ホワイトペーパー

小規模～中規模のエンタープライズ環境向け SSL-VPN導入決定ガイド

ロスリン・リスラー
プロダクトマーケティング・ディレクター

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089　USA
408 745 2000 or 888 JUNIPER
www.juniper.net

ジュニパーネットワークス株式会社
〒163-1035 東京都新宿区西新宿 3-7-1
新宿パークタワー N 棟 35 階
電話　03-5321-2600
FAX　03-5321-2700
URL　http://www.juniper.co.jp

Part Number: 200092-003 JP
January 2006

目次

中小規模企業市場の概要

中小規模企業は、今日の国際経済において最も成長している市場セグメントのひとつです。同市場について議論する前に、対象とする会社規模を定めておく必要があります。中小規模企業の定義はさまざまですが、本書の目的を踏まえ、従業員数が25名を超え、250名未満の企業を対象としたセグメントと定義します。

これらの組織は個々の会社単位でみると規模は小さいですが、集約させた場合、経済的および政治的に非常に大きな力をもっています。米国における2005年の新規雇用は、その60%が中小規模企業によって生み出されています。また、EUだけでも、7,400万名が雇用されています。中小規模企業の存在は、米国のSBA(Small Business Administration)から、ヨーロッパの経済協力開発機構、アジア・太平洋経済協力会議に至るまで、全地域でサポートされています。

国際的な中小規模企業市場の成長は、次の2つの現象から自然に生まれてきたものです。ひとつはナレッジベース型経済の登場、そして、インターネット通信やアクセスが利用できる環境の普及です。

コンピューターやオートメーションの活用により、かつては大企業のみが台頭していた特殊な分野において、小企業でも競争可能になりました。さらに、小規模企業が、変化するビジネス状況に柔軟に対応し、変更にあわせた運営体制のメリットを効果的に発揮することができるようになりました。これには、素早い開発・生産・サービスを通じて、グローバル市場におけるどんな変化に対しても最適化できる柔軟性と能力が必要になります。中小規模企業の場合は、大企業と異なり、組織的なインフラが障害となることがないため、迅速な対応により、ビジネスニーズの変化を逆に利用するといったことができます。

今日の中小規模企業は、情報技術により、そのビジネスのスピードを高速化しています。北米における全中小規模企業市場の複合年間成長率は、総じて、全世界の市場をしのぐとみられています。技術の利用可否が課題となっていたのは、もはや昔のことです。技術を使用する上での違いは、成功できない企業の場合、既に所有している技術の潜在能力を十分に活用していないという点にあります。

リモートアクセスの動向

原動力となっているもうひとつの動向は、インターネットの出現です。情報収集は時間と資源のかかるものでしたが、今日、豊富な情報を誰もがインターネット経由で入手することができ、公平な場となっています。サプライヤー、顧客、遠隔地やモバイル環境の従業員とのリアルタイム通信は、かつて、スタッフの時間、専用回線またはダイアルアップ接続を駆使した大企業における独占領域でした。今や、どんな規模の企業でも、仮想プライベートネットワーク、つまりVPNを使って、インターネットによる接続を活用することができるようになりました。VPNは、インターネットなどの公衆網を使用して、LANで見られるような私的データを送受信するための手段と定義されます。今日のVPNは、サイト間接続を提供するとともに、リモートユーザーやモバイルユーザーにアクセスを提供します。サイト間接続の市場では、このような種類の接続を扱うために設計されたネットワーク層VPN、つまりIPSec VPNが普及しています。特に中小規模企業にとって、さらに複雑な課題は、遠隔地やリモート環境の従業員からのアクセス要求が常に変化しており、かつ急速に増加している点です。

Infonetics社の調査（2005年第3四半期）によると、大半の企業では、リモートアクセスをごくわずかな従業員（通常20%未満）に提供しているだけとなっていますが、これは導入および保守が高価であるためです。同社では、2008年までに、同技術により多くの企業がより多くの従業員にリモートアクセスを提供するようになり、その平均は20%前後から50%に上昇すると推測しています。

