セキュアリモートアクセスソリューション

中川　達実

個人向けADSLなどの高速常時接続インターネットアクセスの普及は，個人のインターネットアクセス環境を激変させるとともに，企業のリモートアクセスのブロードバンド化も促進している。一方，既存のISDN等の閉域網を使用していた従来のリモートアクセスのかわりに，インターネットを使用するには，さまざまなセキュリティ問題を解決する必要がある。本稿ではADSLや無線LAN等のセキュリティリスクの大きいアクセス手段を企業で安全に使用するためのセキュアリモートアクセスソリューションを，（株）アイピイ・ネット（以下IPnet）の構築実績を元に紹介する。

リモートアクセスの課題

個人向けの安価なインターネット接続サービスが普及してきており，従来のリモートアクセス用回線と比較すると，速度が数十倍向上している。また，定額料金でもあるため，時間を気にすることなく使用できるので，割安感がある。当然，自宅や最近各地で設立されているホットスポットなどから高速に社内ネットワークへアクセスしたいという要望が発生している。

企業側にとっても，在宅勤務，小規模事業所を実現するために必要なものでもある。

しかし，インターネットによるリモートアクセスは，図1で示す問題点を抱えている。

- 安価なインターネット接続は品質が保証されない
- 不正アクセスの危険性（各種攻撃，なりすまし）がある
- 最大／最低帯域が保証されない
- 回線に障害が発生した場合，復旧までの時間が保証されない

セキュアリモートアクセスソリューションは，これらの問題を解決するために分析，設計，構築等のサービスを提供する。

セキュアリモートアクセスソリューション概要

IPnetは，お客様の立場にたって，課題分析から幅広い技術・製品選定のコンサルティングを通じて最適なソリューションを提案している。セキュアリモートアク

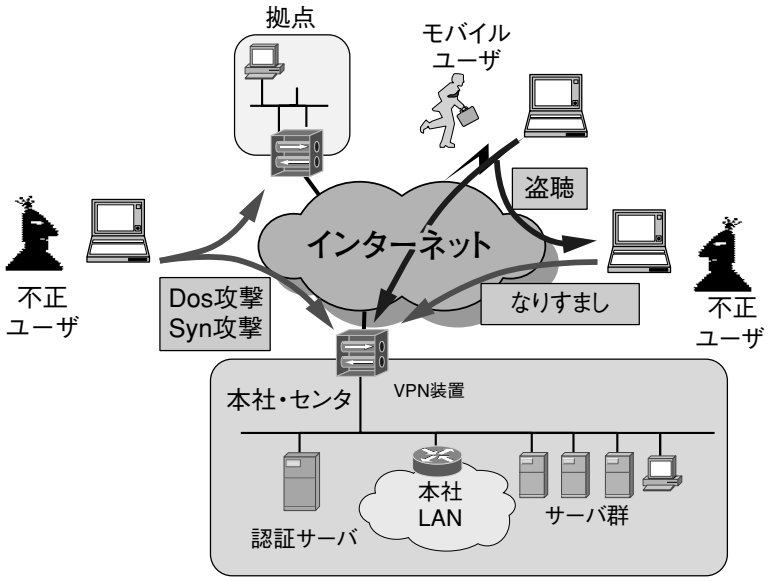

図1　インターネットの脅威

セスソリューションでは，システム導入のメリット・リスク・コストを明確にし，お客様の利用環境に合わせて安全なリモートアクセス環境を提供する。

セキュアリモートアクセスソリューションではお客様のインターネットを経由したリモートアクセス環境を考慮して，主に次の5項目を中心に問題解決にあたっている。

- リスク分析
- 通信品質
- 暗号化プロトコル
- 認証方式
- 暗号鍵管理

(1) リスク分析

セキュアリモートアクセスソリューションでは，リスク分析サービスを提供している。システムを設計／構築を行なう前に，現状および新システムにおける情報資産のリスクを分析する必要がある。リスク分析を十分にしなければ，余計なコストが増加したり，重要な情報が危険にさらされたりする可能性がある。

(2) 通信回線

リスクと要求されるサービス品質を照らし合わせて，インターネットを使用するべきかどうかを決定する。セキュアリモートアクセスソリューションでは，帯域保証が必要な拠点，ADSLが利用できない拠点では，広域LANやIP-VPN（Virtual Private Network）の併用を提案する（図2）。

