

情報漏えいリスクを最適化するアカウント管理手法の評価

秋山 巧^{1,a)} 大谷 和也¹ 柿崎 淑郎¹ 佐々木 良一¹

概要：我々は複数の Web サービスに対してパスワードの使い回しを許容することで、ユーザの負担を軽減しつつ、情報漏えいリスクを低下するアカウント管理手法を提案している。本稿では、提案するアカウント管理手法の有用性評価について述べる。本稿では情報漏えいリスク値という指標を定め、情報漏えいリスク値が最小かつユーザが覚えるパスワードの個数が最小になる場合について考察する。結果として、パスワードの個数は α 群で5個、 β 群で7個となり、その有用性が示された。

TAKUMI AKIYAMA^{1,a)} KAZUYA OTANI¹ YOSHIO KAKIZAKI¹ RYOICHI SASAKI¹

1. はじめに

IPA で公開されているオンライン本人認証方式の実態調査 [1] によると、パスワードリスト攻撃の認知件数が平成 25 年には平成 24 年比で 7 倍にも増加しており、パスワードリスト攻撃は激化している。パスワードリスト攻撃とは、図 1 に示すように、悪意ある攻撃者が大量の ID とパスワードを組み合わせたリストを使い、Web サイトへの不正ログインを試みる不正アクセスの一種である。図 1 に示すように、ユーザが複数の Web サイトに同じパスワードを使い回している状況では、攻撃者が不正ログインに成功してしまうと、他の Web サイトでも同様に不正ログインされてしまう恐れが高くなる。

パスワードリスト攻撃の対策としては、Web サイト毎に異なる ID とパスワードの設定、シングルサインオンや二要素認証の導入などがある。野村総合研究所の調査では、ユーザが Web サービスを使う際に確実に覚えられる ID とパスワードの組み合わせの数は、平均 3.1 個という結果が出ている [2]。また、エムオーテックの調査によれば、3 人に 1 人は同じパスワードを設定し、複数の Web サイトで利用しているという結果が出ている [3]。このように、複数の ID とパスワードの組み合わせを覚えきれなかったり、それらの記憶にかかるコストが高いなどユーザの負担が大きい。

シングルサインオンや二要素認証の導入は、サーバ側での対応が必要であり、ユーザ側のみでの対応はできない。

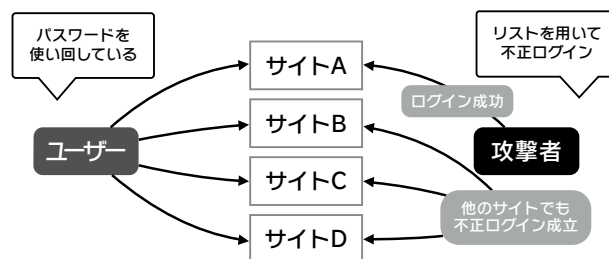


図 1 パスワードリスト攻撃

そこで、ユーザ側のみでできる対策としてパスワードマネージャの利用が考えられる。パスワードマネージャによって、異なる多数のパスワードを集中管理することが可能になり、パスワードの使い回しを防ぐことができる。しかし、パスワードマネージャの利用率は低い現状がある [1]。そのため、パスワード使い回しが行われる現状に対して、多くのユーザが受け入れられる簡便なパスワード管理方式が求められている。

我々は 2015 年に複数の Web サービスに対してパスワードの使い回しを許容することで、ユーザの負担を軽減しつつ、情報漏えいリスクを低下するアカウント管理手法を提案している [4]。本提案手法では、パスワードリスト攻撃による情報漏えいリスクをコントロールし、情報漏えい被害を最小限に抑えることを目的としている。本稿では、提案手法であるアカウント管理手法について、以下の 2 要件を満たすかどうかについて、その有用性を評価する。

要件 1 パスワードリスト攻撃を受けても漏えいする属性を最小限とする

要件 2 記憶すべきパスワードの個数を極力減らす

¹ 東京電機大学
Tokyo Denki University
^{a)} 12fi003@ms.dendai.ac.jp

2. 関連研究

Florêncio らは、パスワードについての研究文献の多くが Web サービスの安全確保やパスワードの基準の設定において実際には役に立たないことから、パスワードの耐久性、強力なパスワードの耐久性の基準を現実的に調査した [5]. その結果、強力なパスワードの作成は記憶するコストに対して、得られるメリットが少ないということがわかった. 文献 [5] ではユーザに対して重要な情報を保有していないアカウントは手間をかけず、重要な情報を保有しているアカウントに焦点を絞ると良いと述べられている.

