Computer Security Symposium 2019
21 - 24 October 2019

ログイン関連画面に潜む脅威：センシティブサービスにおけるアカウント所有の特定

長谷川 彩子[1,a)]　渡邉 卓弥[1]　塩治 榮太朗[1]　秋山 満昭[1]

概要：見知らぬ人物（アウトサイダー）からの金銭目的でのサイバー攻撃が継続的に発生している一方で，最近の研究では身近な人物（インサイダー）からのプライバシー侵害を目的とした攻撃の実態が明らかにされている．本研究ではインサイダーによる攻撃に焦点を当てる．特に，ユーザがアカウントを所有するサービスの中にはそのユーザの嗜好や社会的状況等を間接的に示すものがあるため，アカウントの所有をインサイダーに知られることが重大なプライバシー侵害に繋がる可能性があると考えた．これを踏まえ本研究では，オンラインサービスの各種ログイン関連画面に表示されるメッセージと標的のメールアドレスや電話番号を悪用して，標的のアカウントの所有を特定できる攻撃を発見した．実態調査の結果，調査したほぼ全てのサービスにおいて本攻撃が成功することが判明した．さらにユーザ調査の結果，参加者の80%以上にアカウントの所有を他人に知られたくないセンシティブなサービスが存在すること，その約半数に本攻撃の被害者となりうる行動が見られることなどから，本攻撃がユーザに及ぼす影響が深刻であることが示された．最後に，サービス提供者やユーザに適切な対策を提示する．

Identifying the Existence of a Target's Account on Sensitive Services

Ayako A. Hasegawa[1,a)]　Takuya Watanabe[1]　Eitaro Shioji[1]　Mitsuaki Akiyama[1]

Abstract: Recent studies have focused on privacy threats from insiders (i.e., intimates or acquaintances of a target), such as cyberstalking. In this paper, we present a new form of attack from insiders that identifies the existence of a target's account by using the target's email address (or phone number) and insecure login-related messages displayed. The attack may cause a privacy violation because the kinds of service accounts a target has implies his/her personal preferences or situation. We found that almost all online services were vulnerable to the attack. Moreover, through user studies, we found that over 80% of participants answered that there are sensitive services that they do not want their use of to be known to others and about half of them could be potential victims. Finally, we make recommendations for online service providers and users on the basis of our findings.

1. はじめに

オンラインサービス提供者にとってユーザのアカウント保護は重大な使命であり，多要素認証や CAPTCHA 等の様々なアカウント保護技術がサービスに実装されている．

アカウントに対する攻撃の一つとして，ログインメッセージを悪用して標的のアカウントの所有を暴く攻撃が知られている [1]．攻撃者はログイン画面で標的のユーザ ID を入力し，冗長なメッセージが表示された場合に，攻撃者は標的のアカウントの存在を特定できる．例えば，“パスワードが違います” という冗長なエラーメッセージは，ログイン試行が失敗したことに加えて入力したユーザ ID が存在することを示唆している．攻撃者はこれを悪用してサービスに登録されているユーザ ID のリストを作成することで，パスワード推測攻撃を効率的に実施することができる．本研究では，このような攻撃を許す根本的原因がメッセージ内容の冗長性ではなく，メッセージの非一貫性にあると指摘する．攻撃者は，登録および未登録ユーザに対する各種ログイン関連メッセージが非一貫的であるサー

[1] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories
[a)] ayako.hasegawa.vg@hco.ntt.co.jp

© 2019 Information Processing Society of Japan

ビスにおいて，標的に対して表示されるメッセージをそれらと比較することによって標的のアカウント所有を特定できる．我々は本研究の事前調査において，非一貫的なメッセージを表示するログイン関連画面として，ログイン画面の他にパスワードリカバリー画面およびアカウント作成画面を発見した．

見知らぬ人物（アウトサイダー）による金銭を目的とした総当たりでのサイバー攻撃が継続的に発生している一方で，最近の研究ではパートナー，家族，友人，同僚，知人等の身近な人物（インサイダー）によるプライバシー侵害の実態が明らかにされている [2–4]．これを踏まえ，本研究では，インサイダーが上述した攻撃の攻撃者になりうると想定する．ユーザがアカウントを所有するサービスは，そのユーザの属性，嗜好，指向，信仰，社会的状況などを間接的に示す可能性がある．そのため，ユーザがアカウントの所有を他人に知られたくない “センシティブ” なサービスにおけるアカウント所有情報の漏洩は重大なプライバシー侵害に繋がると考えた．各種ログイン関連メッセージを悪用した攻撃は，高度な技術を必要としないため，ユーザ ID となる標的のメールアドレスや電話番号さえ知っていれば容易に攻撃を遂行できる．また，インサイダーによる特定の標的に対する攻撃は少ない試行回数で済むため，アウトサイダーを想定した CAPTCHA 等の試行回数制限では阻止できない．

