2006－CE－87 (7)
2006／12／9

パスワード再考

前野譲二†
早稲田大学メディアネットワークセンター

概要

パスワードは，最も基本的かつ重要な認証方法として利用され続けている．個人別にカスタマイズされたサービスがWebによって多く提供されるようになっているが，ここでも認証はパスワードが基本である．このような状況の中，管理しなければならないパスワードの数は年々増加をしていくものと考えられる．

一方で，パスワードに利用することのできる文字列長も長くなり，あるいはパスフレーズも利用することができるケースが増えているなど，パスワードに関して常識とされてきた状況は変化しつつある．それにもかかわらず，パスワードに関する教育にはあまり変化が見られない．

本稿では，早稲田大学における利用者のパスワード設定傾向調査を含めて，パスワードとその教育について見直すことを提案する．

Password and its education reconsidered

Joji Maeno
Media Network Center, Waseda University

Abstract

Password has been the most basic and important authentication method. As more and more services are provided with the Internet, mostly with Web, we have to manage more passwords than ever. Although we haven't changed much the way to teach about password, circumstances have been changed. For example, we can use more than 8 characters. Not so many systems allow users to utilize operating system directly, that a compromised account doesn't necessarily mean compromise of a part of the system.

This essay proposes we have to rethink about password scheme and its education.

1．はじめに

インターネットで提供されているサービスの傾向として，静的なページを閲覧させることにより一方的に情報提供するだけでなく，何らかの形でユーザ毎にカスタマイズされたサービスを提供するようになっており，そのため多くのサイトが認証機能を持つようになっている．

一度認証されればHTTP Cookieにより何度も認証を経る必要がないケースが多いとはいえ，本人確認のために利用される認証は，ますます重要で日常的に利用するものとなっている．

認証の方法で最も一般的なのはパスワードであり，これは今も昔も変わっていない．しかし，パスワードを取り巻く状況は様々な面で変化している．その一方で，認証に関する教育は時代の変化にあわせて進歩しているとは言い難い．

そこで，本稿では早稲田大学のシステムについて調査したパスワードの設定状況について概観し，その傾向を論じると共に，パスワードそのものと教育方法について提案を行う．

2．早稲田大学における研究教育用システムと教育の現状

早稲田大学は，6つのキャンパスに5万人を超える学生ならびに教職員を擁している．以前は希望者のみにアカウントが貸与されていたが，現在では履修登録など，学生生活において横断的に活用させるために，入学時にアカウントを一括して発行している．

このアカウントで利用することのできるシステムは，全学を対照に利用されているメール等のシステム（Waseda-net）である．また，早稲田大学で設置されている教室では利用時にIDとパスワードによる認証が求められるが，このIDとパスワードはWaseda-netと同期するよう設計されている．

学生は，入学時にはがき大の用紙を受け取り，Web上でメールアドレス（≒ID）を自ら決定する．パスワー

† joji@mnc.waseda.ac.jp

ドは，はがき大の配布用紙に印刷されているものをそのまま利用するが，随時変更することが可能であり，利用者の管理に任されている．

パスワードには，8文字以上16文字以下を指定することが可能である．初期パスワードは8文字でコンピュータによりランダムに作成したものが渡されており，これには数字，アルファベットの大文字および小文字，記号がすべて含まれるように生成されている．

早稲田大学では単にIDとパスワードを配布するだけでなく，1997年から，すべての新入生を対象としたセミナーを実施し，あるいは全学学生のおよそ4割以上が履修できるリテラシー科目を設置するなどして情報教育に力を入れており，一定の成果を挙げてきた[1][2]．

しかし，パスワードに関する教育については，1997年頃からまったく変わっていない（パスワードの生成方法の解説例までほぼ同一である）．パスワードの扱いについては国家公安委員会や通商産業省など，国からも指針が発表されている[3][4]が，すべてがほぼ同じ内容である．これらは，次のように要約することができる．

(1) パスワードの秘匿に努める（他人に教えない）
(2) 他者が容易に推測できる語句等をパスワードとして設定しない
(3) パスワードを一定期間ごとに変更し，同じパスワードを使い回さない
(4) パスワードを外部に記録しない
(5) 別システムには別のパスワードを利用する

