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。

●遠隔操作ソフトは利用目的を理解してからインストールを、IPAが注意呼び掛け

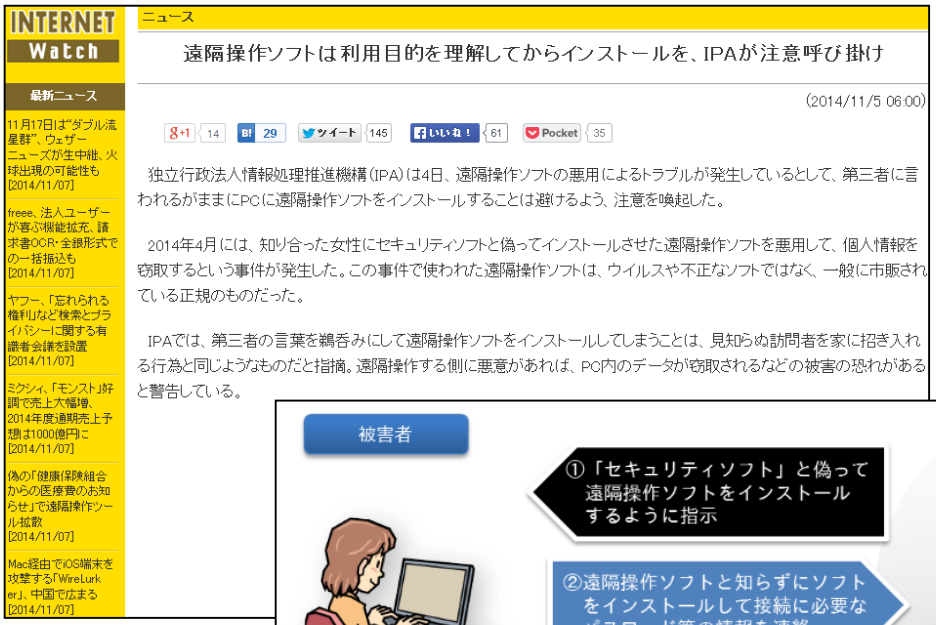
http://internet.watch.impress.co.jp/docs/news/20141105_674474.html
http://www.ipa.go.jp/security/txt/2014/11outline.html

このニュースをザックリ言うと・・・

- 11月4日、独立行政法人情報処理推進機構（IPA）が毎月行っている「今月の呼びかけ」の11月分が発表されました。
- 「プロバイダ料金を安くする」という電話勧誘により、プロバイダ設定変更を行うために遠隔操作ソフトをユーザのPCにインストールさせることに対する相談が2013年に1596件、2014年も9月初頭までに1537件あったことが発表されています。
- また、前後して4月に遠隔操作ソフトを悪用した個人情報の詐取事件が発生していたことを踏まえ、遠隔操作による作業を行う相手や内容、使用されるソフトウェア等について十分に確認を行うこと等を呼びかけています。

AUS便りからの所感等

- トラブル対応等の目的で自分のPCを他人に操作してもらうための遠隔操作ソフトとしては、「LogMeIn」や「TeamViewer」、またWindowsデフォルトのものとして「リモートアシスタンス」等が知られています。
- 外部から操作してもらう場合は、通常PCの本来の利用者側が許可を出す必要があるものの、一旦許可を出せば、操作する側がPCの利用者と同様にあらゆる操作を行うことが可能となり得ますので、IPAも呼びかけている通り、遠隔操作をする側が十分に信頼できるかの確認は大変重要です。



●日本企業のセキュリティー投資、世界平均の半分　民間調査

http://www.nikkei.com/article/DGXLASDZ05HK8_V01C14A1TJ1000/

このニュースをザックリ言うと･･･

- 11月5日（日本時間）、企業コンサルティングのプライスウォーターハウスクーパース（PwC）社は、情報セキュリティや最新のサイバーセキュリティに関する世界規模のオンライン調査「グローバル情報セキュリティ調査(R)2015(日本版)」の結果を発表しました。

