[特集2]

外部からのアタック対策だけではないセキュリティー

組織内ネットワークの情報管理術

情報漏洩　個人情報管理　内部犯行

セカンドステージのインターネットでは、ネットワークを外部から守るセキュリティー対策はすでに当然のものだ。今意識しなければいけないのは、内部犯行による情報漏洩対策などを含めた組織内の情報管理だ。莫大な損害賠償や株価下落による企業価値の低下などの深刻なダメージを引き起こしかねない情報漏洩などの問題の現状とその対策を解説する。

Text：JNSA／不正プログラム調査WG 渡部章（P99～100）
＋株式会社ラック 新井悠（P101～107）＋中村正則（P108～109）
協力：日本ネットワークセキュリティ協会

あなたの会社は本当に大丈夫？
現実のセキュリティー問題となった内部犯行

内部犯罪はもはや無視できない現実である

2003年6月26日、コンビニ大手ローソンのダイレクトメール発送受託企業から約56万件の会員情報が社外に流出したことが明らかとなった。個人情報の漏洩事件が後を絶たない。その多くは人為的な設定ミスや管理ミスであるが、近年、会社や公共団体での内部犯行による情報漏洩が問題になってきている(表1)。人為的なミスや犯罪行為による情報漏洩は、ちょっとした不注意で誰でも当事者となる可能性がある。昨今の事件を他人事と考えず、これを機会に、普段の自分の情報の扱いはもちろん、会社全体で注意して対策をしていくようにしなければならない。

JNSAの調査報告(参考2、100ページ参照)によると2002年の情報漏洩事件は新聞などに報道されてわかっているものだけでも63件にものぼり、41万8716人の個人情報が漏洩したという。その多くはシステムの設定ミスなど管理ミスが原因でウェブから漏洩したものだが、中には情報の持ち出しなど内部犯罪が原因であるものが4件あり、1万9183人(人数不明を含まず)もの個人情報が内部から漏洩している。内部犯行はとかく隠されがちであり、また表面化していないものも含めると、実際の発生件数は計り知れない。それにひきかえ、不正アクセスを原因とする情報漏洩は3件しかなく、被害者も2500人だけであった。また、情報漏洩によって損害賠償が発生したとすると、1件あたり約2億4,000万円の賠償額になり、株価の下落によって企業価値が18億円以上のマイナスになる可能性があるという試算も出ている。

また、警察庁による平成15年度不正アクセス行為対策の実態調査(グラフ1)では、不正アクセスなどのアクセス元に関する問いに、全体では、「社外(学外)国内から」が57.9パーセントと最も高いが、「社内(学内)から」も9.4パーセントあり、内部犯行の事実が明らかになっている。

一方、海外の状況として、米国のComputer Security Institute(参考3)の調査結果を見ると(表2)、調査に回答した356社の74パーセントにあたる263社が過去1年になんらかのセキュリティーインシデントがあったと答えている。また、336社の69パーセントにあたる232社が外からの侵入や攻撃によりインシデントが発生しており、また、328社の68パーセントにあたる223社が内部の原因によってインシデントが発生していると答えている(設問により回答社数が異なる)。つまり、米国では内部に起因するセキュリティーインシデントが、外部のそれとほぼ同じだけあると認識されているのである。

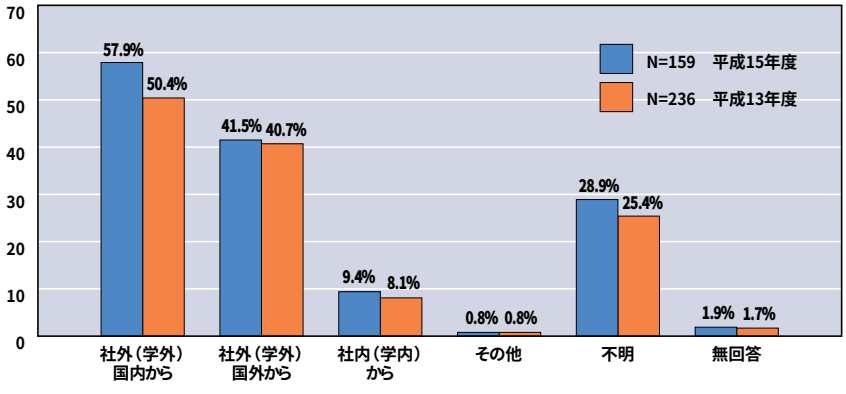
また、米国Information Security Magazine(参考4)の2002年度の調査結果を見ると(グラフ2)、調査に回答した

■表1　個人情報の漏洩が問題となった事例

エステティックサロンのサイトにアクセスして資料請求やアンケートに回答した人の個人情報約3万8千件が閲覧可能な状態になっていた
「サーカム」ウイルスに感染したコンピュータから顧客情報が流出した。(平成13年7月)
化粧品会社がネット上のサイトで管理していた顧客リストが不特定多数から閲覧できる状態になり、約1万人分のリストが漏洩した。(平成13年7月)
オンライン通販会社が、ホームページが使用しているコンピュータに顧客情報を保管していたため、数万件の顧客情報リストが漏洩し、ネット上に流れた。
商品キャンペーンの電子メールリストの登録者約3万3千人に誤ってコンピュータウイルスを添付した電子メールを配信した。(平成13年5月)
電話会社の職員がコンピュータ端末を不正に操作して電話加入者の情報を光磁気ディスクに記録し、イベント企画業者に渡して謝礼を受け取った。(平成12年9月)
京都府宇治市のシステム作りに携わった会社のアルバイト社員が、住民基本台帳のデータ約21万件分を不正に入手して売却した。(平成12年5月)

出典：警視庁サイバーポリス発表資料より

■グラフ1　不正アクセスなどのアクセス元



出典：警視庁、平成15年度不正アクセス行為対策の実態調査

■表2　セキュリティーインシデントを受けた比率

インシデント全体の件数ごとの比率

（パーセント）	1～5件	6～10件	11～30件	31～60件	61件以上	不明
2003年（N=356）	38	20	16※	0	0	26
2002年（N=321）	42	20	8	2	5	23
2001年（N=348）	33	24	5	1	5	31
2000年（N=392）	33	23	5	2	6	31
1999年（N=327）	34	22	7	2	5	29

