350本					
最低被写体照度	1 lx(F1.4 1／60秒)	1 lx (F1.4 1／60秒) 0.06 lx (電子増感32倍時)	1 lx(F1.4 1／60秒)	1 lx (F1.4 1／60秒) 0.06 lx (電子増感32倍時)	2 lx (F2.0 1／60秒)	
S／N	50dB					
周囲環境	−10～50℃ 20～80%RH以下（ただし，結露しないこと）				−10～40℃	
電源	AC100V		VP多重電源ユニットから供給		AC100V	VP多重
外形寸法	約（W）70×（H）60×（D）164（mm）（レンズカバー含む）				φ120×（H）130（mm）	
質量	約0.6kg				約0.7kg	

表5．画像伝送装置の仕様

型名	MVC-8800A	MVC-1180	BC-4100
適用回線	INS64，B／2×B INS1500	INS64，B／2×B I.430	専用線（G.703-a） 6.312Mbps
画像符号化方式	H.261（CIF，QCIF）		MPEG2（MP@ML，SP@LL，MP@LL）
伝送フレーム枚数	最大15フレーム／秒 384kbps回線時	最大15フレーム／秒	30フレーム／秒
映像入出力	NTSCコンポジット信号（1.0$V_{p\text{-}p}$／75Ω）		
音声入出力	−9 dBm／600Ω 平衡	−9 dBm／600Ω 不平衡	0 dBm／600Ω 平衡
制御入出力	RS-232C 1.2／4.8／9.6kbps	センサ入力：8点 カメラ選択：8点 制御入出力：8点 拡張入出力：8点	RS-449 64kbps同期 RS-232C 1.2／2.4／4.8／9.6／19.2kbps 制御入出力：8点
使用環境	5～35℃ 45～85%RH	0～40℃ 40～85%RH	5～35℃ 45～85%RH
電源	AC100V 約78VA	AC100V 最大30W以下	AC100V±10% DC-48V（+5，−6V）
外形寸法	（W）350×（H）105×（D）306（mm）	（W）430×（H）44×（D）280（mm）	（W）430×（H）177×（D）420（mm）
質量	約10kg	約6kg	20kg以下

2.4.1 複合一体型カメラ（屋内・屋外）

複合一体型カメラは，カメラケース，ズームレンズ，回転台，高感度カメラがコンパクトに一体化したカメラで，以下に特長を，表3に主な仕様を示す。

(1) プリセット高速旋回

マイコンでカメラを上下左右に旋回させるパルスモータを2台制御し，あらかじめ設定登録されたプリセット位置（最大128か所）へ高速旋回を可能としている。

(2) 電子感度アップ

電子的にCCD（Charge-Coupled Device）固体撮像素子で一定時間光を蓄積することで，最大32倍の電子感度アップ機能を実現している。

(3) 映像・制御信号を同軸ケーブル1本で伝送

ケーブルの省線化によって取付工事を簡素化するため，映像信号の垂直ブランキング期間に，コントローラ側から5バイト，カメラ側から5バイトの計10バイトのカメラ制御信号を重畳させ，同軸ケーブル1本で伝送可能としている。

(4) ワンタッチオートフォーカス

10倍ズームレンズの採用による広範囲の監視と，パッシブ方式の一種である映像信号中に含まれる高域成分の量を最大とするように制御する山登りサーボ方式を採用したオートフォーカス機能により，煩わしいピント合わせを軽減させている。

2.4.2 カラーカメラ

カラーカメラは，電源がAC100V入力タイプに加え，同軸ケーブルにカメラ電源を多重するVP多重タイプ，電子感度アップ機能の付いた高感度タイプ，監視カメラを意識させないドーム型タイプがある。表4にカラーカメラの仕様一覧を示す。

2.5 周辺機器

周辺機器の充実も図られ，漢字発生ユニットは，マトリックススイッチャに接続することで，カメラ地点名の漢字文字表示切換えができる。また，リレーボックスは，ボイラ室，電源室，危険物管理エリア等に使用する豊富な機種のある耐環境性カメラ装置や，夜間の侵入監視や火災検知等に使用する赤外線カメラ等の特殊カメラの接続を可能としている。

そのほか，選択カメラの設置位置，カメラ切換え操作ボタン，カメラ制御ボタン等をパソコン画面上に分かりやすく表示しビジュアルな操作を提供するパソコン操作器がある。

表6．赤外線カメラの仕様

項　目	三菱電機製		
	IR-M300	IR-M600	IR-M700
赤外線検出器	PtSi (IRCSD)	PtSi (IRCSD)	PtSi (IRCSD)
画素数	256×256	512×512	801×512
検知波長	3～5 μm		
レンズ	赤外線レンズ 125mm F2.0	赤外線レンズ 150mm F1.2	赤外線レンズ 150mm F1.2
雑音等価温度差 (NETD)	0.2℃	0.08℃	0.08℃
視野角	(H)14°×(V)11°		
フィールドタイム	1／60秒		
冷却方式 平均寿命(MTTF)	スターリングサイクルクーラー		
	8,000時間	8,000時間	4,000時間
映像出力	RS-170		
環境条件	−10～50℃　96%RH以下		
入力電源	AC100V	AC100V DC24V	AC100V DC24V
カメラ内蔵フィルタ切換え	内蔵 フィルタ4枚	なし	内蔵 フィルタ2枚

3. 拡張機器

カメラで撮像した画像を遠距離で監視するための画像伝送装置と，特殊用途用カメラについて紹介する。

3.1 画像伝送装置

マルチポイントCCTVシステムは，カメラとマトリックススイッチャ間の距離が同軸ケーブル(5C-2V)で約1.2kmまで延ばすことが可能であるが，この監視カメラシステムの設置場所以外の遠隔地から監視を行う場合，工事費や回線費用の削減から，映像信号を符号化しディジタル回線で伝送する画像伝送装置を使用する場合が多い。

画像伝送装置は，画像信号を高能率符号化によって圧縮し，他の音声やデータと多重して伝送する装置で，H.261，MPEG1，MPEG2等の符号化方式によって大別される。**表5**に画像伝送装置の主な仕様を示す。

3.2 特殊用途カメラ

特殊用途カメラの一つとして，セキュリティ分野で夜間における侵入監視用途や火災検知等に使用される赤外線カメラを紹介する。

赤外線カメラは，高速船の夜間前方監視，養殖漁場の密漁船監視，重要施設の不法侵入者監視，ヘリコプター搭載の防災・火災監視，消防用高所監視等に使用されている。**表6**に赤外線カメラの仕様を示す。

4. むすび

ビルなどの監視においては，従来の単品を使用した簡易システムから，監視のニーズに応じて選択するパッケージシステムへと展開を見せており，高機能化・大規模システム化・低価格化の傾向が強まる。

また，CATV技術を利用したRF-AVネット，又は画像伝送装置を使用したディジタルAVネット等により，広域化・集約監視化が進むと予想される。

今後，社会的なインフラの整備・拡充に伴い，映像／通信／コンピュータを融合した大きなシステムになっていくものと確信する。

参考文献

(1) 佐藤正弘，栗原裕司：監視カメラ・システムの技術動向，セキュリティ産業年鑑'97

(2) 柳本重治：高画質赤外線カメラによる火災検知システム，建築防災　(1997-1)

誤報を低減した侵入監視装置

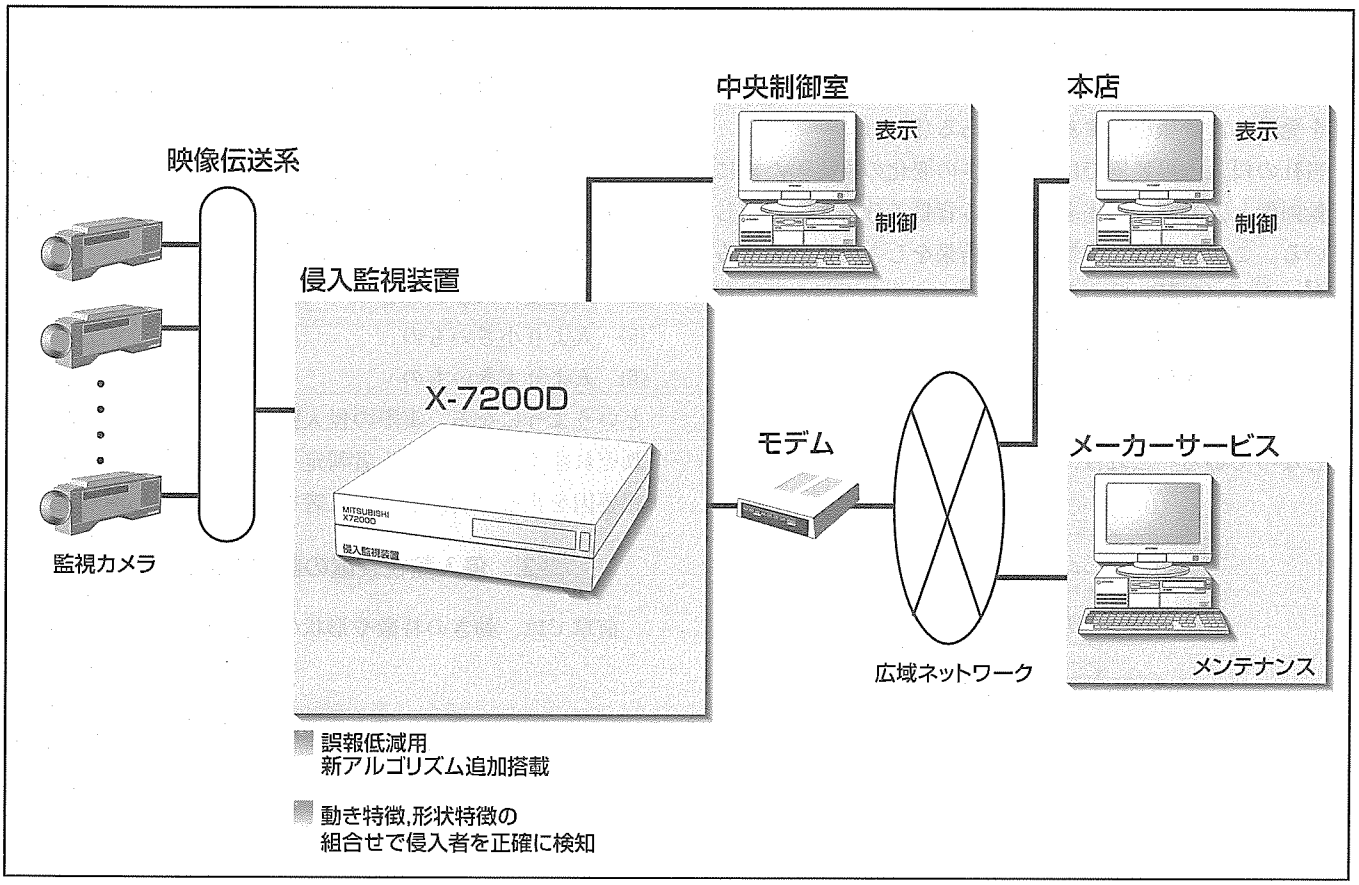
関　明伸*　新房健一***
橋本　学*
鷲見和彦**

要　旨

誤報の少ない連続監視を実現する侵入監視装置を開発した。この装置は，監視員に代わって，監視カメラ映像にとらえられた物体の動きの特徴と形状の特徴から侵入者を判断して警報を発し，監視員にかかる肉体的・精神的負担を大幅に軽減するものである。

この装置は，画像処理によって監視カメラ映像の変化を自動的に検出するもので，その基本アルゴリズムとなる背景差分処理が正確な特徴量抽出を可能とすることから，屋内外の別を問わず，また昼夜兼行で，安定した信頼性の高い侵入者監視を実現している。しかし，ごくまれに，極めて短時間の明るさの変動を伴う事象，例えば監視範囲外からの一瞬の車両によるライトの照射，を誤認識してしまうことがあった。このような事象は通常時には予見が困難なため，現象が生じて始めて再調整が必要であることが判明する。

今般新しく開発した侵入監視装置X-7200Dは，このような急激な明るさ変動に対しても安定した動作を保証する新規アルゴリズムを追加した。これにより，従来まれに誤報の原因となっていた事象の90%を無視することが可能になった。さらに，監視システムに，より柔軟な発展性を提供する16ポジション対応機能やモデムを介した遠隔からの監視制御やサポート機能を搭載し，これまで以上にユーザーの広範なニーズにこたえられる製品となっている。



侵入監視装置X-7200Dを中心とした監視システム

監視カメラで取得された監視映像は，映像伝送系を通じて侵入監視装置X-7200Dへ入力される。侵入監視装置は，中央制御室の制御卓で，各種の設定，動作状況の確認が行える。一方，モデムを介した接続によって遠隔地においても監視状況のモニタができるほか，リモートメンテナンスの機能によって監視装置を常に最高性能に維持することができる。

*産業システム研究所　**同研究所（工博）　***郡山製作所

1. まえがき

従来から行われてきた重要プラントや施設における監視員による不審者発見のための常時監視を自動化する目的に，侵入監視装置が使われている。この装置は，監視カメラを画像センサとして利用して連続自動監視を実現するものであり，監視業務に携わる監視員の肉体的負担を大きく軽減することができる。

ところで，機械による侵入者の監視は検出能力を常に一定に保つことが可能になる反面，人間の監視員であれば容易に判断可能な画像の変動でも誤って侵入者であるとの警報を発することがある。この問題について，当社は，これまで侵入者の動きの特徴や形状の特徴を利用して侵入者検出の信頼性を高めた侵入監視装置を製品化してきた。

本稿では，これら高信頼化手法では排除しきれないまれに発生する誤報の分析と要因，及びその対策方法について述べる。また，この方策を取り入れて新規に開発した侵入監視装置X-7200Dについて紹介する。

2. 画像処理型侵入監視装置

画像処理型の侵入監視装置は，監視カメラ映像を連続したディジタル画像データとして取得しながら時間的な明るさの変化を検出し，この変化を映像中の移動物体による変化と解釈することを基本とするアルゴリズムによって侵入者を発見し，警報を発するものである(**図1**)。

当社の侵入監視装置では，明るさの変化の検出のために，背景画像と入力画像の差を利用する背景差分方式を採用している。この方式は，背景差分の結果をしきい値処理することによって移動物体のきれいなシルエットが得られる利点があり，特徴抽出で正確な結果を得やすい。また，アルゴリズムの前半部分のラベリングまでは主にハードウェアで処理し，特徴抽出以降の後半部分はソフトウェアでの処理となっている。これは，動画像処理に際し，画像中で変化している部分をすべて検出するという処理時間に余裕のない部分をハードウェア化しリアルタイムの処理を実現すると同時に，外部システムとの情報交換の必要な部分をソフトウェアでの処理とすることで，より柔軟なシステム構成を目指した結果である。

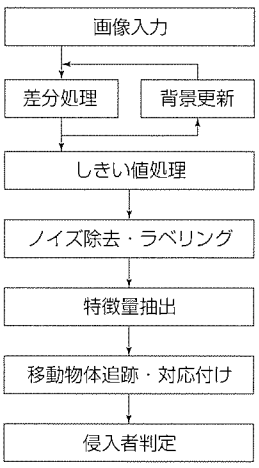


図1. 処理の流れ

この侵入監視アルゴリズムが背景差分処理を基本としているため，恒常的に動いているものが監視範囲内に含まれていると，それらを侵入者として誤って処理し，誤報の原因となることがあった。そこで，従来の高信頼型侵入監視装置では，動きの特徴や形状の特徴を併用して侵入者の検出精度の向上を図っている。例えば，動き特徴を用いることによって，フェンスをよじ登るような人には直ちに警報を発するが道に沿って移動している人は警報を発しないとか，形状の特徴を用いることによって，無人施設内に人がいたら警報を発するが小鳥が飛来しただけでは警報を発しないというようにしている。

主要な警報要因とそれらの特徴について**表1**に示す。

動きの特徴は，警戒領域に侵入する方向へわざわざ入り込むなどの，いわゆる意図的な動きを始め以下の3種類に大別できる。

(1) 意図的な動きをするもの
(2) ほとんど移動しないもの
(3) 上記以外の動きをするもの

このうち警報の対象になるのは，(1)の意図的な動きをするものである。

一方，形状の特徴については，警報の対象になる侵入者が不定形状であることから分類をすると，大きさ別に3段階程度に分けるのがよく，

(4) 人程度の大きさのもの
(5) 人より小さいもの
(6) 人より大きいもの

というようになる。実際の侵入監視装置では，これらをそれぞれ組み合わせて侵入者判定を行うため，ほとんどの警報要因を正確に判断して侵入者を検出することができた。

3. 侵入監視装置の誤報要因の分析

前章では，動きの特徴や形状の特徴を利用した侵入監視

表1. 主な警報要因と特徴

警報要因	動きの特徴	形状の特徴
侵入者	意図的な動き	形状不定 1～2mの高さ
木の枝葉	同じ場所で動かず	風の状況による
小動物	素早く通過	小さい
紙くずなど	風に吹かれるまま	一般的に小さい
日照	ほぼ静止	壁等が一様に変化
水面	同じ場所で動かず	予測不可能
外来光	光源の移動に同期	比較的大きい

装置の高信頼化の技術について述べた。ただし，見落とし(不検知)を最小限にすることと誤報(不要検知)が出ないようにすることを一度に満足することは容易ではなく，まれにではあるが，特定の条件下で依然として誤報となる例が発見された。

例えば，予想外に速い雲の移動による日照変化を誤検出した。照り陰りは後述の背景更新処理で吸収されるような仕組みになっているが，台風直後の雲の動きによる照り陰りによって壁面が誤検出されたものと判断された。白い壁面で反射率が高かったことが原因の一つと思われた。

また例えば，夜間，監視範囲に隣接して存在している道路を通行する車両のヘッドライトからの光線の差し込みを誤検出した。もともと監視範囲に道路が存在していないため装置のセットアップの段階で誤報の可能性を予見しにくく，また，夜間しか発生しないなどの条件が重なって，十分な監視パラメータの調整が行えていなかった。さらに，差し込みの状況によっては，建物の壁面に沿って人物大の明るい部分が移動していくという状況が発生し，誤報を引き起こすことも分かった。

自然現象やこれに類する事象を原因とする誤報については，ほとんどの場合センサである監視カメラの設置位置や角度，画角を見直すことで対処可能であるが，通常，監視員のためのカメラとして設置されているものの場合，このような対応には限界があり，侵入監視装置側での新たな対応策が必要である。

