誌上展示会

第11回

# 不正侵入対策

## セキュリティー対策を見直し、企業の情報漏洩を防ぐ

text: 狐塚 淳

このコーナーは、注目の製品やサービスについて、それを支える技術や市場動向の解説（セミナー）と具体的なサービスを紹介（展示）する、バーチャル展示会。
今回のテーマは「不正侵入対策」。個人情報保護法施行後、特に注目を集めているテーマだ。ここでは、対処法のフレームと最近の動向について解説する。

### ウイルス対策の次は不正侵入への対応

ここ数年、セキュリティー対策の牽引役はアンチウイルスだった。相次ぐウイルス被害報道、続々と登場する新種ウイルス、被害者となる可能性ばかりでなく自分が加害者になってしまう恐怖。何より、コンピュータウイルスという直観的なネーミングが、感染を避けるアクションへとつながったのではないだろうか？　その結果、ウイルス対策のなされていないサーバーやパソコンはほとんどお目にかからなくなった。

一方でW32/Fanbatなど、セキュリティーホールを悪用するウイルスが話題になっていることもあり、ネット上の脅威はウイルス対策ソフトだけでは避けられないということもようやく周知となりつつある。

その中でも特に企業で対策を急がれているのが不正侵入である。2005年4月に施行された個人情報保護法が、そのトリガーとなった。ウイルスの代表的な被害が物理的なマシンの被害と二次感染であるのに対し、不正侵入の代表的な被害の1つとして挙げられるのは情報漏洩だ。もちろん、ウイルスの中にも、マイドキュメントの中身を添付で送付するようなものもあるが、それらはランダム性が高く、選別して情報を盗むケースはまれだ。自社内の情報を選択的に盗まれる恐怖は、個人情報の扱いについての教育が行われ、自覚しつつある企業の人々にとっては、大問題と捉えられる。実際、施行直前には、大規模な個人情報漏洩がいくつもニュースとなり、企業の担当者たちにとっては、対岸の火事ではないという気分が高まったのだろう。

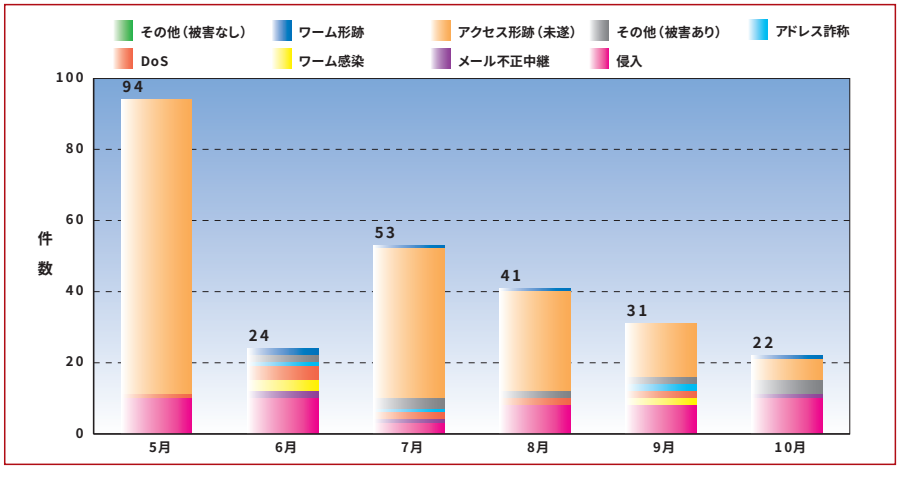


図1　不正アクセス届出状況推移　不正アクセスがなくなることはない
独立行政法人 情報処理推進機構セキュリティーセンター（IPA/ISEC）調べ

### 不正侵入の歴史はインターネットの歴史

不正侵入と一口にくくられるが、その手口は多様であり、さまざまな被害がもたらされる。ここにきて、確かに関心度は高くなっているが、不正侵入自体は昔から珍しいものではない。

日本では1999年には不正アクセス禁止法が成立しており、他人のユーザーIDやパスワードを使用して、利用する権限を持たないコンピュータを不正に使用する行為や、OSやアプリケーションに存在するセキュリティー上の弱点を攻撃し、コンピュータの不正利用や、データやプログラムの改竄、コンピュータを利用不能にする行為は禁じられている。

しかし、ホームページの改竄や、DoS攻撃によるサーバー停止、バックドアを利用しての権限奪取などの被害はなくなることはない（図1）。最近ではウェブアプリケーションからの不正侵入が急増している。

インターネットが実社会にかかわる比重が高くなるほど、そこに潜む悪意も膨張し、手口も巧妙かつ複雑になり、被害は増加し（図2）、多様化していく（図3）。

## OSのセキュリティーアップデートと脆弱性検査の必要性

不正侵入対策がウイルス対策と最も異なるのは、単独の対策だけでは効果が低いという点だろう。ポリシーを設定し、それに基づいて複数の対策を組み合わせ、継続的に対処していかなくては、有効な不正侵入対策とはなりえない。

まずは、多くの不正侵入が入り口として用いるOSやアプリケーションのセキュリティーホールをつぶしたり、バグフィックスパッチを当てるのが基本になるが、それ以前にきちんとアップデートが提供されるOSやサービスの選択が重要になる。サーバーの多くの割合を占めるのはUNIXだが、商用版のOSにはサポートが付随するため、ビジネス利用のサーバーの場合はこれを選択するのがいいだろう。脆弱性が発見された段階から間をおかずにセキュリティーホールをつぶしていくことで、多くの不正侵入を防ぐことができる。

こうした判断を的確に行うためには、OSメーカーのサイトを注意して見に行っているだけでは不十分だろう。サーバーの定期的な脆弱性診断が有効だが、きちんとした対応が伴わなければ意味はないので、次々に脆弱性が明らかになる状況では、管理者の負担増は避けられないだろう。

