大学情報基盤におけるパスワード定期更新の運用と利用者動向

Control of password periodic change and its user trends in university information infrastructure

長谷川孝博†，松村宣顕†，高橋秀年†，井上春樹†
Takahiro Hasegawa†, Noriaki Matsumura†, Hidetoshi Takahashi†, Haruki Inoue†

†静岡大学情報基盤センター
†Center for Information Infrastructure, Shizuoka University

概要

構成員約 12,000 人（アカウント総数約 13,000）の国立大学法人において，120 日間のパスワード定期更新の管理策をシステム要求として徹底実践した場合に起こる課題と成果を 8 年間の運用実績とデータに基づき考察した．パスワード定期更新の管理策を順当に履行できる利用者は約 7 割であった．残る約 3 割のパスワード失効者および忘失者に対して「ID カード認証するパスワード自動再発行機」，「指静脈の生体認証を用いた無人パスワード自動再発行機」および「窓口における対面の再発行申請手続き」を併用して対応した．「ID カード認証するパスワード自動再発行機」が最も有効に機能し，その他の再発行機能が補助的に機能した．その結果，長期に亘る本管理策運用が可能であることが示された．

キーワード
パスワード，情報セキュリティ，ISMS，ITSMS

1. はじめに

近年，世界的な発展を遂げた SNS や電子商取引サイトは，趣味嗜好にも及ぶ個人情報をインターネット上の各所に預ける状況を生み出している．また多くの学術機関においても，情報システムの統合認証化が進み，数千から数万人の単位で個人認証の窓口がインターネット上に公開されている．これらの情報を守る個人認証の仕組みとして，生体認証等の技術[1-3]が研究開発されてきたが，安価で汎用性に足る世界標準の仕組みの普及には至っておらず，ユーザ名（UID）とパスワードによる個人認証は現在でも主流である．そのため，IT サービスの運営組織では，利用者に対して各人の認証情報の管理をいかに適切に行わせるかが重要な課題となっている[4]．これらに係わるリスクの軽減に対し，ISMS[5-8]では情報セキュリティの管理策の一つとしてパスワード定期更新が謳われている．しかしながら，教育と啓発活動に頼るだけで，全ての利用者に適切なパスワード定期更新の管理策を実践させることは容易でない．パスワード有効期限などのシステム的な制約を設けることでパスワード定期更新の徹底を図ることはできるが，その場合，多数のパスワード失効者を救済できるサービス窓口の対応能力が重要となる．仮に，パスワードの再発行業務に遅延や障害が生じれば，組織運営の支障へと直結しかねない．したがって，認証情報の適切な管理策と実装手法について検討することは重要である．

本報では，120 日間隔のパスワード定期更新管理策を 12,000 名規模の大学組織に対して長期間運用した場合に起こる本管理策の有効性と課題について明らかにする．また，本管理策下での利用者の動向についても明らかにする．

著者連絡先：
†静岡大学情報基盤センター　cii@sains.shizuoka.ac.jp

2. パスワード定期更新の実装

2.1. 管理策の概要

静岡大学情報基盤センター（以後,「センター」という）では, 学内の大部分の教職員と全学生に対して, 全学情報基盤システム利用のためのアカウントを発行している. このアカウントを取得することで認証連携されたメール, 教育用情報端末, ホームページ開設, 無線 LAN, 情報コンセント, シンクライアント, 入退室システム等の学内 IT サービスを利用することができる. 認証情報はユーザ名とパスワードから構成されているが, このうち, ユーザ名は部外者にも容易に類推可能である場合が多く, 実質のセキュリティはパスワードの運用の確からしさに大きく関わっている.

センターでは, 約 13,000 の全てのアカウントに対するパスワード定期更新をシステム要求として組み入れることで, 管理策の徹底を図っている. 定期更新期間は 120 日毎であり, 利用者はこの期間内にパスワード変更を行うことによりアカウントの継続利用が可能となる. 実施期間は 2006 年 4 月より 2013 年度 5 月の現在に至る 8 年目の運用を経ている.

2.2. 管理策の実装手法

パスワードの定期更新管理策を実装するための各機能について述べる.

