パスワード再発行方式の安全評価と最適な利用法の提案

久保駿介[1]　杉本大輔[1]　上原哲太郎[2]　佐々木良一[1]

概要： 近年，不正に入手した情報を利用したアカウントの乗っ取りが多発しており，パスワードの設定方法などに関して様々な注意喚起が行われている．しかし，どんなに安全性の高いパスワードを設定しても，パスワード再発行時に脆弱性があると安全性は失われてしまう．ここでパスワード再発行とは，パスワードを忘れた際場合などに新規パスワード作成のため，アカウントの管理先が行う手続きのことを指す．本研究では，パスワード再発行の調査を行い7つの方式があることを明確にするとともに，各方式の安全性の評価を行った．その結果，“ページ方式”の安全性が最も低いことを明らかにするとともに，この方式によってメールアカウントを取得し，それを利用し安全性の高い他サイトのアカウントを取得した場合，安全性の高い方式のアカウントの安全性が低くなることを示した．あわせて，それらの問題点を解決する方法の提案を行っている．

Safety verification of password reissuing method and proposal of most preferable usage method

SHUNSUKE KUBO[1]　DAISUKE SUGIMOTO[1]
TETSUTARO UEHARA[2]　RYOICHI SASAKI[1]

1. はじめに

昨今，不正に入手した情報を利用したアカウントの乗っ取りが多発しており，パスワードの設定法などに関して様々な注意が行われている．しかし，いかに強いパスワードを設定していても，パスワード再発行時の脆弱性をつかれると簡単になり済ましが行われてしまう．現実にパスワード再発行時の脆弱性を利用して，メールを盗み見たという事例も報告されている[1]．パスワード再発行とは，パスワードを忘れた場合などに，新規パスワードの作成のため，アカウントの管理先が行う手続きを指す．

本研究では，種々のパスワード再発行方式の調査を行い，その安全性を実験により評価するとともに，パスワード再発行による乗っ取りを防ぐ手法の提案を行う．パスワード再発行に関する既存研究[6,7,8,9]では，安全性評価や新たな再発行方式の提案などがなされているが，本研究のようにパスワード再発行全体の安全性を評価するアプローチは従来行われていなかったと考える．

2. パスワード再発行方式の調査と分析

2.1 研究概要[2]

パスワードの再発行方式の提案にあたり，まず既存のパスワード再発行方式の種類と問題点について調査を行う．ここでは，パスワード再発行の方式の調査を行い，手続きのパターンを分類し，その結果を用いてフォルトツリー分析を行い，パスワード再発行の最適な方式の提案や問題点の指摘を行った．以下より，行われた調査と分析の結果と挙げられた問題点について述べる．

2.2 調査概要

2.2.1 調査方法

パスワードの再発行方式を調査するにあたって，実際にパスワードの再発行が行われるWebサイトについて調査を行う．具体的には，アカウントの登録を必要とするWebサイトの，初期に設定している再発行手続きの方式について調査を行う．

2.2.2 調査対象サイトについて

調査対象のWebサイトは，ユーザ規模，知名度，ジャンル，Alexaランキング[3]を参考に30サイト選択した．

2.2.3 再発行手続きで要求される情報について

調査対象のうち，最多のものはメールアドレスで，続いて生年月日，秘密の質問，氏名，ID，電話番号となった．また，少数ではあるが郵便番号，ニックネーム，クレジットカード番号などがあった．

