注目されているセキュリティ事故・事件に関する情報 ＜2018年6月版 (第25号)＞(選り抜き版)

2018年6月28日
ＮＴＴデータ先端技術株式会社
セキュリティ事業部

今回のサマリー

「パスワードの定期変更は不要！」
～ 今見直そう、パスワードの設定と運用 ～
パスワードに関する取り扱い方針について、2017年以降に総務省(MIC)や経済産業省(METI)、日本情報経済社会推進協会(JIPDEC)などが相次いで方針転換を行いました。不正アクセスの対策として、従来は定期的なパスワード変更が推奨されていましたが、現在は定期変更は不要であり、より強固なパスワードを用いることが推奨されはじめています。方針転換に至った背景と、企業・個人が取るべき対応について解説します。

「パスワードの定期変更は不要！」
～ 今見直そう、パスワードの設定と運用 ～

1. 行政機関や団体がパスワードの取り扱いについて方針転換 (1/2)

　パスワードに関する取り扱い方針について、2017年以降に総務省(MIC)や経済産業省(METI)、日本情報経済社会推進協会(JIPDEC)などが相次いで方針転換を行いました。
　不正アクセスの対策として、従来は「パスワードは定期的に変更すること」が推奨されてきましたが、**今回の方針転換**により**「パスワードの定期変更は不要。その代わりにパスワードは強固なものを1回設定すること」が推奨**されるようになりました。

1. 行政機関や団体がパスワードの取り扱いについて方針転換 (2/2)

以下に方針転換を表明した主な行政機関や団体を示します。

時期	組織	動き	パスワードの定期変更に関する記述
2016/11	個人情報保護委員会 (PPC)	『個人情報の保護に関する法律についてのガイドライン』を発刊(☆)	当該ガイドラインには、パスワードの定期変更に関する記述なし
2017/5	経済産業省 (METI)	『個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン』を廃止し、個人情報保護委員会が定める『個人情報の保護に関する法律についてのガイドライン』に一元化することを表明(☆)	廃止される『個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」には「パスワードの有効期限を定めることを推奨する」旨が明記されていた
2017/6	米国国立標準技術研究所 (NIST)	『NIST SP 800-63 : Electronic Authentication Guideline』を発刊	当該書には「パスワードの定期変更は必要なし。流出時は変更が必要となる。(弊社訳) 」旨を明記されている
2017/9	総務省 (MIC)	『電気通信事業における個人情報保護に関するガイドライン(H29.4.18版)』を発刊	当該ガイドラインでは、一つ前の版(H27.6.24版)で記されていた「技術的保護措置(パスワードの定期変更)を適切に実施することが必要である」旨が削除された
2017/12	内閣サイバーセキュリティセンター (NISC)	『情報セキュリティハンドブック』を発刊	当該ハンドブックには「パスワードの定期変更は必要なし。流出時は速やかに変更することを推奨する」旨が明記されている
2018/3	総務省 (MIC)	『国民のための情報セキュリティサイト』を公開	当該サイトには「パスワードの定期的な変更が不要」であることが明記されている
2018/4	日本情報経済社会推進協会 (JIPDEC)	プライバシーマーク認定時の審査基準となる『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【第2版】』を発刊(☆)	当該ガイドラインでは、第1版で記されていた「パスワードの有効期限を設定している」の項が削除された

※自組織の動きが、他の組織に大きく影響を及ぼしたと推測できるものについては、星マーク(☆)で表記しています

上記の他にも追従する動きを見せる行政機関や団体が増加しています。
次頁からは、貴社を管轄する行政機関がこの方針転換に追従した場合に備え、どのような対応を検討すべきであるかについて説明します。

2. 従来はなぜ定期的な変更が推奨されてきたか (1/2)

対応内容を考えるにあたり、まずは従来推奨されてきた方針の狙いを紐解いていきます。従来の方針で示されていたパスワードのポリシとして以下の基準が挙げられます。

基準	
文字長	8文字以上
文字種	英大文字/英小文字/数字/記号の内、3種類以上を使用
パスワードの定期的な変更	必要 (頻度は最低1年に1回)

これはアメリカ国防総省(DoD)が2004年に発刊した文献(引用元1.参照)で示された基準に基づくものだとされています。2004年当時のPCの処理速度では、この基準を満たすパスワードを解読するためには1年程度必要でした。

