— AUS（アルテミス・ユーザ・サポート）便り 2017/10/23号 —
https://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。

●Wi-Fiの暗号化通信（WPA2）が解読される脆弱性、スマホ・ノートパソコン等に影響

https://internet.watch.impress.co.jp/docs/news/1086546.html
https://www.ipa.go.jp/security/ciadr/vul/20171017_WPA2.html

このニュースをザックリ言うと・・・

- 10月17日（日本時間）、ベルギーのセキュリティ研究者Mathy Vanhoef氏より、Wi-Fiによる無線LAN通信の暗号化プロトコル「WPA2」に複数の脆弱性が存在することが発表され、これを受けて情報処理推進機構（IPA）等の機関やセキュリティベンダーからも警告が出されています。

- 「KRACKs」と名付けられた一連の脆弱性の悪用により、無線LANの通信範囲内にいる攻撃者がWPA2で暗号化された通信の内容を解読・盗聴、あるいは改ざんすることが可能であるとされており、Windows・Mac・UNIX系（Linux等）からiPhone・Androidのようなスマートデバイスに至るまで、脆弱性の影響範囲は極めて広いものとなります。

- Windowsについては10月11日発表のセキュリティパッチで対応済み、iOS・Androidについても今後パッチがリリースされる予定とされており、IPA等ではこういったセキュリティパッチの適用を呼び掛けています。

AUS便りからの所感等

- 現在Wi-Fiで最もよく利用される暗号化通信プロトコルであるWPA2に関する実装に存在する脆弱性であり、スマートフォン・タブレット・ノートPC等、アクセスポイント（AP）へ接続する側のデバイスでの修正が必要となりますので、上記の通りWindowsでは既にパッチが出ているため、Wi-Fi機能を有効にしているノートPCにおいては特に確実に適用されていることを確認してください。

- 一方で、APの機能を持つルータ等の機器においても、それらがさらに別のAPへ接続する機能を持っている場合に、やはり脆弱性の影響を受けることに注意が必要ですので、機器が持っている機能の把握とベンダーからの情報の参照は不可欠です。

- 今回の脆弱性はWPA2が関係しない暗号化通信には影響しないため、IPA等はHTTPSやVPN等を用いての暗号化通信を行うことを回避策として挙げており、外部から社内ネットワークにアクセスする場合はもちろん、通常のインターネットへのアクセスにおいても、UTM等が備えるVPN機能での接続を経由して行うことにより、WPA2暗号化通信が解読されたとしても通信内容を保護することが期待できます。

INTERNET Watch

WPA2脆弱性「KRACKs」、HTTPS通信時は影響受けず、有線LANやVPNの利用も推奨

岩崎 宰守　2017年10月17日 16:03

独立行政法人情報処理推進機構（IPA）をはじめ、株式会社シマンテックやトレンドマイクロ株式会社、株式会社カスペルスキーといったセキュリティベンダー各社が、WPA2の脆弱性「KRACKs」について注意を喚起している。

IPAによれば、現時点では脆弱性の実証コードや被害は確認されていない。しかし、今後脆弱性を悪用した攻撃が発生する可能性があるとしている。

回避策としては、OSベンダーやWi-Fi機器ベンダー各社が提供するセキュリティ修正パッチを適用すればよいが、パッチが提供されていない機器では、IPAやセキュリティベンダー各社では有線LANやVPNの利用を推奨している。

またIPAでは、「本脆弱性によりHTTPSの通信が復号されることはありません」としている。ウェブサイト閲覧時に、ユーザー側でHTTPとHTTPSの通信を選ぶことはできないが、どのウェブサイトとの通信が安全なのかを把握することはできることになる。

IPA Better Life with IT 情報処理推進機構

WPA2 における複数の脆弱性について

最終更新日：2017年10月18日

※追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

WPA2 (Wi-Fi Protected Access II) は、無線 LAN (Wi-Fi) の通信規格です。

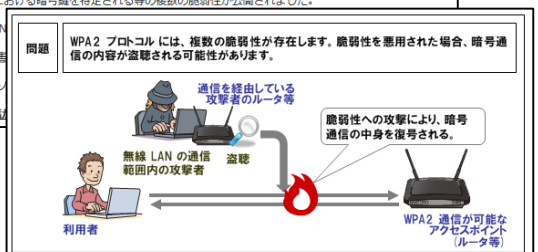
10月16日（米国時間）に、WPA2 における暗号鍵を特定される等の複数の脆弱性が公開されました。

