「ウィルス」と「ネット詐欺」

いかにして、ＰＣ・スマホのセキュリティを維持するか

北摂SITA　12月勉強会（2020年１２月12日）

AO_takatsuki

1．コンピューターウィルス
- 1.1　ウィルスの種類と概要
- 1.2　感染経路と防止策
- 1.3　感染時の症状と対策

2．ネット詐欺
- 2.1　ネット詐欺の種類と手口・対策

1.1　ウィルスの種類と概要

- **「ワーム型ウイルス」**
- ・特徴　　強い感染力・自己増殖機能が強いコンピューターウイルス
- ・感染経路　　コンピューターウイルスが仕込まれているサイトで、**「クリックしたURL」**や
- **「電子メール」**、**「ファイル」**、**「USBメモリ」**などから感染。
- ・作用　　コンピューターの動きを止める、誤作動を誘発する、情報を盗む、
- コンピューター内にウイルスファイルのコピーを複製してハードディスク容量を
- 使いつくす等　発生する。

- **「トロイの木馬型ウイルス」**
- ・特徴　　悪質ではないもの（安全なもの）として知らぬ間に感染。
- ※知らない間に悪意のあるプログラムをインストール・実行し、場合によっては、
- インターネットを通じた犯罪の加担者となったりする可能性あり。
- ・感染経路　　何かしらのプログラムを**インストール**したり、**ファイルを開いたり**することで感染。
- ・作用　　ハードウェア内にある重要な情報を「抜き取られてしまう」、「操作を乗っ取られる」等、
- 発生する。

- **「マクロ型ウイルス」**
- ・特徴　　マイクロソフト社のOfficeアプリケーション（Word、Excelなど）のマクロ機能を利用して感染するタイプのウイルス。
  マクロ機能を乗っ取ることで、ファイルの書き換えや削除などの操作・自己増殖を開始。
- ・感染経路　　ウイルスが仕込まれた**ファイル**を開いたときや、感染している**Officeアプリケーション**を**開いたとき**感染。
- ・作用　　ファイルの削除やアプリケーションの設定が、ウイルスによって変更されてしまい、「作業内容の保存ができない」、「ウイルス付きのメールを大量に送信されてしまう」等発生する。

1.2　感染経路と防止策

● 感染経路

- メールによる感染
- 　①メールの**添付ファイルを開いた**だけで感染。
- 　※悪質なものでは、添付ファイルを開かなくてもウイルスに感染するものもあり。
- 　（メールの表示形式をHTML形式にしている場合）
- 　②メール本文内に記載されている**URLをクリック**することで感染。

- インターネットによる感染
- 　①ウイルスが仕掛けられた**悪意のあるページを閲覧**して感染。
- 　②**ウイルスに感染したファイル**をパソコンに**ダウンロード**し、そのファイルを
- 　　**開く**ことにより感染。

- ネットワークによる感染
- 　①同一ネットワーク内（家庭内で複数のPCを接続等）の1台のパソコンがウイルスに感染し
- 　　**他のパソコンに感染**。

- 各種記憶媒体からの感染
- ①各種**記憶媒体**（※）のデータの中にコンピューターウイルスが含まれていた場合に
- パソコンと接続するだけでウイルスに感染。
- ※USBメモリー、CD-R、DVD-R、BD-R、外付けのハードディスク等

●防止策

＜基本事項＞
①OSやアプリ（OfficeやJava等）のセキュリティ対策を最新のものにしておく。
②セキュリティソフト等を導入する。
③メールの表示形式を、テキスト形式とする。（HTML形式は使用しない）

