二要素認証の利便性向上に向けた一考察：物理デバイスの所持を不要にする二要素認証の提案

高田 哲司[1,a)]

概要：本研究では物理デバイスを所持する必要のない二要素認証（2FA）として，正規ユーザ本人しか知らない URL を 2nd factor とする個人認証手法を提案する．パスワード認証の危殆化にともないその安全性強化法として 2FA が提供されているが，その利用率は依然として低いままである．その原因は，2FA の利用によりコスト負担や利用上の懸念があるからだと考える．そこで本研究ではその原因の 1 つと考える「物理デバイスの所持」という要件を不要にする 2FA 手法について検討し，個人認証を行う Web ページの URL を 2nd factor として秘密情報化する手法を提案する．考察の結果，提案手法の操作方法は既存のパスワード認証とほとんど同じでありつつも，パスワードリスト攻撃やフィッシング攻撃への対策になることについて議論した．多様な Web サービスが存在する中で，既存の 2FA の適用がコスト面で困難なサービスや 2FA の利用要件を満たすことが困難なユーザに対し，パスワード認証よりも安全な新たな個人認証の選択肢を提供しうる手法であると考える．

キーワード：個人認証，二要素認証，ユーザビリティ，所有物，Private URL

A Proposal of Usable Two-factor Authentication by Eliminating a Use of Physical Device

Tetsuji Takada[1,a)]

Abstract: We propose a two-factor authentication (2FA) that does not require the possession of a physical device. 2FA is provided as an option for a user authentication in major web services. However, its adoption rate remains low. This is due to the cost burden and concerns about the use of 2FA. To remedy the issues, we propose an alternative 2FA scheme that assigns a user authentication page to each user, and the URL is considered one of confidential information. Through the discussion, the following two advantages are clarified. (1) The operation of the proposed method is almost the same as the conventional password authentication. (2) The proposed method can improve the security against credential stuffing attack and phishing attack. We believe that the proposed method can provide a new option for users who cannot use existing 2FA schemes and for service operators who are hesitant to provide them.

Keywords: User authentication, Two-factor authentication, Usability, Physical device, Private URL

1. はじめに

Web サービスにとってパスワード認証は現在も必要な仕組みであると考える．その理由は Web サービスの多様性にある．サービス内容についてみてみると，2020 年から始まった Covid-19 感染爆発に対するワクチン接種予約でも Web サービスが運用されるなど公共性の高いサービスもある一方で，学生が講義で得た知識をもとに自分のアイデアを Web サービスとして実装し Internet 上で公開するなど，そのサービス内容は多岐にわたる．また利用ユーザについても同様である．とある国のすべての国民が想定ユーザとなる Web サービスもあれば，大学の事務システムなど，一

[1] 電気通信大学
The University of Electro-Communications
[a)] zetaka@computer.org

部の限定されたユーザしか利用しないサービスもある．この Web サービスにおける個人認証手法として，パスワード認証には以下のような利点がある：(1) ユーザにとって必要な環境は，Web ブラウザと Internet アクセス環境のみ，(2) すぐにサービスを利用開始可能，(3) 利用方法が広く理解されている，(4) 実装・設置が容易．これらの利点は，Web サービスにとって望ましいものである．特に，機材や運営コストはかけられないが運用はしたい Web サービスとか，想定ユーザが多様であり利用環境に機材を所有している制約を置くことが困難なサービスなどでは有用である．

しかし，パスワード認証は以下にあげる攻撃手法により安全性の担保が困難になってきており，実際にも不正アクセスが発生して大きな問題となっている．

- パスワードリスト攻撃
  複数のサービスで同じアカウント情報 (User ID/Password) を使用することを「Password の使い回し」という．この状況において利用サービスの 1 つからアカウント情報が漏洩し，それを攻撃者が入手する．この入手したアカウント情報を利用して攻撃者がほかのサービスへ不正アクセスを試みる攻撃のことを指す．
- 推測攻撃
  人間は安全な Password を作成し，それを記憶保持するのが得意とは言いがたい．よって安全性と記憶保持可能性を天秤にかけた結果，記憶可能性を優先し安全性は低いが記憶保持可能な Password を設定する．しかしそれは攻撃者を含む第三者にとっても推測が容易な Password であり，Password の全件探索を行わなくてもなりすましに成功する可能性が高いという攻撃
- Phishing 詐欺
  本物の Web ページとそっくりの偽ページを作成し，ユーザをその偽ページに誘導して当該サービスのアカウント情報を窃取する攻撃

これらの脅威に対する対策として 2 要素認証 (Two-factor authentication: 2FA) または 2 段階検証 (Two-step verification: 2SV) が主要な Web サービスを中心に提供されている．リモートワークの普及にともない，パスワード認証だけでは安全性が担保できないという観点から業務系サービスを中心にその利用が拡大しているものと推測する [10].

