解 説 エレクトロニック・コマース

5. ECの技術動向：セキュリティ技術

Security Technologies Trend for Electronic Commerce by Katsuhiro NAKAMURA (C&C Media Research Laboratories, NEC Corporation).

中村 勝洋[1]

1 NEC C&Cメディア研究所

1. はじめに

EC(Electronic Commerce ；電子商取引)への動きが大きな脚光を浴びつつある．ここ2～3年，国内外で，ECへ向けたさまざまな実証実験が相次いで行われ，インターネットを通じた電子ショッピングも本格化してきている．オープンネットワークとしてのインターネットの商用利用への解放を契機に，これまでにない新しい形の商取引が生まれようとしている．そこには，商習慣などの文化の問題，倫理・法制上の問題等々，解決すべき課題が数多く横たわっており，とくにセキュリティの問題，すなわち，ネットワーク犯罪としての，“なりすまし”，“盗聴”，“改竄”などの脅威に対しては，何らかの技術的対策や仕組みが必須となっている．

ネットワークでのセキュリティ技術としては，まず外部からシステム内部への不正アクセスを防ぎ，また内部から外部に不正に情報を持ち出すことを防ぐファイヤウォールの技術がある．ファイヤウォールの基本的仕組みは，守るべきシステムとインターネットとの接点に特殊なコンピュータやソフトを組み込んで，不正アクセスを防ぐための防火壁を築くものである．

一方，ネットワーク上での情報内容に対するセキュリティ基本技術としては，暗号・認証技術があり，上記，相手認証，情報の盗視防止や改竄防止などを実現する技術としてとくに最近重視されている．本稿では，まず次章でこの暗号・認証技術について述べ，ついでこの技術をECにおけるセキュリティ技術として利用していくための鍵管理の技術や暗号プロトコル技術，さらにはそのライブラリ・セキュリティミドルウェアについて述べる．ついで，ECを成立させる要でもある電子的決済プロトコルについてSETを中心に説明し，最後に電子マネーの現状を概観して締めくくる．

2. セキュリティ基本技術[1),2)]

2.1 暗号技術

送り手が情報にある秘密の変換を施して相手に伝え，受け手がその逆変換を施して元の情報を復元すること，またはその変換方法のことを暗号方式と呼ぶ．その変換方法を知らない第三者は，その通信から元の情報を盗んだり改竄することができない．現代暗号方式では，変換方法そのものを秘密にするのではなく，変換方法は公開してもそこで用いるパラメータを秘密にすることで逆変換を防止するのが主流である．このパラメータを暗号鍵，または単に鍵と呼び，変換を暗号化，逆変換を復号と呼ぶ．暗号方式には大きく分けて共通鍵暗号方式と公開鍵暗号方式がある．

共通鍵暗号方式は，送り手と受け手で共通の暗号鍵を用いる暗号方式である．そのため，送り手と受け手で互いに前もって共通の暗号鍵を共有しておく必要がある．この暗号鍵を共通鍵暗号で送ると，鍵共有の問題が繰り返されるため，別の安全な手段による配送が必要となる．共通鍵暗号の代表は米国の標準暗号DES(Data Encryption Standard)である．1970年代に登場したDESは，20年を経ていくつかの弱点が発見されるとともに，その鍵空間の小ささ(56bit)から先日ついに計算機による鍵の全数探索解読が実現され，その役割を終えつつある．代わりに，DESを多重化したTriple DESや，DESの弱点を改良した新しい暗号アルゴリズムが多数提案されてきている．

