

# Infomerce SET/OPEソリューション

## Infomerce SET/OPE Solution

山下 修  
Osamu Yamashita

西田 美穂  
Miho Nishida

山崎 真司  
Shinji Yamazaki

宝生 真行  
Masayuki Hojo

### 要 旨

インターネット上の電子商取引におけるクレジットカード/銀行口座を使った即時決済のための世界標準仕様として、SET/OPEが作成された。Infomerce SET/OPEソリューションは、SET準拠であり、また、SET/OPE決済の導入を容易にするサーバ管理型という特徴を持つ日本で唯一のインターネット決済ソリューションである。

#### 1. ま え が き

国内でインターネット利用の世帯普及率が15%を超え、今後、通信料金の定額化が進めばさらなる拡大があると見込まれている。このインターネット利用者を対象とする仮想店舗における商品販売やオンラインチケット予約をはじめとするさまざまな電子商取引市場も、すでに2000億円に迫ろうとしている。このような環境の中で、インターネット上で安全に即時決済するための統一された仕組みを、早期に確立する必要性が叫ばれている。

当社は、インターネット決済の世界標準であるSET<sup>\*1)</sup>/OPE (Secure Electronic Transaction/Online PIN Extensions) に準拠したInfomerce<sup>\*2)</sup> SET/OPEソリューションの提供により、金融機関、仮想店舗、カード利用者(以下、カードホルダ)による統一された即時決済の利用を可能にした。さらに、世界で唯一のサーバ管理型のSET決済システムを採用することにより、カードホルダの利便性を向上させるとともに、金融機関や仮想店舗によるインターネット決済の安価な導入/運用

を実現している。

本稿では、SET/OPE標準、当社の取り組み、ソリューションの特徴について述べる。

#### 2. SET/OPE標準

##### 2.1 技術動向

インターネット上の電子商取引において、従来からよく利用されていた決済方式は、請求書送付による代金の銀行振込であった。しかし、一般のインターネット利用者が使うWWW (World Wide Web) ブラウザがSSL (Secure Socket Layer) をサポートするようになってからは、インターネットでクレジットカード番号を送る方式が広まってきている。

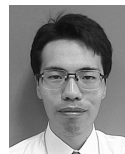
一方で、VISAやMasterCardなどのクレジットカード会社は、クレジットカード番号を送る方式では、本人のサイン(署名)がないことから本人確認ができず、クレジットカード番号が盗用される危険性を認識していた。そのため、本人確認を確実にでき、さらにインターネット上の通信による情報の漏洩や改ざんも防げる、安全で統一されたインターネット決済の策定を早



山下 修  
システムソリューションカンパニー ビジネスソリューション事業部ソリューション開発第二部開発第一チームサブチームリーダー



西田美穂  
システムソリューションカンパニー ビジネスソリューション事業部ソリューション開発第二部開発第一チーム



山崎真司  
システムソリューションカンパニー ビジネスソリューション事業部ソリューション開発第二部開発第一チーム



宝生真行  
システムソリューションカンパニー ビジネスソリューション事業部ソリューション開発第二部開発第一チームチームリーダー

\* 1) SETは、SETCoの商標である。

\* 2) Infomerceは、沖電気工業(株)の登録商標である。

期から行ない、その結果として、SET<sup>1)</sup>が1997年5月に発表された。

SETは、各国、各クレジットカード会社のビジネス要件を幅広くカバーしているが、当初は銀行口座によるインターネット決済は考慮していなかった。しかし、いくつかの先進的な銀行は、わずかな拡張でSETが銀行決済もカバーできることを示し、後に、銀行決済のための拡張仕様であるPBD (PIN-Based Debit) が作成された。PBDはすでにいくつかの金融機関で利用されているが、より広い用途に適用できるように仕様変更が行なわれ、銀行決済のための新仕様としてOPE<sup>2)</sup>が1999年春に発表された。以下では、PBDを含めてOPEと記述する。SET/OPEは、現在はその管理会社であるSET Secure Electronic Transaction LLC (以下、SETCo)で管理されている。SETCoはSET/OPEの仕様解釈、仕様拡張、認定試験などを行なっている。

