連載第6回

”光”新世代ビジョンを支える研究開発の動向

# エンド・ツウ・エンドで、個人と個人が簡単、確実に取引を実現できる電子価値流通技術


日本電信電話株式会社
NTT情報流通プラットフォーム研究所
冨田　清次

日本電信電話株式会社
NTTサービスインテグレーション基盤研究所
菅沼　毅


## はじめに

電子価値流通プラットフォームとは、ネットワークにおける取引の活性化と拡大を目的として、様々な価値を電子化して流通を促進する基盤である。本稿では、簡単、安心、確実な取引に向けた電子価値流通技術の状況、および、レゾナントコミュニケーション時代に向けたP2P電子価値流通技術の概要について紹介する。

## レゾナントコミュニケーションと電子価値流通

2002年にNTTがまとめた「“光”新ビジョン　―ブロードバンドでレゾナントなコミュニケーションの世界へ―」では、レゾナントコミュニケーション環境（ブロードバンド、ユビキタス、安全・確実・簡単でシームレスなユーザビリティ、エンド・ツウ・エンドのコネクティビティ）によって、「時間」と「距離」を克服し、特に、活動範囲の拡大は「商」のボーダレス化をもたらすとしている。

レゾナントコミュニケーション時代に向けては、ネットワークが「時間」「距離」の克服だけでなく、経済活動の基盤となる環境を提供する必要がある。電子価値流通がレゾナントコミュニケーションの時代に目指しているのは、企業と企業、企業と個人の取引だけでなく、個人と個人が簡単、確実に取引を実現できる世界、‘場’（環境）の提供である。これにより、‘場’というコミュニティに参加する個人・個人にとって、「モノ」「サービス」「知」の対価としての「価値」の自由な交換が可能となる。電子価値流通は、レゾナントコミュニケーションにおいて「価値」を運び、コミュニティを活性化させる、いわば触媒として機能するものである。

## 電子価値流通プラットフォーム

NTT情報流通プラットフォーム研究所、NTTサービスインテグレーション基盤研究所では、ネットワークにおける様々な取引の活性化と拡大を目的として、電子価値流通技術の開発を進めてきた。電子価値流通技術における電子価値とは、紙幣（貨幣）、チケット、商品券、会員券、引換券等に代表される多様な価値やモノやサービスを請求する権利を電子化したものである。電子価値流通プラットフォームでは、単に決済手段としての「価値」を流通させるだけではなく、商品やサービス等を電子価値の形で流通させることにより円滑な取引を可能とすることを狙いとしている。

電子価値流通プラットフォームの基礎は、電子マネーシステムと電子チケットシステムである。NTTでは、現金に近いスキームを実現するNTT電子マネー方式を発案し、システム化に向けた技術開発および日本銀行金融研究所との共同研究を実施し、スーパーキャッシュ協議会によるスーパーキャッシュ共同実験やサイバ

ービジネス協議会によるインターネットキャッシュ実験などの実証実験に適用してきた。また、電子チケットシステムの技術開発を進め、その技術は、大手チケット会社の電子チケットサービスに採用された実績を持つ。電子価値流通プラットフォームは、電子マネー、電子チケットを電子価値の流通の観点からアーキテクチャとして統合化したものである。

## 電子価値流通プラットフォームを構成する技術

電子価値流通プラットフォームでは、電子価値をバーチャル（ネットワーク）で流通し、リアル（店舗、イベント会場など）で行使することを想定している。電子価値の流通にあたっては、偽造や不正使用・二重使用に対する対策が必要である。また、リアルでの行使、すなわち店舗や会場などで電子価値を提示してモノやサービスを受けるにあたっては、利用者が店舗や会場まで電子価値を安全に運ぶ手段、および、実際の店舗や会場で安全・確実に電子価値の授受を実現する手段が必要である。

