SMS通知機能を悪用した新たなパスワードリセット脆弱性の脅威評価

柴山 りな[1]　菊池 浩明[1]

概要：簡易かつ安全な多要素認証として広く用いられている SMS(Short Message Service) を用いた認証を悪用したパスワードリセット手法 PRMitM 攻撃が，2017 年 Gelernter らによって提案された．攻撃者は，ユーザに SMS で送信されたパスワードリセットコードをそれと気が付かせぬまま悪意のある中間者サイトに入力させることによって，アカウントを乗っ取る．本論文では，メッセージ冒頭を短く通知をする機能が，PRMitM 攻撃を増長させる可能性があることを主張する．送信されたコードを入力する際，コード以下の注意書や発信者名を読まないため被害につながる恐れがある．そこで，本研究ではユーザ実験を行い，「警告の有無」，「冒頭に警告を記載するかどうか」，「警告の言語」の各要因が攻撃に対する被害率に与える影響を明らかにする．

Impact Accessment of New Password Reset Vulnerablity exploiting SMS Notification

Rina Shibayama[1]　Hiroaki Kikuchi[1]

1. はじめに

不正アクセスや情報漏洩などを防ぐために，2 つ以上の認証方式を組み合わせることでセキュリティの強度を上げる多要素認証が近年推奨されている．ID・パスワードなどと併せて指紋や顔・IC カードなどが使用される．中でも，SMS(Short Message Service) は携帯電話番号へ短文のメッセージを送信する仕組みであり，多要素認証の代表的な手段として，ユーザの携帯電話へワンタイムパスワードを送信することに広く使われている．

しかし，2017 年に SMS 認証を悪用してパスワードを初期化する手法 PRMitM(Passward Reset Man in the Middle) 攻撃が Gelernter らによって提案されている [1]．PRMitM 攻撃は中間者攻撃の 1 種であり，アカウント登録とパスワードリセットの手順が似ていることを利用し，ユーザに勘違いさせアカウントのパスワードを初期化するものである．Gelenter らは，SMS にパスワードリセットであることの警告とサービス名を明記することで，PRMitM 攻撃を防止できると述べている．

しかしながら我々は，近年の機能拡張が著しい SMS に脆弱性があることに気が付いた．それは SMS の冒頭の一部を表示する通知機能である．なぜならば，通知しか見ないで認証コードを入力するユーザには，これらの警告やサービス名が秘匿されてしまうためである．そこで，本稿っではこの仮説を検証するためクラウドソーシングを用いたユーザ実験を行った．

通知による影響を受けやすいように，警告を SMS の上部と下部に記述し，各ケースでの PRMitM 攻撃の被害率を測定する．安全に実験を実施するため，SMS は本物を用いたが，パスワードリセット対象となるサイトは疑似的なサイトを用いた．また，十分な ICT スキルやセキュリティ知識がこの攻撃を防止するのに有効であると予想し，被験者のスキル度合いをアンケートによって評価した．

本稿では，以上の実験結果を示し，被害を広げる要因について考察を与える．また，PRMitM 攻撃を受けないようにする対策について考える．

2. 多要素認証への中間者攻撃の先行研究

2.1 PRMitM 攻撃

PRMitM 攻撃の一連の流れを図 1 に示す．ユーザ U がアカウントを保持する攻撃対象サイト A，攻撃者が用意する中間者サイト B がある．ユーザは中間者サイト B に新規登録するため名前・メールアドレス・電話番号などの情報を入力する．B はこれらの情報を用い，A へユーザのパスワードの初期化を要求する．要求がユーザからのものであることを確認するため，A からユーザ U へパスワードリセットコードが SMS で送信されるが，ユーザ U は B の登

[1] 明治大学 総合数理学部 先端メディアサイエンス学科
Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University

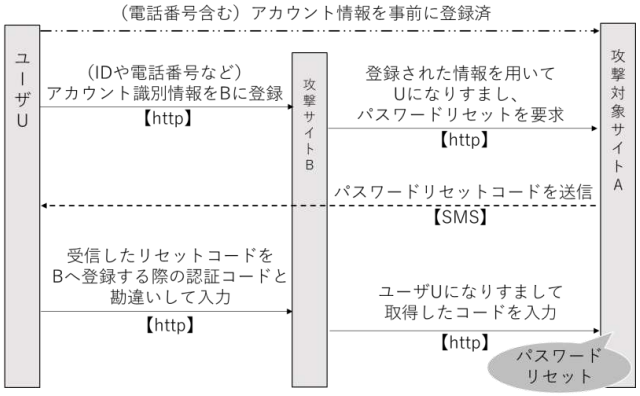

図 1　PRMitM 攻撃の流れ

録時の認証コードであると勘違いして，リセットコードを *B* に入力してしまう.，こうして *B* は *A* に登録されたパスワードをリセットして，*U* になりすます．