これらは一見正論であるように思えるが，現実に即しているとは言い難く，また誰もがこのような管理方法が現実でないことを理解しているにも関わらず，同じような説明と教育を続けている．

ここではパスワードとして記憶しにくいものを記憶するよう説いており，それをメモするのは禁止である．使うシステムの数が増えれば覚えなければならないパスワードの数が増え，しかもそれらを定期的に変更しなければならない．

上記の(2)や(3)を守ろうとすると，どうしても外部への記録を行いたいと考えがちになるだろうし，(5)を守ろうとしても管理しなければならないパスワードの数が増えれば実行が困難となる．

ここで，どのようなパスワード管理方法とその教育が現実的であるかを考えるにあたって，ユーザがどのようなパスワード設定を行っているかという実態を調べることとした．

3．調査方法

Waseda-netには85,000を超えるアカウントが登録されているが，これらのうち実際に学生および教職員によって利用されている，64,652のアカウントについて調査を行った．

Waseda-netは，Waseda-netポータルと呼ばれるポータルサイトから利用できる各種サービスの総称であり，電子メールや休講掲示など，ユーザの学籍情報や教員情報に基づいた，カスタマイズされたサービスの提供が行われている．Waseda-netではシングルサインオンサービスが提供されているが，ここで設定するパスワードはコンピュータ教室での認証や無線LAN利用時の認証など，様々なシステムで同じIDとパスワードによる認証を行っている．

この目的からパスワードは平文で保存されており，パスワードのみをシステムから抽出して分析を行った．

表1：パスワード長の分布

パスワード長	アカウント数
6	1
7	1
8	32,629
9	7,433
10	7,627
11	5,581
12	4,785
13	3,287
14	2,903
15	204
16	201

4．調査結果

パスワードとして設定されている文字列の傾向として，(1)文字列長(2)利用されている文字の種類について調査を行った．

文字列長の分布を，表1に示す．平均は9.47であり，標準偏差は1.90である．

なお，これらのパスワードは一部のシステムではMD5でハッシュ化して保存される．このハッシュ化されたパスワードをJohn The Ripperにかけて辞書攻撃により解析を試みたところ，1,331のアカウントのパスワードを解読することができた．これらのアカウントの平均文字列長は8.46であり，標準偏差は2.00である．脆弱なパスワードを設定しているユーザと一般的なユーザのパスワード長には統計的に優位な差があることが確認された．

システムが指定する最低パスワード長であり，ユーザに配布される際のパスワードの文字列長でもある8文字をそのまま利用しているユーザが，全体の約50%存在する．最低長および配布時のパスワードを改善することで，この状態はいくぶん改善される可能性がある．

