Ⅰ－1 ＪＶ構成メンバー社員・出向者に対応した 生体認証連携モバイルオフィスネットワークの開発と実施

Development and commercial viability of cooperate system between SSL-VPN and biometrics system for small-scale construction sites and loaned employees

佐藤 郁[1] 渡邉 英一[2] 古田 均[3]

Iku Sato, Eiichi Watanabe,Hitoshi Furuta

IPsec-VPN を用いたインターネット VPN の導入により、作業所間のブロードバンド接続が実現したが、海外、出向者、小規模現場、JV 構成メンバーなど固定接続が困難な社員はブロードバンド化から取り残された。出向者や JV 構成メンバーなどの相手先企業のネットワークや自宅やホテル、空港などインターネット接続より、ファイアウォールやNATなどの環境内でも安全に接続する手法としてSSL-VPNを導入した。また、不特定の場所から社内へ接続許可を与えるにあたり本人を特定する必要があるため、指紋を用いた生体認証とSSL-VPNを連携させる方法を開発した。初の商用サービス化を実現し、通信費だけで従来の約35%へのコストダウンを実現した。

With The Internet VPN system of IPsec, construction sites can be connected with broadband network. But overseas sites, small-scale construction sites and loaned employees still connect with narrowband network. Because of the security system (i.e. Firewall, NAT), IPsec-VPN cannot use for the above network. And when the ID and password are stolen, it is easy to access to the company network from the world in secret. So we developed the new system that connects SSL-VPN and biometrics system simply. By using this system with a fingerprint, we can connect them safely. And we can cut cost to 35%.

キーワード： ネットワーク, SSL-VPN, 作業所, 出向者, セキュリティ, 認証, 指紋

Keywords : Network, SSL-VPN, Construction site, loaned employee, Security, Certification, fingerprint

1．はじめに

単独・JV スポンサー（以下 JS とする）作業所、営業所など、小規模拠点を ISDN によるダイアルアップ接続から、ADSL 等を用いたインターネット VPN（以下 本稿で扱う SSL-VPN と区別するため IPsec-VPN とする）による常時接続に変更[1]して約1年が経過した。移行は完了し ADSL 458 拠点、ISDN 98 拠点、FTTH（光ファイバ）12 拠点となった（図-1）。回線の選定にあたっては、優先順位を ADSL、FTTH、CATV、ISDN とした。また、この1年で日最大通信量は 4Mbps から 11Mbps へ、日平均の通信量も 900kbps から 2,700kbps と約 3 倍に増加している（図-2）。通信速度の向上とコストダウンにより、潜在化していた作業所における内外との情報交換ニーズを呼び起こした結果と考えられる。

しかし、高速常時接続環境による問題点も顕在化した。作業所のコンピュータにウィルスやワームが感染すると、作業所内部だけでなく、他支店の作業所や本支店に急速に感染が広がるトラブルが発生した。現在は作業所間の通信プロトコルを制限することで対応しているが、IPsec-VPN は作業所からの情報発信を可能とするネットワークを形成可能なことがその特徴の一つであるため、ウィルスやワームに強い OS が普及し、制限が解除できることを期待する。

一方、IPsec-VPN 接続は従来のダイアルアップ接続に比べ5倍以上の速度と72%のコストダウンを実現した[1]が、いわゆる一人現場や JV 構成メンバー（以下 JM とする）、出向者、海外勤務者は、

- 専用回線の確保
- VPN ルータの導入コスト
- VPN ルータの輸出制限

などの問題により、単独・JS 作業所、営業所、本支店などと同様の常時接続環境で社内ネットワークが利用できないという状態が生じた。これは、社内において取得可能な情

1 ： 正会員 戸田建設(株) 本社土木企画室
（〒104-8388 東京都中央区京橋 1-7-1、Tel :03-3535-1600, E-mail : iku.sato@toda.co.jp）
2 ： 正会員 工博 京都大学 教授 大学院工学研究科土木工学専攻（〒606-8501 京都市左京区吉田本町）
3 ： 正会員 工博 関西大学 教授 総合情報学部総合情報学科 （〒569-1095 大阪府高槻市霊仙寺町 2-1-1）

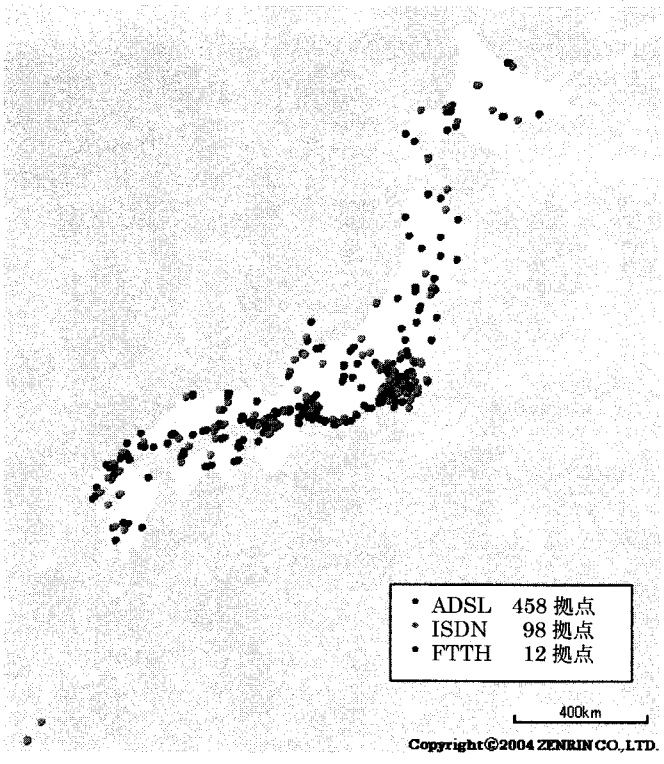


図-1 IPsecVPN拠点分布

報に格差が生じる、いわゆる「デジタルデバイド」である。これらの社員の知識や経験も、貴重な経営資源であり「デジタルデバイド」の解消は喫緊の課題であった。

そこでこの問題を解消するため、個人単位で国内はもちろん世界中から最適な環境で安全に社内へアクセス可能なネットワーク(以下 モバイルオフィスネットワーク)を開発実用化した。本稿ではまず、建設業のモバイルオフィスネットワークに必要とされる要件をまとめ、これらを満足するネットワークの開発とその実施結果について報告する。

2．目的

本システムの目的は、組織内のデジタルデバイド解消であり、どのような環境で仕事をしていても必要に応じて高速回線または常時接続回線でメールを送受信し、社内ホームページを閲覧可能な環境を整備することである。

