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

明治大学　総合数理学部　3年
柴山りな　　菊池浩明

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。

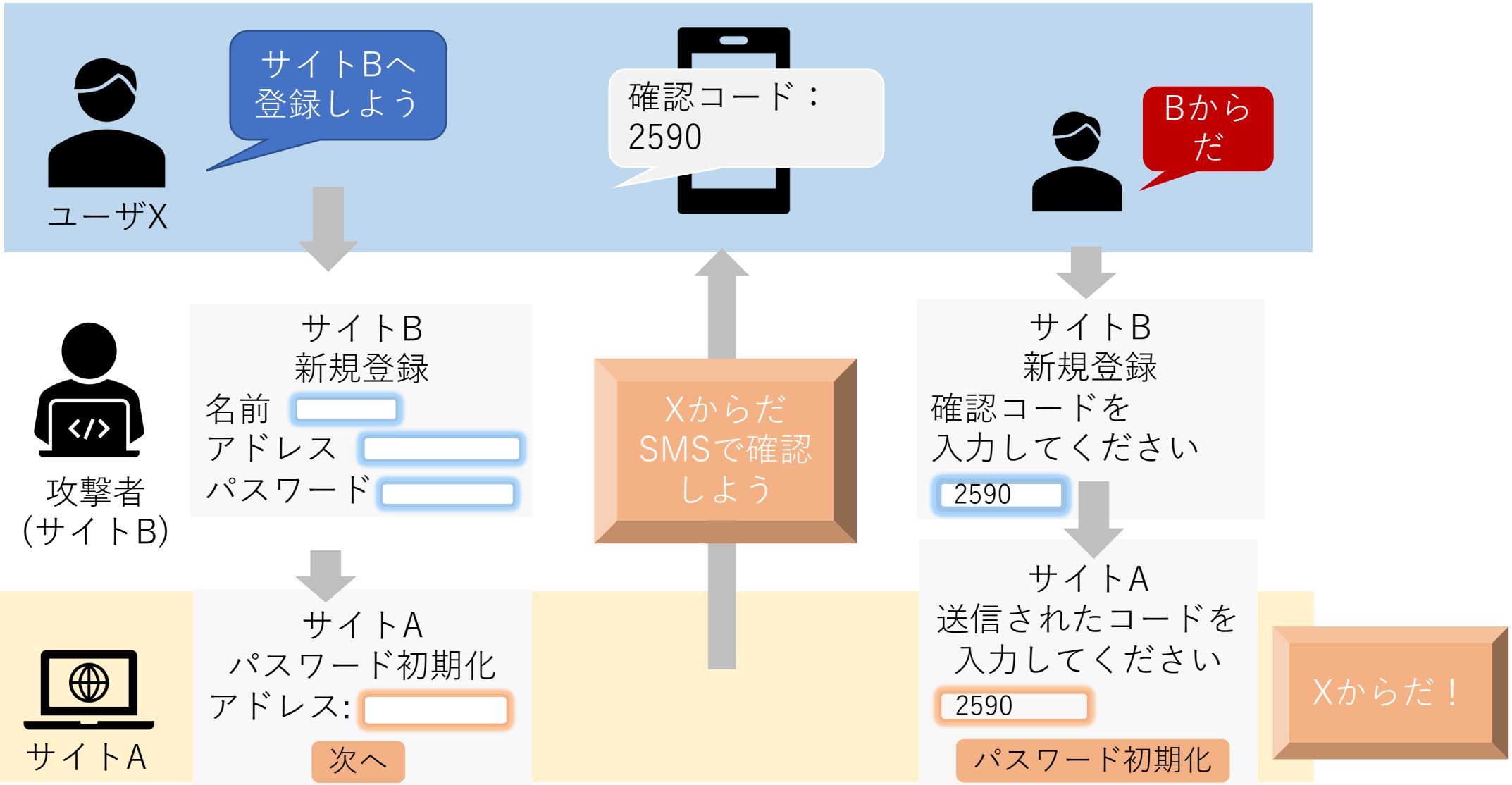
コード入力

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

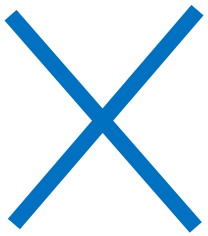
[Gelernter, IEEE Symposium on Security and Privacy 2017]

