POLICE P情報

令和８年
２月号

◆ 自治体広報紙等活用版 ･･･Ｐ．１
◆ サイバーセキュリティに関する普及啓発強化 ･･･Ｐ．２

サイバーセキュリティ月間

「サイバーセキュリティ」について関心を高めよう！

2月1日から3月18日まで

こんにちは県警です

サンテレビ

毎月第１土曜日
午前８時30分～(15分間)
2月の放送は2月7日(土)

パトロールニュース

ラジオ関西

５５８KHzで放送中♩
毎週月曜日
午後０時08分ころ～(約２分間)

ひょうご防犯ネット+(プラス)

アプリになってリニューアル！

従来の「ひょうご防犯ネット」でのお知らせはもちろん、防犯ブザー・性犯罪対策機能など安全・安心をアプリで！

兵庫県警察ホームページ

兵庫県警察を紹介

県警からのお知らせなど
役立つ情報を配信中
【兵庫県警察】で検索！

兵庫県警察公式アカウント

防犯・交通・イベント・採用案内など
県警からのお役立ち情報を配信中！

右側の二次元コードをチェック→
ぜひ登録してください！

兵庫県警察 Facebook
兵庫県警察 X(旧Twitter)
兵庫県警察 YouTube
兵庫県警察 Instagram

兵庫県警察本部県民広報課

自治体広報紙等活用版

【サイバーセキュリティに関する普及啓発強化】

２月１日から３月 18 日までは、サイバーセキュリティ月間です。

○　安全・安心・便利なインターネット環境を構築するためのポイントを「知る」こと

○　サイバーセキュリティ上の脅威から身を「守る」こと

○　移り変わるサイバーセキュリティ上の脅威に対して対策を「続ける」こと

が大切です。

一人一人がサイバーセキュリティについて、関心を高めましょう。

国家サイバー統括室（ＮＣＯ）のホームページ参照

サイバーセキュリティに関する普及啓発強化
～サイバー犯罪対策の推進～　　～サイバー攻撃の脅威～

２月１日～３月 18 日は「サイバーセキュリティ月間」です

フィッシングやサポート詐欺、ランサムウェアなど、皆さんの生活をおびやかす犯罪も身近となっています。

家庭や職場でセキュリティについて話し合い、一人一人が日頃から対策することが何よりも重要です。

政府では、毎年２月１日から３月 18 日を「サイバーセキュリティ月間」と定め、国家サイバー統括室（ＮＣＯ）を中心に、産官学民が連携して、サイバーセキュリティに関する取組を集中的に行っています。

フィッシングメールについて

フィッシングとは、実在するサービスや企業をかたりＩＤやパスワードなどの情報を盗んだり、マルウェアに感染させたりする手口です。

電子メールやＳＭＳのＵＲＬから偽サイト（フィッシングサイト）に誘導し、そこで個人情報を入力させる手口が一般的に使われています。

フィッシングメールには、官公庁や金融機関、宅配業者、通信事業者などの生活に密着した事業者などを装うものから、知人や取引先に成りすましたものなど様々なものが確認されています。

「支払情報が変更された」「１年以上利用がないためアカウントを停止する」などといって確認や再設定を促すものや「セキュリティ上の理由でブロックされている」と不安をあおるもの「お荷物をお届けにあがりましたが不在のため持ち帰りました」と日常生活で利用する宅配業者を装うものなど、信用してもおかしくない内容で届きます。

フィッシングメールやフィッシングサイトは非常に精巧に作られており、本物のメールやサイトと見分けがつかないことが多く、判別は困難です。

【対策】

○　メッセージに記載されたＵＲＬをクリックしない
○　事業者などからの連絡は公式アプリやブックマークした公式ページから確認する
○　パソコンＯＳやソフト、アプリのアップデートを行う
○　ＩＤやパスワードの使い回しはしない
○　身に覚えの無い通信料やアプリのインストールがないかを確認する

偽サイト・詐欺サイトについて

インターネットショッピングにおいて「代金を支払ったが商品が届かない」「別の商品が届いた」など、偽サイトや詐欺サイトによる相談も多く寄せられています。

これらの相談は「商品名で検索をかけた結果、偽サイトや詐欺サイトにたどり着いた」というケースが多くみられます。

さらに、商品が届かないことを連絡すると、担当者から「商品が欠品している。キャッシュレス決済サービス（〇〇Pay など）を使って返金する」と言われ、指示通りにスマートフォンを操作すると、返金を受けるはずのお金を送金させられてしまうという手口が急増しています。

