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。

●「流出を防げた可能性も...」年金情報流出事件の調査報告

http://www.nikkei.com/article/DGXLASDC20H04_Q5A820C1EA2000/
http://itpro.nikkeibp.co.jp/atcl/news/15/082002693/

このニュースをザックリ言うと･･･

- 8月20日（日本時間）、日本年金機構が5月に発生した年金情報125万件の流出事件に関する調査報告書を公表しました。

- 調査結果では、適切な判断次第で情報流出を防ぐことができたにも拘らず、判断を誤ってしまったケースが以下の例のように複数あったことを指摘しています。

① 5月8日および15日に攻撃メールによるマルウェア感染が発生した際、送信元のメールアドレスからの受信を拒否せず、また標的型攻撃ではないかとの疑いが組織として共有されなかった

② 5月18日に職員宛に99通の攻撃メールが届いた際、メールを受け取った各職員に対しメールの添付ファイルを開いたかを確認していなかった（ここで重要なサーバが乗っ取られたことが流出の重大なポイントとされています）

③ 5月21日～23日に計124通の攻撃メールが送られ、結果として年金情報の流出が発生した際、インターネットへの接続遮断等の対策が遅れた

- 年金加入者・受給者の個人情報流出については、当初公表された125万件以外に確認されていない一方、機構職員の個人情報225件、業務用のメールアドレス、および機構内の業務マニュアル等の流出が新たに発表されています。

AUS便りからの所感等

- たった1件のマルウェア感染から全ての問題につながったというものではなく、いくつもの細かい問題を解決しなかった結果が積み重なったことが今回の大規模な情報流出に発展したものと言えるようです。

- 公表された調査報告書をもとに、自組織においてセキュリティ侵害の進行を食い止めるために抑えておくべきいくつものポイントを洗い出し、それらを意識して行動することが肝要です。

- アンチウイルスやUTMの導入は、それらのポイントの中でも最も当然のように行っているべきことの一つでしょう。

日本経済新聞

年金情報「流出防げた」 機構が報告書、組織の問題指摘

2015/8/21 0:30

小 中 大 保存 印刷 リプリント 共有

日本年金機構は20日、サイバー攻撃を受けて125万件の個人情報が流出した問題の調査報告書を公表した。ウイルスメールを受信した後に適切な対応を取れば「流出を防げた可能性があった」と認め、幹部のリーダーシップ不足など前身の旧社会保険庁時代から続く組織の問題が対応不備の根底にあると総括した。ただ組織の改善が進むかどうかは不透明だ。

報告書によると、適切な対応をとれば機構が情報流出を防げた機会は少なくとも4回あった。

関係者を装う「標的型メール」が最初に届いた5月8日に端末1台が感染したが、機構は送信元のメールアドレスの受信拒否設定をせず、大規模攻撃を許す隙を生んだ。

同18日には職員に99通のウイルスメールが届き、19～20日も続いた。機構はメールが届いた職員に対してファイル開封を確認しなかった。これが報告書が感染拡大の「決定的な要因だった」と反省する2度目のミスだ。ここで情報系システムを一括管理する「認証サーバー」の管理者権限が盗まれた。

個人情報の流出は21日から23日の3日間に起きた。この間にも、不審な通信や機構全体のインターネット接続を遮断しないという3度目、4度目の判断ミスが起きた。

画像の拡大

記者会見する日本年金機構の水島藤一郎理事長(右)(20日午後、厚労省)

ニュース 日経コンピュータ

日本年金機構が調査結果発表、「流出防げた、断腸の思い」

2015/08/20

岡田 薫＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

145 おすすめ 6 共有 28 ブックマーク 37 Pocket 77 ツイート シェア

日本年金機構は2015年8月20日、標的型攻撃で125万件の年金情報が漏えいした問題について、調査結果を発表した。同日開かれた会見に臨んだ、日本年金機構の水島藤一郎理事長は「組織としての情報管理体制に問題があった。現場に対してルールを徹底できていなかった」と総括し、謝罪した（写真）。

写真●日本年金機構の水島藤一郎理事長

●ネット広告に潜伏、新ウイルス　世界で130万人感染

http://www.nikkei.com/article/DGXMZO90211800W5A800C1000000/

このニュースをザックリ言うと・・・

- 8月3日（現地時間）、サイバー攻撃対策サービスの米Trustwave社が新たなマルウェア開発キット「Rig 3.0」による広告を悪用した攻撃の兆候を確認したとして注意を呼びかけています。

