忘れた頃にやってくる災いへの備え

総合情報基盤センター　センター長　栗本　猛
（教養教育学系　教授）

「天災は忘れた頃に来る」という名言がありますが、最近は忘れる暇も無いくらいに災害がよく発生しています。毎年のように起こる豪雨、地震や火山活動の活発化などで各地に被害が出ています。地震の予測はまだ困難ですが、雨の方は気象観測技術の発達で数時間以内に豪雨となる予報が出されますので、避難指示に従えば自分の命を守れる確率が高くなります。災害に備える普段からの準備と心構えが重要です。

天災以外でも、情報関係での災いとして、銀行や通信会社の回線トラブル、コンピュータウィルスへの感染、外部からのサイバー攻撃、過失による情報漏洩などのニュースが後を絶ちません。予測不能な地震と違って、これらの多くには普段からしっかりと対策を立てて備えておけば被害を防ぐか、最小限に抑えることが可能です。たとえば、回線に流れる情報量が多くなりすぎることによるトラブルが予想される場合は回線を太くしたり、利用制限をかけたりすることで対応できますし、雷等の事故で回線が切断されてしまう危険性があれば、回線を二重化しておく対応が考えられます。サイバー攻撃への対処としては、関連情報にこまめに注意を払いつつ、OS やソフトウェアのアップデートを怠らない、バックアップをとっておく等があります。

災いへの対応としては、それに要する経費や労力の規模で分類すれば、次の３種類になると考えられます。

A）回線や機器等の大幅な刷新が必要で多くの経費を必要とするもの。（新規の予算か特別予算が必要なもの。）

B）部品や周辺機器の交換、ソフトウェアの更新等で対応できるもの。（通常の予算内で賄えるもの。）

C）日常の業務内で対応可能なもの。（予算を必要としないもの。）

A）については新たな予算が必要となりますから、それが認められなければどうにもなりません。毎年の予算から少しずつ積み立てることができれば、数年かけて対処できます。個人レベルでは、お金をためて新しい PC を買うようなものです。

B）については通常の予算内に含まれている定期的な部品交換はよいのですが、想定外のトラブルが起こったときに予備費で対応できるかが問題です。対応可能としても、それで予備費を使い切ってしまった場合に、新たな別の問題が起こらないとも限りませんので、判断に迷うところです。個人なら有償のサポートサービスを契約するのも一つの手です。

一番大事なのは C）で、日頃から最新の情報を収集し、何かあったときにどう対応するかを心がけておくことです。トラブル時にパニックになることを避けなくてはいけません。可能ならば様々なトラブルを想定したシミュレーションを行い、対応策を検討しておくことが重要です。学校等で行う避難訓練はまさにこのシミュレーションです。その際に必要と思われれば A）や B）で対応すべき事柄をまとめておくとよいでしょう。

しっかりと準備はしたと思っていても、**想定外のことは起こりえます。**それでもパニックを起こさず、まずは深呼吸して冷静さをいくらかでも取り戻してから状況判断しましょう。その時点で可能な応急処置は何か、利用可能な資材と人材はどれだけか、連絡・相談すべき相手はどこか等々を焦らずに検討していってください。大きなトラブルの際には難しいことですが、この心掛けを普段から忘れないようにしてください。