SCIS 2018 2018 Symposium on
Cryptography and Information Security
Niigata, Japan, Jan. 23 - 26, 2018
The Institute of Electronics,
Information and Communication Engineers

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
Impact Assessment of password reset PRMitM attack with two-factor authentication

笹 航太 * 菊池 浩明 †
Kota Sasa Hiroaki Kikuchi

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．

キーワード PRMitM攻撃, 二要素認証, 人間要素

1 はじめに

Yansの報告[1]によると，65%のユーザにパスワードを忘れる傾向がある．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いる．とりわけ，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2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に通知する．

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[2], この手法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り，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，その間にターゲット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，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．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．SMSを読まない原因は明らかになっていない．

そこで本研究では，PRMitM攻撃を模した実験を行い，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．加えて，国内200社の主要なサイトを対象に，用いられているリセットを伝えるSMSメッセージに問題がないか調査を行う．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．

2 PRMitM攻撃

2.1 2要素認証

2要素認証は，単一のパスワード認証に，生体認証やデバイス認証などの他の認証要素を組み合わせた認証方式である．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が必要であり，これらが「本人が知っていること」である．これに，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，このパスワード生成器が「本人が持っているもの」であり，2つの要素を利用して認証する．本研究では，パスワードをリセットするワンタイムパスワードの代わりに，SMSを用いた2要素認証に重点を置く.「本人が持っているもの」は

* 明治大学大学院先端数理科学研究科, 〒164-8525 東京都中野区中野4丁目2−1, Graduate School of Advanced Mathematical Sciences, Meiji University, 4-21-1 Nakano, Nakano-ku, Tokyo, 164-8525, Japan.
† 明治大学総合数理学部, School of Interdisciplinary Mathematical Sciences, Meiji University, 4-21-1 Nakano, Nakano-ku, Tokyo, 164-8525, Japan.

表 1: リセットコードを伝える脆弱な SMS の例 [2]

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

SMS を受信する携帯電話である．

2.2 PRMitM 攻撃を受ける条件

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 [2]．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 1 に示す．ユーザ A はターゲットサイト C にアカウント A を所有している．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．ユーザ A は中間者サイト B に登録するため，ユーザ情報として電話番号を入力する．中間者はこの電話番号を利用して，A になりすまし，C に対してパスワードリセットを要求する．中間者サイト B は登録の手順として，ユーザ A に対して SMS で送られる確認コードの入力を求める．ユーザ A の携帯電話に C からの SMS が送られてくるがユーザ A は中間者サイト B の登録手順である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 のアカウントを乗っ取られてしまう．

Gelernter らは PRMitM 攻撃を受けてしまう条件として，次の 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 1 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がどこから送られてきたのか判断できない．(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．(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．

Gelernter らは 536 人の被験者による実験で，PRMitM 攻撃の効果を明らかにした．SMS によって送られたコードを入力する際に，ユーザの 90.5%は文章を読まずコードだけを見ること，企業名に気付いても，その企業と連携したログイン機能だと思い入力してしまうこと，警告

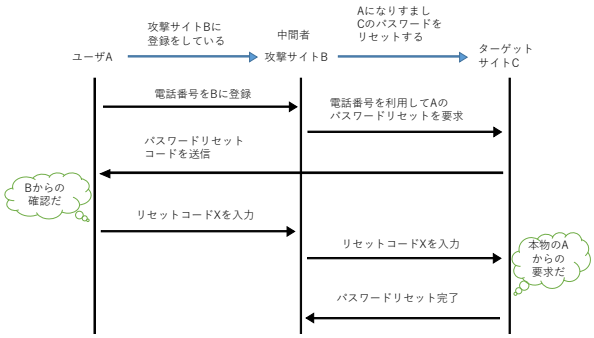

図 1: PRMitM 攻撃の流れ

をしても 79.5%のユーザがコードを入力してしまうことを示した．

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，ユーザは受け取った SMS のコードがパスワードリセットのためであることに気づきやすくなり，攻撃を防ぐ可能性が高まる．また，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 攻撃をするには，ユーザに送られた URL を入力させなくてはならず，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 SeBIS

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 [3]．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．実際の質問は表 10 に示す．

3 潜在的リスクの指摘

3.1 人間要素

PRMitM 攻撃は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，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セキュリティ知識の不足，SMS の文章をよく読まない注意深さの欠如があげられる．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 SMS のメッセージの外観種類による攻撃成功率の検討が行われていなかった．特に SMS の文章を読むかどうかは，ユーザの知識によって大きく異なるだろう．よって本研究では，ユーザのセキュリティ

