ユーザ属性セキュリティ意識と国の違いによる多要素認証方式の志向性の調査

小池 蒼葉 †

明治大学総合数理学部 先端メディアサイエンス学科 菊池研究室 †

1 はじめに

今日, インターネット上のサービスのアカウントの認証方式は, セキュリティ強化を目的として 2 つ以上の認証方式を組み合わせた多要素認証が主流である. その要素には, パスワードなどの知識情報, 携帯電話などの所持情報, 指紋や静脈などの生体情報が挙げられる. 中でも多く採用されているのが知識情報である. これはパスワードと何かしらを組み合わせた二要素認証である. 明治大学のメールシステムである Meiji Mail も学外からのサインインの際の認証方式として採用している.[1] 第一要素として ID とパスワード, 第二要素としてモバイルアプリ, または, SMS で送信される認証コード, 電話メッセージを使用することができる. これらの第二要素は, 所持情報である.

しかし, この多要素認証の脆弱性を悪用してパスワードを初期化する PRMitM(Passward Reset Man in the Middle) 攻撃が Gelernter らにより提案されている. [4] PRMitM 攻撃は, 中間者攻撃であり, アカウント登録とパスワードリセットの手順の類似性を利用してユーザのパスワードを初期化する.[5] 一方, モバイルアプリでの認証は SMS コードを使用しないため中間者攻撃の恐れが無い. 従って, Meiji Mail の 3 つの認証方式の中ではアプリ認証を推奨すべきであると考えるが, 現状は SMS 認証の利用が多い. また, 人の特性の中でも居住国とセキュリティ意識の差や多要素認証方式の関連性があるのではないかと推測する.

そこで, Meiji Mail のサインイン方式の利用の実態と, 人の特性やセキュリティ意識との関連性について調査し, 利用の理由を明らかにする. アプリ認証を推奨するための必要な条件を探る.

本研究の目的は, 多要素認証方式の選択に人の属性とセキュリティ意識がどう関連するかを考察することである. Meiji Mail における調査に加えて, 任意のインターネットサービスの認証方式について国の違いとセキュリティ意識, 認証方式の人気度の関連性を調査する.

†Kikuchi Laboratory, Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University.

2 先行研究

2020 年に野口らは, [2] において“レベル分けによる多要素認証の要否の実現と認証連携の拡張”を発表した. 統合認証基盤における認証の要を Active Directory Federation System から Azure Active Directory へ更新し, 多要素認証をもともと使っていた Office365 の他にも Shibboleth 環境でも可能とし, 対象サービス等によりレベル分けされた多要素認証の要否の制御も可能とする多要素認証システムを構築した. また、同時にネットワーク接続時の認証を認証 s 連携の対象とする拡張おも行った. 結果としては, レベル分け多要素認証を実現でき, 有線ネットワーク接続時の認証をシングルサインオンの対象とすることに成功した. 多要素認証方式の選択状況において, SMS での認証が圧倒的に多かったことを示した.

2023 年に Lyastani らは, [3] において “A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites”を発表した. トップクラスのウェブサイトにおける二要素認証のユーザジャーニーの外部的, 機能的一貫性に関する体系的研究である. 対象のウェブサイトは最低限のデザイン面は一貫して実装されているが, 第二要因の設定や使用については, 多種多様なデザインパターンを示しているとし, 2FA 実装者のためのより一般的な UX ガイドラインを提唱した. また, 2FA のユーザジャーニーに関する新な研究課題を提示した.

3 多要素認証の利用調査

3.1 Meiji Mail 多要素認証の種類

Meiji Mail は学外からのサインインに多要素認証を採用している. 第一要素として ID とパスワード, 第二要素としてモバイルアプリ, SMS で送信される認証コード, または電話メッセージがある. 電話メッセージでの認証は主流ではないため, それ以外の 2 つが主に使われている. SMS コードとモバイルアプリ (Microsoft Authenticator) の認証の使用感の違いを調べるために, 複

数回自身でサインインをし時間を計測した. 結果, メールアプリ (Out look) を使用の場合はアプリの方がより速くサインインをすることができ, ブラウザ (safari) を使用の場合は SMS コードの方がより速いことが分かった. タイムの差はいずれの場合も約 10 秒ほどであった.

