Internet 講座

2021 年 6 月 15 日
パソコンを使いこなす会

【第 6 回分科会のテーマ：－スパム広告・詐欺メッセージ－】

今回は、パソコンやスマホを操作しているとき現れる偽警告・詐欺警告について勉強します。

これらの警告はメールを介してもたらされる事が多いですが、意図せずにインストールしてしまった悪質なアプリがパソコンやスマホで暴れまわることもあります。

また、偽のサイトに誘導して個人情報を入力させて取り込み金銭的な損害を与える詐欺行為に至るものもあります。

これらのスパム広告・詐欺メッセージへの対処方法を勉強して、万一被害にあった場合に公的機関等への相談の仕方を理解しましょう。皆さんの周りにこのような経験をした方がいたら、今回の学習会の内容を教えてあげて下さい。

【最初に Edge を開いてください】

1. 広告宣伝メール
2. 詐欺警告、偽装サイト
3. 架空請求メール
4. フィッシング詐欺
5. ワンクリック詐欺
6. なりすましメール
7. ウイルスメール
8. 偽警告サイト
9. ランサムウェア（Ransomware）
10. マルウェア
11. お金儲けのメール

【具体的内容：－スパム広告・詐欺メッセージ－】

1. 広告宣伝メール

出会い系・アダルト系サイト、サービスや商品販売などに関するものです。中には友達をよそおって返信させようとしたり、サイトへアクセスさせようとするものもあります。不審なメールや身に覚えのない内容、知らないアドレスからのメールは気をつけましょう。

多くの出会い系・アダルト系サイトのメールには、URL やリンクが記載されています。その URL へアクセスしてしまうと、後日、大量の迷惑メールが届いたり、身に覚えのない料金を請求されたりするなどのトラブルがよくあります。

サイトの管理者はあらかじめ、メール本文にあなたのアドレスなどを識別する情報を含む URL を記載していて、この URL がクリックされるとクリックしたユーザのアドレスが特定されて、あなたがサイトを閲覧したことが分かるようになっています。こうして、サイトの閲覧料や利用料などと称して不当な料金を請求されることにつながるわけです。

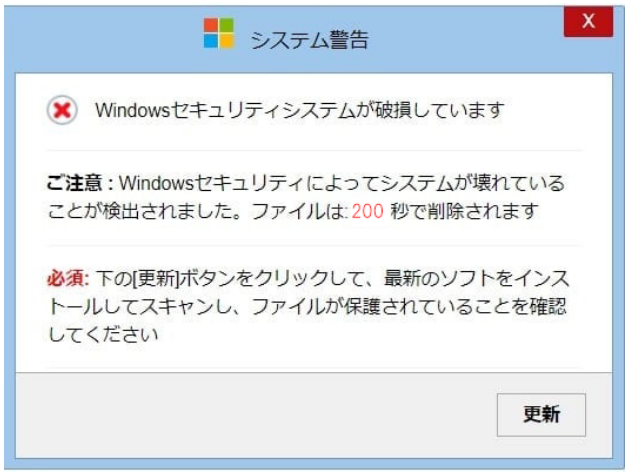
≪迷惑メール相談センター ≫＜＝＝いろんな迷惑メールの例示があります。
https://www.dekyo.or.jp/soudan/contents/news/news.html

≪ネットトラブル 動画 福島県警≫＜＝＝ネットトラブル 動画の例示があります。
https://www.police.pref.fukushima.jp/onegai/jyouhou/hightech2/net-trouble/movie/

◎≪その警告メッセージ、信じて大丈夫？ ブラウザの“偽警告”にご用心！≫11 分
https://www.youtube.com/watch?v=sm1UMc97zRc

