炎上　偽サイト　偽警告

ウイルス感染

誹謗中傷　なりすまし

個人情報流出　ランサムウェア

不正アクセス　偽メール

サイバー空間に潜む脅威と被害の防止

警察では、サイバー犯罪に対する様々な対策を行っています

警察へ寄せられたサイバー犯罪に関する情報を分析し、**事件捜査**を行うほか、**被害企業における対策に必要な情報の提供・助言、他の企業等への被害拡大を防止するための注意喚起**等の被害防止のための取組を行っています。

皆様からの情報提供がサイバー空間の安全につながります。

サイバー犯罪に関する情報の分析

サイバー犯罪事件の捜査

被害の拡大防止・再発防止

サイバー犯罪の被害に遭った場合には、警察本部または最寄りの警察署に通報・相談をお願いします。

北海道警察

サイバーセキュリティ対策本部

サイバーセキュリティ講座はこちらから

身近な脅威と今すぐできる対策例

脅威1　SNS型投資詐欺・ロマンス詐欺に注意

SNSを通じて、暗号資産や株に投資すれば利益が得られるものと思わせ金銭をだまし取る**SNS型投資詐欺**、恋愛感情や親近感を抱かせながら投資に誘導し、投資金名目や交際を続ける名目で金銭をだまし取る**SNS型ロマンス詐欺**が急増しています。

SNS型投資詐欺、ロマンス詐欺被害に遭わないために

SNS型投資詐欺
①投資先が実在しているか・国の登録業者かどうか確認する
②「必ずもうかる」「あなただけ」といった勧誘に注意する
③投資を勧めている著名人のなりすましに注意する

SNS型ロマンス詐欺
①実際に会ったことがない人からお金の話をされたら要注意
②「投資」に誘導されたら要注意

脅威2　フィッシングによる個人情報等の詐取

公的機関や金融機関、ショッピングサイト、宅配業者等の有名企業をかたるメールやSMSを送信し、正規のWebサイトをかたった偽サイトへ誘導することで、認証情報やクレジットカード情報、個人情報を入力させて詐取するフィッシングの被害が増加しています。
詐取された情報が悪用されると金銭的な被害に遭ってしまいます。

フィッシング被害を防ぐために

①メールやSMSのリンクは安易にクリックしない
②利用しているサービスの多要素認証の設定を有効にする
③迷惑メールフィルターを利用する

脅威3　あなたの書き込みは世界中から見られている？

SNSの利用にはリスクがある点に注意しましょう。

モラルを欠いた文章や画像を投稿し「不適切」と認識されて炎上する

内容や設定によっては、名前や学校・会社、場所などが特定される

誹謗中傷やプライバシーの侵害などに該当する書き込みを行う

顔の見えない相手とのやりとりには危険が潜んでいる

トラブル防止のために

①投稿する前に内容を確認する
②プライバシー設定を確認する
③公開範囲を確認する
④写真掲載による位置情報の流出に注意する
⑤SNS上で知り合った人とのやりとりに十分注意する

脅威4　企業を狙うランサムウェアに要注意!!

ランサムウェアとは、金銭を脅し取ることを目的としたソフトウェアで、感染するとコンピュータ内のファイルが暗号化され、ファイルの使用が不可能になる上、暗号化の解除などの名目で「身代金」を要求される手口です。

発生要因/手口

①VPN等の脆弱性やアカウントの管理不備により不正侵入されて感染
②リモートデスクトップのアカウントに不正に侵入されて感染
③メールの添付ファイルやメール本文中のURLリンクから感染

VPN（Virtual Private Network）：仮想の専用線

感染リスクを減らすため

①VPN等の周辺機器やソフトウェアは適宜、修正プログラムを適用する
②VPNやリモートデスクトップのアカウントを適切に管理し、不要なアカウントの削除を確実に実施するとともに、パスキーや多要素認証などを導入する
③パソコンや周辺機器のOS、ウイルス対策ソフトは常に最新状態にアップデートする
④不用意にメールの添付ファイルや本文中のURLリンクを開かない

