昭和37年9月15日第三種郵便物認可　三菱電機技報　76巻4号(通巻851号)　2002年4月25日発行(毎月1回25日発行)

Changes for the Better

# MITSUBISHI

# 三菱電機技報 Vol.76 No.4

## 特集「情報セキュリティ」

2002 4


ISSN 0369-2302 CODEN:MTDNAF

# 三菱電機技報 Vol. 76 No.4 2002


目　次



**表紙**

**暗号技術の今昔**

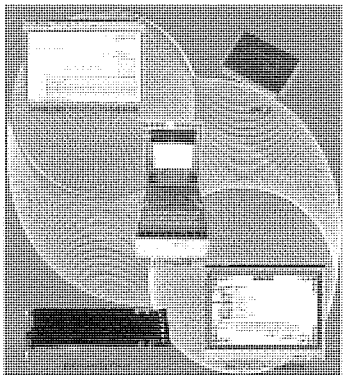
中央の写真は，第二次世界大戦当時ドイツ軍が使用していた暗号器"エニグマ(謎)"である。

周辺の写真は，三菱電機の暗号技術"MISTY"に代表される"現代暗号技術"の粋を応用した三菱電機の情報セキュリティ製品の例である。

左上から時計回りに，三菱電子署名ソフトウェア"MistyGuard＜SignedPDF＞"のサンプル画面，暗号LSIの例，セキュアストレージシステムが発行する保管証明書のイメージ画面，耐タンパー(1)セキュアボードとなっている。

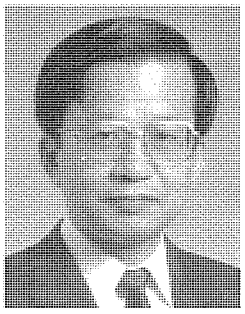
これらの技術の詳細については，それぞれ本編で紹介している。関連ホームページ http://www.security.melco.co.jp/ もご覧ください。

(1)タンパー：物理的な改ざん行為



巻/頭/言

# 情報セキュリティ技術を有効利用するには



東京大学教授 工学博士
生産技術研究所

今井秀樹

不正アクセス，ウイルス，サイバーテロと情報システムに対する脅威は連日のように新聞紙上を賑わし，これに対処するための情報セキュリティ技術の重要性は，言い尽くされているかに見える。しかし，現状で情報セキュリティ技術が有効に利用されているかといえば，多くの場合，答えは否定的にならざるを得ない。

その一つの理由は，現在の情報セキュリティ技術が必ずしも利用者に安心感を与えるものではないことである。例えば，パソコン画面に表示された重要な文書にクリック一つで電子署名をすることに不安を感じる人は少なくない。一方，幾ら安全であっても，使いにくいシステムは敬遠されるか，さもなければ誤用される。情報セキュリティ技術は，一般に理解が難しいものであるし，またそれを用いることにより，システムの使いやすさを損なうという面も持つ。これらの点を改善していくためには，結局，人という要素をより重視して研究開発を進めていくべきであろう。筆者が提唱しているヒューマンクリプトも，その方向を目指すものである。

情報セキュリティ技術が適切に利用されないもう一つの理由は，情報システム開発における競争の厳しさである。多くの情報システムは，少しでも早く開発しなければ，競争に負けてしまう。このため，危険性の多いシステムを市場に投入することも少なくない。確かに，システムによっては，当初から強いセキュリティを持たなくても，問題が生じた場合に対処すれば済むこともある。しかし，適切な情報セキュリティ技術を用いないことで致命的な損害を受けた例は，これまでにも決して少なくない。個々の損害がそれほど大きくない場合でも，セキュリティの弱いシステムが普及して，利用者がそれに慣れてしまった場合，強いセキュリティを持つシステムを利用者に受け入れてもらうのは難しい。これは，結局社会全体に不利益をもたらす。したがって，どのようなシステムであっても，当初から情報セキュリティを十分に考えておくことが重要である。その上で，システムの特性に応じて適切な情報セキュリティ対策を施すべきなのである。

とはいえ，放置しておけば，危険なシステムが安全なシステムを駆逐する傾向のあることは否定できない。安心できるネットワーク社会を構築するためには，公的な支援によって情報セキュリティ技術の開発環境を整える必要がある。特に，情報セキュリティ評価は，適切な情報セキュリティ対策のために必す(須)であるが，高度な専門性を要し，大きなコストも掛かる。幸い，この面で公的な機構が，現在幾つか構築されている。電子政府のための暗号技術評価プロジェクト“CRYPTREC”もその一つであり，情報セキュリティ対策のかなめである暗号技術に関し，信頼できる情報を提供している。しかし，セキュリティ評価は継続的に行う必要があり，CRYPTRECを恒久的な公的機関に発展させていくことが今後の課題である。

もとより，情報セキュリティは技術だけで達成できるわけではない。法・制度，教育・啓発，管理・運用など，多くの面から総合的に対処していく必要がある。しかし，法や制度で人を厳しく縛るより，技術でできるところは技術で対処するのが，人に優しい情報化社会を作る道である。この意味でも，情報セキュリティ技術は今後更に重要性を増していくことは疑いない。

巻頭論文

# 暗号・情報セキュリティの動向



小野修一* 小松田敏二** 竹田栄作***

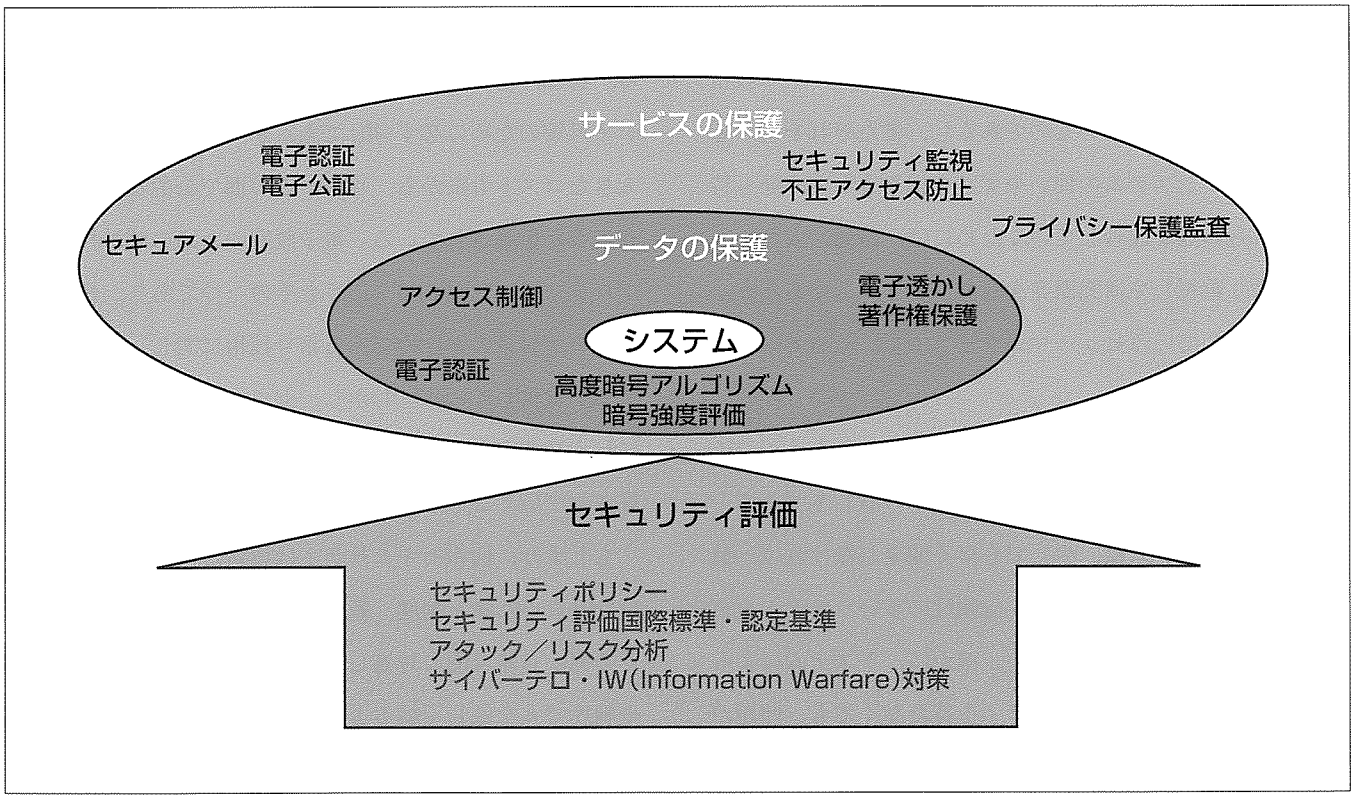
**要　旨**

インターネットに代表されるネットワークと携帯電話が結び付いて文字どおり地球規模のデジタル社会が出現し，社会制度や公共の情報基盤も，それを反映した形態に変化しつつある。今後のデジタル社会をいかに安全なものにしていくかは，国家・社会の基盤にとってその存続にかかわる重大問題であり，企業にとっては死命を制するビジネス課題になっている。それらを支える情報基盤の核となるものが，暗号を中心とする情報セキュリティである。

現代において，なぜ　暗号・情報セキュリティが必要であるか，その役割と意味は何か，どのような応用分野，課題があるかを展望する。さらに，暗号とは何か，その安全性の意味とは何か，コンピュータや通信のデジタル技術とどのような関連にあるのかを，歴史的背景と近年の動向を踏まえて言及し，現代暗号の成り立ち，情報セキュリティの適用形態，三菱電機における技術的活動について触れる。

今後の動向として次に，二つの特徴的な話題を取り上げる。携帯電話の世界的普及，インターネット接続機能の装備により，現在のインターネットのユーザー規模をはる(遥)かにりょうが(凌駕)した音声交信可能なモバイルインターネットの出現が予測される。モバイルインターネットが潜在的に持つ安全上のぜい(脆)弱性を克服するためには，暗号・情報セキュリティの技術はより高度なものが求められる。

また，将来的な量子コンピュータの出現等，分子レベルに迫る半導体・光素子・通信の技術の先に，現在のデジタル暗号によるセキュリティ基盤の安全性の限界が論じられている。デジタル社会の安全性の確保には将来を見据えた技術の追求が要請されており，その代表的なものとして，量子力学の原理，光技術，デジタル技術を統合した量子暗号がある。三菱電機は，2000年9月に国内初の量子暗号の実証実験に成功し，早期の実用化を目指している。




**デジタル社会に向けた暗号・情報セキュリティ技術**

暗号・情報セキュリティ技術をユーザーの視点から見ると，データを保護するためのもの，サービス機能を保護するためのもの，これら保護機能・仕組みを評価し保証するためのものに大別される。


*情報技術総合研究所長　**インフォメーションシステム事業推進本部情報セキュリティ推進センター長　***情報技術総合研究所 情報セキュリティ技術部長

## 1. 安全なデジタル社会

過去の日本の社会，特に国内においては，“水と安全はタダ。”という生活感覚があったものと思われるが，デジタル化された国境のない情報化社会においては，安全性を確保するためにはコストを要することを，新たに認識することは極めて重要である。

セキュリティとプライバシーが確保されて初めて，本格的な情報化推進が行われるであろう。最高の品質の暗号・情報セキュリティをいかに広く多数の人々が享受することができるかが，これからのデジタル社会における安全性の重要なかぎ(鍵)になるであろう。

### 1.1 なぜ 暗号か？

いわゆる古典・近代暗号の時代から別れ，現代の暗号・情報セキュリティの形が初めて表に現れたのは，1970年代と位置付けられている。同時に次の三つのパラダイム変化が起きたと言われる[1]。

(1) 従来，軍事外交の特定組織内に限定して秘密り(裡)に使用されていた暗号が，インターネットに代表されるデジタルネットワーク社会の信頼関係を築くための共通基盤技術となった。同時に，学問上及び商用の公開の場においても研究開発が行われ使用評価される技術となった。

(2) 機能面から見ると，情報秘匿を主目的としていた暗号機能に，人・物・情報の真正性を保証し信用を付与する機能が加わった。言い換えると，情報財流通促進するための認証機能，すなわち署名・改ざん防止機能を持つに至った。

(3) デジタルコンピュータによ(拠)ることを前提とするようになった。すなわち，コンピュータによる暗号化(秘匿)・復号，署名・検証の高速な実現を行う。不正な解読・改ざんに対する安全性評価としてコンピュータによる計算量を尺度とする。解読に要するコンピュータの計算量が解読困難な膨大なものとなるように，暗号装置を設計する。

**暗号の役割**

暗号・情報セキュリティの現代的使命は以下に要約されることになる。

(1) 情報化社会で，個人の権利を守り，法人の権利を守り，国家・社会を安全なものにする。

(2) 信頼関係を築く公開的共通基盤の核となる。

(3) 人・物・情報の真正性保証，信用付与，情報財流通促進の認証を与える。

(4) IT(Information Technology)技術による実用化，具現化が行われる。すなわち，センサ・制御・映像＋通信・コンピュータ＋半導体チップ の技術に融合した安全保持の機能として実装される。

### 1.2 マーケット動向

**応用分野**

我々は，コンピュータがあらゆる所に使用される時代にいよいよ近づいている。コンピュータはより安価に小型になり，電子レンジのような家電から電子誘導ミサイルのような兵器に至るまで，あらゆる電子機器に組み込まれ，ネットワークによる接続の機能が与えられつつある。コンピュータは，IT化という旗印の下，以下のようなマーケット分野を含むすべての業務プロセスに組み込まれていく動向にあり，その結果，従来はオフィス内の会話や書類の中にとどまっていた機微な取扱いを要する情報が，いまやコンピュータに搭載され公衆のネットワーク上に流されて，遠方の第三者による盗難，改ざん，濫用の対象にされる危険性を増大させている。これを防止・軽減するためには，セキュリティ及びプライバシー保護の機能が求められる。

**セキュリティ対象となる(Potential)マーケット分野**

(1) 交通・運輸分野：ITS(Intelligent Transportation System)／ETC(Electronic Toll Collection system)

(2) 高度家庭通信システム：Homeネットワーク統合(衛星，地上波，ケーブル，インターネット，電話網)

(3) エネルギー分野：電力自由化・省力化，電力CALS等によるIT化推進

(4) 携帯電話・端末の普及とモバイルインターネット

(5) マイクロプロセッサに代表されるコンピュータ：ネットワーク化，小型廉価，マルチメディア機能の組み込み，コモディティ化

(6) 社会的に重要(Critical)なシステム： 行政府，防衛，金融，ヘルスケア医療における情報ネットワーク化，情報公開(インターネット)の推進

### 1.3 課 題

事実上すべての機器やIT化された業務プロセスが地球規模のネットワークに接続される日がそう遠くない時期に到来する可能性は高いとみなされ，これが含意するところは極めて意味深いものがあると思われる。例えば，地球の反対側にいる電子的侵入者がある飛行場のセキュリティシステムを無効にしたり軍事防衛施設のゲートを開錠したりすることが可能になること，高速道路を100km以上の速度走行する車のエンジンを停止させ多数の車の衝突事項を引き起こし交通麻ひ(痺)を起こすことができるようになるのであろうことが予測される[2]。社会・公共インフラの変革に伴い，システムIT基盤の安全性・信頼性が求められることは必す(須)である。

社会・公共システムIT基盤の安全性，信頼性を支える要件を次に示す。

(1) 高度セキュリティ(日本の国家・社会として，安全のフレームワーク)

(2) センサ・制御・映像・通信・ITに融合したセキュリティ

(3) インターオペラビリティ

(4) 国際的セキュリティ評価基準の形成と対応(ISO/IEC

JTC1 IS15408，IS17799他）

## 2. 暗号と情報セキュリティ

### 2.1 暗号とは

戦争で暗号が使われた最初の記録が現れるのは，紀元前ジュリアス・シーザーのガリア戦記である。シーザーが，敵に包囲され降伏の瀬戸際にあったキケロにメッセージを送ったことが述べられている[3]。シーザー暗号がいかなるものであったかは，紀元後2世紀にスエトニウスによって著されたシーザーの伝記に記録されている。それによれば，皇帝シーザーは，以降の例に示すように，元の文をその各文字ごとにアルファベットの順位に従って3文字ずつずらしたということである。

シーザー暗号例：

- 平文　veni（来た）　vidi（見た）　vici（勝った）
- 暗号文　YHQL　YLGL　YLFL
- 平文アルファベット
  abcdefghijklmnopqrstuvwxyz
- 暗号アルファベット
  DEFGHIJKLMNOPQRSTUVWXYZABC

暗号においては，元の文を平文（ひらぶん），暗号化された文を暗号文，また，通常のアルファベットを平文アルファベット，文字の位置が置換されたアルファベット（上記では3文字分シフト）を暗号アルファベットと呼ぶ。現代の言い方に従うと，ここで文字をシフトないしは文字を置き換えるという手続きをアルゴリズム，シフト文字数（ここでは3）又は置き換えパタン（ここでは平文アルファベットと暗号アルファベットの対）を鍵という。

図1では，送信者は，平文“veni（来た）vidi（見た）vici（勝った）”を3文字シフトし暗号文“YHQL　YLGL　YLFL”に変換して送ることで盗聴を防ぎ，一方，受信者はこれを3文字戻して復号し送信された元の平文を得ることができる。

これら平文，暗号文，アルゴリズム，鍵という暗号の基本概念は紀元前使われたシーザー暗号においても現代のデジタル暗号においても共通であり，暗号の安全性は，この中で特に鍵を送信者と受信者以外には秘密にしておくことによって保たれる。すなわち，暗号を破る，解読するという行為は，現代では，アルゴリズムは公開という前提の下，平文及び暗号文のデータを入手した第三者（送信者・受信者以外の）が，秘密にされていた鍵を見出すということを意味する。逆に，この第三者による鍵の見出しにくさ，すなわち解読に必要とする時間ないしは解読に要した暗号文及び平文のデータ量の多寡が，暗号の安全性を測る尺度となる。良い暗号とは，この安全性が高いことに加え，鍵を保有する送信者による暗号化並びに受信者による復号化が効率良く行えることが条件となる。鍵を持たない敵が暗号化されたメッセージが読み解けない，又は読み解くのに膨大な日数を要することが必要である一方，シーザーとキケロが暗号化・復号化に手間取ってはならない，瞬時に行えなくてはならないのである。

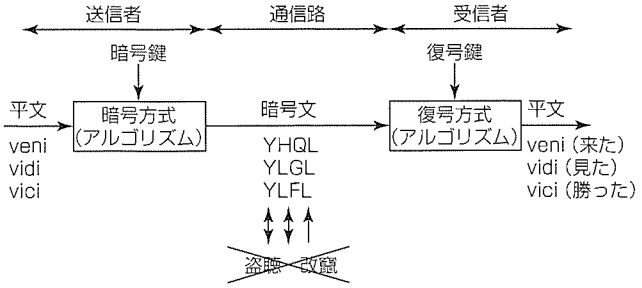



図1．暗号

### 2.2 暗号解読とコンピュータ・通信

第二次大戦中ドイツ軍が使用した通信用暗号機は，エニグマEnigmaという名前であった。これに対する英米共同の無線傍受による情報収集に基づくエニグマ解読作戦は，ウルトラUltraというコード名で呼ばれていた。ウルトラは連合国の対独勝利に多くの貢献をなした。大西洋において，ウルトラによってUボート（ドイツ海軍潜水艦）による攻撃沈没を免れた連合国側船舶は三百隻にのぼると言われている。英米によるエニグマ暗号解読の事実は，大戦中のみならず戦後も長く秘密に保たれていて'70年代に入って初めて公になった[5]。

ウルトラ活動の中核は，ロンドンの北80kmブレッチェリーパークに第二次大戦中置かれた政府暗号学校と称された施設にあった。ブレッチェリーパークでエニグマ暗号解読への突破口を開いたのがアラン・チューリングであった。チューリングは，ブレッチェリーパークに来る前，'36年に“計算可能数について”という論文を発表して，今日のデジタルコンピュータの理論モデルを作り上げていた。チューリングと彼の率いる解読チームは，エニグマ暗号機のメカニズムを解明し，最初の原始的コンピュータとも言うべきエニグマ解読装置を作り上げた。これが稼働し始めた'40年4月以降，英米はドイツの暗号通信を読むことが可能になり，ウルトラ作戦が開始された。最初のコンピュータは暗号解読機であったという事実は，両者の不可分な関係を表すものとされている[3]。

計算に関するチューリング理論は，現代の暗号解読の基盤となったが，現代デジタル暗号の初めとなったDES暗号Data Encryption Standardの基本的アイデアは，通信に関する情報理論の創始者シャノンによって与えられた。シャノンは，'49年“秘匿システムの通信理論”において，'70年代にDES暗号として出現するものの安全性根拠（エントロピーという不確かさに対する確率分布の数学的関数の概念で与えられるもの）とアルゴリズム構成法に関するアイデアを述べている。この論文自体も，防衛軍事にかかわ

るものとして，当初しばらくの間は限定された範囲にのみ知られていた。

### 2.3 現代暗号

(1) DES

'73年5月15日，米国の国家標準規格局The National Bureau of Standard(現在は商務省に属するNIST：National Institute of Standards and Technology)は，連邦政府調達システム用の暗号公募を行った。これが，今日まで最も多く使われてきたといわれるDES暗号の開発につながり，現代暗号として定義される最初のものとなった。

現代暗号と古典暗号との相違比較を次に示す。

古典暗号の世界は，

- 暗号の歴史は人類の歴史と同じ長さ
- 軍事外交目的の非公開技術
- 参加者限定の1対1通信を前提
- 文字の置換を中心とする変換処理

であり，現代暗号の世界は，

- 本格的な開かれた研究は'70年代から
- プライバシー保護目的への利用
- 不特定多数が参加するネットワーク型指向
- デジタル信号の変換処理
- 計算量理論を用いた安全性評価

である。

現代暗号の嚆矢(こうし)DESはIBMによって開発された。当初LUCIFERという名前で出されたものに米国の国家安全保障局National Se-curity Agencyが評価に介在し変更が加えられたものと言われている。DESはまず'75年3月17日に米国連邦政府登録暗号として発表され，その後'77年1月15日に連邦政府のunclassified(外交防衛軍事等の秘匿向けではない)システム向けの標準として採用された。その後5年ごとに連邦政府標準としての見直しが行われ，約20年間事実上国際的標準の位置にあったが，暗号解読法の進歩で安全性の強度が低下したことにより，'99年10月25日にTriple-DES(鍵の長さを3倍にしてDESを三重にかける)に置き換えられた。

(2) 現代暗号の解読

DESに代表される暗号に対する有力な解読法は，鍵総当たり法，差分解読法，線形解読法の三つが挙げられる。初めの二つの解読法は既にDES設計時に考慮されていたと言われている。3番目の線形解読法の発明とその実証実験は，三菱電機の松井による。三菱電機における暗号・情報セキュリティに対する活動もここから始まっている。暗号解読，安全な暗号システムの設計と開発，安全性の評価は三位一体の技術として考えられ(図2)，我々は，そのコンセプトの下，MISTYを始めとする暗号アルゴリズム，それらの情報セキュリティシステムとしての実装，暗号・情報(セキュリティ)システムに対する解読・攻撃の評価技術の開発を行っている。

(3) 適用：背景と形態(情報セキュリティの重要性)

'91年1月に開始された湾岸戦争では，米軍の米国本土の基地とサウジアラビア駐留の部隊との通信の25%がインターネットを経由していた。しかも現在では信じ難いことであるが，インターネット上で平文による通信を行っていたと言われている。"百万$支払えば米国とサウジアラビアを結ぶ米軍の兵站情報ネットワークを大混乱に陥れてやってもよい"というオランダのハッカーグループの申し出にもしイラクのフセインが応じていれば，湾岸戦争における米国の鮮やかな勝利はなかったかもしれない。簡便にして強力な有用性に反比例して，インターネットは安全性に関する脆弱さを抱えたものであった。湾岸戦争後，米国は国家を挙げてこの対策に取り組んでいる[2]。

また，米国においては，2001年度末に，インターネットによる購買者層の一位が女性に移ったという調査統計が出ており，これはインターネット上の電子商取引が本格的になったことを意味すると観測されている。日本においても，携帯電話のi-modeの加入者が3,000万人を超えたと言われている。インターネットの脆弱性の克服には暗号・情報セキュリティが必須となり，それが電子社会秩序を規定し，未来の社会を左右するものとなり，人類に大きな影響を与えるということが認識されてきている。

暗号を実際のシステムに適用する際の形態は，適用範囲，対象，実装，システムのロジスティックスによって次のように多岐にわたっている(図3)。

- 暗号LSIロジック：半導体チップ実装，設計情報IP

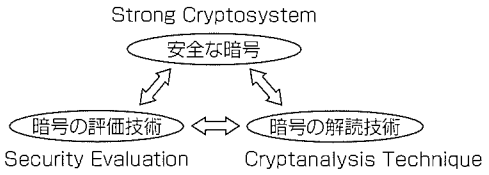



図2．暗号の安全性と暗号解読

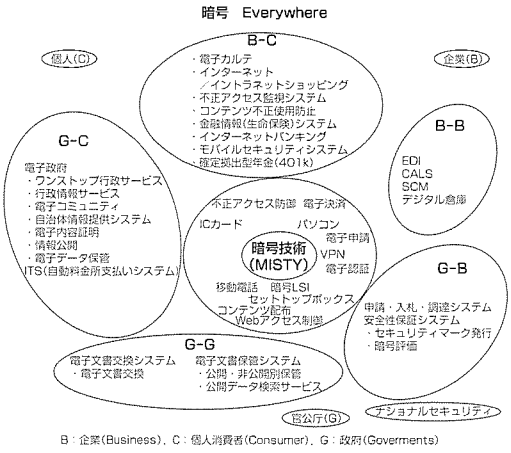



図3．暗号・情報セキュリティ適用対象分野

(Intellectual Property)

- 暗号組み込み機器：携帯電話，通信機器，耐タンパー暗号ボード，ICカード
- 暗号を管理運用するシステム：認証システム，鍵管理システム，不正アクセスの評価・防御システム
- 上記サービス：セキュリティ設計，セキュリティ管理・運用ポリシーの策定・コンサルティング

## 3. 今後の動向

### 3.1 インターネットがモバイルになる

世界の携帯電話の利用者数が2002年の年明け早々に十億人の大台を突破する見通しが報じられた(2001年12月29日，日経新聞)。携帯電話市場調査会社の英EMCによると，2001年末予想は9億8,856万人，世界の約6人に1人が携帯電話利用する計算になる。インターネット接続機能を高めた携帯電話が主流となってくる。

インターネットe-commerce初期に比べ，モバイルインターネットにおけるセキュリティ，プライバシーの必要性への関心はより高いものがあると言われている[6]。インターネットのモバイル版は，今日のインターネットの到達範囲を遥かに凌駕したものになると予想されている。その根拠には，操作が複雑で高価なパソコンを必要としないこと，インターネットの利便性をより広範な使用者人口にもたらしてくれることによると言われている。電信(Telegraph)のマスマーケットを引き継いだものが電話(Telephone)であったことの繰り返しとして，現代版Telegraphであるインターネットを引き継ぐものがまたTelephoneとなるのではないかという予測がされている。これが正しければ，無線を介すること(Wireless)及び使用者規模の格段の大きさが加わることから，インターネットにあった安全上の脆弱さは何十倍にも増幅して引き継がれることになる。オペレータ，携帯電話メーカー，サービスプロバイダーの連携の下，セキュリティ及びプライバシー保護対策が講じられていくことが必須であろう。

モバイルインターネットに関する暗号・情報セキュリティ技術の予測ロードマップを図4に示す。データ通信機能を含めた携帯電話上の暗号・セキュリティ機能の実現と，携帯電話上にそれらを実装していくための暗号ハードウェアチップを含めたコンパクト化の技術が求められる。

### 3.2 更に高い安全性を求めて

暗号解読用の鍵をコンピュータで逐次調べ上げていけば，どのような暗号でもいずれは解読の端緒が開かれるであろう。しかし，それは数千年・数万年の年月を必要とするということで，現代のデジタル暗号の安全性は保たれている。ところが，光子等の量子を利用したコンピュータが実現すれば，暗号解読用の鍵の割り出しは一瞬にして可能となると言われている。

'70年以来，DES暗号や電子署名用のRSA暗号等に代表されるように，暗号開発が暗号解読に技術的に先んじて行われてきた。これにより，今日，インターネット等のネットワーク上での安全な通信・取引が行われるようになりつつあり，この基盤の上に今後のデジタル社会が築かれようとしている。将来の量子コンピュータの出現はこれを根底から破壊するものと考えられる。

しかし，量子コンピュータの出現は今日明日という近い未来ではないという予測がされていた。ところが，それにもかかわらず，量子コンピュータによる計算を行えば現在電子署名という重要な機能を実現する公開鍵暗号が瞬時に解読されるという証明がなされて，暗号・情報セキュリティの世界，また軍事防衛の分野に大きな衝撃を与えた[5]。RSA暗号解読のための素因数分解計算において，129けたの数の素因数分解に600台のデジタルコンピュータで数箇月かかるものが，'94年のAT&Tベル研究所ピーターショア発表の量子コンピュータプログラムによれば，その数の数百万倍の大きさの数を，その数の素因数分解に要した時間の百万分の一の時間で解くことができるということである。発表当時は量子コンピュータが存在せずショア自身による実証実験はなされていなかったが，科学雑誌“Nature”2001年12月発行の掲載記事「IBMの科学者とスタンフォード大学院生のチームによる“ショアのアルゴリズム”の初のデモンストレーション」が行われ，その原理の実証実験による証明の成功が報じられており，量子コンピュータの実現が夢物語でないことを告げている。

このような解読技術に対抗するためには，量子暗号の開発が必要である。量子力学が支配する微小な世界では粒子の状態に影響を与えずにその粒子を観察し状態を決めることは不可能であるといわれている(“不確定性原理”)。この原理を利用したのが量子暗号である。通信の送受信者間で，完全な秘密裡に意思の伝達が可能になる方法として開発が急がれている。

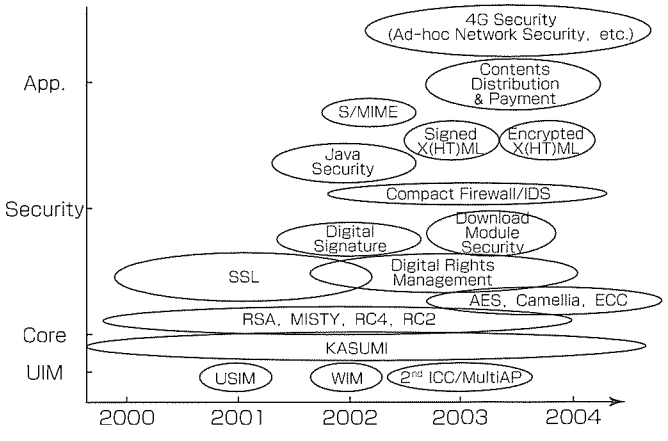



図4．Mobile Security Roadmap

量子暗号は，光とデジタルの技術の融合で実現可能であり，数年以内に実用化されると考えられている。

三菱電機は，'99年量子暗号研究に着手，国内初の光子による量子暗号通信の実証実験に成功した。2000年9月時点で世界最高水準レベルの通信性能を市販の光ファイバを使用して実現した。

量子暗号関連の展望を図5に示す。

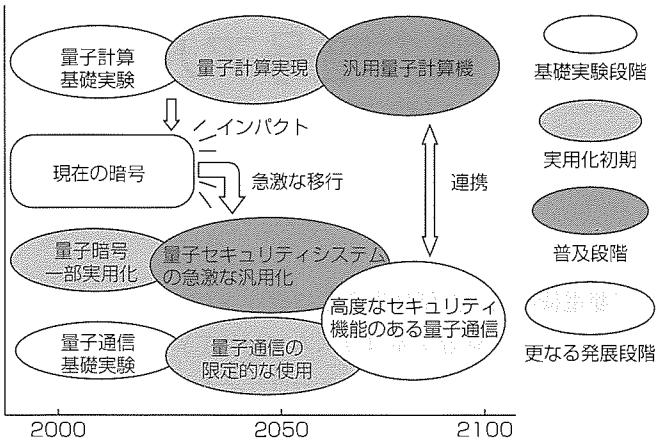



**図5．量子情報通信・処理の将来展望**

## 参考文献


(1) 辻井重男：暗号，講談社選書メチエ73，ISBN4-06-258073-X（1997）

(2) Denning，D.E.：Information Warfare and Security，Addison Wesley Longman，Inc.，ISBN 0-201-43303-6（1999）

(3) Singh，S.：The Code Book，DOUBLEDAY，ISBN 0-385-49531-5（1999）

(4) Stinson，D.R.：Cryptography，CRC Press，Inc.，ISBN 0-8493-8521-0（1995）

(5) 吉田一彦：暗号戦争，小学館，ISBN 4-09-387261-9（1948）

(6) The Internet，Untethered，A Survey of the Mobile Internet，The Economist October 13th-19th（2001）

(7) 竹内繁樹：量子計算と量子情報通信，電子情報通信学会誌　特別小特集・21世紀を展望する，84，No.1（2001）

# 三菱電機の暗号アルゴリズム開発 —MISTY，KASUMI，Camellia—

松井　充*
時田俊雄*
反町　亨*

**要　旨**

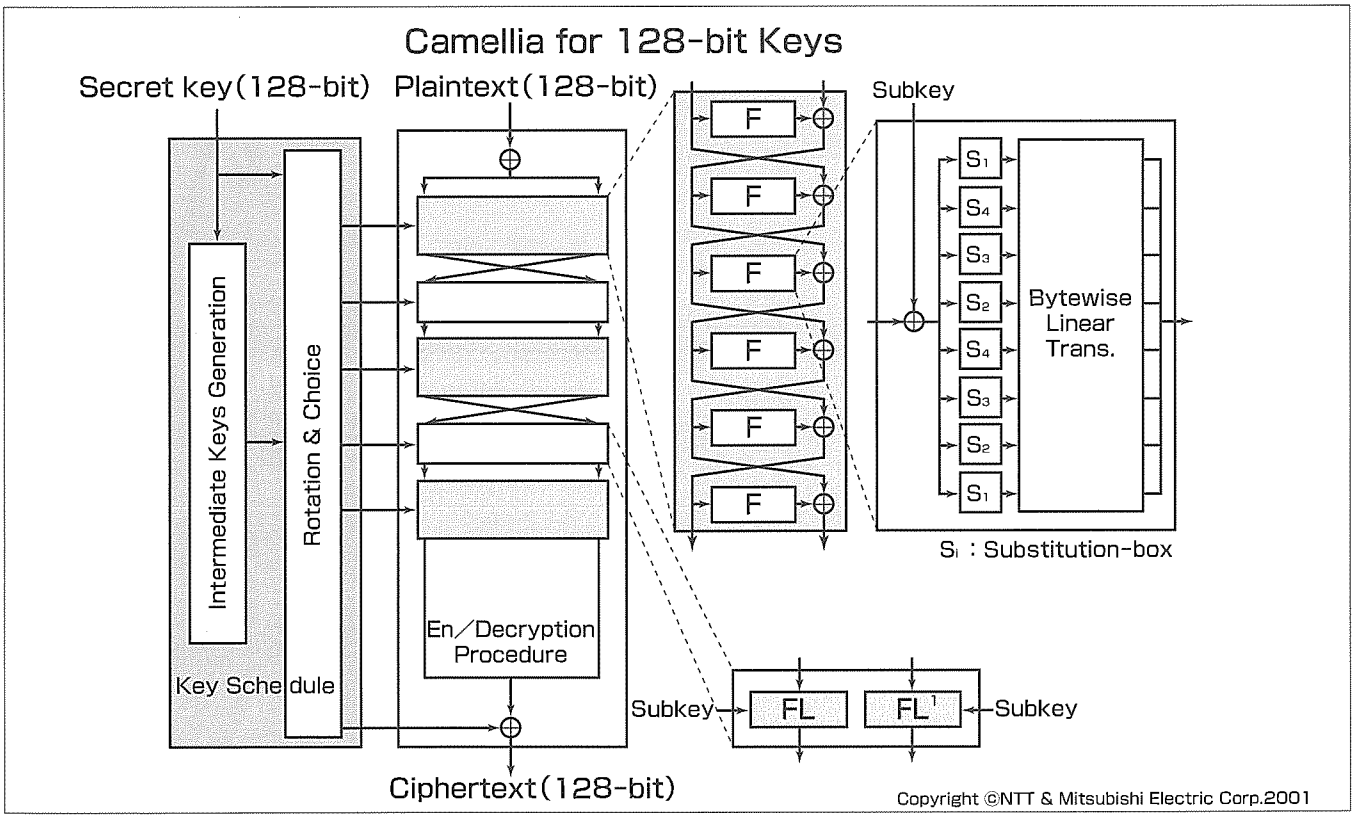
三菱電機の暗号評価技術を基に設計された三つの共通かぎ(鍵)ブロック暗号アルゴリズム“MISTY”“KASUMI”“Camellia”を紹介する。暗号アルゴリズムの設計においては，その安全性はもちろんのこと，速度性能や実装時のサイズ，又は応用の広さなど実用面からの検討が不可欠である。すなわち，安全性と実装性のバランスをどうとるかが，暗号を設計する上において最も困難な部分であると言ってよい。

MISTYは，当社が1996年に発表した64ビットブロック暗号である。MISTYは，ソフトウェアでの高速性だけでなく，ハードウェアでの小型化をも設計目標とした点で，当時としては珍しい方式であった。

その後2000年になって，第三世代携帯電話(W-CDMA)世界標準暗号にMISTYをベースとして欧州で開発された64ビットブロック暗号KASUMIが採用されたが，MISTYがそのベースとなるに至った大きな理由の一つは，MISTYがハードウェアで優れた性能と低消費電力を実現することにあった。

Camelliaは，2000年にNTT㈱と当社が共同で設計した次世代128ビットブロック暗号であり，両社の持つ世界トップレベルの暗号強度評価技術と暗号実装技術を結集して実現されたものである。Camelliaは，次世代暗号にふさわしい高い安全性と，あらゆるプラットフォームで高い性能と小型化が両立できるよう設計されている。

これらの暗号方式はいずれも国内外の研究者から高い評価を得ており，我々は積極的な標準化活動を行っている。今後，これらマルチプラットフォーム共通鍵暗号のニーズはますます拡大していくものと考えられる。




**ブロック暗号アルゴリズムCamellia**

Camelliaは，米国政府標準暗号AESと同じく3種類の鍵サイズ(128ビット，192ビット，256ビット)をサポートする。図は，このうち128ビットの鍵サイズを持つCamelliaの全体図を示したものである。フェイステル型と呼ばれる構造と，鍵によって形が変化する線形関数を組み合わせることによって，高い安全性と小型化を両立させている。

*情報技術総合研究所

## 1. まえがき

三菱電機の暗号評価技術を基に設計された三つの鍵ブロック暗号アルゴリズム“MISTY”“KASUMI”“Camellia”について述べる。

## 2. MISTY

### 2.1 MISTYの設計指針

MISTYとは，当社が設計し1996年にその詳細仕様を学会で公開した128ビットの鍵を持つ二つの64ビットブロック暗号アルゴリズムMISTY 1とMISTY 2の総称名である[(1)(2)]。MISTYは次の三つをその設計基準としている。

(1) 安全性に関する何らかの数値的な根拠を持つこと。
(2) 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。
(3) ハードウェアで十分な高速性を実現すること。

MISTYの安全性については，当時から現在に至るまでブロック暗号に対する極めて強力な暗号解読法とされる差分解読法や線形解読法に対して，数学的に安全性が証明できる“証明可能安全性(Provable Security)”を持つことを大きな特長としている。MISTYでは，新しい段関数構造と入れ子構造(Recursive Structure)を採用することによって，内部演算の並列度を高めて高速化を図りながら同時にこの証明可能安全性を実現している。

また，当時，多くのブロック暗号が特定の仕様のプロセッサ(例えば32ビットIntelプロセッサ)でのみ高い性能を達成するよう設計されていたのに対し，MISTYは，特定の仕様のプロセッサで最高の性能を追及するよりも，8ビットから64ビットまであらゆるプロセッサで実用的な高速性と小型化を実現することを重要視して設計された。このため，特定のプロセッサでのみ高速な命令はMISTYには採用されていない。

またMISTYのもう一つの大きな特長は，ハードウェアに対する親和性である。当時のほとんどの暗号はソフトウェアで実装されることだけを想定しており，このため，ハードウェアでは極端に規模が大きくなったり，又はソフトウェアで実装された場合に比べて速度向上が余り期待できないことが少なくなかった。これに対してMISTYは，例えば論理演算とテーブル参照だけでそのアルゴリズム全体を構成し，しかもそのテーブルの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造をとっている。

MISTY 1，MISTY 2の仕様は段数可変(ただし4の倍数)であるが，その推奨段数はそれぞれ8段及び12段である。現時点では8段版のMISTY 1が利用されることがほとんどであるので，以下も断りのない限りMISTYと言えばこれを指すものとする。

### 2.2 MISTYの現状

MISTYは，その発表以来，数多くのユーザーを得てきた。当社では，暗号ライブラリ(PowerMISTY)やファイル暗号化(CryptoDoc)，電子メール暗号化(CryptoSign)などの汎用ソフトウェア製品でMISTYを採用しているほか，官公庁向けシステムにおいてもMISTYは数多く利用されている。

MISTYのハードウェアでの小型／低消費電力性は他のアルゴリズムにはない特長であり，このことが次に述べる第三世代携帯電話でのKASUMI採用の大きな契機となった。当社では，MISTYのハードウェア設計情報(Verilog HDL)のライセンス供給も行っている。

また，MISTYの安全性については，その発表以来数多くの研究者によって評価が行われている。暗号方式の信頼性は第三者評価の積み重ねによってのみ得られると言ってよい。電子政府向け暗号評価委員会CRYPTRECの報告書によれば，現在利用されている8段版MISTY 1の安全性には現時点では問題がないと報告されている[(3)]。

## 3. KASUMI

### 3.1 KASUMI誕生の経緯

第三世代携帯電話(W-CDMA)の技術標準を議論するコンソーシアム3GPP(3rd Generation Partnership Project)は欧州・日本・米国・韓国・中国の通信標準化団体で構成されているが，この中で情報セキュリティの規格策定に責任を持つのはワーキンググループSA-WG2である。これまで欧州の各種通信暗号方式は3GPPのメンバーでもある欧州通信標準化団体ETSI(European Telecommunication Standards Institute)内の暗号専門家グループSAGE(Special Algorithm Group of Experts)によって設計されるのが通例であり，SA-WG2もこれに習ってSAGEに第三世代携帯電話向け暗号アルゴリズムの設計を依頼した。

これを受けてSAGEでは暗号設計に着手したが，開発に与えられた期間が短かったことなどから，既存の暗号をベースとして開発することを決定し，その暗号としてMISTY 1を採用した。MISTY 1が採用された理由は，その安全性の高さとともに，3GPP側から“ハードウェアで10KGates以下で実現できること”という要求仕様があったのに対し，MISTY 1がその仕様を満足する実装を当時既に実現していた，ほとんど唯一のブロック暗号であったということが決定的であった。

このMISTY 1をベースとして設計された128ビット鍵を持つ64ビットブロック暗号は，MISTYの日本語訳であるKASUMI(霞)の名称が与えられ，2000年1月に正式にW-CDMAの必す(須)暗号として承認されるに至った。

### 3.2 W-CDMA暗号標準のスコープ

KASUMIが必須の標準として利用されるのは，トラン

スポートレイヤの暗号化(Confidentiality)及び完全性(Integrity)メカニズムにおいてである。認証(Authentication)についてはキャリアごとに異なる方式を採用してもよいが，推奨方式(強制力はない)がやはりSAGEによって設計されている。

KASUMIは，MISTY 1を更にハードウェア向けにカスタマイズしたものであり，ハードウェア(LSI)で実装されることを前提としている。なお，KASUMIは3 GPPの各メンバーの共同所有であり，現時点ではこのブロック暗号は3 GPP機器にのみ用いることができ，その利用には3GPPメンバーとの利用契約が必要である(日本の場合は電波産業会)。

KASUMIの仕様書は公開されており，3 GPPのホームページからダウンロードすることができる[4]。今後の第三世代携帯電話の普及とともに，KASUMIは世界中で利用されることになるであろう。

## 4. Camellia

### 4.1 Camelliaの設計指針

Camelliaは，2000年にNTT㈱と当社が共同開発した新しいブロック暗号アルゴリズムで，両社の持つ世界トップレベルの暗号強度評価技術と暗号実装技術を結集して実現されたものである。そのブロックサイズはMISTY，KASUMIの倍の128ビットとなっている[5][6]。鍵は128ビット，192ビット，256ビットの3種類がサポートされており，これらパラメータは，最近米国で標準化された政府標準暗号AESと同一のものを採用している。このパラメータは，次世代暗号にふさわしい，より安全性を高める目的で導入されたものである。

Camelliaは，安全性の点では，差分解読法や線形解読法以降の最新の暗号解読法にも対処するよう設計されただけでなく，今後の暗号解読法の進歩も見越した上で十分な安全性のマージンをとっている。また，昨今の暗号の応用範囲の広がりを考慮して，ICカードのように極めてリソースの限られた環境での実装性から，最新の64ビットプロセッサでの高速性，またハードウェアでは携帯機器などへの応用を考慮して小型低消費電力を実現するなど，あらゆる暗号プラットフォームに適用できるように設計されている。

### 4.2 Camelliaの構造上の特長

Camelliaは，MISTYやKASUMIと同じく，テーブル参照と論理演算だけから構成されており，ハードウェア実装時の性能を考慮して算術演算は用いられていない。一方Camelliaは，MISTYやKASUMIと異なり，バイト(又はワード)単位の演算だけでアルゴリズム全体が構成されており，このため，プロセッサの種類によらずソフトウェアで高い性能が発揮できる。

基本的な構造は，暗号化と復号の回路が共有できるという特長を持つファイステル型と呼ばれる構造を採用しているが，これに加え，鍵によって形が変化する線形関数をその途中に挟み込むことによって暗号解読の困難性を高める工夫がなされている。また鍵のセットアップ時間についても実装時の暗号化と復号の差がないよう設計されており，この暗号化回路と復号回路の共有性・効率性という点においてCamelliaはAESよりも優れている。

CamelliaはISOやNESSIEなどの標準化に提案されており，その安全性については，既に数多くの第三者評価結果が知られている。CRYPTRECの報告書においても，Camelliaの安全性には現時点では問題がないと報告されている[3]。今後，Camelliaは，次世代暗号として幅広く利用されることが期待できる。Camelliaの性能などより詳細についてはhttp://info.isl.ntt.co.jp/camelliaを参照されたい。

## 5. むすび

本稿では，ブロック暗号アルゴリズム“MISTY”“KASUMI”“Camellia”を紹介した。文末に，C言語で記述されたMISTY 1のCBCモードのサンプルプログラムを添付した。これは移植性を重視したもので，ほとんどのANSI-Cコンパイラで動作するよう設計されている。

## 参考文献


(1) 松井　充：ブロック暗号MISTY，信学技報ISEC96-11 (1996)

(2) Matsui, M.：New Block Encryption Algorithm MISTY, FSE'97, Springer LNCS, 1267 (1997)

(3) 情報処理振興事業協会セキュリティセンター：暗号技術評価報告書，CRYPTREC Report 2000 (2001)

(4) 3 GPP homepage：http://www.3gpp.org/

(5) 青木和麻呂，ほか：128ビットブロック暗号Camellia，信学技報，ISEC2000－6 (2000)