これらを踏まえ，本研究ではインサイダーによる標的のアカウント所有特定攻撃によって生じる新たなプライバシー脅威に対して，以下の研究課題に取り組む．

RQ1: ユーザがアカウントの所有を他人に知られたくないサービス（センシティブサービス）はどのようなサービスか．

RQ2: センシティブサービスはアカウント所有特定攻撃に対して安全であるか．

RQ3: アカウント所有特定攻撃はユーザにどれほどの影響を与えるか．

まず，RQ1 を解くため，予備調査としてオンラインアンケートを実施し，参加者から多種多様なセンシティブサービス名を収集した．次に，RQ2 を解くため，実サービスにおける本攻撃の攻撃成功率を測定する実態調査を実施した．この実態調査では，ウェブサイトおよびモバイルアプリにおいて，ログイン，パスワードリカバリー，アカウント作成の 3 画面で表示されるメッセージを調査した．予備調査の参加者から収集したセンシティブサービス，および，Alexa Top Global Sites リスト上位の有名サービスを含む合計 87 サービスを調査した結果，ほぼ全て（86/87）のサービスにおいて本攻撃が成功することが示された．さらに，RQ3 を解くため，ユーザのセンシティブサービスに対する認識や行動を明らかにするオンラインアンケートを実施した．その結果，参加者の 80%以上にアカウントの所有を他人に知られたくないセンシティブサービスが存在すること，彼らの約半数は他人に知られているメールアドレスをセンシティブサービスにも登録しており本攻撃の被害者となりうること，参加者の 25%が本攻撃の “攻撃者” としての願望を秘めていることなどが明らかになり，本攻撃がユーザに及ぼす影響が深刻であることが示された．

本研究の結果は，サービスの各種ログイン関連画面のセキュリティ向上に役立てられる．我々はサービス提供者およびユーザに対して適切な対策を提示するとともに，本研究で明らかにした問題と対策を IPA，JPCERT/CC，OWASP に情報共有し，OWASP が発行するアプリケーション設計のガイドラインの改定に貢献した．

2. 脅威モデル

2.1 本研究と典型的な脅威モデルとの比較

本研究で取り扱う脅威モデルは，攻撃者像，攻撃目的，攻撃方法の点で，パスワード推測攻撃 [1] で想定されてきた典型的な脅威モデルとは全く異なる．

攻撃者像: 典型的な脅威モデルでは，攻撃者は標的と関わりのない見知らぬ人物（アウトサイダー）である．本脅威モデルでは，標的のパートナー，家族，友人，同僚，知人等の身近な人物（インサイダー）が攻撃者となる．インサイダーは標的のメールアドレスや電話番号を知っていると想定する．

攻撃目的: 典型的な脅威モデルでは，アウトサイダーは金銭目的でアカウントの乗っ取りを試みる．本脅威モデルでは，インサイダーは標的のプライバシー侵害を目的とする．ユーザがアカウントを所有するサービスの中にはユーザの属性，嗜好，指向，信仰，社会的状況等を間接的に示すものもあるため，インサイダーは標的がセンシティブなサービスのアカウントを所有しているかどうかを詮索する．例えば，標的が特定の性的指向をもつユーザを対象としたマッチングサービスのアカウントを所有していた場合，インサイダーは標的の性的指向を知ることができる．

攻撃方法: 典型的な脅威モデルでは，アウトサイダーは情報漏洩で流出した大量のユーザ ID を用いて，辞書攻撃等により総当たり的にログインを試みる．本脅威モデルでは，インサイダーは各種ログイン関連メッセージの欠陥を悪用して，標的のメールアドレスや電話番号がユーザ ID として特定のサービスに登録されているか確認する．これには高度な技術は必要なく，標的のメールアドレスや電話番号さえ知っていれば容易に攻撃を遂行できる．また，インサイダーは特定の標的に対し少ないログイン試行回数で攻撃を遂行できるため，従来のアウトサイダーを想定した CAPTCHA 等の試行回数制限では阻止できない．各種ログイン関連メッセージの欠陥を 2.2 節で，欠陥を悪用した具体的な攻撃の流れを 2.3 節で詳述する．

表 1　安全なおよび安全でない各種ログイン関連メッセージの例

画面	入力情報	安全でないメッセージ例	安全なメッセージ例
ログイン	[L–R] 登録ユーザ ID	[L–R–IM] パスワードが違います	[L–SM] ユーザ ID かパスワードが違います
	[L–UR] 未登録ユーザ ID	[L–UR–IM] そのユーザ ID は存在しません	
パスワード	[PR–R] 登録メールアドレス	[PR–R–IM] パスワード再設定用リンクを送りました	[PR–SM] 入力メールアドレスが DB に存在
リカバリー	[PR–UR] 未登録メールアドレス	[PR–UR–IM] 登録されていないメールアドレスです	すればパスワード再設定用リンクを送ります
アカウント	[AC–R] 登録ユーザ ID	[AC–R–IM] そのユーザ ID は既に使用されています	[AC–SM] 入力メールアドレスにアカウント
作成	[AC–UR] 未登録ユーザ ID	[AC–UR–IM] アカウント作成が成功しました	作成用リンクを送ります

2.2　各種ログイン関連メッセージの欠陥

攻撃者は各種ログイン関連メッセージの欠陥を悪用して標的のアカウントの所有を特定する．本研究では，このような攻撃を許す各種ログイン関連メッセージの欠陥の根本的原因が，Bonneau らの研究 [1] で述べられたメッセージ内容の冗長性でなく，メッセージの非一貫性であると指摘する．本節では，事前調査により非一貫的なメッセージを表示すると確認した，ログイン，パスワードリカバリー，アカウント作成の 3 画面について欠陥を具体的に説明する．

