Vol.2017-IS-141 No.7
2017/8/26

二要素認証利用時の安全性に関する一考察

柿崎 淑郎[1,a)]

概要：我々の生活において Web サービスの利用は最早必須に近い存在となっている．そのような重要性の Web サービスのアカウントでありながら，安易なパスワード設定や複数の Web サービスで共通のパスワードを用いるなど，ユーザ自身のセキュリティ意識の低さから，様々な問題が発生している．このような状況にあって，アカウントを守るための手段として，二要素認証が様々な Web サービスで利用できるようになっている．本稿では，二要素認証利用時におけるアカウントの安全性について考察し，ユーザが安全に Web サービスを利用するための方策を述べる．

A Consideration of Security under Two-Factor Authentication

Yoshio KAKIZAKI[1,a)]

1. はじめに

いま，我々の社会活動において，インターネットの活用は当たり前の存在となっている．野村総合研究所の調査 [1] によれば，ID とパスワードによる認証を要する Web サイトの利用は平均して 19.4 サイトであると報告されている．また，覚えていられる ID とパスワードの数は平均で 3.1 組であり，利用する Web サイトのアカウント ID とパスワードを記憶にのみ頼っていた場合，覚えていられるパスワードの数よりも，利用するアカウントの数の方が多いため，いくつかのアカウントで同じパスワードを用いていることが予想される．これはいわゆる「パスワードの使い回し」として知られており，多数のユーザがパスワードを使い回しているという調査結果が国内外から報告されており，大きな問題となっている [2,3]．

このような状況にあって，パスワードを使い回しているユーザを狙った攻撃として，2012 年頃よりパスワードリスト攻撃が激化している [4]．パスワードリスト攻撃とは，なんらかの方法で得られた有効と思われるアカウントリスト（ID とパスワードの対）を用いて，攻撃対象にログインを試みる攻撃手法である．類似の攻撃にはよく使われるパスワードを用いた辞書攻撃があるが，パスワードを使い回している現状においては，有効なアカウント情報があれば，それと同じアカウント情報が他のサイトでも利用されていることが期待され，攻撃の成功確率は辞書攻撃に比べて高くなる．また，辞書攻撃では 1 つのアカウント ID に対して，パスワードには辞書を用いて複数回のログイン試行が行われるため，サービスプロバイダ側に多数のログイン試行記録が残り，複数回のログイン失敗によるアカウントロックなどで攻撃が防ぐことができる．一方で，パスワードリスト攻撃では，1 つのアカウント ID に対しては 1 回しかログイン試行が行われないため，サービスプロバイダ側はその攻撃に気付きにくく，対策が困難である．

このようなパスワードリスト攻撃への対策としては，大きく分けて 2 つある．1 つ目は根本的な対策として，パスワードの使い回しをやめ，すべての Web サイトで異なるパスワードを用いることである．仮にどこかの Web サイトからアカウント情報が漏洩し，攻撃者がアカウントリストを手に入れたとしても，そのパスワードを他の Web サイトで使い回していなければ，パスワードリスト攻撃は成立しない．しかし，先にも述べたように，コンピュータの計算性能や記憶容量とは異なり，人間の記憶力には限界があり，多くのパスワードを覚えることは困難である．そこで，多数のユニークなパスワードをソフトウェアに記憶させて利用するパスワードマネージャの利用や，1 回ログイ

[1] 東京電機大学
Tokyo Denki Uniersity
[a)] kakizaki@mail.dendai.ac.jp

ンすることで以降は ID 連携によって更なる認証を不要とするシングルサインオンの利用などが有効である．

一方で，これらの普及は十分とはいえない．パスワードマネージャは複数のアカウント情報を管理しているため，パスワードマネージャ自体を不正に利用されてしまっては元も子もない．そのため，パスワードマネージャを利用するためのパスワード（マスターパスワードなどと呼ばれる）を設定する．このマスターパスワードは，他人に推測されにくく，辞書攻撃に耐えられるような複雑で長いパスワードが推奨されており，それ自体を覚える困難さがある．

