学んで活かそう
パソコン教室

PCセキュリティの実践

１章：メールによる攻撃の種類と対処方法
２章：ブラウザの攻撃の種類と対処方法
３章：SNSのセキュリティ設定
４章：質疑応答タイム

１章：メールによる攻撃の種類と対処方法

標的型メール攻撃

情報セキュリティ10大脅威2017

順位	組織	昨年順位
1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	7位
3位	ウェブサービスからの個人情報の窃取	3位
4位	サービス妨害攻撃によるサービスの停止	4位
5位	内部不正による情報漏えいと それに伴う業務停止	2位
6位	ウェブサイトの改ざん	5位

＊IPA（情報処理推進機構）の2017年1月31日の発表資料より

どんな攻撃なのか？

標的型メールとは、特定の相手を狙ってまるで疑う余地のない件名や本文でメールを送り付け添付のファイル経由で相手に**ウイルス**や**マルウエア**を感染させます。
この添付ファイルにはPDFファイルやWord、Excel、などの業務ファイルにウイルスが埋め込んであるケースが多いため、ウイルス対策ソフトで検知されにくい上にメールの受信者も不審に思わず開封して感染してしまうのです。

マルウエア(malware)とは：不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称で、コンピュータウイルスやワームなどがある。

ランサムウエアとは：マルウェアの一種である。これに感染したコンピュータは、利用者のシステムへのアクセスを制限する。この制限を解除するため、被害者がマルウェアの作者に身代金（ransomランサム）を支払うよう要求する。

メールの特徴

難易度	特徴
低難易度	他国語が混じっていたり、日本語の「てにをは」がおかしいなどの特徴を持つもの。 標的型攻撃に使われるなりすましメールの特徴をいくつか知っていれば、見分けられる可能性がある。 標的型メールではないもの。 広告メールやフィッシングメールなど、不特定多数の人に送られたもの。 基本的なセキュリティリスクをいくつか知っていれば、見分けられる可能性がある。
中難易度	業務に関連しているように見せかけたメールを攻撃者が作ったもの。 IPAなどのWebサイトにある記述をそのままコピーして利用したもの。 自分に関わりの無い内容が書かれていた場合は、見分けられる可能性がある。 セミナーの案内等見分けが難しいものもあるが、添付書類は安易な実行ファイルレベル。
高難易度	マルウェアを使って実際の業務メールを盗み出し、流用している本文や件名は過去に送受信された業務メールであり、見分けることは困難。添付書類もゼロデイが使用されるなど見極めは不可能。

引用元　株式会社ラック
https://www.lac.co.jp/library/guidebook/14.html

対策は？

・添付ファイルを開かない。

⇒　実際には難しい。プレビューしただけで感染するタイプのものもある。

・メールサービスに危険性のあるメールを排除するゲートウエイサービスを経由させる。

⇒　有償サービス。（準推奨）

・管理者ユーザーでパソコンを使わないで標準ユーザーで運用する。

⇒　無償、インストールが自動で始まらないので安全性が高い。慣れた人に設定をお願いする必要がある。（推奨）

セキュリティのことを勉強するには

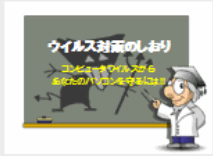
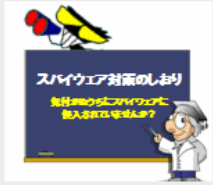
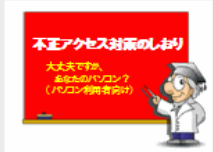
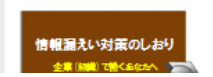
まずはここを抑える

http://www.ipa.go.jp/security/

様々なセキュリティ対策を学べる

https://www.ipa.go.jp/security/antivirus/shiori.html#management_guidebook

IPA対策のしおりシリーズ

1		ウイルス対策のしおり（第10版）（815KB） ～コンピュータウイルスからあなたのパソコンを守るには!!～ （注1）	[英語版] （1.6MB）
2		スパイウェア対策のしおり（第10版）（822KB） ～気付かぬうちにスパイウェアに侵入されていませんか？～ （注1）	[英語版] （4.4MB）
3		ボット対策のしおり（第10版）（1.0MB） ～あなたのパソコンはボットに感染していませんか？～（注1）	[英語版] （2.1MB）
4		不正アクセス対策のしおり（第6版）（779KB） ～大丈夫ですか、あなたのパソコン？（パソコン利用者向け）～（注1）	[英語版] （3.2MB）
5		情報漏えい対策のしおり（第7版）（795KB）	[英語版]

