— AUS（アルテミス・ユーザ・サポート）便り 2017/11/20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。

●Flash Player、Acrobat Reader等セキュリティパッチリリース…Acrobat・Reader 11.xはアップグレードを

http://www.itmedia.co.jp/enterprise/articles/1711/15/news075.html
https://japan.cnet.com/article/35110485/

このニュースをザックリ言うと･･･

- 11月14日（現地時間）、Adobe社より、「Flash Player」や「Acrobat」および「Acrobat Reader」等の同社製品のセキュリティアップデートがリリースされています。

- ◆「Flash Player」は27.0.0.187、◆「Acrobat DC/Acrobat Reader DC」は2018.009.20044 および2015.006.30392、◆「Acrobat 2017/Acrobat Reader 2017」は2017.011.30068がリリースされており、それぞれ脆弱性が修正されていることから、アップデートが推奨されています。

- また、「Acrobat/Adobe Reader 11.x」についても今回11.0.23がリリースされていますが、10月15日でサポートが終了しているため、「Acrobat DC/Acrobat Reader DC」等へのアップグレードが強く呼び掛けられています。

AUS便りからの所感等

- Flash PlayerもAcrobat Readerもこれまで頻繁に脆弱性が発見され、これを悪用してのWebからの攻撃が行われてきました。

- 現在では、主なWebブラウザ（Edge・Chrome・Firefox等）が独自にPDFリーダー機能を備える等、代替となる手段は多く用意されており、これらの活用により、攻撃からのリスクの抑制が期待できます（ただしこれらに脆弱性が全くないとは限りません）。

- この場合は可能であればAcrobat Readerをアンインストールするのがより安全ですが、Acrobat Readerも引き続き使用する場合、IEやFirefoxにプラグインが組み込まれ、これらのブラウザ上で使用される場合がありますので、もし不要であれば無効化設定を行いましょう（https://helpx.adobe.com/jp/acrobat/using/display-pdf-in-browser.html）。

- そしてこういった製品を利用するか否かに関わらず、またアップデートまでのタイムラグにおける攻撃への防御として、アンチウイルスやUTMによる対策は必要不可欠です。

ITmedia エンタープライズ

2017年11月15日 10時20分 公開

Flash PlayerやAcrobat、Readerなどのアップデート一挙公開　深刻な脆弱性に対処

AdobeはFlash PlayerやAcrobat、Reader、Photoshop CCなど多数の製品を対象とするセキュリティアップデートを公開し、多数の脆弱性を修正した。

[鈴木聖子，ITmedia]

印刷／PDF　31 ツイート　20 いいね！　20 シェア　2 B! Bookmark　13 Pocket　G+　通知

米Adobe Systemsは11月14日、Flash PlayerやAcrobat、Readerなど多数の製品を対象に、セキュリティアップデートを一挙公開した。

Flash PlayerはWindows、Mac、Linux、Chrome OS向けのアップデートが公開され、5件の脆弱性を修正した。危険度はいずれも、3段階で最も高い「クリティカル」に分類され、悪用されればリモートでコードを実行される恐れがある。

これらの脆弱性は、Flash Playerのバージョン27.0.0.187で修正された。優先度はWindowsやMacが上から2番目の「2」、Linuxは「3」の位置付けで、現時点で悪用は確認されていないと思われる。

c|net Japan

アドビ、「Flash Player」や「Acrobat Reader」などで多数の脆弱性を修正

Charlie Osborne （CNET News） 翻訳校正： 緒方亮 長谷睦 （ガリレオ） 2017年11月16日 10時16分

シェア 8　ツイート　B! 3　Pocket 33　G+　印刷　メール　保存　クリップ

Adobeが最新のセキュリティアップデートで、「Adobe Flash Player」「Adobe Acrobat」「Adobe Acrobat Reader」などにおける多数のバグに対処した。この中には深刻なものも複数含まれている。

対象となるソフトには、Adobe Flash Player、「Adobe Photoshop CC」「Adobe Connect」、Adobe Acrobat、Adobe Acrobat Reader、「Adobe DNG Converter」「Adobe InDesign」「Adobe Digital Editions」「Adobe Shockwave Player」および「Adobe Experience Manager」が含まれている。

これまでも頻繁にセキュリティアップデートが行われてきたFlash Playerでは、計5件の脆弱性が解消された。

今回明らかにされた脆弱性は、Windows、Mac、Linuxおよび「Chrome OS」版のFlash Playerに影響する。いずれも緊急度はクリティカルとされており、領域外メモリ読み取りと解放後メモリ使用のバグによって、遠隔でのコード実行につながるおそれがある。

●Facebookのパスワード窃取詐欺、エフセキュア社警告

http://news.mynavi.jp/news/2017/11/08/027/

このニュースをザックリ言うと・・・

- 11月1日（現地時間）、セキュリティベンダーのエフセキュア社より、10月15日以降にFacebookユーザを対象にしたフィッシング詐欺の攻撃が確認されたと発表されました。