(1) 利用対象

現在、高速または常時接続回線で社内ネットワークを利用している社員は本支店内勤および、営業所、JS、単独の作業所のうち ADSL・フレッツ ISDN による常時接続が可能な作業所である。従って、対象者は上記以外の社員となる。具体的には、

- JS 単独作業所で常時接続回線が引けない作業所の社員（以下 未接続作業所）
- 出向社員
- JM 社員

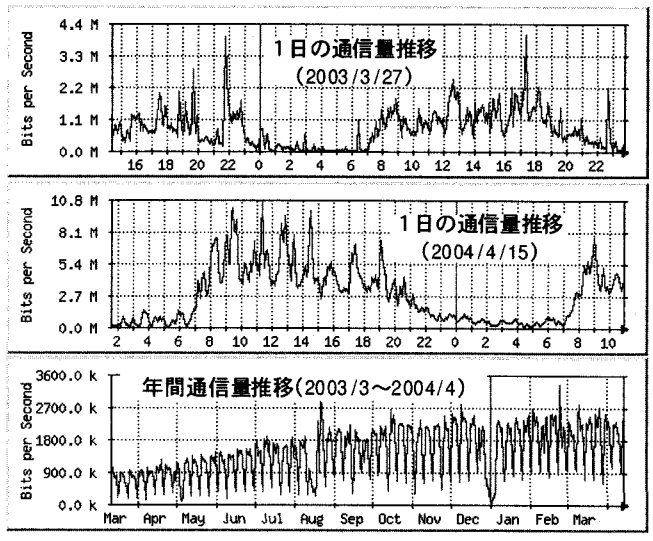


図-2 IPsecVPNの通信量(1秒間のデータ量)

- 海外社員
- 出張中社員

が対象となる。

(2) 想定される環境

利用対象者に想定される場所としては、

- 未設続作業所：事務所、自宅・宿舎
- 出向社員：出向先の企業、自宅・宿舎
- JM 社員：JV 事務所、自宅・宿舎
- 海外社員：事務所、駅、空港、ホテル
- 出張中社員：事務所、駅、空港、ホテル

などがあげられる。

また、インターネットカフェや喫茶店、ホテルなどで貸し出しているコンピュータは、キーロガーやリモート監視といった方法により、容易に情報取得が可能であるため、利用する端末は対象者が管理または所有する端末に限定する必要がある。

3．モバイルオフィスネットワークの要求条件

モバイルオフィスネットワークは不特定の場所を対象とするため、拠点間の WAN と異なり様々な利用環境を想定する必要がある。しかし、想定される環境別に接続方法を用意すると接続や管理が繁雑になり利便性が失われる。従って、想定される環境で共通に利用可能な方式を用いる必要がある。

一方、様々な環境からの接続を可能とした場合、不正アクセスや盗聴等による不正が行われた場所の特定が困難になる。従って、不正アクセスや盗聴防止のセキュリティ対策が必要となる。

ここでは、モバイルオフィスネットワークの要求条件を、

- 回線
- 端末

- セキュリティ

に分けて考える。

（1）回線

不特定の場所からの接続を行う場合、従来は社内や契約したプロバイダのアクセスポイントに設置した機器へアナログの電話回線等を利用したダイアルアップ接続を行っていた。しかし、アナログ電話回線は、距離、時間による従量制の料金であり、コストを低減させるためには、アクセスポイント数を増加させ距離を短くするか、通信速度を増加させて時間を短縮する必要がある。

一方、インターネットへの接続環境は急速に整備されており、企業内はもちろん、空港、駅、喫茶店、ホテルからは無線や有線の LAN 接続が、屋外でも FORMA（NTT DoCoMo）や WIN 端末(KDDI)などの第3世代携帯電話や PHS を用いた高速パケット通信が安価に利用できるようになっている。特に第3世代携帯電話を用いたパケット通信は高速化が著しく、ベストエフォートではあるが FORMA では 384kbps、WIN 端末では 2,400kbps を実現している。このように、インターネットは電話回線の契約などに縛られることなく利用可能となっており、モバイルオフィスネットワークの回線として最も適している。

しかし、プロバイダを通じてインターネットに直接接続するのではなく、出向先やホテルなどの企業からインターネット接続を行う場合には、企業内とインターネットとを区分けするファイアウォールなどの機器が設置されており、通信の制限や IP アドレス変換などを利用しているケースが多い。

通信の制限としては、

- プロキシ（代理）サーバによる接続先制限
- 利用プロトコルの制限

があげられる。プロキシサーバはウィルスチェック、キャッシュ、コンテンツフィルタリングなどを行うものである。また、利用プロトコルはホームページ閲覧用の http、https に制限されている場合が多い。また、IP アドレスの有効利用や外部からの不正アクセス防止の目的で、NAT（Network Address Translation）と呼ばれる IP アドレス変換を用いることも多い。

従ってモバイルオフィスネットワークは、

- ホームページの閲覧用プロトコル（http,https）を用いる
- プロキシサーバへの対応ができる
- NAT への対応ができる

が条件となる。

（2）端末

利用者端末としては、Windows を搭載したパソコンの他、Mac、Linux などの OS、Palm などの携帯端末、携帯電話などが考えられる。最も利用者の多い Windows を搭載したパソコンは対象としなければならない。しかし、携帯端末や携帯電話によるネットワーク利用も普及しており、将来、モバイルオフィスではパソコンに代替される可能性もあるため、Windows 以外の端末も視野に入れる必要がある。

（3）セキュリティ

従来のダイアルアップネットワークの場合、通信回線は電気通信事業者が管理し、電気通信事業法等により盗聴行為が禁止されているため、セキュリティは保たれていると考えられ、特別な対策はなされていない。

一方、インターネットは分散型のネットワークであり、全世界に無数に散らばったコンピュータが相互に接続され、その回線や機能を利用することで成り立っている。つまり、インターネットは特定の事業者の管理下になく盗聴行為を規制する法律も無い。また、情報が流れる経路も障害や混雑度合により変化するため、盗聴やなりすましの危険性がある。従って、インターネットをネットワーク回線として利用する場合には、盗聴やなりすましを防止するために通信内容を暗号化する必要がある。

4．暗号化通信方式

モバイルオフィスネットワークでは外部からインターネットを利用して社内の情報の送受信を行うが、送信側で暗号化し、受信側で復号化や認証を行うことにより、安全な通信を確立することが可能である。このように、インターネットなどの公共回線をあたかも専用線のように利用する方法を、VPN(Virtual Private Network)と呼ぶ。VPN には様々な暗号化方式が利用されているが、安全性が高く広く利用されている方式は、