パスワード長が十分長くなくても，利用しているパス

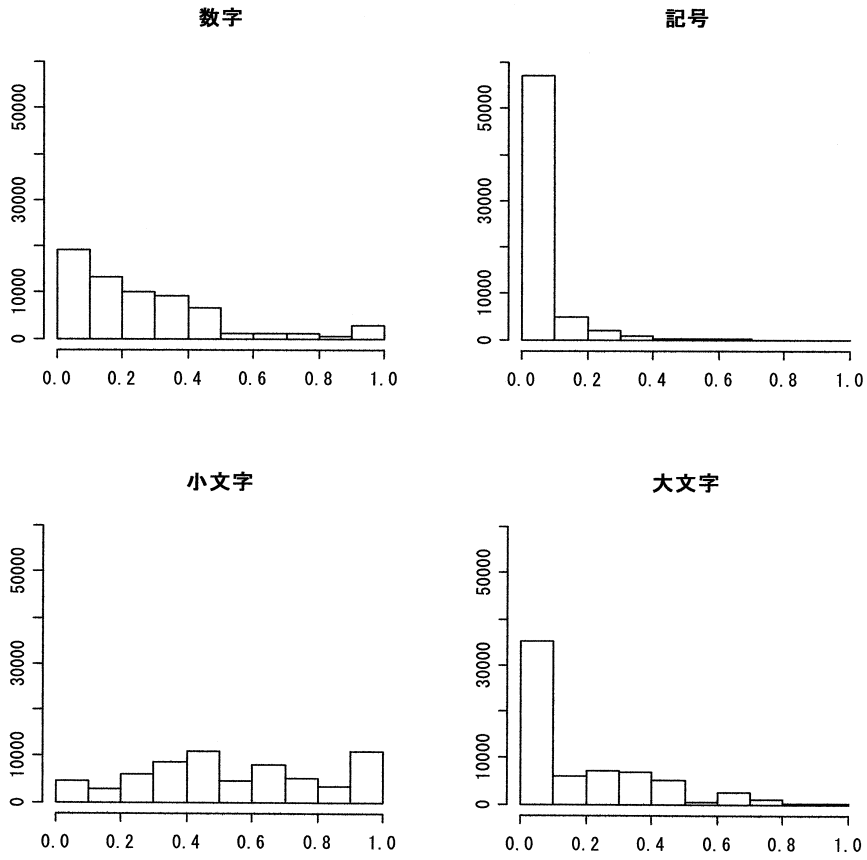

図1：パスワードにおける各文字種の使用割合の分布

ワードの文字種が多様であれば，十分な強度を確保することが可能である．そこで，パスワードの中で数字，記号，小文字，大文パスワード中のそれぞれの文字種がどのような割合で利用されているかを調査した．結果を図1に示す．

このヒストグラムは，それぞれの文字種があるパスワードの中でどれほどの割合で利用されているかということを個別に計算したものをグラフ化したものである．例えば，「数字」のグラフを見ると，0.0 の級に約15,000 の度数がある．これは，パスワードにおいて数字をまったく利用していないユーザが15,000 人いる，ということを示しており，また数字のみのパスワードを利用しているユーザも少なからずいることを示している．

このヒストグラムから理解できるのは，記号はほとんどのユーザが利用していない，ということである．約53,000 名のユーザがパスワードに記号を利用しておらず，記号を1文字でも利用しているユーザは全体の18.26%でしかない．全パスワードデータに占める記号の割合はたった 2.95%に過ぎず，後述するように利用されている記号もごく限定されている．

同様に，大文字の利用も少ないことが分かる．約33,000 人のユーザがパスワードに大文字を利用しておらず，パスワードデータに占める大文字の割合は，16.72%である．つまり，48.41%のユーザしか大文字を使用しておらず，使っても1〜2文字である．

パスワード中で何種類のユニークな文字を利用しているかを調査したものを，図2に示す．これは，例えばパスワードが「aaaaaaaa」であれば，文字は1種類しか利用されていないため，1として計算したものである．この平均値は7.91 であり，標準偏差は1.75 である．図を見ると，8を中心として分布していることが分かる．7および8種類の文字を利用するユーザが全体の56%ほどであり，5種類以下というユーザも5%ほど存在する．

また，パスワードの長さとパスワードで利用されるユニークな文字の数には一定の相関があり，相関係数は

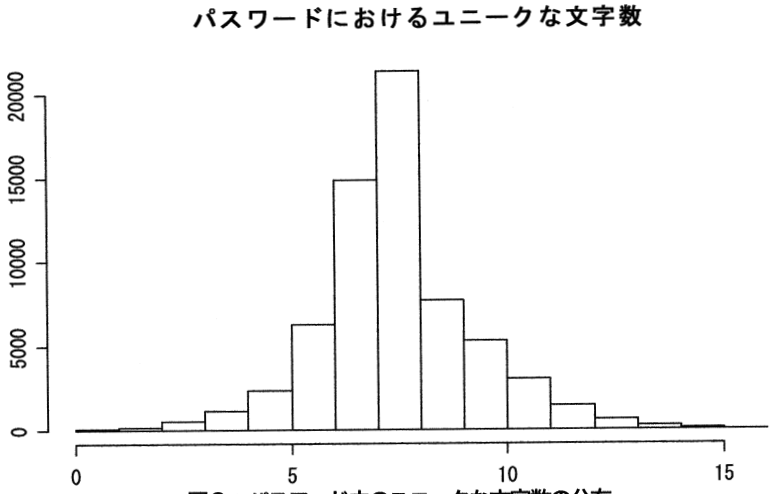

図2：パスワード中のユニークな文字数の分布

64.49%で統計的に有意な相関関係が見られた.

