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。

●年金情報125万件が漏洩、PCのマルウェア感染により発生（その①）

緊急特集!!

http://itpro.nikkeibp.co.jp/atcl/news/15/060101820/
http://mainichi.jp/select/news/20150602k0000m040117000c.html

このニュースをザックリ言うと･･･

- 6月1日（日本時間）、日本年金機構が標的型サイバー攻撃を受け、約125万件の年金情報（加入者の年金番号・氏名・生年月日および住所）が流出したと発表されました。

- 少なくとも5月8日から18日にかけて攻撃者からのメールが同機構職員あてに送信され、複数の職員がメールの添付ファイルを開いたことによりPCがマルウェアに感染、結果として、PC上に保存されていた情報および同一LAN上からアクセス可能だった共有サーバに保存されていた情報が流出したとされています。

- マルウェアが添付されたメールには「『厚生年金基金制度の見直しについて（試案）』に関する意見」といった件名が記されている等、本物のメールに極めて巧妙に似せた内容となっていたとされています。

- 流出した情報は、本来は暗号化された状態でCD-ROMに格納されて渡されており、個人情報を記録したファイルにはパスワードを設定するという内規があったにもかかわらず、前述のとおり共有サーバ等に情報が保存されていたこと、また約55万件の情報についてはパスワードが設定されていなかったこと等の運用上の問題も明らかになっています。

AUS便りからの所感等

- 本年10月より施行、来年1月より運用開始される社会保障･税番号（マイナンバー）制度について、政府は今回の事件が影響することを否定してはいるものの、マイナンバーを発行する側以上に発行された側から託されて管理する企業側にとって、今後の運用に大きく影響する事件であるでしょう。

- 特にこういった標的型攻撃に対しては、もはや各ユーザのリテラシーに依存するのみでは限界という意見も巷では多く、ユーザが悪意のあるメールや添付ファイルを開いてしまい、PCがマルウェアに感染してしまう可能性があることを前提として、感染したPCを介して機密情報が流出される等の被害を最小限に抑えるための対策を考えなければならない時期に来ていると言えます。

- 外部からのマルウェアの侵入だけでなく、マルウェアに感染した場合における、内部の重要なサーバおよび外部の攻撃者のサーバとの通信をも確実に遮断するよう、UTM等の機能をフル活用すること、さらには真に重要な情報にLAN経由でアクセスさせないこと等も考慮したシステム・ネットワーク構成の見直しを行うことも考慮すべきでしょう。

ニュース　日経コンピュータ

日本年金機構にサイバー攻撃、ファイル共有サーバーから125万件の年金情報が流出

2015/06/01
井上 英明＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

1,961　102　216　177　2,722
おすすめ　共有　ブックマーク　Pocket　ツイート
シェア

日本年金機構は2015年6月1日、サイバー攻撃により約125万件の年金情報が流出したと公表した。特定の企業や団体から機密情報を盗み出す標的型サイバー攻撃に遭ったと見られる。通常は基幹システムで管理する個人情報をファイル共有サーバーに移したところ、ウイルスに感染したパソコン経由で流出したという。

年金情報流出:内規違反　55万件にパスワード設定されず

毎日新聞　2015年06月01日　23時42分（最終更新　06月02日　08時17分）

個人情報流出を受けた記者会見をする日本年金機構の水島藤一郎理事長＝厚労省で2015年6月1日午後5時2分、小出洋平撮影

拡大写真

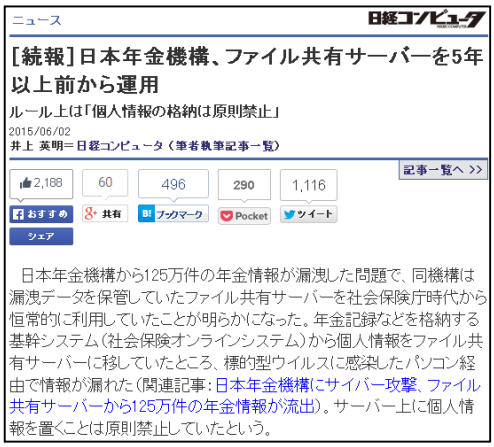
◇日本年金機構、外部流出は計125万件を発表

日本年金機構は1日、職員のパソコンに外部からウイルスメールによる不正アクセスがあり、機構が保有する国民年金や厚生年金などの加入者と受給者の個人情報が外部に流出したと発表した。機構によると、国民年金、厚生年金などの加入者に付与される10桁の基礎年金番号と氏名、生年月日の3情報が約116万7000件▽3情報と住所の計4情報が約5万2000件▽基礎年金番号と氏名の2情報が約3万1000件――の計約125万件に上るとみられる。相談を受けた警視庁は不正指令電磁的記録（ウイルス）供用容疑などにあたる可能性があるとみて捜査を始めた。

●年金情報125万件が漏洩、PCのマルウェア感染により発生（その②）

緊急特集!!

http://www3.nhk.or.jp/news/html/20150601/k10010099511000.html
http://itpro.nikkeibp.co.jp/atcl/news/15/060201844/
http://www3.nhk.or.jp/news/html/20150604/k10010102751000.html



