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を考えるときに、常に頭を悩ます要素は組織に属する人間そのものである。技術を用いて構築したシステムは、基本的には設計通りに機能する。しかし、不確定要素を常に抱えるものは人間そのものである。セキュリティー管理において人間とどう対峙していくのか、内部犯行をいかに押さえ込むか。

第六回

他人は常に敵なり

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

どんなにいろいろなことを考えてシステムを作っても、トラブルの発生を100パーセントなくすことはできない。システムは必ずトラブルを引き起こすのだ。そこで、システム管理を考えるうえではトラブルの発生の可能性をどのようにして下げるかを考え、それを実行する。単体のシステムが故障しやすいのであればバックアップシステムを導入するだろうし、システムの運用が3年以上になるとシステムの故障率が上がることが経験的にわかっているならば、3年未満でシステムを更新することも考えられるだろう。つまり、システム設計とシステム管理を考える場合には、いろいろな手段を使って、システムがトラブルを引き起こす確率を下げることを目標にするのだ。セキュリティーシステムの設計やセキュリティー管理の組み立てでは、リスクの評価から始め、高い確度のリスクを減少させるために必要な投資をすることが、どんな教科書やガイドブックにも書かれている。

ところが、セキュリティー管理を考えるうえでどうしても避けて通れないのが、システムにかかわる「人間」をどのように考えるかである。具体的にはシステムを日常的に使用するユーザーやシステム管理者についてである。人間は思いもよらない間違いを犯す存在である。システムにとっては最も不確定要素を持った関係者と言ってもいいだろう。そして経験上この不確定要素が大きなトラブルを誘発する一番の原因になっている。このため、人間という不確定要素をセキュリティー管理の設計でどのように捉えるかは大きな問題である。

権限管理の限界

システムにおける人間の扱い方については、いろいろな方法がある。

1つの方法は、各ユーザーに対して過不足のない適切なアクセス権限を与え、業務上必要十分な環境を提供し、同時に、業務に関係のない余分なことができる限りできないようにしてしまう考え方だろう。各ユーザーの動きを狭い枠の中に入れてしまおうという考え方だ。

たとえば、通常のユーザーに対してウィンドウズのシステムを割り当て、管理者権限をユーザーに渡す運用は最近では皆無だ。代わりに、各システムのソフトウェア管理は管理者が徹底して行い、さらにユーザーにはそれぞれ独自のユーザーアカウントを設定して、システムに対してアクセスできる範囲を限定する。ソフトウェアのバージョンアップやセキュリティーパッチの適用は管理者が行う。ユーザーは決められたアプリケーションと決められたディスク領域だけを限定的に使って業務をこなしていくという方法だ。さらに最近では、WWWだけをユーザーインターフェイスにすることで、定型業務に携わるユーザーに対して、より一層権限を制限した環境を作り上げて提供する企業も増えている。また、UNIXシステムであれば、グループを適切に設定してファイルアクセスに対してきめ細かな設定をしたり、アクセスできるアプリケーションをうまく制限したりすることが一般的に行われている。このような権限のきめ細かな設定により、ユーザーが本来アクセスする必要のないファイルやアプリケーション、サービスに触れることがないようにしてトラブルを防ぐ方法がある。

この方法は、一般ユーザーがトラブルを引き起こすことを防ぐという面で効果が高い。また、現在の大抵のOSでは、

この方法を実施するに十分な機能を持っており、導入しやすい。また、方法そのものの汎用性も高く、多くの環境に適用できる。しかし、限界もある。十分な権限を持ったユーザーが不注意によるトラブルを引き起こすことをこの方法では阻止できない。たとえば、管理者権限を持ったユーザーが間違えてシステムファイルを消してしまうことは阻止できない。

フェールセーフを導入する

そこで、正当な権限を持ったユーザーが間違えて何かをしてしまったときに、その間違いが致命的にならないようにするメカニズムや取り扱い手順を考えるようになった。これがフェールセーフの考え方である。最近の言葉で言えば、contingency planningと言ってもいいだろう。

権限管理の考え方は、システム運用の基盤を強化するという考え方に基づいているといってもいい。つまり、システムを準備する段階で設計し、適切に運用していくことが求められている。一方、フェールセーフの考え方は、どちらかというと事後対応のメカニズムと考えてしまってもいい。

