CISO STRATEGY

企業のリスクをマネージする戦略考

企業が業務のためのシステムを構築する以上、セキュリティー対策の多くも技術を使ってシステムを構築する。その際に業務上の利便性を犠牲にすることはできない。では、実際にセキュリティーシステムを構築するときの構成、あるいは、使用する技術の取捨選択の判断はどのように行うのか。

第五回 システム構築の表と裏

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

企業などの組織で情報処理システムやネットワークを構築する目的は、企業活動の効率化を推進し、より短時間により多くの利益を上げる基盤を作ることにある。このため、システム構築には無尽蔵に資源（資金や人材など）が投入されることはなく、できる限り必要最小限にとどめようとする力が常に働くことになる。最小の投資で最大の効果を狙うのは、経営者の常である。このため情報システムに対する投資プランが現場から提示されたときには、無駄な投資が含まれていないか、投資に対してどれだけ収益アップが期待できるか、投資量を変化させると収益がどれだけ変動すると考えているかといった面を入念に吟味し、経営者として納得できる投資プランになるようにするのが普通だ。

ところが、セキュリティーシステムに対する投資を考えると、その投資は基本的には利益を生みださない。セキュリティーシステムに対する投資は、将来発生するかもしれない損害を低く抑えるための予防的な投資である。このため、妥当な投資量はどれだけかを突き詰めると、どうしても「本当に必要な投資なのか？」という疑問を心に抱え続けてしまう傾向がある。巨額を投じなくても問題は発生しないのではないか、現場から提示されているリスクは本当に大きなものなのか、投資は今でなくても大丈夫ではないか、そんなことを考えてしまうのだ。

しかし、冷静に考えれば、この状況はおかしなものだ。利益を生む投資の場合、そこで議論される「利益」はあくまでも予測に基づく未実現利益であり、実際に投資をしたとしても期待されただけの利益を生みださないことはいくらでもある。セキュリティーシステムへの投資も、予測に基づく未実現損失なので、利益を生む投資の議論と構造的にはまったく同じである。しかし、単に利益を生まないという一点で、経営者からはひどく冷たく扱われてしまっている。

結局、経営者がどれだけの見識を持ち、どれだけ大胆でどれだけ臆病なのかという点にセキュリティーに対する投資が委ねられている現状を改善しない限り、セキュリティーシステムに対する投資が妥当に行われることはない。この意味で、経営者に正しいマインドを持ってもらうことが重要になっているのだ。しかも、そのマインドの持たせ方は、合理性に満ちた説明に基づいていなければ意味がない。「セキュリティー屋は狼少年みたいなものだ」と言い放つ経営者はいまだに多数存在する。「危ないばかりを強調して、本当に危ないことはなかったじゃないか」と。そのようなマインドを持たせるのではなく、「いろいろ手を打ってきたから何もなかった今日があるのだ」という意識を持たせることが必要だ。何も悪いことが起きなかったのは、何もしなかったからではなく、いろいろと対策を施してきてやっと何も悪いことが発生しない状態が維持されているのだという意識を持たせることが重要である。

戦略1 経営者にセキュリティー投資についての妥当性を理解してもらい、高いマインドを持ってもらうことが必要。そのために、経営者に対する啓発活動と合理的な説明を行うことは大きな意味がある。

想像力と前提条件が大事

セキュリティーシステムを設計するときに、設計する技術者に求められるものは想像力である。対策しなければならない

リスクは何か。実際そのリスクが顕在化したときには、何が起こるか。トラブルが発生したときの影響範囲はどこまでか。どれだけの損害を組織に与えるか。組織が直面するかもしれないトラブルに対して、いろいろな角度から検討することが必要となる以上、技術者は豊かな想像力を持たなければならない。

とはいえ技術者の想像力だけを頼りにすることは危険なので、これまでの知識を集約したさまざまなリスクアセスメントの手法を適用し、もれなく検討することも必要となる。

もっとも問題なのは、問題に気付いていながら、その問題に目を閉じてしまう状態を技術者本人が生み出してしまうことだ。たとえば、組織内部の人間は悪いことをしないという、性善説に基づく仮定を置く場合がその典型例と言える。システム設計に必要となるリスクアセスメントでは、勝手な前提を置くことで、問題に目をつぶることをしてはならない。仮に目をつぶったとしても、目をつぶったことそのものを意識下にとめておかなければならない。具体的には、システム設計の前提条件という形で、記録に残す。そして常に、前提条件を再検討するときに議論しなおせるようにしておくことが必要だ。