(6) Aoki, K., et al.：The 128-Bit Block Cipher Camellia, IEICE Trans. Fundamentals, **E85-A**, No.1 (2001)

```
/*****************************************************************
  A Sample Program of MISTY1 Block Encryption Algorithm in CBC mode

  Key Scheduling  P_Misty1_Keysch( key, ekey )
  Encryption      P_Misty1_Cbcenc( pdat, cdat, ivec, ekey, block )
  Decryption      P_Misty1_Cbcdec( cdat, pdat, ivec, ekey, block )

        key       address of encryption key (16 bytes)
        ekey      address of subkey (sizeof(Uint) * 32 bytes)
        pdat      address of plaintext data  (block * 8 bytes)
        cdat      address of ciphertext data (block * 8 bytes)
        ivec      address of initial vector (8 bytes)
        block     the number of data blocks

        Copyright (c) 2002 Mitsubishi Electric Corporation
*****************************************************************/

typedef unsigned char Ulnt8;
typedef unsigned int Ulnt; /* also works for short and long */

static const Ulnt 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 const Ulnt 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 & ekey[0+((k+0)&7)];¥
r3 ^= r2 & ekey[8+((k+2)&7)];¥
r0 ^= r1 | ekey[8+((k+6)&7)];¥
r2 ^= r3 | ekey[0+((k+4)&7)];¥
}

#define FL_dec( k ) {¥
r0 ^= r1 | ekey[0+((k+4)&7)];¥
r2 ^= r3 | ekey[8+((k+6)&7)];¥
r1 ^= r0 & ekey[8+((k+2)&7)];¥
r3 ^= r2 & ekey[0+((k+0)&7)];¥
}

#define Fl_key( k ) {¥
r0 = ekey[k] >> 7;¥
r1 = ekey[k] & 0x7f;¥
r0 = S9[r0] ^ r1;¥
r1 = S7[r1] ^ ( r0 & 0x7f );¥
r1 ^= ekey[(k+1)&7] >> 9;¥
r0 ^= ekey[(k+1)&7] & 0x1ff;¥
r0 = S9[r0] ^ r1;¥
ekey[ 8+k] = r1 << 9 ^ r0;¥
ekey[16+k] = r0;¥
ekey[24+k] = r1;¥
}

#define Fl_txt( a0, a1, k ) {¥
a1 = a0 >> 7;¥
a0 &= 0x7f;¥
a1 = S9[a1] ^ a0;¥
a0 = S7[a0] ^ a1;¥
a1 ^= ekey[16+(k)];¥
a0 ^= ekey[24+(k)];¥
a0 &= 0x7f;¥
a1 = S9[a1] ^ a0;¥
a1 ^= a0 << 9;¥
}

#define FO_txt( a0, a1, a2, a3, k ) {¥
t0 = a0 ^ ekey[k];¥
Fl_txt( t0, t1, (k+5)&7 );¥
t1 ^= a1;¥
t2 = a1 ^ ekey[(k+2)&7];¥
Fl_txt( t2, t0, (k+1)&7 );¥
t0 ^= t1;¥
t1 ^= ekey[(k+7)&7];¥
Fl_txt( t1, t2, (k+3)&7 );¥
t2 ^= t0;¥
t0 ^= ekey[(k+4)&7];¥
a2 ^= t0;¥
a3 ^= t2;¥
}
```

```
void P_Misty1_Keysch( UInt8 *key, UInt *ekey )
{
	UInt r0,r1;

	ekey[0] = (UInt)key[ 0]<<8 ^ (UInt)key[ 1];
	ekey[1] = (UInt)key[ 2]<<8 ^ (UInt)key[ 3];
	ekey[2] = (UInt)key[ 4]<<8 ^ (UInt)key[ 5];
	ekey[3] = (UInt)key[ 6]<<8 ^ (UInt)key[ 7];
	ekey[4] = (UInt)key[ 8]<<8 ^ (UInt)key[ 9];
	ekey[5] = (UInt)key[10]<<8 ^ (UInt)key[11];
	ekey[6] = (UInt)key[12]<<8 ^ (UInt)key[13];
	ekey[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 );
}

void P_Misty1_Cbcenc( UInt8 *pdat, UInt8 *cdat, UInt8 *ivec, UInt *ekey,
UInt block )
{
	UInt r0,r1,r2,r3,t0,t1,t2,buff[4];

	buff[0] = (UInt)ivec[0]<<8 ^ (UInt)ivec[1];
	buff[1] = (UInt)ivec[2]<<8 ^ (UInt)ivec[3];
	buff[2] = (UInt)ivec[4]<<8 ^ (UInt)ivec[5];
	buff[3] = (UInt)ivec[6]<<8 ^ (UInt)ivec[7];

	while( block != 0 ){
		r0 = (UInt)pdat[0]<<8 ^ (UInt)pdat[1];
		r1 = (UInt)pdat[2]<<8 ^ (UInt)pdat[3];
		r2 = (UInt)pdat[4]<<8 ^ (UInt)pdat[5];
		r3 = (UInt)pdat[6]<<8 ^ (UInt)pdat[7];

		r0 ^= buff[0]; r1 ^= buff[1];
		r2 ^= buff[2]; r3 ^= buff[3];

		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 );

		buff[0] = r2; buff[1] = r3;
		buff[2] = r0; buff[3] = r1;

		cdat[0] = (UInt8)(r2 >> 8); cdat[1] = (UInt8)(r2);
		cdat[2] = (UInt8)(r3 >> 8); cdat[3] = (UInt8)(r3);
		cdat[4] = (UInt8)(r0 >> 8); cdat[5] = (UInt8)(r0);
		cdat[6] = (UInt8)(r1 >> 8); cdat[7] = (UInt8)(r1);

		pdat += 8; cdat += 8; block--;
	}

	ivec[0] = (UInt8)(buff[0] >> 8); ivec[1] = (UInt8)(buff[0]);
	ivec[2] = (UInt8)(buff[1] >> 8); ivec[3] = (UInt8)(buff[1]);
	ivec[4] = (UInt8)(buff[2] >> 8); ivec[5] = (UInt8)(buff[2]);
	ivec[6] = (UInt8)(buff[3] >> 8); ivec[7] = (UInt8)(buff[3]);
}

void P_Misty1_Cbcdec( UInt8 *cdat, UInt8 *pdat, UInt8 *ivec, UInt *ekey,
UInt block )
{
	UInt r0,r1,r2,r3,t0,t1,t2,buff[4],buff2[4];

	buff[0] = (UInt)ivec[0]<<8 ^ (UInt)ivec[1];
	buff[1] = (UInt)ivec[2]<<8 ^ (UInt)ivec[3];
	buff[2] = (UInt)ivec[4]<<8 ^ (UInt)ivec[5];
	buff[3] = (UInt)ivec[6]<<8 ^ (UInt)ivec[7];

	while( block != 0 ){
		r0 = (UInt)cdat[0]<<8 ^ (UInt)cdat[1];
		r1 = (UInt)cdat[2]<<8 ^ (UInt)cdat[3];
		r2 = (UInt)cdat[4]<<8 ^ (UInt)cdat[5];
		r3 = (UInt)cdat[6]<<8 ^ (UInt)cdat[7];

		buff2[0] = r0; buff2[1] = r1;
		buff2[2] = r2; buff2[3] = r3;

		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 );

		r2 ^= buff[0]; r3 ^= buff[1];
		r0 ^= buff[2]; r1 ^= buff[3];

		buff[0] = buff2[0]; buff[1] = buff2[1];
		buff[2] = buff2[2]; buff[3] = buff2[3];

		pdat[0] = (UInt8)(r2 >> 8); pdat[1] = (UInt8)(r2);
		pdat[2] = (UInt8)(r3 >> 8); pdat[3] = (UInt8)(r3);
		pdat[4] = (UInt8)(r0 >> 8); pdat[5] = (UInt8)(r0);
		pdat[6] = (UInt8)(r1 >> 8); pdat[7] = (UInt8)(r1);

		pdat += 8; cdat += 8; block--;
	}

	ivec[0] = (UInt8)(buff[0] >> 8); ivec[1] = (UInt8)(buff[0]);
	ivec[2] = (UInt8)(buff[1] >> 8); ivec[3] = (UInt8)(buff[1]);
	ivec[4] = (UInt8)(buff[2] >> 8); ivec[5] = (UInt8)(buff[2]);
	ivec[6] = (UInt8)(buff[3] >> 8); ivec[7] = (UInt8)(buff[3]);
}
```

# 標準化動向

近澤　武*

**要　旨**

前稿で紹介があったように，三菱電機は“MISTY１”と“Camellia”の暗号アルゴリズムを保有している。当社は，その両者を様々な標準化に提案し，高い技術レベルを示している。

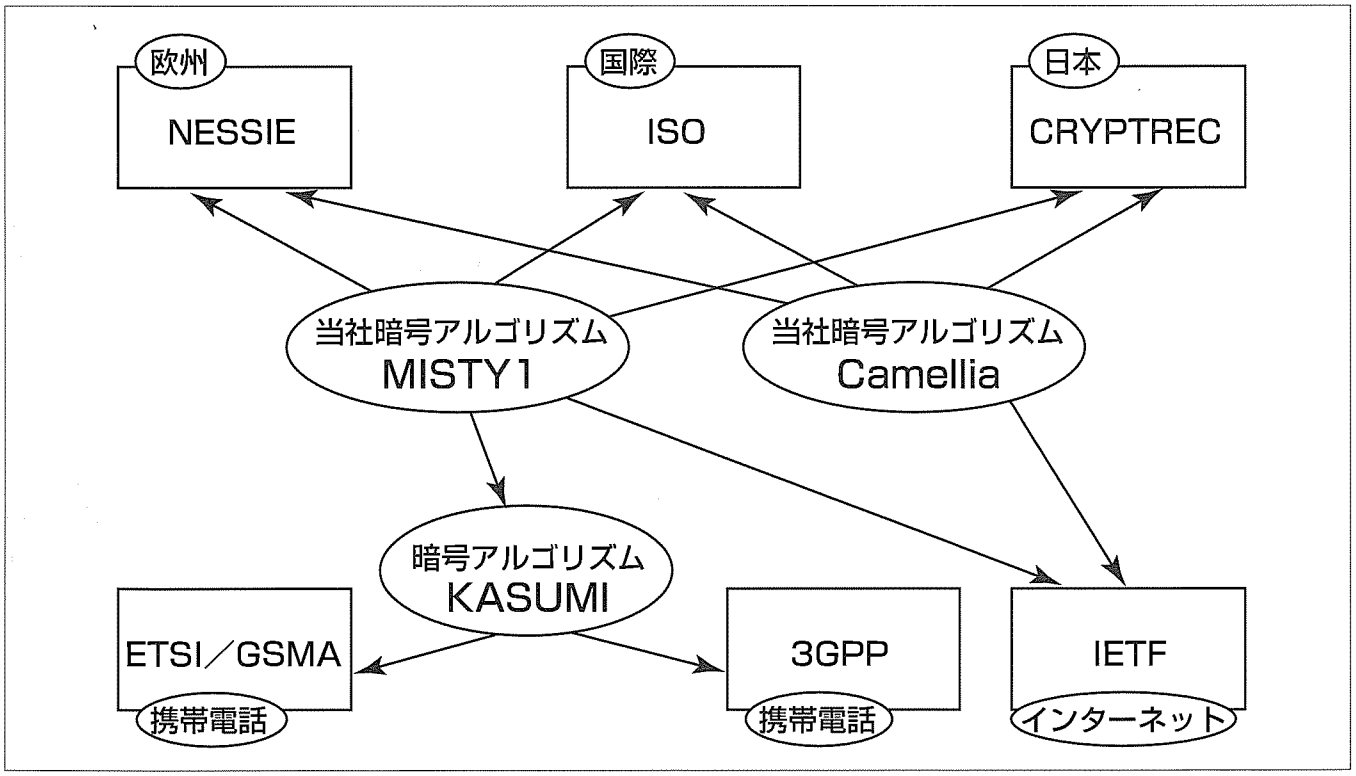
ISO（国際標準化機構）は，最近，暗号アルゴリズムの標準化を開始し，MISTY１，Camellia共に有力候補となっている。

第三世代の携帯電話の標準化を行っている３GPPにおいては，端末と基地局の無線区間の秘匿とデータ認証を行うために，“KASUMI”という暗号アルゴリズムが開発された。KASUMIは当社のMISTY１をベースに移動通信用にカスタマイズしたもので，日本発の暗号アルゴリズムをベースにしたものが唯一の国際標準になったのは日本の暗号史上初めてであり，画期的なことである。欧州の現行方式にもKASUMIをコアとする暗号が使用できるよう，欧州の標準化組織ETSIとGSM関係者の集まりのGSMAと共同で開発中である。

欧州のセキュリティプロジェクトNESSIEは，欧州産業界のための暗号部品推奨リストを作る目的で，2000年に開始された。暗号部品の候補は公募によって集められ，２段階の評価を行って最終リストを完成させることになっている。現在，第一次選考結果が発表され，ブロック暗号のカテゴリーにおいては，日本の他社からの提案アルゴリズムが落選するのに対し，MISTY１，Camellia共に合格している。

日本の電子政府のために設立されたプロジェクトCRYPTRECは，電子政府で適用可能な暗号アルゴリズムのリストを作成することを目的としている。2001年の詳細評価結果では，MISTY１，Camellia共に，安全性及び性能に関し，最高の評価を得ている。

インターネット関連技術の標準化を行っているIETFにはセキュリティに関するWGがあり，MISTY１，Camellia共にTLS WGでTLSのCipher Suiteとして提案されている。なお，MISTY１はRFC2994で参照できる。




**当社の暗号アルゴリズムと標準化**

当社の暗号アルゴリズムMISTY１とCamelliaは，ISO，３GPP，NESSIE，CRYPTREC，IETFなどに提案され，一部は規格化され始めている。当社の暗号アルゴリズムは高い技術レベルにあり，日本のみならず，世界に誇れる技術と言っても過言ではない。

*情報技術総合研究所

## 1. まえがき

本稿では，三菱電機の暗号アルゴリズム“MISTY１”や“Camellia”を提案しているISO(International Organization for Standardization：国際標準化機構)，NESSIE(New European Schemes for Signatures, Integrity and Encryption)，CRYPTREC(暗号技術評価委員会)，IETF(Internet Engineering Task Force)の標準化動向を紹介する。また，携帯電話関係の標準化を行っている３GPP(The 3rd Generation Partnership Project)やETSI(European Telecommunications Standards Institute)／GSMA(GSM Association)の動向も紹介する。

## 2. ISOにおける動向[1]

ISO／IEC JTC１／SC27(International Organization for Standardization／International Electrotechnical Commission(国際電気標準会議)Joint Technical Committee 1／Sub Committee 27(以下，“ISO”という。)では，情報セキュリティに関する標準化を行っている。現在，電子署名，認証手順，暗号化の際に必要な“鍵”の管理等の規格がある。一方，過去にISOでは，米国の暗号アルゴリズムDES(Data Encryption Standard)を国際規格化しようとした際に，米国から輸出規制や強度評価の困難性を理由に反対があったため，標準化を中止し，暗号アルゴリズムの登録制に切り換えた経緯があり，最近までISOでは暗号アルゴリズムの標準化は行われていなかった。

だが，2000年にようやくISOでも18033という番号の新プロジェクトが発足し，暗号アルゴリズムの標準化に着手した。このプロジェクトは四つのパートから構成されており，パート１は総論，パート２は公開鍵暗号，パート３はブロック暗号，パート４はストリーム暗号をそれぞれ規格化する。

パート３のブロック暗号には，米国の新標準暗号アルゴリズムAES(Advanced Encryption Standard)，銀行業界等で使用されているTDEA(Triple Data Encryption Algorithm：Triple DESとして知られている暗号アルゴリズム)，当社のMISTY１やCamellia等も提案されている。現在Working Draftで，2003年ごろ規格化される予定である。

## 3. ３GPPにおける動向[2]

第三世代の移動通信システム(携帯電話)「IMT-2000(International Mobile Telecommunications-2000)」が，2001年10月から，世界に先駆けて，日本で本サービスが開始された。IMT-2000の特長として，グローバル・ローミングの実現，動画などマルチメディアに対応できる端末の採用，地上回線並みの高品質なサービスの提供などが挙げられる。規格策定時に，IMT-2000にはユーザー保護を目的とした高度なセキュリティ技術やプライバシー保護技術の採用が求められ，こうした要望にこたえるため，IMT-2000の一つであるW-CDMA(Wideband-Code Division Multiple Access：広帯域拡散符号分割多元接続。正式名称はDS(Direct Spread)-CDMA)方式の仕様策定に携わる３GPPから委嘱を受けたETSI(欧州電気通信標準化協会)傘下の暗号専門家グループSAGE(Security Algorithms Group of Experts)が，暗号アルゴリズム“KASUMI”を作り上げた。

暗号アルゴリズムKASUMIは，当社の暗号アルゴリズム“MISTY１”を，移動通信システム用にカスタマイズしたものである。KASUMIは，W-CDMAの無線部分の基本的な暗号化技術として使用されている。

日本発の暗号アルゴリズムをベースにしたものが唯一の国際標準になったのは日本の暗号史上初めてであり，画期的なことと言える[3]。

## 4. ETSI／GSMAにおける動向[4][5]

欧州で現在使用されているGSM(Global System for Mobile Communications)と第三世代方式のデュアル機を想定して（同じコアの暗号を使うことにより，リソース，コスト削減が実現できる)，GSMの無線区間に，KASUMIをコアとする暗号アルゴリズムをESTIとGSMAで採用しようとしている。この新暗号アルゴリズムはA5/3と名付けられた。

## 5. NESSIEにおける動向[6]

NESSIEプロジェクトは，EC(European Commission：欧州委員会)のInformation Societies Technology Programme(情報社会技術プログラム)の一つとして，2000年１月から2002年12月までの３年間実施される。米国のAES選定とは異なり，ブロック暗号だけでなく，ストリーム暗号，公開鍵暗号，署名・認証方式，ハッシュ関数，擬似ランダム関数など，暗号部品に関する多くのカテゴリーで推奨リストを作成することになっている。

推奨リストを作成するための選定基準は，安全性，市場の要求，性能，柔軟性の四つであり，2000年３月にアルゴリズム募集を始め，公開討論を目的とした２回のワークショップを経て，2001年９月に第一次選考結果が発表された。**表１**は，第一次選考を通過したアルゴリズムの一覧である。

ブロック暗号のカテゴリーでは，日本からの提案暗号アルゴリズムのうち，当社の暗号アルゴリズムMISTY１とCamelliaのみが第一次選考を通過している。

今後は，2002年10月に第３回のワークショップが開催され，2002年12月に最終選考結果が発表される予定である。

## 6. CRYPTRECにおける動向[7]

日本においては，2003年度をめどとしてその基盤を構築することとされている電子政府において，セキュリティの共通基盤の確保は重要な課題とされている。

とりわけ重要な暗号技術については，電子政府における適切な暗号利用を図るために，政府における利用方針の策定の必要性が指摘されている。他方，国際的には前に述べたISOにおいて暗号アルゴリズムの標準化の動きがあり，日本の対応が問われつつあることからIPA（情報処理振興事業協会）が通商産業省（当時）の委託によって2000年度から実施している。暗号アルゴリズムの標準化は，2000年4月に通商産業省が策定した「情報セキュリティ政策実行プログラム～電子政府のセキュアな基盤構築に向けての通商産業省の貢献～」の重要な一部をなすものである。

このプロジェクトの目的は，日本の電子政府システムに適用可能な暗号技術であって，公募を通じて応募のあったものについて技術的・専門的見地から評価し，安全性・実装性等の特徴を分析・整理したリストを作成することである。作成されたリストは，電子政府で使用する暗号アルゴリズム選定の際の参考情報となる。評価に当たっては，IPAに日本の最高水準の暗号専門家で構成される「暗号技術評価委員会」を組織して行っている。

なお，2001年度からは，経済産業省側のIPAと総務省側のTAO（通信・放送機構）と共同で「暗号技術評価委員会」が運営されている。

公募（評価）対象とする暗号技術は，①公開鍵暗号，②共通鍵暗号，③ハッシュ関数，④擬似乱数生成で，スクリーニング評価と詳細評価の2段階評価を行う。2000年度は，6～7月に公募，7～9月にスクリーニング評価，10月に

表1．NESSIE第一次選考通過アルゴリズム一覧

| | |
|---|---|
| ブロック暗号（応募19件） | IDEA（スイス） |
| | Khazad（ブラジル，ベルギー） |
| | **MISTY 1（当社）** |
| | SAFER$_{++61}$，SAFER$_{++128}$（米国，スイス，アルメニア） |
| | **Camellia（当社，NTT）** |
| | RC6（スウェーデン，米国） |
| | SHACAL（フランス） |
| ストリーム暗号（応募6件） | SOBER-t16，SOBER-t32（オーストラリア） |
| | SNOW（スウェーデン） |
| | BMGL（スウェーデン） |
| 公開鍵暗号（応募9件） | ACE Encrypt（スイス） |
| | EPOC-2（NTT） |
| | PSEC-2（NTT） |
| | ECIES（米国，カナダ） |
| | RSA-OAEP（スウェーデン，米国） |
| メッセージ認証アルゴリズム及びハッシュ関数（応募3件） | Two-Track-MAC（ベルギー，ドイツ） |
| | UMAC（米国，イスラエル） |
| | Whirpool（ブラジル，ベルギー） |
| 電子署名（応募7件） | ECDSA（米国，カナダ） |
| | ESIGN（NTT） |
| | RSA-PSS（スウェーデン，米国） |
| | SFLASH（フランス） |
| | QUARTZ（フランス） |
| 識別方式（応募1件） | GPS（フランス） |

表2．CRYPTREC 2000年度詳細評価結果の抜粋（順不同）[8][9]

| | |
|---|---|
| 共通鍵暗号（64ビットブロック暗号） | 「安全性について，今のところ問題は見付かっていない。処理速度は速いグループである。」と評価されたアルゴリズム：<br>**MISTY 1**，Hierocrypt-L 1 |
| 共通鍵暗号（128ビットブロック暗号） | 「安全性について，今のところ問題は見付かっていない。処理速度は速いグループである。」と評価されたアルゴリズム：<br>**Camellia**，Hierocrypt-3，SC2000 |
| 公開鍵暗号（署名，守秘，鍵共有） | 詳細評価されたアルゴリズムの評価結果がそれぞれ微妙に違うため，本表に列挙すべきものはどれか判断が難しいことと，及び列挙したことによって誤解を与えてしまうおそれがあるため，本表では割愛する。詳細はCRYPTREC2000報告書を参照のこと。 |
| ハッシュ関数 | 「暗号の応用分野で使うのに十分安全であると考えられる。」と評価されたアルゴリズム：<br>MD 5，RIPEMD-160，SHA-1 |
| 共通鍵暗号（ストリーム暗号） | 継続的評価の必要性等指摘されているため，アルゴリズム名の列挙は本表では避けた。 |
| 擬似乱数関数 | 長期使用に注意等指摘されているため，アルゴリズム名の列挙は本表では避けた。 |

スクリーニング結果発表，10～3月に詳細評価，2001年4月に詳細評価が発表された。**表2**は，2000年度の詳細評価結果の抜粋である。MISTY 1，Camellia共に，安全性及び性能に関し，最高の評価を得ている。

2001年度は，2000年度に詳細評価されたアルゴリズムの継続評価と，新規公募のスクリーニング評価を行っている。後者のスケジュールは，8～9月に公募，9～3月にスクリーニング評価である。2002年4月に評価結果発表予定である。

2002年度は，2001年度に応募があり，スクリーニング評価を通過したアルゴリズムの詳細評価を行う予定で，2003年3月に最終的な電子政府推奨暗号リストが完成予定である。

## 7. IETFにおける動向[10]

IETFは，インターネット関連技術の標準化を推進している団体であり，メーリングリストや年3回の会合を中心に活動している。

IETFには八つのエリアがあるが，その一つのセキュリティには，IPSec(IP Security Protocol)，PKIX(Public-Key Infrastructure(X.509))，TLS(Transport Layer Security)等のワーキンググループ(WG)がある。

TLS WGにおいて，当社の暗号アルゴリズムMISTY 1とCamelliaを，TLSのCipher Suiteとして提案中である。なお，MISTY 1はRFC2994で参照できる。

## 8. むすび

当社の暗号アルゴリズムMISTY 1とCamelliaを提案しているISO，3GPP，ETSI/GSMA，NESSIE，CRYPTREC，IETFの標準化動向について簡単に紹介した。この他の標準化にも当社から提案活動を行っているが，紙面の都合で割愛する。以上の標準化の動向を見ても分かるように，当社の暗号アルゴリズムは高い技術レベルにあり，日本のみならず，世界に誇れる技術と言っても過言ではない。

## 参考文献


(1) 情報処理学会　情報規格調査会　国際会議報告 http://www.itscj.ipsj.or.jp/jp/intlmeetrpt.html

(2) http://www.3gpp.org/

(3) 近澤　武，ほか：日本発の技術を3GPPが採用，アルゴリズム「KASUMI」の全貌，日経コミュニケーションブックス モバイル・インターネット最前線，日経BP社，194～199（2000－9）

(4) http://www.etsi.org/

(5) http://www.gsmworld.com/

(6) http://www.cryptonessie.org/

(7) http://www.ipa.go.jp/security/enc/CRYPTREC/index.html

(8) http://www.ipa.go.jp/security/fy12/report/cryptrec-report2k.pdf

(9) JIS TR X 0050：2001「暗号技術評価報告書(CRYPTREC Report 2000)」

(10) http://www.ietf.org/

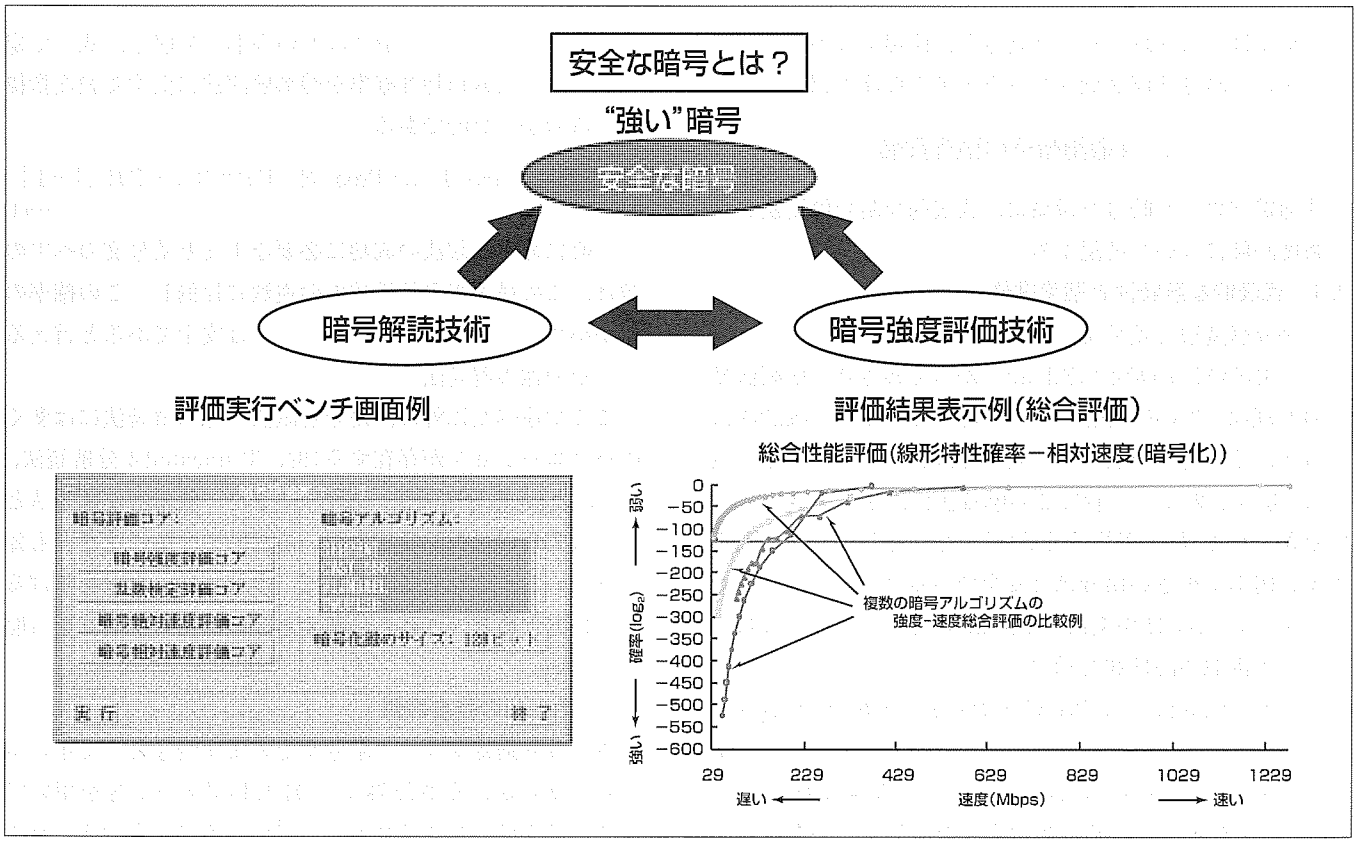
# 暗号強度評価技術

時田俊雄*
酒井康行*
高島克幸*

**要　旨**

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状況で“安全な(＝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，通信路から得られる情報を基に暗号化に必要な情報(＝暗号化鍵。パスワードをイメージすると分かりやすい)を推定(解読)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。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，解読に必要な情報量や計算量を“評価”でき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おり，これらがあって初めて暗号の性能評価が可能となり，より強い暗号の設計が可能となる。

これを実現するために三菱電機が開発したのが本稿で示す“暗号性能評価ソフトウェア”であり，共通鍵ブロック暗号と公開鍵暗号の強度評価を実現する。例えば共通鍵ブロック暗号では，評価者は“評価実行ベンチ”と呼ばれるGUIを通して評価項目(コア)と評価対象暗号を選択し，さらに，必要な各種パラメータを入力／実行することによって様々な強度評価結果を得て，その結果はパソコン上で各種グラフの形で表示される。その特長は，評価者があらかじめ規定されたインタフェースに従って評価項目(コア)及び評価対象暗号を作成／追加することが可能であり，拡張性が高い点が挙げられる。




**安全な暗号と暗号性能評価ソフトウェア**

安全な暗号を設計するためには暗号解読技術と暗号強度評価技術が必要不可欠である。当社の暗号性能評価ソフトウェアは，共通鍵ブロック暗号と公開鍵暗号に関して，各種暗号解読法に対する強度評価結果を客観的な数値データとして示すことを目標に開発された。特に共通鍵ブロック暗号では，暗号強度とソフトウェア実装上の性能を総合的に評価可能である。

*情報技術総合研究所

## 1. まえがき

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。したがって“安全な(＝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，通信路から得られる情報を基に暗号化に必要な情報(＝暗号化鍵。パスワードをイメージすると分かりやすい)を推定(解読)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。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，解読に必要な情報量や計算量を“評価”でき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おり，これらがあって初めて暗号の性能評価が可能となり，より強い暗号の設計が可能となる。

これを実現するために当社が開発したのが本稿で示す“暗号性能評価ソフトウェア”であり，共通鍵ブロック暗号と公開鍵暗号の強度評価を実現する。

本稿では，共通鍵ブロック暗号と公開鍵暗号の強度評価の概説と，暗号性能評価ソフトウェアの機能の紹介を行う。

## 2. 共通鍵暗号の強度評価

共通鍵ブロック暗号を対象に，代表的な暗号解読法とその強度評価について解説する。

### 2.1 代表的な解読法と強度評価

(1) 差分解読法と差分特性確率

差分解読法は1990年にBihamらから提案された解読法で，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，その特徴を利用して暗号化鍵に関する情報を推定する”ものである。一般にこの解読法に対する強度は式(1)で定義される“最大平均差分確率”で与えられ，この最大平均差分確率が小さい暗号ほど安全であると言える。ここで$\Delta P(\neq 0)$，$\Delta C$は平文$P$，暗号文$C$の変化量，(＋)はビットごとの排他的論理和を示す。

$$DP_{max}=\max_{\Delta P\neq 0,\Delta C}\mathrm{Prob}\{F(P+\Delta P)+F(P)=\Delta C\} \quad \cdots(1)$$

ところが，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。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，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，式(2)で定義される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。

$$DP'_{max}=\max\prod_{i=1}^{n}\mathrm{Prob}\{F_i(P_i+\Delta P_i)+F_i(P_i)=\Delta P_{i+1}\} \quad \cdots(2)$$

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，この最大差分特性確率の逆数に比例し，この確率の値が小さければ小さいほどその暗号は安全であると言える。

(2) 線形解読法と線形特性確率

線形解読法は'93年に当社が提案した解読法で，その原理は“平文と暗号文と鍵のビット相関関係を統計的にとらえ，その特徴を利用して暗号化鍵に関する情報を推定する”ものである。この線形解読法に対する強度は式(3)で定義される“最大平均線形確率”で与えられ，この最大平均線形確率が小さい暗号ほど安全であると言える。ここで$\Gamma P$，$\Gamma C$($\neq 0$)を平文$P$，暗号文$C$のマスク値，(・)はビットごとの論理和をとった値のパリティ値を示す。

$$LP_{max}=\max_{\Gamma C\neq 0,\Gamma P}|2\cdot\mathrm{Prob}\{P\cdot\Gamma P=C\cdot\Gamma C\}-1|^2 \quad \cdots(3)$$

ところが，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。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，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，式(4)で定義される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。

$$LP'_{max}=\max\prod_{i=1}^{n}|2\cdot\mathrm{Prob}\{P_i\cdot\Gamma P_i=P_{i+1}\cdot\Gamma P_{i+1}\}-1|^2 \quad \cdots(4)$$

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，この最大線形特性確率の逆数に比例し，この確率の値が小さければ小さいほどその暗号は安全であると言える。

(3) その他の解読法

ここで述べた以外に，差分解読法や線形解読法には多くのバリエーションが存在する(例．Truncated差分解読法，Impossible差分解読法，など)。また，汎用的な解読法としては暗号の代数的性質を用いる高階差分解読法なども知られている。これらに関しては，本稿では，名前を挙げるだけにとどめる。これらに関する詳細は参考文献(2)を参照されたい。

### 2.2 その他の強度評価

以上は共通鍵ブロック暗号をそのまま暗号として用いる場合であるが，それ以外に，OFB利用モード等を用いて擬似乱数生成アルゴリズムとして用いる場合も考えられる。一般に，この場合の強度評価は，統計的手法に基づく乱数性の評価を行う必要がある。乱数性の評価としては，長周期性，線形複雑度，0/1等頻度性などが挙げられる。

## 3. 公開鍵暗号の強度評価

一般に，公開鍵暗号は，安全性の根拠として次に挙げられるような数論的問題に基づいて構成される。

(1) 整数の素因数分解問題
(2) 有限体上の離散対数問題
(3) だ(楕)円曲線上の離散対数問題

本稿では，これらを素因数分解型公開鍵暗号，離散対数型公開鍵暗号，楕円曲線型公開鍵暗号と呼称し，各々について解説する。

### 3.1 素因数分解型公開鍵暗号の強度評価

公開鍵暗号として現在最も普及しているRSA暗号は，整数の素因数分解問題が困難であることを安全性の根拠としている。RSA暗号を解読する一つの方法は，公開情報である合成数$n$(秘密情報である二つの素数の積)を素因数分解することである。

素因数分解を行うアルゴリズムは，大きく次の二つに分類される。

一つは，素因数分解の計算量が分解したい合成数の大きさのみで決まるもの(合成数依存型)である。代表的なものとして，“二次ふるい法”“数体ふるい法”などがある。

もう一つは，計算量が素因数の性質(大きさ，その他)に依存するもの(素因数依存型)である。代表的なものとして，“ロー法”“楕円曲線法”“$p-1$法”“$p+1$法”などがある。

素因数分解問題を解くことは一般的には合成数の大きさが大きいほど難しくなる(準指数時間と呼ばれるオーダーで計算量が増加する)が，合成数がある種の性質を持つ素因数で構成されている場合は，合成数が大きいにもかかわらず容易に素因数分解できることがある。

### 3.2 離散対数型公開鍵暗号の強度評価

素因数分解問題と並んで広く利用されている問題に離散対数問題がある。離散対数問題とは，与えられた素数$p$と，$g$，$y\in\{1, 2, \cdots, p-1\}$から，$y\equiv g^x \bmod p$となる整数$x$を求める問題である。$x$を$p$を法とする数での(離散)対数と呼ぶ。例えば$4\equiv 3^x \bmod 7$となる$x$は4である。実数での対数計算は容易であるが，法$p$での対数計算すなわち離散的世界での対数計算は，$p$が大きい時は難しい。ElGamal暗号は，離散対数問題の困難さに安全性の根拠を置く暗号の代表である。また，最も普及している鍵共有法：Diffie-Hellman(DH)鍵共有法でも，離散対数問題を解く困難さが利用されている(注意：DH鍵共有法は離散対数仮定よりも強い仮定であるDH仮定に安全性の根拠を置いている)。

ElGamal暗号やDH鍵共有を解読する一つの方法は，公開情報$y$，$g$，$p$から，秘密情報$x$を計算することである。その代表的なものに，ロー法，Pohlig-Hellman法，Index-Calculus法，数体ふるい法などがある。離散対数問題を解くことは，素因数分解問題と同様，一般的には各パラメータの大きさが大きいほど難しくなる(準指数時間と呼ばれるオーダーで計算量が増加する)が，ある種の性質を持つパラメータを選択すると，パラメータが大きいにもかかわらず，離散対数計算が容易になることがある。

### 3.3 楕円離散対数型公開鍵暗号の強度評価

RSA暗号やElGamal暗号のアルゴリズムには，整数(正確には有限体)の加法や乗法が用いられる。楕円曲線暗号も同様であるが“楕円曲線上の加算”の利用がその本質である(図1で，点$Q$と点$R$の加算結果が点$S$)。楕円曲線上の加算により，楕円離散対数問題という計算量的問題が数学的に定式化され，楕円ElGamal暗号に代表される楕円曲線暗号はその困難性に安全性の根拠を置いている。一般的に楕円離散対数問題を効率的に解くアルゴリズムは確立されていないが，特殊な楕円曲線に対しては，効率的に暗号解読が行える。

特殊な楕円曲線暗号パラメータに対する攻撃法として，“Pohlig-Hellman法”“MOV法”“FR法”“Satoh-Araki-Semaev-Smart(SASS)法”などが知られている。MOV法，FR法に対して安全性を確保するためには，“楕円曲線のMOV(FR)帰着次数”が大きい必要がある。また，SASS法に対して安全性を確保するためには，“楕円曲線のフロベニウス写像のトレース”が1でない必要がある。また，Pohlig-Hellman法に対して安全性を確保するためには，“楕円曲線の有理点群の位数”が(概)素数になる必要がある。この基準を満たすように楕円曲線暗号パラメータを設定するためには楕円曲線の有理点群の位数を計算する必要があり，その計算には工夫を必要とする。その方法としては，標数に制限がつかない方法としての“SEA法”，小標数の場合にのみ有効な“Satoh法”及びその改良法の“Skjernaa法”“FGH法”“AGM法”などが知られている。

それらアルゴリズムは十分速く動作するが，その原理には，数論の理論が使われていて，現在もその改良の研究は続けられている。また最近“Weil descent法(特にGHS法)”という攻撃法が発見され，その防御のために現在は“素体

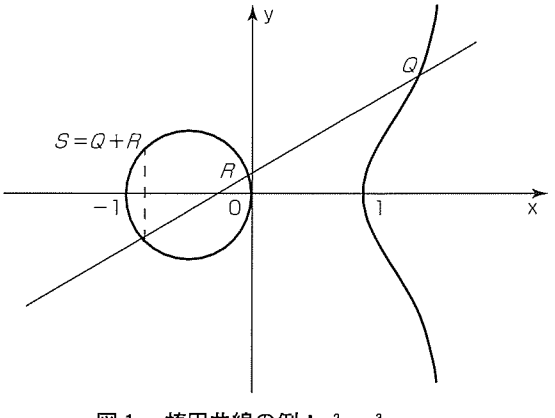



図1．楕円曲線の例：$y^2=x^3-x$

上素数次拡大有限体に値をとる楕円曲線有理点群”を使用することが推奨されている。

## 4. 暗号性能評価ソフトウェア

ここでは当社の暗号強度評価ソフトウェアについて概説する。この暗号強度評価ソフトウェアは大きく共通鍵暗号系と公開鍵暗号系に分けられ，前章までに示した各々の安全性評価の主要部分に対応する。以下，各々について解説する。

### 4.1 共通鍵暗号性能評価ソフトウェア

共通鍵暗号性能評価ソフトウェアの構成を図2に示す。

以下に，共通鍵暗号性能評価ソフトウェアを構成する各ソフトウェアの概要を説明する。

(1) 暗号安全性評価ソフトウェア

評価対象暗号の差分特性確率及び線形特性確率を評価する。また，擬似乱数生成に用いた場合の乱数性評価として，頻度検定，衝突検定及び線形複雑度を評価する。

(2) 暗号速度評価ソフトウェア

評価対象暗号の特定プラットフォーム上での暗号化／復号処理速度(絶対速度)を評価する。また仮想的なプラットフォームを指定し，そこでの処理速度(相対速度)を評価する。

(3) 性能評価対象暗号ソフトウェア

評価対象暗号として暗号アルゴリズムAES(Rijndael)，Serpent，CAST-256及びTwofishの安全性及び絶対速度評価の対象となる機能と，相対速度評価の対象となる機能を持っている。

(4) 暗号評価実行ベンチ

評価パラメータを操作する際のGUI機能を持っている。

(5) 評価結果表示ソフトウェア

評価結果を表示する際のGUI機能を持っている。

### 4.2 公開鍵暗号性能評価ソフトウェア

公開鍵暗号性能評価ソフトウェアの構成を図3に示す。

以下に，公開鍵暗号安全性評価ソフトウェアを構成する各ソフトウェアの概要を説明する。

(1) 公開鍵暗号基本演算ライブラリ

公開鍵暗号に関する基本演算ライブラリである。

(2) 素因数分解型暗号安全性評価ソフトウェア

素因数分解型公開鍵暗号の“二次ふるい法”及び“楕円曲線法”に基づく安全性を評価する。

(3) 離散対数型暗号安全性評価ソフトウェア

離散対数型公開鍵暗号のPohlig-Hellman法及びIndex Calculus法に基づく安全性を評価する。

(4) 楕円離散対数型暗号安全性評価ソフトウェア

楕円離散対数型公開鍵暗号の楕円曲線位数計算(SEA法)，

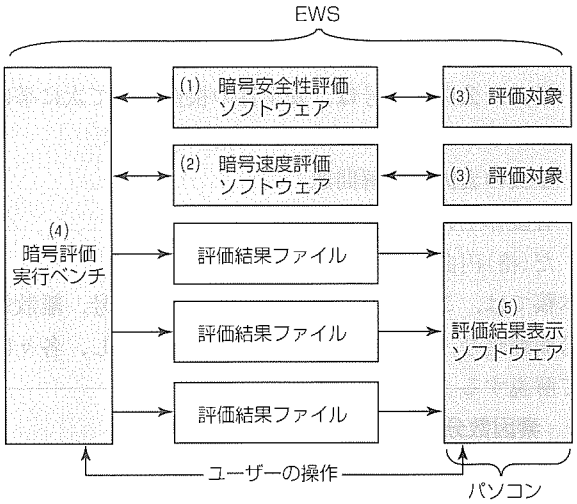



図2．共通鍵暗号性能評価ソフトウェア(構成図)

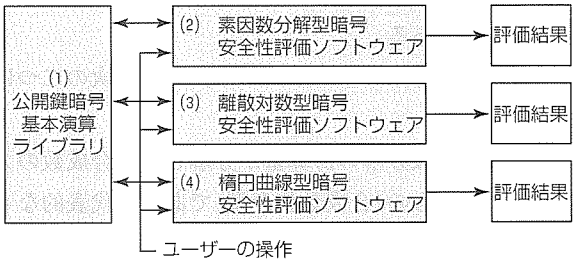



図3．公開鍵暗号性能評価ソフトウェア(構成図)

トレース計算及びMOV帰着次数計算に基づく安全性を評価する。

## 5. むすび

本稿では，共通鍵ブロック暗号及び公開鍵暗号の暗号強度評価技術に関して概説した。また，これらの暗号強度評価を実現するものとして，当社の開発した暗号性能評価ソフトウェアを挙げ，その機能面からの簡単な紹介を述べた。

(注) 本稿で示した暗号性能評価ソフトウェアは，情報処理振興事業協会の次世代デジタル応用基盤技術開発事業「暗号強度評価技術の開発」プロジェクトの成果を含む。

## 参考文献

(1) 情報処理振興事業協会セキュリティセンター：暗号技術評価報告書CRYPTREC Report 2000(2001-3)

(2) 通信放送機構：共通鍵ブロック暗号の選択／設計／評価に関するドキュメント(2000-6)

(3) Cohen，H.：A Course in Computational Algebraic Number Theory，Springer-Verlag(1993)

(4) 天田誠一，ほか：暗号性能評価ソフトウェアの開発，SCIS2000-A51(2000-1)

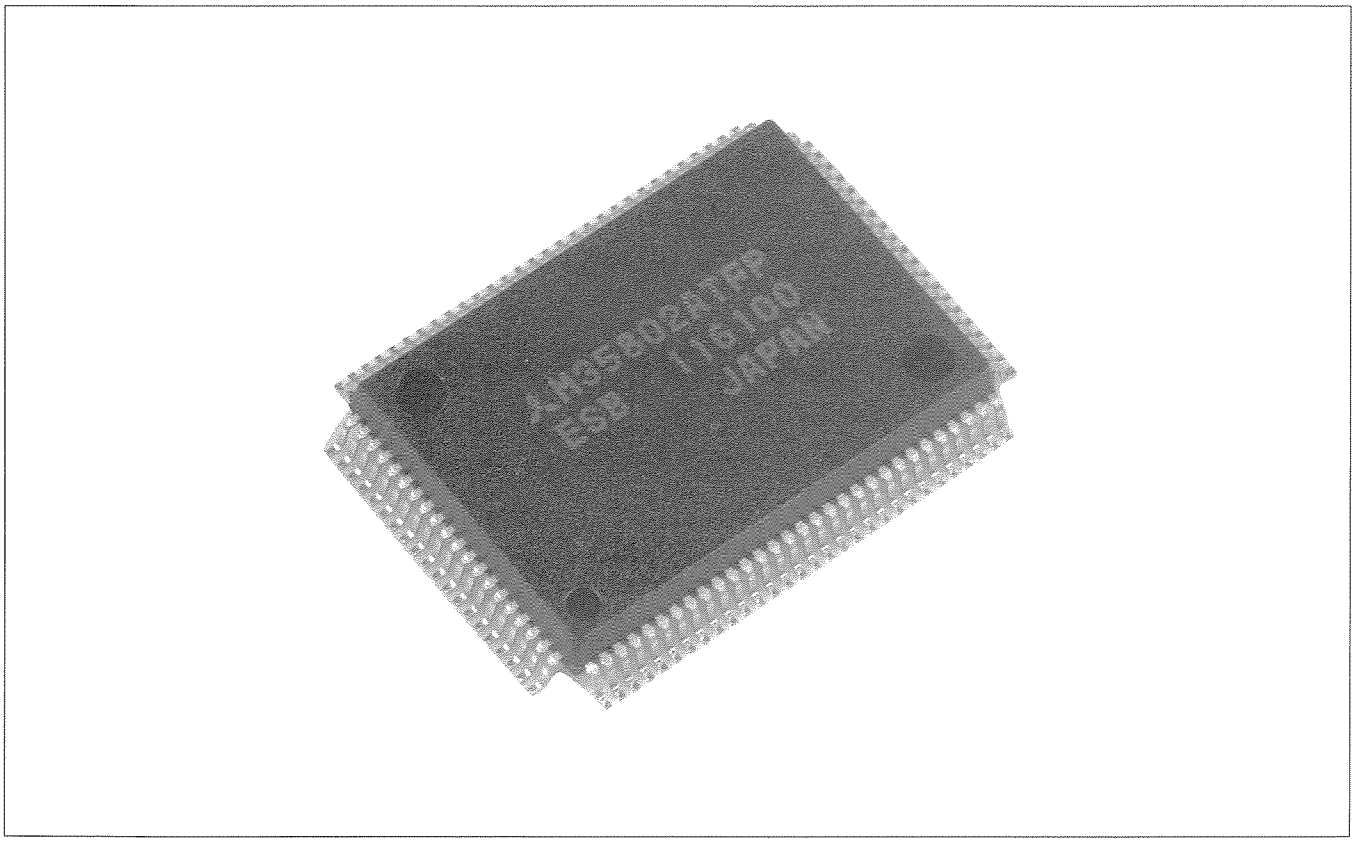
# 暗号アルゴリズムの実装

中嶋純子*　山岸篤弘*
市川哲也**
粕谷智巳*

**要　旨**

インターネットの普及に伴い，ネットワークにおける安全性の確保に注目が集まっている。安全性を確保するための中核技術である暗号アルゴリズムに関する研究開発は，米国のAES，我が国のCRYPTRECや欧州のNESSIEといったプロジェクトの影響もあり，新しい暗号技術（アルゴリズム）の提案が盛んに行われている。これらのプロジェクトで特徴的なことは，暗号の安全性（強度）を評価するだけでなく，実用化を視野に入れた評価も行われている点にある。つまり，暗号技術（アルゴリズム）を実際に使用する場合には，実装設計という過程を経てソフトウェア，ファームウェア（マイクロコンピュータ（以下“マイコン”という。）上での実装）やハードウェアという形態をとる必要があるため，高速実装法や小型化という実装面での研究開発も重要になりつつある。この実装技術の研究開発に当たっては，実装規模と処理性能のバランスをとることが重要となる。

本稿では，ソフトウェア，ハードウェアそれぞれの実装技術について述べる。特にハードウェアで実現する場合には，他の機能と組み合わせた暗号モジュール（暗号機能付きのASIC）として実現されることが多い。このような暗号モジュールを設計するための暗号機能の再利用可能な設計資産（Intellectual Property）についても触れる。



**暗号アルゴリズムを実装した１チップLSIの例**

RSA暗号やMISTY等の暗号技術をマイコンチップと組み合わせて実装した暗号LSIの実装例である。このLSIチップには，暗号アルゴリズムがハードウェア，ソフトウェア又はハードウェアとソフトウェアを組み合わせて実装されている。実装に当たっては，この暗号LSIが適用されるシステムの要求に合わせて，コストと性能の最適化を図った。

*三菱電機㈱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

暗号アルゴリズムは，ソフトウェアやハードウェアという形に実装することで初めて現実のシステムの中で使用することができるようになる。暗号アルゴリズムの研究開発は，米国のAES，我が国のCRYPTRECや欧州のNESSIEといったプロジェクトの影響で新しい暗号技術の提案が盛んに行われている。これらのプロジェクトで特徴的なことは，暗号の安全性(強度)を評価するだけでなく，実用化を視野に入れた評価(実装評価)が行われている点である。その結果，実装技術も大きく進歩している。

本稿では，暗号の実装技術について述べる。

実装に当たっては，使用する環境(プラットフォーム)やセキュリティポリシーを考慮した上で，実装規模と処理性能のバランスをとることが重要となる。以下，実装の形態(ソフトウェアでの実装とハードウェアの実装)に分けて述べ，最後にハードウェア実装の中でも最近注目を集めている再利用可能な設計資産(IP)についても触れる。

## 2. ソフトウェア実装

### 2.1 MISTY1の実装方法

ソフトウェアによる高速化手法には多くの手法が存在する。我々はこれまで，その幾つかの手法をMISTY1[(1)]に適用するとともに，プロセッサの特性に基づいたプログラミングの最適化について考察してきた[(2)~(5)]。

まずMISTY1の仕様図どおりの実装からスタートし，次に，テーブル生成やMISTY1の内部関数の等価変換を行うことにより，更なる高速化を図ってきた。これらのMISTY1アルゴリズムに対する実装方法のバリエーションとして，それぞれサイズの異なるテーブルを用いる下記(1)~(3)の3通りの方法が挙げられる。また，(4)に示す，並列処理に適した実装として知られているBit Slice実装もMISTY1に適用することが可能である。()内の数値はテーブルサイズである。