公開鍵暗号方式では，暗号化と復号で用いる鍵が異なる．まず，受け手は秘密鍵と公開鍵を自分で作成する．秘密鍵から公開鍵を計算するのは容

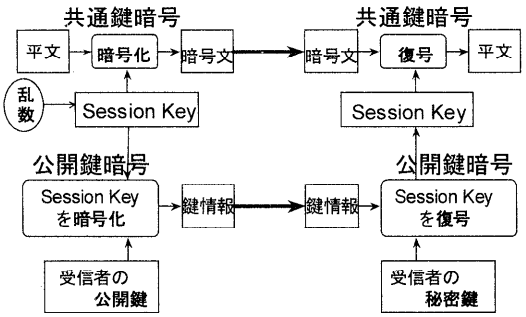

図-1 ハイブリッド方式

易だが公開鍵から秘密鍵を計算する計算量は膨大で現実的に計算不可能であるという性質があるため，公開鍵は誰にでもみせることができる．反対に，秘密鍵の方は通信相手にさえみせる必要はない．送り手が受け手の公開鍵で情報を暗号化した暗号文は，受け手の秘密鍵以外では復号できない．送り手さえも暗号文から情報を復元することはできない．公開鍵暗号の代表例はRSA暗号である．この暗号では，秘密鍵は2つの大きな素数をもとにしており，その積は公開鍵の一部となっている．公開鍵から秘密鍵を計算するには数百桁の整数の素因数分解が必要となり，現実的なコストでは解読できない．

共通鍵暗号と公開鍵暗号を比較した場合，鍵配布の簡便さでは公開鍵暗号に軍配が上がる．しかしながら，公開鍵暗号の処理速度は共通鍵暗号に比べて100～1000倍程度低速であるという問題がある．両者の長所を活かすために，情報の暗号化には共通鍵暗号を利用し，共通鍵暗号の暗号鍵を公開鍵暗号で送るハイブリッド方式の利用が主流である(**図-1** 参照)．

2.2 認証技術

暗号技術の役割として通信の秘匿のほかに，メッセージ認証や相手認証がある．メッセージ認証とは，通信の途中でメッセージが改竄されていないことを保証する技術で，相手認証は通信相手が確かに自分の意図した相手であることを確認する技術である．これらは基本的に，特定の秘密情報をもっていなければ作ることができない暗号文を検証することによって実現される．

共通鍵暗号による暗号通信では，暗号鍵をもっていなければ勝手な暗号文を作ることができないから，暗号文が復号されて意味のある正しい情報になれば，その暗号文を作った相手は正しい暗号鍵をもっている者であり，通信途中で改竄されていないことも確認できる．ただし，正しい情報とそうでない情報を区別するためには，情報に何らかの冗長性が必要である．送信情報全体を暗号変換して作る認証子(Message Authentication Code, MAC)と呼ばれる情報を付加する場合もある．これは後述するSSLなどでも利用されている．共通鍵暗号に基づくメッセージ認証では，この認証子は送信者と受信者の双方が計算することができるので，もし紛争が起こった場合に，送信者と受信者のどちらが悪いのかを第三者が判断することはできない．

公開鍵暗号に基づくメッセージ認証は**デジタル署名**と呼ばれる．先ほどの公開鍵暗号の手順において，秘密鍵と公開鍵の役割を逆転させてみる．すなわち，送信側では送信側の秘密鍵で情報を暗号変換し，受信側ではそれを送信者の公開鍵で復元してみる．復元に用いる公開鍵に対応する秘密鍵を知らなければ，正しく復元できるような暗号文を作ることはできないため，この暗号文を作った者はこの公開鍵の持ち主であることが検証できる．この検証作業は誰でもできるので，送信者と受信者以外の第三者も署名(送信者の暗号変換)を検証できる．デジタル署名技術は電子的な情報に対する印鑑の役割を果たすといわれる所以である．デジタル署名アルゴリズムの代表例もやはりRSA暗号である．

デジタル署名アルゴリズムも公開鍵暗号と同様に処理速度に問題がある．長い文書に対して直接デジタル署名アルゴリズムを施すのはたいへんなので，通常は文書を一定のサイズ(160bit程度)に圧縮した値に対して一度だけデジタル署名を施し，元の文書と組で利用する．この圧縮方式をハッシュ関数あるいはダイジェスト関数と呼び，圧縮した値をハッシュ値またはダイジェスト値と呼ぶ．検証時は，元の文書から求めたハッシュ値に対するデジタル署名が正しければ，文書に対して署名したものとみなす．したがってハッシュ関数には，異なる文書が同じハッシュ値となる衝突が，現実的な計算量では発見できないような性質が要求される．代表的なハッシュ関数には，MD5やSHAなどがある(**図-2** 参照)．

