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

鈴木雅貴（すずきまさたか）／中山靖司（なかやまやすし）／古原和邦（こばらかずくに）

要　旨

近年、ウェブサービスからの情報漏えいが増加するなか、インターネット・バンキングや電子商取引サイト等のサービスにおいてパスワード（以下、「PW」と呼ぶ）を使い回しているユーザを対象とした不正ログイン（パスワードリスト攻撃）が急増している。同攻撃の原因の 1 つとして PW の使い回しが挙げられるが、利用するサービスごとに異なるパスワードを設定すると忘失すると考えるユーザが、やむを得ず行っている場合が多いと考えられる。PW の使い回しを前提とすれば、PW のほかに所持物による確認等を併用する「2 要素認証」が同攻撃への対策となるが、時間やコスト等の問題からすべてのサービスが同対策を直ぐに導入できるとは限らない。このほか、ユーザが記憶すべき PW の数を減らすことで PW の使い回しを回避するという対策もある。1 つは、1 回のユーザ認証で複数サービスへのログインを可能とする「シングルサインオン」であるが、同技術には、不正ログイン発生時の責任の所在が複雑になることを許容できるか、といったビジネス上の問題があり、すべてのサービスで利用できるとは限らない。もう 1 つは、各サービスの PW を 1 つのマスター PW で管理する「パスワード管理技術」である。同技術は、サービス側のシステム改修が不要であるほか、製品も多数存在する。しかし、いくつかの製品に欠陥があることが指摘されている等、同技術に求められる安全性について議論を深めることが不可欠である。そこで、本稿では、同技術の安全性要件や安全性の高い実現方法を示す。

キーワード：　パスワードリスト攻撃、パスワード管理技術、パスワード使い回し、2 要素認証、認証、情報漏えい、なりすまし

本稿の作成に当たっては、電気通信大学の高田哲司准教授から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行あるいは独立行政法人産業技術総合研究所の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

鈴木雅貴　日本銀行金融研究所主査（E-mail: masataka.suzuki@boj.or.jp）
中山靖司　日本銀行金融研究所企画役（E-mail: yasushi.nakayama@boj.or.jp）
古原和邦　独立行政法人産業技術総合研究所研究グループ長
（E-mail: kobara_conf-ml@aist.go.jp）

1. はじめに

近年、ウェブサービスへの不正アクセスによりユーザの認証情報が漏えいするインシデントが増加するなか、各ウェブサービスでパスワードを使い回していたユーザを対象とした不正ログイン（以下、「パスワードリスト攻撃[1]」と呼ぶ）が急増している。例えば、2013年だけでも、インターネット・バンキングや電子商取引サイト等に対してパスワードリスト攻撃による不正ログインが約80万件発生しているとの報道もある[2]。パスワードの使い回しの背景には、ID／パスワードによる本人確認（以下、「パスワード認証」と呼ぶ）を要するウェブサービスを1人のユーザが平均14個利用しているのに対し（トレンドマイクロ［2012］）、約7割のユーザが3個以下のパスワードしか記憶できないということがあり（シマンテック［2013］）、新たな問題として顕現化している[3]。

こうしたパスワードリスト攻撃による自社サービスへの不正ログインを防止するためには、使い回していたID／パスワードが他社サービスから漏えいしても、それだけでは不正ログインが成功しないようにする対策が有効といえる。具体的には、パスワードのほかに、所持物や生体情報を併用する「2要素認証[4]」が挙げられる。金融機関は、ログイン時または重要取引時の少なくとも一方において既に2要素認証を導入しているものの（金融情報システムセンター：FISC［2013］技35）、金融サービスと提携するさまざまな外部サービス（例えば、入金・出金を通知する電子メール等）に関しては、サービス提供者側のシステム改修が必要となることから[5]、同対策が直ぐに利用できるとは限らない。

このほかにも、ユーザがID／パスワードを使い回さなくても済むように、ユーザが記憶すべきパスワードの数を減らす対策も有効である。具体的には、2つの技術的対策が挙げられる[6]。1つは、1回のユーザ認証で複数サービスへのログインを可能とする「シングルサインオン」である。ただし、同対策はユーザ認証作業を外部に委託することになるため、導入に当たっては不正ログインが発生した場合の責

1 このほか、「パスワードリスト型攻撃」、「リスト型攻撃」、「アカウントリスト攻撃」、「リスト型アカウントハッキング」等とも呼ばれる。
2 日本経済新聞［2014］、国家公安委員会・総務大臣・経済産業大臣［2014］、勝村［2014］。また、2013年4月以降に発生したパスワードリスト攻撃について、不正ログインの「成立率（＝成立回数÷試行回数）」が0.15～1.35％であり、パスワードの全数探索攻撃や辞書攻撃の成立率よりも遥かに高いと指摘されている（情報処理推進機構：IPA［2013］）。
3 ユーザによるパスワード管理の実態については、**補論1**を参照。
4 普段とは異なる端末からのアクセス等を高リスクと判断し、追加の認証を行う「リスクベース認証」や「2段階認証」も、広義には2要素認証といえる。
5 一部の製品では、サービス提供者側のシステム修正を必要としないものも存在する。
6 なお、複数のパスワードを管理する非技術的な方法については、**補論2**を参照。

任を自社と委託先でどう分担するのかといった課題等があり、ビジネス上の理由から利用できないケースも想定される。もう 1 つは、各サービスの ID とパスワードをマスターパスワードで管理する「パスワード管理ツール」である。同対策については、サービス提供者側のシステム改修が不要であるほか、多種多様な製品が存在している。ユーザがサービス側の対応を待たずに自衛のために直ぐにでも同対策を利用可能であり、有望な選択肢と考えられることから、本稿の検討対象とする。

パスワード管理技術は、複数サービスの個別パスワードを一元管理しているため、パスワード保護の観点からは個々のウェブサービスよりも高い安全性が求められる。具体的には、サーバへの不正アクセスやユーザ端末の紛失等を考慮し、サーバやユーザ端末からの情報漏えいを想定すべきである。さらに、個別パスワードをマスターパスワードで暗号化する方式が主流であるが、近年の研究成果を踏まえればマスターパスワードが「短い（8 文字程度）」場合には全数探索攻撃等により解読されるリスクがあることも想定すべきである。しかし、実際に典型的なパスワード管理技術に対してこれらの脅威を想定したうえで安全性評価を行ったところ、個別パスワードを保護できないことが明らかとなった。本稿では、こうした安全性評価の内容を示すとともに、これらの脅威に対して安全なパスワード管理技術の実現方式についても検討する。

以下、本稿では、2 節においてパスワードリスト攻撃および同攻撃へのさまざまな対策を紹介したうえで検討対象とする対策を示す。3 節において典型的なパスワード管理方式の潜在的なリスクを示し、4 節において安全なパスワード管理方式の実現方式を説明する。5 節においてパスワード管理に関する考察を行う。

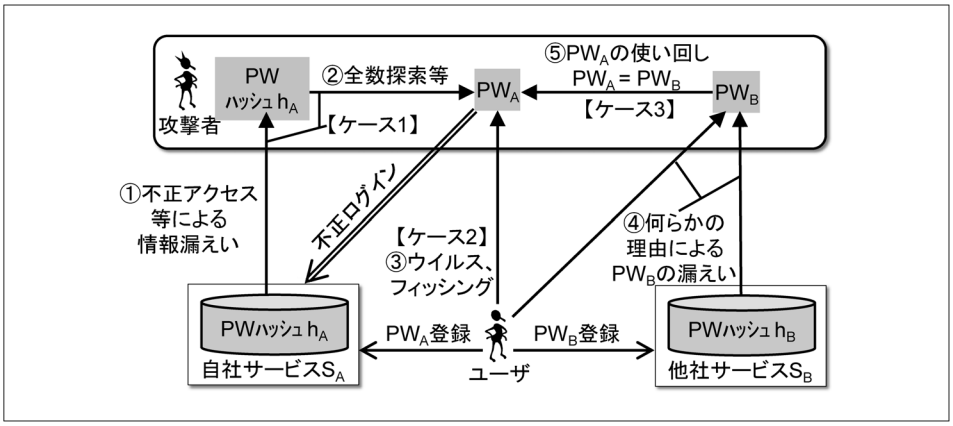
2. パスワードリスト攻撃と対策

本節では、パスワードリスト攻撃および同攻撃へのさまざまな対策を概説したうえで、本稿の検討対象であるパスワード管理技術に関する課題を示す。

(1) パスワードの漏えいとパスワードリスト攻撃

パスワードリスト攻撃を説明するために、自社サービスへの不正ログインが発生するメカニズムから順に述べる。ここでは、パスワード認証を採用している自社サービス（S_A）および他社サービス（S_B）に対して、ユーザがそれぞれ「ID_A，パスワード PW_A」と「ID_B，パスワード PW_B」を設定している状況を想定する（図表 1）。なお、各サービスでは、パスワードそのものではなく、パスワードに不可

図表 1　漏えいしたパスワードを用いた不正ログインの仕組み



逆変換等の暗号化処理（例：ハッシュ関数）を施した値（以下、「PW ハッシュ」と呼ぶ。それぞれ、h_A，h_B）を保存しているとする。自社サービス用のパスワード（PW_A）が漏えいするケースは、主に 3 つある（ケース 1〜3）[7]。なお、説明を単純化するために、攻撃者にとって ID は既知であると仮定する。

ケース 1（自社サービスからの漏えい）

自社サービスのシステムに対する不正アクセスにより PW ハッシュ（h_A）等が漏えいし（図表 1-①）、これらの情報を用いてパスワードの探索（「全数探索攻撃」、「総当り攻撃」、「辞書攻撃」とも呼ばれる）が行われることで、自社サービス用パスワードが推定される[8]（同②）。

ケース 2（ユーザ本人からの漏えい）

ユーザが入力したパスワードが PC に感染したウイルス（キーロガー等）に盗取されたり、フィッシングサイトに誘導されたユーザが同サイトに騙されてパスワードを入力したりすることで（同③）、自社サービス用パスワードが漏えいする。

7 サービス S_A に対して、よく知られている不適切なパスワード（例：「12345678」）を用いて不正ログインを試行する作業を繰り返す攻撃（「オンライン攻撃」と呼ばれる）も想定されるが、同攻撃に対してユーザが行う対策は、PW ハッシュからパスワードを復元する攻撃への対策に含まれるため、本稿では別途取り上げない。また、ソーシャルエンジニアリングによりサービス S_A の提供者から漏えいするケースも考えられるが、サービス提供者側の従業員教育が適切に行われており、そうした攻撃は防ぐことができると仮定し、本稿では同攻撃を取り上げない。

8 2013 年に発生した米 Adobe Systems の情報漏えいでは、ID や暗号化されたパスワード（PW ハッシュ）のほかに、パスワード忘却への備えとして保存されていた「パスワードヒント」が平文のまま漏えいした。同ヒントについては、一部のユーザがパスワードそのものやパスワードを容易に推定可能な情報を登録していたことがわかっている（Ducklin [2013]）。

ケース 3（他社サービスからの漏えい）

何らかの理由により他社サービス用パスワード（PW_B）が漏えいした際に（同④）、複数のパスワードを記憶することに負担を感じているユーザが、自社サービスと他社サービスで同一パスワード（PW_A=PW_B）を設定していたために（同⑤）、結果的に自社サービス用パスワードが漏えいする。こうして漏えいしたパスワードを使った不正ログイン（パスワードリスト攻撃）が近年急増している。同ケースは、「他社サービスからの情報漏えい」と「ユーザによるパスワードの使い回し」の組合せで成立するものであるが、どちらの原因についても自社の管理範囲外での問題であり、自社では防ぐことが難しく、新たな脅威として認識されている。

(2) パスワード管理に関する議論の必要性

上記のケース 1（自社からの漏えい）については、既存のさまざまな対策を講じることで漏えいリスクを軽減できる[9]。他方、上記のケース 2（本人からの漏えい[10]）とケース 3（他社からの漏えい）については、自社の管理範囲外であるため、期待通りに漏えいリスクを軽減できるとは限らない。そのため、安全性を高めるためには、漏えいしたパスワードだけでは不正ログインが成立しないように、所持物や生体情報といったパスワード以外の認証要素を併用する「2 要素認証」を採用することが有効である。

インターネット・バンキングでは、資金移動等の重要取引を行うまでにいずれかのタイミングで 2 要素認証を行っており（FISC［2013］技 35）、パスワードリスト攻撃に対しては耐性があるとも考えられる。しかし、重要取引には至らないまでも不正ログインは発生しているほか（勝村［2014］等）、金融サービスと連携した外部サービスがパスワードリスト攻撃により乗っ取られた場合には、総合的なセキュリティ対策が期待通りに機能しないケースも考えられる。例えば、多くの金融機関では不正送金検知等のために、口座の入金・出金が発生する都度、電子メール等で通知するサービスを提供しているが、同攻撃により電子メール等が乗っ取られると、電子メール等がユーザに適切に届かず、不正送金の検知が遅れることも想定される。

こうしたことから、金融機関だけでなく、連携するサービスにおいても 2 要素認

9 例えば、自社サービスへの不正アクセスの対策、漏えいした PW ハッシュからのパスワード推定を困難にするための対策（「ソルト」や「ストレッチング」の利用、強度の低いパスワードの排除等）が挙げられる（詳細は、徳丸［2011］を参照）。

