明治大学総合数理学部

2020 年度

卒　業　研　究

アドネットワークにおける広告効果指標の調査

学位請求者　先端メディアサイエンス学科

柴山りな

目次

第 1 章

はじめに

1.1 背景

電通によると [1]，日本の広告は 8 年連続でプラス成長をしている．特にインターネット広告費は 6 年連続 2 桁成長で，テレビメディア広告費を超え，2019 年には 2 兆円を超えている．しかし 2018 年，NHK が，あるまとめサイトに曽於市ふるさと納税の広告が掲載されており，そのサイトで広告料を不正に横取りしていた事件を報道した [4]．これは，広告主 (曽於市) や広告配信業者が，広告がいつどこで掲載されているか知らないことが原因のひとつである．インターネット広告では，広告枠に対する広告の掲載とその効果指標の報告を，全てアドネットワーク業者が行っており，これは従来のメディアとの大きな違いである. アドネットワークが出稿した広告の表示回数を表すインプレッション数とクリックされる割合の水増しを行うという不正が問題になってきている.

そこで本研究では，アドネットワークの掲載する広告とその効果指標の正しさを広告主の観点から調査することを目的とする．代表的なアドネットワークに広告を出稿して，クリックして流入したユーザの数，行動などを PHP で取得することにより，正しく広告が配布されているかを調査する.

第 2 章

アドネットワーク

2.1　インターネット広告

インターネット広告には，広告を出稿する広告主，広告を閲覧するエンドユーザ，広告表示枠を提供するパブリッシャ，広告主とパブリッシャの間を取り持つアドネットワークが存在する．

インターネット広告の仕組みを図 2.1 に示す．まず，エンドユーザがパブリッシャ (Web サイト) を訪れた際 (1)，その Web サイト上に仕込まれたアドタグ（HTML 内の<script>タグなど）がブラウザ上に読み込まれる (2)．その後，アドタグについて実行される JavaScript からアドネットワークに対して広告のリクエストが送られる (3)．この際，アドネットワーク上では，アドビッディングと呼ばれる広告枠の競売が行われる (4)．この競売は，入札者の入札額アドタグについて送信されたパブリッシャの情報 (広告枠のサイズなど) や，エンドユーザの情報 (Cookie，OS バージョンなど) が基準となり，落札される．最終的に，その広告枠を買った広告主の広告が，閲覧しているページに表示される (5)．エンドユーザは，広告をクリックすることで広告主の Web サイトに飛ぶ．同時に，閲覧回数 (インプレッション) や広告クリック回数が評価される．

2.2　先行研究

金井らは，広告不正におけるクリック座標に着目した調査を行った [2]．不正クリックには X 座標が共通で，Y 座標のみが異なるクリックが多く見られたことを報告している.Iqbal らは，クリック詐欺に対する新たな不正検出技術を提案している [3]．従来は主にサーバ側からの調査であり， VPN や匿名ネットワークの場合，不正の検出が難しいため，ユーザ側からの調査が出来る新たな技術を提案した．

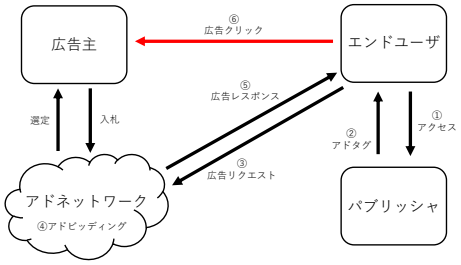

図 2.1　インターネット広告の仕組み

第 3 章

実験

3.1　目的

インターネット広告による集客の実態とアドネットワークによって報告される効果指標の正しさを調査することを目的とする．

3.2　方法

次のように，広告を出稿し，アクセス数・行動などを観測する．2020/11/28 から 2020/12/5 の 7 日間，Google 広告*で図 3.2 のようなディスプレイ広告を出稿した．広告をクリックしたユーザは，図 3.3 の実験用コンテンツページへ遷移する．広告クリックからのアクセスログを PHP で・遷移先コンテンツページでの行動を JavaScript で取得・データベースに格納する．取得した情報の一覧を表 3.1 に示す．

取得したアクセスログの IP アドレスから地域を特定し，地域ごとのアクセス数を取得した．アクセス地域の判別には，MAXMIND 社の GeoLite2-City†のデータベースを利用した．

アクセスしたユーザはコンテンツに興味を持っているのか，クリックがユーザにとって誤操作ではないのかを確認するため，各アクセスの滞在時間とスクロール率を JavaScript で取得した．ページ滞在時間とスクロール率は，0 秒，1 秒，3 秒，5 秒，その後 5 秒ごとに取得した．

スクロール率は，コンテンツ全体の高さのうち，ユーザがスクロールした領域を割合で定める．JavaScript でスクロール量（window.pageYOffset），コンテンツページ全体の高さ（document.documentElement.scrollHeight），ユーザの画面の高さ（document.documentElement.clientHeight）の 3 つの値を取得した（単位：ピクセル）．スクロール率は以下の式で計算される．

$$\text{スクロール率} = \frac{\text{最大スクロール量}}{\text{ページ全体の高さ} - \text{画面の高さ}}$$

スクロール量については，ページ離脱時の値ではなく最大値を採用した．概要を図 3.1 に示す．

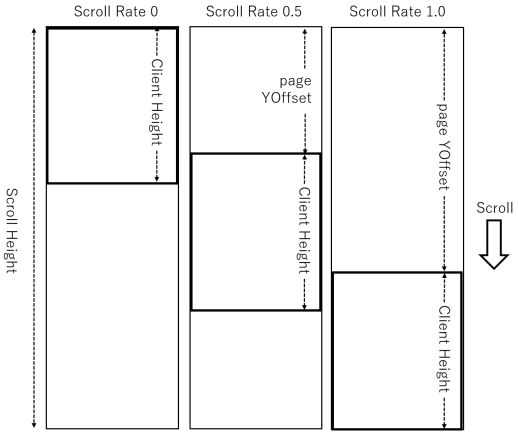

図 3.1　スクロール率の取得指標

表 3.1　取得した情報の一覧

	データの種類
アクセスログ	IP アドレス
	アクセス時刻
	リクエストメソッド
	ユーザエージェント
	リファラー
行動	滞在時間
	スクロール率

図 3.2　実験に使用したディスプレイ広告

3.3　結果

Google 広告に 7 日間出稿した結果を表 3.2 に示す．また，計測したアクセスログの件数とその分析結果を表 3.3 に示す．

*Google 広告, https://ads.google.com/intl/ja_jp/home/
†GeoLite2 City, https://dev.maxmind.com/geoip/geoip2/geolite2/

