復元可能な方法でパスワードを保管しているサービスの実態調査

伊東 和寿[1]　金岡 晃[1]

概要：Web サービスやアプリにおいてユーザから入力されたパスワードは重要な機密情報である。そのため外部からの不正侵入などに備えて解読が困難な状態で保管しているのが理想的とされている。代表例として SHA2 アルゴリズムを用いてハッシュ値に変換して保管するというものがある。しかし、すべての Web サービスやアプリが理想的な保管方法を実装しているとは限らない。個人情報が流出してしまう事件は多く発生しているが、その中にはサーバ側でパスワードを適切に保管しておらず平文もしくは可逆な形で暗号化保管されていたため、不正侵入などの被害にあった際にパスワードが流出したケースが存在する。本研究は、どのようなサービスやアプリが利用者のパスワードを平文もしくは可逆な形でサーバ側に保管しているかどうかの実態を外部観測調査により明らかにすることを目的とする。手法としてはサービスやアプリごとに調査対象をリストアップし、1 サービスあるいはアプリごとに調査を行う。調査の結果 Alexa によるランキングでの上位サイト、Google Play ランキングでの上位アプリともに不適切な保管方法を実装していると確認出来たサービスやアプリは存在せず、総じて平文を返すサービスが多くはないことが本調査により明らかになった。

1. はじめに

Web サービスやアプリケーション（以後アプリと呼ぶ）においてユーザから入力されたパスワードは重要な機密情報である。そのため外部からの不正侵入などに備えて解読が困難な状態で保管していることが理想的とされている。代表例として SHA-256 に代表される暗号学的ハッシュ関数を用いてパスワードをハッシュ値に変換して保管する手法がある。しかし、すべての Web サービスやアプリが理想的な保管方法を実装しているとは限らない。

Web サービスやアプリにおいて個人情報が流出してしまう事件が複数存在している。様々な原因があるとされているが、その 1 つにサーバ側がパスワードを適切に保管しておらず、平文または可逆な形で暗号化保管していたため、不正侵入などの被害にあった際にパスワードそのものが流出するケースが存在する。

利用者が設定するパスワードはサービスやアプリごとに異なるものを付けることが理想的であるが、実際には利用者はしばしば同じパスワードを複数のサービスやアプリに使いまわす傾向があることが知られている [1]。そういった利用者の行動特性を完全に変えることは難しいことを考えれば、パスワードの保管を平文または可逆な形で暗号化保存することは避けるべきである。

本研究ではどのようなサービスやアプリが平文または可逆な形でパスワードをサーバ側に保管しているのかどうかの実態を調査し、それらのサービス間特有の共通点を調査する。サービスやアプリが平文または可逆な形でパスワードをサーバ側に保管しているのかどうかの実態調査として、代表的な Web サービスやアプリに対し外部観測を行う。

平文または可逆な形でパスワードを保管しているサービスについて調査を行ったところ、Alexa の「日本 Top ドメイン」1 位から 103 位までの Web サービスと Google Play の人気全体ランキング「無料 TopAndroid アプリ」1 位から 28 位までを調査した結果、平文または可逆な形でパスワードを保管していると断定できる Web サービスまたはアプリは発見できなかった。このことから、代表的な Web サービスやアプリにはそのようなケースは存在しないことが分かった。

そこでさらなる調査として、平文または可逆な形でパスワードを保管しているとの情報を得られたサービスに対しても調査を行った。40 件の対象を調査したところ、平文または可逆な形でパスワードを保管しているサービスを 7 件発見した。これらの調査をふまえ平文または可逆な形でパスワードを保管しているサービス間特有の共通点について Web サービスやアプリの外観とサーバから提供される

[1] 東邦大学
Toho University

HTML データの 2 つの観点から分析を行ったところ、外観において同様の形式が見られるサービスを発見した。それらの HTML データを比較したところ共通点は見つからず、原因だと考えられるような共通点を発見するには至らなかった。

本論文の構成は以下の通りである。まず第 2 章でパスワードの漏洩事例を複数挙げ、関連する研究を第 3 章で解説する。第 4 章では本研究で行ったパスワード保管方法の外部観測調査について、その調査方法と調査対象、そして調査結果を示す。第 5 章では今後の課題を述べ、第 6 章でまとめる。

