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非技術的な面の設計では、責任と権限、強制と協力をうまく使い分ける必要がある。ところが、一口に使い分けといっても同じ人間が多面的にこれらの役割を果たすのは難しい。そこで、今回は表裏一体となるこれらの組み合わせを現実としてどのように考えるのかについてまとめてみた。

第二回 責任と権限、強制と協力

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

ここ数年、効率的な組織運営にはトップによる統治強化が重要であると強く言われている。これを受けて数年前から、執行役員制度を導入する企業が増えている。執行役員制度のミソは、役員として意思決定にかかわる人を必要最小限まで減らし、即決即断の実行体制を作り出すことにある。これにより、トップによる直接的な指揮体制の創出を狙っている。

最近、私はいろいろな企業の役員の方々に会う機会が増えているが、いただく名刺の肩書きに単に「取締役」とだけ書かれている企業は急減しているように思う。逆に、CEO、CTOといった米国的な執行役員の略称を書いている場合や「○○担当役員」のような責任領域を明示しているケースが増えている。この傾向は大企業であろうが中小企業であろうがあまり関係ないようだ。

考えてみれば、従来の取締役会による集団統治体制は、意思決定の遅さと組織運営における曖昧さが常に付きまとっていた。また、しばしば無責任体制を生み出していた。執行役員制度は、役員会による集団統治の弱点や短所の排除を狙っているのである。執行役員制の導入は、各役員の権限を飛躍的に拡大させるが、当然、同時に責任も大きくなる。したがって責任範囲がはっきりする執行役員制度の方が経営姿勢や執行が明確になるという声も多い。

CIOはCISOを包含する

最近の企業統治スタイルの中では、CIO（Chief Information Officer）の役割に注目が集まっている。現在の企業活動は、情報の取り扱いを真剣に考えなければ成り立たない。企業内部における情報流通基盤の形成、情報利用環境の構築、情報保護、さらには、外部に対して情報をどのように提示していくのかといった、戦略立案と実行が必要である。この情報にかかわる種々の活動を統括する役員がCIOである。

一方、組織におけるセキュリティー管理ではCISO（Chief Information Security Officer）が統括責任を負うというのが普通だ。しかしCISOが行うべき業務は、実はCIOの業務に含まれる。CISOの業務は情報セキュリティー管理に強くフォーカスするのに対して、CIOは情報全般にかかわる業務を統括する立場にある。このことから、CIOのほうがCISOよりも責任範囲が広く、CISOの業務を包含する。実際、CIOがCISOの業務を果たしている企業はたくさん存在する。

前回説明したように組織のセキュリティー管理では全権掌握型のCISOを擁したほうが多くの面でメリットがある。しかし、全権掌握型CISOは、その責任範囲も拡大する。しかし責任範囲の拡大は、1人の人間による誤った判断を引き起こす可能性を増やすことに直結する。もともと人間はいくつものことに同時に対応できるほど器用にはできていない。セキュリティー管理の目的は、組織における情報処理システムに起因するリスクを減らすことが目的である。CISOが全権を掌握する構造で、CISOの存在そのものがリスクになってしまっては元の木阿弥である。

CISOが全権を掌握しつつ、その中で誤った判断や行動を引き起こさないようにするためには、さまざまな知恵が必要となる。今回は、この「知恵」に焦点を当てて考えてみたい。

強制に必要な「教育」と「儀式」

CISOが統括しなければならない業務の1つが、セキュリティーポリシーの策定と、セキュリティーポリシーに合致するさまざまな手続き、約束事、ルールの施行である。

セキュリティーポリシーとは、組織として情報をどのように守るのか、そして守るためには何をするのかというセキュリティー管理についての基本的な考え方を与えるものである。

