第1部

多機能ICチップ等を活用したサービスシステムの基盤整備に関する調査研究

株式会社NTT PCコミュニケーションズ　中村能章氏
NTTコミュニケーションズ株式会社　曽我哲也氏

1. まえがき

リモートでのファイル転送や保守情報の自動探索、あるいはロボットによる情報探索など、データアクセスやサービスを代行するコンピュータのソフトウェアがあります。また、決済などでは端末のIDなどから、場所や所有者を特定することがあります。これらは人と異なり、アクセス権を確認するため、人と同様にソフトウェアやサービスを受ける機器を特定する必要があります。しかし、機器には機器自身の本人性を確認する手段、あるいは本人性を示す情報を安全に格納する手段がありませんでした。

一方で機器の利用状況を考えると、一つはバイオ認証のような一意な本人確認やインタラクティブな認証が困難なことがあります。また、複数のサービスを実現するPCのようなマルチAP（アプリケーション）環境では、機器や重要な情報の盗難やハッキングを考えると、APや機器の認証や認証情報はAP毎に設定することが望ましくなります。

これらを総合すると、セキュリティや情報の利用に関する権利管理や認証には、人の本人確認手段やマルチAPの技術基盤として開発されてきた次世代ICカード技術を応用することが最も近道と考えられます。このため、多機能ICチップ（写真１）をICカードに組み込んで所有者認証をするのと同様に、多機能ICチップをPCやルータといった機器に組込んで所有者認証をするサービスの実現が有効と考えられます。

本稿では、平成16年度に実施した多機能ICチップ等を活用したサービスシステムの基盤整備に関する調査研究の概要紹介と、そこから具体的なサービスとして見え始めてきた、多機能ICチップと２階層PKI（公開鍵基盤：Public Key Infrastructure）技術を組合せたサービスのひとつである、オンデマンドVPN（Virtual Private Network）を実現する認証接続管理サービスの実現手法について述べます。

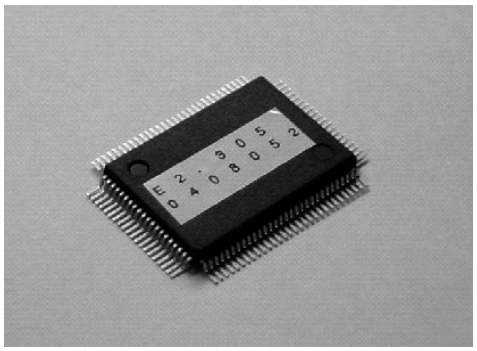

写真１　パッケージ化多機能ICチップ

2. 平成16年度調査研究の概要

平成16年度の調査研究では、多機能ICチップ等を活用したサービスを提供するための基盤となる機能の調査研究と、その基盤を利用したアプリケーションの有効性に関する調査研究を行いました。

多機能ICチップは、暗号機能、デジタル署名機能、アクセス制御と耐タンパ機能を備えることで安全性の高い認証に活用できるわけですが、チップ個体の機能のみではなく、関連するすべてのプレーヤが安全に利用できる仕組み（フレームワーク）を確立することで新しい認証ビジネスの展開が期待されます。次節でもう少し細かく記しますが、基盤のおおもととともいえるチップの正当性を担保する、チップ登録局の機能について調査研究を行いました。そもそもチップの正当性が担保されていなくては、安心して認証に利用することはできなくなってしまいます。

アプリケーションの有効性に関しては、デジタルコンテンツ流通サービスと医療システム機器等のリモートサービスの２つのテーマについて調査研究を行いました。

デジタルコンテンツ流通サービスでは、多機能

ICチップが搭載されたデジタルコンテンツ再生機器を利用し、コンテンツ（音楽等）の利用権を持っている人だけが、正当なデジタルコンテンツ再生機器でしか再生できないことを検証しました。利用権を持つことで複数の機器での再生やアルバムコンテンツに対する利用権管理、利用料や権利料の分配等について調査研究を行いました。次世代コンテンツ流通サービスでは、コンテンツの著作権を保護しながら、利用者が「安心」、「安全」、「便利」にコンテンツの流通・購入ができる仕組みが求められており、多機能ICチップ等を活用したサービス基盤の有効性が確認されました。また本研究を応用することで、コンテンツ流通サービスのみではなく、広くデジタルコンテンツの権利管理に対しても多機能ICチップが有効に活用できるものと考えられます。