「IDC社では、2003年末までに、米国における在宅勤務者、つまり、1ヶ月に3日以上は自宅で勤務する人は、およそ890万人であったと推定している」と、IDC社のホーム・オフィス・プログラム担当シニア・リサーチ・アナリストであるMerle Sandler氏は述べています。中小規模企業は、特に、このセグメントでの伸びを示しています。Infonetics Research社では、「2002年において、小企業の20%、中堅企業の37%、大企業の60%がリモートアクセスVPNを導入しており、2007年までにはそれぞれ50%、74%、90%になるだろう」としています。これらの統計は、中小規模企業における全市場が今後5年間で倍増するということを示しています。とはいえ、コスト、使いやすさ、日常の保守作業といった点を考慮すると、大企業で有効であったリモート・アクセス・ソリューションが、ほとんどの中小規模企業でそのまま利用できるとは限りません。

トータルコスト機器の価格＋有用性＋保守

機器の購入価格自体に関する問題は、比較的簡単に解決できます。大手アナリスト会社では、中小規模企業市場向けの安全なリモート・アクセス・ソリューションとしては、5000ドル以下の価格帯が理想的だとしています。ただし、これは、購入価格がリモート・アクセス・ソリューションに関する唯一の懸案事項であり、導入費や保守コストが一切かからないことを想定したものです。遠隔地のユーザーを接続するためにIPSec VPNを使用するとしたら、この前提条件がすべての製品に当てはまるとはいえません。Network World誌の最新号では、オフィス間の接続にIPSecの採用を強く支援している読者を取り上げ、「サイト間VPNでは、テクニカルトレーニングを受けていないエンドユーザーが、なにかの作業をしなければいけないということはありません」とのコメントを掲載しています。これは、IPSec VPNをサイト間の接続に使用した場合、遠隔地のオフィスのゲートウェイと本社のLANゲートウェイの間で接続が処理され、ユーザーには全く認識されないためです。この読者は同技術を使ったリモートユーザーの接続へと話題を進め、次のように述べています。「当社が直面した問題は、技術知識のない遠隔地のユーザーをクライアント・ソフトウェアに接続しようとすると必ず何らかの問い合わせが発生します。クライアント・ソフトウェアをインストールし、これがどのように動くかユーザーを教育し、接続が切断した場合に保守をするといった際の経費が、本来の価値よりも問題になってきています。」

Network Computing Asia誌（2004年7月号）には、次のように掲載されています。「コスト効率は小企業にとって、大企業と同様に緊急課題ではあるが、中小規模企業の場合、モバイル環境での運用に対応するために必要となる技術的なインフラがあることはまれです。モバイル環境の従業員がアクセスできるメッセージングサーバーやコラボレーションサーバーを稼動させるといったシンプルな課題を検討してみましょう。大企業の場合、トレーニングを受けたIT担当者が管理する環境にサーバーを一台設置し、モバイル環境の従業員にこのサーバーへの安全なアクセスを提供するだけです。中小規模企業には、こういった贅沢な選択肢はありません。少なくとも、大企業がモバイル環境での運用に定期的に使用するようなソリューションは、中小規模企業を対象として縮小化されることはありません。モバイル化する中小規模企業は、異なる方法でモバイル運用に対応していくことが必要になります。」

今日の小規模企業がますます技術的に精通してきて、顧客との接続、在庫の追跡、帳簿の管理にコンピューターを駆使しているとはいえ、IT担当者を社内に配置することはできません。社内ITサポート担当者は、IPSec VPNをリモートアクセス用に実装・導入・設定する必要があります。デスクトップサポートが、ネットワークアドレス変換や、ファイアウォールまたはプロキシのトラバースなどの問題に備えて、モバイルユーザーと作業できることが必要です。また、更新したVPNクライアントを遠隔地のユーザーに提供する必要がある場合は、さらに保守作業が必要です。これは、ネットワークトポロジーへの変更、クライアントOSへの変更、クライアント・ソフトウェア自体への変更がある場合に典型的なケースです。そして、組織内の各新規ユーザーがサポート負担を増すことになります。この結果、多くの中小規模企業では、IPSec VPNの管理に必要となる十分なIT担当者を配置することはないと感じています。