10 ケース 2 に対しては、ウイルス対策ソフトやフィッシング対策ソフト（フィッシングサイトへのアクセスをブロックするソフトウエア）の利用、OS 等のセキュリティパッチの適用等の対策が挙げられる。

図表２　パスワードリスト攻撃への対策の比較

		利点	留意点
サインオン	シングルサインオン	・ユーザが記憶するパスワードの数の軽減 ・サービス側のパスワード等の管理が不要	・不正ログイン発生時の責任分担を明確にする必要がある ・認証サーバへの不正アクセスにより、対応するすべてのサービスへの不正ログインが発生するリスク ・サービス側のシステム改修が必要 ・ユーザが利用するすべてのサービスが同じ認証サーバで利用できない場合、複数のパスワードを記憶する必要がある
管理技術	パスワード	・ユーザはマスターパスワードのみを記憶すればよい ・各サービスのシステムの改修が不要	・同ツールに脆弱性があったり、ウイルスに乗っ取られたりすることで、各サービスのパスワードが漏えいする可能性 ・ユーザが偽ツールを入手する可能性

証の導入が進むことが望ましいが、同対策の導入にはシステム改修が必要となるため直ぐに普及するとは限らない。そこで、パスワードの使い回しを積極的に防止することで、パスワードリスト攻撃による不正ログインを防止する対策に焦点を当てる。

(3)　パスワードの使い回しを回避する対策

本来、パスワードは漏えいした時の影響を限定的にするため、各サービスで異なるパスワードを設定し、使い回しを行うべきではない。しかし、人間の記憶力には限界があり、類推されにくい複雑なパスワードをサービスごとに設定したうえで、記憶のみに頼ってパスワード管理を行うことは現実的には難しい。こうした問題への技術的な対策として、2 つの方法が知られている（図表 2）。

1 つは、1 回の本人確認で複数のサービスへのログインを可能とする技術である「シングルサインオン[11]」であり、ユーザが記憶するパスワードの数を減らすことにつながる。同技術は、ユーザ認証を集中して請け負う「認証サーバ」と委託するサービスから構成される。同技術を利用することで、各サービスは、パスワード等の認証情報を管理する必要がなくなるとはいえ、サービス側のシステム改修が必要となるほか、サービスによっては「ユーザ認証を外部に委託することが許されるのか」とか、「不正ログインが生じた場合の責任分担を明確化できるのか」等のクリアしておくべき課題がある。また、ユーザにとっては、自分が利用するすべてのサービスが同一の認証サーバに委託している場合には、文字通りのシングルサインオンを実現できるが、そうでない場合には結局複数のパスワードを管理することに

11　例えば、Kerberos（Neuman *et al.* [2005]）、OpenID（OpenID Foundation [2007]）、SAML（OASIS [2005]）等が挙げられる。

なる。仮に、普通の人が記憶する限界とされる 3 個を超えるパスワードを管理する必要がある場合には、依然としてパスワードを使い回す可能性が残る。

もう 1 つは、各サービスの ID ／パスワードを「マスターパスワード」により保護しつつ一元管理する「パスワード管理技術」である。同技術をソフトウエア等として実現したものは「パスワード管理ツール」と呼ばれており、表計算ソフトを利用してパスワード等を記録したファイルを同ソフトの保護機能により保護するといったものや（IPA［2013］）、ウェブブラウザのパスワード保存機能、市販の専用ソフトウエアまで多種多様なものが存在する。同ツールを利用する場合、通常、ユーザは 1 つのマスターパスワードを記憶するだけで済み、各サービスにログインする際は、同ツールから対応する ID ／パスワードを入手し、対応するサービスに入力する[12]。このため、サービス側のシステム改修は不要である。他方、ユーザが入手・利用するツールが偽物であった場合、管理されているすべての ID ／パスワードを盗取される可能性があるほか、正規ツールであっても脆弱性を悪用されることで ID ／パスワードが漏えいする可能性がある。

シングルサインオンは、一部のウェブサービスで既に利用されているものの、サービス提供者によってはビジネス上の理由等からユーザ認証を外部委託することが困難なケースがある。そこで、本稿では、サービス提供者の都合によらずに利用可能な「パスワード管理技術」を検討対象とする。

(4) パスワード管理技術に関する検討課題

パスワード管理技術は、各ウェブサービスの個別パスワードを一元的に管理していることから、個別のウェブサービスにおけるパスワードの保護よりも高い安全性が求められる。パスワード管理技術の安全性評価の動向をみると、一部の市販製品において各サービス用の個別パスワードが暗号化されていないといった有益な安全性評価の結果が示されている一方[13]（Belenko and Sklyarov [2012]）、各製品の安全性を比較しているものの、単に、利用されている暗号アルゴリズムを示しただけのものや（ITaP [2008]）、製品の詳細に触れずにいくつかの項目で定性的な評価を行っているもの（Bonneau *et al.* [2012]、McCarney [2013]）も多い。そこで、本稿では、パスワード管理技術が最低限想定すべき脅威を示したうえで、典型的なパスワード

12 パスワードの自動入力機能をもつパスワード管理ツールも存在する。同機能は、利便性に優れるほか、紛らわしい URL のフィッシングサイトであっても、同ツールが正規サイトの URL ではないと機械的に判断しパスワードの入力を回避するため、フィッシング対策として有効と言われている。

13 このほか、特定の形態のパスワード管理ツールに対する攻撃も報告されている（Bhargavan and Delignat-Lavaud [2012]）。

管理技術が同脅威に対して十分な安全性を満たしていないことを説明する。そして、同脅威に対して安全なパスワード管理の実現方法等についても検討する。

3. 検討対象とするパスワード管理方式とその安全性要件

本節では、典型的なパスワード管理方式や想定する安全性要件を示したうえで、情報漏えいに関する脅威と「短い」パスワードに起因する脅威について説明する。そして、これらの脅威を想定すると典型的なパスワード管理方式の安全性が十分ではないことを述べる。なお、本稿では、安全性が十分に高い暗号アルゴリズムを各パスワード管理方式が採用していることを想定し[14]、暗号アルゴリズムの脆弱性に起因する脅威は想定しない。

(1) 典型的なパスワード管理方式

パスワード管理方式では、通常、各サービス用の ID、パスワード（以下、それぞれ「個別 ID」、「個別パスワード」と呼ぶ）、各サービスの URL 等をデータベース（以下、「パスワード DB」と呼ぶ）として記録する（データベースを用いない方式については 5 節（1）で考察する）。典型的なパスワード管理方式では、マスターパスワードから暗号鍵を生成し[15]、同鍵を用いてパスワード DB を暗号化する（以下、「暗号化パスワード DB」と呼ぶ）。各サービスの個別パスワード等を抽出するには、マスターパスワードから生成した暗号鍵で暗号化パスワード DB を復号すればよい。パスワード管理方式は、暗号化パスワード DB を格納する場所に応じて「サーバ管理型」と「ローカル管理型」に分類できる（Karole, Saxena, and Christin [2010][16]、図表 3）。

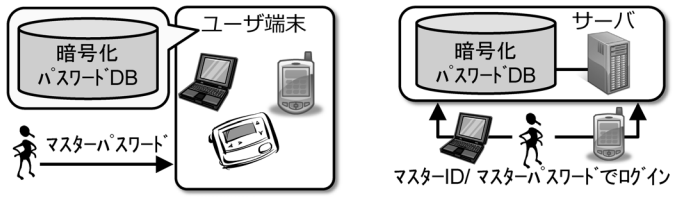
サーバ管理型パスワード管理方式は、暗号化パスワード DB をパスワード管理用サーバ（以下、単に「サーバ」と呼ぶ）に格納し、利用時には、同サーバにログインしたうえで、同サーバから入手した暗号化パスワード DB をユーザの端末上で復

14 各国が、政府系情報システムに利用可能な暗号のリストを公表しており、そうした安全な暗号を利用できる。わが国の電子政府推奨暗号については、総務省・経済産業省［2013］を参照。

15 マスターパスワードから暗号鍵を生成する方法としては、「Password-Based Key Derivation Function 2（PBKDF2）」等が知られている（Kaliski [2000]）。

16 McCarney [2013] では、マスターパスワードを使用せず、ユーザが所有する 2 台の端末にそれぞれ暗号化されたパスワード DB と暗号鍵を格納する方式が提案されている。同方式は、4 節（2）で示す「単純分散方式」をサーバと端末ではなく 2 台のユーザの端末で行う形態といえる。

図表 3　典型的なパスワード管理方式



(a) ローカル管理型　　(b) サーバ管理型

号する[17]。同サーバへのログインには、パスワード管理用の ID（以下、「マスター ID」と呼ぶ）とマスターパスワード[18] のほか、方式によっては追加の認証要素（2 要素認証）が利用される。同サーバにログイン可能な環境であれば、ユーザは任意の端末から個別パスワード等の抽出が可能であり、マルチデバイスに相対的に対応しやすいという特徴がある。

ローカル管理型パスワード管理方式は、暗号化パスワード DB をユーザの端末（PC、スマートフォン、小型の専用装置等）に格納し、利用時には、ユーザが同端末にマスターパスワードを入力し、同端末上で暗号化パスワード DB を復号する。その際、オンライン接続が不要であるという特徴がある。同方式をマルチデバイス対応させるには、複数端末間でのパスワード DB の共有・同期をいかに実現するかという課題がある。例えば、暗号化パスワード DB を USB メモリ等に格納して携帯すれば、任意の端末で暗号化パスワード DB の復号が可能になるが、暗号化パスワード DB の紛失・盗難のリスクは高まる。

(2)　想定する安全性要件

パスワード DB を安全に管理することがパスワード管理方式の目的であり、本人以外（以下、「攻撃者」と呼ぶ）にパスワード DB を漏えいしないことが安全性要件

17 暗号化パスワード DB の復号をサーバ上で行う場合、不正なサーバ管理者に復号結果を盗取されるリスクがある。

18 パスワード管理サーバへのログインとパスワード DB の暗号化に用いる各パスワードを個々に設定可能な方式も存在する。しかし、別々に設定可能だからといって安全性が向上するとは限らない。例えば、短いパスワードを 2 つ使用する方式と倍の長さのパスワードを 1 つ使用する方式のどちらが安全性が高いかは、想定する脅威によって異なる（フィッシング詐欺によりログイン用のパスワードを盗取された場合には暗号化用パスワードを別途設定していれば、そちらは漏えいしないという利点がある。他方、暗号化パスワード DB が漏えいした場合には、暗号化用パスワードの長さによって全数探索攻撃への耐性が決まる）。そこで、本稿では、ユーザが記憶するパスワードは 1 つのみというシンプルな制約のもとで議論することとし、個々にパスワードを設定する方式を検討対象外とする。

となる（安全性要件 1）。なお、サーバ管理者が不正を行う可能性もあるため、本稿では、サーバ管理者も想定する攻撃者に含める。また、ユーザがマスターパスワードをほかのサービス等でも使い回している可能性を考慮し、本稿では、パスワード管理方式に対する攻撃によるマスターパスワードの漏えいを防止できることも安全性要件として想定する（安全性要件 2）。

安全性要件 1：攻撃者に対してパスワード DB を漏えいしない
安全性要件 2：攻撃者に対してマスターパスワードを漏えいしない

(3) 情報漏えいに関する脅威

また、パスワード管理方式を利用するうえで、情報漏えいの観点から次のような脅威が想定される。まず、端末の紛失・盗難により、攻撃者が同端末内のデータを入手する可能性がある（脅威 1）。同様に、サーバへの不正アクセスやサーバ管理者の不正により、攻撃者がサーバ内のデータを入手する可能性もある（脅威 2）。さらに、ユーザがマスター ID ／パスワードを他のサービスで使い回している場合に、この他のサービスを対象としたフィッシング詐欺等により、攻撃者がこれらの情報を入手する可能性もある（脅威 3）。このほか、4 節で扱うパスワード管理方式では、USB メモリやメモ帳等の「外部メモリ」を利用することから、同メモリを盗取した攻撃者がその内部のデータを入手する可能性も想定する（脅威 4）。

脅威 1：ユーザの端末からの情報漏えい
脅威 2：サーバからの情報漏えい
脅威 3：マスターパスワードの漏えい
脅威 4：外部メモリからの情報漏えい

脅威 1（端末からの漏えい）に関連して、端末に感染したウイルスが、端末内で復号されたパスワード DB を盗取する攻撃も考えられる。しかし、端末がウイルス感染した場合には、パスワード管理方式の利用の有無にかかわらず個別パスワードが漏えいする可能性がある。このため、ウイルスによるパスワード DB の漏えいについては、ウイルス対策ソフト等により対策するものとし、本稿では検討対象外とする。ただし、ウイルス感染が疑われる端末を利用する場合においても、認証に対

図表 4　想定する安全性要件と情報漏えいに関する脅威の対応関係

<table>
<tr><th></th><th>安全性要件 1（パスワード DB の保護）</th><th>安全性要件 2（マスターパスワードの保護）</th></tr>
<tr><td>脅威 1（端末からの漏えい）</td><td rowspan="4">検討対象</td><td rowspan="3"></td></tr>
<tr><td>脅威 2（サーバからの漏えい）</td></tr>
<tr><td>脅威 3（マスターパスワードの漏えい）</td><td>検討対象外</td></tr>
<tr><td>脅威 4（外部メモリからの漏えい）</td><td></td></tr>
</table>

しては多端末認証[19]、ログイン後の不正操作に対しては「取引認証[20]」を導入することにより、その影響を軽減することは可能である[21]（鈴木・中山・古原［2013］）。

