クイズで学ぶ
情報セキュリティ

NPO新潟情報セキュリティ協会
落合 博幸

問題1

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

出典：JPCERT/CC 「新入社員等研修向け情報セキュリティクイズ」

すべて！

問題1　解説

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

問題2

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（MicrosoftWord）
C) .pdf（PDFファイル）
D) .jpg（JPEG画像）

出典：JPCERT/CC 「新入社員等研修向け情報セキュリティクイズ」

A

問題2　解説

　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。

問題3

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。

出典：JPCERT/CC 「新入社員等研修向け情報セキュリティクイズ」

C

問題３　解説

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。

問題4

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

出典：JPCERT/CC 「新入社員等研修向け情報セキュリティクイズ」

C

問題4　解説

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。

問題5

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。

出典：JPCERT/CC 「新入社員等研修向け情報セキュリティクイズ」

D

問題５　解説

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。

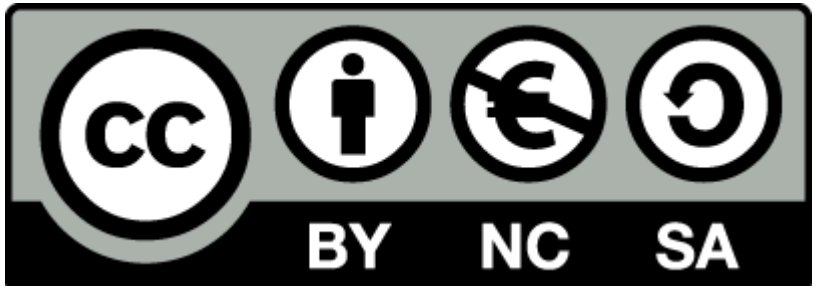
A)について
テキストメールと比した場合のHTMLメールの特徴としては間違っていませんが、対応するHTMLのバージョンの違いや、タグの解釈の違いによる表示の乱れは、ブラウザにも共通する問題です。このような理由でHTMLメールを嫌う人も存在しますが、表示の乱れが直接セキュリティに及ぼす影響は低いと判断できます。

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。

問題6

作品にこのマークが表示されているとき、行ってはいけない行為はどれでしょう？



ア　作品を複製して再配布すること
イ　作品を営利目的で利用すること
ウ　作品を改変して利用すること

オリジナル問題

イ

問題6　解説

このマークは「クリエイティブ・コモンズ・ライセンス」と呼ばれるマークで、著作権者が指定した条件（以下のようなマークにより表現）を守る限り、使用したり再配布したりすることができることを表わしています。

「表示」（Attribution, BY）
作品を複製、頒布、展示、実演を行うにあたり、著作権者の表示を要求する

「非営利」（Noncommercial, NC）
作品を複製、頒布、展示、実演を行うにあたり、非営利目的での利用に限定する

「改変禁止」（No Derivative Works, ND）
作品を複製、頒布、展示、実演を行うにあたり、いかなる改変も禁止する

「継承」（Share Alike, SA）
クリエイティブ・コモンズのライセンスが付与された作品を改変・変形・加工してできた作品についても、元になった作品のライセンスを継承させた上で頒布を認める

したがって、問題のマークの組み合わせは「著作権者のクレジット（氏名、作品タイトルなど）を表示し、かつ非営利目的に限り、また改変を行った際には元の作品と同じ組み合わせのライセンスで公開することを主な条件に、改変したり再配布したりすることができる」という意味になります。

問題7

持っていても児童ポルノ禁止法に触れる可能性のないものはどれでしょう？

ア　宮沢りえ写真集 「Santa Fe」
イ　親戚の小学生男児の全裸画像
ウ　ロリ漫画

オリジナル問題

ウ

問題7　解説

現行法では、

１　子ども（18歳に満たない者。以下、同じ。）を相手に性交や性交類似行為をし、又は、子どもが性交や性交類似行為をしている姿。

２　第三者が、子どもの性器などを触り、又は、子どもが第三者の性器などを触っている子どもの姿が写っているもので、性欲を興奮させ又は刺激するもの。

３　子どもの裸や一部しか服を身に付けていない子どもの姿が写っているもので、殊更に児童の性的な部位（性器若しくはその周辺部、臀部又は胸部をいう。）が露出され又は強調されているものであり、かつ、性欲を興奮させ又は刺激するもの。

が児童ポルノとされています。

　イラスト、コミックのようないわゆる「非実在」の子どもが描かれているものは児童ポルノとはみなされません。

問題8

LINE等SNSで知り合った異性（もしくは同性）から、自撮りした性的な写真や動画を交換しようと言われ、ついつい送ってしまった画像をネタに脅迫される事件を何というでしょう？

