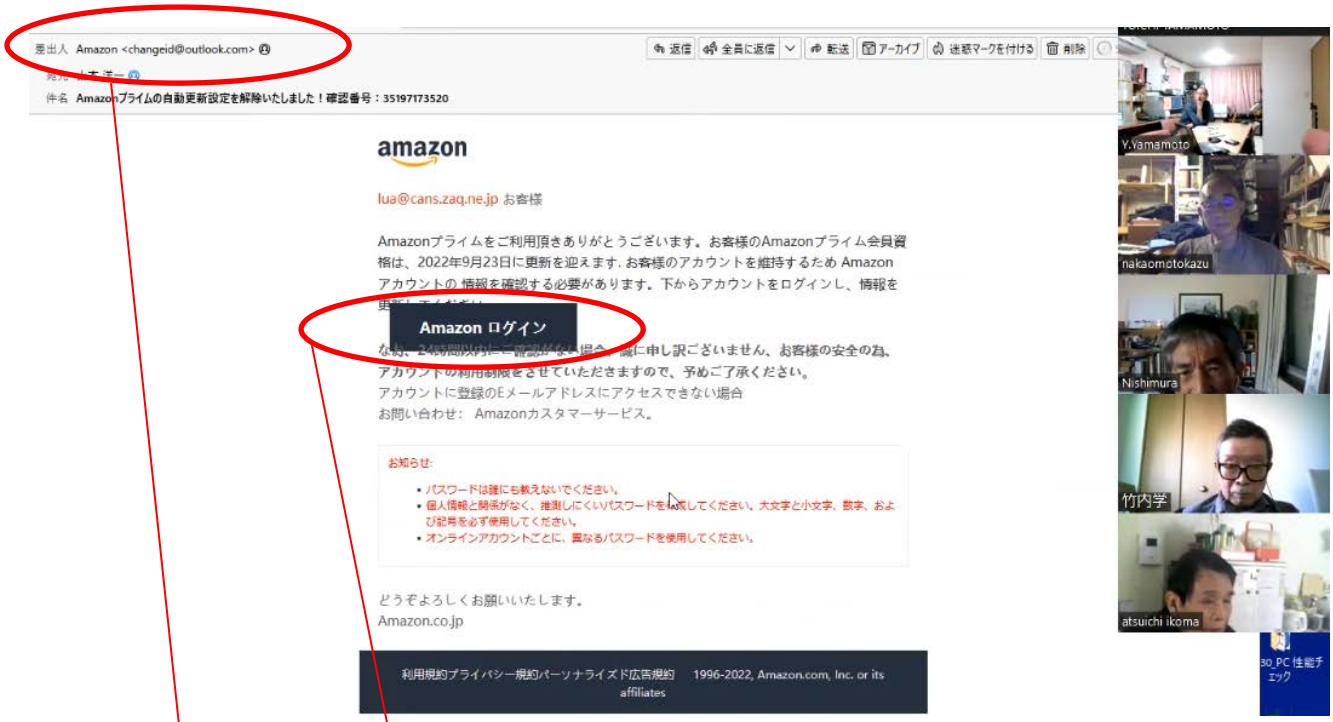
第 125 回 CIS パートナー会議事録（一般様用）

開催日時　2022 年 9 月 25 日（日）　13 時～15 時
講　師　　山本　洋一
テーマ　　詐欺メールの例と処理について

会議風景

1）詐欺メールの例　　t=02:08:00

今朝送られてきた AMAZON を名乗るフィッシングメールの画面



＊疑わしい差出人のメールアドレス　••••　ドメイン名が　outlook はあり得ない。

ハイパーリンクされている URL を調べる

＊　 

この部分を右クリックし URL をコピーして

