パスワード変更警告メールに対する利用者の反応

岸場清悟、入江治行、岩沢和男、津久間秀彦*、稲垣知宏**、
鈴木俊哉、隅谷孝洋**、新畑道江、勇木義則

広島大学総合情報処理センター
739-8526 東広島市鏡山 1-4-2
Tel:0824-24-6252, Fax:0824-22-7043,
kishiba@hiroshima-u.ac.jp, haru@hiroshima-u.ac.jp, iwasawa@hiroshima-u.ac.jp, mpsuzuki@hiroshima-u.ac.jp,
michie@hiroshima-u.ac.jp, yuuki@hiroshima-u.ac.jp,
* 広島大学医学部附属病院
734-8551 広島市南区霞 1-2-3
Tel:082-257-5555, Fax:082-257-5087, tsukuma@hiroshima-u.ac.jp
** 広島大学情報教育研究センター
739-8521 東広島市鏡山 1-7-1
Tel:0824-22-7111, Fax:0824-20-0099, inagaki@hiroshima-u.ac.jp, sumi@riise.hiroshima-u.ac.jp

Users' response against warning mails to change passwords

Seigo Kishiba, Haruyuki Irie, Kazuo Iwasawa, Hidehiko Tsukuma*, Tomohiro Inagaki**,
Syunya Suzuki, Takahiro Sumiya**, Michie Niihata and Yoshinori Yuuki

Information Processing Center, Hiroshima Univ.
Kagamiyama 1-4-2, Higashihiroshima, Hiroshima 739-8526 JAPAN
*University Medical Hospital, Hiroshima Univ.
Kasumi 1-2-3, Minami-ku, Hiroshima, Hiroshima 734-8551 JAPAN
**Research Institute for Information Science and Education, Hiroshima Univ.
Kagamiyama 1-7-1, Higashihiroshima, Hiroshima 739-8521 JAPAN

概要

パスワード変更は利用者のセキュリティ意識の具体的な現れである。広島大学総合情報処理センターでは、パスワード変更促進策を 1997 年 7 月から継続的に行なってきた。利用者のセキュリティ意識を把握するために、最近の利用者動向を約 9 か月にわたり調査し解析した。

キーワード:
センター運営, セキュリティ, パスワード, 利用者モデリング

1 はじめに

大学情報処理センターのシステムは、インターネットブーム以降の利用者層の多様化とともに量的にも質的にも大きな変化を迫られている [1]。これは従来の単純な情報システムから大規模複合型キャンパス情報システム [2] への変化であり、そこでは多様な利用者に対し適切なサービスを行なうことが必要になる。

適切なサービスの企画にあたっては、利用者のモデル化が必要であろう。すなわち、利用者分類の適切な枠組みを構築しなければならない。そのためには、利用者の行動特性を調査・把握して、その内容を分析し類型化す

る必要がある。

そこで利用者の行動特性の一例として、利用者のパスワード変更に注目した。これは利用者のセキュリティ意識を反映するものである。センターが変更促進策を行った場合に、その効果はどの程度かを、調査、評価した。

2 本センター情報システムの状況

広島大学総合情報処理センター（以下本センター）では、学生・教職員の区別なく大学の全構成員にオープンな計算機利用環境を提供している。1996年4月の計算機システム機種更新[3]のあと同年7月より大学全構成員のセンター利用アカウント登録の運用を開始した[4]。アカウント登録にあたっては学部学生は一括して登録し、それ以外は希望者の自主登録としている。1999年12月現在では登録数19835（うち学部学生13267）、このうち後述のパスワードロックの対象になっていない利用者数は14885（うち学部学生10707）となっている。

本センター計算機システムがネットワークを通じて外部と継ることにより、ネットワーク上でのモラル確保とセキュリティ確保の問題は深刻なものになっている。対策としては全利用者を対象としたセンターの利用説明、あるいはセキュリティに関する講習会や授業等が考えられる。しかし本センターの持つマンパワーとのかねあいから、本センターとしてはこれまで実施できていない。ただし1997年度より学部1年生対象の教養的教育の科目として「情報活用概論」「情報活用基礎」「情報活用演習」といった科目が設置されている。

