解 説 エレクトロニック・コマース

4. ECの技術動向：要素技術全般

Elements of EC Technology by Hideo HIYAMA (MITSUBISHI ELECTRIC CORPORATION, Information Technology R&D Center, Information Security Department).

檜山 秀郎[1]

1 三菱電機(株)情報技術総合研究所情報セキュリティ技術部

1. はじめに

ECの要素技術は情報通信技術全般にわたる．また要素技術を応用して実現されるECのコンポーネントにはさまざまなバリエーションがある．ここでは，ECを特徴づける主な要素技術と構成要素について概説する．

2. ECの構成と必要とされる技術

ECの構成要素は現実世界の経済活動をモデルとした消費者，商店，決済センター（または銀行）のほかに，認証局を加えた4つの構成要素に分けられる．それぞれの構成要素はさらにそれらを実現するハードウェアやソフトウェアのコンポーネントから構成される．

(1)消費者

ECにおいて消費者は商品の購入者のことを指す．消費者側では商店にアクセスするためのPCやICカードをもっている．ICカードは本人認証のためのトークンカードの役割や，電子現金を保存する電子財布の役割を果たす．また，ICカードを利用する場合にはネットワークを使わず直接リアルな商店へ行って買い物をし，商店設置のPOS端末から電子決済を行う形態もある．

(2)商店（電子モール）

ECにおいて商店は商品の管理，展示，配送および決済または決済の依頼を行う機能を有する．扱う商品は通信販売のような物品であったり，画像やソフトウェアのようなデジタルコンテンツであったりする．主にWWWサーバとデータベースを組み合わせて構築する．

(3)決済センター

決済センターの役割はバーチャルな金銭価値情報をリアルな経済世界の価値に交換することにある．機能としては銀行やカード会社の役割を担う．決済の形態により実現方式はさまざまであるが，消費者や商店からみると，決済サーバまたは決済ゲートウェイとして機能する，主な決済の形態を以下に示す．これについては改めて後述する．

- 電子現金決済（ストアードバリュー型&ネットワーク型）
- プリペイド型決済
- 電子個人小切手決済
- デビッドカード決済
- 銀行決済（銀行POS）
- クレジットカード決済

(4)認証局

認証局はバーチャル世界で当事者同士の相手認証や信用保証をする認証書の発行機関である．基本原理については改めて後述する．

上記の構成要素を実現するための基本技術は情報通信システム関連技術全般にわたるが，大きく分けて5つのカテゴリに分類することができる．

- ネットワーク技術
- オンライントランザクション技術
- データベース技術
- セキュリティ技術
- プレゼンテーション技術

いずれも必要不可欠な技術であるが，とくに最近のECの実用化に大きく寄与したのはネットワーク技術とセキュリティ技術とプレゼンテーション技術である．

ネットワーク技術はいうまでもなくインターネット/イントラネットの普及にみられる通信インフラの整備である．これにより，企業ユーザのみならず，個人ユーザにまで手軽なネットワークアクセスが可能となり，経済活動としてのECにお

ける購入層が形成された．

次にセキュリティ技術であるが．共通鍵暗号，公開鍵暗号，ハッシュ関数といった**暗号化技術**が計算機能力の向上にともない実用的になったため，これらを組み合わせて使えば，単なる秘匿のほかに，データの非改竄証明と通信の相手認証が可能となった．ECでは必然的に金銭価値情報の移動をともなうので，不正防止のためには，

- ●通信相手の正当性の確認（相手認証）
- ●受信した情報の正当性の確認（非改竄証明）
- ●当事者以外への情報漏洩の防止（秘匿）

が必要条件である．暗号技術はこれに解を与えるものである．ECで安全な商取引を行うために**電子決済**や**電子認証**といった技術があり，この中で暗号技術を中心としたセキュリティ技術が駆使されている．

