Computer Security Symposium 2018
22 - 25 October 2018

プッシュ通知を用いたパスワードマネージャの提案と評価

加藤 公樹[†1]　柿崎 淑郎[†1]　猪俣 敦夫[†1]　佐々木 良一[†1]

概要：現在，オンラインショッピングやインターネットバンキング，ソーシャルネットワークサービスなどの幅広いWebサービスが普及しているが，こうしたWebサービスでは，ID・パスワードによるユーザ認証が多く利用されている．しかし，ID・パスワード認証はユーザが脆弱なパスワードを設定してしまう，同一のパスワードを多数のWebサービスで使いまわしてしまうといった管理上の不備から，不正アクセスの被害に遭う可能性が指摘されている．そうした状況にありながら，依然多くのユーザが不備のあるパスワード管理を続けている．そこで本稿では，そうしたユーザのパスワード管理の安全性を高めるため，パスワードマネージャにスマートフォンによる認証を加え，パスワードの暗記を不要にすることで，従来のパスワードマネージャよりもユーザビリティを高めた，ユーザに負担をかけないパスワードマネージャを提案するとともに評価を行う．

キーワード：パスワードマネージャ，パスワード，プッシュ通知，認証，スマートフォン

Proposal and Evaluation of Password Manager Using Push Notification

Koju Kato[†1]　Yoshio Kakizaki[†1]　Atsuo Inomata[†1]　Ryoichi Sasaki[†1]

Abstract: At the present time, we are required to perform ID/Password-authentication in a wide range of web services such as Internet shopping, Internet banking, social network services. Nevertheless, ID/Password-authentication can cause unauthorized access due to administrative inefficiencies, such as users setting weak passwords or using the same password with many web services. Despite the danger of unauthorized access, many users continue incomplete passwords management. Password manager can prevent these vulnerable management. In this paper, we propose and evaluate a method to increase usability of password manager by abolishing ID/Password-authentication using push notification in order to increase password manager users.

Keywords: Password Manager, Password, Push Notification, Authentication, Smart Phone

1. はじめに

現在では，オンラインショッピングやインターネットバンキング，ソーシャルネットワークサービスといった様々なWebサービスのユーザ認証にはID・パスワード認証が用いられているが，この認証方式は多くのユーザがID・パスワードを安全に管理していない問題が指摘されている．例えば，ユーザは自身が覚えやすいパスワードを設定してしまう傾向から，脆弱なパスワードを設定してしまうといった問題や，ユーザが特定のパスワード文字列を暗記するために，複数のWebサービスで同一のパスワードを使いまわしてしまうといった問題が挙げられる[1, 2]．脆弱なパスワードを設定してしまう問題を防止するアプローチとして，パスワード構成ポリシを適用し，一定の条件を満たさないパスワードをWebサービスが設定できないようにするといった対策や，入力されたパスワードの強度をユーザに通知するパスワードメータを設けるといった対策がある[3]．しかし，これらの対策はユーザがパスワードを使いまわしてしまう問題に対しては効果が得られない．

この問題の対策としては，ID・パスワード認証に加えて二段階認証を導入することや，認証方法そのものを生体認証やセキュリティトークンなどのID・パスワード認証以外の強力な認証方法に変更することが考えられるが，こうした手法も配備のしやすさ（Deployability）の問題から完全に移行するまでには至っていない[4]．ID・パスワード認証の問題をユーザ自身が解決する対策として，パスワードマネージャの利用が考えられるが，現状でパスワードマネージャはあまり一般のエンドユーザには利用されていない[5]．これはユーザがパスワードマネージャに対して時間的制約やユーザビリティなどに不安を持っているためである[6]．

本研究は，従来のパスワードマネージャのユーザビリティを向上することで，ユーザに負担を感じさせないID・パスワードの管理方法を提案する．パスワードマネージャの認証にユーザの所持するスマートフォンを利用することで，ユーザにマスターパスワードを憶えさせる必要が無い，操作が簡単なモデルを構築する．パスワードマネージャのユーザビリティを改善することで，パスワードマネージャの普及率を向上させ，脆弱なパスワード設定やID・パスワードの使いまわしといったユーザによる危険な管理を防止する．

†1 東京電機大学情報セキュリティ研究室
Information Security Lab., Tokyo Denki University

2. パスワードマネージャ

2.1 概要

パスワードマネージャは，複数の ID やパスワードといった認証情報を，一括にまとめて管理するソフトウェアである．ユーザが覚えきれない，管理しきれない ID やパスワードをソフトウェアで記録し，いつでも参照できるようにすることで，ユーザの記憶負担を軽減することがパスワードマネージャの目的である．商用サービスとしては，LastPass[7]や 1Password[8]などが挙げられる．