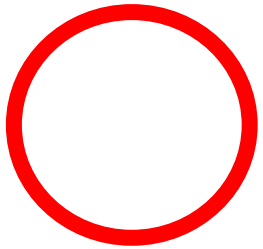


GelerらによるPRMitM攻撃への対策

I. 送信元の明記
II. 認証コード／URLの使用用途の明記
（パスワードの初期化）

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。



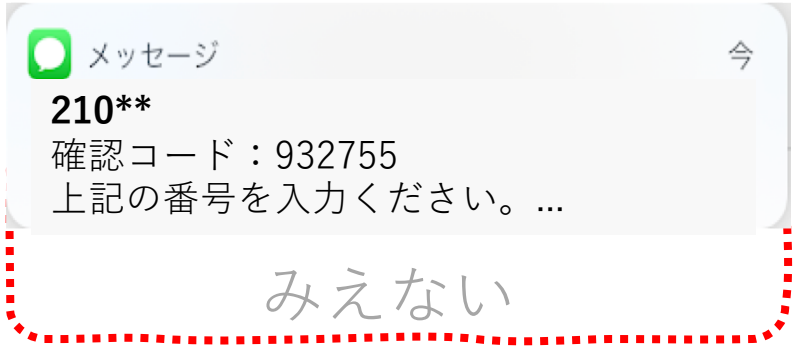


※注意※あなたのFacebookのパスワードが初期化を要求されました。
このコードを他の人に教えたり、Facebook以外のサイトに入力したりしないでください。

あなたのパスワードリセットコードはXXXXXXXです。

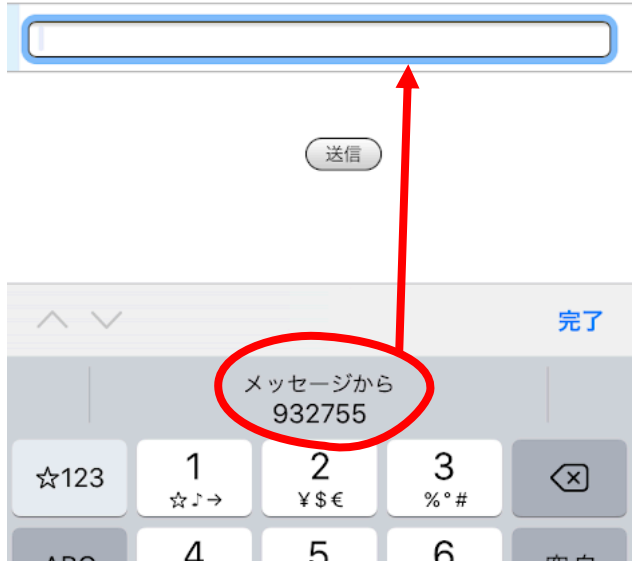
本研究の新規性：被害を増長させる要素

1. 通知



2. メッセージ一覧

3. 自動入力



●本来の内容

確認コード：932755
上記の番号を入力ください。
※これはS! JAPANのパスワードリセットコードです

研究目的

- 通知や自動入力などの機能がPRMitM攻撃の被害率に及ぼす影響を調査する

実験方法

- クラウドワークス・ランサーズで被験者62名を用いた、ユーザ実験

実験方法

- 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）
  - 登録した電話番号に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

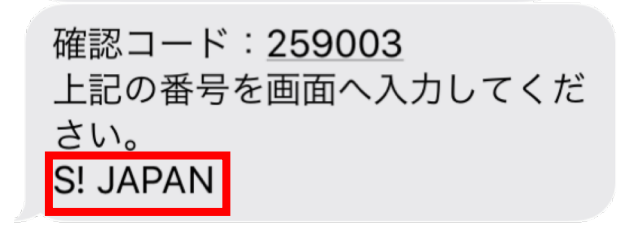
順序	登録サイト	実施目的	認証コード
1	S! JAPAN	登録練習	なし
2	Cowtter	コード入力練習	Cowtter認証コード
3	Majebook	被害要因の調査	S! JAPANパスワードリセットコード