返金名目の詐欺にも注意してください。

【対策】

○　価格の安さや入手困難な商品に惑わされず、信頼できるお店を利用する

○　会社名やサイト名などを検索し、正規サイトが別に存在しないか確認する

○　検索エンジンから直接ショッピングサイトに移動するのではなく、正規サイトのＵＲＬからショッピングサイトに移動する

○　決済方法を確認する

（例）　決済方法が「口座振り込みのみ」になっていないか

（例）　決済方法を「口座振り込み」に変更するよう依頼されていないか

（例）　振込先は法人名かどうか

個人名の場合は、代表者や責任者、運営者以外の個人名になっていないか

上の（例）に該当しない場合でも、偽サイトや詐欺サイトである場合がありますので十分に注意してください。

アカウントの乗っ取り、なりすましについて

ＳＮＳアカウントの乗っ取り、なりすましについても多数の相談が寄せられています。

ＳＮＳには個人情報が多く載せられており非常に大切なものなので、アカウントが乗っ取られることがないよう、ＩＤやパスワードなどの取扱いには気を付けましょう。

●アカウントの乗っ取りの例●

知人を装ってＳＮＳのＤＭ（ダイレクトメッセージ）が届き、

① 「オンラインアンバサダーの座を争っています。投票いただけませんか」などと電話番号を聞かれる

② 電話番号を教えると「あなたの投票を確認したいので、送られてくる６桁の番号を教えて」などといって、ＳＭＳで送られた６桁のコードを聞かれる

③ 自分の携帯電話番号宛に届いた６桁の認証コードを伝える（絶対に他人には教えない）

④ 自分のアカウントのパスワードが変更され、アカウントが乗っ取られて、さらに自分になりすまして詐欺などのＤＭを送られる

というものになります。

【対策】

○ 個人情報を安易に教えない
（「認証コードを教えて」は詐欺と思いましょう）

○ ＩＤやパスワードの使い回しはやめましょう

○ ２段階認証など、更なるセキュリティ対策をしましょう

●アカウントのなりすまし●

著名人を装ったなりすましアカウントも増えています。

著名人からのＤＭ（ダイレクトメッセージ）で「お世話になっております。ご注目とご支援ありがとうございます。感謝の気持ちを込めて、今月から新しいＳＮＳグループを開設しました。投資知識や株式知識などを無料で共有します。参加費や条件は一切ありません」などと送られ、投資詐欺に誘導するものやＩＤ・パスワードを窃取して不正ログインや不正取引、情報漏洩を目的としているものなど、さまざまなものがあります。