２章：ブラウザの攻撃の種類と対処方法

Webサイト経由の悪意のある攻撃

A　ワンクリック詐欺(不正請求）サイト

B　フィッシングサイト

C　偽セキュリティ対策ソフトを提供するサイト

D　迷惑ブログサイトあるいは迷惑ブログコメント・トラックバック

利用者の対策（IPAガイドより）

● パソコンの OS やアプリケーション（ブラウザやメーラーを含む）のぜい弱性を解消し（最新の状態にする）、**セキュリティゾーン設定**を強化（ActiveX、JavaScript の動作抑止）する

●ウイルス対策ソフトで定期的にウイルス検査を実施する

●見知らぬ人からのメールや添付ファイルは安易に開かない

●銀行や信販会社からのメールを安易に信用しない

●OS が表示する警告メッセージが出たら、慌てずに、自分の意思でないダウンロード要求はキャンセルする

●標準ユーザーでパソコンを使う（追加）

詳細情報リンク

■ 身に覚えのない不正請求などの防止
http://www.ipa.go.jp/security/personal/protect/oneclick.html

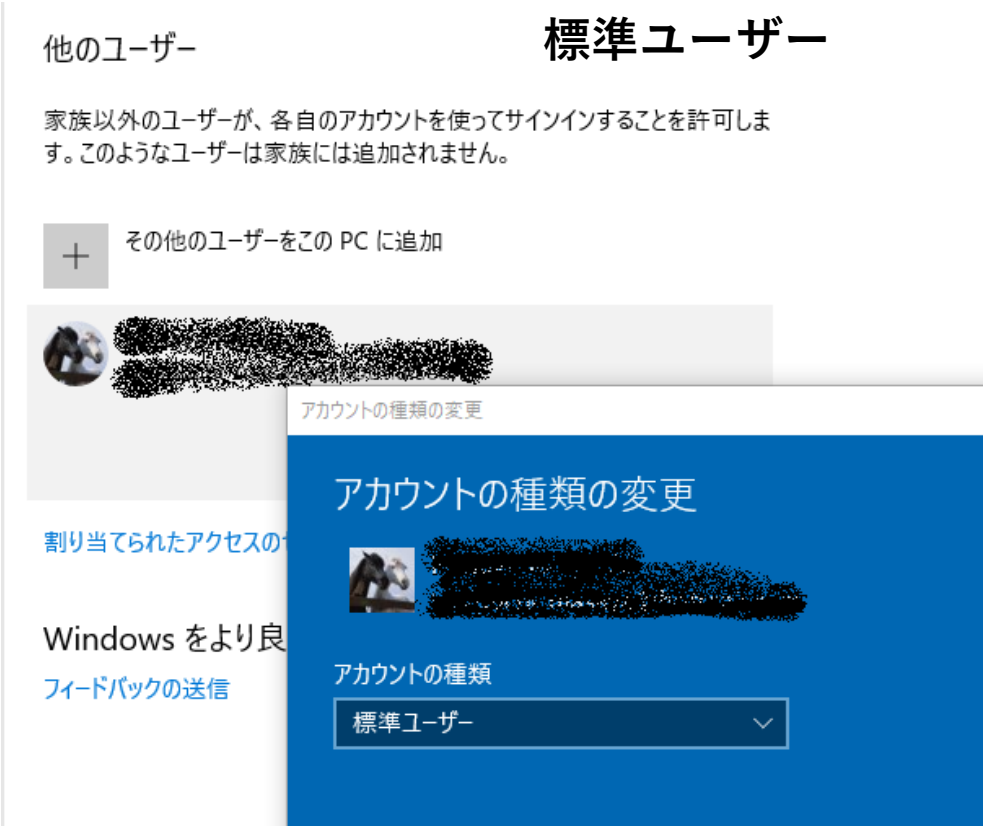
■ フィッシング (Phishing)対策
http://www.ipa.go.jp/security/personal/protect/phishing.html
■ AntiPhishingJapan フィッシング対策協議会
http://www.antiphishing.jp/

■セキュリティゾーンの設定
http://www.microsoft.com/japan/windows/ie/using/howto/security/setup.mspx

ユーザーの違い

管理者

標準ユーザー



〇ユーザーを作成・変更・削除可能
〇アプリのインストール可能

〇ユーザーを変更可能
×アプリのインストール可能
　＊管理者の許可が必要になる

３章： SNSのセキュリティ設定

Facebookプライバシー設定

【ポイント】最初の状態だと友達になりやすい（情報がオープン）になっている

Facebookブロック設定

不幸にしてトンでもない人から誹謗中傷を受けたら「ブロック」できる

Twitterプライバシー設定

４章：質疑応答タイム