Border Protectionの限界

技術者が目をつぶってしまったことで、最近大きな問題になっていることがある。その典型例がBorder Protectionの限界が露呈してきていることだ。

Border Protectionとは、一言で言えば組織と外部との境界面にセキュリティー機能を強化集約して、システム全体を守る考え方である。ファイアーウォールは、この考え方に基づいたシステムだ。Border Protectionは、悪いことは外部からやってくる、外との境界を強固な守りで固めれば、悪いことは内部にはやってこないという考え方に基づいている。たしかに、1990年代後半まではその考え方でも多くのシステムが守れたし、現在でも効果を発揮しているのも事実だ。しかし、それだけでは十分ではないこともわかり始めている。

たとえば、近年大流行をしているネットワーク伝播型ウイルスは、さまざまな経路から感染を引き起こす。大部分のケースでは、他の組織が感染して、インターネット経由で感染が伝播するというもので、この場合にはBorder Protectionは有効に機能する。

しかし、CodeRed、Nimda、SQLslammerの場合には、不幸にも個人的に使用しているラップトップPCが感染し、それを組織内部に接続した途端に、組織内部から感染が急速に広がった状態が、多くの組織で見られた。つまりBorder Protectionのみに頼っていると、いったん内部に問題が持ち込まれると、脆弱な部分が多数あることから、防御が難しいことが明らかになってしまったのだ。

しかし、この問題は、セキュリティー技術者にはかなり以前から認識されていた。トラブルの原因が内部にある場合には、Border Protectionだけでは問題解決につながらないことは、誰もがわかっていたことだ。

結局、これまで目をつぶってきた、内部にトラブルの原因が持ち込まれた場合、あるいは内部の人間によってトラブルが引き起こされた場合の対策が必要になっている。個々のシステムにおけるセキュリティー対策の徹底、さらには内部の人間がトラブルを引き起こすことを前提にしたセキュリティーシステムの構築が必要になっている。この投資だけでも、Border Protectionだけを考えてきた組織にとっては頭の痛い問題であろう。1か所に投資すればよかったのが、すべての情報処理機器に対策が必要で、さらにより多くの投資が必要になるかもしれないのだ。その意味で、目をつぶったことが今になって大きな反動となってしまっている。

戦略2 システム設計の前提条件は必ず明確にしておき、機会があるたびにその前提条件の妥当性を再検討することが必要となる。

守るべきものは何か

もう1つ、システム設計をするときに忘れてはならないのは、何を守るのかという議論だ。

セキュリティー対策をする場合に、まず定番のシステムを構築し、それで思考が停止してしまうケースをよく見かける。たとえば、外部との接続点でファイアーウォールとIDSを仕掛け、各システムにウイルス対策ソフトウェアを導入させ、定期的にソフトウェアを更新する設定をして、それでセキュリティー対策は完了というものである。本当にそれで十分なのか。

たしかに定番システムを導入することは悪い考えではない。すでに実効性があるシステムを導入することであり、投資を考えた場合には合理性が高い。

しかし、組織にとって、取り扱っている情報がビジネスの源であり、その情報が漏洩してしまったらビジネスが維持できないということであれば、定番システムの導入だけではなく、さらに情報漏洩に対する対策が必要になることは明らかだ。あるいは、オンラインサービスの継続的な維持がビジネス上必須であれば、オンラインサービスを提供しているサーバーに対するセキュリティー対策を重点的に行うことも当然考えなければならない。

このような、ビジネスにとって守らなければならないものは何であるのかということを考えたセキュリティー対策を行わなければ意味がない。以前、ある組織のセキュリティー対策について相談を受けたときに、「情報漏洩をいかに防ぐかが問題なんですよ」と言っていたセキュリティー技術者が、その対策としてファイアーウォールにおけるトラフィックの監視強化を言っているのを聞いたときには、この技術

者は一体何を考えているのかと腹立たしくなったことがある。たとえば、情報漏洩を防ぎたいのであれば、最初にやるべきは情報管理体制をどのように構築するのかという制度作りであり、その次にその制度に基づいた、デジタル化された情報の管理基盤の構築だろう。そして、最後にメールなどの外部との通信によって情報が内部の人間によって意図的に漏洩されることを防ぐ意味で、外部との境界面での監視が必要になるだろう。