また、安全なパスワードについて、以下の2つが通説とされている [6].

- (1) パスワードはランダムで強固なものであるべきだ.
- (2) パスワードはアカウント全体で再利用するべきではない.

しかし、実際にはユーザはこれを満たすことはできておらず、複数の強固なパスワードを記憶する決定的な方法はない. そこで文献 [6] では、パスワード管理におけるユーザの労力と情報漏えいしたときに予想される被害を最小化するために、アカウントのグループ分けを行い、それらにパスワードの使い回しを許容としたときに、どのような影響があるかを調査をした. その結果、パスワードの使い回しを許容するとパスワードは強固になり、パスワードの使い回しを許容しないとパスワードは強固ではなくなり、パスワードの使い回しの許容とパスワードの強度とにトレードオフの関係であることが分かった. また、グループ分けをしてパスワードの使い回しを許容した場合、情報漏えいの確率は上がるが予想される被害は低くなることが示された. Florêncio らは、ランダムで強固なパスワードを大量に管理することは実際的には困難であり、脆弱なパスワードまたはパスワードの使い回しを許容しないパスワード管理手法は最適ではないと主張している.

以上を踏まえ、大谷らは、ユーザが実際にアカウントを作成する際にどのような情報が求められるかに基づき、アカウントのグループ分けを行った [4]. アカウント作成の際に求められた情報が似通ったアカウント同士をグループにし、それらにパスワードの使い回しを許容したときに、どのような情報が漏えいする恐れがあるのかを具体的に示した.

パスワードリスト攻撃に対する対策としては、パスワードマネージャの利用、シングルサインオンや二要素認証の導入などがある. しかしいずれもサービス利用者に一定の負担を課すことになる. 高田はパスワードリスト攻撃の対策手法として、個人認証利用者が個人認証の利用可否を自ら制御する「認証シャッター」を提案している [7]. この手法では、いわゆる「シャッター」によって認証を遮断することで、正規利用者が利用する場合のみシャッターを開け

表 1 調査したサイト (一部抜粋)

サイト名	ユーザ名	名前	メールアドレス	携帯番号	国	性別
Google	○	○	○	○	○	△
楽天	○	○	○	×	×	×
Amazon	○	○	○	×	×	×
mixi	○	○	○	×	×	○

て、不正アクセスを防いでいる.

3. アカウント管理手法

本章では、大谷らの提案したアカウント管理手法 [4] について述べる.

3.1 アカウント情報の調査

不正ログインによってどのような情報が漏えいするかを確認するために、Alexa Top 500 (2015 年 1 月 5 日時点) より日本からのアクセスが多い上位 50 サイトを対象に、アカウント情報の調査を行った. これら 50 サイトをまとめて**調査済みサイト群**と呼ぶ. 調査したアカウント情報を以下の4種類に分類した.

登録されている情報

登録されている情報とは、アカウント作成時に必須とされている項目とする. なお、アカウント作成時に要求されるが必須ではない項目については、**登録されていない情報**とした.

登録されていない情報

登録されていない情報とは、アカウント作成時に要求されない情報および、必須ではない項目とする. また、**登録されていない情報は確認できない情報**である.

確認できる情報

確認できる情報とは、マイページ等にログインした際に確認することができる情報であり、**登録されている情報**である. アカウントには様々な情報が記録されているが、その全てを確認できるわけではない. 例えば、マイページなどにおいて、ユーザ名のように表示される情報の他にも、変更は可能だが表示されない情報などがある. このうち、ログイン後には確認することができる情報を**確認できる情報**とする.

確認できない情報

確認できない情報とは、登録されていない情報および登録されている情報のうちマイページ等で確認することができない情報のことである.

調査結果として各サイトにおける**確認できる情報**の一部抜粋を表1に示す. 表1中の○が**確認できる情報**, △が**確認できない情報**, ×が**登録されていない情報**である. 本稿では、これらの情報を総称して**属性**と呼ぶ.