Gelernter らによるとパスワードリセットであることの警告とサービス名を明記することが PRMitM 攻撃に対する基本的な対策である [1]．また，彼らは，リセットコードの替わりに送信元を明記した URL を送ることで，PRMitM 攻撃を受けることがないと主張している．

2.2　笹らによる被験者研究

笹らは，PRMitM 攻撃に対して新たに英数字のリセットコードと長文攻撃を提案し，被験者実験を行った [2, 3, 5]．数字の代わりに英数字を使用すると，コード部分のみが青字になって強調されず，被害率が下げる効果があると主張している．また，一度長文の確認コードを送信し入力させ，2 度目にパスワードリセットコードを入力させる「長文攻撃」では，1 度コードを入力した慣れから被害率が上がるという脅威も提案している．ユーザ実験を行った結果，長文と短文の間，数字と英数字の間の被害率に有意差は認められなかった．

さらに，笹らは PRMitM 攻撃を受けやすい人の人間的特質を SeBIS やアンケートの実施から明らかにした．主要な結果には，50 代以上やパスワードをよく変更する人は被害を受けやすいという傾向が含まれている．また，Gelenter らの提案する URL を埋め込んだ SMS によるパスワードリセットは，普及すると新たなフィッシングの標的になると主張した．

2.3　SeBIS

SeBIS(Security Behavior Intentions Scale) は 2015 年 Serge Egelman らによって開発されたセキュリティ意識の指標である [4].「デバイスの安全確保」,「パスワードの管理」,「Web 使用時の積極的なセキュリティ意識」,「アップデート」の質問に対し，5 段階のリッカート尺度で回答をしてもらい，被験者のセキュリティに対する意識を定量化する．

図 2　メッセージ開封の例 (iPhone)

本稿では，全 16 問を先行研究 [2] を参考に和訳して使用した．

3.　SMS ベース多要素認証の新たな脆弱性

3.1　概要

本来，コードを確認するためには，図 2 のようにメッセージを**開封**することが一般的である．開封すれば全文に目を通すことになる．しかし，図 3 の受信メッセージ**一覧**画面や，図 4 のような**通知**機能では，冒頭 1〜2 行のみが送信元電話番号とともに表示される．もし冒頭にコードを，その下に警告とサービス名を記述する場合，利用者はコード以下を読まないため被害を増長させる．

これらの SMS の開示方法を次のように呼ぶ．

開封　メッセージ用のアプリケーションより SMS の全文を閲覧する方法 (図 2)

一覧　開封と同様のアプリケーションだが，一覧表示された SMS の文頭数行のみの簡略化された部分のみを確認する方法 (図 3)

通知　他のアプリケーション利用中やホーム画面で SMS の受信を通知する短い要約のみを確認する方法 (図 4) OS の違いによって要約の方法は変わるが，メッセージの一部のみしか表示されない．

従って，一覧や通知のいずれも，SMS の一部，多くの場合文頭 2 行のみしか表示されない．

登録を PC で行った場合，スマートフォンのロック画面に認証コードが通知される．図 5 にあるように，iPhone では SMS 本文冒頭または全体が表示されるのに対して，Android では初期設定では本文は表示されない．

また，現在 iPhone の機能に，SMS に送られてきた認証コードを自動で認識し，ワンタッチで入力できる図 6 のような**自動入力**機能がある．キーパッドに表示されたコードをタッチするだけで，SMS 本文を確認する機会すらなく，サービス名や警告を確認せずに入力することができる．以上のように，利便性を向上するために強化された機能の多くが PRMitM 攻撃の被害を増長させる要因になり得る．

3.2　通知を悪用した中間者攻撃

しかしながら，本脆弱性が即ユーザアカウントの乗っ取りを招くわけではない．本脆弱性は機種や登録媒体によって振る舞いが異なり，各自のロック画面や通知の設定によっても異なる．注意深いユーザならば攻撃に気が付くか

図 3　受信メッセージ一覧の例 (iPhone)

