〈製品/ハードウェア〉

SSL-VPN製品「SAFEBORDER」インターネットを活用するブロードバンド時代の業務スタイルへ

SSL-VPN Appliance - SAFEBORDER: Extends Intranet Applications to Internet and Enables New Business Communication Style for Coming Broadband Era

則房雅也 *　西　敏通 **
Masaya Norifusa　Toshimichi Nishi

要　旨

SAFEBORDERはSSL-VPN機能を提供するアプライアンス製品です。SSL-VPNは新しいリモートアクセス手段として注目されており，インターネットをビジネスに有効利用することができると期待されています。一方で，ブロードバンドの普及から，社員，カスタマ，パートナーなどとの企業活動の中心がインターネットへと移行しつつあります。SSL-VPNへの注目は，これらネットワーク利用環境の変化，それに合わせた企業活動モデルへの変革を背景にしています。

本稿ではSSL-VPNの技術的特徴，SAFEBORDERが提供するユニークな機能によって企業活動が容易にインターネットに移行できることを解説します。

SAFEBORDER is an SSL-VPN appliance product that offers a unique remote access solution to any customer. The SSL-VPN market was initiated a year ago in Japan by several leading vendors including NEC, and is about to derive new style of corporate business utilizing the Internet effectively ever than before, and in addition because of the recent rapid increase of broadband communications to any user coincidently. Many corporations have resulted in moving to new network environment to be used as the core of corporate IT activities. SSL-VPN then plays an important role to connect people instantly through the Internet.

In this paper, basic technologies and benefits of SSL-VPN are discussed, and SAFEBORDER's unique features are then explained to show how it can change corporate IT and business style by involving the Internet.

1. まえがき

インターネットは世界中の企業にリアルタイムでインタラクティブなデータ通信環境を提供しています。また，どの企業でも，隅々にまでいきわたったイントラネットを構築し活用しています。これらのネットワークがTCP/IPという共通の通信技術を採用していることで，原理上はイントラネットの隅々からでもインターネットを利用することができます。ところが実際には，イントラネット上にセキュリティ対策が次々と施されてゆき，物理的につながっているインターネットであっても，ユーザが望むような通信が行えるとは限りません。ファイアウォール，NAT（Network Address Translation），プライベートIPの利用が浸透し，これらを前提としたネットワークの構成と運用が行われたため，透過性の高いIP通信を実現できなくなる仕組みがインターネットとイントラネットの間にできあがり，今となってはこれらをそう簡単に別の方式に置き換えることはできません。

この通信が途切れた状況を改善しようと考え出された仕組みがVPN（Virtual Private Network）です。VPNを実現する技術としてはIPSecやMPLS（Multi Protocol Label Switching）が知られています。これらの技術はIPトンネルを使って，主にイントラネット間にVPNを作ることに貢献しました。ブロードバンドが普及しつつある現在，VPNへの期待が末端ユーザにまで広がり，適用対象がリモートアクセスに移っています。リモートアクセスを安全に実現するためには，ネットワーク間にIPトンネルを作る場合と大きく異なる要求が出てきます。その典型的な要求の1つがユーザ認証です。誰でもVPN装置までアクセスできるリモートアクセス環境では，匿名のままユーザのアクセスを許すことはできません。また，こういったユーザが利用するアプリケーションを選別し管理することが重要です。フ

＊ ビジネス開発本部
Business Development Division

＊＊ IPネットワーク事業部
IP Networks Division

ァイアウォールだけに頼ると，ポート番号でアクセス管理することになり，どのアプリケーションを使わせるかなどは制限できません。また，ポートを悪用するアプリケーションの規制も難しいのです。これに対して，SSL-VPN（Secure Socket Layer-Virtual Private Network）ではユーザやアプリケーションを厳密に管理できるのです。

これまでネットワークとアプリケーションの構築は別々に考えられてきました。ネットワークにはインフラとしての役割が期待されます。アプリケーションの動作を制限することはまれです。一方，多くのアプリケーションはLAN環境で使われることを想定して開発されています。LAN上で動けばインターネットでも動くと考えるユーザがたくさんいます。ウェブ化されてインターネットから利用できるようになったアプリケーションもありますが，古くから使われているアプリケーションでは，イントラネットとインターネットの間にあるIP通信の壁を越える機能やセキュリティ機能に対する配慮が十分とはいえません。ユビキタスなブロードバンド環境が手軽に使える時代では，イントラネットで使われてきたアプリケーションが外出先や自宅から使われる機会が増えてきます。このような通信環境の変化と利用形態の多様化を背景に，企業施設内に閉じていたイントラネットの範囲がインターネットのなかにまで仮想的に延びようとしています。これをいかにイントラネットの安全性を保ったまま加速できるかが企業活動存続の鍵になっています。ここにSSL-VPNが1つの解を提供するわけです。

