2005-7-15

混沌とした中から

第24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（4）

今回は情報システム部門の嘆きです。

まず、情報システム部門ですがどのように作られてきたのでしょうか。その経緯は、企業にコンピュータが導入され、システムが導入され、ネットワークが導入され、その経過の中で担当者が置かれ、チームが編成され、情報システム部門となってきたものです。もちろん規模によっては担当者しかいないところもあります。また、初めの頃はシステムを販売する側も、窓口の担当者がいてもらえばそれだけでいいといっていた頃もありました。しかし、システムが拡大し、ほとんどすべてのものがネットワークに接続され、経営資源として情報が重要視されるようになると、本来は情報システム部門の役割も変化するはずでした。それがシステム管理であり、セキュリティ管理です。ところがその実態は、全くヘルプデスクのようなものです。トラブルがあれば行って対応し、端末が変わればインストールし、わからないことがあれば問い合わせが来るといった、「いわれたことをだまってやれ！」といわれる立場であり、「協力して欲しい」などと頼める立場ではないのが実情です。そこがセキュリティ管理運営の主導的立場を取らなければならないというのですから、大変であることは目に見えています。ましてセキュリティポリシーが押し付けのどこかの雛形を持ってきただけの場合は。

セキュリティ管理の難しいところは、セキュリティ対策による機密保護の度合いとアクセスの容易さが相反する関係にあることもあります。厳しい対策基準をもとに手順書が作られた場合、情報を使う場合にそのアクセスに時間や手間がかかって非常に使い勝手が悪いシステムになってしまいます。利便性追求を黙殺しても優先して守るべき機密情報であれば問題ないのですがそのようなシステムばかりではありません。例えば、「パスワードは6ヶ月に1回は変更しなければならない」ということが決められていた場合どうでしょうか。経理部門など機密性の高い情報を取り扱っている意識の高い部署なら問題ないでしょうか、営業部門となると90％以上は守られないのが現実です。必要といわれてもシステムで必須となっていなければ、パスワード設定さえされていないというのが実際のところです。100％実施されなければセキュリティ対策として漏れが生じているということです。また、このような内容を含む手順書があった場合、実行できない手順書ということでこの文書のほとんどの項目が守られない、もしくは無視される可能性が高くなってきます。せっかく作ったポリシーや手順書ではあっても、現場サイドからはポリシーに対する不信感が見えてきます。

この状態では、セキュリティ体制は何も整備できない、「情報セキュリティについて何とかしよう」と思う側と「余計な仕事は勘弁してくれ」という側の戦いになってしまいます。まさに情報システム部門の泣き所です。

さらに、セキュリティの維持は情報システム部門が担当すれば言いという勘違いがセキュリティポリシーを本来守らなければならない一般社員側にあります。ウィルスはウィルス対策ソフトが入っているから十分と考え、システム侵入は自分のところにはない、情報漏洩は情報システム部門がちゃんと対策を採ればいいと考えているのが一般的ではないでしょうか。情報システム部門でいろいろな対策を考え実施しようとしても自分のことと実感がないために対策が十分とならない、情報システム部門の努力が空回りしてしまうのが現実です。まずは実感を持ってもらうこと、意識の高揚が最重点となります。　（次回へ続く）

（今週の情報誌から）

○日経エレクトロニクス　７月１８日号

特集　起動する家庭発電

→家庭の発電は太陽光発電ばかりでなく、エースとして期待を集める燃料電池。家庭での発電の普及の兆しが見えてきた。太陽電池だけでなく、ようやく発売となった燃料電池でなく、ガスエンジンによるコジェネレーションシステムという意外なところから。燃料電池、ヒートポンプ、ガスエンジンの組み合わせから電気を作り、熱での利用、車との連動などでの普及が見えてきた。

○日経パソコン　７月１１日号

特集　ＰＣアーキテクチャー大全

→今年、パソコンのアーキテクチャが大きく変わる。ＣＰＵはデュアルコアとなり、６４ビットにも対応する。メモリはＤＤＲからＤＤＲ２に主流が移り、高速となり、来年にはＤＤＲ３が登場する。さらにＨＤＤにはついに垂直磁気記憶方式が登場し、容量アップし、インターフェースはシリアルＡＴＡⅡの登場で３００ＭＢ／秒となる。今年のパソコンを見るにはこのアーキテクチャの理解が必要。