Authentication Shutter: 個人認証に対する攻撃を遮断可能する対策の提案

高田 哲司 †

† 電気通信大学
182-8585 東京都調布市調布が丘 1-5-1
zetaka @ computer.org

あらまし アカウントリスト攻撃による不正アクセス事案が多発している．この攻撃は複数のサービスにおいて利用者が同一のパスワードを使い回すことが原因と言われている．この問題に対する対策としてパスワード管理ツールの利用やシングルサインオン，二要素認証などが提案されているが，どの対策法にしても利用者に一定の負担を課すことになる．そこで本論文ではこれらとは別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枠組み「認証シャッター」を提案する．この提案により，攻撃者が個人認証を通じて正規の利用者になりすまそうとしても個人認証は決して成功しないようにする．またこの対策手法は，アカウントリスト攻撃以外の攻撃手法に対しても効力を発揮しうる対策となる．

Authentication Shutter: an Alternative Measure against Mass Attack with Leaked Account List

Tetsuji Takada†

†The University of Electro-Communications.
1-5-1, Chofugaoka, Chofu, Tokyo 182-8585, JAPAN
zetaka @ computer.org

Abstract Mass attack to web services with leaked account list has been done in recent days. I propose an alternative measure against the attack called “authentication shutter”.

1 はじめに

アカウントリスト攻撃 (aka. パスワードリスト攻撃, リスト型アカウントハッキングとも呼ばれる．以降本論文ではアカウントリスト攻撃と記す) [1, 2, 3] による不正アクセスが続発している．日経コンピュータの 2014 年 6 月 16 日の記事 [4] によれば，2014 年 6 月以降，日本のネットサービスを狙った不正アクセス事件が多発し，3 週間ほどで 800 万件弱の不正アクセスが行われ，その結果として不正ログインされたと報告されている件数は 50 万件を超えたとの報告されている．またこの攻撃は新たな攻撃手法ではなく，以前から知られている攻撃手法でもある．IPA によると 2013 年以降から多発していることが指摘されて [5]，資料「2013 年度版 10 大脅威」では 8 位「パスワード流出の脅威」として報告されている [6]．また前述の記事 [4] によると，この攻撃方法はもともとオンラインゲームの世界で問題になっていた攻撃手法で，

それが 2013 年頃からゲーム以外のサービスも攻撃対象にしてきた，と述べている．

この攻撃方法が明るみになったきっかけは 2013 年 4 月に発生した電子書籍販売サイト「eBook Japan」への不正アクセスに関する事件報告 [7] だと言われている．この事件報告では，事件の内容について詳しい調査結果が提供されている．その内容によると，不正ログインが成功した 779 アカウントについてそれぞれの認証試行回数 (= パスワードを入力した回数) を調べた結果，最大試行回数で 5 回であり，そのうち 1 回の試行でログインに成功したアカウントが半数近くあったとのことである．この結果から，攻撃者はアカウント名とパスワード情報を事前になんらかの方法で取得 (獲得) し，それを悪用して攻撃を行ったものと推測される．ただし eBook Japan からアカウント情報に関する情報漏洩はないという調査結果から，攻撃者が悪用したアカウント情報は，おそらく「他のネットサービスから漏えいしたアカウント情報」であると推測されている．

これらのことから言えるのは，この攻撃に対してサービス提供側だけで抜本的な対策を行うのは困難だという点である．いくつかの対策手法が提案されてはいるが，それらは利用者になんらかの対応を迫るものであったり，システムに手を加えることで攻撃に対する耐性を改善している．しかしながら，認証システムが攻撃され，その結果として不正ログインにつながる危険性は残る．さらに利用者に対してさらなる負担を強いる結果になるものもある．そこで本論文では，システムに手を入れる必要はあるもの，ユーザへの利用負担増加を抑えつつアカウントリスト攻撃への対策となる authentication shutter の提案について述べる．以降本論文では，2 章で 3 章で 4 章で