## 不正パケットに対応するファイアーウォールとIDS

次に、不正アクセス自体をサーバーに到達させないことが有効だ。この代表的なツールとして最もポピュラーなのが、ファイアーウォールだろう。しかし、ファイアーウォールによって完全なセキュリティーが達成されるわけではなく、次の段階としてIDS(Intrusion Detection System:不正侵入検知)の利用が考えられる。

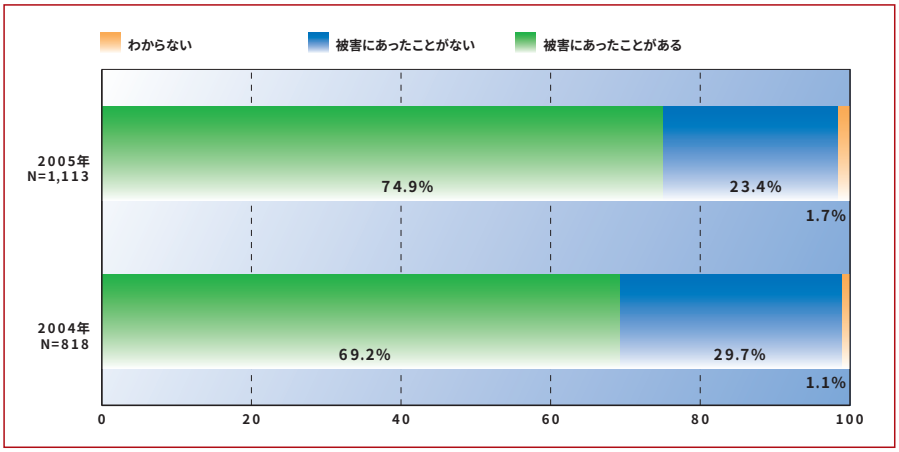


図2　セキュリティー被害の有無(2004年～2005年)
出典:『インターネット白書2005』資料3-5-1(©Access Media/impress, 2005)

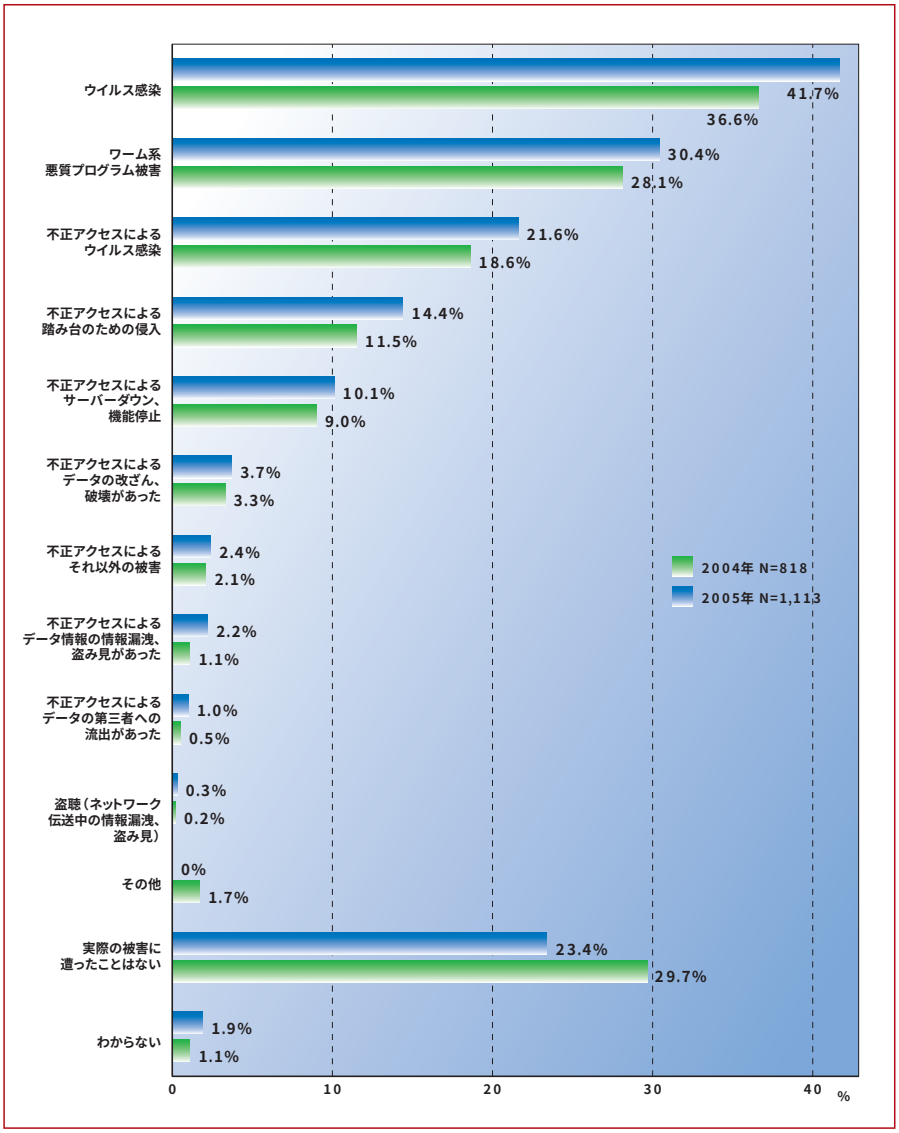


図3　セキュリティー被害の内容(2004年～2005年)(複数回答)
出典:『インターネット白書2005』資料3-5-3(©Access Media/impress, 2005)

ファイアーウォールがあれば不正侵入は防げるのではないかと思っている方もいるかもしれない。ファイアーウォールの基本的な働きは、送信先や送信元のIPアドレス、送信先のポートなど、パケットのヘッダー情報を見て、許可されているサーバーのサービスのみへのアクセスを許可する「パケットフィルタリング」だ。しかし、巧妙なクラッキングは当然IP詐称などを行ってくるので、ファイアーウォールは通行を許可してしまう可能性を消し去れない。