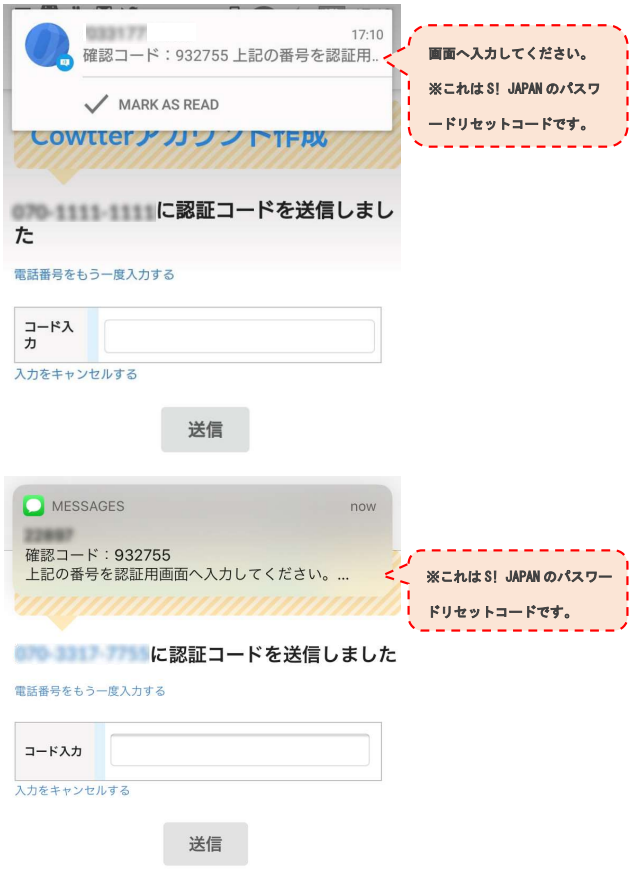

図 4　通知の例（Android(上)，iPhone(下)）

もしれない．1 行か 2 行かの違いや，全文をロック画面で確認するかメッセージを開封して確認するかといった機種間の細かい違いによって，PRMitM 攻撃の被害に影響を与えるかもしれない．

十分なセキュリティ意識があれば，SMS 本文の確認・コードの入力を適切に丁寧に行い，この攻撃を受けないことも予想される．逆に年配者などの，スマートフォンを使いこなせない人は，より被害を受けやすいだろう．

そこで本研究では，被験者 81 人を用いたオンラインによるユーザ実験を行い，通知や自動入力などの SMS の機能やユーザのセキュリティ意識が PRMitM 攻撃の被害に及ぼす影響を明らかにすることを試みる．

図 5　ロック画面での SMS メッセージ受信通知の例（Android(左)，iPhone(右)）

図 6　自動入力の例 (iPhone)

表 1　実験で行われるサイト登録の概要

	登録サイト名	実施目的	認証コード	正しい行動
1	S! JAPAN	登録練習	なし	-
2	Cowtter	コード入力練習	Cowtter 認証コード	入力
3	Majebook	被害要因の調査	S! JAPAN パスワードリセットコード	キャンセル

4.　ユーザ実験

4.1　目的

本実験は，受信したパスワードリセットコードをその用途に気づかぬまま中間者サイトに入力してしまう要因とともに被害者の特性を調査することを目的とする．

4.2　方法

クラウドソーシングサービス「クラウドワークス」*と「ランサーズ」†を利用して被験者 81 人 (男性 44 人，女性 37 人) を用いた SMS 多要素認証による架空ウェブサイトへの登録実験を行う．実験に使用したウェブサイトの例を 7 に示す．サイト登録は合計 3 回行われ，その都度，「登録フォームは使いやすかったか」，「セキュリティに関して安心できると感じたか」などの質問に回答する．3 回の登録

図 7　実験に使用した 3 サイトの登録画面

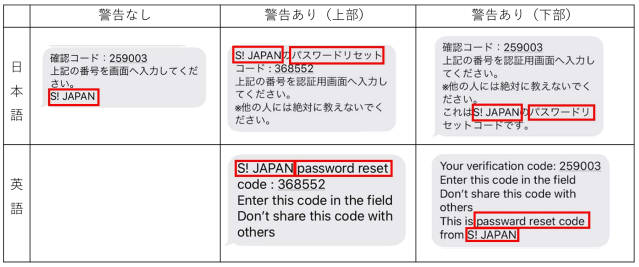

図 8　5 つの SMS 本文

終了後にセキュリティ意識を測る SeBIS(日本語訳) [4] と，コンピュータスキルを測る 3 つの問いに回答する．

3 回の登録の概要を表 1 に示す．1 回目は情報の登録のみ，2 回目は情報の登録と SMS 認証を実施する．実験サイトから被験者への SMS メッセージ送信には「Twilio」‡ を用いた．3 回目では 1 回目のサイトの登録サイトへの PRMitM 攻撃を実施する．ここでは，情報を登録したのちに 1 回目の S!JAPAN のサイトからパスワードリセットコードが送信される．被験者には，もしも登録に疑わしい点があればキャンセルすること事前に指示しておく．ここで図 8 に定められる 5 つの被験者グループに異なる条件の SMS メッセージを送り，被害要因を調査する．

