やっぱり間違いだらけのISO

第8回
「間違いだらけのISO／情報セキュリティ実践編」

DASジャパン株式会社 代表取締役
萩原 睦幸

今回は、実際に情報セキュリティをどのように実現するかの要点を述べてみたいと思う。

ISO 27001やPマークに取り組む上で一番悩ませられるのが、いったいどこまでやればいいのかではないだろうか。例えば入退室管理では、指紋などの生体認証まで必要なのか、受付で簡単な記入で済ませてもよいものか、どうしても迷いが生じてしまう。実際の審査でも、担当審査員の考えがまちまちであることが少なくなく、よけい混乱を与えている面もある。

リスクアセスメント

さて、情報セキュリティの仕組みを構築する上で大きなステップは、リスクを分析し評価する「リスクアセスメント」である。情報セキュリティのリスクは、一般的に情報資産の価値とその情報の扱われ方で決まってしまう。

まずは情報資産の価値の評価であるが、一般にC（機密性）、I（完全性）、A（可用性）の3要素で決まるとされる。ここでのCとAは相反することが考えられる。つまり、機密性が高まればその情報にアクセスする人は限定され、可用性の面では劣ることになる。

ここで留意すべきことは、3つの要素を単純に掛けたり足したりして情報資産の価値を算出しないことである。例えば**図表1**の資産台帳のように、機密性が高い重要な情報であっても、単なる足し算の結果では、機密性が中程度の方が情報資産価値が高くなってしまい、資産価値が正しく評価されないことになる。それを防ぐためには、もっと機密性に比重をおいた計算式が必要であろう。

次にこの情報資産を基にした情報セキュリティのリスク評価であるが、一般的には、リスクの大きさ＝情報資産×（脆弱性＋脅威）の数式で評価される。この数式によれば、情報資産の価値が高くて、それが社外へ漏洩したら多大な損失を被り、しかもその情報の扱いがずさんなら、そのリスクは極めて大きいということになる。

この現状のリスク評価の結果により、各々の情報資産に対するセキュリティ対策がとられるわけだが、とられる対策の程度によりリスクは低減され、対策後のリスクが再評価される。つまりリスク評価は、対策前の評価と対策後のそれと

の2段階がある。

しかし、どのような対策をとったとしても何らかのリスクは残るはずであり、それらを「残留リスク」として認識しておく必要があろう。そして、どこかでこのセキュリティに関わるコストとその対策の効果との兼ね合いを見ながら、あらかじめ定めた受容できる基準に到達するまで何らかの対策でリスクを低減するわけである。

図表1　情報資産登録台帳

情報資産名	機密性（C）	完全性（I）	可用性（A）	情報資産価値＝C＋I＋A
契約書	5	4	2	11
請求書	4	5	2	11
名刺	3	3	4	10
社員名簿	5	4	1	10
アプリケーションソフト	2	5	5	12
共有データ	3	5	4	12

機密性が高いにもかかわらず情報資産の価値は低い

入退室管理

次に、情報セキュリティにとって関係者以外の入室を制限することも重要である。この入退室管理のやり方はさまざまなケースがあってもよいと思われる。高価な生体認証のシステムも時には必要かもしれないが、すべてそこまで強制されているわけではない。自社の現状を考慮しながら、それに見合った仕組みを導入すればよい(**図表2**)。

例えば独立した社屋で社員数が少なく全員が顔見知りであれば、あえて社員証で識別する必要などなく、社員以外の人を識別するだけで十分である。一方、都会の雑居ビルのような場合には、どこの誰かも分からない不特定多数の人が出入りする可能性があるので、関係者以外の勝手な侵入を防ぐ意味では、どこの誰かをあらかじめ知った上で入室を許可する仕組みが必要になってくる。

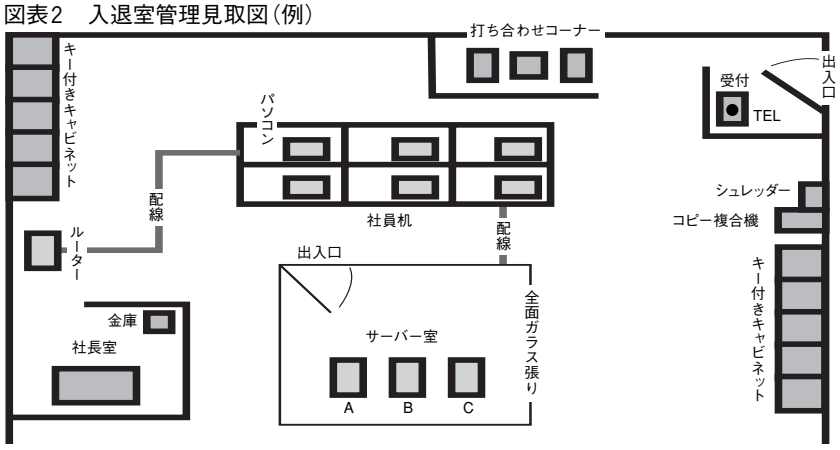
入退室管理のもう一つの大きな目的は、社内の貴重な情報を無断で持ち出すことを防ぐ意味もある。そのためには、誰がいつどのような目的で入室し、どのような作業を行ったか、さらに退室時には情報が持ち出されないようなチェックの仕組みが効いているかが重要なのである。都内のS社のように、入室時に顧客の携帯電話を預かったり、携帯電話の画面にシールを貼って盗み撮りされないよう、万が一の事故に備える会社もある。