パスワードの強度は，一般的にエントロピー（平均情報量）として計算することができる．例えば，数字とアルファベットの小文字だけからなるパスワードであれば，36種類の文字のみであるから1文字あたりのエントロピーは$\log_2(36)$であり，約5.17ビットである．パスワードに利用することのできる文字種はシステムによって違いがあるが，Waseda-netも含めた多くのシステムでおよそ90文字前後であるので，本来であれば1文字あたり6.49程度のエントロピーを得られる．

しかし，文字別の分布を見ると，a, e, h , i, k, m, n, o, r, s, t, u, y, 0, 1, 2など特定の文字への偏りが見られた．特に母音の使用頻度が高いため，何かしらの日本語の単語が利用されているケースが多いだろうことが推察されるため，実際のエントロピーはかなり低いものと思われる．連字（digraph）などを統計的に分析すれば，効果的な攻撃ができる辞書を構築するのは容易であると考えられる．

また記号についても，そもそも使用頻度が低いが，アンダースコア(_)，カンマ(,)，クエスチョンマーク(?)，エクスクラメーションマーク（!）の順で特に使用頻度が特に高く，偏りが大きかった．

5．考察

Yan, Blackwell, Anderson, and Grant[6]によれば，およそ10%のユーザがパスワードに関する教育に従わないという．

早稲田大学の場合，すべての新入生に対して行われているパスワードに関する教育としては，大文字，小文字，記号，数字のすべてが含まれているパスワードを作成することとなっており，前述のように18.26%のユーザしか記号を利用していないため，このような観点からすると8割以上のユーザがパスワードに関する教育に従っていないことになる．

大文字の利用も少ないことを考え合わせると，ユーザはシフトキーを利用した打鍵を嫌っているものと考えられる．つまり，入力が容易で覚えやすい，簡単なパスワードを利用していることが推察される．

では，教育のみではユーザの大半は望ましいパスワードを利用しないことを前提として，我々はどのような対策を行えばよいだろうか．

1つは，パスワードスキームを社会的に統一すること，そしてパスワード変更時にその強度をチェックするという事前審査の強化であると考えられる．

一般的にパスワードは8文字に固定されていた期間が長かったが，そのような制約が無くなってからこれといった合意が無く，何となく「8文字以上」と言われているに過ぎない．様々なシステムで利用可能な最大文字数にばらつきがあり，利用可能な文字種も不統一である．そして，事前審査の行われ方にもばらつきがある．

早稲田大学では，UNIXベースのシステムのアカウントとして提供していたWaseda-net以前のシステムで，Cracklibを組み込んだnpasswdが内部的に利用されていた．このためOSの制約からパスワード長は8文字に限定されていたが，厳格な事前審査を行うことができていた．

Waseda-netへ移行してからパスワードの変更はWebベースのアプリケーションとなり，そこで事前審査が行われなかった時期があった．現在は簡単な事前審査が入るようになっているが，不十分なものでしかない．一般的に見ても，十分な事前審査が行われている例は希であり，パスワードの長さには一定の規制をかけている例は多く見られるが，後はせいぜい数字を入れることを求められる程度であり，強度の確保という観点から見て意味がほとんど無いような事前審査も見受けられる．

Webアプリケーションには学籍情報を扱うものや金

融機関，ショッピングサイトのように重要なものと，よりカジュアルに利用するものがある．つまり，サービスの重要性はシステムによって異なり，重要性によってパスワードの管理の厳格さ，厳密さを変えて対応するのが現実的であると思われる．

しかし，これだけパスワードを利用した認証が広く利用されている現在，パスワードの最低長と最大長，利用可能文字種などについては，ある程度の社会的合意が必要である．またWebアプリケーション向けのパスワード事前審査のためのライブラリを整備することも必要である．

