Vol.2015-DPS-162 No.14
Vol.2015-CSEC-68 No.14
2015/3/5

パスワード再発行の方式の調査及び最適な方式の提案

杉本大輔[†1]　上原哲太郎[†2]　佐々木良一[†3]

近年，不正に入手した情報を利用したインターネット上のメールや各種サービスのアカウントの乗っ取りが多発しており，その方法の１つとしてパスワードの再発行を利用してアカウントを乗っ取る攻撃がある．パスワードの再発行とは，ユーザがパスワードを忘れた際に，新規パスワードの作成のため，データの管理先が行う手続きの事である．再発行手続きの際に要求される情報は様々であり，ID やメールアドレス，生年月日などが挙げられる．これらの情報を用いて本人確認を行った後，いろいろな方法でパスワードの再発行が行われる． 本研究では，パスワードの再発行手続きの調査を行い，手続きに必要な情報や手順を調査し，手続きのパターンを分類する．これらの調査の結果をもとにフォルトツリーによる分析と評価を行い，再発行手続きの最適な方式の提案や問題点の指摘を行う．調査の結果，パスワード再発行の方式は 6 種類の大別されることが分かった．また，フォルトツリー分析の結果，パスワードの再発行手続きで最適と考えられる方式は二重認証型で，危険だと考えられる方式はページ型であることが明らかになった．ページ型については，その脆弱性をついてメールアカウントが乗っ取られた場合，他人のメールアドレスが自由に使えるので，他の再発行の方式の各種サービスのアカウントの乗っ取りが容易になるという重大な問題点も明らかになった．

Study on password re-issuing methods and proposal of most preferable method

DAISUKE SUGIMOTO[†1]　TETSUTARO UEHARA[†2]
RYOICHI SASAKI[†3]

In recent years, there are many illegal hijacks of the account for the Internet services such as mail service. Among them, there is a hijack attack to the account in the case of the password reissue. Here, the password reissue represents that the creation of a new password when the user forgets the password. A variety of information such as ID, email address, and date of birth is required for the authentication of the user, when the password is reissued. This study surveys the procedures and required information for password reissue, and classifies these procedures of password reissue. Based on the survey, safety evaluation is done using fault tree analysis. As a result of the survey, we can know that the type of passwords reissue is divided into six types. Moreover, as a result of the fault tree analysis, it becomes clear that best method is that named password double authentication, and most dangerous method is that named page authentication. If the e-mail account was hijacked when the page authentication was used, it leads serious result because the various services with the account as well as e-mail address of another person can be used freely.

1. はじめに

昨今，不正に入手した情報を利用したインターネット上のメールや各種サービスのアカウントの乗っ取りが多発している．過去の事例では，2013年に男子中学生がパスワードの再発行を用いて，同級生のYahoo!アカウントを乗っ取り，メールを盗み見たという事件[1]がある．

このことから，パスワードの再発行を利用してアカウントを乗っ取られる可能性があると考えられる．

パスワードの再発行とは，ユーザがパスワードを忘れた際に，新規パスワードの作成のため，データの管理先が行う手続きの事である．再発行手続きの際に要求される情報は様々であり，IDやメールアドレス，生年月日などが挙げられる．これらの情報を用いて本人確認を行った後，パスワードの再発行が行われる．

本研究では，パスワードの再発行の方式の調査を行い，手続きのパターンを分類する．調査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う．

このような研究事例は多いと考え，比較のためCiNii ArticlesやGoogle Scholarを用いて文献調査を行ったが同じような研究は見当たらなかった．

†1 東京電機大学
Tokyo Denki University
†2 立命館大学
Ritsumeikan University
†3 東京電機大学
Tokyo Denki University

Vol.2015-DPS-162 No.14
Vol.2015-CSEC-68 No.14
2015/3/5

2. 調査方法と結果

2.1 調査方法

会員登録を必要とするWebサイトを対象とし，新規のアカウントを取得した後，パスワードの再発行を行う．これは，Webサイトが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ためである．