ア　セックストーション
イ　リベンジポルノ
ウ　デジタルタトゥー

オリジナル問題

ア

問題8　解説

ア　正解

イについて
　リベンジポルノとは、離婚した元配偶者や別れた元交際相手等が、相手から拒否されたことの仕返しに相手の裸の写真や動画など、相手が公開するつもりのない私的な性的画像を無断でネットの掲示板などに公開する行為を言います。

ウについて
　デジタルタトゥーは、いったんインターネット上で公開された書き込みや個人情報などが、一度拡散してしまうと、後から消すことが極めて困難であることを、入れ墨（タトゥー）を後から消すことが困難であることに喩えた表現です。

問題9

CSIRTの説明として，適切なものはどれか。

ア　IPアドレスの割当て方針の決定，DNSルートサーバの運用監視，DNS管理に関する調整などを世界規模で行う組織である。

イ　インターネットに関する技術文書を作成し，標準化のための検討を行う組織である。

ウ　国レベルや企業・組織内に設置され，コンピュータセキュリティインシデントに関する報告を受け取り，調査し，対応活動を行う組織の総称である。

エ　情報技術を利用し，信教や政治的な目標を達成するという目的をもった人や組織の総称である。

出典：情報セキュリティスペシャリスト試験 平成26年秋期問題

ウ

問題９　解説

CSIRT(Computer Security Incident Response Team，シーサート)は、組織内など限られた範囲のサイトに関するセキュリティインシデントについて対応するチームや組織の総称です。日本国内のサイトにインシデントに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行う機関“JPCERT”もCSIRT組織です。

ア　ICANN(The Internet Corporation for Assigned Names and Numbers，アイキャン)の説明です。

イ　IETF(Internet Engineering Task Force)の説明です。

ウ　正しい。CSIRTの説明です。

エ　ハックティビスト(Hacktivist)の説明です。

問題10

ディジタルフォレンジックスを説明したものはどれか。

ア　画像や音楽などのディジタルコンテンツに著作権者などの情報を埋め込む。

イ　コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つであり，システムを実際に攻撃して侵入を試みる。

ウ　ネットワーク管理者や利用者などから，巧みな話術や盗み聞き，盗み見などの手段によって，パスワードなどのセキュリティ上重要な情報を入手する。

エ　犯罪に対する証拠となり得るデータを保全し，その後の訴訟などに備える。

出典：情報セキュリティスペシャリスト試験 平成26年秋期問題

エ

問題10　解説

　ディジタルフォレンジックスは、不正アクセスや情報漏えいなどのセキュリティインデントの発生時に、原因究明や法的証拠を明らかにするために対象となる電子的記録を収集・解析することです。

ア　　ステガノグラフィの説明です。

イ　　ペネトレーションテストの説明です。

ウ　　ソーシャルエンジニアリングの説明です。

エ　　正しい。ディジタルフォレンジックスの説明です。

問題11

マルウェアの活動傾向などを把握するための観測用センサが配備されるダークネットはどれか。

ア　インターネット上で到達可能，かつ，未使用のIPアドレス空間
イ　組織に割り当てられているIPアドレスのうち，コンピュータで使用されているIPアドレス空間
ウ　通信事業者が他の通信事業者などに貸し出す光ファイバ設備
エ　マルウェアに狙われた制御システムのネットワーク

出典：情報セキュリティスペシャリスト試験 平成27年春期問題

ア

問題11　解説

　ダークネットは、インターネット上で到達可能かつ未使用のIPアドレス空間のことを指します。通常のインターネット利用を考えれば特定のホストに割り当てられていない未使用のIPアドレス宛にパケットが送信されることは稀なはずですが、実際にダークネットを観測すると相当数のパケットが未使用のIPアドレス宛に送信されているようです。
　これらは、マルウェアが次の感染対象を探すためのスキャンマルウェアが脆弱性を攻撃するためのパケット送信元IPアドレスが詐称されたパケットへの応答パケットなどの不正な活動を目的とするパケットに因るものです。
　つまりダークネットを観測することで、インターネット上で行われている不正活動を把握することが可能になります。基本的にダークネットに到達するパケットは不正なものであるため、観測された全てのパケットを不正なものとみなして分析できる点がダークネット観測の利点です。

ア　正しい。ダークネットの説明です。

イ　ライブネットの説明です。ダークネットと対比して使われる言葉です。

ウ　ダークファイバーの説明です。

エ　産業制御システム（ICS）および遠隔制御・監視システム（SCADA）のことでダークネットの説明ではありません。

問題12

クロスサイトスクリプティングに関する記述として、適切なものはどれか

ア　Webサイトの運営者が意図しないスクリプトを含むデータであっても利用者のWebブラウザに送ってしまう脆弱性を利用する。
イ　Webページの入力項目にOSの操作コマンドを埋め込んでWebサーバに送信しサーバを不正に操作する。
ウ　複数のWebサイトに対して、ログインIDとパスワードを同じものに設定するという利用者の習性を悪用する。
エ　利用者に有用なソフトウェアと見せかけて、悪意のあるソフトウェアをインストールさせ、利用者のコンピュータに侵入する。

