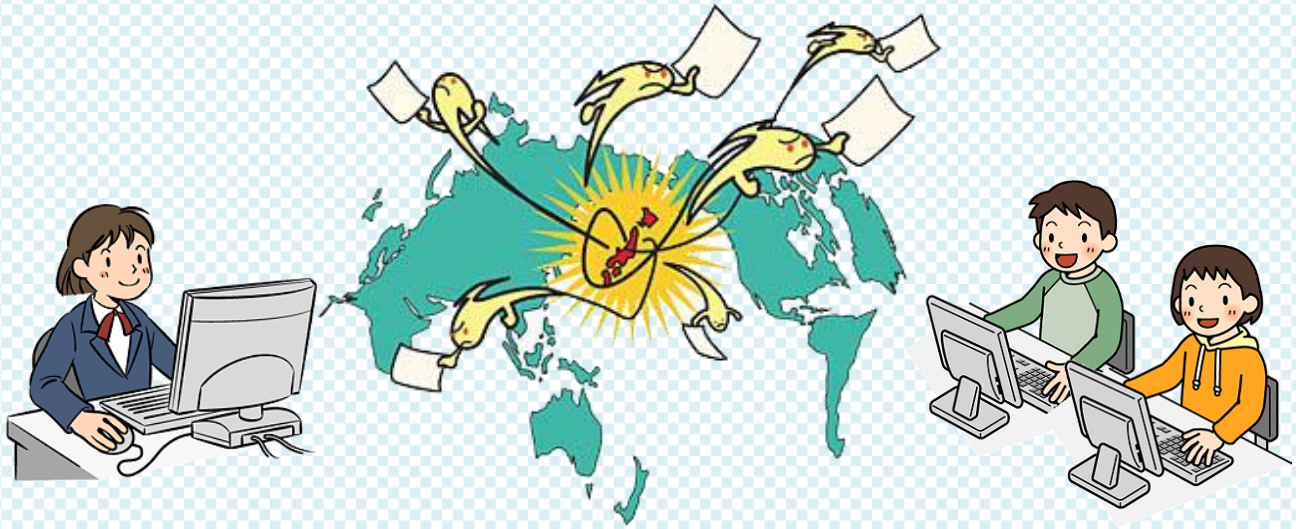
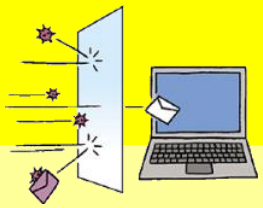
サイバー犯罪対策



巻き込まれない、だまされない！

サイバー犯罪・・・・ コンピュータやインターネットを利用した犯罪

まず対策を！



～違法情報の魔の手から子どもをガードしよう～

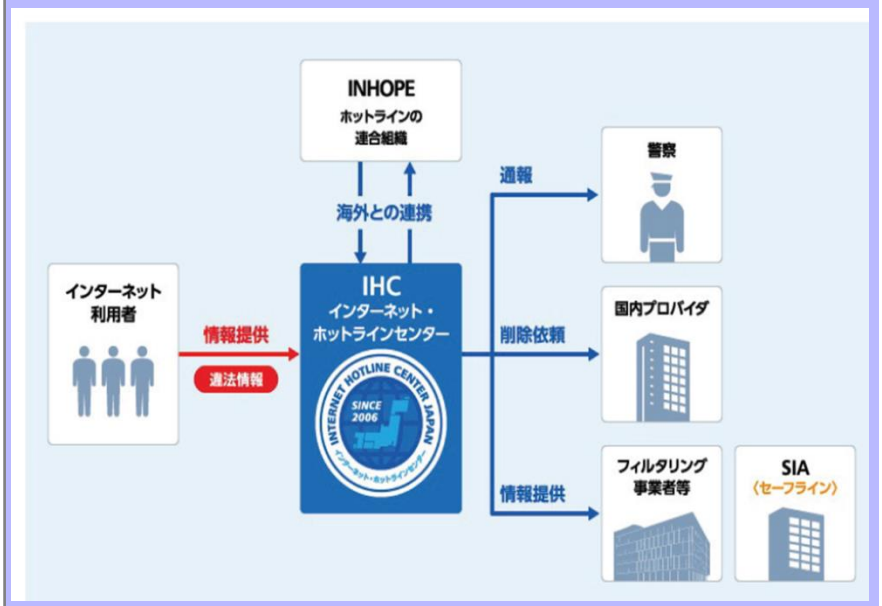
インターネット・ホットラインセンター

インターネット上の違法情報について、広く通報を受け付けています。通報された情報は一定の基準に従って選別した上で、違法情報は警察へ通報するとともに、サイト管理者やプロバイダ等に対し削除を依頼します。