3.2 アカウントのクラスタリング

類似の属性を持つアカウントの組み合わせを得るために、

確認できる情報を用いてアカウントの類似度を算出し、クラスタリングを行う。クラスタリングとは、ある集合を似たような特徴を持ついくつかの集合に分けるものであり、分けられた集合のことをクラスタと呼ぶ。アカウントのクラスタリングにより、類似の属性を持つアカウントの組み合わせを得ることができる。

類似の属性を持ったアカウント同士でグループ分けを行うため、コサイン類似度と k -means 法を用いてクラスタリングを行う。

コサイン類似度の計算式は以下の通りである。

$$\cos \theta = \frac{x \cdot y}{\|x\| \|y\|} \quad (1)$$

式 1 の x と y は**確認できる情報**と**確認できない情報**を要素としたベクトルである。

k -means 法の手順は以下の通りである。

- (1) ある集合に対して、無作為に中心点を k 個作成する。
この k がクラスタ数となる。
- (2) 各データを中心点に一番近いもの同士でグループ分けする。
- (3) 各中心点をグループの中心に移動する。
- (4) 中心点が動かなくなるまで、手順 2, 3 を繰り返す。

4. アカウント管理手法の評価

大谷らは 3 章で述べたアカウント管理手法 [4] を提案しているが、その評価は十分に行われていない。

本稿では、大谷らのアカウント管理手法の評価を目的とする。

Web サービスを利用するユーザにとって、アカウント管理手法が有用であるかを評価する。そこで、有用性の達成要件を以下のように設定した。

要件 1 パスワードリスト攻撃を受けても漏えいする属性を最小限とする

属性が漏えいした場合の脅威を定量的に評価し、不正ログインした際にアカウントから漏えいする属性を最小限にすることで、情報漏えいリスクをコントロールする。

要件 2 記憶すべきパスワードの個数を極力減らす

ユーザの記憶できるパスワードの個数は限られている一方で [2], パスワードマネージャなどの普及は進んでおらず [1], ユーザが記憶するパスワードの個数は少なくなることが望ましい。

4.1 アンケート調査

有用性を評価のための指標を定めるために、本学の学生を対象にアンケート調査を実施した。有効回答数は 88 件であった。

4.1.1 設問とその説明

アンケートの設問とその説明を以下に示す。

所持しているアカウントは何か

調査済みサイト群のうち、所持しているアカウント全てを選択してもらった。

他人（第三者）に知られたら困る情報は何か

属性のうち、回答者が「他人（第三者）に知られたら困る」と感じた情報全てを選択してもらった。本稿では、この情報のことを**機微情報**と呼ぶ。

パスワードの使い回しをしているか

複数のアカウントでパスワードを使い回しているかについて、「はい」か「いいえ」で答えてもらった。さらに、使い回しをしている人については、なぜ使い回しをするのかを尋ねた。以下 5 点の選択肢のうち、当てはまるもの全てを選択してもらった。

- 異なるパスワードが多くなると管理するのが大変だから
- 新しいパスワードを考えるのが面倒だから
- Web サービスへログインしようとするたびにパスワードを参照するのが面倒だから
- パスワードを使い回すことが危険なことだという認識がなかったから
- その他（自由記載）

パスワードをどのように管理しているか

パスワードをどのように管理しているかについて、以下 5 点の選択肢から選択してもらった。

- 記憶している
- メモに記入している
- パスワードマネージャ（専用ソフト）を利用している
- パスワードマネージャ（ブラウザ）を利用している
- その他（自由記載）

4.1.2 結果

各設問への回答の内訳を述べる。

所持しているアカウントは何か

回答の内訳を図 2 に示す。アカウント所持率とは、Web サービス毎に、そのアカウントを所持している回答者の割合をいう。

他人（第三者）に知られたら困る情報は何か

回答の内訳を図 3 に示す。各属性について、「その属性が他人（第三者）に知られたら困る」と感じた回答者数の割合を示している。この回答は、複数回答可能としている。

パスワードの使い回しをしているか

パスワードの使い回しをしているかで「はい」と答えた人は 88 人中 79 人おり、回答者全体の約 90%にも及ぶことが分かった。パスワードの使い回しをする理由の内訳を図 4 に示す。「異なるパスワードが多くなると管理するのが大変だから」と回答した人は 79 人中 73 人おり、約 92%の人が多くの異なるパスワードの管理を大変だと感じていることが分かった。