このセキュリティーポリシーについては、組織構成員全員が同意しているものでなければならない。しかし、組織構成員全員が何もしないで合意するものを作り出すのは難しい。もしも構成員が10人以上の組織でセキュリティーポリシーを作った場合に、最初に作成したセキュリティーポリシーに誰も反対意見を表明しないとしたら、逆に異常な状態だろう。作成したセキュリティーポリシーが誰も反対する気にならないほど抽象的過ぎるか、あるいは、まったく実効性の無いものかもしれない。構成員が多くなればなるほど、全員が簡単に同意することは難しくなる。このために、セキュリティーポリシーの作成プロセスでは版を重ね、できる限り多くの人たちにとって同意できる合理性の高いものに結晶化させていく作業が必須となる。しかし、最後まで納得しない人が存在してしまうのは当然想定される。もしも作成したセキュリティーポリシーに同意してもらえないとしたら、組織として同意を強制しなければならない。

この同意を強制する場合に重要となる作業が「教育」と「儀式」である。

ルールは破るためにある?

まず、教育は同意を強制される人にとって疑念を減らす作業である。何らかのルールを強制されているときに、そのルールは何のためにあるのかがわからなければ、守ろうとする意思が弱くなってしまう。

たとえば、田舎の田畑の中をまっすぐに貫く農道の最高速度が時速40キロに制限されていたら、あなたは制限速度を守るだろうか。正直に申し上げて、私は守ることはないだろう。しかし、最高速度がなぜ時速40キロに制限されているかの理由が提示され、さらに提示された理由に合理性が十分あると感じられればどうだろうか。おそらく多くの人が、そのルールを守ろうと考えるに違いない。このように、教育によって人々は考え方を変え、ルールを遵守することを考えるようになることが多い。もちろん、教育したからといって信念を曲げない人も当然いるから、誰をも納得させて同意させる確実な方法ではないが、少なくとも多くの人の疑問を解消するには教育は役立つ面が多い。

一方、儀式とは形式的なやり方で同意を記録することである。たとえば、同意書にサインさせるのは儀式の典型である。儀式の本質は、自分が同意したということを明示的に示す行為によって、「ああ、自分はこれに同意したのだ」と意識に刷り込むことである。何を同意したのかをしっかりと意識させることによって、ポリシーを忘れさせない効果がある。儀式を行うことによって、ルールの遵守に努めるようになるという効能を期待できるのだ。

教育も儀式も、即効性、確実性は期待できない。しかし同意を強制したときに、強制される側が納得すること、さらに、その同意について翻意しないようなプレッシャーを与える、心理的なストッパーと言ってもいい。ルールは破るためにあるのだという気持ちを、ルールは守るためにあるのだという気持ちに変えさせる力を持っているのだ。

戦略1 同意を強制する場合には、教育と儀式をかならずセットで与えること。

合理性のみが助けである

私たちは、道理がわかっていないことはなかなか実行できない。理由に合理性がないことは納得がいかないものだ。このようなルールを設けたとしても、実行されるとは到底思えない。また、正論そのままのものもあるが、現実的に実行できないものもある。運用面での合理性がなければ、やはり実行されないルールとなってしまう。

これを踏まえると、CISOとしては、セキュリティーポリシーや各種手続き、ルールを作り出すときに、必ず合理性を持ったものを作る努力が必要である。合理性が確保できないと、教育でも説得力のある説明ができなくなってしまうし、そのうえ儀式の効能も薄くなってしまう。決められたルールが的確に適用され、ルールに従って行動や運用がなされることこそが、CISOとして実現しなければならない目標である。

合理性の追求は、実は落とし穴が待っていることもある。たとえば、技術者にとって当たり前のことが、技術者ではない人にとってはまったく難解至極なこともある。あるいは、業務のフローを大きく変えてしまって、現場における合理性を破壊してしまうこともある。このようなことから、ルールが適用される環境、対象となる人たち、そこに存在するシステムをよく見て考えることが必要不可欠である。その意味でCISOは、さまざまなソリューションを提供できる柔軟な思考が必要となる。また、現状を把握するための目と耳を持つことも当然だろう。

戦略2 合理性あるルール、手続きを構築すること。そのとき、適用される環境、対象となる人、システムをよく勘案すること。

CISOの責任を考える

CISOが日常的に行う必要がある業務

の大部分は、いざというときのための準備であることだ。つまり、情報システムにまつわるリスクを一生懸命考え、想定されるリスクにプライオリティーを付けて、どのリスクを優先して排除するかを考え、実際に排除するための準備を着実にこなしていくことになる。「備えよ、常に」である。

