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ついて責任を持たされたあなたは、いま何をしなければならないのか。セキュリティー管理に使用できる技術を買い付けることがあなたの最初に行わなければならない仕事だろうか。実はそれは誤りである。組織として、合理的な判断と迅速な対応ができるための基盤を組織的に作り出すこと、危機対応体制をうまく組織に作りこむことである。

第一回 「判断」するための道筋を作る

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

最近、どの組織でもセキュリティー管理をどのように強化するかについての議論が盛んである。数年前であれば、まずセキュリティー管理の重要性を理解してもらうことから始めなければならない状況が大半であった。しかし、ネットワークを介して伝播するコンピュータウイルスの大量感染、インターネット環境で多発する不正アクセス事件、あるいは、個人情報などの情報漏洩事件などが近年頻発したことから、いまやセキュリティー管理の重要性はシステムの管理運営に携わる技術者だけでなく、エンドユーザーや経営者にも理解されるようになった。現在私たちが考えなければならない課題は「どのようにセキュリティー管理を実施するか」という点につきる。

ところが、セキュリティー管理は具体的に何をするのかと考えると、組織それぞれで答えが異なる。ある組織では情報漏洩を防ぐことがセキュリティー管理の重点目標になることもあるだろうし、他の組織ではネットワークで提供しているサービスを停止させないことが最優先される場合もある。管理対象となるシステムやデータ、サービスなどの違いがあるからこそ、想定されるリスクが異なり、結果として各組織でのセキュリティー管理の実施方法が千差万別になるのは当然なのだ。一方、この多様性が、セキュリティー管理の難しさを高めている。特に、どのような技術を使用して、どのように運用するのかについては、他の組織の事例は参考になるものの、その方法を単純に移植しても役立たない。各組織に適合する個別化が必要となる。

CISOは誰と仕事をするのか？

仮にあなたが属する組織の最高セキュリティー統括管理者に、あなた自身が就任したとしよう。最近の流行語であればCISO（ Chief Information Security Officer）になったという言い方もできる。この場合、あなたはどんな人たちとどんなふうに仕事を進めていかなければならないのだろうか。

当然最初に話をしなければならないのは、組織全体の通信基盤と情報処理基盤を運営しているグループだろう。どのようなシステムがどのように使われているのか、通信基盤への依存度はどのくらいあるのか、どのような種類の情報資源がどの程度存在しているのか——CISOならばセキュリティー管理体制を考えるには、技術的な視点からの基礎情報を得ることは必要不可欠だ。

しかし、基礎情報を得る作業を始めた瞬間に、実は情報処理基盤にかかわるほかの存在に気が付くはずだ。情報処理部門が管理しているシステムを使って、たとえば営業部門がセールス活動を行い、さらに別の部門がセールス活動のデータを使っているようなことがある。確かに情報処理部門がシステムを管理運用しているが、そのシステムのデータは、まったく別の部門の所管で管理されていることがある。このように調べていくと、最近の企業であれば、もはやほぼすべての部門が組織内部の情報処理基盤と通信基盤に依存し、関係を持ち、さらには具体的なデータに対する管理の責任を分散的に負っている状況が明らかになるはずだ。

いったい本当の責任者は誰だ？

どんな組織であっても、権限と責任は表裏一体のものとして考えられている。

ある領域について意思決定できる権限を持っている場合、行った意思決定について責任を負っていると考えるのが普通だろう。

ところが情報処理システムや通信基盤環境でのオペレーションを考えた場合には、この権限と責任の関係が複雑になってしまっているケースが多々ある。たとえば、情報処理部門が全権を掌握してネットワークを運用していたとしよう。このとき、ネットワークに対してサービスを提供するサーバーの管理そのものは情報処理部門が行っていたとしても、その中のデータの利用と管理には営業部門などが深くかかわり、情報処理部門に介入させていないような状況もあるのだ。このような状況だと、システムそのものの運用を司る情報処理部門は、システム運用の停止については常に営業部門との調整が必要となる。

