CISO STRATEGY

企業のリスクをマネージする戦略考

システムの監視、ユーザーの監視、プログラムの実行状態の監視、そして、ネットワークを介して行われる通信の監視。これらの監視は、システムの稼働状況を把握するために必要なだけではなく、外部からの不正アクセス行為、あるいは、内部からの情報漏洩などを把握するために必要となっている。

第九回 監視について考える

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

システムの運用や管理では、システムの現在の状態を把握する手段が必要であることは誰にとっても納得できることだ。状況を把握する手段がないままにシステムを管理することは、言わば目が見えない状態で山道をトレッキングするようなものだ。この場合、自分の身の安全を考えるのであれば身動きしないだろうし、かといって下手に動けば道に迷うのはほぼ確実で、穴に足をとられて転ぶかもしれない。最悪な状況では谷に滑落して落命するかもしれない。システム管理に言い換えれば、管理者としての自分の身を守るつもりになれば、管理者として何も新しいことはせずに前任者がやっていたことをそのまま踏襲するだけに徹するだろう。また、状況を把握しないで管理作業を無理やり遂行すれば本当に必要な管理作業はほとんどできず、下手をすればシステムの運用に大きな影響を与えるトラブルを引き起こしてしまうかもしれない。

「眼の見えない状態でのシステム管理」を回避するためには、管理者はシステムやネットワークの状況を把握するための監視機構を作り出さなければならない。これはプラントシステムなどの大規模システムでは当たり前のことで、監視装置の設置とシステム全体を把握するためのオペレーションセンターの構築が必ず行われている。また、システムを的確に把握するために、どこにどの種のセンサーを設置するのがいいのかということについても積極的に研究されている。

しかしコンピュータネットワークでは、状況把握のための監視機構をシステマティックに構築することは容易ではない。これには2つの理由がある。1つは過少投資を放置する経営者マインドであり、もう1つが監視網構築のための方法が確立していないことである。

企業環境でネットワークの導入が一般化したのは1990年代前半であり、まだまだ組織の存亡にかかわる基幹大規模システムとして組織が認識しているとは言いがたい。実際にネットワークが停止してしまったら、今や大部分の業務が大混乱になると十分に予想されるにもかかわらずである。このため、全般に管理系システムに対しての投資は抑制されることが多い。さらに技術に対する理解不足から、ネットワークの監視機構を必須のものとしてではなく、あくまでも追加的な機構として取り扱ってしまう経営者も後を絶たない。結果として、監視システムに対して過少投資の状況にあったとしても、それを放置してしまう経営者マインドが醸成されていると言ってもいいだろう。

また、監視システムをどのように構築したらいいかという課題に対して答える方法が確立していないのも大きな影響を与えている。このため、ネットワークをシステムとして捉えたときに、その挙動をどのように把握するのかは、管理者の経験や知識に負うところが大きく、結果として監視システムを構築したときに、管理者によって千差万別のシステムが作り上げられてしまうのだ。これは監視システムに対して適正な投資を判断することが難しくなることを意味する。以上のような理由から、組織として監視機構に対する投資が十分に行えない状況にある場合が多い。

戦略1 CIOは、監視機構に対して過少投資になっていないかを十分に注意を払わなければならない。

インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

多種多様なセンサーを置こう

ネットワークの監視網の構築では、多種多様なセンサーを目的に応じて設置する。

代表的なセンサーとしては、侵入検知装置（IDS）が挙げられる。IDSではすべてのトラフィックを監視し、システムに侵入しようとする行為を検知して報告する。ファイアーウォール（FW）もその意味ではセンサーとしての側面を持っている。FWでは、中継しようとするトラフィックを検査して、セキュリティーポリシーに合致しないトラフィックを拒否する。どんなトラフィックが拒否されているかはシステム側で警告を発することもできる。この意味で、FWをセンサーとして捉えることもできる。

さまざまなサーバーから提示される警告も重要な情報となりうる。たとえば、WWWサーバーであれば、バッファーオーバーフローの部分がないかどうかを検査するような不審なアクセスがあれば、当然WWWサーバーとして警告を発するだろう。また、SMTPサーバーであれば、メールに添付されているファイルにウイルス付きのものがないかどうかを検査するのが当たり前になっているが、検査結果に基づいて適切な警告を発してくれる。たとえば、自分のドメインに属するシステムからのメールにウイルスが含まれているような場合には、重要な情報である。恐らく該当するメールを発したシステムはウイルスに感染しているだろう。

