ID ビジネスの現状と課題に関する調査研究

≪報告書≫

平成２２年４月

総務省　情報通信政策研究所

はしがき

インターネットの普及に伴い、そこにおいて提供されるサービスを受けるため、多くの ID が発行されている。しかし、各個人が管理できる ID の数は限られており、そのため、ID を連携したサービスの提供に期待が寄せられている。

ID の連携により、利用者は、入力作業が簡易になるとともに、多くの ID／パスワードを管理する煩雑さを回避できるなど、その利便性は高まると考えられる。一方、事業者としても、顧客を確保し、顧客情報の分析により収益機会を増大させるなどの利点があると考えられる。しかし、事業者としては、連携先も含めたグループ全体の信用を確保し、顧客等の情報管理体制を整備するとともに、プライバシーに関する情報（属性・行動履歴等）の利用に当たり説明責任が生じるなどの課題があるのではないかと考える。今後、インターネットにおけるビジネスを健全に発展させていくためには、ID 連携も含め、利用者が安心して安全にサービスを利用できる環境づくりを関係者が協力して進めていく必要がある。

そこで、インターネットビジネスの基礎となる ID の機能・活用について、その現状を調査するとともに、円滑に ID を連携するための課題を抽出した。

本調査研究の取りまとめに当たっては、株式会社三菱総合研究所の中村秀治主席研究員、安江憲介主席専門研究員、今村圭研究員に御協力いただいた。また、諸外国の動向については、リサーチネット株式会社の安達和夫代表研究員、仙波大輔客員研究員、松山博美客員研究員に御協力いただいた。さらに、インターネットにおいてサービスを提供している事業者の方々にヒアリング調査に御協力いただいた。加えて、国立情報学研究所の岡田仁志准教授に有益なコメントをいただいた。心よりお礼を申し上げる。

なお、本報告書において述べた見解は個人的なものであり、所属する組織のものとは関係ありません。

総務省情報通信政策研究所調査研究部
研究官　大森　審士

－ 目 次 －

序章　本調査研究の背景と目的 ____ *1*

第１章　ID ビジネスの現状 ____ *7*

１　ID の定義、認証ステップ、分類等 ____ **9**

（１）ID の定義 ____ 9

（２）ID の構成要素 ____ 9

（３）ID による認証のステップ ____ 10

（４）ID の分類 ____ 13

２　ID ビジネスの市場動向 ____ **18**

（１）ID ビジネスの定義 ____ 18

（２）ID ビジネスの取組状況 ____ 18

（３）ID ビジネスの発展の方向性 ____ 19

第２章　ID ビジネスの動向 ____ *23*

１　ID ビジネスの展開 ____ **25**

２　ID 連携への期待 ____ **27**

（１）ID の活性化 ____ 27

（２）ID 管理の負担軽減 ____ 28

（３）ID 利用者の増大 ____ 28

（４）ID の価値向上 ____ 29

３　ID ビジネスの類型化 ____ **31**

（１）類型化の考え方 ____ 31

（２）ID ビジネスの類型 ____ 32

（３）各類型の ID 認証プロセスの例 ____ 34

第３章　ID 連携の成立要因 ____ *47*

１　ID 連携の構成 ____ **49**

２　ポータル型の成立要因 ____ **51**

（１）ポータル型のメリット ____ 51

（２）ポータル型のリスクとその回避 ____ 52

３　相互連携型の成立要因 ____ **56**

（１）相互連携型のメリット ____ 56

（２）相互連携型のリスクとその回避 ____ 57

4　エージェント型の成立要因 61
（1）エージェント型のメリット 61
（2）エージェント型のリスクとその回避 62
5　サーチ型の成立要因 65
（1）サーチ型のメリット 65
（2）サーチ型のリスクとその回避 66
5　コミュニティ型の成立要因 69
（1）コミュニティ型のメリット 69
（2）コミュニティ型のリスクとその回避 70
第4章　IDビジネスを取り巻く環境 73
1　我が国政府の取組 75
（1）「通信プラットフォーム研究会」報告書 75
（2）「認証基盤連携フォーラム」における取組 76
（3）「端末プラットフォーム技術に関する研究開発」の実施 76
（4）「公的個人認証サービス普及拡大検討会」における取組 76
（5）「次世代電子行政サービス基盤等検討プロジェクトチーム」の取組 77
（6）「電子政府ガイドライン作成検討会（セキュリティ分科会)」の取組 77
（7）「電子私書箱」に関する取組 77
（8）「社会保障カード（仮称)」に関する取組 78
（9）「納税者番号」等に関する動き 78
2　諸外国における官民連携の動向 80
（1）米国 80
（2）欧州 81
（2）-1　スウェーデン 83
（2）-2　ベルギー 85
（2）-3　オーストリア 89
（2）-4　ドイツ 91
（3）韓国 93
3　ID連携関連技術の標準化の動向 96
（1）OpenID Foundationにおける標準化に係る検討状況（OpenID） 96
（2）OASIS国際標準化コンソーシアムにおける標準化に係る検討状況（SAML） 100
（3）ITU-Tにおける標準化に係る検討状況 104
（4）EUにおける標準化に係る検討状況（eID） 107
終章　IDビジネスの健全な発展に向けて 109

1　政府が取り組むべき方向性 111
2　民間事業者が目指すべき方向性 113
3　利用者が留意すべき事項 114
【補論】我が国における電子認証局の現状 117
（参考文献） 123
参　考 125

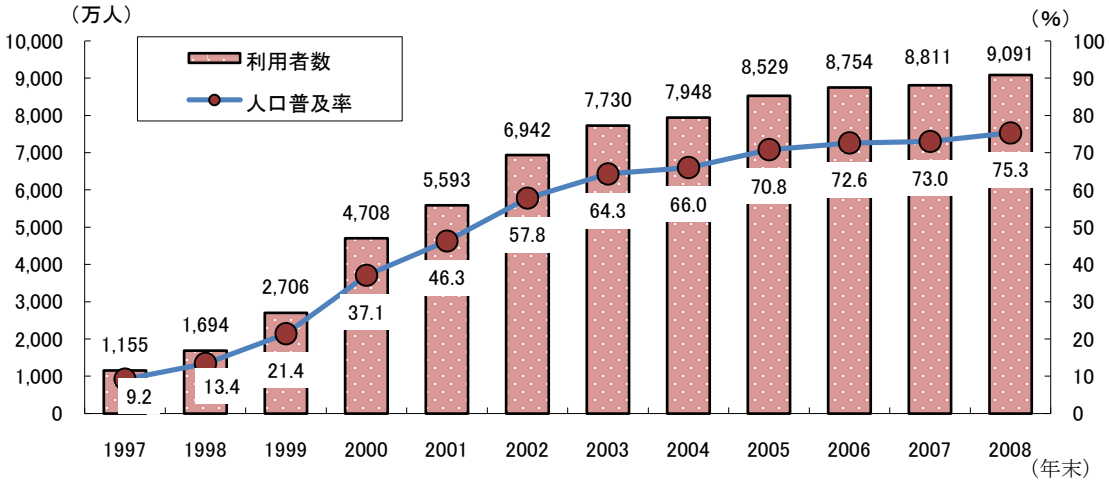
序章　本調査研究の背景と目的

序章　本調査研究の背景と目的

インターネットの普及に伴い、ID を用いた数多くのサービスが提供されるようになってきている。

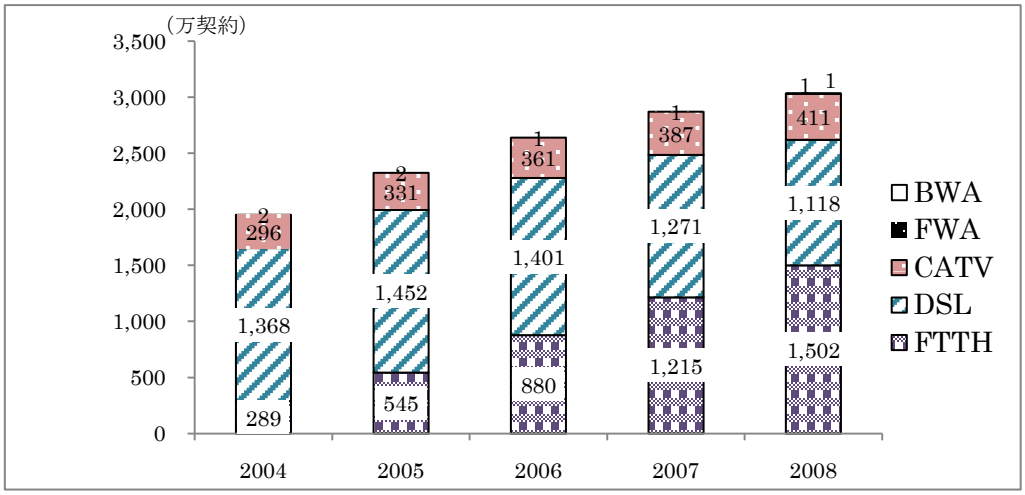
2008 年 12 月末現在、我が国のインターネット利用者数は約 9,091 万人、人口普及率は、75.3%となっている（図 1）。また、2009 年 3 月末現在、我が国におけるブロードバンドサービスの契約数は約 3,033 万、そのうち FTTH アクセスサービスの契約数は約 1,502 万と約半数を占めている（図 2）。このように、我が国では、インターネットの利用が広く普及してきている。

図 1　我が国のインターネット利用者数及び人口普及率の推移



出典：総務省「平成 20 年度通信利用動向調査（世帯編）」報告書 48 頁

図 2　わが国におけるブロードバンドサービス契約数の推移

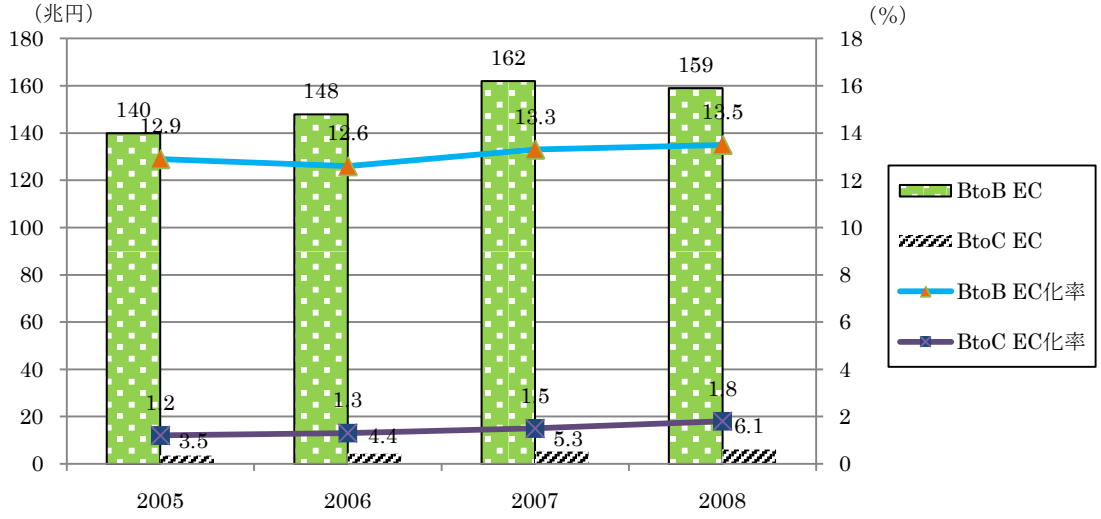


出典：総務省「ブロードバンドサービスの契約数等」より作成

インターネットの Web サイトでは、情報検索サービス、インターネットショッピングや SNS（ソーシャル・ネットワーキング・サービス）、ブログなど、様々な有料・無料のサービスが提供されており、インターネットの普及に伴い、その利用は、企業・個人ともにますます増えている。

例えば、インターネットショッピングなどの電子商取引の市場規模は年々拡大しており、我が国における 2008 年度のBtoC EC（消費者向け電子商取引）の市場規模は 6.1 兆円（EC化率 [1]1.8%）、BtoB EC（企業間電子商取引）の市場規模は 159 兆円（EC化率 13.5%）となっている。（図 3）。また、SNSやブログなど、利用者個人が発信する情報の交換の場を提供するソーシャルメディアの利用者数についてみてみると、2005 年以降、急激な伸びを示している（図 4）。今後もこれらの市場については、拡大していくとみられている。

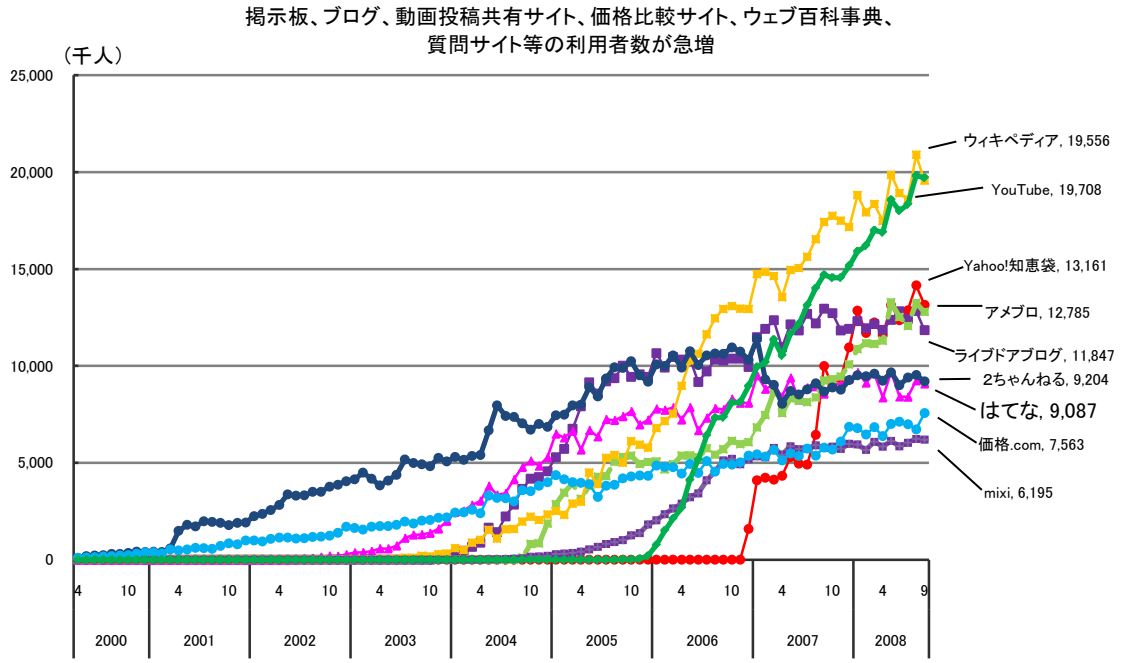
図 3　電子商取引（EC）の市場規模及び EC 化率



出典：経済産業省「平成 17 年度～平成 20 年度　電子商取引に関する市場調査」より作成

[1] EC 化率とは、すべての商取引に占める EC の割合をいう。

図 4　主要なソーシャルメディアの利用者数の推移



出典：総務省『情報通信白書』45 頁

このようなインターネット上のサービスの利用に当たっては、多くのサイトでユーザー登録が必要とされ、それに伴い ID が発行されている。ID は、サービスを提供する事業者がそれぞれのサービスに応じて発行しており、利用者は数多くの ID を保有するようになってきている。

しかし、余りにも多くの ID が付与されると、利用者は、ID 及びパスワードの管理が煩雑になり、同一の ID／パスワードを用いたり、あるいは、余り利用しない Web サイトの ID は登録したまま放置したりするなど、セキュリティ上問題があるような利用の仕方をする可能性がある。あるいは、必要以上に利用することを控えるようになるなど、安心して安全にインターネット上のサービスを利用する便益を享受できなくなる可能性が指摘できる。

一方、事業者からすると、利用者が本当に利用しているか分からない ID に対してもユーザー登録情報の管理コストを費やしている可能性もあり、また、より多くの事業機会がありながら、ID 発行を受けなければならない利用者の必要性がその事業機会の拡大を阻害している可能性も指摘できる。

そもそも、情報通信技術（ICT：Information andCommunication Technology）の利用に関しては、クレジットカード番号やパスワード等の Web サイト等を通じた不正取得、公的機関や企業等が保有する利用者が登録した氏名や住所等の個人情報の流出、他人によるなりすましやホームページの書換え等の不正アクセスといった、様々な問題の発生が懸念されており、ID に関連する個人情報等

の保護や適切な取扱が求められているところである（表 1）。

表 1　ICT の利用への国民の不安感

順位	具体的課題名	不安な人の割合	分野
1 位	クレジットカード番号やパスワード等のウェブサイト等を通じた不正取得	87.4%	プライバシー
2 位	コンピュータ・ウィルス、スパイウェア等への感染	83.8%	情報セキュリティ
3 位	公的機関や企業等が保有する氏名や住所等の個人情報の流出	83.8%	プライバシー
4 位	迷惑メールや迷惑電話	82.4%	違法・有害コンテンツ
5 位	他人によるなりすましやホームページの書きかえ等の不正アクセス	77.0%	情報セキュリティ
6 位	ネット上における噂や流言の拡大、個人攻撃、過剰な反応等	75.6%	ICT 利用におけるマナーや社会秩序
7 位	電子掲示板等への誹謗中傷や権利侵害に関する書き込み	74.5%	違法・有害コンテンツ
8 位	違法な電子商取引の拡大	73.7%	インターネット上の商取引
9 位	ネットショッピング・オークションにおける出品者等とのトラブル	72.9%	インターネット上の商取引
10 位	子どもによる出会い系サイト等の違法・有害サイトへのアクセス	72.4%	違法・有害コンテンツ

出典：総務省「ユビキタスネット社会における安心・安全な ICT 利用に関する調査」（平成 21 年）

このような状況を踏まえ、インターネットビジネスの環境整備及び振興を図るための基礎資料とすることを目的として、インターネットビジネスの基礎となる ID の機能や活用について、その現状を調査するとともに、ID を利用したサービスの発展、そのための利用者の利便性向上と安心・安全な利用のための課題について取りまとめた。

第１章　ID ビジネスの現状

第１章　ID ビジネスの現状

インターネットビジネスの基礎となる ID の機能や活用について述べるに当たり、そもそも、ID とは何か、について述べることにする。すなわち、ID の定義、ID を構成する要素について説明するとともに、認証のステップについて概説する。そして、利用者を特定する強度により ID を分類することにする。

そして、本報告書において ID ビジネスとする対象を明確にし、その取組状況を概説するとともに、その発展の方向性を検討することにする。

１　ID の定義、認証ステップ、分類等

まず、ID の定義とその構成要素、ID を利用したサービスの関係者、ID による認証のステップについて説明する。それを踏まえ、利用者を特定する強度により ID を分類する。

（１）ID の定義

ID とは、一般には、個体や利用者を識別するために用いられる符号のことであり、Identity の略である。

本調査研究では、インターネット上のサービスを対象としているので、「インターネット上のシステムやサービスにおいて、その利用者を識別するもの」としてIDをとらえることとする。別の表現をすると、「ある状況で個人やグループ、組織・企業を特定する情報の総体」と定義することもできる[2]。

（２）ID の構成要素

利用者を特定する情報としてIDをとらえた場合、通常、IDは、3 つの構成要素に分解することができる。すなわち、識別子、クレデンシャル、そして、属性である[3]。それぞれの概要を示すと次のとおりとなる。

表 2　ID の構成要素

[2] 高橋（2009）288 頁。
[3] 同上。

構成要素	機　能	主な例
識別子	ID を識別する	アカウント名、メールアドレス、会員番号、保険証番号、運転免許証番号、社員番号、学生番号、電話番号など
クレデンシャル	ある情報内容の正当性を示す	正当な利用者であることを示すワンタイムパスワード、国籍を示す電子パスポートなど
属性	ID を特徴付ける	個人の場合：氏名、住所、生年月日、所属、役職、信用情報、人間関係、銀行口座番号など 企業の場合：代表者名、所在地、ロゴ、定款、格付け情報、東証コードなど

出典：高橋（2009）288 頁より作成

（3）ID による認証のステップ

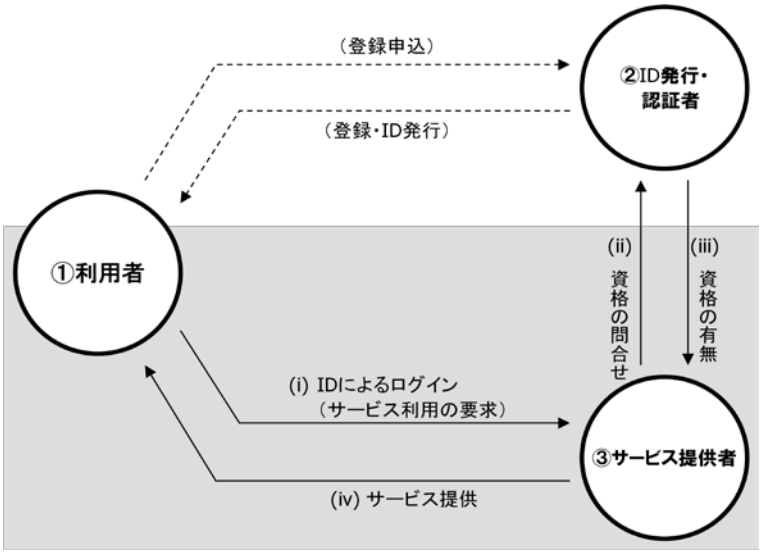
インターネットにおける ID による認証は、基本的には、次の関係者により構成されることになる。

① 利用者（ユーザー）
② ID 発行・認証者（IdP：Identity Provider）
③ サービス提供者（SP：Service Provider）

多くのサービスでは、ID 発行・認証者とサービス提供者が一致している。すなわち、サービス提供者が自ら ID を発行して会員管理等を行うことが多い。

ただし、他の事業者の ID を利用してサービスを提供するような場合には、ID 発行・認証者とサービス提供者とは異なる事業者となる。この場合を図示すると、次のようになる。

図 5　ID の利用に関係する主体



出典：三菱総合研究所

実際の ID の利用において、ID による認証のステップは、次のとおり大きく 3 つに分けることができる。

表 3　ID 認証のステップ

0．オフラインでの証明（書）の入手	・本人確認 ・本人に関する登録情報の確認
①．オンラインでのユーザー登録・ID 発行	・サービス利用に必要な ID 及びパスワードの発行
②．オンラインでの ID 利用	・実際のサービス利用における ID 及びパスワードの利用

出典：三菱総合研究所

本調査研究では、インターネットにおける利用に焦点を当てているので、オンラインでの手続について説明すると、まず、オンラインでユーザー登録を行い、ID の発行を受けることになる。

次に、発行された ID を用いて、利用者としての認証を受け、オンラインでのサービスの利用が可能になる。実際の ID の利用をその構成要素からみると、①識別子により利用者が特定され、②クレデンシャルにより正当な利用者であることが判定され、③必要な属性情報が参照・利用されることになる。

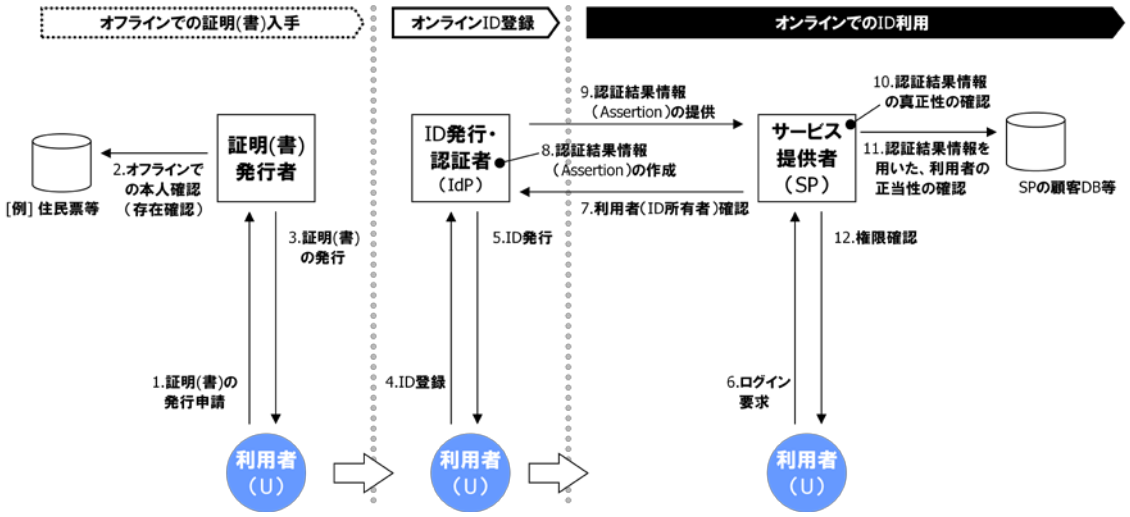
なお、ID を用いて利用されるサービスには、メールアドレス等のみを登

録すれば提供を受けることができるものもあり、提供されるサービスの種類により ID の厳密性は様々である。ID の登録時に本人確認を要する厳密な ID にあっては、オフラインでの証明が必要な場合もある。オフラインでの証明とは、例えば、住民票や運転免許証のような証明書類や住民基本台帳カードなどを利用者に提示させ、ID を利用しようとする者がその本人であることを確認することである。

以上のプロセスは、図 6 及び表 4 に示すように細分化される。

なお、これらの図表では、ID を発行し、認証する者（IdP）と ID により利用者の正当性を確認し、サービスを提供する者（SP）とを区別して記載しているが、サーヒス提供者が ID を発行している場合、両者は一致することになる。

図 6　ID 認証の詳細なプロセス



出典：三菱総合研究所

表 4　ID 認証の詳細なプロセス

	プロセス	概　　要
0．オフラインでの証明（書）入手	1. 証明(書)の発行申請	本人であることの証明（証明書の発行など）を申請
	2. オフラインでの本人確認（存在確認） [Identity Proofing]	住民票などで本人であることを確認（本人が存在することを確認）
	3. 証明(書)の発行 [Certification]	上記を証明するものを発行（例：運転免許証、旅券等）
①．オンラインでのユーザー登録・ID 発行	4. ユーザー登録 [Registration]	証明書をもとに、ネットワーク上の認証サーバ（IdP 側）への利用者 ID コード、パスワード等の認証手段、利用者 ID コードにひも付けられた属性情報の登録
	5. ID 発行	上記 ID コード、パスワードの発行、属性情報の確認
②．オンラインでの ID 利用	6. ログイン要求	利用者がサービス提供者のサーバにアクセスしてログインを要求
	7. 利用者（ID 所有者）確認 [Authentication]	ネットワーク上で、利用者が入力した ID コード及びパスワード等の認証手段に基づき、真正な利用者であることを認証サーバ（IdP 側）が確認
	8. 認証結果情報（Assertion）の作成	認証サーバ（システム）が確認した結果を（所定の形式等の）情報として作成
	9. 認証結果情報（Assertion）の提供	認証サーバ（システム）からサービス提供システム（SP 側）に認証結果情報（及び一部の属性情報）を送付・提供
	10. 認証結果情報（Assertion）の真正性の確認	送付・提供された認証結果情報について、形式、発行者、改ざんの有無などをサービス提供者がチェックし、その内容を信用するか否かを判断
	11. 認証結果情報を用いた、利用者の正当性の確認	認証結果情報より、当該 ID を持つ本人であると確認された利用者がサービス提供者の契約者であることを顧客データベースより確認
	12. 権限確認 [Authorization]	サービス提供者が利用者に対して、要求のあったサービス又は財の提供（引渡し）をしてもよいと判断

出典：三菱総合研究所

（4）ID の分類

インターネットにおけるサービス提供にあっては、そのサービスの内容等に応じて、非常に厳密に本人であることを認証することが必要な場合も、そこま

での認証は必要としない場合もある。ところで、ID は、あらかじめ登録された利用資格に基づいて利用者の資格に応じたサービスを提供するための本人確認手段である。したがって、ID の在り方は、サービスの内容や特徴、登録情報などによって異なることになると考えられる。すなわち、提供されるサービスにおいて利用者資格の判定に求められる厳密さが異なれば、ID による利用者特定強度（本人であるか否かを特定できる強さ）が異なることになる。ID によって利用者を特定する強度は様々なのである。

このような ID による利用者特定強度は、ID を利用したサービスの発展の方向性を検討する上で重要な要素の一つと考えられるので、以下のとおり整理することにする。

ア　利用者特定強度の判定基準

まず、利用者特定強度の判定基準について考察した。その結果、それは、主に 3 つの視点から構成できると思われる。

視点１：利用者の特定は一時的（そのとき限り）でよいのか？恒久的である必要があるのか？

視点２：恒久的な特定を行う場合、本人との同一性（ID を提示している利用者が、その ID の発行を受けた本人であること）が判定できればよいのか？本人との同一性に加えて、その利用者が実在することも判定する必要があるのか？

視点３：実名が求められるのか？利用者が特定できれば仮名[4]でも十分なのか？

第１の視点として、一時的な特定で十分なのか、恒久的な特定が必要なのか、という点が挙げられる。多くの会員組織の場合には、一時的な利用者特定では不十分であり、一般的に、恒久的[5]な特定を想定している場合が多い。

ただし、本調査研究では ID ビジネスについて幅広く検討するため、一時的な特定についても利用者特定強度の区分に含めることにする。

---

[4] 仮名と匿名とは異なる。仮名は、実名とは異なるが、利用者ごとに（同名異人の場合もあるが）一意であるのに対し、匿名は、そもそも利用者ごとの名前が存在しない。仮名の例としては、ハンドルネーム等が挙げられる。

[5] ここで恒久的とは、利用者が退会の手続をとるか、サービス提供者が利用者の利用資格を失効させるまで有効であるという意味である。

第２の視点として、利用者の特定に当たり、本人との同一性が確認できればよいのか、本人との同一性に加えて実際に存在するか否かの確認も必要なのか、という点が挙げられる。後者の場合には、実際に存在することを示すための証明書類の提示や届出が求められることになる。

第３の視点として、実名で利用することが条件になっているのか、利用者が特定でれば仮名での利用も認められるのか、という点が挙げられる。インターネット上で提供されるサービスの場合、メールアドレスやハンドルネームなどの仮名により多くの ID が発行され、利用されているのが実情である。

イ　利用者特定強度の区分

これらの 3 つの視点を組み合わせることで、ID による利用者特定強度の区分を構成することができる。表 5 には、インターネット上でのサービスに限らず、利用者を特定する強度が緩やかなものから厳密なものへと並べてある。

表 5　ID による利用者特定強度の区分

強度区分	定義・説明	例
一時的な特定	その人が、ある条件を満たすことを一時的に証明する。	各種窓口での受付番号カード、レストラン等の入り口での“順番待ち”名簿（ウェイティングリスト）、クーポン券（紙片、携帯電話）など
仮名での存在性	ある仮名の個人を特定する（匿名ではないので個人を特定するが、実名とは限らない。）。	インターネットサービスにおける各種アカウントなど
実名の存在性	ある実名の個人を特定する。	インターネットサービスにおける各種アカウント（実名に限定されるもの）など
実名＋実在証明	ある実名の個人が、実空間（リアル社会）に存在することを証明する。	公的個人認証、運転免許証、パスポート、クレジットカードなど
実名＋実在証明＋特定アカウント	ある実名の個人が実空間（リアル社会）に存在することを、特定のサービス（個人特定・信用強度が極めて高いもの）を通じて高い信用度で証明する。	社会保障番号、納税者番号、クレジットカードなど

出典：三菱総合研究所

以下、それぞれについて、詳しく説明する。

１）「一時的な特定」

「一時的な特定」でよい場合は、特定のいわゆる「ID」を発行する必要性は低く、多くの場合は一時的なカード等が発行されることになる。

ただし、これらも、利用者を特定するという意味では広義の「ID」に含まれると考えることもできる。

この区分については、サービスを利用するに当たり個人を特定することができればよく、事業者のいわゆる会員囲い込み等の必要性、利用者のそれに対する受容性は不要であるため、カード等を発行する形態が合理的と考えられるが、それは、①使い捨て可能な広義の「ID」であること、②気軽に発行・利用可能なこと、などから、今後発展する可能性も考えられる。例えば、携帯電話向けに発行されている電子的なクーポンが、今後、会員サービスとの関係性をどう高めていくか、といった点は興味深い。

２）「仮名での存在性」

「仮名での存在性」でよい場合とは、（サービス提供者からみて）利用者の同一性を判定できれば、実名である必要はないときである。例えば、メールアドレス、SNS 等のアカウント、掲示板のハンドルネーム等は、実名を用いることもできるが、仮名でも問題はない。これらのサービスでは、ある利用者の ID が他の多くの利用者に見えることが多いため、仮名の方が利用者にとっても安心である。また、これらのサービスでは、ユーザー登録・ID 発行の際に、必要となる個人情報も少ない場合が多い。例えば、メールアドレス（＋認証用のパスワード）のみ、という場合も少なくない。

しかし、ID で様々なサービスが利用できるようになると、仮名は、匿名ではないが実名でもない点が問題になる場合も出てきている。例えば、インターネット・オークションや SNS の利用において、ID の不正取得・不正使用等が問題となっている。

３）「実名の存在性」

「実名の存在性」が必要な場合とは、実名でないとサービスを受けられないようなときである。例えば、航空便やホテル等の予約など、実名

での利用が求められるサービスが該当する[6]。

4）「実名＋実在証明」

「実名＋実在証明」が必要な場合とは、利用者の実名による特定だけでなく、実際に存在することの証明も要求されるときである。例えば、金融機関のオンラインサービスなどが該当する。ID 発行の対象となる口座保有者には、口座開設の際に、本人確認すなわち実在証明が条件とされている。

5）「実名＋実在証明＋特定アカウント」

「実名＋実在証明＋特定アカウント」が必要な場合とは、「実名＋存在証明」を、ある「特定のサービス」（社会保障番号、納税者番号、クレジットカード等、個人を特定・信用する強度が極めて高いもの）を通じて証明するときであり、高い信用度で証明する必要がある場合が該当する。

なお、ここでは「特定のサービス」の例として、個人の与信、決済、納税、あるいは、社会保障の受給等にかかわるサービスを挙げたが、運転免許証や旅券も、IC チップの内蔵等により偽変造がますます困難になっていること、また、発給に際しての本人確認が一層厳密になっていること、などの理由により、それらも「特定のサービス」に含まれ得ると考えることができる。

[6] ただし、これらのサービスでは、本人確認、すなわち、実在証明を条件としていることも多い。

2　ID ビジネスの市場動向

本報告書において対象とする ID ビジネスを定義し、その取組の現状、ID ビジネス市場の発展の方向性を検討することにする。

（1）ID ビジネスの定義

インターネットにおいては、ID と関連させて様々なサービスが提供されており（サービスの内容の幅広さ）、また、サービスの利用のために ID の発行が必須である場合と、ユーザー登録を行わなくても一般的なサービスが利用できる場合とがあるが、本調査研究では、インターネット上で何らかの形で ID を用いているサービスは、基本的にすべて検討の対象とすることにする。

そこで、本報告書では、ID ビジネスを次のように定義する。

> **「ID によって認証を行い、それにひも付く利用者の属性や権限を識別して、許可されたサービスを提供するビジネス」**

具体的には、

- 各種の会員向けサービス（ポータルサイト、EC（電子商取引）サイト、各種のサービス提供・予約等のサイト、ニュース・情報提供サイト等）
- ポイントプログラム
- 各種の情報検索サービス
- 掲示板やコミュニティサイト（ブログ、SNS、その他のソーシャルサイト）

などはすべて ID ビジネスの対象に含まれることになる。

（2）ID ビジネスの取組状況

ID ビジネスの取組方針としては、当然のことながら、「自社のサービス・事業をどうすれば発展・成長・拡大・高度化できるか？」ということになる。

その場合、利用者の利便性を高め信頼を獲得することが重要であるが、その実現手段の一つとして、利用者にはユーザー登録をしてもらいIDを発行することになる。

インターネット上の多くのサービスにあっては、サービスを提供する事業者が自らIDを発行し、サービスを提供している。しかし、他の事業者のIDを利用してサービスを提供する事業者もある。すなわち、IDの連携や統合が行われている場合がある。

ID連携・統合については、事業者としては、自社が主として提供するサービスの価値を高めることが重要であり、自社のビジネスモデルに照らして、自社の発行するIDの価値をいかに高めるかといった観点からその方向性を検討している事業者が多いようである。

（3）IDビジネスの発展の方向性

本報告書において、IDビジネスとは、先に述べたとおり「IDによって認証を行い、それにひも付く利用者の属性や権限を識別して、許可されたサービスを提供するビジネス」としており、その用途、利用分野は幅広い。したがって、IDビジネス市場としては、様々な分野を挙げることができる。

IDビジネス市場の傾向を整理すると、以下の4点が考えられる。

＜基本的な市場構造＞

① IDによる利用者特定強度が高まるほど、利用機会そのものは限られていくと考えられる。

② 逆に、利用者特定強度が緩やかなIDの利用機会は、非常に多くあると考えられる。

＜有望と考えられる領域＞

③ 潜在的なIDビジネス市場として、利用者特定強度が緩やかなIDによるビジネスの顕在化が考えられる。

④ もう一つの潜在的な市場として、既に幅広くIDが発行・利用されている「実名の存在性」から「仮名の存在性」までの区分に該当するサービスにおいて、IDの連携・統合等が考えられる。

③は、IDを利用したサービスの事業機会が更に拡大し、現状では顕在化していないサービスの提供や利用が顕在化することを想定している。その場合、IDの機能や価値が現状よりも高まることが重要であると考えられる。例えば、実在する店舗とインターネット上のサービスとの連携などが考えら

れる。インターネット上において、実在する店舗での接客の予約を行うような場合を考えてみると、会員への優待が可能かつ効果的である場合には、インターネットの会員サイトにおいて、IDでログインして実在する店舗の利用を予約し、実際の利用において、実在する店舗にて、キャッシュカード、あるいは、携帯電話の端末等により予約番号を提示して利用する、というようなサービスの流れが考えられる。このようなサービスにより、レストランの予約のリピーター会員向け優待や自動車ディーラー等での試乗予約等において、いわゆるコンバージョン[7]が向上することが期待できる。

ただし、実際にこうしたサービスが可能であるか否かは、実在する店舗の運営上、問題が生じないか、といった面からの検討も必要になってくる。

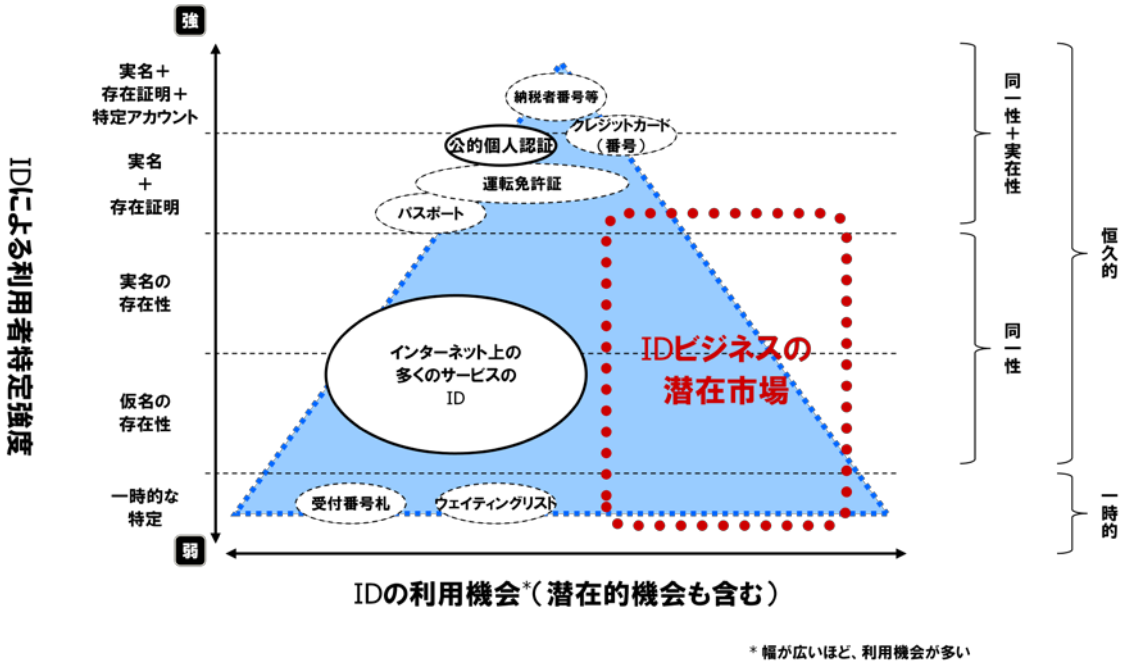
④は、ID の連携や統合によりサービスが相互に連携し、利用者の利便性や ID の価値が高まることを想定している。既に多くの ID が発行されている一方で、余り使われない ID も少なくないのではないかと考えられ、また、複数のサービスを利用する際に、それぞれ異なる ID を入力するのは煩雑であると考えられるところ、ID の連携や統合などにより、利用者の利便性を高めるとともに、ID によるサービスの利用を更に活性化させることが考えられる。

このように、ID ビジネスが、今後、発展していくと考えられる潜在的な分野も多いと考えられる。

そこで、潜在的な市場も含めて、ID ビジネス市場について概観すると、図 7 のようになる。縦軸に ID による利用者特定強度を、横軸に ID の利用機会をとり、ID ビジネス市場を概念的に示している。横軸の幅が広いほど利用機会（潜在的機会も含む。）が多いことを示している。

[7] コンバージョンとは、インターネット上の広告や Web サイトの閲覧者が、それらの主体が望むとおりの行動をとることをいう。

図 7　ID ビジネス市場の概観図



出典：三菱総合研究所

利用者特定強度が緩やかな ID においては、多数のサービスが成立し得ると思われるが、サービスごとに ID を発行するだけでは、利用者によりよく利用されるサービスとそうでないサービスが選別されるだけで、市場全体の成長にはつながらない可能性もある。そこで、各サービスを相互に連携させ、利用者にとっての ID の価値や利便性を高めることが重要になってくるのではないかと思われる。その際、現状では顕在化していないサービスをも含む新たなサービスが提供されたり、既存のサービスの相互連携により新たな利用が行われるようになったりすることも十分に考えられる。

今後、ID ビジネスが潜在市場において発展していくためには、利用者特定強度が緩やかな ID によるビジネスの顕在化、特に ID の連携や統合などに注目する必要があると考えられる。

第２章　ID ビジネスの動向

第２章　ID ビジネスの動向

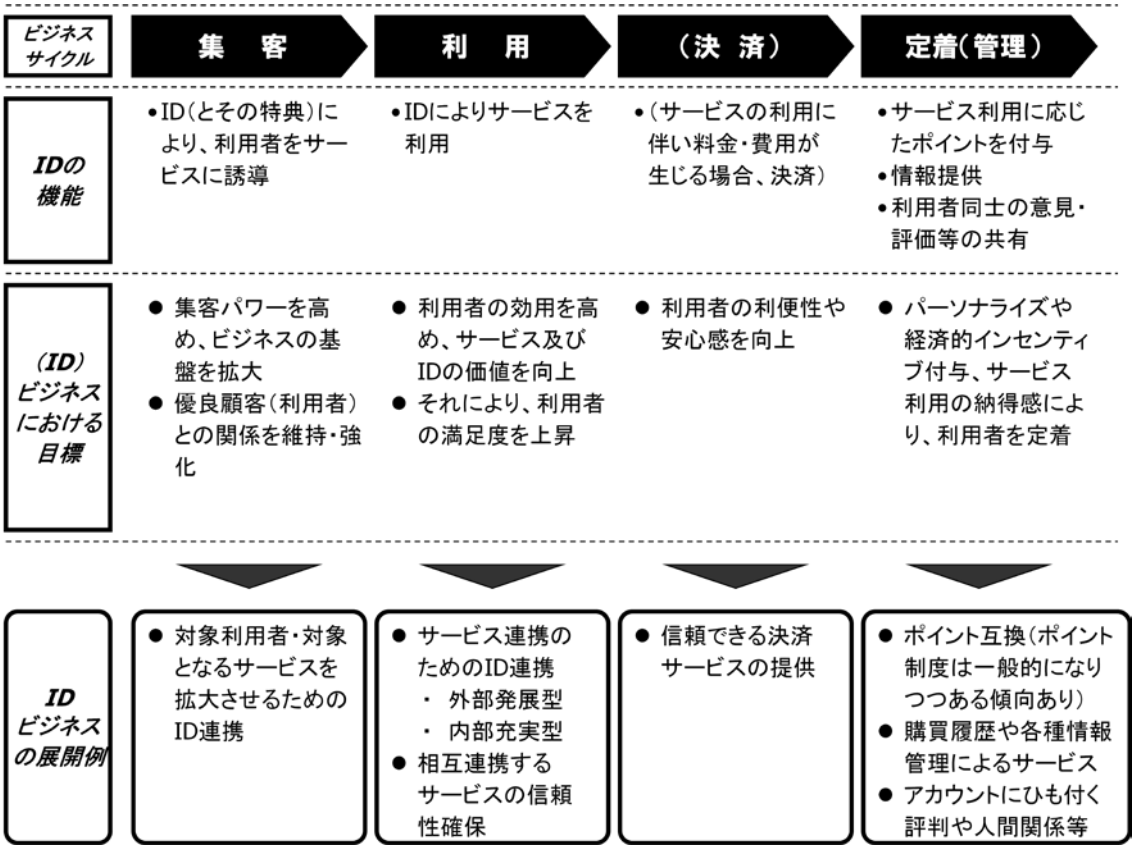
ID 連携については、先進的な取組もみられる一方で、多くの事業者においては、基本的な連携から慎重に取り組んでいる、すなわち、連携先や利用者のニーズ等も踏まえて着実にサービスを高度化していこうとしているのが現状のようである。しかし、今後、ID ビジネスが発展して行くに当たり、特に注目すべきは ID の連携であると考えられる。

そこで、ID ビジネスの展開について概説した上で、ID 連携の可能性を探ることにする。

１　ID ビジネスの展開

ID ビジネスの展開の方向性は、第一義的には各社の事業戦略により決まることになる。ID ビジネスの現状を踏まえ、事業戦略における ID の役割と ID ビジネスの展開例を整理すると、次のようになる。

図 8　事業戦略における ID の役割と ID ビジネスの展開例



出典：三菱総合研究所

ID 連携により自社の ID の価値を高める方法としては、大きく 2 つの方向性がみられる。

① 外部発展型：「外部」との ID 連携

例えば、航空会社の Web サイトに同社の ID でログインし、別の事業者が運営するホテルの予約もできるようにするなど、他の事業者と ID を連携し、相互の役割分担や利用者の動きを合わせることにより事業機会の拡大を図る方向性である。他の事業者が提供するサービスでも自社の ID が使えることにより、自社の ID の価値が高まるとともに、自社が提供するサービスそのものの価値も高まることになる。

② 「内部」での ID 連携

自社やそのグループが提供するサービスにおいて、同一の ID で利用できるようにし、様々な形でサービスを“使い倒してもらう”ことで利用者の利便性を高め、事業機会の拡大を図る方向性である。自社やそのグループにおける様々なサービスの利用を促進することで、自社のサービスの価値が高まることになる。

2　ID 連携への期待

ID の連携へと向かう要因を、大きく以下の 4 つ視点から検討することにする。

- ID の活性化
- ID 管理の負担軽減
- ID 利用者の増大
- ID の価値向上

（1）ID の活性化

本調査研究のために実施した利用者へのアンケート調査の結果[8]、約半数の回答者は 10 サイト以上にユーザー登録しており、それに伴い発行されたIDを保有していることが分かった。回答者のユーザー登録数を平均[9]すると 8.9 サイトとなっている。

一方、ユーザー登録したWebサイトのうち普段よく利用するWebサイトの数は、約 4 割の回答者が 4 サイト以下、約 4 割の回答者が 5～9 サイト、平均[10]すると 6.3 サイトとなっている。

現状では、ユーザー登録するたびに ID が発行されている場合が多く、仮に、利用者がユーザー登録ごとに ID を保有しているとすると、保有している ID の 1/4 は余り利用されていないことになる。

他方、事業者からみると、ID を発行しても利用者に余り利用してもらえないのであれば、自社で ID を発行する意義は薄れる。このような場合、自社で ID を発行する場合と、他の事業者の ID を活用する場合と、どちらがよいか検討する必要が出てくることになる。

こうした、ユーザー登録に伴い発行された ID 数と、実際に頻繁に利用されている ID 数との差を埋める手段の一つとして、ID 連携が考えられる。

---

[8] 利用者に対するアンケート調査の結果は、「参考」にまとめて掲載している。以下同じ。

[9] 15 サイト以上にユーザー登録していると回答した者のユーザー登録数を 15 サイトとして平均した。

[10] 普段よく利用しているサイト数を 15 サイト以上と回答した者の利用サイト数を 15 サイトとして平均した。

（2）ID 管理の負担軽減

発行を受けた ID については、利用者は、それを忘れたり盗まれたりしないように管理する義務を負うことになる。しかし、保有する ID の数が増えると、そのような管理を厳密に実行するのは決して楽なことではない。上記のアンケート調査の結果、こうした管理に問題や不便を感じていないのは、回答者全体の 1 割に過ぎず、残りの 9 割の回答者は、問題や不便を感じていることが分かった。この点を強く認識する利用者は、ID が増えることへの懸念が大きく、新たなユーザー登録を控える可能性が大きいと思われる。

また、事業者からみると、ユーザー登録に際して収集した利用者の個人情報等を管理する費用や煩雑さが、それによって得られる、あるいは、期待される効果よりも上回る場合、負担となることもある。すなわち、利用者の利用頻度が低ければ、利用者の情報管理にかける労力に見合わない場合が考えられるのである。

このように考えると、ID 管理の負担を増やすことなく新たなサービスを利用できるような仕組みがあると、利用者、事業者、双方にとってメリットになると考えられる。そのような仕組みとして ID 連携が考えられる。

（3）ID 利用者の増大

利用者としては、ID 保有数が自ら管理できる ID 数を越え、ID／パスワードの管理に問題や不便さを感じるようになると、必要以上に ID を増やしたくないためにユーザー登録が必要な Web サイトの利用を控えるようになる可能性も指摘できる。すなわち、事業者としては、自社の ID を発行することにより事業機会を失っているかもしれないのである。

また、利用者としては、余り利用しないが今回だけは利用したい、と思うようなサービスにあっては、新たにユーザー登録することなく、既に保有している ID で利用することができ、ID 等の管理の負担や個人情報漏洩等の不安が軽減されるのであれば、利用してみるかもしれない。

このような場合、事業者としては、ID を連携させることにより、自社のサービスの利用機会を提供し、そのよさを利用者に理解してもらうことも一考に値すると考えられる。

また、例えば、知名度の高い事業者であれば、実際にどれだけ利用されるかはともかくとしても、それなりの規模の利用者を集めることは、それほど難しくないと思われるが、知名度の低い事業者の場合には、利用者を増やすのは容易なことではない。このような場合、知名度の低い事業者としては、

知名度の高い事業者が発行する ID と連携することにより、利用者を増やすことも一つの方策となる。

（4）ID の価値向上

本調査研究のために実施した利用者へのアンケート調査の結果によると、ユーザー登録が必須でない Web サイトであっても、会員になれば無料でそれ以上のサービスが受けられる場合、回答者の約半数は「登録する」としている。その理由としては、会員割引やポイント等のメリット、今後よく利用することになりそう、といった回答が多く、利用者としては、それに見合う価値があればユーザー登録する傾向が伺われる。

しかし、ユーザー登録した利用者が、そのままそのサービスを利用し続けるとは限らない。自分にとって、ユーザー登録することに余り価値がない、あるいは、発行された ID の利便性が低い、と思うようになると、利用者は、ユーザー登録を解消（退会等）するか、ユーザー登録は維持してもサービスは利用しなくなるであろう。

こうした事態をできるだけ少なくするためには、利用者（ユーザー登録者）にとって、ユーザー登録する価値を高めること、すなわち、ユーザー登録に伴い発行された ID の価値を高めることが必要であり、そのため、他のサービス事業者との提携やサービスの相互乗り入れ等も行われている。利用者にとって価値が高いと認識された ID は、継続的かつ高頻度で利用されると考えられる。

連携先は、自社が提供するサービスの特徴や当該事業者の事業全体における位置付けなどによっても異なるが、ポイント等を付与し、連携先でも利用できるようにして利用者に関心を持ってもらうことや、密接に関連するサービス間（例：交通機関と宿泊サービス）で連携して利用者に便利さを感じてもらうことなどが代表的な事例として考えられる。

ちなみに、サービス間で連携する場合、それぞれのサービスをシームレスに利用できることが重要であり、そのためには、サービスを連携するだけではなく、それを利用するために必要な ID をも連携させることが重要であると考えられる。

以上、ID 連携へと向かう要因をまとめると、次のようになる。

表 6　ID 連携へと向かう要因

	利用者	事業者
(1) ID の利用度	・　保有する ID の 1/4 はあまり使われていない。	・　余り利用されない ID について、個人情報も含めて管理する費用を削減したい。
(2) ID の管理	・　約 9 割の利用者は、ID／パスワードの管理に問題や不便さを感じている。	・　ID 発行により得られるものが少なければ、情報等の管理の費用や煩雑さが負担になる場合もある。
(3) ID による集客効果	・　新たにユーザー登録することなく、既に保有している ID で利用できれば ID 等の管理の負担や不安感が小さくなる。	・　自社のサービスやサイトの集客力が低い場合、集客力の高い、利用者数の多い他社の ID を利用したい。
(4) ID の価値の向上	・　同様のサービスを利便性の高い ID で利用できれば、利便性の低い ID で提供されるサービスは利用しなくなる。	・　利用者に自社の ID を使い続けてもらうためには、ID の価値を高めていくこと（拡大と深化）が重要である。

出典：三菱総合研究所

3　ID ビジネスの類型化

ID ビジネスは、単独のサービスとして提供されているものも多数あるが、様々な形態や程度の違いがあるにせよ、ID 連携を志向していると考えられるサービスも少なくない。そこで、ID 連携という観点から ID ビジネスを類型化することにした。

なお、現状で既に存在する形態に加え、将来的に考えられるものも含めて検討した。

（1）類型化の考え方

ID ビジネスを ID 連携という観点から類型化するに当たっては、「ID 連携のパターンはなぜ多様化するのか？」について考えることが重要である。これについては、次のように考えた。

インターネット上で多くのサービスが提供され、多くの（顕在＋潜在）利用者が集う状況において、利用者の要望と事業者（ID 発行・認証者（IdP）及びサービス提供者（SP））の期待とがうまく調整されるように、ID 連携のパターンは多様化していくと考えられる。

ここでの「利用者の要望」とは、インターネット上のサービスを利用する上での要望のことであり、「事業者の期待」とは、インターネット上でサービスを提供する上での期待を意味する。

インターネットにおけるサービスを利用するに当たり、利用者の要望としては、次の 2 つが挙げられる。

・選択肢の拡大　　：「多くの中から、よいサービスを利用したい。」
・選択肢の最適化・集約：「よいサービスだけを利用すれば十分である。」

また、事業者の期待としては、次の 3 つが挙げられる。

・事業機会の最大化　　：「多くの利用者に利用してもらいたい。」
・事業機会損失の最小化：「些細な手間等による利用者の“脱落”をなくしたい。」
・優良顧客の獲得　　：「よい顧客を獲得したい。」

以上のような利用者の要望と ID 発行・認証者及びサービス提供者の期待が互いにうまく調整できるように ID 連携のパターンが形成されると考えられる。

（2）ID ビジネスの類型

先に述べた考え方により ID 連携の観点から ID ビジネスの各種事業形態を考え、ID ビジネスを大きく 6 つに類型化した。すなわち、①「連携なし」、②「ポータル型」、③「相互連携型」、④「エージェント型」、⑤「サーチ型」、⑥「コミュニティ型」である。「相互連携型」は、連携の在り方により「事前連携型」と「オープン（アドホック）連携型」とに細分化されると考えた。

各類型について、その特徴を示すと表 7 のとおりであり、類型化の考え方との関係は表 8 のとおりである。

表 7　ID ビジネスの類型

ID ビジネスの類型		特　　徴
①（ID 連携なし）		利用者がサービスごとにそれぞれの ID を管理する。
②ポータル型		ある（親）ID が他でも ID として利用できる。
③相互連携型		連携している事業者・サービスであれば、どの ID でも他の事業者・サービスで利用できる。
	③-1 事前連携型	事業者間の連携関係があらかじめ定められている。
	③-2 オープン（アドホック）連携型	事業者間の連携範囲は定まっているが、直接の連携関係はアドホックに決まる。
④エージェント型		利用者があらかじめ指定したサービスの ID をエージェントが一括して管理する。
⑤サーチ型		利用者の要望やステータスに応じて、適切なサービスを提示し、そのサービスを利用するための臨時的な ID を発行する（検索サイトの ID でサービス提供サイトにログインできる。）。
⑥コミュニティ型		コミュニティの“友人”など利用者間の信頼関係に基づいてサービスの紹介が行われ、コミュニティサイトの ID やその友人の紹介により発行される臨時的な ID によって連携しているサービス提供サイトへのログインが一時的に可能になる。

出典：三菱総合研究所

表 8　ID ビジネスの類型と類型化の考え方との関係

ID ビジネスの類型	利用者の要望		事業者の期待		
	選択肢の拡大	選択肢の最適化・集約	事業機会の最大化	事業機会損失の最小化	優良顧客の獲得
①（ID 連携なし）	―	―	―	―	―
②ポータル型	◎		◎		
③相互連携型					
③-1 事前連携型		◎		○	◎
③-2 オープン（アドホック）連携型	◎		◎		
④エージェント型		◎		○	◎
⑤サーチ型	◎	○	◎		○
⑥コミュニティ型		◎			◎

［注］◎：特に関係が深いと考えられる事項、○：関係していると考えられる事項

※　「◎」、「○」の付いていない事項についても、まったく関係がないわけではない。これらの記号は、ID ビジネスの類型と各事項との関係の相対的な深さを示している。

出典：三菱総合研究所

利用者にとっての選択肢拡大、事業者にとっての事業機会最大化、すなわち、利用者の選択肢拡大による集客規模拡大を考えると、ポータルサイトの ID が他のサービス提供者の Web サイトでも利用できるポータル型になると考えられる。

これに対し、相互連携型のうち事前連携型の場合には、互いに関連性が深い、又は、利用者の利便性向上に関して相乗効果のあるサービス間での連携が多いと考えられ、利用者にとっての選択肢の最適化・集約、事業者にとっての優良顧客獲得･事業機会損失最小化（例：航空券の購入者にホテル予約サービスを提供する場合など）を主目的としていると考えられる。

他方、相互連携型のうちオープン（アドホック）連携型の場合には、そうした事前の関係性はないので、むしろポータル型に近い、選択肢拡大（一つの ID が様々なところで、利用者の選択に基づいて利用可能）による集客力向上を主目的としていると考えられる。

利用者にとって重要な特定のサービス（例：主に決済サービス）を利便性と信頼性の高い形で提供することで、その利用者に対して独占的な存在にな

ることを考えると、利用者があらかじめ指定したサービスの ID をエージェントが一括して管理するエージェント型も考えられる。この場合、利用者にとっては選択肢の集約であり事業者にとっては優良顧客獲得が主目的と考えられる。

将来的なサービス提供形態を考えると、検索サイトの ID でサービス提供者の Web サイトにログインできるサーチ型も考えられる。これは、利用者にとっては選択肢拡大という側面が強いと思われる。事業者にとっては事業機会拡大に加えて、情報検索の対象やその方法（例：検索結果の信頼性や有用性を高めるなど）によっては、優良顧客の獲得も目的とすることができるであろう。

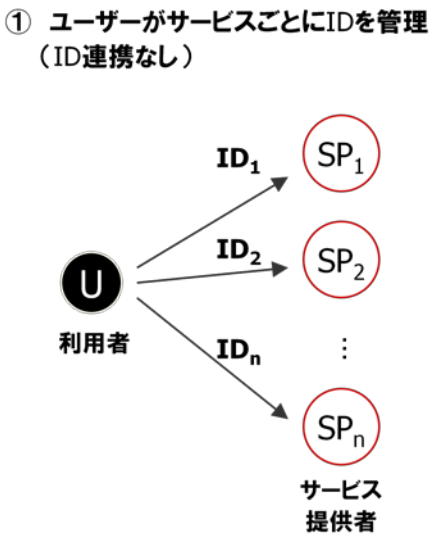
利用者間の人間関係（信頼関係や親密さなど）に基づいて臨時的な ID が発行され、他のサービス提供者が提供するサービスを利用できるようになるコミュニティ型も考えられるが、これは、選択肢の最適化、優良顧客獲得が主目的になると考えられる。

なお、ポータル型、相互連携型、エージェント型及びコミュニティ型については、具体的な ID 連携といえるサービスが現状においてもみられるが、これらの多くは、ID 発行・認証者が提供するサービスとの関連でサービス提供者との連携が行われている。これに対し、特にサーチ型の場合にこの傾向が強いと思われるが、ID を持たなくても利用できるサービスを起点に考えた場合には、ID 連携への期待はなかなか顕在化しないのかもしれない。しかし、そのようなサービスにあっても、ID が必要なサービスと関連している場合、利用者の利便性向上や事業機会の拡大を考えると、ID 連携という方向性も一考に値するのではなかろうか。例えば、本調査研究に当たり実施した利用者へのアンケート調査の結果によると、ID 連携への期待は大きく、サーチ型にあっても、「利用してみたいと思う」回答者が「利用してみたいと思わない」回答者を上回っている。

（3）各類型の ID 認証プロセスの例

ID ビジネスの各類型についてイメージしやすくするために、各類型の ID 認証のプロセスを例示する。

① ID 連携なし

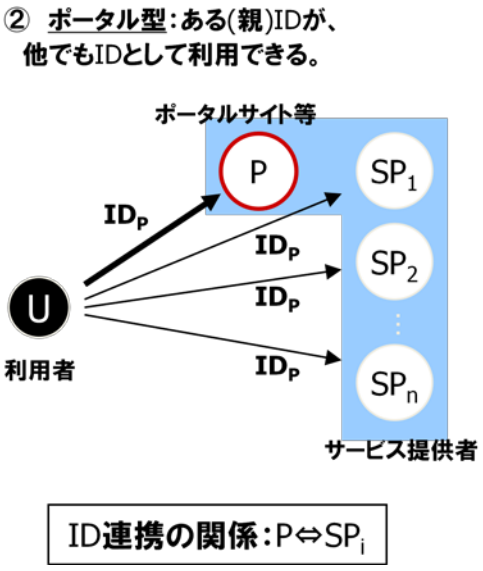


出典：三菱総合研究所

ID 認証プロセスの例

1．利用者が各 Web サイトでユーザー登録をし、ID の発行を受ける。
2．利用者が各 Web サイト（例：SP_1）にアクセスする。
3．各 Web サイトの運営者（例：SP_1）は、独自に保有している ID 情報（例：ID＋PW）を参照して認証する。
4．利用者は、各 Web サイト（例：SP_1）にログインする。
5．各 Web サイト（例：SP_1）での利用者の行動情報は、各 Web サイトの運営者（例：SP_1）のプライバシーポリシー等に基づき、各 Web サイト（例：SP_1）にて取得・蓄積される。
6．ある Web サイトの運営者（例：SP_1）と他の Web サイトの運営者（例：SP_2～SP_n）との間で、利用者の ID 情報や行動情報は、（あらかじめ特に定めている場合を除き、）やりとりされない。

② ポータル型



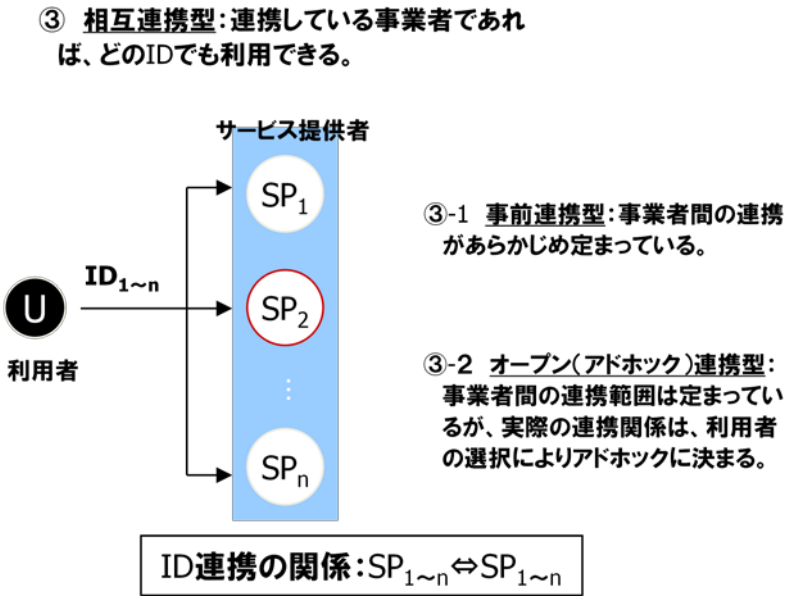
出典：三菱総合研究所

ID 認証プロセスの例

1．利用者がポータルサイト（P）でユーザー登録し、ID の発行を受ける。
2．利用者が各 Web サイト（例：SP_1）にアクセスする。
3．各 Web サイトの運営者（例：SP_1）は、利用者に ID 情報（例：ID＋PW）を要求する。
4．利用者は、ID 情報を入力する。
5．各 Web サイトの運営者（例：SP_1）は、その ID 情報の発行元がポータルサイトの運営者（P）であることを判別して、ポータルサイトの運営者（P）に認証を要求する。
6．ポータルサイトの運営者（P）は、自らが保有している ID 情報を参照して認証し、結果を各 Web サイトの運営者（例：SP_1）に通知する。
7．各 Web サイトの運営者（例：SP_1）は、認証結果に基づき利用者にログインを認める。
8．利用者は、各 Web サイト（例：SP_1）にログインする。
9．各 Web サイト（例：SP_1）での利用者の行動情報は、各 Web サイトの運営者（例：SP_1）のプライバシーポリシー等に基づき、各 Web サイト（例：SP_1）にて取得・蓄積される。
10．利用者の ID 情報は、必要に応じて（主に商品購入やキャンペーン応募などの場合、）ポータルサイトの運営者（P）から各 Web サイトの運営者（例：SP_1）に提供され、各 Web サイトの運営者（例：SP1）は、これを利用し、また、蓄積する場合もある。

11. アクセスした Web サイトの運営者（例：SP_1）と他の Web サイトの運営者（例：SP_2～SP_n）との間で、利用者の ID 情報や行動情報は、（あらかじめ特に定めている場合を除き、）やりとりされない。
12. 利用者の各 Web サイト（例：SP_1）での行動情報は、ポータルサイトの運営者（P）に提供される場合と提供されない場合との両方が想定される。

③　相互連携型



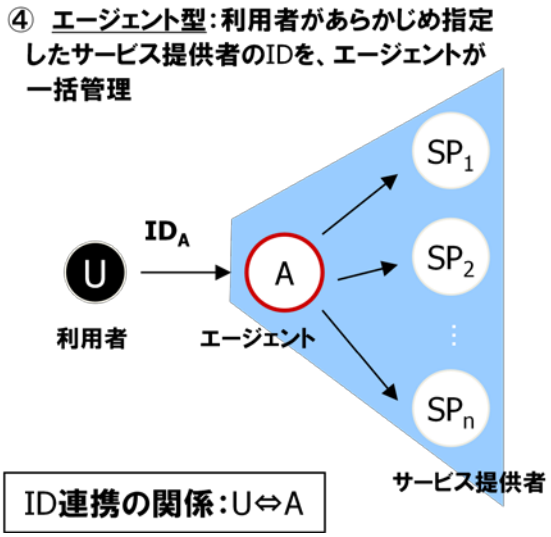
出典：三菱総合研究所

ID 認証プロセスの例

1．利用者がある Web サイト（例：SP_2）でユーザー登録し、ID の発行を受ける。
2．利用者が各 Web サイト（例：SP_1）にアクセスする。
3．各 Web サイトの運営者（例：SP_1）は、利用者に ID 情報（例：ID＋PW）を要求する。
4．利用者は、ID 情報を入力する。
5．各 Web サイトの運営者（例：SP_1）は、その ID 情報の発行元（例：SP_2）を判別して、認証を要求する。
6．ID 発行サイトの運営者（例：SP_2）は、自らが保有している ID 情報を参照して認証し、結果を各 Web サイトの運営者（例：SP_1）に通知する。
7．各 Web サイトの運営者（例：SP_1）は、認証結果に基づき利用者にログインを認める。
8．利用者は、各 Web サイト（例：SP_1）にログインする。
9．各 Web サイト（例：SP_1）での利用者の行動情報は、各 Web サイトの運営者（例：SP_1）のプライバシーポリシー等に基づき、各 Web サイト（例：SP_1）にて取得・蓄積される。
10．利用者の ID 情報は、必要に応じて（主に商品購入やキャンペーン応募などの場合、）ID 発行サイトの運営者（例：SP_2）から各 Web サイトの運営者（例：SP_1）に提供され、各 Web サイトの運営者（例：SP_1）は、これを利用し、また蓄積する。

11. アクセスした Web サイトの運営者（例：SP_1）と ID 発行サイトの運営者（例：SP_2）以外の Web サイトの運営者（例：SP_3～SP_n）との間で、利用者の ID 情報や行動情報は、（あらかじめ特に定めている場合を除き、）やりとりされない。
12. 利用者の各 Web サイト（例：SP_1）での行動情報は、ID 発行サイトの運営者（例：SP_2）に提供される場合と提供されない場合との両方が想定される。

④　エージェント型



出典：三菱総合研究所

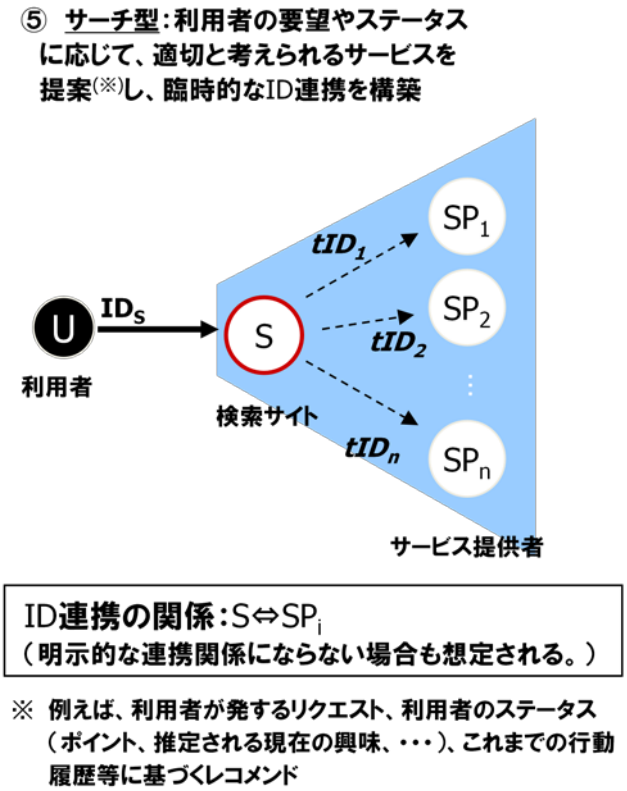
ID 認証プロセスの例

1．利用者がエージェントサイト（A）でユーザー登録し、ID の発行を受ける。
2．利用者が各 Web サイト（例：SP_1）にアクセスする。
3．各 Web サイトの運営者（例：SP_1）は、利用者に ID 情報（例：ID＋PW）を要求する。
4．利用者は、（エージェント（A）が発行した）ID 情報を入力する。
5．各 Web サイトの運営者（例：SP_1）は、その ID 情報の発行元がエージェント（A）であることを判別して、エージェント（A）に認証を要求する。
6．エージェント（A）は、自らが保有している ID 情報を参照して認証し、結果を各 Web サイトの運営者（例：SP_1）に通知する。
7．各 Web サイトの運営者（例：SP_1）は、認証結果に基づき利用者にログインを認める。
8．利用者は、各 Web サイト（例：SP_1）にログインする。
9．各 Web サイト（例：SP_1）での利用者の行動情報は、各 Web サイトの運営者（例：SP_1）のプライバシーポリシー等に基づき、各 Web サイト（例：SP_1）にて取得・蓄積される
10．利用者の ID 情報は、必要に応じて（主に商品購入やキャンペーン応募などの場合、）エージェント（A）から各 Web サイトの運営者（例：SP_1）に提供され、各 Web サイトの運営者（例：SP_1）は、これを利用し、また蓄積する。
11．アクセスした Web サイトの運営者（例：SP_1）と他のサイトの運営者（例：SP_2～SP_n）との間で、利用者の ID 情報や行動情報は、（あらかじめ特に定め

ている場合や利用者が指示した場合を除き、）やりとりされない。

12. 利用者の各 Web サイト（例：SP_1）での行動情報は、エージェント（A）に提供される場合とされない場合との両方が想定される。

⑤　サーチ型



出典：三菱総合研究所

ID 認証プロセスの例

1．利用者が検索サイト（S）でユーザー登録し、ID の発行を受ける。
2．利用者が検索サイトにログインした状態の下、その検索内容や各 ID の状況（例：ポイント等）、蓄積された過去の行動履歴等に応じて、検索サイトの運営者（S）が適切なサービスを提案（表示）する。
3．利用者はそれを見て、興味を持つ Web サイト（例：SP_1）にアクセスする。
4．各 Web サイトの運営者（例：SP_1）は、利用者に ID 情報（例：ID＋PW）を要求する。
5．利用者は、ID 情報を入力する。
6．各 Web サイトの運営者（例：SP_1）は、その ID 情報の発行元が検索サイトの運営者（S）であることを判別して、検索サイトの運営者（S）に認証を要求する。
7．検索サイトの運営者（S）は、自サイトへのログイン状況を認証結果として各 Web サイトの運営者（例：SP_1）に通知する。
8．各 Web サイトの運営者（例：SP_1）は、認証結果に基づき、（臨時 ID（例：tID_1）を発行し、）利用者にログインを認める。

９．利用者は、各 Web サイト（例：SP_1）にログインする。

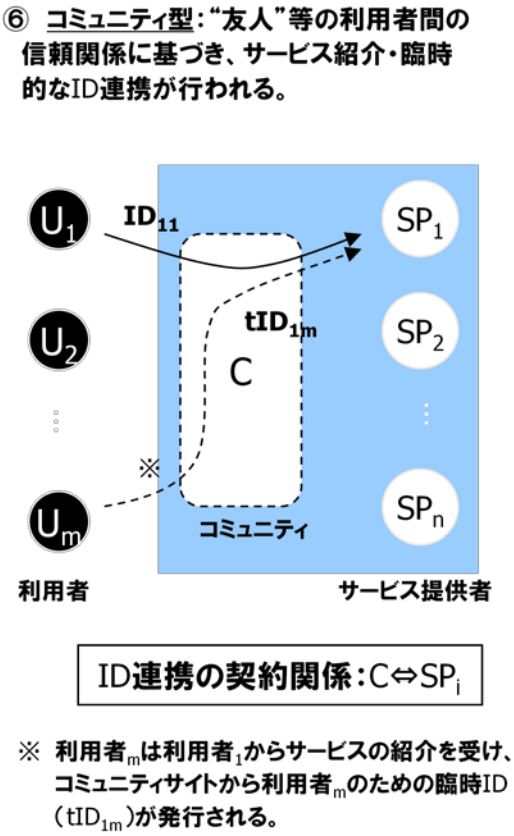
10. 各 Web サイト（例：SP_1）での利用者の行動情報は、各 Web サイトの運営者（例：SP_1）のプライバシーポリシー等に基づき、各 Web サイト（例：SP_1）にて取得・蓄積される。

11. 利用者の ID 情報は、必要に応じて（主に商品購入やキャンペーン応募などの場合、）検索サイトの運営者（S）から各 Web サイトの運営者（例：SP_1）に提供され、各 Web サイトの運営者（例：SP_1）は、これを利用し、また蓄積する。

12. アクセスした Web サイトの運営者（例：SP_1）と他の Web サイトの運営者（例：SP_2～SP_n）との間で、利用者の ID 情報や行動情報は、（あらかじめ特に定めている場合を除き、）やりとりされない。

13. 利用者の各 Web サイト（例：SP_1）での行動情報は、検索サイト（S）の運営者に提供される場合と提供されない場合との両方が想定される。

⑥　コミュニティ型



出典：三菱総合研究所

ID 認証プロセスの例

1．利用者（例：U_1）がコミュニティサイト（C）でユーザー登録し、ID の発行を受ける。

2．利用者（例：U_1）は、コミュニティサイト（C）にログインした状態の下、利用者（例：U_1）が公開している興味や利用者（例：U_1）の持っている各 ID の状況（例：ポイント等）に応じて、コミュニティサイト（C）にログインしている他の利用者（例：U_m）に仲介できる、適切なサービスを提案（表示）する（利用者（例：U_1）は自分がよいと思う／仲介できるサービスを何らかの形で公開）。

3．他の利用者（例：U_m）はそれを見て、興味を抱く Web サイト（例：SP_1）にアクセスする。

4．各 Web サイトの運営者（例：SP_1）は、仲介された利用者（例：U_m）に ID 情報（例：ID＋PW）を要求する。

5．仲介された利用者（例：U_m）は、コミュニティサイト（C）の ID 情報を入力する。

6．各 Web サイトの運営者（例：SP_1）は、その ID 情報の発行元がコミュニティサイトの運営者（C）であること、仲介者がコミュニティサイト（C）の利用者（例：U_1）であることを判別して、コミュニティサイトの運営者（C）に認証を要求する。

7．コミュニティサイトの運営者（C）は、自サイトへのログイン状況を認証結果として各 Web サイトの運営者（例：SP_1）に通知する。

8．各 Web サイトの運営者（例：SP_1）は認証結果に基づき、（臨時 ID（tID_{1m}）を発行し、）仲介された利用者（例：U_m）にログインを認める。

9．仲介された利用者（例：U_m）は、各 Web サイト（例：SP_1）にログインする。

10. 仲介した利用者（例：U_1）には、仲介ポイントが記録される。

11. 仲介された利用者（例：U_m）の各 Web サイト（例：SP_1）での行動情報は、各 Web サイトの運営者（例：SP_1）のプライバシーポリシーに基づき、各 Web サイト（例：SP1）にて取得・蓄積される。

12. 仲介された利用者（例：U_m）の ID 情報は、必要に応じて（主に商品購入やキャンペーン応募などの場合、）コミュニティサイトの運営者（C）から各 Web サイトの運営者（例：SP_1）に提供され、各 Web サイトの運営者（例：SP_1）は、これを利用し、また蓄積する。

13. アクセスした Web サイトの運営者（例：SP_1）と他の Web サイトの運営者（例：SP_2～SP_n）との間で、利用者の ID 情報や行動情報は、（あらかじめ特に定めている場合を除き、）やりとりされない。

14. 仲介された利用者（例：U_m）の各 Web サイト（例：SP_1）での行動情報は、コミュニティサイトの運営者（C）に提供される場合と提供されない場合との両方が想定される。

第３章　ID 連携の成立要因

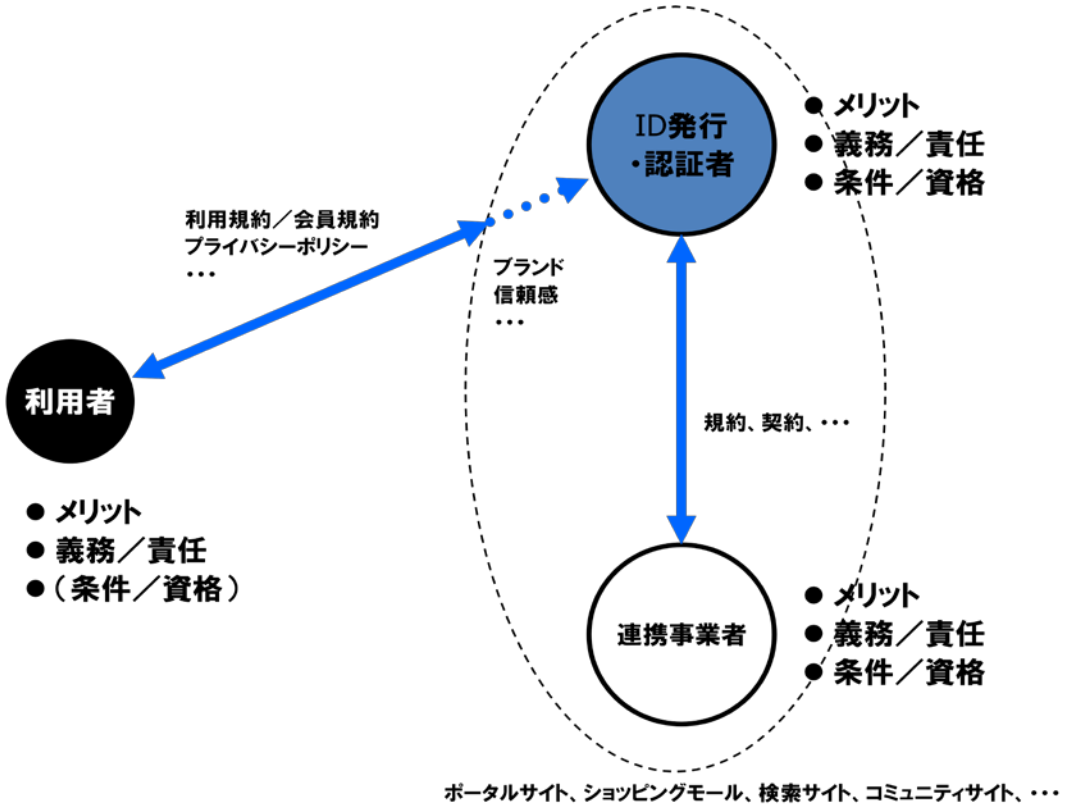
第３章　ID 連携の成立要因

ID ビジネスの各類型を踏まえ、ID 連携が成立する要因や継続していく条件について考察することにする。

1　ID 連携の構成

IDビジネスは 6 分類 7 類型に類型化できると考えられるが、いずれの類型にしても関係する主体は、簡略化すると、利用者、ID発行・認証者（IdP）、連携事業者（ID発行・認証者と連携してサービスを提供する事業者）[11]の三者となる。IDを連携しない場合は、ID発行・認証者と連携事業者が同一となるが、IDを連携する場合、別々の事業者となる。ID連携の構成を図示すると次のようになる。

図 9　ID 連携の概略



出典：総務省情報通信政策研究所、三菱総合研究所

[11] 前章までにおいて「サービス提供者」として説明してきた主体を、本章では、ID を連携する場合のみを扱うので、「連携事業者」として説明することにした。

ID 連携が成立するとともに、継続していくためには、次の 2 点が必要であると考えられる。

- ID 連携により、各主体それぞれがメリットを得ること
- ID 連携において、各主体それぞれが役割や責任を果たすこと

ID 連携が成立し、また、継続していくためには、利用者、ID 発行・認証者、そして、連携事業者それぞれがメリットを得なければならないのは当然のことである。

一方で、ID 連携には、リスクも当然存在し、利用者、ID 発行・認証者、連携事業者それぞれがリスクを回避するよう心がけなければならない。特に、ID 発行・認証者、連携事業者は、リスクを回避することにより、連携した ID の価値が減じることがないよう、お互いに義務や責任が生じることになる。すなわち、ID 発行・認証者と連携事業者は、連携した ID の信頼を維持すべく、相互に義務や責任を負うことになるのである。

そこで、以下、ID 連携の類型ごとに想定されるメリットやリスクを整理し、リスクを回避するために、利用者が注意すべき事項、ID 発行・認証者及び連携事業者が取り組むべき事項を検討することにする。

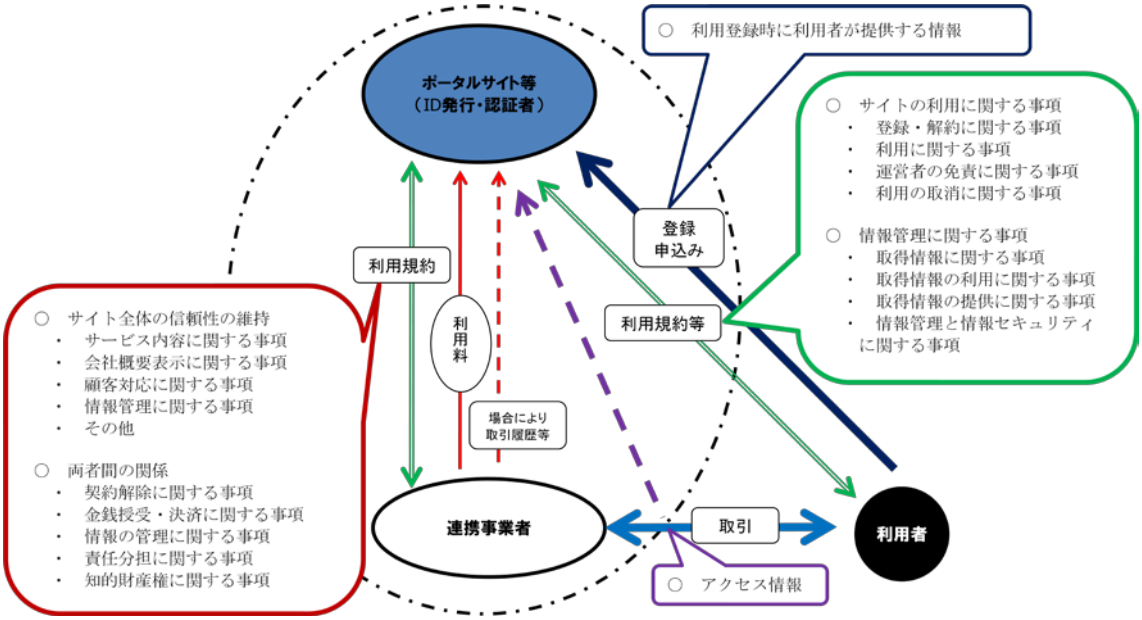
2　ポータル型の成立要因

まず、ポータル型のメリットを考えるとともに、そのリスクとそれを回避するために利用者が注意すべき事項、ID 発行・認証者及び連携事業者が取り組むべき事項について検討し、その成立要因を探ることにする。

（1）ポータル型のメリット

ポータル型における利用者、ID 発行・認証者であるポータルサイト等の運営者、連携事業者の関係を例示すると、次のようになる。

図 10　ポータル型の関係図（例）



出典：総務省情報通信政策研究所

ポータル型の場合、基本的には、ID 発行・認証者であるポータルサイト等の運営者が中心となって、サービスを提供することになる。

利用者は、ポータルサイト等にユーザー登録することにより連携事業者が提供する様々なサービスを受けることができるようになる。利用者としては、ユーザー登録によりポータルサイト等の運営者より発行された一つの ID で、連携事業者が提供する様々なサービスを利用できるメリットがある。

ポータルサイト等の運営者としては、様々なサービスを提供する連携事業者と連携することにより、利用者の利便性を高めて顧客を増やすことがで

きる。ポータルサイト等の利用が増えれば、それに応じて、連携事業者を増やしたり、あるいは、利用数に応じた料金制度としたりすることにより、ポータルサイト等の運営者は、事業を拡大できる。また、ポータルサイト等の運営者は、利用者のアクセス履歴、場合によっては利用者の連携事業者との取引履歴を取得することになっており、様々な情報を一元管理し、経営戦略等に役立てることができる。

一方、連携事業者は、ID 発行・認証者であるポータルサイト等と利用規約を締結し、ポータルサイト等に利用料を支払うことにより、利用者にサービスを提供するのであるが、連携事業者としても、集客力のあるポータルサイト等と連携することにより、自社の商品・サービスを提供する機会を増やすことができる。

（2）ポータル型のリスクとその回避

ポータル型のリスクについて考えると、まず、利用者としては、ユーザー登録するのはポータルサイト等であるが、取引するのは連携事業者である。多くの場合、取引においてトラブルが生じた場合、ポータルサイト等は免責されるようになっており、一方、連携事業者とは取引に限り契約関係にあるため、トラブルが容易に解決できるとは限らない懸念がある。

また、利用者のアクセス履歴、場合によっては連携事業者との取引履歴もポータルサイト等の運営者が取得することがあるため、あるポータルサイトで提供されている多くのサービスを利用すると、そのポータルサイトの運営者に様々な情報を提供することになる。利用者個人を特定されることはないとしても、そのような情報が不本意な形で利用されるおそれはある。

ポータルサイト等の運営者としては、利用者と取引するのは連携事業者であり、その取引においてトラブルが生じると、他の連携事業者も含め ID を連携している事業者全体の信用を失う可能性がある。

また、ポータルサイト等の運営者と連携事業者との責任関係を利用者が認識できるようにそれぞれのWebサイトの概観を工夫しておかないと、利用者が連携事業者との取引において生じた損害についてもポータルサイト等の運営者が責任を負わなければならなくなる場合も想定される[12]。

[12] ①外観上、ポータルサイト等を運営する ID 発行・認証者とサービスを提供する連携事業者が同一の営業主体であると判断されても仕方がない状態にあり、②そうであることについて、ポータルサイト等の運営者に責任があり、③利用者がポータルサイト等の運営者が提供していると誤認して連携事業者と取引をした結果、損害が生じた場合には、商法（明治 32 年法律第 48 号）第 14 条（自

連携事業者としては、ポータルサイト等の運営者による ID 発行、認証サービスが停止されたり、ポータルサイト等の運営者により提供されるサービスの内容の一部が変更されたりする場合に、自社のサービスにも影響が出る可能性がある。ポータルサイト等の運営者との力関係等によっては、その影響が大きくなってしまう場合も考えられる。

また、ポータルサイト等の運営者との契約にもよるが、ポータルサイト等の運営者は利用者に対してその個人情報を適切に保護・利用する義務を負っているため、連携事業者に対しては基本的に個人情報等を提供しない場合も想定される。例えば、利用者が連携事業者のサービスを利用する上で必要最低限の情報については、利用者との利用規約等に基づき提供されるが、それ以外の情報で、顧客管理、CRM[13]等に役立つと考えられる情報については、連携事業者で改めて収集する必要がある場合が想定される。そのような場合、連携事業者において、改めて個人情報等を収集することになるが、利用者によってはそれを嫌がることも考えられ、自社にユーザー登録してもらいサービスを提供する場合に比べると、顧客情報の収集という面では不利になり、経営戦略がうまくいかなくなる可能性はある。

この点については、ポータルサイト等の運営者が連携事業者に経営上のアドバイスをすることにより解消されていると考えられる例もあるが、連携事業者にとって、その有用性の程度によっては、営業面でのリスクを負うことになる。

ア　利用者が注意すべき事項

利用者は、ID／パスワードを適切に管理するなど利用者としての義務、責任を果たすことはもとより、ポータルサイト等の運営者の免責事項、その情報の取扱等については、登録時に提示される利用規約、個人情報保護方針やプライバシーポリシー等に明示されていることが多いので、必ず一読すべきである。ポータル型にあっては、ポータルサイト等の運営者と連携事業者

己の商号の使用を他人に許諾した商人の責任）の類推適用により、ポータルサイト等の運営者が責任を負う場合がある。電子商店街（ネットショッピングモール）運営者の責任について、「電子商取引及び情報財取引等に関する準則」（経済産業省、平成 20 年 8 月）44-47 頁参照。

[13] CRM（顧客関係性管理：Customer Relationship Management）とは、事業者が顧客との長期的な関係を築いていく取組をいう。新規に顧客を獲得するよりも、優良な既存顧客との関係を適切に維持する方が低コストかつ高収益であると考えられている。

との間でユーザー登録情報や取引履歴などをやり取りする例が多く、ユーザー登録に当たり、ひととおり目を通すことが大切である。

本調査研究のために実施した利用者へのアンケート調査の結果によると、ユーザー登録に際しては、既に多くの利用者が利用規約、個人情報保護方針やプライバシーポリシー等を読み、個人情報の取扱、Web サイトが収集する情報やその利用目的等を確認しているとの結果を得ている。しかし、必ずすべて読むと回答した者は、回答者の 2.5%と少なく、必ずすべて読むようにしたいものである。

イ　ポータルサイト等の運営者が取り組むべき事項

ポータル型にあっては、ポータルサイト等の運営者が ID 連携の中心となる。また、利用者の情報もポータルサイト等の運営者に集まるような仕組みとなっている例が多い。したがって、ポータルサイト等の運営者が主となり ID を連携している事業者全体の信頼確保、維持を図っていかなければならない。

多くのショッピングモール運営事業者は、出店事業者及び販売商品について厳しく審査しているようである。事業者によっては、最低でも書面の提出に加え、ポータルサイトで紹介する実際の店舗を目視等で確認している例もある。さらには、定常的に連携事業者のチェックを行っている事業者もいる。

加えて、ポータルサイト等の運営者は、多くの場合、利用者の ID をはじめとする情報の管理にも非常に気を使っているようである。利用者に対しては、利用規約、個人情報保護方針やプライバシーポリシー等において、連携事業者に対しては、ポータルサイトの利用規約において、それぞれ具体的に情報の利用や管理について定めている事業者が多い。ポータル型では、ポータルサイト等の運営者に情報が集まる分、その情報管理に対する責任は、重くなるのである。それらの規定において明示されていることを着実、かつ、継続的に実施していくことが大切である。

この点に関し、本調査研究ために実施した利用者へのアンケート調査の結果によると、ID 連携によって利用者に関する情報を他の事業者へ提供する場合は、利用規約等に記述されているだけでは不十分であり、より分かりやすい説明が求められている。また、他の Web サイトやサービスに利用者の情報の提供をして欲しくない、という意見も多い。このような利用者の要望に配慮した仕組みをいかに考案するかが重要となるであろう。

なお、連携事業者への情報提供の程度について、連携事業者が独自に情

報収集する範囲が大きい仕組みにする場合には、それに見合うメリットを連携事業者に提供することが大切であると思われる。

ちなみに、ポータルサイト等の運営者と連携事業者との利用者に対する責任分担については、利用者がユーザー登録するに当たり提示する利用規約等に規定し、Web サイトの概観を工夫して責任の所在を明確にするだけでなく、より分かりやすい形でポータルサイト等に明記することも考えられるのではなかろうか。

ウ　連携事業者が取り組むべき事項

ポータル型の場合、連携事業者と利用者との間のトラブルが、ID を連携している事業者全体の評価の減少につながることが想定される。仮に、責任は、ある特定の連携事業者にあるとしても、利用者としては、そのような連携事業者と ID を連携しているポータルサイト等の運営者や他の連携事業者への不信につながりかねない。そのため、ポータルサイト等の運営者と連携事業者との利用規約には、連携事業者に対する義務や責任が具体的に細かく明記されている例が多い。

連携事業者としては、自社のみの取引と考えるのではなく、ID を連携している事業者全体の信頼確保、維持という視点を持って事業運営に当たるべきであろう。

もちろん、このような視点は、利用者との取引に限らず、情報の利用や管理等、利用者との関係構築すべてについて必要であると考えられる。

3　相互連携型の成立要因

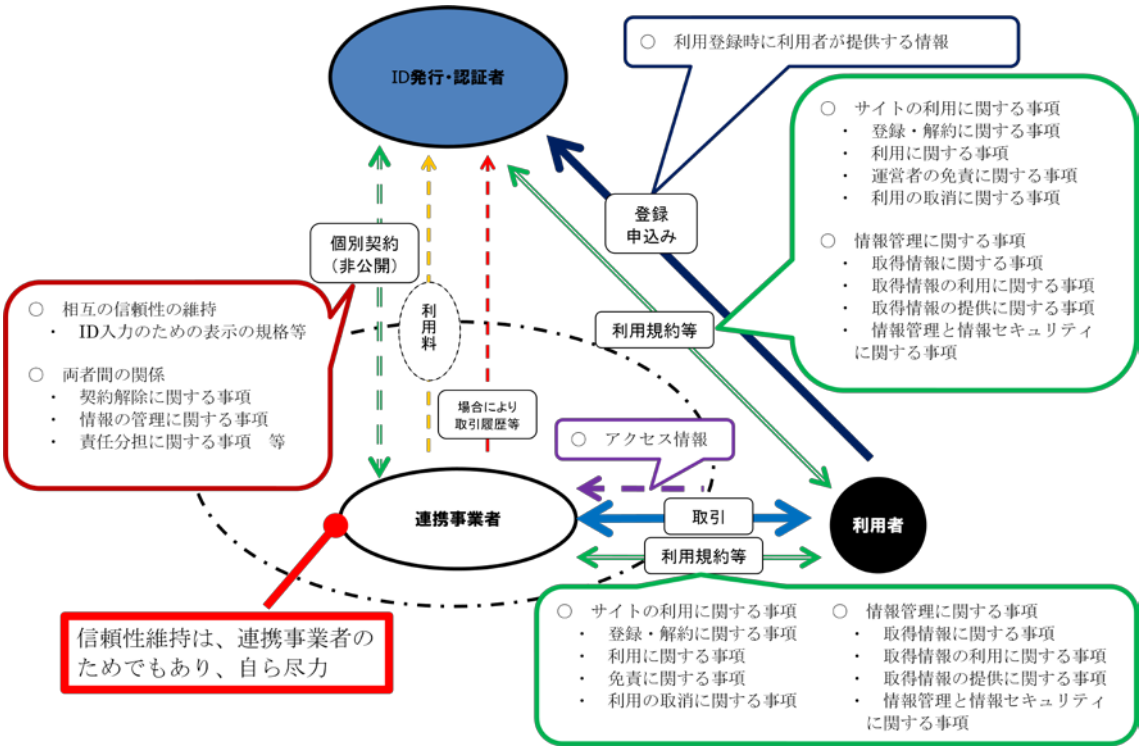
次に、相互連携型のメリットを考えるとともに、そのリスクとそれを回避するために利用者が注意すべき事項、ID 発行・認証者、連携事業者それぞれが取り組むべき事項について検討し、その成立要因を探ることにする。

なお、相互連携型には、事前連携型とオープン（アドホック）連携型の 2 つの類型があるが、共通する部分もあることから、まとめて検討することにする。

（1）相互連携型のメリット

相互連携型における利用者、ID 発行・認証者、連携事業者の関係を例示すると、次のようになる。

図 11　相互連携型の関係図（例）



出典：総務省情報通信政策研究所

なお、相互連携型では、連携事業者も ID 発行・認証者として ID を発行し、認証を行っている場合もあるが、ここでは、ID 発行・認証者と連携事業者を区別するため、利用者は ID 発行・認証者が発行した ID を用いて連

携事業者のサービスを利用する場合とした。

このような場合、事前連携型にあっては、連携事業者が ID 発行・認証者に利用料を支払っている場合もあるが、オープン（アドホック）連携型の場合には、ID 発行・認証者と連携事業者とが直接の契約関係になく、料金の支払いを要しない場合もある。オープン（アドホック）連携型の ID 発行・認証者は、自社の ID の価値を高めることを目的として ID 連携に応じており、収入は、広告収入等によっている場合もあるようである。

このように、相互連携型の場合、基本的には、ID 発行・認証者と連携事業者との関係は、ID 発行・認証者が主となる場合もあるが、ポータル型と比較し、ほぼ対等である。

相互連携型の Web サイトを利用する利用者は、ID 発行・認証者にユーザー登録することにより連携事業者が提供する様々なサービスを受けることができるようになる。利用者としては、ポータル型同様、ユーザー登録により ID 発行・認証者により発行された一つの ID で、連携事業者が提供する様々なサービスを利用できるメリットがある。特に、オープン（アドホック）連携型の場合、ID 発行・認証者が提供する ID と連携させる連携事業者を自ら選ぶことができるようになる。

ID 発行・認証者としては、様々なサービスを提供する連携事業者と ID を連携することにより、自社の ID の利便性を高め、自社の ID の価値を高めることができる。こうすることにより、自社の事業に顧客を引き付けることができ、事業機会の維持、拡大を企図することができる。

一方、連携事業者からすると、ID 発行・認証者に認証に必要なユーザー登録情報を管理してもらうことにより、必要以上の情報を管理する費用が削減できる。また、関連の深いサービスと連携して一貫したサービス群を形成することにより、利用者の利便性を高め、利用者の獲得・定着を促すこともできる。

（2）相互連携型のリスクとその回避

相互連携型のリスクについて考えると、まず、利用者としては、ユーザー登録するのは ID 発行・認証者であるが、取引するのは連携事業者である。事前連携型の場合はもとより、オープン（アドホック）連携型の場合には、本当に連携事業者のサイトであるかどうか、分からない可能性もある。間違って、フィッシングサイトに ID／パスワードを入力したりする可能性も否定できないであろう。また、連携事業者は、サービス提供に当たり必要な情報を利用者に改めて登録してもらう場合もあるが、同一の ID で利用する連

携事業者が多くなっていった場合、利用者は、どの事業者にどのような情報を登録したのか、分からなくなる可能性も想定される。

ID 発行・認証者としては、連携するサービスや事業者が増えると、自社のブランドや ID への信頼性を維持するためのコストが高くなることも考えられる。例えば、ID 連携により ID の登録者・利用者が増加した場合、その個人情報の管理コストは高くなる。個人情報の管理コストは、基本的には、有料サービスの場合は利用者、広告モデルによる場合は広告主、そのほか連携事業者などが負担するが、ID 連携のメリットがこれらの関係者に理解されず、ID 連携により生じた費用が収入を上回る場合には、結果的に ID 発行・認証者が負担することになると考えられる。

また、ID 発行・認証者としては、自社の ID の価値が高まることにより、場合によっては、その不正入手や不正使用の対策コストが増加する場合も考えられる。ID の不正使用の場合には不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号。以下「不正アクセス禁止法」という。）の対象になると考えられるが、ID の不正入手（個人が入手した ID が譲渡・売買されるなど）の場合には、この行為を直接に禁止する法律がないこともあり、対策はいっそう困難となる。

連携事業者としては、ポータル型の場合と同様に、ID 発行・認証者による ID 発行、認証サービスが停止されたり、ID 発行・認証者のサービス内容の一部が変更されたりする場合に、自社のサービスにも影響が出る可能性がある。しかも、オープン（アドホック）連携型による ID 連携では、連携事業者全体の信頼を確保するという意義は薄れ、あくまで ID 発行・認証者が発行する ID の価値を高めるという意義が大きいため、連携事業者としては、そのリスクは大きくなる。

ア　利用者が注意すべき事項

利用者としての義務、責任を果たすこと、例えば、ID／パスワードを管理することはもとより、ID 発行・認証者における免責事項、取得する情報の取扱だけでなく、ポータル型の場合以上に、連携事業者の利用規約、個人情報保護方針やプライバシーポリシー等をよく読まなければならない。ID 発行・認証者が提供するサービスの内容や免責事項、取得する情報の取扱だけでなく、連携事業者のサービスを利用する場合には、連携事業者の会社概要、連携事業者が提供するサービスの利用方法や連携事業者が取得した情報等の取扱、連携事業者の免責事項、さらには、ID 発行・認証者と連携事業者との関係等について、確認する必要がある。

特に、オープン（アドホック）連携型の場合には、ID 発行・認証者の ID／パスワードを入力してもらうために、連携事業者の Web サイトに ID 発行・認証者のロゴが表示されているだけの場合があり、その Web サイトを初めて訪れた者には、本当に ID 発行・認証者と連携している事業者なのかどうか、分からない可能性がある。したがって、利用しようとする Web サイトやその運営者に関する情報をしっかり収集してから利用するよう心がけるべきである。

イ　ID 発行・認証者が取り組むべき事項

相互連携型にあっては、事前連携型とオープン（アドホック）連携型とで多少の程度の差はあるが、ポータル型の場合に比べ、ID 発行・認証者が ID 連携の中心となることはあっても、連携事業者の独立性は保たれていると考えるべきであろう。

したがって、利用者がユーザー登録時に登録した情報に関しても、連携事業者との取引履歴等に関しても、基本的には、ID 発行・認証者と各連携事業者とがそれぞれ管理し、自ら利用するわけであり、ID 発行・認証者の情報管理に関する責任やコスト負担は少なくなると思われる。

しかし、オープン（アドホック）連携型の場合、事前に連携事業者と利用者の ID を連携しているわけではないため、自社が発行した ID を問題があると思われる事業者が利用する場合もあり、そのような場合、ID の認証を行わないようにするなどの対策が必要である。

この点に関し、事前連携型の場合には、ID 連携による自社のメリットだけでなく、連携しても問題がないかについても十分検討の上、ID 連携するかどうか判断しているのが一般的なようである。

ウ　連携事業者が取り組むべき事項

相互連携型の場合、ID 発行・認証者と連携事業者との関係は、ほぼ対等であり、ID 連携による利用者の評価は、自ら高めていかなければならない。すなわち、ID を連携している事業者全体の信頼確保、維持は、自社の信頼確保、維持でもあるということである。

ただし、ID による利用者の認証については、ID 発行・認証者に負っているわけであり、仮に ID 発行・認証者のサービスが変更になったり、中止になったりした場合、特にオープン（アドホック）連携型の場合には、どのようにしてサービスの継続的に提供していくのか、検討しておかなければなら

ないであろう。

また、特にオープン（アドホック）連携型の場合にいえることであるが、ID を連携したからといって、連携事業者の信頼性が高まるとは思えないので、自社の Web サイトに問題がないようにすることはもとより、サービス提供に当たっても利用者が安心して取引できるように、自ら尽力する必要がある。

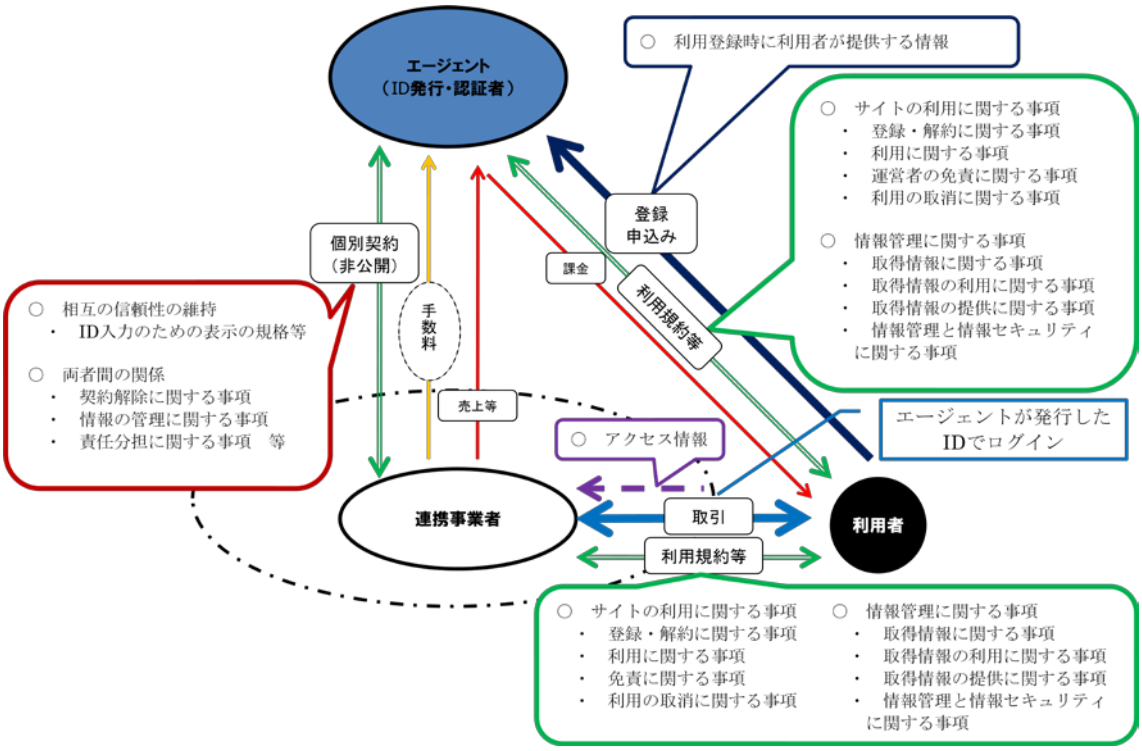
4　エージェント型の成立要因

エージェント型のメリットを考えるとともに、そのリスクとそれを回避するために利用者が注意すべき事項、エージェント及び連携事業者が取り組むべき事項について検討し、その成立要因を探ることにする。

（1）エージェント型のメリット

エージェント型で想定される利用者、ID 発行・認証者であるエージェント、連携事業者の関係を例示すると、次のようになる。

図 12　エージェント型の関係図（例）



出典：総務省情報通信政策研究所

エージェント型として考えられるサービスとしては、ID 発行・認証者であるエージェントが決済代行サービスを行う場合である。例えば、エージェントが発行する ID を用いてログインし、連携事業者が提供するサービスを利用した場合、連携事業者の代わりにエージェントが利用者に課金するような例が考えられる。その場合、連携事業者がエージェントに手数料を支払う

ことになる。

本調査研究のために実施した利用者へのアンケート調査の結果によると、多くの回答者は、決済に関係するクレジットカード情報、住所や電話番号といった個人を特定しやすい情報はできるだけ登録したくないと考えているが、インターネットショッピングでクレジットカードを利用する回答者の約9割がクレジットカード情報を登録している。これより、できるだけ登録したくない情報といえども、サービスに必要であれば、利便性を優先して登録していると考えられる。

利用者としては、できるだけ登録したくない情報を登録する事業者は少ない方がよく、しかも、ユーザー登録によりエージェントにより発行された一つのIDで、連携事業者が提供する様々なサービスが利用できると、その利便性は高まる。

エージェントとしては、様々なサービスを提供する連携事業者と連携することにより、自社のIDの利便性を高め、自社のIDの価値を高めることができる。こうすることにより、自社の事業に顧客を引き付けることができ、事業機会の維持、拡大を図ることができる。

一方、連携事業者からすると、エージェントに認証に必要なユーザー登録情報を管理してもらうだけでなく、利用者への課金も行ってもらうことができ、必要以上の情報を管理したり、利用者へ料金を請求したりする費用や労力が削減できる。

（2）エージェント型のリスクとその回避

エージェント型のリスクとして、特にエージェントが決済代行する例について考えることにする。

まず、利用者のリスクについて考える。エージェントとIDを連携している連携事業者としては、各種の決済代行サービスの一つとして利用者の利便性を考え、IDを連携したサービスを提供している可能性もある。すなわち、連携事業者としては、利用者より取引に係る料金を支払ってもらえればよく、万一、エージェントが当該料金を徴収できなかった場合、自ら徴収しようとすることも考えられる。したがって、利用者としては、二重に課金されないよう、エージェントが信頼できる事業者かどうか、しっかり判断する必要がある。

逆に、利用者から信頼を得られないエージェントでは、事業として成り立たないことになる。

エージェントとしては、利用者に提供するサービスは決済代行のみであ

ったとしても、連携事業者との取引に自社の ID が関係しているわけであるから、自社の ID の価値を高めるためには、連携事業者や連携事業者が提供するサービスの質も高めていかなければならないことになる。

また、利用者と連携事業者が取引し、当該取引により発生した料金の徴収をエージェントが実施するのであるが、取引から課金までの一連の流れの中で、利用者との間にトラブルが生じた場合、エージェントと連携事業者との責任分担が不明確な場合、エージェントに思わぬ責任が生じることになりかねない。

この利用者とのトラブルの問題は、連携事業者も同様であり、エージェントとの責任分担が不明確であれば、思わぬ責任が降りかかり、負担が生じることになりかねない。

ア　利用者が注意すべき事項

利用者としては、ID／パスワードの適切な管理など、利用者としての義務、責任を果たすことはもとより、エージェントの免責事項、取得した情報の取扱等について、ユーザー登録時に、利用規約、個人情報保護方針やプライバシーポリシー等に、ひととおり目を通すことが大切である。ポータル型の場合と比較し、エージェントと連携事業者との関係は、一定程度に限られており、一方、相互連携型の場合と比較すると、ある部分では相互連携型よりも強い関係にある。利用者としては、エージェントが提供するサービスの範囲を正確に把握しておく必要があると思われる。

この点について、ポータル型のところでも言及したが、本調査研究のために実施した利用者へのアンケート調査の結果によると、ユーザー登録に際し、利用規約、個人情報保護方針やプライバシーポリシー等を必ずすべて読むとした回答者は、回答者の 2.5%と少なく、必ずすべて読むようにすべきであろう。

イ　エージェントが取り組むべき事項

エージェントにあっては、利用者ができれば登録したくないと思うクレジットカード情報を扱うのであるから、利用者からの信頼を得ることが最も重要である。そのためには、エージェントは、利用者がユーザー登録時に提供したクレジットカード情報の取扱に注意することはもちろんのこと、そのほかの取得した情報についても、厳重に管理していかなければならないであろう。また、エージェントは、ポータル型におけるポータルサイト等同様に、

連携事業者も含めてIDを連携している事業者全体に対する利用者の信頼を得ることができるよう注意していく必要がある。

エージェントと連携事業者との関係は、ポータル型におけるポータルサイト等と連携事業者の場合に比べると希薄であるが、相互連携型における事業者間の関係と比べると濃厚であると考えられる。というのも、利用者との関係において、エージェントは、ID の発行・認証だけでなく、課金という一つの役割を担っているからである。しかし、連携事業者からみると、決済代行の一サービスとしてエージェントとIDを連携している場合も考えられる。したがって、エージェントとしては、連携事業者との関係をいかに構築していくか、が重要であり、また、連携事業者との責任分担を明確にしておく必要がある。

ウ　連携事業者が取り組むべき事項

連携事業者は、サービス提供から課金・決済に至るまでの流れの中で、エージェントと役割を分担しているわけであるから、エージェント同様、利用者との関係において、責任の範囲を明確にしておく必要がある。

また、連携事業者としては、エージェントと ID 連携するのは、ID の発行・認証を行ってもらうためではなく、利用者の支払の選択肢を増やすためである場合もあるであろう。そのような場合、ID を連携した事業者全体の信頼の維持という考え方はしないかもしれない。しかし、ID 連携により増やした支払の選択肢は、ID を連携しているから可能なのであり、そういった意味で、エージェント等、ID を連携した事業者全体の信頼を維持すべく尽力すべきである。

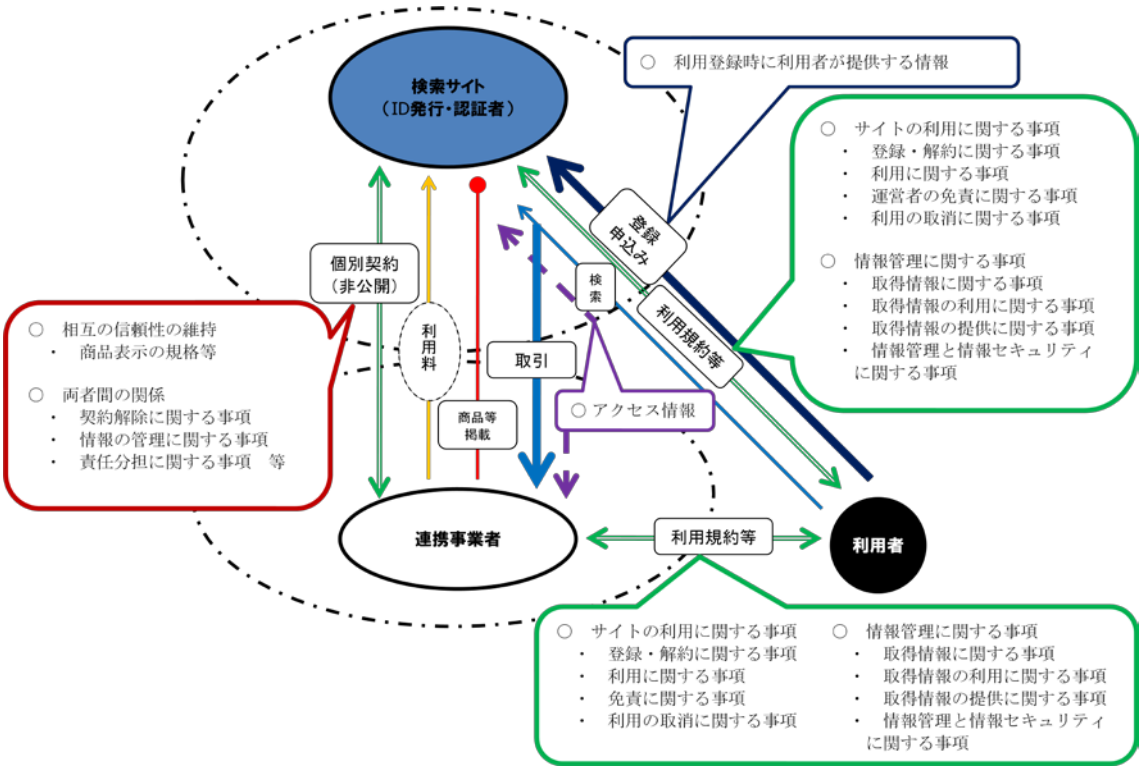
5　サーチ型の成立要因

サーチ型のメリットを考えるとともに、そのリスクとそれを回避するために利用者が注意すべき事項、検索サイトの運営者、連携事業者それぞれが取り組むべき事項について検討し、その成立要因を探ることにする。

（1）サーチ型のメリット

サーチ型で想定される利用者、ID 発行・認証者である検索サイトの運営者、連携事業者の関係を例示すると、次のようになる。

図 13　サーチ型の関係図（例）



出典：総務省情報通信政策研究所

サーチ型の ID 連携とは、例えば、利用者が検索サイトでログインし、商品等を検索した結果、購入したい商品等が見付かった場合、仮に、その商品等を提供する Web サイトを利用するためには別途ログインする必要があっても、検索サイトにログインしていれば、別途ログインすることなく、当該 Web サイトのサービスを受けられるようにすることである。

本調査研究のために実施した利用者へのアンケート調査の結果によると、サーチ型としてIDを連携したサービスを「利用してみたいと思う」と回答した者は、「利用してみたいと思わない」と回答した者を上回った。これは、利用者としては、検索によりよい商品等に出会える機会が増えることになるし、加えて、一つのIDで検索サイトからそのまま商品等を購入するWebサイトにアクセスでき、利用者の利便性に配慮したサービスであるからであると考えられる。無料の検索サイトは数多くあるが、個々のショッピングサイト等にユーザー登録していては、所有するIDの数が増えるばかりであり、検索サイトのIDによりショッピングサイト等を利用できれば、利用者としては、それに越したことはない。

検索サイトの運営者としては、様々なサービスを提供する事業者、しかも質の高いサービスを提供する事業者と連携することにより、自社サイトの利便性を高め、自社の提供する情報検索サービスの価値を高めることができる。また、IDを連携させることにより、利用者の利便性の向上も図ることができる。このようなサービスを提供することで、自社のサービスに顧客を引き付けることができ、事業機会の維持、拡大を図ることができる。

一方、連携事業者からすると、検索サイトとIDを連携させてサービスを提供することにより、検索サイトから自社のWebサイトへと利用者を誘導することができ、事業機会の拡大を図ることができる。

（2）サーチ型のリスクとその回避

サーチ型のリスクとして、まず、利用者のリスクについて考えると、検索サイトを利用する場合、当然のことであるが、検索の結果、表示された商品等が必ずしもよい商品等であるとは限らない。商品として問題があったり、取引する事業者に問題があったりする可能性は否定できない。

また、IDの連携により商品等を提供する連携事業者に検索サイトのIDでアクセスできると、利用者としては便利ではよいが、連携事業者が信頼できる事業者であるかどうか、不安を払しょくしきれないように思う。仮に、連携事業者に問題があった場合、不用意にそのWebサイトを利用すると不本意な状況に追い込まれる可能性もある。

検索サイトの運営者としては、利用者が検索した結果、利用者が望むような商品等を表示できなければ、ビジネスとして成り立たない。それは、商品等の品揃えにもよるし、連携事業者の質にもよるであろう。連携事業者の質との関係で、利用者が連携事業者との取引において問題が生じた場合、検索サイトの信用もなくす可能性がある。また、検索結果の表示方法も、利用

者が利用してみたくなるように工夫しなければ、利用者は、その検索サイトを用いて商品等を購入しようとは思わないかもしれない。

連携事業者としては、検索結果において目立つように表示されなければ、自社が提供する商品等がいくらよいものであっても、利用者にそのよさは伝わらない可能性がある。ポータル型におけるショッピングモールと比較し、連携事業者自ら情報発信できる範囲は更に限定されると考えられ、利用者にいかに自社が提供する商品等をアピールするか、が問題である。

ア　利用者が注意すべき事項

ID を連携しているかどうかにかかわらず、検索サイトを利用するときは必ず注意すべきであるが、利用者は、検索結果のみを信じるのではなく、購入したい商品等についての情報を収集するとともに、それを提供する事業者が信頼できるかどうか、自ら判断する必要がある。検索結果が必ずしも好ましいものばかりとは限らないことは、重々承知しておくべきである。

ID を連携している場合には、ポータル型の場合のように、検索サイトの運営者が連携事業者の信頼性を審査する方式が想定されるが、相互連携型、特に、オープン（アドホック）型の方式と併用してサーチ型のサービスを提供する場合には、検索サイトの運営者による審査は余り期待できないであろう。したがって、そのような場合、利用者の自己責任の範囲は大きくなるので注意を要する。

イ　検索サイトの運営者が取り組むべき事項

検索サイトの運営者としては、ID を連携しているか否かにかかわらず、検索の結果、利用者が望む商品等が表示されるようにするのが第一である。検索の結果に満足しなければ、利用者は、その検索サイトを余り利用しなくなるであろう。したがって、利用者が欲している情報が得られるように検索能力自体を工夫することが大切である。加えて、検索結果については、単に利用者が望む商品等が表示されるだけではなく、その質まで利用者に伝わるように工夫することが大切であると思われる。

ID を連携する場合は、利用者は、検索サイトの ID で連携事業者の Web サイトを利用できるようになるのであるが、連携事業者が信頼できるかどうかは、検索サイトの信頼にもかかわってくる。したがって、ID を連携する場合、検索サイトとしては、連携事業者の経営能力等の判断も重要になってくるであろう。

ウ　連携事業者が取り組むべき事項

連携事業者としては、自社が提供する商品等を、検索サイトにおける検索結果において、いかに利用者に魅力的に見せるか、が大切であると思われる。ポータル型における連携事業者と異なり、自社の Web サイトを検索サイトに設けられるわけではないので、検索結果に表示される商品等の画像等が重要になるのではなかろうか。

また、ポータル型の場合と同様、連携事業者と利用者との間のトラブルが、ID を連携している事業者全体の評価の減少につながることが想定される。仮に、そのトラブルの責任が、ある連携事業者にあるとしても、利用者としては、そのような連携事業者と ID を連携している検索サイトの運営者や他の連携事業者への不信につながりかねない。したがって、連携事業者は、利用者との取引を自社のみの取引と考えるのではなく、ID を連携している事業者全体の信頼確保、維持という視点を持って事業運営に当たるべきであろう。また、逆に、他の連携事業者の責に帰すべきトラブルが、ID を連携している事業者全体の不信につながり、自らも損失を被る可能性があるので、連携先がどのような検索サイトであるのかはもとより、他の連携事業者の動向にも注意する必要があると思われる。

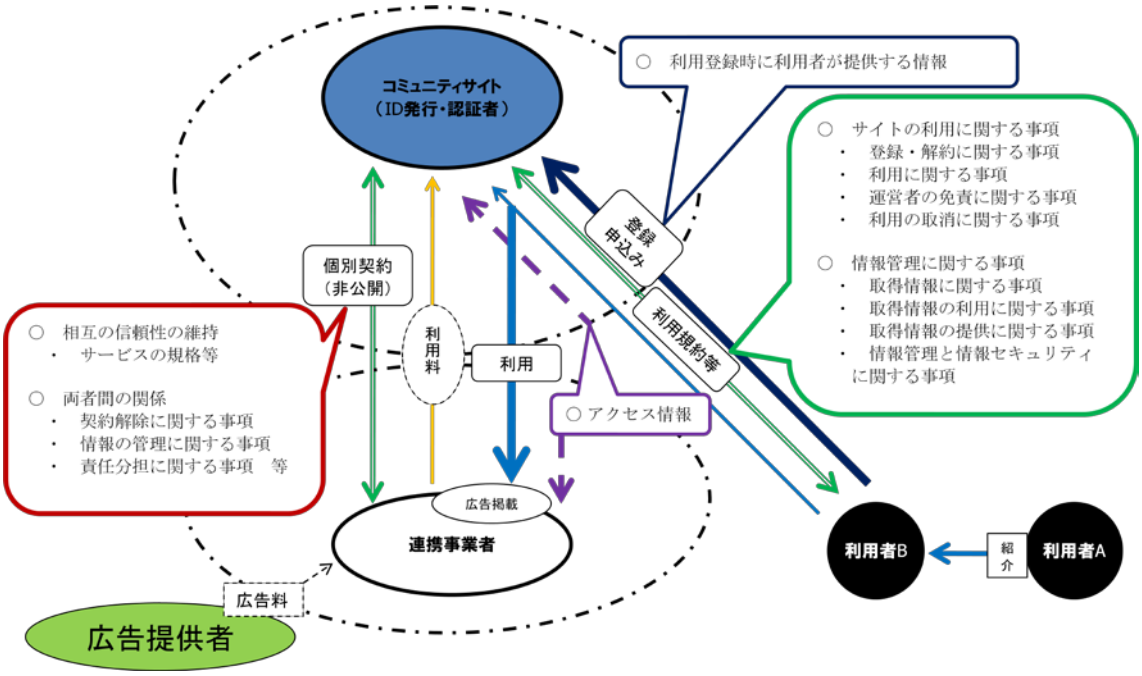
5　コミュニティ型の成立要因

コミュニティ型のメリットを考えるとともに、そのリスクとそれを回避するために利用者が注意すべき事項、コミュニティサイトの運営者、連携事業者それぞれが取り組むべき事項について検討し、その成立要因を探ることにする。

（1）コミュニティ型のメリット

コミュニティ型で想定される利用者、ID 発行・認証者であるコミュニティサイトの運営者、連携事業者の関係を例示すると、次のようになる。

図 14　コミュニティ型の関係図（例）



出典：総務省情報通信政策研究所

コミュニティ型の例としては、コミュニティサイトにおける知り合いの紹介により、新たなサービスを、別の ID を付与されることなく受けられるようになるサービスが考えられる。

本調査研究のために実施した利用者へのアンケート調査の結果によると、コミュニティ型については、「利用してみたいと思わない」と回答した者の方が「利用してみたいと思う」と回答した者より多かったが、SNS をよく利用している回答者に限ると、4 割の回答者が「利用してみたいと思う」と

回答しており、今後、利用者にとって期待される新しいサービスなのではないかと思われる。

利用者としては、他の利用者からの紹介によりサービスを利用することになり、安心してサービスを利用することができる。特に、ある分野に特化した質の高いサービスを利用するためには、同じような趣向を持つ者にそのようなサービスを提供している Web サイトを紹介してもらうのは役に立つであろう。

コミュニティサイトの運営者としては、様々なサービスを提供する事業者、しかも質の高いサービスを提供する事業者と連携することにより、自社が運営するコミュニティサイトの魅力を高め、利用者を増やすことができる。

一方、連携事業者からすると、自社が提供するサービス分野に関心を抱く利用者が集まるコミュニティサイトでサービスを提供することにより、特定の分野の利用者に利用してもらいやすくなる。他の類型により ID を連携するよりもその可能性は大きく、分野特化したサービスを提供する事業者としては、コミュニティサイトの運営者と連携することは非常に有益であると考えられる。

（2）コミュニティ型のリスクとその回避

コミュニティ型のリスクとして、まず、利用者のリスクについて考えると、コミュニティサイトを利用する場合、当然のことであるが、コミュニティの“友人”が必ずしもよい友人ばかりとは限らない。ID の不正使用等により問題のある“友人”と出会う可能性もある。

ちなみに、コミュニティ型の利用者は、他の利用者から紹介された利用者であり、そこにおける ID の価値とは、まさにコミュニティを形成する紐帯といえる。相互連携型のところでふれたとおり、ID の不正使用の場合には不正アクセス禁止法の対象になると考えられるが、ID の不正入手（個人が入手した ID が譲渡・売買される等）の場合には、この行為を直接に禁止する法律がない。コミュニティサイトの運営者としては、自社が提供するコミュニティを守るべく、ID の不正入手を防がなければならないが、その対策はコミュニティサイトの運営者に大きくのしかかってくると考えられる。

また、コミュニティ型の場合、コミュニティサイトにログインしている利用者が、他の利用者の紹介により連携事業者が提供する Web サイトにてサービスを受けることになるが、そこにおいて何らかのトラブルが生じた場合、コミュニティサイトに問い合わせが集中する可能性がある。そのような苦情対応にかかる費用が生じる可能性は否定できない。

一方、連携事業者としては、コミュニティサイトを通じた取引であるため、他の類型に比べ、仲間意識を有する利用者の評判がものをいうことになる。したがって、対象となる顧客層を意識したサービスの提供を求められることになると考えられる。

ア　利用者が注意すべき事項

利用者は、コミュニティサイトの知り合いの評判のみを信じるのではなく、紹介された商品・サービスの内容、それを提供する Web サイトの運営者が信頼できかかどうか、自ら判断する必要がある。そのためには、コミュニティサイトにおける知り合いに紹介されたから利用するというのではなく、サービス内容はもとより、連携事業者についても信頼できるかどうか、調査してから利用するよう心がけるべきであろう。

また、よりよいコミュニティを形成するためには、他者の誹謗中傷、掲示板への好ましくない書き込み、非常識な画像の掲載など、良識のない利用者によりコミュニティが乱されることがないようにしなければならない。そのためには、利用者は、自らの利用に当って注意するとともに、そのような利用を見付けた場合、コミュニティサイトの運営者に連絡するなど、自らよりよいコミュニティ形成のために尽力すべきであろう。

イ　コミュニティサイトの運営者が取り組むべき事項

コミュニティサイトの運営者にとって、コミュニティサイトで形成されるコミュニティは、正に資産といえる。利用者にコミュニティサイトを快く利用してもらい、よりよいコミュニティを形成してもらうためには、コミュニティサイトのマナーを確立しなければならない。その一環として、コミュニティサイトの運営者は、利用者が自社の提供するコミュニティサイトを安心して利用できるように、問題のある“友人”には利用を遠慮してもらわなければならない。そのための費用が収入を上回る場合は、事業として成り立たなくなるので注意を要する。

また、コミュニティサイトでは、利用者の評判により、質の高いサービスが最終的には好評となり、そうでないサービスは淘汰されている場合が多いようである。しかし、一度、信用をなくすと、コミュニティから利用者が離れていくのは早いと思われるので、コミュニティサイトの運営者としては、連携事業者や提供されるサービスの選択には、他の類型同様、尽力すべきであると思われる。

ウ　連携事業者が取り組むべき事項

連携事業者は、自社が提供するサービス分野に関心のある利用者が多くいるコミュニティサイトにおいてサービスを提供する場合、そのような利用者に満足がいくようなサービスの提供に心がけなければ、利用してもらえなくなる可能性は否定できない。すなわち、質の高いサービス提供が求められることを認識する必要があると思われる。

一方で、利用者のコミュニティサイトの評判は、連携事業者が提供するサービスの満足度にもよっている。連携事業者としては、コミュニティサイト自体の評価が下がれば、自社のサービスも利用してもらえなくなるということを十分に自覚してサービスを提供するよう心がけなければならないであろう。

第４章　ID ビジネスを取り巻く環境

第４章　ID ビジネスを取り巻く環境

ID ビジネスに関連して、我が国政府の取組や諸外国における ID 制度、官民連携への取組などを紹介するとともに、ID 連携に係る技術の標準化に向けての動きについて整理することにする。

１　我が国政府の取組

我が国の政府において、ID ビジネスに関連する様々な取組や検討が行われている。ここでは、政府における ID ビジネス発展のための取組だけでなく、民間事業者にも関係する官民連携への動きなどについても紹介する。

（１）「通信プラットフォーム研究会」報告書

総務省は、コンテンツ・アプリケーションをブロードバンド網で円滑に流通させる上で必要不可欠な認証･課金等のプラットフォーム機能の連携強化を図り、新事業の創出を促進するための市場環境の整備に向けて課題を整理し、今後の政策の方向性を検討することを目的として、2008 年 2 月 27 日より「通信プラットフォーム研究会」を開催し、2009 年 1 月 30 日に報告書をとりまとめた。

同報告書では、異なる認証基盤を用いる場合であっても、共通する一つの ID で認証を行えるようにするための環境整備の在り方について検討し、基本的視点として、

① 認証基盤は複数かつ競争的であり、相互に排他的でないこと
② 個人を認証する行為である「本人確認」（authentication）とサービス提供者が契約者にサービス提供するための「権限確認」（authorization）が明確に区別可能（一体的提供でも別々の形での提供でも可能）であること
③ 利用者が自らの属性情報を随時かつ完全に管理可能であること

が求められるとしている。

このような認証基盤の相互運用性の確保に当たっては、認証基盤の統合化（一本化）を目的とするのではなく、基本的には、各事業者の経営戦略等に基づき個別に構築される複数の認証基盤について、段階的にその相互運用性を確保していくことが望ましく、また、個人を識別できる属性情報が本人の意図に反して流通する事態を防止するため、個人の属性情報と直接ひも付けられる ID の管理は、当該 ID を発行した事業者が関係法令に基づいて厳

密に行い、かつ、利用者本人が承諾した場合にのみ当該 ID を個人属性とは切り離されたバーチャルな ID に変換して他事業者に提供する等、個人の属性情報の管理を利用者がコントロールできる仕組みが求められ、その際、個人による承諾についてオプトインとオプトアウトのいずれの仕組みを採用するか等、多様な社会的ルールを広く国民利用者の間で慎重に議論していく必要がある、と指摘している。

（2）「認証基盤連携フォーラム」における取組

「通信プラットフォーム研究会」報告書において、認証基盤の相互運用性に向けたインターフェイスの在り方等について、関係者で構成するフォーラムでセキュリティの確保などの具体的な検討を進めることが適当であると提言された。これを受け、認証基盤連携フォーラムが設立され、総務省からの実証実験費用の支援を受けて、2010 年 3 月まで認証基盤の相互運用性確保に向けた実証実験を実施している。

（3）「端末プラットフォーム技術に関する研究開発」の実施

ID 連携に関する研究開発の例として、独立行政法人情報通信研究機構（NICT）では、「新世代ネットワーク基盤技術に関する研究開発」の一環として、2008 年度からの 3 か年計画で「端末プラットフォーム技術に関する研究開発」を実施している。その内容としては、①ID 連携技術、②端末環境の構築技術、③サービス管理及び連携技術の研究開発であり、株式会社 KDDI 研究所、株式会社日立製作所、富士通株式会社、株式会社 OKI ネットワークスが受託し、初年度の成果として、例えば、携帯可能な端末上でシングル・サイン・オン（SSO）を実現する基本方式を考案、その有効性を確認している。

（4）「公的個人認証サービス普及拡大検討会」における取組

公的個人認証サービスは、第三者による情報の改ざんの防止及び通信相手の確認を行う高度な個人認証機能を安い費用で提供する公的サービスとして 2004 年より提供されている。総務省では、このような公的個人認証サービスの利用サービス拡大、利便性向上、行政分野における更なる利用促進等のための具体的方策について検討を行うため、2009 年 4 月 21 日より「公的個人認証サービス普及拡大検討会」を開催し、主として制度、運用面より

専門的な検討を行い、2009 年 8 月 12 日、「中間取りまとめ」を公表した。「中間取りまとめ」では、公的個人認証サービスの署名検証者（電子署名書の受信者）の範囲拡大について、民間認証局との関係を勘案し、公的個人認証サービスの署名検証者の範囲は、国民が広く利用するなど基盤としての役割が求められる業種を中心に検討することが適当であり、また、制度の信頼性を確保するため、法律上の義務を適切に遂行できる事業者に限定して拡大することが適当と考えられる、としている。

（5）「次世代電子行政サービス基盤等検討プロジェクトチーム」の取組

内閣官房情報通信技術（IT）担当室では、様々な行政手続を基本的にワンストップで簡便に行える次世代の電子行政サービス基盤の標準モデルについて 2010 年度を目途として構築し、実用化を目指すため「次世代電子行政サービス基盤等検討プロジェクトチーム」を設置して検討を重ね、2009 年 12 月 21 日に中間報告書を取りまとめた。中間報告書では、引越等のライフイベントにおいて、行政サービスだけでなく、民間企業の手続をも含めたサービスを提供するための「公共サービス連携基盤（仮称）」を構築することが考案されている。「公共サービス連携基盤（仮称）」は、利用者に対するログイン ID と機関ごとの連携用 ID を発行し、連携用 ID を暗号化して保管、各機関は、自機関用に発行された連携用 ID と各機関用の ID をひも付けて利用する連携方式が検討されている。

（6）「電子政府ガイドライン作成検討会（セキュリティ分科会）」の取組

内閣官房 IT 担当室では、電子政府の手続に応じたセキュリティ確保策等について、政府横断的なガイドラインを策定することに向け、2008 年 10 月 2 日、「電子政府ガイドライン作成検討会」を設置し、議論を重ねている。当検討会には、セキュリティ分科会が設置されており、オンライン手続における認証のリスク等について検討されている。

（7）「電子私書箱」に関する取組

内閣官房 IT 担当室は、医療機関や保険者等が個別に保有している情報を希望者が自ら入手・管理できる「電子私書箱（仮称）」について、「電子私書箱（仮称）による社会保障サービス等の IT 化に関する検討会」を設置し、2008 年 3 月 17 日に報告書を取りまとめた。同報告書において、電子私書箱

（仮称）の利用者が、公的機関だけでなく、民間事業者の情報も入手、閲覧できるようにすることの課題を検討している。

また、内閣官房 IT 担当室は、「電子私書箱（仮称）」の 2010 年頃のサービス開始を目指して、「電子私書箱（仮称）構想の実現に向けた基盤整備に関する検討会」を開催し、2009 年 3 月 31 日に報告書を取りまとめた。同報告書では、利用者の情報を安全に流通させるための認証の基点として電子私書箱（仮称）プラットフォームを構築することとし、そこにおける個人情報保護の要件やセキュリティ確保の必要性などの論点を整理している。

（８）「社会保障カード（仮称）」に関する取組

年金の記録を適正かつ効率的に管理するとともに、国民が容易に自らの記録を管理できるようにする一環として、「社会保障カード（仮称）」を 2011 年度中を目途に導入することとされたため、厚生労働省は、2007 年 9 月 27 日より「社会保障カード（仮称）の在り方に関する検討会」を開催し、2009 年 4 月 30 日、「社会保障カード（仮称）の基本的な計画に関する報告書」をとりまとめた。これまで、「社会保障カード（仮称）」は、年金記録等を簡便に確認でき、年金手帳、健康保険証、介護保険被保険者証の役割を果たすものとして検討され、各制度共通の統一的な番号を利用する案や現在の各制度の番号を直接関連付けた上で、各制度の番号をすべて一つのカードに記録する案などが提示されていた。同報告書では、いずれの案にしても、専用の端末を用いるなど適切な措置を講じなければ IC チップから送り出される情報を不正に読み出されるおそれを完全に否定できず、IC チップの演算機能を活用する公開鍵暗号の技術を活用する方法が安全性においては優れている、としている。また、「社会保障カード（仮称）」の検討に当たっては、他の関連する施策と連携して検討することが必要としている。

（９）「納税者番号」等に関する動き

脱税等を防止するため、税務当局が、納税者から提出される申告書の情報と、取引相手より提出される資料の情報とを、納税者に付番された「納税者番号」をキーとして整理する制度について、これまで様々な検討が行われてきた。

2009 年 12 月 22 日に閣議決定された「平成 22 年度税制改正大綱」では、「社会保障制度と税制度を一体化し、真に手を差し伸べるべき人に対する社会保障を充実させるとともに、社会保障制度の効率化を進めるため、また所

得税の公正性を担保するために、正しい所得把握体制の環境整備が必要不可欠」とし、社会保障・税共通の番号制度導入が述べられている。

なお、当該番号は、納税とも関連はするが、主として給付のための番号として制度設計を進め、その際、個人情報保護の観点が重要であることはいうまでもない、と付言している。

2009 年 2 月 8 日には、「社会保障・税に関わる番号制度に関する検討会」の第 1 回会合が開かれ、2010 年内に基本方針を策定し、2013 年に納税と社会保障のための共通番号制度を導入すべく、内閣官房国家戦略室を中心に省庁横断的な検討が開始された[14]。

14 「『社会保障番号』議論本格化」『読売新聞』2010 年 2 月 9 日 11 面。

2　諸外国における官民連携の動向

諸外国では、政府が提供しているID基盤を民間事業者がサービス提供のために利用したり、政府と民間事業者とのID連携が図られたりしている事例がある。

そこで、今後の我が国におけるIDビジネス及びID連携の在り方を検討する上で参考とするために、諸外国におけるIDに関する制度、IDの官民連携の取組の事例として、社会保障番号を利用している米国、欧州においてeID（electronic ID）制度を構築しているスウェーデン及びベルギー、独特の仕組みを構築しているオーストリア、市民ポータル構築を目指すドイツについて紹介する。また、IDが国民生活に深く根付いているといわれる韓国についても言及することにする。

（1）米国

ア　IDに係る制度

米国では、1936年、社会保障法に基づいて社会保障番号（SSN: Social Security Number）が導入された。本来、SSNは社会保障を受けるための登録番号であり、社会保障庁により付番・管理されているが、1962年からは納税のためにも利用されている。また、米国には戸籍制度がないため、SSNが身分を証明するために用いられるようにもなってきている。

SSNは、年金制度の加入資格を持つすべての者を対象に発行され[15]、アメリカ国籍を有する市民、永住者及び就労許可のある一時滞在者等に対して無料で発行され、無期限に使用できる。

社会保障庁以外の連邦機関や州政府等でもSSNを利用することは可能である。例えば、税務行政の適切な執行を図るため、給与所得情報の照合等にも活用されている。しかし、プライバシー保護の観点から、他の行政機関は、社会保障庁において管理されているデータベースにアクセスすることは原

[15] 米国の年金制度は、社会保障年金制度（OASDI: Old-Age, Survivors and Disability Insurance）、鉄道職員退職制度（RR: Railroad Retirement System）、連邦職員退職制度（CSRS: Civil Service Retirement System。なお、1984年以後に採用された連邦職員にはOASDIが適用されることになり、その上乗せとして連邦被用者退職制度（FERS: Federal Employees Retirement System）が新たに創設されている。）及び州・地方政府職員退職制度（PERISE）があり、SSNは共通して使用できる。

則として禁止されており、当該データベースに登録されている情報を得るためには、情報開示のための厳格な手続を経る必要がある。民間事業者についても、同様の厳格な手続が必要である[16]。

イ　官民による ID 連携

SSN は、本来は、社会保障を受けるための番号である。電子的に記録を管理する場合、社会保障番号を用いると便利であることもあり、従業員管理や医療記録管理、健康保険口座管理のために SSN が利用されるようになっているほか、銀行口座の開設、クレジットカードの取得、運転免許証の取得に当たっては、SSN を提供することが求められる。

統一的な ID による連携は、行政事務の効率化だけでなく、民間事業者によるサービス提供のための情報管理にも有益であり、それらのサービスを利用する者の利便性も向上すると考えられる。しかし、一方で、その場合、不正利用や登録情報が漏えいによる被害は、大きくなる可能性が高くなると考えられる。したがって、ID ビジネスの発展のためには、民間事業者やサービス利用者の利便性を高めることだけでなく、ID 連携により発生する、あるいは、可能性が高まるリスクの側面にも留意することが重要である。

（２）欧州

欧州委員会（European Comission）は、2005 年 6 月 1 日、i2010 を採択し、EU（欧州連合）加盟国の 2005 年から 2010 年までの行動計画を定めている[17]。そこにおいて、公的サービスと生活の質を高める情報社会を目標にし、電子政府（eGovernment）への取組を推進している。そこで重要になってくるのがeID制度の導入であるが、各国におけるeIDの取組状況は次のとおりである。

16 「政府税制調査会海外調査報告（アメリカ、カナダ）」（2009 年 8 月 6 日）<http://www.cao.go.jp/zeicho/siryou/pdf/sg5kai5-1.pdf>参照。

17 Commision of the European Communities, “i2010 - A European Information Society for growth and employment,” January 1, 2005.

表 9　EU 加盟国における eID の整備状況等

Country	ID Card?	Compulsory(i)/ Primary ID	eID Card? (ii)	eID Card Planned?
Austria	yes	No	yes	--
Belgium	yes	yes	yes	--
Bulgaria	yes	yes	(no)	(no)
Cyprus	yes	yes	no	no
Czech Republic	yes	yes	no	no
Denmark	no	--	--	no
Estonia	yes	(yes)	yes	--
Finland	yes	no	yes	--
France	yes	yes	no	yes
Germany	yes	(yes)	no	yes (specs)
Greece	yes	yes	no	no
Hungary	yes	no	no	yes
Ireland	no	--	--	no
Italy	yes	(yes)	yes (partial)	--
Latvia	no	--	--	yes
Lithuania	yes	yes	no	no
Luxembourg	yes	yes	no	yes
Malta	yes	yes	no	yes
Netherlands	yes	(yes)	yes	--
Poland	yes	yes	no	yes
Portugal	yes	yes	yes	--
Romania	yes	yes	no	yes
Slovakia	yes	yes	no	yes
Slovenia	yes	(yes)	no	yes
Spain	yes	yes	yes	--
Sweden	yes	no	yes	--
UK	yes (partial)	unknown	yes (partial)	--
Iceland	yes	yes	no	yes
Liechtenstein	yes	no	no	yes
Norway	no	--	--	no
Total	25	20	10	13

出典：ENISA, “Privacy Features of European eID Card Specifications,” January 27, 2009, p.6.

ここでは、eID が普及し、国民生活に根付いているといわれているスウェーデン及びベルギーについて、現状を紹介する。

また、政府が国民の各種データを一元管理することに対して強い抵抗感があるといわれており、独特の制度をとっているオーストリア、市民ポータルを構築しようとしているドイツの動きについても紹介する。

（2）-1　スウェーデン

ア　ID に係る制度

スウェーデンでは、「住民登録番号（Personal ID number）」を個人識別番号としている。この番号は、住民登録を行っている外国人を含む全国民に付与されている。通常は、出生時に病院から管轄機関である国税庁に直接申請する。

個人に発行されるカードには、スウェーデン市民だけに発行される「国民認証カード（National ID kort）」、スウェーデンの市民やスウェーデン在住の外国人を対象に社会保険事務局が無料で申請希望者に対して発行している「健康保険カード（European Health Insurance Card）」などがある。

イ　官民による ID 連携

スウェーデンの公的個人認証は eID と呼ばれ、eID の取得に当たってはインターネットバンキングを利用していることが条件になっている。すなわち、eID はインターネットバンキングを通じて発行される仕組みとなっており、発行場面において官民が連携している。利用料は政府が負担しているため、国民は無料で eID を取得・利用することができる。

eID は以下の手続きで利用されている。

- 国税庁：税金払戻し銀行口座の指定、特定の修正申告（後記）、税務申告代理人の指定、住民登録申請・変更（住民登録は国税庁が主管している。）
- 社会保険事務所：育児手当申請、払込銀行口座の指定
- 企業登録庁：企業の設立申請・変更

なお、税務申告は修正申告主義を採用しており、雇用主、銀行、証券会社、不動産業者等個人の財産を扱う機関は、法律で個人の税務関連資料を国

税庁に申告することが義務付けられている。そのため、個人に還元される税務申告資料は基本事項が記入済みのもので、個人はそれに対する修正申告を行う。修正申告における認証は 3 段階設けられている。

・電話・SMS（ショートメッセージサービス）：修正申告が不要の場合
・PIN-CODE（銀行の認証 ID）：旅費や被服費等の軽微な修正申告の場合
・eID：不動産売買や転職などの複雑な修正が伴う場合

ちなみに、認証別の電子税務申告の利用状況は次のとおりである。

表 10　スウェーデンの電子税務申告利用状況

	2002	2005	2006	2007	2008
eID 認証	－	429,580	468,787	646,158	839,429
PIN-CODE 認証	415,320	905,211	1,201,311	1,271,004	1,329,921
電話	－	568,694	689,080	799,104	880,837
SMS	－	238,041	322,683	435,212	551,945
合　計	415,320	2,141,526	2,681,861	3,151,478	3,602,132
	11.9%	32.9%	39.4%	46.3%	49.3%

出典：スウェーデン国税庁資料より作成

その他のインターネットサービスにおける認証方式は、次のとおりである。

表 11　スウェーデンにおけるインターネットサービスの認証方式

サービス名	認証方式
インターネットバンキング	8 桁の顧客番号＋4 桁の認証番号でログイン 銀行取引、証券取引等で利用
インターネットショッピング	VISA カード番号を認証コードとして利用
住民票交付	eID により国税庁サイトにログインし､自宅 PC にダウンロード
企業情報取得	企業登録庁から取得するが認証の必要はない（一般公開）
企業情報変更	eID により企業登録庁にログインし、変更情報を申請
私立図書館の書籍借り出し	e-mail アドレスによりログイン
スポーツセンター予約	会員番号を ID としてログイン
法律情報サービス	Netlex 社が発行する認証 ID によりログイン（有料制）
国鉄乗車券予約・航空券予約	VISA カード番号＋国民番号によりログイン 車掌やチェックインカウンターで国民 ID カードと照合
国民番号の発行	出生担当病院より eID にてログインし、国税庁に申請 30 分後に新生児の国民番号を付与

出典：現地在住者へのヒアリング

（2）-2　ベルギー

ア　ID に係る制度

①　国民登録番号

1983 年 8 月に施行された国民登録法により、ベルギー国民及び正規の在留外国人は 11 桁の国民登録番号（RRN Number = Rijksregister / Registre National：National Registry Number）が付番されており、多くの行政手続及びプライバシー委員会（独立機関）が承認した民間の手続において、基礎的な個人識別の手段として用いられている。

ベルギー国民は、市町村窓口に出生を届出た時点で、また、外国人は 1 年以上の在留許可を得た時点で国民登録番号が発給される。

② eID

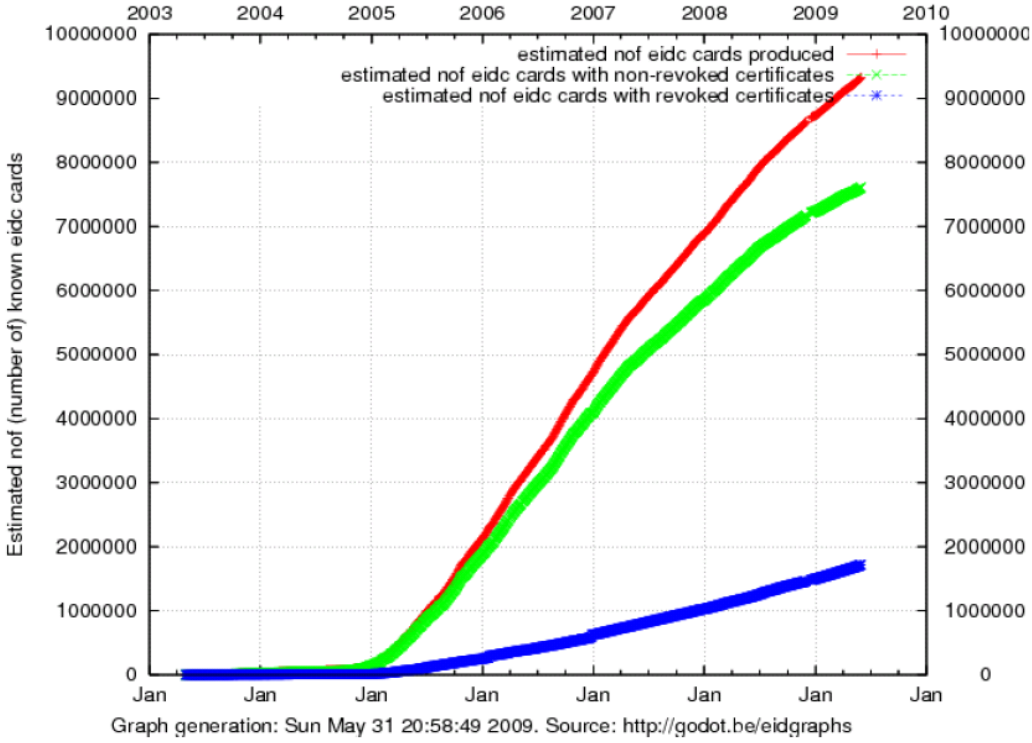
2001 年 7 月、電子政府（eGovernment）における電子的な個人識別のため、12 歳以上のベルギー国民（在留外国人を含む。）に対して eID 及びその格納媒体として e カードを発給することが決定された。eID 及び e カードは、ベルギー国内における官民サービスに共通して利用されると同時に、EU 域内での相互利用性（interoperability）も満足することが要件とされている。

eID の導入と運用には行政機関と共に民間事業者がかかわっており、認証局は政府の指定により複数の事業者が実施している。

なお、eID の登録局（Registry Agent）の役割は、市町村が担当している。これは、eID の登録、更新、失効に必要な出生、死亡、婚姻等に関する情報は市町村が管理しており、eID の正確性を担保するためには市町村が担当するのが相応しいことによる。

2009 年末までには、短期（1 年未満）の在留外国人を除き、すべて eID 及び e カードへの移行が完了する予定である。2003 年から 2009 年までの e カードの発行件数、有効件数及び失効件数の予定は次のとおりである。

図 15　e カードの発行件数の見積



（上から e カードの発行件数（赤色）、有効件数（緑色）、失効件数（青色））

出典：Danny De Cock の Web ページ<http://homes.esat.kuleuven.be/~decockd/wiki/bin/view.cgi/Main/BelgianEidCardGraphsTOC>

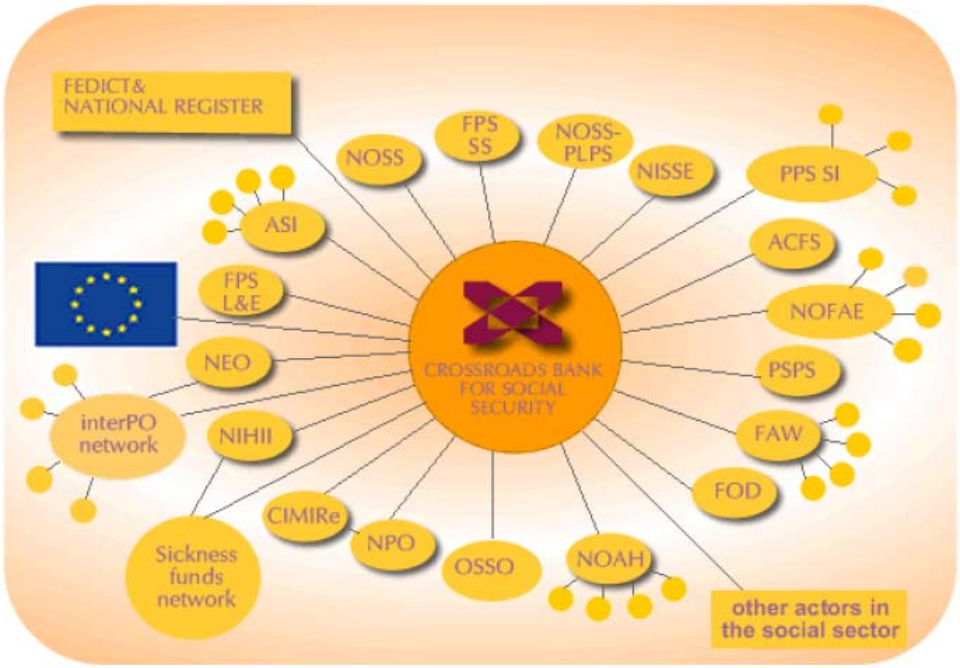
イ　官民による ID 連携

① CBSS（Crossroad Bank for Social Security）

ベルギーの電子政府（eGovernment）における ID 連携の最も先進的なシステムは、社会保障分野における官民のバックオフィス連携を実現した CBSS である。労働関係を中心に社会保障に関する 7 つのアプリケーション（障害者雇用、労働災害、傷病休業、育児休業、高齢者再雇用、休日深夜勤務、失業）の受給資格管理、保険料徴収、補助金・手当て等の給付等のサービスを提供している。

CBSS によって連携する官民のサービス機関には、約 3000 機関・団体が参加している。

図 16　CBSS サービス機関の概要



出典 : CBSS の Web ページ<http://www.ksz-bcss.fgov.be/en/international/page/content/websites/international/aboutcbss.html>

② adapID プロジェクト

eID のアプリケーション分野を拡大することによって、その効果は一層高まることが期待されており、2005 年から adapID と呼ばれるプロジェクトが継続的に推進されている。adapID プロジェクトは、eID の利用に関する標準的な仕様を策定し、官民で eID によるバックオフィス連携のための枠組みを提供している。

adapID プロジェクトによる実施計画として、以下に関する具体的な計画が示されている。

- e-Health
  - 電子カルテ管理（EHRs：e-Health Records Management）
  - 症例検索（Clinical Data Mining）
- e-Government
  - オンライン照会・問合せ
  - ワンストップ・オンライン申請・届出
- 公文書保存（TAS：Trusted Archives）

・　個人交通違反記録（Climinal Records for Road Hogs）
・　個人健診記録（Personal Medical Information）
・　電子署名文書長期保存（Long-Term Archival of Digitally Sighned Documents）

● 電子商取引（Financial）
・　インターネットショッピング
・　インターネットバンキング
・　電子契約

（2）-3　オーストリア

ア　ID に係る制度

オーストリアでは、2004 年に施行された電子政府法に基づき電子政府（eGovernment）への取組を進めている。オーストリアは、ナチス・ドイツにより併合され、国民が政府による厳しい統制を受けた歴史を有しており、政府が国民の各種データを一元管理することに対して強い抵抗感があるといわれている。そのため、オーストリアでは、政府の各機関が保有する個人データを保護するための独特の仕組みを構築している。

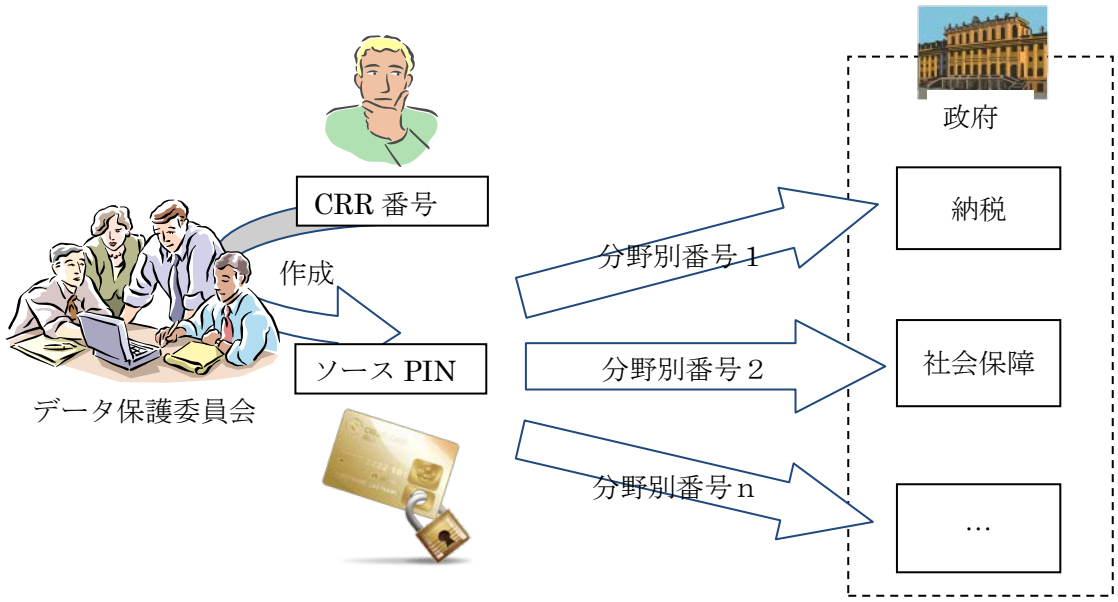
オーストリアの住民登録データは、内務省が管理する中央住民登録簿（CRR: Central Residents Register）において管理されている[18]。しかし、オーストリアでは、CRR番号、ソースPIN、「分野別番号」といった体系を採ることにより、国民に関するデータの保護に配慮するとともに、行政事務の効率化、住民の利便性の向上にも考慮した制度を構築している。

国民が電子行政サービスを利用する場合には、CRR番号を元に第三者機関である「データ保護委員会」[19]がソースPINを発行する。このソースPINに分野コードを加えてハッシュ化することにより「分野別番号」が作成される。ソースPINは本人所有のICカードにのみ記録・保存されるようになっており、「分野別番号」は、各行政機関のみが保存、管理することになっている。また、「分野別番号」からソースPINへの逆変換はできないようになっている。したがって、各行政機関が管理する「分野別番号」よりCRR番号を割り出すことはできず、また、他の行政機関が管理する「分野別番号」と

[18] 在留外国人のデータは、「SR（Supplementary Register）」に登録されている。
[19] データ保護委員会は 6 名の委員で構成されている。委員の内訳は、州の代表 2 名、労働組合の代表 1 名、連邦政府の代表 1 名、経済団体の代表 1 名、裁判所の代表 1 名となっている。各委員は、連邦大統領が任命する。

別の分野の行政機関が管理する「分野別番号」を突合することもできない仕組みとなっている。

図 17　オーストリアの ID 制度のイメージ



出典：国際社会経済研究所監修（2009）等より作成

なお、分野が異なる行政機関間での国民データの交換は、その都度、データ保護委員会を通して行うことになっており、データ保護委員会が仲介・監視することにより、政府による国民に関するデータの不正利用を防止している。

イ　官民による ID 連携

「市民カード」は、インターネットにおける民間サービスにも利用することができる。すなわち、民間事業者は、本人の同意があれば、独自に「民間分野別番号」を生成し、自社が提供するインターネットでのサービスを利用する者のために使用することができる。この「民間分野別番号」は、民間事業者がソース PIN を読み取ることなく生成される仕組みになっている。

このような仕組みを活用することにより、利用者（市民）はインターネットで提供されるサービスごとの複数の ID を管理する煩雑さから解放され、利用者の利便性が高められると考えられる。また、民間事業者としては、本人確認の厳密性を確保するとともに、サービス提供には不要な利用者データ

を取得・管理する必要がなくなり、個人情報の管理コストを適切にする効果が期待できるものと考えられる。

（2）-4　ドイツ

ア　官民による ID 連携

ドイツにおいては、官民連携の ID ビジネスとして市民ポータルの実証実験が本年度から開始されており、来年度から本運用が予定されている。その目的は、市民・企業や行政が信頼して情報交換できること、及び法的拘束力のある官民連携認証基盤の構築である。現在、そのために必要な法律「市民ポータル規制及び更なる規則の変更に関する法律」（ドイツ市民ポータル法）の草案が審議されている。

市民ポータルに至る法整備の流れは以下のようになっている。電子政府（eGovernment）V2 はドイツのハイテク戦略でもあり、ID 戦略の一環として eID の利用環境整備が行われ、その延長として「安全で信頼できる使いやすい通信環境の整備」が検討されて市民ポータル構想が生まれた。これらの法整備プロセスにおいて、仮名による個人情報の確保策は共通の観点になっている。

1997 年　デジタル署名法：タイムスタンプを法定（仮名利用の署名も個人情報保護の観点から承認（機関認証、法人認証にも利用））
2001 年　電子署名大綱法：適格署名と認定署名を設定
2005 年　電子政府 V2 で e カード戦略設定
2009 年　eID カード法：eID カード、適格署名利用環境整備
ドイツ市民ポータル法案審議中

市民ポータルは、政府の運営するポータルサイトではないが、日本の特定認証認定局のように法律に基づき認定された民間業者が、そのサービスを提供する。市民ポータルの主なサービスは、以下のとおりである。

①　De Mail（安全な電子メールサービス）

郵便ポストのように、文書やメッセージをインターネット上で簡単かつ安全に送受信可能にする。政府からの通知文書なども、公的なメール

アドレスでプロバイダから受け取ることができ、仮名（pseudonym）のメールアドレスも入手可能である。

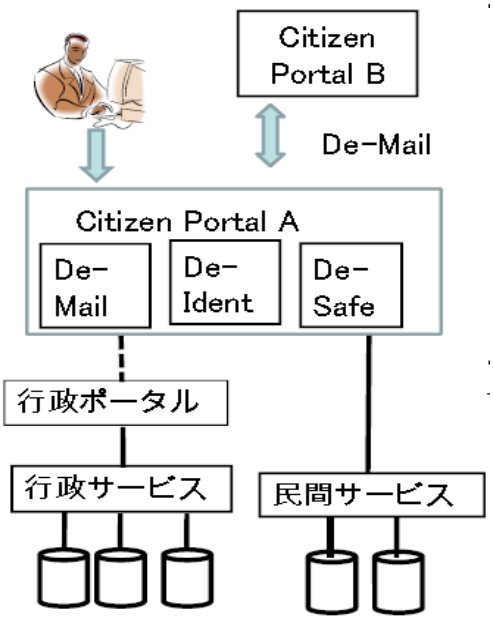
② De-Ident （アイデンティティ証明サービス）

一種の身元確認サービスである。例えば、インターネットで買い物をする場合の年齢の証明などに使用される。利用者の判断により、De-Mailを用いて、De-Mail アドレスあてに送信することもできる。サービス提供業者が保管する属性データは、署名が付され、改ざん等を防止している。保管されるデータは、ID と氏名、住所、出生地、生年月日などである。

③ De-Safe（文書の長期保存サービス（ストレージサービス））

利用者の文書を格納し、長期保存するための「文書庫」と呼ばれる安全なストレージ装置が提供される。De-Mail で文書を受け取った場合は文書庫にコピーされ、文書庫の文書を他の De-Mail 利用者に送信することも可能となる。

図 18 ドイツ市民ポータルの概略



出典：次世代電子商取引推進協議会（ECOM）電子署名普及 WG 資料

ドイツの市民ポータルの特徴は、eID の利用を民間にも開放し、官民共用の電子認証基盤にした点にある。もちろん民間企業の利用においては、事前の eID アクセス権限審査を制度化し、民間事業者によるアクセス権限証明書により運用されている。このアクセス権限証明書のチェックにおいては、当事者相互の認証が可能であり、かつ、選択した情報のみにアクセスが承認される仕組みになっている。また、個人情報の範囲についても登録利用者が選択して送信可能になるなど、個人情報のコントロール権が付与されていると判断される。

このような法整備に加え、標準化や相互運用性確保の基準も整備されつつあるが、EU 全体としても、電子署名の利用は進んでいない。電子署名カードの普及施策として、標準的な SSCD（Secure signature creation device）搭載チップカードの普及が促進されており、e カード戦略として eID カードのみならずジョブカードやヘルスケアカードにも活用されているようである。

（3）韓国

ア　ID に係る制度

韓国では、個人を識別する番号制度として、「住民登録番号」制度が導入されている。住民登録番号は、韓国の市民及び韓国に居住する外国人で一定の資格のある者を対象に、行政安全部（日本の総務省に該当）にて発行されており、現在までの累計登録者数は 4 千万人に及んでいる。

利用分野は、所得税申告、年金受給、運転免許取得、旅券発給、各種公的資格取得、銀行口座開設など幅広い分野にわたり、官民での相互利用についての制限は設けられていない。

住民登録カードについては、1999 年からプラスチックカードの導入と指紋の制度化が図られ、2009 年以降スマートカード型の電子カードの導入が計画されている。住民登録カードは、各自治体（市町村）が発行し、満 17 歳以上の全国民が保有している。住民登録カードには、名前、生年月日、住所、登録地、発行日、国民番号、顔写真、指紋が記載されている。前述のとおり、今後は順次 IC カードへの移行が計画されている。

イ　官民による ID 連携

①　国民向けの電子認証基盤

韓国では、ICTの生活場面への普及に伴い、電子的文書の流通が増加した結果、文書及び個人情報漏洩問題、文書の偽造等の問題を解決するため、インターネット基盤の電子文書流通の安定性の確保の必要性からPKI（Public Key Infrastructure）[20]による認証が急速に広まった。

韓国の PKI 取得比率はインターネット利用者の 58.7%と極めて高く（表 12)、商取引全体の金額に占める電子商取引総額の 27.8%（630 兆ウォン）が PKI を活用している（表 13)。

表 12　韓国のインターネット利用者数及び PKI 発行件数等

インターネット利用者数（2008 年末）	35,360 千人
PKI 発行件数（2009 年 6 月末時点）	20,772 千人
PKI 取得比率	58.7%

出典：韓国情報化振興院『2009 年韓国国家情報化白書』

表 13　韓国の電子商取引の比率

＊電子商取引規模（2008 年）	630 兆ウォン
商取引総額（2008 年）	2,268 兆ウォン
電子商取引比率（PKI 利用比率）	27.8%

出典：韓国情報化振興院『2009 年韓国国家情報化白書』

また、PKI を活用したオンライン株式取引の比率も全体取引の 49.7%と極めて高く（表 14)、同様のオンライン取引上の電子通貨の 1 日平均利用規模は、306 千件、262 百万ウォンに上っている。

表 14　オンライン株式取引の利用状況等

オンライン株式取引	1,586 兆ウォン
全体取引	3,190 兆ウォン
電子商取引比率（PKI 利用比率）	49.7%

出典：韓国情報化振興院『2009 年韓国国家情報化白書』

このように、電子商取引、オンライン株式取引等で PKI が活用されており、市民生活に大きく根付いている様子がうかがえる。

[20] PKI とは、公開鍵暗号方式を用いて、電子署名、電子認証システムを支える公開鍵暗号基盤のこと。

② 認証機関

韓国の公的認証の発行機関には以下の官民の機関があり、どの機関が発行したものでも共通で使用できる。

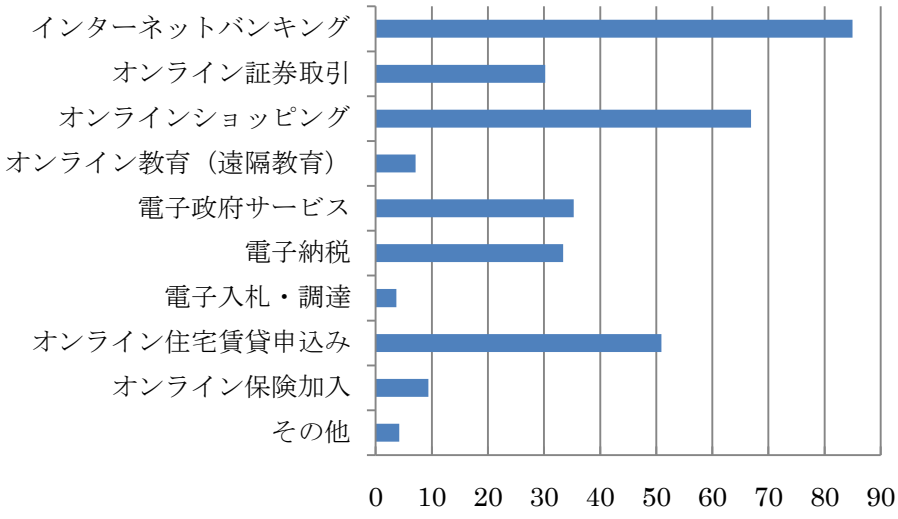
i. 金融決済院
ii. Koskom（韓国証券電算）
iii. 韓国貿易情報通信
iv. 韓国電子認証
v. 韓国情報認証

③ 韓国における PKI の利用場面

特定非営利活動法人東アジア国際ビジネス支援センター（EABuS）が 2009 年 5 月に行った「社会基盤としての国民 ID に関する意識調査」によれば、韓国における PKI の利用場面は、インターネットバンキング、オンラインショッピング、オンライン住宅賃貸申し込みといった民間での利用が圧倒的に多い。

図 19 韓国における PKI の利用場面

Q11> 現在、あなたは公的個人認証をどういう場合によく利用していますか。



出典：EABuS「社会基盤としての国民 ID に関する意識調査」12 頁

3　ID 連携関連技術の標準化の動向

ID 連携の実現に当たっては、ID 認証の技術だけでなく、その経路となるインターネット関連技術、セキュリティ技術など、様々な技術がかかわっている。ID 連携を実現するためには、各主体間でこれら多様な技術に関する共通の認識・仕組みを形成することが不可欠であり、欧米の民間企業を中心とした各団体で ID 連携関連技術の標準化に係る取組が積極的に推進されている。

以下では、ID 連携に係る技術について、主要な標準化団体等における取組の動向について整理を行った。

（1）OpenID Foundation における標準化に係る検討状況（OpenID）

Open ID Foundation は、OpenID の規格の制定・管理を行う米国の非営利法人であり、主に①知財管理、②追加仕様の策定、③技術の普及・啓発活動を行っている。理事企業は、Yahoo!、Google、IBM、VeriSign、Microsoft である。また、Open ID Foundation と連携する団体として、OpenID Foundation Europe 等があり、グローバルな活動を展開している。

日本国内における Open ID 技術の理解促進と普及を図る団体としては、OpenID ファウンデーション・ジャパンが 2008 年 10 月に一般社団法人として発足しており、2009 年 12 月現在、50 社が会員企業として参加している（表 15）。

表 15　OpenID ファウンデーション・ジャパン参加企業等

【会員企業】

株式会社アグレックス
株式会社朝日ネット
株式会社アスタリクス
株式会社イマーディオ
インディゴ株式会社
インフォテリア株式会社
エキサイト株式会社
SBI ホールディング株式会社
NEC ビッグローブ株式会社
NTT ｺﾐｭﾆｹｰｼｮﾝｽﾞ株式会社
株式会社 NTT データ
株式会社 NTT ドコモ
株式会社 NTT レゾナント
沖電気工業株式会社
学校法人河合塾
株式会社 Cuon
株式会社ケイ・プティコム
KDDI 株式会社
サイバートラスト株式会社
株式会社ザクラ
GMO ペイメントゲートウェイ株式会社
株式会社ジェーシービー
シックス・アパート株式会社
セコムトラストシステムズ株式会社
株式会社セブン銀行
セレゴ・ジャパン株式会社
株式会社千趣会
ソフトバンク BB 株式会社
ｿﾌﾄﾊﾞﾝｸ･ﾍﾟｲﾒﾝﾄ･ｻｰﾋﾞｽ株式会社
株式会社損保ｼﾞｬﾊﾟﾝ･ｼｽﾃﾑｿﾘｭｰｼｮﾝ
タイヘイコンピューター株式会社
株式会社ティーガイア
株式会社テクノラティジャパン
ﾃﾞｼﾞﾀﾙｶﾞﾚｰｼﾞｲｰｺﾝﾃｸｽﾄｶﾝﾊﾟﾆｰ
ニフティ株式会社
日本アイ・ビー・エム株式会社
株式会社日本航空ｲﾝﾀｰﾅｼｮﾅﾙ
日本生命保険相互会社
日本電気株式会社
日本ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ株式会社
日本ベリサイン株式会社
株式会社野村総合研究所
株式会社日立製作所
株式会社ミクシィ
三井住友海上火災保険株式会社
株式会社三菱東京 UFJ 銀行
ヤフー株式会社
株式会社ライブドア
楽天株式会社

【アドバイザー】

東京大学大学院情報環境・学際情報学府　須藤　修教授
慶應義塾大学総合政策学部　国領　二郎教授
中央大学大学院戦略経営研究科　杉浦　宣彦教授

【パートナー】

カンターラ・イニシアティブ　ジャパンワークグループ
リバティ・アライアンス　日本 SIG

出典：OpenID ファウンデーション・ジャパン資料

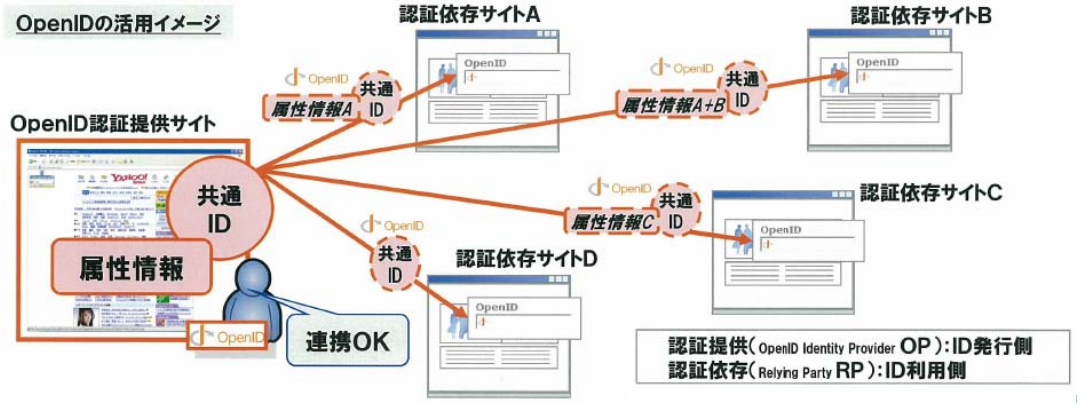
ア　OpenID 技術の概要

OpenID とは、共通のユーザープロファイル（ID、属性）を複数のネットワークサービスで利用可能にする規格である。

その利用のイメージとしては、一つの OpenID 対応サイトで、一度、ID を登録すれば、他の OpenID 対応サイトも、ID を登録することなく、同一の ID でログインできるとともに、利用者の選択により登録情報の連携を行うことができる。

OpenID は、そのモジュールを導入することにより、OpenID 発行者との信頼関係とは関係なく ID の認証を行うことができる。したがって、対象とする領域が利用者の確認（Authenticaton）に絞り込まれており、アクセス制御等の権限確認（Authorization）は行わないことで、プロトコルを『軽く』していることが特徴である。

図 20　OpenID の利用イメージ



出典：OpenID ファウンデーション・ジャパン資料

2009 年現在、世界で 14 億 4000 万 ID が発行され、50,000 以上のサイトで OpenID が利用可能となっている。

イ　OpenID による ID 連携

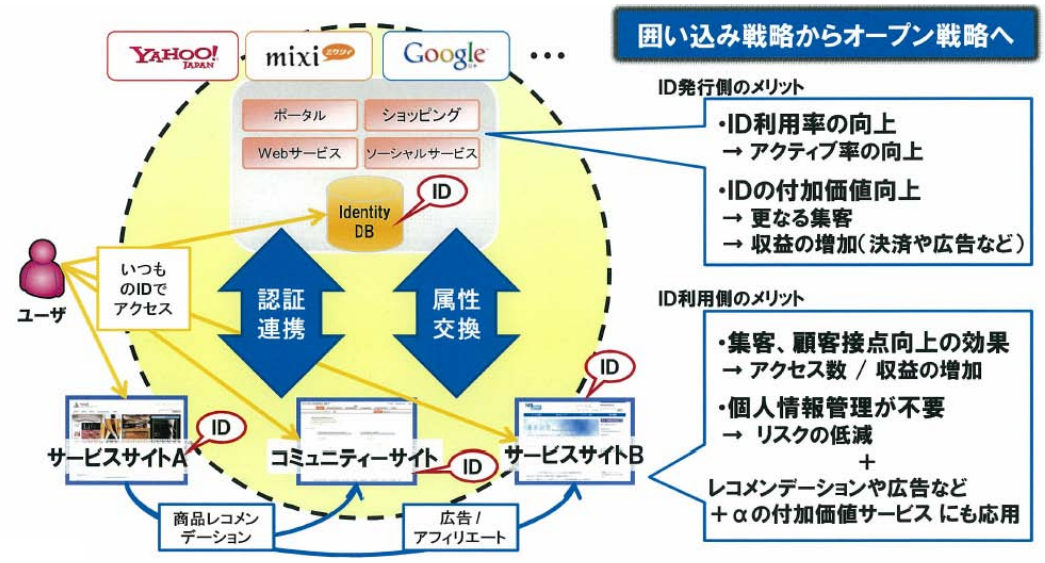
OpenID は、本来の利用方法としては、特に信頼関係を結んでいないある OpenID 発行者サイトの認証機能を利用して ID 認証を行うことが可能であることが特徴であるが、認証元／先を制限することも可能となっている。

OpenID による ID 連携の例は、以下のとおり。

①　経済圏の創出

多数の ID を発行している ID ホルダーを中心に、関連するサービスサイトと ID 連携することにより、ID ホルダーを中心とした「経済圏」を創出する。

図 21　ID 連携による経済圏創出のイメージ

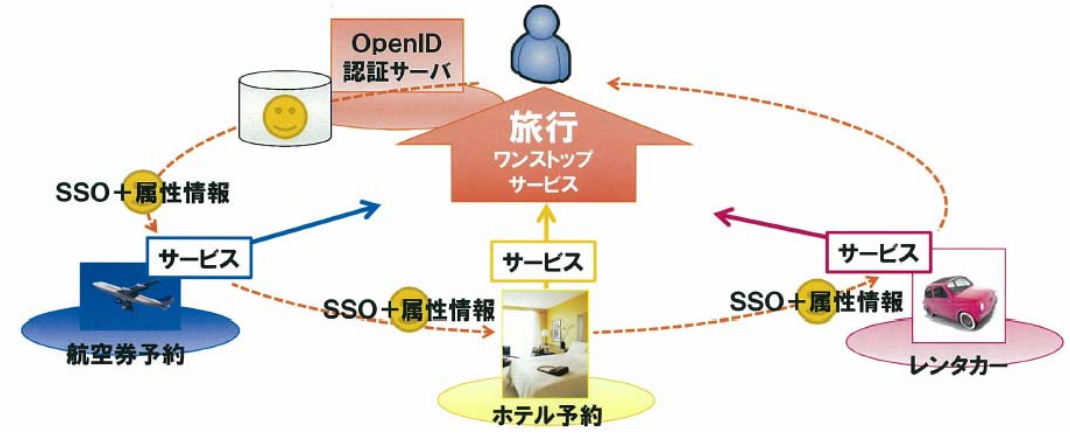


出典：OpenID ファウンデーション・ジャパン資料

② サービスのワンストップ化

連続的に利用することが想定されるサービスサイトを ID 連携することにより、利用者が 1 回の認証で一連のサービスを利用できるようにする。

図 22　ID 連携によるサービスのワンストップ化のイメージ



出典：OpenID ファウンデーション・ジャパン資料

（２）OASIS 国際標準化コンソーシアムにおける標準化に係る検討状況（SAML）

OASIS 国際標準化コンソーシアムは、数百の企業と数万人の個人により構成される国際的な非営利団体であり、SAML 等を含む数十の規格の策定・管理を行っている。主要スポンサー企業（foundational sponsor）として、IBM、Microsoft、Primeton、Sun が参画しており、選挙によって決定される理事（任期 2 年）は 2009 年 12 月現在、IBM、Microsoft、Sun、Nokia、Oracle 等のメンバーが務めている。

ア　SAML の概要

SAML はセキュリティ情報（認証、属性、認可）の交換のための XML 言語である。SAML の特徴は、大きく以下の 2 つである。

①　SSO （Single Sign-On）を実現

プロバイダ間でクッキーを共有せずに SSO を実現する。
ただし、end-to-end のクッキーの利用を制限するものではない（SAML 仕様範囲外）。

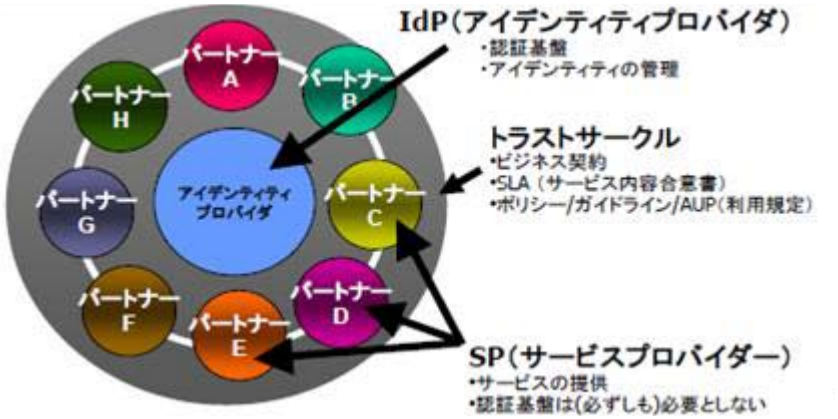
②　セキュリティ情報交換の枠組み

- 通常のブラウザの利用を想定している。
- PKI で導入することが可能である。
- Liberty ID-FF、WS-Security、XACML（eXtensible Access Control Markup Language）等で参照される。

イ　SAML による ID 連携

SAML は、利用者の情報を扱う 1 つの ID 発行事業者（IdP : Identity Provider）と複数のサービスプロバイダ（SP : Service Provider）との間のトラストサークルに基づいて ID 連携を実現する。

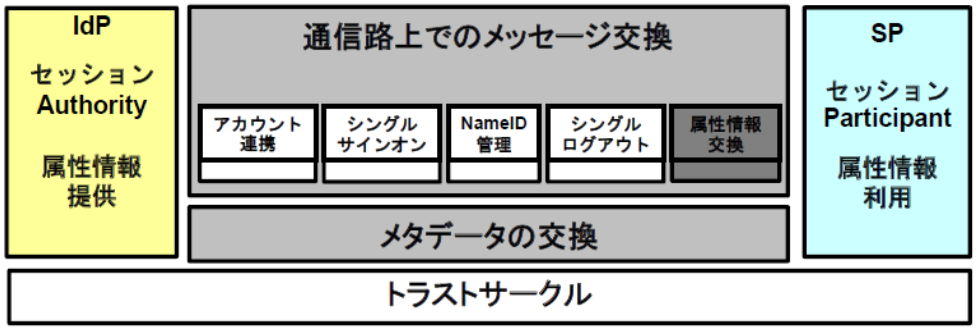
図 23　SAML による ID 連携の前提条件



出典：第一回 Liberty Alliance 技術セミナー資料

SAML による ID 連携は、ID 発行事業者とサービスプロバイダの信用に基づいてメッセージの交換が実施されており、ID 発行事業者は信用できるサービスプロバイダにのみ認証情報を発行し、サービスプロバイダは ID 発行事業者が発行する認証情報を信用することにより実現する。

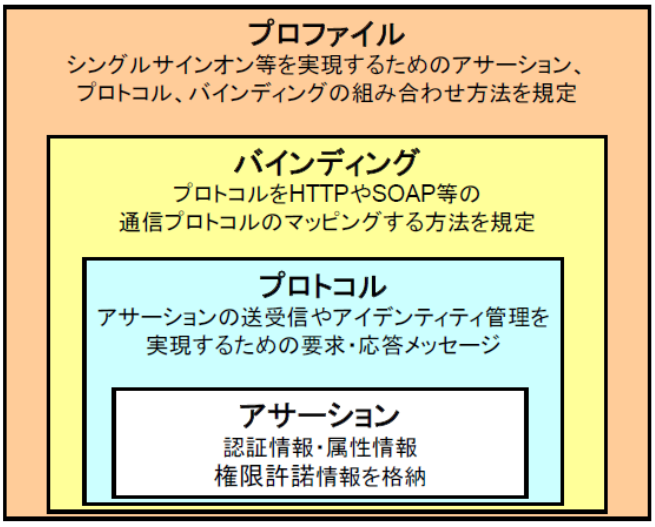
図 24　ID 連携のイメージ



出典：第一回 Liberty Alliance 技術セミナー資料

図 25　SAML における規定事項

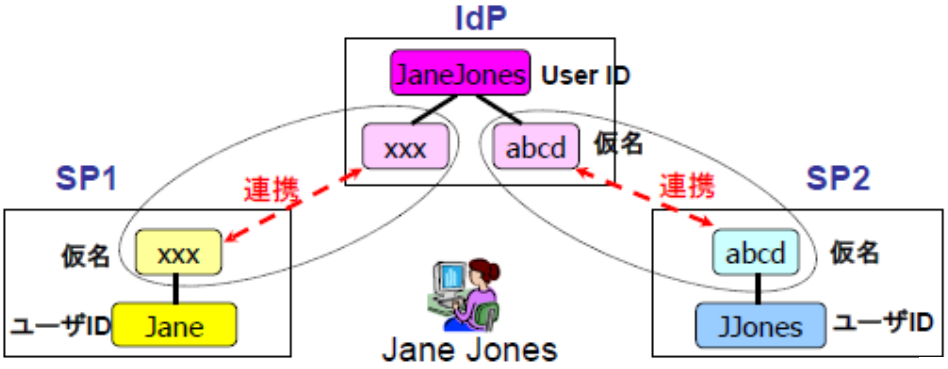
アサーション	・ アサーションの構造と内容を規定する ・ アサーションとは、ID 発行事業者が発行する証明書であり、ユーザー情報を記述
プロトコル	・ アサーションを要求する方法を規定する ・ プロトコルメッセージの XML スキーマを規定する
バインディング	・ SAML プロトコルメッセージを通信路（HTTP や SOAP など）に載せる方法を規定
プロファイル	・ SAML プロトコル、バインディングとアサーションを組み合わせる方法を規定 ・ Web ブラウザを利用したシングルサインオンプロファイル等を規定
メタデータ	・ シングルサインオンやログアウトを実行する方法を記述 ・ サービスのエンドポイントを記述



出典：第一回 Liberty Alliance 技術セミナー資料

それぞれのプロバイダが管理しているユーザーID 情報と ID 発行事業者のユーザーID 情報を関連付けることにより ID 連携を実現する。例えば、ID 発行事業者に登録したユーザーID の仮名を用いた利用者の識別ができる。このような方法により、プライバシー保護を考慮した認証・認可・属性情報の交換が可能となっている。

図 26　仮名による ID 連携のイメージ



出典：第一回 Liberty Alliance 技術セミナー資料

SAML（Open SAML[21]）を基に開発された認証システムとして、Internet2／MACE（Middleware Architecture Committee for Education）[22]が開発したShibboleth[23]がある[24]。Shibbolethでは、属性情報によりサービス提供してよいかどうかの判断を行うようになっており、欧米だけでなく、我が国でも学術認証フェデレーション（UPKI-Fed）[25]において採用されている。

ウ　OpenID と SAML との違い

インターネット上でシングル・サイン・オン（SSO）を実現する技術として、OpenID と SAML は類似しているが、その開発・発展経緯は異なり、結果として機能等に次のような相違がある。

---

[21] OpenSAML とは、米国の 300 以上の大学や企業、政府研究機関が参加する研究開発プロジェクトである Internet2 が開発したオープンソースの認証技術の仕様のことである。

[22] MACE は、Internet2 の教育機関向けプロジェクトである。

[23] Shibboleth は、Internet2／MACE のプロジェクト名でもある。

[24] 大谷誠、江藤博文、渡辺健次、只木進一、渡辺義明「ポータルサイトの強制表示とシングルサインオン」佐賀大学総合情報基盤センターの Web サイト <www.cc.saga-u.ac.jp/opengate/iot0905.pdf>参照。

[25] 学術認証フェデレーションとは、大学や出版社等で構成された連合体のことである。各機関は、学術認証フェデレーションが定めた規程（ポリシー）を信頼し合うことにより相互に認証連携を実現することができる。UPKI イニシアティブの Web ページ<https://upki-portal.nii.ac.jp/docs/fed>参照。

図 27　OpenID と SAML の相違点

	OpenID	SAML
開発経緯	個人が管理する ID 数の削減を目的に開発。	エンタープライズ・システムを超えた SSO の実現のため、標準化した技術として開発。
対象領域	利用者（ID 所有者）の確認（Authentication）が対象。アクセス制御等の権限確認（Authorization）は対象外。	利用者（ID の所有者）の確認（Authentication）、権限確認（Authorization）双方を対象。
ID 連携	Web サイト同士の信頼関係に関係なく ID 連携を実現。	相互に信頼関係を結んだ Web サイト同士でのみ ID 連携を実現。

出典：三菱総合研究所

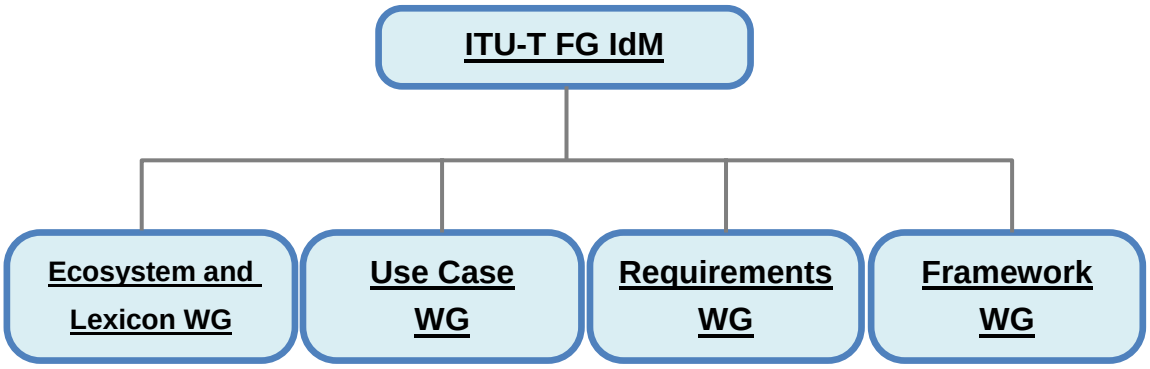
（3）ITU-T における標準化に係る検討状況

ア　FG-Idm（Focus Group on Identity Management）

ITU-T では、まず SG17 配下に設置された FG-IdM において、ID 管理に係る標準化の検討が行われた。FG-IdM は 2006 年 12 月から 2007 年 9 月まで、ID 管理（IdM：Identity Management）全般について集中的に審議を行う組織として設置された。

FG-IdM には 4 つの WG が設置された。

図 28　ITU-T FG-IdM の構成

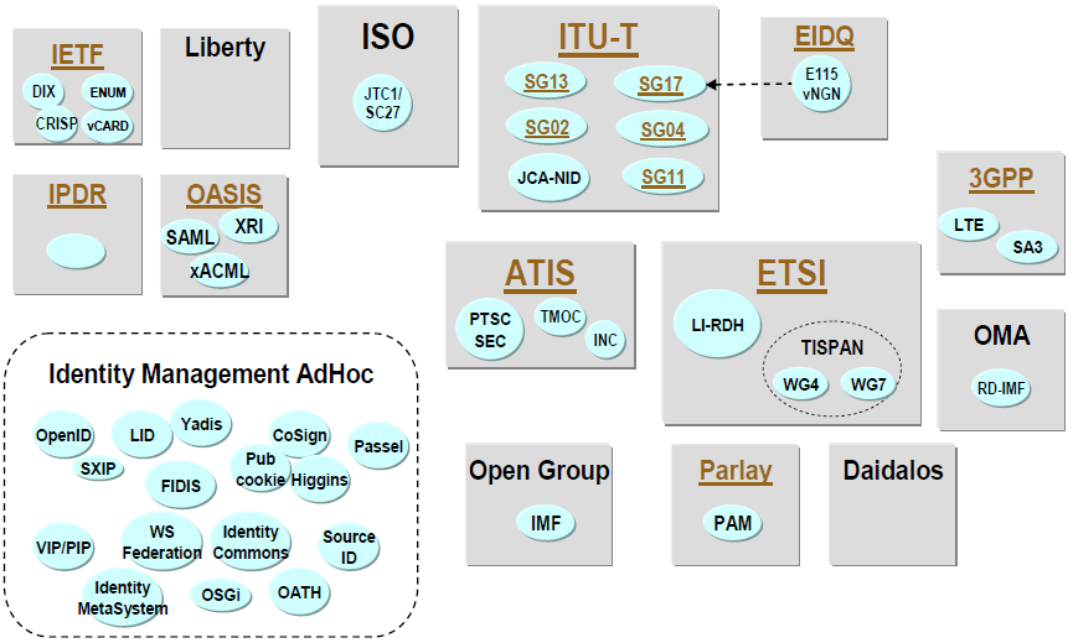


出典：三菱総合研究所

①　用語 WG（Ecosystem and Lexicon Working Group）

用語の定義及び他の ID 管理関連団体（26 団体）との関係整理を行った。

図 29　ID 管理関連団体



出典：NPO 日本ネットワークセキュリティ協会　Network Security Forum 2008 資料

②　ユースケース WG（Use Case Working Group）

ID 管理に係る必要なユースケースとして、以下の観点から分析を行った。

- ID 情報の信頼できる開示及び交換のためのメカニズム並びに品質保証の開発と活用
- 主体の証明・識別・情報の属性及び関連付け・ID パターンの管理
- 承認権限管理者・ID 発行者及び ID 発行者団体間の相互運用性
- ID 管理機能に関連した脅威及びリスク（機密性、完全性、有効性）、並びにリスクの低減方法

③ リクワイアメント WG（Requirements Working Group）

利用事例に基づいた要求事項の整理及びプライバシーを含む法令による制限等の調査、ID 管理業務の現状と要求事項との差の識別を行った。

- 各種 ID 管理に共通なリクワイアメントの整理
  前提とするアーキテクチャモデル、プロビジョニング[26]、ディスカバリ、ID発行・認証者間やID発行・認証者の連携先間での相互運用性、監査、脅威とリスクの軽減、パフォーマンス、信頼性、可用性

- 要求条件を実現する上で現在欠けているソリューションの整理
  共通的な ID 管理アーキテクチャモデルと ID 管理レイヤ、グローバルな開示、グローバルな ID サービスの相互運用性、グローバルな ID 保証（identity assurance）の相互運用性、透明性と通知、オブジェクト管理との統合、異なる法制度間での要求事項の違いの調停

④ フレームワーク WG（Framework Working Group）

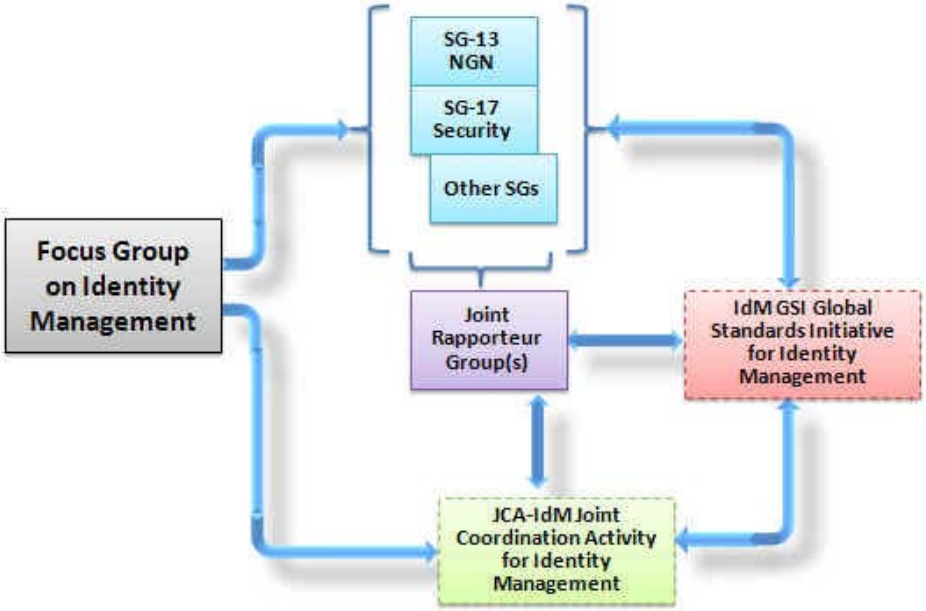
利用事例の検討から導かれた要求事項に適合したアーキテクチャの検討を行った。具体的には、グローバル ID 管理フレームワークに関する主要な構成要素の機能ブロック図を作成した。

イ JCA-IdM（Joint Coordination Activity on Identity Management）

[26] プロビジョニングとは、利用者が利用したい時に利用できるようにしておくことをいう。

FG-IdM の成果を受けて、2007 年 12 月に JCA-IdM の設置が承認され、継続的に ID 管理に係る検討が行なわれることとなった。JCA-IdM の 2009-2012 研究期間の活動は、2009 年 4 月より開始されている。

図 30　JCA-IdM 及び FG-IdM 等の検討グループの関係



出典：ITU-T の Web サイト
<http://www.ituwiki.com/Focus_Group_on_Identity_Management>

（4）EU における標準化に係る検討状況（eID）

EUにおけるeIDの標準化は、2006 年に発表されたi2010 eGovernment アクション・プラン[27]における 5 項目の優先課題の一つであるEU域内での相互利用性（interoperability）に準拠したEU内における電子政府サービスの拡大に不可欠なものとなっている。

EU では、各国で整備されている eID の共通利用及び新しい eID の共通仕様の作成に向けて、様々な調査、実験を実施している。

そのような取組の一つとしてパイロットプロジェクト「STORK（Secure idenTity acrOss boRders linKed）」（3 年間、予算 2000 万ユーロ（約 26 億円））が 2008 年より実施されている。

[27] Commision of the European Communities, “i2010 eGovernment Action Plan: Acceleration eGovernment in Europe for Benefit of All,” April 25, 2006.

ア　STORK の目標及び実施概要

欧州では、国境を越えて通勤することや、近隣国に居住することは珍しくなく、そのため、仕事中や日常生活の中で公共サービスを利用することが容易でない場合がある。そこで、eID を他国でも認証できる EU ワイドなシステムとすることによりこれらの課題を解決すれば、ビジネス及び日常生活において安全に EU 内ならばどこでも eID を利用できる環境を整備することができる。

このように、STORK プロジェクトの目標は、EU 全域において eID の認証を可能とすることである。当プロジェクトでは、以下の 5 つの試験が実施される。

Pilot 1：越境での ID 認証プラットフォーム
Pilot 2：Safer Chat – 子供や少年によるより安全なインターネットの利用促進
Pilot 3：EU 内の他国の大学に通う学生の支援
Pilot4：越境でのオンラインによるセキュアな文書電送
Pilot5：EU 内での市民の住所変更の支援

イ　STORK の成果への期待

STORK プロジェクトでは、各国の eID システムを連携させるための共通仕様の作成、試験及び確認が実施される。当プロジェクトにより作成される共通仕様は、プロジェクトに参加しない国も含めた全 EU 加盟国に照会されるため、EU 全域に影響力を持つものになることが期待されている。

また、作成された共通仕様は、将来において eID を活用したサービスを開発しようとするすべての業界に対して公開される。参考資料、ガイドライン、マニュアル及び教育用マニュアルも作成される予定である。

このような実験的なプロジェクトの成果を通じて、EU 全域で、利用の多いいくつかの公共サービスが国境を越えて円滑に利用できるようになることが期待されている。

終章　ID ビジネスの健全な発展に向けて

終章　ID ビジネスの健全な発展に向けて

最後に、前章までの調査研究結果を踏まえ、ID ビジネスが健全に発展するために、政府が取り組むべき方向性、民間事業者が目指すべき方向性、そして、利用者が留意すべき事項を整理して、本稿を終えることにする。

今後、ID ビジネスの更なる発展のための情報通信政策の企画、立案に当たり、少しでも参考になることを期待したい。

1　政府が取り組むべき方向性

○　各種ガイドライン等を整備し、利用者保護・事業者支援

電子商取引や個人情報保護に関しては既にガイドライン等が存在するが、今後、ID 連携がますます行われるようになると、ID 連携に当たり各当事者が留意すべき点や ID 連携による競争政策上の問題などについて検討していく必要が生じるではないかと思われる。

ID の発行・認証、他社が発行する ID の利用、それに伴い取得する利用者の情報の取扱等について、既存の法令では規制が困難な部分をガイドライン等で定めることにより利用者の保護及び事業者の負担の軽減を図ることは、ID ビジネスの発展にとって重要であると考えられる。

なお、そのようなガイドライン等は、既に事業として軌道に乗っている分野の事業者に過度の負担をかけるものであってはならないことはいうまでもない。

○　ID 連携関連技術の標準化を支援・促進

ID の連携に当たっては、それに係る技術の標準化は重要である。SAML、OpenID など民間主導での取組のほか、諸外国では、例えば、欧州では、EU が中心となって域内での eID の共通利用に積極的に取り組もうとしている。

我が国においても、ID 関連技術の標準化を適切に進めるためには、民間事業者による取組だけでなく、政府による支援や促進（例：公的な分野での標準となる技術の採用等）も重要であると考えられる。また、国際的な標準化の取組に対し、政府としても積極的に貢献していくべきであると考えられる。

○　官民で共用可能な ID 基盤の必要性について検討

諸外国においては、政府が認証基盤を構築した上で、政府だけでなく民間事業者もこれを利用している事例がある。我が国においても、このような方式が効果的であるのか、標準化の推進も考慮して、検討することは有意義であると考えられる。

ただし、「官民連携」ありきではなく、あくまでも利用者の利便性向上、不安解消、という側面から検討することが重要である。諸外国には、統一されたIDを付与している例もある一方、各IDをひも付けて利用者の利便性を向上している例もある。統一されたIDの場合、プライバシー保護の問題や不正利用などによる被害の拡大も懸念されるが、利用者が適宜変更できるようにしたり、あるいは、利用者がいくつかのIDから主として用いるものを自ら選択してその他のIDにひも付けたりするなど、利用者保護に留意することはもちろんのこと、利用者本位の仕組みを検討することが大切である。

なお、国民が不必要に不安を感じたりすることがないようにするとともに、政府が安心・安全なシステムを構築し、国民すべてがICT利用の利益を享受できるよう国民意識を啓発していくことも重要であると思われる。

○　集客力のある事業者同士の「大きなID連携」に向けた支援

集客力のある事業者は既に多くの顧客を有しており、そのような事業者同士がIDを連携することは、経営戦略として採りがたいと考えられる。そのため、集客力のある事業者とそうでない事業者とのID連携は進む一方で、集客力のある事業者同士のID連携は進まない状況が生じる可能性が想定される。

ID連携は、あくまでも事業者の経営戦略によるのであるが、“せめぎあい”状況を打破するためには、必要に応じて政府が支援することも重要であると考えられる。分野横断的、かつ中期的な視点に立って、国民の利便性向上という意味からも「大きなID連携」をコーディネートしていくことは政府の重要な役割の一つではなかろうか。

○　IDの不正取得等への対策

ID連携の進展により、ユーザー登録は比較的容易だが利用価値が高いIDについては、不正取得や不正使用の問題が出てきている。IDの不正使用については、不正アクセス禁止法の対象になると考えられるが、IDの不正取得については、例えば、IDの窃盗それ自体を直接的に規制する法令は存在しない上、IDの取引自体を規制する法令も存在しない。

したがって、このような場合における法制度の整備も含めた対策を進めてい

く必要があると考えられる。例えば、ID／パスワードを「情報」として価値を有するものとして管理できるような制度は考えられないであろうか。

2　民間事業者が目指すべき方向性

○　サービスや情報管理等への信頼を獲得・維持

ID を用いて提供するサービス自体への信頼、また、ユーザー登録やサービスの利用に当たり取得する個人情報等の利用・管理に対する信頼を利用者から得ることが、ID ビジネスが成立する大前提である。

特に、ID を連携する場合、利便性よりも、連携元となる Web サイトの運営者と連携先の Web サイトの運営者の信頼性が重視されることになる。ID 連携を成立させ、維持していくためには、それにより提供されるサービスの信頼性を高めるだけでなく、ID 連携に当たり事業者間で情報を共有、提供する場合、個人情報等の利用や管理に対し、利用者からの信頼を獲得し、維持していくことが重要であると考えられる。

本調査研究のために実施した利用者へのアンケート調査の結果によると、利用者の信頼を得るためには、Web サイトの運営者の情報を十分に開示するとともに、ユーザー登録の解除方法が明示されていることなどが必要とされている。また、利用者から取得する情報を他の事業者に提供する場合には、利用規約等に記載するだけでなく、より分かりやすい説明が求めている。

○　利用者の不安と不便を解消したサービスの提供

本調査研究のために実施した利用者へのアンケート調査の結果によると、ユーザー登録する際に、当該 Web サイトに関する情報を収集するだけでなく、ユーザー登録すると、情報が流出したり、迷惑メールが送付されてきたりすることを心配し、必須項目以外は登録しないようにしたり、フリーメールのアドレスを使っていつでもメールアドレスを変更できるようにしたりしているようである。

中長期的には、ID ビジネスの裾野を更に拡大し、事業機会を増大させるためには、このような利用者の不安感を取り除き、かつ、利用者の ID／パスワードの利用・管理における不便を解消するようなサービスを実現・提供していくことが大切である。

そのためには、ID 連携関連技術の標準化への取組に貢献したり、実際に、他の事業者との ID 連携を検討したりするなど、ID 連携について、前向きに

考えていくことが大切であると考えられる。

○　ID 連携に関する各種データや評価に関する仕組みの整備

本調査研究のために実施した利用者へのアンケート調査の結果によると、ID 連携においては、連携元となる事業者への信頼が重要であると同時に、連携先がどのような事業者であり、どのような情報が、どのようにその事業者に提供され、そして、どのように利用されるのかを気にしている利用者が多かった。

それらについて、利用者がユーザー登録や利用に当たり、参考にできるような仕組み、例えば、ID 連携する事業者が、どの事業者と連携し、どのような情報を、どのように提供し、どのように利用するのか、を登録したり、ID 連携したサービスの利用者がそのサービス内容はもとより、サービスを提供している事業者を評価にしたりするような仕組みを、関係する事業者間で整備できると望ましい。

○　事業者間の利害関係を克服した「大きな ID 連携」

「政府が取り組むべき方向性」でも説明したが、集客力のある事業者は既に多くの顧客を有しており、そのような事業者同士が ID を連携することは、経営戦略として採りがたいと考えられる。そのため、集客力のある事業者とそうでない事業者との ID 連携は進む一方で、集客力のある事業者同士の ID 連携は進まない状況が生じる可能性が想定される。

例えば、国内におけるそのようなある種の“せめぎあい”の状況において、ID を用いてサービスを提供する他国の更に大きな事業者が国内に進出してきた場合には、当該事業者が発行・認証する ID に一元化（併合）されてしまうという可能性も考えられ、各事業者だけでなく、最終的には、利用者の不利益につながる可能性も考えられる。

そのような事態を避けるためには、競争があまり激化していない現在から、集客力のある事業者同士が「大きな ID 連携」の意義や可能性について検討することは、有意義かつ重要であると考えられる。

3　利用者が留意すべき事項

○　ID 利用についての知識を身に付け、注意深く利用

本調査研究のために実施した利用者へのアンケート調査の結果によると、同じ ID／パスワードを利用している利用者も多い（回答者の 4 割強）。このような管理方法は、フィッシングサイト等で ID／パスワードを詐取されると、他の登録サイトへも不正に侵入、利用され、被害の拡大を招く可能性があるので注意を要する。

一人ひとりの利用者が、ID を利用する上で必要最小限の知識を身に付けた上で、利用規約、個人情報保護方針やプライバシーポリシー等を十分確認し、自分及び他人の個人情報を適切に扱うようにすること（例：安易に情報を提供しない等）が大切である。

○　事業者を評価し、健全な発展に寄与

本調査研究のために実施した利用者へのアンケート調査の結果によると、ユーザー登録に当たり、クチコミサイト等を参考にして、当該 Web サイトに関する情報を収集している者も多い。

サービスの質が低い事業者や不正なことを考えている事業者のサービスは、（新しい手口に対して後追いにならざるを得ないときもある）法制度等により防止・排除するだけでなく、利用者自らが、市場において淘汰していくことも重要である。それによって、ID サービスの健全な発展がよりいっそう可能になると考える。

○　不正行為に加担しない

ID を用いた犯罪の多くは、ID の不正な取得等によって成立していると考えられる。利用者が、軽い気持ちでこうした行為に加担したり、こうした行為が犯罪を招くことを知らずに加担したりしている場合もあると想定される。

ID サービスを健全に利用できるようにするためにも、利用者一人ひとりが、ID の不正取得や売買・譲渡等、不正行為に加担しないようにすることが重要である。

【補論】我が国における電子認証局の現状

第４章２（３）でみたように、韓国ではPKI認証の利用が普及している。そこで、代表的な民間電子認証局へのヒアリング調査を実施した結果も踏まえ、我が国におけるPKI認証の状況についても述べることとする。

電子認証局とは、「電子の印鑑に相当する」電子証明書を発行し、その電子証明書が間違いなく本人のものであることを保証するサービスを行っている機関である。現在、電子認証サービスの中核を担っているのは、民間の電子認証局である。電子認証局は、電子証明書の利用範囲により、「パブリック認証局」と「プライベート認証局」に分けられる。前者は、電子証明書の利用者が一般社会に及び、後者は特定組織内（例えば企業内、学内など）に閉じている。

これまで、民間に向けた電子認証サービスを実施しているのはパブリック認証局だけであったが、本年より新たな民間電子認証環境の構築のため、プライベート認証局の活用についても、財団法人日本情報処理開発協会（JIPDEC）において検討が始まっている。

なお、各電子認証局は、その運用方式、信頼性、安全性をサービス利用者等に示すため、CP（Certificate Policy）及びCPS（Certification Practice Statement）という文書を定めている。

- CP（Certificate Policy）
  電子認証局が電子証明書を発行する際の運用方針を定めた運用ポリシー
- CPS（Certification Practice Statement）
  電子認証局の運用方針の実施手順を定めた運用規程書

（１）パブリック認証局

パブリック認証局は、その信頼性が広く社会に受け入れられている点が大きな特徴である。国の認定する特定認定認証局や法務省が運営する商業登記認証局、公的個人認証局、及び一般的なインターネットブラウザ（Internet Explorerなど）にあらかじめ組み込まれている「信頼されたルート認証局」から証明書の発行を受けた認証局など、複数が存在する。基本的に、CP／CPSが公開されており、相手方の電子証明書が提示された場合には、そのCP／CPSの内容を確認し、信頼できるものかを判断することが可能となるため、見知らぬ相手とのやり取りを行う場合に有効である。信頼された認証

局としてブラウザに組み込まれるためには、一定の基準を満たす必要があるなど、パブリック認証局は客観的な審査基準による外部監査を受けている場合もあり、このような証明書の信頼性は高くなる。

（2）特定認定認証局

パブリック認証局の中でも特定認定認証局は、電子署名及び認証業務に関する法律（平成 12 年法律第 102 号。以下「電子署名法」という。）に基づいて認定を受けた認証サービス（特定認証業務）を提供する認証局であり、電子証明書を発行するために個人ユーザーを登録する登録局のサービス業務が主な対象となる。

認定を受けるための審査基準は、個人ユーザーを原則として対面で認証すること、十分な安全性を持った発行システムを運用していること等であるが、一度認定を受けると、認定基準を満たすかどうかの定期的な立ち入り審査を受ける必要がある。したがって、認定を維持するためには継続的な費用負担が発生する。また、認定を受けても法的効力の優位性は得られないこともあり、ビジネスとしての展開に苦慮している。

以下は、2009 年 9 月 4 日現在で登録されている特定認証業務である。

表　特定認証業務及び事業者名等（2009 年 9 月 4 日現在）

特定認証業務の名称	業務を行う者の名称	認 定 日
Accredited Sign パブリックサービス 2	日本認証サービス株式会社	平成 13 年 10 月 19 日
株式会社日本電子公証機構認証サービス iPROVE	株式会社日本電子公証機構	平成 13 年 12 月 14 日
CECSIGN 認証サービス	株式会社コンストラクション・イーシー・ドットコム	平成 14 年 3 月 26 日
セコムパスポート for G-ID	セコムトラストシステムズ株式会社	平成 14 年 7 月 4 日
AOSign サービス	日本電子認証株式会社	平成 14 年 8 月 29 日
e-Probatio PS サービス	株式会社 NTT アプリエ	平成 14 年 11 月 20 日
TOiNX 電子入札対応認証サービス	東北インフォメーション・システムズ株式会社	平成 14 年 12 月 10 日
TDB 電子認証サービス TypeA	株式会社帝国データバンク	平成 15 年 2 月 5 日
ビジネス認証サービスタイプ 1	日本商工会議所	平成 15 年 3 月 12 日
電子入札コアシステム用電子認証サービス	ジャパンネット株式会社	平成 15 年 4 月 21 日
全国社会保険労務士会連合会認証サービス	全国社会保険労務士会連合会	平成 15 年 6 月 10 日
CTI 電子入札・申請届出対応　電子認証サービス	株式会社中電シーティーアイ	平成 15 年 9 月 29 日
よんでん電子入札対応認証サービス	四国電力株式会社	平成 15 年 10 月 2 日
税理士証明書発行サービス	日本税理士会連合会	平成 16 年 1 月 16 日
e-Probatio PS2 サービス	株式会社 NTT アプリエ	平成 17 年 11 月 9 日
日本土地家屋調査士会連合会認証サービス	日本土地家屋調査士会連合会	平成 17 年 12 月 9 日
MJS 電子証明書サービス	株式会社ミクロ情報サービス	平成 18 年 3 月 31 日
司法書士認証サービス	日本司法書士会連合会	平成 19 年 9 月 21 日
NTT ドコモ電子証明書サービス	株式会社エヌ・ティ・ティ・ドコモ	平成 20 年 9 月 3 日

出典：経済産業省資料

現在登録されているのは、19 業務 18 局である。電力系 3 局、士業系 4 局などが多いが、NTT アプリエを除き、1 局 1 業務である。認定取得のための投資に対し、ビジネスが伸びていないことも原因と考えられる。

特定認定認証局の電子証明書発行枚数は、シェアトップクラスの認証局で累計 18 万枚余（2009 年 10 月現在）である。まだ GtoB（政府と企業間）、BtoB（企業間）での電子証明書の需要は少なく、採算ベースに乗らない認証局が大半である。

また、ICT 初心者の利用者が大半であるため、初歩的な問い合わせが多い。本来であれば、電子証明書の発行後のユーザーサポート費用は保守費と

して徴求すべきであろうが、18 局という過当競争下において、電子証明書発行後の保守費を徴求できる市場情勢にない。

なお、電子署名法は自然人の認証を対象としているが、実態上は組織等に所属する自然人の認証というモデルが大半であり、そういった意味において、認証の対象は、自然人ではなく実体上は法人としての側面を持っている。しかしながら、自然人として属性 4 情報をさらして通信する習慣は GtoC（政府と利用者間）以外に根付いていない。そして、GtoC は公的個人認証の範疇であり、コスト比較的に民間認証局の立ち入る余地はない。GtoB、GtoC においては、認定認証局、公的個人認証局、商業登記認証局の 3 タイプの電子証明書と、国の GPKI（政府認証基盤 : Government Key Infrastructure。地方自治体は LGPKI（地方公共団体組織認証基盤 : Local Government Key Infrastructure））の電子証明書によって官製のアプリケーションが動作しており、BtoB よりむしろ政府が牽引しているのが現状である。

また、用途が GtoB の電子入札対応が多く、電子入札の普及と公共工事の減少から、電子証明書の発行が飽和状態になりつつある。そこで、今後の用途として期待されるのが BtoB や BtoC、CtoC（利用者間）の電子契約関連市場である。電子署名法の施行前後からインターネット取引・EC（電子商取引）というかけ声のもと、簡易な物品購入サイト等の売買契約サイトやオークションサイト、あるいは、BtoB 請負契約・受発注システム等の ASP（Application Service Provider）契約サイトが運営されている。しかしながら、比較的安価な契約である BtoC、CtoC では、コストや手間の問題から必ずしも電子署名の導入はなく、本人確認に ID／パスワードという形態が依然として目立つ。

さらに、金額の大きなBtoB請負契約についても、電子証明書は、電子署名法の認定認証局の発行による場合と、認定外の認証局による場合とが混在しており、ほとんど普及には至っていない。当事者や悪意の第三者による改ざん・なりすまし措置が行われた場合の法律的効果の違いは、ほとんど想定されていない。これらは、IT書面一括法 [28]に基づき紙の契約を電子化した場合の電子証明書の運用基準やe-文書法 [29]、電子帳簿保存法 [30]改正に伴う国税

---

28 書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律（平成 12 年法律第 126 号）の略称。

29 「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成 16 年法律第 149 号）と「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」（平成 16 年法律第 150 号）の総称。

30 電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関す

の対応等について、法令間の横の連携を勘案した明確な電子契約の「業務プロセス運用標準」がないことに起因するものとも考えられる。

しかし、最大の理由は、紙社会における人間ベースの融通性が電子社会には適さないことへの認識が低く、電子証明書の有用な活用方法がいまだに浸透していないことにあると考えられる。したがって、民間電子認証局のビジネスモデルについては、大きな変革が訪れないと極めて厳しい経営環境にあるといえる。

（3）新しい民間認証環境の検討

今後に向けた新しい試みとして、本年度より JIPDEC において、プライベート認証局（主として企業内認証局）を活用した民間電子認証環境の検討が開始された。体制としては、有識者委員会（委員長：佐々木良一東京電機大学教授）のもとに以下の 3 検討部会（ビジネスモデル検討部会、ポリシー/基盤システム検討部会、評価基準検討部会）が組織され、その助言を得て JIPDEC がプロジェクトを推進している。

現在、大手企業においてプライベート認証局が設立され、社員証としての電子証明書が普及しつつある。事務所への入退室や、社内システムへのアクセス時の認証に活用されるだけでなく、社内メールや社内保存文書への署名に活用している企業もある。設備が必要な登録業務は、専門の電子認証事業者に委託することで初期投資を削減し、機密保持が要求される登録業務のみ社内で行うことにより、高効率・低コストを実現している。もちろん特定認定認証局のような認定のためのコストも発生せず、証明書記載項目の設定が自由に行えるため、さまざまな用途に使いやすくなる。

このようなプライベート認証局の長所を活かし、これらを連携させて新しい付加価値と利用シーンを創造しようとする企画が「民間電子認証環境」である。具体的には、各企業が発行する社員証としての電子証明書を「ビジネスパス（多目的社員証）」として共通化し、かつ企業内認証局の有効性検証を支える基盤の構築・運用が検討されている。

利用シーンとしては、有効な取引情報として扱える電子署名付き電子メール／電子文書が挙げられる。企業内認証局から発行され、その有効性を検証できる電子署名付き電子メール／電子文書で情報交換を行うことにより、当該企業において作成されたビジネス文書として扱うことが確認され、電子メールのフィッシング対策としても有効である。

る法律（平成 10 年法律第 25 号）の略称。

実運用に合った電子証明書共通化の仕組みにおいては、国や企業を特定する情報が必要となる。しかし、部門名、肩書き、電話番号等の変更頻度の高い情報については外出しし、属性情報の URL 等で管理することで連携コストを削減することが可能である。また、媒体についても媒体フリーや集約化等が検討されている。

（参考文献）

行政情報システム研究所『行政サービス向上のための個人コードのあり方に関する調査研究報告書』
<http://nippon.zaidan.info/seikabutsu/1997/00604/mokuji.htm>
国際社会経済研究所監修『国民 ID　導入に向けた取り組み』（NTT 出版、2009 年）
自治体国際化協会編『各国の電子自治体の推進状況』（自治体国際化協会、2006 年）
情報処理推進機構『情報セキュリティ白書　2008』（実教出版、2008 年）
情報処理推進機構『OSS によって構築可能な認証基盤構成技術の現状と事例調査』（2008 年 2 月）
<http://www.ipa.go.jp/software/open/ossc/download/PKI_Research.pdf>
高橋和之、松井茂記編『インターネットと法〔第 3 版〕』（有斐閣、2004 年）
高橋健司「アイデンティティ管理の現状と今後」『電子情報通信学会誌』92 巻 4 号（2009 年 4 月）
露木康浩、砂田務、檜垣重臣「不正アクセス行為の禁止等に関する法律の解説」警察大学校編『警察學論集』第 52 巻第 11 号（立花書房、1999 年 11 月 10 日）28-61 頁
東京弁護士会インターネット法律研究部編『Q&A　インターネットの法的論点と実務対応』（ぎょうせい、2005 年）
野村総合研究所 ID ビジネスプロジェクトチーム『2015 年の ID ビジネス』（東洋経済新報社、2009 年）
不正アクセス対策法制研究会編『逐条　不正アクセス行為の禁止等に関する法律〔補訂〕』（立花書房、2001 年）

＜参考資料＞

公的個人認証サービス普及拡大検討会「中間取りまとめ」（2009 年 8 月 12 日）
<http://www.soumu.go.jp/main_sosiki/kenkyu/kojin_kakudai/index.html>
次世代電子行政サービス基盤等検討プロジェクトチーム「中間報告書」（2009 年 12 月 21 日）<http://www.kantei.go.jp/jp/singi/it2/nextg/index.html>
社会保障カード（仮称）の在り方に関する検討会「社会保障カード（仮称）の基本的な構想に関する報告書」（2008 年 1 月 25 日）
<http://www.mhlw.go.jp/shingi/2008/01/s0125-5.html>
社会保障カード（仮称）の在り方に関する検討会「社会保障カード（仮称）の基本的な計画に関する報告書」（2009 年 4 月 30 日）

<http://www.mhlw.go.jp/shingi/2009/04/s0430-4.html>
通信プラットフォーム研究会「プラットフォームの在り方」(2009 年 1 月 30 日)
<http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/platform/index.html>
電子私書箱 (仮称) 構想の実現に向けた基盤整備に関する検討会「報告書」(2009 年 3 月 31 日) <http://www.kantei.go.jp/jp/singi/it2/epo-box2/index.html>
電子私書箱 (仮称) による社会保障サービス等の IT 化に関する検討会「報告書」(2008 年 3 月 17 日) <http://www.kantei.go.jp/jp/singi/it2/epo-box/index.html>

オーストリア

Austrian Federal Chancellery, ICT Strategy Unit, "Administration on the NET / The ABC guide of eGovernment in Austria," July 2008.
<http://www.epractice.eu/files/media/media2208.pdf>

韓国

瑞草区 (園田寿訳)「韓国の住民登録制度」
<http://sonoda.e-jurist.net/korea/siryou/seocho.htm>

ベルギー

Danny De Cock, Christopher Wolf, and Bart Preneel, "The Belgian Electronic Identity Card (Overview)," 2006.
<http://www.cosic.esat.kuleuven.be/publications/article-769.pdf>
fedict, "The Electronic Identity Card (EID) Developers Guide."
<http://eid.belgium.be/nl/binaries/eID_Developers_Guide_tcm147-63130.pdf>
Frank Robben, National Office for Social Security, "Belgian Social Security."
<http://unpan1.un.org/intradoc/groups/public/documents/other/unpan022035.pdf >
gemalto, "Belgium- the national eID Card."
<http://www.gemalto.com/brochures/download/belgium.pdf>
IDABC "Study on Mutual Recognition of eSignatures: update of Country Profiles Belgian country profile," July 2009.
<http://ec.europa.eu/idabc/servlets/Doc?id=32321>
"Advanced Applications for e-ID Flanders," April 2006.
<https://www.cosic.esat.kuleuven.be/adapid/docs/adapid-d2.pdf>
"Crossroad Bank for Social Security," (4th Ministerial eGovernment Conference). <http://www.ksz.fgov.be/En/CBSS.htm>
adapID project の Web サイト<http://www.cosic.esat.kuleuven.be/adapid/>

参　考

○　利用者に対するアンケート調査の結果

利用者におけるID利用の現状、IDビジネス利用に当たっての懸念及びID連携に対する期待等について把握するため、利用者に対するアンケート調査を実施した。インターネットにおけるサービスの利用状況やIDの利用に関する調査であるため、ウェブアンケートにて実施することにした[31]。

1　アンケート調査の概要

アンケート調査の概要は、以下のとおりである。

- 調査期間　：2009 年 12 月 18 日（金）～20 日（日）
- 調査方法　：ウェブアンケート調査（調査票は＜別添＞として添付）
- 対象者　　：全国の 20 歳以上のインターネット利用者
- 収集回答数：

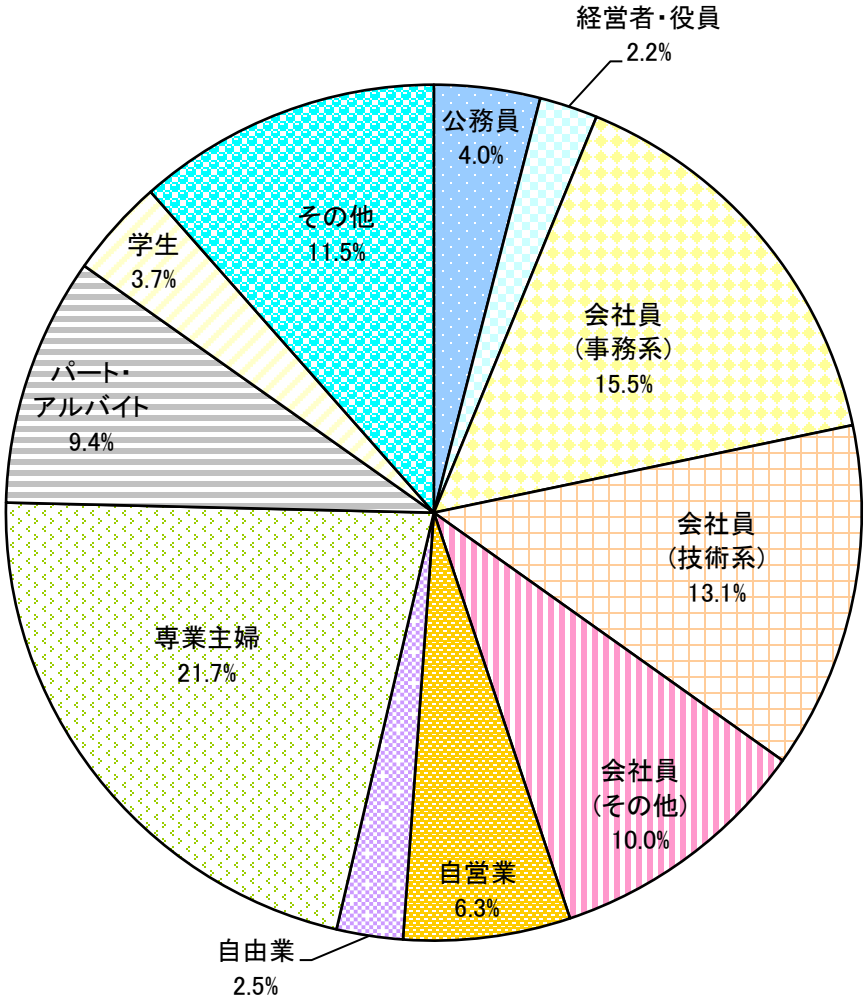
	男性	女性	合　計
20-29 才	103	103	206
30-39 才	103	103	206
40-49 才	103	103	206
50-59 才	103	103	206
60-才	103	103	206
合　計	515	515	1,030

[31] 集計結果について、ウェッブアンケートであるので、インターネット利用者の年齢別割合などにより調整することも考えられるが、調整に当たり参考とするアンケート調査時点のインターネット利用状況に関する資料がいまだ不足していたことから、調整はしなかった。

2　回答者の概要

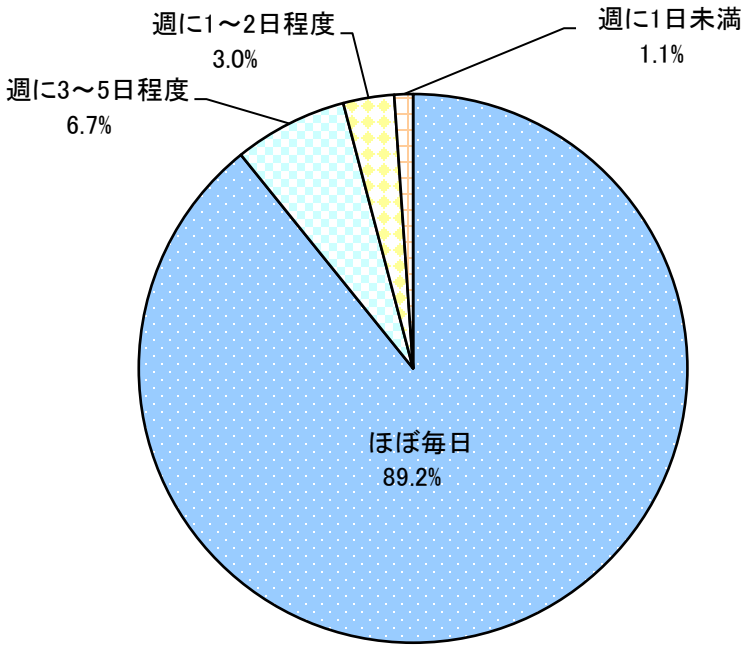
アンケートの回答者の概要は、以下のとおりである。

・　回答者の約 39%が会社員、約 22%が専業主婦である。

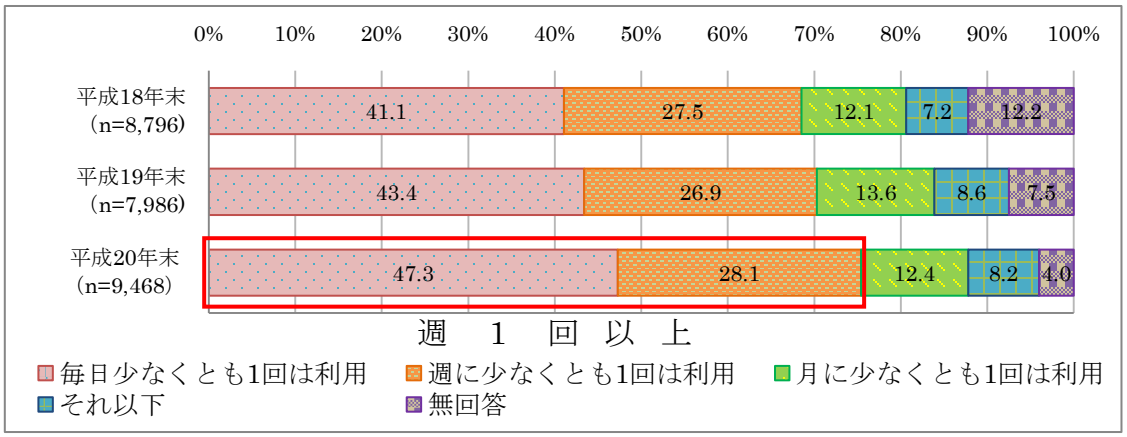


・　回答者の約 90%が「ほぼ毎日」インターネットを利用しており、「週に 3～5 日程度」と合わせると、約 95%以上が週に 3 日以上インターネットを利用している。
・　なお、「平成 20 年通信利用動向調査（世帯編）」では、「週に少なくとも 1 回は利用」又は「毎日少なくとも 1 回は利用」と回答した者の合計が 75.4%となっており、今回のアンケートの回答者は、インターネットの利用頻度が比較的高い利用者と考えられる。

[Q1]あなたはインターネットのウェブサイトを
1週間にどれくらいの頻度で利用しますか？(ひとつだけ)
(n=1,030)



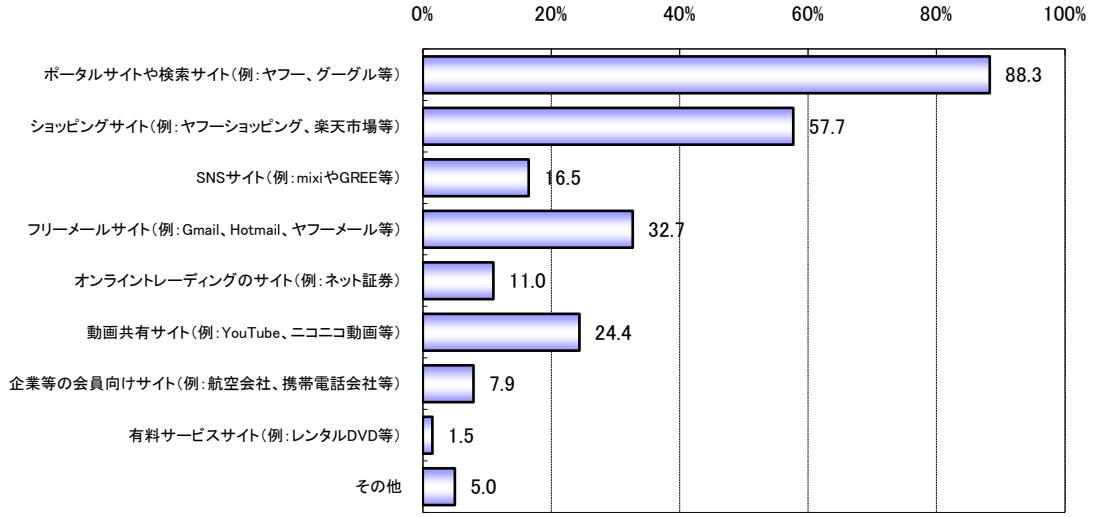
【参考】

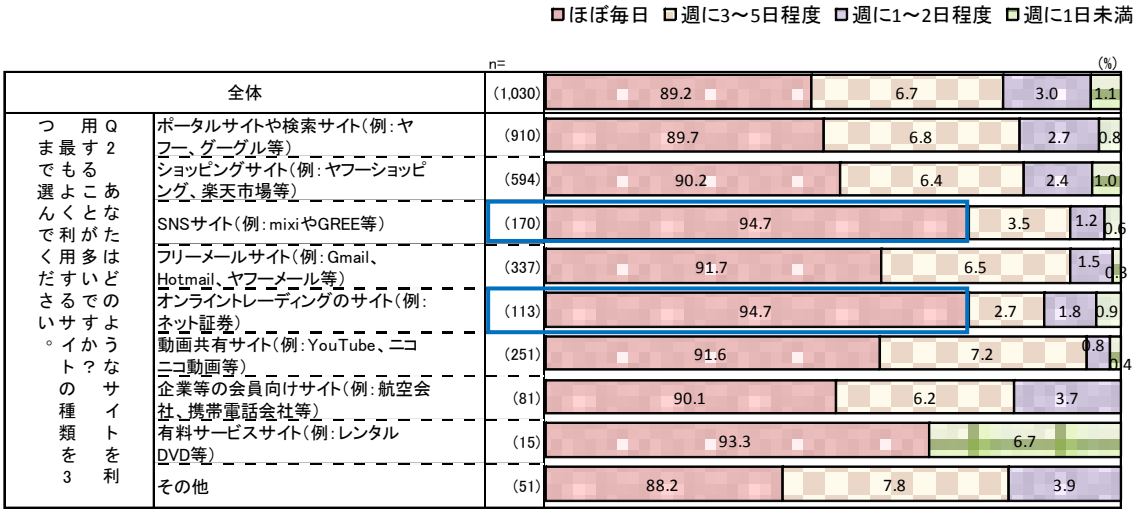


出典：総務省「平成 20 年通信利用動向調査（世帯編）」50 頁

・　回答者の約 9 割が「ポータルサイトや検索サイト」、半数以上が「ショッピングサイト」をよく利用している。また、「フリーメールサイト」（32.7%）、「動画共有サイト」（24.4%）の利用も多い。
・　利用頻度別の内訳を見ると、「SNS サイト」や「オンライントレーディングのサイト」利用者は、「ほぼ毎日」利用している者の割合が高い。

［Q2］ あなたはどのようなサイトを利用することが多いですか？
最もよく利用するサイトの種類を3つまで選んでください。
（n=1,030）



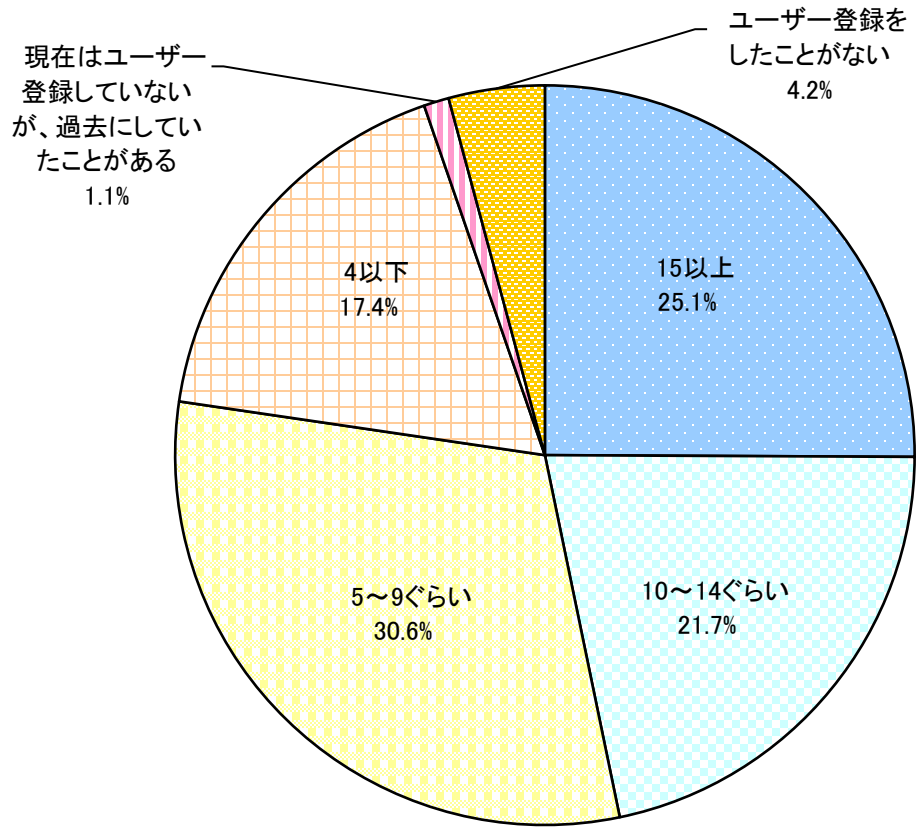


3　調査結果

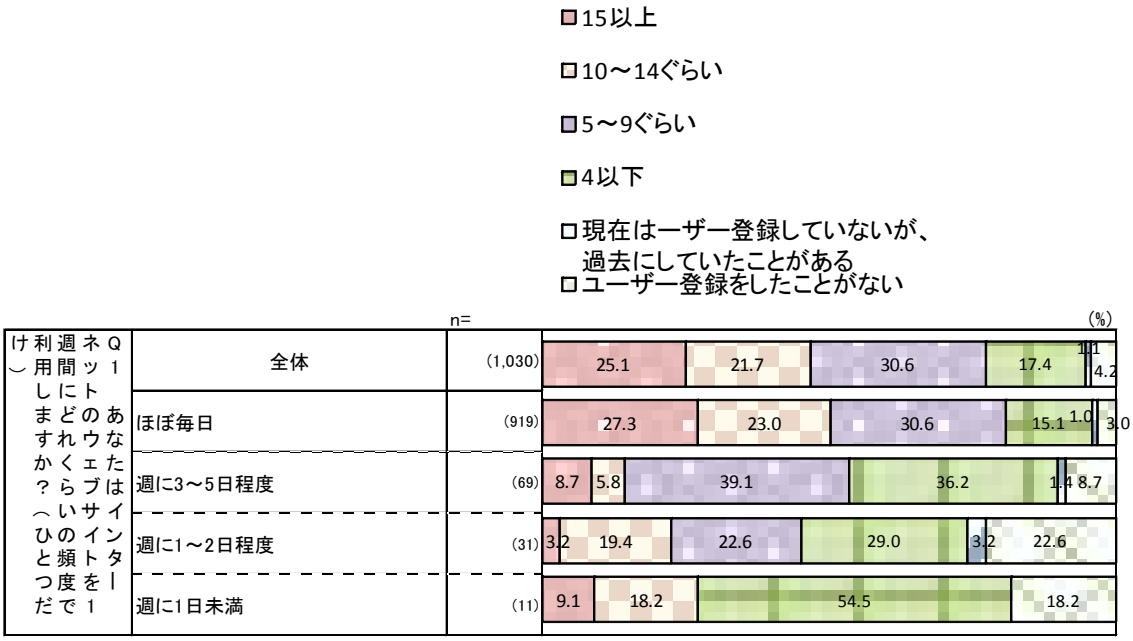
（1）ユーザーID の登録・管理状況

- 回答者の 4 人に 1 人以上が「15 以上」の Web サイトにユーザー登録しており、「10～14」と合わせると約半数が 10 以上の Web サイトに登録し、それに伴い発行された ID を保有している。
- 1 人平均 8.9 サイトに登録にユーザー登録している（「15 以上」と回答した者のユーザー登録数を 15 とした場合）。

[Q3] あなたは、現在、インターネットのいくつぐらいのサイトに
ユーザー登録をしていますか？（ひとつだけ）
（n=1,030）

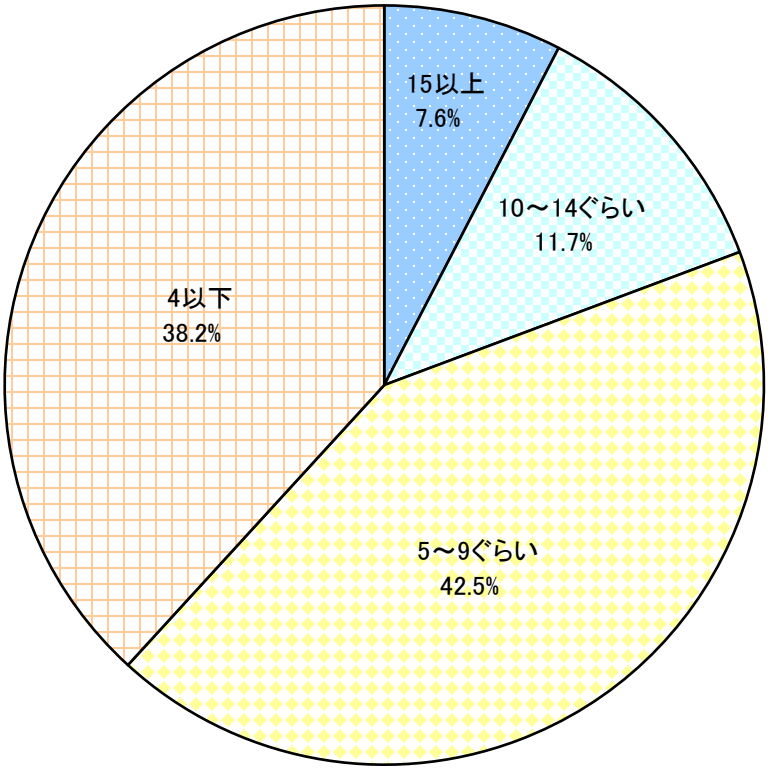


・　インターネットの利用頻度が高い利用者ほど、ユーザー登録数が多い傾向がある。



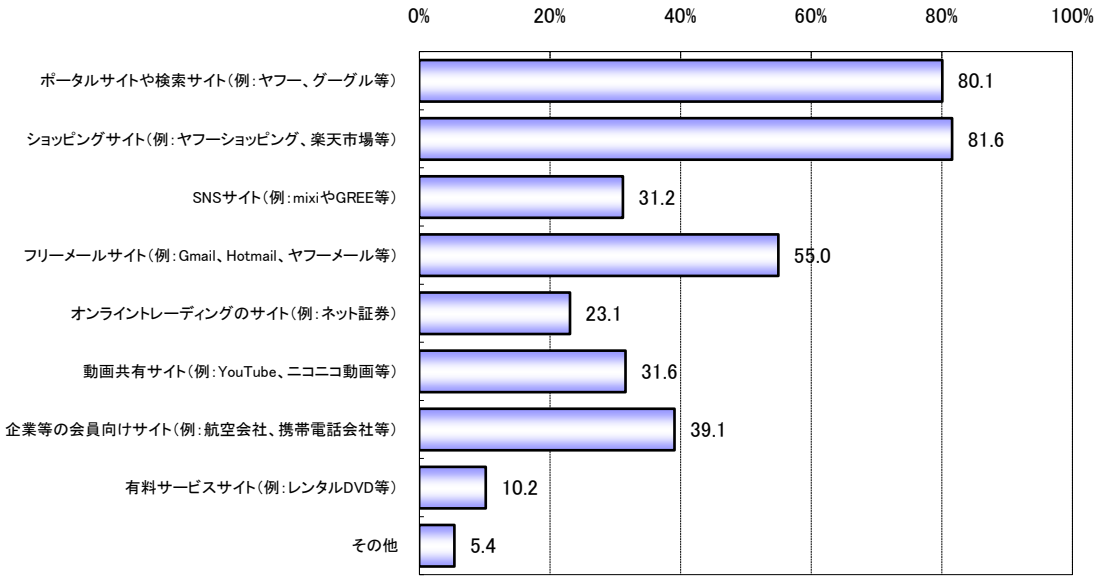
・　普段よく利用する Web サイト数は「5～9」が 42.5%で最も多く、次いで「4 以下」が 38.2%であった。
・　1 人平均 6.3 サイトをよく利用しており（「15 以上」の回答者の利用するサイト数を 15 とした場合）、ユーザー登録した Web サイトの約 1/4 は実際には余り利用されていないことになる。

［Q5］ あなたがユーザー登録をしたサイトの中で、
普段よく利用するサイト数は、どれくらいですか？（ひとつだけ）
（n=976）



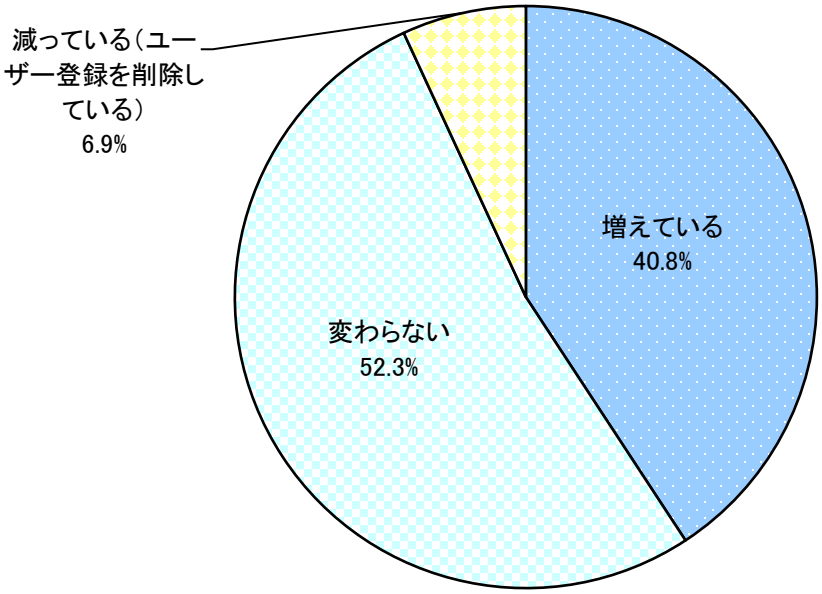
・　ユーザー登録したことのあるWebサイトは、「ポータルサイト」「ショッピングサイト」がそれぞれ80%以上で、「フリーメールサイト」（55.0%）、「企業等の会員向けサイト」（39.1%）がこれに続く。

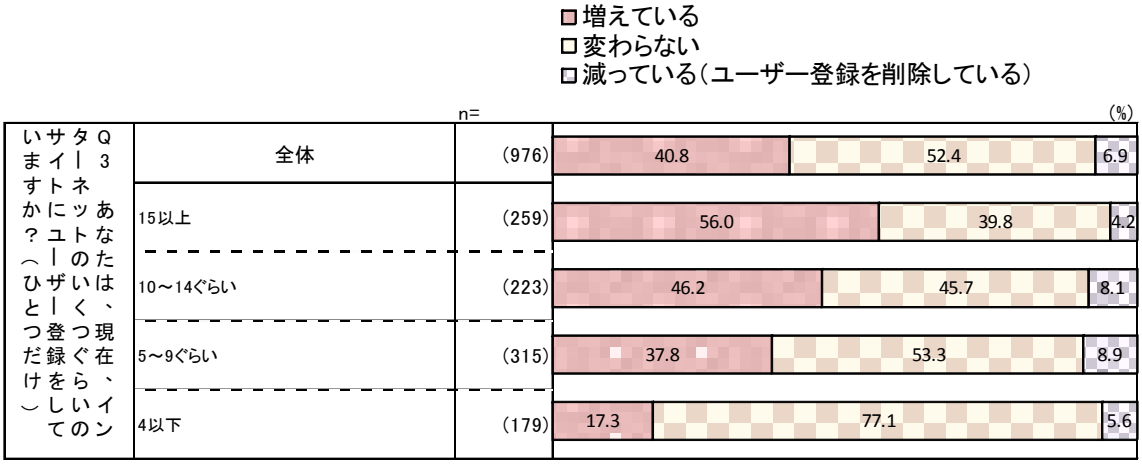
［Q4］ あなたはどのようなサイトにユーザー登録をしたことがありますか？
（いくつでも）
（n=987）



- ユーザー登録数は、約半数の回答者が、1 年前と比べて「変わらない」と回答している。
- また、「増えている」と回答した者が 40.8%である一方、「減っている」と回答した者はわずか 6.9%であり、一人当たりのユーザー登録数は、増加している傾向にある。
- ユーザー登録数が多い回答者ほど、最近 1 年間で、保有する ID が増えていると回答している。

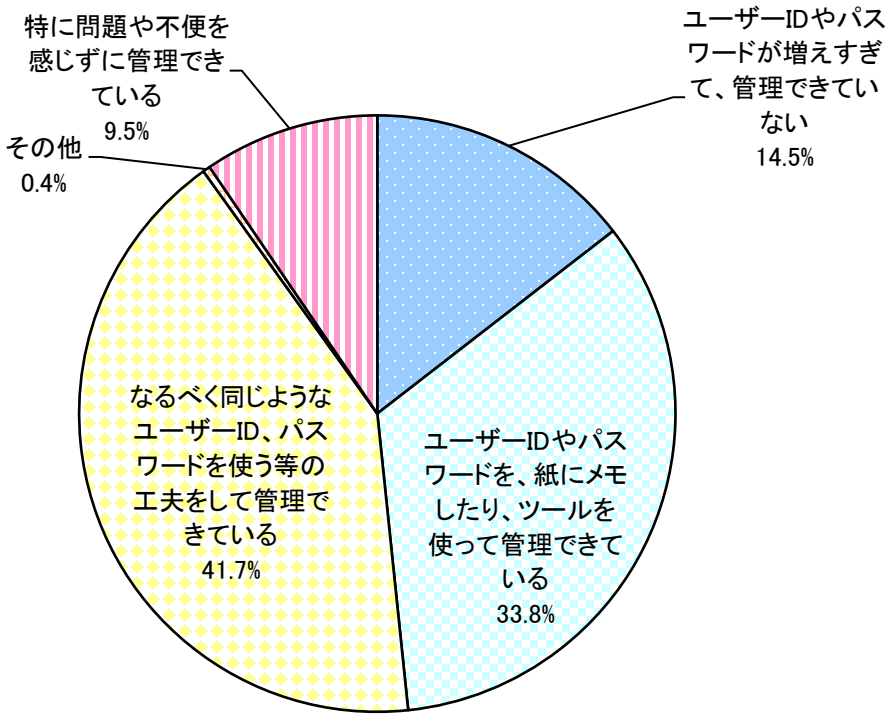
［Q6］ あなたのユーザー登録の数は、
1年前と比べて増えていますか？減っていますか？（ひとつだけ）
（n=976）



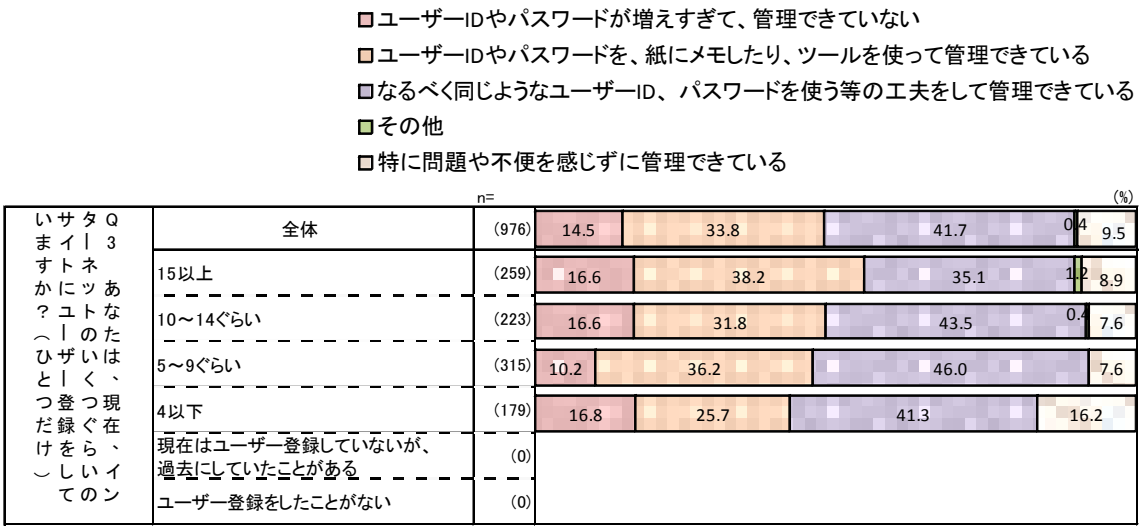


・　登録したユーザーID の管理状況については、「なるべく同じようなユーザーID、パスワードを使う等の工夫をしている」と回答した者が最も多かった。
・　「特に問題や不便を感じずに管理できている」と回答した者は約 10%であり、ほとんどの回答者がユーザーID を管理しきれていない、又は何らかの対策を要していることが分かった。

［Q7］ あなたがユーザー登録したサイトのユーザーIDやパスワードの管理状況について、最もあてはまるものを次の中から選んでください。（ひとつだけ）
（n=976）



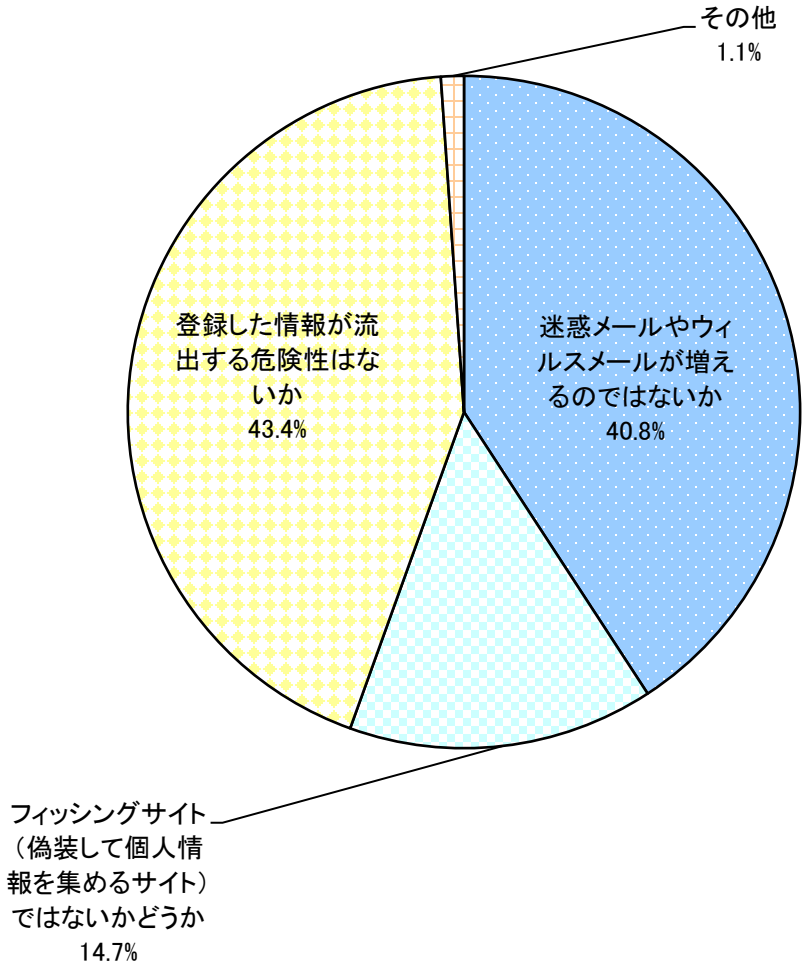
・　保有するID数によらず、ユーザーIDの管理状況は同じ傾向になっている。



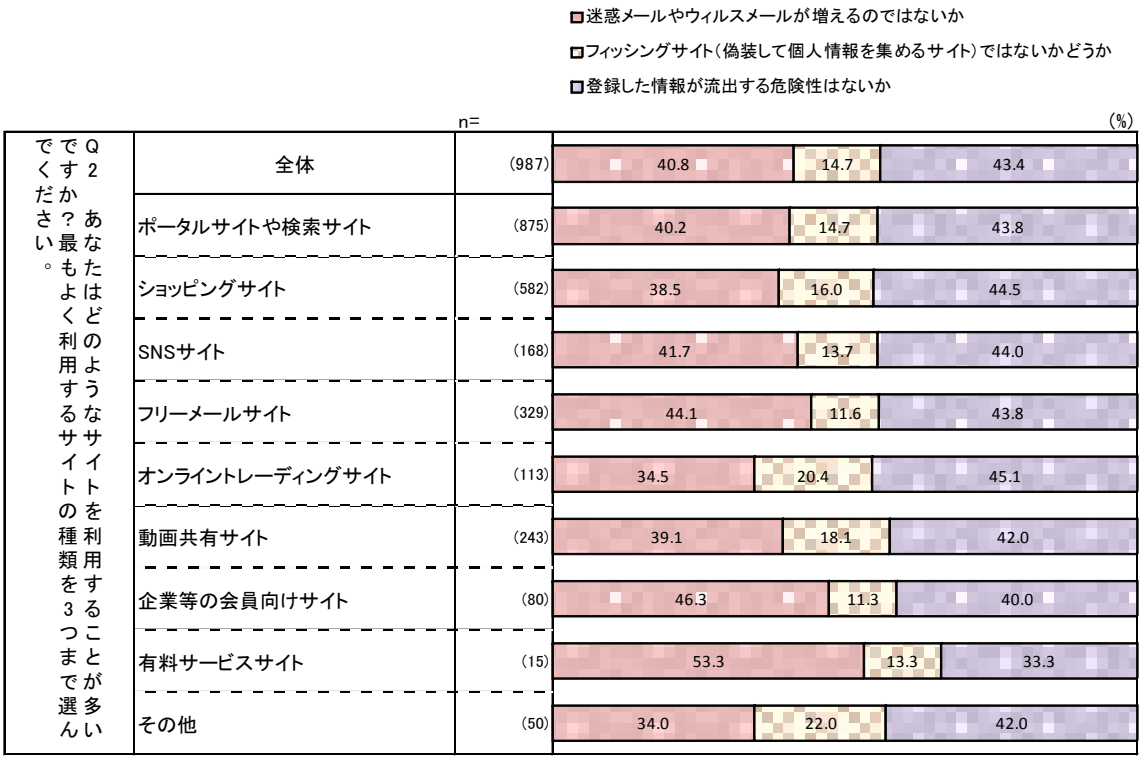
（２）ユーザー登録時の利用者の懸念とその対策

・　ユーザー登録に当たり、最も気にすることは、「登録した情報が流出する危険性はないか」（43.4%）及び「迷惑メールやウィルスメールが増えるのではないか」（40.8%）が、それぞれ回答者の 4 割以上を占めた。

［Q8］ あなたがユーザー登録をする時に、最も気にすることは何ですか？
最もあてはまるものを次の中から選んでください。
（n=987）

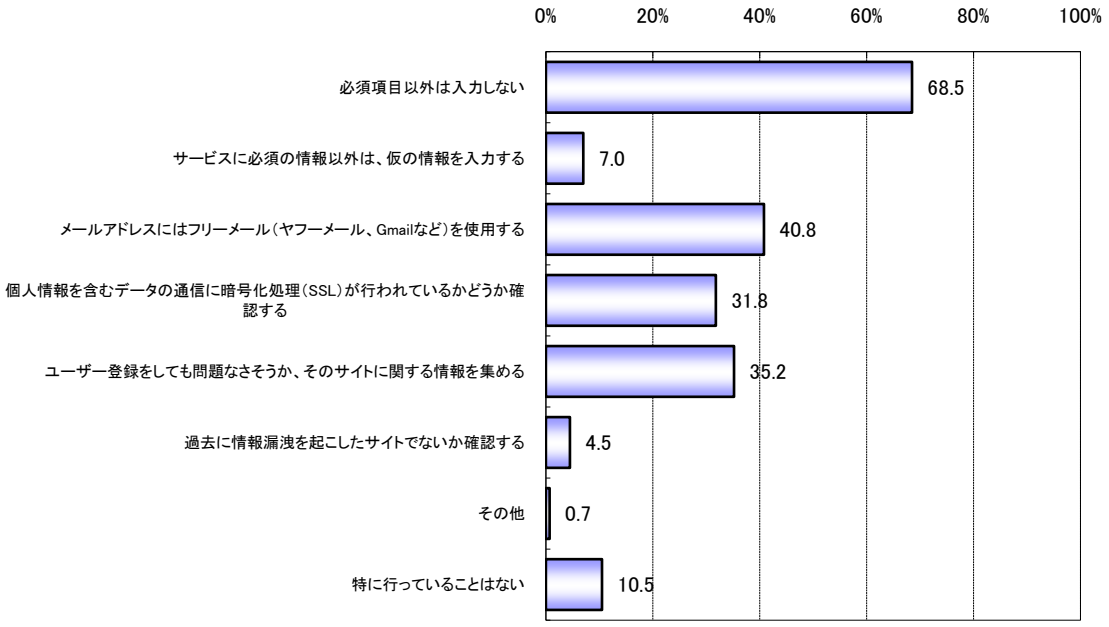


・　ユーザー登録時の懸念について、よく利用するサイト別では、「オンライントレーディング」のサイトで「フィッシング」を気にしている回答者の比率がやや高いが、全体的に大きな差異は見られなかった。



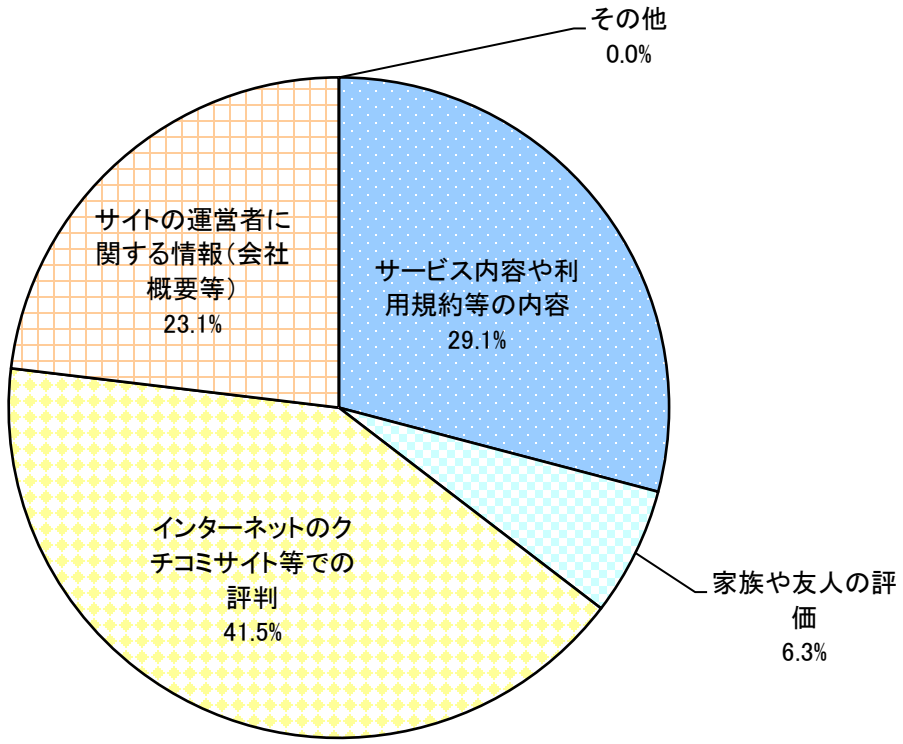
- ユーザー登録時の懸念への対策として、約 9 割の回答者が「必須項目以外は入力しない」、約 4 割が「メールアドレスにはフリーメールを使用する」と回答した。
- 登録する情報は可能な限り少なくし、問題があった場合にはメールアドレスを変えられる（捨てられる）ようにしているものと考えられる。

［Q9］ あなたはユーザー登録をする時に、
どのようなこと（対策）を行っていますか？（いくつでも）
（n=987）

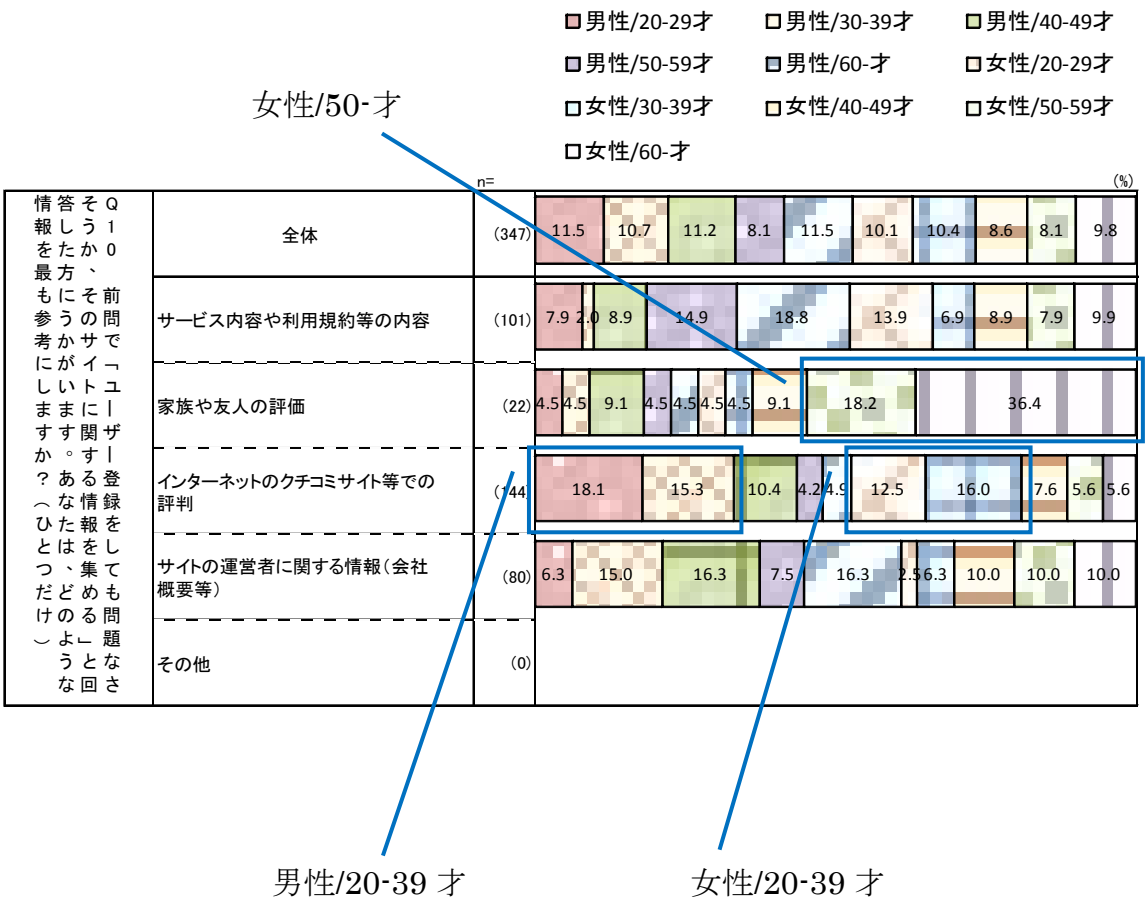


- ユーザー登録時の対策として、「サイトに関する情報を集める」と回答した者の 40%以上が「インターネットのクチコミサイト等での評判」を参考にしている。
- また、「サービス内容や利用規約等の内容」（29.1%）、「サイトの運営者に関する情報（会社概要等）」（23.1%）を参考にしているとする回答も多く、様々な情報の開示が大切であると考えられる。

［Q10］ 前問で「ユーザー登録をしても問題なさそうか、
そのサイトに関する情報を集める」と回答した方にうかがいます。
あなたは、どのような情報を最も参考にしますか？（ひとつだけ）
（n=347）

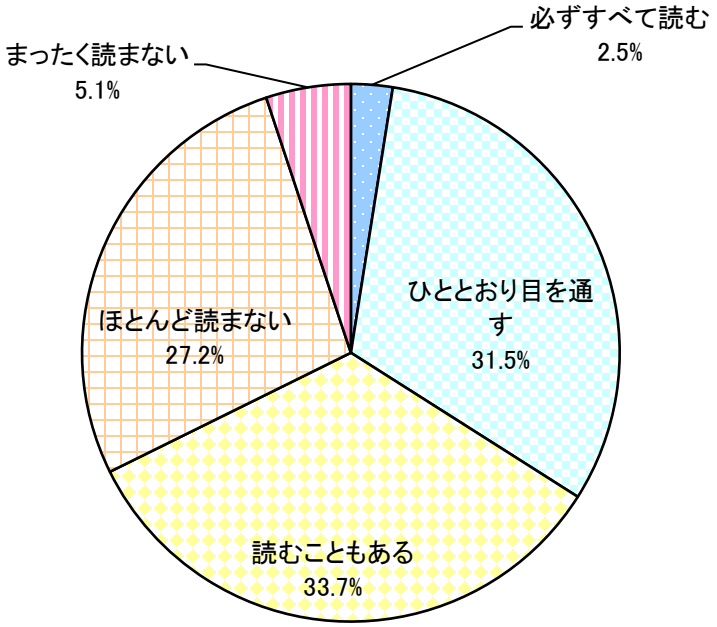


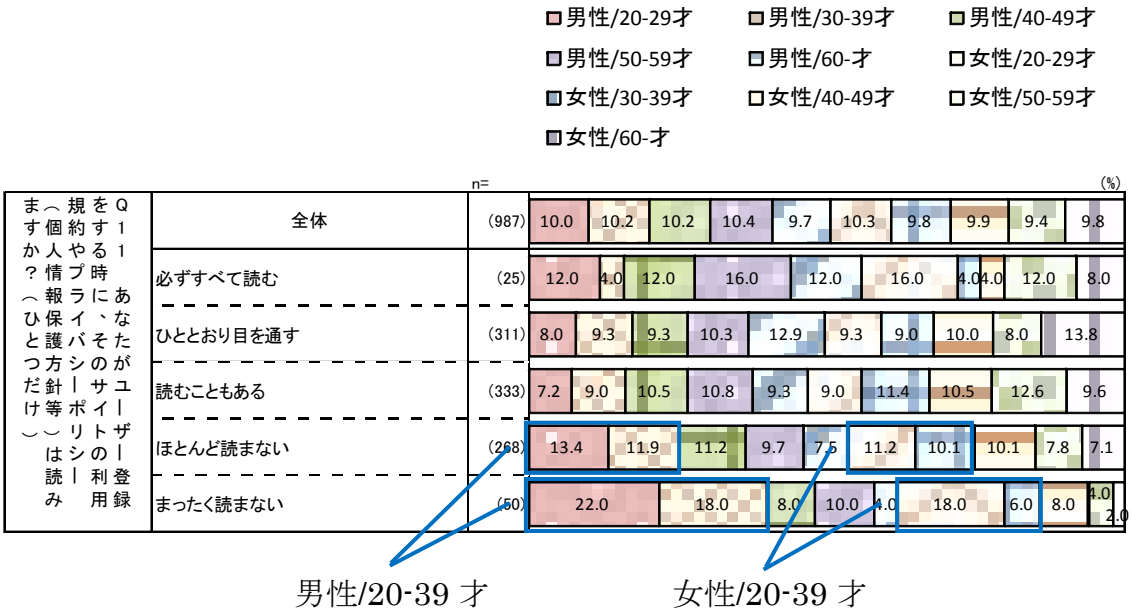
・　ユーザー登録時の対策について、年齢・性別の内訳を見ると、年齢が高い女性ほど「家族や友人の評価」を参考にしている。一方、「クチコミサイト等」を参考にするのは 20～30 代の男女の比率が高い。



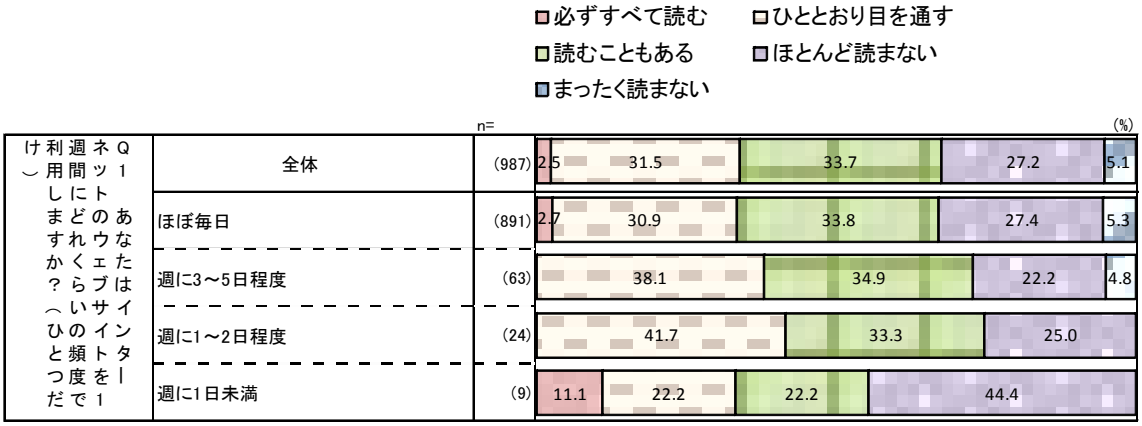
- ユーザー登録に当たり利用規約やプライバシーポリシーを「必ずすべて読む」、「ひととおり目を通す」、「読むこともある」とした回答者を合計すると全体の約 2/3 に達する。
- 「まったく読まない」、「ほとんど読まない」ともに 20 代男女の比率が高い。

[Q11] あなたがユーザー登録をする時に、
そのサイトの利用規約やプライバシーポリシー（個人情報保護方針等）は
読みますか？
(n=987)



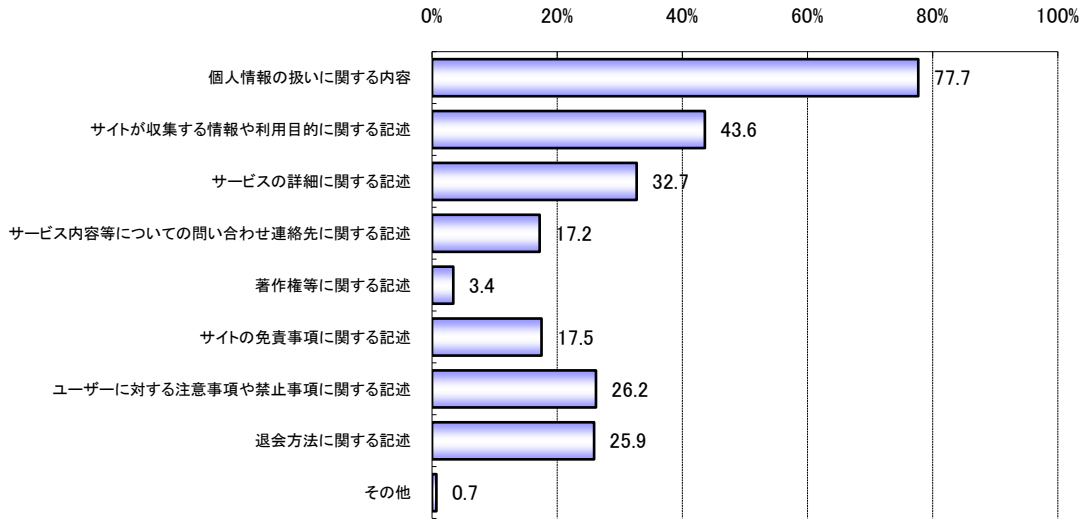


・　ユーザー登録に当たっての利用規約やプライバシーポリシーの確認について、利用頻度別の傾向を見ると、「必ずすべて読む」と回答したのは、「ほぼ毎日」あるいは「週に１日未満」利用する回答者が多かった。



・　利用規約やプライバシーポリシーを読む際は、特に「個人情報の扱いに関する内容」（77.7%）の確認が最も多く、個人情報の扱いについて留意していることが分かる。
・　また、「サイトが収集する情報や利用目的に関する記述」（43.6%）、「サービスの詳細に関する記述」（32.7%）も確認している。

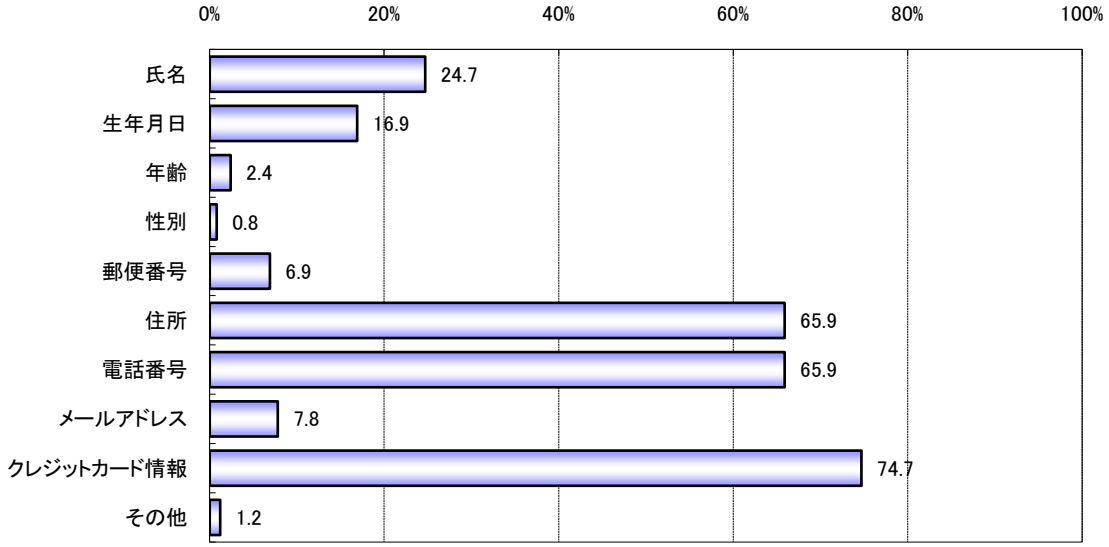
[Q12] あなたが利用規約やプライバシーポリシー（個人情報保護方針等）を読む際に、どのような内容について確認しますか？
特に確認する内容について、3つまで選択してください。
（n=669）



（３）登録情報等に関する利用者の意識

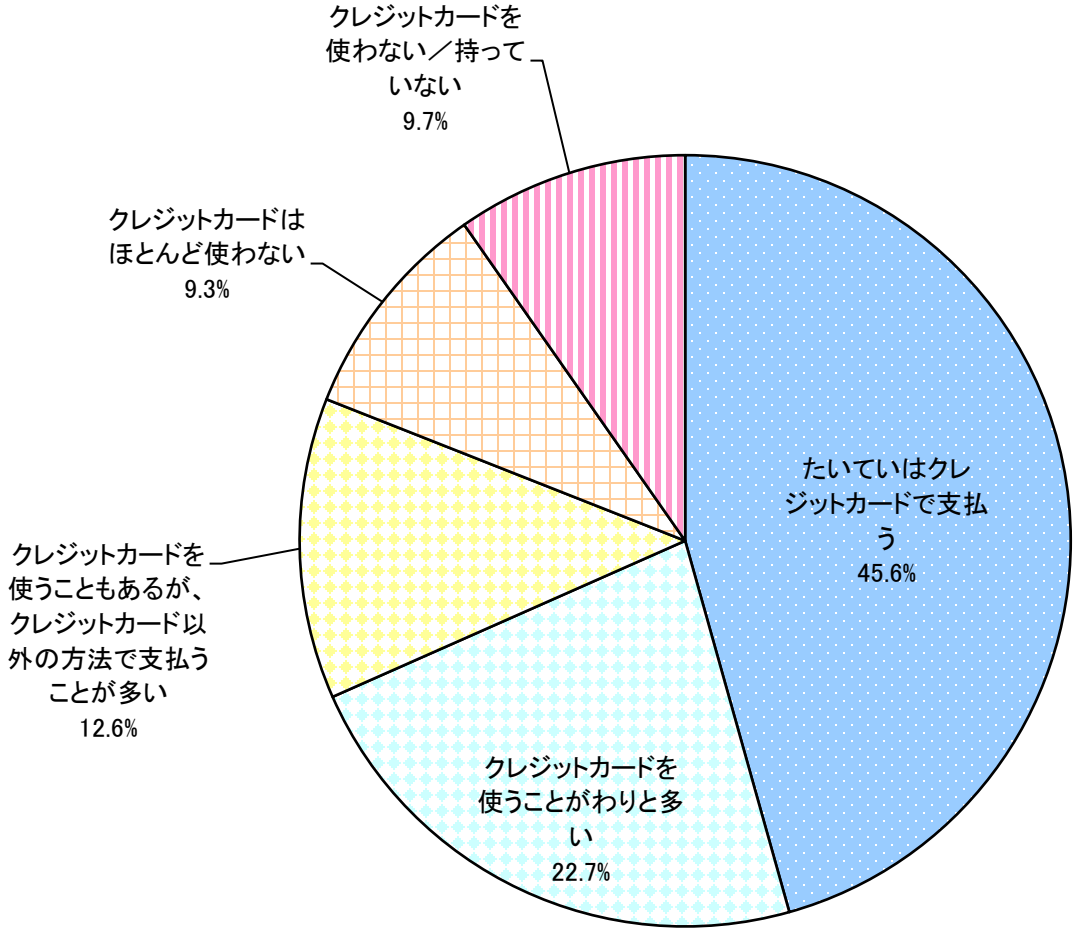
・　ユーザー登録時にできれば入力したくない情報は、「クレジットカード情報」（74.7%）が最も多く、次いで「住所」、「電話番号」（65.9%）が多かった。決済に関係する情報や、自宅等に関する情報は入力したくないものと考えられる。

[Q13] ユーザー登録をする時に、できれば入力したくない情報は何ですか？
3つまで選択してください。
（n=987）



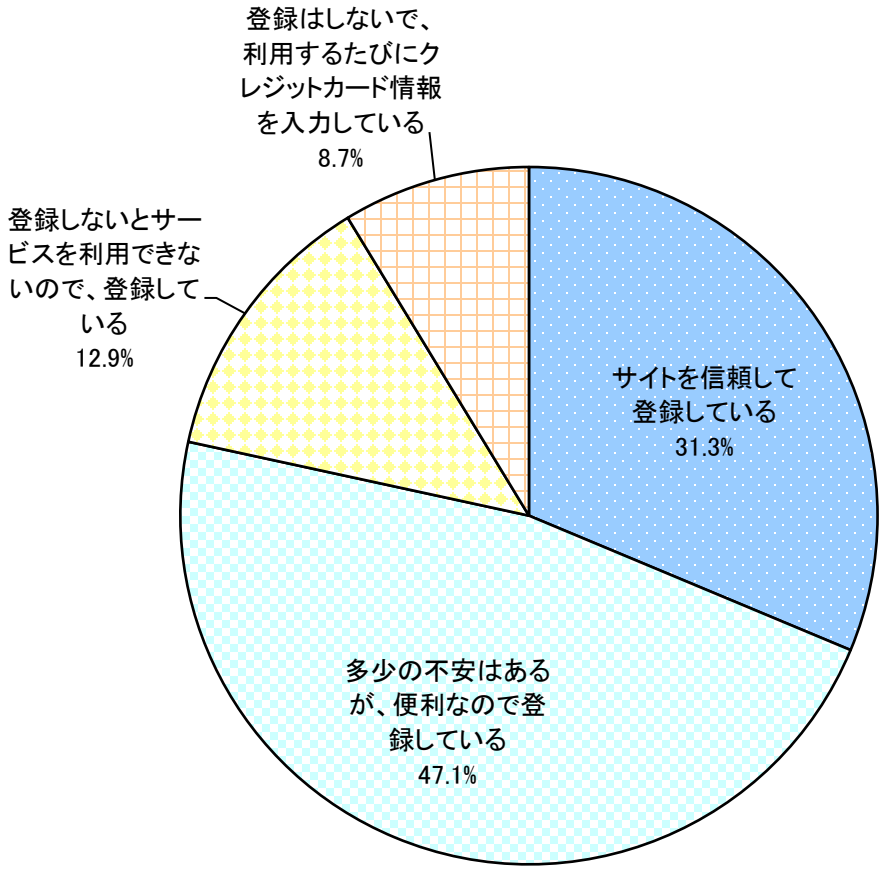
・　インターネットショッピング等の決済について、「たいていはクレジットカードで支払う」、「クレジットカードを使うことがわりと多い」とした回答者を合わせると、約 7 割の回答者がクレジットカードを使用している。

［Q14］ Q4「ユーザー登録をしたことがあるサイト」で
「ショッピングサイト」「有料サービスサイト」を選択した方にうかがいます。
インターネットで買い物やサービスを利用する時に、
クレジットカードで決済する頻度はどのくらいですか？（ひとつだけ）
（n=815）



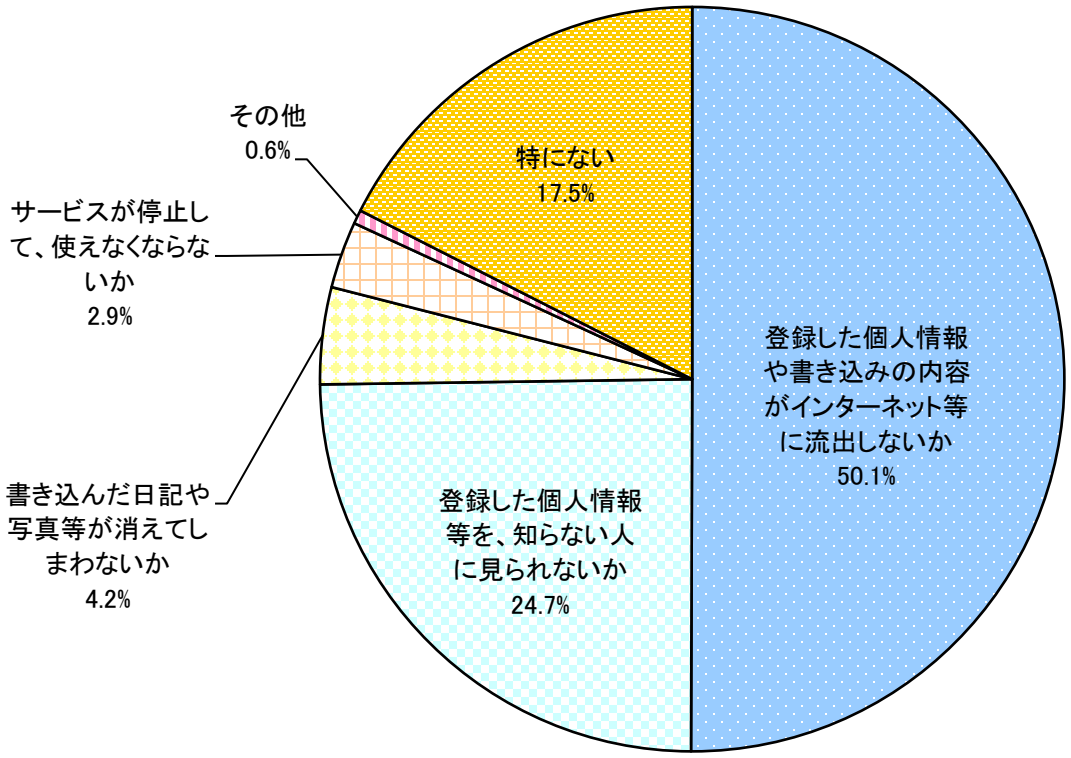
・　クレジットカード利用者の約 9 割がクレジットカード情報を Web サイトに登録している。

［Q15］ショッピングサイトやサービスサイトの利用方法についてうかがいます。
クレジットカードの情報の登録状況として最もあてはまるものを
次の中から選んでください。（ひとつだけ）
※　複数のクレジットカードを登録している方は、
　最も利用するサイトについてお答えください。
（n=736）

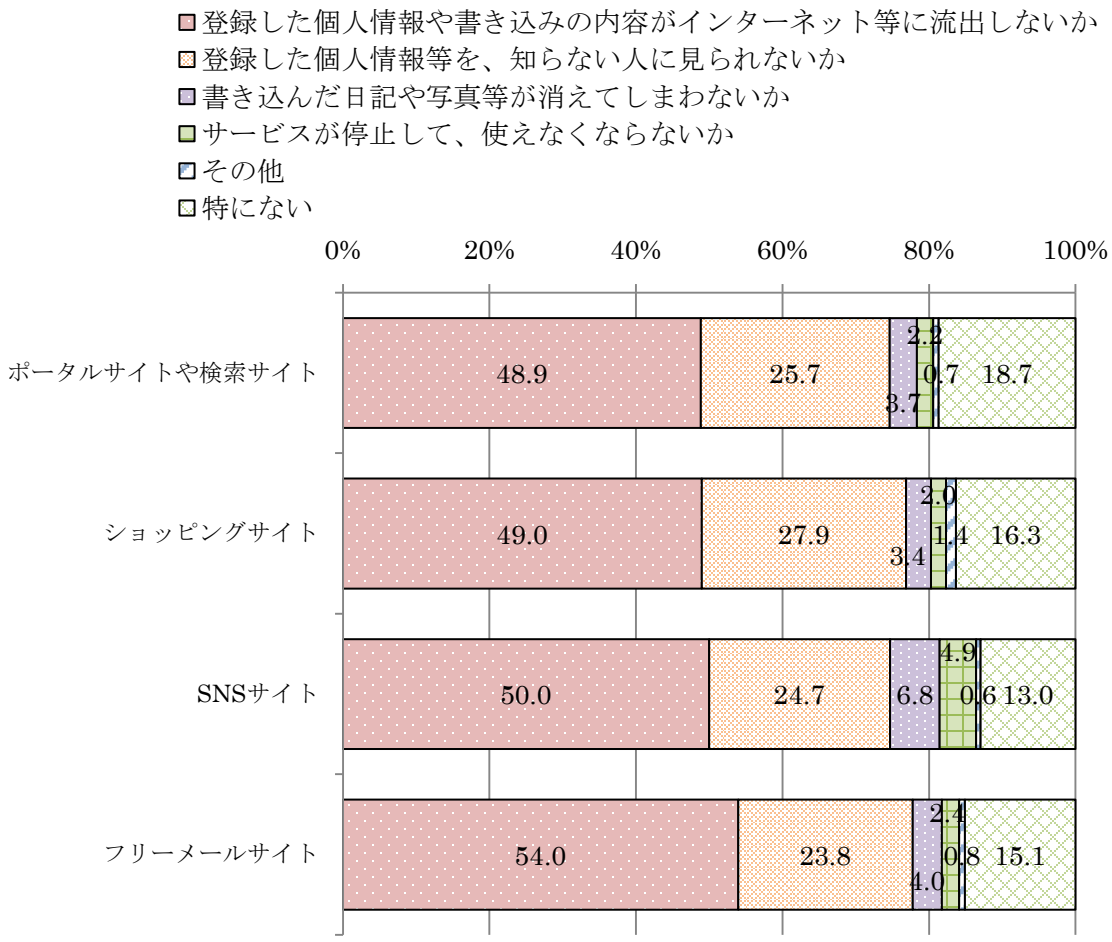


・　SNS サイトの利用者は、登録した個人情報や書き込みの内容が「インターネット等に流出しないか」（50.1%）、「知らない人に見られないか」（24.7%）を気にしている。

［Q16］ Q4「ユーザー登録をしたことがあるサイト」で
「SNSサイト」を選択した方にうかがいます。
SNSサイトを利用する場合に、気にすることはありますか？
最もあてはまるものを次の中から選んでください。（ひとつだけ）
（n=308）

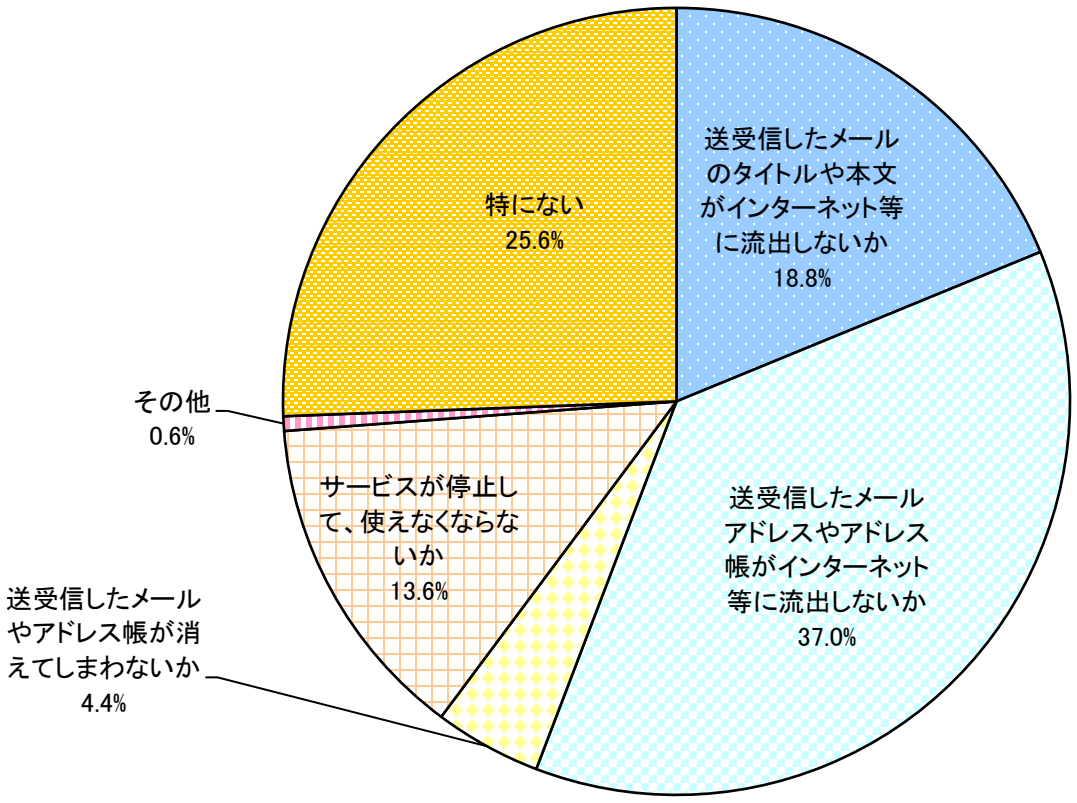


・　よく利用するサイト別に見た場合、特に利用者の多かったサイトの間では、SNS サイトの情報流出等を気にする回答者の割合は、ほぼ同様であった。
・　また、SNS サイトをよく利用する人は、「日記や写真等が消えてしまわないか」「使えなくならないか」といったデータの安全性について気にする傾向が強い。

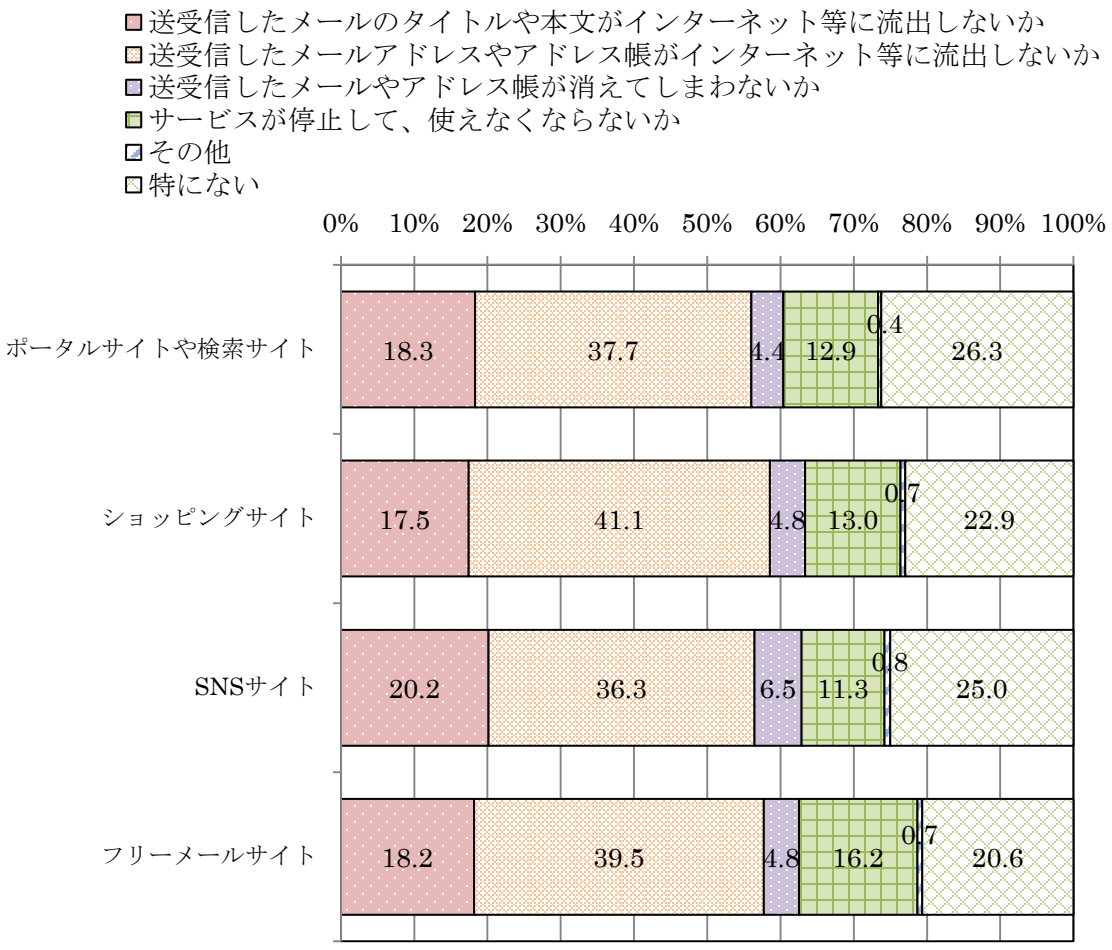


・　フリーメールの利用者は、「送受信したメールアドレスやアドレス帳」（37.0%）や「送受信したメールのタイトルや本文」（18.8%）がインターネット等に流出しないかを気にしている。
・　他方、特に気にしていることはないと回答している回答者も約 1/4 いる。
・　また、フリーメールの利用者は、「サービスが停止しないか」といったサービス面の安定性を気にする傾向が他と比較してやや高い。

［Q17］ Q4「ユーザー登録をしたことがあるサイト」で
「フリーメールサイト」を選択した方にうかがいます。
フリーメールサイトを利用する場合に、気にすることはありますか？
最もあてはまるものを次の中から選んでください。（ひとつだけ）
（n=543）



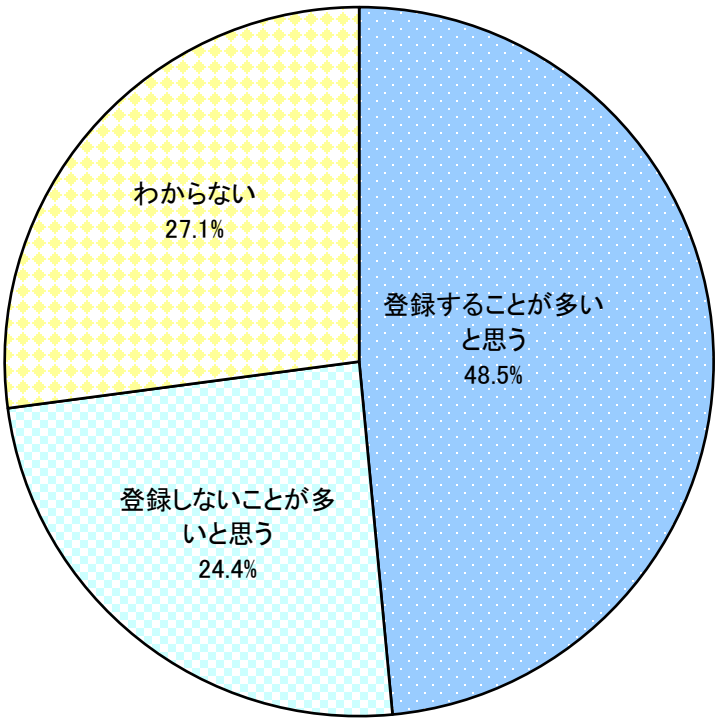
・　よく利用するサイト別に見た場合、特に利用者の多かったサイトの間では、フリーメールの利用に際しての情報流出等を気にする回答者の割合は、ほぼ同様であった。



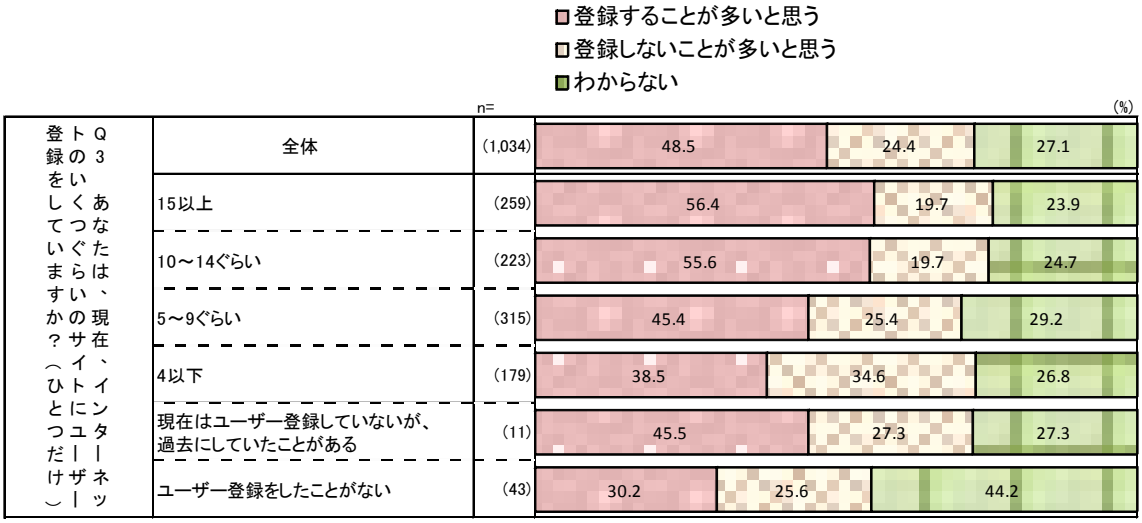
（４）ID 連携への期待等について

- ユーザー登録をしなくてもサービスを利用でき、（無料で）会員になればそれ以上のサービスを利用できるインターネットサイトについて、回答者の約半数が「登録することが多いと思う」と回答している。

［Q18］ ユーザー登録をしなくてもサービスを利用でき、
会員になればそれ以上のサービスを利用できるインターネットサイトがあるとします。
あなたはそのようなサイトにユーザー登録（無料）すると思いますか？（ひとつだけ）
（n=1,030）

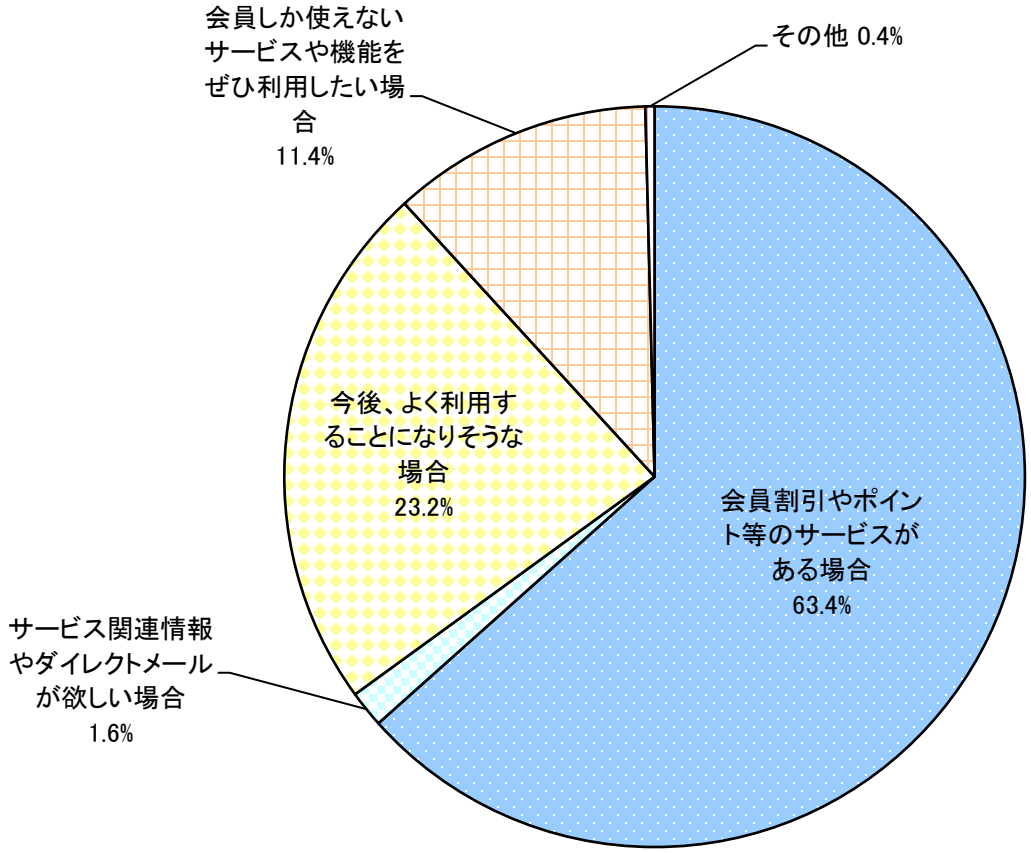


・　ユーザー登録数別の内訳を見ると、登録数が多い回答者ほど、ユーザー登録をしなくてもサービスを利用でき、(無料で) 会員になればそれ以上のサービスを利用できるサイトに「登録する」とした比率が比較的高くなっている。



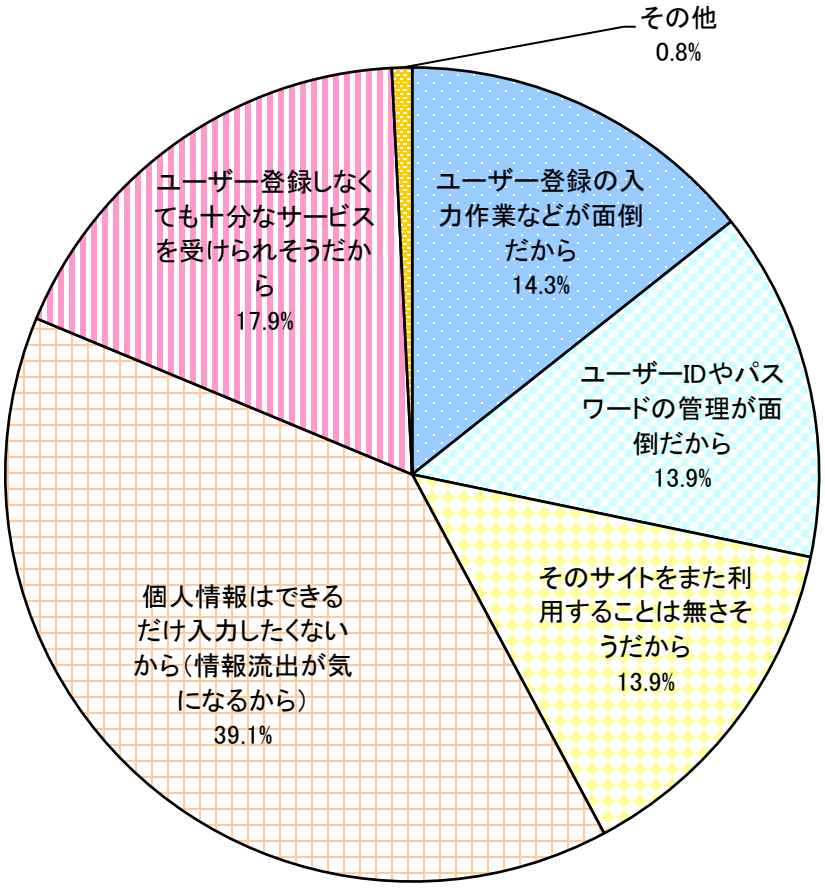
・　ユーザー登録をしなくてもサービスを利用でき、（無料で）会員になればそれ以上のサービスを利用できるサイトに「登録することが多いと思う」理由として、「会員割引やポイント等のサービス」（63.4%）といった具体的なメリットを期待するとともに、「今後、よく利用することになりそうな場合」（23.2%）といった利用頻度に関する回答も比較的多い。

[Q19] 前問で「登録することが多いと思う」を選択した方にうかがいます。
どのような場合に登録しようと思いますか？
最もあてはまるものを次の中から選んでください。（ひとつだけ）
（n=500）



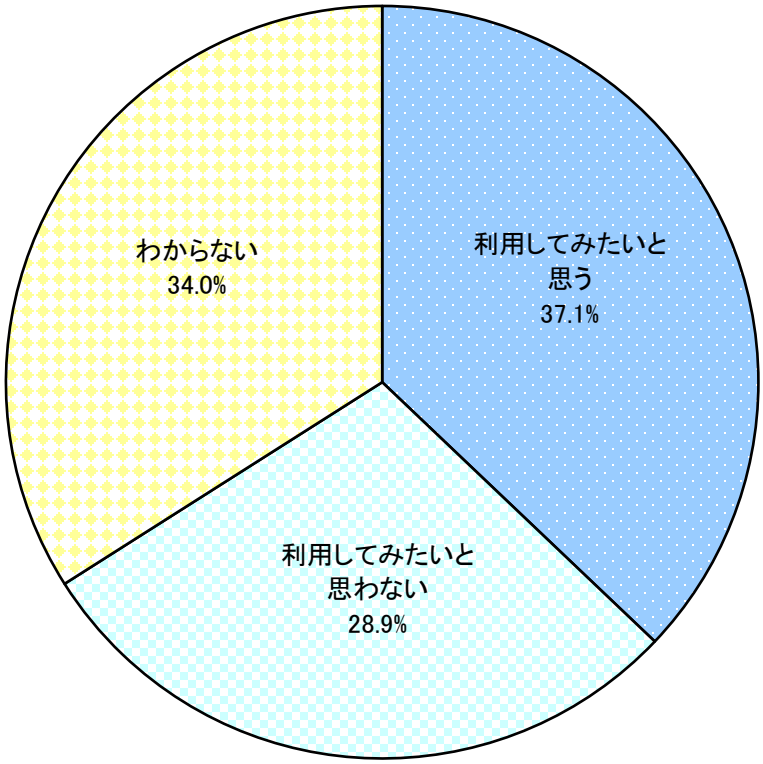
・　一方、ユーザー登録をしなくてもサービスを利用でき、（無料で）会員になればそれ以上のサービスを利用できるサイトに「登録しないことが多いと思う」理由としては、「個人情報はできるだけ入力したくない」（39.1%）が最も多かった。

［Q20］ 前問で「登録しないことが多いと思う」を選択した方にうかがいます。
登録しようと思わない理由として最もあてはまるものを次の中から選んでください。
（ひとつだけ）
（n=251）

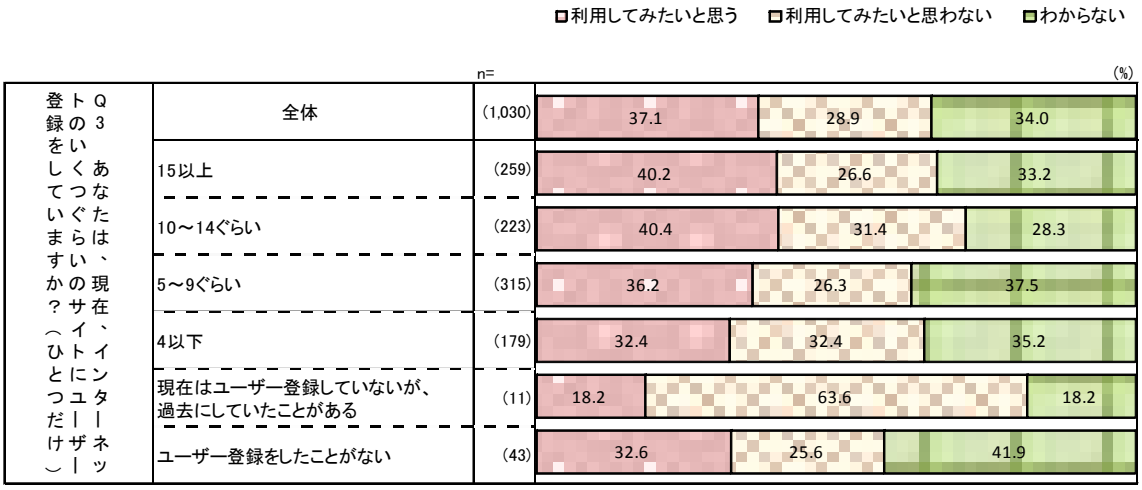


・　ID 連携の一類型として、サイト A のユーザーID を他のサイトでも利用できるサービスを「利用してみたいと思う」（37.1%）回答者が「利用してみたいと思わない」（28.9%）回答者よりも多かった。

［Q21］ あるサイトAにユーザー登録すると、
他のサイトBやサイトCもユーザー登録なしで利用できるサービスがあるとします。
このようなサービスを利用してみたいと思いますか？（ひとつだけ）
（n=1,030）

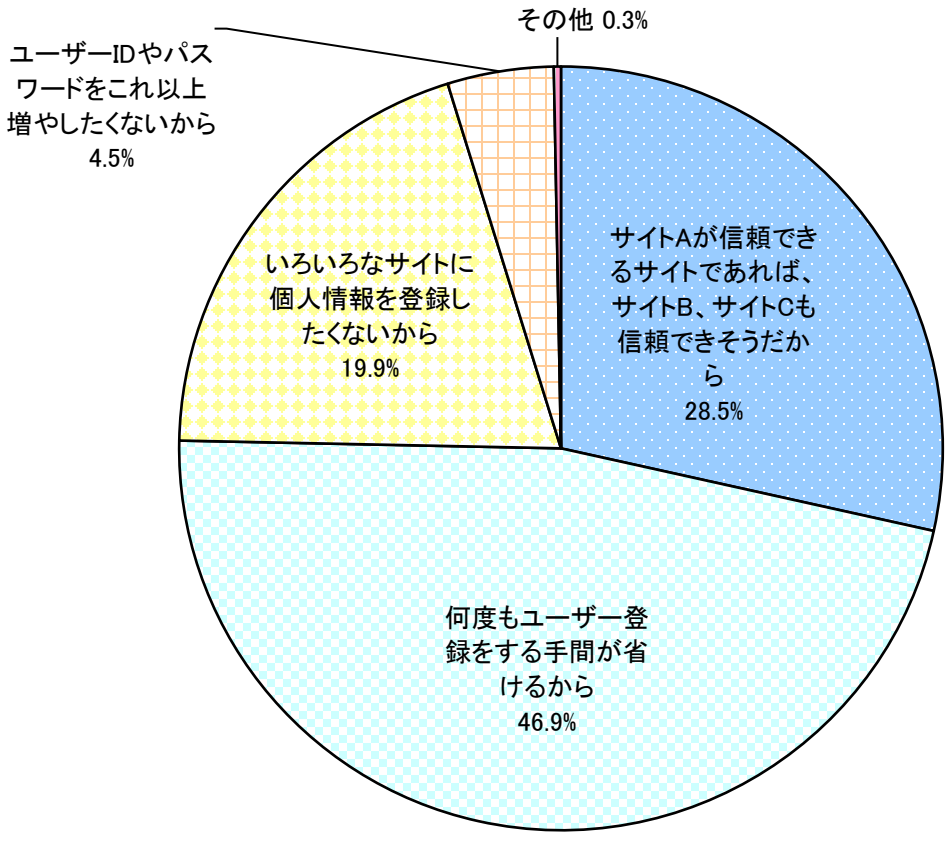


・　ユーザー登録数別の内訳を見ると、登録数が多い回答者ほど、サイトAのユーザーIDを他のサイトでも利用できるサービスを「利用してみたい」と回答した比率が高くなっている。



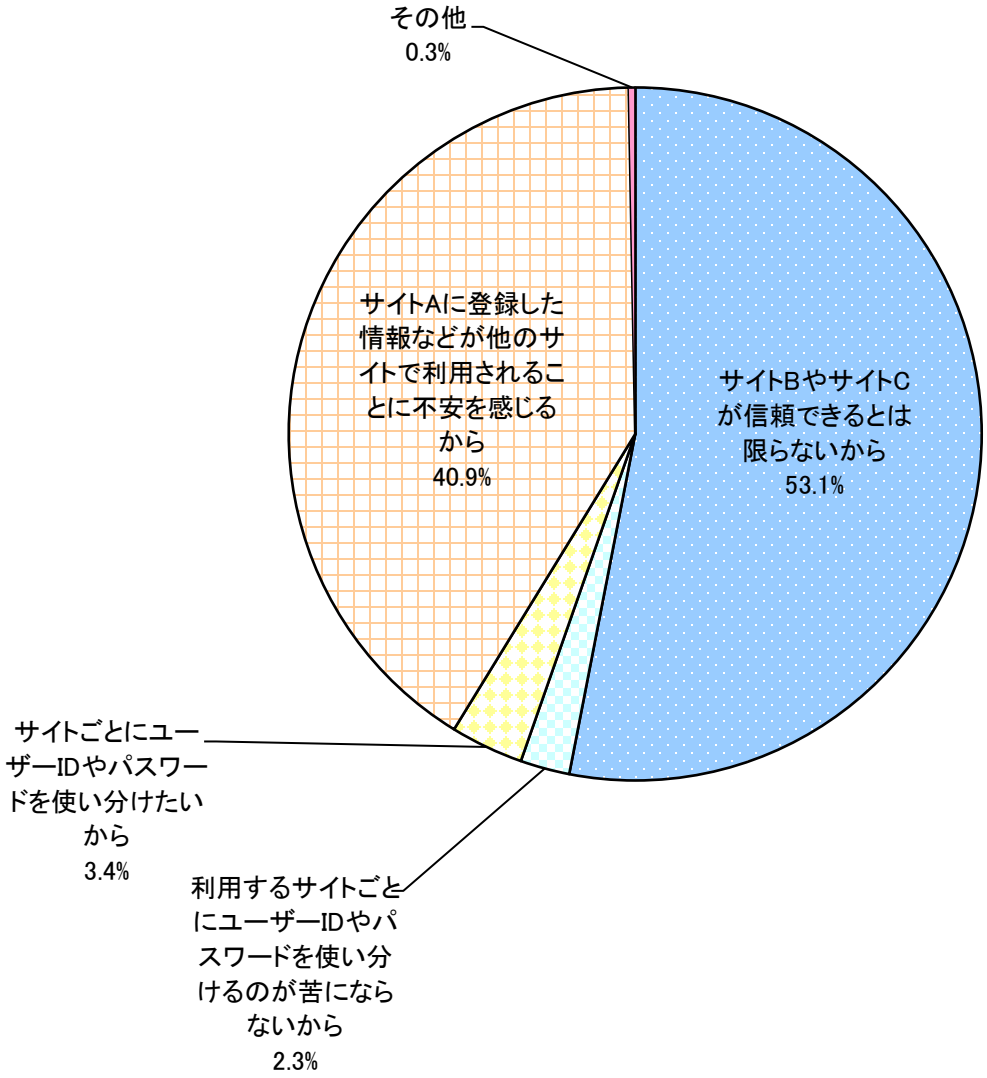
・　サイトAのユーザーIDを他のサイトでも利用できるサービスを「利用してみたいと思う」理由は、「何度もユーザー登録をする手間が省けるから」（46.9%）が最も多く、ユーザー登録に当たっては、その煩雑さが問題となっていると考えられる。
・　また、回答者の1/4以上が「サイトAが信頼できるサイトであれば、サイトB、サイトCも信頼できそうだから」（28.5%）と答えており、連携元となるWebサイトの信頼性も重要と考えられる。

［Q22］「あるサイトAにユーザー登録すると、
他のサイトBやサイトCにもユーザー登録なしで利用できるサービス」を
利用してみたいと思う理由を教えてください。（ひとつだけ）
（n=382）



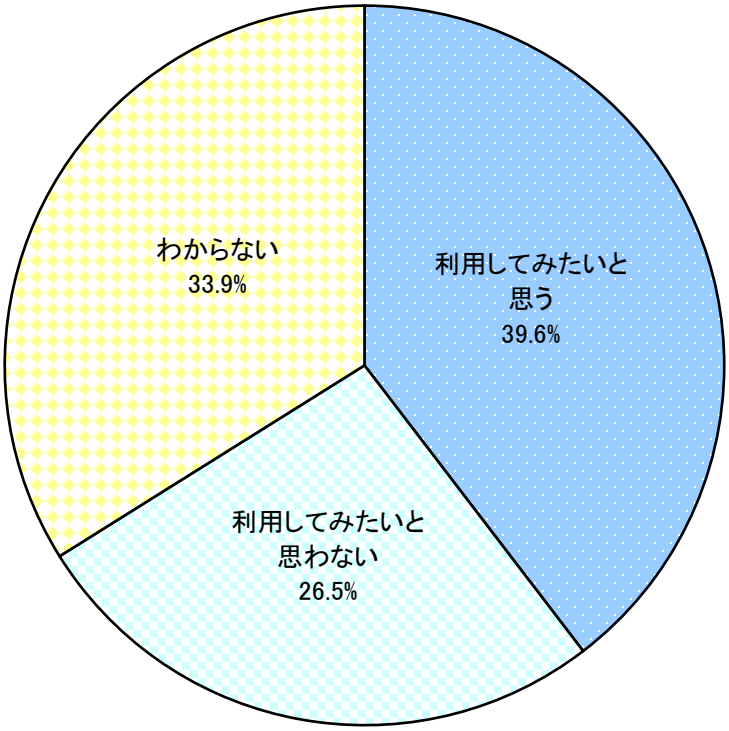
・　一方、サイトAのユーザーIDを他のサイトでも利用できるサービスを「利用してみたいと思わない」理由としては、「サイトB、サイトCが信頼できるとは限らないから」(53.9%)、「サイトAに登録した情報などが他のサイトで利用されることに不安を感じるから」(40.9%)が回答の大半を占めた。比較的慎重な利用者にとっては、ユーザーIDの使い分け等の煩雑さを解消するよりも、各Webサイトの信頼性を確認することが重要であると考えられる。

[Q23]「あるサイトAにユーザー登録すると、
他のサイトBやサイトCにもユーザー登録なしで利用できるサービス」を
利用してみたいと思わない理由を教えてください。(ひとつだけ)
(n=298)



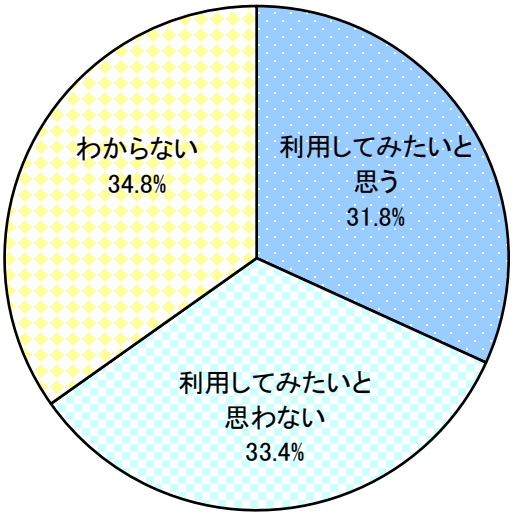
・　ユーザー登録した検索サイトで検索された会員制サイトをユーザー登録なしで利用できるサービスについても、「利用してみたいと思う」（39.6%）回答者が「利用してみたいと思わない」（26.5%）回答者を上回った。

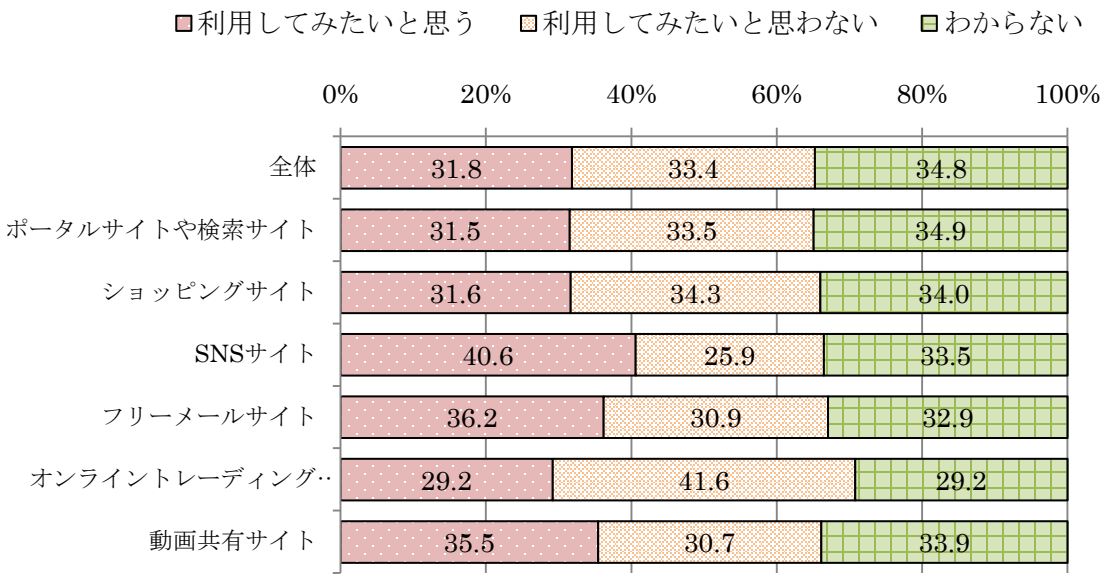
［Q24］ ユーザー登録をした検索サイト（サイトA）で検索すると、
あなたの好みや興味に合いそうなサイト（サイトB）が上位に出て、
サイトBにユーザー登録をしなくても利用できるサービスがあるとします。
このようなサービスを利用してみたいと思いますか？（ひとつだけ）
（n=1,030）



・　ユーザー登録した SNS サイトで友人から紹介された会員制サイトをユーザー登録なしで利用できるサービスについては、「利用してみたいと思う」（31.8%）回答者よりも「利用してみたいと思わない」（33.4%）回答者が多かった。
・　よく利用するサイト別で見ると、SNS サイトの利用者では「利用してみたい」と回答した者の割合が他と比較してやや高かった。

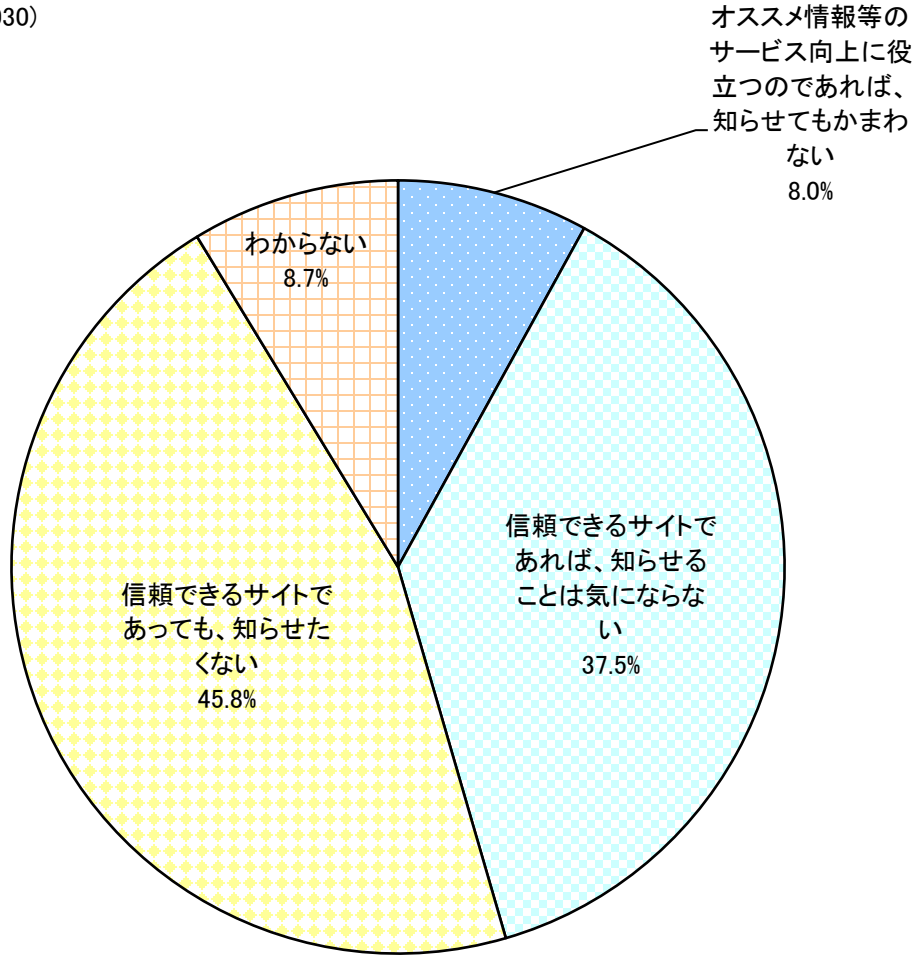
［Q25］ 同じSNS（サイトA）にいる友人から紹介された会員サイト（サイトB）に
あなたが興味を持っている場合、サイトBにユーザー登録をしなくても
利用できるサービスがあるとします。
このようなサービスを利用してみたいと思いますか？（ひとつだけ）
（n=1,030）



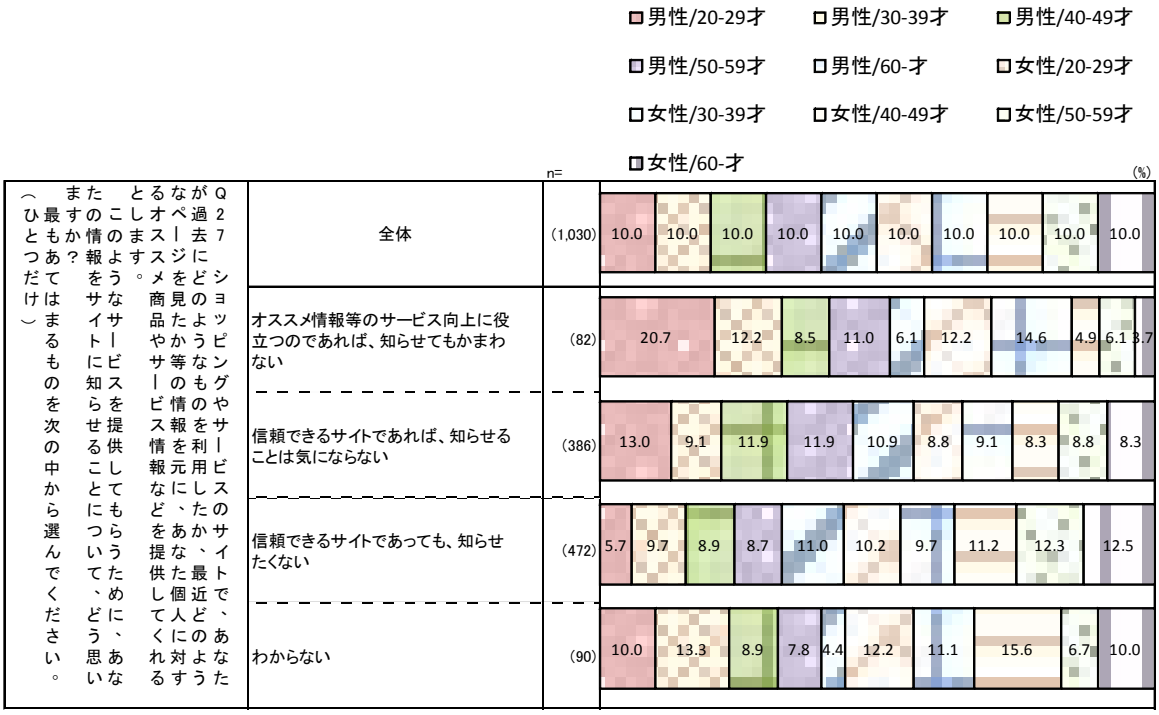


・　行動情報の取得については、回答者の半数近くが「信頼できるサイトであっても知らせたくない」（45.8%）と回答しており、「信頼できるサイトであれば、知らせることは気にならない」（37.5%）を上回った。

［Q27］ ショッピングやサービスのサイトで、
あなたが過去にどのようなものを利用したか、
最近どのようなページを見たか等の情報を元に、
あなた個人に対するオススメ商品やサービス情報など提供してくれるとします。
このようなサービスを提供してもらうために、
あなたの情報をサイトに知らせることについて、どう思いますか？
最もあてはまるものを次の中から選んでください。（ひとつだけ）
（n=1,030）



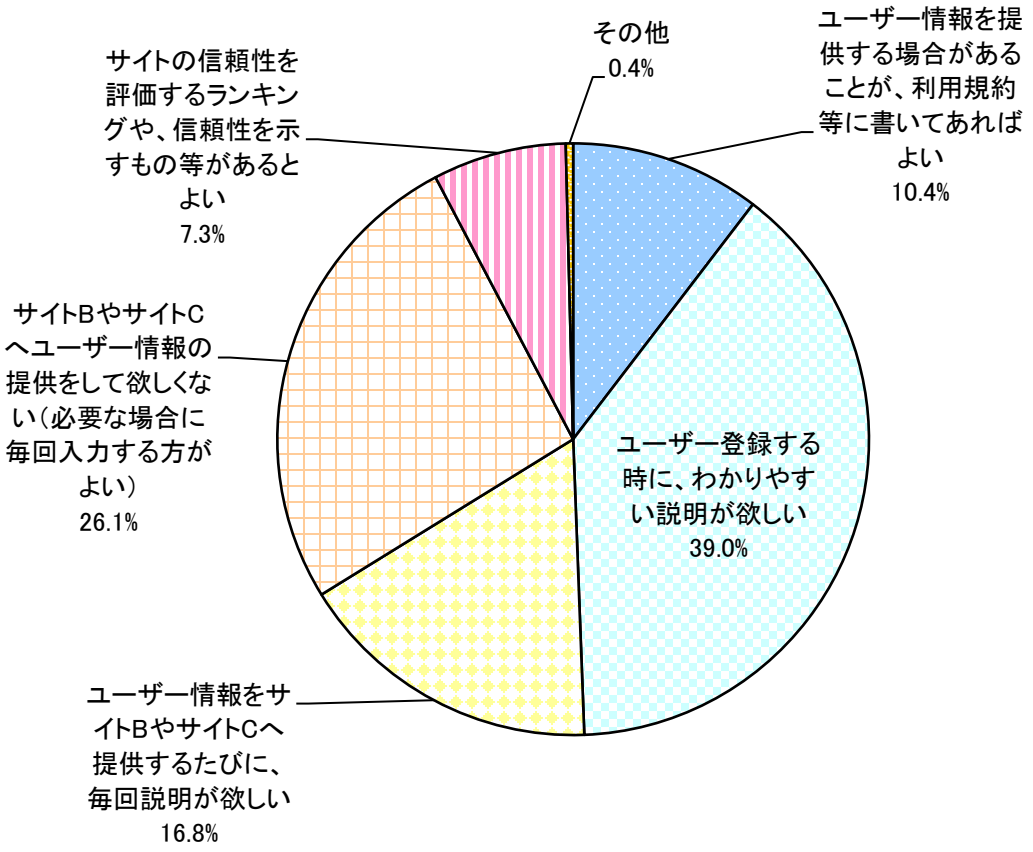
・　行動情報の取得について、性別・年代別では、男女ともに 20～30 代が比較的「知らせてもかまわない」と回答しており、高齢になるほど「知らせたくない」と回答した割合が高い。
・　既に実際のサービスでは行動情報が取得されている場合もあるが、現時点では必ずしも歓迎されていないものと考えられる。



（５）ID 登録を行うサイトへの要望等について

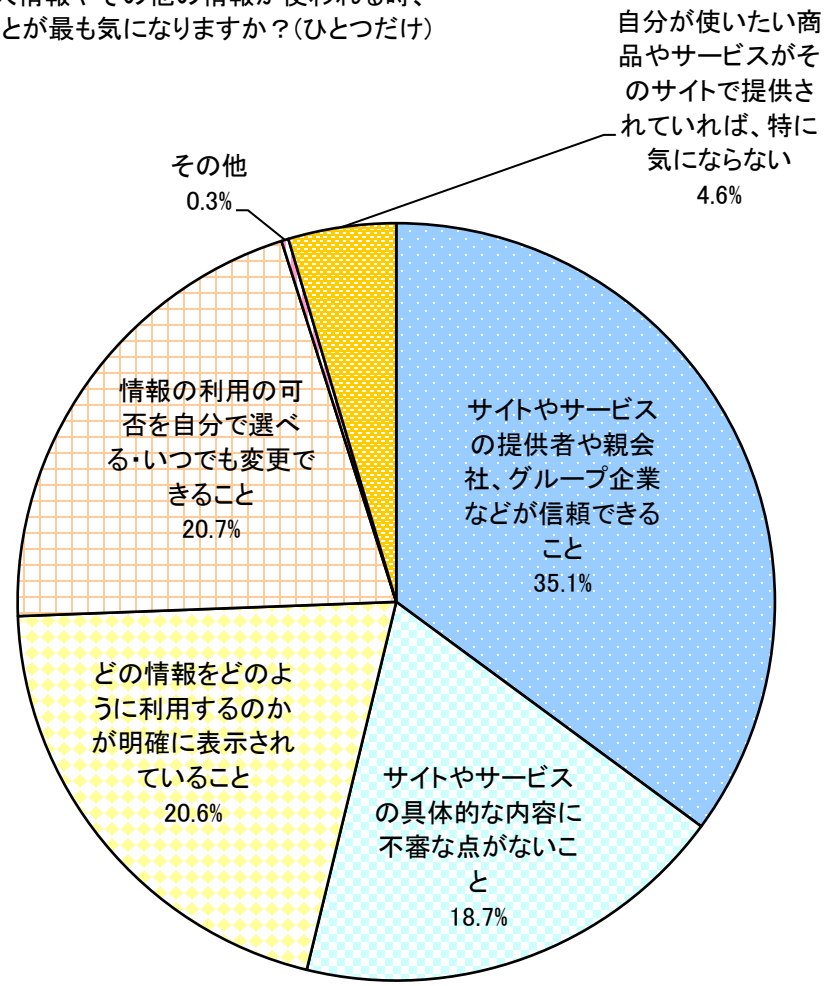
- サイト A に登録したユーザー情報を他のサイトへ提供するに当たり、サイト A に求める対応としては、「ユーザー登録時に分かりやすい説明が欲しい」（39.0%）が最も多く、利用規約等に書いてあるだけでは不十分という認識であると考えられる。
- また、「ユーザー情報の提供をして欲しくない」（26.1%）と回答する者も多く、利用する Web サイト限りでユーザー情報を留めて欲しいと考える利用者も多い。

[Q26] 前問までのようなサービスを利用する場合、
サイトAが持つユーザー情報（個人情報やポイント情報等）が、
サイトBやサイトCへ提供される場合があります。
ユーザー情報の提供にあたり、
どのような対応をサイトAにしてほしいと思いますか？
最もあてはまるものを次の中から選んでください。（ひとつだけ）
(n=536)



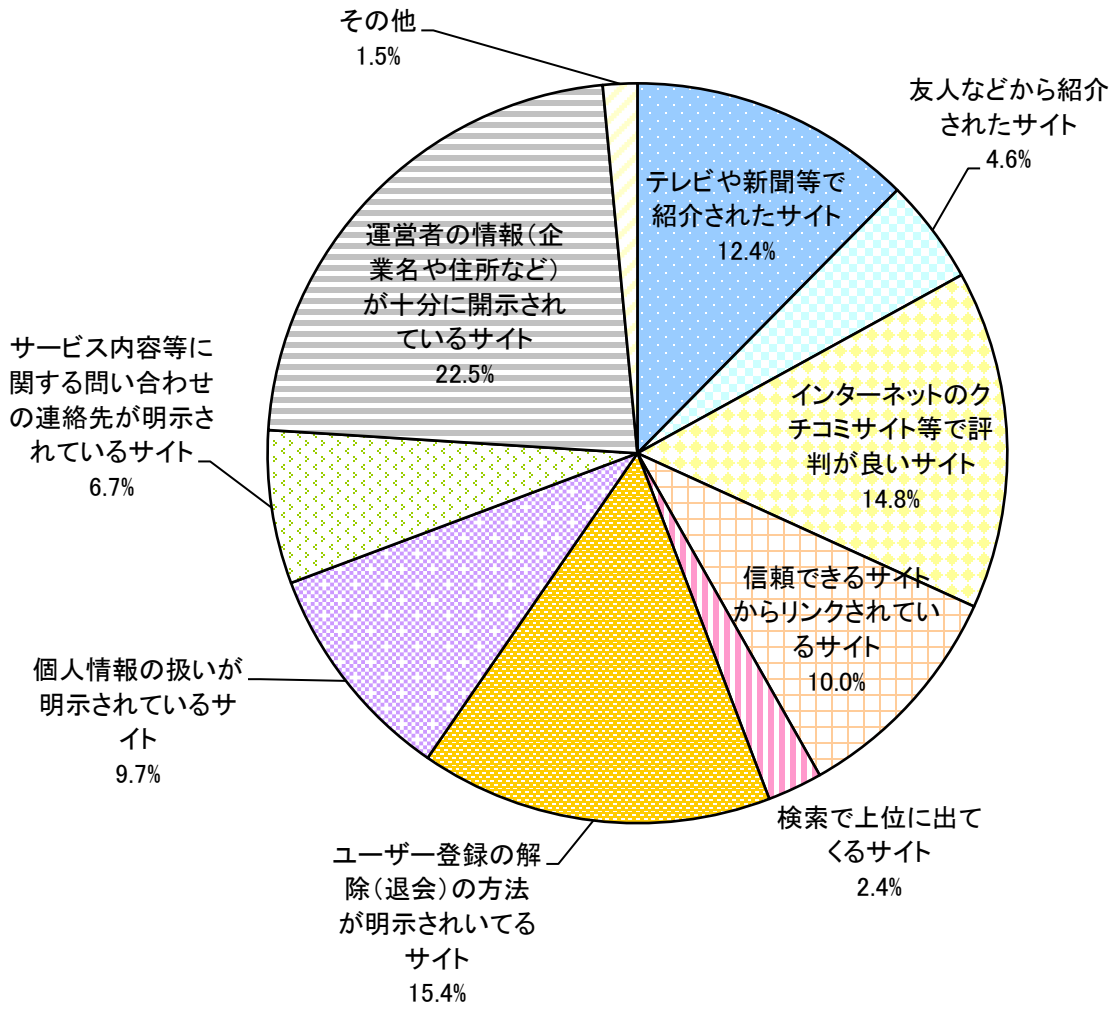
・　Web サイトやサービスで個人情報等が使われるときに気になることは、「サービス提供者やそのグループ企業等が信頼できること」(35.1%) が最も多く、利用者は Web サイトの運営者や関連会社の信頼性を重視していると考えられる。
・　また、「情報の利用の可否を選べること」(20.7%)、「どのように利用するのかが明確に表示されていること」(20.6%) が気になると回答した者も多い。

［Q28］ インターネットサイトやサービスを利用する上で、あなたの個人情報やその他の情報が使われる時、どのようなことが最も気になりますか？(ひとつだけ)
(n=1,030)



・　どのような Web サイトが最も信頼できるかについては、「運営者の情報が十分に開示されているサイト」（22.5%）と回答した者が最も多く、次いで「ユーザー登録の解除の方法が明示されているサイト」（15.4%）、「クチコミサイト等で評判が良いサイト」（14.8%）と回答した者が多かった。

［Q29］ あなたは、どのようなインターネットサイトであれば、
信頼できると思いますか？
最もあてはまるものを次の中から選んでください。（ひとつだけ）
（n=1,030）



（4）まとめ

以上のアンケート調査の結果をまとめると、利用者における ID 利用の現状、ID ビジネス利用に当たっての懸念及び ID 連携に対する期待等は、次のように整理される。

■ ID の利用と管理について

- ユーザー登録したサイト数が平均 8.9 サイトに対して、よく利用するサイト数は平均 6.3 サイトであり、仮にユーザー登録するごとに ID が発行されているとすると、保有する ID の約 1/4 は利用されていない。
- ユーザー登録した Web サイト数は、1 年前と比べて変わらないか、増えている（合わせて 9 割）。
- ID の管理に問題や不便を感じていない利用者は 10%に満たず、多くの利用者が ID 管理に苦労している。
- ID／パスワードの管理方法として、同じ ID／パスワードを利用している利用者が多い（4 割強）ことが分かった。
  なお、このような管理方法では、フィッシングサイト等で ID／パスワードを詐取されると、他の登録サイトへも不正に侵入・利用される可能性があり、被害の拡大を招く可能性があるので注意を要する。

■ ユーザー登録時の留意点と対策

- ユーザー登録に当たり、情報流出や迷惑メール等を気にする利用者が多く、必須項目以外は登録しない、フリーメールのアドレスを使う、当該 Web サイトが信頼できそうか情報を収集する、等の対策をとっている。Web サイトに関する情報としては、クチコミサイト等が多く参考にされている。
- ユーザー登録の際に、多くの利用者が利用規約やプライバシーポリシーを読み、個人情報の扱い、Web サイトが収集する情報やその利用目的等を確認している。
- 決済に関係するクレジットカード情報や、住所や電話番号といった個人を特定しやすい情報はできるだけ登録したくないと考えている。
- 他方、インターネットショッピングでクレジットカードを利用する者の約 9 割がクレジットカード情報を登録しており、できるだけ登録したくない情報といえども、サービスに必要であれば、利便性を優先して登録していると考えられる。

■　ID 連携への期待

・　ユーザー登録が必須でない Web サイトであっても、会員になればそれ以上のサービスを利用できる場合、回答者の約半数は「登録する」としている。登録の理由としては、会員割引やポイント等のメリットや、今後よく利用することになりそう、といった回答が多かった。また、ユーザー登録サイト数が多い回答者ほど「登録する」傾向にある。

・　ID連携について、ポータル型やサーチ型については、「利用してみたいと思う」回答者が「利用してみたいと思わない」回答者を上回った。コミュニティ型については、「利用してみたいと思わない」回答者の方が多かったが、SNSサイトをよく利用する回答者に限ると、「利用してみたいと思う」回答者が 4 割となり、他の 2 類型と同様の回答比率となる。[32]

・　Web サイトやサービスの利用に当たっては、利便性よりも連携元となる Web サイトの運営者及び連携先の Web サイトの運営者の信頼性が重視されている。

・　ID 連携によって利用者の情報を他の Web サイトへ提供する場合は、利用規約等に記述されているだけでは不十分であり、より分かりやすい説明が求められている。また、他の Web サイトやサービスに利用者の情報を提供して欲しくない、という意見も多い。

■　ユーザー登録を行うサイト等への要望

・　利用者の信頼を得るためには、Web サイトの運営者の情報を十分に開示すること、ユーザー登録の解除方法が明示されていることなどが必要とされている。

[32] なお、ID 連携の回答については、どの類型についても、「利用してみたいと思う」、「利用してみたいと思わない」、「わからない」と回答した者がそれぞれほぼ同じような割合となっており、多くの利用者にとって、あまりイメージがわかないのが現状であるとも考えられる。

＜別添＞

アンケート調査項目

Q1　あなたはインターネットのウェブサイトを 1 週間にどれくらいの頻度で利用しますか？（ひとつだけ）

- ほぼ毎日
- 週に 3～5 日程度
- 週に 1～2 日程度
- 週に 1 日未満

Q2　あなたはどのようなサイトを利用することが多いですか？最もよく利用するサイトの種類を 3 つまで選んでください。

1．ポータルサイトや検索サイト（例：ヤフー、グーグル等）
2．ショッピングサイト（例：ヤフーショッピング、楽天市場等）
3．SNS サイト（例：mixi や GREE 等）
4．フリーメールサイト（例：Gmail、Hotmail、ヤフーメール等）
5．オンライントレーディングのサイト（例：ネット証券）
6．動画共有サイト（例：YouTube、ニコニコ動画等）
7．企業等の会員向けサイト（例：航空会社、携帯電話会社等）
8．有料サービスサイト（例：レンタル DVD 等）
9．その他

Q３　あなたは、現在、インターネットのいくつぐらいのサイトにユーザー登録をしていますか？（ひとつだけ）

1．15 以上
2．10～14 ぐらい
3．5～9 ぐらい
4．4 以下
5．現在はユーザー登録していないが、過去にしていたことがある
6．ユーザー登録をしたことがない

Q４　あなたはどのようなサイトにユーザー登録をしたことがありますか？（い

くつでも）

１．ポータルサイトや検索サイト（例：ヤフー、グーグル等）
２．ショッピングサイト（例：ヤフーショッピング、楽天市場等）
３．SNS サイト（例：mixi や GREE 等）
４．フリーメールサイト（例：Gmail、Hotmail、ヤフーメール等）
５．オンライントレーディングのサイト（例：ネット証券）
６．動画共有サイト（例：YouTube、ニコニコ動画等）
７．企業等の会員向けサイト（例：航空会社、携帯電話会社等）
８．有料サービスサイト（例：レンタル DVD 等）
９．その他

Q５　あなたがユーザー登録をしたサイトの中で、普段よく利用するサイト数は、どれくらいですか？（ひとつだけ）

１．15 以上
２．10～14 ぐらい
３．5～9 ぐらい
４．4 以下

Q６　あなたのユーザー登録の数は、1 年前と比べて増えていますか？減っていますか？（ひとつだけ）

１．増えている
２．変わらない
３．減っている（ユーザー登録を削除している）

Q７　あなたがユーザー登録したサイトのユーザーID やパスワードの管理状況について、最もあてはまるものを次の中から選んでください。（ひとつだけ）

１．ユーザーID やパスワードが増えすぎて、管理できていない
２．ユーザーID やパスワードを、紙にメモしたり、ツールを使って管理できている
３．なるべく同じようなユーザーID、パスワードを使う等の工夫をして管理できている
４．その他

５．特に問題や不便を感じずに管理できている

Q８　あなたがユーザー登録をする時に、最も気にすることは何ですか？最もあてはまるものを次の中から選んでください。（ひとつだけ）

１．迷惑メールやウィルスメールが増えるのではないか
２．フィッシングサイト（偽装して個人情報を集めるサイト）ではないかどうか
３．登録した情報が流出する危険性はないか
４．その他

Q９　あなたはユーザー登録をする時に、どのようなこと（対策）を行っていますか？（いくつでも）

１．必須項目以外は入力しない
２．サービスに必須の情報以外は、仮の情報を入力する
３．メールアドレスにはフリーメール（ヤフーメール、Gmail など）を使用する
４．個人情報を含むデータの通信に暗号化処理（SSL）が行われているかどうか確認する
５．ユーザー登録をしても問題なさそうか、そのサイトに関する情報を集める
６．過去に情報漏洩を起こしたサイトでないか確認する
７．その他
８．特に行っていることはない

Q１０　前問で「ユーザー登録をしても問題なさそうか、そのサイトに関する情報を集める」と回答した方にうかがいます。あなたは、どのような情報を最も参考にしますか？（ひとつだけ）

１．サービス内容や利用規約等の内容
２．家族や友人の評価
３．インターネットのクチコミサイト等での評判
４．サイトの運営者に関する情報（会社概要等）
５．その他

Ｑ１１　あなたがユーザー登録をする時に、そのサイトの利用規約やプライバシーポリシー（個人情報保護方針等）は読みますか？（ひとつだけ）

１．必ずすべて読む
２．ひととおり目を通す
３．読むこともある
４．ほとんど読まない
５．まったく読まない

Ｑ１２　あなたが利用規約やプライバシーポリシー（個人情報保護方針等）を読む際に、どのような内容について確認しますか？特に確認する内容について、３つまで選択してください。

１．個人情報の扱いに関する内容
２．サイトが収集する情報や利用目的に関する記述
３．サービスの詳細に関する記述
４．サービス内容等についての問い合わせ連絡先に関する記述
５．著作権等に関する記述
６．サイトの免責事項に関する記述
７．ユーザーに対する注意事項や禁止事項に関する記述
８．退会方法に関する記述
９．その他

Ｑ１３　ユーザー登録をする時に、できれば入力したくない情報は何ですか？３つまで選択してください。

１．氏名
２．生年月日
３．年齢
４．性別
５．郵便番号
６．住所
７．電話番号
８．メールアドレス
９．クレジットカード情報
１０．その他

Q１４　Q４「ユーザー登録をしたことがあるサイト」で「ショッピングサイト」「有料サービスサイト」を選択した方にうかがいます。インターネットで買い物やサービスを利用する時に、クレジットカードで決済する頻度はどのくらいですか？（ひとつだけ）

１．たいていはクレジットカードで支払う
２．クレジットカードを使うことがわりと多い
３．クレジットカードを使うこともあるが、クレジットカード以外の方法で支払うことが多い
４．クレジットカードはほとんど使わない
５．クレジットカードを使わない／持っていない

Q１５　ショッピングサイトやサービスサイトの利用方法についてうかがいます。クレジットカードの情報の登録状況として最もあてはまるものを次の中から選んでください。（ひとつだけ）

１．サイトを信頼して登録している
２．多少の不安はあるが、便利なので登録している
３．登録しないとサービスを利用できないので、登録している
４．登録はしないで、利用するたびにクレジットカード情報を入力している

Q１６　Q４「ユーザー登録をしたことがあるサイト」で「SNS サイト」を選択した方にうかがいます。SNS サイトを利用する場合に、気にすることはありますか？最もあてはまるものを次の中から選んでください。（ひとつだけ）

１．登録した個人情報や書き込みの内容がインターネット等に流出しないか
２．登録した個人情報等を、知らない人に見られないか
３．書き込んだ日記や写真等が消えてしまわないか
４．サービスが停止して、使えなくならないか
５．その他
６．特にない

Q１７　Q４「ユーザー登録をしたことがあるサイト」で「フリーメールサイト」を選択した方にうかがいます。フリーメールサイトを利用する場合に、

気にすることはありますか？最もあてはまるものを次の中から選んでください。（ひとつだけ）

1．送受信したメールのタイトルや本文がインターネット等に流出しないか
2．送受信したメールアドレスやアドレス帳がインターネット等に流出しないか
3．送受信したメールやアドレス帳が消えてしまわないか
4．サービスが停止して、使えなくならないか
5．その他
6．特にない

Q１８　ユーザー登録をしなくてもサービスを利用でき、会員になればそれ以上のサービスを利用できるインターネットサイトがあるとします。あなたはそのようなサイトにユーザー登録（無料）すると思いますか？（ひとつだけ）

1．登録することが多いと思う
2．登録しないことが多いと思う
3．わからない

Q１９　前問で「登録することが多いと思う」を選択した方にうかがいます。どのような場合に登録しようと思いますか？最もあてはまるものを次の中から選んでください。（ひとつだけ）

1．会員割引やポイント等のサービスがある場合
2．サービス関連情報やダイレクトメールが欲しい場合
3．今後、よく利用することになりそうな場合
4．会員しか使えないサービスや機能をぜひ利用したい場合
5．その他

Q２０　前問で「登録しないことが多いと思う」を選択した方にうかがいます。登録しようと思わない理由として最もあてはまるものを次の中から選んでください。（ひとつだけ）

1．ユーザー登録の入力作業などが面倒だから
2．ユーザーID やパスワードの管理が面倒だから

３．そのサイトをまた利用することは無さそうだから
４．個人情報はできるだけ入力したくないから（情報流出が気になるから）
５．ユーザー登録しなくても十分なサービスを受けられそうだから
６．その他

Q２１　あるサイトＡにユーザー登録すると、他のサイトＢやサイトＣもユーザー登録なしで利用できるサービスがあるとします。このようなサービスを利用してみたいと思いますか？（ひとつだけ）

１．利用してみたいと思う
２．利用してみたいと思わない
３．わからない

Q２２　「あるサイトＡにユーザー登録すると、他のサイトＢやサイトＣにもユーザー登録なしで利用できるサービス」を利用してみたいと思う理由を教えてください。（ひとつだけ）

１．サイトＡが信頼できるサイトであれば、サイトＢ、サイトＣも信頼できそうだから
２．何度もユーザー登録をする手間が省けるから
３．いろいろなサイトに個人情報を登録したくないから
４．ユーザーID やパスワードをこれ以上増やしたくないから
５．その他

Q２３　「あるサイトＡにユーザー登録すると、他のサイトＢやサイトＣにもユーザー登録なしで利用できるサービス」を利用してみたいと思わない理由を教えてください。（ひとつだけ）

１．サイトＢやサイトＣが信頼できるとは限らないから
２．利用するサイトごとにユーザーID やパスワードを使い分けるのが苦にならないから
３．サイトごとにユーザーID やパスワードを使い分けたいから
４．サイト Ａ に登録した情報などが他のサイトで利用されることに不安を感じるから
５．その他

Q２４　ユーザー登録をした検索サイト（サイトA）で検索すると、あなたの好みや興味に合いそうなサイト（サイトB）が上位に出て、サイトBにユーザー登録をしなくても利用できるサービスがあるとします。このようなサービスを利用してみたいと思いますか？（ひとつだけ）

１．利用してみたいと思う
２．利用してみたいと思わない
３．わからない

Q２５　同じSNS(サイトA)にいる友人から紹介された会員サイト(サイトB)にあなたが興味を持っている場合、サイトBにユーザー登録をしなくても利用できるサービスがあるとします。このようなサービスを利用してみたいと思いますか？(ひとつだけ)

１．利用してみたいと思う
２．利用してみたいと思わない
３．わからない

Q２６　前問までのようなサービスを利用する場合、サイトAが持つユーザー情報（個人情報やポイント情報等）が、サイトBやサイトCへ提供される場合があります。ユーザー情報の提供にあたり、どのような対応をサイトAにしてほしいと思いますか？最もあてはまるものを次の中から選んでください。（ひとつだけ）

１．ユーザー情報を提供する場合があることが、利用規約等に書いてあればよい
２．ユーザー登録する時に、わかりやすい説明が欲しい
３．ユーザー情報をサイトBやサイトCへ提供するたびに、毎回説明が欲しい
４．サイトBやサイトCへユーザー情報の提供をして欲しくない（必要な場合に毎回入力する方がよい）
５．サイトの信頼性を評価するランキングや、信頼性を示すもの等があるとよい
６．その他

Q２７　ショッピングやサービスのサイトで、あなたが過去にどのようなものを

利用したか、最近どのようなページを見たか等の情報を元に、あなた個人に対するオススメ商品やサービス情報などを提供してくれるとします。このようなサービスを提供してもらうために、あなたの情報をサイトに知らせることについて、どう思いますか？最もあてはまるものを次の中から選んでください。（ひとつだけ）

1．オススメ情報等のサービス向上に役立つのであれば、知らせてもかまわない
2．信頼できるサイトであれば、知らせることは気にならない
3．信頼できるサイトであっても、知らせたくない
4．わからない

Q２８　インターネットサイトやサービスを利用する上で、あなたの個人情報やその他の情報が使われる時、どのようなことが最も気になりますか？（ひとつだけ）

1．サイトやサービスの提供者や親会社、グループ企業などが信頼できること
2．サイトやサービスの具体的な内容に不審な点がないこと
3．どの情報をどのように利用するのかが明確に表示されていること
4．情報の利用の可否を自分で選べる・いつでも変更できること
5．その他
6．自分が使いたい商品やサービスがそのサイトで提供されていれば、特に気にならない

Q２９　あなたは、どのようなインターネットサイトであれば、信頼できると思いますか？最もあてはまるものを次の中から選んでください。（ひとつだけ）

1．テレビや新聞等で紹介されたサイト
2．友人などから紹介されたサイト
3．インターネットのクチコミサイト等で評判が良いサイト
4．信頼できるサイトからリンクされているサイト
5．検索で上位に出てくるサイト
6．ユーザー登録の解除（退会）の方法が明示されているサイト
7．個人情報の扱いが明示されているサイト

８．サービス内容等に関する問い合わせの連絡先が明示されているサイト
９．運営者の情報（企業名や住所など）が十分に開示されているサイト
１０．その他

総務省情報通信政策研究所（調査研究部）

http://www.soumu.go.jp/iicp/

〒100-8926　東京都千代田区霞ヶ関 2-1-2
中央合同庁舎第 2 号館 11 階
TEL:03-5253-5496　FAX:03-5253-5497