図 3.3　実験サイト

表 3.2　Google 広告の掲載結果

インプレッション (広告表示回数)	72,756
広告クリック数	303
クリック率	0.42%

表 3.3　Google 広告からのアクセス数と分析

アクセスログ数	414
ボットからのアクセス数	3
推定アクセス数	304

地域ごとのアクセス数を GeoLite2 と Google 広告とで比較した結果を図 3.4 に示す．GeoLite2 では，304 アクセス中 79 件でデータなしという結果になった．GeoLite2 と Google 広告を比較すると，まず地域が特定されているアクセス数が GeoLite2 では 225 であるのに対し，Google 広告は 301 と多い．また，GeoLite2 は海外からのアクセスが合計 26 アクセスという結果であった．

時間ごとのアクセス数を図 3.5 に示す．0 時台が最も多く，12 時から 23 時にかけてが少なかった．

アクセスに使用されたデバイスをユーザエージェントから判別した結果を図 3.6 に示す．iPhone と Android が 9 割以上を占めた．

流入したユーザの滞在時間とスクロール率を JavaScript で取得した結果をそれぞれ表 3.5，3.4 に示す．304 のうち 113 のアクセスでデータが取得できなかった．データが取得できた 191 アクセスのうち 146 で全くスクロールしないまま，ページを離れていることが確認できた．

3.4　考察

3.4.1　広告クリック数とアクセス数の比較

Google 広告でのクリック数が 303 だったのに対し，表 3.3 より観測されたアクセスログ数は 414 であった．Bot からのアクセスの 3 件を除外すると 411 である．

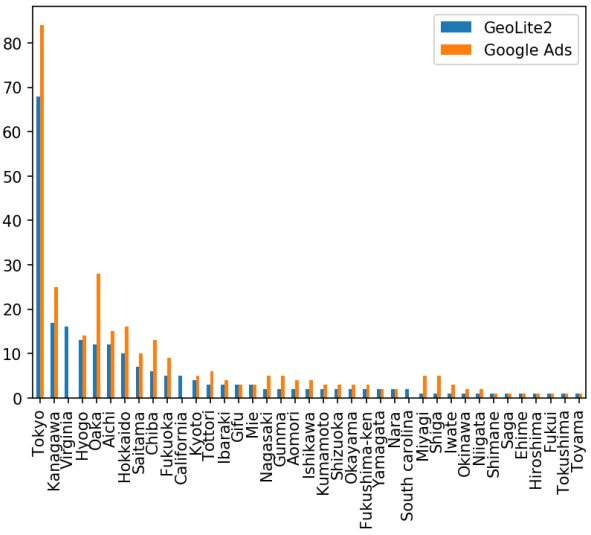

図 3.4　アクセス地域の分布

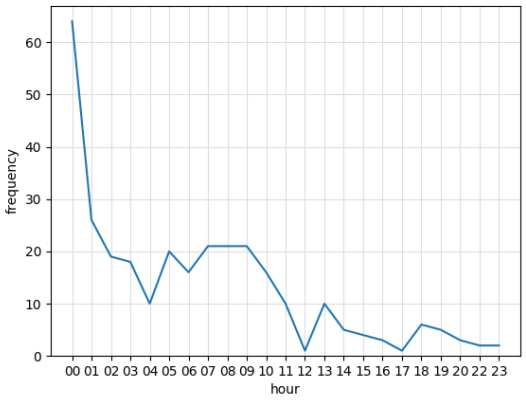

図 3.5　アクセス時間帯の分布

さらに同一 IP アドレスからの 30 分以内のアクセスを 1 として数えると 107 減って 304 となる．この結果は，Google 広告のクリック数と 99.6% 一致する．

表 3.2，3.3 より広告クリック数が 303 だったのに対し，アクセスログ数は 414，ボットと 30 分以内の同一 IP アドレスからのアクセスを除いたアクセス数は 304 であった．同一アクセスと判断する条件を，5 分以内とすると 310，120 分以内とすると 301 となり，いずれにせよ 95% 以上一致する．

3.4.2　アクセスの地域，時刻，デバイス

Google 広告のアクセス地域特定も我々のプログラムと同様 IP アドレスから自動で判定される [5]．したがって図 3.4 より，アクセス数の差は使用する API による誤差であると考えられる．

日本のインターネットの利用時間帯は総務省によると朝 6 時台から 23 時台までが 10% を超える時間帯である [6]．特に 12 時と 20 22 時は 20% を超えて最も利用される時間帯である．しかし本実験でのアクセスの

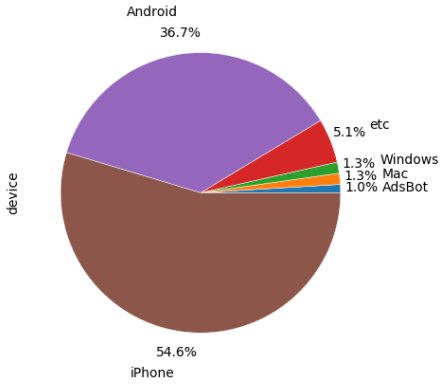

図 3.6　デバイスごとのアクセス数

表 3.4　スクロール率ごとのアクセス頻度

スクロール率	アクセス数
0.0	160
0.1	3
0.2	5
0.3	3
0.4	2
0.5	2
0.6	1
0.7	3
0.8	2
0.9	3
1.0	14

