— AUS（アルテミス・ユーザ・サポート）便り 2016/06/13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。

●福井・池田町議会PCからデータ流出か･･･アダルトサイト閲覧、警告に騙されて遠隔操作ソフトをインストール

http://www.chunichi.co.jp/s/article/20160604902218O6.html
https://www.town.ikeda.fukui.jp/toplink/emergency/p002265.html

このニュースをザックリ言うと･･･

- 6月4日（日本時間）、福井県池田町は、同町議会事務局の業務用PCが乗っ取られ、議会関係のデータが抜き取られた可能性があると発表しました。

- 発表によれば、議会事務局長が同3日にPCでアダルトサイトにアクセスし、その際、画面に「あなたのパソコンはウイルスに感染しています」というメッセージと電話番号が表示されたことからその番号に電話、相手の指示に従うまま、遠隔操作ソフトウェアをインストールしたとのことです。

- PCに入っていたのは議員の個人情報や議案等の公開データがほとんどとされ、他のPCへの侵入は確認されていないとのことですが、同町では福井県警と連携して抜き取られたとみられるデータについて調査中です。

AUS便りからの所感等

- 今回の事件では、「業務に関係ないサイトの閲覧をする」「メッセージに騙されて電話をかける」「そして指示に従って不正なソフトウェアをインストールしてしまう」という風に、PCの乗っ取りに至るまでには複数の重大なミスが重なって起こっています。

- そもそも、メッセージは広告に表示された単なる「ハッタリ」だった可能性、その段階ではウイルスに感染していなかった可能性も考えられます（ただし、アドウェア等がインストールされた結果、ブラウザに表示される広告が差し替えられるケースも珍しくなく、注意が必要です）。

- ともあれ、単にアンチウイルスとUTMによる防御のみならず、各段階でマルウェア感染等の事態に陥らないよう、システムの利用・ネットへのアクセス等にあたっての十分なセキュリティ教育を行い、PCが不審な動きをした等の場合には、誤った知識のもとで事態を悪化させるような勝手な行動をとらず速やかにセキュリティ担当者に連絡する、といったルール作りを徹底すべきでしょう。

中日新聞 CHUNICHI Web

ツイート B! 727 シェア 2559 G+1 53　2016年6月4日 22時18分

ＡＶ閲覧しＰＣ乗っ取られる　福井、池田町議会事務局

福井県池田町は４日、「議会事務局のパソコンが乗っ取られ、議会関係のデータを抜き取られた可能性がある」と発表した。議会事務局長の５０代男性がアダルトサイトを閲覧し、遠隔操作されたという。県警もファイルの流出がないかを調べている。

町によると、事務局長は３日にアダルトサイトを複数回閲覧。画面に「あなたのパソコンはウイルスに感染しています」とのメッセージと、連絡先として「０５０」で始まる電話番号が表示された。

事務局長はこの番号に電話し、片言の日本語を話す男の声による指示通りにパソコンを操作して、遠隔操作ファイルをインストール。約１時間半にわたって電話がつながった状態で遠隔操作される状況を見ていたという。

町によると、このパソコンに入っていたのは、議員の個人情報や議案など一般に公開しているデータがほとんどだが、流出すると問題となるファイルが入っていた可能性も否定できないという。今のところ役場に６０台ほどある他のパソコンへの侵入などは確認されていない。

杉本博文町長と佐野和彦町議長は４日、連名の文書で謝罪した。事務局長は「不適切なサイトを閲覧したうえ、その後の対応も誤り、反省している」と話しているという。

福井県 池田町

役場職員のパソコンが乗っ取られる事象の発生について（お詫び）

最終更新日 2016年6月4日 | ページID 002265 | 印刷

いいね！ 10 ツイート

6月3日金曜日、午後3時ごろ、役場職員のパソコンが遠隔操作により乗っ取られ、データが抜き取られたと思われる事象が発生いたしました。抜き取られた情報の詳細については、現在調査中です。なお、役場内のほかのパソコン及びシステムへの影響はない模様です。住民の皆様をはじめ、池田町にかかわりのある皆様におかれましては、非常に不安とご迷惑をおかけいたしますこと、深くお詫び申し上げます。詳細については、現在、福井県警で調査中です。詳細が分かり次第、ただちにご報告いたします。

事件の経緯

- 日時：平成28年6月3日（金）午後3時ごろ
- 内容：議会事務局のパソコンのデータが外部に抜き取られる。
- 対応状況：福井県警にパソコンを提出し、状況を調査中
- 原因：業務に関係のないサイトを閲覧した可能性が考えられる。
- 被害の状況
  現在のところ、抜き取られた情報は、議会関係のデータと想定される。
  詳細は福井県警にて調査中。

今後の対応

福井県や福井県警と協議の上対応いたします。漏えいした情報の範囲と内容を確認の上、関係者にご説明とお詫びをいたします。また、このことについて、被害届を提出いたします。

●電通大に不正アクセス、フィッシングメール280万件送信

http://www.itmedia.co.jp/news/articles/1606/06/news109.html

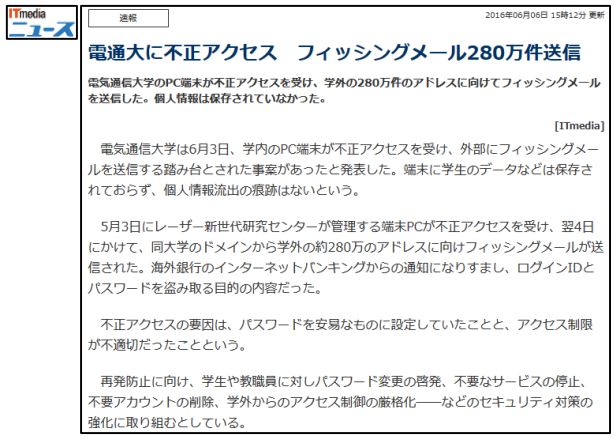
このニュースをザックリ言うと･･･

- 6月3日（日本時間）、電気通信大学（電通大）は、同大学の研究室が管理するPCから学外の約280万のメールアドレスに対しフィッシングメールが送信されたことを発表しました。