2. 詐欺警告、偽装サイト

詐欺警告とは Yahoo などを閲覧している時や動画を視聴している時に画面に突然出てくる警告画面になります。



詐欺警告の指示に従って操作を進めるとパソコンに迷惑ソフトがダウンロードされてしまい嘘の通知を促してきます。

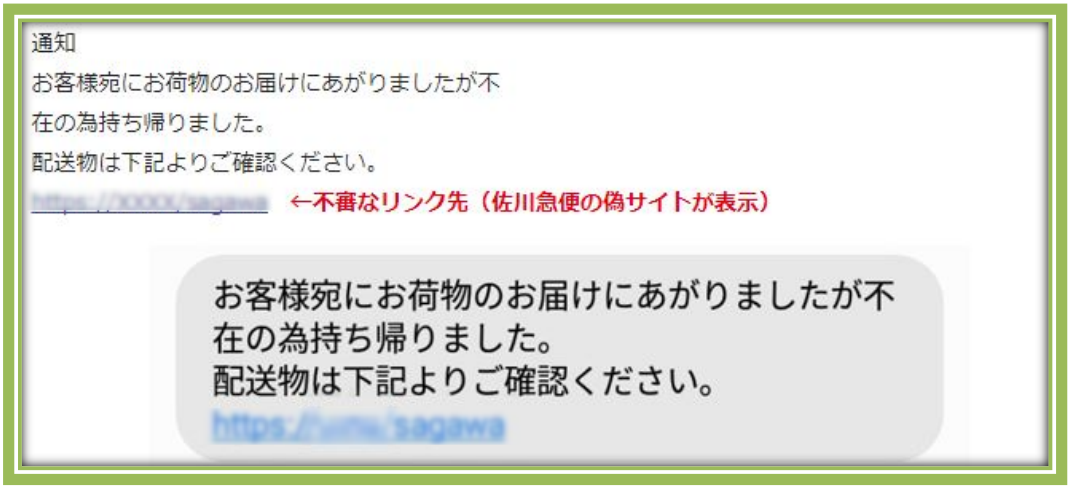
A）【代表的な迷惑ソフト】<==クリックするとテキストが開きます

B）詐欺警告が出やすいサイト

動画サイト、通販サイト、ブログ関連で詐欺広告は出現しやすいですが、最近では佐川、ヤマト、ゆうパック、Apple といった大手のサイトをそっくりに装った偽サイトにも詐欺警告が出現することがあります。

更に精巧に仕組まれているメールにも細心の注意を払う必要があります。某キャリアに勤めている従業員でも騙されてしまう程、そっくりに通知されます。

下記に表示されている画像は実際に佐川急便を名乗った偽サイトからスマホに SMS で届いた詐欺のメッセージです。



C）スマホに表示された偽詐欺警告

iPhone に表示された偽警告画面

　iPhone の場合はネットを使用していると最中に出てくるので無視しましょう。

D）Android に表示された偽警告画面

　Android スマホにも詐欺警告は出てきます。文章もデタラメな詐欺警告なので無視を。

E）PC、スマホに詐欺警告が出た時の消し方

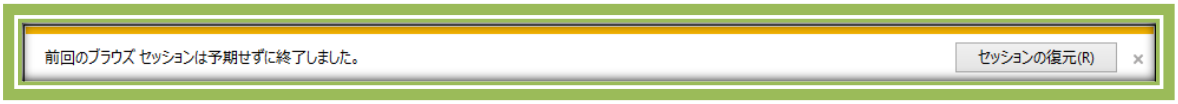
スマホ(iPhone)で詐欺警告を閉じる方法

① 右下に出ている四角が2つ重なっているマークをタッチします。
② 左上の×マーク押します。
③ 検索画面になれば完了

PC で詐欺警告を閉じる方法

① 「Windows」キーと「X」キーを押す。
② 現れたメニューでタスクマネージャー(K)をクリック。
③ タスクマネージャーの中に”Internet Explorer”または”Microsoft Edge”が表示されていれば、どちらかをクリック。
④ 左クリックした後に右下にある”タスク終了”を左クリック。
⑤ 起動している Google Chrome、Internet Explorer、Microsoft Edge 等全ブラウザのタスクの終了をかけます。
⑥ 警告画面が消えたことを確認したら再度、ネットを立ち上げる。
⑦ ネット起動時にいつものホームページ(Yahoo や Google 等)になっていれば終了。

【開いていた Edge をこの手順で閉じてください】



※再度、ネットを開くと下に黄色い吹き出しが出ますが、×(バツ)マークを押して閉じます。セッションの復元を押してしまうと詐欺広告がまた出てきてしまいます。

※タスクマネージャーを使用して詐欺警告を消すこともできず、シャットダウンすることもできない場合は PC の電源を強制的に切る処置になります。

F）迷惑メールがくるきっかけ

それでは、そもそもどうして迷惑メールを受け取ることになったのでしょうか。初めて迷惑メールを受け取ったときに、どうして自分のアドレスがわかったのだろうと、気味が悪くなったり、不思議に思ったりしたことはありませんでしたか。実は、あなたのしている行動が、思いがけない迷惑メールを受け取るきっかけを作っていたのかもしれません。思い当たることがないか以下を参考にしてみてください。