こういった状況はセキュリティー管理の面からは頭痛の種にしかならない。

セキュリティーホールがOSにあるからシステムをいったん停止させてソフトウェアを更新したいと情報処理部門が言っても、セールス部門が「商売の都合上そのまま暫定的に運用してくれ」と言って継続な運用を主張するかもしれない。その際、外部から不正アクセスを引き起こされ、結局サービスが止まってしまったとしたら誰の責任になるのか。このような問題を発生させないために、CISOは組織体制を変更しなければならない。

戦略1 責任の所在が明らかでない状況を生み出さないようにする。

全権を掌握することが大事

この問題を解決する一番簡単な方法は、CISOが全権を掌握することである。つまり、セキュリティーにかかわる問題について、その解決方法、意思決定、責任をすべてCISOが負うような体制を構築することだ。

ところが、セキュリティーにかかわる事案について全権を掌握するようにCISOというポストを設定しても、実際にはそうはならない状況に陥ることがある。つまり、「CISOの言うことを聞かない」状況である。これを解消するためには、組織のセキュリティーポリシーを制定する中で、責任体制を厳密に策定し、CISOが全権を掌握できる構造を組織全体に認めさせることが必要となる。

これに付随して、全権を掌握するために必要となる機能的な組織も作らなければならない。セキュリティーポリシーの策定により、形式上CISOが全権を掌握できるようになっていても、実質的に全権を掌握できなければ、結局は画餅でしかない。

戦略2 CISOにとって機能的な組織を作り出す。

機能的組織はどうあるべきか？

多くの組織で間違いを犯すのが、CISOの管理体系を既存の組織構造に完全に対応させてしまうことである。よくある形式は、取締役の誰かがCISOに就任し、その下に各事業部長が副責任者として名を連ねるような構造である。これで本当に効果的なセキュリティー管理が実現されるのだろうか。

1つだけはっきりしているのは、企業における「経営判断能力」と、セキュリティー管理における「危機管理能力」は別の種類の能力であることだ。経営判断能力は勝負でいかに勝つかという判断力であり、その判断の中ではリスクを抱えることを許容できる。一方、危機管理能力は、多くの要素を相互的に判断してリスクを減らし、手堅い準備と迅速な対応をするための計画能力だと言ってもいい。つまり、危機管理ではより多くのリスクを抱えることは極力排除することを優先する。したがって、経営に最適化されている組織構造に、CISOをトップとする危機管理体制をそのまま当てはめてもうまく機能しない。

セキュリティー管理の作業は大きく2つのカテゴリーに分けられる。1つが「準備」であり、もう1つが「緊急対応」である。

準備は、日常的な作業の中で行われるもので、たとえばデータのバックアップや、システムの検証や改善、新しいシステムの導入時の入念な検査、さらには、ユーザーの教育やサポート業務などが含まれる。これらの業務は、ほかの業務と並列して存在でき、管理構造も既存の構造をそのまま流用しても問題は少ない。

もう1つの作業である緊急対応は、ネットワークやシステムにセキュリティー上のトラブルが発生した場合に、その影響を最小限度に抑え込むことを目的に、通常の権限のさらに上位からシステムやネットワークを運用することにほかならない。

このような視点から考えると、CISOが行わなければならないのは、次の3点になる。

1. 緊急対応を行うための設計と、そのときの命令系統を作ること。
   この命令系統は機能的でなければならず、即応性の期待できる形態でなければならない。事業部長をトップとするような体制を望むのではなく、「具体的なシステムやネットワークの運用に当たっている部署」をそのまま指揮系統に組み入れることを考える。このときに、CISOの発する命令が最優先されるようになっていなければならない。

2. 緊急対応を簡単にするための準備作業を設計できるチームを持つこと。
   通常は組織全体の情報通信システムを設計しているグループがこの任に当たることが多い。このグループは、存在するリスクを直視し、そのリスクを低減するための作業を設計する。多くの