しかし，2FA/2SV による個人認証では以下のようなコストがユーザまたはサービス提供側に発生する．

- 操作コスト: 2 つの機密情報を検証する必要があるため 1 つの時と比較して操作負担は増える
- 機材コスト: 2FA 利用のため，スマートフォン等の携帯端末や専用 Hardware を導入する必要がある
- 運用コスト: 携帯端末であれば通信費や電気代がかかる，専用 Hardware であれば機器交換が必要な場合もある
- サポートコスト: 2FA/2SV に不慣れであったり，設定・操作が容易ではないため，ユーザサポートが必要となる．またなんらかの不具合・障害が発生した際には復旧のための支援も必要となる

そこで本研究では不特定多数のユーザが利用する Web サービスの個人認証を対象とし，物理的なデバイス (携帯端末，USB stick, Code 生成器等) を持たなくても現状の 2FA/2SV と同等程度の安全性を担保しうる個人認証手法を実現する方法について検討を行なった．

その検討の成果として，本論文ではユーザ本人しか知らない URL (以降 *Private URL* と呼ぶ) を個人認証に応用する手法を考案した．この手法の最大の変更点は，サービス利用者は自分専用の個人認証ページでしか個人認証を行えないようにすることであり，これにともないサービス利用者が共通して利用する個人認証ページを不要にする，という点にある．またこの手法に関する安全性と利便性，ならびに Private URL の管理とリスクについて考察を行なった．

以降，本論文では 2 章で既存の 2FA/2SV 手法の問題点について整理し，3 章で先行研究と関連情報について述べる．4 章で提案手法について紹介し，5 章でその安全性と利便性について考察する．

2. 既存の 2FA/2SV 手法の問題点

既存の多くの 2FA/2SV 手法は，物理的な「もの」をユーザが所持していることを前提としている．スマートフォン等の通信可能な携帯端末や専用のコード生成器，USB stick や紙に記載された code 表などが代表例である．これらの機器・情報は正規ユーザのみが所有していて，個人認証を行うときにはいつでも利用可能であることが 2FA/2SV 利用の前提となっている．

しかし現実には，そのような条件をすべてのユーザが満たせるわけではない．また上記のような状況が一時的に満たせなくなるような場面も発生しうる．2FA/2SV 認証のために何かしらの所有物を所持しなければいけないことに対して起こりうる問題点を以下にあげる．

- 紛失，盗難
- 故障
- 機器が利用不能
- 所持し忘れ (今，手元にはない)
- 複数人によるアカウント共有が困難
- プライバシ上の懸念
- スケーラビリティ

機器の紛失や故障は人為的原因によるもののほかに自然災害等により発生する可能性もある．機器が利用不能と

は，通信ができない状況になり 2nd code が取得できない場合や電池残量がなくなり端末自体が利用不能になることを意味している．アカウント共有も 2FA の主要な課題の 1 つであり，所有物が必要になると複数人によるアカウント共有が困難になる．プライバシ上の懸念とは，2FA/2SV を行うために電話番号等をサービス側に提供しなければならなかったり，2FA 用のアプリケーションを私用の携帯端末にインストールしなければならないなどの場合を想定したものである．スケーラビリティの問題とは，利用サービス数の増加にともない所持すべき「もの」の数も増える可能性があり，管理負担が増えることをさす．

これに対し，物理的な機器・情報を持つことなく既存の 2FA/2SV と同等程度の安全性を担保しうる個人認証が実現できるならば，これらの問題点を改善できることになる．それは 2FA の利用における敷居を下げることになるととともに，2FA のユーザビリティ改善にもなると言える．またサービス側にとっても低コストでパスワード認証よりも安全な個人認証を提供することが可能になり，その利用が進めば現状よりもアカウントセキュリティの向上につながると言える．

3. 関連情報・先行研究

2FA のユーザビリティを調査した先行研究は多数ある．そのいくつを紹介する．

Reynolds らの研究 (2018)[2] では，YubiKey と呼ばれる製品を用いた 2FA のユーザビリティについて「2FA の初期設定」とその後の「日常利用」の 2 つのシーンに分けてそのユーザビリティを評価した．実験参加者は大学内で募集した参加者である．また Reynolds らの別の研究 (2020)[1] では，米国の 2 つの大学における 2FA の利用ログとサポートセンターへの対応依頼内容を大規模に調査し，2FA の利用によってかかる時間や発生するエラーとその復旧にかかる時間を調査した．両大学ともに使用されている製品は Cisco Duo[14] である．