(3) 暗号化プロトコル

暗号化としてIPsec，SSL（Secure Socket Layer）等の暗号化方式を決定する。暗号化方式は使用するアプリケーションや接続するリモートサイトとの関係によって決まることが多い。したがって，お客様の使い勝手も考慮すべき項目である。

現時点では，社内拠点接続や社員によるリモートアクセスならばIPsecを使用した，いわゆるインターネットVPNを推奨している。

IPsecを使用する場合，基本的にリモートサイトやリモート端末は，社内ネットワークの延長として考えられるため，情報資源へのアクセスが比較的自由になってしまう。また，暗号化プロトコル非対応のアプリケーションを使うことも多く，IPレベルで暗号化するIPsec以外の選択肢がほとんどない。問題としては，IPsecクライアントソフト等を各クライアントにインストールしなければならない場合が多いことである。これは，社内以外の接続では，受け入れ難いところである。

一方，代理店や関連会社が接続して受発注を行うシステムでは，SSLによるリモートアクセス方式が推奨される。SSLを使用する場合，クライアントは，Internet Explorer等のOSに標準搭載されているブラウザを使用することができる。これにより，SSLに対応したアプリケーション（現状ではWeb）のみにアクセスが可能になり，リモートから情報資源（サーバ）へのアクセスを制限することができる。

