— AUS（アルテミス・ユーザ・サポート）便り 2018/04/23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。

●GWにおける情報セキュリティに関する注意喚起、JPCERT・IPA呼びかけ

https://www.jpcert.or.jp/pr/2018/pr180001.html
https://www.ipa.go.jp/security/topics/alert300419.html

このニュースをザックリ言うと・・・

- 4月19日（日本時間）、多くの企業が長期休暇となるゴールデンウィーク（GW）を迎えるにあたり、JPCERT/CCとIPAより情報セキュリティに関する注意喚起が出されています。

- システム管理者が長期間不在になることによりウイルス感染や不正アクセス等のインシデント発生に気付きにくく対処が遅れてしまう可能性、従業員等が友人や家族と旅行に出かけた際のSNSへの書き込み内容から思わぬ被害が発生する可能性、場合によっては関係者にも被害が及ぶ可能性、などを指摘しています。

- 各組織とも、休暇前にシステムのセキュリティ対策が十分か確認すること、休暇期間中のインシデント対応体制や関係者への連絡方法を調整すること、および休暇明けには不正アクセス・侵入等の痕跡をサーバ等のログから確認することを呼びかけており、実施すべき項目をまとめています。

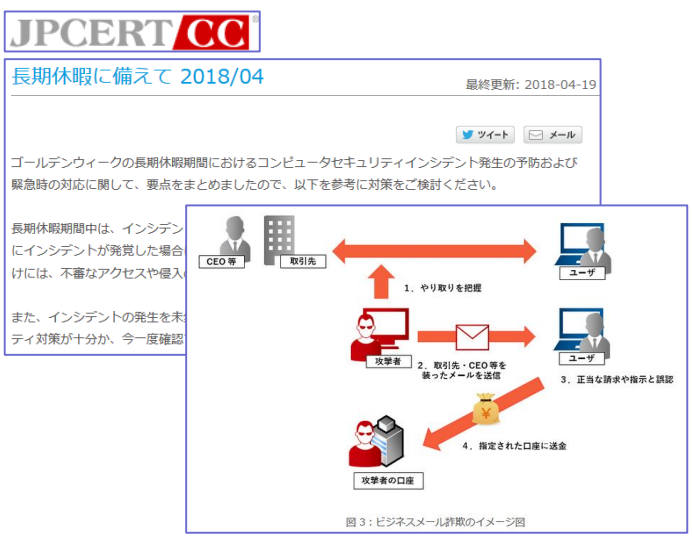
AUS便りからの所感等

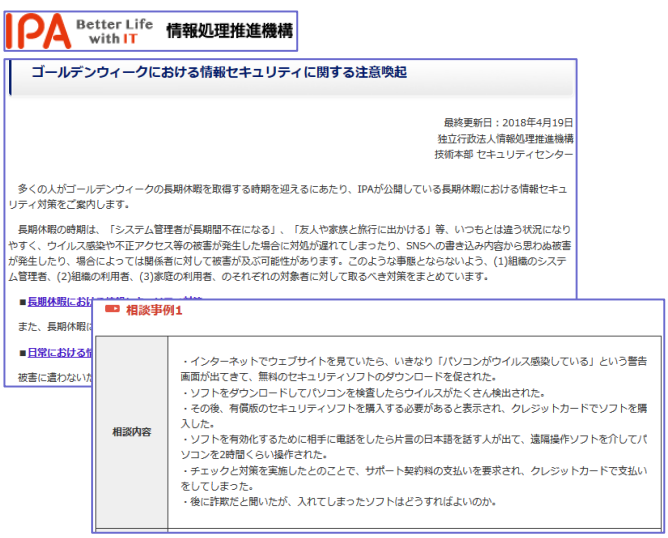
- JPCERT/CCやIPAでは、毎年の夏季や年末年始そして今回のようなGWといった長期休暇の前に、組織内に常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、そういった問題にも早く確実に対応することへの注意を促しています。

- 具体的なインシデントの例として、各組織で「不審なメールへの注意(URSNIF等のばらまき型メール攻撃、ビジネスメール詐欺等)」を、JPCERT/CCでは「適切な設定が行われていないサービスやシステムにおける脆弱性の悪用」、IPAでは「偽のセキュリティソフトをインストールさせる詐欺」等の相談事例を挙げています。

- UTMによるネットワークの防御、ソフトウェアのアップデートやアンチウイルス等を用いてのPCの防御以外にも、全てのユーザに対する随時のセキュリティ教育や情報の共有がそういった攻撃による被害を最小限に抑えられるために大切なことと言えます。

- 万一、GWまでに十分な対応が間に合わなかったとしても、GW明け以降に点検すべきことは多く存在しますし、以後も夏季休暇等に備えて、準備・点検を行うよう意識して頂ければ幸いです。





