平成13年2月2日

報道発表資料

ＮＴＴコミュニケーションズ株式会社
日本電信電話株式会社

接触・非接触共用ＩＣカードで、公開鍵暗号の高速処理を世界で初めて実現

～非接触ICカードによる高セキュリティ電子マネーで支払時間０．４秒を実現～

ＮＴＴコミュニケーションズ株式会社（略称：NTT Com）と日本電信電話株式会社（略称：ＮＴＴ）は、このたびＮＴＴ情報流通プラットフォーム研究所の技術をベースに、市販レベルの接触・非接触共用ＩＣカード（コンビＩＣカード）を用いて、公開鍵ディジタル署名を使用する高セキュリティで高速処理が可能な電子マネーを開発しました。この電子マネーでは、店舗での支払いを０．４秒で処理できるなどの高速性を実現しています。非接触ＩＣカード上で、公開鍵暗号方式による本格的セキュリティを具備した電子マネーなどの高機能アプリケーションを実用化したのは世界で初めてです。

これまで、非接触ＩＣカードは、カードへの電力供給が少ないことなどから、公開鍵暗号など、複雑な演算を伴う高速処理は困難と考えられてきましたが、ＮＴＴでは、公開鍵として従来のＲＳＡ方式（注１）ではなく、処理量の少ない楕円暗号方式（注２）を用い、楕円暗号の演算に特殊な工夫（注３）を行うことにより、高速処理を実現しました。

これにより、非接触ＩＣカードでも、高セキュリティを保持した高速処理が可能となりました。

各種金融カード、電子チケットカード、更には電子政府における公印カードや住民カードなど、あらゆる分野で非接触ＩＣカードに対する公開鍵暗号方式搭載のニーズは大きいため、本方式の実現により今後の非接触ＩＣカードの普及に拍車がかかると考えています（注４）。

利用したＩＣカードは、安価な市販レベルの接触・非接触共用（コンビ）カードで、両インタフェースとも国際標準であるＩＳＯ７８１６（接触）、ＩＳＯ１４４４３（非接触）に準拠しています（注５）。今回、接触・非接触

共用カードを用いたのは、実用上、バーチャル（接触）とリアル（非接触）の連動を考慮したためで、例えば、電子チケットを自宅のＰＣで購入（接触インタフェース）し、駅などのゲートで迅速に改札（非接触インタフェース）するといった使い方を想定しています。

　既にNTT Comは、このＩＣカードを用いたサービスについて、金融、交通、流通、コンテンツ等の業界数社と検討を開始しており、今年中にはサービスを立ち上げる計画です。また、今後は、ＩＣカードの長期利用を可能とするため、ＩＣカード発行後に新しくアプリケーションを追加するという機能も盛り組んでいく予定です。

注１：データの暗号化と復号化で異なる鍵を使用する公開鍵暗号の代表的な方式です。認証やディジタル署名等で広く一般に使用されています。大きな整数の素因数分解の難しさに安全性の根拠を置いています。

注２：ＲＳＡ方式に比べて、より少ない鍵長でも、より解読が困難となることを特長とする公開鍵暗号の一方式です。安全強度にかかわる鍵長は、160bitでＲＳＡ方式の1,000bit程度の強度に相当すると考えられています。名前は、楕円曲線上での演算を利用して、暗号化・復号化を行うことに由来しています。

注３：ICカード内で、公開鍵暗号処理の一部を本番の処理に先行して５０回程度まとめて計算しておき、これを本番の処理で使うことにより、公開鍵暗号のディジタル署名作成時間を従来比の１／３に短縮しました（約0.2秒でのICカード内署名作成を実現）。

注４：これまで、金融分野のＩＣカード化は、効率よく高セキュリティを確保するため、接触型ＩＣカードを軸に検討が進んでいますが、この非接触ＩＣカードの開発により、今後は、非接触ＩＣカードの導入も射程に入ってきました。

注５：ISO14443で国際標準となっているType A、Type Bのいずれかに対応可能（図参照）です。また、利用できる端末を増やすため、Ｔｙｐｅ AとBを同時にサポートする機能も計画中です。

・図　非接触ICカードの種類

【本件に関するお問合せ先】

NTTコミュニケーションズ
先端ビジネス開発センタ
菅沼
Tel：03-6800-3320
E-Mail：info-ab@ntt.com

ＮＴＴ情報流通基盤総合研究所
倉嶋・佐野・池田
Tel：0422-59-3663
Ｅ-mail：koho@mail.rdc.ntt.co.jp

NTT NEWS RELEASE