セキュリティ

もうひとつの重要な検討課題は、やはり、セキュリティです。オープンIPSec VPNトンネルもまた、社内LANへの経路となっています。トンネル自体は暗号化されて安全ですが、接続の一端が外部にオープンになっているとしたら、セキュリティは意味をなしません。サイト間接続の場合は、VPNを使って、既知の2つの団体を接続していると考えられるわけですが、リモートユーザーがLANへトンネリングしている場合はこの限りではありません。リモートアクセスに使用されるネットワーク層VPNのセキュリティは、もともとはLANから削除される情報に重点を置いていました。今日のセキュリティの懸念事項は、ユーザーによってしばしばオープン状態となってしまっているVPNセッションを利用して、トンネルに何が入ってきてしまうことができるのかといった課題を中心としています。

セキュリティは、社内にセキュリティ対策専任のIT担当者が不在である中小規模企業にとって大きな課題です。中小規模企業は集中攻撃の標的にはならないだろうと思っているものの、最近の脅威は悪質性を増しており、ターゲットを絞らずにインターネットを介して広まります。CodeRedやNimdaなど、複雑なウィルス、トロイの木馬、ワームは、どこからでも入ってきます。一方、大企業はセキュリティ担当者を配置して自社を完全に防御しており、結果として、規模の小さい企業の方が標的になることがあります。大企業と違って、小さなセキュリティ侵害であっても、小企業を崩壊させてしまう可能性があります。Microsoft社によると、平均して、小企業では年間6つのセキュリティ問題に対応し、IT予算の20%をセキュリティに費やしています。小企業にとって、セキュリティに費やすこの資源の量は膨大です。中小規模企業が社内セキュリティ担当者を雇用する余裕がない場合、リモート・アクセス・ソリューションの選定において、保護手段が本質的な部分であるとの自覚が必要です。

アクセスのユビキタス性

リモートアクセスにおけるもうひとつの重要な検討課題としては、会社が管理しているノートPCやPC以外のデバイスを使って社内リソースにアクセスする必要があるユーザーの存在があります。接続するにあたり、すべての従業員が会社で管理しているデバイスを提供されていない中小規模企業の場合、これは特に重要です。さらに、従業員のモバイル化が進むにつれ、インターネットカフェや空港のキオスクといった会社管理外のデバイスなど、さまざまなエンドポイントからのアクセスの必要性も増加します。こういった状況における従来のIPSecソリューションの欠点のひとつは、VPNクライアント・ソフトウェアがインストールされたデバイスからのみアクセスが可能な点です。つまり、会社が管理しているPCを持っていない、あるいはその時点でそのようなPCへのアクセスを持たない従業員が、事実上、アクセスできないことになります。出張先や移動中、災害復旧シナリオでのアクセスニーズにおいて、大変重要です。

リモート・アクセス・ソリューションの基準

リモート・アクセス・ソリューションを評価するにあたり、中小規模企業は次の懸念事項を検討する必要があります。これらには、機能的な要件、つまりユーザーを必要とするリソースに接続するソリューション、購入価格・導入費・保守費用・拡張性を含めたトータルコスト、エンドユーザー・データ・社内サーバーを含めたセキュリティ、将来に備えたソリューションの拡張性、ユビキタス性があります。

機能的要件

- 導入により、現状の問題点を解決
- 既存・新規アプリケーションとの連携が可能
- 技術知識のないエンドユーザーが簡単に使用
- ネットワークの再構成が最小限で済む

トータルコストの検討課題

- 購入価格
- 日常の保守作業
- エンドユーザーの教育
- ユーザーサポート（ヘルプデスク）
- 新入社員へのモートアクセスに必要なハードウエア・ソフトウエアを提供するためにかかる時間
- ダウンタイムにおけるコスト