4. 誤報対策のための画像処理アルゴリズム

従来のアルゴリズムで対処が難しく，しかも発生頻度の面からも無視できない誤報の原因としては，前記のものを含めて以下のようなものがある。

(1) 日照の照り陰りの特に急激なもの
(2) 車両のヘッドライトの監視範囲への差し込み
(3) 水たまりの乱反射

これら誤報要因に対して，従来のアルゴリズムでは，いったん監視動作を中断するか，又は動作を継続しても検出結果を無視するか，いずれかの対処方法を採用していた。誤報としては，監視時間全体から見たときの発生割合が特に多いというわけではないが，特定の気象条件や時間に限定的に発生する種類の誤報であるために，監視する側にとっては目立つ種類の誤報である。

そこで，これらの誤報を排除又は低減することを目的とした処理について検討した。上記はいずれも，具体的な何かがその場所に存在しそれが検出されることによって必要のない警報が出されるのではなく，カメラ映像を画像として見たときに，ある部分の明るさが直接的に変化したことを誤認識する類の誤報であることが分かる。

したがって，明るさの変動に対応するための処理を強化してこの問題に対処する必要がある。

侵入監視アルゴリズムが背景差分処理ベースのものであることは前に述べた。この方式で明るさの変動に対応するためには，背景画像を合成する段階で，移動物体による変化以外の明るさ変動を吸収すればよいことが分かる。**図1**の処理の流れの中で，背景更新と呼ばれる処理の部分がこの動作の中心となる。従来のアルゴリズムでは，時刻Tの入力画像$I(T)$に対して背景画像$B(T)$を次のような式に従って合成している。

$$B(T)=B(T-1)+\alpha\,(I(T)-B(T-1))$$

ここで関数αは，**図2**に示すような特性を持つ。図のεは，暗雑音と呼ばれる微小なレベルの輝度のふらつきを吸収するように定められ，通常3～5程度の値が選ばれる。また，δは，処理ごとの背景の明るさの変化に対する追従量を決定するもので，この値の大小によって明るさ変動への追従能力が変化する。

ここで例えば，$\varepsilon=\delta=0$とすると，背景画像は全く更新されなくなり，背景固定型の差分処理となる。また，$\varepsilon=255$とすると，背景画像は入力画像で置き換えられる形となる。これは，フレーム間差分と同様の動作であり，結局，背景更新という考え方の下では背景差分方式はフレーム間差分方式も含む広い概念であることが分かる。

ところで，前述の誤報要因はいずれも，輝度変化の継続時間が短く，フレーム間差分方式のような追従性が高い背景更新方法の下では明確な動きの特徴が抽出されにくくなる。その結果，後の侵入者判定の段階でノイズとして処理され，誤報として検出されることは回避される。このように背景更新処理における設定パラメータを動的に制御すれば，より信頼性の高い監視アルゴリズムが構成できる。

5. 侵入監視装置X-7200D

これまでに述べたような処理をベースに，誤報に対する判定能力を強化したX-7200Dを開発した。外観を**図3**に，主な仕様を**表2**に示す。

この機種では，映像入力数を4チャネルから1チャネルにしたほかは，すべての機能を前機種から引き継ぎ，その上で誤報対策の強化として，前に述べた背景更新の追従性能の切換えを動的に実行できるような機能を実装している。

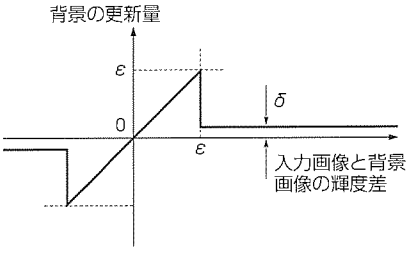


図2. 関数αの特性

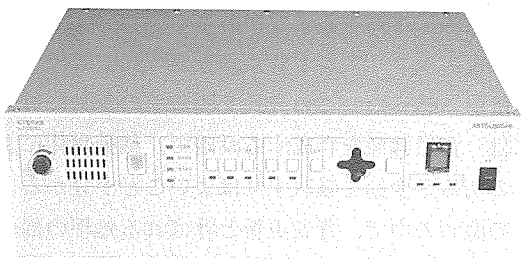


図3．X-7200Dの外観

シミュレーションによれば，これまで誤報となってきたシーンの90%以上を正確にノイズとして排除することが可能になっている。また，これら誤報に対する判定能力の強化以外にも，ユーザーフレンドリなGUIを採用したパラメータ設定機能や電話回線を利用するリモートメンテナンス機能などを持ち，従来以上に広範囲なユーザーニーズにこたえられるハードウェアとなっている。

さらに，画像入力部の直後に設けられたオプションソケットに種々の設備監視用オプションカードを実装し，発煙検出，油漏れ検出，変色検出などの機能を実現したX-7210Dをシリーズ機種として用意し，一層の監視業務の省力化を実現している。

ところで，侵入監視装置による画像監視の能力を人間の監視員のレベルにまで高めるには，全く同一の映像であっても状況に応じて異なった判断をさせる必要があるなど，まだ課題が多い。しかし，これらのほとんどは，これまでに得られた，又はこれから得られる誤報事例を詳細に解析することによって対応策を得ることが可能であると思われる。これからの侵入監視装置は，高い信頼性を備えると同時に，未知の事象にも後から対処できるような柔軟性(例えば，X-7200Dの持つリモートメンテナンス機能など)と操作性も含めた使いやすさが重要になる。

6. むすび

画像処理を用いた高信頼型侵入監視装置において，従来まれに誤報を発する状況を分析して，侵入監視装置の明るさ変動に対応する能力を強化することで大部分が対処可能になることを述べた。

表2．X-7200Dの仕様

項　目	仕　様
映像入力	NTSCコンポジット1チャネル
映像出力	2系統(スルー，エディット各1)
解像度	512画素×480ライン 輝度信号，色信号とも8ビット／画素
特徴データ	面積，縦横寸法／比，移動方向／速度
処理領域	1画面中に最大4か所 それぞれ独立に発報条件設定可能
マスク機能	画面中の監視不要領域をマスク可能
履歴画面	発報前後を任意間隔で9画面
通信機能	一般電話回線による接続可能 ファームウェアの改版，パラメータ調整が可能
使用電源	AC100V±10V
消費電力	200W
外形寸法	(W)424×(D)300×(H)135(mm)
質　量	20kg以下
その他	各種設定のためのGUI装備 プリセット回転台対応

この新規に開発したアルゴリズムを搭載したX-7200Dは，誤報に対する判定能力が大幅に強化され，侵入監視装置をより多くのユーザーの広範囲な要求にも耐え得るものになった。今後は，設備監視用のシリーズ機X-7210Dとともに，重要施設，大規模プラント，一般工場等への導入が積極的に進められていくものと思われる。

参考文献

(1) 関　明伸，黒田伸一：動き情報を用いた高信頼型侵入監視装置，三菱電機技報，**67**，No.7，670～674 (1993)

(2) 新房健一，新谷育夫，土屋徳翁：電力設備映像監視システム，**70**，No.4，70～76 (1996)

統合ビルセキュリティシステム

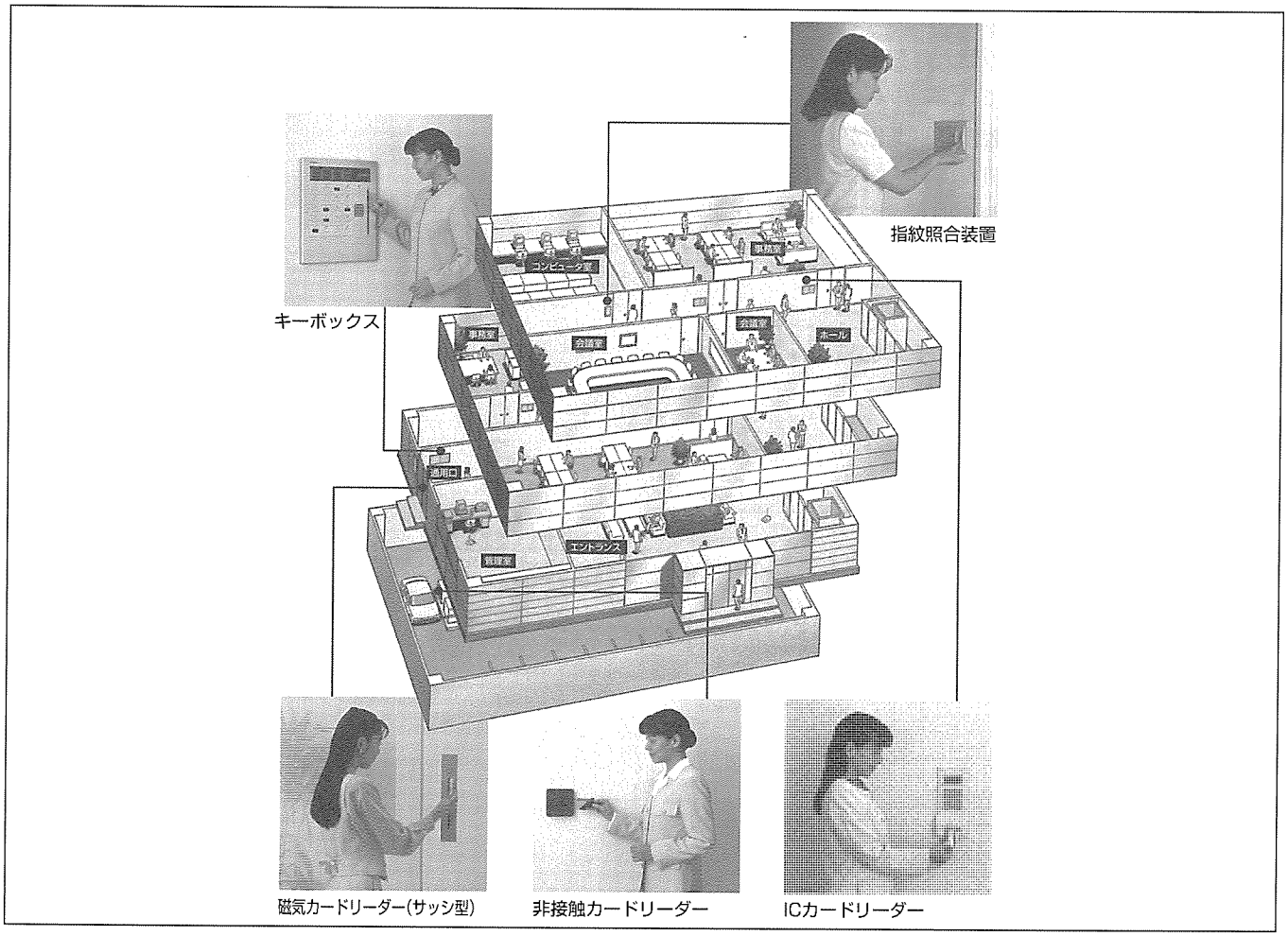
山田邦雄*
曽我部秀史*

要　旨

自社ビル・複合ビルなど建物の用途を問わず，近年，ビル内におけるセキュリティシステムや出入管理システム(Access Control System：ACS)は急速に関心を集めており，エネルギー効率の向上を目指すビル管理システム(Building Automation System：BAS)とともに，ビルの効率・安全運用を行うために必要なシステムとして導入が増加している。三菱電機においても，MELSAFETYシリーズを前者ACSとして，またMELBASシリーズを後者BASとして市場に投入しており，数多くの実績を積み重ねている。ここでは，ビル内セキュリティの概要とACSとBAS機能を統合し，1998年度市場投入する新製品である統合ビルセキュリティシステムについて述べる。

統合ビルセキュリティシステムの特長は次のとおりである。

- ビル管理(BAS)機能の包含
- 昇降機監視機能の包含
- ヒューマンインタフェースにパソコンを導入
- Windows NTベースのソフトウェア
- ネットワーク機能の強化(インターネットへの対応)
- 個人識別端末(カードリーダー，指紋照合装置)の充実
- システム操作権限(ログイン認証)手段の充実



ビルセキュリティシステム

ビル内各区域のセキュリティレベルに適した個人識別端末を設置することで人の出入管理や不正通行防止に効果的に働く。また，出入に連動し，エレベーターサービス階カットや，照明・空調などのビル内諸設備と有機的にリンクしてビルの効率運用を支援する。

*稲沢製作所

1. まえがき

建築物内におけるセキュリティは，従来の金銭や貴金属等の財産を保護する目的のみならず，企業・個人にとっての情報の経済的・戦略的価値を保護するための手段としてその重要性がますます高まっており，ビルセキュリティシステムとして多くの建築物に導入されている。

ビルセキュリティシステムは，不審者の早期発見や犯罪行為の早期発見及び不正通行防止のための防犯設備としての性格と，ビル設備管理とのリンクによるビルの効率的運用や勤務者の快適なオフィス生活を支援するシステムの二つの性格を持っている。特に勤務者などの人の出入管理を行うことに欠かすことのできない個人識別手段は，近年様々に発展している。

従来，ACSにおける個人識別手段は，ID(Identity)カードと呼ばれ特に磁気ストライプ式のIDカード(JISⅡ型等の磁気カード)を利用したものが中心であった。このほかに，IDカードには，ICチップを内蔵した記憶容量の大きなICカードや，操作性・耐環境性に優れる非接触カードなどの多様なカードがACSに使用されている。また，指紋・掌形・こう(虹)彩などの個人の身体特徴を識別する手法も注目されており，当社では，この身体特徴識別手法で高い精度を実現でき，また装置の小型化が可能な指紋照合装置の開発にいち早く取り組んでおり，実績を積んでいる。

本稿では，これらの個人識別端末を適用し，従来のBAS機能も取り込んだ統合ビルセキュリティシステムについて紹介する。

2. ビル内セキュリティの概念

2.1 ゾーニング

ビル内の防犯区域(Zoning)の考え方について述べる。

ビルの防犯区域は，施設対象に応じ，図1のように大きく分けて四つに分割される。

レベルA：電子計算機室，金庫室，通信設備など機密を要する重要区域

レベルB：事務室，店舗など特定の従事者が出入りする専用部

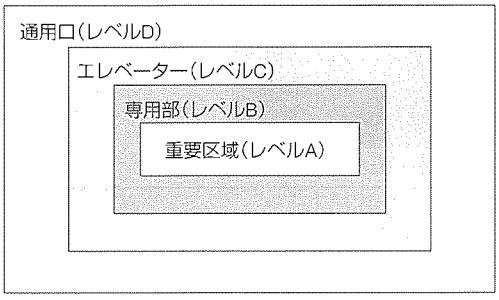
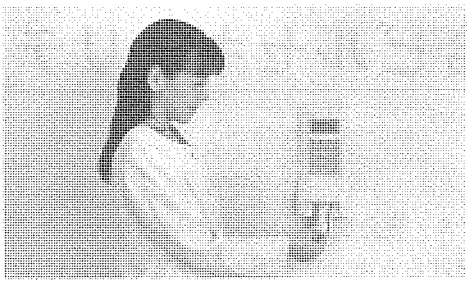


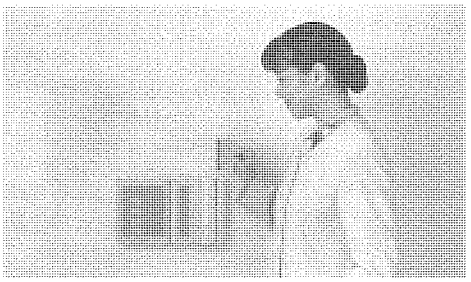
図1． 防犯区域

レベルC：エレベーター

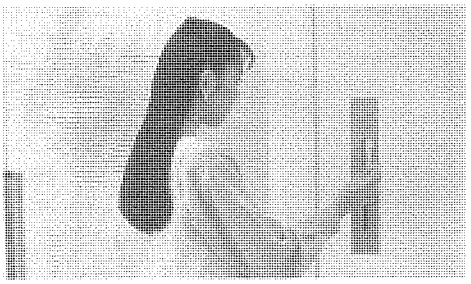


(a)

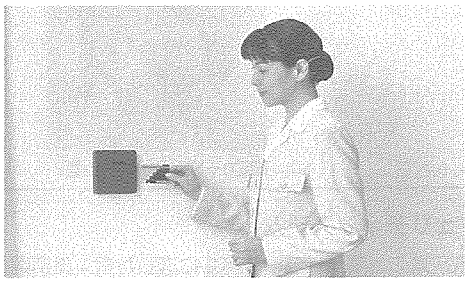
(b)



(c)



(d)



(e)

図2． 各種のカードリーダー

レベルD：出入口，通用口，共用部などの区域

分割された防犯区域の通行ゲートには，それぞれ重要度(セキュリティレベル)に応じ，各々，個人識別端末を設置し，不正通行等を防止することとなる。

2.2 個人識別端末

ACSに必要不可欠な個人識別端末について述べる。

通行ゲートなどにおける通行許可の識別手段としては，

(1) 個人記憶情報識別

(2) 個人携帯情報識別

(3) バイオメトリックス(Biometrics：身体的特徴識別)

が存在する。

上記(1)では，テンキー装置をゲートに設置し，暗証番号(PIN)を入力し，ゲートのロックを解除する，(2)では，カードリーダーを設置し，カード(IDカード)情報を登録情報と照合する，(3)は，個人の身体的特徴を照合する方式であり，指紋(Fingerprint)による識別が近年数多く製品化されており，声紋・掌形・網膜・虹彩なども特定分野で利用されている。

この中で，(2)のIDカードによる識別方式は，現在も主流であり，また，近年のカード社会を反映し，その種類も多様化している。今後も，電子マネー，IC式健康保険証カード，免許証のカード化など，カードの利用がますます増大し，さらに，ICカード(外部端子付き及びコンタクトレス)の国際標準化が進むことで，カードリーダーも発展を続けると予想される。**図2**に各種のカードリーダーを示す。

また，IDカードの種類とその特徴を**表1**に示す。

上記(1)の装置として，当社は，指紋照合装置を'96年1月から発売しており，多数の納入実績を誇っている(**図3**)。また，個人識別装置を用い，通行ゲートのかぎ(鍵)の保管・貸出しを自動で行うキーボックスについても，当社MELBAS／MELSAFETY／MELSENTRYシリーズにおいてシステム化を行っている(**図4**)。

表1．IDカードの種類と特徴

カード種類	セキュリティ性	特　徴
磁気カード	低い	汚れに弱い・安価
ICカード (外部端子付き)	高い	情報量大
非接触カード (コンタクトレス)	高い	耐久性あり

2.3 侵入監視手段

建屋内外の不審者の監視は，各種侵入センサによる検出や，CCTVシステムよるセンターでの監視などによって行う。

この中で，CCTVシステムによる映像監視は，エレベーターかご室内への設置等，最も確実な判断・記録手段として欠かせないものとなっている。

3. 統合ビルセキュリティシステム

3.1 システムの概要

統合ビルセキュリティシステムの特長として下記が挙げられる。

(1) BAS機能(昇降機設備との連動を含む。)及びACS機能の統合

(2) 豊富な個人識別端末の接続

(3) パソコン使用のヒューマンインタフェースプロセッサ

3.2 システムアーキテクチャ

統合ビルセキュリティシステムと現行BAS(MELBAS-A1000EX)及びACS(MELSAFETY-C100)の統合を目指し，以下の機器構成とした。

(1) ヒューマンインタフェースとして，両システムで使用中のエンジニアリングワークステーションの操作性に加え，親和性の向上，周辺機器の充実，機器コストの低減をねらい，パソコンを適用した。