【対策】

○ 著名人や会ったことがない人からのＤＭは疑う

○ 十分な説明がないままグループチャットに誘われたら疑う

○ 「投資テクニックを教えます」「無料」などの文言があれば疑う

○ 著名人からのＤＭや広告であれば、本人が詐欺に関する注意喚起を行っている場合があるので調べてみる

情報発信の紹介

《公式Ｘ》

サイバーセンターの「X」公式アカウントでサイバーセキュリティ情報を発信していますので、フォローして情報収集にお役立てください。

@HPP_c3division　　https://x.com/HPP_c3division

《サイバー防犯通信》

身近なセキュリティのポイントなどを分かりやすくまとめていますので、ご活用ください。

サイバー情報発信室ホームページへ

https://www.police.pref.hyogo.lg.jp/cyber/

子どもを守るために

インターネットは、子どもたちにとっても日常生活に欠かせないアイテムになっています。

そのような中、ＳＮＳやオンラインゲームを通じて知り合った相手に呼び出され被害に遭うケースや裸の写真や動画を送信させられる「自画撮り被害」が発生しています。

どのような危険があるか、安全に使うためにはどうしたら良いかを知り、家庭や学校でルールを作り、守っていきましょう。

また､子どもが困ったときにためらわず相談できるよう､日頃のコミュニケーションを大切にするとともに、信頼できる公的機関に相談してください。

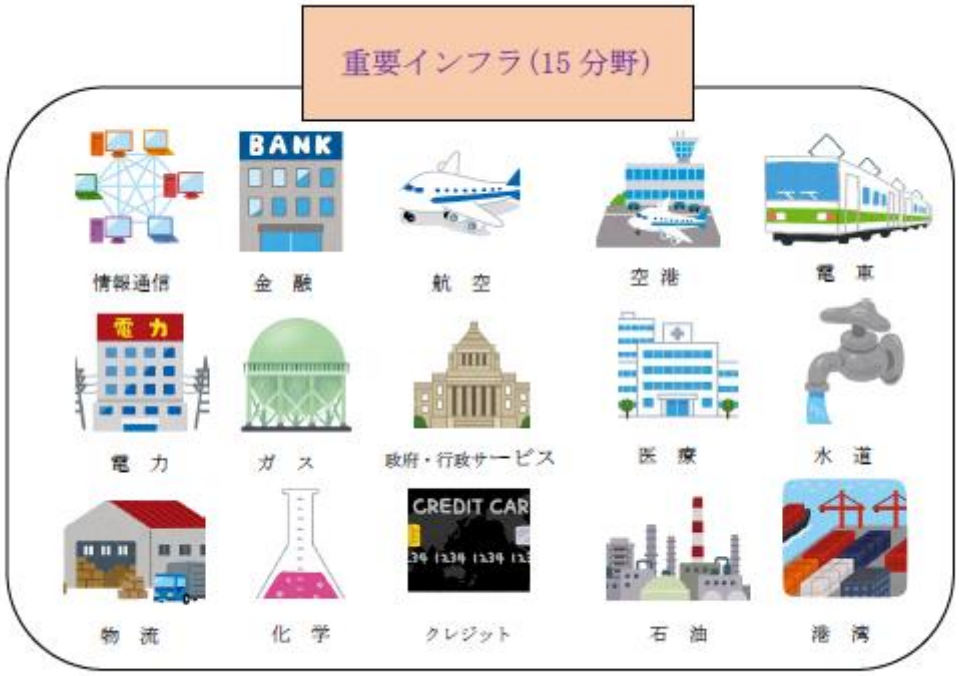
話合いのきっかけに、ぜひサイバー防犯標語「あひルのおやコ」をご活用ください。

サイバー防犯標語「あひルのおやコ」

サイバー攻撃の脅威

サイバー攻撃とは

サイバー攻撃とは、重要インフラ（情報通信・鉄道・電力・医療・物流など15分野）の基幹システムを機能不全に陥れ、社会の機能を麻痺（まひ）させる「サイバーテロ」及び情報通信技術を利用した諜報（ちょうほう）（スパイ）活動である「サイバーエスピオナージ」のことです。



サイバー攻撃には、

① 攻撃の実行者の特定が難しい
② 攻撃の被害が潜在化する傾向がある
③ 国境を容易に越えて実行可能である

といった特徴があり、その脅威は、国の治安、安全保障及び危機管理に影響を及ぼしかねない問題となっています。

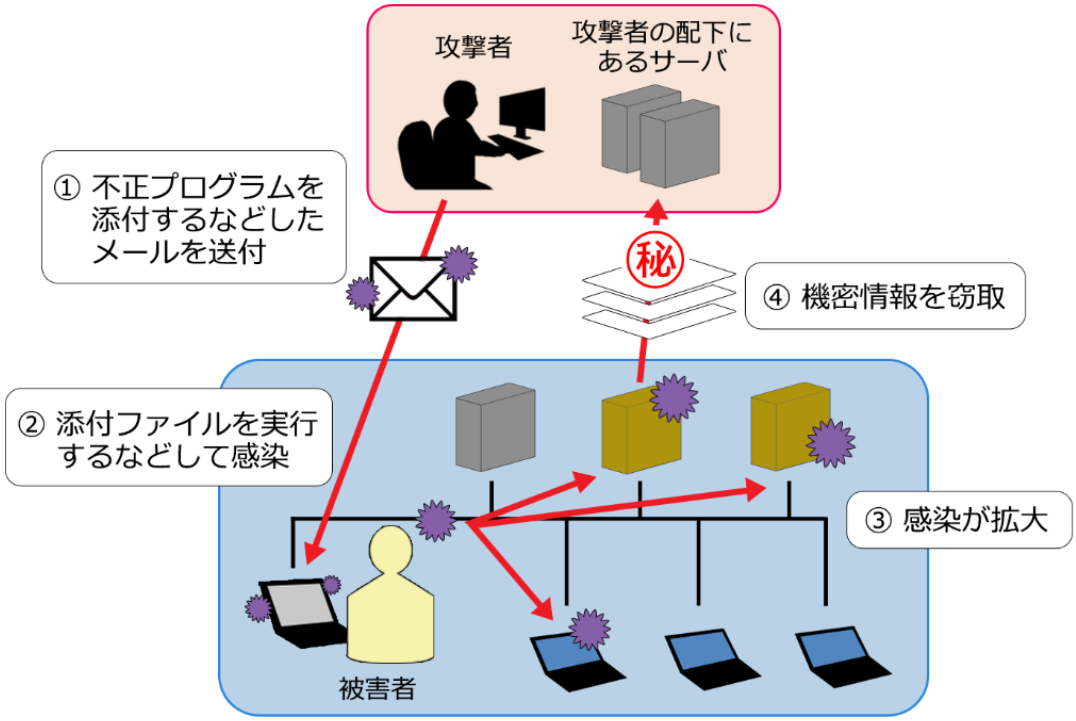
今後も攻撃が継続する可能性がありますので、サイバーセキュリティ対策を強化する必要があります。