シングルサインオンも同様に，シングルサインオンサーバにログインするためのパスワードは攻撃に耐えられるような強固なパスワードであることが望ましく，記憶の困難がある．加えて，シングルサインオンの場合は，ID 連携する先の Web サイトがシングルサインオンに対応していなくてはならないというサービスプロバイダ側の問題もある．

二要素認証は二つの認証要素による認証を行う方式で，なりすましなどによる不正ログインの危険性を低下させることができる．ここで用いられる認証要素には以下のようなものがある．

- 知識によるもの（knowledge factors）
  パスワード，パスフレーズ，PIN など
- 所持物によるもの（ownership factors）
  IC カード，トークン，ワンタイムパスワードなど
- 本人の特徴によるもの（inherence factors）
  指紋，虹彩など

二要素認証では上記の異なる二要素を組み合わせて利用する．例えば，パスワードによる認証と IC カードによる認証，IC カードによる認証と指紋認証などが挙げられる．従来では銀行などの高度なセキュリティが必要なサービスに用いられていたが，近年ではパスワードリスト攻撃などの不正ログインへの対策として，一般的な Web サービスにも広く利用されるようになっている．

このように，異なる二要素の組み合わせによる認証を二要素認証と呼ぶが，Web サービス等では二段階認証と呼ばれることもある．また，異なる二要素の組み合わせではなく，単要素を二回繰り返す認証のことを二段階認証と呼ぶこともある．本稿では，これらを区別することなく，二要素認証と呼ぶこととする．

本稿では，ユーザのオンラインアカウントを攻撃から守る上で，二要素認証がどのように利用され，どのように安全性に寄与しているかを考察する．二要素認証に対応している Web サービスについて，攻撃者がパスワードを忘れたと偽って，対象者のアカウントを乗っ取る方法とその可能性を明らかにするために，パスワードを忘れた場合，どのような方法でログインする手段があるかを調査する．その上で，二要素認証を設定することで，安全性がどのように向上するかを調査する．これらより，ユーザが安全に Web サービスを利用するための方策について考察する．

2. 関連研究

Florêncio らは，強力なパスワードの耐久性の基準を現実的に調査し，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を明らかにした [5]．また，文献 [6] では，パスワード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，パスワード使い回しの許容とパスワードの強度にはトレードオフの関係があることを示した．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．

大谷，秋山らはパスワード使い回しなどによって，アカウントに不正ログインされた場合に，マイページなどから得られるユーザに関する情報について調査している [7–10]．大谷，秋山らの調査から，すべてのアカウントを強力なパスワードで守ることができないのであれば，不正ログイン時の影響や漏えいする情報などに基づいて，アカウントが詐取された場合のリスクを算出し，それに基づくパスワード設定手法を提案している．

久保らは，パスワード再発行方式が 7 つあることを明らかにし，各方式の安全性の評価を行っている [11]．その結果，再発行要求後，Web ページ内で秘密の質問などを用いて本人確認を行う「ページ型」の安全性が最も低いことを明らかにするとともに，パスワード再発行を安全に行う手法の提案を行っている．

3. 二要素認証に対応している Web サービスの調査

二要素認証に対応している Web サービス（金融関係を除く）のうち，大規模で利用者が多い Web サービスについて，二要素目の要素としてどのような認証要素が採用されているかを調査した．調査結果を表 1 に示す．

3.1 二要素認証に用いられる認証要素

表 1 に示した二要素認証に対応している Web サービスが利用している認証要素について説明する．

3.1.1 Time-based One-time Password (TOTP)

表 1 中で「TOTP」とした．Time-based One-time Password (TOTP) は RFC6238 [12] で標準化されており，実装の容易さ，スマートフォンアプリの対応などの理由で，広く利用されている．TOTP のスマートフォンアプリの例を図 1 に示す．

TOTP のアルゴリズム [12] は次の通りである．X はサーバと共有する値で，何秒ごとにワンタイムパスワードを更新するかを示しており，初期値は $X = 30$ 秒である．$T0$ は