Colnago らの研究 [5] は，2016 年から 2017 年にわたり，Carnegie Mellon Univ.(CMU) での 2FA 導入においてユーザがどのように 2FA を利用し，それに伴いどのような問題が発生し，かつ 2FA への認識がどう変化したかをシステムの利用ログとアンケートによって調査した．導入された製品は Duo[14] という製品で，利用形態としてはハードウェアトークン，携帯電話アプリ，USB stick と紙に印刷したコードのいづれかで利用可能であった．

Lang らの研究 [3] では，Google 社員および Google が提供するサービスのユーザを対象として 2FA の評価を行なっている．評価対象の 2FA は Security key とよぶ Universal 2nd factor(U2F) 規格に準拠した USB stick によるものである．また Reese らの研究 [4] では 5 種類の 2FA 手法におけるユーザビリティ評価を行なっている．

これらの研究から既存の 2FA には以下のような問題があることが明らかにされている．

- 利用を始めると「2FA の利用は簡単」と認識される傾向がある
- 2FA の利用により追加で必要となる時間はそれほど大きくない
- 初期設定・環境構築では問題が発生する傾向があり，改善が必要
- 携帯電話による 2FA がエラーを発生させやすい
- 個人認証ができなくなる場面は発生しており，サポートへの負担が発生する
- サービスの価値と Security 要件とのバランスを考えると，Security が必要と言えないサービスに 2FA を適用することに不満が発生している

これらの結果は，既存の 2FA 手法には問題があり改善が必要であることを示している．また，既存の 2FA 手法では多様な Web サービスの Security 機構として適切とは言えない可能性 “One size does not fit all” についても言及されている．

また 2FA の代替手法として Risk-based authentication(RBA) を取り上げ，2FA と RBA の安全性とユーザビリティの比較を行なっている研究もある [7]．しかし，この研究で紹介されている RBA はデバイスの利用履歴と位置情報を用いており，デバイスの所有を前提としている手法であることから，デバイスの所持という面では既存の 2FA 手法と同等と見ることができる．また一度認証を行なったデバイスでは 2FA を利用しなくても認証できる設定 “Remember me” オプションや，個人認証の利用頻度に影響する “Session time out” の設定がユーザビリティに影響することは論文 [1] でも言及されている．このことから言えることは，既存の 2FA 手法は利用頻度が増えると操作負担が大きくなるということであり，こういった仕組みがその負担軽減のために用意されているという点である．

なお 2FA の現状について言及しておく．著名なサービスにおける 2FA の利用率は以下の通りである．

- GitHub ユーザの 1%未満 (2016)[9]
- Gmail ユーザの 10%未満 (2018)[6]
- Twitter ユーザの 2.3% (2020)[8]

また世の中の動向としても 2FA/2SV の利用を推奨する動きがある．Google は 2021 年 5 月，2SV を利用可能なユーザを対象に 2SV を自動的に有効化すると発表している [11]．また Salesforce では 2022 年 2 月 1 日より多要素認証 (MFA) の利用が必須，という方針を公表している [12]．また米国では 2021 年 5 月に大統領令が発令され，その中で「政府機関のシステムやそのシステムを提供するベンダーの認証には MFA を採用すること」と定めています [13]．

このような状況下において，パスワード認証を使用している多様な Web サービスに既存の 2FA/2SV 手法を適用

(1) https://A.example.org/login?*a=Fyam9Q6Dcv*&*b=vJjD3896mc*&*c=Se795qV3wU*
(2) https://A.example.org/login?*p=3VtFLh62Mq*&*s=7Z6hW824NJ*&*v=7nkD94y8fw*
(3) https://B.example.org/*tP9a7HQ586*/*nAs8Erb*/*9u28H34kaLXtA576BVi*/login

図 1 Private URL の例
Fig. 1 Examples of Private URL

していくことは困難であるとと考える．そこで本研究では 2FA における要件の 1 つである「なんらかの物理デバイスを所持する必要がある」という制約をなくすことが可能な 2FA 手法の検討を行なった．

4. Private URL による二要素認証

これまでの考察をふまえ，物理デバイスの所持を想定しない 2FA 手法として，正規ユーザのみが知る URL(=Private URL と呼ぶ) を 2nd factor とする個人認証を提案する．本章では，Private URL をユーザに通知する方法と，その後の URL 管理方法に違いのある 3 つの手法を説明する．

4.1 手法 A: 1 つの秘密情報だけで 2FA

1 つ目の手法は，従来のパスワード認証と同様 1 つの秘密情報だけで 2FA/2SV と同等の安全性を実現しようとする手法である．認証時の手順を以下に示す．

(A1) 認証画面にアクセスする
(A2) User ID を入力する．
(A3) サービス側は Private URL を生成し，それを電子メールでユーザに通知する
(A4) ユーザは Private URL にアクセスし，そこで Password を入力する
(A5) 認証結果を受けとる