- 予測されやすいメールアドレスを使っている
- 迷惑メールに書かれていた返信先アドレスに配信停止メールを送った
- 迷惑メールに書かれている URL にアクセスした
- 出会い系サイトやネットの掲示板にアドレスの登録や書き込みをした
- 自分のブログや SNS にアドレスを掲載した
- あやしいネットショッピングサイトで買い物をした
- セール情報などのメルマガに登録した
- 懸賞やモニター、無料ダウンロードサイトに応募や登録をした

G）迷惑メールは無視が基本

気をつけていても、わたしたちの暮らしの中で、メールをやりとりするため友達にアドレスを伝えたり、サイトへメールアドレスを登録するなどの「迷惑メールが届くかもしれないきっかけ」を作ってしまうのは避けられません。そこで、迷惑メールを受け取ってしまった時は被害を最小限にとどめ、そこから発展するトラブルにあわないために、迷惑メールは開かないようにしましょう。また、問い合わせや返信などは厳禁です。

H）サイトの安全性評価

メール本文に記載されたアドレスをコピーして、下のトレンドマイクロのサイトの検索バーに貼り付けて「今すぐ確認」をクリックすると判定してくれる。

≪トレンドマイクロによる Web サイトの安全性の評価≫
https://global.sitesafety.trendmicro.com/result.php

【偽装サイトメール例】<==クリックするとテキストが開きます
≪詐欺警告、偽装サイトの見破り方と対策方法≫

https://www.nojima.co.jp/support/koneta/26914/
≪【公式】インターネットの利用中に怪しい広告が表示されたときは？≫3 分
https://www.youtube.com/watch?v=GGn0B-BJkFU

≪ネット詐欺の手口・対処法 7 選【セキュリティソフトで防げない】≫20 分
https://www.youtube.com/watch?v=xQaG1 zIcs4

3．架空請求メール

知らないサイトから突然「情報料の請求」や「自宅まで回収しに行く」といった内容のメールが送られてくるケースが増えています。このようなメールを「架空請求メール」と呼び、お金をだましとろうとするメールを利用した詐欺の手口の一つです。

A）まずはあわてず、落ち着いて

もちろん利用していない料金を支払う必要はありません。悪質な業者は、携帯の製造番号を記載し、個人を特定しているかのように高圧的なメールを送り、受信者を不安な気持ちにさせて、連絡してくるのを待っています。あわてて返信や連絡をしてしまえば相手の思うつぼ。

B）相手はあなたを知りません

業者は適当なメールアドレスにランダムに送っているだけなので、必ずしもあなたの名前や住所が知られているわけではありません。払わなければ「自宅を調べて取り立てに行く」と書かれているものもありますが、たいていの場合、電話などで連絡をしない限り、住所を知っていることはありません。ご利用のプロバイダ名、IP アドレス、携帯の固体識別番号などの情報を表示しているものもありますが、これらの情報から住所を調べることはできませんので安心してください。携帯会社やご利用のプロバイダも、お客様の個人情報を厳重に管理しているので、第三者に住所を知らせることはありません。

C）もしもトラブルにまきこまれたら

連絡をしてしまい、メールや電話で何度も督促を受けたり、料金を払ってしまうなどの被害にあったときは、すぐに最寄りの消費生活センターや警察署にご相談ください。

◎≪【アニメ】架空請求にご注意！≫4 分
https://www.youtube.com/watch?v=0JZpHz_CYO0

●参考サイト
≪全国の消費生活センター（国民生活センター）≫
http://www.kokusen.go.jp/map/
≪都道府県警察本部のサイバー犯罪相談窓口等一覧（警察庁）≫
https://www.npa.go.jp/cyber/soudan.htm
●消費者ホットライン
電話：「188（嫌や！）」

4．フィッシング詐欺

フィッシング詐欺とは、ネットバンキングやクレジットカード会社、有名企業になりすまして個人情報をだましとる詐欺の手口です。

手法としては、企業からのお知らせメールを装い、本物そっくりに偽装したホームページへ誘導し、ログイン ID、パスワード、クレジットカード番号などの個人情報を入力させます。情報をだましとられた会員はいつものサイトにログインしたつもりで、後日オンラインバンクの預金残高がなくなっていたり、ログインパスワードが勝手に変更されるなどの状況に、はじめて被害に気づく人が多いといわれています。