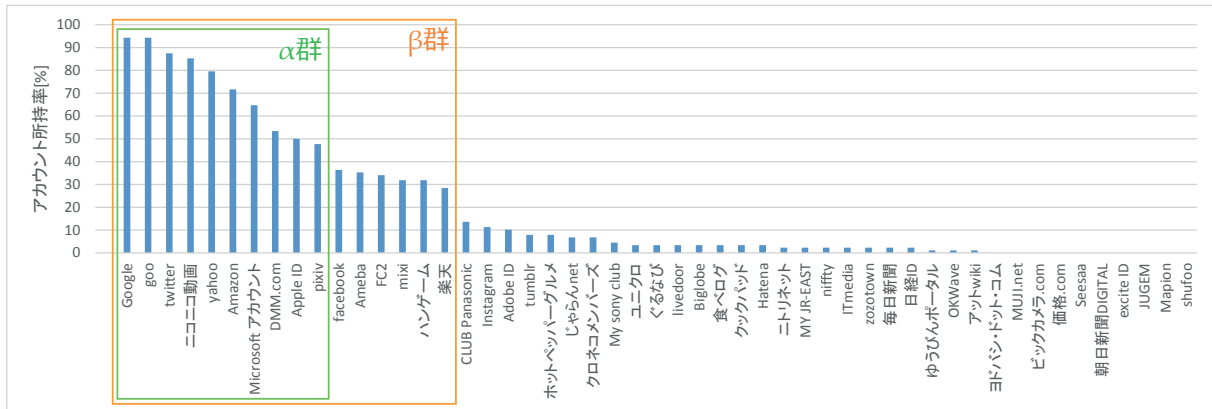


図 2 Web サービス毎のアカウント所持率

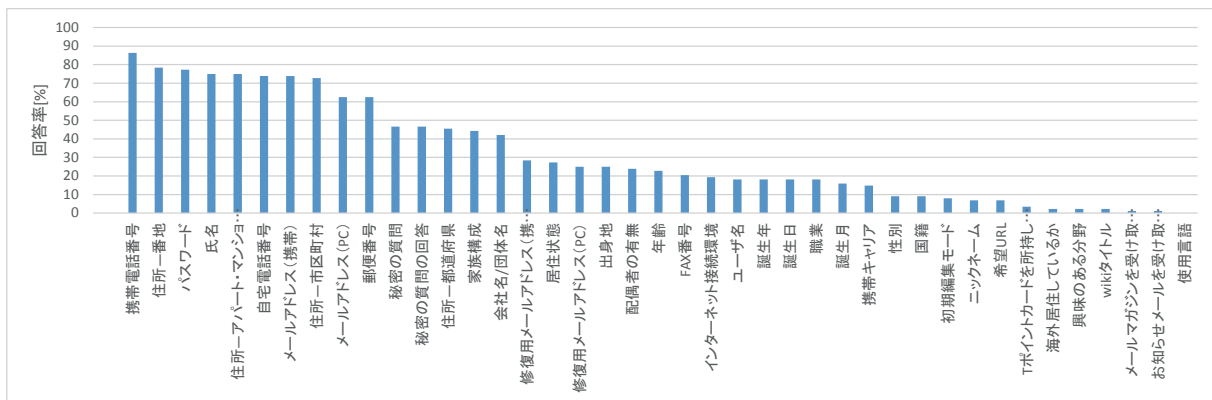


図 3 他人（第三者）に知られたら困ると感じた情報とその回答者の割合

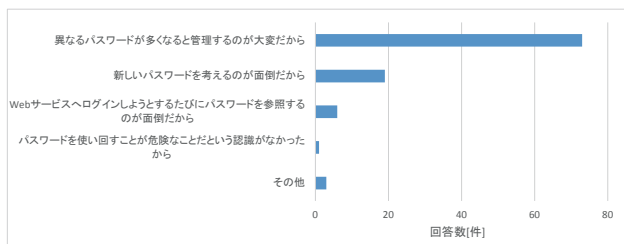


図 4 パスワードの使い回しをする理由

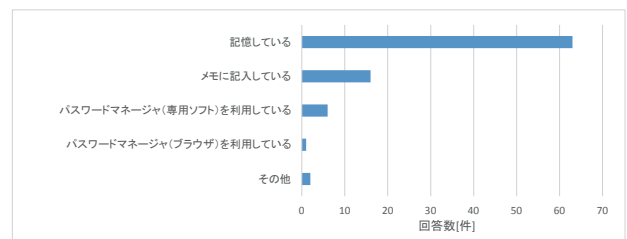


図 5 パスワードをどのように管理しているか

パスワードをどのように管理しているか

回答の内訳を図5に示す。「記憶している」と回答した人は88人中63人おり、パスワードの管理は主に記憶に頼っていることが明らかになった。また自由記載欄にて、「自分のみが知る特定の法則に基づいて各 Web サービスのパスワードを作成し、入力のためにパスワードを思い出している」と回答した人がいた。大きくとらえればこれも記憶に頼っているが、独自のルールを決めてパスワードを作成しているため、単にパスワードを記憶するよりも想起しやすいと思われる。

4.2 有用性評価

アンケート調査で得られた結果に基づいて、アカウント管理手法の有用性を評価する。

4.2.1 評価手順

文献 [5] で Florêncio らが述べるように、機微情報を保

持しているアカウントには注力し、機微情報を保持していないアカウントにかかるコストを削減するべきである。そのため、機微情報を保持するアカウントを除外して、機微情報を保持しないアカウントに対してクラスタリングを行う。クラスタ数は k を変化させてクラスタリングを行い、各クラスタリング結果における情報漏えいにおけるリスク値を評価し、リスク値が最小となるクラスタ数を求める。

本評価実験で用いるアカウント、機微情報、情報漏えいリスク値の定義を以下に示す。

アカウント

ユーザによって所持しているアカウントが異なるため、ユーザに合わせてアカウントを選定しなければならない。そこで本評価実験では、図2に示す集計結果からクラスタリング対象とするアカウントを以下のように設定した。

α群 回答者全体の40%以上が所持しているアカウント

表 2 属性の情報漏えいリスク値 (一部抜粋)

属性	情報漏えいリスク値
携帯電話番号	-
番地	0.784
パスワード	0.772
名前	0.750
アパート・マンション・ビル	0.750
自宅電話番号	0.738