日本国内でも、郵政省、主要な銀行やクレジットカード会社、ベンダが加盟している「日本インターネット決済推進協議会 (JIPPA)」において、SET/OPEはインターネット決済の標準仕様として採用されている。

## 2.2 SET/OPE決済の仕組み

本項では、SET/OPE決済において特徴的な技術と処理の概略を説明する。

### (1) セキュリティ、ビジネス要件と技術的特徴

SET/OPEは、既存のクレジットカード決済/銀行決済のビジネススキームやシステム資産をそのまま利用できるように考慮しつつ、インターネット上の通信プロトコルを規定している。インターネット上の通信は、一般に、情報の漏洩、改ざん、なりすましの危険性があるため、SETはこれらの危険性に対するさまざまな対策を組み込んでいる。以下、特徴的な技術要素を説明する。

#### 支払情報と注文情報の秘密保持 - 暗号化

SET/OPEで扱うデータのうち、支払情報は、クレジットカード番号/口座番号、有効期限、決済用の暗証番号(OPEのみ)、金額などを含み、カードホルダから金融機関に渡されるデータである。これは、SET/OPEにおいてもっとも安全に扱う必要のあるデータの1つである。この支払情報はカードホルダのもとで暗号化され、金融機関のもとでのみ復号可能になっている。この特徴により、支払情報はインターネット上の悪意ある第三者から守られるだけでなく、仮想店舗にも知られることはない。これによ

り、仮想店舗からクレジットカード番号が漏洩することはない。

注文情報は、金額や、支払情報との対応を取るためのIDなどを含み、カードホルダから仮想店舗に渡されるデータである。注文情報は、カードホルダのもとで暗号化され、仮想店舗のもとでのみ復号可能になっている。

#### 相互認証 - デジタル証明書

現実世界でのクレジットカードや銀行カードの利用においては、カードホルダからの「カードの提示」と「サイン」により本人確認ができるが、インターネット決済においてはそれができない。SET/OPEでは、「カードの提示」の代わりに、「デジタル証明書の提示」によりカードの所有を確認している。

デジタル証明書は、金融機関が指定した認証局からカードホルダに発行されるデータである。仮想店舗はカードホルダから提示されるデジタル証明書により、カードホルダがそのカードの正しい所有者であることを確認できる。

また、カードホルダだけでなく仮想店舗や金融機関、さらに認証局そのものもデジタル証明書を持つ必要があり、常にこのデジタル証明書により相互認証を行なう仕組みになっている。

#### 注文/支払の否認防止 - デジタル署名

インターネットでの電子商取引においても一般の商取引と同様、カードホルダからの「注文した」という事実、仮想店舗による「注文を受け付けた」という事実、金融機関による「決済を承認した(そのカード/口座での支払を許可した)」という事実を、相互に確実に確認しあうことが必要になる。SET/OPEでは、デジタル署名により相互に確認することになっている。

デジタル署名は、一般に有効性が認知されている暗号化方式に基づいて作成されるデータで、注文や決済時のデータにデジタル署名を付加することで、それぞれの事実を確実に確認しあうことが可能になっている。

#### 送信されるすべてのデータの保全 - 二重署名

前述のように、支払情報と注文情報はそれぞれ別々に暗号化されるため、両者の対応を保証する仕組みが必要である。SET/OPEでは、二重署名により、これを実現している。

