NEWS RELEASE
NTT
日本電信電話株式会社

２００１年１２月２１日

# 1枚のICカードで旅行、イベント等様々な生活シーンに利用できる電子チケットシステムを開発

～記述の柔軟性、高度な安全性、高速性を共に実現した「FlexTicket」～

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）では、入場券・会員券などの様々な「価値情報」（以下「チケット」）を電子化してネットワーク上で流通させ、利用者（個人）間譲渡も可能な汎用電子チケットシステム「FlexTicket」を開発しました。

この汎用電子チケットシステム「FlexTicket」は、利用者が1枚のICカードを持つことで、コンサートチケットなどの入場券、引換券、宿泊券など、インターネットを介して入手し手軽に利用することが可能になります。また、安心して利用いただくために、電子チケットとしては世界で初めて公開鍵暗号方式(*1)を採用し、公開鍵暗号方式として高速処理を実現する楕円暗号方式(*2)を採用しています。

本技術をベースとして、NTTコミュニケーションズ株式会社と、ぴあ株式会社は、共同で事業化の検討を進めています。

電子商取引が拡大する中、電子チケットの実用化が各方面で進められようとしています。チケット情報を電子化しネットワーク上で“発券”する電子チケットは、紙のチケットに比べて発行や入手が手軽に行えるなど数多くの可能性を有しています。しかし、これまでに実用化された電子チケットは、ほとんど単目的のものであり、新しい電子商取引の枠組みを提供するものではありませんでした。

NTT情報流通プラットフォーム研究所では、電子チケットシステムを、入場券・引換券・宿泊券等の「チケット」をデジタル化して流通させる新たな商取引基盤として、チケット発行者やチケット利用者が、安心・便利、さらに手軽に利用していただけるよう研究開発を進めてきましたが、今回この商用レベルのシステムとして「FlexTicket」を完成させたものです。

「FlexTicket」は、偽造、二重使用、“なりすまし”の防止、プライバシーの保護等に対する高レベルなセキュリティ技術のもと、各種電子チケットの発行・流通・使用（改札）を支援するシステムです。さらに、XML(*3)による

自由な記述ができるため特定の用途にしばられず、あらゆる分野の「チケット」発行者が、独自のプログラムを作成することなく簡単かつ安全に、デジタル化した「チケット」を流通させることができます。また、利用者（個人）間での譲渡も簡単に行えますし、1枚のICカードに異なる発行者のチケットを格納することも可能なため、インターネット上で入手した各種「チケット」情報を格納したICカード１枚で、様々な用途（コンサート入場など）に使用することができます。ICカード以外にも安価なID付メモリカードなどでチケットを持ち歩くことも可能です。

NTT情報流通プラットフォーム研究所では、今後、次世代携帯電話等への展開を図り、ユビキタスコマース(*4)を実現する新たな社会的インフラを構築していく予定です。

**＜主な特徴＞**

１）あらゆる分野のチケットに適用可能

単目的の電子チケット発行システムではなく、記述能力に優れたチケット定義言語で表現するため、あらゆる分野の「チケット」発行者が利用可能です。

アミューズメント：コンサートチケット、スポーツ観戦券、映画前売券等

店舗販売、流通：商品券、食事券、宿泊券、クーポン券等

交通：航空券、マイレージカ ード、定期券等

２）どんなチケットも簡単に発行

チケット毎に専用アプリケーションを必要とした従来の電子チケットシステムと異なり、発行者は各種チケットの運用条件をXMLで定義するだけでチケット発行ができます。そのため、開発コストの大幅な削減と、条件の変更に対応した柔軟なチケット発行が可能です。また、新たな種類のチケットを取り扱い開始する場合でも、既に利用者に配布したICカード等のプログラムを更新する必要はありません。

３）高度な安全性

NTT電子マネー(平成13年11月29日電子マネー報道発表参照 http://www.ntt.co.jp/news/news01/0111/011129.html)のセキュリティ技術を踏襲し公開鍵暗号の採用により、偽造、二重使用、“なりすまし”の防止、プライバシーの保護等に対する高度な安全性を備えています。このため安心してお使いいただくことができます。

４）高速オフライン改札処理

利便性の高い非接触ICカードと高速暗号技術を採用し、改札処理はセ

ンタサーバへのアクセスを行なわずゲート端末で処理される（オフライン改札処理）ため、混み合うコンサート会場でのチケット処理などにおいても高速改札処理が可能です。

**<システム概要>**　【図　参照】

1）専用の接触・非接触デュアルインタフェースICカードを用意します。
2）利用者は、インターネットを介して、電子チケット発行者（もしくは発行代理サービス業者）のサーバにアクセスし、各種「チケット」を購入します。
3）購入した「チケット」を専用端末（リーダ／ライタ付）で非接触・接触デュアルインタフェースICカードに格納します。通常格納は安価な接触リーダ/ライタを使用します。
4）ICカードに格納された「チケット」を実際の使用場面――例えば、コンサート会場の入場口など――で行使すると（専用端末に読みとられると）、「チケット」が削除されます。改札は高速な非接触インタフェースを使用します。
5）FlexTicketをPC等にインストールした者同士であれば、個人間の譲渡も可能です。方法としては、直接（同期的に）「チケット」を送る方法と、間接（非同期的に）チケット口座（メールサーバーのようなもの）を介して送る方法があります。

**<技術のポイント>**

1）チケット定義言語

　チケットによって異なる権利内容（有効期限や座席番号など）および流通条件（発行者や改札者の資格条件など）を、新しく開発したXMLベースのチケット定義言語を用いて記述してあります。そのため、専用アプリケーションを個別に開発することなく、自由度の高い条件設定が可能で、かつ運用条件の変更等にフレキシブルに対応します。

2）原本性保証技術

　「チケット」をICカードに格納するにあたっては、チケット定義言語で記された「価値内容」そのものではなく、その“要約情報”である「トークン」だけを分離して書き込みます。この「トークン」が増加したり、改ざんされたりすることのないような流通プロトコルを使用することにより原本性を保証しています。さらに、種類もサイズも異なる各種電子チケットを容量の小さい「トークン」として共通化して持ち運ぶことが可能になりました。利用者にとっては「トークン」を持つことが

「チケット」の原本を持つことであり、これを消費すれば「チケット」を使用する権利が消失します。

3）電子チケット初の公開鍵暗号方式（楕円暗号）の採用

電子チケットとしては世界で初めて、公開鍵暗号方式を採用しました。これにより高度な安全性を確保しています。また、高速処理に対応するため公開鍵暗号方式として楕円暗号方式を採用しています。これにより、非接触ICカードの採用とともに高速オフライン改札処理を実現しています。

**＜用語解説＞**

*1　公開鍵暗号

暗号化に公開鍵を用い復号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　XML

インターネットの標準としてW3Cより勧告された電子文書の記述言語。次世代HTMLともいわれインターネット(web)との親和性が高い。HTMLと同様にタグに挟まれた値によって表現するが、XMLは文書独自のタグが指定できる。

*4　ユビキタスコマース

実生活空間のいたるところに存在する端末や商品等に埋め込まれたデバイス等を有機的に連携させて行う商取引の形態。携帯電話を利用したモバイルコマースはその最初のステップと考えられる。

・図：様々な生活シーンでサイバーとリアルをつなぐ FlexTicket

【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