2. SSL-VPNについて

2.1 SSL-VPNが現れた背景

SSLはブラウザとともに考え出され，通信プロトコル中に認証と暗号化方式が組み込まれ，ネットワークアプリケーションのセキュリティを実現する上で最も有効な技術といえます。すでに10年以上，認証，暗号化技術として広く使われてきました。

IPSecはSSLより後で標準化され，それまで使われてきた認証，暗号化技術を凌駕すると期待されました。しかし，実際には冒頭で説明したIP通信を遮る壁に阻まれて利用範囲が限られてしまいます。また，ブラウザのようにすべてのPCで使えたわけではなく，ソフトや装置のインストールが必要となったことが普及の足かせとなりました。

こういった10年以上にわたる試行錯誤があり，セキュリティが不可欠の時代となった昨今，個々のアプリケーションに埋め込まなくても，より汎用的な形でSSLが使えるようにとSSL-VPNが開発され市場に投入されたのです。これにより，今まで実現が見送られてきたVPN利用形態が可能となるのです。

2.2 SSL-VPNの特徴

SSL-VPNの最も典型的な特徴は，ユーザPC側にクライアントソフトやVPN装置をインストールしておかなくても

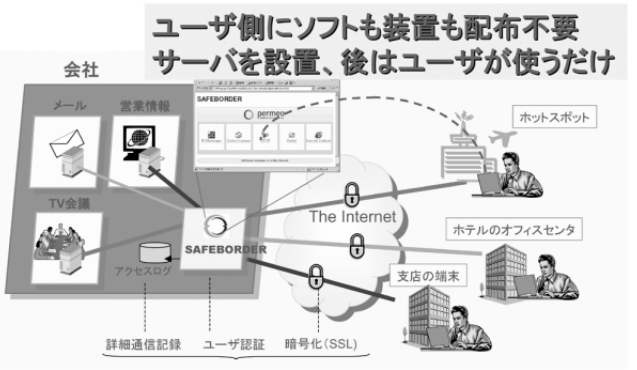

図1　SSL-VPNのメリット:クライアントレス
Fig.1　Client-less as the best benefit of SSL-VPN.

VPNが作れることです。この特徴のおかげで，VPNの利用範囲をインターネットの隅々にまで広げることができ，遠く海外で勤務する社員やパートナーからのリモートアクセスでも受け入れられるのです（図1）。

社外に持ち出したPCでリモートアクセスを行うとき，一般にユーザはイントラネット内のサーバを「pop3.nec.com」のように名前で指定します。IP通信を行うには，この名前に対応するIPアドレスを得る必要があり，内部のDNSサーバに問い合わせなければなりません。ところが，DNSサーバは社外から隠されており，IPアドレスを得ることができません。その結果，アプリケーションが使えないという問題が生じます。見落とされがちですが，適切なDNSサーバにアクセスできないというのはすべてに影響する問題です。SSL-VPNでは，イントラネット内のDNSサーバと交信し，IPアドレスを取得してPC側に伝える仕組みを備えています（図2）。

このように，ダイナミックにVPNを作り，SSLを使った認証と暗号化，DNSへの代理検索など，アプリケーションに対して必要なセキュリティと通信のインフラを提供するのです。

2.3 SSLを使ったVPNの作り方

SSL-VPN装置はPCとサーバの間に位置し，プロキシかトンネリングという技術を使って，アプリケーションの通

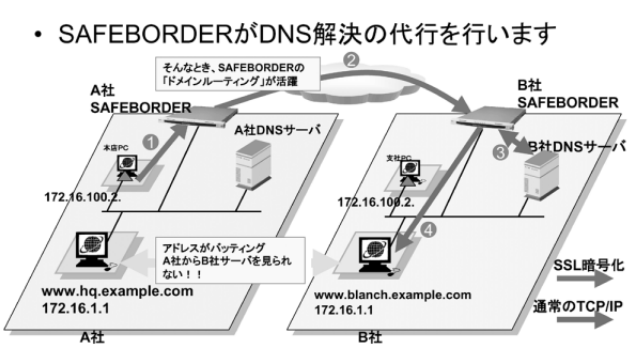

図2　ドメイン名のIPアドレス解決を代行
Fig.2　Resolving hidden private IP address with domain name by proxy.