とは言え実際にCISOが具体的な準備作業をするのかと言えば、実際には対象となるそれぞれの部署でそこで働く人たちを使って準備をすることになる。つまり、CISOは設計者であり、その設計を実際に行う人たちは、また別の人たちとなる。ここに落とし穴が待ち受けている。

「頭」と「手」が分離しているときには、どうしても「手」が「頭」の思ったほどに動いてくれない。セキュリティー管理で行われる種々の準備は「いざというとき」にその力を発揮するが、その「いざというとき」に対して実際に作業する人が実感を持っていなければ、なかなか思ったとおりに作業をしてくれないかもしれない。CISOにとっては合理性があったとしても、作業をする人にとっては合理性を感じられない、あるいは、感じさせていない状況では、不十分な作業しか実行されていないということがよく発生する。

内部の同士だと思っていた人たちが、実はリスクを増大させる原因になることは、よくあることだ。実際、セキュリティー管理作業をすればするほど、また、それを厳密にすればするほど、CISOにとっては組織内部に対する不満が溜まることはよくある。

なぜ、みんなはこちらの考えたとおりに対策を実施してくれないのか――このような状況に遭遇した場合に、CISOが強権的な手法で問題を解決しようとすると「手」との間での軋轢が確実に生じてしまう。たとえば、抜き打ちで監査作業をして、不手際の早急な是正を迫るようなことをついやってしまうが、結局、不満や不平だけを増大させてしまうことが多い。そこで、権限をたくさん握っている人は周到な計画を立て、確実に準備を進め、現場との軋轢が生じないような対策を立てることが求められる。これもCISOの責任でもある。

戦略3 周到に作り出された計画を立案するのは、CISOの責任である。与えられた権限を振り回して強権的な作業しかできないとしたら、そのCISOはあまりに能無しである。

権限の多さは自由度の高さ

与えられた権限が多いということは、ソリューションを考えるときに高い自由度を確保できているという意味がある。つまり、教条主義的に当たり前と思うことをストレートに実施しなくても、結果として同程度の準備あるいはセキュリティー対策が立てられればいいということになる。

たとえば、ある部門に十分なセキュリティー対策を施す必要があるとしよう。その部門には、システムとネットワークを使いこなす技術者が十分にいない状況だったとする。この場合、その部門のシステム環境はそのままにしておいて、その環境を保護するような組織内ファイアーウォールを作ってしまうことで、内部の環境をいじることなく、その部門の保護の度合いを高められるかもしれない。そのために、エンタープライズネットワークの管理運営部隊を動かすこともCISOにとっては可能なことである。

戦略4 CISOに与えられた強い権限によって、ソリューションを考える時の拘束条件を緩和していると考えよ。

同じ意識を持たせることが重要

ところで、私たちが何らかの行動をとるときの原動力は何であろうか――それは、理解である。なぜそのような行動をとらなければならないのかについて合理的な理解を持っていれば、その行動を規制するものはなくなる。物事に対する根源的理解があれば、その行動は正しいと思うのだ。

一方、合理的な理解がない状態、あるいは、自分自身の合理的な理解と実際に指示されている行動に差異がある状態は、行動を強制されたと感じてしまう。

つまり、CISOが考える合理性を多くの人たちが理解するようになれば、強制されたという感覚をユーザーやほかの管理者たちが持つことは減るに違いない。ここに啓発活動を展開する意味がある。つまり、ユーザーやほかの管理者たちが、同じマインドを持つことで、CISOの強い味方になるのだ。

ところが、1つ厄介な問題がある。根源的理解を与えるためには、各々の理解度に合わせた説明によって納得してもらう必要がある。つまり、CISOはさまざまなレベルの人と十分なコミュニケーションを行い、さらに、そこで確実に理解させる腕が必要となる。

