# EC／電子決済システムにおけるセキュリティの考えかた

**Security of Electronic Commerce/Electronic Payment Systems**

謝　偉利　SHA Willie
岩崎　孝夫　IWASAKI Takao

電子商取引(EC：Electronic Commerce)の発展にとって安全な電子決済システムは不可欠である。しかし，電子決済システムはいくら安全でも，コストと使い勝手に問題があるとユーザーには受け入れられない。初期のSET Secure Electronic Transaction(注1)はまさにこういうシステムである。ICカードと組み合わせることやサーバ型Wallet(注2)を導入することによってSETの利便性を高めることができる。このような新たな取組みは初期のSETのセキュリティを補完する面もあるが，一方では新たなセキュリティの問題を発生する。これらの問題はビジネス的，技術的な進歩によって将来には解決されるであろう。

Secure electronic payment systems are indispensable to the development of electronic commerce (EC). However, a secure electronic payment system will not be widely accepted by users if its cost is high and it is difficult to use. The initial stage of Set Secure Electronic Transaction systems has such characteristics. Integrating SET with an IC card and introducing a server-based Wallet can improve the ease of use of SET. These measures can also improve the security of SET in some aspects, but may introduce another level of security problems. These problems will be resolved with enhancements in both business practices and technologies in the future.

## 1 まえがき

昨今，先進各国においてインターネット上での商取引は爆発的に伸びており，ECは導入段階からいよいよ本格的な成長段階に入りつつある。一方，安全な電子決済方式はECの発展にとって不可欠だとされてきたが，その代表格であり事実上の標準(DFS：De Facto Standard)と目されているSETの普及が今一つ進まない。現在のSETのしくみは安全性を重視するあまり，カード会員である消費者(以下，利用者と呼ぶ)や電子商店にとって手間や負担が掛かり，実用的でないという問題がある。実ビジネスにおいては，SETより簡便なSSL(Secure Socket Layer)をベースとしたクレジットカード決済をはじめ，従来のカタログ通販の決済方式が依然主流を占めている。しかし，これらの安易な決済方式は不正などを招きやすく，問題の兆しが最近徐々に現れてきた。VISA International(以下，VISAと略記)によると，インターネット関連のクレジットカード決済は全カード決済の総利用件数のわずか1%程度しか占めないにもかかわらず，トラブルの発生件数は全体の50%近い比率を占めるようになった。今後，EC市場の拡大に伴い，詐欺グループやハッカー(注3)などによる不正は増加すると予想され，安全でかつ実用的な電子決済方式に対するニーズは確実に高まってくる。

当社は，安全な電子決済のインフラとして，SCJ(Smart Commerce Japan)プロジェクトにおいてSETをベースにICカードへの拡張版を開発し，利用者実験を行なった。今後はさらにサーバ型Walletの開発やオープンプラットフォームの採用などにより，SETの実用化を目ざす。ここではSETのセキュリティの考えかた，SETの実用化の課題，当社の実績と今後の取組みについて述べる。

## 2 SETのセキュリティの考えかた

SETはRSA(注4)の公開鍵(かぎ)暗号方式とDES(Data Encryption Standard)の秘密鍵暗号方式を組み合わせ，認証，暗号化，電子署名などの技術を応用し，決済の当事者の認証，決済情報の機密性，決済情報の完全性を実現することを目的としている。

SETのセキュリティの考えかたは，SSLと対比させると理解しやすい。SSLは今日のECにおいて決済の安全性を高める目的で普遍的に使用されていて，いわゆるセッションレベルのセキュリティを提供している。電子商店のサーバと利用者のブラウザ(注5)間でセッション(接続)がいったん確立されると，すべての通信は暗号化されるが，利用者から商店に送ったデータは商店で復号化され，データの

(注1) VISAとMasterCardが発表したインターネット上でクレジットカードを使って安全に決済を行うための総合的な統一規格。
(注2) 消費者が使用するソフトウェアを通称Walletと呼び，主要な機能をサーバ側で実行するWalletのこと。
(注3) コンピュータ ネットワーク上に無断に侵入し，さまざまな犯罪行為に及ぶ知能犯。
(注4) 公開鍵暗号方式を採用した暗号化アルゴリズムの一つ。
(注5) ファイルのデータを次々と見ていくためのソフトウェア。

管理は商店にゆだねられる。利用者は商店がデータを保護してくれることを信頼するしかない。また，商店にとってのリスクは，利用者が本物のカード所有者だという確証がなく，クレジットの支払いを受けられる保証が何もない。オンラインで配信されるソフトウェアグッズの販売の場合は物証が残らないために特にリスクが大きい。

SSLのセキュリティは，当事者である電子商店と利用者がともに善意の者であることを前提としている。それに対して，SETは当事者が悪意の者である可能性もあるという前提でセキュリティを保証する。この考えかたの違いにより，SETはSSLに比べて以下のような特長をもつ。