最後にプレゼンテーション技術であるが，これは**Web技術**に代表されるGUIを駆使したマルチメディア技術である．テキスト，静止画，動画，音声などを組み合わせたマルチメディア検索ソフトウェアであるWebブラウザは操作性のよさと多彩な表現力で，インターネットアクセスを身近なものにし，ECにおけるクライアントソフトウェアのプラットフォームとなりつつある．このWeb技術とデータベース技術やオンライントランザクション技術を組み合わせて**電子モール**が構築できる．

3. ECの要素技術

前述した要素技術の中でもECにとってとくに重要な技術について紹介する．

3.1 Webとそのプロトコル

Webサーバは一種の情報公開サーバで，中のデータはHTMLというフォーマットで記述されたマルチメディア情報である．このマルチメディア情報の閲覧にはブラウザと呼ばれるクライアントソフトウェアを使う．Webサーバとブラウザとの間はHTTPというプロトコルで接続する．ブラウザはGUIを駆使しており，マルチメディア情報の閲覧端末として非常に表現力が豊かでかつ操作性がよい．これはプレゼンテーション技術の1つの集大成である．このユーザインタフェースのよさがインターネットの爆発的な普及に貢献している．ECではこのWeb（サーバとブラウザ）を利用して消費者側の端末や商店側のサーバを構築するのが一般的となっている．

ただ，Webで使われているHTTPプロトコルはTCP/IP上のプロトコルであるがセキュリティ的機能がほとんどない．そこで，TCP/IPの層にセキュリティ機能をもたせたSSLやHTTP自身にセキュリティ機能を拡張したS-HTTPといったプロトコルが生まれてきた．さらにHTTPを単なるデータ転送プロトコルとして使い，その上位層でセキュリティを保つ方式もある．最近話題になっているクレジットカード決済プロトコルであるSETではIITTPをデータ転送プロトコルとして使っている例が多い．

3.2 暗号化技術

暗号化技術はECのセキュリティを支える要の技術である．現代暗号のアルゴリズムは大きく分けて共通鍵（対称鍵）暗号方式，公開鍵（非対称鍵）暗号方式，ハッシュ関数の3種類に分類できる．

（1）共通鍵暗号方式：

共通鍵暗号方式はデータを暗号化するときと復号するときと同一の鍵を使う方式である．鍵は40ビット～256ビットぐらいのものが利用されている．高速処理に向いており，ハードウェアで実装したものは400 Mbpsくらいの暗号化処理能力をもつものもある．この方式は情報の発信者と受信者との間であらかじめ鍵を第三者に知られることなく共有しておかなければならないという条件があり，安全な鍵の配送にはほかの方法を用いる必要がある．一般に共通鍵暗号方式のセキュリティは鍵の保護がどれくらい万全であるかに依存している．暗号強度の1つの目安として鍵の長さ（ビット数）で論じられることが多い．これは暗号解読の手法に「力ずく法（鍵総あたり法）」というのがあって，鍵のビット数が長ければ，解読に時間がかかるからである．米国政府の暗号製品輸出規制の目安の1つにこの共通鍵のビット数があって，ビット数の長いものは輸出許可をとるのが困難である．このほかにもより効率的な解読手法として，「差分解読法」や「線形解読法」が提案されている．共通鍵暗号方式で最も有名なのがDESである．DESの共通鍵は56ビットであるが，最近のCPUの処理能力をもってすれば，DESは実用的な時間内で解読可能になりつつあ

る．このほかの共通鍵暗号方式で代表的なものとしてはRC 5，FEAL，MISTY などがある．

(2)公開鍵暗号方式：

公開鍵暗号方式はデータを暗号化するときと復号するときとで異なる鍵を使う方式である．片方の鍵を公開し，もう片方の鍵は秘密にしておくのでこの名前がある．この方式のアイディアは比較的新しく1976年にDiffieとHellmanらによって発表された．そして1978年には実用的なアルゴリズムとしてRSAが発表されている．RSA暗号は現在は公開鍵暗号方式のデファクトスタンダードの地位を固めている．

