

# 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

笹航太, 菊池浩明 (明治大学)

# 背景：二要素認証を用いたパスワードリセット

①

電話番号/メールアドレス/ユーザー名

パスワード

ログイン

保存する

パスワードを忘れた場合はこちら

②

メールアドレスか電話番号かユーザー名を入力してください

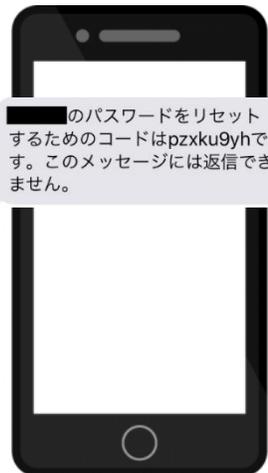
検索

③

■■■■の携帯電話にコードを送信しました。受信したコードを以下に入力してパスワードをリセットしてください。

コードを入力

送信



④

新しいパスワードを入力

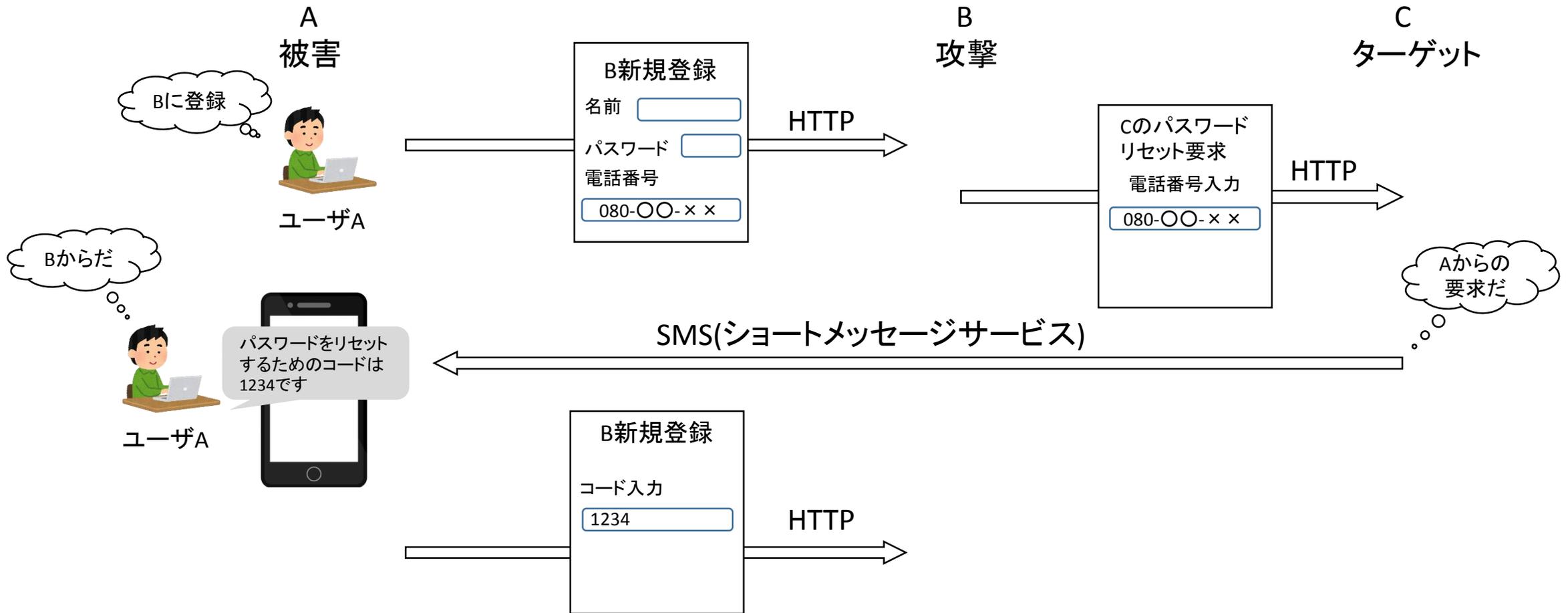
新しいパスワードを再度入力してください

保存する

送信

# Password Reset MitM攻撃

[Gelernter, IEEE Symposium on Security and Privacy 2017]



