— AUS（アルテミス・ユーザ・サポート）便り 2015/03/09号 —

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　3月の呼びかけ「セキュリティの脅威について正しい認識と対策を」

http://internet.watch.impress.co.jp/docs/news/20150303_690873.html
http://www.ipa.go.jp/security/txt/2015/03outline.html

このニュースをザックリ言うと・・・

- 3月2日（日本時間）、独立行政法人情報処理推進機構（IPA）が毎月行っている「今月の呼びかけ」の3月度が発表されました。

- 呼びかけでは、2月17日に発表した「2014年度 情報セキュリティの脅威に対する意識調査」の結果に言及していますが、Windows Update等アップデートを実施していないユーザが約33%、そのうちアップデートの方法がわからないユーザも約10%存在しており、同組織が提供する「MyJVNバージョンチェッカ」を用いる等により、重要なソフトウェアのアップデートを確実に行うよう呼びかけています。

- また、約52%のユーザがPCのデータをバックアップしていないという結果も報告されており、特にデータを不正に暗号化して解除のための身代金を要求する「ランサムウェア」対策のためにも、バックアップを行うことを推奨しています。

AUS便りからの所感等

- IPAでは、2月1日～3月18日を「サイバーセキュリティ月間」と定めていることから、前述した他にも、PCとネットワークあるいはスマートフォンに至るまでを常に安全に保つための「情報セキュリティ対策9カ条(※)」等が挙げられており、セキュリティについて日頃意識している事柄が十分かどうか、改めて確認する良い機会となるでしょう。

- そして、アンチウイルス・UTMは、必ずしもそれだけで不正アクセスやマルウェアから100%防御してくれるわけではありませんが、セキュリティに関する意識の強化・他の各種対策と併せ、最低限の防御策として決して導入が欠かせないものとなります。

INTERNET Watch

ニュース

セキュリティの基本的対策をしていないユーザーが3割程度存在、IPAが再確認呼び掛け

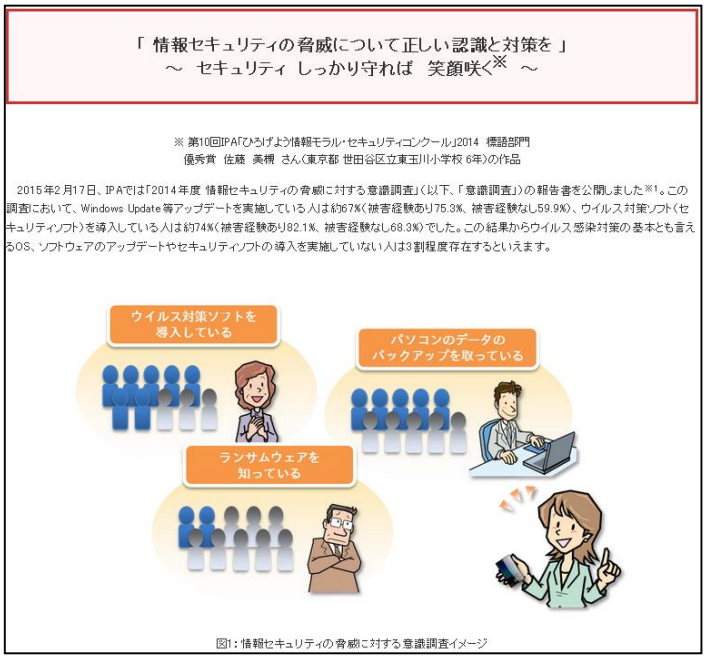
(2015/3/3 12:45)

g+1 11　B! 27　ツイート 89　いいね！ 25　Pocket 25

独立行政法人情報処理推進機構（IPA）は2日、セキュリティに対する意識調査の結果では、基本的な対策を実施していないユーザーが3割程度存在するとして、セキュリティに対する認識を深めて、インターネットを安全に利用するための対策を再確認する呼び掛けを行った。

IPAが行った「2014年度情報セキュリティの脅威に対する意識調査」によると、Windows Updateなどのアップデートを実施している人は約67%、ウイルス対策ソフトを導入している人は約74%となり、未実施のユーザーが3割程度存在。IPAの安心相談窓口に寄せられるウイルス感染や不正アクセスに関する被害でも、基本的な対策ができていれば被害に遭わずに済んだと考えられるケースが多くあり、実態を表した数値と考えられるとしている。