＜操作上の対策＞
①心当たりがないメールに**添付されているファイル**や、**メール本文内のURL**を
むやみに開かない。

②インターネットは必要な情報のみを検索し、むやみに**広告などをクリックしない**。

③所有者や中身に覚えのないUSBメモリーなどは使わない。

1.3　感染時の症状と対策

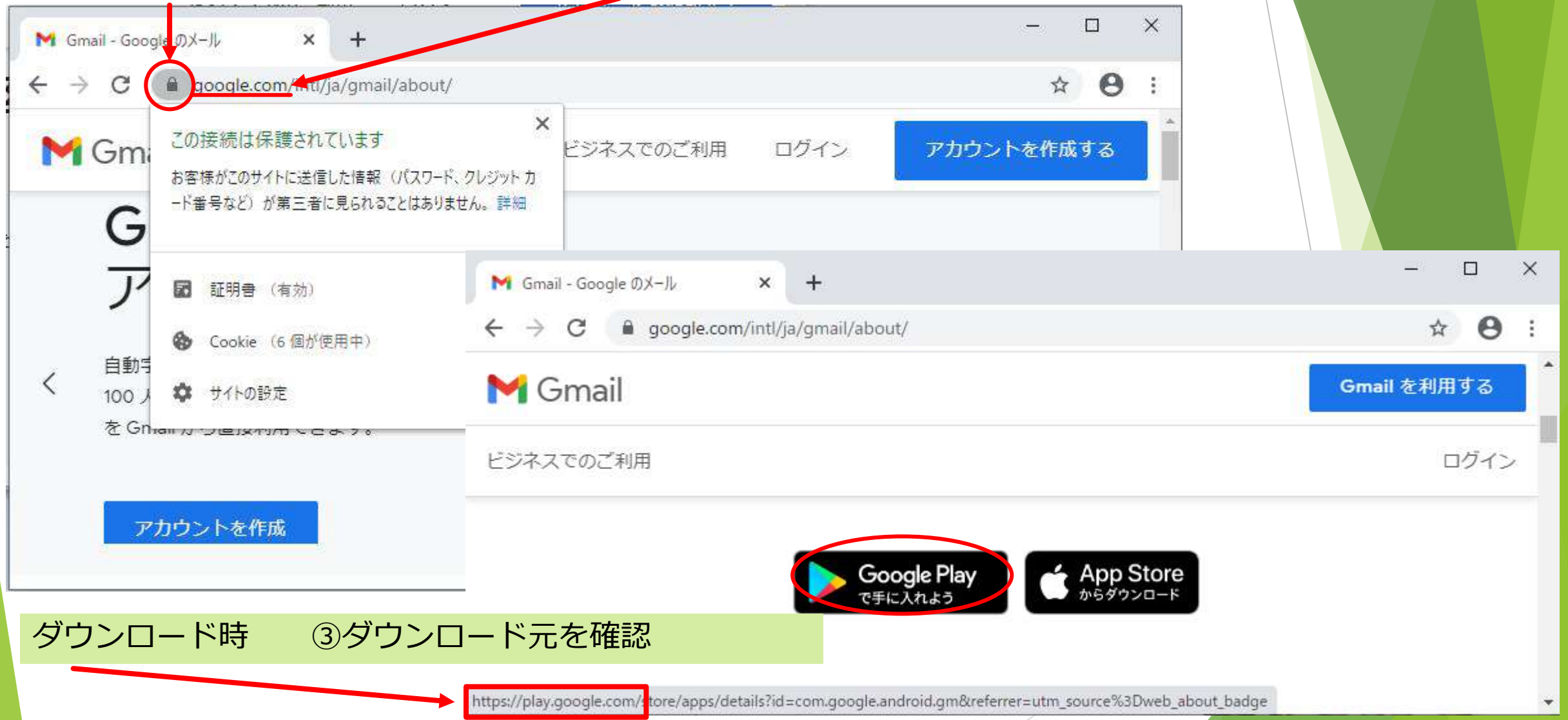
- 感染した場合の症状（下記状況が発生した場合感染の疑いあり)
- ①突然電源が落ちたり、ブラウザが再起動する。
- ②セキュリティソフトが突然終了する。
- ③特に作業していないのにCPU使用率が急上昇する。
- ④動きが遅い、データ通信使用量の消費が多い。