# GelernterのPRMitM攻撃対策

- 対策1:リセットコードでなくURLを送り, 遷移先でパスワードリセット



登録フォーム

コード入力

URLを入力させないと  
乗っ取れない

- 対策2:SMS本文にサービス名を明示する

確認コード: [259003](#)  
上記の番号を画面へ入力してください。  
SI JAPAN

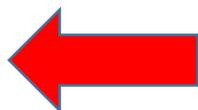
- 対策3: SMS本文にパスワードリセットであることを明示する

SI JAPANのパスワードをリセットするためのコードは[259003](#)です。このメッセージには返信できません。

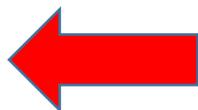
# Gelernterの問題点

1. 人間要素・・・セキュリティ意識, 性別, 年齢などによる差

2. 長文攻撃



3. 数字の認証コード



4. ID連携・・・



5. LVS

- 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
- URLを伝達することが普及すると新たな phishing の標的になる

# Gelernterの問題点

## 2. 長文攻撃

(1)

アカウント登録のために本人確認コードを入力してもらいます。このプロセスでセキュアな登録を実現します。確認のためのコードは[368552](#)です。送信後2つ目のメッセージが送られるのでもう一度コードを入力してください。二度繰り返すことでさらにセキュアなアカウント登録を可能とします。

(2)

S! JAPANのパスワードをリセットするためのコードは[259003](#)です。このメッセージには返信できません。

## 3. 数字の認証コード

S! JAPANのパスワードをリセットするためのコードは**b2g6yk4h**です。このメッセージには返信できません。

S! JAPANのパスワードをリセットするためのコードは[259003](#)です。このメッセージには返信できません。

# 研究目的

- Gelernterの論文が2017年5月に発表されて以降, 対策がどのくらい進んでいるか
- 対策が効果的であるか
- 被害を受けやすいユーザはどんな人か

# 研究方法

## (1)PRMitM攻撃に対して潜在的にリスクを持つ日本の主要ウェブサイトを明らかにする

- Alexaの日本のアクセス top 200のサイトでSMSを用いたパスワードリセットを行っているか調査

〇〇サービスです  
確認コードは  
1234です

パスワードリセット  
の警告がない

1234を入力して  
ください

企業名がない

## (2)PRMitM攻撃を受けるユーザーの特徴調査

- ユーザスタディを行い評価する

# (1)調査結果

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					

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。

## (2) 実験方法

- クラウドソーシングサイトのCloudWorksで184名の被験者によるウェブサイト登録実験を行った
  - 架空の4種類のウェブサイトに登録してもらう
  - いずれも必要事項(名前, パスワード, 電話番号)を入力させる
  - 入力した電話番号宛にSMS送信サービスtwilioを利用したSMSが届く
- 4回の登録のいずれかに脆弱性が含まれている可能性があるという説明
  - 気づいたらキャンセルするよう指示
- 被験者を5グループに分けて実験を行う

# 実験手順

	1種目	2種目	3種目	4種目
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

登録実験

Q0.あなたの年齢を選択してください

20歳未満 ▼

Q1.性別を選択してください

男性 ▼

Q2.Twitterに電話番号を登録していますか

していない ▼

Q3.Facebookに電話番号を登録していますか

している ▼

Q4.Yahooアカウントに電話番号を登録していますか

覚えていない ▼

ユーザアンケート

Q1: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

●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

Q2: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

●全く使っていない ●ほぼ使っていない ●たまに使っている ●しばしば使っている ●いつも使っている ●回答しない

Q3:コンピュータから離れるとき、手で画面をロックする

●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

Q4: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

●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

Q5:必要があるときしかパスワードを変更しない

●全く変更しない ●ほぼ変更しない ●たまに変更する ●しばしば変更する ●いつも変更する ●回答しない

SeBIS

(セキュリティ志向度アンケート)

