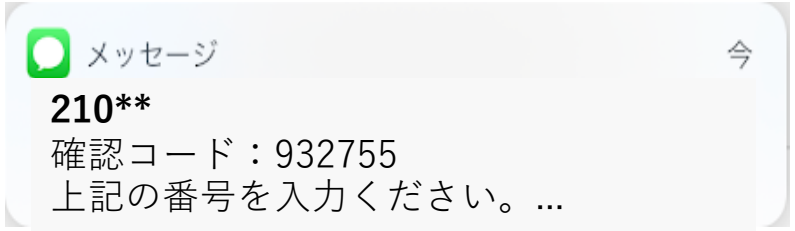
SMS通知機能を悪用した新たなパスワードリセット脆弱性の脅威評価

明治大学 総合数理学部
柴山りな　　菊池浩明

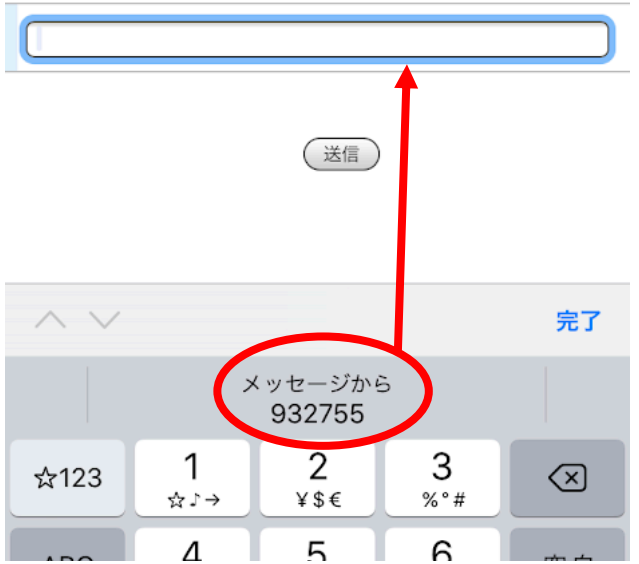
Q. SMSの便利な機能の脆弱性とは？

1. 通知



2. メッセージ一覧

3. 自動入力



認証コードの通知を受け取ったとき、皆さんはどうしますか？

Majebookアカウント作成

070-0011-2233へ認証コードを送信しました。

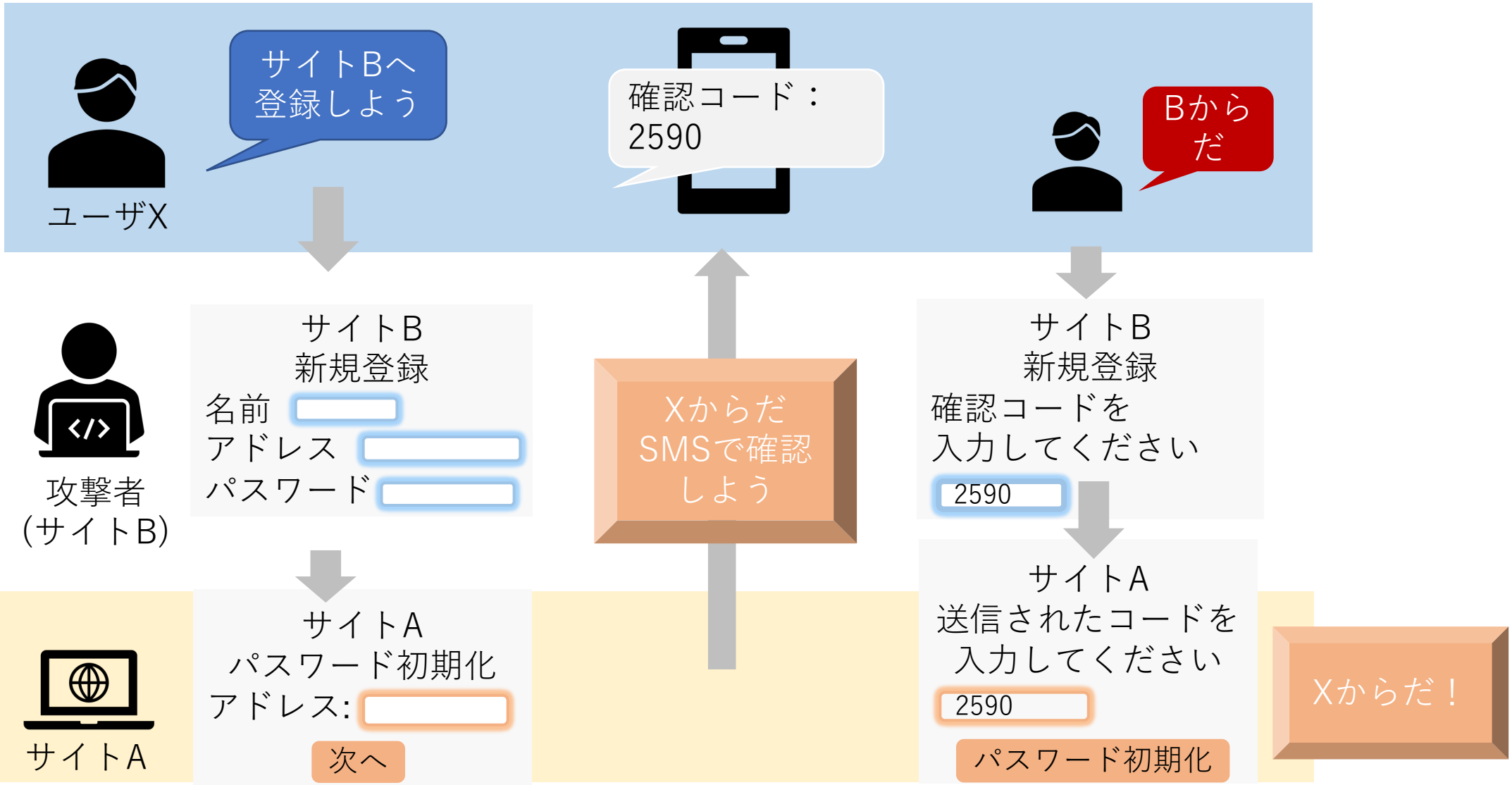
以下に受信したコードを入力してください。

コード入力

送信

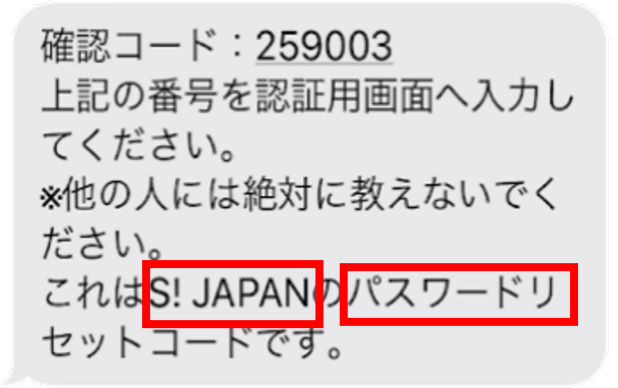
通知の１・２行で、認証コードと勘違いして入力してしまうと、パスワードが誰かに変更されることに…

