CHAPTER 1

ISMS認証を取り巻く環境

1 社会を取り巻く情報セキュリティ事件・事故の変移

ISO27001の初版は、2005年に発行された。その翌年、2006年には、日本語版のJISが発行され、日本におけるISMS認証は広く普及していった。

もちろん、規格が発行されたというだけでISMSが広まるものではなく、情報セキュリティを取り巻く話題は、2005年４月の個人情報保護法の完全施行、SQLインジェクションのぜい弱性をついたウェブサイトの改ざん、ウィニーを通じた情報漏えい事件などがあり、企業がISMS認証に取り組むきっかけともなった。

さて、それから約10年、社会を取り巻く情報セキュリティ事件・事故、そしてその対策はどのように変わってきたのだろうか。

IPA（独立行政法人情報処理推進機構）が、毎年公表している「情報セキュリティ10大脅威」がある。

〈図表1-1　情報セキュリティを脅かす10大脅威　2006年版と2015年版の比較〉

順位	2006年版　脅威の種類
1位	事件化するSQL インジェクション
2位	Winnyを通じたウイルス感染による情報漏えいの多発
3位	音楽CD に格納された「ルートキットに類似した機能」の事件化
4位	悪質化するフィッシング詐欺
5位	巧妙化するスパイウェア
6位	流行が続くボット
7位	ウェブサイトを狙うCSRF の流行
8位	情報家電、携帯機器などの組込みソフトウェアにひそむ脆弱性
9位	セキュリティ製品の持つ脆弱性
10位	ゼロデイ攻撃

➡

順位	2015年版　脅威の種類
1位	インターネットバンキングやクレジットカード情報の不正利用
2位	内部不正による情報漏えい
3位	標的型攻撃による諜報活動
4位	ウェブサービスへの不正ログイン
5位	ウェブサービスからの顧客情報の窃取
6位	ハッカー集団によるサイバーテロ
7位	ウェブサイトの改ざん
8位	インターネット基盤技術の悪用
9位	脆弱性公表に伴う攻撃の発生
10位	悪意のあるスマートフォンアプリ

独立行政法人情報処理推進機構（IPA）HPより

これは前年の情報セキュリティ事件・事故、トピックから10大脅威をランキングしたものである。

ISO27001が発行、運用され始めた2005年の脅威をまとめた2006年版と2015年版を比較してみると次のようなことが見えてくる。

① 新技術普及への対処

2015年版の10位に「悪意あるスマートフォンアプリ」があげられている。

悪意あるアプリをダウンロードし、それが情報窃取につながり、所有者の情報のみならず、そこに登録されている友人、知人の個人情報漏えいや盗んだ情報をもとにしたなりすましなど、被害は所有者のみならず第三者にも広がることがある。

スマートフォンは、2007年のiPhoneの発売、そして2010年のAndroid搭載機の普及により、全世界に普及していった。

つまり、2005年当時、携帯電話はいわゆる“ガラケー”の時代であった。そして、この携帯電話からスマートフォンへの変移において着目すべきは、技術の進化とともに人の意識が進化していないということである。どういうことかと言えば、依然、スマートフォンは携帯電話であるという認識をもった人がとても多い。

日本には、携帯電話にインターネット機能を有したiモード等が普及していたため、携帯端末でインターネットが使えた。しかし、iモードは、言うならば“ある閉じた世界”でのインターネット接続であるが、スマートフォンの場合は、“開かれた世界”のインターネット接続であり、自由度は拡がった半面、そこに内在するリスクも増えてきた。

さらには、OS、メモリー等の進化、SNSの発展により、もはや、スマートフォンは、携帯電話ではなく、通話機能が付いた超小型PCであるとの認識が必要である。

したがって、そこには、これまでの携帯電話と同じセキュリティ対策ではなく、新たな対策が必要になってくるのである。

② 経済的被害、二次被害の増大

2014年７月に発覚したベネッセの顧客情報漏えい事件では、流失情報は3,504万件、そのお詫びおよびセキュリティ対策費として260億円を引当るなど、信頼や企業ブランド価値の毀損のみならず、企業業績へも大きな影響を与えた。

2015年版の10大脅威を見てみよう。

第１位の「インターネットバンキングやクレジットカード情報の不正使用」、上述の顧客情報漏えいもそれに該当する２位「内部不正による情報漏えい」、４位「ウェブサービスへの不正ログイン」、５位「ウェブサービスからの顧客情報の窃取」は、直接的に経済被害につながる。2014年の不正送金被害は、29億1,000万円で、2013年の約２倍になった。