2. 平文パスワード漏洩事例

2.1 宅ふぁいる便の漏洩事件

ファイル転送サービスの宅ふぁいる便から、パスワードやメールアドレス含む 480 万件もの個人情報が流出したことが 2019 年 1 月 22 日に発覚した [2]。宅ふぁいる便サービスを行っているサーバ内に不審なファイルを発見したことから発覚したとされている。追加調査で不審なアクセスログも確認され、被害防止のためサービスを同年 1 月 23 日停止、第一報を発表。その後、情報漏洩を同年 1 月 25 日確認した。漏洩件数は 480 万件でパスワードは平文で保存していたと発表されたが、漏洩した情報が不正利用された事実は確認されていないとしている。

2.2 Facebook パスワード漏洩

Facebook は 2019 年 3 月 21 日、「Keeping Passwords Secure — Facebook」 において、Facebook などのパスワードの一部が平文の形式でログファイルに記録されていたことが明らかになったとして、このセキュリティインシデントに対する Facebook の姿勢や取り組みを発表した [3]。続いて同年 4 月 18 日にリリースの内容がアップデートされ、調査の結果、Instagram のユーザー数百万人分に関してもパスワードがログに記録されていたことが明らかになったと伝えた。Facebook は該当するユーザーに対して通知を行うと説明した。

2.3 Google による G Suite の一部のパスワードの平文保存

Google は米国時間 2019 年 5 月 21 日のブログ記事で、同社サービス「G Suite」の顧客に対し、一部のパスワードを暗号化せず社内サーバーに保存していたと通知した [4]。Google Cloud Trust のエンジニアリング担当バイスプレジデント、Suzanne Frey 氏は投稿の中で、このバグは企業ユーザーにのみ影響すると述べた。

3. 関連研究

3.1 フィッシング対策協議会によるアンケート調査

フィッシング対策協議会の認証方法調査推進ワーキンググループは、インターネットサービス事業者が採用している認証方法に関して実施したアンケート調査について、その結果の一部を 2019 年 5 月に速報値として公表し、その後 7 月に正式版を公表した [5]。

当該アンケートは 2019 年 2 月 19 日から同年 28 日まで、インターネットサービスを提供している事業者に対して匿名で実施され、308 人からの有効回答が得られた。「インターネットサービスの個人認証を主にどのような方法で実施していますか？」との設問では、「ID とパスワードのみ」との回答が 77 %を占め、「多要素認証（二要素認証含）」との回答は 20 %であった。その後行われた正式版での「個人認証を主にどのような方法で実施していますか。」との設問でも、「ID とパスワードのみ」との回答が 76.9%、「多要素認証（二要素認証含）」との回答は 19.8%と速報での結果と変わらずの結果となった。

また、正式版での「Web サイト側のパスワード管理は、何らかの方法で盗まれても問題ない状態で管理（ハッシュ、暗号化など）読めない状態で管理されていますか。」との設問では、「はい」との回答が 86.4%と多数だが、「いいえ」との回答が 13.6%存在した。

これらのアンケート調査の結果より、本研究の調査対象にあたる ID とパスワードのみで認証を行っているサービスが大半を占めているということが得られた。また、パスワードをハッシュ、暗号化していないサービスが 14%もあることから、調査対象である代表的なサービスやアプリの中にもパスワードを平文もしくは可逆な形で保管しているサービスがある可能性が示されたといえる。

3.2 開発者の行動傾向

Naiakshina らは、ソフトウェア開発者がパスワードの保管をどのように実装するかについて継続的な研究を行っている。実験参加者の対象を学生、フリーランス、企業開発者とそれぞれ分けて調査を実施し、そのいずれの結果においてもパスワード保管の実装において不適切な実装が少なくない割合で行われていることを示した [6], [7], [8], [9]。

それらの結果から、適切なレクチャーを受けていない実験参加者はそもそも暗号化やハッシュ化などを施さずに保管する傾向にあることや、ハッシュ化をする際にもソルトやストレッチングの使用がされないなど、適切な保管を実装することは一般的には難しいことであることが示唆されている。