このほか、複数の脅威が同時に顕現化する確率は相対的に低いと考えられるため、本稿においては脅威 1〜4 を複数組み合わせた脅威については検討対象外とし、また、脅威 3（マスターパスワードの漏えい）により安全性要件 2（マスターパスワードの保護）が満たされないことも自明であるため検討対象外とする（図表 4）。

(4)　「短い」パスワードに起因する脅威

約 8 割のユーザが 8〜9 文字ないしそれ以下の桁数のパスワードを利用しているとの調査結果がある（リサーチバンク［2014］）。アルファベット（大文字、小文字）と数字の計 62 文字からランダムに 1 文字を選択する際の情報量は約 6 ビット（$= \log_2 62$）であり、ランダムに選択された 8 文字または 9 文字のパスワードの情報量は、それぞれ約 48 ビット、54 ビットとなる[22]。

パスワードに対する攻撃として、候補となるパスワードを 1 つずつ探索・検査する全数探索攻撃等が知られている。こうした攻撃への耐性は、探索に要する時間で評価されるが、半導体の集積率の向上等の技術進歩により計算機性能は年々向

19 PC とスマートフォンの組合せ等、複数の端末を併用する認証方法。一方の端末がウイルス感染しても、他方がウイルス感染しなければ不正ログイン等を防止できるという特徴を有する。

20 取引認証の実現方法は多種多様である。PC と別のデバイス（携帯電話、USB デバイス等）を併用する方法や、1 台の PC 上でウェブブラウザとは別の専用ソフトウエアを併用する方法等がある。また、振込先等に紐付いた認証コード（Transaction Authentication Number）を利用する方法や、振込先等にユーザの電子署名を付ける方法（Transaction Signing）等がある。

21 国内でも、本年 2 月から取引認証を導入した先が存在する（サイトウ・加藤［2014］）。海外をみると、例えば、シンガポールでは、2012 年末までに取引認証を導入することとの指針が示されているほか（ABS [2012]）、イギリスでも多くの金融機関（HSBC、Barclays、Lloyds、Standard Chartered、RBS 等）が取引認証を導入している。

22 人間が道具を使わずにパスワードを生成した場合、完全にランダムに文字を選択することは困難であり、完全にランダムに選択した場合よりも情報量が低下すると考えられる。なお、パスワードの情報量を評価する研究も行われている（Weir *et al.* [2010]、Burr *et al.* [2013] A2）。

上しており[23]、一定時間で探索可能なパスワードの数も年々増加している。このため、現実的に探索可能なパスワードの数を定期的に評価する必要がある。学界では、パスワードの安全性評価そのものではないが、汎用計算機や専用ハードウエアを用いた暗号解読の実証実験が行われている。具体的には、現在主流の公開鍵暗号「RSA」を対象に、公開鍵のサイズが 768 ビットの場合でも、80 台の計算機に約半年間計算処理を行わせることで、全数探索的に暗号解読可能であることが報告されている（Kleinjung *et al.* [2010][24]）。768 ビットの公開鍵の情報量は 60 ビットに相当すると見積もられており（森川・下山［2011］）、8〜9 文字程度の「短い」パスワードの場合には、全数探索攻撃が現実的な脅威になっているといえる[25]。このほか、英数字 8 文字のパスワードであれば、30 時間程度で探索可能であるとの試算も示されている（徳丸［2011］）。

以下では、ユーザは短いマスターパスワードを利用しており、マスターパスワードの全数探索攻撃は可能であるとの立場で検討を行う。

(5) 典型的なパスワード管理方式の潜在的リスク

典型的なパスワード管理方式（サーバ管理型、ローカル管理型）では、上記の脅威 1 あるいは脅威 2 を想定すると、暗号化パスワード DB が漏えいする可能性がある。パスワード DB の暗号化にはマスターパスワードから生成された暗号鍵が利用されているが、前述のとおりマスターパスワードが短い場合には、全数探索攻撃等によりマスターパスワードを特定されることで暗号化パスワード DB を解読され、その結果、パスワード DB が漏えいするリスクがある。このほか、サーバ管理型については、脅威 3 を想定すると、盗取したマスターパスワード等を用いて攻撃者が正規サーバに不正ログインし、パスワード DB を不正利用する可能性もある[26]。よって、典型的なパスワード管理方式は、脅威 1〜3 を想定すると安全性要件 1（パスワード DB の保護），2（マスターパスワードの保護）を満たさないことがわかる（図表 5）。

23 身近な事例として、同じ金額で購入可能な PC の性能は年々向上していることが挙げられる。

24 過去の RSA の公開鍵の解読記録は、例えば、情報通信研究機構：NICT・IPA［2012］p. 37 図 4.2 を参照。

25 なお、RSA の鍵長については、現在、2,048 ビット（情報量は 108 ビット）以上が推奨されている（Barker *et al.* [2012]、内閣官房情報セキュリティセンター：NISC［2008］）。

26 端末認証を行っている場合、漏えいしたマスターパスワードだけではサーバに不正ログインできないが、脅威 2 によるサーバからの暗号化パスワード DB の漏えいリスクは残る。

図表 5　典型的なパスワード管理方式の潜在的リスク

想定する脅威	ローカル管理型	サーバ管理型
脅威 1 （端末からの漏えい）	暗号化パスワード DB の解読により、マスターパスワードを特定され、かつ、パスワード DB を盗取されるリスク	想定されない
脅威 2 （サーバからの漏えい）	想定されない	暗号化パスワード DB の解読により、マスターパスワードを特定され、かつ、パスワード DB を盗取されるリスク
脅威 3（マスターパスワード等の漏えい）	暗号化パスワード DB が漏えいしていないため、パスワード DB は漏えいしない	サーバへの不正ログインによるパスワード DB の漏えい

4.　安全性要件を満たす実現方式

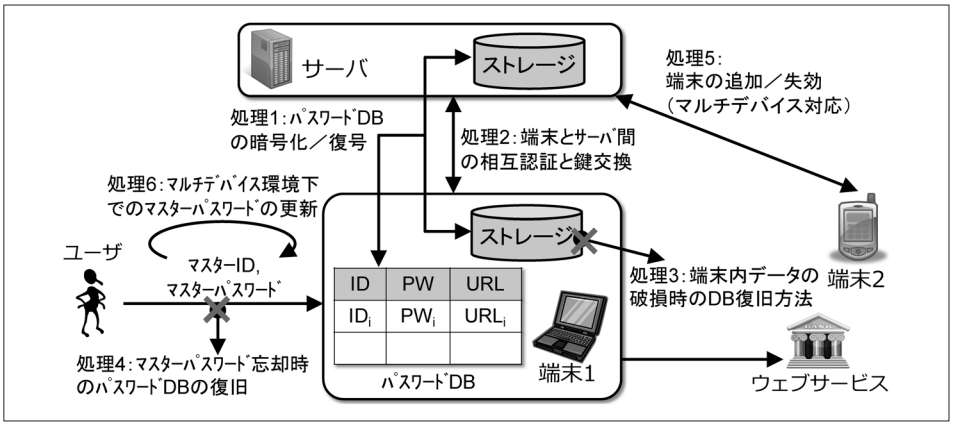
3 節で示したように典型的なパスワード管理方式は、脅威 1〜3 に対して安全性要件 1，2 を満たさないことから、本節では、これらの脅威に対して安全なパスワード管理方式を示す。なお、同方式では外部メモリを使用することから、同メモリからの情報漏えい（脅威 4）も想定する。以下では、まず、検討対象とするパスワード管理方式の形態と各処理（図表 6 の処理 1〜6）を示したうえで、相対的に重要性が高いと考えられる処理 1〜4 について、脅威 1〜4 に対して安全性要件 1，2 を満たす実現方式を示す。残りの処理 5，6 についてはマルチデバイス環境特有のオプション処理であるため**補論 3** で検討する。

(1)　検討対象とするパスワード管理方式の形態と各処理

サーバまたは端末の一方からの情報漏えい（脅威 1 または 2）に耐性を持たせるため、パスワード DB の利用に必要な情報を端末とサーバのそれぞれのストレージに分散して格納する形態（以下、「ハイブリッド管理型」と呼ぶ）を想定する[27]。ま

27 なお、外部メモリでパスワード DB を格納する形態については、同外部メモリを紛失した際にパスワード DB が漏えいするリスク（脅威 1 に相当）があるため、本節では検討対象としない。また、同一のパスワード DB をバックアップのためにローカルとサーバの両方で管理する形態については、ローカル管理型とサーバ管理型を併用した形態であるとみなすことができ、脅威 1，2 の両方の脅威に対して脆弱となることから、本節では検討対象としない。

図表 6　ハイブリッド管理型のパスワード管理方式



た、本稿では、同形態におけるパスワード DB の暗号化／復号に関する処理（図表 6 の処理 1，2）に加えて、障害等の発生時においてもパスワード DB の利用を可能にするための処理（同処理 3，4）や、マルチデバイス環境でもパスワード DB を利用するための処理（同処理 5，6）を取り上げる。各処理の概要は以下のとおりである。

処理 1：パスワード DB の暗号化／復号

パスワード DB を暗号化して保管し、利用時に復号するというパスワード管理方式のもっとも基本的な処理。なお、不正なサーバ管理者等による情報漏えい（脅威 2）への対策のため、サーバ上ではなく端末上においてパスワード DB の暗号化／復号を行うことを想定する。なお、データを正規サーバに預けたり、同データを正規ユーザのみが利用できることを保証するには、サーバ認証（フィッシング詐欺対策）、ユーザ認証（なりすまし対策）、暗号通信用の鍵交換（盗聴・改ざん防止）を行う必要があるが、これらに関連する処理は処理 2 で行い、処理 1 では扱わないこととする。

処理 2：端末とサーバ間の相互認証と鍵交換

端末とサーバ間で安全に暗号通信を行うための処理であり、具体的には、サーバ認証、ユーザ認証、鍵交換の 3 つを行う。この鍵で確立した暗号通信路を利用して、サーバへのデータの格納やサーバからのデータの入手が行われる。ハイブリッド管理型のようにサーバとの通信が発生する形態では必須の処理である。

処理 3：端末内データ破損時のパスワード DB の復旧

処理 1，2 だけでは、PC やスマートフォン等の端末の紛失・故障により端末内のデータが利用できない場合に、パスワード DB を参照できなくなるおそれがある。この場合、パスワード DB で管理している全サービスの個別パスワードを再設定する必要が生じ、ユーザにとって大きな負担となる。そこで、ユーザの端末とは別に用意した USB メモリやメモ帳等の「外部メモリ」に格納したデータとサーバに格納したデータを利用して端末内データを復元することで、パスワード DB を復旧できるようにする。

処理 4：マスターパスワードの忘却時のパスワード DB の復旧

処理 3 と同様に、処理 1，2 だけでは、ユーザがマスターパスワードを忘却した場合に、パスワード DB を参照できなくなるおそれがある。ユーザの端末と外部メモリを利用して忘却したマスターパスワードを復元することで、パスワード DB を復旧できるようにする。

処理 5：新しい端末の追加／失効

近年、PC とスマートフォンあるいは自宅 PC と職場 PC のように複数台の端末を利用するユーザが増加していることから、マルチデバイスへの対応を想定する。具体的には、既にパスワード管理方式に利用している端末（端末 1）を用いて新たな端末（端末 2）を追加することで、端末 2 でもパスワード DB を参照できるようにする[28]。端末 1 からパスワード DB を更新した場合には、端末 2 がパスワード DB を参照する際に、更新内容が反映されているようにする（パスワード DB の同期）。また、端末 2 を紛失した場合には、同端末からのパスワード DB の閲覧を防止するために端末 2 を失効させることが可能とする。

処理 6：マルチデバイス環境下でのマスターパスワードの更新

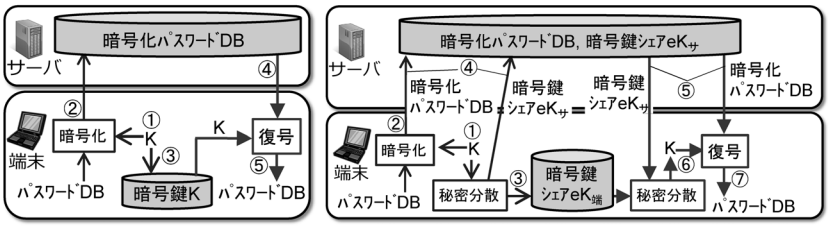
端末 1，2 を利用している状況において、端末 1 でマスターパスワードを更新することで、端末 2 にもマスターパスワードの更新が反映されるようにする。

(2) 処理 1：パスワード DB の暗号化／復号

脅威 1，2 に対して安全性要件 1，2 を満たしつつ、かつ、マスターパスワード変更時に各サービスの個別パスワードの変更を不要とするためには、パスワード DB

28 マルチデバイスを想定したサービス等では、登録済みの汎用端末を用いて新しい端末の追加処理を行う方法が採用されている（Grosse and Upadhyay [2013]）。

図表 7　処理 1 の実現方式



(a) 単純分散方式　　(b) 鍵分散方式

やその暗号鍵等を端末とサーバに分散して保存する必要がある。データを複数に分散する方法としては「秘密分散法[29]（Shamir [1979]）」や、それらを応用した分散オンラインストレージ等がある。以下では、これらの研究成果を踏まえつつ、前述の条件を満たすように一般化した 2 つの方式（それぞれ、「単純分散方式」、「鍵分散方式」と呼ぶ）を示す（図表 7）。

