インターネット利用時の注意点

～被害者にも加害者にもならないために～

保存版

みんなで学ぼう！

和歌山県警察マスコット
きしゅう君

その1　コンピュータウイルスへの感染

1　コンピュータウイルスって何？

ホームページや電子メール、SNSを見たり、使った時などに感染し、機器に侵入して悪さをするソフトウェア・プログラムです。様々な機能を持つものが次々に開発されています。**インターネットに繋げることができる機器全てに感染の危険性があります。**

悪意のあるソフトウェアの総称の意味である**「マルウェア」**とも呼ばれています。

2　感染した時の被害は？

セキュリティの抜け道を作られ、大切な情報を盗まれる

自分が知らない間にセキュリティに抜け穴を作られ、犯罪者が自由に侵入できるようになります。パソコンやスマートフォン、それに接続するUSBメモリやmicroSDカードなどの外部記録媒体等から**あらゆる情報を盗まれてしまいます。**

ランサムウェア感染画面【イメージ】

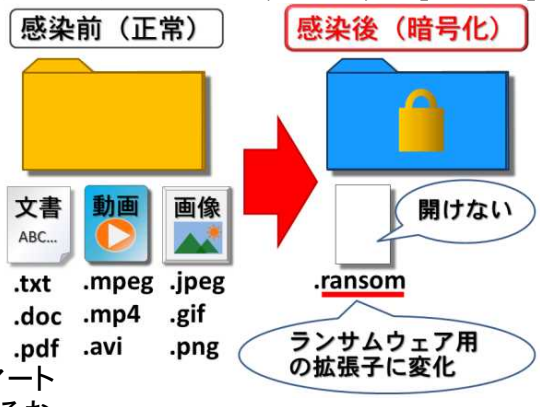
端末やファイルをロックされて使用不可になり復旧と引き替えに『身代金』を要求される

『ランサムウェア』（身代金要求型不正プログラム）と呼ばれるコンピュータウイルスです。世界規模のサイバー攻撃に使われ、各国で大きな被害が発生しました。**金銭を支払っても復旧する保証はありません。**

サイバー犯罪・攻撃に荷担させられる

スマート家電などの『IoT機器』が感染すると、感染したIoT機器が、サービスを提供するコンピュータ（サーバ）に多量の通信を行ってダウンさせる等、**サイバー攻撃に荷担させられてしまいます。**これまでにも、オリンピック・パラリンピック競技大会のような国際的イベントを妨害するためのサイバー攻撃などに悪用されています。

ランサムウェアによるファイルロック【イメージ】



遠隔操作による嫌がらせ、常時監視

無断で保存しているデータを見られる、勝手に書き換えられる、誹謗中傷のメッセージを勝手に送られるなど様々な被害に遭うおそれがあります。Web防犯カメラ、PCやスマートフォンが感染すると、**カメラで利用者の行動を常時監視**されるおそれがあります。

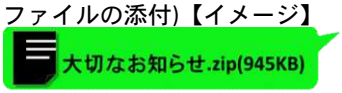
また、犯罪者が、知人や交際相手のスマートフォンに**『盗難防止アプリ』**を勝手にインストールし、行動を監視した事案も発生しています。【『用法上のウイルス』】

端末の常時監視【イメージ】

3 どうやって感染するの？

標的型攻撃(ＵＲＬの添付)【イメージ】

標的型攻撃(ウイルス入り圧縮ファイルの添付)【イメージ】



ファイルを開く

SNSやメールの添付ファイルを開く【**『標的型攻撃』**等】
ホームページからデータをダウンロード。

不正広告【イメージ】

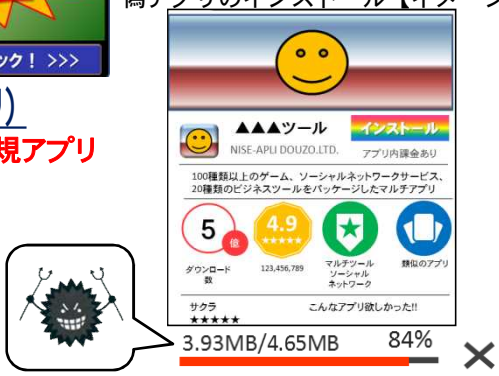
ホームページ(ウェブサイト)の閲覧

改ざんされた正規サイト、偽サイト、不正広告、
SNSやメールの添付URL等へのアクセス。

ソフトウェアやアプリのインストール（偽アプリ）

偽のOS、ソフトウェア、アプリなど（正規マーケットの中に**正規アプリに見せかけたコンピュータウイルス**が存在します。）

偽アプリのインストール【イメージ】



外部記録媒体の接続

すでに感染した外部記録媒体（USBメモリ、microSD、外付けハードディスクドライブなど）
インターネットに接続していなくても感染します。

その2 不正アクセス（不正ログイン）

1 不正アクセスって何？

ネットワーク（インターネットやLAN）を通じて不正な手段を用い、本来アクセスできないコンピュータやネットワークに侵入することです。

他人のID、パスワードなどを無断で使用する、システムの脆弱性（弱点、セキュリティホール）を突く、コンピュータウイルス（「バックドア」）を感染させ侵入経路を作るなど様々な方法があります。

