利用者パスワード変更促進手法と評価

岸場清悟、西村浩二、相原玲二、津久間秀彦 *、

広島大学情報メディア教育研究センター,
* 広島大学医学部附属病院

利用者への警告メール送付を主としたパスワード変更促進手法を実装し、広島大学情報メディアセンターで運用して評価を行なった。３〜４割の利用者が警告に応じてパスワードを変更する成果を挙げたが、２度目以降の警告メールには利用者が慣れてしまい、警告が放置される傾向があることがわかった。

Evaluation of Promotion Methods for Changing Users' Passwords

Seigo Kishiba, Kouji Nishimura, Reiji Aibara, Hidehiko Tsukuma*

Information Media Center, Hiroshima Univ.,
*University Medical Hospital, Hiroshima Univ.

We implemented promotion methods for changing users' passwords in Information Media Center, Hiroshima University, and evaluated them. One of the methods is sending mails to users who have not changed their passwords over 90 days. $30-40\%$ users had changed their passwords at the warning. But, it emarged quantitatively that users tend to negrect the warning mail in the second time.

1　はじめに

多数の利用者によって共有される大規模分散システムのセキュリティ確保にあたっては、利用アカウントのパスワード管理が主要な役割を担っている。しかし現在広く普及しているＵＮＩＸシステムにおいてはパスワードは８文字以内と脆弱であり、さらにネットワークを通したシステム利用によって平文のパスワードがネットワーク上を流通することがままあるため、盗聴の危険も大きい。したがって、このようなシステムにおいてパスワードの有効性を確保するためには、常にできるだけ短期間で本人がパスワードを変更することが要求される。

パスワードの短期間での変更を確保する手法として、システム管理者による強制変更があり、またパスワードエージングによる強制変更も現在の主要なＵＮＩＸシステムには実装されている。しかしこれらの手法は通常の利用を大幅に制限するものであり、大学の情報処理センターのように利用者の自律性が重視されるシステムでは利便性の損失が大きい。

そこで我々は利用者の自発的なパスワード変更を促進するために、利用者への警告を基本としたパスワード変更促進手法を考案し、広島大学情報メディア教育研究センターの情報システムの中に実装して実践評価を行った。

2　本センター情報システムの状況

2.1　利用者構成

広島大学情報メディア教育研究センター（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 [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。2001 年７月現在では登録数 23515（うち学部学生 15180）となっている。

2.2　システム構成

本センターでは 2000 年３月にシステム機種更新を行った。このシステムは、主にメールサーバ、ＷＷＷサーバと多数の利用者端末が、ホームディレク

トリをファイルサーバに共有する構成である。

このシステムを利用者がパスワードを使用する観点から整理すると、次の特徴がある。

1. NIS+を使用したアカウントとパスワード情報の共有
   通信路の暗号化を用いたセキュアなパスワード情報の共有を実現している。このシステムにはNIS+クライアントになれないサーバも一部含まれているが、それについてはscpを用いて暗号化された通信路を通してパスワード情報ファイルを転送し、パスワードの同期を取っている。

2. シングル・サインオンの徹底
   以前のセンター計算機システムにおいては同じアカウントでもサーバによってパスワードが別々であったため、複雑なパスワード管理を利用者に強いることになった。またパスワードに関する質問の対応においても「どの」パスワードかを常に明示しながら対応する必要があり、質問への回答が繁雑になりがちだった。

   今回のシステムでは属する多数の端末と各種のサーバ利用、さらにＰＯＰによるメール受信やダイヤルアップサービスなど、本センターの計算機サービス利用に関して「あるアカウントに対応するパスワード」を統一することを徹底した。

3　パスワード変更促進策の内容

3.1　Web ベースのパスワード変更ページの実装

2000年3月までのシステムにおいては利用者によるパスワード変更は

- 学内端末のパスワードはＯＳ (NEXTSTEP) 付属のＧＵＩツールによる変更
- メールサーバのパスワードはメールサーバ自身へのシェルログインを経てＣＵＩ（passwdコマンド）による変更

となっていた。メールサーバと端末とでそれぞれパスワードを設定する必要があり、さらにそれらのユーザインタフェースが統一されていなかったため、特にメールサーバを学内端末から主に利用する学部学生はしばしばパスワードの管理方法について混乱をきたし、利用者問い合わせが相次いだ。

2000年3月以降の現行システムにおいてはシングル・サインオンが徹底されたため利用者の管理するパスワードはひとつで済むようになった。しかしNIS+ではパスワード情報を利用者自身がアクセスするためのネットワークパスワードをログインパスワードと一致させるための作業を利用者自身が行う必要があり、このためにＯＳに用意されているＣＵＩツールは一般の利用者には到底使いこなせないものであった。