意識調査では、JavaやFlash Playerなどのバージョンアップを行っていないユーザーに理由を尋ねたところ、アップデートの方法が分からないとする回答が約10%あった。IPAでは、PCにインストールされているソフトが最新状態であるか、どのようにアップデートを行えばいいかを確認できるツール「MyJVN バージョンチェッカ」を提供しており、このツールを活用したバージョン管理実施を推奨している。



「 情報セキュリティの脅威について正しい認識と対策を 」
～ セキュリティ しっかり守れば 笑顔咲く※ ～

※ 第10回IPA「ひろげよう情報モラル・セキュリティコンクール」2014 標語部門
優秀賞 佐藤 美視 さん（東京都 世田谷区立東玉川小学校 6年）の作品

2015年2月17日、IPAでは「2014年度 情報セキュリティの脅威に対する意識調査」（以下、「意識調査」）の報告書を公開しました※1。この調査において、Windows Update等アップデートを実施している人は約67%（被害経験あり75.3%、被害経験なし59.9%）、ウイルス対策ソフト（セキュリティソフト）を導入している人は約74%（被害経験あり82.1%、被害経験なし68.3%）でした。この結果からウイルス感染対策の基本とも言えるOS、ソフトウェアのアップデートやセキュリティソフトの導入を実施していない人は3割程度存在するといえます。

図1：情報セキュリティの脅威に対する意識調査イメージ

（※）「情報セキュリティ対策9か条」
http://www.nisc.go.jp/security-site/files/leaflet_20150201.pdf

●国内でのPOSへのマルウェア感染、2014年から本格化...トレンドマイクロ発表

http://news.mynavi.jp/news/2015/02/26/385/
http://www.trendmicro.co.jp/jp/security-intelligence/sr/sr-2014annual/

このニュースをザックリ言うと・・・

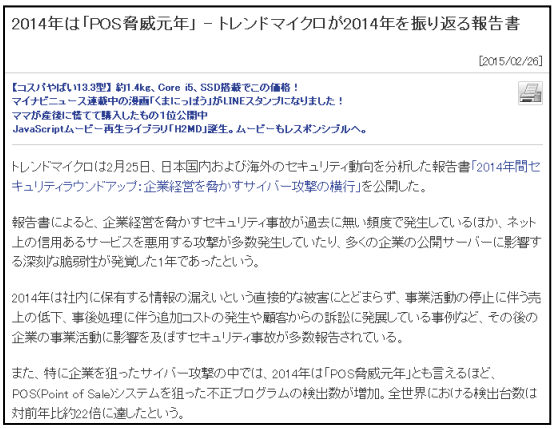
- 2月25日（日本時間）、トレンドマイクロ社が「2014年間セキュリティラウンドアップ：企業経営を脅かすサイバー攻撃の横行」と題した報告書を発表しました。

- レポートでは、「企業経営に影響する規模の被害をもたらすサイバー攻撃」の一つとして、「販売時点情報管理システム(POS)」に感染するマルウェアの存在が挙げられており、クレジットカード番号をはじめとする顧客情報の流出等が発生、またその検出台数は2013年の22台から約22倍となる491台にも上ったとされています。

AUS便りからの所感等

- 近年、組み込み用途のWindows OSで構築される、および専用線等ではなくインターネット経由で中央サーバとデータのやり取りを行うPOSの利用も珍しくなく、一般のPCで利用されるWindowsに感染するマルウェアが同一LAN上から、あるいは外部のネットワークから入り込んで感染する可能性もあるということを今後ますます認識する必要があるでしょう。

- 可能であれば、他のPCを踏み台としてマルウェアがPOSに感染しないよう、特に通信する必要があるサーバ以外はLAN上から隔離すること、組み込み用途のWindowsにも対応するアンチウイルスを導入すること、そしてもちろんUTMの導入によるマルウェアの侵入防止が重要な対策となります。


2014年は「POS脅威元年」－トレンドマイクロが2014年を振り返る報告書

[2015/02/26]

