明治大学大学院　先端数理科学研究科

2018 年度

修士学位請求論文

二要素認証を悪用したパスワードリセット手法 PRMitM の影響評価

学位請求者　先端メディアサイエンス専攻

笹　航太

あらまし

2017 年に Gelernter らによって，2 要素認証を用いてユーザのアカウントを乗っ取ることができる PRMitM 攻撃が提案されている．PRMitM 攻撃では，SMS(ショートメッセージサービス) を用いたパスワードリセット手法を利用することで，ユーザにパスワードのリセットだと気づかせぬまま，悪意のある中間者サイトにリセットコードを入力させる．この研究の発表後，多くの脆弱なサイトではパスワードリセット方式を改良したと考えられるが，国内のサイトの対応状況やユーザへの配慮が十分であるか不確かだった．そこで，ユーザが被害を受ける要因を明らかにするため，184 名の被験者を用いた実験を行い，SMS メッセージを「警告の有無」,「リセットコードが数字のみか英数字」,「1 回の入力か 2 回の入力」と分けることで，攻撃に対する被害率や被害を受ける人間の行動を調査し, 報告する．

目 次

第1章　序論

1.1　研究の背景

パスワード認証はアカウントを守るために最も用いられてきた認証手法である．ウェブサービスを利用するユーザは，パスワードを用いることで不正なアクセスやアカウントの盗難を防いできた．しかし，パスワード認証が持つ多くの脆弱性が明らかになってくるにつれて，様々な攻撃が行われてきた．脆弱性の一つに，ユーザが単純なパスワードを選択してしまうことがある．ブルートフォース攻撃はパスワードを総当たりする攻撃である．仮にパスワードが数字のみの 4 桁で構成されるものならば，0000〜9999 まですべて試す攻撃である．パスワードが短く文字の種類が少ないほど簡単に総当たりできてしまうので [1]，長く複雑なパスワードを設定するように推奨されているが，多くのユーザは必要最低限の簡単なパスワードを使用してしまうことが知られている [2]．パスワードを使いまわしてしまうことも脆弱性の一つである．パスワードリスト攻撃は攻撃者が入手した ID・パスワードのリストを用いて，不正アクセスを試みる攻撃である．パスワードは利用するサービスごとに異なるものを使うことが推奨されている．攻撃者に狙われた脆弱なサイトがパスワードを漏洩してしまった場合，本来セキュアなサイトに対しても，同じパスワードを設定しているために，不正アクセスされてしまう可能性があるためだ．しかし，Das らの報告によると，43〜51%のユーザは複数のウェブサービスで同じパスワードを使いまわしていることが知られている [3]．また，Ur らは，ほとんどのユーザはパスワードの再利用に対して肯定的であると報告している [4]．もう一つの脆弱性として，パスワードを忘れてしまうことがあげられる．パスワードを忘れてしまうと，正規の利用者が自分のアカウントを使えなくなってしまうが，Yans の報告によると，65%のユーザにパスワードを忘れる傾向があるとされる [5]．そこで今日多くのサイトでは，パスワードリセットの手法が用意されており，とりわけ，高いセキュリティを持つと考えられている二要素認証が用いられている．

二要素認証はパスワード認証に加えて異なる要素の認証を用いることで，2 重の認証を行いセキュリティを高める認証手法である．二要素認証を用いることでパスワードの使いまわしや，単純なパスワードを選んでしまうことで生じる危険を防ぐことが出来る．また，パスワードを忘れてしまった場合でも，あらかじめパスワード以外の認証法を設定しておくことでパスワードをリセットすることが可能である．なかでも，あらかじめ登録してあるスマートフォンの電話番号情報を用いた二要素認証によるパスワードリセットが普及している．この方式では，SMS(Short Message Service) を用いてリセットコードをユーザのスマートフォンに通知する．

1.2 現状の問題

二要素認証によるパスワードリセットは便利かつ安全であると考えられていた．しかし，Gelernter らは SMS を用いたパスワードリセットを悪用してアカウントを乗っ取る手法 PRMitM(Password Reset Man in the Middle) 攻撃を提案し [6], SMS を用いたパスワードリセットが安全ではないことを示した．本攻撃は中間者攻撃の一種である．攻撃対象となるユーザには，ウェブサイトに新規登録をしていると思わせ，その間にアカウントを盗みたいサービスにパスワードリセット要求を送る．確認のために送られたターゲットサイトからの SMS のコードを中間者に入力するとアカウントを乗っ取られてしまう．Gelernter らの発表後，多くの脆弱なサイトはこの攻撃を受けないようにパスワードリセットの手続きを改良したとみられるが，改良後もユーザに不親切なメッセージでは依然として本攻撃に脆弱な恐れが残る．また，SMS の内容を読まずにリセットコードを入力してしまう不注意なユーザの配慮が足りないことも懸念されるが，SMS を読まない原因は明らかになっていない．

1.3 従来手法と課題

Gelernter らはユーザスタディを行い，SMS にパスワードリセットであることの警告を含めることで，PRMitM 攻撃の被害を抑制できることを明らかにした．また，SMS でリセットコードではなく URL を送り，遷移先でパスワードリセットをさせる手法を用いることで，PRMitM 攻撃を完全に防ぐことが出来ると示した．

しかし，SMS では送信者がわからないこと，URL のリンク先が正しいかどうか判断できないことなどから，フィッシング攻撃を誘発する恐れがあるため，この手法は脆弱である可能性が残る．よって SMS にパスワードリセットであることの警告を含めることが，現在行える対策であるが，PRMitM 攻撃は人間の不注意や誤解を利用した攻撃であるにもかかわらず，Gelernter らはシステム側の対策を示すのみで，どのようなユーザが攻撃を受けやすいか，攻撃を防ぐためにユーザはどんなことに気を付ければよいか，セキュリティの知識は関係があるのかなどの人間側の要素が明らかになっていない．

1.4 研究の目的

本研究では，リセット被害を受けるユーザの特徴，SMS の特徴を明らかにすることを目的として，PRMitM 攻撃を模した実験を行う．加えて，パスワードリセットを伝える SMS メッセージに脆弱性が含まれるサイトが残っているかどうかを明らかにすることを目的として，国内 200 社の主要なサイトを対象に調査を行う．以上により，PRMitM 攻撃のもたらす潜在的な被害の影響を報告する．

1.5 研究の新規性

本研究の新規性は以下の 2 つである．

PRMitM 攻撃に対して脆弱なパスワードリセットを行っているサービスを明らかにしたこと

国内 200 社の主要なサイトで,「アカウントを作成できるか」,「パスワードリセットに SMS を使用できるか」,「SMS にパスワードリセットであることの警告が含まれているか」を調査し，４つのサービスで PRMitM 攻撃に対して脆弱な SMS が使用されていることを明らかにした.

PRMitM 攻撃の脅威を高める人間の要因を明らかにしたこと

従来の研究では，PRMitM 攻撃に対してユーザの人間的要因がどのように影響するのかどうか不明であった．本研究ではユーザスタディを行い,「複雑なパスワードを設定する」と「リンクが送られてきたとき，どこにつながるか確認する」が PRMitM 攻撃の被害率を下げること,「パスワードを頻繁に変更する」が PRMitM 攻撃の被害率を上げることを明らかにした.

1.6　位置づけ

本研究の従来研究に対する位置づけを述べる.

PRMitM 攻撃に関する研究は Gelernter らによる研究がある．[6]

Gelernter らは大学の学生に対するユーザスタディであり，被験者数は 536 人と本研究よりも多い．しかし着目する要因として，本研究では SMS の要因と人間要因がある．本研究は被験者をいくつかのグループに分けて異なる要因を与えるため，要因数を増やすと，それだけ必要な被験者を増やす必要がある．従来研究では警告の有無と URL を SMS 要因としていた．一方で，本研究では新たな着眼点として，リセットコードの種類（数字英数字）と送られてくる SMS の数（長文）の要因の影響を考える．また，従来手法では考慮されていなかった人間の要素が PRMitM 攻撃に与える影響を明らかにする.

1.7　論文構成

本論文は，6 章で構成される．1 章では研究の背景と目的を述べる．2 章では，先行研究である PRMitM(Password Reset Man in the Middle) 攻撃の説明と PRMitM 攻撃に対する対策を説明する．3 章では先行研究における PRMitM 攻撃の対策手法の問題点を人間要素とシステム要素から提起する．4 章では日本の主要なウェブサイトに対してパスワードリセット手法の安全性を調査する．5 章では PRMitM 攻撃を模した実験を行いユーザが被害を受ける要因を明らかにする．6 章では，本論文をまとめている.

表 1.1: 従来手法との比較

	本研究	従来研究 Gelernter ら [6]
被験者	クラウドソーシングサービスのワーカー	学生
被験者数	△ 184	○ 536
SMS 要因	○ 警告 数字英数字 長文	△ 警告 URL
人間要因	○ 被験者属性 セキュリティ知識	×

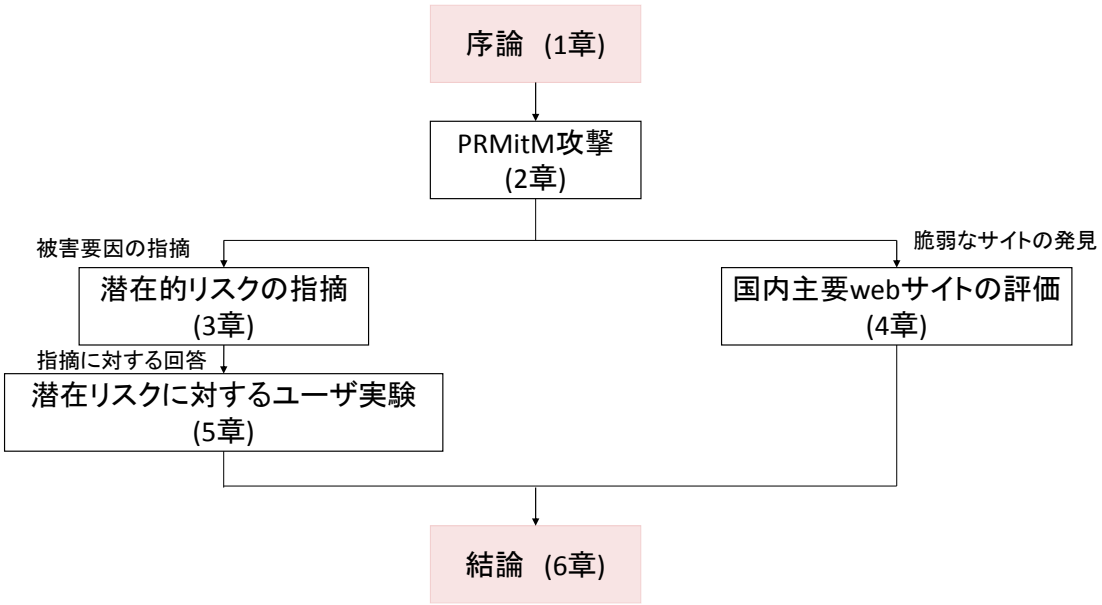

図 1.1: 本論文の構成と各章の関係

第2章　PRMitM攻撃

2.1　二要素認証

二要素認証は,「知っていること」「持っているもの」「生体情報」のうち 2 つの要素を組み合わせた認証方式である．従来の認証は「知っていること」であるパスワード認証のみで行われていた．しかし，単一のパスワード認証には多くの脆弱性が存在していたので，様々な攻撃が行われてきた．

これらの攻撃に対して，二要素認証を利用することで，パスワードが漏洩しても不正アクセスを防ぐことができる．例として，ネットバンキングでの場合を説明する．自分の口座にアクセスする場合，バンキングのアカウントとパスワードに加えワンタイムパスワードが必要である．ここでは，アカウントとパスワードが「本人が知っていること」である．これに,「本人が持っているもの」であるパスワード生成器で生成したワンタイムパスワードを加えて，2 つの要素を利用して認証する．仮にパスワードが漏洩したとしても，パスワード生成器を持っていない攻撃者はバンキングのアカウントに不正アクセスすることができないため，二要素認証を利用することでセキュアな認証を行うことができると考えられている．

その他の認証要素には,「持っているもの」として，スマートフォンや IC カード,「生体情報」として，指紋や顔認証等が用いられる．

2.2　SMS を用いた二要素認証に対する認識

Gelernter らはユニークな 237 人の被験者に対して，SMS を利用することについてのアンケート調査を行った．138 名の学生に「無料のウェブコンテンツを利用するときに，ユーザ登録と携帯電話番号を登録してもよいか」と質問した．結果を表 2.1 に示す．また，99 名の学生に「ファイルをダウンロードするのにケータイ番号が必要なら入力するか」と質問した．結果を表 2.2 に示す.