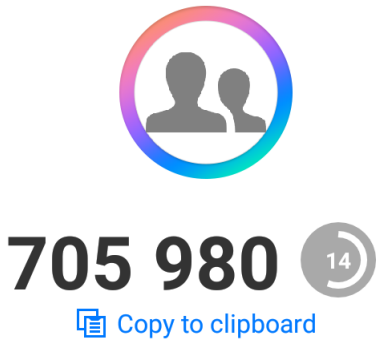

図 1 TOTP の例

Unix エポックであり，$T0 = 0$ である．また，検証者は秘密鍵 K を作成し，QR コードなどを利用して被認証者と共有する．TOTP は $T = \lfloor(\text{Current Unix time} - T0)/X\rfloor$ として，TOTP = HOTP(K,T) となる．ここで，HOTP(K,T) = Truncate(HMAC-SHA-1(K,T) であり，つまり，TOTP は HOTP (HMAC-based OTP) [13] のカウンター C を時間 T に置き換えたものである．

TOTP を用いた二要素認証では，TOTP に対応したソフトウェア（例えば Google Authenticator）を利用して，被認証者はワンタイムパスワードを生成し，検証者に示す．TOTP は SP 800-63B [14] では Single-Factor OTP Device となる．

3.1.2 ショートメッセージサービス（SMS）

表 1 中で「SMS」とした．ショートメッセージサービス（SMS）は携帯電話同士で用いられるメッセージ送受信サービスである．日本においては，いわゆるキャリアメールが普及しているが，全世界的には携帯電話を利用したメッセージ送受信手段として主流である．SMS では電話番号宛にメッセージを送信するため，電話番号の契約者と紐付けることができ，なりすましや不正利用の防止に寄与する．SMS の例を図 2 に示す．

SMS を用いた二要素認証では，被認証者の携帯電話宛に SMS で認証コードを送信し，被認証者は受信した認証コードを検証者に示す．SMS は SP 800-63B [14] では Out-of-Band Devices となるが，SMS の利用は RESTRICTED となっている．

3.1.3 FIDO Universal 2nd Factor（U2F）

表 1 中で「U2F」とした．FIDO は Fast IDentity Online の略であり，新しいオンライン認証技術の標準化を推進している団体で，二要素認証に関する標準である Universal 2nd Factor（U2F）[15] と生体認証を利用したログインを可能とする Universal Authentication Framework（UAF）の二つの標準プロトコルを策定している．

U2F による二要素認証では，U2F 規格に準拠したセキュリティキー（USB キーなど）を利用することで，二要素認証が行える．U2F は SP 800-63B [14] では Single-Factor Cryptographic Devices となる．

