CISO STRATEGY

# 企業のリスクをマネージする戦略考

セキュリティー管理に万全はない。失敗はつきものである。その失敗をどのように消化すべきかについて考える。セキュリティー管理における失敗は、システムを改善するためのキッカケである。このキッカケをうまく使えるかがセキュリティー管理を豊かなものにするポイントとなる。単に失敗として糾弾するだけでは、システムはよくならない。

## 第四回 失敗からの学習

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

セキュリティー管理は、管理対象である情報通信システムにおいて、いわゆるセキュリティーインシデントが発生しないようにすることが目的である。ここで、セキュリティーインシデントとは、各組織で決められているセキュリティーポリシーに違反する事象を指すことが一般的である。したがって、セキュリティーインシデントの実態を考えると、組織ごとに多少の差があるものだ。

しかし、どんなセキュリティー管理を行おうとも、インシデントの発生を想定した対応手順は必ず決めなければならない。インシデント発生の可能性をゼロにすることはどんなに頑張っても不可能であるからだ。セキュリティー管理では、リスクアセスメントの作業によって、システムにとってのさまざまなリスクを明らかにし、顕在化しているリスクに対して対策を立てて対応することになる。しかし、同時に常に顕在化していない未知の原因によって引き起こされるセキュリティーインシデントの発生の可能性を否定することはできないのだ。たとえば、未知のセキュリティーホールを用いた不正アクセス行為というものを考えれば、これまでの経験から発生の可能性がゼロと言い切ることはできないのであるが、しかし具体的対策が立てられるかと言えば、未知であるがゆえに対策を立てることは不可能に近い。したがって、どんなに頑張っても、セキュリティーインシデントが発生する可能性はあり、仮にインシデントが発生してしまったら、できる限り影響範囲を最小化し、同時に短期間にシステムを復旧できるようにすることを目標にセキュリティー管理を設計するのがあたりまえだ。

また、セキュリティー管理に携わる技術者だけがインシデント発生の可能性に対する認識を持っていては仕方がない。システムは誰もが使うものであり、また、組織運営に直接かかわるものである。したがって、組織トップを含めた経営陣やユーザーにおいても、「インシデントは発生する可能性が常にある」という認識を持たなければならない。余談になるが、2002年7月に住民基本台帳ネットワークの運用開始時に、片山総務大臣が「住基ネットワークは100パーセント安全です」という談話が、情報セキュリティー専門家の失笑を誘ったのは有名な話である。

**戦略1** インシデントの発生の可能性は、セキュリティー管理にどれだけ頑張ってもゼロにはならない。このことをみんなが理解するようにしよう。

### 「これは誰の責任か?」という愚問

前節で述べたように、インシデントの発生は避けることができない。もちろん、顕在化しているリスクについて、それを看過し放置していたことでインシデントが発生したならば、その責任は追及されてしかるべきだと考える。しかし真っ当な方法と手順でセキュリティー管理を設計し、運用していたとしたら、その場合には責任追及はどれだけ重要だろうか。

インシデントが発生すると、すぐに「インシデントの発生したことには、誰が責任とるのだ？」と詰問する経営者がいる。確かに、責任問題をうやむやにするのはよくないが、かといって本当に責任追及を厳しく行っても、実はいいことはあまりないのだ。どちらかと言えば、セキュリティー管理の実務に携わっていたスタッフのモラルハザードを起こしてしまう可能性もあるのだ。

インシデントが発生した場合、本来私たちが注視しなければならないことは、発生したインシデントをどれだけ短期間に沈静化させて被害拡大を抑えることができたかであろう。発生したインシデントがネットワーク伝搬型ウイルスのように被害の拡大を引き起こす可能性が高い要因によって引き起こされたのであれば、最初に感染してしまったシステムはどのシステムなのかを解明することにより、責任を負うべき人間を探すことよりも、他のシステムにウイルスが伝搬して被害が拡大してしまうことをいかに抑え込むのかが本当に重要なことだろう。