一方、IDSはパケットの中身を分析して、不正アクセスに特徴的なシグネチャー(コードのパターン)が含まれるかどうかをパターンマッチングによって判断(図4)し、アラートを発したり、ファイアーウォールとの連携でアクセスをブロックしたりする(図5)。なお、自身にブロックの機能まで持った装置をIDS/IPS(不正侵入検知/防御)と呼ぶ。また、異常検出といって、DoS攻撃などで膨大な量のリクエストの発生や、通常とは異なるアクセスに対してもIDSは検出が可能だ。IDSはネットワーク上で内部からのパケットも対象にできるので、企業内部などからの不正アクセスにも有効な対処となる。

## IDS導入運用にチューニングは不可欠

IDSはこのように不審なパケットを検知することで、不正なアクセスに対する有効な砦となり得るシステムだが、いったん導入すればそれでいいというシステムではない。不正侵入の疑いがあるパケットのすべてが不正侵入というわけではないため、アラートのうちあるパーセントはどうしても、不正侵入以外のアクセスに対してのものになってしまう。これを誤検知もしくは過剰検知と呼ぶ。厳しいポリシーを設定すると、アラートが異常に多い状態になってしまうが、ポリシーをゆるくすれば、実際の不正侵入を見逃すことにもなりかねない。

誤検知はチューニングによって減少させることが可能だ。チューニングとはログを分析し、そこから読み取れる不正アクセスの傾向に合わせたアラートポリシーを設定して適用することで、IDSの検知を必要十分な状態に近づける作業だ。不正アクセスのパターンや手口は一定ではなく変化するので、定期的にチューニングを行う必要がある。

社内のネットワーク管理者が一日中誤検知のアラートに悩まされていたのでは仕事にならないし、IDSを理想に近い状態にチューニングしておくためには、それなりの定期的な分析・設定は必要になるわけで、なかなか大変な作業である。

誤検知以外の問題として、IDS自体が非常に高パフォーマンスを要求されるシステムなので、高速なネットワーク環境では、キャプチャリングをミスするケースも生じうるだろうし、大量のアクセスがあればシグネチャーの分析が間に合わないというケースも起こりうる。また、暗号化された通信に対しては分析できないケースも発生しうる。

しかし、それらを考慮しても、IDSは不正侵入に対して効果を発揮するし、それに代わるものはない。

## ウェブアプリケーションファイアーウォール

ファイアーウォールやIDS以外にも、先ほど少し触れたウェブアプリケーション関連の不正侵入への対応も、最近は求められるようになっている。ウェブ運営サイドにとってはマーケティングやセールスの効果を高めるためにもはやなくてはならないウェブアプリケーションだが、そこでは個人情報など重要なデータがやりとりされて蓄積されるため、クラッカーにとって攻撃対象として魅力的である。ま

