— AUS（アルテミス・ユーザ・サポート）便り 2017/07/18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。

●無料Wi-FiサービスとVPNの利用、わずか4人に1人…シマンテック調査

http://www.itmedia.co.jp/mobile/articles/1707/14/news124.html
https://www.symantec.com/ja/jp/about/newsroom/press-releases/2017/symantec_0713_01

このニュースをザックリ言うと・・・

- 7月13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、無料Wi-Fiスポットを利用している全世界15,532人を対象に5～6月に行ったアンケート調査のレポートが発表されました。
- 無料Wi-Fiの安全性については、全体では約60%が「非常に安全」「やや安全」と回答していますが、日本からの回答者は39%にとどまっており、リスクをある程度認識しているとみられています。
- 一方で、Wi-Fi接続時にVPNによる安全性確保を行っているか？については、日本からの回答者のうち「行っている」のは22%となっており、その他48%が「VPNという言葉自体を知らなかった」と回答している、等の結果が出ています。

AUS便りからの所感等

- Webサイトについては全体をHTTPS化する傾向が進んではいるものの、依然暗号化されていないHTTP通信が要求されるケースは多く、その他の通信、例えばメールについては送受信時の通信やメールの内容自体の暗号化はほとんど進んでいません。
- そういった意味でも、VPNによって「Wi-Fiスポットを通る全ての通信が暗号化される」ことを保証することは大事なことと言えます。
- UTM等のVPN機能を外部から組織内のLANに入るだけでなく、そこを経由してインターネット上にアクセスするようにする用途でも有効に活用することを推奨致します。

ITmedia Mobile

ニュース　2017年07月14日 19時40分 更新

「キケン」だけれど「ギガ」のためにはつないじゃう？ ノートン「フリーWi-Fi」意識調査（1/2）

シマンテックが約1万5000人を対象に「フリーWi-Fi」に対する意識調査を行った。そこから見えてくる実情は……？

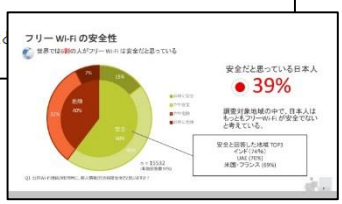
[井上翔，ITmedia]

印刷　通知　28　35　B!　2　0　G+　0

シマンテックは7月13日、同社が5月に実施した無料Wi-Fi（無線LAN）サービスに関するアンケート調査をまとめた「ノートンWi-Fiリスクレポート（2017年）」を公開した。

接続時の暗号化がない無料Wi-Fiスポット（アクセスポイント）は少なくない。設定次第では、同じスポットに接続しているデバイスのデータを参照できてしまうこともある。さらに、悪意を持った第三者が個人情報を入手するために偽のスポットを「立ちあげる」こともある。無料だからといって安易に使ってしまうと、トラブルに巻き込まれてしまう可能性もあるのだ。

その反面、「ギガが減る」ことを避けるために、若者ほど無料Wi-Fiサービスを積極的に活用する傾向にある。また、ローミング料金を節約するため、海外旅行客が無料Wi-Fiサービスを一生懸命探す姿も決して珍しいものではなくなった。



Symantec

消費者のフリーWi-Fiへの依存が明らかに
「フリーWi-Fiは安全ではない」と答えた人は日本が世界最多

「ノートン Wi-Fi リスク レポート」

2017 年 7 月 13 日

セキュリティソフト「ノートン」は、本日、Wi-Fiセキュリティに関する意識調査「ノートンWi-Fiリスクレポート（2017年版）」を発表しました。

シマンテックのノートン事業統括本部マーケティング部 部長の古谷尋は、次のように述べています。「セキュリティ対策が施されていない無料公衆無線LAN（フリーWi-Fi）にはセキュリティ上の危険性があり、フリーWi-Fiについて人びとが安全だと思っていることと実際のセキュリティにはかなりのギャップがあります。プライベートな情報だと思っている端末上の個人情報

フリーWi-Fi接続中の危険な行動が明らかに

- 「フリーWi-Fiは安全ではない」と答えた日本人は全体の61%。調査対象地域の中で日本人は最もフリーWi-Fiの危険性を認識しています。
- それにも関わらずフリーWi-Fi接続中になんらかの危険な行動を取っている人は全体の71%。うち、フリーWi-Fiで銀行口座をチェックしたり金融情報を扱ったりしている人は13%、クレジットカード情報を入力している人は12%となりました。

VPNについて「聞いたこともない」が48%

フリーWi-Fiの危険性を最も認識していながら、個人情報を守る最善の手段である「仮想プライベートネットワーク」（VPN）の認知は世界で最も低いことがわかりました。