インシデントに対して立ち向かうエンジニアは、原因がよく見えない状況で被害の拡大を抑えることに努力する、言ってみれば消防士と同じである。インシデントはまさに火災と同じであり、インシデントを正しく抑え込むことができれば、つまり、火災を鎮火することができれば、その行為を本来たたえるべきであろう。そして、被害が最小にできれば、賞賛に値するはずだ。そして、火災の場合と同じようにインシデントが抑え込まれた後に、実際の原因を解明する「現場検証」が行われるというのが納得できる手順であろう。

一方、インシデントが発生した段階で、すぐさま誰の責任かを問うことは、言ってみれば火災現場での消火作業に取り組んでいる消防士に対して、「まずは君らの火災防止への取り組みを評価するから」と言うようなものだ。そんなことは鎮火してからにしてくれ、というのが本音だろう。コンピュータネットワークにおけるセキュリティーインシデントへの対応でも同じだ。まずはインシデントの影響を押さえ込み、さらには、再発しないように改善することが、他の何よりも優先順位が高い。

**戦略2** インシデント対応では、被害の拡大を食い止めたことを称えるべきであり、責任追及はモラルハザードを引き起こす可能性が高い。

## 原因究明と犯人探し

インシデントが発生してしまった場合、まずはインシデントの影響を最小化すること、つまり、被害の拡大を最小化することが優先される作業であるが、その作業中にも並行して行わなければならない作業がある。それが、原因解明のための情報収集と保全である。さらに、場合によってはインシデントを引き起こした犯人を探し出すために司法当局の捜査に委ねるための、いわゆる証拠を確保することも必要になるかもしれない。

この情報収集保全作業をしている段階で常々考えさせられることは、犯人を見つけることに重きを置くのか、それとも、なぜそのインシデントが発生したのかを追及する原因究明に重きを置くのかという、優先順位設定の問題である。多くの場合には、原因究明に重きを置くのが一般的だと思う。しかし、状況によっては犯人探しに重点をおかなければならないこともある。

セキュリティー管理を考える場合、何を守るべきなのかを考えるのが普通である。つまり、管理対象としての資産はなんであるのかという問題に結論を出しておくことである。多くの場合は、システムやネットワークそのものの安定した稼働に重きを置く。このような場合には、システムの運用に影響を与える事態を発生させないことがセキュリティー管理の基本的な方針になるだろう。セキュリティーインシデントが発生した際には、おそらくその未知の手順によってインシデントが発生させられたと想定してもいいだろう。本来、セキュリティー管理では顕在化しているリスクに対しては何らかの対応をするのが一般的であるから、インシデントが発生すれば、それは未知の手法によるインシデントと考えるべきだろう。したがって、当然原因究明に努めて再発防止を確実なものにすることが重要になるのだ。

一方、システムなどはどうでもよくて、システムが持っている情報そのものを保護対象にする場合には、誰が犯人かを考えることが本当に重要になる。たとえば、オンラインショッピングサービスを運営していて、どうやらお客さんのクレジットカード番号が盗み出されたようだということが発覚した場合には、どのような手順で盗み出されたということを探求することも重要だが、それ以上に誰がどこに持ち出したかが大きな懸念事項となってしまうのだ。

前者の考え方をいわゆるシステムセキュリティーと呼び、後者を情報セキュリ

ティーと呼ぶことも多い。私たちが実施するセキュリティー管理が本来どちらに重点をおいているかを考えることで、どう行動すべきかを考える重要な指針を与えてくれることに気が付いていなければならない。