パスワードマネージャは，Web サービスで登録した ID・パスワードなどの認証情報をマスターパスワードで暗号化し，クラウド上に記録する．認証情報を参照する際に，ユーザはマスターID とマスターパスワードを用いて認証する．このため，ユーザは Web サービスで認証をする際に ID・パスワードを憶えておく必要が無く，Web サービス毎に異なる強力なパスワードを設定することが容易になる．したがって脆弱なパスワードを設定してしまう問題や，複数の Web サービスで同一の ID・パスワードを使いまわしてしまう問題に対してパスワードマネージャは有効な対策である．

一方で，パスワードマネージャに登録する ID・パスワードなどの情報は，マスターパスワードで安全性を保っているため，マスターパスワードを安易なものや他所で使いまわしているものを設定してしまえば，登録済みのすべての情報が危険にさらされてしまう可能性がある．

2.2 一般ユーザのパスワードマネージャに対する評価

近年では，Web サービスの多様化により，ユーザ一人で複数の Web サービスアカウントを作る必要があり，人によっては個人で何十もの ID・パスワードを管理しなければならない場合もある．しかし，そうした状況であってもパスワードマネージャを利用する人は非常に少ない．2017 年に行われたトレンドマイクロのパスワードの利用実態調査[5]によれば，パスワードを管理する方法としてパスワードマネージャを使用している人の割合は，全体の 5%程度だという．

Aurigemma ら[6]の研究によれば，ユーザがパスワードマネージャを利用しない最も主要な理由は,「時間が十分になかった」「惰性で入れていない」「忘れてしまっていた」などの個人的な問題である．また，これらの回答をしたユーザの多くがパスワードマネージャの導入に前向きであるということが判った．つまり，一般ユーザにおいてもパスワード管理の危険性とパスワードマネージャの有用性は理解しているが，実際に利用するには手間や時間が妨げになっていると言える．そのため，パスワードマネージャを一般ユーザに利用してもらうためには，従来のパスワードマネージャよりもユーザビリティを高めた仕組みが必要になる．

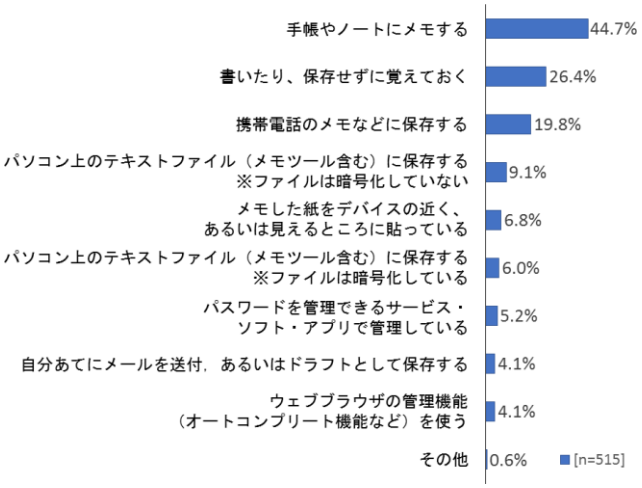

図 1　ユーザのパスワード管理方法

2.3 関連研究

パスワードマネージャのユーザビリティ改善の研究として，McCarney [9]らの研究では，ユーザの持つスマートフォンをトークンにすることで安全性を保つパスワードマネージャ Tapas を提案している．

Tapas は，パスワードマネージャに登録された Web サービスの ID・パスワードなどの認証情報はユーザが持つスマートフォンに保存し，パスワードマネージャを動作させる PC には認証情報を暗号化・復号する共通鍵を保存する．ユーザが PC を用いてパスワードマネージャに登録された Web サービスにログインする際には，ユーザはスマートフォンに保存された認証情報のリストからその Web サービスの情報を選択することで，暗号化された認証情報がスマートフォンから PC へ送信され，PC はあらかじめ所持している共通鍵を用いて受け取った情報を復号し，Web サービスのログインフォームに自動入力する．

Tapas は Web サービスの ID・パスワード参照時に，必ずスマートフォンが必要となる反面，従来のパスワードマネージャに必要だったマスターパスワードを必要としない．そのため，Tapas ではユーザの記憶負担が不要となっている．また，Tapas はスマートフォンに ID・パスワードなどの認証情報を保存していることから，スマートフォンを紛失したときに全ての情報を復号できなくなる問題がある．

