2019年2月1日

修士論文発表会

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

菊池研究室

背景：二要素認証を用いたパスワードリセット

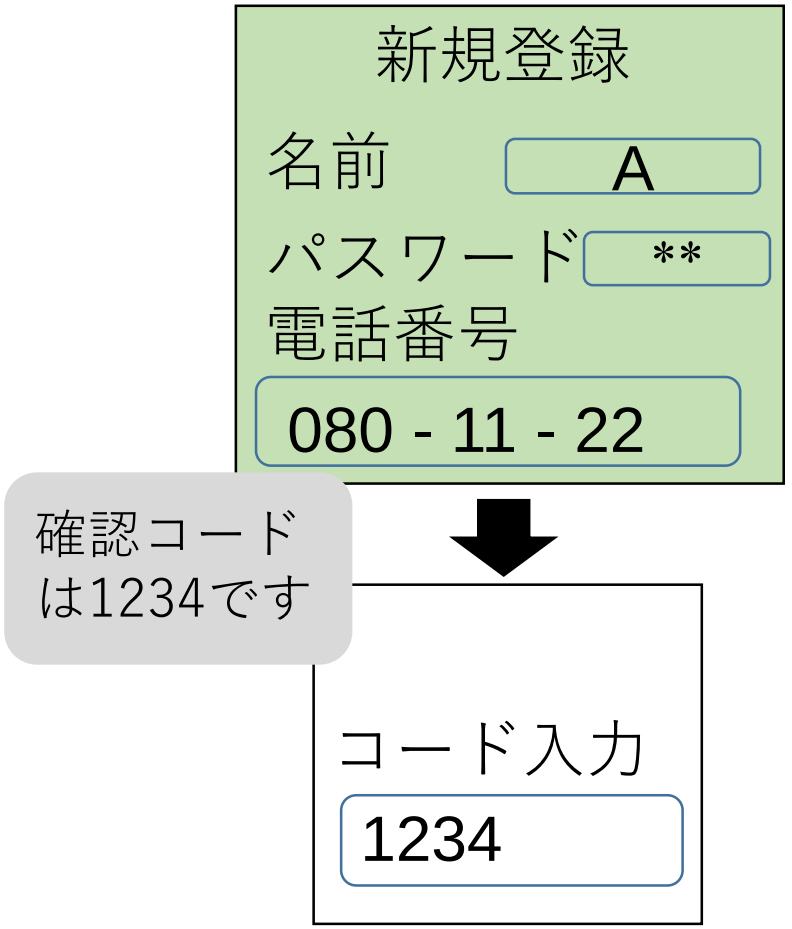
[redacted]の携帯電話にコードを送信しました。受信したコードを以下に入力してパスワードをリセットしてください。