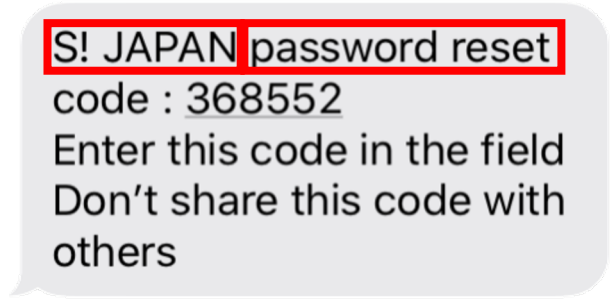
先行研究：Password Reset MitM攻撃
[Gelernter, IEEE Symposium on Security and Privacy 2017]



研究目的

- 以下の4つの仮説を検証すること





【仮説】

1. 警告を下に記すと被害が増える→〇769倍
2. 警告を英語で記すと被害が増える→〇119倍
3. セキュリティ意識が高いと被害を受けない→×
4. 自動入力を利用すると、被害が増える→×

実験方法 1

- クラウドワークス・ランサーズでの被験者81名を用いたユーザ実験
- 架空ウェブサイトへ合計3回登録してもらう
  - 登録情報の入力（名前、パスワード、電話番号）
  - 電話番号にSMS送信サービス*twilio*を利用したSMSが届く
- 3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
  - 気づいたらキャンセルするよう指示

