⑨　データの流出

指導項目の分類	セキュリティに関すること

対象・教科等	高等学校	情報、総合的な学習の時間、特別活動など

指導のねらい	（1） データがどのように流出してしまうのか、経路や方法を知り、セキュリティ対策の必要性を理解させる。 （2） 個人情報がインターネットワーク上でどのように扱われる可能性があるかを知り、個人情報保護の具体的な対策の方法を理解させる。

指導の手引

・個人情報が売買されたり、個人情報の流出が原因で犯罪に巻き込まれたりする事例を挙げて説明する。

・ 個人情報の取得を目的としながら、それを隠して懸賞やアンケートを行う Web サイトや、企業のホームページを偽装した「フィッシング」や「ファーミング」と呼ばれる悪質な Web サイト等を紹介しながら、適切な対処方法を指導する。

・ ハードディスク等の記録媒体をフォーマットしただけでは､特殊なソフトを用いることにより､削除したはずのデータを復元できる場合がある｡データの復元を防ぐためには､専用のソフト等を利用する方法と､記録媒体を物理的に破壊する方法がある｡一度情報が流出すると取り返しがつかなくなるので、パソコンや記録媒体を処分する時は、情報の流出に注意する。

○フィッシング（phishing）

実在する銀行等の企業からのメールを装い、メールの受信者に企業の偽ホームページにアクセスさせて、クレジットカード番号やＩＤ、パスワード等を入力させるなどして不正に個人情報を入手しようとする行為のこと。

それらの情報を元に金銭をだまし取られる被害が欧米を中心に広まっており、今後、日本においても同種の形態による被害が予想されている。

（被害防止策）

・不自然な形で個人情報（クレジットカード番号、ＩＤ・パスワード等）を聞き出そうとするメールに対しては、メールを送信してきたとされる企業の実際のホームページや窓口に問い合わせて確認する。
・クレジット番号やＩＤ・パスワードを安易に入力しない。

○ファーミング(pharming)

一般の利用者が、正しいＵＲＬでホームページを閲覧していても、プロバイダ等が管理するＤＮＳサーバ（ドメイン名と IP アドレスを対応させる機器）の情報を不正に書き換えたり、ウイルスやワーム（自己増殖を繰り返しながら破壊活動を行なうプログラム）等を使って個人のパソコンに保存されているファイルを改ざんする手口で偽サイトへ誘導すること。

利用者は、ブラウザのアドレス・バーには正規の URL が表示されているため、偽サイトと気付きにくい。

＜参考＞

警察庁「インターネットトラブル」
http://www.npa.go.jp/nettrouble/index.htm

警察庁「サイバー犯罪対策」
http://www.npa.go.jp/cyber/index.html

展開例	
学習活動	指導上の留意点
1　本時の学習のめあてを知る 2　ワークシートの事例を読む 3　思ったことを書いてみる 4　友達やグループで「大切なデータが流出する経路」について話し合う 5　意見をまとめて数人が発表する 6　自分の感想や意見を書く 7　本時の学習をまとめる 8　自己評価をおこなう	（Web ページを使った体験的な学習活動を取り入れる場合は、２と３の部分を活動にあてる。） ・「大切なデータ」とはどのようなものか、イメージさせる。 ・「流出」はどのような場合に起こるのか、事例をもとに具体的にイメージさせる。 メディア自体の盗難や紛失、キーロガー（キーボードからの入力を監視して記録するソフト）、スパイウエア（パソコンユーザの行動や個人情報などを収集するソフト）など ・セキュリティ対策の必要性を認識させる。

発展的な学習
・ 個人情報の流出による経済的、社会的な被害状況を理解させる。

関連項目
「コンピュータウイルス」