VPN環境を構築する前に学んでおこう

これが知りたいVPN

本連載では、これからリモートアクセスVPNの導入を検討している読者のために、リモートアクセスVPNにおいて利用されている技術、すなわちIPsecやPPTP、L2TP、SSL-VPNについて、それらの技術的な特徴や違いをわかりやすく解説していく。最終回は、最近注目を集めているリモートアクセスVPN技術である、SSL-VPNについて説明する。

馬場達也

最終回　SSL-VPNを使用したリモートアクセスの仕組み

Supplement

■SSL（Secure Sockets Layer）
1994年にネットスケープコミュニケーションズによって開発されたセキュリティプロトコル。TCPなどのトランスポート層とHTTPなどのアプリケーション層の間に位置するセッション層で動作し、主にWWWサービスのセキュリティの確保に利用される。

■IETF（Internet Engineering Task Force）
インターネットで利用される、プロトコルなどの技術を標準化する団体。標準化された技術仕様は、RFC（Request For Comments）として公開される。

■TLS（Transport Layer Security）
ネットスケープコミュニケーションズによって開発されたSSL3.0をベースにIETFで標準化されたもの。TLS1.0の仕様は、RFC 2246に記述されている。

■IPsec（IP Security）
IPパケットレベルで認証や暗号化を行うことのできるセキュリティプロトコル群。

■PPTP（Point-to-Point Tunneling Protocol）
マイクロソフトなどが提唱した、インターネットを利用したVPNを実現するためのプロトコル。

セッション層で動作するセキュリティプロトコルのSSL

SSLは、1994年にネットスケープコミュニケーションズによって開発されたセキュリティプロトコルであり、主にWWWサービスのセキュリティを確保する機能として利用されている。これまでにSSL2.0、SSL3.0というバージョンが開発されてきた。現在は**IETF**によって、SSL3.0をベースに**TLS**1.0と名称を変更して標準化されている。しかし、現在多く利用されているのは、TLS1.0ではなく、SSL3.0である。

SSLは、トランスポート層であるTCPとHTTPなどのアプリケーション層の間に位置するセッション層で動作する（図1）。このためSSLの機能は、通常はSSLで保護する対象となるアプリケーションに直接組み込む形で実装される。例えば、HTTPをSSLを使用して保護する場合は、Webブラウザに SSLの機能を組み込む形となる。このSSLが適用されたアプリケーションプロトコルのポート番号は、表1に示すようにアプリケーションプロトコルごとに異なる。

しかし、アプリケーションごとにSSLの機能を組み込むのでは、SSLをVPNプロトコルとして利用することはできない。そこで「SSL-VPN」では、HTTP以外のプロトコルをHTTPにプロトコル変換したり、SOCKSでアプリケーションプロトコルをカプセル化してからSSLを適用したりして、SSLをさまざまなアプリケーションが利用できるようにくふうしている。

SSL-VPNは、これまでに紹介した**IPsec**-VPNや**PPTP**-VPN、**L2TP**/IPsec-VPNとは違い、その実現方式は製品によって異なっている。唯一の共通点は、SSLを使用してVPNを構築することくらいだ。したがって、今回は代表的なSSL-VPNの実現方式についてのみ紹介する。

SSL-VPNによって提供されるさまざまな機能

SSL-VPNによって提供される機能を次にまとめてみる。

■トンネリング機能

SSLそのものにはトンネリング機能は備わっていない。このため、SSL-VPNではポートフォワーディングやSOCKSを組み合わせることにより、トンネリングと同等の機能を実現している。これらの仕組みについては、後ほど解説する。

■ネットワーク情報自動設定機能

SSL-VPNでは、SSL-VPNサーバがリバースプロキシとして動作し、リモートアクセスクライアントの代わりに内部サーバに対してアクセスするため、クライアントに内部IPアドレスを割り当てたり、内部DNSサーバのアドレスを設定したりする必要はない。ただし後述するソケットフック方式などのように、DNSサーバのアドレスをクライアントに手動で設定しなければならない場合もある。

