個人対応ＶＰＮ(Virtual Private Network) の外部媒体を用いた実現例

１Ｕ－８
宮川 明子　後沢 忍　稲田 徹
三菱電機（株） 情報技術総合研究所

１．　はじめに

インターネット、イントラネットの普及によって、ネットワーク上には重要な情報が流されるようになり、ネットワークセキュリティへの関心が高まっている。低コストであるこれらのネットワークを活かしながら、専用線と同等の安全性を提供する手段として VPN がある。特に、様々な情報の混在する今日では、VPN の構成単位を個人の権限に関連づけ、個人に対応した VPN を実現するシステムは非常に有効であると言える。

VPN の構成に必要な基本機能は、通信データの暗号化、ユーザ認証によるアクセス制限、暗号鍵など秘密情報の管理である。また、個人を対象とした VPN では、VPN の構成においてユーザの移動に対する柔軟性も重要である。本稿では、秘密情報の管理とユーザの移動に関わる利便性の向上のため、VPN システムに IC カードを用いた実現例を述べる。

２．　IC カードを利用した VPN システムのメリット

我々の提案する VPN システム（前出の論文 1U-06, [1]）では、VPN 管理装置で生成したユーザの秘密情報を事前に VPN 装置や VPN パッケージ内蔵の端末に設定する必要がある。この秘密情報を設定する媒介手段に、IC カードを採用した。

IC カードは、携帯性、機密性ともに非常に優れていることが大きな特長である。IC カードは、PC カード型のリーダに差し込むことによって情報が読み出せるため、ノート PC でも扱いやすい。また、フロッピーのように簡単にアクセスできるわけではなく、専用プログラムを使わなければデータを見ることができないため、情報が漏洩する危険性も低い。したがって、IC カードに秘密情報を記録することによって、システムの安全性を高め、IC カードさえ所持していれば、端末を選ばず個人に対応した VPN を構築することができる。また、本システムでは、ユーザの IC カードの挿入／抜き取りに合わせ、システムへの接続／解除プロセスを開始する機構を設けている。

３．　システム構成

図１に IC カードを利用したシステムの構成を示す。

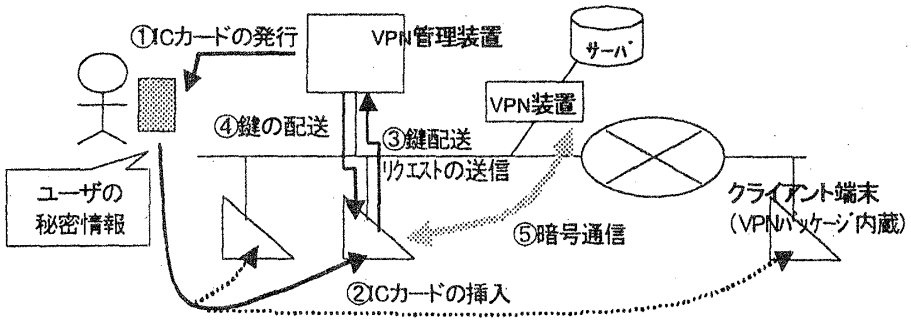

図１ ：IC カードを利用したシステムの構成

An Example of Individual VPN System based on Smartcard Authentication

Akiko MIYAGAWA, Shinobu USHIROZAWA, and Toru INADA
Information Technology R&D Center, Mitsubishi Electric Corporation 5-1-1 Ofuna, Kamakura, 247 Japan

システムを利用するユーザは、まずVPN管理装置においてICカードの発行を受ける（①）。VPN管理装置は、ユーザ情報を登録するとともにユーザの認証に必要な秘密情報を暗号化し、ICカードに記録する。ICカードの発行を受けたユーザは、VPNシステム利用時にクライアント端末にICカードを挿入し、パスワード入力する（②）。ユーザの認証に成功すると、クライアントはVPN管理装置に対して、暗号通信を行うための鍵をクライアントに配送するようリクエストを送信する（③）。リクエストを受信したVPN管理装置は、ICカードの所有者であるユーザのIDに対応した暗号鍵をクライアントに配送する（④）。この結果、同じ暗号鍵を持つクライアント同士が一つのVPNを形成し、暗号通信が可能となる（⑤）。VPNパッケージを内蔵したクライアントにICカードを挿入すれば、モバイル環境においても同等のVPNシステムを実現することができる。

4．　実現方式

図2に本VPNシステムの実現環境を示す。本システムでは、ICカードとアプリケーションのインタフェースにWindowsプラットフォームとICカードの互換APIであるPC/SC（[2]）を使用している。PC/SCに関しては、Microsoftから提供されているコンポーネントMicrosoft SmartCard SDKを利用した。

ICカード、ICカードリーダおよびリーダのドライバは、このPC/SCインタフェースに準拠した製品である。ICカード内部のファイル構造は、本システムの独自仕様とした。これらに加え、暗号化処理には当社のPowerMISTYライブラリを使用している。図2のICカード処理ライブラリは、SDKの提供する低レベルの関数群（ICカードの特定、接続、データ保存等）をICカードの処理に共通する一連の基本処理（リード/ライト、状態取得等）としてにまとめたものであり、アプリケーションは極めて平易なインタフェースでICカードをハンドリングすることが可能となった。また、ユーザがICカードを抜くと、クライアントの状態監視機構により秘密情報は端末から消去されるため、部外者の不正利用を防ぐことができる。

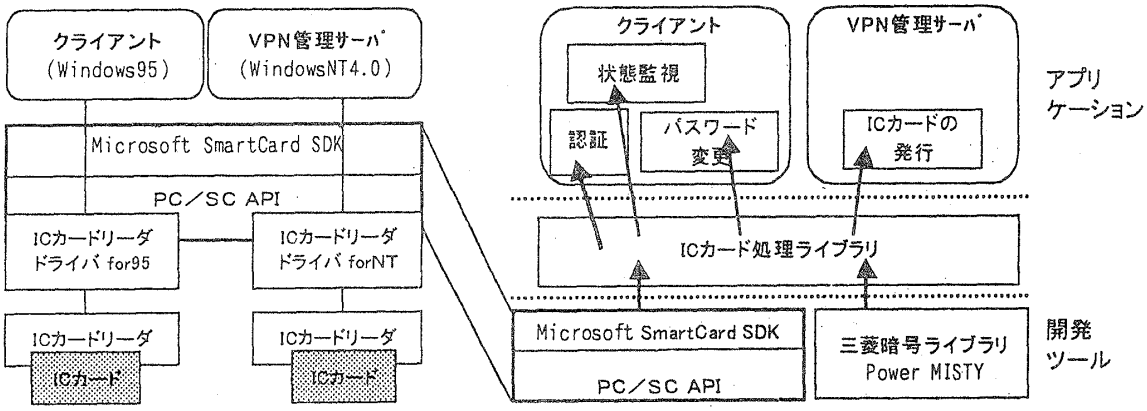

図2：本システムにおけるICカードの動作環境（左）とICカード処理の実現環境（右）

5．　まとめ

本論文では、ICカードを外部媒体に利用した個人対応VPNの実現例について述べた。今後は、大規模システムへの適用、ICカード本来のセキュリティ機能の活用等が課題である。

参考文献

[1] 後沢他, "暗号によって構成されるVPNとその管理手法", 信学技報 IN97－113

[2] PC/SC Workgroup Documents, "Interoperability Specification for ICCs and Personal Computer Systems" ,Revision 1.0, 1997（http://www.smartcardsys.com/）