3.3 パスワードの再利用

複数のサービスを利用することが珍しくなくなった現代では、それぞれのサービスごとに異なるパスワードを設定することが望ましいが、実際には利用者はパスワードを再利用し複数サービスでパスワードを共有する傾向にある。これらは経験的には知られてきたが、2016 年に Wash らにより初めて学術的な調査が行われ、134 人の振る舞いを 6 週間にわたって調査した結果、実験参加者の中では 1 人あたり 1.7-3.4 サイトでパスワードを使いまわしていることが判明した。

利用者はパスワードを再利用をしやすいという前提にたてば、安全なパスワード保管はさらに重要性を増すことがわかる。

4. パスワード保管方法の外部観測調査

4.1 調査方法

本研究の目的は、どのようなサービスやアプリが利用者のパスワードを平文もしくは可逆な形でサーバ側に保管しているかどうかの実態を明らかにすることである。そのためのアプローチとしては外部観測と内部観測の 2 つが挙げられる。内部観測はサーバ側の機密情報を閲覧できなければ実現できないため現実的ではない。よって本研究では外部観測を用いる。

本研究では代表的なサービスやアプリから調査を行い、パスワードを平文もしくは可逆な形でサーバ側に保管しているサービスを発見後、それらを分類分けして共通点や類似点を発見するという方法を採る。まず、代表的なサービスやアプリでパスワードの再設定を試み、サービスやアプリからの応答において設定されたパスワードが返送されてくるかを見る。それによりパスワードを平文もしくは可逆な形で保管されているかを調べる。

次に、可逆な形で保管されているサービスやアプリを分類して共通点または類似点を考察、分析する。これらの調査や考察の段階を踏むことにより、問題のある保管方法を実装してしまう根本的な原因を発見できると考えた。本章ではこれらの調査対象や方法、環境の説明や調査結果を記述する。

4.2 Alexa 上位サービスの Web サイト調査

代表的なサービスにおけるパスワード保管状況を調査するため、Alexa 上位サイトに対して調査を行う。

Alexa 上位サイトのサービスそれぞれにまずユーザ登録を行い、1 度ログオフした後に再ログイン時に“パスワードを忘れた”としてアクションを起こし、その後の対応を確認する。考えられる反応としては元のパスワード開示があるされるものと元のパスワード開示がされないものの 2 種類がある。本調査では元のパスワード開示があるものを捜索していく。

4.2.1 調査対象

Web サービスには個人や企業が運営しているものを含み数多くのサービスがあるが、本研究では代表的な Web サービスを対象にパスワードの保管状況を調査することとし、Alexa が提供する「日本 Top ドメイン」[*1]を参照し、1 位から 103 位までの Web サービスを対象とした。

ユーザが使用する頻度が高く、注目度が比較的高い Web サービスがパスワードを平文もしくは可逆な形で保管しているということは、セキュリティ面での脅威の社会的影響度が高いと考えられる。

4.2.2 調査方法と環境

どのようなサービスがパスワードを平文もしくは可逆な形で保管しているのか共通点や類似点を捜索するために、指標となる項目を挙げる。調査対象のリストアップとして Alexa の日本 Top ドメインに Web ブラウザを用いてアクセスし、サービス名、登録ページの URL、ID 連携の有無や種類をリストアップする。Alexa のランキングは時間を空けると順位が変動する可能性があるため、リストアップは 1 日で実施する。ID 連携が可能なサービスもあるが、ID 連携は使わずにそれぞれのサービス独自のアカウントを作成する。

リストアップ後 1 位から 1 つずつ調査を行う。以下に調査方法を記載する。

- 登録ページ URL にアクセスし、実際にユーザ登録を行う
- 登録画面や登録の際に受信したメールはスクリーンショットを保存する
- ユーザ登録終了後同一サービスに“パスワードを忘れた”とアクションを取り、それに対しサービス側から元のパスワードが返送されるのか、されない場合どのような手続きを踏むのかなどそのリアクションにどのようなパターンがあるのかをスクリーンショットやメモを用いて記録する
  - 登録方法やパスワードの再設定方法などにそのサービス特有の特徴がある場合、それもスクリーンショットやメモを用いて記録する。