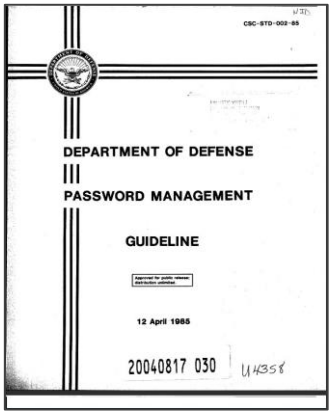
この1年という数字を根拠に、1回/年の周期より短い周期でパスワードの変更を行うことで、攻撃者にパスワードを解読される確率を低減する狙いがありました。

※引用元1：Department of Defense Password Management Guideline
<http://www.dtic.mil/dtic/tr/fulltext/u2/a425705.pdf>
※引用元2：パスワードの最大解読時間測定
<http://www.dit.co.jp/service/security/report/03.html>

文字列(パスワード等)の強度を考慮した文字長 = M
L = 文字列の有効期間
R = 文字列の推定回数
P = 文字列が破られる確率
A = 文字種類
$M = \log_{10}(L*R/P) / \log_{10}(A)$

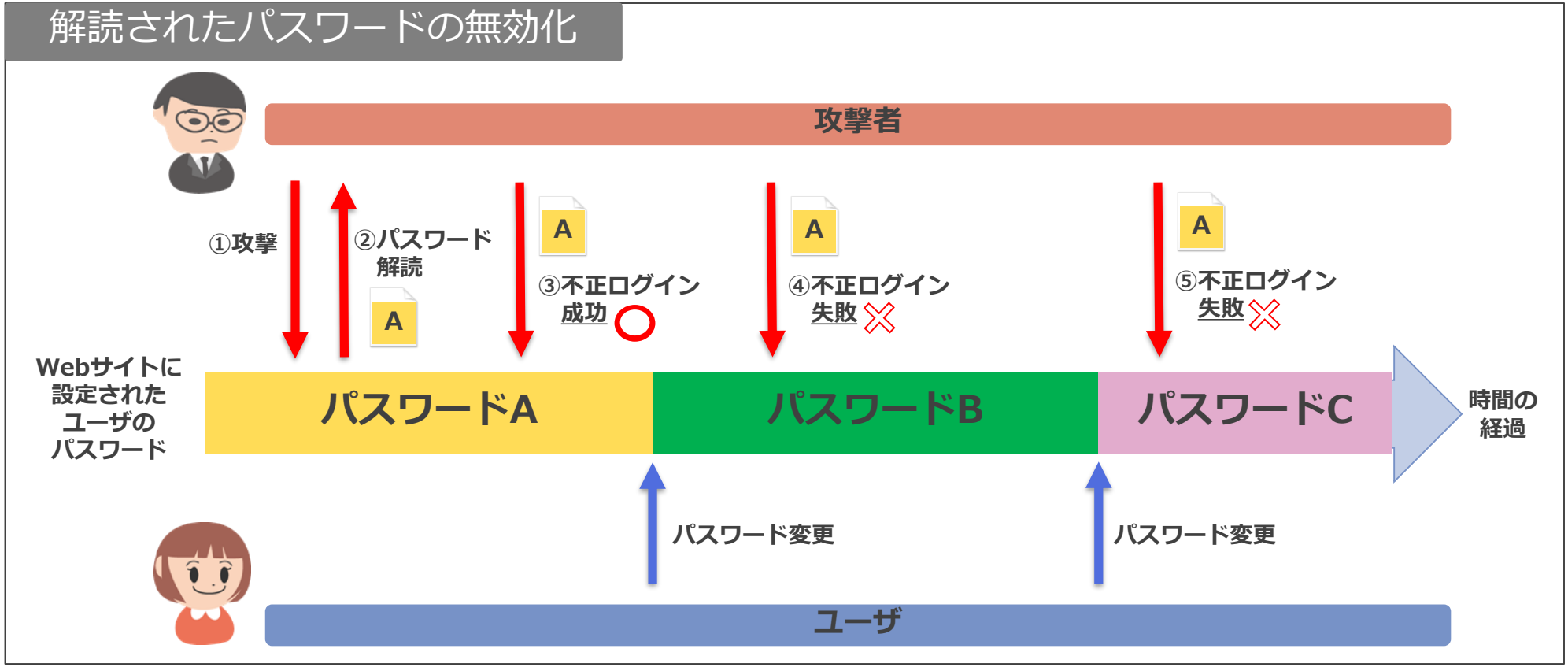
(計算例)
L = 1年間 = 24時間×365 = 8760時間
R = 1秒10回 = 1時間36000回
P = 1/1000000
A = 英小文字 + 英大文字 + 数字 = 62種

