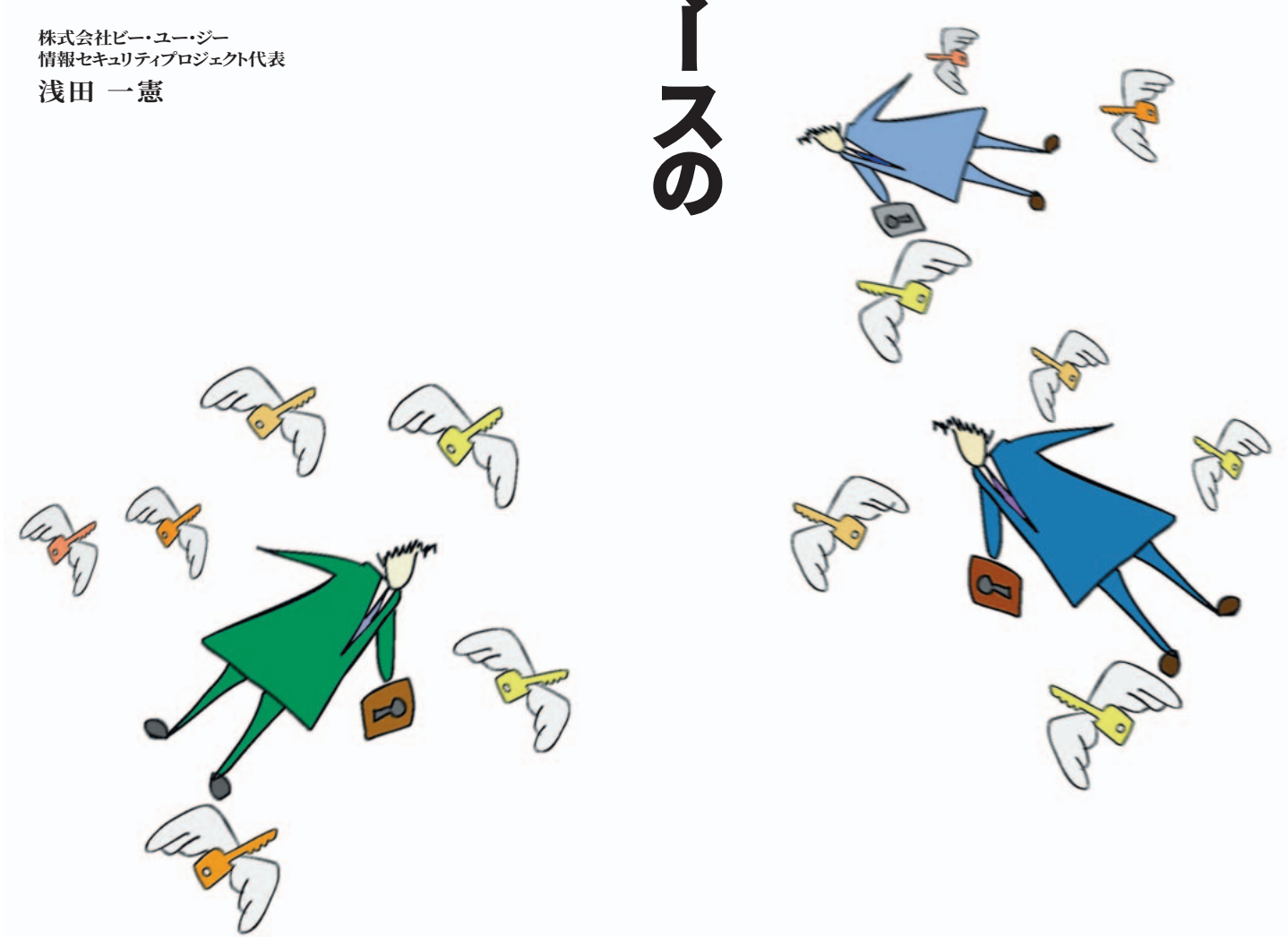
エレクトロニックコマースの基礎技術

【第2回】クレジットカード決済のプロトコル、SET

前回は、エレクトロニックコマースを支える情報セキュリティー技術をめぐる業界動向を概観してみた。そこで中心的な役割を果たすと予想されるのがSET（Secure Electronic Transaction）というクレジットカード決済の世界共通規格であった。今回は、このSETのしくみと実際の運用手順について解説する。