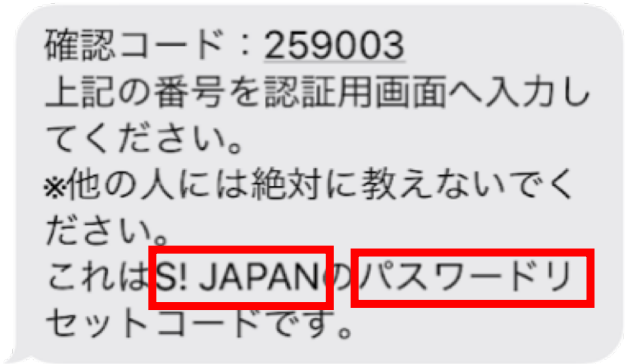
５つの被験者グループ

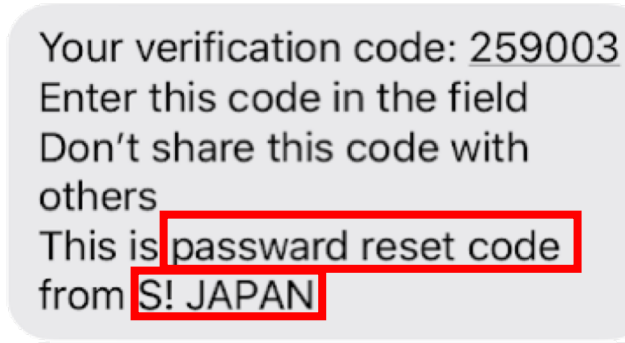
	警告なし	警告あり（上部）	警告あり（下部）
日本語	確認コード：259003 上記の番号を画面へ入力してください。 S! JAPAN	S! JAPANのパスワードリセット コード：368552 上記の番号を認証用画面へ入力してください。 ※他の人には絶対に教えないでください。	確認コード：259003 上記の番号を認証用画面へ入力してください。 ※他の人には絶対に教えないでください。 これはS! JAPANのパスワードリセットコードです。
英語		S! JAPAN password reset code : 368552 Enter this code in the field Don't share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

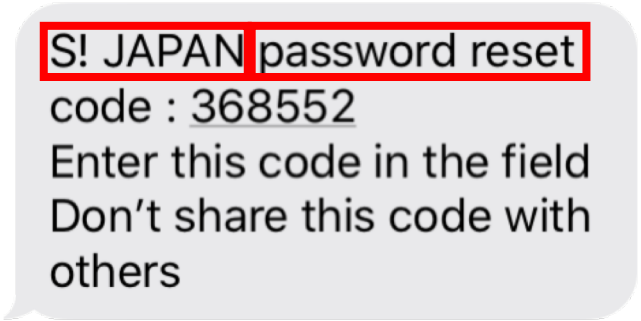
メッセージの種類ごとの被害率

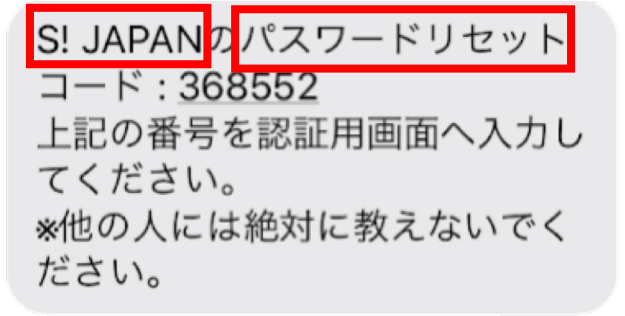
type	SMSの特徴		入力	キャンセル	被害率[%]
	警告	言語			
0	警告なし	日本語	10	3	76.9
1	警告有（下部）	日本語	14	3	82.4
2	警告有（下部）	英語	13	4	76.5
3	警告有（上部）	日本語	0	6	0.0
4	警告有（上部）	英語	8	1	88.9





