SWANStor®

スワンストアホワイトペーパー

2015年8月28日(最終改訂)

エリアビイジャパン株式会社

セキュリティの重要性

IT化の進展とともにビジネスリソースはコンピュータシステムとしてデジタル化され、ネットワークを介してさまざまな場所から、自由にアクセスできるようになって来ています。今や情報のネットワーク化がビジネス成功の鍵のひとつであると言っても過言ではありません。

しかし一方でこうしたビジネスリソースのセキュリティ管理が課題ともなってきています。ビジネスリソースへの不特定多数からのアクセスをいかに防御し、外部への意図しない漏洩を防ぐか。例え社内の人間であっても自由にアクセスさせたくないビジネスリソースをどのようにアクセス規制するか。あるいは、ビジネスリソースへの悪意を持った改竄もしくは破壊行為からいかに守るか。一方で、アクセスの許可されたユーザには許可されたリソースへ自由にアクセスできる環境も提供しなければなりません。さらに、セキュリティ管理に携わる管理者の負担を軽減し、管理コストを押さえることもまた重要となります。

ネットワークと VPN

ビジネスリソースに遠隔から安全にアクセスする手段としてVPN(VirtualPrivateNetwork)が挙げられます。VPNとはもともと、物理的に完全に閉じたネットワークであった「専用線網」を、その運用コスト低減のため、物理的には一般網を共用し、かつ専用線網として仮想的に分離したネットワークのことを指します。

VPNは大きく2種類に分けられます。ひとつは、固定の拠点間をセキュアに接続するネットワーク型のVPNです。2拠点を1対1に、暗号化されたIPトンネルで接続しただけのIPSec-VPNや、帯域保証まで行うIP-VPNなどが該当します。もうひとつは、任意の場所から固定の拠点へセキュアに接続するアクセス型VPNです。アクセス型VPNでは、ネットワーク型ほどの高パフォーマンスは要求されないものの、不特定対地からのアクセスから許可されたアクセスのみを受け付ける機能が重要な要件となります。

アクセス型VPNとネットワーク型VPNは技術的には相対するものではなく、IPSec技術を使ったアクセス型VPNの製品もあります。この場合、通常のケースでは、アクセスするPCには特別なソフトウエアをインストールする必要があります。

IPSecVPN の問題点

IPSec技術を使ったVPNは、社内のネットワークがVPNのトンネルを通じてアクセスしたPCにまで延長されたようなイメージになります。このためアクセスしたPCからは社内ネットワークの任意のリソースに事実上アクセスでき大変便利ではありますが、アクセスアカウントによって参照可能なビジネスリソースを限定させるような用途に向いているとは言えません。またPCの設定によっては、第3者がこのPCを中継して社内ネットワークにアクセスすることが可能になってしまいます。このためアクセスするPCの運用には十分な配慮が必要となります。

SSL-VPN とは

今日、ビジネスリソースの多くはWebベースのインタフェースで構築されています。スケジュール管理、顧客管理はともかく、メールの送受信、ドキュメントの検索と参照など、構築や管理の容易なWebベースのビジネスアプリケーションが主流となっています。こうしたWebベースのアプリケーションへのアクセスに主眼を置いて、しかも一般的なブラウザで、特別なソフトウエアのインストールなしに、かつ安全に外部からアクセスできるソリューション、これがSSL-VPNの基本的なアイデアです。

SSL-VPNではSSL-VPNサーバに相当する装置がちょうどプロキシのような働きをし、アクセスするPCのWebアクセス要求を中継します。アクセスするPCとSSL-VPNサーバとの間はSSL通信により暗号化されているので、他者がその中身をのぞき見ることはできません。またSSL-VPNサーバはユーザからのWebアクセス要求を受け付けるのに際して、アクセスアカウントとパスワードの組み合わせなどによるログイン認証を行い、許可されないアクセスを受け付けないようにしています。またSSL-VPNサーバは中継先のビジネスリソースをアクセスアカウントに応じて限定する機能も有し、ユーザ毎にアクセスできるリソースを絞り込むことができます。もちろんアクセスの基本はブラウザですので、第3者のアクセス要求が中継されてしまうという問題もありません。

SWANStor による SSL-VPN の実現

SWANStorはこのSSL-VPN製品のひとつですが、他のSSL-VPN製品にはない大きな特徴があります。ファイアウォールは外部からの任意のアクセスを遮断したまま、設定変更を施さずに、SSL-VPNを利用することが可能だということです。

SSL-VPNに限らず、他社VPN製品は単一のVPNサーバからなり、これをDMZもしくはファイアウォールの内側に置いて運用します。DMZに配置した場合にはVPNサーバが社内ネッ

トワークにアクセスできるように、またファイアウォールの内側に置いた場合には外部のアクセスユーザがVPNサーバにアクセスできるように、ファイアウォール上に1つないしは複数のポートをあけておく必要があります。この設定では、不特定他者のアクセスや不特定なリソースへのアクセスは許可しないようにするので、それがそのままセキュリティホールになると言うことはできませんが、大変に注意を要する事項であることに間違いはありません。またVPNサーバから社内ネットワークへのアクセスは全く排他する手段がないので、万が一、VPNサーバが乗っ取られるような事態が発生した場合の影響は大きく、VPNサーバの管理は十分な注意が必要となります。