この結果から，ユーザが電話番号をウェブサイトに入力することに対して大きな抵抗はないことが示された．

表 2.1: ユーザ登録と携帯電話番号 [6]

	人数
両方ともよい	84
ユーザ登録だけよい	38
携帯番号だけよい	10
両方ともよくない	6

表 2.2: 携帯電話番号入力 [6]

	人数
即座に入力する	39
最初は友人やオンライン SMS から手に入れようとする	14
すごく欲しいファイルなら入力	18
入力しない	28

2.3 PRMitM 攻撃

2.3.1 先行研究

大文字小文字を含めた長い英数字をパスワードに設定し，定期的にパスワードを変更することがセキュリティを高めると考えられていた．しかし，多くのユーザは自分が設定したパスワードを忘れてしまう傾向にあるため，パスワードを再設定するための手段が必要となる [5][7]．今日，ほとんどのパスワードベースのログインシステムでは，忘れてしまったパスワードをリセットして新しいパスワードを設定する方法が用意されている．

パスワードリセット手法の一つに，メールアドレスを用いた二要素認証が用いられる．パスワード設定時に登録したメールアドレスに対して，パスワードをリセットするためのページに遷移する URL を送ることで，設定者本人のみが安全にアカウントを復旧することができる．また別の手法として，昨今モバイル端末でのインターネット利用が増加しているため [8]，SMS を用いたパスワードリセットも用いられている．

SMS を用いたパスワードリセット手法では，パスワード設定時に登録した電話番号に対して，パスワードをリセットするためのコードが送られてくる．コードが送られるスマートフォンを持っているのは設定者なので，設定者のみが安全にパスワードをリセットすることができる．

これらの手法はセキュアであると考えられていた．しかし，2017 年に Gelernter らは SMS を用いたパスワードリセット手法を悪用したアカウント乗っ取り手法として，PRMitM 攻撃を提案した [6]．PRMitM 攻撃は，アカウント登録とパスワードリセット手法が類似していることを利用した攻撃である．一連の流れを図 2.1 に示す．ユーザ A はターゲットサイト C にアカウント C_A を所有している．PRMitM 攻撃はアカウント C_A を狙った攻撃である．攻撃者は，アカウント登録をしなくては利用することができないサイト B を用意する．サイト B は PRMitM 攻撃を行うための中間者サイトであるが，ユーザには一般的なウェブサイトとの区別はつかない．中間者サイト B のアカウント登録には，SMS を用いた二要素認証を利用していると説明する．ユーザ A は中間者サイト B に登録するため，アカウント名やパスワード等に加えて電話番号を入力させられる．攻撃者はこの電話番号を利用して，ユーザ A になりすまし，ターゲットサイト C に対して C_A のパスワードリセットを要求する．ユーザ A のスマートフォンに対して SMS で C_A のパスワードリセットコードが送られてくる．ユーザ A は中間者サイト B に対して新規登録を行っているものだと思い込んでいるので，攻撃に気づかぬままリセットコードを入力し，C_A のアカウントを乗っ取られてしまう．

Gelernter らは PRMitM 攻撃の脅威を高めてしまうパスワードリセット手法の脆弱性として，次の

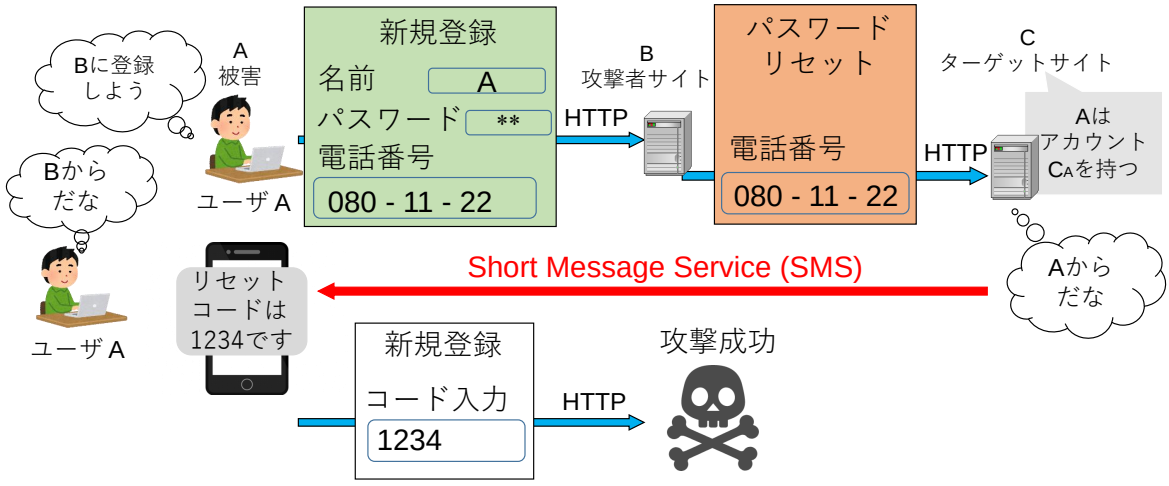

図 2.1: PRMitM 攻撃の流れ

3 つをあげた.

(1) SMS の本文にサービス名がない

(2) SMS の本文にパスワードリセットである警告がない

(3) 秘密の質問によるパスワードリセット

過去に送られていた SMS の例を表 2.3 に示す. (1) の様に SMS の本文にサービス名がないと，ユーザは送られてきたコードの送信元が判断できないため，中間者サイト B から送られたものだと勘違いして，リセットコードを入力してしまう．(2) の様に SMS の本文にパスワードリセットである警告がないと，送られてきたコードが何のために送られてきたのか判断できない脆弱性が生まれる．攻撃者はサイト B に powered by Linkedin と示しておけば，被害ユーザは Linkedin を利用した認証なのだと勘違いして，リセットコードを入力してしまう．(3) の様に秘密の質問でパスワードリセットができてしまうと，電話番号を入力させる必要すらなく，攻撃サイト B の登録時に同じ秘密の質問を設定させるだけでパスワードリセットができる．秘密の質問は答えの推測が容易なため，現在では推奨されていない．Google の調査によると，米国では「好きな食べ物」の質問に対する答えを「ピザ」とすると，1 回の推測だけでも 19.7 %の確率で言い当てることができてしまうことが明らかになっている．[9]

表 2.3: リセットコードを伝える脆弱な SMS の例 [6]

Site	SMS text
(1)Yandex	Your confirmation code is XXXXXX. Please enter it in the text field.
(2) Linkedin	Your LinkedIn verification code is XXXXXX

2.3.2 PRMitM 攻撃の防止法

Gelernter らは PRMitM 攻撃の対策として，パスワードリセット SMS の本文に，送信企業名とパスワードリセットコードであることの警告を含めることを推奨している．これにより，送られてきた SMS に書いてある企業名が入力しようとしているサイトと異なること，登録をしているはずなのにパスワードをリセットしようとしていることに気づき，攻撃を防ぐ可能性が高まる．また，Gelernter らはパスワードリセットコードではなくパスワードをリセットするための URL を送信することを推奨している[1] URL を送る SMS に対して PRMitM 攻撃をすることは極めて困難である．一般的には送られてきた URL はクリックするものだが，PRMitM 攻撃を行うには，ユーザが URL の文字列を中間者サイトに入力しなければならない．URL を入力することは極めて異質であるため，この行動を怪しんだユーザは攻撃を回避することが期待出来る．

2.3.3 問題点

Gelernter らの対策の問題点の 1 つに，ユーザが SMS の文章をしっかりと読まないことが挙げられる．Gelernter らは，パスワードリセットの警告で，PRMitM 攻撃を防ぐことができるかどうかを調査するために，SMS を使用する Facebook ユーザに対する PRMitM 実験を行った．記憶力を試す実験と称して 88 人の被験者を集め，電話番号を入力して送られて来た SMS のコード入力が必須のログインをさせた．42 人の被験者には本物の Facebook のパスワードリセットメッセージ「XXXXXX is your Facebook Password reset code or reset your password here:https://fb.com/l/YYYYYYYYY」を，他の 46 人には Facebook になりすましたサーバからより詳細なメッセージ「*WARNING* Someone requested to reset your Facebook password. DO NOT SHARE THIS CODE with anyone or type it outside Facebook. The password reset code is XXXXXX.」を送信した．被験者はウェブページの入力で嫌な事があれば，すぐに終了することができる．実験終了後，全被験者に対して以下の 3 つの質問を段階的に行った．

1. 被験者の半分はとある操作をされています。あなたは操作されてましたか？
2. とある操作とは，アカウントを乗っ取る操作です。あなたは操作されてましたか？
3. 乗っ取ろうとしているのは facebook アカウントです。あなたは操作されてましたか？

被験者は Yes/No で回答を行い，No と答えた場合，次の質問もされる．実際には全被験者が攻撃を受けているため，Yes と答えることが正しいが，攻撃に気づいていない被験者は No と答えてしまう．

[1] Defense, B. Secure Password Reset Using SMS にて述べている，a link-Via-SMS(LVS)password reset procedure.

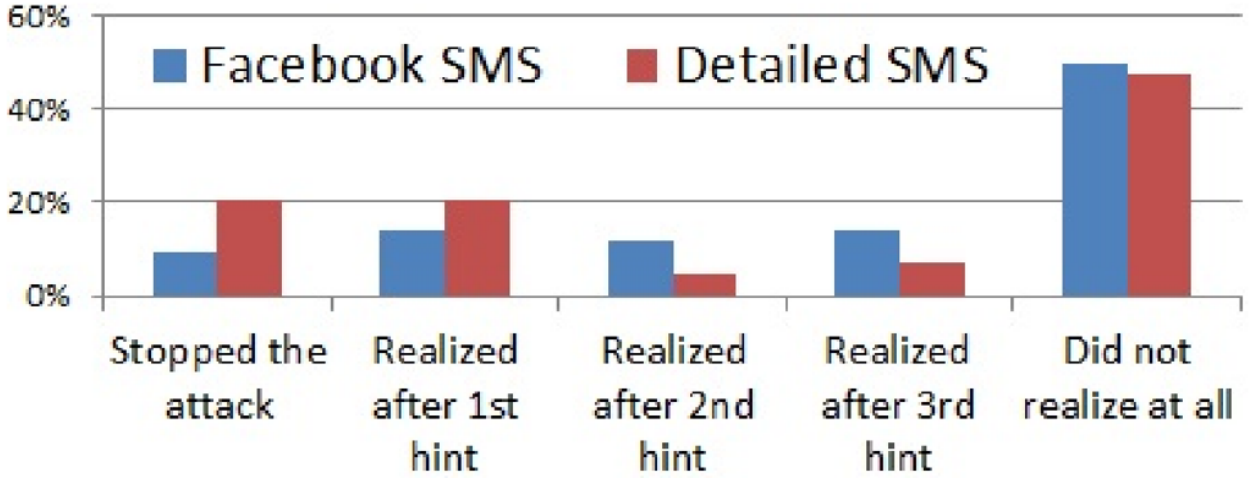

図 2.2: 先行研究の結果 [6]

実験の結果を図 2.2 に示す．本物の Facebook SMS グループは 90.5%に対して攻撃が成功した．一方で詳細な SMS を送られたグループは 79.5%に対して攻撃が成功した．この結果から，警告メッセージは被害者を減らすことはできるが，多くのユーザは変わらず SMS のテキストを読んでいなかったことが明らかになった．

第3章　潜在的リスクの指摘

3.1　人間要素

どれだけセキュアなシステムを使っていても，人間が使っている以上，ミスや誤解などを完全になくすことはできない．悪意のある攻撃者はそういった人間の脆弱性を利用する．人間の脆弱性を狙う攻撃としてフィッシング詐欺が挙げられる．フィッシング詐欺とは，実際に存在する銀行や販売店などを装った電子メールを送り，本物だと信じてしまったユーザから個人情報や金銭をだまし取る行為である．送られてきたフィッシングメールに対して，何らかの違和感・不信感を感じ，被害を避けることができるユーザがいる一方で，何も気付かない，あるいは違和感に気付いても無視してしまうような騙されやすいユーザも存在する．フィッシングメールの被害にあってしまうユーザの性格特性には,「神経症的傾向」や「不安傾向」等が知られている [10].