戦略3 組織にとって第一に守るべきものは何であるのかを考え、その考え方に忠実にシステムを作り出すことを考えなければ意味がない。特に、定番システムを導入し、一時の安心感に浸って思考を停止することは絶対に避けなければならない。

身の丈肩幅に合ったシステム

また、システム設計時によくあるのは、「ほかの組織が○○システムを使っているから、うちも使ってみよう」という話である。もちろん、定番システムを入れる、あるいは、議論の出発点として他組織の事例を調べるのは悪くない。しかし、セキュリティーシステムでは他組織で使っているシステムがそのまま流用できるかどうかはかなり注意しなければならない。

1つは、そのシステムを使いこなすことができるかどうかである。セキュリティーシステムは、単に導入すればそれでおしまいというシステムではない。日々システムを運用し、組織の事情に合ったチューニングを施し、システムが訴えかけてくる警告を理解し、必要があれば追加的な対策を施すことが求められる。つまり、セキュリティーシステムは、「使いこなしてなんぼ」のシステムなのだ。もしも運用に必要な技術者が確保できないのであれば、アウトソーシングを検討するとか、あるいは、技術者の育成も同時に進めて自主運用に早い段階で移行するというようなことを検討することが必要となる。

これも別の組織の話であるが、ファイアーウォールを導入したが、ファイアーウォールの設定ができる技術者が社内にいなかったために、適切に設定されていないファイアーウォールを運用していた組織があった。宝の持ち腐れもいいところだ。使いこなせないものを導入しても意味がない。

戦略4 使いこなせるシステムを導入しなければ、意味がない。使いこなすために、アウトソーシング、技術者の育成は当然考えなければならない。

業務に支障を来たしてはいけない

2番目に、業務に適合しているシステムなのかどうかを検討しなければならない。セキュリティーシステムは、当然組織における情報資産やシステム資産の運用を円滑に、かつ、トラブルなく進めることを目標として構築される。しかし、セキュリティーを偏重するあまり、ユーザーの利便性を下げてしまう可能性がある。ところが、いまや情報処理システムやネットワークシステムにはほぼすべての業務が依存しているから、セキュリティー対策を強固に行いつつも、ユーザーの利便性を犠牲にすることは最低限度にとどめなければならない。利便性を犠牲にして、セキュリティーを優先するというような結論に到達してはいけないのだ。その意味で、他者が使っているシステムが、本当に業務に適合しているかどうかを真剣に検討することが必要だ。

戦略5 セキュリティーシステムの構築では、利用者の利便性の犠牲を最低限度にすることが必須である。

導入するシステムは自分で判断する

3番目に考えなければならないのは、他者が使っているシステムは、自分たちにとって本当に実効性があるのだろうかという点だ。

セキュリティーシステムは、他の技術と同じように実環境での実効性を示したもの、いわゆるフィールドプルーフ(field proofed)されたものを使うことが正道である。実績のないシステムや奇をてらったシステムを使うのは、一種の博打と考えてよい。もちろん、業務とシステム環境の都合から、考えぬいた結果として現時点でベストソリューションとして、どうしても実績のないシステムを導入しなければならないこともある。その場合には、慎重の上にも慎重に、システムを念入りに試験して導入することが必要となる。この意味で、他者が使っているシステムが、本当にうまくいっているシステムかどうかを確認する必要があるだろう。

よく他者が使っているシステムとして漏れ伝わってくる話は、いい話しか聞こえてこないことが多い。特に、システムの販売元や取り扱い代理店からはそんな声しか聞こえてこない。本当は、セキュリティーシステムを売る営業担当者は、システムの良いところと悪いところを正しく顧客に提示して、より良いソリューションを提示できるようにすることが本来必要であるにもかかわらず、セキュリティーシステムでも良いことばかり言う営業が多すぎるという問題も他方ある。だからこそ、他者が使っているシステムについて、合理性の高い評価を手にしなければ、その評判については単純に納得してはいけないのだ。その意味で、システムについては十分に吟味することが必要だし、実際に使っている組織があれば直接問い合わせるのも方法として考えるべきだろう。