- SSH（Secure Shell）
- IPsec
- SSL (Secure Socket Layer)

の3方式である。

（1）SSH

UNIX 系の OS では telnet や rlogin などのリモート通信でログインするためのシェル機能が用意されている。これらはパスワード認証を除き通信は暗号化されておらず、通信内容を容易に盗聴される危険性があった。SSH はこれを暗号化して安全な通信経路を構築する。

通信の認証には公開鍵暗号方式、通信については共通鍵暗号方式を採用し、OSI 参照モデル（図-3）のアプリケーション層を利用している。また、アプリケーション間通信を SSH で暗号化した通信路を使って転送するポートフォアワーディングが利用できる。ファイアウォールが構築されていても SSH が利用できればファイアウォール内外の通信が可能となる。現在は特許が切れたが、SSH は IDEA アルゴリズム特許を利用しており、特許を回避した OpenSSH が公開されるなど、仕様の統一が遅れたため、

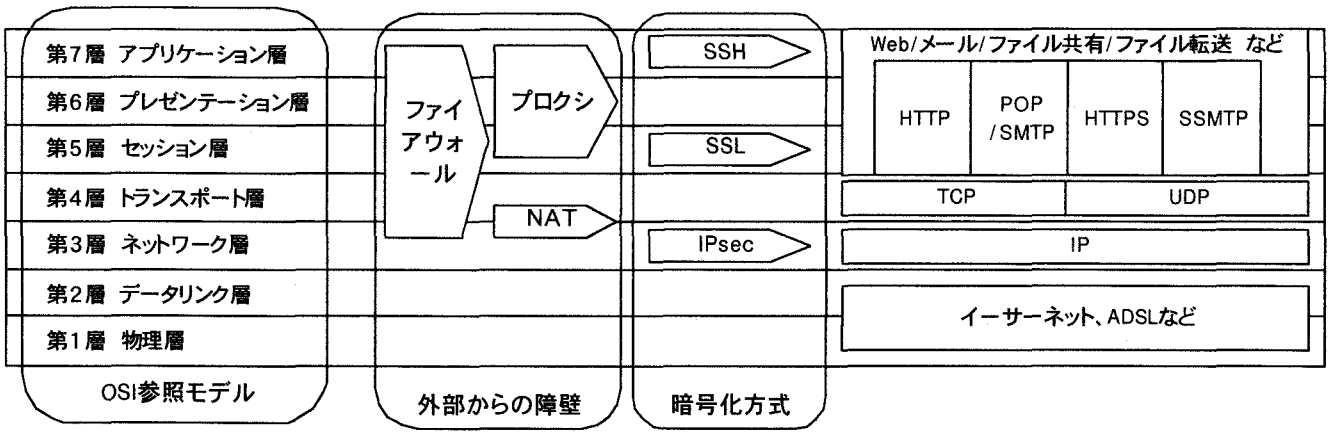


図-3 OSI参照モデルと暗号化方式

- SSH を搭載した機器の低価格化の遅れ
- ベリサイン社などの公開鍵の取得が必要

などの理由により、SSH の利用は主にサーバのリモートメンテナンスなどに利用されている。

（2）IPsec

IPsec はネットワーク層で実装され、パケット毎に暗号化を行っているため、TCP/IP を用いるどのようなアプリケーションであっても暗号化が可能である(図-3)。IETF により VPN プロトコル(RFC2401-2411,他)として標準化されており、ファイアウォールをはじめとする多くの VPN 製品に搭載されている。ネットワークの両端に器機を設置するだけ簡単に暗号化通信を実現できるため、最近ではルータなど安価なネットワーク機器にも搭載され普及が拡大している。現在実施している VPN による作業所接続においても IPsec を搭載したルータを利用している。

しかし IPsec は初期設定項目が多くソフトウエアや異なる機器を接続する場合には、機器の検証や接続パラメータの調整などのノウハウを要する。また、IPsec で用いている IKE(Internet Key Exchange)は固定の IP アドレス(インターネットを利用する場合にはグローバル IP アドレス)を持つセキュリティーゲートウェイやホスト間の暗号化を対象として開発されており、ポート番号の変更を伴う NAT や DHCP を伴う環境では利用できない。NAT を利用した環境で IPsec を実現させるためには、IPsec に対応したルータを用いるか、IPsec の拡張仕様が必要となる。出向先企業、JV の幹事会社、ホテルなどのファイアウォールの仕様変更をすることは困難であるため、IPsec の拡張仕様は現在のところ一般に普及していない。

（3）SSL

SSL は WEB ブラウザと WEB サーバ間で安全な通信を行うために、ネットスケープ社が開発したセキュリティプロトコルである。SSL の最新バージョンは SSL3.0 で、次期の SSL のバージョンから、TLS(Transport Layer Security: RFC2246)1.0 として IETF で標準化される。

また、SSL は銀行や証券会社を始めインターネット上の商取引に広く利用されているため、PC の WEB ブラウザだけでなく、PDA や携帯電話にも搭載されている(図-4)。また、サーバ側でも SSL への変換を高速に行う SSL アクセラレータも多数発売されており、WEB 暗号化の事実上の標準となっている。

SSL の暗号化は TCP パケットのデータ部分だけであり、HTTP や SMTP などのアプリケーション・データ部分だけを暗号化し、TCP ヘッダや IP ヘッダは暗号化しない。従って、ネットワーク上の機器から見れば通常の HTTP や SMTP のデータと変わらないため、SSL の通信を許可していればファイアウォールや NAT による影響をうけない。

利用上の制限としては、HTTP(80)は HTTPS(443)、SMTP(25)は SSMTP(465)など、アプリケーション毎に利用するポート番号が決まっているため、ファイアウォールがこれらの通信を許可する必要がある。HTTPS はインターネット上の商取引で広く利用されており、ホテルなどの商業施設はもちろん、企業内においてもこれらの利用を許可している。HTTP 以外のアプリケーションで SSL を利用する場合には、SSH と同様にポートフォアワーディングが利用できる。