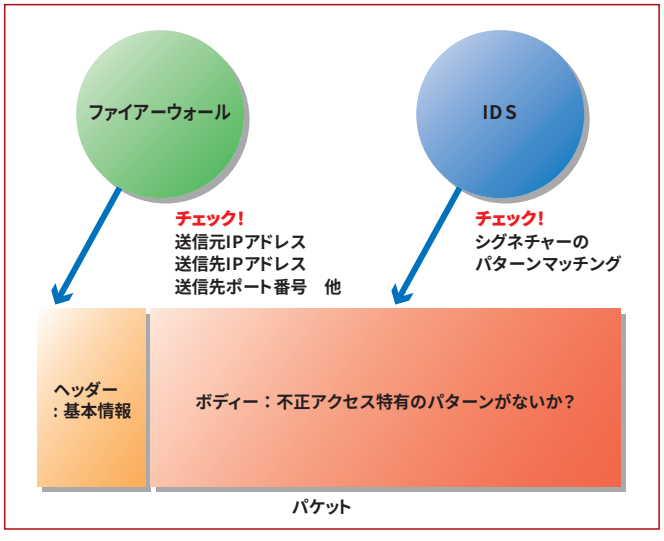


図4　ファイアーウォールとIDSの、パケットの見方の違い

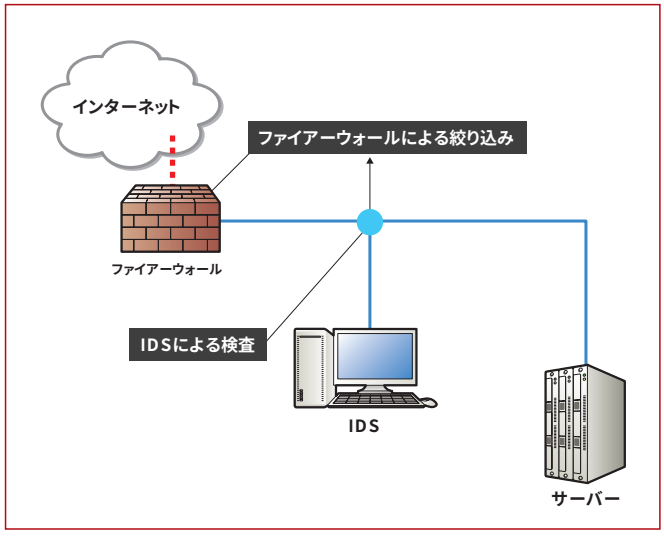


図5　ファイアーウォールとIDSの構成例

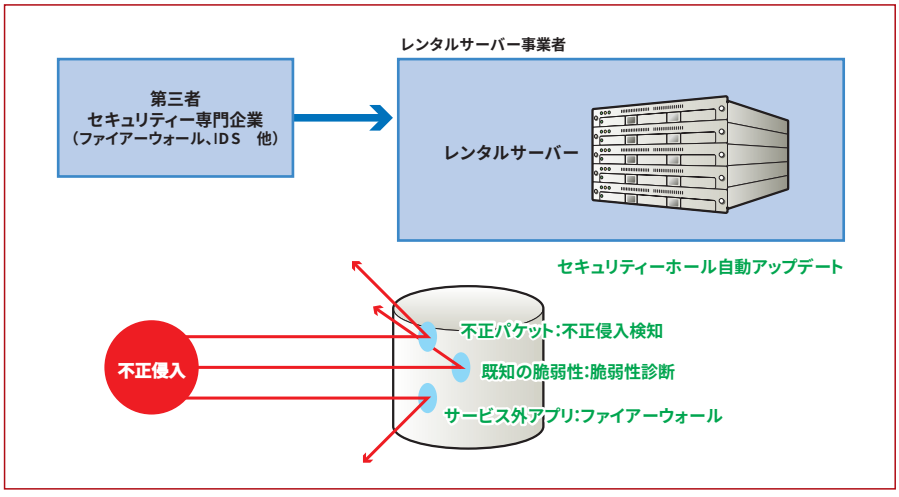


図6　レンタルサーバー事業者の不正侵入対策

**出展企業一覧**

**AT-LINK専用サーバ・サービス**
AT-LINK専用サーバ・サービス　→p.98

**@Next Style**
ワダックス　→p.100

**F-Secure Site Guardアプライアンス**
日本エフ・セキュア　→p.102

た、インタラクティビティー確保のために、穴もできやすい。この目的にはウェブアプリケーションファイアーウォール(WAF)が有効だ。

WAFはHTTP(S)を専門とするファイアーウォールで、通常のファイアーウォールがポートやURLでアクセス許可を判断するのと比べると、パターンファイルとのマッチングによって、ウェブのページ単位まで指定可能な細かい許可などの判断が可能である。

ウェブアプリケーションに関しては、IDSなどでも検知できない不正アクセスを検知して防御することが可能だ。

このように、不正侵入対策は、インターネットの技術進歩に合わせて発生してくる新しい脅威にも対応すべく、常に進歩・改良を求められる技術なのである。

## 統合の動きとレンタルサーバー

こうして見てくると、不正侵入対策と一言でいっても、そう簡単にできることではないということがおわかりだろう。

不正侵入対策を導入しようとしても、企業にとっては、特に、ネットワーク技術者(より専門的にはセキュリティー技術者)の人的負荷が問題になってくるに違いない。

その解決法の1つとして、最近では、ファイアーウォール機能とIDS/IPS機能やその他の機能を1台にまとめた、統合型のアプライアンスも出てきている。複数の機器の設定と整合をとるよりも、1台のアプライアンスにすべての機能を持たせることで手間を減らし、より確実な安全性を追求する試みとして評価できる。

もう1つの解決法は、いわゆるアウトソーシングである。

ウイルス検知の場合は、各ISPなどがサービスを提供しているASPモデルも、ルーターに到達する以前のデータをスキャンするというものだったので、アウトソーシングも簡単だったが、不正侵入対策の場合はそうはいかない。たとえばIDSの検知装置は、一般的にはファイアーウォールの内側、サーバー手前のネットワーク上にある必要がある。

そこで注目されるのが、最近利用者が急増しているレンタルサーバーだ。レンタルサーバーの事業者サイドではセキュリティーについてのさまざまなメニューを用意している。OSのセキュリティーホール通知や、自動アップデートのサービスをメニュー化している事業者も少なくない。また、ファイアーウォールの提供や脆弱性検査、不正侵入検知などのサービスを手がけるところも出てきている。レンタルサーバー事業者が、自社のIDCを対象に不正侵入対策を行い、その安全なサーバーを利用者にレンタルするというサービスだ。これを第三者の専門機関に委託する事業者も現れている(図6)。

今後、多くのインターネットユーザーにとって、不正侵入対策はますます重要になってくるだろうが、その負荷を企業内で背負い込むのはますます難しくなっていくに違いない。そのため、これらの統合された製品やレンタルサーバー事業者のサービスを賢く使いこなし、より安全にサーバーを運営していくことが必要となってくるだろう。

セキュリティーレベルが選択できる専用サーバーを提供

# AT-LINK専用サーバ・サービス

AT-LINK専用サーバ・サービス
[URL]http://www.at-link.ad.jp/


**レンタルサーバー業界ではセキュリティー競争が始まっている。しかし、セキュリティーとは、本来ユーザーが自分の管理するデータの重要度に応じて選択するものではないだろうか？ AT-LINK専用サーバ・サービス（以下at+link）は、そんなユーザー主導のセキュリティーを提案してくれる専用レンタルサーバーサービスだ。**

## 不正侵入対策はOS選びから始まる

不正侵入の大部分はセキュリティーホールがあるところに発生する。たとえば、OSにセキュリティーホールがなければ、不正侵入に遭う危険性は大幅に低くなる。at+linkが提供するセキュリティーの基本はここにある。

『普及価格版専用レンタルサーバーサービス』の先駆的存在であるat+link。今年の大きいトピックスは、従来年間10万円程度のライセンス費用が必要だったRed Hat Enterprise Linux ES（RHEL-ES）を世界で初めて無償で提供したことにある。商用OSと無償OSの最大の相違点はサポートの有無、つまりセキュリティーホールに対していかに迅速な対応がとれるかどうかということであり、ビジネスで利用することの多い専用ホスティングにおいて、これは非常に重要なポイントだ。

その点、このRHEL-ESではRed Hat Networkによる自動セキュリティーアップデートが標準で利用できるため、堅牢なサーバーを構築するのにふさわしいものといえるだろう。

## Linuxのセキュリティーをまず最初に考える

そして、2005年9月からは、それまでのRHEL-ES v.3に加えてv.4の無償提供が開始された。RHEL-ES v.4はLinuxの2.6系カーネルを基に開発された、セキュリティー面で評価の高いOSだ。SE Linux（Security Enhanced Linux）では標準の任意アクセス機能を補完するMandatory Access Control（強制アクセス制御）機能を提供することで不正アプリケーションによるシステムのセキュリティー侵害を防ぐことができる。さらに、バッファフロー攻撃への対処として効果的なメモリー管理の強化や、コンパイルとランタイムの整合性チェック機能が搭載されている。