そこで福光[1]らの研究では，Tapas の環境にパーソナルサーバを追加し，(2, 3)-しきい値秘密分散方式により ID・パスワードなどの認証情報を秘密分散で PC, スマートフォン，パーソナルサーバの 3 つに保存することで，PC，スマートフォンどちらからでも認証情報を復号できる仕組みを提案している．福光らの提案方式では，PC，スマートフォン，パーソナルサーバのどのデバイスが破損もしくは紛失しても，他の 2 つのデバイスが残っていればデータを復元することができる．一方で，パーソナルサーバから分散情報を参照する際にはマスターパスワードが必要になるため，

その点においてはユーザビリティを損なっている．

2.4 考察

2.3 節で述べたパスワードマネージャでは，Web サービスにログインする際に，スマートフォンからその Web サービスの ID・パスワード情報をリストから選択し，PC に送信する必要がある．しかしながら，2.2 節でも述べたように一般ユーザがパスワードマネージャを利用するためにはユーザビリティを高めた仕組みが必要となる．そのため，認証情報を参照する度に煩雑な操作を求められる仕様は好ましくない．

また，近年では Web サービスの多様化やスマートフォンによるインターネット利用者の増加により，個人のインターネット利用率は総人口の 8 割程度にまで達しており，ユーザの IT リテラシの習熟度には差があるものと考えられる[10]．そのため，マスターパスワードをユーザに設定・管理させる方式は，IT リテラシがそれほど高くないユーザに安易なマスターパスワード設定をさせてしまう危険性が高い．

したがって，一般ユーザに提案するべきパスワードマネージャは，操作の工程が少なく，マスターパスワードが不要なものにするべきであると考えられる．

3. 提案手法

本研究では，ユーザが持つスマートフォン本体の認証機能とプッシュ通知機能を組み合わせることによって，マスターパスワードを用いることのないパスワードマネージャを提案する．このパスワードマネージャは，従来必要であったマスターパスワード認証の代わりに，ユーザが持つスマートフォン本体の認証機能（例えば指紋認証，PIN コードなど）を用いることで，手順が煩雑な認証を扱わないことからユーザビリティを保っている．なお，スマートフォンの認証機能を設定していないユーザにとっては，スマートフォン利用時の手間が増加してしまうが，指紋認証などの生体認証を利用することでロック解除の手間は軽くすることができる．また，近年においてはスマートフォンおよびその端末が有する情報自体が非常に重要であり，機密性の高い情報であることから，スマートフォンの認証機能を利用するユーザは増加していくと期待できる．

以下に，本稿で提案するパスワードマネージャの概要を説明する．

3.1 システム構成

提案するシステムの構成要素を以下に説明する．また，システムの構成図を図 2 に示す．

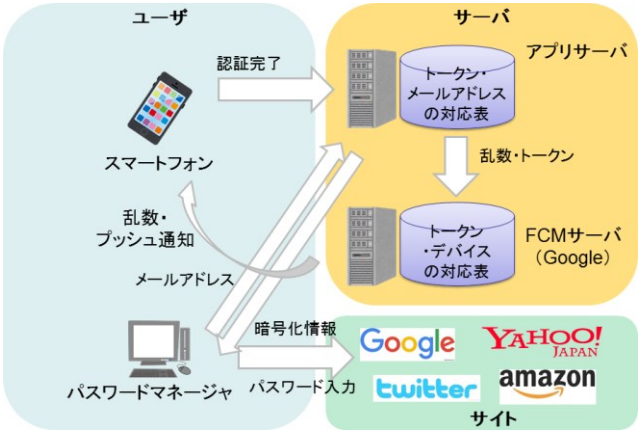

図 2　システムの構成図

- アプリサーバ
  パスワードマネージャアプリケーションの保存データやユーザ情報を登録するデータベースと通信するサーバ．
- FCM サーバ
  Google が提供するメッセージ送信用のプラットフォームサービスのサーバ．ユーザのスマホアプリにプッシュ通知を送信する役割を担う．
- ブラウザプラグイン
  ユーザの PC 上で動作するパスワードマネージャアプリケーション．ブラウザ拡張として実装する．
- スマホアプリ
  ユーザのスマートフォン上で動作するパスワードマネージャアプリケーション．また，このアプリケーションをインストールするスマートフォンは，画面ロック機能を有効にしてあるものとする．

