「インターネット取引に係る個人認証技術を巡る動向」

市川類@JETRO/IPA NY

１．はじめに

近年のインターネットの普及により、一般的な情報の発信や収集だけでなく、バンキングやショッピングなどの取引や個人へのサービス提供が、インターネットを通じて行われるようになってきているが、これらの取引を安心して行うにあたって、個人認証技術は、根幹をなす重要な技術と位置付けられる。

これらの個人認証技術は、現在、情報セキュリティや ID 窃盗等に係る問題全体の中で、その不備が必ずしも大きな問題とされている訳ではない。しかしながら、近年、社会の情報化が進展し、インターネットでの取引の増大に伴うにつれ、特に資金の取引を伴う金融機関や電子商取引を行う企業を中心に、その重要性は、相対的に高まってきている。

このような中、米国においても、もちろん、各企業が、それぞれ求められるセキュリティ水準や連邦政府の基準に踏まえて、導入を進めているが、その際、単にセキュリティを一方的に強化するのみではない点が特徴であると考えられる。すなわち、それぞれのユーザーにおける利便性やコストも踏まえつつ、各社とも柔軟に対応していること、また、特に、米国が強い競争力を有するインターネットサービス企業においては、各社のそれぞれの競争優位を踏まえつつも、広い意味でのセキュリティの確保（すなわち、ユーザーパスワードの増大はセキュリティ上も問題）にも資するシングルサインオン（SSO）システムに向け連携をしようという動きも起こっていることが挙げられる。また、これらの動きに係る技術基盤には、従来からの連邦政府の取り組みが大きな役割を果たしている。

本報告書では、これらの、米国におけるインターネットにかかわる個人認証技術・システムをめぐる最近の動向について紹介する。

２．個人認証技術について

（１）個人認証技術の位置付け

＜個人認証技術の各種システムでの位置付け＞

個人認証技術とは、コンピュータ等にアクセスする際に、そのアクセスしている個人が本人であるか否かを確認する技術であり、これにより、第三者による「なりすまし」を防ぐことを目的とする。

そもそも、個人は、近代経済の取引主体であり、個人を確定することは、当該個人の所有する財産（情報を含む）などの特定と同じであり、経済上の取引にあたっての前提となる。したがって、コンピュータ上でこれらの財産にかかる取引や情報の処理を行うにあたっても、個人を正確に認証することは取引の前提条件となる。このような観点から、特に経済の IT 化が進展し、あらゆるものがコンピュータを通じて情報として取引されるようになる中で、この個人認証技術は、基本的な技術であると位置付けられる。

このような個人認証技術は、一般的に、企業内システムにおける従業員のアクセス、あるいは、企業＝個人（消費者）間の取引における個人（消費者）のアクセスにおいて利用される[1]。これらは、具体的には、なりすましによる以下のような被害を防止しようとするものである。

個人認証技術の利用分野

対象取引	システム	被害
企業内管理	企業系システム（企業内）	権限のない従業員等による不正アクセス等 ・企業秘密の流出
企業＝個人間取引	企業系システム（店舗など）	第三者のなりすましによる不正アクセス ・口座情報など直接的な金銭的な被害 ・個人情報による間接的な金銭的な被害[2]。 ・個人情報（プライバシー）の問題
	インターネット系システム	

本稿においては、主に、後者の企業＝個人間取引のうち、インターネット系のシステムを経由したアクセスについて取り扱う。

＜個人認証技術の要素＞

個人認証技術は、一般的に、生体認証、所有物認証、知識認証のいずれか又はそれらの組み合わせによって行われるが、特にオンラインでの個人認証技術は、少なくとも現時点では知識などの「情報」に大きく依存することが特徴である。

一般的に、対面で取引をする場合には、顔などから個人的特徴をもとに個人を認証（生体認証）することになり、また、場合によっては、併せて、印鑑や身分

[1] 一般的に、企業内システムの場合は、ローカル環境へのログイン（ネットワークや他のデバイスを介さない場合、たとえばコンピュータへのログインなど）が、また、企業系システムの場合は、リモート環境へのログイン（ネットワークや他のデバイスなどを介して認証を行う場合、たとえば電子メールアカウントへのサインインなど）が多い。