戦略5 啓発活動は、異なる立場にいる人たちにCISOと同じ意識を持たせるための有効な道具である。しかし、有効な道具として機能させるためには、高品質なコミュニケーション能力を持たなければならない。

協力を引き出す

CISOが司令官になり、立案した作戦に基づいてさまざまな作業をするエンジニアたちが存在するというのが、基本的なセキュリティー管理体制となるのは、前回も述べたとおりである。しかしながら、その体制は、いわゆる軍隊的な上意下達型の動きを常にするわけではない。当然、セキュリティー的な障害が発生したときには緊急対応の作業の中で軍隊的な動きをすることもあろう。しかし多くの場面では、CISOが計画立案者で、提示された種々の対策についてその本質を理解したエンジニアたちが協力し合いながら動く

ということのほうが、機能的である。

一方、立案したセキュリティー対策のさまざまな方策が設計どおりに実装されているか、機能しているかを調べるために、監査の実施も必要となる。不手際や不具合があれば、それが問題になる前に直すことも必要となる。その意味では、CISOは監督者で実際の作業をするエンジニアたちが評価対象者となる場面も発生する。

CISOが行わなければならないこのような業務の二面性、つまりエンジアたちをチームとして構成して機能的に協力し合う部隊として成立させることと、同時にそのチームが行ったことを包み隠さず評価して不具合があれば直すということが、CISOの姿勢や立ち位置に微妙に影響してくるのは事実である。

しかしCISOとして忘れてはならないのは、セキュリティー対策には定石はあるが、それだけでは不十分で、対象となる環境に対して思いをめぐらし、柔軟な対策を立案していくことがCISOとして本来やらねばならないことである。そのためには、自分の考えたプランについて、常に別の面から再評価する作業を自分に課することが必要となる。しかし、1人の人間が思いを巡らせられる領域は実際には限られているのが現実だ。セキュリティー対策の実施に携わる多くのエンジニアの意見を聞き、評価を受け、その中でセキュリティー対策の質を上げていくことができれば、1人で作業するよりも、もっといいものが生まれてくるに違いない。

その意味で、CISOは、一緒に作業するエンジニアのグループをチームとして構成し、そこから意見がたくさん出てくるような環境をうまく作り出すことが必要になる。また、技術面だけではない検討要素を持つためにも、いろいろな情報を得られるようにしておかなければならないだろう。つまり、セキュリティー対策にかかわる人たちからのインプットが正しく伝わるようなシステムを作り上げることを真剣に考える必要があるはずだ。

戦略6 セキュリティー対策を一緒に実装していくエンジニアやセキュリティー対策にかかわる多くの人たちからのインプットを得られるシステムを作り上げることが重要だ。

さて、今回はCISOの業務に注目して、そこに存在する責任と権限、さらには、強制と協力という視点で、CISOが考えるべきポイントについて議論をしてきた。

この議論を見ると、セキュリティー対策実施のためにCISOが持つべき資質というよりも、リーダーとしての素養は何であるのかという人材論のような話になってしまったことは否めない。しかしCISOがやらなければならない業務は多岐にわたるのは前回も述べたとおりだ。技術的な面だけではなく、非技術的な面でもその能力を発揮しなければならない。また、組織の中で、セキュリティー対策を実装することが確実に行われるような体制作りも必要となる。その意味で、CISOに求められる人間としての「力」は、普通のリーダーよりも高い質が求められる。つまり、CISOは弛まない努力と精進、自分の能力開発における研鑽が必要となる。

なお、今回の議論の中で、教育と啓発活動を区別して使っていることには注意していただきたい。教育は、具体的に何をしなければならないか、何をしてはいけないかというテクニックを与えることを主眼とした技術移転作業という捉え方をしている。一方、啓発活動は、物事の捉え方、問題解決の道筋や考え方、さらには組織にとって何が重要なのかというプライオリティーの考え方を与えるための活動という認識でいる。教育は技術移転という面が強いのに対して、啓発活動はセキュリティー文化を生み出していく素地を形成する。教育と啓発活動は、即効性は期待できないが、多くの可能性を持っている。どちらも、長期的なセキュリティー対策と分類されているのも事実である。

［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