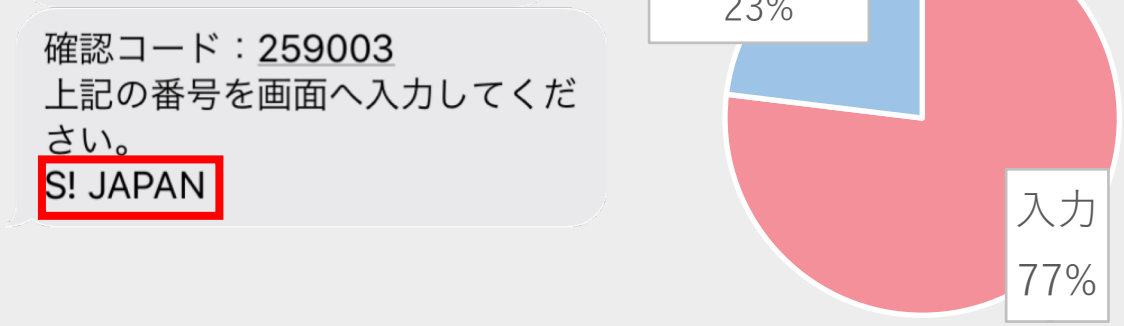




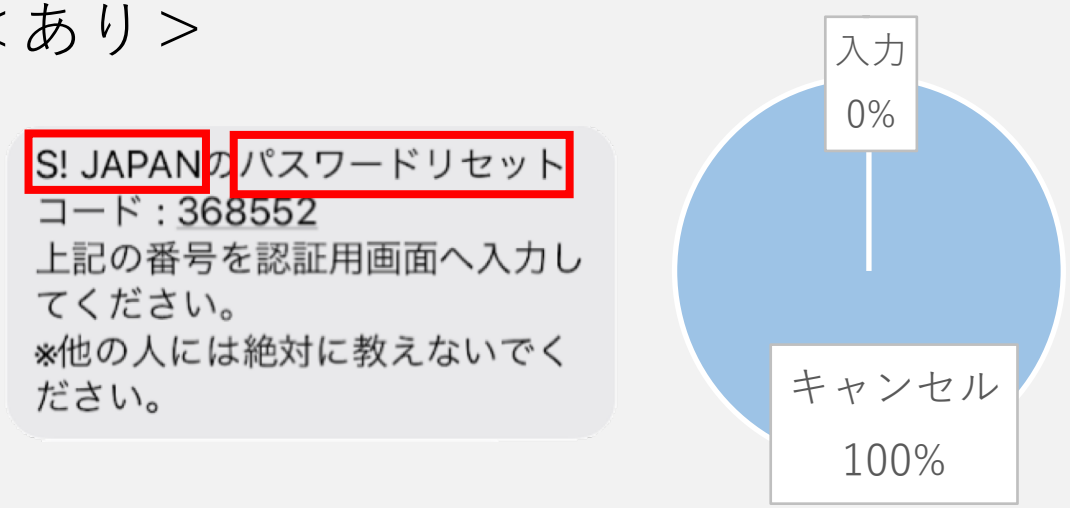


実験結果１（警告の有無）

＜警告なし＞



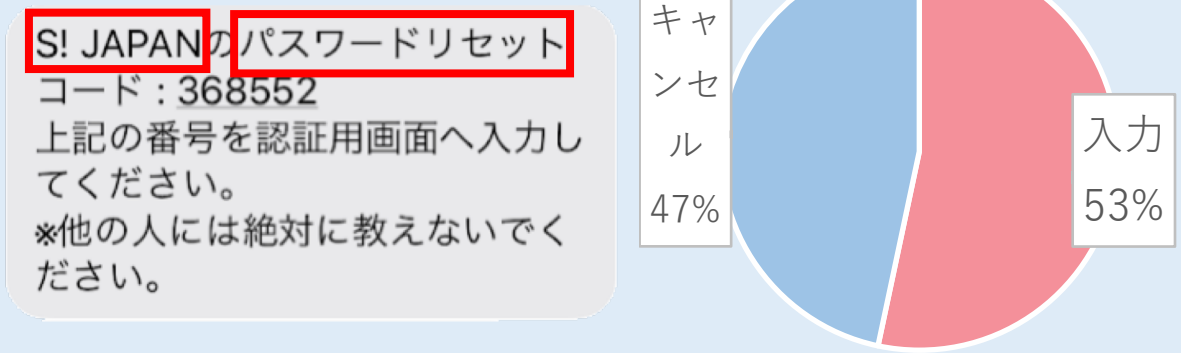
＜あり＞



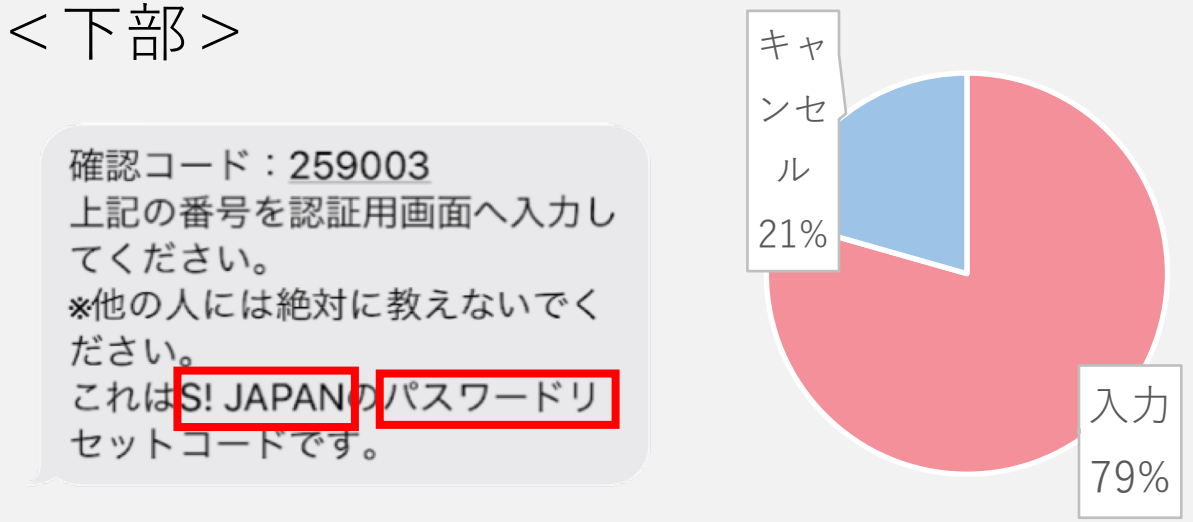
●コードの使用用途の明記は、先行研究通り有効である

実験結果２（上部／下部）

＜上部＞



＜下部＞

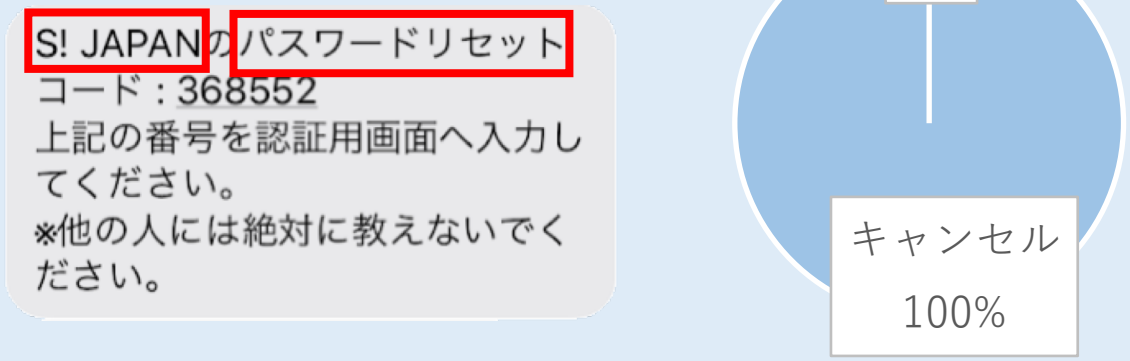


●警告を上部に記載すると，下部の警告と比べて被害が少ない

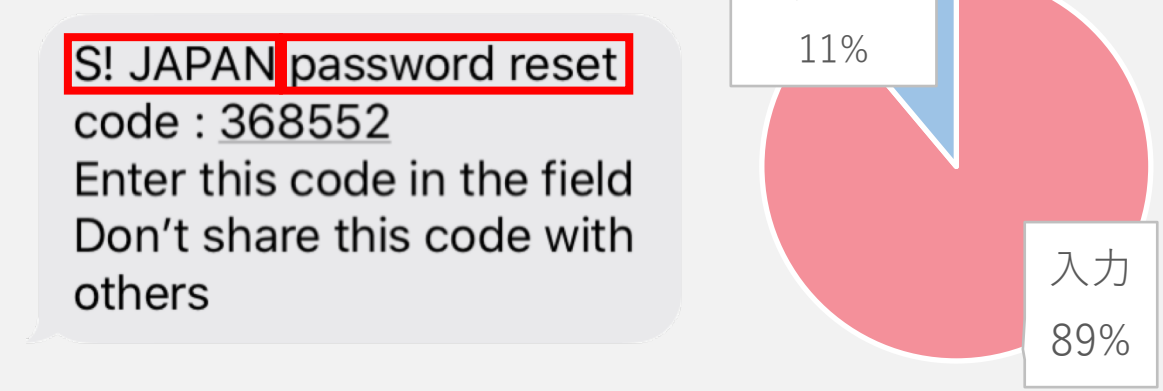
●コードより前や付近に 認証コードの用途を明記することが被害率を下げるために有効