電子価値流通プラットフォームは、電子価値の「発行・チャージ」、「譲渡」、「行使／回収（改札・支払）」から構成されるシステムである。また電子価値の種類により行使／回収の後に発行元に利用情報が戻される「還流」を行う場合がある（図１）。

### （１）公開鍵暗号署名による偽造・改竄防止、二重使用・複製防止

電子価値流通システムでは、公開鍵暗号による電子署名を利用して、偽造・改竄、二重使用・複製などの不正防止を実現している。従来の共通鍵ベースのシステムでは暗号化と復号の際に同じ秘密鍵を使うため、回収機器に鍵を保護する耐タンパ性を有するデバイス（高価格）、例えばSAM（Secure Access Module）チップを装備するか、或いはオンラインでのセンタサーバでの認証処理が必要(通信時間や処理時間を要し、またネットワークやセンタの障害時には利用不可）となる。一方、電子価値流通システムでは公開鍵暗号を利用し、行使/回収の検証には公開鍵を使用するため、回収機器に耐タンパ性デバイス等が不要であり、オフライン（センタ等へのアクセスなし）で行使/回収が可能となるという大きな長所を有する。

偽造・改竄に対しては、発行する電子価値に対して発行者の電子署名を付与し、電子価値の受取時に電子署名を検証することにより、偽造・改竄を検出する。不正使用や否認に対しては、発行時に発行者の電子署名を、回収時に利用者の電子署名を、それぞれ電子価値の受取側が証拠として保持することにより、不正使用や否認を防止する。電子署名では、秘密鍵が漏洩すると第三者が署名生成可能となり証拠能力が失われるので、秘密鍵が漏洩しないことが必須である。電子価値流通システムでは、耐タンパ性の高いICカードもしくはアクセス制限されたネットワーク上のサーバ等を利用して秘密鍵の漏洩を防止している。また、万が一、ICカードの秘密鍵が解読された場合でも、ICカード毎に個別の秘密鍵を割り当てていることから、鍵の漏洩が発覚した当該ICカードの無

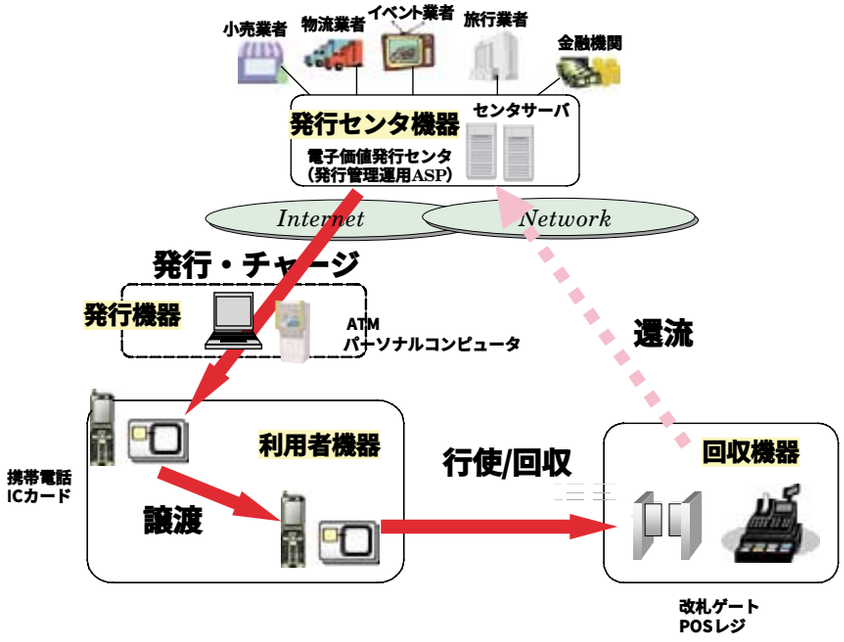


図１　電子価値の流通と構成機器

効化リストを配布し、当該ICカードのみ利用を止めることにより対処する。このように公開鍵暗号を利用していることから、万が一、鍵が漏洩した場合でもシステム全体の崩壊は回避でき、最小のコストでシステムの運用が継続可能である。一方、共通鍵暗号に依存したシステムでは、システム共通の鍵の漏洩がシステム全体の崩壊につながる恐れがあり、流通している全カードを回収・交換するといった事態に成りかねないため、公開鍵暗号によるシステムの優位性は明らかである。