- 発表によれば、PCは5月3日に不正アクセスを受け、以後同4日までの間、海外銀行のインターネットバンキングからの通知（を装いフィッシングサイトへ誘導する）メールが送信されていたとのことです。

- なお、PCには学生のデータ等の個人情報は格納されておらず、流出の痕跡はなかったとされています。

- 同大学では、不正アクセスが発生した要因として「パスワードを安易なものに設定していたこと」「アクセス制限が不適切だったこと」を挙げており、再発防止に向け「全学生・教職員に対しパスワード変更の啓発」「不要なサービスの停止」「不要アカウントの削除」「学外からのアクセス制御の厳格化」等セキュリティ対策の強化に取り組むとしています。



ITmedia ニュース

速報

2016年06月06日 15時12分 更新

電通大に不正アクセス　フィッシングメール280万件送信

電気通信大学のPC端末が不正アクセスを受け、学外の280万件のアドレスに向けてフィッシングメールを送信した。個人情報は保存されていなかった。

[ITmedia]

電気通信大学は6月3日、学内のPC端末が不正アクセスを受け、外部にフィッシングメールを送信する踏み台とされた事案があったと発表した。端末に学生のデータなどは保存されておらず、個人情報流出の痕跡はないという。

5月3日にレーザー新世代研究センターが管理する端末PCが不正アクセスを受け、翌4日にかけて、同大学のドメインから学外の約280万のアドレスに向けフィッシングメールが送信された。海外銀行のインターネットバンキングからの通知になりすまし、ログインIDとパスワードを盗み取る目的の内容だった。

不正アクセスの要因は、パスワードを安易なものに設定していたことと、アクセス制限が不適切だったことという。

再発防止に向け、学生や教職員に対しパスワード変更の啓発、不要なサービスの停止、不要アカウントの削除、学外からのアクセス制御の厳格化――などのセキュリティ対策の強化に取り組むとしている。

AUS便りからの所感等

- 同大学が挙げたセキュリティ対策の取り組みは、いずれも「外部からの侵入防止」を念頭に置いた基礎的な項目であり、各組織において十分に実施されているか、今一度見直しを行うべきです。

- 一方で、「ひとたび侵入されてしまった後」における、内部からの不審なメールの大量送信あるいは外部サイトへの不審なアクセス等についても対策を怠ってはならず、UTMをはじめとするネットワーク機器の設置と適切な設定がこういった「出口対策」についても一助となってくれるでしょう。

●Facebook創業者、Twitter等のアカウントを乗っ取られる

http://www.itmedia.co.jp/enterprise/articles/1606/07/news063.html

このニュースをザックリ言うと･･･

- 6月5日（米国時間）、大手SNS「Facebook」創業者のマーク・ザッカーバーグ氏がTwitter等の別のSNSに登録していたアカウントを乗っ取られた、と米国のメディアが報じました。

- 報道によれば、「OurMine Team」を名乗る集団が同氏のTwitterやPinterestおよびFacebook傘下のInstagramのアカウントに侵入したと宣言し、TwitterおよびPinterestにて不正な投稿を行った模様です。

- 後に不正な投稿とOurMine TeamのTwitterアカウントは削除されており、また後日Facebookからの発表では、Instagramのアカウントについては侵入されていなかったとのことです。

ITmedia エンタープライズ

2016年06月07日 07時13分 更新

ザッカーバーグ氏のSNSアカウントに不正侵入、LinkedInのパスワード流出に関連か

ザッカーバーグ氏のTwitterやPinterestのアカウントが何者かに侵入され、不正な投稿を掲載される被害に遭った。

[鈴木聖子，ITmedia]

マーク・ザッカーバーグ氏（Facebookより）

米Facebookのマーク・ザッカーバーグ最高経営責任者（CEO）が使っていたTwitterなどのパスワードが何者かに盗まれ、アカウントが荒らされる事件が起きた。メディア各社が6月5日に伝えた。

報道によると「OurMine Team」を名乗る集団がTwitterで、ザッカーバーグ氏のTwitterやPinterest、Facebook傘下のInstagramのアカウントに侵入したと公言した。LinkedInから流出したユーザーの個人情報の中に、ザッカーバーグ氏のパスワードがあったとしている。

ザッカーバーグ氏のTwitterのアカウント（@finkd）とPinterestのアカウント（zuck）には、相次いで不正な投稿が掲載された。同氏が使っていたとされる安易なパスワードをあざけるような内容もあった。Twitterで被害に遭ったのはザッカーバーグ氏が2012年1月以来、使っていなかったアカウントだった。

AUS便りからの所感等

- アカウント乗っ取りを行った「OurMine Team」はザッカーバーグ氏のアカウントのパスワードを別のSNS「LinkedIn」の流出したアカウント情報から見つけたと発言しており、同氏が複数のアカウントでパスワードの使い回しを行っていた可能性が考えられます。

- 6月に入り、いくつかのSNSにおいて、不正アクセスによる大量のアカウント情報の流出も報じられており、これらのアカウント情報もアングラ等で流通し、パスワードを使い回しているユーザを狙うさらなる情報源として利用されることでしょう。

- ザッカーバーグ氏のようなIT業界の著名人がアカウント乗っ取りの被害を受けたことを一つの機会として、「推測されにくい、かつサービス毎に少しでも異なるパスワードを用いる」という鉄則を今一度啓発していくことが肝要です。