なお、アカウント登録作業を行う際に、サービスによって過去のログイン情報を読み取って自動でログインしてしまうサービスが存在する。そこで、ログイン情報の保存を避け、円滑に登録作業を進めるために Google Chrome のシークレットモードですべて行った。

4.2.3 調査結果

調査は 103 位までのサービスを対象に行った。それぞれのサービスの情報は、倫理的な観点から詳細な情報を提示することは避ける。

登録作業を行う際に各サービスの登録画面を遷移するご

[*1] https://www.alexa.com/topsites/countries/JP

とにスクリーンショットを用いて保存した。51 位以降は元のパスワード開示があるもののみスクリーンショットを取る方針とした。

Alexa の「日本 Top ドメイン」1 位から 103 位までのリストアップと調査の結果、元のパスワード開示があるものは発見できなかった。103 件中、ユーザ登録がないサービスが 9 件、海外サービスかつ電話番号登録が必要など調査実験において登録が不可能であったサービスが 26 件、サービスが終了していたサイトが 1 件あった。会員登録が完了したサイトは 67 件あり、そのうち登録アカウントが Google に依存するなど重複していたサイトを除くと 48 件となった。重複していたものは Google アカウント、Livedoor アカウント、DMM アカウント、Microsoft アカウント、Amazon アカウントだった。

図 1 は、Alexa ランキング 1、2、5、31 位の Google の登録画面とパスワードを忘れたときの対応画面である。Google は各種サービスの認証機構が統一されており、ログインはすべて同じドメインのページにリダイレクトされる。

4.3 Google Play ランキング上位アプリ調査

Google Play の全体上位アプリに実際に“パスワードを忘れた”としてアクションを起こし、その後の対応を確認する。考えられる反応としては元のパスワード開示があるされるものと元のパスワード開示がされないものの 2 種類がある。本調査では元のパスワード開示があるものを捜索していく。

4.3.1 調査対象

Google Play には有料と無料を含み数多くのアプリが配布されているが、本研究では代表的なアプリを対象にパスワードの保管状況を調査することとし、Google Play の人気全体ランキング「無料 TopAndroid アプリ」[*2]を参照し、1 位から 28 位までのアプリを対象とした。ユーザが使用する頻度が高く、注目度が比較的高いアプリがパスワードを平文もしくは可逆な形で保管しているということは、セキュリティ面での脅威の社会的影響度が高いと考えられる。

4.3.2 調査方法と環境

どのようなアプリがパスワードを平文もしくは可逆な形で保管しているのか共通点や類似点を捜索するために、指標となる項目を挙げる。調査対象のリストアップとして Google Play の人気全体ランキングの無料 TopAndroid アプリを上位からインストールし、ユーザ登録が存在するか確認する。存在する場合 ID 連携可能か、可能ならばその種類も確認し、リストアップする。Google Play のランキングは時間を空けると順位が変動する可能性があるため、リストアップは 1 日で実施する。アプリのインストールには調査用 Android 端末を使用する。

[*2] https://play.google.com/store/apps/top?hl=ja

リストアップ後 1 位から 1 つずつ調査を行う。以下に調査方法を記載する。

- インストールしたアプリに、実際にユーザ登録を行う
- 登録画面や登録の際に受信したメールはスクリーンショットを保存する
- ユーザ登録終了後同一アプリのデータを消去し、ユーザ登録前の状態に戻す。その後“パスワードを忘れた”とアクションを取り、それに対しアプリ側から元のパスワードが返送されるのか、されない場合どのような手続きを踏むのかなどそのリアクションにどのようなパターンがあるのかをスクリーンショットやメモを用いて記録する
  - 登録方法やパスワードの再設定方法などにそのアプリ特有の特徴がある場合、それもスクリーンショットやメモを用いて記録する。

4.3.3 調査結果

調査は 28 位までのアプリを対象に行った。それぞれのアプリの情報は、倫理的な観点から詳細な情報を提示することは避ける。

登録作業を行う際に各アプリの登録画面を遷移するごとにスクリーンショットを用いて保存した。11 位以降は元のパスワード開示があるもののみスクリーンショットを取る方針とした。

