— AUS（アルテミス・ユーザ・サポート）便り 2018/04/09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。

●パスワードの定期的な変更はNG…総務省が方針転換

https://cybersecurity-jp.com/news/23329
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html

このニュースをザックリ言うと・・・

- 3月下旬、総務省がWebサイトにおいて推奨していた「パスワード管理ルールに方針転換があった」として、日経新聞やNHK等で報じられています。

- これまで同省のサイトでは「パスワードを定期的に変更し、使い回さない」こととしていましたが、
◆実際にパスワードを破られアカウントが乗っ取られたり、サービス側から流出した事実がなければ、パスワードを変更する必要はありません
◆むしろ定期的な変更をすることで、パスワードの作り方がパターン化し簡単なものになることや、使い回しをするようになることの方が問題となります
として、ここ数年有力な意見となっていた「定期的な変更は不要」へと改められています。

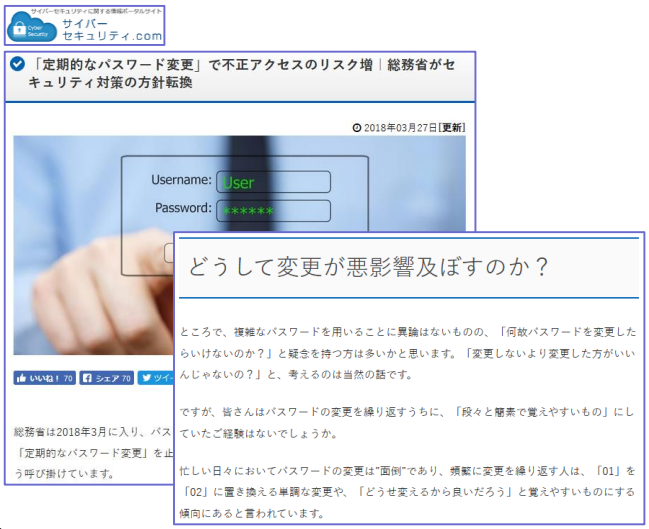
- この他の「パスワードを使い回さない」こと、あるいは「自分や家族の名前」「辞書に載っているような一般的な英単語」「短すぎる」等の文字列は使わないこと については、これまで同様に推奨事項として挙げられています。

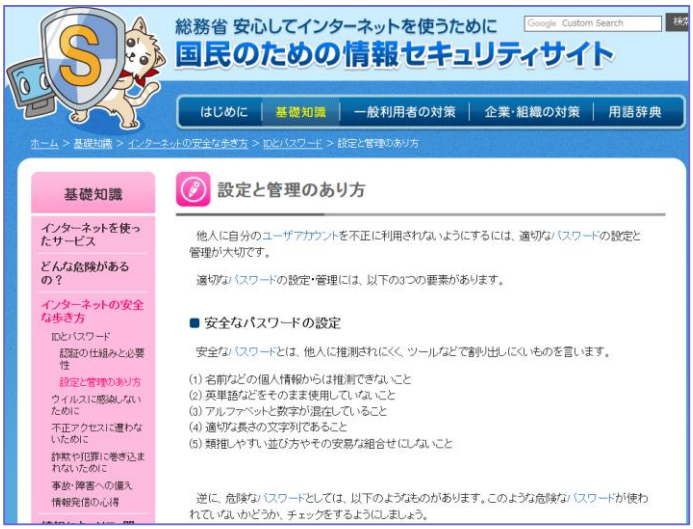
AUS便りからの所感等

- 念頭に置いてほしいのは、文字数や使用可能な文字の種類が多ければ多いほど安全なパスワードとなる余地ができるということであり、「パスワード」という言葉に引っ張られることなく、例えば関連性のない複数（3つ以上）の単語や、他の人が思いついたり推測したりしないような「一文」をパスワードとすること も検討に値します（こういった長いパスワードを「パスフレーズ」と呼ぶこともあります）。

- また、組織内でのアカウントを発行する場合やユーザが登録するサービスを提供する場合において、設定可能なパスワードとして「8文字以内」や「英数字のみ」といった制限を設けることは、前述したパスフレーズを使う余地も与えず、ユーザを危険に晒すことになりかねませんので十分に注意してください。