たとえば、先に例示した管理者が誤ってシステムファイルを消してしまおうとしている状況を考えよう。行為者は管理者であるから、権限管理では対応できないトラブルである。このため、何もしていなければファイルは消えてしまう。

このような状況に対応するためのフェールセーフの構造は何通りも考えられる。たとえば、システム管理者が誤ってシステムの重要ファイルを消すことを防ぐためのツールを仕掛けておいて、ファイルの消去を防ぐという方法もあるだろう。さらに、不幸にもファイルを消してしまい、システムが機能しなくなったときのことを考えてシステムのバックアップを常に確保するようにすることも可能だろう。

戦略1 セキュリティー管理ではトラブルの発生を減らす対応とトラブルが発生してしまってもシステムが機能するようにする対応の両方を入念に考えて実行することが必要。

内部犯行の阻止は難しい

権限管理やフェールセーフの考え方を取り入れたとしても、まだまだ対応できない状況がある。それは内部の人間が意図的にシステム破壊やサービス停止を狙って行動した場合である。システムに直接アクセスできる内部の人間が意図的にシステムにトラブルを引き起こそうとした場合にこれを防ぐのはとてつもなく難しい。

たとえば、システム管理者が悪意を持ってシステムを壊そうとした場合を考えてみよう。悪意を持ったシステム管理者がデータベースや個人のファイルを消してしまったり、ウイルスをばら撒いたり、システムを物理的に壊してしまったりしたらと考えてみればわかりやすい。この場合、普通のシステム管理を行っていただけでは、恐らくシステムの破壊を完全に免れる方法はないだろう。この意味で、内部犯行の阻止は難しいと言わざるを得ない。

もちろん、システム管理、セキュリティー管理をよく設計して稼働させることで、内部犯行の発生を抑える効果、いわゆる抑止力は高まる。実際にシステムやサービスを破壊することが難しいとわかっているならば、本気で実行しようとする人はなかなか出てこないだろう。また、入念なセキュリティー管理の実施によって、システム上で誰が何をしているのかを管理側が的確に漏れなく把握しており、同時にそのような管理体制を敷いていることが内部の人間に周知されているとすれば、意図的にトラブルを引き起そうとする人のやる気をそぐことにつながるだろう。しかしそれでも内部からシステムを壊してやろうとする内部犯行者は登場してしまうかもしれない。このため、内部犯行を引き起こさせないために、技術だけに頼らないさまざまな取り組みが必要になる。以前にも述べたが、服務規程、セキュリティーポリシーに基づいた厳格な手続きの策定と実施、監査の強化と定期的な実施などが必要になる。

戦略2 内部犯行の阻止には十分なセキュリティー管理を行い、それを抑止力とすることが基礎となる。そして、その抑止力を強化するルールや手続きをうまく作ることが必要。

性善説と性悪説

内部犯行までを含めたセキュリティー管理の議論をすると、システム設計の基本的な考え方として、システムにかかわる誰もがシステムに対して悪いことをするかもしれないということを前提にしたセキュリティー管理設計が必要だということに気付く。しかし、そのことがそのまま内部の人間は皆「悪い奴」だという前提でシステムを作らなければならないことには直結しない。この問題を考えるうえで参考になるのが、企業での電子メールの使い方についてのルールだろう。

ネットワークを基盤とした企業の情報化が重要であると声高に叫ばれた1990年代中盤では、電子メールは業務効率化に大きく寄与するとして誰もが絶賛した。すなわち電子メールは企業内外の通信のオーバーヘッドを激減させ、円滑な情報交換を促進させる、組織構造にとらわれない意見交換が可能になるといったさまざまな効能が語られ、積極的に導入された。

一方で2000年頃からは、電子メールは情報漏洩の主なルートになっているとか、電子メールは業務以外の目的で広く使われているため実は経費食いだというような電子メール有害論がメディアでも取り上げられ始めた。この影響なのか、国内においても、やり取りされる電子メールをすべて記録し、その内容を検査することを実施する企業が増えている。また、滑

