ＰＣクラブ１２月度会合

2019. 12. 21

テーマ：情報セキュリティの常識

今月度は、クイズ形式で「情報セキュリティ」について議論したいと思います！！

1. マルウエアの侵入経路は様々考えられるが、次の行為のうち、侵入につながる可能性があるものはどれか？

（1）Webブラウザーで企業のWebサイトを閲覧する

（2）見知らぬドメインからのメールをメールソフトで開く

（3）ネット上で見つけた無料セキュリティソフトをインストールする

（4）他人から渡されたUSBメモリーをPCに挿す

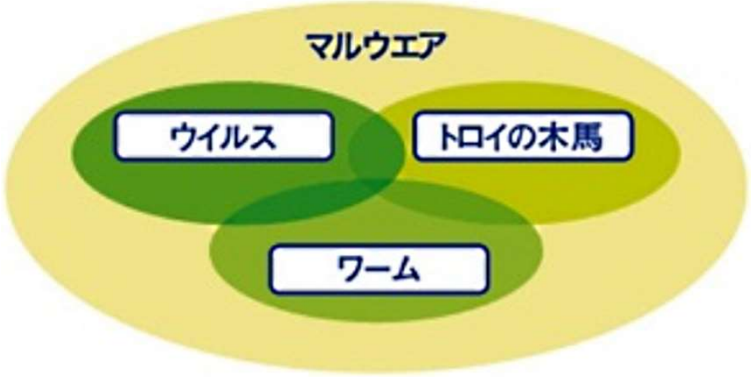
A1：これら4種類の行為は、いずれも可能性有り

（1）Webサイトが改竄され、悪意あるプログラムが埋め込まれていれば、Webブラウザーでこのwebサイトを閲覧するだけで感染する可能性有り

（2）メールソフトにセキュリティ上の不具合があれば、当該悪意あるメールを開いただけで侵入の可能性有り

（3）「無料セキュリティソフト」などとうたって悪意あるプログラムを配布される可能性がある。ダウンロード時には、配布元が信頼できるかを確認する！！

（4）ネットに接続していないPCでも、マルウエア感染の危険は有る。手軽にデータ交換などに使用するUSBメモリーは有力な候補、要注意！！



	ウイルス	ワーム	トロイの木馬
存在形態	別のプログラムに寄生	単独のプログラム	単独のプログラム
感染機能	あり（寄生）	あり（増殖）	なし

2. 迷惑メールは何故増える？

次のうち、迷惑メールの増加につながる可能性のある行為は？

（1）迷惑メール中に書かれていたリンクをクリックしてWebサイトにアクセスした
（2）迷惑メール中に書かれていた「配信停止希望の場合の連絡先」に連絡し、停止を申し入れた
（3）迷惑メールを開かず削除した
（4）HTML形式の迷惑メールを開いた

3. 2020年1月14日にWindows 7のサポートが終了するが、使い続けるのが問題とされる理由は？

（1）Windows 7向けセキュリティソフトが使えなくなるため
（2）Windows 7にセキュリティ上の欠陥が見つかっても、修正プログラムが提供されなくなる（即ちサポート終了）
（3）Windows 7搭載PCが新規に購入できなくなるため
（4）Windows 7関連のセキュリティ情報が、マイクロソフトのWebサイトで読めなくなるため

A2：（1），（2），（4）

・迷惑メール中のリンクには、様々な細工が施されている可能性がある。URLの末尾に特定の文字列を付与するなどして、メールアドレスの特定する。
・HTMLメールの場合は、本文中に埋め込まれた画像がネットから読み出されるように細工されているので、同じことが起る。即ち、迷惑HTMLは開くだけでメールアドレス等が知られてしまう！！
・配信停止連絡も避けるのが無難（信頼出来るサイトは別だが）

※迷惑メールは、開かずに削除するのが一番！！

A3：（2）

マイクロソフトは、2020年1月14日にWindows 7のサポートを終了、サポート終了後はセキュリティ更新プログラム（パッチ）や有償サポートサービスを提供しないとしている。
このためサポート終了後もWindows 7を使い続ければ、新たに見つかった脆弱性を突く攻撃の被害に遭う可能性が高る！！