二重署名により、カードホルダが支払情報のメッ

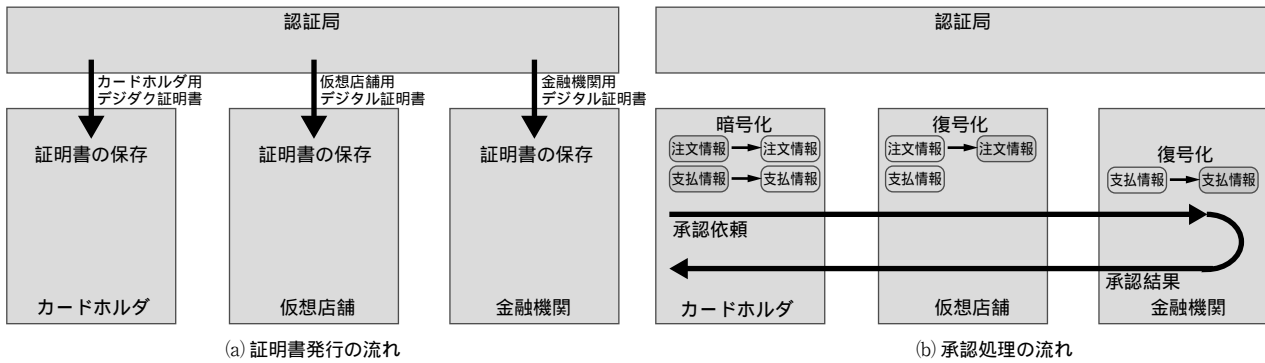


図1 認証局、カードホルダ、仮想店舗、金融機関の関係図  
 Fig. 1 Relationship of Certificate Authorities, Cardholders, Merchants and Financial Institutions

セージダイジェストと注文情報のメッセージダイジェストを連結させたデータの正当性を、仮想店舗や金融機関が検証できるようになっている。

(2) 証明書発行と決済の流れ

SET/OPEにおける各処理はそれぞれ業務と対応付けられており、証明書発行処理、承認処理、売上処理、返金処理、取消処理(承認取消、売上取消、返金取消)、バッチ処理の大きく6つの処理に分けられる。ここでは、SETの基本概念を示すために、証明書発行処理と承認処理を簡単に説明する。

図1の(a)に証明書発行処理の流れを示す。SET/OPEでは、相互認証のために、カードホルダ、仮想店舗、金融機関それぞれにデジタル証明書が必要となる。それぞれにデジタル証明書を発行するのが認証局である。カードホルダ、仮想店舗、金融機関は、決済に先立ち、認証局からデジタル証明書を取得する。取得したデジタル証明書は何度でも利用できるため、保存しておく。決済のたびに取得し直す必要はないが、デジタル証明書には有効期限が設定されている。そのため、有効期限が切れる前に更新処理を行ない、新たなデジタル証明書を取得し直す必要がある。

図1の(b)に承認処理の流れを示す。SET/OPE決済時にカードホルダは支払情報と注文情報を作成し、それぞれを暗号化した後、仮想店舗に送信する。仮想店舗は注文情報のみを復号し、データ内容や整合性を確認の後、カードホルダによって暗号化されたままの支払情報を金融機関に送信する。金融機関は支払情報を復号し、データが示すクレジットカード番号/銀行口座での支払を認めるかどうかを決定し、その結果を仮想店舗に送信する。仮想店舗は、その結果を受け取り、

記録に残すとともに、その結果をカードホルダに送信する。

3. 沖電気のインターネット決済への取り組み

3.1 最先端技術の導入

当社は、SET/OPEが発表された早期から、インターネット決済が世界規模で標準化されることを認識し、また世界的な動きに追随するために、SET/OPEに関して最先端技術を持つ米国GlobeSet社(以下、GlobeSet)の技術を導入することを決定し、アライアンスを結んだ。

GlobeSetは、SET/OPEの作成に当初から参加していた数少ないベンダの1社である。SET/OPE製品も早期から提供しており、SET準拠認定の証であるSETマークを、SET/OPEにおける4種類の製品(カードホルダ向け製品、仮想店舗向け製品、金融機関向け製品、認証局向け製品)すべてで最初に取得したベンダである。また、SETマーク基準が改定された2000年2月に、4種類の製品すべてがSETマークの基準製品として選ばれたわずか2社のうちの1社でもある。さらに、SET/OPEの普及を促進するサーバ管理型の製品を提供している世界唯一のベンダである。

3.2 国内市場への展開

当社は、GlobeSetとのアライアンスをもとに、国内市場へSET/OPEソリューションの展開を行なっている。

製品開発としては、日本市場向けにローカライゼーションを行ない、当社のインターネット仮想店舗ソリューションInfomerce Store/Infomerce Mallへ