1) パスワード期限通知機能

パスワード管理システムは, 120 日のパスワード有効期限が残り 30 日, 14 日, 3 日, 2 日, 1 日になった時点で自動的にパスワード変更依頼のメールを利用者である教職員学生宛に送信する. パスワード変更依頼のメール通知文を図-1 に示す.

本機能は利用者の定期更新の忘失を回避するために必要性の高い機能であった.「7 日前の通知も欲しい」などの要求を受けた.

2) アカウントロック機能

120 日の有効期限内にパスワード変更が行われなかったアカウントはロックされ, サービス窓口でパスワード再発行処理が行われるまで休止状態となる. 休止状態時にはセンターが提供する全てのネットワークサービスを利用できない.

利用者に対して重たい処置であり, 長期休暇明けなど大量の忘失者を出した場合には組織運営に影響を与える事態に成りかねない. 本管理策の認証基盤への組み込みが敬遠される理由の一つであると考えられる. 後述するように, 円滑なパスワードの変更および再発行機能を実装することでこの問題に一定の解決を図ることができる.

○○○○様

For foreign student, refer to
http://www.○○○○○○○○○○○○○○_English.html

日頃より, 静岡大学情報基盤センターのサービス運用に
ご理解, ご協力いただきありがとうございます.

このメールは有効期限をお知らせするためにパスワード管理サーバより
自動配信させていただいております.

あなたのパスワードの有効期限が残り 14 日となりました.
有効期限内のご都合のよい時期に
http://www. ○○○○○○○○○○○○（学外アクセス可能）
よりパスワード変更処理を行って下さい.
http://www. ○○○○○○○○○○○○（学内のみアクセス可能）
をご参照下さい.

※有効期限が切れるとメール転送・作成ホームページ閲覧が停止します.
パスワード再発行で自動的に再開されます. 停止から再開までの間に受信
したメールは転送されません. 再開後, パスワード失効中のメール閲覧方
法は, http://www. ○○○○○○○○○○○○（学内限定）
をご参照下さい.

図-1：パスワード変更依頼のメール通知文

3) パスワード変更と再発行機能

利用者は定期的なパスワード変更または不定期の再発行処理によりアカウントの継続利用が可能となる. パスワードの「変更」とは「パスワードの有効期限切れも忘失もしていない」利用者のみが行える. 一方,「再発行」とは,「パスワードの有効期限切れまたは忘失」をした利用者が行う. 利用者は, (a)の「変更」および, (b), (c), (d)の「再発行」機能が利用できる. (a)－(d)の各方法について述べる.

(a)法：Web による変更

利用者はパスワード変更の Web サイトにアクセスし, パスワード変更操作を行うことができる. 本サービスを利用するには, 有効期限内にある現在のパスワードを覚えている必要があるため, パスワード定期更新の管理策を順当に履行できている利用者であると判断できる. 管理策開始直後

は学内 LAN に閉じたサービスとしていたが，長期出張者や学内 LAN に長期間接続できない利用者への対応にたびたび問題を生じていたため，2010 年に変更サイトをインターネット上へ公開した．

設定するパスワードは，スペースを除くキーボードから入力可能な通常の記号文字で構成することができ，一定の複雑さを満たすことを条件としている．一方，1 世代前のパスワード，Web サイトログイン時に使用したパスワード，ログイン ID と同じパスワードの使用，そしてログインから 5 分以上かけてのパスワード変更操作は不可である．

(b)法：ID カードによる自動再発行

利用者は，ID カード（学生証，教職員証）をパスワード自動再発行機（図-2）のカードリーダに翳すことにより，新しいランダム文字列の有効なパスワードを受け取ることができる．カードリーダの下が小型の熱転写プリンタとなっており，カード手前のスロットからパスワードシートが利用者へその場で排出される仕組みである．パスワード再発行にかかる時間は 5〜10 秒ほどである．

図-2：パスワード自動再発行機

図-3：パスワード再発行シート

図-3 は，図-2 から発行されるパスワードの発行シートの例である．パスワードと発行日付のみが記されており，シートを遺棄した場合にも不正ログインなどの事故へ発展しないよう配慮した．