2　既存の対策手法

アカウントリスト攻撃は，サービス利用者が複数のサービスにおける個人認証で ID とパスワードを使い回すことが原因であるとされている [1, 3]．したがって ID&パスワードの使い回しをさせないようにする対策が重要であり，その方法として「アカウント管理ツール (パスワードマネージャ)」の利用が推奨されている．アカウント管理ツールとは複数の ID とパスワードの組情報を一括管理するためのツールであり，ソフトウェア [8] やクラウドサービス，そして専用機器 [9] などとして実装されている．利用者がパスワードを使い回す理由は，多くのパスワードを記憶保持できないためである．アカウント管理ツールでは，複数の ID&パスワードを記憶するかわりに，その管理ツールのマスターパスワード 1 つだけを記憶しておけば，その中で管理されている ID&パスワードが入力できる仕組みとなっており，利用者の管理負担軽減となる．この手法は認証システムに手を加える必要がなく手軽に始められるのが利点である．なおアカウント管理ツールでもいくつかの問題がすでに発生しており [10, 11]，このツールの安全性向上に関する提案も行われている [14]．

利用者が保持するパスワードを 1 つにするもう 1 つの方法は，シングルサインオン (Single Sign-On:SSO) である．これは 1 回の認証で複数のサービスを利用可能にする仕組みであり，利用者は 1 組の認証情報 (ID/Password) を保持すればよく，また一度認証をしておけば複数のサービスを利用するたびに個人認証を行う必要もなくなる仕組みである．このシステムの問題点は，サービス提供者とは別の第三者または組織に個人認証を委託することになる点である．これが許容されないサービスを運営する組織は，自組織で SSO システムを構築し，そして対象システムを SSO に対応させる必要がある．また多くの利用者が使用する著名なサービスが SSO に対応していくか現時点では不透明であり，Web ブラウザが SSO に対応することが普及の鍵であるという意見もある [13]．SSO へ攻撃やサービス利用における障害点となる懸念もある．

SSO と同様に認証手法に手を加える対策手法として 2 要素認証がある．これはパスワード以外に所有物や生体情報による認証を併用して検証を行う認証手法であり，金融機関やオンラインゲームでは 2 要素認証として導入が始まっている．これもサービス提供側の対応および利用

者への周知/対応が必要になることから，すべてのサービスで実施可能な対策とは言いがたい．

総務省から提供されている事業者向け対策集 [2] では，上記以外にパスワードポリシーの強化と特定条件での通信遮断を提案している．パスワードポリシーの強化とは，有効期限によるパスワード更新の強制、パスワードの管理徹底，パスワード再利用の禁止，推測困難なパスワードの利用強制である．これらの方策がパスワードの使い回しを低減させるかは疑問が残る．また通信遮断は IP アドレスをベースにしたものであり，攻撃元と推測される IP アドレスや普段と異なる IP アドレスからの通信を遮断することを提案している．これらも正規の利用者による個人認証要求を遮断してしまう懸念がある．

このように，いくつかの対策手法があるものの，それぞれに問題が残されている．そこで本論文ではこれらの対策とは別の対策を考えてみる．

3 Authentication Shutter の提案

アカウントリスト攻撃の成立理由は利用者によるパスワードの使い回しであることは前述した．しかし，これはサービス提供者側の責任回避も一因だという見方もできると考える．サービス提供側はパスワードによる個人認証を利用者に強制し，安全性を担保するための負担を利用者に強いておき「利用者が安全なパスワードをポリシーに従い決定し、使用すれば安全性は担保できる」としてサービス運用側はすべきことをしている，という立場である．この考えが妥当だと考えるならば，パスワードで安全性が担保できるとは限らない現状に対して，個人認証を 2 要素認証に変更する負担をサービス運用側が負うことも妥当だといえるかもしれない．

一方，利用者側から現状のサービスにおける個人認証を見た場合，その多くがパスワード認証なのが現実である．パスワードの利用と管理には困難がともなうと言われつつも，決められたパスワードポリシーにしたがってパスワードを設定し，認証を行っているのも 1 つの現実である．この状況において危険なパスワードを利用するのも，パスワードを使い回すのも利用者側から見れば，わかってはいてもやむを得ずせざるを得ないのが現状なのだとも言える．この状況を改善するため，パスワード管理ツールや 2 要素認証を利用するのも 1 つの対策だが，本研究では別の対策として以下の前提条件下でも不正ログインを失敗に終わらせる仕組みが実現できないか検討を行った．