外部からのインシデントの件数ごとの比率

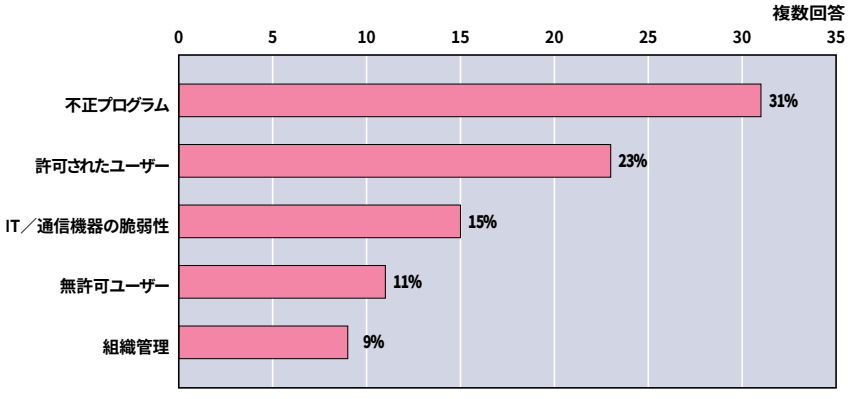
（パーセント）	1～5件	6～10件	11～30件	31～60件	61件以上	不明
2003年（N=336）	46	10	13※	0	0	31
2002年（N=301）	49	14	5	0	4	27
2001年（N=316）	41	14	3	1	3	39
2000年（N=341）	39	11	2	2	4	42
1999年（N=280）	43	8	5	1	3	39

内部からのインシデントの件数ごとの比率

（パーセント）	1～5件	6～10件	11～30件	31～60件	61件以上	不明
2003年（N=328）	45	11	12※	0	0	33
2002年（N=289）	42	13	6	2	1	35
2001年（N=348）	40	12	3	0	4	41
2000年（N=392）	38	16	5	1	3	37
1999年（N=327）	37	16	9	1	2	35

※2003年は「11件以上」の数値を示す　　出典：2003 CSI/FBI Computer Crime and Security Surveyより

■グラフ2　ITセキュリティで最も重要な問題点は？



出典：The 2002 Information Security Magazine (ISM) surveyより

2196社中全体の31パーセントが、ITセキュリティーで最も重要な問題点はウイルスやトロイの木馬などの「不正プログラム」であると答えている。これは近年のウイルス感染の状況から容易に推測できる。ところが、日本で一般的に問題だとされる「無許可ユーザー」が問題であると答えたのはわずか11パーセントであり、その倍以上の23パーセントがアクセス権利を持つユーザーや従業員が問題であるという驚きの報告が出ている。

内部犯罪も性悪説で対抗

これらの調査報告からわかるとおり、企業にとって内部向けの対策の必要性が大きくなっている。これら内部問題は、設定ミスや内部犯罪など人間に起因するものが大多数であるために、セキュリティーポリシーを規定することでシステムの運用管理の手順を明確化し、モラルを向上させる努力が必要である。特にポリシー策定後は、現状に即したポリシーのメインテナンスや、従業員に対して教育を施すことにより情報セキュリティーに対する意識を向上させるなどの運用維持のための努力をしなければ、内部でのインシデントはなくならないだろう。

また、中途採用が常識の時代になり、企業モラルが低下する現状では、性善説に基づいた対策は際立った功をなさなくなってきている。社員のミスによる危険な設定を安全に自動修正する技術や、社員によって組み込まれたハッキングツールを検出する技術や、社員がその職権を悪用して機密データを外部に持ち出すことを防止する技術など、もはや性悪説に基づいて内部犯罪を技術的にコントロールする時期に来ていると言えよう。

【参考1】警察庁サイバーポリスのウェブサイトでは、ハイテク犯罪・サイバーテロの未然防止および被害の拡大防止を図るべく、ネットワークセキュリティーに関するさまざまな情報を提供している。
URL http://www.cyberpolice.go.jp/

【参考2】NPO日本ネットワークセキュリティ協会（JNSA）では、現在20近いワーキンググループが活動を行っているが、前年に引き続き、情報セキュリティーインシデント被害調査をプロジェクトとして行った。
URL http://www.jnsa.org/active1a.html

【参考3】米国の情報セキュリティー教育機関であるComputer Security Instituteでは、毎年FBIと協力して、全米の企業に対して情報セキュリティー調査を実施している。
URL http://www.gocsi.com/

【参考4】米国の情報セキュリティー情報会社であるInformation Security Magazineでは、毎年、全米の企業に対して情報セキュリティーの調査を実施している。
URL http://www.infosecuritymag.com/

漏洩してからでは手遅れだ
情報管理の大原則と具体的対策

大原則はポリシーなどによる運用面での対策

昨今顕在化してきた「内部犯行」だが、いまだ、表沙汰にせずに組織内部で処理されることが多い。内部犯行が露呈した例をいくつか挙げるが、こうした事例は氷山の一角に過ぎない(右)。では、内部犯行に対してどのような対策を、企業や組織はとることができるだろうか?

対策には2とおりのアプローチが考えられる。1つはソフトウェアやツールによる対策、もう1つは情報セキュリティーポリシーの策定・運用を中心とした運用面での対策だ。ソフトウェアなどによる、個別の犯行パターンに対する対策については105～107ページで解説するが、これはあくまでも個別の対応でしかない。情報漏洩を適切に防いで企業活動を継続するためには、セキュリティーポリシーや日々のチェックなど、運用面での対策が大原則となる(102～104ページ)。

事例:顧客になりすました不正送金

2002年5月10日、警視庁ハイテク犯罪対策総合センターと武蔵野署は、インターネットバンキングを経由して約370万円をだまし取ったとして、シティバンクの元派遣社員を不正アクセス禁止法違反、私電磁的記録不正作出・同供用、および電子計算機使用詐欺などの容疑で逮捕した。逮捕された人物は、同行のカスタマーサポートサービスに従事していた当時、口座の暗証番号に生年月日が使われることが多いことに目を付け、口座開設者の口座番号などの個人情報をメモしておき、暗証番号として生年月日が使用可能な顧客2人を特定した。そして、顧客になりすまし、勝手にインターネットバンキングの利用登録を行い、他人名義の銀行口座に不正に送金したのだ。