ID カードを紛失した場合，第三者による成りすまし発行が可能となるため，管理室の付近に設置，監視カメラによる利用監視などを行っている．

(c)法：ID カードと生体認証による自動再発行

パスワード自動再発行機をセンター管理室受付から離れた場所に設置，あるいは 24 時間運用を行うにあたり，本人確認をより高めるために事前に登録した指静脈情報と ID カード情報の双方を確認する認証方式も取り入れている．指静脈をスキャンする初回のみ，サービス窓口で対面の登録作業を必要とする．発行されるパスワードシートは図-3 と同じである．本発行機は，損壊行為のリスクが低い場合には，無人領域に設置でき，監視カメラの設置も必須ではない．

(d)法：再発行申請手続きによる再発行

ID カードの破損や汚損によって，カードリーダで読み取りエラーとなる場合，利用者はパスワード再発行申請書をサービス窓口へ提出することができる．センタースタッフは，本人確認を行った上で管理室内の専用管理用サイトからパスワードの変更を行い，その場で申請者に渡す．一連の処理を対面で行う窓口サービスであり，最も人的資源と時間を要する．

3. 利用者動向

3.1. 発行機能別の利用者の動向

前述した各パスワード変更および再発行方法 (a)－(d)法に関する 2012 年度の利用者動向を以下にまとめる．

(a)法

Web サイトアクセスによる各月のパスワード発行件数を図-4 に示す．パスワード変更の利用総数は 1 年間で 22,004 件であった．4 月と 10 月に件数が多いことは新入生や新規採用教職員がアカウント通知書を受け取った後に覚えやすいパスワードに変更すること，ならびに前後期授業開始に伴うパスワードの再取得に起因し，7 月と 1 月の件数が多いのはパスワード有効期間が 120 日であることから 4 月と 10 月に連動している為

と考えられる．本学の 2012 年 5 月 1 日現在の学生在籍数は 10,389 名であり，教職員数ならびにその他の目的で利用される少数のアカウント等を合わせると 13,000 を超えるアカウントが存在する．このうちの約 10,000 のアカウントが有効に利用されていると仮定した場合，120 日の変更規則によれば，年間 30,000 回以上の変更がなされるはずである．したがって，「パスワードの定期的な変更」をシステム要求として強制的に行った場合，約 7 割程度（73%=22,000/30,000）の利用者が，変更期間内に Web によるパスワード変更処理を実施しているものと判断できる．

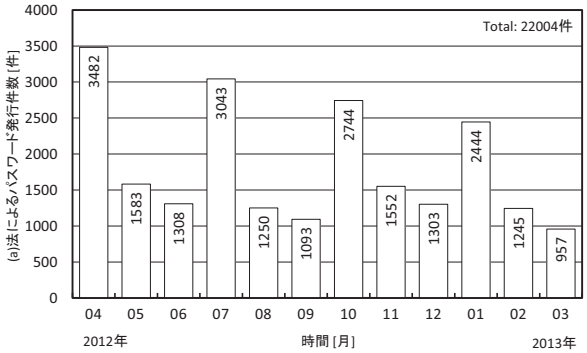

図-4：(a)法によるパスワード変更月別件数

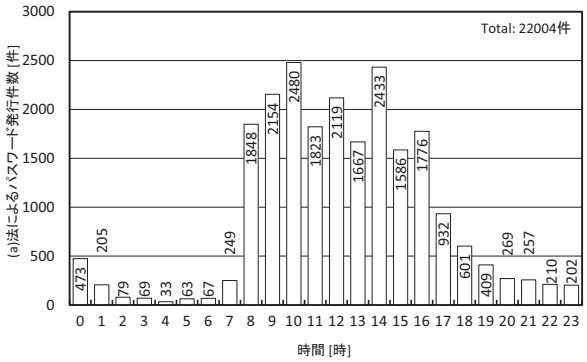

図-5：(a)法によるパスワード変更時間別件数

図-5 は(a)法によるパスワード変更の時間別利用件数である．10 時，14 時台をピークに 17 時以降は徐々に件数が落ちていく中，0 時台にアクセスが若干増えている．これはパスワード有効期限が残り少なくなった際に通知される「パスワード変更依頼メール」が毎日 0 時台に該当者に送信されるためであると推測される．深夜帯のアクセスは出張先，自宅や研究室からの利用が考えられる．深夜利用者の数は少ないが出張等で通常の利用時間とは異なる時間帯にパスワード変更する必要がある場合もあるため，24 時間利用可能なシステムは有効となる．