そもそも、企業がメールで ID やパスワードなどの個人情報を求めることは通常ありません。もし、そのようなメールを受け取った場合は、まず、その企業のホームページで問い合わせ先を確認し、窓口に直接確認するなどの慎重な対応が必要です。

最近では、ネットオークションやオンラインゲームの ID・パスワードも狙われ、盗んだ ID・パスワードを使ったアカウントの不正利用などのサイバー犯罪が問題となっています。ID・パスワードの管理には十分注意し、不審なメールを受け取った際は、メール本文の URL ではなく、必

ずその企業の問い合わせ窓口を調べて直接確認するよう心がけましょう。もし、被害にあってしまった時は、すぐに最寄りの警察署へ相談してください。

フィッシング詐欺メールのブロック

普段使っているメールアドレスにフィッシング詐欺メールが来るときには契約しているプロバイダのフィッシング詐欺メールのブロックサービスを利用しましょう。

ブラウザで「フィッシング詐欺メール ブロック（プロバイダ名）」で検索すればサービスサイトが見つかります。月額 300 円～500 円程度の有料サービスもあります。

【Edge を開いて「フィッシング詐欺メール ブロック（プロバイダ名）」で検索してください】

◎≪【アニメ】フィッシング詐欺にご注意！≫3 分
https://www.youtube.com/watch?v=k83Sp9vqZZE

≪フィッシング対策協議会（一般社団法人 JPCERT コーディネーションセンター）≫

https://www.antiphishing.jp/

≪スマホ利用における脅威疑似体験サイト｜トレンドマイクロ≫スマホ用
https://go.trendmicro.com/jp/forHome/solution/mobilesecurity/tmvr/phishing/howto.html

5. ワンクリック詐欺

大半の広告宣伝メールには URL が記載されていますが、興味本位で URL をクリックしてしまうと、料金請求などのトラブルにあうことがあります。これはクリック詐欺と呼ばれる手法で、迷惑メールの URL をクリックしただけでいきなり「会員登録が完了しました」「入会金〇〇円です」などと記載された画面が表示され、驚いた閲覧者から金銭を振込ませ、だまし取るというものです。

最近はより手口が巧妙になり、1 度のクリックではなく 4 回程クリックさせページを変えていく中に、こっそり規約へのリンクを表示させて、規約に料金が発生することはきちんと書いてあったと一方的に主張するようなものもあります。

サイトを利用する際は、あらかじめ利用規約をしっかり探し、「有料なのか、無料なのか」「あやしい表示がないか」を確認しておきましょう。

◎≪【アニメ】ワンクリック詐欺にご注意！≫3 分
https://www.youtube.com/watch?v=dMyHAh2-suo

≪アクセスしただけで登録されてしまうサイトに注意（神奈川県警察）≫
https://www.police.pref.kanagawa.jp/mes/mesd7015.htm

◎≪ワンクリック詐欺 体験コンテンツ ｜NTT コミュニケーションズ 個人のお客さま≫3 分
https://www.ntt.com/personal/services/option/security/norton_column/isw_oneclick/etc/sgwall_mv_v2_All.mp4

6. なりすましメール

パソコンメールは、メールソフトで送信者アドレスを自由に設定できるので、知り合いや有名企業などを装った「なりすましメール」が可能です。そのため、送信者アドレスが、自分のアドレスになっている迷惑メールがあり、受け取った人は驚いてメールを確認してしまったということがよくあります。

これは迷惑メールを送信する際に、送信者アドレス（From アドレス）が宛先アドレス（To ア

ドレス）と同一となるソフトを使用して送られたもので、受け取った人の気を引いてメールを確認させるためや送信者の身元をわかりづらくしてアドレスによるフィルタリングを回避するためと思われます。しかし、携帯に届くなりすましメールを防止するフィルターを利用することで、このようなメールを防ぐことができます。

A）詐欺・なりすまし防止機能の導入

携帯会社では、パソコンから携帯のアドレスになりすまして送信されたメールを受信しないようにするための「なりすましメール拒否」サービスを提供しています。また、携帯会社によっては携帯のアドレスだけではなく、「送信ドメイン認証技術」を利用して他のドメインになりすましたメールを拒否する方法もありますので、このようなメールが届かないよう、あらかじめ設定しておくとよいでしょう。