- 感染した場合の対策
- ①ネットワークから切り離す。
- ②ウイルス対策ソフトウェアで駆除。
- ※ウィルスソフトは、最新のパターンファイルに更新しておくこと。
- ③駆除確認後、念のためフルでウィルススキャンを実行。
- ウイルスソフトで駆除できなかった場合。
- ④リカバリーやOSの再インストール
- ※リカバリ等に備えて、事前にファイルの定期的なバックアップ等が必要。

●インターネット検索時のチェック項目

信頼できるサイトか　①https か？

信頼できるサイトか　②urlは正しいか？



ダウンロード時　　③ダウンロード元を確認

https://play.google.com/store/apps/details?id=com.google.android.gm&referrer=utm_source%3Dweb_about_badge

「迷惑メール」のサンプル


差出人: @yahoo.co.jp> 送信日時: 2014/03/02 (日) 20
宛先: @hotmail.com
CC:
件名: 「 銀行」本人認証サービス

銀行Eメール配信サービス

2014年「 銀行」のシステムセキュリティのアップグレードのため、貴様のアカウントの利用中止を避けるために、検証する必要があります。

以下のページより登録を続けてください。

https://entry11.bl /loginib/login? TRANID=AA000 001

Copyright(C)2014 The Bank of All rights reserved

不自然な日本語を含む迷惑メールの例

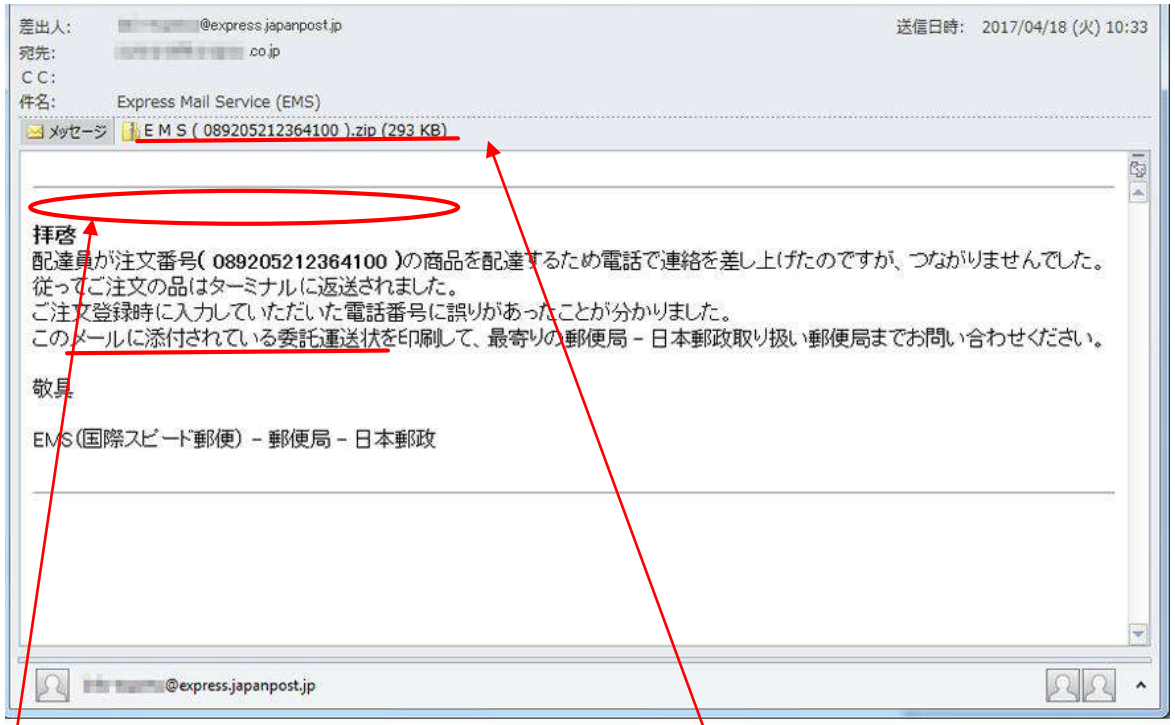
①メールアドレスがフリーメールアドレス
②日本語が不自然


差出人: ヤマト運輸株式会社 <email@kuronek.yamato.co.jp> 送信日時: 2017/04/20 (木) 15:17
宛先:
CC:
件名: 宅急便納品完了のお知らせ
メッセージ ZBA 143671352723.ZIP (141 B)