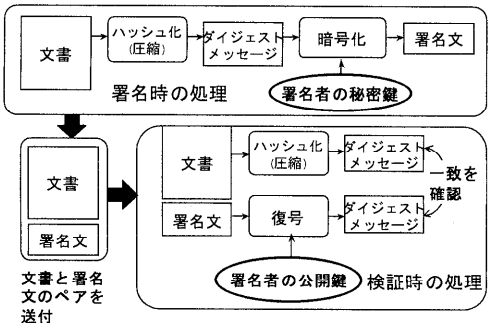

図-2 デジタル署名

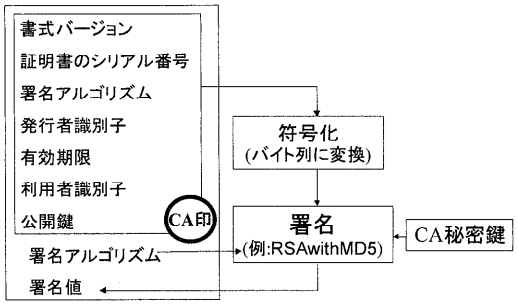

図-3 X.509証明書の書式

2.3 公開鍵管理とCA

前述の公開鍵暗号技術を利用する場合，公開鍵の管理が重要である．通信時に相手の公開鍵を取得して暗号通信や認証を行う場合，その公開鍵が確かに希望する相手のものであるという保証が必要となる．利用者と公開鍵の対応を改竄されると，他者になりすますことができてしまう．

これを避けるためには，利用者の識別子とその公開鍵の対に対して，信頼できる機関がデジタル署名を施すという技術を用いる方法が一般的である．我々の印鑑に対して市役所が印鑑登録証明書を発行するようなものだと考えるとよい．署名を施す機関をCA(Certificate Authority，認証局)と呼び，公開鍵に対してCAが署名したものを証明書(certificate)と呼ぶ．CAは階層化することができ，あるCAの公開鍵はさらに上位のCAによって証明される．ただし，おおもとになる最上位のCAの公開鍵だけは，この方法に頼らず安全な方法で取得しなければならない．

この証明書の枠組みは，ITU/T(旧CCITT)のX.509で標準化されたものが広く使われており，証明書の内容は，証明書のシリアル番号，有効期限，CAの識別子，利用者の識別子，利用者の公開鍵，そして，それら情報に対するCAのデジタル署名などが含まれている(**図-3**参照)．

秘密鍵の盗難や紛失，記載情報の変更など，なんらかの事情にともなって，有効期限内に証明書を破棄したい場合が考えられる．CAが以前に発行した証明書を破棄するには，無効な証明書のリストを配付することによって行う．このリストは，CRL(Certificate Revocation List)と呼ばれ，もちろんこのCRLにもCAのデジタル署名が施されており，悪意による失効などを防止することができる．なお，CAの運用に際しては社会的な安全性をも確保すべく，そのための総合的な指針も検討されている[3]．

このような枠組みの中で，暗号／認証通信の信頼性の一部は，CAによって保たれるということができる．主なCAとして米Verisign社や米GTE社などがあげられ，両社はまた日本支社を設立してCA事業を行っている．国内ではほかにNEC，日立，富士通3社で設立したCAの会社がある．

2.4 秘密鍵管理と耐タンパ技術

前節のような公開鍵の管理とともに，秘密鍵の取扱いも重要である．秘密鍵は決して外部に漏れてはならない．ソフトウェアによる実装では秘密鍵をそのままファイルに書き込んでいるケースがあるが，この場合その計算機が安全であるという前提が必要である．秘密鍵をパスワードで暗号化したファイルを必要時に復元して利用するものもあるが，やはり同様にパスワードが盗まれないことは計算機の安全性に依存する．

