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の多くの場面で文書化が行われる。さらに、運用においては誰が何をしたのかという記録が大量に作られる。この文書化の作業における考え方、さらに蓄積される記録をどのように活用していくのかについての考え方をまとめる。

第三回

文書化して記録する

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

情報通信システムの管理に限らず、一般的にシステム管理作業では、そのシステムに関係する情報を十分に得て初めて管理作業を実施できる。システムの構成、現状、稼働状態、システムが抱える課題、担当者、開発者、開発記録、過去の運用記録といった、種々のシステムにかかわる情報を得て初めて管理作業として何をしたらいいかを考えられるだろうし、具体的な管理作業の計画立案にも着手できるというものだ。的外れな管理作業をいくらやっても、システムの運用に資するところはなく、お金と時間の無駄になってしまうだろう。的外れな管理作業を継続させていると、そのうち本当に必要となる作業に対してコストが負担されないことにもなり、最終的にはシステムの運用そのものを危機に直面させてしまうことにもなりかねない。

的確な作業を適正なタイミングとコストで行うことこそ、管理作業を設計・実行していくときに求められることであり、そのためには対象となるシステムについて正しい理解ができるための情報を得ることが必須である。これはセキュリティー管理作業においても違いがあるわけではない。セキュリティー管理を遂行するうえで、管理に資する情報の集積は必須である。

一方、具体的にセキュリティー管理に資する情報とはどのような情報なのかを考え出すと、その実態、つまりセキュリティー管理を行って何を達成しようとしているかによって、必要となる情報は大きく変化する。たとえば組織内の情報流通管理と情報漏洩防止がセキュリティー管理の目標である場合と、外部にサービスを提供しているネットワークサーバーにおける不正アクセス排除が目標になっている場合では、必要となる情報の種類が大きく異なることは読者の皆さんにも直感的に理解していただけると思う。このようなことから、セキュリティー管理を行う場合に、何を目標として、どのようなことを行おうとするのかを明らかにしておくこと、つまりセキュリティーポリシーの策定が重要になる。

共通認識を形成するのが目的

ところで、「セキュリティーポリシーの策定は、組織におけるセキュリティー管理の憲法を作ることなのです」という難解な説明をするセキュリティーコンサルタントがいるが、セキュリティーポリシーの策定をそんなに難しく言う必要はない。何のためにセキュリティー管理をするのか、目標はなんであるのか、誰が具体的にセキュリティー管理をするのか、といったことを記述することである。そしてセキュリティー管理を、誰もがわかるように5W1Hの視点で書き下すことである。これにより、セキュリティー管理作業を具体的に設計していくために必要な共通認識を形成できるのだ。この共通認識を基盤として、セキュリティー管理のためにどんな情報を集めるのか、どのような情報を捨てられないように運用者に保管を強制するのか、具体的な管理作業として何を誰が行うのか、といったブレイクダウンした設計に進めることができるようになる。

戦略1 セキュリティーポリシーは、「セキュリティー管理について共通認識を形成するために策定する」ことを全員が理解していることがもっとも重要なことだ。

静的情報は文書化でまとめる

さてセキュリティー管理で必要となる

情報に話を戻そう。必要となる情報には一度情報として取りまとめるとその後の更新頻度が比較的低い、言うなれば静的な情報が存在する。その代表例として、現在使用しているシステムとネットワークについての構成情報が挙げられる。ネットワークはどのように敷設されているのか、どのようなネットワーク機器が使われているのか、どのような設定が行われているのか、接続されているシステムには何があるのか、各システムの運用責任者は誰か、といった情報が必須となる。この種の情報は、所定の手続きの中で収集され、文書として作成されていることが多い。つまり、静的な情報を効率よく集めるためには、文書化という制度設計をうまく行うことが必要になる。

