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。

●「2016年の10大セキュリティ事件」、マカフィーが発表

http://www.atmarkit.co.jp/ait/articles/1611/11/news083.html
http://www.mcafee.com/jp/about/news/2016/q4/1110-01.aspx

このニュースをザックリ言うと･･･

- 11月10日（日本時間）、大手セキュリティベンダーのマカフィー（インテルセキュリティ）社より、「2016年の10大セキュリティ事件」が発表されましたが、これは同社が行った調査により認知度が高かったセキュリティ事件に関するランキングで、今年で3回目となります。

- 1位となった「振り込め詐欺／迷惑電話による被害」(認知度51.7%)、2位の「大手金融機関やクレジットカード会社などをかたるフィッシング」(同36.9%)、4位の「公共無線LANのセキュリティ問題」(同33.4%)および9位「ランサムウェア」(同28.0%)が10大事件の中で以前から発生しているものとなっています。

- 一方、今年発生した特色のある事件としては、3位に「ポケモンGOの偽アプリ」(同35.8%)、5位に「Anonymous(ハッカー集団)による日本への攻撃」(同28.9%)、8位に「JTBからの個人情報流出」(同28.3%)等が挙げられています。

AUS便りからの所感等

- 10大セキュリティ事件に関する調査は、日本国内の経営層や情報システム部門などのビジネスパーソンを対象に行われたものですが、振り込め詐欺が1位となっていることは、長年の間事件の発生がメディアで取り上げられ、啓発が行われていることから、さほどITと密接なわけでもない事件でありながらインパクトを保っているものと思われます。

- 同ランキングでは、2014年はベネッセ、2015年は年金機構、それぞれの個人情報流出事件が1位でしたが、今年のJTBの事件は8位だったものの、被害件数は年金機構の事件よりは多くなっており、2017年には同様の規模の事件が国内で起こらないよう願いたいものです。

- 9位のランサムウェアは2014年末よりその脅威が叫ばれましたが、今年初めてのランクインとなっており、依然としてその猛威は続く一方、感染によるファイルの暗号化への対策は、まだ定着しているとは言い難い感があります。

- いずれにしても、各々のセキュリティ問題について適切な対策法を把握して実行すること、またそのためのシステム・ネットワーク構成の見直しにあたっては、アンチウイルスやUTMを確実に利用することが重要なポイントとなるでしょう。

@IT

3位はPokemon GOの偽アプリ、2位はクレカ詐欺、1位は……？：
「2016年の10大セキュリティ事件」、マカフィーが公開

マカフィーが「2016年の10大セキュリティ事件」を発表。2016年は「Pokemon GOの偽アプリ」「ランサムウェアの被害」が急上昇した。

[@IT]

インテル セキュリティ（日本での事業会社はマカフィー）は2016年11月10日、「2016年の10大セキュリティ事件」を発表した。2016年は、「ランサムウェア」や「Pokemon GO」に関連する脅威がトップ10に入った。

1位は「振り込め詐欺／迷惑電話による被害」、2位「大手金融機関やクレジットカード会社などをかたるフィッシング」がランクイン。そして3位には「Pokemon GO」に便乗した偽アプリの事案が入った。

この他、日本でのランサムウェアの被害拡大と認知率の高まりを受け、2015年は圏外だった「ランサムウェア（身代金ウイルス）の被害」が9位に入った。ランサムウェアの脅威は、セキュリティ担当者／IT管理者だけでなく、一般層も含めて意識と関心が高まったことが伺える。

マカフィーによると、日本におけるランサムウェアの被害は2016年初旬から拡大し、特に2016年1月～3月に被害が急増した。同社は、「個人利用が業務利用にかかわらず、スマートフォンやPC、デジタル家電など、ランサムウェアの攻撃によるリスクがあらゆる場面に潜んでいる。今後もランサムウェア攻撃は続くだろう」と、継続した注意を促した。

2016年の10大セキュリティ事件の結果は、同社が日本の経営層／情報システム部門などを対象に行った「2016年のセキュリティ事件に関する意識調査」を踏まえたもの。同調査は同社が毎年実施しているもので、2015年10月～2016年10月に発生したセキュリティ事案に対する認知度をランキング化した。