時刻は 0 時台が最も多く，0 時から 11 時にかけてが 10 人以上と比較的多い時間帯であった．よって，広告は必ずしも時間的に均等にユーザに表示されていないと考えられる．

3.4.3　流入したユーザの振る舞い

ユーザの行動を JavaScript で取得したところ，約 37% の頻度で取得に失敗した．原因としては，ユーザが JavaScript をブロックする設定にしていることが考えられる．

取得できた 191 アクセスのページ滞在時間とスクロール率ごとのアクセス分布を表**??**に示す．表の左上 (ページ滞在時間 10 秒以内) は，広告をクリックしたものの求めていたコンテンツと違ったため，すぐに離脱したと考えられる．また，ユーザの意図しない誤操作による広告クリックの可能性もある．逆に，右下は興味を持って最後までコンテンツを読んでいると考えられる．このどちらかや真ん中のようにユーザは振るまうと予想していたが，実際には左下のスクロールはせずにページに長く滞在するユーザが多く見受けられた．

表 3.5　ページ滞在時間ごとのアクセス頻度

滞在時間 (秒)	アクセス数
0	2
1	39
3	14
5	30
10	10
20	16
30	10
40	2
50	3
60	13
90	6
120	6
121 以上	47

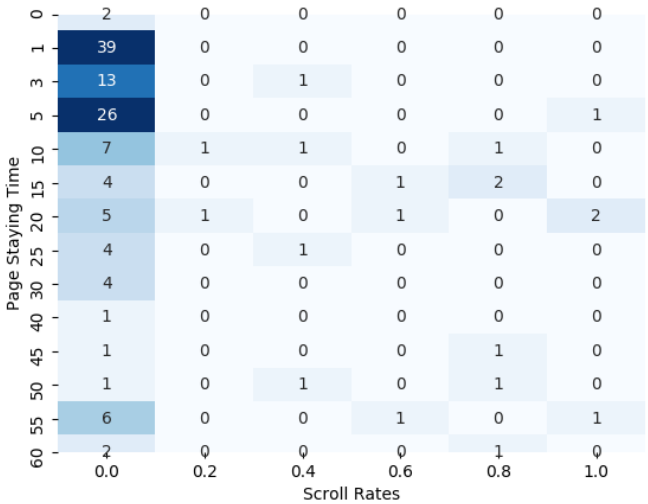

図 3.7　ページ滞在時間 (縦) とスクロール率 (横) ごとのアクセス分布

第 4 章

おわりに

本論文では，Google ディスプレイ広告における広告効果指標の分析を行った．その結果，クリック数とアクセス数は 99.6% 一致した (n = 303)．一方，アクセスしたユーザの 21% が 1 秒以内にページを閉じ，76.4% がスクロールを全くせずにページを閉じていたことが明らかになった．広告がクリックされた時間帯は，0 時 12 時が多く日本のインターネットの利用時間とずれていた．また，アクセス地域は判別に使用する API によってある程度の誤差が生じることも明らかになった．

ただ，広告効果指標からクリックやインプレッションの水増しなどの広告不正について調査するには限界がある．今後は，離脱の理由についてユーザにアンケートの実施など，広告効果指標以外の側面から調査を行う必要がある．

第 5 章

謝辞

本研究を行うにあたり，多くの方より御指導いただきました．特に明治大学総合数理学部先端メディアサイエンス学科，菊池浩明教授に深く感謝申し上げます．共に研究に取り組んでくださった草野くん，予備実験等に協力してくださった菊池研究室の皆様並びに先端メディアサイエンス学科の方々に深く感謝の意を表するとともに，謝辞とさせていただきます．

参考文献

[1] 2019 年日本の広告費，https://www.dentsu.co.jp/knowledge/ad_cost/2019/，2020/12/16 参照.

[2] 金井 文宏，千葉 大紀，高田 雄太，秋山 満昭，八木 毅，波戸 邦夫，”広告ネットワーク上で観測されたユーザアクティビティの分析による広告不正の実態調査”，研究報告セキュリティ心理学とトラスト (SPT) pp. 1-6，No. 17，Vol. 2018-SPT-27，2018.

[3] Md Shahrear Iqbal, Mohammad Zulkernine, Fehmi Jaafar, Yuan Gu, ”Protecting Internet users from becoming victimized attackers of click-fraud”，WILEY，Journal of Software Evolution and Process 2018;30;e1871，2018.

[4] ”もうけは誰の手に?闇に消えるネット広告費”， https://www3.nhk.or.jp/news/special/net-koukoku/article/article_05.html，2020 年 6 月参照.

[5] ”地理データについて”， https://support.google.com/analytics/answer/6160484?hl=ja，2020 年 12 月参照

[6] 総務省，”平成 29 年版 情報通信白書 主なメディアの利用時間帯”， https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc262520.html，2020 年 12 月参照.

[7] ADSTAGE，https://www.adstage.io/，2020 年 12 月参照.

付録 A

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

A.1　はじめに

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近年推奨されている．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(Short Message Service) は携帯電話番号へ短文のメッセージを送信する仕組みであり，多要素認証の代表的な手段として，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，2017 年に SMS 認証を悪用してパスワードを初期化する手法 PRMitM(Passward Reset Man in the Middle) 攻撃が Gelernter らによって提案されている [1]．PRMitM 攻撃は中間者攻撃の 1 種であり，アカウント登録とパスワードリセットの手順が似ていることを利用し，ユーザに勘違いさせアカウントのパスワードを初期化するものである．Gelenter らは，SMS にパスワードリセットであることの警告とサービス名を明記することで，PRMitM 攻撃を防止できると述べている．

しかしながら我々は，近年の機能拡張が著しい SMS に脆弱性があることに気が付いた．それは SMS の冒頭の一部を表示する通知機能である．なぜならば，通知しか見ないで認証コードを入力するユーザには，これらの警告やサービス名が秘匿されてしまうためである．そこで，本稿っではこの仮説を検証するためクラウドソーシングを用いたユーザ実験を行った．