■暗号化機能

SSL-VPNでは、SSLの機能により、**3DES**や**AES**などの共通鍵暗号を使用してアプリケーションプロトコルを暗号化する。通常は、SSLを適用するアプリケーションプロトコルが異なると、SSL適用後のTCPのポート番号も異なる。しかし多くのSSL-VPN製品では、HTTP以外のアプリケーションプロトコルにSSL-VPNを適用した場合でも、ポート番号はHTTPSと同じ443/TCPとなるようにしている。したがって、第3者によって使用しているアプリケーションプロトコルをポート番号から推測されることはない。

■メッセージ認証機能

SSL-VPNでは、SSLの機能により、メッセージ認証コード（**MAC**）を使用することでデータの完全性が確保される。このため、第3者によってデータが改ざんされても、それを検知することが可能となる。

■鍵交換機能

SSL-VPNでは、SSLの機能により、SSLセッションを開始する際に暗号化用または認証用の秘密鍵が自動的にセットアップされる。

■ユーザー認証機能

SSL-VPNでは、SSL-VPNサーバにHTTPSでアクセスすると表示される、ポータルサイトからログインすることでユーザー認証を行う。また、SSLのクライアント認証機能を利用し、証明書ベースでクライアントを認証することも可能である。

SSL適用前	SSL適用後
HTTP（80/TCP）	HTTPS（443/TCP）
SMTP（25/TCP）	SMTPS（465/TCP）
POP3（110/TCP）	POP3S（995/TCP）
IMAP（143/TCP）	IMAPS（991/TCP）

表1● SSLが適用されたアプリケーションプロトコルのポート番号

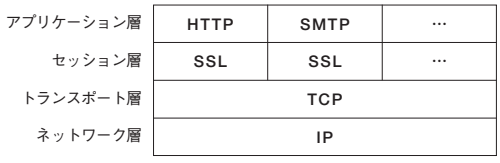

図1● SSLはセッション層で動作する

■スプリットVPN機能

多くのSSL-VPN製品では、スプリットVPNの機能が提供される。このため、企業ネットワーク内へのリソースに対してはSSL-VPN経由でアクセスし、それ以外は直接インターネットにアクセスすることが可能である。

次の機能は、SSL-VPNでは提供されない。

■リプレイ防御機能

SSL-VPNでは、悪意のある第3者が正規のユーザーが送信したSSL-VPNパケットを盗聴し、それを再利用する「リプレイ攻撃」から防御する機能は備わっていない。

さまざまな方式によって実現されるSSL-VPN

SSL-VPNの方式は標準化されていないため、製品によってさまざまである。しかし、多くの場合は次のいずれかであろう。

①プロトコル変換方式

HTTPだけでなく、FTPやWindowsファイル共有（**SMB/CIFS**）などのHTTP以外のアクセスをHTTPにプロトコル変換し、Webブラウザを介してアクセスする。

Supplement

■L2TP（Layer 2 Tunneling Protocol）
データリンク層のレベルでPPP通信をトンネリングするためのプロトコルで、PPTPとシスコシステムズのL2Fが統合されたものである。

■3DES（Triple Data Encryption Standard）
共有鍵暗号である「DES」の強度を高めるために、同暗号化方式を3重にかけるもの。DESはIBMが開発した「Lucifer」を改良して作られたもので、米国の標準暗号となった。

■AES（Advanced Encryption Standard）
米国標準技術局によって定められた、米国政府の次世代標準暗号化方式。従来まで標準暗号であったDESに代わるもの。

■MAC（Message Authentication Code）
ハッシュ関数と認証鍵を使用して生成されるもので、送信するメッセージに添付される。これにより受信者はメッセージの改ざんを検出できる。

■SMB（Server Message Block）
Windows端末などでネットワークを介してファイルやプリンタの共有を行うためのプロトコル。NetBIOS上で動作する。

■CIFS（Common Internet File System）
SMBを拡張したプロトコル。TCP/IP上で動作するので、インターネットを介したファイル共有などが可能となる。

Supplement

■ActiveX
マイクロソフトが開発したインターネットに関連するテクノロジーの総称。ソフトウェアコンポーネントであるActiveXコントロールや、ドキュメントファイルをWebブラウザ上で直接開いて参照することができるActiveドキュメントなどが含まれる。