株式会社ビー・ユー・ジー
情報セキュリティプロジェクト代表
浅田 一憲



インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

1 SETの目的とその機能

電子マネーの持つインパクトを予測した大手クレジットカード会社が先導して推し進めようとしているSETについて、まずその概要を見てみよう。

カード会社のビジネス戦略から生まれたSET

SETは、VISAとMasterCardが共同で開発した、オープンネットワーク上で安全にクレジットカード取り引きを行うためのプロトコルである。つまりSETというのはプロトコルの名前だと考えてよい。GTE、IBM、Microsoft、Netscape、SAIC、Terisa、VeriSignといった企業が規格の制定に協力している。

SETの目的は、VISAとMasterCardが、セキュリティー決済の規格制定のリーダーシップをとることにある。今まで、クレジットカード会社は積極的にコンピュータ技術を取り入れることによって業務を拡大してきた。カードに磁気ストライプを入れ、モデムを使用して会員のデータを確認した後に信用を与えるという方法を取り入れた結果、カード読み取り機などの端末メーカーや決済ネットワーク運営者に料金を払わねばならず、一種の利益構造ができ上がってしまった。インターネット上でのカード決済においても、コンピュータ会社などが主導で規格制定をしてしまうと新たな利益構造が発生してしまう可能性があるので、自ら主導権をとって規格を制定していく必要があったわけである。

規格の制定に際しては、既存の加盟店やカード会員とカード会社の関係を保つこと、VISAやMasterCardのブランドを守ることに留意している。SETは世界の統一規格であり、American ExpressもSETに参加することを表明しているし、他のJCBやDiners Clubといった世界的な大ブランドもたぶんSETに参加するであろう。SETは、どんなハードウェアやソフトウェアのプラットフォームでも動作可能なように作成されており、多機種間での相互接続性が保証される。

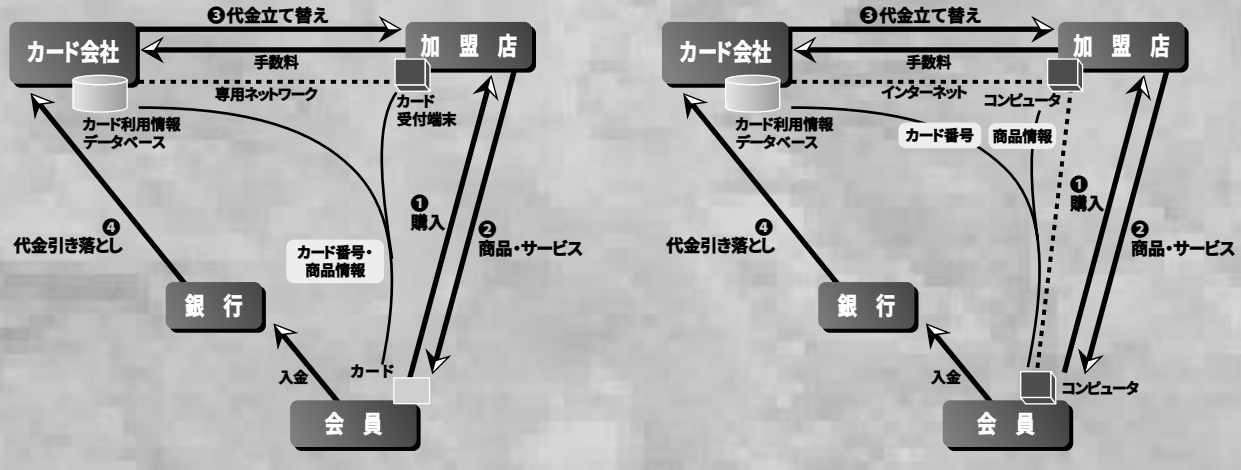
SETによって保証されるビジネス上のセキュリティー

SETを使用すると、売買や決済に関するデータが第三者によって盗み見されず、そのデータは改ざんされていないことを証明でき、カード使用者がクレジットカード会員本人であり、クレジットカードを取り扱っている加盟店も正規のものだという認証を行うことができる。

また、カード会員、加盟店、クレジットカード会社は、それぞれに必要最小限の情報しか得ることができない。加盟店は、カード会員のカード番号などは知ることができないし、カード会社は会員が何を購入したのかを知ることはできない。つまり、データの秘密性と正当性を保証し、相手の認証が行えるというわけだ（図1）。

SETで決めているのは、カード会員が加盟店に対して購入の申し込みを行う「購入メッセージ」、加盟店がカード会社や中継所に対して、カード会員に該当金額の商品を売ってよいかどうかを確認して許可を得

