エキスパート活動　課題 A「個人認証」

□事例から考えよう！　※右の資料を参考に考えよう

＜事例 A＞

(1)ワンタイムパスワードはどのようなパスワードかまとめてみよう。

(2)パスワードが流出した場合でも、ワンタイムパスワードにより不正アクセスを防げる可能性がある。それはなぜか？

＜事例 B＞

(1)なぜ A 助の SNS は乗っ取られてしまったのか原因をあげてみよう。

(2)パスワードの攻撃にはどのような種類があるのかまとめてみよう。

(3)パスワードを作るときに気をつけるべきことは何かまとめてみよう。

□多要素認証

大切なアカウントなどは、知識認証、所有物認証、生体認証から二つ以上の要素を組み合わせて認証を行う、多要素認証が導入されていることが多い。多要素認証は、一つの認証が突破されたとしても、複数の異なる要素の認証が必要なため、不正アクセスの危険性を減らし、セキュリティを高めることができる。また、認証の要素の数は問わないが、２回以上の認証を行うことを多段階認証という。

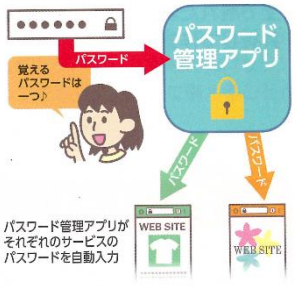
□パスワードの攻撃手法

パスワードを不正に取得するための攻撃手法は次の通りである。パスワードを作成したり運用したりする際には、これらの攻撃手法に耐えられるようにする必要がある。

	攻撃手法
辞書攻撃	辞書や人名録など、既存の文字列を使い、パスワードを生成して解読する。
総当たり攻撃	全通りの数字・文字・記号の組み合わせを試して解読する。ブルートフォース攻撃ともいう。
逆総当たり攻撃	よく使われる脆弱なパスワードを、一つのアカウントに対して１回程度、それをたくさんのアカウントに対して試みる。リバースブルートフォース攻撃ともいう。
リスト型攻撃	別のシステムから何らかの形で流出したパスワードを使い、ほかのサービスへ不正にログインする。
ソーシャルエンジニアリング	ごみ箱から書類を盗んだり、パスワードをのぞき見たりするなど、ICT 技術を使わずに心理的な隙や行動のミスにつけ込む。

□パスワード管理アプリ

近年、さまざまな Web サービスがあるため、たくさんのパスワードを作成、運用しなければならない。そこで、さまざまなパスワードを一括で管理してくれる「パスワード管理アプリ」がある。ユーザは、パスワード管理アプリのパスワードのみ記憶すればよく、ユーザの負担を軽減してくれる。



□ワンタイムパスワード

ログインする際、あらかじめ登録したメールアドレスや、SNS、専用アプリに通知される一度だけかつ短時間有効なパスワードである。ワンタイムパスワードをユーザ ID とパスワードに加えて入力することで、ログインができる。攻撃者にパスワードを不正入手された場合でも、ワンタイムパスワードが必要となるため、不正アクセスを防げる可能性が高まる。

