ネットビジネス プラットフォームを支えるセキュリティ技術
Security Technologies for Net Business Platform

琴屋　秀平 KOTOYA Shuhei
進藤　修一 SHINDO Shuichi
楯岡　正道 TATEOKA Masamichi

インターネットの普及により，ネットワークを利用した電子商取引（EC）は増加の一途をたどっている。インターネット上では電子化された企業情報や個人情報がやり取りされ，これらの情報は常に盗聴や改ざんの脅威にさらされている。また，サーバへのサービス妨害や不正アクセスによるデータの窃盗や破壊も増加している。

ネットビジネス プラットフォームでは，侵入検知／防止技術によってWebページの改ざんや不正侵入などを防止し，暗号化技術を用いたVPN（Virtual Private Network）技術によってネットワーク上での情報盗聴や改ざんなどを防止している。これらの技術の適用により，安全・確実なネットワークアクセスを提供している。

Electronic commerce using the Internet is rapidly evolving and becoming more widespread. With the exchange of electronically processed corporate and personal information on the Internet, such information is constantly exposed to the threat of unauthorized access or alteration. Moreover, the theft and destruction of data by illegal intrusion and service-disrupting attacks are also increasing.

On the Net Business Platform, illegal intrusion and alteration of Web pages are prevented by intrusion detection and prevention technology, while unauthorized access to or alteration of information on the network are prevented by virtual private network (VPN) technology using encryption. Safe and secure network access is ensured by the application of these technologies.

1 まえがき

今日，インターネットの普及・拡大によって，ネットワークを利用したECは実用段階を迎え，利用者も拡大の一途をたどっている。また，ECでは，重要な企業情報やクレジットカード番号，生年月日などの個人情報が電子化され，ネットワーク上で交換されている。

しかし，情報を公開するための技術を中心に発展してきたインターネットでは，情報を守るための十分なセキュリティが確保されていない部分がある。しかも，インターネット上では不正アクセスのためのツールがだれにでも簡単に入手できる。このため，悪意を持った第三者からの不正侵入，データの破壊，又は改ざんなどの被害も増加している。

これらの脅威は直接的にビジネスを阻害するだけでなく，より大きな被害をもたらす可能性がある。ネットビジネスを展開するうえで，これらの脅威への対応は必要不可欠である。

ネットビジネス プラットフォームでは，ネットワークセキュリティ技術を用いた製品を提供しており，これらの脅威に対抗することができる。ここでは，ネットワーク上に存在する脅威を分析し，それに対応するネットワークセキュリティ技術及び製品について述べる。

2 ネットワークセキュリティ

ネットワーク上に存在する脅威と，その対抗策としてのセキュリティ機能について述べる。

2.1 ネットワーク上の脅威

ネットワーク上の脅威は，次のように分類される。

⑴ サーバへのサービス妨害　短時間に大量の要求を送りつけ，サーバが提供している機能やサービスを利用できないようにすること。大量のメールを送りつける“ メール爆弾 ”や，コネクション確立要求パケットを短時間に大量に送りつける“ SYN flooding ”，エコー要求パケットを用いる“ Ping of Death ”などの攻撃がある。

⑵ サーバへの不正アクセス　ネットワークに接続された計算機に不正に侵入して，データを盗んだり，データを破壊すること。侵入者はユーザー名やパスワードを推察したり，セキュリティの弱い部分から不正に計算機にログインして，計算機資源を不正に使用する。

攻撃対象にならない場合でも，セキュリティが十分でないと，他の計算機を攻撃するときの踏台として利用されることもある。

⑶ ネットワーク上でのデータ盗聴／改ざん　ネットワーク上を流れるデータを盗み見たり，勝手に内容を変更すること。インターネットではネットワーク上を流れるパケットを簡単に採取できる。

従来，これらの攻撃を行うためには，ネットワークや計算機に対する高度な知識や経験を必要としていた。しかし，今日では，これらの攻撃を行うためのツールがインターネット上に公開されており，だれでも簡単に入手でき，攻撃を仕

掛けることができる。また，これらの攻撃は常にインターネットから行われるわけではなく，組織内部から行われることもあり，単にインターネットの入口にファイアウォールを設置しただけでは，防ぐことはできない（**図1**）。

