昭和37年9月15日第三種郵便物認可　三菱電機技報　82巻5号（通巻924号）　2008年5月25日発行（毎月1回25日発行）

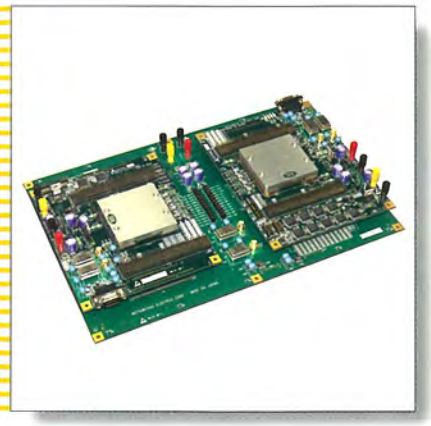
Changes for the Better

MITSUBISHI

三菱電機技報 Vol.82 No.5

2008 5

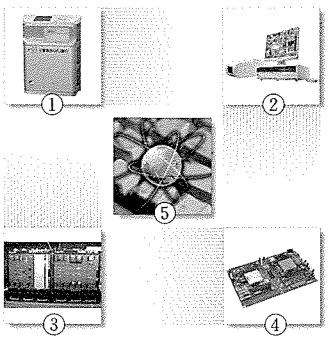
特集「情報セキュリティ技術」



ISSN　0369-2302／CODEN:MTDNAF

三菱電機技報 Vol. 82 No.5 2008

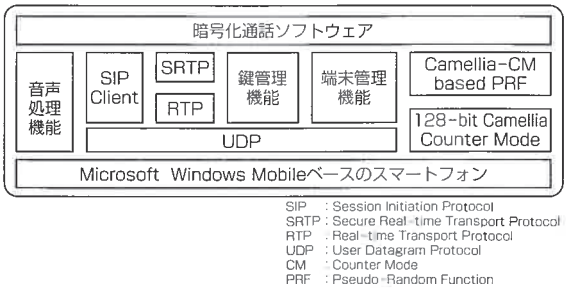
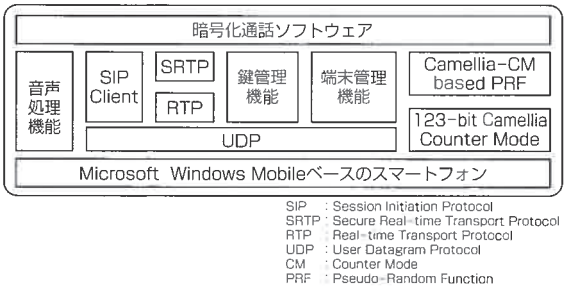
目　次



表紙：情報セキュリティ技術

この特集号の表紙では，情報システムの安全・安心を支える様々な情報セキュリティ技術を紹介している。コンビニ・ボックス・バンク端末は，わたしたちの日々の生活を安全で便利なものにしている(①)。監視カメラシステムは，安全・安心な生活環境づくりに貢献している(②)。また，新たな原理に基づき，解読不可能な暗号を追求していく取り組みとして，量子暗号通信システムの開発も行っている(③)。要素技術としては、物理攻撃に対する高い耐解読性を追求する取り組みの一つが，三菱電機が開発した暗号評価用プラットフォームSCAPEである(④)。当社は今後も，幅広い視点から安全・快適を実現する技術を提供していく。⑤はイメージ写真である。

三菱電機技報　2008年5月号　正誤表

該当箇所	46ページ，図5
正	 **図5．セキュア携帯電話端末のアーキテクチャ**
誤	 **図5．セキュア携帯電話端末のアーキテクチャ**

巻/頭/言

コンテンツについて思うこと

Some Notes on Contents

笠原正雄
Masao Kasahara

21世紀はコンテンツの世紀といわれて久しい。コンテンツは文化的，教育的，産業的，政治的側面を持っており，諸外国に伍(ご)してこの分野で成功するか否かが，我が国の将来を明るくするか否かの鍵(かぎ)を握っている。このように国家にとっても非常に大切な意味を持つ“contents”に対する日本語は何であろうか。英和辞書で調べてみると，中味，内容，目次…などとなっている。しかし日常使用している“コンテンツ”とは，かなりずれがある。大切なことは字義的にとらえるのではなく，その本質をとらえるべく努力することであろう。

コンテンツの本質を考えること。一見難しいことのように思えるが，答えは意外に身近なところに書かれている。例えば“万葉集”の中に，“信濃なる千曲の川の細石(さざれし)も，君し踏みてば玉と拾わん”という歌が詠まれている。美しい感性が胸を打つが，この歌は私達にコンテンツ(シンボル，メディア)のあるべき姿を教えてくれる。つまり，⑴女性の年令は10代後半と思われ，この年令から外れるほどコンテンツとしての細石は不適切なものになること(要件１：コンテンツの良否は観賞者の年令による)，⑵細石は女性の完全に自由な意思のもとに置かれてコントロールされるべきこと(要件２：コンテンツは個人のペースで観賞されるべきもの)，ということを教えている。

万葉の代表的な歌人，大伴家持の歌に“妹が見しやどに花咲き時は経ぬ我が泣く涙いまだ干(ひ)なくに”がある。亡くなった妹を想う家持の心が時を越えて私達の胸を打つ。しかし，この家持の歌を見て驚く人がいるかもしれない。何故なら家持よりも20年も前に山上憶良が“妹が見し棟(あふち)の花は散りぬべし我が泣く涙いまだひ干なくに”という歌を詠んでいるからである。二つの歌を見比べて，現代を生きる私達は著作権侵害？と考えるかもしれない。しかしこれは追和と言われる歌の形式であって，先人の詠んだ歌に美しい旋律がいつまでもこだまするように後世の人達が類歌を詠み，歌の心を伝えていくというものであって，著作権法とは無縁な美しい詩歌の世界なのである。

私の座右の書にシーザ父子に仕えた古代ローマの建築家ウィトルーウィウスが著した“建築書”がある。この本を紐(ひも)解いてみると，“紀元前３世紀エジプトの王プトレマイオスは，コンテンツの創出に全力を尽くし，その一環として詩文競技会を企画した。しかしある競技会で，一位，二位に入った二人の詩人の作品が盗作と判明し，厳しい処分がなされた。”とある。コンテンツは多様な側面を持つが，このような厳しい処分は，当時のプトレマイオス王朝ではコンテンツは政治的，教育的側面が強かったことを伺わせる。これに対し，万葉の時代では文化的側面が強かったと想像される。21世紀，コンテンツはどのような側面を強めるのであろうか。コンテンツの根源にかかわる国家的重要なテーマである。

細石がそうであったように，歌の世界ではシンボル(コンテンツ，メディア)は多くの場合，良きシンボルとして登場する。“このシンボルは良くないよ”という立場から読まれている例を万葉集の中に見出すことは非常に難しい。しかし，万葉の歌人の中でコミュニケーションの問題に大きな関心を寄せていたと思われる大伴家持の歌に“百千度(ももちたび)恋うというとも諸弟(もろと)らが練りの言羽は我は頼まじ”がある。坂上大嬢の愛の想いは，いくら練りに練った言葉で諸弟らによって伝えられてきても，それが伝言である限り良きシンボル(良きメディア)にはならないよ，こんなことを家持は主張している。

ところで，上記の歌にある言羽が言葉に改められたのは平安中期の柱本によるが，家持は言葉は散り落ちる葉っぱではなく，未来社会に向かって永遠に羽ばたきつづけるもの・・・と考えていたに違いない。

以上述べてきたように，コンテンツの本質について万葉集等の身近な存在から，その一端を知ることができる。

近年とみに重要性を増している“情報倫理”の本質も，身近にあるものから鮮やかに見えてくる。情報技術書，又は哲学書等では決して見えなかったことが鮮やかに見えてくる。不思議なことである。

◆大阪学院大学 情報学部 教授　Professor, Faculty of Informatics, Osaka Gakuin University

巻頭論文

暗号技術の現状と将来展望

松井　充*

Technology Trends and Future of Cryptographic Algorithms

Mitsuru Matsui

要　旨

暗号技術は，個人のプライバシー保護や企業機密保護に欠かせない要素技術として，幅広くIT製品やITシステムに利用されている。直接的に見えることは少ないものの，今では暗号をまったく使わずにわれわれが一日を過ごすことが困難とすら言える時代になった。

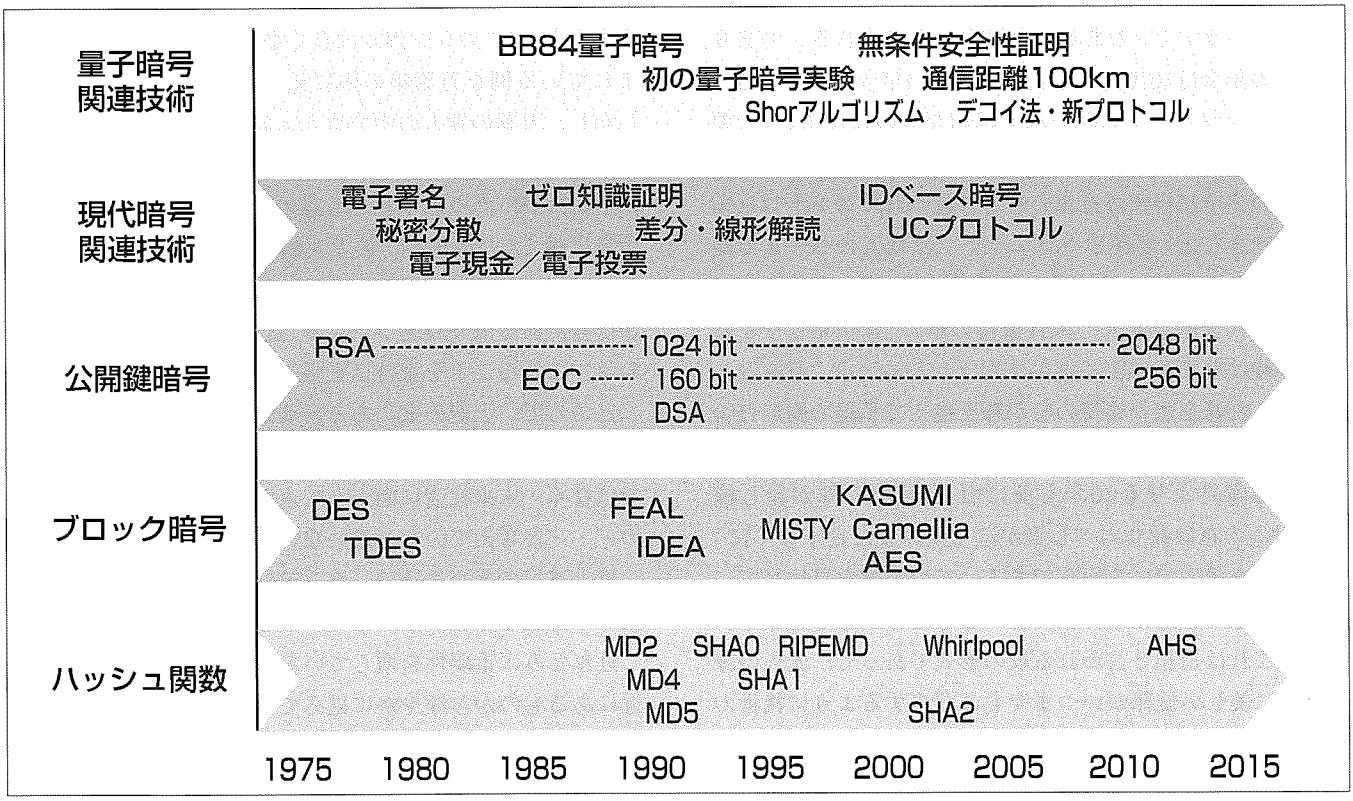
暗号技術を支える暗号アルゴリズムは，その機能に応じて共通鍵(かぎ)ブロック暗号，ハッシュ関数，公開鍵暗号など様々なタイプに分類されるが，それぞれのアルゴリズムはシステムの中で役割分担を行いながら有機的に結合され，情報通信の安全性を支えている。

三菱電機では，1995年以降“MISTY”や“Camellia(NTTとの共同開発)”に代表される共通鍵ブロック暗号を設計し，その仕様を公開するとともに，国内外の標準化に提案する活動を推進した結果，現在ではこれらの暗号アルゴリズムはISO(国際標準化機構)で世界標準に採用されるに至っている。

一方で，暗号アルゴリズムの安全性評価を目的とする解読研究の進歩もめざましい。最近ではハッシュ関数など，現在広く利用されている暗号方式の一部に将来的な安全性の懸念が示され，このため世界的に現方式から新方式への移行が進みつつあるのもまた事実である。

このような背景のもと，本稿では暗号アルゴリズムの安全性の最新状況を，実用的な観点からまとめるとともに，暗号利用に対する将来への指針を与えることを最初の目標とする。またIDベース暗号や量子暗号など最近特に注目を集めている新しい暗号技術の潮流についても概観する。

暗号は数学的安全性だけでなく，そのソフトウェアやハードウェアへの実装上の安全性も実システムでは考慮されなければならない。この点で暗号技術と物理学との接点が広がってきたと言えるであろう。



暗号技術と暗号アルゴリズムの歴史

1970年代半ばに発明されたDES(Data Encryption Standard)暗号とRSA(Rivest，Shamir，Adleman)暗号が現代暗号の幕開けであった。この図はそれ以降の主要な暗号アルゴリズムや暗号関連技術に関する発展を示したものである。公開鍵暗号については鍵長で変遷を示している。RSA暗号の鍵長は2010年以降徐々に2048ビットが主流になると考えられている。またハッシュ関数については現行のSHA(Secure Hash Algorithm)シリーズにかわる新標準AHS(Advanced Hash Standard)が2012年ごろ米国で制定される見通しである。

*情報技術総合研究所 情報セキュリティ技術部長(情報理工学博士)

1. まえがき

暗号技術がわれわれの身近なところで使われるようになってすでに久しい。今では，携帯電話・キャッシュカード・鉄道乗車券・モバイルパソコン・自動車の電子キーなど，われわれの鞄の中には暗号がいくつも入っている。だれもが知らず知らずのうちに日常的に暗号を利用する時代になった。

この背景には，暗号の利用目的が，情報を隠すための“秘匿”から，なりすましを防止するための“認証”や情報の改ざんを防止するための“完全性”に広がったことや，プロセッサやデバイスの低消費電力化・高速化によって，暗号アプリケーションの可能性が大きく広がったことがある。

一方で，暗号技術の進歩は暗号解読技術の進歩でもある。学会では，現在利用されている暗号方式に問題がないかを検証する目的で，暗号解読の研究が日夜行われている。暗号解読技術の進歩こそが暗号技術の進歩であるというのが，暗号研究者のコンセンサスである。

アカデミズムは暗号アルゴリズムに対し，普遍的でかつ極めて高い安全性を要求する。したがって学術的な意味での解読と，特定のアプリケーションでの実際的な意味での解読の可能性との関係は必ずしも自明ではない。この橋渡しが企業における暗号研究者の重要な役割の一つである。

最近になって，現在広く用いられているいくつかの暗号方式について，その危殆(きたい)化，すなわち安全性の低下の可能性が指摘されており，2010年以降の暗号利用に影響が出るといわれている。いわゆる“暗号の2010年問題”であり，世界的に議論されているものである。

このような背景のもと，本稿では，現在われわれの身近で利用されている暗号方式を中心に，その安全性評価の現状について実際的な観点から述べるとともに，最近注目されている新しい暗号技術の概要と，利便性と安全性の観点からその意義についてまとめてみたい。

2. ハッシュ関数の安全性

2.1 ハッシュ関数

ハッシュ関数(Hash Function)は，パスワードの暗号化・電子署名・乱数生成など，極めて多くの応用を持つ暗号のコンポーネントである。暗号用途を明確にするために暗号学的ハッシュ関数(Cryptographic Hash Function)とも呼ばれることもある。

ハッシュ関数は任意長のデータを入力として受けつけ，これを“圧縮”して固定長のハッシュ値を生成する機能を持つ。ハッシュ関数の安全性の要件のうち重要なものとして，一方向性(Onewayness)と耐衝突性(Collision Resistance)がある。一方向性とは出力から入力を逆算することが難しいこと，また耐衝突性とはハッシュ値が同じになるような，異なる2つの入力メッセージを具体的に見つけ出すことが困難なことを意味する。

図1に電子署名におけるハッシュ関数の利用例を示す。署名者はメッセージをハッシュ関数で処理してから秘密鍵演算を実行する。この場合ハッシュ関数の衝突が計算可能，すなわちHash(M)=Hash(M')なる異なる2つのメッセージM，M'が計算できるということは，検証者にとって電子署名がMのものかM'のものか区別できなくなることに相当するため，耐衝突性はハッシュ関数にとって生命線ともいえる重要な性質である。

2.2 ハッシュ関数の例

現在もっとも広く利用されているハッシュ関数は，米国政府標準のSHA1[(1)]である。SHA1が制定されるまでは，MD(Message Digest)シリーズと呼ばれるMD4やMD5が広く用いられており，現在でも一部のアプリケーションではMD5が互換性目的で用いられている。ただしこの章で述べるようにMDシリーズの利用は安全性上推奨できない。

SHA1のハッシュ長は160ビットであるが，これより長いハッシュ長を持つSHA2と呼ばれる新しい米国政府標準もその後制定されている。SHA2はいくつかのハッシュ関数の総称であり，個々のアルゴリズムはハッシュ長を名称につける形でSHA256，SHA384，SHA512などと呼ばれている。

2.3 ハッシュ関数の安全性問題

一般にハッシュ長がnビットであるハッシュ関数の衝突は，$2^{n/2}$の計算量で見つけられることが知られている。したがってハッシュ関数の安全性の上限は$2^{n/2}$ということになる。しかしながら最近になって，いくつかのハッシュ関数はこれ以下の計算量で衝突を求められることが判明し，特にMD4やMD5は実際に衝突の例が報告されるようになった[(2)]。SHA1についても，衝突は報告されていないものの，1～2年の間には見つかるのではないかといわれている。

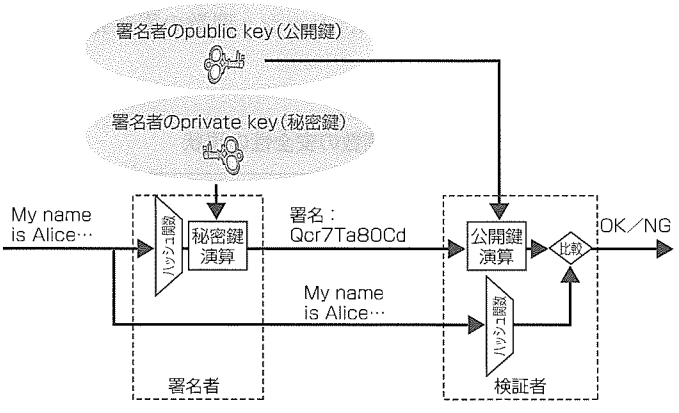


図1．電子署名におけるハッシュ関数の利用例

表1はハッシュ関数の安全性の現状をまとめたものである。ここで段数とは，ハッシュ関数内部の基本関数の繰り返し回数を示したものである。MD4やMD5は簡単に衝突が見つけることができるため，アプリケーションによっては，なりすましや改ざんが可能になることが実際に起こりうるので注意が必要であり，できる限りこれらのハッシュ関数は利用しないことが望ましい。

SHA1については，衝突を求めるための計算量が2^{63}程度であるという報告がなされており[3]，これは本来あるべき計算量2^{80}に比べて10万分の1である。またSHA1の初期バージョンであるSHA0については，アルゴリズムのドキュメント上SHA1と1行しか異ならないにもかかわらず(具体的にはSHA1は数値の回転シフト操作が一回だけ多い)，すでに簡単に衝突が見つかる状態であることを考え合わせると，SHA1の危殆化は無視できないといえる。

一方SHA2については，いずれのアルゴリズムも現時点で衝突が見つかる可能性があるといった報告はなされておらず，学術的な意味でも問題がないといってよい。

2.4 ハッシュ関数の今後

米国政府の情報処理標準を制定しているNIST(National Institute of Standards and Technology)は，電子署名目的でのSHA1の利用を2010年で打ち切ると発表しており，現在SHA1からSHA2へのシフトが急速に進んでいる。またSHA2に安全性の問題はないものの，その構造がSHA1と類似していることから，長期的には新しい構造をもったハッシュ関数を標準化すべきとの意見も存在する。

このため米国NISTでは，SHA2の次の世代の政府標準暗号AHSを選定するためのプロジェクトを2008年に開始する予定であり，新標準制定は2012年ごろの計画である。したがってSHA2の利用はそれまでのつなぎという位置づけになる可能性が高い。

SHA1の衝突が一つ発見されることによって安全性が現実的な意味で脅威にさらされるアプリケーションはほとんどないと考えてよいが，電子署名のように長期間にわたって有効性を保証しなければならないシステムでは新ハッシュ関数への移行は必要である。

このように実システムでは，ハッシュ関数の衝突発見による影響の有無と，システムやデータの有効期間の点から移行の要否を判断することが望まれる。

3. 公開鍵暗号の安全性

3.1 RSA暗号

RSA暗号は1970年代半ばに発明された，最も古い公開鍵暗号の一つであるとともに，その誕生から今に至るまで，常に最も広く用いられている公開鍵暗号でもある。その安全性は，素因数分解問題の困難性に基づいており，鍵の長さ(＝合成数の長さ)を長くすると指数的に解読は困難(＝素因数分解は困難)になると考えられている。

現在RSA暗号は1024ビットの鍵長で用いられることが普通であり，特に重要なシステムで2048ビット以上の鍵が用いられることもある。1024ビットの合成数の素因数分解に必要な計算量はおよそ2^{80}，すなわち80ビット鍵の共通鍵暗号や160ビットのハッシュ長をもつハッシュ関数の安全性と同程度と考えられている。

RSA暗号では，暗号化や復号に必要な計算量は鍵の長さの3乗に比例する。すなわち鍵の長さを2倍にすると演算量が8倍になる。またRSA暗号では，鍵生成のたびごとに素数を生成しなければならず，この計算量は一般に鍵の長さの4乗に比例する。したがって速度が要求されるアプリケーションや，電子証明書を大量に発行するようなシステムでは，鍵の長さが全体の性能に与える影響は極めて大きい。

3.2 RSA暗号の安全性の現状

素因数分解に必要な計算量の下限は知られておらず，またそれが指数時間必要であることすら数学的には証明されていない。しかしながら素因数分解問題は長い歴史を持つ数学上の問題であり，これまでの研究結果からも，それが多項式時間で実行可能であるとは考えられていない。

このような評価は漸近的な評価，すなわち鍵を長くすると安全性が飛躍的に高まっていくことを示すものであり，鍵を一定長に固定したときの素因数分解の計算時間について保証するものではない。個別の合成数の素因数分解の可能性については，研究者が多数の計算機を用いた実験を続けており，表2に示すように，次々と記録が塗り替えられている。現在の世界記録は640ビットである[4]。

表1．ハッシュ関数の安全性の現状

	ハッシュ長	ブロック長	段数	標準	衝突
MD4	128bit	512 bit	48	RFC1320	×
MD5	128bit	512 bit	64	RFC1321	×
SHA0	160bit	512 bit	80		×
SHA1	160bit	512 bit	80	FIPS180-2 ISO10118	△
SHA256	256bit	512 bit	64	同上	○
SHA512	512bit	1024bit	80	同上	○

× すでに衝突が多数見つかっている
△ 衝突が近い将来見つかる可能性が高い
○ 衝突が見つかる兆候は見られない

表2．素因数分解の世界記録の歴史

合成数のビット数	素因数分解がアナウンスされた日
430	1996年4月10日
463	1999年2月2日
512	1999年8月22日
530	2003年4月1日
576	2003年12月3日
633	2005年5月9日
640	2005年11月2日

これらの結果から，1024ビットの合成数がいつ素因数分解されるかを予想することは容易ではないが，もっとも早い場合で2015年位ではないかとの予測もある。このため，ハッシュ関数の場合と同じく，電子署名などで長期にわたる証拠性を確保する必要があるようなアプリケーションでは，RSA暗号の鍵長を2048ビットに移行することが推奨されているのが現状である。

ただし先に述べたように，RSA暗号の鍵長を倍にすることは，アプリケーションの速度への影響が極めて大きいので，その移行は必ずしも容易ではない。次に述べるように，暗号処理の結果の有効性を延長するようなメカニズムで対処することが実際には重要になると思われる。

3.3 長期署名

ハッシュ関数やRSA暗号の危殆化でもっとも影響を受けるのが電子署名アプリケーションであると考えられている。一方で暗号アルゴリズムが危殆化することは，長い目で見ればある程度やむを得ないことであり，暗号アルゴリズムではなく，アプリケーション側で危殆化に対処するメカニズムを作っておくことは当然ながら重要である。

電子署名におけるそのような取り組みの一つが長期証明と呼ばれる技術であり，これは電子証明書が何らかの理由で失効した(例えば期限切れ，秘密鍵の漏洩(ろうえい)，暗号の危殆化など)あとも，証明書作成時の電子署名の有効性を保証することを目的としたものである。

最近JISで標準化が完了した長期署名フォーマットでは，危殆化していない暗号アルゴリズムによるタイムスタンプを付与し続ける間，最初の署名の有効性を延長できる仕組みが取り込まれており[5][6]，今後幅広い分野で利用されることが期待されている。

3.4 IDベース暗号

IDベース暗号(Identity-Based Encryption)は，任意の情報を公開鍵に設定することができる公開鍵暗号であり，その概念提唱は1984年にさかのぼる。その後長らく安全なIDベース暗号の構成は未解決問題であったが，2000年前後についに決定版とも言うべき，実用的で安全性が証明された方式が発明され[7][8]，以来世界中で研究開発が活発に行われている。

表3はRSA暗号，楕円曲線暗号，IDベース暗号それぞれについて，公開鍵と秘密鍵の関係を示したものである。RSA暗号や楕円曲線暗号は公開鍵が関係式の左辺に現れるのに対して，IDベース暗号は秘密鍵が左辺にあり，任意の公開鍵から計算できる関係になっているところが本質的である。このような関係式が25年間だれも発見できなかったのである。

表3．公開鍵暗号における公開鍵と秘密鍵の関係

	公開鍵	秘密鍵	公開鍵と秘密鍵の関係
RSA暗号	N	p，q	N=p×q (p，qは素数) →Nを任意の値には設定できない
楕円曲線暗号	y	x	y=x・P (・は楕円曲線のスカラー倍演算) (Pは共通の公開情報) →yを任意の値には設定できない
IDベース暗号	y	x	x=s・y (・は楕円曲線のスカラー倍演算) (sはセンターだけが知る秘密) →yを任意の値(=ID)に設定できる

現在広く用いられているPKI(Public Key Infrastructure)のフレームワークで利用されている電子証明書は，公開鍵とその所有者の関係を保証することでなりすましを防止することがその目的の一つであったのに対し，IDベース暗号では所有者の情報を公開鍵そのものの中に埋め込めるため，証明書がなくてもなりすましを防止することができるという画期的な特長を持っている。

一方でPKIの枠組みは標準化されて久しく，法的根拠も備わっており，われわれの生活の中に深くとけこんでいるうえ，証明書には失効のメカニズムが備わっていることもあり，IDベース暗号はPKIのライバルというよりも，アプリケーションによって役割分担がなされるのが将来の姿である。まだIDベース暗号を用いた製品は少ないが，高速化に向けた研究開発も急速に進展しており，組み込み系への応用も期待される。

4. 暗号と物理学の融合

4.1 サイドチャネル攻撃と暗号の安全性

暗号製品の小型化と一般への普及に伴い，暗号アルゴリズムの数学的安全性だけでなく，暗号の実装方法の安全性にも関心が集まっている。特にこれまで暗号研究の分野では研究対象となってこなかったような，通常の通信路以外から漏洩する情報や物理現象(サイドチャネル情報)を利用して秘密情報を推定するといった方法が暗号研究の一分野として確立されるまでになっている。

このような解読手法は，場合によっては暗号製品の脆弱(ぜいじゃく)性に直結するだけに，研究者だけでなく，半導体をはじめハードウェアベンダーの関心が高く，関連する研究会への参加者も急激に増加している。

有力なサイドチャネル情報としては，ソフトウェアでは，データに依存して実行時間が変化するメモリアクセス命令や分岐命令を利用するものが有力であり(タイミング攻撃)，ハードウェアでは，デバイスの消費電流を観測して内部の鍵情報を推定する方法(電流攻撃)が広く知られている。このほかにもシステムのエラーメッセージを利用するものや，意図的に一時的なエラーをデバイスに起こし，その場合のハードウェアの動作を観測するといった方法も提案されている。

これらサイドチャネル攻撃の研究から得られる教訓は，暗号実装はただ仕様どおりに行っただけでは不十分であり，慎重な実装が必要であるが，同時にサイドチャネル情報が

解読者に入手できないかぎり攻撃は不可能であるので，現実的な視点から，真に必要な対策を特定して，それを確実に行わなければならないということである。

なお暗号モジュールのセキュリティ要件を定めた米国政府標準の最新版ドラフト[9]では，タイミング攻撃や電流攻撃に対する安全性が要求されている。

4.2 量子暗号技術

単一光子に情報を載せて伝送する量子暗号は，量子物理学の法則で安全性が証明された解読不可能な“究極の暗号”として，各国で開発競争が行われている。最近では100kmに達する光ファイバを用いた量子暗号通信実験が行われており，また伝令つき単一光子源や超伝導を用いた単一光子受信機の開発など，高性能化への取り組みも急速に進歩している。

図2は現代暗号と量子暗号の安全性の関係を図示したものである。量子計算機が実現されると主要な公開鍵暗号が多項式時間で解読されてしまうのに対して，量子暗号は計算機では決して解読されることがない。一方で共通鍵暗号まで量子計算機で解読が容易になるかどうかは知られていないことに注意すべきである。

単一光子で安全性が保証される量子暗号であるが，実際には現在の技術では単一光子生成も単一光子受信も完全には行うことはできない。また量子暗号の安全性評価では，敵は物理法則に違反しないかぎり何でもできるとの前提をおくので，攻撃のシナリオも様々である。このような状況まで考慮した量子暗号の“厳密な”安全性評価は，現在でも活発に行われている研究分野である。

量子暗号で実用レベルで実現されているプロトコルは，今のところEnd-to-Endでの鍵共有がそのすべてであり，また量子暗号単体での鍵共有スピードは現代暗号には遠く及ばないため，量子暗号は共通鍵暗号と組み合わせて利用するのが効果的といえる。近い将来，新しいネットワーク型量子プロトコルの発明によって量子暗号の応用範囲が一気に広がることが予想される。

国内では光ファイバベースの量子暗号が中心であるが，海外では，衛星通信への応用を視野に入れ，光無線量子暗号実験も幾つか行われており，最近では144kmの実験に成功したとの報告もある[10]。この分野での今後の発展も大いに期待できるところである。

5. むすび

アルゴリズムの安全性の現状と，今後期待される暗号技術について具体例を挙げながら述べた。当社ではブロック暗号の開発をはじめ，公開鍵暗号，PKI構築，標準化への参画など暗号技術に関する網羅的取り組みを進めるとともに，暗号実装や量子暗号の分野にも長年注力している。

本稿で挙げた個々の技術への取り組みについては，この特集号の各論文で採りあげているので，詳細についてはそちらを参照されたい。

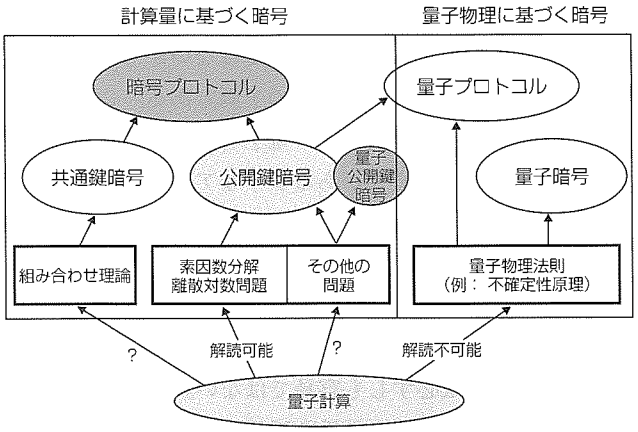


図2．現代暗号と量子暗号の安全性

参考文献

(1) Secure Hash Standard, FIPS Publication 180-2, NIST (2002)

(2) Wang, X., et al.：Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD, Cryptology ePrint Archive 2004/199 (2004)

(3) Wang, X., et al.：New Collision Search for SHA-1, at the rump session of CRYPTO2005 (2005)

(4) RSA-640 is factored, RSA laboratories homepage, http://www.rsa.com/rsalabs/node.asp?id=2964

(5) CMS利用電子署名(CAdES)の長期署名プロファイル, JIS X 5092 (2008)

(6) XML署名利用電子署名(XAdES)の長期署名プロファイル, JIS X 5093 (2008)

(7) 大岸聖史，ほか：楕円曲線上のID鍵共有方式の基礎的考察，ISEC99-57 (1999)

(8) Boneh, D., et al.：Identity based encryption from the Weil pairing, CRYPTO2001 (2001)

(9) DRAFT Security Requirements for Cryptographic Modules, FIPS Publication 140-3 (2007)

(10) Manderbach, T., et al.：Experimental Demonstration of Free-Space Decoy State Quantum Key Distribution over 144km, PRL98 (2007)

IDベース暗号アルゴリズムと暗号メールシステム

高島克幸*
坂上　勉*

Identity-Based Encryption Algorithm and Mail System

Katsuyuki Takashima, Tsutomu Sakagami

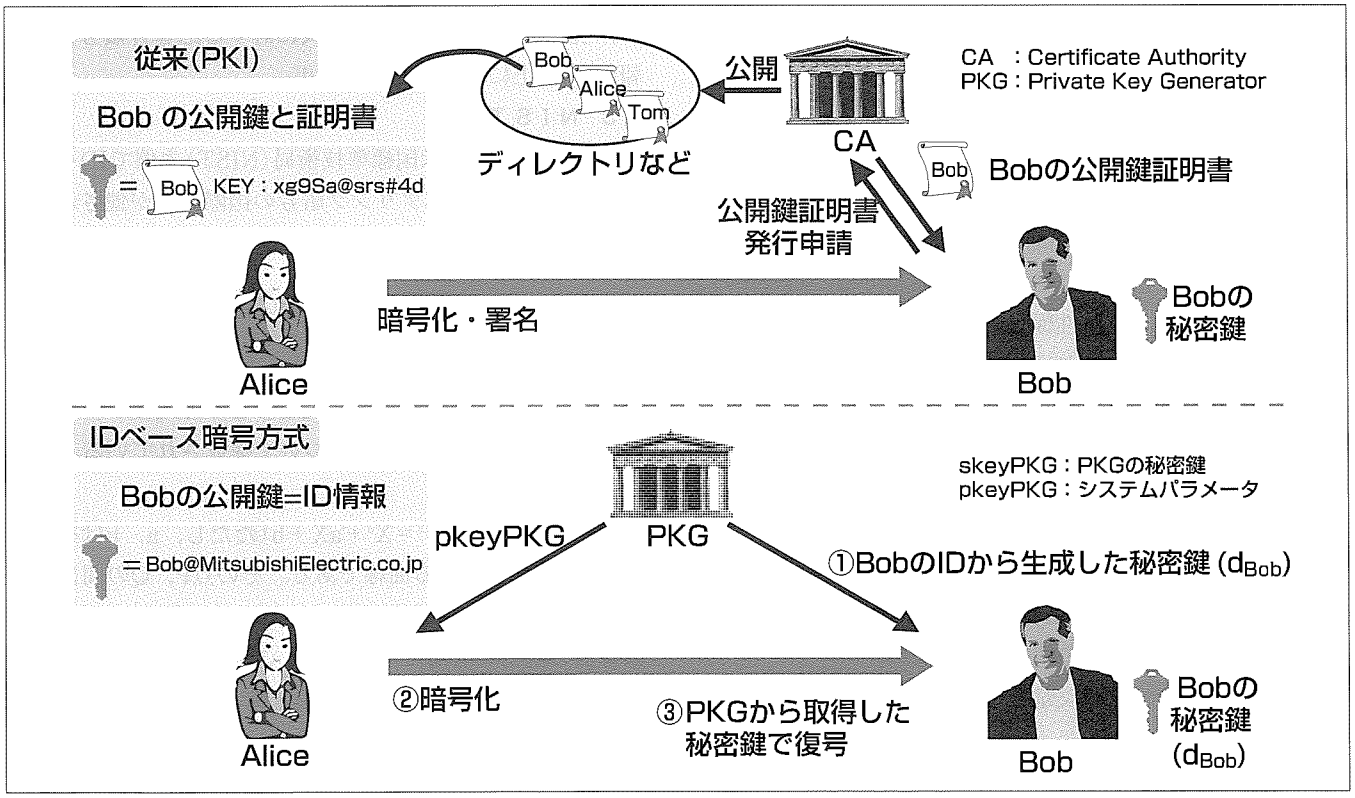
要　旨

情報漏洩(ろうえい)防止のために，暗号機能／機器を導入するのが有効であることは周知であるが，その簡便な導入を可能にする技術がIDベース暗号と呼ばれる暗号技術であり，三菱電機でも積極的に，その研究開発を行っている。IDベース暗号は，ID情報を公開鍵(かぎ)にすることができる公開鍵暗号技術であり，実用的な方式が最近になって初めて提案されたにもかかわらず，その有用性のために，それ以後，IETF(Internet Engineering Task Force)，IEEE(Institute of Electrical and Electronics Engineers)，ISO(International Organization for Standardization)といった各種団体での標準化が急速に進められている。

通常，公開鍵暗号では，暗号化の際に用いる公開鍵の正当性保証のために，公開鍵証明書というデータを用いる。これは，公開鍵と利用者を結び付けるための署名付きのデータである。IDベース暗号では，IDを公開鍵にできるため公開鍵証明書を用いる必要がなく，便利な方式であり，今後，PKI(Public Key Infrastructure)との共存を図りながら，多様なセキュリティニーズに対応できる方式として注目されている。

現在の情報通信技術は，およそ考えられるすべてのものに番号(ID)を割り振り，管理することを可能としたが，その番号体系を利用し，機器認証／管理を行う手段をIDベース暗号は与える。それによって，今後一層複雑化する情報空間での安全性を確保するとともに，従来人手で管理されてきた物／情報を，現在よりはるかに大きいスケールで安全に管理することが可能になる。

本稿では，そのように近年注目されているIDベース暗号技術について，我々が取り組んでいる基盤技術である暗号アルゴリズム改良提案と，それを用いた暗号メールシステムの試作について述べる。



IDベース暗号を適用した暗号メールシステム

IDベース暗号を適用した暗号メールシステムでは，AliceからBobへ暗号通信を行う場合，①BobはBobのIDから生成した秘密鍵をIDベース鍵生成サーバ(PKG)から取得し，② Aliceはシステムパラメータと Bobの IDを使ってメッセージを暗号化し送信し，③それを受け取ったBobは，PKGから取得した秘密鍵でメッセージを復号する。AliceはBobのIDを公開鍵にして暗号メール通信を行うことができ，公開鍵証明書を必要としない。

*情報技術総合研究所

1. まえがき

近年，任意のID情報を公開鍵に使用することができるIDベース暗号が注目されている。IDベース暗号の概念自体は，1984年にShamirによって提唱されているが[1]，その実現は長い間未解決のままであった。それは1999年の境・笠原IDベース鍵共有[2]，2001年のBonehらによる安全性証明付きのIDベース暗号の発表[3]で解決された。そこでは，楕円曲線上のペアリング演算が重要な役割を果たしている。本稿では，**2～4章**でIDベース暗号の技術的概略及び標準化動向を述べたあと，**5章**で我々が開発した効率的なペアリング演算法について，更に，**6章**では試作した暗号メールシステムについて述べる。

2. IDベース暗号

2.1 IDベース暗号方式

IDベース暗号では，任意のIDに対する秘密鍵を生成するIDベース鍵生成サーバPKG(Private Key Generator)が必要である。PKGで用いられる“パラメータ生成関数”及び“秘密鍵生成関数”と，利用ユーザーで用いられる“暗号化関数”及び“復号関数”という4個の関数から構成される。

(1) パラメータ生成関数：鍵のビット長を入力とし，システム全体で用いられるシステムパラメータとPKGの秘密鍵を出力する。

(2) 秘密鍵生成関数：IDとシステムパラメータ，PKGの秘密鍵を入力とし，IDの秘密鍵を出力する。

(3) 暗号化関数：平文とシステムパラメータ，IDを入力とし，暗号文を出力する。

(4) 復号関数：暗号文とシステムパラメータ，IDの秘密鍵を入力とし，平文を出力する。

ここで注意すべきは，暗号化関数の入力IDが公開鍵となっていることである。通常，公開鍵暗号では，暗号化の際に用いる公開鍵の正当性保証のために，公開鍵証明書というデータを用いる。これは，公開鍵に対する署名である。IDベース暗号では，IDを公開鍵にできるため公開鍵証明書を用いる必要がなく，便利な方式となっている。

IDベース暗号が機能するには，上記4関数に対して，次の2条件が満たされることが要求される。

(1) 正しく作成された暗号文を復号すれば，元の平文に戻る。

(2) ID_i以外のIDに対応する秘密鍵を用いても，ID_i宛ての暗号文から，一切平文の情報が漏れない。

2番目の条件は，結託攻撃を考慮した安全性要件になっている。

2.2 鍵カプセル化方式

IDベース暗号は，**1章**で述べたように，実現されてまだ数年であるが，**3章**で述べるようにIETF，IEEE等ですでに活発に標準化が行われている。そこでは，鍵共有のための鍵カプセル化方式(KEM)として定められている場合が多い。IDベースKEMも，**2.1節**のIDベース暗号と同様，4つの関数群からなる。パラメータ生成関数及び秘密鍵生成関数は**2.1節**と同様であるが，暗号化関数及び復号関数は次のように，“鍵カプセル化関数”及び“鍵デカプセル化関数”になる。

(1) 鍵カプセル化関数：システムパラメータとIDを入力とし，送信者-受信者間の共有鍵と，その共有鍵の暗号化を出力する。

(2) 鍵デカプセル化関数：共有鍵の暗号化とシステムパラメータ，IDの秘密鍵を入力とし，共有鍵を出力する。

鍵カプセル化関数では，平文に該当する入力がなく，それに該当する共有鍵が出力されていることが特徴的である。

3. 標準化へ向けた動き

この章では，IETF，IEEE，NIST(National Institute of Standard and Technology)によって行われている標準化へ向けた動きについて述べる。

3.1 IETF

2007年末に，楕円曲線上のペアリング演算に基づいたIDベース暗号がRFC 5091として策定された[5]。ほかにも関連ドラフトが公開されている[6][7]。

3.2 IEEE

IEEE P1363.3で，楕円曲線上のペアリング演算に基づいたIDベースの暗号／KEM，署名，鍵共有法の策定作業が，現在進行中であり，各方式に対する応募書類も含む情報がWEB上に掲載されている[4]。

3.3 NIST

2008年6月に，米国標準技術局(NIST)主催でIDベース暗号を中心にしたペアリング暗号の国際会議が催される予定である。

4. 楕円曲線上の演算

2章のIDベース暗号を実現するために，様々な方式が提案されているが，現実的に使用できる方式はすべて楕円曲線上のペアリング演算に基づいて構成されている。

4.1 加算，2倍算

楕円曲線Eとは $Y^2=X^3+aX+b$(ただし，a，bは有限体の要素)で与えられる曲線である。その点P，Qの間には代数的な加法P＋Qが定義されている。**4.3節**のペアリング演算法の説明に有用であるので，ここでその演算法を**図1**を用いて説明する。まず，PとQを結ぶ直線lの方程式を計算する。そして，Eとlの第3の交点を求める。その点を通るy軸に平行な直線vとEの第二の交点を求める。これがP＋Qである点Rである。2倍算は，P＝Qの場合であり，lがPでのEへの接線になる以外は加算の場合と同様に計算する。

4.2 スカラー倍算

加算に基づくスカラー倍算は，

$$k \cdot P = \underbrace{P + \quad \cdots \quad + P}_{k回}$$

で定義される基本的な演算であり，従来の楕円曲線暗号は，もっぱらスカラー倍算を用いてきた。また，十分大きい素数rに対し，r倍すると，加法の零元になるEの点全体を使用して暗号化処理がなされる。

4.3 ペアリング演算

さらに，最近，有用な演算となっているのが，E上でのペアリング演算である。つまり，2点に対し，e(P，Q)という有限体の要素が対応する写像である。ここでは，特にTateペアリングeとよばれているものを扱う。ここで，

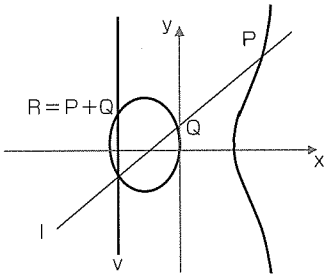


図1．楕円曲線：$y^2=x^3-x$

アルゴリズム 1　Miller アルゴリズム
入力： 楕円曲線上の点 P, Q.
出力： Miller 変数値.
1: 適当な楕円曲線上の点 S を選ぶ.
2: $Q' \leftarrow Q+S, T \leftarrow P$.
3: $i \leftarrow \lfloor \log_2(r) \rfloor - 1, f \leftarrow 1$.
4: while $m \geq 0$ do
5: T を2倍するための直線 l と v を計算.
6: $T \leftarrow 2T$.
7: $f \leftarrow f^2 \frac{l(Q')v(S)}{v(Q')l(S)}$.
8: if r の i 番目のビットが1 then
9: T と P を加算するための直線 l と v を計算.
10: $T \leftarrow T+P$.
11: $f \leftarrow f \frac{l(Q')v(S)}{v(Q')l(S)}$.
12: end if
13: $i \leftarrow i-1$.
14: end while
15: f を出力.