A1, A2 は誰でも実施可能だが，A3 以降は正規ユーザのみが対応可能であるという想定である．なお “Private URL” とは，以下の特徴を持つ URL と定義する:

(i) 通知された人 (=正規ユーザ) のみが知る URL
(ii) URL の path または query 部分にランダム値が含まれる
(iii) 有効期間は有限である
(iv) URL へのアクセスは必ず TLS 通信を使用する

Private URL の例を**図 1** に示す．図中 (1,2) は Query 部にランダム値を含む URL で，3 つの key-value pair が含まれている．(3) は Path 部にランダム値を含む URL である．したがって，第三者が正規ユーザに通知された Private URL を特定することは容易ではないと想定しており，仮に知り得たとしても使用不能になっている可能性もある．

本手法は，既存サービスで用いられている「ユーザ登録・パスワード復元手続き」を流用したものである．この方法ならば，従来のパスワード認証と同様に User ID と Password を入力するだけで個人認証が可能である．また 2nd factor は「正規ユーザだけがサービス側に登録された電子メールを所持している (=利用できる)」こととなる．サービス側からユーザに送られる Private URL により，サービス側がランダムに生成した値を利用しており，それを正規ユーザに送付して個人認証を行なうことで既存の 2FA/2SV における code 生成・通知による仕組みと同等であると考える．

4.2 手法 B: 電子メールを不要にする

電子メール本文に記載される Private URL へアクセスし，User ID/Password を入力する前節の方法はフィッシング攻撃の手口と同じである．また電子メールは暗号化が必ず適用される情報伝達手段ではないため，ユーザ登録やパスワードリセット等その利用頻度が低いものであれば許容される手法かもしれないが，一定の頻度で利用される個人認証のための通信手段としては懸念が残る．また個人認証のためにメールを頻繁に利用するようになると，フィッシング詐欺のメールと正規サービスからのメールの判定に混乱をきたし，フィッシングページにうっかり正規のアカウント情報を入力してしまうリスクも高くなる恐れがある．そこで前節の手法を参考にしつつ，電子メールを不要にする 2 つ目の手法を提案する．

ユーザ登録処理

以下にユーザ登録処理を示す．なお，以下の説明で出てくる “Public URL” とは，「検索エンジンで検索でき，誰でもアクセス可能な URL」のことを意味する．

(B-r1) 登録希望者が Public URL であるサービスのユーザ登録ページにアクセス，電子メールアドレスを入力
(B-r2) 入力されたメールアドレスに Private URL が送付される．その Private URL へアクセスし，その Web ページで User ID と Password を入力しユーザ登録を行う
(B-r3) ユーザ登録が完了すると，サービス側はユーザに対して Web 上で (Private URL, Passcode) の 2 情報を提示するこの Private URL は (B-r2) で受け取った URL とは別のものである．ユーザはこれらの情報を何らかの方法で保存しておく．

この登録処理は，(B-r3) をのぞいて既存のユーザ登録手法と同じである．(B-r3) で得られる 2 情報だが，Private URL は登録ユーザ専用の個人認証用ページを示す URL である．また Passcode は，Private URL のリカバリ時に使用する情報となる．これらの情報は「正規ユーザのみが知っている情報」という状態が維持されるよう管理されるものとする．

認証処理

次に認証処理を以下に示す．

(B1) 登録処理 (B-r3) で取得した Private URL にアクセスする

(B2) User ID と Password を入力，送信する

(B3) 認証結果を受け取る

認証手法は 1 点をのぞいて既存のパスワード認証とまったく同じである．それは (B1) 処理において，自分専用の個人認証ページにアクセスして個人認証を行う点である．つまり各ユーザは (B-r3) で取得した Private URL でしか個人認証を行うことができず，その URL は各ユーザ毎に異なる．つまり自分専用個人認証ページの URL が知っている (=持っている) ことが Password 以外に検証される 2 つ目の機密情報となる．

なお各ユーザに割り当てられる個人認証用 Private URL は，Password 同様に任意のタイミングで変更可能とする．Private URL を紛失・忘却した場合はサービス側が提供する Public URL 上で電子メールアドレスと Passcode の 2 情報を入力する，そうでない場合はサービスに Login したのち Private URL の変更処理を行う．

この手法を提供すると，各サービスは Public URL で個人認証システムを提供する必要がなくなる．またユーザ目線でもメリットはある．Private URL さえ適切に管理できれば，認証操作自体はこれまでと全く同じであり，電子メールでのやり取りも不要となるため，2FA の適用において操作面で負担を増やすことになる可能性は低いと考える．