■情報漏洩、および内部犯行の事例

日付	概要
2003年6月26日	大手コンビニエンスストアであるローソンの発行するカード会員約56万人分の氏名、住所などの個人情報が社外に流出
2003年6月11日	海上保安庁の職員が勤務中に職場のコンピュータを使用し、インターネット上の掲示板に書き込んでいたことが判明。同庁は内部調査を行い、書き込みを行った職員を特定し、口頭で厳重注意を行った
2003年6月9日	神戸市に本店のある富士信用組合は、本店の元融資部課長代理が、兵庫県内の法人や個人の手形不渡り情報計3515件を無断でフロッピーディスクにコピーし、大阪市内にある消費者金融業者に渡したとして、窃盗容疑で生田署に告訴
2003年1月23日	顧客7人の口座番号と貯金残高を探偵事務所の従業員に教え、その見返りとして金銭を得たとして、さいたま市の浦和田島郵便局職員を再逮捕
2002年12月19日	エステティックサロン大手のTBCを経営する「コミー」が管理する5万人余の個人データが流出した問題で、迷惑メールやいたずら電話で被害を受けた10人が同社を相手に総額1,150万円の損害賠償を求める訴えを起こす
2002年12月4日	三重県四日市市で、市の職員が住民情報オンラインシステムを使用し、住民の個人情報を不正照会した疑いが出ている問題で、四日市市は、「市の独自捜査では限界がある」として不正アクセス禁止法違反の疑いで、職員を特定しないまま四日市南署に告発
2002年10月25日	大分医科大の男性教授が部下の女性技官の電子メールを無断で閲覧していたことが発覚し、同大はこの教授を6か月の減給処分に、また、この教授とは別に、職員9人のパソコンに侵入した男性技官を戒告処分にしたと発表

情報漏洩対策を急務にする個人情報保護法

2003年5月23日、個人情報保護法(個人情報の保護に関する法律)が成立した(右表)。施行はまだ先になるが、対象となる規模については「5000人分以上の個人情報を保持する者」という指針が出ている。

これまでは消費者の個人情報は「顧客情報」として組織の財産とみなされることが多かった一方で、蓄積された顧客情報の取り扱いに関する不透明感が存在した。子供が会社に入社したら「フレッシャーズフェア」としてスーツの購入をすすめるダイレクトメールが送られてきたといった経験がある人も多いだろう。また、顧客情報以外にも組織の従業員情報が個人情報とみなされる可能性がある点にも注意してほしい。従業員名簿はもちろんのこと、履歴書、給与データ、住所届などは「インハウス情報」と呼ばれ、個人情報として扱われるのだ。

個人情報保護法にも罰則が設けられている。違反した行為の被害を受けた個人などから、その事業者を監督する主務大臣に通報が行われると、是正の勧告ないし命令が行われ、改善がみられない場合は、6か月以下の懲役または30万円以下の罰金に処せられる。

■個人情報保護法の概要

法律の要旨	個人情報を保持している企業や団体に対して、個人情報を漏えい、毀損などのないよう、適切に管理することを義務付けるもの
対象となる組織	個人情報データベース等を事業の用に供している者
個人情報の定義	生存する個人の情報であり、この情報に含まれる氏名、生年月日などの記述により、特定の個人を識別することのできるもの
法律の対象の組織に課せられる義務	利用目的の特定と明示
	本人の同意なく、目的外の利用に個人情報を使用することを禁止
	偽りやその他不正な手段をもって個人情報を取得することを禁止
	従業者、および委託先の監督
	本人から個人情報の開示請求があった場合は、それを開示しなければならない
	目的が公表されていない場合、もしくは、不正な手段をもって個人情報を取得された場合、本人の要求に応じてそのデータの停止または消去をしなければならない

情報セキュリティーポリシーで組織の情報資産を守る
ISMSやBS7799などの認証は「取得」がゴールではない

内部犯行も含め、情報セキュリティーの確保のためには、情報セキュリティーポリシー（単純に『セキュリティーポリシー』とも呼ばれることもある）の策定と運用が効果的である。情報セキュリティーポリシーとは、各組織の情報システムの利用者の情報セキュリティーに対する意識向上はもちろんのこと、利用者個人の裁量だけで情報の扱いが判断されることのないよう、組織として意思統一され、明文化された文書のことである。

たとえば、コンピュータウイルス対策ソフトウェアは、コンピュータにインストールしただけでは意味がなく、常に最新の状態を保てるように、アップデートを繰り返すことで最大の効果を得ることができる。日々、新たに生まれているコンピュータウイルスを検出し、駆除することができないからだ。では、アップデートはどのくらいの頻度で行えばよいのであろうか？　組織内でこれを行っている頻度や期間は、従業員によってまちまちであることだろう。そこで、「コンピュータウイルス対策ソフトウェアのアップデートは毎週水曜日に必ず1回行う」といったように規定として定め、その周知徹底を従業員に対して行うことで、組織の意識統一を実現できる。この「規定」の集合体が情報セキュリティーポリシーである。

情報セキュリティーポリシーに『情報』という接頭辞が含まれるのには理由がある。組織には、顧客情報から会議の議事録、新製品の設計書などが存在するであろうが、これらは共通して情報であり、資産でもある。こうした情報資産を保護するための規約集が、情報セキュリティーポリシーなのだ。

組織の情報セキュリティー管理にかかわる規格が存在している。そのうちのいくつかを表に示す。ISMS認証やBS7799については、なんとなく耳にしたことのある読者も多いことだろう。情報セキュリティーポリシーを策定して適切に運用することでこうした規格の認定を取得することで、組織の内外に対してセキュリティー管理状態の高さのアピールになるという効果を得ることができるのだ。

こうした認定の取得を中心とした情報セキュリティーポリシー策定のためのサービスを提供している企業は多いので、外部コンサルタントなどと協力してポリシーを作り上げていくことになるだろう。ただ、間違ってはいけないのは、情報セキュリティーポリシーは、「認定を取得するためのもの」ではないということだ。

■情報セキュリティー管理にかかわる認証規格や制度

規格名	概要
ISO/IEC15408	ハードウェアないしソフトウェアを含むセキュリティー製品と、システムの開発や製造、運用などに関する国際標準。ITSEC（Information Technology Security Evaluation Criteria）やCC（Common Criteria）とも呼ばれ、同義で扱われる。 URL http://www.jisc.go.jp/
ISMS	Information Security Management System の略称。正確には「ISMS適合性評価制度」と呼ばれる。情報処理サービス業事業者に対する評価認定制度の1つ。技術的な詳細ではなく全体としてのセキュリティー管理体制を扱う。 URL http://www.isms.jipdec.or.jp/
BS7799	BSI（British Standards Institution：英国規格協会）によって規定されている、企業および団体向けの情報システムセキュリティー管理のガイドライン。ISO/IEC15408と並んで現在最もポピュラーなセキュリティーの規格。 URL http://www.bsi-j.co.jp/
プライバシーマーク	通商産業省の個人情報保護ガイドラインに準拠して個人情報の取り扱いを適切に行っている民間事業者に対して「プライバシーマーク」の使用を認める制度 URL http://privacymark.jp/

