インターネット上の違法・有害情報に関するQ＆A

Q30 インターネット上で違法・有害情報を発見した場合には、どうしたらいいの？

A30 「インターネット・ホットラインセンター」か、警察に通報してください。

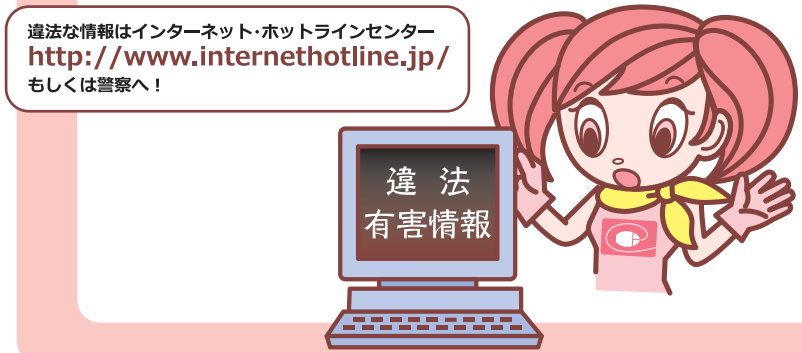
知っておきましょう

インターネット上で違法な情報を発見した場合には、「インターネット・ホットラインセンター」か、警察に通報してください。公序良俗に反するような有害な情報を見つけた場合には、「インターネット・ホットラインセンター」へ情報提供してください。

なお、違法・有害な情報が掲載されているサーバや電子掲示板の管理者に情報提供する方法も考えられます。

- インターネット・ホットラインセンターは、インターネット利用者から違法・有害情報に関する情報提供を受け付け、一定の基準に従って情報を選別した上で、警察への情報提供、電子掲示板の管理者等への送信防止措置依頼等を行う民間団体です。詳しくは、ホームページをご覧ください。
  <インターネット・ホットラインセンター> http://www.internethotline.jp/

- なお、サーバや電子掲示板の管理者が誰かわからないときは、.jpドメインの場合には(株)日本レジストリサービス、.comや.netドメインの場合には国際組織INTERNICの提供するWhoisサービスを利用することで、連絡先を調べることができます。
  <(株)日本レジストリサービスWhois> http://whois.jprs.jp/
  <INTERNIC Whois> http://www.internic.net/whois.html



Q31 インターネット上で自分の権利を侵害するような書き込みを発見した場合には、どうしたらいいの？

A31 サイトの管理者等に対して削除要求できます。

知っておきましょう

ご自身の権利を侵害するような書き込みがあった場合には、プロバイダー責任制限法（※）や名誉毀損・プライバシー関係ガイドライン等に基づき、本人からサイトの管理者等に対して削除の要求をすることが可能です。

※「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報開示に関する法律」

- 具体的な手続き等については、「プロバイダー責任制限法　関連情報webサイト」をご覧ください。
  http://www.isplaw.jp/

Q32 携帯電話やパソコンに楽曲をインターネットでダウンロードするときに何に気をつければいいの？

A32 歌手やレコード会社の許可をもらって配信しているサイトかどうかを確認しましょう。

注意しましょう

平成22年1月の改正著作権法の施行により違法なサイトと知りながら楽曲をダウンロードすることは私的利用目的でも違法になりました。

歌手やレコード会社の許可をもらっているサイトかどうかを確認しましょう。

フィッシング詐欺に関するQ＆A

Q33 フィッシングって何？

A33

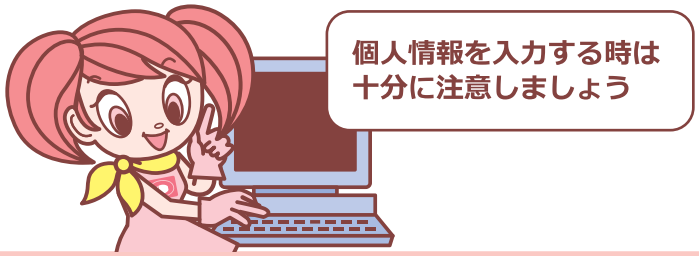
金融機関等を装い、銀行口座番号、クレジットカード番号、ＩＤ、暗証番号やパスワードといった個人情報を巧みに詐取する行為です。