- 世界で最もフリーWi-Fiの危険性を認識していながら、フリーWi-Fiに接続する際にVPNを利用している日本人はわずか22%にとどまります。
- 48%がVPNについて「聞いたこともない」と回答。日本では、VPNの認知が世界で最も低く、浸透していないことが明らかになりました。

他人が所有するWi-Fiに接続を試みたことがある人が19%

- 57%が友人宅、カフェ、ホテルでWi-Fiのパスワードを聞き出すと回答。うち、33%は到着して数分以内に聞き出すと回答しており、外出先でのWi-Fi利用を強く求めています。
- 所有者の許可なく他人のWi-Fiネットワークにアクセスしたことがある人は19%。また、5%が他人のWi-Fiネットワークのパスワードを予測またはハッキングしたと回答しています。

フリーWi-Fi接続の有無が旅行先のホテルを決定－61%

フリーWi-Fiネットワークへ依存する傾向は旅行の際に特に顕著です。

- 強力なフリーWi-Fiに接続できるかどうかは、ホテル（61%）、カフェ・レストラン・バーなどの飲食店（45%）、利用施設（44%）、航空会社（42%）を決める際の重要な要因であると回答しています。

●全国の高専でデータが共有される状態だった…Office365の設定を巡り高専機構に批判集まる

http://nlab.itmedia.co.jp/nl/articles/1707/12/news123.html

このニュースをザックリ言うと・・・

- 7月7日（日本時間）頃以降、全国の高等専門学校（高専）で利用されていたOffice365において、他の高専の情報にアクセス可能な状態であることが指摘され、その後、そのOffice365が停止されるという事態が発生し、Twitter等で取り上げられています。

- Office365は全国の高専を統括する独立行政法人である国立高等専門学校機構（高専機構）が契約していたものを全国の高専で利用していたものとみられ、高専機構によると、共有されていたデータは機構内での授業教材、学生会の資料、および全国の高専に所属する個人の名前等で、外部への共有は無かったとのことです。

- ある高専の学生が問題を指摘した後にOffice365が停止され、メール等のデータが利用できない状態となっており（のちメールは復旧）、高専機構では設定ミスではなく「仕様」であるとの認識とのことです。

AUS便りからの所感等

- 元々「仕様」だったとの結論であることと、指摘を受けて改修を行ったことは必ずしも矛盾するものではありませんが、ともあれ「何も設定しなければデフォルトで共有される」設定となっていたと思われるのが、Twitter上で問題視された要因でしょう。

- 組織で契約したサービスの利用と個人での契約とで事情は変わってくるところはあるとは言え、カレンダーや写真・ストレージサービス等の利用にあたり、入力した情報を自分だけが利用すべきものか、グループ内・あるいは不特定多数の他者と共有すべきものかをユーザ側が認識し、共有状態の確認と適切な設定を行うことは重要なことと言えます。

●原因は3年前に発表された「Heartbleed」、クレカ情報最大6,860件流出か

http://itpro.nikkeibp.co.jp/atcl/news/17/071201895/

このニュースをザックリ言うと・・・

- 7月12日（日本時間）、スパリゾートハワイアンズを運営する常磐興産より、同社ショッピングサイト「ハワイアンズモール」が不正アクセスを受け、クレジットカード情報が流出した可能性があると発表されました。

- 不正アクセスは2月10日から5月25日（この日決済代行会社からの指摘を受けて同サイトでのクレカ決済を停止）の間に発生していたとみられ、調査の結果、OpenSSLの脆弱性「Heartbleed」が原因であることが判明し、対策が行われたとのことです。

- この期間に同サイトで利用したクレジットカードの情報最大6,860件について、カード会員名・カード番号・住所・有効期限およびセキュリティコードが流出した可能性があるとされていますが、一方でスパリゾートハワイアンズ施設内でのクレジットカードの利用については影響はなかったとのことです。

AUS便りからの所感等

- Heartbleed（https://ja.wikipedia.org/wiki/Heartbleed）はOpenSSL 1.0.1系に存在していた脆弱性で、暗号化通信を行うプログラムのメモリ内容が読み取られ、暗号化のための秘密鍵が奪取される可能性があるものです。

- Heartbleedの存在が発表され、修正が行われたのは2014年4月の話ですが、今年1月の時点で脆弱性が残っている機器が約20万台確認されているとのことで（https://japan.zdnet.com/article/35095570/）、PCサーバ以上に、アプライアンスのファームウェアが更新できていないケースが多いと見られます。

- 暗号化通信を行う機器が当時からアップデートされていないのであれば、必ずベンダーへの確認等の上でアップデートを行い、その後念のため、SSLの秘密鍵と証明書の再発行を行うことが重要であり、一方で、攻撃を受けた痕跡は通常のログには残らないため、UTMの導入等により、IDS/IPSによる検知・遮断が有効となるでしょう。