

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。

●パスワード未設定のWebカメラ、第三者が閲覧可能

<http://www.asahi.com/articles/ASH3654C1H36PTILOOW.html>

<http://www.asahi.com/articles/ASH3F5CPWH3FPTILO1S.html>

<http://jp.techcrunch.com/2014/11/08/20141107insecam-displays-insecure-webcams-from-around-the-world/>

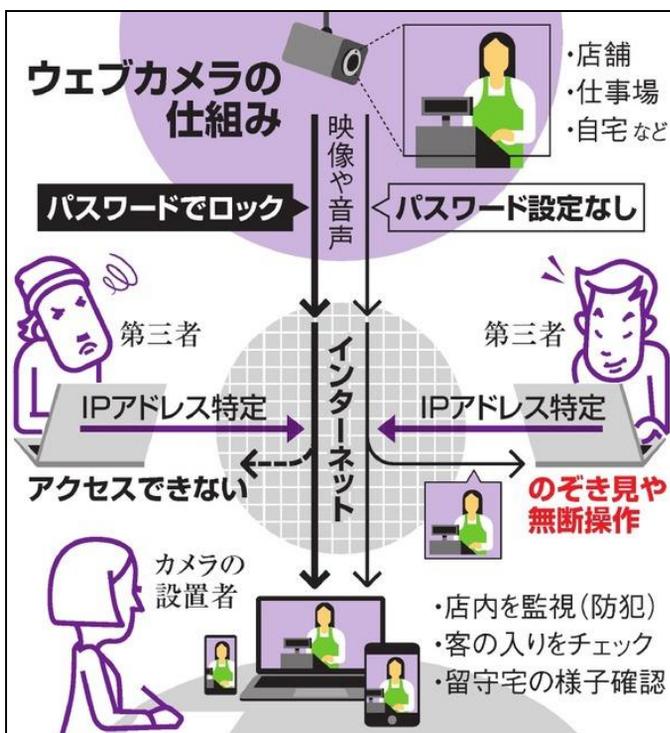


このニュースをザックリ言うと…

- 3月16日(日本時間)、朝日新聞がWebカメラ(ネットワークカメラ)において、商業施設や住宅の映像・音声を第三者が外部から見聞きできる状態にあるということを、独自調査により明らかにしました。
- 同社が国内9千万台以上あるWebカメラのうち2,163台について調査したところ、35%にあたる769台についてパスワードが設定されていないとのこと。
- また、問題のあったWebカメラのほとんどが防犯・監視用である他、工場等に設置されているWebカメラの映像へのアクセスにより、技術的ノウハウが流出する可能性も指摘されています。

AUS便りからの所感等

- こういった問題は海外でも同様に存在する模様で、「世界中の無防備なWebカメラ73,000台の映像を表示できる」とするサイトもあるようです。
- パスワードが設定されていないものの他に機種固有のデフォルトパスワードから変更されていないものもあり、攻撃者であれば容易に不正ログインして映像を閲覧することが可能になるでしょう。
- 月並みではありますが、まずは忘れずにWebカメラに適切なパスワードを設定すること、そして内部LANから、もしくはUTM等によって限られたアクセス元からのみアクセスが可能なネットワーク構成を行うことが重要です。



●公衆無線LANのセキュリティ対策は不十分...総務省発表

http://www.soumu.go.jp/menu_news/s-news/O1ryutsu03_02000091.html

http://internet.watch.impress.co.jp/docs/news/20150316_692978.html



このニュースをザックリ言うと...