稽なことに社員に自由に電子メールを使わせていたことが問題であるとして電子メールの発信には上司の許可を得なければいけないというルールを導入した企業も登場している。

この変化を見ると、最初は「ユーザーは悪いことをしないだろう」という前提で電子メールのシステムを組み立てていたものが、ある時から「ユーザーは電子メールを使って悪いことをするかもしれない」に180度変化したという解釈ができる。性善説から性悪説への基礎変更である。セキュリティー管理の基礎的な考え方を性善説から性悪説に変更する場合、変更それ自体は悪いことではないが、鍵となるのはそのことをユーザーやシステムにかかわる人にどのように理解してもらうかだ。

根源的な理解が必須

私たちは高いモラルを持っているとなかなか悪いことはしないものだ。高いモラルを維持できる環境を作り出していくことがどんな組織においても運営上重要な視点であるだろう。そして、私たちが高いモラルを維持することに力になるのは、他者からの依存感、使命感、達成感だろう。他の人から頼られ信頼されていると実感しているならば、その感覚は高いモラルを維持する力となる。自分自身が行っていることの重要性を理解することで得られる使命感や、行ったことに対して高い評価を得られたと納得する達成感なども、高いモラルを維持する力となる。

性善説に基づくシステム設計は当然のことながら各ユーザーは悪いことをしないという前提から作られているから、悪いことをするかどうかは各ユーザーに委ねられてしまっている。これはセキュリティー管理の面から考えれば当然改善が必要だ。しかし、そこでシステム設計の前提を性悪説に基づくものとして、いきなり「ユーザーは悪いことをするだろうから、監視システムを導入することにした」と言ったらユーザーの共感を得られるだろうか。

仮に性悪説に基づいたシステム設計をしたとしても、システムにかかわる人が仮想敵として扱っているのだということを真正面から伝えられて、それを納得できるだけの強い心を持った人は少ない。そして、そのことを真正直にユーザーに伝えたとしたら、それはモラルハザードの引き金にしかならないだろう。

恐らく性悪説に基づいたシステム設計をしたとしても、その説明は手抜きをせずに行い、同時にそのシステムを使うことの意味や効能を理解してもらい、さらにはそのシステムの応援者になってもらわなければ困るのだ。つまり、セキュリティーシステムは役に立つと心から思ってもらわなければならないのだ。

これを実現するためには、システムにかかわる人たちに問題の本質とその問題を解決するための取り組みについて根本から理解してもらうことが必須である。先の電子メールの例で言えば、組織において情報漏洩が発生することは大きな問題であることは誰もが理解するところだろう。そして、情報漏洩を阻止するために何らかの措置が必要であることも誰もが理解するところだと思う。問題の根源的なことは誰もが理解できる。

合理的な方法を追い求める

そしてさらに重要なのは問題解決に使われる方法が合理性を感じられるものになっていることだろう。先の電子メールの例で言えば、情報漏洩を防ぐためにすべてのメールを検査することを逆に「検閲」とユーザーに認識されてしまったら、このメカニズムはうまくいかない。さらには、上司の許可を必要とする電子メールのシステムがエンドユーザーに対する信頼の欠如だと思われてしまったら、モラルハザードを引き起こすには十分な理由を与えることになる。

頭で問題を理解していても、その解決方法がユーザーにとって合理性が感じられなければ、そこには胡散臭いものを感じ、さらには、疑念を持ち続けることになってしまう。疑いこそが実はモラルを下げる大きな力になる。この意味で問題の理解も重要であり、さらに合理的な方法を提供していくことも重要だ。

戦略3 ユーザーに問題の本質的理解と合理的な解決方法の提示をしなければならない。理解と合理性がモラルを下げない重要な要素となる。

賢いユーザーは管理者を助ける

さらに重要なことは、性善説と性悪説の差は性悪説に基づくシステムのほうが手間とコストがかかるということだ。どのユーザーももしかしたら悪いことをするかもしれないという前提でシステムを構築することは、セキュリティー管理上強靭なシステムを構築することになるが、同時にきめ細かな権限管理とともに、さまざまな可能性を汲んだフェールセーフの構造を組み立てなければならないために、必然的にコストは上昇するのだ。

