FUJITSU

Technical White Paper

SSL-VPN 入門

簡単便利なリモートアクセス手段として注目を集める SSL-VPN。
本書では、SSL-VPN とは何か理解したい人へ、基礎技術である
SSL から、SSL-VPN を実現する様々な方式、さらに SSL-VPN と
安全に使うためのセキュリティ技術まで、SSL-VPN に関する
基本的な情報を提供します。

ネットワークサーバ アイピーコム
IPCOM

目次

1．リモートアクセスと VPN 1
1. 1 リモートアクセスに対するセキュリティの脅威 1
1. 2 リモートアクセスの手段としての VPN 2
1. 3 IPsec-VPN と SSL-VPN 4
2. SSL-VPN の基本動作 6
2. 1 SSL 通信で使われている技術 6
2. 2 SSL 通信の流れ 9
3. SSL-VPN の実現方法 10
3. 1 リバースプロキシ方式 10
3. 2 WEB 以外のアプリケーションを使う方法 12
3. 3 ポートフォワーディング方式 12
3. 4 L2 フォワーディング方式 14
3. 5 まとめ：SSL-VPN の実装方式の比較 16
3. 6 データの流れから見た 3 方式の違い 16
4. SSL-VPN のセキュリティ向上 (認証とアクセス制御) 21
4. 1 ユーザ認証 21
4. 2 アクセス制御 25
4. 3 エンドポイントセキュリティ 26
富士通の SSL-VPN 装置のラインナップ 29

1．リモートアクセスと VPN

1. 1　リモートアクセスに対するセキュリティの脅威

パソコンやモバイル端末の普及に伴い、自宅や出張先から、いつでも企業のイントラネットにアクセスして、オフィスにいる時と同じように仕事をしたい、というリモートアクセスに対する要求が高まってきています。

これまでは、リモートアクセスのため、企業のイントラネットに RAS（Remote Access Server）を設置し、ダイヤルアップで接続する方法が使われてきました。しかし、この方法では利用者数や距離に応じてコストが高くなることや、回線速度が遅いためアプリケーションが使いづらいなどの問題がありました。そこで、最近ではインターネットでブロードバンド回線が普及し、安価で高速通信が可能になってきたことを背景に、インターネットを通じて企業のイントラネットにアクセスしようとするケースが増加しています。

しかし、インターネットを通してリモートアクセスをしようとした場合、以下に示すようなさまざまな脅威が潜んでいます。

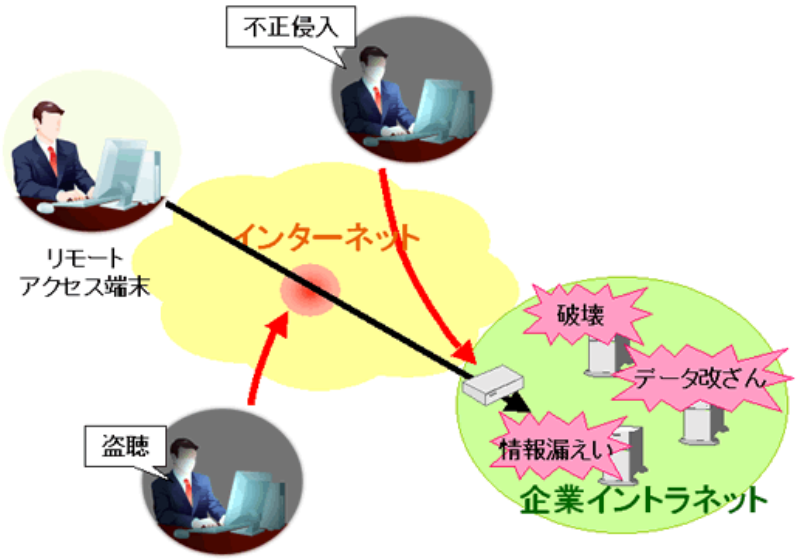


図 1-1. インターネットに潜む脅威

脅威	説明
盗聴	コンピュータやネットワーク上のデータを不正に取得する行為です。 リモートアクセス時に、特に対策もせず平文で情報のやり取りをしていると、第三者に情報を盗聴された時に、パスワードや機密情報を判 読されてしまい、不正侵入につながってしまう可能性があります。
不正侵入	コンピュータへ許可なく侵入する行為です。 侵入されたコンピュータが被害を受けるだけでなく、他のコンピュータへの不正侵入や SPAM メール送信への中継として使われ、加害者 (踏み台) となってしまう場合があります。 <不正侵入で受ける被害> ・ 情報漏えい 個人情報や企業の機密情報を外部に流出させる行為です。 例) 顧客情報が流出し、クレジットカード番号などが悪用されてしまう。 ・ データ改ざん コンピュータのデータを不正に書き換える行為です。 例) WEB サイト内容が提供者の意図していない情報に変更されて、多くの WEB サイト利用者に誤った情報が公開される ・ 破壊 コンピュータ上のデータやプログラムを故意に消す行為です。 例) 企業が蓄えた膨大な情報（顧客情報や企業ノウハウなど) を一瞬に失う その他にも、スパイウェア等を埋め込まれて盗聴が行われる、Dos 攻撃のためのバックドアが仕掛けられるなどの危険があります。

企業のネットワークシステムがこのような脅威による被害を受けると、正常な業務が続行できず多額の損害を被り、さらには社会的な信用まで失墜してしまいます。

1. 2 リモートアクセスの手段としての VPN

インターネットでの脅威を防ぎ、安全なリモートアクセスを実現するために使用されるのが、VPN です。

VPN(Virtual Private Network) とは
不特定多数が使用する共有ネットワーク上に、あたかも専用線のようなネットワークを作り出すことです。VPN に厳密な定義はなく、技術、方法および作り出されたネットワークをまとめて VPN と呼んでいます。
当初は電話回線が対象でしたが、最近ではインターネット上に VPN を構築すること（インターネット VPN）を単に VPN と呼ぶこともあります。本連載でも、特に指定しない場合は、このインターネット VPN を VPN と呼びます。

VPN では、

・トンネリング
・暗号化
・認証

などの複数の技術を用いて、インターネット上で安全な通信を実現します。

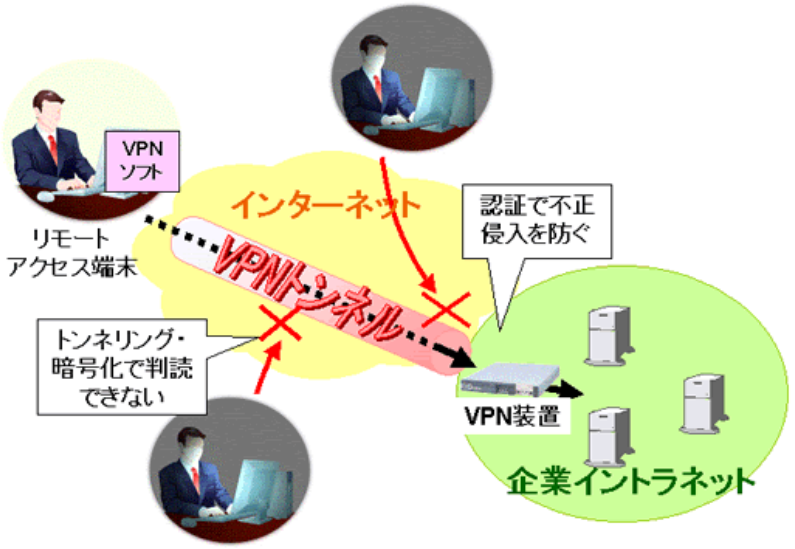


図 1-2. VPN を使ったリモートアクセス

トンネリングとは、通信したいコンピュータとの間に、仮想的な経路を作ることです。

例えば、リモートアクセス端末から企業イントラネット内のサーバにアクセスする場合、まずリモートアクセス端末に搭載された VPN ソフトが、サーバに送るパケットを別プロトコルのパケットで包み (カプセル化)、宛先として VPN 装置のアドレスを付けて、異なるプロトコルやアドレス体系でも通過できるようにします。企業イントラネットに設置された VPN 装置は、送信されてきたパケットから本来のパケットを取り出し、アクセス対象のサーバに送信します。この処理により、リモートアクセス端末とサーバ間にトンネルを掘って直接つないでいるように使うことができます。

また、カプセル化を行う際に内容を暗号化することにより、盗聴されてもデータの内容や送り先を判読できないようにすることができます。 さらに VPN 通信を開始する前に、通信相手との間で認証の方法を決めておき、パケットに認証の情報を付けておくことにより、不正な通信を遮断できるようにします。