4. Microsoft Updateで更新できないのは？

Microsoft Updateは、PCの機能を更新するための機能。これを実行することで、セキュリティ上の不具合を解消するプログラムなどを適用できる。Microsoft Updateで更新できないソフトは？

（1）Microsoft Edge／Internet Explorer
（2）.NET Framework（MSのアプリケーション開発・実行環境）
（3）Java
（4）Word

5. 不適切なパスワードの管理方法は？

（1）複雑で堅牢性が高いパスワードを1つ作り、どのサイトでもそれを利用する
（2）パスワード管理ソフトを使う
（3）手帳などに記録し、鍵付きの引き出しに入れておく
（4）サイトごとに異なるパスワードを利用する

A4：（3）

勿論、マイクロソフトのプロダクツのみが更新の対象

A5：（1）

いくら堅牢なパスワードであっても、使い回すとリスト型攻撃（どこかのサイトで漏洩したパスワードのリストを使って、ログインできるかどうかをいろいろなサイトで試す攻撃）被害に遭う危険がある。

※私の経験
yahoo Mail を通じパスワードを破られた！！
リスト型攻撃はなかったが、パスワードを知ったことにより「他の個人情報をも知った」との脅迫があった。
それは不可能なこと故、無視してyahoo Mail のパスワード変更のみで対処！！

6. ランサムウエアの攻撃手法は？

ランサムとは「身代金」を意味する。ユーザーにとって重要なデータと引き替えに、身代金を支払えと要求される。

（1）SNSなどを通じて個人情報を収集する
（2）企業システムに侵入し、機密情報を盗み出す
（3）個人のPC内に侵入し、データを暗号化・使用不能にする
（4）ネットの闇取引によって、企業の顧客データを入手する

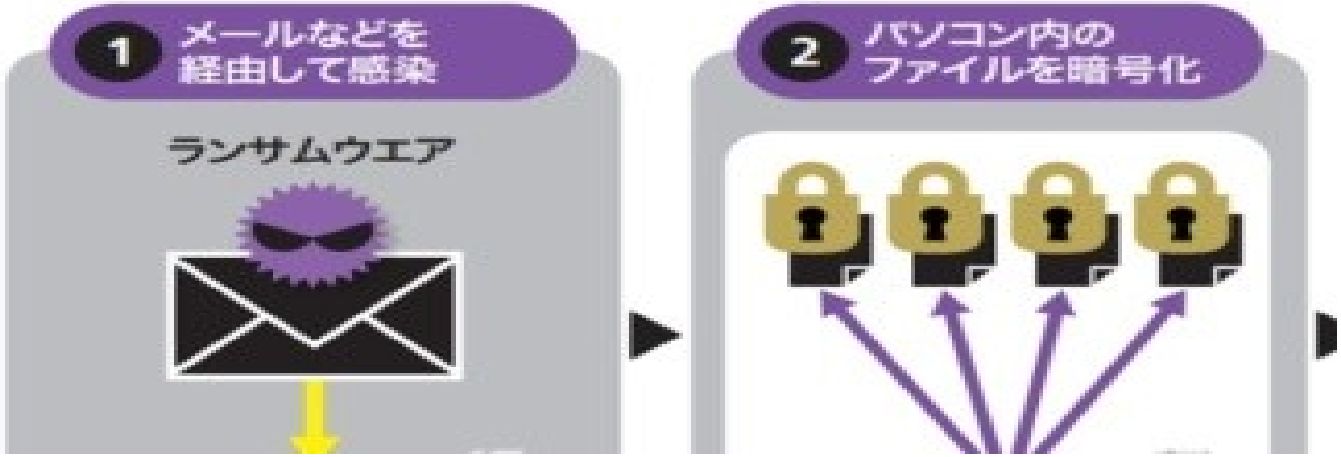
7. 標的型攻撃メールを見抜くポイントは？

標的型攻撃メールを見分けるポイントとして適切なものは？

（1）実績のない相手からのメールは注意する
（2）標的型攻撃メールには必ず添付ファイルが付いている。故に、添付ファイルの有無を確認する
（3）標的にされるのは企業なので、個人メールアドレスはそれほど気にしなくてもよい
（4）メールの本文中にリンクが含まれている場合、URLの冒頭が「https://」になっていれば問題ない