コードを入力

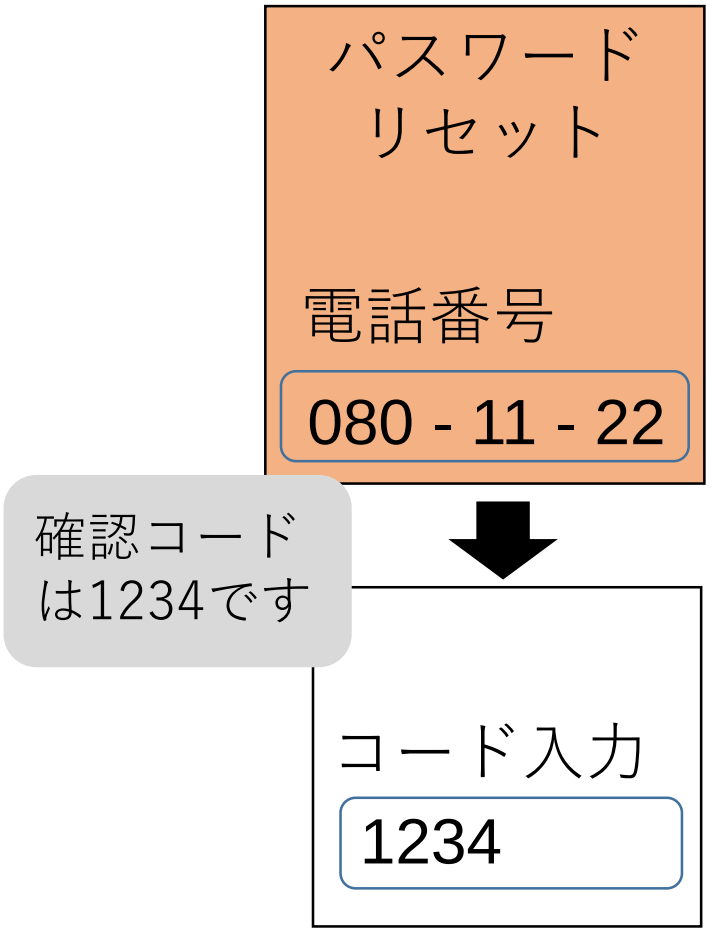
送信

2種類の二要素認証

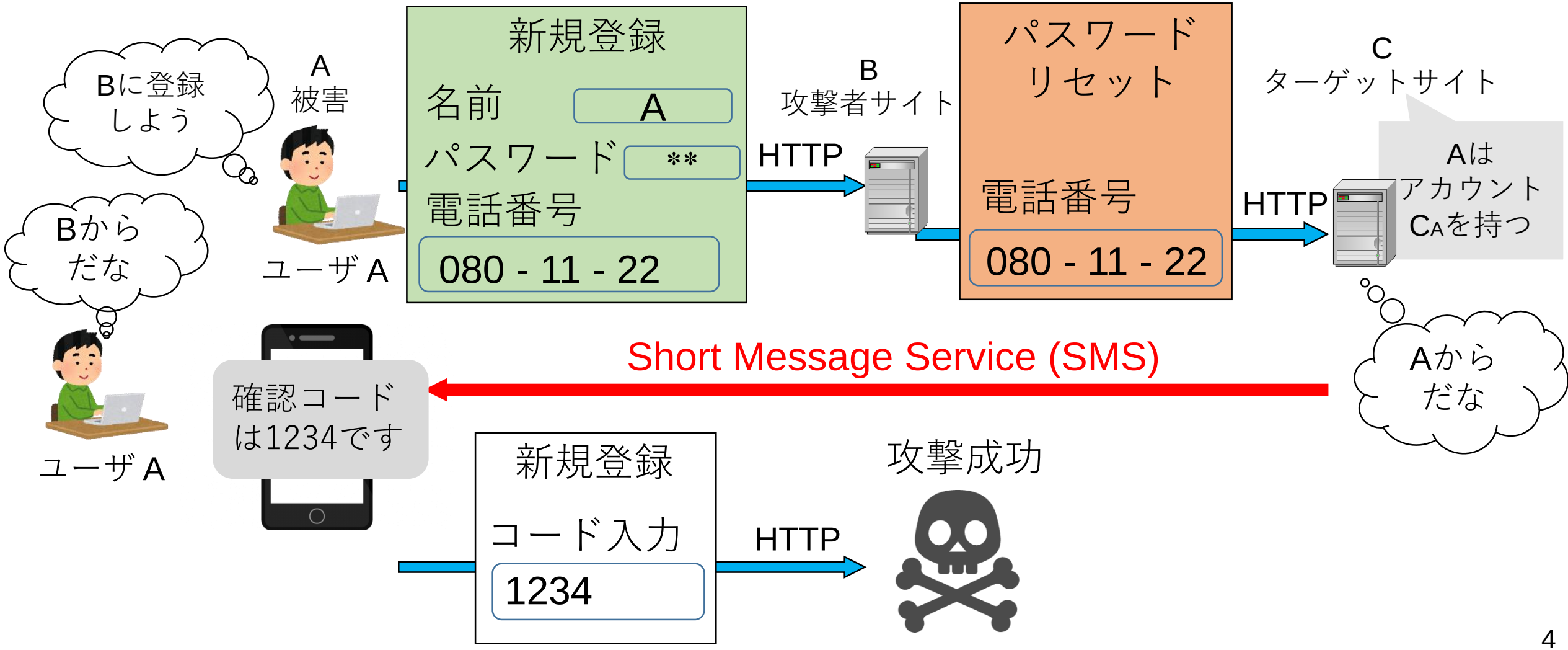
- 新規登録



- パスワードリセット



Password Reset Man-in-the-Middle 攻撃 (PRMitM)
[Gelernter, IEEE Symposium on Security and Privacy 2017]



Gelerntер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

新規登録

コード入力

https://aaaa/bbbb

URLを入力させないと
乗っ取れない

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

- 対策2：SMS本文にサービス名を明示する
- 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

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。

Gelernterの問題点

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

→URLが本物か偽物かの判断がつかない

→新たなフィッシング攻撃の温床となる

2. SMS本文にサービス名を明示する

3. SMS本文にパスワードリセットであることを明示する

→ユーザがSMSの文章を読まない可能性

新たな脅威：長文攻撃

1通目

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36852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通目

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

既存の脆弱性：認証コードの種類

英数字の認証コード

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

数字のみの認証コード

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

リサーチクエスチョン

- 日本のウェブサイトではPRMitM攻撃に対する対策が進んでいるか
- どのようなSMSのメッセージならばPRMitM攻撃の被害を減らすことができるか
- どのようなユーザが被害を受けやすいのか

研究手法

- 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
  - アカウント登録が可能か？
  - SMSでパスワードリセットが可能か？
  - SMSにパスワードリセットであると警告があるか？

- PRMitM攻撃を受けるユーザの特徴調査
  - ユーザスタディを行い評価する

調査結果の例

- SMSを用いたパスワードリセットを行う企業を複数発見した

名前	パスワードリセットのSMS例
Twitter	Twitterのパスワードをリセットするためのコードは160973です。
Yahoo JAPAN	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

- Twitterは警告があるからセキュアなメッセージ
- Yahoo JAPAN は攻撃に対して脆弱なメッセージ

200サイト調査結果

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のメッセージ
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。

ユーザスタディ概要

- 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
  - セキュリティの意識調査と説明し架空の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ウェブサイト登録のための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説明する
  - 脆弱性に気づいたら登録をキャンセルするよう指示

架空の4種類のウェブサイト

	(1)	(2)	(3)	(4)
名前	S! JAPAN	Cowtter	Majebook	Mstagram
送られる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	危険(MitM攻撃)	SSLの影響調査

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

Security Behavior Intentions Scale (SeBIS)

[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，必要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）