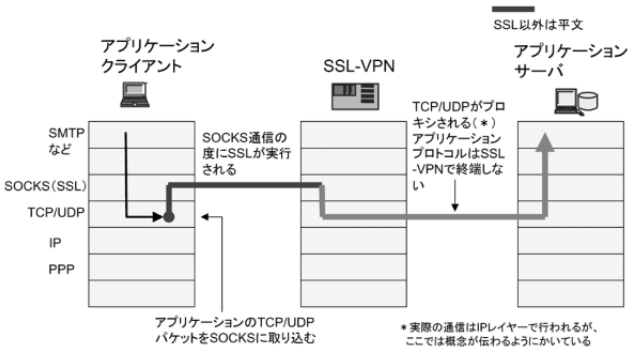

図3　SOCKS+SSLを使うプロキシ
Fig.3　Generic secure proxy with socks and SSL combined.

信を完成させます。

プロキシとしてはHTTPリバースプロキシとSOCKSが使われています。PCからSSL-VPN装置へとSSLセッションを作り，SSL-VPN装置からサーバへとアプリケーションのセッションを作って，これらを一本のようにつなぎます。アプリケーションデータはこの上を流れます（図3）。

単純なウェブアプリケーションしか使わないのであれば，HTTPリバースプロキシ方式が簡単に使えて便利です。ただ，JavaやActiveXを駆使した複雑なウェブアプリケーションになると，通信先がダイナミックに指定されリバースプロキシが機能するとは限りません。

SOCKSはIETFで標準化された，TCP/UDPアプリケーションを汎用的にプロキシするための技術です。暗号化は他の技術を組み合わせることで検討されました。SOCKSにSSLを組み合わせると，ウェブだけでなく多くのアプリケーションにプロキシ通信とSSL暗号化の両方を提供できます。一方，様々なアプリケーションに暗号機能を提供するだけに課題も出てきます。

① 暗号化，復号化を行うことで遅延が生じ，アプリケーションの動作に影響が及ぶことがあります。
② 認証，暗号化，プロキシという処理が加えられると，アプリケーションを使う手順や動作などで，使い勝手の違いが出てしまいます。

もう1つの方式SSLトンネルは，JavaやActiveXを使ってPCとSSL-VPNのあいだに作られます。アプリケーションパケットがトンネルの入り口に送られるとカプセル化されてSSL-VPNまで届きます。ただ，SSLはIPSecと違ってTCPセッションに対して使われる技術なので，複数のセッションを使うアプリケーションになると単純なカプセル化は難しく，プロトコルに応じたVPNモジュールを用意することになります。また，UDP通信にはTCPでカプセル化してからSSLを適用するなどの処理を行う必要があります。前述の①②の課題はSSLトンネルを使う場合にも当てはまります。

認証，暗号化を考慮しないで開発されたアプリケーションをSSL-VPNで使うと，これらの差分がでてくることは避けられません。この差分をどれだけ小さくできるかが，SSL-VPNの実装技術といってよいでしょう。このためにWindowsの機能を最適に使う工夫が行われています。

3. SAFEBORDER

SAFEBORDERではSOCKSとSSLを使ってVPNを作る方式を採用しています。リバースプロキシやSSLトンネル方式とは異なり，SSL-VPN装置でアプリケーションプロトコルを終端させることがないため，高い通信性能と安定性を提供できるからです。また，アプリケーションクライアントをそのまま使えるので，使い勝手をSSL-VPNなしで使う状態に近づけることができます。

3.1　代表的な特徴と方式・実装上の優位点

(1) クライアントレスの実現方式

SSL-VPNにブラウザは必須で，市場のどの製品もがVPN作成をブラウザに依存しています。SAFEBORDERではブラウザに依存する処理を最小限に留めています。ブラウザを使って最初に小さな起動モジュールをダウンロードしますが，この後は，起動モジュールがユーザ認証とVPN作成を行うモジュールをダウンロードします。ブラウザの役割はここまでです。VPNの作成にブラウザの機能を使うことはなく，このダウンロードされたモジュールが行います。ブラウザにセキュリティに関する脆弱性があっても，VPN通信がその影響を受ける可能性はきわめて小さくなります(図4)。

(2) SOCKSとSSLを一体化したVPNチャネル

SOCKSの利点は，①複数のユーザ認証方式を用意しておき，そのなかから選んで使える，②TCPだけでなくUDP通信のプロキシも行える，③DNS検索を代行させられる，④多段にプロキシを設置できる，などです。