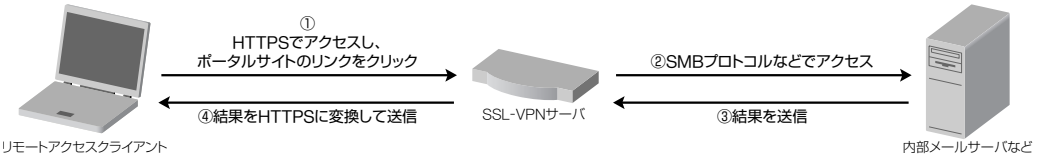

図2● Webブラウザ経由でSSL-VPNを利用する方式の動作

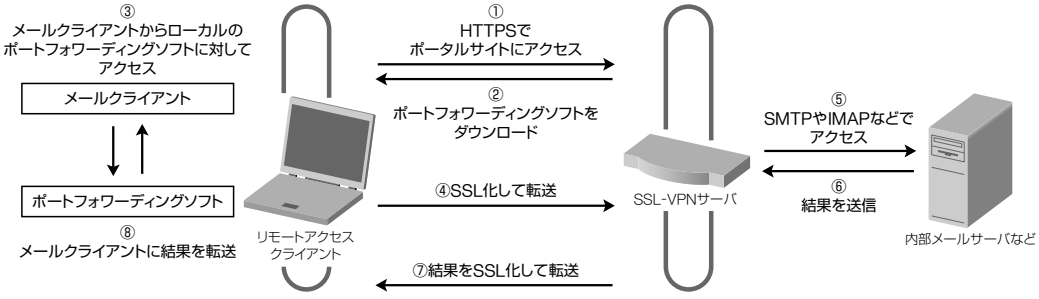

図3● ポートフォワーディング方式でSSL-VPNを利用する場合の動作

②ポートフォワーディング方式

ポートフォワーディングによって、既存アプリケーションからのアクセスに対してSSLを適用し、SSL-VPNサーバに転送する。

③ソケットフック方式

ソケットをフックすることによって、既存アプリケーションからのアクセスをインターセプトし、SSLを適用してSSL-VPNサーバに転送する。

次に、それぞれの方式についてもう少し詳しく説明する。

Webブラウザで手軽にVPNを実現するプロトコル変換形式

プロトコル変換方式では、クライアントは、まずWebブラウザを使用してSSL-VPNサーバにアクセスする(図2)。そうすると、ユーザー認証画面が表示される。ユーザー認証をパスすると、そのユーザーが利用できるリソースへのリンクが表示される。ユーザーが利用できるリソースには、Webベースのアプリケーション以外に、FTPやWindowsファイル共有などを利用するアプリケーションも含まれる。ユーザーがリンクをクリックすると、SSL-VPNサーバは該当する内部サーバに対して、それぞれのアプリケーションプロトコルを使用してアクセスする。その後、得られた結果をWebブラウザに表示できるようにHTTPに変換してクライアントに転送するのである。もちろん、クライアントとSSL-VPNサーバの間はHTTPSが用いられるため、セキュリティが確保される。

この方式では、クライアントはWebブラウザだけを使用すればよく、手軽にVPNを利用できるというメリットがある。しかしSSL-VPNサーバ上で、HTTP以外のプロトコルをHTTPに変換する必要があるため、利用できるアプリケーションが限られるという問題がある。

さまざまなアプリケーションに対応するポートフォワーディング方式

ポートフォワーディング方式は、HTTP以外のプロトコルを使用する既存のアプリケーションを、SSL-VPN経由で利用することを可能にするものだ。この方式では、クライアントは、まずSSL-VPNサーバにアクセスし、HTTP以外のプロトコルにSSLを適用するためのソフトウェア(ポートフォワーディングソフト)をJavaアプレットや**ActiveX**のような形でダウンロードして起動する(図3)。続いて、SSL-VPN経由でアクセスするアプリケーシ