実験結果 1

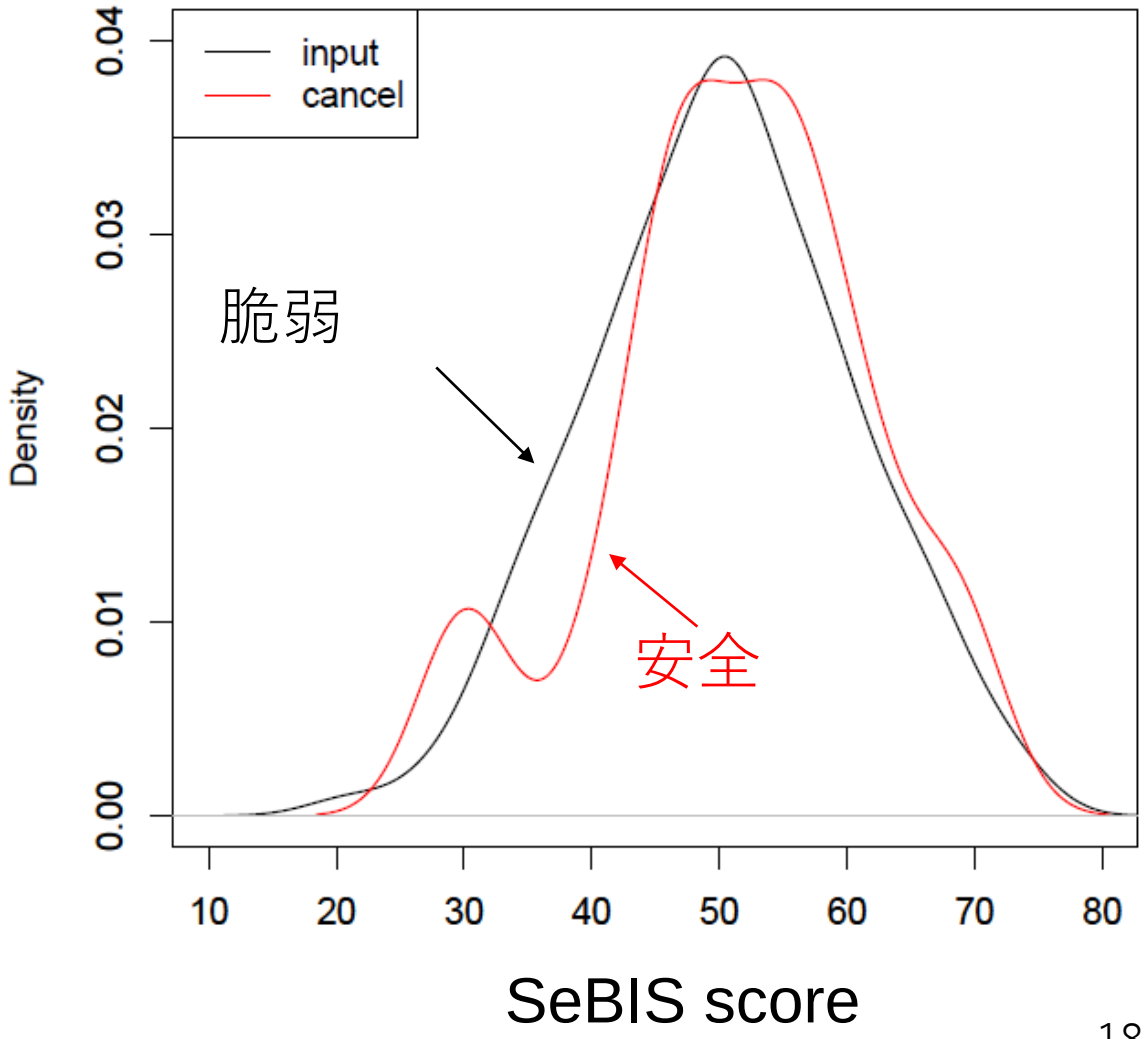
type	SMS スタイル	入力	キャンセル	リセット被害率[%]
0	警告なし	35	2	94.6
1	短文 数字	30	8	78.9
2	短文 英数字	28	12	70.0
3	長文 数字	28	7	80.0
4	長文 英数字	22	12	64.7

X二乗検定

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		

結果 2：SeBIS得点分布

得点	入力	キャンセル	リセット 被害率[%]
50点以上	66	21	75.9
50点未満	54	18	75.0



結果 3：ユーザ属性別被害率

		Enter	Cancel	Total	Successful attack ratio[%]
年齢	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	34	79
	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 Japan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

ロジスティック回帰分析

- 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

頻繁なパスワード変更は危険！

	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	-4.05	1.82	-2.23	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 *

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
- ユーザスタディの結果以下のことが明らかになった
  1. SMSに警告のメッセージを含めることでPRMitM攻撃の被害を減らすことが出来る
  2. 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代以上に多い
  3. 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

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
  - 3614×0.25 = 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
  - 900×35/37= 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
  - 900×30/38= 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