図1：従来のクレジットカード決済とSETによる決済の比較



©1994-2007 Impress R&D

る「与信メッセージ」、加盟店がカード会社に対してクレジットで売った金額の支払請求を行う「キャプチャーメッセージ」などの受け渡し形式と保存形式である。情報セキュリティー技術を使用してそれらのメッセージに電子印鑑を捺印し、暗号化して送受する。使用する暗号アルゴリズム、使用する電子印鑑証明書の受け渡し形式と保存形式も定められている。SETのメッセージは、最終的にはMIME形式にエンコーディングされ、WWWや電子メールでカード決済を行うことができる。

2 SETで使われる技術

次に、SETのシステムを構成するいくつかのセキュリティー技術を紹介しよう。

暗号化とデジタル封筒、電子印鑑証明、割印

SETでは、秘密鍵暗号アルゴリズムはDES、公開鍵暗号アルゴリズムはRSAが使用される。盗み見を防止するために、デジタル封筒（Digital Envelope）という技術を使用する（図2）。

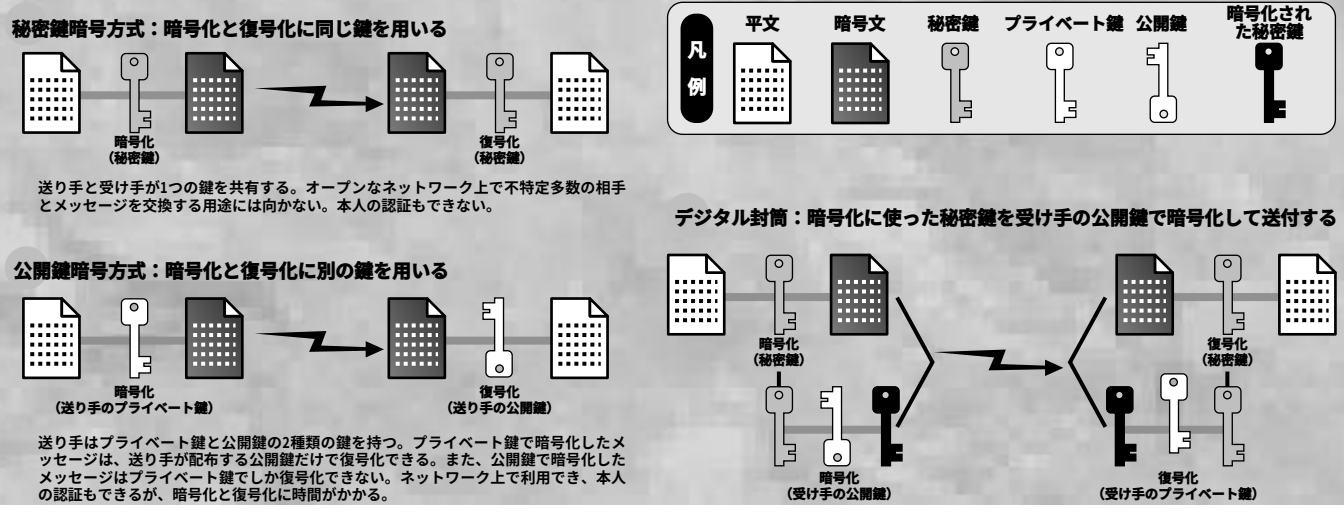
通信する相手の認証と改ざんの検出のためには、電子印鑑（Digital Signature）の技術を使用し、電子印鑑証明書（Certificate）を多用する。また、2つのメッセージを同時に認証するための、割印（Dual Signature）という新しい技術も使用する。

デジタル封筒は、RSA公開鍵暗号とDES（Data Encryption Standard）秘密鍵暗号、そしてBellare-Rogaway Optimal Asymmetric Encription Padding（OAEP）というパディングを使用し、PKCS#1の拡張のフォーマットに準拠する。電子印鑑はRSA公開鍵暗号とSHA-1ハッシュアルゴリズムを使用し、PKCS#7の規格を採用している。

SETでは、電子印鑑証明書が大きな役割を果たす。クレジットカードはプラスチックカードから電子印鑑証明書というデジタルなデータへと変貌する。カード会社が発行したカード会員の電子印鑑証明書が、すなわちデジタルクレジットカードである。ただし、会員番号の漏洩を防ぐためにカード会員の電子印鑑証明書中にはカード番号や有効期限そのものは入っていない。電子印鑑証明書は、このほかに、カード加盟店、カード会社や中継所にも発行され、捺印とデジタル封筒のために使用される。証明書フォーマットは、国際規格であるX.509バージョン3を採用している。