2.2.1　ログイン画面

標準的なログイン画面は，ユーザ ID（メールアドレス，任意のユーザ名，電話番号）とパスワードの組の入力を求める．ログイン画面には，入力形式エラーを除いて 2 種類のエラー状態が存在する．一つは登録ユーザ ID と誤ったパスワードの組が入力されたエラー状態（L–R），もう一つは未登録ユーザ ID が入力されたエラー状態（L–UR）である．ここで，L–R と L–UR で表示されるメッセージが非一貫的であるサービスでは本攻撃が成功する．例えば “パスワードが違います”（L–R–IM）と “そのユーザ ID は存在しません”（L–UR–IM）のように表示するサービスにおいて，標的のユーザ ID を入力して前者のメッセージが表示された場合に，標的のアカウント所有を特定できる．一方で，例えば “ユーザ ID かパスワードが違います”（L–SM）のように，L–R と L–UR で一貫したメッセージを表示するサービスでは本攻撃は成功しない．

2.2.2　パスワードリカバリー画面

標準的なパスワードリカバリー画面では，ユーザにパスワード再設定用リンクを送信するために，ユーザが登録したメールアドレスの入力を求める．パスワードリカバリー画面は，入力形式エラーを除き，登録メールアドレスが入力された通常状態（PR–R），未登録メールアドレスが入力されたエラー状態（PR–UR）の 2 状態に分岐する．例えば “パスワード再設定用リンクを送りました”（PR–R–IM）と “登録されていないメールアドレスです”（PR–UR–IM）のように，PR–R と PR–UR で非一貫的なメッセージを表示するサービスでは，標的のメールアドレスを入力して前者のメッセージが表示された場合に，標的のアカウント所有を特定できる．一方で，例えば “入力メールアドレスが DB に存在すればパスワード再設定用リンクを送ります”（PR–SM）のように，PR–R と PR–UR で一貫したメッセージを表示するサービスでは本攻撃は成功しない．

2.2.3　アカウント作成画面

標準的なアカウント作成画面にはユーザ ID の重複登録を防ぐ機能が備わる．そのため，アカウント作成画面は，入力形式エラーを除き，登録ユーザ ID が入力されたエラー状態（AC–R），未登録ユーザ ID が入力された通常状態（AC–UR）の 2 状態に分岐する．例えば，“そのユーザ ID は既に使用されています”（AC–R–IM）と “アカウント作成が成功しました”（AC–UR–IM）のように，AC–R と AC–UR で非一貫的なメッセージを表示するサービスでは，標的のユーザ ID を入力して前者のメッセージが表示された場合に，標的のアカウント所有を特定できる．一方で，“入力メールアドレスにアカウント作成用リンクを送ります”（AC–SM）のように，AC–R と AC–UR で一貫したメッセージを表示するサービスでは本攻撃は成功しない．

2.3　攻撃の手順

本脅威モデルでは攻撃者（インサイダー）は標的のメールアドレスまたは電話番号を知っていると想定し，それと各種ログイン関連メッセージの欠陥を悪用してアカウント所有特定攻撃を遂行する．なお，簡略のために以降では攻撃者が標的のメールアドレスを悪用する場合の攻撃手順を記すが，実際にはメールアドレスも電話番号も同様に本攻撃に利用できる．本攻撃の攻撃手順の具体例を図 1 に示す．本攻撃は，非一貫的なログイン関連メッセージを表示するサービスを検知する，攻撃可能サービス検知（Phase I）と，標的のメールアドレスがそのサービスに登録されているかを特定する，標的登録特定（Phase II）からなる．

2.3.1　Phase I: 攻撃可能サービス検知

攻撃者はまずサービスに登録していない 2 つのメールアドレスを準備する．次に，標的のアカウント所有を知りたいサービスを列挙する．各サービスにおいて，準備した一方のメールアドレスを用いてアカウントを作成し，表示されたメッセージを収集する．次に，この段階で登録および未登録状態にある 2 つのメールアドレスを各々用いて，3 画面で表示されるメッセージを以下の手順で収集する．

ログイン画面: 登録メールアドレスと，パスワードポリシーを満たす任意の誤ったパスワードの組を入力し，表示されたメッセージを収集する．次に，未登録メールアドレスと，パスワードポリシーを満たす任意のパスワードの組