4.3　被害者の定義

3 回目の登録時，本来ならば SMS 本文を読み，サイト名の相違やパスワードリセットコードであることに矛盾を感じるはずである．被害を受けないためには，選択肢として与えられている「入力をキャンセルする」を選ぶべきである．しかし，SMS 本文を読まないと，このコードを登録時の認証コードと勘違いして入力してしまう．

Majebook の新規登録の手順の途中であるにも関わらず，S! JAPAN のリセットコードを入力してしまった被験者を攻撃の**被害者**とみなす．その条件の，被害者が占める割合を**被害率**とする．例えば，type0 の SMS を受け取った被験者は 19 人，そのうちコードを入力してしまった人は 14 人なので被害率は $R = 14/19 \cdot 100$ と計算される．

*クラウドワークス, https://crowdworks.jp/
†ランサーズ, https://www.lancers.jp/
‡Twilio, https://twilio.kddi-web.com/

表 2　各サイトの使用感と安心感の平均点と標準偏差

サイト名	使いやすいか		安心できるか	
	平均	SD	平均	SD
S! JAPAN	4.07	1.70	5.78	1.12
Cowtter	5.91	1.08	4.95	1.61
Majebook	5.72	1.33	4.22	1.94

表 3　SMS ごとのリセット被害率

type	SMS の特徴		入力	全体	被害率
	警告	言語	人数	人数	[%]
0	なし	日本語	14	19	73.7
1	あり（下部）	日本語	15	19	78.9
2	あり（下部）	英語	16	20	80.0
3	あり（上部）	日本語	0	7	0.0
4	あり（上部）	英語	10	16	67.9

表 4　デバイス種類ごとの被害率と検定結果

デバイス	入力	全体	被害率	χ	p 値
iPhone	21	30	70.0	3.11	0.37
Android	23	31	74.2		
PC	11	20	55.0		

表 5　デバイス種類ごとの被害率と検定結果

デバイス	入力	全体	被害率	χ	p 値
iPhone	5	8	62.5	0.75	0.94
Android	4	9	44.4		

表 6　入力取止の理由

理由	人数
メッセージの内容がよくわからなかったから	7
S! JAPAN と書いてあったから	11
パスワードリセットと書いてあったから	6
信用できないサイトだから	1
メッセージが英文だったから	1

表 7　電話番号入力への抵抗感の平均点と標準偏差
(1:とても抵抗がある 7:完全に抵抗はない)

	入力	取止	SD
良く知られたサイト	4.02	3.73	1.79
初めて見つけたサイト	2.65	2.27	1.52

表 8　入力・確認方法ごとのリセット被害率と検定結果

	方法	入力	全体	被害率	χ	p 値
入力	手入力	44	64	78.8	1.70	0.428
	コピペ	7	10	70.0		
	自動入力	4	6	66.7		
確認	開封	27	40	67.5	1.74	0.418
	一覧	6	11	54.5		
	通知	22	29	75.9		

4.4　結果

表 9　属性ごとの被害率と検定結果

	分類	入力	全体	被害率	χ	p 値
性別	男性	32	44	72.7	1.03	0.319
	女性	23	37	62.2		
年齢	20 未満	0	1	0.0	13.26	0.021*
	20 代	14	17	82.4		
	30 代	14	28	50.0		
	40 代	15	22	68.2		
	50 代	8	9	88.9		
	60 以上	4	4	100.0		

表 10　スキルを測る 3 つの問いと平均点と標準偏差

	質問	入力	取止	SD
1	自分で OS をインストールしたことがありますか	1.51	1.50	0.61
2	自分でネットワークを構築したことがありますか	1.18	1.23	0.40
3	自分でウェブページを作ったことがありますか	1.24	1.23	0.42

実験で送信した SMS の特徴の概要と被害率を表 3 に示す．type3 と 4 が type0，2，3 と比べて被験者数が少ないのは，同じ人数の被験者を type0 5 に振り分けたが，SMS が原因不明のエラーによって送信されなかった事例が多かったためである．