SETで使用するRSA公開鍵暗号の鍵ビットサイズは、捺印目的ではルートCAが2048bitでその他は1024bit、デジタル封筒での鍵配送の目的ではカード会員と加盟店が768bit、その他が1024bitであり、十分に高いセキュリティーレベルであるといえる。現在、SET陣営は、SETをアメリカの輸出規制から除外するように求めており、これだけ長いビット長であるにもかかわらず輸出が許可される可能性が高い。

図2：SETで使用される基本的な暗号技術



インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

3 インターネット/クレジットカード決済の規格

エレクトロニックコマースが具体的にどのように行われるのか、プレーヤー（商取引への参加者）に注目して見ていくことにする。

SETのプレイヤー

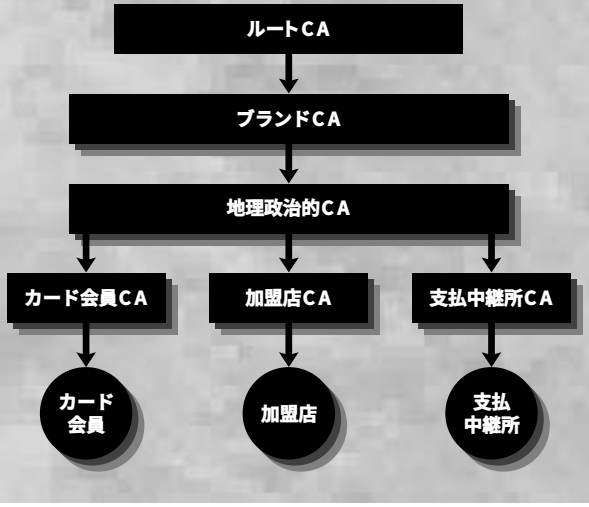
SETでは、次のプレイヤー間のプロトコルが定められている。

○カード会員（Card Holder）
クレジットカードの会員。クレジットカード会社からカードを発行してもらい、加盟店で買い物をする。
○加盟店（Merchant）
クレジットカード会社の加盟店。カード会員に商品を販売する。
○支払中継所（Payment Gateway）
加盟店から与信請求を受け取り、カード会社に取り継ぎする。カード会社自身やカードブランドが行うこともある。
○CA（Certification Authority）
電子印鑑証明書発行局。対象とするプレーヤーごとに複数設置される。それぞれ担当のプレーヤーからの要求を受け、審査をしたうえで電子印鑑証明書を発行する。

SET用のCA

SETでは、多くのCA（電子印鑑証明書発行局）を使用する。まず、SET規格の大元であるルートCA（Root CA）、VISAやMasterといったカードブランドが行うブランドCA（Brand CA）、各ブランドの地方組織が行う地理政治的CA（Geo-Political CA）、カードを発行するカード会社が行うカード会員CA（Card holder CA）、カード加盟店を持つカード会社が行う加盟店CA（Marchant CA）、支払中継所をまとめる支払中継所CA（Payment Gateway CA）である。それぞれのCAは、図3のような階層構造になっており、上位CAが下位CA有効性を保証する。VISAとMasterCardは両者で1つのルートキーを管理し、共同でルートCAを運営する予定であるが、面白いことに、American Expressはそれとは別のルートキーで独自のルートCAを運営する形でSETに参加することを検討しており、同じSET参加カードでも階層の違うものが現れることになるかもしれない。これは、カード会員や加盟店のコンピュータのソフトウェアは複数のルートキーを保持しなければならないということを意味する。このルートキーの扱いに関しては多分に政治的な問題であるので、SETのバージョンが1.0になるまでどうなるかは分からない。

図3：保証の階層構造を持つCA



©1994-2007 Impress R&D

SETのメッセージ

SETでは、主に以下のメッセージのプロトコルが定められている。

❶初期化（Initiate）要求、返答
＝取引を開始するために初期設定を行う
❷証明書（Certificate）要求、返答
＝自身で生成した公開鍵を元に証明書を作成する
❸購入（Purchase Order）要求、返答
＝注文を行う
❹与信（Authorization）要求、返答
＝カード会員と指定金額の取引を行ってよいかどうか審査を行う
❺キャプチャー（Capture）要求、返答
＝代金回収を行う
❻問い合わせ（Inquiry）要求、返答
＝取引の状態を問い合わせる
❼与信取消（Authorization Reversal）要求、返答
＝与信を取り消す
❽キャプチャー取消（Capture Reversal）要求、返答
＝代金回収を取り消す
❾クレジット（Credit）要求、返答
＝精算をやり直す
❿クレジット取消（Credit Reversal）要求、返答
＝精算のやり直しを取り消す