- パスワードを使い回している
- ID とパスワードが漏えいした

そこで「シャッター (鎧戸)」の仕組みに思いいたった．

既存の個人認証は，24 時間 365 日営業で利用者からの要求に応えている一方で，攻撃者からの攻撃も受け付けていると言える．その状況で攻撃者にアカウント名とパスワードを知られた場合，不正アクセスを防ぐことはできない．そこでこの営業時間を正規の利用者が利用する場合のみに制限することが可能になれば，仮にアカウント名とパスワードを攻撃者に知られたとしても，不正アクセスを防ぐことが可能になると考えた．なおいわゆる「シャッター」は現実世界ではお店単位で運用されるのが一般的だが，個人認証の世界ではサービス単位で適用するのは困難だと言える．その理由は，サービスの利用者がどの時間帯に個人認証 (サービス) を利用するかを認証システム側で予測することは不可能だからである．仮に一定精度での予測が可能になったとしても，予測であり利用者が利用しない時間帯にシャッターを開けてしまったり，またその逆も考えられる．したがって，サービス単位ではなく利用者のアカウント単位で個人認証に「シャッター」を実現し，かつその「シャッター」は利用者自身で開閉する．このような仕組みが実現できれば，上に述べた前提条件でも攻撃を失敗に終わらせる仕組みが実現可能となる．つまり，シャッターが降りている間はアカウント名と正しいパスワードを知っていたとしても個人認証を通過できなくするのである．以降、本論文ではこの仕組みを「認証シャッター (Authentication Shutter)」と呼ぶ．

この認証シャッターには，もう一つの役割をもたせる．それは認証の利用状況確認/ 通知機

能である．シャッターの降りている店に悪さをしようとする悪人がいることを店主に伝える警報ブザーや監視カメラと同様，各利用者のアカウントを悪用しようとする試みの事実を正規の利用者にフィードバックする仕組みは，セキュリティ脅威の現実を認識させ，またパスワードの変更や強化に対する妥当な動機付けになると考える．総務省の対策集 [2] でも「ログイン履歴の表示」がサービス運営側における対策の１つとして示されており，被害の拡大を防ぐ方策とされている．また現状でも Google では “アカウントアクティビティ” として過去のログイン履歴が閲覧可能になっている．これを認証シャッターと組み合わせることで認証シャッターをより有用なものにできると考えている．

3.1 実装概要

本節では，Web サービスの個人認証を想定した認証シャッターの実装について一例を示す．図 1 は認証シャッターの処理構成である．

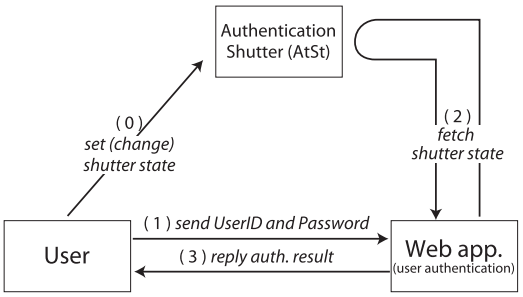

図 1: An Overview of User Authentication with Authentication Shutter

既存の個人認証は利用者 (User) と認証システムを提供するサービス (Web app.) の二者で処理が行われる．これに対して認証シャッターを用いた個人認証では，これらの二者に加えて認証シャッターの処理を行う構成要素が加わることになる．図 2 は，認証シャッター付き個人認証の認証手順を示したものである．

手順を順に説明する．まずはじめに認証を行う利用者は，利用するサービスの自分のアカウントに関する認証シャッターを「開ける」処理を行う (図中処理 a)．次に既存の個人認証と同

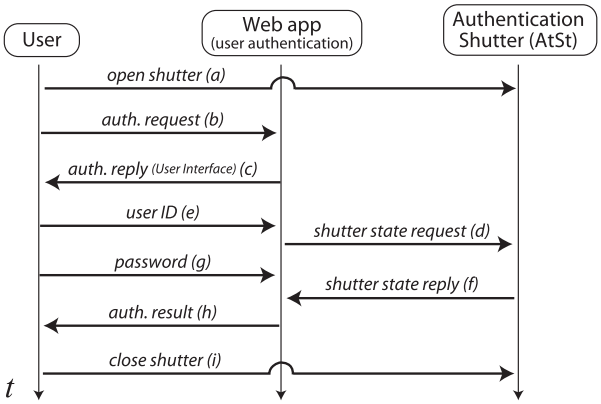

図 2: A Process Flow of a User Authentication with Authentication Shutter

じく認証を行う Web ページにアクセスし，個人認証のための User interface(以降，UI と記す) を表示する (図中処理 b, c)．その後，表示された UI を通じて利用者はアカウント名 (user ID) とパスワードを認証システムに送付する (図中処理 e, g)．その一方で認証システムは，認証シャッターに状態情報の要求を行い (図中処理 d)，その結果として自サービスの特定アカウントに対する認証シャッターの状態値を取得する (図中処理 f)．この状態値は 2 値であり，認証シャッターが開かれているか，閉じられているかのどちらかである．認証システムは，この状況で得られているパスワードと認証シャッターの状態値をふまえて認証結果を利用者に回答する (図中処理 h)．認証処理が終了したら，利用者は認証シャッターを「閉じる」(図中処理 i)．