セキュリティ

- 転送中のデータを暗号化する手段がある
- 特にクライアント側でのポリシー実施と連携し、管理内外のデバイスに対し堅牢なエンドポイント・セキュリティを提供
- 認証サーバーの使用など、セキュリティにおける既存の投資を活用するか、セキュリティ・ポリシーやアプリケーションを導入
- 独自のネットワークセキュリティを提供し、公衆網に直面する DMZ に設置する上で十分安全である
- サードパーティによるセキュリティ監査をパスしている

拡張性

- 現在のリモートアクセスニーズを満たす
- 将来のリモートアクセスニーズを満たす

ユビキタス性

- どこにあるどの PC からでもアクセスを提供
- 管理者が管理するアクセスは、ユーザー単位およびセッション単位で変更され、最大限の制御を実現

SSL-VPN の紹介

SSL-VPNは、インターネットを活用するだけでなく、その使用に固有の特定プロトコルを利用します。特に、セキュア・ソケット・レイヤー、つまり、SSLにおいてです。SSLはもともとオンライン上の金融取引を安全なものにすることを目的に開発されており、ウェブコマースの基盤のひとつとなっています。SSLはすべての標準的なウェブブラウザの一部として組み込まれているため、安全なデータ通信を開始するクライアント・ソフトウェアはエンドユーザーのデバイス側に既に存在することになります。エンドユーザーが会社のノートPC上でクライアントを設定する必要はありません。SSL-VPNは、安全な送信メカニズムとしてSSL/HTTPSを使用しており、これはすべての標準的なウェブブラウザで特にダウンロードすることもなく使用できます。エンドユーザーとLANとの間の「トンネル」は、ネットワーク層ではなく、アプリケーション層を利用します。SSLを使用することで、IPSec VPNに関する以下のような様々な問題を解決することができます。

- インストール不要
- 設定不要
- 一般的なウェブブラウザ利用できるため、ウェブブラウザがあればアクセス可能
- アプリケーション層プロトコルであり、ネットワーク層プロトコルではないため、視認性が高く、きめの細かい制御を提供可能
- NAT やファイアウォールによる通信の問題がない
- SSL は、技術に関係のない人にとっても使い慣れた環境（例 Amazon で本を購入する際に使用）

この結果、主要なアナリストは、2007年までに、リモートアクセスの80%がSSLに取って代わるとの予測をしています。

また、すべてのSSL-VPNが同じではないという点にも注意が必要です。事実、安全な転送メカニズムとしてのSSLの使用は、これらのソリューションが実際に共通している場合のみです。本来の定義は正しいかもしれませんが、実際には、トランスポートの共通性は、各ベンダーのソリューションがどう機能しているかという点に比べたら重要ではありません。SSL-VPNソリューションは、他のリモート・アクセス・ソリューションを検討する場合と同じ条件で評価すべきです。

中小規模企業向けの SSL-VPN

ジュニパーネットワークスでは、中小規模企業から大企業に至るまでのニーズを満たすように設計された一連のSSL-VPNアプライアンスを提供しています。ジュニパーネットワークス Secure Access 700（SA 700）は、中小規模企業向けに設計されています。ジュニパーネットワークのSSL-VPNが、中小規模企業における重要な基準に達していることをご説明します。

機能的な要件

■ **導入により、現状の問題点を解決**

IPSec VPNは、何年にもわたってリモートアクセスの提供に使用されていますが、本来は、サイト間接続を提供することを目的に開発されています。SA 700は、中小規模企業における遠隔地またはモバイル環境の従業員、顧客、パートナーに安全なアクセスを提供することを目的に設計されています。

■ **中小規模企業向けに設計**

SA 700は、従業員数が250名未満の企業向けに設計されています。この設計は、アプライアンスの価格にも反映されています。

■ **既存・新規アプリケーションとの連携が可能**

SA 700は、基本的なアクセス方式としてNetwork Connect機能を使用し、さらにアップグレード・オプションとしてCore アクセス機能も使用可能です。ジュニパーのNetwork Connectは、アダプティブ・デュアルモードのネットワーク層アクセス機能を提供し、IPSecとSSL間で最適な接続方式を検出し、最高レベルのコネクティビティを実現することで信頼性を向上させます。また、Network Connectは、軽量な動的ダウンロードにより実装して、IPSec VPNのメリットをフルに活用することができ、管理コストもかかりません。