一方、入退室管理を磁気カードで行っているところも少なくないが、単なる磁気カードだけでは紛失したカードで本人になりすまし簡単に入室できてしまうから、暗証番号との組み合わせなどの二重管理が必要である。

ID・パスワードでのアクセス制限

企業内にはさまざまな情報があふれている。上層部や幹部だけが知っておくべき重要な人事情報や経営情報もあれば、機密性が高い新製品のための技術情報もあるだろう。その他一般社員が共有すべき社内外の連絡事項や、各社員が自身の仕事を進める上での情報のやりとりもあるに違いない。これらのさま

図表2　入退室管理見取図（例）



ざまな情報に対して、どの情報がどこまでの権限者に公開されるべきかを、あらかじめ決めておくことも極めて重要である。情報アクセスの権限をランク付けしておくわけだが、これにより情報のセキュリティはかなり高まることになる。

もっとも、これは今に始まったことではなく、昔から人事情報などは限られた人しか知り得る立場になかったが。このアクセス制限では、公開対象者を絞り込みすぎて業務に支障をきたすようでは何のための制限なのかが問われるので、臨機応変にアクセス制限を変更できる仕組みも必要だろう。

また、アクセスに必要なパスワードはよく忘れることも多いが、他人に知られないようにするのがまず第一だから、最低8桁以上にし、さまざまな文字・記号を組み合わせて判別しにくい内容にしておくことだ。万が一忘れた場合にも、速やかに再発行できるか、もとのパスワードを容易に再確認できる仕組みも必要である。パスワードを忘れてしまったために業務が長時間ストップしてしまうようでは、システムの不備とみなされても仕方がないだろう。

また、サーバーなどに社員の共有情報が一括して保管してあるケースが少なくないが、自部門に関係しない情報まで誰でもアクセスできてしまうのは問題である。共有してもよいもの、部門や業務特有なものなどを識別し、ここでもアクセス制限をかけておくべきである。

委託先管理

現代の世の中は、自社単独で何から何まですべてこなす時代ではない。協力業者と一体となり仕事の効率と業績アップを狙うのがこれからの企業の生きるべき道である。

このような背景から、重要な情報を委託先に与え仕事の成果を求めるケースが増えている。実は情報漏洩の事故が、これら情報の委託先で発生しているケースが多いのだ。

委託先での事故で考えられる原因の一つに、「責任感の希薄さ」があげられる。委託元から仕事の一部を依頼されるケースが多く、全体が見えないもどかしさがある。したがって、その情報がどの程度重要なのかが認識しづらく、かつ情報セキュリティの仕組みも満足に整備されていない現状では、個人の意識に頼らざるを得ないという弱点もある。

長年付き合いのある委託先については、昔から契約書もないままの「なあなあの付き合い」のところも多く、しがらみを断ち切れないでいる。しかしもうそのような時代ではない。仕事の区分と役割などを明確に記載した「委託先契約書」を取り交わし、お互いの責任範囲をはっきりすべきなのである。

もし委託先で情報漏洩の事故が起こったとしたら、それ相応の負担を求めるべきである。つまり従来の業務委託という形だけの取り交わしではなく、情報の取り扱いや事故時の責任分担などを契約書に盛り込み、委託先に十分説明しておくべきなのだ。

また、ISO 9001と同様に、定期的に委託先に出向き、委託先での情報の取り扱いや保管状況などが適切かどうかをチェックすることも必要である。こうすることによりお互いのコミュニケーションも深まり、かつ委託先に責任感を持たせることにもつながるのである。

セキュリティインシデントと事業継続管理（BCM）

ISO 27001付属書Aの13章と14章に、「情報セキュリティインシデントの管理」と「事業継続管理」のやるべき内容が記載されている。この2つの章は大いに関連していて、何らかのセキュリティ事故が起こったときに、事業継続をいかにはかるかの仕組みづくりを要求している。今の世の中では、セキュリティ事故に限らず、大きな自然災害などに遭遇した場合、いかに事業を継続または速やかに復旧し顧客に迷惑をかけないかが注目されている。

