



## 情報セキュリティについて (IRSME15022)

平成 27 年 11 月 9 日 原田 長州

データを守るという視点で情報セキュリティについて気をつけたい3つのポイントについて記載する。

### ■ 「パソコンをインターネットに接続しないから安心」

重要なデータが入ったパソコンをインターネットにつながなければ、外部からの侵入の不安はなくなるだろうか。インターネット経由からの侵入は防げるだろうか。パソコンに侵入してデータを流出させるのは難しいが、隔離されたはずのパソコンのデータ書き換え、削除などをして損害を与えることは可能だ。

パソコンを外部とのデータのやり取りなしで運用することは難しい。たとえば、郵便番号の更新や実験データの取り込みなどのデータの入出力が発生する。感染経路は、USB メモリーや外付けハードディスクなど外部記憶装置を介して行われることが想定される。OS やアプリケーションソフトの定期的なアップグレードができずにデータ更新で可能なセキュリティホールがあいたままになる可能性もある。

### ■ 「ウイルス対策ソフトが入っているから安心」

ウイルス対策ソフトが最新の状態になっている場合でも、ウイルス対策ソフトではユーザーが実行を許可した「悪意のあるプログラム」は、完全に検知・阻止することはできない。

ウイルス作成をする側になって考えると、ウイルス対策ソフトに検知されにくいものを目指して作成し、市販のソフトで検知できるかどうかを確認してから配布されるはずである。ユーザーが正当なソフトウェアだとおもって「悪意のあるプログラム」を誤って実行してしまうことでウイルスなどを実行してしまうことになる。

ウイルス対策ソフトを購入してインストールしただけでは解決しない面が存在することを知ることが必要だ。ウイルス対策ソフトが入っているからどのようなファイルでも開いても大丈夫であると考えると被害を受けることになる。

### ■ 「どの企業・組織についても適用可能な完璧なルールが存在する」と考えてしまう

今日からセキュリティに対して取り組もうとおもっても、いきなり完璧な状態にすることは

平成 27 年 11 月 9 日

(IRSME15022) 情報セキュリティについて

---

できない。どのようなデータがあるかを洗い出す・社内ルールの策定・必要機器の導入・教育などの工程が必要だ。ある会社で有効なルール・仕組みが、そのまま他社でも有効とは限らない。必要な対策は、各社の規模・業態などによって異なる。セキュリティについては、魔法のように一気に解決させる方法は存在しない。

## ■ まとめ

具体的にすすめる上では、情報機器を導入している事業者自身かその提携先が提供しているサービスを利用することになるとおもわれる。その場合であっても依頼者自身の知識がなければどこまでの対策が必要なのか、費用は妥当なのかも判断できない。

セキュリティ専門の人員を置くことができない規模では、セキュリティ対策は後回しになってしまうことが往々にしてあるため、少しずつでも確実にすすめていくことが求められる。(了)