(1) 仕様図どおりの実装(2.3Kバイト)
(2) FI関数の等価変換による命令数の削減(2.3Kバイト)
(3) 動的なテーブル生成による命令数の削減(9.5Kバイト)
(4) Bit Sliceによる複数ブロックの並列実装(0Kバイト)

### 2.2 RISCプロセッサ上での実装

前記の(2)及び(3)の実装方法では，内部関数を等価変換した結果，テーブルサイズを著しく増加させることなく総命令数を減少させることができた。これらの手法を用いた場合のテーブルサイズは，Pentium(注)-Ⅱ/-ⅢやAlpha-21264などのプロセッサでは1次キャッシュサイズより小さく，実際にこの方法によって，これらのプロセッサで処理速度が大きく向上する[(6)(7)]。また並列処理による(4)の方法では，MISTY1のソフトウェア実装において最高の速度性能を達成した。

これら四つの方法では，スケジュールの実装もそれぞれ異なる。特に鍵に依存するテーブルを持つ実装の場合は，鍵スケジュール部でテーブル生成を行うため，その負荷が大きくなり実用上その時間が無視できない場合もある。したがって，鍵スケジュールの時間を含めた場合を考慮した上で，データサイズや用途に応じて最適な実装法を選択することが望ましい(表1，表2)。

### 2.3 他の暗号との比較

ソフトウェア性能を公平に比較するためには，プラットフォームの統一だけでなくコーディングスタイルや速度測定プログラムを統一することも必要となるが，実際にはアルゴリズムごとにまちまちのプラットフォームと測定方法で速度測定されているのが現実であり，これらを完全に統一して比較することは事実上不可能と考えられる。そこで，ここでは一案として，バイト単位の暗号化サイクル数という観点から現在知られている高速な実装結果をプラットフォームごとに分類せずにまとめた結果を図1に示す。

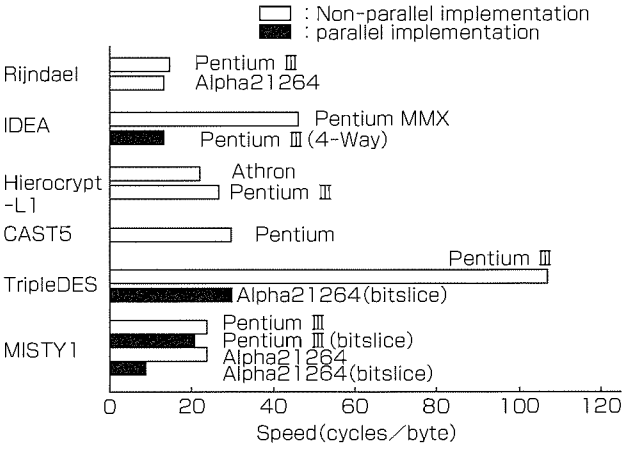
ここで，白色の棒グラフは通常の1ブロック単位での実装，黒色の棒グラフは並列処理を許した場合の速度である。

表1．Alpha21264(667MHz)

| 実装方法 | テーブルサイズ (Kバイト) | 拡大鍵生成 (cycles/key) | 暗号化速度 (cycles/block) |
|---|---|---|---|
| (1) | 2.6 | 109 | 245 |
| (2) | 4.6 | 200 | 197 |
| (3) | 18.9 | 12,450 | 192 |
| (4) | — | 17 | 68 |

表2．Pentium Ⅲ(800MHz)

| 実装方法 | テーブルサイズ (Kバイト) | 拡大鍵生成 (cycles/key) | 暗号化速度 (cycles/block) |
|---|---|---|---|
| (1) | 2.3 | 124 | 219 |
| (2) | 2.3 | 230 | 207 |
| (3) | 9.5 | 8,745 | 193 |
| (4) | — | 46 | 169 |




出典：Rijndael[(6)]，IDEA[(7)]，Hierocrypt-L1[(10)]，CAST5[(6)]，TripleDES(当社実測値)，MISTY1[(1)]

図1．暗号化速度(cycles/byte)

MISTY 1は，1ブロック単位での実装については他の64ビット暗号と同程度の速度だが，並列処理を許せば，レジスタ数の多いプロセッサ(Alpha21264)では128ビットブロック暗号であるRijndaelよりも断然高速になる。これは，MISTY 1がハードウェアで極めて小型なことに起因している。

### 2.4 マイコン上での実装

**表3**，**表4**に機器組み込みマイコン上でのMISTY 1の実装結果について示す。ここでは，三菱電機製マイコンであるM32R，M16C，及び，Z80をターゲットとする。M32RとM16Cはそれぞれ三菱オリジナルの，32ビット，16ビットマイコンである。これらは幅広いラインアップを持ち，一般産業／車載用途，デジタルAV，デジタルイメージング，携帯型民生機器などの様々な分野で広く使われている汎用的なマイコンである。今回は速度を優先するためにサブルーチンを用いずにすべて展開して記述したコードによる実装結果について示しているが，コードサイズを小さくすることを優先して実装することも可能である。Z80は，共通鍵暗号の8ビットマイコン上での実装性評価を行う際の標準的な環境である。8ビットマイコンにおいては，RAMの使用量が少ないことが望ましい。RAM使用量を少なくすることを優先した実装において，十分な小型化かつ高速化が実現できている。

## 3. ハードウェア実装

暗号アルゴリズムのハードウェア実装には，大きく分けて二つの側面がある。第一は，システム，アプリケーションに組み込むためのハードウェア実装である。これは，システム，アプリケーションの要求スペックの下で実装することであり，システム，アプリケーションごとにカスタマイズする必要がある。第二は，ハードウェア実装評価という側面である。これは，公平な評価条件の下で，可能な限り高処理速度な実装や小型化を意識した実装である。

### 3.1 アーキテクチャ設計

MISTY[1]，KASUMI[8]，Camellia[9]，AES(Rijndael)[11][12]など多くの暗号アルゴリズムは，基本的な関数を繰り返すループ構造を持っている。一般的に，このようなアルゴリズムのハードウェア実装アーキテクチャとしては，大きく分けて次のような構成が可能である(**図2**)。

(1) Fully Loop unrolled アーキテクチャ
(2) Loop アーキテクチャ
(3) Pipeline アーキテクチャ

図2の(1)は，F関数をn-round繰り返し行うアルゴリズムのFully Loop Unrolledアーキテクチャの実装例である。このアーキテクチャは，すべての繰り返し関数（round関数）を独立に実装し，1クロックでアルゴリズムの全演算を行うため回路規模は比較的大きくなるが，ループを構成するセレクタや中間値を格納するレジスタもないため遅延時間のオーバーヘッドが少なく，処理速度はアルゴリズム全体で最適化を図れるため比較的高い値を示す。

図2の(2)は，F関数をn-round繰り返し行うアルゴリズムにおいて，F関数を一つだけ実装した場合のLoopアーキテクチャの実装例である。このアーキテクチャは，基本的な関数のみを実装し，これを繰り返すことによってアルゴリズム全体の演算を行うため，回路規模の小型化に優れた方式である。一方，1回の暗号化処理で何度もループを回す必要があるため，ループを構成するためのセレクタやレジスタの遅延時間のオーバーヘッドが多く，処理速度は低くなる傾向がある。回路規模，ループの回数及び処理速度は，ループを構成する基本演算回路の選択によって決まる。

図2の(3)は，F関数をn-round繰り返し行うアルゴリズムをnステージのPipelineアーキテクチャで実装した例である。このアーキテクチャは，アルゴリズム全体を幾つかの機能ブロックごとの動作ステージに分割し，動作ステージごとにレジスタを挿入し，さらに，各動作ステージが互いに独立に動作できるように構成する。このため，回路規模はレジスタ分だけFully Loop unrolledアーキテクチャより大きくなるが，処理速度は各ステージの並列動作によって極めて高い性能を発揮することが可能である。しかし，このアーキテクチャを用いて暗号を利用する場合には，暗

表3．三菱電機製マイコン

| マイコン (MHz) | 拡大鍵生成 (cycles/key) | 暗号化速度 (cycles/block) | ROM／RAM (Kbyte／byte) |
|---|---|---|---|
| M16C(20) | 743 | 1,877 | 3.4／64 |
| M32R(100) | 387 | 793 | 3.7／76 |

表4．Z80

| 拡大鍵生成 | 暗号化速度 (1 block) | ROM (コード+S-box) | RAM (拡大鍵／スタック) |
|---|---|---|---|
| 3,283ステート | 13,553ステート | 1,992バイト | 64バイト／10バイト |

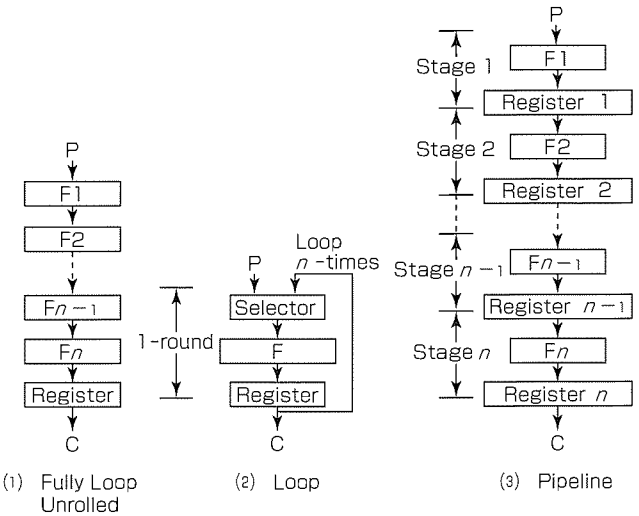



図2．ハードウェア実装アーキテクチャ

号アルゴリズム自体のループバック処理を実現することは困難であることに注意が必要である。

暗号アルゴリズムは，現在FIPS(Federal Information Processing Standard)にて示されている暗号利用モード[13][14]を使用して実装されることが多く，暗号アルゴリズムで処理したデータをフィードバックして次の処理に連鎖させていくモード，すなわち，CBC(Cipher Block Chaining)，OFB(Output Feedback)及びCFB(Cipher Feedback)モードと，連鎖を伴わない利用モードのECB(Electronic Codebook)モード及びCTR(Counter)モードがある。

CBC，OFB及びCFBモードを考慮した場合，(1)のアーキテクチャが処理速度を重視した実装に適している。また，ECB及びCRTモードを考えた場合は，(3)のアーキテクチャが適している。一方，回路規模を重視した実装に適しているのは(2)のアーキテクチャであり，このアーキテクチャは，現在のすべてのモードに対応可能である。

### 3.2 実装に対する考察

これまで我々はMISTY，Camelliaを始めとする種々の共通鍵暗号アルゴリズムやRSA等の公開鍵暗号アルゴリズムに用いられている，“べき乗剰余演算”を取り上げ，ASIC(Application Specific Integrated Circuit)及びFPGA(Field Programmable Gate Array)を用い，ハードウェア実装を行ってきた[15]~[22]。特に，FPGAに関しては，現在，海外の評価等でも多く用いられているXilinx社製のVirtex-Eシリーズ，VirtexⅡシリーズを用いた実装を行ってきた。

近年のハードウェア実装には，VHDL，Verilog-HDL等のHDL(Hardware Description Language)が用いられることが多く，参考文献(15)や(23)に記述されているように，HDLの記述方法や実装するデザインの表現方法の差異によって出来上がるハードウェアの性能が異なってくる。また，実装するターゲットデバイスの違い，すなわち，ASICへの実装とFPGAへの実装では，HDLの記述方法を異にした方がより効率の良い実装が可能となると考えている。

また，ハードウェア実装を行う上で，3.1節の(1)，(2)，(3)又は複合アーキテクチャを用いて実装することを決定するために，回路規模と処理速度のトレードオフ検討，すなわち，回路規模と処理速度のどちらを重視して実装するか，また双方とも重視して実装するのかを決めることも重要となる。

暗号アルゴリズムのハードウェアを実現するためには，ハードウェア設計技術のほかに数学等の知識が必要になってくる。例えば，共通鍵暗号アルゴリズムは，SBOXと呼ばれる非線形な置換表が用いられることが多く，近年，このSBOXはガロア体の演算を基調としているアルゴリズムが増えてきている(MISTYのS7，S9，CamelliaのS1～S4，AES(Rijndael)のSBOXなど)。このため，特に，小型化ハードウェアを実現するためには，数学等の知識は重要なポイントとなり，これらSBOXの小型化を考えるためには，ガロア体の演算知識及び論理圧縮技術が必要になってくる。

このように，効率の良い(性能の良い)実装を行うためには，ハードウェア設計技術，回路規模と処理速度のトレードオフ検討，暗号アルゴリズムの知識及び特徴，数学の知識のみならず，ターゲットDeviceの特徴，論理合成技術など，様々な技術が必要となる。

## 4. セキュリティLSI開発用暗号アルゴリズムIP

ASICやFPGAをターゲットとした開発では，再利用可能な設計資産(機能ブロック)を，一般にIP(Intellectual Property)と呼ぶ。半導体技術の進歩により，大規模LSIを短期間に開発することが可能となり，IP再利用は大規模LSIの設計効率を大幅に向上させる有力な方法となっている。

一方，現代のネットワーク社会では，インターネットや携帯電話，DVD，ICカードなど様々なところで暗号機能を持ったLSIが使われ始めている。このようなセキュリティ機能を持ったLSIを迅速に開発するための手段として，また前節で述べた実装技術を製品に反映させるための手段として，セキュリティLSI開発用暗号アルゴリズムIP(以下“暗号IP”という。)の開発を行った。

### 4.1 IPの分類

IPの分類は様々だが，一般に以下の3種に分類される。

(1) Soft-IP

論理合成可能なHDLで供給される。種々のLSI製造プロセスに対応可能で柔軟性が高い。

(2) Firm-IP

論理合成可能なHDL，LSI製造プロセスライブラリ，フロアプラン情報，又はネットリストで供給される。

(3) Hard-IP

特定のLSI製造プロセス用に配置配線されたレイアウトデータで供給される。一般に特定のLSIプロセス向けに最適化されており，性能の予測性が高い反面，柔軟性が低い。

今回開発した暗号IPは，上記のSoft-IPに相当するものである。しかし，一般のSoft-IPの供給形態である論理合成可能なHDLは，通常可読であるため，リバースエンジニアリングによる小型化技法，高速実装技法等のノウハウの流出が阻止できなかった。また，高度な実装技術やノウハウの公開を前提としてしまうため，価格も高価であった。そこで，我々は，LSI開発における論理合成ツールの業界標準となっている米国Synopsys社のDesignCompiler用のライブラリとして暗号IPを開発した。この手法を用いることで，Soft-IPの持つ様々なLSI製造プロセスに対する高

い柔軟性を損なわず，かつ実装ノウハウの流出を防いで，安価にIPを提供することが可能となった。

この暗号IPにはライセンス管理機能及びIP自体の暗号化機能が組み込まれており，実装ノウハウの保護が可能である。

### 4.2 暗号IPの構成

暗号IPとしての提供内容を**表5**に，サポート暗号アルゴリズムを**表6**に示す。

最新暗号アルゴリズムのサポートだけでなく，**図3**に示すようにカスタマイズや開発環境の提供等のサービスも技術供与として包含している点が特長である。

## 5. むすび

今後の展開としては，だ(楕)円曲線暗号を始めとした，最先端暗号アルゴリズムの迅速な対応が挙げられる。また，実装面での処理性能の向上及び小型化という永遠の課題以外にも，暗号機能を利用するためのユーザーインタフェースの標準化とバリエーションの増加という課題がある。

一方，実装性の評価という側面では，評価基準の確立という課題が残されている。

さらに，暗号IPの利用という面では，より小型・高速化を期待できるFirm-IP，Hard-IPや近年進歩が著しいFPGAに特化したIPの整備だけでなく，技術的なコンサルティングを含めたトータルなサポート体制の確立が必須であると考えている。

**表5．暗号IP提供内容**

| 項　目 | 内　容 |
|---|---|
| 論理合成ツールライブラリ | Standard<br>Evaluate(評価のみ) |
| シミュレーションモデル | Verilog-HDL動作モデル<br>VHDL動作モデル<br>PLIモデル |
| テストベクタ | 論理シミュレーション用<br>製造テスト用 |
| サンプル記述 | Verilog-HDL／VHDL<br>論理合成用スクリプト |
| サービス・その他 | バージョンアップデート<br>I/F回路カスタマイズ<br>FPGAボード等の開発環境 |

**表6．暗号IP提供時期**

| 提供開始 | サポートアルゴリズム |
|---|---|
| 2001年Q2～ | Camellia，MISTY，KASUMI |
| 2001年Q3～ | AES，RSA暗号アクセラレータ |
| 2001年Q4～ | SHA－1 |
| 2002年Q3～ | SHA－192，256，384 |

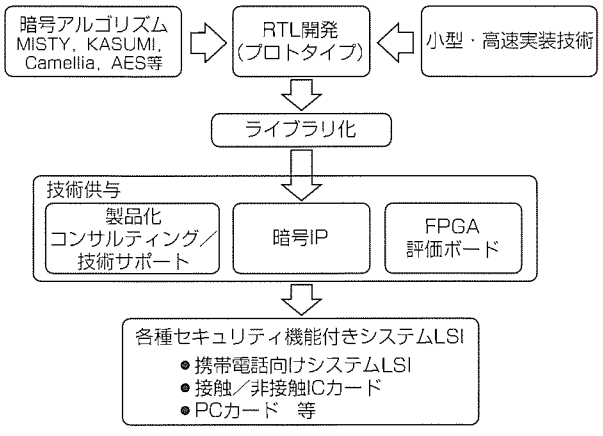



**図3．暗号IPの位置付け**

## 参考文献


(1) Matsui，M.：New Encryption Algorithm MISTY，Proceedings of the Fourth International Workshop of Fast Software Encryption，54～86(1997-1)

(2) 中嶋純子，ほか：共通鍵MISTY 1の最適なソフトウェア実装について，SCIS'2001(2001-1)

(3) Nakajima，J.，et al.：Fast Software Implementation of MISTY 1 on Alpha Processors，IEICE Transaction，E82-A，No.1，107～116(1999-1)

(4) 中嶋純子，ほか：MISTYのソフトウェアによる高速実装法について(Ⅱ)，SCIS'98-9.1.B(1998-1)

(5) Matsui，M.，ほか：MISTYのソフトウェアによる高速実装法について(Ⅲ)，ISEC'2000(2000-11)

(6) Weoss，R.：A comparison of AES candidates on the Alpha 21264，Proceedings of the Third Advanced Encryption Standard Candidate Conference(2000-4)

(7) Lipmaa，H.：Fast IDEA for Pentium MMX compatibles，http://www.tml.hut.fi/～helger/fastidea/

(8) ETSI/SAGE. KASUMI specification：Specification of the 3GPP Confidentiality and Integrity Algorithms Document 2，ETSI/SAGE(1999-12)

(9) 青木和麻呂，ほか：128ビットブロック暗号，信学技報，ISEC2000-6(2000-5)

(10) 佐野文彦：Hierocryptの実装について，SCIS'2001(2001-1)

(11) Advanced Encryption Standard，FIPS 197(2001-11)

(12) AES Algorithm(Rijndael)Information，http://csrc.nist.gov/encryption/aes/rijndael.

(13) DES Modes of Operation，FIPS 81(1980-12)

(14) Recommendation for Block Cipher Modes of Operation-Methods and Techniques，SP 800-38A(2001-12)

(15) 市川哲也，ほか：秘密鍵暗号のH/W設計に関する考察，1997年暗号と情報セキュリティシンポジウム，SCIS97－9D(1997-1)

(16) 市川哲也，ほか：秘密鍵暗号MISTY 1のH/W実装における一方法，1998年暗号と情報セキュリティシンポジウム，SCIS98-9.1.A(1998-1)

(17) Ichikawa, T., et al.：Hardware Evaluation of the AES Finalists, in The Third AES Candidate Conference, printed by the National Institute of Standards and Technology, Gaithersburg, MD, 279～285(2000-4)

(18) 青木和麻呂，ほか：128ビットブロック暗号Camelliaの実装評価，信学技報，ISEC2000-73(2000-9)

(19) 市川哲也，ほか：128bitブロック暗号のハードウェア実装について(Ⅲ)，2001年暗号と情報セキュリティシンポジウム予稿集，SCIS2001-12A-5，669～674(2001-1)

(20) 市川哲也，ほか：ブロック暗号のハードウェア実装に関する評価指標について(1)，信学技報，ISEC 2001-53(2001-9)

(21) 反町　亨，ほか：ブロック暗号のハードウェア実装に関する評価指標について(2)，信学技報，ISEC 2001-54(2001-9)

(22) 長谷川俊夫，ほか：冗長2進表現を利用したべき乗剰余演算回路の分割処理，　計算機アーキテクチャ研究会98-ARC-129-8(1998-5)

(23) Satoh, A., et al.：A Compact Rijndael Hardware Architecture with S-Box Optimization, Advances in Cryptology-ASIACRYPT 2001, LNCS 2248, 239～254(2001)

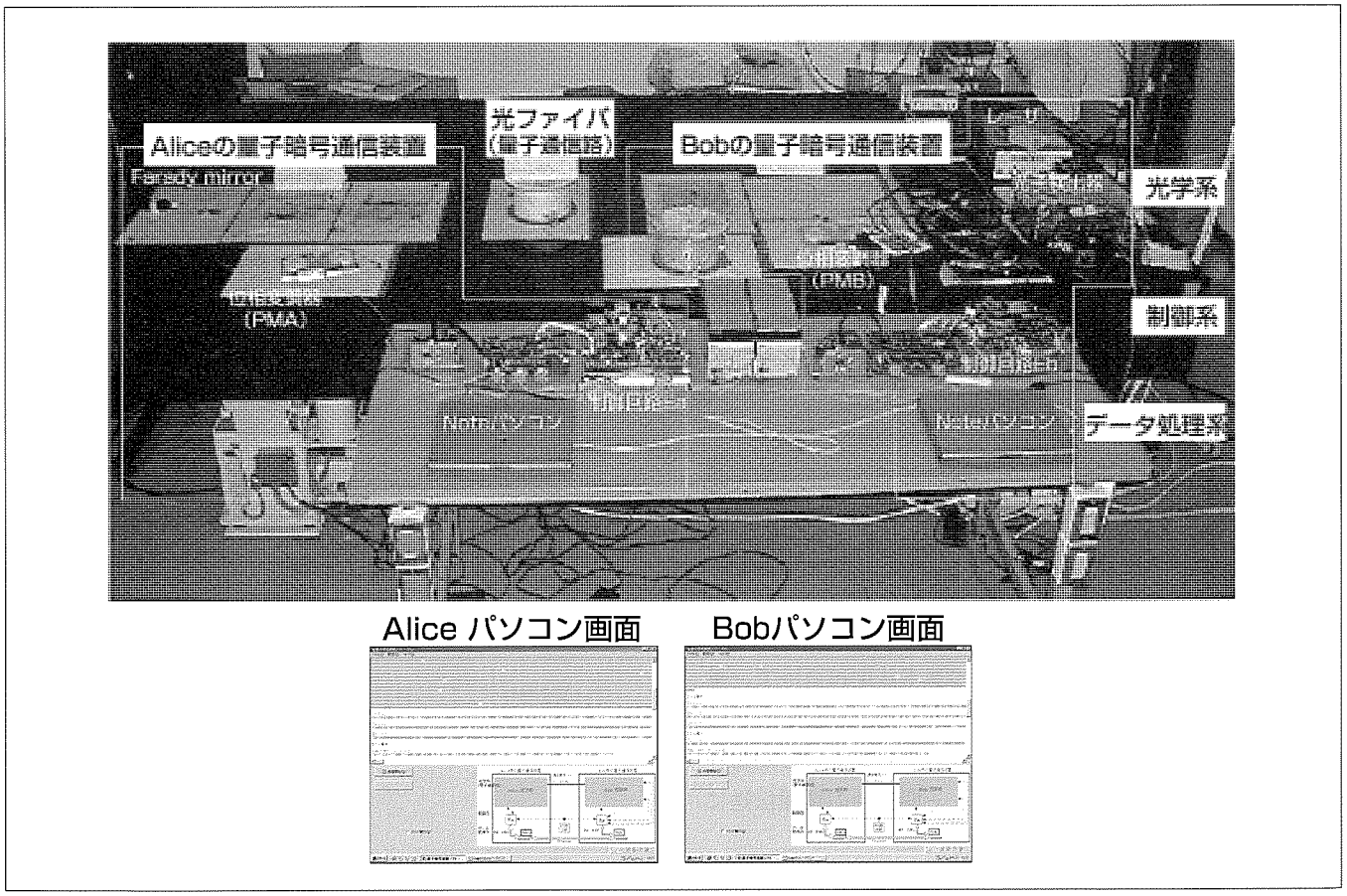
# 量子暗号技術

長谷川俊夫*　安部淳一**
西岡　毅**
石塚裕一*

**要　旨**

量子暗号は，計算機科学と物理学が融合した新しい暗号技術である。特長は，絶対的な安全性が保証されるという点である。またさらに，盗聴されたら検知可能であるという特長も持っている。現代暗号がその安全性の根拠を計算量(時間)に置いているのに対して，量子暗号は，物理の基本法則に基づいて構成されているため，絶対的な安全性が保証されている。このため，将来の計算機性能向上にも，またたとえ新しい概念に基づく量子計算機が実現したとしても全く脅威を受けることがない安全なセキュリティシステムを提供することが可能となる。

本稿では，このような絶対的な安全性を持つ究極の暗号と期待される量子暗号技術について解説する。最初に量子暗号の基本原理について説明し，この物理的な実現方法について示す。次に，三菱電機が国内で初めて量子暗号通信システム実験に成功したが，そのシステム実験について，光学部分，電子制御部分，データ処理部分について説明し，具体的なシステム性能やユーザーI/Fについても紹介する。




**当社の量子暗号通信システム実験**

当社は，北海道大学電子科学研究所竹内助教授と共同で量子暗号の情報セキュリティシステムとしての実現を図り，2000年9月に国内で初めて量子暗号通信システム実験に成功した。量子暗号は，安全性の根拠が計算量理論(計算時間)に基づく現代暗号と異なり，絶対的な安全性を持つだけでなく，盗聴者の検知も可能である。当社の実験では，光ファイバを選択し実現したため，将来既設光ファイバ網に適用可能という点でも大きな意味がある。また，量子暗号をシステムとして実現しており，現実の系において生じるエラー等も除去できるようなデータ処理機能も含んでいる。

*情報技術総合研究所　**同研究所(理博)

## 1. まえがき

情報科学と量子力学の融合によって登場した量子情報技術は，P. Shorによる高速に素因数分解を行う量子コンピュータの提案以来，華々しい脚光を浴びている。これは，公開かぎ(鍵)暗号のような計算量理論に安全性の根拠を置く現代暗号技術が容易に解読される可能性を提示したためである。このように量子情報技術は，情報セキュリティ技術に対して量子コンピュータという鋭い“矛”をもたらしたが，一方で，量子暗号という頑強な“盾”も提供してくれている。この盾は，計算量的安全性に依存しない，いわば，量子力学的安全性という全く新しい安全性の概念に基づく暗号技術である。

このため，量子暗号技術は，現代暗号技術で必然的に脅威となっていた超高性能計算機の出現に対しても絶対的に安全性が保証される。その上，盗聴検知機能というこれまでにない新しい機能も備えているため，“究極の暗号”として期待されている。

本稿では，この量子暗号技術に対して，基本原理と実現方法に簡単に触れ，量子暗号特有のデータ処理について概説した後，当社が国内で初めて成功した量子暗号システム実験を紹介する。

## 2. 量子暗号技術とは

量子暗号技術の中でも最も成功を収めており実用化の最右翼にある量子鍵配布プロトコルについて解説する。このプロトコルは，遠く離れた通信2者(アリスとボブ)の間で秘密鍵を絶対安全に共有するものである。

### 2.1 量子暗号の基本原理

量子暗号では，古典通信と異なり，量子(光子)一個一個に個別の情報を載せて伝送することが基本である。このため，量子力学的効果が前面に現れ，基本法則である不確定性原理と複製不可能定理が重要な役割を果たす。複製不可能定理とは，未知の量子状態の完全な複製を作成することができないことである。また，不確定性原理によると，同時観測できない物理量が存在する。すなわち，一つの物理量を正確に観測すると，もう一つの物理量が全くでたらめになってしまうのである。これらの基本法則によって，量子に情報を載せた状態(キュービット)はその複製ができないし，観測すると2回に1回は失敗してしまうことが物理的に保証されるのである。いわば，一期一会の情報伝送になる。

これを利用して鍵共有を実現するプロトコルが量子鍵配布プロトコルである。この中でも最も有名なBB84プロトコルを図1を基に紹介しよう。

アリスは1キュービットに対して四つの状態を用意する。この四つの状態は二つで一つのペアをなしている。各ペアは一つの物理量に対応しており，一つのペアを正しく測定しようとするともう一つのペアは正しく測定できなくなる。ボブは，この二つのペアに対応した2種類の測定器を持っており，正しい測定器を選択したときのみ正しく状態が測定できる。間違った測定器を選択したのでもう一回測定を行う試みは，前述の物理法則によって不可能である。鍵共有の処理手順は次のとおりである。

(1) アリスとボブは独立に乱数を用意する。アリスはこの乱数に従ってキュービット1個ごとに四つの状態の一つをランダムに選択し，ボブに量子通信路を通じて伝送する。ボブは独立に生成した自分の乱数に従い，二つの測定器から一つをランダムに選択し，伝送されたキュービットを測定する。測定結果は秘密に記録しておく。

(2) キュービットの伝送が済んだら，ボブはどの測定器を用いたかをアリスに連絡し，アリスはその中からどれが正しい測定器を用いていたかを回答する。これは，(盗聴される危険のある)公開通信路で行ってよい。

(3) 次に，アリスとボブは正しい測定が行われたキュービット列のみを抽出すると，2者間で秘密にキュービットの列が共有されたことになる。これを情報ビットに焼き直すと秘密共有ビット列が現れる。

ただし，現実の系では，この共有ビット列中には若干のエラーや盗聴者によるじょう(擾)乱も挿入されている。そこで，現実の環境では，**3章**で述べるような量子暗号特有のデータ処理が必要になる。この処理で，ビットエラーの誤り訂正と盗聴者に漏えい(洩)する情報をできるだけ小さくするプライバシー増幅が実行される。また，ビットレートや量子ビットエラーレート(QBER)も評価するため，盗聴者がいれば，その擾乱が検知されるので，盗聴検知が可能となる。

### 2.2 実現方法

量子暗号を実現する際には，原理的には様々な2状態の量子系が利用可能であるが，これまでの実験では，情報の媒介粒子として光子が用いられている。その理由は，光の扱いやすさと光通信の過去の実績からである。

また，光子への情報の符号化方法には主に，偏光を用いたものと，位相変調を用いたものの二つの方式がある。そ

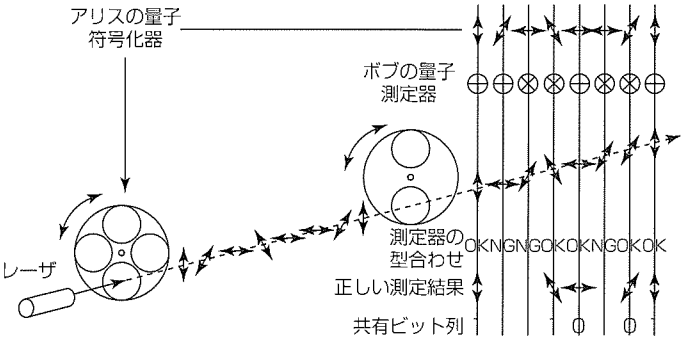



図1．BB84プロトコル(鍵配布)の構成

して，光子が伝達される通信路としては，空気中と光ファイバが考えられる。さらに，鍵共有プロトコルとしては，代表的なBB84プロトコル以外にも，B92，E91，その他幾つかのプロトコルが提案されている。そのため，実現には幾つもの選択肢がある。これまで実験は，IBM，ジュネーブ大学，米国ロスアラモス国立研究所，我々の成果も含めて幾つか量子暗号の実験が行われているが，代表的なものは位相符号化方式で，光ファイバ伝送の実現である。ここでは，光子の生成，伝送，検出の三つを説明する。

#### 2.2.1 光子の生成

量子暗号の情報媒体は単一光子である。現在は，パルスレーザから出た光を減衰器で十分減光し近似的に単一性を実現しているのが通例である。例えば，パルス当たりの平均光子数を0.1個として，2個出る可能性をほとんど無視できる確率に落とす。また，この影響は，後述のデータ処理を施すことで十分に無視することができる。しかし，単一光子生成技術が確立されれば，現在よりも更に高速な量子暗号通信が実現でき，その他の量子情報技術においても重要な要素技術であるため，今後の研究課題でもある。

#### 2.2.2 光子の伝送

自由空間と光ファイバ伝送の2種があるが，系の安定性を保つのが比較的容易なため，現在は光ファイバを用いた実験が主流である。光ファイバ伝送では，その扱いやすさから，符号化方式として位相変調が用いられる。特に，Mach-Zehnder干渉系などを利用して実現される。ただし，複屈折や偏光モードの分散などにより光子の偏光は影響を受けるため，安定した系を構築するために十分考慮する必要がある。また光の波長帯としては，短波長帯と長波長帯があるが，伝送損失の観点のみからいえば長波長帯が長距離通信に向いている。

自由空間の伝送では，近年短波長帯で衛星通信などの実験がなされており，新たな可能性が追求されている。

#### 2.2.3 光子の検出

単一光子検出に関しては，現状での最良の方法は，APD（Avalanche Photo Diode）と呼ばれるデバイスを用いた方法である。その通信波長帯により，Si，Ge，InGaAsの三つの異なる半導体が使われている。短波長帯では室温で検出効率が高い検出器が存在するが，1.55μm帯などの長波長帯では，InGaAsなどで実験がなされているが検出効率は低いという問題点がある。また長波長帯では数十K程度に冷却するために装置が巨大化してしまうため，量子暗号に特化した効率的なAPDの開発が望まれている。

## 3. 実際のシステムに必要なデータ処理

量子暗号の絶対的安全性の議論は，理想的な条件の下，BB84等の量子鍵配送方法が盗聴者の介在を不確定性原理によって必ず検出できるとするものである。しかし，現実の実装環境においては，不可避の物理的エラーが存在する。このため，盗聴者イブは，この物理的エラーに紛れて，アリスとボブに検知されずに部分情報を盗む可能性もある。通常，エラーが起きたビットは潜在的にイブによる不正行為が行われた可能性が高く，したがって，当該ビットを検出し除去することができればより高い安全性が得られる（誤り訂正）。しかし，例えば非常に小さな確率であるが光子発生器が光子を2個同時に送出してしまった場合など，イブは量子通信回線中に誤りを起こすことなく，つまりアリス，ボブに気付かれることなく，そのうちの1個の光子を分離して情報を盗むことができる。このように，誤りのビットを除去してもなお部分情報が漏洩している可能性がわずかであるが存在する。この情報をより小さな空間に一様に写像することで，イブへの情報漏洩をなくそうとするのがプライバシー増幅と呼ばれる方法である。ここでは，データ処理の概念を紹介する目的で，各々最も簡単な処理例を一つずつ紹介する。

### 3.1 誤り訂正（簡単な例）

①アリスは2ビットの組をランダムに選び，その排他的論理和（XOR）値を公開する。②ボブは対応するビットのXOR値が同じかそうでないかをアリスに伝える。③同じであった場合，ビットの組の最初のビットを保存し，2番目のビットを捨てる。④異なる場合は両方のビットを捨てる。ちなみに，③で2番目のビットを捨てるのは量子暗号特有の安全性を保ちつつ誤り訂正をするためであり，これからイブへの1ビット漏洩を反故にすることができる。

### 3.2 プライバシー増幅

①アリスは再び2ビットの組をランダムに選び，そのXORを計算する。しかし，今度はその値を公開しない。②アリスはどのビットを選んだのかのみアナウンスする。③アリスとボブはそれぞれその二つのビットをXOR値に置き換える。これにより，イブが1番目のビットのみを知っていて2番目のビットを知らない場合は，XOR値に関しては何の情報も得られない。また，イブが両方のビットをある確率で知っている場合も，彼女がXOR値を正しく推定できる確率を下げることができ，安全性が増幅される。

## 4. 当社の量子暗号通信システム実験

ここで，当社の量子暗号通信システム実験を説明する。

### 4.1 実験システムの構成

実験システムは，**図2**に示したとおり，光学系，制御系，データ処理系の三つの系で構成される。

(1) 光学系

主に，光子を送信するパルスレーザ，伝送路である光ファイバ，光子を検出する光子検出器などで構成される。ここでは位相変調での実現方式を採用しているため，2者で

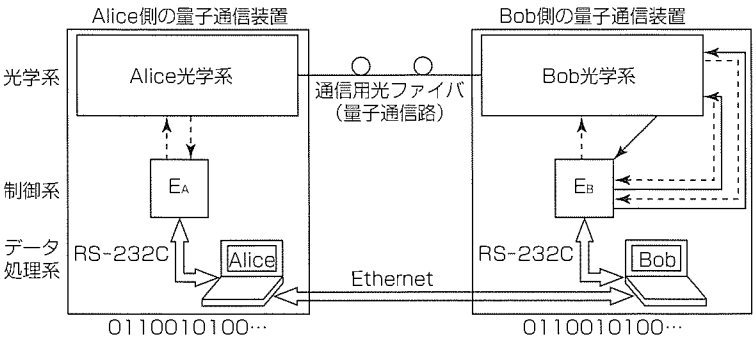



図2．量子暗号通信システムのシステム構成

表1．システムの機能と性能

| 動作環境 | 室温で動作 |
|---|---|
| 機　能 | 1．通信2者間で絶対安全な鍵共有<br>2．通信路上での盗聴検知<br>3．通信エラー等の安全な訂正機能 |
| システム性能 | 1．通信距離　：200m(1km)<br>2．鍵共有速度：1.1kbps(0.7kbps)<br>3．エラー率　：1.7%(5.0%) |

位相変調器を持ち，光子に情報が載せられる。

(2)　制御系

光子に情報を載せるため，位相変調器をタイミングよく電子制御する。また，光子の検出結果も格納する。

(3)　データ処理系

パソコン上で01のデジタルデータを生成し制御系に転送し，制御系でそれに対応した電圧をかけることで光学系での位相変調を行う。また，量子鍵共有プロトコルを光通信の後に実施し，2者間で同じデータ(秘密鍵)を共有する。

### 4.2　システムの機能とその性能

今回は，量子暗号通信システムを構築するに当たり，鍵共有プロトコルとしてBB84プロトコルを，符号化方式として位相変調方式を，通信路として光ファイバを，光の波長帯として830nmを採用した。今回の実験システムの機能と性能は**表1**のとおりである。量子暗号を，原理検証実験ではなく，データ処理機能まで含んだシステムとして実現した[(2)(3)]のは国内で当社が初めてであり，意義は大きい。また通信速度(鍵共有速度)1.1kbps，エラー率1.7%は，共に世界最高レベルの性能を達成することができた。また，通信距離に関しては，1kmでも実験に成功している[(4)]。速度も暗号の秘密鍵の共有という用途を考えれば実用的ともいえる。この実験値(通信距離，速度，エラー率)は特に最適化はしたものではないため，今後，性能の向上が期待できる。またこれとは別に，量子暗号の光学系において新しい方式を考案したことにより，より簡単な系で鍵共有速度を従来方式の約6倍高速にすることが可能で，多人数への拡張可能な量子暗号の実証実験にも成功している[(5)]。

### 4.3　ユーザーI/F

要旨のページに示したとおり，この実験システムは，パソコンの画面から容易に操作できるユーザーI/Fを持っている。

## 5. むすび

本稿では，量子暗号技術に関してその概要と実現方法について説明した。また，我々が成功した量子暗号システム実験についても，具体的な実験構成やパソコン上でのユーザーI/Fについても示し，量子暗号の情報セキュリティシステムとしての実現に関して紹介し，その実用性についても説明した。今後は，実用化に向けて，更なる高性能化を図る所存である。

## 参考文献

(1)　西岡　毅，ほか：量子暗号－－理論と実験，数理科学(2000-9)

(2)　三菱電機NEWS RELEASE，(2000-9-14)

(3)　長谷川俊夫，ほか：量子暗号通信システム実験，QIT 2000-42，(2000-11)

(4)　Hasegawa，T.，et al.：An Experimental Realization of Quantum Cryptosystem，IEICE Trans.Fundamental，**E85-A**，No.1，(2002)

(5)　Nishioka，T.，et al.：Circular Type Quantum Key Distribution，IEEE Photonic Technology Letter (to appear in 2002)

# セキュリティライブラリ

辻　宏郷*
齋藤和美*

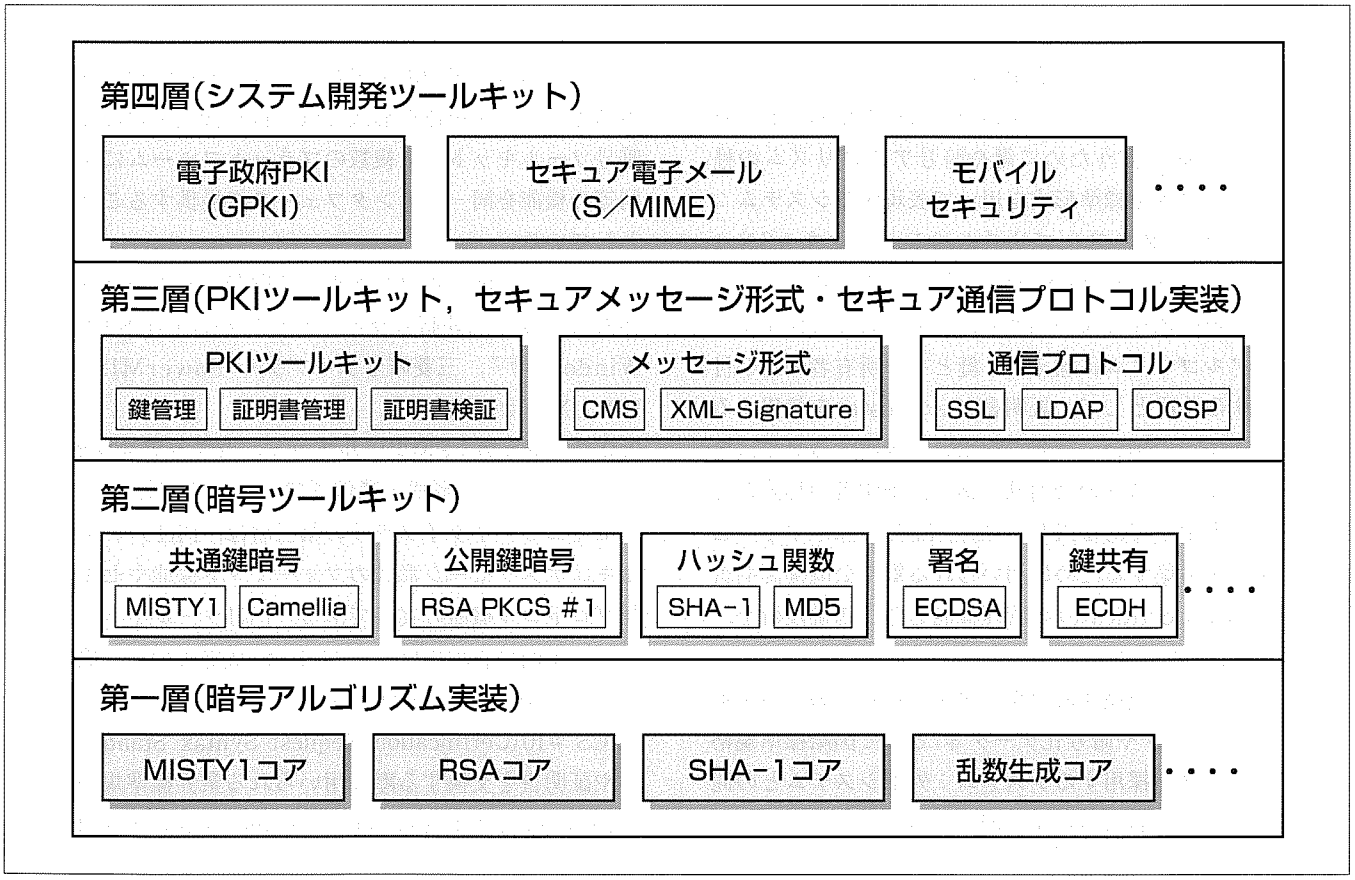
**要　旨**

セキュリティライブラリは，暗号技術を用いた情報セキュリティシステム開発に必要となる基盤技術(暗号アルゴリズム及び関連技術)を実装したミドルウェアである。情報セキュリティシステム構築には各種暗号アルゴリズム，かぎ(鍵)及び証明書の管理機能，セキュアメッセージのフォーマット機能，セキュア通信プロトコル等の実装が必要であり，必要となる暗号アルゴリズムやセキュリティ機能は，システムごとに異なっている。

三菱セキュリティライブラリでは，様々なシステム要件に対応するために，4階層モデルからなるアーキテクチャを設計した。このアーキテクチャでは，第一層：暗号アルゴリズム実装，第二層：暗号ツールキット，第三層：PKI(Public Key Infrastructure)ツールキット，セキュアメッセージ形式・セキュア通信プロトコルの実装，第四層：システム開発ツールキットと定義し，各層の構成要素となるライブラリ，コンポーネントを実装した。

PKI暗号ライブラリ"MCrypto"は，第二層及び第三層に対応する構成要素で，暗号アルゴリズム独立，鍵管理・証明書管理機能，証明書検証機能，生体識別情報を用いた認証機能等の特長を持っている。組み込み機器向け暗号ライブラリ"MC"は，第一層に対応する構成要素で，省資源での動作，可搬性といった組み込み機器での要件を満たすために，必要メモリ容量を制御・削減可能なメモリ管理方式，必要機能に応じたモジュールの再構成，プラットフォームごとに最適化したアルゴリズム・コア採用等の特長を持っている。

今後は，サポートするプラットフォームの拡大や最新標準規格への対応を行っていく予定である。




**三菱セキュリティライブラリのアーキテクチャ(4階層モデル)**

セキュリティライブラリの実装において，4階層モデルからなるアーキテクチャを設計し，各層において提供すべき機能を定義した。第一層は，暗号アルゴリズム(共通鍵暗号，公開鍵暗号，ハッシュ関数等)の実装である。第二層は，暗号ツールキットである。第三層は，PKIに対応する鍵管理機能・証明書管理機能等を実装したPKIツールキット，セキュアメッセージのフォーマット機能とセキュア通信プロトコルの実装である。第四層は，アプリケーションごとに特化したインタフェースを提供するシステム開発ツールキットである。

*情報技術総合研究所

## 1. まえがき

セキュリティライブラリは，暗号技術を用いた情報セキュリティシステム開発に必要となる基盤技術(暗号アルゴリズム及び関連技術)を実装したミドルウェアである。情報セキュリティシステム構築には，各種暗号アルゴリズム，鍵及び証明書の管理機能，セキュアメッセージ形式のフォーマット機能，セキュア通信プロトコル等を実装する必要がある。三菱電機では，社内開発用ミドルウェアとして，様々なセキュリティライブラリを実装し，システム開発に適用するとともに，ユーザーが利用可能なソフトウェア開発ツールキットとして製品化してきた。

本稿では，三菱セキュリティライブラリのアーキテクチャについて述べる。また，その構成要素の機能や特長について紹介する。

## 2. 三菱セキュリティライブラリのアーキテクチャ

### 2.1 セキュリティライブラリの要件

三菱セキュリティライブラリのアーキテクチャ設計に当たり，適用対象である情報セキュリティシステムを，必要とする機能に応じて，以下に示すように分類した。

(1) 暗号アルゴリズムのみを用いたシステムで，外部との相互接続を行わないもの：鍵や暗号アルゴリズムの種別・パラメータ等は独自形式で表現する。

(2) 暗号アルゴリズムのみを用いたシステムであるが，外部との相互接続を行うために鍵や暗号アルゴリズムの種別・パラメータ等を標準形式を用いて表現するシステム：例えば，鍵データやアルゴリズムパラメータをASN.1(Abstract Syntax Notation One)に従って符号化することによって機種に依存しない標準形式に変換して交換する。

(3) 暗号アルゴリズムに加えて，鍵とその所有者の結び付きを証明する手段として，証明書(Certificate)を使用するシステム：多くの場合，証明書を用いて証明する対象は公開鍵暗号アルゴリズムの公開鍵であり，証明書の形式としては国際標準規格であるITU-T勧告X.509を採用する。このシステムを構築するために用いられる鍵や公開鍵証明書(Public Key Certificate)の管理機能を含む基盤技術を，PKI(公開鍵基盤)と呼ぶ。

(4) システム内で交換するセキュアメッセージのデータ形式(署名付きデータや暗号化データ等)として国際標準規格や業界標準規格を採用するシステム：外部システムとの間でデータの交換(相互接続)が可能となる。

(5) システム内部の通信にセキュア通信プロトコルを用いるシステム：セキュア通信プロトコルとして国際標準規格や業界標準規格を採用し，外部システムとの間でも通信(相互接続)可能とする場合が多い。

このように，セキュリティライブラリに求められる機能は広範囲にわたっており，システム開発に必要となる暗号アルゴリズムやセキュリティ機能は適用対象のシステムごとに異なっている。

### 2.2 セキュリティライブラリの4階層モデル

セキュリティライブラリの実装において，前述した様々なシステム要件に対応するために，4階層モデルからなるアーキテクチャを設計した。そして，ライブラリの各機能単位を，4階層アーキテクチャの構成要素として実装した。ここでは，各層において提供すべき機能を定義する。

#### 2.2.1 第一層：暗号アルゴリズム実装

セキュリティライブラリの第一層は，暗号アルゴリズムの実装である。暗号アルゴリズムとしては，共通鍵暗号アルゴリズム(例：MISTY1, Camellia)，公開鍵暗号アルゴリズム(例：RSA)，ハッシュ関数(例：SHA-1)，乱数生成アルゴリズム等がある。暗号アルゴリズムの実装は，適用対象システムのプラットフォームや要件(処理性能や実装サイズ等)に応じて，カスタマイズが必要である。このため，汎用のソフトウェア開発ツールキットとしての製品化ではなく，適用対象システムごとに個別開発を行っている。