公開鍵暗号方式のおかげで暗号はデータの秘匿目的以外に電子署名や相手認証が可能となり，応用分野が大きく広がった．欠点としては計算処理量が非常に多いことで，共通鍵暗号方式に比べて約千倍の計算量が必要といわれている．

このほかの公開鍵方式としてはElGamal暗号などが提唱されている．また次世代の公開鍵暗号方式として最近は楕円暗号方式が脚光を浴びている．

(3)ハッシュ関数

ハッシュ関数は入力データをある一定サイズのランダム性の高いデータに変換する一方向性関数である．一方向性であるから復号はできない．代表的なアルゴリズムとしてMD 2，MD 5，SHAなどがある．通常，送信したい原データ（電文）からメッセージダイジェストと呼ばれるコンパクトで一定サイズのデータを生成するときにこのハッシュ関数を用いる．

この共通鍵暗号方式，公開鍵暗号方式，ハッシュ関数を組み合わせて使うことにより，ECで必須要件の秘匿，相手認証，非改竄証明などが可能となった．3種の方式をどのように組み合わせてこれらを実現するかの原理については本特集「5. ECの技術動向：セキュリティ技術」に譲る．

3.3 電子モール構築技術

電子モールはECの中でバーチャルショップを開設するプラットフォームである．これはデータベース，Webサーバ，決済処理ソフトウェアを組み合わせて構築される一種のオンライントランザクションサーバである．Webサーバに掲載するHTMLコンテンツの作成にはデザイン的要素が強く，専門のデザイナがコンテンツ作成ツール

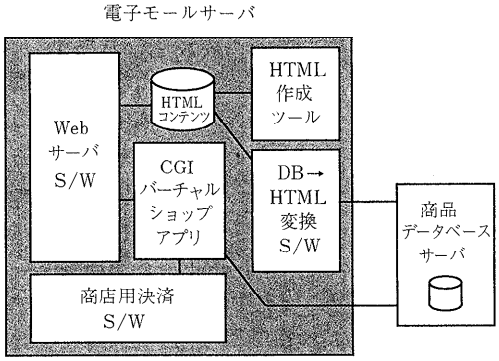

図-1 電子モール構成例

を用いて作成することが多い．ほかに，データベース内のデータからHTMLデータを自動生成する変換ソフトウェアもあり，デザイナが作成するコンテンツと自動生成されるコンテンツを組み合わせて美麗で機能的なバーチャルショップが構築できる．コンテンツの作成技術に関しては本特集「6. ECの技術動向：デジタルコンテンツ作成流通技術」に譲る．電子モールの構築は個別のアプリケーション開発的色彩が強く，一般論的には論じにくいが，一例として図-1に示すような構成がとれる．消費者側の端末からはWebサーバにアクセスして商品情報を閲覧し，消費者側の決済ソフトウェアと呼応して動く商店用決済ソフトウェアが決済サーバと連携して電子決済を行う．

3.4 電子決済技術

現在提案されている電子決済技術は現実の経済活動で利用されている決済方式のいずれかをモデルとしている．これらに共通する特徴をひと口でいうと「電子署名つきの金銭価値情報」ということができる．

主な電子決済方式として電子現金決済，電子プリペイド型決済，電子個人小切手決済，デビットカード決済，銀行決済（銀行POS），クレジットカード決済などがある．また，それぞれの決済方式は

- 通用範囲（オープンループ/クローズドループ）
- 匿名性（あり/なし）
- 商取引形態（先払い/即時払い/後払い）
- 実現形態（ストアードバリュー型/ネットワーク型）

という分類で特徴づけられる．この中で通用範囲

の分類であるクローズドループとは発行主体→利用者→販売者→発行主体というように価値の還流がクローズであることをいっている．これに対しオープンループとは金額価値情報が，発行主体→利用者→販売者→ほかの利用者→…というように流通し，発行主体に戻ってくることなく実際の現金と同様に誰にでもどこでも通用することである．