イ．実現方式

単純分散方式の暗号化処理では、まず、端末内でランダムに暗号鍵（K）を生成し（図表 7(a)-①）、この暗号鍵でパスワード DB を暗号化したうえでサーバに送信する（同②）。暗号鍵については、端末に格納する（同③）。復号処理では、サーバから暗号化パスワード DB を入手し（同④）、端末から読み出した暗号鍵で復号する（同⑤）。

また、鍵分散方式の暗号化処理では、単純分散方式と同様に、端末内で生成した暗号鍵（K）を用いてパスワード DB を暗号化する（図表 7(b)-①②）。さらに、暗号鍵を「秘密分散法」により 2 つの情報（以下、「暗号鍵シェア」と呼ぶ。それぞれ、（eK$_{端}$，eK$_{サ}$）に分割し、一方の暗号鍵シェア（eK$_{端}$）を端末に格納する（同③）。残りの暗号鍵シェア（eK$_{サ}$）と暗号化パスワード DB をサーバに送信する（同④）。復号処理では、サーバから暗号化パスワード DB と暗号鍵シェア（eK$_{サ}$）を入手する（同⑤）。このシェアと端末から読み出した暗号鍵シェア（eK$_{端}$）から秘密分散法により暗号鍵を復元し（同⑥）、暗号化パスワード DB を復号する（同⑦）。

上記の各方式の拡張として、マスターパスワードから生成した鍵で暗号鍵（単純

29 秘密情報（暗号鍵）を複数の情報（シェア）に分割する暗号化技術。通常、シェアから元の秘密情報を求めることは情報理論的に困難である。例えば、秘密情報「10」を「3」と「7」に分割した場合、「3」と「7」が揃えば「10」に復元できるが、「3」だけを入手しても「10」に復元することは困難である。

図表 8　処理 1 の実現方式の安全性評価

	単純分散方式	鍵分散方式
脅威 1（端末からの漏えい）	暗号化パスワード DB が漏えいしておらず、パスワード DB は盗取されない	
脅威 2（サーバからの漏えい）	暗号化パスワード DB からパスワード DB を求めることは計算量的に困難	
脅威 3（マスターパスワードの漏えい）	暗号鍵あるいは暗号化パスワード DB が漏えいしないため、パスワード DB は盗取されない	
脅威 4（外部からの漏えい）	外部メモリを使用しておらず、影響を受けない	
端末からの漏えい情報の無効化	新しい暗号鍵によるパスワード DB の暗号化し直しが必要	暗号鍵シェアの更新が必要（パスワード DB の暗号化し直しは不要）

分散方式の場合）や端末側の暗号鍵シェア（鍵分散方式の場合）を暗号化したうえで端末に格納する方法等がある。

ロ．安全性評価

脅威 1〜4 に対して、パスワード DB が漏えいするか否か（安全性要件 1）の観点から評価する（図表 8）。

脅威 1（端末からの漏えい）に対しては、どちらの方式も端末内にはパスワード DB に関する情報（暗号化パスワード DB 等）を格納していないため、パスワード DB は漏えいしない。また、脅威 2（サーバからの漏えい）に対しては、どちらの方式も暗号化パスワード DB が漏えいするものの、攻撃者は暗号鍵を入手できないため、パスワード DB は漏えいしない。なお、暗号鍵は十分に長い（128 ビット以上）とする。脅威 3（マスターパスワードの漏えい）や脅威 4（外部メモリからの漏えい）に対しては、どちらの方式も影響を受けないことは明らかである[30]。

本稿では検討対象外であるが、攻撃者が端末とサーバそれぞれに格納されている情報を入手した場合（脅威 1，2 の組合せに相当）、上記のいずれの方式においてもパスワード DB を盗取される。仮に端末から情報が漏えいした場合（脅威 1）、サーバから情報が漏えいする前に（脅威 2）、端末から漏えいした情報を無効化できれば、脅威 2 のみを想定した場合と同じ状況になるため、パスワード DB の漏えいを防止できる。端末から漏えいした情報の無効化という観点からみると、単純分散方式については暗号鍵が漏えいするが、新たに生成した暗号鍵でパスワード DB を暗

30 脅威 3 に対しては、どちらの方式もマスターパスワードを使用しておらず、影響を受けない。なお、前述したように、各方式の拡張として暗号鍵や暗号鍵シェアをマスターパスワードで保護する方式も考えられるが、暗号鍵や暗号化パスワード DB が漏えいしていないためやはり影響を受けない。脅威 4（外部メモリからの漏えい）に対しては、どちらの方式も外部メモリを使用しておらず、影響を受けない。

号化し直せばよい。鍵分散方式については、端末からの漏えいにより端末側の暗号鍵シェアが漏えいするが、サーバからサーバ側の暗号鍵シェアが漏えいする前に端末側とサーバ側の暗号鍵シェアを新たに生成して更新すれば[31]、その後、サーバからサーバ側の新しい暗号鍵シェアが漏えいしても暗号鍵の復元を防止できる。つまり、暗号鍵シェアの更新により漏えいした暗号鍵シェアを無効化可能であり、その際、パスワードDBを暗号化し直す必要はないという利点もある。

端末から漏えいした情報の無効化処理を行うタイミングについては、そもそも端末からの情報漏えいをユーザが検知できるのかという現実的な問題がある。例えば、端末を紛失した場合や、端末を一時的に他人に貸していた場合等の特殊なケースにおいては、脅威1の可能性を疑い、無効化処理を行うことが考えられる（紛失した場合には、後述の処理3の実施後に行う）。他方、いつもと変わりなく端末を利用している状況において、ある時点で脅威1の可能性を疑うことは難しく、この場合には、常に情報漏えいのリスクがあるという意識のもと、パスワードDBを参照するたびに毎回無効化処理を行うことが考えられる。

以上を踏まえ単純分散方式と鍵分散方式を比較すると、安全性の観点からはどちらも脅威1〜4に対して安全性要件1，2を満たしており、同程度の安全性といえる。他方、端末から漏えいした情報の無効化処理をみると、単純分散方式はパスワードDBを暗号化し直す必要があるのに対し、鍵分散方式は暗号鍵シェアの更新のみでよく、無効化処理に伴う負担が少なく、利便性に優れるといえる[32]。

(3) 処理2：端末とサーバ間の相互認証と鍵交換

意図した相手と安全に通信を行うためには、当事者間における相互認証と暗号通信用の鍵の交換を行う必要がある。これらの処理を行う暗号技術は、「認証鍵交換[33]」技術と呼ばれており、認証に公開鍵基盤（Public Key Infrastructure）を利用する鍵交換方式（Menezes, Qu, and Vanstone [1995]、ISO/IEC 9798-3）や、認証にパスワードを利用する鍵交換方式（「PAKE[34]」）等、さまざまな方式が提案・利用されている。以下では、インターネット・バンキングをはじめとするウェブサービスで

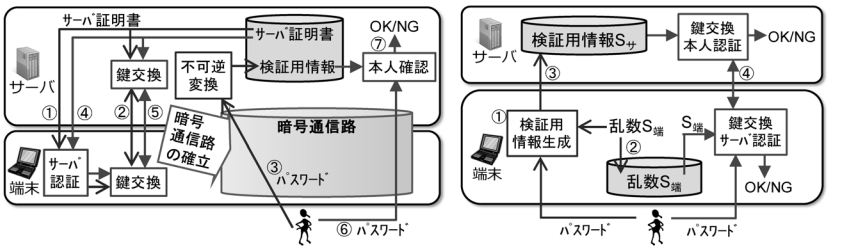
31 例えば、秘密情報「10」の2つのシェア「3」、「7」の一方（「3」）が漏えいした場合には、新たに「12」、「−2」等に分割したシェアを利用すれば、漏えいしたシェアを無効化できる。

32 例えば、14個のウェブサービスのID／パスワード（各8文字）を登録したパスワードDBは、1,800ビット程度（=8文字×8ビット×2（ID／パスワード）×14サービス）になるのに対し、暗号鍵が128ビットの場合、暗号鍵シェアは128ビットである。このことから、暗号鍵シェアの更新の方が、パスワードDBの暗号化し直しよりも負担が少ないことがわかる。

33 AKE：Authenticated Key Exchange。「認証鍵共有」、「認証付き鍵交換」等とも呼ばれる。

34 Password-based Authenticated Key Exchange（Bellovin and Merritt [1992]、ISO/IEC 11770-4等）。

図表 9　処理 2 の実現方式



(a) SSL パスワード混合方式　　(b) LR-AKE 方式

広く利用されている SSL/TLS[35] サーバ認証による鍵交換と（マスター）パスワード認証を組み合わせた方式（以下、「SSL パスワード混合方式」と呼ぶ）と、（マスター）パスワードのほかに端末に格納した乱数等を併用する 2 要素認証方式であり、かつ、他の既存方式よりも情報漏えいへの耐性が高い「LR-AKE[36] 方式（Shin, Kobara, and Imai [2008]）」を紹介する（図表 9）。そのうえで、LR-AKE 方式が安全性要件 2（マスターパスワードの漏えい耐性）を満たすのに対し、SSL パスワード混合方式は同要件を満たさないことを示す[37]。

イ．実現方式

ユーザ認証等のためにサーバに格納される情報を「検証用情報」と呼ぶことにする。同情報は、（マスター）パスワード等を不可逆変換することで算出される。処理 2（端末とサーバ間の相互認証と鍵交換）は、この検証用情報をサーバに登録する処理（以下、「登録処理」と呼ぶ）と、同検証用情報を用いて端末とサーバで暗号通信用の鍵を交換する処理（以下、「利用処理」と呼ぶ）からなる。

ここで想定する SSL パスワード混合方式は、多くのウェブサービスにみられるような以下の処理とする。登録処理では、端末は、サーバから入手したサーバ証明書によりサーバ認証を行い（図表 9(a)-①）、さらに、暗号通信用の鍵を交換することで、暗号通信路を確立する（同②）。そして、この暗号通信路を通じて、ユーザが入力したパスワードをサーバに送信し、サーバがこのパスワードから検証用情報

35 Secure Socket Layer、Transport Layer Security。最新版は TLS 1.2（Dierks and Rescorla [2008]）。

36 Leakage-Resilient Authenticated Key Exchange。

37 なお、SSL/TLS による鍵交換方式には SSL パスワード混合方式以外に、端末に格納した証明書（クライアント証明書）をユーザ認証に用いる「SSL/TLS 相互認証方式」も存在する。ただし、①同方式単体では脅威 1 に対して安全性要件 1 を満たさず、②クライアント証明書に対応する秘密鍵を（マスター）パスワードで暗号化する場合は脅威 1 に対して安全性要件 1，2 をともに満たさず、③（マスター）パスワード認証と組み合わせる場合は脅威 2 に対して安全性要件 2 を満たさないため、同方式の説明は割愛する。

を算出し、ストレージに格納する（同③）。利用処理では、登録処理と同様の手順で暗号通信路を確立し（同④⑤）、ユーザが入力したパスワードをサーバに送信する（同⑥）。サーバは、受信したパスワードとストレージから読み出した検証用情報を用いてユーザ認証を行う（同⑦）。

また、LR-AKE 方式の登録処理では、端末は、内部で生成した乱数（$S_{端}$）とユーザが入力したパスワードから検証用情報（$S_{サ}$）を算出する（図表 9(b)-①）。乱数を端末に格納し（同②）、検証用情報をサーバに登録する（同③）。なお、図表 9(b)-①～③の処理にはサーバ認証は含まれていないため、意図したサーバに検証用情報を登録することを保証するために、例えば、SSL パスワード混合方式のパスワード登録と同様に、サーバの公開鍵で同情報を暗号化したうえでサーバに送信してもよい。利用処理では、端末はストレージから読み出した乱数（$S_{端}$）とユーザが入力したパスワードを用いて、また、サーバはストレージから読み出した検証用情報（$S_{サ}$）を用いて、サーバ認証およびユーザ認証を行いつつ鍵交換を行う（同④）。なお、Shin, Kobara, and Imai [2008] では、端末やサーバからの情報漏えい（脅威 1，2）への対策として、サーバと暗号通信を行うたびに、検証用情報と乱数を更新する処理が必須とされている[38]。

ロ．安全性評価

脅威 1（端末からの漏えい）および脅威 2（サーバからの漏えい）に対する（マスター）パスワードの漏えいの有無（安全性要件 2）について評価する（図表 10）。

SSL パスワード混合方式は、端末にデータを格納しておらず、脅威 1 の影響を受けない。他方、脅威 2 を想定すると、漏えいした検証用情報に対するパスワードの全数探索攻撃によりパスワードを推定されるリスクがある。

図表 10　処理 2 の実現方式の安全性評価

	SSL パスワード混合方式	LR-AKE 方式
脅威 1（端末からの漏えい）	想定されない	乱数しか漏えいせず、マスターパスワードは漏えいしない
脅威 2（サーバからの漏えい）	検証用情報からマスターパスワードが漏えいするリスク	検証用情報からマスターパスワードを推定することは計算量的に困難
漏えい情報の無効化	マスターパスワードの更新が必要	ログイン時に毎回行われる乱数と検証用情報の更新により無効化される（マスターパスワードの更新は不要）

38 処理 1 の安全性評価でも述べたように、現実的には、端末からの情報漏えいを検知することは難しいと考えられる。このため、Shin, Kobara, and Imai [2008] のように、常に情報漏えいのリスクがあるという意識のもと、サーバと暗号通信を行うたびに更新するという方針もありうる。