最後に，4 月から 9 月の前半期でパスワードの変更のピークを分析した．その結果，最も利用件数の多い日時は 4 月 10 日の 11 時台で 124 件であった．授業開始が 10 日であり，この日だけで 580 件のパスワード変更が Web により行われていた．

(b)法

ID カード認証によるパスワード自動再発行機の月別利用件数を図-6 に示す．月別件数を比較するとパスワード自動再発行機はパスワードの忘失時だけではなく，パスワード変更を行わずに期限切れとなってロックされたアカウントの有効化に対しても利用されているため，前後期の授業開始時期や長期休暇明けに利用率が高くなっている．

パスワード定期更新の管理策を開始した 2006 年当初には，自動再発行機が実装されておらず，(d)法の窓口対面による「再発行申請手続き」だけで対応していた．その結果，繁忙期の窓口は大混雑となり，管理策の破綻状態にあった．本法を導入した 2007 年 10 月以降から安定的な管理策の運用が可能になった．人手を介さない自動再発行の仕組みは，本管理策の運用に必須である．

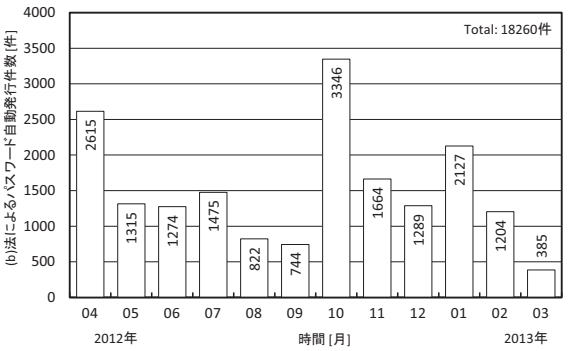

図-6：(b)法によるパスワード再発行月別件数

図-7 に(b)法の時間別利用件数を示す．全体的には休み時間の関係で 11 時と 13 時に落ち込んでいるが，正午をピークとした正規分布に近い．パスワード自動再発行機は 24 時間利用可能な状態であるが，設置建屋の入室制限等もあり，利用のあった時間帯は 8 時～21 時台までとなっている．

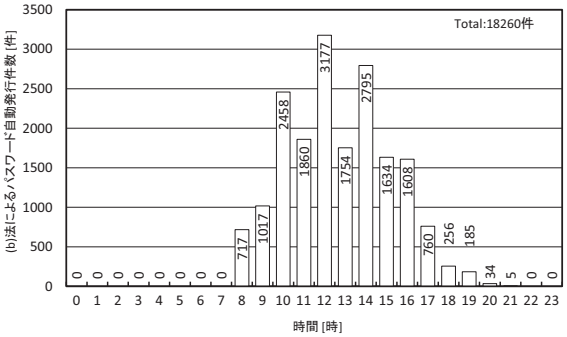

図-7：(b)法によるパスワード再発行時間別件数

(c)法

ID カードと指静脈認証による自動再発行機[3]を使用したパスワード再発行は1年間で112件の利用にとどまった. 図-8 に本法の月別利用件数を示す. 本法が利便性と高セキュリティを兼ね備えているにも係わらず利用者数が伸びない理由として，1) 窓口における指静脈登録時の手間がかかる，2) 利用者が求めるセキュリティ意識レベルに合致していない, 3) (a), (b)および(d)法によって，管理策の運用がほぼ充足されている，4) 指静脈データは, 高度な不可逆の暗号化を行った上で認証サーバに保持されるが, 生体情報をスキャンされることに利用者の抵抗感が払拭できていない，などが挙げられる.