【コスパやばい13.3型】約1.4kg、Core i5、SSD搭載でこの価格！
マイナビニュース連載中の漫画「くまにっぱう」がLINEスタンプになりました！
ママが産後に慌てて購入したもの1位公開中
JavaScriptムービー再生ライブラリ「H2MD」誕生。ムービーもレスポンシブルへ。

トレンドマイクロは2月25日、日本国内および海外のセキュリティ動向を分析した報告書「2014年間セキュリティラウンドアップ：企業経営を脅かすサイバー攻撃の横行」を公開した。

報告書によると、企業経営を脅かすセキュリティ事故が過去に無い頻度で発生しているほか、ネット上の信用あるサービスを悪用する攻撃が多数発生していたり、多くの企業の公開サーバーに影響する深刻な脆弱性が発覚した1年であったという。

2014年は社内に保有する情報の漏えいという直接的な被害にとどまらず、事業活動の停止に伴う売上の低下、事後処理に伴う追加コストの発生や顧客からの訴訟に発展している事例など、その後の企業の事業活動に影響を及ぼすセキュリティ事故が多数報告されている。

また、特に企業を狙ったサイバー攻撃の中では、2014年は「POS脅威元年」とも言えるほど、POS(Point of Sale)システムを狙った不正プログラムの検出数が増加。全世界における検出台数は対前年比約22倍に達したという。

●成田空港のWebサイトが改ざん被害

http://www.narita-airport.jp/jp/news/150305.html
http://internet.watch.impress.co.jp/docs/news/20150306_691572.html

このニュースをザックリ言うと・・・

- 3月5日（日本時間）、成田国際空港を運営する成田国際空港株式会社から、自社のWebサイトが外部からの攻撃によって改ざんされていたことが発表されました。

- 被害を受けたのは成田空港ホームページ（http://www.narita-airport.jp/）および成田国際空港株式会社ホームページ（http://www.naa.jp/）で、サイトのコンテンツ管理システム（CMS）に侵入され、3月3日0時20分から3月5日1時00分の間、一部ページへのアクセスにより悪意のあるサイトへリダイレクトされるようになっていたとのことです。

AUS便りからの所感等

- CMSによっては古いバージョンの脆弱性を突かれる攻撃も報道されることが多いため、CMSやそれに更新のためにアクセスするクライアントPCがターゲットとされないよう、常に最新のバージョンになっているか確認することが重要です。

- 発表によれば、サーバ上からはマルウェアが検出されておらず、前述のとおりリダイレクトを行うよう細工されていた模様とのことで、このような形の改ざんも素早く検知できるようユーザと同様に外部から随時Webサイトにアクセスしてチェックを行うことも大事であり、その際に実際にマルウェアに感染してしまうことのないようアンチウイルス・UTMによる防御も必要不可欠となります。


成田国際空港 公式WEBサイト

バリアフリーページ | ENGLISH | 한국어 | 简体中文 | 繁體中文

お問い合わせ・ご意見はこちら　検索キーワードを入力

HOME | フライト情報 | 出発・到着・乗継 | 交通アクセス | ターミナル案内 | レストラン・ショップ | トラベルサポート | イベント・お楽しみ

NARITA AIRPORT　マップのご利用方法

HOME ≫ お知らせ

お知らせ

弊社ホームページ改ざんに関するお詫びと復旧のご報告

2015年3月5日

弊社サイトの一部において、第三者からの不正アクセスにより改ざんされていることが判明したため、同サイトを2015年3月5日1時00分 ～17時37分の間閲覧し調査しておりましたが、原因を特定しサイトを復旧いたしましたのでご報告いたします。ご利用いただいておりますお客様におかれましては、ご迷惑をお掛けしましたことを、深くお詫び申し上げます。

■今回の事象について

サイトを更新するシステムであるCMS（Contents Management System）に対して外部から侵入し、サイトを書き換えることで、ウイルスに感染するサイトへ誘導する攻撃内容がありました。

■対象ページ　※以下サイトの一部のページ

成田空港ホームページ
http://www.narita-airport.jp/
成田国際空港株式会社ホームページ
http://www.naa.jp/