- 3月16日(日本時間)、総務省が観光客を対象に実施した公衆無線LANの利用に関するセキュリティ意識調査の結果を発表しました。

- 発表によると、日本人観光客の中では、公衆無線LANに関して何らかのセキュリティ対策をとっている割合は47.1%に留まっています。

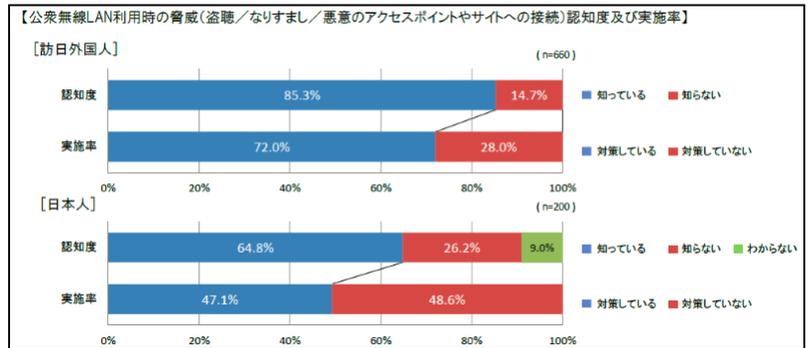
- また「知らないSSID(無線LAN(Wi-Fi)におけるアクセスポイントの識別名)には接続しない」「アクセスポイント(AP)の暗号化種類の確認と適切な対応」「SSLサイトの確認と重要な情報入力に係る適切な対応」といった基本的な対策についても、日本人観光客の実施率は2~3割と著しく低い結果となっています。

AUS便りからの所感等

- 公衆無線LANはその特性上基本的には安全な通信手段ではなく、暗号化されていない通信を同一APのユーザから覗き見される等の危険性があります。

- 公衆無線LANの利用にあたっては、問題点を十分に把握した上で、VPNによる全ての通信の暗号化といった対策を取ることを強く推奨します。

- UTMにはVPN機能を備えているものも多く、独自のVPNを構築するために活用するのも有用でしょう。



セキュリティ対策の実施率は、訪日外国人が72.0%、日本人が47.1%と、日本人観光客の対策実施率が低い

●Flash Playerの修正されたばかりの脆弱性を悪用する攻撃、サイトへのアクセスでマルウェアに感染

http://internet.watch.impress.co.jp/docs/news/20150323_694094.html

<http://blog.trendmicro.co.jp/archives/11147>



このニュースをザックリ言うと...

- 3月23日(日本時間、以下同様)、トレンドマイクロ社がFlash Playerにおいて先日修正された脆弱性を悪用する攻撃が確認されたとして警告しています。

- 問題となった脆弱性は、3月13日にFlash Player バージョン17.0.0.134のリリースによって対策されていたものです。

- 同社ブログでは、マルウェア作成に利用されるツールに脆弱性を悪用する機能が追加されたことと、そのツールで作成されたと見られる不正なFlashファイルが埋め込まれたWebサイトの存在が確認された模様です。

AUS便りからの所感等

- 今回のFlash Playerのアップデートは、メジャーバージョンが変更される(今回は16→17)形でのアップデートであり、Windows7上のIE用およびFirefox用のものについては、通常行われる自動更新がすぐには行われないことに注意が必要です
(Google Chromeに同梱されるもの、およびWindows8/8.1上のIE用のものは自動更新されます)。

- Flash Playerのバージョンを確認の上、公式サイトからインストーラーをダウンロードして手動でアップデートすることを強く推奨するとともに、アップデートが適切に行われるまでのタイムラグを突いてのマルウェア感染を防ぐため、アンチウイルス・UTMによる防御も不可欠でしょう。

INTERNET Watch ニュース

Flash Playerの修正されたばかりの脆弱性を悪用、日本の成人向けサイトなど介して感染

2015/3/23 15:00

トレンドマイクロ株式会社は、Flash Playerの最新アップデートで修正されたばかりの脆弱性を悪用した攻撃が確認されているとして、注意を喚起した。悪用サイト訪問者の9割以上が日本のユーザーだという。

トレンドマイクロでは、3月18日(「Nuclear」と呼ばれるエクスプロイトキット(脆弱性を利用した攻撃を行うために使用するツールキット)による不正活動の兆候を確認。この活動では、3月12日に公開されたFlash Playerのセキュリティアップデートで修正された脆弱性「CVE-2015-0336」を、エクスプロイトキットが利用するように更新されていた。