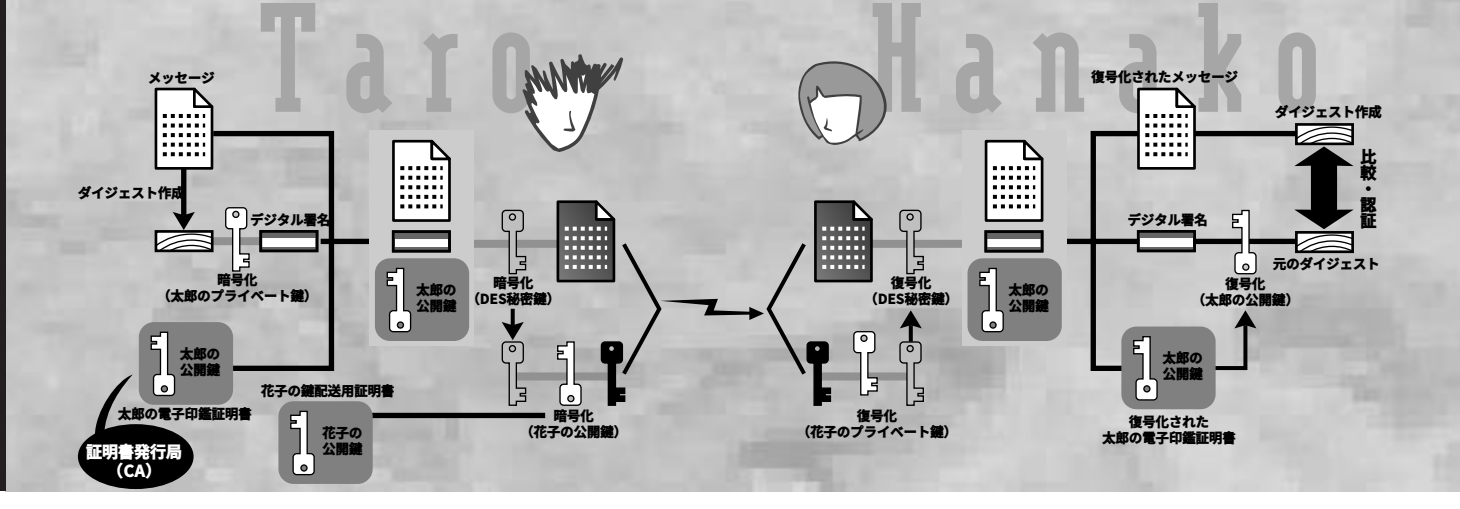
メッセージプロトコル基本型

SETではいろいろなメッセージを扱うが、どのメッセージのときでも同じ基本型に沿って送受される。

太郎さんが花子さんに対して、あるメッセージを送信する場合を例に説明してみよう（図4）。

❶太郎は、花子の鍵配送用証明書を入手しておく。送信したいメッセージを作成する。
❷太郎は、SHA-1アルゴリズムを使用してメッセージのメッセージダイジェスト（そのデータの特徴を示す160ビットの値）を計算する。メッセージダイジェストを自分の捺印用プライベート鍵（R#1-PV）を使用してRSAで暗号化する（メッセージに太郎の電子印鑑を捺印する）。
❸太郎は、元のメッセージとCAに発行してもらった自分の捺印用電子印鑑証明書、暗号化されたメッセージダイジェストの3点を1つのメッセージにし、ランダムに生成したDESの鍵（D#1）を使用してそのメッセージをDESで暗号化する。使用したDES鍵を、花子の鍵配送用証明書中の鍵配送用公開鍵（R#2-PB）を使用してRSAで暗号化して添付する（メッセージを花子宛てのデジタル封筒に入れて封印をする）。
❹太郎は、デジタル封筒を花子に送信する。花子は、デジタル封筒を受け取る。
❺花子は、自分の鍵配送用プライベート鍵（R#2-PV）を使用してRSAで暗号化されているDESの鍵（D#1）を復号化する。その鍵を使用し、DESで暗号化されている元のメッセージと太郎の捺印用電子印鑑証明書、暗号化されたメッセージダイジェストを復号化する（花子宛てのデジタル封筒を開封し、中身を取り出す）。
❻花子は、太郎の捺印用電子印鑑証明書を、ルートキーからのキーチェインをたどって正しいかどうか確認する（電子印鑑証明書の正当性を確認する）。
❼花子は、太郎の捺印用電子印鑑証明書から太郎の捺印用公開鍵（R#1-PB）を