ニュース　日経コンピュータ

[続報]日本年金機構、ファイル共有サーバーを5年以上前から運用

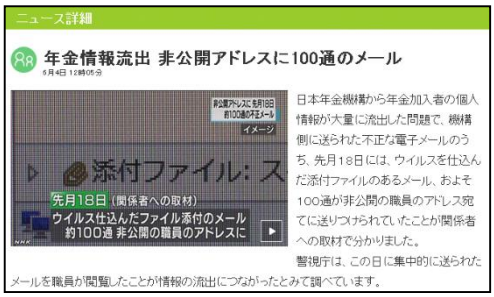
ルール上は「個人情報の格納は原則禁止」

2015/06/02
井上 英明＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

2,188　60　496　290　1,116
おすすめ　共有　ブックマーク　Pocket　ツイート
シェア

日本年金機構から125万件の年金情報が漏洩した問題で、同機構は漏洩データを保管していたファイル共有サーバーを社会保険庁時代から恒常的に利用していたことが明らかになった。年金記録などを格納する基幹システム（社会保険オンラインシステム）から個人情報をファイル共有サーバーに移していたところ、標的型ウイルスに感染したパソコン経由で情報が漏れた（関連記事：日本年金機構にサイバー攻撃、ファイル共有サーバーから125万件の年金情報が流出）。サーバー上に個人情報を置くことは原則禁止していたという。



ニュース詳細

年金情報流出 非公開アドレスに100通のメール
5月4日 12時05分

日本年金機構から年金加入者の個人情報が大量に流出した問題で、機構側に送られた不正な電子メールのうち、先月18日には、ウイルスを仕込んだ添付ファイルのあるメール、およそ100通が非公開の職員のアドレス宛てに送りつけられていたことが関係者への取材で分かりました。

警視庁は、この日に集中的に送られたメールを職員が閲覧したことが情報の流出につながったとみて調べています。

専門家「過去にない被害レベル」

情報セキュリティに詳しい立命館大学の上原哲太郎教授は、今回の情報流出について「国の機関から国民の情報が流出した事案としては過去最大規模で、内容も、住民基本台帳で扱う住所や名前などの4情報より機密度が一段高いレベルのものが流出したとみるべきだ」と指摘しています。

上原教授は「年金事務所で作業のために一時的にシステムから引き出した情報を、作業の終了後も放置していたために起きたのではないか」と分析していて、こうした作業を行う端末がインターネットと接続できる環境にあったことも大きな問題だと指摘しています。

上原教授は、こうした被害を防ぐためには、個人情報を扱う端末とインターネットを接続する端末とを分けること、それに、一度取り出した情報は確実に消すことが重要だと話しています。そのうえで、日本に住む人すべてに12桁の番号を割りふるマイナンバー制度にも影響は避けられないとしていて「新たな制度では、マイナンバーにさまざまな情報をひもづけて管理するためそうした情報の取り扱いや対策を見直す必要が生じる可能性がある」と述べています。

不正メールの内容は

関係者によりますと、送りつけられたメールのタイトルは、「厚生年金基金制度の見直しについて（試案）」に関する意見、給付研究委員会オープンセミナーのご案内、厚生年金徴収関係研修資料、医療費通知、の4種類だったということです。

また、送信元のフリーメールのアドレスも4種類あり、いずれも無料で取得できるものだったということです。

このうち、先月8日に送りつけられたメールは、「『厚生年金基金制度の見直しについて（試案）』に関する意見」のタイトルでメールの本文には外部リンクのアドレスが記されていて、クリックするとウイルスに感染する仕組みになっていました。

不正なメールは、4種類のタイトルと4種類のアドレスを組み替えるなどして、少なくとも5種類あったということです。

●警視庁、ロジテック製無線LANルータへの攻撃を確認

http://news.mynavi.jp/news/2015/06/02/290/
http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku505.htm

このニュースをザックリ言うと・・・

- 6月2日（日本時間）、警視庁サイバー犯罪対策課がロジテック製無線LANルータ3製品のファームウェアの脆弱性を突いた攻撃を確認したとして警告しています。

- 問題が確認された製品は「LAN-W300N/R」「LAN-W300N/RS」「LAN-W300N/RU2」でシリアルナンバー(製造番号)の末尾が「B」かつファームウェアのバージョンが「2.71」のものとなっており、脆弱性を突かれることにより、ルータがISPに接続するためのPPPoE情報を奪取される可能性が指摘されています。

- ロジテック社では2012年にファームウェアの修正版を公開済みでしたが、今回の発表を受けて改めて修正版の適用を呼びかけています。

AUS便りからの所感等

- PPPoE情報の奪取により、他者が契約したISP接続契約を勝手に利用される恐れがあります。

- PCと比べ、ルータ等のネットワーク機器のファームウェアは顧みられることが少ない傾向にあり、重要なアップデートが行われないケースも珍しくありません。

- 組織内で利用しているネットワーク機器のメーカー・機種を十分に把握し、またメーカーからのファームウェアリリース情報を確実に入手し、速やかにアップデートを行う運用を確立させることは、ネットワーク全体のセキュリティを確保するためにも欠かせないことと言えます。

左から、LAN-W300N/R、LAN-W300N/RS、LAN-W300N/RU2