2.2.4 再発行手続きの方式について

以下に分類した再発行手続きについて示す．

URL 型

再発行要求後，登録したメールアドレスにメールが送信され，メールに記載された URL から再発行手続きのページに行く．

1 東京電機大学
Tokyo Denki University

2 立命館大学
Ritsumeikan University

認証キー型

再発行要求後，登録したメールアドレスにメールが送信され，メールに記載された認証キーを Web サイトで入力し再発行を行う．

パス発行型

再発行要求後，登録したメールアドレスにメールが送信され，メールに記載されている新しく発行されたパスワードを使用する．

URL&認証キー型

再発行要求後，登録したメールアドレスにメールが送信され，メールに記載された URL から再発行のページへ行き，認証キーを入力し再発行を行う．

二重認証型

再発行要求後，登録したメールアドレスにメールが送信され，メールに記載された URL から再発行のページへ行き，本人確認の情報を再度入力する．

ページ型

再発行要求後，Web ページ内で秘密の質問などを用いて本人確認を行う（メール不要）．

特殊型

再発行要求後，登録したメールアドレスにメールが送信され，メールで一部隠されたパスワードが送られてくる．

7 種の方式のうち，メールアドレスに依存しない方式はページ型のみである．

2.3 フォルトツリー分析

2.3.1 フォルトツリー作成について

上記の再発行手続きに関してリスク分析を行う．ここでは，分類した再発行の方式ごとに，フォルトツリーを作成した.頂上事象を再発行手続きにより，悪意のある第三者にアカウントを盗まれるとする.図1に，URL型のWebサイトを基にしたフォルトツリーを示す．AND記号は，配下の全ての条件が満たされた場合，成立する．OR記号は，配下のいずれかの条件が満たされた場合，成立する．

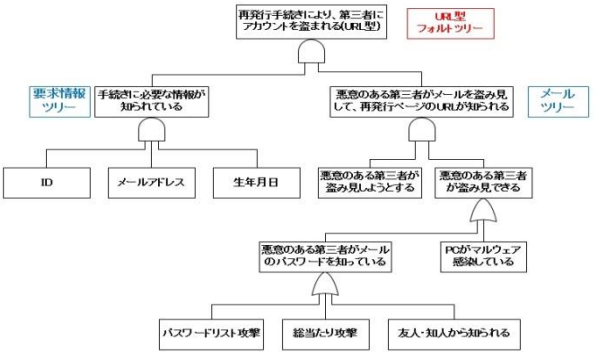

図１．　フォルトツリーの一例

それぞれのフォルトツリーにて，手続きに必要な情報が知られているという項目のツリーを要求情報ツリーとし，悪意のある第三者がメールを盗み見して，再発行ページの URL が知られるという項目のツリーをメールツリーとする．要求情報ツリーは，再発行手続きに必要な情報が，第三者に知られる場合の評価を行うものであり，メールツリーは，メールで送られてきた再発行手続きに必要な URL などの情報が，第三者に知られる場合の評価を行うものである．

2.3.2 フォルトツリーによる評価方法

図1のフォルトツリーを用いて，再発行手続きの方式についてリスク分析の説明を行う．対象として，ユーザと悪意のある第三者の関係を，研究室（会社）の同僚，友人，他人の場合の3通りとする．分析を行う際の評価値は，0に近いほど安全であり，1.0に近いほど危険である．

以下に，フォルトツリー分析で用いる評価値とそれに対応する悪意のある第三者が情報を入手する難易度について記述する．

表１．　再発行手続きに必要な情報を入手する難易度

評価値	入手難易度
1.0	公開情報，簡単に推測できる，簡単に教えてもらえる
0.1	知ることが出来る，推測できる，教えてもらえる
0.01	知ることは困難である，推測は困難である，教えてもらうことは困難である
0	知ることは不可能である，推測は不可能である，教えてもらうことは不可能である

表２．　要求情報ツリーの評価値

再発行に必要な情報	研究室(会社)の同僚	友人	他人
ID	0.1	0.1	0.01
メールアドレス	1.0	1.0	0.01
生年月日	1.0	1.0	0.01

表1の評価値を基に研究室11人に対し，再発行手続きに必要な情報を入手する難易度を4段階で評価してもらうアンケートを行い，表2の結果となった．評価値は要求情報ツリーで用いているものである．メールツリーの，PCがマルウェア感染しているという項目の評価値は，IPAの資料[4]を参考に設定している．メールツリーの盗み見しようとするという項目と，メールのパスワードを知っているという項目の評価値は，独自に定めたものである．