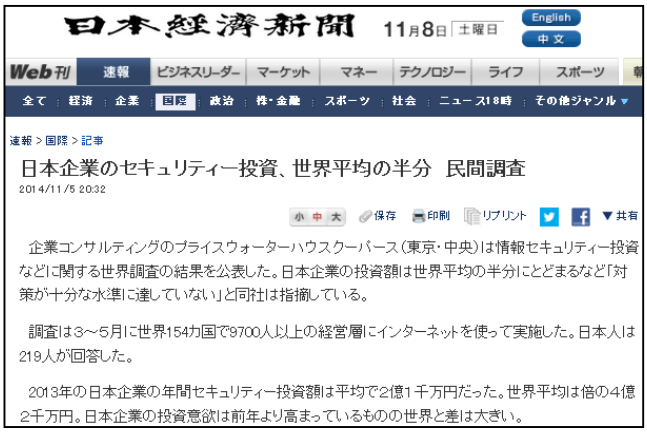
- 同結果では、企業の情報セキュリティへの年間投資額は世界全体平均の4.2億円に対して日本企業平均は年間2.1億円と2倍の差があることや、日本企業の4割以上がインシデントの発生要因を把握できていない、役員クラスの情報セキュリティリーダーが不足している等、情報セキュリティに対して日本企業の対策が十分な水準に達していないとされています。

- 同社ではこの結果を踏まえ、「適正なセキュリティ投資」「内部犯行への対策」「セキュリティ管理のリーダーシップ」が日本企業に求められるものと示唆しています。

AUS便りからの所感等

- 「水と安全は無料」という日本人によくみられる誤解、決まったゴールというものが見えづらいこと、世界的な不況からの復調に遅れをとっていること等が、日本におけるセキュリティへの投資が十分ではない原因と考えられます。

- 「セキュリティへの投資」を如何に行うかは難しいところですが、現時点でのセキュリティレベルを十分に把握し、それに見合った複数の多面的な対策を検討していくこと、例えば最低限UTMの導入などが重要となるでしょう。



日本経済新聞　11月8日 土曜日　English　中文

Web刊　速報　ビジネスリーダー　マーケット　マネー　テクノロジー　ライフ　スポーツ

全て　経済　企業　国際　政治　株・金融　スポーツ　社会　ニュース18時　その他ジャンル

速報 > 国際 > 記事

日本企業のセキュリティー投資、世界平均の半分　民間調査

2014/11/5 20:32

小 中 大　保存　印刷　リプリント　共有

企業コンサルティングのプライスウォーターハウスクーパース（東京・中央）は情報セキュリティー投資などに関する世界調査の結果を公表した。日本企業の投資額は世界平均の半分にとどまるなど「対策が十分な水準に達していない」と同社は指摘している。

調査は3～5月に世界154カ国で9700人以上の経営層にインターネットを使って実施した。日本人は219人が回答した。

2013年の日本企業の年間セキュリティー投資額は平均で2億1千万円だった。世界平均は倍の4億2千万円。日本企業の投資意欲は前年より高まっているものの世界と差は大きい。

●国内の.comサイトをターゲットとしたドメインハイジャック発生

http://www.nikkei.com/article/DGXLASDZ05H3S_V01C14A1000000/
https://www.jpcert.or.jp/at/2014/at140044.html

このニュースをザックリ言うと･･･

- 11月5日、一般社団法人JPCERT/CC、および.jpドメインの管理登録を行っているJPRS社より、国内組織をターゲットとした「ドメインハイジャック」が複数報告されていると相次いで発表されました。

- ドメインハイジャックの対象となったのは.comドメイン名のもので、ドメインを管理する組織あるいはそこから指定された登録業者やその代理店のネットワーク等への侵入によって情報が書き換えられ、攻撃者が用意したネームサーバの情報が追加されることにより、偽のサイトへの誘導等の被害が発生していた模様です。

AUS便りからの所感等

- ドメインハイジャックは、本来のサーバへの侵入・データ改ざんが行われないため、内部からは管理者に気付きにくく、一方外部からはせいぜいネームサーバやWebサーバの構成に変更があった程度に受け取られる可能性も高いでしょう。

- サーバ側の対策としては、サーバへのアクセスが急激に減少していないかログをチェックすることや、管理者側が想定していないサーバ構成の変更が発生していないか、外部サービスによる監視を行うこと、等が挙げられます。

- ユーザ側の回避策としては、HTTPSサイトであればSSL証明書が不正なものかをチェックすることが挙げられるほか、UTMやアンチウイルスによる防御は、ドメインハイジャックそのものを検出できるとは限らないものの、偽サイトへのアクセスによるマルウェアのダウンロード等を食い止めるには有効でしょう。