ブラウザで「なりすましメール ブロック（プロバイダ名）」で検索すればサービスサイトが見つかります。月額 300 円～500 円程度の有料サービスもあります。

B）携帯会社のなりすましメール対策

●参考サイト

◎≪身に覚えのない自分からのメールにご注意ください！Docomo≫
https://www.nttdocomo.co.jp/info/spam_mail/column/20161220/index.html

≪携帯電話・PHS アドレスを装ったなりすましメール防止機能設定のお願い au≫
http://www.au.kddi.com/wau/notice/meiwaku/oshirase/narisumashi.html
≪ケータイトラブル：なりすましメールにだまされていませんか SoftBank≫
https://www.softbank.jp/mobile/support/accident/#tabitem_2

【なりすましメールの例】<==クリックするとテキストが開きます

7．ウイルスメール

迷惑メールには悪質なコンピュータウイルスが含まれているケースが多くなっています。ウイルスメールの中には、利用者がメールを開いたり、ネットでサイトを閲覧したときにパソコンに気づかれないよう侵入し、乗っ取ってしまうものがあります。これを「ボットウイルス」と呼んでいます。

乗っ取られてしまったパソコンは、ボットウイルスに感染した他のパソコンと共にボットネット（パソコン群）の一部となり、外部の司令塔から遠隔操作を受けて大量の迷惑メールを世界中に送信するようになります。ボットウイルスは、パソコンの所有者に気づかれないように活動するため、感染してもすぐには分かりません。感染したパソコンの所有者は、被害者であると同時に、自分が知らないうちに迷惑行為を行う加害者となってしまうのです。迷惑メール送信者にパソコンを悪用されないためには、Windows Update を必ず実施して OS の状態を最新に保ち、あわせてセキュリティソフトの利用をおすすめします。

A）ウイルスに感染すると

- メールを送るたびに相手にウイルスまで送ってしまい、気づかないうちにウイルスをばらまく犯人になってしまう
- パソコンが外部から遠隔操作されて迷惑メールを大量に送信してしまう
- パソコンが動作の途中で止まってしまう
- パソコン内に保存している情報が盗まれる
- 保存していたデータが破壊される、または削除される
- パソコンやソフトウェアが正常に動かない（ブラウザが立ち上がらない等）

B）ウイルスに感染しないためには

① パソコンの OS やソフトウェアを最新の状態に更新する

Windows 等の OS やソフトウェアには「セキュリティーホール（ぜい弱性）」と呼ばれる欠陥や問題点が発見されることがあります。セキュリティーホールをそのままにして利用していると、ウイルス感染や不正操作などの被害にあう恐れがあり、とても危険です。

セキュリティーホールが見つかると、修正プログラムが随時公開されますので、ウイルスに感染しないためにも、定期的にプログラムの更新をしておきましょう。

② ウイルス対策ソフトを利用する

インターネット上のサービスの利用や USB メモリなどの外部記憶媒体を通じてコンピュータウイルスに感染する危険性があります。ウイルス感染の危険性を軽減するために、ウイルス対策ソフトを利用しましょう。

なお、ウイルス対策ソフトを利用していてもパターンファイルと呼ばれるウイルス定義ファイルの更新を行っていないと新種ウイルスに対応することができません。常にパターンファイルを最新の状態に保ち、定期的にコンピュータをスキャンすることが必要です。

③ HTML メールは使わないようにする

HTML メールは、自由に文字の色や大きさを変更したり、イラストや写真で装飾できるなど便利なメール形式です。しかし、この機能を悪用したウイルスもあり、HTML メールを開く、またはプレビュー画面を表示しただけでウイルス感染してしまう場合があります。HTML メールは通常見ない・使わないように設定し、必要な場合のみ利用するようにしましょう。

④ 不審なメールの添付ファイルは開かない

ウイルスは、メールの添付ファイルに仕掛けられている場合も多いため、見知らぬメールの添付ファイルは、安易に開いてはいけません。

最近では、差出人を詐称したウイルスメールが多く見受けられます。知人からのメールだったとしても不審な点がある場合は、その知人に確認するなど十分注意してください。このようなウイルスメールからパソコンを守るためにも、添付ファイルを開く場合でもウイルス検査を行ってから開くようにしましょう。

C）ウイルスに感染したときは

もし、最近パソコンの挙動がおかしいと感じたときは、すぐにウイルス対策ソフトやセキュリティサイトでのオンラインスキャンで検査してください。ウイルス対策ソフト等でコンピュータウイルスが検知されれば、削除や駆除などが自動で行われます。まれにソフトが起動しなかったり、操作方法がわからないときは、IPA 情報セキュリティ安心相談窓口へご相談ください。