最終的な評価値をxとした，セキュリティ強度のランクを表3に示すように設定した．

表３．　セキュリティ強度のランク

ランク	最終評価値
A	$0 \leqq x < 0.1 \times 10^{-7}$
B	$0.1 \times 10^{-7} \leqq x < 0.1 \times 10^{-5}$
C	$0.1 \times 10^{-5} \leqq x < 0.1 \times 10^{-3}$
D	$0.1 \times 10^{-3} \leqq x < 0.1 \times 10^{-1}$
E	$0.1 \times 10^{-1} \leqq x \leqq 1.0$

2.3.3 評価による結果

フォルトツリー分析をそれぞれの方式に行った結果を表4に示す．

表４．　フォルトツリー分析による結果

再発行手続きの方式	研究室(会社)の同僚	友人	他人
URL型	C	C	A
認証キー型	C	C	A
パス発行型	C	C	A
URL&認証キー型	C	C	A
二重認証型	B	B	A
ページ型	E	E	C

評価の結果，セキュリティ強度が強い方式として二重認証型，セキュリティ強度が弱いものとしてページ型があることが明らかとなった．以下の図2にページ型のフォルトツリーを示す．

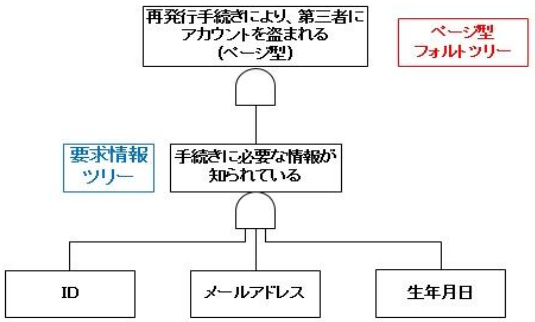

図２．　フォルトツリー分析による結果

図2から，ページ型の再発行方式が単純なものであることが見て取れる．

3.　複合型攻撃に関する検討

3.1　フォルトツリー分析による調査概要

ページ型を採用している Web サイトには，メールサービスを提供しているものもある．これらのアカウントが乗っ取られた場合，メールを利用し再発行を行う方式のセキュリティ強度が非常に弱くなり危険となる可能性がある．例えば，メールサービスを提供しているサイトのアカウントを乗っ取り，そのアカウントを利用して，強くガードされている二重認証型のアカウントを容易に乗っ取ることができる可能性がある．これが実際簡単に起こり得るかをフォルトツリー分析により評価する．

3.2　フォルトツリーについて

3.2.1 フォルトツリーの作成

頂上事象に，二重認証型の標的アカウントに不正侵入される，という事象を設定する．以下に作成したフォルトツリーを示す．

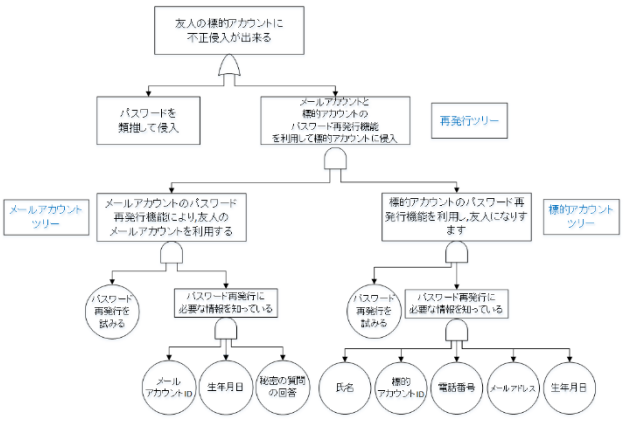

図３．　標的アカウントに不正侵入するツリー

このフォルトツリーはパスワードを類推して侵入という事象と，メールアカウントと標的アカウントのパスワード再発行機能を利用して侵入という再発行ツリーから成っている．また，再発行ツリーはメールアカウントと標的アカウントのパスワード再発行機能を利用して標的アカウントに侵入，というツリーと，メールアカウントのパスワード再発行機能により友人のメールアカウントを利用する，というツリーから成り，前者のツリーを標的アカウントツリー，後者のツリーをメールアカウントツリーとする．