万が一感染した場合に備えて

①重要なデータは必ずバックアップを取る
②バックアップを取った媒体は、必ずネットワークから切り離して保管する
③有事に備えて専門担当部門（CSIRT）を設置し、対応手順の策定や教育等を行う

脅威5　内部不正による情報漏えい等の被害

従業員や元従業員等の組織関係者による機密情報の持ち出しや、社内情報の削除等の不正行為が発生しています。
組織関係者による不正行為は、組織の社会的信用の失墜や損害賠償、業務停滞等による経済的損失を招きます。

対策と対応

①情報資産を把握し、その重要度を把握した上で重要情報の管理者を定める
②重要情報の利用者IDおよびアクセス権の登録・変更・削除に関する手順を定めて運用し、不要な利用者ID等は直ちに削除する
③重要情報の格納場所や重要情報を扱う執務室への入退室を管理する
④重要情報へのアクセス履歴や利用者の操作履歴等のログを記録する

脅威6　取引先などをかたる「偽メール」に注意

【標的型メール】

業務に関連した正当な電子メールを装い、マルウェア（コンピュータウイルス）を添付した電子メールを送信し、受信者のコンピュータをマルウェアに感染させる手口です。

【BEC：Business E-mail Compromise（ビジネスメール詐欺）】

犯人が企業経営者や取引先業者になりすまし、標的とする会社にメールを送信して金銭等をだまし取る手口です。

標的型メールや偽メール等によるウイルス感染や情報流出を防ぐために

①不用意にメール本文中のURLリンクや添付ファイルを開かない
②本物のメールかどうか分からない場合には、送信元にメール以外の手段（電話や面接）で送信事実を確認する
③「100%防ぐことはできない」ということを理解し、万が一に備えて対応要領や体制づくりをしておく

脅威から身を守るために

サイバーセキュリティは『知識』より『意識』!!

最新の脅威や手口の知識を持っていても、行動に移して対策しなければ、被害を未然に防ぐことはできません。
『意識』があってはじめて『知識』が生かされます。

OSやソフトウェアは常に最新の状態にしましょう！

アップデートには、機能追加や性能向上と、不具合の修正という、大きく２つの目的があります。最新の状態にしないと、不具合が修正されず、危険な状態となります。

ウイルス対策ソフトを導入しましょう！

常に最新のウイルスに対応できるよう、OSやソフトウェアと同様に更新が必要です。
ただし、対策ソフトで完璧にウイルスを防ぐことはできません。

IDやパスワードをしっかりと管理しましょう！

パスワード等は人目につくところに書いておかないようにしましょう。
紙に書いて他人に見られない場所に保管したり、パスワード管理ソフトを使用したりすることも有効です。

大事なデータはバックアップしましょう！

万が一のウイルス感染等に備え、大切なデータは、セキュリティの強い安全なクラウド上へ保管するなど、バックアップを行いましょう。

従業員教育（人的対策）を行いましょう！

従業員教育を行い、セキュリティ意識を身につけてもらいましょう。
これにより被害に遭いにくい職場環境を構築できます。

この資料で紹介したサイバー空間における脅威と対策は、ほんの一例です。
サイバー空間の脅威（手口）は時間の経過とともに変化していきますが、私たちが講ずる基本的な対策や心構えはそう大きく変わることはありません。
まずは皆さん自身がサイバーセキュリティに対する「意識」を持つことから始めていきましょう！

北海道警察　サイバーセキュリティひろば　検索

サイバー衛生管理研修のお知らせ

日本サイバー犯罪対策センターでは、オンラインによるサイバー衛生管理研修を実施しています。お気軽に参加してください。

- 研修システムへのアクセス
- 利用者登録
- 事前アンケート
- オンライン研修の実施
- 確認クイズ・事後アンケート

サイバー衛生管理とは？
日常的にIT環境の衛生管理を行い、パソコンなどのIT端末を健康な状態に保つことです

※ 北海道警察は「サイバー衛生管理研修」に協力しています

https://doukei.hygiene.jc3-learning.org/