通知による影響を受けやすいように，警告を SMS の上部と下部に記述し，各ケースでの PRMitM 攻撃の被害率を測定する．安全に実験を実施するため，SMS は本物を用いたが，パスワードリセット対象となるサイトは疑似的なサイトを用いた．また，十分な ICT スキルやセキュリティ知識がこの攻撃を防止するのに有効であると予想し，被験者のスキル度合いをアンケートによって評価した．

本稿では，以上の実験結果を示し，被害を広げる要因について考察を与える．また，PRMitM 攻撃を受けないようにする対策について考える．

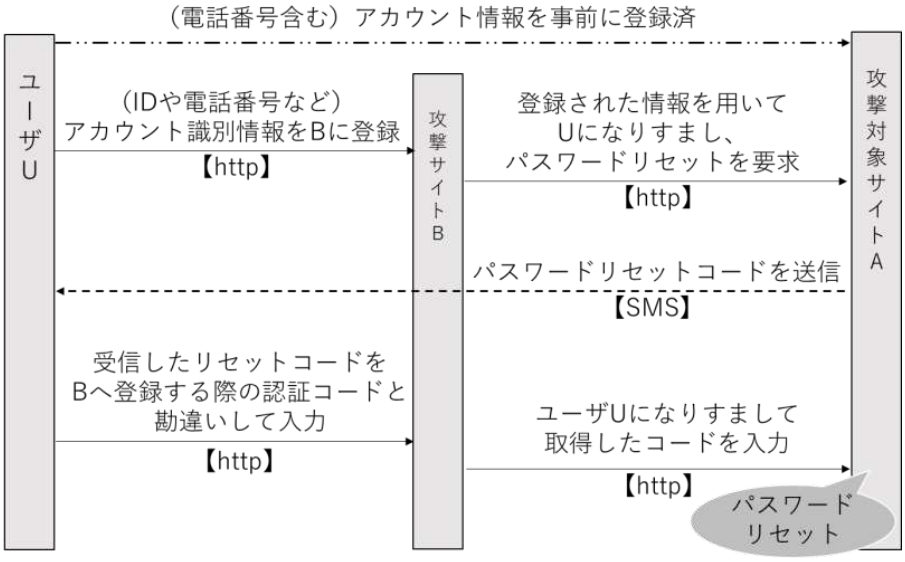

図 A.1　PRMitM 攻撃の流れ

A.2　多要素認証への中間者攻撃

A.2.1　PRMitM 攻撃

PRMitM 攻撃の一連の流れを図 A.1 に示す．ユーザ U 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 U 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 U 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.，こうして B は A に登録されたパスワードをリセットして，U になりすます．

Gelernter らによるとパスワードリセットであることの警告とサービス名を明記することが PRMitM 攻撃に対する基本的な対策である [1]．また，彼らは，リセットコードの替わりに送信元を明記した URL を送ることで，PRMitM 攻撃を受けることがないと主張している．

A.2.2　SeBIS

SeBIS(Security Behavior Intentions Scale) は 2015 年 Serge Egelman らによって開発されたセキュリティ意識の指標である [4].「デバイスの安全確保」,「パスワードの管理」,「Web 使用時の積極的なセキュリティ意識」,「アップデート」の質問に対し，5 段階のリッカート尺度で回答をしてもらい，被験者のセキュリティに対する意識を定量化する．

本稿では，全 16 問を先行研究 [2] を参考に和訳して使用した．

図 A.2　メッセージ開封の例 (iPhone)

A.3　SMS ベース多要素認証の新たな脆弱性

A.3.1　概要

本来，コードを確認するためには，図 A.2 のようにメッセージを**開封**することが一般的である．開封すれば全文に目を通すことになる．しかし，図 A.3 の受信メッセージ**一覧**画面や，図 A.4 のような**通知**機能では，冒頭 1〜2 行のみが送信元電話番号とともに表示される．もし冒頭にコードを，その下に警告とサービス名を記述する場合，利用者はコード以下を読まないため被害を増長させる．

これらの SMS の開示方法を次のように呼ぶ．

開封　メッセージ用のアプリケーションより SMS の全文を閲覧する方法 (図 A.2)

一覧　開封と同様のアプリケーションだが，一覧表示された SMS の文頭数行のみの簡略化された部分のみを確認する方法 (図 A.3)

通知　他のアプリケーション利用中やホーム画面で SMS の受信を通知する短い要約のみを確認する方法 (図 A.4) OS の違いによって要約の方法は変わるが，メッセージの一部のみしか表示されない．

従って，一覧や通知のいずれも，SMS の一部，多くの場合文頭 2 行のみしか表示されない．

登録を PC で行った場合，スマートフォンのロック画面に認証コードが通知される．図 A.5 にあるように，iPhone では SMS 本文冒頭または全体が表示されるのに対して，Android では初期設定では本文は表示されない．

また，現在 iPhone の機能に，SMS に送られてきた認証コードを自動で認識し，ワンタッチで入力できる図 A.6 のような**自動入力**機能がある．キーパッドに表示されたコードをタッチするだけで，SMS 本文を確認する機会すらなく，サービス名や警告を確認せずに入力することができる．以上のように，利便性を向上するために強化された機能の多くが PRMitM 攻撃の被害を増長させる要因になり得る．

A.3.2　通知を悪用した中間者攻撃

しかしながら，本脆弱性が即ユーザアカウントの乗っ取りを招くわけではない．本脆弱性は機種や登録媒体によって振る舞いが異なり，各自のロック画面や通知の設定によっても異なる．注意深いユーザならば攻撃に気が付くかもしれない．1 行か 2 行かの違いや，全文をロック画面で確認するかメッセージを開封して確認するかといった機種間の細かい違いによって，PRMitM 攻撃の被害に影響を与えるかもしれない．

図 A.3　受信メッセージ一覧の例 (iPhone)

表 A.1　実験で行われるサイト登録の概要

	登録サイト名	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

十分なセキュリティ意識があれば，SMS 本文の確認・コードの入力を適切に丁寧に行い，この攻撃を受けないことも予想される．逆に年配者などの，スマートフォンを使いこなせない人は，より被害を受けやすいだろう．