携帯メールアドレス	0.738
市区町村	0.727
PC メールアドレス	0.625
郵便番号	0.625

(Google から pixiv まで 10 個)

β群 回答者全体の 20%以上が所持しているアカウント

(Google から楽天まで 16 個)

機微情報

ユーザによって機微情報の捉え方が異なっていることは、アンケートの結果から明らかである。そこで本評価実験では、図 3 に示す集計結果から機微情報を以下のように設定した。

- (1) 回答者全体の 80%以上が機微情報だとしている属性 (携帯電話番号)

情報漏えいリスク値

本評価実験では情報漏えいリスク値として、図 3 に示す集計結果より、各属性への回答率を採用した。表 2 に各属性の情報漏えいリスク値の一部抜粋を示す。なお、「携帯電話番号」は機微情報であり、この属性を含むアカウントはクラスタリング対象外となるため、情報漏えいリスク値を設定しない。

用いるアカウントで分けた α 群、 β 群のそれぞれに対して、機微情報を含むアカウントを除外した後に、残ったアカウントでクラスタリングを行い、クラスタリング結果毎に情報漏えいリスク値を求める。具体的には、クラスタに含まれる各属性の情報漏えいリスク値の総和を各クラスタの情報漏えいリスク値とする。

4.2.2 評価結果

表 4 に α 群の算出された情報漏えいリスク値を示す。図 6 に α 群のクラスタリング結果を示す。図 6 中の番号はクラスタを識別している。表 3 に情報漏えいリスク値が最小だった $k = 4$ におけるクラスタ毎のアカウント内訳を示す。ここで、 $k = 1$ は全てのアカウントにパスワードを使い回している状態であり、 $k = 9$ は全てのアカウントに独立したパスワードを設定している状態である。

また、表 6, 7, 8 に、 $k = 4$ におけるクラスタ 1, 2, 3 に属するアカウントが保持している属性を示す。なお、クラスタ 4 は一つのアカウントしか含まないため、本文中で示す。表 6, 7, 8 中における○は**確認できる情報**、×は**確認できない情報**である。

表 3 α 群の $k = 4$ におけるクラスタ毎のアカウント内訳

クラスタ 1	pixiv ニコニコ動画		
クラスタ 2	Twitter	DMM.com	Amazon
クラスタ 3	Yahoo!	Microsoft	goo
クラスタ 4	Apple ID		
(除外したアカウント)	Google		