順序	登録サイト	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

実験方法２：５つの被験者グループ

	警告なし	警告あり（上部）	警告あり（下部）
日本語	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のパスワードリセットコード：368552 上記の番号を認証用画面へ入力してください。 ※他の人には絶対に教えないでください。	確認コード：259003 上記の番号を認証用画面へ入力してください。 ※他の人には絶対に教えないでください。 これはS! JAPANのパスワードリセットコードです。
英語		S! JAPAN password reset code : 368552 Enter this code in the field Don’t share this code with others	Your verification code: 259003 Enter this code in the field Don’t share this code with others This is password reset code from S! JAPAN

実験方法 3

- **SeBIS（全16問・選択式）**
  デバイスの安全確保
  パスワードの管理
  Web 使用時のセキュリティ意識
  アップデー ト

- **アンケート**
  属性
  使用デバイス
  入力・確認方法

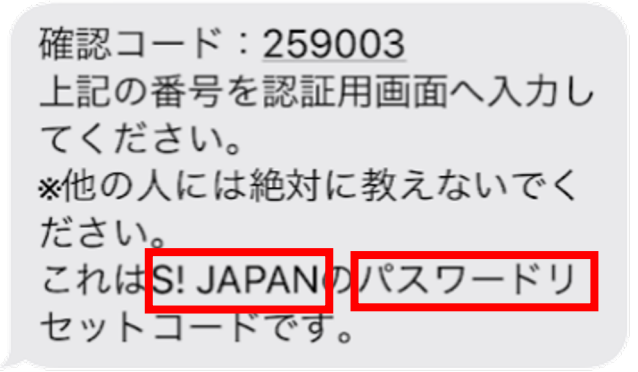
7	アカウントごとに違うパスワードを使っている	1.536	0.540
10	リンクが送られてきたとき，どこにつながるか確認しないでクリックする	0.664	0.609
16	使用しているプログラムが最新であることを確認するようにしている	1.233	0.787

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

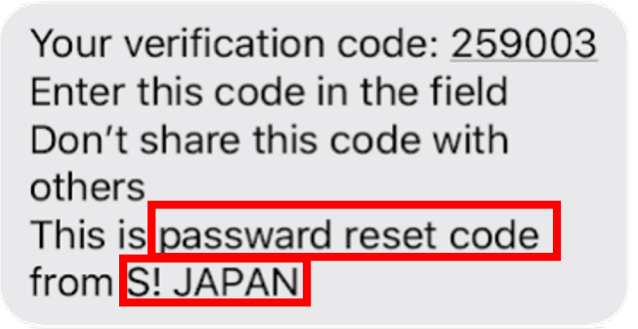
実験結果：
メッセージの種類ごとの被害率

type	SMSの特徴		入力	キャンセル	被害率[%]
	警告	言語			
⓪	なし	日本語	14	5	73.7
①	あり（下部）	日本語	15	4	78.9
②	あり（下部）	英語	16	4	80.0
③	あり（上部）	日本語	0	7	0.0
④	あり（上部）	英語	10	6	67.9