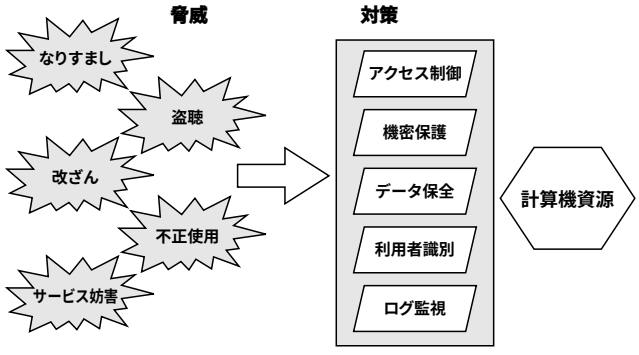

図1．ネットワーク上の脅威と対策　ネットワーク上には様々な脅威が存在し，対策が必要である。
Network security threats and countermeasures

2.2　脅威への対応策

これらの脅威に対するためには，次のようなセキュリティ機能が必要とされる。

⑴　アクセス管理　　計算機上に保持される各種の資源に対して，だれが何にアクセスしてよいか，どのような操作をしてよいかを管理する。許可されていない利用者に対しては情報へのアクセスを禁止し，いつ，だれがどの資源にアクセスしたかの記録を保持する。

⑵　機密保護　　ネットワーク上を流れるデータや計算機上のファイルに蓄えられたデータを暗号化することにより，権限のない利用者にはアクセスができないようにする。

⑶　データ保全　　不正侵入などによりデータが改ざんされたり，破壊された場合に速やかに復旧するために，必要なデータは定期的にバックアップを取り，保存しておく。

⑷　利用者識別　　現在，情報にアクセスしている利用者が，ほんとうに許可されている利用者なのか確認して承認する。

⑸　ログ監視　　サービスを提供する計算機がどのように利用されているか，定期的に記録を採取して確認することにより，攻撃をすばやく検知して対策をとる。

3　Webセキュリティ技術

ネットビジネスにおいては，Webサーバへのアクセスがベースとなっている。Webサーバへの攻撃は直接にビジネスが妨害されることになり，極めて影響が大きい。ネットビジネスの基本となるWebサーバへの攻撃を中心に，攻撃パターンとそれに対応する防御技術について述べる。

3.1　Webサーバへの攻撃

Webサーバへの主な攻撃としては，サービス妨害と不正アクセスがある。

サービス妨害の攻撃を受けると，提供している情報が利用できなくなったり，取引が停止してしまうなどの損害を受ける。また，不正アクセスの攻撃を受けた場合は，データの破壊など直接的な損害を被るだけでなく，サーバ上の個人情報の流出により，社会的信用の失墜や損害賠償訴訟を受けるなどの二次的な損害も被ることもある。

Webサーバへの侵入手段としては，辞書攻撃や管理者から直接聞き出すことによりユーザー名とパスワードを探し出し，特権を持つユーザーになりすまして侵入する方法がある。また，基本ソフトウェア（OS）やWebサーバ，及び会話的にサーバを利用する場合に使用されるCGI（Common Gateway Interface）プログラムに存在する，セキュリティが弱い部分（セキュリティホールと呼ばれる）を利用した攻撃がある。

3.2　Webサーバ防御方法

Webサーバをターゲットとした攻撃に対応するための方法を示す。

⑴　WebサーバやOSのセキュリティホールを閉じる
　一般に使用されるWebサーバソフトウェアやOSには特定バージョンごとにセキュリティホールの存在が知られている。セキュリティホールを閉じるための処置をとるか，もしくは対応したバージョンに入れ替える。

⑵　不必要なサービスを停止する　　OSで提供しているサービスやWebサーバに標準的に添付されているCGIプログラムにも，セキュリティホールが存在するものがある。不要なサービスは利用できないように停止，又は削除する。

⑶　ユーザーアカウント管理やパスワード管理を徹底する
　Webサーバへログインできるユーザーは，可能な限り制限する。パスワードについても容易に推測できるものは使用せず，定期的に更新するように管理する。特に，パスワード入力なしにログインできるユーザーアカウントやゲスト用のユーザーアカウントは削除する。

3.3　ネットビジネスでのWebセキュリティ技術

ネットビジネスでは，上で述べた方針に従ってサーバを運用し，ファイアウォールを組み合わせて防御するのが一般的である。しかし，ファイアウォールではWebサーバへの要求パケットは遮断できないので，正当な要求パケットを利用した攻撃を検知して防御することは困難である。

そこで，アクセス制御の一つの方法としてWebサーバへの攻撃を検知し，侵入を防止する機能を持った侵入検知シ

ステム(IDS：Intrusion Detection System)と呼ばれる技術がある。

IDSは攻撃パターンを記憶したデータベースを持ち，ネットワーク上を流れるパケットを常時監視している。送受信されるパケットが特定の攻撃パターンに合致した場合，該当のパケットを破棄して，指定された方法で異常を通知する。攻撃パターンは定期的に更新されており，新たに発見されるセキュリティホールに追従することができる。

