— ＡＵＳ（アルテミス・ユーザ・サポート）便り 2015/06/22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。

●サイバー攻撃調査をすぐにして――IPAが緊急提言

http://www.itmedia.co.jp/enterprise/articles/1506/03/news080.html
http://www.itmedia.co.jp/enterprise/articles/1506/11/news049.html
https://www.ipa.go.jp/security/ciadr/vul/20150602-secop.html

このニュースをザックリ言うと・・・

- 独立行政法人情報処理推進機構（IPA）が相次ぐ情報漏洩事件を受けて、6月2日および6月10日（ともに日本時間）に注意喚起を行っています。

- 2日の注意喚起では、多くのセキュリティ関連組織・企業が主張しているのと同様に「マルウェアに感染することを前提としたセキュリティ対策」そして「多層防御」を重要視しており、後者については「ウイルス感染リスクの低減」「重要業務を行う端末やネットワークの分離」「重要情報が保存されているサーバでの制限」「事後対応の準備」といったポイントを挙げています。

- 続く10日の注意喚起では、マルウェアの活動の痕跡を確認し、早期の検知と被害低減に取り組む必要があるとしており、活動痕跡確認のポイントとして「ファイアウォール、プロキシサーバの確認」「業務上想定していない通信の確認」「Active Directoryのログの確認」「Active Directoryサーバやファイルサーバなどの確認」を、また不審なログを発見した際の対応として「該当の端末のネットワークからの切り離し」「ファイアウォールやプロキシサーバでのブロック」「セキュリティベンダなどの専門家への相談」を挙げています。

AUS便りからの所感等

- 「感染しないこと」に重きを置く、あるいは「人間が注意すること」に頼った防御だけでは、いざそれが破られたときの漏洩の食い止めと早急な復旧を達成するのは難しく、マルウェアがどこでどう活動しているかを素早く検知できる体制はその意味でも重要となります。

- 個々のPCへのセキュリティソフトのインストールとUTMの導入は、マルウェアの内部での活動および外部への通信の検知をより迅速に行うことの一助になると言えるでしょう。


ITmedia エンタープライズ

2015年06月03日 12時14分 更新

マルウェア感染前提の対策と運用の徹底を（1/2）

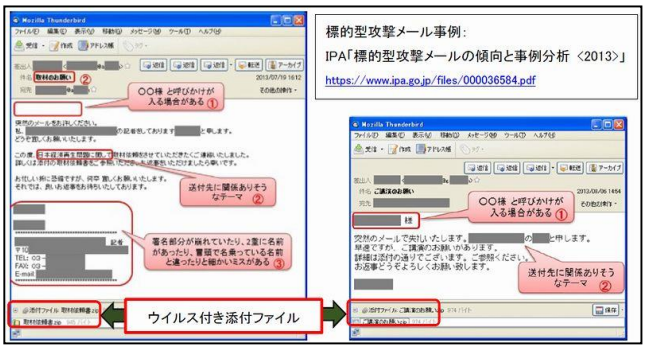
IPAは感染を防ぐだけでなく、感染したことによる被害を少なくするための対策とその運用の実施を改めて呼び掛けた。

[ITmedia]

印刷／PDF　ツイート 71　いいね！ 32　チェック　g+1 1　Pocket 16　通知

PR アプリ開発コンテストに応募して、Watson研究所へ行こう！
PR 福岡 大阪 名古屋開催：@IT・IIJ共催セキュリティイベント

マルウェアに感染することを想定した「多層防御」と運用管理が重要――。日本年金機構での個人情報漏えいが発生したばかりだが、情報処理推進機構（IPA）は6月2日、企業に対してセキュリティ対策とその運用管理を徹底することを呼び掛けた。複数の対策を組み合わせる「多層防御」を講じることで、マルウェア感染による被害を小さくすることが求められる。




ITmedia エンタープライズ

2015年06月11日 06時45分 更新

サイバー攻撃調査をすぐにして――IPAが緊急提言

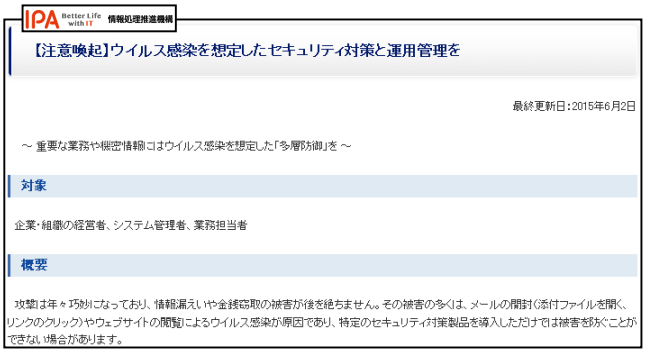
標的型サイバー攻撃被害を相次ぐ状況に、IPAが調査の実施を企業に求めている。

[ITmedia]

印刷／PDF　ツイート 155　いいね！ 350　チェック　g+1 4　Pocket 32　通知

PR アプリ開発コンテストに応募して、Watson研究所へ行こう！
PR 収集した大量データをセキュリティ対策にどう活かすのか？

国民年金機構や東京商工会議所などで標的型サイバー攻撃とみられる大規模な情報漏えい事案が相次ぐ事態を受け、情報処理推進機構（IPA）は、企業や組織にマルウェア活動の調査などサイバー攻撃への対応を急ぐよう呼び掛けた。攻撃の早期検知と被害低減への取り組みをシステム運用管理の定常業務に組み込んでほしいとしている。


