2ZA-03

多要素認証を悪用したパスワードリセット手法 PRMitM 攻撃の被害を増加させる新たな要因の調査 †

柴山 りな　　菊池 浩明

明治大学 総合数理学部 ‡

1 はじめに

近年，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 は携帯電話番号へ短文のメールを送信する仕組みであり，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，SMS 認証を悪用してパスワードを初期化する手法 **PRMitM** 攻撃が Gelernter らによって提案されている [1]．この攻撃はアカウント登録とパスワードリセットの手順の類似性を利用し，ユーザのパスワードを初期化するものである．

一連の流れを図 1 に示す．ユーザ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，ユーザは *B* の登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．

[1] によると，警告とサービス名の明記が PRMitM 攻撃に対する基本的な対策である．しかしながら我々は，SMS の冒頭の一部を表示する通知機能に脆弱性があると主張する． アプリケーションで受信メッセージ一覧を確認する際も，図 2 のように，冒頭 2 行のみが送信元電話番号とともに表示される．冒頭にコードを記載し，その下に警告とサービス名を記載する場合，利用者はコード以下を読まないため被害を増長させる．また，自動入力機能も，SMS を確認する機会がなく，被害を増長させる要因である．

そこで本研究では，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機能が本攻撃の被害率に及ぼす影響を明らかにすることを試みる．

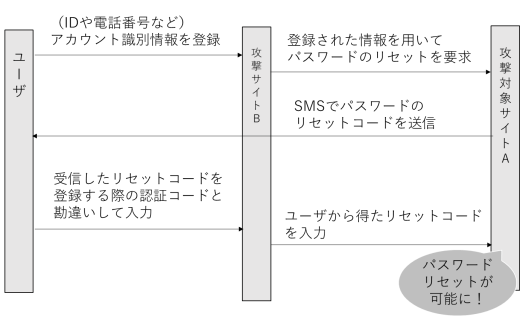

図 1　PRMitM 攻撃の流れ

2 ユーザ実験

2.1 実験方法

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を調査することを目的とする．

クラウドソーシングサービス[a] [b]を利用して被験者 62 人 (男性 29 人，女性 33 人) を用いた架空ウェブサイトへの登録実験を行う．サイト登録は合計 3 回行われ，その都度サイトに対する使用感と安心感を回答する．3 回の登録終了後にセキュリティ意識を測る SeBIS(日本語訳) と，コンピュータスキルを測る問いに回答する．1 回目情報の入力のみ，2 回目は情報の入力と SMS 認証[c]を練習として実施する．3 回目では情報を入力したのちに他サイトからの認証コード (パスワードリセットコード) が送信される．ここで表 2 に定められる被験者グループに異なる条件を与え，被害要因を調査する．このとき被験者は入力取止という選択肢も与えられている．新規登録の手順の途中であるにも関わらず，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．

2.2 結果と考察

中間者サイトへリセットコードを入力してしまった人が全体を占める割合を**被害率**とする．実験で送信した SMS の種類の概要と被害率を表 1 に示す．

図 2　メッセージ開封・メッセージ一覧・通知の例

†Investigation of new threats to accelerate the password reset attack PRMitM exploiting multi-factor authentication

‡Rina Shibayama, Hiroaki Kikuchi, School of Interdisciplinary Mathematical Science, Meiji University.

[a] クラウドワークス, https://crowdworks.jp/

[b] ランサーズ, https://www.lancers.jp/

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

表 1　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	10	13	76.9
1	あり（下部）	日本語	14	17	82.4
2	あり（下部）	英語	13	17	76.5
3	あり（上部）	日本語	0	6	0.0
4	あり（上部）	英語	8	9	88.9

表 2　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	10	13	76.9	0.136	0.713
1	警告有	14	17	82.4		
3	日本語	0	6	0.0	11.429	0.001
4	英語	8	9	88.9		
3+4	上部	8	15	53.3	3.468	0.063
1+2	下部	27	34	79.4		

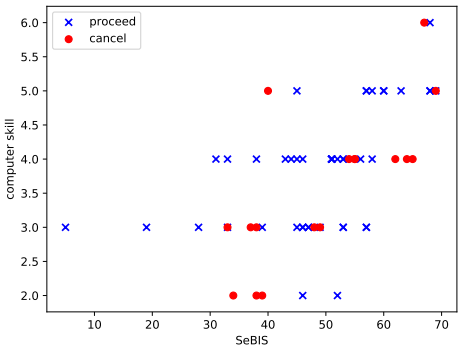

図 3　SeBIS とコンピュータスキルと PRMitM 攻撃被害の散布図

2.2.1　SMS メッセージの特徴

SMS の特徴ごとの被害率と自由度 1 でカイ 2 乗検定を行った結果を表 2 に示す．日本語／英語で Type1+3, 2+4 とせず Type3 と 4 のみを採用したのは，1 と 2 で下部のみに警告した場合，警告自体が読まれておらず，言語間の差が表れないと判断したためである．

警告あり／なしでは被害率に有意差が認められなかった ($p = 0.713$)．このことから多くの利用者はメッセージの文面を読まずにコードを入力していると考えられる．

警告を上部に記載すると，下部の警告と比べて被害が少ない傾向が見られた ($p = 0.063$)．利用者は本文を読むのではなくコードを探すので，コードより前や付近に認証コードの用途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．

メッセージが英語では 89 %がコードを入力してしまったのに対し，日本語ではコードを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．

また，入力をキャンセルした理由は，「S! JAPAN とあった」が最も多く 7 人，「メッセージ内容がわからない」が 6 人，「パスワードリセットとあった」が 3 人であった．

2.2.2　確認・入力方法と被害の関係

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 ($p = 0.943$)．

認証コードを「メッセージ開封」「メッセージ一覧」「画面上部の通知」で確認することによる有意差は認められなかった ($p = 0.443$)．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) メッセージの冒頭 2 行のみが表示されると，どちらも利用者は知る由がないため全員が被害を受けると予想していたが，被害率は一覧・通知ともに 100 %には及ばなかった．ただし，確認方法の選択肢を文章で示したため，我々の意図通りに解釈している可能性が考えられる．

2.2.3　セキュリティ意識とコンピュータスキル

SeBIS の各質問を説明変数，入力／キャンセルを目的変数としてロジスティック回帰分析を行った結果，「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」人は $e^{-0.688} = 0.462$ で被害を受ける確率が半分以下で有意差があった (p=0.039)．それ以外の項目に有意差は認められなかった．また，SeBIS とコンピュータスキルに関する問いを，それぞれ 0-80 点，0-6 点で評価した．散布図を図 3 に示す．

コンピュータスキルが中程度のときは SeBIS が低い層が被害を受けやすかった．意識が低いユーザはコードの入力という作業以外に注目せず完了している可能性がある．一方スキルが低い (3.0 以下) では，逆に SeBIS が高い層が被害を受けている．彼らはコード認証への慣れがあったのかもしれない．

3　おわりに

警告の有無・記載位置・言語の各要因が PRMitM 攻撃に対する被害率に与える影響を明らかにするためユーザ実験を行った．その結果，警告を冒頭に明記すること・日本語であることは攻撃に対する被害を減少させることを示した．逆にコードの確認・入力方法は被害率に大きな影響を与えないことが明らかになった．また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] N. Gelernter, et. al, “The Password Reset MitM Attack”, IEEE Security and Privacy, 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, pp.1-8, 2018.

[3] S. Egelman, E. Peer, “Scaling the Security Wall Developing a Security Behavior Intentions Scale (SeBIS)”, SIGCHI , pp.2873-2882, 2015.