— AUS（アルテミス・ユーザ・サポート）便り 2016/07/04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。

●NTT東西の「ひかり電話ルータ」に脆弱性･･･ルータ上で不正なコマンド実行等の恐れ

http://internet.watch.impress.co.jp/docs/news/1007288.html
https://jvn.jp/jp/JVN77403442/
http://web116.jp/ced/support/news/contents/2016/20160627.html

このニュースをザックリ言うと･･･

- 6月27日（日本時間）、NTT東日本・西日本が提供する「ひかり電話」用機器「ひかり電話ルータ」に脆弱性が存在するとして、独立行政法人情報処理推進機構（IPA）および一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）から発表がありました。

- 対象機器は、PR-400MI（単体型）、RT-400MI（ONU一体型）、RV-440MI（VDSL一体型）の3機種となっています。

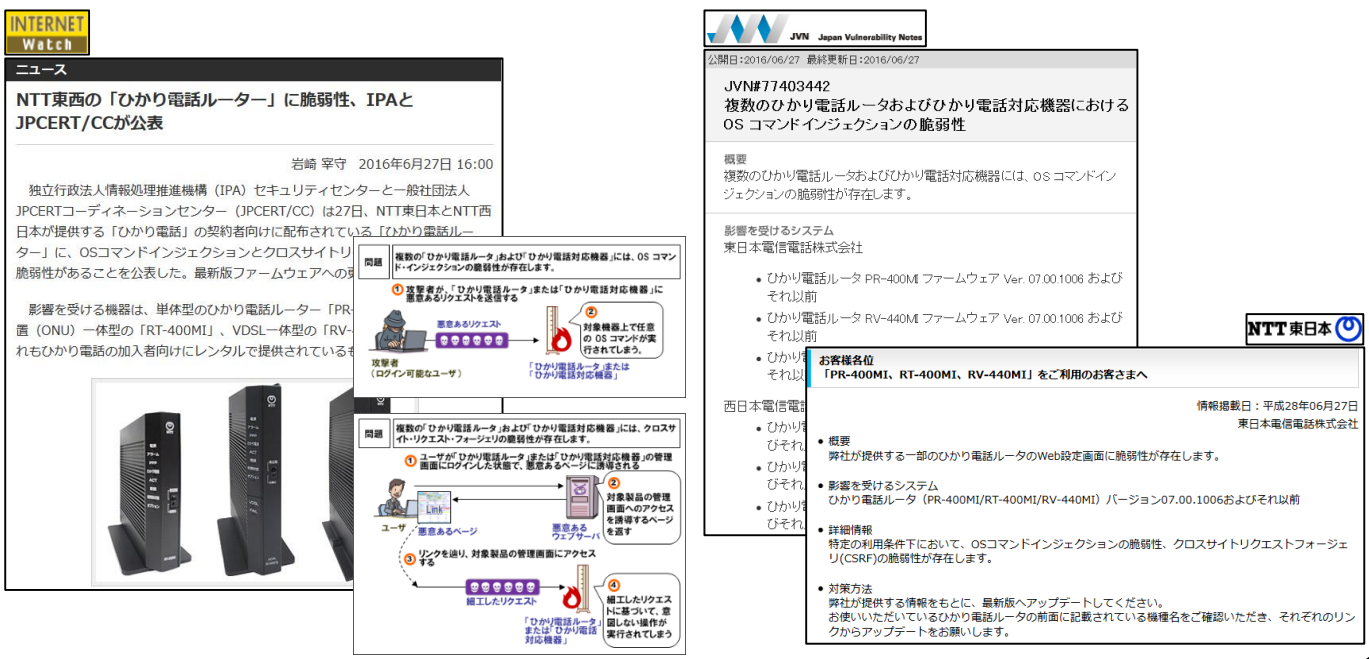
- 脆弱性を突くことにより、攻撃者に機器を乗っ取られる等の恐れがあり、ファームウェアをアップデートするよう推奨されています。

AUS便りからの所感等

- 今回問題とされた脆弱性はいわゆる「OSコマンドインジェクション」と言われるもので、主にWebアプリケーションに存在する脆弱性を突くことにより、OS上で任意の不正なコマンドを実行することが可能になるものです。

- もう一つの脆弱性として「クロスサイトリクエストフォージェリ(CSRF)」も報告されており、ルータの管理者を不正なページに誘導することにより、攻撃者が指定した不正な設定をその管理者権限で強制的に実行させられる恐れがあるとされており、管理者にとっての回避策としては、管理画面での作業が終わったら確実にログアウトすることが挙げられます。

- ルータ等ネットワーク機器のファームウェアについては、アップデートが見落とされる可能性が高く、情報資産管理の視点からも、全ての機器について欠かさずアップデートが行われているかに十分注意してください。



