— AUS（アルテミス・ユーザ・サポート）便り 2017/01/30号 —
http://www.artemis-jp.com

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。

●【注意喚起】日本語の件名･本文持つウイルスメール拡散中！

http://internet.watch.impress.co.jp/docs/news/1040885.html
https://twitter.com/MPD_koho

このニュースをザックリ言うと･･･

- 1月17日（日本時間）以降、警視庁のTwitterアカウントやJC3（日本サイバー犯罪対策センター：https://www.jc3.or.jp/topics/virusmail.html）より、日本語の件名・文章を持つウイルスメールが「拡散中！」だとして注意喚起が出されています。

- 1月17日に拡散が確認されたウイルスメールは、件名が「御請求書」「取引情報が更新されました」「【発注書受信】」「備品発注依頼書の送付」「依頼書を」「送付しますので」「発注依頼書」「（株）発注書」といったものとなっています。

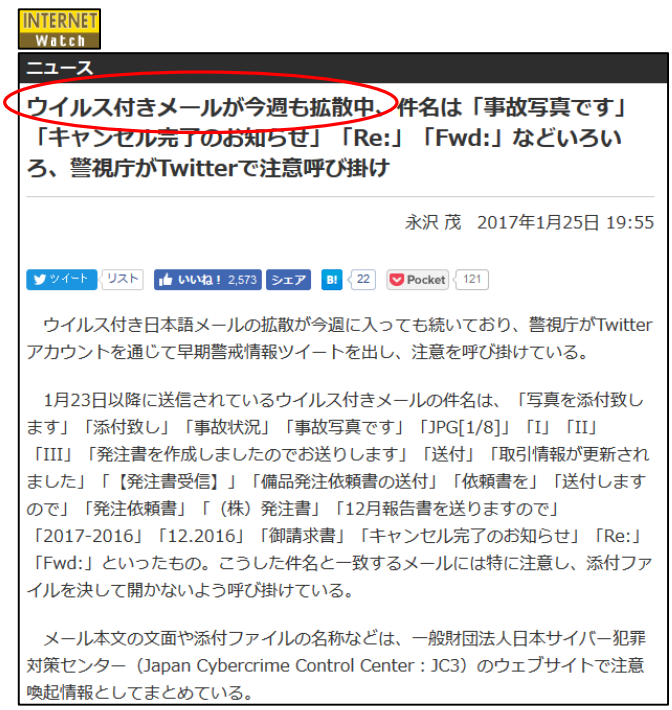
- また、1月23日以降には、新たに「写真を添付致します」「添付致し」「事故状況」「事故写真です」「JPG[1/8]」「I」「II」「III」「発注書を作成しましたのでお送りします」「送付」「12月報告書を送りますので」「2017-2016」「12.2016」「御請求書」「キャンセル完了のお知らせ」「Re:」「Fwd:」といった件名のものも確認されているとのことです。

- これらのウイルスメールは、国内インターネットバンキングの利用者を狙うマルウェア「URSNIF」への感染を目的としたものとされています。

AUS便りからの所感等

- この手のウイルスメールが外国語だったり、違和感のある片言の日本語だったりして見破りやすいものは今もありますが、もはやそれしかないという時代は終わったと言ってよいでしょう。

- とにかく最低限の基本として、アンチウイルスやUTMによる防御を行うこと、万が一の感染時の影響を最小限に抑えられるようシステム・ネットワークの見直しを行うこと、そして人間側の行動としても、「不審な添付ファイルやリンクは開かない」といったものに留まらない、安全なデータのやりとり等のルールを検討することが今後は重要となってくると考えられます。


INTERNET Watch

ニュース

ウイルス付きメールが今週も拡散中、件名は「事故写真です」「キャンセル完了のお知らせ」「Re:」「Fwd:」などいろいろ、警視庁がTwitterで注意呼び掛け

永沢 茂　2017年1月25日 19:55

ツイート　リスト　いいね！ 2,573　シェア　B!　22　Pocket　121

ウイルス付き日本語メールの拡散が今週に入っても続いており、警視庁がTwitterアカウントを通じて早期警戒情報ツイートを出し、注意を呼び掛けている。

1月23日以降に送信されているウイルス付きメールの件名は、「写真を添付致します」「添付致し」「事故状況」「事故写真です」「JPG[1/8]」「I」「II」「III」「発注書を作成しましたのでお送りします」「送付」「取引情報が更新されました」「【発注書受信】」「備品発注依頼書の送付」「依頼書を」「送付しますので」「発注依頼書」「（株）発注書」「12月報告書を送りますので」「2017-2016」「12.2016」「御請求書」「キャンセル完了のお知らせ」「Re:」「Fwd:」といったもの。こうした件名と一致するメールには特に注意し、添付ファイルを決して開かないよう呼び掛けている。

メール本文の文面や添付ファイルの名称などは、一般財団法人日本サイバー犯罪対策センター（Japan Cybercrime Control Center：JC3）のウェブサイトで注意喚起情報としてまとめている。


警視庁 広報

フォロー 5　フォロワー 60,086　いいね 3

ツイート　ツイートと返信　メディア

警視庁広報課さんがリツイート
警視庁犯罪抑止対策本部 @MPD_yokushi · 1月26日
【サイバー犯罪対策課】
ウイルス付メールが拡散中！件名は「キャンセル完了のお知らせ」。本文は添付書類の確認を求める内容となっていますが、添付ファイルは書類を装ったウイルスです。ご注意ください！
1　504　140