人間の認知的な誤解を利用する PRMitM 攻撃も同様に，ユーザの特徴によってリスクが変化すると考えられる．攻撃を受けやすいユーザの特徴として，セキュリティ知識の不足からパスワードリセットコードだと気付いてもよくわからないまま入力してしまうことや，SMS の文章をよく読まない注意深さの欠如等が考えられる．Gelernter らの研究では，これらの人間要素の影響やユーザの属性および警告の有無以外の SMS のメッセージの種類による攻撃成功率の検討が行われていなかった．よって本研究では，ユーザのセキュリティに対する知識や，SMS の種類を考慮した PRMitM 攻撃の潜在的なリスクを明らかにする．

3.2　新たな攻撃の可能性

本節では，SMS を用いた二要素認証に潜む潜在的な脆弱性である人間の脆弱性を利用し，新たな PRMitM 攻撃の提案を行う．

3.2.1　長文攻撃

警告メッセージや企業名の表示などは，SMS を用いた二要素認証を初めて利用するユーザや手順を忘れてしまったユーザに対しては効果的だろう．しかし，認証の手順は毎回同じなため，ユーザが慣れてしまい，効果が薄れてしまうことが考えらえる．セキュリティ広告は危険なサイトやセキュアでないサイトに接続する際に表示することで，ユーザに安全な行動を促すが．Krol らの研究では従来の警告文よりも具体的な危険性を示したセキュリティ警告に対して，80%のユーザが警告を無視し，警告を無視したユーザの内 45%は警告に対する倦怠感があったとして，警告文を読んでいなかったこ

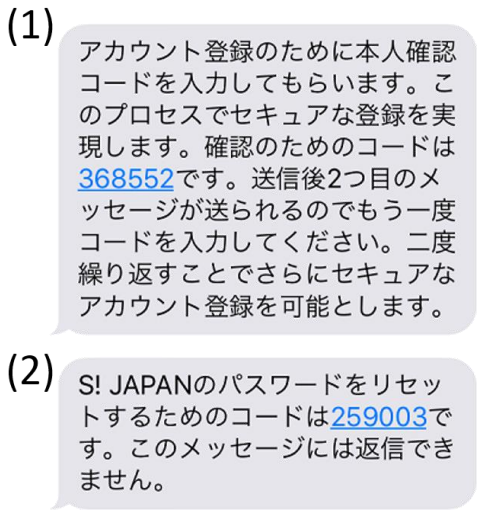

図 3.1: 長文攻撃の流れ

とが明らかになった [11]．こうしたユーザの同じものに対して慣れてしまう性質を利用した新たな攻撃「長文攻撃」を提案する．

長文攻撃はユーザにコードを複数回繰り返し入力させる手法である．1 度目の SMS は攻撃者が用意したフェイクの SMS を送信し，コードを入力させる．2 度目以降は従来の攻撃と同様にターゲットサイト C からのパスワードリセットコードが送信される．ユーザ A は 1 回目の入力と同じ行動の繰り返しのために，2 回目の入力では，警告や企業名の有無にかかわらず，文章を読まずにコードだけを探して入力してしまい，アカウント A を乗っ取られてしまう．図 3.1 の SMS(1), (2) を例に挙げる．ユーザ A は中間者サイト B に新規登録するために必要であると指示されているので，B から送られてきた (1) の SMS に記されたコード「368552」を入力する．1 通目の SMS はメッセージが長く読むのが大変なため，メッセージを読まずにコードだけを探すユーザが多くなるだろう．また，文章を読んだユーザもコードの入力手順に慣れてしまう。1 つ目のコードが入力されたら，次に攻撃者はユーザ A のふりをして，ターゲットサイト C である「S! JAPAN」に対してパスワードリセットを求める．S! JAPAN はユーザ A の電話番号宛にパスワードリセットコードが記された SMS を送信する．ここで，ユーザ A は (1) でコードを見つけて入力するという作業に慣れてしまい，コードを探せばメッセージを読む必要はないと考え，(2) の SMS に C(“S! Japan”) と明記されていることに気付かずにコード「259003」を B に入力するだろう．なお，(1) と (2) で送信元が異なるので，画面上に (1) と (2) が同時に表示されることはない．

3.2.2 数字の認証コード

iPhone と一部の Android 端末には，連続した数字を電話番号だと認識してリンクを張る機能がデフォルトで設定されている．PRMitM 攻撃において，この機能は大きな脆弱性を生むと考えられる．

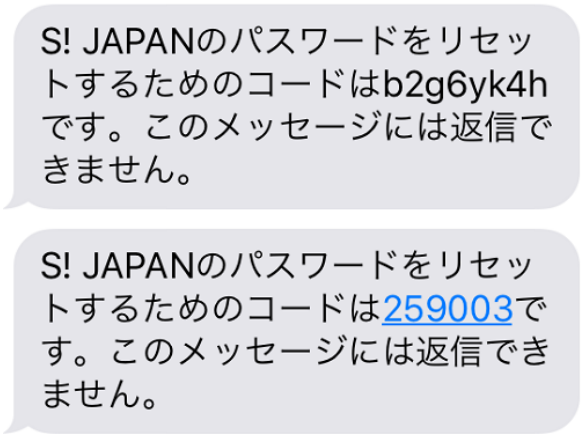

図 3.2: 数字のみと英数字の SMS

図 3.2 の数字のみのリセットコードと英数字のリセットコードの違いを確認しよう．リセットコードが英数字であると他の文章と同一になるため，リセットコードだけを探してもある程度文章が目に入ってくるので，違和感に気付きやすくなるだろう．一方で，リセットコードが数字であるメッセージでは，「259003」の色が青くなり，下線を引かれて強調されている．これにより，コードの入力を単純で億劫な作業であると考えるユーザは，本文を読まなくても簡単にコードを発見できてしまうため，警告メッセージや企業名が書かれていても気づくことができないため，PRMitM 攻撃の被害を受ける可能性が高くなってしまう．これらの特性から，リセットコードが数字であることが脆弱性であると考えられる．

3.3 ID 連携

OpenID[12] 等の ID 連携を用いることで，既に登録してあるアカウントを使用し，異なるサービスの新たなアカウントを取得することが出来る．例として，ニコニコ動画に使われているバーナーを図 3.3 に示す．仮に Twitter のアカウントは持っているが，ニコニコ動画のアカウントを持っていないユーザがいるとする．このユーザは Twitter の ID とパスワードだけで，面倒設定を省きニコニコ動画のアカウントを手に入れることが出来る．現在，OpenID 連携において二要素認証は用いられていないが，セキュリティ強化の名目で導入される可能性は否定できない．

しかし，SMS を用いた OpenID による登録は，PRMitM に対して脆弱である．ID 連携における Replying party が中間者 B となり，ターゲットサイト C を ID Provider とした ID 連携のふりをして，ユーザ A をだます PRMitM の変形が考えられる．この時，ユーザは気づくことが出来ないままリセットコードを入力して，ターゲットサイト C のアカウントを乗っ取られてしまう．

図 3.3: OpenID を用いたログインの例 (ニコニコ動画ログイン)

3.4 Link-via-SMS(LVS)

Gelernter らの提案する URL リンクを埋め込んだ SMS によるリセット手法には次の問題がある

1. 短縮 URL(http://bit.ly/xxx) ではリンク先が正しいかどうか分からない.
2. SMS の送信元が意図したサイト先であるかの確認ができない.
3. SMS で URL を伝達することが普及すると新たな phishing の標的になる.

1 のように短縮 URL を用いられると，危険な URL に気づくことができなくなってしまう．ブラックリストに載っているような危険な URL を再利用することが可能になってしまうだろう．2 で指摘したように URL ではクリックして遷移してみなければ自分の意図しているサイトかどうかわからないため危険である．遷移した瞬間にコンピュータウイルスなどをダウンロードさせるようなウェブサイトにつながってしまう可能性がある．3 のように SMS で URL を用いることが一般化すると，偽物のリンクを送る攻撃が増えるであろう．実際に，佐川急便で荷物の再配達の登録を装ったフィッシングメールが送られる事件が起こった [13]．以上の理由から，リセットコードの代わりに URL リンクを用いたとしても安全を保障できるわけではないと我々は考える．

3.5 SeBIS

ユーザのセキュリティ知識を調査するために本研究ではセキュリティ意識の指標として SeBIS（Security Behavior Intentions Scale ）を用いる．

SeBIS は Serge Egelman らが提案した，セキュリティ志向度の指標である [14]．全 18 問のセキュリティ意識に関する質問に対して 5 段階で答える．18 問のうち 6 問目と 17 問目は，回答者が質問に

表 3.1: 正しく回答をしているかを判断する問

Q6	質問にきちんと答えていることを確認したいので，いつもするを選んでください
答え	全くしない　ほぼしない　たまにする　しばしばする　いつもする　回答しない
Q17	この質問の回答として，いつもしているを選択してください
答え	全くしていない　ほぼしていない　たまにしている　しばしばしている　いつもしている　回答しない

対して正しく回答をしているかを判断するための問いである．実際の質問を表 3.1 に示す．回答の合計スコアが高いほど回答者はセキュリティ意識が高いと判断する．

本研究では，原文を和訳し，否定的な質問項目をすべて肯定的に書き換えて用いた．問 6，問 17 以外の質問は表 5.7 に示す．

第4章　国内主要webサイトの調査

4.1　目的

Gelernter らの発表後，多くの脆弱なウェブサイトは PRMitM 攻撃に対する脆弱性を改良したとみられるが，ユーザに不親切なメッセージでは依然として本攻撃に脆弱な恐れがある．よって国内主要 200 サイトを調査して PRMitM 攻撃を受けてしまう脆弱性が残っているウェブサイトを明らかにする．

4.2　方法

2017 年 2017 年 8 月 18 日〜12 月 13 日の間に Alexa Japan[15] の top200 のウェブサイトに対して，次の 3 つの項目を調査する．

1. アカウント登録が存在するか
2. SMS を用いたパスワードリセット手法が用意されているか
3. SMS 本文にパスワードリセットであることの警告が記載してあるか

本調査では，SMS 本文にパスワードリセットであることの警告が記載されていないものを脆弱であると設定する．

4.3　結果

調査結果を表 4.1 に示す．[6] で指摘された，サービス名の表記がないサイトは 0 であった．しかし，SMS を用いたパスワードリセットを行っているウェブサイトで，SMS 本文に警告が記載されていなかったものは 15 件存在した (同じアカウントを共用しているサイトを除くと，ユニークなアカウントは 4 件だった)．SMS 本文に警告が記載されていないサービス名と SMS の内容を表 4.2 に示す．