(1)電子現金決済

電子現金の大きな特徴は匿名性ということと，オープンループ性である．ほかの決済方式はいずれも匿名性なしかつクローズドループであるので，この2つの特徴が電子現金の定義といってもよい．

現在提案されている電子現金はMONDEXに代表されるICカードを使ったストアードバリュー型電子現金とデジキャッシュ社のE-cashに代表されるネットワーク型電子現金の2つの方式がある．いずれも即時払い形式であり，電子現金と現実世界の現金との交換は銀行で行う．

前者のストアードバリュー型電子現金は価値のコピー防止などのセキュリティ基盤をICカード等のハードウェアにおいている．利用者は銀行から現金を引き出して財布に入れて使うのと同様の感覚で銀行から自分のICカードに価値情報を充塡して使う．ICカード内の価値情報は銀行を介さず，利用者間での交換（すなわち決済）も可能である．このICカード内の価値情報の交換は現実の商店や銀行でも可能だし，インターネットのようなネットワークを介しても可能となる予定である．

後者のネットワーク型電子現金では消費者と商店は銀行とネットワーク接続しながら利用者間決済を行うのを前提としている．価値情報は利用者や商店のコンピュータ上にコピー可能なデータとして保存されている．価値情報の二重使用防止にはブラインドシグニチャーという技術が用いられる．ただし利用者がコンピュータ上にもっている価値情報が他人に無断でコピーされて先に使われてしまうと，現金が盗まれたのと同様の結果となり，正当な利用者はもはやその価値情報（電子現金）を使うことができなくなる．

(2)電子プリペイドカード決済

電子プリペイドカード決済は読んで字のごとく先払い型決済である．これはとくに小額決済に向いている．利用者はあらかじめ何らかの方法でプリペイドカード価値情報を購入しておく．そして商店での購入のたびにプリペイド価値情報を小出しに使っていく．この方式は利用範囲がプリペイド価値情報を発行する特定の商店やグループに限定されるクローズドループ型である．利用範囲が限られているため相互運用性の要件は低く，技術的にも法律的にも問題が少ない．プリペイドカード型決済にもストアードバリュー型とネットワーク型がある．ストアードバリュー型の代表的なものにVISAキャッシュがある．ネットワーク型の場合は利用者のプリペイド価値情報を決済サーバ上に保存しておく形態が多い．

(3)電子個人小切手決済

個人小切手は日本ではあまり一般的ではないが米国では広く利用されている．紙の小切手を電子的な小切手に置き換え，小切手帳も電子化し，暗号化技術に基づく電子署名を実際の署名の代わりに使うというものである．価値情報の発行者は利用者自身で，後日利用者の銀行口座から現金が引き落とされる．したがって特徴はクローズドループ型，匿名性なし，後払い型，ネットワーク型となる．主に米国のFSTC（Financial Service Technology Consortium）で検討されている．

(4)デビットカード決済

英国で始められた制度で，利用の数日後に利用者の口座から代金が自動的に引き落とされる．電子小切手とクレジットカード決済を合わせたようなイメージである．技術的な特徴は電子小切手と同様，クローズドループ型，匿名性なし，後払い型，ネットワーク型となる．ICカードなどを店舗に設置してあるPOS端末で使うのが前提．

(5)銀行（銀行POS）決済

デビットカードと似た仕組みであるが，利用者の銀行口座からの即時払いのところが異なる．クローズドループ型，匿名性なし，即時払い型，ネットワーク型となる．これもICカードなどを店舗に設置してあるPOS端末で使うのが前提．消費者のPCなどからインターネットを使って接続する方式はまだない．

(6)クレジットカード決済

ECにおけるクレジットカード決済の特徴はクローズドループ型，匿名性なし，後払い型，ネッ

トワーク型である．これは消費者側からみた場合，電子小切手やデビットカードと似ている．しかしこれらとは異なり，クレジットカード決済は全世界的に普及している．また，不正や事故発生時のリスク管理体制も整っているし，法制度上の問題点も少ない．今，ECの世界ではストアードバリュー型電子現金とならんでもっとも実用化に力が入っている方式である．