表 4 α 群の算出された情報漏えいリスク値

k	情報漏えいリスク値	k	情報漏えいリスク値
1	5.375	6	4.215
2	5.375	7	4.215
3	4.375	8	4.215
4	4.215	9	2.784
5	4.215		

表 5 β 群の算出された情報漏えいリスク値

k	情報漏えいリスク値	k	情報漏えいリスク値
1	5.852	8	4.215
2	4.602	9	4.215
3	4.784	10	4.215
4	4.784	11	4.215
5	4.215	12	4.215
6	4.215	13	4.215
7	4.215	14	2.784

表 5 には β 群の算出された情報漏えいリスク値を示す。

5. 考察

まず、 α 群において情報漏えいリスク値が最小かつ k が最小の $k = 4$ におけるクラスタリング結果と算出された情報漏えいリスク値について考察する。

表 6 に示すクラスタ 1 が保持している属性より、クラスタ 1 に属する全てのアカウントに同じパスワードを設定し、パスワードリスト攻撃をされた場合、ニックネーム、ユーザ名、生年月日、性別、PC メールアドレス、国籍、都道府県、使用言語が漏えいする。これらの属性の情報漏えいリスク値は、表 9 に示す通りである。これらの総和である 1.644 がクラスタ 1 の情報漏えいリスク値となる。

表 7 に示すクラスタ 2 が保持している属性より、クラスタ 2 に属する全てのアカウントに同じパスワードを設定し、パスワードリスト攻撃をされた場合、ニックネーム、名前、ユーザ名、PC メールアドレスが漏えいする。これらの属性の情報漏えいリスク値は、表 10 に示す通りである。これらの総和である 1.624 がクラスタ 2 の情報漏えいリスク値となる。

表 8 に示すクラスタ 3 が保持している属性より、クラスタ 3 に属する全てのアカウントに同じパスワードを設定し、パスワードリスト攻撃をされた場合、名前、ユーザ名、生年月日、性別、PC メールアドレス、国籍、郵便番号、職業、インターネット接続環境が漏えいする。これらの属性