SWANStorはサーバとゲートウエイに2分割された構成を有し、この2つで「SSL-VPNサーバ」と同等の機能を果たします。SWANStorサーバとSWANStorゲートウエイは暗号化されたセッションを張り、またSWANStorゲートウエイとアクセスPCの間はSSLセッションで暗号化されているので、第3者が通信内容を盗聴することはできません。さらに、SWANStorサーバとSWANStorゲートウエイのセッションはサーバからゲートウエイに向けて張られるため、ファイアウォールの内向きのポートは全て遮断したままでの運用が可能です。技術的には、ファイアウォールがありながらも、社内のPCが社外のWebサイトにHTTPSでアクセスできるのと等価となります。SWANStorサーバとSWANStorゲートウエイの間にプロキシサーバがあっても、運用上問題はありません。SWANStorサーバとゲートウエイの間の通信はSWANStor固有のプロトコルで情報の交換を行っているため、万が一SWANStorゲートウエイが乗っ取られても、そこからSWANStorサーバに直接アクセスできるわけではありません。

SWANStor の構成

SWANStorシステムを通じてビジネスリソースにアクセスするためには、アクセスユーザはまず適切なSWANStorゲートウエイのアドレスを知る必要があります。通常のWebブラウザでSWANStorゲートウエイにアクセスすると、最初にサーバ名、ログイン名およびパスワードの3種類の情報が問い合わされます。それらに適切な入力をすることでSWANStorシステムにアクセスすることが許可され、社内ビジネスリソースにアクセスすることが可能となります。アクセスユーザにはこのSWANStorゲートウエイが社内のビジネスリソースそのもののように見えますが、実体はSWANStorシステムの奥にオブラートされ、ファイアウォールなどで守られています。

1台のSWANStorゲートウエイには複数のSWANStorサーバを接続することが可能で、ユーザのアクセス要求はログイン時に入力されるSWANStorサーバ名を使って適当なサーバに振り分けられます。ユーザがSWANStorシステムにログインした後は、SWANStorサーバ名とランダムに割り振られるセッションIDでユーザのアクセスは管理されるので、間違って別

のサーバに転送され、誤ったビジネスリソースにアクセスされるという心配はありません。また、SWANStorサーバとSWANStorゲートウエイの間の通信は前述したとおり暗号化されているため、たとえこれらが離れた距離に設置されていたとしても、これを第三者に傍受される心配はありません。

SWANStor とアクセス制御

SWANStorには次のような3種類のアクセス制御機能があります。SWANStorではまず、正しいゲートウエイアドレス、SWANStorサーバ名、ログイン名、およびパスワードの4つの項目がそろわない限りビジネスリソースにアクセスすることができません。ログイン名とパスワードの認証については標準のパスワード認証方式のほか、LDAP、RADIUS、RSASecurID、WindowsNT(Windowsバージョンのみ)などの外部認証データベースや、鍵認証、ワンタイムパスワード等を利用することができ、より極め細やかなアカウント管理が可能となっています。

次に、それぞれのアクセスユーザをグループとして分類することができ、グループ毎にアクセス可能なビジネスリソースを定義することができます。例えば販社A用のカタログ情報のサイトと販社B用のカタグ情報サイトといったように、それぞれアクセスできる場所を分けることができます。更に許可されていないファイルへのアクセスをブロックするアクセスレベル制御の機能も有しており、こうしたリソースへの故意のアクセスができない仕組みも持ちます。例えば1つのWebサーバ上に販社A社用の情報と販社B社用の情報が共存しているようなケースでは、アクセスレベル制御機能は有効でしょう。

SWANStor とセキュリティ管理

上記のアクセス制御機能は全てSWANStorサーバ側で実現されます。設定はWebベースの制御コンソールであるサーバマネージャで行います。SWANStorサーバはもちろん、SWANStorシステムを使ってアクセスされるWebサーバ、認証サーバなど全てのビジネスリソースはファイアウォールの内側に配置することが可能で、SWANStorサーバとSWANStorゲートウエイのセッション以外の別のセッションを必要とはしません。

SWANStorゲートウエイはアクセスユーザのブラウザからはWebサーバのように見えますが、実際には要求を中継する機能しか有せず、SWANStorゲートウエイ上ではCGIも動作しません。万が一社内のWebサーバにトロイの木馬のようなプログラムが植え付けられたとしても、意図しない通信がSWANStor経由で外部に流れることもありません。これはSWANStor

システムが受動的にしか動作せず、必ずまずアクセスするの要求があって、その要求に対する応答をアクセスするに向けて返すことしかできないような設計になっているためです。つまり、外部からのアクセスについてはSWANStorサーバ上のアクセスログなどの監視にて行い、内部から外部への不審なアクセスについてはプロキシサーバやファイアウォールでフィルタするといったことが可能になります。

まとめ

総括すれば、SWANStorを使用したSSL-VPNにはセキュリティ管理上いくつかの利点があります。

一つ目は、外部からの直接アクセスは全てファイアウォールで遮断できるため、内部リソースへの不用意な進入についての管理の手間を軽減させることができます。二つ目は、内部から外部への不審なアクセスについても、その監視項目を絞り込むことが可能になります。プロキシやファイアウォールでのアクセス許可ポートの絞込みや、プロキシにアクセスパスワードを設定することで、そもそも不審な外向きの通信を遮断することが可能になります。三番目は、SWANStorゲートウエイのみを外部に出し、認証サーバを含めた全てのリソースをファイアウォールの内側に保護することで、不審者の攻撃に対する監視ポイントを1点に絞ることが可能となります。

もちろんSWANStorを導入したからといって、セキュリティが万全になるわけではありません。特にSWANStorゲートウエイの管理については十分な注意が必要です。しかし、監視ポイントの絞り込みによるセキュリティ管理負担の軽減をはかり、かつSSL-VPNの利便性を活用できる、SWANStorはそのようなリモートアクセスソリューションを提供します。