これに、TCP-Wrapperによるアクセス制御を施したうえで、ユーザーに提供される。まずはOSレベルでの高いセキュリティーを基本とし、そこに豊富なセキュリティーオプションをユーザーが選択することで防御を強化していくスタイルをとっている。

## ユーザーが選択できるセキュリティーオプション

at+linkで、ユーザーが選択できるセキュリティー関連オプションは非常に豊富だ。たとえば、リモートからの安全な管理を可能にする「SSL-VPNサービス」はレンタルサーバーを安全に運用するためには必須の機能だ。at+linkのSSL-

キャンペーンマシン

| | CPU | メモリ | HDD | 初期費用 | 月間利用料 |
|---|---|---|---|---|---|
| リフレッシュ! | Celeron1.1GHz | 512MB | 120GB | 36,750円 | ●東京NOC利用の場合<br>30,450円(23,100円)<br>●富山NOC利用の場合<br>19,950円(14,700円)<br>●帯域保証回線サービス<br>23,100円(17,850円) |
| Celeron Mパッケージ | Celeron M 360(1.4GHz：L2 1MB) | 512MB | SATA80GB | 68,250円 | |
| Pentium Mパッケージ | Pentium M 735(1.7GHz：L2 2MB) | 512MB | SATA80GB | 84,000円 | |
| ターボパッケージ512モデル | Celeron-D 336(2.8GHz：L2 256KB) | 512MB | SATA160GB | 84,000円 | |
| ターボパッケージ1GBモデル | Celeron-D 336(2.8GHz：L2 256KB) | 1GB | SATA160GB | 94,500円 | |
| ターボパッケージ2GBモデル | Celeron-D 336(2.8GHz：L2 256KB) | 2GB | SATA160GB | 126,000円 | |

SATAトリプルディスクパッケージ（RAID1+バックアップディスク）

| | | | | | |
|---|---|---|---|---|---|
| モンスター630パッケージ1GBモデル | Pentium 4　630(3GHz：L2 2MB)<br>Hyper-ThreadingXD bit機能対応 | 1GB | SATA160GB | 126,000円 | ●東京NOC利用の場合<br>35,700円(28,350円)<br>●富山NOC利用の場合<br>25,200円(19,950円)<br>●帯域保証回線サービス<br>28,350円(23,100円) |
| モンスター630パッケージ2GBモデル | Pentium 4　630(3GHz：L2 2MB)<br>Hyper-ThreadingXD bit機能対応 | 2GB | SATA160GB | 147,000円 | |

注：月間利用料金（）は、代理店または2台目以降の料金

VPNは、クライアントがActiveXコントロールとして実装されているため、ユーザーはブラウザーからの利用が可能だ。

また、標準でHTTPポートとSSH/Telnetポートに対する24時間・365日体制の死活監視を利用できるほか、オプションでサービス(アプリケーション)やプロセスの稼動まで監視できる「サーバウォッチ」も選択できる。これは監視エージェントによる動作監視を行い、障害発生時には、ユーザーとat+linkに対して通知が行われるというもの(手順書に基づく一次対応の有無も選択できる)。これ自体をセキュリティーというべきかどうかは難しいところだが、ユーザーがセキュリティーを求める大きな要因として、ビジネス利用のサーバーのダウンタイムを減らしたいということがあるので、早期に障害を知るサービスは有用だといえるだろう。また、キャンペーンマシンには、迅速な復旧を実現する「オートリブーター」が標準装備されており、再起動実施時の通知メールがオプションで選択できる。

さらにファイアーウォールやウイルスチェッカーも共用、専用の両方で用意されているほか、ファイアーウォールやIDS(侵入検知システム)/ADS(自動防衛システム)、VPN、ロードバランシング、ウイルスプロテクションの機能を一台で実現可能な統合セキュリティーアプライアンス「VSR」シリーズを利用することにより、運用責任者の負担を大幅に減らすことができるだろう。

そのほか、改竄通知ソフトのTripWireを使用した「ファイル改竄通知」サービスもある。

重要なのは、これらのサービスを、ユーザーが、自由に選択して利用できる点だ。セキュリティー対策はすべてをやればいいというものではなく、データの重要度にあわせて、必要な対策をとることが重要である。そのための選択肢が十分に用意されているのがat+linkといえるだろう。