(2) 同様に，ヒューマンインタフェースのオペレーティングシステムとして，MS-Windows NT(以下"NT"という。)を採用した。これにより，多くの市販パッケージソフトウェアの効果的な活用ができる。また，NT標準搭載のTCP／IPプロトコルによるネットワーク構成で，ビル内OA-LANと接続し，データベースの共有化(オープン化)

図3．指紋照合装置

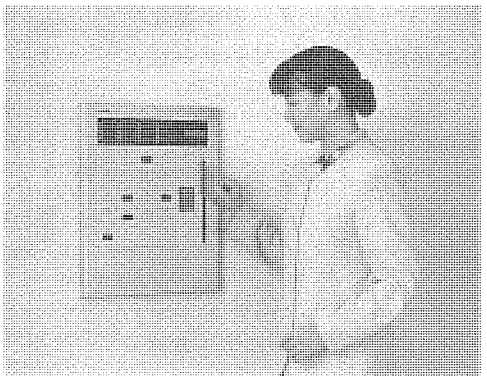


図4．キーボックス

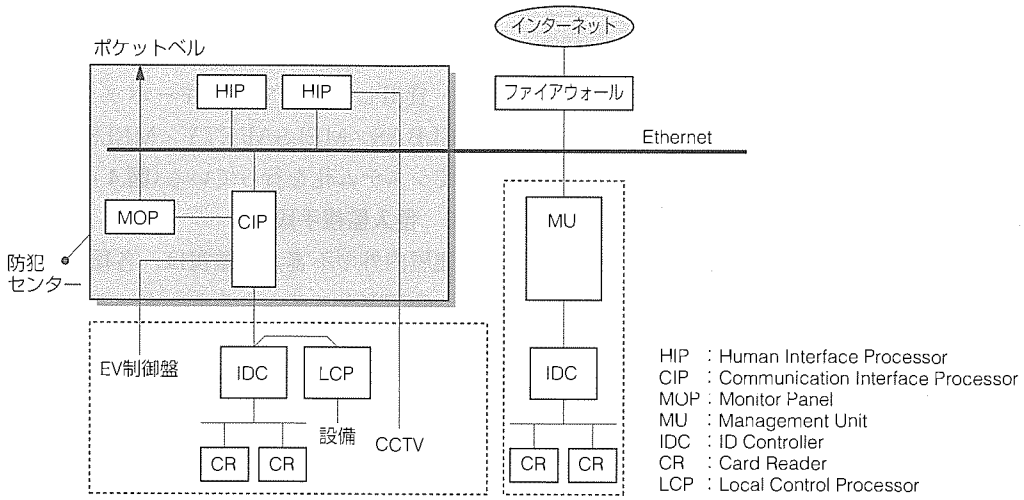


図5．統合ビルセキュリティシステムの構成

を実現するとともに，NTのデータセキュリティ機能を最大限に利用できる。

(3) ローカル装置としては，MELBAS／MELSAFETYで多くの実績を誇る入出力装置と個人識別制御装置を流用し改良した。

(4) 個人識別端末としては，磁気カードリーダー，非接触カードリーダーに加え，新規開発品である新型指紋照合装置と薄型ICカードリーダーを適用可能とした。

図5に，統合ビルセキュリティシステムのシステム構成を示す。

3.3 機　能

統合ビルセキュリティシステムの機能一覧を**表2**に示す。

3.4 個人識別端末

磁気カードリーダー，非接触カードリーダー，鍵管理装置のほかに，指紋照合装置の一層の低コスト化・小型化と性能向上を目指した新型指紋照合装置，及びICカードリーダーの小型化を実現した薄型ICカードリーダーを用意した。

(1) 新型指紋照合装置

登録された指紋データと採取指紋画像を照合する。

偽造が困難な点でセキュリティ性の高い場所に適しており，煩雑なIDカードの発行管理から運用管理者を解放した点で，様々な分野での適用が予想される。また，システムアクセス時

表2．統合ビルセキュリティシステムの機能(1)

	機能項目		機能概要
共通機能	警報監視		侵入警報，火災警報，各機器・システムの異常警報を監視する。
	状態監視		機器・システムの運転状態，部屋の状態を監視する。
	警報ごとのパターン設定		警報ごとに8種類の警報パターンが設定でき，パターンにより，ブザー鳴動有無などが設定できる。
	遠隔制御操作(個別・グループ)		扉の施解錠，機器の起動／停止，警備や通行モードの切換えを個別又はグループごとに制御できる。
	発停失敗監視		制御出力の所定時間以内に状態が制御出力と一致しない場合，警報とする。
	不一致監視		制御出力から所定時間経過後，常時不一致を監視し続け，状態が制御出力と不一致になった場合，警報とする。
	グループ設定		複数の扉や機器をまとめて一つのグループとして設定でき，そのグループを各種機能で制御するよう設定できる。
	スケジュール制御		予約された時刻パターンに基づき扉の連続施解錠，警備切換えができる。当日から7日間有効な臨時変更が可能。
	警備連動制御		警備の入／切に連動して照明や空調の制御を行う。
	火災連動制御		火災発生時に，その警戒区画に関連した区画の非常解錠制御や空調機器等の停止制御を行う。
	グラフィック表示		グラフィック画面での監視・制御ができる。
アクセスコントロール機能	通行制御		
		キーレス	カードを鍵として使用し，扉の連続施錠／解錠を行う。
		防犯キーレス	上記キーレス機能に加え，施錠中は侵入監視を行う。
		アクセスコントロール	常時施錠され，カード操作時のみ一時解錠する。
	キーボックス		ビルの玄関などにキーボックスを設置し，テナントなどの鍵を管理する。
	通行可能な扉と時間帯の設定		個人ごとに通行可能な扉と時間帯の組合せを設定できる。
	IDカードの発行・登録		カードの登録・抹消・発行を行う。
	事故カード処理		カードの紛失・盗難等に伴う無効処理を行う。
	IDCの入出力信号による制御		IDCへの外部信号入力により，設定した扉を一時／連続施解錠切換え，警備切換え，通行モード切換えを行う。
	会議室予約管理		会議室予約管理システムから設定された情報を基に，該当会議室への入退室を管理する。
	巡回監視		管理要員の巡回監視を行う。
	巡回履歴		管理要員の巡回履歴を表示・印字する。
	他のシステムカードの共用		他のシステムで書かれたカードにこのシステムのデータを上書きすることにより，そのカードが使用できる。
	カード発行システムとの接続		他のカード発行システムと接続し，カードデータを伝送することによってカードの共有管理等が可能。

表2．統合ビルセキュリティシステムの機能(2)

	機能項目	機能概要
設備管理機能	計測監視	アナログ計測を自動的に行い，計測値を表示する。
	計量監視(検針)	各メータから出力されるパルス信号を自動積算し，積算値を表示する。
	遠方設定操作	空調機器への温度，湿度，ダンパ開度などの設定を行う。
	傾向測定監視	設定された計測・計量データを一定周期(1分，10分，60分の周期で60周期分)で格納し，トレンドデータとして折れ線グラフで表示する。
	デマンド監視制御	取引用電力量計(MOF)からのパルスによって受電電力量を積算し，一定周期(30分)のデマンド予測を行う。
	力率改善制御	受電部における無効電力を計測し，常に高効率で運転できるよう進相コンデンサの投入／遮断を制御する。
	停電時制御	商用電源停電時には，設定された設備機器に対して，その時点における運転スケジュール及び停電前の運転状態に基づいて自動再投入を行う。
	復電時制御	商用電源復電時には，設定された設備機器に対して，その時点における運転スケジュール及び停電前の運転状態に基づいて自動再投入を行う。
	定期点検通知	設定した運転時間に達した設備をリスト表示する。
	運転時間積算	設備の運転時間を積算し，設備の保守支援データとする。
	起動回数積算	設備の起動回数を積算し，設備の保守支援データとする。
	警報回数積算	設備の警報回数を積算し，設備の保守支援データとする。
	日報・月報・年報	各種設備のアナログ計測値・パルス計量値等を一定の書式でロギングプリンタに印字記録する。
	自動検針	パルス計量値及び運転時間を毎月集計して，一定の書式でロギングプリンタに印字記録する。
管理運用	操作許可制限	パスワード・カード情報・指紋データを設定することによって，オペレータが操作できる範囲を限定できる。
	ヒストリー(履歴)	過去における通行制御，機器の状態変化，警報の発生／復旧等を時系列順に表示できる。
	サマリー(集約)	現在継続中の警報の部屋や機器，未確認の警報を画面に表示できる。
	外部記憶装置への保存	外部記憶装置に履歴，日報・月報データ等を保存できる。
	ポケットベル呼出し	オペレータ不在時等に重要な設備機器に異常が発生した場合に，登録されているポケットベル番号を呼び出す。
	遠隔発報	設備や警備の異常を発報する。
	インターネット／イントラネット対応	Webサーバを設置することにより，テナント内ブラウザからデータ照会・設定が可能。

(ログイン時)の判定にも，パスワードなどの代替に利用が可能であり，このシステムにおいても操作権限手段の一つとして適用されている。

この装置は，当社独自の照合方式により，読み取り判定時間約1秒という高速化を実現し，また誤認識率は，他人受入率0.002%以下(テンキー利用時)，本人拒否率0.1%以下の高精度を実現した。

(2) 薄型ICカードリーダー

壁面取付けの省スペース型のICカードリーダーである外形幅130mm，高さ260mm，露出厚さ33mm(埋込み部50mm)と従来のものに対し小型化を実現している。

4. むすび

ビルセキュリティシステムは，近年のパソコン，インターネット／イントラネット，さらにはマルチメディア化の進展とともに，ますます情報化・ネットワーク化が進んでいる。

センターに設置される監視装置は，他のOA設備と接続されて相互にデータを共有しあうシステムへと展開しており，不審者の発見等の防犯設備としてだけではなく，システムへの不正アクセスやデータ改ざん等の情報セキュリティに関しても，従来にも増して強化していかなければならない。

今後も，システム自体のセキュリティも考慮しつつ，機能拡張と改良を重ねていく所存である。

JapanNet認証サービスを利用した社内情報システム

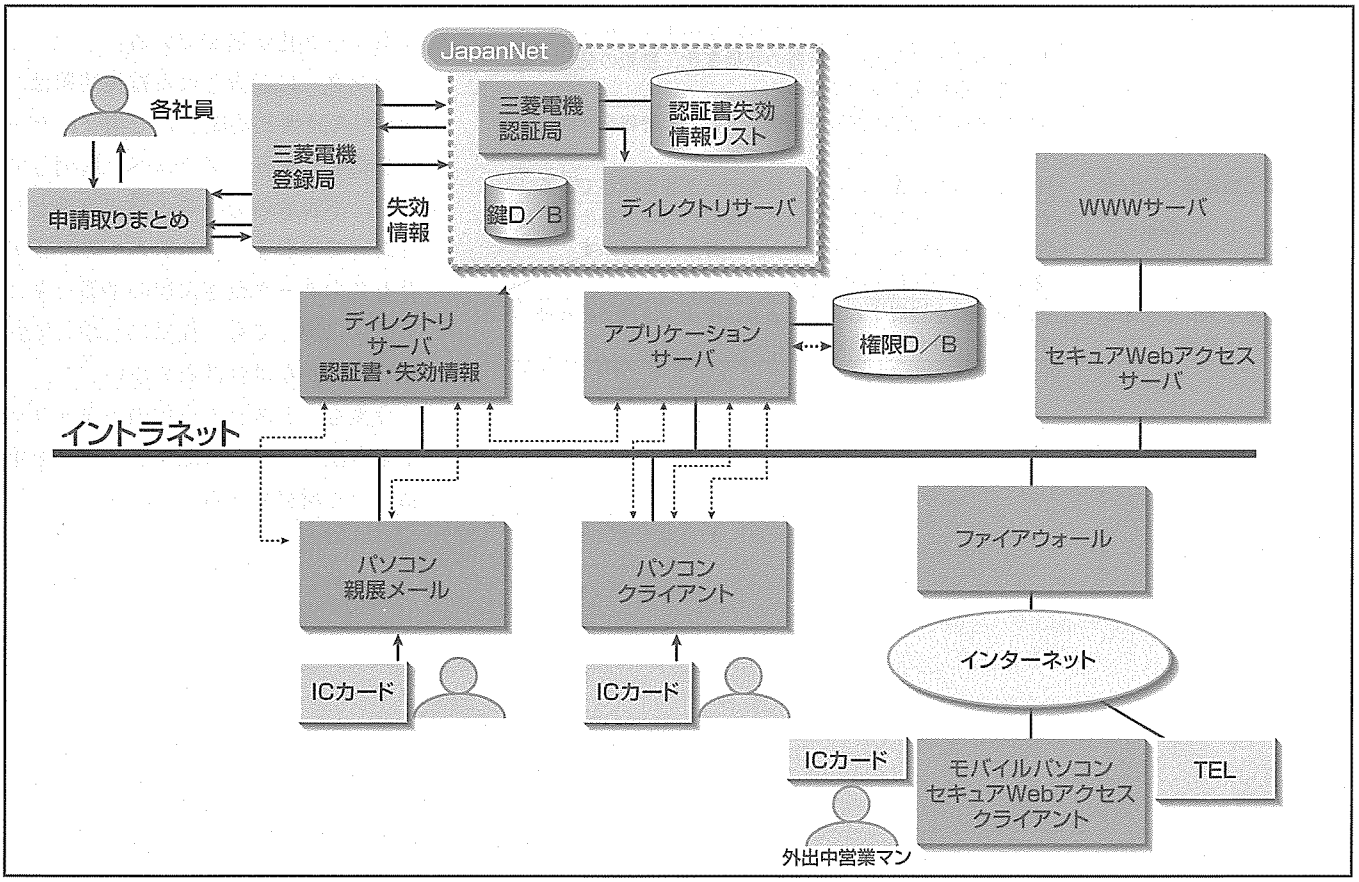
遠藤　淳*
桑原　悟**

要　旨

近年の急速なインターネットの普及により，オープンアーキテクチャなインターネット技術を利用したネットワークコンピューティングによる企業内経営基盤の再構築が始まっている。企業では，パソコンやLANの普及をベースに，部門間・企業間の相互接続性や安価なシステム構築コスト等のメリットから，デファクトスタンダードなインターネット技術を利用した社内網(イントラネット)の導入検討が行われている。三菱電機のイントラネットである“MELIT”も部門LANの拡張とともに年々拡大し，情報化オフィスのインフラとしての活用が期待されている。しかし，オープンアーキテクチャなネットワークは，従来のクローズドなネットワークシステムに比べて不正アクセスの脅威が増大することから，情報の秘匿や利用者の識別(個人認証)などのセキュリティが重要な課題となっている。

当社では，データの暗号化と個人認証を実現する情報セキュリティ環境を構築するため，第三者機関の認証局(JapanNet)を利用した認証システムを導入して運用評価している。

数年後には，社員に秘密かぎ(鍵)と認証書が格納されたICカード社員証を配布して，役職や業務等の権限データベースと組み合わせて利用することにより，ネットワークでの盗聴，改ざん，成り済まし，否認といった脅威を意識せずに，メールによる人事秘の親展送信や幹部への経営支援情報の公開，出張先からのWeb情報へのアクセス等，様々なアプリケーションが実現できる情報セキュリティ環境の構築を目指している。



社内認証システムの将来構想

将来の社内認証システムでは，認証局で発行する秘密鍵と認証書を格納したICカードを社員に配布し，権限データベースと組み合わせて利用することにより，イントラネット上に構築した様々なアプリケーションシステムをネットワーク上の脅威から守り，安全に運用することができる。

*ビジョン21事業化推進センター　**経営情報システム部

1. まえがき

企業内では，パソコンやLANの普及をベースに，デファクトスタンダードなインターネット技術を利用した社内網(イントラネット)の導入検討が盛んに行われている。

情報サービス産業協会によるユーザーアンケート調査(1996年)では，現在イントラネットを利用していると回答した企業と今後の利用を検討していると回答した企業を合わせると7割以上に達するとの結果が出ている。今後，企業のイントラネット構築により，ますますインターネット関連技術が発達し，インターネットやイントラネットを利用したネットワークシステムが普及拡大すると予想される。

インターネットやイントラネットを利用したネットワークでの情報共有は，企業にメリットを及ぼす反面，ネットワーク上に流れる情報が途中で盗聴・改ざんされたり，他人への成り済ましによるシステムへの不正侵入の脅威にさらされる危険がある。また，ネットワークで商取引に関連する重要な情報のやり取りを電子的に行う場合，実際には受信しているのに送信を否認されてしまう危険性もある。このため，当社では，ネットワーク上の脅威である盗聴・改ざん・成り済まし・否認から企業内の情報やシステムを防御する手段として，暗号技術を利用したディジタル認証技術の活用を検討している。

2. 概　要

当社では，'90年に各拠点のLANを接続して，“MELIT”の名称でイントラネットを構築した。当初は，研究所や開発場所のUNIXワークステーション間で，主にファイル転送による研究開発のコラボレーション用途で利用されていた。その後，パソコン上でのTCP／IPアプリケーションの発達によって急速にMELITに接続される端末数が増加し，電子メール全社展開施策により，全社ネットワークインフラとして活用されるようになってきた。現在，電子メールのアカウント数は4万1千，WWWを閲覧するソフトウェア(ブラウザ)の普及率は全社の課長以上で90%，本社地区では担当者を含めて70%に達している。

MELITでは，社外からの不正アクセスを防止するため，厳しいセキュリティ基準を設けて，ファイアウォールによるセキュリティ対策を行っているが，今後更にMELITを経営情報基盤として発展させていくためには，機密情報の暗号化や職制や資格に応じた情報のアクセス制御が必要となる。これらを実現する方法として，当社では，信頼できる第三者機関の認証局(以下“CA”という。)であるJapan Netを利用して認証書を発行する認証システムを導入し，運用評価している。認証書は，個人ごとに持つ秘密鍵と対で利用する公開鍵にCAのディジタルサインを付けて，秘密鍵の真正性(本人の秘密鍵であること。)を保証するものである。ネットワーク上で利用する電子的な社員証の役割を果たすことができる。図1に示すように，電子署名によって確かに本人であることを証明したり，情報を暗号化して相手に親展で届けることができる。