(1) SSLは二者間プロトコルであるのに対し，SETは電子商店と利用者間に金融機関を加えた三者間プロトコルである。金融機関の決済ゲートウェイを加えることによって，インターネットと従来の決済ネットワークをオンラインで結び，利用者端末から金融機関のホストまでスルーして決済データの安全性を保証する。SETの論理構成を図1に示す。

(2) SSLは，電子商店が特定な認証局が発行した認証書を保持する正当な法人であることを認証するだけで，カードを扱える正当な加盟店であることを保証しない。SETは，決済の当事者がすべて本物の有資格者であるということを保証する。SETはこれを実現するしくみとして信用の階層構造とそれに伴う一連の運用ルールで保証する。SETの信用の階層構造を図2に示す。

(3) SSLは決済情報を当事者以外に対して秘匿する。SETは，決済情報を当事者以外に対してだけでなく，当事者間でも必要に応じてデータを秘匿する。例えば，利用者のカード番号を電子商店経由で金融機関に送るが，カード番号を電子商店に対して秘匿したほうが安全である。SETはカード番号を含むPI(支払い情報)は金融機関の決済ゲートウェイの鍵で暗号化され，金融機関だけが復号できるしくみになっている。

(4) SSLは決済情報を当事者以外による改ざんから守る。SETは決済情報を当事者以外による改ざんから守るだけでなく，当事者自身が合意した決済データを片方が途中で勝手に改ざんできないことを保証する。SETはこのためにデュアル署名という電子署名の方式を導入し，利用者と電子商店の双方で作成されたPIとOI(注文情報)を割り印署名することにより，利用者と電子商店のいずれかによる改ざんを防止する。

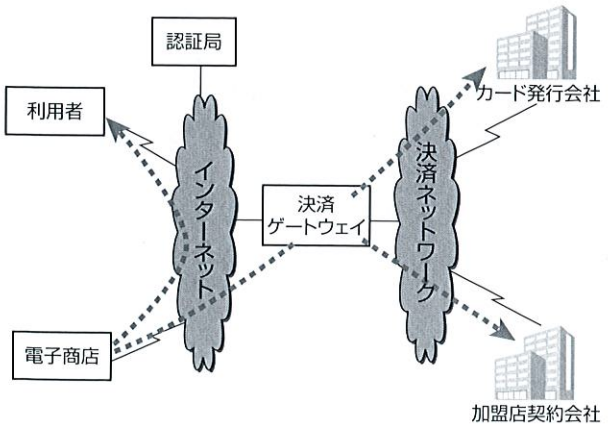


図1．SET論理構成図　SETは，オープンなネットワーク上で安全に決済を行うためのプロトコルである。
Conceptual diagram of SET

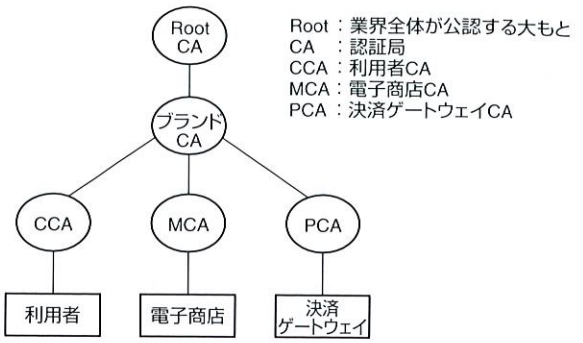


図2．信用の階層構造　業界全体が公認するRootが信用の根元となり，下位階層の信用を連鎖的に保証する。
Hierarchy of trust

## 3 SETの意義

今日のカードの約款では，カードの支払いに本人の署名がない場合，本人による利用否認が金融機関に持ち込まれると，商店はチャージバック(注6)される。つまり，SSLによるカード決済では，係争時には電子商店がその支払いを負う可能性が高い。これに対してSETが普及してくると，決済の当事者にとって以下のようなメリットがある。

(1) 電子商店による水増し請求，架空請求などの不正を防止できる。

(2) 利用者による偽りの利用否認を防止できる。

SET取引きを規定するカード約款では，SETの電子署名は実署名と同様に見なされ，商店が直ちにチャージバックされることがなくなる。それ以上に，SETのもつ重要な意義は係争の発生をほとんど未然に防ぐことができることである。

(注6) カード会員から請求に対してクレームがあった場合，カード会員の金融機関が調査したうえで，商店に非が認められた場合にカード会員の金融機関が商店の金融機関に対して返金を請求する行為。