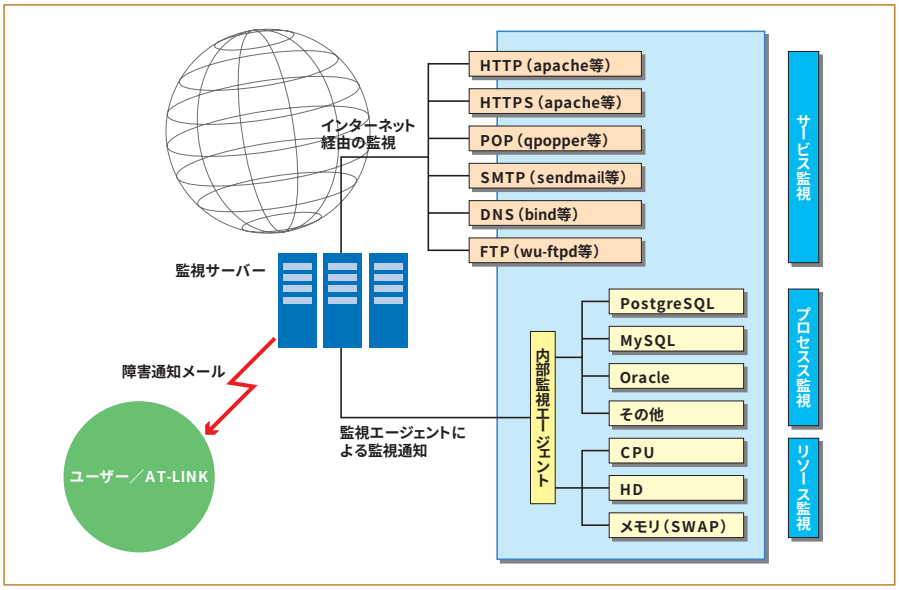

図1 サーバーウォッチ概念図

## 用途や目的に応じて選択できるサーバーマシン

at+linkはセキュリティー面だけでなく、サーバーマシンの構成についても自由度は高い。豊富なラインナップからマシンを選び、さらにハードディスクやメモリーを組み合わせることにより、用途や目的にあわせたマシンが構築できる。また、Linuxだけでなく Windows Server や Apple Xserve も選択することができる(ただし、Windows Server の利用には一定の条件があるほか、一部のオプションはLinux以外のOSから利用できないものもあるため、その点はチェックが必要だ)。

気になる利用料金も、キャンペーンマシンで月額19,950円から(2台目以降14,700円)と、安価に押さえられている。

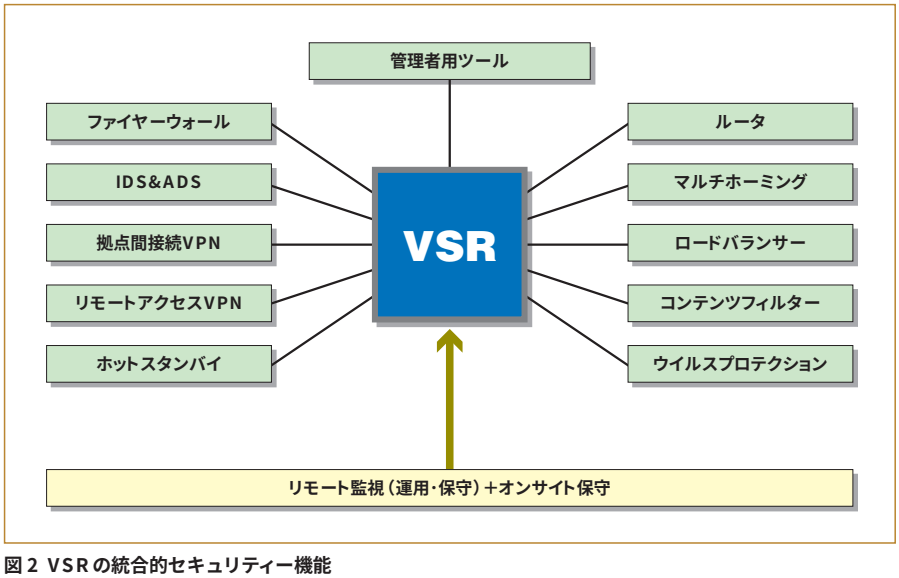

図2 VSRの統合的セキュリティー機能

問い合わせ先
AT-LINK専用サーバ・サービス
03-5785-0555
pr-info@at-link.ad.jp

一段上のセキュリティー環境を提供する共有型レンタルサーバー

# @Next Style

ワダックス

[URL] http://www.wadax.ne.jp/


**ウイルス対策だけでは十分なセキュリティーとはいえない。高まる不正侵入検知のニーズに、ワダックスがセコムとの提携で打ち出した共有レンタルサーバーサービス「@Next Style」は、標準で不正侵入検知と脆弱性診断を導入し、さらにはセコムトラストネットのSSL証明書付のサービスも選択できる、高度なセキュリティー機能を提供している。**

## 不正侵入検知への高まるニーズに対応

個人情報保護法の施行などにより、セキュリティーへの関心が高まっている。また、不正侵入による被害も多数報道されているため、ウイルス対策の次は不正侵入対策を、と考える企業は少なくないが、不正侵入検知を自前で行おうとすると、ウイルス対策とは比較にならない高額な費用がかかってしまう。

ワダックスが2005年11月に提供を開始した、共用レンタルサーバーサービスの新ブランド「@Next Style」は、低料金の共有レンタルサーバーサービスながら、セコムの不正侵入検知を導入し、なおかつ2カ月に1度の脆弱性診断までセットになっているため、事前に不正侵入の原因となる脆弱性までチェックできるというたいへんセキュリティー効果の高いサービスだ。

加えて、これまでレンタルサーバー業者が、自己判断で行っていたセキュリティー基準を、同分野で実績のあるセコムの評価を導入したという点で、客観的にも高度な信頼性の持てるサービスである。

## セキュリティーと容量で選べる2つのパック、6つのサービス

「@Next Style」には2つのパック、6つのサービスが用意されている。月額料金1,995円からの「@Next Style スタンダード・セキュリティ・パック」と、セコムトラストネット社の実在性認証付きSSL証明書「セコムパスポート for Web」が付属する「@Next Style プロフェッショナル・セキュリティ・パック」の2種が、それぞれディスク容量でブロンズ（420MB）・シルバー（640MB）・ゴールド（1.06GB）の3つのサービスに分かれている。

すべてのサービスに、セコム不正侵入検知サービスと2カ月に一度のセコムトラストネットの脆弱性診断が導入されているため、高度なセキュリティーが実現されている。また、毎月メールマガジンも発行され、不正侵入検知やセキュリティー状況、ウイルス検知数、スパム検知のトレンドなどがレポートされる。「@Next Style」は、そのほかにウイルスチェックやスパムフィルターはもちろんPOP over SSL／SMTP over SSLなども標準で利用が可能など、とにかくセキュリティー面での充実が目立つ。