ョンのアクセス先の設定を、通常の内部サーバではなく、ローカルホスト上のポートフォワーディングソフトに送信するように設定する。

例えばメールクライアントであれば、通常は内部メールサーバのアドレスが設定されているが、ポートフォワーディング方式を使用したSSL-VPNでは、これをループバックアドレス（127.0.0.1）に変更するのである。こういったアプリケーションの設定変更を、ユーザーが手動で行わなければならない製品もあるが、ポートフォワーディングソフトがクライアントのhostsファイルなどを自動的に修正し、内部サーバのアドレスを127.0.0.1と設定することで、パケットの転送先をローカルホスト上のポートフォワーディングソフトにしている製品も多い。

このように、クライアントアプリケーションからのアクセスを受信したポートフォワーディングソフトは、そのアプリケーションプロトコルデータにSSLを適用し、SSL-VPNサーバに送信する。SSL-VPNサーバでは、SSLの復号処理を行い、アプリケーションプロトコルデータをあらかじめ設定されたサーバの特定のポートに転送する。

この方式を使用することで、Webブラウザ以外のアプリケーションを利用できるが、あらかじめSSL-VPNでアクセスする内部サーバのアドレスとポートを、SSL-VPNサーバに登録しておく必要がある。また製品によっては、クライアントアプリケーションのアクセス先の設定をSSL-VPNを利用するたびに変更しなければならない場合があり、事前の設定に手間がかかるという問題もある。

ソケットフック方式ではSOCKSが通信をインターセプト

ポートフォワーディング方式では、アプリケーションのアクセス先をループバックインタフェースに変更する必要があった。しかし、**SOCKS**v5を使用してソケットをフックし、アプリケーションから企業ネットワークあてのアクセスをインターセプトすることによって、アプリケーションのアクセス先を変更せずにSSLを適用することができる、ソケットフック方式を用いた製品も多い。

SOCKSは、セッション層で動作する汎用的なプロキシプロトコルであり、RFC 1928に記述されている（図4）。この方式では、クライアントはまずSSL-VPNサーバにアクセスし、SOCKSクライアントをJavaアプレットやActiveXとしてダウンロードして起動する（図5）。クライアント上のアプリケーションを使用して内部サーバにアクセスしようとすると、SOCKSクライアントがそのアクセスをインターセプトし、SOCKSでカプセル化する。SOCKSでカプセル化したデータには、同時にSSLも適用される（SOCKS over SSL）。

またこの方式では、あらかじめ利用するアプリケーションの情報を登録しておく必要が

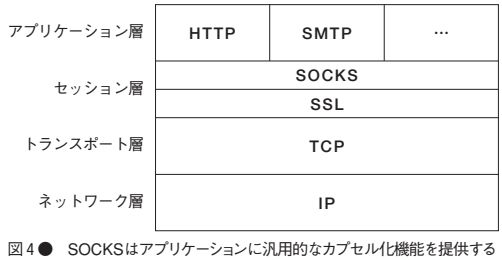

図4● SOCKSはアプリケーションに汎用的なカプセル化機能を提供する

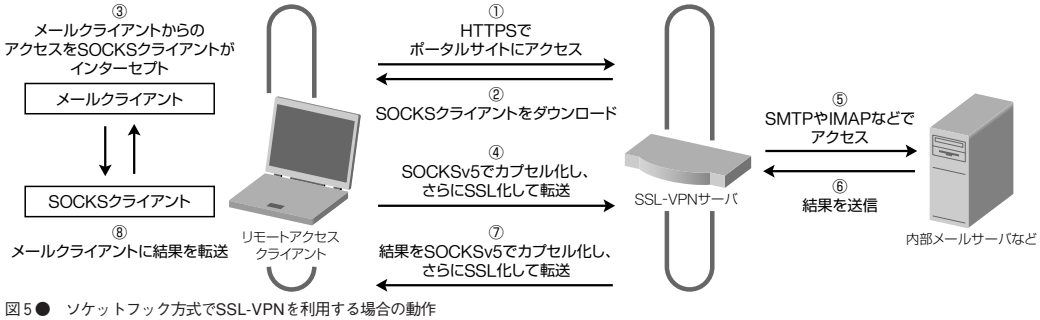

図5● ソケットフック方式でSSL-VPNを利用する場合の動作

Supplement

■SOCKS
NECを中心として開発されたプロキシプロトコル。セッション層で動作し、トランスポート層での通信の代理を行う。

Supplement

■RADIUS（Remote Authentication Dial In User Service）
米国リビングストンが開発した、ダイヤルアップユーザー認証方式。RFC 2138/2139にて標準化されている。ユーザー情報をデータベースで管理する。