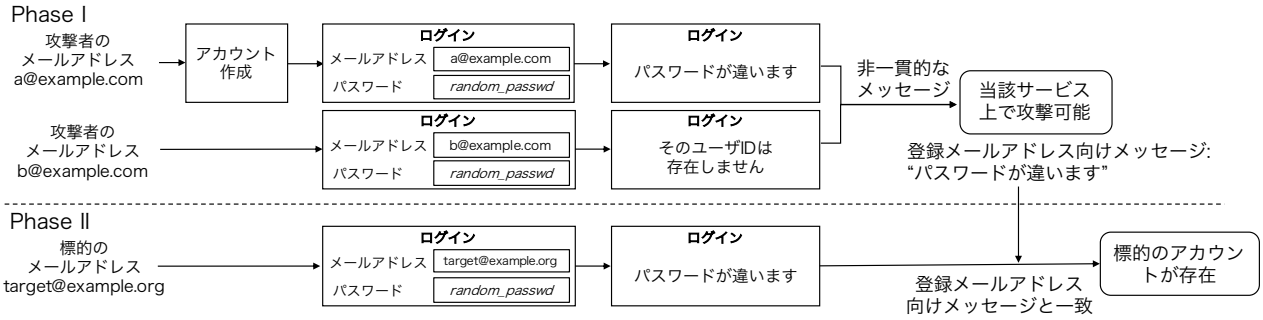

図 1 攻撃の手順（ログイン画面を悪用した例）

を入力し，表示されたメッセージを収集する．

パスワードリカバリー画面: 登録メールアドレスを入力して表示されたメッセージ，および，未登録メールアドレスを入力して表示されたメッセージを収集する．

アカウント作成画面: 登録メールアドレス，パスワードポリシーを満たす任意の誤ったパスワード，および，その他入力必須項目があれば有効な形式で任意に入力し，表示されたメッセージを収集する．未登録メールアドレスに対する表示メッセージは，アカウント作成時に既に収集した．

登録および未登録メールアドレスを用いて収集したメッセージが非一貫的であるログイン関連画面が 1 種類以上存在する場合，当該サービス上で攻撃が可能である．

2.3.2 Phase II: 標的登録特定

Phase I で非一貫的なメッセージを表示すると判明したログイン関連画面に標的のメールアドレスを入力し，表示されたメッセージを収集する．このメッセージが，Phase I で収集した登録メールアドレス向けメッセージと一致する場合，標的は当該サービスのアカウントを所有すると特定して攻撃を終了する．

3. 予備調査

RQ1 を解くために，アカウントの所有を他人に知られたくないサービスを問うアンケート調査を実施した．

3.1 方法

アンケートはクラウドソーシングサービス Amazon Mechanical Turk（MTurk）[5] 上で実施した．アンケートはアカウントの所有を他人に知られたくないサービスを問う 1 問からなり，複数回答可能の選択肢として 11 種のサービスカテゴリーを用意した．加えて，具体的なサービス名を記す任意回答欄も設けた．参加資格をタスク承認率 97%以上の U.S. の住人，報酬額を 1 ドルに設定して募集を実施し，614 名から回答を得た．平均回答時間は 1.9 分であった．

3.2 結果

選択肢と回答結果を表 2 に示す．81.6%（501/614）の参加者には他人にアカウント所有を知られたくないセンシティブサービスのカテゴリーが 1 つ以上存在した．特に，マッチングサービスとアダルトコンテンツサービスは過半数の参加者が選択した．重複を除いて合計 267 個のセンシティブなサービス名が参加者から挙げられた．その中には，特定の性的指向をもつユーザを対象としたマッチングサービス，特定の悩み事を相談する掲示板サービス，性感染症検査結果を照会するヘルスケアサービス，生活保護受給者向けの行政サービス等，非常にセンシティブであると想定されるサービスが多数含まれていた．

表 2 アカウント所有を知られたくないサービス（複数回答可）

マッチング	54.4%	アダルトコンテンツ	50.5%
ソーシャルネットワーク	19.9%	転職	17.6%
掲示板	14.3%	金融	12.5%
ショッピング	8.8%	ヘルスケア	4.6%
クラウドストレージ	4.4%	その他	3.9%
なし	18.4%		

表 3 実サービスで用いられるユーザ ID の種別

	#	メールアドレス	任意のユーザ名	電話番号
センシティブ	84	82.1%	42.9%	9.5%
有名	45	77.8%	46.7%	17.8%
合計	109	79.8%	44.0%	8.3%

4. 実態調査

RQ2 を解くために，実サービスの各種ログイン関連メッセージを収集して本攻撃の攻撃成功率を測定した．

4.1 方法

4.1.1 サービス選定

実態調査では，予備調査で収集した 267 個のセンシティブサービスから調査対象を選定した．各カテゴリーの調査上限サービス数を表 2 の回答分布に沿うように定めた後，各カテゴリーにおいて回答者数が多い順にサービス名を選択することで，84 個のサービスを調査候補とした．

また，センシティブサービスと有名サービスの安全性の傾向を比較するするため，有名サービスの調査も実施した．Alexa Top Global Sites リスト（2018 年 7 月 23 日取得）の上位のサービスから，アカウント制でないサービス，英語以外のサービス，有料サービス，ユーザ ID が重複するサー

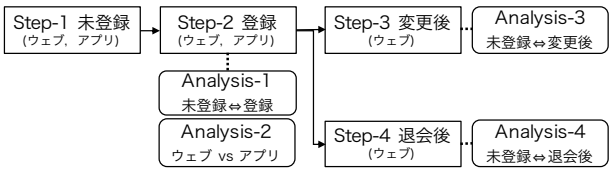

図 2 実態調査における評価プロセスの概要

ビスを除き，45 個の有名サービスを調査候補とした．

調査候補とした 84 個のセンシティブサービスと 45 個の有名サービスの中には 20 個の重複が含まれ，調査候補サービスは合計で 109 個となった．次に，この 109 個の調査候補サービスのユーザ ID の種別を調査した．結果を表 3 に示す．ユーザ ID としてメールアドレス，任意のユーザ名，電話番号が使われており，このうちの複数の項目をユーザ ID として使えるサービスも多く見られた．特に，ユーザ ID としてメールアドレスを使うことのできるサービスが最も多く，全体の 79.8%（87/109）を占める．本脅威モデルでは攻撃者（インサイダー）は標的のメールアドレスを悪用することを想定するため，最終的にこの 87 個のサービスを実態調査の調査対象とした．この 87 個のサービスは，69 個のセンシティブサービス，および，35 個の有名サービスからなり，17 個の重複を含む．

