

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。

●Windows7サポート終了でも3割以上のPCが移行漏れか、IDC Japanが調査

<http://itpro.nikkeibp.co.jp/atcl/news/17/030700726/>
<http://www.idciapan.co.jp/Press/Current/20170307Apr.html>



このニュースをザックリ言うと…

- 3月7日(日本時間)、IDG Japan社(以下IDG社)より、国内企業におけるWindows7からWindows10への切り替え行動に関する調査結果が発表されました。
- 2020年1月に全てのサポート終了が予定されているWindows7ですが、調査結果によれば、現時点で切り替え計画のある企業は56%となっています。
- 計画のある企業においても、2019年末の時点での進捗率は65.4%に留まり、依然34.6%のPCがWindows7のままとなる見込みで、2014年のWindows XPサポート終了時はその1年前におけるXP残存率が29.3%だったのを踏まえると、それよりも多い数値となっています。
- IDG社では、XPの時よりも移行に遅れが生じる可能性の他、サポート終了前後に買い替え需要が集中することにより、企業のIT予算が圧迫され得ることや、買い替え需要後に企業PC市場が一気に冷え込む可能性を指摘しており、早いうちからWindows10への切り替えを行うことにより、PC買い替え需要の平準化を進めることが大事だとしています。

AUS便りからの所感等

- Windows10のリリースから1年半以上が経過していますが、7からの使い勝手の変化や、昨年7月まで行われていた無償アップグレードのやり方に対する批判が移行計画の鈍化にいくばくか影響している面もあると見られます。
- 一方で、2020年1月というリミットよりも前に、より新しいアーキテクチャのCPUについてはWindows10のみのサポートとなるという話も出てきており、今後の新しいPCの購入では10の導入が前提となってくることでしょう。
- あらゆるOSにはサポート期限があり、それを超えた利用は基本行うべきではなく、OSの移行は必ず発生するという前提にしたシステム構成の構築に努め、現時点で10への対応を全くしていない場合でも、可能な限り早く検証を行い移行していく体制を整えましょう。



Windows 7サポート終了でも3割以上のPCが移行漏れか、IDC Japanが調査

IDC Japanは2017年3月7日、国内企業を対象に実施した、2020年1月予定のWindows 7延長サポート終了への対応状況の調査結果を発表した。

調査結果によると、Windows 7の切り替え計画のある企業は56%となっており、2019年末の時点でも34.6%稼働見込み(65.4%が移行済み)で、2014年のWindows XPサポート終了時の29.3%に比べて、移行漏れが懸念されています。

年	Large	SMB	Total
2016年	16.8%	18.5%	17.8%
2017年	32.5%	33.3%	32.9%
2018年	48.3%	55.0%	50.0%
2019年	69.6%	65.4%	62.7%
2020年	90.1%	80.0%	73.5%

「Windows 10に切り替えるに当たって、今後どのような計画で切り替えが行われるか進捗率をお答えください」への回答
 Windows 10への対応スケジュールがある企業における台数進捗率。Largeは従業員規模500人以上、SMBは500人未満の企業。出所：IDC Japan



～2020年のWindows 7の延長サポート終了に警鐘を鳴らす～
 国内企業PCのWindows 10への切り替え計画分析結果を発表

2017年3月7日
 IDC Japan株式会社

- ・ Windows XP延長サポート終了1年前のWindows XP搭載PCの残存率は、全企業PCのうち29.3%であった。
- ・ Windows 7延長サポート終了1年前の2019年におけるWindows 7 PCの残存率は34.6%と推計
- ・ Windows 10への移行を早めに推進することで、Windows 7サポート終了直前のPC需要の急増を軽減し、需要の平準化を目指すことが重要

IT専門調査会社 IDC Japan 株式会社(所在地:東京都千代田区九段北1-13-5、代表取締役:竹内正人、Tel代表:03-3556-4760)は、2020年1月に予定されているWindows 7の延長サポート終了(以下EOS: End of Support)に向け、国内企業で主に利用されているWindows 7のWindows 10への切り替え行動について調査し、その分析結果を発表しました。

IDCは、Windows XP EOS時と比較分析をした結果、Windows 7 EOS時にもWindows XP EOS時と同様の急激な買い替えが進められる可能性が低く、警鐘を鳴らしています。

まず、2014年のWindows XP EOS当時の状況を振り返ると、Windows XP EOSの1年前に、企業で稼働するPCの29.3%がWindows XPを搭載されたPCでした。これを企業規模別に見ると、中堅中小企業(従業員数500人未満)では24.0%、大企業(従業員数500人以上)では35.4%と、顧客数が多くシステム規模が大きい企業の方がWindows XPを搭載するPCの残存率が高かったことがわかりました。しかしながら、総務省やマスコによるWindows XPのセキュリティリスクに関する注意喚起が効果的でもあり、2013年後半～2014年前半にかけて、Windows 7を中心とした次世代OSのPCへの買い替えが行われました。結果、この時期の国内PC出荷数は、過去最大規模となりました。