標的アカウントツリーは友人の標的アカウントを乗っ取る事が可能かを評価するものであり，メールアカウントツリーは友人のメールアカウントを乗っ取ることが可能かを評価するものである．

メールアカウントツリーと標的アカウントツリーの，パスワード再発行に必要な情報を知っている，という事象の基本事象は，パスワード再発行に必要な情報を表している．

またこのフォルトツリーでは，侵入に利用する手口は特別な技術，知識を持たない一般人でも可能なものを対象としているため，パスワード再発行による侵入とパスワードを類推しての侵入の 2 つを対象としている．

3.2.2 フォルトツリーの評価と考察

作成したフォルトツリーを利用し，前章で挙げられた問題について評価を行う．評価値が 0 に近いほど安全であり，1 に近いほど危険である．

以下に分析に用いる評価値を記述する．

表 5．　パスワード再発行に必要な情報の評価値

項目	評価値
ID(メールアカウント)	0.1
ID(標的アカウント)	0.1
生年月日	1.0
氏名	1.0
メールアドレス	1.0
電話番号	0.1
秘密の質問の回答	0.1

再発行手続きに必要な情報を入手する難易度の評価値は，先行研究の評価値を参考に設定した．表 1 の評価値を元に，パスワード再発行に必要な情報に評価値を設定した結果，表 5 のようになった．この評価値を元に，値を設定したフォルトツリーを以下の図 4 に示す．

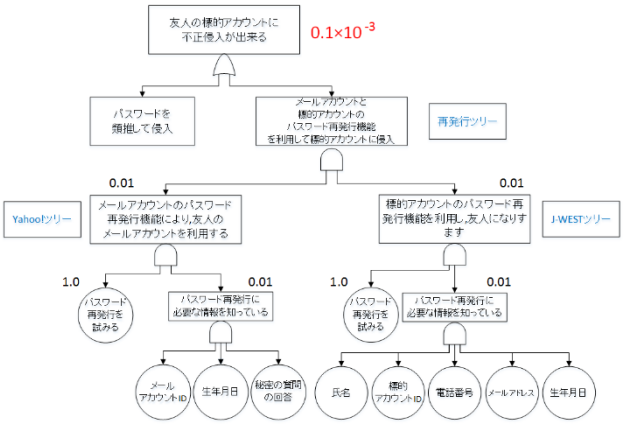

図 4．　評価値を追加したフォルトツリー

評価値を追加した結果，フォルトツリーの評価値が0.1×10^{-3}となった．作成したフォルトツリーより，この場合のセキュリティの強度ランクは表 3 の D に該当する．この結果から，先行研究で挙げられた問題は実際に起こり得る危険があると言える．そのため，このような乗っ取りを防ぐ手法が必要であると考える．

3.3 実験について

3.3.1 実験概要

フォルトツリー分析の結果，メールアカウントが乗っ取られた場合，セキュリティの強い二重認証型のアカウントが乗っ取られる危険性が高いことが明らかとなった．そこで実験を行い，メールアカウントを乗っ取られた場合に，それを利用し登録した他のアカウントの乗っ取りが成功するかを検証し，その割合を明確化する．ここでは，フォルトツリーと同じくセキュリティの強い標的アカウントとして，二重認証型を採用しているアカウントを利用する．

前提条件を以下に示す．

・友人:著者と同じ部活動に所属していた人物
・悪意のある友人は，友人のメールアカウントと生年月日，携帯電話番号を事前に得ている．
・アカウントの設定は全て初期状態
・アカウント登録では，必須項目のみ入力
・登録する情報は本人の情報を登録．