ヤマト運輸をご利用いただきありがとうございます。
宅急便をお受け取り店舗へ納品しましたので、ご来店ください。
■伝票番号：759433940653
お受け取りの際は、下記のものを必ずご持参ください。
1．本人確認証（運転免許証等）
2．ご印鑑
（お問合せ先）
ヤマト運輸株式会社
お客様サービスセンター
0570-200-736
※このメールに返信されましても、お答えする事は出来ませんのでご了承願います。

ヤマト運輸株式会社

配達業者を装う迷惑メール
①荷物の受取人の名前（受信者名）が記載されていない
②添付されている圧縮ファイル（拡張子が.zipのファイル）の中にあるファイルを受信者が開いてしまうとウイルスに感染



添付されている圧縮ファイル（拡張子が.zipのファイル）の中のファイルを開いてしまうとウイルスに感染

荷物の受取人の名前（受信者名）が記載されていない

2．ネット詐欺
2.1　ネット詐欺の種類と手口・対策

- ◎**フィッシング詐欺**　　フィッシングはphishingという綴りで、魚釣り（fishing）と洗練（sophisticated）から作られた造語
- 　実在の企業名をかたる「なりすましメール」を送り、偽のサイトにアクセスさせ、ID・パスワードなどの個人情報を盗み悪用する手口。
- ◎**ワンクリック詐欺**
- 動画閲覧中に突然「会員登録完了」などのメッセージを表示し、高額な料金請求をしてくる手口。
- ◎**偽警告**
- 「ウイルスが見つかりました」などの偽の警告メッセージを表示し、偽セキュリティソフトを買わせたり、ウイルス駆除費用を請求する手口。
- ◎**偽通販サイト**
- 一見、普通のショッピングサイトに見えるが、お金だけ搾取して商品を送ってこない、または粗悪品・偽ブランド品を送ってくる手口。
- ◎**ランサムウェア**　　Ransomware、身代金を意味する「Ransom」と「Software」による造語
- パソコンやスマートフォンをロックして使えなくする悪意のあるソフトウェア。ロック解除のために金銭（身代金）を支払うよう求めてくる手口。

◎フィッシング詐欺

- 典型的な手口としては、クレジットカード会社や銀行からのお知らせと称したメールを送信したり、リンクをクリックさせる。
- 本物そっくりな偽サイトに利用者を誘導。
- クレジットカード番号や口座番号などを入力するよう促し、入力された情報を盗み取る。

○×カードより

いつも当社のクレジットカードをご利用頂きまして、誠にありがとうございます。

最近、他人のクレジットカードを利用して、不正にショッピングを行う悪質な犯罪が増加しています。そのような不正利用への対策として、当社では一定期間ごとに暗証番号の変更をお願いしています。
以下のURLから弊社のホームページに接続して頂き、お名前、クレジットカード番号、暗証番号をご登録ください。

http://www.××××.com/henkou/

なお、このメールをお受け取り頂いてから1ヶ月以内にご登録頂かなければ、お持ちのクレジットカードがご利用できなくなるため、ご注意ください。

＜対策＞

不審なメールのURLをクリックしない。

※金融機関では口座番号や暗証番号を電子メールで問い合わせることはない。
URLにアクセスする場合は、以下を確認。
①契約時に通知されているURLと同じかどうか。
②Webブラウザのアドレス欄の左端にある鍵のアイコンをクリックして表示される証明書が本来の企業のWebサイトか。
⇒　重要な情報の入力を求めるページで、SSLが使用されていない場合は、まずはフィッシング詐欺を疑う。