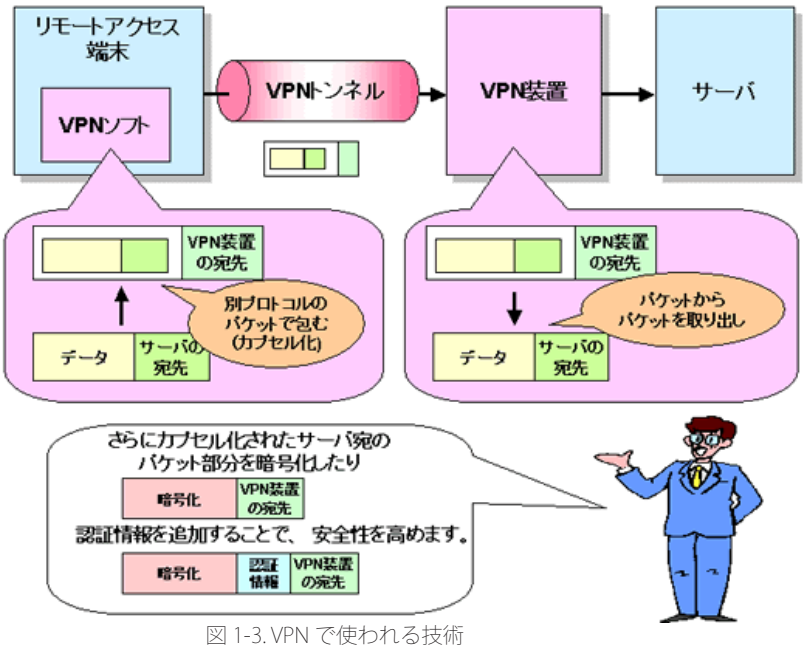


図 1-3. VPN で使われる技術

VPN を実現する主な方法としては、IPsec(Security Architecture for Internet Protocol) を使用した IPsec-VPN と、SSL(Secure Socket Layer) を使用した SSL-VPN があります。

1. 3 IPsec-VPN と SSL-VPN

IPsec-VPN とは、IP 層で暗号化・認証を行う IPsec を用いて VPN を構築する方法です。IPsec-VPN では、企業イントラネット側の VPN 装置との間に VPN トンネルを作るため、リモートアクセス端末に専用のソフトをインストールする必要があります。また､暗号化や認証のための設定など環境設定項目が多く、ユーザに負担がかかります。

SSL-VPN は、リモートアクセス端末と企業イントラネット側の VPN 装置間で SSL 暗号通信を行うことにより VPN を構築します。SSL 機能は、WEB ブラウザやグループウェアにあらかじめ搭載されているため、専用ソフトのインストールの必要がなく、使用可能機器の範囲も広くなっています。また、特別な環境設定を行う必要はありません。

IPsec-VPN と SSL-VPN のどこが違うのか、表にまとめると次のようになります。

	IPsec-VPN	SSL-VPN
リモートアクセス端末への専用ソフトインストール / 環境設定	× 必要 環境設定も複雑 (専用ソフトは、IPsec-VPN 装置と同一メーカーの製品が原則)	○ 不要 専用ソフトが必要な場合は自動インストール、自動環境設定
リモートアクセス端末機器 (各社の製品ごとにサポート機器は異なります)	△ 専用ソフトが対応している装置（パソコンが中心）	○ パソコン PDA、携帯電話 (WEB ブラウザ使用)
コンテンツやサーバに対するアクセス制御	△ 難しい	○ 容易
初期導入コスト	○ 低い	△ 高い
運用管理コスト	△ 高い	○ 低い
既存ネットワークへの適用性	△ NAT(アドレス変換)、ファイアーウォール越えなどの考慮が必要	○ シームレスに導入可能
性能 (処理速度・アクセス速度)	○ SSL-VPN より高速	△ IPsec-VPN より低速

このように、リモートアクセスにおいては、SSL-VPN が IPsec-VPN よりも適していると言えます。ただし、リモートアクセスのように拠点と不特定多数の地点ではなく、拠点と拠点といった決まった地点を接続する場合には、専用ソフト管理などの運用コストが抑えられるため、高速な IPsec-VPN の方が適しています。

本書では以降、SSL-VPN について、SSL 通信の仕組みや、SSL-VPN を実現する具体的な方式、また安全性を高めるために必要な認証やアクセス制御について説明していきます。

2. SSL-VPN の基本動作

第 1 章で説明しました通り、SSL-VPN は、リモートアクセス端末と企業イントラネット間を SSL で通信します。 そこで、まず SSL ではどのようにしてインターネット上での安全な通信を実現しているかを説明します。

2. 1 SSL 通信で使われている技術

SSL では、暗号化や認証といった複数の技術を用いて通信の安全性を高めています。

● 暗号化

盗聴を防ぐために有効な方法として挙げられるのが、暗号化です。 暗号化は、ある条件に基づき決まった手順に従ってデータを変換することです。変換に使う条件は「鍵」、変換の手順はアルゴリズムと呼ばれます。

例：古代ローマのシーザー (カエサル) が使ったと言われる、アルファベットを 3 文字ずらす (ABC → DEF)「シーザー暗号」の場合、鍵が「3」、「アルファベットを鍵の数だけずらす」がアルゴリズムとなります。

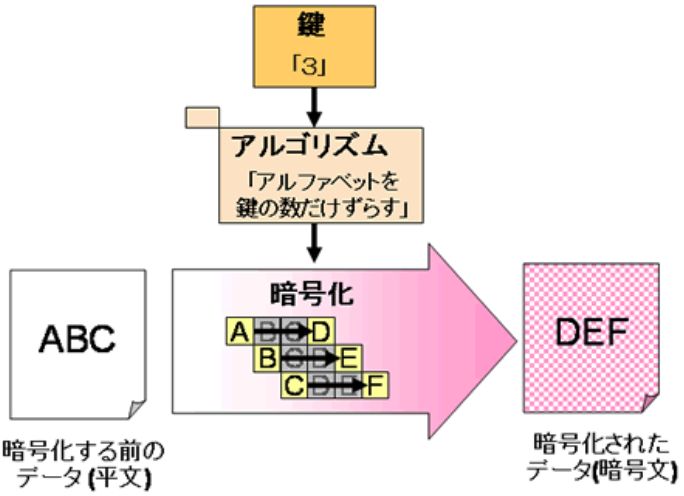


図 2-1. 暗号化の仕組み

シーザー暗号で暗号化されたデータは、暗号化と同じ鍵の数だけアルファベットを逆にずらせば元に戻せます。このように、データの暗号化と、受信した暗号文を元に戻す復号化のために同じ鍵を使う方式を、共通鍵暗号方式と呼びます。この場合、鍵 (共通鍵と呼びます) を第三者に知られると暗号文を解読されてしまうため、盗聴や情報漏えいの危険性があります。このため、共通鍵は当事者しか知らないようにする必要があります。

共通鍵暗号方式では、同じ鍵を相手と自分が持っていなくてはならないため、鍵を相手に必ず渡しておかなければなりません。鍵をそのまま平文で渡すと、盗まれてしまう可能性があります。かといって暗号化して送っても、相手が鍵を持っていないので復号化できません。
この鍵の受け渡しの問題を解決するために考案されたのが、

・データの暗号化と復号化の鍵を別にする

方法です。
この方法では、片方の鍵で暗号化したものはもう一方の鍵でしか元に戻せない鍵のペアを作ります。そして、片方の鍵だけを通信相手に渡し（こちらの鍵を公開鍵と呼びます）、残った方は本人だけが使えるよう厳重に管理しておきます（こちらは秘密鍵と呼びます）。公開鍵を受け取った通信相手は、その鍵を使ってデータを暗号化して送信します。

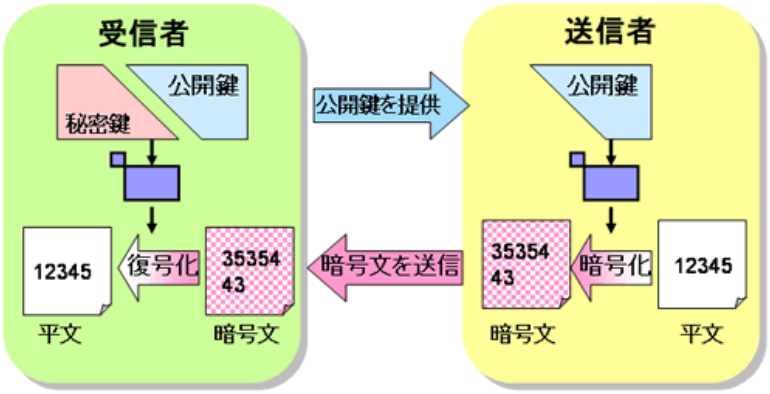


図 2-2. 公開鍵を使った暗号化

暗号化されたデータを元の平文に戻せるのは秘密鍵だけなので、公開鍵が受け渡しの途中で盗まれても問題ありません。この方法は、公開鍵暗号方式と呼ばれています。（但し、この方式は暗号化と復号化の計算が複雑で時間がかかるため、大量のデータの暗号化には公開鍵で共通鍵を暗号化して送るハイブリット暗号方式が用いられます）

公開鍵暗号方式で使われる公開鍵・秘密鍵を使うと、通信されてきたデータが本当に通信相手からのものなのか見分けることもできます。
通信相手に公開鍵を渡している状態で、秘密鍵でデータを暗号化して送信した場合、通信相手はデータが公開鍵で復号できるか否かによって、正しい通信元からのものなのかを判断できます。これは、通信データに署名や実印を押して送っているようなものなので、電子署名と呼ばれます。