2016年の10大セキュリティ事件ランキング（マカフィー）

順位	セキュリティ事件（時期）	認知度（%）
1	振り込め詐欺／迷惑電話による被害（1年を通して）	51.7
2	大手金融機関やクレジットカード会社などをかたるフィッシング（1年を通して）	36.9
3	人気のPokemon GOをかたる偽アプリを発見（2016年7月）	35.8
4	公共無線LANのセキュリティ問題（1年を通して）	33.4
5	国際的ハッカー集団「アノニマス」による日本への攻撃（2015年10月～2016年2月）	28.9
6	米連邦捜査局（FBI）が米アップルに対して、銃乱射事件の犯人が使っていたiPhoneのロック解除を要請、プライバシーの問題に注目が集まる（2016年2月）	28.9
7	米ヤフーで、国家が関与するとみられるサイバー攻撃を2014年に受け、5億人以上の個人情報が流出（2016年9月）	28.9
8	JTBで、旅行商品をインターネット販売する子会社が標的型攻撃のメールからマルウェアに感染、最大約793万人分の個人情報が流出した可能性（2016年6月）	28.3
9	ランサムウェア（身代金ウイルス）の被害（1年を通して）	28.0
10	佐賀県で、県立学校の情報システムが不正アクセスを受け、個人情報を含むファイル約15万3000件が漏えい、17歳の少年が逮捕される（2016年6月）	21.6

intel Security

第3回「2016年のセキュリティ事件に関する意識調査」を実施　インテル セキュリティ、2016年の10大セキュリティ事件ランキングを発表

～ランサムウェアや大規模な情報流出など、個人や企業への攻撃が顕著に　デジタル経済を保護するサイバーセキュリティへの取り組みが必要な時代に～

2016年11月10日

インテル セキュリティ(日本での事業会社：マカフィー株式会社、所在地：東京都渋谷区、代表取締役社長：山野 修)は本日、日本国内の経営層や情報システム部門などのビジネスパーソンを対象に「2016年のセキュリティ事件に関する意識調査」を実施し、その結果を踏まえた2016年の10大セキュリティ事件を発表しました。

今年は、これまでの調査と同様に引き続き振り込め詐欺やフィッシングなど、身近なセキュリティの脅威が上位にランクインしたほか、昨年はTOP 10のランク外(17位)だったランサムウェアに関する被害が新たに9位に入り、人々のランサムウェアへの意識や関心が大きく高まっていることが明らかになりました。また、社会現象にもなったアプリ「ポケモンGO」の人気に便乗した偽アプリの発見が3位に入っており、人々の興味や関心を悪用したサイバー犯罪者の巧妙な手法がクローズアップされた結果となっています。そして、国際的ハッカー集団「アノニマス」による日本の空港、新聞社、官公庁などを標的とした攻撃や、国内大手旅行会社への標的型攻撃による大量の個人情報流出など、国境の無いサイバー空間で日本を標的とした攻撃がさらに厳しくなっている現状を反映した一年でした。インテル セキュリティでは、現在そして将来にわたって日本を狙うセキュリティ上の脅威は引き続き高まることが予想されるなか、脅威に対抗するためのセキュリティ人材の不足や、セキュリティに対する国民的なリテラシーの向上など、官民問わず一丸となった取り組みがこれまで以上に求められていると考えています。

●米Yahoo!、2013年に10億人分以上の個人情報流出

http://www.itmedia.co.jp/news/articles/1612/15/news089.html

このニュースをザックリ言うと・・・

- 12月14日（米国時間）、米Yahoo!社より、「Yahoo!」ユーザ10億人分以上の個人情報が2013年8月の攻撃によって盗まれていた可能性があると発表されました。

- 同社は9月22日にも「Yahoo!」ユーザ5億人分の個人情報が2014年の攻撃で流出していたと発表していますが（AUS便り 2016/09/26号参照）、今回はそれ以前に発生した攻撃によるものとなります。

- 流出した個人情報は、ユーザの名前・メールアドレス・電話番号・生年月日・ハッシュ化されたパスワードおよび秘密の質問と答え（一部ユーザ）とされ、ハッシュ化（元の値の推測が困難な形に変換）されていないパスワード・クレジットカード・銀行口座情報は含まれていないとのことです。

- なお、「Yahoo! JAPAN」については、日本のヤフー社により、前回同様影響はないと発表されています。

AUS便りからの所感等


ITmedia ニュース

米Yahoo!から10億人の情報流出　日本のヤフーは「現時点では影響なし」

米Yahooが、これまでに10億人以上のユーザーの個人情報が盗まれていたと発表した件について、日本のヤフーは、「現時点では影響はない」とコメントした。

[ITmedia]