アカウント登録をしたサイトには，特定の国の番号でしか登録できないウェブサイトや有料会員のみアカウントを持てるサイトが存在したため，SMS のパスワードリセットの有無を調査できなかったウェブサイトが 11 件ある．調査したすべてのウェブサイトを表 4.3 に示す．

表 4.3: top200web サイト

ランク	名前	URL
1	Google	http://www.google.co.jp/

2	Google	http://www.google.com/
3	Youtube	http://www.youtube.com/
4	Yahoo Japan	http://www.yahoo.co.jp/
5	Amazon	http://www.amazon.co.jp/
6	Facebook	http://www.facebook.com/
7	niconico	http://www.nicovideo.jp/
8	Twitter	http://www.twitter.com/
9	楽天	http://www.rakuten.co.jp/
10	Wikipedia	http://www.wikipedia.org/
11	FC2	http://www.fc2.com/
12	Twitter	http://www.t.co/
13	百度	http://www.baidu.com/
14	価格.com	http://www.kakaku.com/
15	livedoor	http://www.livedoor.com/
16	Ameba	http://www.ameblo.jp/
17	Amazon	http://www.amazon.com/
18	qq	http://www.qq.com/
19	Instagram	http://www.instagram.com/
20	livedoor	http://www.livedoor.com/
21	tmail	http://www.tmall.com/
22	Yahoo	http://www.yahoo.com/
23	NAVER まとめ	http://www.naver.jp/
24	taobao	http://www.taobao.com/
25	reddit	http://www.reddit.com/
26	Microsoft	http://www.live.com/
27	Apple	http://www.apple.com/
28	DMM.com	http://www.dmm.co.jp/
29	BUYMA	http://www.buyma.com/
30	goo	http://www.goo.ne.jp/
31	chatwork	http://www.chatwork.com/
32	livedoor Blog	http://www.blog.jp/
33	xvideos	http://www.xvideos.com/
34	pornhub	http://www.pornhub.com/
35	weblio	http://www.weblio.jp/
36	sohu.com	http://www.sohu.com/
37	JD.com	http://www.jd.com/

38	msn	http://www.msn.com/
39	日本郵政	http://www.japanpost.jp/
40	Microsoft	http://www.microsoft.com/
41	GitHub	http://www.github.com/
42	Hatena	http://www.hatena.ne.jp/
43	5 ちゃんねる	http://www.2ch.net/
44	NETFLIX	http://www.netflix.com/
45	sina.com	http://www.sina.com.cn/
46	weibo	http://www.weibo.com/
47	Tmall	http://www.list.tmall.com/
48	asos	http://www.asos.com/
49	食べログ	http://www.tabelog.com/
50	Hatena Blog	http://www.hatenablog.com/
51	Dailymotion	http://www.dailymotion.com/
52	PayPal	http://www.paypal.com/
53	Bing	http://www.bing.com/
54	5 ちゃんねる	http://www.5ch.net/
55	ebay	http://www.ebay.com/
56	360	http://www.360.cn/
57	livedoor Blog	http://www.doorblog.jp/
58	Adobe	http://www.adobe.com/
59	Tumblr	http://www.tumblr.com/
60	Dropbox	http://www.dropbox.com/
61	Office 365	http://www.office.com/
62	日本経済新聞	http://www.nikkei.com/
63	Linledin	http://www.linkedin.com/
64	メルカリ	http://www.mercari.com/
65	朝日新聞	http://www.asahi.com/
66	impress	http://www.impress.co.jp/
67	imgur	http://www.imgur.com/
68	stackoverflow	http://www.stackoverflow.com/
69	SAKURA internet	http://www.sakura.ne.jp/
70	DMM.com	http://www.dmm.com/
71	WordPress	http://www.wordpress.com/
72	NHK	http://www.nhk.or.jp/
73	Google	http://www.google.com.hk/

74	LINE	http://www.line.me/
75	Amazon	http://www.cloudfront.net/
76	BBC	http://www.bbc.com/
77	Qiita	http://www.qiita.com/
78	Twimg	http://www.twimg.com/
79	産経新聞	http://www.sankei.com/
80	産経新聞	http://www.sankei.com/
81	ITmedia	http://www.itmedia.co.jp/
82	VALUE COMMERCE	http://www.valuecommerce.com/
83	IMDB	http://www.imdb.com/
84	日経 BP 社	http://www.nikkeibp.co.jp/
85	Ameba	http://www.ameba.jp/
86	Feedly	http://www.feedly.com/
87	Xhamster	http://www.xhamster.com/
88	So-net	http://www.so-net.ne.jp/
89	FC2	http://www.himado.in/
90	Seesaa BLOG	http://www.seesaa.net/
91	FARFETCH	http://www.farfetch.com/
92	ヨドバシ.com	http://www.yodobashi.com/
93	ヤマト運輸	http://www.kuronekoyamato.co.jp/
94	PopAds	http://www.popads.net/
95	CNET	http://www.cnet.com/
96	Booking.com	http://www.booking.com/
97	livedoor Blog	http://www.livedoor.biz/
98	vk	http://www.vk.com/
99	Ask	http://www.ask.com/
100	The Pirate Bay	http://www.thepiratebay.org/
101	livedoor Blog	http://www.livedoor.biz/
102	indeed	http://www.indeed.com/
103	マイナビ	http://www.mynavi.jp/
104	MUFG	http://www.mufg.jp/
105	eroterest	http://www.eroterest.net/
106	NIH	http://www.nih.gov/
107	Pinterest	http://www.pinterest.jp/
108	AliExpress	http://www.aliexpress.com/
109	openload	http://www.openload.co/

110	excite	http://www.excite.co.jp/
110	SOUND CLOUD	http://www.soundcloud.com/
111	The Guardian	http://www.theguardian.com/
112	indeed	http://www.indeed.com/
113	楽天カード	http://www.rakuten-card.co.jp/
114	Stack Exchange	http://www.stackexchange.com/
115	Pinterest	http://www.pinterest.com/
116	Microsoft	http://www.microsoftonline.com/
117	百度	http://www.hao123.com/
118	ZOZOTOWN	http://www.zozo.jp/
119	cookpad	http://www.cookpad.com/
120	deloton	http://www.deloton.com/
121	BIGLOBE	http://www.biglobe.ne.jp/
122	The New York Times	http://www.nytimes.com/
123	YOMIURI ONLINE	http://www.yomiuri.co.jp/
124	オレ的ゲーム速報	http://www.jin115.com/
125	小説家になろう	http://www.syosetu.com/
126	livedoor	http://www.blogimg.jp/
127	Google	http://www.google.com.sg/
128	気象庁	http://www.jma.go.jp/
129	EPWK	http://www.epwk.com/
130	Amazon	http://www.amazon.co.uk/
131	@nifty	http://www.nifty.com/
132	Gigazine	http://www.gigazine.net/
133	Avgle	http://www.avgle.com/
134	WhatsApp	http://www.whatsapp.com/
135	同程旅遊	http://www.ly.com/
136	BBC	http://www.bbc.co.uk/
137	mixi	http://www.mixi.jp/
138	AbemaTV	http://www.abema.tv/
139	楽天銀行	http://www.rakuten-bank.co.jp/
140	Avgle	http://www.avgle.com/
141	slack	http://www.slack.com/
142	WIKIWKI	http://www.wikiwiki.jp/
143	CSDN	http://www.csdn.net/
144	日刊スポーツ	http://www.nikkansports.com/

145	漫画村	http://www.mangamura.org/
146	WoW Korea	http://www.wowkorea.jp/
147	Spotify	http://www.spotify.com/
148	Google	http://www.google.com.tw/
149	アルク	http://www.alc.co.jp/
150	aws	http://www.amazonaws.com/
151	Google	http://www.googleusercontent.com/
152	togetter	http://www.togetter.com/
153	Evernote	http://www.evernote.com/
154	mozilla	http://www.mozilla.org/
155	楽天	http://www.rakuten.ne.jp/
156	wikiHow	http://www.wikihow.com/
157	tenki.jp	http://www.tenki.jp/
158	ALIPAY	http://www.alipay.com/
159	The Washington Post	http://www.washingtonpost.com/
160	気象庁	http://www.jma.go.jp/
161	エロマガ	http://www.mmaaxx.com/
162	salesforc3e	http://www.force.com/
163	毎日新聞	http://www.mainichi.jp/
164	txxx	http://www.txxx.com/
165	HOT PEPPER	http://www.hotpepper.jp/
166	w3schools.com	http://www.w3schools.com/
167	コンピュータウイルス	http://www.hitcpm.com/
168	ANA	http://www.ana.co.jp/
169	NORDSTROM	http://www.nordstrom.com/
170	T-POINT	http://www.tsite.jp/
171	FANDOM	http://www.wikia.com/
172	UNIQLO	http://www.uniqlo.com/
173	FE.fr	http://www.femmevetements.net/
174	Money Forward ME	http://www.moneyforward.com/
175	iwanttodeliver.com	http://www.iwanttodeliver.com/
176	SBI 証券	http://www.sbisec.co.jp/
177	RAPID GATOR	http://www.rapidgator.net/
178	excite blog	http://www.exblog.jp/
179	Anitube	http://www.anitube.se/
180	Tmall	http://www.detail.tmall.com/

181	GameWith	http://www.gamewith.jp/
182	はちま起稿	http://www.esuteru.com/
183	Infoseek	http://www.infoseek.co.jp/
184	SoftBank	http://www.softbank.jp/
185	shopbop	http://www.shopbop.com/
186	天涯社区	http://www.tianya.cn/
187	C 級 hack(シクハック)	http://www.ldblog.jp/
188	Yahoo Japan	http://www.geocities.jp/
189	GoDaddy	http://www.godaddy.com/
190	bitFlyer	http://www.bitflyer.jp/
191	savefrom.net	http://www.savefrom.net/
192	taojindi	http://www.taojindi.com/
193	Share Videos	http://www.share-videos.se/
194	Walmart	http://www.walmart.com/
195	ぐるなび	http://www.gnavi.co.jp/
196	Nyaa	http://www.nyaa.si/
197	zhanqi	http://www.zhanqi.tv/
198	BEST BUY	http://www.bestbuy.com/
199	B9GOOD	http://www.b9good.com/
200	SMBC	http://www.smbc-card.com/

4.4 考察

調査結果では，警告が記載されていない 15 のウェブサイトがあった．その理由として電話番号の登録が必須でないことが考えられる．例えば，Yahoo Japan ではアカウントを作る際のフォームには電話番号の登録がなく，アカウント作成後に任意で追記する仕様である．Amazon では，専用のスマートフォンアプリで電話番号を登録しないと，通常のウェブブラウザではパスワードリセットができない．一方で，電話番号だけでアカウントを作成できる Twitter や Facebook には警告が明示されていた．従って，上記の 15 サービスの SMS に警告がないからといって即，脆弱性というわけではない．

表 4.1: top200web サイト統計情報

<table>
<tr><td>アカウント登録なし 27</td><td colspan="5"></td></tr>
<tr><td rowspan="4">有 173</td><td>SMS なし</td><td colspan="4">145</td></tr>
<tr><td rowspan="3">有</td><td rowspan="3">28</td><td>警告なし</td><td>15</td><td>Yahoo JAPAN</td></tr>
<tr><td>警告有</td><td>12</td><td>Twitter</td></tr>
<tr><td>URL 有</td><td>1</td><td>Instagram</td></tr>
<tr><td>計 200</td><td colspan="5"></td></tr>
</table>

表 4.2: パスワードリセット警告なしの SMS を使うサービス

サービス	Alexa ランク	SMS 例
Google	1	G-910957 is your Google verification code.
Yahoo JAPAN	4	確認コード:375403 上記の番号を画面へ入力してください Yahoo! JAPAN
Amazon	5	お客様の Amazon 確認コードは 160973 です。
LinkedIn	63	LinkedIn の検証コードは「123512」です。

