CISO STRATEGY

企業のリスクをマネージする戦略考

この10年間、基幹ネットワークのネットワークセキュリティー管理の考え方は、ファイアーウォールのような組織の内と外の境界で防護する境界防衛が中心だった。この機構は多くの組織に導入されてその効果を発揮しているが、近年の状況の変化に追随できなくなってきており、本来の機能を果たせなくなってきている――。

第七回 境界防衛の限界

text : 山口英 奈良先端科学技術大学院大学情報科学研究科教授

インターネットは、90年代初頭に商用化されたことにより急速に規模を拡大した。それまでは大学や一部研究機関、政府組織などの特定の組織だけが接続されていたが、商用化により料金さえ支払えれば誰もがインターネットに接続できるようになったことで、当時でもセキュリティー管理をどのように行うかが大きな関心事であった。

セキュリティー管理の重要性は認識されていたが、具体的にどのようにするかは90年代初頭には手探りの状態にあった。しかし、システムへの攻撃リスクが顕在化した商用化直後から1つの考え方が急速に広まった。それは組織内ネットワークとインターネットとの接続点にファイアーウォール（fire wall、以下FW）と呼ばれる特別な仕掛けを設置する考え方であった。このFWは防火壁という名前のとおり、外部で交換される種々の悪意ある通信を遮断し、組織として受け入れることを許した通信のみを通過させるものである。さらに、FWを設置したことによって不必要な通信サービスはFWを通過できなくなるが、電子メールやWWWといった必要なサービスはFWに併設したアプリケーションゲートウェイによって中継する。この外部と内部を中継するアプリケーションゲートウェイを設置するための、FWによって管理されたネットワークセグメントをDMZ（非武装地帯：De-Militarized Zone）と呼ぶ。

このような外部と内部の境界に特別な機構を用意し、内部のネットワークとシステムを守るという境界防衛（border protection）の考え方は、90年代前半に確立したものである。現在では、FW設置はインターネットに接続するときに必要不可欠なものだと捉えられている。

しかし、FWが使われ出したときに活発に議論されていたことで、最近では忘れてしまっていることがある。それは、FWはあくまでも暫定的な解決方法だと、当時のセキュリティー専門家達が考えていたことだ。

FWは経済的な解決方法

セキュリティー対策を考える場合、ネットワークに接続されているすべてのシステムに対して十分なセキュリティー対策を講じることが必要である。しかし、個々のシステムに対してセキュリティー対策を十分に講じるには多大な手間がかかる。各システムはハードウェア、OS、アプリケーション、使用形態、システムに対する業務の依存度、さらには、その業務の重要度などが千差万別である。このため、各システムに適合したセキュリティー対策を施すには、システムごとのカスタマイズが発生してしまい、多大な手間となる。この手間を何とか小さくしたいが、セキュリティー対策を十分にできないだろうかと考えたのだ。

そこで、2つの大きな前提を置くことで、この手間を省こうと考えた。1つは、トラブルは内部ネットワークに接続されたシステムからは引き起こされないという前提である。簡単に言えば内部犯行は発生しないと考えようということだ。もう1つが、内部で使われるシステムの大多数がクライアントとして利用され、極めて少数のシステムが外部に対してサービスを提供するサーバーとして使われるという前提である。

実はこの2つの前提からFWを作り出すことが可能となったのだ。トラブルは常に外部からやってくると仮定するから

こそ、境界防衛で十分であることが暗黙の了解となった。さらに内部のシステムの大部分がクライアントとしての機能しか果たさないという前提から、FWではフィルタリングやNATを使って外部から流入する通信を遮断しても大きな影響を与えることはないという考えに至った。外部のシステムにサービスを提供するサーバーがあったとしても、DMZに設置すればサービスをFWの管理下で提供できる。

この2つの前提があったからこそ、FWの設置によって各システムに施すべきセキュリティー対策を減らすことができ、また、セキュリティー対策そのものもFWに関連したシステムに集中的に行うことで、全体のセキュリティーレベルの引き上げにつなげられた。別の言い方をすれば、FWによってセキュリティー管理に対する投資を一点に集中させられたと言ってもいいだろう。その意味でFWは経済的に効果の高い解決方法であった。