本稿では，当社がイントラネットで導入する認証システ

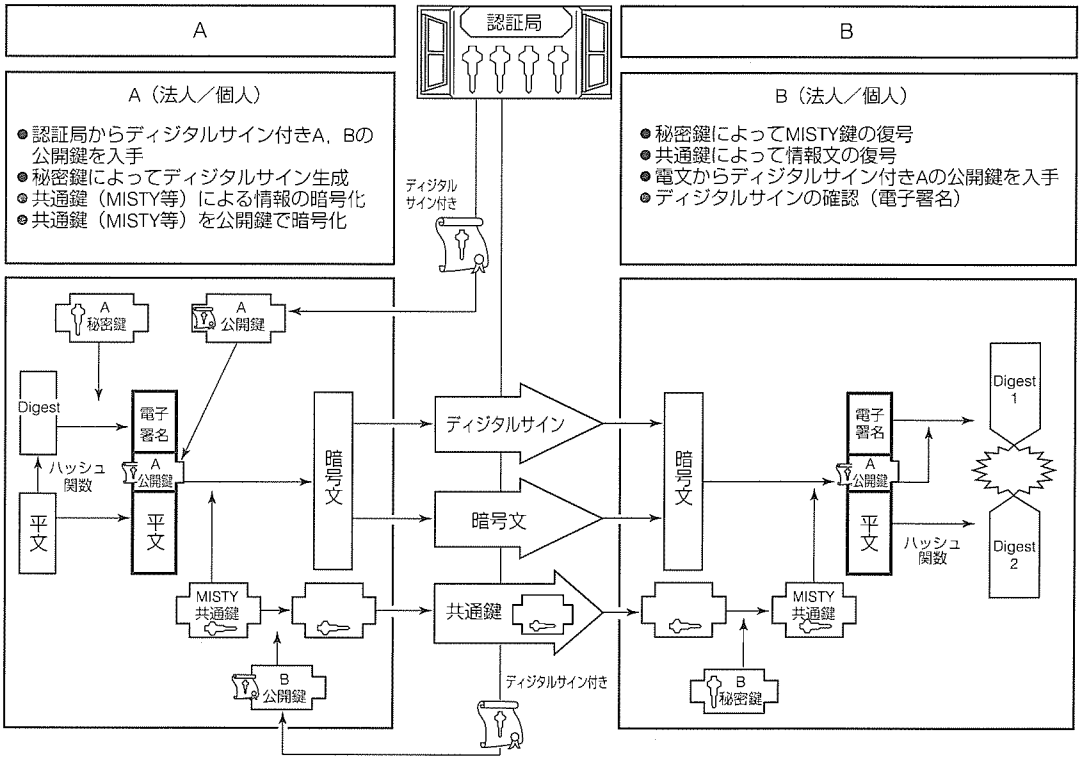


図1．署名・暗号化を用いた情報提供の仕組み

ムの考え方と認証書を利用した企業内アプリケーションについて紹介する。

3. 企業における認証システムの運用

認証システムの主な機能として，認証書の発行申請受付，申請書の審査，本人確認，認証書の発行・更新，認証書の失効，鍵の生成，鍵管理等がある。

3.1 認証書の発行申請受付・審査

企業内のイントラネットでは，社外秘等の情報を守るため，役職や業務ごとに情報やアプリケーションへのアクセス権を設定する高度なセキュリティを確保しなければならない。認証書は，ネットワークに接続されているのが正当な社員であることを保証するとともに，どの部門に所属するだれかを識別するために利用している。このため，認証書の発行審査については，従来の社員証相当の厳しい運用管理が求められる。

現在社内で運用評価している認証システムでは，認証書発行の申請受付，申請書の審査，本人確認などの業務を行う登録局(以下“RA”という。)を当社内情報システム部門に試験的に設置し，JapanNetに認証書の発行依頼情報を受け渡す運用を行っている。

3.2 認証書の発行・更新

認証書は，RAからの発行依頼情報を受けてCAが発行する。

認証書のフォーマットは国際規格のX.509によって標準化されており，本人に関する情報等を格納することができる。当社では，氏名や役職，組織名や電子メールアドレス等の変更が発生するものは，変更の運用及びコストが問題となるため，全社でユニークとなり入社以来不変な社員番号を本人情報として格納している。

有効期限についても，更新時の運用とコストを考慮し，一般の認証書では有効期限を１年間としている場合が多いが，セキュリティとのトレードオフで発行・更新時に有効期限を任意に設定できるようにしている。

発行した認証書は，成り済まし防止のため，秘密鍵とともにICカード等の物理的な媒体に格納し，対面で本人を確認して直接受け渡し，本人が常に携帯する運用が最も安全である。現在はフロッピーディスクを利用して運用評価しているが，数年後，ICチップのメモリ容量の増大やICカードリーダーライタの普及に合わせて，秘密鍵と認証書をICカード社員証として社員に配布することを検討している。

3.3 鍵 管 理

秘密鍵と公開鍵の生成は，インターネット上で一般に行われている認証サービスの場合，認証書の発行を申請する個人の端末で行っている。企業で認証システムを運用する場合は，不測の事態に備え，本人以外の人が暗号文書を復号できるように鍵を管理しておく必要がある。このため，当社では，秘密鍵と公開鍵をJapanNetで生成し，秘密鍵のバックアップを管理している。不測時には，正当な理由に基づき，適切な手続きを行うことにより，本人以外でも秘密鍵が利用できる運用を可能としている。

3.4 相 互 認 証

将来インターネットを利用してグローバルな企業間で情報交換する場合，相手の企業で利用している認証書が正当なものであることを検証できなければならない。異なるCAで発行された認証書の正当性を検証する手段として，相互認証がある。

JapanNetでは，米国認証局との間で認証書発行の運用基準等を確認し，互いの信頼性を保証する相互認証実験を行っている。

4. 三菱電機の社内認証アプリケーションの実現

当社では，'97年10月からJapanNetのルートCAの下に運用評価用の三菱電機CAを設置して，三菱電機専用の認証書を発行している。認証書の発行と運用管理に関する実証を行い，課題を抽出するとともに，認証書を利用した親展メールの運用評価を行っている(図２)。

運用評価では，パイロットユーザー約100人からスタートし，'98年度中に，本社の上級管理職への拡大，更に課長レベルへの拡大を図る。アプリケーションとしては，“親展メール”“HTMLコンテンツ(アクセス管理)”“業務アプリケーション(権限管理)”を実現し，最終的には，2000年をめどに社員証の機能との統一化による本格運用を目指している。

利用者インタフェースは，アプリケーションによらず一環している必要があるが，本運用評価では，

- 秘密鍵の携帯の有無のチェック
- 秘密鍵の正当な使用者の証としてのパスワード入力

を基本とする利用者インタフェースを目指している。

これらのチェックのタイミングは，対象となるセキュリティの重要性により，“都度のチェック”“利用開始時のみのチェック”“一定時間無入力時のチェック”などを選択的に採用する。

また，JapanNetのルート認証書，三菱電機CAの認証書及びその個人の認証書は本来ネットワーク上にあり，アクセス可能であればよいことになるが，ネットワークのトラフィック負荷とサーバ等の資源の負荷を軽減する意味から，社員個人向けの秘密鍵と同じ媒体(当面はフロッピーディスクで実現。)にこれらを格納する形態を採る。

4.1 親展メール(署名・暗号化メール)

企業内での機密情報や秘匿を要する情報のやり取りをオープンアーキテクチャのネットワーク上で実現するには，送り手と受け手(複数の場合もある。)間での内容の暗号化

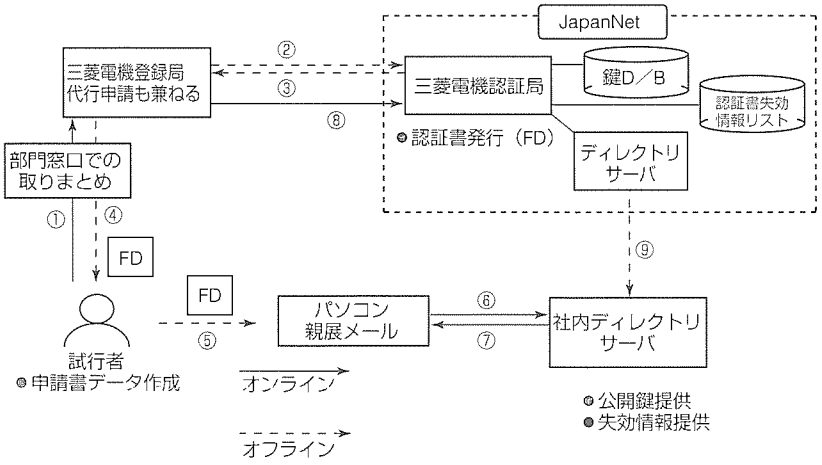


図２．JapanNet発行認証書試行環境

に加え，確かに送り手が作成したものであることの証明が必要となる。

これらの実現手段として，当社の三菱メッセージ暗号ソフトウェアMistyGuard“CryptoSign”を用い，共通鍵方式と公開鍵方式の両方を組み合わせたハイブリッド暗号方式を採用した(**図１参照**)。

通信文(又は任意のアプリケーションのファイル)は，毎回異なる共通鍵で暗号化し，その暗号文と暗号化に用いた共通鍵をネットワーク上の認証書から得た受け手の公開鍵で暗号化し，この両者を受け手に送ることで，経路上の暗号化を実現する。

受け手は，自身の管理する秘密鍵で共通鍵を復号し，これを用いて通信文(又は任意のアプリケーションのファイル)を復号する。

4.2　HTMLコンテンツの管理

イントラネット上のサーバに掲載する情報の中には，アクセスできる相手を限定する必要のある内容がある。このようなアクセス権の設定管理のため，当社のWebアクセス制御及びコンテンツデータの通信経路上の暗号化製品である三菱セキュアWebアクセスMistyGuard“TRUST WEB”を用い，三菱電機CAの社員向け認証書とサーバ認証書によるアクセス管理を実施した。

サーバとネットワークの間にTRUSTWEBサーバを配置し，ユーザーパソコンにはTRUSTWEBクライアントを導入して，サーバ，ディレクトリ，ファイル単位のきめ細かなアクセス権設定を実現する。

4.3　業務アプリケーションにおける権限

経理処理等に代表される業務アプリケーションでは，システム上で，決済等の権限行使の実現が必要である。これらアプリケーションでの各種権限は，職制のデータベースとともに，アプリケーション権限のデータベースとして管理し，各アプリケーションは，ユーザーの権限行使(承認ボタンを押すなど。)のステージでそのデータベースを参照する。

オープンアーキテクチャのネットワーク上でのセキュリティ実現のため，アプリケーションプログラムとデータベースの間の通信は，三菱電機CAの社員向け及びサーバ向け秘密鍵／認証書(公開鍵を含む。)を用いて暗号化を行い，盗聴，成り済まし(盗聴データの不正再使用)を防止する。また，権限データベースには，部門のプロセス管理者の署名を施し，改ざんの検知を行う。これら一連の機能を，当社の三菱暗号ライブラリ“PowerMisty”とそのオプションであるSMTK(Secure Message Tool Kit)及びLDAP(Lightweight Directory Access Protocol)の通信セグメントによって実現する。

ここで，プロセス管理者は三菱電機CAから社員向け秘密鍵／認証書の発行を受けるが，これは，社員個人に対してのものとは別に，役割としての“プロセス管理者”向けとして発行を受けることとした。

さらに，これらの権限管理を各アプリケーションが統一的・効率的に実現できるよう，各アプリケーションに埋め込むことのできるテンプレートを作成し，これを活用する。

5.　今後の課題

第一に，利便性，特にユーザーインタフェース(使い勝手)とセキュリティ強度との相反する要求をどう満足するかが鍵となる。セキュリティの強度を求めるために利用者に負担を強いると，その仕組み自体への抵抗感から，使用されなくなる。しかし，利用者の利便性だけを追求していては十分なセキュリティは実現できない。利用者の理解を得るための教育等の投資も含め，両者のバランスの見極めが重要である。

ユーザーインタフェースについては，更に，統一性の観点も重要である。この点では，個々のブラウザやメーラのインタフェース機能に依存せざるを得ない。また，現行では，独自の利用者認証(多くは，独自のユーザーIDとパス

ワード)を必要とするソフトウェア製品に対しても，X.509に基づく統一的な利用者認証，いわゆる“シングルサインオン”の対応が期待される。

また，セキュリティ強度の面では，サーバ，認証ツール間通信での成り済ましに対抗しなくてはならない。セキュリティの実現にはコンポーネントの組合せは必す(須)であるが，組合せによる予期せぬセキュリティホールの発生の可能性もあり，この点での検証も重要である。

次に，相当規模のユーザーを持つイントラネットでは，ネットワーク自身やサーバ等のネットワーク上の資源の負荷が問題となる。セキュリティのための負荷増を極力減らす工夫も，個々のセキュリティ製品やそれらを組み合わせた運用環境において重要な課題である。

最後に，新技術，新製品への対応も重要な課題となる。情報セキュリティに関する技術は今後加速度的に進歩するものと思われ，特に“スマートカードの機能向上”や“指紋等による個人識別技術”は，今後数年で安価に実現され得るものである。これらの技術，製品動向も注視してトータルな情報セキュリティ環境を実現していかなければならない。

6. むすび

ディジタル認証技術による一環した情報セキュリティ環境は，企業内はもとより，企業間の機密，秘匿を要する情報のシステム化を可能にし，トータルなホワイトカラーの生産性向上につながる。

また，企業内の業務処理における不正防止の仕組みとして，企業自身だけでなく，顧客や株主の利益を守ることにつながるものであり，国際規格に基づく技術の採用と各業務アプリケーションへの適用は，企業の信頼性の尺度として今後ますます注目されていく。

運用評価の各ステージでのノウハウの蓄積とCA，RA，及び企業内利用ソフトウェア製品へのフィードバックを行い，企業向けディジタル認証のトータルな環境の提供に向け，今後も適用を拡大しつつ，ブラッシュアップを継続していく計画である。

参考文献

(1) 佐々木武男，大谷彰宏，佐々木道雄，勝山光太郎，佐伯正夫，中村吉人：ジャパンネット㈱向け電子商取引システム，三菱電機技報，72，No.2，166～169 (1998)

(2) 電子商取引実証推進協議会 認証局検討WG：認証局検討報告書 (1997-3)

(3) 電子商取引実証推進協議会 認証局検討WG：本人認証技術検討WG中間報告書 —— 参照モデルと評価基準 v0.5 —— (1997-5)

(4) 社団法人情報サービス産業協会：情報サービス産業白書 (1997)

ノンストップ自動料金収受システム

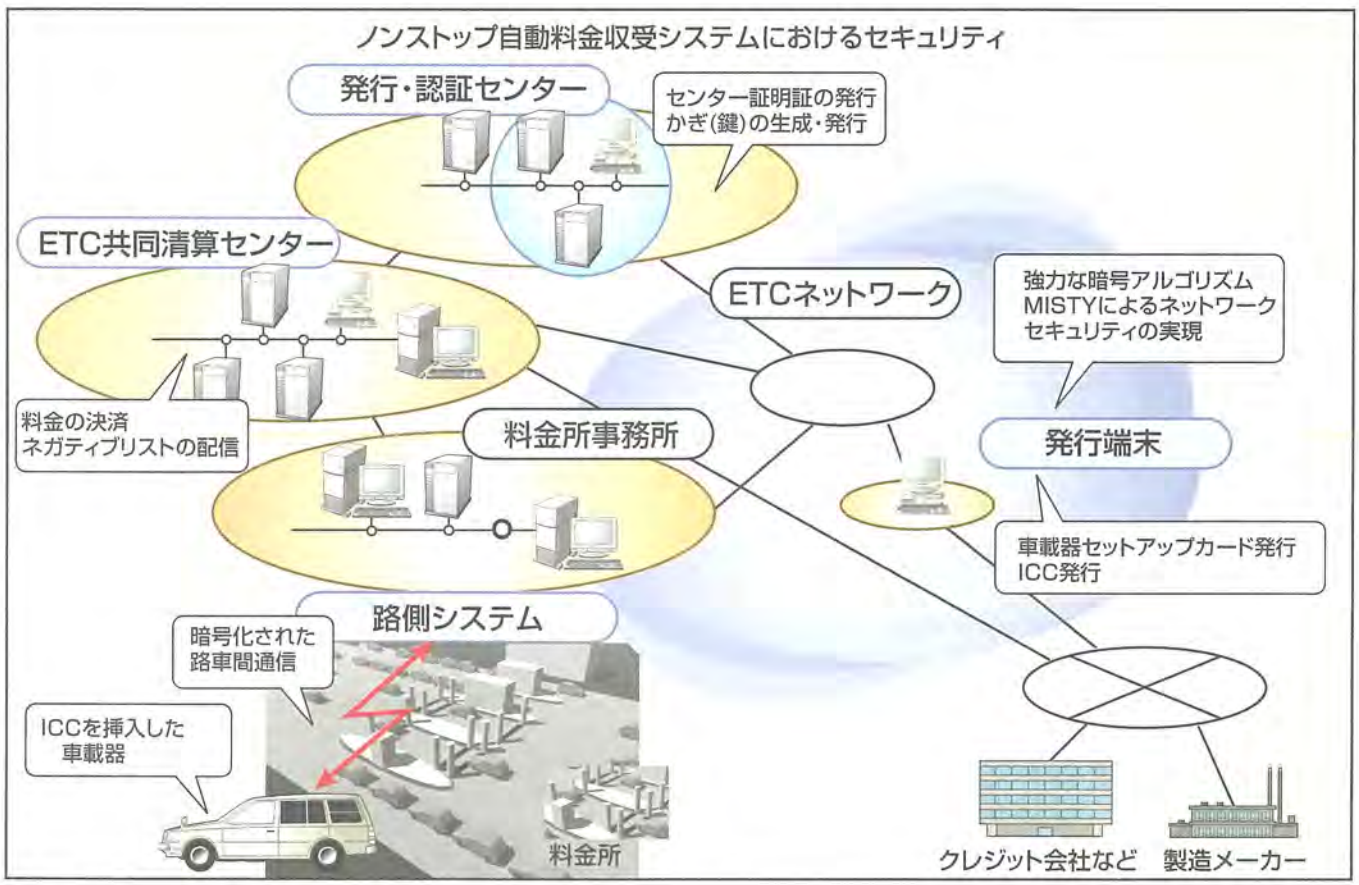
内藤　博*　近澤　武**
森吉国治*　野崎　充***
相川昭仁*

要　旨

ノンストップ自動料金収受システム(Electronic Toll Collection System：ETC)は，車両が有料道路の料金所を通過した際に，路上に設置された路上機と車両に搭載された車載器との間で無線通信によって料金の収受が行われるシステムであり，1999年夏に実用化が計画されている。システムにおいて，このような無線通信による料金の収受形態が採られた場合，通信内容の傍受や通信データの改ざん等が発生する可能性がある。また，料金所における料金収受に関する料金情報及び個人情報は，ネットワークを介して上位システムに伝送されるため，ここでも通信情報の傍受やデータの改ざん等の脅威にさらされることになる。