4.1.2 評価プロセス

実態調査では 4 段階の登録状態（未登録，登録，変更後，退会後）において，3 画面（ログイン，パスワードリカバリー，アカウント作成）のメッセージを収集して評価した．評価プロセスの概要を図 2 に示す．

全調査対象サービスに対して，まず，未登録（Step–1）状態にある調査専用メールアドレスを用いて 3 画面のメッセージを収集した．続いて，調査専用メールアドレスを調査対象サービスに登録し，登録（Step–2）状態となった調査専用メールアドレスを用いて 3 画面のメッセージを収集した．Step–1 と–2 においては，ウェブサイトだけでなく，Google Play ストアでインストール可能なモバイルアプリがある場合にはモバイルアプリのメッセージも収集した．これは，モバイルアプリを用いて本攻撃が遂行されることも十分に考えられるためである．

さらに，ランダムに選定した 42 個および 60 個の調査対象サービスに対して，登録した調査専用メールアドレスを別のものへ変更後（Step–3），および，サービス退会後（Step–4）の状態においても，調査専用メールアドレスを用いてウェブサイトにおける 3 画面のメッセージを独立に収集した．

なお，メッセージ収集の過程においては，攻撃者は標的のメールアドレス以外，つまりパスワード等は知りえないという状況を再現した．また，入力形式エラーがメッセージに影響しないよう注意した．すなわち，パスワード入力欄や個人情報入力欄には，パスワードポリシーや入力形式を満たし登録には用いていない任意の文字列を入力した．

Step–1 から–4 を通して，87 個の調査対象サービスから合計 1146 個の各種ログイン関連メッセージを収集した．

Analysis–1 では，ウェブサイトにおける本攻撃の攻撃成功率を測定する．未登録（Step–1）および登録（Step–2）状態で収集したウェブサイトにおける 3 画面のメッセージを各々比較した．各画面において Step–1 と–2 で表示するメッセージが一貫していた場合に，その画面は安全であると判定した．その上で 3 画面全てが安全である場合のみ，そのサービスは本攻撃に対して安全であると判定した．これは，1 つでも安全でないログイン関連画面があると，攻撃者はその画面を悪用して本攻撃を遂行できるからである．

Analysis–2 では，ウェブサイトとモバイルアプリで本攻撃の攻撃成功率に違いがあるのか調査する．まず，未登録（Step–1）および登録（Step–2）状態で収集したモバイルアプリにおける 3 画面のメッセージの一貫性を Analysis–1 と同様の方法で評価した．その後，サービス毎に，モバイルアプリにおける安全なログイン関連画面の数と，ウェブサイトにおける安全なログイン関連画面の数を比較した．

Analysis–3 と–4 では，メールアドレス変更およびサービス退会という行動が，既にセンシティブサービスに登録しているユーザにとって本攻撃への有効な対策になりうるかを調査する．Analysis–3 では，未登録（Step–1）と変更後（Step–3）の状態で収集したウェブサイトにおける 3 画面のメッセージの一貫性をを Analysis–1 と同様の方法で評価した．同様に，Analysis–4 では未登録（Step–1）と退会後（Step–4）の 3 画面のメッセージの一貫性を評価した．

表 4 ウェブサイトにおいて各種ログイン関連画面が安全であるサービスの割合（Analysis–1）

	#	**L**	**PR**	**AC**	**L ∩ PR ∩ AC**
センシティブ	69	72.5%	36.2%	2.9%	0.0%
有名	35	54.3%	28.6%	8.6%	2.9%
合計	87	71.3%	35.6%	3.4%	1.1%

L:ログイン，**PR**:パスワードリカバリー，**AC**:アカウント作成

4.2 結果

4.2.1 Analysis–1: ログイン関連メッセージの一貫性

Analysis–1 の結果を表 4 に示す．驚くべきことに，ウェブサイトにおいて 3 画面全てが安全であるサービスは，センシティブサービスで 0.0%（0/69），有名サービスでも 2.9%（1/35）のみであった．つまり，ほぼ全てのサービスにおいて本攻撃が成功することを示す．また，アカウント作成画面が安全であるサービスは，全体の 3.4%（3/87）のみであり，ログイン画面（71.3%）やパスワードリカバリー画面（35.6%）に比べて極端に少ない．これは，攻撃者がアカウント作成画面の調査から攻撃を開始すると非常に効率的に攻撃を遂行できることを意味する．

安全であった 1 サービス（*Craigslist*）を除くと，センシ

表 5　ウェブサイトと比較したモバイルアプリの安全性 (Analysis-2)