なお、従来のワダックスの共有レンタル

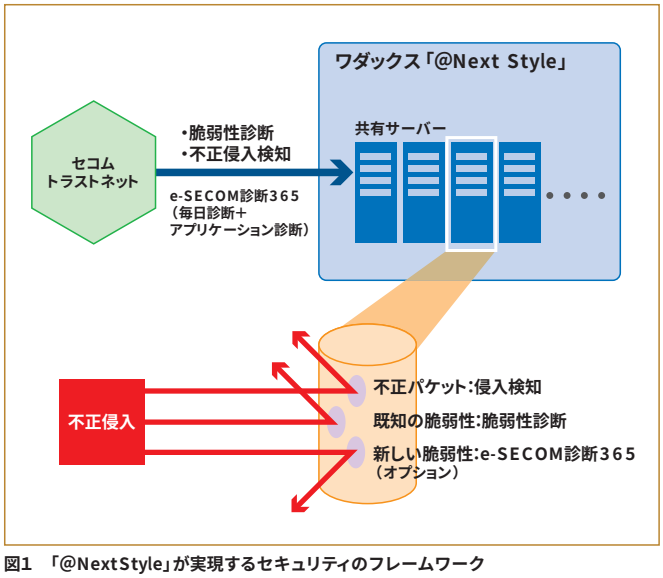


図1 「@NextStyle」が実現するセキュリティのフレームワーク

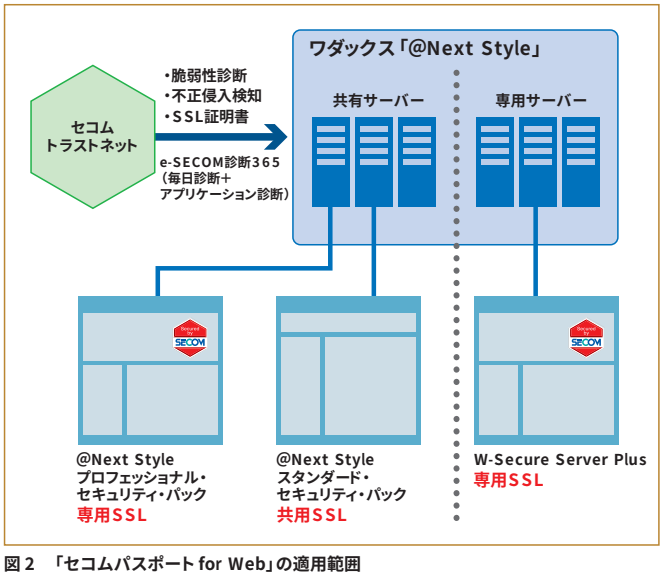


図2 「セコムパスポート for Web」の適用範囲

サーバーサービスのブロンズ・シルバー・ゴールドサービスは「@Next Style」に統合されていく。それ以外のプラチナ・ダイヤモンド・エグゼクティブのサービスは新規申込みを停止しながらも、新サービスと同等の基準で運用されていく。

## 「セコムパスポート」付の「プロフェッショナル・パック」

両パックの最大の差異は、「スタンダード・パック」で提供されるのが共用SSLであるのに対し、「プロフェッショナル・パック」では専用SSLである「セコムパスポートfor Web」が提供される点だ。

SSL証明書は、サーバー運営者にとっては馴染み深いものではあっても、そのサイトを利用する一般の人にはなかなかわかりづらい。鍵のアイコンがページに現れれば、安全な通信ができるらしいことは知っていても、そのSSL証明書を確認したときに、それが信頼のおける発行者によるものなのかどうかの判断はつきにくい。しかし、そこにリアルでのセキュリティーや警備に実績のあるセコムの名称があれば、一般の人にとっても、その信頼性は格段に理解しやすくなる。

たとえばレンタルサーバーを利用してオンラインショップを開設する場合、共用SSLを使用すれば、クレジットカード情報なども安全に送受信が可能だが、ショップ利用者からは、その安全性は、ブラウザー右下の鍵アイコンでしか計れない。一方、専用SSLの「セコムパスポートfor Web」の場合、6角形のセコムWebステッカーをショップホームページに貼れるため、そのサイトがセコムによって守られていることがわかり、信頼性がぐっと増す。

しかも、通常、専用SSLの申し込みには面倒な書類記入などが必要になるが、「プロフェッショナル・パック」なら、「セコムパスポートfor Web」が標準提供されるため、一括申し込みが可能だ。

また、「プロフェッショナル・パック」はオプションで「e-SECOM診断365」の利用も可能だ。こちらはセコムトラストネットにより365日毎日セキュリティー診断が行われるサービスで、世界標準のクレジットカード業界向け情報セキュリティー基準である「PCI」に適合しているとともに、SANSやFBIが警告するトップ20の脆弱性についての診断も含まれている。より機密性、重要性の高いデータが含まれるサーバーに選択したいサービスだ。

## セキュリティー以外も多機能なサービス

「@Next Style」は、セキュリティー以外の機能も非常に充実している。

CGIやPHPへの対応はもちろん、データベースではMySQL、PostgreSQLに対応しているため、機能豊富なウェブの構築が可能となっている。

また、もうひとつの特徴として、新たに@Next Style Blogを標準提供している。話題のブログを簡単に、独自ドメインで利用できるサービスだ。コントロールパネルから簡単にインストールでき、ビジネスやホビーのブログに利用できる数十種の豊富なテンプレートから選択するだけで好みのブログを構築できるサービスだ。

なお、@Next Style「リリース記念キャンペーン」として、2006年1月末までに申し込むと、6サービスとも初期費用が無料となっている。

## 専用サーバーのセキュリティーには「W-Secure Server Plus」

ワダックスのセコムのセキュリティーを使用したセキュアなサービスは、専用レンタルサーバーで、2005年4月より先行して提供されている「W-Secure Server Plus」がある。

「W-Secure Server Plus」は「セコムパスポートfor Web」「セコム不正侵入検知サービス」と「定期的な脆弱性診断」という充実したセキュリティー機能を、商用Linux上で利用できる。アラート発生時のユーザーへの24時間緊急連絡や、年6回のサーバー脆弱性診断後のセキュリティー対策や、OSのセキュリティーアップデートなどを、ワダックスサイドで対策代行を行うメニューも用意されている。また、6月からはユーザーサイドで専用サーバーを自由に設定・操作可能な「W-Secure Server Plus Self」も提供されている。こちらは、セキュリティー機能としては「W-Secure Server Plus」と同等だが、コストは低く、サーバーにより自由度を求める、ある程度の技術力を持ったユーザー向けの選択肢だ。