## 4 当社の取組み

当社は95年度の通商産業省EC推進事業の一環で，VISAと共同でSCJというコンソーシアム(協会)を設立し，一般商店であるリアルモールとインターネット上の仮想店舗であるバーチャルモールで共通に使えるICカードによる決済の実証実験を推進した。バーチャルモールの決済手段として，SETとこれをさらにICカードに拡張したシステムを開発し，世界で初めてICカードを使ったSETの実験を行なった。図3にSCJバーチャルモール実験の構成を示す。

当社はSETがまだSEPPやSTTと呼ばれていたころから，ICカードとSETとの組合せによるメリットに着目し，取組みを始めた。そのメリットとは以下のとおりである。

(1) ポータビリティ　ICカードさえもっていれば，自宅のパソコン(PC)や街頭のキオスク端末などを利用して決済を行える。

(2) カード存在証明　カード発行元が，利用者がICカードを持っており，それが偽造されたものではないことを確認できる。

(3) カードホルダ関与証明　カード発行元が，カードホルダが利用していることを，確認できる。

また，実験をとおしてわかったメリットとして

(4) カードホルダへの利便性向上　純粋のSETの実験では，カードホルダが自身の認証書取得の手続きに手間がかかり，それを煩わしいと感じており，また，その際のトラブルが一番多かったがそれらを解決できた。

(5) 運用コストの削減　例えば，上記手間が省けるためユーザーサポート業務を軽減できる，などが挙げられる。

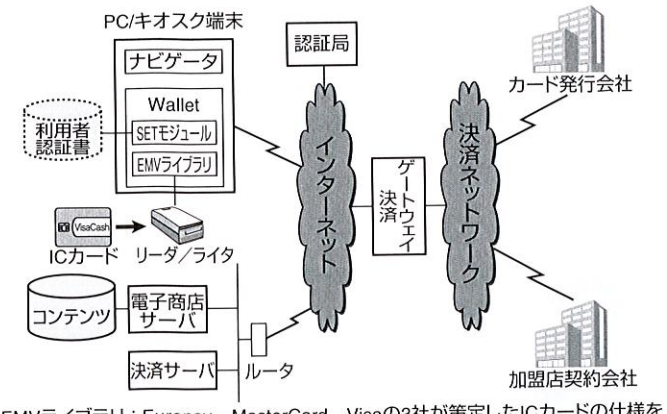


図3．SCJバーチャルモール実験構成図　SCJのバーチャルモール実験では，利用者がICカードを使ってインターネット上でSETによる決済を行う。

SCJ Virtual Mall Pilot

それでは，どのようなしくみによってこれらのメリットが生じるのであろうか。SETの推進機関であるSETCo(SET Secure Electronic Transaction LLC)(注7)に提案されているICカードとSETの組合せはいくつかのバリエーションがあるが，当社が注力するしくみは，①ICカードにSETの認証書と電子署名機能をもたせること，②既存のICカード型クレジットカードをそのまま使う，という2種類である。前者は，SETの認証書と鍵の安全な保管庫としてICカードを用いるという方式である。そして，カードホルダの秘密鍵を必要とする処理をカードで処理する。後者は，SETの電子署名の替わりに，既存のICカード型クレジットカードの署名機能を利用するという方式である。

これらのいずれの方式でも，ポータビリティと安全性(秘密鍵を盗まれない)を両立できる。そして，そのICカードしか生成できないデータの照合によるカード存在証明と，カード利用時の暗証番号確認によるカードホルダ関与証明を実現できる。さらに，方法②の場合は，既存のIC型のクレジットカードをそのまま使えるという意味で，ビジネス上でのメリットも大きい。

## 5 現在のSETの課題

従来型SET構成の問題点は，以下のとおりである。

(1) 利用者の端末にプログラム(図3のWallet)をインストールする必要があり，利用者の利便性を損なうだけではなく，運用者側の負担も大きい。

(2) このプログラムが数Mバイトにも及び，作成・配布コストが掛かる。いくらCD-ROMが安価になったとはいえ，全カードホルダに配るにはかなりのコストアップとなる。

(3) 新しい技術・規格に対応するためのアップグレードをするたびに，上記(1)，(2)の問題が生ずる。

(4) SET Wallet(通常型のWallet)の処理が重く，利用者の環境によっては動作が困難な場合がある。

## 6 Thin Wallet

Thin Walletとは，従来型SET構成の問題点を克服するために考案されたサーバ型Walletアーキテクチャである。図4にこのアーキテクチャを示す。SETの処理自体はWallet機能をもたせたサーバで行い，クライアントにはグラフィカルユーザーインタフェース(GUI)を中心とした機能だけを置くという構成が考え出された。さらに，こ