また，車両に搭載される車載器や個人が所有するICカード(ICC)は，不特定多数の利用者の管理下に置かれる。さらに，これらを発行し活性化する装置は，道路事業者から業務委託された業者でも管理する場合が考えられ，このような車載器／ICCの発行／活性化においてもデータ改ざん等の脅威に対する対策が必要となる。

したがって，ETCにおいては，暗号技術を用いた暗号通信や相互認証によるセキュリティシステムの構築が重要であり，三菱電機が提案するETCにおけるセキュリティシステムについて述べる。



ノンストップ自動料金収受システムの構成例

不特定多数の利用者がICCと車載器を利用し，かつ全国を網羅するネットワーク上で料金情報や個人情報が通信されるため，確実な料金収受は当然のことながら，車載器から発行・認証のセンター系システムまで統一されたセキュリティコンセプトでシステムを構築することが重要である。三菱電機が開発した暗号アルゴリズム"MISTY"を中心に，トータルシステムセキュリティを実現する。

*鎌倉製作所　**情報技術総合研究所　***公共事業部

1. まえがき

ETCは，料金所における渋滞解消，管理コストの節減，キャッシュレス化による利便性の向上等を目的とし，建設省及び道路4公団(日本道路公団，首都高速道路公団，阪神高速道路公団，本州四国連絡橋公団)が中心となって導入を計画している。

ETCでは，路車間通信でのデータの改ざん，傍受等の問題，車載器やICCの成り済まし，料金所で収集されたデータの上位システムへの伝送時のデータ改ざん，傍受など様々な脅威が考えられ，これらの対策が重要となる。

当社では，建設省及び道路4公団による共同研究を始めとして，ETCの開発に取り組んできた[1]。また，暗号アルゴリズム“MISTY”を使用したセキュリティシステムの構築に取り組んでいる。

本稿では，当社が提案するセキュリティシステムについて紹介する。

2. システムの概要

2.1 システムの目的

日本におけるETCは，次に示す内容を実現することを目的として導入が計画されている。

- 料金の収受にかかわる時間の削減
- 渋滞の緩和に伴う燃費節約と周辺環境の保全
- キャッシュレス化によるユーザーサービスの向上
- 料金の収受にかかわる管理費用の節約

また，ETCに対する基本要求は次のとおりである。

- 交通がふくそう(輻輳)する中で多様かつ確実な料金収受
- セキュリティの確保とプライバシーの保護

2.2 システム運用の概要

当社が開発した路側システムや車載器等を図1～図4に示す。これらの機器はセキュリティ機能を持っており，セキュリティに関する運用について以下に示す。

(1) 発行端末による車載器活性化とICCの発行

車載器は，カーディーラー等で販売され，セットアップカード(SC)の挿入によって活性化(車検情報・鍵情報の登録)が行われる。鍵情報は，発行・認証センターで作成し，発行端末でSCに書き込まれる。

ICCは，発行・認証センターからの鍵情報と発行端末で登録する個人情報を記録して発行される。

(2) 路車間通信

車両が料金所を通過する際，車載器と路上機間で暗号通信によって個人情報や通行履歴等を交信し，料金を収受する。このとき，ICCの正当性を確かめるため，ネガティブチェックも実行する。

(3) 発行・認証センター

このシステムで使用する車載器(SC経由)，ICC，路上機に対して，鍵情報や証明証を発行し，機器の正当性を確保する。

(4) ETC共同精算センター

ETC共同精算センターは，通信ネットワークによって伝送された料金所で収集した料金情報に対して，決済処理

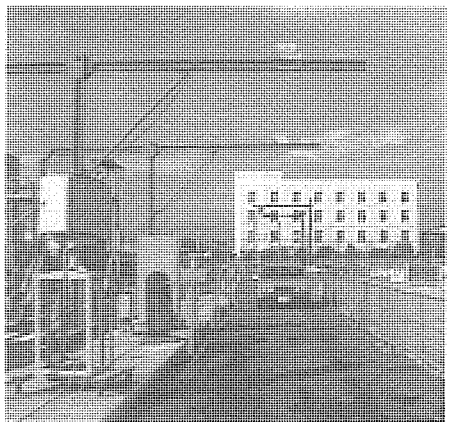


図1．鎌倉テストフィールドの路側システム

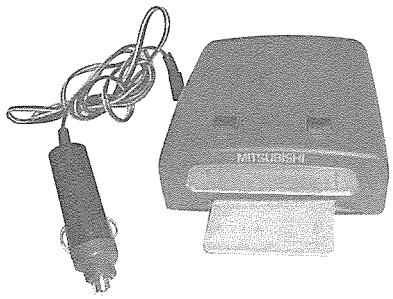


図2．ICCと車載器の外観

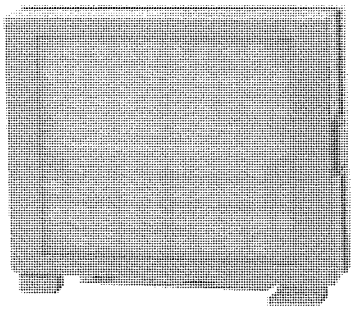


図3．路上機(アンテナ)の外観

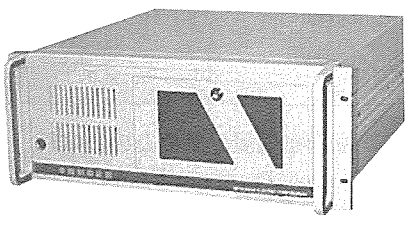


図4．路上機(制御装置)の外観

表1．ETCにおける脅威

ETCの特徴	考えられる主な脅威
●車載器・ICCについては，不特定多数の利用者が存在し，システム自体を直接利用する。	●車載器の偽造・変造 ●ICCのデータ改ざん，偽造 ●車載器から路上機への車両情報，課金情報の不正通知 ●他人のICCに蓄積されている個人情報の盗聴によるプライバシー漏えい(洩)(社会的問題発生)
●車載器は，オフラインでのICCリーダ／ライタ端末となる。	
●無線や有線のネットワークを介して多額の金銭情報を収受する。	●内外部のネットワーク上に流れる課金情報やICCの個人情報に対する改ざん
●オープンなネットワークとの接続がシステム内に存在する。	

を実行する。また，ネガティブリストの登録や配信処理もここで実行する。

2.3 システム構成上の課題

このシステムは，次の特徴がある。

- ●車載器やICCは，不特定多数の手に渡り使用される。
- ●料金収受は無線通信による。
- ●料金情報はネットワークを介してETC共同精算センターで収集され，決済処理が行われる。

システムセキュリティを確保するため，次の課題の解決が重要である。

- ●利用者所有の車載器やICCの不正使用への対応
- ●無線通信において，高速な認証／暗号通信の実現
- ●ETCネットワークの機密性・完全性の確保

3. 脅威の分析とセキュリティモデルの構築

ETCは日本全国に展開されるシステムであり，万一セキュリティが破られた場合，その波及被害は膨大なものになる。したがって，セキュリティが破られることがないシステムを前提にシステムを構築しなければならない。

当社は，世界的にも評価の高い暗号アルゴリズムであるMISTYを始め，ネットワークセキュリティシステムの開発を推進してきた。

以下に，ETCにおける脅威分析と，これに基づくETCセキュリティモデルを提案する。

3.1 ETCにおける脅威の分析

セキュリティシステムの構築に当たって，まず脅威の分析・評価を行う必要がある。ETCでは，これまで料金所の収受員が確認しながら行っていた各種業務を，最新の無線通信技術とコンピュータテクノロジーを駆使して自動的に処理する。したがって，従来の料金収受システムでは考えられなかったような様々な脅威が発生するおそれがある。

ETCにおいて考えられる脅威を**表1**に示す。

3.2 脅威への対処と適用技術

脅威への対処として，システムに必要な機能と適用技術等を**表2**に示す。

3.3 ETCセキュリティモデル

当社の提案するETCセキュリティモデル例を**図5**に示す。また，このセキュリティモデルにおける主要技術を以下に示す。

表2．脅威への対処としてシステムに必要な機能と適用技術

必要な機能	適用技術・方式など
路車間通信におけるデータ傍受・改ざんの防止	●情報の暗号化
成り済まし防止 ●ICCや車載器の偽造・変造等への対処 ●他人のICC個人情報の盗み取りへの対処	●ディジタル署名技術を活用した相互認証方式の適用
ネットワーク上の情報に対する改ざんの防止 ●ネットワーク上の金銭情報等の改ざんへの対処	●情報の暗号化技術，及びディジタル署名技術を適用

(1) SAM(Secure Application Module)

車載器，ICC，路上機等の料金情報を扱う機器には，セキュリティを確保するために，暗号の仕組みを持つSAMが組み込まれる。

このSAMには，発行・認証センターで生成し配送された証明証と暗号鍵等の鍵情報が格納される。SAM搭載機器間では，SAMに内蔵された暗号アルゴリズムと鍵情報により，通信相手の相互認証を行い，暗号化によって情報を秘匿化して通信ができる。これによって，SAM搭載機器のセキュリティを確保することができる。

(2) 発行・認証センター

発行・認証センターは，SAM製造メーカーや車載器製造メーカー，及びSCとSC発行端末，ICCとICC発行端末，路上機等の関連機器に対して，センターの証明証を発行するとともに，暗号鍵の生成と配布を行う。SCを車載器へ挿入することにより，車載器のSAMにセンターの証明証，暗号鍵(秘密鍵)及び車検証情報が書き込まれ，車載器として使用可能となる。

(3) 認証方式

車両が料金所を通過する際，ICC-車載器-路上機間で料金情報や個人情報等の重要な情報が交信されるため，これらの機器間及び関連している装置間において相手認証が必要となる。当社が採用している相手認証方式は，次の3方式である。

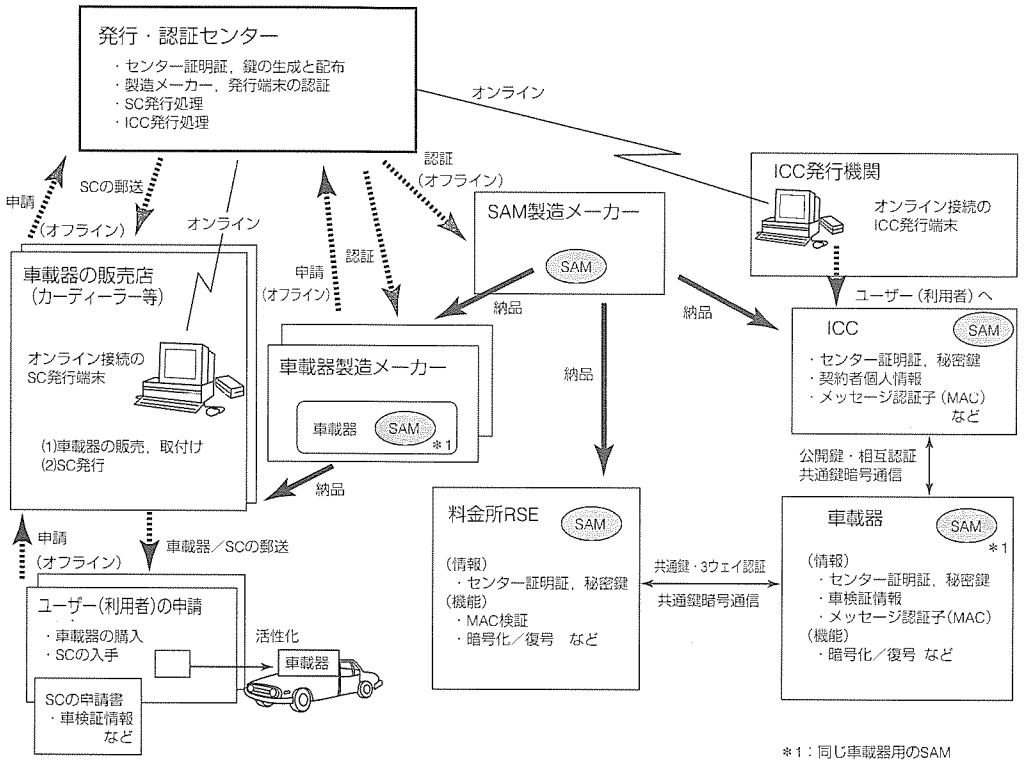


図5．ETCセキュリティシステム例

(a)　公開鍵暗号を利用した相手認証

認証処理の高速性をさほど要求されないICCと車載器間，発行・認証センターと路上機間，発行・認証センターとICC発行端末／SC発行端末間における相互認証を行う。

(b)　共通鍵暗号を利用した3ウェイ認証による相手認証

認証の高速性を要求される車載器と路上機間における相互認証を行う。

(c)　オフライン配送による相手認証

発行・認証センターとSAM製造メーカー間等の認証を行う。

これら以外に，車載器やICCに含まれる重要情報(契約者個人情報等の料金収受に関係する情報)にはメッセージ認証子(MAC)を付与して改ざんを防止している。

(4)　暗号方式

ICCや車載器の盗難等によって暗号アルゴリズムが悪意を持つ第三者に知られる可能性があることから，一般研究機関で暗号アルゴリズムの解読法に対して安全である評価がなされている必要がある。当社では，アルゴリズムが公開されていても高いセキュリティ強度を持っている共通鍵暗号のMISTY1を推奨している。

3.4　ネットワークセキュリティ

ETCネットワークでは料金情報だけでなく契約者個人情報等のプライバシー情報も通信されるため，その情報を暗号化して秘匿を行うことを当社は推奨している。今やイントラネットのLAN上のデータをパソコンで盗聴できる時代であり，イントラネットの内外からの盗聴や改ざんを防止する安全なネットワークの構築がETCにおいても要求される。

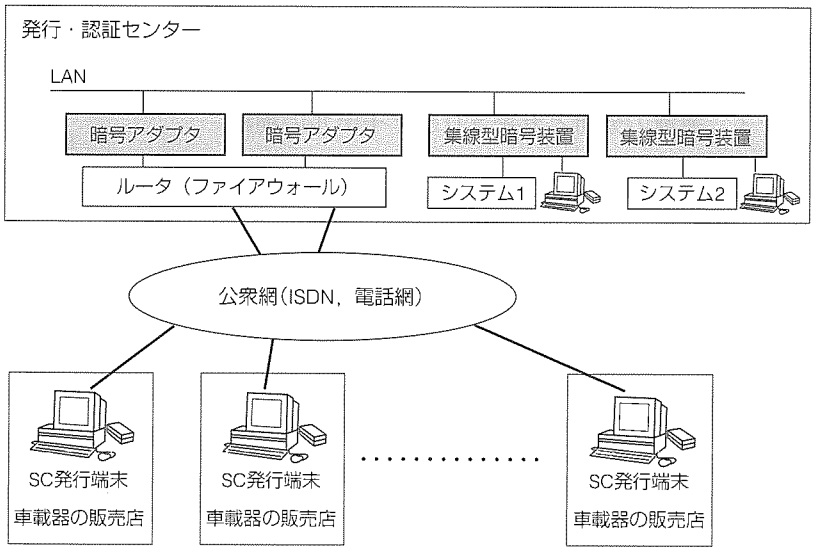
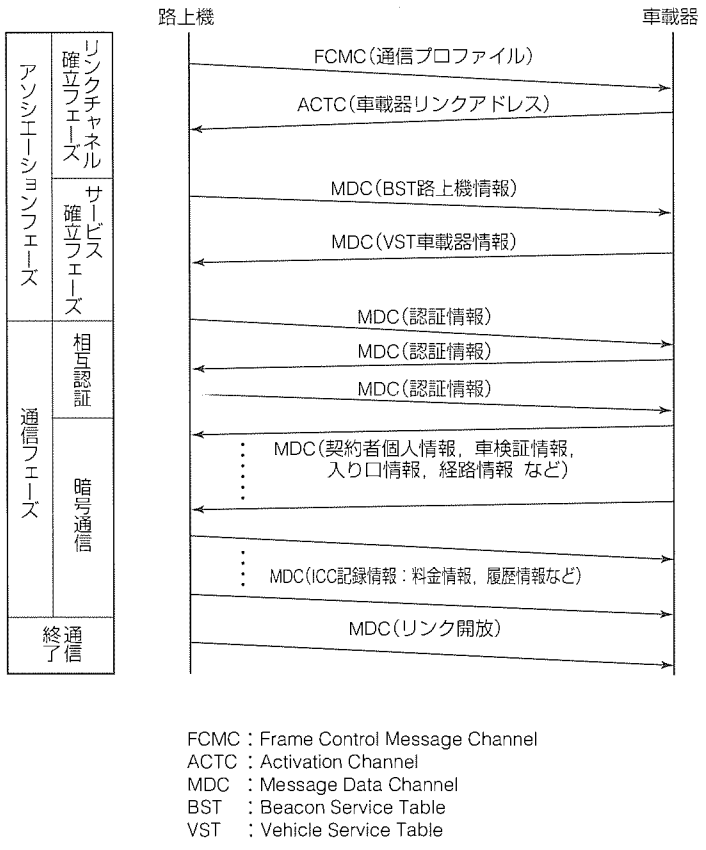


図6．発行・認証センターとSC発行端末の接続例

図6に発行・認証センターとSC発行端末の接続例を示す。図では，車載器の販売店に設置されたSC発行端末が，公衆網を介して，発行・認証センターと接続されている。公衆網を介した通信では，暗号アダプタとSC発行端末間



FCMC：Frame Control Message Channel
ACTC：Activation Channel
MDC：Message Data Channel
BST：Beacon Service Table
VST：Vehicle Service Table

図7．通信トランザクション例

で暗号通信することで，盗聴や改ざんを防止できる。またネットワーク接続された内部のシステム間通信では，集線型暗号装置で暗号通信を行うことにより，盗聴や改ざんを防止できる。当社は暗号アダプタ及び集線型暗号装置としてMELWALL3000シリーズを推奨しており，この方式による発行・認証システムのモデルを構築し，評価中である。

3.5 路車間通信におけるセキュリティ

路上機と車載器との間の路車間通信は，5.8GHz帯アクティブ方式が採用されており，通信プロトコルも含め標準化が進められている。この通信は，料金所における最大車両速度80km／hに対応し，1通信領域において，同時に2台の車両と通信可能となっている。また，高速道路本線上では，車両速度180km／hまで対応する。