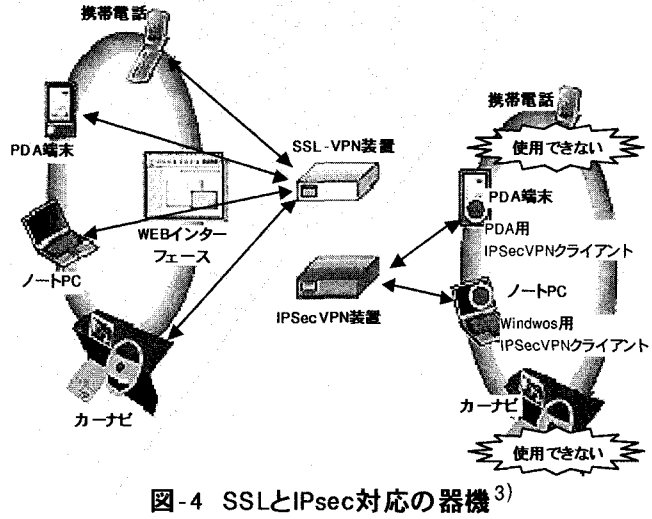


図-4 SSLとIPsec対応の器機[3)]

表-1 暗号化通信方式の比較

	SSL	SSH	IPsec
標準化	○	×	◎
対応サーバ機器	○	△	◎
クライアント	◎	○	○
NAT	○	○	×
ポート制限	○	△	×
総合評価	○	△	×

（4）モバイルオフィスネットワークに適した暗号化通信方式

以上より、暗号化通信方式の比較を表-1 に示す。SSL はネットワークの透過性も良く、携帯電話を始め多くの機器に標準機能として搭載されているため利便性も高い。従って、モバイルオフィスネットワークの暗号化通信方式として SSL を採用した。

5．認証方法

SSL を用いることにより、https が使える場所（インターネットショッピングやインターネットバンキングが利用できる端末）ならば世界中どこからでも社内へのアクセスが可能になる。また、接続回線を選ばないので、ホテルや自宅のインターネット接続はもちろん、第3世代携帯電話、定額料金 PHS、今後拡大が予想される屋外無線 LAN など、TPO に応じた最適な回線を選択することが可能となる。

しかし、この事は新たな問題を提起することとなる。現在巷を賑わしている情報漏洩防止、つまりセキュリティである。

（1）SSL と認証方式

従来のダイアルアップ接続によるリモートアクセスでは、

- アクセスポイントの電話番号
- ID
- パスワード

が必要であるが、これらの接続情報が盗まれた場合、なりすましによるアクセスが可能となり、その発見や場所の特定が困難である。

そこで、ダイアルアップ接続によるリモートアクセスを行う場合には、

- コールバック
- 識別着信（発信者番号認証）

などの認証を追加してセキュリティを強化している。たとえ、ID とパスワードを盗まれたとしても接続には登録済の電話回線を入手せねばならず、電話などが盗難された段階でパスワードを変更することにより被害を最小限に抑えることができる。

しかし、SSL は普通の WEB アクセスなので、コールバックや識別着信など電話回線を前提とした対策がとれないだけでなく、接続経路に NAT やプロクシ等が用いられてしまうと、接続時に利用されている IP アドレスさえも識別できず、接続場所の特定も不可能に近い。

一般的に対応策として、IC カードやワンタイムパスワードの利用や、使用する PC に IC カードや指紋などの読取装置を付けて PC 本体を保護する方策が取られている。しかし、IC カードやワンタイムパスワードは、盗難時の対策のために PIN 番号と言われる暗証番号を要求するが、IC カードやパソコンに付箋などで PIN 番号を記入してしまうと暗証番号の意味をなさない。また、利用者教育を十分に行って管理方法を徹底したとしても、PIN 番号に社員コードを利用する、パソコンなどの携帯品に管理番号として PIN 番号を利用したステッカーが貼り付けられているといった可能性もある。また、PC 自体を生体認証で保護する場合にも、

- 目を離したスキに生体情報を登録される
- OS の起動ディスクなどを利用してログインされる

などの危険性がある。

そこで、SSL による遠隔地接続を行う場合には、アクセス許可の段階で確実にユーザ本人を特定する方策、つまり本人認証が必要である。

（2）本人認証方式

ユーザ本人を特定する方法を安全性の高い順に示すと、

a. 本人の記憶
b. 本人の身体的特徴
c. 本人の所有物

となる。

これらの中で最も偽造が困難なのは a である。しかし、個人差はあるが、記憶は失われる可能性があるため、生年月日、内線番号、氏名など本人にゆかりのある言葉や数字を利用する傾向にある。またランダムな文字列を利用したとしても、忘れないために手帳や付箋紙などに記録した段階で本人確認方法としては有効ではない。偽造されにくい IC カードやワンタイムパスワードを利用する方法もあるが、前述のように、PIN 番号も一緒に盗難された場合には、容易になりすましが可能である。

一方、b は「生体（バイオメトリクス）認証」と呼ばれ人体の特徴を利用することから、偽造や盗難が困難であり、本人認証の方法として様々な方法が用いられている。

（3）生体認証方式

生体認証には指紋を始め、虹彩、顔、音声、サイン、掌形、血管、DNA など様々な方法がある。それぞれ特色があるが、リモートアクセスで用いるための装置としては、

表-2 生体認証読取装置の比較

	指紋	虹彩	顔	音声	サイン	掌紋	血管	DNA
携帯性	○	○	○	○	△	×	△	×
コスト	○	△	○	○	△	×	×	×
普及	○	△	△	△	△	△	×	×
心理的抵抗	△	△	○	○	×	△	△	×
総合	○	△	○	○	△	×	×	×

- 小型・軽量
- 安価
- 壊れにくい

などの条件が必要である。生体認証装置の携帯性、コスト、普及、心理的抵抗についての比較を表-2 に示す。利便性を考慮すると、特殊な装置を用いない方法が適しており、音声や顔について現在普及しているカメラ付き携帯電話の利用を検討したが、

- 海外で利用できない
- 利用環境（背景や騒音など）の影響を受ける

等の理由により採用を見送った。

一方、指紋は読取装置の低価格化が進み、特徴の抽出・認証アルゴリズムの開発により、ナローバンドでの利用も可能となっている。しかし、指紋は犯罪捜査に広く利用されてきた経緯から、指紋は個人を特定する手段としての理解は高いものの、プライバシーの一部であるとの認識も根強く、指紋登録への抵抗が少なからずある。また、指紋が薄い人や特徴点がとりにくい場合には利用できないという問題点もあった。また、読み取り装置やガラス面への指紋の残留、ゴミの付着によって、誤認識を生じる場合もある。