文書化の考え方として、まったく性格の異なる2つのアプローチが存在する。1つは、最終的な結果だけを文書にしてまとめるという考え方であり、もう1つが結果だけでなく結果に至るプロセスも記述するという考え方である。たとえば、会議を行ったときの議事録の作り方を考えてみればこの2つの違いがよくわかると思う。前者の方針であれば会議で決定された事項を書き下すことになり、後者の方針であればなぜそのような結論を導いたのか、そしてそのときに出された意見は何であったのかをも記述するのである。セキュリティー管理に使われる情報のうち、更新頻度の少ない静的な情報では、実は手間はかかるが後者の方針で取りまとめられた情報のほうが役立つことが多い。ネットワーク構成情報であっても、なぜこのような設計が行われたのか、なぜ改修が行われたのか、そのようなプロセスについての情報も併せて記録されていることが望まれる。よくネットワーク管理をしているときに、あるIPアドレスのブロックが特定の人に割り当てられているのに、その割り当てが何のために行われたのかがわからないことで、管理責任が曖昧になることがある。しかし、おそらく意思決定をしたときには何らかの理由や目的があって対応したに違いない。このような背景情報が記録されているだけで、将来的な手助けになることが多い。

戦略2 文書化によって作成される情報では、その背景情報を併せて記録するようにすると、セキュリティー管理では役立つ。特に、改変・改修・変更を加えたときには、「なぜ改変を行ったのか」がわかるような情報があると大助かりである。

情報の新鮮さを保つこと

もう1つが、情報の保管や更新などの情報の運用にかかわるコストは、セキュリティー管理を行う側が最終的に負担する構造を持たなければならないことを意識することだ。いろいろな組織のセキュリティー管理の実態を見てきて思うのは、セキュリティー管理に着手したときには、セキュリティー管理グループだけではなく、ほかの多くの人もそれに賛同して力を合わせて作業をし、結果として豊かな情報を蓄積できている。しかし、運用を行っていく中で、その熱意が冷めてくると情報の更新が行われなくなってきて、結果としてセキュリティー管理グループが持っている情報は古いままになっているということが散見される。情報を必要としている人が、その情報の新鮮さを保つ仕掛けをうまく考えてやらないと、なかなか情報を最新に保つのは難しい。どんなにルールを作ろうが、結局他人事と考えてしまう状況にあれば、情報更新は放置されることが多いのだ。その意味で、情報更新を何らかの別のメカニズムと同期させて行うようなことも考えるべきである。たとえば、商店では月末に定期的に棚卸をして在庫を確認するが、運用しているシステムについての情報の更新でも、この棚卸のようなメカニズムを作ることが重要だと考えている。四半期に一度、必ず資産チェックと同じタイミングでネットワーク構成を確認するとか、コンピュータの保有状況を確認するとか、そのような工夫をしながら情報更新機構を作り上げる努力が必要だろう。

この工夫を凝らす中で、情報システム、特にデータベースの利用をうまく行うことが鍵になることも多い。実はセキュリティー管理のために必要となる情報が、他の目的で作り出されていることも多い。アカウント情報については組織構成員のデータベースと連携させることで二重の情報収集の必要がなくなり、どれだけのコンピュータを管理対象にしなければならないかという問題は、資産台帳と同時に新たな情報処理機器の発注台帳などのデータベースを組み合わせれば母集団をリスト化できるというようなことがある。また、建物の工事図面や内装図面などの情報が蓄積されているのであれば、それにネットワークの構成を埋め込むことで有意義な情報を作り出せるだろう。既存の情報資産の再利用という視点で、セキュリティー管理に資する情報の確保と運用も当然考えるべきである。

戦略3 セキュリティー管理に既存の情報資産を活用することも、当然検討に値する作戦である。

動的情報は運用で集められる

一方、システムの運用状況にかかわる情報は、動的な情報の典型的なものである。たとえば、今日の午前10時にシステムを利用していたユーザーは誰であるのかを調べたいというようなことは、セキュリティー管理でしばしば発生する。このような管理作業を支える情報は、運用の中で、特にシステム運用ログとして生まれてくるのが普通だ。その意味で、セキュリティー管理でログ管理の重要性がよく取り上げられているのである。

