特集2

社会人のセキュリティ 常識・非常識

PHOTO：© Image Source/amanaimages

“やってはいけない”理由を知って危険を防ぐ

職場には、情報セキュリティに関するさまざまなルールがある。「ばれなければ大丈夫」などと甘く考えてはいけない。ルールを破ると、会社全体に被害が及ぶ恐れがある。そうならないためには、“やってはいけない”ルールの本質を理解することが重要。何かあってからでは遅すぎる。今すぐ「セキュリティの常識」を身に付けよう。

（勝村 幸博）

4月に入社した新入社員も、早2カ月が過ぎ、職場に慣れ始めたころだろう。ただ、職場にはさまざまなルールがあるので、とまどうことは少なくないはず。その一つが、情報セキュリティに関するルールだ。パソコンやインターネットなどの利用について、さまざまな禁止事項や制限事項が設けられ、職場での「セキュリティの常識」になっている（図1）。

例えば、業務とは無関係のWebサイトの閲覧や書き込みを禁止している職場は少なくない。最近増えているのは、USBメモリーなどの外部記憶装置の利用制限。私用メールを制限したり、パスワードの設定方法や管理方法について指示したりする職場もある。自分が使いたいソフトウエアを自由にインストールできない場合もある。

セキュリティのルールにとまどっているのは新入社員に限らない。中堅社員やベテラン社員の中にも、ルールの存在を知りながら、無視している人は少なくないだろう。

そのため、多くの会社や組織では、セキュリティに関する研修や講習会を実施し、ルールの徹底を図っている。しかしながら、守られないケースは少なからず存在するという。

なぜ守られないのか。「ルールが守られないのは、何のためにやっているのか分からないため」（情報セキュリティに関するセミナーの講師などを務める、ディアイティ セキュリティガバナンスビジネス部部長の河野省二氏）。例えば、Webの私的利用の禁止については、「業務の妨げになる」という理由だけで禁止されていると勝手に判断。「ばれなければいいだろう」と、こっそり怪しいサイトを閲覧したり、掲示板サイトに書き込んだりする……。

「ルールを守らせる立場の上司なども、部下に『なぜ守られなければいけないのか』と聞かれると、『ルールだから』としか答えられないことが多い」（河野氏）。

サボリ防止だけではない

もちろん、業務効率の低下を防止するために定められているルールもある。だからといって、「見つからなければ大丈夫。たとえ見つかったとしても、謝れば許してもらえるだろう」などと高をくくっていると、大変な事態を招く恐れがある。情報セキュリティに関するルールの多くは、「セキュリティの事故から会社や社員を守るため」（河野氏）に定められているからだ。

現在では、パソコンやネットの利用は業務を遂行する上で不可欠。だが、利用にはさまざまな危険が伴う（図2）。具体的な危険としては、ウイルス（マルウエア）感染、情報漏えい、迷惑メールの受信、不正アクセスなどが挙げられる。これらの結果、信用の失墜、事業の中断による利益損失、復旧コスト、損害賠償などが発生する恐れがある。

被害に遭うと、その影響はルールを破ったユーザーだけにとどまらない。会社全体が影響を受ける。例えば、ウイルスに感染した場合、その損害額は中小企業で1社当たり平均およそ430万円、大企業では1億3000万円になるという試算がある（図3）。この調査では、実際に被害に遭った会社へのアンケートなどを基に、被害額を算出するためのモデルを作成し、被害額を試算した。

試算によれば、業務を中断されることで発生する「本来なら得られるべきだった売上」が被害額のほとんどを占め、ウイルスを駆除したり、パソコンを元の状態に戻したりするための「復旧コスト」は微々たるものだったという。

「危ない危ないと脅かすだけではルールは守られない。なぜそのルールがあるのか、破るとどうなるかといった本質を理解する必要がある。そうすれば、ルールの重要性が分かるだけではなく、ルールにない行為についても、それが危険なことかどうかを判断できるようになる」（セキュリティセミナーの講師などを務める、ラック セキュリティ能力開発センターの長谷川長一氏）。

セキュリティルールの「本質」とは何か？ 次ページからは“やってはいけない”ルールを取り上げ、それらの意味や守らなかった場合の危険性を解説する。

●職場のパソコンで禁止／制限されている行為の例

- 業務に関係のないWebサイトの閲覧や書き込み
- USBメモリーなどの外部記憶装置の利用
- 会社から与えられたメールアドレスの私的利用
- 容易に推測できるパスワードの設定
- 私用ソフトウエアのインストール

図1 自由に使える個人のパソコンとは異なり、職場のパソコンにはさまざまな禁止事項や制限事項がある。業務効率やモラルのためだけではなく、セキュリティのために禁止／制限されていることも多い

●パソコンやネットの利用にはリスクが伴う

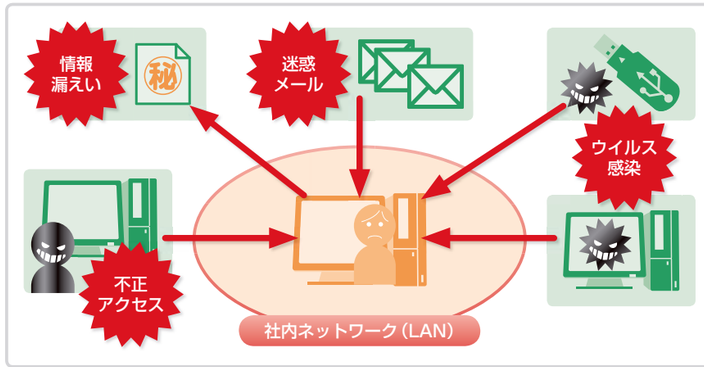

図2 業務上、パソコンやインターネットの利用は不可欠。だが、利用にはさまざまな危険（リスク）が伴う。それらの危険から、企業／組織や社員を守るために設定されているのが情報セキュリティに関するルールである

●ウイルスによる被害額、大企業なら1億円以上

	大手・中堅企業（従業員300人以上）	中小企業（同300人未満）
ウイルス被害がなければ得られたと予想される売上	1億2949万7000円	413万6000円
復旧に要するコスト	15万3000円	17万2000円

図3 2006年に情報処理推進機構（IPA）が発表した、ウイルスによる被害額の試算結果。被害に遭ったことのある企業／組織へのアンケートやヒアリングを基に、被害額を算出した。被害額のほとんどは、本来なら得られるべきだった売上。復旧コストはわずかだった