戦略1 とりあえず、FWは投資効果の高いセキュリティー対策と言える。使わない手はない。

FWを乗り越えるトラブル

さて、FWを成立させている2つの前提が崩れてしまったらどうなるだろうか。FWの考え方が生み出されてから10年が経過した現在、まさにFWの2つの前提が崩れ始めている。

1つ目の、内部ネットワークに接続されたシステムから引き起こされるトラブルはないという前提は、ネットワーク伝搬型のウイルスによって簡単に崩されてしまっている。今やウイルスは電子メールやWWWアクセス、さらには、直接ネットワーク越しにシステムに対して頻繁に入ってくる。特に電子メールやWWWアクセスによってシステムに入り込んでしまうケースは後を絶たない。このような状況では、いくらFWがあったとしても内部のシステムがウイルスに感染する状況が発生してしまい、場合によっては内部で大流行するようなこともしばしば見られる。

2つ目の、内部のシステムの大半はクライアントとして使われるという前提は、近年のP2P型サービスの普及に伴って崩されている。特にここ1、2年で大流行すると言われているIP電話（VoIP）サービスでは、サービスを利用するシステムは、発呼時にはクライアントになるが、着呼時にはサーバーとしての振る舞いをする。つまり、内部ネットワークに接続されたシステムにおいても、外部から直接通信を受けなければならないものが登場してしまう。この場合には、NATは論外であるが、単純なパケットフィルタリングFWにおいても、そのルール記述は大変難しいものとなる。

このようなことから、先に述べた前提に基づいたFWは、最近ではますます機能せず、逆にユーザーの使い勝手を邪魔するものとなりはじめている。

戦略2 ウイルス/ワーム対策にはFWは無力だと認識すべし。また、P2P型サービスを使いたい場合にも、FWは機能の再定義が必要。

ブロードバンド化に頭を悩ます

さらにFWの存在意義に追い討ちをかけているのが、近年のブロードバンド化である。これまでの組織内ネットワーク環境といえば、イーサネット技術を基盤として、GbE（ギガビットイーサ）を使ってバックボーンを構成し、100Base-Tによって端末を収容するのが一般的であった。しかし、最近では10Gbpsイーサネットを使ってバックボーンを構成し、1000Base-Tによる端末収容も始まっている。この場合、外部との接続もブロードバンド化によって数百Mbpsの接続から、最近では10Gbps回線による接続も始まっている。このような外部接続回線にFWを接続した場合、10Gbpsの帯域性能を持ったFWを作ろうとすると大変高価なものになってしまう。実は、1Gbpsの帯域性能を持ったFWも現時点でもかなり高価なものである。

結局のところブロードバンド化した回線に対してFWの性能向上が十分に行われていない。このため、どれだけ対外接続回線をアップグレードしても、FWの性能が向上しない限り、対外接続回線を十二分に使い切ることはほとんどできないことが起きてしまう。

ファイアーウォールの問題点とは

ここまで述べてきたように、10年前に概念が設計されたFWは、少しほころびが見えてきている。少なくともネットワーク伝搬型ウイルスについては、FWはまったく防御効果がない。また、多くのアプリケーションの基本的な考え方になるであろうP2P型サービスは、現在のFWとは相性が大変に悪い。これらのことから10年前に考え出されたFWを中心とした境界防衛の考え方は、そろそろ改訂が必要になりつつあるのだ。

現時点でのFWの問題点は、①FWで防げないセキュリティー上のトラブルからシステムをどのように防護するのか、さらに②FWの性能をどのように上げるか、そして③P2P型サービスのようにFWと相性の悪いサービスをどのように収容するのか、という3点に集約できるだろう。

エンドノード管理が基本

まず①については、システムそのもののセキュリティー防護レベルを上げるように努力するしかない。つまり、FWの概念が生み出された頃の議論に立ち返って、すべてのエンドノードのセキュリティー管理レベルの向上が必須であるという認識に基づいてセキュリティー管理