責任者自ら情報の価値を判断してポリシーを策定する
「丸投げ」で策定されたポリシーは形骸化する

「きみ、明日からこれをやってくれ」という一言だけで、方針や方策については一切関知しないという「丸投げ」的な仕事の依頼は日常茶飯事だろう。組織の情報資産を保護すべく行われる情報セキュリティーポリシーの策定と運用においても、「ISMS認証を取得したいので、情報セキュリティーポリシーを作ってくれ」という一言だけで、ポリシー策定の仕事全体が丸投げされることがあるが、これは本質を見失った誤りである。

「情報セキュリティーは技術的な問題である」として技術担当部門に情報セキュリティーについての懸念事項が持ち込まれることは多い。確かに、昨今の情報ネットワークテクノロジーの発達はすさまじいものがあり、技術的な裏付けなしに具体的な対応を行うことが難しい。

しかし、技術的な対応を行う前に「どの情報に資産価値があり、どの程度のリスクが存在し、そうしたリスクからどの程度の保護を行う必要性があるのか」を明確にする必要がある。すべての情報を完全に守ることはリスクとコストのバランスに問題があるし、このステップなしに技術的な対応を行っても、現場任せの場当たり的な対処になり、せっかくの情報セキュリティーポリシーが形骸化してしまうことは目に見えている。

組織の保持している情報資産と、直面しているリスクの評価を行うことは、経営方針や組織の戦略に密接にかかわってくる重要な問題であり、事業者自らが判断を行い、定めるべきである。情報セキュリティーポリシーは、その結果を受けて作られるものなのである。

情報セキュリティーポリシーの作成を検討しているならば、できれば、情報セキュリティーの課題に事業者自らがリーダーシップをとって取り組んでいるということを、従業員の前で宣言していただきたい。そうすることだけでも、情報セキュリティーポリシーの策定と運用に関する促進剤として働いてくれるはずである。

実際の運用を考慮して現実的なポリシーを策定する
厳しすぎる規定がポリシーをダメにする

情報セキュリティーポリシーの策定が終わり、いざ運用のフェーズに移ったとして、規定を守らない従業員の姿が目につく。なぜと思うこともあるだろうが、実際には実現することが難しい規定が定められていることも多々ある。
ありがちなのは「パスワードに関する規定」である。パスワードは基本的に複雑なものを使用し、かつそれを覚えることが最も良い、高い機密性が求められるものであることはもはや周知の事実だろう。しかし、これを規定としてただ単に「パスワードを複雑なものにし、それを覚えること」としてしまうと現場とのギャップが発生する可能性がある。
組織内の根幹をなすルーターのような重要機器が停止し、業務に大きな影響を生じたとする。ここで、ルーターを管理する技術部門の担当者が、たまたまその日は休暇を取っていたとしよう。パスワードは情報セキュリティーポリシーによって複雑であり、規定によってメモなどには書かれていない。担当者の携帯電話に電話を入れてみるが、応答がなく、そうしている間にも刻一刻とロスが発生していく。これは組織内での例だが、電子商取引サイトのインフラ部分で発生した場合は、より損害が大きくなることは容易に想像できる。
こんなケースを情報セキュリティーポリシーの策定の際に想定しておけば、重要なシステムや機器の管理用のパスワードは紙に書いておき、それを鍵付きの保管庫に入れ、厳重に管理する、といった別枠の規定を設けておくこともできたであろう。ポリシーは運用するためにあるのだということを忘れてはいけない。

ポリシーは「新しい制限事項」ではない
運用の現場との対話が生み出すセキュリティーポリシーの理解

情報セキュリティーポリシーの策定に際しては、さまざまな部署の従業員を参加させ、各規定に対する意見を求めることが必須だ。ただ、利便性を損なうからといって従業員が反対しかねない規定もあるだろうが、それは実行できないというわけではなく、「今まで」とのギャップを感じているという意思表示に近いだろう。そうした場合には、意見に耳を傾けながらも、その規定によって保護される情報があり、それが組織全体に対して重要な意味をなすということを根気強く説明することがよいだろう。
残念ながら、こうした対話が従業員との間で行われることはまれである。情報セキュリティーポリシーは「新しい制限事項」として従業員の間に受け入れられてしまう恐れがある。そうではなく、組織と経営環境である社会との関係を考えれば、情報化が進む社会の中で情報セキュリティーは今後果たすべき役割として重要な位置を占めており、その責任が従業員1人1人にかかわってくることについて理解できるはずだ。そういったことまで含めて現場の従業員と対話を行うことが、そうした誤解を解きほぐすことになるだろう。

情報セキュリティーは戦略として捉える
「後ろ向き」ではない、組織の責任としての経営課題

情報セキュリティーは、組織内の体質や風土を改革するための柱となるものである。特に「コンプライアンス」と呼ばれる組織内での倫理や規定の遵守については、個人情報保護法の登場で急速に重要課題となりつつある。これまでは、そうした倫理や規定については組織内の一部門の問題として捉えられ、場当たり的な処置で対処されてきた。情報セキュリティーに対する投資も、個々の問題の解決策のためだけにある「利益を生まない後ろ向きの投資」とみなされてきた。
しかし、情報漏洩に代表されるような、組織の不祥事が明らかになれば、社会からは、果たすべき責任を怠っているとみなされる。また、「組織のため」という名目で暴挙ともとられかねないことをやろうとする「憂国の士」の従業員がどの組織にも存在していることだろう。こうした従業員も含めて、倫理と規定について議論する、または対話を行うような場を作る、または、外部から講師を招聘して教育してもらうことは、はたして後ろ向きの投資だろうか？
「憂国の士」は必ずしも組織にとって毒ではない。むしろ、問題に対して率先垂範で改善を考えている人材であり、彼らを巻き込んで従業員の意識改革に取り組むことはこの上ないことではないだろうか。
最近では、情報セキュリティー投資評価（Return On Security Investment：ROSI）という指標が生まれており、「投資によって、どれだけ効果的なセキュリティーを実現するか」を計るための指針となるものとして注目を集めている。すなわち、コスト効果に優れたセキュリティー対策を実現するための方策ができつつある。
「異常なし」というのは、あたりまえのことのように思える。また、「なにも起こらない」ことに投資をしたとしても、費用対効果が非常に見えづらい。それでも、組織が大きくなれば大きくなるほど、「なにも起こらない」という確率は確実に下がってくるはずだ。そして、「困ったことが発生しました」ということが伝達しにくい組織風土もまた、組織の大型化に伴って生まれやすい。
情報セキュリティーを経営課題とみなし、それを戦略的に位置付けることが、IT化社会のなかで組織が責任を果たしていくうえでの基本となるのである。

情報漏洩対策チェックリスト

情報漏洩全般に対するセキュリティー対策でチェックしておくべき20項目を挙げておく。
主に情報を扱う業種であれば、1つでもチェックが漏れていれば、情報セキュリティーポリシーの策定、または見直しを検討するべきだろう。