そこで、感熱式スイープ型指紋センサ（図-5）と周波数解析法による認証方式によりこれらの問題を解決した。

従来の指紋センサは指を置く面型の読取装置であったが、感熱式スイープ型指紋センサは棒状のセンサ上で指を滑らせて指紋を読み取る。棒状のセンサが指表面の凹凸による温度差を、連続して短冊状にスキャンすることで、指の横長極小領域の凹凸情報を取得する。しかし、スイープ型で従来のマニューシャ法（図-6）とよばれる特徴点の位置関係を利用した指紋認証アルゴリズムを利用するためには、ファックスのように一定速度で指を動かしてスキャンしなければならず読み取りが難しい。そこで、得られた凹凸情報を横方向にスライスし、その断面を波形とみなし、この波形のスペクトル系列を用いた、「周波数解析法」（図-6）という新しい指紋認証アルゴリズムで解析することで、高精度の指紋認証を行うことが可能になった。

さらに、「周波数解析法」ではサーバ上に指紋画像が直接保存されないため、指紋採取への抵抗も少ない。

このセンサは 35(W)×74(D)×18(H)[mm]と小さく、重さも

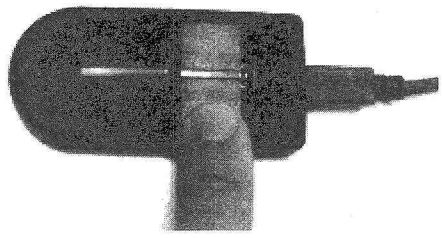
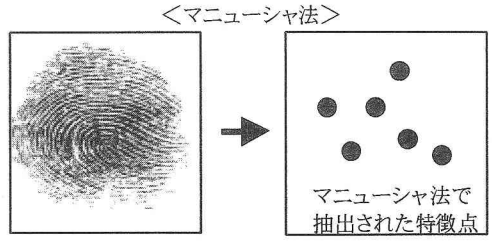
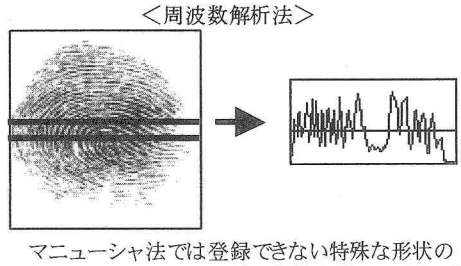


図-5 感熱式スイープ型指紋センサ



特徴点のしきい値を10個に設定したマニューシャ法アルゴリズムの場合、6個しか特徴点がとれないような指紋は登録できない。



マニューシャ法では登録できない特殊な形状の指紋(同心円に近い形状の指紋など)でも登録が可能

図-6 マニューシャ法と周波数解析法

25g 程度と軽く、モバイル用途に適しているだけでなく、棒状センサは読み取りの度に指でなぞるため、汚れの付着も少なく、残留指紋により誤認識する事もない。

現在スイープ型指紋センサは、携帯電話の FORMA (NTT DoCoMo)や PDA の iPAQ(HP)など様々な製品に搭載されており、さらに普及が拡大し低価格化が促進するものと予想される。

6．SSL-指紋認証連携システムの開発

モバイルオフィスネットワークでは、指紋認証により本人を確認した後に、SSL を用いて通信を暗号化し、社内とユーザのコンピュータとの間に VPN（以下 SSL-VPN）を構築するが、指紋認証によりSSL-VPN へのログインを許可するシステムは実用化されておらず、新たに開発する必要があった。

（1）SSL-VPN の認証方式

SSL-VPN の認証手順は図-7 のように、ユーザが SSL-VPN 装置に WEB ブラウザから接続要求を出す（①）。

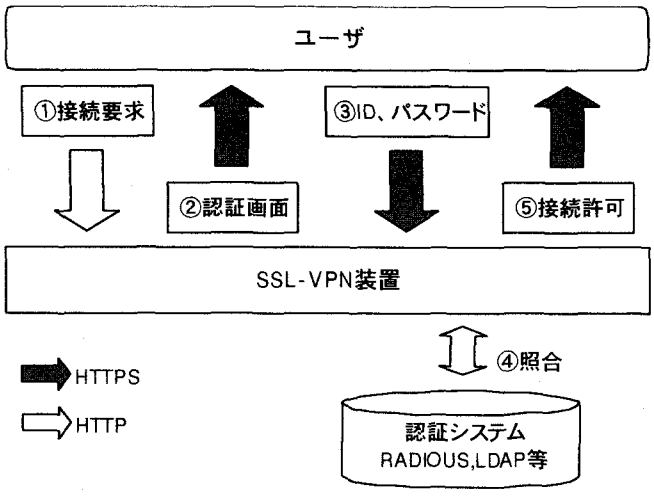


図-7　SSL-VPNの認証手順

HTTPSのセッションを確立して認証画面を表示する(②)。ユーザがIDとパスワードを入力する(③)と、SSL-VPN装置は認証システムに問合せ(④)、認証されると接続を許可する(⑤)。

SSL-VPNに生体認証を用いる場合、パスワードの代わりに指紋を用いることとなる。しかし、指紋画像は数十キロバイトあり、特徴点情報だけでも数十から数百バイトになる。一方、認証システムでサポートされるパスワード文字数は、Ciscoルータは25文字まで、PIXファイアウォールは63文字まで、RADIUS(Remote Authentication Dial-In User Service)は128文字まで、LDAP(Lightweight Directory Access Protocol)でも512文字まで等に制限されており、指紋の特徴点情報を直接扱うことができない。指紋の特徴点情報に対応させるために、SSL-VPN装置を改良することも検討したが、SSL-VPN装置は高度なセキュリティ情報を管理する装置のため、膨大な費用と時間が必要であった。そこで、SSL-VPN装置の既存認証機能を用いて指紋認証を行う方法を開発した。

(2) SSL-指紋認証連携システム

開発したSSL-指紋認証連携システムのフローを図-8に示す。まず、ユーザはWEBブラウザより、指紋認証サーバへ接続要求を行う(①)。指紋認証サーバはユーザ側で指紋認証ソフトを起動し、ユーザに指紋認証画面を表示する(②)。ユーザは指紋認証画面にユーザIDを入力し、指紋読取装置より指紋を入力する。指紋認証ソフトは入力された指紋より特徴点情報を算出し、入力されたIDとともに暗号化して指紋認証サーバへ送付する(③)。指紋認証サーバは送付された情報を復号化し、IDと特徴点情報の組合せがサーバ上に保存されている指紋の特徴点情報と同一の指から読み取られたものかを検証する(④)。同一と認められない場合にはエラーを返す。同一と認められた場合には、十分な長さをもったパスワードを生成し、認証システムへIDと生成したパスワードを登録する(⑤)。同時にユーザの指紋認証ソフトへも認証許可の情報と新しく生成したパスワードを暗号化して送付する(⑥)。