SSLの利点は，⑤証明書を使ってクライアント/サーバ認証が行える，⑥最も安全な暗号化通信を行える，などです。それぞれの項目を組み合わせて相乗的に機能するように一体化させています。この一体化により，プライベートIPやNATで受ける通信上の制限を解決し，匿名性を排除して，信用できる暗号化で安全なVPN通信をイントラネットとイ

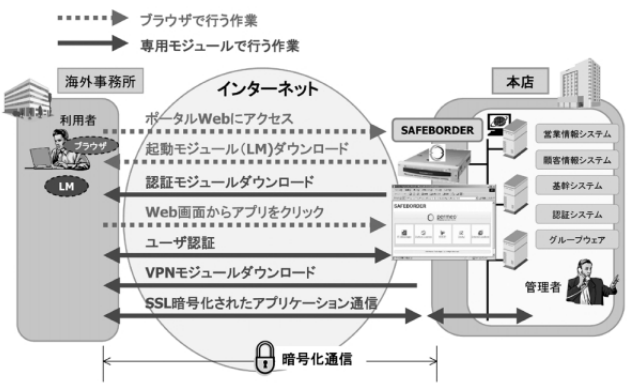

図4　クライアントレスVPNの実現手順
Fig.4　Sequence to establish VPN from client-less condition.

ンターネットの間に実現することができるのです。

(3) ユーザとグループを使った認証とアクセス管理

信頼できるネットワークアクセス管理を行うには，厳密なユーザ認証が基本になるという認識がようやく定着してきました。一方で，ユーザ認証への要求は多様です。1つの方式に統一したいという要求もあれば，複数の方式を場合分けして使いたいと要求もでてきます。

また，グループ単位で管理を行いたいという要求も一般的です。ただし，セキュリティ脆弱性を生じないためには，ユーザ認証は個人に対して行い，グループはアクセス管理の対象や条件を与えるときに使うべきです。SAFEBORDERでは，それぞれのユーザを認証し，認証の結果得られるIDでユーザの属するグループを決め，グループごとに与えたアクセス制御ポリシーを適用することができます。認証方式には，PKI，ワンタイムパスワードなどを選んで，RADIUSやLDAPと組み合わせて利用することができます(図5)。

(4) ログ管理とオーディット

IP装置ではIPアドレスを元にしたログしか残せないため，ログを見てもユーザやアプリケーションを識別することが難しく，トラヒック状態を監視する以上の期待はできませんでした。ところが，ユーザ認証で始まり，指定されたアプリケーションを起動するSSL-VPNでは，ログにユーザIDやアプリケーションを区別する情報を残せます。このため，ログ管理，監査への期待が高まっています。SAFEBORDERでは，ユーザID，時間，転送データバイトなどの入ったログを，いかなる量，期間であってもデータを蓄積，解析できるように，外部に専用サーバをおいて監視，報告が行えるようにしています。

3.2 アプライアンスとして実現する利点

SSL-VPNをアプライアンス製品で提供する理由は，①導入の容易さ，②OS要塞化によるセキュリティレベルの向上と脆弱性報告時の対応しやすさ，③バックアップと障害時の復帰，などを標準的にすばやく提供できるようにするためです。これによって最初の導入だけでなく，後で装置を追加する場合でも，OSの要塞化などをゼロから行う必要はなく，セキュリティを保障したゲートウェイをすぐに実装できるのです。SAFEBORDERでは，SSLレイヤーでアプリケーションの通信を実現しますが，アプリケーションが使われていないと，どこへのアクセスもIPレイヤーで止められていて，VPNに使うポート以外ではパケットを受け付けない装置になります。IPルーティング機能は無効にしてプロキシでしか通信させないので，内部のサーバのIPアドレスが外に知られてもIPパケットが届いてしまうことはありません。

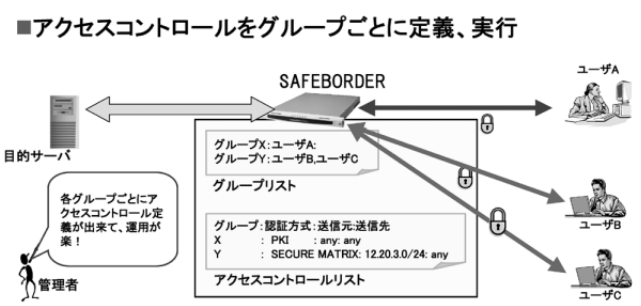

図5 ユーザとグループ管理

Fig.5 User management based on grouping concept.