通信トランザクションでは通信リンクを確立した後に路上機と車載器で相互認証を実施する必要があり，扱うデータは暗号化して通信を行うため，通信トランザクションでの暗号化／復号処理に高速性が要求される。このため，路車間の相互認証では，公開鍵暗号と比較して高速処理が可能な共通鍵暗号方式を採用している。

図7に通信トランザクション例を示す。

4. 今後の展開

当社では，車載器，路上機等の路側システムの開発とともにETC運用の検討を行い，また，脅威分析によってセキュリティモデルを作成し，運用性に優れかつセキュリティ対策で抜けのないETCトータルシステムの実現に向けて開発を推進している。

システムの実現のために，以下の課題に対応していく。

(1) 高速処理可能なSAMの開発

料金所を高速で走行する車載器と路上機が相互認証し暗号通信を実行するために，高速処理が可能なSAMが必要となる。当社では，高速処理可能な共通鍵暗号アルゴリズムMISTYを用いたSAMを提案している。

(2) ETC用ICCの実現(将来の電子決済への展開)

電子決済等で用いられているEMV規格準拠のICCは，ETCの特殊性を考慮されていないため，当面はETC専用ICC使用に限定される。今後は，利用者へのサービス向上のため，他のアプリケーションにも利用可能なようにクレジットカード会社との連携を図り，ETCとしての要求を取り入れたクレジットカードを整備していくことが必要である。また，将来構想として，Javaカード機能を活用したマルチパーパス化を進め，他の交通機関との共用化が必要と考えられる。

5. むすび

ETCにおいて当社が提案するセキュリティシステムについて述べてきたが，ETCの実用化に向けて，各種セキュリティシステムの検討を進めており，暗号，ディジタル署名，認証等の最新の情報セキュリティ技術をETCに適用し，外部脅威からシステムを保護することにより，安全で信頼性の高いシステムの実現に向けて具体化を進める。また，ICCの標準化動向や電子マネーへの適用など，将来の動向も念頭に置きながらETCのセキュリティシステムの開発を推進していく。

参考文献

(1) 特集“進化する知的道路交通システム”，三菱電機技報，70，No.12，1152～1239 (1996)

次世代汎用インバータ“FREQROL-A500シリーズ”

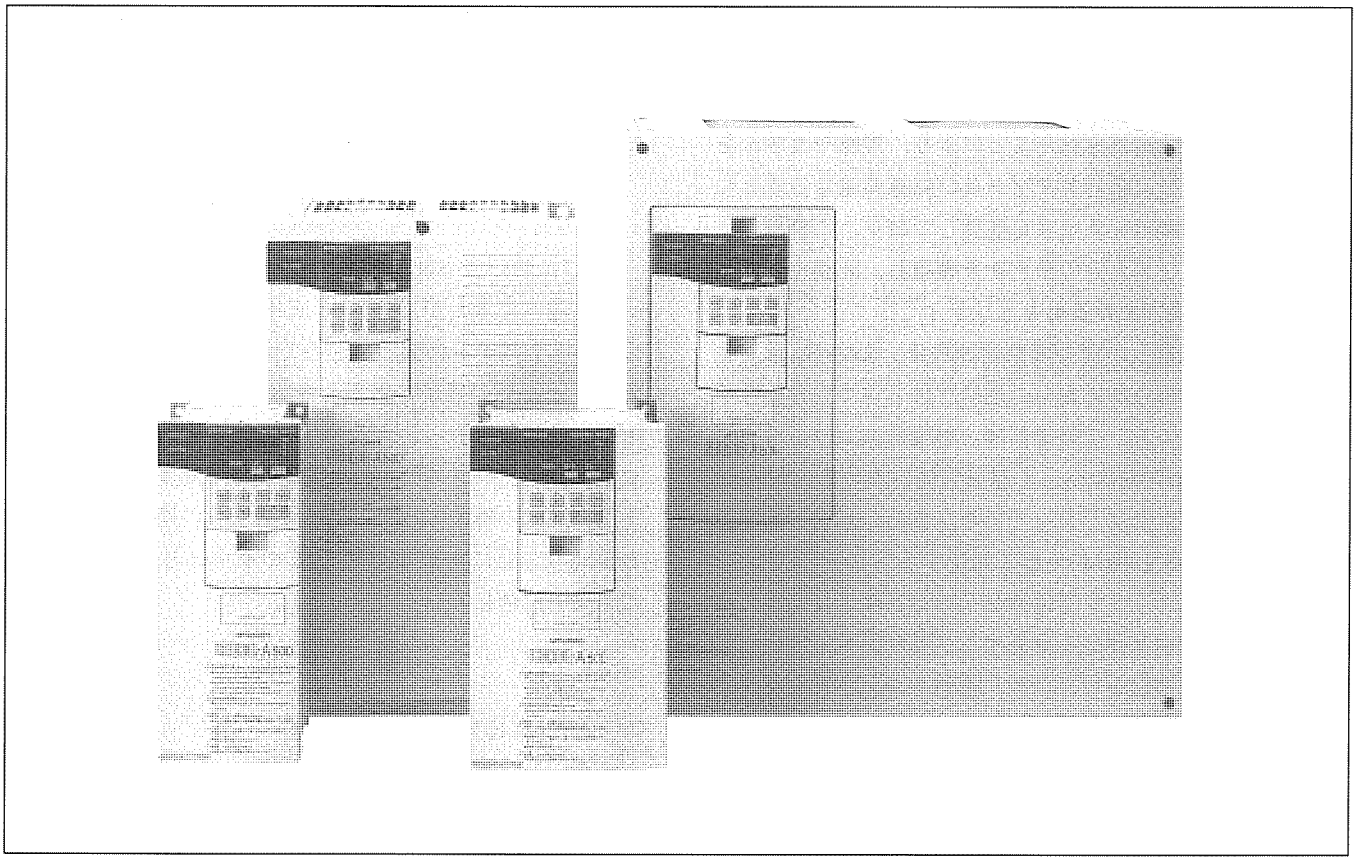
桜井寿夫* 貝谷敏之*
栗山茂三* 奥山美保**
今中 晶*

要 旨

次世代汎用インバータとして“FREQROL-A500シリーズ”を開発し製品化した。CPUとして32ビットのRISCマイコンを採用して制御の高速化を図り，主回路制御に専用LSI(スマートドライバ)を開発し，高速・高精度に制御が可能となった。また，制御方式としてアドバンスト磁束ベクトル制御を開発し，さらにモータ定数をインバータが自動測定するオートチューニングを開発した。

オートチューニングでは，オフラインとオンラインの2方式を準備した。特にオンラインオートチューニングでは，運転開始時に短時間で直流励磁を行うことで，モータの一次抵抗と二次抵抗を同定する方法を採用し，これにより，モータの温度上昇によるモータ定数の変化の影響を最小限に抑えた。この結果，速度制御範囲1：120を実現し，業界トップクラスの駆動性能を得た。

さらに，回転むらは，スマートドライバの効果によって従来比1／2以下とした。また，Soft PWM(Pulse Width Modulation)制御を新規開発し，モータからの励磁騒音を分散させることによって耳障りな音を減らすことができた。操作性向上として，LCDバックライト付きパラメータユニットを開発し，8か国対応の表示を可能とした。メンテナンスの向上として，脱着端子の採用，冷却ファンのON／OFF制御による長寿命化，冷却ファンのカセット方式を採用した。グローバル化への対応として，オープンネットワークへの対応，安全規格への対応，240V／480V電源への対応も実施した。



次世代汎用インバータFREQROL-A500シリーズ

アドバンスト磁束ベクトル制御，オンラインオートチューニングを搭載した最新鋭の汎用インバータFREQROL-A500シリーズで，業界トップクラスの駆動性能を実現した。また，簡単操作，メンテナンス性の向上、海外規格への対応(UL，cUL，EN)などの特長を持ち，三菱汎用インバータの最高峰機種である。

*名古屋製作所 **産業システム研究所

1. まえがき

汎用インバータは，最新のパワーエレクトロニクス技術とモータコントロール技術を駆使した製品である。省エネルギー，省力ニーズにこたえて開発された汎用インバータは，当初，ファン，ブロア等の空調機器，ベルトコンベヤ，ターンテーブル，リフタのような搬送装置への適用がその主な用途であった。近年，あらゆる産業分野に使用されるようになり，今や駆動制御装置の中心的位置を占めている。

汎用インバータの適用分野拡大が進む中，従来の汎用インバータでは実現できない高度な駆動性能・高トルク出力や，高精度の周波数制御，超低速から高速まで安定したトルク特性等を求める声が一層強まっている。

今回，これらの高性能の要求にこたえるため，次世代汎用インバータ“FREQROL-A500シリーズ”を開発した。本稿では，その最新技術，及び機能について述べる。

2. FREQROL-A500の概要

FREQROL-A500シリーズは，200V／400V系電源に合わせて，それぞれ0.4～55kWの15容量，全30機種がラインアップされている。また，機能面，性能面，操作性，拡張性の点で，当社汎用インバータの最高峰に位置するものである。FREQROL-A500は，電源電圧，容量によらず全シリーズが同一の仕様で製品化されている。前ページにシリーズの外観を示す。

2.1 特　長

主な特長は次のとおりである。なお，FREQROL-A500の仕様概要を**表1**に，従来機種との比較を**図1**に示す。

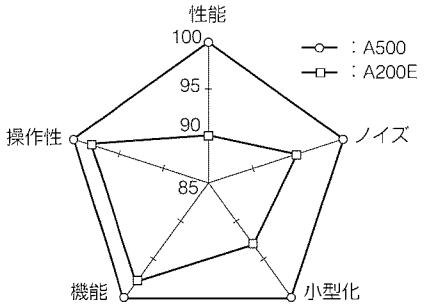


図1．従来機種との比較

表1．FREQROL-A500の仕様概要

No.	項　目		FREQROL-A500
1	容量・電圧レンジ		0.4～55kW／200V 0.4～55kW／400V (240V(22kW以下)・480V対応)
2	周波数範囲		0.2～400Hz
3	制御方式		高キャリア周波数PWM制御(Soft-PWM制御) V／F制御，アドバンスト磁束ベクトル制御，ベクトル制御
4	性　能	速度制御範囲	1：120(力行)
		始動トルク	150%／0.5Hz(アドバンスト磁束ベクトル時)
		ベクトル制御(PG付き)	可(サーボロック，0速)
		0速度制御	150%／0Hz(PG付き)
5	機　能	オートチューニング	オフライン／オンライン
		冷却ファンON／OFF制御	可
		PID制御	あり(PID標準)
		多段速	15速
		加減速時間	3個
		インテリジェント機能	最短加減速，最適加減速，省エネルギー，昇降機
		シンクとソース切換え	可
6	P　U	構成	FR-DU04標準装備 8か国語PU04(オプション)
		入力方式	上下キー(FR-DU04)／10キー入力(FR-PU04)
		LCD(バックライト)	FR-PU04に装備
		コピー機能	標準で内蔵
7	内蔵 オプション	種類・構成	PLG，オリエント，ディジタル入力，リレー出力，計算機リンク，アナログ出力，パルス列入力，ディジタル出力，12ビットディジタル入力，通信
		通信　標準	RS485×1ch
		通信	CC-Link，ModbusPuls，Profibus-DP，DeviceNET
8	構　造	NEMA規格対応	NEMA1(22kW以下)
		制御端子の脱着方式	全容量可
		カセット式冷却ファンの交換	可
		DCL接続	全容量接続可
9	規　格		UL／cUL／EN

(1) 駆動性能の向上

高速RISCマイコンを採用し，当社独自のアドバンスト磁束ベクトル制御とオンラインオートチューニング機能により，始動時にモータ定数を素早くチューニングすることによってモータの温度に影響されない高精度運転と超低速域までの高トルク・安定運転を可能とした(速度制御範囲1：120，当社従来比6倍)。

また，インバータの主回路の状態を直接監視し出力波形を制御するスマートドライバ(当社独自の新開発ASIC)を開発し，低速時の回転むらを当社従来比1／2以下に改善した。

(2) 簡単操作，簡単メンテナンス

冷却ファンはON／OFF制御の採用によって長寿命化を可能とし，またカセット方式としたことによってユーザー交換を可能とした。さらに，制御端子台を脱着式端子台とすることにより，インバータ交換時のメンテナンス時間の大幅短縮を実現した。また，専用セットアップソフトウェアを準備し，短時間での立ち上げを可能とした。パラメータユニットは，バックライト付きLCDとし，8か国語表示可能とした。

(3) 低騒音，低ノイズ

従来の高周波PWM方式の低騒音モードに加え，モータ金属音の成分を分散化することでモータ励磁音を低減するSoft-PWM制御方式(発生ノイズは非低騒音運転並み)を開発した。

(4) 海外仕様・安全規格への標準対応

海外の標準仕様(240V／480V電源，入出力端子のシンクとソース切換えなど)への対応を可能とし，北米や欧州の安全規格(UL，cUL，EN)にも標準品で対応可能とした。

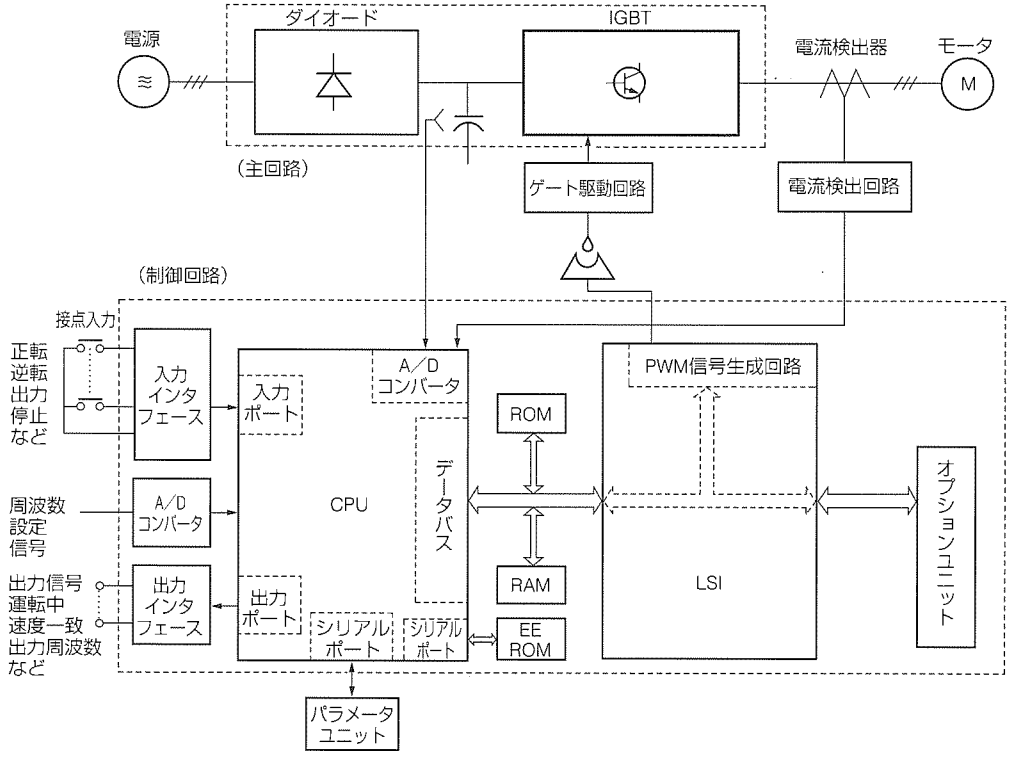


図2．従来の回路構成

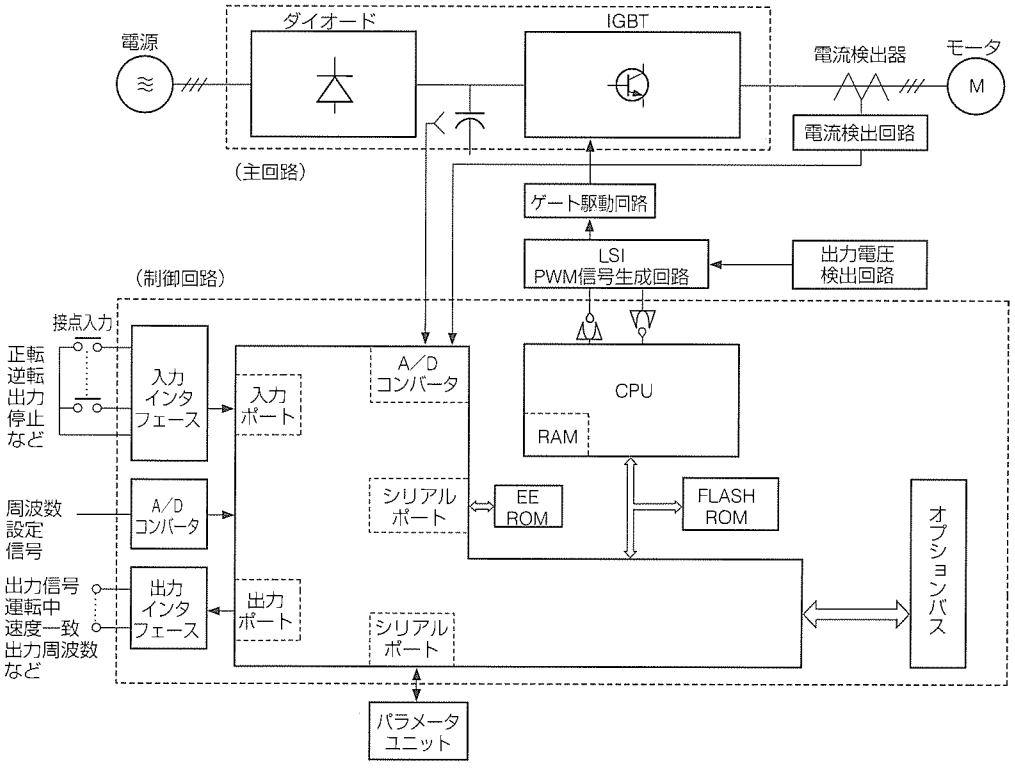


図3．FREQROL-A500の回路構成

また，内蔵オプションの装着により，世界の主要オープンネットワーク(CC-Link，DeviceNET，Profibus等)にも接続可能とした。

2.2 構　成

図2に従来の汎用インバータの回路構成，図3に今回開発したFREQROL-A500シリーズの回路構成を示す。駆動能力向上のため主回路電位で動作するPWM信号作成のための専用LSI(スマートドライバ)を新たに開発して採用した点が，回路構成上の大きな特長である。

制御回路では，使用するCPUに内部32ビット構成のRISCマイコンを採用し，高性能・高機能化を図った。また，プログラムを格納するメモリにはフラッシュROMを採用し，プログラムの変更を容易にした。パラメータユニットとの交信は，RS485の規格に準拠したことにより，パラメータユニットを外して，外部コントローラとの交信も可能とした。