そこで本研究では，被験者 81 人を用いた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 SMS の機能やユーザのセキュリティ意識が PRMitM 攻撃の被害に及ぼす影響を明らかにすることを試みる．

A.4　ユーザ実験

A.4.1　目的

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とともに被害者の特性を調査することを目的とする．

A.4.2　方法

クラウドソーシングサービス「クラウドワークス」*と「ランサーズ」†を利用して被験者 81 人 (男性 44 人，女性 37 人) を用いた SMS 多要素認証による架空ウェブサイトへの登録実験を行う．実験に使用したウェブサイトの例を A.7 に示す．サイト登録は合計 3 回行われ，その都度，「登録フォームは使いやすかったか」，「セ

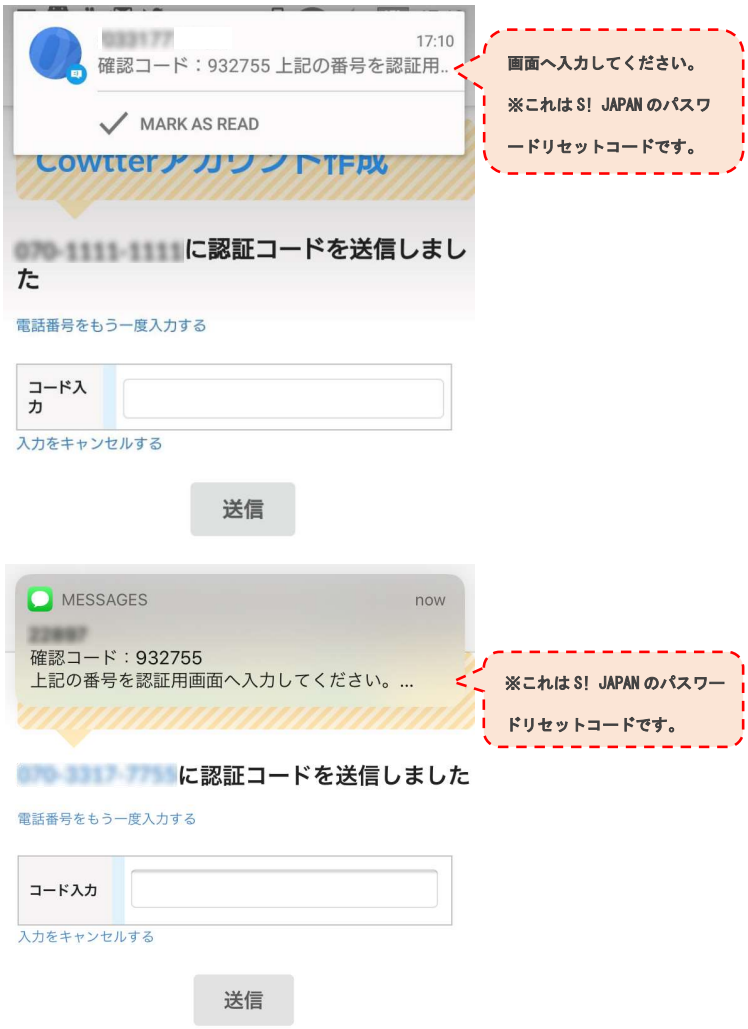

図 A.4　通知の例（Android(上)，iPhone(下)）

キュリティに関して安心できると感じたか」などの質問に回答する．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)[4] と，コンピュータスキルを測る 3 つの問いに回答する．

3 回の登録の概要を表 A.1 に示す．1 回目は情報の登録のみ，2 回目は情報の登録と SMS 認証を実施する．実験サイトから被験者への SMS メッセージ送信には「Twilio」‡を用いた．3 回目では 1 回目のサイトの登録サイトへの PRMitM 攻撃を実施する．ここでは，情報を登録したのちに 1 回目の S!JAPAN のサイトからパスワードリセットコードが送信される．被験者には，もしも登録に疑わしい点があればキャンセルすること事前に指示しておく．ここで図 A.8 に定められる 5 つの被験者グループに異なる条件の SMS メッセージを送り，被害要因を調査する．

A.4.3　被害者の定義

3 回目の登録時，本来ならば SMS 本文を読み，サイト名の相違やパスワードリセットコードであることに矛盾を感じるはずである．被害を受けないためには，選択肢として与えられている「入力をキャンセルする」

図 A.5　ロック画面での SMS メッセージ受信通知の例（Android(左)，iPhone(右)）

図 A.6　自動入力の例 (iPhone)

を選ぶべきである．しかし，SMS 本文を読まないと，このコードを登録時の認証コードと勘違いして入力してしまう．

Majebook の新規登録の手順の途中であるにも関わらず，S! JAPAN の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．その条件の，被害者が占める割合を**被害率**とする．例えば，type0 の SMS を受け取った被験者は 19 人，そのうちコードを入力してしまった人は 14 人なので被害率は $R = 14/19 \cdot 100$ と計算される．

図 A.7　実験に使用した 3 サイトの登録画面

	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 passward reset code from S! JAPAN

図 A.8　5 つの SMS 本文

A.4.4　結果

実験で送信した SMS の特徴の概要と被害率を表 A.3 に示す．type3 と 4 が type0，2，3 と比べて被験者数が少ないのは，同じ人数の被験者を type0 5 に振り分けたが，SMS が原因不明のエラーによって送信されなかった事例が多かったためである．

デバイスごとの被害率と独立性の検定の結果を表 A.4 に示す．デバイスのユーザーエージェントを元に分類した．アンケートでも機種を回答してもらったが，ユーザーエージェントと一致していない被験者が 2 名見受

*クラウドワークス, https://crowdworks.jp/
†ランサーズ, https://www.lancers.jp/
‡Twilio, https://twilio.kddi-web.com/

表 A.2　各サイトの使用感と安心感の平均点と標準偏差

サイト名	使いやすいか		安心できるか	
	平均	SD	平均	SD
S! JAPAN	4.07	1.70	5.78	1.12
Cowtter	5.91	1.08	4.95	1.61
Majebook	5.72	1.33	4.22	1.94