●ヤマト運輸を装った不審メール出回る･･･添付ファイルを開かないよう注意

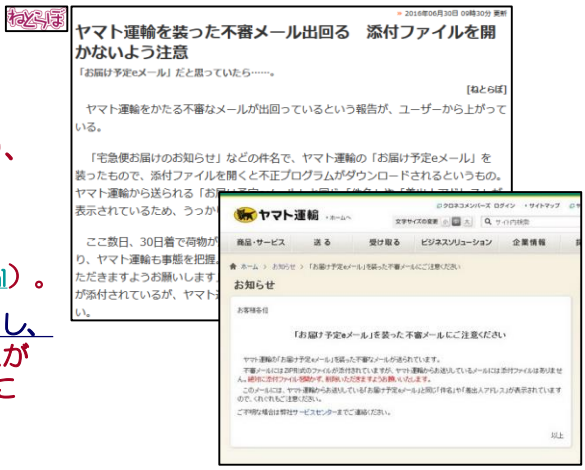
http://nlab.itmedia.co.jp/nl/articles/1606/30/news081.html

このニュースをザックリ言うと･･･

- 6月29日（日本時間）、ヤマト運輸より、同社を騙る不審なメールが出回っているとして注意が呼び掛けられています。

- 問題のメールは同社サービス「お届け予定eメール」を装ったものとされ、送信者アドレス（From:）が「@kuronekoyamato.co.jp」等、件名（Subject:）が「宅急便お届けのお知らせ」等となっている点、および文面は本物に似せていますが、マルウェア入りのZIPファイルが添付されているのが特徴です。

- 同社では、「実際に送信するメールにファイルが添付されることはない」として、絶対に添付ファイルを開かず、削除するよう警告しています。



AUS便りからの所感等

- 大手業者のネットサービスになりすましてのメール送信については、マルウェアの拡散手段としてポピュラーなものであり、3月には日本郵政を騙るメールも出回っています。（AUS便り2016/02/22号参照。
なお6月7日には日本郵政が同様の注意喚起を行っています：
http://www.post.japanpost.jp/notification/notice/2016/0607_01.html）。

- メールの送信者アドレス等は改ざんが容易で、メーラーで表示し、差出人や文面を見て判断するのは危険であり、発信元IPアドレスが本物かどうか等をUTMその他により機械的にチェックするようにしてください。

●佐賀県学校教育ネットワークに不正アクセス、少年逮捕へ

http://itpro.nikkeibp.co.jp/atcl/ncd/14/457163/062801558/

このニュースをザックリ言うと･･･

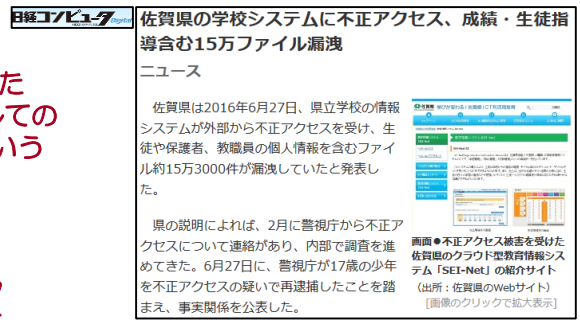
- 6月27日（日本時間）、佐賀県より、同県の学校教育ネットワークに対する不正アクセスがあったと発表があり、同日17歳の少年が不正アクセス禁止法違反容疑で逮捕されました。

- 発表によれば、被害を受けたのは県教育委員会の教育情報システム「SEI-Net」や県立の学校の校内LAN上にある「校務用サーバ」等で、影響を受けた学校は9校にのぼるとされており、2月15日に警視庁から連絡を受けたことから発覚したとしています。

- 不正アクセスを行ったとされる少年は、テレビの有料放送を無料視聴するための不正プログラムを配布した容疑で既に逮捕されており、押収されたPCからは現時点で生徒・保護者・教職員9589人分の個人情報等を含む約21万ファイルが確認されている模様です。

- 不正アクセスは警視庁から連絡がある前、少なくとも2015年4月以降には少年を含む複数名のグループで行われていた模様で、また、学内向け無線LANに校外からアクセスして校内LANに侵入したとされています。

AUS便りからの所感等



- 佐賀県は全国に先駆けて学校等教育システムのIT化を進めてきたことが度々ニュースになっていましたが、一方で電子教科書としてのタブレットPCの導入等における問題も指摘され、拙速であるという意見も少なくなかったようです。

- 今回の不正アクセスの対象となったシステムにおいても、システム構築やアカウント管理の面で杜撰な点が指摘されておりますが、これを他山の石とし、自社システム・ネットワーク全体が不正アクセスの適切な遮断や速やかな検知が行える設計になっているかの確認、そして適宜UTMの設置を含めた見直しは必要不可欠でしょう。