図4に新規開発した複合モジュールを示す。モジュール内部に，主回路素子以外に，ゲート駆動素子，検出回路を取り込み，小型・高機能化を図っている。

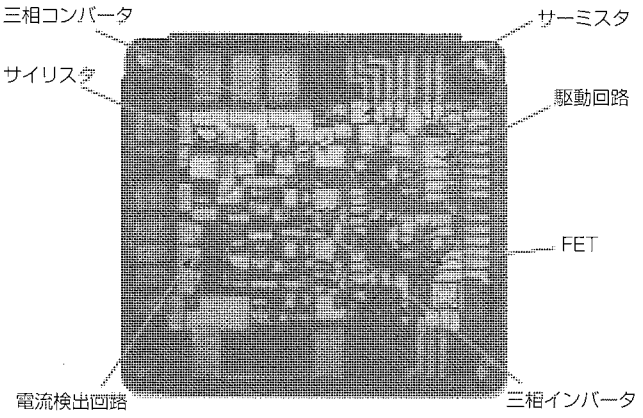


図4．複合モジュール

3. 駆動性能向上

3.1 アドバンスト磁束ベクトル制御

0.5Hz 150%トルク，速度制御範囲1：120(力行時0.5～60Hz)を実現するため，アドバンスト磁束ベクトル制御方式を開発した。

アドバンスト磁束ベクトル制御のブロック図を図5に示す。インバータの出力電流を検出し，一次角周波数ω_1で回転するd-q軸上の励磁相の電流i_dとトルク相i_qの電流とに分解する。

安定化補償電圧演算部では，誘導電動機の一次束が所定の値を安定に保つように，d軸(励磁相)の補償電圧V_{cd}とq軸(トルク相)の補償電圧V_{cq}を演算する。また，滑り周波数演算部では，誘導電動機の一次磁束λ_dを演算し，これと励磁相の電流i_d及びトルク相の電流i_qを用いて滑り周波数$\widetilde{\omega}_s$を高精度に演算する。

この演算されたd軸及びq軸の補償電圧V_{cd}，V_{cq}と滑り周波数$\widetilde{\omega}_s$を用いて，d軸及びq軸の一次電圧V_d，V_qと出力周波数ω_1を次式によって制御する。

$$\left.\begin{aligned} V_d &= K_1 \cdot i_d + V_{cd} \\ V_q &= K_2 \cdot i_q + V_{cq} + K_3 \cdot \omega_1 \end{aligned}\right\} \quad \cdots\cdots (1)$$

$$\omega_1 = \omega^* + \widetilde{\omega}_s \quad \cdots\cdots (2)$$

ただし，

K_1 ：d軸分一次抵抗補正ゲイン
K_2 ：q軸分一次抵抗補正ゲイン
K_3 ：励磁電圧(V／f)ゲイン
ω_1 ：出力周波数
ω^*：目標周波数

つまり，モータの一次磁束が所定の値になるように式(1)で出力電圧を制御し，また，誘導電動機の実回転周波数が目標周波数に一致するように式(2)で出力周波数を制御する。

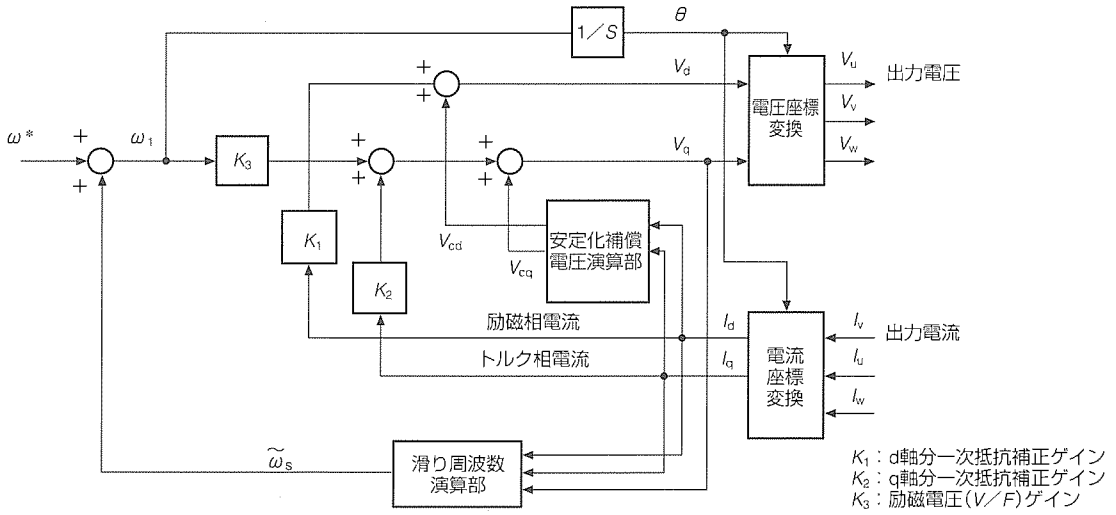


図5．アドバンスト磁束ベクトル制御のブロック図

このアドバンスト磁束ベクトル制御を適用することにより，低周波数域から高周波数域まで安定して高トルクを得ることができ，負荷(トルク)変動に対しても回転数偏差を小さく保つことが可能となった。

3.2 オートチューニング

オフラインオートチューニングは，アドバンスト磁束ベクトル制御で運転するのに必要なモータ定数(**図6**：モータの等価回路参照)をインバータ自身が自動測定し記憶する機能である。定数が未知であるようなモータを使用する場合でも，この機能によってアドバンスト磁束ベクトル制御を行い，十分な性能を得ることができる。アドバンスト磁束ベクトル制御で必要なモータ定数は，モータの温度によって変化する。モータ定数が変化しても安定な制御を維持するために，毎回始動時にモータ定数を自動測定して定数の補正を行うオンラインオートチューニングを開発した。

(1) オフラインオートチューニング

オフラインオートチューニングは，次の3区分で構成される。

(a) R_1(一次抵抗)のチューニング

(b) R_2(二次抵抗)，l_1(一次漏れインダクタンス)，l_2(二次漏れインダクタンス)のチューニング

(c) L_1(一次インダクタンス)のチューニング

R_1は，従来ダブルブリッジや電圧降下法といった抵抗測定試験によって求められていたが，インバータでは，直流電圧Vを印加し，電流iを検出することでV/iから求める。R_2，l_1及びl_2は，従来拘束試験によって求められたが，インバータでは，短時間に低い単相交流電圧を印加し定格電流を流す。そうすることによって滑りSが最大となるため，拘束試験と等価にできる。このときの電力・電圧からR_2，l_1，l_2を計算する。L_1は，モータを無負荷で，定格速度付近で回転させる試験が一般的である。同期速度で回転させることによってR_2/Sが無限大となる。この状態では等価回路における二次側の電流が0となり，また定格電圧を印加しているので一次抵抗の電圧降下分は無視できるため，L_1を計算することができる。インバータでは，アドバンスト磁束ベクトル制御で同期速度付近まで回転させ，励磁電流の誤差が0になるようにM(励磁インダクタンス)を調整しL_1を求める。

(2) オンラインオートチューニング

オンラインオートチューニングは，アドバンスト磁束ベクトル制御運転を行う際の始動時に直流励磁をかけることでモータ定数を求め，オフラインオートチューニングで求めたモータ定数に対して温度補償を行う。オンラインオートチューニング時間はモータによって異なるが，最小約50ms～最大約500msとなる。

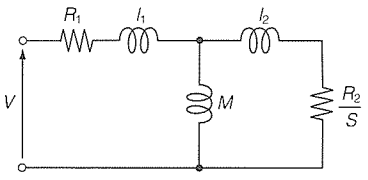
オンラインオートチューニングのブロック図を**図7**に示す。図に示すように，始動時の直流励磁をステップ状に印加し，そのときの実電圧Vと電流iとRISCマイコン内のモータの数学モデル(推定器)から求まる電圧の誤差によってR_1(一次抵抗)とR_2(二次抵抗)を同時同定する。

このR_1とR_2をアドバンスト磁束ベクトル制御で使用することにより，R_1とR_2の温度補正が可能となり，モータ温度に影響されない高精度運転と，超低速までの高トルク・安定運転が可能となる。

3.3 スマートドライバ

インバータの主回路の状態を直接監視し出力波形を制御するスマートドライバ(当社独自の新開発ASIC)を開発し，低速時の回転むらを当社従来比1／2以下に改善した。

従来の汎用インバータでは，制御回路で作成したPWM信号を絶縁してIGBTの駆動信号とした。PWM信号には，IGBTの上下短絡を防止するため，上下のIGBTを共にOFFさせる期間(上下短絡防止期間)を設ける必要がある。この上下短絡防止期間中，出力電圧は負荷電流によって変化するため，指令した設定値どおりの電圧が得られなくなり，電動機の回転が不安定となることがある。特に低騒音型インバータ(高周波インバータ)ではこの影響が顕著となり，従来，負荷電流を基にPWM信号を補正していたが，負荷電流の検出精度により，影響を完全に除去することは困難であった。このため，今回，主回路電位で動作する専用のPWM信号作成用LSI(スマートドライバ)を開発した。このLSIは，制御回路のCPUの電圧指令に応じてPWM信



R_1 ：一次抵抗
R_2 ：二次抵抗
l_1 ：一次漏れインダクタンス
l_2 ：二次漏れインダクタンス
M ：励磁インダクタンス
S ：滑り
$L_1=l_1+M$：一次インダクタンス
$L_2=l_2+M$：二次インダクタンス

図6．誘導電動機の等価回路

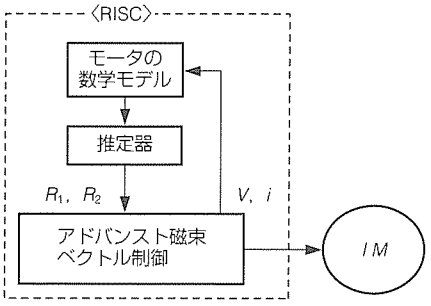


図7．オンラインオートチューニングのブロック図

号を作成するが，電動機の回転不安定現象を抑えるため出力電圧をフィードバックし，PWM信号を補正する。

3.4 性能及び試験結果

(1) S-T特性

図8に，アドバンスト磁束ベクトル制御時の速度－トルク特性例を示す。この例では，0.5から60Hzまでの範囲(1：120)で安定したトルクが得られ，出力トルクに対する回転速度の変動も非常に小さくなっている。

(2) オンラインオートチューニングの効果

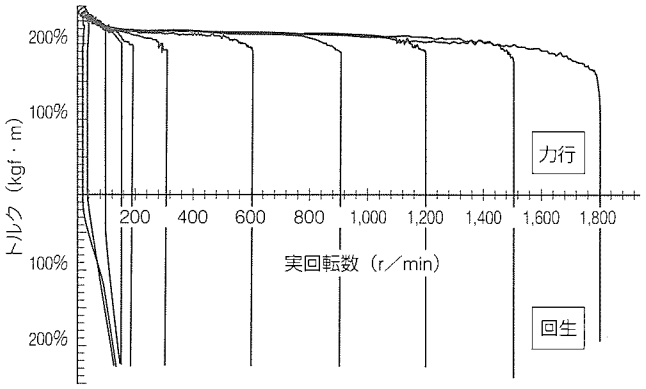


図8．アドバンスト磁束ベクトル時の速度-トルク特性例（モータSF-JR 4P 3.7kWの場合）

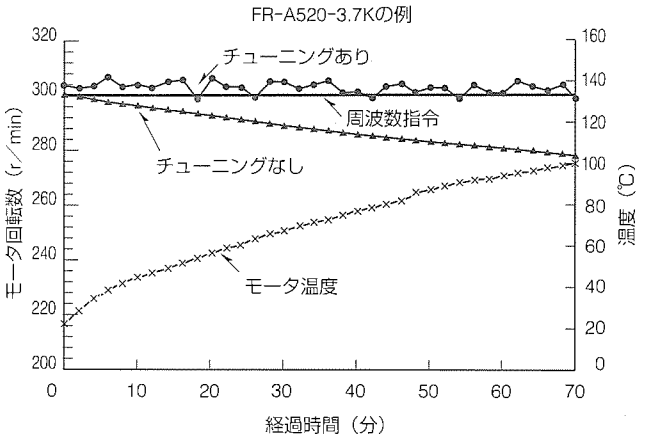


図9．オンラインオートチューニングの効果

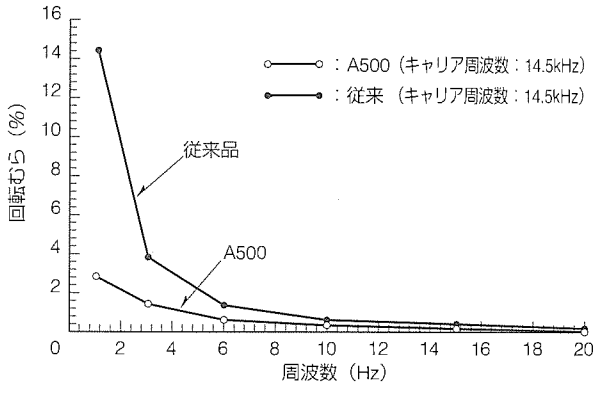


図10．回転むら特性

図9に，オンラインオートチューニングの効果を示す。100%負荷を印加し，モータを300r／minで繰り返し起動停止を行ったときの動作を表したものである。時間の経過とともにモータ温度が約20℃から100℃に上昇するが，オンラインオートチューニングありの場合は，時間経過しても回転速度の低下はない。ところが，オンラインオートチューニングなしの場合は，モータ定数の補正ができないため，インバータの内部で使用しているモータ定数と実際のモータ定数の差が大きくなり，このため滑り補正で求められた滑り周波数の推定誤差が発生し，速度が低下する。

オンラインオートチューニングは，始動時に短時間でモータ定数を検出する方法を採用しているので，始動停止を繰り返す用途では，効果的に作用すると言える。

(3) 回転むら

図10に，回転むらの比較データを示す。低速域において，スマートドライバの効果によって従来に比べて回転むらが低減されている(従来比1／2以下)。

4. 環境適合(Soft-PWM制御)

インバータでモータを駆動すると，キャリア周波数に起因する音がモータから発生する。キャリア周波数が1kHz程度で低い場合には，モータから金属質の耳障りな磁気騒音がした。この磁気騒音を低減するため，従来機種ではキャリア周波数を10～14.5kHzとし，磁気騒音を人の耳に聞こえない周波数域に移すことで低騒音化を図った。しかし，高キャリア周波数化は，騒音という面では良い効果が得られたが，発生ノイズが増加し，課題として他の機器への悪影響，漏れ電流の増加の副作用が残った。そこで，キャリア周波数を上げずに，磁気騒音成分を分散させる“Soft-PWM制御”を開発し，人に優しい音とし，モータ磁気騒音の低減を図った。

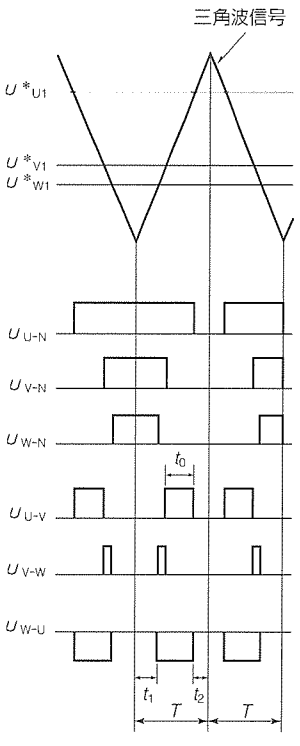


図11．Soft-PWM

三相インバータのPWM制御の実現方法として三角波比較方式がある。**図11**に，指令電圧を一定値とした場合の三角波比較方式による各相のスイッチングタイミングを示す。三角波比較から得られた各相の直流母線負極側N点に対する電圧，及び線間電圧は，図に示すパルス電圧となる。こ

のパルス状の電圧が印加され，この時間平均値が指令電圧の線間電圧値に等しくなる。ここで線間電圧を決めているのは，例えばU-V間の電圧V_{u-v}では電圧が出力されているパルス幅t_0である。このパルス電圧の出力タイミングを変えても出力電圧は同じである。このパルス電圧の出力タイミングを時間的に変える方式，すなわち($t_{11}+t_{12}$)の時間値を保ちながらt_{11}とt_{12}の配分を時間的に変化させる方式がSoft-PWM制御である。この方式により，モータからの励磁騒音を分散させることができる。

Soft-PWM制御の場合と従来の方式の比較を図12，図13に示す。図13からモータ騒音がキャリア周波数の2倍の周波数で極めて高くなっていることが分かる。図12のSoft-PWM制御では，図13と異なり，モータ騒音のピークが分散されていることが分かる。

5. 操作性向上(使いやすさ)

5.1 パラメータユニット

操作パネル及びオプションのパラメータユニットには，パラメータコピー機能を標準装備した。インバータと操作パネルをRS485で接続し，専用の通信プロトコルを使用し，インバータに保存されているパラメータ情報を操作パネルに転送し，操作パネル内のEEROMに記憶可能とした。万一インバータの交換が必要になった場合に，本体を交換後，操作パネル(又はパラメータユニット)に記憶しておいたパラメータ情報をインバータに書き込むことにより，パラメータの復旧が迅速にかつ確実にでき，インバータを素早く立ち上げることができる。また，パラメータユニットにはバックライトLCDとテンキー入力方式を採用し，日本語，英語，ドイツ語，フランス語，イタリア語，スペイン語，スウェーデン語，フィンランド語の8か国語表示を可能とした。