実験結果３（日本語／英語）

＜日本語＞



＜英語＞

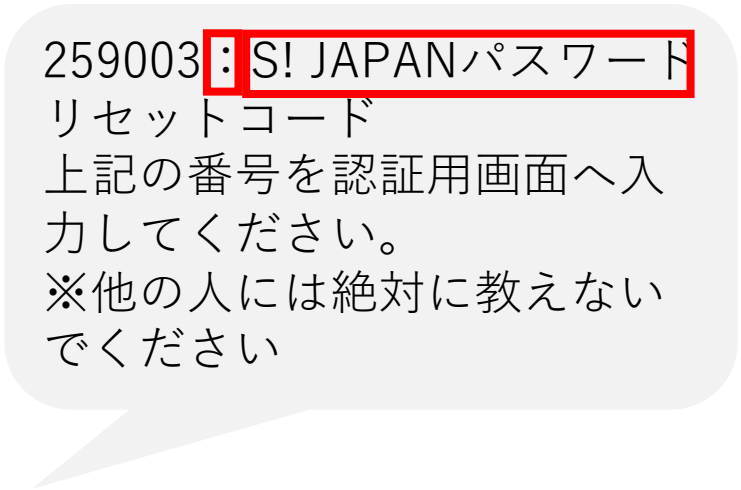


●英語では 89 %がコードを入力してしまったのに対し，
日本語ではコードを入力した者はいなかった

●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

対策

1. 自動入力させない
2. 送信元・用途は上に
3. 海外サイトでも、日本人が使う場合は日本語で



SeBIS（ロジスティック回帰分析の結果）

	質問	e	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	0.953	0.854
7	アカウントごとに違うパスワードを使っている	1.721	0.148
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）	0.462	0.039
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	0.879	0.709
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	1.306	0.576

- 全18問

- 「必要最低限の文字数を超えるパスワードを設定する」人は、攻撃の被害を受けにくい

まとめ

- **通知で見られる位置に**、認証コードの用途および送信元企業名を明記することが被害率を下げるために有効

- **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

- **自動入力されない形式でのコードの明記**が必要