$M = \log_{10}(8760*36000/(1/1000000)) / \log_{10}(62)$ = 約 8.08 桁



2. 従来はなぜ定期的な変更が推奨されてきたか (2/2)

　また、パスワードを定期的に変更することで、攻撃者にパスワードを解読された場合に解読されたパスワードを無効化する副次的な効果も見込めるといった主張もありました。



3. 運用していく中で見えた効果の薄さ

　ただし、この対応は2018年時点ではあまり効果的ではありません。原因としてPCの処理速度が向上したことが挙げられます。
　パスワードの解読に1年程度要すると結論付けられたのは、あくまで2004年時点でのPCの処理速度に基づくものです。2012年時点で13.5時間で解読することができたという情報があり、この数値に基づくのであれば半日に1回パスワードを変更しなければなりません。また2018年時点ではさらに短い周期での変更が求められることとなります。
　これは運用として現実的な周期ではありません。

　またこの運用を続けていく中で、ほとんどのユーザが「同一のパスワードを繰り返し設定する」ようになりました。人間である以上、覚えていられるパスワードには限界があり、同一のパスワードを使用することは仕方がないことなのかもしれませんが、結果としてパスワードの定期変更がより効果の低い対策となってしまいました。

　そのため今回の「**パスワードの定期変更は不要**。その代わりに**パスワードは強固なものを1回設定する**こと」という方針転換に至ったとされています。

4. どのようなパスワードを設定すべきか (1/3)

　ではユーザはどのようなパスワードを設定すべきなのでしょうか？
設定すべきパスワードを示すにあたり、「従来推奨されていた”強固なパスワード”の根拠」と「パスワードを解読/推定する攻撃手法」について考えてみます。

　まずは「従来推奨されていた”強固なパスワード”の根拠」になりますが、こちらは既に説明をしたとおりです。アメリカ国防総省(DoD)が2004年に示した数値から、以下の基準を満たすパスワードを設定することで十分な強度を満たすと捉えられてきました。

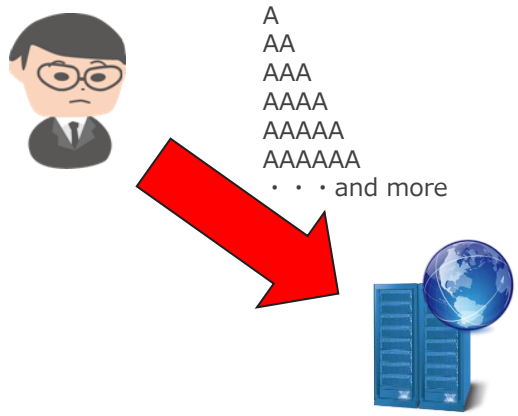
基準	
文字長	8文字以上
文字種	英大文字/英小文字/数字/記号の内、3種類以上を使用

　そして「パスワードを解読/推定する攻撃手法」について、さまざまな手法のうち代表的なものを3つ、次頁に示します。

4. どのようなパスワードを設定すべきか (2/3)