デバイスごとの被害率と独立性の検定の結果を表 4 に示す．デバイスのユーザーエージェントを元に分類した．アンケートでも機種を回答してもらったが，ユーザーエージェントと一致していない被験者が 2 名見受けられた．自分の機種を正しく把握していない場合があると判断して，ユーザーエージェントを採用した．また，PC で登録した人の使用したスマートフォンの機種ごとの被害率と検定結果を表 5 に示す．SMS の受信に使用した機種は，アンケートの回答結果をもとに集計した．

登録した架空の 3 サイトに対する使用感と安心感の平均点とそれぞれの標準偏差 (SD) を表 2 に示す（1：とても安心できない／とても使いにくい，7：とても安心できる／とても使いやすい）．標準偏差はすべての項目で 2 以下と小さいが，サイトごとに差は見られなかった．

被害を受けなかった人が，入力の取止をした理由の人数を表 6 に示す．取止の理由についてはサービス名の相違が最も多かった．

良く知られたサービス／初めて見つけたサービスでの電話番号の入力に抵抗があるか回答してもらった結果を表 7 に示す．

コードの確認及び入力方法別の被害率を表 8 に示す．方法の特定はアンケートによる自己申告である．最も一般的なコードの入力方法は手入力，コピー＆ペースト，自動入力のうち手入力で，81 人中 64 人であった．確認方法は開封（メッセージ全文を表示），一覧（受信 SMS 一覧画面），通知（画面上部のバナー通知），その他から選択回答してもらった．主な確認方法は，「開封」が 81 人中 40 人と「通知」が 30 人に分かれた．入力方法・確認方法ともに「その他」が 1 人であった．

表 11　SeBIS 質問文とロジスティック回帰分析

	質問	e^{β}	p 値
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	1.177	0.842
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	0.657	0.611
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	0.140	0.024*
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	0.550	0.482
5	必要があるときしかパスワードを変更しない	0.540	0.397
6	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	-	-
7	アカウントごとに違うパスワードを使っている	1.536	0.540
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）	0.714	0.676
9	必要がない場合は，パスワードに特殊文字を含めない	0.509	0.363
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	0.664	0.609
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	1.735	0.375
12	安全に送信されることを最初に確認せずに，ウェブサイトに情報を送信する	1.804	0.429
13	リンクをクリックする前にマウスカーソルをリンクに乗せ，訪れる URL を確認する	1.406	0.614
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	0.659	0.576
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	1.149	0.840
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	1.233	0.787
17	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	-	-
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	0.409	0.304
	合計点	0.083	0.032*

性別・年代ごとの被害率を表 9 に示す．年代別に見ると 20 代と 50 代以降では被害率が 8 割を超えていた．

スキルを測る 3 つの問いと平均点，標準偏差を表 10 に

表 12　SMS ごとのリセット被害率と検定結果

type	特徴	入力	全体	被害率	χ	p 値
0	警告無	15	20	75.0	11.81	0.001***
3	警告有	0	7	0.0		
3	日本語	0	7	0.0	7.74	0.005***
4	英語	10	16	62.5		
3+4	上部	10	23	43.5	8.37	0.004***
1+2	下部	31	39	79.5		

表 13　SeBIS とスキルの合計点の統計量

	平均値		SD	t 値	p 値
	入力	取止			
SeBIS	49.6	48.8	12.0	0.132	0.896
スキル	3.93	3.96	1.01	-0.266	0.792

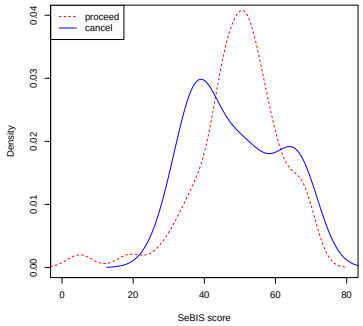

図 9　入力／キャンセル別の SeBIS 点数分布図

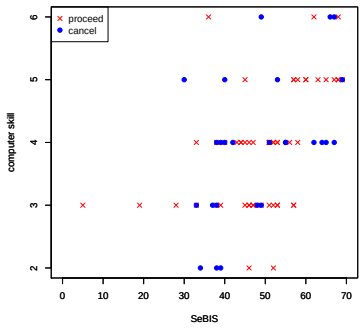

図 10　SeBIS とコンピュータスキルと PRMitM 攻撃被害の散布図

示す．アンケートは「ある」(2 点)，「ない」(1 点)，「対象物が何かわからない」(0 点) から選択する形式である．

SeBIS の質問文を表 11 に示す．回答は 5 段階と回答しないの 6 つから選択する方式である（0:回答しない 1:まったくそうでない 5：いつもそうしている）．

