— AUS（アルテミス・ユーザ・サポート）便り 2016/07/11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。

●パスワードの定期変更をユーザに求めるべきではない･･･NISTの文書でも明示へ

http://internet.watch.impress.co.jp/docs/yajiuma/1007177.html
http://nlab.itmedia.co.jp/nl/articles/1606/28/news127.html

このニュースをザックリ言うと･･･

- 6月23日（米国時間）、米国国立標準技術研究所（NIST）傘下のコンピュータセキュリティ研究部門Computer Security Division（CSD）が発行した、ログイン等の認証に関するドラフト文書「SP 800-63B」において、パスワードの適切な管理に関する推奨事項が述べられています。
- 当該文書では、パスワードの変更について「定期的な変更を求めるべきでない」「(不正ログイン等の)攻撃を受けた証拠がある場合にのみ、例外として変更を求めるべきである」としています。
- また、パスワードのヒント等で用いる、いわゆる秘密の質問についても「登録させるべきではない」等ともしています。
- なお、CSDの文書は、米政府機関が行うセキュリティ対策の指針とされる他、世界中の政府機関・民間企業の参考にもされています。

AUS便りからの所感等

- パスワードの変更に関する議論は長年続いていますが、セキュリティ技術者の間では、国内で依然として重要視されている「定期変更する」というルールの実効性に疑問が呈されており、例えば「Password1」等、元のパスワードに数字を足したりするだけの変更をユーザが行う可能性も指摘されています。
- そして、近年目立つようになった連鎖的な不正ログイン事件を鑑み、各サービスでのパスワードの使い回しを避ける方がよほど重要であるとする意見が有力です。
- とにかく、攻撃者から推測されにくいパスワードを設定させることが重要であり、また、マルウェアの侵入やフィッシングによるパスワード奪取の恐れも考慮し、アンチウイルスやUTMによる対策も欠かせません。

INTERNET Watch
やじうまWatch

「パスワードの定期変更をユーザーに求めるべきではない」……NISTの文書でついに明示へ

tks24　2016年6月27日 05:55

NIST（米国国立標準技術研究所）の傘下部門であるCSD（Computer Security Division）が発行する文書のひとつ、Special Publicationは、米国の政府機関がセキュリティ対策を実施する際の指針になる文書として、世界中で一目を置かれる存在だ。そんな中、先週末にドラフトとして公開された文書「800-63B」の「5.1.1.2. Memorized Secret Verifiers」が、これまでのパスワード定期変更論争に終止符を打つものとして注目を集めている。詳細は原文を当たられたいが、パスワードの定期変更では「Password1」といった具合に末尾に数字を追加するなど、その規則性が容易に推測できることなどから、システムはパスワードの定期的な変更をユーザーに要求すべきではないというもの。併せて秘密の質問も使用するべきではないとしており、今後のさまざまな認証システムの開発に多大な影響を与えることは確実だ。攻撃を受けた証拠がある場合は例外だと明記されていること、またこの文書そのものが現時点ではまだドラフトであることは留意する必要があるが、このままいくと、パスワードを定期変更を要求されることが過去のものになる日は近そうだ。

- DRAFT NIST Special Publication 800-63B（NIST）
  https://pages.nist.gov/800-63-3/sp800-63b.html

ねとらぼ

» 2016年06月28日 15時34分 更新

「パスワードの定期変更はすべきでない」　米研究機関がセキュリティ対策関連の文書で明言

「秘密の質問」も使用してはならないとも記載されています。

[斎藤真二，ねとらぼ]

アメリカの科学研究機関NIST（米国国立標準技術研究所）のコンピューターセキュリティ担当部門、CSD（Computer Security Division）が発行した文書「800-63B」が注目を集めています。デジタル認証のガイドラインとして書かれたもので、パスワードに関する項目に、「パスワードの定期変更はすべきでない」と明記。セキュリティの常識を変える可能性があります。

焦点となった文言は、「5.1.1.2. Memorized Secret Verifiers」に記載。「ユーザーが攻撃を受けたとの証拠の下に変更を要求した場合を除き、認証側は定期的にパスワードの変更を求めるべきではない」と述べられています。パスワードの定期変更を促すWebサービスは多いですが、ユーザーが前のパスワードに数字を加えるなど、予測しやすい変更を行ってしまいがちなのも事実。そういった観点からの記述と思われます。

同項目では、例えば「最初に飼ったペットの名前は？」といった、いわゆる「秘密の質問」についても否定。パスワードのヒントとなるものに、本人以外のアクセスを許可すべきではないとしています。