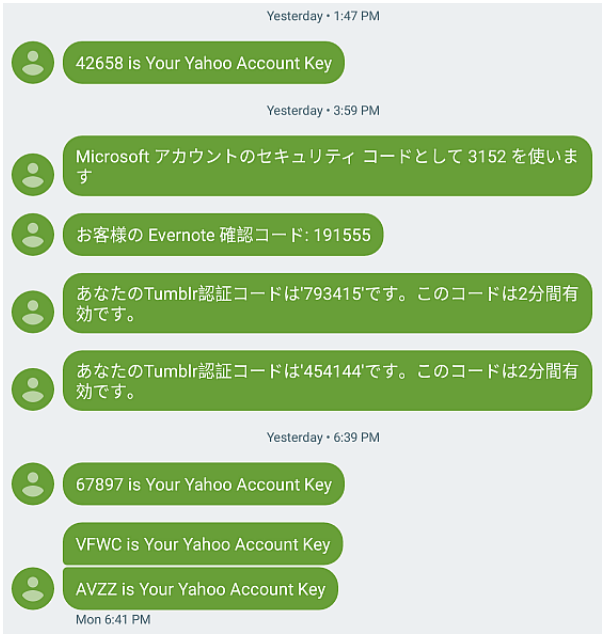

図 2 SMS の例

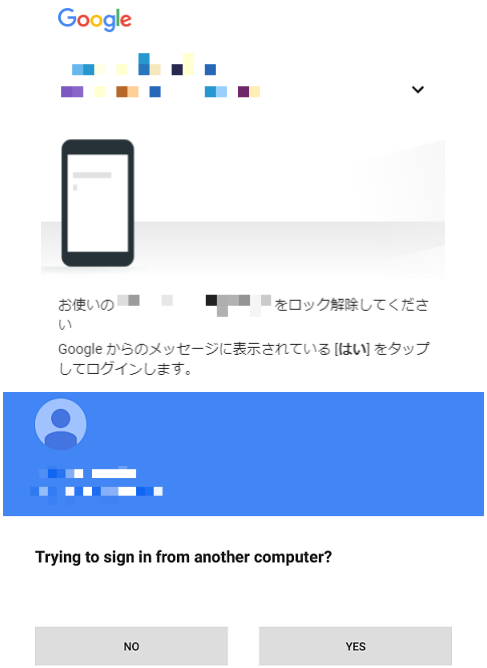

図 3 他端末の例

3.1.4 他の端末の利用

表 1 中で「他端末」とした．既に認証済みの端末に対して，認証の確認通知を行い，被認証者はその確認通知に対して応答することで，認証が行われる．この方式の例を図 3 に示す．

他の端末を利用した認証は SP 800-63B [14] では Out-of-Band Devices となる．

3.1.5 電子メールの利用

表 1 中で「メール」とした．登録されているメールアド

レスに対して，認証コードあるいは専用 URL が送信され，被認証者は検証者に対して認証コードを示すか，あるいは専用 URL をクリックすることで，認証を行う．

電子メールを利用した認証は SP 800-63B [14] では Out-of-Band Devices となるが，同じ通信路が利用される場合，二要素認証としての要件を満たさない．

3.1.6 音声通話の利用

表 1 中で「音声」とした．SMS の類似であるが，テキストメッセージではなく，電話番号に対して発信し，音声通話について認証コードが伝えられる．

音声通話を利用した認証は SP 800-63B [14] では Out-of-Band Devices となる．

3.1.7 専用デバイスの利用

表 1 中で「専用」とした．TOTP ではスマートフォンアプリなどのソフトウェアが用いられるのに対して，特定サービスにのみ利用できる専用のワンタイムパスワードトークンデバイスによって認証する．

専用デバイスを利用した認証は SP 800-63B [14] では Single-Factor OTP Device あるいは Multi-Factor OTP Devices となる．

3.1.8 バックアップコードの利用

表 1 中で「BC」とした．バックアップコードとは，スマートフォンの紛失や通信圏外などの理由により，TOTP，SMS，音声通話などでコードが利用できない場合に利用される，一度しか使用できない乱数である．基本的には，バックアップコードを二要素認証として使うのではなく，あくまで，非常時におけるログイン手段として利用されることが想定されている．

バックアップコードは SP 800-63B [14] では Look-Up Secret となる．

4. パスワード忘却時の調査

二要素認証未設定時において，パスワードを忘れた場合，どのような方法でログインする手段があるかを調査した．この調査は久保ら [11] の調査を参考として，表 1 に示した各 Web サイトにおける 2017 年 7 月時点での現状を調査した．この調査の目的は，攻撃者がパスワードを忘れたと偽って，対象者のアカウントを乗っ取る方法とその可能性を明らかにすることである．調査の結果を表 2 に示す．

パスワードを忘れた場合，何らかの手段で本人確認が必要になる．表 2 より，ほぼすべての Web サイトで，登録したメールアドレスに対して，パスワードを再設定する URL を送ることで，本人確認とアカウント復旧を行っている．Yahoo はアカウント作成時に SMS による認証が必要であり，パスワードリセット時においても SMS による認証で本人確認を行っている．また，メールアドレスが利用できない場合に備えて，有人サポートによる対応を行っている Web サイトも多い．

表 1 二要素認証に対応している Web サービスの例

Web サービス名	二要素目
Amazon	TOTP/SMS/音声
Amazon Web Services	TOTP/専用
Apple	SMS/他端末/BC
Dropbox	TOTP/SMS/U2F/BC
Evernote	TOTP/SMS/BC
Facebook	TOTP/SMS/U2F/他端末/BC
GitHub	TOTP/SMS/U2F
Google	TOTP/SMS/U2F/音声/他端末/BC
Instagram	SMS/BC
LINE	SMS/他端末
Microsoft	TOTP/SMS/メール/音声
Slack	TOTP/SMS/BC
Tumblr	TOTP/SMS
Twitter	TOTP/SMS/BC
Yahoo (US)	SMS/音声
Yahoo Japan	TOTP/メール
Wordpress.com	TOTP/SMS
クロネコヤマト	メール