◎ワンクリック詐欺

- 利用者の興味を引きそうな電子メールや電子掲示板などを利用し、いかにも正当な契約手続きが完了しているかのように見せかけ、利用料を不正に請求。
- 料金請求の際、携帯電話の個体識別番号や、パソコンの固有識別番号等の情報などを表示させ、利用者の個人情報が“複雑な技術によって”特定されたように見せかける。
- 「スマートフォンでの新しい手口」　①自動的に電話を発信させる
- 　　②請求画面が表示された時にシャッター音が聞こえる

ご入会ありがとうございます。あなたの個体識別番号は以下の通りです。

2468XXXXX

サービスのご利用料金は1ヶ月間で8,000円です。1週間以内にお振り込み頂けなかった場合には、ご自宅にまで回収にお伺いすることになります。その場合には、延滞料金30,000円および回収にかかる実費と交通費で32,000円、合計62,000円を追加して頂戴することになりますのでご了承ください。なお、お支払い頂けない場合には、裁判所からご連絡がいくことになります。

＜対策＞

不用意にWebサイトにアクセスせずに、電子メールや電子掲示板の文面をきちんと読んで利用。

クリックした場合。

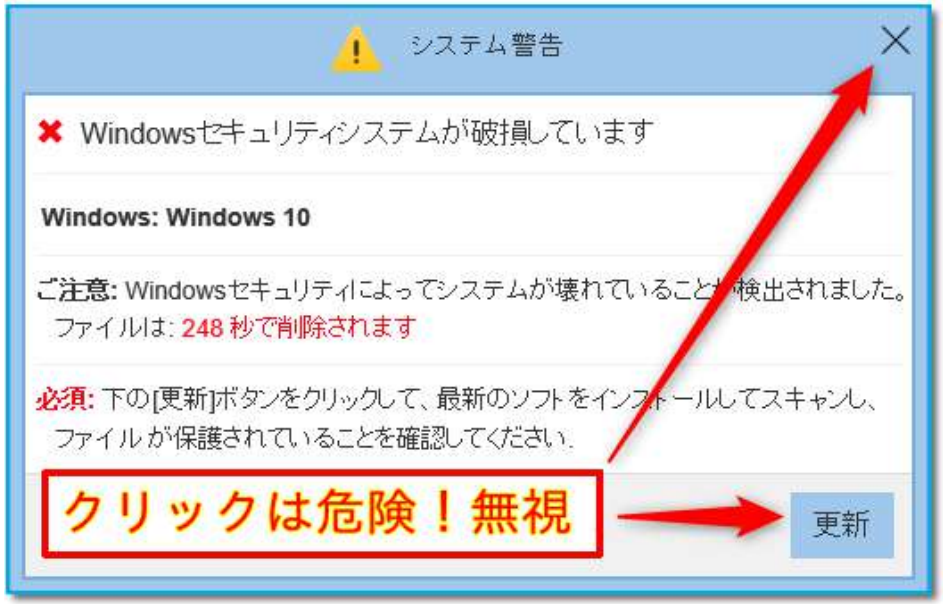
①あたかも個人が特定されたような表現で、「お支払い頂けない場合には、自宅にまで伺います」といった脅し文句が書かれていても、真に受けないこと。

②業者に連絡を取らないこと（利用状況や支払理由などを確認する等のため）。

⇒　トラブルになりそうなときには、表示されているデータを保存したり、画面を印刷したりしておくこと。
総務省電気通信消費者相談センター、消費生活センター、警察などに相談。

◎偽警告

- パソコン画面にウイルス感染の警告を出し、Windowsパソコンで、突然「システム警告」「システム破損」と表示。ブラウザーを閉じられない状態にする。
- 対策ソフトの名目などで金銭をだまし取る。