人権侵害、知的財産権侵害等に係る通報等他の機関・団体において処理することが適当なものについては、専門的な対応を行っている関係機関・団体に対して情報提供を行います。

パソコンからは
http://www.internethotline.jp/
携帯電話はこちらから→

※　取り扱う違法情報の範囲については、上記サイトに掲載しているホットライン運用ガイドラインをご覧ください。
※　自殺予告など緊急に対応が必要な情報は、警察に１１０番通報してください。



鳥取県警察

フィルタリング対策を！

パソコンや携帯電話で手軽に利用できるインターネットは、違法な薬物販売や自殺の呼びかけ、わいせつな画像、さらには出会い系サイトなど、青少年に悪影響を及ぼし、犯罪に巻き込む恐れのある違法・有害サイトともつながっています。保護者のみなさんは子どものインターネット利用状況を把握し、安全で安心なインターネット利用のために、利用してはいけないサイトを決めるなどのルールについて子どもと話し合いましょう。

フィルタリングとは、インターネット上の有害サイトにアクセスできないようにする機能です。子どもにせがまれたからといって安易にフィルタリングを解除してはいけません。また、フィルタリングを使用していても有害サイトにアクセスしてしまうことがあることについて子どもと話し合いましょう。

携帯電話の場合

携帯電話会社各社がフィルタリングサービスを無償で提供しています。ただし、サービスを利用するには申し込みが必要です。
詳細についてはご契約されている携帯電話各社にお問い合わせください。

パソコンの場合

量販店などで販売されているフィルタリングソフトをパソコンにインストールする方法や、プロバイダが提供しているフィルタリングサービスに加入する方法があります。詳細については、フィルタリングソフトを提供しているメーカーやご契約されているプロバイダにお問い合わせください。

ID・パスワード設定を！

たかがパスワード、されどパスワード（なりすまし対策）

利用者ＩＤおよびパスワードの組み合わせは、情報システム(サービス)が個人(あなた)を特定するために用いるものです。利用者 ID は、情報システムで利用者毎に割り振られる場合がありますが、パスワードはあなたが設定(変更)すべきものです。

利用者ＩＤおよびパスワードの組み合わせは、情報システムがあなたを特定するための唯一の情報であると考え、安易な設定をしない、他人に教えない、定期的にパスワードを変更する、といった対策をとるようにしましょう。

パスワードの設定例

① 大文字・小文字・数字・記号の組み合わせ
　→記号(!、#等)、数字、英字を適当に織り交ぜる
② 長いパスワード → 最低８文字以上
③ 推測しづらく自分が忘れないパスワード
　→無作為で意味を持たない文字列であること