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[2]を参考に30サイト選択した．

2.3 再発行手続きで要求される情報について

再発行手続き時の本人確認の際に要求される情報について表 1 に示す．

表 1 再発行手続きで要求される情報

要求される情報	件数
メールアドレス	29
生年月日	14
秘密の質問	11
氏名	10
ID	10
電話番号	7
郵便番号	2
ニックネーム	1
クレジットカード番号	1

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．

調査対象の Web サイトと再発行手続きで要求される情報について図 1-1 から図 1-6 に示す．

	メールアドレス	電話番号	生年月日	氏名	ユーザID	秘密の質問
Amazon	✔					
楽天市場	✔			✔		
SUUMO	✔					✔
TOWN WORK	✔		✔	✔		
ニコニコ動画	✔	✔				

✔:必須項目
✔:任意選択項目

図 1-1 再発行手続きで要求される情報

	メールアドレス	電話番号	生年月日	氏名	ユーザID	秘密の質問	※1 その他
Google	✔						
Phantasy StarOnline 2	✔		✔	✔	✔	✔	
Twitter	✔	✔			✔		
Yahoo! JAPAN	✔	✔	※2 ✔		✔	※2 ✔	✔
Microsoft	✔						

✔:必須項目　　※1:ニックネーム・クレジットカード番号
✔:任意選択項目　　※2:セットで必要な項目

図 1-2 再発行手続きで要求される情報

	メールアドレス	電話番号	生年月日	氏名	ユーザID	秘密の質問
My JR-EAST	✔		✔	✔	✔	✔
J-WEST		✔	✔	✔	✔	
じゃらん	✔	✔	✔	✔		
るるぶトラベル	✔	✔		✔		
H.I.S.	✔	※ ✔	✔	※ ✔		※ ✔

✔:必須項目　　※秘密の質問 or 氏名＋電話番号
✔:任意選択項目

図 1-3 再発行手続きで要求される情報

	メールアドレス	電話番号	生年月日	氏名	ユーザID	秘密の質問
Ameba	✔					
Goo	✔		✔		✔	
livedoor	✔				✔	
価格.com	✔		✔			
pixiv	✔				✔	

✔:必須項目
✔:任意選択項目

図 1-4 再発行手続きで要求される情報

	メールアドレス	電話番号	生年月日	氏名	ユーザID	秘密の質問	郵便番号
Seesaa	✔						
はてな	✔						
@nifty	✔		✔		✔	✔	✔
cookpad	✔						
日本郵便	✔						

✔:必須項目
✔:任意選択項目

図 1-5 再発行手続きで要求される情報

Vol.2015-DPS-162 No.14
Vol.2015-CSEC-68 No.14
2015/3/5

図 1-6 再発行手続きで要求される情報

図 1-1 から図 1-6 は, 調査した 30 件の Web サイトが再発行手続きの際に要求する情報についてまとめたものである. 赤のチェックマークは，再発行手続きに必須の情報であることを表し，黒のチェックマークは，任意で選択する情報であることを表している．例として，図 1-3 のじゃらんでは，メールアドレスと氏名が必須の情報であり，これらの情報と電話番号または生年月日のどちらかを選択して入力する必要があるということである．

2.4 再発行手続きの方式について

再発行手続きのパターン名と件数を表 2 に示す.

表 2 再発行手続きのパターン

番号	パターン名	件数
1	URL型	18
2	認証キー型	4
3	パス発行型	1
4	URL＆認証キー型	2
5	二重認証型	5
6	ページ型	3
7	特殊型	1

以下に分類した再発行手続きの説明と採用しているWebサイトを示す.

1. 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（以降，この記述を省略），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．
(Amazon，楽天市場，Google，Twitter，価格.com 等)

2. 認証キー型
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．
(TOWNWORK，Yahoo!JAPAN，MicroSoft，じゃらん)

3. パス発行型
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．
(SUUMO)

4. URL＆認証キー型
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．
(J-WEST，日本郵便)

5. 二重認証型
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．
(My JR-EAST，J-WEST，pixiv，朝日新聞デジタル，BIGLOBE)

6. 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）．
(Yahoo!JAPAN，@nifty，excite)

7. 特殊型
メールで一部隠されたパスワードが送られてくる．
(H.I.S)