4.5　分析

SMS の特徴ごとの独立性の検定を自由度 1 のカイ 2 乗検定で行った結果を表 12 に示す．$*$ を有意水準 10 % ($p < 0.1$)，$***$ を有意水準 1 % ($p < 0.01$) とする．警告あり／なし，日本語／英語，警告の位置が上部／下部でいずれも有意差 ($p = 0.001$，$p = 0.005$，$p = 0.04$) が認められた．警告ありに type3 のみを採用したのは，type1 で下部に警告した場合，警告自体が読まれておらず，警告なしの場合との差が表れないと判断したためである．同様の理由で，日本語／英語で Type1+3，2+4 とせず Type3 と 4 のみを採用した．

表 14　ロジスティック回帰分析

	Estimateβ	Std. Error	z value	$Pr(>\|z\|)$
(Intercept)	8.082	5.521	1.464	0.143
x_2	-6.673	2.440	-2.734	0.006***
x_3	-2.244	1.444	-1.554	0.120
x_4	-4.776	1.674	-2.853	0.004***
$x_{1,1}$	-1.381	0.714	-1.934	0.053*
$x_{1,2}$	0.617	0.394	1.569	0.117
$x_{2,1}$	2.372	0.930	2.550	0.011*
$x_{2,2}$	-1.303	0.445	-2.931	0.003***
$x_{3,1}$	-1.294	0.508	-2.546	0.011*
$x_{3,2}$	0.792	0.286	2.766	0.006***
x_{q0}	0.993	0.504	1.971	0.049*
x_{q1}	-2.283	1.254	-1.821	0.069*
x_{q2}	-1.604	0.785	-2.042	0.041*
x_{q3}	0.918	0.686	1.338	0.181
x_{q4}	-0.309	0.561	-0.551	0.582
x_{q5}	-0.344	0.356	-0.968	0.333
x_{q6}	0.643	0.396	1.626	0.104
x_{q7}	3.583	1.773	2.021	0.043*
x_{s1}	-0.043	0.058	-0.749	0.454
x_{s2}	0.302	0.576	0.525	0.600

コードの確認及び入力方法別の独立性の自由度 2 のカイ 2 乗検定結果を表 8 に示す．入力方法・確認方法による有意差はいずれにも認められなかった ($p = 0.428$，$p = 0.418$)．

性別・年代ごとの被害率と独立性の検定の結果を表 9 に示す．独立性の検定の結果，性別では有意差はなかったが ($p = 0.319$)，年代では有意水準 5 % での有意差が認められた ($p = 0.021$)．

デバイスごとの被害率を独立性の自由度 2 のカイ 2 乗検定の結果，表 4 より，iPhone，Android，PC 間で統計的な有意差は見られなかった ($p = 0.374$)．

セキュリティ意識 (SeBIS) とコンピュータスキルを，それぞれ 0-80 点，0-6 点で評価した．SeBIS とスキル値の散布図で図 10 に示す．SeBIS とスキルの合計点の統計量と Weltch の検定結果を表 13 に示す．検定の結果，SeBIS の合計点，スキルの合計点ともに入力した被験者とキャンセルした被験者の平均に有意差は見られなかった．

また，SeBIS 合計点の点数分布を図 9 に示す．入力とキャンセルの間で特筆すべき差は見受けられなかった．

SeBIS の各質問と合計点を説明変数，入力／キャンセルを目的変数としてロジスティック回帰

$$\log \frac{p}{1-p} = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_{19} x_{19}$$

を行った結果を表 11 に示す．各質問の回答を「はい」「いいえ」の 2 つに分け，合計点は 50 点以下と 51 点以上に分けて分析を行った．結果，SeBIS の合計点が 51 点以上の 50 点以下に対する調整済オッズ比 OR は

$$\frac{\text{合計点高い人の被害率/合計点高い人のキャンセル率}}{\text{合計点低い人の被害率/合計点低い人のキャンセル率}} = e^{-2.487} = 0.083$$

で有意であった ($p = 0.032$)．50 点以上の被験者は 50 点以下と比べて被害を受けるオッズが 1/10 以下に減少する．また，「コンピュータから離れるとき，手動で画面をロックする」人のそうでない人に対するオッズ比 $OR = e^{-1.964} = 0.140$ で，被害を受ける確率のオッズが 1/7 程度に減少する ($p = 0.024$)．それ以外の項目に有意差は認められなかった．