IPA Better Life with IT 情報処理推進機構

【注意喚起】ウイルス感染を想定したセキュリティ対策と運用管理を

最終更新日：2015年6月2日

～ 重要な業務や機密情報にはウイルス感染を想定した「多層防御」を ～

対象

企業・組織の経営者、システム管理者、業務担当者

概要

攻撃は年々巧妙になっており、情報漏えいや金銭窃取の被害が後を絶ちません。その被害の多くは、メールの開封（添付ファイルを開く、リンクのクリック）やウェブサイトの閲覧によるウイルス感染が原因であり、特定のセキュリティ対策製品を導入しただけでは被害を防ぐことができない場合があります。

●石油連盟、上田市、協会けんぽ…マルウェア感染相次いで確認

http://www.yomiuri.co.jp/national/20150615-OYT1T50070.html
http://www.shinmai.co.jp/news/20150617/KT150616FTI090027000.php
http://www.itmedia.co.jp/news/articles/1506/18/news068.html

このニュースをザックリ言うと･･･

- 6月16日（日本時間、以下同様）、大手石油会社からなる石油連盟は、同5日に複数のPCがマルウェアに感染し、給湯器の補助金申請者およびアンケート回答者のべ約27,000人分の個人情報が流出した恐れがあると発表しました。

- 同15日には、長野県上田市は、市役所庁内ネットワークが標的型攻撃を受けてマルウェアに感染し、同日にネットワークをインターネットから遮断したことを発表しましたが、住民台帳等の基幹ネットワークとは分離されており、後者は元々インターネットに接続されていないことから、個人情報流出については確認されていない模様です。

- また同17日には、全国健康保険協会（協会けんぽ）の4台のPCがマルウェアに感染し、外部と不正な通信を行っていた可能性があると発表しましたが、個人情報流出の有無については調査中とのことです。

AUS便りからの所感等

- マルウェア感染被害とその報道が相次いでいますが、上田市のようにネットワークの適切な分離によって被害が最小限に抑えられているとみられるものもあり、被害の規模や個人情報・機密情報流出の有無にかかわらず、あらゆるケースが今後の対策の参考・教訓となり得ます。

YOMIURI ONLINE

石油連盟、PC感染で2万7千人分の情報流出か

2015年06月16日 07時24分　ツイート 15　おすすめ 12　g+1 2

石油元売り会社でつくる石油連盟（会長＝木村康・JX日鉱日石エネルギー会長）は15日、事務局の複数のパソコンがウイルスに感染し、給湯器の補助金を申請した人など2万7000人分余りの個人情報が流出した恐れがあると発表した。

- システム・ネットワークの構成が内部でのマルウェアの拡散や情報流出が容易となるものになっていないかの見直し、そして構成の変更にあたってはUTM等の導入が必要不可欠でしょう。

●メール誤送信、日本郵政から約7,500人分の個人情報が流出

http://itpro.nikkeibp.co.jp/atcl/news/15/061001955/
http://www.japanpost.jp/information/2015/20150610110867.html

このニュースをザックリ言うと･･･

- 6月10日（日本時間）、日本郵政株式会社は「建設工事発注情報メールサービス」登録者約7,500人分の個人情報（登録者名、メールアドレス、電話番号および住所）を誤って流出させたと発表しました。

- 流出が発生したのは同8日で、登録者情報データを添付したメールをサービス登録者に対し誤送信したとされており、同社では2時間後に当該メールの削除を依頼するメールを送信したとのことです。

AUS便りからの所感等

- メールによる誤送信のケースとしては、他にも同報メール送信時に送信先を「Bcc:」ではなく「Cc:」等で指定するといったものも古典的な例として知られます。

- 対策としては、メールサーバあるいはその前段のUTMにおいて、メールの誤送信の可能性があればその配信をストップして警告を返すといったシステムの構築が推奨されます。

JP 日本郵政 HOLDINGS

発表日：2015年6月10日

タイトル：建設工事情報発注メールサービス登録者情報の誤送信について

日本郵政株式会社

去る2015年6月8日に、弊社において建設工事発注情報提供先である建設工事発注情報メールサービス登録者の情報を誤送信していることが判明しました。
情報を適切に取り扱うべき事業者として、このような事態を招きましたことは、誠に申し訳なく、関係者の皆さまに深くお詫び申し上げます。
今後こうした事態が発生しないように、情報の管理を強化し、再発防止に努めてまいります。

ニュース　日経コンピュータ

日本郵政から約7500人分の個人情報が漏洩、メールサービス登録者全員に誤送信

2015/06/11
清嶋 直樹＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

133 おすすめ　15 共有　24 ブックマーク　48 Pocket　60 ツイート　シェア

日本郵政は2015年6月10日、個人情報約7500件を含む電子メールを誤送信していたことが判明したと発表した。6月8日に、「建設工事発注情報メールサービス」（画面）に登録している約7500人のメールアドレスに対し、同サービス登録者約7500人分の登録者名・メールアドレス・電話番号・住所を含むファイルを誤送付したという。日本郵政は2時間後に情報の削除を依頼するメールを送信した。

画面●日本郵政の「建設工事発注情報メールサービス」
［画像のクリックで拡大表示］