表 2 にある様に，調査対象の Web サイトで最も採用されていた手続きの方式は URL 型である．また，7 種の方式のうち，メールアドレスに依存しない方式は 6 のページ型のみである．このことから，再発行手続きの安全性の多くはメールアドレスおよびパスワードが知られていないことに依存していると言える．

Vol.2015-DPS-162 No.14
Vol.2015-CSEC-68 No.14
2015/3/5

3. フォルトツリー分析

3.1 フォルトツリーの作成について

各方式の安全性を評価するために再発行の方式ごとに，フォルトツリーを作成した．頂点を再発行手続きにより，第三者にアカウントを盗まれるとする．

図2に，URL型のWebサイトを基にしたフォルトツリーを示す．ここで，AND記号は，回路の子全ての条件が達成された場合，実行されることを意味する． OR記号は，配下のいずれかの項目が達成された場合，成立することを意味する．

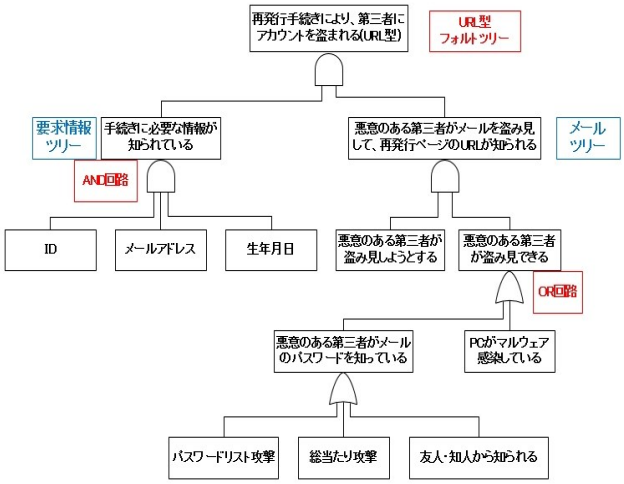

図2　URL型のフォルトツリー

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る．ここでは，必要な情報をID，メールアドレス，生年月日の3種としている．これは，要求情報ツリーを固定化することで，再発行手続きのパターンによる差異を明確にするためである．

また，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や認証キーなどの情報が，第三者に知られる場合の評価を行うものである．

悪意のある第三者が盗み見できるという項目では，悪意のある第三者がメールアカウントのパスワードを知っている，PCがマルウェアに感染してメールを勝手に転送される，ショルダーハックによりメールの内容を見られる，という3種類の項目を想定している．ここでは，Webサイトの管理者に対してのクラッキングやマンインザブラウザ攻撃，通信回路でのメールのタッピングなどは考慮していない．クラッキングとマンインザブラウザ攻撃は，悪意のある第三者がこれらを行うことができる状況にある場合，直接パスワードを盗める状態にあると考えられるため，パスワードの再発行を行う必要性がないからである．また，通信回路でのメールのタッピングは一般的には不可能であるとされているためである．