表 2 二要素認証未設定時におけるパスワード忘却時の対応

Web サービス名	対応
Amazon	メール
Amazon Web Services	メール
Apple	メール/本人確認
Dropbox	メール
Evernote	メール
Facebook	メール
GitHub	メール
Google	メール/本人確認
Instagram	メール
LINE	メール
Microsoft	メール/SMS/音声/本人確認
Slack	メール
Tumblr	メール
Twitter	メール
Yahoo (US)	SMS
Yahoo Japan	メール/本人確認
Wordpress.com	メール/SMS
クロネコヤマト	メール

このように，ネット上における連絡手段として，事実上，メールが唯一の手段となっている．また，携帯電話番号を登録した場合，携帯電話への SMS あるいは音声通話も重要な連絡手段となる．そのため，メールアカウントのパスワードを忘れたり，携帯電話を紛失等で使えない場合の対応は，より難しくなる．

いくつかの Web サイトはメールによるパスワードリセット以外の方法として，追加の本人確認を行っている．Microsoft はメールアドレスが利用できない場合に備えて，更なるアカウント復元手順を準備している．この手順では，生年月日，アカウントを作成した国などの情報に加え，過去に対象のアカウントで使ったことがあるパスワードの入力，最近メールの宛先として使ったメールアドレス，最近送信したメールの件名などによって，総合的に本人確認を行っている．

Google も同様に，更なる本人確認手段を準備している．この手段には，覚えている最後のパスワード，アカウントを作成した年月が用いられる．

Yahoo は生年月日と秘密の質問の組み合わせ，クレジットカード番号と生年月日の組み合わせ，T カード番号のいずれかで本人確認を行っており，第三者が知り得る情報が用いられている．

Apple は生年月日と秘密の質問が用いられる．

これらの Web サイトはメールアカウントを提供していたり，スマートフォンの利用に必要なアカウントを提供していたりしている．そのため，これらの Web サイトは，他の Web サイトに比べて，そのアカウントの重要性が高く，利用不可能となった場合の影響が特に大きい．

このように，これらの重要性が高い Web サイトでは，様々な方法で本人確認を試みている．しかしながら，パスワードを使い回していた場合や，パスワードが漏洩した場合などにおいては，過去に使っていたパスワードは第三者に知られる恐れがあり，また，宛先メールアドレスやメールの件名も，第三者に知られにくい情報ではないため，攻撃者によるアカウントの乗っ取りの可能性は有り得る．なお，SP 800-63B [14] において，秘密の質問は SHALL NOT[*1] となっている．

5. 二要素認証設定時の調査

5.1 設定可能な二要素認証の調査

4 章で示したように，二要素認証未設定時においては，パスワードがアカウントを守る主たる要素であった．これに対して，二要素認証を設定した場合，攻撃者がパスワードを知り得たとしても，二要素目の認証に対応できなければ，アカウントを乗っ取ることはできない．そのため，二要素認証を設定すれば，パスワードと二要素目の組み合わせでアカウントを守ることができる．まず，二要素認証を適用した場合に，アカウントのセキュリティがどのように向上するかを調査する．

表 1 に示したように，TOTP に対応している Web サイトが 13 箇所（72%）であり，SMS に対応している Web サイトが 15 箇所（83%）であり，ほぼ大半がこの 2 つに対応している．両方ともに対応している場合の使われ方は様々であるが，およそ以下のように分類できる．

- TOTP と SMS は排他的利用である
- TOTP を有効にしても SMS と併用でき，同じ認証コードである
- TOTP を有効にしても SMS と併用できるが，異なる認証コードである