ユーザの指紋認証ソフトは復号化した情報から認証許可を確認すると、SSL-VPN装置へ接続要求を行う(⑦)。SSL-VPN装置はHTTPSのセッションを確立し、認証画面を送付する(⑧)。指紋認証ソフトはこの認証画面に、IDと直前に指紋認証サーバから送付されたパスワードを入力しSSL-VPN装置へ送付する(⑨)。SSL-VPN装置は送られてきたIDとパスワードを認証システムに照合する(⑩)。認証システムはSSL-VPN装置から送られたパスワードと指紋認証システムにより登録されたパスワードを照合しする。これらが一致した場合にSSL-VPN装置に認証情報を送付し、SSL-VPN装置は接続を許可(⑪)し、指紋認証ソフトへ初期画面を送付する。指紋認証ソフトは初期画面を

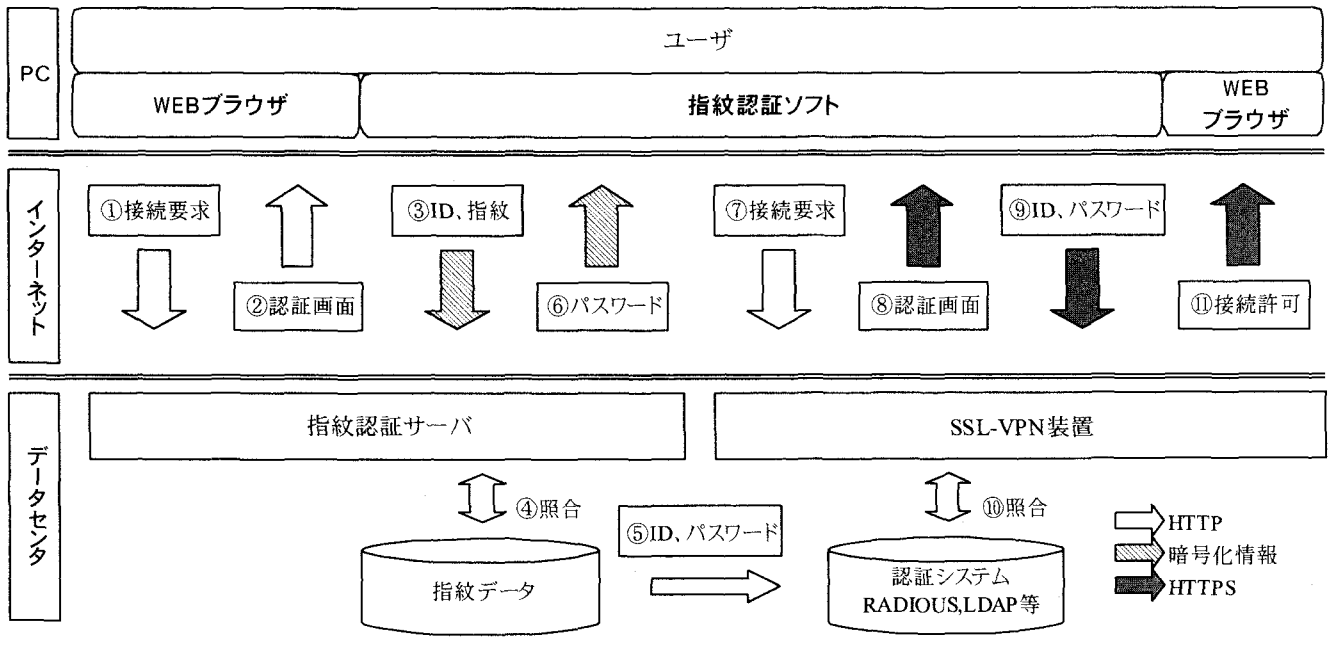


図-8　SSL-VPN、指紋認証　連携システム

表-3 PHS、携帯電話料金比較

2004年4月現在

社名	プラン	速度* (kbps)	40MB ダウンロード時	
			時間 (分)	月額 (円税別)
KDDI	標準	14.4	379	35,648
	高速	144	38	35,948
	シングル	2,400	2	34,268
	パケット割WINミドル	2,400	2	8,192
	パケット割 WIN スーパ	2400	2	7,500
ドコモ	FORMA	384	14	51,293
	FORMA(パック 20)	384	14	36,668
	FORMA(パック 40)	384	14	20,284
	FORMA(パック 80)	384	14	11,900
	DoPa(ベーシック)	28.8	190	67,236
	DoPa(ミドル)	28.8	190	50,536
	DoPa(フラット)	28.8	190	18,304
vodafone	データバリューパックレギュラー	384	14	5992
	データバリューパックスーパー	384	14	10,600
DDI	パケコミネット	32	171	8,530
	つなぎ放題	32	171	5,800
	つなぎ放題＋128K	128	43	9,300

* 速度は最高速度

**ダウンロード時間および費用は最高速度より計算

受け取ると、WEB ブラウザに画面を表示し終了する。

（3）SSL-指紋認証連携システムの特徴

本システムは、パスワード長やその方式を自由に設定できるため、RADIUS、LDAP などパスワード長の異なる種々の認証システムと連携することが可能である。また、通信機器や OS など認証を伴うシステムの多くは、RADIUS、LDAP などの認証システムと連携が可能であるため、これらの認証システムを容易に指紋認証システムへ変更することが可能である。また、本方式は指紋だけでなく顔や音声などのシステムでも利用可能であり、要求されるセキュリティに合せて利用することができる。

7．通信手段

モバイルオフィスネットワークで利用可能なリモートアクセス環境としては、家庭や事業所内のインターネット接続の他、携帯電話、PHS、無線 LAN などがある。携帯電話、PHS などのデータ通信は通話時間による従量制から、パケット課金に移行している。携帯電話とPHS のデータ転送量に応じた料金比較を表-3 に示す。月 40MB のダウンロードの場合は、au の「パケット割 WIN スーパ」が DDI の PHS の「つなぎ放題」に次いで安くなっており、今後のエリア拡大が期待される。