二重使用・複製に対しては、これらを防止する為、電子価値を安全に管理できる物理的媒体を用い、秘密鍵と同じくICカードまたはアクセス制限されたネットワーク上のサーバなどで管理する方式としている。また、物理的な耐タンパ性への依存だけではなく、運用技術による対処も併用し多重の対策を講じている。

### （2）チャレンジ－レスポンスによる価値移動

機器間の電子価値の移動、すなわち、電子価値の発行における発行センタ機器から利用者機器への電子価値の移動、譲渡における利用者機器から利用者機器への電子価値の移動、行使／回収における利用者機器から回収機器への電子価値の移動においては、チャレンジ－レスポンスによる授受を行う。チャレンジ－レスポンスによる授受の際のセキュリティの確保については、先に述べた公開鍵による電子署名技術を核として実装している（図２）。

### （3）非接触支払いと高速性

電子マネーのリアル環境での使用には、非接触での支払いの利便性と高速性が普及のキーポイントとなると想定し、非接触ICカードを使用した高速な支払い技術の開発を推進して来た。2001年２月には、接触・非接触共用ICカードを使用して公開鍵暗号方式の電子マネーを世界で初めて実現した。

公開鍵暗号方式による電子価値流通プラットフォームは、既に述べたように不正発生時の影響範囲の局所化など、安全性の点で共通鍵暗号方式に比べ優れているが、ICカードへの適用においては処理速度が実用化の課題であった。これまで公開鍵暗号としてはRSA暗号が最も一般的であったが、安全性を確保するためには長い鍵長が必要となる※1。

また、カード内に保管する鍵データサイズ及び署名データサイズも大きくなることから利用時の通信時間も長くならざるを得なかった。さらに、RSA暗号では多くの計算能力を必要とし、処理能力の低いICカード上のプロセッサでは電子署名生成処理に大きな時間がかかっていた※2。

これに対して我々は、同レベルの安全性を確保しながら短い鍵長（160ビット程度）で済む楕円暗号方式（ECDSA）による電子署名を採用した。楕円暗号方式では、非接触ICカード上でも冪乗計算をアクセラレータ等で処理することにより、高速に署名を生成することが可能である。また、署名データサイズも小さく、通信時間が短縮できる。さらに送受信のパケットサイズの最適化をはじめとする様々なチューニ

