電子マネーシステムを支える基盤技術
―利便性とセキュリティを両立させるために―

現在、電子マネーはコンビニやスーパー、鉄道、バスといった多くの場所で利用されており、社会インフラの１つと言えるほど生活に身近なものとなっている。本稿では、この電子マネーについて、ビジネス、システム、そのシステムを構築するプロジェクトという観点で、筆者の経験を踏まえ解説する。

社会インフラとなった電子マネー

電子マネーとは、一般に「お金の価値を電子化した決済手段」の１つと定義される。具体的には、現金の価値を電子化してICカードに保存（チャージ）し、支払いの際には保存された現金相当額を加盟店側に移転する方式と、「BitCash」のようにインターネット上の決済に使うものがある。本稿では、ICカード型の電子マネーに限定して話を進める。

2001年に、JR東日本の「Suica」や、ビットワレット社が運営する「Edy」といった非接触型ICカードの電子マネーが日本で初めて登場して以後、電子マネーは徐々に普及していった。2007年には、首都圏の私鉄各社が「PASMO」を導入し、またスーパーやコンビニなどで利用できる「nanaco」（アイワイ・カード・サービス社）や「WAON」（イオンリテール社）が登場するに及んで、電子マネーの普及はさらに進んだ（2007年は「電子マネー元年」と呼ばれる）。2009年に野村総合研究所（以下、NRI）が実施したアンケート調査によると、電子マネーは首都圏の人口当たりの保有率が８割を超え、社会インフラの一部となっていることが示された。

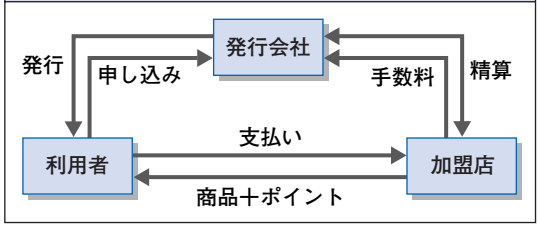
電子マネービジネスのプレーヤー

電子マネーをビジネスの側面から見ると、そのプレーヤーは発行会社、加盟店、利用者の３つに分類される（図１参照）。

発行会社は、電子マネーを発行し、加盟店と精算ができるようにシステムを整備する。発行会社は電子マネーを利用することの利便性のほか、ポイントプログラムなどのサービスを提供することによって利用者を獲得する。加盟店に対してはマーケティング上のメリットを提供する。発行会社は加盟店から手数料を徴収することによりビジネスを成り立たせている。

加盟店は、電子マネーの利用場所を提供すると同時に、利用者がチャージした金額や支払いに使った金額を集計して、発行会社との間で精算処理をする。加盟店にとってのメリットは、利便性やポイントプログラムのよう

図１　電子マネービジネスのプレーヤー



野村総合研究所
基盤サービス事業本部
システム基盤統括一部
上級テクニカルエンジニア
河野勝利（こうのしょうり）
専門は金融系システムの基盤方式設計など

なサービスを提供することにより、顧客の獲得や囲い込みが図られることである。

利用者は、小銭が不要で、機器にかざすだけで精算できる利便性や、ポイントが付与されるなどの経済的メリットから電子マネーを決済手段として利用する。多くの電子マネーでは、ポイントを電子マネーに交換し、現金相当額を利用することもできる。

電子マネーシステムの概要

(1) システムを構成する機器類

一般に電子マネーシステムは、ICカード、ICカードの情報を読み書きするリーダー／ライター、およびリーダー／ライターと通信を行うサーバー機器類によって構成される。

①ICカード

日本では、ソニー社の「FeliCa」という非接触型のICカード技術が、「Suica」「nanaco」「Edy」など多くの電子マネーで採用されている。「FeliCa」は他のICカード規格よりリーダー／ライターとの通信速度が速いことから、POS（販売時点管理）レジより高速な処理が求められる交通改札の用途として「Suica」に採用され、これを機に広く普及することとなった。ICチップには、現金相当額が書き込まれているが、その情報は簡単に変更されないように暗号化されている。「FeliCa」では共通鍵暗号化方式が用いられている。

「FeliCa」以外の非接触型のICカードとしては、国際規格ISO 14443に準拠したType-AおよびType-Bと呼ばれるカードが世界的に多く利用されている。日本でも、タバコ自販機用の成人識別カード「taspo」がType-Aを、住民基本台帳カードやICパスポート、ICカード運転免許証がType-Bを採用している。

②リーダー／ライター

リーダー／ライターには、その筐体中にプログラムや暗号化のための鍵情報を内蔵し、単体で読み書きができるインテリジェント型と、サーバー機器からの操作でカード情報を読み書きする非インテリジェント型がある。インテリジェント型は、内蔵する鍵情報やプログラムが外部に漏れることを防ぐための耐タンパー性（後述）を有している。

通常、リーダー／ライターはPOSレジなどの端末機器に接続して使われる。POSレジはリーダー／ライターから情報を受け取りセンターサーバーへ中継する。

非インテリジェント型のリーダー／ライターとしては、PCなどのUSBポートに接続して使用する「パソリ（PaSoRi）」がある。ICカードをこの機器にかざすだけで、電子マネーの入金や決済ができるようになっている。