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

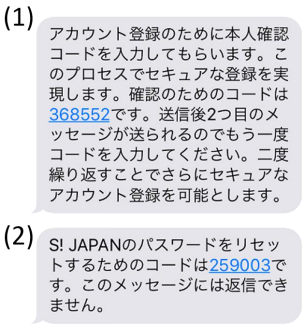

図 2: 長文攻撃の流れ

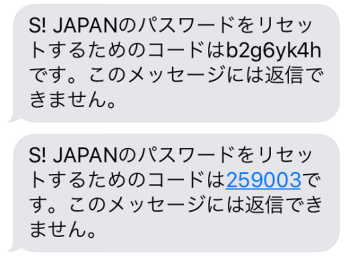

図 3: 数字のみと英数字の SMS

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 長文攻撃

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．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 回目の入力は文章を読まずにコードだけを見て入力してしまい，アカウント A を乗っ取られてしまう．図 2 の SMS(1), (2) を考えよう．ユーザ A は中間者サイト B に登録するため，B から (1) の長文を送った後でターゲットサイト C から (2) の短文を送る．A は (1) で慣れているので，(2) の SMS に C(“S! Japan”) と明記されていることに気付かないでコードを 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．

3.3 数字の認証コード

iPhone と一部の Android 端末では，連続した数字を電話番号だと認識してリンクを張る．図 3 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リンクの強調がされないため，リセットコードにのみ注目されることを防ぎ，攻撃を受けにくいと考える．

図 4: OpenID を用いたログインの例 (ニコニコ動画ログイン)

3.4 ID 連携

OpenID[4] 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．ニコニコ動画に使われているバーナーを図 4 に示す．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，C を ID Provider とした ID 連携のふりをして 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，C のアカウントを乗っ取られてしまう．

3.5 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

- 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．
- 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．
- 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．

それゆえ，リセットコードの代わりにするべきではないと我々は考える．

4 国内主要 web サイトの調査

4.1 目的

国内主要サイトの PRMitM 攻撃を受けてしまう脆弱性と対応が必要なウェブサイトを明らかにすること．

4.2 方法

2017 年 2017 年 8 月 18 日〜12 月 13 日の間に Alexa Japan[5] の top200 のウェブサイトに対して，アカウントを登録し，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採用されているか，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．

表 2: top200web サイト統計情報

アカウント登録なし	27				
有	173	SMS なし	145		
		有	28	警告なし	15	Yahoo JAPAN
				警告有	12	Twitter
				URL 有	1	Instagram
計	200				

表 3: 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。

4.3 結果

調査結果を表 2 に示す．[2] 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 17 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 3 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しか，アカウントを持てない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．

5 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，リセット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，ユーザがどのような要因でパスワードリセットコードを入力してしまうかを明らかにする．

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 [6] を用いて，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 4 に示す．SMS の送信には，Twilio[7] のプログラマブル SMS を用いた．被験者は 4 種類の架空のウェブサイトに，名前，パスワード，電話番号を入力して登録を完了する．SMS でなんらかのコードが送られてくるので，入力かキャンセルをする．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．

図 5: 実験で用いる登録画面 (1)

表 4: 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

被験者は表 6 の 4 つの架空のサイト全てに順に次の登録作業を行う．(1) 登録のみ．この入力画面を図 5 に示す．(2) 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．(3) 被験者を 5 グループに分け，それぞれに表 7 で定めた異なる 5 種類のタイプの SMS を（1）で登録したウェブサイトから送信する．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．(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，表 5 に示すアンケートに答える．全ての SMS に送信元企業名は記載されている．全ての登録が終了した後，SeBIS のアンケートを行う．

表 5: 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 6: 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
操作	終了	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

表 7: 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

本実験では，type0 をベースライン条件として設定した．もし type 1 +3 と type 2+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 type 1 +2 と type 3+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，基本情報フォームの入力からリセットコード入力かキャンセルにかかる時間を測定した．

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 [7] 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．

5.4 結果

実験の結果を表 8 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．

表 8: 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 9: 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

表 8 の SMS の条件が被害率に及ぼす影響を明確にするため，各検査項目の条件についての表 11 の 4 つの分割表を求めた．

キャンセルの理由と結果を表 9 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．

入力とキャンセルにかかった時間の分布を図 6 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 (3) の攻撃に対して入力した人とキャンセルした人の各々の結果を表 10 に示す．SeBIS の合計点数を図 7 に示す.[2]