表 A.3　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	14	19	73.7
1	あり（下部）	日本語	15	19	78.9
2	あり（下部）	英語	16	20	80.0
3	あり（上部）	日本語	0	7	0.0
4	あり（上部）	英語	10	16	67.9

表 A.4　デバイス種類ごとの被害率と検定結果

デバイス	入力	全体	被害率	χ	p 値
iPhone	21	30	70.0	3.11	0.37
Android	23	31	74.2		
PC	11	20	55.0		

表 A.5　デバイス種類ごとの被害率と検定結果

デバイス	入力	全体	被害率	χ	p 値
iPhone	5	8	62.5	0.75	0.94
Android	4	9	44.4		

けられた．自分の機種を正しく把握していない場合があると判断して，ユーザーエージェントを採用した．また，PC で登録した人の使用したスマートフォンの機種ごとの被害率と検定結果を表 A.5 に示す．SMS の受信に使用した機種は，アンケートの回答結果をもとに集計した．

登録した架空の 3 サイトに対する使用感と安心感の平均点とそれぞれの標準偏差 (SD) を表 A.2 に示す（1：とても安心できない／とても使いにくい，7：とても安心できる／とても使いやすい）．標準偏差はすべての項目で 2 以下と小さいが，サイトごとに差は見られなかった．

被害を受けなかった人が，入力の取止をした理由の人数を表 A.6 に示す．取止の理由についてはサービス名の相違が最も多かった．

良く知られたサービス／初めて見つけたサービスでの電話番号の入力に抵抗があるか回答してもらった結果を表 A.7 に示す．

コードの確認及び入力方法別の被害率を表 A.8 に示す．方法の特定はアンケートによる自己申告である．最

表 A.6　入力取止の理由

理由	人数
メッセージの内容がよくわからなかったから	7
S! JAPAN と書いてあったから	11
パスワードリセットと書いてあったから	6
信用できないサイトだから	1
メッセージが英文だったから	1

表 A.7　電話番号入力への抵抗感の平均点と標準偏差 (1:とても抵抗がある 7:完全に抵抗はない)

	入力	取止	SD
良く知られたサイト	4.02	3.73	1.79
初めて見つけたサイト	2.65	2.27	1.52

表 A.8　入力・確認方法ごとのリセット被害率と検定結果

	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		

表 A.9　属性ごとの被害率と検定結果

	分類	入力	全体	被害率	χ	p 値
性別	男性	32	44	72.7	1.03	0.319
	女性	23	37	62.2		
年齢	20 未満	0	1	0.0		
	20 代	14	17	82.4		
	30 代	14	28	50.0	13.26	0.021*
	40 代	15	22	68.2		
	50 代	8	9	88.9		
	60 以上	4	4	100.0		

も一般的なコードの入力方法は手入力，コピー＆ペースト，自動入力のうち手入力で，81 人中 64 人であった．確認方法は開封（メッセージ全文を表示），一覧（受信 SMS 一覧画面），通知（画面上部のバナー通知），その他から選択回答してもらった．主な確認方法は，「開封」が 81 人中 40 人と「通知」が 30 人に分かれた．入力方法・確認方法ともに「その他」が 1 人であった．

性別・年代ごとの被害率を表 A.9 に示す．年代別に見ると 20 代と 50 代以降では被害率が 8 割を超えて

表 A.10　スキルを測る 3 つの問いと平均点と標準偏差

	質問	入力	取止	SD
1	自分で OS をインストールしたことがありますか	1.51	1.50	0.61
2	自分でネットワークを構築したことがありますか	1.18	1.23	0.40
3	自分でウェブページを作ったことがありますか	1.24	1.23	0.42

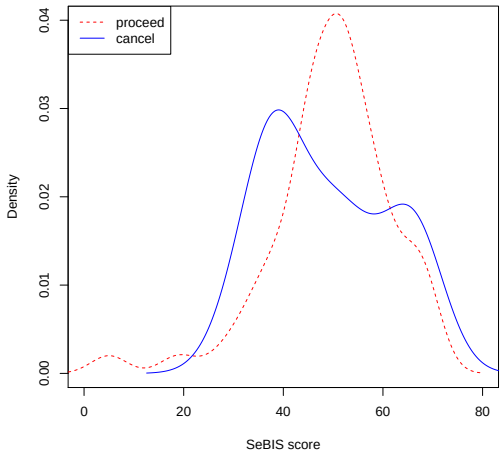

図 A.9　入力／キャンセル別の SeBIS 点数分布図

いた．

スキルを測る 3 つの問いと平均点，標準偏差を表 A.10 に示す．アンケートは「ある」(2 点),「ない」(1 点),「対象物が何かわからない」(0 点) から選択する形式である．

SeBIS の質問文を表 A.11 に示す．回答は 5 段階と回答しないの 6 つから選択する方式である（0:回答しない 1:まったくそうでない 5：いつもそうしている）．

A.4.5　分析

SMS の特徴ごとの独立性の検定を自由度 1 のカイ 2 乗検定で行った結果を表 A.12 に示す．∗ を有意水準 10 % ($p < 0.1$)，∗∗∗ を有意水準 1 % ($p < 0.01$) とする．警告あり／なし，日本語／英語，警告の位置が上部／下部でいずれも有意差 ($p = 0.001$，$p = 0.005$，$p = 0.04$) が認められた．警告ありに type3 のみを採用したのは，type1 で下部に警告した場合，警告自体が読まれておらず，警告なしの場合との差が表れないと判断したためである．同様の理由で，日本語／英語で Type1+3，2+4 とせず Type3 と 4 のみを採用した．

コードの確認及び入力方法別の独立性の自由度 2 のカイ 2 乗検定結果を表 A.8 に示す．入力方法・確認方法による有意差はいずれにも認められなかった ($p = 0.428$，$p = 0.418$).