4.3 手法 C: 各ユーザが自分専用の Web システムを持つ

前節の手法により，個人認証時に電子メールを使用する必要性をなくすことはできた．しかし，サービス使用時に Private URL が必要となるため，(a) Private URL を Web ブラウザにブックマークする，(b) 使用機器内に電子データとして保存する，(c) 手帳にメモして所持し，必要に応じて URL をタイプ入力する，等の対応が必要となる．すると以下のような懸念が生じる．

- Private URL の管理負担増
- URL 入力による操作負担増
- Malware，不正アクセス，不正利用による機器からの情報漏洩
- 対象サービス数の増加にともなう上記懸念の増大

これらの問題に対処するため，各ユーザが自分専用の Web システムを所有し，前節の手法における個人認証用 Private URL をその Web システムで集約，一元管理する．したがってユーザがサービスに Login する場合，必ずこの Web システムから各サービスの個人認証ページにアクセスすることになる．よって正規ユーザは，自分専用 Web システムの URL だけ知っていれば，利用するサービス数が増えたとしても提案手法による個人認証を行うことができる．

表 1　提案した 3 手法の特徴比較

Table 1　Comarison table of the features of the three proposed methods

	手法 A	手法 B	手法 C
Private URL の有効期限	1 回のみ	中期的	中期的
電子メールのやり取り	必要	-	-
Web システムの所有	-	-	必要
URL 管理負担	なし	大	小
URL 入力負担	なし	あるかも	なし
スケーラビリティ	○	×	○

本研究では，この Web システムを “Auth-base” と呼ぶこととする．Auth-base は例えるならば「ユーザ専用の個人認証用オンラインブックマークシステム」と言える．ただし，一般のブックマークシステムと異なるのは，(a) システムの利用者は 1 名だけであり，(b) 個人認証処理を行う Web ページの URL しか管理せず，(c) 保存された URL の共有・開示は行わない, という点が異なる．また上記 (a) にある通り，Auth-base ではアクセスしてきたユーザが正規ユーザであることを検証するため，個人認証が必要となる．

5. 考察

5.1 改善点について

提案した手法は，Private URL という【情報】を各ユーザに割り当て，所持させることで実行可能な 2FA を提案した．これによりスマートフォン等の携帯端末や USB stick をはじめとする物理デバイスを所持しなくても利用可能な手法となっている．これは以下の利点をうむと考える．

- 物理デバイスを用意・維持するためのコスト不要
- 利用方法に関する学習コスト・操作コスト不要
- 機器の利用不能状態によるサービス利用不能化の回避
- 2FA 利用に対するユーザの心理的障壁低下

また上記以外に 2 章で述べた問題点である「紛失，プライバシ上の懸念，スケーラビリティ」の 3 点についても改善可能性があると考えている．紛失の問題だが，Private URL は紛失してもすぐに再発行できるため 迅速にリカバリすることが可能である．物理デバイスの場合これは困難である．プライバシ上の懸念についても問題は発生しない．提案手法の利用に際して User ID/Password の他に必要なのはサービス側で生成された Private URL だけであり，ユーザからサービス側に対して電話番号等の情報を提供する必要はなく，特定のアプリケーションをインストールしてその利用を強制されることもない．

スケーラビリティの問題とは，利用サービス数の増加にともなう 2nd code 用デバイス・情報の管理負担が増えることを意味する．既存の 2FA ではサービス数の増加にともない所持しなければいけない物理デバイスや利用しなければならないアプリケーションが増える可能性がある．こ

れに対して提案手法では，Private URL の提供・管理方法によって異なるが，手法 A では個人認証のたびに Private URL が電子メールで通知されるため，サービス数が増えても Private URL の管理負担が増えることはない．手法 C では Private URL を Auth-base 上で管理するため，利用サービス数が増えても Private URL の管理負担が増えることはないと考える．手法 B では Private URL の管理をユーザに委ねているため，サービス数の増加にともない管理負担も増えることになる．今後，パスワードマネージャや URL ブックマーク等の仕組みを流用するなど，Private URL 管理の負担を増大させない仕組みを実現することは今後の課題である．

5.2 利便性について

提案手法における最大の利点は，既存のパスワード認証と操作方法がほぼ同じことである : (手順 a) 個人認証を行う Web ページへアクセスする，(手順 b) User ID/Password を入力する，(手順 c) 認証結果を知る (個人認証に成功した場合，サービスにログインできる)．唯一の違いは，(手順 a) においてアクセスする個人認証のための Web ページが各ユーザ毎に異なり，それは秘密情報になったという点だけである．したがってパスワード認証の利用経験があるユーザならば，提案手法による 2FA を利用するにあたって新たに学習しなければならないことはごく僅かであり，苦労なく提案手法による 2FA を利用できるものと考えている．これは特定の物理デバイスを所持する必要がない，という利点とあいまって，2FA の利用に対するユーザの心理的障壁を下げることに寄与しうる利点だと考える．