第5章　潜在リスクに対するユーザ実験

5.1　目的

ウェブ登録の際に認証コードを入力しているつもりで，気付かずにリセットコードを入力してしまうことで，PRMitM 攻撃の被害を受けてしまうが，その原因が SMS によるものなのかユーザの特徴によるものなのか明らかになっていない．よって本実験では，ユーザのどのような要因がパスワードリセットコードの入力を促しているのかを明らかにする．

5.2　方法

クラウドソーシングサイトであるクラウドワークス [16] を用いて実験協力の募集を行い，集まった被験者 184 名による架空のウェブサイトへの登録実験を行う．被験者の属性を表 5.1 に示す．本実験では，被験者のスマートフォンに SMS を用いてメッセージを送信する．SMS の送信には，Twilio[17] のプログラマブル SMS を用いた．

被験者は実験開始時に次のように説明される

「この実験はセキュリティ意識の調査実験です．これから表示される 4 種類の架空のウェブサイトに登録する必要があります．しかし，被験者の中には脆弱性を持つサイトが表示される可能性があります．もしも表示されたサイトが安全なものでないと感じたら，登録をキャンセルしてください.」

しかし，実際には全被験者に対して 3 回目の登録時に脆弱性のあるサイトを表示する．脆弱性のあるサイトでの登録において，気付かずに登録を完了してしまったユーザを脆弱，途中で気づいて登録をキャンセルしたユーザを安全と判断する．

表 5.1: 被験者情報

	男	女
20 歳未満	1	2
20 代	32	32
30 代	25	39
40 代	21	16
50 歳以上	11	5
合計	90	94

図 5.1: 実験で用いる登録画面 (1)

表 5.2: 登録実験のサイトと測定目的

	(1)	(2)	(3)(攻撃)	(4)
名前	S! JAPAN	Cowtter	Majebook	Mstagram
SMS で表示されるもの	SMS なし	Cowtter の確認コード	S! JAPAN のリセットコード	Mstagram の確認コード
目的	登録練習	SMS の練習	パスワードリセットの要因調査	SSL の影響調査

架空のウェブサイトの登録手順を説明する．まず初めに図 5.1 のような入力画面が表示されるので，名前，パスワード，電話番号を入力して登録を完了する．以後ウェブサイトのタイトルが異なるだけで，登録フォームは同じ形式である．次に，SMS でなんらかのコードが送られてくるので，安全だと判断できればコードを入力，危険だと判断すればキャンセルを選択する．被験者が行う行動を表 5.2 に示すとともに，詳細を以下で説明する．全ての SMS に送信元企業名は記載されている．実験サイトは研究室内サーバに設置し，TLS 通信を用いている．

(1) 最初の登録のみ．

(2) 最初の登録の後，SMS で確認コードが送られてくるので，コードの入力かキャンセルをする．この SMS で送られる確認コードは入力しても問題ない安全なコードである．

(3)(攻撃) 最初の登録の後，SMS で (1) で登録したサイトからパスワードリセットコードが送られてくる．被験者を 5 グループに分け，それぞれに表 5.3 で定めた異なる 5 種類のタイプの SMS を

表 5.3: パスワードリセットコードの種類

type	警告	数字	英数字	長文	人数
0	×	○	×	×	37
1	○	○	×	×	38
2	○	×	○	×	40
3	○	○	×	○	35
4	○	×	○	○	34

送信する．ここで，警告，数字，英数字は 3 章で定義した攻撃である．長文のグループは SMS が 2 通送られる．1 通目のコードを入力した後で，type1,2 と同様の SMS が送られてくる．この SMS で送られるパスワードリセットコードを入力したユーザは脆弱である．

(4) (2) と手順は同じだが，コードの入力画面のみ通信が暗号化されない．

1 つの登録が終わるごとに，一連の登録手順に対して以下のアンケートを行う．

1. どれくらい使いやすかったですか

2. どれくらいセキュリティに関して安心できると感じましたか

全ての登録が終了した後，ユーザの属性に関するアンケートと SeBIS を行い実験を終了する．

本実験では，type0 をベースライン条件として設定した．もし type1+3 と type2+4 に有意差が認められれば，数字と英数字の場合で攻撃に対する耐性に影響を及ぼしている可能性がある．同様に type1+2 と type3+4 に差があれば，長文攻撃は脅威である．

リセットコードを入力する際，SMS をどれ位丁寧に読んでいるかを測るために，それぞれのウェブサイトでの基本情報フォームの入力から作業終了までにかかる時間を測定した．もしも作業時間が長いほど被害率が低ければ，SMS を丁寧に読むほど攻撃を受けづらいと言えるだろう．また，作業時間が極端に短ければ SMS をあまり読んでいないと判断できる．逆に，あまりにも時間がかかった場合でも，作業そのものに集中していないと考えられるため，SMS をあまり読んでいないと考えられる．

5.3 倫理

本実験では架空のウェブサイトを用いており，実施にパスワードリセット攻撃を行っていない．実験に参加する被験者は実験開始前にウェブ上で付録 A の取得情報などに関する同意取っている．

本実験では被験者の電話番号を取得して，送信サービス [17] に委託して SMS を送信している．被験者には，そのことを同意の上で参加してもらっており，第三者提供にはあたらないため，SMS を送るために取得したものであり，第三者に提供する目的ではないため，クラウドワークスの禁止事項 (3)「 特定個人の氏名・住所・電話番号・メールアドレスなど第三者が見て個人を特定できる情報を第三者に提供する行為」に違反しないと考える．

表 5.4: type ごとのリセット被害率

type	SMS	入力	キャンセル	リセット被害率 [%]
0	警告なし	35	2	94.6
1	数字・短文	30	8	78.9
2	英数字・短文	28	12	70.0
3	数字・長文	28	7	80.0
4	英数字・長文	22	12	64.7

表 5.5: キャンセルの理由

理由	人数
仕組みがよくわからなかったから	10
S! JAPAN と書いてあったから	14
パスワードリセットと書いてあったから	16
1 通目の SMS が長かったから	1

5.4 結果

実験の結果を表 5.4 に示す．SMS タイプなどの条件 x におけるリセット被害率 R_x は

$$R_x = \frac{x \text{でコードを入力した人数}}{x \text{の被験者数}}$$

と定める．例えば，

$$R_{type1} = \frac{30}{38}$$

である．ここで，入力は (3) に対してリセットコードを中間者 B に入力してしまった被害数を示す．

キャンセルの理由と結果を表 5.5 に示す．2 つ以上の理由でくキャンセルした人はいたかもしれないが，複数選択できるようにはしていない．

被験者の性別や年齢などの属性についてのリセット攻撃に対する被害率 R を表 5.6 に示す．概して，70%〜80%に分布している．最も R が高いのは，50 代以上や Facebook への登録を覚えていない層であり，SMS の条件をよく理解せず，盲目的にコードを入力している可能性がある．

入力とキャンセルにかかった時間の分布を図 5.2 に示す．type0,1,2 に対して，type3,4 の平均回答時間が長いのは，入力が 2 回だからである．

SeBIS の結果の平均と標準偏差を表 5.7 に，SeBIS の合計点数を図 5.3 に示す．また，SeBIS の全回答結果を付録 B に示す.[1]

各ウェブサイトの登録手順における使用感と安心度に関するアンケートの結果を表 5.8 に示す．

[1]問 6, 17 は問題に答えているかの確認であり，正しい回答をしていない被験者は除いている．

表 5.6: 利用者属性別の PRMitM 攻撃被害率

		入力	キャンセル	計	リセット被害率 [%]
性別	男	66	24	90	73
	女	77	17	94	82
年代	20 未満	2	1	3	67
	20 代	48	16	64	75
	30 代	50	14	64	78
	40 代	27	10	37	73
	50 代以上	16	0	16	100
twitter に電話番号を登録	している	27	7	37	73
	していない	95	31	126	75
	わからない	21	3	24	88
Facebook に電話番号を登録	している	41	12	53	77
	していない	85	29	114	75
	わからない	17	0	17	100
Yahoo に電話番号を登録	している	39	7	46	85
	していない	74	28	102	73
	わからない	30	6	36	83
携帯電話の機種	iPhone	57	17	74	77
	Android	64	16	80	80
	その他	22	8	30	73

5.5 考察

5.5.1 人間要素の効果

各条件である「警告の有無」,「リセットコードが数字のみか英数字か」,「メッセージが 1 通か 2 通か」の影響を評価するために，それぞれ type0 と type1，type1+3 と type2+4，type1+2 と type3+4 を比較する．そして，これらの条件による差が偶発でないかを確かめるため，帰無仮説「コードを入力して被害を受ける数は，条件 x に対して独立である」をおいて，自由度 1 のカイ二乗検定 (両側検定) をした．結果を表 5.9 に示す．*を $p < 0.1$(有意水準 10%) とし，***を $p < 0.01$(有意水準 1%) とする．

カイ二乗検定の結果，type 0 と type 1 には有意差が認められ ($p = .09 < 0.1$)，警告の有無がパスワードリセット攻撃に対して影響を与えたことが明らかになった．type1+3 と type2+4 を比較すると，コードを英数字にすることでリセット被害率は減少したが，数字のみと英数字の間に有意差は認められなかった ($p = .14 < .01$)．また，type1+2 と type3+4 を比較した結果，長文と短文の間にも有意差は認められなかった ($p = .94 < .01$)．一方で，http と https の間には被害率に有意差が認められた ($p < .001$)．この結果から，ユーザは http と https の違いに注意を向けていることが示された．

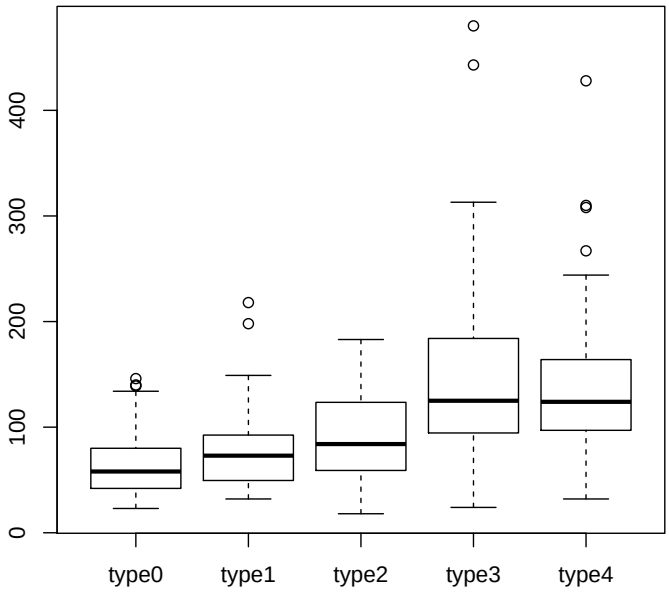

図 5.2: 各タイプの回答時間の分布

5.5.2 時間的要素

type0,1,2 はコードの入力が 1 回，type3,4 は入力が 2 回であるので，両者間の時間の差は妥当なものであるため，各 type 間に注目すべき時間の差は見られなかった．また，攻撃を受けたかどうか，リセットコードが数字，英数字かどうかも入力の時間に影響しなかった．このことから，多くのユーザは SMS で送られてきたコードを入力する際に，どのような内容がかかれていようと，メッセージを数秒しか読まずに判断していると考えられる．

5.5.3 SeBIS セキュリティ志向度と被害率

被験者全体の平均得点が 50.3 点だったので，50 点以上を閾値として，入力した人数とキャンセルした人数を表 5.10 に示す．また，被験者の属性についての SeBIS の差を表 5.11 に示す．リセットコードを入力した被験者とキャンセルした被験者で SeBIS の得点に大きな差は見られなかった．また，セキュリティ志向度が高くなるような被験者の属性は存在しなかった．