認証キー型からページ型のフォルトツリーを図3-1から図3-5に示す．

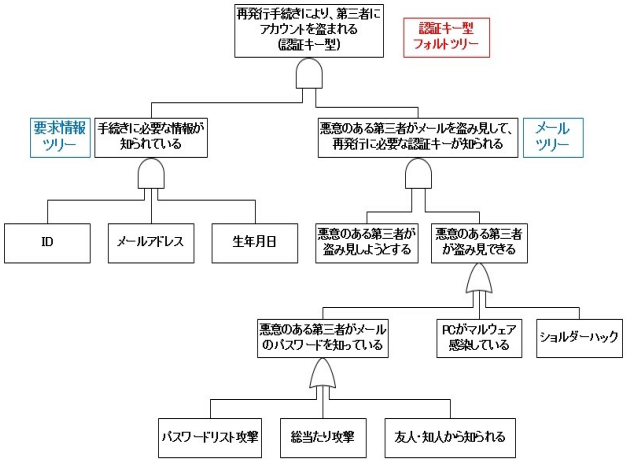

図3-1　認証キー型のフォルトツリー

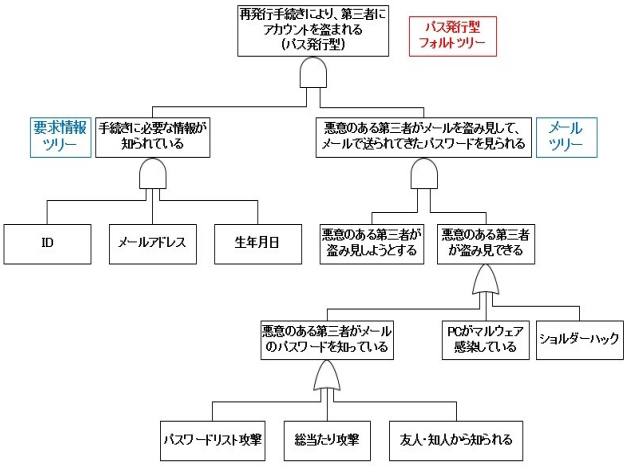

図3-2　パス発行型のフォルトツリー

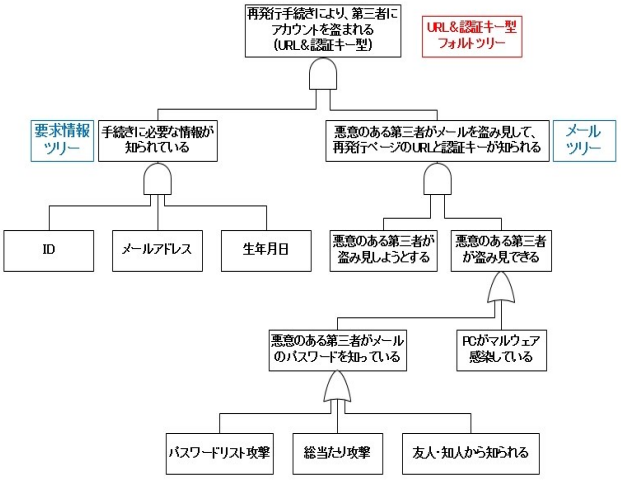

図3-3　URL&認証キー型のフォルトツリー

Vol.2015-DPS-162 No.14
Vol.2015-CSEC-68 No.14
2015/3/5

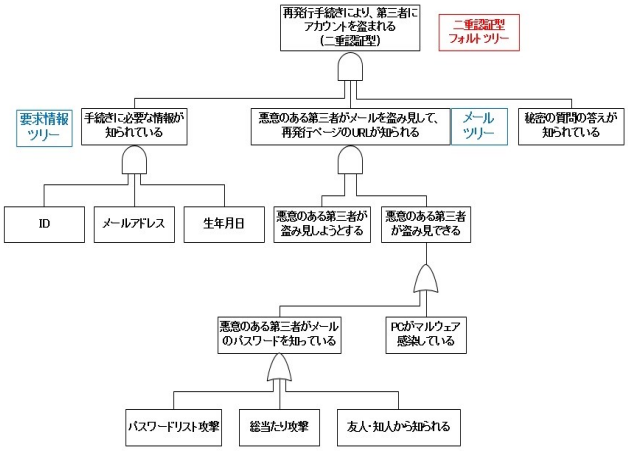

図3-4　二重認証型のフォルトツリー

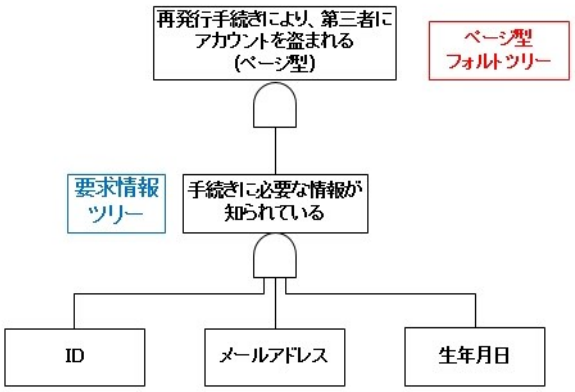

図3-5　ページ型のフォルトツリー

これらのフォルトツリーは，URL型のフォルトツリーと比較して，要求情報ツリーが同一であり，メールツリーの一部が異なっている．二重認証型のツリーには，秘密の質問が知られているというツリーを追加している．また，ページ型のツリーは，要求情報ツリーのみの構成とし，メールツリーを削除している．