3.2 方法

本研究は Google Form を用いたアンケートによって行った. アンケート項目は, 性別や年齢等の基本情報とセキュリティ志向度指標 SeBIS の質問と多要素認証の認証方法についての質問で構成されている. 実験は Meiji Mail のアカウントを持つユーザ間での比較を対象にしたものと, 国外の人を対象にしたものの 2 種類である. Meiji Mail のアカウントを持つユーザには, 多要素認証の認証方法の質問にて Meiji Mail の認証方式についてのものと, それ以外のスマートフォンを使用した多要素認証について尋ねた. 質問項目について, Meiji Mail のものについては採用している認証方式やその選択理由, それ以外のものについては最も利用頻度の高い認証方式や中間者攻撃の認知等である. また, 国外の被験者にはスマートフォンを使用した多要素認証についての質問に限定した. 質問項目について, 最も利用頻度の高い認証方式や中間者攻撃の認知等である.

3.3 SeBIS

SeBIS は Serge Egelman らが提案したセキュリティ志向度の指標である. この尺度は, 一般的なセキュリティに関するアドバイスに対するユーザが従う程度の治療値である. 「ほとんどのユーザに適用可能なセキュリティ行動」と「広く受け入れられているセキュリティ行動」 に大別し質問で構成されている. それぞれの質問は肯定的な表現と否定的な表現を混ぜながら作られており, 5 段階のリッカート尺度 ([強くそう思わない] から「強くそう思う」) で回答される. 表 1 で示す Meiji Mail ユーザを対象に行った実験で用いた質問項目は, 笹らによって [6] 和訳されたものである. また, 表 2 で示す国外の人を対象にした実験で用いた質問項目は, それらをそれらを再度自身で英訳したものである.

4 Meiji Mail のユーザを対象にした調査

4.1 概要

本調査は Meiji Mail のアカウントを持つ 57 名のユーザを対象に行った. ユーザの基本情報を表 3 に示す. アンケート項目は基本情報に加えて, SeBIS(セキュリティ志向度指標), Meiji mail の多要素認証, Meiji mail 以外のスマートフォンを使用した多要素認証の各々について計 4 種類から成る. 人の特性やセキュリティ意識と多要素認証方式の関係について明らかにする.

4.2 セキュリティ意識と属する学部の関連について

取り扱う学業柄, 総合数理学部の学生はセキュリティ意識が他の学部生と比べて高いのではないかと考えた. これについて, 総合数理学部とその他の学部別の SeBIS の合計得点の箱ひげ図を表 1 に示す. この箱ひげ図から, 総合数理学部のものの方がデータの範囲が広いことや外れ値があることが分かる. 総合数理学部は最大値が 67, 最小値が 34 で 2 つの外れ値をデータ範囲が 33 であるのに対し, その他学部の最大値は 58, 最小値は 38 でデータ範囲は 20 である. よって, 総合数理学部の方がその他学部よりも 13 点データ範囲が広い. 一方, 平均得点, 中央値はそれぞれ総合数理学部が 49.7, 45.5 でその他学部が 47.5, 46 とあまり違いが見られない. これらのことから, 総合数理学部には著しくセキュリティ意識が高い人が一定数いるが, それらを除くと他学部の人とさほどセキュリティ意識に差は見られないことが分かる.

4.3 認証方式の人気度・セキュリティ意識との関連

セキュリティ意識が高い人は認証方法でモバイルアプリを選択するのではないかと予測した. 背景には, 第一章で述べたように SMS コードによる認証は中間者攻撃の恐れがあることから安全性が無いことが提起されているため, その存在を知っている人はアプリを選択すると考えられたことがある. Meiji Mail の認証方式の人気の割合を図 2 で示す. SMS コードが 40 人で全体の 70.2%, モバイルアプリが 17 人で 29.8% と SMS コードがより人気であった. また、図 3 には認証方法ごとの SeBIS の得点分布を箱ひげ図で示す. このグラフから, モバイルアプリのものの方が全体的なデータの値が高いことが分かる. SMS コードのものの外れ値を除く最大値は 58 で最小値は 34, 平均値は 47 であるのに対し, モバイルアプリのものは最大値が 77 で最小値が 41, 平均値が 52 とより高得点を記録している. このことから, モバイルアプリ使用者の方が SMS コード使用者よりも高いセキュリティ意識を持つ人が多いことがわかった.

4.4 考察

本実験結果より, 学部とセキュリティ意識の関連は見られなかったが, 認証方式の主流が SMS コードである中で, セキュリティ意識が高い人ほどモバイルアプリでの認証を傾向がわかった. しかし, 中間者攻撃の存在を知っている人が必ずしもモバイルアプリでの認証を選択しているわけではないため, また別の理由からアプリを選択している可能性が考えられる. また, 各認証方法を初期設定時に選んだ理由を表 5 と表 6 に示す. 表 5 から SMS コードの選択理由は“馴染みがある”ことや“他の方法を知らない”ことが多いことが分かる. また, 表 6 からモバイルアプリの選択理由は“他の方法を知らない”ことが多く, “馴染みがある”ことはあまり多くないことが分かる. これらのことから, SMS コードでの認証が主流であることは慣れ親しんでいることが大きな要因となり, モバイルアプリでの認証を試すことを妨げているのではないかと考えられる. よって, モバイルアプリでの認証を増やすためには, 様々な人気ウェブサイトやツールがモバイルアプリでの認証を推奨することが必要であると考える.