表 1: パスワードと認証シャッター状態値による認証結果

	Password	Shutter state	Auth. result
A)	Correct	Open	Success
B)	Correct	Close	Failure
C)	Wrong	Open	Failure
D)	Wrong	Close	Failure

この説明からわかるように，難しい作業を利用者に強いるものではなく，現実世界でのシャッターと同じように利用前にシャッターを「開け

て」，利用後にシャッターを「閉じる」という行為が追加で必要になるだけである．

3.2 認証システム側の変更点

図 2 より認証システム側では 2 つの変更が必要になる．1 つは認証シャッターの状態値を取得する処理が新たに必要になる点であり，もう 1 つは認証判定処理を変更する必要がある点である．

認証シャッターの状態取得処理は，認証利用者から認証システムにアカウント名が送られてきた後，当該利用者の認証シャッターからサービス名称をキーとして現在の認証シャッターの状態値を取得する．前述の通り，返り値は 2 値であり認証シャッターが開いている (“0”) か，閉じている (“1”) かのどちらかである．なおこの処理を行うために認証シャッターの場所を示す情報が必要となる．またこの情報は各サービスにおける秘密情報の一部となるべき情報である．したがって，サービス利用開始時に利用者がサービス側に預ける利用者情報は (アカウント名、パスワード、認証シャッター URL) であり，うち後者の 2 情報は秘密扱いとする．また認証シャッター URL は，パスワードと同様，個人認証通過後であれば値を変更できるものとする．

認証判定処理は，これまでパスワードの値のみで行っていたが，認証シャッターを利用する場合はパスワードと認証シャッターの状態値の 2 つの値を入力として判定を行う．認証に成功するのはパスワード値が正解で，かつ認証シャッターの状態値が開かれている場合のみとする．表 1 にパスワードの値と認証シャッターの状態値の組み合わせと，各状況における認証結果を示す．このようにパスワード値が正解であるとしても，認証シャッターの状態値が閉じられていれば認証には成功しない．したがって認証シャッターを利用していれば，仮にアカウント名とパスワードが漏えいしたとしても，認証シャッターを閉じた状態にしておけば攻撃者が個人認証を不正にパスし，正規ユーザになりすますことはできなくなる．

3.3 Authentication Shutter の実装

Authentication Shutter は大きく二つの機能を持つ．1 つは認証シャッターの状態値を設定および提供する機能である．もう 1 つは個人認証の利用状況確認/ 通知機能である．これらは Web アプリケーションとして実装することを仮定して話を進める．

認証シャッターの状態値は (サービス名称，アカウント名) の組情報をキーとしてそれぞれ維持される．サービスが Twitter でアカウント名が uectokyo の場合の認証シャッター情報の例を図 3 に示す．Value の値は開放 (=0) と閉鎖 (=1) の 2 値である．

図 3: An Entry of Authentication Shutter Information

状態値の認証システムへの提供については REST 型 API として実装可能である．ただし攻撃者に認証シャッターの状態値を知られることは，それ自体が正規ユーザへのなりすましに直接つながるわけではないものの，望ましくはない．そこで状態値の提供については，状態値提供 API の URL において Path 部分にランダム値を含めることで安易に状態値を知られないようアクセス制御するものとする．

一方，認証シャッターの状態値変更は Web アプリとして実装可能である．UI としてはラジオボタンで認証シャッターの開閉を指示できるだけで良い．また状態値の設定を攻撃者に無断で変更されては困るため，以下の 2 つの仕組みでアクセス制御を行う．