しかし、公開鍵暗号方式にも実は問題があります。公開鍵の受け渡しの際に、第三者が通信相手になりすましていた場合、公開鍵で重要な情報を暗号化して送信しても、鍵自体がなりすましている第三者からのものであるため、

簡単に情報を復号化されてしまい、情報漏えいの脅威につながる危険性があります。

● 公開鍵の認証方法

公開鍵のなりすまし問題を解決するため、公開鍵の正当性を信頼できる機関 (認証局) によって証明してもらう方法が考案されています (この方法は、役所に行って印鑑証明書を作り、本人証明として相手に提示することによく似ています)。

公開鍵の認証方法の例として、下の図を使って、クライアントである A さんに対しサーバの B さんが公開鍵を渡すケースを説明します。

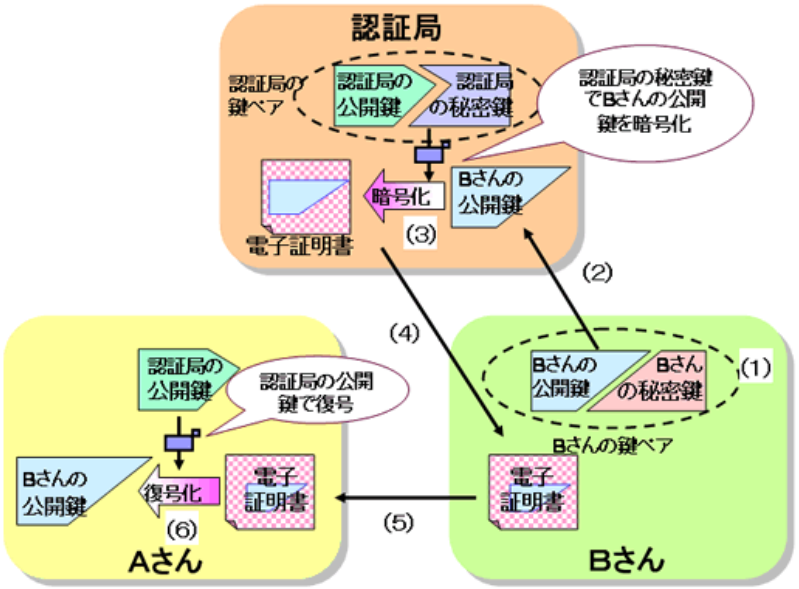


図 2-3. 認証局を使った公開鍵の認証方法

(1)B さんは公開鍵と秘密鍵のペアを作成します

(2)B さんの公開鍵を認証局に送付し、公開鍵が本物であることを証明する電子証明書の作成を申請します

(3) 認証局で B さんの身元を審査し、問題ないことを確認後、B さんの公開鍵を認証局の秘密鍵で暗号化し、電子証明書を作成します

(4) 認証局は、作成された電子証明書を B さんへ送信します

(5)A さんが B さんと暗号通信を開始する時に、B さんから A さんへ電子証明書を送付します

(6)A さんが認証局の公開鍵を使って電子証明書から B さんの公開鍵が取り出せれば、B さんからの公開鍵であることが証明されます

この認証方法は、認証局は B さん以外の人に B さんの電子証明書を出さない、という前提の元に成り立ちます。このため、認証局には必ず信頼できる機関を選択することが重要です。

2. 2 SSL 通信の流れ

下の図を使って、クライアントとサーバ間の SSL 通信の流れについて説明します。
まず、サーバは秘密鍵と公開鍵を作り、認証局から電子証明書をもらってきておきます。クライアントは、認証局の公開鍵を持っておく必要がありますが、有名で信頼性の高い認証局の公開鍵は、既に WEB ブラウザなどに入っているため、特に何もしなくても大丈夫です。

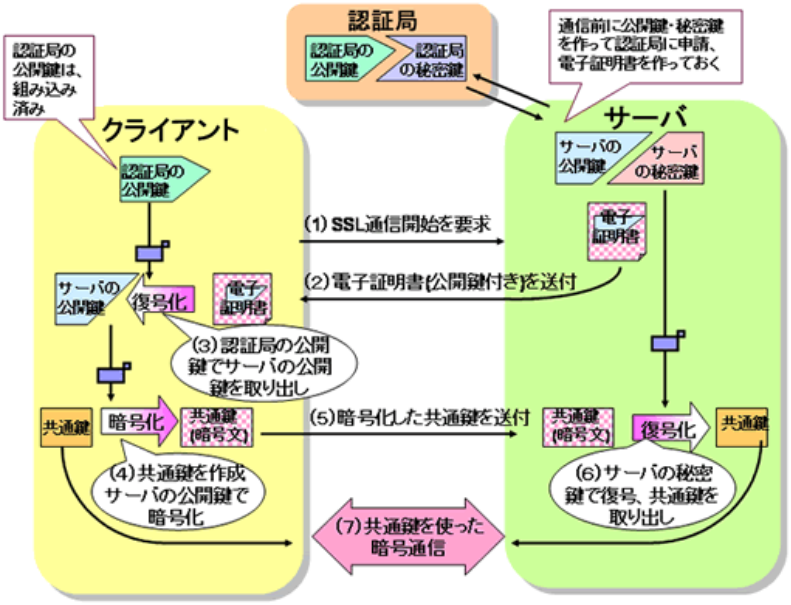


図 2-4. SSL 通信の流れ

(1) クライアントは、サーバに対し、SSL で通信したいことを告げます
(2) 通信を受けたサーバは、クライアントにサーバの公開鍵を含む電子証明書を送ります
(3) クライアントは、認証局の公開鍵で電子証明書からサーバの公開鍵を取り出します
(4) クライアントはサーバとの通信で使う共通鍵を作り、サーバの公開鍵で暗号化します
(5) クライアントは暗号化された共通鍵をサーバに送信します
(6) サーバは、サーバの秘密鍵で共通鍵を復号化して取り出します
(7) サーバ・クライアントともに共通鍵を入手したので、以降はこの共通鍵を使って暗号通信を開始します（SSL 通信確立）

ここまで、SSL 通信の概要について解説してきました。それでは、次からこの SSL 通信を使った SSL-VPN が、どのように実現されているかを見ていきます。

3. SSL-VPN の実現方法

SSL-VPN では、これまで説明してきた SSL と様々な機能を組み合わせて VPN を構築します。

まず、SSL-VPN を実現する最も簡易な方式である「リバースプロキシ方式」について、説明していきます。
その後、より幅広いアプリケーションに対応する方法として、「ポートフォワーディング方式」と「L2 フォワーディング方式」について説明します。

3. 1 リバースプロキシ方式

リバースプロキシとは、インターネットからイントラネット内のサーバへのアクセスを中継する機能です（通常のプロキシサーバは、イントラネットからインターネットへ中継するため、本機能はリバース (逆の）プロキシと呼ばれます)。
リバースプロキシ方式は、SSL とリバースプロキシを組み合わせて、インターネット上に公開されていない、イントラネット内のサーバ（WEB やファイル、FTP サーバ）にアクセスすることを可能にします。

それでは、次の図でリバースプロキシ方式がどのようにおこなわれるか、見ていきましょう。
まず前準備として、企業イントラネットに設置された VPN 装置に、外部からのアクセスする場合とイントラネット内からアクセスする場合のサーバの URL を設定しておきます。

(1) 利用者は、リモートアクセス端末で WEB ブラウザを開き、HTTPS(WEB でのデータのやり取りに使う HTTP に SSL を対応させたもの) で VPN 装置へアクセスします (HTTPS を使う場合、URL の最初が "https:// ～ " となります)

(2)VPN 装置は受け取ったアクセスを解析し、企業イントラネット内のサーバのアドレスに変換します。この時、企業イントラネット内のサーバは SSL 対応していないので、VPN 装置が HTTPS を HTTP に変換します。