図4：SETメッセージの基本パターン



インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

取り出し、RSAで暗号化されているメッセージダイジェストを復号化したものと、自ら元メッセージからSHA-1アルゴリズムを使用して計算したメッセージダイジェストと比較することによって元メッセージが正しいかどうかを確認する（捺印されている電子印鑑を確認し、元メッセージの正当性を確認する）。

以上の作業で、花子は、受け取ったメッセージは確かに太郎が送ってきたものであり、途中で改ざんされていないことを確認できる。また、この過程で第三者がメッセージを盗み見することはできない。

購入要求メッセージ

SETのメッセージのうち、購入要求について具体的な手順を以下に説明する（図5）。これらのメッセージはすべてインターネット上のコンピュータ間で交換されて処理される。

本稿に関するお問い合わせは、電子メールにて infosec@bug.co.jp までお願いします。

図5：SETで扱われる購入要求のメッセージ

カード会員 初期化要求▶ **加 盟 店**

1 カード会員（Card Holder）は、購入物を決定する。
2 カード会員のソフトウェアは、加盟店（Merchant）に初期化要求（Initiate Request）を送る

カード会員 ◀返答 **加 盟 店**

3 加盟店のソフトウェアは、初期化要求を受け取る。
4 加盟店のソフトウェアは、初期化要求の返答（Response）を生成し、加盟店の電子印鑑を捺印する。
5 加盟店のソフトウェアは、加盟店と支払中継所（Payment Gateway）の鍵配送用証明書を添付したうえで、返答を送信する。

カード会員 発注▶ **加 盟 店**

6 カード会員のソフトウェアは、初期化返答を受け取り、印鑑証明書の正当性を確認する。
7 カード会員のソフトウェアは、返答の中の電子印鑑を確認し、初期化返答の正当性を確認する。
8 カード会員のソフトウェアは、ショッピングのときに得られた情報を元に注文書（Order Information）を作成する。
9 カード会員のソフトウェアは、支払指示書（Payment Instruction）に必要事項を書き込み完成させる。
10 カード会員のソフトウェアは、注文書に支払指示書との割印（Dual Signature）を捺印する。
11 カード会員のソフトウェアは、支払指示書に注文書との割印を捺印する。
12 カード会員のソフトウェアは、捺印済みの注文書を加盟店宛てのデジタル封筒に入れて封印する。
13 カード会員のソフトウェアは、捺印済みの支払指示書をカード会員のアカウント情報とともに支払中継所宛てのデジタル封筒に入れて封印する。
14 カード会員のソフトウェアは、暗号化した注文書と支払指示書の両方を加盟店に送付する。

カード会員 ◀返答・注文の実行 **加 盟 店** 与信要求▶ **カード会員**

15 加盟店のソフトウェアは、自分宛てのデジタル封筒を開封し、注文書を取り出す。
16 加盟店のソフトウェアは、注文書に添付されているカード会員の印鑑証明書の正当性を確認する。
17 加盟店のソフトウェアは、注文書の割印を確認し、注文書の正当性を確認する。
18 加盟店のソフトウェアは、カード会員の要求を実行する（与信請求のため、支払指示書を支払中継所に転送することも含む）。--> 与信へ（省略）
19 加盟店のソフトウェアは、注文返答書（Purchase Response）を作成し、加盟店の電子印鑑を捺印する。
20 加盟店のソフトウェアは、注文返答書をカード会員に送る。
21 与信が得られた場合、加盟店はカード会員の注文を実行する（品物を発送するなど）。

カード会員 確認・保存

22 カード会員のソフトウェアは、加盟店の捺印用印鑑証明書の正当性を確認する。
23 カード会員のソフトウェアは、注文返答書の電子印鑑を確認し、注文返答書の正当性を確認する。
24 カード会員のソフトウェアは、注文返答書を保存する。

©1994-2007 Impress R&D

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp

Copyright © 1994-2007 Impress R&D, an Impress Group company. All rights reserved.