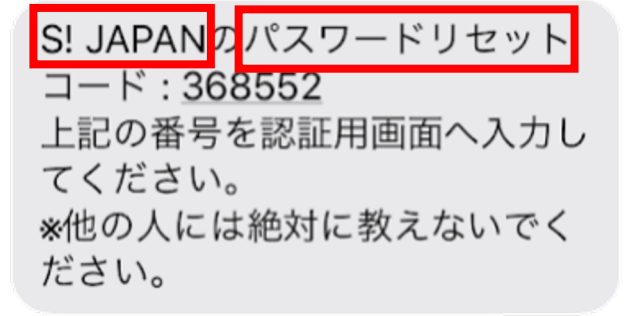
①



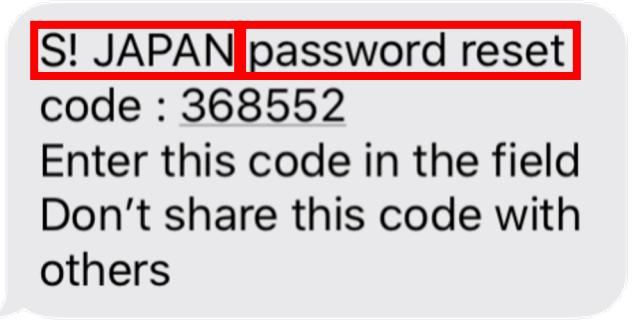
②



③



④

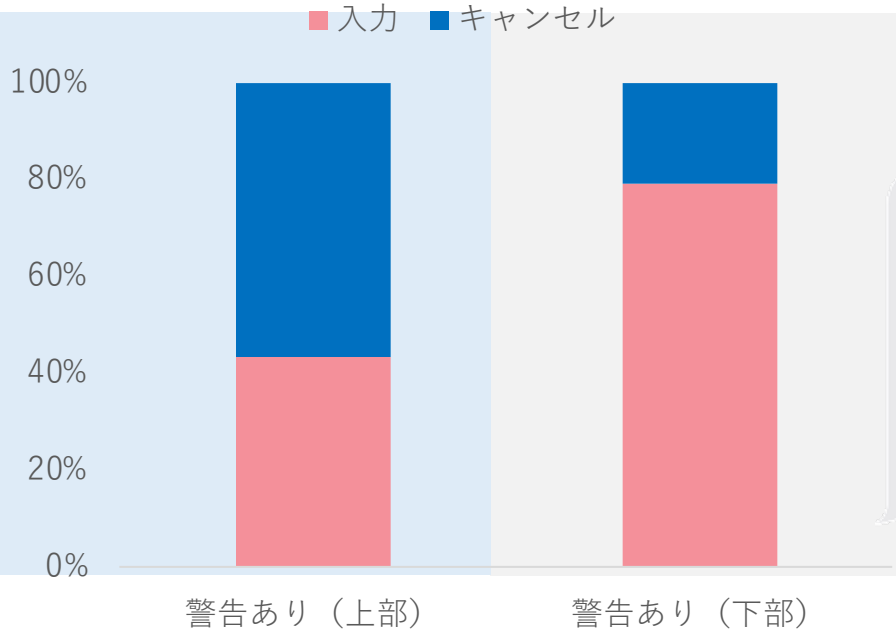


実験結果：警告位置

【仮説１】警告を下に記すと被害が増える→○769倍

＜上部＞

S! JAPANのパスワードリセット
コード：368552
上記の番号を認証用画面へ入力してください。
※他の人には絶対に教えないでください。



＜下部＞

確認コード：259003
上記の番号を認証用画面へ入力してください。
※他の人には絶対に教えないでください。
これはS! JAPANのパスワードリセットコードです。