出典：平成27年度春期ITパスポート試験公開問題

ア

問題12　解説

　クロスサイトスクリプティングとは、スクリプトが埋め込まれたページをそのまま利用者に送ってしまうという脆弱性を利用した攻撃手法です。

アは○　　クロスサイトスクリプティング

イは×　　OSコマンドインジェクション

ウは×　　パスワードリスト攻撃

エは×　　ウイルス一般。特にトロイの木馬

問題13

ディジタルコンテンツのコピープロテクトは，ディジタルコンテンツに関する著作者の権利を保護するための技術である。コピープロテクトを無効化する機能をもつプログラムの販売を禁止しているものはどれか。

ア　コンピュータ不正アクセス対策基準
イ　著作権法
ウ　電気通信事業法
エ　不正アクセス行為の禁止等に関する法律

出典：平成27年度春期ITパスポート試験公開問題

イ

問題13　解説

アは×
　コンピュータ不正アクセス対策基準は，コンピュータ不正アクセスによる被害の予防，発見及び復旧並びに拡大及び再発防止について，企業等の組織及び個人が実行すべき対策をとりまとめたものです。

イは○
　著作権法では，ソフトウェアや音楽・映像コンテンツなどの違法コピーを禁止しています。

ウは×
　電気通信事業法は，電話やインターネットなど電気通信サービスを提供する会社に検閲の禁止，秘密の保護，利用の公平などの義務を定めた法律です。

エは×
　不正アクセス行為の禁止等に関する法律は，ネットワークに接続されアクセス制御機能をもつコンピュータに，なりすまし行為などで不正アクセスを行ったり試みたりすること，それを幇助することを禁じた法律です。

問題14

電子メール送信時に送信者に対して宛先アドレスの確認を求めるのが有効であるセキュリティ対策はどれか。

ア　OP25Bによるスパム対策
イ　SPFによるスパム対策
ウ　電子メールの誤送信対策
エ　電子メールの不正中継対策

出典：平成23年度秋期基本情報技術者午前問題

ウ

問題14　解説

送信者の不注意に対しての対策だからウが○。
ウ以外は、受信側ISPのメールサーバでの対策。受信者への迷惑メール対策サービスです。

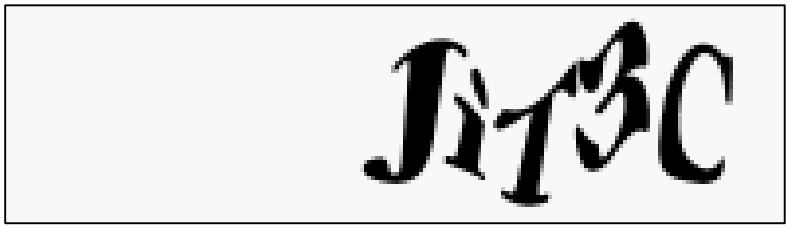
OP25B（Outbound Port 25 Blocking）：迷惑メール防止のため、ISPが特定のメールサーバ以外のサーバからの受信を拒否する仕組み。通常使用されるSMTPのポート番号25を閉ざして特定の番号を設定する。

SPF（Sender Policy Framework）：差出人のメールアドレスが他のドメインになりすましていないかどうかを、受信側ISPのメールサーバで検出する仕組み。フィッシング詐欺などには効果がある。

参照：「スパムメール対策」

問題15

電子掲示板やブログに投稿するとき，図のようなゆがんだ文字の画像が表示され，それを読み取って入力するよう求められることがある。その目的はどれか。



ア　システムが想定する表示機能をブラウザがもっているかどうかを判断する。
イ　事前に投稿を許可された利用者であることを認証する。
ウ　ディスプレイの表示機能に問題がないかを判別する。
エ　プログラムによる自動投稿を防止する。

出典：平成22年度春期ITパスポート試験公開問題

エ

問題15　解説

ア、ウは×
「投稿するとき」としているので，ア・ウは目的ではありません。そもそも，機能がない環境ならば，この画像は見えない。

イは×
「Webページを実際に閲覧している人には読めるが，その他の手段（プログラム）では読めない」ようにする手段である。許可されていない人もこのページは閲覧できるのだからイは×。

エは○
メールアドレスや臨時のパスワードを知られたくないようなときに用いることが多い。

クイズは終わりです。

あなたは
何問正解しましたか？