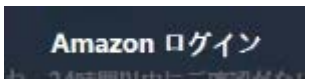
メモ帳にペーストすると

URL:　https://www.byglmgirhg.com/jp

実際に誘導されるハイパーリンク先が読み取れた。

きわめて疑わしい URL であることが分かる。

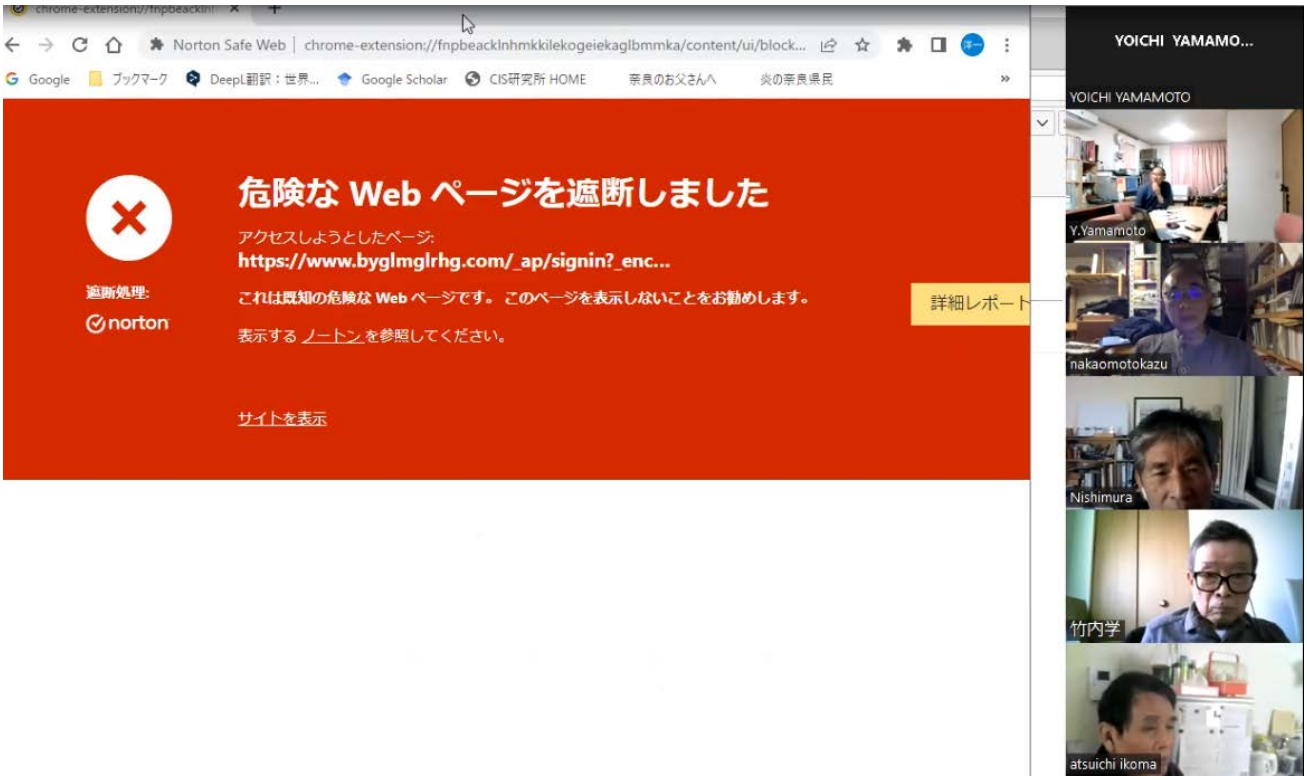
以上より、このメールは、AMAZON を騙るフィッシングメールと断定できる。

注意:　 

を「左クリックしないように」

間違って、押してしまった場合、セキュリティー対応ソフトが PC を守ってくれる。
下の例では、Norton の場合の「危険な Web ページを遮断」した場合の画面である。