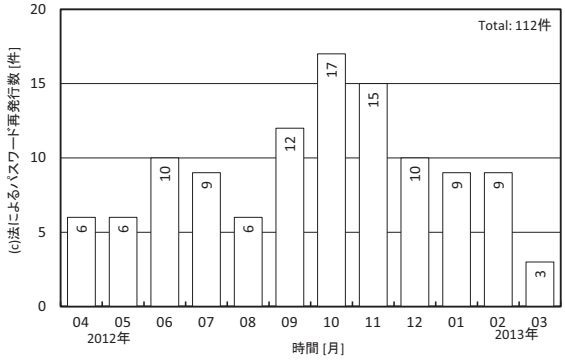

図-8：(c)法によるパスワード再発行月別件数

(d)法

センタースタッフが管理用サイトからパスワードの再発行を行った件数は1年間で674件であった. 図-9 にパスワード再発行申請手続きによる月別再発行件数を示す. 前後期授業開始の 4 月と 10 月にその他の月の 2 倍から 3 倍に再発行件数が増えていることが分かる. 発行処理は，窓口でスタッフと対面で行われ, 申請書の記入も必要なるため， 1 人当たり 3 分程度の時間を要する.

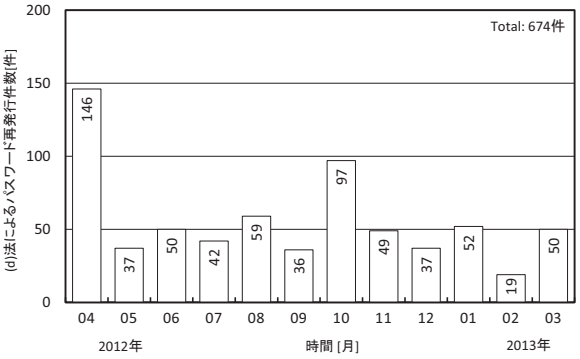

図-9：(d)法によるパスワード再発行月別件数

3.2. その他の利用者の動向

本学では, S キャンパスと H キャンパスの主要 2 キャンパスがあり，それぞれ 267 台，195 台の教育用情報端末が整備された演習室がある. この主たる利用者は演習室で行われる授業に出席する学部生であり，平成 24 年 5 月現在の在籍状況は S と H キャンパスでそれぞれ 5499，3354 名であった．各キャンパスでは，(b)法と(c)法の自動再発行機までの距離に大きな差がある．S キャンパスではその距離が近く, H キャンパスでは棟を隔てたかなり遠い距離にある.

図-10 は「(b)法によるパスワード自動再発行の後の当日に(a)法によって Web からのパスワード変更を実施した利用者数」の月別変位である.

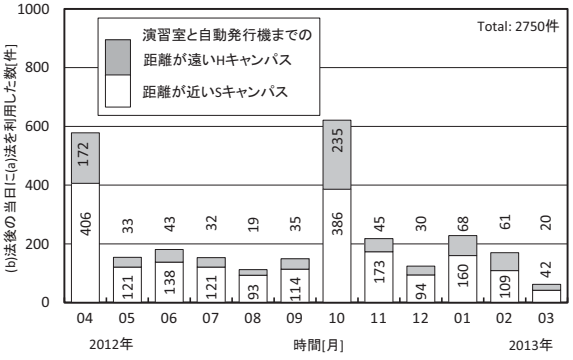

図-10：(b)法後の当日に(a)法でパスワードを再設定した利用者数のキャンパス別の変位

図-10 と図-6 を比較すると，(b)法で受け取ったランダム文字列のパスワードを, 覚えやすい自分のパスワードに変更する利用者が少ないことが

分かる．たとえば，ピークの 10 月においては 18.5%（=621/3346）の利用者しかパスワードの変更を行っておらず，残りの 8 割程度の利用者は，図-3 に示したパスワード再発行シートを保持して，初期再発行のランダムパスワードをそのまま利用し続けていると考えられる．