Google Play の人気全体ランキング「無料 TopAndroid アプリ」1 位から 28 位までのリストアップと調査の結果、元のパスワード開示があるものは発見できなかった。内訳として、全 28 件中登録がないアプリが 6 件、登録不可能であったアプリが 5 件あった。登録完了したアプリは 16 件あり、そのうち端末の Google アカウントに自動連携でログインされたアプリが 3 件、登録アカウントが Google に依存するなど重複していたアプリを除くと 12 件となった。重複していたものは、Google アカウント、d アカウントだった。

4.4 Web 検索または SNS 検索によりパスワード保管が適切でないと情報が得られたサービスに対する調査

Alexa が提供する「日本 Top ドメイン」の上位 103 位までと Google Play の人気全体ランキング「無料 TopAndroid アプリ」の上位 28 位までの調査では平文または可逆な形でパスワードを保存しているサービスは見受けられなかった。そのため追加調査として、代表的なサイトやアプリだけではなく、Web や SNS でパスワードを可逆な形で保存していると報告があるサービスに対して調査を行った。

4.4.1 調査対象

本調査では平文または可逆な形でパスワードを保存しているサービスを発見するために、Web 検索や SNS 検索を行いそのサービスが元のパスワードが返送されると情報を得られたサービスに対して調査を行う。