LR-AKE 方式は、脅威 1 により乱数（$S_{端}$）が漏えいする。乱数にはパスワードに関する情報が含まれておらず、乱数からパスワードは漏えいしない。他方、この乱数を使って、パスワードを変えながらサーバに対して不正ログインの試行を繰り返し、サーバの反応（認証結果）を手掛かりにパスワードを推定する方法が想定される[39]。しかし、同攻撃によりパスワードを推定するには、最大 200 兆回程度の不正ログインの試行が必要であり、推定は現実的に困難といえる[40]。脅威 2 により検証用情報（$S_{サ}$）が漏えいするが、同情報の算出に利用する乱数を十分大きくすることで（例：128 ビット以上[41]）、同情報からパスワードを求めることが計算量的に困難になる。

漏えいした情報の無効化という観点からみると、SSL パスワード混合方式については、脅威 2 により検証用情報が漏えいすると、パスワードを更新し、それを改めて記憶する必要がある。LR-AKE 方式については、脅威 1 または脅威 2 により乱数（$S_{端}$）または検証用情報（$S_{サ}$）が漏えいするが、前述のとおり、これらの情報は端末とサーバが暗号通信を行うたびに毎回更新されるため、古い乱数と検証用情報は無効化される。また、パスワードは漏えいしないため更新不要である。

以上を踏まえると、SSL パスワード混合方式が脅威 1，2 に対してパスワードを漏えいするリスクがあるのに対し、LR-AKE 方式ではそうしたリスクがなく相対的に安全性が高いといえる。

（4） 処理 3，4：パスワード DB の復旧

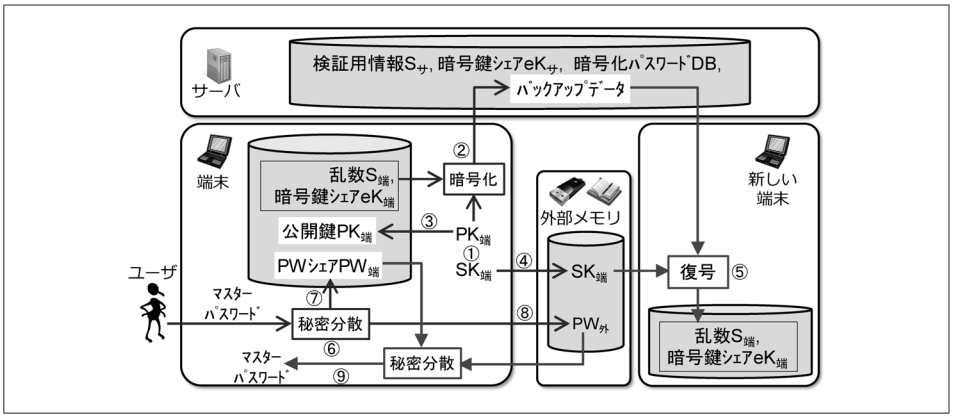
処理 3（端末内データの破損時の復旧）および処理 4（マスターパスワードの忘却時の復旧）は、処理 1，2 の任意の実現方式と組み合わせることが可能であるが、処理 3，4 の実現方式をより具体化するために、処理 1，2 の特定の実現方式に固有のパラメータを用いて説明する。具体的には、前述した処理 1，2 の各実現方式のうち安全性が相対的に高いもの、あるいは、安全性が同程度の場合には利便性の高いものを想定する。つまり、処理 1 の実現方式として鍵分散方式、処理 2 の実現方式として LR-AKE 方式を想定した場合の処理を示す（図表 11）。この想定下で

39 サーバの反応を手掛かりにパスワードを探索する攻撃は「オンライン攻撃」と呼ばれる。他方、SSL パスワード混合方式に対する脅威 2 のように、入手した情報（検証用情報）を攻撃者の手元で解析する攻撃は「オフライン攻撃」と呼ばれる。

40 パスワードが 8 文字の英数字（62 種類）の場合、候補が約 200 兆個（$= 62^8$）存在する。こうした攻撃（オンライン攻撃）に対しては、1 回の試行に要する時間を長くする、ログインが連続して失敗した場合にはアカウントをロックする等の対策が知られている（総務省［2013］）。

41 3 節（4）で述べたように、情報量が 60 ビット程度の場合には解読可能であることが実証されている。安全性を確保するには解読可能な情報量より大きくする必要があり、現在は、情報量として 128 ビット以上を要求することが一般的である。

図表 11　処理 3，4 の実現方式



は、端末には「乱数 $S_{端}$、暗号鍵シェア $eK_{端}$」が格納され、サーバには「検証用情報 $S_{サ}$、暗号鍵シェア $eK_{サ}$、暗号化パスワード DB」が格納されている。処理 3 については、松中らが提案した公開鍵暗号方式を用いる復旧方式をパスワード管理方式に適用した場合の実現方式を示す（松中・蕨野・杉山［2007］）。また、処理 4 については、秘密分散法を利用した実現方式を示す[42]（Shamir [1979]）。

イ．実現方式

処理 3，4 はそれぞれ、データ破損やマスターパスワード忘却といった障害の発生に備えた「バックアップ処理」と、障害発生時に破損したデータやマスターパスワードを復旧する「復旧処理」からなる。処理 3 のバックアップ処理では、まず、端末において、公開鍵（$PK_{端}$）／秘密鍵（$SK_{端}$）を生成し（図表 11-①）、端末内のデータ（乱数 $S_{端}$、暗号鍵シェア $eK_{端}$）をこの公開鍵で暗号化したもの（以下、「バックアップデータ」と呼ぶ）をサーバに格納する（同②）。公開鍵は端末に、秘密鍵は外部メモリにそれぞれ格納する（同③④）。なお、公開鍵のバックアップは不要である。その後、端末が故障した場合には、新しい端末を用いて復旧処理を行う。具体的には、サーバから入手したバックアップデータを外部メモリから読み出した秘密鍵で復号することで、端末内データを入手する（同⑤）。なお、処理 1，2

42 平野・森井［2011］においても、マスターパスワードの復旧方式が提案されている。具体的には、マスターパスワードを秘密分散法により複数の PW シェアに分割し、各 PW シェアをそれぞれ異なる「秘密の質問への回答」を使って保護したうえで端末に保存するという方式である。秘密の質問による保護については、安全性は高くないとの実験結果が報告されていることに加え（Schechter, Brush, and Egelman [2009]）、平野らの方式では、脅威 1（端末からの漏えい）により保護された PW シェアが漏えいするため、攻撃者が全数探索攻撃や辞書攻撃によりマスターパスワードを復旧できる可能性がある。

の実現方式で示したように、端末に格納された暗号鍵シェアや乱数は適宜更新されるため、更新のたびに公開鍵を用いてバックアップデータを生成し、サーバに送信する必要がある。サーバは、受信した新しいバックアップデータを格納し、古いものを削除する[43]。

処理4のバックアップ処理では、端末において、秘密分散法によりマスターパスワードを2つのシェア（以下、「PWシェア」と呼ぶ。それぞれ、$PW_{端}$、$PW_{外}$）に分割する（同⑥）。一方のPWシェアは端末に、他方のPWシェアは外部メモリにそれぞれ格納する（同⑦⑧）。復旧処理では、端末および外部メモリから読み出した各PWシェアから秘密分散法によりマスターパスワードを復旧する（同⑨）。なお、理由は後述するが、端末に格納したPWシェアは、処理3のバックアップ処理（同②）の対象には含めない。このほか、マスターパスワードを更新した場合は、更新前のマスターパスワードと端末側のPWシェアから、端末側の新しいPWシェアを生成すればよく、外部メモリ側のPWシェアを更新する必要はない[44]。

処理3，4では、バックアップ処理で一度外部メモリにデータ（秘密鍵、PWシェア）を格納すれば、復旧処理以外では外部メモリを使用しないため、パスワード管理方式の利便性を損ねないといえる。

ロ．安全性評価

脅威4（外部メモリからの漏えい）により、パスワードDBやマスターパスワードが漏えいするか否か（安全性要件1，2）を分析する（図表12）。

脅威4により、攻撃者は秘密鍵（$SK_{端}$）と外部メモリ側のPWシェア（$PW_{外}$）を盗取する。攻撃者は、秘密鍵を用いて処理3の復旧作業を行うことで、端末内データ（暗号鍵シェア $eK_{端}$、乱数 $S_{端}$）を入手できる（このデータには、端末側のPWシェアは含まれない[45]）。しかし、処理1，2の実現方式について議論したとおり、

43 処理3については、LR-AKE方式の拡張により対応する方法も提案されている（恩田ほか［2011］、Shin, Kobara, and Imai [2011]）。1つは、1台の端末のほかに2台のサーバを用いることで、1台が利用できなくなっても残りの2台からデータを復旧するという方法（LR-AKEクラスターモード）である。もう1つは、LR-AKE方式を利用して、パスワードDBを別途バックアップしておくという方法である（LR-AKEバックアップ処理）。なお、同方法は、パスワードDBを更新するたびにバックアップし直す必要がある。

44「マスターパスワード（PW_M）＝端末側PWシェア（$PW_{端}$）＋外部メモリ側PWシェア（$PW_{外}$）」かつ「新しいマスターパスワード（PW'_M）＝新しい端末側PWシェア（$PW'_{端}$）＋新しい外部メモリ側PWシェア（$PW'_{外}$）」であるとする。このとき、$PW_{外}$ と $PW'_{外}$ が同じであるとすると、$PW'_{端}$ は、「$PW'_{端} = PW'_M - PW_M + PW_{端}$」により求まる。

45 仮にバックアップデータに端末側のPWシェアが含まれる場合、脅威4（秘密鍵、外部メモリ側PWシェアの漏えい）を想定すると、まず、攻撃者は、入手した秘密鍵を用いて処理3の復旧処理を行い、端末内のデータ（暗号鍵シェア、乱数、端末側PWシェア）を入手する。ここで、2つのPWシェアが揃うため、攻撃者はマスターパスワードを復旧し、さらに、乱数や暗号鍵シェアも利用して正規ユーザになりすましてサーバと通信を行い、パスワードDBを入手できる。

図表 12　処理 3，4 の実現方式の安全性評価

	処理 3（端末内データ破損時の復旧）の実現方式	処理 4（マスターパスワード忘却時の復旧）の実現方式
脅威 4（外部メモリからの漏えい）	端末側の暗号鍵シェアや乱数を入手できるが、これらの情報からは、パスワード DB やマスターパスワードは漏えいしない。	PW シェアが揃わないため、マスターパスワードは漏えいしない。
外部メモリからの漏えい情報の無効化	サーバのバックアップデータを、新たに生成した公開鍵を用いて作成したバックアップデータに置き換える必要がある。	端末用の古い PW シェアを削除し、マスターパスワードから新たに PW シェア（外部メモリ用、端末用）を生成する必要がある。

暗号鍵シェアや乱数が漏えいしても、パスワード DB やマスターパスワードは漏えいしない。また、攻撃者は、外部メモリ側の PW シェアを入手しているものの、処理 4 によるマスターパスワードの復旧処理を行うために必要な端末側の PW シェアを入手していないため、マスターパスワードを求めることは困難である。

漏えいした情報の無効化という観点からみると、処理 3 の実現方式に関しては、端末が新しい公開鍵／秘密鍵を生成し、同公開鍵でバックアップデータを作成し、サーバに送信すればよい。サーバは受信した新しいバックアップデータを格納し、古いものを削除する。新しい公開鍵は端末のストレージに、新しい秘密鍵は新しい外部メモリに格納する。処理 4 の実現方式に関しては、端末内に格納された古い PW シェアを削除したうえで、マスターパスワードを新しい PW シェアに分割し、一方を端末に、他方を新しい外部メモリに格納すればよい。なお、マスターパスワードの更新では、外部メモリ側の PW シェアが漏えいしていないため、同シェアを更新する必要がない点が漏えい情報の無効化処理と異なる。

5.　考察

パスワードリスト攻撃に対しては、他にも運用上の工夫等を行うことによってリスクを軽減することも考えられる。本節では、サービス固有の情報から個別パスワードを生成する方法、ID 等の設定方針によりパスワードリスト攻撃を回避する方法について、その有効性や留意点に関して述べる。また、パスワード管理ツールに類似した機能を持つサービスとして、アカウント・アグリゲーション・サービスを取り上げて考察する。

(1) サービス固有の情報から個別パスワードを生成する方法

本稿では、ランダムに生成した個別パスワードをデータベースで管理する方法（以下、「データベース方式」と呼ぶ）を想定したが、このほかに、各サービスのURLといったサービス固有の公開情報とマスターパスワードから個別パスワードを生成する方法（以下、「公開情報利用方式」と呼ぶ）も知られている[46]（平野・森井［2011］）。同方式では、秘密の情報を端末等に別途格納する必要がなく、利便性が高いようにみえる。しかし、あるサービスの個別パスワードが漏えいした状況を想定すると、同方式に固有のリスクがあることや、個別パスワードの更新に手間が掛かることがわかる。

まず、同方式の固有リスクを説明する。攻撃者が、当該サービスの固有パスワードを入手した場合、同サービスのURLと組み合わせることで、全数探索攻撃によりマスターパスワードを求められるリスクがある。マスターパスワードが求められた場合には、別のサービスの個別パスワードも漏えいする[47]。