他にも、３位「標的型攻撃による諜報活動」によって、個人情報が漏えいし、二次被害につながるケースもあり、情報セキュリティのぜい弱性をつかれたり、サイバー攻撃による経済的被害は年々増大している。

③ 新たな手口はいきなり出てくるものではない

2006年版の５位に「悪質化するフィッシング詐欺」がある。

2015年、１位の「インターネットバンキングやクレジットカード情報の不正使用」の不正入手手段の一つとしてフィッシングがあり、その手口は10年前から存在したのである。

これまで金融機関が対策をとらなかったわけではなく、インターネットバンキングの利用者の増大、利用者のリスク認識の感度、そして手口の巧妙化など、さまざま要因が被害の拡大を招いてきたのであろう。

さらに今後の同様の被害は続くであろう。技術的対策、人的対策の必要性は言うまでもないが、“他山の石”に学ぶことも重要である。

セキュリティ事件・事故が発生した時、必ずと言ってもいいほど“模倣犯”が現れる。

自身が被害者にならないため、また悪事に加担しない（踏み台にされない）ためにも、事件・事故を他山の石として対策をとらなければならない。

インターネット上を検索すれば、事件・事故をまとめたサイトも多数あ

るので、そこから学ぶのも一つの手段である。

④ やはり、最大のリスクは“人”

2006年版、2015年版いずれを見ても、事件・事故となるには、そこには必ず人が介在する。

例えば、OS、ソフトウェアにぜい弱性があろうとも、そこに攻撃をしかけなければ、情報漏えいにつながったりしないだろう。

2015年度、特徴的だったのは、開発サイドが公表したぜい弱性情報にもとづき攻撃コードを作成、攻撃するという新たな手口である。利用者側の対応が間に合わなかったり、公表された情報そのものに気づかなかいことさえありうる。

開発サイドのセキュリティ強化策を逆手にとり、攻撃をしかけるという、これまでの常識では対処できない事件・事故だが、それを仕掛けるのも人である。1位の「インターネットバンキングやクレジットカード情報の不正利用」、2位の「内部不正による情報漏えい」も、人が仕掛ける。

インターネット上の不正送金や個人情報の窃取は、人の罪悪感を麻痺させるのかしれない。そこには現実のお金はなく、盗むという行為もない。行為がないのではなく認識がない。つまり、そこに“現物”“現実”はなく、不正をはたらく者にとってデータ、数字を動かしているにすぎず、罪悪感が希薄になるのかもしれない。

こうした犯罪の背景に、近年の多様な雇用形態が取りざたされる。多くの企業で、同じ職場に正規、非正規社員、さらには外注業者が働くことは珍しい光景ではない。そこには賃金格差があり、会社のみならず社会に対する不平不満が存在すると言われる。

ベネッセ事件も、そうした背景があったと言われた。

いずれにせよ、情報、そして組織を守るのも人、それを破ろうとするのも人。

セキュリティ対策の一番の重点ポイントは、人である。

⑤ 法整備、体制の確立

さて、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）も、IPA同様、「セキュリティ10大ニュース」を毎年発表している。

〈図表1-2　2014セキュリティ10大ニュース〉

【第１位】９月25日　ベネッセ個人情報漏えい事故の調査報告書を公表
【第２位】11月６日　サイバーセキュリティ基本法が成立
【第３位】４月７日　Heartbleedなどぜい弱性が多発（４、５月）
【第４位】８月１日　オンラインバンキング不正送金の被害急増
【第５位】11月13日　日本サイバー犯罪対策センター（JC３）設立
【第６位】４月４日　警察庁、ビル管理システムの探索行為に注意を喚起
【第７位】10月１日　マイナンバー制度準備進む
【第８位】９月３日　POSマルウェアによる5600万件のカード情報流出が発覚
【第９位】　９月17日　被害が止まらないパスワードリスト攻撃
【第10位】９月18日　DDoS攻撃業者を使ったオンラインゲームの業務妨害で高校生を書類送検

その2014年の10大ニュースに目を向けてみる。

IPAと同様なトピックもあるが、特徴的だったのが、国の法整備、体制確立である。

これまでセキュリティ対策に国の法整備、体制確立が追いついていないと言われてきたが、２位の「サイバーセキュリティ基本法成立」、５位の「日本サイバー犯罪対策センター設立」など、ひとつの転換期を迎えたと言える。

また逆に新たな法律に対応するために、組織にセキュリティ強化策が求められるケースも現れてきた。

番号法にもとづくマイナンバー制度がそれである。

さすがにセキュリティ対策は情報システム部門に任せておけばよいと考える経営者はいないだろうが全社的対応を迫られる。