主な迷惑メール・ウイルス対策ソフト

- ウイルスバスター（トレンドマイクロ株式会社）
- カスペルスキー（株式会社カスペルスキー）
- ノートン（株式会社シマンテック）
- マカフィー（マカフィー株式会社）

D）メールだけじゃない。ホームページから感染するウイルスには要注意！

Windows をはじめとする各種 OS やソフトウェアには「セキュリティーホール（ぜい弱性）」と呼ばれるシステム上の欠陥や仕様上の問題点が発見されることがあり、セキュリティーホールを利用して、ホームページを閲覧しただけで感染させる Web 感染型ウイルスが多くなっています。

ACTIVE（Advanced Cyber Threats response InitiatiVE）では、ボットウイルスへの感染防止のための知識や駆除対策手順が紹介しています。また、感染していないかの確認、駆除ツール実施手順も説明していますので、パソコンの挙動がおかしいと思ったときはすぐに

対策してください。
●参考サイト
マルウェアに感染しないために（ACTIVE）
パソコンユーザのためのウイルス対策 7 箇条（独立行政法人情報処理推進機構セキュリティセンター）

8. 偽警告サイト
≪パソコン操作中に、突然警告音が鳴りすぐに電話するように表示された≫
http://www.kokusen.go.jp/t_box/data/t_box-faq_qa2016_39.html
≪インターネット使用中に大音量で警告音が鳴り、警告メッセージが出ました。≫
https://www.nojima.co.jp/support/faq/33847/
もしパソコンでインターネット利用中に突然大音量で警告音（エラー音）が鳴り響き、ウイルスに感染しています、システムが損傷していますなどの警告メッセージと今すぐ電話やインストールするように表示された場合、まず電話もアプリのダウンロードもお待ちください！
これは数年前から猛威を振るっている偽警告サイトの可能性があり、国民生活センターや神奈川県警などから注意勧告されています。
偽の警告で不安をあおり、架空のセキュリティ契約を結ばせる巧妙な手口で実際に被害が発生しています。これからお伝えする確認すべきことに当てはまりませんか？

A）確認すべきこと
- マイクロソフトやアップルからの警告のように表示がされているが、URL に microsoft・apple がともに入っていない
- 「次のウイルスに感染しています。3 つのウイルス。セキュリティチェックでは～」と表示されている
- システムの損傷度を 66.7%や 28.1%など具体的な数字で提示してくる
- 大きなエラー音が絶えず流れている
- 有料アプリの登録画面を紹介される（クリックする場所まで教えてくれるなど、異様なほど親切な登録サイト）
- サポートセンターの電話番号へ連絡するよう誘導される（連絡すると片言の日本語を話すスタッフがでる）

この中から一つでも当てはまる状況があると詐欺の可能性があります。
上記に当てはまっている場合、詐欺サイトの可能性が高いです。

B）被害にあわないようにするには
- 今すぐにスキャンをクリックしない
- 絶対に個人情報を入力しない
- 絶対に電話をかけない
- カード番号などの情報を伝えない
- すぐにブラウザを終了し Cookie の消去とウイルススキャンをする
- 万一契約してしまった場合はすぐに消費生活センターや警察へ相談する

エラー音や損傷率で不安をあおり、公式サイトに見せかけて信用させ、クレジットカードで支払をさせる巧妙な手口です。今すぐにスキャンを絶対にクリックせず、×でブラウザを終了してください。
クリックしなければ契約したことにはなりません。×で閉じられない場合も落ち着いて以下の対策を参照ください。

C）【ブラウザを終了できない場合】＜＝＝クリックするとテキストが開きます

D）契約をしてしまったとおもったら
　クレジットカードの番号を入力してしまったり、電話で教えてしまったといった場合は契約してしまっている可能性があります。
　この契約の恐ろしいところは
- 継続して請求が発生する（サブスクリプション契約）可能性がある
- 契約相手が海外におり日本の法律だけでは簡単に解除ができない可能性がある

ですが、万が一契約をしてしまった場合もあきらめないでください！
　まずは消費生活センターへ至急相談しましょう。また警察へ被害届を提出することで 2 次 3 次の請求を止めることができる可能性があります。
E）手続きについては各クレジット会社盗難窓口などへご相談ください。

