2005-8-15

混沌とした中から

第26号
発行責任者　稲崎義明

日本式セキュリティポリシーについて（６）

日本的企業でセキュリティはどのような立場に置かれているかを考えるとき、その責任の所在がはっきりしていないため、組織としてそのリスクに目をつぶるということになっています。情報が組織内で使われる場合、多くの人がその情報にタッチし、加工し、コピーし、いろいろな使い方をされます。そうなったときにこの情報に対する管理責任はどうなっているかというと、誰も持っていないため、情報リスクに対する配慮がされない、必要性が感じられないということになります。そのため、何かあったときにはすべてがライン管理(情報管理)に責任が唐突に集中するということになってしまいます。そのため、責任範囲を細分化することは、情報の取り扱いに関する意識と責任を両立させ、セキュアな業務プロセスを確立するための前提論として重要なことになります。

セキュリティポリシーを策定する第一段階は、業務における情報の取り扱いに関する責任の明確化と範囲の設定です。企業に所属している限り、社内の情報に関わることになります。「取り扱っている情報は取るに足らないものだから、セキュリティなんて関係ない」という人がいればその人は社外の人ということになります。また、「セキュリティなんて面倒。気にしていたら仕事が出来ない。」といっている人は仕事を刷る資格がないということになります。確かに仕事は出来るかもしれませんがそれ以上のリスクが発生することになります。第一段階のポリシーは、まずスタートですから、現在存在するリスクの可能性とダメージ、そして国際規格に照らした場合のNGポイント、これらから予測される金額的損失を付帯して、ポリシーの第一次原案と作成企画書の承認を経営者に求めることになります。承認されれば、個人の責任の明確化が出来ることになります。情報セキュリティについては「誰一人として例外ではない」という考え方を植え付け、業務関連情報に対する個人責任の明確化を図り、全員の意識向上、レベルアップが可能になります。責任の所在をはっきりさせ、その所属する部署でどのようにしてその責任に対応するかを自らの手法で実現させていく。これは、個人責任主義にのっとった欧米的手法ではなく、日本的であり、部署ごとに検討、実施するといった方法です。

確かに、初めの内容はこれまでのものの焼き直しに近く、画一的なものになりかねませんが、日本的のよいところは、部署としての動きが出来るようになれば、よりよいもの、現実に即したものが出てくるところにあります。そのためにも、「時間がかかっても自社のポリシーは自社で改定する」ことが必要です。改定作業にはもちろん不満を持った人をどんどん参加させ、きちんと万が一のリスク、ダメージを理解したうえでとうろんすることによってそしきにフィットしたものにブラッシュアップすることが出来ます。また、環境は常に変化します。昨日まで大丈夫であったことが今日には時代遅れになるかもしれません。そのためにも定期的、不定期に必要に応じてセキュリティポリシーの見直しを行うことが必要です。「ＰＤＣＡサイクル」は、必須のシステムです。セキュリティはポリシーを作れば、規則を作ればすむものではありません。個人に対する教育、セキュリティの意識向上、ＰＤＣＡサイクルの活用は継続して管理運用されなければならないものです。日本的である「のどもと過ぎれば」といった感じで、一時期に一気にいろいろ作ってしまうところが多いようですが、終わりのないものがセキュリティ管理です。企業の各部署に根付いた「日本式セキュリティポリシー」を作っていかならない時期に来ています。　（連載終了）

（今週の情報誌から）

○日経エレクトロニクス　８月１５日号

特集　電源もチップに載る

→現在ＬＳＩの動作電圧は半導体の微細化により、長らく＋５Ｖであったものが、＋３．３Ｖに下がったかと思っていると、現在＋１Ｖ前後にまで低下している。そのためちょっとしたことで誤動作してしまう。対抗としてはプリント配線基板上に出カップリングコンデンサや電磁波吸収シートなどの「力技」で対抗している。効果的なコンデンサのシミュレーションや電源と負荷との距離を身近くするなどの対処が取られてきたが、ついにＬＳＩ上に電源回路（ＤＣ－ＤＣコンバータ）を載せてしまう。

○日経パソコン　８月８日号

特集　ネット詐欺なんか怖くない

→インターネットは便利になってきた反面増えてきたのはネット詐欺。不当な請求からフィッシング詐欺など。不当な請求で増えてきたのはワンクリック詐欺とインターネットオークションでのトラブル。フィッシング詐欺は、本物と見分けにくい巧妙なものも存在する。