3 パスワード変更促進策の内容

3.1 調査対象のシステム構成

2000年3月まで[1]の本センターのシステム構成[3]を、利用者がパスワードを使用するという観点から整理すると次のようになる。

1. ユーザエントリマシンとダイヤルアップサービス
   ユーザエントリマシン（以下ue）はメールサーバとWebサーバを担当し、またtelnetサーバとしてUNIX利用環境全般を提供する、利用者サービスの中心となるサーバマシンであった。ダイヤルアップサービスは本センター利用者に電話回線を通じたネットワーク接続手段を提供するもので、近年の大学情報センターにおいては最重要なサービスのひとつになっている。これらにより提供する下記のサービスにおいて、ユーザ認証の手段として共通のパスワードを使っていた。
   - ueへのtelnetログイン
   - ue経由のPOPによるメール取り込み
   - ueとのFTPによるファイル転送
   - ダイヤルアップサーバを用いたＰＰＰ接続

   このパスワードの管理はueで行なっており、利用者がパスワードを変更するには、
   - ueでpasswdコマンドを用いる
   - Eudoraの拡張機能(poppassd)を用いる[2]

   という手段を用意していた。
2. その他
   上記の他にセンターでは教育研究用システムや科学計算用の演算サーバなどを運用しており、これらにおいてもユーザ認証の手段としてパスワードを使っていた。このパスワードはそれぞれのシステム・サーバにおいて独立の管理になっていた[5]。

3.2 パスワード関連セキュリティ対策

パスワードについては各種ガイドライン[6][7]も参考に、1997年度にパスワード管理に関連する次のようなセキュリティ強化対策を策定した。

1. ９０日以上の未変更パスワードに対する警告
   パスワードを９０日間変更しない利用者に対し、すみやかにパスワードを変更するよう促す警告メールを送付し、またログインメッセージで警告を出した。警告の間隔は短すぎると煩わしく、長すぎれば効果が薄いので、９０日の設定は、学生が通学する大学暦の半期の間に一度は警告が行われることを目安にしている。
   毎日１回、自動的にチェックと警告メール送信を行なった。また、警告メール送信にもかかわらずさらに長期にわたりパスワードを変更しない利用者に対し、125日ごとに再度警告メール送信を行った。
2. 長期非使用アカウントのパスワードロック
   ueと教育研究用システムについて該当システムを７カ月以上使用していないアカウントを対象にパ

[1] 本センターでは2000年3月に機種更新を行った。後述するデータの採取期間が2000年3月までになっているのはこのためである。
[2] 1997年8月サービス開始

スワードロックを行った。7カ月は大学の半期を考慮したものである。ただし学部学生に関しては授業とのかねあいがあり、2年生については年度はじめにいったんパスワードロックを解除する取り扱いになっている。

3. アクティブパスワードチェック
   ue のパスワードファイルに対してフリーソフト crack 及び辞書ファイル pubdic を用いてパスワードチェックを行ない、破られやすいパスワードについて早急なパスワード変更を促す警告メールを利用者宛てに送付した。警告メールには一般的なパスワードの使用心得と変更方法の概要も付けた。
   当初、定期的（約3カ月ごと）に行なう予定であったが、手動での作業ということもあり、実績としては不定期の実施になった。
4. ue での APOP, OTP の試行運用
   ネットワーク盗聴対策として、ネットワーク上をパスワードが平文のまま流れないようにするためのツールを試行的に運用した。将来は強制的な運用を目指すこととしていたが、現時点でのクライアントの対応状況や、他のより安全性の高いツール (SSH 等) の台頭などを考慮すると、APOP や OTP の強制はもはや現実的ではないと思われる。