このコストを圧縮する方法としては、管理者サイドが信頼できるユーザーを増やしていくことである。もしも信頼できるユーザーであれば、最低限のフェールセーフ機能は必要となるだろうが、そのユーザーが何か悪いことをするかもしれないという前提でのシステムを組み込む必要はなくなる。

信頼できるユーザーを増やすためには、ユーザーに対する教育と啓発の機会を増やし、ユーザーが正しい認識を持って行動することを促す継続的な取り組みが必須だ。また、システム管理者との間でのコミュニケーションが円滑に行われる基盤を作り出すことが重要である。たとえば、ウイルス対策でも、ユーザーから管理者が信頼されていて、何か変なことがあればすぐに報告が寄せられて対応できる環境と、ユーザーが管理者を信頼し

ていなくて自分が使っているシステムがおかしくなっていても「なにか管理者がまた作業をしているんだろう」と放置されてしまう環境と、どちらが管理者にとって手間がかからない環境だろうか。また、どちらがトラブルを未然に防ぐ、あるいは、トラブルの拡散を防止する環境だろうか。

つまり、信頼できるユーザーを増やし、さらにユーザーとの間で相互信頼と円滑なコミュニケーションができる体制が確立していることが、実はセキュリティー管理コストを低減させながらトラブルの発生を強く抑止することが可能になるのだ。一言で表せば、賢いユーザーは管理者を助けてくれるのだ。

戦略4 念には念を入れてトラブルに強いシステムを作ることは重要だ。しかしそれ以上に賢いユーザーを育てていくことが管理コストを低減させ、同時にトラブルの発生を強く抑止する環境をつくることにつながる。

「嘘」と「秘密」には覚悟を

セキュリティー管理者にとっての甘い誘惑は「嘘」と「秘密」である。

ユーザーには正論を述べ、あたかも合理的な管理を行っているかのような印象を与える情報をインプットしていて、その裏で実はもっとあくどいことをしているような状況を考えてみよう。電子メールの例で言えば、「さまざまなトラブル防止のために、わが社から発信される電子メールは念のために記録する」という言い方でユーザーを納得させているとして、その裏ですべてのメールを検査しているようなことを考えてみればよい。確かに、このような「嘘」をつくことは簡単だし、魅力的な役に立つ「嘘」に見えるかもしれない。しかし、どんな嘘でもバレれば不信感を強烈に増大させることにしかならない。特に管理者の嘘は、ユーザーに対して大きく不信感を持たせてしまう。

ではバレないようにすればいいのか――つまり、管理側に「秘密」を持つことがいいことなのだろか。電子メールの検閲も管理グループの中で秘密にしてしまい、一般ユーザーには教えないようにしてしまえば嘘も本当になる。これも管理者から見れば魅力的な方法かもしれない。しかし、秘密裏に何らかの処理を行うことは、実行したことに対して客観的な評価を与える機会を大きく減らし、さらにその実行によってトラブルを引き起こしたときには、そのトラブルまでも秘密にするという何重もの秘密の上塗りに通じる。結局のところ、説明責任を果たせない状況を生み出すことにもなり、結果としてユーザーの信頼感を損なうことにもなりかねない。

この意味で、嘘と秘密は管理者にとって魅力的な方法に見えるかもしれないが、実際にはその方法を採用するのであれば、相当覚悟を決めて始めるべきだ。セキュリティー管理を行う場合には、秘密を持つことは必要になることがある。したがって、秘密を持つことを否定する気はない。また、秘密を持つことで、どうしても嘘をつかなくてはならないこともあるのだ。しかし、それによってセキュリティー管理全体の信頼感、合理性、運用性を損なうことがあってはならない。その意味での抑制は必要なる。

人間の問題は一筋縄ではいかない

今回は、セキュリティー管理における「人間」の問題を取り上げてみた。特に最近、性悪説に基づいたセキュリティーシステムの一般化が声高に言われるようになっているが、それほど簡単にシステムが構築できるものではない。性悪説に基づいてシステムを作るのであれば、より一層のユーザーからの信頼獲得と、ユーザーの高いモラル維持に対して努力が必要となる。何重もの予防をすることでトラブルから巧みに逃れ、同時に賢いユーザーを増やすことで無用なコストアップを避ける。そのような目標でシステム設計を頑張ってもらいたいものだ。

［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