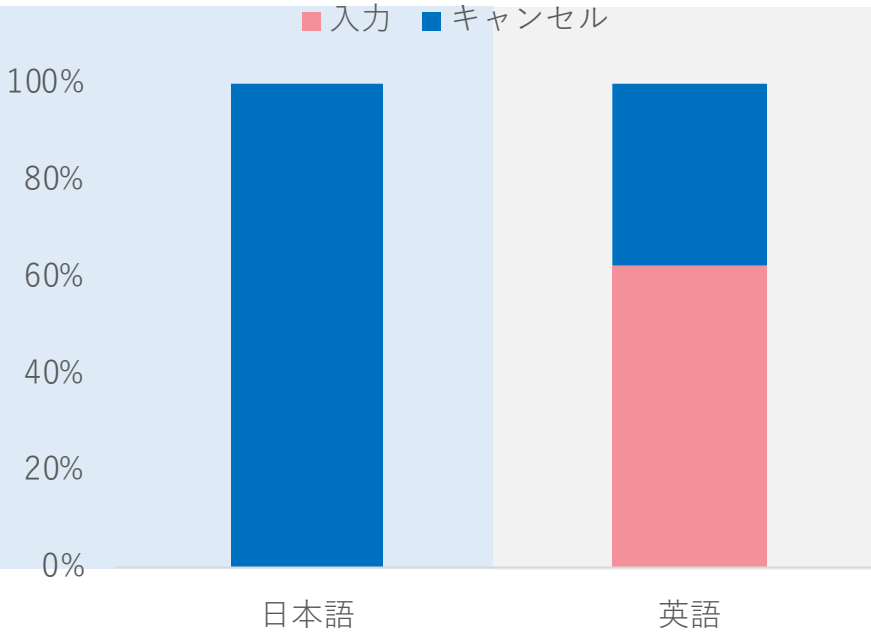
●SMS上部に認証コードの用途を明記することが被害率を下げるために有効

実験結果：警告の言語

【仮説２】警告を英語で記すと被害が増える→〇**119倍**

＜日本語＞

S! JAPANのパスワードリセット
コード：368552
上記の番号を認証用画面へ入力してください。
※他の人には絶対に教えないでください。



＜下部＞

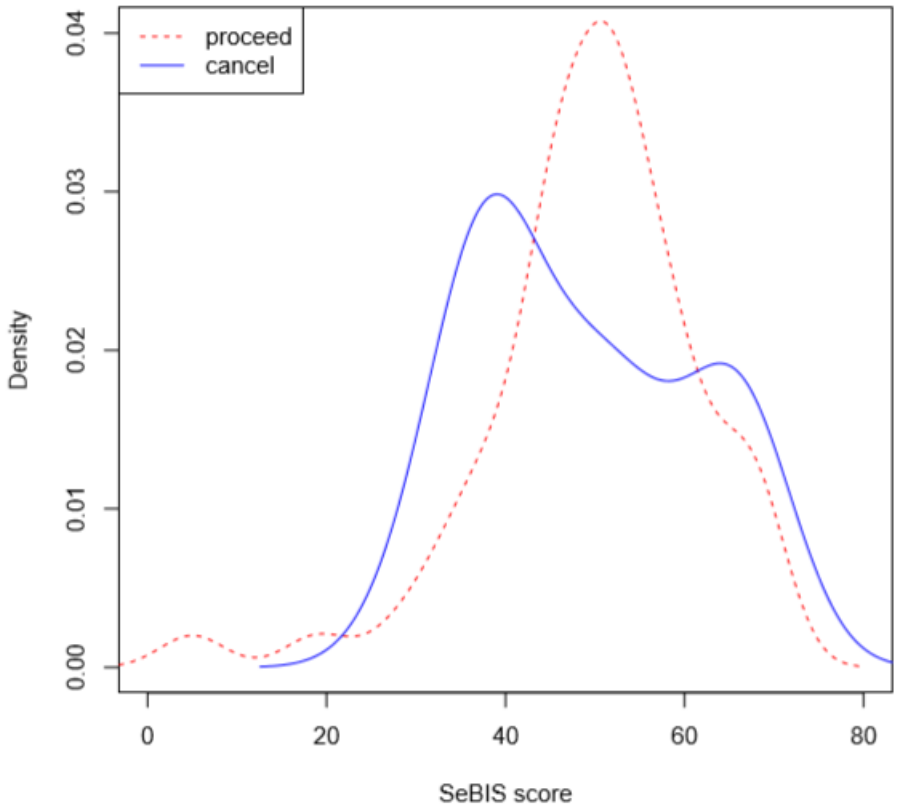
S! JAPAN password reset
code : 368552
Enter this code in the field
Don’t share this code with others

●メッセージの内容が即座に理解できない場合（英語），
利用者は立ち止まらず入力してしまう

実験結果：SeBIS

【仮説３】セキュリティ意識が高いと被害を受けにくい→ ×

	平均値		SD	t 値	p 値
	入力	取止			
SeBIS	49.6	48.8	12.0	0.132	0.896



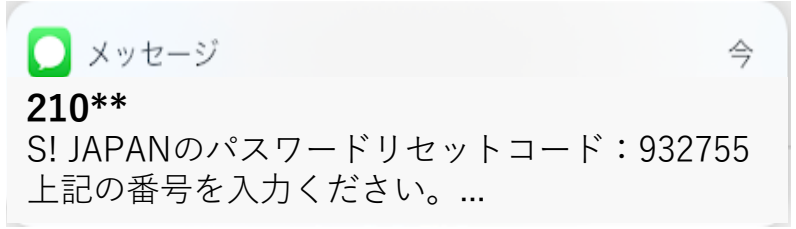
	質問	e^{β}	p 値
1	コンピュータを長時間放置したとき，自動的にロックするような設定にしている	1.177	0.842
2	ノートパソコンやタブレットのロックを解除するとき，パスワード/パスコードを使っている	0.657	0.611
3	コンピュータから離れるとき，手動で画面をロックする	0.140	0.024*