Network Connectは各種のプラットフォーム上で動作可能なため、OSの選択肢は制限されません。

Coreアクセス方式は、完全にクライアントレスのアクセスを提供し、エンドポイントからリソースを選択します。Coreアクセス方式は、ウェブベースのアプリケーション、ファイル、標準準拠のメール、telnet/SSHセッションに加えて、複雑なJavascript・DHTML・VBScript・Flash・XMLなどを使ったアプリケーションへの安全なアクセスを提供します。

■ **技術知識のないエンドユーザーが簡単に使用**

SA 700は、ウェブ上の金融取引において国際標準となっているSSLを使用します。ユーザーがアクセスする上で、技術的な知識は必要とされません。

■ **ネットワークの再構成が最小限で済む**

SA 700は、文字通り、プラグ＆プレイ方式です。1時間以内で実装することができ、ネットワークインフラへの変更も不要です。ほとんどのファイアウォールはSSLトラフィック用のポートであるPort 443からのトラフィックを許可するように設計されており、ファイアウォールの設定変更も不要です。

トータルコストの検討課題

- **購入価格**

  SA 700 SSL-VPNは、ほとんどの中小規模企業で容易に購入ができる価格設定をしています。また、10ユーザーから25ユーザーまで、同時に利用できるユーザー数を増やすことができます。

- **日常の保守作業**

  SA 700には、日常の保守作業は不要です。新規ユーザーや新しいアプリケーションの追加も、数回のマウス操作で完了します。

- **エンドユーザーの教育**

  SA 700は、ほとんどのエンドユーザーが採用しているシンプルなウェブユーザーインタフェースとSSLを採用しているため、エンドユーザーへの教育は不要です。

- **ユーザーサポート（ヘルプデスク）**

  IPSec VPNのエンドユーザーサポートのほとんどは、可用性の問題、ISP互換性の問題、NATの問題、またはファイアウォールやプロキシのトラバースの問題に起因しています。SA 700の場合、これらの問題は皆無です。

- **新入社員へのモートアクセスに必要なハードウエア・ソフトウエアを提供するためにかかる時間**

  これは、ほとんどの企業にとって、IPSec VPNの隠れたコストを認識する簡単な方法です。新規ユーザーの設定にかかる時間と労力は、導入時に影響を及ぼすことができないコストです。新規にユーザーを追加するには、名前、認証、アクセス制御をアプライアンスに追加するか、既存のユーザーディレクトリを流用するだけの簡単さです。

- **ダウンタイムにおけるコスト**

  信頼性またはセキュリティ問題のいずれかが原因となり、ダウンタイムが発生する場合もコストが発生しています。SA 700は、公衆網への接続を前提として設計された堅牢なアプライアンスで、複数のサードパーティのセキュリティ関連団体により継続的な監査を受けています。さらに、クラス最高のマルウェア防御を搭載しているため、攻撃を原因としたウンタイムからネットワークを防御することができます。

セキュリティ

- **転送中のデータを暗号化する手段がある**

  IPSecおよびSSLは共に強力な暗号化を使用し、送信中のデータを類似した方法で保護します。

- **特にクライアント側でのポリシー実施と連携し、管理内外のデバイスに対し堅牢なエンドポイント・セキュリティを提供**

  セキュリティ・ポリシーの実施は、SA 700を使えば簡単です。エンドユーザーのデバイスは、SSL-VPNへの認証提示を許可する前にセキュリティレベルを確認されます。（このため、たとえば、主なキーストロークロガーから防御）。また、SA 700にはマルウェア保護機能が搭載されているため、エンドポイントが本当に安全であることを確実にします。ジュニパーネットワークスSecure Accessシリーズの本格的な機能を備えたデバイスとして、SA 700もまた、J.E.D.I(Juniper Endpoint Defense Initiative)を活用しています。このソリューションは、クライアント側およびサーバー側のAPIを使用して、業界をリードするサードパーティ製セキュリティ・アプリケーション（Antivirus、Personal Firewall、Virtual Desktopなど）を容易に統合することを可能にします。