注意しましょう

フィッシング（Phishing）とは、クレジットカード会社や銀行、オンラインショッピング事業者、オークション事業者等を装った電子メールを不特定多数に送り、偽のホームページにアクセスするよう仕向け、銀行口座番号、クレジットカード番号、ＩＤ、暗証番号やパスワードといった個人情報を巧みに詐取する行為です。

金融機関等が個人情報等をメールで尋ねるようなことはほとんどありませんが、もし、個人情報を入力させるようなメールを受信した場合は、メール本文にあるリンクはクリックせずに、送信元のホームページ等を確認する等十分注意して対応してください。

また、最近はセキュリティの脆弱性を利用し、正しいホームページアドレスを入力しても偽のホームページに自動的につながるようにして、個人情報を入力させようとするファーミング（Pharming）と呼ばれる新たな手口も出現していますので、注意が必要です。



●フィッシング対策に対する政府の取組み

各都道府県警察の「フィッシング110番」ホームページ
http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

フィッシング対策協議会ホームページ
http://www.antiphishing.jp/

ネットセキュリティに関するQ＆A

Q34 コンピュータウイルスへの感染や第三者の不正な侵入（不正アクセス）といった、インターネット上の危険からコンピュータを守るためには、どんな対策をすればいい？

A34

基本となる情報セキュリティ対策には、以下の３つがあります。

①ソフトウェアの更新（最新のセキュリティパッチの適用）

Webブラウザや電子メールソフト、OSでは、情報セキュリティ上の問題を解決するための修正プログラムが、メーカーから提供されることがあります。これらの修正プログラムを定期的に適用して、できる限りソフトウェアを最新の状態に保つように心がける必要があります。

②ウイルス対策サービス・ソフトの導入

最近のコンピュータウイルスは、電子メールやホームページを見ただけで感染するウイルスばかりではなく、勝手にインターネットを通じて感染するタイプのウイルスも出現してきています。ウイルスに感染しないようにするためには、ウイルス対策サービス・ソフトを導入することが必要です。

③パーソナルファイアウォール・ブロードバンドルータの利用

コンピュータを不正アクセスから防ぐためには、パーソナルファイアウォールというソフトウェアの導入が効果的です。パーソナルファイアウォールを導入すると、ハッカーの不正侵入やウイルスの侵入を防いだり、自分のコンピュータを外部から見えなくしたりすることが可能になります。また、ブロードバンドルーターにはファイアウォール機能が内蔵されているため、ブロードバンドルーターを設置することでパーソナルファイアウォールを導入した場合と同じ効果を得ることができます。

●インターネットを利用する際の情報セキュリティ対策については、この他にも利用の際の心構え等のご留意いただきたい事項があります。これらについては、以下のサイトをご覧ください。

総務省「国民のための情報セキュリティサイト」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm

総務省・経済産業省連携ボット対策プロジェクト「Cyber Clean Center」
https://www.ccc.go.jp/

インターネット上のマナーに関するＱ＆Ａ

Q35 チェーンメールが送られてきました。同じ内容のメールを他人にも送るように書いてあるけれど、どうしたらいい？

A35

受信しても転送せずに削除し、後は気にしないようにしましょう。

チェーンメールとは、一般的に同じ内容を不特定多数の人に転送するように求める迷惑メールのことです。
チェーンメールは転送されることを目的としているため、「転送すると幸せになる」、「転送しないと不幸になる」等、さまざまな内容で転送させようとします。
チェーンメールは、ただのいたずらの場合もありますが、メールに記載されているＵＲＬをクリックすると、登録料を払えと要求するいわゆる「ワンクリック詐欺」のようなものもあります。
チェーンメールは受信しても転送せずに削除し、後は気にしないようにしましょう。