5 国の異なる全ての人を対象にした調査

5.1 概要

本実験は, 様々な国に住む性別や年齢の異なる 23 名のユーザを対象に行った. ユーザの基本情報を表 4 に示す. アンケート項目は基本情報について, SeBIS について, スマートフォンを使用した多要素認証についての 3 種類からなる. それぞれの質問の回答データを収集し, 国の違いとセキュリティ意識や多要素認証方法の選択の関連について考察する.

5.2 国の違いとセキュリティ意識の違い

本実験に協力したユーザの国について, アメリカ州、アジア州、ヨーロッパ州という区分に分けた際のセキュリティ意識の違いを考察する. アメリカ州には USA とブラジル国籍のユーザが合計 6 名, アジア州には台湾と韓国と日本のユーザが合計 10 名、ヨーロッパ州にはイタリアとフランスとスイスのユーザが合計 6 名属している. それぞれの州ごとの SeBIS の得点分布を表 4 の箱ひげ図に示すが, このグラフから, 州によってセキュリティ意識が大きく異なることはないことがわかる. そこで, 日本とその他の国との間で比べるため, 4 章の実験で得た 57 名の日本人のデータと本実験の日本人 3 人のデータと, その他の国の 20 人のデータを用いてセキュリティ意識の違いを調べた. その結果を表 5 に箱ひげ図で示す. このグラフから, 日本の外れ値を除くと海外のデータの方がやや高い値を示すことが分かる. 海外のものの最高値が 70 で最低値が 37, 平均値が 53.6 なのに対し, 日本のものは最高値が 64, 最低値が 34, 平均値が 48.7 であった. しかし, データの数の違いや, 日本のデータは学生が大半を占めるのに対し, 海外のデータは社会人を含んでいることから, 海外と日本の違いであるとは言い切れない.

5.3 認証方法の人気度・セキュリティ意識との関連

最も使用する頻度の高い認証方法の統計を表 6 に示す. 最も多く使用する認証方法を一つ回答せよという質問の結果, SMS コードによる認証が 11 名で全体の 47.8% と最も多く, 次に生体認証が 9 名で全体の 39.1%, 次にモバイルアプリによる認証が 3 名で全体の 13% であった. やはり海外でも SMS によるワンタイムパスワードを利用した認証が主流であることがわかった. 次に多かった生体認証については, SMS やモバイルアプリでの認証の中でショートカットとして使用している可能性が高いため, あまりあてにならない結果だと推測する. モバイルアプリの認証を選択した人数は 3 名であったが, そのうち日本人が 1 名, 台湾人が 2 名で全員 20〜24 才であった. このことから, 日本や台湾などのアジア圏の方がアプリの浸透があるとも考えられる. また、図 7 にはモバイルアプリによるワンタイムパスワードと SMS コードによるものごとの SeBIS の得点分布を箱ひげ図で示す. 生体認証については前述のとおりあてにならないと判断したため比較対象から外した. このグラフから, それぞれを選んだ人の SeBIS の得点分布はさほど変わらないことが分かる. モバイルアプリを選んだ人の平均は 50.6 であり, 最低値は 46, 最高値は 58, SMS コードを選んだ人の平均値は 52.9 であり, 最低値は 42, 最高値は 63 である. モバイルアプリのデータ数が 3 であるのに対し SMS コードのものは 11 であることからデータの数に差があることから, これだけでは関係性が分からないと判断する.