また上記の他に，(a) 動作環境構築・ソフトウェアのインストールが不要，(b) 複数人によるアカウント共有が可能，(c) 認証手法が変化しないため，パスワードマネージャや Web ブラウザの拡張機能等の既存システムも継続利用可能といった利点がある．

5.3 安全性について

パスワード認証の脅威である以下の 3 つの攻撃手法に対し，提案手法の安全性について考察する．

パスワードリスト攻撃

パスワードリスト攻撃とは「攻撃者が正規ユーザの User ID/Password を知っている状況でなりすまし行為を行う」ものとして議論を進める．つまり既存のパスワード認証では即座になりすましに成功されてしまう状況である．この攻撃に対して提案手法は一定の安全性を担保可能である．それは特定のユーザになりすますためには User ID/Password の他に個人認証を行う Web ページの URL が必要となるからである．攻撃者がそれを取得しない限り User ID/Password を持っていたとしてもなりすましは困難である．

なお個人認証用 Web ページを示す Private URL も User ID/Password と一緒に漏洩する可能性はある．しかし，その場合でも他のサービスでなりすましを行うことは困難である．Private URL は各サービスでランダム生成されるため，とある Service から (User ID/Password/Private URL) の 3 情報が漏洩したとしても，その漏洩した Private URL は他のサービスで必要な Private URL と異なるからである．

Phishing 攻撃

Phishing 攻撃に対する安全性だが，提案手法は一定の安全性があると考える．提案手法でサービスに Login するのに必要な情報は (User ID/Password/Private URL) の 3 情報である．このうちユーザ・インタフェース (UI) を通じて入力する必要のある情報は User ID/Password の 2 つだけであり，Private URL を UI 経由で入力する必要はない．Private URL は個人認証ページにアクセスするのに必要な情報であり，アクセスしたあとは不要な情報だからである．そもそも Private URL は，正規ユーザとサービス側で共有されている秘密情報であるため，それをユーザに問うこと自体不自然である．したがって攻撃者が 3 情報の入力を促すような偽物の Web ページを作成して 3 情報を窃取しようとしても，「個人認証ページは User ID/Password を入力するだけであり，Private URL を入力させるのはおかしい」となり，明らかに偽の個人認証ページであることに気づくことができるようになる．

また SMS や電子メール等で Phishing ページの URL を通知し，ユーザを誘導する行為も明らかにおかしな行為となる．前述の通り，Private URL は秘密情報の 1 つである．その Private URL をサービス側からユーザに通知すること自体，個人認証を運営するサービス側の行為としてあってはならない行為となるからである．したがって，Phishing ページにユーザを誘導するために URL を通知したメッセージを何らかの方法で行う自体が発生した場合，それは明らかに Phishing 攻撃であると判断できるようになる．

しかしながら，提案手法が Phishing 対策に対する強固な対策になるとは言いがたい．提案手法に対するユーザの理解不足により Private URL を入力してしまう可能性はある．また提案手法における Private URL の通知と管理方法に依存したリスクもある．手法 B では Private URL の管理をユーザに委ねており，個人認証のたびに URL を入力する利用法もありうる．この場合，ユーザの勘違いや思い込みにより本来は入力する必要のない箇所に Private URL を入力してしまう懸念はある．また手法 A では個人認証操作の一環として電子メールによる URL 通知とその URL へのアクセスが必要となっている．この操作手順を

Phishing 攻撃に悪用される懸念もある．

こういった懸念を提言するため，Auth-base という Private URL を管理する仕組みを提案した．Auth-base で Private URL の管理を行うことで，Private URL の管理負担を低減でき，ユーザが Private URL の値を知る必要もなく，電子メールのやり取りも不要となる．よって前述の手法 A，B におけるリスクは低減できる．また Auth-base を利用により，ユーザの個人認証処理に対する認識を「個人認証は必ず Auth-base から始める」というものに変化させる．それにより電子メールや SMS 等で通知される URL やリンクボタン等を用いて個人認証ページにアクセスし個人認証をすることはありえない．という文化にしていければと考えている．

Man-in-the-Middle 攻撃

本論文で提案している 3 手法は Man-in-the-Middle 攻撃 (MITM 攻撃) には脆弱である．個人認証を行うのに必要な 3 情報 (User ID/Password/Private URL) は Network 経由でユーザ-システム間でやり取りされる．よって，通信経路上で通信内容を窃取された場合第三者がなりすましを行うのに必要な 3 情報を攻撃者に盗まれることになる．今回提案の 3 手法は，どれも Transport Layer Security(TLS) 通信で通信を行うことが必須条件であり，通信経路上で MITM 攻撃が発生していなければ安全性が担保される仕組みとなっている．また MITM 攻撃が行われることを想定し，One-time コードや Challenge and Response 方式を提案手法内に組み込みことも検討していきたい．これは今後の課題である．