●Adobe、7月13日にAcrobatとReaderのセキュリティアップデートを予告

http://www.itmedia.co.jp/news/articles/1607/08/news061.html

このニュースをザックリ言うと・・・

- 7月7日（日本時間）、Adobe社は同社のPDFリーダー（Acrobat Reader DC・Adobe Reader XI）、およびAcrobatのセキュリティアップデートを7月13日（同じく日本時間）にリリース予定であることを発表しました。

- 詳細は不明ですが、修正される脆弱性は複数あり、現在の最新バージョンを含むすべてのバージョンに存在する模様です。

- なお、最近の傾向から、同日には同社のFlash Playerについてもアップデートがリリースされる可能性がありそうです。


ITmedia ニュース

速報

2016年07月08日 07時36分 更新

Adobe、AcrobatとReaderのセキュリティアップデートを予告

深刻な脆弱性を修正するアップデートを米国時間の7月12日に公開する。この日はMicrosoftも月例セキュリティ情報を公開する見通し。

[鈴木聖子，ITmedia]

米Adobe Systemsは7月7日、Adobe AcrobatとReaderのセキュリティアップデートを米国時間の12日に公開すると予告した。

アップデートはWindows版とMac版が対象。連続トラックのAcrobat DC／Acrobat Reader DC 15.016.20045までのバージョンと、クラシックトラックの15.006.30174までのバージョン、およびデスクトップ向けAcrobat XI／Reader XI 11.0.16までのバージョンに存在する複数の深刻な脆弱性に対処する。

AUS便りからの所感等

- Adobeがこの日に月例のセキュリティアップデートをリリースするのは、同日にMicrosoftが行う同様のリリースに合わせてのもので、ここ数年間に多くのベンダーがMSに倣い、この日にリリースを行う傾向が定着しています。

- Adobe Reader X（XIの一つ前のバージョン）は昨年11月にサポートが終了しているため、もしそれ以前のAdobe Readerを利用し続けている場合は、必ずアップグレードを行ってください。

- PDFリーダーの脆弱性を悪用されるケースは、大抵が不正なPDFファイル等を開くことによるものであり、ブラウザに組み込まれたプラグインから呼び出されるケースを狙い、Webから不正なファイルをダウンロード・表示させるケースも珍しくありません。

- こういったケースを少しでも回避できるよう、普段からのアップデートと、アンチウイルスやUTMによる多重防御が肝要です。

●イギリス大企業の49%以上が退職者アカウントを削除していない

http://internet.watch.impress.co.jp/docs/column/security/1008598.html

このニュースをザックリ言うと・・・

- 6月1日（現地時間）、アクセス権管理ソリューションを提供する英8MAN社より、イギリスの従業員1000人以上の企業に属しているIT専門家100名に対して行った、退職者のアカウントの処理に関する調査結果が発表されました。

- 調査では、「退職時に確実にアカウントを削除している」という回答は34%である一方、「離職1ヶ月後まで保持」13%、「6ヶ月後まで保持」23%、「1年後まで保持」9%、「1年以上後もアカウントにアクセス可能」4%となり、合わせて49%が「すぐに削除していない」という結果となりました。

- この他、「すぐに削除していない」とされたアカウントの持っていた権限に関する調査で、「ネットワーク上のファイル等へのアクセス」65%、「メールへのアクセス」55%、「システムの管理者権限」が実に22%に上っていた、等の結果が出ています。

INTERNET Watch

	全体	従業員1000～3000人	従業員3000人～
離職後1カ月後まで保持	13%	10%	16%
離職後6カ月後まで保持	23%	30%	16%
離職後1年後まで保持	9%	10%	8%
離職後1年以上でまだアクセス可	4%	6%	2%
そのようなことはない	34%	26%	42%
分からない（確認したことがない）	17%	18%	16%

AUS便りからの所感等

- 退職者のアカウント、特にメール送受信や社内LANへのリモートアクセスといったものについては、そのまま放置しておくと第三者のみならず、時には既に退職した本人が悪用する恐れがあります。

- 一方で、外部から直接アクセスできない場所（社内ネットワーク上のサーバ等）でのアカウントであっても、やはり放置されていると、リモートアクセスを踏み台にする等で侵入した攻撃者にとって格好のターゲットとなり得るでしょう。

- 全てのユーザアカウントを洗い出して適切な管理下に置き、ユーザの退職時には、所有していたメール・文書等のデータを確保し、後任のユーザに移行させた上で確実に削除することが重要です。

- 退職者アカウントへの不正アクセスの試行、あるいは乗っ取られたアカウントからの不正行為を検知するため、IDS・IPSの設置も検討すべきです。