次に、Windows 7 EOSに伴うWindows 10への移行計画を分析すると、2016年時点でWindows 10への切り替え計画のある企業は約56%にとどまっています。これを企業規模別に見ると、中堅中小企業では約45%、大企業では約67%と、大企業の方が切り替え計画のある比率が高くなっています。また、切り替え計画のある企業におけるWindows 10への切り替え進捗率をみると、Windows 7のEOSの1年前にあたる2019年末の進捗率は65.4%、つまりWindows 7の残存率の34.6%を超える見込みであることがわかりました。これをWindows XP EOS 1年前のWindows XP搭載PCの残存率29.3%と比較すると、Windows 7 EOS時の方が古いOSを搭載したPCの割合が高くなるという分析結果となりました。更に、Windows XP EOS 1年前のWindows XP残存率と同様に、大企業の方が新しいOSへの切り替え進捗率が低い結果となりました。

●「フォントが見つかりません」…偽警告でChromeを狙うランサムウェア

<http://forbesjapan.com/articles/detail/15413>
<http://forbesjapan.com/articles/detail/14874>



このニュースをザックリ言うと…

- 3月3日(現地時間)、「Forbes JAPAN」誌のWebサイトにおいて、Google Chromeの偽警告からランサムウェア「Spora」に感染させようとする攻撃について警告が出されています。

- 偽警告は、「HoeflerTextフォントが見つかりません(The “HoeflerText” font wasn’t found)」という文面で、Chromeのプラグインが期限切れになっていると見せかけた内容のダイアログになっており、ここで「Update」をクリックするとSporaに感染する恐れがある模様です。

- ただし記事によれば、Chromeのセキュリティ機能により「(ファイル名)は一般的にダウンロードされておらず、危険を及ぼす可能性があります。」というメッセージが表示されるため、「破棄」をクリックすることにより、マルウェアのインストールを防ぐことができるとされています。

AUS便りからの所感等

- 自分のPC等をセキュアに利用するための普段からの心掛けとして、
①こういった攻撃が発生しているという情報等を普段から幅広い情報収集によって得ること、②利用しているソフトウェアやWebサイトの挙動を十分に把握すること、③普段と違う挙動が発生したら(やはり情報収集により)同様の報告がないか調べること、などが挙げられます。

- 記事によれば、この攻撃を検知するアンチウイルスソフトはまだ少ないとのことで、ことランサムウェアについてはアンチウイルスソフトが検出せずに感染してしまうケースも多いのですが、今回のようにブラウザのセキュリティ機能が遮断してくれる場合もあり、アンチウイルス・ブラウザ・UTM等どれか一つだけではない、複数を組み合わせた多層防御が改めて重要であると言えます。



●開発用PCがマルウェア感染、Androidアプリ132個にも混入か

<http://itpro.nikkeibp.co.jp/atcl/idg/14/481542/030300341/>



このニュースをザックリ言うと…

- 3月3日(現地時間)、セキュリティベンダーの米Palo Alto Networks社より、「Google Play」で公開されていたAndroidアプリの中にマルウェアが組み込まれたものが132個見つかったと発表されました。

- これらのアプリは、多くがガーデニングやテラスのレイアウトなど、デザインのアイデアを紹介するアプリで、実行すると一見無害なWebページを表示しますが、不審な外部サイトにアクセスする仕掛けが含まれていたとのことです。

- アクセス先には、Windowsに感染するマルウェアをホスティングしていたサイトが存在していた模様で、他にもWindowsで使われるVBScriptのコードが組み込まれたものもあったことから、アプリ開発者が使用していたWindows PCがマルウェアに感染し、そこからアプリにも入り込んだ可能性があるとされています。

- 問題のあったアプリは既に全て取り下げられており、またアクセス先の不審なサイトも2013年に閉鎖済みだったとのことです。

AUS便りからの所感等

- 幸いにもこのアプリに混入していたマルウェアはAndroidデバイス上で深刻な被害をもたらすものではなかったようですが、記事でも指摘されるように、このケースを模倣し、より現実的な攻撃を行うアプリが開発される恐れは確かに存在します。

- Windows PC等と同様、AndroidデバイスにもAndroid用に提供されているアンチウイルスアプリを導入することが重要ですし、屋外等でスマートフォンを使う場合でも、可能な限りUTMへのVPN接続を経由して外部に接続することにより、場合によってはアプリが不審な通信を行っていることを検知し、遮断することができることでしょう。