パスワードを解読/推定する攻撃手法

総当たり攻撃

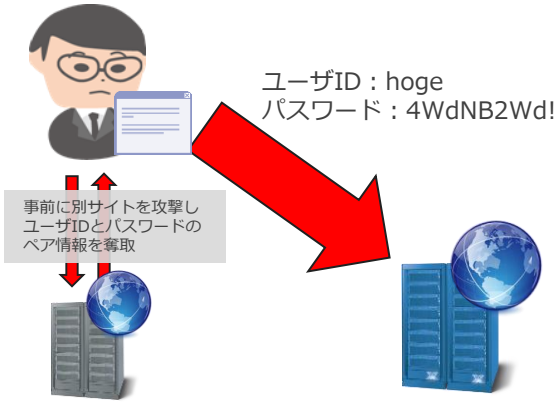


すべての組み合わせの
文字列を試す

辞書攻撃

パスワードとしてよく使用される
フレーズを試す

リスト型攻撃



他のサイト等で奪取した
パスワードを試す

攻撃手法	手法概要	効果的な対策方法
総当たり攻撃	すべての組み合わせの文字列を試す	全てのパターンを施行するため、時間は要しますが、理屈的には必ずいつかパスワードは見破られます。 容易に見破られないようにするためには、後述する”強固なパスワード”を設定することが効果的です。
辞書攻撃	パスワードによく使用されるフレーズを試す	意味のあるフレーズや、ユーザID/個人情報に関連するようなフレーズを避けることが効果的です。
リスト型攻撃	他のサイト等で奪取したパスワードを試す	ユーザIDとパスワードを複数のサイト/システムで使いまわしている場合に、他の攻撃手法と比較して短時間/高確率でパスワードが破られます。 パスワードのフレーズそのものより、使いまわさないようにする運用面の対策が効果的です。

4. どのようなパスワードを設定すべきか (3/3)

以上のことを踏まえ、ユーザは以下の基準を満たすパスワードを設定すべきであるといえます。

弊社が推奨する基準		参考：NISCの推奨する基準
文字長	10文字以上	同左
文字種	英大文字/英小文字/数字/記号の内、4種類を使用	同左

上記基準を満たすパスワードであれば、先述の2012年の試算でも解読するのに341年程度必要であることとなり、システムのライフサイクルを考慮すると、十分な強度を満たしているといえます。

ただしこれは先述の「総当たり攻撃」に対する強度であり、設定したパスワードに”よく使用されるフレーズ”(※)が含まれていたり、複数のサイト/システムで使いまわしているような場合、「辞書攻撃」や「リスト型攻撃」により容易に見破られてしまいますので注意が必要です。

※一部では、複数のフレーズの組み合わせで構成される長い文字列をパスワードにするという手法も取られています

5. 企業側はどのような対応が必要か (1/2)

企業側の対応としてはユーザが強固なパスワードを設定できるよう、環境を整備していくことが重要となります。

具体的には、大手B2CサイトであるJAL社やANA社のマイレージ会員サイトがかつてパスワードを数字4桁でしか設定できないような作りとしていたように、サイト/システム側で脆弱なパスワードしか設定できない仕様としてしまっていないか、**サイトの要件や仕様を見直す**ことから始めてください。

また特別の要件がない限りは、**強固なパスワードしか設定できないようにサイト/システム側で強制**することも、ユーザに安心してサービスを活用してもらうために有効な対応となってきます。

その他、万が一認証を突破されたケースを想定して、認証が行われるタイミングや、普段と異なる端末やIPアドレスからのアクセスがあったタイミングで、あらかじめ登録されたユーザの**メールアドレスにメールを送信**することも、ユーザの助けを借りて早期にインシデントの発生に気づくための取組として有効な対応といえます。

5. 企業側はどのような対応が必要か (2/2)

　さらに、金銭情報や個人情報など重要な情報を取り扱うサイト/システムである場合は、**二要素認証の導入**も検討してください。
　知っている要素(パスワード)の他に、持っている要素(ハードウェア/ソフトウェアトークン)や本人である要素(SMS/メール)を取り入れることでより強固な認証システムを築くことが出来ます。
　その他の代替手段として、コンピュータによる機械的な総当たり攻撃を防止するためにCAPTCHAなどを採用するサイト/システムも増えてきています。各々のサイト/システムの特性に合わせて検討してください。

CAPTCHAに代表される認証方式

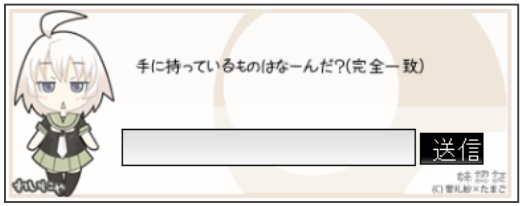
CAPTCHA

人間にしか判読できない文字を
表示し入力させる

画像選択認証

指定[猫]の画像のみを選択させる
(機械で判別することは困難)

問いかけ認証



絵と文書の内容を理解させたうえで
その答えを入力させる

いずれも、コンピュータによる機械的な認証を困難にするための仕組みとして用いられています

※引用元：妹認証　<http://www.okanesuita.org/auth_sister/>
　　ねこ認証　<http://magic3.net/item_988.html>