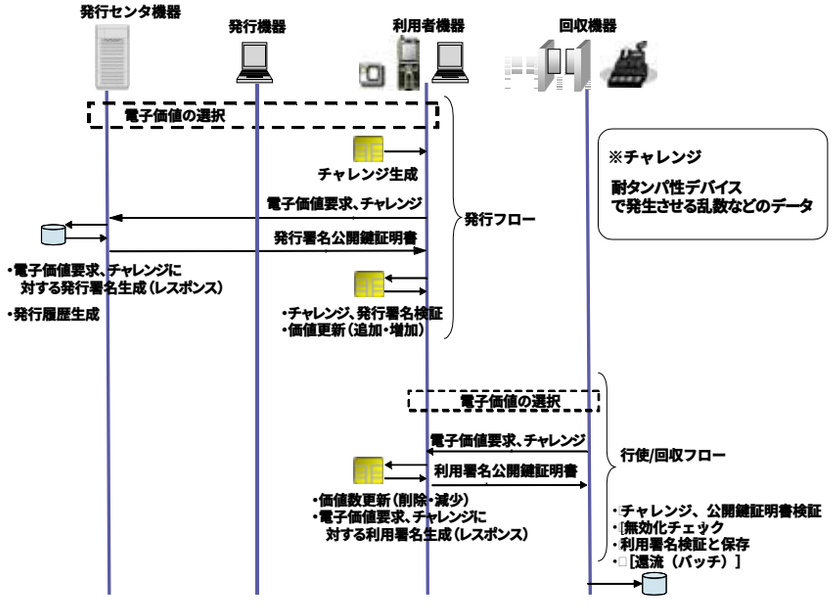


図２　電子価値の発行、行使/回収

ングとICカードとリーダライタとの通信の高速化などを実施し、2001年11月には、支払い時間250msを達成、さらに2003年３月には、共通鍵方式の電子マネーをも凌ぐ60msを達成する等、公開鍵暗号方式を利用した決済手段として世界最高水準を達成した。近年、非接触ICカードによる鉄道改札システムの普及が進んでいるが、性能要件の厳しいこの分野でも一般に高速化に有利な共通鍵方式を用いて100ms程度と言われており、公開鍵方式を用いながらこれを大きく凌いだことになる。

※１：現状、1024ビット以上の使用が推奨されている

※２：ICカードチップによってはRSAなどの暗号処理向けにコプロセッサを搭載するものもあるが、当然、これを有するチップの単価は高くなる

### （４）様々な価値への対応

電子価値流通システムでは、サービスやモノを請求する権利をXML（eXtensible Markup Language）で記述し、属性を定義するだけで様々な権利の流通を可能としている。例えばテレホンカード、図書カードやパスネットカードのようなプリペイドカードでは、基本的には通貨単位と残額の２つの属性を管理すればよいが、電子価値の場合には発行者や電子価値が保証する内容は様々であり、この多様性にXMLでの記述により対応している。

また、ICカードなどリソースの小さなメディアでの取り扱いを可能とするため、トークン方式と呼ぶ技術を開発した。有効期限、利用条件などをXML文書として表現すると、数キロバイトに達する場合もある。これでは、数十キロバイト程度のメモリしかない一般的なICカードでは、数個の電子価値しか格納できないのに加え、ICカードとリーダライタとの間の通信時間が大きくなり、実用的な性能で発行・回収ができないという問題も発生する。トークン方式では、電子価値の内容（電子価値定義と呼ぶ）と電子価値が本物かどうかを識別する認証データ（トークンと呼ぶ）を分離し、価値の所有権としてのサイズの小さなトークンのみを安全に流通させる。電子価値定義は参照やコピーを許すのに対して、所有権を示すトークンはICカード等に格納して流通させることによりコピー等を許さず、トークンの移転により所有権の移転を実現している。

### （５）様々な機器への展開、モバイルへの対応

電子価値流通プラットフォームが社会インフラとなるには、汎用性や高速性等で技術的に優れているだけではなく、様々な装置に組み込むための実装技術が重要である。そこで、POSレジ端末、ゲート装置、公衆電話、自動販売機、決済用ハンディターミナル等々、様々な機器へ組み込むための技術開発を行った（図３）。

また、近年急速に普及した携帯電話を利用者機器として、例えばPOSレジや改札ゲートで利用可能とすることも重要である。我々は、携帯電話利用の電子価値流通システムとして、ｉアプリ／赤外線通信（IrDA）を利用したシステム、二次元バーコード／RFタグを利用したシステムを開発した（図4）。二次元バーコード／RFタグによる電子


図３　様々な機器への電子価値流通技術の組み込み


図4 携帯電話を利用した電子価値流通

価値流通システムでは、改札時に携帯電話のディスプレイ上に二次元バーコードで表示した電子価値情報と、携帯電話ストラップに埋め込んだRFタグのIDを同時に読み取る。二次元バーコード自体は簡単にコピー可能であるため、RFタグのID情報を含む電子署名をバーコード情報として発行する。これにより、RFタグを所有する人以外が不正にコピーしたバーコード情報と別のRFタグを提示して場合、署名に含まれるIDとの不一致が検出され、不正利用が発覚する。

以上の方式は、現行の携帯電話機でも利用可能であるが、将来的には、FOMA等の第三世代携帯電話が有するUIM（Universal Identifier Module）カード等に電子価値格納機能を拡張することにより、電子価値の財布化が進むと考えている。

この他、リアルでの電子価値の利便性向上に向けて、金融関係を中心に普及している接触型ICカードを格納し、非接触での利用を可能とするICカードブースターやその技術を利用した表示機能付ICカードなども試作し新たな利用シーンの創出にも取り組んでいる（図5）。

## レゾナントコミュニケーションとP2P電子価値流通

冒頭で述べたように、レゾナントコミュニケーション時代に向けて電子価値流通が目指しているものは、これまでの、企業と企業、企業と個人を中心とする取引だけでなく、個人と個人が簡単、安心、確実に取引を実現できる世界、‘場’（環境）の提供である。この実現に向け、さらに個人間の取引に焦点を当てたP2P電子価値流通の構成技術に取り組んでいる。P2P電子価値流通技術により、‘場’というコミュニティに参加する個人・個人にとって、「モノ」「サービス」「知」を示す「価値」の自由な交換が可能となる。

ネットワーク上で、個人-個人間の安全・安心な取引を実現する形態としては、個人と個人の間に立つエスクローサービスなどの第三者を介在して取引を行う仲介者介在型の形態が一般的である。エスクローサービスとは、買主に商品が正常に届くまで、買主からの商品の代金を一時的に預かり、買主に商品が届いたことを確認して、その代金を売主に送金するサービスである。

エスクローの役割が介在することは、安心な取引の実現の点では優れている。しかしながら取引の内容や条件によっては必ずしも第三者を介することなく、取引を実施する当事者間で直接やりとりを実施したほうが好ましい場合も存在する。仲介者介在型では、仲介者に取引の保証を期待できる一方、仲介コストが必要となり、また技術的には仲介システムへの負荷の集中や24時間運転などが課題となる。これに対して、仲介者を介することなく当事者間で直接電子価値のやりとりが行えれば、


図5　ICカードブースター、表示機能付ICカード

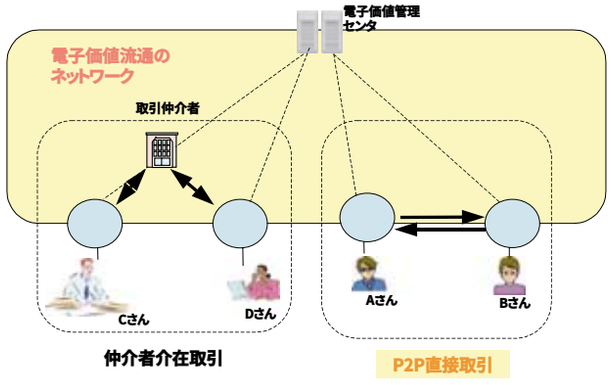


図６　P2P直接取引と仲介者介在取引

これらの課題の解決につながる。このような形態をP2P直接取引と呼び、現在、技術開発を進めている（図６）。

なお、P2P直接取引と仲介者介在取引は、排他的な関係すなわちどちらかが優れているとか、いずれかの方式に統一すべきというものではなく、取引対象・内容や条件によって適宜選択されるべきものである。

### （１）ダイレクト価値移動

電子価値の発行や譲渡、支払い／回収といった電子価値の移動には、先に述べたチャレンジ－レスポンス方式が一般的である。ネットワークにおいてチャレンジ－レスポンスによる電子価値の移動を行う場合、あらかじめ、価値の受け側から送り側にチャレンジデータの送信を行い、それから価値の送受、価値の送達確認など、複数回のインタラクションを行う必要がある。