ID・パスワードの管理やセキュリティ対策をきちんとしていないと被害に遭うおそれがあります。

2 不正アクセスされた時の被害は？

- インターネットバンキングの不正送金
- インターネットショッピングの不正購入
- オンラインゲームなどサービスの不正操作
- 情報の盗み見、窃取、改ざん(情報流出)
- なりすましによる詐欺・情報発信
- ホームページの改ざん・消去

3 事例①『フィッシング』

正規の金融機関やショッピングサイトなどを装い、ID、パスワード、クレジットカード番号、氏名・住所などの**個人情報を入力させて盗む方法です。**

ホームページへのログインなどと称して入力を求める**「サイト構築型」**、会員情報の確認などと称したメールを送りつけ入力を求める**「メール送信型」**があります。

被害者を欺くため、正規のものとそっくりに作られており、ウイルスに感染させるために**偽アプリのインストールを求める**手口もあります。

フィッシング入力画面【イメージ】

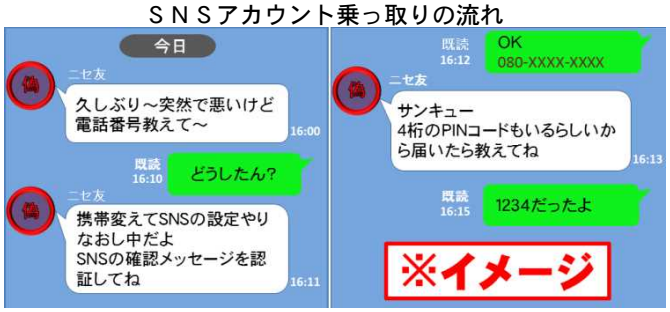
様々なサービスを装い、情報の入力を求めてくるのでご注意を

4 事例②『アカウント乗っ取り』

友人・知人を装い、SNSアカウントへのログインに必要な電話番号や認証番号（PINコード、これに類する番号）等を聞き出す手口です。不用意に認証番号を教えると、不正にログインされてアカウントを乗っ取られ、パスワードを変更されます。

認証番号を聞き出そうとしてきた時は要注意です。

ＳＮＳアカウント乗っ取りの流れ



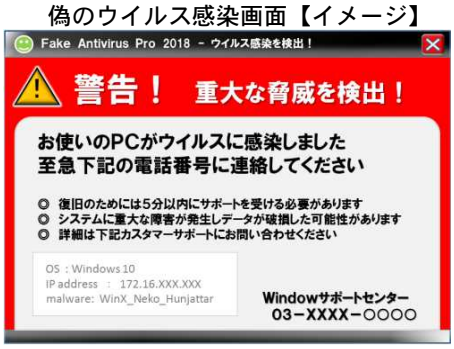
その3 インターネット詐欺

1 インターネット詐欺の現状は？

アダルトサイトの利用料金、懸賞金（品）の当選など様々な内容の架空請求が横行しています。

近年は偽サイト、サポート詐欺などによる被害も発生しています。

偽のウイルス感染画面【イメージ】



2 サポート詐欺

ポップアップ機能を使って**偽のコンピュータウイルス感染画面を表示させて**利用者を動揺させ、感染画面内の偽サポートセンターに電話させて**サポート費用を騙し取る**手口です。

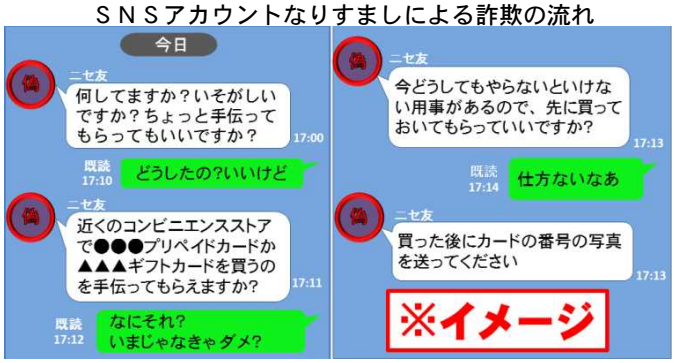
ウイルス駆除の作業を装うために**遠隔操作ソフトをインストールさせられるため、不正操作されるおそれがあります。**

