新入社員等研修向け
情報セキュリティクイズ

一般社団法人　JPCERTコーディネーションセンター

情報セキュリティクイズについて

- 情報セキュリティクイズは、業務でPCを使用する場合、覚えておくと参考になるようなTipsをクイズ形式で紹介します。

クイズに登場するキャラクターは「セキュリイヌ」といいます。
サーバ管理から PC のメンテナンスまで幅広くこなすシステム管理担当者で、トラブルに動じないまったりした性格。趣味はコネクタ集め。

特技:
◎コンピュータウイルスの気配を察知できるらしい（鼻で？）
◎Tシャツ一枚で長時間サーバルームにこもれる（コールドアイルはむしろ快適空間）。犬なので。

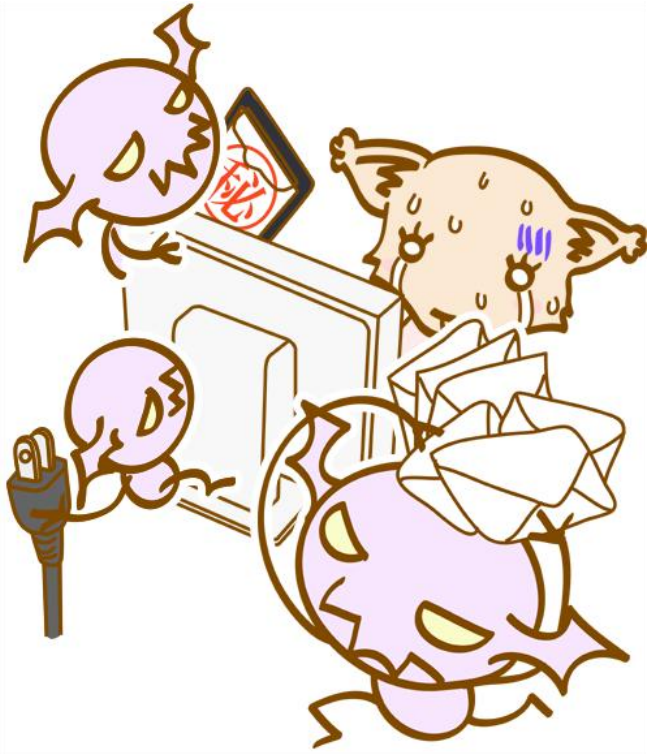
セキュリイヌ

1. 電子メールに関するクイズ

JPCERT CC®

- 差出人が詐称されたメールを見分けるため、チェックしたほうがよいものは次のうちどれでしょうか？

A) ヘッダの詳細情報
B) メール本文の署名欄
C) 送信者のアドレス
D) 電子署名の有無



正解：すべてチェックすべき情報

**電子メールは、本文やヘッダ情報を含めて詐称や偽装が簡単にできてしまいます。
したがって、ある特定の情報だけでは「なりすましメール」なのかどうかの判定はできません。技術的なメールのフォーマット情報に頼るのではなく、本文の書かれ方、内容や前後のシチュエーションに不自然な点はないか、など総合的な判断が重要です。**

A)について
通常表示されないヘッダ情報には、送信者に関する情報が含まれています。ヘッダ情報も不審なメールをチェックする方法のひとつですが、これも偽装することが可能なので確実な方法ではありません。

B)について
本文の署名欄も簡単に偽装できる部分です。また、最近では携帯電話のメールやWebメールのアカウントなどを業務に使う人もいますので、同一人物でも同じ署名を使うとは限りません。あくまでチェックポイントのひとつです。

C)について
送信者のメールアドレスもヘッダ情報の一部なので、A)と同様に判断材料にはなりますが、確実な判定ができるとは限りません。

D)について
電子署名は、メールの作成者や改ざんの有無を確認するために有効なツールですが、電子署名を付すための鍵データや証明書が本人以外に利用されてしまうと意味をなさなくなってしまいます。理屈は印鑑と同じで、印鑑が押されていても本人が押したとは限らないということです。このような場合、法的な効果については議論の余地があるにしても電子署名も、判断材料の“ひとつ”としてとらえるべきものです。

2. 電子メールの添付ファイルに関するクイズ

JPCERT CC®

- 電子メールに添付されるファイルに関し、拡張子が次のように付されていた場合、最も注意すべきものは次のうちどれでしょうか？

A) .exe（実行可能ファイル）
B) .doc または.docx（Microsoft Word）
C) .pdf（PDFファイル）
D) .jpg（JPEG画像）