を組み立てなおす必要がある。このためには、すべてのエンドノードにおけるセキュリティーポリシーの策定、そして、必要なセキュリティー対策を実施する。

このときに重要なのは、すべてのエンドノードに対して見直しをすることで、セキュリティーポリシーに従うことのできないシステム、あるいは、セキュリティーポリシーを実装できない運用体制であるシステムを発見し、これらのシステムをネットワーク環境から取り除くことだ。経験的に言えば、システムにかかわるセキュリティートラブルは、十分な管理作業が行われていなかったシステムや、利用者が勝手に持ち込んだシステムなどから引き起こされることが多い。このため、すべてのエンドノードを点検する段階で、これらのトラブルを引き起こしそうなシステムのあぶり出しをする。FWを使っている間は、FWを重点的に管理し、エンドノードの管理は比較的緩い対応をしていることが多いだろう。その意味で、エンドノードの現状を把握し、問題のあるシステムを取り除くのだ。

戦略3 エンドノードの管理を徹底する。FWに依存した管理体制から、本来求められていたエンドノードの強化にシフトさせる。

コストを抑えるための手法

さらに管理者として考えなければならないのは、エンドノードのセキュリティー管理を徹底したときに予想される管理コストの上昇である。これを抑え込むためには、管理作業を徹底して自動化できるような機構の導入が必要だ。たとえば、システム設定の一括管理や自動パッチ適用環境を構築したり、必要なソフトウェアのバージョンアップを一括管理するシステムを構築したりすることは大きな効果がある。これらのエンドノードの一括管理システムは、近年複数のベンダーからパッケージソフトウェアが提供されるようになっている。特にクライアントシステムとして使われるウィンドウズシステムに適用できるパッケージソフトウェアが多い。

また、セキュリティー面から考えて管理コストの高いOSやシステムを使うのを避けるという手段もあるだろう。たとえば、メールサーバーを構築することを考えたときに、どのOSを基盤としたシステムを使うのが簡単だろうかと考えてみるのがいいだろう。最近では、電子メールはウイルス配布装置としても機能するので、メール本文からのウイルス除去機能を持つことが求められている。また、SPAMの除去もユーザーから強く求められるだろう。これらの条件を考えた、さらに管理者として管理しやすいプラットフォームを考えれば、自ずと結論が出るのではないだろうか。

ファイアーウォールの性能改善

一方、②の性能については、これまでサーバーの性能向上で使われてきた負荷分散装置（ロードバランサー）を使ったクラスター型FWを構築することで解決ができる。1台1台のFWについてはパフォーマンスを稼ぐことはほとんどできないかもしれないが、クラスター化によってシステム全体としては十分なパケット転送性能を提供するのだ。最近の1Gbps以上の帯域でインターネットと接続している組織では、今やクラスター型FWを使うのが当たり前になり始めている。最近のシステム性能の急激な上昇により、FWでもパケット転送能力が1Gbpsを達成しているものが出てきているが、FWにおける耐故障性能を考えるうえでFWのバックアップを準備する場合に、クラスタ型ーFWは単に性能の面だけでない利点が多い。

戦略4 FWのパケット転送能力向上に対する取り組みが必要になっている。現時点では、クラスター化したシステムを使うのが一般的。

P2Pは許すべきか禁止すべきか

P2P型アプリケーションのようにFWとの相性の悪いサービスをどのように扱うかは頭の痛い問題である。

1つの考え方は、P2P型アプリケーションを使うホストはFWに頼らないホストとするという考え方もあるだろう。たとえば、ポリコムなどのH.323テレビ会議システムは、相手のシステムから着呼する必要があるので、インターネット側から自由にアクセスできなければ意味がない。そのために、テレビ会議システムを稼働させるエンドノードではグローバルIPアドレスを与え、FWでアクセス制限を行わないことになる。