  最初に端末のチェックを行った後、その結果に応じてユーザーをRole（アクセスグループ）にマッピングすることができ、ヘルプデスクに頼らずに修正することも可能です。 たとえば、アクセスする前に最新版のアンチウイルス・シグネチャを必要とするポリシーを実施し、ヘルプデスクの介在なしにエンドユーザーがシグネチャをダウンロードできるようにすることができます。

  SA 700は、主要な認証方式および認証ストアとの完全互換性を備えています。さらに、別のレベルのポリシー実施を自分で設定することも可能です。

- **認証サーバーの使用など、セキュリティにおける既存の投資を活用するか、セキュリティ・ポリシーやアプリケーションを導入**

  SA 700は、認証情報用の独自の暗号化データベースを搭載しており、あるいは、デュアルファクタ認証方式やX.509デジタルクライアント認証といった主な認証方式や、すべての主要AAAサーバー（LDAP、AD/NT、RADIUSなど）とのシームレスな互換性を備えています。

  また、一流のセキュリティベンダーとのAPIレベルでの統合化を提供し、一貫したセキュリティ状況を確実にし、非適合のエンドポイントを修正する手段を提供します。

- **独自のネットワークセキュリティを提供**

  SA 700は、特定目的用のジュニパーネットワークスのInstant Virtual Extranetプラットフォームをベースとしています。このプラットフォームは、大手サードパーティのセキュリティエキスパートによる厳格な監査を合格した堅牢な専用プラットフォームです。

- **サードパーティによる監査を通過していること**

  中小規模企業の多くは、すべてのデバイスのセキュリティ状況を評価するために社内資源を費やすことができません。 このため、サードパーティに依存してこのようなノウハウを提供することが必須となります。 ジュニパーネットワークスのSecure Accessプラットフォームは、CyberTrust社（前TruSecure社）、iSECパートナー各社、ICSAラボなどのサードパーティのセキュリティ専門家により継続的に監査されています。

拡張性

- **現在のリモートアクセスニーズを満たす**

  SA 700はアプリケーション層デバイスであるため、クライアント・ソフトウェアのインストール・設定・保守が不要で、新規ユーザーの追加も簡単です。もし、同時に使用するユーザー数を増やしたい場合、ソフトウェアのアップグレードをするだけの簡単さです。ハードウェアの変更は不要です。

ユビキタス性

- **どこにあるどの PC からでもアクセスを提供**

  Coreアクセス方式はどんなブラウザ上でも利用できるため、いつでもどこでもアクセスができます。

- **管理者が管理するアクセスは、ユーザー単位およびセッション単位で変更され、最大限の制御を実現**

  2種類のアクセス方式（CoreおよびNC）を採用したSA 700の総合的なAAAフレームワークにより、ユーザーやセッション単位での細かなアクセスを提供することができます。

結論

遠隔地やモバイル環境の従業員の増加といった動向がみられる中で、中小規模企業市場は全世界で急成長を遂げています。コスト効率に優れた堅牢なリモート・アクセス・ソリューションは、もはや贅沢なことではなく、ビジネスに必須と言えます。同時に、中小規模企業にはセキュリティ専任のIT担当者が不在であることが多いため、採用するソリューションは導入・管理が簡単であることが必須条件です。少ない技術的な知識やトレーニングで、エンドユーザーが簡単に使用できるようなソリューションであることが必要です。

SSL-VPNは中小規模企業のニーズに非常に適合しており、アナリスト、技術誌、エンドユーザーからも推奨されています。ジュニパーネットワークスのSA 700 SSL-VPNは、中小規模企業が求めていたシンプルさ、安全性、手ごろな価格帯を実現したリモート・アクセス・ソリューションを実現します。