場合、この作業は技術的に検討して行われるが、場合によっては業務フローを変更したり、既存の管理責任体制を変更したりすることが必要になる。この場合には、CISOが非技術的な課題を解決するためのチームを編成する。

3. CISOの下で作られた準備のプロセスが確実に実施されるように、既存の管理責任構造の中で了承が得られること。
設計した準備作業が行われなければ、緊急対応の作業時に大きな問題が起きてしまう。このようなリスクの発生を避けるために、作業には正しく準備が行われているかを確認するための監査も含まれる。

この3つのCISOが行うべき作業のうち、2番目の作業が既存の管理構造からは一番恐怖感を持たれる内容である。というのも、非常時だけとはいえ、既存の命令系統とは違う系統が生まれてしまうからだ。CISOは、緊急時用の別命令系統が存在したとしても、業務に大きな影響を与えないことを確信させる必要がある。このためには、「準備」のプロセスを既存の管理構造に属する人と一緒に綿密に設計することが肝要である。「準備」が入念に行われて、緊急時にもリスクが低減されていることが確信できれば、既存の管理構造からの恐怖感は小さくなるに違いない。

戦略3 CISOが動かす命令系統と、既存の管理構造との折り合いをつける。

全権を掌握できない場合には

不幸にして全権を掌握できない場合でも、何らかの方法で組織全体のセキュリティー管理を把握し、その改良に取り組まなければならない。これまで私が見てきたCISOによる全権を掌握できなかった多くの組織では、問題解決に「緩やかな連合軍構想」が実現されていることが多い。CISOによる全権掌握がなくても、実際の情報システムやネットワークにかかわる現場のスタッフは、セキュリティー管理を日常的な業務として対応しなければならない状況に追い込まれている。このため、いろいろな事業部の現場担当同士で、あくまでも個人的な関係に立脚する相互協力体制ができあがっていることが多い。そこで、この相互協力体制を支援しながら全体のセキュリティー管理レベルを向上させていくこと、つまり「緩やかな連合軍構想」を実現していくことが、1つの方法となっていた。

このような体制がある組織は沢山あるが、うまく機能しているところは相互に経験をシェアする仕掛けができあがっている。たとえば、非公式ながらセキュリティー担当者同士の連絡会が定期的に開催されていたり、あるいは管理者同士のメーリングリストやWWWサイトが用意されて情報が積極的に共有されていたりする。セキュリティー管理者同士の情報流通を促進する基盤を作り出すことも「緩やかな連合軍構想」には不可欠だろう。セキュリティー関連の情報流通基盤の成立は、通常の組織でも重要である。

戦略4 セキュリティー関連の情報流通基盤は、組織体制にかかわらずにうまく作る。

資金と人材を確保するために

最近多くの組織で問題となるのは、セキュリティー対策の資金をどのように準備するのか、そして、セキュリティー管理に実際に携わる人をどのように確保するのかということだろう。これは真にCISOが統括すべき事項である。

まず資金に関しては、経営側はセキュリティー管理の重要性は理解していても、昨今の不況の影響であまり多くの資金を使うことには否定的なことが多い。セキュリティー管理をいくら強化しても新たな収入が得られるわけではなく、経営側としてはコスト上昇に直結する事項だという認識がある。しかし、真面目にセキュリティー管理を実施するためには新たな投資が必要となるのも事実である。

人材の問題も大きい。現在のセキュリティー管理は、アマチュアでは対応できなくなり始めている。特に情報処理システムへの業務の依存度の上昇は、トラブルを短時間に、かつ、影響範囲をできる限り小さく抑え込むことを要求するようになった。情報処理システムに大きな障害が発生すると、実際に経済的損失を組織に与えるからだ。このため、正しく設計されたトラブル即応体制と適切な技術の投入が必要となる。これは、セキュリティー管理がプロの仕事になり始めていることを意味する。ただし、セキュリティー管理のための人材は、利益を生み出すことはない。確率的に予測される損失やリスクを減らすことにしか貢献できないのだ。