5.4 考察

本実験結果から, 国の違いによるセキュリティ意識の違いや, 多要素認証方法の違いは見られないことが分かった. どの国でもモバイルアプリよりも SMS コード

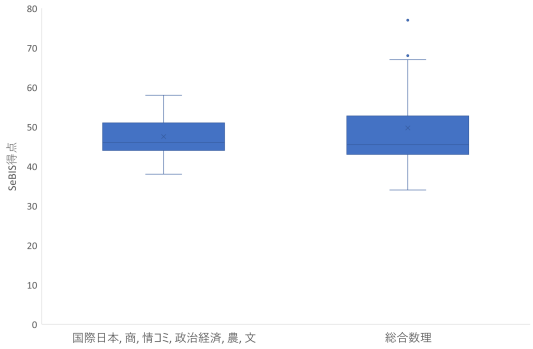

図 1　学部別の SeBIS 得点分布箱ひげ図

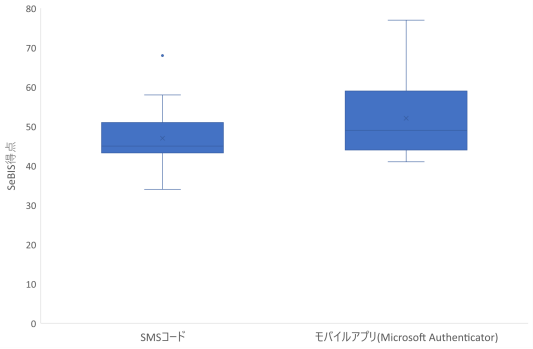

図 3　認証方法別の SeBIS 得点分布箱ひげ図

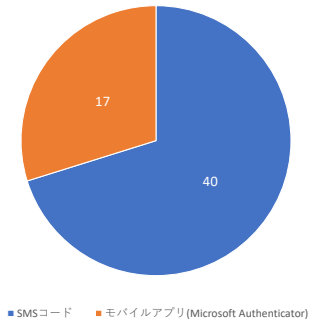

図 2　認証方法の割合

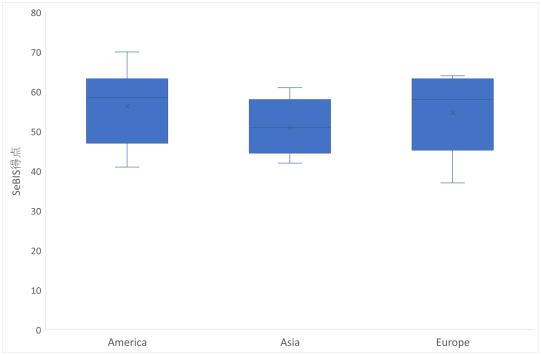

図 4　州別の SeBIS 得点分布箱ひげ図

によるワンタイムパスコードを第二要素とした認証がまだまだ主流であると考えられる.

6　おわりに

本実験から, 学部や国などの人の属性と選択する認証方式には相関が見られないこと, 主流の認証方式がどの国でも SMS コードであることが分かった. また, モバイルアプリを認証方法に選ぶ人のセキュリティ意識は SMS コードのものよりも高い傾向が見られた. しかし中間者攻撃の認知や安全面が必ずしもモバイルアプリを選択する理由ではなく,「他の方法を知らなかったから」等の消極的な理由が主であった. また, SMS コードを認証方法に選択する理由は「慣れ親しんでいるから」がほとんどであった. これらのことから, モバイルアプリでの認証方法の安全性や利便性を広く認知させること, モバイルアプリでの認証を推奨することが必要であると結論付ける.

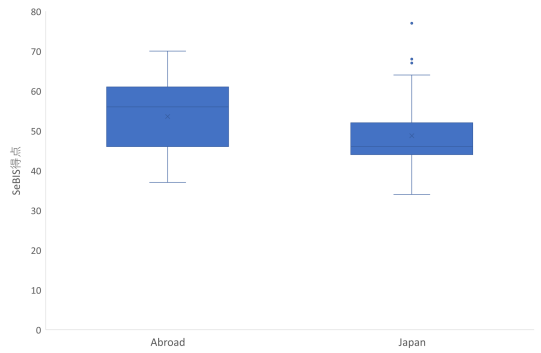

図 5　日本とその他の国の SeBIS 得点分布箱ひげ図

参考文献

[1] 明治大学, MeijiMail 多要素認証 (https://www.meiji.ac.jp/isc/mm-mfa/mfa.html, 2023.12 参照)

表 1　SeBIS 質問項目 (日本語)

番号	質問内容
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。
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。
3	コンピュータから離れる時、手動で画面をロックする。
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。
5	必要があるときしかパスワードを変更しない。
6	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。
7	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)
8	必要が無い場合は、パスワードに特殊文字 (¥や*) を含めない。
9	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。
10	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。
11	安全な通信か確認することなくウェブサイトに情報を提出する。(例：SSL, ”https://”, ロックアイコン)
12	リンクをクリックする前に、マウスアイコンをリンクに乗せ訪れる URL を確認する。
13	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。
14	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。
15	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。
16	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。

表 2　SeBIS 質問項目 (英語)