学生数の多い S キャンパスでの利用数が各月とも H キャンパスを上回っているが，これは総数 8853 名の学部生の比率が S：H＝62:38 で分かれていることの要因も含まれる．そこで，「(b)法後の当日に(a)法を利用した数」を「(b)法を利用した数」で除した値を各キャンパスについて算出し，人数比の影響を小さくして観察した．図-11 に結果を示す．

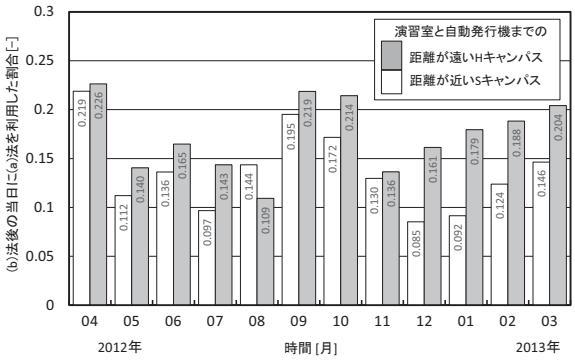

図-11：「(b)法後の当日に(a)法を利用した数」と「(b)法を利用した数」の割合

11 月と 12 月を境界として明確な違いが現れている．11 月までの割合はほぼ拮抗しているが，12 月以降では H キャンパスの学部生が，S キャンパスの学部生よりも高い率で，(b)法の後に(a)法を利用してパスワードを覚え易いものに変更していることが解る．これは自動再発行機が遠いことを学んだ H キャンパスの利用者らの自主的な行動と考えられる．一方で，S キャンパスではその逆の学習，すなわち「パスワードはいつでも簡単に得られる」と学習されてしまい，ワンタイムパスワード的な利用が多くなっていると考えられる．

このような利用者の動向は，自動再発行機の設置数を少なくしても，パスワード定期変更の管理策の運用を助ける方向に働くことを示唆するものであり，本管理策の浸透を制御し得る一つのパラメータと成り得る．また，自分のパスワードを管理しようという意識と行動が薄れる意味で「サービスへのアクセスが便利なほどセキュリティが低下しがち」という情報セキュリティと IT サービスの利便性のバランス関係をよく表しているとも言える．

なお，本運用では各キャンパスに (b)法と(c)法の自動再発行機をそれぞれ 1 台ずつ設置しているに過ぎない．1 万人規模の利用者に対して，この台数が一つの目安になると思われる．

4. 考察

ISMS では，パスワードを定期更新するよう「利用者に助言」することが求められている．ここで「助言」に留めているのは，冒頭に述べたようなパスワード定期更新の管理策における理想と現実の乖離があるからだと思われる．この問題は，企業組織と比較して，統制力の弱い大学・学術組織においては，より顕著に現れているものと思われる．

自動再発行機のアクセス件数は，毎年 15,000 件以上であった．この数は全構成員が年 1 回以上利用した数に相当する．定期更新を「助言」や「啓発」の域に留めている組織の場合でも，パスワード認証システムの下では，定期的なパスワード変更が求められ，また，パスワードの忘失はなくならないことから，IT サービスレベル向上のマネジメント活動[9]を意識すれば，自動再発行機の設置は重要である．

近年，パスワードの定期更新よりも使い回しの問題が取り沙汰されている．しかしながら，それはパスワード定期更新の重要性が低下したという意味ではない．銀行，大手ポータルサイトや SNS では，継続的にパスワードの定期更新が啓発され続けている．IT サービス提供者がパスワード管理策の維持向上に努めることは，利用者への情報セキュリティに関する教育，啓発の端緒としても合理的に機能する．

本報で論じた全組織的なパスワード定期更新の運用は単純かつ明快であるがゆえ，そこで起こる利用者動向，課題，その有効な解決策についても端的な結果が示されたのではないかと考える．

5. まとめ

有効アカウント数約 10,000（発行総数は約 13,000）を有する国立大学法人において，パスワード定期更新の管理策をシステム要件として完全実装した場合に起こり得る状況を以下にまとめる．

1) パスワード定期更新の管理策を順当に履行する利用者は 7 割程度であり，残る 3 割の利用者に対する有効な再発行の手段を用意する必要がある．

2) (a)法の Web 変更手段は，7 割程度におよぶ管理策の順当な履行者をサポートする重要な機能である．長期または海外出張者をサポートするためには，学外からのアクセスが可能な 24 時間運用のサービスにすることが必要であった．