	#	同じ	低い	高い
センシティブ	46	71.7%	19.6%	8.7%
有名	31	71.0%	22.6%	6.5%
合計	63	71.4%	19.0%	9.5%

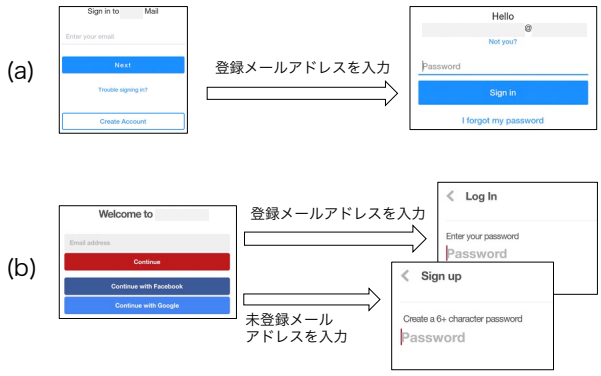

図 3　モバイルアプリの安全でないログイン画面の例

ティブサービスのほうが有名サービスより安全な傾向にあることが伺える．例えば，ログイン画面が安全であるサービスの割合は，センシティブサービスで 72.5%（50/69）であり，有名サービスの 54.3%（19/35）より高い．センシティブサービスのカテゴリー別に比較すると，マッチング，転職，金融ではログイン画面とパスワードリカバリー画面の両方が安全であるサービスの割合が高く，これらのカテゴリーではプライバシーを重視していると考えれられる．

4.2.2　Analysis–2: モバイルアプリの安全性

87 個の調査対象サービスのうち，63 個がモバイルアプリを提供していた．Analysis–2 の結果を表 5 に示す．71.4%（45/63）のサービスはウェブサイトとモバイルアプリで安全性が同じであった．続いて，モバイルアプリのほうが安全性が低くなるサービスが多かった．特に，モバイルアプリではログイン画面が安全でないサービスが増加した．これは，ウェブサイトではユーザ ID とパスワードの入力欄を 1 画面内に表示するが，モバイルアプリでは図 3–(a)，(b) のようにログイン画面を 2 分割して段階的に表示するサービスが複数見られたためである．これらのサービスは，最初の画面で入力されたユーザ ID の登録状況により次に異なる画面を表示するといった非一貫的な応答を見せる．なお，Analysis–1 で唯一安全であった *Craigslist* はモバイルアプリも安全であった．

4.2.3　Analysis–3: メールアドレス変更の有効性

42 個のサービスのうち，40 個がメールアドレス変更機能を備えていた．このうち 92.5%（37/40）のサービスでは，変更前のメールアドレスを入力した際，3 画面全てで未登録メールアドレス向けメッセージが表示され，本攻撃は成功しなくなっていた．よって，知人に知られていないメールアドレスへの変更は本攻撃への有効な対策と言える．

4.2.4　Analysis–4: サービス退会の有効性

60 個のサービスのうち，42 個が退会機能を備えていた．このうち退会後には本攻撃が成功しなくなるサービスは 47.6%（20/42）のみであったため，退会は本攻撃への有効な対策とは言えない．退会後も攻撃可能なサービスの中には，退会を明示するメッセージを表示するものもあった．

5.　ユーザ調査

RQ3 を解くために，ユーザのセンシティブサービスに対する認識や行動を明らかにするアンケート調査を実施した．

5.1　方法

アンケートは予備調査と同様に MTurk 上で実施した．アンケートは，参加者属性，アカウント所有を他人に知られたくないサービスの有無とその理由，知人のアカウント所有を知りたい願望の有無とその動機，および，センシティブサービスに登録するメールアドレスを問う全 9 問からなる．参加資格は予備調査と同様に設定した．基本報酬額を 2 ドルに設定し，任意回答の自由記述欄に回答を記述した参加者には追加ボーナス 1 ドルを支払った．不注意な回答をした 24 名を除去し，447 名分の回答を分析した．参加者の 53.7%が男性，45.2%が女性，1.1%はその他または無回答を選択した．参加者の年齢は 19 歳から 76 歳までの平均 36.8 歳であった．平均回答時間は 8.8 分であった．なお自由記述回答は全て英語で記述されているため，分析後に日本語に翻訳した上で本稿に掲載する．

5.2　結果

5.2.1　アカウント所有を他人に知られたくない理由

アカウントの所有を他人に知られたくないサービスがあると回答した参加者は 82.1%（367/447）おり，そのうち 267 名が具体的な理由を挙げた．そこで，テーマ分析法（thematic analysis）で帰納的コーディングを行い，理由を 3 テーマに分類した．2 名のコーダーによるコーディングの信頼性は，コーエンのカッパ係数で k=0.84 であった．

85.4%（228/267）の回答が 恥ずかしさ（Embarrassment）に分類された．参加者はオンラインサービスの利用は個人情報の一つと考え，それを他人に知られると単純に恥ずかしいと答えた．例えば，“マッチングサービスの利用は日常生活でデート相手を見つけれらないことを示すから恥ずかしい”，“女性のアダルトサイトの利用は未だタブーであるから恥ずかしい”，“ローンサービスの利用により借金を周囲に知られるのは恥ずかしい”，といった回答が挙がった．11.6%（31/267）の回答は仕事への影響（Effect on work）に分類された．参加者は，会社での人事評価に影響することを恐れ，“上司にアダルトサイトや転職サービスの利用を知られたくない”，のように答えた．残りの 3.0%（8/267）の回答は 不道徳な行動（Immoral behavior）と分類され

表 6　センシティブサービスに登録するメールアドレス

(i) センシティブでないサービスにも登録し，かつ，他人に知られたメールアドレス	30.5%
(ii) センシティブでないサービスにも登録し，かつ，誰にも知られていないメールアドレス	15.0%
(iii) センシティブサービスのみに登録し，かつ，他人に知られたメールアドレス	14.7%
(iv) センシティブサービスのみに登録し，かつ，誰にも知られていないメールアドレス	39.5%
(v) その他	0.3%