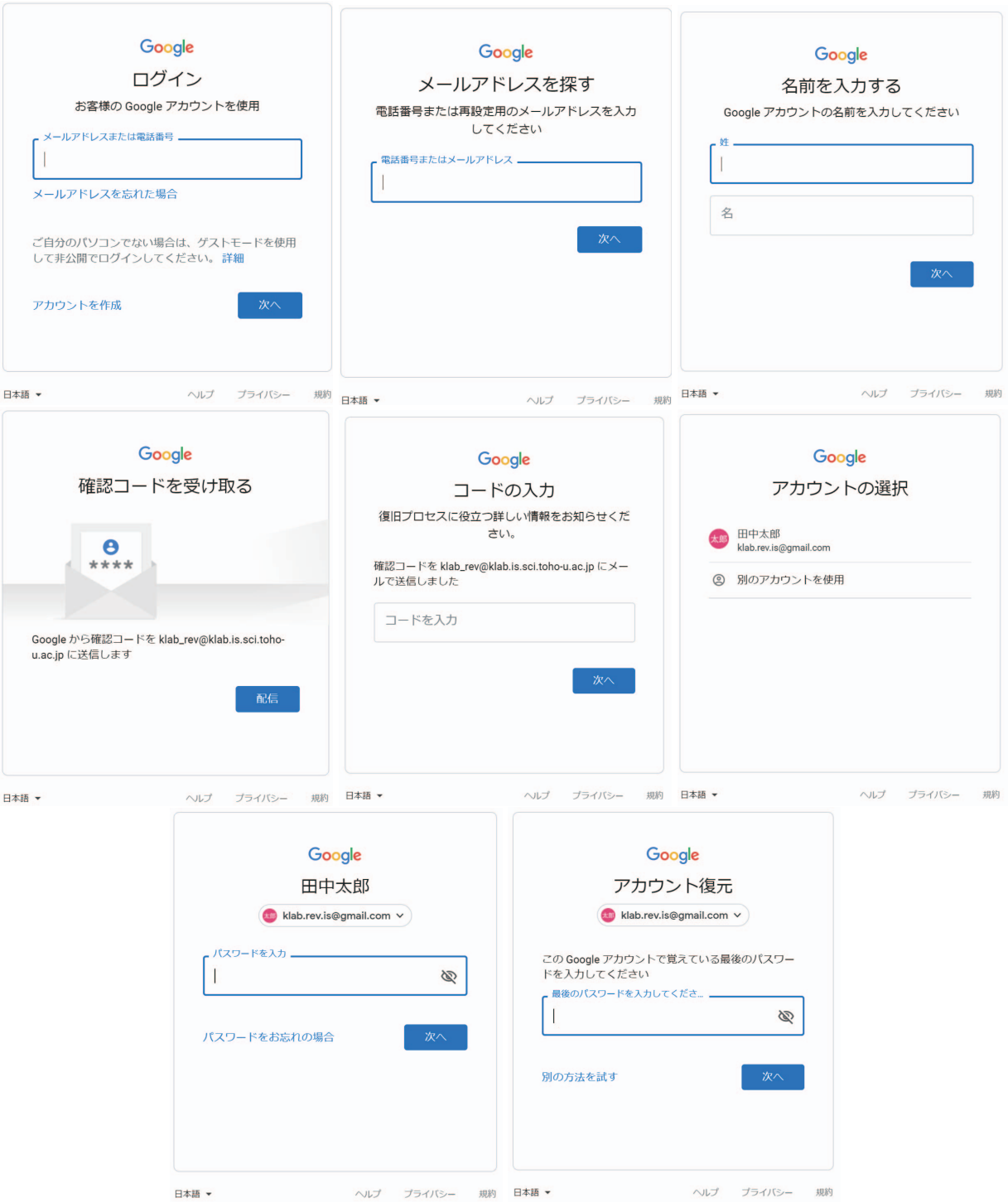

図 1　Google (Alexa 1,2,5,31 位) の登録画面と“パスワードを忘れた”としたときの対応画面

4.4.2　調査方法と環境

本調査は元のパスワードが返送されると情報を得られたサービスに対して調査を行うため、調査方法と環境は 4.2 で調査した Alexa トップサイトに対する方法や環境と同様に行う。

4.4.3　調査結果

調査対象のリストアップは Web 検索結果と Twitter での検索結果をもとに行った。検索は以下のフリーワードで行い、その後さらにリストアップ対象を精査した。

- 「パスワード　平文で」
- 「パスワード　メールに」

4.4.4　調査結果

リストアップ後実際に調査した件数は 40 件となった。そして調査の結果、元のパスワード開示があるサービスを合計 7 件発見した。また、元のパスワード開示は無かったが、“パスワードを忘れた”とアクションを起こした後、新パスワードまたは仮パスワードをメールに送信したサービスが 3 件存在することを確認した。

調査対象を元のパスワードが返送されると情報を得られたサービスに限定したが、調査の結果では実際に元のパスワードが返送されたサービスは多くはなかった。元のパスワードが返送されるとの情報があったサービスの中にも、情報が提供された時期には平文で保管されていたがその後改修されたケースが複数あるものと類推できる。

4.4.5 平文または可逆な形でパスワードを保存しているサービス間での共通部分の分析

4.4 の調査を通して平文または可逆な形でパスワードを保存しているサービスを発見できた。それらの情報を用いて、平文または可逆な形でパスワードを保存しているサービス間での共通部分の分析を行う。目的として特定の実装や特定の事業者によってこの状況が牽引されている可能性を知るということが挙げられる。

4.4.6 分析方法

平文または可逆な形でパスワードを保存しているサービス間に外観とサーバから提供される HTML データにおいて類似点があるか分析する方法を取る。これまでの調査で、平文または可逆な形でパスワードを保存しているサービスを複数発見しそのサービス特有の特徴を記録した。それらの特徴を外観とサーバから提供される HTML データの 2 つの観点から照らし合わせ、共通部分を捜索する。

4.4.7 分析結果

分析の結果、2 つのサービス間に外観において同様の形式が見られた。それぞれのサービスの情報は、倫理的な観点から詳細な情報を提示することは避ける。

その後、2 つのサービス（サービス A とサービス B とする）のサーバから提供される HTML データを照らし合わせた。サービス A の HTML には「action=”index.aspx”」、サービス B の HTML には「action=”/7cn-webapp/mobile/WMShinkiTorokuNyuryoku.do?&timestamp=20201201170229”」との記述があった。ユーザから入力されたデータを送信する場所に関係する記述だが、サービス A は.aspx となっていサービス B は.do と、サービスを構成するアーキテクチャが異なっており共通点は見られなかった。その他のサービスも 2 つの観点から照らし合わせたが、原因だと考えられるような共通点を発見することはできなかった。