標的アカウントの再発行に必要な情報を以下の表 6 に示す．

表６．　再発行の際に要求される情報

	標的アカウント
ID	○
名前,登録名	○
生年月日	○
メールアドレス	○
電話番号	○
秘密の質問	−

3.3.2 実験方法

著者の 1 人が悪意のある人のロールプレイヤーとなり，著者が友人のメールアカウントと事前に得ている情報を利用し，標的アカウントの乗っ取りを試みる．

3.3.3 実験結果

実験の結果を表 7 に示す．

表７．　実験結果

	標的アカウント 乗っ取り
友人A	○
友人B	○
友人C	○
友人D	×
友人E	×

今回は 5 人の友人に対して実験を行い，3 人の標的アカウントを乗っ取ることに成功した結果となった．

3.3.4 考察

友人 D, E の標的アカウントが乗っ取れなかった理由としては，標的アカウントに登録された電話番号が携帯電話番号ではなく自宅電話番号であったためだと考える．

3 件の標的アカウントを乗っ取れたという結果から，メールサービスを提供しているアカウントの乗っ取りに成功した場合，そのメールアカウントを利用した乗っ取りが容易に行えてしまうと考えられる．そのため，パスワード再発行の安全性はメールアカウントの安全性に依存していると考えられる．

4.　詳細実験

4.1 詳細実験概要

3 章の結果から，パスワード再発行の安全性は，メールアカウントの安全性に依存していることが明らかとなった．そこで本実験では，セキュリティの弱いメールアカウントを乗っ取る実験を友人と研究室の同僚に対して行い，乗っ取れた割合を明確化する．

実験に用いるアカウントは，ページ型を採用しているメールアカウントとしている．

前提条件を以下に示す．

・友人:同じ部活動に所属していた人物
・研究室の同僚:自分と同期配属された人物．
・悪意のある友人は，研究室の同僚と友人のメールアカウントの ID と生年月日を事前に得ている．
・生年月日:本人の情報を登録．
・秘密の質問の回答を SNS の閲覧によって探しても良い．

4. 2 実験方法

著者の 1 人が悪意のある人のロールプレイヤーとなり，著者の友人，研究室の同僚が実験用に作成したメールアカウントの乗っ取りを試みる．なおこの実験では，再発行を要求する回数は 50 回までとしている．

4. 3 実験結果

実験の結果を以下の表 8, 9 に示す．

表８．　友人に対する実験結果

	秘密の質問	再発行 要求回数	乗っ取り
A−1	初めての習い事は	1	○
A−2	初めての習い事は	10	○
A−3	初めてデートした場所は	21	○
A−4	父親の出身地は	29	○
A−5	高校時代の所属クラブは	2	○
A−6	初めて飛行機で行った場所は	2	○
A−7	父親の出身地は	50	×
A−8	子供の頃の憧れのヒーローは	50	×
A−9	子供の頃の憧れの職業は	50	×
A−10	一番上のいとこの名前は？	50	×

表９．　研究室の同僚に対する実験結果

	秘密の質問	再発行 要求回数	乗っ取り
B-1	初めての習い事は	3	○
B-2	高校時代の所属クラブは	8	○
B-3	高校時代の所属クラブは	3	○
B-4	子供の頃の憧れの職業は	50	×
B-5	初めて飛行機で行った場所は	50	×
B-6	初めて飛行機で行った場所は	50	×
B-7	父親の出身地は	50	×
B-8	小学校の頃のあだ名は	50	×
B-9	初めてデートした場所は	50	×
B-10	初めて飛行機で行った場所は	50	×