正解：A） .exe（実行可能ファイル）

メールに添付された実行可能ファイルは、実際にどのようなプログラムが実行されるかわからないものがあるので注意してください。
特に、マルウエアが自己解凍ファイルとして送られる場合などは、「自己解凍ファイルだから、ファイルをフォルダに展開するだけだ」と思ってファイルをクリックしてしまうと、知らないうちにマルウエアが実行されてしまい、思わぬ結果を招きます。
実行可能ファイルがより危険なのは、使っているPCに脆弱性などの弱点がなくても、権限あるユーザの指示（クリック）によりプログラムが実行されてしまうからです。

B）について
ワープロソフトや表計算ソフトに組み込まれているマクロ機能を利用したマルウエアも存在するので、Word、Excelファイルなども注意すべきファイルですが、アプリケーションの脆弱性が放置されていなければ、容易にはマルウエアに感染することはありませんので、アプリケーションのセキュリティアップデートを正しく適用する、添付ファイルの自動ウイルスチェックを有効にしておく、などの対策によってインシデントのリスクをかなり下げることができます。

C）について
PDFファイルを表示するアプリケーションの脆弱性を狙ったマルウエアも増加しているので、アプリケーションのセキュリティアップデートを放置しておくと、PDFファイルも危険な場合があります。

D）について
JPEG画像ファイルも、C）のPDFファイルと同様な危険性があります。対策も同様に、ウイルスチェックやセキュリティアップデートの実施が基本となります。

3. USBメモリの取り扱いに関するクイズ

JPCERT CC®

- 会社のWindows PCでUSBメモリを使う場合、有効なマルウエア感染予防対策は次のうちどれでしょうか？

A) 外付けドライブ（HDD、CD-ROM、USBメモリ等）のオートラン機能を有効にする。
B) 本体ソケットではなくUSBハブを利用して接続する。
C) SHIFTキーを押しながらUSBメモリを挿入する。
D) データを保存する前に必ずフォーマット（初期化）しておく。

正解：C） SHIFTキーを押しながら挿入

USBメモリなどの自動実行機能（オートラン機能）を利用して、不正なプログラムを実行するマルウェアも存在しますので、PC本体で、USBメモリの自動実行機能を停止しておくか、Windows PCではSHIFTキーを押しながらUSBメモリを挿入するなどの対策が考えられます。Windows PCでは、SHIFTキーを押しながらUSBメモリを挿入することにより、自動実行機能を停止させることができます。覚えておきましょう。

ただし、USBの自動実行機能を停止するだけで対策は十分ではありません。日ごろの機器の管理やデバイス挿入時のウイルスチェックなどが重要であることはいうまでもありません。

A）について
上記のとおり、オートラン機能は感染しているマルウエアを起動させてしまう可能性があるので、業務用PCなどは機能を無効にしておくことが望ましいといえます。

B）について
USBメモリを接続する場合、PC本体にあるソケットを利用するか、拡張した外付けハブを利用するかの違いは、マルウエア感染に影響を与えるものではありません。

D）について
データを保存する前にフォーマット（初期化）しても、そのあとのコピー操作でマルウエアに感染する可能性があります。これも、感染予防になる対策とはいえません。

暗号化機能つきUSBメモリ

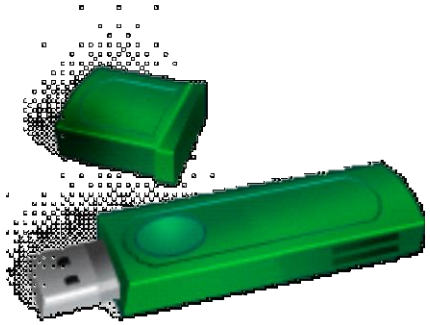
JPCERT CC®

USBメモリなど取り外し可能な記憶デバイスについては、紛失・盗難のリスクがつきものです。紛失・盗難時のデータ漏洩のリスクを低減させるため、保存する電子データを暗号化しておくことをお勧めします。
復号用のパスフレーズには、英数字、大文字小文字、記号を含めた強固なものを使用してください。