セキュリティーソフト　Norton　がブロックした例



Norton の例

2） 経済産業省のアナウンス

CIS

＜＜参考＞＞
1990年4月10日に通商産業省が制定した「コンピュータウイルス対策基準」では、コンピュータウイルスを次のように定義しています。

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

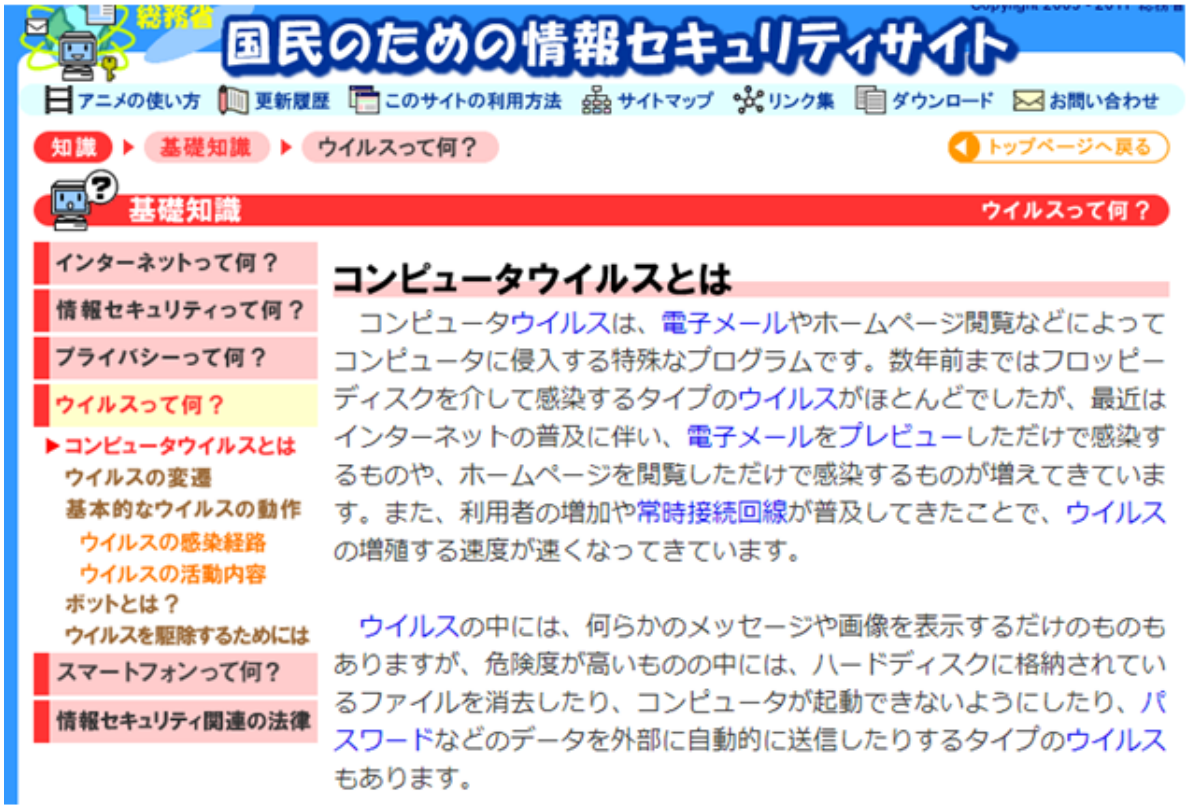
(1)自己伝染機能
自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

(2)潜伏機能
発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、条件が満たされるまで症状を出さない機能

(3)発病機能
プログラムやデータ等のファイルの破壊を行ったり、コンピュータに異常な動作をさせる等の機能

※2001年1月6日より通商産業省は経済産業省に移行しました。

https://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/kiso/k04_virus.htm 4



https://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/kiso/k04_virus.htm 3

3）ウイルス感染経路

CIS

ウイルス感染経路

特徴:
多くのコンピュータウイルスは増殖するための仕組みを持っている。

例:
コンピュータ内のファイルに自動的に感染したり、ネットワークに接続している他のコンピュータのファイルに自動的に感染したりするなどの方法で自己増殖する。
コンピュータに登録されている電子メールのアドレス帳や過去の電子メールの送受信の履歴を利用して、自動的にウイルス付きの電子メールを送信するものも多く、世界中にウイルスが蔓延する大きな原因。

対策:
ウイルスに感染しないようにするためには、ウイルス対策ソフトが必要。 また、常に最新のウイルスに対応できるように、インターネットなどでウイルス検知用データを更新する。

https://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/kiso/k04_virus.htm

＊セキュリティーソフトの例

非表示ボタン		×	×	×	×
ソフト名 クリックでレビューページへ		ESET	ノートン セキュリティ	カスペルスキー 2019	ウイルスバスター クラウド
パッケージ					
特徴		動作軽い	バランス型	セキュリティ重視	初心者向け
動作の軽さ	軽さ総合評価	8点	8点	7点	6点
	PC起動時間	+6.0%	+2.6%	+1.9%	+17.8%
	WEBサイト表示	+6.9%	+6.9%	+15.2%	+37.6%
基本機能	ウイルス検出	99.46%	99.90%	99.90%	100%
	ファイアウォール	✓	✓	✓	
	脆弱性対策				
安全強化	危険サイト検知				
	ネット銀行保護	✓		✓	✓
	PC盗難対策	✓			
	パスワード管理	上位版のみ	✓		オプション
	保護者機能				
サポート		電話：毎日 9 - 17時	電話：平日 10 - 19時	電話：毎日 9:30 - 18時	電話：毎日 9:30-17:30
一言評価		動作が軽い 低価格	動作軽く 防御性能も高い	全方向の 防御性能が 一番高い	初心者向き