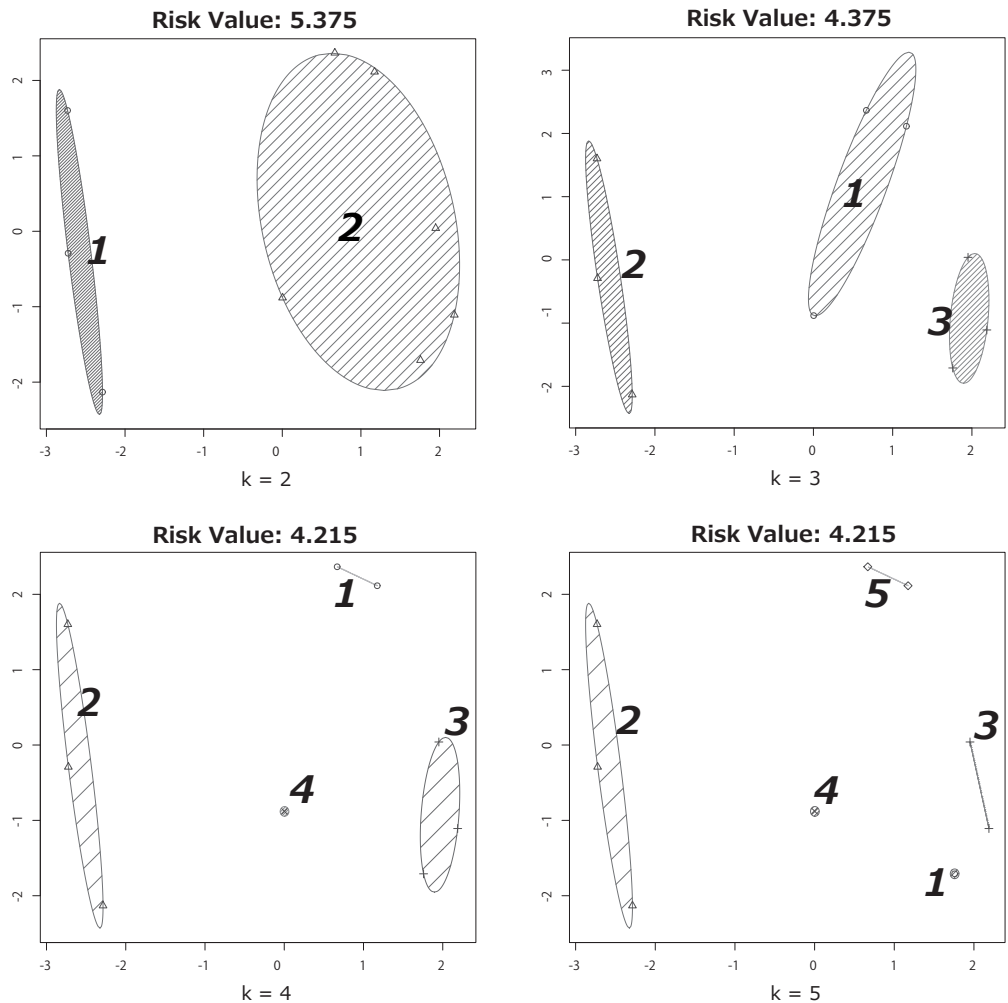


図 6 α 群のクラスタリング結果と算出された情報漏えいリスク値 ($k = 2, 3, 4, 5$)

表 6 クラスタ 1 が保持している属性

サイト名	ニックネーム	ユーザ名	生年月日	性別	PC メールアドレス	国籍	都道府県	使用言語
ニコニコ動画	○	○	○	○	○	○	○	×
pixiv	○	○	○	○	○	×	×	○

表 7 クラスタ 2 が保持している属性

サイト名	ニックネーム	名前	ユーザ名	PC メールアドレス
Twitter	○	×	○	○
Amazon	×	○	○	○
DMM.com	×	×	○	○

表 8 クラスタ 3 が保持している属性

サイト名	名前	ユーザ名	生年月日	性別	PC メールアドレス	国籍	郵便番号	職業	インターネット接続環境
goo	○	○	○	○	○	×	○	○	○
Yahoo!	×	○	○	○	○	×	○	×	×
Microsoft	○	○	○	○	○	○	○	×	×

の情報漏えいリスク値は、表 11 に示す通りである。これらの総和である 2.871 がクラスタ 3 の情報漏えいリスク値となる。

クラスタ 4 は Apple ID のみであり、名前、ユーザ名、生年月日、PC メールアドレス、国籍、都道府県、市区町村、

番地、秘密の質問、使用言語を保持している。これらの属性の情報漏えいリスク値は、表 12 に示す通りである。これらの総和である 4.212 がクラスタ 4 の情報漏えいリスク値となる。

各クラスタ中で最も情報漏えいリスク値が大きいクラス

表 9 クラスタ 1 が保持している属性の情報漏えいリスク値

属性	情報漏えいリスク値
ニックネーム	0.068
ユーザ名	0.181
生年月日	0.136
性別	0.090
PC メールアドレス	0.625
国籍	0.090
都道府県	0.454
使用言語	0

表 10 クラスタ 2 が保持している属性の情報漏えいリスク値

属性	情報漏えいリスク値
ニックネーム	0.068
名前	0.750
ユーザ名	0.181
PC メールアドレス	0.625

表 11 クラスタ 3 が保持している属性の情報漏えいリスク値

属性	情報漏えいリスク値
名前	0.750
ユーザ名	0.181
生年月日	0.136
性別	0.090
PC メールアドレス	0.625
国籍	0.090
郵便番号	0.625
職業	0.181
インターネット接続環境	0.193

表 12 クラスタ 4 が保持している属性の情報漏えいリスク値

属性	情報漏えいリスク値
名前	0.750
ユーザ名	0.181
生年月日	0.136
PC メールアドレス	0.625
国籍	0.090
都道府県	0.454
市区町村	0.727
番地	0.784
秘密の質問	0.465
使用言語	0

タ 4 の 4.212 が $k=4$ におけるクラスタリングの情報漏えいリスク値となる。なお、図 6 の $k=4$ の情報漏えいリスク値は 4.215 となっているが、これは丸め誤差の影響である。

α 群の算出された情報漏えいリスク値について考察する。 $k=9$ はクラスタリング対象のアカウント数とクラスタ数が同じため、パスワードの使い回しを全くしていない状況を表す。対して、 $k=1$ は α 群の全アカウントについてパスワードを使い回している状況を表す。クラスタ数 k の増加に伴い情報漏えいリスク値が低下していることから、パスワードの使い回しをしないほど情報漏洩リスク値は低く抑えられ、つまり安全であると言える。パスワード