通信路上での不正を防止するだけならローカルな計算機が安全だという仮定も許されるかもしれない．しかしながら，今後暗号技術が一般的になるにつれ，秘密鍵の重要性はますます大きくなると思われる．その場合，計算機の安全性を前提とするソフトウェアによる保護には限界がある．これを解決するためには，秘密鍵を内蔵した装置が装置内部で暗号処理を行い，秘密鍵自体は決して外部に出さないように，たとえ分解されてもたとえば内部情報が消滅したりするような仕組みが必要となる．このような技術を**耐タンパ技術**という．耐タンパ技術は，金庫のような頑丈な筐体に装置を閉じ込める形態や，暗号機能をもつ半導体チッ

プなどに特殊なコーティングを被せるものなどがある．ICカードは後者の代表であり，セキュリティを高めるためにはICカードを秘密鍵の保持手段とするのが望ましい方向といえる．

3. セキュリティプロトコルとミドルウェア

暗号技術の実用化動向として，従来セキュリティの考慮されてなかった電子メールにおいて，通信秘匿，相手認証の機能を提供する電子メールの暗号化が活発である．PGP(Pritty Good Privacy)や PEM(Privacy Enhanced Mail)，S/MIMEなどがその代表である．

また，インターネット上で爆発的に普及したWWW(World Wide Web)の仕組みでセキュリティを確保することができるSSL(Secure Socket Layer)[4]やSecureHTTPなどの技術の利用も普及しつつある．SecureHTTPはその名のとおり，WWWで利用されるHTTPというプロトコルに暗号・認証機能を拡張したものである．既存のHTTP文書の内容に，前述のPEMなど別の技術の利用を可能としてセキュリティ機能を実現するものである．これに対してSSLは，WWWに限らずTCP通信一般に適用可能な技術である．ここでは，広く普及し，電子商取引とも関連が深いSSL技術について紹介する．

SSLは米NetScape社により提唱された規格であり，公開鍵暗号技術と，前述のX.509証明書を用いて，インターネット上の通信の暗号化，および相手認証を可能とする．代表的なWWWブラウザであるNetscape NavigatorやMicrosoftのInternet Explorerなどに標準で組み込まれていることもあり，主にWWW上でのセキュリティを確保するためのデファクト標準技術となっている．

SSL上の通信では，セッションとコネクションという2つの接続形態がある．1つのセッションの上に複数のコネクションが利用可能である．一般のTCP通信に該当するのはコネクションであり，セッションは複数のコネクションで共通な情報を保存・再利用して通信のオーバヘッドを削減する仕組みといえる．

通信接続に際してクライアントとサーバはハンドシェークと呼ばれる交渉を行う(図-4参照)．まず，双方で発生した乱数を交換するとともに，暗号・圧縮方式について合意し，サーバによってこの通信のセッションIDが付与される．次に，互いの証明書または公開鍵を送り合い，クライアントは別の乱数を相手の公開鍵で暗号化するとともに自分の秘密鍵でデジタル署名してサーバに渡し，サーバはこれを復号・検証することで同じ乱数を共有する．最初に交換した乱数を含めて3つの乱数から48バイトのマスタシークレットを生成する．このマスタシークレットと最初に交換した乱数から，データ暗号鍵や認証子作成鍵を作成し，これ以降の実際の通信に利用する．

次回のコネクションでは，クライアントが前回のセッションIDを指定することにより，暗号・圧縮方式の合意や，マスタシークレットの共有の手続きを省略することができる．指定されたセッションのマスタシークレットを再利用し，新たに双方で発生した乱数を作用させてデータ暗号鍵や認証子作成鍵を作成する．この仕組みは，同一のクライアント・サーバ間で何度も接続を繰り返すことの多いWWWアクセスにおいて効率がよい．

公開鍵としては前述のX.509証明書のほかに，CAによる証明のない公開鍵や，たとえばクライアントが公開鍵をもっていないことも許している．このように証明書を用いない場合の相手認証の信頼性は低下するが，それでも通信の秘匿やメッセージの改竄防止，およびセッションを通じて相手が同一であることは保証される．