5. 今後の課題

本研究では有名サイトやアプリのパスワード管理状況を調査し、平文または可逆な形でパスワードを保管しているサービス間の共通点を捜索し、原因分析を行った。本研究では外部観測によるアプローチを採用したが、外部観測に基づく実験では得られる情報に限度があるため、内部観測やそれに類する手法を用いることで、調査の精度や効率を上げることができると考える。また、比較対象のサービスを増やし、平文または可逆な形でパスワードを保管しているサービスの共通部分の分析を行う必要がある。そして、その分析結果から平文または可逆な形でパスワードを保管しているサービスの根本的な原因を特定することも今後の課題の 1 つである。

6. まとめ

Web サービスやアプリにおいてユーザから入力されたパスワードは重要な機密情報であるため外部からの不正侵入などに備えて解読が困難な状態で保管していることが理想的とされているが、Web サービスやアプリにおいて個人情報が流出してしまう事件が存在する。一部の理由として、パスワードを平文または可逆な形で保管していることに起因する。

本研究はどのようなサービスやアプリが平文または可逆な形でパスワードをサーバ側に保管しているのかどうかの実態を明らかにすることを目的とした。そのためのアプローチとして代表的な Web サービスやアプリから調査を行った。Alexa の「日本 Top ドメイン」1 位から 103 位までの Web サービスと Google Play の人気全体ランキング「無料 TopAndroid アプリ」1 位から 28 位までを調査した結果、平文または可逆な形でパスワードを保管していると断定できる Web サービスまたはアプリは発見できなかった。そこで、平文または可逆な形でパスワードを保管しているとの情報を得られたサービスに対して別途調査を行った。40 件の対象を調査したところ、7 件平文または可逆な形でパスワードを保管しているサービスを発見した。これらの調査をふまえ平文または可逆な形でパスワードを保管しているサービス間特有の共通点について Web サービスやアプリの外観とサーバから提供される HTML データの 2 つの観点から分析を行ったところ、外観において同様の形式が見られるサービスを発見した。それらの HTML データの 2 つの観点から照らし合わせたところ共通点は見つからず、原因だと考えられるような共通点を発見するには至らなかった。今後の課題としては、比較対象のサービスを増やし、平文または可逆な形でパスワードを保管しているサービスの共通部分の分析、可能であれば内部観測やそれに類する手法を用いて調査の精度や効率を上げることが挙げられる。そして、その結果から平文または可逆な形でパスワードを保管しているサービスの根本的な原因を特定することなどがある。

Alexa の上位サイトや Google Play の上位ランクアプリなどに平文または可逆な形でパスワードを保管しているサービスは見つからなかったことは、リスクが喫緊のことでないことを示す。しかし、これまで報告されたサービスでは依然パスワードを平文または可逆な形でパスワードを保管している実態が明らかになり、それらのサービスには利用者数が多いサービスもあった。リスク自体は引き続き存在することが示されるなど、本研究によりそのリスクの実態が明らかになった。

参考文献

[1] Wash, Rick, et al. "Understanding password choices: How frequently entered passwords are re-used across websites." Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). 2016.

[2] 宅ふぁいる便の衝撃的漏えい、しかしパスワードの平文保存は「超レアといえない現実」. https://www.sbbit.jp/article/cont1/36041, (参照 2019-10-08).

[3] Keeping password secure — facebook. https://about.fb.com/news/2019/03/keeping-passwords-secure/, (参照 2019-10-08).

[4] Notifying administrators about unhashed password storage. https://cloud.google.com/blog/products/g-suite/notifying-administrators-about-unhashed-password-storage, (参照 2019-10-08).

[5] インターネットサービス提供事業者に対する「認証方法」に関するアンケート調査結果. https://www.antiphishing.jp/news/pdf/wg_auth_report01_20190701.pdf, (参照 2019-07-01).

[6] Naiakshina, Alena, et al. "Why do developers get password storage wrong? A qualitative usability study." Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017.

[7] Naiakshina, Alena, et al. "Deception task design in developer password studies: Exploring a student sample." Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). 2018.

[8] Naiakshina, Alena, et al. "" If you want, I can store the encrypted password" A Password-Storage Field Study with Freelance Developers." Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. 2019.

[9] Naiakshina, Alena, et al. "On Conducting Security Developer Studies with CS Students: Examining a Password-Storage Study with CS Students, Freelancers, and Company Developers." Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 2020.