エキスパート活動　課題Ｂ　「マルウェア」

□事例から考えよう！　※右の資料を参考に考えよう

＜事例１＞

(１)ウイルス対策ソフトウェアとは、どのようなソフトウェアかまとめてみよう。

(2)ウイルス対策ソフトウェアを入れないと、どのようなトラブルがコンピュータに起きるのか考えてみよう。

(3)ウイルス対策ソフトウェアは、どのような仕組みでウイルスを検知するのか調べてみよう。

＜事例2＞

(１)ウイルススキャンは、どのような機能か調べてみよう。

(2)ウイルスに感染しないためには、どうすればよいのか考えてみよう。

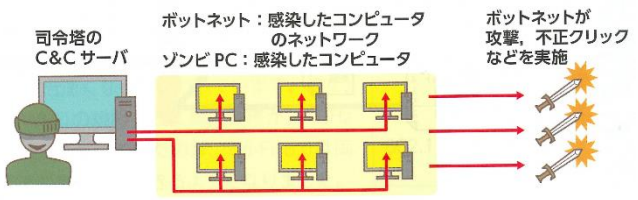
(3)ウイルス定義ファイルは、なぜ定期的な更新が必要なのかまとめてみよう。

□マルウェア（または単にウイルス）の種類

マルウェアには、次のようなさまざまな種類がある。

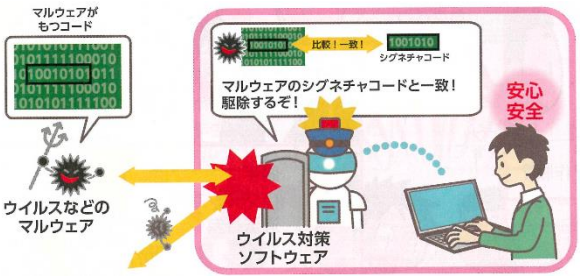
名称	特徴、症状
コンピュータウイルス	ワープロソフトやメールソフトなど、ほかのソフトウェアにもぐりこんで寄生し、ファイルの破壊などを行う。
ワーム	ソフトウェアに寄生せず、完全に自立して存在し、自己増殖する。
トロイの木馬	実用性や娯楽的要素を含んだ有用なプログラムに見せかけて侵入する。
スパイウェア	コンピュータ内に保存された個人情報やコンピュータの使用履歴、ブラウザの閲覧履歴などを無断で第三者に送信する。
アドウェア	ユーザが意図しない広告を強制的に表示する。
キーロガー	キーボードの入力情報を記録するもので、デバッグなどに利用するツールだったが、パスワードを盗むことに悪用されることがある。
ランサムウェア	感染したパソコンをロックしたり、ファイルを暗号化したりすることによって使用不能にしたあと、もとに戻すことと引き換えに身代金を要求する。

□ボットネット　※最新のウイルス攻撃



パソコンやスマートフォンがボットと呼ばれるマルウェアに感染すると、端末が第三者の指示通りに動く操り人形のようになってしまう。ボットに感染した端末が、ほかのボットに感染した端末とともにネットワークが組まれることで、不正アクセスの踏み台になったり、DDoS 攻撃（Distributed Denial of Service　分散型サービス拒否攻撃）に利用されたりするといったさまざまな犯罪に悪用されることになります。

□ウイルス対策ソフトウェアの仕組み



ウイルス対策ソフトウェアは、エンジニアやシステムによって発見されたウイルスのデータを解析し、その一部分であるデータを切り抜いたシグネチャコードと、コンピュータ内に保存されたり通信されたりしているデータを比較照合することでウイルスを検出する。このウイルスを検出するために使用する情報をウイルス定義ファイルという。

□マルウェアから身を守るための対応と対策

(1)マルウェアに感染した!?と思ったら

①ネットワークから切断する：マルウェアの中には、ネットワークを使い、他のコンピュータに感染しようとしたり、攻撃しようとしたりするものが存在する。そのため、マルウェアに感染した場合は、LAN ケーブルを抜く、無線 LAN をオフにするなどして被害の拡大を食い止めることが大切である。

②ウイルス対策ソフトウェアと隔離・駆除：ウイルススキャンをし、マルウェアの特定、マルウェアに感染したファイルの特定と隔離、その駆除を行う。感染後はウイルス対策ソフトウェアのスキャンを回避してしまうマルウェアも存在するため、感染しないよう注意が必要である。