SMS のタイプ，被験者の属性等多くの要因のうち，攻撃の被害を受ける要因を明らかにするため，ロジスティック回帰を行った．目的変数を入力／キャンセル，説明変数を SMS のタイプ（警告有無 x_1，警告上部 x_2，警告下部 x_3，言語 x_4），3 つのウェブサイトについての使用感 $x_{1,1}$,$x_{2,1}$,$x_{3,1}$，安心感 $x_{1,2}$,$x_{2,2}$,$x_{3,2}$，SeBIS，スキル値の合計点 x_{s1},x_{s2}，アンケートの各質問に対する回答 x_{q1},x_{q2},$x_{q3} \ldots x_{q7}$ とした．結果を表 14 に示す．警告位置が上部と日本語のとき調整オッズ比はそれぞれ $e^{-6.673} = 0.0013$，$e^{-4.776} = 0.0084$ となり，被害を受けにくいことが明らかになった．

5. 考察

5.1 SMS メッセージの特徴

表 12 より，警告あり／なしでは被害率に有意差が認められた．このことから先行研究通り警告とサービス名の明記は有効であるといえる．

警告を上部に記述すると，下部に比べて被害が少なかった．コードより前に認証コードの用途・サービス名を明記することが被害率を下げるために有効だと考えられる．

SMS が英語では 16 人中 10 人がコードを入力したのに対し，日本語では 7 人中入力した者はいなかった．よって，メッセージの内容が即座に理解できない場合，利用者は立ち止まらず入力してしまうと考えられる．ただし，SMS が英語であること自体に違和感を覚え入力しなかったユーザも 1 名見受けられた．コードの用途や警告が明解であるときのみ，その記載が有効になると考える．

5.2 確認・入力方法と被害の関係

表 8 より，実験内での認証コードの入力方法「手入力」，「コピー＆ペースト」，「自動入力」間で有意差は認められなかった．「自動入力」の場合，SMS 本文を確認せずにワンタッチでコードが入力されるため全員が入力すると予想していたが，6 人中 4 人が入力するにとどまった．自動入力際にも，画面上部の通知を併せて確認しているユーザもいると考えられる．

表 8 より，認証コードを「開封」，「一覧」，「通知」で確認することによる有意差は認められなかった．メッセージ下部に警告とサービス名を記載する場合 (Type1 と 2)，一覧や通知ではメッセージの冒頭 2 行のみが表示され，全員が被害を受けると予想していた．しかし被害率は一覧・通知で 54.5 %，75.9 %にとどまった．原因としては，被験者は実際には「開封」して全文を確認していてもアンケートでは「一覧」と回答していることが考えられる．アンケートでの確認方法の選択肢の説明として開封を「メッセージ確認画面を開き，メッセージを開いた」，一覧を「メッセージ確認画面を開いた（開封はしない）」，通知を「画面上部に表示される通知を見た」と文章で表現したため，我々の意図通りに解釈していない可能性があるためである．

5.3 属性

表 9 より，年代間では，20 代・50 代以上で被害率が高かった．20 代では認証コードの入力への慣れ，50 代以上では SMS 認証のコード入力自体に気を取られていることから，SMS 本文への注意が薄く，指示通りに素直にコードを入力している可能性がある．

5.4 デバイス

表 4 より，iPhone，Android，PC 間では，被害率に統計的有意差は見られなかった．図 4 のように SMS メッセージが画面上部に通知される際，iPhone では文頭 2 行が表示されるのに対して，Android では文頭 1 行のみが表示される．デバイス間で違いが見られないことから，通知で表示される情報の量は被害率に影響を与えないと考えられる

また，表 5 より，PC を使用して回答した場合，SMS メッセージ受信に使用した機種が iPhone と Android とで被害率に有意差は見られなかった．ロック画面で SMS を確認する場合，iPhone では全文または冒頭 2 行が表示されるのに対し，Android では本文は表示されない．Android の場合，メッセージを開封する必要があるので，被害率は低くなると予想したが，有意差は見られなかった．

5.5 セキュリティ意識とコンピュータスキル

図 10 より SeBIS とスキルの間にはゆるく正の相関が見られるが，被害（proceed）は広く分布しており，セキュリティ意識・スキルと被害率は独立であると考えられる．また，表 13 の Weltch の検定結果でも，SeBIS とスキル値の合計点の平均に有意差は見られなかった．セキュリティ意識や ICT が高ければ被害を受けにくいと予想していたが，どちらも被害に影響を与えないという結果になった．