6. 個人側はどのような対応が必要か

　個人側の対応としては、先述の「どのようなパスワードを設定すべきか」で示したとおり、**強固なパスワードの設定**と**運用面の見直し**を行ってください。

　再掲も含みますが、先に挙げた対応の他、以下のような取り組みも効果的ですので検討するようにしてください。

対応のポイント		
強固なパスワードの設定	文字長	10文字以上
	文字種	英大文字/英小文字/数字/記号の内、全ての種類を使用
運用面の見直し	よく使用されるフレーズをパスワードに含めない	
	複数のサイト/システムでパスワードを使いまわさない (ユーザIDの扱いも同様で、複数のサイト/システムで使いまわさないことが重要)	
	パスワードを単純化/パターン化しない (パスワード1:[gsHeh**1**f!fh]、パスワード2:[gsHeh**2**f!fh]　赤字部分以外同一)	
	httpのサイトや、暗号化されていないメールでパスワードの登録や授受を行わない	
	家族/友人/知人にパスワードを伝えない (特にSNSへ書き込むなど、第三者の目に触れることがないよう注意が必要)	

7. まとめ

　従来安全とされてきた基準も、コンピュータの処理速度の向上など技術の進歩や人の運用次第で、陳腐化するケースがあります。

　企業側は、技術動向だけでなく、関連する省庁などの動向を見守るとともに、ユーザがよりセキュアにサイト/システムを使用できるよう、仕様などの見直しを行ってください。

　ユーザ側も現在と過去、それぞれで安全とされてきた基準とその根拠を知識として知ったうえで、自身がどのような対応をとるべきであるか考える必要があります。
　今回世間的にも基準が大幅に見直されたため、一度自身の対応を見直してみる良いタイミングとしてください。

8. 参考URL (1/2)

- 個人情報保護委員会(PPC)：個人情報の保護に関する法律についてのガイドライン (通則編)
  https://www.ppc.go.jp/files/pdf/guidelines01.pdf
- 個人情報保護委員会(PPC)：個人情報の保護に関する法律についてのガイドライン (外国にある第三者への提供編)
  https://www.ppc.go.jp/files/pdf/guidelines02.pdf
- 個人情報保護委員会(PPC)：個人情報の保護に関する法律についてのガイドライン (第三者提供時の確認・記録義務編)
  https://www.ppc.go.jp/files/pdf/guidelines03.pdf
- 個人情報保護委員会(PPC)：個人情報の保護に関する法律についてのガイドライン (匿名加工情報編)
  https://www.ppc.go.jp/files/pdf/guidelines04.pdf
- 総務省(MIC)：電気通信事業における個人情報保護に関するガイドライン
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html
- 総務省(MIS)：国民のための情報セキュリティサイト
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html
- 経済産業省(METI)：コンピュータ不正アクセス対策基準
  http://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm
- 米国国立標準技術研究所(NIST)：Digital Identity Guidelines
  https://pages.nist.gov/800-63-3/
- 内閣サイバーセキュリティセンター(NISC)：情報セキュリティハンドブック
  https://www.nisc.go.jp/security-site/handbook/index.html
- 日本情報経済社会推進協会(JIPDEC)：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【第2版】
  https://privacymark.jp/system/guideline/pdf/guideline_V2_180410.pdf
  https://privacymark.jp/system/guideline/pdf/guideline_V2_shinkyu180410.pdf

8. 参考URL (2/2)

- PCISSC：PCI DSS v3.2
  https://www.pcisecuritystandards.org/document_library
- 金融情報システムセンター(FISC)：金融機関等におけるセキュリティポリシー策定のための手引書 第2版
  <Web公開なし>
- ISMS：JIS Q 27002_2014 [ISO/IEC 27002_2013]
  http://kikakurui.com/q/Q27002-2014-01.html
- マイナビニュース："パスワードの定期変更"はもはや無意味! セキュリティの現実を直視すべし
  https://news.mynavi.jp/article/20130731-itsummit/
- アメリカ国防総省(DoD) ：Department of Defense Password Management Guideline
  http://www.dtic.mil/dtic/tr/fulltext/u2/a425705.pdf
- ディアイティ：パスワードの最大解読時間測定
  http://www.dit.co.jp/service/security/report/03.html

NTT DATA

Trusted Global Innovator