ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

## ●IPAが2014年に発生した「情報セキュリティ10大脅威」を発表

http://www.ipa.go.jp/security/vuln/10threats2015.html
http://www.ipa.go.jp/files/000043628.pdf

### このニュースをザックリ言うと・・・

- 2月6日（日本時間）、独立行政法人情報処理推進機構（IPA）は、2014年に発生した情報セキュリティの事故・事件のうち、社会的に影響が大きかったと考えられる「脅威トップ10」を発表しました。

- ランキングは1位が「オンラインバンキングやクレジットカード情報の不正利用」、以下「内部不正による情報漏えい」「標的型攻撃による諜報活動」「ウェブサービスへの不正ログイン」「ウェブサービスからの顧客情報の窃取」「ハッカー集団によるサイバーテロ」「ウェブサイトの改ざん」「インターネット基盤技術の悪用」「脆弱性公表に伴う攻撃の発生」「悪意のあるスマートフォンアプリ」となっています。

### AUS便りからの所感等

- 1位となった「オンラインバンキングやクレジットカード情報の不正利用」において、PCに感染したマルウェアが偽のログイン画面を表示して、アカウント情報や振込の際の番号カードに書かれた番号を詐取する手法が使われる等、多くの脅威においてマルウェアによる不正行為、もしくはマルウェアに感染させようとする不正行為が関わっています。

- こうした様々な攻撃から身（PCや情報資産など）を守るためにも、アンチウイルスとUTMによる防御は必ず行うように強く推奨します。

IPA Better Life with IT 情報処理推進機構

最終更新日：2015年2月6日

### 「情報セキュリティ10大脅威 2015」の順位を発表

「情報セキュリティ10大脅威 2015」は、2014年に発生した情報セキュリティの事故・事件のうち、社会的に影響が大きかったと考えられる脅威から、情報セキュリティ分野の研究者、企業の実務担当者など64組織96名のメンバーからなる「10大脅威執筆者会」の審議・投票を経てトップ10を選出したものです。今年は近年の情報セキュリティの重要性や変化の速さを考慮し、順位を先行して公表しました。また、例年通り3月にこの「情報セキュリティ10大脅威 2015」の詳しい解説資料を本ページで公開する予定です。

「情報セキュリティ10大脅威 2015」

1位「オンラインバンキングやクレジットカード情報の不正利用」
2位「内部不正による情報漏えい」
3位「標的型攻撃による諜報活動」
4位「ウェブサービスへの不正ログイン」
5位「ウェブサービスからの顧客情報の窃取」
6位「ハッカー集団によるサイバーテロ」
7位「ウェブサイトの改ざん」
8位「インターネット基盤技術の悪用」
9位「脆弱性公表に伴う攻撃の発生」
10位「悪意のあるスマートフォンアプリ」


2015年も継続して企業や組織、個人のいずれも様々な脅威にさらされることが見込まれます。被害に遭わないためには、まず脅威の手口を理解し、「明日は我が身」という意識で、適切な対策を講じる必要があります。

第1位　オンラインバンキングやクレジットカード情報の不正利用

ウイルスやフィッシング詐欺により、オンラインバンキングの認証情報やクレジットカード情報が窃取され、本人になりすまして不正に利用や送金が行われた。また、2014年は個人だけでなく法人口座からの不正送金被害が急増したことが特徴的だった。

［主な対策］ウイルス対策ソフトの導入、ソフトウェアの更新、ワンタイムパスワードの利用

# ●NASがスパムメール送信の踏み台に…管理パスワード変更せず

http://www.itmedia.co.jp/news/articles/1502/03/news076.html
http://www.tmu.ac.jp/news/topics/10006.html?d=assets/files/download/news/press_20150202.pdf

## このニュースをザックリ言うと・・・

- 2月2日（日本時間）、首都大学東京は、同大学の南大沢キャンパス(東京都八王子市)に設置されたNASがスパムメール送信の踏み台になっていたことを発表しました。

- 同大学では、別のNASが外部からFTPアクセスが可能になっていたために個人情報が流出する問題が発表されたばかりでした。

- 1月27日 15:06から16:37の約1時間半の間に約10万通のスパムメールを送信していたことが確認されていますが、今回問題になったNASはFTPアクセスを無効にしていた一方で、管理者パスワードが初期値のままだったとのことです。


## AUS便りからの所感等

- ネットワーク機器における管理者パスワードの初期設定情報は、商品毎に共通しているものであれば誰でも入手可能で、あらゆるメーカーについてのそういった情報を集めたサイトも存在します。

- ひとたび内部ネットワークへの侵入に成功した攻撃者に狙われる可能性も十分に考えられますので、外部から直接アクセスできないLAN上に設置した機器であっても、必ずパスワードの設定を行ってください。

# ●Flash Playerのセキュリティホール報告と修正相次ぐ

http://blog.trendmicro.co.jp/archives/10786
http://blog.trendmicro.co.jp/archives/10837

## このニュースをザックリ言うと・・・

- 1月から2月上旬にかけて、Flash Playerにおいて相次いでセキュリティホールが報告され、一時は修正版が出るまでの間に「0-day(ゼロデイ)攻撃」として悪用される事態となりました。

- 1月13日（日本時間、以下同様）、Flash Player 16.0.0.257がリリースされましたが、その約10日後の1月22日、未修正のセキュリティホール2件を悪用する攻撃ツールが出回っているとセキュリティベンダー等から発表され、それらを修正するために1月23日に16.0.0.287、1月28日に16.0.0.296がリリースされました。

- しかし2月2日、16.0.0.296にも別のセキュリティホールが存在し、動画サイト等の広告を通じて攻撃が行われるといった事例が確認され、2月6日に16.0.0.305がリリースされました。


## AUS便りからの所感等

- Flash Playerは度々のようにセキュリティホールが狙われるうえ、Webサイト自体がクラックされていなくても、そこに表示される広告等から攻撃を行う等が可能です。

- ブラウザによってはFlash PlayerやJavaといったプラグインをデフォルトで無効化し、クリックして表示できるようにする設定も可能です。

- しかし、悪意のあるコンテンツかどうかクリックしないと分からないケースもありますから、やはりアンチウイルスとUTMによる防御は欠かせません。