Tya-net Newsletter
富山大学
総合情報基盤センター
No.49

重要

パスワード管理特集

パスワードは，コンピュータやネットワークを利用する上でなくてはならないものです。このパスワードが他人に知られてしまうと，あなたの大切な情報が悪用されてしまいます。

次の４つの事項に注意し，パスワードを適切に管理しましょう。

(1) 適切な文字列のパスワードを設定する
(2) パスワードを使いまわさない
(3) パスワードは正しく保管する
(4) パスワードは正しいタイミングで変更する

適切な文字列のパスワード

攻撃者は，コンピュータを使ってパスワードを解析します。数字だけのパスワード（例：123456）はコンマ数秒で解析されてしまいます。簡単なパスワードは，攻撃者に「どうぞ利用してください」と言っているようなものです。次のルールを遵守した文字列を利用しましょう。

- ○ 名前などの個人情報から類推されない文字列であること
- ○ 英単語など辞書に掲載されている文字列は使用しないこと
- ○ アルファベット（大文字／小文字），数字，記号が混在していること
- ○ 適切な文字数（８文字以上）であること

Check!

パスワードの使い回し禁止

最近，ダークネットと呼ばれる裏世界のマーケットにおいて，漏洩したID／パスワードの組み合わせ情報が売買されているという報道を耳にした方は多いと思います。セキュリティ関係機関から情報提供を受け，ダークネット上に流通しているデータを解析したところ，[u-toyama.ac.jp]を含むデータが187件見つかり，そのうち4件が学内システムのパスワードと一致しました。

ダークネットへの流通経路は不明ですが，一度流通したデータは瞬く間に攻撃者間で共有され，消去されることはありません。攻撃者は入手したID／パスワードの組み合わせを利用し，すぐに他のサービスへ不正アクセスを試みます。

複数のサービスでパスワードを使い回した場合，どこかのサービスで情報が漏洩すると，連鎖的に被害に遭うことになりますので，サービス毎に異なる文字列のパスワードを設定しましょう。

パスワードの保管

サービス毎に異なるパスワードを設定すると，たくさんのパスワードを管理することになり，忘れる可能性が高くなります。では，たくさんの異なるパスワードを忘れないためにはどうすればよいのでしょうか。

i メモを利用する
IDとパスワードを紙にメモして，人目のつかない鍵のかかる場所に保管する

ii パスワード付電子ファイルを利用する
WordやExcelには，パスワードが設定できます。WordやExcelの１ファイルにIDとパスワードをメモして，パスワード付きで保存することで，１つのパスワードを記憶するだけで済みます。　※ただし，ファイルは厳重に管理しましょう。

iii パスワード管理ソフトを利用する
パスワード管理するためのソフトウェアがあります。このようなソフトウェアを利用することで，１つのマスターパスワードを管理するだけで，必要に応じたパスワードを自動入力してくれます。
例）Password Manager,1Passwordなど

パスワードの変更

以前は，パスワードは定期的に変更するべきだと言われていましたが，統計調査によると，定期的なパスワード変更の強制は，同一パスワードの使い回しや再利用などを誘発し，セキュリティの向上にはつながらないことが判明しました。

現在では，定期的なパスワード変更を強制するのではなく，パスワード漏洩の可能性（※）が発生した段階で，変更することが推奨されています。

※海外のホテルなど，セキュリティレベルの低い（もしくは不透明な）ネットワークを利用した場合や，利用承認書を紛失した場合など，「自分以外の誰かにパスワード情報が入手される可能性が少しでも発生した場合」と定義。

ダークネットには
- 攻撃者によってハッキングされたサイトから漏洩した情報
- フィッシングメールによって漏洩した情報
- ウイルス感染によって漏洩した情報

など，セキュリティ事案によって漏洩した様々な裏情報が流通しています。ダークネットに流通した情報の回収／削除は不可能なので，「セキュリティ事案を起こさないこと」が重要です。

富山大学 総合情報基盤センター
2018年8月8日
http://www.itc.u-toyama.ac.jp/
内線：6946（五福）

▶ バックナンバー：http://www.itc.u-toyama.ac.jp/cn/

セキュリティ対策情報

長期休暇中に使用しない機器は
1. LANケーブルを抜いて
2. シャットダウン
が一番安全!
(休暇明けの復旧をお忘れなく)

長期休暇に伴うセキュリティ対策について

長期休暇を狙ったサイバー攻撃が世界各国で増加しています。各人が適切に対策を実施しなければ甚大な被害が発生する場合があります。以下にセキュリティ対策方法等を簡潔にまとめましたので，必ずご確認願います。

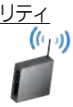
なお，不審な点を発見された場合は，最寄の総合情報基盤センターへ早急にご相談ください。

Check! パソコン編

- □ OSに修正プログラムを適用する
  - □ Windows → Windows Update
  - □ Mac → ソフトウェア・アップデート
- □ 導入しているアプリケーションに修正プログラムを適用する
  - □ Adobe製品全般（特にReader/Acrobat）
  - □ Java　□ Flash
  - □ JustSystem製品全般（特に一太郎）
- □ ウイルス対策ソフトの定義ファイルを最新の状態に更新し，完全スキャンを行う　重要！

