サイバー犯罪を増やさないために

実際の社会で犯罪行為にあたることは、インターネット社会でも許されません。
「インターネットだから」「仲間だけの秘密だから」と気軽にしてしまったことでも、犯罪者として検挙されてしまうのです。

事例

脅　迫

インターネットの掲示板に「今週の日曜日、××郵便局に討ち入る。止める気でいるなら頑張りたまえ。」等の書き込みをして脅迫した。平成16年5月、脅迫罪で検挙（群馬）。

事例

ストーカー行為

交際を断られたかつての見合い相手に対して、「付き合ってくれ」などの電子メールを執拗に送信するなどのストーカー行為を行った。平成16年6月、ストーカー規制法違反で検挙（静岡）。

事例

著作権侵害

ファイル共有ソフトWinnyを利用して映画データをインターネット上に公開し、不特定多数の者が自由にダウンロードできる状態にした。平成15年11月、著作権法違反で検挙（京都）。

事例

不正アクセス行為

電子メール等を利用して「アイテムを譲る」等と言葉巧みに持ち掛けてだまし、オンラインゲーム・サービス用ID15個のパスワードを入手して不正アクセスした上、他人のアイテムを自分のものとなるよう移動させた。平成16年4月、不正アクセス禁止法違反で検挙（京都）。

**また、自分で犯罪を犯さなくても
適切な情報セキュリティ対策を講じていなければ
知らず知らずのうちに犯罪者に利用されてしまったり
犯罪にまきこまれたりしてしまうこともあるのです。**

無線LANのセキュリティ

無線LANはケーブルをつながなくてもネットワーク接続ができて大変便利ですが、
セキュリティ対策が不十分なまま利用していると、他人から侵入され、
パソコン内のデータを改ざんされたり、犯罪に悪用されたりする危険があります。

無線LANを利用する際の注意点

- 購入したままで利用するのはやめ、利用するときは必ずセキュリティの設定をする。
- 使用しないときはパソコンや無線LANルータの電源を切る。

踏み台・ウイルス感染源に

近年ブロードバンド環境も普及しつつあり、サイバー攻撃を受ける危険だけでなく、
自分のパソコン等がいわゆる踏み台として利用され、
サイバーテロ等の重大な犯罪に悪用される危険も高まっています。
また、ウイルスの感染源となって不特定多数の人に被害を与えてしまう危険もあります。

踏み台やウイルス感染源にならないために

- ウイルス対策ソフトを導入し、常に最新のバージョンにする。
- OSやソフトウェアのセキュリティ・パッチをこまめに適用する。
- 常時接続の場合にも、使用しないときにはパソコンの電源を切る。
- ファイアーウォールなどの防御用ソフトを利用する。