4. 利用例

(1) NECでは，SAFEBORDERを複数台並べた冗長構成をとって，マトリクス型ワンタイムパスワードを使った社員向けリモートアクセスサービスを実現しています。現在数千人ほどの社員が利用登録しており，常時数百人がイントラネットへとアクセスしています。社内の情報共有ウェブ，電子メール，人事システムなどを，海外，国内出張先であっても，インターネットにアクセスできさえすれば，会社にいるときと同じように利用することができます。承認や手続き申請事項など，従来であれば会社でないと進められなかったことが，外出先からでも行えるようになり，本人だけでなく，周囲の人の作業効率も上がっています。

(2) 兼松(株)様では，海外にたくさんのオフィスを抱えており，本社でイントラネットに公開している情報を，海外で仕事をする人たちも共有できることが課題でした。VPNの利用は決まっていたのですが，技術者やベンダーが現地にいるとは限らず，ソフトや装置を送ってインストールすることも難しく，そこでSSL-VPNが候補に上がったのです。SAFEBORDERは，情報共有に使っているLotus Notesが使えた点，この先ほかのアプリケーションを使うときでも，新たなソフトを追加せずに使えるという点，現地での運用を考えたTOCという観点が評価され採用されました。

5. 今後の課題

SSL-VPNはクライアントレスという特徴から，便宜性とセキュリティが両立する手法として注目され，社員のリモートアクセス用途で使われ始めました。この後すぐに社員から協力会社，パートナー，一般ユーザへと利用対象を広げることが求められるようになり，管理できないユーザのPCを信用してVPNアクセスを受け入れてよいのかという課題が提起されました。また情報漏えいへの危惧から，一時的に参照された情報がPCに残る可能性への指摘も出ています。これに対して，ブラウザの一時ファイルを削除してからVPNを終了する，VPNを作成する前にPCのセキュリティ状態をチェックする，などの機能が追加されつつあります。SAFEBORDERでもこういった点を強化してゆきます。

しかし，SSL-VPNで動的に送り込む小さなモジュールを使ってPC上のOSやアプリケーションに関わるすべてのセキュリティ項目を管理できるわけではありません。これらの管理を本来の仕事とする検疫システムやPC資産管理シ

ステムが注目されています。これらのシステムにとってSSL-VPNは1つのアプリケーションであり，検疫が済むまで動いてはいけないアプリケーションです。SSL-VPNとこれらPCセキュリティシステムとは，コンセプトも目的も起動のタイミングも異なっています。お互いに矛盾しない機能を提供し，それぞれの通信を止めることがないよう，役割を明確に分けた共存を実現することが重要です。たとえば，検疫が済んだら誰がどんなアプリケーションを使っているか分からないというのでは問題です。検疫が済めばSSL-VPNが起動し，利用することが許されるアプリケーション，アクセスしてよいネットワークやサーバへの通信がきちんと管理される，というような分担です。SAFEBORDERでは，お互いの特徴を最大限生かせる共存を実現することをまず目標と考えています。

6. むすび

冒頭で説明したように，本来SSL-VPNが解決すべき課題はインターネットの本質にも触れる難問です。ブラウザとJavaを使えば何とかなるというものではありません。実際，この半年の間に，より多くのアプリケーションをSSL-VPNで使えるようにして欲しい，同時にユーザの使うPCのセキュリティを管理して欲しい，という課題が持ちこまれてきています。安易な実装でSSL-VPNとうたっている製品で要求を満たすことは難しく，技術的にしっかりした土台の上に築かれた製品が解を提供することになるでしょう。ワームやウイルス，不正アクセス手法の高度化，イントラネットの外でも同じアプリケーションが利用されることになり，他のセキュリティシステムとの融合，共存を求める多くの声がSSL-VPNベンダーに持ち込まれるでしょう。SSL-VPNは通信を安全に広げる技術であり，その周りに安全を脅かす通信を阻止するセキュリティ技術がそろえられて，お互いの良さをより発揮できます。これをひとつのシステムにまとめてしまうと，通信を遮断する機能が強化され続けてVPNの利点が消えてゆくことになります。この点に十分な注意を払い，VPNとセキュリティの必要な接点を理解し，お互いがそれぞれの機能を最大限生かすような方向で同期して改良されてゆくべきだと考えます。

筆者紹介

Masaya Norifusa
則房　雅也（のりふさ　まさや）　1980年，NEC入社。現在ビジネス開発本部エキスパート。情報処理学会，ISSA各会員。
ISSA：Information System Security Association

Toshimichi Nishi
西　敏通（にし　としみち）　1990年，NEC入社。現在ブロードバンドネットワーク事業本部IPネットワーク事業部エキスパート。