4 警告メールの効果

以下では、利用者のパスワード変更に関する各種統計をとり、上記の対策のうち特に継続的に実施することのできた「９０日以上の未変更パスワードに対する警告」について、その効果を統計から評価する。

まず、1999 年 6 月 18 日から 2000 年 3 月 18 日のあいだに各アカウントで2度以上パスワードを変更している場合に、そのパスワード変更間隔を数え上げ、間隔日数に対してプロットした（図-１）。90 日付近に圧倒的に大きなピークがあり、多くの利用者が警告を目安にパスワードの変更を行っていることがわかる。また 215 日付近のピークは、前述の2度目の警告メールに対応しているものと思われる[3]。

パスワード変更における行動特性をさらに詳しく見るため、1999 年 6 月 18 日から 2000 年 3 月 19 日にかけての、各アカウントのパスワード変更回数を調べた (表-1)。１回以上変更しているアカウントが全体の 50%程度である。また、3 回変更しているアカウントがやや多いことが目立つ。データ取得日数が 270 日間なので、3 回変更しているアカウントはほぼ９０日の間隔でパスワードの変更を行っていることになり、警告メールの効果は大きいと言える。

3 回以上変更しているアカウントはほぼ９０日以内にパスワードの変更を行う、センターが推奨する形のパスワード管理を行っていると推定される。該当するアカウント数は使用アカウント全体の 13%強である。

いっぽう、約半数のアカウントでは調査期間内に一度もパスワード変更を行っていない。利用者のセキュリティ意識のあらわれではあるのだが、計算機システム全体でパスワードが複数あって分かりにくい、あるいはコマンドベースのパスワード変更方法に慣れていないといった利用者から見たセンター計算機システムの使いにくさも影響しているのではないだろうか。

また、1 回だけ変更しているアカウントも多い。初めての警告に対しては素直に従ってパスワード変更を行い、2 度目以降は警告に慣れてしまっているものとも思われる。しかし利用者のパスワード変更に対する行動原理を明らかにするには、さらに各アカウントへの警告メールとパスワード変更行動の関連を詳しく解析する必要があろう。

5 おわりに

2000 年 3 月に運用を開始した新センター計算機サービスでは、全てのサービスについてパスワードを統一して管理し、変更方法も Web ブラウザを用いて行えるようシステムを作り込んだ [8]。このことによりサービスと利用者認証の構成が利用者にも分かりやすくなることを期待しているが、その評価は今回と同様の利用動向調査を通じて今後行う必要がある。

この報告ではパスワード変更促進策の効果について評価したが、一般にセキュリティ対策は、利用者の理解と協力があってこそ大きな効果をあげることができる。ＩＣカードや指紋認証など多様な認証方法が普及しはじめている現在、パスワード変更促進策についてもそれ自体のみを目的とするのではなく、センター利用者のセキュリティ意識の向上に資するものでなければならない。このような活動を企画し、利用者からの理解と協力を得るためには、多様な利用者への適切なサービスと広報を行うことが前提になる。そのためにも、利用者の行動特性のさらなる調査・分析に基づく利用者の適切なモデリングが必要であろう。

[3] ただし、全体のデータ取得日数が 270 日であるので、この図の 135 日以上の部分は定量的にはそれ以下の部分と比較できない。

謝辞 本研究の一部は、文部省科学研究費補助金萌芽的研究「人間集団の行動特性を考慮した大規模複合型情報システム」（課題番号 11878066）の支援を受けた。

参考文献

[1] 原山美知子, 佐藤俊介, 田中昌二, “協議会資料に基づく近年の国立大学情報処理センターの動向”, 学術情報処理研究 No.3, pp.31-48, 1999.