資金と人材の問題については、「一度痛い目に合えば、セキュリティー管理に対する投資の大切さを心から理解するよ」と言う専門家もいる。しかし、「痛い目」が組織にとって教訓となり、大きな損失を与えないものである保証はどこにもない。この意味で「痛い目」を期待してはならない。

資金と人の問題を解決するためには、セキュリティー管理に対する継続的な投資が大切なことを経営側に理解させることが必須である。このためには、CISOはさまざまな手段をとる必要がある。たとえば、他の組織で発生したセキュリティートラブルをケーススタディーとして学び、その轍を二度と踏まないようにすることも効果的だろう。

なによりセキュリティー管理で実施すべきことを一覧にし、各項目に必要な費用と、同時に実施の優先度を示すことが必要不可欠である。CISOにとって、「私のセキュリティー対策一覧表」を作成して常に更新することが重要になる。最終的

には、一覧表を経営側に対して提示し、その妥当性を検討してもらうことも必要だろう。

いまや「セキュリティー対策は重要だ」という掛け声だけでは組織は動かない。合理性を持ったアプローチが必要となる。

戦略5 セキュリティー対策の検討では、コストと優先度を常に考える。

選択する技術についても考慮する

使用する技術について、どのような選択をするかもCISOは考えておかなければならない。

セキュリティー管理を考えると、さまざまな技術が必要となる。資金をかければかけるほど、いろいろなことができるようにもなる。たとえば、資金をかければ、組織構成員全員のシステムを改造し、誰が何をしているかをすべてモニターして記録するような環境だって構築できるのである。このような中で、CISOは技術投資に対する妥当性を常に考えなければならない。本当に守るべきことについて、明確な見識を持つことが必要なのだ。何を守るのか、誰から守るのかという視点が明確でないと、結局対策として妥当かどうかを判断できないので、思いつくものは何でもやってしまうことになり、結果として過剰な投資になってしまう。

戦略6 守るべきものは何かについて、常に明確な考え方を持つ。

原理主義者にはならない

CISOがしばしば陥ってしまう誤りは、セキュリティー管理のためには、ほかのことを犠牲にしてもいいという勘違いだろう。セキュリティー管理は何のために行うのかと言えば、本来組織が行う業務に対するリスクを減らすことであり、セキュリティー管理を目的化してはいけない。

セキュリティー管理のために多少の利便性を犠牲にすることは許容できるが、実際は業務にオーバーヘッドを加えていることにほかならない。つまり、業務のパフォーマンスを下げているのだ。セキュリティー管理のために業務を遅滞させることがまかり通るのであれば、セキュリティー管理を実施するグループはCISOも含めて組織の鼻つまみ者である。その意味で、セキュリティー管理が重要とはいえども、実際の現場の業務フローに対して大きく影響を与えたり、あるいは、業務推進を遅滞させたりするようなことを平気で行うCISOになってはならない。セキュリティー管理をするうえで、現場との折り合いをつけることも必要なのだ。

戦略7 セキュリティー管理は、金を生み出す業務に対するリスクを低下させるものなので、業務に不要なオーバーヘッドを与えるような情況は避ける。

さて、今回は組織内にセキュリティー管理体制を作り上げるときに、その司令官でもあるCISOがどのような考え方を持つべきかについて、私なりの考え方を述べた。特に、いくつかの肝心な項目については文中に「戦略」で示した。読者の多くは「いろいろ言っているけれども明確にどうしたらいいのかは何も言っていないじゃないか」と批判されるかもしれない。これは、各組織で行うセキュリティー管理の具体的な設計は、各組織で異なることにも起因する。

また、CISOは大変な作業をしなければならないポストだと思われたかもしれない。CISOが行わなければならないことは本当に沢山ある。しかしその多くは準備のプロセスに使われることであり、準備を定常的に実施する体制ができていれば、実はそんなに多くの仕事が目の前にいきなり積まれるわけではない。日頃の努力が大変さを減らすポイントだと考えるといいだろう。

［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