ログ管理で、どのようなログを収集して蓄積するのがいいのかは、セキュリテ

ィー管理を設計するうえで決められるというのが教科書的な言い方だろう。しかし、本当に必要なことは、収集しているログを解析すると、あるシステムで、あるいは、ある特定のサービスで、そのときに何が起きたかを合理的に判断できるように十分なログを残しておくという考え方だ。

トラブルが発生したときに、一般のユーザーは「システムがおかしくなった」という反応をすることが大部分である。システム運用管理者にとっては、「おかしくなった」というのは、一体どういう状態になったのかを判断しなければならない。そして、セキュリティー管理では、さらに、なぜそのような状態になってしまったのかという原因までを追求することになる。この意味で、セキュリティー管理で必要となる情報は、単純なシステム運用管理で必要になる情報よりも、より多くの種類、より詳細な情報を得なければならないことになる。

セキュリティー管理をしていると、トラブル発生時にシステムに何が起きて、何が起きなかったのかをはっきりさせることが重要だということがわかってくる。たとえば、OSがクラッシュして停止したときに、事故なのか意図的に行われたことなのかを判断しなければならないし、その原因も見つけなければならない。確かにトラブルが発生したが、悪いことは起きていないという確認もしなければならない。悪いことが起きているのであれば、なぜそのような事件が引き起こされたのか、誰がやったのかというところまで追求し始めることになる。ここまで深く状況を把握するために必要な情報を得ておく必要があるのだ。

戦略4 ログは、何かが起こったときの状況を再現するために記録する。したがって、通常のシステム運用管理で必要となるログよりも詳細な情報が必要になることが多いことを理解すべきだ。システム標準のログは、比較的役立たないことも多い。

どこまで記録するのか

このため、セキュリティー管理を意識すると、なんでもログに残したくなるのは当然のことと言えよう。しかし、ログを蓄積する記憶媒体の限界や、あるいは、運用上の機密保持ルール、場合によってはプライバシーの問題を考慮すると、なんでもログに残すことは不可能である。このため、セキュリティー管理の方針によって、ログを残す精密さに差をつけることが必要になる。この差のつけ方がセキュリティー管理の難しさであり、腕の見せ所であるとも言える。

注意しなければならないのは、ログはあくまでも記録であり、その記録が正しいかどうかは記録作成メカニズムに大きく依存する。たとえば、侵入検知装置(IDS)を使っていると痛感するが、通常のネットワークアクセスを誤認して侵入を試みているアクセスだと報告することが多い。IDSが生成するログ1つを見て、これが誤認したケースなのか、あるいは本当に侵入を検知したのかを判断するためには、実は異なる別のセンサーなりログなりから判断することが必要になる。つまり、1つのログだけに依存するような記録の取り方は、しばしばログとして役立たない状況を生み出すことがあることを理解し、ログの中味についてクロスチェックができる環境を作っておくことが必要となるのだ。

戦略5 1つのログを盲信しない。かならずログに記録されている事項が正しいかどうかをクロスチェックできる環境を作っておかなければならない。

解析ツールは事前に作成する

ログについて重要なことは、ログを解析するツールは必ず事前に作っておき、そのツールを日常的に利用する体制を構築しておくことである。

そして、ログ解析に使われるツールが生成する情報しか、セキュリティー管理に使えないことも認識しておこう。トラブルが起きてからログ解析を行うと、解析ツールが出力する結果がまったく使い物にならないことを発見して愕然とすることがあったというシステム管理者の武勇伝を話題にすることが多い。これは道具を用意しておいても、日頃使っていないと、その道具が何に使えるかを正しく把握できないからだ。使い方を正しくわかっていてこそ、役立つ道具といえる。

解析ツールを日頃から使っておくことが重要なのは、システムのマイナーチェンジでログの構造がしばしば変わることがあることだ。たとえば、OSにパッチを適用したときに、OSが生成する各種ログの書式が変わったり、あるいは、ログに書かれる情報の表現形式が変わったりすることがある。これによって、ログ解析ツールがうまく機能しないことも実際に頻発する。解析ツールを日頃使っていると、不具合は即座に発見できる。しかし、トラブルが発生したときになって初めて解析ツールが使い物にならないことがわかるのは、不幸というよりも壊滅的な状況に自分自身を追い込んでいるとしか言いようがない。その意味で、日常的に解析ツールを使い、その適用性を確認しておくことも重要だ。