ほかに通信の秘匿・認証を実現する方法として，VPN(Virtual Private Network)と呼ばれる技術がある．これは，TCP/IPの上に暗号化したTCP/IPプロトコルを載せるもので，原理的には

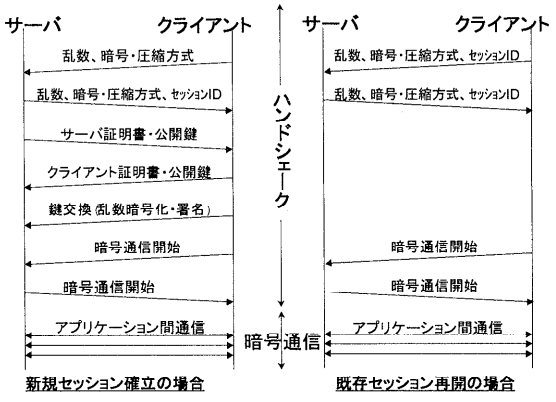

図-4 SSLプロトコル

SSLと同様の方法を使っている．基本的には，ファイヤウォールで守られた複数のイントラネットやサテライトオフィスを接続するために，インターネットを利用するのであるが，インターネット通信も暗号化すれば第三者による盗聴や改竄やなりすましなどの不正を防止できるため，仮想的に専用線とみなすことができる．現状ではファイヤウォール製品ごとに独自のVPN方式を使っているものが多く，同一のファイヤウォール製品同士でしか通信できない場合が多い．

暗号技術を利用するソフトウェア開発環境の動向も重要である．暗号アルゴリズムを実行するプログラムの開発には専門知識が必要であるため，アプリケーション開発者やユーザのために，これらをソフトウェアライブラリとして提供しているものもいくつかある．前述のSSLについてはSSLeayというフリーのソフトウェアライブラリが流通している．

より一般的なセキュリティ機能を提供するライブラリとして，インターネット上ではRFC-1509やRFC-2078などでGSSAPI(Generic Security Service API)と呼ばれるAPIが提案されている．国内でもSecureWare[5]というGSSAPIに準拠したソフトウェアライブラリが市販されている．RSAデータセキュリティ社ではRSAREF，BSAFE，JSAFEなど，暗号利用のレベルに対応したライブラリをいくつか提供している．MicrosoftはCryptoAPIというAPIのみを定め，その下にCSP(Cryptographic Service Provider)として実際の暗号処理を行う部品を自由に追加できる仕組みを開発している．

4. ECでのセキュリティ技術と標準プロトコル

ECにおけるビジネス形態には，消費者がインターネットを利用してオンライン電子ショッピングなどの商取引を行う狭義のECと，さらには，オープンなインターネット上での企業間での電子商取引に加え，電子入札，オンラインマーケティング，ネットワークパブリケーション，ゲーム開発等々の新規ビジネスが展開されていく広義のECとが考えられる．現在はこの狭義のECの定着化へ向けた実用化・実証実験が進められつつ，広義のECへの利用方法の模索・実験が検討されている段階であるといえる．

ECにおけるビジネスを定着させる上での基本的なセキュリティの課題としては，(1)取引き情報の秘匿あるいはプライバシーの確保，(2)取引き情報や相手の真正性の保証，(3)電子的決済方法の確立などが考えられる．(1)は暗号化の技術で，(2)はデジタル署名・認証技術である程度の解決をみることができるが，(3)の電子的決済の方法との融合をいかに進めるかが問題となる．