性別・年代ごとの被害率と独立性の検定の結果を表 A.9 に示す．独立性の検定の結果，性別では有意差はな

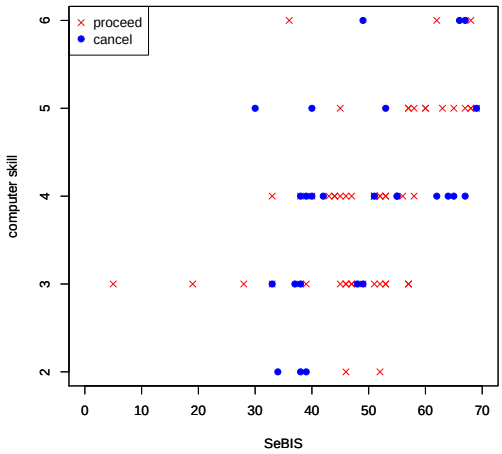

図 A.10　SeBIS とコンピュータスキルと PRMitM 攻撃被害の散布図

かったが ($p = 0.319$)，年代では有意水準 5 %での有意差が認められた ($p = 0.021$).

デバイスごとの被害率を独立性の自由度 2 のカイ 2 乗検定の結果，表 A.4 より，iPhone，Android，PC 間で統計的な有意差は見られなかった ($p = 0.374$).

セキュリティ意識 (SeBIS) とコンピュータスキルを，それぞれ 0-80 点，0-6 点で評価した．SeBIS とスキル値の散布図で図 A.10 に示す．SeBIS とスキルの合計点の統計量と Weltch の検定結果を表 A.13 に示す．検定の結果，SeBIS の合計点，スキルの合計点ともに入力した被験者とキャンセルした被験者の平均に有意差は見られなった．

また，SeBIS 合計点の点数分布を図 A.9 に示す．入力とキャンセルの間で特筆すべき差は見受けられなかった．

SeBIS の各質問と合計点を説明変数，入力／キャンセルを目的変数としてロジスティック回帰

$$\log \frac{p}{1-p} = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_{19} x_{19}$$

を行った結果を表 A.11 に示す．各質問の回答を「はい」「いいえ」の 2 つに分け，合計点は 50 点以下と 51 点以上に分けて分析を行った．結果，SeBIS の合計点が 51 点以上の 50 点以下に対する調整済オッズ比 OR は

$$\frac{\text{合計点高い人の被害率/合計点高い人のキャンセル率}}{\text{合計点低い人の被害率/合計点低い人のキャンセル率}} = \mathrm{e}^{-2.487} = 0.083$$

で有意であった ($p = 0.032$)．50 点以上の被験者は 50 点以下と比べて被害を受けるオッズが 1/10 以下に減少する．また，「コンピュータから離れるとき，手動で画面をロックする」人のそうでない人に対するオッズ比 $OR = \mathrm{e}^{-1.964} = 0.140$ で，被害を受ける確率のオッズが 1/7 程度に減少する ($p = 0.024$)．それ以外の項目に有意差は認められなかった．

SMS のタイプ，被験者の属性等多くの要因のうち，攻撃の被害を受ける要因を明らかにするため，ロジスティック回帰を行った．目的変数を入力／キャンセル，説明変数を SMS のタイプ（警告有無 x_1，警告上部 x_2，警告下部 x_3，言語 x_4），3 つのウェブサイトについての使用感 $x_{1,1}$,$x_{2,1}$,$x_{3,1}$，安心感 $x_{1,2}$,$x_{2,2}$,$x_{3,2}$，SeBIS，スキ

ル値の合計点 x_{s1},x_{s2}，アンケートの各質問に対する回答 x_{q1},x_{q2},$x_{q3}\ldots x_{q7}$ とした．結果を表 A.14 に示す．警告位置が上部と日本語のとき調整オッズ比はそれぞれ $e^{-6.673} = 0.0013$，$e^{-4.776} = 0.0084$ となり，被害を受けにくいことが明らかになった．

A.5 考察

A.5.1 SMS メッセージの特徴

表 A.12 より，警告あり／なしでは被害率に有意差が認められた．このことから先行研究通り警告とサービス名の明記は有効であるといえる．

警告を上部に記述すると，下部に比べて被害が少なかった．コードより前に認証コードの用途・サービス名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．

SMS が英語では 16 人中 10 人がコードを入力したのに対し，日本語では 7 人中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．ただし，SMS が英語であること自体に違和感を覚え入力しなかったユーザも 1 名見受けられた．コードの用途や警告が明解であるときのみ，その記載が有効になると考える．

A.5.2 確認・入力方法と被害の関係

表 A.8 より，実験内での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．「自動入力」の場合，SMS 本文を確認せずにワンタッチでコードが入力されるため全員が入力すると予想していたが，6 人中 4 人が入力するにとどまった．自動入力際にも，画面上部の通知を併せて確認しているユーザもいると考えられる．

表 A.8 より，認証コードを「開封」,「一覧」,「通知」で確認することによる有意差は認められなかった．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)，一覧や通知ではメッセージの冒頭 2 行のみが表示され，全員が被害を受けると予想していた．しかし被害率は一覧・通知で 54.5 %，75.9 %にとどまった．原因としては，被験者は実際には「開封」して全文を確認していてもアンケートでは「一覧」と回答していることが考えられる．アンケートでの確認方法の選択肢の説明として開封を「メッセージ確認画面を開き，メッセージを開いた 」，一覧を「メッセージ確認画面を開いた（開封はしない)」，通知を「画面上部に表示される通知を見た」と文章で表現したため，我々の意図通りに解釈していない可能性があるためである．

A.5.3 属性

表 A.9 より，年代間では，20 代・50 代以上で被害率が高かった．20 代では認証コードの入力への慣れ，50 代以上では SMS 認証のコード入力自体に気を取られていることから，SMS 本文への注意が薄く，指示通りに素直にコードを入力している可能性がある．

A.5.4 デバイス

表 A.4 より，iPhone，Android，PC 間では，被害率に統計的有意差は見られなかった．図 A.4 のように SMS メッセージが画面上部に通知される際，iPhone では文頭 2 行が表示されるのに対して，Android では文頭 1 行のみが表示される．デバイス間で違いが見られないことから，通知で表示される情報の量は被害率に影響を与

