

特集 3 商・材・研・究

SSL-VPN装置

リモート接続でIPsecを代替 認証システムとの連携に商機

インターネットVPN構築の新たな手段として注目を集めるSSL-VPN。これまで抱えていた「価格×アプリケーション限定」という課題も解消されつつあり、本格的な普及期を迎えようとしている。

Webブラウザ等に標準搭載されている暗号化技術「SSL(Secure Socket Layer)」を応用し、インターネットVPNを構築するシステムがSSL-VPN装置だ。

このSSL-VPN装置の市場が急速な立ち上がりを見せている。

米Netilla社の「Netilla Security Platform」を販売するアイ・ティ・フロンティア・ソリューション推進統括本部ソリューションセンターネットワークソリューション部の奥西眞弓担当部長は、「7月のプレスリリース後の4カ月間、非常に多くの引き合いを受けており、すでに50件以上の商談が動い

ている。セキュリティ製品の中ではこれまでにないほど足が早い」と語る。

また、AEP Systems社の「AEP SureWare A-Gate」を販売する住商エレクトロニクス・ネットワークソリューション事業部セキュリティシステム第1部第3課の小林邦宏氏も、「6月の販売開始から順調に出足を伸ばしている。ユーザーも大企業からSOHO規模まで幅広い層からの引き合いを受けている」と好調ぶりを述べる。

WebブラウザのみでVPN実現

従来、インターネットVPNの構築は、レイヤ3層の技術であるIPsecが

主に用いられてきたが、ここに来てSSL-VPNが注目を集めている理由は、IPsec VPNと比べた導入の容易さに加え、運用・管理負荷を大幅に削減できる点がある。

IPsec VPNを構築する場合、センター側だけでなく、接続する拠点ごとにもVPN装置を置く必要がある。また、直接クライアントPCからネットワークへアクセスする場合には、PCに専用のVPNソフトウェアをインストールしなければならない。

接続対象となる拠点多く、かつ点在する場合、初期設定作業や障害対応のための現地サポート等、情報システム担当者の負担も高くなる。

一方、SSL-VPNは標準的なブラウザを用いるだけでVPNが構築できる。面倒なインストールや初期設定も不要なため、システムに不慣れな

社員でも簡単に使える。情報システム担当者にとっても初期導入や運用に関わるさまざまな負荷から解放されるというわけだ。

しかし、SSL-VPN製品には当初2つの課題があった。「価格」と「利用アプリケーションの制限」だ。

IPsec VPN装置は、ブロードバンドルーターへのIPsec機能搭載等、急激に低価格化が進んでおり、リモート側の機器では7万円を切るものも登場している。

SSL-VPN製品は、クライアント側に専用の機器やソフトウェアを必要としないものの、センター側に設置する機器が高額なため、小規模拠点や接続するユーザーが少ない場合、IPsec VPN装置と比較して著しくコスト高になるケースがある。

また、アプリケーションの面では、IPsecはレイヤ3のネットワーク層で実装されるため、Webベースのアプリケーションだけでなく既存のメールやグループウェア、さらにはホストシステム等、通信する上位プロトコルの種類を問わない。

一方、SSL-VPNは基本的にWebベースのアプリケーションしか利用できない。既存のクライアントサーバーアプリケーションやホスト系システムを利用するには、それらをWeb対応する等のカスタマイズが生ずる。

しかし、アイ・ティ・フロンティアの奥西担当部長は、「この2つの課題はすでに解消されており、導入に対する

表 IPsecとSSL-VPNの機能比較

	IPsec	SSL-VPN
センター側装置	VPN装置	SSL-VPN装置
リモート側	VPN装置またはクライアントソフト	不要(Webブラウザのみ)
プロトコル	IP	TCP(UDP)
メリット	ネットワーク自体をトンネル化することで、どのようなアプリケーション、プロトコルでも利用可能 クライアント側にソフトまたはVPN装置が必要なため、管理面で煩雑ながら低価格化が進んでいるため導入コストを抑えられる	ブラウザさえあればどこからでもインターネットへアクセスが可能 基本的にクライアントソフトをインストールする必要がないため、管理コスト、負荷を削減できる
活用シーン	拠点間接続に効果的	リモートアクセスに効果的

ハードルも下がっている」と語る。

まず価格面については、100万円を切る製品が相次いで登場、ユーザーの導入意欲を喚起している。

アプリケーションに対する制限も解消されつつある。JavaアプレットやActiveX等の外部モジュールを用いることで、従来ではカスタマイズが必要だったアプリケーション利用が可能になっているのだ。

SSL-VPNの諸課題は解消されつつあり、本格的な普及への道筋が見え始めている。

リモート接続でIPsecに代わる主役に

インターネットVPNの主な接続形態は、拠点同士をVPN接続する「サイト間接続」と外部ネットワークから内部ネットワークへVPNで接続する「リモートアクセス」の2種類に大別される。SSL-VPNは、クライアントPCとサーバー間のVPN通信を容易に実現する点から、後者で使われているケースが多い。

具体的な事例が、営業担当者が外出先や出張先から社内サーバーへ

アクセスするというもの。特に海外の小規模駐在所から国内本社へのリモートアクセスの用途で引き合いが増えている。

また、工事現場等、一定期間だけ設営される拠点や、客先に常駐して作業する派遣社員の自社へのアクセス用途としても利用が進んでいる。

企業だけでなく、教育機関での導入も盛んなようだ。住商エレクトロニクスの小林氏は、「大学からの引き合いも多い。最近では教員、学生向けにWeb、ファイル、メールサーバーを構築し情報発信を行うところが増えており、そこでのセキュリティ確保の手段として注目を集めている」と語る。

さらに、SSL-VPNを「アウトソーシングサービス」として提供する動きも見られ始めている。

ノーテルネットワークス・アルテオングループエンタープライズチャネルズ営業部チーフネットワークアーキテクトの犬塚昌利氏が、「収益性向上のための付加価値サービスとして、キャリアがSSL-VPNを取り込み始めた」と語るように、NTTコミュニケーション