【大手クレジット会社の盗難・紛失相談窓口】＜==クリックするとテキストが開きます

○≪【アニメ】サポート詐欺にご注意！≫3 分
https://www.youtube.com/watch?v=W42VT8FgDfw

◎≪新表示マイクロソフトセキュリウイルスサポート詐欺に注意≫6 分
https://www.youtube.com/watch?v=moQvwXzEdaA

9．ランサムウェア（Ransomware）
https://www.npa.go.jp/cyber/ransom/main1.html
　ランサムウェア（Ransomware）とは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせて作られた名称であり、コンピュータウィルスの一種です。
　このウィルスに感染するとパソコン内に保存しているデータを勝手に暗号化されて使えない状態になったり、スマートフォンが操作不能になったりしてしまいます。また、感染した端末の中のファイルが暗号化されるのみではなく、その端末と接続された別のストレージも暗号化される場合もあります。
　そして、その制限を解除するための身代金を要求する画面を表示させるというウイルスです。
　ランサムウェアの感染経路としては、主に犯罪者が送付したメールの添付ファイルを開いたり、本文中に記載されたリンク先をクリックしたりすることが考えられますが、第三者のウェブサイトを改ざんして、ウェブサイトにアクセスしただけでウイルスに感染するという仕組みを構築し、多くの人にランサムウェアを感染させようとする例も確認されていますので注意しましょう！

≪あなたのファイルを Panda ウイルスにより暗号化しました。≫
http://www.ne.senshu-u.ac.jp/~proj28-19/tasa/ransomware2/example_pop.html

ランサムウェアの感染経路（広告型）
　広告型ランサムウェアは、Windows にのみ感染する、とても気づくことが困難で非常に危険なもので、次の条件にはまり、ネットサーフィンをしているだけで侵入を許してしまうものです。
- Adobe Flash Player を更新せず旧バージョンのまま放置すること
- 毎月実施される Windows Update が行われてない
- Java を更新せず旧バージョンのまま放置している
- Adobe Reader を更新せず旧バージョンのまま放置している

　対策としては、以上の項目に当てはまらないことはもちろんの事、サイトを見ているだけでも脆弱性を悪用されてランサムウェアに感染するということがあるので、OS などを常に最新の状態にアップデートすることなどが重要です。また、重要なデータなどは普段からバックアップを取っておくことも必要です。

ちなみに別にいかがわしいサイトを見ていたから感染するというわけでもないのです。広告型ランサムウェアに感染している人がいたら、温かい目で見守り助けてあげましょう。

ただし、ワンクリック詐欺に感染した人はほぼアダルトサイトなので、多少冷ややかな目で見ても良いのかもしれません。

10. マルウェア

マルウェア(Malware)とは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称です。

マルウェアには次のようなものがあります。

① ウイルス
他のプログラムに寄生して、そのプログラムの動作を妨げたり、ユーザの意図に反する、有害な作用を及ぼすためのプログラムで、感染機能や自己拡散機能を持つ

② ワーム
独立のファイルで、他のプログラムの動作を妨げたり、ユーザの意図に反する、有害な作用を及ぼすためのプログラムで、感染機能や自己拡散機能を持つ

③ トロイの木馬
ユーザの意図に反し、攻撃者の意図する動作を侵入先のコンピュータで秘密裏に行うプログラム

④ スパイウェア
感染したパソコンの内部情報を外部に勝手に送信する

⑤ キーロガー
ユーザのキーボード操作をそのまま外部に送信する。スパイウェアの一種

⑥ バックドア
攻撃者が侵入するためのネットワーク上の裏口を開ける

⑦ ボット
攻撃者からの指令により、他のコンピュータやネットワークへの攻撃や、サーバからのファイルの盗み出しなど有害な動作を行うプログラム

≪8-1 マルウェアとは≫
https://www.jnsa.org/ikusei/03/08-01.html

マルウェアへの感染の兆候

次のような場合は、マルウェア感染を疑ってください。

- パソコンの起動に時間がかかるようになった、または、起動できなくなった
- システムの動作速度が遅くなった、または、途中で動かなくなった
- 画面上に、奇妙なメッセージが表示された、または、音楽が流れた
- 突然データが消えた
- 身に覚えのないメールを送信している
- ネットワークトラフィックが、異常に高くなっている