- 攻撃者はオークションによって買い付けた広告枠で、Rig 3.0が埋め込まれた広告を配信するという手口をとっており、最悪の場合、不正な広告がブラウザに表示されるだけでマルウェアに感染する可能性があるとしています。

- 同社の研究チームによれば、6週間でRig 3.0が埋め込まれた広告は350万人のユーザに対して配信され、うち4割弱にあたる130万人についてマルウェアの感染が確認された模様です。

AUS便りからの所感等

- 用いられるツールによる攻撃の多くは Flash Player・Javaといったプラグインの既知の脆弱性を突くものであるため、OSを含めたPC上の各種ソフトウェア（Office等含む）を常に最新に保つことが根本的な対策となり、また、ブラウザや拡張による広告のブロック、あるいは広告がクリックしないと再生されないようブラウザのプラグイン設定を行うことも効果的です。

- 一方で未修正の脆弱性を突くケースも少なからず存在しますので、こういった攻撃から可能な限りPCを防衛するため、アンチウイルス・UTMの導入が重要な役割を果たすことでしょう。

日本経済新聞

ネット広告に潜伏、新ウイルス　世界で130万人感染

2015/8/7 6:30

小 中 大　保存　印刷　リプリント　▼共有

VB

サイバー攻撃対策サービスの米トラストウエーブの研究チームは、ハッカーがコンピューターウイルスに感染させる広告を表示するために利用している「エクスプロイトキット」（脆弱性攻撃ツール）の新たなバージョンを発見した。

■いつも見ているサイトの広告で感染

ハッカーはまず、オークション方式で実施されるリアルタイム取引でネットの広告枠を買い付ける（編集部注：この仕組みをプログラマティックバイイングと呼ぶ）。それから、コンピューターの脆弱性を判別する攻撃ツール「リグ3.0」をその広告に埋め込んで「トロイの木馬」タイプのウイルスを仕掛ける。すると、脆弱なコンピューターの持ち主は不正広告をクリックしなくても、ページを見ただけでトロイの木馬をダウンロードしてしまう。つまり、大部分の人は手遅れになるまで感染していることに気付かない。

●Windows 10便乗のランサムウェア、アップグレードに見せかけ身代金要求

http://www.itmedia.co.jp/enterprise/articles/1508/03/news040.html

このニュースをザックリ言うと・・・

- 7月31日（現地時間）、大手ネットワーク機器ベンダーの米Cisco Systems社は、同29日にリリースされた「Windows 10」に便乗し、ランサムウェア（感染したPCのファイルを人質に金銭等を要求するマルウェア）への感染を仕向けるメールが出回っていると同社ブログで発表しました。

- メールは「Windows 10 Free Update」という件名でMicrosoftからのものに偽装していますが、ヘッダ情報から、タイのIPアドレスから送信されているとみられています。

- アップグレードのための実行ファイルを装ったメールの添付ファイルを実行することにより、ランサムウェア「CTB-Locker」に感染してPC上のファイルを暗号化し、96時間以内に暗号化解除のための身代金を支払うよう要求する仕組みになっているとのことです。

AUS便りからの所感等

- Windows 10の登場はIT業界における大きなイベントであり、しばらくはこれに便乗した様々な攻撃が行われると考えられます。

- こういった攻撃からの防御のためにも、アンチウイルスあるいはUTMの導入は必須でしょう。

- また、Microsoftがこういったアップグレードのためのプログラムをメールで配布することは通常考えられないことを認識し、慎重な行動をとることも求められます。

ITmedia エンタープライズ

Windows 10便乗のランサムウェア、アップグレードに見せかけ身代金要求

Microsoftからの正規メールに見せかけた内容に騙されて添付ファイルをクリックするとランサムウェアに感染し、身代金を要求される。

[鈴木聖子, ITmedia]

印刷／PDF　ツイート 128　いいね！ 255　チェック　0　Pocket 17　通知

PR 営業支援システムを開発したい。外注先を探すならコチラ

PR SAP製品は弊社には「高嶺の花」だと思ってました。

米Microsoftが29日にリリースした「Windows 10」に便乗し、ユーザーのファイルを人質に取って身代金を要求するランサムウェアに感染させようとするメールが出回っているという。米Cisco Systemsが7月31日のブログで伝えた。

それによると、問題のメールは英語で「Windows 10 Free Update」という件名が付いている。送信元は偽造され、Microsoftから届いた正規メールのように見せかけてある。ただしヘッダを調べると、送信元のIPアドレスがタイにあることが分かるという。