これらによって，ID とパスワードによるログインが可能な状態であっても，さらに TOTP あるいは SMS による認証コードの入力が必要となり，正しい認証コードが入力できない場合，ログインはできない．認証コードは概ね 6 桁の数字で 30 秒ごとに変化する．TOTP の場合，この認証コードを得るには，TOTP を生成するソフトウェアが必要であり，主にはスマートフォンのアプリが利用される．SMS の場合も，SMS を受信する携帯電話，スマートフォン，タブレットなどが必要になる．そのため，スマートフォンを他人が容易に利用できるような状況下では，効果が低下する．

次に，バックアップコードを採用している Web サイトが多く，8 箇所（44%）である．バックアップコードは，数字 8 桁，12 桁，英数字 10 桁など，Web サイトによって様々である．バックアップコードは，3.1.8 項でも説明したように，一度しか使用できない乱数列であり，何度でも作り直しができる．このように，バックアップコードは複雑であり，覚えやすい文字列でもないため，覚えておくことは困難であるため，何らかの方法で保管しておくことが求められる．保管方法としては，印刷，スクリーンショットなどが推奨されている．印刷した場合，ID・パスワードとともに，同じ手帳に挟み込んだ保管すると，バックアップコードは二要素認証として効果は無くなる．スクリーンショットの場合，そのスマートフォンの安全性に依存するが，それ以外にも写真のバックアップなどでクラウドストレージを用いていれば，そのクラウドストレージの安全性も関係してくる．

最後に，表 1 では「他端末」と示した Web サイトが 4 箇所ある．これは，既にログイン済みの信頼できる端末に対して，ログインを確認するメッセージがアプリケーション経由で表示され，それに対するユーザの応答で，ログインの可否を決める．Google は「スマートフォンを使用してログイン」と呼んでおり，この方式を有効にすると，TOTP や SMS などの二要素認証は無効になる．この方式

[*1] Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., “What was the name of your first pet?”) when choosing memorized secrets.

もスマートフォン等の端末の安全性に依存するが，他の方式に比べて，ユーザの利便性は高い．

5.2 アカウント詐取の調査

次に，二要素認証を設定した場合における，対象者のアカウントを乗っ取る方法について調査する．

二要素認証を設定した場合，ID とパスワードの対が合っていたとしても，さらに二要素目による認証を必要とする．そのため，二要素認証が完了できない場合，ログインされることはない．二要素目として設定したデバイスが使用できない場合，複数の二要素認証を設定していれば，そのいずれかを利用してログインすることができる．また，バックアップコードが利用できる場合は，バックアップコードでもログインが可能である．対して，これらのいずれもが利用できない場合，有人サポートでの対応となる．

二要素認証を設定した状態で，パスワードリセットの手順は，二要素認証未設定時と同様の手順で行うことができる．つまり，登録されているメールアドレスに対して，パスワードを再設定する URL が送られてくる．ただし，二要素認証が設定されている場合，パスワード変更後のログイン時に二要素認証が行われるため，パスワードリセットをしただけでは，アカウントを乗っ取ることはできない．

このように，二要素認証を設定することにより，未設定時に比べて，安全性は格段に向上する．

6. 考察

4 章で示したように，二要素認証未設定時においては，アカウントはパスワードによってのみ守られている．対して，二要素認証設定時は，パスワードに加えて，二要素目の要素による認証によっても守られており，より安全性が高い．

ただし，二要素認証の場合，二要素が揃うことでログインできるため，SMS を受信するためのスマートフォンが使えない状況や，TOTP を生成するアプリが使えない状況では，二要素認証未設定時に比べて，安全性が向上する一方で，ユーザのログインは困難になる．

また，Google など，ログイン済みの信頼できる端末に対して通知を行う仕組みでも，スマートフォンやタブレットなどが必要となっており，ユーザのオンラインアカウントを守るために，スマートフォンの重要性が高まっている．現代社会においては肌身離さず持ち歩くことの多いスマートフォンを利用して，セキュリティを高める仕組みは，現実的な解であると考えられる．

