— AUS（アルテミス・ユーザ・サポート）便り 2016/12/05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。

●【注意喚起】冬期休暇は特にセキュリティ対策を･･･IPA等の情報に要注目

https://www.ipa.go.jp/security/measures/vacation.html
https://www.jpcert.or.jp/pr/2015/pr150006.html

このニュースをザックリ言うと･･･

- 年末年始の休暇期間（あるいは休暇明け）に、特に企業ユーザの隙を突いての攻撃が行われる可能性があります。

- こういった攻撃の可能性に備えて、今年もセキュリティ機関より、インシデント発生予防・発生時の対応等、注意点のまとめが公開されるものとみられます。

- ここでは例として、独立行政法人情報処理推進機構（IPA）とセキュリティ専門機関JPCERT/CCを挙げますが、いずれも12/2時点では2015年の情報となっており、アップデートは12/20前後に行われる見通しであるものの、現在掲載されている情報は決して1年たっても陳腐なものではない普遍的な内容が主です。

AUS便りからの所感等

- セキュリティ機関が発表する注意点は、年末年始あるいはゴールデンウィークや夏期休暇といった長期休暇はもちろん、普段から文書化や各社員での意識合わせ等をしておくべき事項がほとんどであり、休暇入りの直前ではなく、せめてこのAUS便りをご覧になったその日から準備を始め、点検を行うよう意識して頂ければ幸いです。

- また、企業ユーザがプライベートでSNSやクラウドサービスを利用する場合等についても注意が促されており、情報の発信が特定範囲に限定されているか、不特定多数向けに公開すべきでない情報を公開していないかに注意しましょう。

- さらに、複数のサービス間、あるいは同じサービスでプライベート用・会社用等複数のアカウントを用いている場合でも、それぞれでパスワードの使い回しを行わないようにし、連鎖的な不正アクセスに繋がらないよう対策しましょう。


IPA Better Life with IT 情報処理推進機構

長期休暇における情報セキュリティ対策

掲載日：2015年12月21日
独立行政法人情報処理推進機構
技術本部　セキュリティセンター

0. はじめに | 1. 組織のシステム管理者向け | 2. 組織の利用者向け | 3. 家庭の利用者向け

0. はじめに

2. 組織の利用者向け

～ 長期休暇前の対策 ～

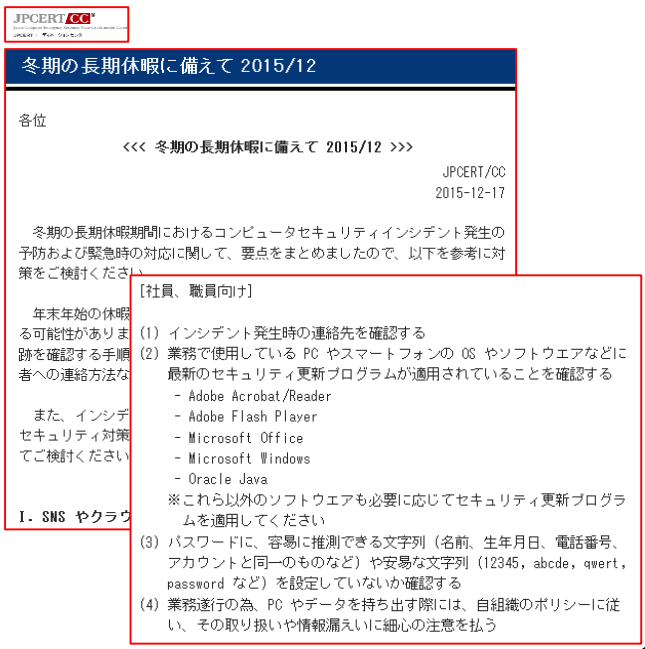
1. 機器やデータの持ち出しルールの確認と遵守
長期休暇に社外での対応が必要となるなどパソコン等の機器やデータ等の情報を持ち出す場合は、持ち出しルールを事前に確認、遵守してください。

2. 使用しない機器の電源OFF
長期休暇中に使用しない機器は電源をOFFにしてください。

～ 長期休暇中の対策 ～

1. 持ち出し機器やデータの厳重な管理
自宅等に持ち出したパソコン等の機器やデータは、ウイルス感染や紛失、盗難等によって情報漏えい等の被害が発生しないよう、厳重に管理してください。

～ 長期休暇明けの対策 ～


JPCERT/CC

冬期の長期休暇に備えて 2015/12

各位

<<< 冬期の長期休暇に備えて 2015/12 >>>

JPCERT/CC
2015-12-17

冬期の長期休暇期間におけるコンピュータセキュリティインシデント発生の予防および緊急時の対応に関して、要点をまとめましたので、以下を参考に対策をご検討ください。

年末年始の休暇
る可能性がありま
跡を確認する手順
者への連絡方法な

また、インシデ
セキュリティ対策
てご検討ください

I. SNS やクラウ

[社員、職員向け]

(1) インシデント発生時の連絡先を確認する
(2) 業務で使用している PC やスマートフォンの OS やソフトウエアなどに最新のセキュリティ更新プログラムが適用されていることを確認する
- Adobe Acrobat/Reader
- Adobe Flash Player
- Microsoft Office
- Microsoft Windows
- Oracle Java
※これら以外のソフトウエアも必要に応じてセキュリティ更新プログラムを適用してください
(3) パスワードに、容易に推測できる文字列（名前、生年月日、電話番号、アカウントと同一のものなど）や安易な文字列（12345，abcde，qwert，password など）を設定していないか確認する
(4) 業務遂行の為、PC やデータを持ち出す際には、自組織のポリシーに従い、その取り扱いや情報漏えいに細心の注意を払う