3) (b)法は, 再発行の手段として最も有効であり，必須の機能と判断できる. 他人の ID カードで成りすましの再発行が可能であるため，監視カメラによる装置監視は必須である．

4) 生体認証を用いた(c)法は，セキュリティ的には最も堅牢であるが，利用者数は伸びない．その理由は「3.利用者動向」で述べた．

5) 従来型の窓口サービスである(d)法は，最後の救済手法として必須である. 年間 600 から 700 件程度の再発行が見込まれる．そのうち 4 月と 10 月の授業開始月に，100 から 150 件が集中する．さらに各ピーク月内では授業開始直後の週に集中している．窓口サービスには，これらの発行数に耐え得る発行効率と安全性を兼ね備えた手順の確立が求められる．

6) (a)法による変更と(b)法による再発行の総数は，年間 40,000 回を超えている．これは約 10,000 人の利用者が年間 3 回以上のパスワードの変更または再発行した数に相当する．したがって，(a)法と(b)法の組み合わせは本管理策の運用における必須かつ主要な機能である．

7) (b)法によるパスワード自動再発行のランダム文字列パスワードを当日中に変更した利用者は 18%程度であった．ただし，演習室から自動再発行機までの移動距離が長い設置場所の利用者には，(a)法を用いて覚えやすいパスワードに変更する割合が高くなる傾向が観察された．一方，自動再発行機までの移動距離が短い利用者は，再発行のランダムパスワードを変更することなく，ワンタイムパスワード的に自動再発行機を利用する傾向が観察された．自動再発行機へのアクセスの容易さ（距離や設置台数）が，本管理策の浸透を図る上で，一つのパラメータと成り得る．

本論文の結論を次にまとめる．すなわち，120 日間隔のパスワード定期更新管理策を 12,000 名規模の大学組織に対して長期間運用することは可能であった．そこでは，少数台のパスワード自動再発行機を利用者との近すぎない距離において運用することが, 管理策の履行率を高める効果として観察された. 管理策の有効性の一つとして, 管理策を順当に履行する 7 割の利用者が観察された．

参考文献

1) 居城秀明，金岡晃，岡本栄司，金山直樹: タッチパネルによる手指の行動的特徴を用いた生体認証に関する一考察，情報処理学会研究報告マルチメディア通信と分散処理(DPS), Vol.2013-DPS-154, No.15, pp.1-8 (2013).
2) 春日大樹，大和田勇人: 眼底画像を用いた位相限定相関法によるバイオメトリクス認証, 情報処理学会第 74 回全国大会講演論文集, Vol.2012, No.1, pp.25-27 (2012).
3) 戸部剛男，長谷川孝博，水野信也，井上春樹，山崎國弘，吉田仙良: 指静脈認証統合システムによるリスク管理手法，情報処理学会研究報告インターネットと運用技術(IOT), Vol.2010-IOT-10, No.8, pp.1-4 (2010).
4) 西垣桂，齊藤明紀: 省力化を実現するための忘失パスワード再設定システム，情報処理学会研究報告インターネットと運用技術(IOT), Vol.2009, No.21(2009-IOT-4), pp.173-178(2009).
5) JIS Q 27001: 2006 (ISO/IEC 27001:2005): 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項，日本規格協会 (2006).
6) JIS Q 27002: 2006 (ISO/IEC 17799:2005): 情報

技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範, 日本規格協会 (2006).
7) 長谷川孝博, 井上春樹ら: 実践 ISMS 講座 情報セキュリティマネジメントと経営戦略, 静岡学術出版理工学新書 (2007).
8) 井上春樹, 長谷川孝博ら: 大学の IT コンプライアンス Vol.1, 静岡学術出版理工学新書 (2007).
9) JIS Q 20000-1: 2012 (ISO/IEC 20000-1:2011): 情報技術－サービスマネジメント－第 1 部:サービスマネジメントシステム要求事項, 日本規格協会 (2012).