(3)VPN 装置は、サーバにアクセス、サーバからの応答を VPN 装置が受け取って HTTPS に変換し、リモートアクセス端末へ返します。

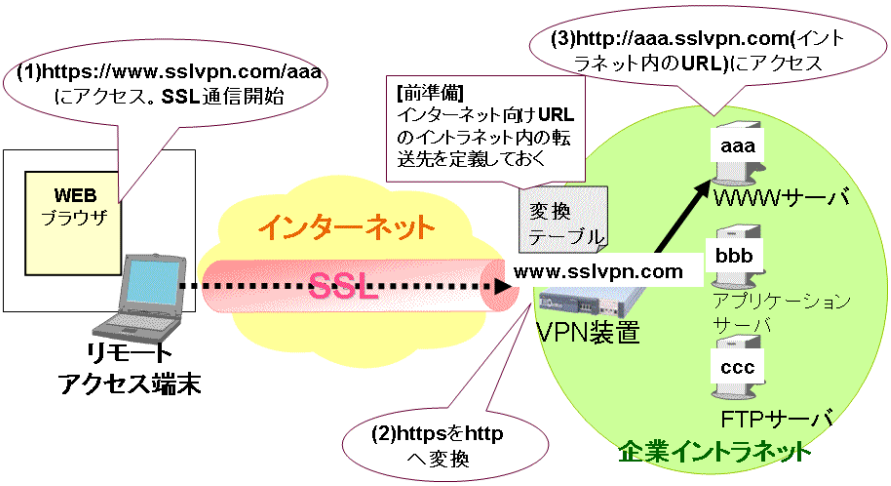


図 3-1. リバースプロキシ方式

この方法の利点としては、WEB ブラウザで URL を指定するだけで、簡単に安全に企業イントラネット内にアクセスできることが挙げられます。アクセスしたい企業イントラネット内のサーバを直接インターネットに接続しなくてすむため、企業イントラネットの既存のポリシーの変更の必要がなく、ポリシー変更に伴うサーバの設定ミスで機密情報を公開してしまった、などの危険性を避けることができます。

一方、WEB ブラウザ上で動作しないとアプリケーションが使えないため、サポートできるアプリケーションが限られてしまいます。

3. 2 WEB 以外のアプリケーションを使う方法

リバースプロキシ方式では、インターネット上の通信の SSL 化に WEB ブラウザの SSL 機能を使っているため、WEB ブラウザで動作しないアプリケーションは使えませんでした。そこで考えられたのが、リモートアクセス端末に Java や ActiveX で作られたモジュールを追加して通信を SSL 化する方法です。

SSL-VPN のモジュールの仕様は各社で様々ですが、多くの製品の場合、利用者の負担を増やさないよう、WEB ブラウザからモジュールが自動でダウンロード、自動設定されるようになっています。中には、SSL-VPN の使用が終了したら、モジュールを自動削除し、設定をインストール前に戻すことにより、リモートアクセス端末への負荷を抑えるようになっているものもあります。

モジュールを使った方式の内、代表的なものとして、ポートフォワーディング方式と L2 フォワーディング方式があります。続く 3.3 章で、ポートフォワーディング方式を、3.4 章で L2 フォワーディングを説明します。

3. 3 ポートフォワーディング方式

一般的に企業イントラネットとインターネットの間には、ファイアーウォールを設置し、インターネットから利用できる企業イントラネットのアプリケーションを制御します (WEB サイトは参照できるが、Telnet はできないなど)。制御には、通信されるデータに含まれる、ポート番号と呼ばれるアプリケーションの種類を示す情報が使われます。

ポートフォワーディング(別名ポート転送、ポートマッピング)とは、ファイアーウォールを通過できないアプリケーションのデータのポート番号を、通過できるアプリケーションのポート番号に変換することにより、企業イントラネットとインターネットとの間の通信を可能にする機能です。ポートフォワーディング方式では、この機能を用い、任意のアプリケーションの通信を HTTPS のポート番号に変換し、ファイアーウォールを通過させることで SSL-VPN を実現します。

それでは、下の図でポートフォワーディング方式がどのように行われるか見ていきましょう。
まず前準備として、企業イントラネットに設置された VPN 装置に、外部からのアクセスを許す企業イントラネット内のサーバのアドレスとポート番号を設定しておきます。

(1) 利用者は、リモートアクセス端末の WEB ブラウザから、VPN 装置に HTTPS でアクセス、ポートフォワーディング用モジュールをダウンロードします

(2) リモートアクセス端末にインストールされたモジュールが、VPN 装置との間に SSL 通信のための SSL トンネルを確立します
モジュールは、リモートアクセス端末の hosts ファイル (コンピュータ名のホスト名に対応する IP アドレスを記述したファイル。通信の前に参照) を編集し、アプリケーションが企業イントラネット内のサーバにアクセスしようとした時、そのデータがモジュールに送られるようにしておきます
(3) 利用者は、リモートアクセス端末でアプリケーションを起動し、企業イントラネット内のサーバにアクセスします
(4) アプリケーションのデータは、編集された hosts ファイルにより、モジュールが取得。HTTPS 化し、(2) で確立された SSL トンネルを使って、VPN 装置へ送信します
(5)VPN 装置は、受け取った HTTPS データを復号化して、アプリケーションのデータを取り出します
(6)VPN 装置は、前準備で定義されている企業イントラネット内のサーバの情報 (アドレスやポート番号) を元に、アプリケーションのデータをリモートアクセス端末がアクセスしたいサーバに送信します。サーバは受け取ったデータの応答を VPN 装置へ送り、VPN 装置がデータを HTTPS 化してリモートアクセス端末へ送信します※この方式では、(3) で hosts ファイルを変更するため、リモートアクセス端末で管理者権限が必要です

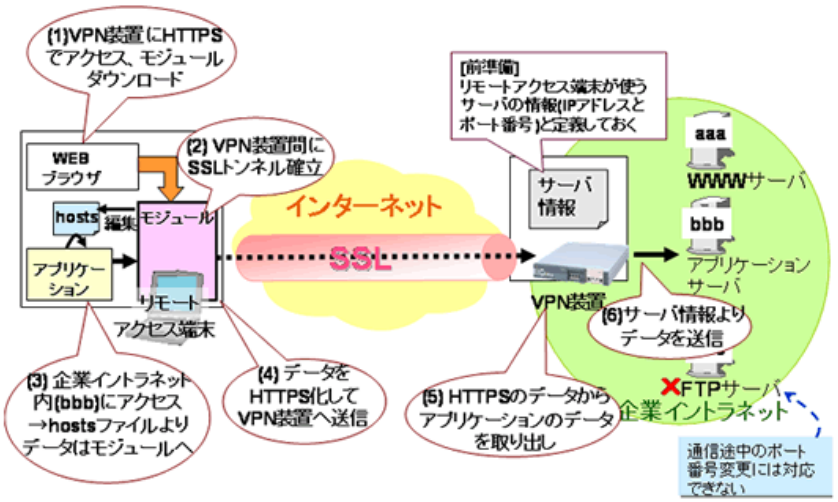


図 3-2. ポートフォワーディング方式

以上により、ポートフォワーディング方式では、WEB アプリケーション以外のデータもモジュールが HTTPS 化することにより、SSL-VPN を実現します。但し、ポートフォワーディング方式では、企業イントラネット内で使えるサーバのポート番号を VPN 装置に定義しておかなくてはいけないため、FTP(アクティブモード) や MSN Messanger でのファイル転送など、通信中にポート番号が変わるアプリケーションは使えない場合があります。

3. 4 L2 フォワーディング方式

L2 フォワーディングは、アプリケーションのデータを HTTP のパケットに入れてカプセル化し、SSL で暗号化する方式です。カプセル化するデータは、サーバのポート番号や IP アドレスなどが含まれたデータ (OSI 参照モデルでいうところの第二層 (Layer 2) のデータ) であるため、“L2” フォワーディング方式、または ”L2” カプセル方式と呼ばれます。L2 フォワーディング方式では、ポートフォワーディング方式と異なり、VPN 装置側で定義ファイルにポート番号を設定しておく必要がないことから、幅広いアプリケーションをサポートすることが可能です。

それでは、次の図で、L2 フォワーディング方式がどのように行われるか見ていきましょう。
まず前準備として、企業イントラネットに設置された VPN 装置にリモートアクセス端末用に、企業イントラネット内のサーバの使っていない IP アドレスを設定しておきます。

(1) 利用者は、ポートフォワーディング方式と同じように、リモートアクセス端末の WEB ブラウザから、VPN 装置に HTTPS でアクセス、L2 フォワーディング用のモジュールをダウンロードします
(2) リモートアクセス端末にインストールされたモジュールは、VPN 装置との間に SSL 通信のための SSL トンネルを確立します
また、リモートアクセス端末上に、NIC(ネットワークカード) が追加されたかのように見える仮想 NIC を構築し、送信するデータは全て仮想 NIC を通るように設定します。仮想 NIC には、VPN 装置で設定された企業イントラネット内の IP アドレスがに割り当てられます
(3) 利用者は、リモートアクセス端末でアプリケーションを起動し、企業イントラネット内のサーバにアクセスします
(4) アプリケーションのデータは、仮想 NIC によって宛先をチェックされ、企業イントラネット内のサーバ宛の場合、モジュールにより HTTPS 化されます (この時データの送信元には、仮想 NIC の IP アドレスが設定されています)。その後データを (2) で確立された SSL トンネルを使って、VPN 装置へ送信します
(5)VPN 装置は、受け取った HTTPS データを復号化して、アプリケーションのデータを取り出します
(6)VPN 装置は、データを企業イントラネット内のサーバに送信します。サーバは受け取ったデータの応答を、送信元のリモートアクセス端末の仮想 NIC 宛に送りますが、前準備により VPN 装置へ回送され、VPN 装置がデータを HTTPS 化してリモートアクセス端末へ返します