手法由来のリスクについて

提案手法の安全性は，Private URL が第三者に容易に特定されない，という前提のもとで成り立つものである．Private URL にどれだけの乱数値を含めるかにも依存するが，URL スキャンを行うのにどれだけの時間がかかるか？はサーバ側の実装方法と環境による．これについては評価を行うとともにスキャンを困難化する対策が必要があると考えている．

なお上記 URL スキャンにより Private URL が特定されたとしても，攻撃者がなりすましを成功させるためにはもう 1 つクリアしなければならない課題がある．それはスキャンによって特定された URL がどのユーザのための個人認証ページなのかを知ることである．Private URL は各ユーザに個別に割り当てられている．したがって特定された URL で個人認証が行えるのはそのサービスに存在するユーザのうちの特定一人だけである．しかしながら，それを知るためには，サービス側，ユーザ側または Auth-base に保存されているアカウント情報を盗む必要があることから容易なことではない．また特定された URL において個人認証が行えるはずの User ID とは異なる User ID を入力して個人認証を試みた場合，サービス側はそれが明らかに不正ログイン行為であると判定できる．よって提案手法は，サービス側が不正行為に対して迅速に対応できる仕組みにもなる．

次に Auth-base に関するリスクについて述べる．Auth-base も Web システムであり，ここから Private URL 情報が漏洩する可能性がある．しかし前述同様，Auth-base から漏洩する情報は特定 1 ユーザが利用する複数サービスの Private URLs であり，それだけでは各 Private URL でログイン可能な User ID や Password は分からない．よって Auth-base からの情報漏洩だけで，即座になりすましが可能になるという事態にはならない．また Auth-base は 1 ユーザ=1 システムを前提としているため，Auth-base から情報漏洩が発生したとしても，それで被害を受けるのは特定 1 人だけにとどまり，大規模インシデントになる可能性はない．そうとはいえ，Auth-base は攻撃者の興味を惹くと推測する．Auth-base の不正利用を防ぐため，個人認証を設けるとともに Auth-base の URL も定期的に変更するなどの運用が必要であろう．これも今後の課題とする．

5.4 利便性と安全性のバランスについて

5.2 節で述べた通り，提案手法は既存のパスワード認証とほぼ同等の操作で，かつ物理デバイスを所持することなく 2FA を行える手法である．しかしその一方で 5.3 節で述べたとおり，MITM 攻撃に対する安全性は担保できない手法となっている．また Malware 感染や正規ユーザの管理不行き届きにより Private URL が悪意ある第三者に盗まれるリスクもある．よって提案手法は既存の 2FA 手法よりも安全性と利便性の双方において優れた手法とはいえない．パスワード認証と既存の 2FA の中間地点，すなわち安全性はパスワード認証よりは改善されているものの，既存の 2FA には及ばない，一方で利便性はパスワード認証よりは手間がかかるものの，既存の 2FA よりは利便性が高い手法になっていると考える．

著者はこのようなバランスを持つ 2FA 手法も選択肢の 1 つとして提供されるべきだと考える．パスワード認証の危殆化にともない，パスワード認証の安全性を改善する仕組みが必要となっており，その代表的手法として 2FA が運用されている．しかし，既存の 2FA は安全性を重視するあまり「簡単に使えるけれど，前述したコストが発生し，面倒だし困ることもある」と評価される手法になっており，結果的に「2FA は利用可能だが，実際に利用しているのは少数派」という状況になっていると推測する．こういった状況を改善していく上で別の選択肢 (個人認証手法) が提示され，それにより既存のパスワード認証から脱却するユーザを増やしていくことが現実的に不正アクセスに対するセキュリティを改善していくことにつながると考えるから

である．今回の提案手法は安全性重視になっている既存の2FA に対する別の選択肢として，安全性は若干低下するものの利便性を向上させる 2FA を提案することで，それを現実化することに資するものと考えている．

6. おわりに

Web サービスの多様性を考えると，最低限のセキュリティ機能としてパスワード認証は依然として必要であろうと考える．しかし，パスワード認証が Web サービスのユーザアカウントを保護する仕組みとして不十分であることも明らかである．この問題に対する対策として二要素認証 (2FA)/二段階認証 (2SV) が提供されているが，その利用・運用にはユーザ側にもサービス側にもコストが発生するため，2FA/2SV を提供していないサービスもあり，また提供されていたとしてもその利用率は低い状況にある．