漏えいした個別パスワードを更新するには、2つの方法が考えられる。1つは、マスターパスワードを更新する方法である。この場合、利用しているその他の全サービスの個別パスワードも更新することになる。各サービスにおける個別パスワードの更新作業は、通常、ユーザが手作業で行うため、利用しているサービスの数が多いほど、個別パスワードの更新作業は大きな負担となる[48]。もう1つは、マスターパスワードは更新せず、当該サービスの個別パスワードだけを更新する方法である。例えば、サービスごとに乱数やカウンタ等を設定し、URL、乱数等、マスターパスワードから個別パスワードを生成するようにすればよい。しかし、同方法では、サービスごとの乱数等をデータベースとして端末等に格納する必要があり、データベース方式と本質的に変わらないと考えられる。

46 パスワードを生成する方法には、URL等の公開情報を用いる方法（公開情報利用方式）のほかに、ユーザが生成する方法、サービス提供者が指定する方法、ソフトウエア等を利用して機械的に生成する方法等がある。

47 このほか、サービスのURLが変更された場合、同サービスの個別パスワードが生成できなくなるリスクも指摘されている（平野・森井［2011］）。

48 個別パスワードの更新を目的としていなくとも、何らかの理由によりマスターパスワードの更新を行った場合にも、すべてのサービスの個別パスワードの更新が必要となる。こうした更新作業の負担を減らすには、例えば、パスワード管理ツールを使うことで、各ウェブサービスの個別パスワードを自動更新できる機能があるとよい。同機能があれば、パスワードの定期更新を自動化することも可能になる。社内向けではあるが同機能を実装した製品が存在する。

(2) ID 等の設定方針によりパスワードリスト攻撃を回避する方法

パスワードリスト攻撃に対しては、2 要素認証を行うことが望ましいが、前述のとおり直ぐに利用できるとは限らない。そこで、個別 ID や個別パスワードの設定方針を工夫することでパスワードリスト攻撃を回避する方法について考察する。多くのサービスでは、ユーザが個別 ID ／個別パスワードを選択できる。ユーザが記憶する個別 ID や個別パスワードの数を極力減らしつつ、パスワードリスト攻撃に耐性を持たせるためには、例えば、個別 ID を使い回すことは許容する一方、個別パスワードはサービスごとに確実に変えればよい。しかし、実際には個別 ID ／個別パスワードを使い回すユーザが多く、不正ログインにつながっているのが実情である。

他方、インターネット・バンキングのように、サービス提供者が個別 ID を指定するという方針もみられる[49]。この場合、ユーザが同サービスで指定された ID をわざわざ他のサービスで使い回すことはないことが期待されるため、同サービス以外から個別 ID ／個別パスワードが漏えいしても、同サービスへの不正ログインを防止できる。しかし、電子メール等のように、個別 ID をログインだけでなく、ユーザ間のメッセージのやり取り等にも利用するサービスにおいては、ID の文字列自体に意味を持たせることが多く、サービス提供者が一方的に個別 ID を指定することは難しい[50]。また、既に発行された個別 ID を変更するには別ユーザとして登録し直す必要がある等、実質的に個別 ID を変更できないサービスも多い[51]。

このほかにも、個別 ID をユーザに選択させる代わりに、個別パスワードを使い回せないようにするという方針が考えられる。単純には、サービス提供者が各ユーザの個別パスワードを指定し、ユーザによる任意のパスワードへの更新を禁止とすればよい。ただし、この方法では、仮に不正ログインが発生した場合に、サービス提供者も個別パスワードの漏えい元として疑われる可能性がある。そこで、個別パスワードの一部（例：先頭 4 文字）をサービス提供者がランダムに指定し（以下、「SP 指定部」と呼ぶ）、残り（以下、「ユーザ指定部」と呼ぶ）をユーザが選択するという方法が考えられる。他のサービス提供者もこの方法を採用している場

49 ただし、サービス提供者が個別 ID を指定することにより利便性が低下するため、サービス提供者によっては、ユーザが別途個別 ID を設定することを許可している。この場合、パスワードリスト攻撃のリスクが生じる。

50 1 つのメールアドレスを複数のサービス（例：srv1，srv2）で使い分ける方法も存在する。例えば、Google 社の Gmail では、1 つのメールアドレス（例：○○@gmail.com）に対して任意の別名アドレス（エイリアス。例：○○+srv1@gmail.com、○○+srv2@gmail.com）を作成できる。

51 サービス提供に利用するユーザ ID とは別にログイン専用に用いる ID（個別 ID に相当）を設定可能なサービスも存在する。例えば、Yahoo! JAPAN 社では、ユーザ ID（Yahoo! JAPAN ID）とは別にログイン専用の ID（シークレット ID）を設定可能である。同社のユーザ ID は変更できないものの、シークレット ID は、適宜更新可能である。

合、ユーザはユーザ指定部を使い回す可能性があるものの、SP 指定部については各サービスに固有であるため使い回すことができない。そのため、あるサービスからユーザ指定部が漏えいしたとしても、パスワードリスト攻撃を無力化できると期待される[52]。

(3) アカウント・アグリゲーション・サービスに関する留意点

パスワード管理技術と同種の技術を背景とした「アカウント・アグリゲーション・サービス」（以下、「口座情報集約サービス」と呼ぶ）が、近年注目されている[53]。同サービスがパスワード管理技術と技術的に同じであることに加え、同サービスが対象とする口座情報が主にインターネット・バンキング等であることから、同サービスに関する留意点について考察を行う。

イ. 口座情報集約サービスの概要

口座情報集約サービスは、ユーザが予め、自分の複数の金融機関の口座情報等を同サービスに登録しておくことで、同サービスがユーザに代わって各口座から利用履歴や残高を入手し、集約した情報をユーザに提供するというサービスである（図表 13）。特に、スマートフォンの普及とともに、同サービスの実現に専用サーバ（以下、「集約サーバ」と呼ぶ）を用いる形態が広まりつつあり、同形態における国内ユーザは 120 万人を超えている（日本経済新聞［2013］）。

同サービスでは、各口座へのログインに必要な情報（ID、パスワード等）を同サービスに登録する必要があるため[54]、パスワード管理技術と同種の技術であるといえる。また、同サービスに情報収集を行わせるだけでなく、同サービスを使って各口座（ウェブサービス）へログインする機能も一部では提供されており、パスワード管理技術として利用されることもある。同サービスについては、ユーザにとって、ひとつひとつ自分で各ウェブサーバにログインして情報収集する必要がないというメリットがある反面、第三者である口座情報集約サービスにユーザ自身がパスワード等を漏えいしているという見方もできる[55]。

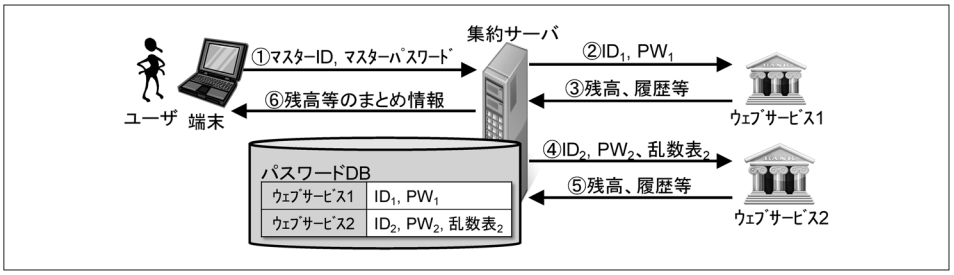
52 ユーザ指定部が既知の場合、ランダムに生成した SP 指定部と組み合わせて不正ログインの試行を繰り返す攻撃が想定される。同攻撃により不正ログインが成立するには最大 148 万回（$= 62^4$。英数字 4 文字の場合）の試行が必要であり、サービス提供者がリアルタイムに同攻撃を検知・防止できると考えられる。

53 こうした背景には、スマートフォンの普及とともに、スマートフォンから利用可能な口座情報集約サービスが複数登場してきたことが挙げられる。

54 現行サービスの詳細は非公開であるが、口座に入金・出金があれば同サービスが自動で通知する機能もあることから、集約サーバが個別パスワード等を利用可能な状態にあると推測される。

55 口座情報集約サービスの利用規約等には、通常、同サービスの利用によってユーザが被害を受けたと

図表 13　アカウント・アグリゲーション・サービス



備考：ユーザは、予めウェブサービス 1，2 のログインに必要な情報（個別 ID 等）を集約サーバに登録しておく。ユーザがマスター ID ／マスターパスワードを用いて同サーバにログインすると（①）、同サーバがユーザに代わって各ウェブサービスにログインし、残高等の情報を入手する（②～⑤）。そして、同サーバは、それらの情報を集約してユーザに渡す（⑥）。なお、ユーザが集約サーバにログイン（①）を行わなくとも、定期的に情報収集を行い（②～⑤）、新着情報等をユーザに伝える（⑥）サービスも存在する。

ロ．口座情報集約サービスの潜在的リスクと 3 つの対策

口座情報集約サービスの安全性に関しては、本稿で議論したように、サーバへの不正アクセスやサーバ管理者の不正によりサーバから情報（平文のパスワード DB）が漏えいするリスク（脅威 2）を想定した場合、各ウェブサービスへの不正ログインのリスクがある。また、ログインに乱数表を併用する一部のインターネット・バンキングについては、「乱数表の全マス」を同サーバに預ける必要があるため、脅威 2 による不正送金のリスクもある。こうしたリスクを軽減するために、同サービスの提供者自身が適切に情報漏えい対策を講じることは言うまでもないが、このほかにも以下のいずれかの対策（対策 1～3）を検討することが望ましい。

対策 1 は、脅威 2 が顕現化したとしてもインターネット・バンキングの不正送金だけは防止するという目的のもと、金融機関が行う対策である。具体的には、資金移動等の取引時のセキュリティレベルをログイン時よりも高くするという対策である。例えば、ログイン時にパスワード認証を行い、取引時には 2 要素認証を行うといった設定や、ログイン時に 2 要素認証を行い、取引時に取引認証を行うといった設定が考えられる。

対策 2 は、脅威 2 が顕現化したとしても各ウェブサービスへの不正ログインを防止するという目的のもと、口座情報集約サービスの提供者が行う対策である。具体的には、本稿で示したハイブリッド型のパスワード管理方式のように、集約サーバがユーザからパスワード DB を平文のまま預からない形態を採用するという対策で

しても、事由のいかんを問わず、同サービスの提供者は責任を負わないものとすることが明記されている。

ある。ただし、同対策では、ユーザが集約サーバにログインしないと各ウェブサービスから情報を収集できないという制約が発生する。

対策 3 も、対策 2 と同様に、脅威 2 に基づく各ウェブサービスへの不正ログインを防止するという目的のもと、口座情報集約サービスの提供者と各ウェブサービスの提供者が協力して行う対策である。具体的には、集約サーバがユーザ本人として各ウェブサービスに「ログイン」するのではなく、ユーザの口座情報を「参照する権限」等を同サーバに付与する技術（「代理アクセス技術」等と呼ばれる。例：OAuth〈Hardt [2012]〉、OpenID Connect〈Sakimura *et al.* [2014]〉）を採用するという対策である。同対策を採用した場合、ユーザが集約サーバにログインしてない状態でも各ウェブサービスから情報収集が可能となる。

6. おわりに

パスワードは、ユーザ本人や他社サービスといった自社の管理範囲外から漏えいする可能性があり、パスワード以外の認証要素を利用したユーザ認証に移行すべきといった指摘がある（Narcisi [2013]）。しかし、ビジネス判断として 2 要素認証を採用しないサービスや、2 要素認証の 1 要素としてパスワードを利用するサービス等が存在することや、使い勝手の良さからパスワードが長年使われてきたこと等を考慮すると、当面はパスワードの利用が続くと予想されるため、パスワードを少しでも安全に使っていく取組みが重要になる。

パスワード管理についてみると、強度の高いパスワードを 1 つ生成することは、パスワード生成時にユーザが入力したパスワードの強度を可視化するツール（パスワードチェッカー）等が普及してきたほか、具体的な生成方法[56] が多くの場所で紹介されるようになり、ユーザにとってハードルが低くなってきている。しかし、パスワードの使い回し防止に関しては、そうした呼び掛けや「紙に書いてはいけない」等の注意事項が示される一方で、複数のパスワードを使い分ける方法は明示されないことが多い。その結果、パスワードを使い分けるための実践方法がわからないユーザが、仕方なくパスワードを使い回しているのが実情と考えられる[57]。こうした状況を打開するには、パスワードの使い回し防止のために、専門家・ユーザ・

56 例えば、「I am a Student」等の英文を作成し、このうち何文字かを別の文字や記号に置換したもの（例：1am@$tuDent）をパスワードとする方法や、自作した乱数表の縦や横に並んだマスに書かれた文字をパスワードとする方法（内田［2005］）等がある。

57 IPA［2013］に「覚え切れないパスワードを実際にどうしたらいいか分からない利用者も多いのではないでしょうか」との記述があるほか、辻［2014］にも「その状況（パスワードリスト攻撃による被害）がなかなか無くならない理由の 1 つは、幾つかの「鉄則」を示すのみで、その実施方法が示されないことで、結果として無理難題となっている」との記述がある（括弧は著者注）。

サービス提供者等の間でオープンに議論することが重要である。例えば、こうした対策の1つであるパスワード管理ツールについては、求められる安全性要件や脅威を議論したり、ユーザが信頼できるツールを入手するための枠組み（第三者による評価、ツールの配付方法等）についても検討することが有用であろう。これに加えて、パスワード管理ツール以外の対策についても利用の可否や推奨される利用方法等を検討しながら、関係者のコンセンサスを醸成し、現実的で有効な対策を広めていくことが有用だと考えられる[58]。