● ネットワーク

- ☐ 会議室に、誰でも使える空いたネットワーク接続口はありませんか？
- ☐ メーカー出荷状態のままで使っている無線LANはありませんか？
  また、無線LANの暗号化キーは定期的に変更していますか？
- ☐ 社内LANの盗聴チェックは行っていますか？
- ☐ 退職者のネットワークやメールのアカウントは即時に停止するルールがあり、実行されていますか？
- ☐ メール監視の抜き取りテストやPC管理状態の抜き打ち検査をしていますか？
  また、していることを皆が知っていますか？
- ☐ 仕事の持ち帰りで自宅アドレスにメールでファイルを送っていないですか？
- ☐ テストデータに「生データ」を使っていないですか？
- ☐ ウイルスが発見されたとき、まず感染したPCのネットワークケーブルを外すことを徹底していますか？

● ドキュメント

- ☐ バックアップメディアはちゃんと保管できていますか？　紛失したことはないですか？
- ☐ 重要な書類は自らシュレッダーに投じていますか？
- ☐ 机の上に書類を出したまま帰宅している人はいませんか？
- ☐ パスワードの書かれた付箋をディスプレイに貼っていたりしませんか？
- ☐ 必要のなくなった個人情報を保管し続けていませんか？

● ルール

- ☐ 高性能カメラ機能付き携帯電話の持ち込みは、制限していますか？
- ☐ 業務分掌の中に情報セキュリティー対策としての責任が明記されていますか？
- ☐ 機密保持をテーマとした教育や訓練は行われていますか？
- ☐ 懲罰規則は、皆が知っていますか？
- ☐ 清掃会社との機密保持契約は、大丈夫ですか？　無人状態での清掃はありますか？
- ☐ システム会社との機密保持契約は、大丈夫ですか？　無人状態での作業はありますか？
- ☐ 職場の同僚は、会社への不満を募らせていませんか？

Note：ここからは、技術的な対策をいくつか紹介していくが、必ず前述のように経営戦略として情報セキュリティーをとらえていくことを実行してから、こうした対策について検討していただきたい。

機密文書がCD-Rで持ち出された
圧倒的に多いメディアによる流出

［インシデント］

機密文書は、紙媒体だけでなくCD-R、MO、フロッピーディスクにコピーして持ち出されることがある。情報を売却することを目的にした故意に加えて、自宅に持ち帰ろうとした仕事の書類が入ったカバンをなくした、といった過失も含まれるため、こうした持ち出しによる情報漏洩は圧倒的に多い。

［防御策］

DRM（Digital Rights Management）を使うのが1つの対策となる。DRMは、もともとは音楽や映像を配信する際の著作権保護のために利用されてきたもので、暗号化とアクセス権の管理を併用することで、不正コピーを防止できる。このテクノロジーを利用して、デジタル文書の閲覧、印刷、変更、コピー、それからデスクトップのキャプチャーなどを防ぐことができるのだ。

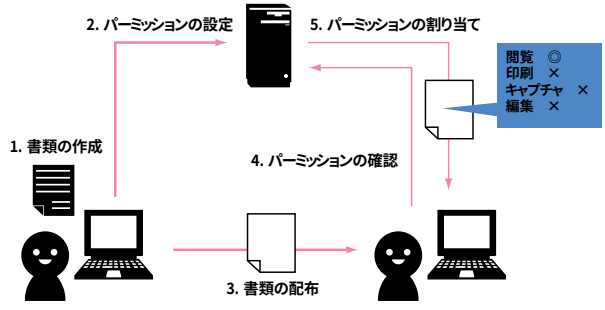
中でも一番注目されているのが、この夏から提供が開始される予定の、マイクロソフト社のRMS（Windows Rights Management Services）である。RMSは次期Office製品のOffice 2003で作成された文書に対して印刷、変更、コピーなどの許可／不許可（パーミッション）を設定し、ユーザーごとのアクセス権限を設定できる（図）。

こういった製品を利用することで、デジタル文書を印刷して持ち出す、あるいは、フロッピーディスクなどに収めて持ち出すといった犯行が行われる可能性を低くすることができる。

紙媒体の情報は持ち出しを防ぐための物理的な保護手段が必要だということは周知の事実だが、同様に、個人情報などにアクセスできるオペレーターの端末に接続されているフロッピーディスクやMOなどのドライブはリスクにつながることを理解すべきだ。

また、最近ではデジカメやカメラ付き携帯電話を使った犯行がある。技術的な対策としてはレンズを覆うことや、オフィス内に監視カメラを設置することぐらいしかできないので、基本的には情報セキュリティーポリシーなどのルールで持ち込みを禁止するしかない。特に、高性能化したカメラ付き携帯電話はデジカメなどよりもはるかに「さりげなく」情報を持ち出せるので、情報が命の組織では対策が必要だ。

RMSが稼働するシステム



従業員がメールの盗聴をしていた
現状では情報を裸で送っているに等しいメール

［インシデント］

メールの盗聴には、ネットワーク上を流れるデータを取得する「スニッファー」と呼ばれるプログラムが使われる。メールは基本的に暗号化されていないため、スニッファーを使うことでメールを盗聴して、本来中身を知り得ないはずの情報を入手できるのだ。

［防御策］

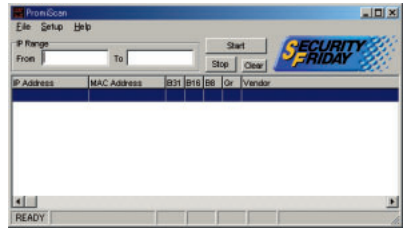
セキュリティーフライデー株式会社 URL がフリーで提供している「PromiScan」（図）を使えば、スニッファーを実行しているシステムを検出できる。スニッファーを実行しているシステムが特定のパケットに対して応答することを利用して検出を可能にしている。また、こうしたツールを使うだけでなく、情報セキュリティーポリシーでスニッファーの利用禁止と、不定期にスニッファーの検出が行われることを明示することで、さらに抑止効果も望める。

さらに、PGPなどのメールを暗号化できるツールを使うと、盗聴されることがあっても中身を読まれることはない。相手もメールの暗号化を利用していないといけないのが難点だが、社内でメールの暗号化を使うルールがあれば、比較的重要な書類がメールでやりとりされる可能性の高い社内のやりとりは安全になるだろう。

しかし、これだけでメールの盗聴を防げるわけではない。たとえば、盗聴者がメールサーバーの設定を変更できるシステム管理者であれば、メールの転送設定を変更できるので、重要な情報を扱っている役職者のメールをすべて自分のアカウントに転送できてしまう。このような場合には、なかなか突き止めにくい。