の使い回しを許容する場合、情報漏えいリスク値は $k=4$ から $k=8$ にかけて一定となり、最も低い値である。よって、要件 1 と要件 2 を満たす最適な k は 4 である。機微情報を保持する Google には個別にパスワードを設定するため、ユーザが記憶すべきパスワードの数は 5 個となる。

β 群の算出された情報漏えいリスク値について考察する。 $k=14$ はクラスタリング対象のアカウント数とクラスタ数が同じため、パスワードの使い回しを全くしていない状況を表す。パスワードの使い回しを許容する場合、情報漏えいリスク値は $k=5$ から $k=13$ にかけて一定となり、最も低い値である。よって、要件 1 と要件 2 を満たす最適な k は 5 である。機微情報を保持する Google と Facebook には個別にパスワードを設定するため、ユーザが記憶すべきパスワードの数は 7 個となる。

なお、 β 群においては表 5 から分かるように、 $k=3$ よりも $k=2$ の方が小さい情報漏えいリスク値となっている。今回は属性の類似性に着目してクラスタリングを行っているため、クラスタリング結果が必ずしも情報漏えいリスク値を最小とするものではない。そのため、いわゆる局所解に陥ったものと推測される。しかし、本研究では各 k における厳密な情報漏えいリスク値を求めることが目的ではなく、情報漏えいリスク値が最小かつ最小となる k を求めることが目的である。情報漏えいリスク値を加味したクラスタリングを行うことで厳密解を求めることもできるが、本研究の目的と簡便さから考えて、大きな問題にはならない。

6. おわりに

本稿では大谷らが提案したアカウント管理手法 [4] について、情報漏えいリスク値という指標を導入し、その有用性を評価した。その結果、アカウント 10 個の α 群に対してはパスワード 5 種類、アカウント 16 個の β 群に対してはパスワード 7 種類を設定することで、ユーザの負担を軽減しつつ、情報漏えいリスクを最適化できることが分かった。管理すべきパスワードの数を減らすことでユーザの負担を軽減しつつ、情報漏えいリスクを最適化できるため、大谷らのアカウント管理手法は有用であると言える。

今後の展望として、異なるアカウント群、機微情報を設定した場合、つまり個々のユーザに適応した状況でも情報漏えいリスク値とパスワード数の最適化が望めるかを検証する必要がある。そのために、多くのユーザが所有しているアカウントを選択し、機微情報を設定することで、クラスタリング結果を得られるツールの開発が必要である。

参考文献

- [1] IPA 独立行政法人情報処理推進機構：オンライン本人認証方式の実態調査、入手先 (<http://www.ipa.go.jp/security/fy26/reports/ninsho/>) (参照 2015-02-06)。
- [2] 株式会社野村総合研究所：利用者登録する商品・サービスを選別する傾向が強まった生活者と顧客情報の鮮度維

- 持を望む事業者～生活者と事業者を対象とした ID に関する実態調査～, 入手先 (<http://www.nri.com/jp/news/2012/120208.html>) (参照 2015-02-02).
- [3] エムオーテック株式会社: パスワード情報漏えい “パス漏れ” に要注意!! 3 人に 1 人が同じパスワードで複数の Web サービスを利用!, 入手先 (<http://www.motex.co.jp/nomore/report/1105/>) (参照 2015-02-02).
- [4] 大谷和也, 柿崎淑郎, 佐々木良一: 情報漏えいリスクを低減したアカウント管理手法, 情報処理学会研究報告, Vol.2015-IS131 No.1, pp.1-6 (2015).
- [5] Dinei Florêncio, Cormac Herley and Paul C. van Oorschot: An Administrator’s Guide to Internet Password Research, *Proc. The 28th Large Installation System Administration Conference (LISA14)*, pp.44-61, (2014).
- [6] Dinei Florêncio, Cormac Herley and Paul C. van Oorschot: Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts, *Proc. The 23rd USENIX Security Symposium (USENIX Security 14)*, pp.575-590, (2014).
- [7] 高田哲司: Authentication Shutter: 個人認証に対する攻撃を遮断可能する対策の提案, コンピュータセキュリティシンポジウム 2014 (CSS2014), 3C1-3, 2014.