- 一部報道において、一般的な英単語の一部の文字を「O(ゼロ)→O(オー)」「1→i(アイ)」「a→@」のように変えて使うことを推奨するものもありましたが、近年のブルートフォース（総当たり）攻撃用のツールではこういったものには対応済みであるため危険とされており、そもそも「パスワードを定期的に変更する」ことも長年の間有効なものとされていた経緯があり、ある時点で推奨されていたことが数年後には否定されるという事態は今後も起きることでしょう。





●「iPhone X獲得のチャンス」…日本郵便やGoogleをかたる当選詐欺サイトに注意

https://twitter.com/nisc_forecast/status/981705655592431616

このニュースをザックリ言うと・・・

- 4月2日（日本時間）以降、日本郵便や内閣サイバーセキュリティセンター（NISC）より、日本郵便等をかたるフィッシングサイトが確認されているとして注意が呼び掛けられています。

- トレンドマイクロ社の解説で挙げられているフィッシングサイトの一例では、iPhone XやサムスンのGalaxyスマートフォンを獲得する、あるいはiPhone 7を100円で購入できるキャンペーンと誤認させ、クレジットカード情報を入力させるものとなっています。

- Twitter上では、日本郵便の他にGoogleからのキャンペーンをかたるものも同時期に確認されています。

AUS便りからの所感等

- 今回のフィッシングサイトも「https://」ではなく「http://」のサイトが多く見られ、特にGoogleについては、同社があらゆるサービスにおいて常時HTTPS化を進めており、そういう点からも疑うことができるでしょう。

- しかし近年話題となっているLet's Encrypt等の無料でSSL証明書を発行できるサービスがそのうちフィッシングサイトでも使われるようになれば、「https://」を使っているかどうかで見抜くことがいつ無意味になってもおかしくありません。

- Google Chromeブラウザのアンチフィッシング機能では既に今回発生したようなフィッシングサイトに対応し遮断するケースもあるようで、フィッシングに騙されないようにするため、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全て活用し、かつ本物のログインページにはブラウザのブックマークからアクセスするといった自衛策をとる等を心がけるようにしましょう。

●クレジットカード情報約6700件流出…原因は暗号化通信ソフトの脆弱性

https://netshop.impress.co.jp/node/5020

このニュースをザックリ言うと・・・

- 3月30日（日本時間）、調味料等の通信販売サイト「トキワオンラインショップ」運営元の常盤商事より、同サイトで2017年11月1日までに発生していたとされる個人情報流出についての詳細が発表されました。

- 流出は2017年12月20日の時点で第一報が発表されており、2016年10月23日～2017年11月1日の間に同サイトで決済に使われた最大6679件のクレジットカード情報（会員名・番号・有効期限・セキュリティコード）が被害を受けていたとされています（会員のパスワードは流出していなかったとのことです）。

- 今回の発表では、委託先の会社が構築したサーバにおいて、暗号化通信ソフトウェア「OpenSSL」の古いバージョンが使われており、脆弱性を悪用して外部からの不正アクセスを受けたことが流出の原因と結論付けています。

AUS便りからの所感等

- OpenSSLはインターネットの暗号化通信の基盤として広く使われているソフトウェアですが、2014年4月に「Heartbleed」と呼ばれる、サーバ上のメモリが読み取られる可能性がある脆弱性が発見されたのをはじめ、時々脆弱性が発見されることがあります。

- Heartbleedの存在が発表されて3年たった2017年7月、その脆弱性を突いた攻撃によりクレジットカード情報が流出する事件も発生しており、今回については、実際にそれが原因だったと確定したわけではありませんが、問題となったサーバで使われていたOpenSSLのバージョンもHeartbleedの脆弱性があるものでした。

- Linux OSにおいては可能な限りディストリビューションが提供するパッケージからソフトウェアをインストールし、またセキュリティパッチを含むアップデートを一括管理で行うべきであり、バージョンアップについても計画的に行うことが肝要です。