# 被験者グループ

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

確認コード：[259003](#)  
上記の番号を画面へ入力してください。  
S! JAPAN

S! JAPANのパスワードをリセットするためのコードは[259003](#)です。このメッセージには返信できません。

S! JAPANのパスワードをリセットするためのコードはb2g6yk4hです。このメッセージには返信できません。

アカウント登録のために本人確認コードを入力してもらいます。このプロセスでセキュアな登録を実現します。コードは[368552](#)です。送信後2つ目のメッセージが送られるのでもう一度コードを入力してください。二度繰り返すことでさらにセキュアなアカウント登録を可能とします。

S! JAPANのパスワードをリセットするためのコードは[259003](#)です。このメッセージには返信できません。

# SeBIS(Security Behavior IntentionsScale)

[Serge Egelman, SIGCHI Conference on Human Factors in Computing Systems (CHI' 15)]

- セキュリティ志向度を調査する質問
  - 全18問(内2問は問題をきちんと回答しているかを判別する問題)
  - 5段階で回答し, 点数が高いほどセキュリティ意識が高い

5	必要があるときしかパスワードを変更しない
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
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)

- セキュリティ意識が高いほど, 攻撃を受けにくいと考えた

# 実験結果

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

確認コード：[259003](#)  
上記の番号を画面へ入力してください。  
S! JAPAN

S! JAPANのパスワードをリセットするためのコードは[259003](#)です。このメッセージには返信できません。

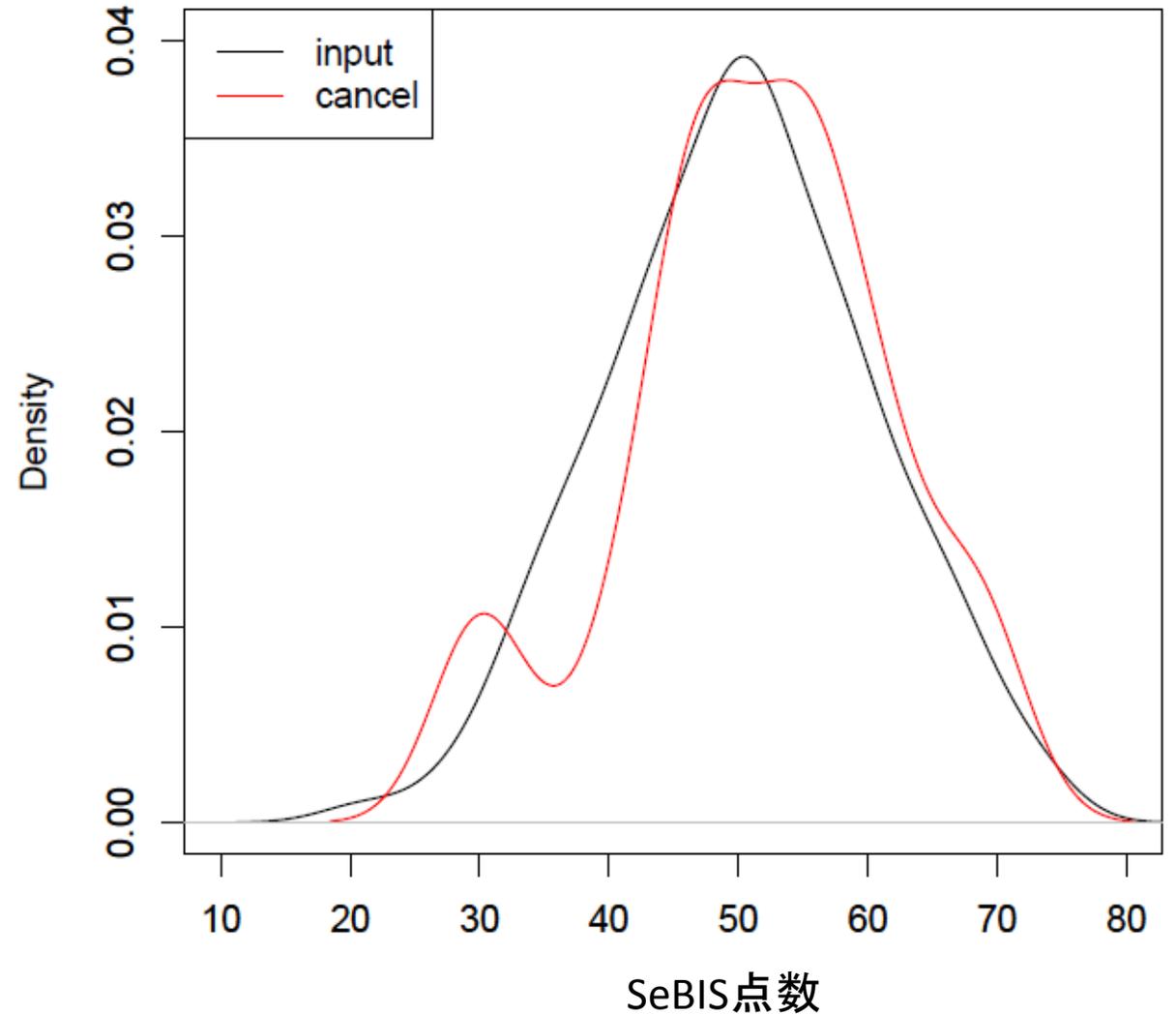
S! JAPANのパスワードをリセットするためのコードは**b2g6yk4h**です。このメッセージには返信できません。