6. 対策

PRMitM 攻撃を防止する 3 つの対策を提案する．

1 つ目は自動入力させないことである．確認したところ，SMS 本文で「:」の後にコードがあるとコードと認識されて自動入力機能が使用される．そこで，**パスワードリセットコードに限り，「：」を使わない**フォーマットを用いてコードを送信することを提案する．

2 つ目は送信元のサービス名・コードの使用用途を**メッセージ上部に明記する**ことである．下部に書いた場合，ユーザは読み飛ばしているというよりも目に入ってすらいない可能性があるからである．

3 つ目は，**本文をできるだけ明瞭にする**ことである．ユーザは SMS 本文をほんの数秒しか見ずにコードを入力している．したがって，その短い間に理解できる内容にすることが，メッセージを伝えるのに有効であると考える．

7. おわりに

本論文では，送信されたコードを SMS 文頭に表示する通知機能は，SMS 多要素認証を悪用して，アカウントを乗っ取る脅威があることを示した．ユーザ実験の結果，警告を下部に明記すること・英語であることは攻撃に対する被害を増加させること，警告の有無・記述位置・言語の各要因が攻撃に対する被害率に影響を与えることを示した．一方コードの確認・入力方法は被害率に大きな影響を与えない．本実験では利用率は 1 割以下であったが，今後認証コードの自動入力が普及すると，被害は増える可能性がある．

参考文献

[1] Nethanel Gelernter，Senia Kalma，Bar Magnezi，Hen Porcilan，“The Password Reset MitM Attack”，IEEE Symposium on Security and Privacy (SP)，pp. 251-267，2017.

[2] 笹，菊池，“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”，Symposium on Cryptography and Information Security，2018.

[3] Kota Sasa, Hiroaki Kikuchi，“Impact Assessment of Password Reset PRMitM Attack with Two-Factor Authentication”, IEEE Conference on Dependable and Secure Computing，pp.90-97，2018.

[4] Serge Egelman，Eyal Peer，“Scaling the Security Wall Developing a Security Behavior Intentions Scale (SeBIS)”，ACM Conference on Human Factors in Computing Systems，pp. 2873-2882，2015.

[5] Kota Sasa, Hiroaki Kikuchi，“Impact Assessment of Password Reset PRMitM Attack with Two-Factor Authentication”, Journal of Internet Technology，vol. 20，no. 7，pp. 2297-2306，2019.

付　　録

A.1 実験の中止について

本実験では「クラウドワークス」と「ランサーズ」で被験者を募集して実験を行った際，利用規約違反により実験を中断されている．違反内容の詳細を問い合わせたところ，クラウドワークスはクライアントの電話番号を取得することを目的としない場合でも，電話番号やメールアドレス等の直接連絡先を入力させることは禁止しているとの回答であった．また，ランサーズに問い合わせたところ，「ステルスマーケティングに該当する恐れ」，「ランサーズのサイト上ではないクライアントのやりとり（ランサーズのサイト外でのアンケートおよび SMS の送信）」の 2 点について違反があるということであった．

特にランサーズでは仕事の依頼方式によっては，電話番号の交換が許されるので勘違いしてしまった．本実験では取得した電話番号を SMS を送るという目的のみに使用していて，データとして保存しておらず，連絡をとることはしていない．

個人情報の取り扱いについて利用規約をよく読み，十分理解した上で被験者の募集を行うべきであった．

A.2 アンケート本文

表 A·1　実験に使用したアンケート本文と選択肢

	質問と選択肢
0	あなたの年齢を選択してください
	20 歳未満／ 20〜29 歳／ 30〜39 歳／ 40〜49 歳／ 50〜59 歳／ 60 歳以上
1	性別を選択してください
	男性／女性
2	SMS で受信したコードをどのように入力しましたか
	手入力／コピー＆ペースト／入力候補を選択した／コードを一度も入力していない
3	コードをどのように確認しましたか
	メッセージ確認画面を開き，メッセージを開いた メッセージ確認画面を開いた（開封はしない） 画面上部に表示される通知を見た その他
4	普段コードを確認する際は，どのように確認しますか
	メッセージ確認画面を開き，メッセージを開く メッセージ確認画面を開く（開封はしない） 画面上部に表示される通知を見る コードを確認しない
5	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りますか
	完全に抵抗はない／ (中略) ／とても抵抗がある
6	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りますか
	完全に抵抗はない／ (中略) ／とても抵抗がある
7	実験に使用した携帯電話の種類は何ですか
	iPhone ／ Android ／その他
8	Android と答えた方は端末の種類を教えてください