えないと考えられる

また，表 A.5 より，PC を使用して回答した場合，SMS メッセージ受信に使用した機種が iPhone と Android とで被害率に有意差は見られなかった．ロック画面で SMS を確認する場合，iPhone では全文または冒頭 2 行が表示されるのに対し，Android では本文は表示されない．Android の場合，メッセージを開封する必要があるので，被害率は低くなると予想したが，有意差は見られなかった．

A.5.5　セキュリティ意識とコンピュータスキル

図 A.10 より SeBIS とスキルの間にはゆるく正の相関が見られるが，被害（proceed）は広く分布しており，セキュリティ意識・スキルと被害率は独立であると考えられる．また，表 A.13 の Weltch の検定結果でも，SeBIS とスキル値の合計点の平均に有意差は見られなかった．セキュリティ意識や ICT が高ければ被害を受けにくいと予想していたが，どちらも被害に影響を与えないという結果になった．

A.6　対策

PRMitM 攻撃を防止する 3 つの対策を提案する．

1 つ目は自動入力させないことである．確認したところ，SMS 本文で「:」の後にコードがあるとコードと認識されて自動入力機能が使用される．そこで，**パスワードリセットコードに限り，「：」を使わない**フォーマットを用いてコードを送信することを提案する．

2 つ目は送信元のサービス名・コードの使用用途を**メッセージ上部に明記する**ことである．下部に書いた場合，ユーザは読み飛ばしているというよりも目に入ってすらいない可能性があるからである．

3 つ目は，**本文をできるだけ明瞭にする**ことである．ユーザは SMS 本文をほんの数秒しか見ずにコードを入力している．したがって，その短い間に理解できる内容にすることが，メッセージを伝えるのに有効であると考える．

A.7　おわりに

本論文では，送信されたコードを SMS 文頭に表示する通知機能は，SMS 多要素認証を悪用して，アカウントを乗っ取る脅威があることを示した．ユーザ実験の結果，警告を下部に明記すること・英語であることは攻撃に対する被害を増加させること，警告の有無・記述位置・言語の各要因が攻撃に対する被害率に影響を与えることを示した．一方コードの確認・入力方法は被害率に大きな影響を与えない．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．

A.8　参考文献

[1] Nethanel Gelernter，Senia Kalma，Bar Magnezi，Hen Porcilan，“The Password Reset MitM Attack”，IEEE Symposium on Security and Privacy (SP)，pp. 251-267，2017.

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，2018.

Kota Sasa，Hiroaki Kikuchi，“Impact Assessment of Password Reset PRMitM Attack with Two-Factor Authen-

tication”，IEEE Conference on Dependable and Secure Computing，pp.90-97，2018.

Serge Egelman，Eyal Peer， “Scaling the Security Wall Developing a Security Behavior Intentions Scale (SeBIS)”，ACM Conference on Human Factors in Computing Systems，pp. 2873-2882，2015.

Kota Sasa，Hiroaki Kikuchi， “Impact Assessment of Password Reset PRMitM Attack with Two-Factor Authentication”，Journal of Internet Technology，vol. 20，no. 7，pp. 2297-2306，2019.

表 A.11　SeBIS 質問文とロジスティック回帰分析

	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*
4	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	0.550	0.482
5	必要があるときしかパスワードを変更しない	0.540	0.397
6	質問にきちんと答えていることを確認したいので，いつもするを選んでください	-	-
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
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）	0.714	0.676
9	必要がない場合は，パスワードに特殊文字を含めない	0.509	0.363
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
11	どのサイトに訪れたかを URL ではなくサイトの外観と雰囲気で判断している	1.735	0.375
12	安全に送信されることを最初に確認せずに，ウェブサイトに情報を送信する	1.804	0.429
13	リンクをクリックする前にマウスカーソルをリンクに乗せ，訪れる URL を確認する	1.406	0.614
14	セキュリティ上の問題が発見されても誰かが直すだろうからそのまま使い続ける	0.659	0.576
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	1.149	0.840
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
17	この質問の回答として，いつもしているを選択してください	-	-
18	自分のアンチウイルスソフトウェアが定期的に更新されていることを確認する	0.409	0.304
	合計点	0.083	0.032*

表 A.12　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	15	20	75.0	11.81	0.001***
3	警告有	0	7	0.0		
3	日本語	0	7	0.0	7.74	0.005***
4	英語	10	16	62.5		
3+4	上部	10	23	43.5	8.37	0.004***
1+2	下部	31	39	79.5		

表 A.13　SeBIS とスキルの合計点の統計量

	平均値		SD	t 値	p 値
	入力	取止			
SeBIS	49.6	48.8	12.0	0.132	0.896
スキル	3.93	3.96	1.01	-0.266	0.792

表 A.14　ロジスティック回帰分析

	Estimateβ	Std. Error	z value	$Pr(>\|z\|)$
(Intercept)	8.082	5.521	1.464	0.143
x_2	-6.673	2.440	-2.734	0.006***
x_3	-2.244	1.444	-1.554	0.120
x_4	-4.776	1.674	-2.853	0.004***
$x_{1,1}$	-1.381	0.714	-1.934	0.053*
$x_{1,2}$	0.617	0.394	1.569	0.117
$x_{2,1}$	2.372	0.930	2.550	0.011*
$x_{2,2}$	-1.303	0.445	-2.931	0.003***
$x_{3,1}$	-1.294	0.508	-2.546	0.011*
$x_{3,2}$	0.792	0.286	2.766	0.006***
x_{q0}	0.993	0.504	1.971	0.049*
x_{q1}	-2.283	1.254	-1.821	0.069*
x_{q2}	-1.604	0.785	-2.042	0.041*
x_{q3}	0.918	0.686	1.338	0.181
x_{q4}	-0.309	0.561	-0.551	0.582
x_{q5}	-0.344	0.356	-0.968	0.333
x_{q6}	0.643	0.396	1.626	0.104
x_{q7}	3.583	1.773	2.021	0.043*
x_{s1}	-0.043	0.058	-0.749	0.454
x_{s2}	0.302	0.576	0.525	0.600