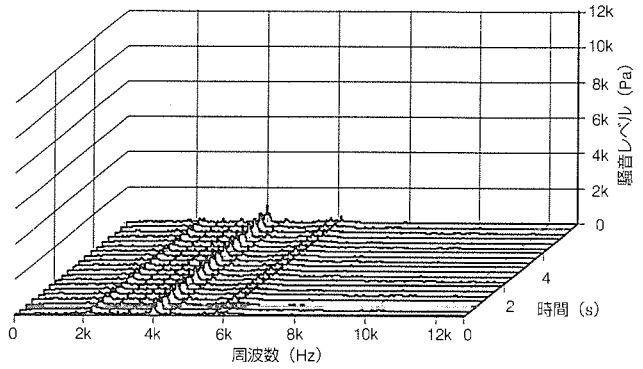


図12. モータ騒音データ例（Soft-PWM運転）

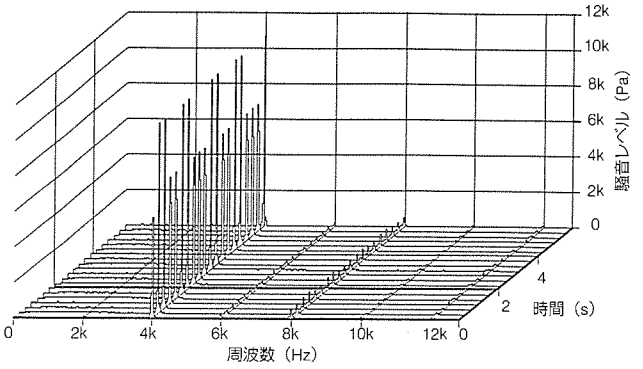


図13. モータ騒音データ例（非低騒音運転）

5.2 端子台の脱着方式，冷却ファンのカセット交換

図14に脱着式制御端子を示す。制御端子を脱着方式とすることにより，配線を外すことなくメンテナンスが可能となり，客先での作業性を向上させることが可能となった。

汎用インバータは半永久的な寿命を持つ電子部品で構成されているが，冷却ファンでは，機構部品のため寿命があ

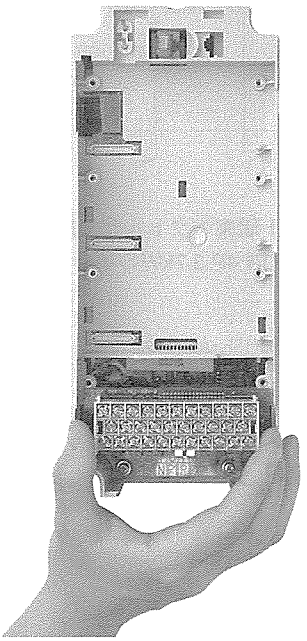


図14. 脱着式制御端子

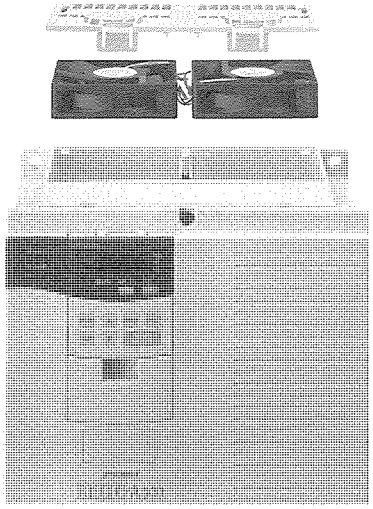


図15. 冷却ファンカセット

り，メンテナンスが必要となる。このため，主回路素子の温度を検出し，一定温度以下の場合冷却ファンを停止させる制御を行い，冷却ファンの長寿命化を図っている。また，冷却ファンを交換する必要が生じたとき，図15に示すように，簡単に冷却ファン交換ができるような構造とした。

5.3 セットアップソフトウェア

セットアップソフトウェアを準備し，短時間での立ち上げを可能とした(表2)。

6. グローバル対応

6.1 オープンネットワーク

世界の主要ネットワークに接続可能とした(表3)。

6.2 海外仕様・安全規格への標準対応

240V／480V電源，入出力端子のシンクとソース切換えなどの対応を可能とし，北米や欧州の安全規格(UL，cUL，EN)にも標準品で対応可能とした。

表2．セットアップソフトウェア“FR-SWO-SETUP-WJ”の仕様

動作環境	動作マシン：DOS／V，PC98，AXなどWindowsが動作する機種 Windows　：Windows95，Windows3.1 メモリ　　：8Mバイト以上（推奨16Mバイト） HD容量　：16Mバイト	
対象インバータ	FREQROL-A500，FREQROL-E500	
主要機能	パラメータ設定	約300のパラメータ設定及び編集
	ファイル	パラメータ，運転データのファイル保存，印刷
	モニタ	各種モニタ情報の表示（データ表示，メータ表示，オシロ表示など）
	テスト運転	外部シーケンスレスでの試運転，オートチューニング
	診断機能	故障診断，健康診断

表3．FREQROL-A500のネットワーク

ネットワーク	オプション形名	プロトコル	規格	通信速度 子局台数・最長伝送距離
Profubus-DP	FR-A5NP	Profibus準拠	RS485	9,600bps～12Mbps
			9ピンDsub	126台1,200～100m
Device Net	FR-A5ND	CAN準拠	RS485	125～500kbps
				64局500～100m
CC-LINK	FR-A5NC	HDLC準拠	RS485	156kbps～10Mbps
			端子台 ツイストペアケーブル	1局専有：42台 1,200～100m
Modbus plus	FR-A5NM	Modbus社準拠	RS485	1Mbps
			9ピンDsub	32台
RS485	FR-A5NR	三菱専用プロトコル	RS485	300bps～19.2kbps
			端子台	32台500m

7. むすび

以上“FREQROL-A500シリーズ”の概要，特長，及びそれらを支える新技術について紹介した。アドバンスト磁束ベクトル制御，オンラインオートチューニング機能及びRISCマイコンの採用で，駆動性能が大幅に向上したこと，またSoft-PWM制御採用による耐環境への取組を述べた。また，脱着端子，冷却ファンのカセット方式，冷却ファンのON／OFF制御の採用によってメンテナンス性を大幅に向上させた。

このような特長を持ったFREQROL-A500シリーズが，汎用インバータの適用範囲を広げていくことを切に望んでいる。

当社では，需要家各位のご指導とご協力を得ながら，今後とも汎用インバータの“性能”“機能”“使いやすさ”の向上と“環境適合”“グローバル”への対応，高信頼性の追求を図るため，より一層技術開発に取り組んでいく所存である。

スポットライト

三菱ネットワークセキュリティ MELWALL3000シリーズ

企業ネットワークのインフラとしてインターネットを活用するいわゆるイントラネットは，着々と浸透しつつあり，さらに，モバイルコンピューティングやエクストラネット構築へと広がりを見せています。その反面，オープンな環境であるインターネット／イントラネット上では，不正侵入やデータの盗聴，改ざんなどの脅威が常にあることを認識していなければなりません。このため，システム構築の際には，細心のセキュリティ対策が不可欠です。インターネットを企業の情報インフラとして活用するためにネットワーク上に構築する仮想的な経路のことをVPN(Virtual Private Network)と呼びます。三菱ネットワークセキュリティMELWALLシリーズ(以下"MELWALLシリーズ"という。)は，暗号技術を用いて安全なVPNを構築し，第三者の盗聴や不正アクセスからユーザーの大切な情報を守るネットワークセキュリティ製品です。

MELWALL シリーズには，以下の製品があります。

(1) 既存ルータの直下に配置し，ネットワーク単位のVPNを構築する"暗号アダプタMELWALL A3000"

(2) 12ポートの10BASE-Tハブ型で，端末単位のVPNを構築する"集線型暗号装置MELWALL H3000"

(3) モバイル端末やSOHOなど，遠隔からのダイヤルアップIP環境をサポートする"暗号ドライバソフトウェア(WAN対応) MELWALL P3000"，及びLAN上の端末をサポートする"暗号ドライバソフトウェア(LAN対応) MELWALL P3000CL"

(4) かぎ(鍵)管理などをリモートから実施するための"鍵管理ソフトウェアMELWALL Mgr"

特　長

- 既存のシステムへの導入が容易
- モバイル環境も含め，幅広いセキュリティニーズに対応
- 暗号通信と平文通信との混在が可能(特例通信)
- 世界トップレベルの暗号強度

暗号アダプタMELWALL A3000

MELWALLの仕様

項　目	A3000／H3000	P3000／P3000CL
対応機種	—	DOS／V(PC／AT互換)機 NEC PC9800シリーズ
動作OS	—	Windows95 Windows NT 4.0(P3000のみ)
暗号化対象プロトコル	IP，IPX	IP
暗号アルゴリズム	MISTY(鍵長128ビット)	
VPN	最大32(IPのみ)	最大8
特例通信	最大64(IPのみ)	最大128
ネットワーク管理	SNMP(H3000のみ)	—
鍵の設定変更	マニュアル設定又はMELWALL Mgrからのリモート配送	
寸法・質量	A3000：(W)203×(D)240×(H)41(mm)，2.5kg H3000：(W)430×(D)240×(H)43(mm)，3.5kg	—
電源条件	AC100V，50／60Hz，20W	—

侵入監視装置　（特許　第1773639号，特公平4-45879号）

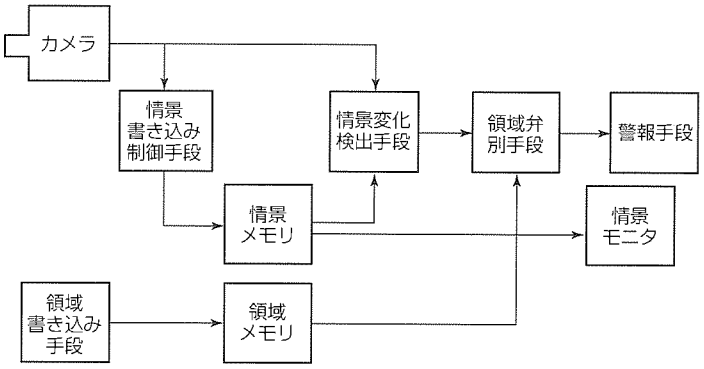
発明者　　池端重樹，磯貝文彦

この発明は，プラント，工場又は建造物などの，特定の禁止領域への侵入を監視する装置に関するものである。

従来の侵入監視装置では，複雑な形状の領域，例えば特定機器類の周辺や，複数の立入禁止区域などへの侵入のみを選択的に監視するのが非常に困難であった。

この発明は上記のような欠点を除去するためになされたもので，図にこの発明のブロック図を示す。情景メモリにあらかじめ記録された過去の情景情報があり，これとカメラから得られる新しい情景情報を情景変化検出手段に入力し，２枚の画像の演算処理を行い，新しい画像の変化分を検出する。情景書き込み制御手段は，上記情景メモリの内容を所定の規則で書き換えるための制御を行う。領域メモリには領域書き込み手段を介してあらかじめ侵入禁止領域を書き込み，その内容は領域弁別手段に送出される。領域弁別手段には情景変化検出手段からの出力信号が印加されており，もし情景変化検出手段の出力信号が領域弁別信号の示す領域内に含まれておれば，警報手段を駆動する。

以上のように，この発明の侵入監視装置は，侵入禁止領域を任意に指定して書き込むことができるので，情景内の特定選択領域への侵入監視が可能となり，また設定時や移設時の調整がユーザー側でも簡単に行える等の効果がある。



暗号化方式及び暗号化方法　（特開平4-365240，米国特許　第5,488,661号）

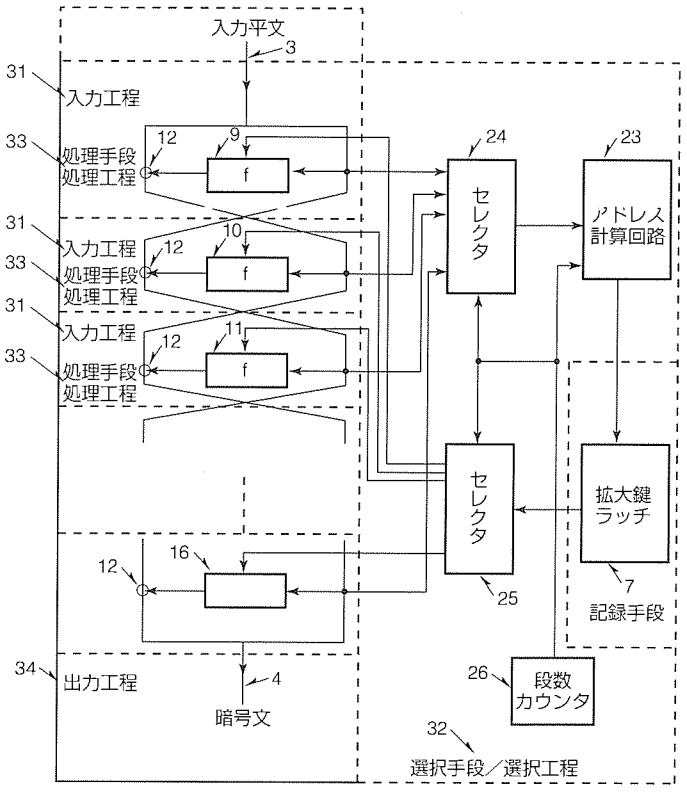
発明者　　松井　充

この発明は，情報通信の分野で，ランダム性の高い暗号化方式を得ることを目的としている。

従来の暗号化方式は各処理ブロックに入力される拡大かぎ(鍵)のアドレスが固定されており，このため，選択平文攻撃が可能な通信路では，盗聴者が拡大鍵をすべて求めることができるという問題点が指摘されている。

この発明は，以上のような問題点を解消するためになされたものである。図はこの発明による暗号化回路である。データランダム化部において拡大鍵を各アドレスに記録した拡大鍵ラッチ(7)を設け，拡大鍵の一つをパラメータとして入力し，このパラメータを用いて入力情報を暗号に変換して出力する処理ブロック(9，10，11～16)において，上記処理ブロックに入力される拡大鍵を一つ選択するために，アドレスを平文又は入力情報に依存して変化させるセレクタ㉔を備えた。

平文又は入力情報に依存して暗号鍵又は拡大鍵の内容を変化させることができるので，高いランダム性を得ることができ，これによって解読の危険性を減少させることができる。



指紋照合装置　（特許　第2059309号，特公平7-85261号）

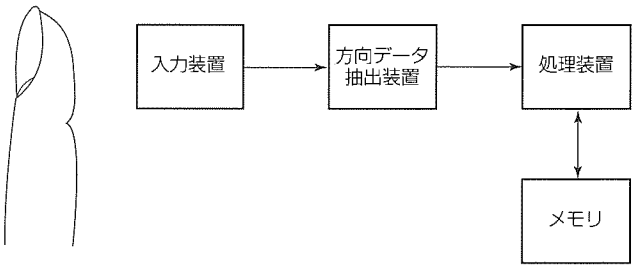
発明者　笹川耕一

この発明は，特定領域への出入りや情報端末へのアクセス等に際して，個人を識別又は照合するために利用する指紋照合装置に関するものである。

従来の装置は，被験者がディスプレイ上で登録指紋に入力指紋を重ね合わせる必要があった。このため，登録指紋が被験者に観察され，この登録指紋が模造される危険があった。

この発明は，上記の欠点を解消するためになされたもので，図にブロック接続図を示す。指紋の登録時には，入力装置から取り込まれた登録すべき指紋から，方向データ抽出装置によって小領域ごとの指紋隆線の方向データを抽出する。方向データを，処理装置によって抽出された特徴データとともに，ID番号と対応させてメモリに記憶しておく。入力指紋との照合時には，方向データ抽出装置で入力指紋の方向データを抽出する。これと，被験者によって入力されたID番号によって読み出された登録指紋の方向データとを比較し，入力指紋と登録指紋の位置ずれを自動的に検出し，両指紋の位置合わせを行う。

この構成により，両指紋の位置や向きを自動的かつ確実に一致させることができ，指紋の照合作業が迅速に行える。



三菱電機技報　72巻5号　1998年5月22日　印刷
（無断転載・複製を禁ず）　1998年5月25日　発行
編集人　鈴木　新
発行人　鈴木隆二
発行所　三菱電機エンジニアリング株式会社
ドキュメント事業部
〒105-0004
東京都港区新橋六丁目4番地9号　北海ビル新橋
電話（03）3437局2692
印刷所　菱電印刷株式会社
発売元　株式会社　オーム社
〒101-0054
東京都千代田区神田錦町三丁目1番地
電話（03）3233局0641
定価　1部735円（本体700円）送料別
お問い合せ先　giho@hon.melco.co.jp

スポットライト

メッセージ暗号ソフトウェア MistyGuard“CryptoSign”

インターネットやイントラネットの発展とともに，電子メールは，今日のビジネスに欠かせない情報伝達手段となりました。しかし，オープンな環境で使われる電子メールには，常に第三者からの脅威にさらされる不安があります。

- だれかが差出人に成り済まして送ったのでは
- 途中で内容が書き換えられているのでは
- 途中でだれかに内容を読まれているのでは

こうした不安を，三菱電機は，世界トップレベルの暗号技術で解決しました。メッセージ暗号ソフトウェアMistyGuard“CryptoSign”は，既存の電子メール環境に簡単にセキュリティ機能をプラスすることができる製品です。

特　長

1．ディジタル署名と暗号化によるセキュリティの向上

“ディジタル署名”で送信者と文書内容の確認をし，“暗号化”で受信者のみが文書を読めるようにします。これにより，成り済まし，改ざん，盗聴，といった事故を未然に防ぐことができます。

2．認証局と連携したユーザー認証が可能

三菱認証サーバシステムMistyGuard“CERTMANAGER”で発行した認証書を使用することにより，セキュリティレベルの高いユーザー認証を実現できます。

3．業界標準のS／MIME準拠

MistyGuard“CryptoSign”で作成するディジタル署名／暗号化メッセージは，業界標準であるS／MIMEに準拠しています。

4．既存メールシステムとの連携

添付ファイル形式を利用しているので，任意のメーラーを使ってセキュアメールを実現できます。また，MAPI(Messaging API)連携によるメール送信も可能です。

5．ファイルの暗号化にも対応

ファイルの暗号化機能によって，ファイルのFTP転送時に暗号化したり，機密情報を暗号化して保存するなど，多様な用途に使うことができます。

6．管理ツールを用いた一括管理が可能

MistyGuard“CryptoSign”を多人数で使う場合には，全員の認証書やアドレス帳の管理を，CryptoSign管理ツールを用いて一括して行うことができます。

暗号アルゴリズムMISTY

画面イメージ

MistyGuard “CryptoSign” の仕様

ディジタル署名	メッセージ縮約(ダイジェストの生成)	SHA-1	動作環境	対応OS	Microsoft Windows95日本語版 Microsoft Windows NT4.0日本語版 Microsoft Windows NT3.51日本語版 (Service Pack 5以上)
		MD5			
	ディジタル署名	RSA(鍵長：1,024ビット)			
暗号化	共通かぎ(鍵)暗号	MISTY(鍵長：128ビット)		対応機種	各社PC／AT互換(DOS／V)機
		DES(鍵長：64ビット)		必要メモリ容量	16Mバイト以上(Windows95の場合) 20Mバイト以上(Windows NT Workstationの場合) 28Mバイト以上(Windows NT Serverの場合)
		DES-EDE3 (鍵長：192ビット)			
	共通鍵の配送方式	RSA(鍵長：1,024ビット)		必要ディスク容量	約10Mバイト以上

MD5　：Message Digest 5
SHA-1　：Secure Hash Algorithm 1
RSA　：Rivest，Shamir，Adlemanが考案した公開鍵暗号アルゴリズム
MISTY　：三菱電機が考案した共通鍵暗号アルゴリズム
DES　：Data Encryption Standard
DES-EDE3：DES Encryption Decryption Encryption 3（Triple DES）