3.2 フォルトツリー分析による評価方法

図2と図3-1から図3-6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評価を行う．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．評価値が0に近いほど安全な方式であり，1.0に近いほど危険な方式とする．

以下に，フォルトツリー分析で用いる評価値について記述する．

表 3 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	知ることができる，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 4 要求情報ツリーの評価値

手続きに必要な情報	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 5 メールツリーの評価値

項目	評価値
悪意のある第三者が盗み見しようとする	0.001
悪意のある第三者がメールのパスワードを知っている	0.01
PCがマルウェア感染している	0.06
ショルダーハック	0.01（他人の場合のみ0）

表3の評価値を基に研究室11人に対しアンケートを行い，表4の結果となった．これらの評価値は要求情報ツリーで用いるものである．また，表5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[3]を参考に設定している．悪意のある第三者が盗み見しようとするという項目の評価値と悪意のある第三者がメールのパスワードを知っているという項目とショルダーハックの評価値は独自に定めたものである．また，秘密の質問が知られているという項目の評価値は，内容によって入手難易度が異なるため一律で0.01としている．

具体的に評価値を入力した，悪意のある第三者が友人の場合のURL型のフォルトツリーを図4に示す．

Vol.2015-DPS-162 No.14
Vol.2015-CSEC-68 No.14
2015/3/5

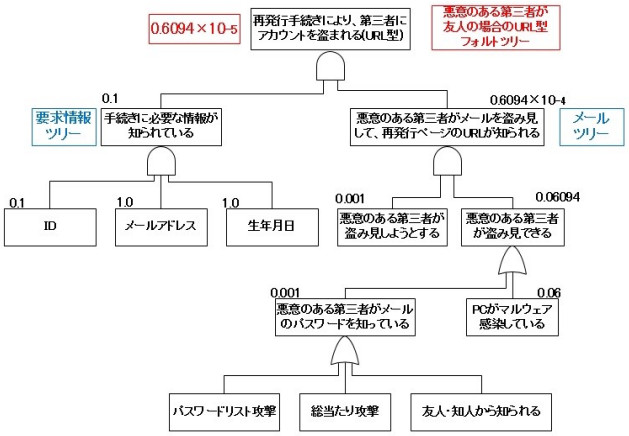

図4　評価値を入力したURL型のフォルトツリー

図4では，要求情報ツリーの評価値が0.1となり，メールツリーの評価値が0.6094×10^{-4}となっている．そして，最終的な評価値は0.6094×10^{-5}である．図4の様に評価値を入力し，他の方式についても計算して評価を行う．

最終的な評価値をxとした，セキュリティ強度のランク設定を表6に示す．

表 6 セキュリティ強度のランク

ランク	最終評価値
A	$0 \leqq x < 0.1\times10^{-7}$
B	$0.1\times10^{-7} \leqq x < 0.1\times10^{-5}$
C	$0.1\times10^{-5} \leqq x < 0.1\times10^{-3}$
D	$0.1\times10^{-3} \leqq x < 0.1\times10^{-1}$
E	$0.1\times10^{-1} \leqq x \leqq 1.0$

Aランクが安全な方式であり，Eランクに近づくほどセキュリティ強度が低い方式である．図4のフォルトツリーの最終評価値は，表6のCに該当するため，セキュリティ強度はCランクとなる．

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7と表8に示す．

表 7 フォルトツリー分析による最終評価値

再発行手続きの方式	最終評価値		
	研究室（会社）の同僚	友人	他人
URL型	0.609×10^{-5}	0.609×10^{-5}	0.609×10^{-10}
認証キー型	0.703×10^{-5}	0.703×10^{-5}	0.609×10^{-10}
パス発行型	0.703×10^{-5}	0.703×10^{-5}	0.609×10^{-10}
URL＆認証キー型	0.609×10^{-5}	0.609×10^{-5}	0.609×10^{-10}
二重認証型	0.609×10^{-7}	0.609×10^{-7}	0.609×10^{-12}
ページ型	0.1	0.1	0.1×10^{-5}