●Android 5以前に感染するマルウェア「Gooligan」

http://www.itmedia.co.jp/enterprise/articles/1612/01/news066.html

このニュースをザックリ言うと・・・

- 11月30日（現地時間）、大手セキュリティベンダーであるチェックポイント社より、古いAndroidデバイス（スマートフォン等）に感染するマルウェア「Gooligan」について警告が出されています。

- GooliganはAndroid 4および5に感染し、デバイスのroot権限を奪取して、保存されたGoogleアカウントの認証トークンを盗み出し、GMail等に不正アクセスするとされています。

- Gooliganはサードパーティーのアプリストアで配布されているアプリから拡散し、1日に13,000台のペースで感染を拡大しているとされており、100万以上のGoogleアカウントが不正アクセスの被害を受けている模様です。


ITmedia エンタープライズ

2016年12月01日 08時07分 更新

Androidマルウェア「Gooligan」横行、100万超のGoogleアカウントに不正アクセス

Gooligan感染するとAndroid端末のroot権限を取得されて認証トークンを盗まれ、Google PlayやGmailなどの主要Googleアカウントに不正アクセスされる恐れがある。

[鈴木聖子，ITmedia]

印刷／PDF 119 ツイート 62 いいね！ 62 シェア 16 Bookmark 22 Pocket 3 G+1 共有する 通知

セキュリティ企業のCheck Point Software Technologiesは11月30日、Androidマルウェア「Gooligan」を仕込んだアプリがサードパーティーのアプリストアなどを通じて出回り、100万以上のGoogleアカウントが不正アクセスの被害に遭っていることが分かったと伝えた。被害に遭ったデバイスは1日に1万3000台のペースで増え続けているという。

Check Pointのブログによると、Gooliganには感染した端末のroot権限を取得して、認証トークンを盗み出す機能があることが判明。攻撃者にこのトークンを使われれば、Google PlayやGmail、Google Photos、Google Docs、G Suite、Google Driveなどの主要Googleアカウントに不正アクセスされる恐れがある。

AUS便りからの所感等

- Androidの現行バージョンは7ですが、より以前のバージョンが搭載された古いデバイスの中にはバージョンアップが提供されないケースも珍しくなく、チェックポイント社の発表では、現在使われているAndroidデバイスの74%をAndroid 4と5で占めている模様です。

- AndroidはもはやWindowsと同様にマルウェアの格好のターゲットとなっており、主なセキュリティベンダーからはWindowsと同様にAndroidにもアンチウイルスソフトが提供され（無料のものもあり）、これをインストールすることが最低限のセキュリティ対策となるでしょう。

- もちろん、偽のアンチウイルスソフトを掴まされては元も子もありませんので、Androidアプリのインストールにあたっては、公式のGoogle Playから行うこと、インストールするアプリについてレビュー以外にも十分に情報収集を行うことが肝要です。

●自衛隊 通信システムに侵入、情報流出は否定

http://www.tokyo-np.co.jp/article/national/list/201611/CK2016112802000128.html

このニュースをザックリ言うと・・・

- 11月28日（日本時間）、共同通信等のメディアより、防衛省と自衛隊が運用する防衛情報通信基盤（DII）が9月頃に不正アクセスを受けたと報じられました。

- 陸上自衛隊（陸自）の内部情報が流出した可能性があるとされていますが、陸自では否定しています。

- 報道によれば、DIIおよび防衛省外のネットワークの両方と接続している、防衛大学校と防衛医科大学校のPCが侵入され、これを踏み台にしてDIIに侵入したとされています。

- DIIはメールを通じてのマルウェア感染防止のためオープン系（部外系）とクローズ系（部内系）に分かれており、今回侵入されたのはオープン系ですが、個々のPCは双方のシステムに接続し、切り替えながら使用するようになっていたとのことです。


東京新聞 TOKYO Web

陸自　システム侵入被害　サイバー攻撃、情報流出か

ツイート 4 シェア 125 G+1 2　2016年11月28日 朝刊

防衛省と自衛隊の情報基盤で、駐屯地や基地を相互に結ぶ高速・大容量の通信ネットワークがサイバー攻撃を受け、陸上自衛隊のシステムに侵入されていたことが、複数の同省関係者の話で分かった。防衛省が構築した堅固なシステムの不備を突かれたと確認された。詳細な記録が残されておらず、被害の全容は判明していないが、内部情報が流出した可能性が高い。

複数の自衛隊高級幹部は「危機的で相当深刻な事態だ。早急に再発防止策を必要がある」と強調。一方、情報セキュリティーを担当する防衛省の斎藤隆「個別の案件には答えられない」とコメントした。

防衛省は外部接続を制限するなど防御態勢を強化してきたが、それを上回る手法から国家などが関与した組織的攻撃の疑いが強い。九月ごろに確認し、サイバー攻撃への警戒レベルを引き上げた。

関係者によると、攻撃を受けたのは、防衛省と自衛隊が共同で利用するネットワーク「防衛情報通信基盤（DII）」。接続する防衛大と防衛医大のパソコンが不正被害に遭ったとみられる。このパソコンを「踏み台」として利用した何者かがシステムにも侵入した可能性が高い。防衛省は確認後、防衛省・自衛隊全体で利用を一時禁止した。

AUS便りからの所感等

- 二つのネットワークが相互に隔離されている場合は、それぞれのネットワークで使用するPCも別々のものであることが理想ですが、PCが一方のネットワークでマルウェアに感染した状態でネットワークの切り替えを行えば、マルウェアによる侵入を媒介してしまうことになります。

- 外部に持ち出したPCを再度ネットワークに接続する際は、マルウェアに感染していないか事前に検疫を行うことが強く推奨されますが、これは今回のケースでも言えることで、隔離されたネットワークの双方に接続する必要がある場合は、なおさらその点には注意が必要でしょう。