図2．Millerアルゴリズム

IDベース暗号に最も重要なペアリングeの性質は，双線型性と呼ばれる次の性質である。

$$e(uP, vQ) = e(P, Q)^{uv}$$

この双線型性によって，IDベース暗号をはじめとする各種暗号応用技術が実現されている。このスカラー倍算とペアリング演算を用いて，2章のIDベース暗号が実現される。

5. ペアリング演算アルゴリズムの改良

ペアリング計算は，大きくMillerアルゴリズムと最終べキ乗算とで構成されており，Millerアルゴリズムの効率化が，そのパラメータ選択法と関連して多く研究されている。

図2に示すアルゴリズム1が一般的なMillerアルゴリズムである。本稿では，詳細な説明は省略するが，**4.1節**にある加算・2倍算アルゴリズム中に現れる直線l，vを用いて計算されていくことをアルゴリズム1は示している。

このようなアルゴリズムの効率化に関する研究は多く報告されているが，我々は，Scottによって提案された方式を，安全性が柔軟に変更可能な方式に拡張した[9]。そこでは，高速化が図れる曲線として，$Y^2=X^3+b$，ただし，有限体の位数として$p \equiv 1 \bmod 3$なるpを用いている。この曲線は，1の3乗根βによって，$(x, y) \rightarrow (\beta x, y)$という作用を持っており，それを利用して高速化を図ることができる。

6. 暗号メールシステムの試作

IDベース暗号を使用した暗号メールシステムを試作した(図3)。開発したのはIDベース鍵生成サーバPKGと，利用ユーザーが暗号メールの送受信に使用する暗号メールクライアントである。試作したシステムによって，公開鍵証明書の管理やパスワードの事前共有を行うことなく，暗号メールの送受信を行うことが可能である。次にその実装内容について述べる。

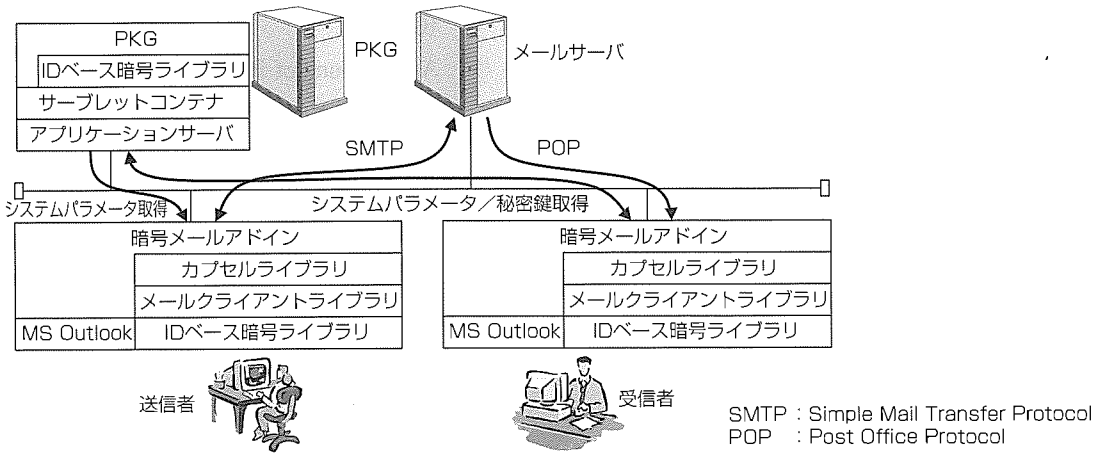


図3．試作したIDベース暗号メールシステムの構成

6.1 PKG

IDベース暗号でPKGはシステムの要(かなめ)と言えるものである。利用ユーザーに対するシステムパラメータpkeyPKGの配布や，利用ユーザーの秘密鍵の生成など，IDベース暗号システム全体の動作に不可欠な機能を受け持っている。今回の実装では，ファイアウォールやプロキシサーバの存在など近年の企業ネットワーク環境を考慮し，暗号メールクライアントからPKGへアクセスするためのプロトコルとしてhttp(HyperText Transfer Protocol)／https(http Security)を採用した。その上で，http／https上で暗号メールクライアントとPKGが複雑な構造を持つデータのやり取りを行う必要性を考慮して，アプリケーション間通信を行うプロトコルとしてSOAP(Simple Object Access Protocol)を採用することとした。下位プロトコルがhttp／httpsであるため，PKGの実装はWEBベースのアプリケーションサーバ上に行うこととし，サーブレットとして実装した。

6.2 暗号メールクライアント

暗号メールクライアントとしては，アドインを利用して機能拡張が可能であることや，我々が過去に機能拡張を行った実績などからOutlook2003(注1)を採用することとした。下位のライブラリ部分はC／C++で，上位のGUI(Graphical User Interface)関連の部分はVB(Visual Basic)で記述されている。

6.3 PKG−メールクライアント間通信データ

PKGとメールクライアント間の通信データは，下位プロトコルとしてSOAP over http/httpsを採用したこともあり，XML(eXtensible Markup Language)でデータフォーマットを定義している。

6.4 暗号メールデータ

暗号メールクライアントから送信される暗号メールのデータ形式としては当社独自のカプセル形式を採用した。カプセル形式は，データの暗号化だけでなく受信側でのデータに使用制限(印刷可否，切り貼り可否など)を行うことができる，従来当社情報技術総合研究所で研究してきたデータ形式である。

6.5 今後の展望

IDベース暗号は新しい暗号方式であるため，例えばPKGからクライアントにシステムパラメータを配布する方法や，PKGからクライアントに秘密鍵を渡す方法などの規格はIETFで検討中であり，まだ決まっていない。IETFでは暗号メールのデータ形式としてS/MIME(Secure/Multipurpose Internet Mail Extension)で採用されているCMS(Cryptographic Message Syntax)をベースに，IDベース暗号用のデータ形式を加える方向で検討が行われている。今回は独自方式で実装したが，今後IETFの規格化への提案，規格に準拠するための開発を行っていきたい(**3.1節**)。

(注1) Outlookは，Microsoft Corp.の登録商標である。

7. むすび

ID情報を公開鍵にでき，公開鍵暗号機能の簡便な導入を可能にするIDベース暗号について，改良アルゴリズム提案と暗号メールシステムの試作について述べた。

参考文献

(1) Shamir, A.：Identity−based cryptosystems and signature schemes, Crypto 84, LNCS No.196, Springer Verlag, 47〜53 (1985)

(2) 大岸聖史，ほか：楕円曲線上のID鍵共有方式の基礎的考察，電子情報通信学会 技術報告，ISEC99-57, 37〜42 (1999)

(3) Boneh, D., et al.：Identity based encryption from the Weil pairing, Crypto 2001, LNCS No.2139, Springer Verlag, 213〜229 (2001)

(4) IEEE P1363.3：Identity−Based Public Key Cryptography
http://grouper.ieee.org/ groups/1363/IBC/

(5) IETF RFC 5091：Identity-Based Cryptography Standard (IBCS) #1：Supersingular Curve Implementations of the BF and BB1 Cryptosystems (2007-12)

(6) IETF Internet Draft：Identity-based Encryption Architecture

(7) IETF Internet Draft：Using the Boneh-Franklin and Boneh-Boyen identity-based encryption algorithms with the Cryptographic Message Syntax (CMS)

(8) Applications of Pairing-Based Cryptography: Identity-Based Encryption and Beyond
http://csrc.nist.gov/groups/ST/IBE/index.html

(9) Takashima, K.：Scaling security of elliptic curves with fast pairing using efficient endomorphisms, IEICE Trans. on Fundamentals, **E90−A**, No.1, 152〜159 (2007)

量子暗号の開発動向と安全性評価技術

長谷川俊夫*
石塚裕一*
鶴丸豊広**

Research Trend of Quantum Cryptography and Security Anaylsis

Toshio Hasegawa, Hirokazu Ishizuka, Toyohiro Tsurumaru

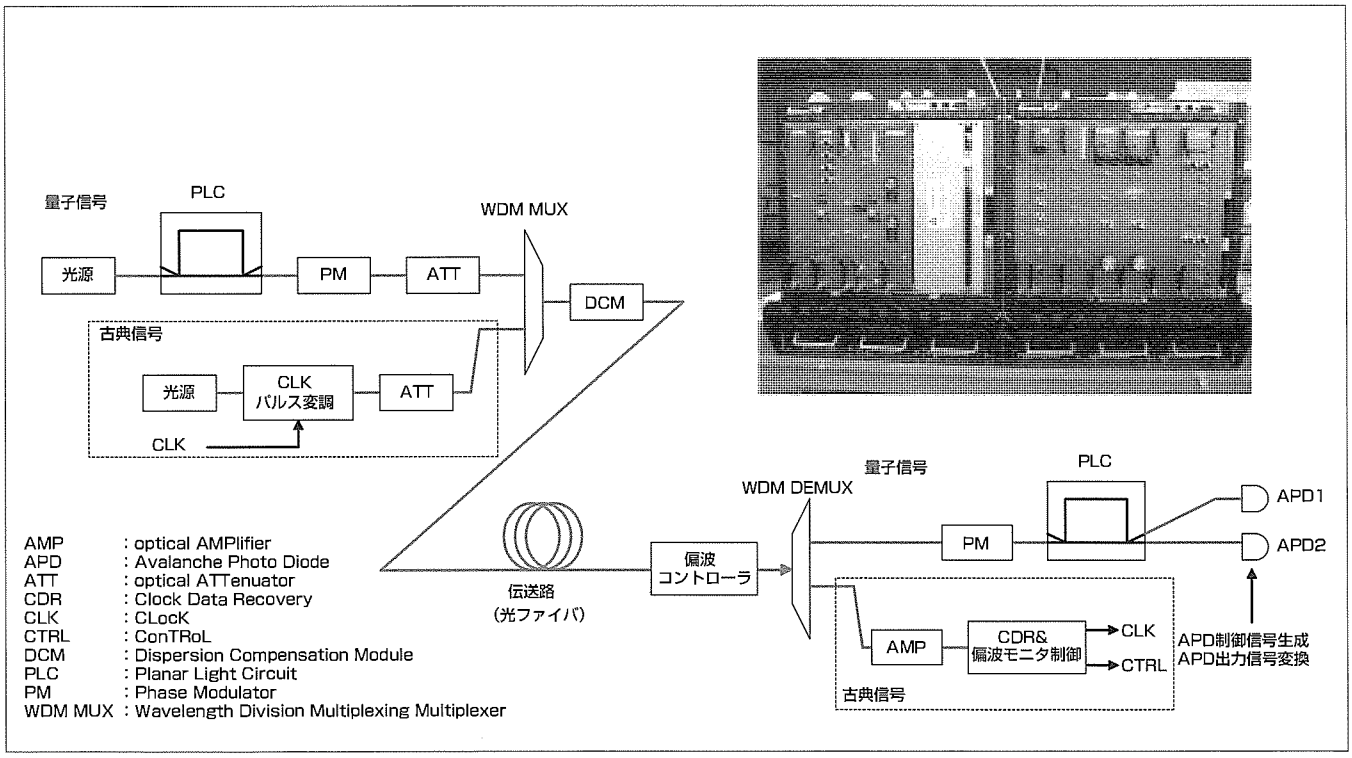
要　旨

量子暗号は物理の基本原理を利用しているため，物理法則で安全性が保証され，究極の安全性を提供する暗号技術である。量子暗号は，量子情報技術の中で最も多く実験や装置開発・フィールド試験が行われており，これまで，光学スキームとして一方向型やプラグアンドプレイ方式などによって100km程度の長距離実験が行われるにいたっている。また最近では，量子暗号の鍵(かぎ)配布プロトコルの中で代表的なBB84を改良し理想的な単一光子源を前提にしなくても，微弱コヒーレント光を用いて長距離での安全性が確保できる方式(例えばデコイ方式，差動位相シフト方式)が提案され期待されている。この場合，実装も比較的容易で，高速化開発に適した方式でもある。ただし，新しい方式に関しては今後まだ安全性の議論を行っていく必要があり，安全性評価技術が非常に重要となってきている。

現在，量子暗号の研究開発は，実用化を目指した装置開発の段階に到達しており，高い安定性を持ち，高速で将来のネットワーク化にも対応可能なものが望まれている。三菱電機が取り組んでいるものも，目標性能として通信距離50km，速度 1Mbpsの実用的な装置で次のような特徴を持っている。

(1) 古典信号と量子信号の時分割伝送(古典信号には，クロック情報及び偏波ゆらぎ補正情報を載せ，量子信号とあわせて送信する。受信側で信号分離し，クロック再生と偏波ゆらぎ補償のフィードバック制御を実施し安定性を高める。将来は経路選択／切替情報を載せることが可能である。)

(2) BB84，デコイ方式，DPSQKD(Differential-Phase-Shift Quantum-Key-Distribution)の量子暗号プロトコル方式で光源繰り返し速度GHzレベル，数十km伝送対応の高速化に対応



開発中の量子暗号装置の基本構成とATCA規格準拠の量子暗号装置写真

当社が開発中の量子暗号装置の基本構成と装置の外観(右上)を示す。左上が送信側装置，右下が受信側装置である。高い安定性と高速化を特長とする。古典信号と量子信号の時分割多重分離，波長分離技術によって，古典信号に含まれるクロック・偏波情報をモニタし，同期ゲート制御及びフィードバック制御を行う。これによって環境温度変化や偏波ゆらぎを補償し，高い安定性を実現する。また，効率的実装のため，送受信システムをさらに機能分割し，ATCA (Advanced Telecom Computing Architecture) 規格準拠の装置を開発した。

*情報技術総合研究所　**同研究所(理博)

1. まえがき

量子暗号[1]は，究極の安全性を実現する暗号技術である。現代暗号は将来量子計算機のような超高速な計算機が実用化すると解読できてしまうという課題があるが，量子暗号は物理の基本原理を利用し，物理法則で安全性が保証され，この問題点を克服している。このような量子暗号技術は，量子情報技術の中で最も多く実験や装置開発・フィールド試験が行われており，理論面でも新方式の提案も含め活発に議論されている。本稿では，量子暗号の研究開発に関して，国内外の動向，これまでの当社の成果及び現在取り組んでいる実用化に向けた研究開発に関して述べる。また，重要になっている量子暗号の安全性評価技術についても述べる。

2. 研究開発動向

量子暗号の実験では，符号化方式として位相変調がよく用いられるが，この場合，干渉計(例えばMach-Zhender干渉計)を構成して，その干渉結果を光子検出器で測定する。実際の通信実験では，干渉計の安定性を高めるなど様々な工夫が必要なため，改良されて用いられる。光学スキームの代表的な方式は，通常の送信側に光源を，受信側に検出器を配置する一方向型，光源と検出器を同じ側に持ち光路は往復させてゆらぎ補償する往復型(プラグアンドプレイ"plug&play"方式)などがある。"plug&play"方式では，受信者側から送信者側に送信される際の光ファイバ伝送中の擾乱(じょうらん)と，ファラデーミラーで反射されて戻る際に光ファイバ伝送中の擾乱の効果が往復路を通ることでちょうど補償でき，安定的な系となるのが大きな特徴である。このように安定性が高いplug&play方式はこれまでの主流であったが，この方式は受信側に光源と検出器があり，強度の大きな入力となる光源の散乱光の影響でエラー率増大につながる可能性があり，長距離化を図る場合には障害となる。また安全性の面でも，実装攻撃の一種(いわゆる"トロイの木馬攻撃")に弱いという問題がある。これらの理由から近年は，一方向型が長距離化に関して有利でよく用いられている。この場合，干渉計の安定性を維持するために光路長調整などの動的な補償が必要である。

光ファイバでの実験／開発はこれまで積極的に行われ，東芝欧州研など100kmを超える実験室内の長距離実験[2]の報告がいくつかなされている。また，既設光ファイバを用いた遠方2地点フィールド実験も，例えばジュネーブ大学の67km実験[3]，当社の96km実験[4]，中国USTC(University of Science and Technology of China)の125km実験[5]などが行われている。**表1**にBennett-Brassard 1984方式(BB84方式，いわゆるデファクト方式)を用いた代表的な遠方2地点フィールド実験の例を示す。

フィールド試験では，送受信装置間での同期確立，安定性の実現が重要となる。光子検出タイミングは数百psの精度であわせる必要があるため，光同期及びタイミング同期機能は不可欠である。同期は，クロック同期信号を通常強度の光信号を使って量子信号と一緒に送信して実現するのが回線の有効利用の点からも望ましい。通常強度のクロック同期信号を，波長多重技術等を用いて非常に微弱な量子信号と同じファイバで送る場合は，高アイソレーションの波長分離が技術課題となる。

また安全性評価技術に関しても進展が続いており，それに伴って新たな量子暗号方式が提案されている。かつてはどの研究機関の量子暗号実験でもほぼ常に，方式としてはBB84方式，光源としては微弱レーザ光が用いられていた。ただしこの種のシステムはPNS攻撃(Photon Number Splitting Attack)と呼ばれる攻撃に弱く，厳密な安全性基準を適用すると，通信距離の限界が25km程度未満となることも知られていた。この状況を救うために，実際の量子暗号システムに対しては"平均光子数0.1以下の微弱レーザ光を単一光子とみなす"という不完全な基準を適用することが，最近まで学会レベルで世界的に許容されていた。この背景として次のような暗黙の共通認識があった。

長距離で無条件安全性を達成するためには本来，厳密な単一光子源が不可欠とされるが，その開発は困難である。そこでひとまず光源としては微弱レーザ光で代用し，検出器や光学系など他の部分の研究開発を進めて量子暗号システムの完成を優先させる。後に単一光子源が安価に構築できる時代になったら，光源としてそれを組み込むことはいつでも可能であるからである。

しかしこの状況も，BB84方式の改良版である"デコイ方式(Decoy Method)"が提案されてここ数年で大きく変わった。この方式の特長は，単一光子源を用いなくても微弱レーザ光によって長距離で厳密な無条件安全性が達成できることにある。これによって研究の主流が，完全に無条件安全な量子暗号システムをいかに効率的に実装するか，に移りつつある。

デコイ方式の基本はBB84方式と同一だが，送信者が各パルスの光強度をわざとランダムに変調する。なおかつ受信者がその光を受信するまでその強度分布は明かさない。この状況では盗聴者は各パルスの光強度分布を知らずに攻

表1．光ファイバによる量子暗号システム実験の代表例

研究機関（年）	光学スキーム	波長(μm)	伝送距離(km)	誤り率 QBER(%)	生鍵伝送レート(bps)
Geneva(2002)*	P&P	1.55	67(Field)	6*	150*
Mitsubishi(2004)	P&P	1.55	96(Field)	9.9	8.2
USTC(2004)	一方向	1.55	125(Field)	6	—
Toshiba R.E.(2005)*	一方向	1.3／1.55	20.3(Field)	0.87*	430*

＊ 平均光子数の設定が通常の倍の0.2の実験
QBER：Quantum Bit Error Rate

撃を行わざるを得ず，攻撃の影響が受信者側での信号検出率に統計的な矛盾として表れることになる。これによって前述のPNS攻撃が精度よく検出でき，より安全な量子暗号が実現できる。デコイ方式については無条件安全性が理論的に証明されており，その結果140km程度の長距離が実現できると試算されている。そしてこれまで実際に約100kmの光ファイバ実験，自由空間144km実験が報告されている。

また，デコイ方式よりもさらに簡易な装置で安全な長距離実装を実現しようとする方式として“差動位相シフト方式(DPSQKD方式)”がある。これは装置構成としては量子暗号でない通常の光通信の方式(DPSK方式)そのままであり，このため比較的安価にシステムが構成できる。しかも光強度を極限まで弱めてあるために量子論的性質が顕著にあらわれていて，このために量子暗号として使えるというのが基本のアイデアである。安全性面でのBB84方式との最大の違いは，秘密鍵のビット情報が複数の光パルスに符号化されているため，盗聴行為の影響が多数の光パルスにわたるので検出しやすい，というところにある。提案者らは当初，この方式によれば通信距離及び通信速度ともデコイ方式を上回れるとしていた。ただし厳密な安全性証明は与えず“個別攻撃(Individual Attack)”という限られた条件下のみで安全性を議論していた。そしてその評価結果に基づいて100～200kmでの実験結果を報告し世界最長距離を主張していた。しかしその後当社によるより厳密な安全性評価の研究の結果によって，これらの実験の量子暗号は実際には安全ではなく，さらにDPSQKD方式一般の通信距離の限界はたかだか95kmであることが示された[6]。したがってこの方式は長距離通信には向いていないことが判明し，現在では短距離における高速通信での安全性が議論の争点となっている。

3. 当社のこれまでの研究開発

3.1 2005年度までの取り組み

当社は1999年から研究開発に取り組み，2000年に北海道大学と共同で短波長(830nm)量子暗号通信システム実験[7]に成功し，その後2001年から第I期のNICT((独)情報通信研究機構)委託研究“量子暗号技術の研究開発”を日本電気㈱，東京大学と5年間実施してきた。ここで当社は“単一光子生成技術”“単一光子検出技術”“乱数発生技術”“量子暗号鍵配布システム技術”を担当した。2002年に通信波長帯1,550nm高性能単一光子検出器(暗計数率 約10^{-6}，検出効率 約20%)を開発，これを用いた87km長距離量子暗号通信システム実験[8]，2004年には既設ファイバ(大阪-京都間)での96kmフィールド試験[4]で実用性を示したなどの成果をあげた。また最終年度には高速化を目指し，4波波長多重の量子暗号装置の開発を行い機能検証を行った。その他にも新しい光学スキーム・プロトコル研究では，新たな“還流型量子鍵配布方式”を提案し，従来方式よりも通信速度を高速かつ多人数通信可能な方式の実証実験[9]も行っている。また展示会(国際展示会ITU TELECOM WORLD 2003，2006，RSA Conference 2005 Japanなど)に量子暗号装置を出展し，応用アプリケーションとして量子暗号秘匿電話／テレビ電話の例も示した。

3.2 実用化に向けた研究開発

2006年度からは第Ⅱ期のNICT委託研究“量子暗号の実用化のための研究開発”(5年間を予定)で，量子暗号ネットワークを実現するために必要な高速高安定量子伝送技術，鍵管理・安全性保証技術の開発を進めている。目標性能として通信距離50km，速度1Mbpsという，より実用的な量子暗号装置である。現在，開発を進めているのは，主に次のような特徴を持つ装置である。

(1) 古典信号と量子信号の時分割伝送(古典信号には，クロック情報，及び偏波ゆらぎ補正情報を載せ，受信側で信号分離し，クロック再生と偏波ゆらぎ補償のフィードバック制御を実施し安定性を高める。また，将来は経路選択／切替情報を載せることを可能とする。)

(2) BB84，デコイ方式，DPSQK方式の量子暗号プロトコル方式で光源繰り返し速度GHzレベル，数十km伝送対応の高速化に対応した装置

3.3 量子・古典多重信号伝送技術の開発

量子信号と古典信号の時分割多重を用いた多重分離技術をキーとしている。具体的には，古典信号に含まれるクロック情報と偏波情報をモニタし，同期ゲート制御，フィードバック制御によって，環境温度変化，偏波ゆらぎを補償する方式を検討し実装した。量子暗号通信は単一光子レベルの微弱光で，通信装置制御用信号は古典光レベルの高強度である。この古典通信路を実現するために，従来は物理的に別回線を用いる方法や古典通信路と量子通信路に同一の物理回線を用いて波長多重によって分離する方式がとられていた。しかし，前者は設備コストに問題があり，後者は量子信号と古典信号の分離の難しさに課題があった。このため，波長多重や時分割多重によって量子信号と古典信号を同一の物理通信路を用いて伝送，分離する装置開発を目指している。時分割多重制御装置では，古典制御信号によって，通信路の光ファイバの伝搬特性(偏波ゆらぎなど)の補償，クロック伝送を実現する。また，経路制御情報の伝送も目指し，ネットワーク化に対応も視野に入れている。

3.4 高速化対応の光学系装置開発

量子・古典多重信号伝送技術と高速単一光子検出技術を組み合わせ，最終目標の1つである1Mbps@50kmを実現するために必要な光学系として実験系(**図1**)を検討した。プロトコルは，BB84，デコイ方式又はDPSQKDをベースとし，光源繰り返し速度GHzレベル，数十km伝送を行うことを特長とした高速量子暗号装置である。また，光学系

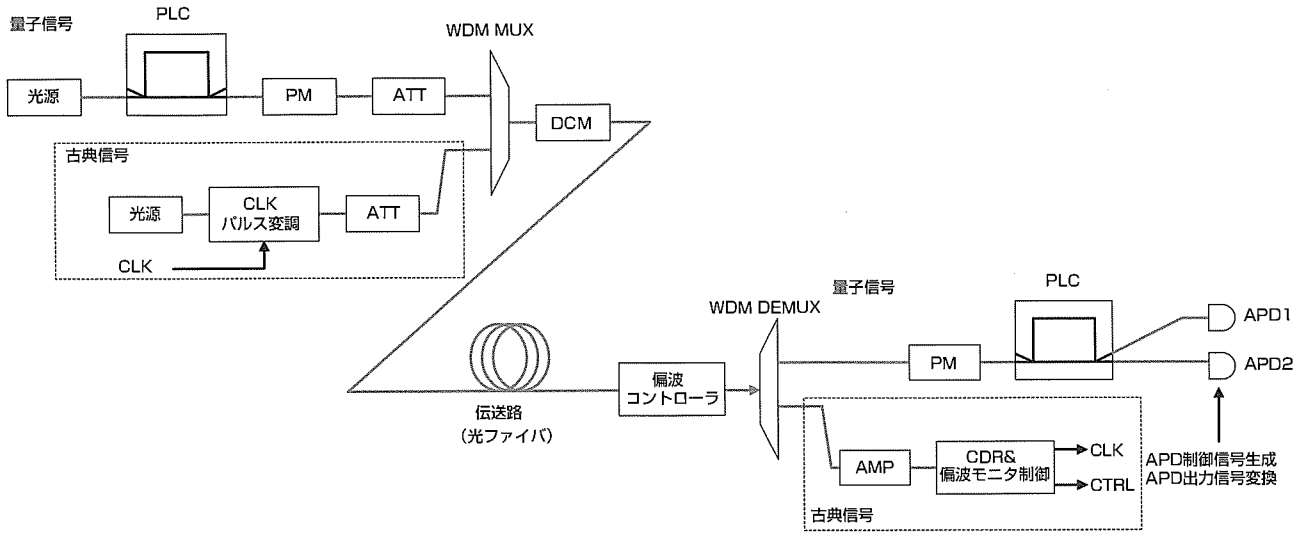


図1．開発中の量子暗号装置の基本構成

システム・電子制御システムを効率的に構築するための装置をどのような機能によって基板に分割したら良いか，また効率的かを検討した。具体的には，Advanced TCAを採用して，送信側や受信側をさらに機能分割したモジュールを基板として構成した(扉ページの装置写真参照)。量子光と古典光の光源は，DWDM CW DFB(Dense Wavelength Division Multiplexing Continuous Wave Distributed FeedBack)レーザモジュールで，波長は1550.918nm(古典信号)，1549.315nm(量子信号)とし，駆動周波数は$\nu=1$GHzまで対応できるよう設計している。波長多重信号分離では，DWDM DEMUX(DEMultipleXer)で，2つの信号のチャネルのアイソレーションを80dB以上の性能を持つように設計し，この実験で，微弱な量子信号を強度の強い古典信号から精度良く取り出すことを確認する予定である。

3.5 安全性評価技術

当社では実験と並行して，安全性に関する理論研究も従来進めている。最近の成果としてはまず2章で述べたとおり，DPSQKD方式に対する新攻撃方法の提案及びそれに基づく安全性解析の結果がある[6]。またデコイ方式に関する理論研究も北海道大学と共同で進めており，2007年度にはイールド(yield)と呼ばれるパラメタの上限と下限を厳密に見積もるための数学的な解析方法を新たに開発した[10]。これによってデコイ方式の通信距離・通信速度の更なる向上が実現できる。

またさらに，量子鍵配送に限らない，認証・署名等を含めた一般の量子暗号プロトコルに関する理論的研究も従来行っている。この方面での成果としては量子ビット列コミットメントに関するものがある[11][12]。

4. むすび

量子暗号の研究開発動向，当社の成果や現在取り組んでいる実用化に向けた研究開発について，また量子暗号の安全性評価技術についても述べた。量子暗号は理論的な安全性証明を与えられて意味を持つものであり，現実の量子暗号装置の開発を着実かつ効率的に進めていくためにもこれらの理論解析が非常に重要となる。現在でも新方式の模索は続いており，本稿で触れたデコイ方式，DPSQKD方式以外にも，六状態方式，連続変数方式など新プロトコルがその後続々と提案されている。ただし安全性証明の進展は必ずしもその速度に追いつかず，無条件安全性が示されているものはどちらかというと少数派である。安全性評価の動向を正しくとらえつつ，当社としても独自の研究を続けていくことが今後とも引き続き重要であると考える。

本稿の一部は，NICTの委託研究“量子暗号の実用化のための研究開発”の一環として実施された。

参考文献

(1) 佐々木雅英，ほか監修：量子情報通信，オプロトニクス社（2006）
(2) Gobby, C.：Appl. Phys. Lett., 84, 19, 10（2004）
(3) Stucki, D.：New J.Phys., 4, 41（2002）
(4) Hasegawa, T., et al.：CLEO/Europe-EQEC2005, EH3-4, Munich（2005）
(5) Mo, X., et al.：Opt. Lett., 30, 2632（2005）
(6) Tsurumaru, T.：Phys. Rev. A 75, 062319（2007）
(7) Hasegawa, T., et al.：IEICE E85-A No.1, 149（2002）
(8) Hasegawa, T., et al.：CLEO/QELS2003, QTuB1, Baltimore（2003）
(9) Nishioka, T., et al.：IEEE PTL 14,4（2002）
(10) Tsurumaru, T., et al.：Phys. Rev. A 77, 022319（2008）
(11) Tsurumaru, T.：Phys. Rev. A 71, 012313（2005）
(12) Tsurumaru, T.：ibid 74, 042307（2006）

伝令付き単一光子源による量子暗号実験

西岡　毅*
鶴丸豊広*

Quantum Key Distribution Experiment with the Heralded Single Photon Source

Tsuyoshi Nishioka, Toyohiro Tsurumaru

要　旨

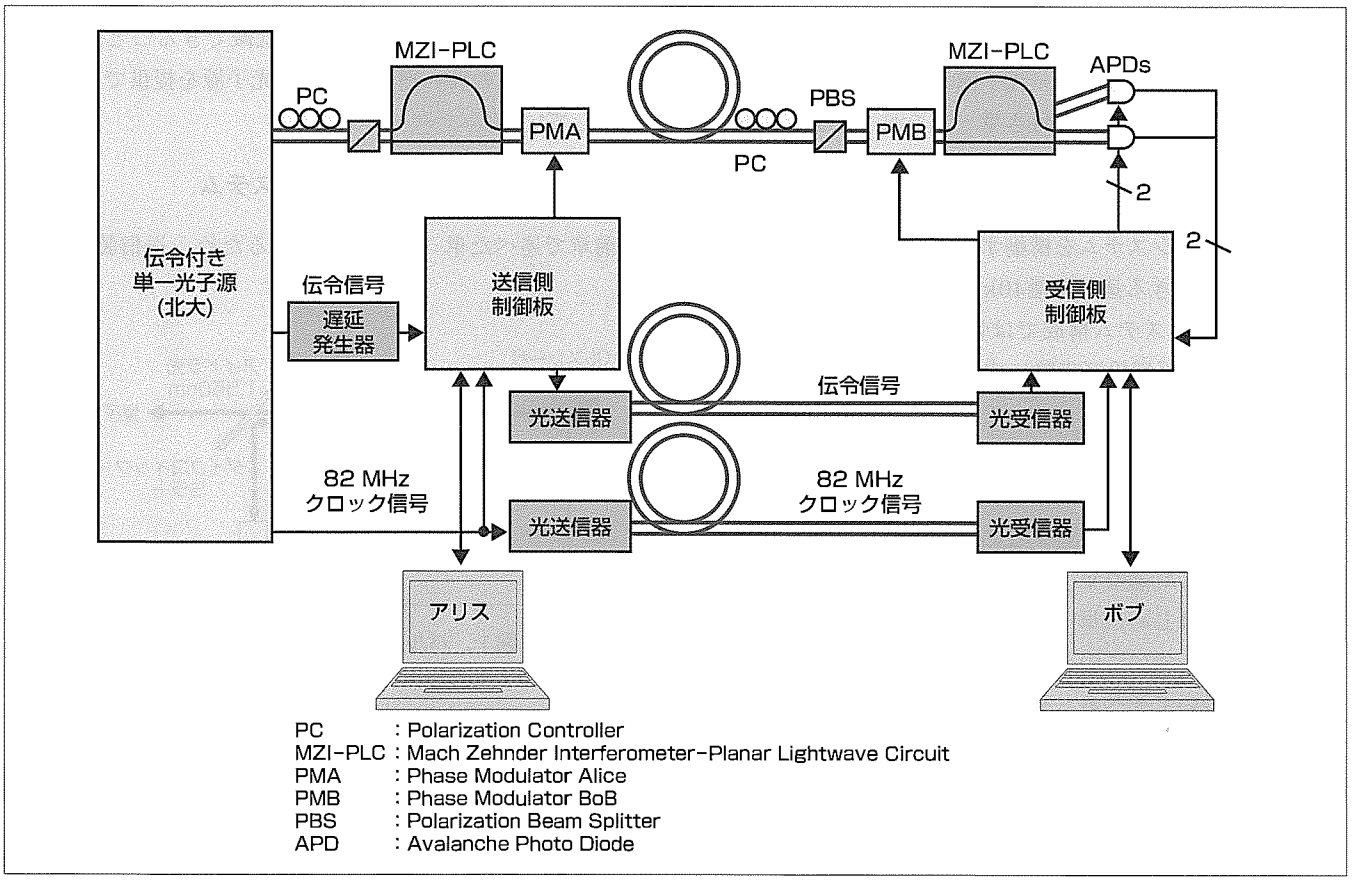
近年量子暗号通信実験が相次いで報告されているが，そのほとんどは光子源として微弱レーザ光源を用いたものである。一方で，装置の不完全さがどのようなセキュリティホールをもたらすかも研究されている。この研究によると，微弱レーザ光源のように光子を2個以上放出する場合のある不完全な光子源は，光子数分割攻撃と呼ばれる攻撃によって盗聴が可能になることが分かってきた。このため，安全性の保証される通信距離が25km前後と予想外に短いことが指摘されている。

本稿では，このような脅威への対策として光子源をより完全に近づける方針を採用し，北海道大学電子科学研究所の竹内繁樹教授グループが開発した伝令付き単一光子源を用いた量子暗号システムを開発し，量子暗号実験に成功したことについて述べる。

この量子暗号システムでは伝令信号と呼ばれる制御信号に加えて，クロック信号も制御信号として用いることでシステムの信頼性を向上させている。

これによって安全性の保証された通信距離の大幅な延伸を達成し，通信距離40kmでは量子鍵(かぎ)配布実験に，通信距離80kmでは原理検証実験に成功した。

また，厳密な意味での安全性の評価手法を確立し，この開発した評価手法で上記2つの実験についての安全性を確認することができた。



伝令付き単一光子源を組み込んだ量子暗号システム

左端の伝令付き単一光子源からは，上から順に単一光子，伝令信号，クロック信号が出力されている。単一光子は偏波制御子(PC)，偏光ビームスプリッタ(PBS)，マッハツェンダ干渉計を構成する石英平面光回路(MZI-PLC)を通って，位相変調器(PMA，PMB)でランダム変復調を受け光子検出器(APD)で検出される。この単一光子に先立って伝令信号が出力される。クロック信号と単一光子とのジッタは極めて小さい。

*情報技術総合研究所(理博)

1. まえがき

光子一つ一つに異なる情報を載せることで，量子暗号は盗聴検知を可能とし，無条件の安全性を保証することができる。近年多くの量子暗号実験の報告がなされており，ようやく実用化の段階に入りつつある。

しかしながら，多くの実験では光子源として微弱レーザ光が用いられている。微弱レーザ光ではほとんどの場合光子があっても1個であるが，中には2個以上出る場合もある。2個以上光子が放出される場合検知されることのない盗聴が可能になるので不完全な光子源となっている。

この光子源の不完全さに着目して厳密に安全性を評価する研究が2000年代から盛んになった。この研究によると，微弱レーザ光を用いた量子暗号実験で安全性が保証できる通信距離が案外短く25km前後である[1]。

このため，厳密な意味で安全性を保証できる通信距離を伸ばす方向での研究が盛んになった。これには大別して2つの方向がある。1つは不完全な光子源でも安全性が保証できるようにプロトコルを改良する方向である。例えば，SARG(Scarani-Acin-Ribordy-Gisin)，デコイ，DPSQKD(Differential-Phase-Shift Quantum-Key-Distribution)等のプロトコルが成功を収めている。もう1つは光子源を完全にすることでセキュリティホールをなくす方向である。このような単一光子源としては，パラメトリック下方変換を用いた伝令付き単一光子源，量子ドットを用いた光子源がある。