対策としては、まず、メールサーバーを含め、重要なシステムへの物理的な保護を行うことである。そして、こうした重要なシステムで作業が行われる場合は、必ず2人以上の人間で行い、そして要職にある従業員を伴うことを情報セキュリティーポリシーで規定をする。あるまじき行為をチェックするためだ。

URL http://www.securityfriday.com/



メールを使って機密データが外部に送信された
あらかじめ周知したうえでのメール監視が抑止効果を持つ

［インシデント］

前述のDRM製品やRMSを使ったとしても、正規の「それを編集可能な従業員」はコピーなどが可能なため、悪意があれば持ち出されてしまう可能性もある。しかも、持ち出しはフロッピーディスクなどの外部媒体に限らず、メールに添付して送信される可能性もある。

［防御策］

メールによる持ち出しに関しては、通信の監視で対応する。指定されたキーワードがメールの内容に含まれている場合に警告を出す監視ソフトウェアなどがあるのでそれも併用するべきだろう。現在は、メールの監視が情報漏洩の防止の目的のために行われることを事前に組織内に通知してあり、かつその目的に沿った監視を行うのであれば、業務に使用するために提供しているメールシステムでの監視は法的に問題ないというのが一般的な見解だ。監視した内容が記録され、かつ、適切に保管されていれば、たとえメールの本文や添付ファイルに暗号化がなされていても、メールを使って機密データを送信したと疑わしい人間を特定する手がかりになる可能性がある。

公開サーバーを通して個人情報が漏洩した
設定とセキュリティーホールを継続的に確認

［インシデント］

厳密に言えば内部犯行ではない場合が多いが、内部の人間の過失による情報漏洩という点で重要である。公開ウェブサーバーから情報が漏洩する事例が2002年5月を中心に多発した（上表）。外部からのアクセスが可能でファイル一覧を表示できる場所に機密ファイルが存在していた過失が原因だ。また、増加傾向にあるのは、ウェブアプリケーションの「セキュリティーホール※」が原因で、顧客情報にアクセスされてしまう例だ。

［防御策］

情報セキュリティー責任者の任命や情報セキュリティーポリシーといった包括的なアプローチが大前提となる。技術的なアプローチは根本的な解決ではないことを忘れないでほしい。

①不正アクセス対策製品の導入

セキュリティーレベルを向上させ、情報漏洩を未然に防ぐことができる（下表）。

②ペネトレーションテスト（疑似侵入検査）

了解を得て、実際のサーバーやネットワークを不正アクセスの手法で攻撃するテスト。継続的に行うことで、日々発見され続けるセキュリティーホールや設定の不備を検出して対策できる。

※セキュリティーホールとは、システムの停止や侵入を許してしまう、ソフトウェアのバグを指す。

■2002年5月を中心にした公開サーバー経由の情報漏洩事件

日付	概要
2002年5月27日	エステティックサロン大手のTBC（東京ビューティーセンター）のウェブサーバーで、約3万件の個人情報が閲覧可能な状態になっていた
2002年5月27日	建材メーカーであるYKKの子会社、YKKアーキテクチュラルプロダクツのウェブサーバーで、アンケートに回答した約4万5千人分の住所、氏名や年齢、電話番号、電子メールのアドレスなどが閲覧可能な状態になっていた
2002年5月28日	日本大学のウェブサーバーで、通信制大学院の願書を請求した約1800人分の名前や住所などが閲覧可能な状態になっていた
2002年5月28日	日本テレビの関連会社「日本テレビエンタープライズ」のウェブサーバーで、同社の ウェブサイトに寄せられた242人分の意見と、住所や名前などが閲覧可能な状態になっていた
2002年5月28日	全日空の関連会社「全日空ワールド」のウェブサーバーで、パンフレットを請求した約1500人分の住所や名前などが閲覧可能な状態になっていた

■不正アクセス対策に有用なアプリケーション

ファイアーウォール： 外部の信頼できないネットワークからの不正な通信を遮断することで、組織内部のネットワークを保護するシステム	iptables（フリーソフトウェア） URL http://www.netfilter.org/
	FireWall-1 URL http://www.checkpoint.com/products/protect/firewall-1.html
	Microsoft Internet Security and Acceleration Server URL http://www.microsoft.com/japan/isaserver/
	NetScreen URL http://www.netscreen.com/products/datasheets/
	Cisco Secure PIX Firewall URL http://www.cisco.com/japanese/warp/public/3/jp/product/product/security/pix/
IDS： Intrusion Detection System。侵入検知システム。通信を監視して、不正アクセスの可能性のあるものを検知し、警告を発するシステム	Snort（フリーソフトウェア） URL http://www.snort.org/
	Cisco Secure IDS URL http://www.cisco.com/japanese/warp/public/3/jp/product/product/security/ids/
	ISS RealSecure URL http://www.isskk.co.jp/enterprise.html
	Dragon IDS URL http://www.enterasys.co.jp/products/ids/
ウェブアプリケーション保護ソフトウェア： ウェブアプリケーションのセキュリティーホールを利用したと思われる攻撃を検出し、遮断するソフトウェア	AppShield URL http://www.shield.ne.jp/appshield/
	SecureIIS URL http://canon-sol.jp/product/si/
	InterDo URL http://www.dit.co.jp/kavado/interdo.html
	guard3（フリーソフトウェア） URL http://www.trusnet.com/tools/guard3/
	URLScan（フリーソフトウェア） URL http://www.microsoft.com/japan/technet/security/tools/tools/locktool.asp
整合性確認ソフトウェア： ファイルシステムの整合性を確認し、ファイルの改ざんや上書きを検知し、警告を発するソフトウェア	TripWire URL http://www.tripwire.co.jp/
	WinInterrogate（フリーソフトウェア） URL http://winfingerprint.sourceforge.net/wininterrogate.php
	YAKITORI（フリーソフトウェア） URL http://www.yakitori.biz/

紛失したノートパソコンから情報が漏れた
パスワードや暗号化による事前の対策をポリシーで規定

[インシデント]

重要な案件のファイルが詰まっているノートパソコンをうっかり紛失してしまうこともある。パスワードでロックがかかっていても、入手したノートパソコンからハードディスクを取り出して、別のコンピュータに接続すれば、パスワードがなくても中身を読み出せてしまう。

[防御策]

①パスワードによる保護

ノートパソコンを携帯して持ち歩く場合には、最低限OSレベルでのパスワードによる保護を行っておく必要がある。面倒だからと言ってパスワードなしでログオンできるようにしていると、拾ったノートパソコンの電源を入れるだけで、そのノートパソコンの内容をすべて読み取ることができてしまい、大幅に危険性が増す。