この環境を考えると、どうしてもエンドノードでのセキュリティー管理を徹底することが必要となる。このためには、同一のシステムはソフトウェアのバージョン管理などを一括して管理することで、セキュリティーホールを抱え込むことを極力排除する。さらに、VLAN機能などを使って同じサービスを使うシステムを同じセグメントにまとめてしまうことも効果が高い。仮にシステムにセキュリティーホールが見つかった場合には、そのセグメントを外部から切り離したり、あるいは、監視を強めたりすることが簡単にできる。このような少しの工夫でP2P型サービスを使うシステムの管理を簡単できるだろう。

もう1つの考え方は、当面P2P型サービスの利用を禁止するというものである。これは進歩に逆行するように思われる読者もいるかもしれない。たしかにP2Pはこれからのサービス構築の主要なパラダイムとして使われていくだろう。しかし、現時点でのP2P型サービスの多くがセキュリティー面での問題を抱えているのも事実である。たとえば、ファイル交換型P2Pサービスの代表的なシステムであるWinnyでは、交換されるファイルの多くにウイルスが付着している

ことが観測されている。また、ほかのP2P型システムでも同様の問題が指摘されている。現在のP2P型システムは発展途上段階にあり、機能的には大変興味深くても、セキュリティー機能が十分でないケースも多いのだ。その意味で使わせないということもある。

もう1つの可能性は、P2P型システムを自前で用意することである。たとえば、MSNメッセンジャーは、多くの人たちが使用する大変興味深いP2P型サービスである。しかし、このサービスは、メッセージ交換は現実には(他人が管理する)サーバーで中継されるシステムであり、交換される情報が漏洩する可能性もゼロではない。

また、直接相手システムとの間でファイルを交換できるが、これもセキュリティーポリシーの面から考えると見知らぬ第三者との間でのファイル交換を制限しないとすると問題が多い。

このようなことから、P2P型サービスでも自前でサービスを用意し、いわゆる不特定多数が利用できるサービスをユーザーに使わせないということも、1つの考え方だろう。実際、MSNメッセンジャーサービスは、マイクロソフトによってエンタープライズサービスとして独自に運用できるシステムが商品として提供されている。社内サービスとしてP2P型サービスを構築し、社内ユーザーには積極的にそのサービスを使わせるようにし、さらに外部からはVPNなどの認証機構を用いたアクセス手段でサービスにアクセスするというような対策も有効だろう。ユーザーが勝手にP2P型サービスを使い始めるような状況を放置するのは問題なのだ。

戦略5 FWと相性の悪いP2P型サービスについては、知恵を使ってうまい管理を行うことが必要。禁止するだけでは意味がない。変化に追随すること。

結局はユーザーの啓蒙が一番

最近のセキュリティー関係のトラブルを見ていると、FWの存在を前提にしたウイルスや、FWの本来の意味を台無しにするユーザーの行動が引き金になっているケースが多い。典型的なものが、ウイルスに感染したラップトップPCを持ち歩いて、いたるところに感染を飛び火させているユーザーの存在だろう。

このようなユーザーを発見し、そのユーザーを厳重に注意してペナルティーを与えるのは簡単なことだ。しかし、問題はネットワーク環境、ユーザーの利用形態、使用するアプリケーションなどが急激に変化しており、その変化にセキュリティー管理が追随できないことがより大きな問題だとして捉えるべきだろう。セキュリティー管理者は、状況の変化への機敏な対応が求められているのだ。

また単にセキュリティーポリシーを厳しくして、ユーザーの行動を制限することばかりに注力するのではなく、ユーザーが実行してしまいそうな行為を想定して、何らかのセキュリティートラブルを引き起こすことがあっても、それが波及しないような環境を作っておくことが重要だろう。そして、ユーザーに対しても、セキュリティーポリシーに反するような行為が与える影響について、正しい理解を持ってもらうことが必要である。

FWが十分に有効だった時代は、ある意味でセキュリティーの集中管理が可能な時代であった。しかし現在では、すべてのユーザーの協力を得て、分散的にセキュリティー管理を実施し、環境全体としてセキュリティー保全レベルを高める時代になっている。この意味で、すべてのユーザーがセキュリティー管理の当事者であるという意識を持って行動してもらう必要がある。ユーザーを味方につけるセキュリティー管理こそ、変化に機敏に対応できる基盤である。

［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