医療システム機器等のリモートサービスでは、多機能ICチップが組み込まれたネットワーク機器と医療システム機器を利用し、医療機関と医療システム機器の保守事業者間でのリモートサービスモデルについて調査研究を行いました。医療システム管理分野では、インターネットを利用した医療システム機器障害時の迅速な対応等の明確な課題があります。一方で医療機関内では、カルテ等の極めて秘匿性の高い個人情報が扱われており、ネットワークアクセス時には厳密な認証が求められています。医療機関と医療システム機器を保守している保守事業者間をインターネットVPNで接続し、医療システム機器とリモートメンテナンス実施者との相互認証を行います。これらの接続、認証を多機能ICチップ内に格納したPKI情報をもとに厳格にコントロールすることで、医療関連分野の求める高いセキュリティ等のニーズにもマッチした仕組みを開発しました。次節で詳しく紹介する認証接続管理サービスです。平成16年度の対象は医療機関と保守事業者間でしたが、地域医療や遠隔医療での医療機関間連携にも適用が可能であると考えられます。またさらには、医療関連分野のみならず、デジタル家電のリモートサービスや企業間ネットワークサービスにも応用が可能と考えられます。

3. 認証接続管理サービス概要

ここでは、認証接続管理サービスの実現のキー技術である２階層PKI技術とサービスの実現手法について述べます。

3.1　２階層PKI

２階層PKIは、リアルなサービスに用いる認証情報やAP情報、並びにこれらを管理するAPをICカードやセキュアチップに安全に搭載する運用技術を提供します。２階層PKIの第２階層はサービス階層であり、第１階層のPKIで所有者や機器を認証した上で機器に格納して利用されます。以下では、第１階層のサービスを実現するプレーヤについて説明します。

プレーヤは、チップ登録局、多機能ICチップのチップ製造業者、多機能ICチップを組み込んだ機器を製造する機器製造業者、これらの販売業者、機器管理者です。チップ製造業者、機器製造業者は、チップ登録局から情報管理規定に基づいて認定、あるいは必要であれば暗号化のためのPKI証明書を貰います。チップ製造業者は、チップ登録局から仮鍵または輸送鍵の配布を受け、チップをロックした状態で出荷します。機器製造業者は、チップ登録局から第１階層の証明書の配布を受けて機器組み付け時にチップに証明書を格納して製品を出荷します。販売業者は、機器をユーザに引き渡すと同時に、チップ登録局に機器の所有者名を事後登録します。以後、所有権の移転や盗難等の所有権がなくなった場合はチップ登録局に機器の無効申請を行って不正アクセスを防御します。ユーザは、この事後登録を行う際に、第２階層の証明書やAPをチップに受け取ることができます。プレーヤ間の概略ワークフローを図１に示します。

第２階層のサービスを受ける、チップ登録局へのユーザ登録（機器登録）のための認証情報を製造段階で安全に組み込む第１階層を規定したことによって、各機器の固体識別が可能になりました。また、MACアドレス（Media Access Control address：各Ethernetカードに付与されている固有のID番号）のようなIDではなく、所属組織等の属性も格納できる証明書をチップへ格納する方法まで規定したことで、成りすましや盗難等の異常事態によるセキュリティホールの発生を抑えることができるようになりました。

２階層PKIは、PKI技術を用いたサービスにおいて重要な秘密鍵の生成や鍵管理を多機能ICチップに任せます。さらに、鍵の生成や管理をシステムで一元的に管理できるため、人の介在によるヒューマンエラーが発生し難い、安全性の均質化が保障できます。また、多機能ICチップ内のAPと対になったAP情報のバックアップ環境が構築できるため、TPM（Trusted Platform Module：TCG（Trusted Computing Group：PC関連メーカを中心とした標準化団体）で定義されたセキュリティの仕様に準拠したセキュリティチップ）のような鍵の喪失でサービスのリカバリができなくなるようなこともありません。

この技術を用いれば、PKI導入の大きな阻害要因であった、従来は人的リソースに任されていたPKI

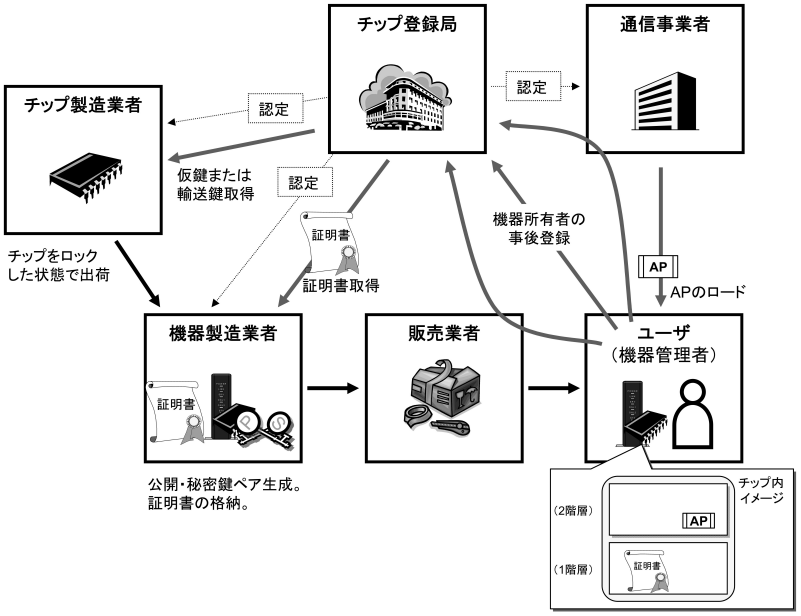

図１　第１階層のプレーヤモデル

の証明書や鍵管理がシステマティックに実現できます。これは、SOHOや個人レベルの専門知識やセキュリティ管理が不十分な分野でもPKI技術を利用して安全な情報管理ができる可能性を提示しています。

3.2　オンデマンド通信への展開

本節では、認証接続管理サービスの実現するオンデマンド通信に関するサービス要件を明確にすると共に、このサービスに関わるプレーヤとシステム構成について述べます。

(1) サービス要件

従来のセキュアな通信は、企業ネットワーク向けの専用線やIP-VPN、Webのようなユーザサービスをターゲットにしたssl（Secure Socket Layer：インターネット上で情報を暗号化して送受信するプロトコル）のようなものが代表的でした。前者は、セキュリティポリシーが同一のイントラ環境に用いられることが多く、ミッションクリティカルな業務系処理向けに静的なネットワークを構築していました。後者は、オンデマンドでのサービス要求に応じてWebに接続する場合の転送情報の秘匿に用いられています。現在は、前者のVPNを後者のインフラとして使われる、より安価なインターネットに転換する動きが顕著になっています。

この場合、VPNについては盗聴に対する安全性だけが語られ、通信していない時間帯における外部からの攻撃に対する対策はあまり議論されていません。従来のファイアーウォールやVPNパラメータによる通信路形成は、パラメータの払出しや管理が人手に任されており、人為的にパラメータ操作ができる手段が残されているため、どうしてもハッキングを防ぐことができない問題を内在させています。このような企業間通信において安全なネットワークを構成するには、オンデマンドでリモートサービスが実行される環境での類似の検討されたものをベースに機能検証することが最も有効です。

医療分野では、医療情報自体が患者の個人情報であり、欧州のPrivacy Directive（1995）や米国のHIPAA（1996）に代表されるプライバシー保護関連の法律、並びにこれらに基づいたシステム化が早々に行われてきました。これらの欧米の法制度化に合わせて、日米欧三極の医療画像工業会が作ったSPC（Security and Privacy Committee）がリモートサービスに関するガイドラインを策定しています。さらに、このガイドラインを満足させる既存技術を認知しています。これらのシステム化では、署名・認証、暗号化、改ざん検知等の重要な技術としてPKIがキーになっています。一方、鍵管理や認証局等の運用コストが導入後の課題として顕在化しています。我々は、このSPC要件をベースにシステムを設計することとしました。

SPC要件は次のようになっています。

①外部からのアクセスポイントは一つに絞る。

②アクセスポイントでは、少なくともアクセス元の機関認証を行う。

③内部のアクセス先までの経路を保証できるよう

にする。
④内部でのアクセスは監視できるようにし、不正な動作があった場合は通信を切断できる。
⑤通信路は暗号化する。
⑥アクセスログは、発信者、アクセスポイント、アクセス先の三点で突合してシステム監査できるようにする。
⑦セキュリティポリシーを策定し、自身とリモートアクセス者がその遵守を担保する。

例えば数人で運営される診療所を対象に、これらの要件に合致したサービスが低コストで実現できることも要件として加え、ネットワーク機器（写真２）やサービスを開発します。

(2) プレーヤモデル

オンデマンド通信には、２階層PKIの第１階層のプレーヤに加えて、第２階層の認証局、機器管理者、ユーザ、通信事業者がプレーヤとしてはいります。第２階層のプレーヤモデルを図２に示します。

機器管理者は、所属機関を代表し、機器の所有者、多くの場合は法人を証明する証明書を発行する認証局から機器管理者とその所属機関を明示した証明書をICカードに搭載して発行してもらいます。この証明書は、オンデマンド通信に関わるサービスの利用者認証、機器に所有者を埋め込んだ第２階層の証明書の生成に用います。

機器管理者は、所属機関にある管理端末でICカードを用いて認証を受けてオンデマンド通信事業者の提供する認証接続管理サーバにアクセスします。機器管理者は、ユーザが通信サービスを受けるために次の事前設定を行います。

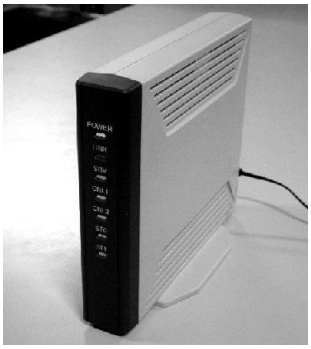

写真２　多機能ICチップ搭載ルータ

①機器管理者は、所属機関で経路管理の対象となる、すべての機器を認証接続管理サーバに登録する。
②機器管理者は、管理対象となる通信経路をすべて認証接続管理サーバに登録する。

ユーザは、機器管理者が認証接続管理サービスに関わる設定をすべて終わった後に、端末からAPを起動して通信相手に直接発信して通信パスを形成します。このとき、通信路の形成には、認証接続管理サーバが作成した認証用の第２階層の証明書が配布されます。この第２階層の証明書は接続機器の中に閉じ込められるため、人為的に成りすましをすることができません。

(3) システム構成

本節では、システムの構成概要について述べます。本システムは、通信事業者の提供する認証接続管理サーバとユーザの購入したオンデマンド通

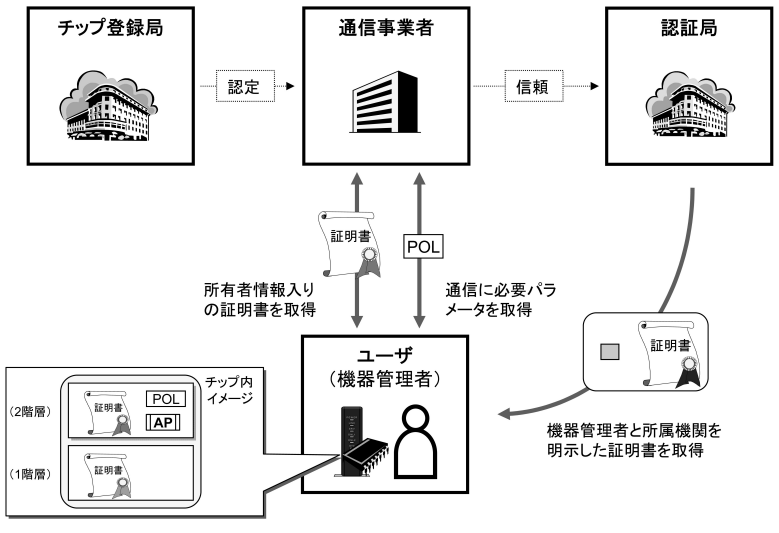

図２　第２階層のプレーヤモデル

信用ルータ（セキュアコネクタ）と端末アダプタ（セキュアアダプタ）で構成します。

認証接続管理サーバは、プレーヤモデルの項で記述したように機器管理者向けのルート管理サービスを提供します。セキュアコネクタやセキュアアダプタは、認証接続管理サーバからオンデマンドで、組み込まれた多機能ICチップにサービス情報を書き込みます。

セキュアコネクタは、IKE（Internet Key Exchange：暗号化方式の決定や鍵の交換、相互認証に使われるプロトコル）認証とIPSec（IP Security Protocol：インターネットで暗号通信を行うためのプロトコル）通信ができるセキュアネットワークと、インターネットアクセスができるノーマルネットワークの二つのゾーン管理ができるルータです。セキュアコネクタ間は、グローバルアドレスで直接接続、認証を行います。セキュアアダプタは、PCのLANアダプタとしてICカードによるアクセス者の可否の認証を行います（図３）。

システムの設計方針を明確にするため、サービス要件に基づいたオンデマンド通信の設計方針について述べます。

①外部からのアクセスポイントは一つに絞り、ここで認証接続管理サーバの発行した第２階層の証明書で接続機関の妥当性を認証する。
②アクセスポイントの認証情報に基づいて設定された経路の端末やサーバにルーチングする。接続先では、選ばれた接続形態よって、発信者の認証や機器の認証を行って二重に不正アクセスを防ぐ。
③無線LAN等での内部盗聴を防ぐため、内部の通信路も暗号化が選択できるようにする。また、アクセス監視ができるように、ルータでは暗号化を一旦解いて不正動作の検出ができるようにする。
④通信路は、通信相手毎に異なる証明書を用いてIKEで認証を行い、IPSecで暗号化して伝送する。
⑤発信者、アクセスポイント、アクセス先の三点で突合してシステム監査できるように時刻合せ機能をルータに具備する。
⑥相手が接続して安全か、接続すべき相手か確認するため、通信を行う相手同士がお互いに接続要求を挙げた場合にのみ接続を許可するコ・オンデマンド通信で通信経路を保障する。これによってセキュリティポリシーの遵守対象を限定かつ担保する。盗難、接続拒否等のステータスの変化に対しては、即時にすべての関連機器の情報を変更して不正アクセスの発生を防止する。

4. あとがき

多機能ICチップ等を活用したサービスシステムとして、ここで紹介した認証接続管理サービスのようなサービスの実現が見え始めてきています。これは一つの具体的な例だと思います。多機能ICチップはその名の通り、一つのチップで複数のサービスに対応することが可能です。何かをきっかけに多機能ICチップ搭載機器が広く世の中に増えることで、その可能性から、多くの付加サービスが生まれ、来たるべきユビキタス時代においての安心、安全を担保する重要な社会インフラになるものと考えます。

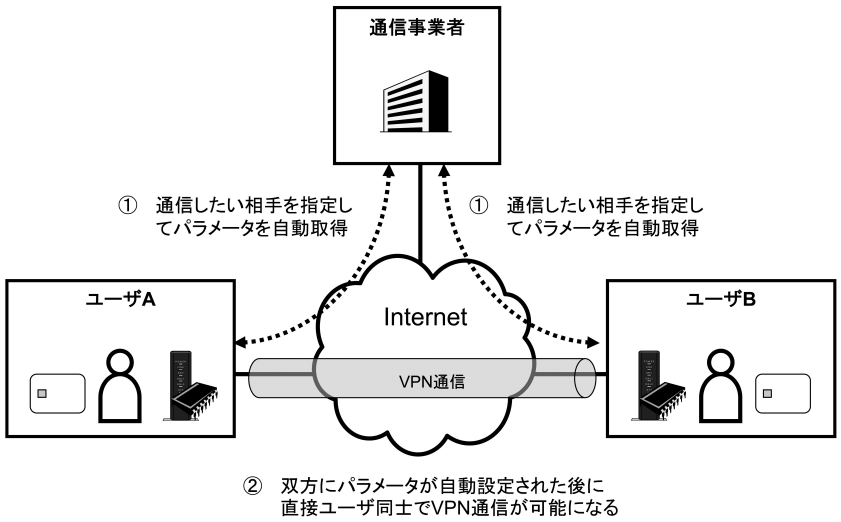

図３　オンデマンドなVPN通信