[2] 津久間秀彦, 入江治行, 岩沢和男, 岸場清悟, 稲垣和宏, 隅谷孝洋, 秋元志美, “大規模複合型キャンパス情報システムと利用者指向のサービス運営プロセス”, 学術情報処理研究 No.4 に掲載予定

[3] 岸場清悟, 入江治行, “総合情報処理センターのシステム構築－教育と研究の統合環境－”, 平成 8 年度情報処理教育研究集会講演論文集,pp.209-211,Dec 1996;
入江治行, 津久間秀彦, 岸場清悟, 加登基二, 新畑道江, “広島大学総合情報処理センター新計算機システムの運用管理について”, 情報処理学会第 4 回分散システム運用技術研究会, pp.31-36, Nov 1996.

[4] 勇木義則, 津久間秀彦, 新畑道江, 千々松範朗, 入江治行, “大学全構成員のセンターシステム利用を目指して－利用者管理の運用を中心に－”, 平成 8 年度情報処理教育研究集会講演論文集,pp.325-328,Dec 1996.

[5] 岸場清悟, 勇木義則, 新畑道江, 稲垣和宏, 岩沢和男, 隅谷孝洋, 津久間秀彦, 入江治行, , “大学構成員全員登録下でのパスワード漏洩対策とその効果”, 学術情報処理研究 No.3, pp.53-58, 1999.

[6] 「コンピュータ不正アクセス対策基準」 通商産業省告示第３６２号、平成８年８月８日施行

[7] 「ネットワーク管理者ガイドライン」広島大学情報通信メディア委員会、平成９年施行
http://www.hiroshima-u.ac.jp/Committee/media/admin.html

[8] 岩沢和男, 津久間秀彦, 新畑道江, 岸場清悟, 入江治行, 稲垣和宏, 隅谷孝洋, 秋元志美, 勇木義則, “大学情報サービス基盤としてのアカウント体系”, 学術情報処理研究 No.4 に掲載予定

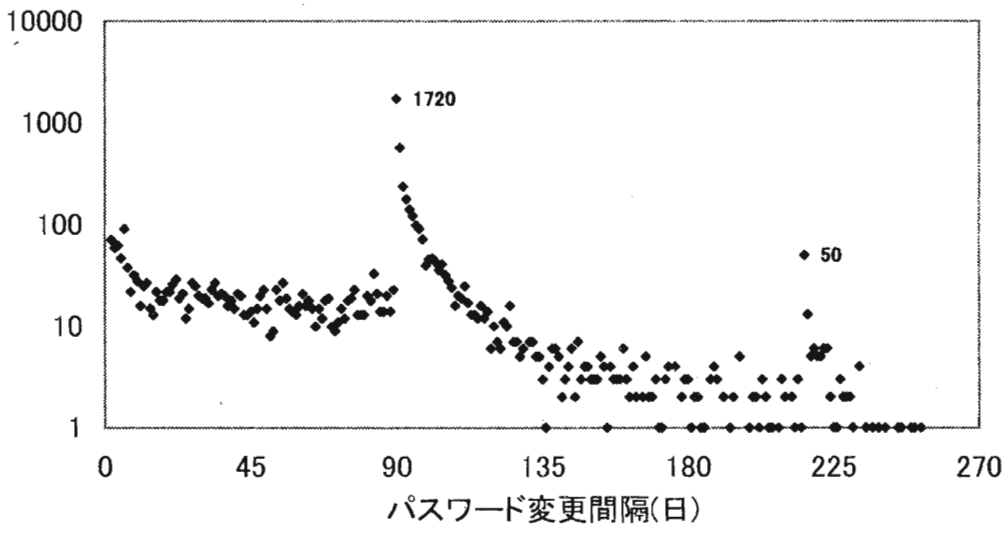

図-1 パスワード変更間隔の度数分布(1999/06/18～2000/03/19)

全アカウント(1999/12現在)		19835
ロックされていないアカウント		14885
パスワード変更 (1999/06/18 ～ 2000/03/19)	*1回以上*	*7471*
	1回	4048
	2回	1472
	3回	1825
	4回	82
	5回以上	44

表-1 全利用者のパスワード変更回数分布