手順 1): Web アプリを通じて認証シャッター操作要求を出す．この際，操作を希望する認証シャッターのサービス名とアカウント名を指示する．

手順 2): Web アプリは認証シャッター状態値変更処理への URL を電子メールで返送

する．この URL は path 部分にランダム値を含み，使い捨てとする．

手順 3): 利用者は受信した電子メールに記載の URL にアクセスし，認証シャッターを操作 (状態値を変更) する．

この方法は様々な Web サービスで行われているアクセス制御である．認証シャッターの操作要求のために個人認証を行わなかった理由は 2 つある．1 つは認証システム改善のために認証システムを利用するのは本末転倒と考えたためである．認証システムの安全性改善のために認証を必要となるならば，改善が必要な認証システムそのものを改良すべきであろう．またすでに 2 要素認証という改善策も提案されている．もう 1 つの理由は，認証シャッターの不正操作がなりすましに直結するわけではない点である．認証シャッターを攻撃者に操作され，仮にシャッターが開かれたとしても，それがなりすましに直結するわけではない．したがって上記の手順により認証シャッターからの電子メールを受信できる人だけが操作可能であればよいと考えた．

もう 1 つの処理は，個人認証の利用状況確認/通知機能である．認証シャッターでは図 1 からもわかる通り，個人認証を利用すると認証システムから認証シャッターへ状態値取得のアクセスが発生する．つまり個人認証を利用するたびにそれが認証シャッターに通知される仕組みとなっている．この仕組みをふまえ，あるユーザが自身で利用している複数サービスのアカウントを 1 つの認証シャッターで制御するとする．すると，そのユーザが所有する全アカウントの認証利用状況が一カ所に集約可能になる．この利用履歴情報を利用者に提供し，自身が持つアカウントの不正利用がないかを自分自身で監査可能にすることはアカウントの不正利用対策として望ましい．これまでは各サービス毎に提供されていた個人認証利用履歴が一つに集約できれば，監査にかかる手間も削減される．またユーザも攻撃されたアカウントとそうでないアカウントを簡単に把握可能になる．この情報を利用すればユーザが持つ他のアカウントに攻撃がおよぶ前に適切な対策を取ることも可能になる．

通知機能は前述の仕組みにより通知される個人認証の利用状況を電子メールで能動的に知らせる仕組みである．ただし認証シャッターからの通知ではその仕組み上「とあるサービスの認証を行っている」という事実しか通知できない．ただしその際に認証シャッターの状態値を利用することは可能なので，その認証行為が明らかに攻撃とおぼしきものか，正規利用者によるものかは判定可能である．通知の即時性と通知量のバランスを見て個別に設定可能なことが望ましいが，認証シャッターが閉じている際の認証行為は攻撃と見なして即時通知し，認証シャッターが開いている時の認証行為は正常な認証利用と見なして数時間に一回程度，利用履歴を集計して通知するというのが望ましいと考える．

4 考察

本研究で提案している対策手法「認証シャッター」は「攻撃にも耐えうる対策」ではなく「攻撃を無効にする対策」という点で既存のアカウントリスト攻撃対策とは大きく異なると考える．アカウントリスト攻撃に端を発した提案ではあるが，その効力はその攻撃だけに限定されず，個人認証に対する他の攻撃に対しても効力を発揮しうる対策手法であると考える．

また認証シャッターは，アクセス制御付きの個人認証と同じと見なすことができる．特定の IP アドレスからしかアクセスできないサービスで個人認証を行う場合などがこれに該当するといえる．しかし認証シャッターの特徴は，アクセス制御がサービスのアカウント単位で行なえるため，既存のアクセス制御よりもきめ細かくアクセスを制御することが可能な点である．

また認証シャッターでは総務省の対策集 [2] で対策の 1 つとしてあげられている「休眠アカウントの廃止」も対応可能である．それは認証シャッターを「オートロック」付きにすればよい．つまり利用者からの要求により認証シャッターを開いたとしても，一定時間経過後には自動的に閉じる仕組みにすることで，自動的に認証シャッターが有効となるようにすればよい．こうすれば使われないまま放置されたアカウントが存在したとしても，それらのアカウントは認証シャッ

ターによって自動的に保護され，攻撃の試みは失敗に終わることになる．

さらに認証シャッターではフィッシング詐欺対策にもなると考えられる．認証システム側には秘密情報としてアカウント名、パスワードの他に認証シャッターの URL を設定することになる．正規の認証システムはこの URL を持つが，Phishing 目的のために作成された偽認証システムはこの URL を持ち得ない．この差を利用し，認証後に個人認証利用履歴を確認して利用履歴があれば正規の認証システムとなるが，なければ Phishing 詐欺であると判定できる．