4） コンピューターウイルスの種類

NET の脅威を防ぐための準備はいかにすべきか。 先ずは、ウイルスとはどのようなものがあるのかを調べておく。コンピューターウイルスは多種多様、代表的な「ワーム」・「トロイの木馬」等について調べてみる。

4-1） ワーム

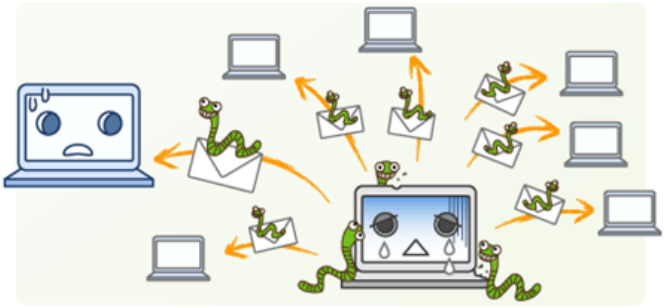
CIS

ワーム

ワームとは、インターネットやUSBメモリーなどを通じてコンピューターに感染し、さまざまな被害をもたらすウイルスです。

インターネットの中を虫のように這い回って、別のパソコンに感染していくことから、ワームという名前がつけられたと言われています。

ワームは、その強力な感染力により被害を拡大していきます。ウイルス付きのメールを知らないうちに大量に送ってしまうという手法が典型的です。
パソコンからパソコンへと感染していくため、感染スピードが速いことが特徴です。



https://www.sony.jp/support/vaio/beginner/school/security/03.html

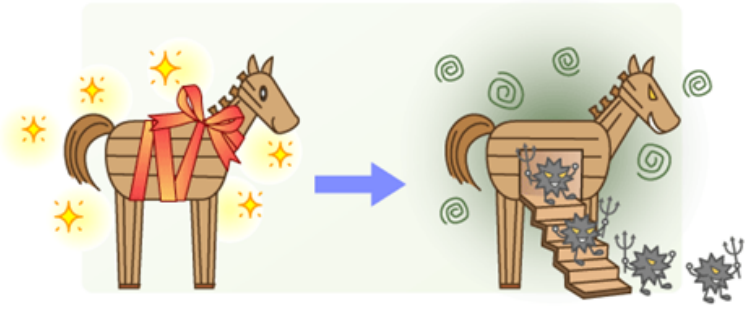
4-2） トロイの木馬

CIS

トロイの木馬

トロイの木馬は、ギリシア神話に登場するトロイの木馬になぞらえて名前がつけられたウイルスで、**ユーザーにとって便利なソフトや楽しそうなゲームのように見せかけて**、それを実行するように仕向けます。これにひっかかって**実行をしてしまうと、トロイの木馬に感染**してしまいます。

トロイの木馬に感染すると、**個人情報を盗まれてしまったり、コンピューターの設定を勝手に変えられてしまう**などの症状があらわれます。



木でできており、中に人が隠れることができるようになっていた。転じて、内通者や巧妙に相手を陥れる罠を指して「トロイの木馬」と呼ぶことがある。 wiki

https://www.sony.jp/support/vaio/beginner/school/security/03.html

4-3) スパイウェア

スパイウェアとはコンピュータ ウイルスのように、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せたりするものを指す。

潜入経路は？

多くはユーザーが気づかずに自分でインストールしていたと思われます。たとえば、無償の音楽再生プログラムやフリーソフトウェア/シェアウェアをダウンロードした時、メインの機能とは別にユーザに関するデータを収集し配信する機能も含まれていることを気がつかなかった可能性がある。