EC用のクレジットカード決済方式としてVISAとMASTERが提唱するSETがある．SETは昨年2月，5月，8月とドラフト版の仕様が出され，今年5月末に正式版としてVer.1.0の仕様が公開された．現在世界中でSETの開発や実験運用が実施されており，電子決済の中ではもっとも広く普及する方式と思われる．SETは消費者のもつPCからインターネットを介して仮想商店へアクセスすることを前提としたアプリケーション層プロトコルである．暗号技術としては現在はDESとRSAを使っている．

3.5 電子認証技術

ECにおける認証技術とは次の3つの要件を満たす技術である．

- 通信相手が確かに自称どおり本物であって偽者でないことを確認できること．
- 通信内容が途中で改竄されていないことを確認できること．
- その通信相手の信用力を確認できること．

最初の要件である相手が本物であるという確認は従来ユーザIDとパスワードを通信して行うのが普通であった．しかしECでは公開鍵暗号方式の原理を用いて行う．これは，受信者の受け取ったデータが発信者の公開鍵で正しく復号できれば，そのデータは発信者だけがもっているはずの秘密鍵で暗号化されたものなので，確かに発信者は偽者でないとみなせる，という原理に基づいている．なお，ECでもユーザID+パスワードによる相手確認も補助的には使われている．

次の要件である，通信内容の非改竄証明もまた公開鍵暗号方式の原理を用いる．これは送信するデータをハッシュ関数にかけ，メッセージダイジェストを生成し，これを発信者の秘密鍵で暗号化することによって行う．これを一般に電子署名という．データとそれに添付した電子署名を受け取った受信者は，発信者の公開鍵で電子署名を復号して得たメッセージダイジェストと，受け取ったデータから直接生成したメッセージダイジェストとを比較し，両者が一致していれば受け取ったデータは途中で改竄されていないと確認できる．

最後の要件である通信相手の信用力の確認とはECが商取引を前提としているだけに，経済的，社会的信用の確認のことを指している．この信用力は技術だけでは保証することはできず，ネットワーク上のバーチャル世界で確認した信用力を実世界上の社会的，経済的信用力に結びつける枠組みが必要となってくる．この枠組みが認証書と認証局という概念である．この枠組みと認証書のフォーマットを規定したのがITU-TのX.509という勧告である．この規約により，ECの相互運用の条件が整ったといえる．

認証書はECの利用者に対してあらかじめ認証局が発行する電子的証明書である．この認証書には利用者のIDや各種属性と，利用者の公開鍵，それにこの認証書の発行機関である認証局の署名が入っている．認証局は認証書を発行するときに，発行する相手の社会的，経済的信用力を確認する．そして，確かに認証局は証明書の発行相手の信用を確認して保証するという意味合いで，認証局自身の署名を証明書に入れ込んでおくのである．もちろん社会的，経済的信用のない相手に対しては，認証局は証明書を発行しないのが原則である．

ECの利用者である消費者や商店はそれぞれ自分の認証書の発行を認証局から受けている．電子商取引の現場では，取引相手の認証書を検証しあい，検証結果が正しければ，認証局があらかじめ信用調査を済ませて，相手の信用力を保証してくれているとみなす．

認証局は認証書の発行相手の社会的，経済的信用を保証するのであるから，認証局自身に信頼できる第三者機関としての社会的信用がなければならない．したがって認証局の運営主体は公的行政機関であったり，社会的信用のある複数の大企業が共同出資（または運営）する組織だったりする．

さらに認証局の信用を維持するためには運営上のセキュリティ要件を満たす必要がある．認証局の人的管理，組織的管理，物理的管理，技術的管理などのセキュリティポリシーを定め，これに基