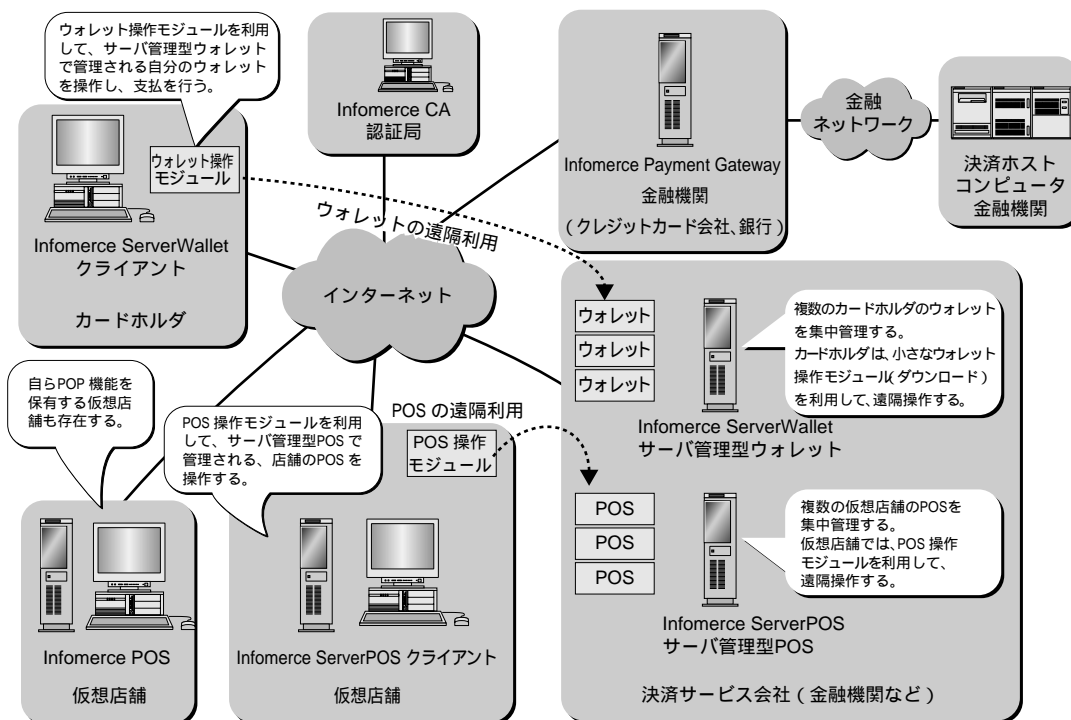


図2 Infomerce SET/OPEソリューション全体図  
Fig. 2 Infomerce SET/OPE solution overview

SET/OPE決済機能を追加した。

また、SET/OPEは、異なるベンダ製品との相互接続性が従来から大きな課題となっていることから、日本国内で有力な金融機関のSET/OPEシステムとの相互接続試験の実施、そのフィードバックのGlobeSetへの提供を通し、数多くの金融機関のSET/OPEシステムと相互接続性を確保してきた。現在、当社製品は、日本でもっとも相互接続性のある製品として認識されている。すでに、複数の仮想店舗で、SET/OPE決済用の製品として採用されており、郵便貯金、銀行、クレジットカード会社と接続しての運用に供されている。特に、2000年3月に開始された「郵貯インターネットホームサービスの実証実験」では、50%の仮想店舗で当社製品が採用されている。

また、1999年には、銀行、クレジットカード会社、モール事業者の協力のもとに、「サーバ管理型SET決済システムによる電子商取引実証実験」を当社主体で行なった。この実証実験では、すでに運用を開始しているSET/OPE決済システムと当社のサーバ管理型SET/OPE製品とを実際に接続して実証実験を行ない、既存システムとの相互接続性を確認するとともに、サー