この結果から，セキュリティ知識に対して大きな影響を及ぼす被験者の属性は存在しなかったが，PRMitM 攻撃を受けてしまうことにセキュリティ知識の高低は影響を及ぼさないことが明らかになった．

5.5.4 ロジスティック回帰

SMS のタイプ，被験者の属性等の多くの要因の内，リセット攻撃を受ける主要な因子を明らかにするため，被害を受ける確率 p を目的変数とし，他の交絡因子，SMS のタイプ x_1,x_2, x_3, 3 つのウェ

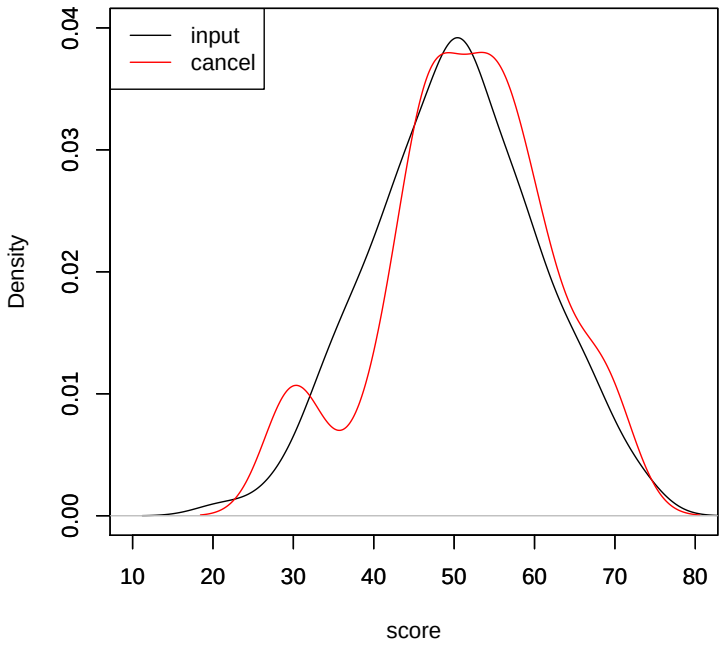

図 5.3: 入力とキャンセルした被験者のセキュリティ志向度と被害率の SeBIS 点数分布

ブサイト登録についての使用感 $x_{1,1}$, $x_{2,1}$, $x_{3,1}$　と安心度 $x_{2,1}$, $x_{2,2}$, $x_{3,2}$, 被験者属性についてのアンケート，年齢 $x_{4,0}$, 性別 $x_{4,01}$，Twitter に電話番号を登録しているか $x_{4,1}$，Facebook に電話番号を登録しているか $x_{4,2}$，Yahoo アカウントに電話番号を登録しているか $x_{4,3}$，よく知られたサービスのアカウントを作成するために電話番号を使用することに抵抗はあるか $x_{4,\ 4}$，初めて見つけたサービスのアカウントを作成するために電話番号を使用することに抵抗はあるか $x_{4,5}$，実験に使用した携帯電話の種類は何か $x_{4,7}$，SeBIS の各質問の答 x_{q1}, x_{q2}, ..., x_{q18} を説明変数としたロジスティック回帰，すなわち，

$$\log \frac{p}{1-p} = \beta_0 + \beta_1 x_1 + \cdots + \beta_{18} x_{18}$$

を行った．結果を表 5.12 に示す．例えば，警告なし $(x_1 = 0)$ に対する，警告有 $(x_1 = 1)$ による被害確率の調整オッズ比は，

$$\frac{\text{警告なし被害率}}{\text{警告なしキャンセル率}} \Big/ \frac{\text{警告有被害率}}{\text{警告有キャンセル率}} = e^{\beta_1} = 0.286$$

しかし，有意水準に達していない．一方，x_{q5}(SeBIS 問 5「必要あるときしかパスワードを変更しない」) については，$p = 0.00058 < 0.001$ であり水準 1%を超えて有意である．このオッズ比は，$e^{2.45} = 11.59$ である．この結果から，パスワードをよく変更する人は，しない人の 11.6 倍リセット攻撃の被害を受けやすいことが明らかになった．これまでパスワードは頻繁に変更することが推奨されてきたが，従来とは反対の結果となった．原因の一つとして，頻繁にパスワードを変更することで，SMS のパスワードリセットを用いてのパスワード変更になれてしまっていることが考えられる．アカウントの登録もパスワードの変更も送られてきたコードを入力するという手順は同じなので，普段通りに行動

してしまう．たとえメッセージに警告文が含まれていても目に入らない．メッセージを見ずとも何をすればよいか理解しているためである．結果として，慣れてない人よりも簡単にリセットコードを入力してしまうだろう．また別の原因として，パスワードをよく忘れる人がパスワードを頻繁に変更していることが考えられる．このようなユーザはそもそも盗まれて困るようなアカウントは所有していないと考えられるので，攻撃に対する警戒心が薄くなってしまうのだろう．

SeBIS 問 8 は,「新しいオンラインアカウントを作るとき，必用最低限の文字数を超えるパスワードを設定する」である．この結果から，十分に長いパスワードを設定する人は $e^{-5.08}$ 倍 $= 0.56$ に被害を下げることが明らかになった．長い複雑なパスワードを設定することで，同じパスワードを使い続けているため，パスワードの変更になれておらず，SMS のメッセージをしっかりと呼んでいたためだと考えられる．この結果は従来の考えと比較しても妥当な結果であり，PRMitM 攻撃を防ぐ手段の一つは長いパスワードを設定することであると言える．

SeBIS 問 10 は,「リンクが送られてきたとき，どこにつながるか確認しないでクリックする」である．この結果から，リンクが送られてきたとき，どこにつながるか確認しているユーザは $e^{-0.98} = 0.37$ に被害を下げることが明らかになった．原因としては，リンクを確認する几帳面さや怪しいリンクを簡単にクリックしない注意深さが，SMS のメッセージ確認を怠ることがないセキュアな行動をとらせていると考えられる．

5.6 PRMitM 攻撃のインパクト評価

本研究の結果から，実際の企業に対してどれほどの影響を及ぼすかを Yahoo Japan を例に考察する．Yahoo Japan の SMS には警告がなく，リセットコードは数字のみなので，表 5.4 を参照し，type0 と type1 の警告の有無に対するオッズ比は $\frac{35}{2}/\frac{30}{8} = 4.67$ となる．よって，警告なしの場合は警告有の場合と比較して 4.67 倍パスワードリセット攻撃を受けやすくなる．Yahoo Japan のアクティブユーザ数は 2016 年 9 月の時点で 3,614 万人と言われている [18]．表 5.6 の結果から，Yahoo アカウントに電話番号を登録している被験者は 46/180=0.2555... なので，約 26%のユーザが電話番号を登録していると考えられる．よってヤフーに電話番号を登録しているユーザ数を $3614 \cdot 0.256 = 925.184$, 約 925 万人であると仮定する．

警告なしの場合では，$925 \cdot \frac{35}{37} = 875$ つまり，875 万人が潜在的に被害を受ける可能性があるが，警告有の場合では $925 \cdot \frac{30}{38} = 730.3$ なので 730.3 万人まで潜在的被害者を減らすことが出来る．

表 5.7: SeBIS 指標

番号	質問	μ	σ
1	コンピュータを長時間放置したとき，自動的にロックするような設定にしている	3.44	1.745
2	ノートパソコンやタブレットのロックを解除するとき，パスワード/パスコードを使っている	3.97	1.583
3	コンピュータから離れるとき，手動で画面をロックする	2.65	1.580
4	携帯電話のロックを解除するために PIN またはパスコードを使用する	3.38	1.823
5	必要があるときしかパスワードを変更しない	2.30	0.932
7	使っているアカウントごとに違うパスワードを使っている	3.01	1.302
8	新しいオンラインアカウントを作るとき，必用最低限の文字数を超えるパスワードを設定する（8 文字以上なら，9 文字以上で設定）	3.51	1.534
9	必要がない場合は，パスワードに特殊文字（¥や＊）を含めない	1.89	1.108
10	リンクが送られてきたとき，どこにつながるか確認しないでクリックする	3.61	1.206
11	どのサイトに訪れたかを URL ではなくサイトの外観と雰囲気で判断している	2.72	1.115
12	安全な通信か確認することなくウェブサイトに情報を提出する（例 : SSL，”https : //”，ロックアイコン）	3.18	1.261
13	リンクをクリックする前に，マウスアイコンをリンクに乗せ訪れる URL を確認する	2.93	1.233
14	セキュリティ上の問題が発見されても誰かが直すだろうからそのまま使い続ける	3.52	1.135
15	ソフトウェアのアップデートについてのメッセージが表示されたらすぐにインストールする	3.52	1.141
16	使用しているプログラムが最新であることを確認するようにしている	3.21	1.137
18	自分のアンチウイルスソフトウェアが定期的に更新されていることを確認する	3.49	1.292
合計		50.3	10.314

表 5.8: 各サイトの使用感と安心感の平均

	質問 1．使いやすかったか	質問 2．安心できたか
(1) S! Japan	5.98	4.14
(2) Cowtter	5.83	5.03
(3) Majebook	5.19	4.64

表 5.9: SMS の種類によるリセット被害の分割表

type		入力	キャンセル	リセット被害率 [%]	χ	P 値
0	警告無し	35	2	94.6	2.7333	0.09828*
1	警告有	30	8	78.9		
1+3	数字のみ	58	15	79.5	2.088	0.1485
2+4	英数字	50	24	67.6		
1+2	短文	50	19	72.5	0.0053	0.9421
3+4	長文	58	20	74.4		
入力 2	https	164	20	89.1	24.2937	8.27e-07***
入力 4	http	124	60	67.3		

表 5.10: SeBIS 点数によるリセット被害率

	入力	キャンセル	被害率
50 点以上	66	21	75.9
50 点未満	54	18	75.0

表 5.11: SeBIS 点数による属性の差

		50 点以上	50 点未満	計
性別	男	51	34	85
	女	36	38	74
年代	20 未満	2	0	2
	20 代	26	19	45
	30 代	31	33	64
	40 代	17	17	34
	50 代以上	11	3	14
twitter に電話番号を登録	している	15	13	28
	していない	61	50	111
	わからない	11	9	20
Facebook に電話番号を登録	している	27	19	46
	していない	54	48	102
	わからない	6	5	11
Yahoo に電話番号を登録	している	25	17	42
	していない	49	38	87
	わからない	13	17	30
携帯機種	iPhone	30	23	53
	Android	41	35	76
	その他	16	14	30

表 5.12: ロジスティック回帰分析

	Estimateβ	Std. Error	z value	Pr(>|z|)
(Intercept)	-1.68	4.64	-0.36	0.717 *
x_0	-1.25	163	-077	0.443
x_1	-3.31	1.60	-2.07	0.038 *
x_2	-4.46	1.93	-2.31	0.021 *
x_3	-4.05	1.82	-2.23	0.026 *
x_4	1.21	0.46	2.54	0.011 *
$x_{1,1}$	0.88	0.36	2.47	0.013 *
$x_{1,2}$	0.59	0.48	1.23	0.219 *
$x_{2,1}$	-1.35	0.45	-2.99	0.002***
$x_{2,2}$	-0.65	0.30	-2.18	0.029 *
$x_{3,1}$	1.63	0.36	4.54	5.61e-06 ***
$x_{3,2}$	0.65	0.45	1.46	0.145
$x_{4,0}$	-0.33	0.83	-0.39	0.694
$x_{4,01}$	-0.55	0.57	-0.96	0.339
$x_{4,1}$	0.23	0.40	0.58	0.564
$x_{4,2}$	-0.58	0.53	-1.11	0.269
$x_{4,3}$	-0.29	0.28	-1.03	0.302
$x_{4,4}$	0.47	0.32	1.49	0.137
$x_{4,5}$	0.65	0.70	0.93	0.350
$x_{4,7}$	0.01	0.28	0.02	0.981
x_{q1}	-0.54	0.34	-1.60	0.110
x_{q2}	0.29	0.26	1.09	0.278
x_{q3}	0.15	0.29	0.52	0.601
x_{q4}	2.45	0.71	3.44	0.00058 ***
x_{q5}	-0.57	0.44	-1.28	0.199
x_{q7}	-0.58	0.29	-1.97	0.048 *
x_{q8}	0.41	0.37	1.13	0.259
x_{q9}	-0.98	0.46	-2.10	0.0362 *
x_{q10}	-0.33	0.37	-0.89	0.376
x_{q11}	0.41	0.40	1.01	0.314
x_{q12}	-0.34	0.41	-0.82	0.414
x_{q13}	0.22	0.34	0.64	0.524
x_{q14}	-0.24	0.44	-0.55	0.581
x_{q15}	0.85	0.45	1.87	0.060
x_{q16}	-1.27	0.45	-2.81	0.004965 **
x_{q18}				