10 人の友人と研究室の同僚に対して実験を行い，それぞれ 6 人と 3 人のアカウントを乗っ取ることが出来た．

4. 4 考察

友人と研究室の突破率の差は，秘密の質問の類推の容易さ，著者との親密度の差，セキュリティ知識の差などが表れた結果だと考えられる．また，秘密の質問のうち，“高校時代の所属クラブは”や，“初めての習い事は”の突破率が 100%であったことについては，質問に対する回答の選択肢が絞られるためだと考えられる．

以上のことから，ページ型を採用しているアカウントはパスワード再発行による乗っ取りが容易であるため，乗っ取られる危険性が高いということが言える．

5.　対策検討のための調査

5.1　調査 A

5.1.1 概要

実験結果から，ページ型を採用しているアカウントが乗っ取られやすい事が明らかとなった．そこで，調査 A では各サービスのパスワード再発行に必要な情報と，アカウントを乗っ取った際にそのアカウントから得られる情報をまとめることで，パスワード再発行がメールアドレスを必要とする割合と，アカウントからの情報入手の容易さを明らかにする．

5.1.2 調査方法

アカウントの再発行に必要な情報の調査結果と，アカウントから得られる情報[5]を纏める．調査対象は 2015 年 1 月の Alexa TOP 500 の日本からのアクセスが多い上位 50 サイトとする．

また，この実験で作成するアカウントは，全て必須項目のみの入力で作成されている．

5.1.3 実験結果と考察

調査の結果を以下の表 10 に示す．ここでの+1, +2 は再発行の際に要求される情報のうち，メールアドレス以外の情報の数を表している．

表１０．　調査結果

再発行に 必要な情報	サイト件数	突破されてしまった場合 新たに得られてしまう情報
メールアドレス のみ	18	名前,生年月日,メールアドレス,住所, 電話番号,郵便番号
メールアドレス ＋1	17	出身地,年齢
メールアドレス ＋2以上	10	なし
メールアドレス なし	3	なし
他サービスに 依存	1	なし

調査結果から，メールアドレスのみで再発行できるアカウントとメールアドレス+1 の情報で再発行できるアカウントの 2 つから，再発行に必要な情報をほとんど得られるという結果となった．そのため，パスワード再発行の安全性は，やはりメールアカウントの安全性に依存していると言える．

5.2　調査 B

5.2.1 概要

調査と実験から，パスワード再発行を安全に利用するためには，メールアカウントの安全性が重要であることが明らかとなった．そこで調査 B では，実際に無料メールサービスを扱うサービスのセキュリティ機能を調査し，それぞれのセキュリティ機能を比較することで，パスワード再発行による乗っ取りを防止する最適な手法を提案する．

5.2.2 調査方法

メールサービスを扱うサービスに登録し，そのサービスのセキュリティ機能を纏めそれぞれの機能と比較する．

調査対象は，ページ型を採用しているものを 2 件，ページ型以外を採用しているものを 2 件とする．

5.2.3 調査結果と考察

調査結果を以下の表 11, 12 に示す．ログインアラートはログインした際に，指定した連絡先へ通知を行う機能を指し，セキュリティアラートは，登録情報に変更があった場合に指定した連絡先へ通知を行う機能を指す．また，SMS 利用は通知や再発行メッセージの送信先に SMS を利用出来ることを指している．

表１１．　調査結果（ページ型）

	ログイン履歴	ログインアラート	セキュリティアラート	2段階認証	SMS利用
サービスA	○	○	○	○	×
サービスB	○	×	○	×	×

表１２．　調査結果（ページ型以外）

	ログイン履歴	ログインアラート	セキュリティアラート	2段階認証	SMS利用
サービスC	○	○	○	○	○
サービスD	○	○	○	○	○

調査の結果，同じページ型のサービスでもセキュリティ機能に差があることが明らかとなった．このことから，ページ型のメールサービスでも機能を十分に活用することで，安全に利用できるものもあると考えられる．しかし，セキュリティアラートなどはメールアドレスを乗っ取られている場合には，なり済まし者に送られるので効果はあまりなく，二段階認証機能を活用することが重要であると考えられる．

