6.3 データの取り扱い

6.3.1 不正アクセス

■ 不正アクセスの脅威

不正アクセスとは、一般に、コンピューター等を利用する正当な権利のない者が、不正な手段でコンピューター等を利用することを指しています。

パソコンをインターネットに接続すれば、不正アクセスを受ける危険性が格段に高まります。なぜなら、インターネットへの接続は、パソコンを世界中に接続させるからです。広い世界の中には、残念ながら悪意を持った者も多く存在します。インターネットへの接続は、それらの悪意を持った者とも通信を可能とする行為でもあるのです。そのため、インターネットに接続したパソコンは、不正アクセスの危険があると考えましょう。

■ 不正アクセスの被害

直接的な不正アクセスの被害としては、データやシステムの破壊、情報の漏えいなどがあげられます。これらは、不正侵入を受けた側が、被害者となる場合です。

これに対して、不正アクセスにより不正行為に加担させられる場合もあります。それは、自分のパソコンに不正な活動をするプログラムが送り込まれ、そのプログラムが不正行為を行うといった場合です。たとえば、特定のサーバーを攻撃するようなプログラムを送り込まれることもあります。いわゆるボットがこれに該当します。

また自分のパソコンが不正な行為に加担させられる他の例として、盗み出された情報の悪用があります。たとえば、メールのアカウントやパスワードなどの設定情報が盗みだされると、迷惑メールの送信元として詐称されることがあります。つまり、不正アクセスを防止しないことは、詐称できるメールアドレスを提供して、少なからず、迷惑メールの送信に協力していることとなってしまうのです。

たとえ不本意であっても、上記のような不正行為に加担させられると被害の範囲が自分だけにとどまりません。他人に迷惑をかけてしまうという意味では、自分だけが被害を受けるときより、被害は甚大です。

■ 不正アクセス禁止法

不正アクセスを禁止および防止するために、2000 年に**不正アクセス禁止法**が施行されました。この法律により、不正アクセス行為が禁止され、違反した場合には罰則が適用されるようになりました。また、不正アクセスを助長する行為、たとえば他人のパスワードを漏えいさせるなどの行為も禁止され、処罰の対象となりました。

この法律では、以下のような行為が不正アクセス行為にあたるとされています。

- 他人のパスワードや暗証番号を利用する。
- セキュリティホールを利用して、不正にアクセスする。
- 他のコンピューターを踏み台にして、不正にアクセスする。

いずれの不正アクセス行為も、アクセス制御機能により利用が制限されているコンピューターに対して、ネットワークを介してアクセスした場合に限定されています。法律上の不正アクセスに該当しない具体例には、以下のような場合があります。

- データやフォルダーに適切なアクセス権が設定されていない。
- ネットワークがファイアウォールによって守られていない。
- ネットワークを介さずに直接コンピューターを不正に操作する。

これは見方を変えれば、アクセス制御をしていないコンピューターが不正に利用されても、この法律では処罰できないということになります。したがって、パソコンの利用者や管理者は、自らの手で自らのパソコンを守る必要があるのです。

6.3.2 個人情報の取り扱い

■ 個人情報に対する意識の高まり

近年、特に取り扱いに対して注意が要求されるようになったもののひとつが個人情報です。これにはパソコンやネットワークにおける技術の進歩が大きく関わっています。

メールや IP 電話など費用が安いコミュニケーション手段も個人情報が悪用されやすい環境をつくってしまいました。

たとえば、個人情報１万件を入手した者が１万人全員にダイレクトメールのはがきを郵送すれば、数十万円もの費用がかかりますが、電子メールでダイレクトメールを送れば、郵送の費

NOTE

不正アクセス禁止法：正式には「不正アクセス行為の禁止等に関する法律」。

用はほとんどかかりません。また電話セールスも同様です。従来の電話であれば高い市外通話料金が必要ですが、IP 電話を利用すれば全国一律の低料金で利用することができます。市民生活を豊かにするための通信手段の低コスト化は、不正行為を行うためのコストも下げてしまったのです。

このように個人情報は以前より悪用されやすい環境になっています。そして一度漏えいした個人情報は容易に複製できるため、回収することは困難です。したがって、個人情報の漏えいには以前にも増して注意を払う必要があるのです。

■ 個人情報の取り扱い上の注意点

個人情報は、漏えいさせてはならないことは当然ですが、それだけでは不十分です。個人情報は、以下のような適切な取り扱いをする必要があります。なお、**個人情報保護法**によって、個人情報取り扱い事業者（個人情報データを保有する事業者が対象）に対しては、以下の点などが義務付けられています。

- 利用目的をできる限り特定しなければならない
- 利用目的の達成に必要な範囲を超えて取り扱ってはならない
- 偽りその他不正の手段により取得してはならない
- 取得したときは利用目的を通知又は公表しなければならない
- 個人データを正確かつ最新の内容に保つよう努めなければならない
- 安全管理のために必要な措置を講じなければならない
- 従業者・委託先に対する適切な監督を行わなければならない
- 本人の同意を得ずに第三者に提供してはならない
- 取扱事業者名、利用目的等を本人の知り得る状態に置かなければならない
- 本人の求めに応じて保有個人データを開示しなければならない
- 本人の求めに応じて訂正等を行わなければならない
- 本人の求めに応じて利用停止等を行わなければならない
- 苦情の適切かつ迅速な処理に努めなければならない

NOTE

個人情報保護法：正式名称は「個人情報の保護に関する法律」。

6.3.3 ファイル交換ソフト

ファイル交換ソフトとは、特定のサーバーがなくても、パソコン同士で直接データを交換できるソフトウェアのことを指し、利用者間で手軽にデータの受け渡しができる点が特長です。これらのソフトは「P2P ソフト」とも呼ばれています。

ファイル交換ソフトを利用する際には、著作権や知的財産権に注意を払う必要があります。著作権の中には、公衆送信権という権利があり、ここでは、著作者以外が公衆に対して送信するだけでなく、送信可能な状態に置くことも対象としています。したがって、著作者に無断で、不特定の者がファイル交換ソフトにより受信可能な状態にするだけで、著作権法に抵触する行為となります。

著作権法に抵触しない限りは、ファイル交換ソフトの利用そのものが法律やマナーに反することではありません。しかし、近年ファイル交換ソフトを標的とするマルウェアによって、さまざまな被害が発生しています。代表的なものは、暴露型ウイルスです。ファイル交換ソフトの機能を使って、パソコンやネットワーク内の情報を、手当たり次第に外部へ流出させてしまうのです。

このような被害を防ぐため、外部へ流出してはならない情報が入ったパソコンでは、ファイル交換ソフトを利用すべきではありません。情報が一度流出すると、元に戻すことは現実的には不可能だからです。

NOTE

P2P：Peer to Peer　仲間同士の意味。