警視庁広報課さんがリツイート
警視庁犯罪抑止対策本部 @MPD_yokushi · 1月26日
【サイバー犯罪対策課】
ウイルス付メールが拡散中！件名は「Re:」「Fwd:」「FW:」。本文は添付写真等の確認や返信を求める内容となっていますが、添付ファイルは画像等を装ったウイルスです。ご注意ください！
2　513　148

警視庁広報課さんがリツイート
警視庁犯罪抑止対策本部 @MPD_yokushi · 1月25日
【サイバー犯罪対策課】
ウイルス付メールが拡散中！件名は「12月報告書を送りますので」「2017-2016」「12.2016」。本文は添付書類の確認を求める内容となっていますが、添付ファイルはエクセルファイルを装ったウイルスです。ご注意ください！
218　79

●Windows 7は現代のセキュリティ要件にこたえられない

http://news.mynavi.jp/news/2017/01/19/087/

このニュースをザックリ言うと・・・

- 1月27日（米国時間）、IT情報ブログExtremeTechにおいて、ドイツにおけるマイクロソフトのWindows担当責任者が「Windows 7に関してセキュリティパッチを当てていたとしても今後十分にセキュアであるとは言えない」とする警告が掲載されました。

- デスクトップOSとして依然48%のシェアを誇るWindows 7ですが、既に発売から7年が経過していることから、この担当責任者は「現代の技術の要求や企業のIT部門のセキュリティに対する高い要求にこたえることができない」と発言しているとのことです。

- Windows 7のサポート期限は2020年までとなっており、よりセキュアとされるWindows 10への移行がセキュリティ対策の重要なポイントとされています。

AUS便りからの所感等

- Windows 10のような新しいOSには、攻撃によって脆弱性を突かれた場合の影響を最小限に食い止めるなどの各種セキュリティ機能はもちろん、普段意識することがない機能を含め新しい機能が備わっており、OSのアップグレードにあたってはこれをうまく活用することにより、ネットワーク全体のセキュリティを高めることが期待できます。

- 一方で、使用しているソフトウェアが対応していない、または予算などの要因から、Windows 7どころかXPを使い続けている組織も少なからず存在しますが、XPは既にサポート期限が切れているため、これを用いているPCは可能な限りUTM等で隔離されたネットワーク上に配置すべきです。

マイナビニュース

Microsoft、「Windows 7は現代のセキュリティ要件にこたえられない」と警告

後藤大地
[2017/01/19]

ExtremeTechに1月17日(米国時間)に掲載された記事「Microsoft warns Windows 7 is dangerously insecure in 2017 - ExtremeTech」が、MicrosoftがWindows 7に関してセキュリティパッチを当てていたとしても今後十分にセキュアであるとは言えないと警告していることを伝えた。

同記事は、Microsoftドイツの Windows担当責任者のMarkus Nitschke氏が公式ブログへの投稿に基づくもの。Markus氏は「Windows 7は、現代の技術の要求や企業のIT部門のセキュリティに対する高い要求にこたえることができない」とコメントしている。

Windows 7は2009年に登場したデスクトップ向けのオペレーティングシステム。Net Applicationsの報告によれば、Windows 7のシェアは2016年12月の段階で48%以上を占めており、デスクトップ向けのオペレーティングシステムとしても最も高いシェアを確保している。

●IPA、Webサイトの脆弱性点検を呼び掛け　中国サイトに約400件の情報登録

http://www.itmedia.co.jp/enterprise/articles/1701/25/news107.html

このニュースをザックリ言うと・・・

- 1月25日（日本時間）、情報処理推進機構（IPA）より、WebサイトにおけるSQLインジェクション等の脆弱性についての点検と改修を行うよう注意喚起が出されました。

- IPAによれば、中国のセキュリティ情報サイトにおいて、SQLインジェクションの脆弱性があるとされた日本のWebサイトが約400件登録されていたとのことで、既にその過半数の248件について、管理者へ連絡を取っているとのことです。

- 特に、入力フォームを用意し、情報の収集の仕組みを設けている場合等は、個人情報を収集・管理していなくてもサイトの改ざん等の攻撃を受ける可能性があるとしています。

AUS便りからの所感等

- WordPressに代表されるCMS（コンテンツマネジメントシステム）等により、見栄えのするWebサイトの構築がより簡単に行えるようになりましたが、特に一旦作ったきりで更新しないケースがソフトウェアがアップデートされず脆弱性をはらんでいるという意味でも危険性が高いと考えられます。

- IPAでは「安全なウェブサイトの作り方」等、Webサイトの点検・改修それぞれにおいて有用な資料を公開しており、是非とも参照することを推奨致します。

- 併せて、WAF等の機能を備えたUTMの設置による攻撃への対処、あるいはどこかに問題がないか？ 改修は十分か？について、セキュリティ診断を受けることも重要です。

ITmedia エンタープライズ

2017年01月25日 16時40分 更新

IPA、Webサイトの脆弱性点検を呼び掛け　中国サイトに約400件の情報登録

SQLインジェクションの脆弱性が存在する約400サイトの情報が中国のポータルサイトに登録されていたといい、悪用の恐れもあることから緊急点検や改修の実施を呼び掛けている。

[ITmedia]

情報処理推進機構（IPA）は1月25日、Webサイト運営者などに対して脆弱性の点検や改修を速やかに実施してほしいと呼び掛けた。中国のポータルサイトに約400件の脆弱性を抱えるWebサイトの情報が登録されているといい、脆弱性の悪用による改ざんや情報流出などの恐れがあるとしている。

IPAによると、情報が登録されていたのは中国の脆弱性情報ポータルサイト「WooYun」で、2016年2月以降、国内の約400サイトの脆弱性が登録されていたことが分かった。同サイトは現在、閉鎖状態にあるという。