一方ページ型以外のサービスには，ページ型のサービスと比較して，SMS が利用出来るという特徴があった．この機能を活用し，再発行メッセージの受け取り先を携帯電話番号にすることで，パスワード再発行によるメールアカウントの乗っ取りの危険を防ぐことが出来ると考えられる．

6. 提案

以上の実験と調査の結果から，パスワード再発行方式を安全に利用する手法の提案を行う．

まず，先行研究で提案されていたページ型再発行方式については，パスワード再発行により乗っ取られる危険があることが明らかとなった．このことからユーザは，ページ型を採用しているサービスを利用すべきではないと考える．そしてページ型を採用している企業は，ページ型の再発行方式を廃止すべきであると考える．

また，パスワード再発行を安全に利用するためには，メールアカウントの安全性が重要であることが明らかとなった．このことから，ユーザは自分が利用しているメールサービスのセキュリティ機能を確認し，2 段階認証を適用させることが重要であると考える．また，再発行メッセージの受け取り先をメールアドレスではなく，携帯電話番号にすることでパスワード再発行によるメールアカウントの乗っ取りを防ぐことが出来ると考える．

以上 4 つをこの研究における提案とする．

7. 終わりに

本研究では，先行研究で評価された再発行方式の安全性を検証し，アカウントから得られる情報と再発行に必要な情報を調査することで，ページ型の危険性を明らかにし，パスワード再発行を安全に利用する手法の提案を行った．再発行の安全性はメールアカウントの安全性に依存しており，メールサービスを提供している企業は，パスワード再発行に弱い方式を使うべきではないと言える．また，パスワード再発行に SMS を用いることで乗っ取りの危険性を抑えられるという見通しを得た．

このような結果を受けて，弱い方式を採用している企業の責任者の方と会って，問題の指摘を行った．その結果，弱い方式を廃止する方向で検討していただけることとなった．

今後は，より安全にアカウントを運用する手法を提案していく．

参考文献

[1] 徳丸浩:Yahoo!ジャパンの「秘密の質問と答え」に関する注意喚起，徳丸浩の日記，入手先 <http://blog.tokumaru.org/2013/06/yahoo.html>(参照 2015-09-06).

[2] 杉本大輔，上原哲太郎，佐々木良一：パスワード再発行方式の調査及び最適な方式の提案，研究報告マルチメディア通信と分散，Vol.2015-DPS-162，No.14，pp1-7(2015).

[3] Akky AKIMOTO:日本の人気サイトランキング 500，入手先< http://akimoto.jp/japan/>(参照 2015-01-05).

[4] 情報処理推進機構:コンピュータウイルス・不正アクセス届け出状況および相談受付状況[2013 年年間]，情報処理推進機構，入手先< https://www.ipa.go.jp/security/txt/2014/2013outline.html>(参照 2014-10-16).

[5] 大谷和也，柿崎淑郎，佐々木良一：情報漏えいリスクを低減するアカウント手法，研究報告情報システムと社会環境，Vol.2015-IS-131，No.1，pp.1-6(2015).

[6] 大畑幸矢，松田隆宏，松浦幹太：証明可能安全なパスワード再発行プロトコルについて，コンピュータセキュリティシンポジウム 2014 論文集，Vol.2014，No.2，pp.1081-1088(2014)

[7] 平野亮，森井昌克：パスワード運用管理に関する考察および提案とその開発，ライフインテリジェンスとオフィス情報システム，Vol.111，No.286，pp.129-134(2014).

[8] Javed, A., Bletgen, D., Schewenk, H., et al.: Secure Fallback Authentication and the Trusted Friend Attack, Distributed Computing Systems Workshop, pp.22-28 (2014).

[9] Schechter, S., Bernheim Brush, A. J., Egelman, S.: It's no secret Measuring the security and reliability of authentication via 'secret' questions, IEEE Symposium on Security and Privacy, pp.375-390(2009).