アカウント登録のために本人確認コードを入力してもらいます。このプロセスでセキュアな登録を実現します。コードは[368552](#)です。送信後2つ目のメッセージが送られるのでもう一度コードを入力してください。二度繰り返すことでさらにセキュアなアカウント登録を可能とします。

# SeBIS分布

- セキュリティ志向度の質問であるSeBISの合計点数によって攻撃を受けるかどうかは差がなかった
- 全体の平均点は50.3点

	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



# 利用者属性別被害率

		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

# 評価1. カイ二乗検定

type		入力	キャンセル	リセット被害率 [%]	$\chi$	P 値
0	警告無し	35	2	94.6	2.7333	0.09828*
1	警告有	30	8	78.9		有意水準10%を満たす
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		有意水準0.1%を満たす

# 評価2. ロジスティック回帰分析

- 警告なし ( $x_1 = 0$ ) に対する, 警告有 ( $x_1 = 1$ ) による被害確率のオッズ比

$$e^{1.25} = 3.49$$

警告なしは警告有に比べて3.5倍  
攻撃を食らいやすい

- SeBIS問5(必要があるときしかパスワードを変更しない)のオッズ比は

$$e^{2.45} = 11.59$$

- 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

	Estimate $\beta$	Std. Error	z value	Pr(> z )
(Intercept)				
$x_0$	-1.68	4.64	-0.36	0.717 *
$x_1$	-1.25	1.63	-0.77	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 *

# PRMitM攻撃のインパクト評価

確認コード: [540987](#)  
上記の番号を画面へ入力してください。  
Yahoo! JAPAN

- Yahooが受ける可能性のある被害推定

- Yahooアカウントのアクティブユーザが3,614万人(2016年9月)
- $3614 \times 0.25 = 900.3$
- →Yahooに電話番号を登録しているユーザ数が約900万人であると仮定する

電話番号を登録	入力	キャンセル	計	割合
している	39	7	46	0.25
していない	74	28	102	0.55
わからない	30	6	36	0.20

- 警告なし

- $900 \times 35/37 = 851.4$
- 851万人が被害を受ける可能性がある

type		入力	キャンセル	リセット被害率[%]
0	警告なし	35	2	94.6
1	警告あり	30	8	78.9

- 警告有

- $900 \times 30/38 = 710.5$
- 710万人まで被害を減らすことが出来る

type		入力	キャンセル	リセット被害率[%]
0	警告なし	35	2	94.6
1	警告あり	30	8	78.9

# まとめ

- 日本のアクセス top 200のサイトでPRMitM攻撃の対策をしていないウェブサービスが4件あることを示した
- PRMitM攻撃の影響評価を行い、警告とリセットコードを英数字にすることが有効であることを示した
- 被害ユーザはアカウント登録をしたか覚えていない、または50代以上に多かった
- パスワードをよく変更するユーザは、あまり変更しないユーザの11.6倍被害を受けやすいことを示した