**サービス料金表**

| パック | サービス | 初期費用 | 月額換算料金 | 容量 |
|---|---|---|---|---|
| @Next Style スタンダード・セキュリティ・パック | ブロンズ | 3,000円 | 1,995円〜 | 420MB |
| | シルバー | 3,000円 | 2,834円〜 | 640MB |
| | ゴールド | 3,000円 | 3,834円〜 | 1.06GB |
| @Next Style プロフェッショナル・セキュリティ・パック | ブロンズ | 12,600円 | 6,388円〜 | 420MB |
| | シルバー | 12,600円 | 7,263円〜 | 640MB |
| | ゴールド | 12,600円 | 8,138円〜 | 1.06GB |

※「リリース記念キャンペーン」として1年契約の場合、2パック6サービスとも初期費用が無料（2006年1月末まで）

**プロフェッショナル・パック　オプション**

| | | |
|---|---|---|
| e-SECOM診断365 | 設定費用 | 31,500円 |
| | 初期料金 | 105,000円 |
| | 年間料金 | 504,000円 |

※「リリース記念キャンペーン」として設定費用が無料（2006年1月末まで）

問い合わせ先
株式会社ワダックス
http://www.wadax.ne.jp/
0120-963-388

不正アクセスとウイルスから同時に守る、統合Webサイト防御アプライアンス

# F-Secure Site Guard アプライアンス

日本エフ・セキュア株式会社

[URL] http://www.f-secure.co.jp/


**Webアプリケーションの普及に伴って、これまでのFirewallやIDS、IPSでは守りきれない高度な攻撃が増えてきた。日本エフ・セキュアのF-Secure Site Guardアプライアンスは、こうした攻撃を退けるとともに、Webサーバーへのウイルス侵入・拡散を防止する機能を併せ持った統合型のWebサイト防御ソリューションだ**

## Webアプリケーションの普及で問われる既存のセキュリティー

企業サイトやECサイトなど、Webアプリケーションを使用するサイトは非常に増加した。ネットビジネスを展開するうえで、Webアプリケーションは必須の存在になってきたといってもいいだろう。

しかし、Webアプリケーションによってユーザーとのコミュニケーションが深まれば、サイトに蓄積される情報も多量かつ重要になってくる。それを狙った高度で多彩な攻撃が見られるようになってきた。

SQLインジェクションやクロスサイトスクリプティング、クッキー情報の盗難、フォースブラウズなど、最近話題に上るネット脅威は、従来型のセキュリティーによる対処では、その全てをカバーすることは難しく、また個別対応で人的リソースを消費してしまうなどの問題も持っている。

日本エフ・セキュアの「F-Secure Site Guardアプライアンス」は、こうした攻撃からWebサイトを守るとともに、ウイルス検査機能も併せ持った、統合的なセキュリティーアプライアンスだ。

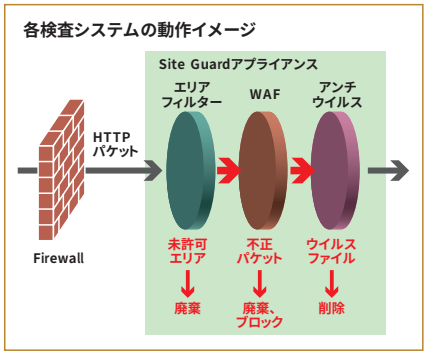


図1　Site Guardアプライアンスシステム稼動イメージ

## Site Guardアプライアンスの多彩な特長

「F-Secure Site Guard アプライアンス」の最大の特徴は、Webアプリケーション Firewall機能（以下、WAF）とアンチウイルス機能を併せ持つ点だろう。設定の難易度が高いと言われるWAF機能だが、株式会社ラックの定義ファイルを用いる事で容易に設定・導入を行う事ができるようになっており、アラートとログの機能も充実している。

また、アンチウイルス機能はLibra、Orion、AVPの3つのエンジンを使用しており120Mbpsの高速スキャンが可能と、統合的にWebサーバーの脅威を取り除くことが可能だ。

WAFによる防御方法は攻撃の種類によって異なるが、たとえばWebの改ざんにはCookie情報を暗号化し、hidden、selectなどの固定パラメーターを記憶しての検知・防御が可能であるし、SQLインジェクションなどに関しては、シグネチャーベースでの検知・防御が可能だ。また、フォースブラウズにはセッション管理でエントリーページ以外への直接アクセスを禁止するのが有効だ。

「F-Secure Site Guard アプライアンス」は日本語GUIの設定・管理画面を持ち、整理された項目への設定だけで、WAFの高度な利用が可能であるため、導入が容易な点も管理者にはありがたい。導入構成の自由度も高く、インライン透過型、Proxy型、負荷分散装置と連携可能なL4型も選択可能だ。インライン透過型、Proxy型で冗長機能を使用できる。

また、脅威の低減にはエリアフィルター機能も有効だ。たとえば日本と米国のみのHTTPアクセスを許可するなどして、踏み台サーバー越しの、Webアプリケーションへの攻撃機会を最小にとどめられる。

WAF、アンチウイルス、エリアフィルターとも定義ファイルを自動更新可能なため、常に最新情報を基にした効率的なWebサーバーのセキュリティー対策が可能である。

価格は1ユニット248万円（サポート込、税抜き）で、次年度以降のサポートライセンスは年間49万6千円となっている。


図2　直観的な設定が可能な日本語GUIによる管理画面

問い合わせ先

日本エフ・セキュア株式会社

045-440-6610

Japan@F-Secure.com

# ［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp