オンライン本人認証方式の実態調査
報告書

平成 26 年 8 月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目　次

1. はじめに 4
1.1. 背景・目的 4
1.2. 調査内容と調査報告書の構成 4
2. オンライン本人認証の概要 5
2.1. 認証と認証手段 5
2.1.1. 認証の 3 要素 5
2.1.2. 認証手段（トークン） 6
2.1.3. 認証方式 7
2.1.4. その他の認証方式 11
2.1.5. アイデンティティ管理 11
2.1.6. 電子認証のアーキテクチャモデル 13
2.2. オンライン認証のフレームワーク 15
2.2.1. 認証フレームワークの基本概念 15
2.2.2. 認証フレームワークの例（ID 連携/認証連携） 15
2.3. オンライン本人認証における危険性 17
2.3.1. パスワードに対する攻撃 17
2.3.2. 認証プロセス等への攻撃 17
3. オンライン本人認証に関連したインシデント状況 19
3.1. パスワードリスト攻撃 19
3.1.1. 被害件数と事例 20
3.1.2. 政府・業界団体による対策の呼びかけ 22
3.2. ウイルスによる認証情報の窃取 27
3.2.1. 件数と事例 27
3.2.2. 手口 27
3.2.3. 業界団体等からの対策呼びかけ 28
3.3 インシデント事例の分析（インタビュー調査の結果） 31
4. オンライン本人認証にかかる実態調査 37
4.1. サービスサイト側 37
4.1.1. 調査実施の概要 37
4.1.2. 認証方式の状況 38
4.1.3. ID の設定について 39
4.1.4. パスワードの設定状況 42
4.1.5. ID 連携について 46
4.1.6. 認証プロトコルの安全性・SSL 通信の有無 47

4.2. 利用者側 48
4.2.1. 調査実施の概要 48
4.2.2. 調査仮説の設定 49
4.2.3. 調査結果 50
4.2.4. 仮説の検証 72
5. 課題と対策 83
5.1. インターネットサービス提供者の対策 85
5.1.1. 利用者が許容範囲な ID・パスワードの検討 85
5.1.2. 各種サービスで扱う情報の資産価値に応じた対策の検討 85
5.2. インターネットサービス利用者の対策 90
5.2.1. 安全なオンライン本人認証方式を選択するために 90
5.2.2. 現実的な脅威を防ぐために利用者が独自に実施できる対策 91
5.2.3. パスワード管理を支援する参考情報 92
5.3. 課題 95
付録 1：アンケート調査票 96
付録 2：その他のアンケート調査結果票 111

1. はじめに

1.1. 背景・目的

オンライン本人認証は様々なシステムやサービスで利用されているが、システムやサービスの 8 割程度が ID・パスワードによる認証であるといわれる（シマンテック社による調査 [1]）。一方、個人の ID・パスワードが窃取され、不正アクセスに悪用される情報セキュリティインシデントが多発している。独立行政法人情報処理推進機構（以下「IPA」という。）では、これらの本人認証に係るインシデントの発生を受け、インターネットサービス利用者（個人）とサービス提供者の実態を調査し、双方にとって安全でかつ実装に過剰な負荷がかからないオンライン本人認証方式の要件を検討するため、本調査を実施した。

1.2. 調査内容と調査報告書の構成

オンライン本人認証方式における実態調査として、公開情報及びインタビューを基に具体的なインシデント事例を調査した。また、インターネットサービスサイトを対象として、サービス利用者に要求している認証情報についての調査、およびインターネットサービス利用者（個人）を対象として、本人認証に関するアンケート調査を実施した。

本調査報告書では、第 2 章にオンライン本人認証の概要、第 3 章にオンライン本人認証に関わる具体的なインシデントに関する調査結果を報告する。第 4 章では、インターネットサービスにおいて提供しているオンライン本人認証の実態調査の結果、及びインターネットサービス利用者を対象としたオンライン本人認証のアンケート調査結果を報告する。最後に第 5 章でオンライン本人認証に関する課題と対策を報告する。

[1] http://internet.watch.impress.co.jp/docs/news/20131031_621665.html

2. オンライン本人認証の概要

本章では、オンライン本人認証の概念、認証手段や方式、オンライン本人認証における主体または関与者（エンティティ）とその役割を示すオンライン本人認証のフレームワーク、オンライン本人認証における危険性など、オンライン本人認証の概要を述べる。

2.1. 認証と認証手段

認証及び認証手段に必要となる技術の概要を次に示す。

2.1.1. 認証の 3 要素

認証方式には以下に説明する 3 つの要素「記憶」、「所持」、「バイオメトリクス情報」があり、認証の 3 要素とも言われる。認証はこれらの 3 要素のどれか、又は複数の要素の組み合わせで実現する。

・記憶（SYK: Something You Know）

本人のみが記憶しているデータに基づいて利用者を認証する方法であり、パスワード、パスフレーズ、PIN（Personal Identification Number）などがこれに当たる。これらの記憶データは他人に知られないようにしておかなければならない。

・所持（SYH: Something You Have）

本人のみが所持している物によって利用者を認証する方法であり、IC カードやスマートカード、ワンタイムパスワードのトークンなどがある。これらの所持物を他人に貸したりしてはいけない。所持物は紛失や盗難の危険性がある。紛失や盗難時の安全性のためにこれらのカードを利用するに当たっては記憶要素（PIN）と組み合わせで用いることが多い。

・バイオメトリクス情報 （SYA: Something You Are）

本人の生体に基づくデータにより利用者を認証する方法であり、本人の特性としての指紋、音声、虹彩、顔の形などを識別することによる。この方法は本人に結びついたデータによるもので記憶忘れや所持物の紛失などの問題はない。

2.1.2. 認証手段（トークン）

認証手段については、NIST が 2006 年に公表し、2013 年 8 月に改版した Electronic Authentication Guideline（NIST SP 800-63-2）（以降、NIST ガイドライン）が参考となる。NIST ガイドラインでは、「電子認証」を「電子的な手段によって情報システムに提供されるユーザ身元識別情報の信用を確立するプロセス」と定義している。本報告書におけるオンライン本人認証と同義である[2]。電子認証に用いられる要素にトークン（Token）やクレデンシャルを定義している。トークンとは、「認証要求者が所持し管理するもの」であり、認証情報等の認証に用いる情報を格納または出力するハードウエアやソフトウェア、あるいは知識等の認証情報そのもの（パスワード等）等である。 主なトークンの種類とその特徴を表 1 に示す。

表 1 主なトークンの種類とその特徴

種類	特徴
パスワードトークン（PW トークン）	利用者が記憶している秘密情報のみを利用して認証を行う。
ソフトウェアトークン（SW トークン）	ハードディスクなどの媒体に暗号鍵を格納し、この鍵を利用して認証情報を出力することで認証を達成させる。暗号鍵の保護機構はソフトウェアにより実装されるため、柔軟な運用が可能である一方で、一般的にハードウエアトークンよりも暗号鍵の複製に対する耐性を確保しづらい。また、トークンを活性化させるためにパスワードの入力を利用者に求める機能を有する場合がある。
ワンタイムパスワードトークン（OTP トークン）	認証に使用する「ワンタイム（一回限り）」のパスワードを生成する機能を有するトークンであり、装置や紙等のハードウエア、あるいはソフトウェアといったさまざまな実装方法が有り得る。また、トークンを活性化させるためにパスワードの入力を利用者に求める機能を有する場合がある。
ハードウエアトークン（HW トークン）	保護された暗号鍵を備えているハードウエアデバイス。この鍵を利用して認証情報を出力することで認証を達成させる。暗号鍵の保護機構はハードウエアにより実装され、ハードウエアトークンからは暗号鍵を取り出すことができないものとする。また、トークンを活性化させるためにパスワードの入力を利用者に求める機能を有する場合がある。

NIST ガイドラインではトークンを 9 種類に分類しており、複数の要素を用いる場合もある。表 2 に 9 種類のトークンの種類と定義を示す。要素の種類は SYK(Something You Know)、SYH(Something You Have)、SYA(Something You Are)の 3 要素があり、表内の○は必須の要素であり、□はいずれかの要素を用いることを示す。

[2] 以降は、特に NIST の文書を参考とする場合のみ、「電子認証」と呼ぶ

表 2　NIST ガイドラインにおけるトークンの種類と定義

要素				名称	概要及び利用方法
数	SYK	SYH	SYA		
単要素	○			記憶された秘密トークン (Memorized Secret Token)	サービスサイトとの間で共有する秘密情報を使った認証。
	○			事前登録知識トークン (Pre-registered Knowledge Token)	あらかじめサーバに登録した質問に対する回答による認証。
		○		ルックアップ秘密トークン (Look-up Secret Token)	サービスサイトとの間で共有される秘密情報を使った認証。
		○		帯域外トークン (Out of Band Token)	あらかじめ登録した携帯電話やスマートフォンなどに通知されるワンタイムパスワードによる認証。
		○		単要素ワンタイムパスワードデバイス (Single-factor (SF) OTP Device)	トークンによって生成されるワンタイムパスワードによる認証。
		○		単要素暗号デバイス (SF Cryptographic Device)	暗号機能をもつハードウエアによる認証 TLS のクライアント認証(″certificate verify″メッセージ)
複数要素	□	○	□	複数要素ソフトウェア暗号トークン (Multi-factor (MF) Software Cryptographic Token)	利用するための第 2 の認証を必要とする情報による認証(暗号機能を使うための情報)。
	□	○	□	複数要素 ワンタイムパスワードデバイス (MF OTP Device)	利用するための第 2 の認証を必要とするトークンによって生成されるワンタイムパスワードによる認証。
	□	○	□	複数要素暗号デバイス (MF Cryptographic Device)	利用するための第 2 の認証を必要とする IC カードなどの暗号機能をもつハードウエアによる認証。

2.1.3. 認証方式

表 2 に示した 9 種類のトークンについて、以下に各トークンを用いた認証方式の具体的な利用例を示す。

(1) 記憶された秘密トークンの利用例

記憶された秘密トークンの具体的な利用例としては、サービス利用者が事前にサービス提供者に登録した ID とパスワードによって認証する方式がある。記憶された秘密トークンを用いた認証の具体的な例としてパスワードによるオンライン本人認証の概要を図 1 に示す。なお、図 1 では、インターネットサービス提供者とインターネットサービス利用者は、事前に秘密情報としてパスワードを共有し、相互に正しい相手先であることを確認していることとする。

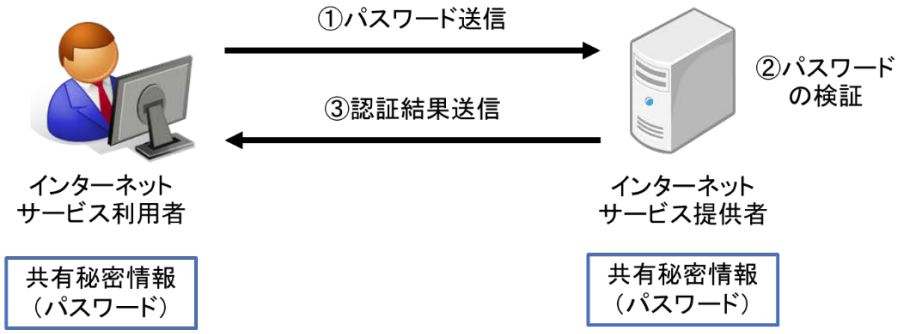


図 1 パスワードによる認証

① 認証要求者であるインターネットサービス利用者は、検証者であるインターネットサービス提供者にパスワードを送信する。なお、インターネット環境においてパスワードを平文で送信すると盗聴の危険性があるため、SSL 等の暗号化を行う必要がある。
② インターネットサービス提供者は、受信したパスワードと事前に共有しているパスワード（秘密情報）との一致を検証する。なお、インターネットサービス提供者が保存しているパスワードは、平文ではなく、ハッシュ化など難読化した状態格納する必要がある。
③ インターネットサービス提供者は、インターネットサービス利用者に認証結果を送信する。

パスワード認証以外にも、サービス提供者から受信したチャレンジ値とパスワードを基にした演算結果を送信することで、パスワードそのものを送信せずに認証を行う方法（チャレンジ／レスポンス方式）がある。

(2) 事前登録知識トークンの利用例

事前登録知識トークンの具体的な利用例としては、秘密の質問（ペットの名前は？母親の旧姓は？等）や複数の画像を表示し、事前に登録していた画像を正しく選択できるかを確認する方法である。これらはリスクに応じて追加的に本人認証を要求する「リスクベース認証」に用いられる場合もある。リスクベース認証の一例として、連続して認証を失敗した場合に、追加的に秘密の質問や画像を選択させ、連続試行回数の時間間隔を空けることで、連続自動入力プログラムによる不正ログイン攻撃を防御するために用いられる。

(3) ルックアップ秘密トークンの利用例

ルックアップ秘密トークンの具体的な利用例としては、マトリクス認証や乱数表及び CATPTCHA[3]がある。CATPTCHA は、オンラインサービスの登録時及び利用時に歪んだ文字等含んだ画像を表示し、その文字を正しく入力した場合に認証許諾する方式である。当初は、SPAM 対策の一環として、ロボットによる不正なアカウント登録及びオンライン掲示板の投稿などの防止策として人間とロボットを区別するために用いられていたが、現在では多要素認証の一種として利用される場合もある。一方、演算処理能力の向上により画像解析及び OCR 技術も向上したことからロボットで正しい文字を読み取り入力し、CATPTCHA をパスすることが可能になって

[3] CATPTCHA は、Completely Automated Public Turing test to tell Computers and Humans Apart（コンピュータと人間を区別する完全自動化公開チューリングテスト）の略称である。

いる。また、事前登録知識トークンと同様に、連続して認証を失敗した場合に、「リスクベース認証」にも用いられる。

(4) 帯域外トークンの利用例

帯域外トークンの具体的な利用例としては、携帯電話やスマートフォンに送信した確認コードを回答させる方法がある。また、事前登録知識トークンと同様に、連続して認証を失敗した場合に、携帯電話やスマートフォンに確認コードを送り回答させる方法を追加する「リスクベース認証」にも用いられる。

(5) 単要素／複数要素ワンタイムパスワードの利用例

ワンタイムパスワードの具体的な利用例としては、一定期間有効なワンタイムパスワードをデバイス等に表示し、これをサイトへ入力する方法がある。ワンタイムパスワードには、①ハードウエアトークン、②ソフトウェアトークンがある。①ハードウエアトークンは、カード形式、キーホルダ形式、USB キー形式等があり、②ソフトウェアトークンは PC アプリケーション型、モバイルアプリケーション型がある。アプリケーションをインストールせずに、Web ブラウザ経由でワンタイムパスワードを表示する形式もある。また、ワンタイムパスワードを生成する方式としては主に以下の 3 種類がある。

- 時間同期方式: トークンと認証サーバが保持している時刻に基づいてパスワードを生成する。
- カウンター同期方式: トークンと認証サーバが保持する内部カウンターの値に基づいてパスワードを生成する。
- チャレンジレスポンス方式 : 認証サーバがチェレンジ値を送信し、トークン側がレスポンスを算出した値またはレスポンス値に基づいてパスワードを生成する。

なお、単要素ワンタイムパスワードと複数要素ワンタイムパスワードの違いは、複数要素ではワンタイムパスワードの利用時に PIN（Personal Identification Number）入力等によってトークンを活性化する点にある。

具体的な例として複数要素ワンタイムパスワード（時間同期方式）によるオンライン本人認証の概要を図 2 に示す。なお、この図では、インターネットサービス提供者とインターネットサービス利用者は、事前に秘密情報として PIN とワンタイムパスワードデバイス（インターネットサービス提供者はワンタイムパスワードを生成するために必要なシークレット）を共有し、相互に正しい相手先であることを確認していることとする。

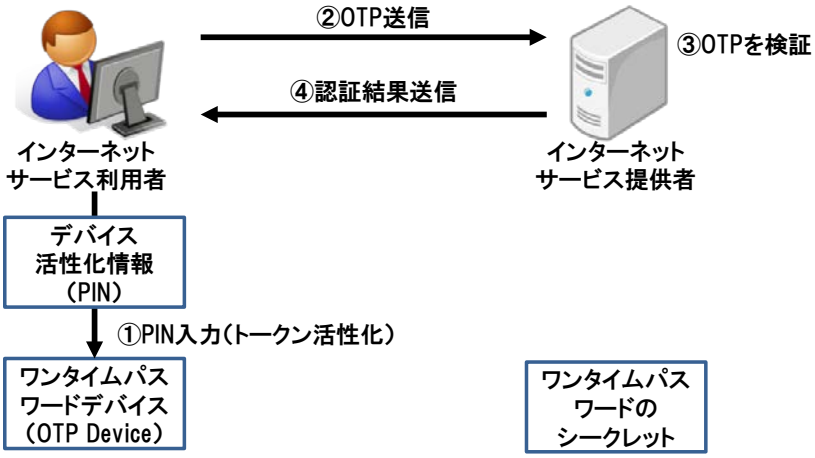


図 2 ワンタイムパスワードによる認証の概要

① 認証要求者であるインターネットサービス利用者は、ワンタイムパスワードデバイスに対して PIN を入力し、トークンを活性化する。
② インターネットサービス利用者は、検証者であるインターネットサービス提供者にワンタイムパスワード（図 2 の OTP）を送信する。なお、ワンタイムパスワードデバイスには、デバイスごとに固有なシークレットが存在し、このシークレットと現在時刻からワンタイムパスワードを生成する。
③ インターネットサービス提供者は、事前に共有しているシークレットと現在時刻からワンタイムパスワードを計算し、受信したワンタイムパスワードとの一致を検証する。
④ インターネットサービス提供者は、インターネットサービス利用者に認証結果を送信する。

(6) 複数要素ソフトウェア暗号トークンの利用例

複数要素ソフトウェア暗号トークンとは、ディスク上のファイル等、ソフトウェア内に認証用の暗号鍵を保持したものであり、PIN 入力や生体認証によるトークンの活性化が必要なものである。例えば、TLS[4]のクライアント認証では、認証要求者であるインターネットサービス利用者は、あらかじめ PIN を入力してトークンを活性化し、サーバから送られてきたチャレンジメッセージ（Hello メッセージ）からトークン内に保持した秘密鍵を使用して署名値（certificate verify）を生成してインターネットサービス提供者に送付する。インターネットサービス提供者は、署名値を検証することによりインターネットサービス利用者を認証する。

(7) 単要素／複数要素暗号デバイスの利用例

暗号デバイスとは、IC カードや USB トークン等に認証用の暗号鍵を保持したものである。単要素暗号デバイスと複数要素暗号デバイスの違いは、複数要素では暗号鍵の利用時に PIN 入力等によってトークンを活性化する点である。

暗号デバイスの利用例としては、TLS のクライアント認証に用いる場合があげられる。((6)と同様の流れ)

[4] **TLS**（Transport Layer Security）プロトコル。Web ブラウザなどに使われる暗号化、認証機能を実現するプロトコルのひとつ

2.1.4. その他の認証方式

前述の 9 種類の認証方式以外に、インターネットサービスで利用されている認証方式を説明する。

(1)多段認証・多要素認証

複数の要素（SYK、SYH、SYA）を用いる認証方式を「多要素認証」というのに対して、同じ要素の認証を多段で実施する認証方式を「多段認証」や「多段階認証」という。例えば複数のパスワード（記憶された秘密トークン）を用いる認証方法がある。後述する金融分野では、第一暗証番号、第二暗証番号を設定することで本人認証と取引を行う際の認証（取引認証と呼ばれる）の二段階の認証を実施している。

(2) リスクベース認証

インターネットサービスの一部では、リスクベース認証が導入されている。リスクベース認証とは、通常とは異なる環境（例えば、普段とは異なる IP アドレスや ISP 及び OS や Web ブラウザ等）からの認証要求があった場合に、追加的に認証する方式である。追加する認証には、秘密の質問と対応する答えを確認する（前述の(2)事前登録知識トークンや(3)ルックアップ秘密トークン）、登録しているスマートフォンに送信した認証コードを確認する（前述の(4)帯域外トークン）等がある。

通常と同じ環境からの認証要求には追加的な本人認証を行わず、通常と異なる環境からの認証要求には追加的に本人認証を行うことから、一定の利便性を保ちつつ、異なる環境からの不正アクセスに対して認証を高めることができる。一方、正規なインターネットサービス利用者が異なる環境から認証要求を行う場合（例えば、急な海外出張先でスマートフォンの送信された認証コードが受信できない等）には、使い慣れていないと追加的に確認する認証情報を忘れ、認証ができず、サービスを利用できないこともある。さらに、通常の環境と通常ではない環境等の区別が難しい場合も存在する。

2.1.5. アイデンティティ管理

インターネットサービス利用者は、特定の企業や団体に所属する属性・アイデンティティや個人としての属性・アイデンティティなど様々な属性・アイデンティティを持つ。そのため、オンライン本人認証は、これらのアイデンティティを確認するプロセスともいえる。これらの認証におけるライフサイクルやステータスの遷移を示した文献は少ないが、アイデンティティ管理技術[5]では、認証情報を含むアイデンティティ管理の一般的なライフサイクルが示されている（**図 3** を参照）。アイデンティティ管理の一般的なライフサイクルでは、登録、活性、更新、休止、抹消がある。これらの中で活性と更新は、アイデンティティが利用可能な有効状態（Active）での実施が必要とされる。

[5] アイデンティティ管理技術解説、独立行政法人情報処理推進機構　セキュリティセンター、2013 年 1 月

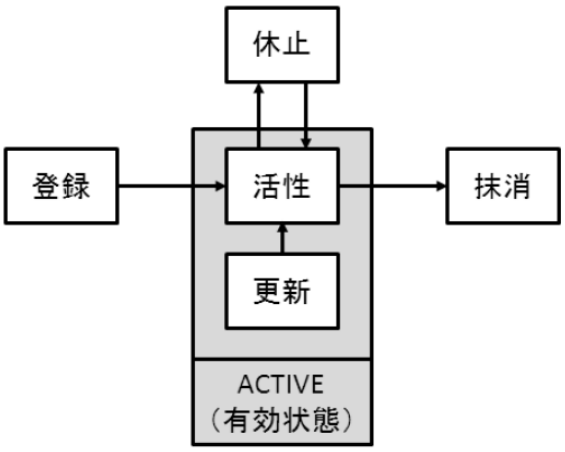


図 3　ID 管理ライフサイクルモデル

アイデンティティ管理の一般的なライフサイクルのプロセスと内容を**表 3** に示す。なお、アイデンティティ情報を利用できるようなライフサイクルである「登録」、「更新」、「休止」、「抹消」等の一連のプロセスはプロビジョニングとも呼ばれる。

表 3　ID 管理ライフサイクルのプロセスと定義

プロセス	内容
登録	アイデンティティ情報及び認証情報の登録を希望するエンティティに対し、身元確認や本人確認を行い、情報管理者による審査等を経て、エンティティを特定する識別子の生成した上でアイデンティティ情報及び認証情報を利用前に登録する。
有効状態（活性）	登録されたアイデンティティ情報及び認証情報を「活性」化（Activate）し、利用可能な「有効状態」にする。有効状態において各エンティティは、アイデンティティ情報及び認証情報を用いて認証を行うことが可能となる。例えば、サービスの提供者は、認証を行い識別子の正当性を確認し、識別子に紐づいた属性情報等の認証情報をもとに提供するサービスレベルやアクセス制御等を行った上で特定のサービスを提供（認可）する。
更新	登録済みの活性状態にあるアイデンティティ情報及び認証情報に含まれる属性情報は、エンティティあるいは情報管理者（サービス提供者）の意向や状況によって更新される。例えば、特定サービスの一般会員から特別会員（プレミアム会員等）への登録情報の変更も含まれる。
休止・抹消	エンティティや情報管理者（サービス提供者）の意向や状況によって、アイデンティティ情報及び認証情報を「休止」の状態や「抹消」する。例えば、特定サービスの利用期間が切れた利用者のアイデンティティ情報や及び認証情報を一時的に利用できない「休止」の状態にし、利用期間を延長する場合には「休止」を解除、利用期間を延長しない場合には「抹消」する。

インターネットサービスでは、表 3 で示したアイデンティティ管理の各プロセスの中の「更新」、「休止」が短期的に繰り返される可能性がある。例えば、「更新」は、ID・パスワードによる本人認証ではパスワードの定期的な更新が求められるため、属性情報の更新と比較し、頻繁に更新が実施されることも考えられる。また、「休止」は、認証要求において連続失敗が一定回数になった場合、また短時間に認証試行を繰り返す場合、及び通常とは異なる環境（IP アドレス等）からの認証試行を繰り返す場合等の不正ログイン攻撃と考えられる際に数分から 1 日程度といった比較的短期間のアカウントロック（アカウントの休止）を対策技術として導入しているサービスも存在する。

2.1.6. 電子認証のアーキテクチャモデル

「2.1.2. 認証手段（トークン）」、「2.1.3. 認証方式」、「2.1.4. その他認証方式」、「2.1.5. アイデンティティ管理」で記述した内容の位置づけを、NIST ガイドラインにおける電子認証のアーキテクチャモデル（**図 4**）を用いて説明する。また、図中の用語説明を**表 4** に示す。

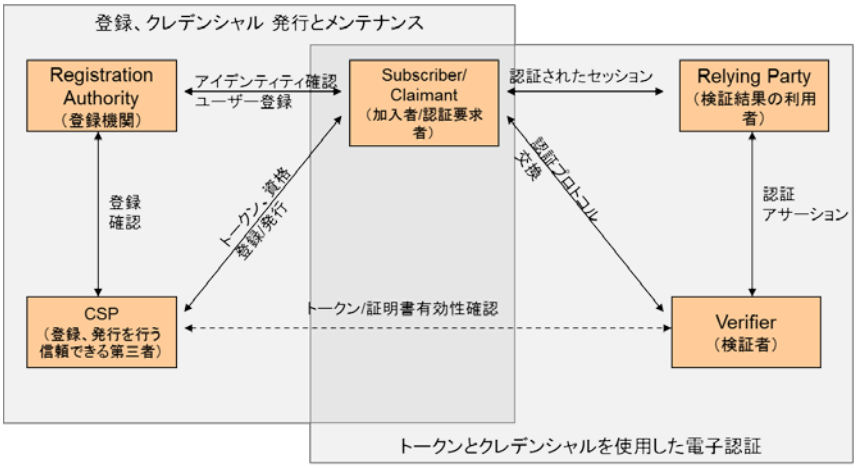


図 4 NIST の電子認証のアーキテクチャモデル

表 4 NIST の電子認証のアーキテクチャモデルの用語定義

用語	定義
アサーション（Assertion）	検証者から、その検証者に依拠する当事者に対して送られる、加入者に関する身元識別情報を収めた表明。アサーションには検証済みの属性が含まれることがある。アサーションは、ディジタル署名されたオブジェクトであったり、セキュアなプロトコルを通じて信頼できる情報源から取得できたりする。
認証要求者（Claimant）	認証プロトコルを使用して身元を証明する当事者。
クレデンシャル（Credential）	身元識別情報（および場合によってはそのほかの属性）と、特定の人物が所持し管理しているトークンとを公的に結び付けるオブジェクト。
クレデンシャルサービスプロバイダ（Credentials Service Provider、CSP）	加入者トークンの発行または登録を行い、電子的クレデンシャルを加入者に発行する、信頼のおける機関。CSP が、登録機関と、登録機関が運営する検証者を兼務することがある。CSP は、独立の第三者機関である場合がある。また、独自に使用するクレデンシャルを発行する場合がある。
加入者（Subscriber）	CSP からクレデンシャルまたはトークンを受け取り、認証プロトコルにおいて認証要求者となる人物。
トークン（Token）	認証要求者が所持し管理しているなんらかの情報（通常は鍵またはパスワード）。認証要求者の身元識別情報の認証に使用される。
身元識別情報（Identity）	個人のユニークな名前。個人の法的な名前は必ずしも一意とは限らないため、個人の身元識別情報には名前全体が一意となるように十分な補足情報（たとえば、住所、あるいは従業員番号や口座番号といったユニークな識別子など）を含める必要がある。
登録機関（Registration Authority、RA）	CSP に対し加入者の身元を証明し、その保証を行う、信頼のおける機関。RA は CSP の一部である場合がある。または、CSP から独立しているものの、1 つ以上の CSP と連携することもある。
検証結果の利用者（Relying party）	通常、トランザクションの処理や、情報またはシステムへのアクセス許可の付与を目的として、加入者のクレデンシャルを利用するエンティティ。
検証者（Verifier）	認証要求者がトークンを所持していることを認証プロトコルを使用して確認することにより、認証要求者の身元識別情報を検証するエンティティ。この目的のために、検証者はトークンと身元識別情報を結び付けるクレデンシャルの有効性を検証し、それらの状態を確認しなければならないこともある。

図 4 の右側は、利用者がインターネットサービス提供者のサービスを利用する為に、電子認証を実施する場合を示している。「加入者／認証要求者（Subscriber／Claimant)」はインターネットサービス利用者であり、「検証結果の利用者（Relying Party)」及び「検証者（Verifier)」がインターネットサービスとなる。なお、以下で示すとおり、加入者は認証を要求する場面において認証要求者となる。以下に図右のプロセスを説明する。

1. 認証要求者は、認証プロトコルを用いて認証要求者がトークンを所持・管理していることを検証者に証明する。
2. 検証者は、加入者のアイデンティティをトークンに結び付けるクレデンシャルを検証するために CSP と対話する。
3. 検証者と RP が独立している場合、検証者はアクセス・コントロールまたは認可を決定するために、RP に対して加入者（認証要求者）のアサーションを提供する。
4. 加入者と RP の間で認証されたセッションを確立する。

上記「1.」のプロセスで使用するトークンは「2.1.2. 認証手段（トークン)」で記述したトークンであり、トークンの所持・管理を証明する方式は「2.1.3. 認証方式」や「2.1.4. その他認証方式」で記述した認証方式である。

図 4 の左側は、利用者のアイデンティティの登録、発行、メンテナンスのフェーズを示している。つまり、「2.1.5. アイデンティティ管理」で記述した ID のライフサイクルは、加入者（Subscriber）と登録機関（RA）／CSP（Credentials Service Provider）との間で実施される各処理を示す。以下に図左のプロセスを説明する。

1. 個々の認証申請者は、RA に対して登録プロセスを通じてユーザ登録とアイデンティティ確認を申請する。
2. RA は認証申請者のアイデンティティ確認を行う。
3. アイデンティティ確認が成功した場合、RA は CSP に対して新たな加入者（認証要求者）の登録確認を行う。
4. 加入者と CSP の間でトークンとトークンに対応するクレデンシャルを確立する。
5. CSP は少なくとも加入者の資格、クレデンシャルとそのステータス及び有効期限等を登録データして所持する。また、加入者は自らのトークンを所持する。

RA と CSP の最も単純で一般的な実施形態は、RA と CSP は個別の機能として同じエンティティに存在する。一方、電子認証のアーキテクチャでは RA は、複数の独立した CSP と関係を有する場合もある。同様に CSP は独立した複数の RA と関係を有する場合もある。

以上のように認証のフレームワークについては、認証を求めるエンティティの属性や資格等の確認において関連する各エンティティの責任分担や、信頼が重要である。

2.2. オンライン認証のフレームワーク

2.2.1. 認証フレームワークの基本概念

ここでは、本報告書で扱う認証における主体または関与者（エンティティ）とその役割を示すフレームワークを説明する。

「認証」のためには、まず、「識別」が必要であり、識別した個人に対して認証を行う。広義の意味では、識別、認証、認可を含んで「認証」と呼ばれることもある。また、インターネット環境におけるオンライン本人認証では、認証者と認可者が同一な場合も多い。基本概念を以下に示す。

- 識別(Identification)： Who Are You？ 特定の個人を見分けること
- 認証（Authentication）:Is it really you? 識別された個人が正当であることを確認すること
- 認可（Authorization）:Are you authorized to access this resource 認証された個人に対してサービスを提供するかどうかを決定すること

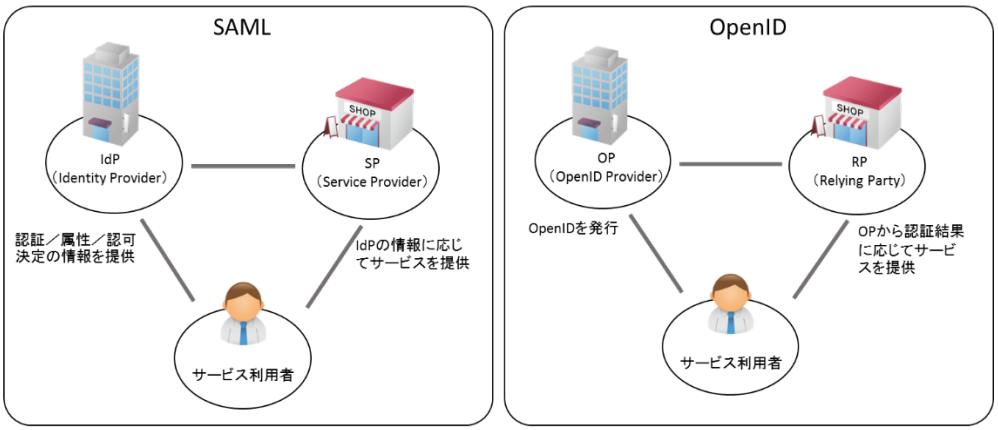
「認証」では識別された個人の属性（役割や権限等）に基づき、本人または本人性を確認することが求められる。多くのインターネットオンラインサービス等では、個人に対して認可を行うサービス提供者が個人を識別し、かつ認証を付与するが、認証と認可は別のエンティティが実施することも可能である。例えば、異なる個人の ID を連携する ID 連携の技術仕様である SAML（Security Assertion Markup Language）では、認証オーソリティ、属性オーソリティ、認可決定オーソリティと機能別ににそれぞれが定義されている。またインターネットにおける共通の ID 情報を利用できる OpenID では、認証サービス（認証し、検証する）を提供する OP（OpenID Provider）と認証サービスを利用してサービスを提供する RP（Relying Party）が定義されている。

2.2.2. 認証フレームワークの例（ID 連携/認証連携）

システム間やサービス間の認証連携やID連携により多様なサービスを提供する例がみられる。これらに対応する認証フレームワーク関連の技術として、SAML や OpenID がある。

SAML（最新は SAML2.0）は、サービス間でのセキュリティ・アサーションの交換に関するフレームワークを定めている。セキュリティ・アサーションを利用することで、各種 Web サービス間で認証／属性／認可決定に関する情報交換が実現でき、一度の認証で複数の Web サービスが利用できる SSO を実現する。OpenID（厳密には認証技術に OpenID Connect、認可技術に OAuth2.0）は、Web ブラウザを用いて異なる Web サイト間で属性情報の要求・提供と認証結果に関するプロトコルを定めている。これは、2 つの Web サイト間における、Web ブラウザを用いたアイデンティティ情報（エンティティの認証結果と属性情報）の要求と応答を行うためのプロトコルとして策定された。SAML は、アイデンティティ連携で必要な要素を包括的にカバーしたフレームワークを提供し、アイデンティティ連携においては、Web サイトが属するドメイン間の信頼関係を事前に確立することが前提となる。一方、OpenID は、Web サービスに特化したプ

ロトコルを提供し、Web サイト間はユーザの意図にしたがって動的に信頼関係を確立する。SAML と OpenID の概要を図 5 に示す。



項目	SAML	OpenID
概要	サービス間でのセキュリティ・アサーション交換のフレームワーク	Webブラウザを用いた、Webサイト間での属性情報の要求・提供と認証結果のプロトコル
ID等の発行者	IdP（Identity Provider）	OP（OpenID Provider）
サービス提供者	SP（Service Provider）	RP（Relying Party）
Webサイト間の信頼関係	Webサイトが属するドメイン 間の信頼関係を、事前に確率することが前提	Webサイト間はユーザの意図にしたがって動的に信頼 関係を確立

図 5 SAML と OpenID の概要

2.3. オンライン本人認証における危険性

オンライン本人認証における具体的な危険性を、多く利用されている ID・パスワードによる認証を対象とした攻撃と認証プロセス等への攻撃について述べる。

2.3.1. パスワードに対する攻撃

パスワード認証は実装が容易であり、特別な知識や専用機器やデバイスも必要ないためサービスサイトは導入し易く、利用者にも受け入れられ易い。一方、パスワード認証の強度はパスワードの強度に依存し、事前に設定、共有したパスワードが推測されにくいこと等を考慮する必要がある。以下に、パスワードに対する主な攻撃を示す。

表 5　パスワードに対する主な攻撃

主な脅威	説明
総当たり攻撃（ブルートフォース攻撃）	すべてのパスワードの組み合わせを試行する攻撃である。非常に多くの組み合わせがあるため、効率的ではないが、数字 4 文字等のパスワード長が非常に短い場合には有効である。また、総当たりする順番を工夫し、短いパスワード、小文字だけのパスワード、大文字が含まれるパスワード、長いパスワードといった順で攻撃することもある。
逆総当たり攻撃（リバースブルートフォース攻撃）	パスワードを固定し、ID を変えて攻撃を試みる手口。サービスサイト側では、ID に対して複数のパスワードを試行しないため、パスワードの複数回ロック規制などは効果がない。
類推攻撃	利用者の個人情報（例えば、ユーザ名/ログイン名、恋人/友人/身内/ペットの名前、自分/友人/身内の出身地や誕生日、車のナンバープレート、携帯電話の番号、会社の電話番号、住所、お気に入りの有名人の情報等）からパスワードを類推する攻撃である。
辞書攻撃	パスワードとして使われていそうな文字列を数多く収録したリスト（辞書）を用意して、それらを試行する攻撃である。
事前計算攻撃（オフライン）	パスワードファイルを盗み、パスワード辞書の文字列をハッシュ化して、試行する攻撃である。ハッシュ値のテーブルを効率的に管理するレインボーテーブルを使ったレインボー攻撃も知られている。

2.3.2. 認証プロセス等への攻撃

オンライン本人認証とは、インターネット等を用いたオンライン環境で本人認証を実施することである。すでに述べたように、本人確認は、認証を要求する認証要求者と認証情報を発行する認証発行者間（または認証を提供する者）で正しい本人であることを確認する。認証発行者は、認証要求者本人を確認した後に、認証情報を発行する。認証情報の発行については、認証要求者本人以外に知られることなく正しい認証要求者のみに発行されなければならない。認証要求者は、認証発行者から得た認証情報を他者に知られることなく安全に保管し、認証を必要とする場合に認証情報を他者に知られることなく認証検証者（インターネットサービスの場合はインターネットサービス提供者等）に示すことで本人認証が正しく行われる。

表 6 に主なオンライン本人認証のプロセスに関する脅威を示す[6]。

[6]各府省情報化統括責任者（CIO）連絡会議決定の「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（以下、電子署名・認証ガイドライン）」を参考とした

表 6　認証プロセス等における脅威例

脅威	説明
オンライン上での推測	攻撃者が、繰り返しログインを試行するなどして、認証情報（パスワード等）を推測する。
オフライン分析	トークン（認証情報等）が不正に解析される。
DoS 攻撃[7]	ネットワークに接続されたコンピュータに過剰な負荷をかけて、サービスの提供を不能に陥れる攻撃を行う。
DDoS 攻撃[8]	標的に対して、複数のコンピュータ等を利用して DoS 攻撃を行うこと。攻撃元のコンピュータは、攻撃者自身のものとは限らず、ウイルスへの感染により意図せず攻撃者のコンピュータとなる場合もある。
フィッシング	利用者を欺いて、不正なサイトに誘い出し、情報を不正に取得する。
ファーミング	利用者を、強制的に不正なサイトにアクセスさせ、情報を不正に取得する。
盗聴	通信を盗聴し、情報を不正に取得する。
リプレイ攻撃	認証に関する通信を盗聴し、同じ内容を再度送信してなりすましを行う。
セッション・ハイジャック	認証プロトコルが完了した後に、利用者とサービス提供者の接続を奪うことによって、正当な利用者に代わってサービスを利用する。[9]
中間者攻撃[10]	利用者とサービス提供者の通信を中継する形で横取りし、改ざん等の不正を行なう。

オンライン手続におけるリスク評価及び電子署名・認証ガイドラインを基に IPA が作成

[7] Denial of Service：分散サービス妨害
[8] Distributed Denial of Service：分散サービス妨害
[9] これらの脆弱性への対策については、安全なウェブサイトの作り方、知っていますか？脆弱性等を参照。
http://www.ipa.go.jp/security/vuln/websecurity.html 、http://www.ipa.go.jp/security/vuln/vuln_contents/
[10] Man-in-the-Middle attack、MitM

3. オンライン本人認証に関連したインシデント状況

本章では、特に近年多発している主な攻撃として 3.1 にパスワードリスト攻撃と被害を 3.2 にウイルスによる不正送金の被害を、公開された情報により紹介する。3.3 には、主にパスワードリスト攻撃に遭遇した企業やその企業に関連する団体へのインタビュー調査の結果について述べる。

3.1. パスワードリスト攻撃

インシデントの中でもインターネットサービスサイトに対するパスワードリスト攻撃の事案が多発している[11]。パスワードリスト攻撃とは、悪意のある者が、何らかの方法で事前に入手した ID とパスワードのリストを流用し、自動的に連続入力するプログラム等を用いてそれら ID とパスワードを入力することで、インターネットサービスサイトにログインを試みる攻撃である(図 6)。　複数のインターネットサービスにおいてインターネットサービス利用者が ID とパスワードを同一のものを使用している場合、その中のいずれかのインターネットサービスで利用している認証情報（アカウント情報）が漏えいすると、悪意ある者が他のインターネットサービスで同じ ID とパスワードを用いて、インターネットサービス利用者 X になりすましてログインすることが可能となる。

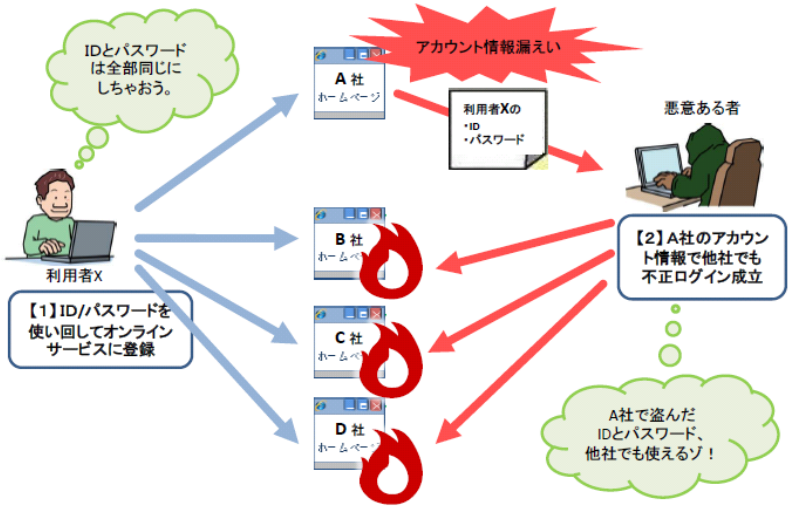


図 6　利用者の観点から見たパスワードリスト攻撃による被害のイメージ図

[11] IPA では、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！」によってインターネットのサービス利用者に注意喚起を行った。http://www.ipa.go.jp/security/txt/2013/08outline.html
なお、パスワードリスト攻撃には、リスト型アカウント攻撃、連続自動入力プログラムによる攻撃、など複数の呼称がある。

3.1.1. 被害件数と事例

国家公安委員会、総務大臣、経済産業大臣が公表している「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（平成 26 年 3 月 26 日）」[12]（以降不正アクセス等の状況報告書）では、一般的な不正アクセス行為の認知件数とともに、事業者から得た「連続自動入力プログラムによる不正ログイン攻撃」（本報告書におけるパスワードリスト攻撃と同同義）の件数を報告している。平成 24 年度から本攻撃の件数が報告されているが、攻撃件数は、表 7 に示すように平成 25 年は、平成 24 年と比べ約 7 倍増加した。

表 7　不正アクセス行為の認知件数等

認知件数／届出件数	平成 24 年	平成 25 年
不正アクセス行為の認知件数	1,251	2,951
連続自動入力プログラムによる攻撃※1	114,013	約 800,000

不正アクセス等の状況報告書を基に IPA が作成

※1：不正ログイン攻撃については、ID・パスワードの正規利用権者に対する被害の確認を行っていないことから、認知件数が不正アクセス行為の事実を確認することができた場合とはいえない。

「検挙した」不正アクセス禁止法違反に係る犯行の手口についても、インターネットサービス利用者のパスワードの設定や管理の甘さにつけ込んだものが平成 25 年に急増している。不正アクセス等状況報告書における不正アクセス行為に係る犯行の手口の内訳を表 8 に示す。

表 8　不正アクセス行為に係る犯行の手口の内訳

手口分類	平成 24 年		平成 25 年	
利用権者のパスワードの設定･管理の甘さにつけ込んだもの	122	22.9%	767	79.5%
言葉巧みに利用権者から聞き出した又はのぞき見たもの	229	43.0%	64	6.6%
識別符号を知り得る立場にあった元従業員や知人等によるもの	101	19.0%	56	5.8%
共犯者等から入手したもの	22	4.1%	35	3.6%
スパイウェア等のプログラムを使用して識別符号を入手したもの	29	5.5%	25	2.6%
フィッシングサイトにより入手したもの	18	3.4%	9	0.9%
他人から購入したもの	0	0.0%	7	0.7%
その他	11	2.1%	2	0.2%
合計	532	100.0%	965	100.0%

2013 年に発生したパスワードリスト攻撃 20 件の事例について公開情報を基に整理した内容を表 9 に示す。公表されている不正ログインの試行件数（A）と不正ログインの成立件数（B）から不正ログイン成功率（B/A）を算出してみると、不正ログイン成功率の高低は、試行回数とは関係なく、低い事例で 0.1%程度、高い事例では 2.5%程度である。

[12] http://www.npa.go.jp/cyber/statics/h25/pdf041.pdf

表 9　主なインシデント事例と発生時期

被害企業	不正アクセス期間	不正ログインの試行件数(A)	不正ログインの成立件数(B)	不正ログイン成立率※(B/A)
T サイト	3 月 26 日 7 月 15 日	－	299 27	－
MyJR-EAST	3 月 31 日	約 26,000	97	0.37%
goo	4 月 1 日～4 月 9 日	－	108,716	－
eBookJapan	4 月 2 日～4 月 5 日	2,821	779	－
フレッツ光メンバーズクラブ	4 月 4 日 4 月 9 日～4 月 10 日	約 20,000 約 24,000	30 77	0.15% 0.321%
mopita	4 月 18 日～4 月 19 日	－	5,450	－
dinos	5 月 4 日～5 月 8 日	約 1,110,000	約 15,000	1.35%
ワタシプラス	5 月 6 日～5 月 12 日	約 240,000	682	0.28%
三越オンラインショッピング	5 月 6 日～5 月 23 日	5,202,002	8,289	0.16%
阪急オンラインショッピング	不明～5 月 13 日	－	2,382	－
ハピネットオンライン	4 月 24 日～5 月 31 日	－	最大 16,808	－
じゃらん net	2 月 14 日～2 月 16 日 6 月 3～6 月 15	約 1,100,000	27,620	2.51%
ニッセンオンラインショッピングサイト	6 月 18 日	11,031	126	1.14%
クラブニンテンドー	6 月 9 日～7 月 4 日	15,457,485	23,926	0.16%
KONAMI ID ポータル	6 月 13 日～7 月 7 日	3,945,927	35,252	0.89%
楽天市場	不明～7 月 8 日	－	－	－
@nifty	7 月 14 日～7 月 16 日	－	21,184	－
Gree	7 月 25 日～8 月 5 日	7,748,633	39,590	0.51%
Ameba	4 月 6 日～8 月 3 日	－	243,266	－
@games	8 月 3 日～8 月 13 日	－	83.961	－

※「不正ログイン成立率」は、企業が公表した数値（A および B）を基に算出。

パスワードリスト攻撃は以下に述べる 3 つの特徴をもつ。まず、(パスワードリスト攻撃によって）攻撃者が不正にログインできた場合、サービス提供者は当事者しか知り得ない情報によって認証された正規の利用者とみえる。このため、サービス提供者自身による被害の発見は容易ではない。一方、正規の利用者は攻撃者によってサービスの不正利用や他の情報を搾取されることとなり、サービス提供者は、正規のサービス利用者ではない攻撃者に対してサービスを提供することとなり、サービス提供者と利用者の双方にとって不利益や被害が発生する。

次に、サービス提供者にとって、情報を不正に入手されたサービスサイトとして風評被害の懸念がある。また対策を公開することによってさらに攻撃手法が高度化することも推測できることから一部のガイドラインは具体的な対策手段が公開されることが少ない傾向にある。さらに、対策については一部の業界や分野を除き、各々の企業が独自に検討し実施している状況である。

そのほかの特徴として、総務省の「パスワードリスト攻撃による不正ログインへの対応方策について」において、リスト型攻撃による被害の特徴が表 10 のようにまとめられている。

表 10　リスト型攻撃による被害の特徴（総務省による）

・ ある程度の期間にわたって攻撃が行われているものがあり、攻撃が検知されるまでに時間を要するものがあること ・ 数万単位での不正ログインが検出されていること ・ 利用者からのログインができないといった通報、大量のアクセスエラーの発生、特定の IP アドレスからの不正なログインの検知、社内の調査によって攻撃が検知されていること ・ 氏名、性別、生年月日、住所などの個人情報が閲覧されている可能性があること

なお、本調査では、表 9 に示したパスワードリスト攻撃事例で被害のあった企業及び関連団体を含む 10 社／団体に対してインタビュー調査を実施した（3.3 を参照）

3.1.2. 政府・業界団体による対策の呼びかけ

本節では、パスワードリスト攻撃に関する対策検討の状況について特定業界団体における技術的対策の検討動向、政府による対策の呼びかけの内容について述べる。

(1) 業界団体における技術的対策

オンライン本人認証については、各業界団体等において技術面及び運用面での対策をガイドライン等で推進している。以下に金融分野及びオンラインゲーム分野の対策を紹介する。

①　金融分野

金融分野においては、金融情報システムセンター（FISC：Center for Financial Industry Information Systems）の「安全対策基準 第 8 版 追補」及び一般財団法人全国銀行協会の「インターネット・バンキングに係る預金等の不正な払戻しへの対策について」でパスワードリスト攻撃対策に関する記述が存在する。「安全対策基準 第 8 版 追補」[13]では、（技 35）にて、以下の通りオンライン本人認証を用いた技術的対策が記されている。利用時には ID・パスワード以外の認証が必要であり、ID・パスワードの以外の認証方式を提供する場合でも携帯電話利用する認証方式（例えば、携帯電話番号を登録させ、SMS（ショートメッセージ）等によって任意の認証コードやワンタイムパスワードを送信し、それを入力させて確認する認証方法）では、ID・パスワードが漏えいした場合も想定し、異なる認証を行った後に登録することが推奨されている。

表 11　安全対策基準 第 8 版 追補における本人認証の記述

・ 個人顧客を対象とするインターネット･バンキングにおいては、ログイン時と重要取引時の少なくともどちらか一方で、固定式の ID･パスワードのみに頼らない認証方式の導入が必要である。 ・ ID･パスワードを用いて携帯電話の識別番号を金融機関に登録する方式においては、ID･パスワード漏洩時に、第三者の携帯電話番号の識別番号を、不正に登録されるリスクがあるため、登録時には異なる認証を用いることが望ましい。

一般財団法人全国銀行協会の「インターネット・バンキングに係る預金等の不正な払戻しへの対策について」[14]では、表 13 の記述があり、対策例の（1）及び（2）において複数要素を用い

[13] 金融情報システムセンター、2013/03/01 https://www.fisc.or.jp/isolate/?id=609&c=topics&sid=77&dc=3
[14] 一般財団法人全国銀行協会、平成25年11月14日 https://www.zenginkyo.or.jp/news/2013/11/14160001.html

た認証が推奨されている。（3）及び（4）はウイルスによる認証情報窃取に対する対策である。

表 12 インターネット・バンキングに係る預金等の不正な払戻しへの対策について

1. インターネット･バンキングにおけるセキュリティ対策の強化
お客さまがご利用になるパソコンが、コンピューターウイルスに感染した場合にも、インターネット･バンキング取引に係る預金等の不正な払戻しが行われることのないよう、個人･法人等のお客さまの属性を勘案し、セキュリティ対策の強化に努める。
具体的には、足下で発生している犯罪手口に留意し、次のような対策を 1 つまたは複数組み合わせるなどして、順次、対策を講じていくよう努める。 対策の検討に当たっては、将来発生が懸念される犯罪手口への対応策も考慮に入れるものとする。
【対策例】
(1)ワンタイムパスワード(ハードウエアトークン、ソフトウェアトークン、電子メール通知等)の採用。なお、電子メール通知方式の場合は、お客さまの携帯電話アドレス宛に送信する等、取引に利用しているパソコンとは別の機器への送信を強く推奨する。
(2)お客さまが取引に利用しているブラウザとは別の、携帯電話等の機器を用いる取引認証の導入。
(3)お客さまのパソコンのウイルス感染状況を検知し、警告を発するソフトの導入と、場合により取引を遮断する対処。
(4)お客さまに対するセキュリティ対策ソフトの無償配布。 等

② オンラインゲーム分野

オンラインゲーム分野では、日本オンラインゲーム協会にて「パスワードリスト攻撃に対する対策ガイドライン」[15]を作成しているが、このガイドラインは、実際のセキュリティ対策等の情報が含まれているため非公開である。また、業界内で利用するワンタイムパスワード認証基盤が構築されている[16]。

表 13 日本オンラインゲーム協会、「ランダム型アイテム提供方式における表示および運営ガイドライン」および「セキュリティガイドライン」を公表
http://www.japanonlinegame.org/pdf/JOGARelease120815.pdf より抜粋

- インシデント発生時の情報共有に関するガイドライン
- パスワードリスト攻撃に対する対策ガイドライン
- ワンタイムパスワード等セキュリティソリューションガイドライン
- セキュリティベンダー関連団体との連携ガイドライン

※上記ガイドラインには、実際のセキュリティ対策等情報が含まれるため非公開とさせていただきます。

(2) 政府による対策の呼びかけ

パスワードリスト攻撃の多発を受け、前述の「不正アクセス等状況報告書」及び総務省の「リスト型アカウントリスト攻撃による不正ログインへの対応方策について」で呼びかけている具体的な対策を紹介する。

15 日本オンラインゲーム協会、2012 年 8 月 15 日
http://www.japanonlinegame.org/pdf/JOGARelease120815.pdf
16 オンラインゲーム、スマートフォンゲームの JOGA セキュリティシステムについて（2011 年 11 月）
http://www.jssec.org/dl/111117/4_amemiya.pdf

①　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

「不正アクセス等の状況報告書」では、不正アクセス行為に対する「防衛上の留意事項」として利用権者の講ずべき措置とアクセス管理者等の講ずべき措置が示されている。これらには、フィッシング対策等に加え、パスワードリスト攻撃への対策が記載されている。報告書にある利用権者（インターネットサービス利用者のこと）の講ずべき措置を表 14、アクセス管理者等の講ずべき措置を表 15 に示す。

オンライン本人認証技術の選択に関しては、利用権者の講ずべき措置として金融機関等が提供するワンタイムパスワードを積極的に利用すること（下表：フィッシングに対する注意）、アクセス管理者の講ずべき措置として、インターネットショッピング、オンラインゲーム、インターネットバンキング等のサービスではワンタイムパスワード等による認証の強化が求められている。インターネットショッピング、オンラインゲーム、インターネットバンキング以外のサービスに関する認証方式の選択方法や推奨等は示されていない。

表 14 防御上の留意事項（利用権者の講ずべき措置）

措置	内容
フィッシングに対する注意	電子メールにより、本物のウェブサイトに酷似したフィッシングサイトに誘導したり、添付されたファイルを開かせたりして、ID・パスワードやクレジットカード情報を不正に取得する事案が多発していることから、発信元に心当たりのない電子メールに注意する。また、金融機関等が電子メールで口座番号や暗証番号、個人情報を問い合わせることはなく、これらの情報の入力を求める電子メールはフィッシングメールであると考えられることから、情報を入力しない。さらに、金融機関等が提供するワンタイムパスワード等の個人認証方法を積極的に利用する。
パスワードの適切な設定・管理	言葉巧みに聞き出した ID・パスワードによる不正アクセス行為、利用権者のパスワードの設定の甘さにつけ込んだ不正アクセス行為、知人等による不正アクセス行為が多発していることから、パスワードを設定する場合には、ID と全く同じパスワードや ID の一部を使ったパスワード等、パスワードの推測が容易なものは避ける、複数のサイトで同じパスワードを使用しないなどの対策を講じる。また、パスワードを他人に教えない、パスワードを定期的に変更するなど自己のパスワードを適切に管理する。
不正プログラムに対する注意	コンピュータに不正プログラムを感染させ、他人の ID・パスワードを不正に取得する事案が多発していることから、信頼できない電子メールに添付されたファイルを不用意に開いたり、信頼できないウェブサイト上に蔵置されたファイルをダウンロードしたりしない。また、不特定多数が利用するコンピュータでは重要な情報を入力しない。さらに、コンピュータウイルス対策等の不正プログラム対策（ウイルス対策ソフトの利用のほか、オペレーティングシステムやウイルス対策ソフトを含む各種ソフトウェアのアップデート等）を適切に講ずる。金融機関等が提供するセキュリティ対策ソフトを積極的に利用する。

表 15 防御上の留意事項（アクセス管理者等の講ずべき措置）

措置	内容
フィッシング等への対策	フィッシング等により不正に取得した ID・パスワードを使用した不正アクセス行為が多発していることから、インターネットショッピング、オンラインゲーム、インターネット・バンキング等のサービスを提供する事業者にあっては、ワンタイムパスワード等により個人認証を強化するなどの対策を講ずる。
パスワードの適切な設定・運用体制の構築	利用権者のパスワードの設定の甘さにつけ込んだ不正アクセス行為が多発していることから、アクセス管理者は、容易に推測されるパスワードを設定できないようにする、定期的にパスワードの変更を促す仕組みを構築する、複数のサイトで同じパスワードを使用することの危険性を周知するなどの措置を講ずる。
ID・パスワードの適切な管理	ID・パスワードを知り得る立場にあった元従業員による不正アクセス行為も引き続き発生していることから、従業員が退職した時や特定電子計算機を利用する立場でなくなった時には、当該従業員に割り当てていた ID を削除したり、パスワードを変更したりするなど識別符号の適切な管理を徹底する。
セキュリティ・ホール攻撃への対応	セキュリティ・ホール攻撃の一つである SQL インジェクション攻撃を受け、クレジットカード番号等の個人情報が流出する事案や、Web サーバの脆弱性に対する攻撃を受け、ホームページが改ざんされる事案が発生していることから、アクセス管理者は、プログラムを点検してセキュリティ上の脆弱性を解消するとともに、攻撃の兆候を即座に検知するためのシステム等を導入し、セキュリティ・ホール攻撃に対する監視体制を強化する。

② パスワードリスト攻撃による不正ログインへの対応方策について

総務省の「パスワードリスト攻撃による不正ログインへの対応方策について」では、リスト型攻撃対策集として、攻撃を予防する対策と攻撃による被害の拡大を防ぐ対策をまとめている。攻撃を予防する対策を表 16 に、攻撃による被害の拡大を防ぐ対策を表 17 に示す。

表 16　リスト型攻撃対策集（攻撃を予防する対策）

対策	内容
1. ID・パスワードの使い回しに関する注意喚起の実施	サービス毎に異なる ID・パスワードを設定するよう利用者に注意喚起する
2. パスワードの有効期間設定	パスワードに有効期限を設定し、利用者に定期的に変更させる
3. パスワードの履歴の保存	数世代前に使用したパスワードへの変更を認めないようにする
4. 二要素認証の導入	ID・パスワード以外の認証要素（ワンタイムパスワード等）を追加する
5. ID・パスワードの適切な保存	サービス運営事業者において暗号化等 ID・パスワードの適切な保存を行う
6. 休眠アカウントの廃止	長期間利用実績の無いアカウントをデータも含めて削除する
7. 推測が容易なパスワードの利用拒否	パスワードポリシーを定め、推測が容易なパスワードの利用を拒否する

表 17　リスト型攻撃対策集（攻撃による被害の拡大を防ぐ対策）

対策	内容
1. アカウントロックアウト	同一の ID に対して一定の閾値以上の認証エラーが発生した際にアカウントを一時停止する
2. 特定の IP アドレスからの通信の遮断	特定の IP アドレスから閾値以上のログイン要求が発生した際に、当該 IP アドレスからの通信を遮断する
3. 普段とは異なる IP アドレスからの通信の遮断	通常ログインされている IP アドレスとは大きく異なる IP アドレスからのログイン要求が発生した際に、当該 IP アドレスからの通信を遮断する
4. ログイン履歴の表示	ログイン履歴を保存し、利用者がアカウントの利用実績を認識できるように設定する

以上の対策は、インターネットサービス提供者が実施する対応方策を示しているが、パスワードの設定は、インターネットサービス利用者自身が行うものである。同じインターネットサービスで取り扱う情報が同じであっても、個々のインターネットサービス利用者によってリスクの評価は異なる。そのため、パスワードを設定するインターネットサービス利用者に対してリスク分析の重要性、リスク分析の結果に応じた適切なパスワード設定の重要性を啓発することは必要であるが、すべてのサービスサイトでサービス提供者側のリスク分析の結果によってパスワードポリシーを一方的に強制的することは議論の余地がある。

② まとめ

前述したふたつの報告書に示された対策について整理したものを表 18 に示す。防衛上の留意事項（「不正アクセス等状況報告書」）は、インターネットサービス提供者が行う措置と利用者が行う措置に分かれ、リスト型攻撃対策集（総務省による）はインターネットサービス提供者が行う措置だけが記載されている。4.二要素認証の導入を検討すること、ID・パスワードに関しては、1.パスワードの使い回しの注意、2.パスワードの有効期間の設定、7.推測が容易なパスワードの設定に関する対策が共通である。

表 18 防衛上の留意事項とリスト型攻撃対策集の共通対策

	対策内容	提供者の措置		利用者の措置
		リスト型攻撃対策集	防御上の留意事項	
攻撃を予防する対策	1.ID・パスワードの使い回しに関する注意喚起の実施	○	○	○
	2.パスワードの有効期間設定	○	○	○
	3.パスワードの履歴の保存	○		
	4.二要素認証の導入	○	○	○
	5.ID・パスワードの適切な保存	○	○	
	6.休眠アカウントの廃止	○		―
	7.推測が容易なパスワードの利用拒否	○	○	○
攻撃による被害の拡大を防ぐ対策	1.アカウントロックアウト	○		―
	2.特定の IP アドレスからの通信の遮断	○		―
	3.普段とは異なる IP アドレスからの通信の遮断	○		―
	4.ログイン履歴の表示	○		
その他	・フィッシングに対する注意		○	○
	・不正プログラムに対する注意			○
	・セキュリティ・ホール攻撃への対応	○	○	

3.2. ウイルスによる認証情報の窃取

パスワードリスト攻撃とともにウイルスによる認証情報の窃取を起因とした不正送金の被害が多く発生している。ここでは公開情報をもとに調査した件数や事例及び手口や対策などを述べる。

3.2.1. 件数と事例

警察庁が公表している「平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について（平成 26 年 1 月 30 日）」では、インターネットバンキングに係る不正送金の被害件数と被害額が報告されている。平成 23 年には 165 件、約 3 億円を超える被害があったが、平成 24 年には 64 件、約 4,800 万円と一時的に被害は減少する。平成 25 年では 6 月以降に被害が急増し、1,315 件、約 14 億円を超え、過去最大の被害であった。さらに、平成 26 年度の 5 月までで昨年度と同程度等の被害額となり、過去最大であった昨年度の被害額以上の被害額になることは確実である。

表 19 インターネットバンキングに係る不正送金事犯の発生状況（平成 25 年中）

年	被害件数	被害額
平成 25 年	1,315 件	約 14 億 600 万円
平成 24 年	64 件	約 4,800 万円
平成 23 年	165 件	約 3 億 800 万円

3.2.2. 手口

基本的な手口は、インターネットバンキング利用者のパソコンにウイルスを感染させ、不正なポップアップ画面を表示し、インターネットバンキングの ID、パスワード、暗証番号、乱数表、合言葉を盗み取る方法である（図 7 参照）。攻撃者はウイルスによって窃取した認証情報を不正送金などで利用する。

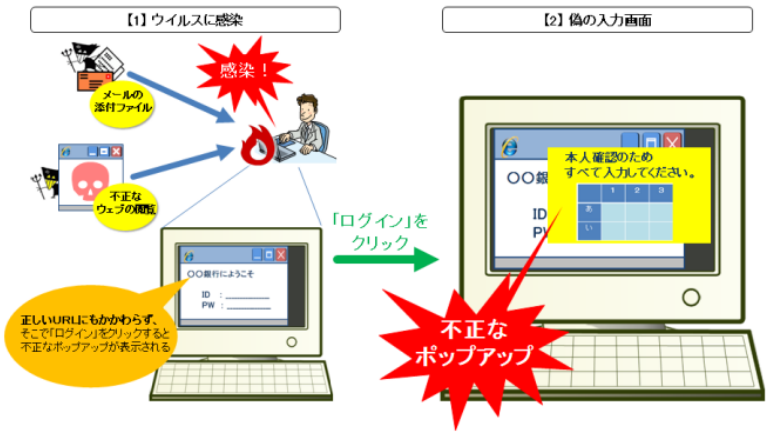


図 7 不正なポップアップ画面を表示させる手口のイメージ図 [17][18]

[17] 2012 年 12 月の呼びかけ「ネット銀行を狙った不正なポップアップに注意！」
https://www.ipa.go.jp/security/txt/2012/12outline.html

別の例では、ワンタイムパスワード認証を利用している場合、ワンタイムパスワードをウェブメールで受け取る設定で、認証情報等を不正に取得される事例があった（2013 年 11 月以降）。この手口のイメージ図を図 8 に示す。図 8 の「①ログイン、送金操作」によって「②メールによるワンタイムパスワード通知」が行われるが、「③メール確認」及び「④ワンタイムパスワード取得」を行う PC 環境等がウイルスに感染している場合、インターネットバンキングの ID、パスワード、乱数表、合言葉に加えて、ワンタイムパスワードを受信するためのウェブメールサービスの ID、パスワードも盗み取るという手口である（図 8 の⑤）。

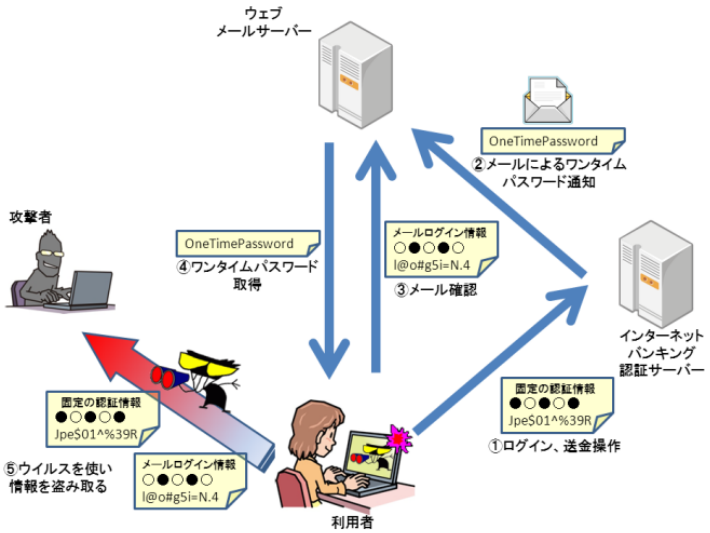


図 8 メールで受け取るワンタイムパスワードを不正取得される手口のイメージ図

3.2.3. 業界団体等からの対策呼びかけ

ウイルスによる不正送金と前述のパスワードリスト攻撃との違いは、利用者が推測困難なパスワードを設定してもウイルス感染を防げないことにある。これらの対策について、フィッシング対策協議会、一般社団法人全国銀行協会、警察庁が公表している、対策の概要及びガイドラインの概要を以下に示す。

① インターネットバンキングの不正送金にあわないためのガイドライン

フィッシング対策協議会では、「インターネットバンキングの不正送金にあわないためのガイドライン（2014 年 05 月 12 日）[19]」において乱数表等の第二認証情報の入力を慎重に行う等の運用上の対策を示している。以下に対策内容を示す。

---

18 2013 年 9 月の呼びかけ「 インターネットバンキング利用時の勘所を理解しましょう！
https://www.ipa.go.jp/security/txt/2013/09outline.html

19 https://www.antiphishing.jp/report/guideline/internetbanking_guideline.html

表 20 インターネットバンキング不正送金にあわないためのガイドライン

共通項目 （鉄則）	・ 乱数表等（第二認証情報）の入力は慎重に行う ・ インターネット利用機器を最新の状態に保つ
PC 環境	・ ソフトウェアのこまめなアップデートで常に最新状態に保つ ・ ウイルス対策ソフトを利用！ 検知用データは常に最新に保つ ・ 基本ソフト（OS）のアップデートも忘れずに行う ・ 怪しいサイトへのアクセスは避ける
スマートデバイス環境	・ アプリのこまめなアップデートで常に最新状態に保つ ・ セキュリティソフトを利用！ 検知用データは常に最新に保つ ・ 基本ソフト（OS）のアップデートも忘れずに行う ・ アプリは正規アプリマーケットからインストールする

② 法人向けインターネット・バンキングにおける不正送金について

一般社団法人全国銀行協会では、「法人向けインターネット・バンキングにおける不正送金にご注意！[20]」において運用上の対策を示している。以下に対策内容を示す。

表 21 法人向けインターネット・バンキングにおける不正送金の注意事項

1. ご利用者のパソコンの状態に関する対策
（1）基本ソフト（OS）やウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新する。
（2）パソコンにセキュリティ対策ソフトを導入するとともに、最新の状態に更新する。
2. インターネット・バンキングの運用における対策
（1）取引の申請者と承認者とで異なるパソコンを利用する。
（2）パスワードを毎月変更する。
（3）振込・払戻しなどの限度額を必要な範囲内でできるだけ低く設定する。
（4）不審なログイン履歴がないかを確認する。
（5）振込先の事前登録などの取引銀行が提供するセキュリティ対策を導入・利用する。

単なるログイン履歴の表示だけではなく、ログイン時にスマートデバイス等に取引内容を通知する対策もある。これらの正常系・異常系のログインをサービス提供者に通知する方法については、正常なログインの結果が表示された場合には、不正ログイン試行がなかったことを確認でき、また不正ログインの試行（異常系のログイン）があった場合には、サービス利用者は不正ログインを身近な脅威として検知可能であるため、有効な対策と考えられる。

③ インターネットバンキングに係る不正送金事案への対策について

警察庁では、「インターネットバンキングに係る不正送金事案への対策について（平成 25 年 5 月 1 日）[21]」においてワンタイムパスワードの利用を推奨している。以下に対策内容を示す。

表 22 インターネットバンキングに係る不正送金事案への対策について

・ ウイルス対策ソフトを導入する。
・ パソコンの OS や各ソフトウェアを最新の状態にする。
・ ワンタイムパスワードを利用する。
・ 不審な入力画面等発見した場合は金融機関等に通報する。

[20] http://www.zenginkyo.or.jp/topic/sagijiken_ib_co/
[21] http://www.npa.go.jp/cyber/warning/h25/130501.pdf

メールにワンタイムパスワードが送信される場合は、PC 上で受け取るメールのアドレスではなく、携帯電話のメールアドレスを登録し、携帯電話等でワンタイムパスワードを受信するように設定することが効果的であることが補足されている。

3.3 インシデント事例の分析（インタビュー調査の結果）

パスワードリスト攻撃事例で被害のあった企業及び関連団体を含む 10 社／団体に対してインタビュー調査を実施し、インシデント事例を分析した。表 23 にインタビュー調査概要を示す。なお、ほぼすべてのインタビュー対象企業は、企業・団体名を公開しないことを希望したため、企業・組織名と回答内容を対応づけていない。

表 23 インターネットサービスサイトの調査概要

項目	概要
調査対象	インシデント事例を有する国内インターネットサービス提供者及び関連団体等 10 社/団体 ＜内訳＞ ・実際に被害を受けた企業：6 社 ・上記企業及び業界の関連団体：4 組織
調査実施期間	2013 年 9 月～2014 年 4 月
調査項目	過去遭遇したオンライン本人認証に係るインシデントの発生状況及び対策に関する技術およびビジネス上の課題等 Ⅰ.現状の対策 1.ベースとなる認証方式（ID・パスワードや ID 連携等） 2.多重認証（ワンタイムパスワード、乱数表等） 3.リスクベース認証（接続・利用環境の相違、属性に関する質問等） 4.パスワード変更の方法やパスワード変更を促す通知 5.参照しているガイドライン及び業界団体の検討内容の有無 6.その他 Ⅱ.インシデント事例 1.インシデント有無 ①インシデントを発見したきっかけ及び対策 ②インシデントの対象となった認証技術 ③対策規模（人員）や期間、対策による低減度合い 2.インシデント事例の変遷や最近の傾向 3.インシデント後の対策（教訓を含む） ①インシデント発生前と後での本人認証方式の変化 ②インシデント被害及び対策に関する直接的・間接的な影響 ③インシデントを未然に防ぐために必要だった対策 Ⅲ.今後求められる対策 1.今後のインターネットサービス提供者におけるセキュアな本人認証やサービス提供のために必要と思われる対策 ①インターネットサービス提供者が行うべき対策 ②インターネットサービス利用者（個人）が行うべき対策 2.対策に関する技術およびビジネス上の課題 3.検討する上で重要となる情報等

(1) 被害に遭遇した時点の状況

すべての企業(6 社)で ID・パスワードによる認証を実施していた。ID・パスワードの保持数を削減させることが可能な、ID 連携を採用している企業は 1 社のみであった。多要素認証として、ワンタイムパスワードが 3 社、リスクベース認証は 4 社が、それぞれ一部のサービスに導入している状況であった。被害後、利用者に対するパスワードの変更要請は、5 社で一般的な告知を行っている。

(2) インシデント発生に際しての対応等

インシデントの検知・発見やその後の対策状況についてのインタビューでは、以下にあげる状況であった。ただし、対象組織が少ないため、必ずしもすべての企業に断定できるわけではない。

a) 発覚のきっかけ、検知について

- 他者からの情報提供や他社で発生した事件を受けて自社を調査して発覚した。
- 自動プログラムによる高速スピードのログイン試行を防ぐことは可能だが、近年の攻撃は巧妙となっており、アクセス間隔があいているなど、長期間にわたった攻撃が発生している。このような攻撃を検知するのは難しい。

b) インシデント対応

- クレジットカード情報が流出した場合には、その被害の発覚に一定に期間を要するため、その間のモニタリング対応が必要となった。
- 複数のサービスを実施している企業では、被害にあったサービス以外についても確認を要し、非常に時間を要した。
- 緊急的な対応が必要となるため、通常業務が滞る。
- 情報共有の場があり、インシデント情報を入手した。これは、事前に注意喚起等は可能だが、防ぐことはできない。

c) 利用者への周知・注意喚起等

- パスワード変更を呼び掛けるアナウンスを実施した。
- パスワードを変更しないとサービスを再開できないようにした。
- 報道はあったが、ユーザは事の重大性を理解していないと感じる。
- パスワード管理はユーザの責任でもある。

d) インデント対応後の対策

- 特に対策を追加していない。
- インシデント発生時にすでにワンタイムパスワード（オプション）を提供している
- ワンタイムパスワードを提供しているが有償であり、普及しない。
- 具体的なインシデント内容は CSIRT で共有することが可能ではないか。

(3) 今後求められる対策・課題など

- 最も効率的なのは、利用者が適切なパスワードを設定すること。
- OpenID（ID 連携）の活用
- セキュリティ保護ツールの充実
- ワンタイムパスワードの提供。
- 複数要素認証
- 新たな認証（ワンタイムパスワードや複数要素認証）を導入するのはコストがかかり、有償とすると利用されない。
- ユーザへの情報提供および啓発。年齢層に従った啓発活動が必要
- 技術的には種々考えられるかもしれないが、ビジネス上の要件とビジネスの持続性を考慮す

る必要があり、適切な対策を決定するのは難しい。
- パスワードリスト攻撃では、そもそもアカウントを流出させない対策が必要で、これが強固である必要がある。
- 業界他社とのインシデント情報共有体制が必要
- フィッシングサイトの対策のためには双方向認証も必要
- 緊急時の人的リソース割り当てを検討しておくこと
- パスワードポリシーを厳しくすると、ビジネスインパクトが大きい。
- 流出したアカウントの情報を共有できれば、被害は未然に防げるのではないか
- ユーザに多くの対策を求めるのは難しいことから、ID 連携は一つの解となる。
- 使用したいサービスがすべてID連携をしているわけではないので､問題解決にはならない。

(4) インシデントを未然に防ぐために必要だった対策

公開情報及び当事者や関連団体に対するインタビュー調査の結果から、インシデントを未然に防ぐために必要と考えられる対策を、①技術的な側面、②情報共有的な側面。③体制面と分類し、以下に述べる。

① 技術的な側面

ID・パスワードによる認証以外の認証方式や複数要素認証及び ID 連携の導入を検討すべきであったとする企業もあった。他方で認証方式の新規導入についてはビジネス面での影響を踏まえ、長期の検討期間を要するため、具体的に導入検討に至る企業は少ない。また、多くの企業から不正アクセス行為の認証状況のモニタリング（ログの監視）などを実施することで早期に発見、対応できた可能性が指摘された。しかしながら、このためには、脅威情報等を事前に収集しておく必要がある。また、サービスサイト側からは一見して正常な認証行為と見え、不正なアクセスであることを検知することは困難であるため、不正認証試行を分析・検知できる技術が発展するとよい。

② 情報共有的な側面

○脅威情報の共有（事前情報の共有）

攻撃を受ける前に、事前に「どのようなサービス」に対して「どのような攻撃」が発生し、「どのような被害」が生じているのかについては、事前に収集できていた企業と収集できていなかった企業が存在した。このため、不正アクセスの検知が早い段階で可能だった場合と、発覚が遅かった企業がある。不正アクセス（認証試行）は、巧妙化しており、短時間に試行を繰り返すだけではなく、長期間にゆっくりと試行を繰り返す場合や、特定 IP アドレスからの試行ではなく、複数の IP アドレスから試行する場合もあり、これらの攻撃に関する最新情報の共有が有効と考えられている。ただし、パスワードリスト攻撃では情報共有によってモニタの注意のレベルを上げることは可能だが、防ぐことはできない。

○対策情報の共有（事後対策の共有）

「どの程度」対策を行うべきか、及び「サービス利用者に告知すべき内容」についても情報が無く対策に苦労したという企業が多かった。標的型攻撃などではすでに情報共有の仕組みがあるが、同様にパスワードリスト攻撃に対しても、発生状況の把握、手口の分析、再発防止のための対策の検討とその検討結果に関する情報の周知や共有を可能とするしくみは役に立つ。

② 体制面

パスワードリスト攻撃の攻撃を受けたことを確認し、対策を行う際に、人的リソースの割り当てがスムーズに実施できず、関連する開発者及びサポート人員など限られた人員で対策した例もあり、インシデント対応体制の観点からの対策も必要である。また、サービス利用者から金銭的被害の報告がなかった場合でも、クレジットカード情報の不正利用による決済の有無を確認する必要があるため、決済期間を考慮し少なくとも 2 ヶ月間は監視体制が必要であった 。

(2) インシデントによる被害状況

公開情報及び当事者や関連団体に対するインタビュー調査の結果から、インシデントによる影響を①直接的な影響と②間接的な影響に分類した、以下にこれらの概要を報告する。

① 直接的な影響

○金銭的な被害

インターネットバンキングにおける不正送金等のインシデントと比較して、パスワードリスト攻撃による金銭的な被害報告は多くないが、特典ポイントに関連した操作が発生した事例は、金銭的な被害となる。

○対策及び他サービスの確認に係る工数

対策に携わるための人件費が必要となった。また、一企業において複数のインターネットサービスサイトを提供し、その中の 1 つのインターネットサービスサイトにインシデントが発生した場合、企業としては、インシデントが発生したサービスサイト以外の他のサービスサイトについても安全性を確認すべきと考え、他のサービスサイトについても、攻撃の有無を確認し、そのための工数と期間が相当必要となった。また、クレジットカード情報の流出の恐れがあるインシデントでは、被害が判明するために 2 か月間が必要となり、その間の対応が必要である（再掲）。

②間接的な影響

○スパムメールの大量配信等による他の脅威への拡大

インターネットサービスの多くは、メールの到達性によって本人を確認する。また、パスワードの再発行等をメールで送信する場合もある。不正に収集された ID・パスワードにメールの認証情報が含まれる場合には、メールを閲覧し、再発行されたパスワードを入手すること、不正にパスワード再発行することが可能である。ウェブメールサービスではこのようにして入手したメールアドレスとパスワードによる不正利用の事例も存在する。

また、アカウントの不正利用によるスパムメールの大量配信が行われた事例も存在した。スパ

ムメールの大量配信によりマルウェアの配布が行われ、ボットなど他の脅威に繋がる可能性がある。図 9 にパスワードリスト攻撃によって他の脅威に繋がる全体像を示す。一般に、図の赤字で示したパスワードリスト攻撃による「①リスト型サービスアカウント 不正アクセス」、サービス管理・運用面の脆弱性を利用した「②サービスアカウント／パスワード大量漏洩」、及びこれらで不正に入手した情報を基に行う「③マルウェア感染、個人アカウント／パスワード漏洩、ボット化」が注目されている。しかし、脅威がさらに拡大し、「①パスワードリスト攻撃」によって「②’スパム大量配信、マルウェア配布」が行われ、「③マルウェア感染から個人アカウント／パスワード漏洩、ボット化」に至り、「④システムアカウントの不正アクセス」が発生しているという指摘があった。

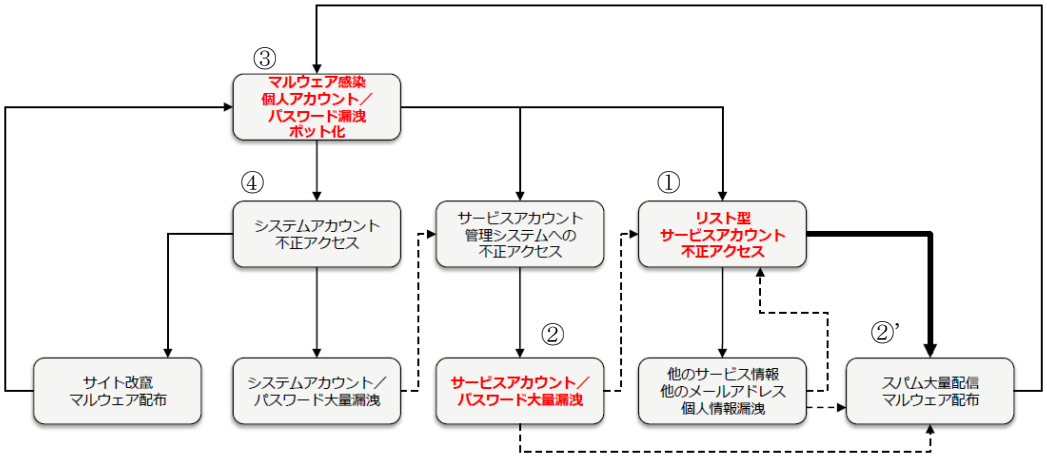


図 9　アカウントの不正アクセスによるマルウェア配布の構図

○対策人員に係る定常業務の遅延

緊急的にインシデント対策として割り当てられた人員が通常行う定常的な業務の遅延が見られた。

(5) 技術及びビジネス上の課題

インターネットサービス提供者は、技術的な検討だけではなく、ビジネス的な検討も踏まえて本人認証方式を選択し提供する。既存の本人認証の選択や新規の本人認証の導入選定においても様々な検討が必要となる。インタビュー調査の結果から主な検討事項を挙げる。

○ID・パスワード認証について

- パスワードポリシーを変更する場合など、インターネット利用者に対して新たに制限や制限を行うと、利用者数の低減などの恐れがある。また、新たな制限を行う必然性を示す必要がある。そのため、自社や他のインターネットサービスのインシデント事例を参考にする場合（他サービスが不正アクセスを受けているため自サービスのパスワードポリシーを厳しくする等）があり、対策の実施が遅れる。

○専用デバイスを用いた認証について

- オプションとしてワンタイムパスワードの導入やトークンデバイスの導入を行っている場合でも有料で提供する場合には、これらの導入が進まない場合が多い（例えば、ワンタイムパスワードの新規導入時期に無料配布し、一定期間後に有料化に切り替えると利用率が低下する等）。

○ID 連携の導入について

- 利用者が複数の ID・パスワードを記憶するには限度がある。そのため、管理すべき ID・パスワード数を削減させる意味で ID 連携を検討する余地がある。
- 一般的な利用者や一般会員ではなく、特別な利用者や特別会員には独自に利用者を管理し、より良いサービスを提供したいと考える傾向があり、このような場合には ID 連携を利用せず、独自に ID を発行して管理する。また、ID 連携の導入を検討する場合に自社と競合関係にあるインターネットサービス提供者が提供する ID を ID 連携に利用することは好まれない。ID 発行者の信頼性の維持確認や事業継続性などの保証などの課題、及び ID 提供条件の変更等も考慮する必要があり、これらが障壁となり導入できない場合もある。
- SNS の ID やアカウントを利用してサービスを提供している場合、ID 以外に必要な情報が不足することなども考えられるため、不足している情報を利用者から独自に得る必要があり、この場合は、ID 連携等には向かない。また、決済などを行うサービスの場合は、ID 連携を利用する際に ID の管理主体や管理方法についての責任分解が明確でなくなる可能性があり、導入できない。

○ID・パスワードの設定基準に関する指標・ガイドラインについて

- ID・パスワードに関する具体的な指針やガイドラインを求める意見が多数あった。一方、指針やガイドラインが対象とする範囲は、一般的なインターネットサービス全般を対象とするものと、より具体的に特定分野のサービスのみを対象としたものを求める意見があった。

4. オンライン本人認証にかかる実態調査

4.1. サービスサイト側

本調査では、国内外のインターネットサービスサイトで提供されているオンライン本人認証方式の調査、並びに、過去オンライン本人認証に係るインシデントが発生した企業及び業界団体等に対するインタビューを調査した。インタビュー調査の詳細は、3.2 に記載したとおりである。

4.1.1. 調査実施の概要

各インターネットサービスサイトにおける調査項目などは表 24 に示す通りである。

表 24 インターネットサービスサイトの調査概要

区分	項目	概要
サイト調査	調査対象	国内外のインターネットサービスサイト ・ 国内サービスサイト：100 サイト ・ 海外サービスサイト：30 サイト
	調査対象環境	・ PC 環境 ・ スマートデバイス環境（スマートフォン、タブレット） なお、スマートデバイスでの利用環境が提供されているサイトについては、ブラウザとスマホ専用アプリを含む。
	調査方法	実際に各サイトへアクセスし、利用者登録等を実施。なお、契約等を必要とするサービスについては、利用者登録を行わず、公開情報から本人認証方式に関連する情報を収集。
	調査実施期間	2013 年 11 月～2014 年 3 月
	調査項目	・ 利用者登録時に要求する情報 ・ 認証方式、通信方式の種別 ・ 認証情報の内容、変更方式 ・ 多重認証の場合は、各認証方法 （ID・パスワードの場合は、ID およびパスワードの安全性に対する条件） 等
インタビュー調査	調査対象	インシデント事例を有する国内インターネットサービス提供者及び関連団体等（10 者）
	調査実施期間	2013 年 9 月～2014 年 4 月
	調査項目	過去遭遇したオンライン本人認証に係るインシデントの状況及び対策に関する技術およびビジネス上の課題（詳細は 3.2 参照）

調査対象のインターネットサービスサイトについては、4.2 のインターネットサービス利用に対するアンケート結果から抽出した代表的な業種（金融、ポータル、オンラインショッピング、オンラインゲーム、SNS など）を踏まえ、8 種類のサービスに分類した。以下にサービス分類を示す。

表 25 調査対象のインターネットサービス分類

サービス分類名	主なサービス
1) 金融	銀行、信託、証券、保険、クレジットカード、キャッシング
2) 通販･物品購入	総合通販、ギフト･クーポン･チケット(共同購入)、インテリア･日用雑貨、美容･健康器具･ファッション、音楽･書籍購入、家電･パソコン
3) オンラインゲーム	オンラインゲーム
4) 交通･運輸･旅行	運輸、旅行･宿泊･ホテル、レンタカー･タクシー予約
5) 学習･教育･就職	人材紹介、転職･就職、教育(e-Learning、英会話等)
6) ポータルサイト	ポータルサイト
7) 情報配信･提供	SNS、口コミサイト、アンケート、ヘルスケア、イベント開催支援
8) 通信･放送･報道	通信、放送、報道･ニュース

PC 環境及びスマートデバイス（スマートフォン、タブレット）環境で調査を実施したサイトのサービス分類ごとの件数は以下の通りである。

表 26　サイト調査件数

サービス分類名	調査件数	
	PC 環境	スマートデバイス環境
1)金融	34	0
2)通販･物品購入	26	7
3)オンラインゲーム	9	2
4)交通･運輸･旅行	22	5
5)学習･教育･就職	3	0
6)ポータルサイト	8	0
7)情報配信･提供	25	12
8)通信･放送･報道	6	4
計	133	30

4.1.2. 認証方式の状況

① 認証方式（PC 環境）

サービス提供時に用いられている認証方式について、標準で提供されている認証方式とオプションで提供されている認証方式のすべてをまとめた結果（実数と各サービス分類の比率）を表 27 に示す。表中、例えば標準で ID・パスワードによる認証を、オプションでワンタイムパスワードが提供されている場合は、ID・パスワードとワンタイムパスワードに各々記載している。

サービス利用時の認証方式は、すべてのサイトで ID･パスワードによる認証が利用されている。金融分野では第二認証(2 つ目のパスワードを用いる認証)やワンタイムパスワード(表中:OTP)、スマートフォン専用アプリとして提供しているワンタイムパスワード（表中 : OTP(スマートフォン)）等が利用されている割合がその他のサービスに比べて高い傾向にある。その他のサービスでは、ID・パスワードによる認証以外の比率は低い。

表 27　サービス別認証方式（PC）　（セル内下段は、割合%）

	ID・パスワード	第二認証	秘密の質問	CAPTCHA	マトリクス・乱数表	OTP	OTP（スマートフォン）	複数要素OTP
金融	34	17 (50%)	1 (3%)	0	9 (26%)	18 (53%)	14 (41%)	0
通販･物販購入	26	0	0	2 (8%)	0	0	0	0
オンラインゲーム	9	0	1 (11%)	2 (22%)	0	2 (22%)	1 (11%)	1 (11%)
交通･運輸･旅行	22	0	0	0	0	0	0	0
学習･教育･就職	3	0	0	0	0	0	0	0
ポータルサイト	8	1 (13%)	3 (39%)	0	0	1 (13%)	3 (39%)	0
情報通信･提供	25	1 (4%)	1 (4%)	1 (4%)	0	0	1 (4%)	0
通信･放送･報道	6	0	0	0	0	0	0	0
	133	19	6	5	9	21	19	1

② 認証方式（スマートデバイス環境）

スマートディバイス環境に対するサービスサイトの認証方式は、ID・パスワードのみの認証が9割以上を占めている。一方で、ID・パスワードに加えて他の認証も導入されているサイトも一部存在し、CAPTCHA認証やワンタイムパスワードが利用されている。本調査対象先の中でワンタイムパスワードが導入されているサービスでは、セキュリティトークンとして、アプリ型トークン、PC一体型トークン、ハードウエアトークンが選択できる形となっている。

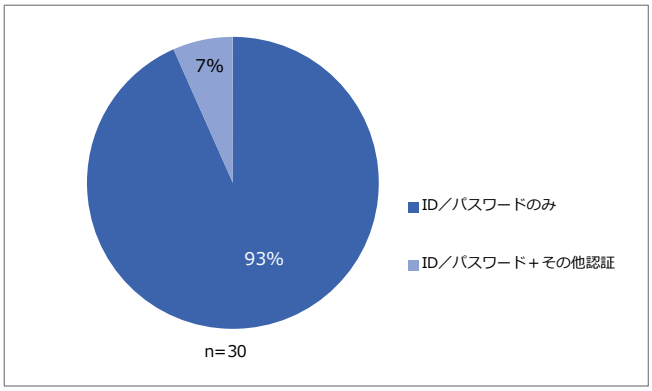


図 10　サービス利用時の認証方式（スマートデバイス）

4.1.3. ID の設定について

ID の設定状況（PC 環境及びスマートデバイス環境）は、メールアドレスを ID として設定できるケースが半数以上を占める。メールアドレスの ID としての設定を許容することは、他のサイトの利用時や普段の連絡のやり取りの中で、漏洩しやすい環境を生み出していると考えられる。また、複数の異なるサービスサイトで同一の ID（メールアドレス）を用いることは、同一人物で

あることを示すことである。漏えいした場合に攻撃者にとってよりなりすましをしやすい情報を提供することとなる。さらに、メールアドレスをスパムメールなどに悪用される恐れもある。

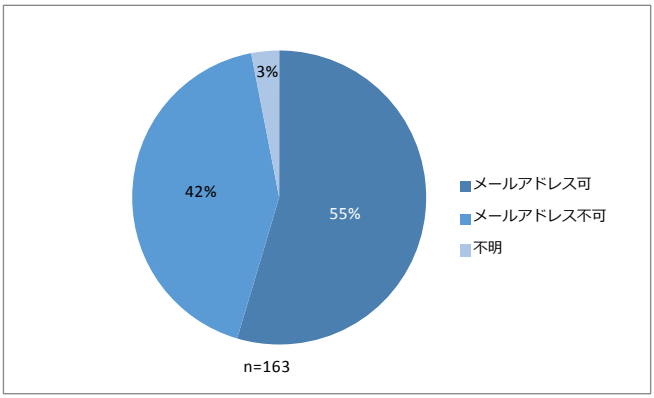


図 11　ID の設定状況

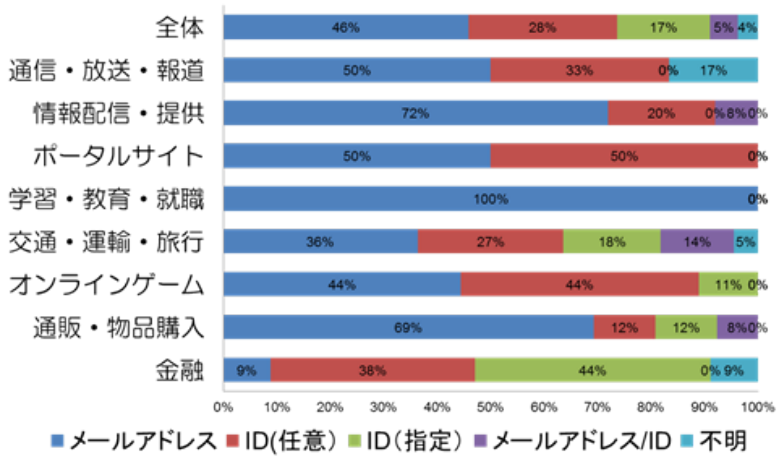
① ID の設定（PC 環境）

サービス分類別（PC 環境）で見ると、通販・物品購入サイト、情報配信・提供サイトでは、メールアドレスを ID として設定することが多い。一方、金融関係のサービスでは、メールアドレスが ID として使われているケースは他サービスに比べて少なく、サービス提供者が ID を自動発行するケースも多く（44%）見られる。

表 28　サービス別 ID の設定状況（PC）

サービス分類	メール アドレス	ID（任意）	ID（指定）	メール アドレス／ID	不明
1）金融	3	13	15	0	3
2）通販・物品購入	18	3	3	2	0
3）オンラインゲーム	4	4	1	0	0
4）交通・運輸・旅行	8	6	4	3	1
5）学習・教育・就職	3	0	0	0	0
6）ポータルサイト	4	4	0	0	0
7）情報配信・提供	18	5	0	2	0
8）通信・放送・報道	3	2	0	0	1
計	61	37	23	7	5

- ID（任意）：サービス利用者が ID を設定
- ID（指定）：サービス提供者が ID を設定
- メールアドレス／ID：利用者がメールアドレス又は ID のどちらかを設定



② ID の設定（スマートデバイス環境）

スマートデバイス環境での調査結果を見ても、メールアドレスが ID として利用されているケースが最も多く、調査対象先の半数を占めている。次いで、サービス利用者が自由に ID を設定するケース（ID（任意））が 27%、メールアドレスと ID を選択できるケース（メールアドレス／ID）が 17%という順となっている。また、ID がサービス提供者から発行されるケース（ID（指定））も一部存在している。

利用者が自由に ID を設定できる場合、設定できる文字数の範囲は 3～32 文字であった。また、設定可能な文字種は「半角英数字」が大半を占め、一部「記号」も使用できるサイトも存在するが、少ない状況である。

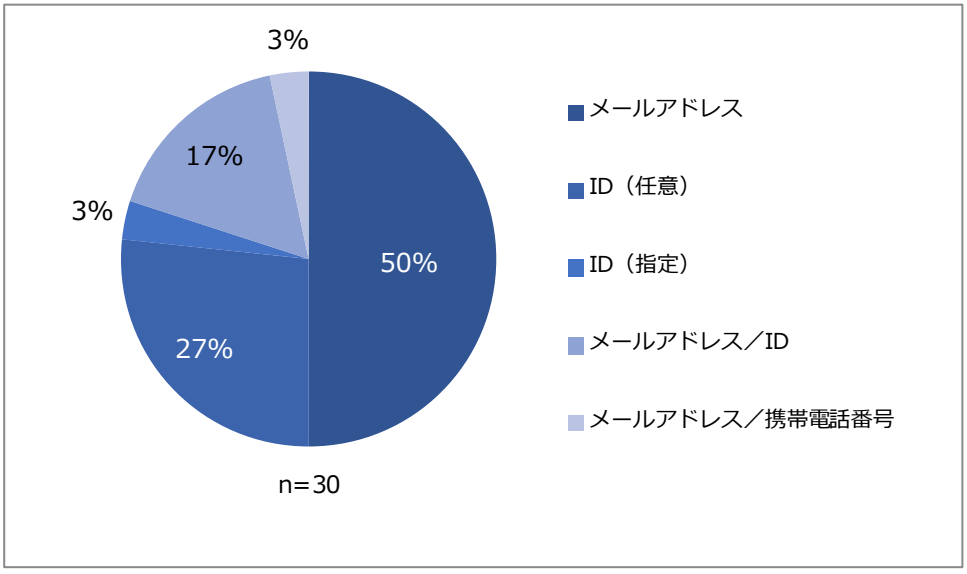


図 12　サービス登録時の ID 設定状況（スマートデバイス）

4.1.4. パスワードの設定状況

① パスワードの自動設定の状況

調査対象先サイトのうち、9 割以上のサイトでパスワードは利用者が登録する形となっており、一部サービス事業者がパスワードを自動発行するケースも見られるが極僅かである。なお、下表では任意設定と自動発行の双方を選択できるサイトは、任意設定と自動発行それぞれに記載している。

表 29　サービス別パスワード設定状況（PC 及びスマートデバイス）

サービス分類	任意設定	自動発行	不明
1）金融	28	1	8
2）通販・物品購入	24	2	0
3）オンラインゲーム	8	0	1
4）交通・運輸・旅行	21	0	1
5）学習・教育・就職	2	1	0
6）ポータルサイト	8	0	0
7）情報配信・提供	22	0	3
8）通信・放送・報道	5	0	1
計	118	4	14

② パスワードの桁数（PC 環境）

パスワードを設定する際の最小桁数は、4～8 桁に分布している。6 桁以下の下限設定をしているインターネットサイトは全体の 57%を占めており、利用者が比較的短いパスワードを設定できる状況となっている。

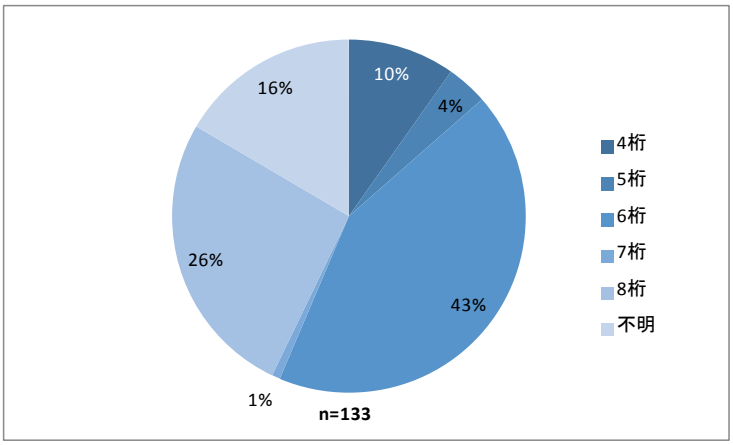
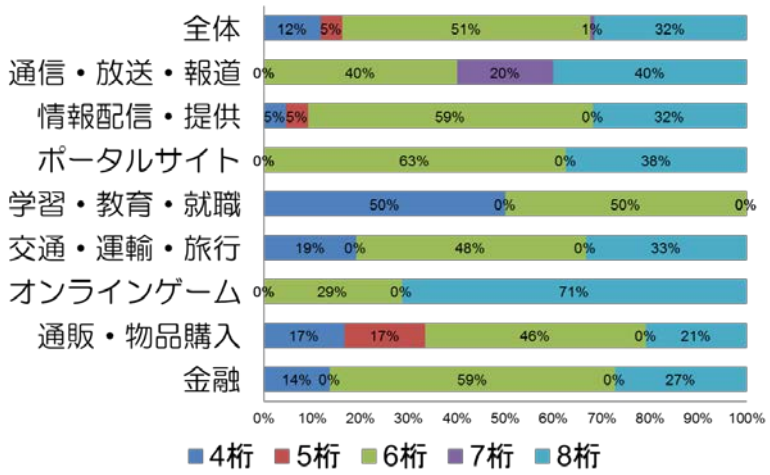


図 13　パスワードを設定する際の最小桁数（PC）

サービス分類別のパスワードの最小桁数を表 30 に示す。図 13 にて示した不明（22(16%)）を除いた最小桁数である。4 桁及び 5 桁等の最小桁数が低い分野は、1)金融、2)通販・物販購入、4)交通・運輸・旅行等のサービスである。

表 30　サービス分類別のパスワードを設定する際の最小桁数

サービス分類	最小桁数				
	4桁	5桁	6桁	7桁	8桁
1）金融	3	0	13	0	6
2）通販・物品購入	4	4	11	0	5
3）オンラインゲーム	0	0	2	0	5
4）交通・運輸・旅行	4	0	10	0	7
5）学習・教育・就職	1	0	1	0	0
6）ポータルサイト	0	0	5	0	3
7）情報配信・提供	1	1	13	0	7
8）通信・放送・報道	0	0	2	1	2
計	13	5	57	1	35



③　パスワードの文字種（PC 環境）

パスワードに使用できる文字種は、「半角英数のみ」のケースが 7 割を占めている。半角英数に加えて「特殊文字」や「記号」を使用できるサービスサイトも一部存在するがそれほど主流とは言えない。

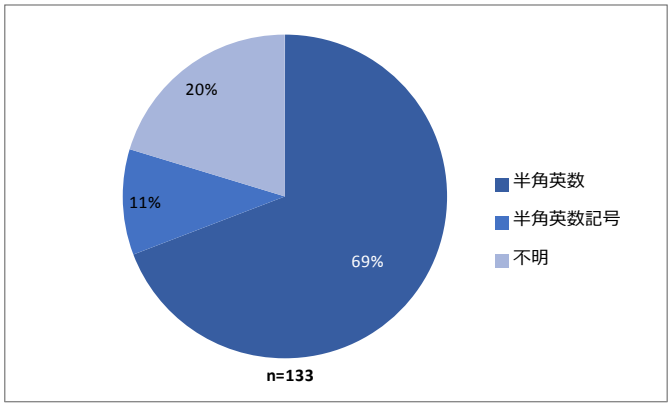
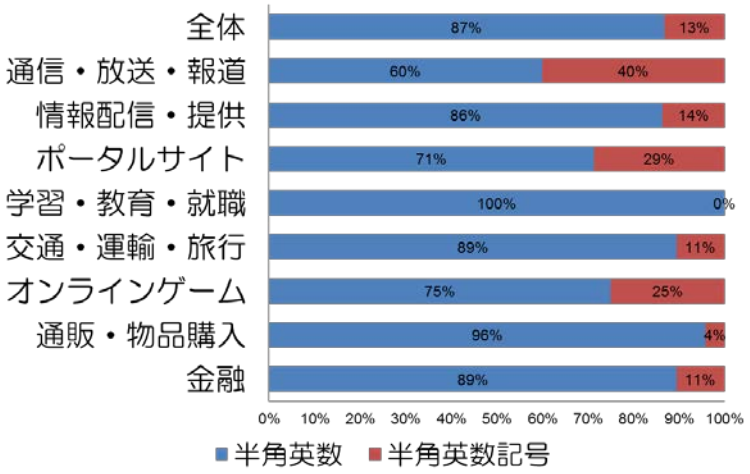


図 14　パスワードに使用可能な文字種（PC）

サービス分類別のパスワードの文字種を表 31 に報告する。図 14 にて示した不明 (27 (20%)) を除いた文字種である。サービス分類に大きな差はなく全体で半角英数が 87%、半角英数記号は 13%であった。

表 31　サービス分類別のパスワードに使用可能な文字種

サービス分類	文字種	
	半角英数	半角英数記号
1）金融	17	2
2）通販・物品購入	23	1
3）オンラインゲーム	6	2
4）交通・運輸・旅行	17	2
5）学習・教育・就職	2	0
6）ポータルサイト	5	2
7）情報配信・提供	19	3
8）通信・放送・報道	3	2
計	92	14



④　パスワードの桁数（スマートデバイス環境）

スマートデバイス環境での調査では、パスワードがサービス提供者により自動設定されるケースは、調査対象先 30 件のうち、1 件のみであり、他の 29 件は、利用者が自由に設定できる形となっている。

パスワードとして設定できる文字数の範囲は、6～32 文字であった。設定文字数の下限は、PC 環境での調査と同様に、6 桁が最も多く 61%を占めており、比較的短いパスワード設定が可能となっている。次いで、8 桁が 32%、残り 7%が 7 桁という状況である。

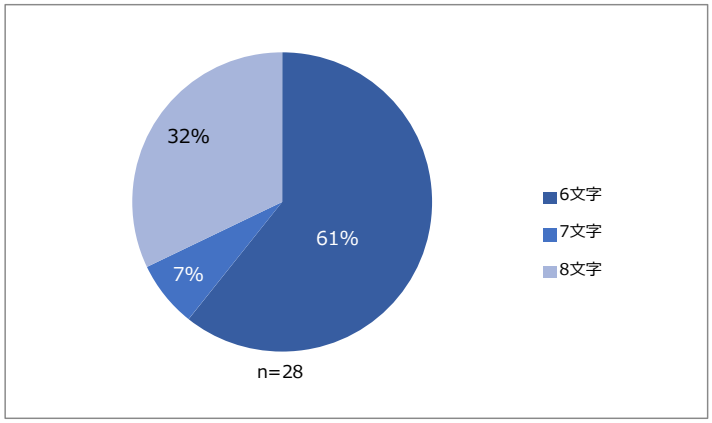


図 15　パスワード最小桁数の状況（スマートデバイス）

⑤ パスワードの文字種（スマートデバイス環境）

パスワードとして設定可能な文字種は、PC 環境と同様に、「半角英数字」が最も多く、全体の83%を占め、使用可能な文字種が少ない状況である。

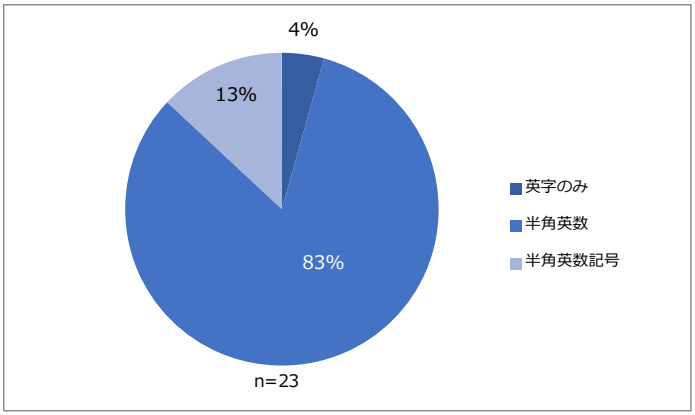


図 16　パスワード使用可能文字種の状況（スマートデバイス）

4.1.5. ID 連携について

PC 環境における ID 連携の有無に関する調査では、76%のサイトが ID 連携を実施していない。一方で、スマートデバイス環境における調査では、調査対象先 30 件のうち、33%（10 件）が連携ありなっている。連携元は、Facebook が 6 件と最も多く、次いで、Google、Twitter、Docomo、au、Linkedin の 2 件であった。

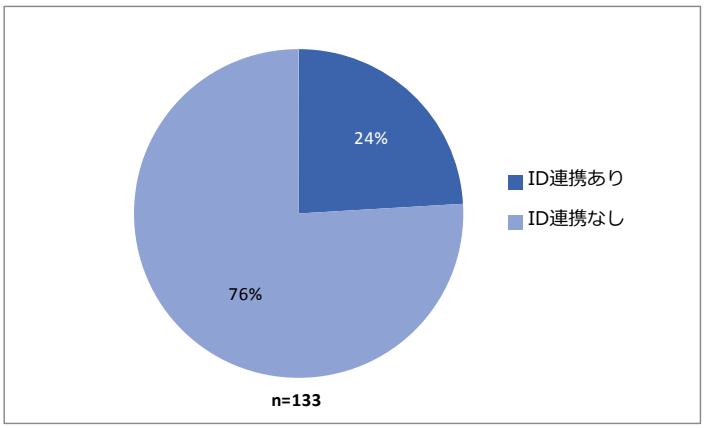


図 17　ID 連携の状況（PC）

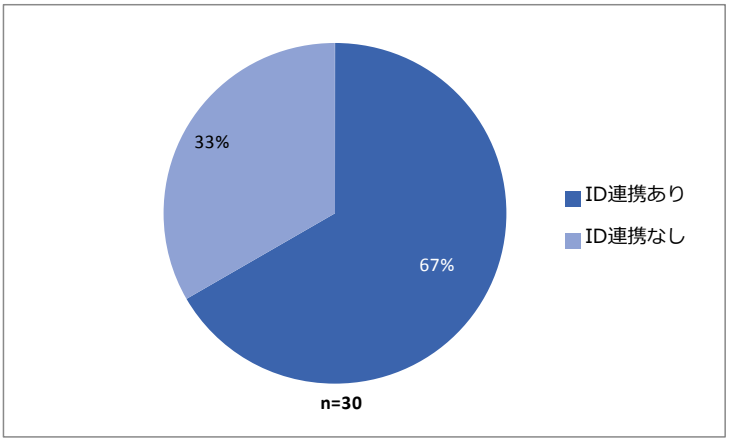


図 18　ID 連携の状況（スマートデバイス）

4.1.6. 認証プロトコルの安全性・SSL 通信の有無

サイトが重要な情報を送受信する際に、安全な通信を実現する SSL 通信[22]を利用しているかの調査結果を示す。調査対象先サイト 133 のうち、128（96%）が SSL 通信方式を採用していた。また、サービス別では、ほとんどのサービスが 9 割以上の割合で SSL 通信方式を採用しているが、3）オンラインゲーム、8）通信・放送・報道　は 8 割台と他サービスに比べると比較的低い。EV-SSL（脚注参照）については、調査対象先サイト 133 のうち、48（36%）が導入している。サービス別では、ほとんどのサービスが 2 割程度の EV-SSL 実施率であるのに対して、金融は 85%と他のサービスに比べ高い。

表 32　SSL 通信

	調査数	SSL	EV
1）金融	34	34　(100%)	29　(85%)
2）通販・物品購入	26	25　(96%)	5　(19%)
3）オンラインゲーム	9	8　(88%)	2　(22%)
4）交通・運輸・旅行	22	22　(100%)	5　(22%)
5）学習・教育・就職	3	3　(100%)	0　(0%)
6）ポータルサイト	8	8　(100%)	2　(25%)
7）情報配信・提供	25	23　(92%)	4　(16%)
8）通信・放送・報道	6	5　(83%)	1　(16%)
計	133	128　(96%)	48　(36%)

[22] SSL 通信とは、Secure Sockets Layer による通信であり、公開鍵証明書によって通信相手となるインターネットサービス提供者が運営するサーバの認証を行うとともに、通信の暗号化及び改ざん検知を提供する。また、EV-SSL は、extended validation SSL の略であり、公開鍵証明書の発行審査（身元確認等）において、通常の SSL よりも厳格な審査を行うものである。

4.2. 利用者側

4.2.1. 調査実施の概要

本調査では、個人を対象としたウェブアンケート調査を実施した。調査対象等の実施概要は、**表 33** の通りである。20～60 代の男女 2,060 名を対象に実施した。

表 33 実施概要

項目	概要
調査実施	ウェブアンケート調査
調査対象	インターネットモニタ会社の保有する台帳から対象者を選定
回収件数	2,060 件 20代 30代 40代 50代 60代 計 男性 206 206 206 206 206 1,030 女性 206 206 206 206 206 1,030 計 412 412 412 412 412 2,060
設問数	40 問
調査実施期間	2014 年 4 月 4 日～2014 年 4 月 7 日
調査項目	• 個人がサービスサイトを利用する際に登録する情報 • 個人がサービスサイトを利用する際に使用する認証方式の種類 • 個人による ID・パスワードを記憶するためのツールの利用状況 • ID やパスワードへの条件とその強度についての個人の知識の状況 • 個人の認証方式と登録に対して、抵抗感、受容の程度、使いやすさ、必要性、サービスサイト種別との関係などの意識 • その他、オンライン本人認証方式の安全性を保持するために必要と考えられる項目

4.2.2. 調査仮説の設定

本調査では、「パスワードの安全性とデータの価値の関係性」、「パスワードの安全性の知識と実態」、「ID 設定の意識」、「ID／パスワードの安全性と運用の関係性」の観点から仮説を設定して設問を作成し、結果の検証を行った。本調査で設定した仮説とこれを検証するための設問は**表 34** の通りである。

表 34 本調査における仮説と設問の対応

仮説		対応する設問
仮説 1	設定するパスワードの安全性は保護すべきデータの価値に依存する。	Q19-21 あなたが、金銭に関連したサービスサイト／個人的な情報に関連したサービスサイト／その他のサービスサイトを利用する際に望ましいと思う本人確認方法（認証方式）について、以下のそれぞれについてお答えください。
仮説 2	パスワードの安全性への知識はあるが、実際はその通りに設定していない	—
	(2-1)パスワードの安全性についての知識がある	Q2 パスワードを作成する際、安全性を高めるために必要だと思う事項で当てはまるもの全てをお答えください。
	(2-2)パスワードの文字数は少ない方が楽である	Q3-5 あなたが金銭に関連したサービスサイト／個人的な情報に関連したサービスサイト／その他のサービスサイトを利用する際に用いるパスワードについてお答えください。あなたは、どのようなパスワードを設定していますか。
	(2-3)覚えやすいパスワードを設定している	Q3-5 あなたが金銭に関連したサービスサイト／個人的な情報に関連したサービスサイト／その他のサービスサイトを利用する際に用いるパスワードについてお答えください。あなたは、どのようなパスワードを設定していますか。
	(2-4)複数のサイトで同一のパスワードを設定している	Q6 あなたは、複数のサービスサイトで同一のパスワードを利用していますか。
	(2-5)パスワードを変更することは少ない	Q8 あなたは、パスワードをどのくらいの周期で変更していますか。 Q9 あなたは、パスワードをどのタイミングで変更していますか。複数サイトを利用している場合は、最も利用頻度の高いサービスについてお答えください。
仮説 3	ID の設定に対して安全性への知識はない	—
	(3-1)ID の設定に対して安全性を意識することはない	Q28-30 あなたが、金銭に関連したサービスサイト／個人的な情報に関連したサービスサイト／その他のサービスサイトを利用する際に用いる ID についてお答えください。
	(3-2)複数のサイトで同一のIDを設定している	Q28-30 あなたが、金銭に関連したサービスサイト／個人的な情報に関連したサービスサイト／その他のサービスサイトを利用する際に用いる ID についてお答えください
	(3-3)ID にメールアドレスを設定している	Q28-30 あなたが、金銭に関連したサービスサイト／個人的な情報に関連したサービスサイト／その他のサービスサイトを利用する際に用いる ID についてお答えください
仮説 4	ID/パスワードの設定には、安全性と運用とのトレードオフが存在する。 ID/パスワードについては、その安全性、運用に対するトレードオフがある。	Q7 あなたが、いくつかのサービスで同一のパスワードを利用している理由をお答えください。

4.2.3. 調査結果

主たるアンケート調査の結果を示す。この他の結果については巻末の付録 2 を参照。

① 回答者の属性

回答者のインターネットに接続している端末の状況を示す。本調査の回答者は、93.0%がパソコンからインターネットに接続し、49.6%がスマートフォンからインターネットに接続している。タブレット端末からインターネットに接続している回答者も 15.6%いる。

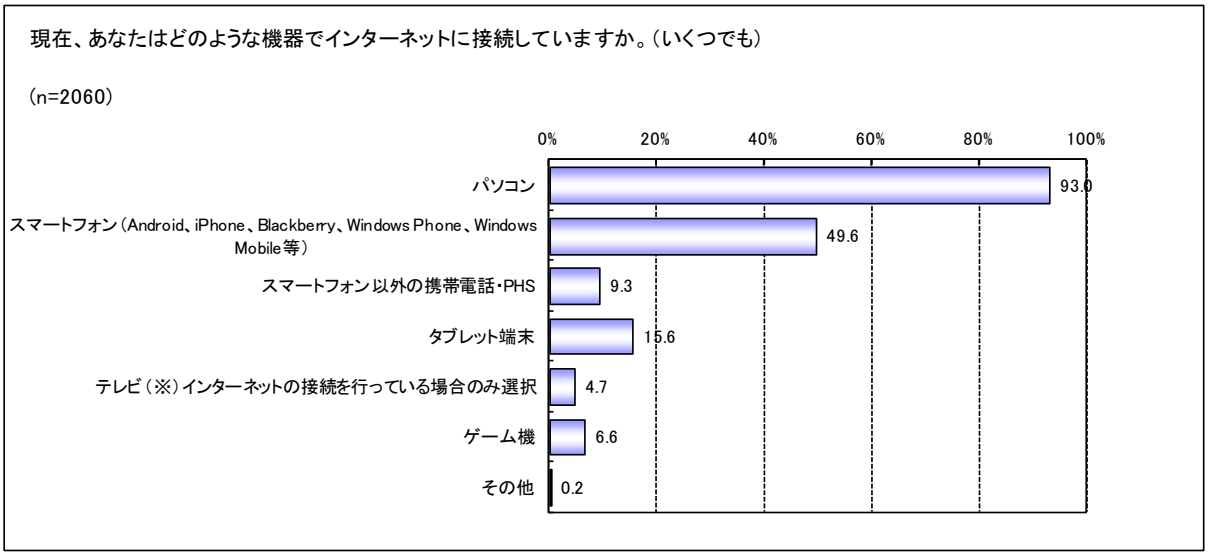


図 19　インターネット接続機器

利用しているインターネットサービスの結果を示す（図 20）。本調査はウェブアンケート調査であるため、「アンケートサイト」の利用が高めに出ているが、これを除くと、総合通販が 58.4%、銀行・信託が 56.6%、クレジットカードが 45.1%となっている。後述の金銭に関するサービスサイトの利用も多い。

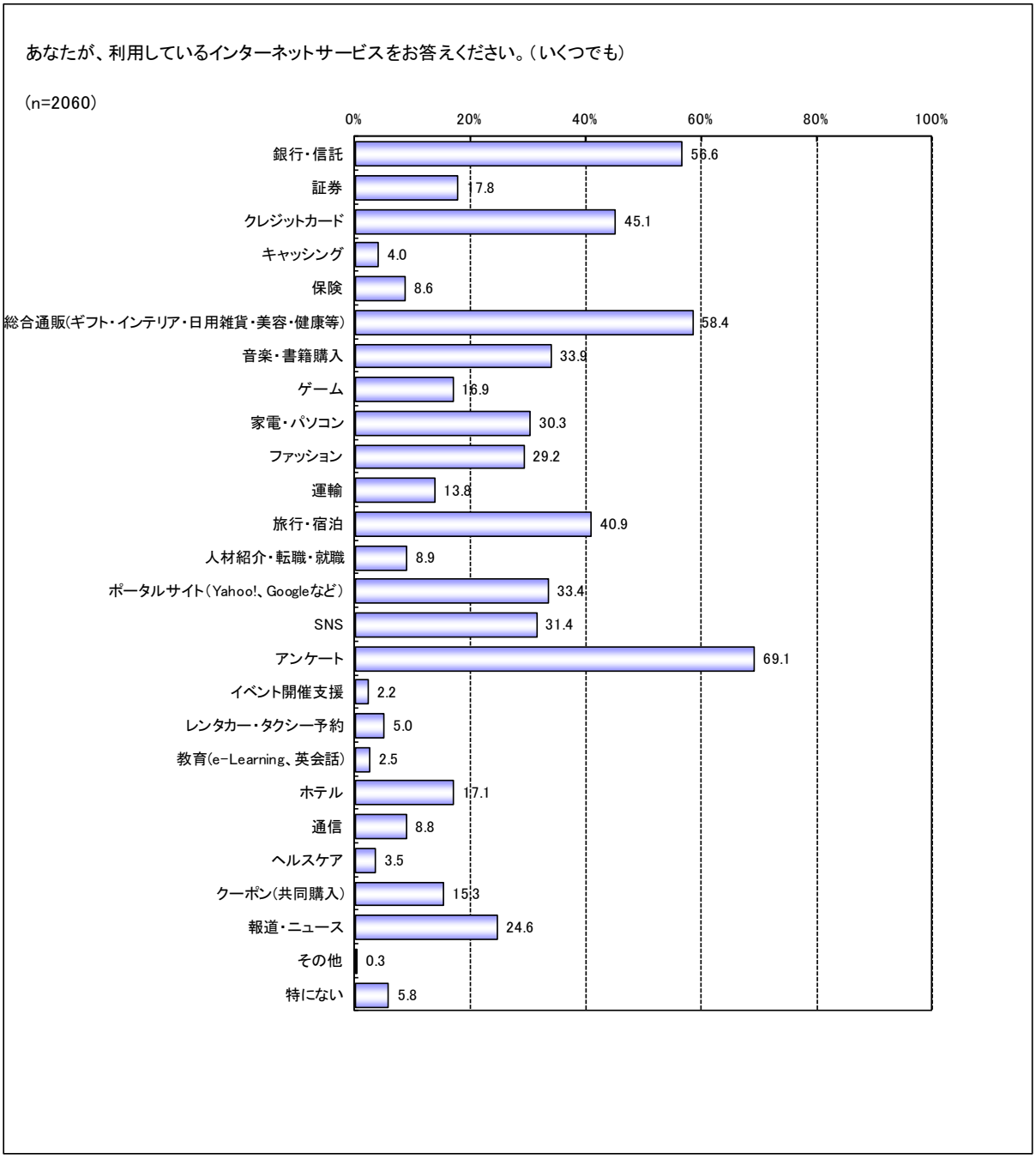


図 20　インターネット利用状況

② パスワード利用の実態

図 21 に、パスワードに関する知識として、パスワードを作成する際の安全性を高めるために必要な事項について尋ねた結果を示す。

この結果によると、「英字（大文字、小文字含む）、数字、記号を組み合わせた文字列であること」、「名前や誕生日など推測されやすい文字列を使わないこと」は、7 割を超える回答者が認識している。また、「文字数は 8 文字以上であること」についても 67.2%と、7 割近い回答者が認識している。一方、他のサイトで用いたパスワードを流用しないことについては 40.9%の回答者が認識している状況である。

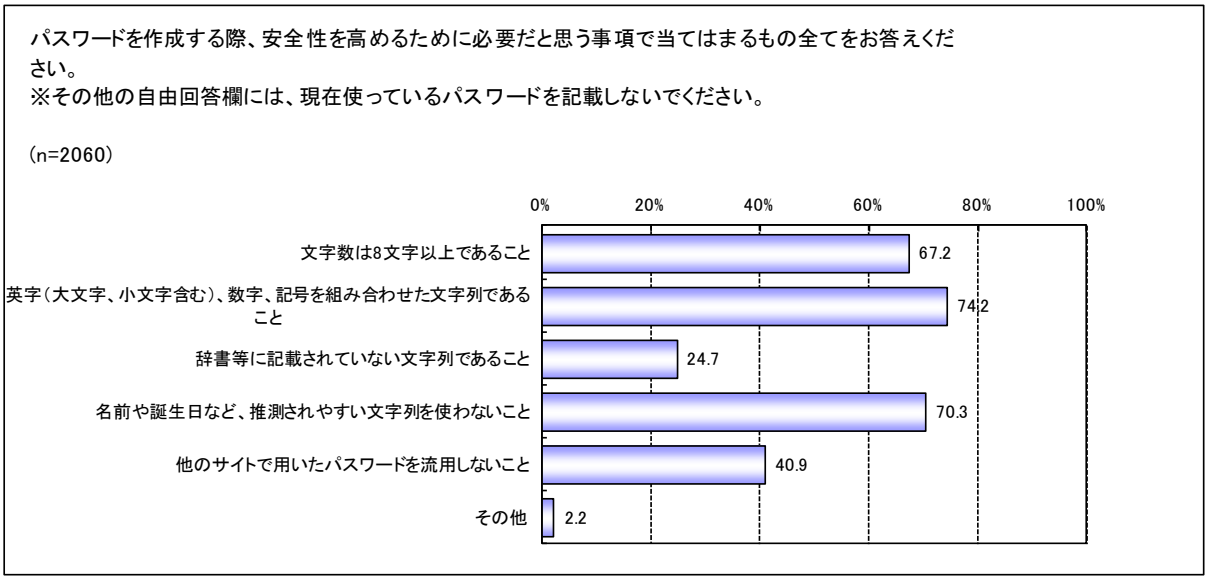


図 21　パスワードに関する知識

サービスサイト別にパスワードや ID の利用実態や意識について把握を行った。各サービスサイトの定義は**表 35** の通りである。

表 35　サービスサイトの定義

種別	定義
金銭に関連したサービスサイト	クレジットカード情報や銀行口座情報等を取扱うサービス。 （例：銀行のオンラインバンキングのサイト、ショッピングサイト等）
個人的な情報に関連したサービスサイト	ブログやマイクロブログ及び SNS 等を含む個人的な情報や近況を発信するサービスのことであり、情報発信先は特定の個人に限定した場合も限定しない場合も含む。 （例：Twitter、Facebook 等）
その他のサービスサイト	金銭情報や個人情報の配信を行わないサービスのことであり、主に情報収集を目的に利用するサービス。（例：会員制のニュースサイト等）

図 22 に金銭に関連したサービスサイトのパスワードの構成について尋ねた結果を示す。この結果によると、パスワードの構成として最も多いのは、「ランダムな英数字の組み合わせ」(26.8%)である。これに次いで、「ご自身・ご家族等のお名前にちなんだもの」(19.0%)、「ご自身・ご家族等の誕生日にちなんだもの」(17.2%)がそれぞれ 2 割近い結果となっている。

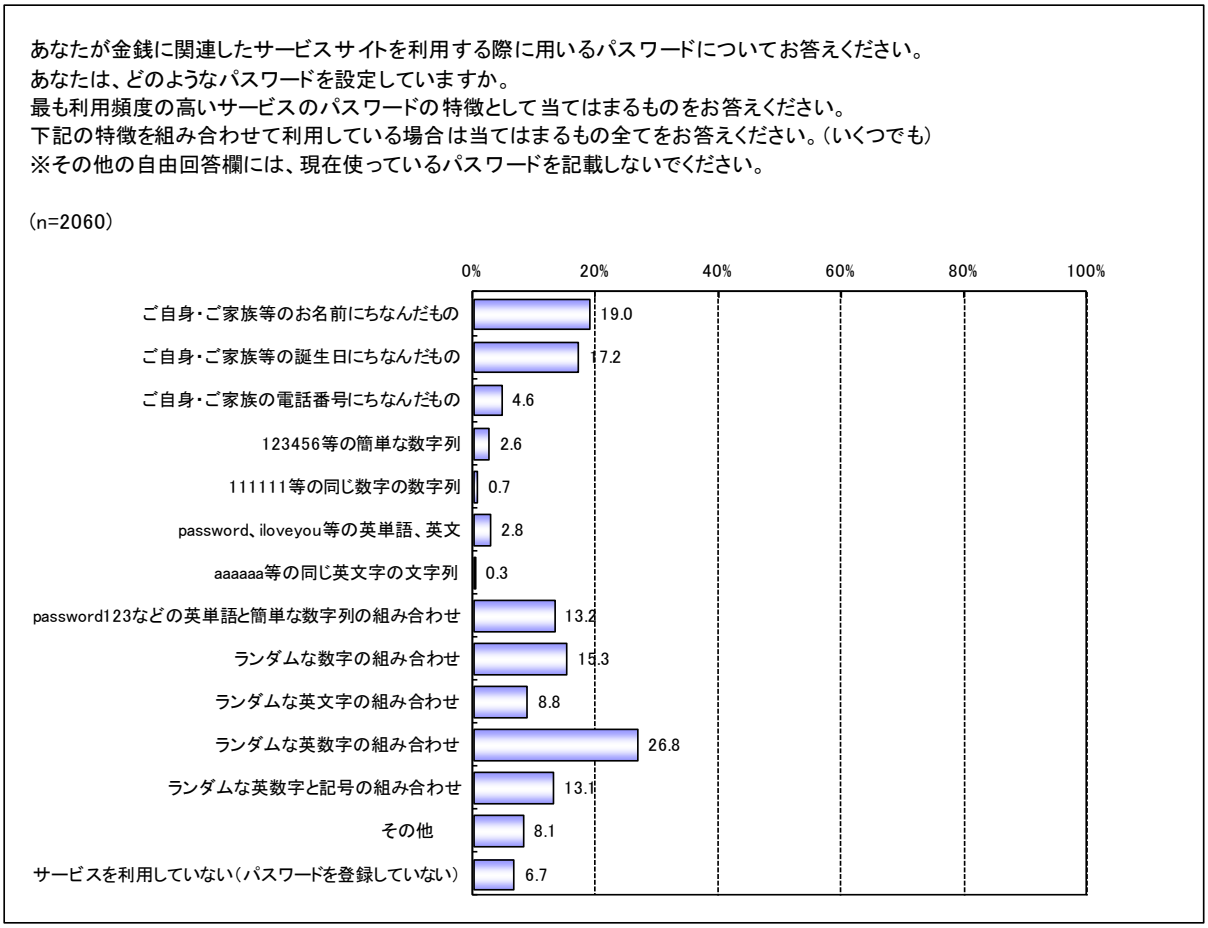


図 22　パスワードの構成（金銭に関連したサービスサイトの利用）

図 23 に、個人的な情報に関連したサービスサイトのパスワードの構成の結果を示す。この結果によると、パスワードの構成として最も多いのは、「ランダムな英数字の組み合わせ」（26.2%）である。これに次いで、「ご自身・ご家族等のお名前にちなんだもの」（21.1%）、「ご自身・ご家族等の誕生日にちなんだもの」（17.9%）が 2 割近い結果となっている。

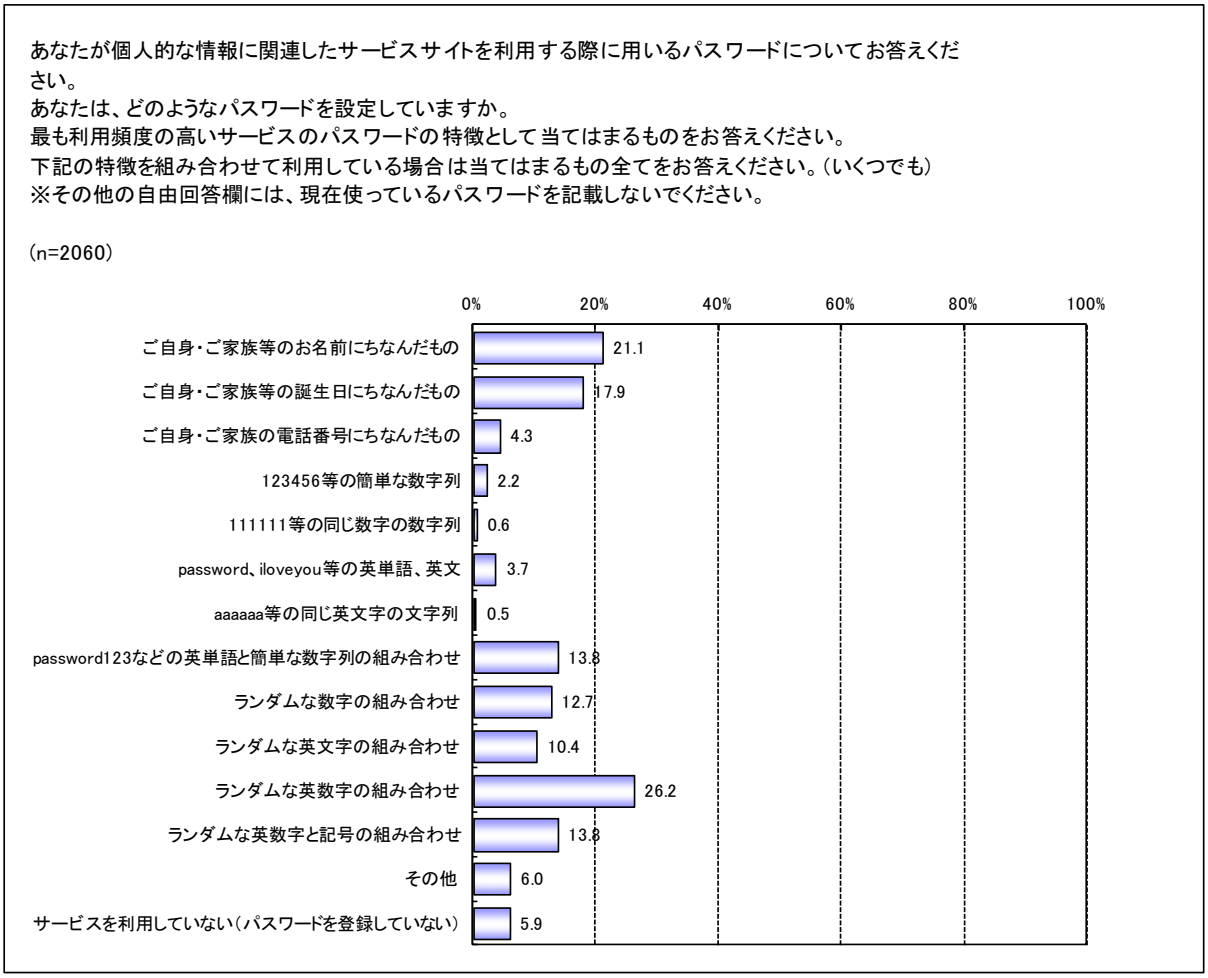


図 23　パスワードの構成（個人的な情報に関連したサービスサイトの利用）

図 24 に、その他のサービスサイトのパスワードの構成の結果を示す。この結果によると、パスワードの構成として最も多いのは、「ランダムな英数字の組み合わせ」（25.3%）である。これに次いで、「ご自身・ご家族等のお名前にちなんだもの」（21.1%）、「ご自身・ご家族等の誕生日にちなんだもの」（17.8%）が 2 割近い結果となっている。

このように、サイトの種別によって、パスワードの構成に大きな変化はないという傾向があった。

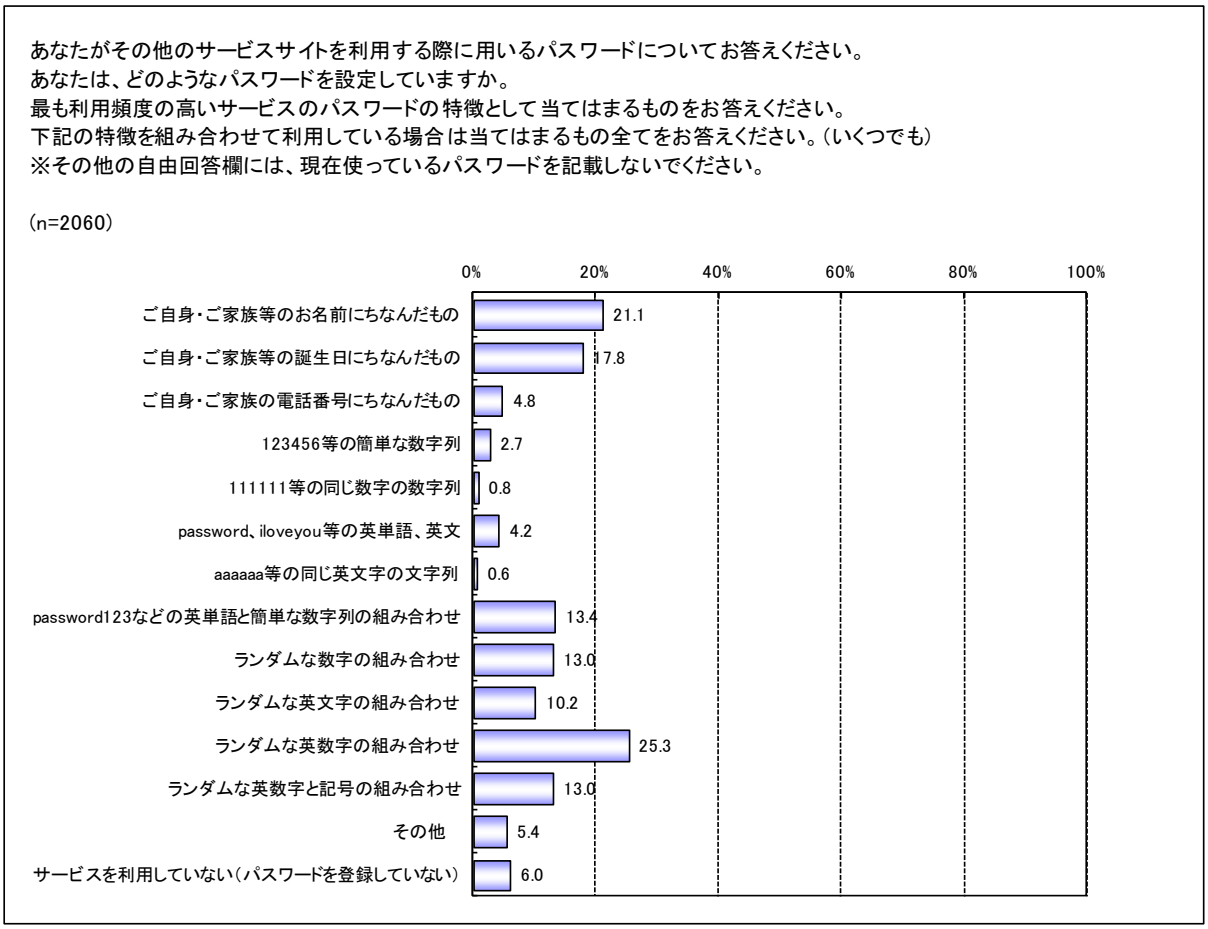


図 24　パスワードの構成（その他のサービスサイトの利用）

次に、パスワードの使いまわしについて尋ねた結果を示す。図 25 に、金銭に関連したサービスサイトの状況を示す。この結果によると、「他のサービスサイトと同一のパスワードは利用していない」という結果が 43.3%と最も多いが、金銭に関連したサービスサイトで、同一のパスワードを利用している回答者も 25.4%いるという結果となった。金銭に関連したサービスサイト以外での使い回しは少ないが、それぞれ 12～13%程度は使いまわしているという結果となった。全体として、「他のサービスと同一のパスワードは利用していない」と「複数のサービスサイトを利用していない」を除くと、41.8%がパスワードを使いまわしていることになる。

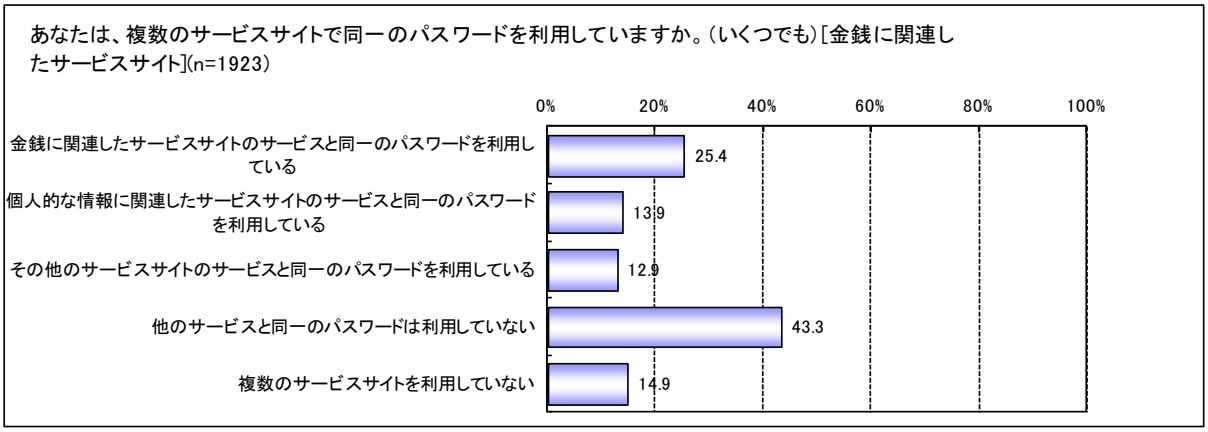


図 25　パスワードの使い回しの状況（金銭に関連したサービスサイトの利用）

図 26 に、個人的な情報に関連したサービスサイトのパスワードの使い回しの状況の結果を示す。この結果によると、「他のサービスサイトと同一のパスワードは利用していない」という結果が 32.0%と最も多いが、個人的な情報に関連したサービスサイト同士で同一のパスワードを利用している回答者も 25.6%いるという結果となった。金銭に関連したサービスサイトの利用と比較すると、パスワードを使いまわして利用している傾向が読み取れる。

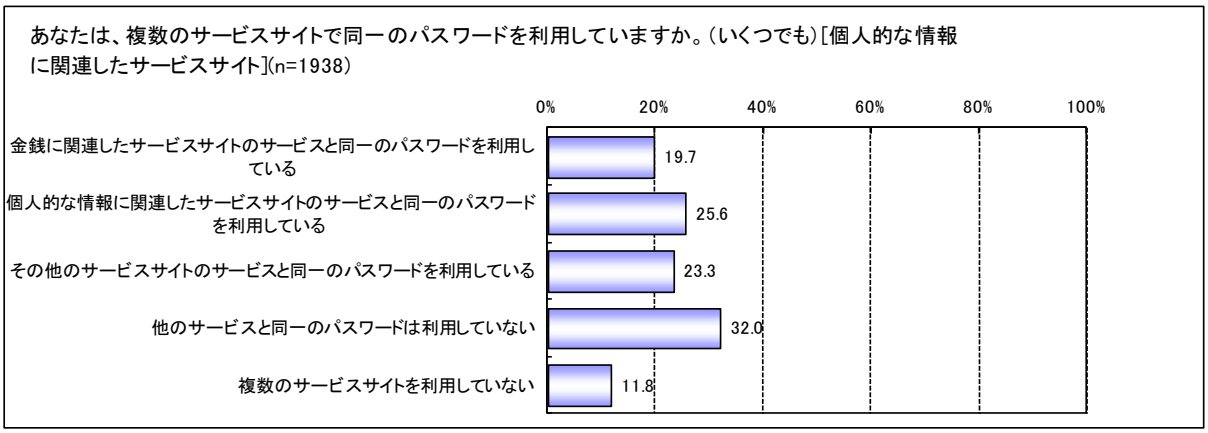


図 26　パスワードの使い回しの状況（個人的な情報に関連したサービスサイトの利用）

図 27 に、その他のサービスサイトのパスワードの使い回しの状況の結果を示す。この結果によると、「他のサービスサイトと同一のパスワードは利用していない」という結果が 30.4%と最も多いが、その他のサービスサイト同士で同一のパスワードを利用している回答者も 30.4%いるという結果となった。個人的な用法に関連したサービスサイトと同様で、金銭に関連したサービスサイトの利用と比較すると、何らかの形でパスワードが使いまわされている傾向が読み取れる。

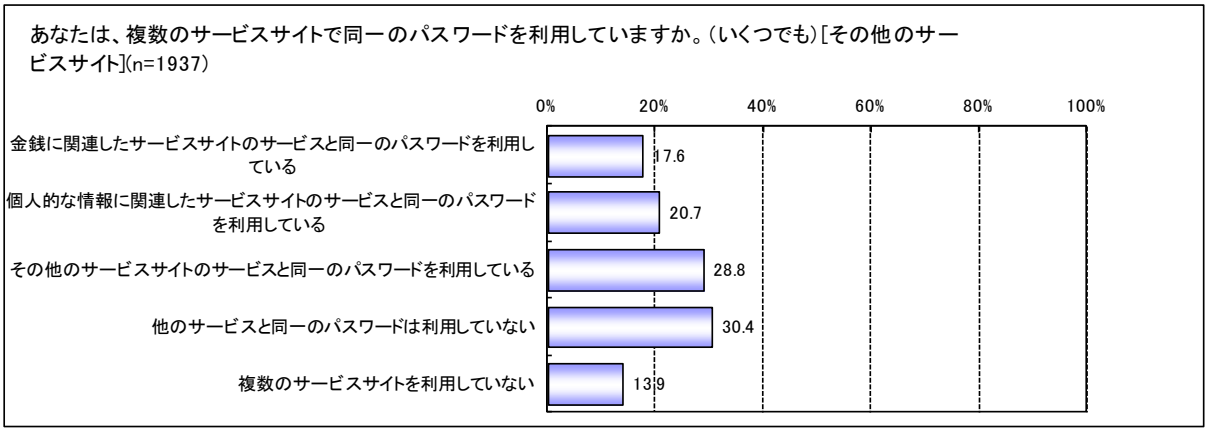


図 27　パスワードの使い回しの状況（その他のサービスサイトの利用）

図 28 に、同一のパスワードを利用している理由の結果を示す。この結果によると、「(パスワードを同一にしないと）パスワードを忘れてしまうから」が 64.1%で最も多い。また、「複数のパスワードを管理するのが面倒だから」も過半数を超える 51.3%となった。

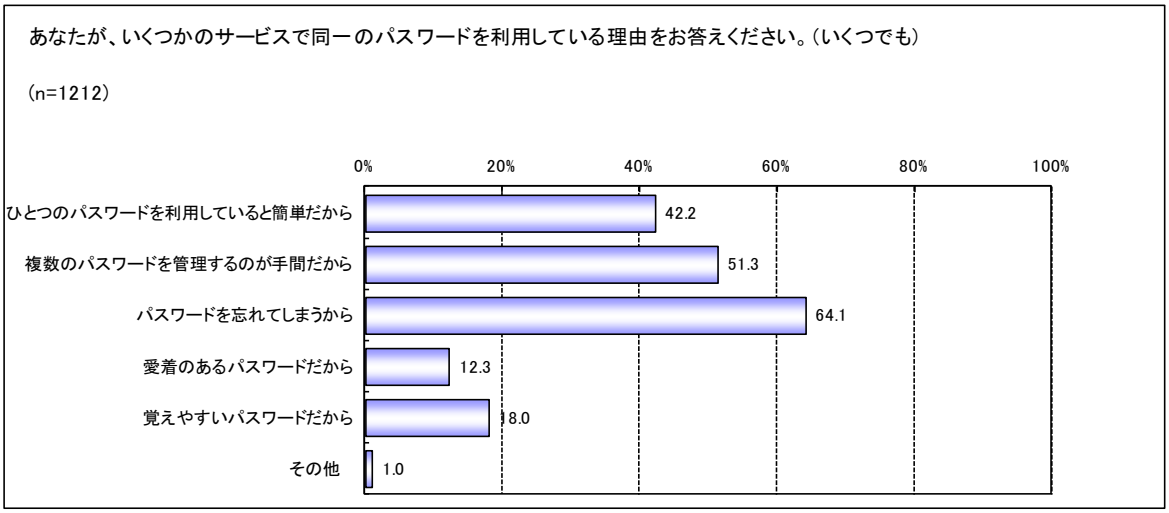


図 28　同一のパスワードを利用している理由

次に、パスワードの管理として、「パスワード変更の周期」の実態について図 29 に示す。金銭に関連したサービスサイトでは、41.3%が変更を実施していない。その他のサービスサイトでは、51.0%がこれまでにパスワードの変更を行っていない。1 年以上の周期で変更を行った回答者は 3 割程度含まれる。個人的な情報に関連したサービスサイトで、これまでに変更をしたことのない回答者は、46.9%である。金銭に関連したサービスサイトよりは長く、その他のサービスサイトよりは短い周期でパスワードの変更が行われている。

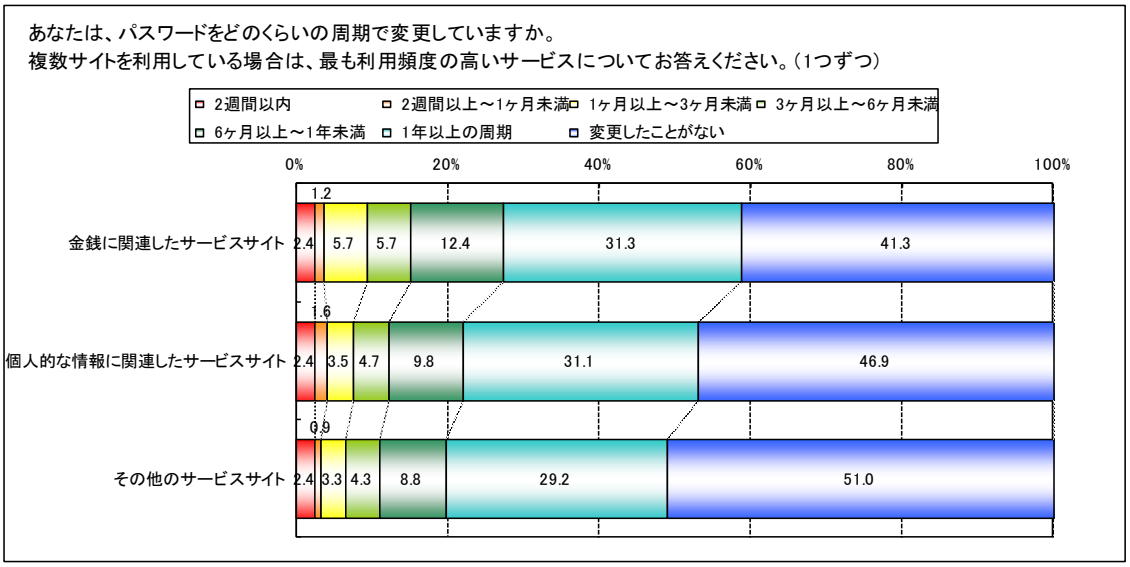


図 29　パスワードの変更周期

図 30 に、パスワード変更のタイミングの結果を示す。この結果によると、金銭に関連したサービスサイトでは、「変更を促す警告によって変更を実施する」回答者が 65.5%である。個人的な情報に関連したサービスサイト、その他のサービスサイトも 6 割近い回答者が変更を行っている。ただし、個人的な情報に関連したサービスサイト、その他のサービスサイトは、2 割程度の回答者が変更を促す警告を受けても、パスワードの変更を実施していない。

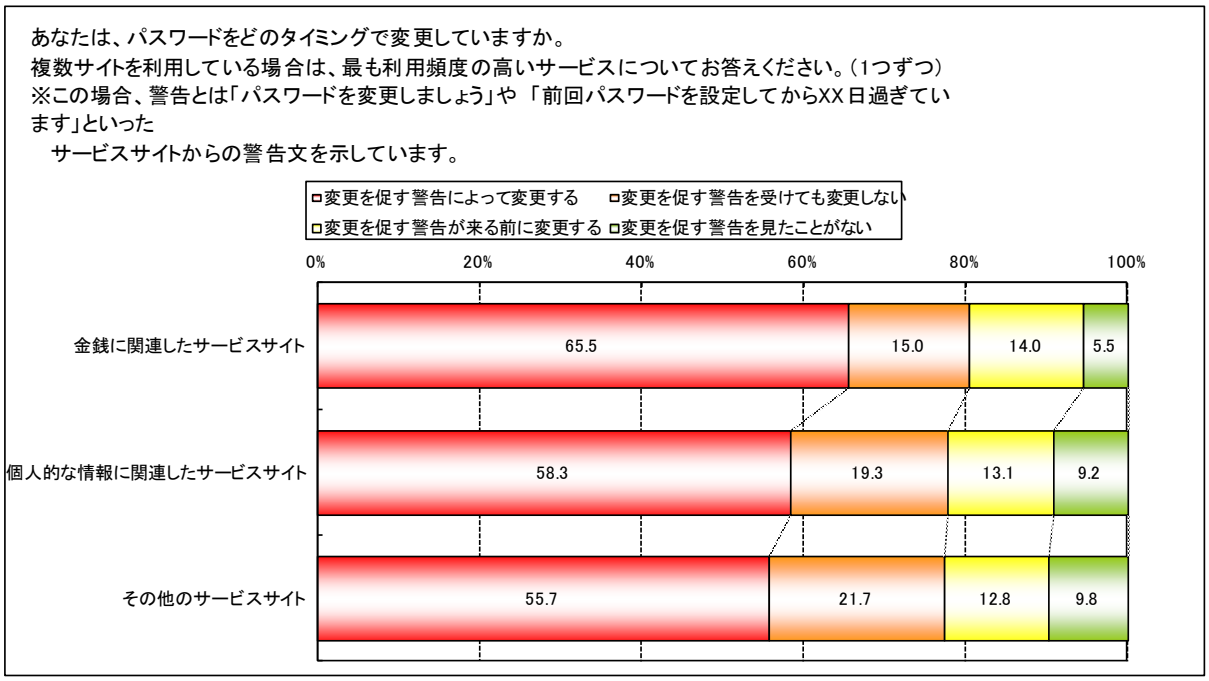


図 30　パスワードの変更のタイミング

③ ID の利用実態

図 31 に、金銭に関連したサービスサイトの ID の構成の結果を示す。この結果によると、任意の英単語と数字の組み合わせが 46.4%と最も多い。これに、ランダムな英数字の組み合わせが 29.4%と続く。他のサービスサイトと比較して、メールアドレスの利用は少ないが、金銭に関連するサイトでも 17.3%の回答者が利用しているという結果となった。

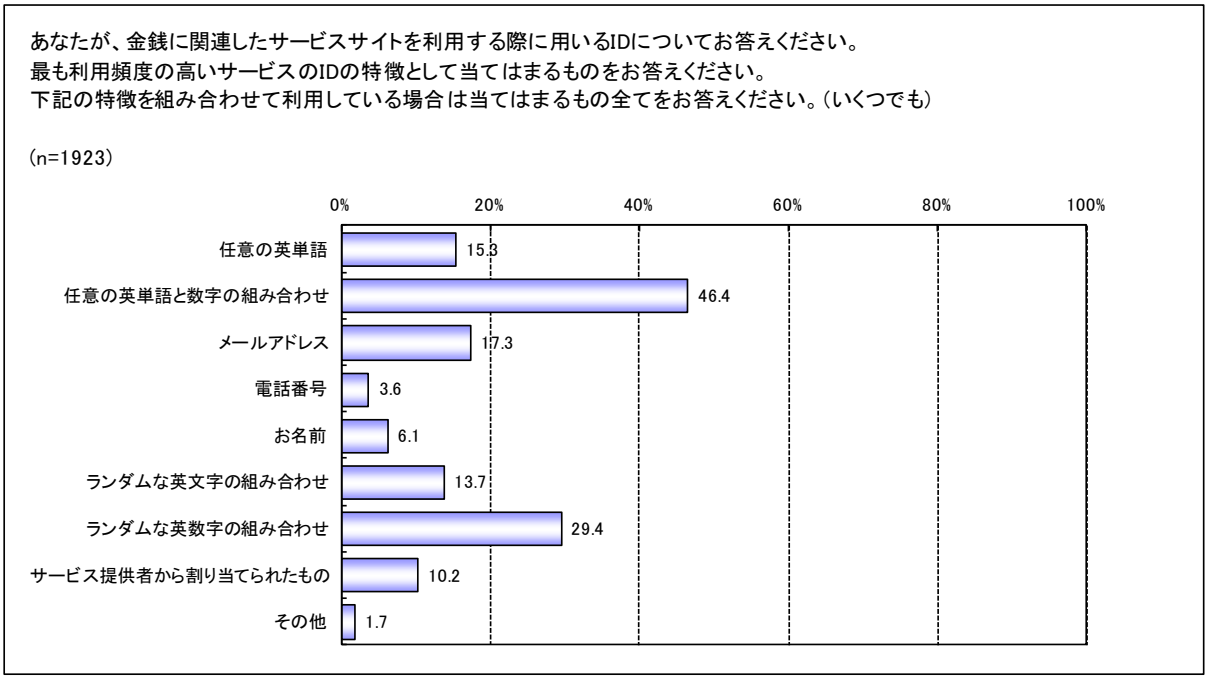


図 31　ID の構成（金銭に関連したサービスサイト）

図 32 に、個人的な情報に関連したサービスサイトの ID の構成の結果を示す。この結果によると、任意の英単語と数字の組み合わせが 43.9%と最も多い。これに、ランダムな英数字の組み合わせが 29.2%と続く。メールアドレスを利用している回答者は 22.9%となった。

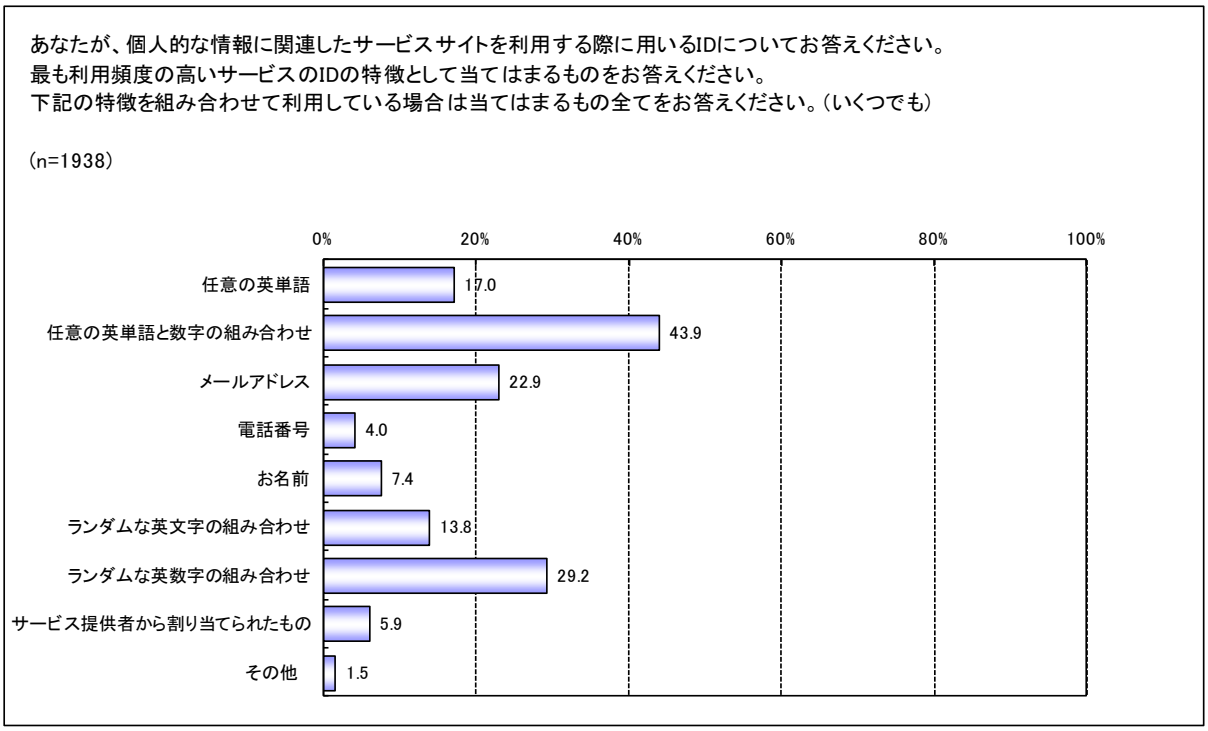


図 32　ID の構成（個人的な情報に関連したサービスサイト）

図 33 に、その他のサービスサイトの ID の構成の結果を示す。この結果によると、任意の英単語と数字の組み合わせが 43.4%と最も多い。これに、他のサービスサイトと同様に、ランダムな英数字の組み合わせが 28.0%と続く。メールアドレスを利用している回答者は金銭に関連したサービスサイト、個人的な情報に関連したサービスサイトより多く、26.3%であった。

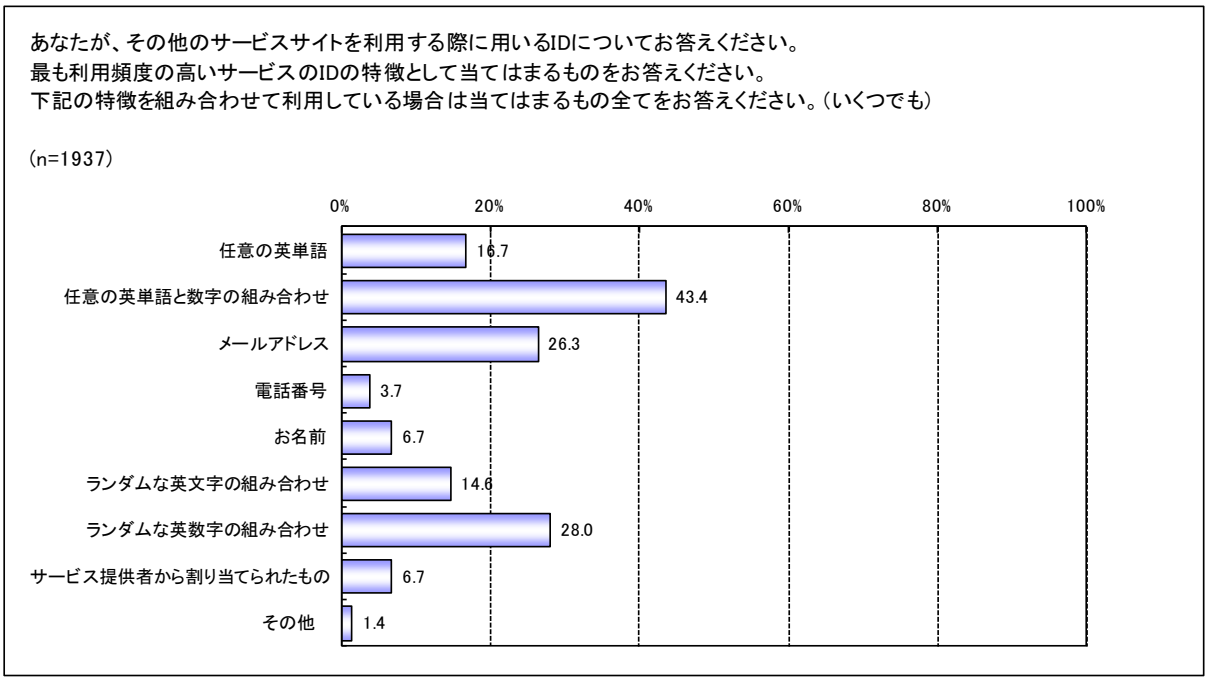


図 33　ID の構成（その他のサービスサイト）

④ 利用者の ID やパスワードの保有状況

図 34 に、インターネット上のサービスサイトを利用するために保有している ID の数の結果を示す。最頻値は、3 個である(19.9%)。1～5 個までで回答者の 63.4%を占める。6～10 個までは 23%（累計で 86.4%）、11~15 個までが 4.3%(累計で 90.7%)である。

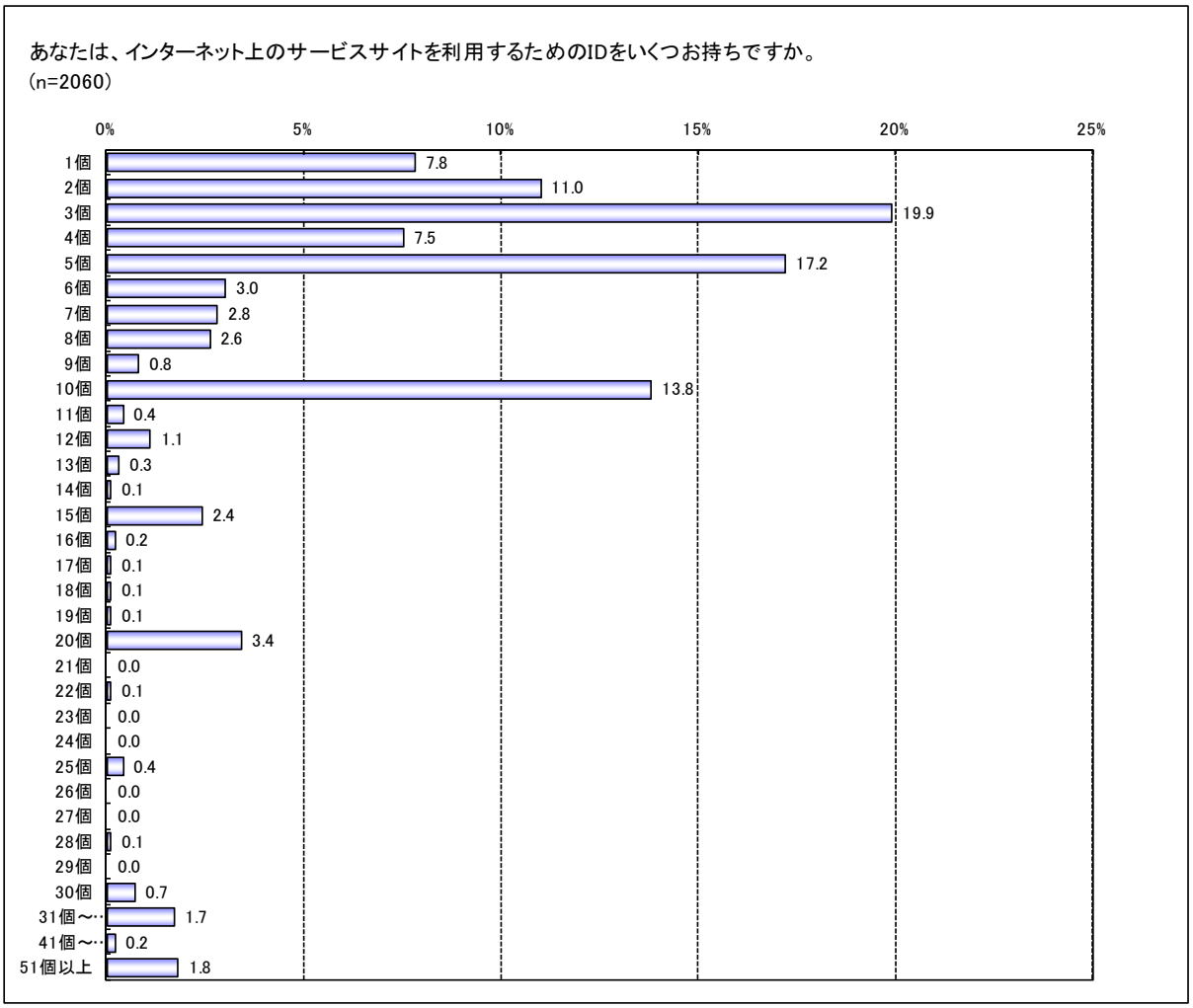


図 34　利用しているサービスサイトの ID の数

図 35 に、記憶できると自信のある ID の数の結果を示す。この結果によると、3 個が最も多く、約 3 割を占める。0 個（ID は覚えられない）の回答者は 2.5%となっている。0～5 個までで回答者の 85.1%を占め、0～10 個までの回答者の累計は約 95%となる。

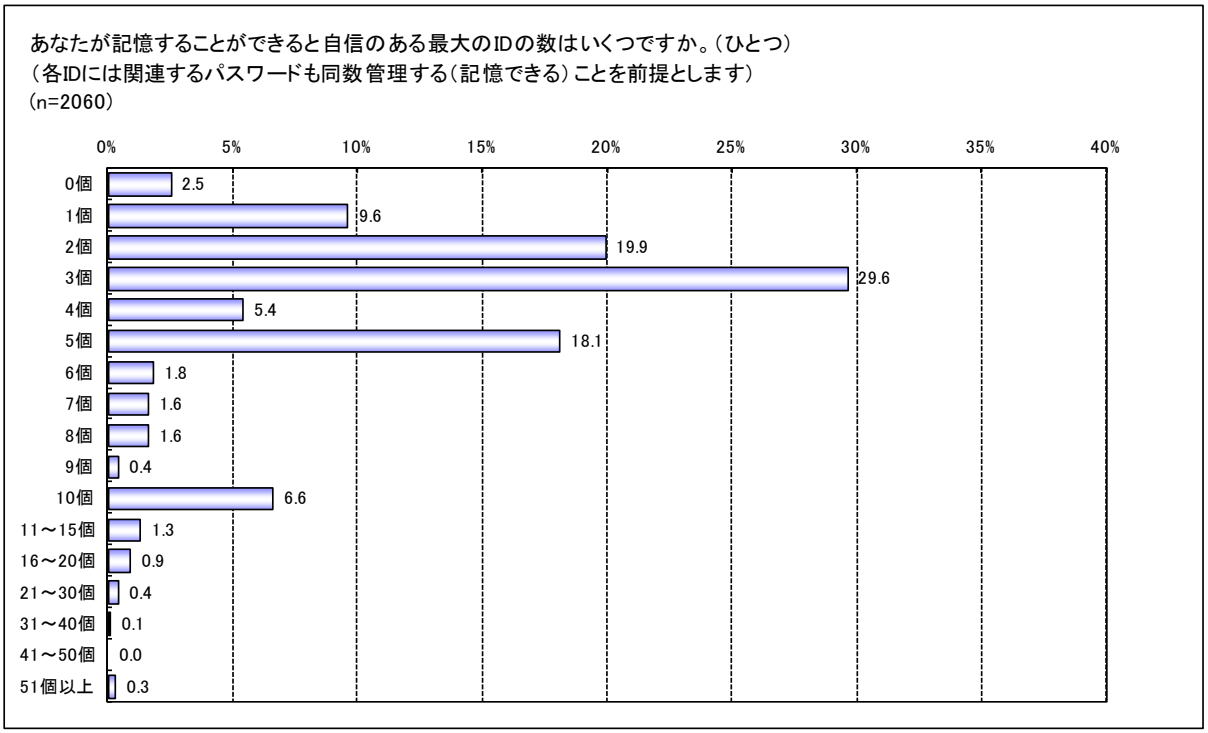


図 35　記憶できる ID の数

図 36 に、ID・パスワードの保管方法の結果を示す。この結果によると、「記憶している」が 65.5%と最も多い。「紙に記載して保管している」回答者も 42.2%いる。パソコン内部に記録している回答者も 21.5%見られるが、インターネットブラウザに記憶（12.1%）させていたり、パスワード管理ツールを利用（6.0%）している回答者は少ない。

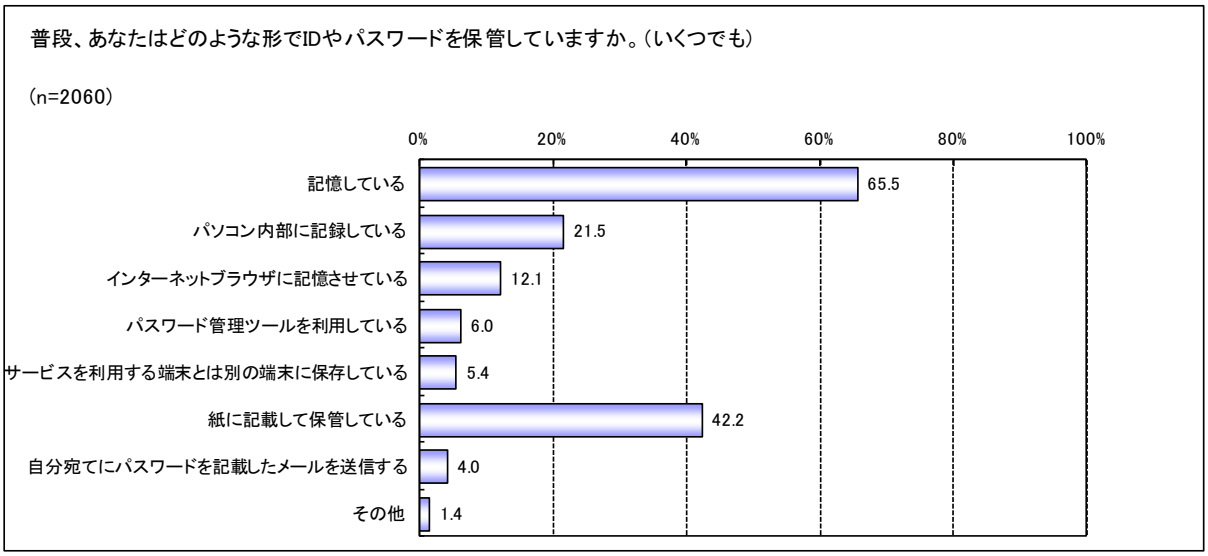


図 36　ID やパスワードの保管方法

図 37 に、記憶できる ID の個数を上回っている場合にさらにサービスを追加するかどうかについて意向を尋ねた結果を示す。この際、「記憶ではなく、メモなどに記録する」が 42.6%と最も多く、「他のサービスと同じものを登録する（ID を使いまわす）」が 17.8%と続く結果となった。専用のツールなどで ID を管理するという回答は 10.2%であった。

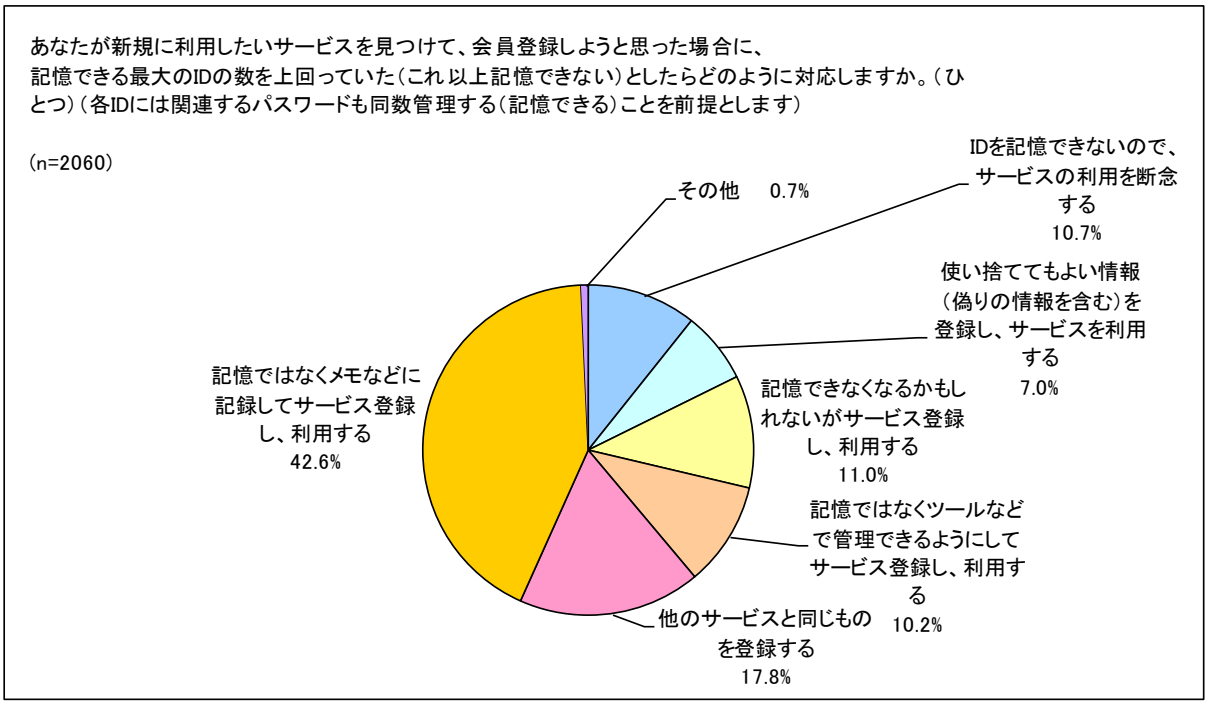


図 37　記憶できる ID の数を上回るサービスサイトの取り扱い

図 38 に、ショッピングサイトの例を取った、「認証方式変更への考え方」の結果を示す。

本設問では、ショッピングサイトを利用していると仮定して、認証方式に変更があった場合にどの程度の変更であれば許容できるか（サービスを利用し続けるか）について尋ねている。この結果によると「8 文字以上のパスワード設定が必要」である場合は 71.8%の回答者が許容し、サービスを利用し続けるという結果になった。「英字数字の組み合わせが必要」な場合も、約半数の回答者が許容の範囲内の変更であるとしている。「ID をメールアドレス以外のものに設定することが必要」となった場合は、33.4%が変更に対応するとしている。

8 文字以上のパスワードは 71.8%が許容するにもかかわらず、12 文字以上のパスワードとなると、24.5%まで許容できる回答者が減少する。複数のパスワードや認証方式の組み合わせになると、許容できる回答者は、15%前後となった。

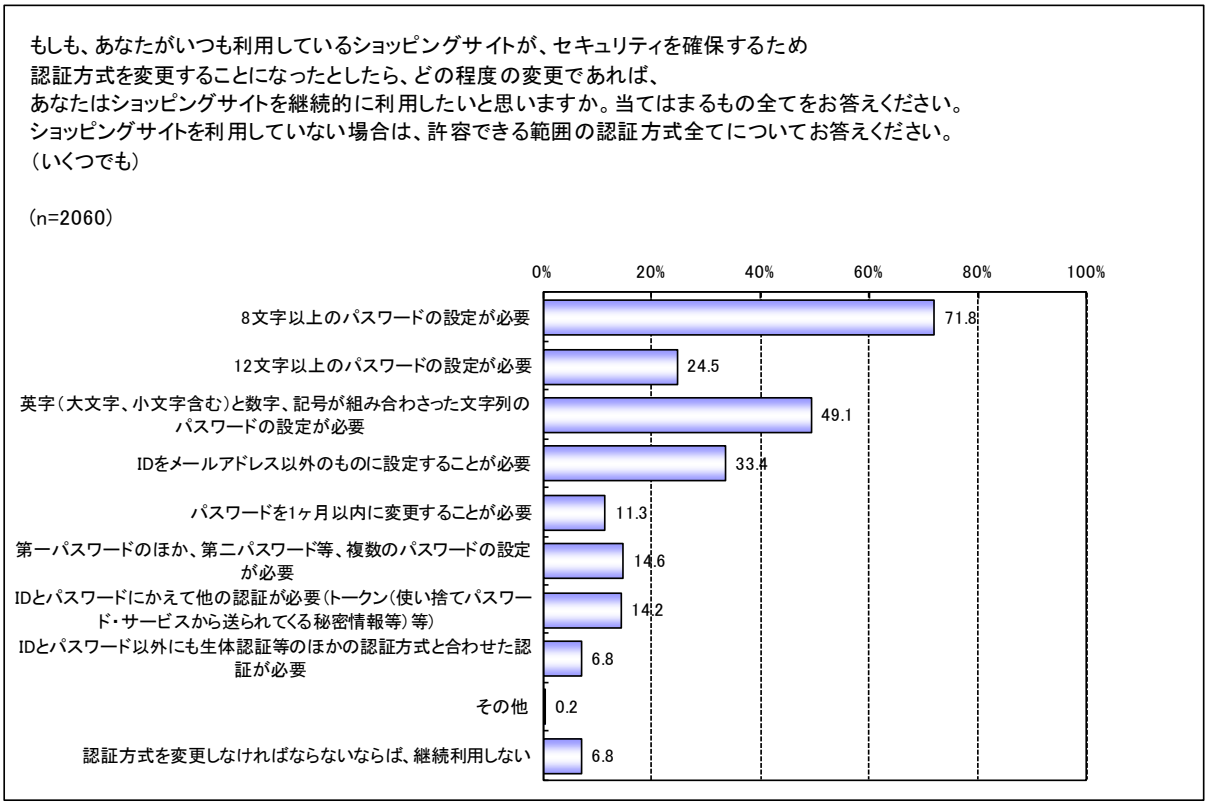


図 38　認証方式　変更への考え方

⑤　アイデンティティ連携の利用意向について

アイデンティティ連携における認証情報を管理するサーバを ID サーバと定義し評価、利便性、安全性、利用意向の結果を示す。なお本調査において、ID サーバとは、図 37 のように定義した。

表 36　ID サーバの定義

あなたが、あるサイト(ID サーバと呼ぶ)にご自身の個人情報を登録すると、他の複数のサイト間で必要に応じて登録した情報を共有するサービスがあります。 これは、あなたがあるサービスサイトにログインしようとしたとき、ID サーバがあなたの ID であなたを確認し(認証)し、ID サーバに登録した必要な情報のみをサービスサイトへ引き継ぐことができる仕組みとなっています。そのため、あなたは最初に情報を登録したサイトの ID をひとつ持つと、それぞれのサイトで個別に ID を持つ必要はありません。また、それぞれのサイトに個別に個人情報を登録する必要もありません。

図 39 の ID サーバの評価の結果を見ると、24.7%が「良い仕組みだと思う」と評価している。なお、本調査で実施した ID サーバの評価、利便性、安全性、利用意向は、「どちらともいえない」といった回答が 5 割程度を占めている。ただし、本調査では、上述のように ID サーバの定義を説明した上で調査を実施したが、回答者にとって ID サーバは身近なものとは言い難く、回答者の理解が不足していた可能性があるため、結果の見方には留意が必要である。

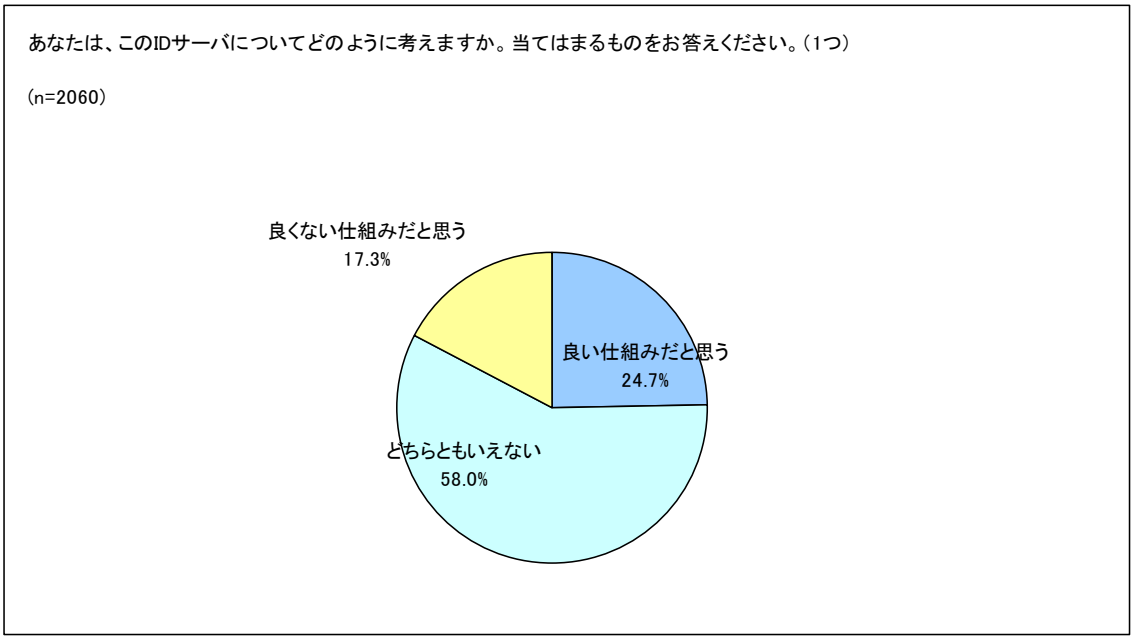


図 39　ID サーバの評価

ID サーバの利便性についての考えの問いには、44.5%が「便利である」と回答している（図 40)。

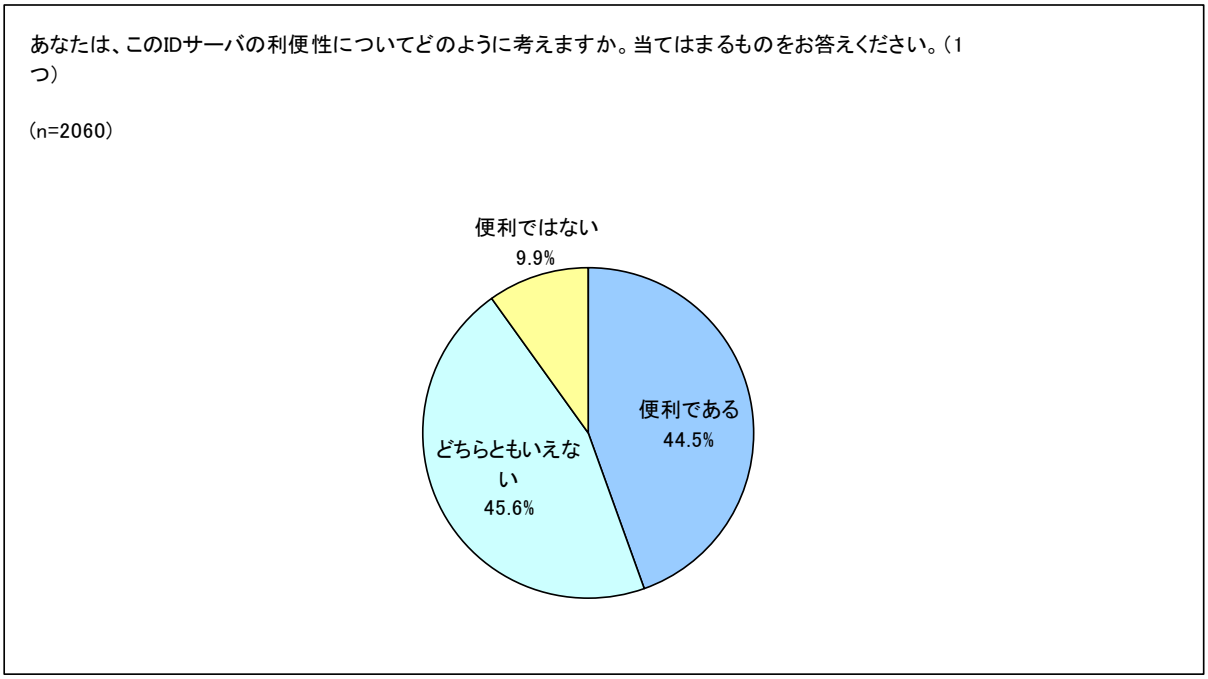


図 40　ID サーバの利便性

図 41 の ID サーバの安全性に対する考えの結果では、「安全である」という回答は 2.4%にとどまり、48.3%が「被害を被るかもしれない」としている。

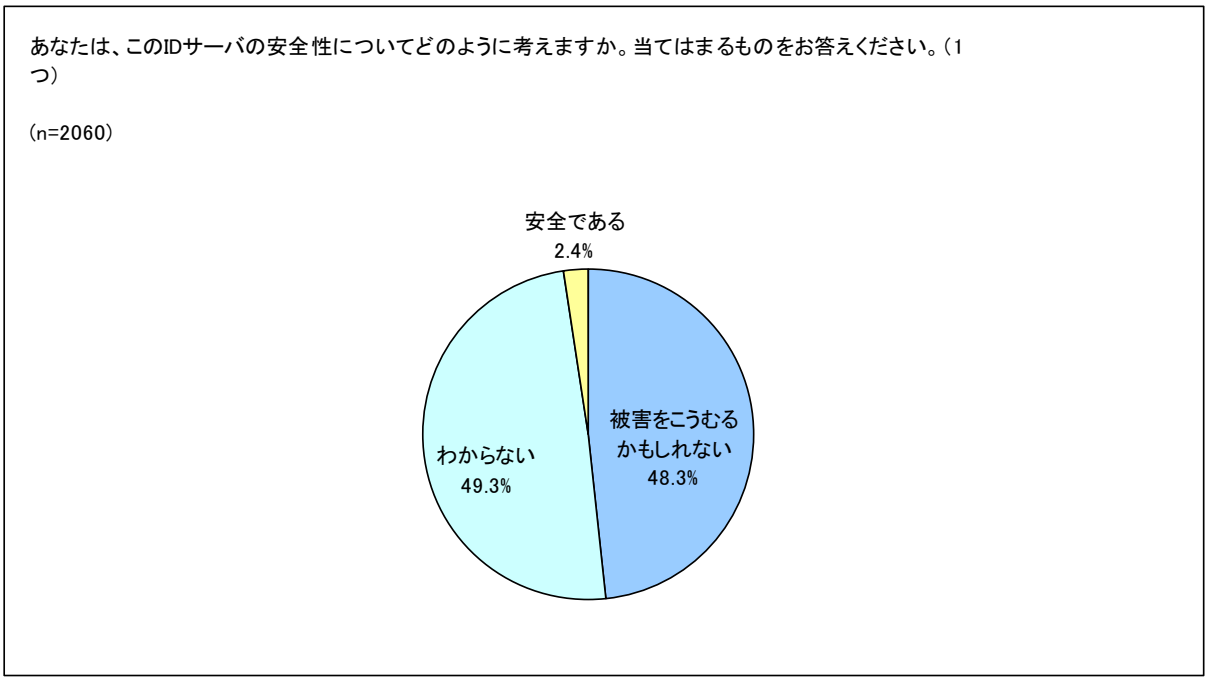


図 41　ID サーバの安全性

ID サーバの利用意向の結果を見ると、「使ってみたい」という回答は 18.3%であり、「使いたくはない」の 30.4%を下回る結果となった。（図 42）

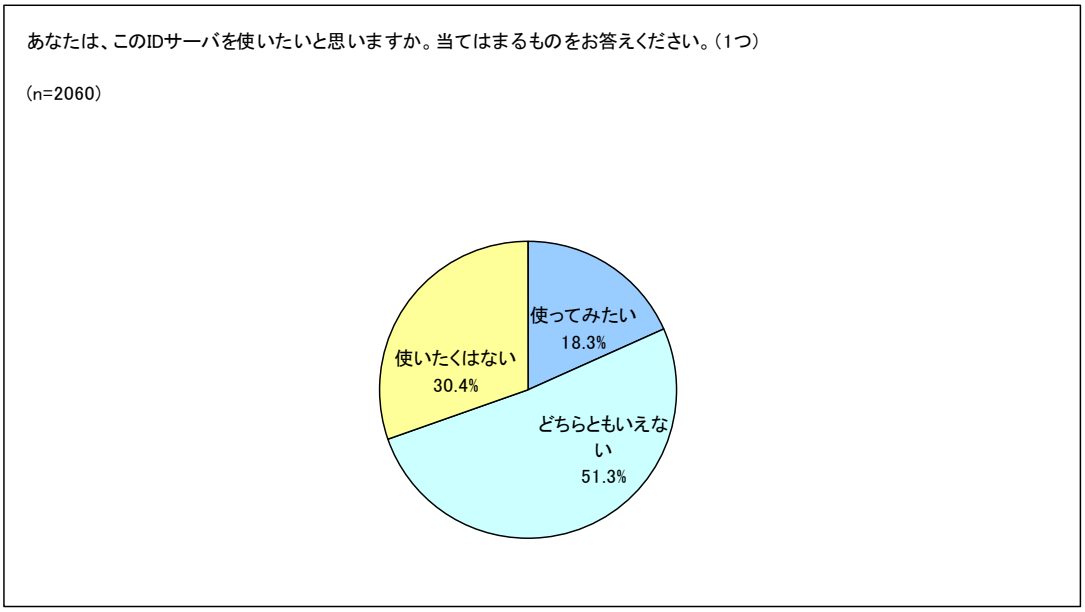


図 42　ID サーバの利用意向

ID サーバに登録した ID や個人情報がサイバー攻撃にあったときに備えて、利用料（保険料）を支払ってもよいと思うかについて尋ねた結果を図 43 に示す。この結果によると、「支払ってもよい」という回答は 35.0%となっている。

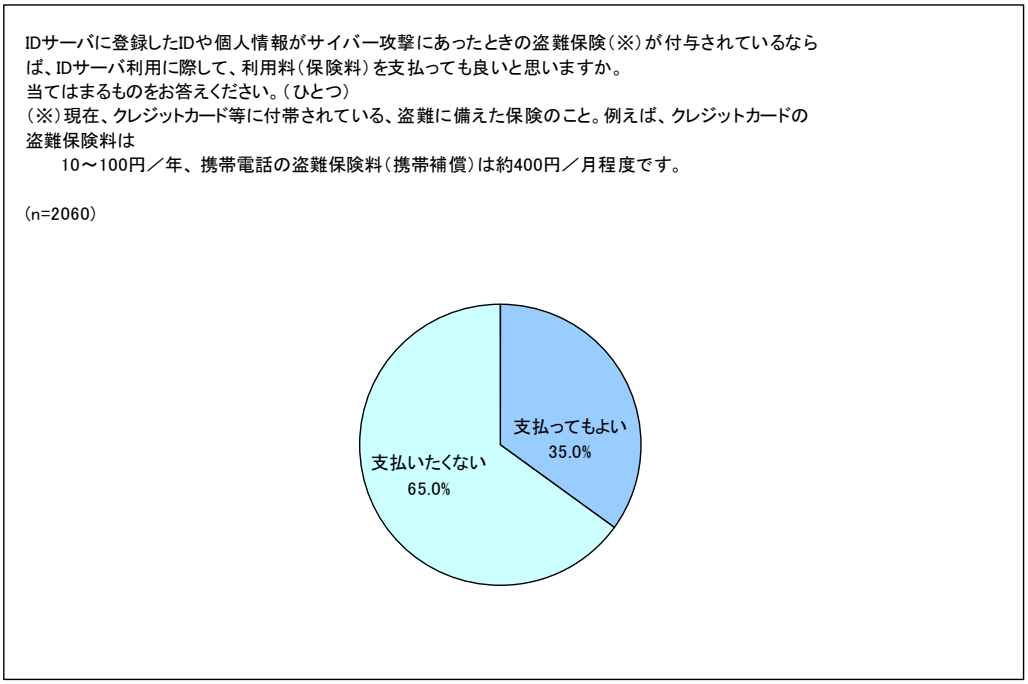


図 43　ID サーバに保険金を支払っても良いと思うか

図 44 に、ID サーバの利用料（保険料）について PSM 分析[23]を行った結果を示す。この結果によると、最低価格（安すぎてあてにならない金額と高いと感じる金額の交点）は 500 円、妥協価格は（安いと感じる金額と高いと感じる金額の交点）は 900 円、最高価格（安いと感じる金額と高すぎて当てにならない金額の交点）は 1000 円である。

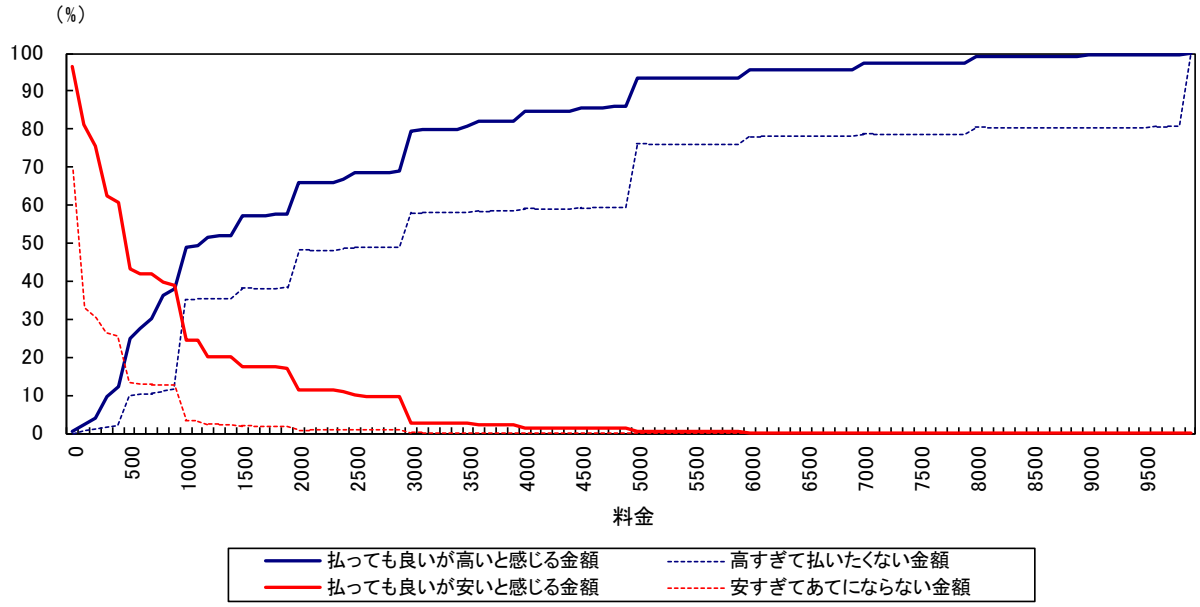


図 44　ID サーバに関わる料金の感度

[23] PSM 分析とは、マーケティング調査に用いられる、消費者のサービスや商品の価格感を探るための手法。適性な価格を導き出す上で基準となる価格帯を分析することができる。

⑥ 望ましいと思う本人認証の方式

金銭に関連したサービスサイトを利用する際に望ましいと思う本人確認方法の結果を示す(図 45)。この結果によると、「サービスサイトとのあなたとの間で共有する秘密情報を使った認証(ID・パスワード（この時のパスワードは、8 文字以上で推測しにくい英数字・記号の組み合わせとする）による認証など)」が「望ましい」という回答が最も多く 84.3%である。「会員登録時などあらかじめサイトに登録した質問とその回答による認証(「ペットの名前は？」、「母親の旧姓は？」といった質問等による認証)」が 71.7%、「2 種類の認証方式を使い、2 つ目の認証は、何らかの秘密情報を使った認証（暗号機能を使うための情報）」が 69 .7%でこれに続く。現在、金銭に関連したサービスサイトで用いられている認証方式を「望ましい」とする回答が多く見られる。

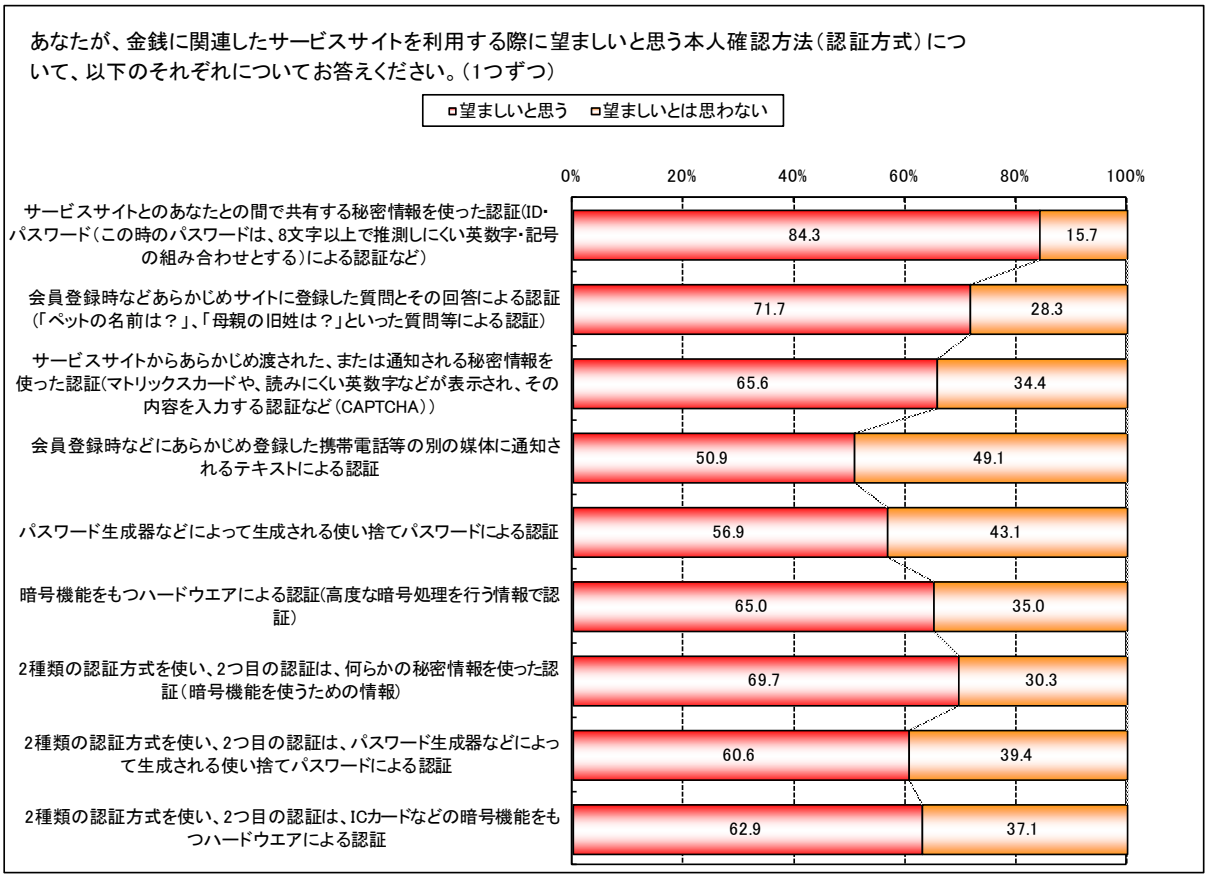


図 45　望ましいと思う本人認証の方式（金銭に関連したサービスサイト）

個人的な情報に関連したサービスサイトを利用する際に望ましいと思う本人確認方法の結果を示す(図 46)。この結果によると、「サービスサイトとのあなたとの間で共有する秘密情報を使った認証(ID・パスワード（この時のパスワードは、8 文字以上で推測しにくい英数字・記号の組み合わせとする）による認証など)」が「望ましい」という回答が最も多く 86.0%である。「会員登録時などあらかじめサイトに登録した質問とその回答による認証(「ペットの名前は？」、「母親の旧姓は？」といった質問等による認証)」が 72.8%、「サービスサイトからあらかじめ渡された、または通知される秘密情報を使った認証(マトリックスカードや、読みにくい英数字などが表示され、その内容を入力する認証など（CAPTCHA）)」が 62.8%でこれに続く。「サービスサイトとのあなたとの間で共有する秘密情報を使った認証(ID・パスワード」「会員登録時などあらかじめサイトに登録した質問とその回答による認証」は、金銭に関連したサービスサイトよりも「望ましい」という回答の割合が高い。

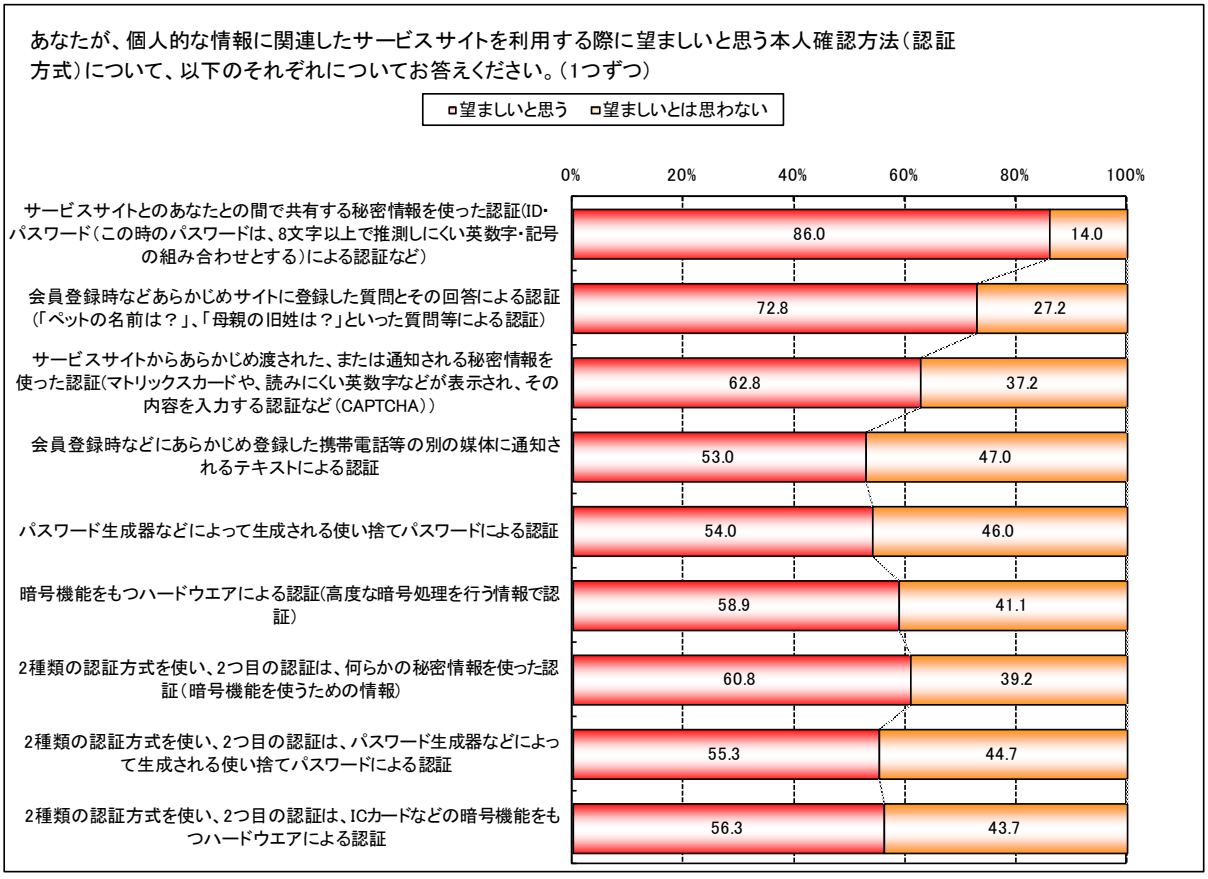


図 46　望ましいと思う本人認証の方式（個人的な情報に関連したサービスサイト）

その他のサービスサイトを利用する際に望ましいと思う本人確認方法の結果を示す（図47)。この結果によると、「サービスサイトとのあなたとの間で共有する秘密情報を使った認証(ID・パスワード（この時のパスワードは、8文字以上で推測しにくい英数字・記号の組み合わせとする）による認証など)」が「望ましい」という回答が最も多く84.3%である。「会員登録時などあらかじめサイトに登録した質問とその回答による認証(「ペットの名前は？」、「母親の旧姓は？」といった質問等による認証)」が71.9%、「サービスサイトからあらかじめ渡された、または通知される秘密情報を使った認証(マトリックスカードや、読みにくい英数字などが表示され、その内容を入力する認証など（CAPTCHA）)」が60.5%でこれに続く結果となった。

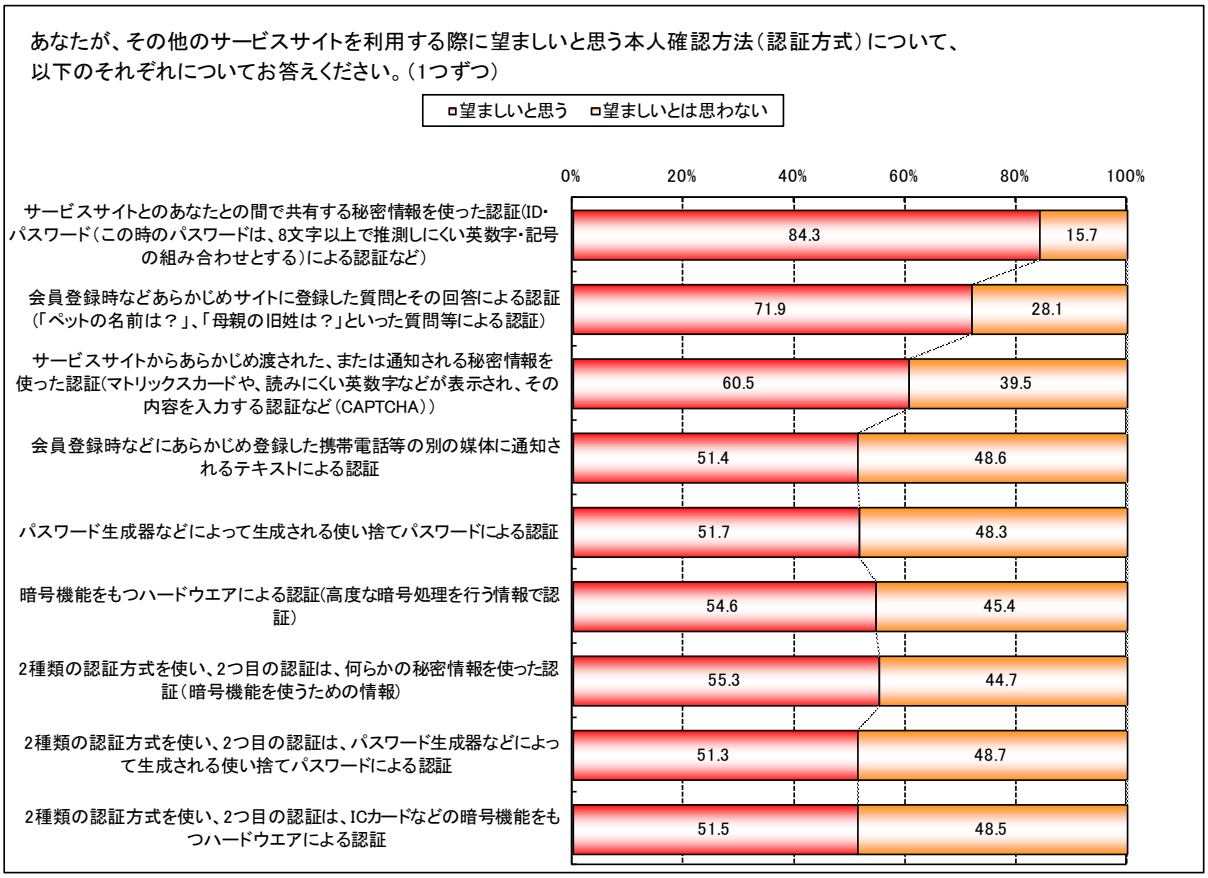


図 47　望ましいと思う本人認証の方式（その他のサービスサイト）

4.2.4. 仮説の検証

仮説（4.2.2 で策定）に基づいて、「①パスワードの安全性とデータの価値の関係性」、「②パスワードの安全性の知識と実態」、「③ID 設定の意識」、「④ID／パスワードの安全性と運用の関係性」について検証を行う。

①　パスワードの安全性とデータの価値の関係性

図 48～図 50 に、それぞれのサイトを現在利用している回答者が望ましいと考える認証方式の結果を示す。この結果によると、その他のサービスサイトに関する認証は、金銭に関連するサービスサイト、個人的な情報に関連したサービスサイトと比較して、「サービスサイトとのあなたとの間で共有する秘密情報を使った認証」、「会員登録時などあらかじめサイトに登録した質問とその回答による認証」といった現状で各種サービスに幅広く普及している認証方式を除くと、全般的に各種認証方式を「望ましい」とする回答が低い結果となった。つまり、金銭に関連するサービスサイト、個人的な情報に関連したサービスサイトの方が複雑な認証方式が望まれる傾向が読み取れる。

特に、金銭に関連するサービスサイトでは、2 種類の認証方式を使った認証を「望ましい」とする回答率が高く、複雑性の高い認証の意向が高く、利用者に受け入れられやすい認証方式であることが推察される。

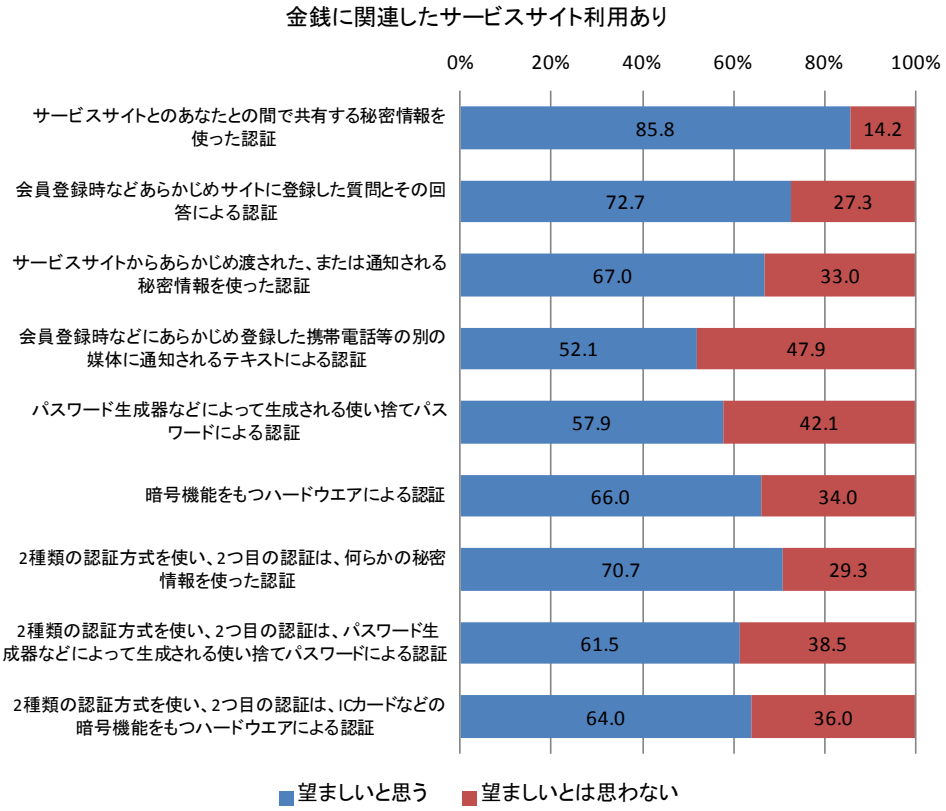


図 48　金銭に関連したサービスサイトで望ましい認証方式

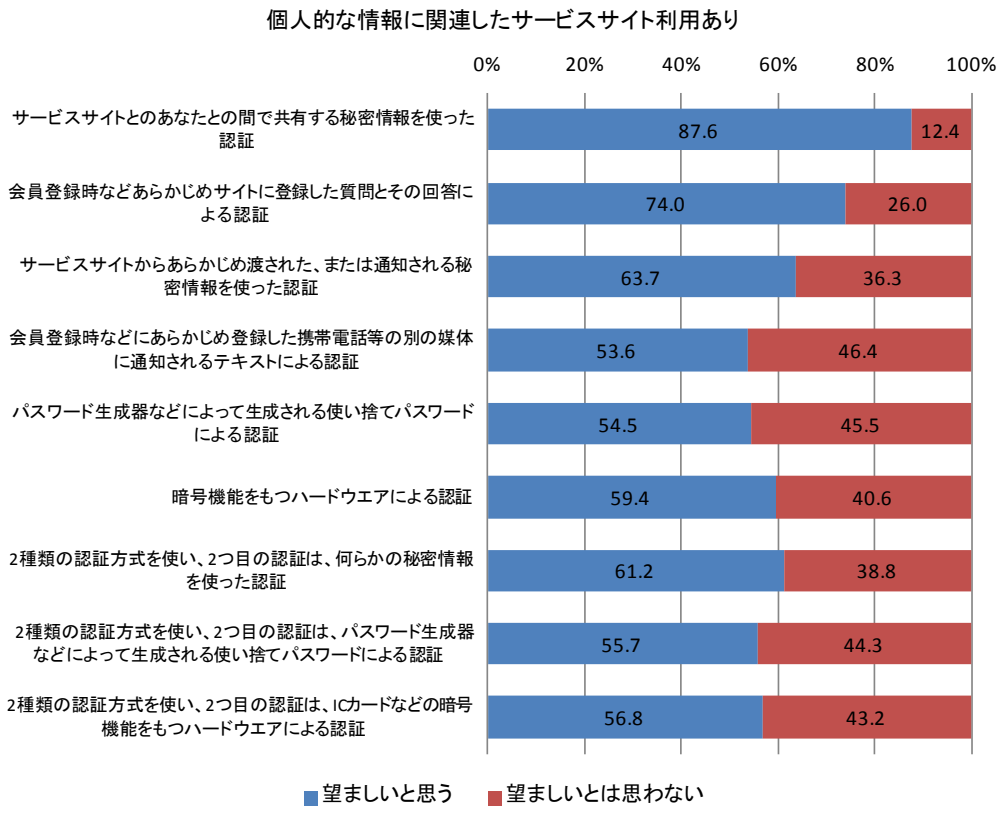


図 49　個人的な情報に関連したサービスサイトで望ましい認証方式

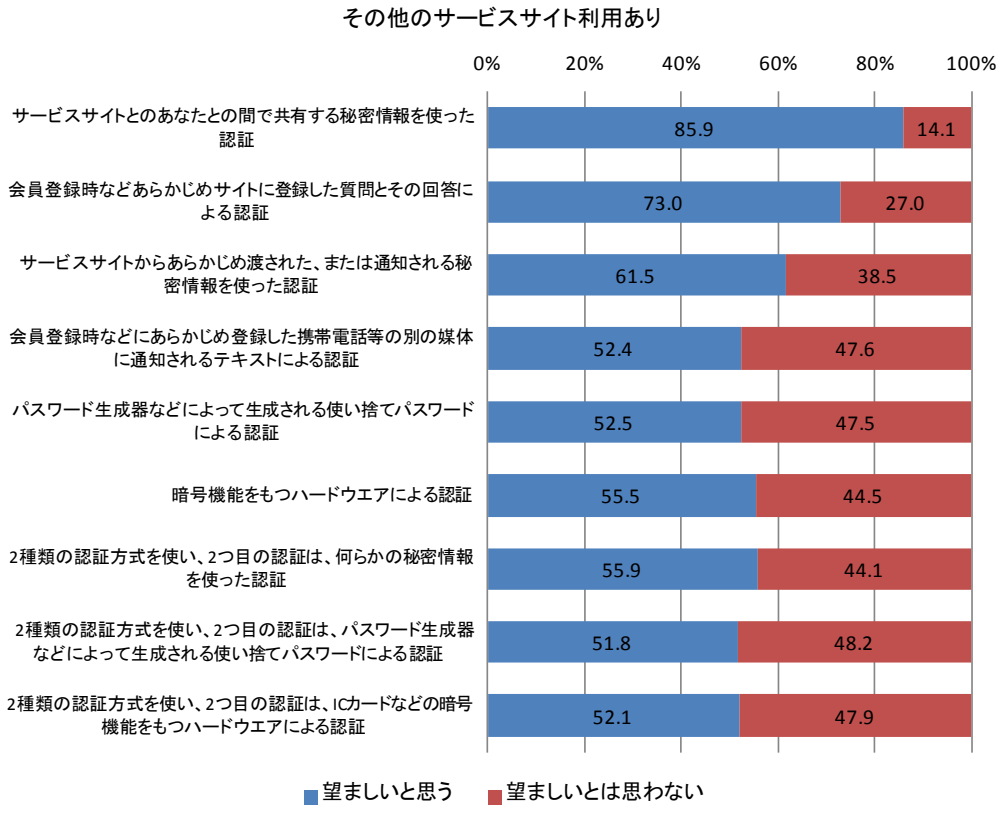


図 50　その他のサービスサイトで望ましい認証方式

② パスワードの安全性の知識と実態

以下では、パスワードの安全性についての知識を有している者と知識を有していない者がどのようなパスワードの管理を行っているかについて検証を行った。

「パスワードの安全性についての知識」として、**図 51**, **表 37** のパスワードに関連する知識の結果から、回答者を得点に応じて、高群、中群、低群に分けて分析を行っている。

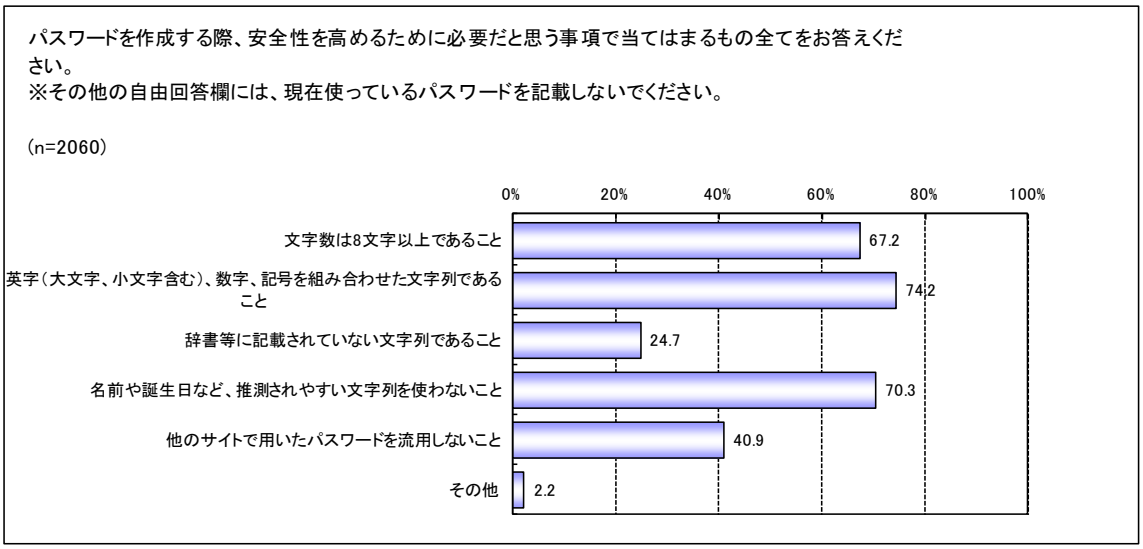


図 51　パスワードに関する知識（再掲）

表 37　「パスワードに関する知識」の結果によるカテゴリ分類の概要

(1)	本調査による選択肢は、全て正しい知識であったことを踏まえ、回答者がいくつ選択したかに応じて、回答者に 0～6 点の得点を割り振った。 ＜パスワードの知識に関する選択肢＞ ・文字数は 8 文字以上であること ・ 英字(大文字、小文字含む)、数字、記号を組み合わせた文字列であること ・ 辞書等に記載されていない文字列であること ・ 名前や誕生日など、推測されやすい文字列を使わないこと ・ 他のサイトで用いたパスワードを流用しないこと ・その他
(2)	(1)の手順で、得点化したところ、平均点は 2.9、標準偏差が 1.4 であった。そのため、高群を 4 点以上、中群を 3 点、低群を 2 点以下としてカテゴリ化した。この分類を行うと、高群が 679 名、中群が 430 名、低群が 951 名となった。

図 52～図 54 に、知識別に見たパスワードの運用の結果を示す。この結果によると、高群のほうが、各種サービスサイトにおいて「他のサービスと同一のパスワードを利用していない」という回答の割合は高い。パスワードの使いまわしをしていないグループを見ると、パスワードに関連する知識を有している者が多いといえる。ただし、個人的な情報に関連したサービスサイトやその他のサービスサイトの結果をみると、パスワードに関連する知識のあるはずの高群も、パスワードを使いまわしている現状が読み取れる。金銭に関連したサービスサイトでは、高群のパスワードの使いまわしが少ないため、サービスサイトに預ける情報によってパスワードの運用を変えるという運用実態も想定されるが、知識が高くてもパスワードを使いまわしている実態が読み取れる。

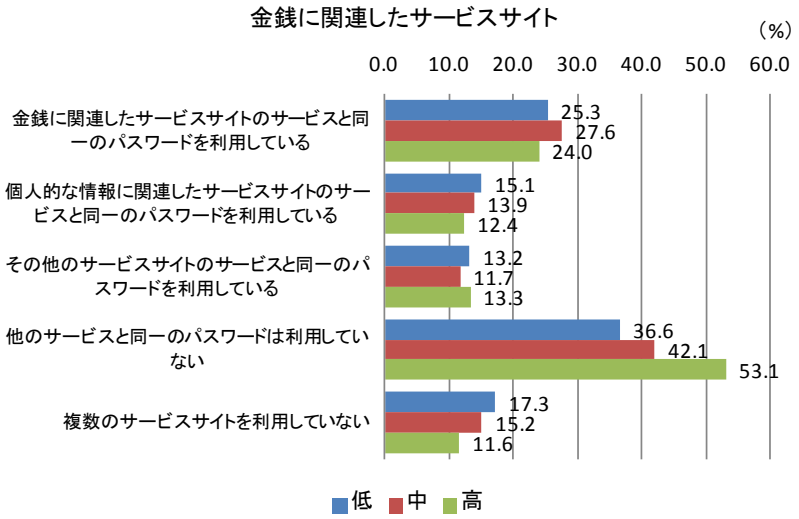


図 52　パスワードの使いまわしの状況（金銭に関連したサービスサイト／知識別）

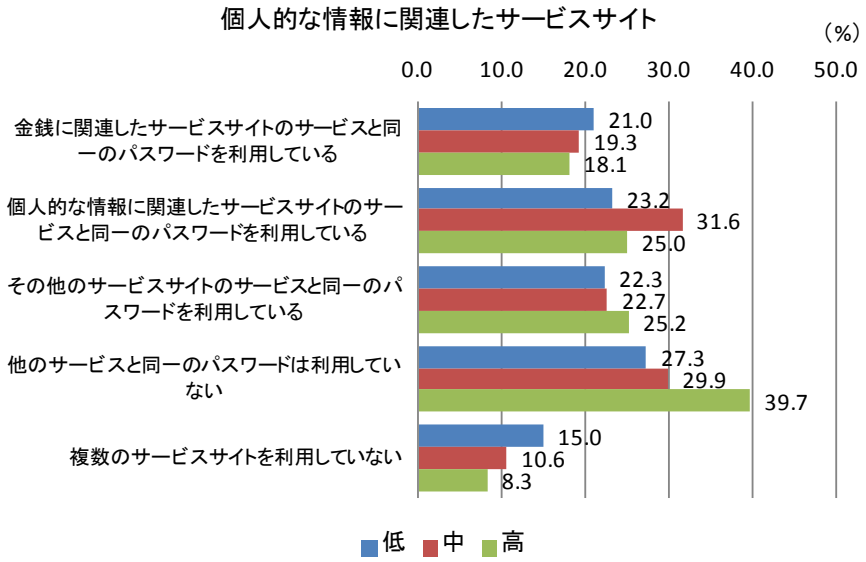


図 53　パスワードの使いまわしの状況（個人的な情報に関連したサービスサイト／知識別）

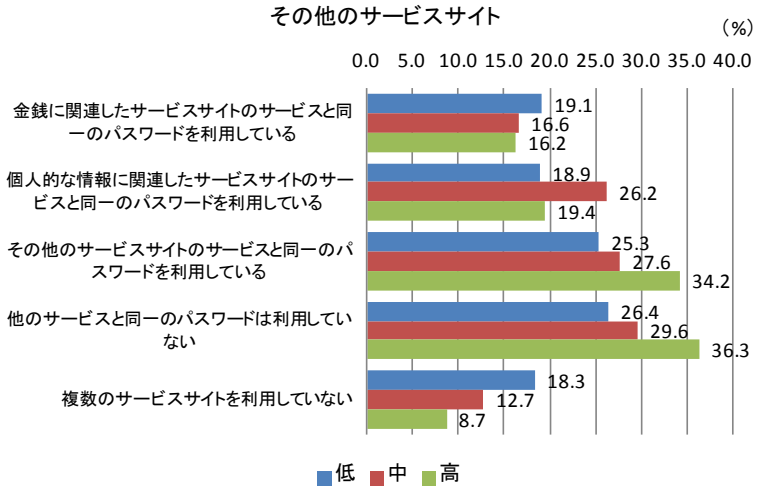


図 54　パスワードの使いまわしの状況（その他のサービスサイト／知識別）

図 55 に、知識別に見たパスワードの管理方法の結果を示す。この結果によると、低群はパスワードを「記憶」しており、高群は各種方法でパスワードを管理している傾向が見られる。高群は、他の群と比較すると、「インターネットブラウザへ記憶」、「パスワード管理ツール」といったパスワードを管理するための電子的な仕組みを活用している割合がわずかながら高い。

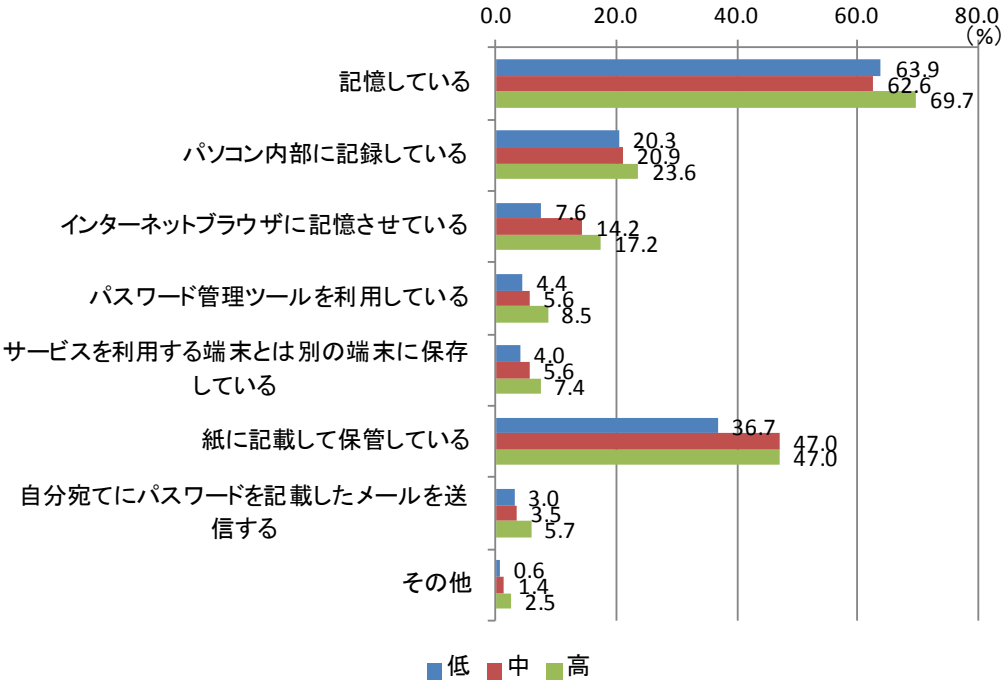


図 55　パスワードの管理方法（知識別）

図 56～図 58 に、知識別に見たパスワード変更の周期の結果を示す。この結果によると、高群は何らかの周期でパスワードの変更を行っている。ただし、金銭に関連したサービスサイト、個人的な情報に関連したサービスサイト、その他のサービスサイトで、高群は「6 ヶ月以上 1 年未満の変更」が他の群と比較すると高くなっており、できる限り長い期間、同じパスワードで運用しているという実態が読み取れる。

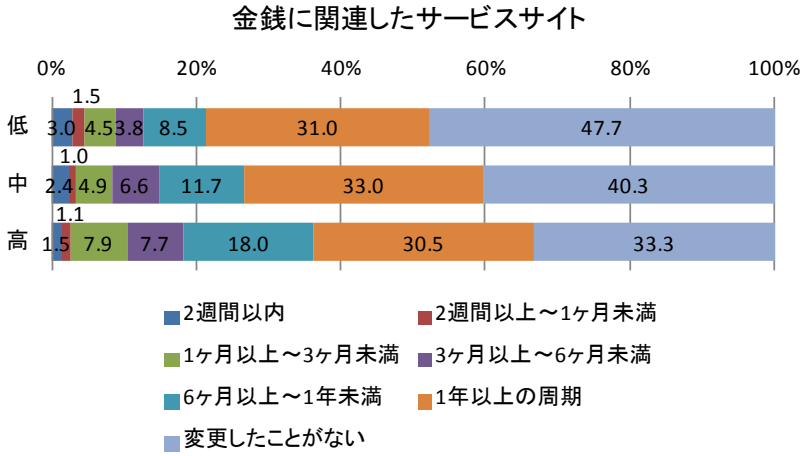


図 56　パスワードの変更の周期（知識別／金銭に関連したサービスサイト）

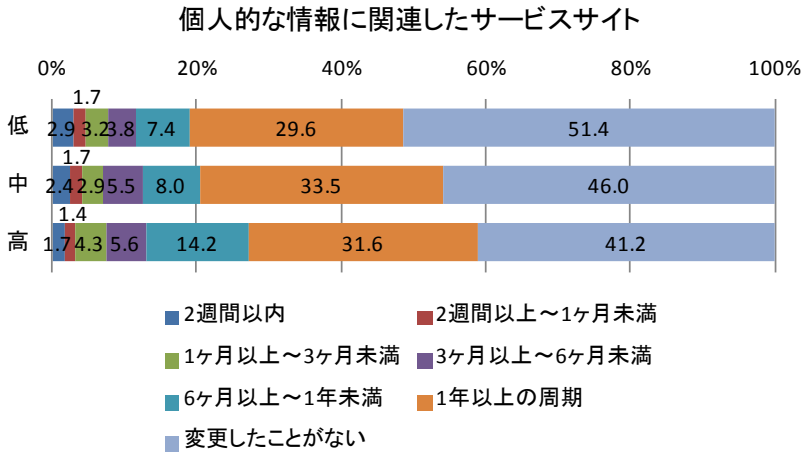


図 57　パスワードの変更の周期（知識別／個人的な情報に関連したサービスサイト）

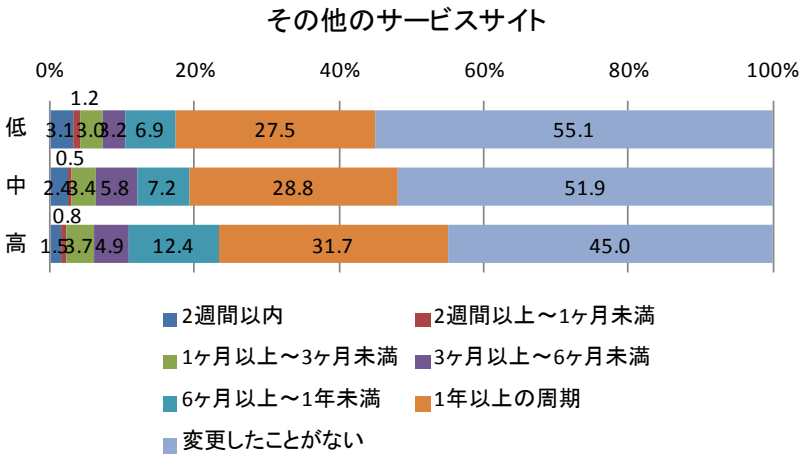


図 58　パスワードの変更の周期（知識別／その他のサービスサイト）

③　ID 設定の意識

以下に、ID 設定の実態の結果を示す。なお、本調査では、ID に関する知識を等設問は設定していないため、知識別として②で定めたカテゴリを用いて検証を行った。

図 59～図 61 に、知識別に見た ID の設定状況の結果を示す。この結果によると、「ランダムな英数字の組み合わせ」を ID として設定しているものは知識が高いほど多いという傾向が見られる。ただし、「任意の英単語」、「任意の英単語と数字」、「メールアドレス」を ID として設定している回答者は知識を問わず一定数見られる。特にメールアドレスを ID として設定している回答者は、個人的な情報に関連するサービスサイト、その他のサービスサイトで知識を問わず、2 割を超える。

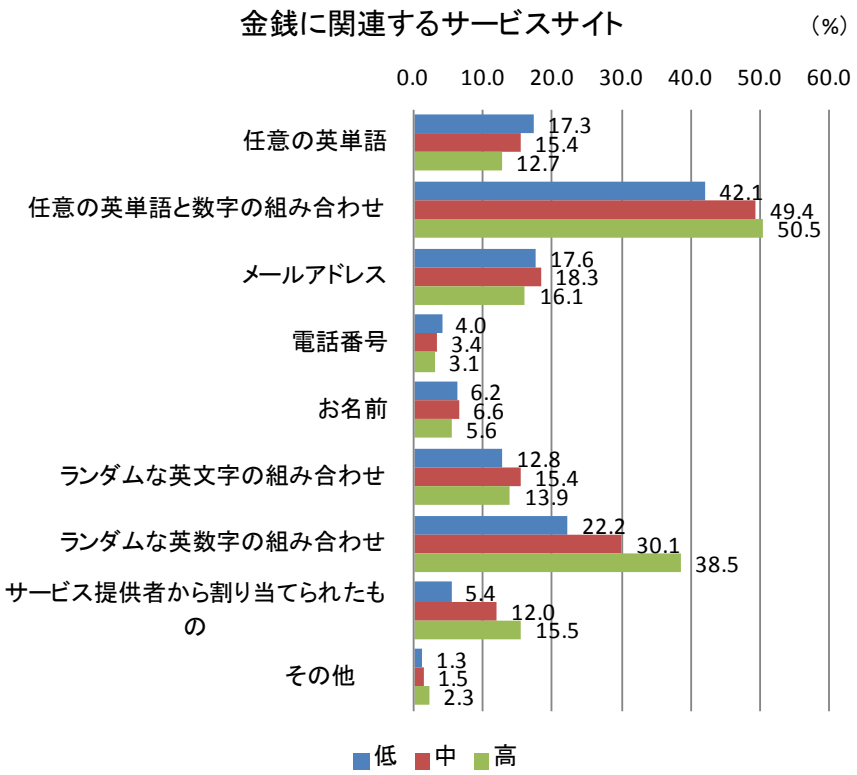


図 59　ID の構成（知識別／金銭に関連するサービスサイト）

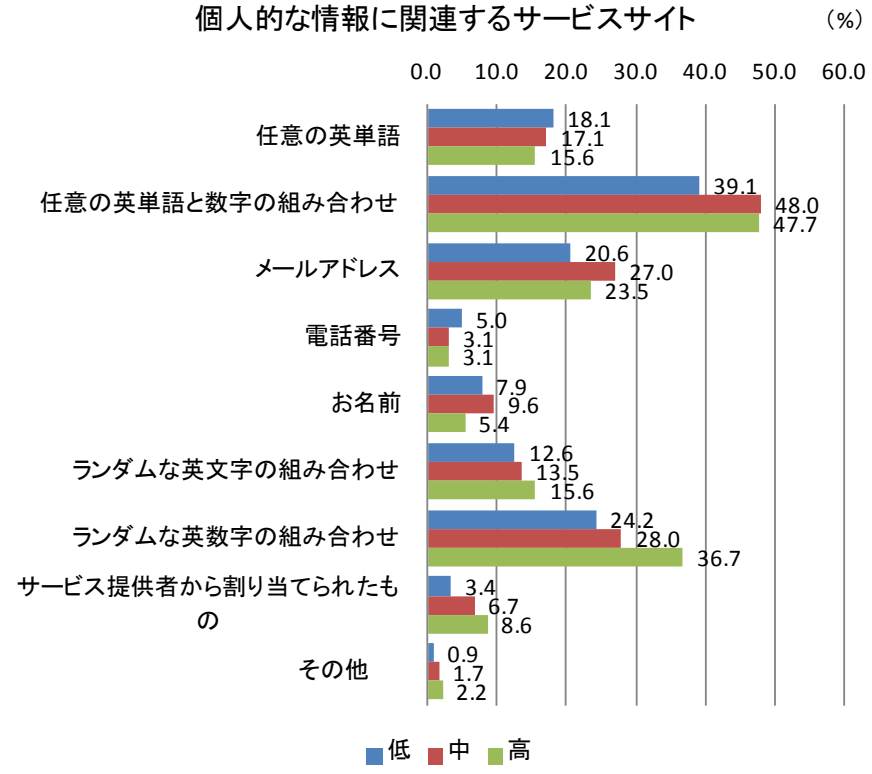


図 60　ID の構成（知識別／個人的な情報に関連するサービスサイト）

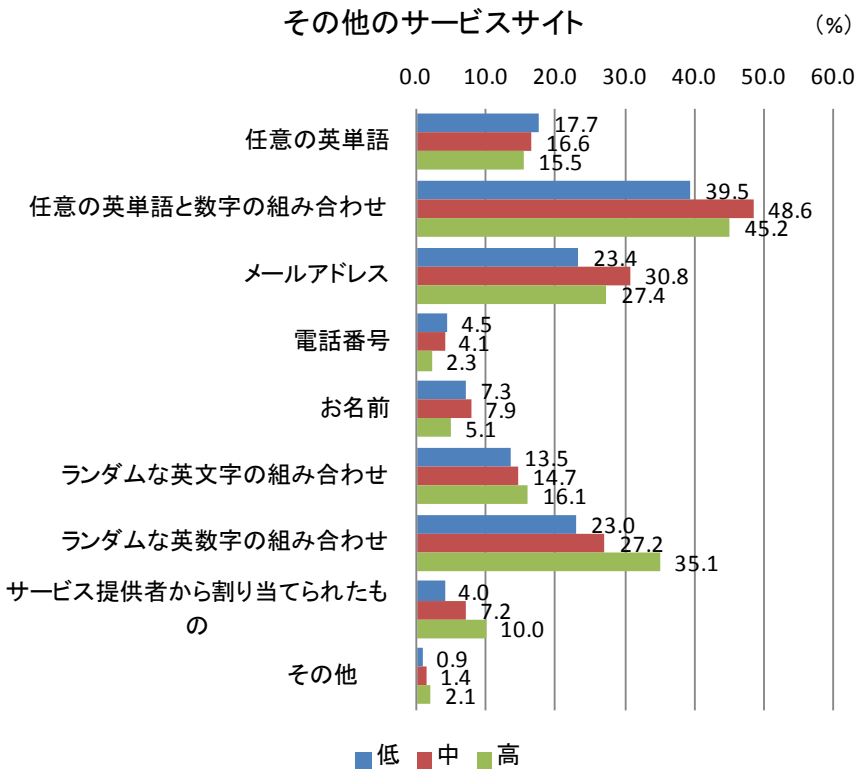


図 61　ID の構成（知識別／その他のサービスサイト）

図 62～図 64 に、ID サーバの評価を知識別に見た結果を示す。この結果によると、低群と比較すると、中群、高群のほうが ID サーバの利便性を評価している傾向が見られる。また、安全性については、高群の 59.8%が「被害をこうむるかもしれない」と考えており。中群、低群と比較して高い結果となった。利用意向としては、高群、中群の 2 割が利用意向を示している。ID サーバの安全性について正しい情報が普及すれば、高群、中群を中心に利用意向も高まるのではないかと推察される。

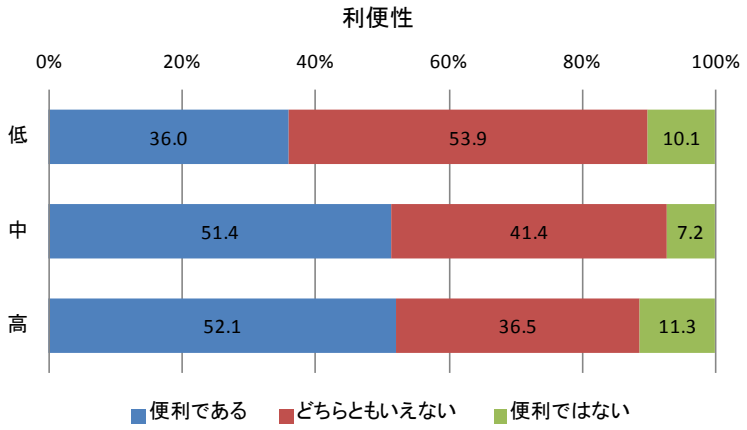


図 62　ID サーバの利便性の評価（知識別）

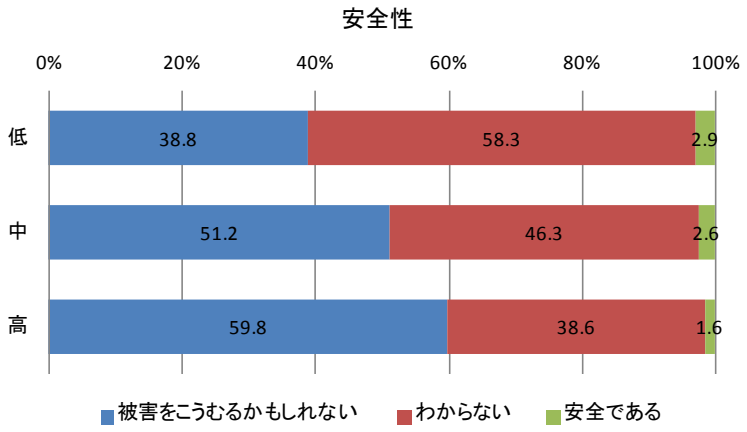


図 63　ID サーバの安全性の評価（知識別）

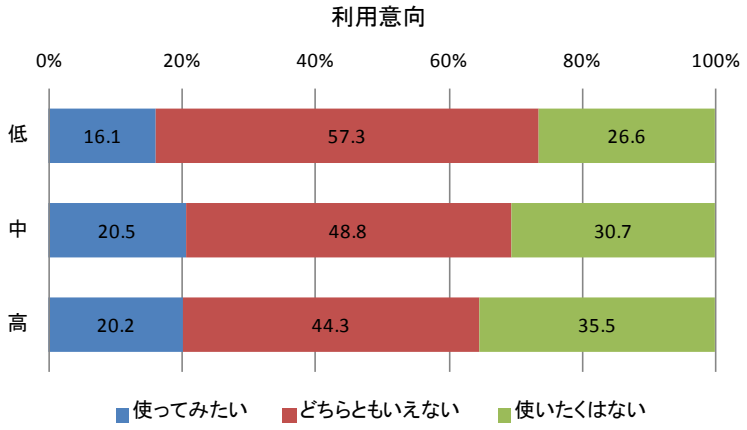


図 64　ID サーバの利用意向（知識別）

④　ID／パスワードの安全性と運用の関係

上述のように、パスワードに関する知識を有する者であっても、パスワードを使いまわしたり、パスワードの変更周期が長いという現状が見られる。この要因を分析するために、パスワードを使いまわす理由の結果を**図 65** に示す。パスワードを使いまわす理由として、パスワードに関する知識があると想定される高群、中群は、「パスワードを忘れてしまうから」「複数のパスワードを管理するのが手間だから」といった回答率が高くなっている。これは、管理が煩雑になるので、パスワードを使いまわして手間を省こうとしている背景が読み取れる。

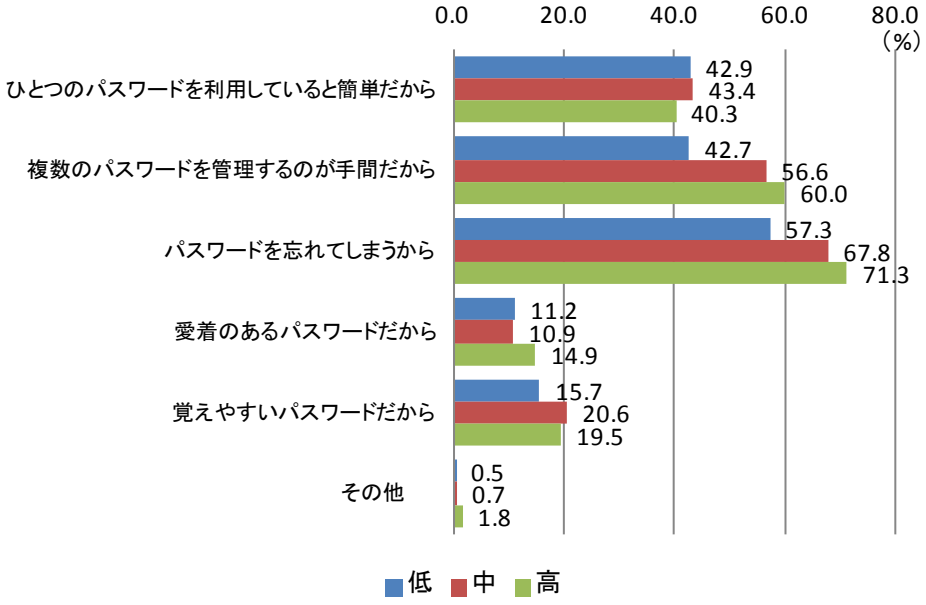


図 65　パスワードを使いまわす理由（知識別）

5. 課題と対策

オンライン本人認証の実態を調査した結果を基に検討した課題と対策を報告する。

はじめに利用者の実態調査の結果及びサービスサイトの実態調査の結果からオンライン本人認証に関する課題を以下に抽出する。

○主な利用者の実態調査の結果

本実態調査の結果では、利用者が、記憶できる ID は 1~5 個までが全体の 85%を占める。利用している ID は 1~10 個までが全体の 86.4%を占める。また、安全なパスワードが何かをおおむねが知っている（約 70%）が、ランダムな英数字記号からなる安全なパスワードを設定しているのは僅か 13%と低く、他サイトとパスワードを使い回しているのは半数以上と、安全なパスワードの設定・運用ができていない。

○主なサービスサイトの実態調査の結果

サービスサイト調査の結果から、すべてのサービスサイトで ID・パスワードによる認証を提供しているが、その他のオンライン本人認証方式の提供は約 10%以下と少ない状況である。インタビュー調査の結果によると、サービスサイトは、ID・パスワードによる認証は、ID・パスワード以外の知識やデバイスが不要なため導入し易く、サービス利用者に受け入れられ易いと推察されている。

ID・パスワードによる認証において入力を求めるパスワードの最小桁数は、サービスサイト調査の結果では、PC 環境で 4 桁～7 桁が全体の約 60%程度（スマートデバイス環境では約 70%）であり、短い桁数で本人認証を実施している。インタビュー調査では、サービスサイトでは、パスワードポリシーを厳しくするとサービスの利用率の低下や、ID・パスワード失念や変更に関するサポートコストが増加することを危惧する意見が見られた。また、他のオンライン本人認証方式への移行に関するインタビュー調査の結果では、サービスサイト側は、パスワードリスト攻撃を防ぐために ID・パスワードによる認証以外を提供したいという意見があるものの、ワンタイムパスワードデバイス等の認証デバイスは、有料オプションとなり利用率が低くなり、さらに、認証デバイスを用いた認証は、認証デバイスを所持していることが前提となるため、利用率が低下する可能性を懸念する見解が得られた。

ID 連携に関するサービスサイト調査の結果では､ID 連携を提供しているサービスサイトは PC 環境で 24%（スマートデバイス環境では 67%）と低い状況であり、インタビュー結果では、IdP が ID を提供しなくなるおそれ（事業継続性も含む）があり、ID 連携の導入が困難な場合もあるという声があった。

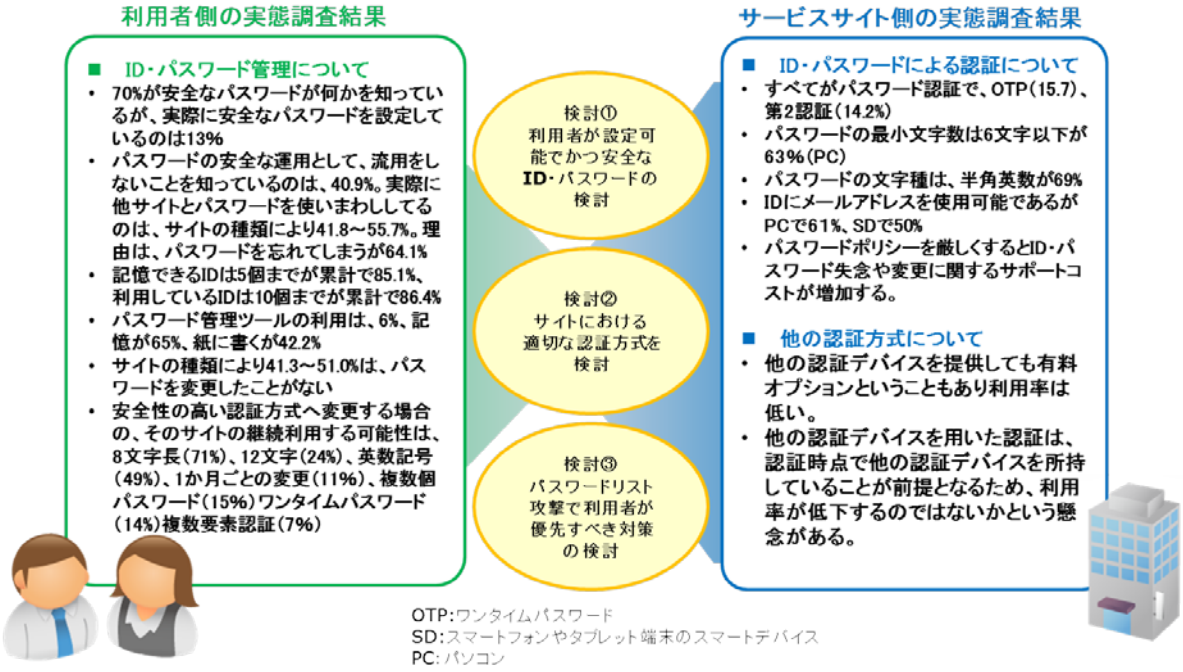


図 66　オンライン本人認証の課題概要

利用者側は ID・パスワード管理の負荷から ID・パスワードを使い回すなど安全な設定や管理を実施できていないことから近年ではオンライン本人認証に係る多くのインシデントが発生している。そのため、利用者とサービスサイトの双方が実現可能で安心して利用できるオンライン本人認証を検討する必要がある。以下に検討事項を示す。

①　利用者が許容する ID・パスワードの検討（提供者向け）

サービスサイトの実態調査から ID・パスワード認証から他の認証方式への移行を進めるためには一定の期間を要することが考えられる。そのため、現状で実現可能な対策として利用者が許容する ID やパスワード（文字種や桁数等）を検討する。

②　各種サービスで扱う情報に応じた対策の検討（提供者・利用者向け）

推測困難なパスワード及び一定期間でのパスワード変更、パスワードの世代管理による以前に設定したパスワードの設定禁止等、パスワードポシリーを厳しくするとパスワードの使い回しを助長することも考えられる。一方、サービスによって扱う情報やリスクは異なるため、リスクに応じたパスワードの設定や認証方式の選択を行うことが望ましい。そのため、各種サービスで扱う情報に応じた設定等を検討する。

③　現実的な脅威を防ぐために利用者が独自に実施できる対策の検討（利用者向け）

利用者は、安全なパスワードが何かを概ね理解しているが、安全なパスワードの設定を行っていない。ただし、実態調査の結果によると、「金銭」、「個人」、「その他」の各サイトの順に、安全なパスワードの設定の度合いを低くしていることから、利用者は、その情報の重要度、脅威等

を正しく理解すれば、リスクに応じた行動に変化することが期待できる。まず、現実的な脅威への対策を検討、実施するうえでの考え方を検討する。また、安全なパスワード管理やパスワードの変更等を確実に実施するためには、脅威情報及び対策に関する啓発活動が重要である。

上記に基づき検討した結果を以降に示す。検討①を 5.1.1 に、検討②を 5.1.2、5.2.1 に、検討③を 5.2.2 に示す。

5.1. インターネットサービス提供者の対策

5.1.1. 利用者が許容範囲な ID・パスワードの検討

利用者に対するアンケート結果において、金銭に関連したサービスサイトを利用する際に望ましい本人認証方式の質問では、推測しにくいパスワードによる認証など上位 5 つの回答は、すべて 65.0%以上であった（図 67 下図左）。一方、具体的なシーンを設定した設問 「ショッピングサイトでセキュリティを確保するために認証方式を変更しても継続してサービスを利用する認証方式」の質問への回答では、8 文字以上のパスワードによる認証が 71.8%であったものの、その他の認証方式については 50%未満であった（下図右）。

この結果から、ID・パスワードによる認証方式から他の認証方式に変更する場合は、継続利用が低下する可能性がある。また、当初から ID・パスワードによる認証を提供している場合には、8 文字以上のパスワード設定に変更しても継続利用が低下する可能性が低いことがわかる。

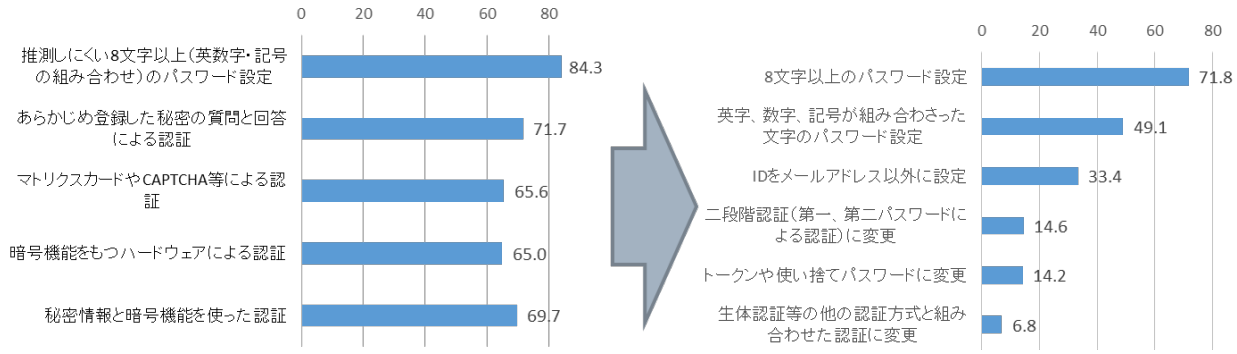


図 67　認証方式の変更に関する利用者アンケートの結果概要

サービスサイトの調査結果では、PC 環境ではパスワードの最小桁数が 4 桁～7 桁が 58%、スマートデバイス環境では 68%（6 桁～7 桁）であったが、これらのサイトは 8 桁以上に設定変更しても利用者は許容可能であると考えられる。

5.1.2. 各種サービスで扱う情報の資産価値に応じた対策の検討

インターネットサービス提供に関するパスワードポリシーについては、政府が呼びかける推奨内容を 3.1.2 に示した通りである。一方、インタビュー調査の結果ではインターネットサービス利用者に強固なパスワード管理を強制すると利便性を損ない利用率の低下や利用者の低下を招く恐れがあることが示されている。そのため、インターネットサービス提供者は、むやみに、強

固なパスワードポリシーを設定、強制するのではなく、自らが提供するサービスに対するリスク分析を行い、適切な本人認証方式を設定し、さらに、ID・パスワード認証であればこれも、リスクに応じたパスワードポリシーを定めることが重要である。以下にこれらを検討するためのリスク分析手法を紹介する。

(1) サービスで取り扱う情報に基づいたリスク分析について

各種サービスで取り扱う情報に応じて本人性確認の厳密性は異なる。例えば、金融サービスでの取引、決済や行政サービスでの住民情報の登録、閲覧等では信頼できる厳密な本人性確認が必要となる。一方、ニュース・記事の閲覧や収集にはサービス利用者の登録する情報が少なく情報漏えい等の影響がなければ、上述のサービスと比べて本人性確認の信頼性や厳密性は低い。このようにアイデンティティや認証に求められる信頼性に対する保証の程度を保証レベル（LoA: Level for Assuarance）という。

電子政府におけるリスク分析及び LoA の検討については、内閣官房 IT 担当者及び情報セキュリティセンター（NISC）が、各府省情報化統括責任者（CIO）連絡会議において「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（以下、電子署名・認証ガイドライン）」を 2010 年 8 月に公表している。この電子署名・認証ガイドラインは、民間のインターネットサービスを対象としていないが、リスクの影響度、被害規模のレベル、それらを踏まえた総合的リスク評価というリスク分析の手法が示された。本報告書の対象とする各種サービスにおいても、扱う情報に応じた対策を検討するためにリスク分析を行う必要があると考える。

認証情報の登録、発行・管理、トークン自体の強度、認証プロトコルの認証情報のライフサイクル各々で求められる信頼度に合わせ、保証レベルが定められる（図 68 参照）。

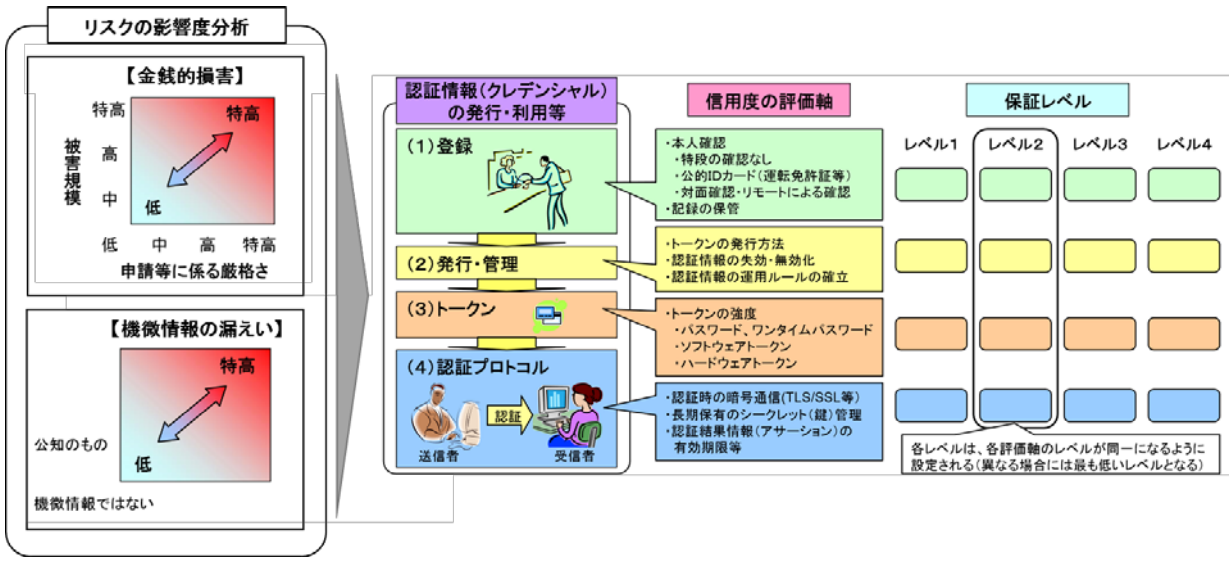


図 68　リスク分析と保証レベルの概要

認証情報のライフサイクルの各フェーズは同一のレベルを設定する必要があり、ライフサイクルの一部が他に比べて低いレベルがあれば、全体としては最も低いレベルとなる。電子署名・認証ガイドラインで示された主な対策基準を図 69 に示す。

保証レベル	登録	発行・管理	トークン	認証プロセス	署名等プロセス
レベル4	(窓口) ・写真付き身分証明1種の提示 ・申請情報の台帳照合 ・重複登録ではないことの確認	・手渡し、本人限定受取郵便、によるトークン発行	・レベル3の基準に加え、耐タンパ性が確保されたハードウェアトークンを利用すること	・レベル3と同等の基準	・電子政府推奨暗号リストに記載の署名方式 ・電子署名用の証明書の用途は電子署名限定
レベル3	(窓口) ・写真付き身分証明1種(or他2種)の提示 ・申請情報の台帳(又は公的証明書)照合 (郵送 or オンライン) ・申請書に対する電子署名 ・申請情報の台帳(又は公的証明書)照合	・レベル4の方法に加え、書留郵便、書留郵便＋ダウンロード、電子署名＋ダウンロード、によるトークン発行	・レベル2の基準に加え、複数の認証要素を利用すること	・レベル2と同等の基準に加え、フィッシングの脅威に対する耐性	・電子政府推奨暗号リストに記載の署名方式
レベル2	(窓口) ・写真付き身分証明1種(or他2種)の提示 (郵送 or オンライン) ・申請情報に他機関の登録情報(クレジットカード番号等)を含めて申告	・レベル3の方法に加え、分割配付(一方を郵送)、メール通知後のダウンロード、によるトークン発行	・認証情報の推測確率が16384分の1未満であること	・レベル1と同等の基準に加え、盗聴、セッション・ハイジャック、中間者攻撃の脅威に対する耐性	
レベル1	(窓口 or 郵送 or オンライン) ・身元確認は不要 ・メールアドレスの到達確認	・レベル2の発行方法に加え、電子メールによる送付、ダウンロード、によるトークン発行	・認証情報の推測確率が1024分の1未満であること	・オンライン上の推測、リプレイ攻撃の脅威に対する耐性	

図 69　電子署名・認証ガイドラインの主な対策基準

電子署名・認証ガイドラインの脅威に対するリスク分析では、組織の運営や資産または個人に及ぼす被害規模のレベルを「影響度」から 4 つのレベルに分類している。致命的または壊滅的な悪影響を及ぼすと予想されるものが「特高」、重大な悪影響を及ぼすと予想されるものが「高」、限定的な悪影響を及ぼすと予想されるものが「中」、測定可能な結果をもたらさないものが「低」である。さらに、対象となるオンライン手続に対して、「金銭的損害」と「機微情報の漏えい」の 2 つを主たるリスクとし、事案がもたらす被害規模と申請などに係る厳密さから「低、中、高、特高」の 4 段階のレベルを設定し、基礎的なリスクの影響度を導出している。表 38 に被害規模のレベルを示す。

表 38 被害規模のレベル

レベル	金銭的損害の程度	情報に含まれる機微(センシティブ)の度合い
特高	1,000 万円以上の金銭的損害	生命の危険または差別や名誉毀損等の社会的不利益につながるもののうち、回復が困難なもの [24]
高	100 万円以上、1,000 万円未満の金銭的損害	特高と中の中間に位置するもの
中	100 万円未満の金銭的損害	公知のもの
低	金銭的損害なし	機微情報ではないもの

上記の基礎的なリスクの影響度における「金銭的損害」と「機微情報の漏えい」を踏まえた総合的なリスク評価を表 39 に示す。

[24] 「個人情報保護マネジメントシステム－要求事項（JIS Q 15001）」で収集禁止の個人情報として定義されているものなど

表 39 総合的リスク評価の導出方法

金銭的損害に係るリスクの影響度	機微情報の漏えいに係るリスクの影響度	総合的なリスクの影響度
高	中	変更について検討（中 or 高）
高	高	高
高	特高	変更について検討（高 or 特高）

上記の総合的なリスク評価を本調査におけるインターネットサービスの分類に適用を試みる。インターネットサービスで取り扱う情報については、4.2.3.調査結果で示したサービスサイトの定義を用いて「金銭に関連したサービス」及び「個人的な情報に関連したサービス」、これらの金銭、個人情報を含まない「その他のサービス」として検討することができる。各サービス分類における被害規模及び総合的なリスク評価は**表 40** の通りである。

表 40 サービスサイトの定義と被害規模・総合的リスク評価

種別	定義	被害規模	総合的リスク評価
金銭に関連したサービスサイト	クレジットカード情報や銀行口座情報等を取扱うサービス。（例：銀行のオンラインバンキングのサイト、ショッピングサイト等）	中～高程度（金銭的損害）	中～高程度（金銭的損害）
個人的な情報に関連したサービスサイト	ブログやマイクロブログ及び SNS 等を含む個人的な情報や近況を発信するサービスのことであり、情報発信先は特定の個人に限定した場合も限定しない場合も含む。	中程度（機微の度合）	中程度（機微の度合）
その他のサービスサイト	金銭情報や個人情報の配信を行わないサービスのことであり、主に情報収集を目的に利用するサービス。（例：会員制のニュースサイト等）	低（金銭的損害、機微の度合）	低（金銭的損害、機微の度合）

上記で示したサービスサイトにおける総合的なリスク評価を用いて、パスワード及び事前登録知識の実現例を以下に示す。

(2) パスワード・事前登録知識の実現例

電子署名・認証ガイドラインでは、前述した総合的リスク評価を考慮し、抽象的な保証レベルを定義している。「保証レベル 1」は、総合的なリスク影響度が小（金銭的損害がなし、情報に含まれる機微情報がなし）であり、特定される身元識別情報の信用度がほとんどない。この「保証レベル 1」[25]の想定サービスの例にウェブサイトにおけるオンラインディスカッション等がある（OMB M-04-04(米国の連邦政府機関向けの電子認証に関わるガイダンス)参照）。また、「保証レベル 2」は、総合的なリスク影響度が中（金銭的損害が 100 万円未満、情報に含まれる情報は公

[25] なお、電子署名・認証ガイドラインで定義している認証に関する各手段（身元保証、プロセス、トークン）については、電子署名・認証ガイドラインを参照。

知のもの）であり、特定される身元識別情報の信用度がある程度ある。この「保証レベル 2」の想定サービスの例示としては社会保障サービス等である（OMB M-04-04 参照)。電子署名・認証ガイドラインでは、電子署名を用い本人認証の対策基準を示すことを意図しているため、認証情報（トークン）に係るパスワードや事前登録知識は、電子署名を格納した IC カード等を活性化するための PIN を含む（特に、有効期間は IC カードの PIN 設定を想定しているためパスワードの有効期間に設定すべきではない)。そのため、本調査で扱う ID・パスワードによる認証のパスワードに適用することはできないが、総合的なリスク評価に応じたパスワードポリシーの設定を検討する上で参考となる。表 41 に具体的な対策基準の実現例を示す。レベル 1 及びレベル 2 の実現例の中で一般的なインターネットサービス提供において参考になる例はパターン②である。また、この実現例で重要事項を以下に示す。

- 無作為（ランダム）に設定したパスワードの桁数に比べユーザ選択によるパスワードの場合は桁数を長く設定する必要がある。
- ユーザ選択によるパスワードの設定には禁止単語の要件が求められる場合がある。
- すべての設定において連続失敗回数によるパスワード入力可否が定められている。

表 41 トークンの対策基準の実現例
引用:電子政府ガイドライン表 A.3.10

保証レベル	実現例
レベル 1	**【記憶された秘密など(パスワード、事前登録知識の確認など)】** パターン① ・ 文字種:94 種類の文字(アルファベット、数字、記号) ・ 桁数: 4 桁以上の無作為(ランダム)のパスワード ・ 連続失敗: 3 回連続失敗時は 1 日間パスワード入力不可 ・ 有効期間:有効期限 10 年以内 パターン② ・ 文字種:94 種類の文字(アルファベット、数字、記号) かつアルファベット･数字･記号のすべてを用いる ・ 桁数:7 桁以上のユーザ選択によるパスワード ・ 禁止単語:辞書に掲載された単語ではない ・ 連続失敗: 3 回連続失敗時は 1 日間パスワード入力不可 ・ 有効期間:有効期限 10 年以内 パターン③ ・ 文字種:数字 ・ 桁数:8 桁以上の無作為(ランダム)のパスワード ・ 連続失敗:3 回連続失敗時は 1 日間パスワード入力不可 ・ 有効期間:有効期限 10 年以内 パターン④ ・ 文字種:数字 ・ 桁数:8 桁以上のユーザ選択によるパスワード ・ 連続失敗:5 回連続失敗時はパスワード変更を強制
レベル 2	**【記憶された秘密など(パスワード、事前登録知識の確認など)】** パターン① ・ 文字種:94 種類の文字(アルファベット、数字、記号) ・ 桁数:5 桁以上の無作為(ランダム)のパスワード ・ 連続失敗:3 回連続失敗時は 1 日間パスワード入力不可 ・ 有効期間:有効期限 10 年以内

保証レベル	実現例
	パターン② ・ 文字種：94 種類の文字（アルファベット、数字、記号） かつアルファベット・数字・記号のすべてを用いる ・ 桁数：8 桁以上のユーザ選択によるパスワード ・ 禁止単語：辞書に掲載された単語ではない、 ・ 連続失敗：3 回連続失敗時は 1 日間パスワード入力不可 ・ 有効期間：有効期限 10 年以内 パターン③ ・ 文字種：数字 ・ 桁数：9 桁以上の無作為（ランダム）のパスワード ・ 連続失敗：3 回連続失敗時は 1 日間パスワード入力不可 ・ 有効期間：有効期限 10 年以内 パターン④ ・ 文字種：数字 ・ 桁数：12 桁以上のユーザ選択によるパスワード ・ 連続失敗：5 回連続失敗時はパスワード変更を強制
レベル3	**【複数要素認証または複数トークンによる認証】** ・ パスワード付きソフトウェアワンタイムパスワードトークン ・ パスワード付きソフトウェアトークン ・ パスワード付きハードウェアワンタイムパスワードトークン

5.2. インターネットサービス利用者の対策

5.2.1. 安全なオンライン本人認証方式を選択するために

インターネットサービス利用者が安全なオンライン本人認証方式を選択するためには、パスワードリスト攻撃の対象である ID・パスワードによる認証方式だけではなく、他の認証方式を選択するよう検討する必要がある。また、同様のサービスを提供するインターネットサービス提供者が複数存在した場合は、パスワードリスト攻撃の被害にあわないために ID・パスワードによる認証方式以外の認証方式を提供しているインターネットサービス提供者を選択することが望ましい。また、複数の認証方式には、リスクベース認証や新たな ID・パスワードの増加を避けることができる ID 連携等も含まれる。

安全なオンライン本人認証方式を選択するために、どのようなサービス提供者がどのような認証方式を提供しているのかをまとめた情報等[26]もある。新たにインターネットサービスの利用を考える場合には、このような情報を確認することで、より安全なオンライン認証方式を提供しているインターネットサービスを選択することが可能である。一方、現時点では国内のインターネットサービスサイトをまとめた情報は存在せず、掲載情報の網羅性や信頼性及び更新の頻度等は不明なため、インターネットサービス利用者が安心して参照できる情報を整備する必要がある。

なお、リスク分析に基づいた認証方式の選択及び ID・パスワードの検討結果については 5.1.2 を参照。

[26] Two Factor Auth List http://twofactorauth.org/

5.2.2. 現実的な脅威を防ぐために利用者が独自に実施できる対策

前項では、パスワードリスト攻撃の被害にあわないためにID・パスワードによる認証方式以外の認証方式を選択することが望ましいことを述べた。しかし、ID・パスワード方式しか提供しないインターネットサービスも多い。このため、現実的な脅威を防ぐために利用者が独自に実施できる対策について検討した結果を示す。まず、オンライン本人認証において認証情報を適切に管理することはインターネットサービス利用者の責任であり、適切に管理できていないことを原因とした被害についてはインターネットサービス利用者の責任である。現時点の脅威であるパスワードリスト攻撃等への対策を考慮した場合に最低限必要と考えられる検討ポイントを以下に示す。

(1) パスワードリスト攻撃への対策について （最優先）

サービスサイトで取り扱う情報等をパスワードリスト攻撃の脅威から防ぐためには、ID・パスワードの使い回さない、推測が容易なパスワードを設定しない、及びID・パスワードを適切に保存することが必要である。

(2) 認証方式の併用による安全策について （攻撃の検知等による被害低減策）

ID・パスワードによる認証を提供しているインターネットサービスでもリスクベース認証や認証連続失敗回数によって一定期間アカウントロックする機能を提供している場合ある。これらの認証方式や機能を併用することにより、不正アクセス攻撃の検知が可能となる場合もあるため、被害を低減するためにもID・パスワードによる認証とこれらの認証を併用しているインターネットサービスを選択することが望ましい。

(3) その他のパスワード管理策について （さらに安全にする対策）

利用していないアカウントの廃止や、パスワードの履歴保存により数世代前に使用したパスワードへの変更を行わない。

なお、(1)の対策を実施しなければ、これらの対策を実施していてもパスワードリスト攻撃を防ぐことはできないため、はじめにどのようなID・パスワードを設定するか、また設定したID・パスワードをどのように管理するかという基本的な管理策の検討、見直し（(1)の対策）を優先すべきである。

具体的な対策内容を表 42 に示す。なお、下表では「最優先」を◎、「攻撃の検知等による被害低減策」を○、「さらに安全性にする対策」を△としての優先度を示す。

表 42　ID・パスワード管理の優先度について

区分	対策	内容	優先度
既存の ID・パスワードの管理	1.ID・パスワードを使い回さない	インターネットサービス毎に異なる ID・パスワードを設定する。	◎
	2.推測が容易なパスワードを設定しない	推測が容易なパスワードを設定しない。また、文字種や桁数等が少ないサービスは再度利用すべきかを検討する。	◎
	3.ID・パスワードの適切な保存・管理	PC に ID・パスワードを保存する場合には、暗号化等を実施する。ID・パスワード管理を支援するツールを利用する方法及び適切な管理方法[27]を定めて管理することが可能である。	◎
	4.パスワードの定期変更	パスワードを定期的に変更する。※上記 1～3 の適切な保存及び管理・設定方法の検討を優先する必要がある。	◎
	5.パスワードの履歴の保存	数世代前に使用したパスワードへの変更を行わない。※上記 1～3 の適切な保存及び管理・設定方法の検討を優先する必要がある。	△
	6.利用していないアカウントの廃止	利用していないサービスのアカウントを廃止、削除する。一方、他と同じ ID・パスワードを設定していない場合や推測が容易なパスワードを設定していない場合には、この対策の優先度は下がる。 ※上記 1～3 の適切な保存及び管理・設定方法の検討を優先する必要がある。	△
認証方式・サービスの見直し	7.ID・パスワード以外の認証方式を併用しているインターネットサービスを選択する	ID・パスワード以外の認証方式(リスクベース認証等を含む)を併用しているインターネットサービスを選択する	○
	8. ID 連携を採用しているインターネットサービスを選択する	不要な ID・パスワードを増やさないために ID 連携を採用しているインターネットサービスの選択を検討する	○

5.2.3. パスワード管理を支援する参考情報

サービス利用者に求められる ID・パスワードの管理は、管理を支援するツールを利用することで管理コストを軽減できる。以下に、1）メモ帳で管理する場合、2）PC 等にファイルとして保存・管理する場合、3）Web ブラウザに記憶・保存する場合、4）パスワード管理ツールを利用する場合を例に、各管理方法の良い点、検討すべき点、さらに参考となる情報を紹介する。現在のインターネットサービスは、PC 以外にスマートデバイスなど利用できる環境が広がっている。これらの機器に ID・パスワードを保存する方法によっては、機器の共有等の状況により ID・パスワードが他者に漏えいする可能性があるため、下記の検討すべき点を含め、適切な管理方法の検討が望まれる。

[27] パスワードの管理方法や利用方法については、「コンピュータウイルス・不正アクセスの届出状況[2011 年 5 月分]」等情報セキュリティ対策情報を参照　https://www.ipa.go.jp/security/txt/2011/06outline.html

(1) メモ帳（紙媒体）等で管理する場合

一般的な特徴	・ ICT(PC やスマートデバイス)に不慣れな利用者でも運用可能 ・ ツールの購入やインストール等が不要 ・ 異なる PC 等で利用する場合でも、ID・パスワードを保存したファイルの共有が不要 ・ 利用者自らが考えたオリジナルな管理方法の適用が可能(ID とパスワードを別のメモで管理する、パスワードの前後に余分な文字を付け加えておく等)
留意点	・ 第三者に見られないようにメモ帳(紙媒体)の保管場所を検討する必要がある ・ 紛失や置き忘れの対策を検討する必要がある
参考情報	ID とパスワードを別々に保存する方法については、(2)を参照

(2) PC 等にファイルとして保存する場合

一般的な特徴	・ ツールの購入やインストール等が不要 ・ 利用者自らが考えたオリジナルな管理方法の適用が可能(ID とパスワードを別のファイルで管理する、パスワードの前後に余分な文字を付け加えておく等)
留意点	・ 異なる PC 等で利用する場合には、ID・パスワードを保存したファイルの共有方法を検討する必要がある ・ PC の共有時に注意する必要がある
参考情報	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 ～ https://www.ipa.go.jp/security/txt/2013/08outline.html

(3) Web ブラウザに記憶・保存する場合

一般的な特徴	・ 基本的にはツールの購入やインストール等が不要である(一部の拡張機能やツールは有料) ・ 自動的に登録・入力した ID・パスワードを管理できる ・ 複数の ID・パスワードを管理できる ・ ID・パスワードを自動的に暗号化保存する ・ パスワードの自動入力ができる
留意点	・ 一部の Web ブラウザでは、アカウント登録により、異なる PC 環境でも同期が可能となり、ID・パスワードを共有する必要がない一方で、アカウント登録は、他サービスと連動しているため、意図しないアカウント登録やサービス利用(連携)を増やす可能性がある ・ 一部の Web ブラウザでは、管理対象パスワードの表示にはマスターパスワードの入力を必須としている。また、利用している PC の管理者権限でないとパスワードの修正、変更等ができない場合もあり、パスワード管理の権限設定や管理手順等を事前に調査しておく必要がある ・ PC の共有時に注意する必要がある ・ サポートが終了する、セキュリティパッチの適用等、常に情報収集を行う必要がある ・ データをクラウド上に保存するタイプの場合、情報漏えいが懸念される

参考情報	各 Web ブラウザの Q&A 等を参照 ■パスワードを記憶して Web フォームに情報を入力する - Windows ヘルプ http://windows.microsoft.com/ja-jp/internet-explorer/fill-in-forms-remember-passwords-autocomplete#ie=ie-11 ■保存したパスワードを管理する http://windows.microsoft.com/ja-jp/windows-vista/manage-stored-passwords ■Firefox のパスワードマネージャ | Firefox ヘルプ https://support.mozilla.org/ja/kb/password-manager-remember-delete-change-passwords ■ウェブサイトのパスワードを管理する - Chrome ヘルプ https://support.google.com/chrome/answer/95606?hl=ja ■Mac ハンドブック:Safari で Web をブラウズする http://support.apple.com/kb/HT6074?viewlocale=ja_JP

(4) パスワード管理ツールを利用する場合

一般的な特徴	・ 自動的に登録・入力した ID・パスワードを管理できる ・ 複数の ID・パスワードを管理できる ・ ID・パスワードを自動的に暗号化保存する ・ パスワードの自動入力ができる ・ クラウドを介して、様々なデバイス(PC・スマートフォン・タブレット等)で利用できる ・ バックアップを保存することができる ・ パスワード生成も可能なものもあり、自身でパスワードを考える手間がかからない
留意点	・ ツールの購入やインストール等が必要である(フリーソフトもあり) ・ Web ブラウザの拡張機能で実現している場合と個別デバイスの製品がある。それぞれの特徴を調査する ・ 一部の製品では、複数の PC 環境や、PC とスマートデバイス等での共有機能が提供されているため利用する環境に合わせて製品を選択する ・ PC の共有時に注意する必要がある ・ サポート終了やセキュリティパッチの適用等、常に情報収集を行う ・ 偽セキュリティ製品でないかを調査する必要がある ・ データをクラウド上に保存するタイプの場合、情報漏えいなどへ対策がされていることを確認する
参考情報	JNSA のソリューションガイド等を参照 http://www.jnsa.org/JNSASolutionGuide/

5.3. 課題

本調査では、オンライン本人認証方式における実態調査として、近年多発しているパスワードリスト攻撃について、20 件の公開情報調査及び 10 件のインタビュー調査を通じて具体的なインシデント事例を調査した。また、インターネットサービスサイト 130 サイトを対象として、サービス利用者に提供している認証方式及び要求している認証情報について調査し、インターネットサービス利用者 2,060 人を対象として、本人認証に関するアンケート調査を実施した。

以下に引き続き検討が必要な事項について示す。

(1) 指標・ガイドラインの検討

ID・パスワードに関する具体的な指針やガイドラインを求める意見が多数あった。一方、指針やガイドラインが対象とする範囲は、一般的なインターネットサービス全般を対象とする意見と、より具体的に特定分野のサービスのみを対象としたものを求める意見があった。しかし、現在のインターネットサービスは、様々なサービスがあり各々のサービスが連携している場合や様々な環境（PC やスマートデバイス等）に対して提供しているため、すべてのサービスを包含する指針やガイドラインを策定するためには、これらのリスクを評価、分析したうえで汎用的なものとする必要がある。また、特定分野を選定する場合もその分野における必要性を確認する必要がある。指標及びガイドラインの作成については、さらに詳細な調査、分析が必要である。

(2) 脅威情報や対策情報を共有できるスキーム構築や整備

パスワードリスト攻撃による不正アクセスの脅威情報について、アクセス先の IP アドレスや環境（OS 及びブラウザ等）及び不正アクセスに利用された ID・パスワード等を共有することが重要と考えられる。フィッシング対策の一部では、フィッシングサイトの IP アドレスの共有等は実施されているものの ID･パスワードの共有は実施形態を含め議論･検討している状況である。この実施に関しては関連技術（DB 暗号や検索可能暗号）の進展や運用方法を含め、引き続き検討することが望まれる。また、脅威に対抗できるオンライン本人認証方式や対策検討の結果についても情報共有することが重要であり、例えば、ID・パスワード認証の典型的な問題とそれに対する解決策を整理し、再利用できるようにまとめたもの等の検討も必要である。

(3) インターネットサービス提供者の重要情報の管理対策

認証情報の適切な設定・管理は、認証要求者の責任であるため、インターネットサービスの本人認証において設定する ID･パスワードはインターネットサービス利用者が適切に設定、管理することが求められる。一方で、一部のインターネットサービス提供者においては、利用者が設定したパスワードや本人確認に用いる秘密の質問とその回答を暗号化及びハッシュ化せず平文で保存しているサービス提供者もあるため、パスワードリスト攻撃を受けることについては、サービス利用者だけの責任とは言い難い状況である。現状として、これらの管理不備が発生した場合であっても、サービス提供者自らが定めた第三者委員会による調査の結果が公表されるのみであるため、インターネットサービスの安全な利用を促進するためには、サービス提供者に対してこれらの管理不備の自主的な改善を促す取組や仕組みの検討が必要である。

付録１：アンケート調査票

Q1 あなたが安全だと思うパスワードをご記入ください。(現在使っているパスワードは絶対に入力しないでください)※回答は、半角英数字で記入してください。

1. Q1S1【　　】

Q2 パスワードを作成する際、安全性を高めるために必要だと思う事項で当てはまるもの全てをお答えください。※その他の自由回答欄には、現在使っているパスワードを記載しないでください。

☐ 1. 文字数は8文字以上であること
☐ 2. 英字(大文字、小文字含む)、数字、記号を組み合わせた文字列であること
☐ 3. 辞書等に記載されていない文字列であること
☐ 4. 名前や誕生日など、推測されやすい文字列を使わないこと
☐ 5. 他のサイトで用いたパスワードを流用しないこと
☐ 6. その他　具体的に:【　　】[　　]

Q3

あなたが金銭に関連したサービスサイトを利用する際に用いるパスワードについてお答えください。あなたは、どのようなパスワードを設定していますか。最も利用頻度の高いサービスのパスワードの特徴として当てはまるものをお答えください。下記の特徴を組み合わせて利用している場合は当てはまるもの全てをお答えください。(いくつでも)※その他の自由回答欄には、現在使っているパスワードを記載しないでください。

☐ 1. ご自身・ご家族等のお名前にちなんだもの
☐ 2. ご自身・ご家族等の誕生日にちなんだもの
☐ 3. ご自身・ご家族の電話番号にちなんだもの
☐ 4. 123456等の簡単な数字列
☐ 5. 111111等の同じ数字の数字列
☐ 6. password、iloveyou等の英単語、英文
☐ 7. aaaaaa等の同じ英文字の文字列
☐ 8. password123などの英単語と簡単な数字列の組み合わせ
☐ 9. ランダムな数字の組み合わせ
☐ 10. ランダムな英文字の組み合わせ
☐ 11. ランダムな英数字の組み合わせ
☐ 12. ランダムな英数字と記号の組み合わせ
☐ 13. その他　具体的に:【　　】[　　]
☐ 14. サービスを利用していない(パスワードを登録していない)

Q4 あなたが個人的な情報に関連したサービスサイトを利用する際に用いるパスワードについてお答えください。あなたは、どのようなパスワードを設定していますか。最も利用頻度の高いサービスのパスワードの特徴として当てはまるものをお答えください。下記の特徴を組み合わせて利用している場合は当てはまるもの全てをお答えください。(いくつでも)※その他の自由回答欄には、現在使っているパスワードを記載しないでください。

☐ 1. ご自身・ご家族等のお名前にちなんだもの
☐ 2. ご自身・ご家族等の誕生日にちなんだもの
☐ 3. ご自身・ご家族の電話番号にちなんだもの
☐ 4. 123456等の簡単な数字列
☐ 5. 111111等の同じ数字の数字列
☐ 6. password、iloveyou等の英単語、英文
☐ 7. aaaaaa等の同じ英文字の文字列
☐ 8. password123などの英単語と簡単な数字列の組み合わせ
☐ 9. ランダムな数字の組み合わせ
☐ 10. ランダムな英文字の組み合わせ
☐ 11. ランダムな英数字の組み合わせ
☐ 12. ランダムな英数字と記号の組み合わせ
☐ 13. その他　具体的に:【　　】[　　]
☐ 14. サービスを利用していない(パスワードを登録していない)

Q5

あなたがその他のサービスサイトを利用する際に用いるパスワードについてお答えください。あなたは、どのようなパスワードを設定していますか。最も利用頻度の高いサービスのパスワードの特徴として当てはまるものをお答えください。下記の特徴を組み合わせて利用している場合は当てはまるもの全てをお答えください。(いくつでも)※その他の自由回答欄には、現在使っているパスワードを記載しないでください。

- □ 1. ご自身・ご家族等のお名前にちなんだもの
- □ 2. ご自身・ご家族等の誕生日にちなんだもの
- □ 3. ご自身・ご家族の電話番号にちなんだもの
- □ 4. 123456等の簡単な数字列
- □ 5. 111111等の同じ数字の数字列
- □ 6. password、iloveyou等の英単語、英文
- □ 7. aaaaaa等の同じ英文字の文字列
- □ 8. password123などの英単語と簡単な数字列の組み合わせ
- □ 9. ランダムな数字の組み合わせ
- □ 10. ランダムな英文字の組み合わせ
- □ 11. ランダムな英数字の組み合わせ
- □ 12. ランダムな英数字と記号の組み合わせ
- □ 13. その他　具体的に:【　】[　]
- □ 14. サービスを利用していない(パスワードを登録していない)

Q6　あなたは、複数のサービスサイトで同一のパスワードを利用していますか。(いくつでも)

	1 金銭に関連したサービスサイトのサービスと同一のパスワードを利用している	2 個人的な情報に関連したサービスサイトのサービスと同一のパスワードを利用し	3 その他のサービスサイトのサービスと同一のパスワードを利用している	4 他のサービスと同一のパスワードは利用していない	5 複数のサービスサイトを利用していない
1. 金銭に関連したサービスサイト	□	□	□	□	□
2. 個人的な情報に関連したサービスサイト	□	□	□	□	□
3. その他のサービスサイト	□	□	□	□	□

Q7　あなたが、いくつかのサービスで同一のパスワードを利用している理由をお答えください。(いくつでも)

- ☐ 1. ひとつのパスワードを利用していると簡単だから
- ☐ 2. 複数のパスワードを管理するのが手間だから
- ☐ 3. パスワードを忘れてしまうから
- ☐ 4. 愛着のあるパスワードだから
- ☐ 5. 覚えやすいパスワードだから
- ☐ 6. その他　具体的に:【　】[　]

Q8　あなたは、パスワードをどのくらいの周期で変更していますか。複数サイトを利用している場合は、最も利用頻度の高いサービスについてお答えください。(1つずつ)

	1 2週間以内	2 2週間以上～1ヶ月未満	3 1ヶ月以上～3ヶ月未満	4 3ヶ月以上～6ヶ月未満	5 6ヶ月以上～1年未満	6 1年以上の周期	7 変更したことがない
1. 金銭に関連したサービスサイト	○	○	○	○	○	○	○
2. 個人的な情報に関連したサービスサイト	○	○	○	○	○	○	○
3. その他のサービスサイト	○	○	○	○	○	○	○

Q9　あなたは、パスワードをどのタイミングで変更していますか。複数サイトを利用している場合は、最も利用頻度の高いサービスについてお答えください。(1つずつ)※この場合、警告とは「パスワードを変更しましょう」や「前回パスワードを設定してからXX日過ぎています」といった　サービスサイトからの警告文を示しています。

	1 変更を促す警告によって変更する	2 変更を促す警告を受けても変更しない	3 変更を促す警告が来る前に変更する	4 変更を促す警告を見たことがない
1. 金銭に関連したサービスサイト	○	○	○	○
2. 個人的な情報に関連したサービスサイト	○	○	○	○
3. その他のサービスサイト	○	○	○	○

Q10 あなたが、金銭に関連したサービスサイトを利用する際に情報を登録する際の考え方について当てはまるものをお答えください。(1つずつ)

		1 抵抗がある	2 やや抵抗がある	3 どちらでもない	4 あまり抵抗はない	5 抵抗はない
1.	口座番号やクレジットカード情報	○	○	○	○	○
2.	住所、氏名、性別、生年月日などの個人の情報	○	○	○	○	○
3.	顔(ただし、データは顔認証のために利用する)	○	○	○	○	○
4.	指紋、網膜、虹彩、静脈	○	○	○	○	○
5.	所属組織名(会社名、学校名)	○	○	○	○	○
6.	年収や資産情報	○	○	○	○	○
7.	健康保険証番号、免許証番号	○	○	○	○	○

Q11 あなたが、個人的な情報に関連したサービスサイトを利用する際に情報を登録する際の考え方について当てはまるものをお答えください。(1つずつ)

		1 抵抗がある	2 やや抵抗がある	3 どちらでもない	4 あまり抵抗はない	5 抵抗はない
1.	口座番号やクレジットカード情報	○	○	○	○	○
2.	住所、氏名、性別、生年月日などの個人の情報	○	○	○	○	○
3.	顔(ただし、データは顔認証のために利用する)	○	○	○	○	○
4.	指紋、網膜、虹彩、静脈	○	○	○	○	○
5.	所属組織名(会社名、学校名)	○	○	○	○	○
6.	年収や資産情報	○	○	○	○	○
7.	健康保険証番号、免許証番号	○	○	○	○	○

Q12

あなたが、その他のサービスサイトを利用する際に情報を登録する際の考え方について当てはまるものをお答えください。(1つずつ)

	1 抵抗がある	2 やや抵抗がある	3 どちらでもない	4 あまり抵抗はない	5 抵抗はない
1. 口座番号やクレジットカード情報	○	○	○	○	○
2. 住所、氏名、性別、生年月日などの個人の情報	○	○	○	○	○
3. 顔(ただし、データは顔認証のために利用する)	○	○	○	○	○
4. 指紋、網膜、虹彩、静脈	○	○	○	○	○
5. 所属組織名(会社名、学校名)	○	○	○	○	○
6. 年収や資産情報	○	○	○	○	○
7. 健康保険証番号、免許証番号	○	○	○	○	○

Q13 あなたは、このIDサーバについてどのように考えますか。当てはまるものをお答えください。(1つ)

○ 1. 良い仕組みだと思う
○ 2. どちらともいえない
○ 3. 良くない仕組みだと思う

Q14 あなたは、このIDサーバを使いたいと思いますか。当てはまるものをお答えください。(1つ)

○ 1. 使ってみたい
○ 2. どちらともいえない
○ 3. 使いたくはない

Q15 あなたは、このIDサーバの利便性についてどのように考えますか。当てはまるものをお答えください。(1つ)

○ 1. 便利である
○ 2. どちらともいえない
○ 3. 便利ではない

Q16 あなたは、このIDサーバの安全性についてどのように考えますか。当てはまるものをお答えください。(1つ)

○ 1. 被害をこうむるかもしれない
○ 2. わからない
○ 3. 安全である

Q17

IDサーバに登録したIDや個人情報がサイバー攻撃にあったときの盗難保険(※)が付与されているならば、IDサーバ利用に際して、利用料(保険料)を支払っても良いと思いますか。当てはまるものをお答えください。(ひとつ)(※)現在、クレジットカード等に付帯されている、盗難に備えた保険のこと。例えば、クレジットカードの盗難保険料は　　10～100円／年、携帯電話の盗難保険料(携帯補償)は約400円／月程度です。

○ 1. 支払ってもよい
○ 2. 支払いたくない

Q18 利用料としてどの程度の価格を支払っても良いと思いますか。1円～1万円の範囲内でお答えください。

1. Q18S1【　　】円
2. Q18S2【　　】円
3. Q18S3【　　】円
4. Q18S4【　　】円

Q19 あなたが、金銭に関連したサービスサイトを利用する際に望ましいと思う本人確認方法（認証方式）について、以下のそれぞれについてお答えください。（1つずつ）

		1 望ましいと思う	2 望ましいとは思わない
1.	サービスサイトとのあなたとの間で共有する秘密情報を使った認証(ID・パスワード（この時のパスワードは、8文字以上で推測しにくい英数字・記号の組み合わせとする）による認証など）	○	○
2.	会員登録時などあらかじめサイトに登録した質問とその回答による認証（「ペットの名前は？」、「母親の旧姓は？」といった質問等による認証）	○	○
3.	サービスサイトからあらかじめ渡された、または通知される秘密情報を使った認証(マトリックスカードや、読みにくい英数字などが表示され、その内容を入力する認証など（CAPTCHA））	○	○
4.	会員登録時などにあらかじめ登録した携帯電話等の別の媒体に通知されるテキストによる認証	○	○
5.	パスワード生成器などによって生成される使い捨てパスワードによる認証	○	○
6.	暗号機能をもつハードウエアによる認証(高度な暗号処理を行う情報で認証）	○	○
7.	2種類の認証方式を使い、2つ目の認証は、何らかの秘密情報を使った認証（暗号機能を使うための情報）	○	○
8.	2種類の認証方式を使い、2つ目の認証は、パスワード生成器などによって生成される使い捨てパスワードによる認証	○	○
9.	2種類の認証方式を使い、2つ目の認証は、ICカードなどの暗号機能をもつハードウエアによる認証	○	○

Q20 あなたが、個人的な情報に関連したサービスサイトを利用する際に望ましいと思う本人確認方法（認証方式）について、以下のそれぞれについてお答えください。（1つずつ）

		1 望ましいと思う	2 望ましいとは思わない
1.	サービスサイトとのあなたとの間で共有する秘密情報を使った認証(ID・パスワード（この時のパスワードは、8文字以上で推測しにくい英数字・記号の組み合わせとする）による認証など）	○	○
2.	会員登録時などあらかじめサイトに登録した質問とその回答による認証（「ペットの名前は？」、「母親の旧姓は？」といった質問等による認証）	○	○
3.	サービスサイトからあらかじめ渡された、または通知される秘密情報を使った認証(マトリックスカードや、読みにくい英数字などが表示され、その内容を入力する認証など（CAPTCHA））	○	○
4.	会員登録時などにあらかじめ登録した携帯電話等の別の媒体に通知されるテキストによる認証	○	○
5.	パスワード生成器などによって生成される使い捨てパスワードによる認証	○	○
6.	暗号機能をもつハードウエアによる認証(高度な暗号処理を行う情報で認証）	○	○
7.	2種類の認証方式を使い、2つ目の認証は、何らかの秘密情報を使った認証（暗号機能を使うための情報）	○	○
8.	2種類の認証方式を使い、2つ目の認証は、パスワード生成器などによって生成される使い捨てパスワードによる認証	○	○
9.	2種類の認証方式を使い、2つ目の認証は、ICカードなどの暗号機能をもつハードウエアによる認証	○	○

Q21 あなたが、その他のサービスサイトを利用する際に望ましいと思う本人確認方法（認証方式）について、以下のそれぞれについてお答えください。（1つずつ）

		1 望ましいと思う	2 望ましいとは思わない
1.	サービスサイトとのあなたとの間で共有する秘密情報を使った認証(ID・パスワード（この時のパスワードは、8文字以上で推測しにくい英数字・記号の組み合わせとする）による認証など）	○	○
2.	会員登録時などあらかじめサイトに登録した質問とその回答による認証（「ペットの名前は？」、「母親の旧姓は？」といった質問等による認証）	○	○
3.	サービスサイトからあらかじめ渡された、または通知される秘密情報を使った認証(マトリックスカードや、読みにくい英数字などが表示され、その内容を入力する認証など（CAPTCHA））	○	○
4.	会員登録時などにあらかじめ登録した携帯電話等の別の媒体に通知されるテキストによる認証	○	○
5.	パスワード生成器などによって生成される使い捨てパスワードによる認証	○	○
6.	暗号機能をもつハードウエアによる認証(高度な暗号処理を行う情報で認証）	○	○
7.	2種類の認証方式を使い、2つ目の認証は、何らかの秘密情報を使った認証（暗号機能を使うための情報）	○	○
8.	2種類の認証方式を使い、2つ目の認証は、パスワード生成器などによって生成される使い捨てパスワードによる認証	○	○
9.	2種類の認証方式を使い、2つ目の認証は、ICカードなどの暗号機能をもつハードウエアによる認証	○	○

Q22 普段、あなたはどのような形でIDやパスワードを保管していますか。（いくつでも）

□ 1. 記憶している
□ 2. パソコン内部に記録している
□ 3. インターネットブラウザに記憶させている
□ 4. パスワード管理ツールを利用している
□ 5. サービスを利用する端末とは別の端末に保存している
□ 6. 紙に記載して保管している
□ 7. 自分宛てにパスワードを記載したメールを送信する
□ 8. その他　具体的に:【　　】[　　]

Q23 ログインする端末によって、IDやパスワードの保管の方法に違いがありますか。(ひとつ)

- ○ 1. 違いがある→ 具体的に:【 】[ ]
- ○ 2. 違いはない

Q24 あなたは、インターネット上のサービスサイトを利用するためのIDをいくつお持ちですか。

- ○ 1. 1個
- ○ 2. 2個
- ○ 3. 3個
- ○ 4. 4個
- ○ 5. 5個
- ○ 6. 6個
- ○ 7. 7個
- ○ 8. 8個
- ○ 9. 9個
- ○ 10. 10個
- ○ 11. 11個
- ○ 12. 12個
- ○ 13. 13個
- ○ 14. 14個
- ○ 15. 15個
- ○ 16. 16個
- ○ 17. 17個
- ○ 18. 18個
- ○ 19. 19個
- ○ 20. 20個
- ○ 21. 21個
- ○ 22. 22個
- ○ 23. 23個
- ○ 24. 24個
- ○ 25. 25個
- ○ 26. 26個
- ○ 27. 27個
- ○ 28. 28個
- ○ 29. 29個
- ○ 30. 30個
- ○ 31. 31個～40個
- ○ 32. 41個～50個
- ○ 33. 51個以上

Q25 あなたが記憶することができると自信のある最大のIDの数はいくつですか。(ひとつ)(各IDには関連するパスワードも同数管理する(記憶できる)ことを前提とします)

- ○ 1. 0個
- ○ 2. 1個
- ○ 3. 2個
- ○ 4. 3個
- ○ 5. 4個
- ○ 6. 5個
- ○ 7. 6個
- ○ 8. 7個
- ○ 9. 8個
- ○ 10. 9個
- ○ 11. 10個
- ○ 12. 11～15個
- ○ 13. 16～20個
- ○ 14. 21～30個
- ○ 15. 31～40個
- ○ 16. 41～50個
- ○ 17. 51個以上

Q26

あなたが新規に利用したいサービスを見つけて、会員登録しようと思った場合に、記憶できる最大のIDの数を上回っていた（これ以上記憶できない）としたらどのように対応しますか。（ひとつ）（各IDには関連するパスワードも同数管理する（記憶できる）ことを前提とします）

○ 1. IDを記憶できないので、サービスの利用を断念する
○ 2. 使い捨ててもよい情報（偽りの情報を含む）を登録し、サービスを利用する
○ 3. 記憶できなくなるかもしれないがサービス登録し、利用する
○ 4. 記憶ではなくツールなどで管理できるようにしてサービス登録し、利用する
○ 5. 他のサービスと同じものを登録する
○ 6. 記憶ではなくメモなどに記録してサービス登録し、利用する
○ 7. その他　具体的に:【　】[　]

Q27 あなたはパスワードを忘れたとき、どうしますか。（ひとつ）

○ 1. 再発行の手続きをする
○ 2. そのサイトを利用することをあきらめる
○ 3. これまでにパスワードを忘れたことはない

Q28

もしも、あなたがいつも利用しているショッピングサイトが、セキュリティを確保するため認証方式を変更することになったとしたら、どの程度の変更であれば、あなたはショッピングサイトを継続的に利用したいと思いますか。当てはまるもの全てをお答えください。ショッピングサイトを利用していない場合は、許容できる範囲の認証方式全てについてお答えください。（いくつでも）

□ 1. 8文字以上のパスワードの設定が必要
□ 2. 12文字以上のパスワードの設定が必要
□ 3. 英字（大文字、小文字含む）と数字、記号が組み合わさった文字列のパスワードの設定が必要
□ 4. IDをメールアドレス以外のものに設定することが必要
□ 5. パスワードを1ヶ月以内に変更することが必要
□ 6. 第一パスワードのほか、第二パスワード等、複数のパスワードの設定が必要
□ 7. IDとパスワードにかえて他の認証が必要（トークン（使い捨てパスワード・サービスから送られてくる秘密情報等）等）
□ 8. IDとパスワード以外にも生体認証等のほかの認証方式と合わせた認証が必要
□ 9. その他　具体的に:【　】[　]
□ 10. 認証方式を変更しなければならないならば、継続利用しない

Q29

あなたが、金銭に関連したサービスサイトを利用する際に用いるIDについてお答えください。最も利用頻度の高いサービスのIDの特徴として当てはまるものをお答えください。下記の特徴を組み合わせて利用している場合は当てはまるもの全てをお答えください。（いくつでも）

□ 1. 任意の英単語
□ 2. 任意の英単語と数字の組み合わせ
□ 3. メールアドレス
□ 4. 電話番号
□ 5. お名前
□ 6. ランダムな英文字の組み合わせ
□ 7. ランダムな英数字の組み合わせ
□ 8. サービス提供者から割り当てられたもの
□ 9. その他　具体的に:【　】[　]

Q30

あなたが、個人的な情報に関連したサービスサイトを利用する際に用いるIDについてお答えください。最も利用頻度の高いサービスのIDの特徴として当てはまるものをお答えください。下記の特徴を組み合わせて利用している場合は当てはまるもの全てをお答えください。(いくつでも)

- ☐ 1. 任意の英単語
- ☐ 2. 任意の英単語と数字の組み合わせ
- ☐ 3. メールアドレス
- ☐ 4. 電話番号
- ☐ 5. お名前
- ☐ 6. ランダムな英文字の組み合わせ
- ☐ 7. ランダムな英数字の組み合わせ
- ☐ 8. サービス提供者から割り当てられたもの
- ☐ 9. その他　具体的に:【　　】[　　]

Q31

あなたが、その他のサービスサイトを利用する際に用いるIDについてお答えください。最も利用頻度の高いサービスのIDの特徴として当てはまるものをお答えください。下記の特徴を組み合わせて利用している場合は当てはまるもの全てをお答えください。(いくつでも)

- ☐ 1. 任意の英単語
- ☐ 2. 任意の英単語と数字の組み合わせ
- ☐ 3. メールアドレス
- ☐ 4. 電話番号
- ☐ 5. お名前
- ☐ 6. ランダムな英文字の組み合わせ
- ☐ 7. ランダムな英数字の組み合わせ
- ☐ 8. サービス提供者から割り当てられたもの
- ☐ 9. その他　具体的に:【　　】[　　]

Q32　下記の項目について、あなたのインターネットを利用する際の考え方に近いものをご回答ください。(ひとつずつ)

		1 そう思う	2 どちらかといえばそう思う	3 どちらともいえない	4 どちらかといえばそう思わない	5 そう思わない
1.	安全なパスワードを設定している人は、特別にセキュリティ意識の高い人だ	○	○	○	○	○
2.	安全なパスワードを設定する人は暇な人だ	○	○	○	○	○
3.	安全なパスワードを設定することに良い印象をもつ	○	○	○	○	○
4.	安全なパスワードを設定している人は少ない	○	○	○	○	○
5.	今後は、安全なパスワードを設定する人が増えそうだ	○	○	○	○	○
6.	安全なパスワードを設定することに関心を持つ人が増えている	○	○	○	○	○
7.	周囲の人が安全なパスワードを設定し始めたら、自分も関心をもつと思う	○	○	○	○	○
8.	安全なパスワードを設定することは考慮するほどの重要事項ではない	○	○	○	○	○
9.	安全なパスワードについて深く検討したことがない	○	○	○	○	○
10.	世の中の状況に沿ってセキュリティ対策をしている	○	○	○	○	○
11.	安全なパスワード設定をすることが世の中から期待されている	○	○	○	○	○
12.	安全なパスワードを設定することは評価される	○	○	○	○	○
13.	私は、安全なパスワードを設定したい	○	○	○	○	○
14.	私は、安全なインターネットの利用に貢献したい	○	○	○	○	○
15.	私は、情報セキュリティに強い関心を持っている	○	○	○	○	○

Q33　あなたが安全なパスワードを設定することについて考えをお答えください。(ひとつずつ)

		1 そう思う	2 どちらかといえばそう思う	3 どちらともいえない	4 どちらかといえばそう思わない	5 そう思わない
1.	安全なパスワードを設定することは、安全なインターネット利用によいことだ	○	○	○	○	○
2.	安全なパスワードを設定することは、自分のためによいことだ	○	○	○	○	○
3.	安全なパスワードを設定することに非常に関心を持っている	○	○	○	○	○
4.	安全なパスワードを設定することは、その利点(メリット)を比較すると手間がかかりすぎる	○	○	○	○	○
5.	安全なパスワードの設定を検討する余裕はある	○	○	○	○	○
6.	安全なパスワードを設定するための手間は惜しまない	○	○	○	○	○

Q34　下記の項目について、あなたのインターネット利用状況に近いものをご回答ください。(ひとつずつ)

		1 すでに設定している	2 設定するつもりだ(具体的な予定がある)	3 そのうち設定するつもりだ(具体的な予定はない)	4 今のところ設定するつもりはない(状況次第である)	5 設定するつもりはない
1.	特に条件はなく安全なパスワードを設定したい	○	○	○	○	○
2.	運用が複雑であったり、記憶することが困難である等がなければ安全なパスワードを設定したい	○	○	○	○	○
3.	記憶することが困難であったり、運用が複雑でも安全なパスワードを設定したい	○	○	○	○	○

Q35　下記の項目について、あなたのインターネットを利用する際の考え方に近いものをご回答ください。(ひとつずつ)

		1 そう思う	2 どちらかといえばそう思う	3 どちらかといえばそう思わない	4 そう思わない
1.	パスワードの安全性が低いことで、深刻な被害を受けるだろう	○	○	○	○
2.	将来、自分自身が被害を受ける可能性があるだろう	○	○	○	○
3.	安全性の高いパスワードを利用することは、被害を防ぐことに有効だ	○	○	○	○
4.	安全性の高いパスワードを設定することは、自分にとって技術的・知識的に難しい	○	○	○	○
5.	安全性の高いパスワードを設定することは、自分にとって、実行に伴う負担やリスクが大きい	○	○	○	○
6.	自分には安全性の高いパスワードを設定する責任がある	○	○	○	○
7.	多くの人が安全性の高いパスワードを設定しているだろう	○	○	○	○
8.	自分が安全性の高いパスワードを設定することを周囲の人たちは期待しているだろう	○	○	○	○
9.	自分だけは、被害を受けないで済むだろう	○	○	○	○

Q36　現在、あなたはどのような機器でインターネットに接続していますか。(いくつでも)

□ 1. パソコン
□ 2. スマートフォン(Android、iPhone、Blackberry、Windows Phone、Windows Mobile等)
□ 3. スマートフォン以外の携帯電話・PHS
□ 4. タブレット端末
□ 5. テレビ(※)インターネットの接続を行っている場合のみ選択
□ 6. ゲーム機
□ 7. その他　具体的に:【　】[　]

Q37 あなたが、利用しているインターネットサービスをお答えください。(いくつでも)

- □ 1. 銀行・信託
- □ 2. 証券
- □ 3. クレジットカード
- □ 4. キャッシング
- □ 5. 保険
- □ 6. 総合通販(ギフト・インテリア・日用雑貨・美容・健康等)
- □ 7. 音楽・書籍購入
- □ 8. ゲーム
- □ 9. 家電・パソコン
- □ 10. ファッション
- □ 11. 運輸
- □ 12. 旅行・宿泊
- □ 13. 人材紹介・転職・就職
- □ 14. ポータルサイト(Yahoo!、Googleなど)
- □ 15. SNS
- □ 16. アンケート
- □ 17. イベント開催支援
- □ 18. レンタカー・タクシー予約
- □ 19. 教育(e-Learning、英会話)
- □ 20. ホテル
- □ 21. 通信
- □ 22. ヘルスケア
- □ 23. クーポン(共同購入)
- □ 24. 報道・ニュース
- □ 25. その他　具体的に:【　　】[　　]
- □ 26. 特にない

Q38 あなたのICT(情報通信技術)活用度として当てはまるものをお答えください。(ひとつ)

- ○ 1. メールの送信、ブログ・SNS等の書き込みなど、自ら情報発信を積極的に行っている
- ○ 2. メールの送受信、ホームページ・ブログ・SNS等の閲覧・書き込みなど、ネット利用には支障はないレベルである
- ○ 3. メールの受信や、情報の検索、特定のホームページ・ブログ・SNS等の閲覧など、情報収集目的の利用は自分ひとりで可能であるが、自ら情報を発信するような利用は難しい
- ○ 4. メールの受信や、情報の検索、特定のホームページ・ブログ・SNS等の閲覧など、情報収集目的の利用について、誰かの補助や助言があれば実施できる
- ○ 5. 上記のようなことをやった経験がほとんどない／上記のようなことはできない

Q39 あなたの世帯の年収は、税込みでおよそどのくらいですか。(ひとつ)

- ○ 1. 200万円未満
- ○ 2. 200万円～400万円未満
- ○ 3. 400万円～600万円未満
- ○ 4. 600万円～800万円未満
- ○ 5. 800万円～1，000万円未満
- ○ 6. 1，000万円～1，500万円未満
- ○ 7. 1，500万円～2，000万円未満
- ○ 8. 2，000万円以上

Q40 あなたの最終学歴をお答えください。(ひとつ)

- ○ 1. 大卒以上
- ○ 2. 高専・短大卒
- ○ 3. 高卒
- ○ 4. 中卒
- ○ 5. その他　具体的に:【　　】[　　]

付録 2：その他のアンケート調査結果票

本文で説明していないアンケート結果を示す。

① ID やパスワードの管理方法

図 70 に、ログインする端末によって、ID やパスワードの保管方法に違いがあるかどうかの結果を示す。この結果にあると、「違いがある」という回答は 3.3%で、大多数の回答者が端末に関係なく同じような保管方法をとっていることが読み取れる。

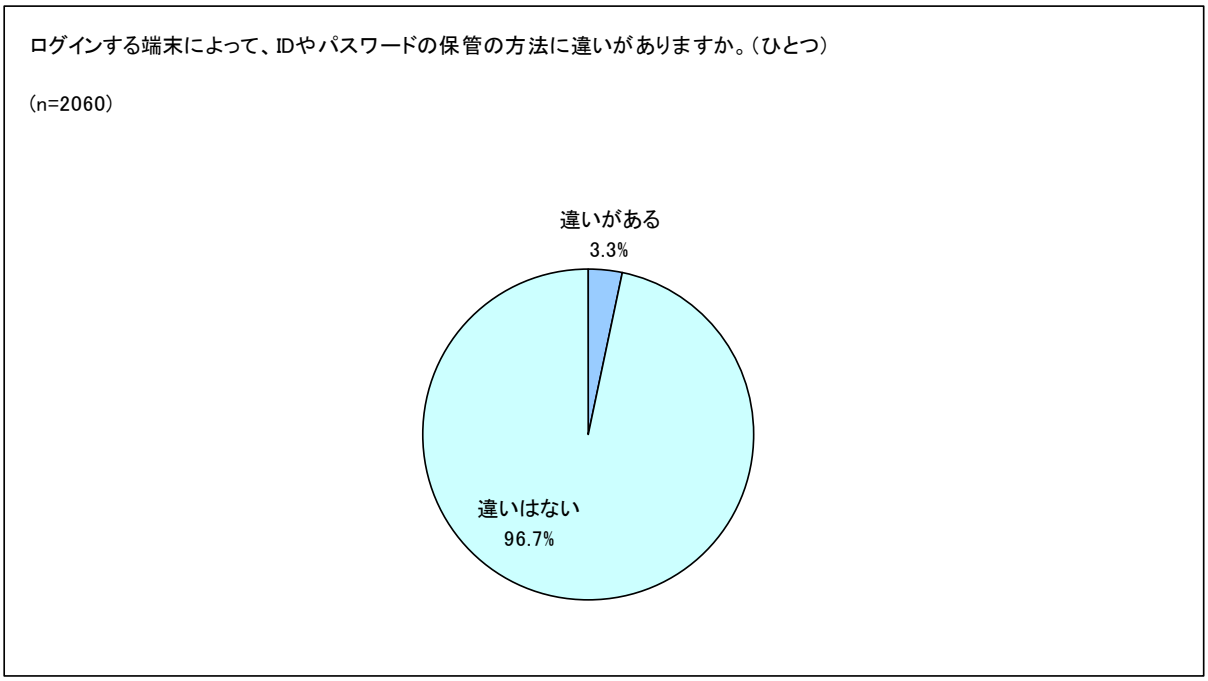


図 70　端末によって ID やパスワードの管理方法に違いがあるか

図 71 に、パスワードを忘れた際の対応の結果を示す。この結果によると、「再発行の手続きをする」が 91.5%である。

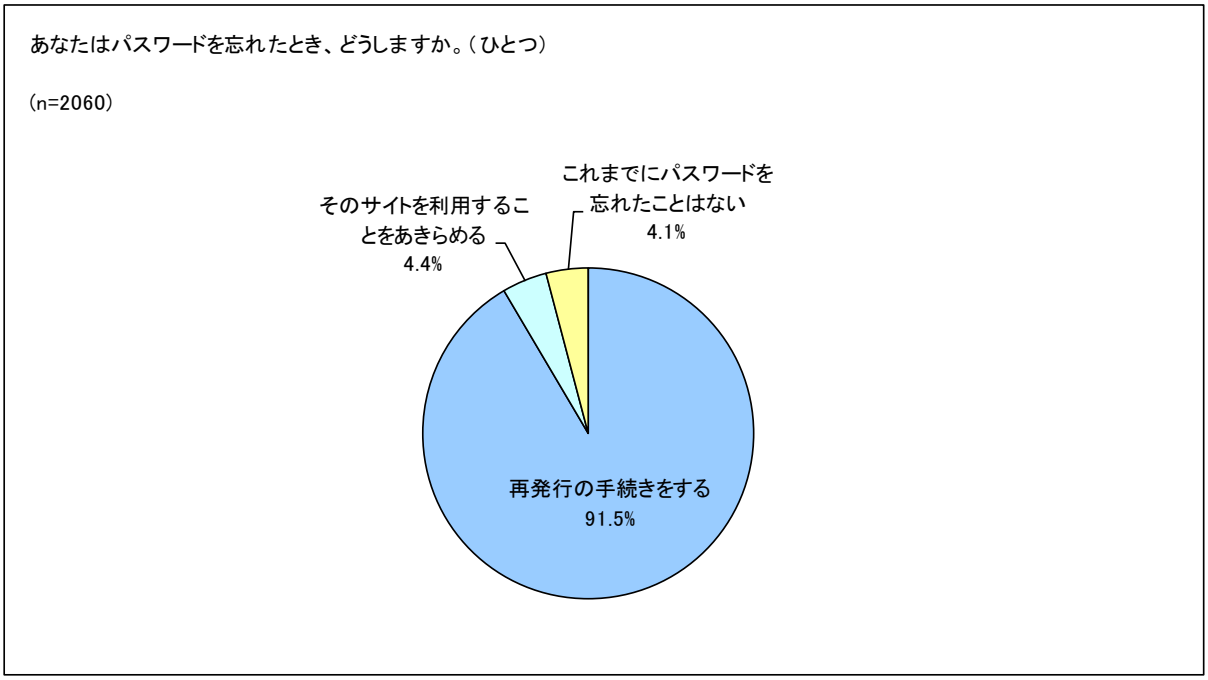


図 71　パスワードを忘れた際の対応

② サービスサイト利用の際の考え方

図 72 は、金銭に関連したサービスサイトを利用する際に、各種情報を登録することについてどの程度、抵抗があるかを示した結果である。「抵抗がある」「やや抵抗がある」の結果に着目すると、顔、健康保険証番号／免許証番号、口座やクレジットカード情報は、他の情報と比較して、抵抗感が強い。ただし、金銭に関連したサービスサイトでは、サービスをするために口座やクレジットカード情報が欠かせない場合も多いため、他のサービスサイトと比較すると抵抗感は低い。

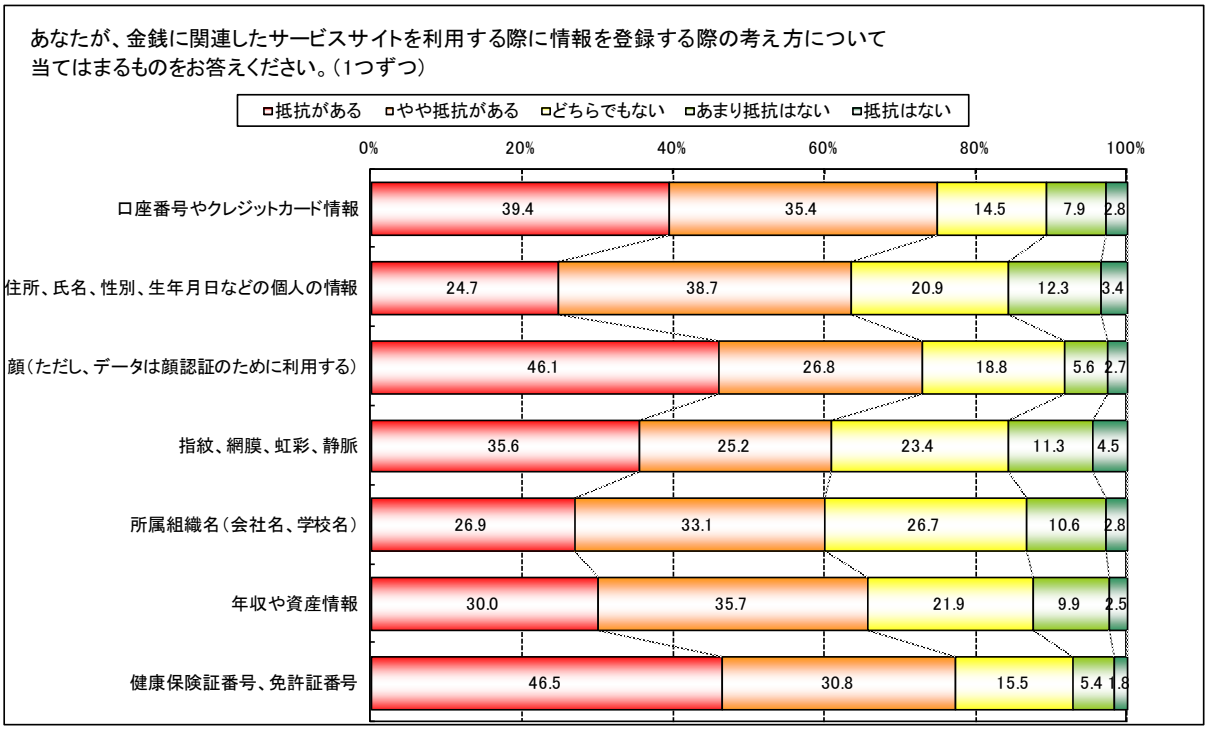


図 72　情報を登録する際の考え方（金銭に関連したサービスサイト）

図 73 は、個人的な情報に関連したサービスサイトを利用する際に、各種情報を登録することについてどの程度、抵抗があるかを示した結果である。「抵抗がある」「やや抵抗がある」の結果に着目すると、口座やクレジットカード情報、健康保険証番号／免許証番号、顔の順序で、抵抗感が強い結果となった。上述のように、金銭に関連したサービスサイトと比較すると、個人的な情報に関連したサービスサイトで各種情報を登録する方が抵抗感は強いという傾向が見られる。

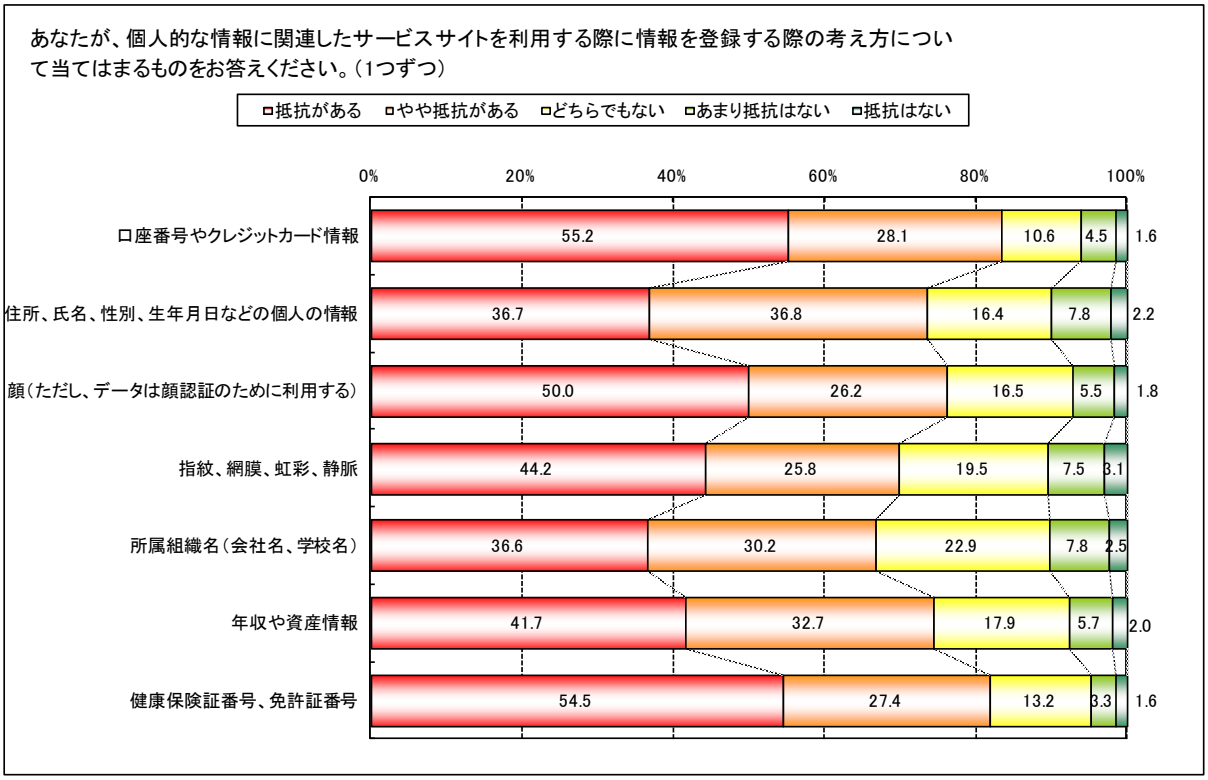


図 73　情報を登録する際の考え方（個人的な情報に関連したサービスサイト）

図 74 は、その他のサービスサイトを利用する際に、各種情報を登録することについてどの程度、抵抗があるかを示した結果である。「抵抗がある」「やや抵抗がある」の結果に着目すると、個人的な情報に関連したサービスサイトと同様に、口座やクレジットカード情報、健康保険証番号／免許証番号、顔の順序で、抵抗感が強いという結果となった。

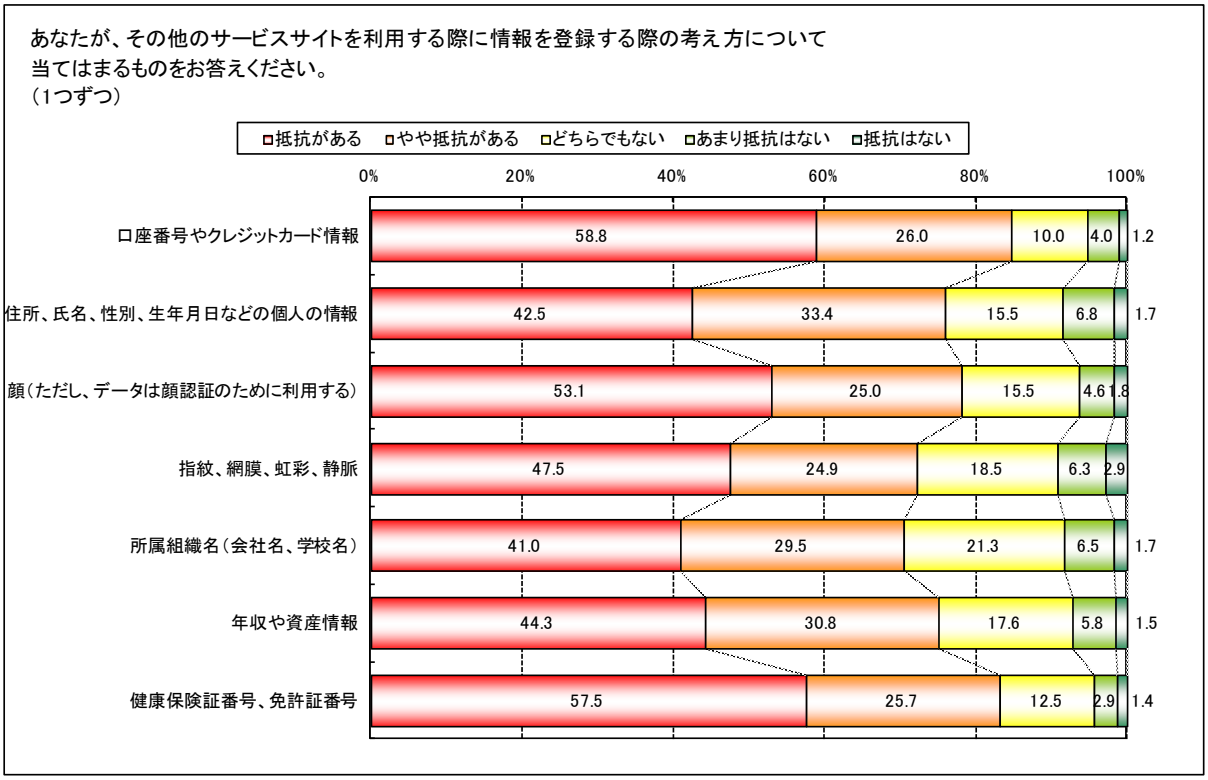


図 74　情報を登録する際の考え方（その他のサービスサイト）

③　インターネット利用の際の考え方（詳細）

図 75、図 76 に、インターネット利用の際の考え方の結果を示す。

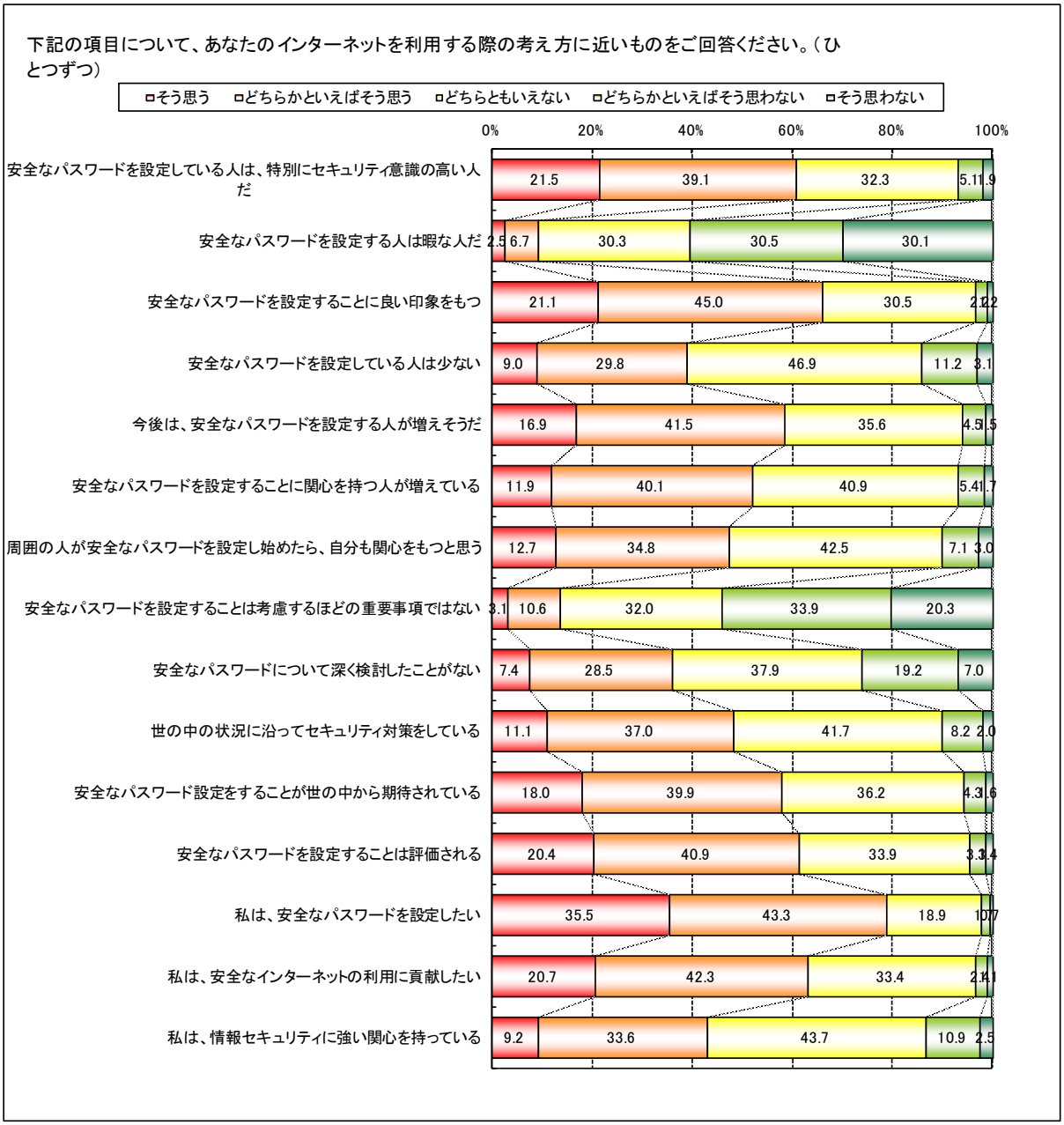


図 75　インターネット利用の際の考え方（その 1）

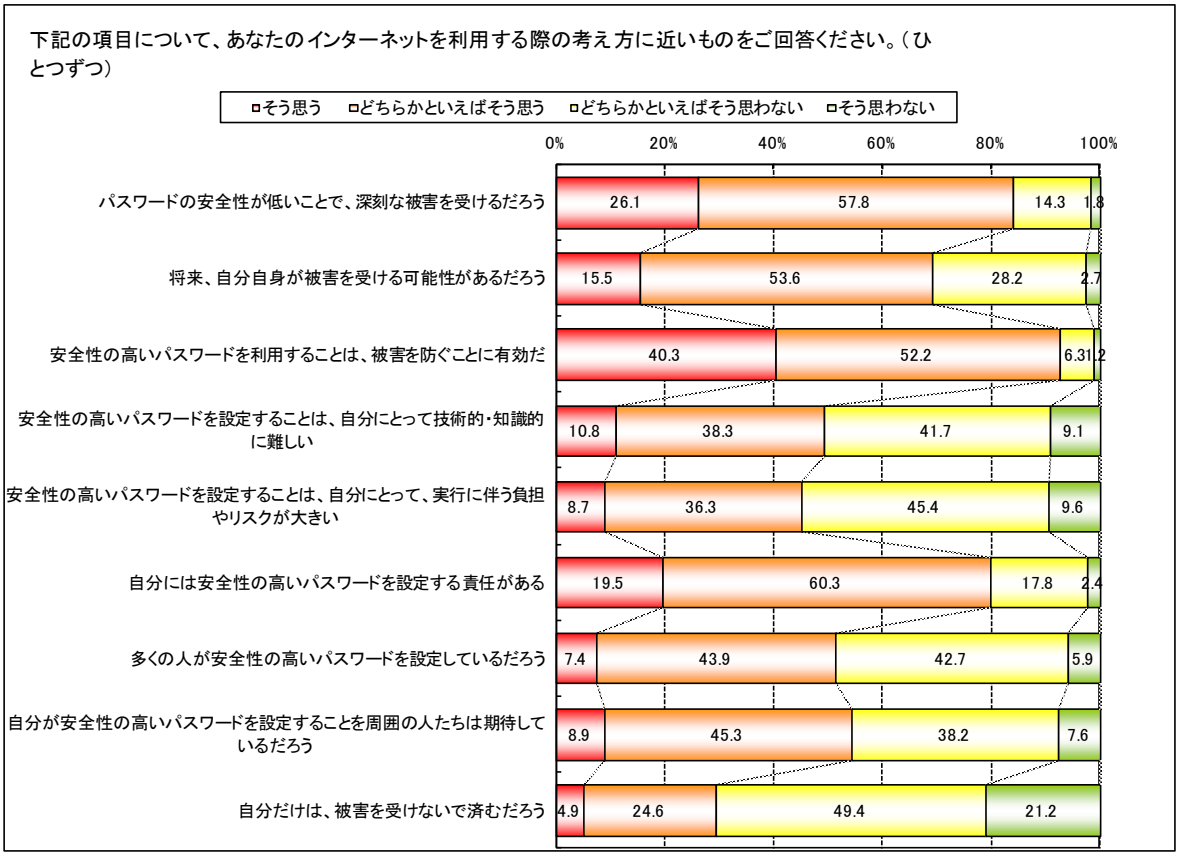


図 76　インターネット利用の際の考え方（その 2）

図 77、図 78 に、パスワード設定についての考え方の結果を示す。

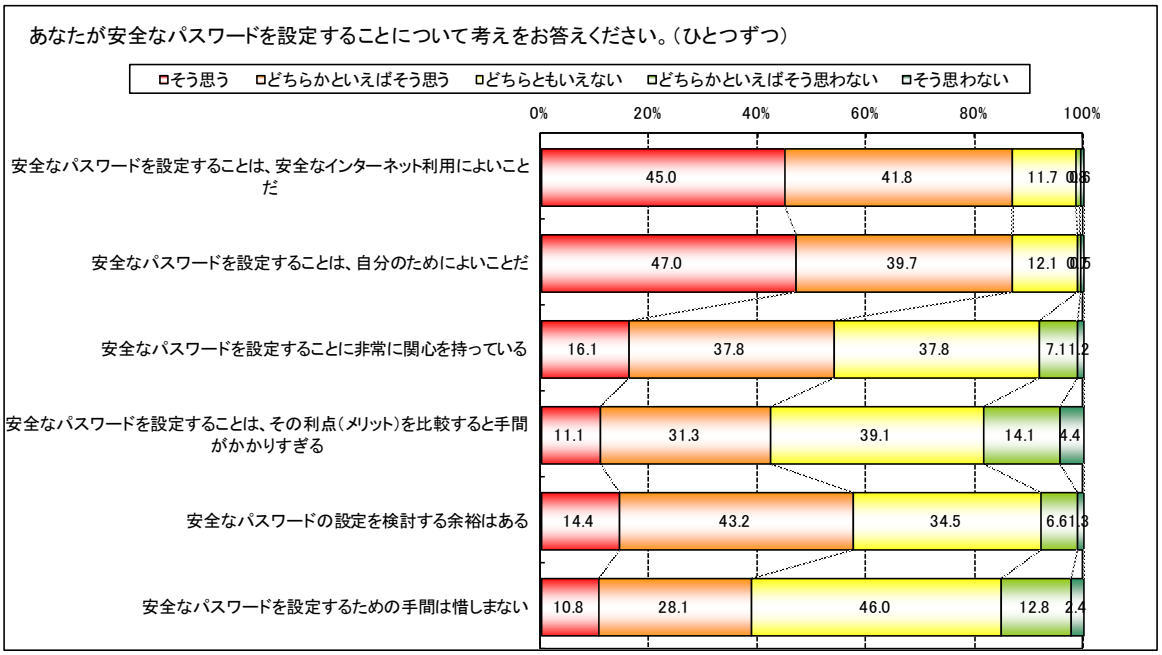


図 77　パスワード設定についての考え方（その 1）

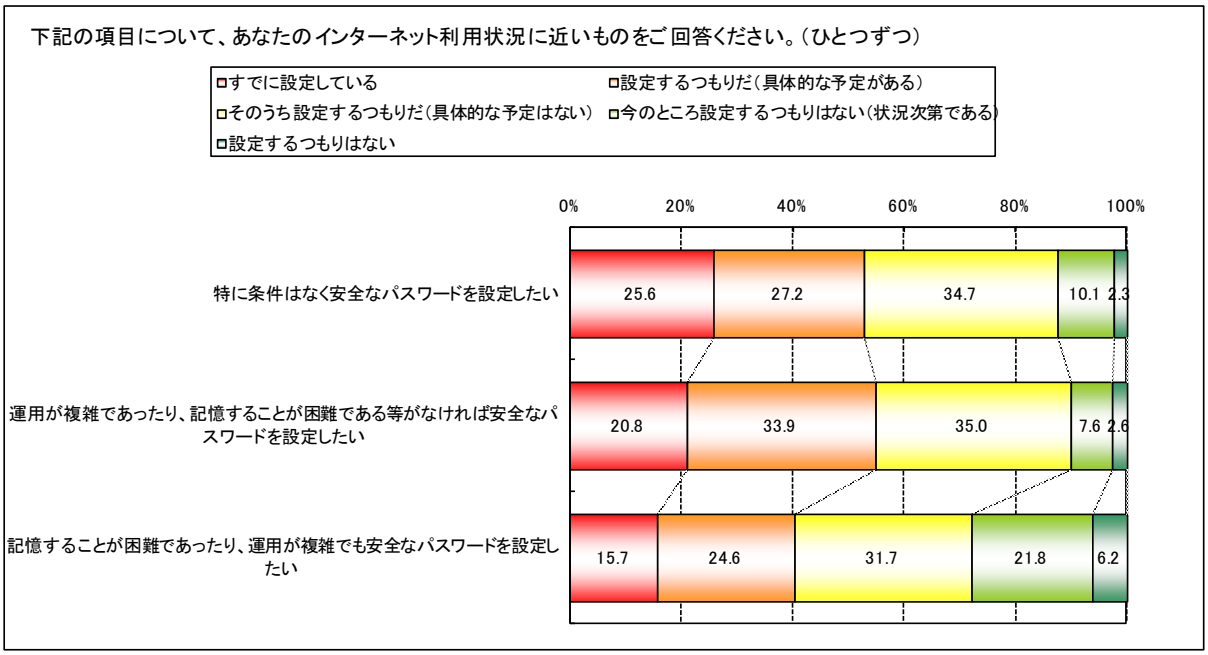


図 78　パスワード設定についての考え方（その 2）