■NAT（Network Address Translator）
IPパケット中のIPアドレスを変換する機能。この機能により、プライベートアドレスが割り当てられたノードから透過的に、グローバルアドレスが用いられるインターネットへのアクセスが可能となる。

ないため、最も手軽な方式であると言えるだろう。ただし製品によっては、クライアントが使用するDNSサーバのアドレスを内部DNSサーバのアドレスに変更する必要があるので注意してほしい。

Webブラウザ1つで簡単にアクセス それがSSL-VPNの最大の特徴

SSL-VPNによるリモートアクセスVPNを導入する際は、企業ネットワーク側に、SSL-VPNを確立するためのSSL-VPNサーバやユーザー認証を行うための**RADIUS**サーバが必要となる（図6）。ただし多くのSSL-VPNサーバ製品には、RADIUSサーバと同等の機能が組み込まれているものも多いので、導入する製品の機能を事前にチェックしておくとよい。

クライアントについては、SSLに対応したWebブラウザがあれば、通常は特別なソフトウェアをインストールする必要はない。ただし、UDPアプリケーションや複数のTCPセッションを使用するアプリケーション、あるいはTCPのポート番号を動的に選択して使用するようなアプリケーションを使用する場合は、専用のソフトウェアをあらかじめインストールする必要がある場合もある。また、ファイアウォールにおいて、SSL-VPNサーバに対するHTTPS（443/TCP）の通過を許可する設定が必要となる。

SSL-VPNの利点の1つは、クライアント側に特別なソフトウェアをインストールする必要がないため、共用端末でも利用できる点であろう。しかし共用端末を使用する場合は、Webブラウザに一時ファイルやブラウザ履歴、保存されたパスワードといった情報やダウンロードしたファイルなどが残らないようにする必要がある。製品によっては、ログオフ時にこれらの情報やファイルを自動的に消去する機能を備えたものもあるので、このような機能があるかどうかも製品選択のポイントとなるだろう。

F/WやNATの問題は存在しないが アプリケーションが限定される

これまで、SSL-VPNの機能について述べてきた。ここで、SSL-VPNを使用したリモートアクセスの長所と短所についてまとめると次のようになる。

■長所

- SSL対応のWebブラウザがあれば、クライアントに特別なソフトウェアをインストールする必要がない。
- クライアントが所属するネットワーク上のファイアウォールで、HTTPS（443/ TCP）が許可されていれば、ファイアウォールの設定を変更せずにリモートアクセスVPNを利用することができる。
- SSL-VPNはTCPを使用するため、間に**NAT**が介在しても問題が発生しない。
- SSLでは、使用する暗号化アルゴリズムや認証アルゴリズムが追加できる仕組みになっているので、使用しているアルゴリズムにセキュリティ上の欠陥が見つかっても、別の強力なアルゴリズムに容易に乗り換えることができる。

■短所

- 製品により利用可能なアプリケーションが異なる。特に、UDPを使用するアプリケーションや、動的なTCPポートを使用するアプリケーション、複数のTCPセッションを使用するアプリケーションは利用できない可能性がある。