また、無線 LAN の接続拠点も全国的に拡大している。ホットスポット(NTT コミュニケーションズ)、M フレッツ(NTT

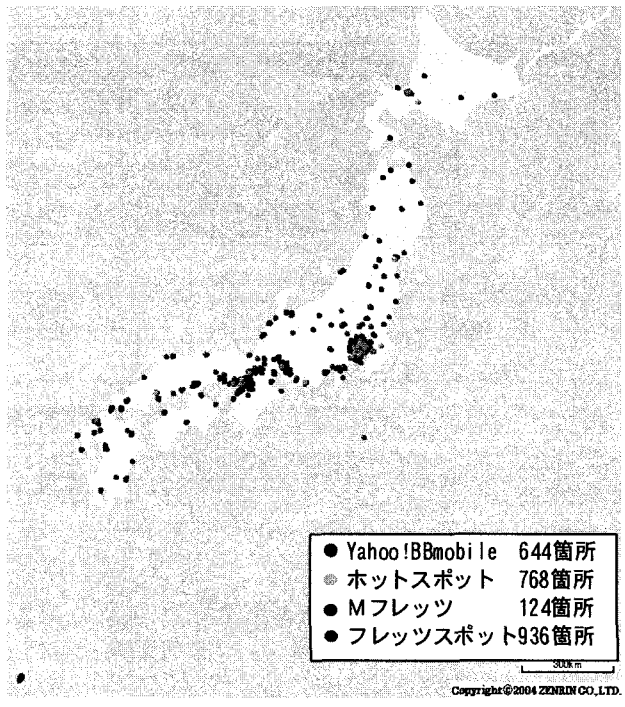


図-9 無線LAN接続拠点分布

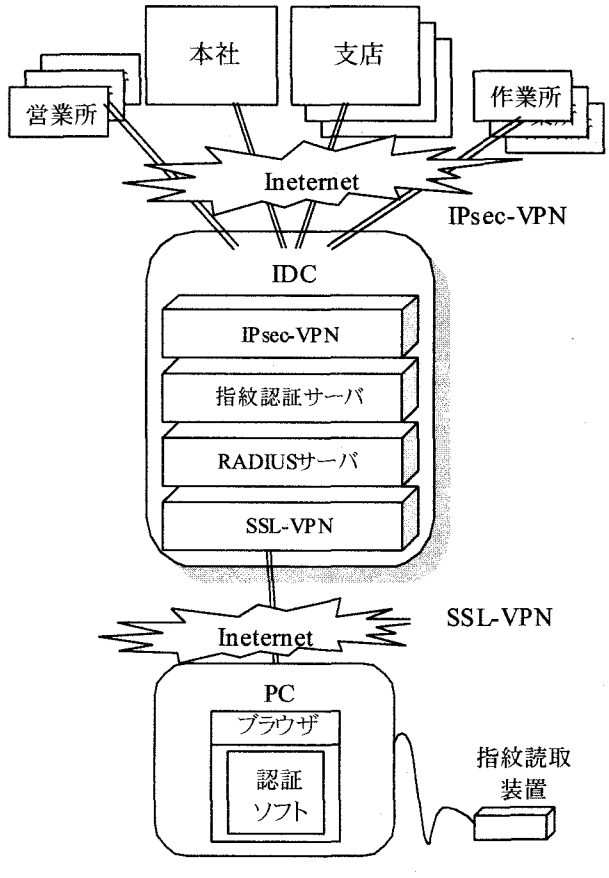


図-10 全体構成

東日本)、フレッツスポット(NTT 西日本)、Yahoo! BB mobile(ソフトバンク、BB テクノロジー、Yahoo!)の主要4社2,472 拠点でサービスが行われている。図-9 に無線 LAN の事業者別分布を示す。

8．実施状況

本システムは、2003 年 12 月より試験運用を開始し、2004 年 1 月より本稼働を開始した。海外からの接続のため 24 時間 365 日のサービスが必要となるため、第三者機関によるサービスとして実施し、筆者の所属する機関だけでも現在約100人が利用している。

（1）全体構成

本システムは図-10 のように、リモートユーザが SSL-VPN で IDC に接続すると、IDC は各拠点との IPsec-VPN によって接続されているため、各拠点との通信が可能となる。

機器構成は IDC に設置した、

- 指紋認証サーバ
- RADIUS サーバ
- SSL-VPN サーバ

と、クライアントPCに実装された、

- 指紋読取装置
- 指紋認証ソフトウエア

で構成した。

（2）認証手順

ユーザは、WEB ブラウザを利用して指紋認証サーバのホームページにアクセスする。この画面に ID を入力し、指紋読取装置より指紋を入力する(図-11)。入力後、指紋認証サーバより認証結果が通知され、許可されると SSL-VPN サーバへ転送され社内のホームページが自動的に表示される(図-12)。ユーザはパソコンのブラウザで、指紋認証システムの URL へのショートカットを選択して、パスワードの代わりに指紋をスキャンさせるだけで特別の操作は必要なく、ユーザにやさしいシステムとなっている。

（3）指紋情報の登録

ID と指紋特徴点情報の登録作業は本システムの要となる。生体認証は本人確認の手段であり、ID と指紋が一致することで本人と保障しなくてはならない。従って、指紋登録作業は申請者が本人であることを確認するため、社員データベースの写真と比較し、本支店の管理部で行われている。従って、出向者や海外勤務者は指紋登録のために本支店へ出向かなければならない。指紋データは1ユーザにつき3指まで登録を可能としている。システム性能としては 10 指まで登録が可能であるが、照合スピードと指のケガなどへの対応から、効き指と左右1指づつの3指とした