4.1 クレジットカード用電子決済プロトコル

電子ショッピングが始まったころ，通常のクレジットカードによる決済と組み合わせた決済を実施する試みがなされた．しかし，当初はクレジットカード番号をオープンなネットワークの上で流したため，多くの被害が発生した．そのため前章で述べたように，Netscape社のブラウザではSSLが採用され，クレジット番号を第三者に対して秘匿するための暗号化が行えるようになった．さらには，ネットワーク上でのセキュリティで問題となる，「第三者によるクライアントへのなりすましや商用サーバへのなりすまし」，「ネットワーク上を流れる情報の第三者による傍受や改竄」といった問題も防止できるようになったことから，電子ショッピングの流行に拍車がかかった．ただ，SSLのみでは，クレジット番号が第三者に秘匿されていても，商用サーバ(販売店)には秘匿されていない点や，利用者(クライアント)と販売店の間で，事実と異なる送信否認や受信否認が起こったときの争いを解決できる形にはなっていないといった点，さらには，クレジット会社に利用者のプライバシーにかかわる購買履歴情報が残ってしまう点などが問題としては残っていた．

決済面で全世界をカバーしているという強みをもつクレジットカード会社，とくにVISAとMASTERは，決済システムからECに本格的に切り込むため，それぞれの独自の決済プロトコルであるSTTとSEPPを，前者はMicrosoft社，後者はNetscape社をパートナにして開発した．しかし，世界的なネットワークビジネスでのEC決済の共通インフラを早急に構築することを得策として歩み寄り，1996年2月，両方を統合した決済プロトコルSET(Secure Electronic Transaction)[6]を発表した．**図-5**，**図-6**に決済プロトコルSETの概略を示す．

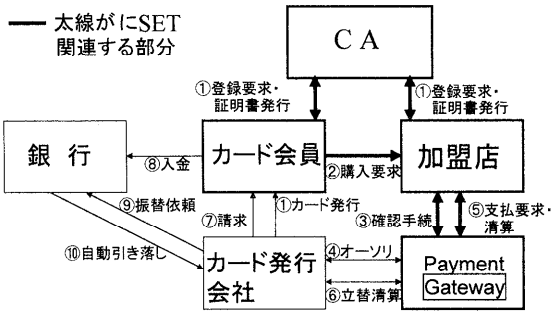

図-5 クレジットカード処理の流れ

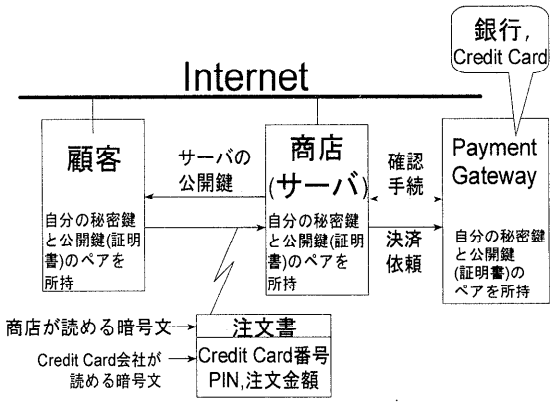

図-6 SETの概要

図からもわかるように，SETでは，従来からのクレジットカードの仕組みを前提として利用し，ネットワーク利用に関わる部分のみをカバーしている．また発注情報やカード番号などの支払い情報の内容に対するデジタル署名を行い，さらには，発注情報は加盟店のみ，支払い情報はカード会社のみがみれるように署名に工夫を施している．このため，上記SSLの問題点は改善されている．

インターネット上でのクレジットカードによる決済プロトコルとして，SETはDeFacto Standardとしての地位を占め，通産省が1995年に開始したEC推進事業のなかでも，SETの標準仕様に日本独自の仕様拡張(米国の標準的なカード決済では対応できないボーナス一括払いやリボルビング払い対応)を行った決済プロトコルSECE(Secure Electronic Commerce Environment)が富士通・日立・NECにより開発されつつある．一方，米国RSA社はSETに準拠したアプリケーション開発用キットS/PAYを開発しており，それを日本向けに拡張した開発キットJ/PAYもNECと共同開発されつつある．

4.2 電子マネーのためのセキュリティ技術[7]