利用目的にあった VPN技術を選択しよう

今回は、SSL-VPNを使用したリモートアクセスVPNについて述べた。

最後に、これまで本連載で紹介したIPsec-VPN、PPTP-VPN、L2TP/IPsec-VPN、SSL-VPNを利用したリモートアクセスの長

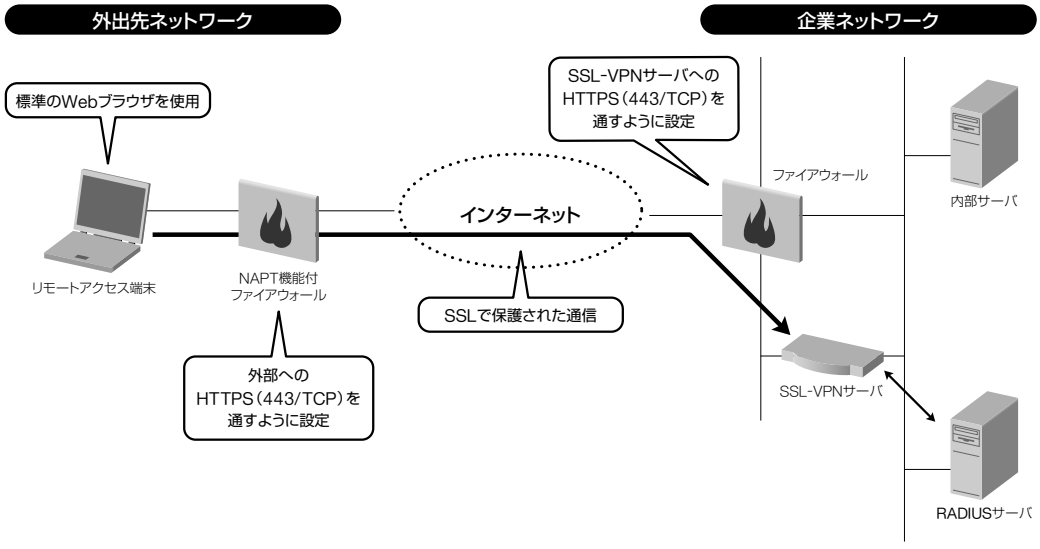

図6● SSL-VPNを使用したリモートアクセスVPNの導入例

所および短所をまとめてみたい。リモートアクセスVPNを導入する際にはぜひ参考にしていただきたい。

■IPsec-VPN

セキュリティは非常に高いが、あらかじめリモートアクセスクライアントに、VPN機器のベンダーが提供するクライアントソフトウェアをインストールしておく必要がある。したがって、管理の手間がかかってもセキュリティを重視したいというユーザーにお勧めする。ただし、NATトラバーサルや**XAUTH**などのユーザー認証、mode-cfg（**IKE-CFG**）のネットワーク情報自動設定機能を利用できるかどうかを確認しておく必要がある。

■PPTP-VPN

Windows標準のクライアントソフトウェアが利用できるため、クライアントへのインストールの手間がかからない。また、安価なブロードバンドルータなどにも実装されているため、導入コストを低く抑えることができる。しかし、暗号化アルゴリズムが**RC4**だけとなる、メッセージ認証機能が備わっていないなど、セキュリティ面で問題がある。したがって、高いセキュリティはそれほど必要としないが、リモートアクセスVPNを手軽に導入したいというユーザーにお勧めする。

■L2TP/IPsec-VPN

IPsecの高度なセキュリティとL2TPが提供する標準のリモートアクセス機能を利用することができる。また、Windows標準のクライアントソフトウェアが利用できる場合が多い。しかし、対応している製品が少なく、また利用例も少ないのが欠点である。したがって、これまでPPTP-VPNを使用していたユーザーが、セキュリティを強化する目的で乗り換えるような場合にお勧めする。

■SSL-VPN

SSL対応のWebブラウザさえあれば、リモートアクセスクライアントに特別なソフトウェアをあらかじめインストールする必要がない。しかし、利用できるアプリケーションが限られるという欠点がある。したがって、クライアントの数が多く、クライアントソフトウェアのインストールや設定の手間を省きたいというユーザーにお勧めする。ただし、製品によっては利用できないアプリケーションが存在するため、導入する前に利用可能なアプリケーションを確認しておく必要がある。

NTTデータ　馬場達也

Supplement

■XAUTH（Extended Authentication within IKE）
IKEプロトコルを拡張したもので、ワンタイムパスワードやRADIUSを利用したユーザー認証を行うもの。

■IKE-CFG（The ISAKMP Configuration Method）
リモートアクセスでIKEを利用するために拡張されたもので、主にネットワーク情報やセキュリティポリシーの管理などを行う。

■RC4（Rivest's Cipher 4）
RSAセキュリティのRivest氏が開発した、ストリーム暗号化アルゴリズム。