＜対策＞
警告表示が次々と繰り返されるが、クリックせずすべて無視する。
ブラウザを終了させることができない場合、下記手順にて停止させる。

「停止手順」
①キーボードで[Ctrl]＋[Shift]＋[Esc] 同時押し、タスクマネージャーを起動。
②プロセス画面にて、開いていたブラウザーを探し選択、右下のタスクの終了（複数存在する場合あり）をクリック。
③ブラウザーを開き直すし、「セッションの復元」が表示されたら、「Ｘ」で閉じる。

◎偽通販サイト

- 実在する通販サイトを模倣していたり、一見すると問題無いショッピングサイトでも、注文したものと異なる模倣品が届いたり、商品が届かず返金もされない対策ソフトの名目などで金銭をだまし取る。
- **商品が送られてこないだけでなくカード情報が不正利用されてしまう**危険がある。

(商標侵害が疑われる衣類販売サイト：消費者庁発表)

消費者庁は不審なサイトのリストを公開
消費者庁では2019年4月19日に「悪質な海外ウェブサイト一覧」を更新
https://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/pdf/caution_internet_190920_0001.pdf

＜対策＞

● **サイトのURLに怪しい点がないかチェック　URLが一文字違う等（www.nitori-net.jp <> www.mitori-net.jp）**
URLの左端に**「鍵マーク」**がついていなかったり、**「https://~」**で始まっていないサイトは通信が暗号化されていない。
また、URLの終わりが「.top」「.xyz」「.bid」など見慣れないものの場合も注意が必要。

● **会社の概要、販売者の情報をチェック**
会社の概要や販売元といった販売者情報を確認するように心がける。

● **店舗ロゴと販売商品をチェック**
取扱商品が、店舗名とあまりにも関係ないものを取り扱っている場合は注意。

● **決済方法をチェック**
代金の支払い方法として、銀行振込しか選択できず、クレジットカードや代引きがなどの決済方法が選べない場合は注意。

◎ランサムウェア

- スパムメールや、改ざんした正規サイトから、脆弱性を攻撃する不正サイトへ誘導され、ランサムウェアに感染する。
- ランサムウェアが活動開始すると、感染PCの特定機能を無効化し操作不能にする、もしくは、データファイルを暗号化し利用不能にする。
- PCを感染前の状態に戻すことと引き換えに金銭の支払いを要求する画面が表示。
- 身代金の要求に加え、暗号化する前にデータを窃取しておき、「支払わなければデータを公開する等」脅迫する。(カプコン、2020年11月初めにランサムウェア攻撃を受ける)

WannaCryptor に感染させられた端末の画面

＜対策＞
あらゆる面でのセキュリティの強化で対応する必要がある。
ウイルス対策、不正アクセス対策、脆弱性対策など、基本的な対策を、確実かつ多層的に適用する必要あり。

その他
◎スパイウェア

- 知らないうちにパソコンにインストールされ、個人情報を盗み出したりユーザーの操作に反してパソコンを動作されたりする。
- 怪しげなメールの添付ファイルを開いた時、メールの本文に記載されたURLをクリックした時、Webサイトから素性がよくわからないソフトをダウンロードした時に侵入。
- 一度パソコンの中に入ってしまうと、検出ソフトを使わなければ削除することが難しい。

- **感染確認・駆除する方法**
- セキュリティ対策ソフトを利用

- **<対策>**
- 不審なソフトはインストールしない
- 怪しいポップアップなどはクリックしない
- 怪しいサイトには接続しない
- 不審なメールは開かない

◎まとめ

- ウイルス・詐欺対策（メール）
- ①不審なメールは開かない。
- ②不用意に、メールの添付ファイルを開かない。
- ③不用意に、メール本文中のURLをクリックしない。
- ④身元のはっきりしないファイルは、ダウンロードしない。

- ウィルス・詐欺対策（インターネット）
- ①不用意にWebサイトにアクセスしない。
- ②アクセス先が、信頼できるサイトかを常に注意する。

◎セキュリティ情報サイト

https://www.ipa.go.jp/security/measures/index.html	独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/kokokara/	独立行政法人情報処理推進機構
https://jvn.jp/	脆弱性対策情報ポータルサイト

以上