3 なりすましによる詐欺

乗っ取ったSNSなどのアカウントを使い、**元のアカウント主になりすまして行う詐欺**です。

犯罪者は騙す相手に、コンビニエンスストア等で**プリペイドカードを購入させ、カードに記載されているシリアルナンバーを聞き出そうとします。**（シリアルナンバーを写真撮影させ、画像データを送付させる手口があります。）

ＳＮＳアカウントなりすましによる詐欺の流れ



4 偽サイト・詐欺サイト

ロゴの転用など**実際に存在するサイトを真似て作ったサイト**を偽サイト、**購入代金等を騙し取るため、正規のサイトに見せかけて作ったサイト**を詐欺サイトと言います。

偽サイト等の特徴をよく確認し、少しでも不審なサイトの利用を避けましょう。

偽（詐欺）サイト【イメージ】

① 通信が暗号化されていないことが多い
② URLが特徴的（他国のレンタルサーバで、ドメインネームが安価に取得できるものが多く、正規サイトと酷似している等）
③ 支払方法が限定的（「銀行振込だけ」等）
④ 会社情報が記載されていない（あっても他社の無断転用や存在しない情報の場合も）
⑤ 実際の連絡方法がメールのみ
⑥ 日本語が不自然（外国語を機械翻訳）
⑦ ロゴ等が無断転用されている（コピー）
⑧ 極端に値引きされている

その4　インターネット利用時の危険から身を守る

1　インターネットの特徴（危険性）

- 情報が**一瞬で世界中に拡散**し、**悪意のある人も目に**します（流出した情報は**二度と削除できません**）。
- 匿名性、手軽さを背景に、**大量の情報（善悪・真偽）、多様な意見（賛否）**が出まわります。
- 情報の入手・発信は、**年齢層を問わず、利用者自身の判断・責任で行う**こととなります。

2　被害者にならないために

- **自分の個人情報、画像、行動履歴を掲載しない、相手に送信しない**

  つきまとい、ストーカーなどの被害に遭うおそれがあります。
  GPS機能付きカメラで撮影された画像には位置情報が残っている可能性があります。
  LINE、FacebookなどSNSの場合、**プロフィール等の公開設定を制限し、友達申請の承認を慎重に**しましょう。

- **インターネットで出会った相手を簡単に信用しない**

  SNS、ホームページ上におけるやりとり、出会い系・援助交際・自殺サイト（誘う書き込み含む）等で知り合ったり出会った相手から犯罪被害を受けるケースが増加しています。**画像の拡散をネタにした脅迫（リベンジポルノ等）、わいせつ行為、監禁、略取・誘拐、最悪の場合殺害される等の事件が発生**しています。

  犯罪者は『理解者のふり』をして近づく
  「友達の友達」は『知り合い・友達ではない』

3　加害者にならないために

- **メッセージ、画像、動画の投稿時は内容に気をつける【人の気持ちへの配慮】**

  本当に発信して良い情報かよく考えてから投稿しましょう。**自然災害発生時のデマ投稿は大混乱を招きます。**

  名誉毀損、業務妨害など投稿だけで犯罪になることも
  損害賠償・慰謝料を請求される
  「炎上」して世界中から批判にさらされる
  解雇・退学など社会的制裁を受ける

- **インターネット上のサービスは、法律や利用規約（ルール）に沿って利用する**

  アカウントの転売、データのダウン（アップ）ロード等は、内容により犯罪になるおそれがあります。**利用規約に違反**してデータの消失等トラブルに見舞われた場合、**管理者からアカウントを凍結されたり、保証や復旧を拒否される**場合もあります。

対策　インターネットを安全に利用するために

1　**ウイルス対策ソフトの利用・常に更新**　ウイルス検知率を高めましょう

2　**OS・ソフトウェア・アプリを常に更新**　アップデートやパッチで弱点を修正

3　**ID・パスワードを正しく管理**　「初期値、使い回し、推測しやすい、他人に教える」等は絶対 ✖

4　**定期的にバックアップをとる**　ウイルス感染時など復旧に有効　保存先はネットから必ず切断

5　**スマート家電等を正しく管理**　初期パスワードの変更、接続設定の確認

6　**公衆無線LAN利用時の注意**　暗号化・信頼性の無いアクセスポイントは要注意

7　**新たな認証方法**　多要素認証の利用を　ﾜﾝﾀｲﾑﾊﾟｽﾜｰﾄﾞ　トークン　生体認証(指紋、顔等)

8　**書き込み・データの送信前に確認**　相手はあなたを狙った犯罪者かも

9　**脅威・手口を知る**　各機関のホームページ等で最新の手口を知りましょう

検索ワード例　「警察庁」「NISC」「JC3」「IPA」「国民のための情報セキュリティサイト」など

10　**冷静な対応**　被害に気づいたら**速やかにネットワークを切断**、警察・通信事業者等に相談

【発行元】　和歌山県警察本部サイバー犯罪対策課　　073-423-0110㈹