11. お金儲けのメール

あやしい副業をもちかける勧誘メールには要注意

「短時間で高収入！」「簡単に儲かる！」「月収○○万円」などというメールを受信したことはありませんか？

最近、こんな手軽なサイドビジネスや副業を勧誘するメールが増えていますので注意が必要です。やってみようかなと思って申し込みをすると、「仕事の紹介をするには、紹介料が必要です」「これから紹介する仕事をするには、その前に簡単な試験を受ける必要があります」「試験のための研修がありますから、教材の購入が必要です」など、次々と最初の説明にはなかったことを言い出されたりします。結局、仕事の紹介は受けられずに高額な費用を取られたり、高い教材を買わされたりして、お金だけだまし取られることになりかねません。簡単にお金儲けができるなどという話はないのです。決して信じてはいけません。

高齢者や女性に多い？悩みの相談で高額謝礼にだまされた

悩みを聞いてくれた人に「お金をあげたい」などといったメールから有料の出会い系サイトなどに誘導され、高額な利用料を支払ってしまった高齢者や女性の被害が急増しています。

相手の巧妙な言葉を信じて、謝礼目当てに有料メールを何度もやり取りさせて、サイトの利用料として高額な料金が発生していたという手口です。中には、悩み相談の相手を放っておけずにメールのやりとりを続けていたという被害者もいるため、だまされていることになかなか気づけない場合もあります。悩みを聞いてくれた人に「お金をあげたい」などといったメールから有料の出会い系サイトなどに誘導され、相手の巧妙な言葉を信じて有料メールを何度もやり取りするうちに高額な利用料を支払ってしまった高齢者や女性の被害が急増しています。

有名人になりすますサクラがほとんど

悩み相談の人物として多いのは、「高額財産のあるお年寄り」「アイドル」「有名企業の社長」「医者」などを自称するサクラです。話を長引かせるためのウソは実に巧妙で、「あなたがいないと寂しい」「若い人の生活の援助をしたい」などと架空の話に引き込んで有料メールを続けさせます。女性の場合は、「某男性アイドルグループの○○です。悩みがあるけど立場上誰にも言えないから聞いてほしい」などといった言葉にだまされて被害にあう傾向があります。サクラを見抜くのはむずかしいため、気づいたときには料金を払ってしまった後だったという場合もありますが、お金を支払った証拠が残っていれば取り返せる可能性もありますので、すぐに消費生活センターへ相談してください。

12. チェーンメール

チェーンメールは、この手紙を回さないと不幸になるといった「不幸の手紙」のメール版で、受け取った人に誰かに転送させることを目的とした迷惑メールです。

転送されることが目的なので受け取った人に対して、「誰かに送らなければ不幸になる」「危害を加える」など脅かす内容が多く、主に小中学生などの子どもの間でやり取りされています。これは、大人ならすぐに誰でも嘘だと分かる内容でも、「殺しにいく」「呪われる」などの脅迫的な言葉に怖くなり不安になって、どうしても無視できない子どもが友人たちに送ってしまうからです。

なお、チェーンメールは迷惑メールであると説明しましたが、一般的な迷惑メールとの違いはなんでしょうか。それは「送信者が必ず知り合いである」という点です。一般的な迷惑メールなら、携帯会社が提供する迷惑メールフィルターが利用できますが、チェーンメールは別です。普段やりとりする友人のアドレスを受信拒否するわけにはいきませんし、内容がさまざまにあるチェーンメールをカテゴリ別のフィルターですべてブロックすることもできません。チェーンメールを止めるには、送ってきた友人たちに直接止めるよう伝えるか、無視するしかありません。中に

は同じ内容のチェーンメールを複数の友人から何通も送られてくる場合もあり、迷惑メールを受け取るストレス以上のわずらわしさを感じることは明らかです。
　そこで、チェーンメール転送防止の始めはまず、送られてきた自分が止めることです。

撃退！チェーンメール
　チェーンメールについて、さまざまな内容や転送してはいけない理由をわかりやすく紹介。不安な時の転送先アドレスはパソコン・携帯用あわせて 20 個用意しています。
撃退！チェーンメール　データ公開
　当センターへ寄せられたチェーンメールの転送数や内容などを紹介
迷惑メール相談センター　モバイルサイト

http://www.dekyo.or.jp/soudan/m/
●パンフレット

◎≪チェーンメール対策 BOOK「撃退！チェーンメール＆メッセージ」≫
https://www.dekyo.or.jp/soudan/data/chain/chainbook.pdf

以上