表 8 フォルトツリー分析による評価ランク

再発行手続きの方式	セキュリティ強度		
	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

表7と表8より，パスワード再発行の方式で最適だと考えられるものは二重認証型である．また，最も危険な方式と考えられるものはページ型である．

4. 考察

二重認証型を採用しているWebサイトは，pixiv，朝日新聞デジタル，BIGLOBEなどがあった．この方式のセキュリティ強度が高いのは，他の方式より本人確認の回数が多いからだと考えられる．

ページ型を採用しているWebサイトは，Yahoo!JAPAN，@nifty，exciteで，これらのWebサイトにはメールサービスがある．これらのアカウントが乗っ取られた場合，メールを利用する再発行の方式のセキュリティ強度が低くなる可能性があり危険である．例えば，Yahoo!JAPANのアカウントを乗っ取り，メールサービスを利用して，Amazonのアカウントを乗っ取ることが可能となる．

メールサービスがあるアカウントが乗っ取られた場合のフォルトツリーを図5に示す．

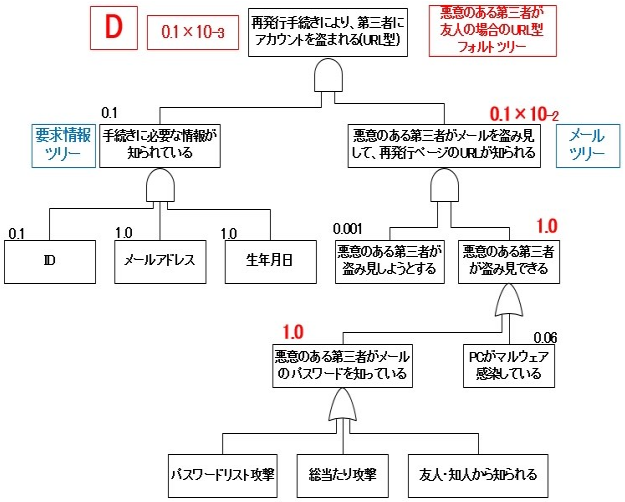

図5　メールアカウントが乗っ取られた場合のURL型のフォルトツリー

ページ型を利用してアカウントを乗っ取った場合，悪意のある第三者はメールのパスワードを知っていることにな

るので，評価値が1.0となりメールツリーの評価値が2桁大きくなる．その為，最終評価値も1.0に近くなり危険度が増加し，セキュリティ強度が1ランク下がるという結果となった．

5. 終わりに

本研究では，パスワードの再発行の方式について調査を行い，再発行手続きの方式を分類した．また，分類した再発行の方式についてフォルトツリーを用いて分析し，評価を行った．

調査の結果，パスワード再発行の方式は6種類に大別されることが分かった．

また，フォルトツリー分析の結果，パスワードの再発行手続きで最適と考えられる方式は二重認証型で，危険だと考えられる方式はページ型となった．ページ型については，その脆弱性をついてメールアカウントが乗っ取られた場合，他人のメールアドレスが自由に使えるので，他の再発行の方式の各種サービスのアカウントの乗っ取りが容易になるという重大な問題点も明らかになった．

今後の展望としては，調査対象の追加やページ型のセキュリティ強度実験を考えている．

調査対象の追加は，スマートフォンアプリケーションや，悪い例としてセキュリティ強度が低いと思われるWebサイトの調査を検討している．

また，ページ型のセキュリティ強度実験は，ページ型を用いて実験用メールアカウントを乗っ取ることができるか，乗っ取ったアカウントを利用して，他の方式のアカウントを奪うことが可能であるか調査を行う．この調査から，ページ型のメリットとデメリットを把握し，今後も必要な方式であるのか，廃止すべきなのか，もしくは改善点を検討する．

謝辞 本研究を進めるにあたり，アンケートや研究の相談などでご協力を頂いた情報セキュリティ研究室の皆様に深く感謝致します．

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
http://blog.tokumaru.org/2013/06/yahoo.html
[2] Akky AKIMOTO 日本の人気サイトランキング500
http://akimoto.jp/japan/
[3] IPA コンピュータウイルス 不正アクセスの届出状況 2013
https://www.ipa.go.jp/files/000036445.pdf