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

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

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@ipc.hiroshima-u.ac.jp, yuuki@ipc.hiroshima-u.ac.jp, michie@ipc.hiroshima-u.ac.jp,
inagaki@ipc.hiroshima-u.ac.jp, iwasawa@ipc.hiroshima-u.ac.jp, haru@ipc.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, sumi@riise.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@ipc.hiroshima-u.ac.jp

Measures against leakage of passwords, with registration of all members in Hiroshima University

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

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

概要

広島大学総合情報処理センターにおいて平成９年７月より行なってきたパスワード漏洩対策について、その効果を評価した。対象利用者の３割が対策に応じてパスワード変更を行なっており一定の成果はあったものの、目標に対しては効果は不十分なものであった。

keywords:
センター運営 セキュリティ パスワード 利用者対応

1 はじめに

広島大学総合情報処理センター（以下センター）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。平成８年４月の計算機システム機種更新 [1] 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 [2]。

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８月現在では登録数 24000（うち学部学生 16577）、後述のパスワードロックの対象になっていない実質的な利用者数でも 17620（うち学部学生 10787）となっている。センターの持つマンパワーとのかねあいから、登録に際して利用方法やセキュリティに対する講習会や授業等はセンターとして特には実施していない[1] 。

いっぽう、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基本的かつ深刻なものになっている。ここではセキュリティ確保の問題のうち、利用者認証の主要な手段であるパスワードの管理を利用者とともに如何に行なうか、その効果はどの程度かを、必ずしも計算機技術に明るくない大量の利用者層にサービスを拡大した状況において定量的に評価し、今後のセンター情報サービスの方向性を探るための手がかりとしたい。

2　対策の内容

2.1　センターのシステム構成

現在のセンターのシステム構成 [1] 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
   主に次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る。
   - ユーザエントリマシン（以下 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 (poppasswdd) を用いる[2]

   という手段を用意している。
2. 教育研究用システム
   センターが運用している教育研究用システムの NEXTSTEP 端末において、ユーザ認証の手段としてパスワードを使っている。このパスワードは ue とは別管理になっており、利用者がパスワードを変更するには端末上で GUI による手段が用意されている。
3. その他
   上記の他にセンターでは科学計算用の演算サーバなどを運用しているが、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る。このパスワードはそれぞれのサーバにおいて独立の管理になっている。

2.2　パスワード関連セキュリティ対策

パスワード対策については各種ガイドライン [3][4] も参考に、平成９年度にパスワード管理に関連するセキュリティ強化対策を策定した [5]。まず ue で管理するパスワードについて、平成９年７月から次の対策を開始した。

1. 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、チェックを通らなかったもの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する。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る。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、これまでの実績としては不定期の実施になっている。
2. 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す。毎日１回、自動的にチェックと警告メール送信を行なっている。

[1] 平成９年度より、学部１年生対象には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

[2] 平成９年８月サービス開始

3. 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する。将来は強制的な運用を目指す。

さらに平成１０年１月には 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スワードロックを開始した [6]。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を行なっている。

3　パスワード対策に関する統計

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。

3.1　警告対象者数の推移

９０日以上パスワードを変更していないアカウント数の、警告開始当初からの推移を調べた（図１）。

一括登録している学部学生が含まれているためにパスワードロックの運用の影響が入ってしまっているが、その影響を差し引いて見るとほぼ横ばいである。この間利用者数は増加しているので、一定の成果は上がっていると言えるが、全ての利用者が９０日以内にパスワードを変更するという目標は達成できていない。

3.2　警告の効果

平成 11 年６月 18 日から８月 10 日にかけて、警告対象者が実際に警告に応じてパスワードを変更したかどうかを調べた（図２）[3]。

平均して警告当日に約 17 %がパスワードを変更しており、警告後 10 日までに約 30 %がパスワードを変更している。警告後 11 日以降にもパスワードの変更が観察されるが、もう日を追っても変更数がほぼ一定になり、警告との相関関係がほとんどなくなっていると考えられる。６割以上の利用者が警告されてもパスワード変更を行なっていない。なお、学部学生を除くと変更率が少し高くなる。

3.3　パスワード変更日の分布

利用者のパスワードの変更日を、ある一日を取り出してスナップショットで調べた（図３）。

目標である９０日以内に変更している利用者は約 30 %であり、１年以内に変更している利用者は約 70 %である。これも学部学生を除くと変更率が 10 %ほど高くなる[4]。

4　パスワード対策の効果評価

ここまでセンターで行なってきたパスワード漏洩対策は、基本的には「適切なパスワードの使用と定期的なパスワード変更を利用者に要求し、パスワード管理の不十分な利用者にはその旨通知して速やかなパスワード変更を促す」というものであった。今回、この通知の効果を利用者の動向も含めた形で調査した。利用者の３割程度がパスワードについて（自発的ではないにしても）目標とする頻度で変更していると評価される。

パスワードの管理はその性質上、利用者の理解と協力があってはじめて安全対策が成立する。単にセンターから利用者に強制するだけでは、センターサービスの運用について安全性を高めることにはならないであろう。

しかしながら、もしパスワードについて利用者により厳格な管理を求めるとするならば、単に通知を行なうだけではなく次のような対策が必要になると思われる。

- 利用者全員を対象にしたパスワードに関する講習、特に登録時に初期講習を徹底すること
- パスワード管理が一定基準より甘い利用者を対象に、パスワードロックなどの強制処置を行なうこと