電子決済手段の1つとして，電子マネーが注目され，各社からさまざまな方式が提案され，活発な実用化や実証実験が行われている．電子マネーを実現する技術は，その実現形態によっていくつかに分類できる．ここでは代表的なタイプに用いられているセキュリティ技術についていくつか紹介する．クレジット型と呼ばれるタイプは，クレジットカードや小切手と同様の決済方法であり，利用者が支払いの意思を証明することで決済される．実現は簡単であるが，誰が何を購入したかなどのプライバシーの保護に難が残る．前述のSETによる決済や，CyberCacheなどが代表的である．

Digicache社のe-cacheでは，銀行の署名が施されたデジタル情報が現金の役割を果たす．利用者が銀行からこの現金を受け取る際にブラインド署名という技術を用いることで，発行した現金データは銀行にもわからなくなり，現金の利用を追跡できない．支払いをする場合，この現金情報にある変換を施した情報を提出することで，店舗では銀行の署名を検証できる．しかし，もし利用者がその現金データを二度利用すれば，追跡が可能になる仕掛けがしてある．

Mondexの電子マネーではICカードが，蓄積された金額情報を内部に保持しており，ATMで預金をカードに転送すればこの値が増加し，買い物をすれば減少する仕組みであり，電子財布とも呼ばれる．カード間の価値の移動も可能である．ここではICカードの物理的安全性を前提としている．秘密鍵を封じ込めた耐タンパ性のICカードは，クローンを偽造することが困難であるから，その秘密鍵で認証に成功したICカードは本物であると信頼することができる．Mondexマネーは ICカードを信頼することで成り立っている．

5. あとがき

ECのためのセキュリティ技術の動向について概観した．書き終えてみて，ECに関する技術の奥深さを痛感している．本タイトルで書くべきことが，まだまだ多く残されているからである．電子マネーに関する諸問題と今後[7]，CALSやオー

プン EDI(Electronic Data Interchange)[8]におけるセキュリティとの関係，電子すかし技術とマルチメディア情報の著作権[9]との関係，鍵(データ)回復技術の動向と今後[10]，プライバシー保護を考慮した，プロファイル情報の交換のための規格案[11]等々，社会的な構造変化を引き起こす要因を含むECであればこそと考えつつも，本稿が何らかの形で読者諸氏のお役に立てれば幸いである．

参考文献

1) Kaufman, C., Perlman, R. and Speciner, M.: Network, Security, 500p., Prentice Hall PTR (1995).
2) Schneier, B.: Applied Cryptography Second, Edition, 750p., John Wiley&Sons, Inc.(1996).
3) たとえばhttp://www.ecom.or.jp/about_wg/wg08/guidline.htm
4) 稲村 雄: WWW, Open Design, No.14, pp.100-117, CQ出版社 (1996).
5) SecureWare/開発キットリファレンスマニュアル, NEC (1996).
6) VISA, MASTER: Secure Electronic Transaction (SET) Specification Ver.1 (May 1997).
7) たとえば岩村 充：電子マネー入門，187p.，日経文庫，日本経済新聞社 (1996).
8) たとえばhttp://www.ecom.or.jp/jedic/index.htm
9) たとえば名和小太郎：サイバースペースの著作権，中公新書 (1996).
10) たとえばhttp://www.kra.org/
11) http://www.w3.org/TR/NOTE-OPS-FrameWork.html

(平成9年8月11日受付)

中村 勝洋(正会員)

1945年生．1967年東京大学工学部計数工学科(数理工学コース)卒業．同年NEC中央研究所入社．以後，符号理論，暗号理論，とくに各種デジタル通信系，記憶系での誤り訂正符号や，回線暗号方式，情報セキュリティ方式の研究開発などに従事．1988年C&C情報研究所情報基礎研究部長，1994年C&C研究所統括部長，1996年同所セキュリティ統括部長，1997年C&Cメディア研究所主席技師長，現在に至る．この間，1985年米国UCLA客員研究員．1996年度電子情報通信学会情報理論研究専門委員会委員長．「暗号と情報セキュリティ」(辻井・笠原編，1990，昭晃堂)第7章執筆．電子情報通信学会，情報理論とその応用学会各会員．

e-mail:nakamura@ccm.cl.nec.co.jp