戦略6 ログ解析ツールは事前に準備し、日常的に使いこなしておくことが重要である。

手引書とは何か

セキュリティー管理で重要な文書化作業に手引書を作ることがある。これは、トラブルが発生したときに、そのトラブルにどのように対応したらよいかを書き下したような対応マニュアルや、あるいは、部署で何らかの意思決定をするときにセキュリティーをどのように考えたらよいのかというようなガイドラインが含まれる。

まずガイドライン作りは、これはセキュリティーポリシーの策定とセットで実施すべきものである。しかし、ポリシーとは異なってガイドラインの役割は、それぞれの状況や部局などの具体的な想定を行って、そこでセキュリティーポリシーに従って行動をするためにどうしたらいいかという具体的な指針を与えることである。この意味で、実務に役立つものが作られなければならない。ガイドラインは、どうしてもその対象となる領域の当事者と一緒になって策定することが必要となる。この意味で、セキュリティー管理担当者は、その当事者に対するコンサルタントとして機能することになる。当事者と一緒になって作業を進めていくとどうしても「現場の都合」という理由でポリシー違反を意図的に行ってしまうことが多々発生することだ。ここで重要なのは、このポリシー違反をいかに防ぎ、かつ、現場が困らないようにするかのソリューションをコンサルタントとして提供することである。このソリューションを提供しないで教条的にポリシー遵守ばかりを言うセキュリティー管理者が最近多いので「セキュリティー原理主義者」と陰口をたたかれることも多くなっている。このような知恵のない対応はセキュリティー管理に対して反感を持たせるだけではなく、実際のシステム利用者におけるモラルハザードを引き起こすことにもなる。その意味で、知恵ある対応が必要になる。

戦略7 ガイドライン作りは、当事者たちと一緒に作成することが必須だが、そこでポリシーと現場の両方を成立させるソリューションを提供することがセキュリティー管理者の役割である。セキュリティー原理主義者になってはいけない。

対応マニュアル作りは必須

重要な手引書である「トラブル発生時の対応マニュアル」作りは、多くの組織で必要性が認識されているにもかかわらず、その実施が遅れているものである。単純なシステムトラブルに対する対応マニュアルは用意されていることが多いが、地震や水害、火災などの災害や、サービス妨害攻撃（DoS攻撃）が行われた場合の対応、情報漏洩が発生した場合の対応など、さまざまな状況での対応マニュアルが作られるべきである。この対応マニュアル作りは、どうしても後手に回ることが多いが、実際にはこの手のマニュアルが充実している組織ほど、実際のトラブルからの立ち直りが早いという調査結果もある。

対応マニュアル作りは、実は自分たちが行っているビジネスにとって何が重要なのかという優先順位付けを行う解析能力と、どのようなリスクが発生しうるかという想像力に裏打ちされる作業であり、十分な対応マニュアル作りが行われるところには、実際には豊かな判断力を持ったマネージメントが存在していると言える。

対応マニュアル作りは、セキュリティー管理を組み立てていく段階での仔細な検討を行う訓練として、また、対応マニュアルの有効性を確保するための練習として取り組んでいくのがいいアプローチだと考えている。そして、実際に役立つ対応マニュアルを作り出すことで、いざというときに役立つものがあるということにもなるだろう。

セキュリティー管理の多くの部分が実は準備作業に費やされるわけで、「備えあれば憂いなし」という言葉がぴったりと当てはまるものである。その「備え」を考え、点検することが、対応マニュアル作りというプロセスの中で、あるいは、対応マニュアルの点検・更新という作業の中で行われるとも言えよう。その意味で、対応マニュアル作りに真剣に取り組み、それを活用していくこともCISOは十分に考えなければならない。

［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