もう1つの対策は，少ない文字種で十分な強度を得られるパスワードスキームを考えることである．

この場合，パスフレーズを利用するのが1つの対策となるであろう．同様の考え方として，十分に長いパスワードを利用できるようにした上で，脈絡無く指定する単語2つを数字や記号で結びつけて利用する，という方法がある．

例えば，「stagnant3flamingo」のように，それぞれ独立した，無作為に選ばれた単語を数字や記号で挟む，というものである．

このようにして作成されたパスワードの強度は，正しく作成された8文字からなるパスワードと比較して，ほぼ同じか，若干落ちる程度である（英単語の平均的なエントロピーの評価によって結果は異なる）．しかし，この方式によれば，記憶のしやすさは大きく改善される．また，このようなパスワード生成規則であることを仮に攻撃者が知っていたとしても，数十万とある辞書の単語のそれぞれについてすべての組み合わせを試していかなければならないため，辞書攻撃に対する強度は十分に確保されている．また，パスワードの文字列長が一定以上確保できているシステムであれば，すぐに利用し始めることができるパスワード生成規則である．

ところで，脆弱なパスワードがシステム全体のセキュリティ上に対して持っている含意も，以前とは異なるものとなっている．

従来典型的であった，UNIXシステムのアカウントを発行し，OSそのものを利用させるためにIDとパスワードを提供する，という状況は減少している．このようなサービス提供形態では，ユーザのパスワード漏洩やパスワードクラックは，単にユーザの個人情報が漏洩するにとどまらず，システム全体に対する脅威となり得た．UNIXシステムにログインができてしまうケースもよく見られたし，システムへの足がかりを得るという意味で末端のユーザを最初の攻撃対象にすることはよく行われていた．

現在では，OSを直接利用させているケースは希である．多くの場合，個人のパスワード漏洩の影響は，個人情報の漏洩や，そのIDを用いたネットワークへの不正な接続程度にとどまるものと思われる．

しかし，パスワードによる認証は各種Webアプリケーションで頻繁に利用されており，ユーザが管理しなければならないIDとパスワードは増えていることも考慮しなければならない．

その結果，利用するシステムが増えると同じパスワードが使いまわしされる傾向が高くなるという報告[6]があるように，あるパスワードが漏洩した際の情報漏洩のリスクはかえって高まっているとも考えられる．

谷津[7]，前野他[2]が指摘するように，サービスの重要性や自己の個人情報管理，あるいはリスク管理という観点から，パスワードに関する教育を再検討する必要がある．具体的には，パスワードをサービスの内容や漏洩時の影響に従って分類し，異なった管理方法を指導するのが現実的だろう．

6．おわりに

本稿ではパスワードの実態について分析を行うとともに，パスワードの管理法とその教育について提案を行った．

今後の課題として，パスワードの設定傾向を言語学的に統計分析するとともに，早稲田大学におけるシステムと教育の改善を通じて，どのように設定傾向が変化するか評価したいと考えている．

参考文献

[1] 前野譲二，原田康也，楠元範明，瀧澤武信，早稲田大学メディアネットワークセンターにおける導入教育の課題，平成14年度情報処理教育研究集会講演論文集，pp.175-178，2002.

[2] 前野譲二・原田康也・辰己丈夫，「危機管理としての情報倫理教育」と「一般ユーザのための情報リスク管理」，情報処理学会1998年度夏のプログラミングシンポジウム，pp.139-143, 1998.

[3] 国家公安委員会，情報システム安全対策指針，国家公安委員会告示第19号，1999.

[4] 通商産業省，コンピュータ不正アクセス対策基準，通商産業省告示第950号，2000.

[5] Smith, R.E., Authentication, Addison-Wesley, 2002.（稲村 雄 監訳，認証技術，オーム社，2003.）

[6] Yan, J., Blackwell, A., Anderson, R., and Grant, A., The memorabilitiy and security of passowrds -- some empirical results, University of Cambridge Computer Laboratory Technical Report, No.500, 2000.

[7] 谷津貴久，大学生のパスワード利用状況とその忘却経験，MNC Communications，Issue 7，2004.

[8] Klein, D. V., Foiling the Cracker; A Survey of, and Improvements to Unix Password Security, Proceedings of the 14th DoE Computer Security Group, May 1991.