6 評価

6.1 web サイト調査

4 章の調査結果では，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

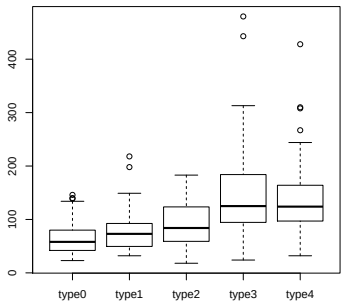

図 6: 各タイプの回答時間の分布

[2] 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 10: 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

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．

6.2 人間要素の効果

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 11 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．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．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，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．

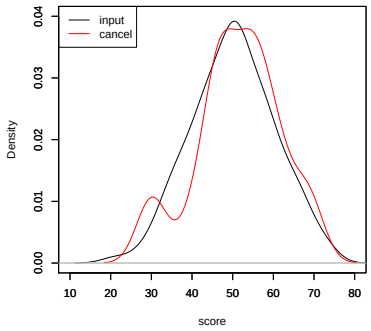

図 7: 入力とキャンセルした被験者のセキュリティ志向度と被害率の SeBIS 点数分布

表 11: 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 4	http	164	20	89.1	24.2937	8.27e-07***
入力 2	https	124	60	67.3		

6.2.1 入力とキャンセルの差

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 12 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．

6.2.2 SeBIS セキュリティ志向度と被害率

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．被験者全体の平均得点が 50.3 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 13 に示す．また，被験者の属性についての SeBIS の差を表 15 に示す．

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 つのウェブサイト登録についての

表 12: 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

使用感 $x_{1,1}$, $x_{2,1}$, $x_{3,1}$　と安心度 $x_{2,1}$, $x_{2,2}$, $x_{3,2}$, 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．結果を有意な p 値になったものに絞って表 14 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，

$$e^{2.45} = 11.59$$

であり，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を示している．これは，頻繁にパスワードを変更する人ほど，コードの入力に対して警戒が薄いことが原因として考えられる．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」であり，設定する人は $e^{-5.08}$ 倍 $= 0.56$ に被害を下げる．リセット被害を受ける被験者は必要最低限のパスワード文字数を設定する傾向にあることが明らかになった．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」であり，同様に，$e^{-0.98} = 0.37$ に被害を下げる．リセット被害を受ける被験者はリンクの先を確認せずにクリックしてしまう傾向があることが明らかになった．

表 13: 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 14: ロジスティック回帰分析 (一部)

	Estimateβ	Std. Error	z value	Pr(>|z|)
(Intercept) x_0	-1.68	4.64	-0.36	0.717 *
x_1	-1.25	163	-077	0.443
x_2	-3.31	1.60	-2.07	0.038 *
x_3	-4.46	1.93	-2.31	0.021 *
x_4	-4.46	1.93	-2.31	0.026 *
$x_{1,1}$	1.21	0.46	2.54	0.011 *
$x_{1,2}$	0.88	0.36	2.47	0.013 *
$x_{2,2}$	-1.35	0.45	-2.99	0.002***
$x_{3,1}$	-0.65	0.30	-2.18	0.029 *
$x_{3,2}$	1.63	0.36	4.54	5.61e-06 ***
x_{q5}	2.45	0.71	3.44	0.00058 ***
x_{q8}	-0.58	0.29	-1.97	0.048 *
x_{q10}	-0.98	0.46	-2.10	0.0362 *

6.2.3　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，type 別の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．これは，被験者が送られてきたコードを入力する際に，SMS の内容を数秒しか読んでいないためだと考えられる．

6.3　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，type0 と type1 の警告の有無に対するオッズ比は

$$\frac{35}{2} \Big/ \frac{30}{8} = 4.67$$

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 [8]．表 12 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．

表 15: 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

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．

7 おわりに

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 PRMitM 攻撃の潜在的な脅威の評価を行った．日本のアクセス数上位のウェブサイトで 17 社が SMS を用いたパスワードリセットを行っており，そのうち 12 社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．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] 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.

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

[3] 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).

[4] OpenID Japan，https://www.openid.or.jp/

[5] 日本のアクセス数上位サイト by アレクサ，http://akimoto.jp/japan/

[6] クラウドワークス，https://crowdworks.jp/

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

[8] paymentnavi，http://www.paymentnavi.com/paymentnews/61930.html

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。