58 このほか、ユーザのパスワード管理意識を高めることも有用である。例えば、ユーザのアカウントに対して（第三者が）ログインを試行して失敗に終わった場合に、その後、ユーザ本人がログインした際にログインの失敗があった旨を通知することで、ユーザにアカウントが狙われているという危機意識を持たせられると期待される。こうした通知を行う製品（例：PCのハードウエア全体の暗号化を行う製品〈NEC Pointsec〉）も存在する。

参考文献

内田勝也、「固定パスワード（Reusable Password）再考」、『情報処理学会全国大会講演論文集』第 67 巻第 4 号、2005 年、345〜346 頁

梅澤克之・加藤崇利・田代　卓、「認証済み Cookie 情報の端末間での連携技術の開発と評価」、コンピュータセキュリティシンポジウム、D1-3、2009 年

恩田泰則・辛　星漢・古原和邦・今井秀樹、「クラウド環境に適したオンラインデータ分散管理方式」、暗号と情報セキュリティシンポジウム、3F2-3、2011 年

勝村幸博、「足利銀行のネットバンクに 15 件の不正ログイン、不正送金は確認されず」、IT Pro by 日経コンピュータ、2014 年 4 月 7 日

金融情報システムセンター（FISC）、『金融機関等コンピュータシステムの安全対策基準・解説書（第 8 版追補）』、FISC、2013 年

国家公安委員会・総務大臣・経済産業大臣、「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」、2014 年

サイトウイサム・加藤秀行、「ネットバンキングで不正アクセスが増加　銀行側もさまざまなセキュリティ対策を実施」、MONEYzine、2014 年 5 月 18 日

シマンテック、「「個人・企業のパスワード管理」に関する意識調査結果のご報告」、2013 年

情報処理推進機構（IPA）、「「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〜」、今月の呼びかけ、2013 年 8 月

————、「「オンライン本人認証方式の実態調査」報告書」、2014 年 8 月

情報通信研究機構（NICT）・情報処理推進機構（IPA）、「暗号方式委員会報告」、『CRYPTREC Report 2011』、2012 年

鈴木雅貴・中山靖司・古原和邦、「インターネット・バンキングに対する Man-in-the-Browser 攻撃への対策「取引認証」の安全性評価」、『金融研究』第 32 巻第 3 号、2013 年、51〜76 頁

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」、総務省、2013 年 12 月

————・経済産業省、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」、2013 年 3 月 1 日

辻　伸弘、「See new world―振り返るとセキュリティ・ダークナイトはいるよ（前編）―」、Atmark IT、2014 年 3 月 28 日

徳丸　浩、「ハッシュとソルト、ストレッチングを正しく理解する―本当は怖いパスワードの話―」、Atmark IT、2011 年 10 月 6 日

トレンドマイクロ、「Web サイトのパスワード利用実態調査」、2012 年 12 月 14 日

————、「パスワードの利用実態調査 2014」、2014 年 6 月 12 日

内閣官房情報セキュリティセンター（NISC）、「政府機関の情報システムにおいて使用される暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」、2008 年
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）」、日本経済新聞 電子版、2013 年 3 月 4 日
日本経済新聞、「国内でネット家計管理広がる　自動家計簿など、スマホ追い風」、日本経済新聞 電子版、2013 年 8 月 25 日
――――、「不正ログイン被害 68 万件　使い回しパスワード標的」、日本経済新聞 Web 刊、2014 年 2 月 24 日
野村総合研究所、「利用者登録する商品・サービスを選別する傾向が強まった生活者と顧客情報の鮮度維持を望む事業者～生活者と事業者を対象とした ID に関する実態調査～」、News Release、2012 年 2 月 8 日
平野　亮・森井昌克、「パスワード運用管理に関する考察および提案とその開発」、『電子情報通信学会技術研究報告　ライフインテリジェンスとオフィス情報システム』vol. 111 no. 286、2011 年、129～134 頁
富士通、「いつも同じだと危険！複数のパスワードを管理する 5 つの心得」、パソコン活用クローズアップ！、2013 年 7 月 31 日
松中隆志・蕨野貴之・杉山敬三、「携帯端末におけるデータ保護手法の提案と実装」、暗号と情報セキュリティシンポジウム（SCIS）、4B2-3、2007 年
森川郁也・下山武司、「暗号等価安全性」、『電子情報通信学会誌』vol. 94、2011 年、987～992 頁
リサーチバンク、「パスワード管理と認証に関する調査。ID&PW の管理、男性は「記憶」女性は「紙にメモ」。」、2014 年
Narcisi, Gina、「数年でパスワードのない世界に―PayPal 幹部が認証変革―」、ITmedia、2013 年 6 月 10 日
Barker, Elanie, William Barker, William Burr, William Polk, and Miles Smid, “Recommendation for Key Management―Part 1: General (Revision 3),” National Institute of Standards and Technology (NIST) Special Publication 800–57, 2012.
Belenko, Andrey, and Dmitry Sklyarov, ““Secure Password Managers” and “Military-Grade Encryption” on Smartphones: Oh, Really?,” Black Hat Europe, 2012.
Bellovin, Steven M., and Michael Merritt, “Encrypted Key Exchange: Password-based Protocols Secure against Dictionary Attacks,” IEEE Computer Society Symposium on Research in Security and Privacy, 1992, pp. 72–84.
Bhargavan, Karthikeyan, and Antonie Delignat-Lavaud, “Web-based Attacks on Host-Proof Encrypted Storage,” USENIX Workshop on Offensive Technologies (WOOT), 2012.
Bonneau, Joseph, Cormac Herley, Paul C. van Oorshot, and Frank Stajano “The Quest to

Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," IEEE Symposium on Security and Privacy, 2012, pp. 553–567.

Burr, William E., Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus, "Electronic Authentication Guideline," NIST Special Publication 800-63-2, 2013.

Dierks, Tim, and Eric Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," Internet Engineering Task Force (IETF), RFC 5246, 2008.

Ducklin, Paul, "Anatomy of a password disaster—Adobe's giant-sized cryptographic blunder," Naked Security, November 4, 2013.

Grosse, Eric, and Mayank Upadhyay, "Authentication at Scale," IEEE Security and Privacy, vol. 11, issue. 1, 2013, pp. 15–22.

Hardt, Dick, "The OAuth 2.0 Authorization Framework," IETF, RFC 6749, 2012.

Information Technology at Purdue (ITaP), "Password Manager Software," Purdue University, 2008.

International Organization for Standardization (ISO) and The International Electrotechnical Commission (IEC), "ISO/IEC 9798-3: Information Technology—Security Techniques—Entity Authentication—Part 3: Mechanisms Using Digital Signature Techniques," ISO, 1998.

———, and ———, "ISO/IEC 11770-4: Information Technology—Security Techniques—Key Management—Part 4: Mechanisms based on Weak Secrets," ISO, 2006.

Kaliski, Burton, "PKCS #5: Password-Based Cryptography Specification Version 2.0," IETF, RFC 2898, 2000.

Karole, Ambarish, Nitesh Saxena, and Nicolas Christin, "A Comparative Usability Evaluation of Traditional Password Managers," International Conference on Information Security and Cryptography (ICISC), 2010, pp. 233–251.

Kleinjung, Thorsten, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman J. J. te Riele, Andrey Timofeev, and Paul Zimmermann, "Factorization of a 768-bit RSA Modulus," *CRYPTO, Lecture Notes in Computer Science (LNCS)*, vol. 6223, 2010, pp. 333–350.

McCarney, Daniel, "Password Managers: Comparative Evaluation, Design, Implementation and Empirical Analysis," Carleton University, 2013.

Menezes, Alfred, Minghua Qu, and Scott Vanstone, "Some New Key Agreement Protocols Providing Mutual Implicit Authentication," Workshop on Selected Areas in Cryptography (SAC), 1995, pp. 22–32.

Neuman, Clifford, Tom Yu, Sam Hartman, and Kenneth Raeburn "The Kerberos Network Authentication Service (V5)," IETF, RFC 4120, 2005.

OpenID Foundation, "OpenID Authentication 2.0—Final," 2007.

Organization for the Advancement of Structured Information Standards (OASIS), "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS Standard, 2005.

Sakimura, Natsuhiko, John Bradley, Michael Jones, Breno de Medeiros, and Chuck Mortimore, "OpenID Connect Core 1.0," OpenID Foundation, 2014.

Schechter, Stuart, A. J. Bernheim Brush, and Serge Egelman, "It's No Secret: Measuring the Security and Reliability of Authentication via 'Secret' Questions," IEEE Symposium on Security and Privacy, 2009, pp. 375–390.

Shamir, Adi, "How to Share a Secret," Communications of the ACM, vol. 2 no. 11, 1979.

Shin, SeongHan, Kazukuni Kobara, and Hideki Imai, "Secure PAKE/LR-AKE Protocols against Key-Compromise Impersonation Attacks," Symposium on Information Theory and its Applications (SITA), 2008, pp. 965–970.

———, ———, and ———, "A Secure Public Cloud Storage System," IEEE Internet Technology and Secured Transactions, 2011, pp. 103–109.

The Association of Banks in Singapore (ABS), "The Association of Banks in Singapore Announces Measures to Enhance the Security of ATM Cash Withdrawals and Card Payment Infrastructure," Media Release, 2012.

Weir, Matt, Sudhir Aggarwal, Michael Collins, and Henry Stern, "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords," ACM Conference on Computer and Communications Security (CCS), 2010, pp. 162–175.

補論 1.　パスワード管理に関するユーザの実態

パスワード管理に関するユーザのアンケート結果が公表されている。各結果をまとめると図表 A-1 のとおりである。

図表 A-1　パスワード管理に関するユーザの実態

		トレンドマイクロ［2012］	トレンドマイクロ［2014］	リサーチバンク［2014］	シマンテック［2013］	野村総合研究所［2012］
1 ユーザが利用するウェブサービスのうち、「パスワード認証」を行うサービスの数	1〜4 個	平均 14	—	—	26%	平均 19
	5〜9 個				29%	
	10〜19 個				24%	
	20 個以上				10%	
	把握せず				11%	
自分が記憶できるパスワードの個数	0 個	—	—	—	6%	平均 3
	1 個				12%	
	2〜3 個				52%	
	4〜5 個				19%	
	6 個以上				11%	
全サービスで使用するパスワードの個数	1 個	14%	16%	16%	15%	—
	2〜3 個	55%	56%	50%	47%	
	4〜5 個	17%	12%	21%（4 個以上）	8%（4 個以上）	
	6 個以上	5%	9%			
	全て異なる	8%	7%	13%	29%	
パスワードに利用する文字種 (*1)	1 種類	13%	—	11%	—	—
	2 種類	67%		74%		
	3 種類	14%		15%（3 種類以上）		
	4 種類	7%				
パスワードの文字数	4〜5 文字	2%	—	2%	—	—
	6〜7 文字	24%		23%		
	8〜9 文字	55%		56%		
	10〜15 文字	17%		17%		
	16 文字以上	2%		3%		
パスワードの管理方法 (*2)	記憶する	44%	37%	41%	56%	—
	紙にメモ	35%	44%	41%	36%	
	ファイルで PC 等に保存	23% (*3)	33% (*4)	22%	17%	
	ウェブブラウザに保存	5%	6%	19%	9%	
	パスワード管理ツール（専用ツール／サービス）	3%	4%	5%	7%	
	メールで保存	6%	5%	—	3%	

備考：パスワード認証とは、ID ／パスワードのみ行われるユーザ認証を指す。小数点以下は四捨五入した。回答が複数種類ある項目については、最も多い回答の背景を色塗りした。パスワード認証に関するサービス提供者へのヒアリングやユーザへのアンケートの結果は、IPA［2014］でも報告されている。*1：文字種とは、アルファベットの「大文字」・「小文字」、「数字」、「記号／特殊文字」の 4 種類を指す。*2：複数回答。*3：PC に保存（13%）と携帯電話に保存（10%）の合計。*4：PC に暗号化せずに保存（12%）、PC に暗号化して保存（5%）、携帯電話に保存（16%）の合計。

補論 2.　複数の個別パスワードを管理する非技術的な方法

本稿では、技術的な対策に焦点を当ててきたが、非技術的な対策についても紹介する。具体的には、複数の個別パスワードを管理する対策や（下記（1）、（2））、管理する個別パスワードの数を減らす対策（下記（3））が知られており、それぞれ以下のとおりである。

（1）　ID ／パスワードの分離保管

IPA［2013］では、サービスの個別 ID と個別パスワードを異なるファイル（以下、それぞれ「ID ファイル」、「PW ファイル」と呼ぶ）に記録し、各ファイルを別々に保管するという方法が示されている（図表 A-2）。この方法では、仮に一方のファイルを盗取されても、個別 ID と個別パスワードが揃わないため、不正ログインが防止できると期待される。具体的には、まず、ID ファイルに「サービス名、個別 ID」のほかに、任意のインデックス番号（No.）をサービスごとに記録し、PW ファイルには、対応するサービスのインデックス番号と個別パスワードを記録する。同時に盗取されるリスクを抑えるために、各ファイルを別々に保管する（例：PC と紙、PC とスマートフォン、スマートフォンと紙）。紙で保管する場合には、鍵の掛る机の引出しや財布等で保管することも考えられる。