※この方式では、(2) で仮想 NIC をインストールするため、リモートアクセス端末で管理者権限が必要です

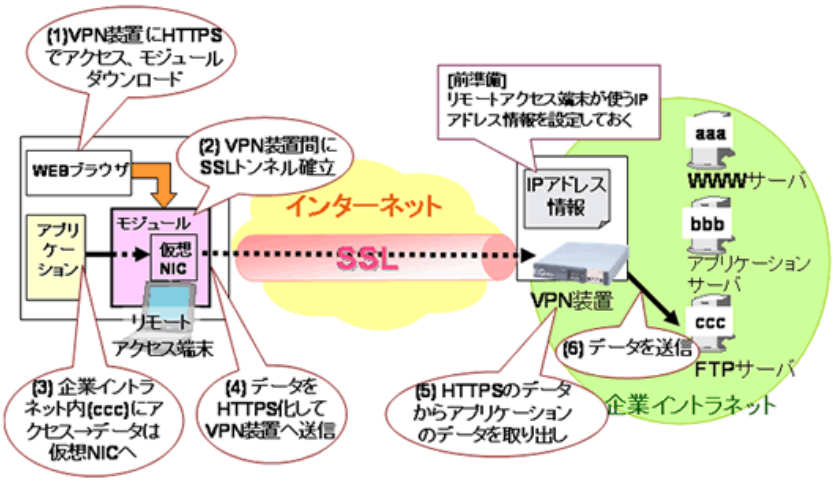


図 3-3.L2 フォワーディング方式

この方式では、リモートアクセス端末で HTTPS 化される前のデータの宛先には企業イントラネット内サーバのアドレス、VPN 装置が取得する企業イントラネット内のサーバが返答するデータにはリモートアクセス端末の仮想 NIC のアドレスが設定された状態になっており、ポートフォワーディング方式と異なり、 VPN 装置でデータの宛先やポート番号の設定が必要ないため、通信途中でポート番号が変わるアプリケーションも使用可能です。但し、本方式ではリモートアクセス端末の対象 OS が Windows のみの製品が多く見受けられます。

3. 5 まとめ：SSL-VPN の実装方式の比較

これまで、SSL-VPN を実現する方法として、リバースプロキシ方式、ポートフォワーディング方式、L2 フォワーディング方式の 3 方式について説明してきました。 各方式の違いをまとめると、以下のような表になります。

	リバースプロキシ方式	ポートフォワーディング方式	L2 フォワーディング方式
リモートアクセス端末側構成要素	WEB ブラウザ	WEB ブラウザ＋モジュール (WEB からダウンロード、自動インストール)	WEB ブラウザ＋モジュール (WEB からダウンロード、自動インストール) 使用可能アプリケーション
使用可能アプリケーション	△ WEB アプリケーション	○ 通信中ポート番号が変わるものは使用できない場合あり	◎ ほとんどのアプリケーションで使用可能
リモートアクセス端末機器 (各社の製品ごとにサポート機器は異なります)	○ WEB ブラウザが動く端末	△ モジュールの仕様によって制限 利用時に管理者権限が必要	△ モジュールの仕様によって制限 (Windows2000 以上の場合が多い) 利用時に管理者権限が必要
用途	出張先の端末などから簡単に使いたい 使用アプリケーションは WEB メールや WEB 型グループウェアなど WEB ページ中心	クライアント端末の OS が様々である ある程度の種類のアプリケーションを使いたい	アプリケーションを制限なく使いたい 使用されるクライアント端末の種類は限られている

SSL-VPN を導入しようとする場合、それぞれの特徴を把握し、自社のネットワークポリシーや利用機器にあった方式を選択することが必要です。

3. 6 データの流れから見た 3 方式の違い

これまで説明してきた、リバースプロキシ方式、ポートフォワーディング方式、L2 フォワーディング方式について簡単に処理方法や使用できるアプリケーションの違いを説明してきました。
ここからは、何故その違いが出てくるのか、データの流れから、詳細な説明をしておきます。

ネットワークを理解する場合、OSI 参照モデルと呼ばれる階層モデルがよく使われます。このモデルは、沢山ある通信プロトコル (コンピュータ同士が通信を行おうとする場合、相手と何をどんな形式でどのようにやり取りするのかを決めたもの) を機能ごとに 7 つの階層に分けて定義したものです。階層化により、ある階層内の処理を考えるときには別の階層内の処理のことは考えなくても済むなど、各層の機能の独立性が高くなったことで様々なネットワーク機器

の組み合わせ、メーカーの異なるコンピュータでの通信ができるようになりました。

OSI 参照モデルに通信プロトコルを当てはめると以下のようになります。

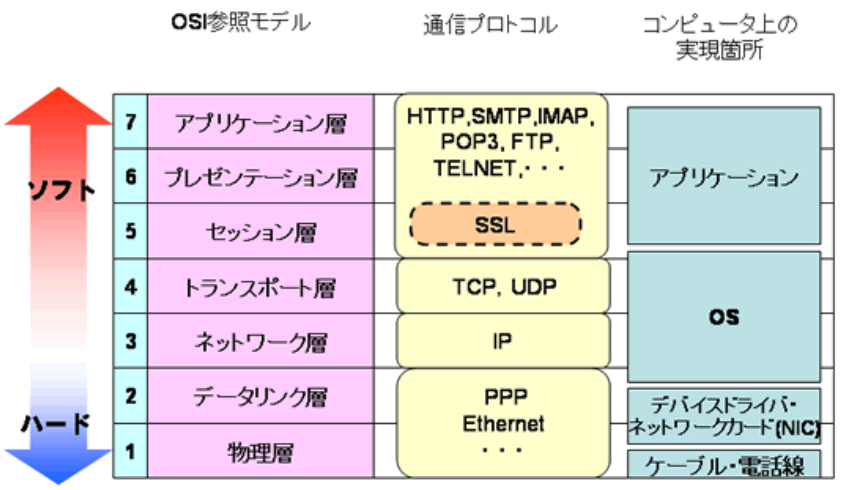


図 3-4.OSI 参照モデル

このモデルでは、他のコンピュータへデータを送信する場合、上の階層から下の階層へと流れていくと考えます (受信の場合は、逆に下から上へ流れます)。送信データは階層を移動するごとに、ヘッダーと呼ばれるその層で処理する情報を付けられて下の層へ渡されます。下の層は、上の層から来たデータ (ヘッダー付) の内容を見ずひとかたまりと見なし、自分の層のヘッダーを付けて、下の層に渡します (このようにして上の層から下の層へとデータを引き渡す仕組みをカプセル化といいます)。

各階層を流れるデータの処理は、図の右側に示すように、アプリケーション、OS、ドライバなどが手分けして行っています。SSL-VPN で使用している SSL プロトコルは、アプリケーションが担当します。

リバースプロキシ方式では、下の図のようにリモートアクセス端末の SSL を担当するアプリケーションとして WEB ブラウザを使って SSL-VPN を実現しています。このため、リバースプロキシ方式は、WEB ブラウザで動作しないアプリケーションは使えません。

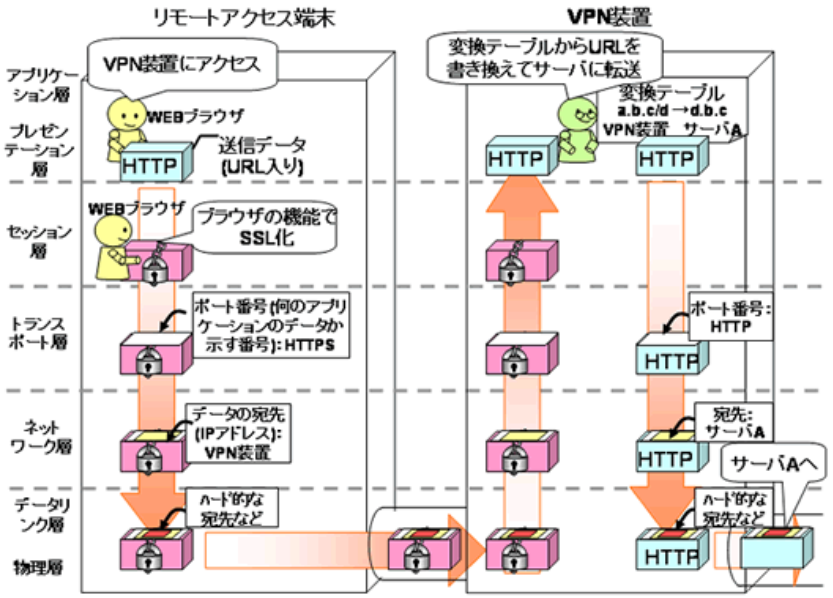


図 3-5. リバースプロキシ方式

これに対し、ポートフォワーディング方式では、リモートアクセス端末で企業イントラネット内にアクセスしようとしたデータを、モジュールが取得して SSL 化することで、WEB ブラウザによらないアプリケーションの SSL-VPN 対応を実現しています。