サイバー攻撃の手口

サイバー攻撃に用いられる手口としては、攻撃対象のコンピュータに複数のコンピュータから一斉に大量のデータを送信して負荷を掛けるなどし、そのコンピュータによるサービスの提供を不能にする「DDoS 攻撃」やセキュリティ上のぜい弱性を悪用するなどして攻撃対象に侵入するもの、不正プログラムに感染させることにより管理者や利用者の意図しない動作をコンピュータに命令するものなどがあります。

また、不正プログラムに感染させる手口としては、業務に関連した正当なものであるかのように装った電子メールによる「標的型メール攻撃」が代表的です。

事例として、添付された圧縮ファイルを開くよう誘導するメールやメール中のリンク先に接続するよう誘導するメールがあり、国内でも多数発生しています。



【標的型メール攻撃による情報窃取の例】

攻撃事例

近年、国内外において政府機関や重要インフラ事業者などに対するサイバー攻撃が発生しており、最近の主な攻撃事例として

○　令和７年上半期、政府機関や金融機関などの重要インフラ事業者における DDoS 攻撃とみられる被害

○　令和７年４月、大手通信事業者に対する不正アクセス及び個人情報の流出などの事案が発生しています。

サイバー攻撃に対する警察の取組

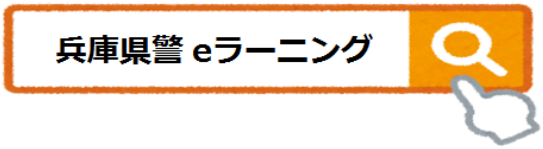
兵庫県警察では、サイバー攻撃対策を担当する「サイバー攻撃対策隊」を設置しているほか、各部門が連携し、サイバー攻撃の実態解明や被害の未然防止などを推進しています。

また、民間事業者などとの協力関係を確立して被害の未然防止を図るなど、サイバー攻撃をめぐる新たな情勢に対処するための対策に取り組んでいます。

県警では、Web 上でサイバーセキュリティに関する知識や対応方法を習得できる「サイバーセキュリティ e ラーニングシステム」を提供しています。

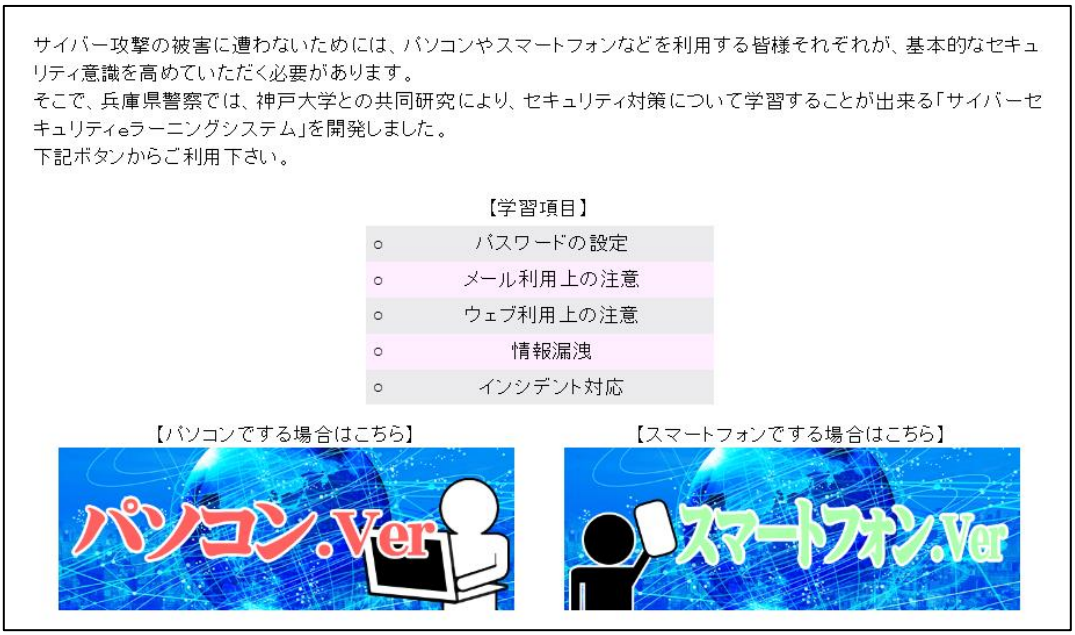
【ご利用方法】

① まずは Web で検索



兵庫県警察ホームページ
サイバー攻撃対策

② 「パソコン.Ver」「スマートフォン.Ver」のバナーを選択！



③　学習項目を選択してスタート


学習項目一覧

項目	基礎知識編	ストーリー編	テスト編
①パスワード設定	-	-	-
②メール利用	-	-	-
③ウェブ利用	-	-	-
④情報漏洩	-	-	-
⑤インシデント対応	-	-	-

○：学習済み/合格，－：未学習，×：不合格

前回の学習項目へ

《サイバー企画課》
《サイバー捜査課》
《公安第一課》