戦略6 使用するシステムについては、その評判を鵜呑みにしない。自分自身の目で確認し、その有効性を納得することが大事だ。

暗号化は諸刃の刃

情報保護を考えた場合、暗号化の手法を取り入れることは必要となる。たとえば、文書を暗号化したり、通信路を暗号化したり、そんな対策は今や当たり前のものになっている。

しかし暗号化を過信してはならない。念のために書くが、ここで私が指摘するのは暗号そのものの問題ではなく、暗号化を使ったシステムの運用の問題である。

暗号化の手法は、本来多くの面に配慮して使わなければ意味がない。たとえば、ある文書を暗号化して保存していたとしよう。この文書を参照した誰かが復号した文書を平文のままで保存し、かつ、誰からも見えるフォルダーに入れておいたら、暗号化の意味はまったくなくなる。また、暗号化しておいても、復号鍵を忘れてしまった場合に問題だと、平文の文書をそのままバックアップにしまいこむようなことをした場合、バックアップの保管が適正に行われてなければ、リスクは逆に増大してしまう。

暗号化を使うのであれば、いくつかの基本原則を守る必要がある。

- 暗号化システムを利用するユーザーを限定し、その取り扱い方法を正しく身に付けさせる。
- 暗号化を適用する範囲を明確にし、ユーザーが暗号化されている重要情報を取り扱っていることを強く意識させる。
- 暗号化された情報資源にアクセスできる環境を限定する。そもそも暗号化して保存しなければならないような情報をネットワーク環境で共有するようなことが許されるのかを十分吟味する必要がある。
- 暗号化のためのシステムは、その機能、限界、使用する前提条件を十分に理解する。これらが利用環境に適合しない場合には、他のシステムを検討する勇気を持つ。

よく情報保護のための環境をどのように設計するかという議論をすると、「それは暗号化で対応します」という答えを述べる技術者が大半だ。そして、「じゃぁ、どんなシステムにするの?」という問いかけに対しては、具体的な利用環境が提示されないことが多い。私たちは、暗号化という道具を使いこなしているわけではない。また、過去にも暗号化という道具をうまく使いこなせたケースは本当に少ない。もしも暗号化をソリューションとして使うのであれば、本当にいろいろなことを考えてシステムを設計することが必須となることを肝に銘じるべきだ。

戦略7 情報の暗号化を使う場合には、運用環境の設計を入念に行う

認証も非常に大きな問題となる

もう1つセキュリティー技術者が安易に考えてしまうのが、ユーザーの認証方法である。たとえば、再利用可能なパスワードはネットワーク盗聴に弱いので、使い捨てパスワードを使いましょうという議論は納得できる。しかし、最近よくあるのが、ICカードを使って認証をしますとか、指紋などの生体計測技術を利用しますということだ。本当にこれらが自分の環境にとって実用的なのかどうかは十分に考え抜かなければならない。

たとえばICカードを考えよう。認証トークンを入れておき、それを認証の1つの要素として使うのが一般的である。しかし、ICカードは盗難されることもある。盗難されたカードを使ってアクセスできるようなシステムではどうしようもない。生体計測を利用する場合には、その計測デバイスがない場合のアクセスをどのように考えるのかを綿密に設計する必要がある。結局、生体計測を使えない環境でもアクセスを許すのであれば、結局保護レベルは低下してしまう。

償却、更新そして増強

本稿の最後に述べたいのは、セキュリティーシステムの償却期間についてである。セキュリティーシステムは、常にそれを破る側の技術力との競争に晒されるという宿命がある。このため、セキュリティーシステムそのものに脆弱性が発見されてしまった場合には、そのシステムそのものを改修して強力なものにする必要がどうしても発生する。この意味から言えば、通常のシステムのように○年償却で設計し、期間満了で更新という考え方だけでは対応できないと言ってもいいだろう。場合によっては、償却期間未了でもシステムの更新・増強をしなければならないこともあるのだ。

逆に、償却期間満了という理由でいきなりシステムを更新してもよいかについても、十分な検討が必要である。セキュリティーシステムは、ある意味で組織に強く絡み合うシステムである。セキュリティーシステムは、技術的な要素だけから構成されるのではなく、手続き、ルール、ポリシーなどの非技術的な要素も含む。したがって、単に償却期間満了だからと言って安易にシステムを入れ替えると、非技術的な要素との整合性が保たれなくなることもある。この意味で、セキュリティーシステムの入れ替えをする場合には、周りとの関係を十分にチェックしてから、問題が発生しないように更新を実施することが必要になる。

更新や増強といったことを円滑に行うためには、システムそのものを日頃から正しく理解し、どこに問題があるのか、どんなシステムとの関連性が強いのかを意識しておくことが重要である。

最後にもう一度。何も起きないことは、何もしないことから生まれるわけではなく、毎日何かをしているから何も起きない状態を維持できるのである。これを肝に銘じること。

［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