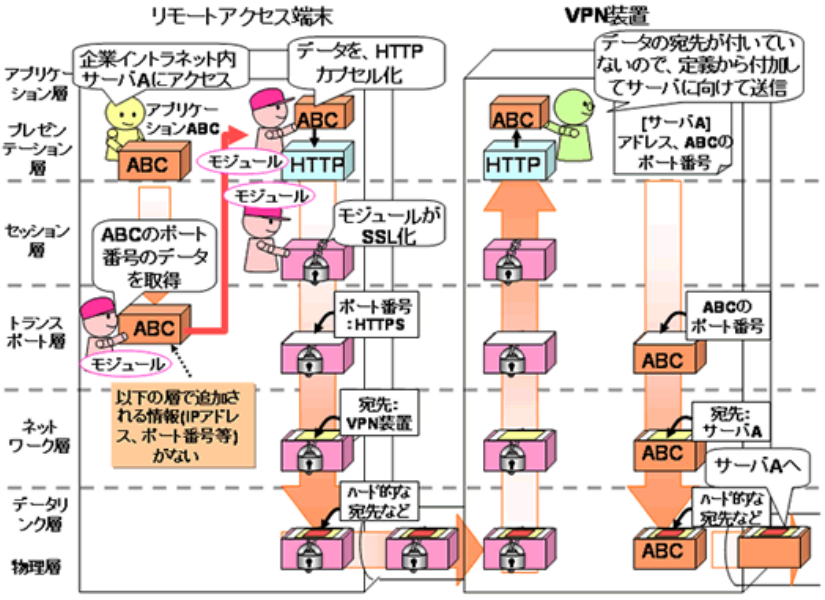


図 3-6. ポートフォワーディング方式

ポートフォワーディング方式では、モジュールは、データの送信先がリモートアクセス端末自身を示す IP アドレス (127.0.0.1：ループバックアドレス)、かつ VPN 装置で設定されたアプリケーション (上記の図では ABC) のポート番号を持つデータを取得するよう設定され、トランスポート層でデータが来るのを待っています。 本方式使用時には、モジュールにより hosts ファイルで企業イントラネット内サーバのホスト名に対応する IP アドレスにループバックアドレスが設定されているので、ABC が作った企業イントラネット内向けのデータは自分宛になり、モジュールに取得されます。
取得されたデータは、アプリケーション層で HTTP カプセルされますが、この時カプセル化されるデータには、ポート番号や IP アドレスなどが付いていない状態になっています。このため、データを受信した VPN 装置でカプセル化を解除してデータを取り出した後に、それらの情報を付ける必要があります。このため、予め企業イントラネット内のサーバの IP アドレスやポート番号を VPN 装置に設定しておかなければならず、ポート番号が固定ではないアプリケーションは対応し難くなっています。

L2 フォワーディング方式では、ポートフォワーディングよりも下の階層で、モジュール (仮想 NIC) がアプリケーションのデータを取得します。

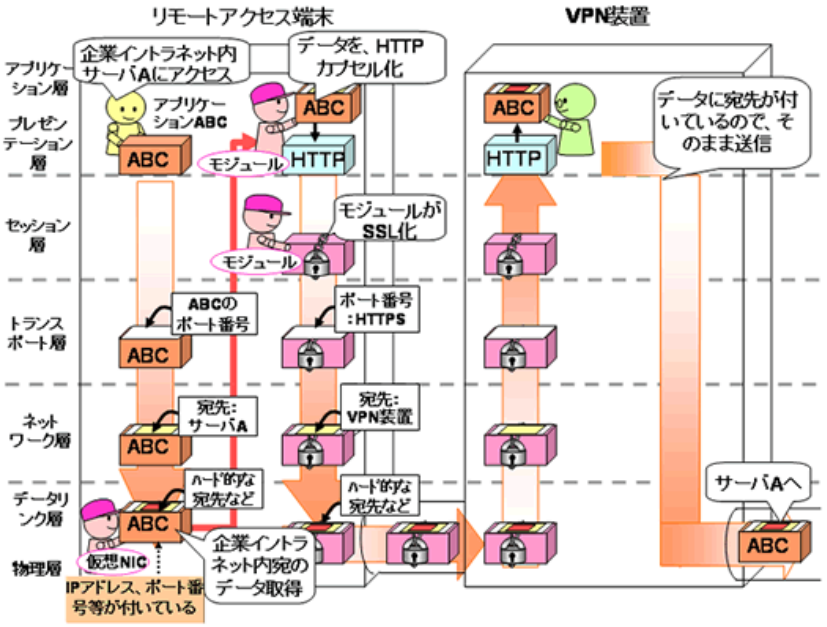


図 3-7.L2 フォワーディング方式

L2 フォワーディング方式では、HTTP カプセル化するデータには IP アドレスやポート番号などが付いた情報なので、VPN 装置側での追加が必要ないため、3 方式の中で、使用できるアプリケーションの制限が最も少なくなっています。但し、仮想 NIC が ActiveX で作られていたり、インストールに ActiveX コントロールが使われている製品が多いため、リモートアクセス端末が Windows 限定になってしまうことがあります。

ここまで説明してきた SSL-VPN の各実現方法により、インターネット上の経路の安全性を高めることが可能です。しかし、より安全な通信を行うためには、企業イントラネット内にアクセスする場合の認証や使用範囲の制限などが必要です。次章では、SSL-VPN で使われるユーザ認証やアクセス制御について説明します。

4. SSL-VPN のセキュリティ向上 (認証とアクセス制御)

SSL-VPN は、専用ソフトを使わず企業イントラネット内への自由なアクセスを実現するため、利便性、簡易性の面で優れています。しかし、見方を変えると、悪意を持った第三者の不正侵入の危険性を高めることにもなります。また、近年リモートアクセスが原因で、企業イントラネット内部へウイルスが侵入するケースも増えています。
今回は、一般的な SSL-VPN 装置に搭載されている、リモートアクセスの安全性を高めるための以下の機能について説明します。

・ユーザ認証
・ アクセス制御
・エンドポイントセキュリティ

4. 1 ユーザ認証

IPsec-VPN の場合、リモートアクセス端末側に専用ソフトのインストール、および設定に使う情報 (鍵) の登録が必要なことが、不正侵入を防ぐことに役立っていました。これに対し、SSL-VPN では専用ソフトを使用しないため、よりしっかりしたユーザ認証を行うことが重要です。
ネットワークで使われている代表的なユーザ認証方法としては、パスワードを使う方法や電子証明書を使う方法が挙げられます。

【パスワードを使った認証】

● 固定パスワード
パスワードによる認証でよく使われるのが、毎回同じパスワードを用いる固定パスワードと呼ばれる方法です。この方法は単純で利用者への負担も軽いなど利点もありますが、入力時の第三者による盗み見や、キーロガーと呼ばれるキーボードからの入力を記録するソフトを仕掛けられることによりパスワードを取得されてしまうと、企業イントラネットへの不正侵入を容易に許してしまうなど問題もあります。

● ワンタイムパスワード
固定パスワードでのパスワード盗用の危険を回避するため、アクセスのたびにパスワードを変える方法です。1 回限りでパスワードが使えなくなるため、使い捨てパスワードとも呼ばれます。
ワンタイムパスワードの代表的な方式として、チャレンジレスポンス方式と同期方式があります。

a. チャレンジレスポンス方式

認証サーバから送られてくるチャレンジコードを元に、リモートアクセス端末でパスワードを暗号化して送信 (レスポンス) する方式です。フリーソフトとして公開されている Bellcore 社が開発した S/Key などがこの方式にあたります。

S/Key は以下のような仕組みで、ワンタイムパスワードを作成します。
まず、前準備として企業イントラネット内の認証サーバ (VPN 装置が兼ねる場合もあります) に利用者がパスワードを入力します。認証サーバは、入力されたパスワードに認証サーバが生成したシードと呼ばれる文字列を付けて、設定回数分暗号化して格納します (暗号化の回数はシーケンス番号と呼ばれます)。

(1) リモートアクセス端末から、認証サーバにユーザ ID を送ります
(2) 認証サーバは、シーケンス番号とシードをリモートアクセス端末へ送信します
(3) 利用者は、認証サーバに入力したパスワードを、送られてきたシーケンス番号とシードを元に暗号化します。暗号結果がワンタイムパスワードになります
(4) リモートアクセス端末から、ワンタイムパスワードを認証サーバへ送信します
(5) 認証サーバで、送られてきたワンタイムパスワードが一致すれば、認証は成功です