強固なパスフレーズの作り方については、以下の資料等を参考にしてください。

■新入社員等研修向け情報セキュリティマニュアル
https://www.jpcert.or.jp/magazine/security/newcomer.html

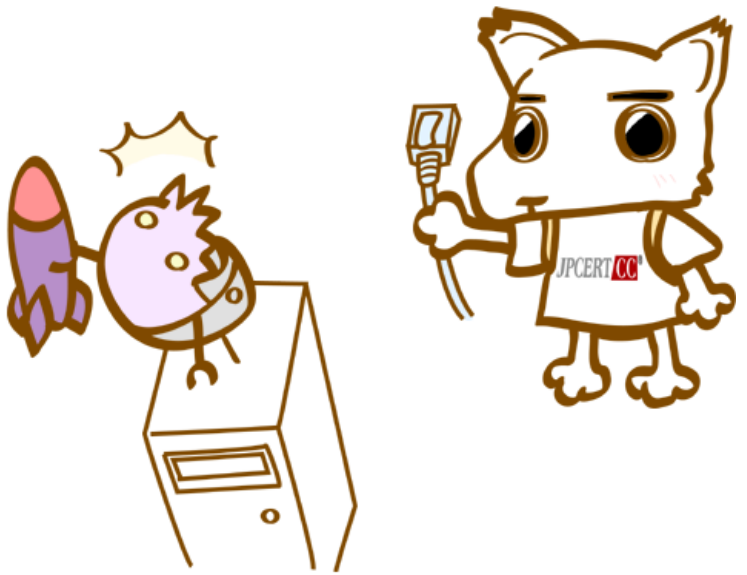
■Microsoft – 強力なパスワード：その作り方と使い方 –
http://www.microsoft.com/japan/protect/yourself/password/create.mspx



4. Windows利用テクニックに関するクイズ

- Windows PC の画面をパスワードロックするためのショートカットキーの操作は次のうちどれでしょうか？

A） Alt ＋ Tab
B） CTRL ＋ V
C） Windows ロゴキー ＋ L
D） F2



正解：C） Windowsロゴキー ＋ L

Windows PCのキーボードの左側最下列にWindowsの窓のマークが刻印されたキーがあります。このキーとアルファベットのLキーを同時に押すと、簡単に画面にパスワードロックをかけることができます。PCの画面をロックしないまま席を離れると、自分が知らないうちに勝手にPCを操作されてしまう危険があり、データへのアクセス制御等の社内ルールが意味をなさなくなってしまう可能性がありますので、席を離れる際にはPCの画面をロックする習慣を身につけるようにしてください。

A）について
ALTキーとTabキーを同時に押す操作は、Windowsの作業ウィンドウを切り替えるショートカットキーです。

B）について
CTRLキーとVキーを同時に押す操作は、クリップボードなどからのデータを貼り付ける（ペースト）ためのショートカットキーです。

D）について
F2キーは、選択したフォルダやファイルの名称を変更するショートカットキーです。

5. HTMLメールに関するクイズ

- HTMLメールは、画像やフォントなど多彩な表現が可能になりますが、セキュリティの観点からは好ましくないと評されています。その理由となるHTMLメールのリスクを最も適切に言い表しているものは次のうちどれでしょうか？

A) メールソフトのバージョンによって、画面が乱れたり、送信者の意図どおりに表示されないことがあるから。
B) HTMLメールは転送中にエラーになる確率が高いから。
C) メールサイズが大きくなり、ネットワークに負荷がかかるから。
D) テキストメールよりも不正なプログラムなどを埋め込みやすいから。

正解：D） 不正なプログラムを埋め込みやすい

JPCERT CC®

HTMLメールは、画像や文字フォントなど多彩な表現が可能になりますが、HTMLのソースコード内には、それらの表現に必要なタグ、およびスクリプトなど画面表示には現れない要素が多数含まれています。そのため、HTMLメールに不正なスクリプトを埋め込むことにより、閲覧者のPCに本人の意図しない動作を行わせる攻撃に悪用されることがあります。
HTMLメールは、本文中に、関連URLへのリンクタグなども含めることができますが、リンク先として表示されるサイト名やURLとは異なる、全く別のサイトを実際のジャンプ先に指定することができるため、閲覧者の意に反して、マルウェアの配布サイト等に誘導することができてしまいます。
このように、HTMLメールは、テキストメールよりウイルスなどのマルウェアを隠ぺいしやすい特徴があり、セキュリティ上好ましくないといわれています。

A)について
テキストメールと比した場合のHTMLメールの特徴としては間違っていませんが、対応するHTMLのバージョンの違いや、タグの解釈の違いによる表示の乱れは、ブラウザにも共通する問題です。このような理由でHTMLメールを嫌う人も存在しますが、表示の乱れが直接セキュリティに及ぼす影響は低いと判断できます。

B）について
テキストメールに比してHTMLメールがエラーを起こしやすいという事実はありません。

C)について
HTMLメールは、画像やバナーなどのグラフィックデータなどとともに送信され、通常のテキストメールよりサイズが大きくなる傾向はありますが、WordファイルやPDFファイルを添付して送信するほうが、ファイルのサイズは大きくなる場合が多いといえます。