- 攻撃は、まず10月15日以降スウェーデンのFacebookユーザに対して行われ、17日にはフィンランドのユーザ、19日にはドイツのユーザへと対象を移していったとされています。

- 攻撃者はAndroidやiOSのユーザをターゲットにしてFacebookのアカウント情報を奪取していった他、広告サイトへのリダイレクトによる広告詐欺を通じて収益を挙げることも試みたとされています。

AUS便りからの所感等

- この攻撃に関連してユーザから発生したクリック数は20万回に到達しており、その80%近くが前述の三ヶ国からのものだったとのことです。

- 同社ではこのような攻撃に引っかかったと感じたらすぐにパスワードを変更すること、また予め二段階認証を有効にしておくことを推奨しています。

- この他にも、PCかスマートデバイスかに関わらず、不正なリンクやサイトへのアクセスを事前に食い止めるようなセキュリティソフトやブラウザの機能を可能な限り有効化するべきでしょう。

マイナビニュース

Facebookのパスワード窃取詐欺、AndroidとiOSで要注意

後藤大地
[2017/11/08]

世界最大規模のソーシャルネットワークサービスであるFacebookは日本でも多くのユーザーが利用している。通勤時間帯にスマートフォンでFacebookアプリを操作しているユーザーも多い。登録されているユーザーとの連絡手段としてはもちろん、ニュースや話題を得るチャンネルとしても使われている。しかし、このアプリ経由でやってくるメッセージをすべて信頼してよいわけではない。

詐欺ページ - 資料：F-Secure提供

F-Secureはこのほど、「Facebook Password-stealing Phishing Attack Hits Hard On Android And iOS Users」において、10月15日からスウェーデンのFacebookユーザを対象にフィッシング詐欺キャンペーンの展開を確認したと伝えた。この攻撃は17日にフィンランドのFacebookユーザーへ、19日にはドイツのFacebookユーザーへと対象を移していったという。このキャンペーンが展開されていた間のクリック数は20万回に到達しており、その80%近くがドイツ、スウェーデン、フィンランドからのものだったとしている。

●社内のIoTデバイス把握できず、責任の所在も不明…セキュリティ企業が実態調査

http://www.itmedia.co.jp/news/articles/1711/09/news057.html

このニュースをザックリ言うと・・・

- 11月8日（現地時間）、IoTセキュリティを手掛ける米ForeScout Technologies社より、米・欧・オセアニアの6ヶ国の組織を対象とした「IoTセキュリティの現状について」の調査結果が発表されました。

- 6ヶ国内の従業員2500人以上の組織におけるITおよび事業部門の責任者603人への質問の結果、「自分たちのネットワークに接続されたデバイスを100%は把握できていない」との回答が全体の82%に上っています。

- また、77%が「IoTデバイスの増加が重大なセキュリティ上の課題を生じさせている」と認識、同様に76%が「IoTに関する不安からセキュリティ戦略の見直しを迫られている」と回答、等としています。

AUS便りからの所感等

- ForeScout社では「新しいデバイスがネットに接続される度に、企業に対する攻撃経路は増える。たった1台のデバイスからネットワーク全体に侵入され、業務が混乱して業績に影響が出ることもある」と警告しています。

- スマートデバイスが定着しだした2009年、私物のデバイスを業務で利用する「BYOD」という概念が提唱されたときにも言われてきたことですが、社内ネットワーク内に存在するあらゆるネットワークデバイスについて存在を把握し管理することや、新たなデバイス、一旦外部に持ち出されたデバイスの接続に対し十分な検疫を行い、内部へのアクセスに制限をかけること等が今後さらに重要となってくるでしょう。

ITmedia NEWS

速報

2017年11月09日 08時10分 公開

社内のIoTデバイス把握できず、責任の所在も不明――セキュリティ企業が実態調査

世界の約600社を対象とした調査で、82%が「自分たちのネットワークに接続されたデバイスを100%は把握できていない」と回答した。

[鈴木聖子，ITmedia]

社内で増え続けるIoTデバイスの存在はIT担当者も把握しきれず、責任の所在もあいまいになりがち――。IoTセキュリティを手掛ける米ForeScout Technologiesが11月8日に発表した調査結果で、大企業のそんな実態が浮き彫りになった。

調査はForeScoutの委託でForrester Consultingが実施し、米欧やオーストラリアなど6カ国で従業員2500人以上の組織を対象として、ITおよび事業部門の責任者603人にIoTセキュリティの現状について質問した。

その結果、82%が「自分たちのネットワークに接続されたデバイスを100%は把握できていない」と回答。90%は、今後数年でそうしたデバイスの数はさらに増えると予想した。