3.2 システムの動作

提案するパスワードマネージャについての具体的な動作手順を説明する．パスワードマネージャの機能として，初期登録，認証情報登録，認証情報復号，端末復元の 4 つの機能がある．以下に各機能の手順を示す．なお，サーバとブラウザ，およびスマートフォン間の通信には TLS 通信が利用できるものとする．

(1)　初期登録

ユーザは PC のブラウザにブラウザプラグインを，スマートフォンにアプリをインストールする．ユーザはスマートフォンアプリにメールアドレスを登録する．スマートフォンアプリは入力されたメールアドレスと，アプリインストール時に発行されるプッシュ通知用のトークンをアプリサーバに送信する．尚，この際入力するメールアドレスは，スマートフォン以外の環境から受信できるものとする．アプリサーバは情報を受け取った後，認証用ページを作成し，ページの URL を受け取ったメールアドレスへ送信する．

ユーザは受け取ったメールに記載されている URL へアクセスし，アプリサーバは新規のユーザとしてメールアドレスとトークンをデータベースへ登録する．

また，ブラウザでは ID・パスワードなどの認証情報を暗号化するための共通鍵を生成する．この共通鍵をブラウザは QR コードを用いてスマートフォンアプリに送信する．ブラウザとスマートフォンは，共通鍵を端末に保存する．

(2)　認証情報登録

認証情報登録機能は，ブラウザもしくはスマートフォンアプリ上でパスワードマネージャに Web サービスの ID・パスワードなどの認証情報を登録する際に使用する機能である．

まず，ユーザはブラウザもしくスマートフォンアプリ上でパスワードマネージャのユーザ認証を行う．

- ブラウザからユーザ認証を行う場合

ユーザはブラウザプラグイン上から 3.2.1 節で登録したメールアドレスを入力する．ブラウザは入力されたメールアドレスを端末に保存する（2 回目以降のユーザ認証ではメールアドレスの入力は不要になる）．ブラウザは入力されたメールアドレスをアプリサーバに送信し，アプリサーバは登録されているユーザのリストから受け取ったメールアドレスと同一のメールアドレスを持つユーザを検索する．検索からユーザが見つかった場合，アプリサーバはユーザ認証用の乱数を生成・保存してから，見つかったユーザのプッシュ通知用トークンと生成した乱数を FCM サーバに送信する．FCM サーバは受け取ったトークンに対応するスマートフォンに受け取った乱数を送信する．乱数を受信したスマートフォンアプリは，ユーザにパスワードマネージャを利用しようとしているかどうかの確認をプッシュ通知で表示する．ユーザが表示された画面上から承認をすると，スマートフォンアプリは受信した乱数をアプリサーバに送信する．ただしこの際，指紋認証や PIN コード認証などスマートフォンの認証を行わなければ，プッシュ通知の承認は出来ないものとする．アプリサーバは受け取った乱数とあらかじめ保存していた乱数が同一であるかを確認する．乱数が同一であれば，アプリサーバはブラウザプラグインとセッションを開始する．

- スマートフォンアプリからユーザ認証を行う場合

ユーザはスマートフォンで生体認証や PIN コード認証などの認証を行ってから，スマートフォンアプリを起動する．

ユーザ認証を行ったあと，パスワードマネージャは ID・パスワードなどの認証情報を端末に保存している共通鍵を使用して暗号化しアプリサーバに送信する．アプリサーバは受け取った認証情報を保存する．なお，スマートフォンアプリで操作する場合は，暗号化した認証情報を端末にも保存する．

(3)　認証情報復号

認証情報複合機能は，Web サービスにログインする際にパスワードマネージャから ID とパスワードの認証情報を取り出し，復号する機能である．

まず，ユーザは PC もしくはスマートフォン上のブラウザで，ログインしたい Web サービスにアクセスし，ログインフォームを開く．その後，ユーザは 3.2.2 節と同様の手順でブラウザもしくはスマートフォンアプリ上でパスワードマネージャのユーザ認証を行う．ユーザ認証を行ったあと，パスワードマネージャはブラウザで開かれている Web サービスの URL から登録されている認証情報を検索し，対応する ID とパスワードを自動入力する．

(4)　端末復元

端末復元機能は，パスワードマネージャを利用していた PC もしくはスマートフォンを紛失･破損などの理由で使用できなくなってしまった場合に利用する機能である．

まず，PC を利用できなくなった場合，ユーザは代わりの PC のブラウザにブラウザプラグインをインストールする．その後，3.2.1 節と同様に共通鍵を生成し，スマートフォンアプリと共有する．その後，スマートフォンアプリは端末に保存している認証情報を保存している共通鍵で復号し，新しく受け取った共通鍵で暗号化する．