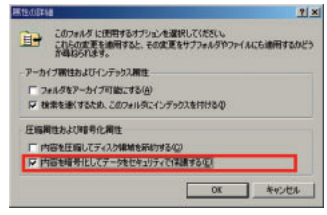
同時に、BIOSレベルでのシステム起動用のパスワードを設定しておくとさらによい。製品によってはハードディスクのロック機能を兼ねていて、ハードディスクがノートパソコンから抜き取られてもその内容を閲覧できなくなる。従業員が使用するノートパソコンの選定時にはこの点も考慮するとよいだろう。ただし、そうした製品を購入しても、ハードディスクのロックを設定し忘れればまったく意味がないので、情報セキュリティーポリシーなどで規定することが望ましい。

②OSの標準機能による暗号化

Windows 2000から、暗号化ファイルシステム(Encrypting File System:EFS)と呼ばれるファイルとディレクトリーの暗号化機能が実装された。この機能は、公開鍵暗号方式をもとにしており、秘密鍵なしではデータを読み出せない。

ファイルやフォルダーを右クリックして[プロパティ]を選択し、[全般]タブの[詳細]ボタンを押し、[内容を暗号化してデータをセキュリティで保護する]のチェックボックスをオンにする(図)。機密データ用のフォルダーを新たに作成し、そのフォルダーにEFSを適用しておくことで、このフォルダー内に新規に作成されるファイルとフォルダーはすべて暗号化されることになる。これで、ハードディスクを抜き出されてしまったとしても、データが暗号化されているのでかなり安全である。

どちらも「事前に行うべき対策」であることは言うまでもない。情報セキュリティーの管理では、「転ばぬ先の杖」が常に必要となってくるのだ。



使用済みのハードディスクに残っていた情報が漏れた
使い終わったPCのハードディスクはツールを使って抹消処理をする

[インシデント]

2002年1月16日、福岡県警の内部データが残ったままの中古パソコンがリサイクルショップで販売されていたことが判明した。福岡県警職員の私物で、データを消去しないまま廃棄を販売店に依頼したところ、そのまま流れたということだ。これは過失によるものだが、データを削除しても、ハードディスク上では削除マークが付いて見えなくされるだけで、実はデータはそのまま残っている。市販のデータ復旧ソフトウェアを使えばデータを取り出せる可能性があるのだ。フォーマットして備品として管理されているハードディスクでも、持ち出されれば情報漏洩につながりかねない。

[防御策]

備品のハードディスクでも、内容を完全に消去することが望ましい。

①市販のソフトウェアを使う

市販されているデータ削除ソフトを使えば、ハードディスクの内容を完全に消去できる。消去の方式はさまざまなものがあるが、どれを利用しても特に問題はないだろう。

②ウィンドウズ付属のツールを使う

cipher.exeは、Windows 2000 SP3以降やWindows XPで利用できるNTFSファイルシステム用のユーティリティーである。cipherにワイプスイッチ(/W)を付けて実行すると、まずすべてゼロを書き込み、次にすべて1を書き込み、最後にランダムなデータを書き込むことで、ディスクの内容を完全に消去する。消去対象のハードディスクを2台目のハードディスクとして接続して、空のNTFSパーティションを作ってから、このドライブを消去する。たとえば、D:ドライブのデータを消すには次のようにする。

```
C:\> cipher /W:D:\
```

③入退出の記録

備品管理だけでなく、休日出勤や残業時の手続きでも、従業員がオフィスにいることを記録できることが望ましい。カードキーなどによる物理的な保護をしても、その記録が残っていなければ、問題が表面化した際の手がかりが消えてしまう。

怨恨などの理由で、休日出勤や残業を装って同僚のハードディスクからメールの内容などの情報を取り出す従業員がいた場合、その入退出の記録が後からの調査に役立つ。同様に、備品の倉庫として使用されている部屋にも物理的な制限を行い、入退出の記録をとっておくことが望ましい。

経営者が積極的に参加すべきコーポレートガバナンス

プロに聞くポリシーの策定・運用から得た教訓

三位一体で運用するセキュリティーポリシー

最後に、実際のビジネスの現場における情報セキュリティーの現状について見てみよう。

企業活動における情報リスク分析とそのセキュリティー対策に関しては、情報関連企業で構成される「情報サービス産業協会」URL 01 という団体で議論が重ねられてきた。

「そこで、情報リスクを脅威の観点からどのように分類するかについても検討してきたのですが、その結果大きく“人為的か環境的か”“意図的か偶発的か”という2つの軸に従った分類方法を採用しました」（某メーカー系企業セキュリティー担当者）

具体的には、(1)人為的で意図的（不正／犯罪）、(2)人為的で偶発的（人的エラー、誤操作、過失）、(3)環境的で偶発的（障害、災害）という分類になる。

そのうちの「人為的で意図的」なリスクが、ここ1年くらい増加してきているという（表）。

そういったリスクの回避・低減の具体的な方策としてまず考えられるのが、セキュリティーポリシーの策定だ。とはいっても、単にセキュリティーポリシーを作ればいいというものではもちろんない。

「重要なのは情報管理、セキュリティー技術、人的体制が『三位一体』となって運用されることなのです。しかし現状ではまだ、それぞれが『島』の状態で、必ずしも有機的に運用されているとは言えません」（前出のセキュリティー担当者）という言葉が象徴しているように、現実にはまだビジネスの現場レベルでの意識が低いため、多種多様なリスクの存在に対する想像力に欠けているというのが正直なところだと言う。日本では「水と安全はタダ」という神話が、まだまだ神通力をもっているようだ。

そのためか、最近では外資系企業を中心に、社員のリスク意識を高めるために、入社契約時にセキュリティーについての厳格な取り決めを明示するケースが増えていると言う。たとえば、「もしあなたが契約に違反して内部情報を漏らした場合、会社は必ずあなたを裁判に訴えます」というようにである。あるいは実際に、「この情報が流出したら1件あたりいくらの損害になる」ということを、具体的金額を示しながら意識を高めていくということも有効かもしれない。

実際にセキュリティーポリシーを「運用する」ということ

そんな中、策定したセキュリティーポリシーを形骸化させない有効な手段として、最近注目されているのが、国際標準に則った情報セキュリティーマネジメントシステムである「ISMS（Information Security Management System）」だ。

これは、「個別の問題ごとの技術対策のほかに、組織のマネジメントとして、自らのリスク評価により必要なセキュリティーレベルを決め、プランを持ち、資源配分して」システムを運用するための評価制度である URL 02 。