メーカーにとって、大切な顧客への製品の供給が一時たりとも途絶えるのは許されないことなのである。例えば製品の部品を供給する業者が、何らかのトラブルで部品を供給することができなくなったら、供給されるメーカーはもとよりその製品を購入する一般の消費者にまで迷惑が及ぶことになる。つまりメーカーとしては、何があったとしても部品供給業者に事業を継続してもらう必要があるし、その事業継続力がない業者は、やがて切り捨てられる運命にあるのだ。

現代の多くの企業は、さまざまな情報システムを活用し事業を営んでいる。もしその情報システムが何らかのインシデントでダウンしてしまったら、事業は立ち行かなくなってしまう。そのためには、

情報のバックアップの仕組みを構築しておく必要があるのだ(**図表3**)。例えば何らかのトラブルで飛行機の片側のエンジンが停止したとしても、残りのエンジンを駆使することにより、最寄りの飛行場に無事着陸できるのと同じことを考えるべきなのである。

つまり、現状のシステムがダウンしたとしても、バックアップ用のシステムで事業を継続しながら、速やかに正常なシステムを復旧させる仕組みの構築である。北陸地方のT企業では、メイン工場のほかに2キロほど離れた場所でも、規模は1/5ほどだが、同じ情報システムで事業を行っている。もともとそちらで創業を始めたが、事業の発展に伴い手狭になり、現在のメイン工場を建設したとのことだが、まさに事業継続の要件を満たしている。

またインシデントに遭遇したときに、いかに早く復旧できるかも顧客から信頼を得る大きな要素である。そのためには復旧する手順をあらかじめ決めておき、定期的にインシデントを想定し、現実に復旧できるかどうかを確かめておくことも重要なことである。ISO 14001の「緊急時対応」と同じように考えればよい。それでなくとも事故時には気持ちが動転しているはずだから、そのときに冷静に行動するためには前もって訓練しておくのが一番だからである。

監視の重要性

人間は他人の監視の目があると、何らかの違反や犯罪を躊躇するものである。警察の目が行き届かないと、平気で信号を無視し横断してしまう人が少なくないが、交番が近くにあると、このような行動は起こさないのが普通である。情報セキュリティの管理でも同じことがいえよう。誰かの監視があると、人は罪を犯そうとはしない。最近はこの効果が認識され、監視カメラの売れ行きが好調のようだが、監視カメラで一部始終録画されていると思うと、とても思い切った行動には出られない。

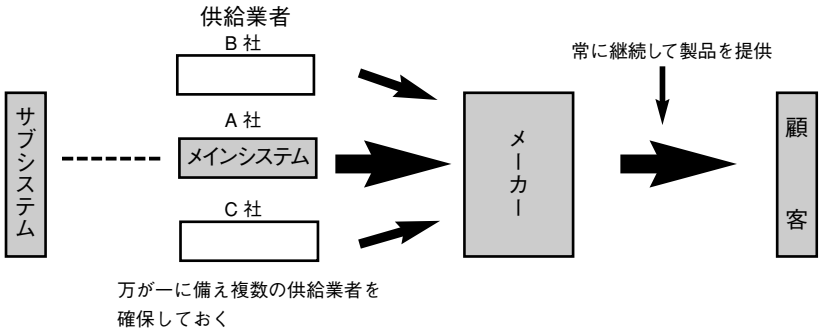
一方オフィスの中の行動についても、第三者の目による監視の効果は大きい。自分以外の第三者がいるということでいろいろな行動にブレーキがかかるのである。したがってコストをかけて大げさな監視システムを導入しなくても、お互いの行動を監視するということを意識するだけでも、セキュリティ事故はかなりの程度防止できるのだ。

しかしあまりこれが行き過ぎると人間同士の不信感につながるから、それだけは避けなければならない。要は皆でとり決めたルールを本人が遵守しているかどうかの監視だけでよいのである。

他人を監視するということは、自分でもそのルールを遵守するという意識が芽生えるはずである。考えてみれば、意識するしないに関わらず、企業内の行動は常に誰かの監視下で行われていることに気がつく。その意味では、がんじがらめの仕組みよりも、この生きた社員同士の「相互監視」を随所に組み込んだ仕組みの構築を目指すべきではないか。

▼

図表3　事業継続管理の仕組み



DASジャパン株式会社
代表取締役
萩原 睦幸

【プロフィール】2006年10月、英国系(UKAS)審査機関設立。組織に役立つ審査を理念に全国展開中。著書及び講演多数。『ISOが見る見るわかる』『間違いだらけのISO審査』『よくわかる日本版SOX法』他。著書は韓国語、中国語、タイ語にも翻訳されている。