スマートフォンが利用できなくなった場合，ユーザはブラウザプラグインからスマートフォン紛失の手続きを行う．この際，ユーザはパスワードマネージャに登録しているメールアドレスをブラウザプラグインに入力する．メールアドレスを受け取ったサーバは，登録されているユーザから当該のメールアドレスを持つアカウントを検索し，該当するアカウントがあれば，そのメールアドレスに対してスマートフォンの再登録手続きをするかどうかの確認を行うページの URL を記載したメールを送信する．ユーザが記載された URL にアクセスすれば，アプリサーバはユーザのメールアドレスに対してアカウントの引継ぎコードを送信する．ユーザは新しいスマートフォンにスマートフォンアプリをインストールし，スマートフォンアプリ上の引継ぎ画面において引継ぎコードを入力する．スマートフォンアプリはプッシュ通知用のトークンをサーバに送信し，サーバは新しいスマートフォンに引継ぎ情報を入力したかどうかを確認するページの URL を記載したメールをユーザのメールアドレスへ送信する．ユーザが記載された URL へアクセスすると，アプリサーバは送られたトークンをアカウントに再登録する．

表 1　UDS フレームワークによる評価

	U1	U2	U3	U4	U5	U6	U7	U8	D1	D2	D3	D4	D5	D6	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11
提案方式	○	○	△	○	○	○	○	△	○	△	○			○	○	○	○	○				△	△	○	○
パスワード認証					○	○	△	○	○	○	○	○	○	○		△						○	○	○	○
福光らの研究	○	○	○	△	○	○	○	△	○	△	○			○	○	○	△				○	○	△	○	○
LastPass	△	○	△	△	○	○	○	△	○	△	○		○		△	△					○	○	○	○	○

○：項目を満たしている　△：条件付きで項目を満たしている　空欄：項目を満たしていない

U1	記憶不要性	D1	身体障害による制限	S1	物理監視への耐性	S9	第三者が必要ない
U2	多数登録による負荷	D2	1 人当たりのコスト	S2	標的型攻撃の耐性	S10	不正に開始できない
U3	持ち運ぶものが無い	D3	サーバとの互換性	S3	総当たりへの耐性	S11	リンク不可
U4	物理的労力が不要	D4	プラグイン不要	S4	辞書攻撃への耐性		
U5	覚えやすい	D5	実績	S5	マルウェア耐性		
U6	短時間で使える	D6	特許による保護	S6	バックエンド攻撃		
U7	頻度の低いエラー			S7	フィッシング耐性		
U8	簡単な復元			S8	デバイス盗難耐性		

4. 評価

本章では，本稿で提案するパスワードマネージャを UDS フレームワーク[4]を用いて評価する. UDS フレームワークは，ユーザビリティ（Usability），配備のしやすさ（Deployability），安全性（Security）の 3 つの評価軸に含まれる 25 個の評価項目から，認証プロトコルの性能を比較評価できるフレームワークである.

提案したパスワードマネージャと，パスワード認証，福光らの研究[1], LastPass[7]のそれぞれを UDS フレームワークによって評価した結果を表 1 にまとめる．表 1 の○は対応する項目を満たしていることを表し，△は条件付きで満たしていることを表している．なお，本稿で提案するパスワードマネージャ以外の評価結果は，従来の研究の評価結果に基づくものである[1, 4, 9].

提案するパスワードマネージャは，ユーザビリティの面で従来のパスワードマネージャより利点がある．これは提案するパスワードマネージャはマスターパスワードが不要で，かつ必要な操作が少ないことが要因である.

特に提案方式に利点があるのは，U4 の「物理的労力が不要」の項目である．この項目は，ボタンを押す以上の労力がない事を評価する項目である，提案方式では初期登録と端末復元以外では基本的にボタンを押すのみでユーザ認証や認証情報の参照が可能であるため，この項目に利点があるものと考えられる.

ただし，U3 の「持ち運ぶものが無い」の項目に関しては福光らの研究が優れているが，これはスマートフォンを利用しなくても，マスターパスワードを用いることによって ID・パスワードを復元できるためである．本稿で提案するパスワードマネージャでは，ユーザが危険なパスワードを設定してしまうことを防止するため，この要素は除外している.