#### 2.2.2 第二層：暗号ツールキット

セキュリティライブラリの第二層は，暗号ツールキットである。暗号ツールキットは，データの署名生成と検証，暗号化と復号，ハッシュ値の生成等の暗号処理を行うライブラリである。鍵や暗号アルゴリズムの種別やパラメータ，署名等のデータを標準形式で取り扱う機能を含んでいる。暗号ツールキットは，複数のプラットフォームに対応して，同等の機能を同一のインタフェースで提供することを目的としている。

第二層に対応するソフトウェア開発ツールキット製品の例としては，三菱暗号ライブラリ“PowerMISTY(注) for Windows(注)”，三菱暗号ライブラリ“PowerMISTY for HP-UX(注)”がある。

#### 2.2.3 第三層：PKIツールキット，セキュアメッセージ形式・通信プロトコルの実装

セキュリティライブラリの第三層は，PKIツールキット，セキュアメッセージ形式のフォーマット機能やセキュア通信プロトコル機能の実装である。PKIツールキットは，鍵管理・証明書管理機能，証明書検証機能等のPKI機能を提供する。証明書の発行申請に用いられる業界標準規格PKCS #10(Certification Request Syntax Standard)や，鍵や証明書を交換する際に用いられる業界標準規格PKCS #12(Personal Information Exchange Syntax Standard)等の標準データ形式の作成機能を含んでいる。また，セキュアメッセージ形式のフォーマット機能は，署名データ等のセキュアメッセージで用いられている業界標準規格CMS(Cryptographic Message Syntax)，XML-Signature等のフォーマット作成機能の実装である。セキュア通信プロト

コル機能は，認証・暗号化プロトコルSSL(Secure Socket Layer)／TLS(Transport Layer Security)，証明書をディレクトリサーバから取得するためのLDAP(Lightweight Directory Access Protocol)，証明書の有効性を検証サーバに問い合わせるOCSP(Online Certificate Status Protocol)等のプロトコル実装である。

#### 2.2.4 第四層：システム開発ツールキット

セキュリティライブラリの第四層は，第一層から第三層までの構成要素を用いてアプリケーションごとに特化したインタフェースを提供するシステム開発ツールキットである。例えば，電子政府システム向けPKIライブラリ(GPKIライブラリ)，セキュア電子メール(S／MIME)システム開発用ライブラリ，モバイル・無線通信向けのセキュリティライブラリ等が該当する。適用対象システムを限定した専用の簡易インタフェースを提供する。

第四層に対応するソフトウェア開発ツールキット製品の例としては，鍵や証明書の管理機能とともに暗号メッセージの業界標準規格であるPKCS #7 (Cryptographic Message Syntax Standard)に従った署名付きメッセージや暗号化メッセージの作成機能を提供する三菱認証ライブラリ“CertMISTY[注] for Windows”がある。

## 3. 三菱セキュリティライブラリの特長

ここでは，三菱セキュリティライブラリの構成要素のうち，第二層及び第三層に対応するPKI暗号ライブラリMCryptoと，第一層に対応する組み込み機器向け暗号ライブラリMCについて，その設計方針と機能，特長について述べる。

### 3.1 PKI暗号ライブラリMCrypto

PKI暗号ライブラリMCryptoは，各種計算機システムを対象とした暗号ツールキット，PKIツールキットである。三菱セキュリティライブラリアーキテクチャにおける第二層と第三層に位置付けられ，セキュアメッセージ形式のフォーマット機能を含んでいる。MCryptoのサポートする暗号アルゴリズム，プラットフォーム等を**表1**に示す。

MCryptoは，以下に示す特長を持っている。

#### 3.1.1 暗号アルゴリズム独立

MCryptoは，暗号アルゴリズムから独立したAPI(Application Program Interface)と実際に暗号処理を行うCSP(Cryptographic Service Provider)の二階層構成となっている。CSPを交換することによって，アプリケーションプログラムを変更することなく，暗号アルゴリズムの種類や強度を変更することができる。

#### 3.1.2 鍵管理・証明書管理機能

MCryptoは，PKI対応機能として，公開鍵暗号アルゴリズムの公開鍵ペア(公開鍵と秘密鍵)を，管理媒体を用いて生成・格納・検索・削除する管理機能を提供する。鍵管理機能は，管理媒体上の秘密鍵を用いた演算(署名生成又は復号)機能を含んでいる。また，公開鍵とその使用者の結び付きを証明するITU-T勧告X.509準拠の公開鍵証明書，失効した公開鍵証明書の情報を記載した証明書失効リスト(Certificate Revocation List：CRL)を，管理媒体を用いて格納・検索・削除する管理機能を提供する。管理対象とする公開鍵証明書には，自分の証明書，他者の証明書，信頼するCA証明書がある。公開鍵ペア，公開鍵証明書，CRLを保管する管理媒体として，固定ディスク，計算機上のメモリ空間(一時的なキャッシュとして利用)，フロッピーディスク，ICカード，鍵管理装置(耐タンパーセキュアボードTURBOMISTY等)等を選択することができる。また，管理媒体の業界標準規格PKCS #11(Cryptographic Token Interface Standard)に準拠した鍵・証明書管理デバイスを利用することができる。MCryptoの鍵管理・証明書管理機能は，このような管理媒体の違いを意識せずに，同一のインタフェースで管理媒体上の鍵や証明書を取り扱うことができる(**図1**)。

#### 3.1.3 証明書検証機能

PKIでは，公開鍵証明書の有効性を検証する処理が不可欠である。証明書の検証は，基本となる国際標準ITU-T勧告X.509の規定を基として，インターネットPKI(IETF

**表1．PKI暗号ライブラリMCryptoのサポート機能**

| | |
|---|---|
| 共通鍵暗号アルゴリズム | MISTY1，DES，Triple-DES，RC2 |
| 公開鍵暗号アルゴリズム | RSA(PKCS #1 v2.0) |
| ハッシュアルゴリズム | SHA-1，MD5，MD2 |
| 署名アルゴリズム | RSA(PKCS #1 v1.5)<br>ECDSA(ANSI X9.62) |
| 鍵共有アルゴリズム | ECDH(ANSI X9.63) |
| メッセージ認証コード | HMAC-SHA1，HMAC-MD5(RFC 2104) |
| パスワードベースの暗号化アルゴリズム | PKCS #5 v2.0<br>PKCS #12 v1.0 |
| 符号化アルゴリズム | Base64(RFC 2045) |
| 証明書・CRLの形式 | X.509 certificate v3，X.509 CRL v2 |
| セキュアメッセージ形式及びデータ形式 | PKCS #1 v2.0，PKCS #7 v1.5<br>PKCS #8 v1.2，PKCS #10 v1.0<br>PKCS #12 v1.0 |
| プラットフォーム | Microsoft[注] Windows 95／98／Me／2000<br>Microsoft Windows NT[注] 3.51／4.0<br>Microsoft Windows CE 2.11<br>HP-UX，Solaris[注] |

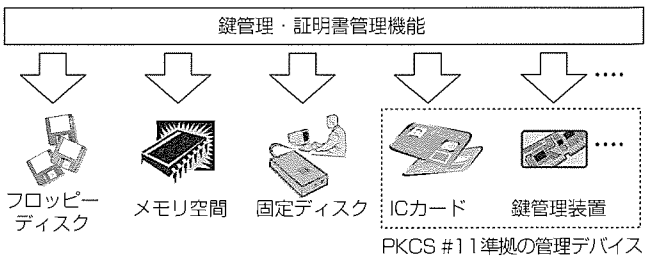



**図1．MCryptoの鍵管理機能・証明書管理機能**

PKIX WG)，金融向けPKI(ANSI X 9)，医療向けPKI(ISO TC215)等，適用分野ごとのプロフィル(サブセット)化が進められている。MCryptoの証明書検証機能は，X.509規定の標準検証処理を行う基本部と，システムごとに必要となる追加検証処理を行う拡張部で構成されており，様々なPKIプロフィルに対応した証明書の検証が可能である。また，相互認証(Cross Certification)下における，相互証明書(Cross Certificate)を含む複雑な証明書検証処理に対応している。

### 3.1.4 生体識別情報を用いた認証機能

PKIでは，利用者の秘密鍵を安全なデバイス(例えば，ICカード)に保管して署名生成や復号を行う。このとき，鍵管理デバイスの盗用による不正使用を防止するために，通常は，パスワードを用いて利用者の認証を行う。MCryptoの機能を拡張し，当社製指紋照合装置FPR-DTと組み合わせることによって，ICカード使用時の利用者認証を指紋で行う指紋認証機能を開発した。この機能をセキュア電子メール製品，三菱メッセージ暗号ソフトウェア“MistyGuard(注)＜CryptoSign(注)＞”に組み込むことによって，パスワードの代わりに指紋照合を用いて署名生成や復号を可能とするシステムを試作した。

## 3.2 組み込み機器向け暗号ライブラリMC

組み込み機器向け暗号ライブラリMCは，携帯電話や携帯情報端末等を始めとする組み込み機器において，各種暗号アルゴリズムに対応した暗号処理を行うためのライブラリである。三菱セキュリティライブラリアーキテクチャの第一層に位置付けられ，計算機システム向けの暗号ツールキット(第二層)を実装する際のモジュール部品としても使用可能である。暗号ライブラリMCのサポートする暗号アルゴリズム，プラットフォームを表2に示す。

### 3.2.1 組み込み機器向けアルゴリズムの実装要件

組み込み機器を対象とした暗号アルゴリズムの実装では，以下の要件を満たす必要がある。

(1) 省資源での動作

処理能力の低いCPUや少ないメモリ容量など，適用分野ごとに異なる，制約された環境下で動作可能であること。

(2) 可搬性

組み込み機器ごとに異なるオペレーティングシステムや開発環境下で，モジュール生成や実行が可能であること。

### 3.2.2 組み込み機器向け暗号ライブラリMCの特長

暗号ライブラリMCは，前述した実装要件を満たす暗号アルゴリズムの実装であり，以下に示す特長を持っている。

(1) 必要メモリ容量を制御・削減可能なメモリ管理方式

暗号処理に必要となるメモリ(内部で使用する作業領域，出力用バッファ領域)は，利用者が確保したメモリを使用する。ライブラリ内部において，動的なメモリ取得を行わないので，実行時の必要メモリ容量を利用者が制御できる。

表2．暗号ライブラリMCのサポート機能

| | |
|---|---|
| 共通鍵暗号アルゴリズム | MISTY1，DES，RC2，RC4互換 |
| 公開鍵暗号アルゴリズム | RSA（PKCS＃1 v2.0） |
| ハッシュアルゴリズム | SHA－1，MD5 |
| プラットフォーム | Microsoft Windows，Linux(注)<br>組み込み機器専用OS |

(2) 必要となる機能に応じたモジュールの再構成

ユーザーの要件に応じて，必要となる暗号処理機能(暗号化・復号，データの一括入力・分割入力等)のみを組み合わせて，コンパクトなモジュール構成が可能である。

(3) プラットフォームごとに最適化したアルゴリズム・コア

アルゴリズムのコアロジックには，各種プラットフォームに共通のC言語版を用意するとともに，特定のプラットフォーム(例えば，Pentium(注) II以降のインテル製CPU限定)に特化したアセンブラ言語版を個別に用意している。

## 4. むすび

暗号技術を用いた情報セキュリティシステム開発用ミドルウェアである三菱セキュリティライブラリのアーキテクチャ，その主要構成要素であるPKI暗号ライブラリMCrypto，組み込み機器用暗号ライブラリMCについて紹介した。

暗号アルゴリズム，PKI，セキュア通信プロトコル等は常に進化しており，国際標準規格や業界標準規格の改訂が常時続けられている。また最近では，携帯電話にセキュア通信プロトコルSSLやX.509公開鍵証明書が実装されるなど，計算機以外のシステムにおいてPKIを用いたセキュリティが搭載されるようになってきた。

今後は，組み込み機器向けセキュリティライブラリの第二層や第三層の需要が拡大すると考えられる。セキュリティライブラリを引き続き実装し，サポートするプラットフォームの拡大や最新標準規格への対応を行っていく予定である。

## 参考文献

(1) Tsuji, H., et al.：Cryptographic Library Architecture for Secure Application Development，電子通信学会技術報告，ISEC97-47（1997）

(2) 齋藤和美，ほか：楕円曲線暗号アルゴリズムの実装と評価(1)～(2)，情報処理学会第61回全国大会論文集，2F-3，2F-4（2000）

(3) 辻　宏郷，ほか：PKI暗号ライブラリにおけるICカードの利用(1)～(4)，情報処理学会第58回全国大会論文集，2L-04～2L-07（1999）

(4) 榊原裕之，ほか：相互認証を実現する証明証検証ソフトウェアの試作，情報処理学会第59回全国大会論文集，5T-03（1999）

(5) 太田英憲，ほか：生体識別技術のPKIへの適用と評価，情報処理学会第61回全国大会論文集，1F-6（2000）

# 耐タンパーセキュアボード“TURBOMISTY”

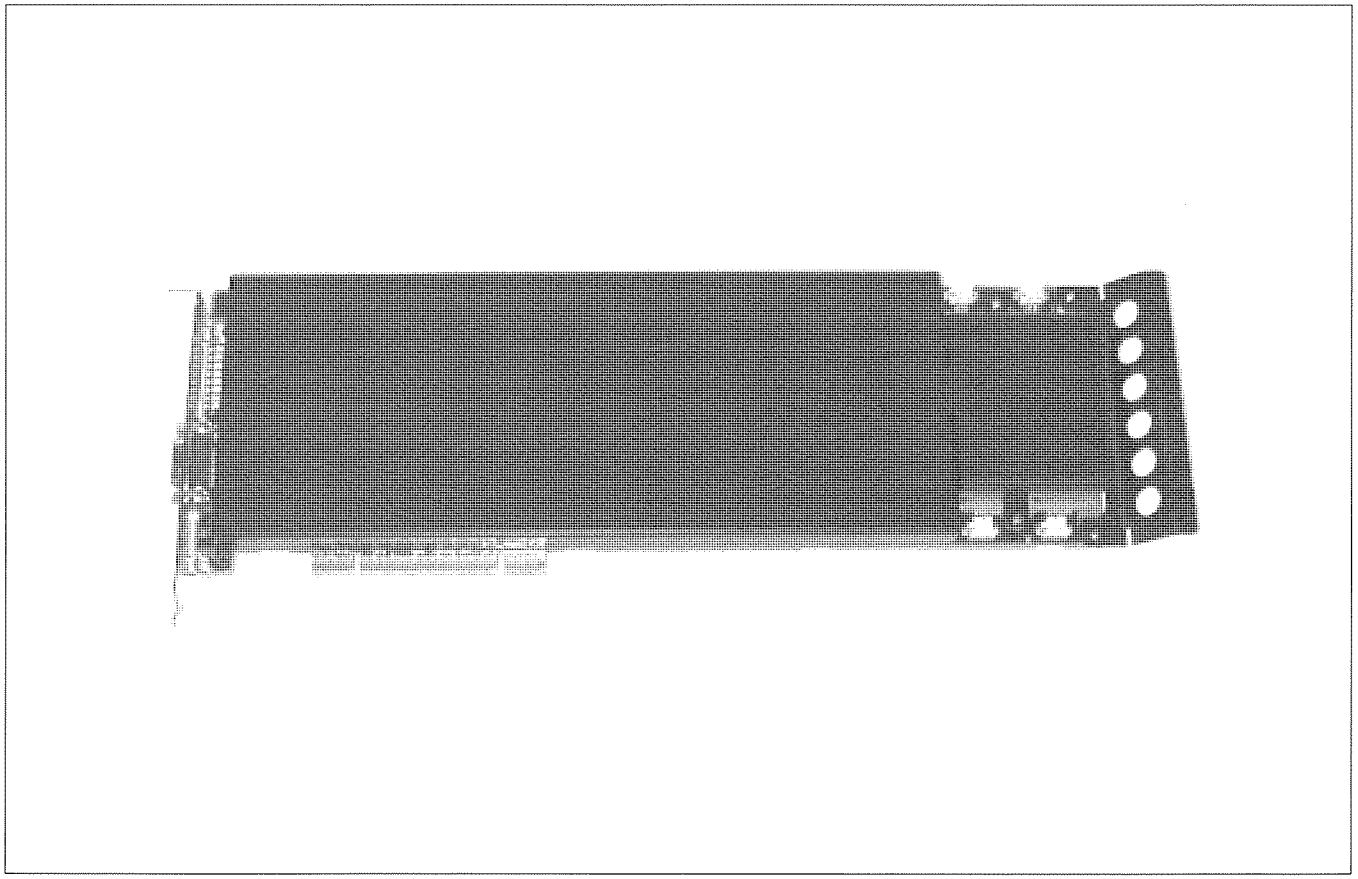
中川路哲男*
竹原　明**

**要　旨**

暗号機能の実装において，パソコンやUNIX(注)などの汎用的なアーキテクチャの計算機上でのソフトウェアによる実現では，解析される可能性が残るため，安全性に限界がある。耐タンパーセキュアボード“TURBOMISTY”は，この点を解決するための専用ハードウェアであり，暗号演算を安全にかつ高速に実行する機能を持っている。計算機内のPCI(Peripheral Component Interconnect)バススロットに装着可能なボードであり，RSAやMISTYなどの暗号処理をボード上で実行する。その特長は“耐タンパー”と呼ばれる不正アクセス防止機構であり，ボードの引き抜きや不正解体などのボード上の機密情報への不正アクセスを検知すると，自動的に機密情報を消去することによってその盗難を防止する。また，アプリケーションプログラムへ提供するインタフェースとしては，ICカード等で業界標準となっているインタフェースを採用している。

今後のセキュリティシステムの本格的実用化に向けては，認証サーバやSSL(Secure Socket Layer)サーバなどのセキュリティ確保がますます重要になってくる。これらでのセキュリティ要件をソフトウェアによる実現だけで満足することはできないため，このような専用ハードウェアの必要性が増大すると予想される。実際，米国では，政府調達基準(Federal Information Processing Standards：FIPS)において耐タンパー性のレベルを分類・規定しており，このような専用ハードウェアによる実現を調達の要件としているシステムも増えつつある。

本稿では，耐タンパーセキュアボードTURBOMISTYの機能，特長などについて述べる。



**耐タンパーセキュアボード“TURBOMISTY”**

このボードは，パソコンやUNIXサーバのPCIスロットに装着されるボードである。1台の計算機に4枚まで装着可能である。

*情報技術総合研究所(工博)　**同研究所

## 1. まえがき

セキュリティ機能の中核となる暗号演算の実装においては，演算の途中結果や演算に必要となるかぎ(鍵)情報の機密性を保つ必要がある。特に公開鍵暗号系の秘密鍵は，デジタル署名の礎となる情報であり，厳重に管理される必要がある。しかしながら，汎用的なアーキテクチャの計算機上でのソフトウェアによる実現では，メモリやディスクの解析により，これらの機密情報が漏えい(洩)する可能性がある。

本稿では，このような問題点を解決するために開発した耐タンパーセキュアボード“TURBOMISTY”の機能，特長を述べる。

## 2. 開発の目的

TURBOMISTYは秘密鍵の安全な管理を主たる目的として開発を行った。暗号モジュールの安全性の基準としては，米国政府の調達基準としてFIPS140-1[1]があり，近年これを満たす耐タンパーハードウェアを使用することを調達要件とするシステムが増えてきている。そこで，TURBOMISTYでは，FIPS140-1レベル3に適合するように設計を行った。

FIPS140-1レベル3で規定されている主な要件は以下の点である。

(1) 鍵情報や認証用パラメータなどのセキュアな情報をハードウェアによって物理的に保護すること。

(2) 装置解体などの不正なアクセスを自動検出して内部に保持している情報を消去すること。

(3) IDに基づくオペレータ認証を行うこと。

また，単に秘密鍵を管理するだけではなく，TripleDES，MISTYといった共通鍵暗号の専用LSIを搭載することにより，暗号エンジンとしての利用も可能となる暗号ボードを目的としている。

性能に関してはコストと性能とのバランスを考慮し，単一ボードで最高性能を目指すのではなく，複数枚使用することによる性能向上を可能とするように開発した。

## 3. TURBOMISTY

### 3.1 特　長

TURBOMISTYは以下の特長を持っている。

(1) FIPS140-1レベル3相当の耐タンパー機能による堅牢性を提供する。

(2) 鍵管理APIとして業界標準となっているPKCS(Public Key Cryptography Standards)#11[2]準拠のソフトウェアインタフェースを提供しており，他社のPKCS#11アプリケーションとの接続が可能である。

(3) 複数枚のボードを使用することにより，アプリケーションから意識することなく複数ボードでの負荷分散処理が可能である。

(4) PCIボードとして実装することにより，同一のボードでパソコンやワークステーションでの使用が可能になっており，他のプラットフォームへ比較的容易に移行することができる。

(5) ファームウェアのアップデートにより，だ(楕)円曲線暗号などのアルゴリズムを後から追加することが可能である。

### 3.2 機　能

(1) 耐タンパー機能

以下の不正なアクセスを自動検出し，内部に保持している機密情報をすべて自動的に消去する。

- 本体計算機からのボードの抜き取り
- ボード上のカバーの取り外しや破壊

(2) 公開鍵暗号演算

公開鍵暗号方式としてはRSAを採用し，また演算に関しては以下の機能によって秘密鍵を完全にボード内部に隠ぺい(蔽)し，外部への漏洩を防止する。

- 公開鍵対生成
- 秘密鍵／公開鍵の保管
- 秘密鍵／公開鍵演算
- 秘密鍵バックアップ

秘密鍵バックアップの詳細については**3.5節**で述べる。

(3) 共通鍵暗号演算

DES，TripleDES，MISTYによる暗号化／復号演算機能を提供する。

(4) ハードウェア乱数生成

ハードウェアベースの乱数生成機構により，ソフトウェアによる疑似乱数よりも純度の高い乱数を得ることが可能である。

(5) 証明書格納

X.509に基づく証明書を格納／取り出して使用することが可能である。

(6) メッセージダイジェスト生成

MD5，SHA1によるメッセージダイジェスト生成機能を提供する。

(7) SSLサーバ接続

インターネットにおけるブラウザとWebサーバ間のセキュア通信プロトコルとして広く普及しているSSLにおいては，SSLサーバの秘密鍵管理が重要である。現状のほとんどのSSLサーバは秘密鍵をディスク上のデータとして管理しているが，**図1**に示すように，TURBOMISTYとSSLサーバとを組み合わせることで，SSLコネクション確立時に使用するSSLサーバの秘密鍵を安全に管理することが可能である。

また，暗号関連処理をTURBOMISTYで行うことによ

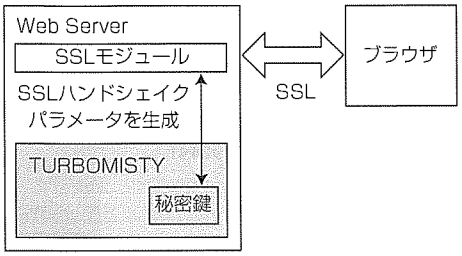



図1．SSLサーバとの接続

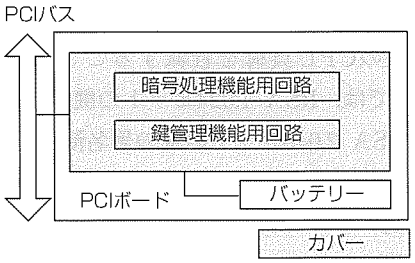



図2．ハードウェア構成

り，本体CPUの負荷を軽減することも可能になる。

(8) 負荷分散処理

詳細は**3.4節**で述べる

(9) アルゴリズム追加

TURBOMISTYのファームウェアをアップデートすることで新たなアルゴリズムを追加することが可能である。

### 3.3 ハードウェア構成

TURBOMISTYは**図2**に示すようなPCIボードとして実装されている。基板上の回路から鍵情報や演算過程のデータを読み取られることを防止するため，単面実装とし，実装面をカバーで覆う構造としている。

カバー外部にはホストが停止中に内部の鍵を保持するためのバッテリーを備えており，それ以外の暗号処理や鍵の管理実行する構成要素はすべてカバー内部に実装されている。

### 3.4 ソフトウェア仕様

ソフトウェアインタフェースは，暗号モジュールのインタフェースとして業界標準となっているPKCS#11を提供している。

PKCS#11はマルチスロット対応のAPIであり通常は1デバイスを1スロットとして扱うが，TURBOMISTYでは，1ボードを論理的に8スロットとして扱うことにより，例えば1ボードで複数のCAの秘密鍵を管理することが可能となっている。また，最大4ボードを搭載することが可能であり，最大32スロットまで使用可能である。論理スロットとボードとの対応はPKCS#11ライブラリ内部で管理しており，アプリケーションからは単に複数のTURBOMISTYが装着されているように扱うことができる。

また，設定により，**図3**のようにPKCS#11ライブラリ内部で装着されている複数ボードの排他制御を行い，マルチスレッド／マルチプロセス環境で処理を複数ボードに分散させて実行することが可能になっている。

この場合，アプリケーション側からは1スロットとして認識されるため，処理させるボードをアプリケーション側で意識する必要はなく，アプリケーションを修正することなく複数ボードでの負荷分散処理が可能になっている。

### 3.5 秘密鍵のバックアップ

TURBOMISTYでは，耐タンパー機構により，不正なアクセス検出時には自動的に内部に保持している秘密鍵を消去することによって鍵の漏洩を防止する。したがって，運用に当たっては，不正アクセスによって鍵が消去された場合やボードの故障などに備えて秘密鍵をバックアップしておく必要がある。

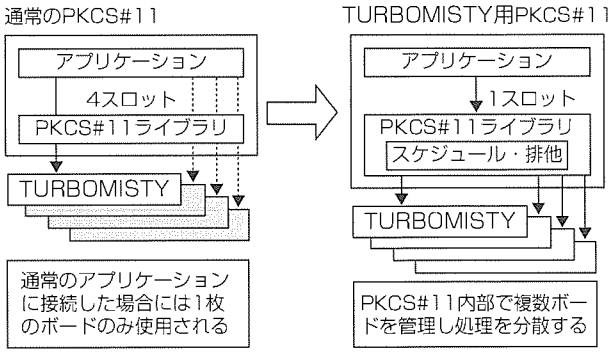



図3．PKCS#11ライブラリによる分散処理

バックアップデータはTURBOMISTYの外部に保管しておくことになるが，TURBOMISTY外部でバックアップデータから元の秘密鍵が復元されてしまうとTURBOMISTYで管理している効果がなくなるため，安全な方式でバックアップする必要がある。

このため，TUROBMISTYでは，秘密鍵をバックアップする際，内部でMISTYによって秘密鍵を暗号化した上，シークレットシェアによって断片に分割し，複数人で分散管理することで安全性を高めている。

バックアップした秘密鍵をTURBOMISTYにリストアするためには，バックアップ時に指定した数のバックアップ断片をそろえる必要があり，単独でのリストアを防止している。

バックアップ断片はフロッピーディスク又はICカードに保管し管理する。バックアップ断片は暗号化されているため，内容が漏れても安全上問題ないが，ICカードに保管することによってコピーを防止でき，より安全に管理することができる。

### 3.6 性　能

セキュアボードによる利点は，安全性だけでなく，性能面にも存在する。暗号処理，特に公開鍵系暗号における秘密鍵処理は，多倍長演算によってCPU資源を大量に消費

する。セキュアボード内で暗号処理を実行することにより，本体計算機のCPU負荷を軽減することになる。TURBOMISTYでは，RSA 1,024ビットの鍵の署名演算を5～6個/秒，RSA 2,048ビットの鍵の署名演算を1個/秒程度の性能で実行可能である(Windows NT(注) 4.0，Pentium(注) Ⅲ(500MHz)のパソコンに装着し，PKCS#11のレイヤで評価した場合)。

また，署名生成を複数ボードによって負荷分散した場合には，ほぼボード数に比例して性能が向上しており，負荷分散処理の効果が十分得られている。

### 3.7 TURBOMISTYの運用管理

TURBOMISTYの運用管理は，図4に示すホスト上の管理ツールから実行することができる。管理ツールの主な機能は次のとおりである。

- ボードの状態表示
- ボードの初期化／PINなどのパラメータの設定
- 鍵／証明書の一覧表示
- 秘密鍵のバックアップ／リストア

### 3.8 仕　様

TURBOMISTYの主な仕様を表1に示す。

## 4. 相互接続性

現状では，TURBOMISTYと以下の製品との接続・相互動作が確認されている。

(1) Entegrity AssureTransaction[3]

AssureTransactionは，金融系認証基盤Identrusのコンポーネントの一つとして認定されているEntegrity社のDSMS(Digital Signature Messaging System)である。

TURBOMISTYは，AssureTransactionとの接続性が認められ，Chrysalis社やnCipher社などの海外ベンダーの製品とともにEntegrity社の認定HSM(Hardware Security Module)として認定されている。

(2) Netscape iPlanet Web Server

iPlanet Web Server(以下"iWS"という。)はSSLで使用する内部暗号モジュールのAPIがPKCS#11で提供されており，外部暗号モジュールと切り換えて使用することができる。iWSにTURBOMISTYのPKCS#11ライブラリを登録することにより，iWSの秘密鍵をTURBOMISTYで管理することができる。

## 5. むすび

PKI(Public Key Infrastructure)の進展に従って電子商取引などが広く普及するのに伴い，システムの安全性の核となる鍵管理の重要性が今後ますます高まると予想される。今後，更なる高機能・高性能化を図るとともに，TURBOMISTYが様々なセキュリティシステムで使用されていくことを期待する。


図4．管理ツール画面

表1．TURBOMISTYの仕様

| | |
|---|---|
| PCIバス | PCI 2.1規格準拠，33MHz同期式<br>32ビットバス |
| サイズ | PCIフルサイズ<br>(W)106.7×(D)312(mm) |
| FIPS140-1への対応 | レベル3相当 |
| インタフェース | PKCS#11 ver2.01 |
| ボード1枚のスロット数 | 8 |
| 最大ボード数(スロット数) | 4 (32) |
| ボード1枚の格納秘密鍵数 | 32 |
| ボード1枚の格納証明書数 | 64 |
| アルゴリズム | RSA(512-2048)，<br>MISTY，DES，TripleDES<br>MD5，SHA-1 |
| 乱数生成 | H／W乱数 |
| 対応OS | Windows NT／2000<br>Solaris7<br>HP-UX11.0(対応予定) |

## 参考文献

(1) FIPS140-1
http://csrc.nist.gov/publications/fips/fips1401.htm

(2) PKCS#11 Cryptographic Token Interface Standard
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/

(3) Entegrity AssureTransaction
http://www2.entegrity.com/products/trust_identrus.shtml

# PKI構築技術

坂上　勉*
佐伯正夫*

**要　旨**

三菱電機PKI(Public Key Infrastructure：公開かぎ(鍵)基盤)システムは，多様なPKIアプリケーション構築のための基盤とするために，基本構成要素層，認証構成要素層，セキュアプロトコル層，及びシステム構成部品層からなるレイヤ アーキテクチャを採用している。また，本格的実用とPKIアプリケーションの効率的な運用・保守のために重要な種々のPKI構築技術の研究開発を進めている。ここでは，特に中核的な認証構成要素層に関して，重要性が高く最近注目されている次のPKI構築技術について，開発成果や効果などを紹介する。

(1)　CAシステム構成技術(IA／RA分散)

IA(Issuing Authority：発行局)とRA(Registration Authority：登録局)を分散させるなど，CA(Certification Authority：認証局)システムを必要に応じて構成可能とする。CAの運用効率が向上する。

(2)　ICカードプリンタ利用技術

ICカードへの証明書発行を表面印刷しながら複数枚一括処理可能とする。証明書発行の運用効率と信頼性が向上する。

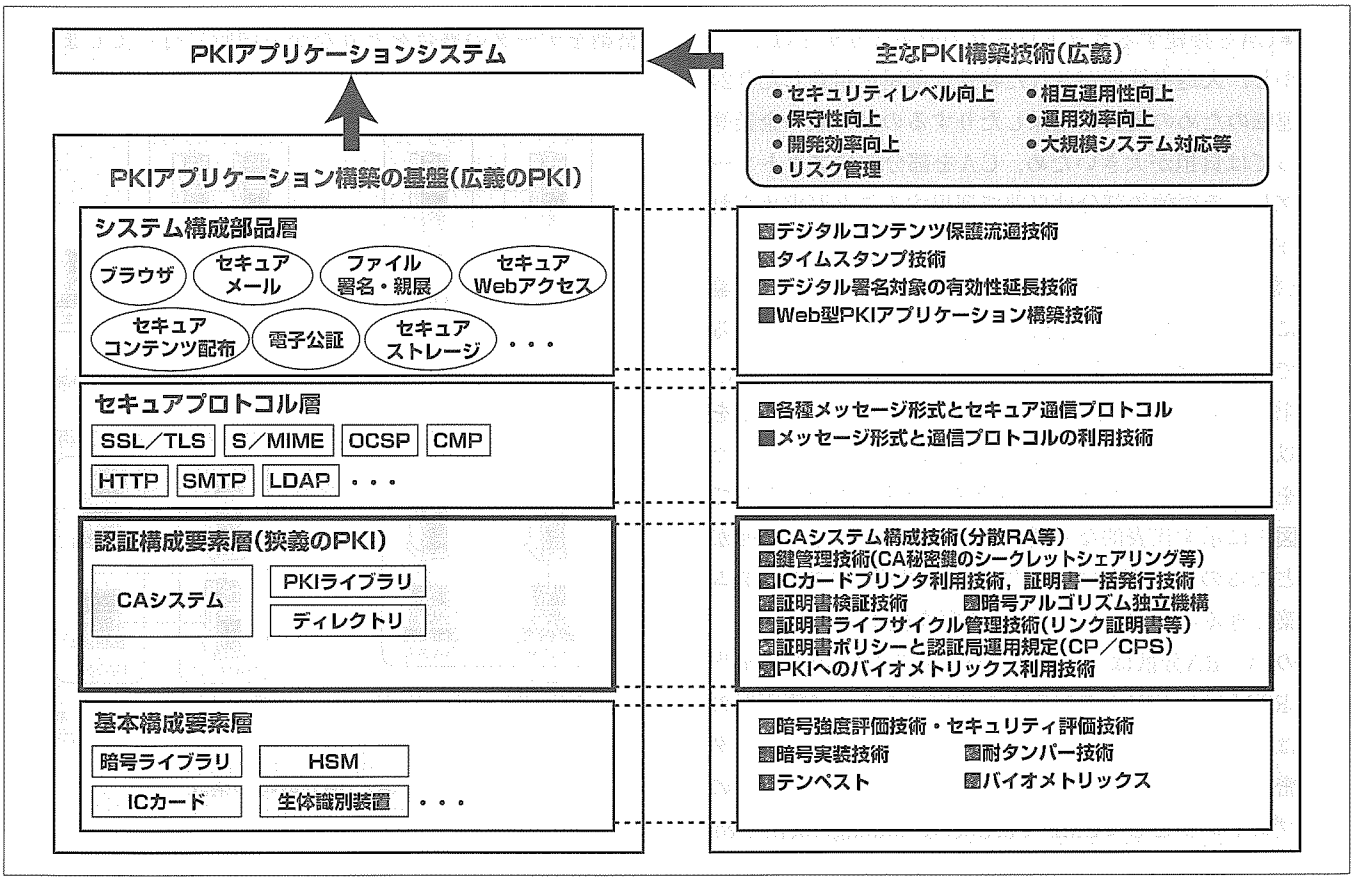
(3)　リンク証明書

世代の異なるCAから証明書を発行された利用者間での証明書検証を可能とする。利用者側の運用効率が向上する。

(4)　暗号アルゴリズム独立機構

PKIアプリケーションが用いる暗号アルゴリズムを容易に切換え可能とする。保守性が向上し，リスク管理にも有用である。

最後に，三菱電機PKIシステムの特長を簡単に紹介する。




**PKI構成要素と構築技術**

三菱電機PKIシステムは，多様なPKIアプリケーションの構築基盤とするために，基本構成要素層，認証構成要素層，セキュアプロトコル層，及びシステム構成部品層からなっている。本格的な実用に供するPKIアプリケーションを効率良く開発・運用し将来にわたって維持／改良していくために，この各層に対応した種々のPKI構築技術が重要となる。

*情報技術総合研究所

## 1. まえがき

PKIシステムは，1995年ごろから民間や公的機関のプロジェクトとして様々な実験システムが構築されてきたが，近年，中央省庁の電子政府システムなどでようやく実用システムとして利用され始め，正に情報セキュリティの“鍵”を握るシステムとして注目されている。

一口にPKIシステムと言っても一般には幾つかの要素によって構成されており，PKIシステムの利用目的／利用方法／他のシステムとの連携方法などによって，いかようにも変化するものである。

本稿では，PKIシステムを実運用するためのPKI構築技術の中でも特に最近注目されている技術について紹介するとともに，三菱電機製品での開発成果や効果について紹介する。

## 2. CAシステム構成技術（IA／RA分散）

CAが証明書に署名するために使用する鍵が漏れてしまうとPKIシステム全体が崩壊してしまうため，実運用するためのPKIシステムを構築する場合，以下のような点について考慮する必要がある。

- CAを設置する部屋の入退室管理はどうするか？
- CAは24時間運転する必要があるか？
- CAを接続するネットワークのセキュリティは？

しかし，入退室管理がされた特殊な部屋を用意したり24時間運転のための要員を確保したりするのは一般の企業等にとっては負担が大きいため，CAを部分的にアウトソーシングし，その他の部分は自前で運用することが求められるようになってきている。

CAを部分的にアウトソーシングするためには，CAを論理的に幾つかの“要素”に分解して考えることが必要になる。そこで当社では，CAをIAサーバ，IA端末，RAサーバ，RA端末の四つの要素に分解して考え，この四つの要素を二つ以上の場所に物理的に分散して配置できるようにした。これをIA／RA分散と呼ぶ。IAとRAの配置の形態としては，**図1**に示す代表的な4種類を始めいろいろな組合せが可能となるので，運用ニーズに応じた最適なCAシステムを構築できる。なお，IAとRAの役割を**表1**に示す。

このIA／RA分散は，認証サーバシステムMistyGuard(注)<CERTMANAGER>D00版から利用できる。各要素間の通信はSSL(Secure Sockets Layer)を使用して通信データの機密を守り，IAサーバ-RAサーバ間の通信にはSSLの上位プロトコルとしてCMP(Certificate Management Protocol)を採用している。

## 3. ICカードプリンタ利用技術

利用者の秘密鍵／証明書を保管する媒体としては幾つかの候補があるが，対タンパ性／経済性／利便性を兼ね備えた媒体として利用されているのがICカードである。

現在利用可能なICカードには様々な種類があるが，PKIで利用するICカードは，利用者の秘密鍵／証明書を保管するメモリに加えて，ICカード内で秘密鍵演算を行うためのプロセッサを備えたものである。このようなICカードでは，演算のために秘密鍵をICカードの外に取り出す必要がないので，デジタル署名を出先で行うような場合でも，安心して利用することができる。

このように便利なICカードであるが，大量のICカードに秘密鍵／証明書を格納する実用システムを構築する際には，以下の点に注意を払う必要がある。

(1) ICカードの表面には利用者の名前や所属を印刷したりエンボスしたりする必要がある。

(2) ICカード表面に印刷される利用者の名前等とICカード内に格納される秘密鍵／証明書が合っている必要がある。

(3) ICカード内に秘密鍵／証明書を格納する際には格納するデータの機密が保たれる必要がある。

上記の(2)を満足させるためには，何らかの方法で格納する秘密鍵／証明書とICカード表面の印刷データとの対応をとる必要があるが，大量にICカードを発行することを考えるとこれを人手で行うことには限界がある。そのため，印刷／エンボスとICカード内への秘密鍵／証明書の格納をデータの整合をとりながら同時に行ってしまうIC

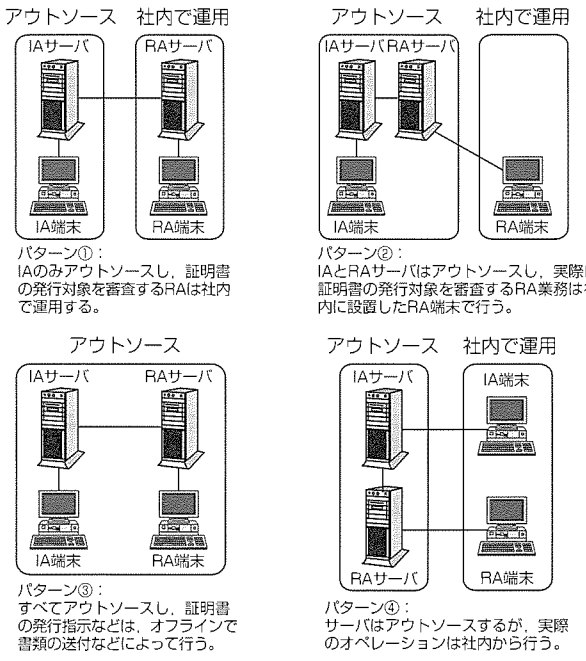



**図1．IA／RA分散時の構成**

**表1．IAとRAの役割**

| | 役　割 |
|---|---|
| IA | 発行する証明書にデジタル署名をするための公開鍵対を管理し，RAからの指示に基づいて証明書を生成する。 |
| RA | 証明書の発行対象からの要求を審査し，審査結果によってIAに対して証明書の生成を指示する。 |

カード印刷発行機が利用されるようになってきた。

当社では，認証サーバシステムMistyGuard＜CERT-MANAGER＞と大日本印刷㈱製のICカード印刷発行機CX710を連携させることによってICカードへの秘密鍵／証明書の格納と表面印刷を同時処理可能とするとともに，数百枚を一括処理可能として，運用効率と信頼性を向上させている。

## 4. リンク証明書

証明書には有効期限があり，CAの証明書といえどもいずれ有効期限が切れるときがくる。そうなると，そのCAが過去に発行した証明書は，有効期限が切れていなくても使用できなくなる。このような問題を避けるため，CAの証明書は有効期限いっぱいまで署名に利用するのでなく，有効期限前に更新する。**図2**にその様子を示す。

ここではCAの証明書の有効期間は5年あるが，署名には3年しか使用しないこととしている。利用者の証明書の有効期間は2年なので，CAの証明書は有効期間を2年残した状態で更新すれば，CAの証明書が期限切れになっても発行済みの証明書が使用できなくなるということが起きない。

このような運用をしている場合，図の網掛けの期間は，1代目のCAの秘密鍵／証明書で署名された利用者1の2代目の証明書と，2代目のCAの秘密鍵／証明書で署名された利用者2の1代目の証明書が同時に有効となっている。利用者1と利用者2の信頼点証明書はそれぞれCAの1代目の証明書と2代目の証明書であるため，例えば利用者1が利用者2の証明書を検証しようとしても署名の検証ができないことになる。この問題を解決する方法として以下の二つが考えられる。

(1) CAの秘密鍵／証明書を更新したら，新しいCAの証明書をアプリケーションに信頼点として取り込ませる。

(2) リンク証明書を使用する。

従来は(1)の方法が一般的であったが，GPKIシステムやIdentrusシステムなどで(2)のリンク証明書が利用されるようになってきており，当社も対応している。

リンク証明書を使用する場合には，CAの秘密鍵／証明書を更新した際に，$n$代目の公開鍵を入れて$n+1$代目の秘密鍵／証明書で署名をした証明書(OldWithNew)と，$n+1$代目の公開鍵を入れて$n$代目の秘密鍵／証明書で署名をした証明書（NewWithOld)の二つのリンク証明書を作成しておく。証明書の検証を行うには，例えば，**図3**のように利用者1の証明書を利用者2が検証する場合，利用者2の信頼点である$n+1$代目のCAの証明書からリンク証明書を使って利用者1の証明書を検証すればよい。リンク証明書を導入することによって，CAの証明書が更新されても利用者側は今までどおり運用を続けられることから，運用効率が向上する。

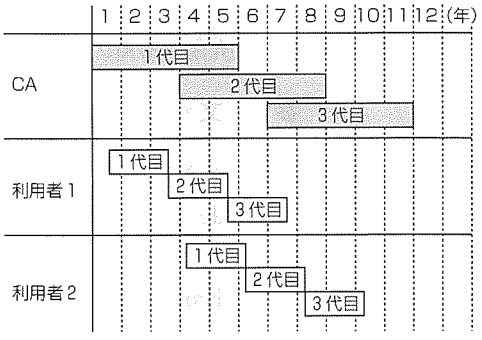



**図2．証明書の有効期限と更新**

## 5. 暗号アルゴリズム独立機構

暗号技術及び暗号解読技術の進歩に伴って，現在安全と評価されている暗号であっても将来にわたって安全とは限らない。将来の危たい(殆)化の高まりに備えて代替の暗号アルゴリズムに容易に切り換えられるように，また今後のより良い暗号を容易に採用できるようにしたい。このようなニーズにこたえるため，パラメータの変更や一部のモジュールの入換えによって，利用する暗号アルゴリズムを容易に切り換えられる機構(暗号アルゴリズム独立機構)を開発している。認証サーバシステムMistyGuard<CERT-MANAGER>や，認証ライブラリCertMISTY(注)などの当社製品には，基本的に同様な機構を実装した。なお，このような機構は攻撃対象となりやすい場合もあるため，主に次のことに注意を払う必要がある。

- 切換え設定の正当性検証(切換え設定情報の改ざん防止)
- 切換え方法の選択(インストーラ又はプログラムで切換え設定を固定化するか，利用者が切換え可能とするか)
- 入換えモジュールのアクセス制御／改ざん防止

## 6. 三菱電機PKIシステムの特長

最後に，三菱電機PKIシステムの特長を，次の3点に集約して簡単に紹介する。

- ハイレベルセキュリティ
- 豊富なセキュアコンポーネントとPKIソリューション

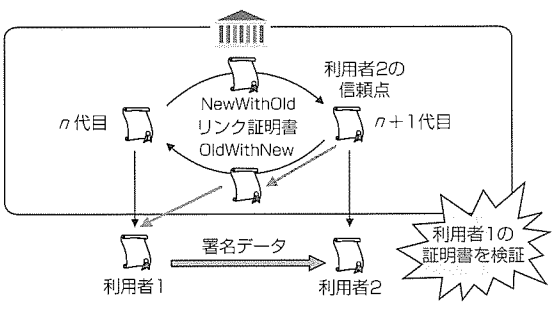



**図3．リンク証明書を使った証明書検証**

●高度な相互運用性と運用効率

### 6.1 ハイレベルセキュリティ

(1) 高度な暗号アルゴリズム

親展／秘匿通信に用いる共通鍵暗号アルゴリズムとして，MISTYを始めとする複数のアルゴリズムを使用できる。MISTYは，差分解読法／線形解読法による客観的評価尺度によって暗号強度が数値化され強いことが保証されている。MISTYの技術は，KASUMIとして，次世代携帯電話の世界標準に採用された。

(2) 耐タンパーセキュアボード

HSM(Hardware Security Module)として，FIPS 140レベル3相当の耐タンパー性が高い自製の耐タンパーセキュアボードMISTYKEYPER等を業界標準インタフェースで利用できる。セキュリティの根幹であるCAの秘密鍵やアプリケーションサーバの秘密鍵を厳重に保護可能で，また，秘密鍵のバックアップについては，シークレットシェアリング方式による複数人管理が可能であるとともに，シークレットシェアのICカードへのバックアップも可能である。

(3) ICカード

利用者の大切な秘密鍵を公開鍵暗号演算可能なICカードに安全保管した状態で，かつ業界標準インタフェースで使用できる。

(4) CAサーバによるキーアーカイブ

認証サーバシステムMistyGuard<CERTMANAGER>は利用者の秘密鍵を安全保管するキーアーカイブ機能と再発行機能を備えており，不測の事態に対する回復が可能である。

(5) 暗号アルゴリズム独立機構

PKIアプリケーションが用いる暗号アルゴリズムを容易に切り換えることができる。暗号の危殆化に備えるため，また今後のより良い暗号に切り換えるためにも有用である。

### 6.2 豊富なセキュアコンポーネントとPKIソリューション

(1) セキュアコンポーネントによる効率的なシステム構築

セキュアメール，セキュアWebアクセス，コンテンツ配布(デジタルコンテンツ保護流通)，セキュアストレージ，不正アクセス防止基盤，PDF電子署名システムなどシステム構成部品としてそのまま利用可能な製品群を装備しているので，短期間に効率的にPKIアプリケーションシステムを構築できる。

(2) 業務に最適な専用システム構築

汎用性と自由度の高い認証ライブラリCertMISTYを用いて，業務に最適な任意のPKIアプリケーションプログラムを自在に開発することができる。

(3) EC・セキュリティソリューションの提供

設備・要員・運用管理を含めたトータルなセキュリティシステムを構築し運用するための，CP(Certificate Policy：証明書ポリシー)及びCPS(Certification Practice Statement：認証局運用規定)の策定サービスを提供している。また，社会，産業，生活等の分野別各種ソリューション及びセキュリティコンサルティングサービスを提供している。

### 6.3 高度な相互運用性と運用効率

(1) 相互運用性を高める種々の機能

相互認証機能，豊富な証明書拡張子，業界標準プロトコル(SSL, LDAP, OCSP, CMP等)，暗号アルゴリズム独立機構などを備えており，他の認証ドメインと信頼関係を結ぶことができる。また，他社製品と組み合わせてシステム構築することもできる。

(2) 多様なポリシーにこたえる多彩な証明書発行形態

オフラインで証明書申請・発行ができるほか，セキュア電子メール用のS／MIME証明書，ブラウザ用のSSL証明書をオンラインで申請・発行できる。また，証明書申請・取得の操作は一般利用者にとって簡単でないという運用上の問題があるが，代行申請機能によって，利用者はICカード又はFDに格納された秘密鍵と証明書を受け取るだけという運用を実現できる。さらに，秘密鍵及び証明書の保管媒体は，必要に応じてICカード，FD，HD又はHSMを選択できる。