(注7) VisaとMasterCardが共同で設立したSETの発展を推進するための組織で，通常“セットコ”と呼ばれる。

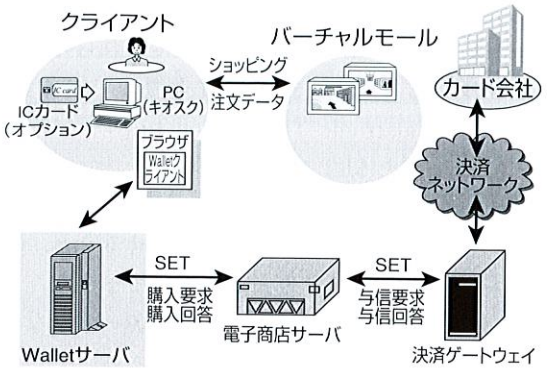


図4．サーバ型Walletアーキテクチャ　従来型のWalletをクライアントとサーバに分割し，クライアントのWalletを軽くすることにより利用者とカード会社の負担の軽減を図る。
Server-based Wallet architecture

のWalletをHTML(Hyper Text Mark-up Language)やJava(注8)といったダウンローダブル(注9)なモジュールだけで構成すると，利用者の環境としてWebブラウザのような標準的な環境さえ整っていれば，SET決済を利用することができるのである。また，利用者の環境としてPCだけではなく，ケーブルテレビや衛星放送のSTB(Set Top Box)(注10)などでも，インターネットへのアクセス機能をもつ環境でも利用可能となってくる。

同時に，Wallet機能をもたせたサーバで，カードホルダの認証書などの管理を一元的に行うことにより，利用者は認証書の取得といった作業から解放される。そしてそれは運用者側のメリットにもつながる。

## 7 新たなる課題

必然的にICカードとサーバ型Walletを結び付けたアーキテクチャが考えられる。それが当社の推す安全な電子決済が普及するためのSETのアーキテクチャである。しかし，ここにいくつかのセキュリティ上の課題が存在する。それを以下に示す。

(1) ICカードをアクセスするためには，ローカルリソースのアクセス権が必要となる。例えば，WalletをJavaで記述した場合，ローカルリソースへのアクセス権を得るために署名付きアプレット(注11)にする必要がある。しかし，誰の署名を施せば良いのであろうか。そして，利用者はその署名者を本当に信じてよいのだろうか。現在Javaアプレットの署名は，SETにおける認証書の階層構造とは独立に存在するため，トラブル発生時の保証などの枠組みを別途検討する必要がある。

(2) WalletとWalletサーバの間の通信は，安全性のためにSSLを用いる。しかし，どんなに強力なSSLを用いても，通信相手が正しいWalletサーバ(悪影響を与えないサーバ)かどうか知る手段がない。わかっているのは相手が，どこかの認証局が発行した認証書をもっており，その範囲での会社プロフィールがわかるだけである。前項と同様に，SSLの認証書はSETにおける認証書の階層構造とは独立に存在するため，トラブル発生時の保証などの枠組みを別途検討する必要がある。

これらの課題の根本的な問題点は信用である。これに対してどんな解が考えられるだろうか。一つには，アプレットの署名者やSSLの認証書をSETの信用階層の枠組みに組み込むこと。そうすれば，SETの枠組みにおいて信用できる署名付きアプレットや，信用できる認証書をもったWalletサーバになり，これらの課題は一気に解決可能であろう。事実，Walletサーバ構成についてはSETの推進機関であるSETCoにおいても議論が活発になってきており，これらの課題がクリアになる日も近いと想像している。

## 8 あとがき

当社は，SCJ(パート1)の経験をベースに，ICカードとSETを組み合わせた電子決済システムの実用化を目ざし，利用者にとって使いやすい商品とサービスを提供していく計画である。現在，新たなプロジェクトとしてSCJパート2を計画しており，SET WalletのThinクライアント化(Thin Wallet)，ICカード・インタフェースの汎(はん)用化，クライアント側ソフトウェアのJava化を行なっていく予定である。Walletの事前インストレーション(ソフトウェアのインストール)と認証書取得作業が不要となり，STB, NC(Network Computer)，移動電話などのようなデバイスからもWalletの利用が可能となる。利用者にとって，いつでも，どこでもSETを利用できる環境を実現していきたい。

(注8) Javaは，SunMicrosystems社の商標。
(注9) ネットワーク上のサーバから手元のPCへソフトウェアを書き込むこと。
(注10) テレビにCATV(有線テレビ)やインターネットを接続するための装置。
(注11) ほかのソフトウェアの中で動作する各種ソフトウェア。



謝　偉利　SHA Willie
情報・社会システム社 流通・放送・金融システム事業部 マーケティング事業推進担当主務。EC事業推進に従事。
Distributing, Broadcasting & Banking Systems Div.


岩崎　孝夫　IWASAKI Takao
デジタルメディア機器社 青梅工場 コンピュータソフトウェア設計部主務。ECシステム開発，Java Card開発に従事。情報処理学会，電子情報通信学会会員。
Ome Operations