**戦略3** 実施するセキュリティー管理の目標は、システムセキュリティーなのか、情報セキュリティーなのか、あるいは、その両方なのか。これがわかっていないと、緊急対応時の情報収集のやり方を間違うこともありうる。

## 手直しにはお金が必要

セキュリティーインシデントが発生してしまったということは、セキュリティー管理において失敗が発生したことと等しい。発生したインシデントの被害拡大を阻止することが短時間にできず、かなり大きな被害を発生させてしまったら、セキュリティー管理においては大失敗の醜態を晒したことになる。このような失敗を引き起こしてしまった場合には、失敗を反省するとか後悔するとかいったことは一般的には重要だろう。しかし、セキュリティー管理においては、失敗がなぜ起きてしまったのか、そして、失敗を再発させないためには何をしたらよいのかを考える、つまり、失敗から学ぶことが一番重要なのだ。

インシデントが発生した場合には、さまざまなログ情報を解析することで何が起きたのかを調べてシステムを再構築することにある。そして、その再構築の過程で原因を究明することなる。

もちろん、簡単に解決してしまうインシデントも数多くあるし、一方簡単に原因究明ができず、原因究明を始めたら、ある意味で研究になってしまうというような難解なインシデントも発生しないわけではない。とはいえ、最終的に原因がわかると、再発を防止するためには、大抵システムを改修する必要が出てくる。このシステム改修では、最悪の場合、システムを廃棄するというかなり大掛かりで乱暴なオプションから、単純にセキュリティーパッチを適用するという典型的な軽微な作業で改修が終わるものまである。しかし、どんな改修改善であれ、その場合にはお金が必要となる。

前節で火災の話をしたが、火災が発生してしまった場合には、大抵の場合に火災保険によって火災が発生したことによる損害を補償してくれる費用を確保することができる。この意味で、インシデントが発生した場合に、それに対応するための原資として「保険」が存在していると言ってもいい。ところが、コンピュータネットワーク系のインシデントの場合には保険制度が一般化しているわけではない。このため、二度と同種のインシデントを発生させないために行われるシステム改修のための資金調達のオーバーヘッドは大きなものになる。下手をすれば、インシデントは何とか押さえ込んだとしても、その先で改修のための資金を手にできないため、リスクは顕在化し、そのリスクの発生の可能性も確認している段階で、そのリスクに対応したセキュリティー管理施策が実施できないことにもなってしまうのだ。実際、期中での追加的な予算を支出することが難しい組織も、官公庁・地方公共団体で数多くある。この意味で、いざというときにはシステムの改修ができる資金のプールについても議論が必要となる。

**戦略4** インシデント再発防止のために、システム改修のための資金調達が必須。突発事故の事後対応に資する資金をどのようにプールするかは、かならずCIOは考えなければならない。

## 内部犯行は大きな課題

セキュリティー管理で本当に頭の痛い問題は、組織構成員によって内部から引き起こされるセキュリティーインシデントをどのように取り扱えば適切なのかという問題だろう。実際、日本ネットワークセキュリティー協会の平成14年度に行われた調査によれば、近年発生したセキュリティーインシデントの43パーセント程度が内部犯行であったことが報告されている。また内部犯行問題は年々大きくなっていると言ってもいい。

内部犯行の本質的に嫌なところは、システム内部から身内に裏切られる構造である。

本来、セキュリティーインシデントは組織外部からの攻撃によって起こるという仮定が正しいとすれば、外部とのネットワーク接続点にファイアーウォールやIDSなどのセキュリティー機器を十分に設置し、そこで外部からやってくる「悪いこと」をまとめて管理下に置いてしまうということであろう。これにより、投資の一点集中が行われ、小さなシステム投資によって大きな成果を得られるのだ。

ところが、内部犯行に対応する場合には、組織内部のユーザーは悪人だと仮定して、ネットワークの構造、サービス提供の構造、サービスそのものの内容について吟味を行い、各組織構成員に割

り当てられている業務と情報アクセス権を逸脱することがない合理的なシステムを実装することが必要になる。さらに、そのシステム利用状況をいつでも監査できるような情報収集体制も合わせて構築することが必要になる。これだけを書き下しただけでも、内部犯行に対応するためにはより多くの投資が必要になることがわかるだろう。