(3) 多様なポリシーにこたえる自由度の高いCAシステム構成

多階層CA構成，CA間の相互認証，分散RA構成，同一マシンへの複数CA搭載，同一CAによる複数種類の証明書発行，証明書検証サーバ，日本語対応証明書，リンク証明書などを必要に応じて自由に選択できるとともに，豊富なカスタマイズ機能を備えているので，証明書ポリシーに適合した最適なCAシステムを構築することができる。

(4) 証明書の一括処理

証明書の申請から発行までの一連の処理を，一括して大量処理することができる。また，複数の証明書を一括して失効させることができる。さらに，ICカードプリンタを利用して複数枚のICカードへの証明書発行と表面印刷を一括処理することができるので，正確で効率的な運用が可能である。

## 7. むすび

PKIアプリケーションへの適用実績をフィードバックしながら，今後とも構築・運用・保守をより容易にするためのPKI構築技術を磨いていく所存である。

## 参考文献

(1) RFC2459：Internet X.509 Public Key Infrastructure Certificate and CRL Profile

(2) RFC2510：Internet X.509 Public Key Infrastructure Certificate Management Protocols

(3) RFC2511：Internet X.509 Certificate Request Message Format

# 電子文書に対する署名技術

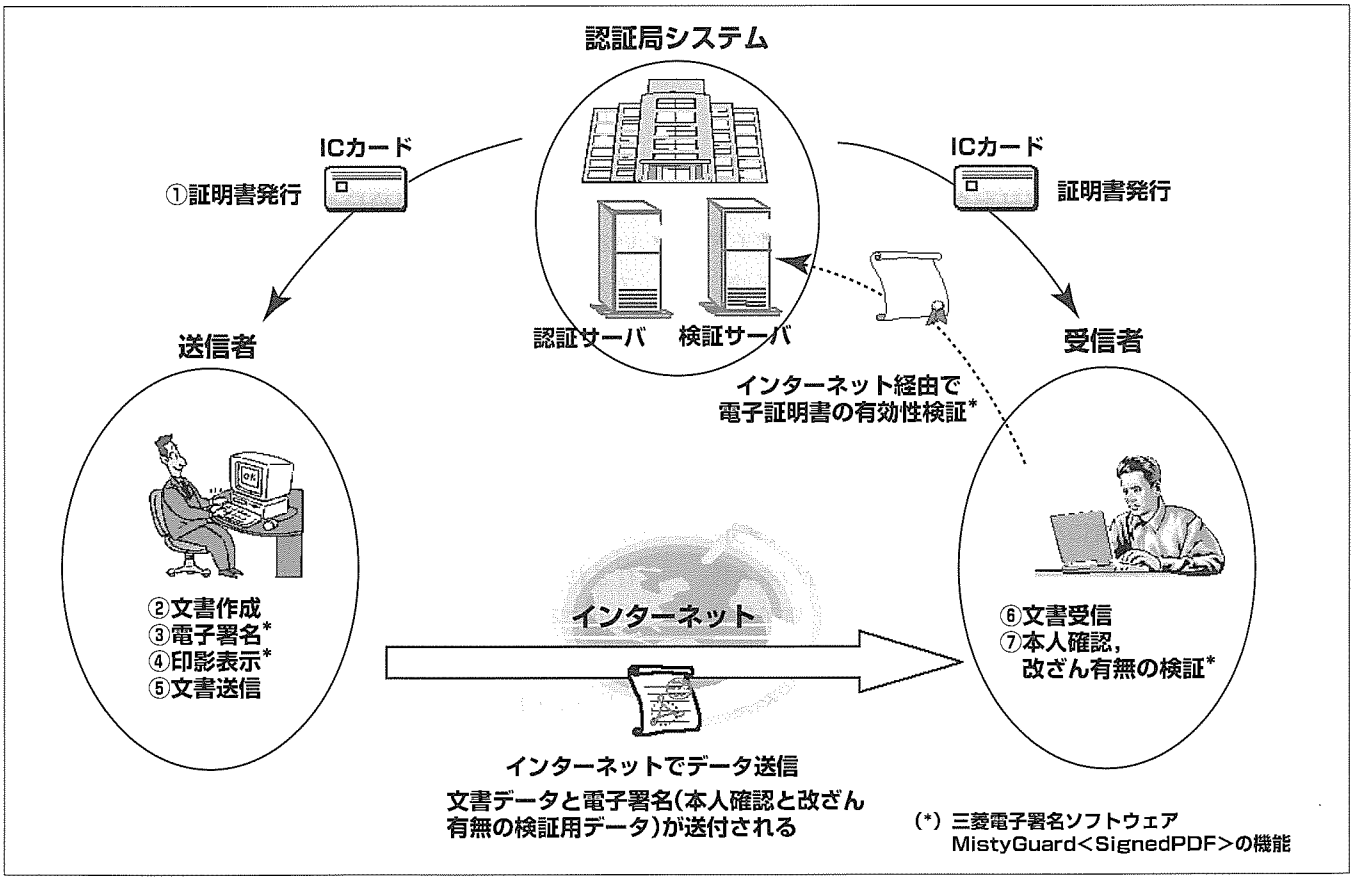
鈴木　博*　清水可奈子**
大澤　尚**　佐伯正夫*
植村　穣**

**要　旨**

2001年4月に施行された電子署名法(「電署名及び認証業務に関する法律」)，2003年度における電子政府の実現などPKI(Public Key Infrastructure)の整備が本格化している中，従来紙で取り交わされていた各種申請書類や企業内／企業間における承認／決裁文書の電子化が急速に進んでいる。また，インターネット上における文書交換においても，電子メールを使用した電子文書の送受信やWWW(World Wide Web)サーバのホームページからの電子文書のダウンロードなどが一般的になりつつある。しかし，文書の電子化に当たっては，文書作成者の本人確認，文書の改ざん検出などセキュリティ上の問題を解決する必要があり，電子文書に対する署名技術が不可欠なものとなる。

多種多様な電子文書形式のうちインターネット上での文書交換に広く使われているAdobe(注) PDF(Portable Document Format)ファイルやXML(Extended Markup Language)ファイルへの署名技術，さらには新署名データ形式であるCMS(Cryptographic Message Syntax)等の研究開発を行っているが，本稿では，PDFファイルを対象とした電子署名製品"三菱電子署名ソフトウェアMistyGuard(注)<SignedPDF(注)>"の署名技術を中心に解説する。

SignedPDFは，ICカードを使用してPDFファイルに対して電子署名を行い，さらに電子署名を視覚的に表すため電子署名に対応した印影イメージを表示させることを特長とした製品である。各種申請業務や社内ワークフロー等，これまで押印が必要なために文書の電子化が進まなかった業務に適用することができ，ペーパーレス化や文書送付のスピードアップ化によるコストダウンを実現可能とする。




**SignedPDFシステムの構成例**

SignedPDFは，ICカードを使用してPDFファイルに電子署名を行い，さらに電子署名に対応した印影イメージを表示させることを特長とした製品である。各種申請業務や社内ワークフロー等，これまで押印が必要なために文書の電子化が進まなかった業務に適用することができ，ペーパーレス化や文書送付のスピードアップ化によるコストダウンを実現可能とする。

*三菱電機㈱情報技術総合研究所　**三菱電機インフォメーションシステムズ㈱

## 1. まえがき

IT(Information Technology)の普及により，企業や官公庁などが扱う文書の電子化が急速に進んでいる。また，インターネット上における文書交換においても，電子メールを使用した電子文書の送受信やWWWサーバのホームページからの電子文書のダウンロードなどが一般的になりつつある。企業や官公庁においては扱うすべての文書を電子化したいとのニーズが高まっており，特に公的な届出や取引など署名・押印が必要とされる文書の電子化要求に対する法的基盤を整備するために，2001年4月に電子署名法が施行された。さらには，2003年度における電子政府実現に向けて，PKIの整備が本格化している。しかし，文書の電子化に当たっては，文書作成者の本人確認，文書の改ざん検出，及び電子文書へのなつ(捺)印表示などが課題となっていた。これらの課題を解決するために，電子文書交換に広く利用されているAdobePDFファイル(以下"PDFファイル"という。)に電子署名を施し，さらに電子署名を印影(印鑑)イメージで表示する製品"三菱電子署名ソフトウェアMistyGuard<SignedPDF>"(ミスティガード サインドピーディーエフ：以下"SignedPDF"という。)を開発した。

本稿では，SignedPDFを実現しているセキュリティ技術，及びSignedPDFの適用事例を中心に述べる。

## 2. SignedPDFの特長

SignedPDFは，Adobe(注) Acrobat(注)及びAdobe Acrobat Approvalのプラグインソフトウェアとして開発した。Adobe Acrobat及びAdobe Acrobat Approvalには電子署名機能は存在するが，電子署名を施すための暗号かぎ(鍵)(公開鍵暗号方式における秘密鍵)や署名者の電子証明書がパソコンのハードディスク内に格納されている。SignedPDFでは，個人認証媒体としてICカードを採用することでセキュリティレベルを更に向上させた。

以下，この製品の特長について概説する。

### 2.1 電子署名を利用者になじみの深い印影イメージで表示

文書に電子署名を施すことによって文書作成者の本人確認及び文書の改ざん検出を行うことができるが，電子署名は，通常人間の目には見えない電子データとして文書に付加されている。したがって，文書の送信者(作成者)や受信者は電子署名が施されていることを視覚的に確認することができない。実社会で我々が公的文書などに押印して，それが視覚的に確認できることと比べると，利用者にとっては大きな違いがあった。

SignedPDFでは，電子署名が施されたことを文書作成者の印影イメージで表示することで，より現実社会での運用に近づけている。さらに，印影イメージをクリックすることで署名検証を行うことができ，文書作成者の特定や文書改ざんの有無を視覚的に一目で確認することが可能となる。

これにより，これまで押印が必要であるため文書の電子化が進まなかった行政機関への届出や申請，企業間商取引，企業内のワークフローシステムなどへの適用が可能となり，ペーパーレス化や文書送付のスピードアップ化によってシステム運用時のコストダウンを実現している。

さらに，電子署名が施された文書を保管することによって原本性の確認を任意のタイミングで行うことができ，文書の監査にも対応することが可能となる。

### 2.2 個人認証媒体としてICカードを利用

SignedPDFでは，個人を認証する媒体としてICカードを利用している。ICカードはカード内の情報の改変やカードそのものの偽造が困難なため，第三者による成り済ましを防止することができる。さらに，ICカード内のデータにアクセスするにはパスワードが必要であるため，盗難や紛失時にも不正利用される可能性は非常に低く，セキュリティレベルはかなり高いものとなる。

ICカード内には，ICカード所有者本人の秘密鍵，電子証明書，印影などが格納されており，これらを使用することで電子署名の生成及び電子署名の検証が実施される(3章参照)。

### 2.3 認証局システムとの連携

SignedPDFで利用するICカードには電子署名生成や署名検証の際に使用される本人の秘密鍵や電子証明書が格納されており，これらは，認証局システムによって発行される。また，署名検証の際には，検証に使用した電子証明書の有効性を確認するために，認証局システムで運用されている証明書検証サーバと連携することができる。認証局システムは，SignedPDFの機能ではないが，認証局システムにおける以下のサービスを当社が提供しており，SignedPDFがそのサービスと連携することでさらに使いやすいシステムの構築を可能としている。

(1) 認証局サービス

SignedPDFの利用者であるお客様の認証局を構築するサービスである。これにより，お客様自身の認証局から発行された電子証明書をICカードに格納し，SignedPDFを利用することが可能となる。

(2) 認証局ハウジングサービス

SignedPDFの利用者であるお客様の認証局の運用を代行するサービスである。認証サーバ設備はお客様所有のものであるが，その設置場所及び運用を代行する。これにより，お客様による認証局運用の負荷を軽減させることができる。

(3) 認証局ホスティングサービス

SignedPDFの利用者であるお客様に対し，認証局機能をインターネット経由で提供するサービスである。これにより，お客様自身が認証局を用意する必要がなくなり，特に小規模システムにおいては認証局構築・運用のコストダ

ウンを実現することができる。

(4) 検証局サービス

署名検証に使用する電子証明書は，例えば社員の退職等によって失効させなければならない場合がある。失効した証明書を使用して署名検証を実施しても署名検証自体が無意味となるため，証明書の有効性を確認することが必要となる。署名検証に使用した証明書が有効か否かを回答(確認)するサービスが検証局サービスである。署名検証後，証明書の有効性検証を行うことで，システムのセキュリティレベルを更に向上させることができる。

(5) ICカード発行代行サービス

ICカード内には所有者本人の秘密鍵，電子証明書，印影などが格納されるが，それらの発行(生成)を行い，発行した秘密鍵，電子証明書，印影をICカードに格納するサービスがICカード発行代行サービスである。お客様に代わってこれらの作業を代行することで，お客様は発行されたICカードを個人認証媒体として使用すればよく，システムを利用する際のこれら準備作業に煩わされることなくSignedPDFシステムを使用することが可能となる。

## 3. SignedPDF実現方法

SignedPDFでは，以下の方法により，PDFファイルに対する電子署名の生成，署名検証を行っている(図1，図2)。

(1) Word(注)やExcel(注)などの文書作成ツールによって電子文書を作成する。

(2) 作成した電子文書をPDFファイルに変換する。

(3) 変換したPDFファイルに電子署名を施すため，ICカードをICカードリーダーに挿入し，ICカードを利用するためのパスワードを入力する。

(4) SignedPDFは，署名対象ファイルに対応するメッセージダイジェストを生成し，ICカード内の秘密鍵によってメッセージダイジェストを暗号化することで，文書作成者の電子署名を作成する。電子文書には，生成された電子署名及び作成者の電子証明書が付加される。

(5) 文書作成者は，SignedPDFによって生成された署名付きPDFファイルを，電子メールなどの手段によって受信者にあてて送付する。

(6) 受信者は，送付された電子文書に付加された電子署名の検証を行う。電子署名の検証は，PDFファイルとともに送付された電子証明書から作成者の公開鍵を取り出し，その公開鍵によって電子署名を復号することで行う。正しく復号できれば署名検証が成功し，文書作成者の本人確認と文書が改ざんされていないことが確認される。

(7) 前記(6)において署名検証に使用した電子証明書が失効している場合には，署名検証が無意味なものとなる。このため，電子証明書の有効性を保証するために証明書検証サーバに証明書が有効か否かを確認し，よりセキュリティレベルを上げることができる。証明書検証サーバには，OCSP(On-line Certificate Status Protocol)サーバによるもの，LDAP(Lightweight Directory Access Protocol)サーバにCRL(Certificate Revocation List)を格納して実現するものなど，幾つかの実現方法がある。

(8) 署名検証の結果はPDFファイル上に視覚的に表示される。有効な署名であることが確認された場合には印影イメージ上に表示されていた“？”は消滅し，無効な署名であった場合には印影イメージ上に“X”が表示される。

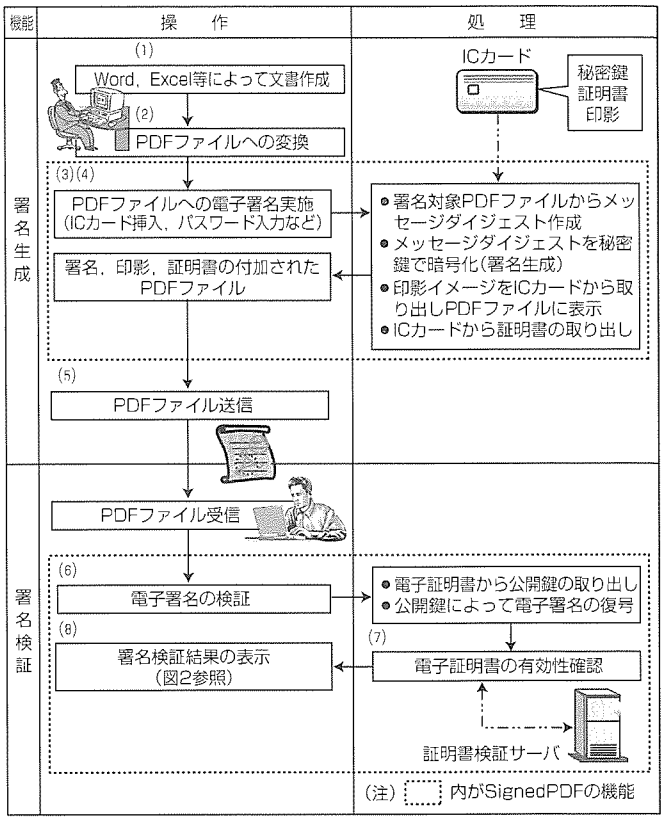



図1．SignedPDFの処理手順

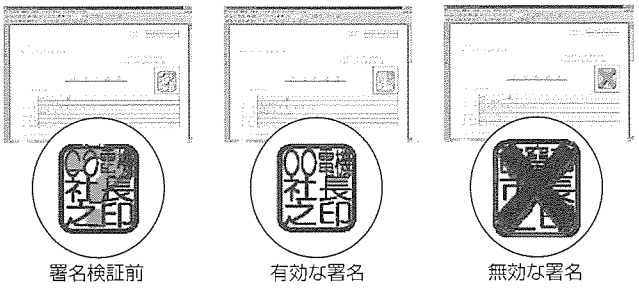



図2．SignedPDFによる電子署名検証結果

## 4. 適用事例

SinedPDFが適用可能でありペーパーレス化や文書送付のスピードアップ化によってコストダウンが実現できるシステム例として，電子申請システムを紹介する。

SingedPDFは，これまで押印が必要なために電子化が

進まなかった金融機関や電力会社への申請手続，行政機関への届出や申請手続など，各種申請業務に適用することができる。ここでは，企業から行政機関への申請業務を例に紹介する(図3)。

製品の海外輸出許可申請や新薬品の許可申請などの申請業務を行う場合には，あらかじめ申請企業側及び行政側とも認証局からSignedPDFを使用するためにICカードが発行されている。

(1) 申請企業側の手順

①必要とする申請書様式を，WWWサイトからのダウンロードや電子メールなどによって行政側から入手する。

②入手した申請書様式によって申請書を作成する(入手した申請書様式がPDFファイルであれば入力エリアに必要事項を記入する。入手した申請書様式がWordやExcelなどであれば申請書作成後PDFファイルに変換する必要がある。)。

③作成した申請書(PDFファイル)に対して，Signed-PDFを使用して電子署名を実施する。この際，ICカードに格納されている秘密鍵が使用され，さらに，電子署名が施されていることを示すためにICカードに格納されている印影イメージがPDFファイル上に表示される。

④電子署名を施したPDFファイルを行政側に送付する。送付手段は，WWWでのアップロードや電子メールでの添付ファイルなど，システム構築方法によって異なることとなる。

(2) 行政側の手順

①受け取った申請書をAdobe Acrobat又はAdobe Acrobat Approvalによって表示する。この際，印影イメージ上には“?”が表示されるが，これは署名の検証が行われていないことを示している。

②SignedPDFの機能によって署名検証を実施する。

③前記署名検証が成功した後，署名検証に使用した申請企業側の電子証明書の有効性を確認するために，SignedPDFは，証明書検証サーバに対して自動的に証明書の有効性確認を行う。署名検証が成功し，さらに証明書検証サーバで証明書の有効性が確認された場合は，印影イメージ上に表示されていた“?”は消滅し，有効な電子署名であったことが示される。電子署名が無効であった場合(署名検証に失敗するか証明書が失効している場合)は，印影イメージ上に“X”が表示される。

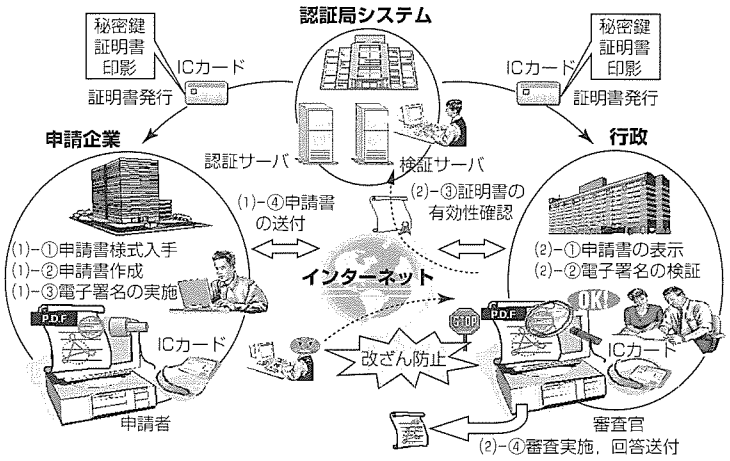



図3．適用事例(電子申請システム)

④有効な電子署名であった場合，行政側は申請内容の審査を行い，回答を作成し申請企業に返送する。この際，行政側もSignedPDFを使用し，回答文書であるPDFファイルに行政側の電子署名を付加する。

SignedPDFは，電子申請システムだけでなく，社内での各種報告書，旅費精算書，りん(稟)議書などを扱うワークフローシステムにも適用することができる。SignedPDFは，社内ワークフローで必要とされる複数の人間が署名を順次実施する多重署名の機能もサポートしている。

## 5. むすび

インターネットでの文書交換が普及するにつれ，電子文書に対する署名のニーズはますます高まってくることが予想される。現時点では対象とする文書はPDFファイルのみであるが，XMLファイルへの署名機能や受信文書に対して自動的に署名・押印・検証を行う署名検証サーバ，又暗号化メッセージ構文CMSへの対応等の研究開発を進めており，今後その成果を新製品に反映していく計画である。

# セキュアストレージ —電子カルテへの適用—

宮崎一哉*
茗原秀幸**

**要　旨**

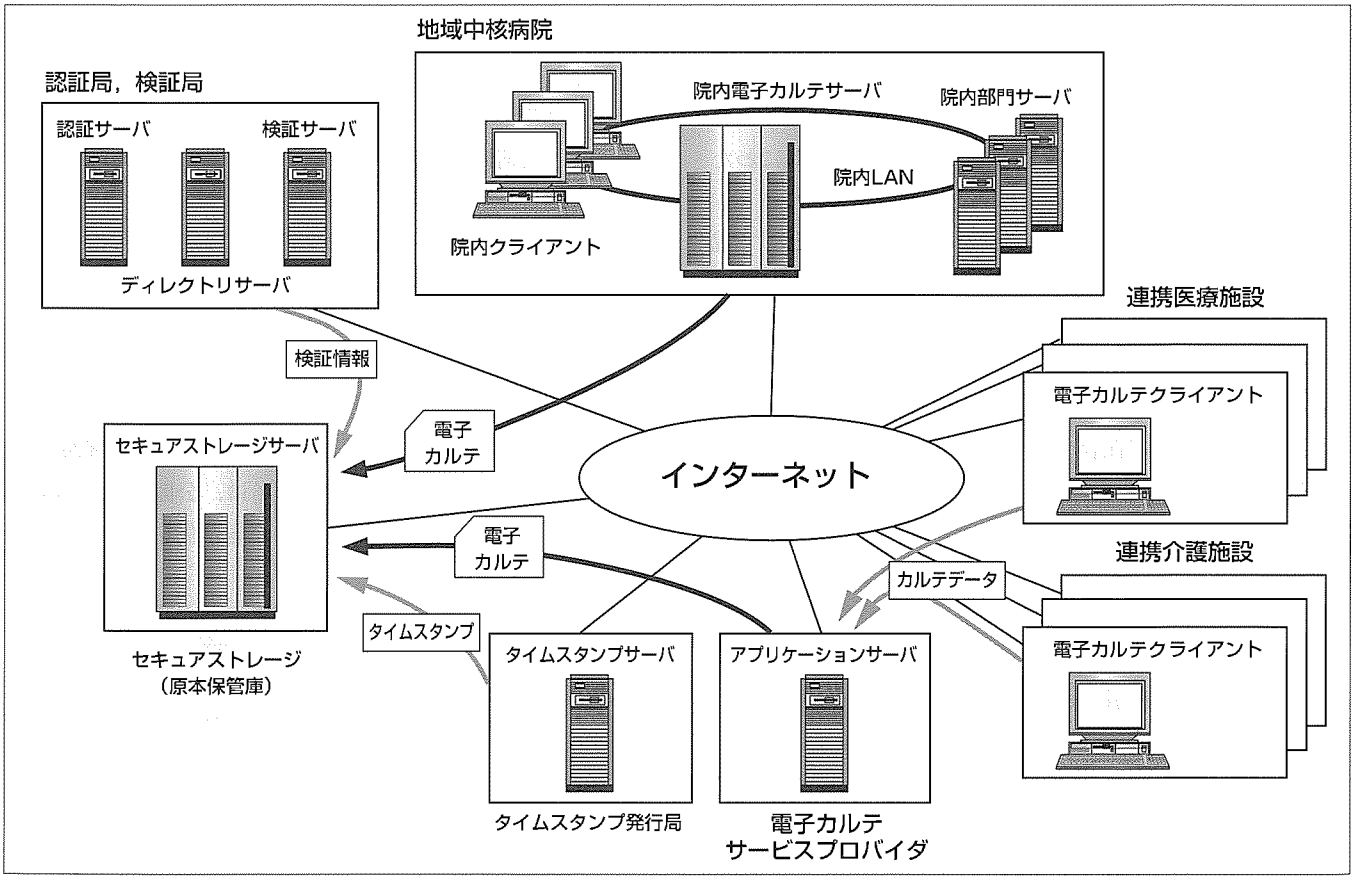
企業や官公庁などにおける業務の電子化に伴い，重要な文書の電子化が急速に進行している。近い将来，電子化される文書の中には，数十年といった長期間にわたって保存することが義務付けられるものも含まれることが見込まれる。

一般に，紙に書かれた文書やマイクロフィルムに記録された文書と異なり，電子化されたデータには改ざん(竄)，漏えいなどの脅威が付きまとうが，こうした脅威に対抗し，原本性を保証することによって電子文書を法的に有効な実効ある文書と位置付けることができ，その結果，真のペーパーレス化が推し進められることになるものと考える。

セキュアストレージは，デジタル署名などのPKI(Public Key Infrastructures：公開かぎ(鍵)基盤)に立脚した情報セキュリティー技術を利用したものであり，電子文書の原本性を長期間にわたって保証する技術である。標準的なフレームワークを用いており原本性の検証が容易であること，デジタル署名の有効性延長技術を備えており原本性を長期間保持できることなどが特長である。

医療分野でも電子化が推進されており，カルテの電子保存に関する指針も示されている。今回，医療現場に普及しつつある電子カルテシステムに対しセキュアストレージを適用し，その有効性を検討した。

今後，セキュアストレージが，医療分野にとどまらず，多くの分野におけるIT化やペーパーレス化に資するものと考える。




**セキュアストレージの電子カルテシステムへの適用**

地域中核病院の院内クライアント，連携医療施設，連携介護施設の電子カルテクライアントで生成されたカルテデータは，それぞれ，院内電子カルテサーバ及び電子カルテサービスプロバイダを経由して電子カルテの原本がセキュアストレージで保管される。セキュアストレージでは，電子カルテの真正性を保証するために電子証書を発行管理し，また，真正性を長期間保証するために安全なタイムスタンプや認証書の検証情報を収集し，デジタル署名の拡張を行う。

*情報技術総合研究所　**医療システム統括部

## 1. まえがき

企業や官公庁などにおける業務の電子化に伴い，契約関係書類，行政文書，電子カルテなど，重要な文書の電子化が急速に進行している。近い将来，電子化される文書の中には，5年，10年，30年，それ以上の長期間にわたって保存することが義務付けられるものも含まれることも想像に難くない。

一般に，紙に書かれた文書やマイクロフィルムに記録された文書と異なり，電子化されたデータには，改竄やすり替え等が容易で痕跡も残らない，盗難，漏えい，盗み見が大量かつ秘密裏に行われやすい，などの安全面での脅威がつきまとう。こうした脅威に対抗し，原本性を保証[1]することによって電子文書を法的に有効な実効ある文書と位置付けることができ，その結果，真のペーパーレス化が推し進められることになるものと考える。原本性を保証するための効果的な技術として，デジタル署名がある。2001年4月1日に電子署名法(電子署名及び認証業務に関する法律)が施行されたことにより，その効果が法的に裏付けられることとなった。ところが，デジタル署名はその効果とともに幾つかの問題点を併せ持つため，単にデジタル署名を電子文書に付与するだけでは長期間原本性を保証することはできない。

今回開発したセキュアストレージ技術は，デジタル署名などのPKIに立脚した情報セキュリティ技術を利用した技術であり，これによって電子文書の原本性を長期間にわたって保証することができる。

本稿では，セキュアストレージの概要と，一例として電子カルテシステムへの適用について述べる。

## 2. 電子文書長期保存の必要性

各種契約書，行政文書，電子カルテなど，法的又は商習慣的に原本を長期間保存することが要請されている文書が存在する。電子化が進む中，前章で述べた電子文書のぜい(脆)弱性が原因で，この要請にこたえるためには余儀なく紙媒体やマイクロフィッシュで長期保存をしていたのが実情である。

電子文書の原本性を確保するためには，電子文書が，いつ，だれによって作成されたもの(又は承認されたもの)であり，それが改竄されていないこと(これらをまとめて電子文書の真正性と呼ぶこととする。)を保証する仕組みが必要となる。PKIにおけるデジタル署名は，電子文書の真正性確保のための最も有力な方法と目されており，昨年施行された電子署名法によって法的な裏付けも得られた。

ところが，単純にデジタル署名を用いただけでは，“だれが作成したものでありそれが改竄されていない”ことまでは保証し得るが，“いつ”を保証することができない。また，デジタル署名の有効性には，時間的な制約が存在する。つまり，公開鍵証明書(認証書)の有効期限切れや失効，デジタル署名に用いられる鍵やアルゴリズムの危たい(殆)化などにより，デジタル署名の有効性は失われてしまう。そこで，デジタル署名を利用して長期間にわたって電子文書の真正性を確保するには，何らかの新しい工夫が必要となる。

## 3. セキュアストレージ

セキュアストレージは，長期間にわたって真正性を確保しながら電子文書を保存するための技術である。その概要は次のとおりである。

### 3.1 電子証書による電子文書の真正性保証

セキュアストレージでは，クライアントからの要求により，文書の登録，検索，参照，削除などを実行する。このとき，以下の内容を保証するための電子証書を発行し，管理する(図1)。

- 文書の作成者又は登録依頼者
- 預かった文書が改竄されていないこと
- 文書に対する登録，検索，参照，削除などのアクセスの事実及び日時

電子証書は，対象文書のハッシュ，アクセス情報，そして3.3節で述べる安全なタイムスタンプ[2]などを含んだ情報とそれに対するデジタル署名で構成される。また，3.2節で述べるデジタル署名の有効性の長期にわたる保持技術により，長期間にわたり電子証書の有効性を保つことができる。従来から提案されている耐タンパーなハードウェアで原本性を確保する技術ではその正当性を客観的に検証することが極めて困難であったが，今回開発した技術は，PKIに基づくソフトウェアによって実現した技術であるため，第三者が標準的な手段で容易に正当性を検証することが可能である。

### 3.2 長期保存におけるデジタル署名の有効性の確保

電子証書で利用するデジタル署名は，公開鍵証明書の有効期限，失効，鍵やアルゴリズムの危殆化など，本来，時

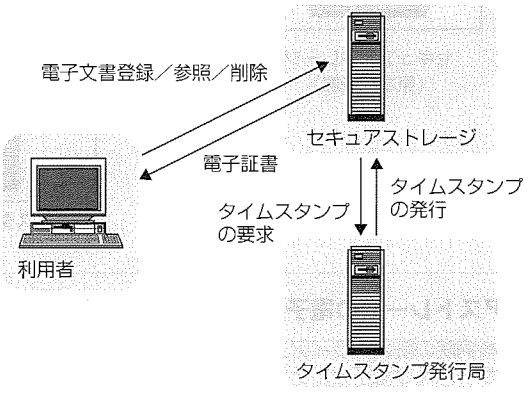



図1．セキュアストレージの位置付け

間経過に伴って有効性を保証できなくなる可能性をはらんでおり，このような時間的制約を乗り越えるための仕組みが必要となる。

この対応として，IETF(Internet Engineering Task Force)やETSI(European Telecommunications Standards Institute)で標準化が進められている書式[3][4]をベースとして，デジタル証明書の失効に関する情報や安全なタイムスタンプを時間経過とともにデジタル署名に対して拡張していく技術を開発した(図2)。この技術開発は，IPA事業「電子政府情報セキュリティ基盤技術開発事業 ― 長期保存文書のための電子署名期限延長技術開発 ― 」の一環として電子文書長期保存技術検討コンソーシアムの一員として実施したものである。

標準化の進められている書式はデジタル署名の作成者又は検証者といった当事者自らが署名を拡張し保管することが想定されていたが，今回の技術では署名の拡張及び保管処理を第三者に委託することができるよう改良を加えた。

この技術を用いることにより，デジタル署名の持つ時間的制約を克服するデジタル署名の有効性延長サービスを，第三者による単体のサービスとしても提供することが可能となる。

### 3.3 電子文書の作成日時の保証

デジタル署名は，データの作成者やデータが改竄されていないことを保証できるが，時刻に関する保証，例えばデータが作成された日時の保証はできない。

安全なタイムスタンプは，デジタルデータに対して，①ある時刻に存在していたこと，②その時刻以降に改竄されていないこと，の二つを保証する技術である。タイムスタンプは，TTP(Trusted Third Party：信頼できる第三者機関)であるタイムスタンプ発行局が証明したいデータのハッシュ値と時刻情報を組み合わせたものにデジタル署名を施した形式であり(図3)，IETFで標準化活動が進められており，RFC3161[5]として標準化された。

我々はIETF標準に準拠したタイムスタンプサーバソフトウェアを開発し，電子証書の作成やデジタル署名の有効性延長に利用している。

以下に，セキュアストレージの特長をまとめて示す。

(1) 安全なタイムスタンプ付きの電子証書を発行することにより，電子文書に対する真正性を保証

(2) 署名延長を用いてデジタルの署名の有効性を維持し，署名文書及び電子証書の長期にわたる真正性保証を実施

(3) 署名者又は検証者の委託を受け，第三者であるエージェントが電子署名文書の長期保存を実施可能

(4) 標準的データ形式を採用しており，真正性の検証をオーソリティに委託する必要がなく，クライアント(署名者，検証者，仲裁者)自身で実施することが可能

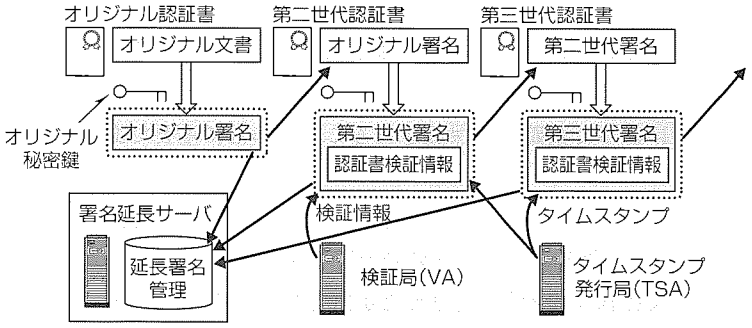



図2．署名の有効性延長

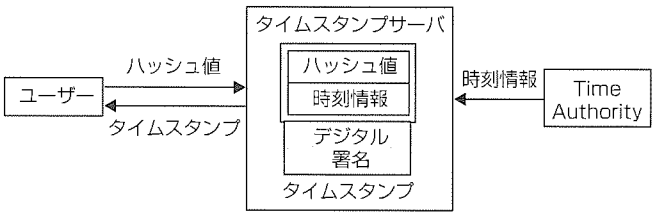



図3．安全なタイムスタンプ

## 4. 電子カルテにおけるセキュアストレージの適用

平成10年6月，厚生省の“カルテ等の診療情報の活用に関する検討会”において診療情報の電子化を今後一層推進すべきとの報告がなされ，平成11年4月22日付の“診療録等の電子媒体による保存について”によって電子媒体による保存の基準が明確化された[6]。その基準は“データの真正性，見読性及び保存性”(電子保存三原則)を基本とし，“プライバシー保護”や“証拠能力・証明力”にまで言及するものとなっている。

以下，電子カルテにおけるセキュアストレージの位置付け，必要性，及び適用事例について述べる。

### 4.1 技術的対策と運用的対策による相互補完

電子カルテを採用する場合，真正性，見読性，保存性，プライバシー保護及び証拠能力・証明力の確保を，技術的対策と運用的対策の相互補完で対応することとなる。そのため，技術的対策が確実であればあるほど運用的対策が容易になる。電子カルテシステム導入推進担当者からすれば，運用コストを抑え十分な技術的対策を施したシステムの導入が望まれる。セキュアストレージは，電子保存三原則の確保を技術的側面からサポートし，証拠能力・証明力の確保を容易にすることが可能である。

### 4.2 証拠能力・証明力の確保

「高度情報通信社会推進本部制度見直し作業部会報告書平成8年6月」によれば，“電子データの証拠能力及び証明力の確保については，データの入力及び出力の正確性を確保するとともに，データの改変の可能性を減殺することにより電子データの信頼性を高め，かつこれに対する責任

の所在を明らかにする必要がある"としている。証明力については裁判官の自由な判断にゆだねられているが，その評価は電子データの正確性等の評価に依存するため，技術的対策によって正確性が保証されることは非常に重要である。

セキュアストレージは，利用者のデータ入力及び出力内容に応じ，"利用者""データの内容""その時刻""コミットメント又は操作の種類(入力したか出力したかなど)"を示す電子証書を発行することにより，電子文書の真正性を確保する"電子公証機能"を持っている。これにより，技術的にその正確性を保証することができ，証拠能力・証明力の確保に資することができる。

### 4.3 データの改変の可能性の減殺

カルテは医師法によって5年間の保存義務があるが，電子カルテは，従来の紙カルテに比べ保管スペースが小さくて済むようになることから，より長期の保存が可能となる。先進的な病院では，"生涯電子カルテ"のコンセプトの下に，患者の一生分の電子カルテを蓄積する計画を推進している。このような100年近い長期保存を行う場合，現在一般的に利用されている暗号が陳腐化し，通常の電子署名を行っただけでは改竄防止が困難になる。そのため，セキュアストレージでは，署名延長技術を用いて長期保存にも耐えるシステムを採用している。

### 4.4 電子カルテシステムとの連動

セキュアストレージはあくまで保管庫であり，カルテをそのままの状態で安全に長期保存するものであるため，長期保存したデータの見読性を保証するには保存するカルテが将来にわたって容易に見読可能な構造でなければならない。しかし，電子カルテシステムは医療情報システムベンダー各社が独自の仕様で開発を行っており，各社独自のデータ構造のまま保存した場合，システムのリプレース等によってカルテの表示が不可能になる可能性も否定できないため，長期的な見読性の保証ができなくなる。

そこで，平成11年度厚生省委託事業によって作成された「電子保存された診療情報録の交換のためのデータ項目セット」(以下"J-MIX"という。)のXMLファイルをカルテとして保存することにより，将来にわたって電子カルテシステムとの連携を保証するとともに，カルテ単独での見読性を保証する仕組みを構築した。電子カルテシステムは当日確定処理されたカルテデータをJ-MIX形式のXMLファイルとしてセキュアストレージに転送するだけでよく，それ以降の電子保存三原則の確保についてはセキュアストレージが管理する電子証書によって行うため，電子カルテシステム側では高コストの電子保存システムを構築する必要がない。

### 4.5 電子カルテシステムへの適用事例

要旨のページの図のシステムは，経済産業省の「先進的IT活用による医療を中心としたネットワーク化推進事業 ― 電子カルテを中心とした地域医療情報化 ―」において，医療法人鉄蕉会による亀田病院を中心とした南房総地域の医療情報ネットワーク推進事業に採用された。この事業では，地域連携のための電子カルテシステムの電子保存三原則対応を実現するために，地域連携用のASP型電子カルテシステムのカルテ原本のバックアップをJ-MIX形式のXMLファイルとして保管している。

## 5. むすび

文書の電子化において，文書のライフサイクルの最終ステップに位置付けられる"原本の長期保管"が取り残されており，これがペーパーレス化を阻害する大きな要因となってきた。セキュアストレージは，電子署名法の施行によって法的裏付けを得たデジタル署名技術を駆使して，電子的な原本を長期間にわたって保存することを可能とする技術である。

医療分野では，厚生労働省において電子カルテの外部保存についての検討が行われており，従来は不可能であったASP型の電子カルテシステムが今後普及していくことが予想されている。また，従来病院内で保管していた電子カルテを，より堅牢なデータセンターに保管したいという要望もある。これらの受け皿としてセキュアストレージを活用することで低コストでの電子カルテシステム構築が可能となる。

セキュアストレージでは，電子文書に対する様々なコミットメントを保証する電子公証機能を保有しており，電子原本の保管のみでなく，EDIのような電子データや電子文書の交換における否認防止にも活用できる。我々の提案するセキュアストレージは，医療を始めとする他の多くの業界におけるペーパーレス化，IT化の推進に貢献することができると考える。

## 参考文献


(1) 総務庁共通課題研究会報告書：インターネットによる行政手続の実現のために(2000-3)

(2) 宮崎一哉：電子文書における署名とタイムスタンプについて，三菱電機技報，**75**，No.2，152～154（2001）

(3) RFC3126：Electronic Signature Formats for long term electronic signatures（2001-9）

(4) ETSI Standard：ETSI TS 201 733 Electronic Signature Formats（2000-12）

(5) RFC3161：Time-Stamp Protocol(TSP)（2001-8）

(6) 財団法人医療情報システム開発センター：診療録等の電子媒体による保存に関する解説書（1999-10）

# メモリカードを用いたデジタルコンテンツ配布システム

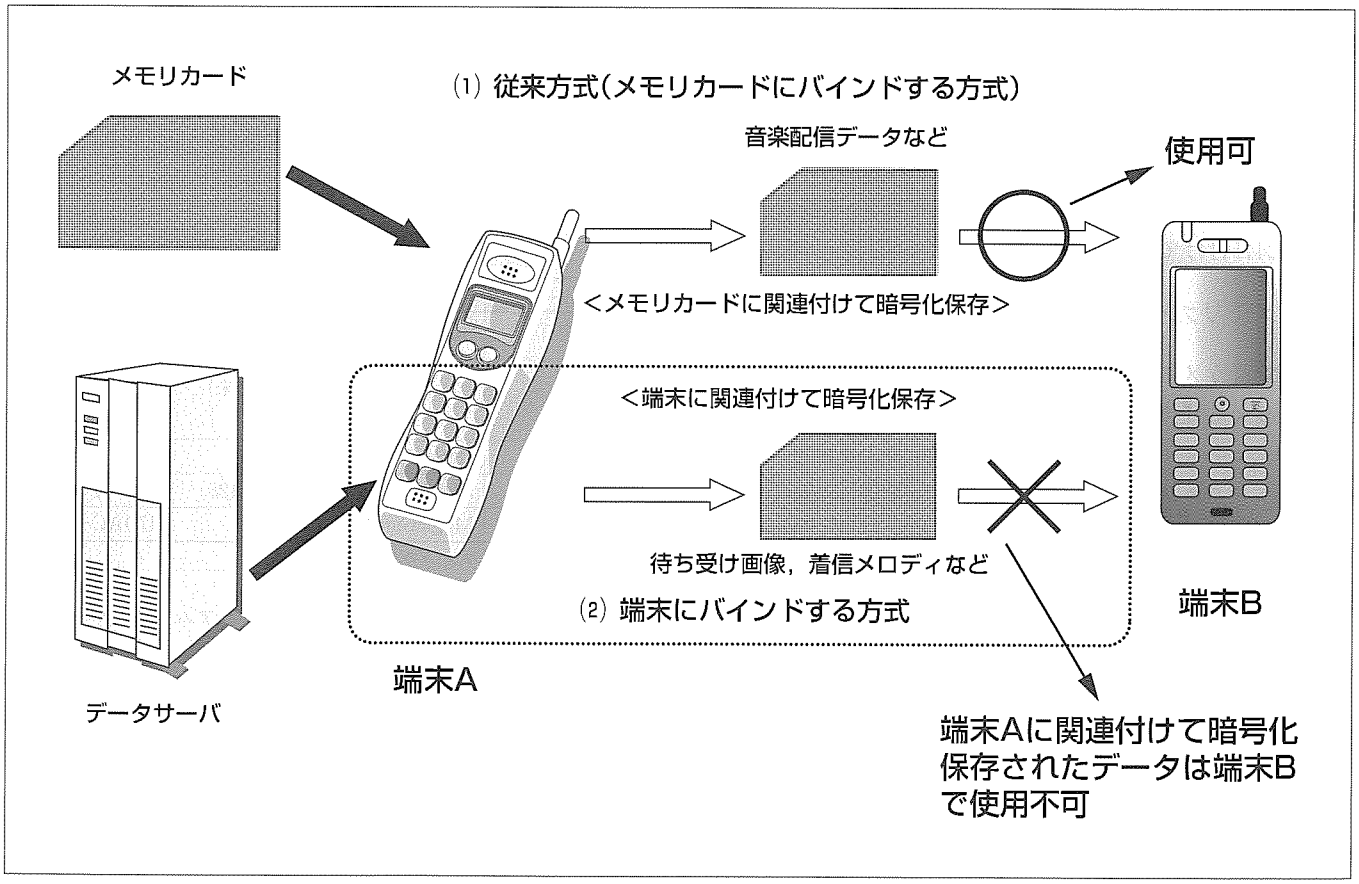
宮崎一哉*
中嶋春光*

**要　旨**

次世代携帯電話向けデータ配信サービスに代表されるデジタルコンテンツ配信ビジネスでは，大容量のデジタルコンテンツデータの配信が予定されている。これに対応して，モバイル機器には，大容量のデジタルコンテンツデータをバックアップするために，メモリカードなどの小型のリムーバブルメディアを利用することが考えられる。ところが，デジタルコンテンツデータの保存に際しては，不正コピーによる違法な二次利用の防止など配信事業者の権利を守るための技術，すなわち著作権保護技術が必要となる。

従来のメモリカードにおける著作権保護技術は，メモリカード間での不正コピーを防止する技術であり，携帯電話におけるコンテンツ配信，つまり個別の機器ごとに使用を許可するようなコンテンツには適用できなかった。

そこで，従来の著作権保護技術に加え，上記の要請に適合した方法でメモリカードにデジタルコンテンツデータを安全かつ高速に保存する技術を開発した。従来のデジタルコンテンツデータをメモリカードにバインドする方式と，三菱電機が開発した端末にバインドする暗号化保存方式を使い分けることにより，データの二次利用を想定していないデジタルコンテンツ配信ビジネスに対して，配信事業者の要求に適合した方法で権利を守りながら対応することが可能となる。




**携帯電話への適用例**

従来のメモリカードにバインドする著作権保護方式によってコンテンツを格納した場合，メモリカード間でのコピーは不可能になるが，端末Aに配信されたコンテンツが他の端末Bでも使用できる。一方，端末にバインドする著作権保護方式によってコンテンツを格納した場合，メモリカード間でのコピーは可能だが，端末Aに配信されたコンテンツは他の端末Bでは使用できない。両方式を使い分けることにより，コンテンツホルダの要求に応じた配信が可能になる。

*情報技術総合研究所

## 1. まえがき

次世代携帯電話向けデータ配信サービスに代表されるデジタルコンテンツ配信ビジネスでは，大容量のデジタルコンテンツデータの配信が予定されている。これに対応して，モバイル機器には，大容量のデジタルコンテンツデータをバックアップするために，メモリカードなどの小型のリムーバブルメディアを利用することが考えられる。ところが，デジタルコンテンツデータの保存に際しては，不正コピーによる違法な二次利用の防止など配信事業者の権利を守るための技術，すなわち著作権保護技術が必要となる。

従来のメモリカードにおける著作権保護技術は，メモリカード間での不正コピーを防止する技術であり，携帯電話におけるコンテンツ配信，つまり個別の機器ごとに使用を許可するようなコンテンツには適用できなかった。

そこで，ネットワークメディアとして既に1,000万枚以上の出荷実績を持つソニー㈱の“メモリースティック”の技術と三菱電機の高度なセキュリティ技術(暗号化アルゴリズム“MISTY”[1])とを融合させることにより，上記の要請に適合した方法でメモリースティックにデジタルコンテンツデータを安全かつ高速に保存する技術を開発した。ソニー㈱が従来から持っているデジタルコンテンツデータをメモリースティックにバインドする“MagicGate”方式と当社が開発した暗号化保存方式を使い分けることにより，データの二次利用を想定していないデジタルコンテンツ配信ビジネスに対して，配信事業者の要求に適合した方法で権利を守りながら対応することが可能となる(本件は2001年5月24日付けで広報済み)。

## 2. メモリカードにおける従来の著作権保護方式

ここで言うメモリカードとは，フラッシュメモリを内蔵した小型メモリカードのことで，コンパクトフラッシュ，スマートメディア，マルチメディアカード，メモリースティックなどがその例である。メモリカードは，スマートメディアを除き，内部にコントローラとフラッシュメモリを持ち，データはコントローラを通してフラッシュメモリに読み書きされる[2]。

著作権保護機能を備えたメモリカードに，マジックゲートメモリースティック(MG-MS)[3]，SDカード[4]，セキュアマルチメディアカード(SMMC)[5]がある(**表1**)。

これらのメモリカードが実装している著作権保護方式は，コンテンツをメモリカードにバインドする方式である。

コンテンツをメモリカードにバインドする著作権保護方式の概念を**図1**に示す。

それぞれのメモリカードはメディア固有かぎ(鍵)を持っている。メディア固有鍵は，通常，メモリカードごとに異なる値である。メディア固有鍵は，メモリカード内のユーザーアクセス不可なセキュアな領域に保存されているため，メモリカード間でのコピーはできない。

コンテンツは，メモリカード内に格納される際に，メディア固有鍵を利用しなければ復号できないように暗号化された状態で保存される。

したがって，あるメモリカードに保存したコンテンツを悪意を持つユーザーが他のメモリカード(メモリカード2)にコピーしても，メディア固有鍵が同一でないため，コピーしたコンテンツを復号できない。つまり，コンテンツはメモリカードにバインドされている。

## 3. 端末にバインドする著作権保護方式

一方，今回当社が開発した方式は，コンテンツを端末にバインドする著作権保護方式である。以下，その実現方式について説明する。

### 3.1 外部出力時の処理(図2)

(1) ランダムなコンテンツ鍵Kcでコンテンツを暗号化する。

(2) ランダムな固有鍵生成ロジックインデックス番号iによって一意に決まる固有鍵生成ロジックFtiで，端末に固有な端末固有IDtから端末に固有な鍵(端末固有鍵Kti)を生成する。

(3) 端末固有鍵Ktiでコンテンツ鍵Kcを暗号化する。

(4) 暗号化コンテンツ，固有鍵ロジックインデックス番号i，暗号化コンテンツ鍵を格納したカプセルファイルを生成し，保存する。

**表1．著作権保護機能を備えたメモリカード**

| | MG-MS | SDカード | SMMC |
|---|---|---|---|
| 規格策定 | SONY | 松下電器産業<br>東芝<br>SanDisk(米) | 日立製作所<br>三洋電機<br>Infineon Technologies AG(独) |
| 協力企業 | 189社 *1 | 381社 *2 | 39社 *3 |
| 容量(MB) | 32，64，128 | 32，64，128 | 32，64 |
| 著作権保護技術 | MagicGate | CPRM | UDAC-MB |

*1 メモリースティック賛同企業
*2 SDA(SD Association)参画企業
*3 ケータイ de ミュージック・コンソーシアム・メンバー

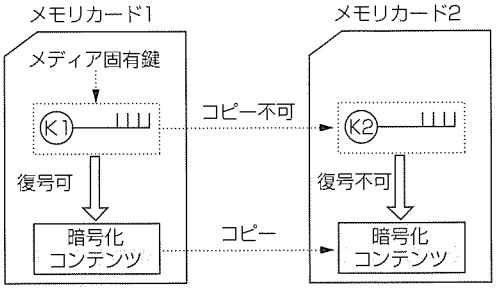



**図1．メモリカードにバインドする著作権保護方式**

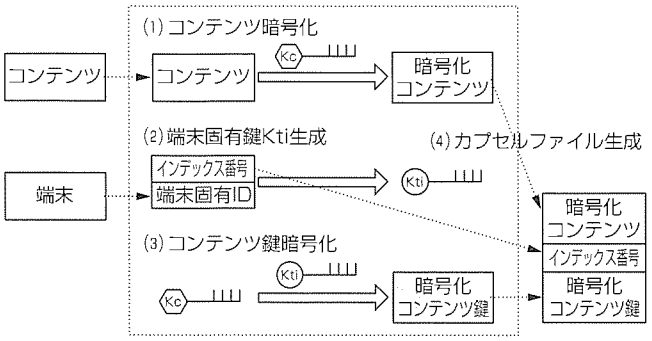



図2．外部出力時の処理

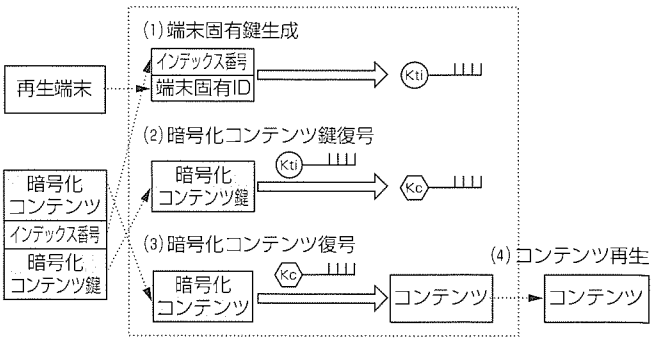



図3．再生時の処理

### 3.2 再生時の処理（図3）

(1) 固有鍵生成ロジックインデックス番号iによって一意に決まる固有鍵生成ロジックFtiで，端末に固有な端末固有ID tから固有鍵Ktiを生成する。

(2) 暗号化コンテンツ鍵を固有鍵Ktiで復号する。

(3) 暗号化コンテンツをコンテンツ鍵Kcで復号する。

(4) コンテンツを再生する。

したがって，ある端末でメモリカードに保存したコンテンツを悪意を持つユーザーが再生権限を持たない別の端末で再生しようとしても，その端末固有IDが同一でないため，コンテンツを再生できない。つまり，コンテンツは端末にバインドされている。

また，この著作権保護方式においては，次の脅威への対抗も可能である。

### 3.3 端末の成り済まし対策

端末の固有IDを書き換え，コンテンツの再生権限を持つ端末に成り済ます(固有IDが同一になるよう書き換える)ことで，再生権限を持たないコンテンツを再生できてしまう。

ここで，ある端末の固有IDを書き換えるためには専用機器や特殊なツールが必要であり，一般ユーザーがこの攻撃を実現することは困難である。また，端末の固有IDに対する耐タンパー性を強化することで，この攻撃に対する安全性を向上させることができる。

### 3.4 メモリに展開されたデータの取得

コンテンツの再生中，攻撃者が端末の内部メモリ領域に動的に展開されるデータを取得した場合，コンテンツの平文データが流出してしまう。

ここで，内部メモリ領域に動的に展開されるデータを取得するためには専用機器やツールが必要であり，一般ユーザーがこの攻撃を実現することは困難である。また，内部メモリ領域に動的に展開されるデータに対する耐タンパー性を強化することで，この攻撃に対する安全性を向上させることができる。

### 3.5 カプセルファイルの解析

ユーザーがパソコン等を利用してカプセルファイルを解析しカプセルファイルに格納されている暗号化コンテンツを復号できた場合，平文データが流出してしまう。

固有鍵の安全性が保証される場合，暗号化コンテンツ，及び暗号化コンテンツ鍵のそれぞれに対する攻撃は，実装する暗号アルゴリズムの安全性に依存する。差分解読法，線形解読法のそれぞれに対してその安全性が数学的に証明されている当社暗号アルゴリズムMISTYを実装することで，上記攻撃に対して十分な安全性を保証できるようになる。

また，固有鍵の安全性は，固有鍵を生成するときの種である固有ID，及び固有鍵生成ロジックの安全性に依存する。端末によって異なるが，固有IDをそのユーザー自身にさえも秘密にすることは困難であることが多く，その場合，固有鍵生成ロジックを秘密にすることが重要になる。なお，ここで，固有鍵生成ロジックは端末内部の静的なプログラム(＋データ)として実装される。

ここで，端末内部の静的なプログラムやデータにアクセスするためには専用機器や特殊なツールが必要であり，一般ユーザーがこの攻撃を実現することは困難である。また，端末内部の静的なプログラムやデータに対する耐タンパー性を強化することで，この攻撃に対する安全性を向上させることができる。

## 4. 携帯電話端末向けユーザーコンテンツへの適用

近年，iモード等の携帯電話端末向け情報配信サービスを利用して着信メロディやゲーム(Java(注)アプリケーション)等のユーザーコンテンツを配信するコンテンツ配信サービスが進展している。

このコンテンツ配信サービスの進展に伴い，ユーザーが購入したコンテンツを保存できるように小型外部記憶媒体であるメモリカードを装着可能な携帯電話端末が各携帯電話端末メーカーによって開発され，市場に現れつつある。

当社でも，昨年度，メモリースティックを装着可能なメモリースティック対応携帯電話端末(以下“MS対応携帯電話端末”という。)を試作開発した。

上記試作開発において，メモリースティックに保存されるコンテンツの著作権保護を目的にこの著作権保護方式を実装した。

MS対応携帯電話端末の試作開発において，端末を一意に識別するための固有IDに携帯電話端末の電話番号を使用した。

電話番号を固有IDとすることで，ユーザーが携帯電話端末本体を変更した場合でも，同じ電話番号を継続して使用するならば，変更前の携帯電話端末で再生できるコンテンツはすべて変更後の携帯電話端末でも再生できるようになる。

## 5. コンテンツ販売サービスへの応用

この著作権保護方式を応用することにより，マルチメディアキオスクを利用したコンテンツ配信サービスの改善が可能となる。

携帯電話端末向けマルチメディアキオスク対応コンテンツ配信システム（**図4**）[6]は，携帯電話端末向け情報配信サービスとメモリカード対応携帯電話端末を利用することによって，ユーザーがマルチメディアキオスク操作時に感じる“煩わしさ”や“束縛感”を軽減し，かつ，コンテンツの不正コピー防止を実現するシステムである。

このシステムで，ユーザーは，携帯電話端末向け情報配信サービスを利用して，プライベート空間（好きな時間，好きな場所）でコンテンツを検索する。その結果，携帯電話端末向け情報配信サーバからコンテンツのID及びユーザーの携帯電話端末でのみ生成可能な固有鍵で暗号化されたコンテンツ鍵をダウンロードし，これらのデータをメモリカードに保存する。

次に，ユーザーは，コンビニエンスストア等に設置されているマルチメディアキオスクにメモリカードを装着し，コンテンツを購入する。このとき，マルチメディアキオスクは，メモリカードに保存されているコンテンツID及び暗号化コンテンツ鍵をロードし，コンテンツIDに対応するコンテンツをカプセルファイルの形で自動的にメモリカードに保存する。このとき，メモリカードに保存されるコンテンツは携帯電話端末にバインドされる。

上記により，ユーザーがマルチメディアキオスク操作時に感じる“煩わしさ”や“束縛感”の軽減，及び販売するコンテンツの著作権保護を同時に実現できるようになる。

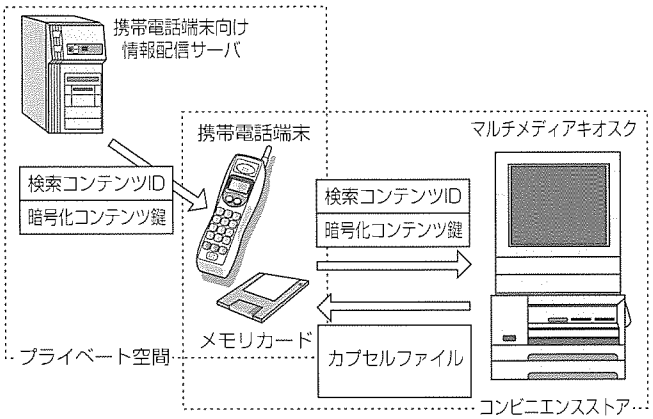



**図4．マルチメディアキオスク対応コンテンツ配信システム**

## 6. むすび

従来のメディアバインド方式に加え本稿で紹介した端末バインド方式を利用することにより，配信事業者の要求に適合した方法で権利を守りながらコンテンツ配信のビジネスを展開することが可能となる。

本稿ではメディアとしてメモリカードのみを取り上げたが，この方式自体がメモリカードの種別に何ら制限を受けることがないことはもちろん，ハードディスク，CD-ROM，CD-R，MO，DVDなどのメモリカード以外のストレージメディアにも適用可能なものである。携帯電話を始め，様々なPDAへの適用や周辺ビジネスの展開への貢献が期待される。

## 参考文献

(1) 松井　充，ほか：ブロック暗号アルゴリズム“MISTY”，三菱電機技報，**72**，No.5，400～403（1998）
(2) 芳尾太郎，ほか：全ての機器にメモリ・カード，Nikkei Electronics，No.768（2000-4-24）
(3) MemoryStick Information for Developers，“http://www.memorystick.org”
(4) SD Card Association，“http://www.sdcard.org”
(5) ケータイ de ミュージック・コンソーシアム，“http://www.keitaide-music.org”
(6) 中嶋春光，ほか：携帯電話端末向けマルチメディアキオスク対応コンテンツ販売システムの実現方式，情報処理学会第62回全国大会，3～7（2001）

# 不正アクセス対策技術

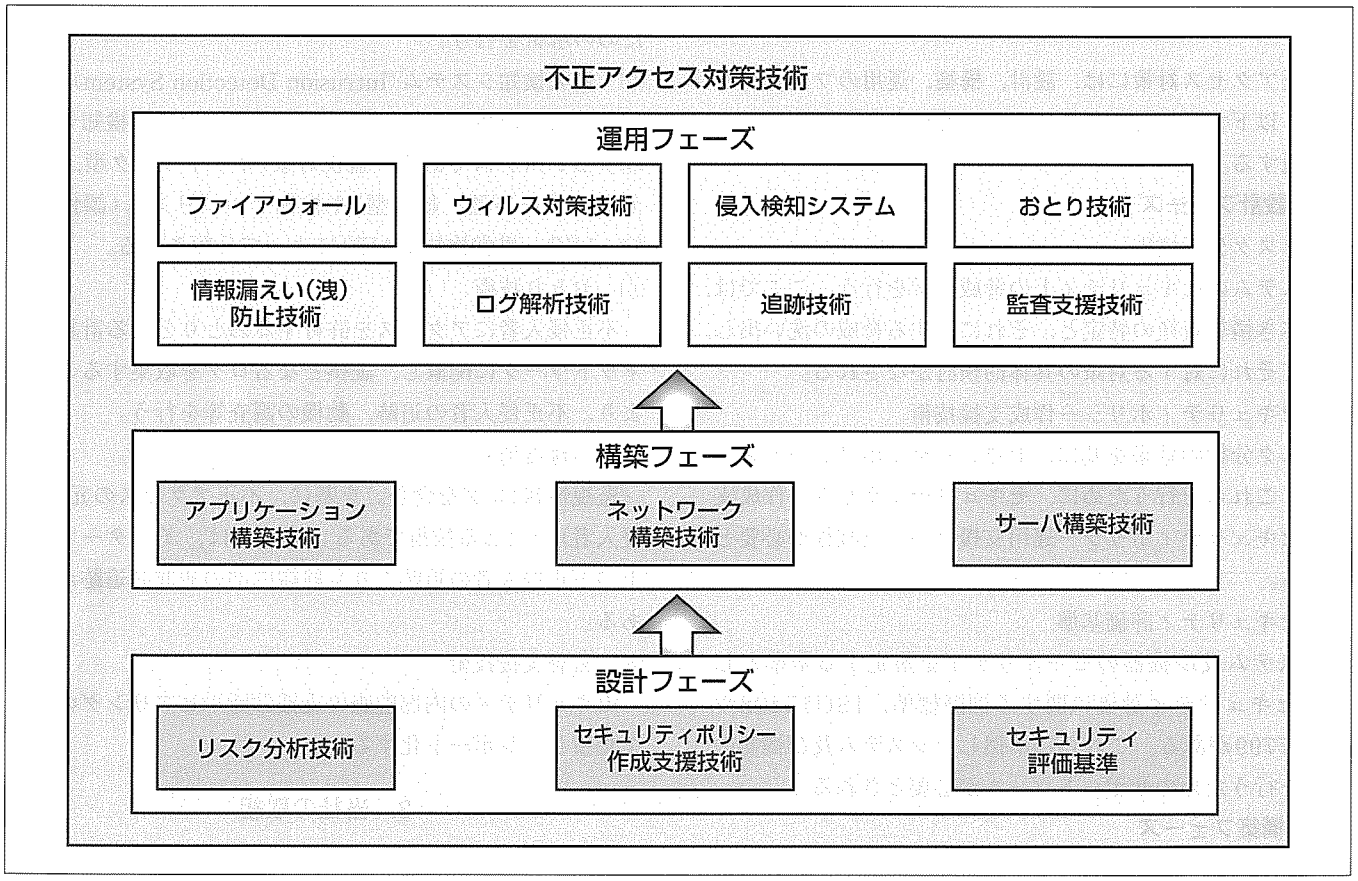
藤井誠司*
勝山光太郎**

**要　旨**

不正アクセス対策の重要性が認識され，ファイアウォール等の不正アクセス対策が実施されるようになった。しかし，不正アクセスの手法は常に進化を続け，より高度な不正アクセス対策技術が求められている。また，インターネットの普及が管理対象のネットワークの大規模化を促進したため，情報システムをトータルに守る仕組みとして個々の不正アクセス対策ツール群を統合的に効果良く，管理・運用することが重要となってきている。三菱電機では，このような状況に対応する不正アクセス対策要素技術及びシステムの研究開発を行っている。

本稿では，不正アクセス対策における設計，構築，運用フェーズごとに必要とされる不正アクセス対策技術について概説し，当社が取り組んでいる不正アクセス対策技術の中から，監査支援技術である統合型セキュリティ診断ツール及び侵入検知技術を発展させたおとり誘導による不正アクセス対策システムについて述べる。

今後は，これらの技術を高度にセキュリティな不正アクセス対策を必要としている社会重要インフラシステムへ展開していく。




**不正アクセス対策技術**

不正アクセス対策には，設計，構築，運用のフェーズがある。各々のフェーズは，不正アクセス対策技術によって構成される。三菱電機は，これらを構成する不正アクセス技術及びそれらの要素技術で構成されるシステムの研究・開発を行っている。

*情報技術総合研究所　**同研究所(工博)

## 1. まえがき

インターネットの進展に伴い，電子商取引なども活発に行われるようになり，セキュリティの重要性が増してきている。ネットワーク化により，情報システムは，常に，盗用，不正アクセス，データの改ざん，システムの破壊や利用妨害といった脅威にさらされている。これに加えて，組織内部のものによる意図的な脅威についても無視できない状況がある。

現状では各種の不正アクセス対策のためのツールはばらばらに提供されていることが多く，ツールの体系化が求められている。ツールを体系化することにより，ユーザーはそれぞれのツールの機能，役割，位置付けを明確に把握でき，有効な対策を推進可能となる。

情報システムをトータルで守る仕組みとして，情報セキュリティ管理アーキテクチャを構築し，ツール群を効果的に組み合わせ，運用可能とする必要がある。

本稿では，不正アクセス対策技術について概説するとともに，三菱電機の不正アクセス対策技術への取組の一部として，統合型セキュリティ診断ツール及びおとり誘導による不正アクセス対策システムについて述べる。

## 2. 不正アクセス対策技術

不正アクセス対策には，設計，構築，運用のフェーズがある。以下では，各々のフェーズで使用される技術について概説する。

### 2.1 設計フェーズ

(1) リスク分析技術

システムのセキュリティ上の脅威解析を行う。ここでは，守るべき情報資産の特定と，それに対する脅威の洗い出し，そしてそれに対する対策の具体的検討がなされる。

(2) セキュリティポリシー作成支援技術

リスク分析の結果を基に，セキュリティポリシーを策定する。これらを行うために，セキュリティポリシー作成支援やセキュリティポリシー運用支援といった技術が必要とされる。

(3) セキュリティ評価基準

システム及び機器のセキュリティを規定する基準として，セキュリティ評価に関する国際標準，ISO15408やISO17799がある。これらに準拠したシステム及び機器の開発を行うためのサポートツールが必要とされる。

### 2.2 構築フェーズ

バッファオーバーフローなどのぜい(脆)弱点への攻撃に対応できるようにアプリケーションを設計・構築すること，脆弱点が報告されたOSやアプリケーションに適切なパッチを適用すること，ファイアウォールやルータ，ハブなどのネットワーク機器や，Webサーバやメールサーバ，DNSサーバなどのサーバアプリケーションをセキュアに設定することなどにより，セキュリティの高い計算機及びネットワークを構築することが重要である。

### 2.3 運用フェーズ

(1) ファイアウォール

内部ネットワークと外部ネットワークを遮断し，アクセス制御を行う。最近では，インターネットを利用する個人ユーザーの増加を反映して，ユーザーの端末上でファイアウォール機能を実現するパーソナルファイアウォールの利用が増えている。

(2) 情報漏洩防止技術

メール監視，Web監視等により，内部から外部への情報流出の防止や，好ましくない情報や業務と関係ない情報へのアクセス制限を行う。

(3) ウイルス対策技術

メール，Web，FTPなどにより，内部ネットワークへ送信されるウイルスの監視・除去を行う。最近のウイルスを利用した不正アクセスの増加により，重要性を増している。

(4) ログ解析技術

管理者が監査証跡(ログ)を容易に監査できる形式への変換やログの中から不正アクセスに関連する情報を抽出するための解析を行う。

(5) 侵入検知システム(Intrusion Detection System)

計算機及びネットワークへの不正アクセスを検知し，管理するシステムである。監視対象(ネットワーク型，ホスト型，サーバ型，統合型)や検知アルゴリズム(誤使用検知：MID，異常検知：AID)によって分類される。

(6) おとり技術

不正侵入者にアクセスを許可するおとりとなる計算機をネットワークに配置し，証拠となるログを収集することにより，不正侵入者の追跡，動機の調査等を行う。

(7) 追跡技術

監視情報(ログを含む。)を基に，不正アクセスの元(不正侵入者)をたどる技術である。現状では，インターネット上の不正侵入者の追跡よりも組織内部の犯罪の追跡が主である。

(8) 監査支援技術

セキュリティの内部監査の支援診断やヒアリングの結果を集積し，レポート化する。

## 3. 当社の取組

前節で述べたセキュリティ対策技術について，当社は要素技術の研究開発やそれらによって構成されるセキュリティシステムの開発を行っている。

通産省平成10年度第三次補正予算事業「産業・社会情報化基盤整備事業」の中で，大規模なマルチベンダー環境に

対する外部からの不正アクセスを検知し防御する「不正アクセス防止基盤システム」を富士通㈱，㈱日立製作所と共同で開発した。このシステムでは，マルチベンダー環境における外部からの不正アクセスの検知・防御を主ターゲットとしている。これを実現するために，監視，対策決定，設定変更を連携して行う枠組みである統合フレームワークを策定するとともに，そのフレームワークに準拠したプロトシステムの開発を行った。

以下では，その他の不正アクセス対策技術の開発例として，監査支援技術である統合型セキュリティ診断ツール，及び侵入検知技術を発展させたおとり誘導による不正アクセス対策システムについて紹介する。

### 3.1 統合型セキュリティ診断ツール

セキュリティ診断ツールは，検査対象のネットワーク又はホストに対してセキュリティ脆弱点を検査することにより，検査対象の危険度を評価し報告することを目的とする。

サイトの安全性を保つためには，不正アクセスに対するサイトの脆弱性を定期的に監査する必要がある。そのため，近年，様々なセキュリティ診断ツールが開発され販売されている。しかし，これらは，指定されたホスト上のセキュリティホールを検出し，それぞれの危険度を評価し報告するのみであり，以下のような問題点がある。

- 複数のセキュリティホールが組み合わされた場合のリスクを評価できない。
- 致命的なセキュリティホールを持つホストを踏み台として更に内部のホストへの攻撃が行われた場合のリスクを評価できない。

図1に，統合型セキュリティ診断ツールのシステム構成を示す。統合型セキュリティ診断ツールは，上記の問題点を解消するために，セキュリティホールを検出する機能に加え，次のような特長を持つ。

- クラッカーの一般的な攻撃手順をスクリプトに記述し，複数のセキュリティホールを組み合わせた攻撃を自動的に試みる。
- 侵入に成功したホストを踏み台として更に内部のホストへの侵入を試みる。

具体的には，次のような機能を提供する。

(1) 対象となるサイトに対して擬似的な攻撃を行い，侵入可能性を検証する。

(2) 検査実行モジュールをプラグインとして実現し，柔軟な検査モジュールの追加・変更が可能である。

(3) 検査実行モジュールの収集した情報の他の検査へのフィードバックができる。

(4) 典型的な攻撃手順をシナリオとして定義し，シナリオに沿ってプラグインを実行する。

(5) 攻撃に成功したホストを経由して，更に内部に存在するホストへの検査を行う。

### 3.2 おとり誘導による不正アクセス対策システム

おとり技術は，不正侵入者をおとりサーバへ誘導し，長時間滞在させることにより，不正侵入者の行動を記録した監査証跡(ログ)を取得する技術である。

従来のおとりシステムは，正規サーバ群の中におとりサーバを配置することにより，正規サーバが不正侵入者から不正アクセスされる確率を低減するとともに，不正侵入者がおとりサーバへアクセスすることによってログを取得する。

今回開発したシステムの構成を図2に示す。このシステムでは，不正侵入者が偶然におとりサーバへアクセスする

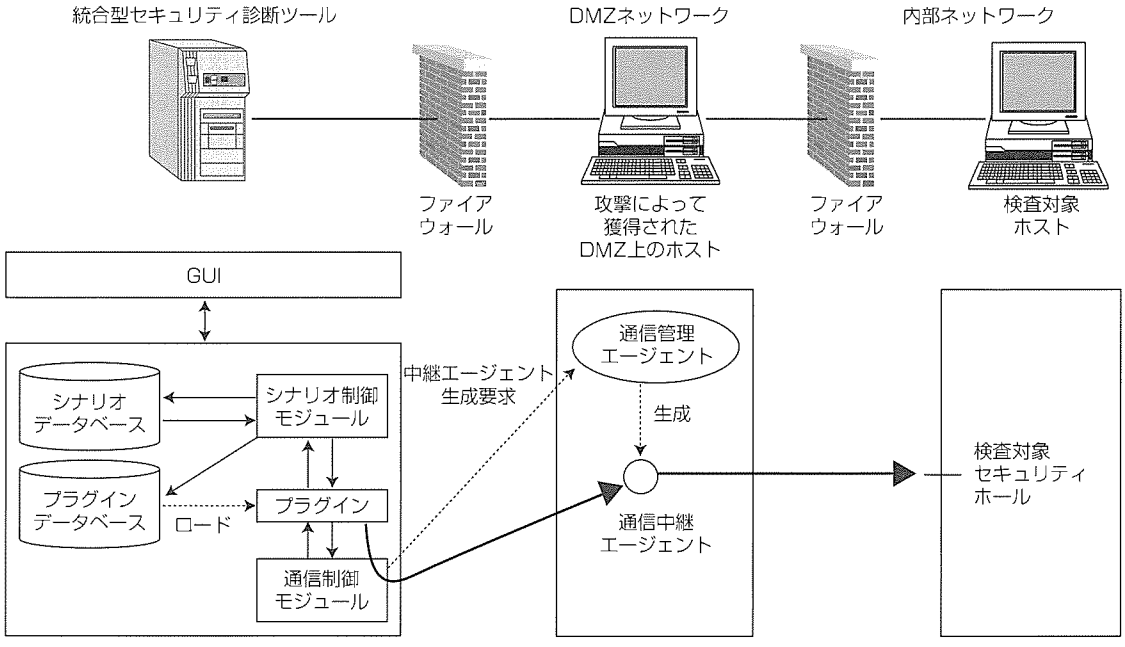



図1．統合型セキュリティ診断ツールのシステム構成

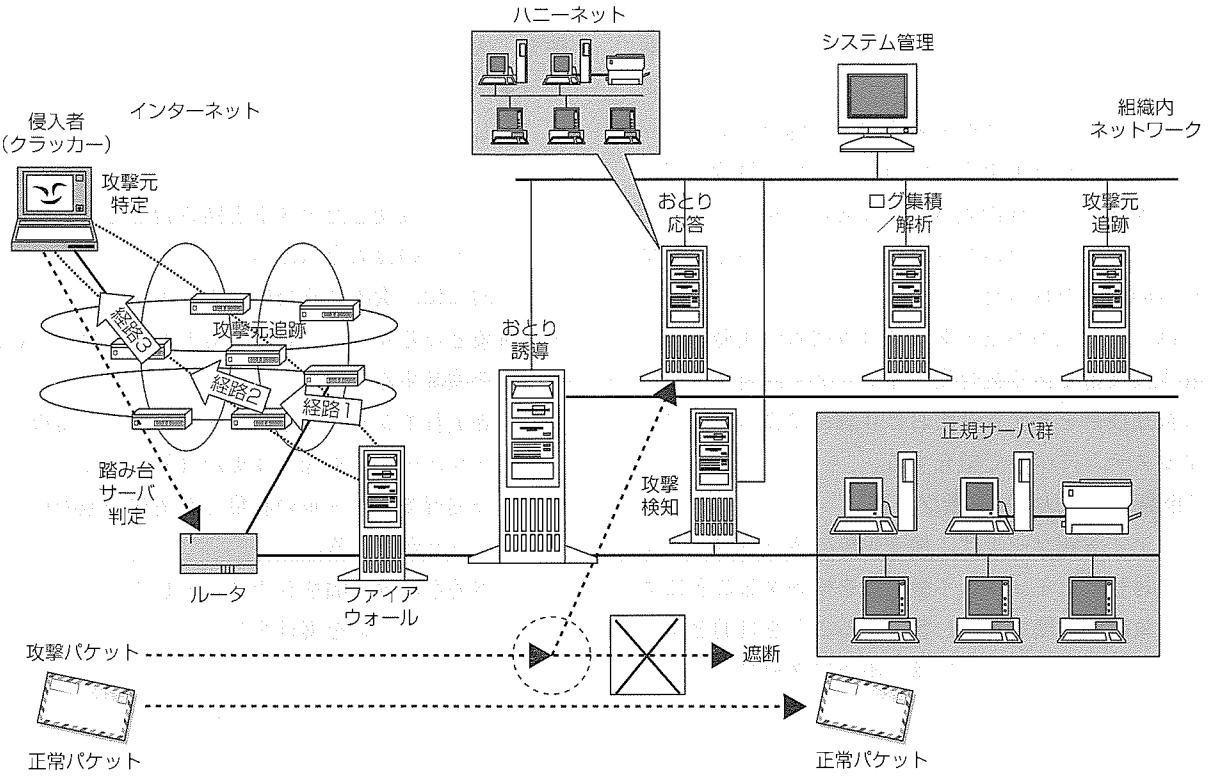



図2．おとり誘導による不正アクセス対策システムの構成

ことを待つだけではなく，不正侵入者の不正アクセスを検知した後，不正侵入者をおとりサーバへ誘導する。これにより，正規のサーバの安全性を保持しながら，侵入者の行動を記録することができる。また，不正侵入者をおとりサーバへ長期間又は繰り返しアクセスさせるための機能を提供することにより，攻撃元の追跡，不正侵入者の目的及び行動の解析などのログ解析を実現する。

以下では，このシステムの機能について説明する。

(1) おとり機能

侵入検知機能によって不正アクセスが検知された後，不正侵入者から送信された攻撃パケットをおとりサーバに誘導する。そして，おとりサーバにおいて，不正侵入者へ適切な応答を返すことにより，対処を実施する時間の導出及び脅威の特定のための監査証跡(ログ)を収集する。

(2) ログ解析

ログの安全な保管を行うために，管理ネットワーク内の1か所のサーバに集積する。そして，集積したログを解析することにより，不正アクセスの検知，攻撃手法の解析，攻撃者の目的の特定等を行う。

(3) 攻撃元追跡

攻撃元の追跡に必要となるネットワーク情報及びホスト情報を取得し，ログとして集積する。集積されたそれらの情報を解析することによって，踏み台サーバを判定し，攻撃経路及び攻撃元を特定する。

## 4. むすび

以上，不正アクセス対策技術について説明し，当社が取り組んでいる不正アクセス対策技術の中から，統合型セキュリティ診断ツール，及びおとり誘導による不正アクセス対策システムについて述べた。

本稿で述べた技術については，既にプロトタイプは終えており，製品化を目指した開発を進めている。

今後は，より高度な不正アクセス対策を必要としている社会重要インフラシステムへ展開していく。

# セキュリティポリシー

青木　尚*

**要　旨**

電子商取引等いわゆるIT革命（情報革命）が情報化・ネットワーク化の進展を加速し，産業や政府活動の多くは，情報システムへの依存性をますます高めている。

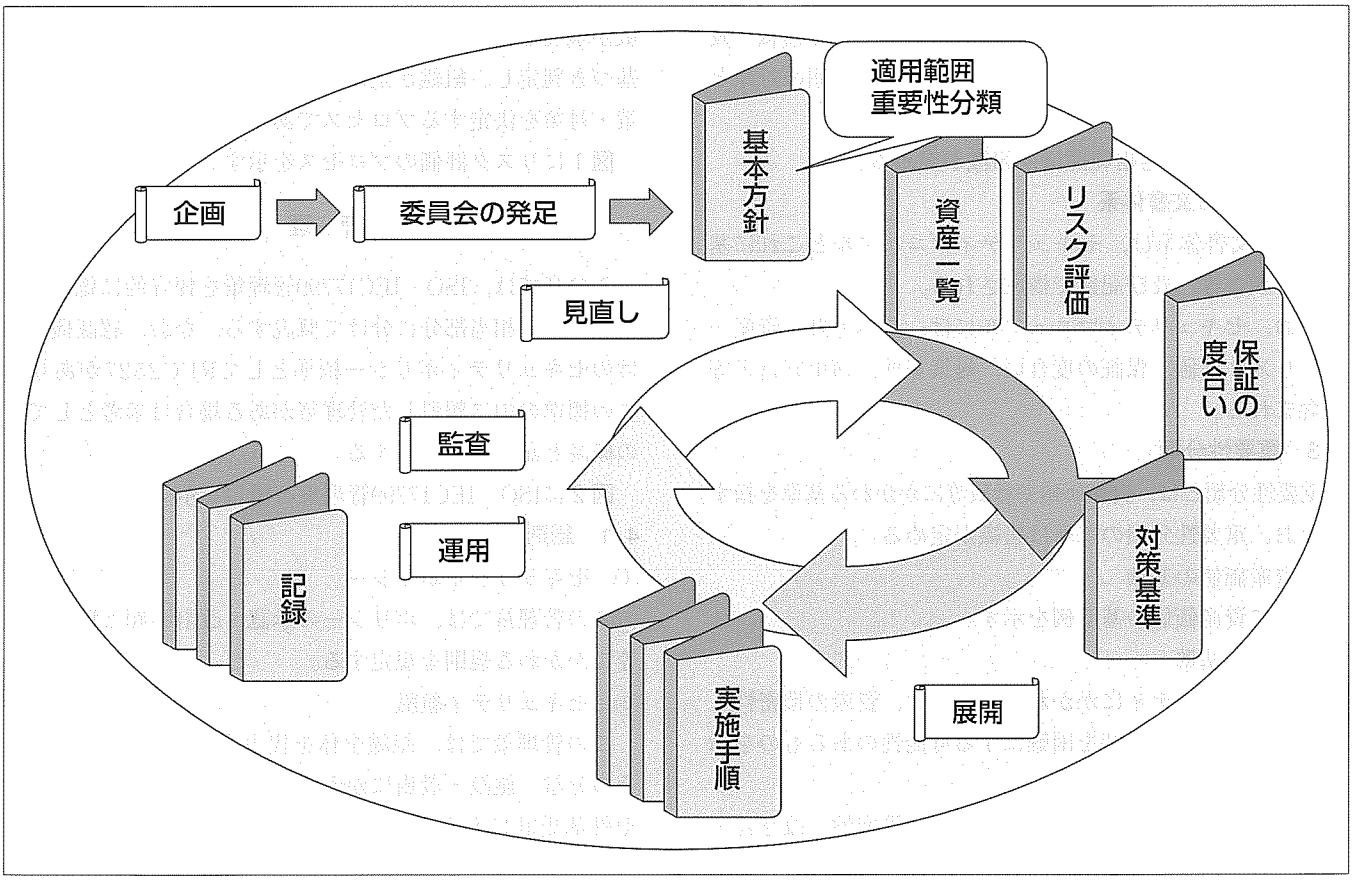
これに伴い，情報システムの安全面や信用面等から，情報システムを支える情報セキュリティの維持・向上が重要になってきた。

事実，コンピュータウィルスや踏み台攻撃等，情報及び情報システムは，その盗用，不正アクセス，改ざん，破壊，又は利用妨害などの脅威に常にさらされており，これに加えて，組織内部者の意図的な脅威についても無視できない。

これに対して，従来までは，入退管理，ウィルス対策，及びファイアウォールやIDS（侵入検知システム）等のシステムで対策してきたが，ここにきて，経営層・管理層の説明責任・危機管理，及び法的準拠性がクローズアップされてきて，組織や体制の下に総合的・体系的な管理を行う標準的なISMS（情報セキュリティマネジメントシステム）の導入が経営的に注目されている。

このような中，日本政府は，ISO／IEC17799（情報セキュリティ管理実施基準）の前身である英国標準BS7799等を参考に，「情報セキュリティポリシーに関するガイドライン」（2000－7）を発行し，省庁のセキュリティポリシー構築施策を展開した。また，金融庁も同様な施策を金融機関に対して行ってきた経緯がある。

現在は，ISMSの運用面の整備が行われており，例えば，㈶日本情報処理開発協会が2002年度以降の本格運用を目標にISMS適合性評価制度を準備している。




**ISMS導入・運用プロセス**

ISMSを導入し運用するには，例えば，情報システム管理部門などがISMSの導入を経営層・管理層に起案し，経営層・管理層の承認に基づいて組織全体の代表からなる委員会を発足し，策定するISMSの委員会決定と経営層・管理層の承認を取り付け，運用管理・見直し等を行うプロセスを経る。

*三菱電機インフォメーションシステムズ㈱

## 1. まえがき

本稿では，ISMSとセキュリティポリシーの概要を説明する。

## 2. ISMSの位置付け

(1) 総合的・体系的なISMS

ISMSは，“情報システム”“設備”の導入に加え，その“利用”“運用”，記録されたデータの“取扱い”，開発するための“基準”，及び紙に記録されたものなど“媒体”や“情報”，並びに情報に接するすべての“人”を網羅して運用管理する総合的・体系的な仕組みとして位置付けられる。

(2) 組織として統一されたISMS

ISMSは，組織の各部門が独自に扱いを判断することがない仕組みとして位置付けられる。

(3) 評価・見直しサイクルを持つISMS

ISMSは，新たな脅威や環境の変化に対してメンテナンスされる仕組みを持つ。

## 3. ISMSの概要

### 3.1 ISMSの適用範囲

例えば，コンピュータ，ネットワーク，ソフトウェア等の情報システム，情報システムに記録されている情報，及びこれらの情報に接するすべてのものが適用範囲の対象となる。

なお，ISMSの適用範囲は，組織が定める。

### 3.2 ISMSの文書体系

ISMS文書体系は，セキュリティマニュアルとこれに基づく手順書等，及び記録で構成される。

なお，セキュリティマニュアルには，基本方針，資産一覧，リスク評価，保証の度合い，対策基準，適用宣言書等が含まれる。

### 3.3 重要性分類

重要性分類とは，資産価値や脅威等にかかわる基準を指す。

なお，重要性分類の基準は組織が定める。

(1) 資産価値の基準

**表1**に資産価値の基準例を示す。

(2) 脅威の基準

情報セキュリティにかかわる脅威とは，資産の機密性・完全性・可用性の維持を困難にする可能性のあるものを指す。

具体的な脅威例として，漏えい(洩)は機密性，改ざん・否認・成り済ましは完全性，システム停止・サービス妨害は可用性に分類できる。

**表2**～**表4**に脅威の基準例を示す。

### 3.4 リスク評価

リスク評価とは，資産の価値，及び資産の脅威とその脅威が現実となる資産のぜい(脆)弱性(弱点)を重要性分類に基づき判定し，組織が定める保証の度合いに基づいて管理策・対策を決定するプロセスである。

**図1**にリスク評価のプロセスを示す。

**表1．資産価値の基準例**

| 基準 | 定　義 |
|---|---|
| 1 | 経営・業務遂行に重大な影響がでる可能性がある |
| 2 | 経営・業務遂行に影響がでる可能性がある |
| 3 | 経営・業務遂行への影響が無視できる |

**表2．機密性の基準例**

| 基準 | 定　義 |
|---|---|
| 1 | 開示された場合の影響が極めて大きい |
| 2 | 開示された場合の影響が大きい |
| 3 | 開示された場合の影響が無視できる |

**表3．完全性の基準例**

| 基準 | 定　義 |
|---|---|
| 1 | 改ざんされた場合の影響が極めて大きい |
| 2 | 改ざんされた場合の影響が大きい |
| 3 | 改ざんされた場合の影響が無視できる |

**表4．可用性の基準例**

| 基準 | 定　義 |
|---|---|
| 1 | システム停止許容時間が数分程度 |
| 2 | システム停止許容時間が数時間程度 |
| 3 | システム停止許容時間が数日程度 |

## 4. 管　理　策

この章では，ISO／IEC17799管理策を便宜的に総則相当部分と細則相当部分に分けて概説する。なお，認証機関向けのセキュリティポリシー標準としてRFC2527があり，この標準の中に類似した管理策がある場合は参考としてその概説と記述例を記述する。

**図2**にISO／IEC17799管理策の構造を示す。

### 4.1 総則相当部分

(1) セキュリティポリシー

この管理策では，ポリシーの承認・改訂手順と周知手順等にかかわる規則を規定する。

(2) セキュリティ組織

この管理策では，組織全体を代表するISMS管理体制とその分掌，施設・設備にかかわる認可プロセス，派遣受けや外部委託にかかわる契約管理等に関する規則を規定する。

**図3**にISMS管理体制の一例を示す。

(3) 財産の分類及び管理

この管理策では，重要性分類の判定と管理責任者の割り付けた資産目録の策定にかかわる規則を規定する。

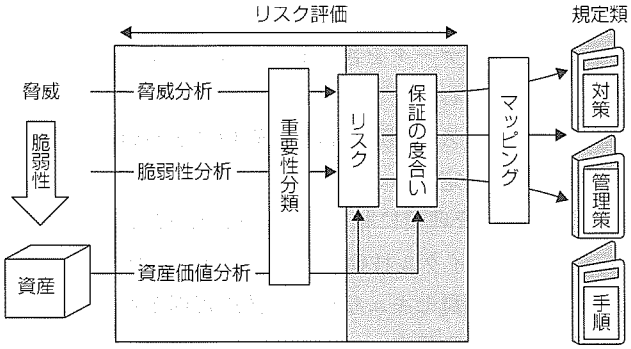



図1．リスク評価のプロセス

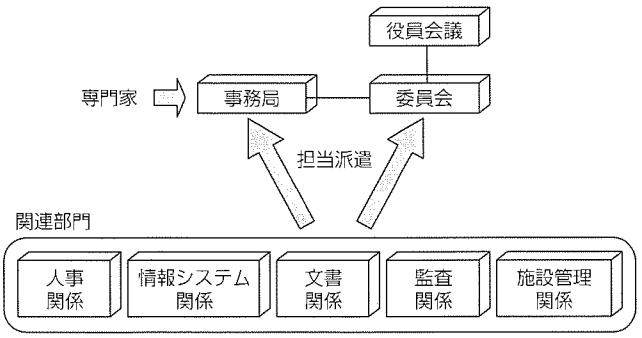



図3．ISMS管理体制例

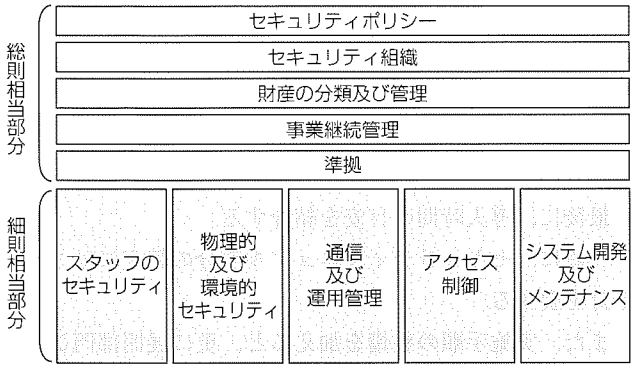



図2．ISO／IEC17799管理策の構造

(4) 事業継続管理

この管理策では，重要なビジネスプロセスの障害に対する復旧計画，及びそのシミュレーション等の保護策を規定する。

なお，この管理策に相当するRFC2527の条項である「4.8危たい(殆)化と災害復旧」では，ハードウェア，ソフトウェア，データ，特に認証機関の秘密鍵の損失・漏えい（洩)等の危殆化やバックアップサイトのセキュアな構築等にかかわる手順及び保護策を規定するとあり，例えば，“本認証機関は，被災事実をホームページ上で公開し，リポジトリ情報は，24時間以内にバックアップデータから復元するか，少なくとも被災1ケ月前までの情報をアーカイブデータから復元する”などが記述例として挙げられる。

なお，この管理策の一部は，“災害復旧計画”又は“事業継続計画”として別に策定され運用される場合がある。

(5) 準拠

この管理策では，知的所有権や個人情報保護を含む法令・契約・標準・監査等の要求事項や義務にかかわる準拠策，及び組織の記録の保護策等を規定する。

なお，この管理策に相当するRFC2527の条項である「2.4解釈と遵法」では，準拠法や紛争解決手続きを規定するとあり，例えば，“本CPS(認証機関運用規程)は，日本法及び政省令に基づき解釈される”などが記述例として挙げられる。

### 4.2 細則相当部分

(1) スタッフのセキュリティ

この管理策では，分掌の定義，資格基準，教育，訓練，問題報告手順，懲戒等の管理策を規定する。

なお，この管理策に相当するRFC2527の条項である「5.3要員管理策」では，要員の経歴・素性確認，トレーニング要件，役割ローテーション等を規定するとあり，例えば，“本認証機関基幹認証システムの操作要員は，過去15年間犯罪を起こしていないことを宣誓する書類に毎年署名する”などが記述例として挙げられる。

(2) 物理的及び環境的セキュリティ

この管理策では，施設・設備にかかわる安全領域の設定と入退管理，設備の窃盗，災害対策，電源・ケーブル配線等の環境セキュリティ，メンテナンス管理，媒体保管・郵便物・印刷物の保護やオフィスの施錠等にかかわる保護策を規定する。

なお，この管理策に相当するRFC2527の条項である「5.1物理的管理策」では，監視設備，ガード設備，ロック設備，トークンを使用したアクセスコントロール，バイオメトリクスを使用したアクセスコントロール，アクセスリストに基づいたアクセスコントロール等を規定するとあり，例えば，“本認証機関は，基幹認証システムを特別な区域に設置し入退管理を行うほか，基幹認証システムおよび当該システムに付帯する電源等の環境設備にアクセス管理システムを装備する”などが記述例として挙げられる。

(3) 通信及び運用管理

この管理策では，施設・設備・システムの変更管理，問題管理手順，職務の分離や複数人管理等の権限分散，運用システムと開発・試験システムの物理的及びアクセス権の分離，システム受け入れ基準，ウィルス等の対策，ネットワークとコンピュータの管理者分離，バックアップポリシー，媒体管理，文書管理，媒体搬送・情報交換管理，廃棄管理等の運用策を規定する。

なお，この管理策に相当するRFC2527の条項である「5.2手続的管理策」では，システム管理者のシステム設定・生成・起動・運用管理，システムセキュリティ責任者

のアカウント管理，システム監査人と監査ファイルの管理など信頼を必要とする役割と義務を規定するとあり，例えば，“本認証機関は，CP(証明書ポリシー)／CPS管理者，証明書ライフサイクルサービス業務管理者，認証システム管理者，監査者の職務を分離し，また，加入者秘密鍵の生成は複数人で行う”などが記述例として挙げられる。

なお，この管理策の一部は，“変更管理規程”“問題管理手順”“事故報告手順”として別に策定され運用される場合がある。

(4) アクセス制御

この管理策では，アクセス管理方針を定め，ユーザー登録・抹消手順，ユーザーパスワード管理，特権管理，診断ポート管理等のアクセス権認可及びアクセス権管理を規定する。また，設備やサービスに対する認可されていないアクセスの防止策や接続時間の制限等のアクセス管理，記録，監視，及び警報手順，又はネットワークの経路制御や分離等の管理策を規定する。

なお，この管理策に相当するRFC2527の条項には「3識別と認証」「5.1.2物理的アクセス」「5.2.3役割別識別と認証」「6.4活性化データ」「6.5コンピュータセキュリティ管理策」「6.7ネットワークセキュリティ管理策」があり，例えば，“本認証機関は，基幹認証システム室に侵入検知システムを設置し，入退に際しては，2人以上の身体的特徴を確認・記録している”“本認証機関が使用するコンピュータシステムはISO／IEC15408レベル2以上に準拠しているものを使用する”“本認証機関は，ネットワークのアクセス制御としてファイアウォールを設置する”などが記述例として挙げられる。

なお，この管理策の一部は，“入退管理規程”“アクセス権認可規程”“アクセス管理規程”“ネットワーク管理規程”として別に策定され運用される場合がある。

(5) システム開発及びメンテナンス

この管理策では，ユーザーデータの消失・変更・誤用にかかわる防止策を規定する。また，プログラムソース，ライブラリ，試験データを含むシステムファイルの保護策として，試験を含む開発システムの認可手順，操作者限定にかかわるアクセス権認可，複数人管理にかかわる操作要領等の管理策を規定する。

なお，この管理策に相当するRFC2527の条項である「6.6ライフサイクル技術管理策」では，開発環境セキュリティ，開発要員セキュリティ，構成管理セキュリティ，ソフトウェア工学規定，フェールセーフ設計などに関して規定するとあり，例えば，“本認証機関は，TSDM(Trusted Software Development Methodology)とSEI-CMM(Software Engineering Institute's Capability Maturity Model)に準拠したシステム開発を行う”などが記述例として挙げられる。

## 5. むすび

最後に，導入時間の目安を紹介する。

一般に，セキュリティマニュアル部分の策定には3～9か月を要する。

また，実施手順の整備を加えると，更に展開部門ごとに2～6か月を要する。

なお，上述の数値は，これまでの経験に基づく目安であり，適用範囲，組織の規模，及び予想外の組織間調整時間などによって変動する場合がある。

## 参考文献

(1) ㈶日本規格協会：ISO／IEC17799（2000-12）
(2) Network Working Group：RFC2527（1999-3）
(3) ㈶日本情報処理開発協会：ISMS適合性評価制度の概要（2001-3）
(4) 情報セキュリティ対策推進会議：情報セキュリティポリシーに関するガイドライン（2000-7）

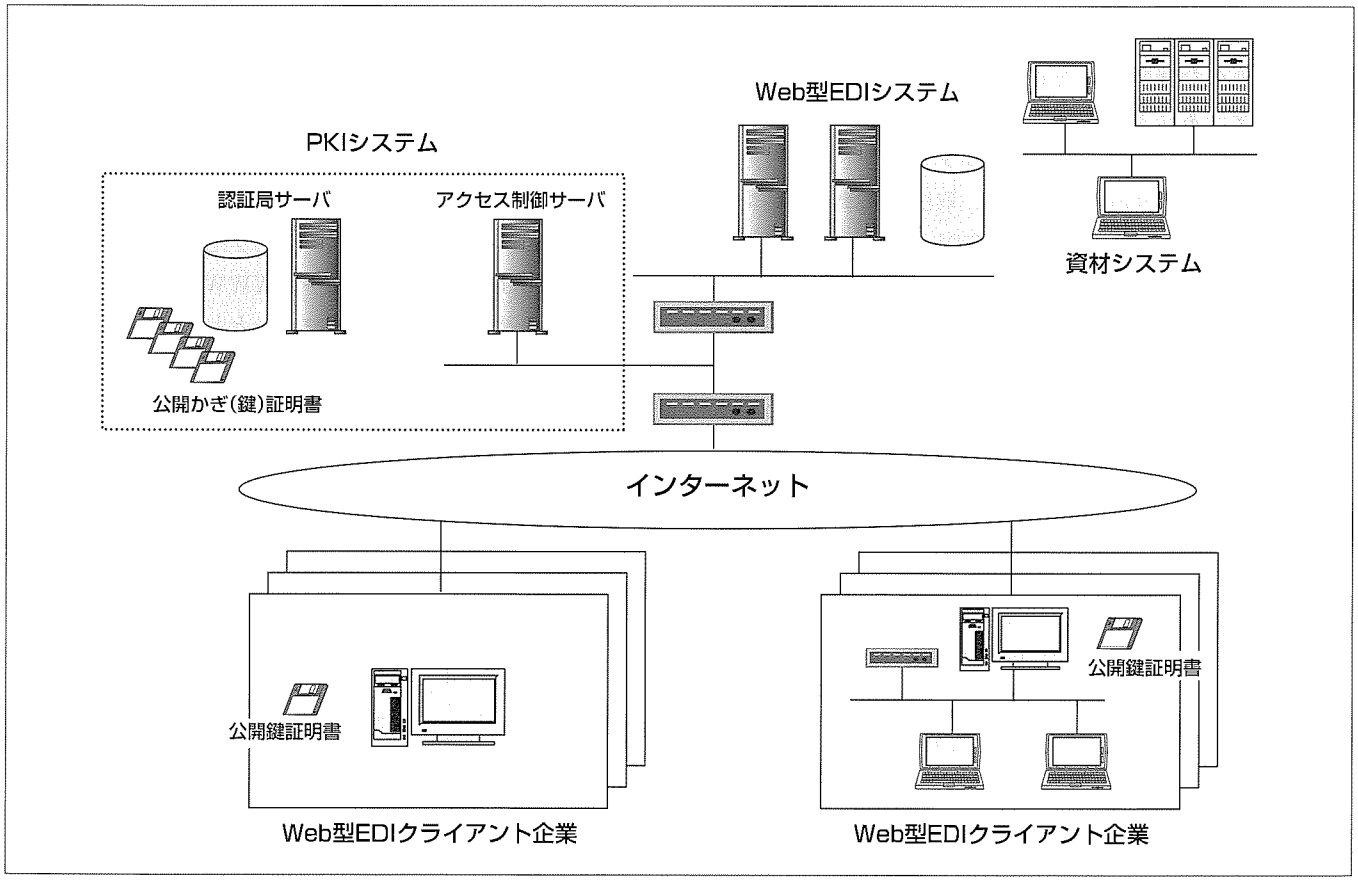
# PKI応用 ―EDIにおけるPKIの適用―

遠藤　淳*
田中　学*

**要　旨**

現在，大手企業の資材部門では，更なる業務効率化のために電子資材取引システムであるEDI(Electronic Data Interchange)の利用率100%を目指した検討を行っており，取引件数の少ない取引先でも安価で簡単にEDIを導入できるインターネットを利用したWeb型のEDIシステムの構築が進んでいる。しかし，その一方で，インターネットの抱えるセキュリティ上の問題に対する対策が課題となっている。このような問題に対する解決策の一つとして，PKI(Public Key Infrastructure)技術の導入が有効である。

本稿では，三菱電機のPKI技術をベースとした製品とその応用形態について，三菱セキュアWebアクセスMistyGuard(注)“TRUSTWEB(注)”を中心とした認証システムと，EDIアプリケーションの連携方法とその効果について述べる。また，PKIシステムの運用にかかわる問題点と対応策について解説する。




**Web型EDIシステムにおけるの応用**

PKIシステムの導入により，インターネットを介して安全にクライアント企業と接続する安価なWeb型のEDIシステムを構築する。これにより，EDIを利用するクライアント企業を拡大し，業務の効率化を図ることができる。

*三菱電機インフォメーションシステムズ㈱

## 1. まえがき

インターネットの普及や電子署名法の施行などにより，PKIを利用してセキュリティを確保するシステム事例が増加している。

本稿では，三菱セキュアWebアクセスMistyGuard "TRUSTWEB"を利用して構築した電子資材取引(EDI)システムへのPKI適用事例を基に，アプリケーションシステム構築におけるPKIの実装と課題について述べる。

## 2. EDIにおけるPKIの応用

### 2.1 旧来のEDIシステムの課題

EDIシステムは，商取引に関する重要な受発注情報を企業間で電子的に交換するシステムである。旧来のEDIシステムでは，資材調達を行う企業と取引を行うサプライヤー側の企業ともにEDI専用のシステム構築が必要であり，ネットワークとして専用線を利用していた。このため，初期導入時と運用時に高額な費用負担が必要となり，費用負担に見合う導入効果が期待できる取引規模の大きい企業しかEDIを導入できないという課題があった。資材調達業務の更なる効率化を図るためには，すべての取引企業とEDIを実現できるシステムが必要となっていた。

### 2.2 Web型のEDIシステム

前節で述べた課題の解決策として，Web型のEDIシステムとインターネットの導入が有効である。企業は，通常利用している一般的なブラウザとインターネット接続設備のみでEDIが利用できる。このため，取引規模が小さい企業でも費用対効果が得られる安価なEDIシステムの構築が可能となる。ただし，インターネットの利用により，新たな課題も発生する。インターネットは特定な2者間を接続する専用線と異なりだれでも接続可能なネットワークであるため，新たに情報セキュリティリスクに関する対策が必要となる。

### 2.3 PKIの構成要素

インターネット経由での利用を前提としたWeb型のEDIシステムにおいて，必要とされるセキュリティ要件のうち，次の4点は特に重要である。

(1) 取引者の認証(成り済ましの防止)
(2) 取引情報の開示対象者以外への秘匿(情報漏えい(洩)の防止)
(3) 取引内容の完全性の保証(改ざん防止)
(4) 取引事実の証明(否認の防止)

これらのセキュリティ要件を，クローズドな仕様に基づく認証・暗号システムによって実現することは可能である。しかし，他のシステムとの互換性を保つことが困難となるため，インターネット上で多くの相手に対して利用を広げていくときの障害となる。これに対してオープンなPKIの公開鍵証明書(以下"証明書"という。)，デジタル署名及び暗号技術に立脚したシステムの場合，様々なプラットフォームで利用可能であり，インターネット上のほぼあらゆる相手が利用可能となる。これらPKI技術を組み合わせて作られるWeb型のEDIシステムのセキュリティ構成要素，又は仕組みとしては，次に挙げるものが必要である(図1)。

(a) 証明書を発行する認証局
(b) 証明書によるサーバ側のユーザー認証システム
(c) 証明書によるサーバ認証と高度暗号通信が可能なクライアントソフトウェア(エンドユーザー側)
(d) コンテンツのデジタル署名及び検証を行うシステム
(e) 統一された認証方式に基づくアクセス制御システム
(f) 発行した証明書の提供，失効証明書の管理を行うシステム
(g) 電子公証サービス局

これらのうち(a)，(b)，(c)，(d)は必す(須)の要素であり，(e)，(f)は大規模なシステムの場合，運用上必要となる要素である。(g)は不特定多数の企業間の電子商取引で必要とされる(電子公証制度は，2000年4月に電子公証法が成立公布されてガイドラインが示され，法的な整備が進められている)。

### 2.4 TRUSTWEBによるEDIシステムへのPKIの適用

#### 2.4.1 TRUSTWEBの機能と適用事例

TRUSTWEBは，Webアプリケーションシステムに PKIを適用するためのパッケージソフトウェアであり，以下の機能を実現する。

(1) 電子証明書によるクライアント認証とサーバ認証
(2) サーバ-クライアント間の高度暗号通信
(3) WWWサーバ(コンテンツ)のアクセス制御

TRUSTWEBは，通信経路中にWWWサーバとブラウザから見て透過的に動作するプロキシとして導入される。これにより，認証，高度暗号化通信，及びアクセス制御をWWWアプリケーション側から分離した形で一元管理し運用できるため，Webアプリケーションシステムの構築が容易となる。

TRUSTWEBは，高度暗号通信方式としてインターネットで広く利用されているHTTPS(Secure Socket Layer：

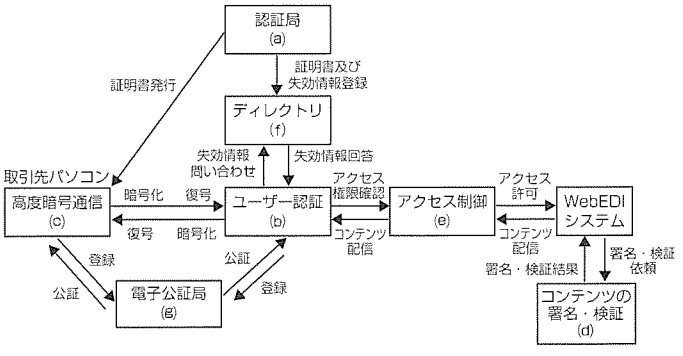



図1．Web型EDIシステムにおけるPKIの構成要素

SSL)，及び三菱電機の開発した世界最高水準の強度を持つ共通鍵暗号MISTYを使用する暗号化HTTP(MISTYで暗号化された情報をHTTP上に乗せて流す方式)の二つの方式をサポートしている。これにより，利用企業のネットワーク構成やセキュリティポリシーに応じてクライアントごとに二つの方式を使い分けしたシステム構成とすることができる。SSL方式とした場合は，ブラウザのみで専用クライアントソフトウェアが必要ないため，クライアントの環境構築が容易となる。一方，MISTY方式(専用クライアントソフトウェア使用)では，強い暗号強度とHTTPに対するより高度な透過性が実現される。

### 2.4.2 TRSUTWEBのEDIシステムへの適用事例

三菱電機では，家電から宇宙，防衛と事業分野が多岐にわたっており，千社を超す企業と資材取引を行っている。システムにおける取引先企業とのセキュリティレベルも事業分野に応じて要求レベルが異なる。このため，EDIシステムにTRUSTWEBを導入して，展開が容易なSSL方式とMISTY方式を使い分けたシステムの運用を行っている。

また，新たに関連会社と資材情報を共有化して三菱電機グループ全体として資材調達の効率化を目指したWeb型の情報共有システムを構築したが，TRUSTWEBにアクセス制御情報を追加するだけで容易にPKIベースのセキュリティ機能を実装することができた(図2)。さらに今後，電子商談システムや指名公開入札システムでのTRUSTWEB利用も検討されている。

### 2.4.3 ディレクトリサーバとの連携

EDIシステムでは，取引先ごとに開示されるコンテンツや利用できるトランザクションが異なるが，さらに，アクセスした時点で取引先に与えられている権利や取引の状況などに応じて複雑な制御ルールに基づいて動的に作成され提供されるコンテンツもある。TRUSTWEBのアクセス制御権管理は，静的なコンテンツにのみ対応した枠組みとなっており，アプリケーション寄りの動的なコンテンツのアクセス制御を行うには不十分な面があった。このため，Webアプリケーション側で認証情報に対応するコンテンツ制御のための情報を別途保持しなければならず，複数のWebアプリケーションを構築した場合，一つの取引先に対する制御情報であっても，Webアプリケーションごとに分散保持しなければならないという問題があった。

この問題に対して，TRUSTWEBでは，Webアプリケーションの複雑なコンテンツ制御に必要な制御情報をディレクトリサーバに集中して管理し，必要に応じてWebアプリケーションがTRUSTWEBのユーザー認証情報をキーにしてディレクトリから情報を取り出して利用できる機能をサポートした。このシステムは図3のような構造になっている。

処理の流れとしては次のようになる。まず，ユーザーの要求はいったんTRUSTWEBでPKIベースの認証が行われる。このとき，暗号通信文は復号され平文に戻されるとともに，改ざんや成り済ましのチェックが行われる。

TRUSTWEBは，認証結果に基づいて個々の要求にユーザー識別情報(ID＋パスワードなどあらかじめ登録された文字列)を付加する。この要求がWebアプリケーションに渡されると，アプリケーションはTRUSTWEBが付加したユーザー固有の識別情報を取り出し，それをキーとしてディレクトリサーバにコンテンツ制御情報(ユーザーが持っている実行権限やロール情報)を要求する(これによってシングルサインオンが可能となる)。

ディレクトリサーバはコンテンツ制御情報をWebアプリケーションに返し，それに基づいてWebアプリケーションが動作を決定する。

TRUSTWEB側のユーザー識別情報は，定期的にディレクトリサーバ上のデータと同期がとられるようになっている。認証時にTRUSTWEBからディレクトリサーバに直接コンテンツ制御情報を取りに行かない理由は，DMZに置かれるTRUSTWEBからイントラネット内のディレクトリサーバへユーザー要求の延長で直接アクセスしない(でき

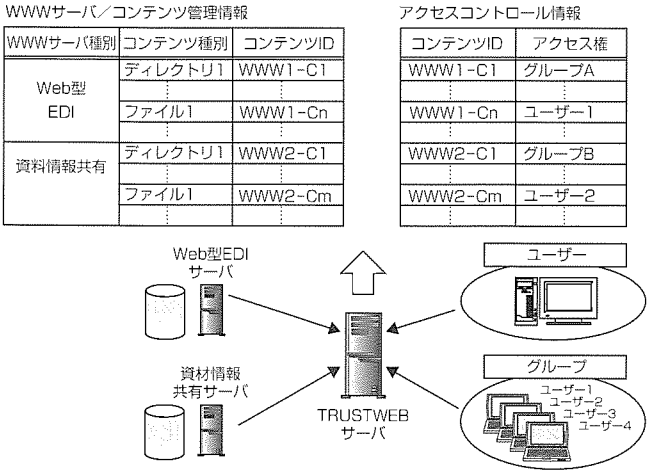



図2．TRUSTWEBのアクセス制御情報管理の仕組み

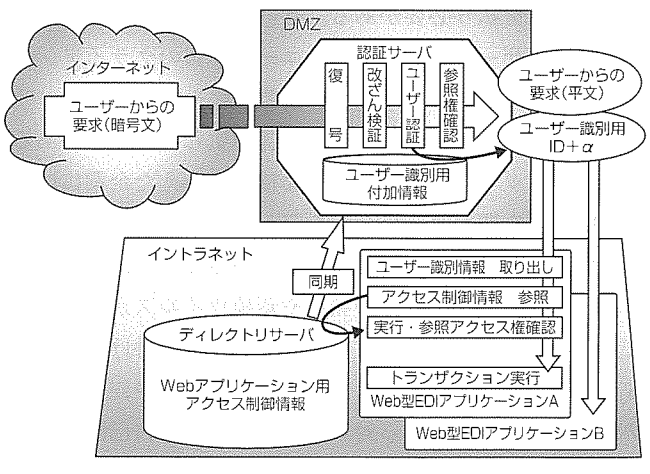



図3．Webアプリケーションと認証システムの連携の仕組み

ない)ようにするためで，セキュリティをより高めるためにこのような方式としている。

また，不正なユーザーからのWebサーバへのアクセスに対する防御，相手に対する警告の発信などはTRUSTWEBが保持する静的なアクセス制御情報に基づいて行うようになっており，Webサーバやディレクトリサーバに負荷を掛けずに処理できるようになっている。

## 3. PKIのシステム運用における課題

三菱電機の事例のように資材業務の効率化を目指し取引企業とより広範囲な業務システムにおいてPKIを適用していく場合，運用面で考慮すべき事項が幾つかある。

ここでは認証に関係する問題に絞って述べる。

### 3.1 認証対象レベルの多様化への対応

資材取引では，初回取引の企業，取引実績のある企業，企業の規模などによって必要な認証対象のレベルが異なってくる。例えば初回取引の場合，会社単位(又は代表権のある個人に対して)で識別できればよく，せいぜい1枚の証明書があればよいが，取引が拡大し，より複雑かつ多くの取引を行うようになると，会社単位から取引する部材を担当している部署単位での認証，特定の決済権限を持つ者とそうでない者の識別など，より細分化されたレベルでの認証が必要となるケースもある。このように，認証すべき対象のレベルは時間の経過とともに変化していくため，発行する証明書とアプリケーションで要求される認証対象レベルの変更を的確に対応付けられるよう，あらかじめ認証ポリシー(CP)を策定して，複数の認証レベルの証明書の発行が安全に実施できるよう認証局システムを構築しておく必要がある。これによって認証対象レベルの変更時の混乱や誤りを防ぐようにすべきである。

### 3.2 認証クライアントのセキュリティ

インターネット上で特定多数を取引相手にする以上，ユーザー認証のかなめ(要)となる認証・暗号通信クライアント(この場合特にブラウザを指す)のセキュリティ確保には十分な注意を払う必要がある。せっかく高度な暗号と認証技術でユーザーを識別しても，ユーザー側のクライアントがハッキングされていた場合，情報漏洩や成り済まし，サーバのウイルス感染など様々な被害が生じるおそれがある。インターネット取引でこのような損害を与えた企業には損害賠償責任を問われる場合もあるが，ユーザー側の意識は十分に高いとは言えず対策も遅れていることは，近年のホームページ書き換え事件の頻発や新種ウイルスが出るたびに大きな被害をもたらしていることからも裏付けられている。サーバ側へのウイルス対策ソフトウェアや侵入検知ソフトウェアの導入による対策はもちろんだが自己防衛だけでは不十分であり，各企業の取引レベルに応じて，①ワクチンソフトウェアの導入やウイルス検査エビデンスの提出などを義務付ける，②ブラウザやOSに対するセキュリティ対策パッチを適用しているか確認する，③高度な権限を持つ証明書は比較的短い有効期限とするなど，エンドユーザー側のセキュリティ向上も含む防衛策をとっていく必要がある。またこれらは，被害が出たとき又はそのおそれが生じたときの対策も含め，認証ポリシー(CP)や認証実施規定(CPS)又はCP／CPSから策定される具体的施策リストに盛り込まれるべきものである。

### 3.3 互換性の問題

PKI技術はオープンであると述べたが，同時に急速に拡大，詳細化，多様化が進んでいる技術でもある。このため基本的な仕様の互換性は維持されているものの，メーカーや開発時期などによって互換性の低い新しい機能や仕様が付け加えられている製品もあるのが現状である。このため，特にマルチベンダーを重視するシステムでは，証明書の発行内容や形式，又は暗号機能などに関して，十分な検討と互換性検証を行っておく必要がある。三菱電機の事例では，認証局，認証システムを1社に統一した上，ブラウザなどの互換性について十分に検討を重ねており，このような問題は生じていないが，今後の新しいPKIシステムの登場などに十分注意を払っていく必要がある。

## 4. PKI導入のメリット

PKIをアプリケーションシステムのセキュリティ基盤として採用することのメリットは，次の三つに集約される。

(1) 基本技術＋応用技術が確立していること

(2) 技術がオープンになっていて互換性があること

(3) インフラ(ブラウザ)をだれもが入手し利用できること

特に(3)によって，導入コストを抑えつつ，短期間で高度なセキュリティ付きの大規模なPKIシステムを構築することが可能となる。

## 5. むすび

電子署名法の施行や“電子政府”“電子自治体”などの行政システムでのPKIの利用拡大により，2002年以降，アプリケーションシステムとPKIの連携や異なるPKIシステム間の相互乗り入れニーズがますます高まってくると想定される。三菱電機でもEDI用に取引企業に発行した証明書の多目的な活用を検討している。

今後，PKIのメリットを最大限に活用できるようにするためには，検証サービスや電子公証サービス等の社会的なセキュリティ基盤との連携や，リアル社会の印鑑やサインと同様に低コストで使いやすく様々なアプリケーションで利用できる仕組みが必要である。TRUSTWEB等のPKIパッケージソフトウェアの開発及び機能強化などにより，PKIのアプリケーションへの適用や実装を更に高度に，そして容易にしていかなければならない。

# 電子政府・電子自治体への取組

並河　誠*
高橋　浄*

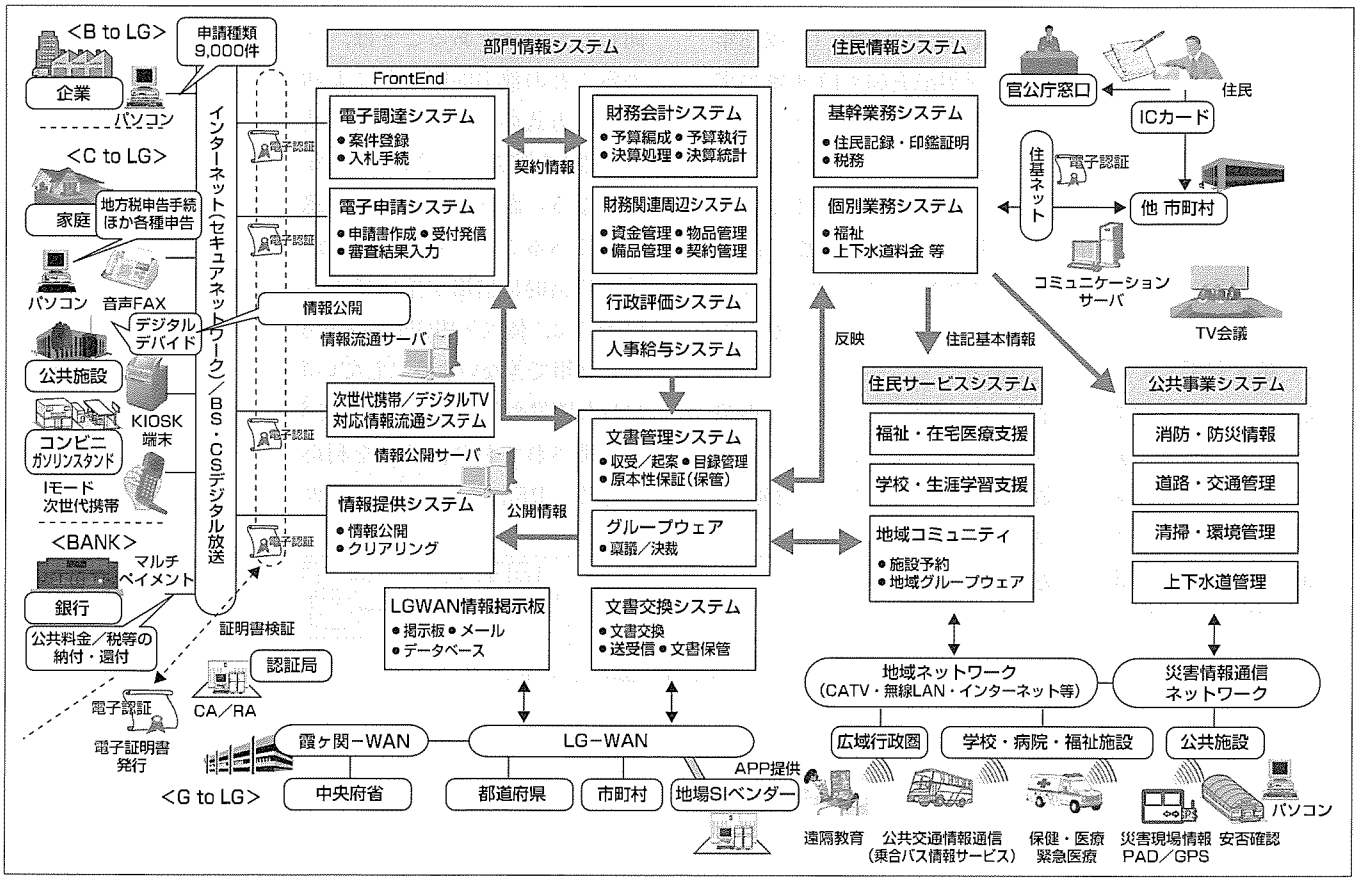
**要　旨**

政府は我が国が世界最先端のIT国家となることを目指して様々な施策を実行中であり，電子政府・電子自治体関連は予算編成の重点分野にも組み入れられている。

下図は，自治体を例にした行政の電子化全体像を描いたものである。狭義の意味での電子自治体は電子申請，電子入札ととらえられているが，広義で考えると，住民情報システム，部門情報システム，住民サービスシステム，公共事業システムと大きな広がりを持っている。現在の政府の施策の中では，電子申請，電子入札に重点が置かれているため，三菱電機も電子申請システムを第一ターゲットとして取り組み始めている。

本稿では，第一ターゲットの電子申請システムを中心に，電子政府・電子自治体に対するこれまでの当社の取組を紹介する。

2章では，現在までの国の動向，今後の計画について，概要を紹介する。3章では，電子認証基盤として実用化されているPKI(Public Key Infrastructure)方式の概要を説明する。4章では，当社の考える電子申請システムの実現機能，認証局の構成について説明する。5章では，電子自治体展開へ向けての当社の取組の例として，ASP(Application Service Provider)とiDC(internet Data Center)と組み合わせたシステムについて概要を紹介する。




**自治体における行政の電子化構築全体イメージ図**

この図は，行政全体の電子化をイメージ化したものである。大きく分類すると，基幹システムと呼ばれる"住民情報システム"，各部門ごとで利用される"部門情報システム"，住民の方々が利用する"住民サービスシステム"，公共事業関係を管理する"公共事業システム"に分かれる。
当社は"部門情報システム"の電子申請システムを第一ターゲットとして，行政の電子化へ取り組んでいる。

*システム統括部

## 1. まえがき

我が国でのインターネット利用者数が4,700万人を超える現在，電子政府・電子自治体実現への社会的条件が徐々に整ってきているととらえることができる。さらには，バブル崩壊後なかなか回復の兆しが見えてこない日本経済の中で，厳しい財政状況の政府・自治体にとっても，IT革命を推進し活力ある発展が可能となる社会を形成することが喫緊の課題である。韓国，シンガポールを始めとするアジア諸国のIT化・ブロードバンド化に遅れをとってきた我が国も，政府の施策に基づき，官民一体となって世界最先端のIT国家の形成に取り組み始めている。

本稿では，三菱電機がこれまで実績を積み上げてきた電子政府に対する取組，及び今後の電子自治体への展望について，電子申請システムを中心に紹介する。

## 2. 国の動向

政府は，我が国が世界最先端のIT国家となることを目指し，平成12年7月のIT戦略会議，IT戦略本部の創設に始まり，IT基本法の施行(平成13年1月)，e-Japan戦略(平成13年1月)，e-Japan重点計画(平成13年3月)，e-Japan2002プログラム(平成13年6月)と次々と施策を打ち出している。また，経済財政諮問会議「骨太の方針」(平成13年6月)でも予算編成の重点分野に「世界最先端のIT国家の実現」が組み入れられ，官民を挙げてIT化施策を推進中である。

さきのe-Japan重点戦略で「電子政府の実現」として挙げられている項目については，その後の諸施策では，「行政情報の電子的提供」「申請・届出等手続の電子化」「政府調達の電子化」「地方公共団体の取組支援」などの「行政の情報化」というキーワードで具現化され，中央府省から先行して順次着手している状況である。

既に，経済産業省では，平成13年11月から汎用電子申請システム(ITEM2000)によって一部の手続においてインターネットを利用した電子申請が可能となっている。2003年を目標にほぼすべての手続(国の手続約11,000件オンライン化，地方公共団体の手続約5,000件オンライン化条件整備)で実現していく計画である。また，国土交通省では，平成13年10月から一部の直轄事業についてはインターネットを利用した電子入札が可能となっており，今後対象事業を順次拡大していく計画である。

これらの電子政府の実現は，利用者(住民・企業等)の利便性の向上を目指すことが第一の目的ではあるが，それとともに，行政サービスの質的向上，行政の透明性の実現，行政事務の効率化を促進することとなる。

## 3. 電子認証基盤

電子申請システムは，住民・企業が従来紙で行っていた申請・届出等の手続を，インターネットを利用して電子的に行えるようにするものである。申請者は，官公庁へ申請書を取りに行くのではなく，申請書様式を電子データとしてダウンロードする。申請書を手書きで作成するのではなく，電子データとして申請書を作成する。申請書を郵送又は官公庁へ持参するのではなく，インターネットを利用して送信する。これらがすべて自宅又はオフィスのパソコンからできるようになるシステムである。

これらを実現するためには，認証という仕組みが必要となってくる。インターネット(ネットワーク)を利用した申請では，相手の顔が見えないため，申請を行っている人が本当にその本人であるかを確認することが必要である。また，送信されてきた申請書が改ざんされていないことを確認する必要がある。これらを確認するための基盤として，これまでPKI方式が実用化され，普及してきている。PKI方式とは，公開かぎ(鍵)・秘密鍵の二つの鍵ペアを生成し，本人しか知り得ない秘密鍵をキーとして署名文を作成し，一般に公開している公開鍵で署名文を検証することによって相手方が本人であることを確認する方式である。鍵を公開しても安全であることは，公開鍵から秘密鍵を計算で求めることの数学的困難さによ(拠)っている。

PKI方式の場合には，相手方の署名の正当性(公開鍵の正当性)を確認するために，第三者機関である認証局が必要となる。認証局は，本人確認のための証明書を発行する機関であることから，信頼を求められるものであり，社会的・経済的に信用が確保できる機関である必要がある。現段階では，個人・組織の秘密鍵をICカードに保存し，所有者しか利用できないようにしているのが一般的である。認証局には公開鍵や失効情報がだれでも利用することができるように公開されており，それを利用して署名の検証を行うことになる。PKI方式による認証の仕組みの概念を**図1**に示す。

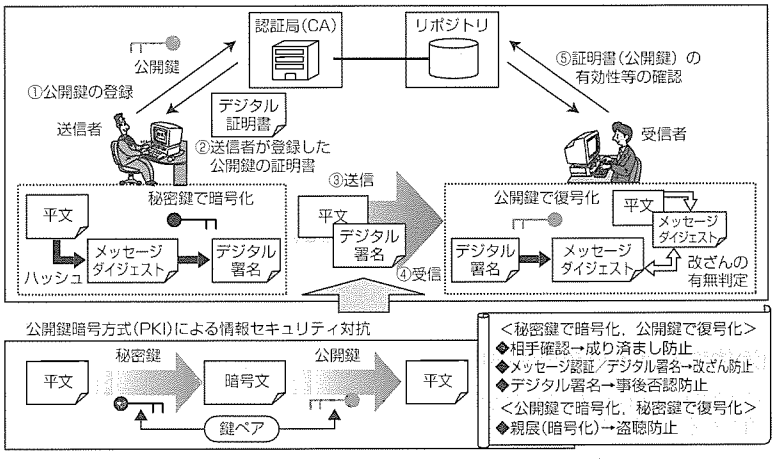



**図1．公開鍵暗号(PKI)方式の仕組み**

このPKI方式による公的認証基盤として，GPKI(Government PKI)，LGPKI(Local Government PKI)，公的個人認証基盤を構築することが計画されている。

GPKIは，“政府認証基盤”のことであり，ブリッジ認証局及び府省認証局で構成され，府省の組織認証を行う。ブリッジ認証局とは，複数の府省認証局と民間認証局等との信頼関係を仲介することによって府省認証局同士，又は府省認証局と民間認証局とが個別に相互認証することの煩雑さを解消するための認証局である。

LGPKIは，“地方公共団体における組織認証基盤”のことであり，各都道府県の認証局などで構成され，各地方公共団体の組織認証を行う。LGPKIの基本方針としてLGWAN(Local Government Wide Area Network)の認証基盤を利用する形態とすることとなっている。GPKIのブリッジ認証局とも接続される計画である。

“公的個人認証基盤”は，全国の住民を対象に個人認証を行う。個人認証については，住民基本台帳と密接なかかわりがあるため，総務省の「地方公共団体による公的個人認証サービスのあり方検討委員会」(平成13年8月中間報告)等の検討結果を待つ必要がある。

これらの認証基盤において，現在提案が進められている中央府省における電子申請システムでは，次の種類の認証機能を利用する。

(1) 申請者の本人確認

申請者の本人確認は，GPKIのブリッジ認証局と相互認証する認証局が発行する証明書(申請者証明書)を使った署名の検証及び証明書の有効性確認を行う。

(2) 官職の本人確認

官職の本人確認は，認証局が発行する証明書(官職証明書)を使った署名の検証及び証明書の有効性確認を行う。

(3) 文書の非改ざん確認

文書の非改ざん確認は，署名に含まれるダイジェストと送付されてきた文書のダイジェストを比較することによって行う。

## 4. 三菱電機の考える電子申請システム

電子政府における電子申請システムの機能の概要を**図2**に示す。

電子申請システムの構成は，申請者が利用する「民側機能」と官公庁職員が利用する「官側機能」及び「認証局機能」に分けることができる。民側機能は「①申請系」「⑤公文書受信系」の二つに分類することができる。官側機能は「②受付系」「③審査・決裁系」「④発行系」の三つに分類することができる。これらは，現在総務省において検討中である「汎用受付システムの基本仕様」(平成13年10月中間報告)に沿ったものとしていく計画である。それぞれの機能は**表1**のとおりである。

また，電子署名法(平成13年4月施行)に基づいて本人確認，非改ざん確認を行う認証局に必要とされる機能構成は**図3**のとおりである。

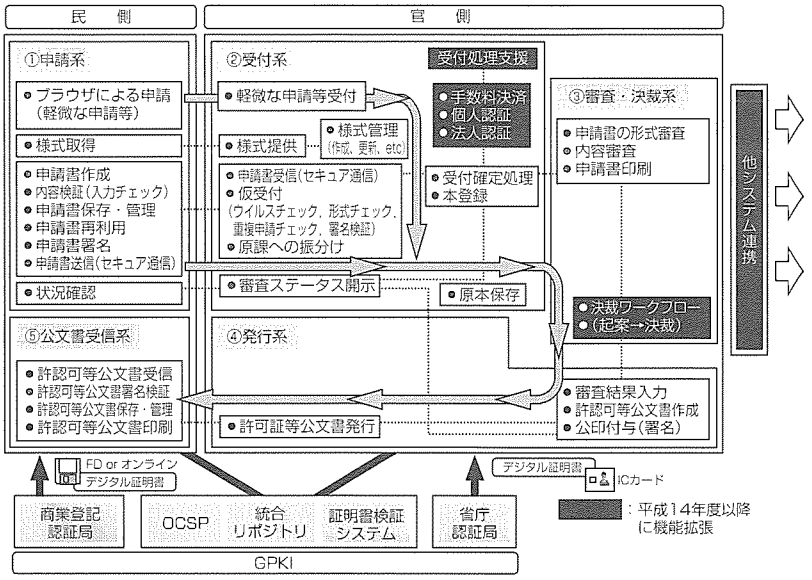



図2．電子申請システムの構成

表1．電子申請システムの機能

| 機　能 | 説　明 |
|---|---|
| ①申請系 | 申請者による申請書の作成と官側システムへの送信を行う機能。<br>政府認証基盤対応での申請(通常申請)と，ユーザーID／パスワードレベルでの認証を行う軽微な申請(簡易申請)の二つの申請形態を提供。 |
| ②受付系 | 申請者から送信された申請データの受信処理を行い，本人確認，非改ざん確認をチェックした上で受付の確定までを行う機能。 |
| ③審査・決裁系 | 受け付けられた申請データに対し，起案し決裁を行うまでの機能。 |
| ④発行系 | 受付確定後の受付確定通知や審査完了後の審査完了通知，許認可等公文書のデータを申請者から要求に応じ，発行(送信)する機能。 |
| ⑤公文書受信系 | 官側システムから受付確定通知や審査終了通知を受信したり，許認可等公文書に対し，本人確認，非改ざん確認をチェックした上で受信処理を行う機能。 |

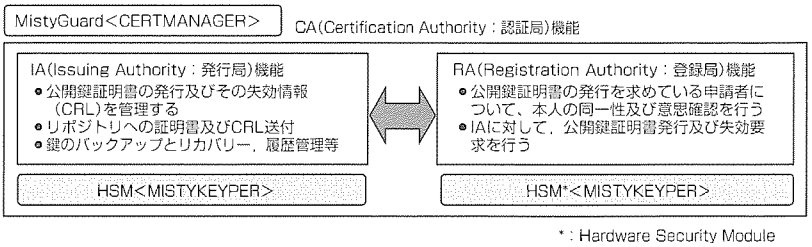
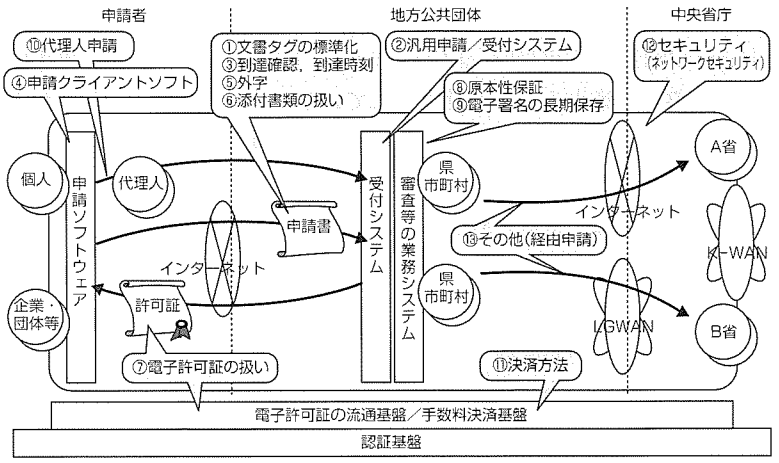



図3．認証局の構成

認証局(CA)には，IA(発行局)とRA(登録局)の二つの機能がある。RAは，証明書の発行要求に対して申請内容などから本人の同一性及び意思確認を行い，証明書を発行してよいと判断された場合は，IAに対して証明書発行要求をする。IAは，証明書を発行する以外に，証明書がもはや信用できない種々の事象が生じたら，証明書を失効させ，CRL(証明書失効リスト)を発行する。

認証局自身の秘密鍵は，決して外部に漏れてはならないものであり，ハードウェア的に耐タンパ性(不当な手続きによってデータを取り出そうとした場合にデータが消滅するなどの防御措置が採られていること)が確保されたシステムである必要がある。当社では，CERTMANAGER，MISTYKEYPERを活用し，GPKI対応の認証局を実現している。

電子申請システムにおいては，今後国から指針等が示されることも考慮しつつ，図4に挙げる技術的課題を解決していく必要がある。



(地方公共団体行政サービスオンライン化促進協議会：e-自治体協議会プラットフォーム委員会より)

図4．電子申請システム構築の共通技術課題

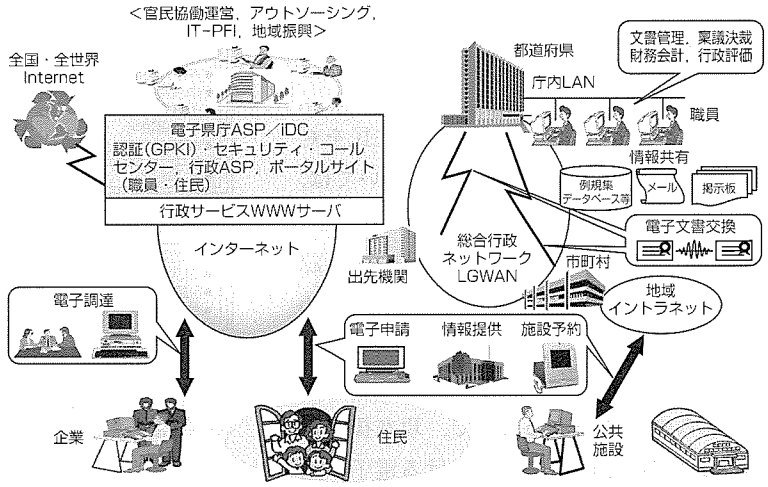



図5．ASP／iDCへの展開

## 5. 電子自治体展開への取組

自治体と中央府省では予算規模が異なるため，これらのシステムを自治体へ展開していくためには，価格的に自治体の予算規模に合わせたシステムを指向していく必要がある。近年注目されているASPやiDCは，このための一つの解決策となり得る。ASPとは，従来のソフトウェアの提供形態(物の提供)とは異なり，ネットワーク経由で業務ソフトウェアなどのアプリケーションの機能を提供する形態である。ユーザーは，パソコンがあれば，ネットワーク経由で最新のアプリケーションを低コストで利用できる。iDCとは，インターネットサーバの維持管理サービスを総合的に提供する。情報化投資削減のアウトソーシング手法として注目されている。

図5に示す形はASPとiDCを組み合わせた一つの構成例で，複数の自治体が一つのシステムを共有する形で，情報システム業務をアウトソーシングすることができる。電子申請システムを電子県庁ASP／iDCに導入し，県及び県内市町村が共同でこのシステムを利用する。この方式で，自治体側は，初期コスト削減，運用職員の負荷削減，24時間365日サービスの提供などの様々なメリットを受けることができる。現在，総務省で検討されている「汎用受付システムの基本仕様」でも，共同運営方式という位置付けで検討を進めている。

## 6. むすび

以上，当社の電子政府に対するこれまでの取組，電子自治体展開への取組について概要を紹介した。このような最先端のシステムは，技術革新のスピードが速く，常に最新の技術を取り入れていく必要がある。今後の2003年までに電子政府の実現，それ以降の電子自治体の実現に向けて，タイムリーに新技術を取り入れ，住民・企業にとって利便性の高い最適なシステムを構築していく所存である。

# 薄型・小型指紋センサ

佐藤行雄* 近藤潤一**
岡本達樹* 坂下徳美***
橋戸隆一*

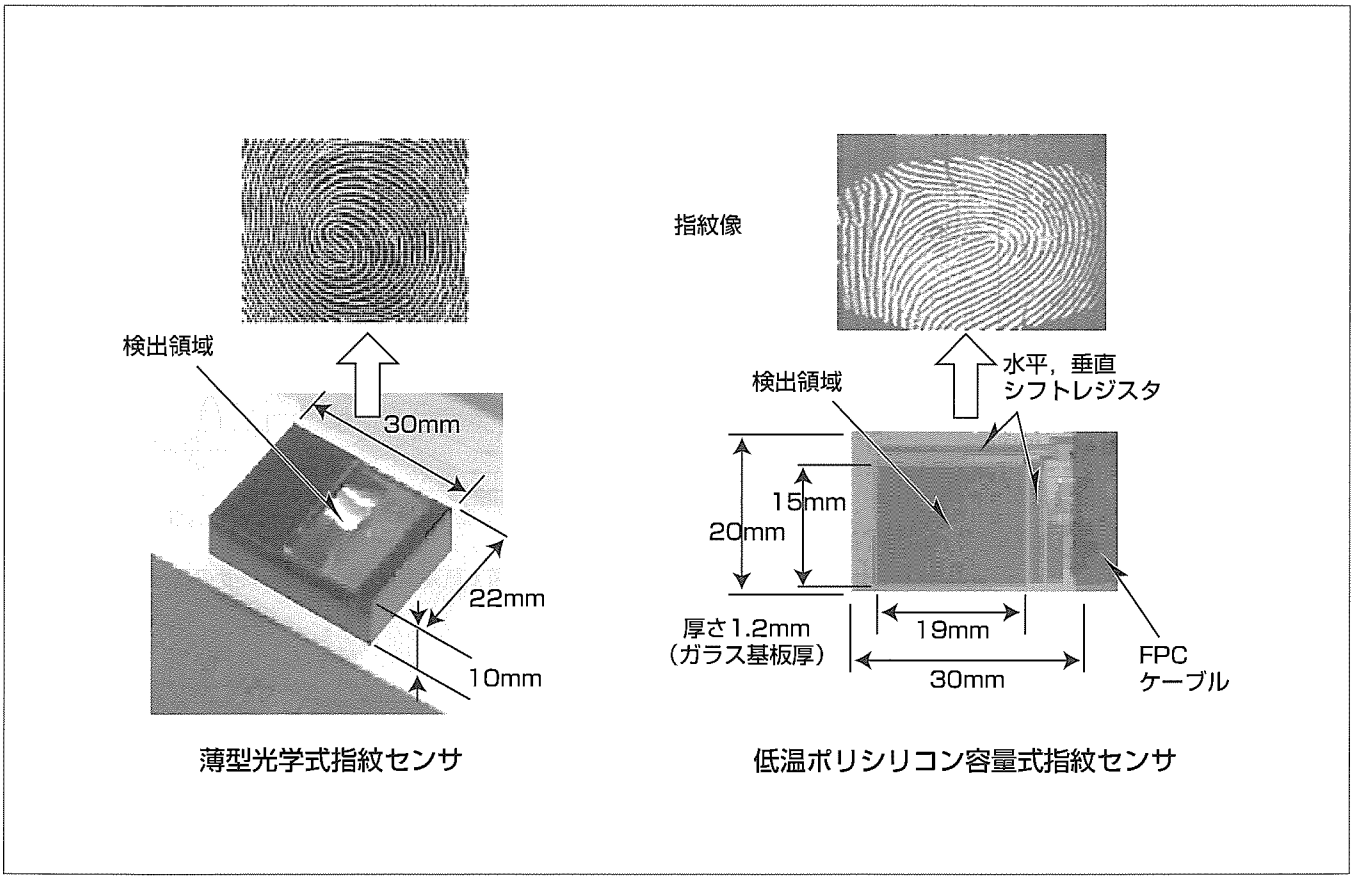
要 旨

近年，情報通信技術の急激な発展により，パソコン，携帯情報端末(携帯電話，PDA(Personal Data Assistant)等)を使って，場所を選ばず簡単に必要な情報の入手，お金のやり取りを含む決済を行える時代がやってきた。反面，これらの機器におけるセキュリティの確保が大きな問題であり，暗証番号，カード等の認証手段に対し，指紋も加えた複合的な手法により，簡便でかつ比較的信頼性の高いセキュリティシステムを構築したいという要求が高まっている。

一方，従来の指紋センサでは，センササイズでこれらの情報機器に対し適用が難しい場合がある。このような観点から，薄型・小型の光学式指紋センサ，及び先端液晶の製造技術である低温ポリシリコン化薄膜トランジスタ(TFT)技術を適用した容量式指紋センサを開発した。

光学式指紋センサはノート型パソコン等への組み込みを一つのターゲットとしており，厚さ10mm，長さ30mm，幅22mmでありながら，性能面では検出領域18mm×12mm，解像度50μm，ひずみ2%以下と，指紋センサとして必要にして十分な機能を実現している。

一方，低温ポリシリコン方式容量式指紋センサは携帯電話，PDA等小型の携帯情報端末機器への適用を目指したもので，厚み1.2mm，長さ30mm，幅20mm，検出領域19mm×15mmである。画素ピッチ60μmの原理実証モデルを試作し，低温ポリシリコン化技術を適用したものとして初めて，実用的なレベルで指紋認証できることを実証した。




**薄型・小型指紋センサの外形と取得した指紋像**

パソコン，PDA，携帯電話等の携帯情報機器への搭載を目的とした二種類の薄型・小型指紋センサを開発した。光学式指紋センサでは，低発散角光源の適用により，厚さ10mmにおいて50μmの分解能，ひずみ2%以下を達成し実用の域にある。また，次世代品である容量式指紋センサでは，低温ポリシリコン化TFT技術を適用し，初めて指紋認証できることを実証している。

*先端技術総合研究所 **情報技術総合研究所 ***システムLSI事業統括部

## 1. まえがき

近年，本格的な情報化時代を迎えるに当たり，情報に対するセキュリティ管理が極めて重要となっている。特に，従来は一部の高度な知識を持つ専門家のみがネットワーク環境を使っていたのに対し，パソコン，携帯電話を始めとする携帯端末の発展，インターネットを起爆剤とする高速通信インフラの整備により，だれもが場所を選ばず簡単に情報を入手し，また，お金のやり取りを行えるようになった。情報入手の手軽さが増せば増すほど，逆に他人に盗まれる危険性も増していると言える。これらの危険性から守るため，パスワード，又は磁気・ICカードによる個人認証が一般に行われているが，ますます高度化する犯罪者から守るには十分とは言えず，指紋，こう(虹)彩，声紋，顔面等で個人を識別するバイオセンサとの組合せによってセキュリティ面での強化を図ることが考えられている。なかでも指紋による個人認証は，既にビルの入退場管理等において多数導入されており，一般的な手法として認知されつつある。この手法を携帯端末機器に導入しようという動きは自然な流れであるが，一方で，従来の指紋センサでは，センササイズの関係で適用が難しい場合がある。このような視点から，薄型・小型の光学式指紋センサ，及び先端液晶製造技術である低温ポリシリコン化TFT技術を適用した容量式指紋センサを開発した。以下に各指紋センサ技術の概要について述べる。

## 2. 薄型光学式指紋センサ

指紋を検出するセンサには指紋像を撮像する光学式指紋センサ，指紋とセンサとの間に形成される静電容量を検出する容量式指紋センサ，及び指表面の熱分布を検知する感熱式指紋センサが一般に使われている[1]。この中で，光学式センサは，古くから開発されており，現在最も普及している。高精度の指紋像を取得でき，かつ，静電気的なノイズに対して強いという特長がある。

開発した光学式指紋センサの主な仕様値を**表1**に示す。寸法は厚さ10mm，長さ30mm，横幅22mmであり，ノートパソコン，PDA等に組み込み可能な厚み・大きさを実現している。指紋を検出するための領域は18mm×12mmであり，分解能の面では指紋センサの必要条件とされている50μmが確保されている。

**表1．薄型光学式指紋センサの主な仕様**

| 項目 | | 仕様 |
|---|---|---|
| 検出領域 | | 18mm×12mm |
| 検出画素数 | | 352×288 |
| 分解能 | | 50μm |
| 画像ひずみ | | 2%以下 |
| サイズ | 厚さ | 10mm |
| | 長さ | 30mm |
| | 横幅 | 22mm |

指紋センサの構成を**図1**に示す。このセンサは指紋の検出面を照明する光源，検出面をセンサ上に縮小転写する縮小光学系，及び人工網膜LSI(画素数352×288)で構成される。光学系の薄型化に伴い，指紋像が生成される検出面と対応する人工網膜LSI表面各位置の光路長に大きなずれが生じるため，薄型化の一般的な問題である大きなひずみの発生，及び解像度の低下が現れるところである。ここでは，照明光源として発散性の少ない光源を採用することで解像度を確保するとともに，ひずみ2%以下を実現している。これは，指紋センサの重要な特性である本人拒否率，及び他人受入れ率低減に有用な特性である。

**図2**は，このセンサによって撮影した画像処理前の一定間隔の格子像である。同図において，濃い実線は実際に得られた格子像，また，薄い実線はひずみがない場合の理想的な格子を示している。最大ひずみは1.7%であることが分かる。また，要旨のページに示したように汗せん(腺)まではっきり見えるコントラストの高い指紋像が得られており，解像度は検出領域全域で50μmに対しMTF(Multi Transfer Function)30%以上を確保している。

光学系は，低コスト化の観点から樹脂成形レンズを採用している。また，樹脂成形の自由度を最大限に生かし，必要に応じて複数回折り返す光路構成とし，厚み・大きさを低減している。

指紋センサとしての基本機能を満足しつつ，ノートパソコンに組み込み可能な薄型化を実現したことが大きな特長と言える。

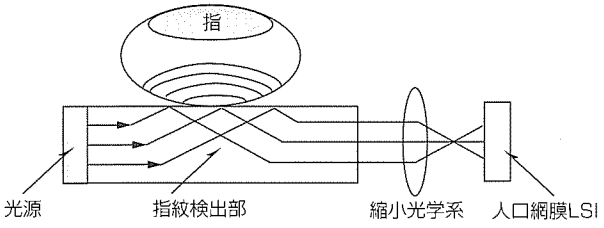



**図1．薄型光学式指紋センサの構成**

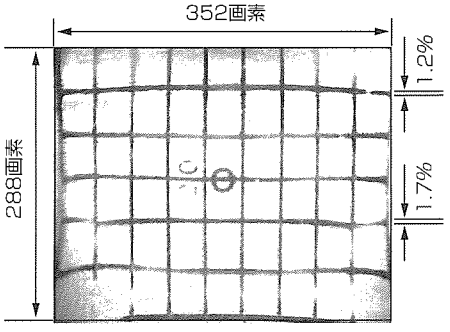



**図2．グリッド像(ひずみ評価結果)**

## 3. 低温ポリシリコン容量式指紋センサ

### 3. 1 容量式指紋センサ

前章に紹介した指紋センサは光学式としては薄い厚み10mmを実現しているが，携帯電話，小型携帯機器等の携帯情報端末では既に電子部品が隙間なく挿入されており，その組み込みは難しい。そのような用途では，容量式指紋センサの適用が一般に考えられている。容量式センサでは，半導体製造プロセスを使って，検知電極と指との間に生成される静電容量を通常は複数のトランジスタからなる回路で検出する。検知電極のピッチは，必要解像度を確保する観点から，おおむね50μmピッチで設置されている。ここでの問題は，指の指紋像を検出するために例えば15mm×15mmといったかなり大きい検出面が必要になることである。シリコン基板は基本的に高価であり，最先端の超LSIでは，回路の線幅を0.2μm未満といった極端に細線化することで，単位面積当たりに製作するトランジスタの個数を増大し，ウェーハ面積を増大することなく製品の高付加価値化を図っている。しかしながら，指の大きさでその必要なウェーハ面積が決まる容量式指紋センサでは，コスト低減が難しく，その普及を妨げる大きな要因の一つとなっている。この問題を解決するための一つの手段として，最先端液晶において採用されている低温ポリシリコン化TFT技術を使って容量式指紋センサを試作し，実用的なレベルで指紋認証できることを実証した。この技術の概要について以下に紹介する。

### 3. 2 低温ポリシリコン方式指紋センサの原理[2]

図3に指紋検出のための原理を示す。容量式指紋センサでは一定ピッチで設定された各感知電極に対し，一端にバイアス電圧$V_{SR}$を印加した信号検出のための静電容量$C_t$が接続されている。一方で，感知電極表面には保護膜を介して指紋検出対象となる指が置かれる。いま，指がアース電位になっていると仮定すると，各感知電極には，指と感知電極の間で形成されるギャップに応じた浮遊容量$C_{f1}$が生成される。保護膜部での静電容量を$C_{f2}$とすれば，各感知電極には，$C_{f1}$と$C_{f2}$の合成容量である$C_f$と$C_t$の比に応じた分圧電圧$V_G$が発生する。この$V_G$を検出することによって指紋像を取得することができる。

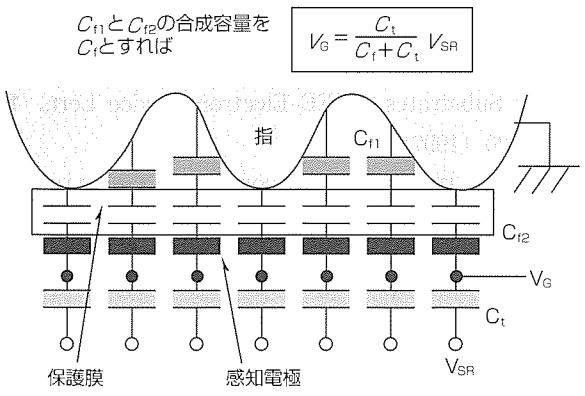



図3．容量式指紋センサの原理

指紋像を検出するために提案した具体的な指紋検出回路を図4に示す。従来の指紋検出回路では，まず，1個のトランジスタを使って静電容量$C_f$に電荷を充電し，次に2個目のトランジスタを使って蓄えられた電荷を読み出すという方法が採られていた。このため，一つの検知電極に対し2個のトランジスタを作り込む必要があった。低温ポリシリコン方式のトランジスタでは適用されるトランジスタの線幅ルールが5～20μmオーダーにあるため，画素50μm角に2個のトランジスタを形成すると静電容量$C_f$を形成するために必要な感知電極サイズが確保できないという問題があった。実際，低温ポリシリコン方式を採用した指紋センサは既に報告されているが，そのセルピッチは100μm(254dpi)にとどまっており，指紋センサに必要な条件とされている50μmは実現が難しい状態であった[3]。

ここでは，トランジスタ1個で検出する回路を提案することによってこの問題を克服した。図において，1個のトランジスタのゲートに対し感知電極が接続されている。ソース-ドレイン間で形成される浮遊容量が分圧用静電容量$C_t$の役割を果たしている。この際，一定のパルス幅を持つバイアス電圧$V_{SR1}$が印加されると，分圧電圧$V_G$(浮遊容量$C_f$)に応じてゲートが開き，主電流が流れるため，信号検出用のコンデンサHRにおいて$V_G$に対応した充電電圧が検出される。

従来の単結晶ベースのトランジスタにこの回路を適用した場合，その動作しきい値電圧が0.7V程度であるため，HRに対応した電圧が隣接するトランジスタのゲート-ドレイン間にも印加され，本来コンデンサHRを充電すべき電荷が隣接のトランジスタ回路にリークするという問題が生じる。しかしながら，低温ポリシリコン方式のトランジ

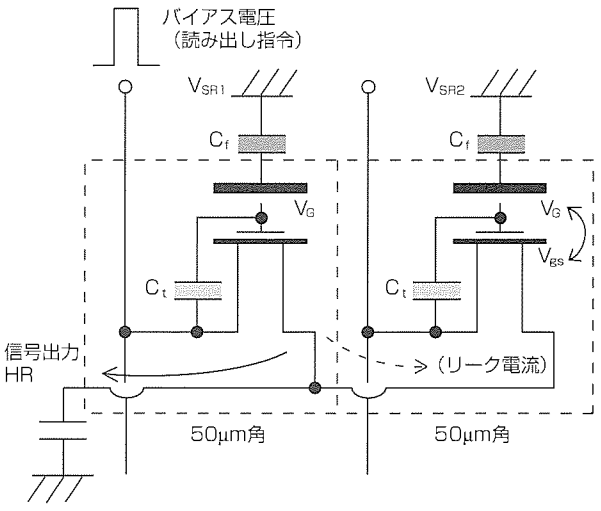



図4．容量式指紋センサ検出回路

スタでは，しきい値電圧が2.5Vから3.0Vと高いため，その分リーク電流が流れ出すしきい値電圧が増大し，検出信号に対するダイナミックレンジを大きくとることができる。

### 3. 3　試作したデバイスの概要

図5に試作した指紋センサのレイアウトを示す。

Vertical Shift Registerは縦方向のスキャン用レジスタである。アレー内の配線数を減らす目的から，シフトレジスタ出力をそのままアレーへの電源線としている。

Horizontal Shift Registerは水平方向のスキャン用レジスタである。

READOUTはアレーからの信号を出力し，スキャンラインと出力線をリセットするための回路である。

これらすべての回路は，低温ポリシリコンプロセス技術を用いて，ソーダガラス基板上に製作されている[4]。

表2に，試作した指紋センサの仕様を示す。今回のデバイスでは原理実証を目的としており，マージンをとって容量が大きくできるように60μmピッチ(423dpi)としている。この試作結果から，50μmピッチのものも製作可能であることが確認された。

始めの要旨の項に試作した装置によって取得した指紋像を示しているが，極めてコントラストの高い指紋像が得られていることが分かる。指紋認証ソフトウェアを介して指紋検証を行った結果，先に開発した光学式指紋センサレベルに近い認証性能が得られることが確認された。

低温ポリシリコンによるTFT製造技術は，安価な大型のガラス基板上に液晶ディスプレイを製作するために開発されたものであり，容量式指紋センサの低コスト化に対し，一つの現実的な解を与えるものであると考えている。

## 4. むすび

ノートパソコンへの組み込みをねらった薄型・小型指紋センサを開発した。厚さ10mm，長さ30mm，幅22mmでありながら，性能面では検出領域18mm×12mm，解像度50μm，ひずみ2％以下と，指紋センサとして必要にして十分な機能を備えている。

一方，携帯電話，PDA等小型の携帯情報端末機器への適用を目指した低温ポリシリコン方式容量式指紋センサを提案し，原理実証を行った。ここでは厚さ1.2mm，長さ30mm，横幅20mm，検出領域19mm×15mmのセンサを試作し，従来の光学式指紋センサとほぼ同等の認証能力があることを確認した。現状個人用情報端末機器への適用に対し，一つの現実的な解を与えるものと期待される。

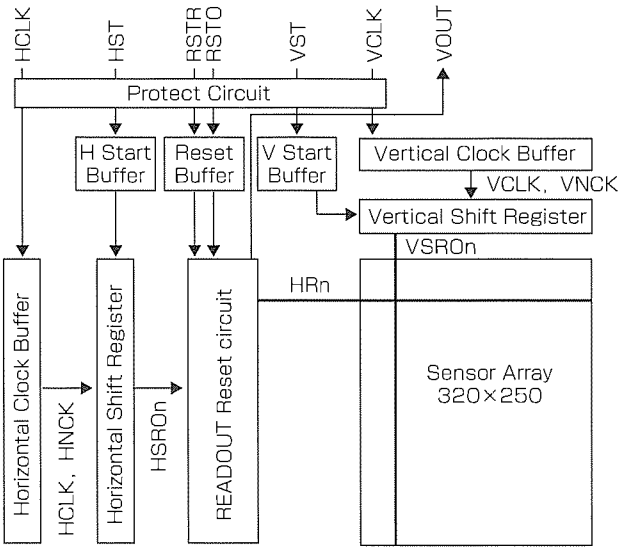



図5．容量式指紋センサのレイアウト

表2．容量式指紋センサ試作チップの仕様

| 項　目 | | 仕　様 |
|---|---|---|
| 検出領域 | | 19mm×15mm |
| 検出画素数 | | 320×250 |
| セルサイズ | | 60μm×60μm |
| 印加電圧 | | 5 V |
| 消費電力 | | 1.2mW |
| サイズ | 厚さ | 1.2mm |
| | 長さ | 30mm |
| | 横幅 | 20mm |

上記の薄型・小型光学式指紋センサについては既に実用化段階にある。一方，低温ポリシリコン容量式指紋センサについては，容量式で課題である静電耐圧の問題についてまず現状を把握し，今後対策を講じていく必要がある。

## 参考文献

(1) 内田　薫：映像情報メディア学会誌，**55**，176～179 (2001)

(2) 橋戸隆一，ほか：低温poly-Si製容量型指紋センサ，信学技報，ICD2001-26，15~21 (2001)

(3) Young, N., et al.：Novel Fingerprint Scanning Arrays using Polysilicon TFT's on Glass and Polymer Substrates, IEEE Electron Device Lett., **18**, 19～20 (1997)

(4) Tokioka, H.：AM-LCD 1996Digest, 113～116 (1996)

# デジタル写真プリントエンジン

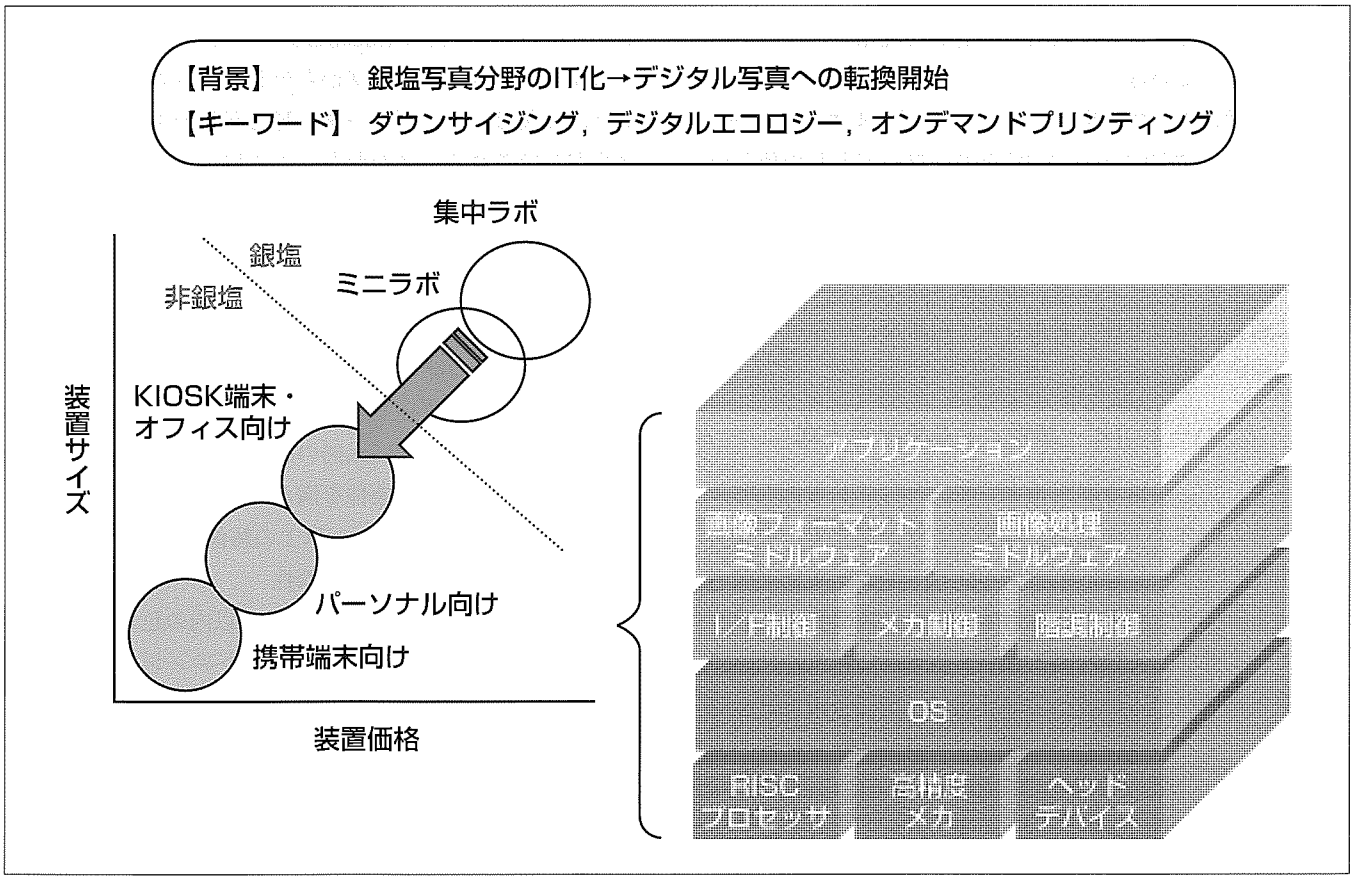
山田敬喜*
木村修也**
高橋正敏*

**要　旨**

ハードコピー分野は，インパクトからノンインパクトへ，そしてモノクロ／カラーからフルカラーへと市場と技術が進化している。WYSIWYG(What You See Is What You Get)の観点からは，概念が確立された第三世代のDTP(Desk Top Publishing)を経て，高精細ハードコピー技術との結合による第四世代の実用化がスタートした。

フルカラーを実現する方式は数多く提案されているが，昇華型記録は，最も高精細なフルカラー画像が得られるデジタルプリント方式の一つである。昇華型プリントエンジンの実用化は，TV等のビデオプリンタとしての応用から始まり，最近ではデジタルスチールカメラの普及を背景に，デジタル写真分野への応用が急速に拡大しつつある。

本稿では，“ダウンサイジング”“デジタルエコロジー”“オンデマンドプリンティング”をキーワードとした新しいデジタル写真対応のプリントエンジン，すなわち，既存の銀塩市場形態と一線を画したKIOSK端末やオフィス向け業務用プリントエンジン及び携帯端末向けプリントエンジン等に適した画像処理ミドルウェア技術及び高精度紙搬送技術について述べる。三菱電機は，優れた階調制御技術に加えて，マルチプラットフォームに対しても柔軟に対応可能なエンジンアーキテクチャや先行的なロール紙プリント機構の高度化等により，高速・高画質，高信頼性を実現している。




**デジタル写真市場展開とプリントエンジンプラットフォーム**

銀塩写真分野のIT化により，集中ラボやミニラボからエンドユーザーがより手軽に写真を扱うことのできるプリント環境へ移行しつつある。これに伴い，プリントエンジンは，低価格化・小型化へと進み，新しい三つの分野への展開が予想される。デジタル写真対応のプリントエンジンプラットフォームは，RISCプロセッサや高精度メカ，各種ミドルウェア等で構成され，“よりきれいに”“より速く”“より安く”を追い続ける。

*情報技術総合研究所　**京都製作所

## 1. まえがき

デジタルスチールカメラ市場は急速に拡大し，2001年上期の国内出荷台数は200万台に達した。今後も，パソコンや携帯端末への画像入力機器として，更なる急成長が期待できる。一方，ハードコピー分野は，インパクトからノンインパクトへ，そしてモノクロ／カラーからフルカラーへと市場と技術が進化している。ハードコピーに関連するWYSIWYGの技術変遷を**表1**に示す。WYSIWYGの概念はデータ処理や文書処理に続くDTP世代で確立され，現在は，レイアウトから色彩まで一致する第四世代の実用化がスタートしたところである。

フルカラーを実現する方式は数多く提案されているが，今後は，普通紙化と高画質化に分化していくと考えられる。現在のところ，前者では電子写真方式が，後者では昇華型記録方式が有望である。三菱電機がフルカラーの本命と位置付けている昇華型プリントエンジンの実用化は，TV等のビデオプリンタとしての応用から始まった。そして，女子高校生の間でブームとなったシールプリント等を経て，最近では，デジタルスチールカメラの普及を背景にデジタル写真分野への応用が急速に拡大しつつある。これらは，現像する必要がなく簡単に写真を入手できるというデジタル写真の特長をデジタル入出力機器が具現化できつつあることを意味している。

本稿では，“ダウンサイジング”“デジタルエコロジー”“オンデマンドプリンティング”をキーワードとした新しいデジタル写真対応のプリントエンジン，すなわち，既存の銀塩市場形態と一線を画したKIOSK端末やオフィス向け業務用プリントエンジン及び携帯端末向けプリントエンジン等に適した画像処理ミドルウェア技術及び高精度紙搬送技術について述べる。

## 2. ハードコピー技術と昇華型記録方式

ハードコピー技術をエネルギー変換としてとらえると，電気信号の物理像への変換と考えることができる。すなわち，ハードコピーとは，サーマルヘッド等のプリントデバイスによって電気信号を各種エネルギーに変換し，このエネルギーに感応して物理像を形成するものである。

三菱電機のハードコピー関連技術は，1970年代前半の漢字プリンタ用電子写真記録，'70年代後半のファクシミリ用静電記録や感熱記録からスタートした。そして，'80年代には，カラー市場の拡大を予見し，原理的に高画質記録が可能な昇華型記録方式に着目するとともに，フルカラー記録への先べん(鞭)をつけた。印刷・デザイン，医療，アミューズメント分野等で市場形成的役割を果たしたのが“CPシリーズ”や“Sシリーズ”であり，業務用途を中心に堅調に推移している。最近では，現像廃液処理が不要でシステムをコンパクトに構成できるという特長から，銀塩写真システムからの代替が証明写真分野でも開始されている。

染料の拡散現象を用いた昇華型記録方式では，階調及び色再現性に優れた分子レベルの混色画像が得られる。それゆえに，銀塩等を使わない電子的な記録方式の中では最も高精細なフルカラー記録が可能である。昇華型記録は，原理的に，普通紙記録にはなじまない。この方式の特長が最大限に発揮できる分野は，より高品位なフルカラー画像を必要とする用途，すなわち，デジタル写真用途が最も適している。そして，この方式の特長を一層明確にするためには，安定した高精細フルカラー画像を得るための技術開発が最大の課題である。

**表1．WYSIWYGの技術変遷**

| 分　類 | WYSIWYGレベル | 対　象 | 製　品 |
|---|---|---|---|
| 第一世代 | 意味の一致 | データ，文字 | データ処理 |
| 第二世代 | レイアウトの類推 | 文字，表 | ワープロ |
| 第三世代 | レイアウトの相対的一致 | 文字，表，図形，マルチカラー | DTPシステム |
| 第四世代 | 色彩の一致 | 文字，表，図形，フルカラー | フルカラーシステム，デジタル写真システム |

## 3. デジタル写真プリントエンジン

### 3.1 デジタル写真市場展開とプリントエンジン

銀塩写真分野はアナログからデジタルへの技術転換期にあり，今後は，コンピュータ分野と同様のダウンサイジング化が想定される。すなわち，汎用機やミニコンに相当する集中ラボ(集配処理)やミニラボ(店頭処理)から，ワークステーション，パソコン等に対応するKIOSK端末，オフィス向けやパーソナル・携帯端末向けへの展開である。また，環境問題に配慮する必要性から，現像廃液等の産業廃棄物レス化やオンデマンドプリンティング化がデジタル革命を加速するキーワードとなる。さらに，デジタル写真の技術的な定義としては，人間の眼の分解能や積分能力等を考慮した，次の三つの条件を満たすことが望ましい。

- 12～20ピクセル／mm以上の解像度
- 各色8ビット以上の階調性
- 一画面内の色差1.6，画面間3.2以内の色再現性

一方，デジタル写真対応のプリントエンジンは，RISCプロセッサや高精度メカ，各種ミドルウェア等で構成され，“よりきれいに”“より速く”“より安く”が永遠に追い求められる。三菱電機は，業界最高速レベルの昇華型プリントエンジンに加え，マルチプラットフォームに対しても柔軟に対応可能なエンジンアーキテクチャやロール紙プリント機構の高度化等によって高速・高画質，高信頼性を実現している。

### 3.2 プリントエンジンアーキテクチャ

KIOSK端末やオフィス向け業務用プリントエンジン，携帯端末向けプリントエンジン等のマルチプラットフォー

ムに対しても柔軟に対応可能なプリントエンジンアーキテクチャの例を**図1**に示す。プリントエンジンは，I／F Cont，RISCプロセッサ(20MHz以上)，Engine Cont等で構成され，例えば，入力画像データがVGA(Video Graphics Array)程度であれば20～30Kゲートのハードウェアと1Mビット程度のミドルウェアで構成される。主要機能を以下に示す。

(1) I／F Cont

SCSI(Small Computer System Interface)やUSB(Universal Serial Bus)等のI／Fを制御し，データパスを共通化する(I／Fのモジュール化)。

(2) Power Cont

ACアダプタや電池駆動を可能とする。未使用時には自動的にパワーオフする省電力機能も備えている。

(3) RISCプロセッサと画像処理ミドルウェア

シンプルなハードウェアとRISCプロセッサ上で動作する高速ミドルウェア構成を採用している。画像処理ミドルウェアフローを**図2**に示す。まず，画像データは，フォーマット変換でJPEGデコードされ，回転／変倍処理される。そして，ヒストグラム等を利用した適応型画像補正やLUT(Look Up Table)等を用いた色変換処理が施される。フィルタリング処理とユニフォーミティ処理は画像のひずみを補正するものである。なお，高画質化に必要なユニフォーミティ処理については**3.3節**で述べる。

(4) Engine Cont

プリントヘッドのI／F制御や高速記録時の蓄熱補正等を行うとともに，多値レベルで与えられる画像データを2値化する。フルカラー記録を行うには，同一ラインで複数回の2値化データをヘッドに転送し，その都度階調制御する。ゆえに，$n$値の場合には，$n-1$回のデータ転送と$n-1$回の階調制御が必要である。そして，階調レベルごとにパルス幅変調し，画像データと記録濃度(又は明度)の関係にリニアリティを持たせている。

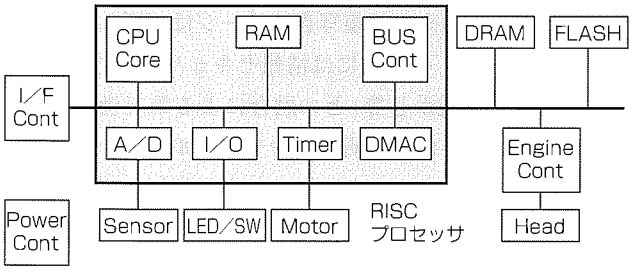



**図1．デジタル写真プリントエンジンアーキテクチャ**

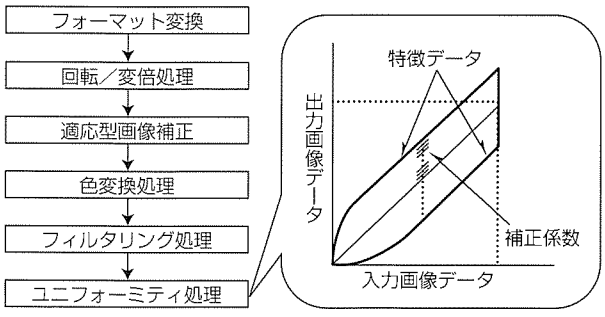



**図2．画像処理ミドルウェアフロー**

### 3.3 ユニフォーミティ処理

画像処理ミドルウェアの一例としてユニフォーミティ処理について紹介する。ライン型ヘッドデバイスを使用する場合には，通常，濃度むらが発生する。ヘッドに起因する濃度むらはその構造や電気的な要因による装置固有のものが多く，また，幾つもの要因が複雑に絡み合っている。ユニフォーミティ処理はこれらの濃度むらを総合的に補正するもので，処理の基本方針は次のとおりである。

(1) メモリ容量を削減するため，特徴的な特性データをあらかじめ求めておき，演算によって画像データを補正する。

(2) 高濃度側の補正も確実に行うため，処理後のビット数を大きくする。

具体的には，以下の手順に従う。

各ピクセルの記録濃度を$D_i$(iはピクセルの位置)とし，ピクセル総数を$n$とすると，平均濃度$D_m$は，

$$D_m = \left(\sum_{i=1}^{n} D_i\right) / n \quad \cdots\cdots(1)$$

で表される。各ピクセルの濃度誤差$E_i$は，記録濃度$D_i$と平均濃度$D_m$を演算することで求められるが，最大で$i$個になる場合がある。そこで，誤差$E_i$に，例えば0.05ごとの幅を設定して複数グループに分割し，グループごとに補正係数$K$を設定する。なお，補正係数$K$は，各ピクセルの濃度が等しくなるように決定すればよい。

$$K = 1 / E_i \quad \cdots\cdots(2)$$

次に，各階調レベルごとに式(2)を求め，画像データの入力値と補正値の関係をグラフ化すると，ほぼ同様の特性を示した。今回はここに注目している。すなわち，代表的な特徴データのみを抽出し，この特徴データとピクセルごとの補正係数$K$を演算すれば，テーブル容量を1／10以下にすることが可能となる。さらに，高画質化を実現するために，補正後の画像データビット数を1ビット増加させる。評価結果では，20%程度の濃度むらでも2～3%以内に補正することが可能になり，画質が大幅に向上している。

### 3.4 ロール紙プリント機構

KIOSK端末やオフィス向けプリントエンジンには，銀塩写真並みの画質と高信頼性に加え，ユーザーを待たせない“高速プリント”，ニーズに合わせた“多様なメディアサイズ”，システムに合わせた“多彩なI／F”や“省スペース”，専属オペレータを必要としない“簡便性”や“紙ジャムレス”等が要求される。このような要求にこたえるためにデジタル写真プリント機能を強化したのが昇華型プリントエンジンCP8000Dである。

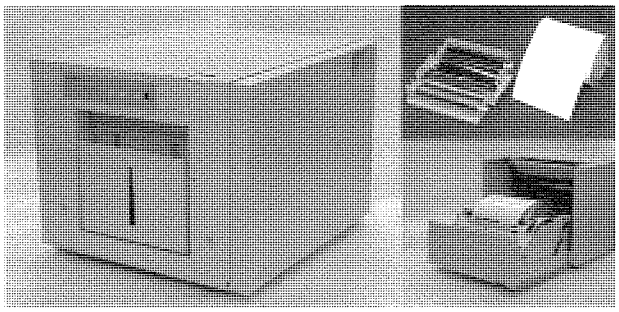
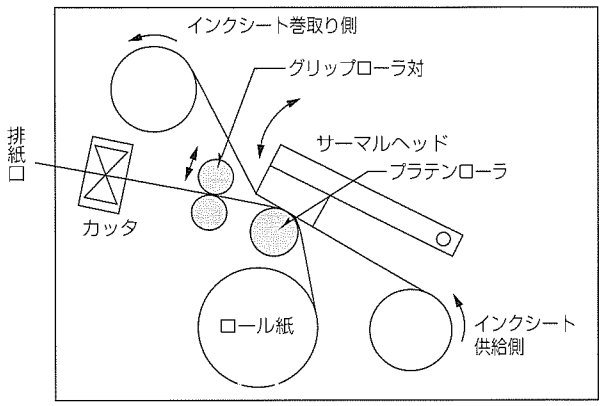


図３．CP8000Dの外観

表２．市場要求とCP8000Dの基本仕様

| 市場要求 | | 基本仕様 |
|---|---|---|
| 銀塩写真並みの画質 | | 解像度：12ピクセル/mm |
| 銀塩写真並みの耐久性 | | 保護層プリント |
| ユーザーを待たせない高速プリント | | 約15秒/L判 |
| メディアサイズの多様化 | | L判／A6／A5ワイド／ポストカード |
| 多様なシステムへの対応 | | I／F：パラレル／SCSI／USB |
| 狭い店内やオフィスの有効活用 | 省スペース | 容積：32リットル |
| | 大容量 | L判240枚 |
| 専属オペレータレス | | 簡単装着，紙ジャムレス |




＜制御フロー＞
(1) ロール紙の先端をグリップローラ対にセット
(2) コマンド受信後，グリップローラ対が閉じてロール紙を保持
(3) サーマルヘッドが下降してインクシートとロール紙を密着
(4) グリップローラがロール紙を排紙口側に搬送
(5) インクシートはロール紙からの摩擦力によってロール紙を搬送
(6) サーマルヘッドが発熱してイエロー画像をプリント
(7) イエローのプリントが終了するとサーマルヘッドは上昇し，ロール紙とインクシートの圧着を解除
(8) インクシートを次の色まで巻き取り
(9) グリップローラが逆転してロール紙を逆送
(10) 同様に，マゼンタ，シアン，透明保護層をプリント
(11) プリント完了後，ロール紙を搬送し，所定位置で切断

図４．ロール紙プリント機構と制御フロー

CP8000Dの外観及び基本仕様を**図３**と**表２**に，ロール紙プリント機構とその制御フローを**図４**にそれぞれ示す。CP8000Dでは，12ピクセル/mmの高解像度化によって写真並みの画質を実現しているとともに，表面に透明保護層を重ねることで耐久性も高めている。また，32リットルの小容積にL判240枚という大容量メディアを搭載し，約15秒の高速プリントを達成している。さらに，L判／A６／A５ワイド／ポストカード等の多様なメディアサイズにも対応している。そして，前面操作が可能なフロントオープン方式に加え，記録メディアの交換等を容易にするカセット／ロール紙装着方式を採用することによって操作性を一層高めている。

ロール紙プリント機構にはプリントごとの給紙動作がないため，紙ジャムが原理的に発生しにくい。KIOSK端末では無人運転を前提としているため装置停止が最も嫌われ，また，メンテナンス作業者の熟練も期待できないため，“給紙ジャムが発生しない”“記録メディアのハンドリングがしやすい”等は極めて大きなメリットとなる。

## 4. むすび

三菱電機は，優れた階調制御技術に加えて，マルチプラットフォームに対して柔軟に対応可能なエンジンアーキテクチャやロール紙プリント機構の高度化等により，常に高速・高画質，高信頼性に挑戦し，アプリケーション創出に貢献している。例えば，シールプリントによるデジタルプリントコミュニケーション文化の創出はその好例である。

今回述べたような新しいデジタル写真プリントエンジンの普及が現実のものとなるには，CPUの高度化やデジタルスチールカメラの更なる普及のほか，次の三つがキーとなる。

(1) フルカラー画像を本格的に扱えるマルチメディアコンピュータや携帯端末の普及
(2) 写真を超える高画質・低価格プリントエンジンの供給
(3) ブロードバンドインターネットをより意識したアプリケーションソフトウェアの充実

これらの項目が達成された日には本格的なデジタル写真時代が到来し，従来の銀塩写真イメージは一新しているであろう。さらに，その先には情報セキュリティ技術（デジタル署名や電子透かし等）との融合による第五世代セキュアイメージング時代が証明写真やデジタルコンテンツ分野を中心にスタートするであろうことを付け加えておく。

## 参考文献

(1) 大西　勝，ほか：感熱昇華記録転写型技術，電子写真学会誌，**33**，No.2，69～74（1994）
(2) 山田敬喜，ほか：昇華型プリンタの高精細化技術，Workshop Electronic Photography '91，85～88（1991）
(3) 山田敬喜：三菱昇華型フルカラープリンタS340形，カラーグラフィック研究会，**3**，No.3，9～21（1991）
(4) 山田敬喜：第29回日本伝熱シンポジウム講演論文集，C241，485～486（1992）
(5) 山田敬喜，ほか：リライタブル記録媒体の記録消去特性(I)，画像電子学会誌，**21**，No.5，546～552（1992）

# 特許と新案＊＊＊

三菱電機は全ての特許及び新案を有償開放しております

有償開放についてのお問合せは
三菱電機株式会社　知的財産渉外部
電話(03)3218-9192(ダイヤルイン)

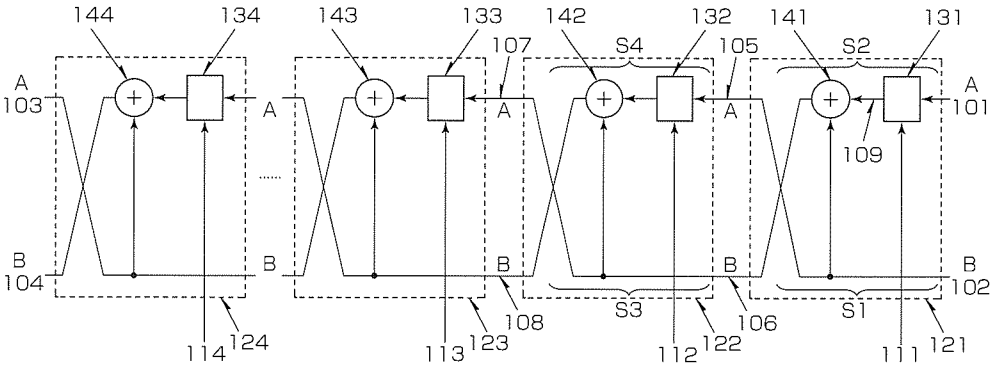
## データ変換装置（特許　第3035358号，国際公開W097／09705号）

発明者　　山岸篤弘

この発明は，情報通信等においてデジタル情報を保護する入力データの暗号化と復号化，及びデータ拡散等のためのデータ変換装置に関するものである。従来のデータ変換装置は，順次処理であるため処理が遅くなるという課題があった。

この発明は，上記の課題を解消するためになされたもので，複数の副変換処理を並列で行えるように構成して，暗号化・復号化及びデータ拡散等のデータ変換処理の高速化を目的とする。図はこの発明による暗号化回路である。この発明にかかわるデータ変換装置は，任意の二つのA入力データとB入力データに対し，二つの非線形変換(131, 132)と二つのかぎ（鍵）パラメータ(111,112)を並列に作用させる機構を備え，その二組の変換結果の各々を二組の排他的論理和（141,142)を介して次の段への入力とする構成をとっている。この構成を縦続接続することで，奇数段相当の演算と，偶数段相当の演算を並行して処理でき，演算の高速化を図ることができる。

なお，この発明は，MISTYの一層の普及を目指し，暗号アルゴリズムMISTYを搭載した製品を開発し事業化していただける企業，法人を対象に使用許諾契約を締結していただいた上で無償で許諾しております。



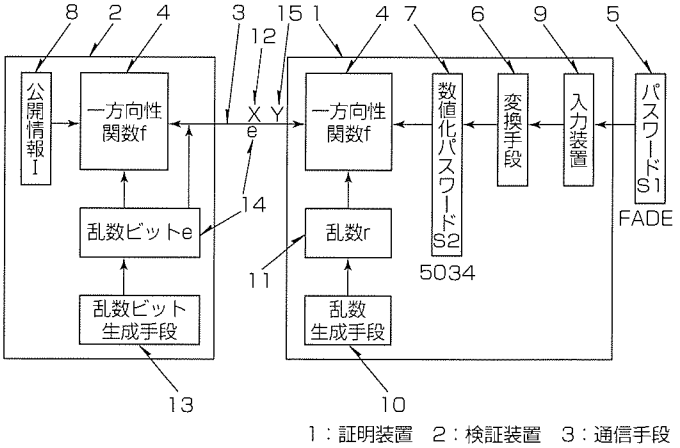

## 認証方法（特許　第2993275号，特開平5-323874号）

発明者　　小林信博，櫻井幸一，岡本隆司

この発明は，ユーザーの入力したパスワードを用いてユーザーの認証を行う認証方法に関するものである。従来の認証方式においては，パスワードを記憶した媒体を用いるため，ユーザーに成り済ますことが可能であるという問題があった。

この発明は，記憶媒体とその読み取り装置を不要にすることを目的としており，装置が安価な認証方法を提供するものである。

この発明では，証明装置に入力したパスワードS1(5)を数値化パスワードS2(7)に変換し，この数値化パスワードS2(7)を用いて，零知識証明方式により，安全に入力者の認証を行うことができる。図はこの発明による認証方法である。この認証方法では，あらかじめ公開した一方向性関数f(4)を証明装置(1)と検証装置(2)に組み込み，さらに，入力されたパスワードS1を一方向性関数f(4)で変換した公開情報Ⅰ(8)を登録する。認証時には，証明装置(1)は，入力されたパスワードS1と乱数r(11)から，一方向性関数fで初期応答文X(12)を生成し，検証装置に初期応答文X(12)を送信する。検証装置は，受信した初期応答文Xを種とする乱数ビットe(14)を生成し，証明装置に送信する。証明装置では検証装置から送信された乱数ビットe，一方向性関数f，乱数r，数値化パスワードS2を用いて応答文Y(15)を生成し，検証装置に送信する。検証装置では，受信した応答文Yを，一方向性関数f，初期応答文X，乱数ビットe，公開情報Iを用い，零知識証明方式の認証を行うことができる。




1：証明装置　2：検証装置　3：通信手段

We Head 21
特許有償開放

特許と新案
三菱電機は全ての特許及び新案を有償開放しております

有償開放についてのお問合せは
三菱電機株式会社　知的財産渉外部
電話(03)3218-9192(ダイヤルイン)

## 暗号化方式（特許　第2862030号，特開平4-365240号）

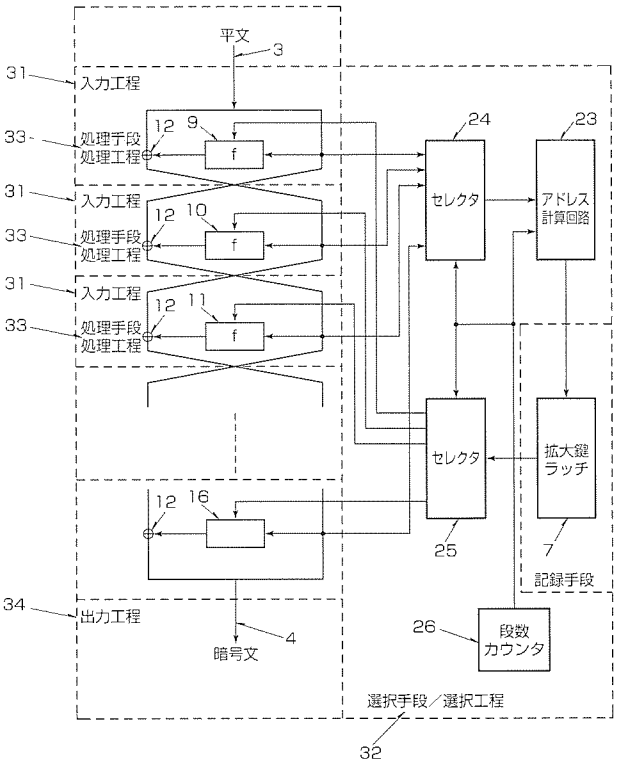
発明者　　松井　充

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

従来の暗号化方式は，以上のように構成されるので，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において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，上記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。




### 〈本号記載の商標について〉

| | |
|---|---|
| "Adobe""Acrobat" | Adobe Systems Incorporatedの商標である。 |
| "CryptoSign""TRUSTWEB""MistyGuard" | 三菱電機㈱の登録商標である。 |
| "CertMISTY""PowerMISTY" | 三菱電機㈱の登録商標である。 |
| "Java""Solaris" | 米国Sun Microsystems,Inc. の商標又は登録商標である。 |
| "Linux" | Linus Trovalds氏の米国及びその他の国における商標又は登録商標である。 |
| "Microsoft" | 米国Microsoft Corp. の米国及びその他の国における登録商標である。 |
| "Pentium" | 米国Intel Corp. の登録商標である。 |
| "SignedPDF" | 三菱電機㈱が商標出願中である。 |
| "UNIX" | 米国The Open Group Ltd. が独占的にライセンスしている登録商標である。 |
| "Word""Excel""Windows""Windows NT" | 米国Microsoft Corp. の商標又は登録商標である。 |
| "HP-UX" | 米国Hewlett-Packard Companyのオペレーティングシステムの名称である。 |

そのほか，本号に記載されている会社名，製品名はそれぞれの会社の商標又は登録商標である。

〈次号予定〉三菱電機技報 Vol.76 No.5 「省エネルギー機器・技術」特集／「低圧遮断器の最新動向」特集

三菱電機技報編集委員
委員長　井手　清
委員　中村治樹　畑谷正雄　吉原孝夫
栗原幸志　村松　洋　松本　修
浜　敬三　安福正樹　西谷一治
中島克人　荒木政敏
河内浩明　山木比呂志
事務局　松本敬之
本号取りまとめ委員　竹田栄作
飯島康雄

三菱電機技報　76巻4号　　2002年4月22日　印刷
（無断転載・複製を禁ず）　　2002年4月25日　発行
編集人　井手　清
発行人　福本紀久男
発行所　三菱電機エンジニアリング株式会社　e-ソリューション&サービス事業部
〒105-0011　東京都港区芝公園二丁目4番1号
秀和芝パークビルA館9階　電話（03)3437局2692
印刷所　株式会社　三菱電機ドキュメンテクス
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

URL　http：//www. melco. co. jp/giho/
三菱電機技報に関するお問い合わせ先　cep. giho@ml. hq. melco. co. jp

© 2002 Mitsubishi Electric Corporation, printed in Japan

スポットライト

# 三菱電子署名ソフトウェア “MistyGuard<SignedPDF>”(注)

2001年4月に施行された「電子署名法」により，従来は紙に印鑑を押印する形でなされていた文書交換が，電子署名を押印することで電子的な文書も正式文書として取り扱われる法的基盤が整備されました。また，同時期に施行された「IT書面一括法」により，従来書面による交付，手続が必要だったものを，電子メール等の電子的手段によって行うことも可能となりました。これに関連して，改正対象となった法律は50に及び，電子政府の2003年実現，eコマースの進展と相伴って電子署名ソフトウェアの導入気運は確実に高まっております。

SignedPDFは，PDFファイルに対してICカードを利用して電子署名を行い，印影を表示するシステムとしては国内初の製品であり，社内のりん(稟)議書から企業間の正式文書，官公庁への申請書提出まで幅広くご利用いただけます。

## 特　長

(1)　企業間及び企業内の文書交換の効率アップ

電子署名の押印により，“なりすまし”や“改ざん”のリスクを回避することができるので，正式な文書交換にご活用いただけます。正式文書を紙と検印という形態からSignedPDFを導入してネットワークで容易に送受信する形態に移行することで，書面の送付時間の大幅な短縮が可能になります。社内稟議で活用すれば，出張先からでも検印が可能であり，意思決定の迅速化と業務の効率化にもつながります。

また，従来は郵送によって企業間で交わされていた請求書や発注書等を電子化することで，大幅に郵送コストが削減できます。紙文書全般を電子化しネット送受信するのに最適な仕様のPDFを採用しておりますので，あらゆる文書の交換に適用できます。

さらに，PDFは，XMLを始めとしたデータベースとの親和性も高く，既存の業務システム，データベースと連携させることで，紙ベースで業務を行っていた場合に必要だった再入力業務を不要にします。シームレスなシステム構築が可能となり，業務コストが削減されます。

(2)　なじみのある“印影イメージ”はそのままに

SignedPDFは，電子署名を押印する際に，紙への押印同様にPDFの署名領域に対して印影イメージを表示します。したがって，いままでの書類イメージをそのまま電子化することが可能になります。印影は，日本企業の商習慣の継続といった点からだけでなく，不可視的な電子署名を可視的に表現するためにも必要です。

また，印影をダブルクリックするだけの簡単操作で，署名検証(本人確認・改ざん検知)を行い，署名のステータスは図1のとおり分かりやすく表現されます。

(3)　ICカード利用による堅固なセキュリティ

SignedPDFのご利用に当たっては，電子署名を押印する際に必要となる認証局から発行される証明書及び秘密かぎ(鍵)はICカードに格納します。証明書等をパソコンに保存している場合は出張先での利用は困難な場合もあり，また，パスワードの類推や盗難によるリスクが内在しております。ICカードは内部情報の改変や偽造が困難であるのと同時に内部の情報はパスワードによって保護されているため，ふん(紛)失した場合でも内部情報の読取は難しく，よりセキュリティが堅固であると言えます。

## 主な用途・対象分野

- 企業・組織内及び企業間でのワークフローシステム(各種手続・決裁全般)
- 金融機関，製造業，電力業界対応の文書交換，原本保存，及び申請業務等
- 電子政府・電子自治体における文書交換，電子申請，情報公開等
- 建設CALSにおける電子調達，電子納品等
- 医療分野での医薬品申請等
- 電子商取引における電子伝票，電子カタログや電子帳票，電子帳簿等

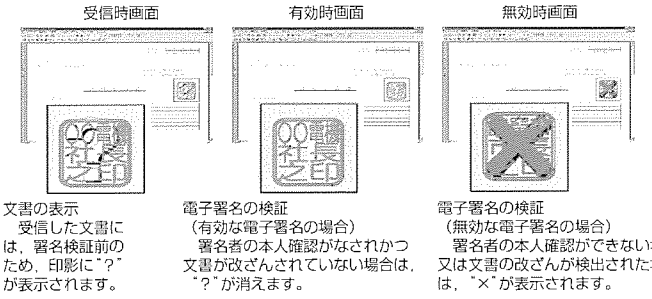



図1．文書受信時の画面表示例

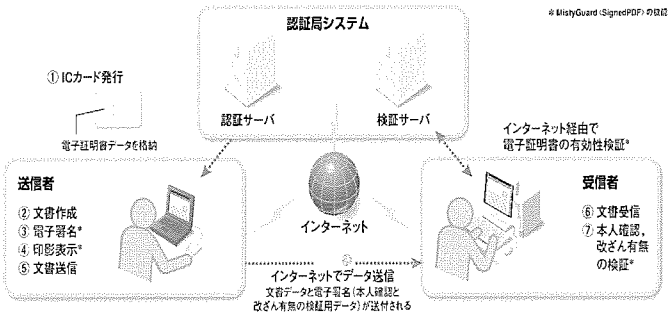



図2．MistyGuard<SignedPDF>のシステム構成例

住　所：〒100-8310 東京都千代田区丸の内2-2-3
会社名：三菱電機インフォメーションシステムズ株式会社　お問い合わせ先：インターネットセキュリティ事業推進プロジェクト
TEL　03-3218-3237　E-Mail：security@isd2.mdis.co.jp