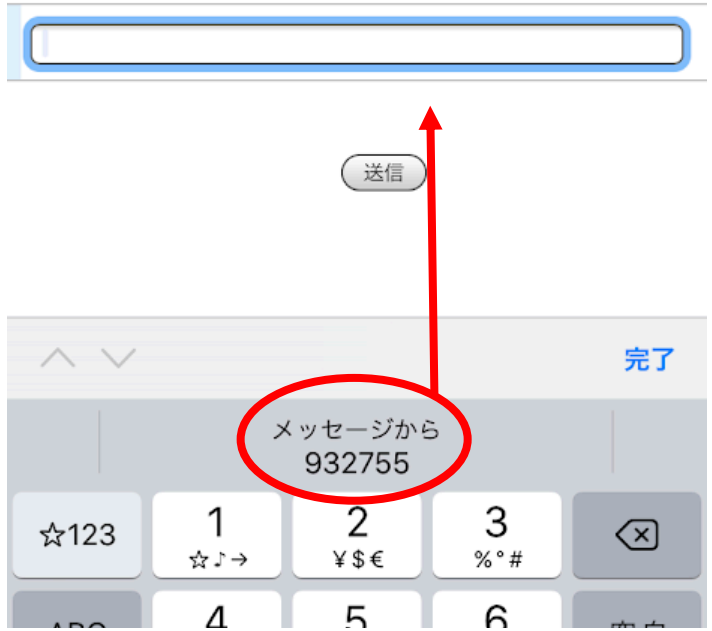
- 「コンピュータから離れるとき、手動で画面をロックする」人は、攻撃の被害を受けにくい（$\frac{1}{7}$）

実験結果：入力・確認方法

【仮説４】自動入力を利用すると、被害が増える→ ✕

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





- 自動入力を利用した人の被害率は66.7%で、高くなかった

ロジスティック回帰分析

- SMSの種類、登録サイトへの使用感と安心感、年齢・性別、コードの確認・入力方法、使用デバイスとSeBIS・スキルの合計点を説明変数としてロジスティック回帰分析をした

- 警告上部 OR=$e^{-6.673}$ =0.0013→$\frac{1}{769}$ 倍
- 日本語 OR=$e^{-4.776}$ = 0.0084→$\frac{1}{119}$**倍**
- で被害を受けにくい

$\frac{1}{3}$倍

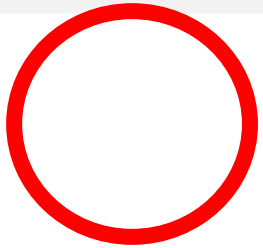
2.21倍

	Estimate	Std. Error	z value	Pr(>|z|)	
(Intercept)	8.082	5.521	1.464	0.143	
上部	-6.673	2.44	-2.734	0.006	***
下部	-2.244	1.444	-1.554	0.12	
日本語	-4.776	1.674	-2.853	0.004	***
使用感１	-1.381	0.714	-1.934	0.053	*
安心感１	0.617	0.394	1.569	0.117	
使用感２	2.372	0.93	2.55	0.011	*
安心感２	-1.303	0.445	-2.931	0.003	***
使用感３	-1.294	0.508	-2.546	0.011	*
安心感３	0.792	0.286	2.766	0.006	***
年齢	0.993	0.504	1.971	0.049	*
性別	-2.283	1.254	-1.821	0.069	*
入力方法	-1.604	0.785	-2.042	0.041	*
確認方法	0.918	0.686	1.338	0.181	
確認方法２	-0.309	0.561	-0.551	0.582	
抵抗感１	-0.344	0.356	-0.968	0.333	
抵抗感２	0.643	0.396	1.626	0.104	
スマホ	3.583	1.773	2.021	0.043	
SeBIS	-0.043	0.058	-0.749	0.454	*
スキル	0.302	0.576	0.525	0.6	

対策

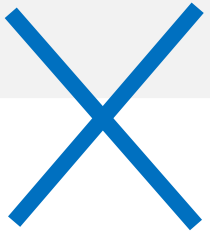
1. 自動入力させない
2. 送信元・用途は上に

259003：S! JAPANパスワードリセットコード
上記の番号を認証用画面へ入力してください。
※他の人には絶対に教えないでください



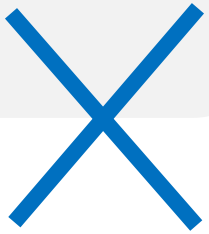
自動入力されてしまう

S! JAPANパスワードリセットコード：259003
上記の番号を認証用画面へ入力してください。
※他の人には絶対教えないでください



通知で送信元・用途が不明

259003：確認コード
上記の番号を認証用画面へ入力してください。
※パスワードリセットコードなので他の人には絶対教えないでください
S! JAPAN



まとめ

- パスワードリセットコードを知らせるSMSで
  - 下部で警告すると、119倍にリスクが増える
  - 日本語で警告すると、$\frac{1}{790}$倍にリスクを下げる