NEWS RELEASE

NTT

日本電信電話株式会社

（報道発表資料）

２００１年１１月２９日

交通機関や店舗での決済に安全で高速に利用できる電子マネーを実現

～バスの精算からレジの支払いまで、バス車内や公衆電話機でチャージも可能に～

日本電信電話株式会社（以下NTT、本社：東京都千代田区、代表取締役社長：宮津純一郎）は、支払い処理にスピードが要求される交通機関などでの利用に適し、さまざまな決済シーンで利用可能な非接触型ICカードの公開鍵暗号電子マネーシステムを実用レベルで完成しました。公開鍵暗号(*1)による署名処理時間は最短で１msecを達成しており、電子マネー支払い処理時間は250msec以下を実現しました。これは、セキュリティ度の高い公開鍵暗号を非接触型ICカードに搭載したものとしては世界最高速の処理能力を有するもので、プリペイドカードとして店舗レジ等での利用にとどまらず、非接触・高速の特徴を活かしてバスなどの交通機関にも適用できます。また、ICカード公衆電話機を電子マネーの入金（チャージ）に利用することも可能になります。

電子商取引の拡大や電子政府構想の進展に伴い、ICカードに寄せられる期待が高まっています。最近では、これまで金融機関などに導入されてきた接触型ICカードに加えて、端末にかざすだけで決済処理などが完了する、より使い勝手のよい非接触型ICカードが注目を浴びています。

NTT情報流通プラットフォーム研究所では、今年２月、楕円暗号方式(*2)を用いることで公開鍵暗号にそなわる高セキュリティ特性に加えて高速処理も可能にした電子マネー方式を開発するなど（http://www.ntt.co.jp/news/news01/0102/010202.html）、安全性と高速処理をともに実現する非接触型ICカード搭載公開鍵暗号電子マネーシステムの開発に努めてきました。今回開発した電子マネーシステムは、更なる高速化を図るとともに、これまでのNTT電子マネー技術を集大成し実用レベルにまで高め、これによりバスの精算からレジの支払いまでさまざまなシーンで利用可能としました。

本システムの最大の特長は、支払い処理の高速性です。スピーディな支払い処理が求められる決済にも適用できるよう、高速処理が可能な楕円暗号署名を採用し、

さらに支払い場面で要求される暗号処理の一部を事前に処理する技術を導入した結果、公開鍵暗号の署名処理時間は最短で１msecを達成し、電子マネー支払い処理時間は250msec以下を実現しました。これはバス乗車券システムなどにも適用できるレベルであり、実際に乗車券システムへの適用を進めています。このことにより運賃精算処理時間が大幅に短縮されます。

さらに、電子マネーの入金（チャージ）端末としてNTT東日本・西日本のICカード公衆電話機（平成13年9月末現在：全国約42,200台設置）を利用可能とする技術も開発しました。これにより、金融機関の専用端末（ATMなど）だけでなく、ICカード公衆電話機を利用して口座から手軽に電子マネーを入金（チャージ）することができます。実現にあたっては、NTT研究所が開発した非接触型ICカード技術、ICカード公衆電話機技術を利用し、さらに今回電子マネーセンタのサーバ側からICカード公衆電話機を制御する方式を採用しました。

この電子マネーシステムは、ICクレジットカード端末規格であるEMV仕様(*3)や、金融機関等で検討が進められているオフラインデビット(*4)に関する仕様なども参照しており、コンビニエンスストアや百貨店をはじめ全国あらゆる店舗の決済手段としても適用可能です。本実装は、NTTコミュニケーションズ株式会社と連携して行いました。

NTT情報流通プラットフォーム研究所では、本研究を踏まえて、今後は、携帯電話を“財布代わり”に用いるモバイル・ペイメントへの適用に向けた研究を進めていく予定です。

＜システムの特徴＞

１）　スピーディな支払い処理が可能
非接触型ICカードと公開鍵暗号の組み合わせでは世界最高速となる支払い処理時間250msec以下を実現しています。このため、ICカードバス乗車券に適用した場合、これまでの磁気カード利用時(800msec程度)と比べ、はるかにスピーディな支払い処理が可能となります。

２）　ICカードバス乗車券システムではオフラインチャージを実現
ICカードバス乗車券システムでは運転手経由で電子マネーの入金（チャージ）が行えるオフラインチャージシステムも採用しています。そのため、電子マネーの誤発行を防ぐ独自のセキュリティ技術を導入し、実用化ニーズに対応しています。

３）　入金端末としてのICカード公衆電話機利用
いつでもどこでも電子マネーの入金が行えるようICカード公衆電話機でもチャージが行えるようにしました。今回、開発した方式はICカード公衆電話機に電子マネー処理用のソフトウェアを搭載することが不要です。このため、ICカード／チップ

との通信機能が提供されれば、携帯電話にも簡単に適用可能です。

４）　様々な用途に適用可能
　EMV仕様や全銀協のオフラインデビット仕様も参照してICカードに実装しているため、コンビニエンスストアや百貨店をはじめとする様々な店舗端末への適用が可能です。

＜技術のポイント＞

（ICカードの公開鍵暗号処理で世界最高速を達成）
　署名処理などの支払い時に必要とされる暗号処理アルゴリズムのうち、特定部分をあらかじめ計算する「事前処理」方式を採用することで、処理時間を「事前処理」なしに比べて1/10に短縮し、署名処理時間最高1msecという世界最高速の処理速度を実現しました。また、支払い処理時間は楕円暗号署名の採用やプロトコルの最適化、リーダライタなどの処理の最適化を図ることで、250msec以下という世界最高速の高速性を実現しました。

＜用語解説＞

***1　公開鍵暗号**
　暗号化に公開鍵を用い復号化に秘密鍵を用いる暗号方式。公開鍵が公開できることから鍵管理が容易、またメッセージの暗号化のみならず電子署名や共通鍵交換にも用いることができる反面、暗号化・復号のための演算処理が複雑で処理速度に難点を有する。しかし、最近では、高速処理を実現する様々な方式が開発されている。

***2　楕円暗号方式**
　RSA（*5）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。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。名前は、楕円曲線上での演算を利用して、暗号化・復号を行うことに由来している。

***3　EMV(Europay/Mastercard/Visa)**
　ヨーロッパのクレジットカード会社3社が共通で策定したＩＣクレジットカードの統一仕様。事実上の世界標準となっている。

***4　オフラインデビット**
　金融機関が、預貯金を直接の裏付けとしてバリュー（価値）を管理し、センター（ホスト）に接続（アクセス）することなく、オフラインでバリューの払い出しを可能とする取引をいう。（通常のデビットでは、一般にセンターホストに接続し、オンラインでバリューの払い出しが行われる）バリューの精算は即時ではなく、後

日行われる。

***5　RSA暗号方式**

　データの暗号化と復号で異なる鍵を使用する公開鍵暗号の代表的な方式。認証やディジタル署名等で広く一般に使用されている。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る。名称は、共同開発者３人の名前（R.Rivest, A.Shamir, L.Adleman）に由来する。

・参考図：NTT電子マネー技術の適用分野を拡大

【本件に関するお問い合わせ】
ＮＴＴ情報流通基盤総合研究所
企画部　広報担当　飯塚、佐野、池田
TEL：0422-59-3663
E-mail：koho@mail.rdc.ntt.co.jp

NTT NEWS RELEASE