そこでネットワーク上のどこからでも利用者が統一されたＧＵＩでパスワード変更作業ができるよう、Webベースのパスワード変更ページを自作した。このパスワード変更ページは、当初本システムの「利用者管理システム USAGI」（学内利用者が自らのアカウント作成をオンラインで行うシステム）の一部として実装し2000年4月7日に公開したが、

- 利用者管理システムの実装上、その一部として実装すると学内ネットワークからのアクセスに制限されざるを得なかったのだが、パスワード変更は学外ネットワークからの可能としたい
- そもそもパスワード変更はアカウント作成とはサービスの質が違う

図１：パスワード変更ページ

ことから、独立したサービスとして全面的に実装をやり直して 2000 年１１月８日に公開した。その後さらにシングル・サインオンを徹底するため、システム内メールサーバの APOP パスワードを同時に変更する機能を付加して現在に至っている（図１）

NIS+マスタサーバと https サーバを別マシンが担当する構成にする必要があったため、変更ページはやや複雑な実装になった（図２）。

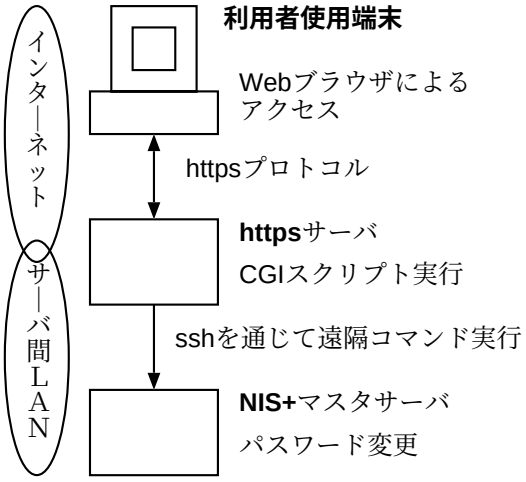

図２：パスワード変更ページの実装概要

3.2　メール等による警告

各種ガイドライン [3][4] も参考に、1997 年度から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行ってきた。

(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警告を行うこととした。警告の間隔９０日の設定は、学生が通学する大学暦の半期の間に一度以上警告が行われることを目安にしている。

方法としては、NIS+クライアントでパスワード情報から利用者毎の最近パスワード変更日を毎日１回採取し、自動的に該当者にパスワードを変更するよう促す警告メールを送付するとともに、メールサーバへのシェルログインに際するログインメッセージの出力設定を行なった。警告メールにはパスワード変更用ページへの案内を付けた。また、警告メール送付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ては、125 日ごとに再度警告メール送付を行なった。

機種更新前のシステムにおいても同様の警告メール送付を行なっていた [5] が、本システムにおいては導入後も数カ月のあいだパスワード情報中のパスワード変更日情報が安定して正しい情報を出せなかったため、警告メールの送付再開は結局 2000 年 11 月 16 日となった。

(2) アクティブパスワードチェック

本システムにおいてパスワードを検査し、破られやすいパスワードを使っている利用者に対し警告を行うこととした。

方法としては本システムのもつ CRYPT 暗号化されたパスワード情報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、チェックに該当した利用者には早急なパスワード変更を促す警告メールを送付した。警告メールにはパスワード変更用ページへの案内を付けた。

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、実際には不定期の実施になっている。

4　警告メールの効果

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、2000 年６月からの約１年間の日毎パスワード変更数を図３に示す。警告再開日以降、明らかににパスワード変更者数が増加している。