パスワード盗難対策

① 定期的にパスワードを変更する
② 紙に書き留めない
③ パソコンに保存しない
④ 人に教えない

利用者ID	複雑に
パスワード	複雑に

※使いまわし厳禁
※ＩＤ・パスワードは複雑に
※みんな同じＩＤ・パスワード
※単純なＩＤ・パスワード

子どもが狙われている！

～ルールやマナーを守って、トラブルに巻き込まれない～

コミュニティサイトで出会いを求めない！

軽い気持ちで始めたメール交換や書き込みで知り合った者に、監禁されたり殺害される事件が起きています。

見ない

～「出会い系サイト」は法律により１８歳未満は利用禁止～

「出会い系サイト」を１８歳未満の者が利用することも、大人が１８歳未満の者に交際の書き込みをすることも、法律で禁止されています。

書き込まない

～出会いを求める書き込みは危険～

一度書き込みをすると、相手はいろいろな手で誘ってきます。また、出会い系サイトではなくても出会いを求める書き込みは危険です。

絶対に会わない

～誘われても絶対に会ってはダメ～

メールで「優しそうな人」と思わせるのが犯罪者の手口。どんな危険が待ち受けているかわかりません。直接会うのは絶対にダメです。

プライバシーは守る

～個人情報は公表しない～

写真や住所、電話番号、学校名など、個人を特定できる情報は、犯罪被害の要因となりますので、安易に書き込まないように注意しましょう。

ネットゲームはルールを守る！

ネットゲームに不正アクセスして他人のアイテムを盗むなど、詐欺や窃盗まがいの犯罪が増えています。

教えない

～ID・パスワードは誰にも漏らさない～

パスワードを知られると、知らないうちにログインされ、アイテムを盗まれたりします。

複雑にする

～わかりやすいパスワードは避ける～

ネットの先には、パスワードを狙っている者がいるかもしれません。ＩＤと同じや、電話番号、誕生日などすぐに見破られるパスワードは禁物です。

ルールを守る

～不正アクセスは犯罪と心得る～

たとえゲームでも、他人のＩＤ・パスワードを無断で使うと「不正アクセス禁止法違反」という犯罪です。ルールやマナーを守ってこそ、楽しくゲームができると心得ましょう。

悪口や嫌がらせはしない！

掲示板やブログ、コミュニティサイトなどへの他人の悪口や嫌がらせ行為はトラブルの原因です。

悪口を書かない

～自分が嫌なことを他人にしてはダメ～

いたずらや興味本位で、掲示板などに他人の悪口を書き込むことは、名誉棄損などの罪になることがあります。

マナーを守る

～他人の個人情報を勝手に載せない～

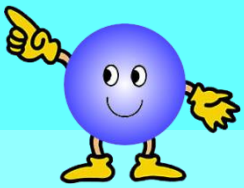
他人の個人情報を本人の許可なく掲載すると、プライバシーの侵害となるおそれがあります。

相談する

～悪質な書き込みは削除の相談を～

悪質な書き込みや個人情報を掲載された場合は、保護者に相談し、サイト管理者やプロバイダに削除を要請しましょう。

巧妙な落とし穴にご注意！



～ネットの先に潜む危険なワナにだまされない～

覚えのない請求メールが届いたら慌てて支払わない！

利用した覚えのない有料サイトの料金を請求される「架空請求」メールやリンクをクリックしただけで料金が請求される「不当請求(ワンクリック請求)」による詐欺が増えています。

無視する

～身に覚えのない請求メールは、無視する～

「有料」の明確な表示のないサイトについては、一切支払う必要はありません。身に覚えのない請求メールが届いても、無視しましょう。

問い合わせない

～送信元に問い合わせたりしない～

メールの返信や、送信元への問い合わせは、かえって危険です。心配なときは、受信メールを証拠として保存しておきましょう。

フィッシングの誘導につられない！

暗証番号などを狙う

フィッシングとは、実在の金融機関や企業からのメールを装い、偽のホームページに誘導して口座番号や暗証番号、ＩＤ、パスワードを入力させ、不正に情報を入手する手口です。犯人はそうして得た情報を他の犯罪に悪用します。

安易に答えない

～口座番号などの個人情報の問い合わせメールは要注意～

口座番号や暗証番号、ＩＤ、パスワード、さらには個人情報を問い合わせるメールやホームページは要注意。安易な回答は禁物です。

クリック前にまずチェック

～社名や内容に不審な点がないか確認～

メールに掲載されたリンクは、すぐにクリックしないことが肝心。企業名・金融機関名が正しく記入されているか、内容に不審なところはないかを確認しましょう。不審な点があるときは、１０４(電話番号案内)等で確認した電話番号で、送信元の企業や金融機関に直接問い合わせましょう。

URLを確認

～リンク先のＵＲＬやページの内容をチェック～

メールのリンクページを開いたときは、ホームページの上段に表示されるＵＲＬやページ内容に不審な点がないか確認しましょう。

スマートフォン利用者の方へ

スマートフォンは、パソコンと同じWebサイトが閲覧できたり、ゲームや便利な機能を追加するアプリ（プログラム）を自由に追加できたりと、その実態は携帯電話よりも、むしろパソコンに近いといえます。
このため、スマートフォンにはパソコンと同じような情報セキュリティ対策が必要となります。

最新の状態で使う

スマートフォンのOS（AndroidやiPhoneのiOS）やアプリは、セキュリティ対策や機能強化のためバージョンアップ（アップデート）が行われます。OSやアプリは常に最新の状態で使うようにしましょう。

信頼できるところからインストールする

メールで紹介されたアプリや、いわゆるアプリケーション・ストア（「Google Play」（Android）やApp Store（iPhone））以外で配布されているアプリには、コンピュータウイルスが組み込まれていることがあります。スマートフォンのアプリは、公式サイトからインストールするようにしましょう。

セキュリティアプリを利用する

最近ではスマートフォンを狙ったコンピュータウイルスが増えてきているため、パソコン用と同じような機能を持つセキュリティアプリが販売されています。スマートフォンを安全に使うため、セキュリティアプリの利用をおすすめします。

サイバー犯罪に関する情報提供のお願い

鳥取県警察では違法な情報を中心に県民のみなさまからの情報をお待ちしています。
特に、鳥取県内のインターネット利用者やプロバイダ等が関係する情報をお寄せください。

警察総合相談電話

携帯電話・ＰＨＳからも利用できます
☎ ＃9110

ダイヤル回線の電話及びＩＰ電話の方は直通電話
☎ 0857-27-9110

サイバー犯罪に関する相談・情報提供専用メールアドレス

✉ K_haiteku@pref.tottori.lg.jp

※この連絡先はフィッシング１１０番も兼ねています。フィッシングに関する情報、相談もお寄せください。