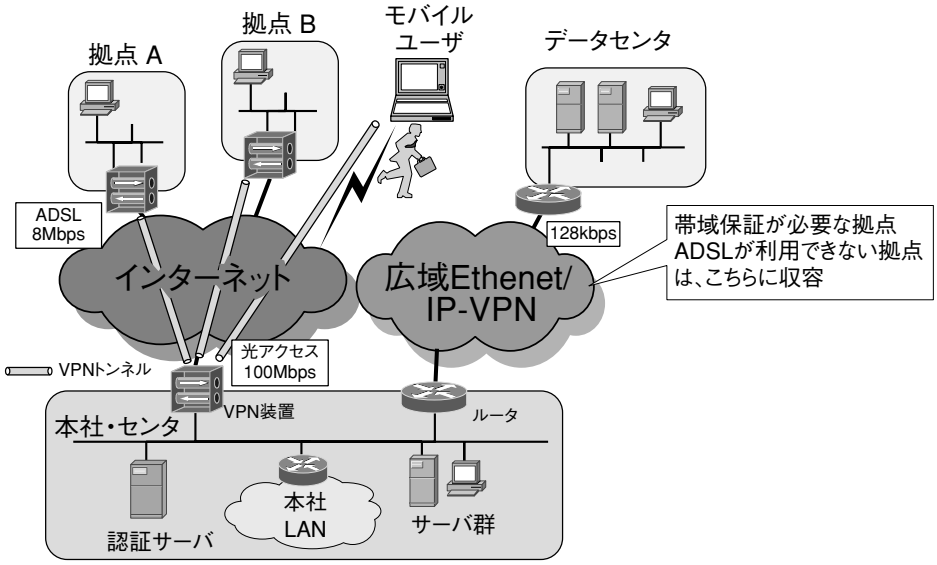

図2　インターネットVPN構成図

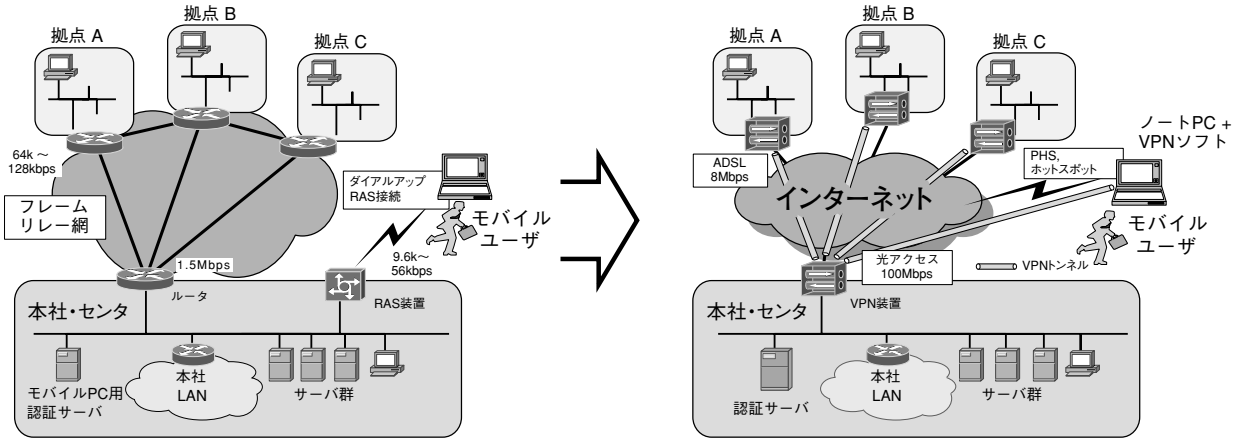

図3　リモートアクセス事例

(4) 認証方式

リモートからアクセスしてくる個人を認証するための方式を決定する。使用者の数が多いとコストや運用の手間に大きな影響を与えるが，安全のレベルを左右するため，最適な方式の選択が必要となる。セキュアリモートアクセスソリューションでは，パスワード方式，電子証明書，トークン，指紋認証等の生体認証方式を組み合わせて提供することができる。

セキュアリモートアクセス事例

図3に，A社におけるセキュアリモートアクセスソリューションによるシステム事例を示す。

このシステムは，これまで拠点間接続をフレームリレー網で接続し，社外からのリモートアクセスのために，モデムによるRAS（Remote Access Service）接続システムを構築していた。しかし，データ通信量の増加に伴い，地方拠点やモバイルユーザから不満の声があがるようになり，業務に支障をきたすまでになった。そこで，ネットワークの改変時期でもあり，A社は次期ネットワーク構築を弊社に依頼した。

IPnetでは，A社の情報資産のリスク分析を行い，運用費，可用性，セキュリティ面を検討した結果，拠点間接続とリモートアクセスをインターネットVPNで統合することを提案し，A社は採用を決定した。

これにより，セキュリティレベルを低下させずに，回線速度は飛躍的に高速化され，月額運用費は，76万円から30万円への削減。6ヶ月で初期費用も回収するコストメリットを出した。