このような複数回のインタラクションを利用者が操作するのは、利用者にとっては非常に煩雑である。インタラクションを行う代理人（プロキシ）で解決するアプローチもあるが、送り側のプロキシと受信側のプロキシ間でのインタラクションには、異常時の対処等をはじめとするトランザクションの管理が必要となり、やはり複雑なものとなる。

ダイレクト価値移動とは、価値の送り側から受け側に対して、複数回のインタラクションなしに1回で価値を移動するものであり、送り側から受け側へは非同期に送信が可能となる。P2P直接取引においては、利用者にとってもまた実現方法としても簡易に操作・構成できることが好ましいが、ダイレクト価値移動によれば、電子価値をメールなどに添付して送付することも可能となる（図７）。

### （２）電子価値交換

公正な取引は、基本的には相互に価値を交換することによってなされる。また等価な価値の交換は当事者にとって納得のいくものである。例えば、物品売買の場合は、物と金銭との等価な交換であるし、また、代金の振込みは後日という場合の取引は信用に基づくもので、物品と受取書との交換によって公正な取引と見なせる。支払いに際して、受領したことの証としての領収書やレシートを受領し公正な取引が行われた証拠とするが、これはお金と領収書の交換とみなすこともできる。

ネットワークを介した取引においては特に様々な点で不確実性を伴うことから、公正な取引の実現には公平な価値交換を基本として組み立て

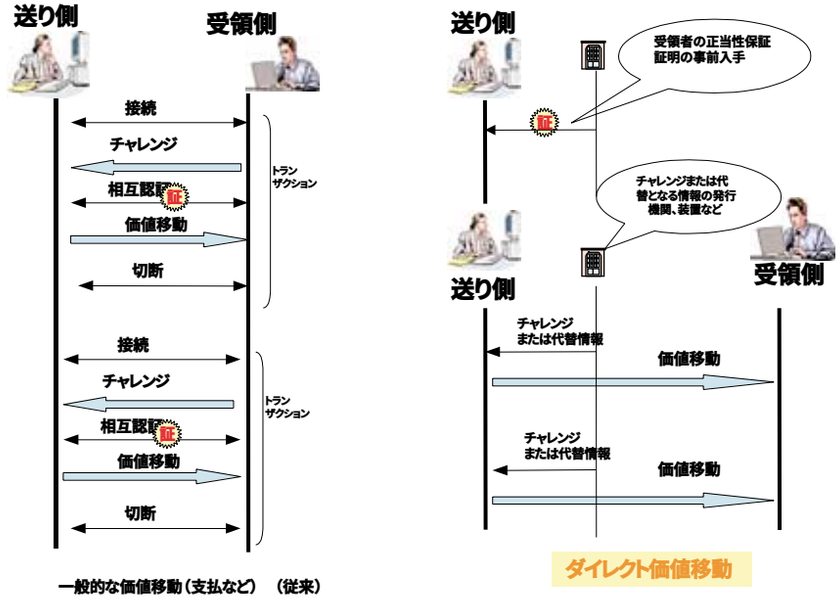


図７　ダイレクト価値移動

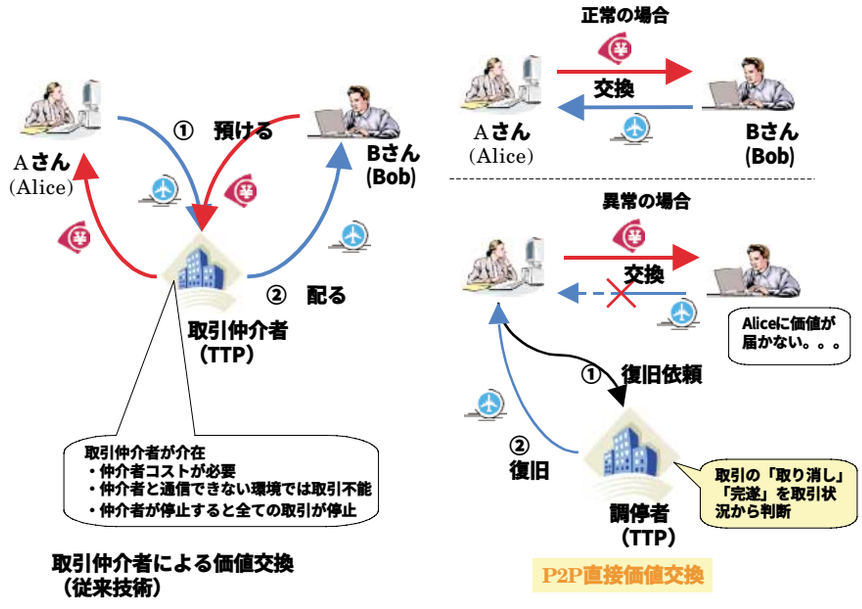


図８　公平な電子価値交換

ることが重要であるが、ネットワークでの公平な交換の実施は非常に難しい。リアルでの取引は、実際に対面で交換を行うことから、ほぼ同時に交換が実施でき、また、交換内容に不正が検出された場合には即座にその場で対処できるが、ネットワークで交換を行う場合には、同時の交換はほぼ無理であり、対価が渡されることなく持ち逃げされてしまうかもしれない。さらに、不正等が発覚した場合には、その解決は非常に困難となる。取引相手は、実は素性が知れない人かもしれないし、また、不正後、行方をくらましてしまっているかもしれない。たとえ相手が特定できたとしても、様々な理由をつけて取引事実を否認するかもしれないし、相手に渡してしまった電子価値を取り返えそうにも、既に第三者に所有権が移動しているかもしれない。このような課題を解決するために、ネットワークにおける公正な価値交換の実現が重要である。