また、DoS攻撃を考えれば、どのホストからどのようなトラフィックが発せられているかを監視するべきだろう。これにはL3スイッチやルーターなどのネットワーク構成機器において、適切なトラフィックカウンターを用意したり、あるいは、RMON機能（遠隔地のネットワークの通信状況を監視する機能）を用いてトラフィックを計測したりすることが必要になる。

このように、セキュリティー管理で使われるセンサーの多くは、通常使用している機器に用意されている機能をうまく使うことで構築できる。たとえ、サーバーやネットワーク構成機器ではない、個々のユーザーが用いるPCなどでも、実はセンサーとして情報を得られる場合も多い。その意味で、各システムがどのようなセンサーとして利用できるのかを常日頃から考えておいたほうがいい。

戦略2 監視網を構成するセンサーの多くは、通常使っているシステムに用意されている機能を流用できる。常日頃から、どのようなセンサーとして利用できるかを考えておくべきだ。

管理系網の分離が必要となる

監視網を構築するときに、センサーだけではなく、センサーから発せられる情報をどのように集めるかを考えることが必要になる。これまでの多くのネットワーク環境では、ユーザーのためのトラフィックと管理のためのトラフィックを分離せずに1つのネットワークで混ぜて扱う方法が一般的であった。しかし、ISPのネットワークでは管理トラフィックを一般ユーザートラフィックと混ぜないようにしたほうがいいという考え方が支配的であり、管理トラフィックを分離して扱ういわゆるアウトバンド管理が行われている。企業の基幹業務のネットワークに依存する度合いが高まるにつれて、企業においてもこのアウトバンド管理を導入することが増加している。

また、本当に止まらないネットワークを作ることを考えれば管理用ネットワークを物理的に分離したネットワークとして構築する必要があったが、最近の論理ネットワーク技術、たとえばイーサネットでのVLAN（仮想的に物理線上にLANを構築する技術）をうまく使って、理論的に管理用ネットワークを分離することも行われている。これは、網の構築コストを抑えつつ、サービス系と管理系を分けることによって管理トラフィックを分離するだけではなく、安全性も高いネットワークを作ることを狙いとしている。

戦略3 サービス系ネットワークと管理系ネットワークを分離したアウトバンド管理が広がりつつある。セキュリティー的に強いネットワークを作ることを考えれば検討の価値は高い。

直感と楽観ではいけない

監視システムでは、ネットワークの各所に配置されたセンサーからの情報を収集し、解析し、現在のネットワーク環境で何が起きているかを把握することが目的となる。このことから、セキュリティー管理責任者としては、次の2点を明確に理解している必要がある。

1. 何を知るために監視網を構築するのか（目的の明確化）。
2. 目的に合致した監視網となっているのか（適切な構築）。

当たり前の話だが、適切なセンサーを使わずして、適切な情報を得ることなど不可能である。IDSでネットワークを流れるトラフィックの流量を知ろうとするのはまったくの間違いである。そのためには、スイッチやルーターにおけるトラフィック計測機能をうまく使うほうが適切であろうし、さらには、専用のトラフィック計測装置を使うほうが精度の高い計測が可能になる。この意味で、目的に合致したセンサーを使うことが必要である。

また、センサーのないところでは情報を得られない。したがって、想像力を働かせて状況を考えるしかないのだが、監視対象によっては想像力が有効でないものも多い。その意味で、本当に知りたいことを知るために適切なセンサーが適切な

©1994-2007 Impress R&D

場所にインストールされているのかということも十分に考えなければならない要素である。

ここで一番怖いこととして私たちが常に忘れてはならないことは、監視網を作ると、その監視網が何も警告を発しないときには、何もトラブルが発生しているはずはないと考えるオペレーターが非常に多いことである。つまり監視網が目的に合致した形で作り上げられている場合には、このオペレーターの判断も大きくは間違うことはないだろう。しかし、目的に合致していない監視網から得られた情報でトラブルは起きていないと判断するのであれば、大きな間違いを起こすことが多い。そして、過去にプラントや各種システムに発生した大規模なトラブルでは、目的に合致していないセンサーから得られている情報だけに頼ったことにより、判断を誤って大きなトラブルに発展させてしまったケースが多い。