バ管理型SET/OPE決済システムの有効性を確認した。この実証実験は、サーバ管理型SET/OPE決済システムとしては世界で最初の実証実験となっている。

#### 4. Infomerce SET/OPEソリューションの特徴

##### 4.1 Infomerce SET/OPE製品の特徴

図2にSET/OPE決済システムの全体図を示す。

当社のInfomerce SET/OPEソリューションのベースとなる製品は、カードホルダが利用するInfomerce ServerWallet、仮想店舗が利用するInfomerce ServerPOSおよびInfomerce POS、金融機関が利用するInfomerce Payment Gateway、認証局が利用するInfomerce CAの4種類5製品であり、Infomerce SET/OPEソリューションではSET/OPEで必要となる4種類すべての製品を提供している。また、これら5製品は、すべてSET準拠の認定を受けており、SETマークを取得した製品である。

Infomerce SET/OPE製品の最大の特徴は、日本国内で唯一のサーバ管理型のSET/OPE製品であるInfomerce ServerWalletとInfomerce ServerPOSにあ

る。Infomercer ServerWalletは、カードホルダが利用するサーバ管理型のSET/OPE製品である。従来の他社のSET/OPE製品では、カードホルダはウォレットと呼ばれるソフトウェアを金融機関からCD-ROMなどで入手し、自分のPCにインストールするなどの手間が必要であった。Infomercer ServerWalletでは、カードホルダは約50Kバイトのウォレット操作モジュールを、決済サービス会社が管理するサーバ管理型ウォレットからダウンロードするだけで済むようになっており、カードホルダの手間を大幅に軽減している。このことにより、金融機関はウォレットを配布するためにCD-ROMを配らなくて済むため、ウォレット配布コストが約10分の1で済み、さらに、カードホルダはインターネット上のどこからでも自分のウォレットを利用できるようになった。

Infomercer ServerPOSは、仮想店舗が利用するサーバ管理型のSET/OPE製品である。従来の他社のSET/OPE製品では、仮想店舗はPOSと呼ばれるソフトウェアの導入コストを負担しなければならず、さらに運用には専門知識の修得が必要であった。Infomercer ServerPOSでは、仮想店舗はPOS操作モジュールを入手するだけでよく、POSそのものは決済サービス会社が管理するサーバ管理型POSで管理/運用されるため、修得しなければならない知識の量が大幅に軽減されている。

また、Infomercer POSを除く4製品は、暗号処理や暗号鍵の管理を安全に行なうためのハードウェアセキュリティを利用することが可能になっている。ハードウェアセキュリティは、暗号鍵や署名鍵の生成や管理を行ない、暗号化、復号化、デジタル署名の作成など、SET/OPEで必要になるすべての暗号処理をハードウェア内部で処理する専用のハードウェアである。また、ハードウェアセキュリティは、自らが生成した暗号鍵そのものをハードウェアの外には取り出せないよう物理的なプロテクションがかけられているため、内部犯罪さえも防ぐ手段として利用可能になっている。

4.2 トータルソリューションを提供

表1 Infomercer SET/OPEソリューションサービス一覧  
Table 1 Infomercer SET/OPE solution services

サービス名	サービス概要
コンサルテーションサービス	顧客要件に基づいたシステム構成の選択 金融機関等の紹介、新規ビジネススキームの確立など
システム構築サービス	既存システムを利用した決済システム組み込みの開発サポートや、ネットワーク環境を含めたシステム全体の構築サービスなど
テスト環境利用サービス	顧客が導入したシステムの試験をサポートするための、テスト用証明書発行など
接続テスト実施サービス	システム稼動開始直前の、金融機関と実際に接続しての試験の、スケジュール調整から金融機関への報告書作成まで
アンサーリングサービス	問い合わせ対応、バージョンアップの連絡など

Infomercer SET/OPEソリューションは、単なるパッケージ製品の提供にとどまらず、導入、開発、テスト、サポートなど、各種のサービスを含めたトータルソリューションとなっている。以下では各サービスについて簡単に説明する。

(1) コンサルテーションサービス

SET/OPE決済を導入する顧客は、仮想店舗を運営する顧客なのか、決済サービスを運営する顧客なのかなどにより、システム構成の選択や導入までのスケジュールが変わる。また、SET/OPE決済は新しい市場であるため、現状の製品や市場環境そのままでは必ずしも顧客要件を満たしていないこともある。そのような場合の各所との調整や、場合によっては新しいビジネススキームの確立なども含め、さまざまなコンサルテーションサービスを提供する。

(2) システム構築サービス、開発サポート

SET/OPE決済を導入する顧客に対して、ネットワーク環境も含めたシステム全体の構築サービスを提供している。特に、SET/OPE決済を持つ仮想店舗に関しては、顧客によって、システム構成も非常に多岐にわたるため、コンサルテーションを通して、顧客要件に合ったシステム構築サービスを行なっている。

たとえば、仮想店舗システムをすでに持っている、そこにSET/OPE決済を導入する顧客に対しては、Infomercer POSまたはInfomercer ServerPOSを基本に、顧客の仮想店舗システムとInfomercer POSまたはInfomercer ServerPOSとの接続を行なうための開発サポートを提供する。まったく新規にSET/OPE決済機能を持つ仮想店舗システムを導入する顧客に対しては、

当社の仮想店舗構築・運用システムであるInfomerce StoreまたはInfomerce MallとInfomerce POSまたはInfomerce ServerPOSを組み合わせたシステム構築サービスを提供する。

### (3) テスト環境利用サービス

SET/OPE決済は、カードホルダ、仮想店舗、金融機関、認証局の4つに相当するシステムが相互に接続されて実現されるが、顧客はこれら4つの中の1つか2つのシステムを導入するだけであり、他のシステムについては、既存の、そして通常は他の運営者が運用しているシステムを利用することになる。しかし、顧客が導入するシステムをテストするときには、これら4つのシステムが必要になる。そこで、当社のSET/OPE製品を導入した顧客には、当社のテスト環境利用サービスを提供する。当社のテスト環境は、4つのシステムすべてを備えており、顧客のシステムからはインターネット経由で接続し、テストのために利用できるようになっている。

### (4) 接続テスト実施サービス

顧客が導入したシステムは、稼働開始直前に実環境での接続テストが必要になる。この接続テストでは、テスト内容、スケジュール、接続のためのシステム設定が金融機関や顧客のネットワーク構成によって異なるなど、高度な専門知識が要求される。当社は、運用開始直前のこの金融機関との接続テスト実施サービスを提供する。このサービスは、接続テスト実施前のスケジュールやテスト項目の調整から、テストの実施、実施報告書の作成までを提供する。

### (5) アンサリングサービス

顧客が導入したシステムが稼働開始した後は、顧客からの各種問い合わせ対応やバージョンアップの連絡等のために、アンサリングサービスを提供している。アンサリングサービスは、電子メールやWebページで問い合わせを受け付け、電子メール等で回答を送るサービスになっている。本サービスにより、顧客は安心し

てシステムの運用を続けることができる。

## 5. あ と が き

Infomerce SET/OPEソリューションは、仮想店舗運営者や金融機関に、インターネット上の電子商取引における安全なクレジットカード決済/銀行決済を実現するシステムを提供するトータルソリューションである。本ソリューションは、インターネット決済の標準であるSET/OPEに準拠し、かつ日本で唯一のサーバ管理型のSET/OPE製品を持つという特徴を有している。

SET/OPE仕様はすでに次バージョンの仕様検討が進められており、本ソリューションも、次バージョン仕様の早期サポートにより他社製品に対する優位性を確保していく必要がある。そして、日本でもっとも相互接続性のあるSET/OPE製品としての優位性を維持するため、そして当社顧客が電子商取引の拡大を通してメリットを享受できるように、さらに多くの金融機関との相互接続を確立していく必要がある。そして、顧客に対しインターネット決済サービスを自ら提供する金融機関向けには、早期にSET/OPE決済を導入できるよう、Infomerce Payment Gatewayを中心としたソリューションを開発し、提供していく。

標準化活動については、GlobeSetと協力して、日本国内では「日本インターネット決済推進協議会(JIPPA)」において、国外では「SETCo」において、インターネット決済の標準化に貢献しており、今後もこの活動を続けていく所存である。

## 6. 参 考 文 献

- 1) SET Secure Electronic Transaction Specification, Version 1.0, SET Secure Electronic Transaction LLC, 1997年5月
- 2) Online PIN Extensions to SET Secure Electronic Transaction Version 1.0, SET Secure Electronic Transaction LLC, 1999年