どのような症状が起きるか？

- ユーザーの個人情報を収集　パスワードやクレジットカード番号など
- 強制的に特定の Web サイトへ誘導　特定のサイトに誘導されてしまう
- 不要なポップアップによる操作性の低下　ポップアップを消すと、新しいポップアップ広告を表示
- ブラウザ セキュリティ設定の変更　どんなプログラムも警告なしでインストールさせられてしまう
- システムが不安定になる　バックグラウンドでスパイウェアが動くことでパソコンの動作が極端に遅くなったり、システムが不安定になる

https://prius.hitachi.co.jp/support/beginner/faq/700043/700043.html

4-4) スケアウェア

スケアウェアとは、「ウイルスに感染しています」という嘘のメッセージを画面上に表示し、金銭や個人情報を盗み取る偽セキュリティソフトのことを主に指します。

この手口は新しいものではありませんが、最近また被害が増えてきています。

ウイルス対策ソフトを導入していなかったり、不審なメールを開いてしまうことで、気づかないうちにスケアウェアを自分のパソコンにダウンロードしてしまうことが多いです。

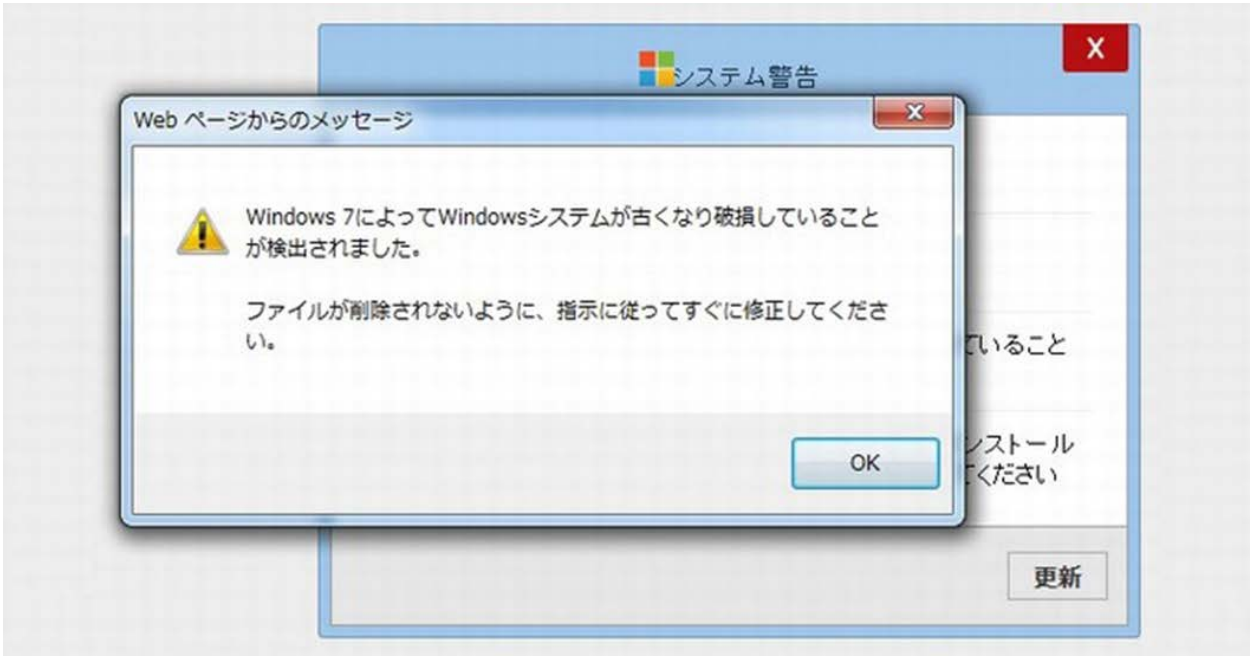
ウイルス対策ソフトは必ず導入しましょう。

T=02:43:52

5)　ウイルス発見例とその対策

　ホームページを閲覧していたら、突然「Windows 7 によって Windows システムが古くなり破損していることが検出されました。 ファイルが削除されないように、指示に従ってすぐに修正してください。」 というようなメッセージが表示されたら注意しましょう！このメッセージは Windows の正式なメッセージではなく、偽物です。

　このメッセージの「Windows 7 によって」の部分は、Windows 10 を使っていれば「Windows 10 によって」に代わります。 そして、このメッセージの後、「システム警告！」というウィンドウとともに「Windows セキュリティシステムが破損しています」と表示されて、ソフトの更新を促されます。



これは偽物ですので、絶対にクリックしないようにしましょう。

重要:

ブラウザを閉じてしまえば大丈夫

上の状況では、まだウイルス感染していません。

この段階では、特にウィルスが入ってしまっているようなことはありませんので、このメッセージさえ閉じてしまえば大丈夫です。お使いのブラウザ（インターネットを閲覧する為のソフト）の右上に表示されている

「×」ボタン（ウィンドウを閉じるボタン）をクリックして、ブラウザを閉じてしまいましょう。

「×」ボタンをクリックしても、ウィンドウが閉じられないような場合には、**キーボードの「Ctrl」＋「Alt」＋「Del」キーを同時に押します。**すると、項目が表示されますので「タスクマネージャー」をクリックします。

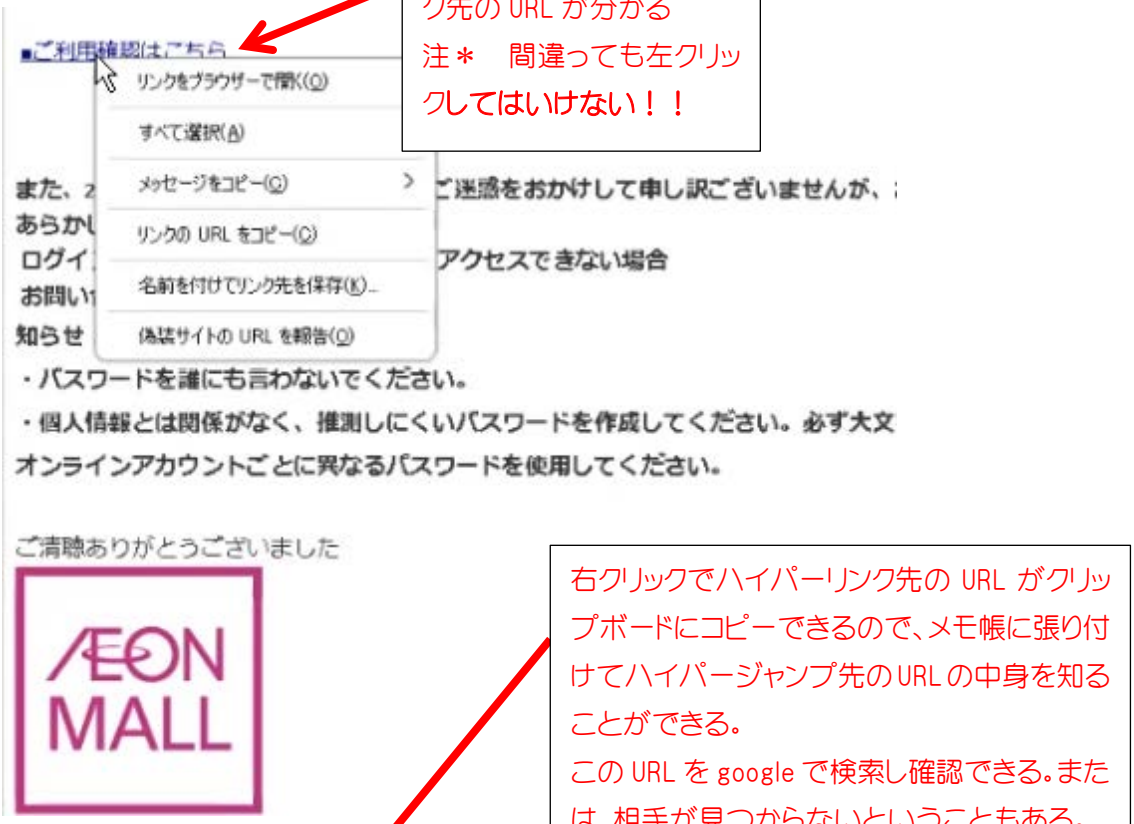
　其れもできないとき（緊急事態発生）電源ボタン長押しで強制終了する。

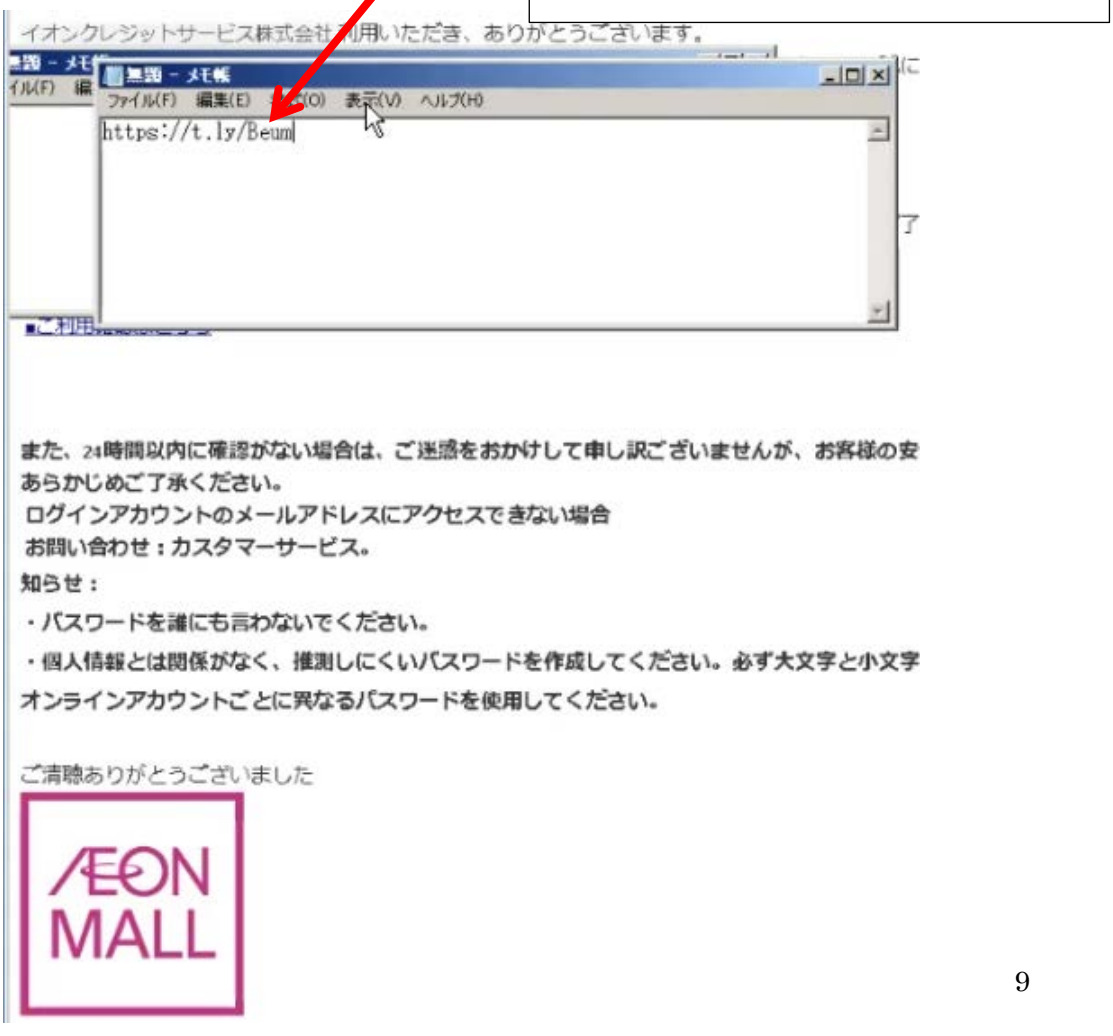
CPU が動作をとめてしまうので、データーの改ざんや消去などすべての動作を停止できる。

「Windows セキュリティシステムが破損しています」、というような詐欺メッセージは、他にも似たようなものが沢山あります。 もしも、そのようなメッセージが表示された場合には、メッセージ中のボタンは絶対にクリックしないようにして、**まずはウィンドウを閉じてしまいましょう。**

6) 詐欺メールの例と処理について

偽の URL を見る実験:





将来の話題になりそうな討議が有った。 BS プレミアム 「ヒューマニエンス」等…

会議終了時、NHK-BS の話題で「笑わない数学」が面白い・・・・数学の難問を大真面目に解説。

8) 今後の日程

第 126 回 10 月 30 日 (日)13 時 ～ 久米 健次 様
第 127 回 11 月 27 日 (日)13 時 ～ 寺川 雅嗣 様
第 128 回 12 月 18 日 (日)13 時 ～ 神田 忠起 様

HP http://www.cis-laboratories.co.jp/index.html
以上

2022-9-26 文責 山本洋一