また APOP、OTP、SSH 上の RSA 認証など、より安全性の高い利用者認証手段の導入も、対応クライアン

[3] 図２、図３の統計については、平成 11 年度入学の学部学生のアカウントの影響を除いたものを用いている。これは一括登録されていてかつ未だパスワードロックの対象になっていないので、実際に使用していないものが含まれてしまうため。

[4] 300 日付近と 480 日付近に見られる値の飛びは、それぞれ前年後期開始時の学部学生パスワードロック一括解除と前年度はじめの新規登録の影響である

トソフトが容易に入手可能な現在では検討に値する。ただし、安全性を高めようとすれば代わりに従来の UNIX パスワードを使用しないことにする必要があり、切替えに伴う混乱の大きさを考えると、大学の情報処理センターとして認証方法の切替えに踏み切るのは困難を伴う。導入にあたっての効果の定量的な見積りや、利用者のシステムやセキュリティに関する理解の度合を思料しつつ、サービス内容を決定する必要があるだろう。

参考文献

[1] 岸場清悟, 他,“ 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, 他,“ 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.

[2] 勇木義則, 他,“ 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.

[3] 「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

[4] 「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

[5] http://www.ipc.hiroshima-u.ac.jp/announce/security.html

[6] http://www.ipc.hiroshima-u.ac.jp/announce/passlock.html

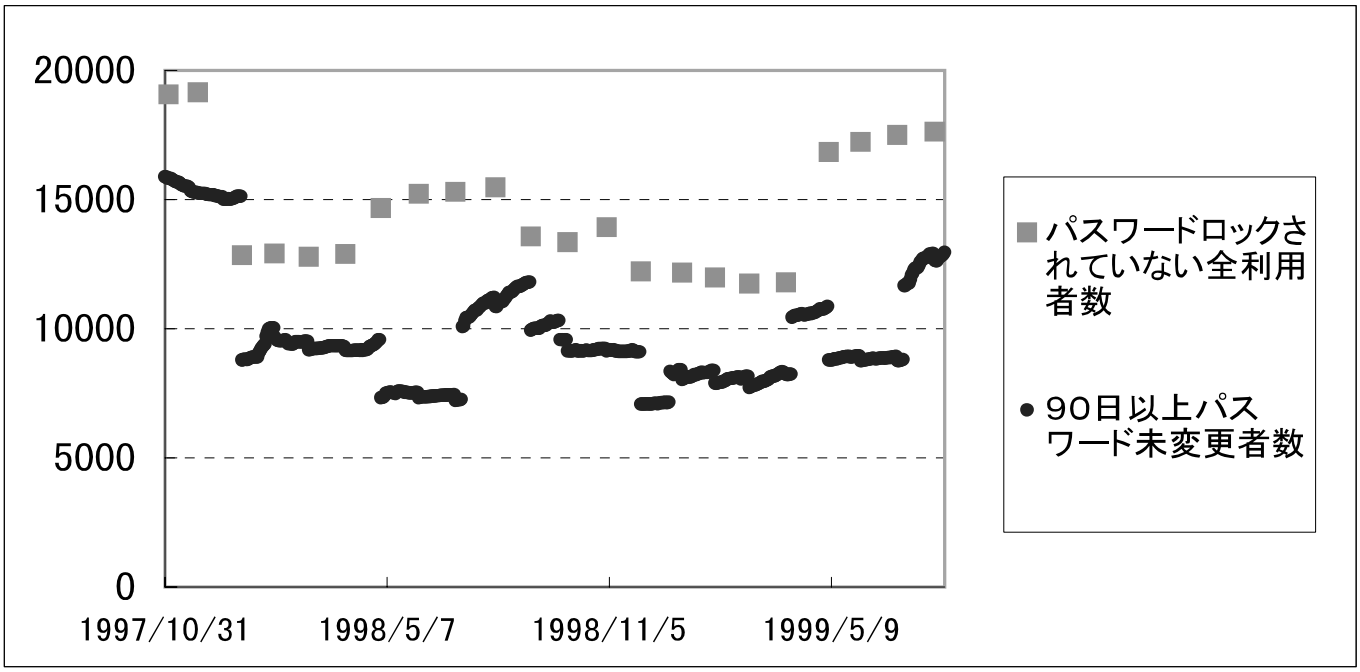

図 1: ９０日パスワード未変更・警告対象者数

警告数	当日	翌日	2日	3日	4日	5日
3302(2254)	553(471)	162(136)	92(63)	55(43)	36(29)	25(18)
比率(%)	16.7(20.9)	4.9(6.0)	2.8(2.8)	1.7(1.9)	1.1(1.3)	0.8(0.8)

6日	7日	8日	9日	10日	11日～	未変更
22(19)	25(22)	23(14)	14(13)	18(13)	119(90)	2158(1326)
0.7(0.8)	0.8(1.0)	0.7(0.6)	0.4(0.4)	0.5(0.6)	3.6(4.0)	65.3(58.8)

図 2: パスワード未変更警告メール送付後の、パスワードを変更する時期（1999-06-18～1999-08-10 の総数）

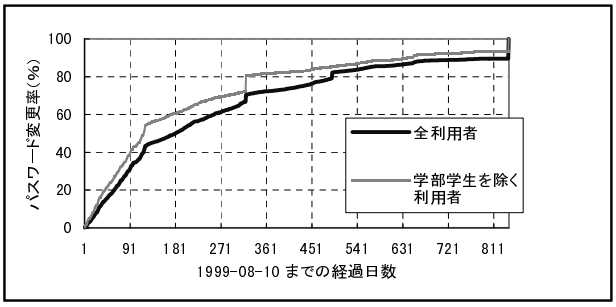

図 3: パスワード変更日分布（1999-08-10 現在）