そこで本研究では，2FA の利用要件にある「何らかの物理デバイスを所持する」という要件を不要とする 2FA 手法として，特定ユーザしか知らない URL (Private URL) を 2nd factor とする 2FA 手法を提案した．Web サービスでは個人認証を行う Web ページにアクセスし，User ID/Password を入力してログインを行うが，提案手法ではこの「個人認証を行う Web ページ」をユーザ毎に個別の URL を割り当て秘密情報とする．これにより攻撃者が他者の User ID/Password を窃取したとしても，なりすまし行為を行うこと自体困難にすることができる．また個人認証を行う Web ページの URL が公知ではなくなるため，SMS や Phishing メール等で「この URL からログインしてください」という通知を受けること自体が不自然なこととなり，Phishing 攻撃対策にもなる．

この提案手法における安全性と利便性について考察を行なった．その結果，提案手法は既存の 2FA 手法より安全性で劣る面はあるが，物理デバイスの所持という制約がなくなり，その制約にまつわる問題点を改善できる手法であることを明らかにした．多様な Web サービスが存在する中で，既存の 2FA 手法を導入するほどコストはかけられないがパスワード認証の安全性を強化する手法は必要と考えるサービス運営者は少なくないと考える．このような状況において，既存の 2FA 手法以外の選択肢を提供しうる手法を提案できたと考えている．今後の課題だが，Private URL にまつわるリスク評価とその管理・運用を支援する auth-base について設計を進め，提案手法の実装可能性を検証する．またシステムの実装ができ次第，既存の 2FA 手法と提案手法についてユーザビリティと安全性認知について比較評価を行う計画である．

参考文献

[1] Reynolds. J, Samarin. N, Barnes. J, Judd. T, Mason. J, Bailey. M, and Egelman. S: Empirical Measurement of Systemic 2FA Usability, 29th USENIX Security Symposium, pp.127–143, (2020). available from ⟨https://www.usenix.org/conference/usenixsecurity20/presentation/

[2] Reynolds. J, Smith. T, Reese. K, Dickinson. L, Ruoti. S, and Seamons, K.: A Tale of Two Studies: The Best and Worst of YubiKey Usability, IEEE Symp. on Security and Privacy (SP 2018), pp.872–888, (2018). available from ⟨https://doi.org/10.1109/SP.2018.00067⟩

[3] Lang J., Czeskis A., Balfanz D., Schilder M., and Srinivas S.: Security Keys: Practical Cryptographic Second Factors for the Modern Web, Financial Cryptography and Data Security (FC 2016), (2017). available from ⟨https://doi.org/10.1007/978-3-662-54970-4_25⟩

[4] Reese. K, Smith. T, Dutson. J, Armknecht. J, Cameron. J, and Seamons. K: A Usability Study of Five Two-Factor Authentication Methods, Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), pp.357–370, (2019). available from ⟨https://www.usenix.org/conference/soups2019/presentation/reese⟩

[5] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. Christin, "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University, CHI Conference on Human Factors in Computing Systems (CHI 2018), (2018). available from ⟨https://dl.acm.org/doi/abs/10.1145/3173574.3174030⟩

[6] Thomson, I.: Who's using 2FA? Sweet FA. Less than 10The Register, (2018). available from ⟨https://www.theregister.com/2018/01/17/no_one_uses_two_factor_a

[7] Wiefling. S, Dürmuth. M, and Iacono. L,: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication, Annual Computer Security Applications Conference (ACSAC '20), (2020). available from ⟨https://doi.org/10.1145/3427228.3427243⟩,

[8] Twitter, Inc., Account Security in Transparency report, (2020). available from ⟨https://transparency.twitter.com/en/reports/account-security.html#2020-jul-dec⟩

[9] Heim, P.: An inside look at how we keep customer data safe, (2016). available from ⟨https://blog.dropbox.com/topics/product-tips/dropbox-customer-data-safety⟩

[10] Wharton, Z.: Multi-factor authentication adoption: 75yubico Blog, (2021). available from ⟨https://www.yubico.com/blog/75-of-enterprise-security-managers-plan-to-increase-mfa-spending-according-to-new-study-by-yubico-and-451-research/⟩

[11] Risher, M.: A simpler and safer future – without passwords, Google Blog, (2021). available from ⟨https://blog.google/technology/safety-security/a-simpler-and-safer-future-without-passwords/⟩

[12] Salesforce help, 多要素認証 (MFA) への対応のお願い, (2021). available from ⟨https://help.salesforce.com/s/articleView?id=000356005&type=1⟩

[13] The White House, Executive Order on Improving the Nation's Cybersecurity, (2021). available from ⟨https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/⟩

[14] Duo, Multi-Factor Authentication from Duo, available from ⟨https://duo.com/product/multi-factor-authentication-mfa⟩

[15] yubico, The YubiKey, available from ⟨https://www.yubico.com/products/⟩