電子決済用セキュアプロトコルｉＫＰと暗号方式

1Ｊ－2

長谷 容子

日本アイ・ビー・エム（株）東京基礎研究所

1. はじめに

インターネット上でエレクトロニック・コマース（電子商取り引き）を行うためのシステムを考えるとき、重要な課題の１つは、安全で効率的な電子決済用プロトコルの確立である。その有力な候補の１つにｉＫＰ（Internet Keyed Payment Protocol）[1]がある。

ｉＫＰは、インターネット上で消費者、加盟店、クレジットカード会社の３者が、相互に相手の正当性を確認しながら、それぞれが必要な情報のみをやりとりし、安全に電子決済を行うためのプロトコルであり、プロトコル中では公開鍵暗号方式を用いている。

本講演では、ｉＫＰ中で公開鍵暗号方式が使われることにより、電子決済中でどのようなセキュリティが達成されるかの特徴を述べ、更に、他の暗号方式使用の可能性と問題点を解析する。

2．ＳＬＩＰの暗号化

ｉＫＰには、図１に示すような、主に６つのメッセージフローがあり、これらのメッセージフローを通して、消費者は、商品の注文内容を加盟店に伝え、更に、その決済に必要な情報をクレジットカード会社に伝える。また、受け取った情報をもとに、加盟店は商品を発注し、クレジットカード会社は決済処理への業務を進めることになる。

ここで、特徴的なのは、消費者が、ｉＫＰのＰＡＹＭＥＮＴメッセージで運ぶクレジットカード番号や有効期限などの機密情報（以下ＳＬＩＰと呼ぶ）を、クレジットカード会社の暗号用公開鍵で暗号化することである。したがって、このＳＬＩＰはクレジットカード会社が持つ復号用秘密鍵でしか復号することができない。このことによって、消費者のＳＬＩＰが送信中に盗聴されるのを防ぐだけでなく、加盟店にさえもクレジットカード番号を知られることなく消費者のプライバシーが守られ、安全に電子決済が行えるのである。

3．ｉＫＰメッセージのデジタル署名化

ｉＫＰの中でも３ＫＰを考えるとき、消費者、加盟店、クレジットカード会社は、それぞれデジタル署名用の秘密鍵（もちろん、それらに対応する公開鍵も存在する）を持つことが条件付けられ、これらの秘密鍵を使って、それぞれがｉＫＰメッセージにデジタル署名を施し送り出す。この署名は、対応する公開鍵によって誰でも検証することができるが、署名を施せるのは秘密鍵を持っている送信者だけであり、悪意を持った第３者がメッセージの内容を改ざんして署名しなおしたり、送信者になりすましてメッセージに署名したりすることはできない。

また、ｉＫＰでは、秘密鍵に対応した公開鍵はＣＡ（Certification Authority）によって認証、及び、有効性が管理されているものを使用することを前提としており、署名したメッセージ送信後にその署名用秘密鍵の無効性を理由に、送信者がメッセージの送信事実を否定（しらばっくれ）することができないようになっている。

4．ｉＫＰのセキュリティと暗号方式

これまで述べてきた特徴は、ｉＫＰプロトコルが公開鍵暗号方式を使用することによって達成され

Cryptography in Secure Electoronic Payment Protocol iKP

Yohko Hase

IBM Research, Tokyo Research Laboratory

1623-14 Shimotsuruma, Yamato, Kanagawa 242, Japan

るものであり、すなわち公開鍵暗号方式であれば、どの暗号でも（たとえばＲＳＡ，ラビン、エルガマルなど）達成されるものである。

それでは、この公開鍵暗号方式を共通鍵暗号方式に置き換えてみたらどうであろうか。

まず、ＳＬＩＰの暗号化であるが、共通鍵暗号方式を用いると、暗号化されたＳＬＩＰの復号化はクレジットカード会社の秘密鍵だけでなく、消費者の持つ秘密鍵によっても行えることになる。ｉＫＰにおいて消費者が自分で暗号化したＳＬＩＰを自分自身で復号化してもメリットはないが、暗号化したＳＬＩＰを復号化できる鍵がクレジットカード会社以外にも存在するということで、秘密に保持するべき情報が増えることになり、鍵管理に気を配らなければならない。また、セキュリティ上、消費者とクレジットカード会社が１対１の鍵を持つことを前提とするならば、クレジットカード会社は消費者の数だけの鍵を秘密に保持しなければならず、インターネット上の多数の消費者を考えるとき、鍵管理が困難になることは避けられない。

次に、ｉＫＰメッセージのデジタル署名化について考えてみよう。共通鍵暗号方式を用いたデジタル署名では、署名文の第三者による改ざんは公開鍵暗号方式を使用したときと同様に防ぐことができるが、送信者と同じ鍵を持つ受信者によって改ざんされる可能性が残ってしまうことになる。このことは、たとえば、消費者が送った署名つきメッセージの内容を加盟店が改ざんでき、その事実の追求が困難であることを意味し、セキュリティ上大きな問題となる。また、鍵管理の困難さについては前に述べたものと同じである。

このように、ｉＫＰにおいて公開鍵暗号方式の代わりに共通鍵暗号方式を用いようとすると、セキュリティ上いくつかの不都合が生じることになる。

５．おわりに

電子決済用セキュアプロトコルｉＫＰは、公開鍵暗号方式を使用することによって効率的な運用及び、高度なセキュリティを維持している。プロトコル中では、どの公開鍵暗号を使用すべきかなどの束縛はなく、システム設計者に選択の余地を残している。しかしながら、実際にシステム構築を考えるとき、公開鍵暗号の中のどの暗号を使用するかについては、セキュリティレベル、パフォーマンス、その他の色々な条件から検討されるべき問題であり、安全で、効率的な電子決済用プロトコルの確立、更には、インターネット上のエレクトロニック・コマースが世の中に受け入れられ発達していくための重要な鍵の一つを握っている問題と思われる。

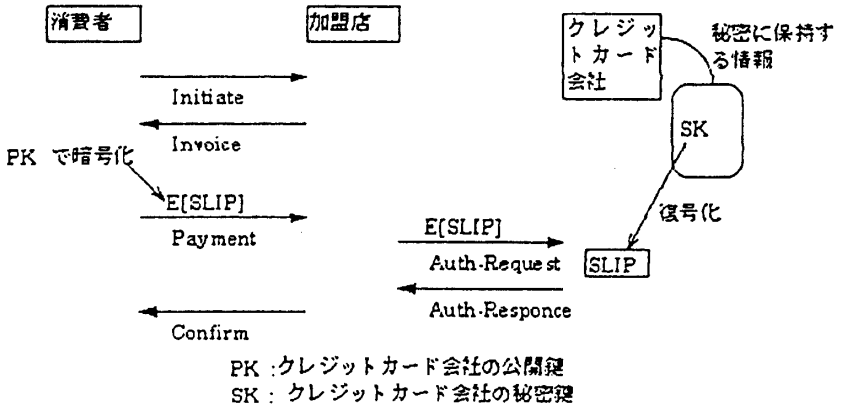

図１ 公開鍵暗号方式を使用するiKPとSLIP

[参考文献]

[１] Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Michael Waidner:
iKP - A Family of Secure Electronic Payment Protocols
<http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/>