5 おわりに

本論文では，アカウントリスト攻撃への対策として「認証シャッター」という対策手法を提案した．当該攻撃に対する既存の対策手法はいくつか提案されているが，個人認証の利用者に一定の負担を課す手法であった．これに対して提案手法は，現実世界でのシャッター (鎧戸) と同じく既存の個人認証手法に対してアクセス制御を加える手法である．この認証シャッターによるアクセス制御は各サービスにおけるアカウント単位で行われ，その制御も各利用者が行うという点も既存のアクセス制御とは大きく異なる．またこの対策手法は「攻撃にも耐えうる対策」ではなく「攻撃を無効にする対策」となっており，既存の個人認証手法を流用しつつ，パスワードの使い回しをしていたとしても当該攻撃に対する安全性を高めうる対策となっている．

また本論文では認証シャッターの実装方法についても検討を行い，その一実装例についても考察を行った．Web サービスの個人認証を想定し，認証システムを提供するサービスとは別の構成要素として認証シャッターを実装することにより，個人認証へのアクセス制御だけでなく，利用者が利用している複数サービスでのアカウントの利用履歴の一括管理や，攻撃とおぼしき認証行為の即時通知も可能になることを示した．

参考文献

[1] トレンドマイクロ: アカウントリスト攻撃，<http://www.trendmicro.co.jp/jp/security-intelligence/threat-solution/access/index.html>, (参照 2014-08-24).

[2] 総務省: 「リスト型アカウントハッキングによる不正ログインへの対応方策について (サイト管理者などインターネットサービス提供事業者向け対策集)」の公表, <http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000063.html>, (参照 2014-08-24).

[3] IPA: 2013 年 8 月の呼びかけ - 「全てのインターネットサービスで異なるパスワードを!」～多くのパスワードを安全に管理するための具体策～<http://www.ipa.go.jp/security/txt/2013/08outline.html>, (参照 2014-08-24).

[4] 清嶋 直樹: 3 週間で 50 万件超の不正ログイン、「リスト型攻撃」が止まらない，<http://itpro.nikkeibp.co.jp/article/COLUMN/20140624/566362/>, (参照 2014-08-24).

[5] IPA: 「オンライン本人認証方式の実態調査」報告書について, <https://www.ipa.go.jp/security/fy26/reports/ninsho/index.html>, (参照 2014-08-24).

[6] . IPA: 「2013 年版 10 大脅威」～身近に忍び寄る脅威～，<http://www.ipa.go.jp/security/vuln/documents/10threats2013_slide.pdf>, (参照 2014-08-24).

[7] eBookJapan サポートセンター: 【重要なお知らせ】不正ログインに関する最終報告，<http://www.ebookjapan.jp/ebj/information/20130405_access.asp>, (参照 2014-08-24).

[8] AgileBits Inc.: 1Password - Have you ever forgetten a password?, Available from <https://agilebits.com/onepassword>, (参照 2014-08-24).

[9] KING JIM: パスワードマネージャ「ミルパス」, <http://www.kingjim.co.jp/sp/pw10/>, (参照 2014-08-24).

[10] , トレンドマイクロ: 「OpenSSL」の脆弱性「Heartbleed」によるパスワードマネージャーへの影響について, <http://esupport.trendmicro.com/solution/ja-JP/1103140.aspx>, (参照 2014-08-24).

[11] , ITPro: Web 版のパスワード管理ツールに潜む危険性、研究者が指摘, <http://itpro.nikkeibp.co.jp/atcl/idg/14/481709/071700003/>, (参照 2014-08-24).

[12] 西本逸郎:「賢い」情報管理で安全と便利を両立 ツイッターの個人情報流出の教訓 (下), <http://www.nikkei.com/article/DGXNASFK2600O_W3A220C1000000/>, (参照 2014-08-24).

[13] S.Sun, E.Pospisil, I.Muslukhov, et al.: What makes users refuse web single sign-on?: an empirical investigation of OpenID, In Proc. of 7th Symp. on Usable Privacy and Security (SOUPS '11), 20 pages, ACM, (2011).

[14] 鈴木雅貴, 中山靖司, 古原和邦: パスワードの使い回しおよび漏えいへの対策の検討 - ユーザによる安全なパスワード管理を目指して, 入手先 <http://www.imes.boj.or.jp/research/papers/japanese/14-J-09.pdf>, (参照 2014-08-24).