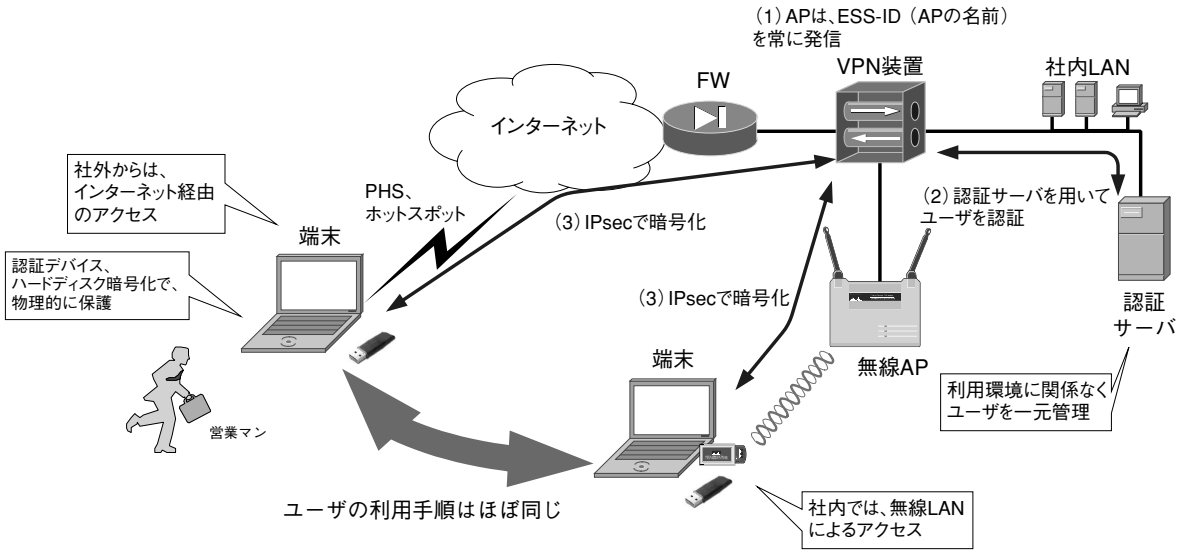

図4　セキュアリモートアクセスの応用

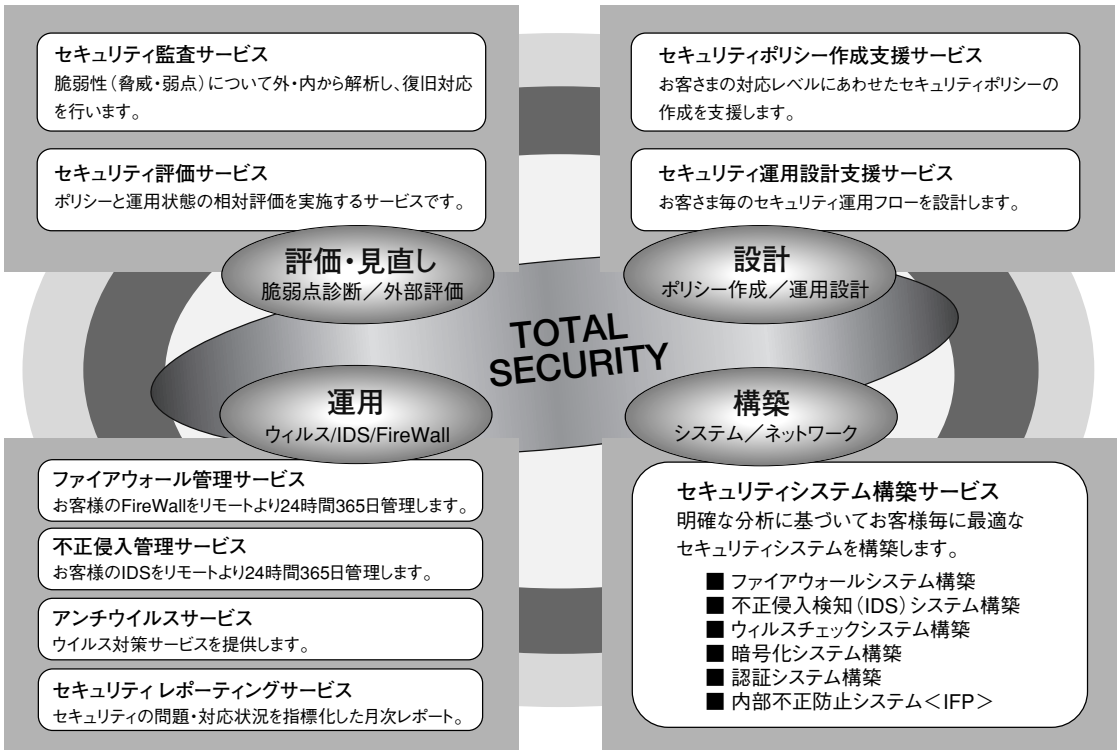

図5　IPnetセキュリティソリューション

セキュアリモートアクセスの応用

図4は，セキュアリモートアクセスソリューションの仕組みを社内で使用する無線LANにも適用することにより，モバイル端末に安全性と操作性の良さを提供した構成例である。

外出が多い営業部門等で，個人にノートPCが配布されるような環境では，社外ではインターネットVPN，社内では無線LANに接続して可搬性を高めたいという要望がある。その場合，図4のように，IPsecをインターネット経由だけでなく，無線LANでも使用することにより，以下の事項を実現できる。

- ユーザ管理の一元化
- 利用手順の単一化
- 暗号の強度化

さらに認証用トークンやハードディスク暗号化等の機能を統合して，安全度を高めたものにしている。

IPnetセキュリティソリューション

今回は，IPnetのセキュリティソリューションの内，リモートアクセスに特化したソリューションを紹介した。図5は，IPnetのセキュリティサービスを体系的に示したものである。評価／見直し，設計，構築，運用というセキュリティライフサイクルの4つのステージに分類されている。「評価／見直し」では，脆弱点診断や外部評価を，「設計」ではポリシー作成，「構築」では最新の技術と機器でセキュアなシステム構築を，「運用」では，日々運用管理を行っていく上で，管理者の負担を減らしてセキュリティレベルを保つためのサービスを提供している。

◆◆

●筆者紹介

中川達実：Tatsumi Nakagawa.株式会社アイピイ・ネット企画開発本部