このように，スマートフォンがセキュリティ上，重要な役割を担うようになっているが，スマートフォン自体の安全性については，議論の余地がある．3.1.2 項で述べたように，SMS の利用は SP 800-63B [14] において RESTRICTED となっている．例えば，スマートフォンアプリが SMS へのアクセス権限を持っていた場合，SMS に届く認証コードを盗み見ることが可能である．TOTP を生成するスマートフォンアプリを用いる場合も，スマートフォン端末自体のセキュリティロックを掛けずに利用することもできる．スマートフォンの盗難や紛失に備えて，十分な安全性のセキュリティロックを掛けることが望ましい．Android のパターンロックの安全性は高くないことが指摘されている [16] が，近年のスマートフォンには，指紋認証などの生体認証システムが導入されているものも少なくなく，安全性と利便性の両立のためには，積極的に活用していくことが望ましい．

一方で，スマートフォンを持たない，あるいは使うことができない，子どもあるいは年配者などのオンラインアカウントを安全に守る手段については，検討の余地がある．

参考文献

[1] 野村総合研究所：生活者と事業者を対象とした ID に関する実態調査，http://www.nri.co.jp/news/2012/120208.html. accessed Aug. 7, 2013.
[2] 情報処理推進機構：全てのインターネットサービスで異なるパスワードを！，https://www.ipa.go.jp/security/txt/2013/08outline.html (2013). accessed Jul. 25, 2017.
[3] JPCERT コーディネーションセンター：STOP!!パスワード使い回し!!キャンペーン 2016，https://www.jpcert.or.jp/pr/2016/pr160003_detail.html (2016). accessed Jul. 25, 2017.
[4] 情報処理推進機構：パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ，https://www.ipa.go.jp/about/press/20140917.html (2014). accessed Jul. 25, 2017.
[5] Florêncio, D., Herley, C. and Oorschot, P. C. V.: An Administrator's Guide to Internet Password Research, *Proc. The 28th Large Installation System Administration Conference (LISA14)*, pp. 35–52 (2014).
[6] Florêncio, D., Herley, C. and Oorschot, P. C. V.: Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts, *USENIX Security Symposium*, pp. 575–590 (2014).
[7] 大谷和也，柿崎淑郎，佐々木良一：情報漏えいリスクを低減するアカウント管理手法，情報処理学会研究報告，pp. 1–6 (2015). Vol.2015-IS-131 No.1.
[8] 秋山巧，大谷和也，柿崎淑郎，佐々木良一：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，情報処理学会研究報告，pp. 1–8 (2015). Vol.2015-IS-132 No.9.
[9] Akiyama, T., Otani, K., Kakizaki, Y. and Sasaki, R.: Evaluation of a Risk-based Management Method for Online Accounts, *Proc. of The Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec2015)*, IEEE, (online), DOI: 10.1109/CyberSec.2015.19 (2015).
[10] Kakizaki, Y., Akiyama, T., Otani, K. and Sasaki, R.: Online Accounts Management Method using Risk-based Approach, *Journal of Computer and Communications*, Vol. 4, No. 14, pp. 26–36 (online), DOI: 10.4236/jcc.2016.414003 (2016).
[11] 久保駿介，杉本大輔，上原哲太郎，佐々木良一：パスワード再発行方式の安全評価と最適な利用法提案，マルチメディア，分散，協調とモバイル（DICOMO2016）シンポ

ジウム，pp. 352–258 (2016). 2D-4.
[12] M'Raihi, D., Machani, S., Pei, M. and Rydell, J.: TOTP: Time-Based One-Time Password Algorithm, RFC6238 (2011).
[13] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D. and Ranen, O.: HOTP: An HMAC-Based One-Time Password Algorithm, RFC4226 (2005).
[14] Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E. and Richer, J. P.: Authentication & Lifecycle Management, NIST SP 800-63B, https://doi.org/10.6028/NIST.SP.800-63b (2017).
[15] Srinivas, S., Balfanz, D., Tiffany, E. and Czeskis, A.: Universal 2nd Factor (U2F) Overview, https://fidoalliance.org/specs/fido-u2f-v1.1-id-20160915/fido-u2f-overview-v1.1-id-20160915.html (2016). accessed Jul. 6, 2017.
[16] Uellenbeck, S., Dürmuth, M., Wolf, C. and Holz, T.: Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns, *Proceedings of the ACM-CCS'13*, ACM, pp. 161–172 (2013).