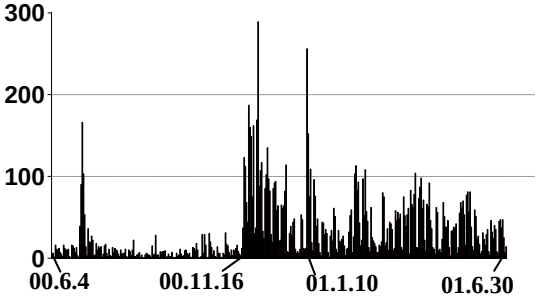

図３：パスワード変更者のべ人数の推移

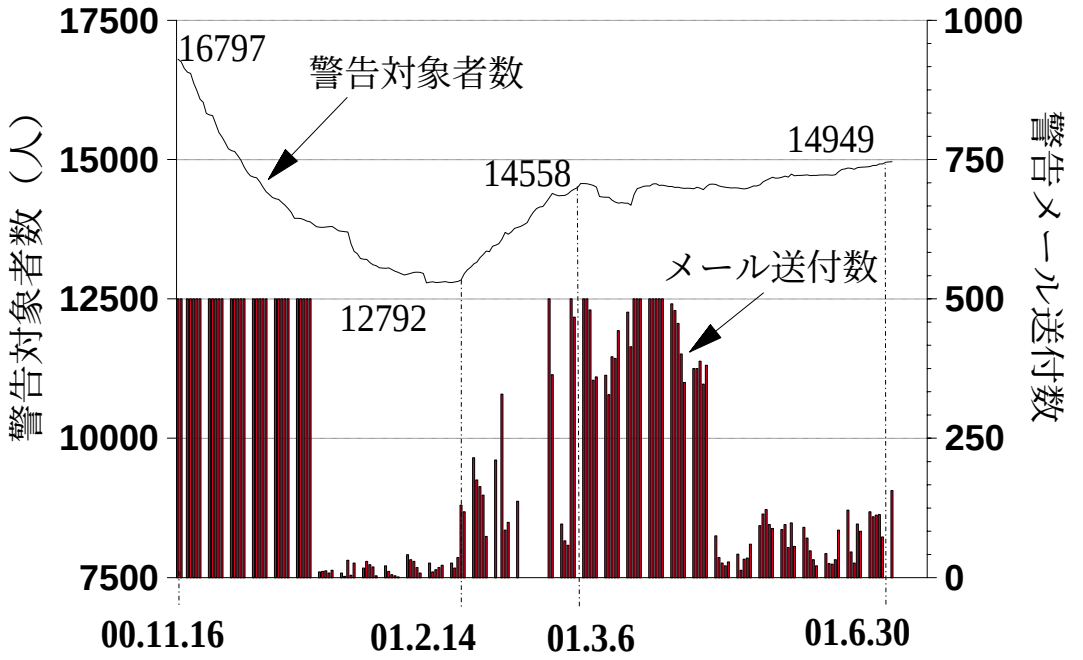

図４：警告対象者数、警告メール送付数の推移

さらに警告対象（９０日以上パスワード変更を行なっていない）のアカウント数（折れ線）と警告メール送付数（棒）を図４に示す。ただし警告メールは問い合わせ対応を考慮して、月～金曜日の朝に１日あたり５００通を限度として送付している。

警告再開当初は警告メールに呼応して警告対象数が減少しているが、その後さらに９０日経過して２度目の警告が行なわれる時には逆に増加していき、一定数に達してほぼ横ばいになっている。これは警告に対する「慣れ」から警告メールを無視してパスワードを変更せずにおいた利用者が相当数いることを表しているものと思われる。

そこで、警告メールが利用者にどのくらいのインパクトを持っているかを評価するために、警告対象者がメールを受け取った後で実際にパスワードを変更したかどうかを集計した。再開直後 (警告メール送付が 00.11.16-00.12.29 のもの) のインパクトと、２度目以降 (警告メール送付が 01.2.14-01.6.23 のもの) のインパクトの違いを調べた。また、学部学生についてはセンターが一括登録しているため、実際には使っていないアカウントが含まれていることを考慮して、学部学生を除いた集計も付した。

警告再開直後のパスワード変更率は３割弱、学部学生を除いても４割弱である。また２度目以降の警告に対する変更率は約５%低下しており、警告への「慣れ」の程度が定量的に表れていると考えられる。

警告メール送付日	メール送付数	パスワード変更数（変更率）
00.11.16-00.12.29	17000	4577(27.9%)
〃（学部学生除く）	6219	2181(36.1%)
01.2.14-01.6.23	19098	3965(21.8%)
〃（学部学生除く）	8249	2601(32.5%)

表１：警告メールによるパスワード変更率

5　まとめ

2000 年３月に運用を開始した本センター情報システムでは、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。このシステム上で利用者のパスワード管理を支援するために、２０００年１１月からパスワード変更促進策を再開し、その効果を評価した。再開当初には明らかな効果が表れたが、何度か警告メールが届くうちに利用者が慣れてしまい、警告が放置される傾向があることがわかった。

なお、従来の CUI によるパスワード変更ではなく、Web ブラウザを使うパスワード変更ページを導入することによって利用者と利用者対応スタッフの負担が軽減される効果も大きいと思われる。今回は定量的な評価ができなかったが、例えば利用者から

の質問受け付けメール窓口ではそのページを紹介することで回答が済むようになり、問い合わせ対応が格段に楽になっている。

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。今回の研究をもとに、パスワードをはじめとする利用者認証のより安全な運用方法について、利用者動向を考慮しつつ検討を行ないたい。

謝辞

このパスワード変更促進策の実践にあたり、広島大学情報メディア教育研究センタースタッフの協力を得ました。特に USAGI 版パスワード変更ページの製作に携わった岩沢和男氏には、利用者から見たパスワード変更の問題点や利用者管理の考え方について、多くの示唆をいただきました。またパスワード変更ページへの APOP パスワード同時変更機能の付加実装は田島浩一氏の協力によるものです。記して感謝します。

なお、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）の支援を受けました。

参考文献

[1] 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.

[2] 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.

[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] 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, “パスワード変更警告メールに対する利用者の反応”, 学術情報処理研究 No.4, pp.99-103, 2000.