第6章　結論

本稿では，SMS を用いた 2 要素認証方式のパスワードリセット手法を悪用した，PRMitM 攻撃に注目し，主要サイトの PRMitM 攻撃に対する危険度調査と，被験者実験による人間的要素を利用した PRMitM 攻撃の潜在的な脅威の評価を行った．

主要使途に対する危険度調査では，日本のアクセス数上位のウェブサイトで 28 サイトが SMS を用いたパスワードリセットを行っており，そのうち 15 サイトにはパスワードリセットの SMS 本文に，パスワードリセットであることの警告が記載されていなかった．しかし，警告のない 15 サイトにはドメインが異なるだけの同一サイトが含まれていたため，同じアカウントを共有しないユニークなサイトは「Google」,「Yahoo JAPAN」,「Amazon」,「LinkedIn」の 4 サイトであった．

PRMitM 攻撃の潜在的な脅威の評価では，被験者による実験により，警告の有無，リセットコードの種類，長文の SMS による攻撃によって，PRMitM 攻撃の被害が，4.6 倍，1.86 倍，0.91 倍になることを示した．また，パスワードをよく変更する人は，この攻撃を 11.59 倍受けやすいことを示した．ただし，リセットコードの種類，長文の SMS による攻撃による差は 10%有意水準に届かなかった．また，被験者の属性，リセットコードの入力にかかる時間は，リセット被害率に対して影響を与えないことを示した．

警告を記載しても PRMitM 攻撃の被害を完全に防ぐことはできないため，より安全なパスワードリセット手法を検討していく必要があると考えている．

参考文献

[1] 株式会社ディアイティ　セキュリティ調査レポート Vol.3 パスワードの最大解読時間測定，https://cybersecurity-jp.com/cyber-terrorism/17426，2019 年 1 月 8 日参照.

[2] A. Adams and M. A. Sasse, “Users Are Not The Enemy,” Commun. ACM, vol. 42, no. 12, pp. 40 46, 1999.

[3] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The Tangled Web of Password Reuse. In Proceedings of the 2014 Network and Distributed System Security Symposium (NDSS), 2014.

[4] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor. “I Added ‘!’ at the End to Make It Secure”: Observing Password Creation in the Lab. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS), pp. 123 140, 2015.

[5] J. J. Yan, A. F. Blackwell, R. J. Anderson, and A. Grant: Password memorability and security: Empirical results, IEEE Security and Privacy, vol. 2, no. 5, pp. 2531, 2004.

[6] Nethanel Gelernter, Senia Kalma, Bar Magnezi, Hen Porcilan: The Password Reset MitM Attack, IEEE Security and Privacy 2017.

[7] M. Zviran and W. J. Haga, “A comparison of password techniques for multilevel authentication mechanisms,” The Computer Journal, vol. 36, no. 3, pp. 227-237, 1993.

[8] 総務省　平成 2 9 年通信利用動向調査ポイント，http:/www.soumu.go.jp/johotsusintokei/statistics/data/180525_1.pdf，2019 年 1 月 8 日参照.

[9] Google Developer Japan Blog，https:/developers-jp.googleblog.com/2015/07/blog-post_8.html，2017 年 10 月 28 日参照.

[10] Halevi, T., Lewis, J., & Memon, N.D. (2013). A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. Proceedings of the 22nd International Conference on World Wide Web, 737-744.

[11] K. Krol, M. Moroz, and M.A. Sasse: Don ’ t work. can ’ t work? why it ’ s time to rethink security warnings， CRiSIS，Oct 2012.

[12] OpenID Japan，https:/www.openid.or.jp/，2017 年 10 月 8 日参照.

[13] SAGAWA，http://www2.sagawa-exp.co.jp/whatsnew/detail/721/#c26，2019 年 1 月 8 日参照.

[14] Serge Egelman, Eyal Peer: Scaling the Security Wall Developing a Security Behavior Intentions Scale (SeBIS), SIGCHI Conference on Human Factors in Computing Systems (CHI' 15).

[15] 日本のアクセス数上位サイト by アレクサ，https:/www.alexa.com/topsites/countries/JP，

[16] クラウドワークス，https:/crowdworks.jp/，

[17] Twilio，https:/twilio.kddi-web.com/

[18] paymentnavi，http://www.paymentnavi.com/paymentnews/61930.html，2017 年 10 月 23 日参照.

謝辞

本論文の作成にあたり，終始適切な助言を賜り，また丁寧に指導して下さった菊池浩明先生に深く感謝致します.

合同ゼミにおいてご助言をいただいた静岡大学創造科学技術大学院　西垣正勝教授，静岡大学情報学部情報科学科講師　大木哲史先生，東京電機大学理工学部理工学科情報システムデザイン学系助教稲村勝樹先生に心から感謝致します.

菊池研究室に所属する同期，後輩たちは積極的に実験協力をしてくれました．ありがとうございます.

FMS の異なる研究室の院生たちも実験に協力していただきましたこと感謝しています.

業績

1. 関川　慧，下野　弘朗，笹　航太，松井　啓司，荒川　薫，“ε-フィルタを用いたリアルタイム顔画像美観化システム”, **電子情報通信学会** *(IEICE 2015)*, ISS-P-78, 2015.
2. 笹　航太, 清水　雄太, 菊池　浩明, “あみだくじを用いた対話的なブラウザ履歴漏洩の研究”, **情報処理学会第** *78* **回全国大会**, 6V-04,pp.557-558, 2016.
3. Kota Sasa, Yuta Shimizu, Hiroaki Kikuchi “Interactive History Sniffing Attack with Amida Lottery”, *2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, pp.599-602, 2016.
4. 笹　航太, 菊池　浩明, “二要素認証を悪用したパスワードリセット手法 PRMitM の影響評価”, **暗号と情報セキュリティシンポジウム** *(SCIS 2018)*, 2018.
5. Kota Sasa, Hiroaki Kikuchi “Impact Assessment of Password Reset PRMitM attack with Two-factor Authentication”, *The 2018 IEEE Conference on Dependable and Secure Computing (DSC 2018)*, pp.90-97, 2018.

付 録 A　実験の同意書

アカウント登録のユーザビリティ調査における個人情報の取り扱いについて
個人情報の利用目的
以下の研究を遂行するために個人情報を取得します。

1. ユーザアカウント登録におけるユーザビリティに関する研究
2. ユーザアカウント登録におけるセキュリティに関する研究
3. 携帯電話やスマートフォンを用いた二要素認識に関する研究
4. ユーザの IT に関する知識に応じたセキュリティに関する研究

個人情報の取得本実験では、実験協力者様の携帯電話かスマートフォンの電話番号とセキュリティに関する経験や意識などのアンケート調査項目を取得します。

個人情報の利用取得した個人情報は本実験内で実験協力者様に SMS(ショートメッセージサービス) の送信に関わる研究目的の範囲内で利用いたします。研究結果を論文等により公表いたします。

個人情報の利用委託取得した電話番号に SMS を発信するため，SMS 発信サービス業者に委託します。

個人情報の第三者への開示・提供弊研究室は、実験協力者様よりお預かりした個人情報を適切に管理し、 研究目的を達成したらすみやかに廃棄いたします。個人情報を第三者に開示いたしません。

付 録B　SeBIS結果一覧

表 B.1: SeBIS 結果

被験者	Q1	Q2	Q3	Q4	Q5	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q18
1	5	5	5	5	2	2	4	3	3	4	5	5	5	5	5	5
2	1	1	1	5	3	3	2	2	4	3	1	3	1	3	2	4
3	3	5	2	2	2	4	3	1	3	2	2	1	3	2	1	3
4	2	2	2	5	2	3	3	2	4	4	4	4	4	2	2	3
5	5	5	5	5	3	2	3	2	3	4	5	4	5	3	4	4
6	5	5	3	5	3	4	4	3	4	3	4	4	2	4	4	4
7	2	5	4	5	3	4	4	3	4	2	3	2	5	4	4	4
8	5	5	1	1	1	1	5	1	5	2	5	5	5	5	5	5
9	5	5	1	1	1	1	5	1	5	2	5	4	5	5	5	5
10	5	5	5	5	3	4	5	2	5	4	5	3	4	4	5	4
11	5	5	4	5	1	3	2	1	2	5	1	1	2	4	1	1
12	1	1	1	1	3	5	4	1	5	4	3	4	4	4	4	5
13	5	5	5	2	3	4	4	1	4	2	2	3	4	4	4	5
14	4	4	4	5	2	2	5	1	3	4	3	3	4	4	3	4
15	1	1	1	1	3	4	2	2	3	2	2	3	4	3	2	3
16	5	5	5	5	3	3	3	3	5	5	5	3	5	2	5	5
17	2	2	2	5	2	3	3	1	3	2	2	4	3	5	5	5
18	5	5	3	4	3	4	5	2	4	3	4	4	4	4	3	5
19	1	1	5	1	1	2	4	1	2	2	2	1	1	1	1	1
20	4	5	1	4	2	2	4	2	3	3	3	2	3	2	3	3
21	2	2	3	1	2	2	2	1	3	3	3	3	4	3	3	4
22	1	5	3	5	3	3	5	1	4	3	3	4	4	3	3	3
23	5	5	2	4	4	2	5	2	3	2	4	4	4	1	1	2
24	2	2	2	2	2	4	2	4	4	2	3	2	4	3	2	3
25	1	1	1	1	1	1	1	1	2	2	1	2	1	3	1	1
26	2	5	1	1	1	3	5	2	2	2	3	4	3	5	4	1
27	1	1	1	1	2	2	4	1	2	3	2	1	3	2	1	2
28	2	4	1	5	2	3	5	3	4	3	3	3	2	2	4	3
29	1	5	4	1	2	2	2	1	4	3	3	2	2	2	2	2
30	5	4	1	5	2	3	4	1	3	3	4	4	3	4	3	4
31	2	1	1	1	2	4	4	2	4	1	2	1	3	2	2	4
32	5	5	4	5	2	5	2	3	5	3	5	4	4	3	4	2
33	5	5	5	5	4	3	5	2	5	2	3	3	2	3	3	3
34	5	5	1	1	1	2	5	2	5	1	4	3	4	4	2	2
35	5	5	4	5	2	5	4	2	3	3	4	3	3	4	3	5
36	5	5	1	5	3	4	3	2	5	5	5	5	5	5	5	5
37	2	2	2	2	1	1	1	1	5	3	3	4	2	5	3	4
38	5	5	1	5	3	4	3	2	5	5	5	5	5	5	5	5
39	5	5	5	5	3	2	3	2	4	3	3	3	5	2	4	4
40	1	1	1	1	1	2	5	1	3	4	1	2	2	3	2	1