情報通信システムであっても、ほかのシステムの運用で得られている教訓に学ぶべきである。つまり、目的が明確に設定され、その目的に合致した監視網が構築されているのかどうかを常に考えて監視網を管理して運用することが必要である。その意味で、管理者は常に合理的に判断することと、悲観的に物事を考える癖をつけるべきである。楽観と直感に頼るのはあまりに危険である。本当に自分の判断は合理性があるかを常に点検し、何も問題がなくても何かを見落としているのではないかという悲観的な前提で行動していれば、トラブルの発生を抑制する効果は高い。少なくとも、直感と楽観からの判断よりも、頼りがいのある判断が生まれてくるだろう。

戦略4 監視網を構築する目的を明確に設定し、その目的に合致した監視網が構築されているかどうかを常に点検することが必要。

コストと利益の関係を算出する

「セキュリティー管理では、ネットワークの状況を把握するために監視網を構築するのが重要だ」と講演で説明すると、監視網の構築にどの程度のコストを負担するのが適切だろうかという質問をたびたび受ける。これほど答えるのに難しい問題はないが、CISOはこの問題を考えなければならない。

まず、そもそもセキュリティー管理をするうえでリスクアセスメントは必ずやらなければならない。予想可能なリスクを想定して、統計確率などの考えを駆使して期待損失を計算するのである。そして、たとえば今後1年間の期待損失が得られたならば、そのうちの何割を実際にセキュリティー管理に投資するかを経営陣が決めるのがコスト同定のプロセスである。簡単に言えば、リスクアセスメントによって「このまま放置すると、今後1年間にどれだけ被害が発生する可能性が高いか」という値を得て、その情報を元にセキュリティー管理のための投資額を決めるということだ。この意味で、リスクアセスメントは一度実施すれば十分というものではなく、少なくとも定期的に実施する必要があるし、また、組織構造や情報通信システムが大きく変更されたときには、リスクアセスメントを適宜実施することが必要になるだろう。さて、ここで得られた投資額が、少なくとも使える費用の上限になるということは理解してほしい。

次に、セキュリティー管理の中で、どの程度を監視網の運用に投資していいと考えるべきか。少なくとも監視という業務は定常的に24時間、365日行われる業務である。したがって、監視業務は実は何も悪いことが起きないときのセキュリティー管理の中心的な業務になる。そこで、この業務のオーバーヘッドをどれだけ減らすのかという算定をする必要があるだろう。当然、たくさんのセンサーを設置して多くの情報を得て解析し、多くのことを知る必要があるとしたら、その監視網構築と運用には多くのコストが必要になってしまう。そして、その監視網が本当に必要かどうかを考える必要がある。

監視網に適切な投資をすると、実は定常的な監視コストを抑えられ、かつ、機能的にレベルの高いものを作り上げられる可能性が高い。一方、システムに対する投資が過小であった場合には、何かトラブルが発生した際には人海戦術でトラブルを終息させることが必要になる。人海戦術をとるだけの十分な人員が確保できると踏むのであれば、監視網には大きく投資しなくていいかもしれない。しかし、最近の経済状況とネットワークへの業務依存度の上昇を考えれば、読者の皆さんには私の答えは明らかだと思う。

戦略5 監視網の構築には適切な投資が必要。過少投資になると、トラブルが発生した場合には人海戦術でトラブルを終息させなければならないことになる。つまり、過少投資は業務を止めてしまうリスクを高めることになる。

人の秘密を蜜の味にしないために

誰でも、ほかの人が何をしているかを覗き見たくなるのは普通のことだ。否定することはない。誰だって覗き見趣味は持っている。

さて、これが組織の情報通信システムの監視となると、どのように考えるべきか。これには2つの観点からの議論が必要である。1つが情報漏洩阻止の考え方、もう1つがプライバシー管理の考え方である。