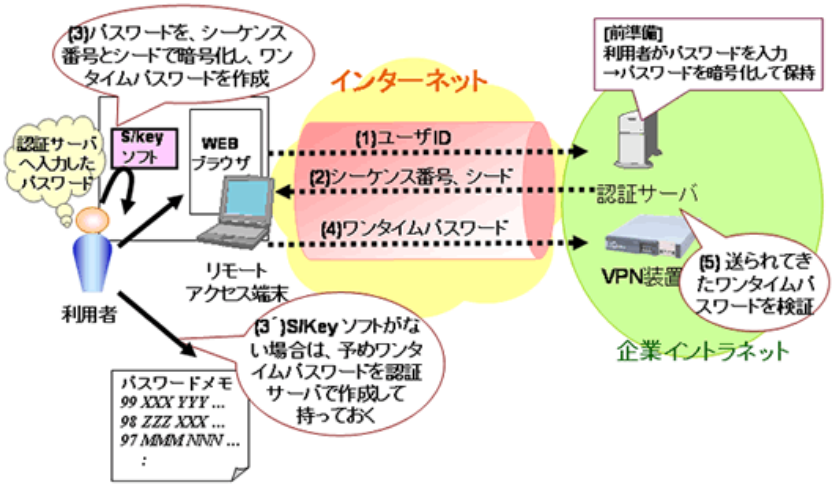


図 4-1.S/Key によるユーザ認証

S/Key では、(3) で計算に使うシーケンス番号が認証が成功するたびに減っていくため、ワンタイムパスワードは毎回変わります。シーケンス番号が 0 になると、強制的に認証サーバにパスワードの再登録が必要になります。但し、この方法を使うには、ワンタイムパスワード計算用のソフトのリモー

トアクセス端末へのインストールが必要となり、SSL-VPN の利点であるクライアントレスが損なわれることになります。予めアクセスする回数分のワンタイムパスワードを認証サーバで計算し、メモなどに書いて持っておくこともできますが、その場合はメモの管理に細心の注意が必要です。

b. 同期方式

クライアント端末と認証サーバで、同期する情報を用いて、パスワードを生成する方法です。同期する情報には、時間 (タイムシンクロナス方式) や利用回数 (カウンタ同期方式) などが使われます。この方式として有名なものに、RSA Security 社の SecurID(タイムシンクロナス方式) があります。

この方法では、トークンと呼ばれる、パスワードを生成する機器を利用者が持つことになります。トークンには、カードやキーホルダーなどのハードトークンと、PC や携帯端末などにインストールするソフトトークンがあります。

利用者は、前準備として、トークンと認証サーバの同期情報を合わせておきます。リモートアクセス端末から認証サーバにアクセスする時、利用者はトークンに表示されるトークンコードと予め設定されている識別情報 (PIN：Personal Identification Number) からワンタイムパスワードを作成して入力し、認証サーバに送信します。認証サーバでも、同期情報を元にワンタイムパスワードを作成し、送られてきたものと比較して認証を行います。

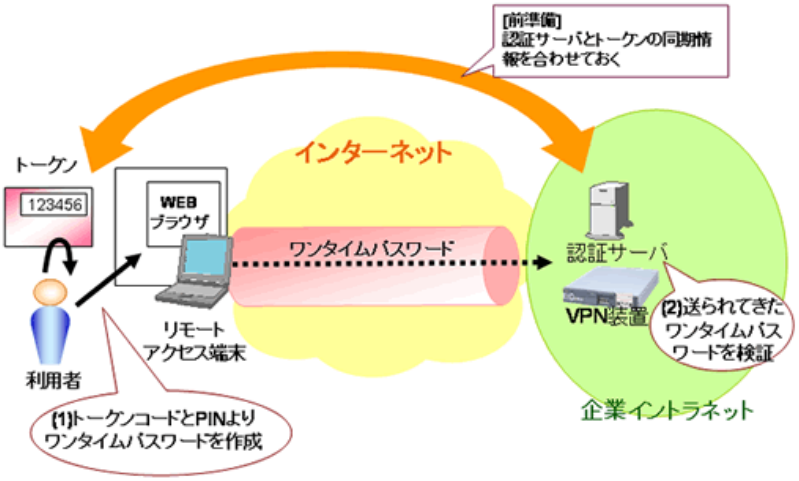


図 4-2. 同期方式によるユーザ認証

この方法の場合、同期情報が変化するごとに、ユーザが入力する情報が必ず変わるため、盗み見等の対策として有効です。但し、利用者のトークン常備が必要になり、特にハードトークンを紛失したり壊したりした場合には、再度購入しなければなりません。

c. その他の方式

ワンタイムパスワードにはこの他にも、画面上にランダムに表示される数字や文字の絵の表から、利用者が決めておいた位置にあるものをパスワードとして入力する、マトリクス認証などがあります。

【電子証明書を使った認証】

今度はパスワードを使うのではなく、第 2 章で説明した電子証明書を使ってアクセスの正当性を判断する方法を説明します。

この方法は、リモートアクセス端末用の電子証明書 (クライアント証明書) を作っておき、VPN 装置との SSL 通信開始時に、VPN 装置からの電子証明書を受け取るだけではなく、リモートアクセス端末からもクライアント証明書を送り、VPN 装置側で証明書の内容をチェックすることにより、正当なユーザからのアクセスかどうかを判断します。

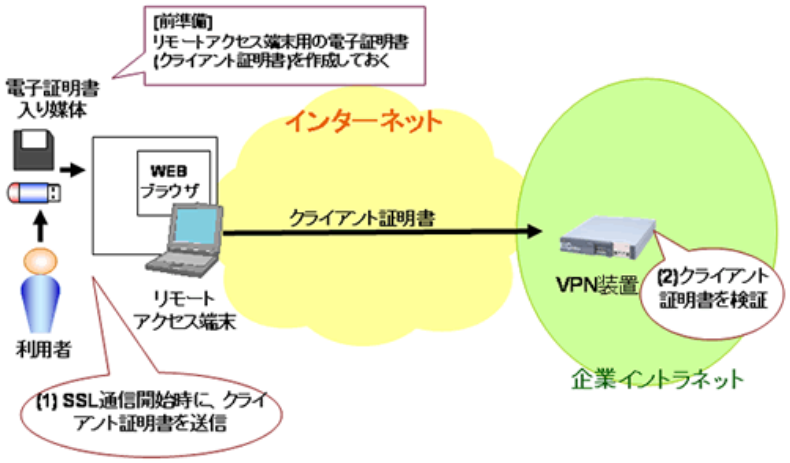


図 4-3. クライアント証明書によるユーザ認証

この方法では、SSL 通信で使用する電子証明書を使用するため、VPN 装置側に認証用ソフト等をインストールしたり、認証サーバを構築したりする必要がありません。但し、利用者はリモートアクセス端末のためのクライアント証明書を入手し、VPN 装置に送信できるよう設定するなどの作業が必要になります。このため、利用者は、クライアント証明書をリモートアクセス端末にインストールして持ち歩くか、フロッピィディスクや USB メモリ、IC カードなどに入れて携帯しておかなければなりません。
また、インターネットカフェなどでアクセス後、WEB ブラウザにクライアント証明書が残っていたりすると、不正侵入の危険性がありますので、必ず削除するなど注意が必要です。

【認証の組み合わせ】

これまで説明してきた認証方法は排他的なものではありません。複数の認証方法を組み合わせて使った場合、最終的にアクセスするためには全ての認証方法を破らなくてはならないため、不正侵入へのハードルを高くすることができます。
但し、複数の認証方法の組み合わせは、ユーザ認証のセキュリティを向上させますが、認証手順の増加など利用者の負担も大きくなります。

ユーザ認証の方法にはそれぞれ一長一短があるため、利用者のスキルや環境(利用端末の種類や、トークンや証明書の所有方法など)を考えて選ぶことが重要です。また、ユーザ認証に LDAP(Lightweight Directory Access Protocol) や RADIUS(Remote Authentication Dial-In User Service) 等を使うことも考えられます。このため、SSL-VPN 製品を選択する際には、連携可能な外部認証サーバも大きなポイントになります。

4. 2 アクセス制御

アクセス制御とは、設定条件に従って、サーバやネットワークへのアクセスを許可したり制限したりすることです。
SSL-VPN では実現方式によりアクセス制御が可能な範囲が異なり、使用できるアプリケーションが幅広いほどアクセス制御が難しくなっています。具体的には、L2 フォワーディング方式、ポートフォワーディング方式、リバースプロキシ方式の順に細かなアクセス制御が可能になります。

● L2 フォワーディング方式
L2 フォワーディング方式では、VPN 装置は、リモートアクセス端末と企業イントラネット内のサーバの通信データを中継するだけです。VPN 装置でアクセス制御を行う製品もありますが、通常は別途アクセス制御用にファイアーウォールなどを設定する必要があります。

● 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では、送信先の企業イントラネット内のサーバ (IP アドレス) とアプリケーションのポート番号を定義しておき、リモートアクセス端末から受け取ったデータを定義に従って、企業イントラネット内のサーバに転送します。この定義により、リモートアクセス端末のアクセス先を指定したサーバとアプリケーションのみに制限することができます。

● リバースプロキシ方式
リバースプロキシ方式では、サーバごとのアクセス制御に加え、指定した URL やディレクトリのみアクセスできるように設定できます。また、利用者ごとに、アクセスできる URL を設定することも可能です。

上記の各実現方式での特徴を踏まえて、前述のユーザ認証と組み合わせてアクセス制御を行うことにより、より利用者に合ったセキュリティ確保ができるようになります。
例) 利用者の業務内容ごとに、アクセス制御を実施