Number	Questions
1	Whenever I step away from my computer, I lock the screen.
2	I use a password/passcode to unlock my laptop or tablet.
3	I manually lock the screen when leaving the computer.
4	I use a PIN or passcode to unlock the phone.
5	Once I create a password, I tend to never change it.
6	I use a different password for each account I use.
7	When creating a new online account, set a password that exceeds the minimum number of characters required. (If it is more than 8 characters, set it to
8	Do not include special characters (! or *) in passwords unless necessary.
9	When a link is sent to me, I click on it without checking to see where it leads.
10	I judge which site was visited by the appearance and atmosphere of the site, not the URL.
11	I submit information to a website without verifying that the data communication is secure. (Ex. SSL, ”https://”, a lock icon)
12	When browsing websites, I frequently mouseover links to see where they go, before clicking them.
13	Even if a security problem is discovered, someone will fix it, so I continue to use it.
14	I apply software updates as soon as my computer prompts me.
15	I make sure that the programs I’ m using are up-to-date.
16	I check that my anti-virus software is regularly updated.

[2] 野口, 大瀧, 山本, 西原, 外岡, “レベル分けによる多要素認証の要否の実現と認証連携の拡張”, 学術情報処理研究 Mo.24 JACN 2020

[3] Lyastani, Backes, Bugiel,“A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites”, Network and Distributed System Security (NDSS) Symposium 2023

[4] Nethanel Gelernter, Senia Kalma, Bar Magnezi, Hen Porcilan,“The Password Reset MitM Attack”, IEEE Security and Privacy 2017,

[5] 柴山, 菊池, “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”, 情報処理学会創立 60 周年記念 第 82 回大会, 2020

[6] 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”, 2018 Symposium on Cryptography and Information Security Niigata, Japan, Jan. 23 - 26, 2018

[7] Egelman, Peer, “Scaling the Security Wall, Developint a Security Behavior Intentions Scale(SeBIS)”, CHI2015, pp2873-2882

表 3　Meiji Mail ユーザ実験基本情報

		人数 (名)	割合 (%)
性別	男性	17	29.8
	女性	40	70.2
学年	1 年	8	14.0
	2 年	11	19.3
	3 年	10	17.5
	4 年	27	47.4
	教授	1	1.8
学部	総合数理	26	45.6
	国際日本	20	35.1
	情報コミュニケーション	4	7.0
	農	1	1.8
	文	2	3.5
	政治経済	1	1.8
	商	3	5.3
留学生		1	1.8

表 4　国別ユーザ実験基本情報

		人数 (名)	割合 (%)
性別	男性	6	26.1
	女性	17	73.9
年齢	～19 歳	3	13.0
	20～24	10	43.5
	25～30	3	13.0
	31～	7	30.4
国	USA	5	21.7
	台湾	7	30.4
	イタリア	2	8.7
	韓国	1	4.3
	フランス	2	8.7
	スイス	2	8.7
	ブラジル	1	4.3
	日本	3	13
社会人経験の有無	ある	17	73.9
	ない	6	26.1

表 5　認証方法に SMS コードを選んだ理由

理由	数
馴染みがあるから	16
他の方法 (があるの) を知らなかったから	10
アプリが使用できなかったから	2
特に覚えていない	11

表 6　認証方法にモバイルアプリを選んだ理由

理由	数
他の方法 (があるの) を知らなかったから	7
馴染みがあるから	2
友達にやってもらった	1
電話番号を変更したから	1
一度試したら早かったから	1
特に覚えていない	5

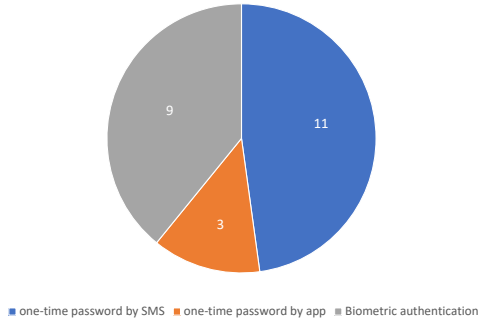

図 6　人気な認証方法

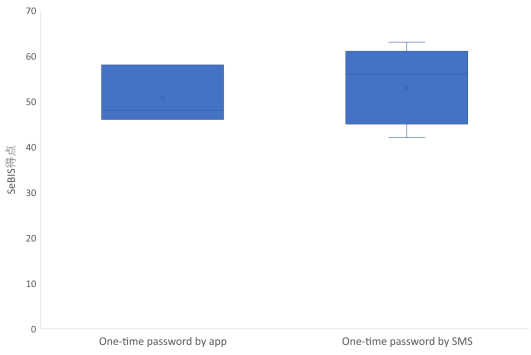

図 7　認証方法別の SeBIS 得点分布箱ひげ図 (国別)