一般的には、このような公平な価値交換には、信頼できる第三者（TTP: Trusted Third Party）を介して実施する方法がとられ、TTPが取引内容や取引の当事者の正当性確認を行うとともに、交換の責任を負う。

これに対して我々は、取引の際にはTTPを介在することなく電子価値の交換を行い、万が一不正や異常が発生した場合にのみ、調停者を介して解決する仕組みを構成する技術について検討を進めている（図8）。

当然であるが、交換に際して交換する価値、交換の当事者、第三者である調停者の正当性の保証が必要であり、これらに関しては、電子署名技術、電子価値流通技術が基盤として利用されている。

## 今後の展望

電子価値流通プラットフォームは電子価値を流通させるための基盤であり、核となるプラットフォームである。来るべきレゾナントコミュニケーションの時代に向けて、さらに個人間の自由かつ安全な取引の実現のためにP2P電子価値流通に向けた取り組みを推進している。これらは安全・確実な取引に向けた取り組みのひとつであり、レゾナントコミュニケーション時代に向けた決済・取引については、多方面から様々な新しい手段が検討される必要がある。

■参考文献
1）市川晴久、第3章：新世代ビジョンを支えるプラットフォーム技術「電子価値流通」、日経ニューメディア別冊「NTTの”光“新世代ビジョン」、日経BP社、pp.134-144、2003
2）日本電信電話、携帯電話やICカードを、安全・確実・自在に使える"夢の財布"へ 進化させる『電子価値流通プラットフォーム』を開発 －あらゆる「価値」をディジタル化して流通できる電子価値流通サービスを実現可能に－、報道発表、2003.3.24
http://www.ntt.co.jp/news/news03/0303/030324.html
3）写真で見る最先端のICカード・テクノロジー「電子価値流通プラットフォーム」のプロダクツを一挙公開！、CardWave 2003年6月号 pp.28-29、(株)シーメディア
4）Takeshi Suganuma、“Development of an Electronic Value Distribution Platform”、New Breeze 2003 No.3 Summer、pp.18-19、ITU Association of JAPAN



問い合わせ先
NTT情報流通プラットフォーム研究所
富田　清次
TEL　046-859-2065
E-mail:st@isl.ntt.co.jp