Check! ネットワーク機器編

- □ ネットワーク機器（複合機やルータ等）に適切なセキュリティ対策を行う
  - □ 最新のファームウェアを適応する
  - □ 管理画面へ適切なパスワード設定する
  - □ セキュリティ機能を活用し，適切な設定／管理を行う
    - □ アクセス制限機能
    - □ MACアドレス制限機能　重要！
  - □ 通信／利用記録等のログ（履歴）に不審な点がないか確認する



※機種やメーカーによって対応事項／方法が異なります。メーカーサイトを確認する／メーカーサポートに問い合わせる等，ご自身で適切に対応してください。

Check! サーバ編

- □ 各種修正プログラムを適用する（yum update等）
  - □ 稼動サービス等の脆弱性に関する情報収集に努め，適切に対応する
- □ サーバーの設定や履歴の確認を行う
  - □ 強固なパスワードの設定
    （8文字以上かつ大文字や数字を組み合わせる）
  - □ 稼動サービスの確認（psコマンド）
  - □ アクセス制限等の適切な設定／管理
  - □ 接続 / ログイン / 操作等履歴の確認　重要！
    （lastコマンド，/var/log配下の確認）

Check! メール編

- □ 迷惑メールや標的型メール攻撃を防ぐ手段はありません
  - □ 上記のようなメールは必ず届くものと自覚する
  - □ ユーザの勘違いや操作ミスが狙われている点を自覚する
- □ メール情報の改ざんは容易に可能であることを理解する
  - □ 差出人情報はメールソフトの設定レベルで改ざんできます
  - □ HTML形式のメールは正規メールのソースコードをコピペするだけで誰でも全く同じものが作成できます　Apple 楽天 …etc
- □ メール本文にURLやリンクがある場合はまずは疑う
  - □ 少しでも疑問に思った場合は，インターネットで正規ウェブサイトを確認する一手間を加えましょう
- □ 標的型メール攻撃の添付ファイルはウイルス対策ソフトで検出できない場合があります
  - □ 標的型メール攻撃の添付ファイルは原則新種のコンピュータウイルスなので，注意が必要です
  - □ 確認が必要な場合は，最寄りの基盤センターへ相談ください
- □ 自身の操作に責任を持つ
  - □ 「気づかずに，ついうっかり，よく分からない」は免責の理由になりません
  - □ Enterやクリックは，押印署名と同様です
    （あなた自身が許可して，実行したものと解釈されます）
- □ 被害軽減のポイントは"初期対応"です
  - □ "しまった！"と思ったら，すぐに最寄りの基盤センターへ連絡を！
    （迅速に適切な初期対応をすることで被害は軽減できます）

Check! Web管理者編

- □ CMSは最も狙われやすいシステムであることを理解する
  - □ CMSは便利な半面，運用には多くのプログラムが必要なため脆弱性やバグ等へ迅速に対応する必要があります
  - □ CMSは"使う"ものではなく"管理"するためのシステムです
    （システムの管理ができるからこそ運用が成立し，利用することができます）　Wordpress Joomla …etc
  - □ 脆弱性に関する情報収集に努め，常に最新パッケージを適用する
- □ パスワード管理や履歴管理は適切に行う
  - □ 強固なパスワードの設定
    （8文字以上かつ大文字や数字を組み合わせる）
  - □ ファイル／コンテンツの作成日時，アクセス／操作等履歴の確認

※　記載事項は一般的な必要最低限の対策事項です。機器管理者は管理状況に合わせて適切に対応してください。

[参考] 情報セキュリティ　(IPA)
https://www.ipa.go.jp/security/index.html

おまけのコラム

～ ネットワークに繋ぐ機器にはEOLがあります ～
(EOL = End Of Life)

シリアル番号を登録すると，サポート情報を定期的にメール配信してくれるサービス等を上手に活用しましょう!(メーカーによる)

EOLを迎えた無線LAN機器を使用し続けた結果，脆弱性を悪用されて通信情報を傍受される等の被害が多発しています。
特に家庭向けのネットワーク機器類はEOLが短い（＝メーカーサポートが打ち切られる期間が短い）傾向があるので注意が必要です。
メーカーのサポートサイトを確認したり，メーカーサポート情報のメールマガジンに登録するなど，情報収集を行い適切に管理してください。

ちょっと解説

- ○ 人間に寿命があるように，ネットワークプリンタ，ルーター，無線LANルータなどネットワーク機器類にも寿命（EOL）が存在します。
- ○ EOL機器は保守部品の製造が中止されるため，修理などのメーカーサポートが一切受けられなくなります。
- ○ EOL製品はソフトウェア開発等が中止されるため，ファームウェアのアップデートやセキュリティ修正プログラムの提供がなくなります。

富山大学 総合情報基盤センター
2018年8月8日
http://www.itc.u-toyama.ac.jp/
内線：6946（五福）

▶ バックナンバー：http://www.itc.u-toyama.ac.jp/cn/