41	5	5	5	5	3	4	5	2	4	4	5	5	5	3	3	5
42	1	1	3	5	2	2	5	1	4	3	3	4	3	3	2	0
43	2	2	4	2	2	3	4	3	3	3	2	3	4	3	3	3
44	5	5	5	5	3	3	3	1	4	2	5	5	5	4	4	5
45	5	5	5	5	3	4	4	2	4	5	2	3	2	4	3	4
46	2	1	2	2	2	2	2	2	2	3	4	2	4	3	3	3
47	2	2	2	2	2	3	2	2	3	3	3	3	2	3	3	3
48	5	5	1	5	2	3	3	2	3	2	2	2	5	3	3	4
49	1	1	1	1	2	2	2	1	4	2	3	3	3	3	3	3
50	5	5	5	3	3	4	4	4	4	3	4	3	3	3	3	4
51	2	5	4	5	3	4	5	2	3	4	4	3	4	1	3	4
52	5	5	4	5	4	5	5	3	5	3	3	4	5	3	2	3
53	5	5	5	5	2	2	3	2	2	2	3	2	5	2	2	2
54	1	2	1	5	1	3	5	1	2	1	1	1	4	3	5	1
55	5	5	5	1	3	5	5	3	4	5	5	5	4	3	1	5
56	1	5	1	1	2	2	2	2	4	1	1	1	1	4	3	3
57	5	5	2	5	1	1	5	1	3	2	4	3	4	2	2	4
58	1	1	1	5	1	2	5	2	1	1	1	1	2	2	1	2
59	5	5	2	5	1	1	1	1	3	3	1	3	5	2	3	2
60	5	5	2	4	2	1	5	1	5	3	4	2	3	3	1	1
61	5	2	1	5	2	3	3	2	5	3	2	1	4	2	1	2
62	5	5	3	5	3	2	2	2	3	4	4	3	4	5	3	4
63	5	5	2	5	2	3	4	1	2	1	2	1	2	4	3	4
64	5	5	3	1	2	2	3	2	5	1	3	1	5	5	5	5
65	5	5	3	5	2	2	4	3	1	3	2	3	3	3	3	4
66	5	5	2	5	3	5	5	4	5	1	5	5	4	5	5	5
67	2	5	4	5	2	3	4	3	3	3	2	2	4	2	2	3
68	5	5	2	5	2	5	5	2	2	2	3	3	2	4	2	2
69	5	2	2	2	2	3	5	2	5	2	4	4	2	5	5	4
70	1	1	1	1	1	4	4	1	5	5	5	4	1	5	5	3
71	5	5	5	5	4	4	3	2	5	4	5	5	4	5	4	5
72	5	5	5	5	4	4	5	3	3	3	4	4	3	5	4	5
73	1	5	5	5	1	1	2	1	2	2	2	3	4	5	2	2
74	1	5	1	1	3	5	4	4	3	2	2	2	2	3	2	3
75	5	5	2	2	2	3	5	1	2	3	3	2	4	3	3	3
76	5	5	5	5	2	2	4	1	4	3	2	2	2	4	3	3
77	2	1	1	1	2	4	5	1	1	4	2	1	3	3	1	1
78	1	1	1	1	2	3	3	2	1	5	1	1	3	2	2	1
79	5	5	3	4	1	2	1	3	2	1	1	5	1	5	4	4
80	5	5	3	5	2	2	1	5	4	2	5	2	1	1	1	4
81	3	5	4	5	3	4	5	2	3	4	3	2	3	4	5	5
82	5	5	5	5	4	5	5	3	1	5	5	5	5	4	5	5
83	5	5	5	5	5	5	5	3	5	5	4	4	5	2	5	5
84	3	3	3	3	4	4	5	3	2	3	3	4	4	5	5	5
85	5	5	5	5	3	4	4	2	4	4	4	4	2	4	3	4
86	5	5	1	3	2	3	5	2	4	2	3	2	4	4	3	4
87	5	5	2	5	1	4	3	1	5	3	5	2	4	4	5	4
88	5	5	2	2	3	4	5	2	3	2	4	3	2	5	4	5
89	4	5	3	5	4	2	2	1	3	2	3	2	5	3	3	2
90	1	5	1	5	2	3	5	2	5	2	4	1	5	5	2	2
91	5	5	1	4	1	2	5	4	2	3	2	3	2	4	2	4

92	5	5	5	1	3	4	5	3	5	3	5	1	5	5	5	5
93	5	5	3	4	4	4	5	2	4	3	2	4	2	2	3	4
94	2	3	5	1	2	1	1	1	2	4	1	1	4	5	1	1
95	1	1	1	1	2	2	3	2	2	3	2	3	3	3	3	3
96	5	5	5	5	2	3	3	2	1	3	3	2	3	4	2	3
97	2	5	2	5	2	3	2	2	3	2	3	2	2	5	2	2
98	1	5	5	5	3	2	2	2	4	3	1	3	4	5	4	1
99	5	5	1	1	2	2	1	2	3	4	2	2	4	4	2	3
100	2	1	1	2	3	2	4	1	4	3	3	2	2	4	4	4
101	1	1	5	2	2	3	5	2	2	3	4	4	4	3	2	2
102	5	5	2	2	2	2	5	2	5	2	3	4	5	5	4	4
103	5	5	3	5	3	4	4	2	5	4	4	3	3	3	4	3
104	2	2	2	1	2	4	2	2	3	3	5	3	5	3	3	2
105	5	5	1	1	1	3	4	3	4	3	4	3	5	4	4	3
106	2	5	2	5	3	4	3	2	3	2	3	3	4	4	3	3
107	1	5	1	5	1	1	1	1	4	3	4	1	4	1	1	5
108	5	5	3	5	2	2	2	2	4	2	4	4	4	2	4	4
109	5	5	2	5	3	4	4	2	4	3	3	3	3	4	3	3
110	5	5	2	5	2	3	5	2	5	4	3	2	4	3	4	4
111	4	5	3	4	3	4	2	2	3	2	3	3	4	3	3	2
112	5	5	3	5	1	3	5	1	4	1	2	1	5	3	2	2
113	1	3	1	5	2	2	3	1	3	2	2	2	4	4	2	2
114	5	5	2	5	2	5	4	1	3	1	2	3	5	2	3	5
115	2	3	5	2	4	3	4	4	4	2	2	3	3	3	4	4
116	5	5	1	5	1	3	1	1	1	1	3	1	1	3	1	1
117	2	4	5	2	2	2	3	1	3	4	2	3	3	4	4	3
118	5	5	3	4	4	3	5	2	5	3	4	4	4	4	5	5
119	5	5	5	5	4	4	5	5	5	4	2	3	3	3	4	5
120	3	2	1	1	1	3	2	2	4	3	5	4	2	3	3	5
121	1	5	1	1	3	3	3	2	4	3	3	1	2	3	1	4
122	1	5	4	5	1	5	3	4	4	5	5	2	5	3	4	5
123	2	5	3	2	3	4	3	3	4	1	5	4	3	5	4	5
124	1	2	2	1	2	3	4	1	4	4	4	2	4	3	4	5
125	5	5	1	1	2	3	1	1	4	5	5	4	4	5	3	3
126	3	5	3	1	1	5	5	5	4	5	3	5	1	3	4	4
127	5	5	5	5	4	5	2	5	5	1	3	3	4	3	3	4
128	5	2	2	1	3	2	1	1	3	2	3	3	4	3	4	5
129	5	5	1	5	3	4	5	3	4	2	2	3	3	3	4	5
130	1	5	2	5	3	4	5	2	5	1	5	1	5	5	3	3
131	1	1	1	1	2	3	4	1	3	3	3	3	2	4	3	4
132	5	5	5	5	2	2	5	1	5	1	4	4	3	5	3	3
133	1	1	1	1	3	3	3	2	4	4	3	5	5	3	3	1
134	5	5	4	5	3	3	5	2	4	3	5	4	4	2	4	4
135	2	1	4	5	1	5	5	1	5	2	5	3	2	5	4	4
136	5	5	4	5	1	3	4	1	3	4	2	4	2	5	1	2
137	5	5	1	5	3	4	5	1	5	2	2	3	5	5	3	4
138	5	5	4	5	2	4	5	5	5	3	4	4	4	5	5	5
139	1	5	2	1	3	1	1	1	2	3	3	2	4	3	3	2
140	2	1	1	1	2	3	3	4	5	2	2	3	3	2	2	3
141	3	4	3	5	2	3	4	2	4	3	3	2	2	4	4	4
142	5	5	5	4	3	4	5	3	4	2	3	3	4	5	4	5

143	3	3	1	3	2	4	5	2	5	2	3	4	3	4	3	3
144	5	5	4	2	2	4	4	1	3	3	4	3	4	4	3	3
145	1	5	1	5	5	3	3	1	5	2	2	3	4	3	3	4
146	2	2	1	2	2	3	5	1	5	4	5	4	2	2	4	4
147	5	5	2	5	3	5	5	5	5	1	3	2	4	3	3	3
148	3	2	1	1	3	3	1	3	4	2	3	4	3	4	4	4
149	5	4	1	2	3	4	5	1	5	4	3	1	5	5	5	5
150	5	5	2	5	2	3	3	1	3	4	3	2	3	4	3	3
151	5	5	1	1	2	2	3	1	2	4	2	1	3	3	4	3
152	4	5	4	1	4	4	5	3	2	2	2	2	2	3	3	5
153	5	5	1	5	3	4	2	1	4	3	4	3	3	3	3	4
154	1	4	1	5	2	1	1	1	3	2	1	1	3	3	3	1
155	4	5	2	5	2	3	3	1	5	3	3	3	4	3	2	2
156	1	5	1	5	1	5	5	2	4	1	1	2	5	5	4	4
157	5	4	1	4	3	3	3	1	4	3	4	5	5	4	3	4
158	1	5	4	5	2	5	2	2	5	3	5	4	4	2	4	4
159	4	2	2	5	2	4	3	1	4	2	3	2	4	3	2	3
160	1	1	1	5	2	3	5	1	3	2	2	3	3	5	4	3
161	3	5	1	5	3	4	3	2	5	3	5	5	4	4	4	4
162	4	3	3	2	4	5	5	2	4	4	5	5	5	5	4	4
163	1	5	1	5	3	4	5	1	2	2	3	3	3	5	3	3
164	2	2	2	2	2	2	2	2	2	4	2	2	3	3	3	3
165	5	5	5	5	1	4	5	4	5	4	5	5	5	5	5	5
166	1	1	1	1	2	3	5	3	4	3	3	3	3	4	3	4
167	5	5	5	1	1	4	2	1	3	4	2	2	2	3	2	4
168	1	2	1	2	2	3	5	2	5	3	2	4	4	5	2	2
169	5	5	2	5	2	4	5	1	4	2	2	3	2	4	4	5
170	3	3	1	5	3	3	3	1	2	5	3	2	2	4	3	4
171	4	5	2	5	2	4	3	2	3	3	3	2	4	4	2	1
172	2	1	1	1	3	3	5	1	5	2	1	2	4	3	3	3
173	4	5	4	4	3	5	3	2	3	3	2	3	4	3	3	3
174	1	1	1	1	3	4	4	2	5	1	4	3	5	4	3	3
175	1	1	1	1	3	4	4	2	4	2	4	4	5	4	3	3
176	2	3	3	5	3	5	5	2	4	3	4	1	5	3	3	4
177	5	4	2	5	3	3	5	2	3	2	4	3	5	2	3	3
178	5	5	5	5	4	4	5	1	4	2	3	3	5	5	5	5
179	5	5	1	5	2	3	5	1	3	2	2	3	2	2	3	2
180	5	5	5	3	3	3	3	2	5	4	4	5	5	5	5	5
181	5	5	2	4	2	2	2	1	3	3	3	3	3	4	2	2
182	1	5	1	5	3	4	3	2	3	5	2	2	5	4	3	3
183	5	5	4	5	2	5	5	1	4	1	2	1	2	3	2	4
184	5	3	3	2	2	2	2	2	3	2	3	3	4	4	3	4