③サーバー

リーダー／ライターおよびその情報を中継するPOSレジと相互に通信を行い、業務処理をコントロールする。非インテリジェント型のリーダー／ライターの場合は、サーバーから直接、ICカード情報の読み書きを行う。鍵情報などの機密情報は、HSM（Hardware

Security Module）と呼ばれる装置（後述）に格納して外部への流出を防いでいる。

(2) 高いセキュリティを保つ仕組み

電子マネーシステムのセキュリティで特徴的なのは、上で少し触れた耐タンパー性である。ここでは、耐タンパー性を実現する仕組みについて簡単に解説する。

①耐タンパー性とは

かつて、米国のテレビ映画として人気を博し、劇場映画にもなった『ミッション・インポッシブル』に、ミッション（指令）を再生したテープが「このテープは自動的に消滅する」と言って焼失してしまうおなじみのシーンがある。ミッションの内容が敵に知られないようにする仕組みである。これと同じように、耐タンパー性は、内部の情報を解析されたり改ざんされたりすることに対する防御力を意味する。耐タンパー性を実現する方法には論理的なもの（プログラムにより実装する）と物理的なものがある。物理的な方法では、装置やメモリーから情報を解読しようと試みると、情報が読み出せないように内部回路が破壊される。通常、電子マネー（ICカード）には物理的な対策がとられている。

②耐タンパー性を実装したHSM

上記の耐タンパー性をハードウェアとして実装し、暗号鍵情報などの重要な情報を格納する機器がHSMである。HSMは、格納された鍵情報を使って暗号化・復号処理プログラムを機器内部で実行する。これにより、鍵情報を露出させることなく、安全に決済などの処理を行うことができる。

セキュリティと利便性の両立

電子マネーシステムは、セキュリティを高めるため、定期的もしくは各種条件が合致した時に、リーダー／ライターとサーバー機器が通信を行うようになっている。通信の間は利用者はICカードをリーダー／ライターにかざしていなくてはならず、また通信は通常WAN（広域通信網）回線を経由するため処理時間が長くなり、スピーディーな決済という利便性が損なわれることになる。そこで、さまざまな工夫を行ってかざす時間を最小限に感じさせるようにする必要がある。

そのためには、リーダー／ライターとサーバー機器の通信時間をたとえば2秒以内にするなどの性能目標を決める。これを実現するには、まず業務要件と処理内容を精査して、一連の処理を利用者のかざす動作に直接関係する部分とそうでない部分に分ける。次に、直接関係しない部分はバックグラウンド処理として利用者に処理を感じさせないようにする。かざす動作に関係する部分は、データベースのテーブル設計や電文設計などを工夫することで処理時間を短縮する。これにより処理時間を1秒程度にすることも可能である。

電子マネーシステム構築における留意点

電子マネーシステムを構築するプロジェク

トでは、セキュリティ面で通常の業務システムとは異なる施策が設計段階から必要である。以下では、秘密保持契約、情報の重要度のレベル分け、および権限の分散について、その要点を述べる。

(1) 秘密保持契約の締結

外部のベンダーに作業を委託する場合、秘密保持契約の締結は当たり前のことであり、普通に行われているであろう。とくに電子マネーシステムは高いセキュリティが求められる情報を扱うため、プロジェクトに参加する企業は秘密保持契約の締結が必すとなる。ベンダーとは、たとえプロジェクトへの参加が確定的な場合であっても、秘密保持契約の締結が済むまでは情報連携を行わないといった厳格な運用が必要である。

(2) 情報の重要度のレベル分け

プロジェクトで扱う情報は、暗号鍵情報を含めて、常にその重要度をレベル（セキュリティレベル）分けし、レベルに応じて、仕様検討会などへの参加者を限定することなどが必要である。特に、重要度レベルの高い情報については参加するベンダーとメンバーを絞り込み、一部のベンダーの一部のメンバーしか知り得ないように情報統制を行う。たとえば、重要度レベルの低い概要的なシステム仕様や業務内容は広くメンバーに公開するが、ICカード情報を更新するプログラムのロジックや、暗号鍵情報のHSMへの格納方法などについての検討会へは、限られたベンダーやメンバーだけが参加できるようにするべきである。

このような施策は、一面では情報共有を制限するものであるため、プロジェクトの遅延の原因になり得ることは事実である。だからといって、重要情報を安易に共有させるといったことを認めてはならないであろう。

(3) 権限の分散

重要度のレベル分けとともに、情報の登録や変更の権限を一人に集中させないことも必要である。たとえばHSMへの情報の登録・変更を、権限を持つメンバーが一定数以上参加しなければできないようにすることなどが考えられる。権限を持たせるメンバーには登録・変更専用のカードを１枚ずつ渡しておく。メンテナンスなどでHSM内の登録情報を更新する際は、このカードを持つメンバーを決められた人数だけ集め、カードを交互にHSMに認識させないと更新作業ができないようにするなどの方法がある。権限分散の考え方は、電子マネーシステムでは広く取り入れられている。

電子マネーの仕組みについて、ビジネス、システム、構築プロジェクトの観点から解説してきた。既述のように電子マネーはすでに社会インフラとして定着しており、NRIは今後も消費者が安心して利用できる電子マネーシステムの構築のために努力していきたいと考えている。 ■