た．例えばある参加者は，“結婚しているのにマッチングサービスを利用すべきではないから”，と回答した．

5.2.2　知人のアカウント所有を知りたい願望

アカウント所有特定攻撃は高度な技術を要しないため，知人のアカウント所有を知りたい願望をもつ人物が実際に攻撃者になることも考えられる．そこで，知人のアカウント所有を知りたい願望をもつ参加者，つまり，潜在的な攻撃者がどれほどいるか調査した．参加者に，メールアドレスを知っている知人が特定のサービスのアカウントを所有しているか知りたいと感じたことがこれまでにあるか尋ねた．結果，25.3%（113/447）の参加者が “ある” と回答した．なお，社会的望ましさのバイアス（social desirability bias）により，実際の潜在的な攻撃者の割合はこれより多い可能性がある．そのうち 38 名が具体的な動機を挙げた．インサイダーによる攻撃の動機は Usmani ら [4] によって明らかにされているため，本研究ではそれをもとに演繹的コーデイングを実施した．2 名のコーダーによるコーディングの信頼性はコーエンのカッパ係数で k=0.85 であった．

63.2%（24/38）の回答は嫉妬（Jealousy）に分類された．多くの参加者がパートナー，元パートナー，片思いの相手，失恋相手等がマッチングサービスを利用しているかを気にしていた．34.2%（13/38）の回答は好奇心（Curiosity）に分類され，参加者は知人の趣味趣向や状況に関する好奇心を持っていた．“友人の趣味を知ってより親しくなりたい”，“同僚が転職を検討しているのか知りたい” といった回答が挙がった．参加者の一人（2.6%）の回答は，Usmani ら [4] の調査にはない，心配（Worry）に分類した．具体的には “子供が危険なサービスを使っていないか心配だから” といった親心が述べられていた．

5.2.3　センシティブサービスにおけるセキュリティ行動

本攻撃の潜在的な被害者の割合を明らかにするために，センシティブサービスがあると答えた 367 名の参加者に対し，センシティブサービスに登録するメールアドレスを尋ねた．選択肢と結果を表 6 に示す．選択肢（i）と（iii）を選択した 45.2%（166/367）の参加者は他人に知られたメールアドレスを登録しており，本攻撃の潜在的な被害者と言える．興味深いことに，選択肢（iii）と（iv）を選択した 54.2%（199/367）の参加者は，センシティブサービスとそうでないサービスを区別するというセキュリティ行動を見せたが，本攻撃に対して適切な行動は（iv）だけである．

6.　議論

6.1　プライバシーとユーザビリティ

各種ログイン関連メッセージにおけるプライバシーリスクとユーザビリティはトレードオフの関係にある．例えばログイン画面において，安全なメッセージ（表 1 L–SM）が表示された際には，ユーザはログインエラーの原因を直ちには特定できない．このように安全なログインメッセージの導入はユーザにログイン試行回数の増加をもたらしうるが，ログイン画面においてユーザへの適切な説明と誘導を行うことでユーザの負担を軽減できると考えられる．例えば，ユーザにパスワードリカバリー画面でメールアドレスを入力するよう促し，そのメールアドレスにパスワード再設定用メールが届くかどうか確認させることで，ユーザはログインエラーの原因がユーザ ID（メールアドレス）とパスワードのどちらであるかを特定できる．

6.2　サービス提供者への提言

本研究のユーザ調査において参加者がセンシティブであると挙げたサービスにおいては，プライバシーを重視し，安全な各種ログイン関連メッセージを表示するのが合理的であると思われる．最も根本的な対策は，各種ログイン関連画面において，未登録，登録，変更後，退会後といった全ての状態のユーザ ID に対して，一貫したメッセージ（表 1 L–SM, PR–SM, AC–SM）を表示することである．なお，センシティブであるか一概に判断できないサービスでは，ユーザにプライバシー重視かユーザビリティ重視かどちらのメッセージを表示するか選択させることも考えられる．

6.3　ユーザへの提言

現状ではほぼ全てのサービスにおいて本攻撃が成功するため，ユーザは自身のプライバシーを守るために防御策をとる必要がある．有効な防御策は，センシティブサービスには，他人に知られておらず，推測もされない，専用のメールアドレスを登録することである．また，Sign In with Apple [6] はサービスごとに専用のランダムなメールアドレスを生成するため，本攻撃に対して有効な防御策である．既にセンシティブサービスに他人に知られたメールアドレスを登録してしまったユーザには，他人に知られていないメールアドレスへの変更が有効である．実態調査の結果，メールアドレス変更により 92.5%のサービスで本攻撃のリスクが除去されることが示された．