米Yahoo!が12月14日（現地時間）、過去に受けたサイバー攻撃で10億人以上のユーザーの個人情報が盗まれていたと発表した件について、「Yahoo！JAPAN」を運営する日本のヤフーは、「現時点では影響はない」とコメントした。

米Yahoo!とYahoo！JAPANはシステムやサービスが異なるため、米Yahoo!の流出は、Yahoo！JAPANには「基本的には影響しない」という。

Yahoo! JAPAN @Yahoo_JAPAN_PR　フォローする

米ヤフーの情報流出について報道がされておりますが、Yahoo! JAPANへの影響はありません。
ご心配をおかけし、申し訳ございません。
2016年12月15日 14:08

- 前回発表分と重複（同じユーザの情報が2度流出）している可能性もありますが、合わせて延べ15億人分の個人情報が流出ということでインパクトは極めて大きく、ネット最大手サービスが如何に攻撃者にとって格好のターゲットかを物語っています。

- パスワードそのものは含まれていないものの、発表を見る限りでは、今日では脆弱であると指摘されているハッシュ化アルゴリズムを用いているとみられ、比較的現実的な時間で元のパスワードを割り出される可能性があります。

- Yahoo!でアカウントを登録していたユーザは、速やかにパスワードを変更することはもちろん、そこで使っていたパスワードを他のサービスで使い回していなかったか確認し、こちらについても必要に応じてパスワードを変更するようにしてください。

●「Apache HTTP Web Server 2.4」に複数の脆弱性、修正版のv2.4.25が公開

http://forest.watch.impress.co.jp/docs/news/1036332.html

このニュースをザックリ言うと・・・

- 12月20日（米国時間）、Apache Software Foundationより、世界で最も利用されているWebサーバソフトウェア「Apache HTTP Server(以下Apache)」の最新バージョン2.4.25がリリースされました。

- リリースの内容は5件の脆弱性の修正で、それらの脆弱性は、情報漏洩や意図しない外部リソースへのアクセス、サービス拒否(DoS)、リクエスト分割やキャッシュ汚染などを引き起こす恐れがあるとされています。

AUS便りからの所感等


窓の杜 WINDOWS FOREST

ニュース

「Apache HTTP Web Server 2.4」に複数の脆弱性、修正版のv2.4.25が公開

情報漏洩や意図しない外部リソースへのアクセス、DoSなどが引き起こされる恐れ

樽井 秀人　2016年12月21日 16:47

The Apache Software Foundationは20日、Webサーバーソフト「Apache HTTP Web Server」v2.4.25を公開した。本バージョンは現行の安定版v2.4.x系統の最新版で、CVE番号ベースで5件の脆弱性が修正されている。

"JVN"の脆弱性レポート（JVNVU#99304449）によると、これらの脆弱性は「Apache HTTP Web Server」v2.4.25より前のバージョンに影響し、情報漏洩や意図しない外部リソースへのアクセス、サービス運用妨害（DoS）、リクエスト分割やキャッシュ汚染などを引き起こす恐れがあるという。「Apache HTTP Web Server」を運用しているサーバー管理者は、早急に最新版へアップデートする必要がある。

なお、v2.4.24はリリースされなかったため、「Apache HTTP Web Server 2.4」の最新版はv2.4.25となっている。

The Apache Software Foundationのリリースページ

- Apacheの1.3系・2.0系は既にサポートが終了、2.2系についても今回のようなセキュリティリリースがまだありませんが、Apache 2.2系以前をソースからコンパイルしている場合、一部の脆弱性は2.2系以前では影響しない可能性があるものの、完全な対策や先進的な機能の活用のため、2.4系への移行を推奨致します。

- 一方、Linuxディストリビューションのパッケージから導入している場合、CentOS 6等ではApache 2.2系が引き続き使用され、2.4.25に適用されたセキュリティの修正が2.2系に独自に適用されることになりますが、それでも安定性を重視するならば、パッケージの更新を待つのが得策でしょう。

- 修正された脆弱性の中には、7月にCGIやPHPとの組合せにおいて問題になるとされた「httpoxy」が含まれますが（AUS便り 2016/07/25号参照）、設定により回避可能ですので、脆弱性を突かれる可能性があるか確認することを推奨致します。

- これらの修正版へのアップデートや回避策の適用は根本的対策のため決して欠かせないことですが、それまでに攻撃を受ける可能性を緩和するため、UTMやWAFの設置が一助となるでしょう。