IDSはネットワークに通常の計算機と並列に設置する傍受型と，ルータやブリッジのように直列に設置するフィルタ型がある。傍受型ではネットワーク上のパケットを監視するため，ネットワークトラヒックに与える影響がないという利点があるが，攻撃が複数のパケットの送受信ではなく，単一のパケットで行われた場合には防御できない欠点がある。一方，フィルタ型ではいったんパケットを受信して転送するため，性能に影響がでる場合もあるが，単一のパケットによる攻撃も防御できる利点がある(**図2**)。

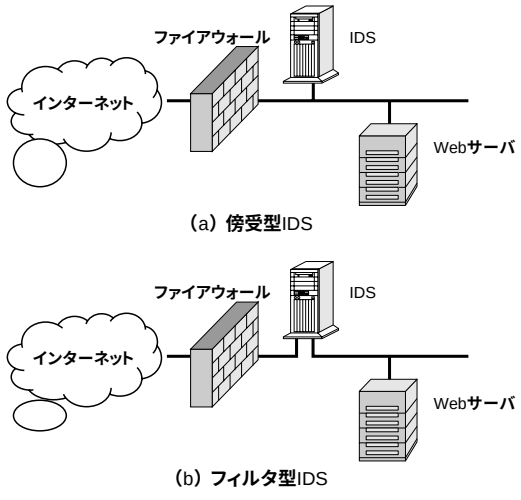

図2．IDSの種類　IDSには傍受型(a)とフィルタ型(b)がある。
Types of intrusion detection system (IDS)

ネットビジネス プラットフォームでは，より確実にWebサーバを制御できるフィルタ型IDS製品を提供している。

4 安全な通信路を確保するVPN技術

ネットビジネスでは，企業情報や個人情報など，今までは外部に現れることのなかった各種の機密情報が電子化され，インターネット上でやり取りされるようになる。これらの情報への盗聴や改ざん，なりすましなどを防ぐためにも，情報の機密性確保は重要である。

機密保護を実現する技術として，特定の計算機間で暗号化されたパケットを用いた通信を行い，安全な通信路を確保するVPN技術がある。

4.1 暗号化技術

インターネット上でやり取りされるIP(Internet Protocol)パケットのセキュリティを確保するための規格としてはIPsec(IP security)がある。IPsecはAH(Authentication Header)及びESP(Encapsulating Security Payload)から構成されている。AHは一方向関数を用いて，情報の保全性及び信憑(しんぴょう)性を確保し，情報の偽造や改ざんを防止する。ESPでは暗号化技術によって正当な受信者だけが情報を復号化でき，情報の機密性が確保される。

AHやESPを利用するためには，通信する当事者間で鍵(かぎ)情報を共有する必要がある。この鍵情報の交換について規定しているのがIKE(the Internet Key Exchange)である。IKEでは公開鍵暗号方式の一つであるDH(Diffie-Hellman)法を使用して，鍵情報を交換している。

4.2 ネットビジネスにおけるVPN技術

ネットビジネスプラットフォームでは，VPN技術を用いて機密保護を実現するゲートウェイ製品を提供している。

この製品は，インターネット上でIPsecとIKEをサポートした他のゲートウェイ製品との間で鍵情報を交換してVPNを構築する。暗号化方式としては，DES(Data Encryption Standard)及びTriple-DESをサポートしている。VPN技術によって，一般にセキュリティが弱いと言われるインターネット上で盗聴や改ざん，なりすましなどの心配のない安全な通信を実現できる。

5 あとがき

ネットビジネス プラットフォームでは，セキュリティ技術を応用した製品と，診断技術，構築技術，監視技術によるサービスを組み合わせることにより，インターネット上で安全なネットビジネスを容易に展開することができる。

琴屋　秀平　KOTOYA Shuhei
デジタルメディアネットワーク社 府中デジタルメディア工場 コンピュータソフトウェア部グループ長。ネットワークソフトウェアの開発に従事。情報処理学会，IEEE会員。
Fuchu Operations−Digital Media Equipment

進藤　修一　SHINDO Shuichi
デジタルメディアネットワーク社 府中デジタルメディア工場 コンピュータソフトウェア部主務。ネットワークソフトウェアの開発に従事。情報処理学会会員。
Fuchu Operations−Digital Media Equipment

楯岡　正道　TATEOKA Masamichi
デジタルメディアネットワーク社 コンピュータ&ネットワーク開発センター 開発第三部。セキュリティソフトウェアの開発に従事。情報処理学会会員。
Computer & Network Development Center