●Pマーク発行機関も「パスワード定期変更は不要」

https://www.nikkei.com/article/DGXMZO29214870Q8A410C1CR8000/

このニュースをザックリ言うと・・・

- 4月10日（日本時間）、「プライバシーマーク(Pマーク)」を発行する日本情報経済社会推進協会（JIPDEC）より、同協会が公開している「JIS Q 15001:2006をベースにした個人情報保護マネジメントシステム実施のためのガイドライン」の一部改訂が発表されました。

- 改訂内容としては、組織内でのアカウント・パスワードの設定・利用における具体的な対策の例として「パスワードの有効期限を設定していること」を挙げていたのを削除し、「複数のサービスで同一のパスワードを使い回さないこと」「漏えいした、または漏えいのおそれがあるパスワードは、速やかに変更すること」を追加しています。

- 3月下旬に総務省が「定期的なパスワードの変更は不要」と方針転換した（「AUS便り 2018/04/09号」参照）ことへの対応とみられています。

AUS便りからの所感等

- Pマーク発行・更新の際の審査基準ともされていた当該ガイドラインの改訂は、ここ数年のパスワードの管理に関する議論とそれにともないセオリーが変化していっている流れの一つであり、取得を目指す事業者のみならず、既に取得した業者においても是非ともこれを踏まえてパスワードポリシーの見直しを図ってほしいものです。

- 今回の改訂内容に加え、特にWebサービス等の運営にあたっては、ユーザ側が設定するパスワードについて、最大文字数を8文字・12文字といった短いものに制限せず、より長い文字数のパスワード（パスフレーズ）をも受け入れるようにすることがブルートフォースへの耐性を強化することにつながるでしょう。

日本経済新聞

Pマーク発行機関も「パスワード定期変更は不要」

社会

2018/4/10 17:56

保存 共有 印刷 その他

個人情報を適切に扱う事業者に与えられる「プライバシーマーク（Pマーク）」を発行する一般財団法人の日本情報経済社会推進協会（東京・港）は10日、認定時の審査基準を改定し、インターネット利用時のパスワードの定期的な変更を不要にする方針を示した。総務省などの方針転換に対応した。Pマークを取得済みの約1万5千社・団体でも同様の動きが広がりそうだ。

同協会が見直したのは企業が顧客らの個人情報を適切に扱っているかを審査する基準。情報流出を防ぐ手法の例示から「パスワードの有効期限の設定」「同一パスワードの再利用を制限」という表記を外した。

日立製作所や富士通、パソナなど約1万5千社・団体が取得するPマークは、官公庁が事業委託の条件にすることも多い。認定更新には2年ごとに審査を受けねばならない。従業員や顧客らにパスワードの定期変更を求めてきた企業も、対応を変える可能性がある。

●「Apple IDが不正に利用」…ソフトバンクをかたるフィッシングメール確認

https://www.softbank.jp/mobile/info/personal/news/support/20180418a/

このニュースをザックリ言うと・・・

- 4月18日（日本時間）、ソフトバンクをかたるフィッシングメールが確認されているとして、同社およびフィッシング対策協議会より警告が出されています。

- 警告によれば、フィッシングメールは、件名が「【重要】ソフトバンク株式会社から緊急のご連絡」、本文には「お客様のApple IDが不正に利用され、お客様のご契約内容がソフトバンクまとめて支払いに変更された可能性がございます」等と記載、本文の先頭と中程にソフトバンクのページへのリンクに偽装してフィッシングサイトへ誘導するリンクが貼られています。

- 同協議会では、現在もフィッシングサイトが稼働中であり、今後も類似のサイトが公開される可能性もあるとし、このようなフィッシングサイトにてMy SoftBank ID（携帯電話番号、パスワード等）を絶対に入力しないよう呼びかけており、また、ソフトバンクでもフィッシングサイトの一例を画像で示し、URLが正規のMy Softbankログイン画面のもの（id.my.softbank.jp）か確認するよう呼びかけています。

AUS便りからの所感等

- 今回のフィッシングは少なくとも4月12日頃から確認されており、比較的巧妙に本物に偽装した内容とされています。

- 多くの例と同様、フィッシングサイトはURLが「http://」となっておりますが、近年は無料でSSL証明書を発行できるサービスが話題となっており、いつフィッシングサイトで利用されてもおかしくはありません。

SoftBank

ソフトバンクを装う電子メールに関するご注意

ツイート いいね！0

掲載日：2018年4月18日

ソフトバンクのメールサービス※1宛に、ソフトバンクが送信元であるかのように装った、フィッシング目的の不審なメールが確認されています。このような不審なメールを受信した際は、メール本文のURLリンクをクリックしたり、万が一クリックしたとしても、My SoftBankの携帯電話番号とパスワードの入力、ワンタイムパスワードの入力をしないようご注意ください。

※1 「○○○@i.softbank.jp」または「○○○@softbank.ne.jp」のメールアドレスを指します。

- フィッシングに対する自衛策としては、Webブラウザ・アンチウイルスおよびUTMのアンチフィッシング機能を有効に活用することの他、本物のログインページをブラウザのブックマークに登録してそこからアクセスすることが挙げられます。