A6：（3）

・個人のPC内に侵入し、データを暗号化・使用不能にする！！
元に戻したければ金銭を支払うよう求めるマルウエアである。
ランサムウエアは、メールの添付ファイルなどとして送られ、PCの脆弱性を突いて侵入します。修正プログラムの適用など基本的なセキュリティ対策が必須



A7：全て適切ではない

標的型攻撃とは、特定の企業・組織を狙ってマルウエアを添付したメールや詐欺サイトへの誘導URLを含むメールを送信する手口！！
個人メールアドレスの場合は、基本的に「迷惑メール」に対する注意点と同様に考える。

8. スマートフォンは危ない？

スマートフォンのセキュリティについて述べた次の説明のうち、最も適切なのはどれ？

(1)PCと同じく、スマホでもアプリの更新プログラム適用によってセキュリティを高められる
(2)スマホでは、メールの添付ファイルによるマルウエア感染の心配はない
(3)「Google Play」のような正規アプリストアでの配布アプリなら問題ないが、それ以外の手段で配布されているアプリには危険なものがある
(4)iOS搭載のスマホやタブレットは、セキュリティ上の危険はない

A8：（1）

・スマホにも、マルウエア感染などセキュリティ上のリスクがある
・「Google Play」のように審査制度を設けている正規のアプリストアにも、マルウエアが紛れ込んでいる危険性がある。
・Andoroidに比べれば少ないものの、iPhoneやiPadでもマルウエア感染のリスクはゼロではない
※また、偽メールによる被害に遭う可能性は、PCと同じようにある

9. 役所の文書から情報漏洩、原因は？

昨年、中央省庁や地方自治体の文書から、個人情報など非公表情報が漏洩してしまう事故が相次いだ！！特に、財務省が公開した森友学園との交渉記録の件で有名に！！この事故の原因は？

（1）誤って、非公開箇所を削除する前のデータを公開してしまった
（2）Excelファイルで、重要データが別タブに残っていた
（3）PDFファイルで当該箇所を墨塗りにしていたが、黒塗りの方法が不十分だった
（4）Word文書から消したはずのデータが、変更履歴に残っていた

A9：（3）

事故を公表した省庁や自治体は、情報が漏洩したPDFファイルの具体的な作成方法を明らかにしていないが、ある程度推測可能！！

定番のPDF編集ソフト「Adobe Acrobat Pro DC」なら、ハイライト機能を使ったか、図形を使って消したと考えられる。いずれも文書の表面を黒く塗って隠しただけで、簡単なパソコンの操作で読み取ることができる。

※最新の話題として、「桜を見る会」の参加者名簿問題があった。
紙情報はシュレッダーにかけられ廃棄、電子情報は消去との答弁であった！！
しかし、電子情報の復元は可能

1）情報は共有されており、どこかにある時点までは絶対に残っていたはず
2）ファイル消去だけでは物理的には消えていない。
3）ディスクシュレッダー等の消去ソフトを使っていても、再現は不可能ではない！！

10. 東京オリンピック・パラリンピックで使われる生体認証技術とは？

（1）顔認証
（2）指紋認証
（3）静脈認証
（4）虹彩認証

A10:（1）

2020年「東京五輪・パラリンピック」における大会関係者の入場管理にNECの顔認証システムが採用される。選手やスタッフ、ボランティアなど約30万人が対象で、不正な入場を防ぐ。大会関係者の入場管理に顔認証システムが活用されるのは、五輪・パラリンピック大会で初めてとのこと
採用されたのは、NECの顔認証エンジン「NeoFace」を活用した入場管理システム。ICチップ入りIDカードと事前に撮影・登録した大会関係者の顔画像を紐づけたうえで、入場ゲートに設置した顔認証装置で本人を認証をする仕組み

※入出国管理も顔認証に！！