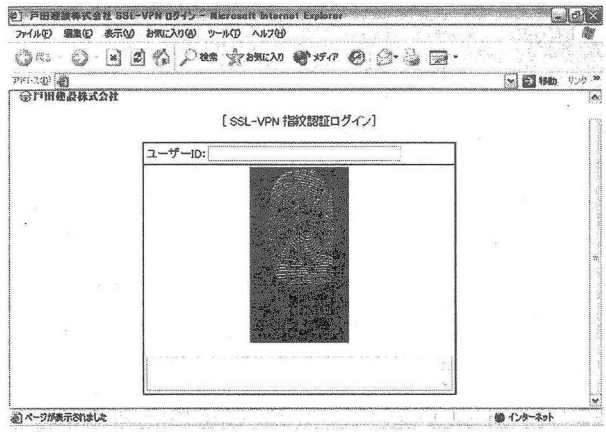


図-11 指紋入力画面

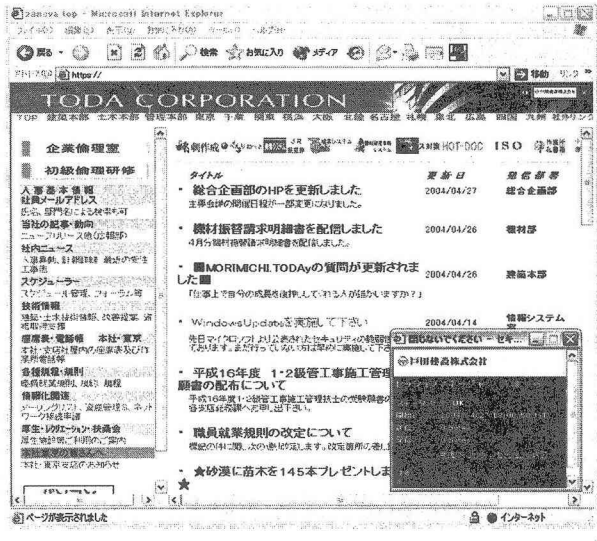


図-12 ログイン後初期画面

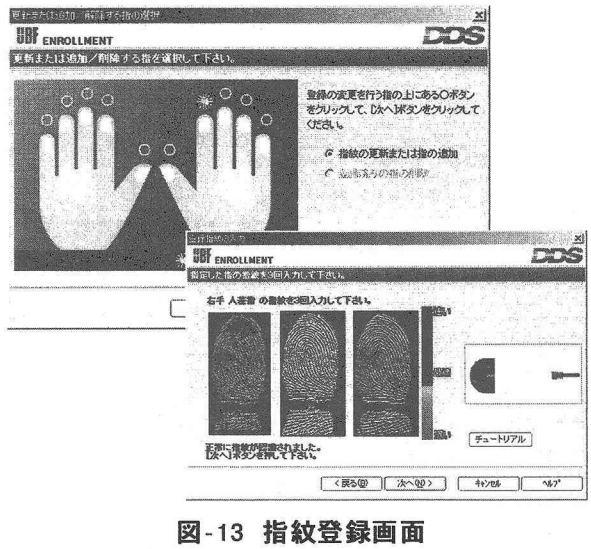


図-13 指紋登録画面

(図-13)。

（4）認証速度

認証に必要な速度はクライアントPC の性能や認証サーバまでのネットワークの状況に影響される。従って、クライ

表-4　接続形態別通信速度比較

	SSL-VPN(A)	外部*1(B)	比(A/B)
ADSL*2	1,641	1,136	144%
無線LAN*3	2,833	3,130	91%
PHS128K*4	100.0	83.5	120%
PHS64K	56.7	54.7	104%

*1: BNR スピードテスト
(http://www.musen-lan.com/speed/)により計測
*2: eAccess(Biglobe) リンク速度 2048kbps
*3:Yahoo! BB Mobile マクドナルド東京駅店で計測
*4:KWINS(KCCS) ベストエフォート

表-5　IPsec-VPN と SSL-VPN のコスト比較

	SSL-VPN	IPsec-VPN
器機費用	30,000 円	120,000 円
接続料	0 円 (JV 回線利用)	6,700 円 (ADSL*3)
VPN 利用料	5,000 円	7,000 円
年間*1	70,000 円	204,400 円
比率	34.2%	—

*1:器機費用は 36 ヶ月で算出
*2:ADSL は OCNADSL「フレッツ」8M 専用タイプで算出

アントで計測した時間は正確な認証速度ではない。参考のため、クライアントで指紋スキャナに指を当ててから認証結果が表示されるまでの時間を計測すると、1～2 秒であった。

認証速度としては十分高速であり、実用面でも問題は無い。SSL-VPN では、接続後 Java を利用した SSL-VPN ソフトウエアのダウンロードを行うため、通信回線によっては数分要する。従って、指紋読み取り(図-11)から初期画面表示(図-12)までの時間は1～2分である。

（5）通信速度

通信速度は、様々な通信条件で設置したクライアントより、SSL-VPN で接続した本社内のデータと、インターネット上の主要サイト(WebARENA、ASAHI-Net)にあるデータをダウンロードし、その所要時間より算出した(表-4)。接続先のサーバやネットワークの混雑状況の影響も考えられるが、主要サイトよりも SSL-VPN、IPsec-VPN を経由して本社内からデータを取得する方が早いという結果も得られた。

（6）コスト

IPsec-VPN と SSL-VPN のコスト比較を表-5 に示す。JM 現場で社員1名が幹事会社のインターネット接続を利用して社内ネットワークにアクセスした場合、年間約 13 万円 65%のコストダウンが可能となる。

高速で社内ネットワークに接続可能となる利便性の向上、本人認証によるセキュリティの向上などによる効果に加え、世界中の社員へセキュリティを確保した状態での情報伝達が可能になったことで、給与明細、論文集、社報などの電子化が可能になり、全社で年間数億円のコスト削減が可能になると予想している。

9．おわりに

簡易ではあるが、速度計測によれば本サービスは「インターネット上の主要サイトを利用するのと同様の快適さで社内ネットワークが利用できる」という結果となっており、SSL-VPN の有効性が確認できた。

SSL-VPN 導入で課題となるセキュリティ確保も、いわば認証の最終手段でもある生体認証を導入することで解決した。

指紋認証を導入するにあたり、利用者の抵抗を少なからず予想していたが、指紋認証を利用することで十分なセキュリティが保てるという安心感と利便性の向上による相乗効果からか、逆に積極的な協力が得られている。

指紋登録には本人確認という相応の手間が必要となるため、今回の指紋データベースは SSL-VPN に限らず他のシステムからも利用可能になっている。指紋認証は容易に本人確認ができるため、システム毎にパスワードを設定する必要がなく管理も容易であるので、近い将来、様々なシステムの入り口で指紋認証が利用されることになるだろう。

特に公共構造物はあらゆる場所に点在しているため、事業者毎に専用ネットワークを構築することは困難であり、本方式により民生用のインターネットを安全に利用することで、今後拡大が予想される維持管理業務の効率化に寄与すると考える。

一方、生体認証システムは身体的特徴を利用するため、利用対象者を拡大する場合には、指紋を読み取りにくい人などへの配慮が必要となる。本システムは様々な認証へも応用可能であるため、虹彩や音声などを組合せ、バリアフリーな個人認証システムやサービスも可能であり、利用範囲の拡大が期待される。

参考文献

1) 佐藤郁他：作業所接続に対応したインターネットVPN システムの開発、土木情報利用技術論文集、vol.12、pp. 53-64、2003年.
2) 独立行政法人 情報処理推進機構：各国バイオメトリクスセキュリティ動向の調査、http://www.ipa.go.jp/security/fy15/reports/biometrics/index.html、2004.2
3) 独立行政法人 情報処理推進機構：リモートアクセス環境におけるセキュリティ、http://www.ipa.go.jp/security/awareness/administrator/remote/index.html、2002.3

(2004.5.10受付)