また，セキュリティの面でも一部に従来のパスワードマネージャよりも利点がある．これは提案するパスワードマネージャがマスターパスワードを利用せず，ユーザ認証時にユーザのスマートフォンにプッシュ通知が行くことから不正なユーザからのアクセスを即座に制限することができる事が要因である.

S3，S4 の項目は，パスワード推測攻撃（脆弱なパスワードおよび辞書攻撃，レインボーテーブルなど関連する辞書攻撃）の成功確率がユーザによって制限され得ることを述べている．提案する方式はマスターパスワードを使用しないが，第三者がユーザのメールアドレスを推測してアクセスを試みることは可能である．しかしながら，その工程においてプッシュ通知がユーザのスマートフォンに届くため，ユーザは第三者のアクセスを拒否することができる. また，以後その接続元からのアクセスを制限することが可能であるため，推測攻撃を抑制することができる.

ただし，セキュリティの面では欠点もある．S8 の項目は物理的な認証要素が盗まれた場合に安全性がそこなわれないかどうかという項目である．提案方式では，ユーザのスマートフォンをユーザ認証に使用するが，スマートフォンは使用時に指紋認証や PIN コード認証が必要になるため，この項目は条件付き達成となる．また，S9 の項目は認証システムが信頼できる第三者を必要としないことの項目であるが，提案システムはアプリサーバ及び FCM サーバを利用するため，この項目はセキュリティが低下する.

5. まとめ

本稿では，ユーザのスマートフォンとその端末へのプッシュ通知を組み合わせることで，ユーザのユーザビリティを追求したパスワードマネージャを提案・評価した．本提案方式は，マスターパスワードの代わりに，ユーザが持つスマートフォンの指紋認証や PIN コードなどの認証機能を用いることで，ユーザビリティを高めた方式である．従来のパスワードマネージャでは，リテラシがそれほど高くないユーザはマスターパスワードにも弱いパスワードを選びがちであったが，提案方式ではマスターパスワードを利用しないことにより，総当たり攻撃に対しても利点があることが分かった．

また, 近年ではパスワード認証に代わる認証方式として，FIDO が注目されてきている．しかしながら，FIDO に対応したデバイスが一般ユーザに普及するにはまだ時間を要すると言われており，また Deployability の観点からも全ての Web サービスがパスワード認証を廃止するとは考えにくい．そのため，本方式は今後も有用性がある仕組みであると考える．

参考文献

[1] M. Fukumitsu, S. Hasegawa, J. Iwazaki, M. Sakai, and D. Takahashi, “A proposal of a password manager satisfying security and usability by using the secret sharing and personal server,” in Proc. Advanced Information Networking and Applications (AINA), 2016 IEEE 30th International Conference on, Mar. 2016, pp. 661-668.

[2] R. Wash, E. Rader, R. Berman, and Z. Wellmer, “Understanding password choices: how frequently entered passwords are re-used across websites,” in Proc. Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, June 22–24, USENIX, pp. 174-188.

[3] 菅井琢 and 金岡晃, “実利用されているパスワード強度メーターの分析と検証,” 情報処理学会研究報告, 2016-DPS-168, vol.2016, no. 16, pp. 1-6, Nov. 2016.

[4] J. Bonneau, C. Herley, PC. Van. Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in Proc. Security and Privacy (SP), 2012 IEEE Symposium on, May 2012, pp. 553-567.

[5] トレンドマイクロ：パスワードの利用実態調査 2017，トレンドマイクロ株式会社(オンライン)，入手先 < https://www.trendmicro.com/ja_jp/about/press-release/2017/pr-20171005-01.html> (参照 2018-08-17).

[6] S. Aurigemma, T. Mattson, and L. Leonard, “So much promise, so little use: what is stopping home end-users from using password manager applications?,” Proc. HICSS-50. I&DE. Innovative Behavioral IS Security and Privacy Re-search Minitrack, Jan. 2017.

[7] LogMeIn Inc., “LastPass [Online],” LogMeIn Inc., https://www.lastpass.com/ja, [Accessed July 17, 2018].

[8] AgileBits Inc., “1Password [Online],” AgileBits Inc., https://1password.com/jp/, [Accessed July 17, 2018].

[9] D. McCarney, D. Barrera, J. Clark, S. Chiasson, and, P. C. van Oorschot, “Tapas: design, implementation, and usability evaluation of a password manager,” Proc. ACSAC '12., pp.89-98, Dec. 2012.

[10] 総務省：基本データと政策動向，総務省(オンライン)，入手先 <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd252120.html>(参照 2018-08-18)