株式会社LAC　JSOC事業本部・セキュリティー担当部長　斉藤稔氏

そのISMSを、取得決定からわずか半年で認証にこぎつけたのが、（株）LACのセキュリティー構築・運用サービスを担当するオペレーションセンター、JSOCである。同社JSOC事業本部・セキュリティー担当部長である斉藤稔氏は、ISMSと情報漏洩対策についてこう語る。

「当社の場合、データごとのアクセス制限はもちろん、離席時には自分のマシンへのスクリーンロックを義務付け、プリントアウトした書類には必ず機密度に応じたスタンプを押印するなど、とにかく情報管理の細かい部分にまで規定を設けています」

セキュリティー関連の業務は社内に設けられた20名の幹部社員で構成される「セキュリティー委員会」が担当する。そこから随時、セキュリティーポリシーの改訂情報などが発信されている。情報は基本的にすべて「Living Policy」という同社が販売もするウェブベースのグループウェアを介して受発信されている。そこから情報確認の指示メールを出したり、実際に社員

■洗い出し、特定されたリスクのまとめ

		洗い出した（発見した）リスク	特定したリスク	備考
人為的	意図的	43%	39%	不正・犯罪
	非意図的	39%	50%	不正・犯罪の一部、人的エラー、障害
偶発的		18%	11%	災害

出典：情報サービス産業協会　平成14年度 情報サービス業におけるリスクマネジメント調査報告書

が情報を閲覧したかどうかも確認したりできるのだという。

「さらに当社は業務柄24時間で動いていますから、パソコン、デスク、ファクスからホワイトボード上の板書まで含め、およそ目に見える箇所すべてに、情報が放置されていないかチェックしています」（斉藤氏）

しかし、内部情報漏洩でもっとも警戒するのは、社員の退社時だという。

「実際にはもう辞めているのに、企業によってはしばらく前のアカウントを残しておくところもまだあるようですが、その時期がいちばん危ないんです。外部の端末からそのアカウント経由で内部データを閲覧して……などというリスクは当然あるわけです。ですから当社では、退社したらもうすぐにそのアカウントは削除するようにしています」（斉藤氏）

こうしたISMSに沿ったきめ細かいセキュリティーマネジメントを運用していくことは、かなり有効だと斉藤氏は言う。一方で、すべての情報漏洩を100パーセント防げるわけではなく、意図的な内部犯行を防止するのは、社員の意識しかない、とも言う。

そして「情報漏洩はある」という前提に立ったとき、重要になるのは「余分な情報をもたないということと、漏れた情報を追跡できるシステムをもつこと」（斉藤氏）なのである。

経営トップの積極的参加なくして情報リスク対策なし

ただし、そういった取り組みが作業を担当する現場レベルにとどまっている限り、いくらポリシーを作っても、苦心してISMSを取得しても、実はまったく意味がない。冒頭のセキュリティー担当者は、こうも言っている。

「結局この情報セキュリティーについては、『どのリスクまでは許容し、どのリスクはきっちり回避する』といったコストとのトレードオフに関する判断を含めて、最終的にはコーポレートガバナンスの問題だと思っています」それは結局、「経営トップの積極的参加なくして情報リスク対策なし」ということである。

しかし、実際にすべての経営者が情報リスクについてきちんと理解し、効果的運用に協力的かというと、そこもまだまだ改善の余地があるようだ。別の情報系企業のセキュリティー担当者は、ISMSを引き合いに出してこう語る。

「ひとくちにISMS取得と言っても、取得後の現実運用と、そもそもこちらが大きかったりするのですが、入札時に有利な材料となるなど、ISMSがもたらすメリットに対する経営トップの営業的思惑のギャップに悩んでいるところは多いのではないでしょうか」

つまり、せっかく取得したISMSが、単なる営業ツールとしてしか機能しないケースがあり得るのだ。前出のセキュリティー担当者が続ける。

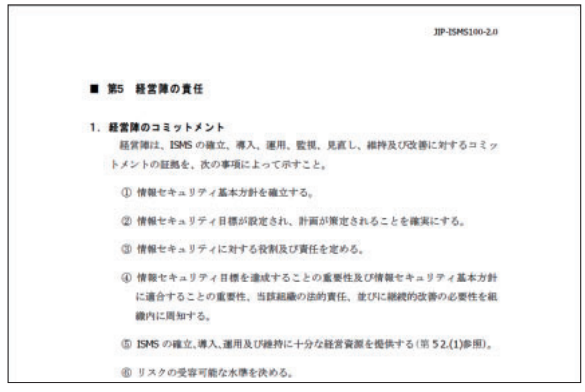
「いくらISMSへの作業協力をお願いしても、ボトムアップだと結局最後には『わかったけど、とりあえずそれはそっちでやっておいてくれ』で終わってしまうんです。そういう場合は、外部コンサルタントなりを呼んできて、まったくの第三者的見地から事の重要性を説いてもらうしかないのかもしれないですね」

そのISMSだが、これまでのVer.1.0は2004年9月いっぱいで廃棄され、その後はVer.2.0へ移行することが決まっている（Ver.2.0はすでに公開済み）。そしてそこでは新たに「経営陣の（ISMSへの）責任、コミットメント」が明文化されて盛り込まれている。認証取得各社の取り組みに注目したい。

社団法人 情報サービス産業協会
URL 01 http://www.jisa.or.jp/

ISMS
URL 02 http://www.isms.jipdec.or.jp/isms/

株式会社LACの販売する「Living Policy」は情報セキュリティーポリシーの策定、管理、運用を支援するツール。策定の時間を大幅に短縮するサンプルポリシーも魅力だが、最大の特徴はもちろんオンラインでポリシーを管理し、ユーザーに参照確認を要求したり、ポリシーの内容に関するテストを行ったりできる管理・運用の部分だ。


JIP-ISMS100-2.0

■ 第5 経営陣の責任

1. 経営陣のコミットメント

経営陣は、ISMSの確立、導入、運用、監視、見直し、維持及び改善に対するコミットメントの証拠を、次の事項によって示すこと。

① 情報セキュリティ基本方針を確立する。

② 情報セキュリティ目標が設定され、計画が策定されることを確実にする。

③ 情報セキュリティに対する役割及び責任を定める。

④ 情報セキュリティ目標を達成することの重要性及び情報セキュリティ基本方針に適合することの重要性、当該組織の法的責任、並びに継続的改善の必要性を組織内に周知する。

⑤ ISMSの確立、導入、運用及び維持に十分な経営資源を提供する（第5.2.(1)参照）。

⑥ リスクの受容可能な水準を決める。

ISMS認証基準（Ver. 2.0）の第5章では、「経営陣の責任」として、経営陣のISMSへのコミットメントと、ISMSのための経営資源の運用管理が定義されている。

［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