（2）　使い回す文字列とサービス固有の文字列の組合せ

富士通［2013］や辻［2014］では、サービスごとにまったく異なる個別パスワードを用意するのではなく、「使い回し用の文字列」と「サービス固有の文字列」を組み合わせることで、サービスごとの個別パスワードを生成する方法が示されてい

図表 A-2　ID ／パスワードの分離保管（イメージ）

No.	サービス名	個別 ID
1	○○ 銀行	aaaa
2	△△オンラインショップ	bbbb

（a）ID ファイル

No.	個別パスワード
1	4gs2FWo3qq
2	RF3jfei3ie

（b）PW ファイル

備考：例えば、「○○ 銀行」にログインする場合には、両ファイルの No. 1 の情報を参照する。

る。サービス固有の文字列については、①サービスから容易に推測できるものを選択する方法と（例えば、「Hogehoge Mail」というサービスに「HM」という文字列を割り当てる。富士通［2013］）、②極力ランダムに選択する方法（例えば、同サービスに「8i$」という文字列を割り当てる）がある。

上記①の方法については、第三者がサービス固有の文字列を推測できる可能性がある。このため、同方法により作成した個別パスワードが漏えいした場合、5 節（1）の考察と同様に、使い回し用の文字列（マスターパスワードに相当）が求められ、推測された他のサービスの固有文字列（URL に相当）と組み合わせられることで、不正ログインが成立する可能性がある。富士通［2013］にも、個別パスワードが漏えいした場合には、使い回し用の文字列が漏えいするため、すべてのパスワードを更新することが望ましいとの説明がある。上記②の方法については、サービスごとの固有文字列をいかに管理するかという問題があるが、辻［2014］では、使い回す文字列を記憶し、サービス固有の文字列のみを紙に書くことで、仮に、紙を盗取されても個別パスワード全体の漏えいは防止するというアイデアが示されている。

（3） サービスの重要度に応じたパスワードの使い分け

西本［2013］では、個別 ID と個別パスワードが漏えいすることを前提に、漏えい時の影響を局所化する方法が示されている（図表 A-3）。具体的には、自分が利用している各サービスが乗っ取られた場合を想定し、①同サービスに紐付いている別サービスへの不正ログインにつながる、②金銭的被害が発生する、③金銭的被害に繋がりにくい、④サービス提供者を信頼してよいかわからないといった影響度合いの観点から分類する。上記③や④のグループに分類されたサービスについては、同グループ内の別サービスとパスワードを使い回すことで記憶するパスワードを減らすことも考えられる。ただし、この方法を実施しても、ユーザが記憶するパスワードの数が 3 個よりも多くなる場合には、パスワード管理ツールや前述の（1），（2）の方法を利用することも考えられる。

図表 A-3　サービスの重要度に応じたパスワードの使い分け

サービス例	分類	パスワード管理	備考
主に利用する電子メール	①	超厳重	・同サービスを別サービスの個別パスワード再発行に利用している場合、同サービスへの不正ログインが別サービスへの不正ログインにつながる。 ・自分が管理していない端末でログインした場合、同端末での利用が終わり次第、パスワードを変更すべき。
別サービスのログインに利用可能な SNS	①	厳重	・自分の友人とのコミュニケーションが可能であり、なりすましにより金銭では解決できない深刻な事態に陥る可能性もある。
インターネットバンキング、クレジットカード、電子商取引サイト	②	厳重	・これらのサービスは標的になりやすいため、慎重な管理が必要。
有料サービス	③	必要に応じて管理	・新聞社サイト等は、不正ログインされても、情報をただで読まれる程度であり、金銭的被害が想定し難い。 ・同グループのサービス間でパスワードを使い回すのは現実的な対応。
無料の情報提供サービス	③	必要に応じて管理	・厳重なパスワード管理は不要であり、同グループのサービス間で複雑ではないパスワードを使い回すのは現実的な対応。
信頼してよいかわからないサービス	④	簡単でよい	・入力したパスワード等が盗取されるリスクを考慮し、分類①～③で使用したパスワードとは別のパスワードを使う必要がある。

備考：西本［2013］を基に作成。

補論 3.　安全性要件を満たすパスワード管理方式（処理 5，6）

以下では、処理 5（端末の追加／失効）と処理 6（マルチデバイス環境下でのマスターパスワードの更新）の実現方法と安全性評価についてそれぞれ説明する。その際、処理 1，2 の実現方式に固有のパラメータを用いて説明するために、処理 3，4（パスワード DB の復旧）と同様に、処理 1 の実現方式として鍵分散方式、処理 2 の実現方式として LR-AKE 方式を想定する。

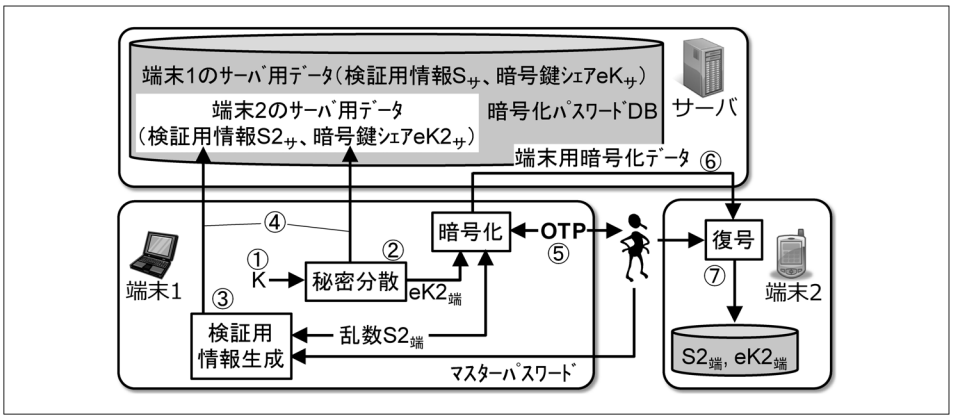
(1)　処理 5：端末の追加／失効

処理 5 では、既に登録されている端末（端末 1）を信頼し、同端末を利用して新たな端末（端末 2）の追加処理を行う。その際、端末 1，2 が同じ暗号化パスワード DB と暗号鍵（K）を利用することで、どちらの端末からでもパスワード DB の更新が行えるようにする（図表 A-4）。

イ．実現方式

処理 5 の端末の追加処理では、まず、端末 1 は、処理 1 のパスワード DB の復号処理と処理 2 の利用処理（サーバとの暗号通信）を行い、暗号鍵（K）を復号する（図表 A-4-①）。次に、端末 1 は、端末 2 用のデータを生成する。具体的には、処理 1 の暗号化処理と同様に、秘密分散法により暗号鍵から 2 つの新しい暗号鍵シェア（$eK2_{サ}$、$eK2_{端}$）を生成するほか（同②）、処理 2 の登録処理と同様に、新しい乱数（$S2_{端}$）を生成し、この乱数とマスターパスワードから検証用情報（$S2_{サ}$）を算出する（同③）。このサーバ用の暗号鍵シェアと検証用情報（以下、「端末 2 のサーバ用

図表 A-4　処理 5 の実現方式



データ」と呼ぶ）については、端末 1 がサーバに送信する（同④）。端末 2 用の暗号鍵シェアと乱数（以下、「端末 2 の端末用データ」と呼ぶ）を端末 2 に格納すれば、端末 2 の追加処理は完了する。

端末 1 と端末 2 がユーザの手元で安全に通信できる環境であれば[59]、同環境を利用して端末 2 の端末用データを端末 2 に送信すればよい。以下では、こうした環境を仮定しない場合の方法を示す。端末 1 は、ワンタイムパスワード（OTP）を生成し（同⑤）、この OTP を用いて端末 2 の端末用データを暗号化し（以下、「端末 2 の端末用暗号化データ」と呼ぶ）、サーバ経由で端末 2 に送信する（同⑥）。ユーザは、端末 1 に表示された OTP を端末 2 に入力することで、端末 2 の端末用暗号化データを復号し、ストレージに格納する（同⑦）。仮に、端末 2 を紛失した場合には失効処理を行う。具体的には、端末 1 等を通じて[60]、サーバから端末 2 のサーバ用データ（検証用情報、暗号鍵シェア）を削除すればよい。

なお、端末 1，2 が追加されている状態では、仮に端末 2 の内部データが破損しても、端末 1 からパスワード DB を利用可能であるほか、端末 1 を用いて新たな端末（端末 3）を追加することが可能であるため、処理 3（端末内データ破損時の復旧）を行う必要はない。

ロ．安全性評価

脅威 2（サーバからの漏えい）により、攻撃者（不正な管理者等）が端末 2 のサーバ用データ（暗号鍵シェア $eK2_{サ}$、検証用情報 $S2_{サ}$）や端末用暗号化データを盗取した場合に、パスワード DB やマスターパスワードが漏えいするか否か（安全性要件 1，2）を評価する。OTP を十分に長くすることで（ランダムに選択した 20 文字の英数字を OTP とする場合、情報量は約 120 ビット）、端末 2 の端末用暗号化データの解読が計算量的に困難になる。また、サーバ用データや暗号化パスワード DB を盗取しただけでは、パスワード DB やマスターパスワードを求められないことは前述のとおりである（4 節（1）、（2））。

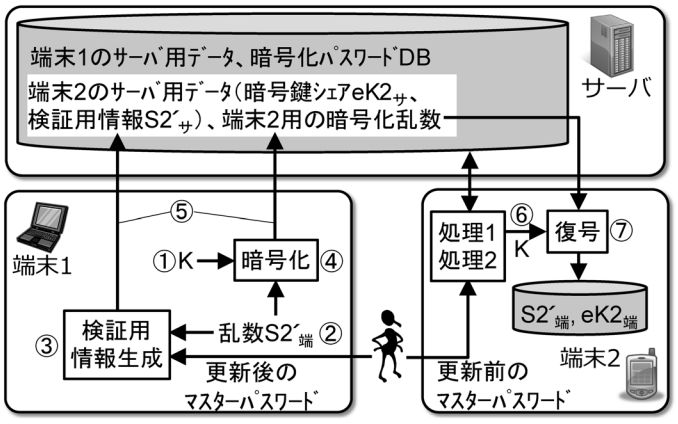
（2） 処理 6：マルチデバイス環境下でのマスターパスワードの更新

処理 6 は、端末 1 においてマスターパスワードの更新を行った際に、他の端末（端末 2）において改めてマスターパスワードを更新することなく、新しいマスターパスワードに移行する処理である（図表 A-5）。直感的には、処理 5 と同様に、端

59 安全に通信可能な環境とは、例えば、2 つの端末が Bluetooth（梅澤・加藤・田代［2009］）、家庭内 LAN、USB 等で直接通信可能な場合や、端末 2 の端末用データを端末 1 のディスプレイに QR コードで表示し、これを端末 2 の内蔵カメラで読み取る等の手段が利用可能な場合を想定している。

60 運用によっては、コールセンターに連絡する等の方法もありうる。

図表 A-5　処理 6 の実現方式



末 1 が新しいマスターパスワードを用いて端末 2 のサーバ用データと端末用データを生成し、各データをサーバと端末 2 にそれぞれ格納するという処理である。その際、処理 5 とは異なり、処理 6 ではパスワード DB の暗号化／復号に利用する暗号鍵（K）を端末 1，2 の両者が使用できるため OTP は不要である。なお、ユーザの手元で端末 1，2 が安全に通信可能な場合の処理は自明であるため割愛する。

イ．実現方式

予め端末 1 は、処理 1 のパスワード DB の復号処理と処理 2 の利用処理（サーバとの暗号通信）を行っており、暗号鍵（K）を復号しているとする（図表 A-5-①）。端末 1 が、マスターパスワードの更新を行う場合、端末 1 用に新しい乱数（$S'_{端}$）を生成し、この乱数と新しいマスターパスワードから新たに検証用情報（$S'_{サ}$）を算出し、乱数を端末 1 に、検証用情報をサーバにそれぞれ格納する。更新前の乱数と検証用情報は削除する。

その後、処理 6 が行われる。まず、端末 1 は、端末 2 用に新しい乱数（$S2'_{端}$）を生成し（同②）、この乱数と新しいマスターパスワードから新たに検証用情報（$S2'_{サ}$）を算出する（同③）。この新しい乱数を暗号鍵で暗号化し（以下、「端末 2 用の暗号化乱数」と呼ぶ。同④）、端末 2 用の検証用情報とともにサーバに格納する（同⑤）。次に、端末 2 は、更新前のマスターパスワードを用いて、一度、処理 1 のパスワード DB の復号処理と処理 2 の利用処理を行い、暗号鍵を復号する（同⑥）。そして、この暗号鍵を用いて、サーバから入手した端末 2 用の暗号化乱数を復号し、乱数を端末 2 のストレージに格納する（同⑦）。更新前の検証用情報と乱数は削除する。

前述の処理では、端末 1 でマスターパスワードを更新した後も、新しいマスター

パスワードに対応したデータ（乱数）を端末 2 に格納するために、更新前のマスターパスワードが必要となる。仮に、更新前のマスターパスワードを忘却した場合には、端末 2 を一度失効し、処理 5 により改めて追加すればよい。

ロ．安全性評価

脅威 2（サーバからの漏えい）により、攻撃者（不正な管理者等）が端末 2 用の暗号化乱数を盗取するものの、暗号鍵で保護されており、攻撃者は乱数を入手できない。処理 6 によって攻撃者が新たに有益な情報を得られるわけではないため、パスワード DB やマスターパスワードは漏えいしない（安全性要件 1，2 を満たす）。