・派遣社員など利用可能な範囲を制限しておきたい場合
⇒ リバースプロキシ方式を選択し、派遣社員の所属する部の WEB サーバのみ閲覧可能
・ネットワーク管理者など全てにアクセスしたい場合
⇒ 全ての方式を利用可能とし、制限を付けない。

利用者のセキュリティのレベルによってアクセス制御

・クライアント認証とワンタイムパスワードの場合など信頼性が高いアクセス
⇒ L2 フォワーディング方式の利用を許可する
・ 固定パスワードのみなど信頼性が低いアクセス
⇒リバースプロキシ方式で、WEB ページ閲覧だけ可能

4. 3 エンドポイントセキュリティ

通常企業イントラネットは、ファイアーウォールなどにより外部から守られ、セキュリティ管理者によって内部のコンピュータのウイルス対策やパッチ適用を指導されることにより、その安全を保っています。 これに対し、SSL-VPN はインターネットから企業イントラネット内に自由にアクセスする、いわば抜け道を構築します。しかも、抜け道からアクセスしてくるのが、セキュリティ対策が取られていないインターネットカフェや個人の PC などの場合、ウイルスの持ち込みや、情報漏えいの危険性が高くなります。
このため、SSL-VPN を導入する場合には、リモートアクセス端末へのセキュリティ対策も考慮しておくことが重要です。このようなシステムの末端に接続するコンピュータへのセキュリティはエンドポイントセキュリティと呼ばれ、近年注目されてきています。
エンドポイントセキュリティの代表的な機能としては、クライアントチェッカ (別名、クライアントチェック)、キャッシュクリーナー (別名、キャッシュクリーニング、キャッシュクリーンナップ) が挙げられます。

● クライアントチェッカ
企業イントラネットへのリモートアクセスでまず懸念されるのが、リモートアクセス端末からのウイルスやワームの侵入です。これを防ぐためには、リモートアクセス端末がどういう状態にあるのかチェックし、それに応じた処理をすることが考えられます。

具体的には、予め VPN 装置に、以下のようなセキュリティポリシーに沿ったチェック項目を設定しておきます。

・OS 版数
・パッチ適用状態
・ウイルス対策ソフトやパーソナルファイアーウォールの有無
・ウイルス定義の更新状況 etc.

アクセスしてきたリモートアクセス端末を VPN 装置は設定されたセキュリティポリシーに従ってチェックし、問題が検出された場合、

・接続を拒否する
・チェック内容に応じて特定のサーバにアクセスさせる (Update サイトにのみアクセス可、など) etc.

という対策を行います。

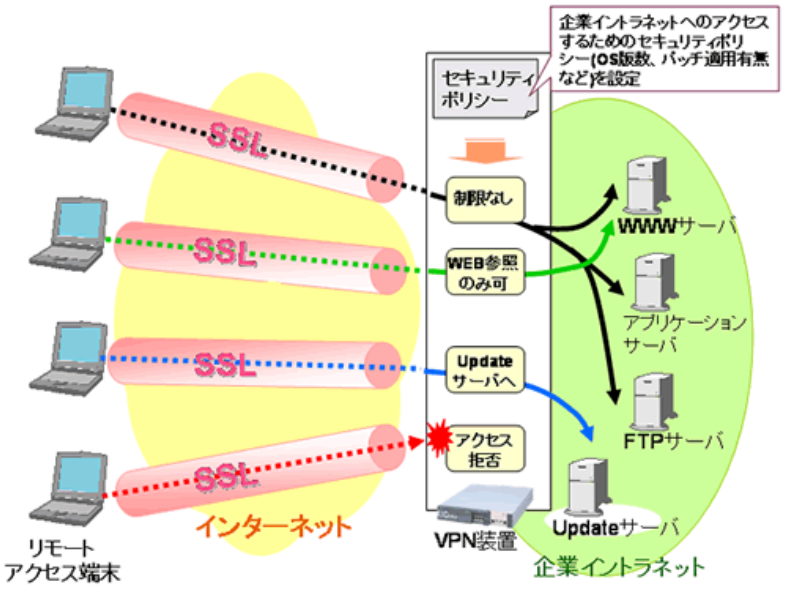


図 4-4. クライアントチェッカ

● キャッシュクリーナー

通常、WEB ブラウザは、アクセスした WEB ページの情報を一定期間キャッシュとして保持しています。このため、インターネットカフェの PC でアクセスした場合や、アクセスしたモバイル端末等を盗まれた場合、WEB ブラウザのキャッシュから企業イントラネットへの接続 URL やパスワードが露見して不正侵入されたり、アクセスした企業イントラネット内の機密情報を見られて情報漏えいに繋がったり、などの危険が考えられます。
このため、キャッシュクリーナー機能では、リモートアクセス端末で企業イントラネット内へアクセスした間の WEB ブラウザのキャッシュ、履歴等

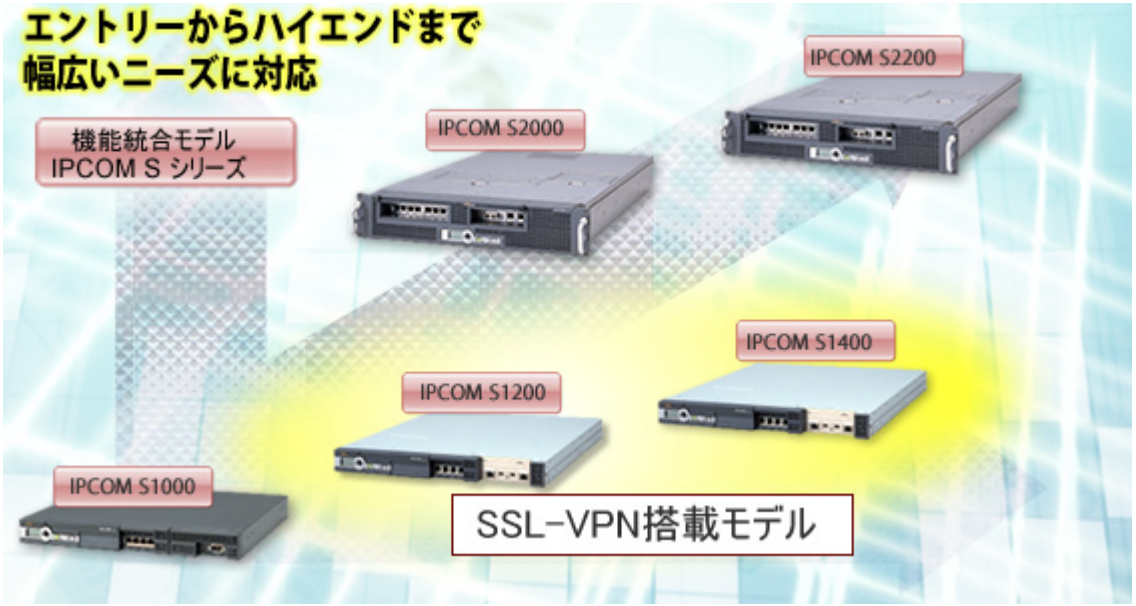
を強制削除し、リモートアクセス端末にアクセスの痕跡を残さないようにします。

SSL-VPN 装置では、その簡易性によるセキュリティリスクに対し、ユーザ認証やアクセス制御、エンドポイントセキュリティなど安全性を高めるための様々な機能を搭載しています。
SSL-VPN を利用する際には、まずリスクをしっかり認識した上で、上記で説明したセキュリティ機能から、企業のネットワークポリシーや、従業員の業務形態にあったものを選択して導入し、安全性を高めることが重要です。

富士通の SSL-VPN 装置のラインナップ

IPCOM S シリーズ 製品情報 http://primeserver.fujitsu.com/ipcom/

これまでご紹介してきた SSL-VPN は、IPCOM S1200 および 1400 に搭載されています。IPCOM S1200 および 1400 では、SSL-VPN 機能に加え、ルータやファイアーウォール、負荷分散など、企業イントラネットがインターネットに繋ぐ上で必要な機能を、1 台に集約して提供しています。



モデル	特長
IPCOM S1400 	ギガビット・イーサネット対応し、主に中小拠点規模システムに必要なネットワーク機能を一括搭載 ・拠点向け高性能モデル ・ 1U、GigabitEthernet ・ IPsec-VPN、SSL-VPN、SSL アクセラレーター ・ レイヤー 7 帯域制御、リンク負荷分散 ・ ホットスタンバイ
IPCOM S1200 	主に中小拠点規模システムに必要なネットワーク機能を一括搭載 ・拠点向けミッドレンジモデル ・ 1U、10/100MbpsEthernet ・ IPsec-VPN、SSL-VPN、SSL アクセラレーター ・ FNA ルーティング、レイヤー 7 帯域制御、リンク負荷分散 ・ ホットスタンバイ

これからも進化し続ける IPCOM S シリーズに御期待下さい。

ネットワークサーバ アイピーコム
IPCOM

SSL-VPN 入門

富士通株式会社

2005 年 10 月 初版
SFP-B0304-05-01