同時に、内部犯行が発生した場合に、なぜその内部犯行が発生したのかを解明することは複雑になってしまう。

たとえば、最近いろいろな組織で多発しているセキュリティーインシデントが、本来持ち出してはならないデータが内部者によって外部に持ち出されてしまうものである。このインシデントが発生した場合、どこに原因があるのかを考えると、本当に多くの可能性があるのだ。情報システムのアカウント管理と情報に対するアクセス権の管理の方法が悪い場合もあるだろう。しかし、アカウントシステムに対して何でもできるシステム管理者であれば、実際にはアカウントシステムは無力であるので、別の方法で情報を守らなければならない。では、実際にどんな方法で保護しているのか。システムに対する物理的なアクセス制限は正しくかけられていたのだろうか。とりとめなくここに書いてしまったが、本当に知恵をめぐらすことが必要だ。

**戦略5** 内部犯行を防ぐためには、本当に知恵を絞ってシステムを構築する必要がある。さらに、そのシステムとは単に情報通信システムだけではなく、服務規程、手引きやガイドラインなどの記述や、さらには、教育制度、人事給与制度などにも影響される。多面的に検討すべし。

## フィードバックのかけ方

発生したインシデントについて、どのように発生し、どのように沈静化し、さらに、再発防止をどのように行ったのか、という情報は、実務に携わるエンジニアだけが共有すべきものではない。これは経営トップから末端のユーザーに対してもフィードバックをかけることが重要である。これはセキュリティー管理が機能していることを示すという意味もあり、また、同時に合理的な行動を経営者からエンドユーザーまで促すことにつながる。

**戦略6** 発生したインシデントについては、経営者からエンドユーザーに対してまで必要に応じて事実をうまくフィードバックすることが重要。

セキュリティー管理は、実際には利益を直接生み出すものではなく、また、いざというときに機能することが求められているものである。したがって、何事も発生しなければ経営者としては経費カットを目標にセキュリティー管理にかかわる資金を切り詰めることを考え出すことも十分予想される。また、経営者はセキュリティーの専門家でもないので、実際には情報通信システムのセキュリティー管理がおろそかになった場合に、どれだけの被害が発生するかという面に対して適切な判断を下せる能力があることは少ない。このため、セキュリティー管理が正しく機能していて、正しく機能できている理由を経営者に対して伝えることは大きな意味があり、さらに、セキュリティー管理の実務グループに対する信頼感の醸成が可能となる。

また、エンドユーザーにとっても、セキュリティー問題が何も珍しい問題ではなく、日常的に意識を持って対応すべき事項であることを認識する機会として使ってもいいだろう。

どちらにしろ、うまい形でのフィードバックをかけることが重要である。そして、実際に経営者、あるいは、エンドユーザーを自分たちの味方にするために、ある程度の見識を持ってもらうことを目指すのが大事だろう。

今回はセキュリティーインシデント発生という、セキュリティー管理での失敗が発生してしまった状況で、この失敗から何を学ぶのか、この失敗をどのようにうまく利用するのかについて、私なりの考えを述べた。最近、失敗学というのがブームで、多くのビジネス書で失敗からいかに学ぶかを伝えている。これらの失敗学系ビジネス書は大変興味深いことが書かれている。しかし、情報通信システムのセキュリティー管理においてはインシデント発生は情報通信システムの運営における本来不確実性の現れと考えるべきである。不確実性をもった系の制御は、単純な失敗からの復旧とは違うという点は強く認識すべきだ。このため、実際には多くのビジネス書は適用可能な知識を伝えていない。また、セキュリティー管理では極めて合理的な結論への誘導が必要になる。しかし、多くの失敗学では、精神論がしばしば展開されている。この2点に注意しながら巷の「失敗学」を学んでみるのもいい経験となるだろう。

# ［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