づいた厳しい運営管理が必要である．なお，このセキュリティポリシーの枠組みはいろいろなところで検討されているが，まだ統一的なものには至っていない．

以上のものがすべてそろって，ECでのバーチャルな世界で確認した信用力が実世界での社会的，経済的信用力に結びつけられていることになる．

4. ECの要素技術と一般的組合せ

先に述べたようにECは現実世界の経済活動をモデルとした消費者，商店，決済センター（または銀行）のほかに，認証局を加えた4つの構成要素でとらえることができる．電子決済の方式にはいくつかのバリエーションがあり，一元的にはいえないが，大まかな動きは以下のようになりうる．

認証局はECの参加者（この場合は消費者，商店，決済センター）の社会的，経済的な信用確認をあらかじめ行って，認証書を発行しておく．消費者はインターネット経由で商店を訪れ，Webで商品情報の閲覧を行う．気に入った商品があれば，認証書で互いに相手の真正性と信用を確認しあった後，決済処理を行う．決済処理は決済の種類によって流れが異なるが，たとえば，MONDEXのような電子現金の場合，消費者と商店間の二者間決済となり，クレジットカード決済であるSETプロトコルでは消費者と商店と決済センターの三者間決済となる．なお，認証書による相手確認は決済処理の中で自動的に行われることが多い（図-2参照）．

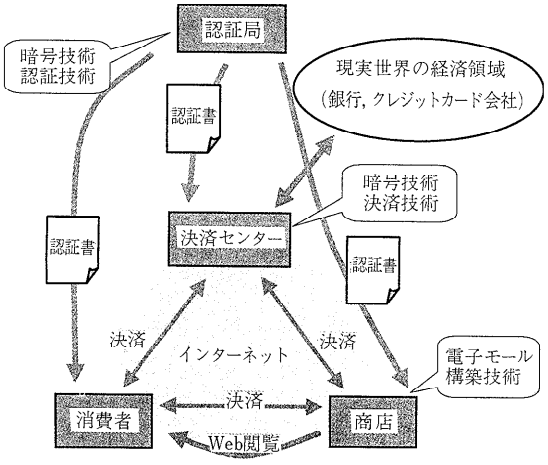

図-2 ECの構成例

5. おわりに

ネットワーク技術，セキュリティ技術，プレゼンテーション技術など，さまざまな分野の技術がそれぞれ熱心な研究者たちの手により独自にあるいは連携しながら発展/成熟してきた．ECはそれらさまざまな技術を要素として使い，新たな技術領域と経済領域を形成するシステム技術である．またECは社会制度に密接に連携したシステム技術のため，その意味で究極の形態というのはありえない．よってECを支える要素技術もまた社会的要請に合わせてますます広範なものになっていくと思われる．本稿で紹介した要素技術はごく一部でしかも紙面の関係上表面的な説明に止まったが，ほかにも多くの研究者に支えられた多様な要素技術があることを明記しておく．

参考文献

1) 山川 裕：エレクトロニックコマース革命，日経BP社 (1996).
2) (財)流通システム開発センター：欧州電子マネーシステム調査団報告書 (1996).
3) (社)日本電子工業振興会：電子決済システムの動向に関する調査報告書 (1997).
4) 辻井重雄，笠原正雄：暗号と情報セキュリティ，昭晃堂 (1990).
5) 池野信一，小山謙二：現代暗号理論，電子情報通信学会.
6) 松井 充：ブロック暗号アルゴリズムMISTY，電子情報通信学会信学技報 TECHNICAL REPORT OF IEICE ISEC 96-11 (July 1996).
7) VISA, MASTER: Secure Electronic Transaction (SET) Specification Book 1, 2, 3 (May 1997).

(平成9年7月1日受付)

檜山 秀郎

1984年東京大学大学院工学系研究科修士課程修了．同年三菱電機(株)入社，1990年イリノイ州立大学コンピュータサイエンス学科卒業MS取得．現在三菱電機(株)情報技術総合研究所勤務．情報セキュリティシステムの開発に従事．