(2)簡単にできるマルウェア対策

①基本ソフトウェア（OS：オペレーティングシステム）とウイルス定義ファイルの更新し、常に最新の状態にする

②メールに添付された不審なファイルやURLは開かない

③ウイルス対策ソフトウェアを用いて定期的にウイルススキャンをする、また外部記憶装置（USB メモリ等）を接続する際にもウイルスチェックを行う

エキスパート活動　課題Ｃ　「不正アプリ」

□事例から考えよう！　※右の資料を参考に考えよう

＜事例Ａ＞

(1)安全なアプリの条件について考えてみよう。

(2)安全なアプリを入手するためには、どうすればよいのかを調べ、まとめてみよう。

(3)アプリの利用に必要がないと考えられる個人情報を提供すると、どのような問題が起きるのか考えてみよう。

＜事例Ｂ＞

(1)スパイウェアに感染したのは、どの段階か考えてみよう。

(2)スパイウェアは、どのような不正をはたらいたのか考えてみよう。

(3)出所が不明なアプリをダウンロードすると、どのような危険性があるのかまとめてみよう。

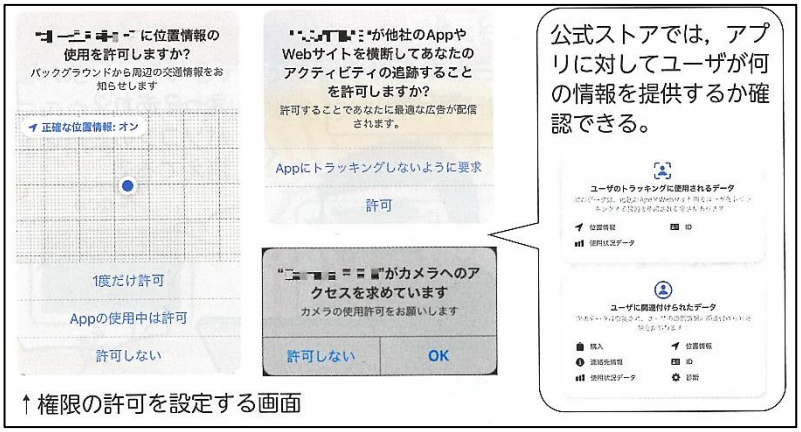
□安全なアプリの入手

インターネットには、危険なアプリがたくさん存在している。安全にアプリを利用するためにも、アプリの入手先と提供する情報などに注意する。

スマートフォンの場合、Android では「Google Play」、iOS では「App Store」という公式ストアが存在している。これらの公式ストアに存在するアプリは、事前にコンピュータや人による審査が行われたものであるため、**安全である可能性が高い**。しかし、審査の目をかいくぐって公式ストアに登録されていることもあるので、**ダウンロードする前に、アプリの提供元、アプリに提供するデータや許可する権限などについて、利用規約をよく読んで確認**し、不審な内容がないか確認する。

□アプリの許可にする権限の管理

安全なアプリと判断した場合でも、むやみに権限の許可をせず、本当に許可する必要があるかどうかを判断し、設定する必要がある。(右図)



□アプリの自動更新設定とサポート切れのアプリケーションの危険性

新しい機能の追加や不具合の解消、セキュリティの脆弱性(ぜいじゃくせい)(**セキュリティホール**と呼ばれる)に対する修正プログラムを実行するため、アップデートが行われる。**自動的にアップデートが行えるように設定しておくと、常に最新の状態でアプリを使用できるので安全**である。しかし、今のアプリに替わる新しいアプリが登場したりサービスが終了したりすると、サポートが終了となり、アプリの更新が行われなくなることがある。そのまま使い続けると、セキュリティの脆弱性を抱えたまま、アプリを利用することとなるため、サイバー攻撃の標的になる可能性が高くなる。サポートが切れたアプリは絶対に使わないようにする。

□スパイウェアとは?

スパイウェアは、**コンピュータに侵入してコンピュータ内部の情報を収集し、外部へ情報を漏えいさせるプログラム**である。スパイウェアはユーザに気付かれないように情報を流出させようとするため、コンピュータに症状が出ないことがある。

スパイウェアの侵入経路は多岐にわたり、アプリやメール、Web サイトの閲覧で侵入する可能性がある。

侵入を防ぐためには、安易にアプリをダウンロードしたり、添付ファイルを開いたりしないことや、OS とウイルス対策ソフトウェアを常に最新の状態にしておくことが大切である。