組織にとって情報漏洩のリスクは年々増大する一方である。さらに、最近しばしば発生した個人情報の流出事故は、多くの企業に個人情報漏洩のインパクトの

インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

大きさを認識させた。さらに2003年には個人情報保護法が成立し、個人情報保護を義務付ける制度がスタートする。

また、企業が持つさまざまな知的財産についてもその流出を防ぐ方策が必要になっているという認識が強い。特に技術開発情報や特許出願前の技術情報については相当厳格な管理が始まっている。電子メールなどで組織外の人たちに対して簡単に情報を漏洩させられる環境が多いことも、この危機感を高めている。

このようなことから、組織外部とインターネットを介した通信を基本的に禁止し、外部との通信を許可制にしている組織も登場してきている。また、社員すべてのメールのやり取りを本文も含めて記録し、常にその中味を監視している企業も存在している。つまり、情報漏洩を防ぐために、すべての通信を徹底的に監視しようという動きである。このような取り扱いには私自身は一定の理解を持っている。しかし、次のような問題を解決してなければならないと思う。

①すべての通信を記録し、監視対象に置いていることをすべての社員に伝えて理解を得ていること。これは情報漏洩について企業運営側が真剣に本気で取り組んでいるという態度を示すだけではなく、その意味を社員にわからせるという意味もある。

②できる限り技術を用いて解決する努力をしていること。たとえば、先に述べたように電子メールの利用を許可制にするというのは愚の骨頂である。利便性を犠牲にせずに、技術をうまく使って解決することが必要であり、また、利用者の利便性を下げることも許容できないのが一般的であるからだ。

③情報漏洩を防ぐという目的を逸脱しないこと。特に、メールなどのプライベートな利用について必要以上の干渉とペナルティーを与えるようなことをしないこと。よく問題になるのは、電子メールの私的利用をどこまで許容するのかということである。たとえば、会社のメールアドレスを使っているときには、会社の看板を背負って通信しているという感覚を持ってもらわなければならない。と言っても、私的な通信だって混ざることもある。情報漏洩を防ぐためにルールを作ったとしたら、そのルールを私的利用にまで拡大すべきではないし、もしも私的利用を制限したいのであれば、そのルールを作るべきだ。

④監視にかかわる作業者の守秘義務を明文化し、さらにそのルールを厳密に適用すること。ユーザーの信頼を得られるオペレーションだけが監視を正当化する力である。

現在であれば、実はメールアカウントを自分で用意することも簡単にできるようになった。その意味では、会社のメールアカウントは、会社員としての目的に合致しているものにしか使ってはいけないという形での、力強い宣言をしてもいいだろう。しかし、その宣言に基づいて、あまりに各個人の行動に介入しすぎる対策をしては、うまく機能しないのだ。

監視網の標準化が重要

監視網を作っていくうえで、もう1つ重要なのは、できる限り自分たちの標準化を行っておくべきである。

たとえば、管理系網はどのように運営するのか、また、どのように理論的に隔離するのか。センサーにアクセスするプロトコルは何を使うのか、また、ソフトウェアのバージョンは何か。センサーから得られる情報をどこに収集し、どのように管理するのか。収集した情報に誰がアクセスできるのか。

このような条件を明らかにし、さらにその理由は何であるのかを文書化しておくことが重要である。

なぜ標準化を行うのかについては、いくつかの理由があるが、もっとも大きな理由は、管理系網を作り上げたときに考えたことを忘れやすいということだ。また、問題が発生したときに、やっつけで作ったシステムがそのまま生き残ってしまうことも多いのだ。このようなことから、現実には、管理系システムにおいて整合性を保つことは大変な難しいのだ。このために、どんなシステムを作ったのかを少なくともメモにして、あとから見直しができるようにしておく必要がある。また、管理系システムがどのような能力を持っているのかを別の管理者が見直せるようにするためにも、文書化は重要である。

そして、さらに管理系システムを組み上げる際に自分自身で決めた標準を持っていると、上記の作業がさらに簡便に行えるようになる。

戦略6 監視網を構成する技術と構成について、自分たちの標準化を行っておこう。

セキュリティーの質を上げる監視

セキュリティー管理においては、監視機構は重要な役割を負っている。その意味で、CISOは巧みに、そしてできる限り多くの知恵を集めて監視機構を構築することが必要だ。よい管理系を作り上げれば、セキュリティー管理の質も格段に改善されることは確かである。

©1994-2007 Impress R&D

［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

Copyright © 1994-2007 Impress R&D, an Impress Group company. All rights reserved.