本稿では，後者の方向を採用し，伝令付き単一光子源を用いた量子暗号システムを構築することによって，厳密な安全性の保証できる通信距離40kmにおける量子鍵配布実験，またこのシステム構成では世界最長となる通信距離80kmにおける原理検証実験に成功したことについて述べる。

なお，このシステムで用いた伝令付き単一光子源は北海道大学電子科学研究所竹内繁樹教授のグループが開発したもので，将来の量子リピータとの接続までを見据えた量子暗号システムに好適な単一光子源である[2]。

本稿では，はじめに単一光子源，並びに，量子暗号システムについて，次にこのシステムを用いて行った2つの重要な実験について述べる。そして，これらの実験が厳密な意味で安全であることを示すために安全性の評価について述べる。

2. 単一光子源

伝令付き単一光子源は，非線形光学結晶であるBBO(β-BaB_2O_4)結晶によるパラメトリック下方変換を基にしている。パラメトリック下方変換とは，BBO結晶に波長390nmのポンプ光を入射すると，この入射光よりも波長の長い2つの光，波長521nmのシグナル光と波長1,550nmのアイドラ光が発生する現象である(図1)。

この現象を光子レベルでみると，入射したポンプ光の光子がよりエネルギーの低い1組の光子対になって発生することになる。伝令付き単一光子源では発生した光子対の1つシグナル光子を観測することで，アイドラ光子を壊すことなく検知し利用することができる。

この方式ではパルスレーザをポンプ光として用い，発生したシグナル光子を光子検出器(Single-Photon Counting Module：SPCM)で検出する。この検出信号が伝令信号となり，アイドラ光子の発生を知らせてくれる。パルスレーザのパルスと同期したクロック信号も出力されており，アイドラ光子の発生の有無はこのクロック信号が規定する規則的なタイムスロット上に乗って繰り返されている。このため，アイドラ光子の発生は全くランダムに起こるわけではなく，オンデマンド性及び規則性の高い単一光子源が構成できることになる。

この単一光子源の発生する光子の完全さ，又は，単一性については，アイドラ光子について，同時に光子が1個しか発生しない確率P(1)，2個発生する確率P(2)を実測することで確認できる(図2)。

図2をみると，ポンプ光出力を調整することで，P(1)をほぼ一定に保ちつつ，P(2)を低減できることがわかる。これは完全性の高い理想的な単一光子源を提供できることを示している。

3. 量子暗号システム

前章で述べた単一光子源を用いるため，送信装置(アリ

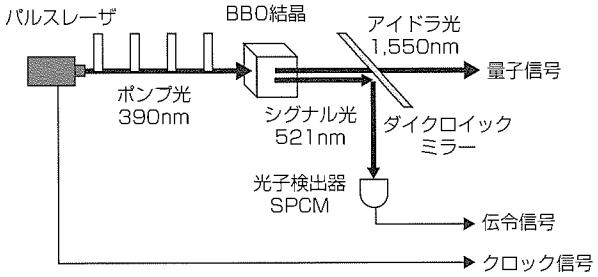


図1．パルス駆動伝令付き単一光子源

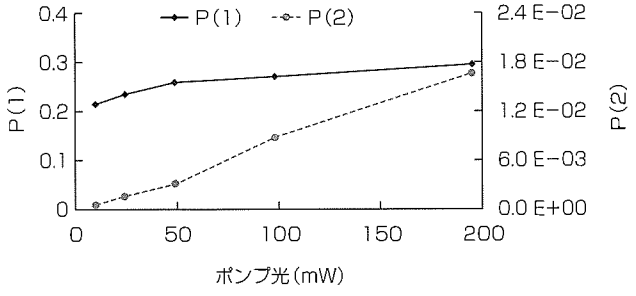


図2．ポンプ光と光子数との関係

ス)から受信装置(ボブ)へと光子が向かう一方向型の量子光学系を採用した(図3)。

このシステムは，図3の上から量子信号系，伝令信号系，クロック信号系の3つから構成されている。特にパルス駆動型の単一光子源の特徴を生かしてクロック信号系が組み込まれていることが大きな特徴である。

量子光学系は，主に石英平面光回路を用いた非対称マッハツェンダ干渉計(MZI-PLC)で構成されており，この特徴的な長さが40cm(時間2nsに相当)であることと光子検出器の動作特性から，時間的な制御精度(ジッタ)が100ps以下であることが要求される。

一方，伝令信号系は単一光子源に組み込まれた光子検出器(SPCM)によってジッタが500ps程度と大きく，伝令信号系だけでは量子信号系をうまく制御できないことになる。

このため，ジッタ1ps程度を保証できるクロック信号系を導入し，伝令信号による各制御信号をクロック信号に同期させることで高精度な制御系を確立し，高効率，長距離通信可能なシステム構築に成功した。

4. 量子暗号実験

前章までに述べたシステム構成を用いて2つのエポックメイキングな実験を実施したので次に述べる。1つは，通信距離40kmにおける量子鍵配布実験[3]であり，2つ目は，通信距離80kmにおける原理検証実験である[4]。

4.1 通信距離40km量子鍵配布実験

通信距離40kmでは，アリス，ボブ双方で位相変調を行い，BB84(Bennett-Brassard 1984)プロトコルを実施した。通信路は距離40km，通信損失9.8dBの分散シフトファイバ(Dispersion Shifted Fiber：DSF)を用いた。単一光子源の動作条件は，伝令信号レート12.4kHz，送信側出力ポートにおけるP(1)＝0.0423，P(2)＝1.48×10^{-5}である。この値は通信距離40kmで十分な単一光子性を持つことを保証する。光子検出器は，APD1が量子効率9.62%，暗計数率2.05×10^{-6}で，APD2が量子効率8.64%，暗計数率2.05×10^{-6}で動作させた。

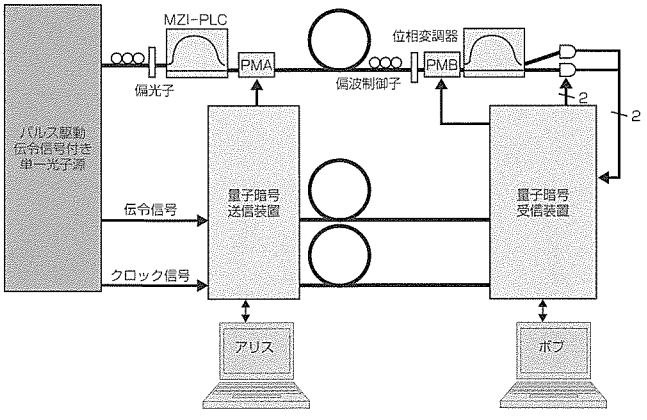


図3．伝令付き単一光子源を組み込んだ量子暗号システム

表1の実験結果は3,276,800パルスの伝令信号に対して271イベントの光子検出器の発火から得たものである。

この結果は，ビットレート0.54bps，量子ビットエラーレート(Quantum Bit Error Rate：QBER)4.23%を示しており，微弱レーザ光では厳密な安全性が保証できない通信距離40kmで量子鍵配布の確認ができたことを意味している。

4.2 通信距離80km原理検証実験

この実験は，前節の量子暗号システムがどのくらい長距離まで適用可能かを検証するために行った単一光子干渉実験である。通信距離80kmは分散シフトファイバで，分散40ps/nm，分散シフト7ps/nm/nmであり，この量子干渉系の特徴的長さ2nsが耐えられる限界値に相当する。通信損失18dBも光子検出器のSN(Signal to Noise)限界に迫っている。このため，受信側位相変調器(PMB)を取り除き，送信側のみ2値ランダム変調で実験を実施した(図4)。

このとき，光子検出器は，APD1が量子効率5.6%，暗計数率8.1×10^{-7}で，APD2が量子効率5.4%，暗計数率1.1×10^{-6}で動作させた。単一光子源は，原理検証実験であるので，伝令信号レート299kHz，P(1)＝0.32，P(2)＝3.46×10^{-2}というやや大きすぎる設定で動作させた。

この結果は平均QBER＝8.2±0.8%を示し，将来的に十分な調整，装置の改良を施すことで，安全な通信距離が80kmまで延伸できることが確認できた。

5. 安全性の評価

量子暗号とりわけBB84方式の安全性は，QBER，及び複数光子生成確率$P(2)$(Multi-photon Probability)という2種類のパラメータによって決定される。量子暗号でEveの盗聴行為は量子操作として記述され，盗聴を行うことが

表1．量子鍵配布実験結果

アリス側変調パターン	ボブ側変調パターン	正	誤	無効
0，π	0	72	2	−
π/2，3π/2	0	−	−	70
0，π	π/2	−	−	59
π/2，3π/2	π/2	64	4	−

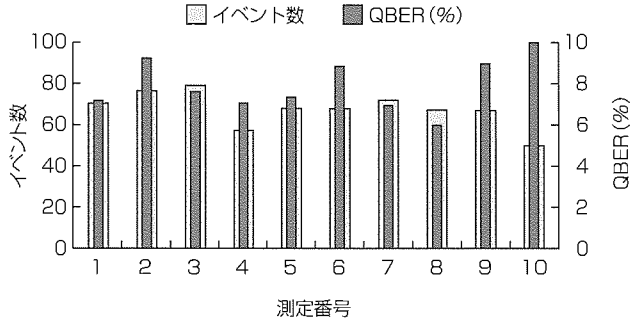


図4．伝令パルス8,192,000個に対する受信イベント及びQBERの測定結果

光パルスの状態の変化をもたらす。そして変化の度合いとQBERとには相関があるので，QBERを事後に統計的に検証することによって盗聴が検知できる。また，現実の装置では送信者Aliceがある確率で複数光子を放出するが，その影響を考慮した場合にはQBERだけでは不足であり，複数光子生成確率$P(2)$も検証しなければならない。これはいわゆるPNS攻撃(Photon Number Splitting Attack)と呼ばれる攻撃があるためである。

AliceとBobは，量子通信(本稿では単一光子による通信)が終わった後に，ビット列の一部をランダムサンプリングし，それらの値をLAN(Local Area Network)等で開示しあうことによってQBERを統計的に推定する。そして生鍵(Raw Key)の誤り訂正(Error Correction：EC)をする。また一方でこうして得られたQBERと$P(2)$の値とから，盗聴者Eveが得ることのできる情報量の上界Iが算出できる。そしてそのIに相当するビット数を秘匿性増強（Privacy Amplification：PA）によって消去すれば完全な秘密鍵(Secret Key)が得られる。

一般にQBERや$P(2)$が高い場合はEveによる盗聴の度合いが高いことを意味し，秘密鍵は生成できない。一方でこれらのパラメータが十分小さい場合でも，安全な秘密鍵の長さを正確に推測する必要がある。秘密鍵と生鍵の長さ比を一般に秘密鍵生成速度R又は鍵レートと呼ぶが，これを算出することが安全性評価の最終目標である。

この実験では無条件安全性を達成することを目標とし，また鍵蒸留(Key Distillation)，すなわちEC及びPAは送信者Aliceから受信者Bobへの一方向通信で行われるとする。さらにECやPAにおけるブロック幅はそれぞれ十分長いと仮定し，したがってブロック切り出しに際しての誤りビット数や複数光子パルス数の統計的分散は無視できると仮定する。

この状況での鍵レートRは参考文献(5)のタグ付きキュービット(Tagged Qubit)の議論によって与えられ

$$R=1-\Delta-H_2(e)-(1-\Delta)H_2\left(\frac{e}{1-\Delta}\right)$$

となる。ただしここでeはQBER，$\Delta=P(2)$は複数光子生成確率，H_2は2値エントロピー$H_2(x)=-x\log x-(1-x)\log(1-x))$である。本稿における秘密鍵生成レートはすべてこの公式に基づいて算出した。

6. むすび

伝令付き単一光子源を用いた量子暗号システム及びその2つの重要な実験，安全性の評価について述べた。今後はデコイプロトコルを採用することで高性能化を図る予定である。

本稿の一部は，情報通信研究機構の委託研究「量子暗号の実用化のための研究開発」の一環として実施されたものである。

参考文献

(1) Lütkenhaus, N.：Security against individual attacks for realistic quantum key distribution, Phys. Rev. A 61, 052304 (2000)

(2) Soujaeff, A., et al.：Heralded single photon source at 1550 nm from pulsed parametric down conversion, J. Mod. Opt. 54, 467 (2007)

(3) Soujaeff, A., et al.：Quantum key distribution at 1550nm using a pulsed heralded single photon source, Optics Express 15, 726～734 (2007)

(4) Nishioka, T., et al.：Single-photon interference experiment over 80 km with a pulse-driven heralded single-photon source, IEEE Photo. Tech. Lett. に採録

(5) Gottesman, D., et al.：Security of Quantum Key Distribution with Imperfect Devices, Quant. Inf. Comput. 5, 325 (2004)

耐タンパー評価・対策技術

佐伯　稔*

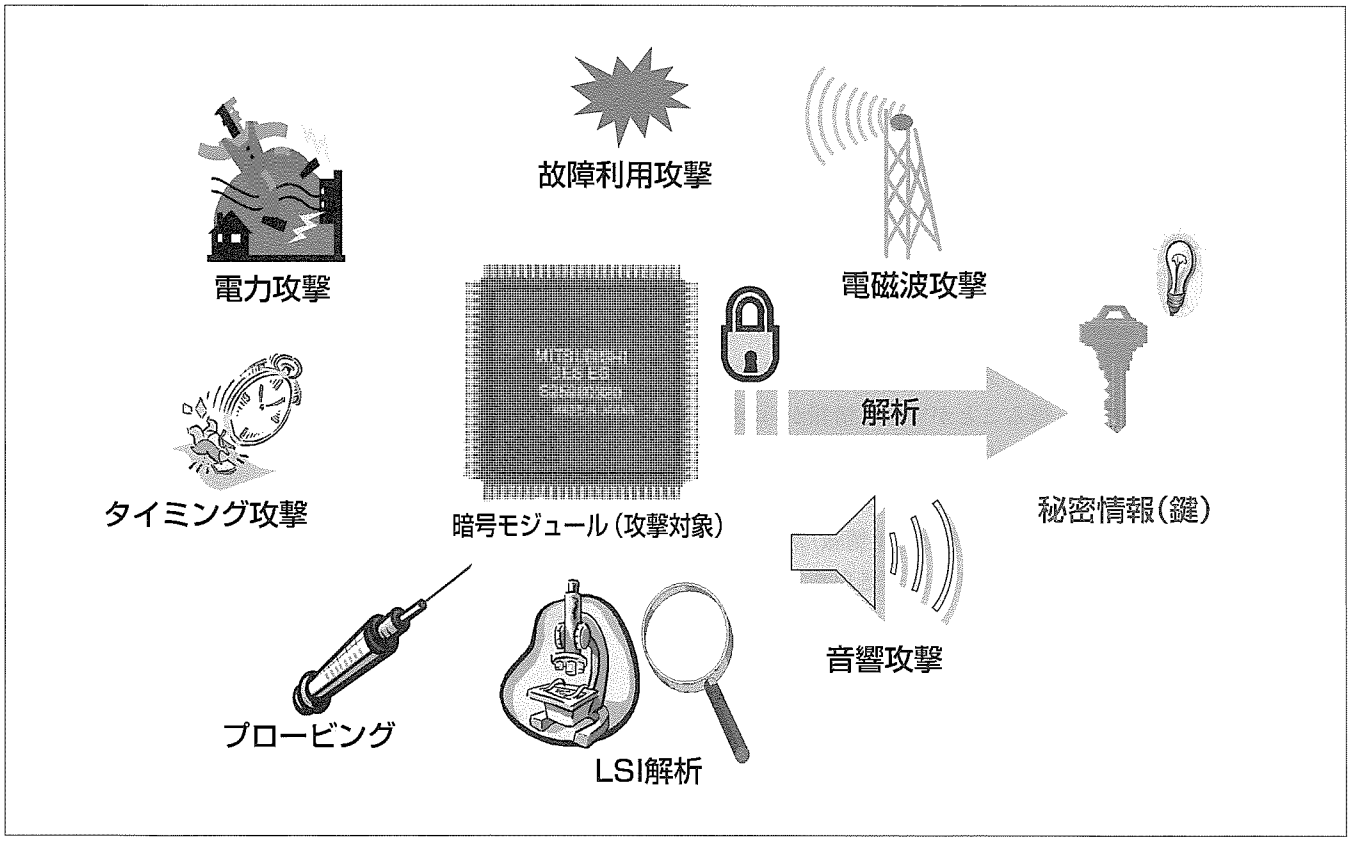
Tamper-resistance Evaluation and Countermeasure Technology

Minoru Saeki

要　旨

情報セキュリティ技術は，情報化社会を支える重要な技術であり，中でも暗号技術は最も重要な基盤技術の一つである。従来，現代暗号の安全性は主に暗号アルゴリズムの数学的(暗号学的)な安全性を根拠としており，暗号に対する攻撃(解読)も数学的な手法に基づくものが大半であった。一方，1990年代後半から，暗号アルゴリズムが実装された暗号モジュールに対する物理的・工学的な様々な攻撃法が登場し，情報セキュリティに対する新たな脅威となってきた。特に，暗号モジュールの処理時間や消費電力といったいわゆるサイドチャネル情報を解析する“サイドチャネル攻撃”と呼ばれる攻撃法は，強力な攻撃法として注目されている。暗号モジュールが，いかに数学的に安全な暗号アルゴリズムを用いても，その実装次第では，サイドチャネル攻撃によって，内部の秘密情報を簡単に解析されてしまう可能性がある。したがって，暗号モジュールには数学的な安全性だけでなく，実装面での安全性(耐タンパー性)も求められる。安全な実装を実現するためには，高度な耐タンパー評価・対策技術が不可欠である。

本稿では，サイドチャネル攻撃の中でも特に強力な攻撃法の一つである差分電力攻撃(Differential Power Analysis：DPA)を取り上げ，三菱電機が保有する評価技術や対策技術について述べる。また，暗号モジュールの耐タンパー性に関する国内の公的機関の取り組みや，国内外の標準化動向についても簡単に述べる。



暗号モジュールは様々な物理的攻撃にさらされる(イメージ)

数学的には事実上解読不能な暗号アルゴリズムを用いても，暗号モジュールの実装次第では，物理的な解析(攻撃)によって比較的簡単に解読されてしまう可能性がある。

*情報技術総合研究所

1. まえがき

情報化社会の進展とともに，データの盗聴・偽造・改ざんなどの防止又は検出などを実現する情報セキュリティ技術はますます重要となっている。情報セキュリティの中でも，暗号技術は不可欠な基盤技術の一つである。従来，現代暗号の安全性は主に暗号アルゴリズムの数学的(暗号学的)な安全性を根拠としており，暗号に対する攻撃(解読)も数学的な手法に基づくものが大半であった。一般に，現在広く用いられている暗号アルゴリズムの数学的解読には，地上のすべての計算機を用いても何億年も要するとされており，事実上解読不能といってよい。ところが，最近になって，暗号アルゴリズムではなく，それが実装された暗号モジュールに対する物理的・工学的な様々な攻撃法が登場し，情報セキュリティに対する新たな脅威となってきた。特に，暗号モジュールから生じる副次的な情報，すなわち，処理時間や消費電力といったいわゆるサイドチャネル情報を解析する“サイドチャネル攻撃”と呼ばれる攻撃法は，強力な攻撃法として注目されている。いかに数学的に安全な暗号アルゴリズムを用いても，その実装次第では，これらの攻撃によって，解読されてしまう可能性がある。このため，暗号モジュールには数学的な安全性だけでなく，実装面での安全性(耐タンパー性)が必要となり，当社もこの分野の研究開発に積極的に取り組んでいる。

本稿では，サイドチャネル攻撃の中でも特に強力な攻撃法の一つである差分電力攻撃(DPA)を取り上げ，当社が保有する評価技術や対策技術について述べる。また，暗号モジュールの耐タンパー性に関する公的機関の取り組みや，標準化動向についても簡単に述べる。

2. サイドチャネル攻撃概要

数学的な暗号解読は，公開パラメータ，平文，暗号文といった通常のチャネルから得ることができる情報から秘密情報(鍵(かぎ))を導出する。一方，サイドチャネル攻撃では，暗号処理中の暗号モジュールが発生する消費電力や電磁波などの副次的な物理量(サイドチャネル情報)から鍵を導出する(図1)。これらの物理量は，暗号処理を実現するのがハードウェアであれソフトウェアであれ，普通に実装した場合，微小ではあるが必ず鍵の値に依存した差異を持つものである。この差異を様々な手法で解析することで，鍵の値を推定する攻撃法が，サイドチャネル攻撃である。従来はこのような微小な差異にはほとんど注意が払われていなかったため，サイドチャネル攻撃は暗号実装に対する現実的な脅威と言え，早急に対策技術を確立することが望まれている。また，一般に，数学的な暗号解読が専用の解読装置又は膨大な計算機パワーを必要とするのに対して，サイドチャネル攻撃では市販の比較的安価な測定器などで解読可能な点も，サイドチャネル攻撃が脅威とみなされる要因の一つである。

着目するサイドチャネル情報の種類や解析の種類に応じて，様々なサイドチャネル攻撃が存在するが，今までに提案されている代表的なものを次にいくつか示す。

- タイミング攻撃(Timing Analysis：TA)：条件分岐の成立の有無，キャッシュのヒット／ミスヒットなどによって変化する処理時間の違いから鍵を推定する攻撃法である。
- 電力攻撃(Power Analysis：PA)：データに依存した暗号装置の消費電力の変化を解析して鍵を推定する攻撃法で，単純電力攻撃(Simple Power Analysis：SPA)，差分電力攻撃(DPA)などがある。図2に電力攻撃の基本的な測定系を示す。
- 電磁波攻撃(Electromagnetic Analysis：EMA)：暗号装置から発生する電磁波を解析する攻撃法である。電力攻撃と同様に，単純電磁波攻撃(Simple Electromagnetic Analysis：SEMA)，差分電磁波攻撃(Differential Electromagnetic Analysis：DEMA)などがある。

そのほかにも，これらを組み合わせた攻撃や暗号装置の瞬間的な誤動作を利用した攻撃など多くの攻撃法が知られており，今後もその種類は増えていくと予想される。

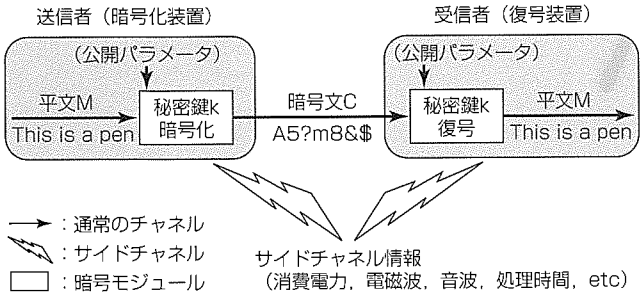


図1．通常のチャネル情報とサイドチャネル情報

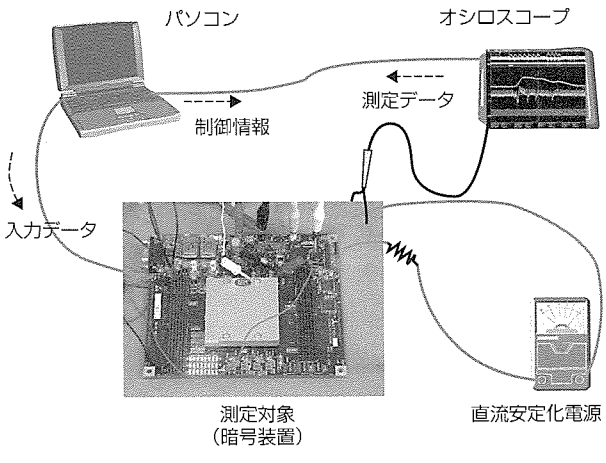


図2．電力攻撃の基本的な測定系

3. 当社の取り組み

当社は，“MISTY”やNTTとの共同開発の“Camellia”など，数学的な安全性に優れた暗号アルゴリズムを開発してきたが，数学的安全性だけでなく，実装面の安全性(耐タンパー性)評価技術にも積極的に取り組んでいる。安全な実装を実現するためには，高度な耐タンパー評価・対策技術が不可欠である。この章では，サイドチャネル攻撃の中でも特に強力な攻撃法の一つである差分電力攻撃(DPA)を取り上げ，当社が保有する評価技術や対策技術について述べる。

3.1 DPA評価技術

DPAは，鍵の値に依存したごくわずかな消費電力の偏りから鍵の値を解析する強力な攻撃法である。この攻撃では，まず**図2**のような測定系を構築し，測定対象(攻撃対象)が暗号処理を実行している最中の消費電力波形を大量に取得した後，鍵の部分ごとに統計処理に基づく全数探索を行う。米国政府標準暗号アルゴリズムであるAES(Advanced Encryption Standard)をDPA対策なしで実装した回路の部分鍵(8ビット)を，DPAによって全数探索した結果を**図3**に示す。図の横軸は8ビットの部分鍵が取り得る0から255までの値，縦軸はDPAの統計処理結果(差分電力)である。図中で，差分電力が突出したピークを示した箇所の横軸の値が，正解鍵の値である。同様の手順を，鍵の残りの部分に対しても繰り返すことで，すべての鍵が求められる。

当社では，**図3**で示したような評価結果が簡単に得られるような，測定対象(攻撃対象)の消費電力自動測定環境とDPAの統計処理環境を構築している。また，サイドチャネル攻撃評価用プラットフォーム(Side Channel Attack Platform for Evaluation：SCAPE)[1]を開発し，サイドチャネル攻撃の研究に用いるとともに，暗号システム開発時の事前安全性評価に活用している。SCAPEは様々な暗号システムのDPA耐性を，極めて低ノイズの環境で製品化前に評価可能である。**図4**にSCAPEの外観を示す。さらに，当社は，暗号回路の設計段階で効率的かつ高精度にDPA耐性を評価可能な論理シミュレーションベースDPA評価技術を確立し，それを利用した暗号LSI開発フロー[2]も提案している。この手法を適用することで，開発の初期段階でDPA耐性の評価と対策が可能となり，DPAに対して安全な暗号LSIを効率的に開発できる。LSI開発には大きな製造・人的コストを要するため，これらの事前評価は重要かつ有効である。

3.2 DPA対策技術

当社では暗号装置のハードウェアレベル，ソフトウェアレベル，システムレベルといった各階層で耐タンパー性に注意を払った実装を考慮している。ここでは，当社のハードウェアとソフトウェアのDPA対策技術について述べる。

当社が開発した半導体素子レベルのDPA対策技術として，RSL(Random Switching Logic)[3]が挙げられる。RSLは鍵に依存した消費電力の偏りを根本的に排除することで，暗号回路をDPAによる攻撃から防御する。**図5**は，既存の対策回路とRSL回路を筆者らがFPGA(Field Programmable Gate Array)に実装し，攻撃結果を比較した

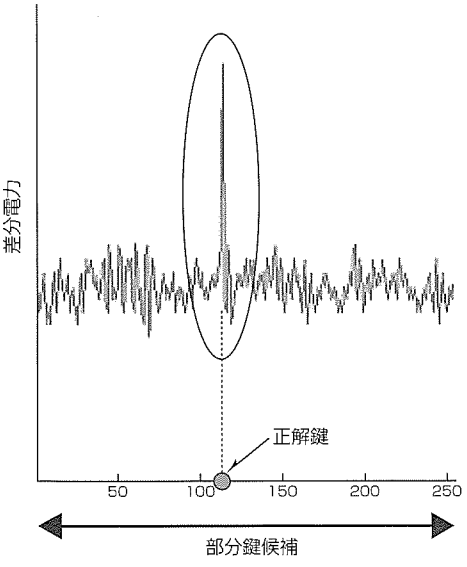


図3．DPAによる部分鍵の攻撃結果例

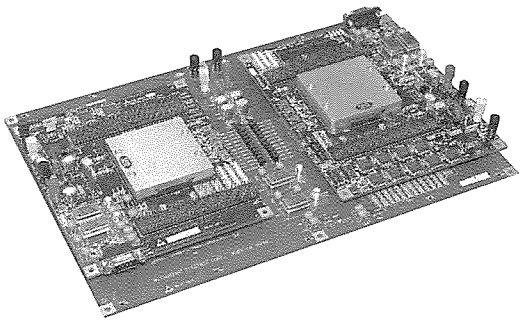


図4．三菱電機製評価用プラットフォーム(SCAPE)の外観

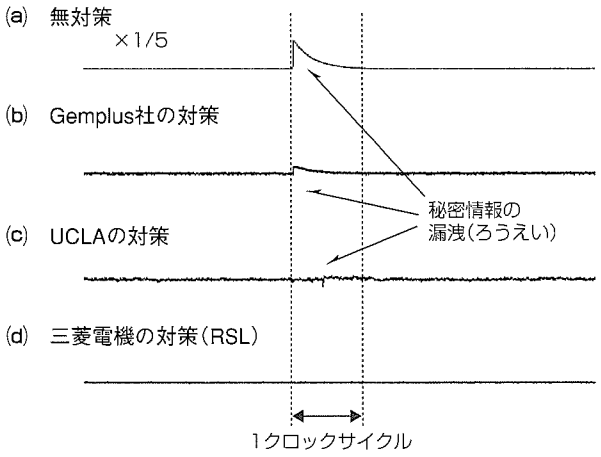


図5．DPAによる攻撃結果の比較例

ものであり，各回路に対するDPAの統計処理結果(DPAトレース)を縦に並べて表示している。DPAトレース上に有意なスパイクが存在すると，その回路はDPAによって鍵が求められる可能性がある。無対策回路と比較すると，どの対策回路もDPAに対して効果があるが，中でもRSLの効果が特に高いことがわかる。なお，RSLはDPAだけでなく，差分電磁波攻撃などの他の強力な攻撃に対しても極めて高い安全性を備えていることを確認している。RSLは，あらゆる暗号アルゴリズムのハードウェア実装に汎用的に適用可能な技術である。

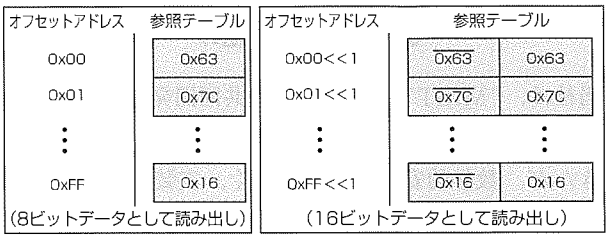
暗号アルゴリズムをソフトウェアで実装する際，メモリ上に用意したテーブルを参照することがよく行われる。この場合，メモリの特性によっては，読み出すデータのハミング重み(1であるビットの数)に依存した消費電力の差が発生し，DPAによって攻撃可能となることがある。このような場合は，例えば，**図6**の(b)に示すように本来のデータとその1の補数をセットにしたテーブルを用意し，テーブル参照後の演算時には本来のデータ部分のみを用いることで，処理性能を低下させることなく，DPA耐性を向上できる。同様の手法は，ハードウェアによる実装の場合でも有効である。

本稿では詳細は割愛するが，サイドチャネル攻撃全般に対して耐性を持つ楕円曲線暗号(Elliptic Curve Digital Signature Algorithm：ECDSA署名)の実装技術として，当社，NTT，㈱日立製作所が共同開発した"CRESERC(クレサーク)"が挙げられる。

一般に，耐タンパー性向上のためには，性能，回路規模，プログラムサイズなどに何らかのオーバーヘッドを伴う。当社は，要求されるセキュリティレベルに応じ，オーバーヘッドが最小となるような対策技術を追求し続けている。

4. 公的機関の取り組みや標準化動向

サイドチャネル攻撃が登場して以来，その解析方法や対策方法が国内外で盛んに研究され，耐タンパー性の重要性に関する認識も広まってきた。国内では，CRYPTREC(CRYPTogpahy Research and Evaluation Committees)や㈶日本規格協会　情報技術標準化研究センター(INSTAC)などが，サイドチャネル攻撃や耐タンパー技術の調査を進めるとともに，標準的評価プラットフォームの仕様(INSTAC-8/32)を策定し，その仕様に準拠した評価プラットフォームを企業や大学に配布している。当社製評価用プラットフォーム(SCAPE)もこの仕様に準拠したものの一つである。また，2006年度に経済産業省の委託事業の中で(独)産業技術総合研究所と東北大学が開発したサイドチャネル攻撃用標準評価ボード(SASEBO)は，当社も開発に参画し，SCAPEの技術や知見を投入したものである。



(a) 通常のテーブル　(b) ハミング重み一定化テーブル

図6．テーブル参照時のハミング重み一定化の例

耐タンパー性に関する客観的な安全性評価基準としては，米国連邦標準規格FIPS 140，国際規格ISO/IEC 19790，日本工業規格JISX 19790などや，それぞれに対応した試験要件規格が挙げられる。特に，現在策定中のFIPS 140-3には，サイドチャネル攻撃に対するセキュリティ要件が多く反映される予定である。これらの評価基準は，電子政府の調達基準としても推奨されるものである。CRYPTRECやINSTACは，国内向けの基準策定や，世界標準の基準へのコメント送付などの標準化活動を行っている。当社もこれらの委員会に参加し，耐タンパー性に関する研究や，標準化に貢献している。

このように，サイドチャネル攻撃や耐タンパー技術の研究や標準化は着実に進められているが，十分なメカニズムの解明や対策方法の確立など，今後の研究成果に期待するところが大きいことも，また現状である。

5. むすび

情報セキュリティに対する新たな脅威の一つであるサイドチャネル攻撃に関して，当社が保有する評価・対策技術と，公的機関の取り組みなどを述べた。今後，安全な情報化社会の実現に向けて，暗号モジュールの実装面の安全性(耐タンパー性)がますます重要になっていく。当社はその実現に向けて継続して取り組んでいく。

参考文献

(1) 市川哲也，ほか：サイドチャネルアタック評価用プラットフォームの開発，2004ソサイエティ大会講演論文集，IA-7-2 (2004)

(2) 佐伯　稔，ほか：RSL技術を用いた耐DPA暗号LSIの設計手法―設計段階における事前DPA評価―，2008年暗号と情報セキュリティシンポジウム(SCIS2008)，2A1-4 (2008)

(3) Suzuki, D., et al.：Random Switching Logic: A New Countermeasure against DPA and Second-Order DPA at the Logic Level, IEICE Trans. Fubdamentals E90-A(1), 160～168 (2007)

暗号アルゴリズムのハードウェア実装技術

鈴木大輔*

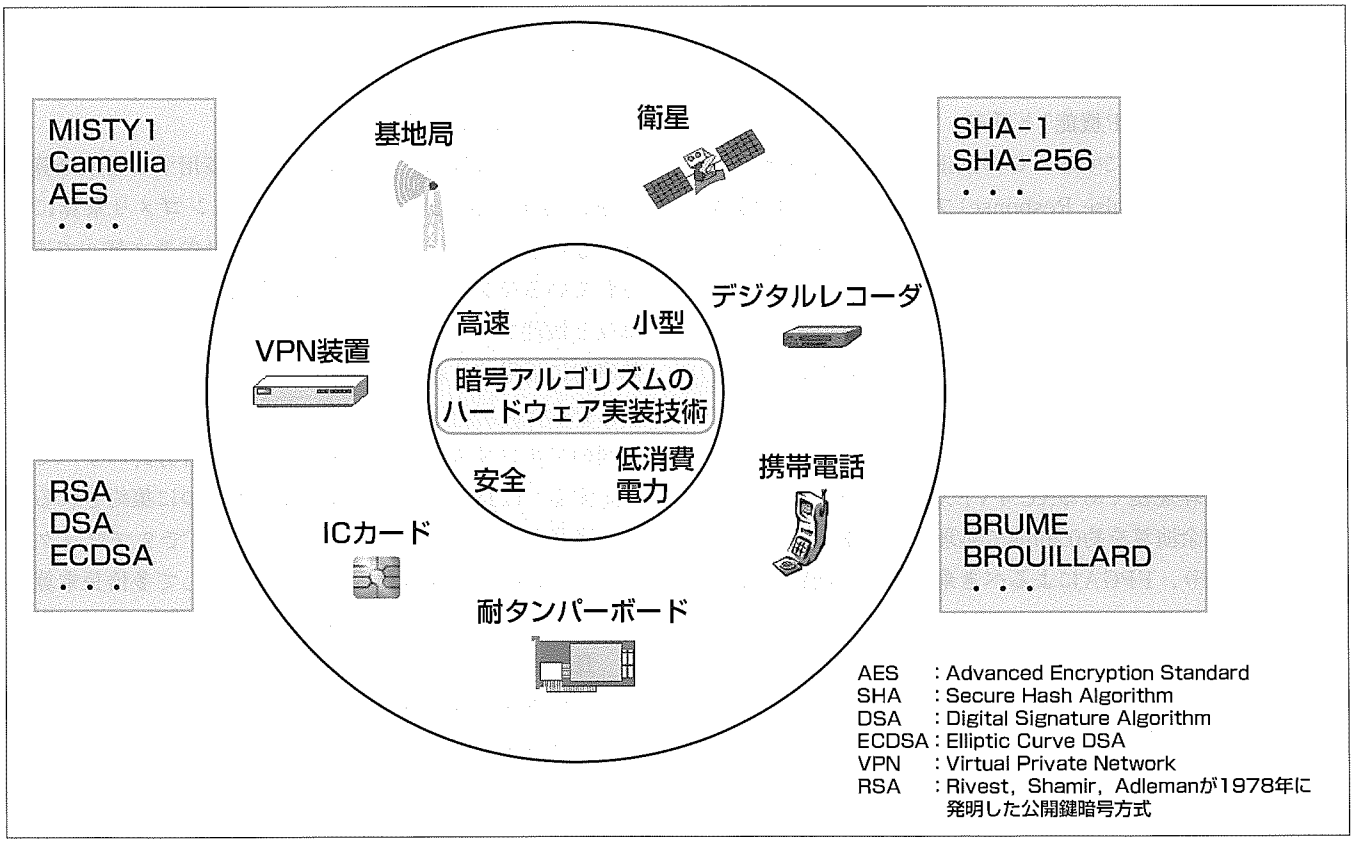
Hardware Implementation for Cryptographic Algorithm

Daisuke Suzuki

要　旨

近年，小型機器やデバイス単体が通信機能を持つことによってセキュリティ機能が不可欠となりつつある。また，ネットワークの高速化に伴い，SSL(Secure Socket Layer)等で必要な暗号化処理をより効率的に装置内で処理することが求められている。従来の高速化手法としては，ASIC(Application Specific Integrated Circuit)やDSP(Digital Signal Processor)を用いたアクセラレーションが一般的である。しかしながら，ASICの開発はコストが高く，セキュリティの要件上，アルゴリズムやそのパラメータが変更されうる暗号処理に対し，柔軟性に乏しい。またDSPを用いた処理方式は，ソフトウェアをベースに構築可能なため，柔軟性は高いが，ASICと比較すると処理性能は劣る。柔軟性と性能を満たす解決策として，FPGA(Field Programmable Gate Array)を用いた処理方式が提案されている。FPGAは，開発コストが低く，回路の変更が可能なため柔軟性が高い。また，容易に実動作までの実現が可能である。三菱電機はセキュリティ機能の中でも処理が重いとされる公開鍵(かぎ)暗号系の処理をFPGA上で専用LSI並みの高速処理を可能とするハードウェア実装技術を開発した。当社が試作したべき乗剰余演算回路は512ビットのべき乗剰余演算を約0.26msで処理可能である。これは，筆者が知る限り，FPGAによるべき乗剰余演算回路としては世界最速である。また，回路規模は4,000slices程度であり，Virtex-4(注1)シリーズで最小の論理規模のFPGA上でも実装可能である。この技術によって様々な機器で低コストに暗号処理のアクセラレーションが可能となる。

(注1)　Virtexは，Xilinx, Inc. の登録商標である。



暗号アルゴリズムのハードウェア実装技術とアプリケーションへの展開

ICカード等の小型機器から携帯基地局向けの高速通信機器まで，暗号アルゴリズムのハードウェア実装技術は幅広く展開されている。

*情報技術総合研究所

1. まえがき

RSA暗号に代表される公開鍵暗号のハードウェアによる高速実装に関する研究は，これまでに数多く行われており，特にモンゴメリ乗算[1]を処理する回路アーキテクチャの提案は多数存在する。これらの研究は大きく分けて2つの議論がある。一つは一般的なCMOS(Complementary Metal Oxide Semiconductor)ゲートでの実装を想定した効率的なアーキテクチャの議論であり，二つ目はFPGA等の特定のデバイスに特化したアーキテクチャの議論である。

後者の議論は，ここ10年ほどの間でFPGAのアーキテクチャが大きく進化していることを背景としている。現在のFPGAは，ユーザーロジックを構成するために存在するRAM(Random Access Memory)ベースのルックアップテーブル(LUT)とフリップ・フロップ(FF)の他に，マルチプレクサ(MUX)，シフトレジスタ及び2値加算器等の基本機能や大規模の2ポートメモリや乗算器等があらかじめハードマクロとして搭載されている。このため，CMOSゲートレベルでの効率的な回路アーキテクチャがFPGA上でも効率が良いとは限らず，前述のようなあらかじめ搭載されているハードマクロを活用したアーキテクチャが提案されるようになった。

FPGAベンダのXilinx社が発表したVirtex-4シリーズやSpartan-3A(注2) DSPシリーズは，従来の乗算機能単体ではなく，複数パターンの積和演算処理を動的に変更可能とした機能ブロックをハードマクロとして搭載している。以下この機能を“DSP機能”と呼び，このハードマクロを“DSP48”と呼ぶことにする。このDSP機能の活用例として高速FIR(Finite Impulse Response)フィルタや，画像処理用のコーデックなどの回路についてはいくつか報告があるが，暗号処理に関する報告は数少ない。本稿では，このDSP機能の性能を最大限に引き出し，モンゴメリ乗算及びべき乗剰余演算を処理する回路構成とその諸性能について述べる。

本稿で述べるべき乗剰余演算回路は，Virtex-4シリーズで最小の論理規模であるXC4VFX12-10上で，512ビットべき乗剰余演算を約0.26msで処理可能である。これは，筆者が知る限り，FPGAによるべき乗剰余演算回路としては世界最速である。

2. 処理方式

ここでは，RSA暗号等の公開鍵暗号系の処理で支配的となるモンゴメリ乗算と，その繰り返し処理であるべき乗剰余演算の高速演算アルゴリズムについて述べる。

2.1 設計方針

高効率なハードウェア実装を実現するために，次に示す4つの設計方針に基づき回路構成を検討した。

①DSP48が最大動作周波数で動作可能な構成

②モンゴメリ乗算中，DSP48の処理はストールが発生しないような構成

③512ビットや1024ビット等の複数のビット長を同一の回路で処理可能な構成

④最小論理規模のFPGAに実装可能な構成

①及び②はFPGAの持つハードマクロの性能を完全に引き出すための設計方針である。③は，実装のターゲットがFPGAであるため，ビット長に応じた回路を再コンフィギュレーションすることで対応する方式も考えられる。しかし，FPGAの再コンフィギュレーション時間は数ms～数十msかかることが知られており，アプリケーションによっては許容されない。加えて，DSP48が持つ演算パターンをダイナミックに切り替える機能をフル活用する意味でも，③を要件とした。④は，筆者の経験上，暗号の演算を行うためだけに大規模のFPGAを使用し，かつそのリソースをほとんど使用するようなケースはまず考えられない。一方で，具体的にどの程度の回路規模が一般に許容されるかを定量的に示すことは難しい。これらのことから，わかりやすい目安として，各FPGAのシリーズで最小論理規模のデバイスをターゲットとした場合でも実装可能であるという基準を設けた。Virtex-4シリーズの場合，最小論理規模のデバイス名はXC4VFX12-10であり，この場合，利用可能なリソースは，5,472 slices，32 DSP48，36 BRAM(Block RAM)となる。

2.2 モンゴメリ乗算

モンゴメリ乗算は，公開鍵暗号系で多用する剰余乗算を，高速に処理する方式の一つである。モンゴメリ乗算には様々なバリエーションがあるが，我々は参考文献(2)で述べられているモンゴメリ乗算の処理方式に対して，その処理単位と処理フローを拡張し，またFPGAのハードマクロを効率的に活用できるように改良した。**図1**にそのアルゴリズムを示す。

図のアルゴリズムは**2.1節**で述べた設計方針のすべてを満足する。改良のポイントは，以下の3つに集約される。

①各多倍長加算処理は，1回のループで2ブロック分(34ビット)の加算を行い，それに対して多倍長乗算処理は半分のループ回数($\alpha r/2$)で処理する方式への改良である。これによって，DSP48は最大動作周波数で動作させつつ，他のユーザーロジックはその半分の動作周波数で動作すれば全体のスループットを維持できるようになるため，ハードマクロ以外で構成される回路のタイミング制約が緩和され，現実的な回路が構成可能となる。

②分岐処理の導入によって，Algorithm 1をパイプライン処理した際にストールを回避可能な処理フローを実

(注2) Spartanは，Xilinx, Inc. の登録商標である。

Algorithm 1 Montgomery Multiplication for Virtex-4

Setting
基数: $2^k = 2^{17}$, レイテンシ定数 : $d = 1$,
DSP48 の個数 : $\alpha = 17$,
$2 < M < 2^h$, $h \in \{512, 1024, 1536, 2048\}$
$0 \leq A, B < 2^{h'}$, $h' = h + 35$
ブロック長: $n = \lceil h'/17 \rceil$,
1 つの DSP48 が処理するブロック数 : $r = \lceil n/17 \rceil$,
$A = \sum_{j=0}^{\alpha r-1} (2^{17})^j a_j$, $B = \sum_{j=0}^{n+1} (2^{17})^j b_j$,
$M'' = \sum_{j=0}^{\alpha r-1} (2^{17})^j m_j$, $S_i = \sum_{j=0}^{\alpha r-1} (2^{17})^j s_{(i,j)}$,
$a_j, b_j, m_j, s_{(i,j)} \in \{0, 1, \cdots, 2^{17} - 1\}$,
$j \geq n$ のとき $a_j = b_j = 0$,
$j \geq \lceil h/17 \rceil$ のとき $m_j = 0$

Input A, B, M''
Output $\mathrm{MM}(A, B) = S_{n+3} \equiv ABR^{-1} \bmod M$,
$0 \leq S_{n+3} \leq 2\tilde{M}$

```
begin
  S_0 := 0; q_{-1} := 0;
  for i:=0 to n + 1 do
    carry := 17'b0; cv := 1'b0; cs := 1'b0;
  /* 多倍長乗算処理 1 : MUL_AB */
    for j:=0 to αr − 1 do   carry| p_j := b_i a_j + carry;
  /* 多倍長乗算処理 2 : MUL_MQ */
    for j:=0 to αr − 1 do
      if(j = 0) carry| v_0 := q_{i−d} m_j + p_0;
      else      carry| u_i := q_{i−d} m_j + carry;
  /* q_i の導出処理 : ADD_V0S1 */
      q_{i+1} := v_0 + s_{i,1};
  /* 多倍長加算処理 1 : ADD_PU */
    for j:=0 to αr/2 − 1 do
      if(j = 0) cv|v_1|v_0 := (p_1|17'b0) + (u_1|v_0);
      else   cv|v_{2j+1}|v_{2j} := (p_{2j+1}|p_{2j})
                                 +(u_{2j+1}|u_{2j}) + cv;
  /* 多倍長加算処理 2 : ADD_VS */
    for j:=0 to αr/2 − 1 do
      cs|s_{(i+1,2j+1)}|s_{(i+1,2j)} := (v_{2j+1}|v_{2j})
                                 +(s_{(i,2j+2)}|s_{(i,2j+1)}) + cs;
  end for
  S_{n+3} := S_{n+2}|s_{(n+1,0)};
end
```

図 1．Virtex-4 向けモンゴメリ乗算アルゴリズム

現している。

③DSP48の使用個数 a を固定したアルゴリズムとなっているため，異なるビット長の入力に対しても同一の回路で処理可能である。

3. ハードウェア構成

ここでは，Algorithm 1 を効率的に実行する回路構成について述べる。**図 2** はAlgorithm 1 の各処理を行う基本回路である。

入力A及びM''は34ビット(2ブロック)ごとに左から入力し，それぞれ所定のDMEM(Data MEMory)に格納する。M''はべき剰余演算の開始直後に格納するだけでよい。よって，モンゴメリ乗算ごとに更新するのはAのみである。DMEMはシングルポートメモリで構成している。一番の左のDMEMにa_j($0 \leq j \leq r-1$)が格納された段階でその下部に接続される回路はAlgorithm 1 に従って処理を行う。最下位ブロックの乗算処理(MUL_AB,MUL_MQ)を担当するDSP48は，キャリーの有無に応じて演算を切り替えながら処理を行う。それ以外のDSP48はキャリーの経路に応じて演算機能を切り替えて処理を行う。

ADD_PUの処理は，図の中段に示した加算器とLA 1 (Latency Adjuster 1)で構成される回路で行う。まず，DSP48から出力されるMUL_ABの演算結果はクロック(clk 1)の立下りで2ブロック同時に加算器に入力する。このとき，他の入力はすべて0にクリアすることで，MUL_ABの演算結果をそのままLA 1 に格納する。続いて，MUL_MQの演算結果に対しては，あらかじめLA 1 に格納されたMUL_ABの演算結果と加算処理を行う。このとき，MUL_ABとMUL_MQの演算結果が入力される時間差は，r/2サイクルとなる。加算処理のけた上げ伝播は，再度同じ加算器への伝播か，又は隣の加算器への伝播の2つのケースに対応する必要がある。図の回路では，タイミングを改善することを目的として，双方のケースごとに異なるけた上げ用のFFを実装している。

図の下段に示した回路はADD_VSの処理を行う。この回路はADD_PUの演算結果が出力されたタイミングでLA 1 及びLA 2 から出力される$s_{(i,\ 2j+1)}$及び$s_{(i,\ 2j+2)}$の2ブロックに対して同時に加算処理を行う。このとき，$s_{(i,\ 2j+2)}$は，最初のサイクルのみ図中右側のLA 1 の出力となり，以降は左側のLA 2 の出力となることに注意する。

以上の構成によって，**2. 1節**で述べた設計方針のすべてを満足する処理が実現できる。より詳細なハードウェア構成については参考文献(3)を参照されたい。

4. ハードウェア性能

図 2 で示したモンゴメリ乗算回路をベースに試作したべき乗剰余回路の諸性能を示す。**表 1** にXC4VFX12-10SF363をターゲットデバイスとして配置配線した結果と従来研究との比較を示す。この処理性能は，筆者が知る限りFPGAによるべき乗剰余演算回路としては世界最速である。また，使用SLICE数は4,000slices程度であり，Virtex-4 シリーズで最小の論理規模のFPGA上でも実装可能である。加えて，512ビットから2048ビットまでのべき乗剰余演算を同一の回路で処理することが可能であり，高いスケーラビリティを持つ。

5. むすび

公開鍵暗号のハードウェアによる高速実装を例として暗号アルゴリズムのハードウェア実装技術について述べた。このほかに，ブロック暗号やストリーム暗号及びハッシュ関数等のセキュリティシステムの構築に必要な機能についても数々のハードウェア開発実績がある。

今後の展開として，これらハードウェア実装技術を駆使し，アプリケーションごとに最適化した開発を行っていく。

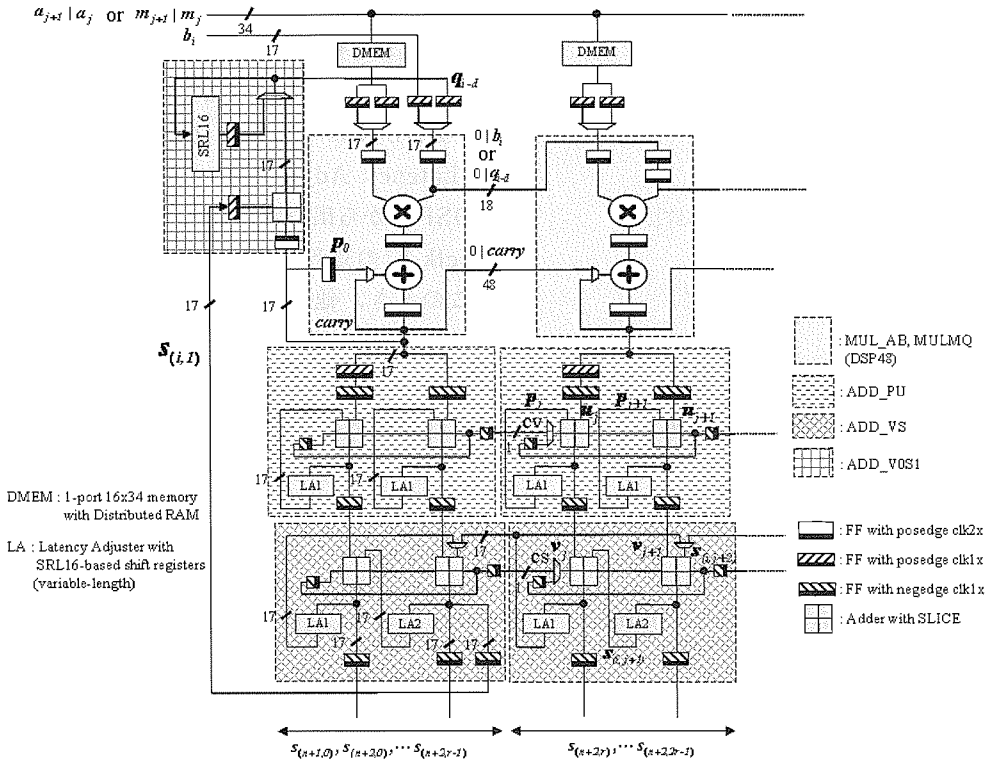


図２．モンゴメリ乗算回路

表１．試作回路の諸性能及び従来研究との比較

Architecture	提案手法	参考文献(4)	参考文献(5)
Target device	XC4VFX12-10	XC2V3000-6	XC40250XV
Scalability	Y	N	N
512bit MEX time	0.26ms(max)	0.59ms(avr)	2.93ms(max)
512bit MEX area	3937slices +17 DSP48	8235slices +32 multipliers	3413slices
1024bit MEX time	1.71ms(max)	2.33ms(avr)	11.95ms(max)
1024bit MEX area	3937slices +17 DSP48	14334slices +62 multipliers	6636slices

＊　MEX：べき乗剰余演算

代表的な用途としては，VPNに代表されるネットワーク機器，携帯電話やその基地局，耐タンパーボード等が挙げられる。また，サイドチャネル対策技術との融合を図り，ICカード等のハイレベルなセキュリティを要求されるような用途へも展開し，適用範囲を拡大していく予定である。

参考文献

(1) Montgomery, P.L.：Modular Multiplication without Trial Division. Mathematics of Computation, **43**, No. 170, 519～521 (1985)

(2) Orup, H.：Simplifying quotient determination in high-radix modular multiplication, Proc. of the 12th Symposium on Computer Arithmetic, 193～199 (1995)

(3) Suzuki, D.：How to Maximize the Potential of FPGA Resources for Modular Exponentiation. CHES 2007, LNCS, **4727**, 272～288 (2007)

(4) Blum, T., et al.：High－Radix Montgomery Modular Exponentiation on Reconfigurable Hardware, IEEE Transaction on Computers, **50**, No.7, 759～764 (2001)

(5) Tang, S. H., et al.：Modular Exponentiation using Parallel Multipliers, FPT 2003, 52～59 (2003)

ブロック暗号アルゴリズム実装性能評価

中嶋純子*
松井　充**

Performance Evaluation of Block Encryption Algorithms on Core2

Junko Nakajima, Mitsuru Matsui

要　旨

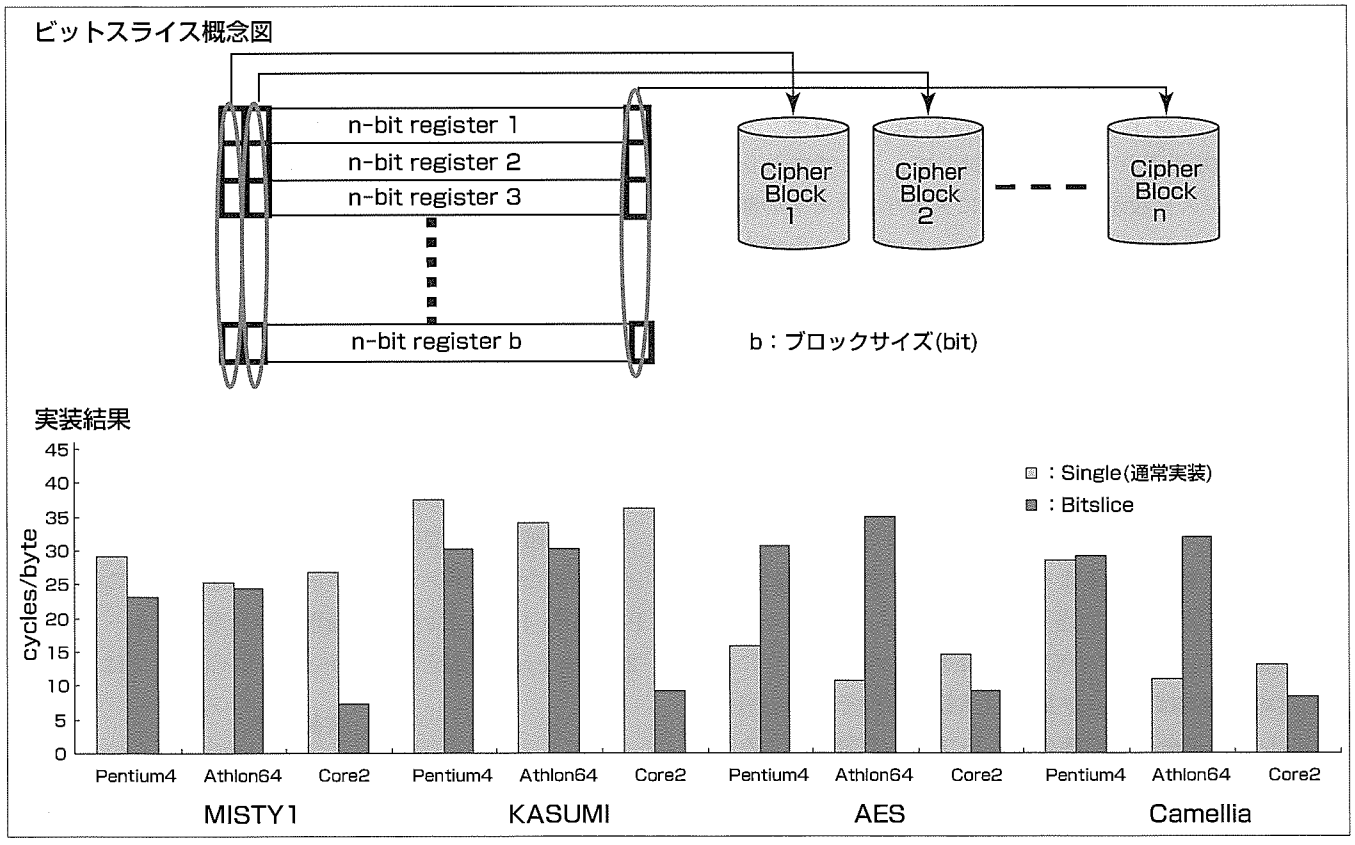
ブロック暗号のソフトウェアによる高速化手法である“ビットスライス実装”を，Intel(注1)の新しいプロセッサCore 2 (注1)に適用した結果について述べる。ビットスライス実装はこれまでRISC(Reduced Instruction Set Computer)プロセッサ上で特に有効性が実証されてきた一方で，PC(x86)プロセッサ上では次に示す理由によってあまり利用されることがなかった。

(1) PCプロセッサはレジスタ数が少ないため，ビットスライス実装ではメモリアクセスの頻度が高くなり，これが速度のボトルネックになる。

(2) ビットスライス実装は特殊なデータフォーマットを利用するので，既存の実装とデータの互換性を保持するためには，暗号化／復号処理の前後にフォーマット変換処理を必要とする。

本稿ではCore 2プロセッサで大幅に強化されたSIMD(Single Instruction Multiple Data)整数命令を用いて(1)(2)の課題がともに克服できることを明らかにする。またこの結果KASUMIが通常の実装の4倍高速化できること，AES(Advanced Encryption Standard)でも既存の結果よりも高速な実装がビットスライスで実現できることを示す。ビットスライス実装は，その潜在的な高速性のみならず，今後暗号化モードとして主流になるとみられるCTR(CounTeR)モードなどで使用可能であることに加えて，キャッシュ攻撃のようなサイドチャネル攻撃に対して安全であるという有効な長所も備えているため，今後実用面でもますます重要になると考えられる。

(注1)　Intel，Coreは，Intel Corp.の登録商標及び商標である。



ブロック暗号アルゴリズム実装性能評価

ビットスライス実装の基本的概念を上図に示す。ビットスライス実装ではn-bit長のCPU(Central Processing Unit)レジスタを用いて，nブロック分のデータを並列に処理する。このとき，ソフトウェア1命令が，n個のハードウェアロジックゲートに相当する演算となる。また上記グラフはブロック暗号アルゴリズム(MISTY1，KASUMI，AES，Camellia)を各種プロセッサ上で実装した結果を示す。ビットスライス実装をCore2に適用した結果，KASUMIが通常の実装の4倍高速化でき，AESでも従来よりも高速な実装を実現した。

*情報技術総合研究所　**同研究所(情報理工博)

1. まえがき

本稿では，暗号のソフトウェアによる高速化手法である“ビットスライス実装”を，Intelの新しいマイクロアーキテクチャとして初めて登場したCore 2プロセッサ上に適用した結果について述べる。

Core 2はPentium 4(注2)(NetBurstアーキテクチャ)の次の世代のプロセッサであるが，その構造からみるとPentiumⅢ，PentiumMの延長上にあると考えられる特徴を持つ。これまで最先端プロセッサに対する性能比較は，暗号アルゴリズムの実装のみならず，様々なベンチマークテスト等によって評価及び議論の対象となっているが，暗号実装という観点から見るとアーキテクチャによって同じプログラムの速度が全く変わるという事実から，プラットフォームの変遷の過程に沿って，最適な実装法を検討することは重要であると考えられる。

一方，ビットスライス実装とは1997年にBihamが提案した複数ブロックを並列に処理するソフトウェアによる実装方法であり[5]，n-bit長のレジスタを用いた1ソフトウェア命令をn個のハードウェアロジックゲートとみなした処理を行う。そのため，暗号アルゴリズムのハードウェア規模が小さくターゲットプロセッサのレジスタ数が多い場合，この実装法での高速化が期待できる。また，鍵(かぎ)の値に依存したテーブル参照がないことからキャッシュ攻撃のようなサイドチャネル攻撃に対して安全であるという利点を持つ。

これまで，ビットスライス実装はRISC型プロセッサ上で有効性が実証されてきたのに対して，PCプロセッサ(x86)はレジスタ数が少ないためにメモリアクセスの頻度が多くなり，これが速度のボトルネックになることから，この実装には不向きとされていた。今回，我々はCore 2で新たに実現された点としてPentium 4／Athlon64(注3)に比べて特にSIMD命令が強化されたことに注目した。従来のプロセッサ上では，バス幅が64ビットであったために128ビットXMM命令を内部的に2つの64ビット命令に分割して実行しなければならないというボトルネックがあったのに対して，Core 2では128ビット命令を分割することなくそのまま処理できるようになった。これは単純に2倍の性能向上を意味する。さらに3つのALU(Arithmetic and Logic Unit)すべてでXMM命令を実行できるようになったため，例えばレジスタ間論理演算命令はそれに相当するx64レジスタ命令と同等のスループットを発揮できるようになった。このようなSIMD命令の改善によって，これまでのプロセッサ上ではSIMD命令のパフォーマンスの悪さがネックとなっていたビットスライス実装法で，Core 2上では性能が大きく向上することが期待できるようになった。

そこで，新たに128ビット環境を活用し，新しいプロセッサのアーキテクチャを考慮しながらブロック暗号(MISTY，KASUMI，AES，Camellia)のソフトウェア実装について検討し，高速化手法について考察を行った。

この結果，まずKASUMIがビットスライス実装では通常の実装の4倍高速化できることを示した。MISTY／KASUMIは元来ハードウェアサイズが小さいアルゴリズムであるという特長が生かされ，PentiumⅢ上でもすでにビットスライス実装の方が普通の実装よりもやや高速という結果を得ていた[8]。それに対してAESではこれまでのプロセッサ上では常に普通の実装の方が高速であったのだが，Core 2上ではついにビットスライス実装の性能が普通の実装よりも上回るという初めての結果を確認した。

表1に我々がソフトウェアプログラム開発及び測定に用いた実装環境を示す。

2. Core 2アーキテクチャ

Pentium 4ではパイプラインを細かく切って動作周波数を上げるとともに，デコード後にマイクロオペレーション(μ ops)と呼ばれるRISC命令をトレースキャッシュに蓄えてループ処理効率を上げるという特徴を持っていた。ところがプロセッサの高周波数化を優先し，またキャッシュサイズを肥大化したことによる弊害として消費電力の増大が問題となった。それに対してCore 2では，1コアでモバイル分野にも適応するために低消費電力化が不可欠であったことから周波数よりもスケーラビリティを上げる方向に転じている。Core 2のパイプラインステージ数は14で，これは従来Pentium 4(Prescottコア)の半分以下となっている。またPentium 4にみられたトレースキャッシュを伴ったデコードではなく，オンラインでのデコード方法になった点はそのメカニズムも含めてPentiumⅢに似ている。またPentiumMにみられたfusion機能がCore 2ではより強化されており，fused μ opsはAthlon64のmacro-operationと非常によく似たものとなっている。

表2に暗号実装で主として用いる命令について実験によって求めたレイテンシとスループットを示す。この表で，Pentium 4のx64命令では論理演算命令のスループットが2μ ops/cycleを超えていなかったが，Core 2では3μ ops/

表1．実装環境

Processor Name	Intel Pentium4 561	AMD Athlon64 3500+	Intel Core2 Duo E6400
Core Name	Prescott	Winchester	Conroe
Clock Frequency	3.6GHz	2.2GHz	2.13GHz
Cache(Code／Data)	12Kμ ops／16KB	64KB／64KB	32KB／32KB
Memory	1GB	1GB	1GB
Operation System	Windows XP 64-bit Edition		
Compiler	Microsoft Visual Studio 2005		

(注2) Pentiumは，Intel Corp.の登録商標である。
(注3) Athlonは，Advanced Micro Device, Inc. の商標である。

cycleに向上したこと，またPentium4で右シフト命令と左右ローテート命令のレイテンシが極端に長かったのがCore 2では改善されていることが確認できた。さらに，XMM命令ではレジスタ間の移動及び論理演算命令のスループットが1から3になり，同時に以前は長かったレイテンシも改善され，x64命令と同等性能になっている。一方，Core 2の最も大きなボトルネックは命令フェッチが1サイクルあたり最大16バイトという制限に起因するものと考えられる。実際にプログラムの高速化を行う場合には，ニーモニック及びレジスタの選択によってできる限り命令長を短くする等の工夫が必要である。

3. KASUMI

UMTS／GSM(Universal Mobile Telecommunications System／Global System for Mobile Communications)の標準暗号である64-ビットブロック暗号KASUMIは，MISTYをベースとした設計によってハードウェア向きの構造を持ちビットスライス実装での高速化が期待できる。**図1**の左にKASUMIのFI関数を示す。図の右は，等価変形することによってFI関数に要する命令数を削減可能であることを示す。MISTY，KASUMIはともにドミナントな内部関数であるFI関数の中にS7，S9と呼ばれる2種類のS-boxを持つが，その数がMISTYは3(S7-S9-S7)に対してKASUMIでは各2の計4である。そのためテーブル参照の総数の違い(KASUMI=96，MISTY=76)が決定的な要因となり，KASUMIはMISTYよりも暗号化処理が低速である。その一方で，**図2**に示すようにKASUMIの鍵スケジュールは非常にシンプルであるという特長がある。KASUMIの拡大鍵は秘密鍵と定数とをXOR(eXclusive OR)することで生成され，各段で用いられる副鍵(1段あたり16ビット長×8個)は，拡大鍵及び秘密鍵から切り出された16ビットをそのまま又は固定ビット数だけ左回転したものとなっている。ビットスライス実装ではシフト／回転処理に対して演算が全く発生しないため，KASUMIの鍵スケジュールに要する時間は暗号化処理と比べてごくわずかとなる。**表3**に我々の実装結果を示す。表中のビットスライス(BS)は128ビットXMM命令を用いたビットスライス実装，Single(Sing)は1ブロック単位での通常実装であることを意味する。KASUMIのCore 2でのビットスライス実装は通常実装と比べて暗号化処理は4倍，鍵スケジュールでは30倍以上高速となることを確認した。

表2．命令のレイテンシとスループット

Processor	Pentium4	Athlon64	Core2
Operand type	64－bit general registers		
mov reg，(mem)	4，1	3，2	3，1
mov reg，reg	1，3	1，3	1，3
add reg，reg	1，2.88	1，3	1，3
xor／and／or reg，reg	1，7/4	1，3	1，3
shr reg，imm	7，1	1，3	1，2
shl reg，imm	1，7/4	1，3	1，2
ror／rol reg，imm	7，1/7	1，3	1，1
Operand type	128－bit XMM registers		
movaps xmm，(mem)	-，1	-，1	-，1
movaps xmm，xmm	7，1	2，1	1，3
paddb／w／d xmm，xmm	2，1/2	2，1	1，2
paddq xmm，xmm	5，2/5	2，1	1，1
xorps／andps/orps xmm，xmm	2，1/2	2，1	1，3
psllw／d／q xmm，imm	2，2/5	2，1	2，1
pslldq xmm，imm	4，2/5	2，1	2，1
punpcklbw／wd／dq xmm，xmm	2，1/2	2，1	4，1/2
punpcklqdq xmm，xmm	3，1/2	1，1	1，1
pmovmskb reg，xmm	-，1/2	-，1	-，1

4. AESとCamellia

AESとCamelliaはともにGF(2^8)の逆元演算に線形同値なS－boxを用いており，この命令数が全体の速度に最も影響をおよぼす。我々が知るビットスライス実装の観点からもっとも小さなS-boxは，部分体を用いるものでありGF(2^8)の逆元をGF(2^4)の演算で構成し，さらにGF(2^4)の演算をGF(2^2)の演算で構成する。ここで指数2の部分体上の基底としてTr(a)＝1となるaに対して(1，a)を採るところが本質である。これによってx，y，z，uを部分体

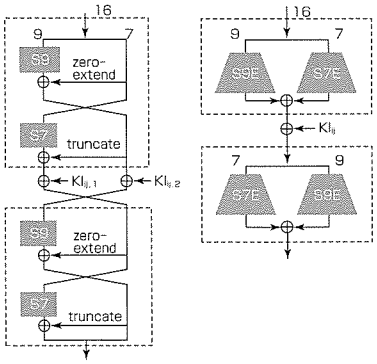


図1．KASUMIのFI関数

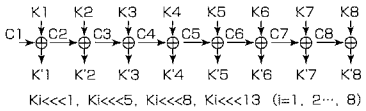


図2．KASUMIの鍵スケジュール

表3．KASUMIとMISTY1の実装結果

Processor	Pentium4		Athlon64		Core2	
KASUMI						
Style	BS	Sing	BS	Sing	BS	Sing
Cy/blk	241	300	241	272	74	290
Cy/byte	30.1	37.5	30.1	34.0	9.25	36.3
Inst/cycle	0.71	1.69	0.71	1.86	2.31	1.75
Cy/Keysch	8	104	7	64	2	78
MISTY1						
Style	BS	Sing	BS	Sing	BS	Sing
Cy/block	185	234	195	203	59	214
Cy/byte	23.1	29.3	24.4	25.4	7.38	26.8
Inst/cycle	0.72	1.82	0.68	2.10	2.26	1.99
Cy/Keysch	57	244	57	240	16	178

表4．AESとCamelliaの実装結果

Processor	Pentium4		Athlon64		Core2	
AES						
Style	BS	Sing	BS	Sing	BS	Sing
Cy/blk	491	256	560	170	147	232
Cy/byte	30.7	16.0	35.0	10.6	9.19	14.5
Inst/cycle	0.80	1.18	0.70	2.74	2.66	2.00
Camellia						
Style	BS	Doubl	BS	Doubl	BS	Doubl
Cy/blk	467	457	510	175	135	208
Cy/byte	29.2	28.6	31.9	10.9	8.44	13.0
Inst/cycle	0.72	0.94	0.65	2.46	2.47	2.07
Format conversion						
Cy/blk	41.5		28.1		15.4	
Cy/byte	2.59		1.76		0.96	
Inst/cycle	0.72		1.06		1.96	

の元とするとき，$(x+ya)(z+ua)=(xz+yuNr(a))+((x+y)(z+u)+xz)a$となるため，GF($2^{2n}$)の乗算がGF($2^n$)の乗算3回(と加算4回)で実現できることとなる[6]。ビットスライスでのS-box 1個あたりの命令数は約200であり，1ブロックあたりAESは160回，Camelliaは144回のS-box参照があることを考慮すると，例えば128ブロック並列処理の場合S-boxの総処理量は1ブロックあたりそれぞれ250命令，225命令の計算となり，これは全命令数の70%程度を占めている。我々のAESの実装結果を**表4**に示す。Core 2での通常実装の性能はPentium 4の通常実装と比べ1ブロックあたりのサイクル数が若干少なくなっているものの，Athlon64と比較するとまだ性能差は著しい。これはAthlon64が1サイクルあたり64ビットのメモリ読み込みが2回できるのに対してCore 2は1回だけである点によっている。一方，128ビットXMMレジスタを用いたビットスライス実装では，Core 2のSIMD命令強化の効果がはっきり現れている。この実装は通常実装よりも50%以上高速であり，また64ビット汎用レジスタを用いたビットスライス実装の2倍の性能を実現している。これは，レジスタサイズが64ビットから128ビットと2倍になったことがそのまま性能に現れているといえる。Pentium 4やAthlon64ではビットスライス実装は通常の実装に比べて50%低速であったことを考えると，Core 2のSIMD命令の性能向上は著しい。筆者らが知る限り，これはAESのビットスライス実装の性能が通常の実装の性能を上回った最初の例である。

次にCamelliaの実装結果についてみると，通常実装でこれまでいずれのプラットフォームでもAESには及ばなかったが，Core 2の2ブロック並列実装(**表4**中にDoubleとして表示)ではAES(通常実装Single)を上回る性能が見られる。アルゴリズムとしての並列度という意味ではAESはCamelliaより明らかに優れているので，この結果は予想されたものである。これに対してビットスライス実装では，いずれのプロセッサでもCamelliaがAESより高速な結果が得られている。これはS-boxの個数がCamelliaの方が16個少ないということが最大の理由である。

ところでビットスライスは特殊なデータフォーマットによって行われるので，主として互換性維持のためには暗号化／復号処理の前後でフォーマット変換を行う必要がある。この変換では全ビット位置を置き換えるため，これをオーバーヘッドとしてとらえると実際には無視できない演算量となる。それがビットスライスの実用化を困難としていた要因の一つであったが，今回のCore 2上での実装では1バイトあたり1サイクル以下の性能を実現したことによって，前後に2回の変換処理を含めても速度性能が通常実装よりも大きく上回るという結果が得られた。

5. むすび

Intelの最新プロセッサであるCore 2は，特にSIMD命令で極めて高い性能を発揮していることを，本稿ではブロック暗号のビットスライス実装の観点から明らかにした。PCプロセッサでAESが通常の実装よりビットスライスの性能がはっきり高くなるという事実は，ビットスライス実装がテーブル参照を行わないためキャッシュ攻撃などの実装攻撃に対しても安全であるという長所と考え合わせると，本稿で示された結果は，今後共通鍵暗号の利用(例えば利用モードなど)を論じる上での一つの転換点ともなり得る結果であると考える。

参考文献

(1) Matsui, M.：New encryption algorithm MISTY, Proceedings of Fast Software Workshop FSE'97, Lecture Notes in Computer Science, 1267, 54～68, Springer-Verlag (1997)

(2) 3GPP TS 35.202 v6.1.0：3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2:KASUMI Specification (2005)

(3) Aoki, K., et al：The 128-Bit Block Cipher Camellia, IEICE Trans. Fundamentals, Vol.E85-A, No.1, 11～24 (2002)

(4) Federal Information Processing Standards Publication 197：Advanced Encryption Standard (2002)

(5) Biham, E.：A Fast New DES Implementation in Software, Proceedings of Fast Software Workshop FSE'97, Lecture Notes in Computer Science, Vol.1267, 260～272, Springer-Verlag (1997)

(6) Nakajima, J., et al：Fast Software Implementations of MISTY1 on Alpha Processors, IEICE Trans. Fundamentals, Vol.E82-A, No.1, 107～116 (1999)

(7) Matsui, M.：How Far Can We Go on the x64 Processors?, Proceedings of Fast Software Workshop FSE2006, Lecture Notes in Computer Science, Vol.4047, 341～358, Springer-Verlag (2006)

ITセキュリティ評価基準ISO/IEC15408と三菱電機グループの取り組み

泉　幸雄*
森垣　努**
山本俊輔**

ISO/IEC15408 IT Security Evaluation Criteria and Our Activities

Yukio Izumi, Tsutomu Morigaki, Shunsuke Yamamoto

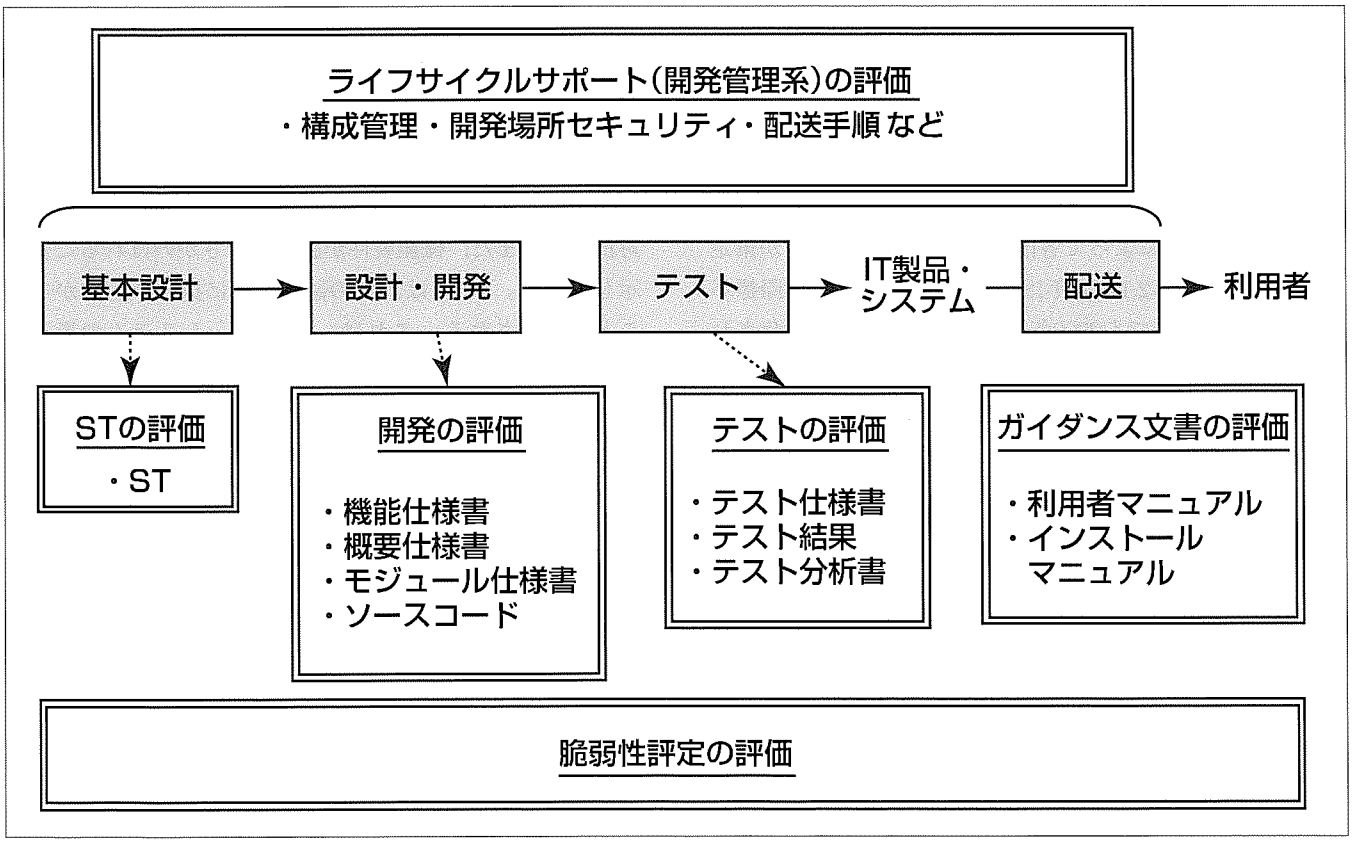
要　旨

近年，ITの普及とともに情報資産の価値が増加し，情報資産を扱うIT製品・システムのセキュリティの重要性が増している。このような状況で，IT製品・システムの利用者は，自分の環境に合ったセキュリティ機能を具備したものを多数の製品の中から調達する必要があるが，自らセキュリティ評価を行うことは多大のコスト・時間がかかるという問題点があった。また，IT製品・システムの開発者は，製品を幅広く販売したくても，それまで国ごとに運用されていたセキュリティ評価制度で，認証取得することはコスト・時間の面で問題があった。

このような背景のもと，公的に認められた第三者がIT製品・システムのセキュリティ評価をするための国際的統一基準CC(Common Criteria)が1999年に作られ，同年ISO/IEC(International Organization for Standardization/International Electrotechnical Commission)15408として国際標準化された。我が国でも，この評価基準を用いた第三者評価認証制度の運用が2001年4月から開始された。

ISO/IEC15408におけるセキュリティ評価はIT製品・システムを様々な側面から検査するため，セキュリティ基本設計書(ST)，設計文書，マニュアル，開発管理文書等の証拠資料が必要となる。評価申請した開発者は，ISO/IEC15408で規定された要件を満たし，所定の内容を含む証拠資料を評価機関に提出し，評価機関によって第三者評価が行われる。

本稿では，このITセキュリティ評価基準ISO/IEC15408及び三菱電機グループにおける取り組みについて述べる。



開発フローとISO/IEC15408評価の観点

図中，一重枠が開発フローを，二重枠が評価の観点を表す。ISO/IEC15408に基づく評価では，セキュリティ基本設計文書(ST)，設計文書，テスト，マニュアルの評価のほか，開発管理にかかわる評価も実施される。また，評価者が独自に脆弱(ぜいじゃく)性分析を行う。評価形態には，開発者が提出した設計文書等の証拠資料の検査，サイト監査，テスト実施がある。ただし，評価保証レベルに応じて評価内容は異なる。

*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

近年，ITの普及とともに情報資産の価値が増加し，情報資産を扱うIT製品・システムのセキュリティの重要性が増している。このような状況で，公的に認められた第三者がIT製品・システムのセキュリティを評価するための国際的統一基準CCが1999年に作られ，同年ISO/IEC15408として国際標準化された。我が国でも，この評価基準を用いた評価認証制度の運用が2001年4月から開始された。

本稿では，このITセキュリティ評価基準ISO/IEC15408及び三菱電機グループの取り組みについて述べる。

2. ISO/IEC15408の概要

ISO/IEC15408は，IT製品・システムのセキュリティ機能が矛盾なく適切に設計され，正しく実装されていることを客観的に評価する国際基準である。ISO/IEC15408以外のセキュリティ関連国際標準として，運用組織のセキュリティ対策に対するISO/IEC27001，暗号モジュールのセキュリティに対するISO/IEC 19790，暗号アルゴリズムを客観的に評価して標準化を行ったISO/IEC18033などがある(**表1**)。これらはすべて第三者評価に関連しているものであり，第三者によるセキュリティ評価は世界的な潮流である。

2.1 ISO/IEC15408の経緯

ISO/IEC15408が策定される以前，米国のTCSEC(Trusted Computer System Evaluation Criteria)，欧州のITSEC(Information Technology Security Evaluation Criteria)など各国独自のセキュリティ評価基準が存在していた。1999年，米国，カナダ，欧州(英国，フランス，ドイツ，オランダ)によって各国の基準を統合したCCが策定され，バージョン2.1が同年ISO/IEC15408として国際標準化された。我が国でも2000年にJIS X5070としてJIS化されている。CCとISO/IEC15408は異なる文書であるが，ほぼ同じ内容であるため，ISO/IEC15408は通称CCと呼ばれる。

策定された当初のCCのバージョンは2.1であるが，これ以降，改定が行われて，現在ではバージョン3.1が使用されている。バージョン3.1では，初期のバージョン2シリーズと内容が若干異なるが，基本的な概念は同じである。本稿はバージョン3.1を対象として述べる。

2.2 ISO/IEC15408の内容

ISO/IEC15408は次の三部構成になっている。

(1) パート1(概説と一般モデル)

このパートには，用語の定義，基本概念やセキュリティ一般モデルが記述されている。また，PP(Protection Profile)と呼ばれる製品カテゴリのセキュリティ要求仕様書やST(Security Target)と呼ばれる特定製品のセキュリティ基本設計書の仕様が記述されている。PPは，一般的にはIT製品・システムの利用者がその製品カテゴリに対するセキュリティ要求を特定のフォーマットに従ってまとめたものであり，第三者評価を受けた後に公開される。我が国では評価済みPPは公開されていないが，欧米ではIT製品カテゴリごとに公開されている。

一方，STはIT製品・システムの開発者によって特定製品に対して作成される。STはPPに準拠して作成されることも，準拠せずに作成されることもある。前述のように我が国にはPPが存在しないので，我が国で評価されたSTのほとんどはPPに準拠せずに作成されたものである。STは，TOE(Target Of Evaluation)と呼ばれる評価対象となるIT製品・システムの概要，想定される脅威や前提条件などセキュリティ的な課題，対策方針，機能要件などが矛盾なく記述されるもので，そのフォーマットはISO/IEC15408で規定されている。**図1**に，課題，対策方針，機能要件における論理的な対応関係を示す。

図1は，定義された課題は対策方針，機能要件によって対抗され，また，機能要件が課題までさかのぼれることを示している。STでは，この論理関係に抜けや矛盾がないことが要求される。これは，IT製品・システムの過不足ないセキュリティ機能を実現するために重要である。

(2) パート2(セキュリティ機能コンポーネント)

このパートは，IT製品・システムが備えるべきセキュリティ機能のカタログ集になっている。例えば，利用者認

表1．第三者セキュリティ評価に関する国際基準

国際標準	内　容
ISO/IEC27001	●運用組織 ●2005年にIS化(ISO/IEC27002は2000年) ●英国規格BS7799がベース
ISO/IEC15408	●IT製品・システム ●1999年にIS化 ●CCとほぼ同じ内容
ISO/IEC19790	●暗号モジュール ●2006年にIS化 ●米国連邦情報処理規格FIPS140－2がベース
ISO/IEC18033	●暗号アルゴリズム ●2005年にIS化

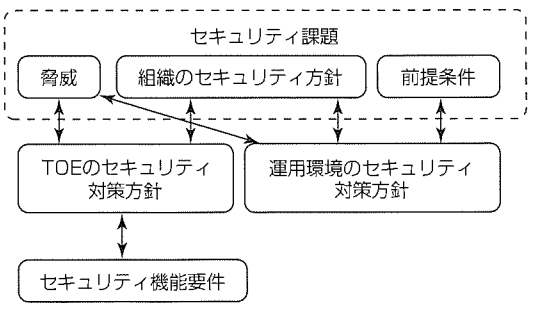


図1．STにおける論理関係

証，アクセス制御，セキュリティ管理，暗号操作などのセキュリティ機能が11の大分類から構成されている。PPやSTの作者は，セキュリティ対策方針を実現するための要件として，これらの中から選択し，STやPPに記載する。また，ISO/IEC15408に定義されていない独自の要件をPPやSTの作成者が定義して使用することも許されている。

(3) パート3（セキュリティ保証コンポーネント）

このパートは，セキュリティ保証要件のカタログであり，設計から製品化に至る過程で，セキュリティ機能が正しく実装されていることを保証するための要件が記載されている。つまり，IT製品・システムの開発者はこれらの要件を満たす必要がある。保証要件は，例えば，設計文書，マニュアルやテストに対する要件，開発管理の手続きや配送手順などに対する要件など8つの大分類から構成されている。

また，保証要件は，評価の深さ・範囲・厳格さの観点でレベル付けされている。そのレベルに応じてパッケージ化されたものが評価保証レベルEAL（Evaluation Assurance Level）であり，ISO/IEC15408ではEAL 1から7まで7段階に定義されている（EAL 7が最高位）。低いEALの要件はより高いEALに包含されている。EALは高ければ良いというものではなく，EALが高くなると，評価にかかるコスト・時間が増加する。したがって，そのIT製品・システムの使用目的や環境，保護対象資産の価値や評価にかかるコスト・時間から総合的に決められるべきである。一般的に，EAL 1からEAL 4までが商用製品対応，EAL 5以上がナショナルセキュリティ対応と言われている。

3. 評価認証制度

3.1 ITセキュリティ評価及び認証制度

我が国で，ISO/IEC15408を評価基準とするITセキュリティ評価及び認証制度（Japan Information technology Security Evaluation and Certification scheme：JISEC）は2001年4月に開始された。この制度を図2に示す。この制度は経済産業省の指導のもとに運用されている。認定機関の審査を受け，公的に認められた評価機関は申請者の依頼によって，ISO/IEC15408に基づいた評価を行う。そして，評価機関は認証機関に評価報告書を提出し，認証機関が認証書を発行する。認証機関と認定機関は，国ごとに一つ存在しており，我が国では，前者は独立行政法人情報処理推進機構（IPA），後者は独立行政法人製品評価技術基盤機構（NITE）がその役を担っている。また，評価機関として2008年1月現在4つの組織がある。

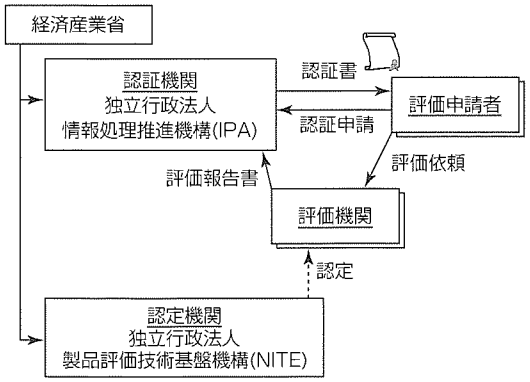


図2．我が国のITセキュリティ評価及び認証制度

また，認証取得済み製品の後続バージョンの製品に対して，当初の認証の効果を継続しようとする保証継続という制度もある。この場合，後続バージョンの製品の評価は不要となる。ただし，後続バージョンに対する変更がセキュリティ的に影響を受ける場合には適用できず，再評価を受け認証を取得しなければならない。

3.2 CCRA

CCRA（Common Criteria Recognition Arrangement）は，CCに基づいた評価・認証を相互に承認する協定である。この協定によって，ある国で認証された製品は，加盟国の中でも認証された製品として扱われる。2008年1月現在で欧米含め25か国が加盟している。CCRAへの加盟の形態は2種類あり，上述の制度を持ち認証書を発行できる国と，制度はないが他国で認証された製品を認証済み製品として受け入れる国がある。我が国は，2003年10月に認証書を発行できる国としてCCRAに加盟している。なお，この協定はCCの枠組みの中でのものであり，ISOとしてのものではない。

4. 動　向

4.1 調達の動向

2005年12月に，内閣官房情報セキュリティセンターで“政府機関の情報セキュリティ対策のための統一基準（全体版初版）”が策定された（2007年6月に第二版が発行された）。この統一基準は，各府省庁が情報セキュリティの確保のために採るべき対策，及びその水準を更に高めるための対策の基準を定めたものであり，ISO/IEC15408の認証取得を活用する内容が不可欠事項として含まれている。

また，ICAO（国際民間航空機関）を中心にして世界各国が取り組んでいるパスポートのICカード化でもISO/IEC15408の認証取得が調達の条件に使用された[1]。このように，ISO/IEC15408による第三者セキュリティ評価を含めた調達は今後も増加していくと想定される。

4.2 認証取得の動向

認証取得製品はOS，データベース，PKI（Public Key Infrastructure），スマートカードなどのほか，近年ではデジタル複合機，デジタルカメラなどもITセキュリティ製品として認証を受けている。2008年3月現在，我が国では146製品が認証取得している。

5. 三菱電機グループの取り組み

5.1 認証取得

三菱電機グループは，2005年に㈱三菱東京UFJ銀行とともに他社に先駆けて金融端末分野でISO/IEC15408の認証を取得した。この金融端末は，コンビニ・ボックス・バンク（CBB）と呼ばれ，エンドユーザーに住所変更届け等の従来銀行窓口で行っていたサービスの一部を提供するために銀行内外の店舗に設置される。**図3**にCBBの外観を示す。

エンドユーザーはRFID（Radio Frequency IDentification）内蔵の専用申込書に必要事項を記入後，本人確認用に暗証番号を端末に入力する。端末では，時刻や暗証番号などの情報を三菱電機の暗号アルゴリズム“MISTY１”で暗号化してRFIDに記録する。暗号鍵は，端末内部に格納されている三菱電機の耐タンパ暗号ボード“TURBO-MISTY”で管理されている。センターに配送された専用申込書は復号され，本人確認後，届け出内容の処理が実施される。

このようなシステムでエンドユーザーの暗証番号は機密性が非常に高い情報である。この情報を保護するための端末が備えるセキュリティ機能，すなわち暗号化機能と保守機能を対象にISO/IEC15408の評価を受けた。評価保証レベルは，評価コストと評価にかかわる時間，サービスを開始するリリース時期との関係などからEAL２とした。

CBBの開発にあたり，効率的にISO/IEC15408の評価認証を受けるため，開発初期の段階からISO/IEC15408の概念を導入した。基本設計，開発，テスト，出荷という開発フローで，初期の基本設計の段階でSTを作成し，セキュリティ機能要件やシステム全体での暗号操作・暗号鍵管理の仕様を決定した。これらのST作成と仕様決定は，並行して行った。つまり，決定された仕様をSTに反映し，また逆にSTの検討結果を仕様に反映させた。ST作成以降の設計・開発・テスト・マニュアル作成などはSTをベースとし，EAL２で規定されている保証要件を従来の開発フローに取り入れながら実施した。これによって，出戻りが少ない効率的な評価を受けることができた。

5.2 ツール開発

従来の開発では作成されていなかったSTを効率的に作成するため，ST作成支援ツールとST評価支援ツールを開発した。作成支援ツールでは，**2.2節**で述べたSTの論理関係を入力することによって，入力内容の矛盾をチェックした上で所定フォーマットのSTファイルを出力する。評価支援ツールは，完成したSTの論理関係を抽出し，その関係の確認を支援するものである。これらのツールの利用によって，ISO/IEC15408になじみのないST作成者でも効率的にSTを作成することができる。

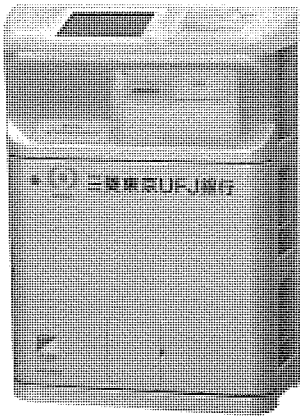


図3．CBBの外観

6. むすび

ITセキュリティ評価基準ISO/IEC15408及び三菱電機グループの取り組みについて述べた。ISO/IEC15408は第三者セキュリティ評価の基準ではあるが，認証取得のみならず，その概念を開発に取り込むことで製品・システムのセキュリティ的品質を向上させることができるものと考えている。

今後も製品・システムのセキュリティ品質を向上させる研究やセキュアな製品・システムの開発に取り組んでいく。

参考文献

(1) 平松雄一：ICカード利用の最新動向，月刊自動認識，1～4（2005-8）

(2) Izumi, Y.：Application of the Common Criteria to a Terminal for Banking Services, 6th International Common Criteria Conference 2005, A2-02 (2005) http://www.ipa.go.jp/event/iccc2005/program.html

(3) 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室：情報技術 セキュリティ評価のためのコモンクライテリア，2006年9月，バージョン3.1 改訂第1版（平成19年3月翻訳第1.2版）http://www.ipa.go.jp/security/jisec/evalbs.html

DSRCシステムにおけるセキュリティ技術

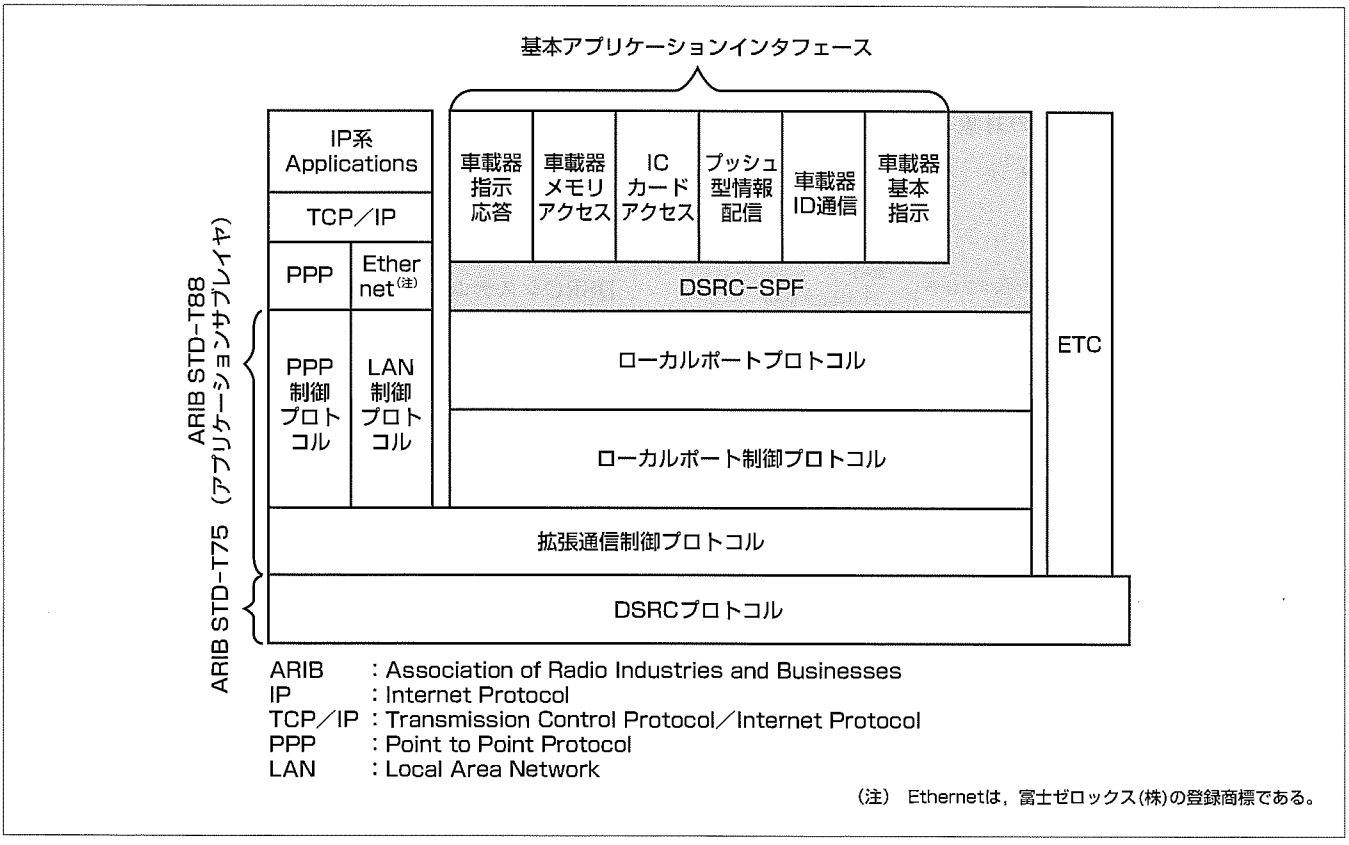
三澤　学*　　小泉　薫†
伊川雅彦**
岡　賢一郎***

Security Technology for DSRC Systems

Manabu Misawa, Masahiko Ikawa, Kenichiro Oka, Kaoru Koizumi

要　旨

DSRCシステム(Dedicated Short-Range Communication System)とは，車両に搭載された車載器と道路に設置された路側機とが通信を行うことで多様なサービスを提供するシステムである。ETC(Electronic Toll Collection System：有料道路自動料金支払いシステム)はDSRCシステムの一つのサービスとしてすでに運用され，利用率70%を超えるほどに普及している(2008年1月国土交通省)。ETC以外のサービスとしては，駐車場自動入退場，ガソリンスタンド自動決済，各種情報提供等が開始されており，DSRCシステムは，ITS(Intelligent Transport Systems)の中核システムの一つとして位置付けられている。DSRCシステムのプロトコルは，路側機－車載器間の無線インタフェースについて規定した(社)電波産業会規格ARIB STD-T75，同規格のDSRCプロトコルの通信機能を補完し複数アプリケーションの実行を可能にするARIB STD-T88(アプリケーションサブレイヤ)，各アプリケーションに対してセキュリティ機能を提供するDSRC-SPF(Security PlatForm)，DSRCシステムで必要とされる基本機能を定義した基本アプリケーションインタフェースで構成される。DSRC-SPFは多種の認証プロトコルに対応可能で，上位のアプリケーションに対して選択可能なセキュリティ機能を提供する柔軟なプロトコルである。



DSRCシステムのプロトコル構成

DSRCのプロトコル構成を示す。DSRCシステムのセキュリティ機能を担うDSRC-SPFは，アプリケーションサブレイヤのローカルポートプロトコルの上位に位置する。DSRC-SPFは車載器－路側器間の相互認証と基本アプリケーションインタフェースのプロトコルデータユニットの暗号化／復号，MAC(Message Authentication Code)生成／検証を行う。

*情報技術総合研究所　**先端技術総合研究所　***姫路製作所　†鎌倉製作所

1. まえがき

DSRCシステムとは，車両に搭載された車載器と道路に設置された路側機とが通信を行うことで多様なサービスを提供するシステムである。ETCはDSRCシステムの一つのサービスとしてすでに運用され，利用率70%を超えるほどに普及している(2008年1月国土交通省)。ETC以外のサービスとしては，駐車場自動入退場，ガソリンスタンド自動決済，各種情報提供等が開始されており，DSRCシステムは，ITSの中核システムの一つとして位置付けられている。特に2006年1月19日に発表された"IT新改革戦略"ではIT政策の重点として"世界一安全な道路交通社会－交通事故死者数5,000人以下を達成－"が掲げられており，安全運転支援システム等の安全・安心への貢献が期待されている。これらのサービスでは，無線通信路上を経由して走行の判断にかかわる情報や金銭にかかわる情報が取り扱われるため，なりすましや盗聴，改ざんといった脅威から路側機及び車載器を保護する必要がある。

本稿では，DSRCシステムにおけるセキュリティ技術であるDSRC-SPFについて述べる。

2. DSRCシステムのプロトコル構成

DSRCシステムのプロトコル構成を図1に示す。ARIB STD－T75は，路側機－車載器間の無線インタフェースについて規定した規格であり，OSI(Open Systems Interconnection)参照モデルの7層構造のうちレイヤ1，レイヤ2，及びレイヤ7を標準化の対象としており，ETCはARIB STD-T75上に位置する[1]。

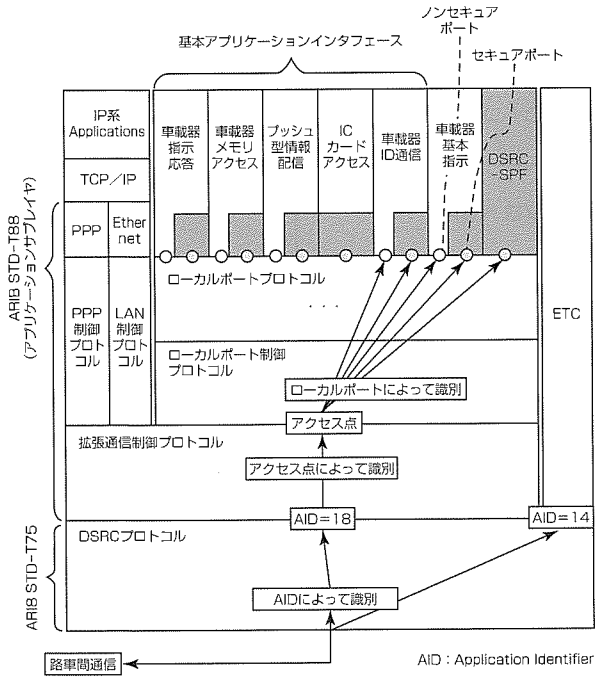


図1．DSRCシステムのプロトコル構成

ARIB STD-T88(アプリケーションサブレイヤ)は，ARIB STD-T75で規定するDSRCプロトコルスタックとアプリケーションの間に位置し，ARIB STD T-75のDSRCプロトコルの通信機能を補完して複数アプリケーションの実行を可能にするとともに，アプリケーションに対してDSRCを意識させないプラットフォームを提供する規格である。アプリケーションサブレイヤのローカルポート制御プロトコルでは，後述の基本アプリケーションに代表される非ネットワーク系におけるマルチアプリケーションへ対応するため，アプリケーションごとにローカルポートを割り当て，アプリケーションを識別する[2]。

DSRC-SPFは，基本アプリケーションインタフェースとアプリケーションサブレイヤのローカルポートプロトコルの間に位置し，車載器－路側機間の相互認証と基本アプリケーションインタフェースのプロトコルデータユニットの暗号化／復号，MAC生成／検証を行う。

基本アプリケーションインタフェースは，ローカルポートプロトコルの上又はDSRC-SPF上に位置し，基本アプリケーションごとに定義された機能を提供する。基本アプリケーションには，DSRC-SPFを利用してアクセスできるローカルポート(セキュアポート)とDSRC-SPFを利用せずにアクセスできるローカルポート(ノンセキュアポート)とが割り当てられており，相互認証が正常に完了した場合にのみセキュアポートへのアクセスが可能となる。ノンセキュアポートに対しては，ICカードアクセスアプリケーションを除いて，相互認証の有無や成否にかかわらずアクセス可能である。

3. 基本アプリケーションとDSRC-SPF[3]

3.1 基本アプリケーションインタフェース

DSRCシステムでは多様なサービスに対応するため，あらかじめ必要と想定される基本アプリケーションを定義している。車載器は基本アプリケーションを実装し，路側機は基本アプリケーションを組み合わせて使用することで提供するサービスを実現するというコンセプトを採用している。そして基本アプリケーションを使用するためのインタフェースを基本アプリケーションインタフェースと呼んでいる。基本アプリケーションの機能は次の通りである。

(1) 車載器指示応答アプリケーション：車載器に対して特定の指示情報を通知するとともに車載器のボタン等で入力された情報を路側機へ返す機能を持つ。

(2) 車載器メモリアクセスアプリケーション：路側機が車載器のメモリに自由な形式で読み書きできる機能を持つ。

(3) ICカードアクセスアプリケーション：ISO/IEC7816対応のICカードと通信できる機能を持つ。

(4) プッシュ型情報配信アプリケーション：車載器に対してコンテンツ又はコンテンツの位置を送信する機能を持つ。

(5) 車載器ID通信アプリケーション：車載器が持つ固有IDを路側機へ通知する機能を持つ。

(6) 車載器基本指示アプリケーション：最小限度のHMI(Human Machine Interface)機能を提供する場合に使用され，車載器に対して特定の指示情報を通知する機能を持つ。

実現されているサービスとアプリケーションの対応例を**表1**に示す。

表に示すサービスに想定される脅威として次のものが挙げられる。

- 駐車場自動入退場／ガソリンスタンド自動決済サービス
  - 入退場や決済に用いるID等の盗聴
  - 車載器のなりすまし
- 情報提供サービス
  - 車載器に提供される情報の改ざん
  - 情報提供側となる路側機のなりすまし

このように，無線通信路上での脅威は大別されるものの，サービスの内容や環境によって想定される脅威は異なるため，必要とされる対策も異なる。DSRCシステムでは走行中の車両にサービスする場合，時間的な制約からすべてのセキュリティ機能を使用することが困難な状況が想定されるため，使用するセキュリティ機能をサービスに応じて適切に選択する必要がある。

また認証プロトコルや暗号方式については，サービス提供者ごとに異なる方式を使用する可能性があり，複数種類のセキュリティ方式に対応する必要がある。

3.2 DSRC-SPF

DSRC-SPFの機能を**図2**に示す。DSRC-SPFを使用する際には，まずDSRC-SPFに割り当てられたローカルポートを利用して，ネゴシエーションと呼ばれる複数のセキュリティ方式の中から使用するセキュリティ方式を選択する処理が行われる。その後，選択したセキュリティ方式が定める手順で相互認証が行われ，認証完了後に各基本アプリケーションのプロトコルデータユニットの暗号化／復号やMAC生成／検証が行われる。

なお認証完了後にセキュアポートを利用するかどうかはローカルポートプロトコルのトランザクションごとに選択可能である。

3.3 各基本アプリケーションでのアクセス制御

車載器メモリアクセスアプリケーションにおけるアクセス制御を**図3**に示す。車載器メモリアクセスアプリケーションで扱われるメモリ領域は，個別のレコードごとにアクセス制御についての属性が設定されている。ノンセキュアポートから通常のレコードはアクセスできるが，DSRC-SPFの認証が必要なレコードに対してはアクセスできない。逆にセキュアポートを利用すれば，どちらのレコードもアクセス可能である。

車載器ID通信アプリケーションは，車載器メモリアクセスアプリケーションと同様にIDごとにアクセス制御についての属性が設定されており，DSRC-SPFの認証を必要とするIDについては，セキュアポートからのアクセスのみが許可される。

ICカードアクセスアプリケーションは，クレジット決済での利用を想定しているため，ノンセキュアポートからのアクセスは許可されない。つまりICカードアクセスアプリケーションを利用するためにはDSRC-SPFの利用が前提となる。

表1．各種サービスとアプリケーションの対応例

サービス ＼ アプリケーション	駐車場自動入退場		ガソリンスタンド自動決済	情報提供
	例1	例2		
車載器指示応答		○		
車載器メモリアクセス				○
ICカードアクセス		○		
プッシュ型情報配信				○
車載器ID通信	○		○	
車載器基本指示	○		○	

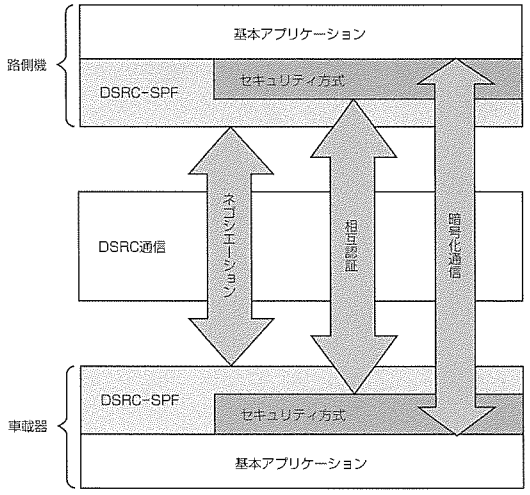


図2．DSRC-SPFの機能

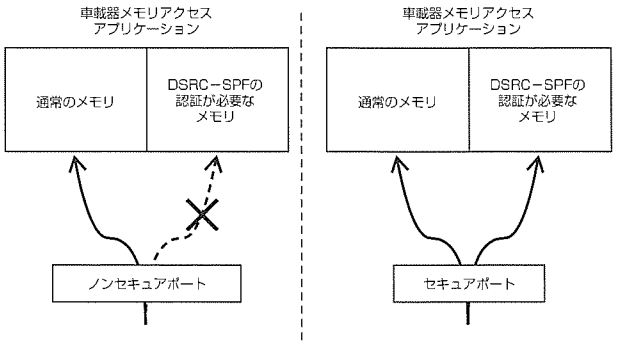


図3．車載器メモリアクセスにおけるアクセス制御

プッシュ型情報配信アプリケーションは，セキュアポートとノンセキュアポートとで異なるタイプのコンテンツを受信できるような設定が可能である。

車載器指示応答アプリケーション，車載器基本指示アプリケーションについては，DSRC-SPFの有無にかかわらず，すべての機能が使用可能である。

これまで述べた通りDSRC-SPFを利用した通信は，①セキュリティの交渉→②相互認証→③暗号化通信の順で行われるが，DSRCの通信ゾーンは20～30m程度と非常に短い距離であり，時速100km/hで走行した場合，１秒程度で通過してしまう。車載器は，その間にネゴシエーションと相互認証を行い，サービスによっては大量のデータを暗号化又は復号しなければならない。一方，路側機では，同時に複数の車載器と接続する可能性があり，その場合には車載器と同等の処理を並列に行わなければならない。この処理を実現するためには，下位レイヤでの効率的な送受信処理はもちろんのこと，高速な暗号処理が必要である。

4. むすび

ITSにおいて中核システムになるとされるDSRCシステムと，そこで使用されるセキュリティ技術であるDSRC-SPFについて述べた。DSRCシステムは次世代の道路システムで，特に安全・安心への貢献が期待されるシステムの一つである。これまで車載器－路側機間のセキュリティとしてDSRC-SPFの検討を行ってきたが，今後は，システム面，運用面からの検討を行い，DSRCシステムの普及を促進する。

参考文献

(1) ARIB STD-T75 狭域通信(DSRC)システム標準規格，(社)電波産業会

(2) ARIB STD-T88狭域通信(DSRC)アプリケーションサブレイヤ標準規格，(社)電波産業会

(3) ITS FORUM RC-004 狭域通信(DSRC)基本アプリケーションインタフェース仕様ガイドライン，ITS情報通信システム推進会議

三菱デジタルCCTVシステム“MELOOKμ”の映像情報セキュリティ

山口晃由*
上田智弘**

Information Security for Mitsubishi Digital CCTV System “MELOOKμ”

Teruyoshi Yamaguchi, Tomohiro Ueda

要　旨

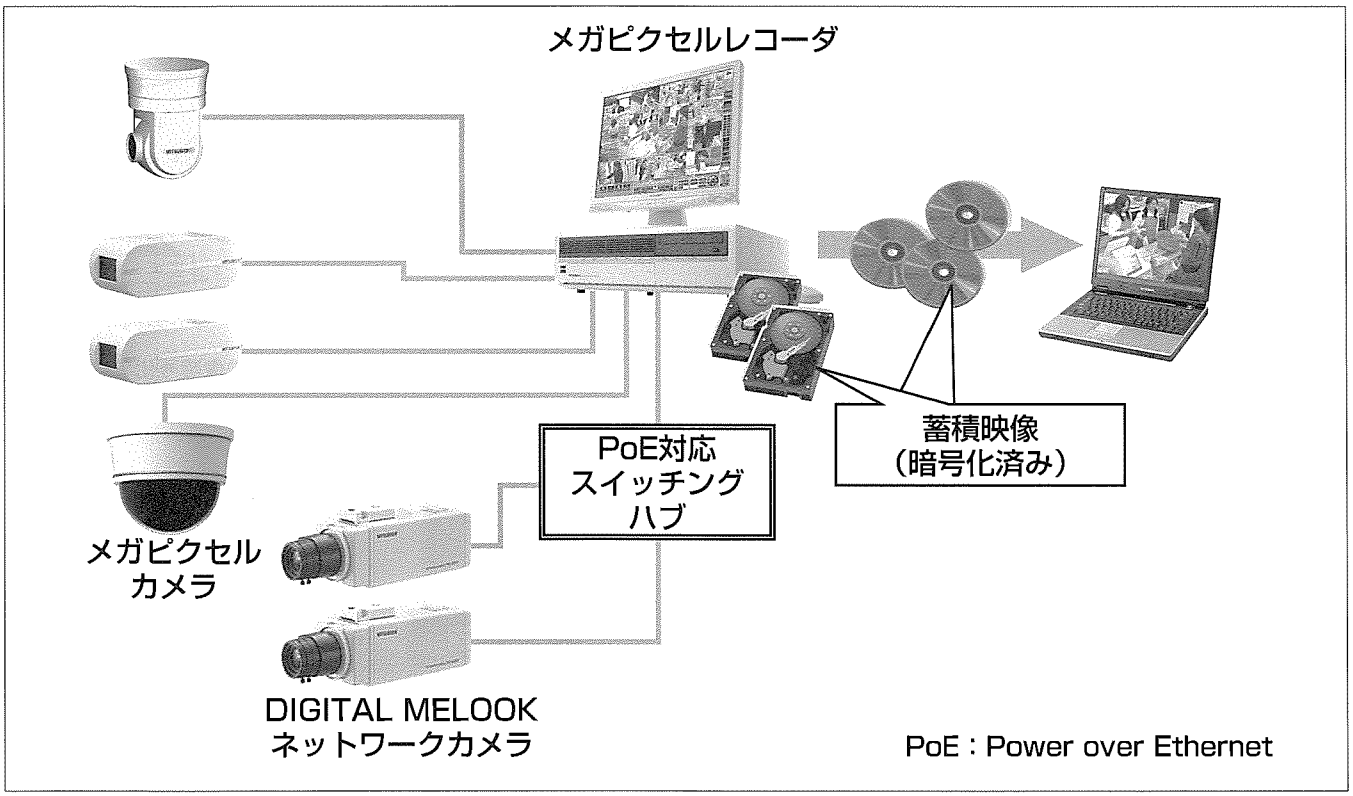
近年の犯罪件数の増加と，犯罪検挙率の低下を背景に，監視カメラを用いた映像監視システムを導入する施設が増加している。その中でもデジタルCCTV(Closed Circuit Television)は，ビル・パーラーなど大規模店舗を中心に導入が進んできたが，今後，コンビニエンスストアなどの小規模店舗への導入が進むと予想される。

コンビニエンスストアなどの小規模店舗向けの映像監視システムには，高精細画像によるリアルタイム監視を，導入しやすい価格で実現することが求められている。

一方で，無制限な監視カメラの設置はプライバシーを侵害するという声も少なからずある。映像監視への理解を得るためには，映像情報を適切に扱うことが重要である。特に，通信路の盗聴や，映像を蓄積したストレージの盗難といった不正行為から，映像情報を確実に保護することが求められる。

三菱電機では，中小規模店舗向けの映像監視システムとして“MELOOKμ(メルックミュー)シリーズ”を開発した。MELOOKμは，メガピクセル映像のリアルタイム監視・記録をアナログシステム並みの低価格で実現した。これによって，店舗出入口やATMコーナーにおける人物の人相・服装にとどまらず，これまで困難であった店舗のレジにおける紙幣の種別や商品ラベルも識別可能となる。また，世界最高水準の暗号技術によって，映像データを暗号化してレコーダに記録でき，第三者による内蔵ハードディスクやコピーメディアなどへの不正アクセスなど，情報漏えいのリスクを軽減できる。

本稿では，MELOOKμにおけるセキュリティ技術に焦点をあてて述べる。



三菱デジタルCCTVシステム“MELOOKμ”

三菱デジタルCCTVシステムMELOOKμは，メガピクセルカメラとメガピクセルレコーダとで構成される。メガピクセルカメラで取得した高精細画像を，メガピクセルレコーダで蓄積・表示する。また，メガピクセルレコーダには，従来の“DIGITAL MELOOKシリーズ”のネットワークカメラも接続可能である。蓄積された映像は当社独自の暗号技術“MISTYファミリーBROUILLARD(ブルイヤール)”で暗号化され，蓄積画像のセキュリティを確保する。

*情報技術総合研究所(工博)　**コミュニケーション・ネットワーク製作所

1. まえがき

映像監視システムは，監視カメラによって監視及び映像の蓄積を行い，犯罪行為の抑止や証拠収集を行うシステムである。近年の犯罪件数の増加や，犯罪検挙率の低下などの社会背景を受け，防犯を目的として映像監視システムを導入する施設が増加している。その市場は，今後ますます増加する傾向にある。その中でもデジタルCCTVは，駅舎やビル・パーラーなどの中大規模施設を中心に普及してきたが，コンビニエンスストアや金融機関店舗等の中小規模施設への導入が進むと予想される。これらの施設では，高精細画像による映像監視を優れたコストパフォーマンスで導入できることが求められる。

一方で，無制限な監視カメラの設置がプライバシーを侵害するおそれもある。映像監視システムの設置に際しては，監視映像の安全かつ適切な管理が求められる。

当社では，映像監視システムの容易な導入と，簡便な映像情報管理を実現するデジタルCCTVシステムMELOOKμを開発した。MELOOKμは，優れたコストパフォーマンスでメガピクセルの高精細画像を記録・表示するだけでなく，当社の暗号技術MISTYによって，ハードディスクやDVD(Digital Versatile Disk)媒体等にコピーした映像を不正な盗聴から保護する。

本稿では，MELOOKμのセキュリティ機能を中心に述べる。

2. 三菱デジタルCCTVシステムMELOOKμ

2.1 MELOOKμの構成

デジタルCCTVシステムMELOOKμは，最大8台のメガピクセルカメラと，最大8台のDIGITAL MELOOKシリーズネットワークカメラをメガピクセルレコーダに接続し，映像の収集・蓄積・表示を行う。メガピクセルカメラはメガピクセルレコーダと直接接続する。DIGITAL MELOOKシリーズネットワークカメラはスイッチングハブを経由してメガピクセルレコーダと接続する。レコーダに記録された映像は，必要に応じてDVDにコピーできる(図1)。

2.2 MELOOKμのセキュリティ機能

MELOOKμでは，蓄積データ保護のために，取得した映像をリアルタイムで暗号化して蓄積する。表示の際は暗号化映像をリアルタイム復号して表示する。DVD等へのコピーは暗号化したままコピーする。蓄積の段階で映像が暗号化されているため，ファイルビューアによる直接閲覧等，正規の方法以外では映像を閲覧できない。よって，DVDやHDD(Hard Disk Drive)等が盗難にあっても，映像情報を保護できる(図2)。

また，メガピクセルレコーダは，ユーザー認証によるアクセス制御を行う。アクセス制御によって，ユーザーの操作を制限する。DVDデータへのアクセスは，DVDコピー時に同封される専用の再生ソフトウェアで行う。DVD再生時にもユーザー認証を行う。

さらに，メガピクセルレコーダは，接続されるハードディスクを認証し，その成否によってアクセス制限を設けている。これによって，不正利用者が，あるメガピクセルレコーダで蓄積された映像を，ハードディスクごと他のメガピクセルレコーダへ接続しても，蓄積データへのアクセスを制限できる(図3)。

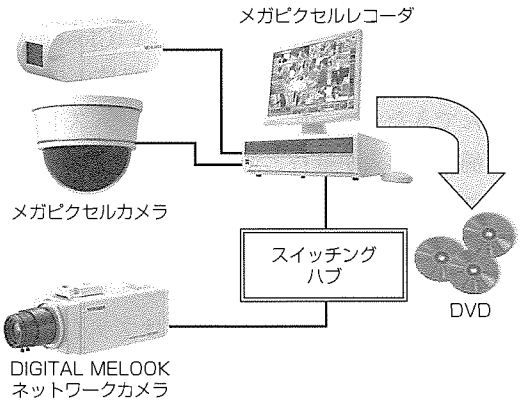


図1．三菱デジタルCCTVシステムMELOOKμ

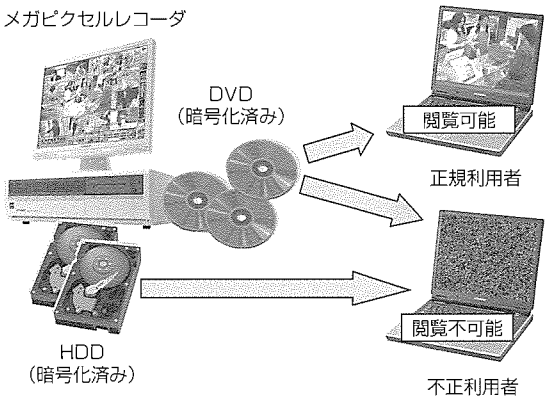


図2．MELOOKμにおける映像暗号化

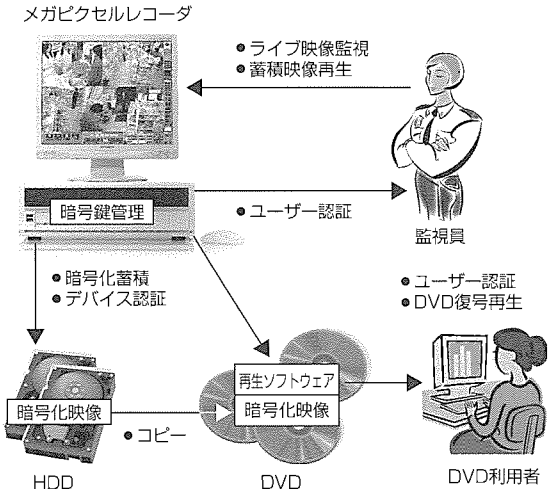


図3．MELOOKμのセキュリティ機能

3. MELOOKμにおけるセキュリティ技術

3.1 暗号化蓄積

デジタルCCTVシステムでは，カメラから取得される大量の映像を高速に蓄積し，表示しなければならない。MELOOKμでは，メガピクセル(Super eXtended Video Graphics Array：SXVGA)画質の映像に対し，蓄積時に映像暗号化処理を，表示時に映像復号処理を行う。これに伴って，暗号化・復号処理の高速化が要求される。

MELOOKμの場合，最大で80Mbps(注1)の暗号処理性能が要求される。一方で，暗号処理以外の処理も行う必要があるため，暗号処理にかけられる負荷をできるだけ抑える必要がある。一般にこれらの要求を満たすためには，専用ハードウェアを用いる必要がある。

当社では，ソフトウェアによる暗号処理でハードウェア並みの性能を実現し，装置のコスト低減を図るために，MISTYファミリーとして，ソフトウェアでの高速処理能力と，十分な安全性を両立させた新しい暗号アルゴリズムBROUILLARDを開発した。

BROUILLARDは，大きなメモリ空間のランダムアクセスによって高速性と安全性を実現している。BROUILLARDはPentium 4(注2)(3 GHz)での実装で，8 Gbpsの暗号化速度を実現することができる。

MELOOKμでは，BROUILLARDの適用によって，80Mbpsの暗号処理をソフトウェアで実現している。

3.2 暗号鍵(かぎ)管理

メガピクセルレコーダは，映像を暗号化してストレージに保存する。そのため，暗号化に用いる鍵情報は厳重に管理されなければならない。同時に，正規の利用者には使いやすい鍵情報を提供する。

メガピクセルレコーダは，初回起動時に映像暗号鍵を生成する。映像暗号鍵の生成はランダムに行われるため，異なるレコーダで同じ映像暗号鍵を持つ可能性は非常に小さい。そのため，あるレコーダで暗号化された映像は，基本的に当該レコーダ以外では開くことはできないメカニズムを採用している(注3)。このように生成した映像暗号鍵を，複数のパラメータで暗号化して，複数の不揮発領域に格納している。不揮発領域に格納された映像暗号鍵はすべて暗号化されているので，不揮発領域からの不正なデータ抜き取りに対して安全である。

メガピクセルレコーダの通常起動時は，システム領域から，暗号化された映像暗号鍵を取得・復号する。展開された映像暗号鍵を用いて，実際の映像を暗号化する。

データ領域にコピーされた暗号化された映像暗号鍵は，後述するデバイス認証で用いる。

DVDコピー時は暗号化された映像暗号鍵，暗号化映像，再生ソフトウェアをコピーする。DVD再生時は，再生ソフトウェアを起動し，パスワードを入力する。入力されたパスワードが正しければ，当該映像暗号鍵を復号し，暗号化映像の復号・再生を行う。パスワードが不正であれば映像暗号鍵を復号することはできないので，暗号化映像の再生は不可能である(**図4**)。

3.3 ユーザー認証

メガピクセルレコーダは，利用者が入力したパスワードを認証することで，必要なアクセス制御を行う。

表1に利用者のレベルと各レベルで許可される操作を示す。店員レベルは，ライブ映像監視のみを行うことができる。店長レベルは，ライブ映像監視のほかに，蓄積映像の再生とカメラ操作を行うことができる。オーナーレベルは，最高権限を持っており，各種設定変更やDVDコピーを行うことができる。店員レベルでの操作には，パスワード認証を必要としないが，店長レベルとオーナーレベルでの操作には，パスワード認証を必要とする。

DVD再生のためのパスワードは，DVDコピー時に設定する。DVD再生時は，設定したパスワードを入力することで映像を再生できる。

店長レベル及びオーナーレベルのパスワードは，各レベルで認証後に変更することができる。

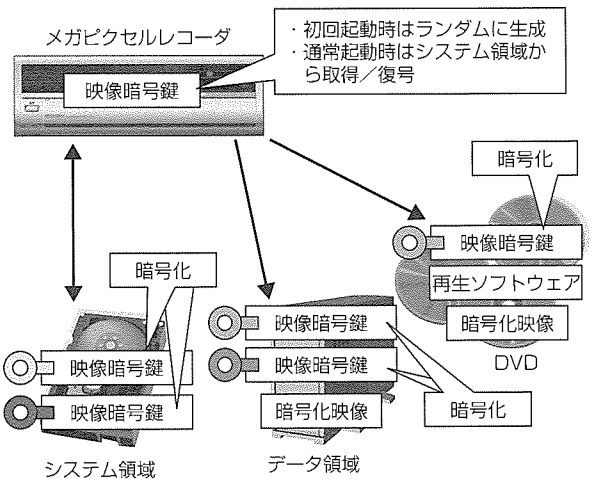


図4．MELOOKμの暗号鍵管理

表1．利用者の権限と許可される操作

利用者権限	許可される操作	パスワード認証
Lv.1（店員レベル）	・ライブ映像監視	不要
Lv.2（店長レベル）	・Lv.1で許可される全操作 ・蓄積映像再生 ・カメラ制御	必要
Lv.3（オーナー レベル）	・Lv.2で許可される全操作 ・各種設定変更 ・DVDコピー等	必要

(注1) 暗号化と復号の両方を含む。
(注2) Pentiumは，Intel Corp. の登録商標である。
(注3) 例外的に，後述するデバイス認証を行うことで，他のレコーダでも開くことができる。

3.4 デバイス認証

MELOOKμでは，増設ユニットによるHDDの増設を行うことができる。増設ユニットは，取り付け・移設が容易となる反面，移設先でのアクセス権の管理が課題となる。増設HDDを移設した場合，正規利用者は移設先で参照できるが，不正利用者には参照させてはならない。

メガピクセルレコーダは，接続されているHDDが，当該レコーダ本体で設定したものか，他のレコーダで設定されて移設されたものなのかを認証する。レコーダ本体が設定したものであれば，通常利用と同様に用い，そうでなければ，正規利用者判定のためのパスワード認証を行う(注4)。増設HDDには，暗号化された移設元の映像暗号鍵が格納されている。移設先のレコーダは，入力されたパスワードを検証した後，HDDに格納された移設元映像暗号鍵を復号してRAM(Random Access Memory)領域に展開する(図5)。

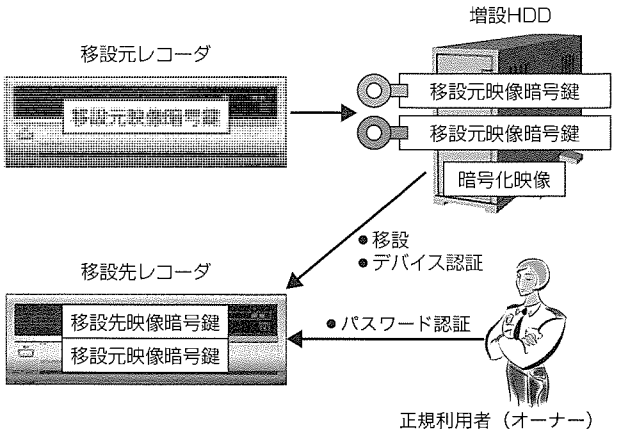


図5．MELOOKμにおける増設HDDの移設

4. むすび

三菱デジタルCCTVシステムMELOOKμに搭載されているセキュリティ機能について述べた。MELOOKμでは，映像のリアルタイム暗号化蓄積，暗号鍵管理，ユーザー認証，デバイス認証などの技術を組み合わせて，個人情報である映像情報を不正行為から保護し，適切に管理する。

今後，MELOOKμはWeb配信機能やバックアップHDD増設機能などを搭載する予定である。Web配信機能では，セキュアな映像暗号鍵配送やセキュアな遠隔ユーザー認証を，バックアップHDD増設機能では，安全かつ柔軟なデバイス認証を実現する予定である。

(注4) このパスワード認証機能は対応予定，増設HDDの設定によってはパスワード認証しないこともある。

参考文献

(1) 三菱デジタルCCTVシステム“MELOOKμ(メルックミュー)”発売，三菱電機広報発表資料，通信No.0709，(2007-11-06)

(2) 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン，経済産業省（2004-10）

(3) 機器組み込み用高性能暗号アルゴリズム“BRUME”と“BROUILLARD”を開発，三菱電機広報発表資料，開発No.0517（2005-9-12）

セキュア携帯電話システム

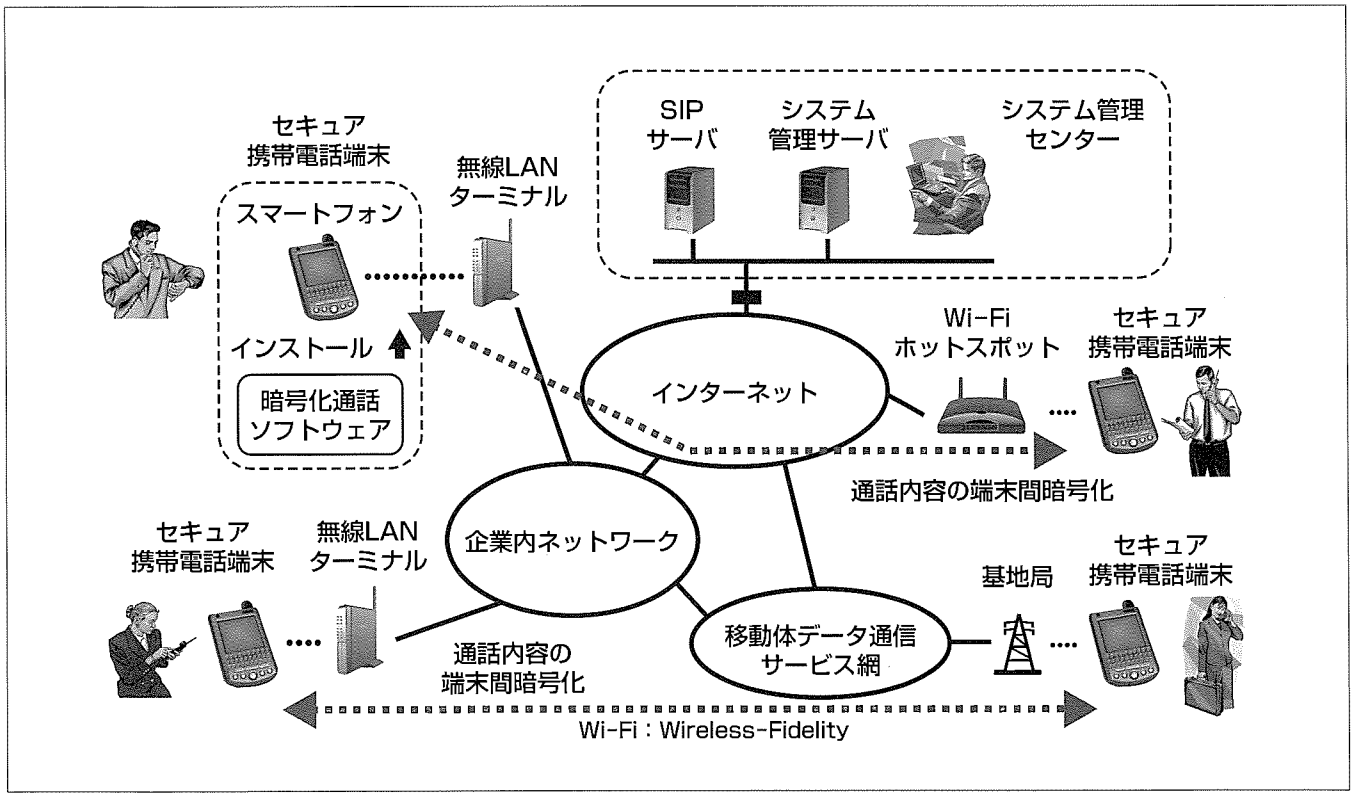
辻　宏郷*
米田　健**

Secure Mobile Phone System

Hirosato Tsuji, Takeshi Yoneda

要　旨

モバイル通信端末の高性能化・高機能化や無線通信サービスの帯域拡大に伴い，端末間で音声・テキスト・静止画・動画等をリアルタイムで通信することが可能になった。機密性の高い業務に利用する場合，端末間の通信内容の盗聴防止は必要不可欠である。携帯電話と基地局，携帯情報端末と無線LAN(Local Area Network)アクセスポイント等の無線通信区間には，暗号化による盗聴防止対策が施されているが，その先のネットワークやインターネット上での通信は保護されていないため，確実な盗聴防止には，端末と端末の間でEnd-to-Endの暗号化を行う必要があり，端末同士で暗号鍵(かぎ)を共有する技術が不可欠である。また，端末を紛失した場合に備えて，端末内情報の漏洩(ろうえい)や成りすましによる不正利用等の脅威に対する対策が必要である。モバイル通信端末間通信用の暗号鍵の共有方式として，システム管理サーバで暗号鍵を一括生成し，各端末に事前配布することによって通信開始時の鍵共有処理を不要とする鍵配布・共有プロトコルを設計した。また，端末紛失・盗難時に端末の不正利用防止や端末内機密情報の保護を実現する端末管理プロトコルを開発した。これらの暗号鍵・端末の管理方式の応用例として，モバイル通信端末の音声通話を端末間のEnd-to-Endで暗号化することによって通話内容の盗聴防止を実現したセキュア携帯電話システムを設計・試作した。セキュア携帯電話端末間で暗号化通話が可能であること，通話内容の暗号化処理に伴うオーバーヘッドは無視できる範囲内であること，パケット伝達遅延や消失の少ないネットワーク状況で違和感なく通話できることを確認した。



セキュア携帯電話システム

セキュア携帯電話システムは，モバイル通信端末間でEnd-to-Endの暗号化を行うことによって，通話内容の盗聴を防止するシステムである。暗号化に用いる鍵は，システム管理サーバで一括生成し，各々の端末に事前配布することで，暗号化通話開始時，端末間の鍵共有処理を不要とする。端末紛失・盗難発生時に，システム管理サーバからの遠隔操作によって，端末の不正利用防止や端末内のプログラム・暗号アルゴリズム・データ等の機密情報を消去する機能を提供する。スマートフォンに暗号化通話ソフトウェアをインストールしてセキュア携帯電話端末とする。

*情報技術総合研究所　**同研究所(工博)

1. まえがき

モバイル通信端末の高性能化・高機能化や無線通信サービスの帯域拡大に伴い，端末間で音声・テキスト・静止画・動画等をリアルタイムで通信することが可能になった。機密性の高い業務に利用する場合，端末間の通信内容の盗聴防止は必要不可欠である。一般に，携帯電話と基地局，携帯情報端末と無線LANアクセスポイント等の無線通信区間には，暗号化による盗聴防止対策が施されているが，その先のネットワークやインターネット上での通信は保護されていないため，確実な盗聴防止には，端末と端末の間でEnd-to-Endの暗号化を行う必要があり，このためには端末同士で暗号鍵を共有する技術が不可欠である。また，端末を紛失した場合に備えて，端末内情報の漏洩や成りすましによる不正利用等の脅威に対する対策が必要である。

本稿では，モバイル通信端末間暗号化通信用の鍵の共有及び端末紛失・盗難時の対策を両立させた暗号鍵・端末管理技術について述べる。また，これらの技術を用いて端末間の通話内容の盗聴防止を実現したセキュア携帯電話システムの設計と試作について述べる。

2. 暗号鍵と端末の管理方式

2.1 暗号鍵の配布・共有方式

モバイル通信端末間のリアルタイム通信をEnd-to-Endで暗号化するための暗号鍵の配布・共有方式としては，次に示す方法が考えられる。

(1) 事前共有

端末間の通信手順を実行する前に，何らかの手段を用いて暗号鍵を事前共有しておく方式である。例えば，あらかじめ端末配布時に必要な鍵をすべて埋め込んでおく方法があるが，同じ鍵や限られた鍵集合を使い続けるので，安全性に問題がある。

(2) 端末間の鍵共有アルゴリズムを用いた共有

Diffie-Hellman鍵共有アルゴリズムやRSA(注1)鍵配送アルゴリズム等の公開鍵暗号アルゴリズムを用いる方式である。公開鍵の正当性を証明するために，CA(Certification Authority)の発行する公開鍵証明書を導入する必要がある。また，通信開始前の鍵共有処理に時間を要する場合がある。

(3) システム管理サーバを用いた鍵の配布・共有

システム管理サーバによって集中的に暗号鍵を生成し，各々の端末に配布する方式である。本稿で述べる暗号鍵の管理技術では，この方式を採用している。

2.2 システム管理サーバを用いた鍵の配布・共有方式

暗号鍵の配布・共有方式として，システム管理サーバを用いた鍵配布・共有プロトコルを設計した。この方式は，次に示す特長を持っている。

(1) 鍵配布・共有時の暗号化や改ざん検出を含む暗号処理に共通鍵暗号アルゴリズムのみを使用しており，モバイル通信端末で公開鍵暗号アルゴリズムや公開鍵証明書の検証処理を実装する必要がない。

(2) システム管理サーバで暗号鍵を一括生成する。

(3) システム管理サーバで生成した暗号鍵を事前配布することによって，通信開始時の鍵共有処理を不要とし，即時暗号化通信を可能とする。

(4) モバイル通信端末の紛失・盗難が発生した場合，システム管理サーバから鍵の無効化を指示する命令を発行することによって，該当端末を用いた盗聴や成りすまし通信を防止する。

次に，具体的な鍵配布・共有手順を示す。

2.2.1 デバイス鍵の事前共有

あらかじめ，システム管理サーバで，モバイル通信端末ごとに異なるデバイス鍵を生成し，各々の端末に事前配布する(図1)。この結果，システム管理サーバと各々の端末は，それぞれのデバイス鍵を共有し，デバイス鍵を用いた暗号化や改ざん検出用認証値の演算を行うことで，システム管理サーバ・端末間の通信をセキュアに行うことができる。すなわち，システム管理サーバと各端末の間で，安全な通信路が確保されている。

2.2.2 マスター鍵の一括生成と配布

運用期間中，システム管理サーバは各々の端末間で暗号化通信に必要となるすべての暗号鍵(マスター鍵)を生成し，その鍵を利用する端末のみが復号可能となるように暗号化する。例えば，AliceとBobが暗号化通信するためのマスター鍵を生成し，AliceとBobの端末のデバイス鍵でのみ復号可能となるように暗号化する。暗号化したマスター鍵は，システム管理サーバから各端末への制御コマンドを送信するための通信路を通して，各々の端末に配布する(図2)。マスター鍵は，定期的に(例えば24時間ごとに)更新するとともに，端末に届かなかった場合に備えて，同じ鍵を繰り返し再送する。

2.2.3 セッション鍵の生成

システム管理サーバによるマスター鍵の配布によって，

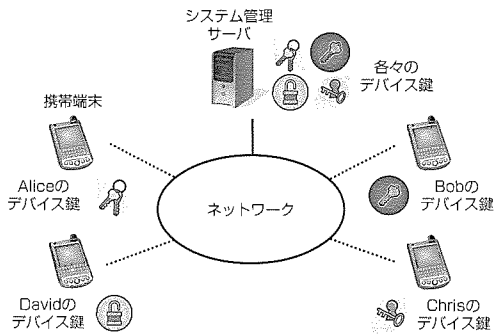


図1．デバイス鍵の事前共有

(注1) RSA：Rivest, Shamir, Adlemanによって開発された公開鍵暗号アルゴリズム

暗号化通信開始時，各々の端末は，マスター鍵を事前共有している。各々の端末は，マスター鍵を直接暗号化に利用する代わりに，マスター鍵から計算して求められるセッション鍵を生成し，通信内容を暗号化する。セッション鍵は，一定回数の暗号化に使用するごとに，再生成する。

2.2.4　マスター鍵の転送

マスター鍵は，システム管理サーバで一括生成・配布し，各々の端末では生成しない。通信相手端末にシステム管理サーバから配布されるマスター鍵が届かなかった場合に備えて，各端末はシステム管理サーバから受信した配布形式のマスター鍵(利用端末向け暗号化及び改ざん検出用認証値付き)を，そのまま端末内部に保管する。通信開始時，相手端末との間でマスター鍵の共有状態でない場合，保管していた端末から相手端末へ，配布形式のマスター鍵を転送する。転送されたマスター鍵を受け取った端末は，その正当性を確認した上で利用する。

2.3　端末紛失・盗難時の対策

モバイル通信端末の紛失・盗難によって，端末内に格納したプログラム(暗号アルゴリズムを含む)や機密情報の漏洩や端末の不正利用が行われる可能性がある。例えば，最近の携帯電話の場合は，携帯電話通信事業者が遠隔ロック機能を提供しているが，端末の種類や通信事業者の提供サービスに依存せずに端末紛失・盗難時のセキュリティ対策を実現する端末管理プロトコルを設計した。

2.3.1　紛失端末の不正利用防止

端末の紛失・盗難などの“事件”が発生した場合，該当端末を入手した者が正規利用者に成りすまし，他の端末利用者と通信を試みる可能性がある。端末使用時の利用者認証(暗証番号，指紋等)に加えて，他の端末利用者に事件の発生を通知するとともに，該当端末と他の端末の間で通信を禁止する。例えば，端末紛失の連絡を受けた場合，システム管理サーバで端末無効化命令を生成し，各端末に緊急配布する。命令を受信した各端末は，通信禁止となった端末リストを保持するとともに，該当端末との間のマスター鍵を端末から消去する。命令の不達に備えて，システム管理サーバは命令を再送するとともに，端末間で命令を転送しあうことによって，通信禁止端末リストを更新する(図3)。

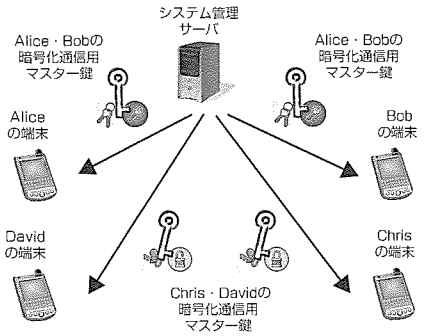


図2．マスター鍵の一括生成と配布

2.3.2　紛失した端末内の機密情報保護

端末の紛失・盗難発生時，状況によっては，端末の不正利用防止に加えて，端末内部に格納されたプログラム，暗号アルゴリズム，鍵等の機密情報の第三者による解析を防止する必要がある。例えば，端末盗難の連絡を受けた場合，システム管理サーバで端末初期化命令を生成し，各端末に緊急配布する。この命令は該当端末に直接送信するほか，全端末に送信して，他の端末経由で命令を転送する。これによって，該当端末内の機密情報を消去する(図4)。

2.3.3　紛失端末以外の端末の継続的利用可用性

端末の紛失・盗難発生時，該当端末を排除するための対策処理によって，それ以外の端末の利用に影響が出ないことが求められる。前節及び本節で述べた暗号鍵と端末の管理方式は，この要件を満たしている。

3.　セキュア携帯電話システム

3.1　セキュア携帯電話システムの設計

前章で述べた暗号鍵・端末の管理方式の応用例として，モバイル通信端末の音声通話を端末間のEnd-to-Endで暗号化することによって，通話内容の盗聴を防止するとともに，端末紛失・盗難時のセキュリティ対策を施したセキュア携帯電話システムを設計した。

3.1.1　暗号化通話内容の通信方式

セキュア携帯電話システムでは，通話内容(音声)を暗号化して，端末間でやり取りする。音声は，端末が持つ音声符号化機能によってデジタルデータに変換した後，共通鍵暗号アルゴリズムを用いて暗号化する。暗号化された音声

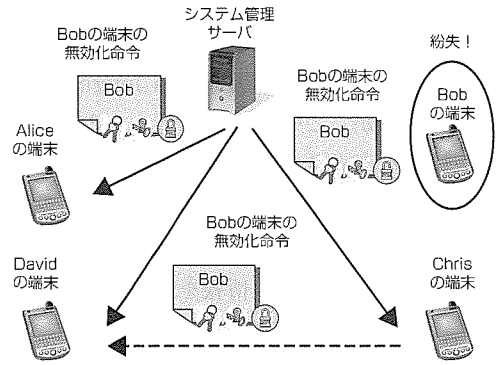


図3．端末無効化命令の生成と配布，転送

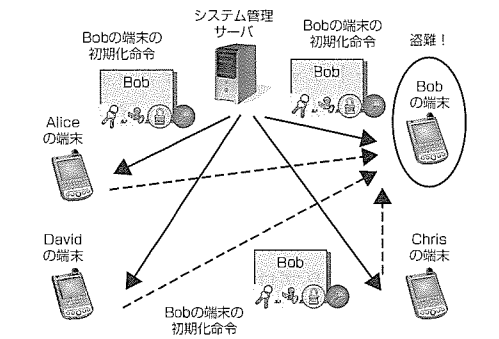


図4．端末初期化命令の生成と配布，転送

データを，端末の持つ通信機能を用いて，移動体データ通信事業者やインターネット接続事業者の提供するデータ通信サービスを通して交換することによって，暗号化通話を実現する。

3.1.2 セキュア携帯電話端末の実現方式

セキュア携帯電話端末の実現方式としては，

(1) 専用端末(ハードウェア)を開発する。

(2) 既存のモバイル通信端末にアドオンで使用する付加装置(ハードウェア)を開発するとともに付加装置を用いて暗号化通話を実現するためのドライバ(ソフトウェア)を開発する。

(3) 既存のモバイル通信端末を用いて暗号化通話を実現するアプリケーション(ソフトウェア)を開発してインストールする。

の3種類の方法が考えられる。各方法は，安全性とコストの面で一長一短であるが，今回は第3の方法を選択した。ただし，現時点では，暗号化通話を実現するネイティブソフトウェアをインストール可能なモバイル通信端末は限られているため，Microsoft(注2) Windows Mobile(注2)をベースとするスマートフォンを利用し，これらの端末に暗号化通話ソフトウェアをインストールすることでセキュア携帯電話端末とする。

3.1.3 通信プロトコル

セキュア携帯電話システムにおける暗号化通話の基本的な仕組みは，暗号化を施したVoIP(Voice over Internet Protocol)であり，業界標準プロトコルであるSIP(Session Initiation Protocol)，RTP(Real-Time Transport Protocol)，SRTP(Secure Real-time Transport Protocol)[2]を採用する。SRTPで暗号化に用いる鍵を共有する手段の候補の一つとして，MIKEY(Multimedia Internet KEYing)[1]が規定されているが，このシステムでは，**2章**で述べた鍵管理と端末管理を両立させたプロトコルを採用する。また，端末間で共有済みの鍵が存在しない場合のネゴシエーションや鍵の転送を行うため，SDP(Session Description Protocol)を拡張して，これらの情報をSIPメッセージとともに交換する。

3.1.4 システム構成

扉ページの図は，セキュア携帯電話システムの典型的な構成例を示した図である。暗号化通話ソフトウェアをインストールしたスマートフォンを，セキュア携帯電話端末とする。企業内インターネット，インターネット接続事業者や移動体データ通信事業者の提供するデータ通信サービス網を端末間通信路として用いる。また，システム管理センターを設置し，SIPサーバ(セッション管理に用いるSIPアドレスの登録機能やSIPプロトコルの中継機能を提供)，

(注2) Microsoft, Windows Mobileは，米国Microsoft Corp. 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。

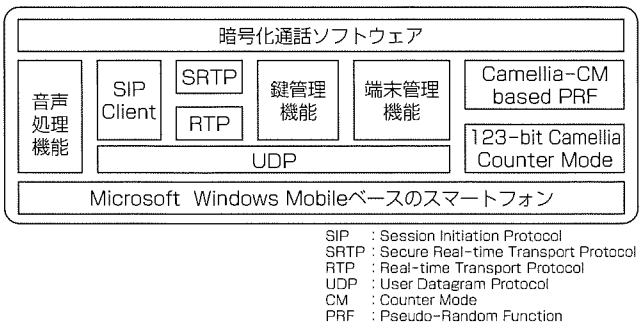


図5．セキュア携帯電話端末のアーキテクチャ

システム管理サーバ(暗号化通話に用いる初期鍵の一括生成と配布，端末紛失・盗難発生時の鍵の無効化処理，端末を管理して紛失・盗難発生時に遠隔操作で端末を無効化する等の処理を実施)を設置する。

3.2 セキュア携帯電話システムの試作

前節で述べた設計方針に従って，セキュア携帯電話システムのプロトタイプを開発した。試作したセキュア携帯電話端末のアーキテクチャを，**図5**に示す。暗号化VoIP，鍵管理，端末管理に必要な各プロトコルを実装した。また，SRTPにおける共通鍵暗号アルゴリズムとして，標準で規定されたアルゴリズムの代わりに，NTTと当社が共同開発し，電子政府調達暗号等に採用された"Camellia[3]"を実装した。

無線LAN(IEEE 802.11b/g)及び移動体データ通信サービスに対応したセキュア携帯電話端末を用いて暗号化通話を行った。通話内容の暗号化処理に伴うオーバーヘッドは無視できる範囲内であること，暗号化した音声のデータ通信パケットの伝達遅延や消失の少ないネットワーク状況で違和感なく通話できることを確認した。今後も評価実験及び改良を継続する計画である。

4. むすび

モバイル通信端末間でリアルタイム通信を行う際，盗聴を防止するための端末間暗号化通信用の鍵の共有及び端末紛失・盗難時の対策を両立させた鍵・端末管理技術を開発した。これらの技術を用いて，モバイル通信端末間の通話内容の盗聴防止を実現したセキュア携帯電話システムを設計し，試作システムを開発して暗号化通話が可能であることを確認した。

参考文献

(1) RFC 3830, MIKEY：Multimedia Internet KEYing (2004)

(2) RFC 3711, The Secure Real－time Transport Protocol(SRTP) (2004)

(3) RFC 3713, A Description of the Camellia Encryption Algorithm (2004)

Javaによる状況依存アクセス制御技術

松田　規*
米田　健**

Context-dependent Access Control for Java

Nori Matsuda, Takeshi Yoneda

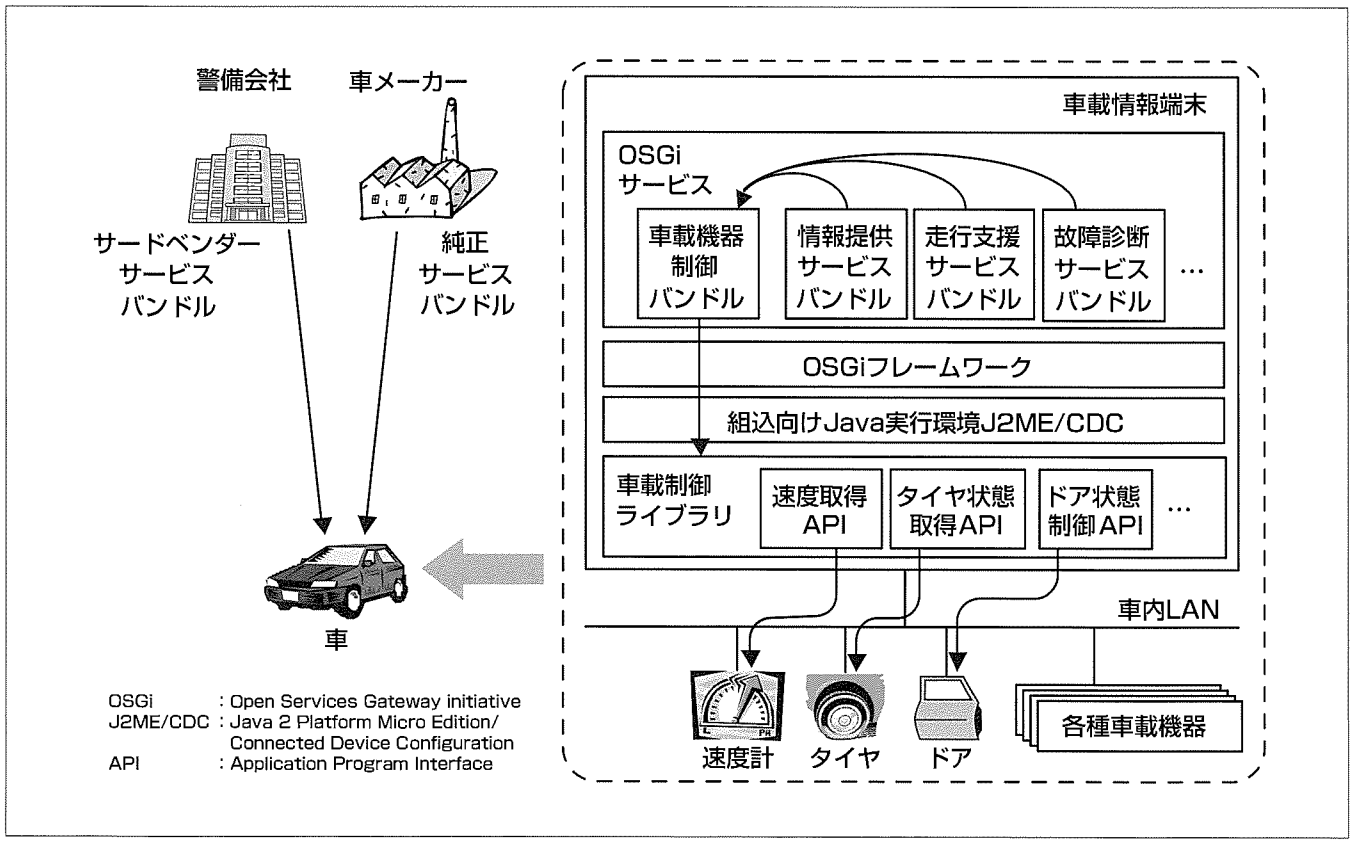
要　旨

近年，プローブカーやリモート制御などのテレマティクスサービスが研究されている。その実現には，インターネットと車内LAN(Local Area Network)を接続する車載情報端末が必要となる。車載情報端末には，ソフトウェア開発の効率化と多様化するサービスへの対応のため，Java(注1)実行環境を搭載し，Javaアプリケーションを追加する仕組みが求められている。また，エンジン制御等の制御機能やナビ操作機能も動作するため，Javaアプリケーションによって安全運転が脅かされないように不正な処理を遮断する必要がある。

しかし，Javaアクセス制御機能では，状況に応じたアクセス制御ができないという問題点がある。例えば，テレマティクスセンターが提供する情報を画面表示するプログラムが，運転中に頻繁に詳細情報を表示することはドライバーの注意力が散漫になるため好ましくないが，車の走行状態を考慮して画面表示をアクセス制御することはできない。

そこで本稿では，セキュアな車載Java実行環境を実現するため，Javaで状況依存アクセス制御を実現するための方式について述べる。この方式では，アクセス権限が有効となる状況条件が指定できるようにアクセス制御ポリシーを拡張した。権限認証時には，状況条件を検証してアクセス権限の有効性も判定することによって，状況依存アクセス制御を実現した。また，従来のJavaアクセス制御の動作に影響は与えず，更にJavaソースコードの改修が不要という特長を持つ。

（注1）　Javaは，Sun Microsystems, Inc. の登録商標である。



車載情報端末へのソフトウェアダウンロードとその内部構成

車メーカーの純正サービスだけでなく，警備会社などのサードベンダーが提供するサービスを実現するプログラムは，OSGi仕様に基づくバンドルとして車載情報端末にダウンロードされる。車載情報端末では，各種車載機器を制御するための車載制御ライブラリをJavaから利用できるようにするための車載機器制御バンドルが提供され，ダウンロードしたバンドルから車載機器の制御が可能となる。

*情報技術総合研究所　**同研究所(工博)

1. まえがき

Java実行環境J2ME/CDCでは，アプリケーションごとにアクセス権限を与え，リソースへのアクセスを制御することができる。さらに，ライブラリが独自のリソースへのアクセス権限を定義する仕組みも提供されている。しかし，J2ME/CDCのアクセス制御アルゴリズムでは，事前に付与されたアクセス権限に基づいたアクセス制御は可能だが，状況に応じたアクセス制御は行えないという問題点がある。例えば，テレマティクスセンターが提供する情報を画面表示するプログラムを考える。このプログラムが，運転中に頻繁に詳細情報を表示することは，ドライバーの注意力が散漫になるため好ましくない。このようなケースに対応するためには，速度計やドアロック等の車載機器の状況を考慮することが可能な，状況依存アクセス制御の実現が必要不可欠である。

そこで本稿では，J2ME/CDC上で状況依存アクセス制御を実現する方式の開発成果について述べる。具体的には，アクセス権限が有効となる状況条件が指定できるように拡張したアクセス制御ポリシー，及び状況条件を検証してアクセス権限の有効性も判定することで，状況依存アクセス制御を実現した仕組みについて述べる。

2．実用化に向けた技術課題

車載情報端末では，車の状況によって実行可能な操作が変化するという特徴がある。例えば，次のようなユースケースが考えられる。

(1) 情報提供サービス

センターからドライバーの嗜好(しこう)に応じた情報を提供するサービスである。走行中は情報の表示は禁止し，停車中のみ表示可能としたい。

(2) 走行支援サービス

運転挙動や車両状態を把握し，燃費効率向上のための改善提案を行うサービスである。各種車載機器の負荷上昇を防止するため，状態取得は一定間隔をおいたときのみ実施可能とし，また，CPU(Central Processing Unit)負荷が高いときはデータマイニングを禁止としたい。

しかし，J2ME/CDCでは，状況に依存したアクセス権限という考え方がないため，上記のような制限を課すことができない。そこで，エンジンやドアロック等，車載機器の状態を考慮可能な状況依存アクセス制御の実現が必要となる。

上記の例から，状況とは，ある時点での車の状態に加え，過去の処理時刻からの経過時間も考えられることが分かる。そこで，車載情報端末に搭載する状況依存アクセス制御方式では，次の2点の実現を目標とした。

①ある時点での状況に基づくアクセス制御

走行状態，ドアロック状態，走行位置等，ある時点の状況に依存した状況条件付きアクセス権限を実現

②過去の処理履歴を状況とみなしたアクセス制御

過去のアクセス権限行使回数又は間隔に依存するアクセス権限を実現

なお，例でも示したように，制御対象やサービス内容によって考慮すべき状況の内容だけでなく，状況数も異なる。また，プログラムは製品製造時にインストールされるだけでなく，製品出荷後に追加されるケースも考えられる。

そこで，次の点を満たすべき要件とした。

- アクセス権限ごとに複数の状況条件を設定可能
- 任意のタイミングで状況条件を追加可能
- 従来の状況非依存なアクセス権限も利用可能
- Java組み込みアクセス権限にも適用可能
- Java実行環境のソース改修が不要

次に，その実現方式について述べる。

3. 状況依存アクセス制御方式

3.1 状況条件の実現

状況に応じて有効となるアクセス権限を定義するため，**図1**に示す状況条件Conditionクラスを導入する。

状況条件とは，例えば①停車中，②CPU負荷10%以下，③過去に未実行等の条件を抽象化した概念である。抽象メソッドとして，状況条件を検証するcheckメソッドを宣言する。各状況条件は，依存する情報に応じて，Conditionクラスの実装クラスとして実現する。これによって，様々なバリエーションの状況条件を定義できる。

また，製品出荷後に新たな状況条件を追加できるように，状況条件の実装クラスを任意のタイミングで追加できる仕組みも実現した。具体的には，状況条件設定ファイルで状況条件名を宣言し，依存する状況に対応した実装クラス名を複数列挙する。また，実装クラスごとに1個のインスタンス化パラメータを指定する。状況依存アクセス制御アルゴリズムは，この設定ファイルを見て実装クラスを動的に読み込むため，設定変更だけで状況条件を追加可能である。また，複数の状況条件をグループ化可能となる。

図2の例では，状況条件名“stop”は，車が停車中かどうかを判断するための状況条件である。実装クラス名は速度を判断するSpeedometerConditionクラスで，インスタン

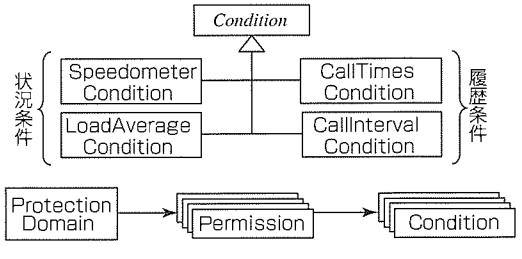


図1．状況条件のクラス構成

ス化パラメータとして速度0を与える。これによって，SpeedometerConditionクラスのCheckメソッドを呼んだ際に，速度が0かどうかの判断が行われる。次の例で示した状況条件名“interval50”は呼び出し間隔が50ms以上かどうかを判断する状況条件であり，動作の仕組みは状況条件“stop”と同様である。

3.2 状況条件とアクセス権限との関連付け

Java実行環境にロードされたすべてのクラスは，ロード元のファイルパス等や，Jarファイルにだれの署名が付加されているかを考慮して，Java実行環境が作成したProtectionDomainのいずれか一つに登録される。このProtectionDomainには，アクセス制御ポリシーに基づいてアクセス権限Permissionが割り当てられているため，クラスは登録されたProtectionDomainのアクセス権限を行使できるようになる。これが，Java実行環境がクラスに対してアクセス権限を与える仕組みである。

状況依存アクセス制御方式では，図1に示すように，このProtectionDomainに関連付けられた各アクセス権限に対して，複数の状況条件を関連付ける。そして，それらのすべての状況条件が成立しているときにのみ，そのアクセス権限が有効であると考える。これによって，状況依存アクセス制御の要(かなめ)である状況条件付きアクセス権限が定義できる。

3.3 アクセス制御ポリシーの拡張

前節では，ProtectionDomainに割り当てられたアクセス権限に対して状況条件を関連付けることを示した。このアクセス権限のProtectionDomainへの関連付けは，アクセス制御ポリシーによって指定されるため。Java実行環境が定義するアクセス制御ポリシーも，状況依存アクセス権限が指定できるように拡張する必要がある。具体的には，従来の付与アクセス権限に加えて，前述した状況条件名を指定できるように拡張する。状況条件名は複数の状況条件のグループ名であるため，アクセス権限に複数の状況条件を関連付けることになる。

はじめに，現在のJavaアクセス制御アルゴリズムでは，状況条件を指定できるアクセス権限が存在しないため，新たに状況条件付きアクセス権限を表すクラスConditionalPermissionを定義する。このクラスは，Java仕様で規定されたアクセス権限Permissionの派生クラスとして定義しており，2個のパラメータを取ることができる。このクラスは，第一引数としてアクセス権限，第二引数として状況条件名を指定する。

```
alias stop
  SpeedometerCondition, 0 ;

alias interval50
  CallIntervalCondition, 50 ;
```

図2．状況条件の設定ファイルの例

その例として，停車中にのみドアロック解除が可能なアクセス権限を与える場合の例を示す。図3のように，第一引数にドアロック解除権限と，そのアクセス権限クラスに与える引数2個，第二引数に停車中という状況条件を示す状況条件名“stop”を指定することによって，停車中にのみドアロック解除が可能なアクセス権限が指定できる。

3.4 状況依存アクセス制御アルゴリズム

前述したアクセス制御ポリシーの拡張によって，アクセス権限に対して状況条件を関連付けることができた。次に，アクセス制御アルゴリズムに対して，状況条件の検証とアクセス権限行使履歴の保存の2点を拡張する。

一般にJavaアプリケーションは，複数のベンダーが提供する複数のクラスによって構成される。そのため，利用されるクラスは異なるProtectionDomainに属し，付与アクセス権限もクラスごとに異なる可能性が高い。Javaアクセス制御が採用するドメインセキュリティモデルでは，このような構成に適するアクセス制御アルゴリズムを提供する。

具体的には，アクセス権限認証が必要になったとき，コールスタック上にあるすべてのクラスに関して，対応するProtectionDomainを取得する。そして，各ProtectionDomainに割り当てられた付与アクセス権限の中に，利用したいアクセス権限(行使アクセス権限)が含まれているかどうかを検証する。もし，すべてのProtectionDomainの付与アクセス権限に行使アクセス権限が含まれる場合，“アクセス権限有”とする。どれか一つでも持たないものがあれば，“アクセス権限無”とする。

状況依存アクセス制御では，図4に示すように，行使アクセス権限と付与アクセス権限の包含関係を検証する際に，状況条件が成立するかどうかの検証を行う。行使アクセス権限が付与アクセス権限に含まれ，かつ，すべての状況条件が成立するときに，“アクセス権限有”と判定する。

```
grant “smartkey.jar”{
  # 停車中にのみ全てのドアロック解除可能
  permission ConditionalPermission,
    “DoorLockPermission, *, unlock”, “stop” ;
}
```

図3．アクセス制御ポリシーの例

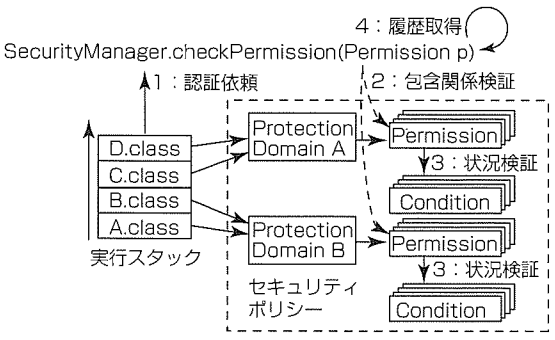


図4．状況依存アクセス制御アルゴリズムの概念

3.5 状況依存アクセス制御の組み込み

Javaアクセス制御の実装では，権限認証の高速化のために，行使アクセス権限と付与アクセス権限のクラス名が同一でない場合，異なる権限と見なして検証をスキップする。そのため，前述のように状況条件付きアクセス権限ConditionalPermissionをアクセス制御ポリシーで指定しても，その評価は一切行われない。

そこで，従来のアクセス権限の比較処理に加えて，状況条件付きアクセス権限ConditionalPermissionも比較を行うアクセス権限比較クラスを作成した。そして，アクセス制御ポリシーの読み込みの際に，このクラスにアクセス権限を保持させるように変更することで，アクセス権限認証の際にこのクラスが利用されるようにした。

なお，アクセス制御ポリシーはシステムごとに異なるフォーマットで保管されることが考えられる。そこで，Java実行環境では，アクセス制御ポリシーファイルを読み込むクラスを，設定で容易に変更できる仕組みを用意している。そこで，この仕様に従ってアクセス制御ポリシーを読み込むクラスを作成し，その中で我々が実装したアクセス権限比較クラスをインスタンス化した。これによって，Javaソースコードを改修することなく，この機能追加が実施できた。また，従来のアクセス権限処理も正しく実装しているため，従来の状況非依存なアクセス権限も利用可能である。

3.6 履歴登録の実施

過去のアクセス権限行使回数又は間隔に依存するアクセス権限を実現するためには，アクセス権限の行使履歴を保管する必要がある。

検討の結果，アクセス権限行使履歴は，“アクセス権限有”と判定された後に取得するべきと考えた。現状のJavaアクセス制御のクラス構成から，この結果を知りうるのは，SecurityManagerのみであることが分かった。そこで，SecurityManagerで，アクセス権限認証が完了した後にアクセス権限行使履歴を取得することとした。

なお，J2ME/CDC自身も多くのアクセス権限を行使して処理を行う。そのため，すべてのアクセス権限行使履歴を時系列に並べて保存することは，履歴情報参照時の性能低下を招くため好ましくない。そこで，付与アクセス権限の行使回数と行使間隔に基づく状況条件を実現するために必要な履歴情報のみを取得することとした。

3.7 アクセス制御ポリシーの配布

車の安全性を保つためには，安全性が検証されたアクセス制御ポリシーが必要となる。その配布方法として，車メーカーが一括してポリシー設定を行う方法が考えられる。

初期設定時，車載情報端末には，車メーカー内のアプリケーション認定機関で慎重に検討されたアクセス制御ポリシーが組み込まれる。その手順として，最初にユースケースを網羅的にリストアップして，それぞれ必要なアクセス権限を洗い出す。その後，安全運転の観点から，関連付けるべき状況条件をすべてリストアップする。これによって，ユースケースごとに必要最小限のアクセス権限セットが決定できる。最後に，出荷時にインストールされる各アプリケーションの用途に応じて，必要なアクセス権限セットを選択してアクセス権限ポリシーを作成する。

運用時に，アプリケーション認定機関は，車メーカーやコンテンツプロバイダが作成したアプリケーションの動作検証を実施する。そして，動作の正当性が検証できた場合だけ，その用途に応じたアクセス権限セットを選択し，車載情報端末にポリシーを設定する。

このようにアプリケーションの用途に応じて車メーカーが慎重に決定したアクセス権限ポリシーで動作の制御ができるため，安全性の確保が可能となる。

4. むすび

車載Javaプラットフォームのセキュリティを向上させるため，J2ME/CDCで状況依存アクセス制御を可能とする実現方式について述べた。具体的には，状況条件という概念をドメインセキュリティモデルに導入し，これをアクセス権限と関連付ける仕組みを実現することによって，状況条件付きアクセス権限と履歴条件付きアクセス権限を利用可能とした。

今後は，実際のテレマティクスサービスのユースケースに適用し，機能の十分性の評価を実施していきたい。また，ネットワーク経由での制御も考慮し，リモートユーザーに応じたアクセス制御へも拡張を図っていきたい。

参考文献

(1) 松田　規，ほか：状況依存アクセス制御方式によるセキュア車載Javaプラットフォームの実現，情報処理学会論文誌，**46**，No.12，2983～2996（2005）

(2) Gong，L.，et al.：Implementing Protection Domains in the Java Development Kit 1.2，Internet Society Symposium on Network and Distributed System Security，San Diego，CA，125～134（1998）

(3) Gosling，J.，et al.：The Java Language Specification，Addison Wesley（1996）

センサセキュリティ技術

伊藤　隆*
米田　健**

Sensor Security Technology

Takashi Ito, Takeshi Yoneda

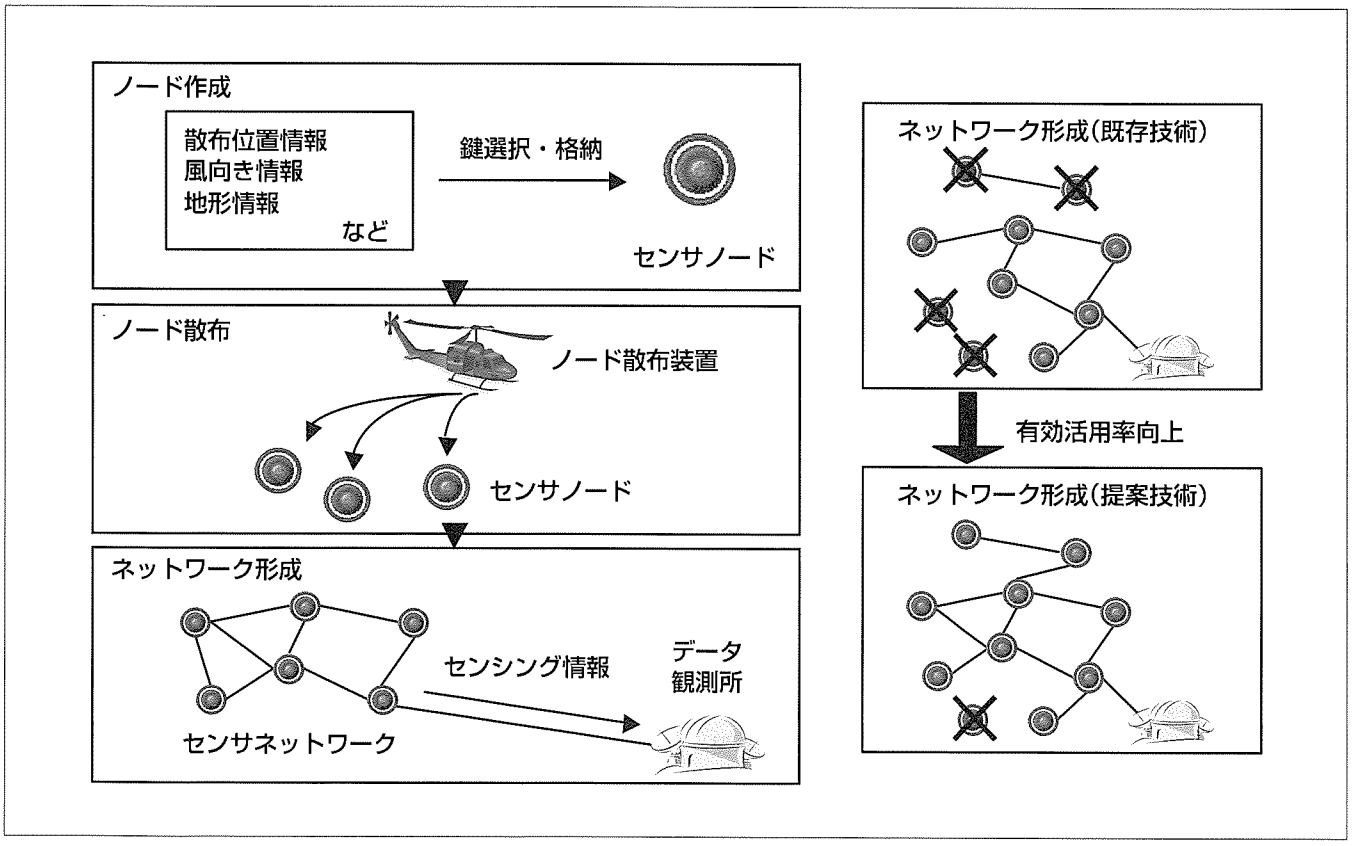
要　旨

センサネットワークは，大量のセンサノードから構成されるアドホックネットワークであり，ビル・工場管理，物流管理，環境情報の収集など，多方面への応用が期待されている。その中でも，ヘリコプターなどの移動体が広域を移動しながら大量のセンサノードを散布する“散布型センサネットワーク”は，迅速なネットワーク形成や，人手による設置が困難な場所でのネットワーク形成などが容易であるという好ましい性質を持つため，近年注目されている。

一般に，センサノード間の通信には無線が利用されるため，暗号化などのセキュリティ技術を用いた情報保護が必要不可欠である。このため，ノード間で安全に暗号鍵(かぎ)を共有する必要があるが，非力なCPU(Central Processing Unit)，小容量のメモリが用いられる散布型センサネットワークでの実現は容易ではない。

一つの解決策として，ランダムに選択した鍵を各ノードに格納し，確率的な鍵共有を可能とする“ランダム鍵格納方式”がある。また，この改良として，ノードを規則的に散布するという前提のもとで，鍵共有の成功確率を改善する方式が提案されている。しかしこれらの方式は，ノード散布手段に関する自由度が低く，散布手段によっては鍵共有の成功確率が大きく低下してしまうという問題があった。

我々の提案するランダム鍵格納方式では，散布における予想着地点の情報を鍵格納時に利用することで，任意の散布手段への適合を可能とする。提案方式について，鍵共有の成功確率を計算機実験によって評価した結果，散布の均一性を重視する散布手段のもとで，既存方式よりも40%高い成功確率を達成する結果が得られた。



散布型センサネットワーク

図左は散布型センサネットワークの形成手順を表したものである。散布位置などの事前情報を用いて選択した暗号鍵を各センサノードに格納し，これらノードをヘリコプターなどの移動体を用いて空中から散布する。図右は提案技術の利用による性能向上の様子を示したものである。安全に暗号通信を行えるノード対(線で結ばれたノード対)が増え，ネットワークから孤立するノード(×印のノード)を削減することができる。

*情報技術総合研究所　**同研究所(工博)

1. まえがき

センサネットワークは，大量のセンサノードから構成されるアドホックネットワークであり，ビル・工場管理，物流管理，環境情報の収集など，多方面への応用が期待されている。その中でも，ヘリコプターなどの移動体が広域を移動しながら大量のセンサノードを散布する“散布型センサネットワーク”は，迅速なネットワーク形成や，人手による設置が困難な場所でのネットワーク形成などが容易であるという好ましい性質を持つため，近年注目されている。

一般に，センサノード間の通信には無線が利用されるため，暗号化などのセキュリティ技術を用いた情報保護が必要不可欠である。このため，ノード間で安全に暗号鍵を共有する必要があるが，非力なCPU，小容量のメモリが用いられる散布型センサネットワークでの実現は容易ではない。

一つの解決策として，ランダムに選択した鍵を各ノードに格納し，確率的な鍵共有を可能とする“ランダム鍵格納方式”がある。また，この改良として，ノードを規則的に散布するという前提のもとで，鍵共有の成功確率を改善する方式が提案されている。しかしこれらの方式は，ノード散布手段に関する自由度が低く，散布手段によっては鍵共有の成功確率が大きく低下してしまうという問題があった。

本稿では，散布における予想着地点の情報を鍵格納時に利用することで，任意の散布手段に適合するランダム鍵格納方式について述べる。また，鍵共有の成功確率を計算機実験によって評価した結果，散布の均一性を重視する散布手段のもとで，既存方式よりも40%高い成功確率を達成する結果が得られたことについても述べる。

2. 散布情報を利用したランダム鍵格納方式

散布型センサネットワークで，既存の鍵共有方式を利用することは，次の理由から困難であった。

- 公開鍵方式の利用は非力なCPUには不向きである。
- 全体で1個の共通鍵を利用する方式は鍵漏えいに弱い。
- 他のすべてのノードと共通鍵を共有する方式は，メモリ容量の制限を考慮すると現実的でない。

これらの問題点を解決する方式として，ランダム鍵格納方式がEschenauerらによって提案された[2]。これは，事前に生成された鍵の集合(以下“鍵プール”という。)から複数の鍵をランダムに選択し，これらを各ノードに格納することで，任意の2ノードがある程度の確率で共通の鍵を保持することを期待する方式である。これによって，各ノードが保持する鍵数を現実的な値に抑えることが可能となる。

この改良として，ノード散布の位置情報を鍵格納時に利用する方式が，Duらによって提案されている[3]（以下“group-based scheme”という。)。group-based schemeでは，次の“グループ散布モデル”を仮定している。

- 散布するノードをl個のグループに分割する。
- ノード散布対象空間をl個の長方形に分割し(以下，各長方形を“散布エリア”という。)，l個のノードグループと1対1に対応させる。
- 各散布エリアに対応づけられたノードを，散布エリア中心の上空の散布点から散布する。

図1は，ノード散布対象空間を3×3の散布エリアに分割した例である($l=9$)。この場合，散布するノードを9グループに分割して各散布エリアに対応させた後，ヘリコプターなどの移動体が各散布エリアに対応する散布点(黒丸)まで移動し，そこから対応するノードを一斉に散布し，これを9地点のそれぞれで繰り返すことになる。

センサネットワークを効率よく形成するためには，“近い2ノードは鍵を共有するが，遠い2ノードは鍵を共有しない”という性質を満たすことが望ましい。group-based schemeでは，散布エリアごとに異なる鍵プールを利用することで，これを達成している。

3. 散布の確率分布を利用したランダム鍵格納方式

この章では，我々が提案するランダム鍵格納方式について述べる。我々の方式では，前述の性質を満たすために，ノード散布対象空間内の各地点と鍵との対応を表すkey-position mapを事前に生成する。鍵格納の際には，key-position map上の予想散布領域に含まれる鍵をランダムに選択する(**図2**)。予想散布領域は，散布の確率密度関数(Probability Density Function：PDF)から得られる。以降，提案方式をPDF-based schemeという。

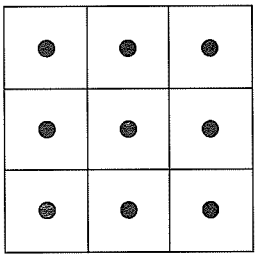


図1．散布エリアと散布点

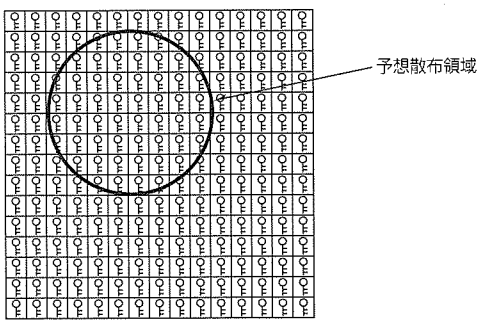


図2．Key-position mapと予想散布領域

3.1 前提条件

散布型センサネットワークで，ノードを空中から散布する場合，空気抵抗などの影響によって，地上での配置にばらつきが生じる。このばらつきは，確率密度関数を用いて表すことができる。PDF-based schemeでは，ノード配置の確率密度関数が既知である，又は推定できることが前提条件である。なお，風のない状態で軽いノードを散布する場合，各ノードは水平方向にランダムに移動しながら落下すると考えられ，この場合の確率密度関数は二次元正規分布となることが知られている。

3.2 鍵格納アルゴリズム

PDF-based schemeでは，次の手順で鍵格納を実行する。

[準備]

(1) セキュリティパラメータn，mを決定する。nは鍵プール中の鍵総数，mは各ノードに格納する鍵数である。これらは，各ノードのリソース，及びネットワークの連結性やノード盗難に対する耐性などの要件を考慮して決定する(**4.1節**)。

(2) ノード散布対象空間を，同じ大きさのn個の区域に分割する(以下，各区域を"鍵エリア"という。)。

(3) n個の鍵を生成する。

(4) n個の鍵をn個の鍵エリアと1対1で対応させることで，key-position mapを作成する(例えば**図2**のようなkey-position mapが作成される。)。

[鍵格納]

(5) ノードSの配置の確率密度関数に従い，Sの予想配置を一点サンプリングし，Pとする。

(6) Pを中心とする半径rの円内から一点をサンプリングし，Qとする(rは各ノードの通信可能距離を表す。)。

(7) Qを含む鍵エリアをAとし，(4)でAに対応付けられた鍵を，Sに格納する。Sに同じ鍵が格納されている場合は(5)からやり直す。

(8) Sにm個の鍵が格納されるまで，上記の処理(5)～(7)を繰り返す。

(9) 鍵格納(5)～(8)を全ノードに対して行う。

図3は，1個のノードに1個の鍵を格納する処理(5)～(7)の具体例を表す説明図である。簡単のため，確率密度関数として，ある円内で一様で，円外では0であるようなものを用いる。(5)では，ノードSの予想配置Pを，大円(Sの予想散布領域を表す。)の中からランダムに選択する。(6)では，点Qを，小円(Pの通信可能領域を表す。)の中からランダムに選択し，(7)で，点Qに対応づけられた鍵(図で灰色表示したもの)をSに格納する。

前述したように，散布型センサネットワークでは，直接通信できる2ノードは共通の鍵を保持することが望ましいが，直接通信できない2ノードは共通の鍵を保持する必要がない。したがって，効率的な鍵共有を行うためには，2ノードが近ければ近いほど，高確率で共通の鍵を保持していることが望ましい。PDF-based schemeを利用すると，2ノードの散布点が近い場合，**図4**の各円内で表される鍵プールが多くの共通部分を持つことになるため，2ノードが共通の鍵を保持する確率が高くなる。このように，key-position mapを利用することで，任意の散布点及び確率密度関数に対して"2ノードが近ければ近いほど高確率で鍵共有できる"という性質を達成することができる。

3.3 Group-based schemeとの比較

group-based schemeはグループ散布モデルにのみ適用可能であり，その散布点は格子状に並んだ規則的なものに限定される。一方，PDF-based schemeには散布点に関する制限がまったくないため，任意の散布モデル(例えば，不規則に並んだ散布点からの散布，ヘリコプターと車を併用した散布など)に適用することができる。加えて，PDF-based schemeでは，すべての散布点が散布前に確定している必要がないため，空中の任意の地点で位置を測定し，リアルタイムに鍵を格納してノードを散布するといった臨機応変な散布も可能である。これによって，散布の際に，決められた散布点にヘリコプターを正確に移動させるといった高度な操縦技術が不要となる。また，風などの気象条件を即座に反映した散布も実現可能である。

4. 性能評価

前章では，我々の提案方式であるPDF-based schemeが定性的な利点を持っていることを述べた。この章では，

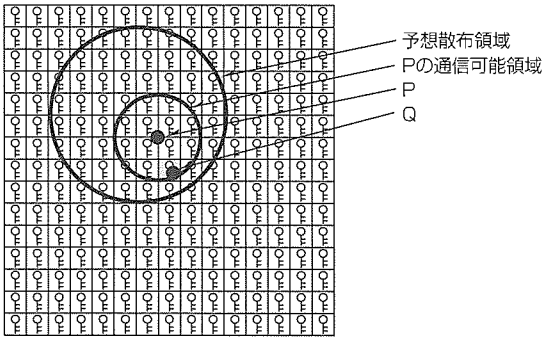


図3．P，Qをサンプリングして格納する鍵を決定

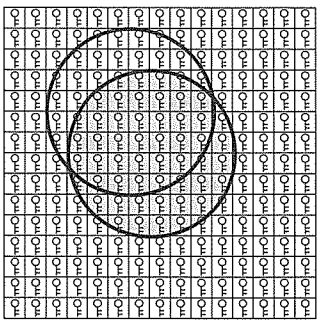


図4．散布点が近い2ノードに対応する鍵プール

定量的な観点から性能を評価する。

4.1 性能評価指標

ランダム鍵格納方式の性能を評価するためのいくつかの指標が提案されている。本稿では，ネットワークの連結性を指標とした性能値について述べる。

ネットワークの連結性を表す指標local connectivityは，“通信可能領域内にある2ノードが共通の鍵を保持する確率”で定義される。local connectivityが高いほど，安全に通信できるノード対が増え，全体的な通信オーバーヘッドも低減される。

4.2 ネットワークの連結性

ここでは，2種類の散布モデルについて，group-based schemeとPDF-based schemeの連結性を比較した計算機実験の結果について述べる。

4.2.1 標準的なグループ散布モデル

Duらの論文に記載されているものと同じ，最も標準的な散布モデルである。実験条件は次のとおりとした。

- 鍵プール中の鍵総数nは100,000
- ノード総数は10,000
- ノード散布対象空間は1,000m×1,000m
- ノード散布対象空間を10×10の散布エリアに分割し，各散布エリアの中心を散布点とする
- ノード散布の確率密度関数は，散布点を中心とする，標準偏差50mの二次元正規分布
- ノードの通信可能距離は40m
- group-based schemeにおけるoverlapping factor(鍵プール同士の重なりを表す値)はa=0.167，b=0.083
- 10回の実験における平均値を算出

図5は，各ノードの鍵数mを変化させたときのlocal connectivityの値である。図より，m<70ではgroup-based schemeの方が高い連結性を示しているが，m>70ではPDF-based schemeの方が上回っていることが分かる。

4.2.2 散布エリアの分割を細かくした場合

グループ散布モデルで，全体的なノードの分布を均一にするためには，散布エリアの分割を細かくする必要がある。そこで，**4.2.1項**の条件から次の点のみを変化させて実験を行った。

- ノード散布対象空間を20×20の散布エリアに分割し，各散布エリアの中心を散布点とする

図6は，各ノードの鍵数mを変化させたときのlocal connectivityの値である。**4.2.1項**の結果(**図5**)と比較すると，PDF-based schemeは同程度の連結性を達成しているが，group-based schemeは連結性が大きく低下している。この結果から，group-based schemeは散布エリアの分割に関する制限を持つが，PDF-based schemeはそのような制限を持たないことが分かる。

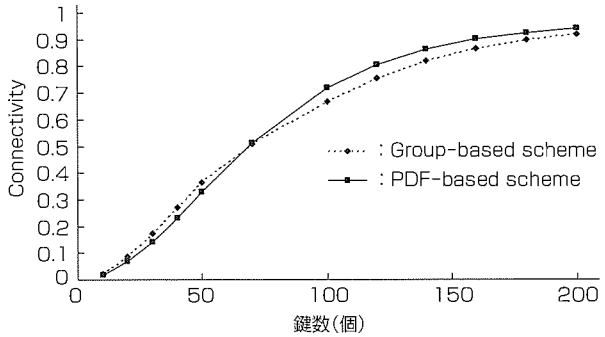


図5．Local Connectivity(標準的散布モデル)

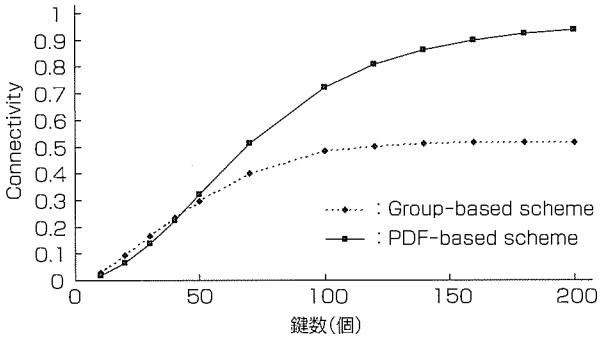


図6．Local Connectivity(20×20の散布エリア)

5. むすび

散布型センサネットワークで，散布の確率分布を利用して鍵格納を行うPDF-based schemeについて述べた。この方式は任意の散布モデルに適用可能であるため，できるだけ均一に散布を行いたい場合や，不規則な散布を行う場合など，あらゆる場面に有効利用できる。また，具体的な条件のもとで，この方式がgroup-based schemeよりも高い連結性を達成できることを示した。

本稿で示した連結性の値は，すべて計算機実験によって得られたものである。今後の課題として，ランダムグラフ理論を用いた連結性の解析的評価が挙げられる。

参考文献

(1) 伊藤　隆，ほか：散布型センサネットワークにおける散布の確率分布を利用した鍵格納方式，電子情報通信学会論文誌，**J89-A**，No.12，1034～1043（2006）

(2) Eschenauer，L.，et al.：A key-management scheme for distributed sensor networks，Proc. 9th ACM Conf. on Computer and Communications Security，41～47（2002）

(3) Du，W.，et al.：A key management scheme for wireless sensor networks using deployment knowledge，Proc. IEEE INFOCOM 2004，586～597（2004）

PKI技術への当社の取り組み

武田　哲*
山中忠和*
茗原秀幸**

Our Efforts to PKI Technology

Satoshi Takeda, Tadakazu Yamanaka, Hideyuki Miyohara

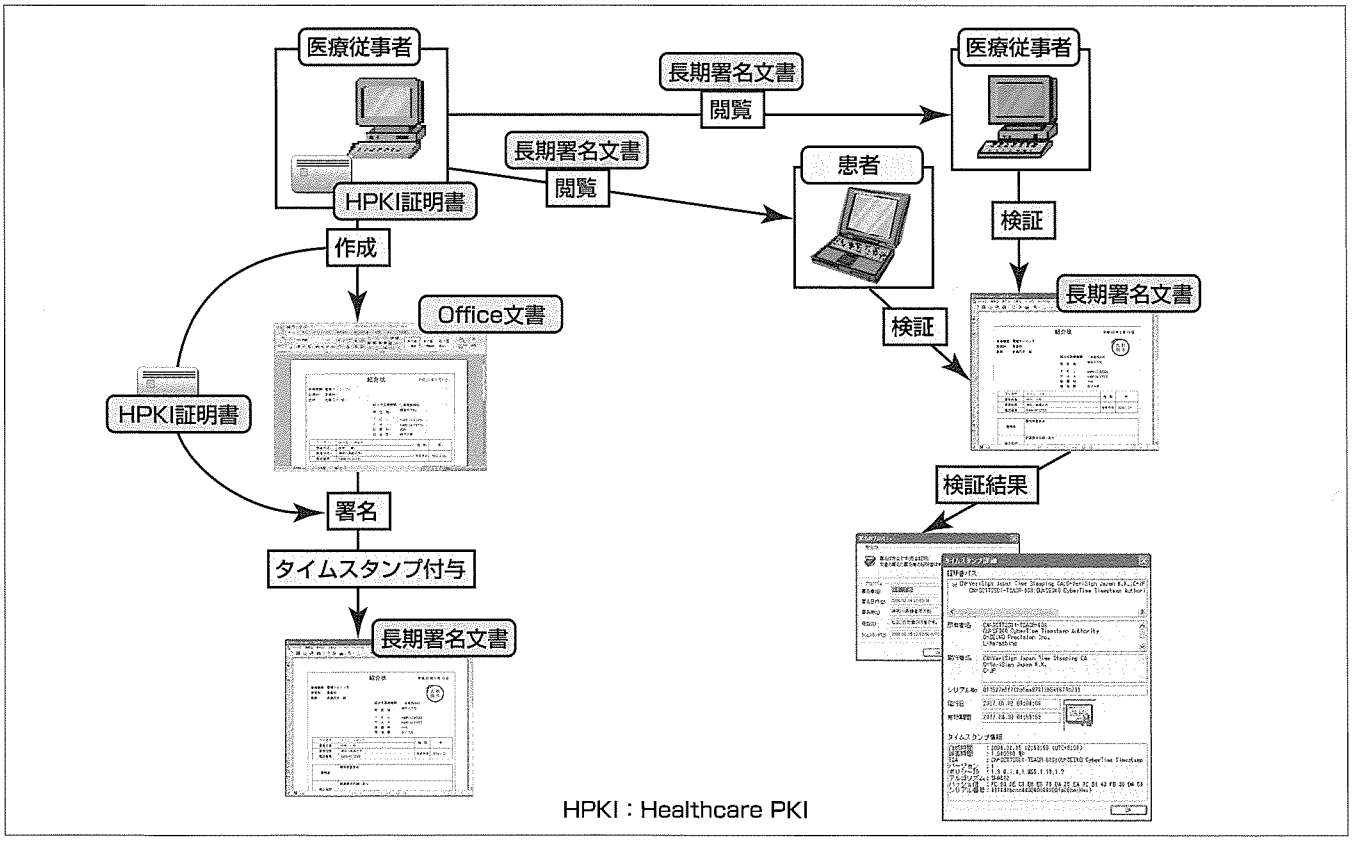
要　旨

e-文書法の施行によって電子文書の保存が認められ，記名押印又は署名に代わりPKI（Public Key Infrastructure）技術に基づく電子署名を利用することで署名付きの文書の電子化が可能になった。しかしPKIでは電子文書の保存期間中に署名用の電子証明書の有効期間が過ぎてしまうと，電子文書に対し行った電子署名の有効性を確認できなくなってしまうという問題を抱えている。

長期署名技術は，電子証明書の有効期間後も電子署名の有効性を保証する技術で，国際的な標準仕様として定義されている。日本では日本工業標準調査会（JISC）で長期署名フォーマットのJIS化審議が行われ，また保健医療福祉情報システム工業会（JAHIS）で，医療文書の電子保存や電子署名についてガイドライン作成や規格検討が行われている。

三菱電機はJIS原案を作成した次世代電子商取引推進協議会（ECOM）やJAHISの委員会に参画し，長期署名フォーマットのプロファイル策定や相互運用性テストに参加してきた。ECOM相互運用性テストでは当社が開発した長期署名ライブラリが合格し，JIS案長期署名プロファイルへの準拠性を確認できた。さらに長期署名ライブラリを使用したMicrosoft(注1) Officeアドイン長期署名アプリケーションを試作し，Office上で長期署名フォーマットの構築や検証を実現した。Office上で紙文書と同様の法的効力がある電子署名を行った電子文書の作成・保存ができ，紙や管理コスト，時間コストの削減が見込まれる。

（注1）　Microsoftは，米国及びその他の国における米国Microsoft Corp.の登録商標である。



Microsoft Officeアドイン長期署名アプリケーション

Office上で長期署名フォーマットの構築や検証を実現する。医療文書など法律で保存期間が定められた文書への電子署名が生成でき，これまでの紙文書に替わり，e-文書法における電子保存の要件を満たす電子文書の作成・保存が可能になる。

*情報技術総合研究所　**本社

1. まえがき

2001年に施行された電子署名法「電子署名及び認証業務に関する法律」によって，PKI技術に基づいた電子署名が法的効力を持つようになり，電子署名された電子文書を作成した本人の確認と電子文書の非改ざんについて，署名検証技術による電子的確認が法的に可能となった。この結果，公共機関の電子入札や国税電子申告・納税システムe-Taxなどの電子申請・申告システムで，申請データや申告データへの電子署名の利用が進んでいる。

また，2005年に施行されたe-文書法「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」によって，民間に保存が義務付けられている文書の電子データでの保存が認められ，領収書や損益計算書，診療録などこれまで紙での保存が義務付けられていた文書の一部は，紙同様に文書の電子データでの保存が認められるようになった。

電子保存される文書の作成者の確認や改ざん防止には電子署名が有効である。しかし電子署名の検証に用いられる電子証明書について，電子署名法では有効期間は5年を超えないとされており，一方で電子保存される文書の法律で定める保存期間は，領収書や損益計算書が7年など，5年を超える書類が多い。このため，電子文書の保存期間内に電子署名を行った電子証明書が有効期間を過ぎてしまい，電子署名の有効性を確認できなくなってしまうことが問題となる。

長期署名技術は，電子証明書の有効期間後も電子署名の有効性を保証する技術で，IETF(Internet Engineering Task Force)やETSI(European Telecommunications Standards Institute)で標準化されている。ECOMからは長期署名フォーマットのJIS化提案が行われており，長期署名フォーマットのプロファイル策定や，策定したプロファイルに基づく複数ベンダー間による相互運用性テストが実施されてきた。JAHISでは保健医療福祉情報システムの相互運用性確保のため，医療文書の電子保存や電子署名についてガイドライン作成や規格化が行われている。

当社はECOMやJAHISの委員会に参画し，長期署名フォーマットのプロファイル策定や相互運用性テストに参加してきた。本稿では当社におけるPKI技術への取り組みとして，ECOMやJAHISにおける標準化活動と，当社開発状況について述べる。

2. 標準化動向

2.1 長期署名フォーマット

電子署名は，電子文書の真正性を保証する技術であり，利用者が信頼する認証局が発行する電子証明書とその秘密鍵(かぎ)を用いて電子署名を生成し，電子証明書と公開鍵を用いて有効性検証を行う。電子署名の有効性は電子証明書の有効期間内であること，失効していないことによって確認できる。電子証明書の失効は，証明書発行後の秘密鍵の漏洩(ろうえい)やアルゴリズムの危殆(きたい)化，証明書の記載内容の変更などが考えられる。失効が生じた場合，電子署名が偽造される可能性が否定できないため，電子文書作成当時の電子署名の有効性を保証することができない。電子署名の有効性を保証するためには，電子文書作成当時に電子署名が存在したことを示す必要がある。電子署名には生成した時刻を属性として設定することが可能であるが，これは通常マシンのシステム時刻が設定されるため，信頼性のないシステム時刻では，電子署名の有効性を保証することができない。生成時の電子署名の有効性を後日確認できるようにするためには，次の点が要件となる。

- 署名存在時刻を確定する。
- 再検証に必要な証拠情報を明確化する。
- 電子署名文書と再検証に必要な情報を改ざん検知可能な状態にする。
- 電子署名文書と再検証に必要な情報を改ざん検知可能な状態のままで保存する。

これらの要件を満たすフォーマットとして長期署名フォーマットがある。長期署名フォーマットは“電子証明書の有効期限後でも，古い暗号アルゴリズムが危殆化しようとも”電子署名の有効性を保証できるフォーマットである。長期署名フォーマットのデータは**図1**のとおり，電子文書や署名値(ES)に加え，署名存在時刻を示す署名タイムスタンプ(ES-T)，検証情報として使用する電子証明書や失効情報へのリファレンス情報(ES-C)，署名値及び署名タイムスタンプの検証情報として使用する電子証明書や失効情報(ES-X)，さらにアーカイブタイムスタンプ(ES-A)を含める。タイムスタンプとは，電子文書が“いつ”存在し

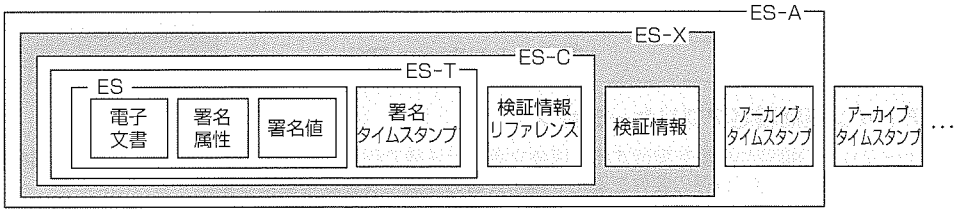


図1．長期署名フォーマット

たかを証明する時刻データであり，日本でタイムスタンプの発行サービスを行う機関は，認定制度によってタイムスタンプの信頼性が担保されている。危殆化していない暗号アルゴリズムによるアーカイブタイムスタンプを付与し続ける間，電子署名の有効性を延長することができる。長期署名フォーマットに含まれる署名値及び署名タイムスタンプ，電子証明書や失効情報の整合性を検証することによって，長期間データの真正性が維持されていたことを証明することが可能となる。

長期署名フォーマットはCMS(Cryptographic Message Syntax)，XML(eXtensible Markup Language)署名の拡張フォーマットであり，それぞれCAdES(CMS Advanced Electric Signatures)，XAdES(XML Advanced Electric Signatures)と呼ばれており，RFC 3126[1]やETSI TS 101 733[2]，ETSI TS 101 903[3]で標準規格となっている。

2.2 JIS案長期署名プロファイル

ECOMでは電子署名の保存技術に関するガイドラインの作成や調査研究が行われており，その中で当社は電子署名普及ワーキンググループ(WG)の活動に参画している。電子署名普及WGでは電子文書の長期保存に関する研究が行われており，その一環として前節で述べた長期署名フォーマットのプロファイル(長期署名プロファイル)の標準化活動が進められている。その活動の中でETSIとの間で意見交換を行い，ECOMが作成した長期署名プロファイルとETSI仕様のプロファイルとの整合化を図った上で長期署名プロファイルのJIS案“CMS利用電子署名(CAdES)の長期署名プロファイル”[4]，“XML署名利用電子署名(XAdES)の長期署名プロファイル”[5]が作成された。さらに“電子文書長期保存ハンドブック”[6]ではCAdES，XAdESデータの生成及び検証にかかわる処理系を正確に実装するための手順等について記されている。

2.3 JAHISの取り組み

e-文書法の成立後，各省から出されたe-文書法に関する主務省令で，文書の作成で記名・押印に代わる氏名等を明らかにする措置として，電子署名が定められている。

厚生労働省は診療録等の電子保存に関して“医療情報システムの安全管理に関するガイドライン”(安全管理のガイドライン)を作成し，このガイドラインの中で，法令で定められた記名・押印を電子署名で行うことについて次の点が示されている。

- 認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと。
- 電子署名を含む文書全体にタイムスタンプを付与すること。

JAHISは保健医療福祉分野の標準化を推進しており，保健医療福祉情報システムの相互運用性確保のため，電子保存や電子署名の標準化が進められている。“保存が義務付けられた診療録等の電子保存ガイドライン”(JAHIS電子保存ガイドライン)[7]では，診療録等の電子保存に関する要件が，前記安全管理のガイドラインよりさらに具体的に示されている。

まず電子保存する診療録等への電子署名に用いる電子証明書については，認定特定認証事業者の発行する電子証明書ではなく，e-文書法施行後に厚生労働省によって整備されている保健医療福祉分野PKI(HPKI)の電子証明書が推奨されている。HPKIの証明書ポリシーでは，電子証明書に資格情報を記載するために，証明書拡張フィールドにhcRole属性を使用できる。署名検証者はhcRoleによって，署名者が医師など国家資格を持つことや病院長など医療機関の管理責任者であることを識別できる特徴がある。

またタイムスタンプの付与については，付与する対象として，次のどちらかの方式を採用するよう示されている。

①電子署名を含む文書全体(文書＋署名値)

②文書全体に対してなされた電子署名の値

さらに証明書の有効性については，タイムスタンプ付与時点で電子署名が有効であったことを示すために，証明書検証に必要となる認証パス上の証明書や失効情報などの情報の真正性を保って保存するよう示され，格納形式は前記標準の長期署名フォーマットが推奨されている。署名者は，自ら保存義務がある文書はES-Aフォーマットまで，外部提出用の文書はES-Tフォーマットまでを作成するよう示されている。

電子署名及びタイムスタンプが付された電子文書の署名検証や証明書検証を確実に行えるようにするため，現在“JAHIS ヘルスケアPKIを利用した医療文書に対する電子署名規格”[8]が策定中である。

3. 当社の取り組み

3.1 ECOM長期署名プロファイルのJIS案による相互運用性テスト

ECOMでは2006年度から2007年度にかけて複数ベンダー間での相互運用性テスト“長期署名プロファイルのJIS案による相互運用性テスト”が実施された。相互運用性テストは当社を合わせ18社が参加し，㈶日本データ通信協会から時刻認証業務認定事業者の認定を受けたタイムスタンプ発行サービスを行う3社の協力で行われた。相互運用性テストは次の2種類のテストからなる。

(1) オフライン長期署名フォーマット検証テスト

ECOMからJIS案長期署名プロファイルに準拠した長期署名データ，検証データ，設定データが用意され，参加各社の製品又は試作品がオフラインで長期署名データの有効性を検証し，ECOMが想定した結果と合致するか確認するテスト。

(2) 製品マトリックス相互運用テスト

参加各社の製品(試作品)によって作成したデータが，他社の製品で検証しJIS案に準拠した生成機能及び検証機能が実装されているか確認するテスト。ECOMによって検証データ，設定データが用意され，タイムスタンプは協力3社のタイムスタンプ局を利用して実施する。

当社は開発したCAdES，XAdES双方のライブラリのJIS案長期署名プロファイルへの準拠性を確認するため，相互運用性テストに参加した。テストではまず当社ライブラリによって他社作成の長期署名フォーマットデータが準拠性を持っていることを確認した。並行して当社も長期署名フォーマットデータを作成し，当社作成データが他社検証機能で正常に検証できていることが確認された。このことから，当社CAdES，XAdES双方のライブラリのJIS案長期署名プロファイルへの準拠性を確認することができた。

3.2 Officeアドイン長期署名アプリケーション

e-文書法によって領収書や損益計算書，診療録といった文書についても電子保存が認められるようになり，長期間真正性を保証する電子文書を作成するアプリケーションのニーズが高まってきている。電子文書作成アプリケーションから直接電子署名を生成することを目的として，広く電子文書作成に利用されているMicrosoft Office 2007用アドインとなる，Officeアドイン長期署名アプリケーションを開発した。

Officeアドイン長期署名アプリケーションは，JAHIS電子保存ガイドラインで外部提出用文書への適用が推奨されているES-Tフォーマットのデータを構築，検証する機能を持ち，PDF(Portable Document Format)文書のCAdESデータ及びOpenXML文書のXAdESデータを作成する。作成機能では，CAdESデータの場合はPDF文書作成後，PDF文書の署名生成，タイムスタンプ付与を行い，XAdESデータの場合はOffice上で作成されたOpenXML文書の署名生成，タイムスタンプ付与を行い，CAdES，XAdESそれぞれのES-Tフォーマットデータを作成する。

これまではOfficeで文書を作成後，印刷した紙文書に押印し保存していたが，Officeアドイン長期署名アプリケーションによって，Office上で長期署名フォーマットの構築や検証を実現し，紙文書と同様の法的効力がある電子文書の作成・保存が可能になる。この結果，紙や管理コストの削減，電子メールやファイルサーバを利用し即時のデータのやり取りやデータ共有による時間コストの削減が見込まれる。

4. むすび

電子署名の有効性を長期間にわたって保証する長期署名技術の標準化と，当社開発状況について述べた。Officeアドイン長期署名アプリケーションは医療分野に限らず，保存期間が定められている文書の電子署名アプリケーションとして，幅広い分野で適用可能と考える。また三菱署名有効性延長システムと組み合わせることで，長期署名の有効性を自動的に延長することが可能である。さらに長期署名ライブラリを既存のアプリケーションに組み込み，様々な製品で長期署名が生成可能となるよう検討する。

参考文献

(1) RFC 3126：Electronic Signature Formats for long term electronic signatures (2001)
(2) ETSI TS 101 733 V1.7.3：CMS Advanced Electronic Signatures(CAdES) (2007)
(3) ETSI TS 101 903 V1.3.2：XML Advanced Electronic Signatures(XAdES) (2006)
(4) 次世代電子商取引推進協議会：CMS利用電子署名(CAdES)の長期署名プロファイル (2007)
(5) 次世代電子商取引推進協議会：XML署名利用電子署名(XAdES)の長期署名プロファイル (2007)
(6) 次世代電子商取引推進協議会：電子文書長期保存ハンドブック (2007)
(7) 保健医療福祉情報システム工業会：保存が義務付けられた診療録等の電子保存ガイドライン (2007)
(8) 保健医療福祉情報システム工業会：JAHIS ヘルスケアPKIを利用した医療文書に対する電子署名規格(案) (2007)

情報セキュリティガバナンスシステム

近藤誠一* 佐伯保晴***
撫中達司** 遠藤 淳***
鶴川達也*

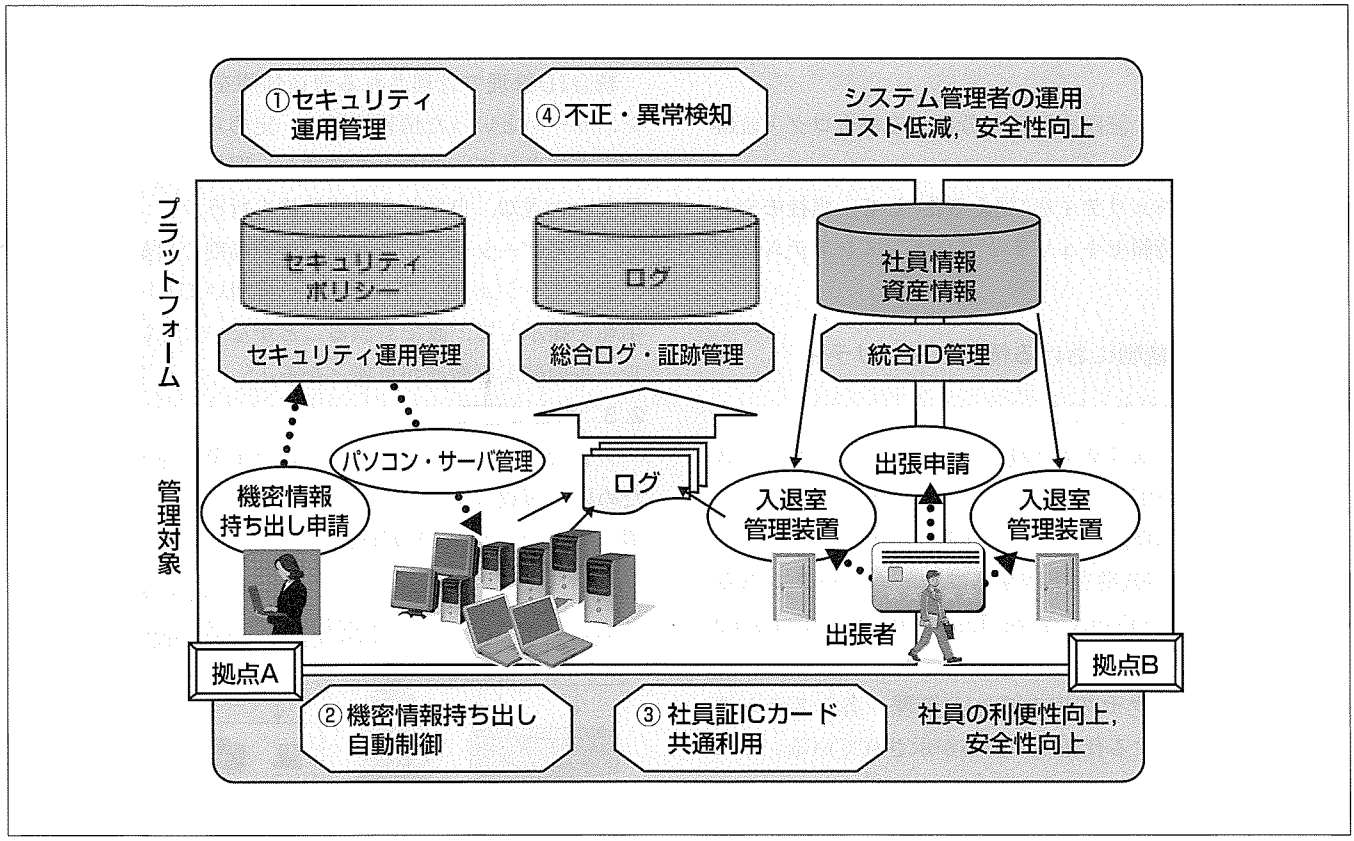
Information Security Governance System

Seiichi Kondo, Tatsuji Munaka, Tatsuya Tsurukawa, Yasuharu Saeki, Jun Endo

要 旨

増加・多様化するセキュリティ脅威によるデータ破壊や情報漏えい事故など，情報セキュリティ対策の不備が原因で被る経済的な損害は，社会的責任も含めると膨大なものになる。一方で，2005年に個人情報保護法，2006年に会社法，金融商品取引法が施行され，コンプライアンス経営が，企業にとって不可欠な課題となっている。しかし，そのための技術的な対策が人に依存している限り，周知・教育だけでは徹底は難しく，継続的にセキュリティを維持・向上していくためには，体系的な統制が有効であると考えられている。そこで，セキュリティ統制で必要とされるセキュリティポリシー，社員情報・資産情報，ログをデータベース化して集中管理し，セキュリティ運用管理技術，統合ID管理技術，統合ログ・証跡管理技術を適用した情報セキュリティガバナンスシステムを三菱電機のモデル地区に構築し，その検証を行った。

システム構築の結果，①パソコン・サーバのルール適合性チェック自動化によるシステム管理者の運用コスト低減，安全性向上，②機密情報の外部持ち出し時の社員の利便性向上，安全性向上，③出張先での本人の社員証ICカードを使用した入退室による社員の利便性向上，安全性向上，④異種ログの組み合わせ分析による不正・異常検知，といった効果が得られた。このシステムの構築・運用ノウハウを今後のセキュリティシステム構築に活用していく所存である。



情報セキュリティガバナンスシステムのモデル地区適用全体構成

①セキュリティ運用管理：資産情報として管理されるパソコン・サーバを対象にセキュリティポリシーの管理実施支援，監査，是正を行う。
②機密情報持ち出し自動制御：セキュリティポリシーで定められた持ち出し手順に則って許可された資産の持ち出し，証跡管理を行う。
③社員証ICカード共通利用：セキュリティポリシーで定められた出張先入場承認手順に則って別拠点の入退室装置に社員証情報を配布する。
④不正・異常検知：多様なログ，外部持ち出しファイルを集中管理し，社員情報，資産情報を補って追跡し，セキュリティポリシー違反を検知する。

*情報技術総合研究所 **同研究所(工博) ***本社

1. まえがき

IT利活用の進展に伴い，セキュリティ脅威は年々増加・多様化の一途をたどっている。ウイルスによるデータ破壊や情報漏えい事故など，セキュリティ対策の不備が原因で被る経済的な損害は，自社のみではなく，取引先や顧客にまで及ぶため，社会的責任も含めると膨大なものになる。一方で，2005年に個人情報保護法，2006年に会社法，金融商品取引法が施行され，上場企業には内部統制システムの整備と内部統制報告書の提出が義務付けられるなど，法律が整備され，コンプライアンス経営が，企業にとって不可欠な課題となっている。

このような環境のもと，これまでの情報セキュリティ対策のように，個別の脅威に対して個別に対策を施すと，導入コスト，運用コストが増大するだけでなく，費用対効果が見えなくなり，将来コストの算定が困難になるという課題が発生する。また，情報セキュリティ関連のみならず，入退室管理システム，監視カメラなどの物理セキュリティ，社員証発行管理，採用・異動，資産管理などの人事・総務・経理関係のシステムも含めた，トータルなリスクマネジメントとして検討することが重要である。

本稿では，

(1) 会社規則，運用手順を定めたセキュリティ運用管理
(2) 従業員，派遣社員，情報資産の統合ID管理(アイデンティティ管理)
(3) 実行した行為，証跡を蓄積・分析する統合ログ・証跡管理

によって情報セキュリティを“見える化”して，当社モデル地区に構築した情報セキュリティガバナンスシステムについて述べる。

2. 内部統制における情報セキュリティ

2.1 見える情報セキュリティ

多様化するセキュリティ脅威への対応，トータルなリスクマネジメントを実現し，継続的に維持・向上させていくためには，体系的な内部統制の仕組みが有効であると考えられている。内部統制を実現するフレームワークであるCOBIT(Control Objectives for Information and related Technology)[1]では，会社規則に則ったプロセスの整備，ユーザー情報，アクセス権の統合ID管理，各システムのログを集積・監査する仕組みの構築が示されている。これを情報セキュリティに適用し，“見える”情報セキュリティを実現したプラットフォームを図1に示す。次の3つの要素から構成される。

(1) セキュリティ運用管理

“情報資産のルールが守られているか”を見える化する。ルールに則った手続きの実行支援，監査，是正を行う。

(2) 統合ID管理

“誰が何をできるか”を見える化する。ユーザー情報，情報機器，コンテンツのIDの管理と，アクセス権の管理を行う。

(3) 統合ログ・証跡管理

“誰が何をしたか”を見える化する。行為をログとして管理するだけでなく，社外送信したメール，社外へ持ち出す媒体に格納した機密情報を，事故に備えて保全する。

これらの統制を行う仕組みを用いて，運用中の情報セキュリティの維持・向上を支援する。

2.2 セキュリティ運用管理

個人情報保護法，不正アクセス禁止法などの法制度，ISO/IEC27001，ISMS(Information Security Management System)などの標準セキュリティ基準に基づいてセキュリティポリシーが定められる。しかし，セキュリティポリシーを文書化して従業員個人に周知するのみでは，正しい手順に則った措置，不備が発見されたときの対策実施の徹底，実施状況の把握が課題となる。特に，セキュリティ維持の手順は，複雑性が増して，教育，利便性，ルールの変更などの問題によって，ITシステムによる自動化抜きでは網羅性，確実性の観点から徹底が困難であると考えられる。そこで，規則の実行支援として次の2点の機能を実現した。

(1) 情報機器に対するセキュリティ設定自動チェック

統合ID管理で管理される資産情報を参照して，パソコン，サーバといった情報機器に，定められたセキュリティ設定が施されていることを確認し，問題がある場合は，管理者への通知，自動的な是正措置を行う。

(2) ナビゲーションによる手続きの高度な自動化

ナビゲーション，ワークフローを用いてルールに則った手順を提示して，誰でも誤ることがないようにすることで，ルールの確実な徹底が可能となる。

2.3 統合ID管理

アクセス制御ポリシーに基づいた企業全体の統制を行うために，複数のシステムで扱うユーザー情報，情報機器情報，コンテンツ情報のID管理を統一的に行う仕組みを提

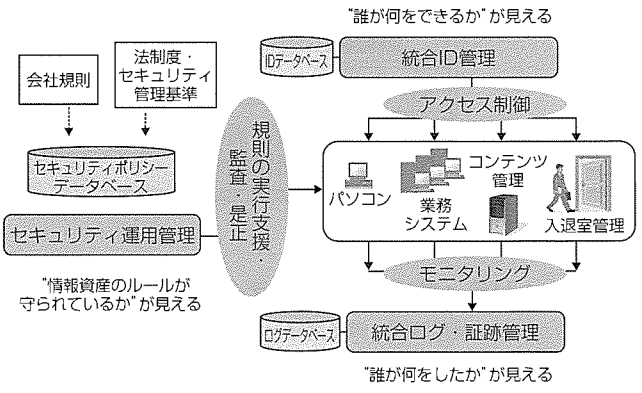


図1．“見える”情報セキュリティ

供する。特に大企業では，認証・認可を必要とする多様なシステムが，地理的に分散して配置されているため，入社・異動・退職などの人事異動，施設・設備配備などの変更情報を遅延なく反映することが課題となる。また，出張者・訪問者・社員証紛失者への一時的な権限付与・取り消しに即座に対応する必要がある。統合ID管理では，日本的な組織階層構造に則したアクセス権定義をルールベースで行うロールベースアクセス制御[2]拡張モデルを採用して，ユーザー情報の多様な変化に対応したアイデンティティライフサイクルの管理を可能とした[3][4]。

2.4 統合ログ・証跡管理

“誰が何をしたか”を蓄積し，参照可能とするためには，次の点が課題となる。

①多様性：対象とするシステムが多様なため，異なる形式のログに対応する必要がある。

②大規模：すべての従業員，すべての情報機器のログを蓄積するためには，テラバイト級の大規模ログに対応する必要がある。

③証拠：漏えい事故対策のためには，外部に流失した情報の再現が必要となる。

①，②に対しては，出力されたすべての可変長の項目をそのままの形式で圧縮保存し，高速検索可能とする技術を実現した[5]。また，統合ID管理で管理される情報を補うことによって，異種ログのトレースが可能となる[4]。③に対しては，添付ファイルを含むメール，インターネットへのアップロードファイル，持ち出し用の機密ファイルを一括保存し，高速検索可能とした。

3. 情報セキュリティガバナンスシステム

3.1 セキュリティ運用管理システム

セキュリティ対策の導入は，一方でITの利便性を低下させるため，対策の不徹底によるセキュリティ事故が発生している。セキュリティ設定や確認作業が，人手で行われていることが，設定確認の漏れやモラル低下を引き起こしている。そこで，ITの利便性を維持したままセキュリティ対策を実現することでセキュリティ事故の防止を図るため，セキュリティ運用管理システムを構築した。このシステムの全体構成を**図2**に示す。監視対象であるパソコン，サーバのセキュリティ設定を定義したセキュリティポリシーをプログラムから分離してデータベース化し，LAN(Local Area Network)接続された監視対象のパソコン，サーバを定期的に，自動チェックする。

このシステムの導入効果を次に示す。

(1) セキュリティ設定確認作業・監査の網羅性，確実性向上

監視対象が一定のセキュリティレベルに到達可能となる。実施状況が実時間で把握可能なため，違反状態にある期間を最小化することが可能となる。

(2) セキュリティ設定確認作業・監査の作業効率向上

セキュリティ監視の自動化による情報収集コスト削減，及び，結果の一元管理による確認作業の効率化を図ることが可能となる。

特長として，自然言語で記述されたセキュリティポリシーとの整合性チェック支援，プログラムから独立したセキュリティポリシー管理，監視項目設定が挙げられる。

3.2 機密情報持ち出し自動制御システム

社外でプレゼンテーションを実施したり，電子メールを利用したりする際，機密情報を可搬媒体・機器に格納して社外に持ち出す必要性がある。持ち出した媒体・機器の盗難・紛失時に，機密情報が漏えいしないようにするために，ファイルの暗号化などを手順に組み込んだルールを定める対策がとられる。しかし，人の運用に委ねると操作誤り，ルールの不徹底のため，漏えいのリスクが高まる。そこで，手順の自動実行，機器の自動チェックを行うシステムを構築した。このシステムを利用した持ち出し手順を**図3**に示す。

①機密情報持ち出しワークフローに起票する。ルールに沿って，誤りなく，また，自動的に実行可能なように，ナビゲータの指示に従って実行する。

②**3.1節**で示したセキュリティ運用管理システムを用いて，持ち出し機器がセキュリティポリシーに沿った設定になっていることを自動的に確認する。

③管理者が申請内容の確認を行う。システムによって自動的にチェックがなされていることのみの確認で，個

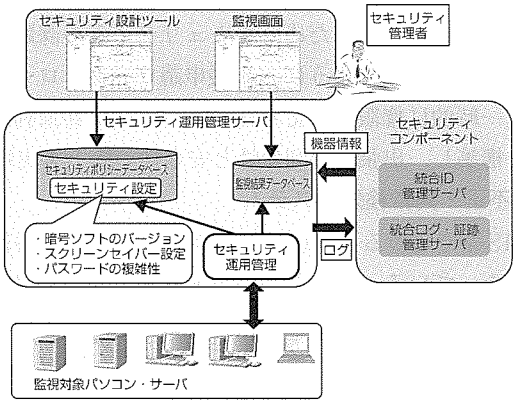


図2．セキュリティ運用管理構成

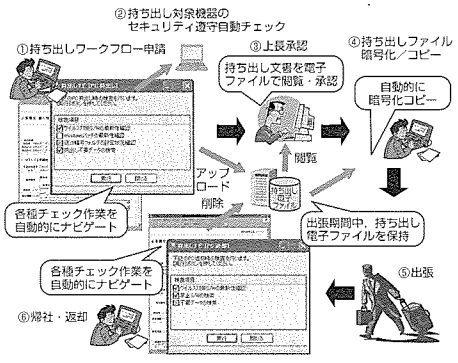


図3．機密情報持ち出し自動制御システムを利用した機密情報の持ち出し手順

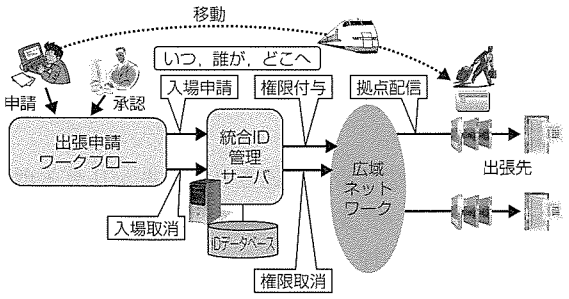


図4．社員証ICカード共通利用システム

別詳細チェックは不要である。

④許可された機密情報を自動的に暗号化して持ち出し媒体・機器にコピーする。持ち出し情報は，事故発生時に備えて，帰着時まで，一括保存される。

⑤帰着時は，ナビゲータに沿って，機密情報の削除などを自動的に行う。

このシステムの特長・効果を次に示す。

- 手順のナビゲート，自動化によって，ルールに反する誤りを防止するとともに，利便性が向上する。
- 機密情報ファイルの暗号化／コピーの自動化によって安全性が向上する。

3.3 社員証ICカード共通利用システム

ICカードで入退室管理を行う場合，安全性を確保するため，その拠点で勤務する従業員に限定して権限を与えることが多い。そのため，出張者には，人手による本人確認と臨時カード発行といった運用で対応することが一般的である。しかし，入退室管理システムには，臨時カードによる入場のみが記録されるため，セキュリティ上の課題が残る。そこで，**図4**に示すように，出張申請ワークフローに基づいて，一時的に権限を与える社員証ICカード共通利用システムを構築し，出張時の利便性と安全性の向上を実現した。

3.4 不正・異常検知システム

ISMS等で定めるように，各種システムのログ蓄積が一般的となっている。しかし，不正・異常検知で活用するためには，単独のシステムのログ分析のみでは限界がある。このシステムでは，複数の異種ログを集積，分析して不正行為，異常行為の可能性の確認が可能となる。**図5**にモデル地区におけるシステム構成例を示す。ファイルサーバ，入退室管理システム，**3.2節**の機密情報持ち出し自動制御システムのログを集積し，異常行為を検出する。例えば，在室していないユーザーがファイルサーバを操作するといった履歴矛盾を不正行為，異常行為のリスクの候補として確認作業を行う。このシステムの特長として，ID情報を補完した追跡，持ち出された機密情報の蓄積による事故発生時の影響度の把握が挙げられる。

4. 考　察

大手企業では情報セキュリティ対策のツール導入がほぼ

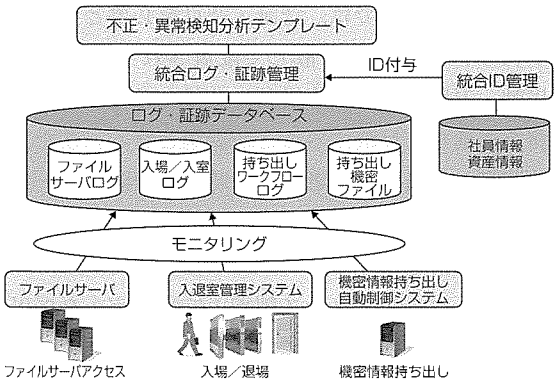


図5．不正・異常検知システム

完了した段階となっているが，運用時の課題が明確化しつつある。当社モデルシステムの構築成果は既存の各種セキュリティツールを連携して安全性・利便性を向上させるセキュリティ運用の深化を実現するベストプラクティスとして顧客に紹介できるものと期待できる。また，セキュリティ対策はコーポレートのリスクマネジメントとして実施されることから，セキュリティポリシーに基づいて定められる各種実施基準の全社適用状況をCISO(Chief Information Security Officer)などに一元的に見える化できるようにするソリューションへの要請は大きいと考えている。

5. むすび

セキュリティ統制で必要とされるセキュリティ運用管理技術，統合ID管理技術，統合ログ・証跡管理技術を開発し，当社モデル地区に適用した情報セキュリティガバナンスシステムについて述べた。このシステムの効果を高めるためには，既存システム，既存運用であらかじめ準備しておくことが望ましい事項があるものと考えている。また，統制のために集中管理された各種情報の安全性，可用性を高める必要があると考えている。

参考文献

(1) IT Governance Institute, COBIT 4.1 (2007)

(2) Ferraiolo, D.F., et al.：Role－Based Access Control, Second Edition, Computer Security Series, ARTECH HOUSE (2007)

(3) 近藤誠一，ほか：ロールベースアクセス制御情報の多バージョン並行処理制御を利用した監査ログトラッキング手法，情報処理学会論文誌，**46**，No.SIG18 (TOD 28)，103～115 (2005)

(4) 近藤誠一，ほか：ユーザー情報の多様な変化に対応したアイデンティティライフサイクル管理技術，三菱電機技報，**80**，No.10，627～630 (2006)

(5) 郡　光則，ほか：多種多様なログの統合管理を実現する“LogAuditor Enterprise”，三菱電機技報，**80**，No.10，615～618 (2006)

特許と新案＊＊＊

三菱電機は特許及び新案を有償開放しております

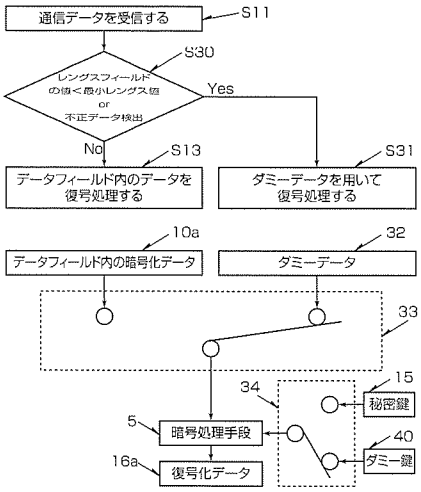
有償開放についてのお問合せは
三菱電機株式会社　知的財産渉外部
電話(03)3218-9192(ダイヤルイン)

暗号通信装置　特許第3902440号(特開2003-134110)

発明者　山田敬喜，佐藤恒夫

この発明は，暗号通信装置内の秘密情報を読み出す困難性を向上させる装置に関するものである。従来の暗号通信装置では，秘密情報を用いて演算を行う際に，電力波形や処理時間など攻撃者に有益な情報が外部に漏れてしまい，なりすましや改ざん，通信の回線盗聴などに対して十分なセキュリティの確保ができないという課題があった。

この発明は，これらの課題を解決するためになされたもので，通信データの真偽性を判断し，その真偽に応じて処理フローを制御することで，十分なセキュリティを確保しつつ，耐タンパ性に優れた暗号通信装置を得ることを目的とする。図はこの発明による処理フロー及び実装ブロック図である。この発明にかかわる暗号通信装置は，通信データを受信する(S11)とデータのレングスフィールドの値と暗号通信装置内に記憶されている最小レングス値を比較，又は，レングスフィールドの値と実際に受信したデータ長を比較するなどして，データの真偽を判定する(S30)。不正データであれば，ダミーデータを用いて復号し(S31)，不正データでなければ，データフィールド内のデータを復号処理する(S13)。ダミーデータ(32)やダミー鍵(かぎ)(40)は乱数発生器などで生成し，切り替え手段(33，34)でデータフィールド内の暗号化データ(10a)や秘密鍵(15)と切り替えて，暗号処理手段(5)に送り，復号化データ(16a)を得る。この処理フローによって，データの真偽判定に応じて処理フローを制御し，攻撃者には無益な情報を与え，セキュリティを確保する。



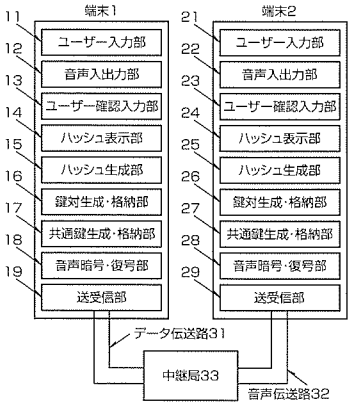
共通鍵共有方法　特許第3917330号(特開2000-354031)

発明者　米田　健

この発明は，端末間の暗号通信に用いる共通鍵(かぎ)を安全・簡便に共有する方法に関するものである。従来の共通鍵共有方法では，端末に事前に秘密鍵と公開鍵証明書を割り当てる。端末は，共通鍵を生成後，相手端末の公開鍵証明書を検証し，公開鍵証明書に含まれる公開鍵で共通鍵を暗号化する。そして，暗号化した共通鍵を相手端末に送付することで安全に共通鍵を共有する。しかし，公開鍵証明書を端末に発行する手順は複雑であるという課題があった。

この発明は，これらの課題を解決するためになされたもので，共有した共通鍵と共有に用いた公開鍵を結合した情報のハッシュ値を視覚的に表示する手段と，音声ハッシュ値の入出力手段によって，公開鍵証明書を用いることなく，安全な共通鍵共有を実現することを目的とする。

図はこの発明のブロック図である。端末１では，鍵対生成・格納部16で公開鍵・秘密鍵を生成後，公開鍵を相手端末に送付する。端末２は，共通鍵生成・格納部27で共通鍵生成後，受け取った公開鍵で暗号化して送り返す。端末１，２で，上記の公開鍵と共通鍵を結合した情報からハッシュ値をハッシュ生成部15，25で生成し，ハッシュ表示部14，24に表示する。利用者は，表示されたハッシュ値と相手利用者が音声で伝えるハッシュ値が一致していれば，ユーザー確認入力部13，23を押下し，暗号通信を開始する。この発明によって中継局33による公開鍵のすり替えに対しても安全な共通鍵の共有を実現できる。



暗号化装置及び暗号化方法及び暗号化プログラム及び復号装置及び復号方法及び復号プログラム及び暗号化復号システム　特許第4015385号(特開2003-046501)

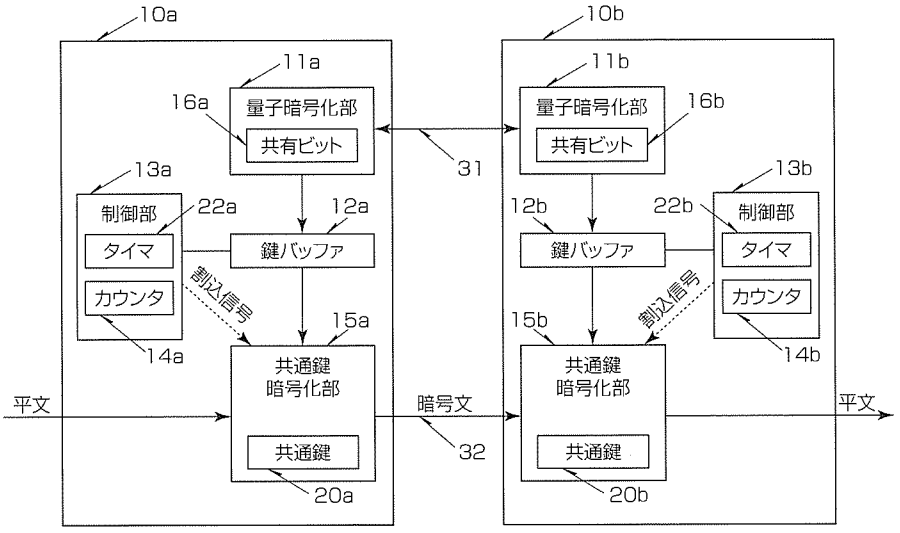
発明者　松井　充

この発明は，量子暗号と共通鍵(かぎ)暗号を組み合わせた暗号化方法並びに復号方法に関するものである。従来の量子暗号とバーナム暗号を組み合わせた暗号化方法では，暗号化速度が著しく遅く，また最低暗号処理速度が保証されないという課題があった。

この発明は，このような課題を解決するためになされたもので，データの暗号処理の安全性の強化と高速化の両立を目的としている。

図の左側はこの発明による暗号化装置，右側は復号装置のそれぞれ一実施例である。量子暗号化部(11)によって量子通信路(31)を介して共有されたビットは，鍵バッファ(12)に順次蓄えられ，これが所定のビット数に到達するたびごとに制御部(13)からの指示で共通鍵暗号化部(15)に供給される。共通鍵暗号化部はこのビット列を共通鍵(20)として，古典通信路(32)を用いて平文の暗号化並びに暗号文の復号を実行する。

制御部(13)はまたタイマ(22)を持ち，所定の時間内に共通鍵暗号化部へのビット供給行われなかった場合には，割り込み信号を発生し，共通鍵暗号化部の動作を一時的に遅らせる。これによって，量子通信路で盗聴が行われた場合に，その間に生成された共通鍵を用いてデータを暗号化してしまうリスクを回避するとともに，通常時には共通鍵を頻繁に更新することで，安全かつ高速な暗号通信を提供することができる。



〈本号記載の商標について〉
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.82 No.6 特集「高周波・光デバイス」

三菱電機技報編集委員
委員長　山口隆一
委員　小林智里　増田正幸　滝田英徳
佐野康之　糸田　敬　世木逸雄
江頭　誠　河合清司　長谷勝弘
木槻純一　逸見和久　光永一正
河内浩明　橘高大造
事務局　園田克己
本号取りまとめ委員　松井　充

三菱電機技報　82巻5号　2008年5月22日　印刷
(無断転載・複製を禁ず)　2008年5月25日　発行
編集人　山口隆一
発行人　園田克己
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
〒102-0073　東京都千代田区九段北一丁目13番5号
日本地所第一ビル　電話(03)3288局1847
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945円(本体900円)送料別

三菱電機技報 URL　URL http://www.mitsubishielectric.co.jp/corporate/giho/
三菱電機技報に関するお問い合わせ先　URL http://www.mitsubishielectric.co.jp/support/corporate/giho.html
英文季刊誌「MITSUBISHI ELECTRIC ADVANCE」がご覧いただけます　URL http://global.mitsubishielectric.com/company/rd/advance/

スポットライト

ファイル暗号ソフトウェア
MistyGuard<CRYPTOFILE PLUS>活用例

CRYPTOFILE PLUSは，多彩な暗号化機能で，情報漏洩(ろうえい)防止とIT(情報技術)の利便性の両立を可能にするソフトウェアです。パソコンに導入するだけで使い始めることができ，パソコン内のファイルに加え，共用ファイルサーバ内のファイル暗号化も可能です。また，機密ファイルをリムーバブルディスクに書き出したり，インターネットを経由して発信する際に，そのファイルを暗号化することによって，第三者への情報漏洩を防止できます。ファイルを自動的に暗号化することもできますので，暗号化を意識する必要がありません。さらに，ディスクドライブ単位の常時暗号化ができるので，パソコンの紛失や盗難にあっても，ディスクからの情報漏洩を防止できます。また，ユーザーにとって負荷がかかる導入作業やメンテナンスは，簡単にインストールでき，管理サーバも不要で，セキュリティポリシー変更も容易なことから，エンドユーザーとシステム管理者の負荷を最小限に抑えられます。

<主な活用例>

1．暗号化操作漏れの防止

暗号化したいフォルダを，あらかじめ指定しておけば，フォルダ内のファイルは一定時間ごとに暗号化されるので，人的な暗号化操作漏れを防止できます。

2．パソコン共同利用者に対しての情報漏洩防止

CRYPTOFILE PLUSのログインユーザーに特定した暗号化／復号が可能です。第三者からの不正アクセスや，パソコン盗難時の情報漏洩を防止します。

3．プロジェクト部外者からの情報漏洩防止

例えば，プロジェクトメンバーのみで共有する機密ファイルは，そのメンバーのパソコンに配布される鍵(かぎ)を用いて暗号化し，同じ鍵を持つパソコンでしか復号できません。

4．離席時の画面からの情報漏洩防止

離席操作又は一定時間の無操作によって自動的にスクリーンセーバーを起動し画面ロックを行います。画面の盗み見や不正操作を防止します。

5．モバイルパソコンに対する情報漏洩防止

ドライブ単位(システムドライブは除く。)で暗号化の範囲を設定することができ，利用者は暗号化／復号を全く意識することなく，ディスク上のファイルは常時暗号化されていますので，ディスクからの情報漏洩を防止します。

6．リムーバブルメディア書き出しによる情報漏洩防止

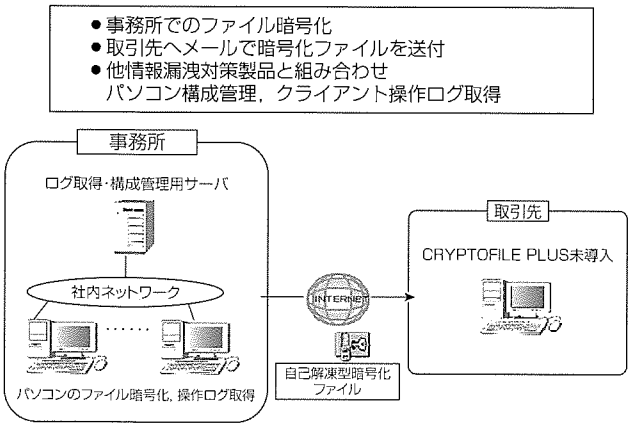
リムーバブルディスクへの書き込みを禁止することができます。また，暗号化したときだけリムーバブルディスクに書き出せる運用も可能です。

7．取引先へ情報を安全送付

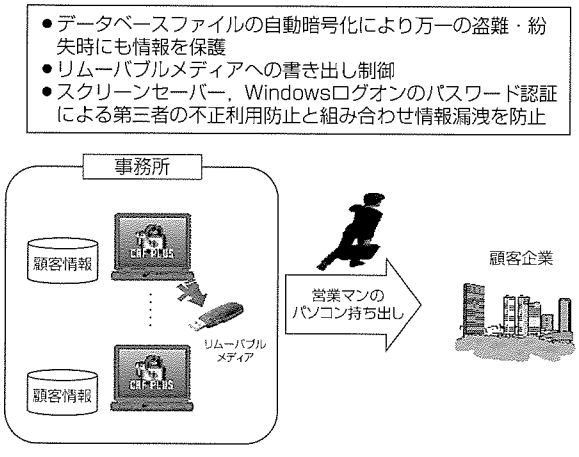
社外へのファイルの持ち出しを安全に行うために，自己解凍型の暗号化ファイルを作成できます。ファイルの解凍・復号は，パスワードを入力するだけで，CRYPTOFILE PLUSを持たないパソコンでも復号できます。

8．初期インストールの自動化

セキュリティポリシーを設定してインストーラを作成し，対象パソコンでインストールを手動で行うのが一般的ですが，インストールを自動化することが可能です。また，導入後のセキュリティポリシーの変更はアンインストールせずに行うことができます。



＜事例１＞　個人情報／機密文書の漏洩防止



＜事例２＞　顧客情報の漏洩防止

住　所：〒108-0023　東京都港区芝浦4－13－23（MS芝浦ビル）　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：セキュリティ・プラットフォーム営業部　TEL（03）5445－7766