本脆弱性が悪用された場合、無線LAN

現時点で、攻撃コードおよび攻撃被害

各製品開発者からの情報に基づき、ソ

なお、本脆弱性によりHTTPSの通信が



図：脆弱性を悪用した攻撃のイメージ

●メール経由の脅威、他の感染経路と比べて倍…シマンテック調査

http://news.mynavi.jp/news/2017/10/06/074/

このニュースをザックリ言うと・・・

- 10月5日（日本時間）、大手セキュリティベンダーのシマンテック社より、「Email Threats 2017(メール経由の脅威、2017年版)」と題したレポートが発表され、メール経由の脅威が他の感染経路に比べて2倍も高くなっているとの実態が報告されました。

- レポートでは、2017年の上半期に悪質なメールを受け取った経験があるメール利用者は9人に1人の割合となっており、業種別では特に卸売業が4人に1人の割合という高確率となっています。

- また、悪質なメールとして、マルウェアが添付されたものに限らず、会社の経営陣等になりすまして送金や機密情報の奪取を目論むビジネスメール詐欺（BEC）についても触れており、月に約8000社の企業がBECの標的になったとされています。

AUS便りからの所感等

- レポートで示されている悪質なメールの例として、
件名「New Order(新規の注文について)」、
本文には「弊社からの問い合わせにご対応いただき、
ありがとうございます(後略)」と書かれ、
要件の詳細を記載したとするPDFファイル（マルウェア）が添付されているものが挙げられており、このようなメールでマルウェアに感染させようとする攻撃が依然有効であることが窺え、アンチウイルス・ブラウザ等のアンチフィッシング機能・UTMによる多重防御による対策をとることが大事です。

マイナビニュース

メール経由の脅威は、他の感染経路と比べて2倍 - シマンテック

[2017/10/06]

シマンテックは10月5日、公式ブログにおいて、同社のISTR(インターネットセキュリティ脅威レポート)特別レポート「Email Threats 2017(メール経由の脅威、2017 年版)」で、メール経由の脅威が他の感染経路に比べて2倍も高くなっている実態が報告されていると伝えた。

メール利用者のうち9人に1人が、2017年の上半期に悪質なメールを受け取った経験があるという。さらに、業種によってその確率が上がり、卸売業では4人に1人という高確率となっている。

ブログでは、悪質なコードが添付されたメールに加え、ビジネスメール詐欺(BEC)の脅威についても触れている。BECでは、会社の経営陣あるいはサプライチェーンや指揮系統上の有力者になりすました詐欺師が、ユーザーを欺いて送金させたり、機密情報を共有させたりするといった手口が用いられる。

- 一方のBECについては、なりすます人間のPCにマルウェアを感染させ、それを踏み台にしてメールを送る等の手法がよくとられており、こういう面で加害者となる可能性にも十分注意が必要であり、不正なメールの外部への送信や内部サービスへの不正ログインを食い止めるための対策もまた不可欠です。

●パスワードを使い回している人は85%…トレンドマイクロ調べ

https://japan.cnet.com/article/35108356/

このニュースをザックリ言うと・・・

- 10月5日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、「パスワードの利用実態調査 2017」と題し、515人のWebサービスユーザに対するアンケート結果によるレポートが発表されました。

- 複数のWebサービスで同じパスワードを使い回しているユーザは85.2%に上り、2014年調査時の93.1%よりは下がったものの、依然高い割合となっています。

- また、使い回すパスワードの数について「2～3種類」と答えた割合は56.4%→41.4%と減少した一方、「4～5種類」と答えた割合は12.0%→17.7%、「6種類以上」は8.9%→10.7%とそれぞれ増加しており、「使い回すパスワードの数を増やすことにより、リスク低減を試みる傾向がある」と推測しています。

AUS便りからの所感等

- パスワードの使い回しに対しては、ユーザが登録する複数のサービスに芋づる式に不正ログインされてしまうリスト型攻撃が問題視された2014年以降、JPCERT/CCがキャンペーンを行う等、各所での啓発が継続的に行われています（AUS便り 2017/08/07号参照）。

- アンケート回答者の多くがサービス毎に異なるパスワードを設定することに対し「忘れてしまう」「考えるのが面倒」と、またパスワードの管理方法として「手帳等にメモする」と回答していることを踏まえ、トレンドマイクロ社ではパスワード管理ツールの使用を推奨しています（※パスワード管理ツールを使う際は、そこで用いる「マスターパスワード」について、自分が決して忘れず、かつ他人には推測できない十分強力なパスワードを設定することに注意しましょう）。

cnet Japan

パスワードを使い回している人は85%--トレンドマイクロ調べ

トレンドマイクロは10月5日、ID・パスワードでのログインが必要なウェブサービスにおける、パスワードの利用や管理の実態を調べる「パスワードの利用実態調査 2017」の結果を発表した。調査対象は515名。調査期間は2017年6月22～23日。