6.4　研究倫理

実態調査では，実サービスへの負荷を低減するために，ログイン試行回数を最小限に抑えるよう注意深く評価プロセスを設計した．また，我々が用意した調査専用メールア

ドレスおよびアカウントのみを利用したため，一般ユーザがこの調査に関わることは一切なかった．ユーザ調査は所属組織の承認を得て実施した．

本研究で扱った各種ログイン関連メッセージの欠陥は，個別のソフトウェアの脆弱性でなく，サービス全般の設計に起因する問題である．このため，個別の事業者に対する通知よりも，本研究で明らかにした問題と対策方法をアプリケーション設計のガイドライン等に追記して広く世の中に普及させることが効果的だと考えた．よって本研究内容を IPA，JPCERT/CC，OWASP に情報共有し，これまでに OWASP が発行するアプリケーション設計のガイドラインである ASVS [7] および Authentication Cheat Sheet [8] に問題提起と対策方法を追記して改定することに貢献した．さらに IPA の “安全なウェブサイトの作り方” についても改定の追加項目の一つとして調整を進めている．

7. 関連研究

7.1 アカウントセキュリティ

Bonneau らは，ウェブサイトのログインメッセージがアカウント所有特定に繋がる危険性を言及した [1]．本研究も各種ログイン関連メッセージに着目しているが，以下の点で Bonneau らの研究と大きく異なる．本研究では，有名サービスとセンシティブサービスの両方，ウェブサイトとモバイルアプリの両方を調査する等，包括的な実態調査を行った．また，Bonneau らがアウトサイダーによる攻撃を想定し，CAPTCHA 等の試行回数制限の実装を有効と見なして調査したのに対し，本研究ではインサイダーによる攻撃を想定したため，試行回数制限を有効と見なしていない．さらに本研究では，各種ログイン関連メッセージの欠陥の根本的原因が，Bonneau らが指摘したメッセージ内容の冗長性でなく，登録および未登録ユーザ ID に対するメッセージの非一貫性にあると指摘した．

アカウント所有特定攻撃は，他にも Bortz ら [9] と Schrittwieser ら [10] によって言及されている．Bortz らは登録および未登録ユーザ ID に対するシステムの応答時間の違い，Schrittwieser らは SMS のアドレス帳機能をもとに攻撃を実証した．さらに，アカウント特定攻撃として，友人検索機能を悪用するもの [11] やユーザブロック機能を悪用するもの [12] 等がある．これらの攻撃手法は，タイミングサイドチャネル [9, 12], CSRF [9, 12], サービス特有の機能の悪用 [10–12] に大別できる．これらの分類の手法に対し本攻撃は，少ない試行回数での決定論的アプローチである点，攻撃用スクリプトにアクセスさせる必要がない点，アカウント制のサービス全般で攻撃可能な点で各々異なる．

7.2 インサイダーによるプライバシー侵害

最近の研究では，インサイダーによるプライバシー侵害の実態が明らかにされている．Freed らは，親密なパートナーからのプライバシー侵害においては高度な技術力を要しない行為（物理的な脅し行動，スパイウェアのインストール等）が行われていることを示した [2]．また，サイバーストーキングはインサイダーからの被害が多いことや [3]，インサイダーからの Facebook アカウントへの不正アクセスに関して加害者・被害者がともにユーザ調査参加者の二割以上存在することが明らかになっている [4]．本研究で述べた攻撃も高度な技術は不要であり，インサイダーにより遂行される可能性が十分に考えられる．

8. おわりに

本研究では，インサイダーによる脅威モデルに着目し，センシティブサービス上で標的のアカウントの所有を特定する新しいプライバシー脅威を発見した．実態調査の結果，ほぼ全てのサービスにおいて本攻撃が成功することを示した．また，ユーザ調査の結果，80%以上の参加者にセンシティブなサービスが存在すること，その約半数の参加者に本攻撃の被害者になりうる行動が見られること，参加者の 25%が攻撃者としての願望を秘めていることが判明した．これらの結果から，本攻撃がユーザへ深刻な影響を及ぼすことが示された．さらに我々はサービス提供者およびユーザへ実用的な提言を行うとともに，OWASP のガイドライン改定に貢献した．

参考文献

[1] J. Bonneau and S. Preibusch, “The password thicket: technical and market failures in human authentication on the web,” In *Proc.* of *WEIS*, 2010.

[2] D. Freed *et al*, “A Stalker’s Paradise: How intimate Partner Abusers Exploit Technology,” In *Proc.* of *CHI*, 2018.

[3] H. Dreßing *et al*, “Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims,” *Cyberpsychology, Behavior, and Social Networking*, vol.17, 2014.

[4] W. A. Usmani *et al*, “Characterizing Social Insider Attacks on Facebook,” In *Proc.* of *CHI*, 2017.

[5] Amazon Mechanical Turk, `https://www.mturk.com/`

[6] Sign In with Apple, `https://developer.apple.com/sign-in-with-apple/`

[7] OWASP, “Application Security Verification Standard,” `https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project`

[8] OWASP, “Authentication Cheat Sheet,” `https://www.owasp.org/index.php/Authentication/_Cheat_Sheet`

[9] A. Bortz *et al*, “Exposing private information by timing web applications,” In *Proc.* of *WWW*, 2007.

[10] S. Schrittwieser *et al*, “Guess Who’s Texting You? Evaluating the Security of Smartphone Messaging Applications,” In *Proc.* of *NDSS*, 2012.

[11] M. Balduzzi *et al*, “Abusing Social Networks for Automated User Profiling,” In *Proc.* of *RAID*, 2010.

[12] T. Watanabe *et al*, “User Blocking Considered Harmful? An Attacker-controllable Side Channel to Identify Social Accounts,” In *Proc.* of *EuroS&P*, 2018.