[2] 具体的には、盗難された個人情報に基づく、クレジットカードの新規作成や携帯電話の新規契約とその使用、偽小切手の発行、盗んだ社会保障番号を使用して職を得たり、住宅を賃貸するなどの被害など。
http://www.consumer.gov/sentinel/trends.htm

証明書などで認証（所有物認証）することになる。資金面での取引の場合には、現金を所有しているか、あるいは、小切手の場合は、印鑑、サイン（署名）があるかで本人であるかを確認する。

これに対し、コンピュータにアクセスする場合は、同じように、生体認証、所有物認証に加えて、知識認証（パスワード、暗証番号など）が追加されることが特徴である[3]。具体的には、以下のとおり。

個人認証にかかる要素（例）

	対面取引	企業系システム	インターネット系
生体認証	視認、サイン	生体認証技術	（生体認証技術）
所有物認証	鍵、印鑑、身分証明書 現金	ID カード 銀行・クレジットカード	ID（ログインネーム）、トークン
知識認証		パスワード（暗証番号等）	パスワード（暗証番号等）

このうち、企業系システムについては、ID カード、各種カードなどの物理的な所有物認証と、パスワードなどの知識認証の組み合わせに加え、もっとも確実であるとされる生体認証技術[4]の導入が近年進みつつある[5]。

一方、これに対して、インターネット系システムでの認証において、最も一般的に使われている認証方法は、ID とパスワードの組み合わせによって行われる一要素認証である[6]。これは、インターネット系のシステムの場合は、一般的に、端末として PC を利用するものであり、PC において生体認証（や所有物認証）が可能となるようなハードウェアが、コスト面等[7]により、各インターネットユーザには普及していないことが要因として挙げられる[8]。このため、これらの認証として利用される要素としては、一般的には、パスワードなどのキーボードで入力可能

[3] http://www.securityfocus.com/infocus/1513

[4] 生体認証技術としては、指紋に加え、指静脈、掌静脈、虹彩などの認証技術がある。

[5] 例えば、出入系の管理や、店舗での銀行・クレジットカードのシステムなど。また、民間企業だけでなく、連邦政府などの各種システムにも生体認証技術が多く取り入れつつある。ただし、一般的には、生体認証技術に関しては、米国よりも、個人情報保護法などで規制色の強い日本の方が、市場が発展しており、また、ベンダーも日本企業が競争力を有するとされる。

[6] パスワードは知識と考えられ、一方の ID（ログインネーム）は、個人に割り当てられたものであるため、所有物であるとする見方もあるが、ID(ログインネーム)自体は、パスワードと対になって初めて認証要素としての役割を果たすため、認証の主要な要素とみなされず、したがって、ID・パスワードによる認証は、一般的に一要素認証と考えられている。

[7] 生体認証（特に指紋）の場合、ハードウェアに係るコスト面に加え、心理的障壁も大きな要因として挙げられる。

[8] 企業内システムでの事務系のシステムも同じであるが、企業負担による導入が可能であるため、日本などでは導入が進みつつある。

な知識認証（及び情報としての所有物認証）に依存することになる。（そのような中、今後インターネット系のシステムにおいても、生体認証技術を取り込もうとする新たな動きが想定されるが、本稿では取り扱わない。）

＜個人認証技術とセキュリティ＞

これらの個人認証技術は、必ずしも新しい技術ではないが、いずれにせよ、これらの技術を導入すればセキュリティ上完璧となるようなものではなく、いずれにせよ、他人がアクセスする、いわゆるなりすましなどに係る危険性が存在する。

一般的に、対面取引（実世界）においても、なりすましによる被害は、多く、存在する。具体的には、その多くは、物理的な所有物の窃盗によるものであり、例えば、身分証明書の窃盗改ざんや、物理的所有物についても、現金、クレジットカードの盗難などは、昔から存在する大きな問題である。

これに対し、インターネットを通じた取引の場合については、上記の問題に加えて、対面でないが故に、顔（生体）を覚えられる可能性が低いことに加え、①認証の要素となる所有物も「情報」であるため、盗まれやすく、流出しやすいこと、②特に、ローカルと異なって、インターネットの場合は、ネットワークを経由する場合に、そこから流出する可能性があることが、更にセキュリティ上の問題点として追加される。

具体的に、このような個人認証情報が流出する経路としては、一般的には、以下のとおり、管理する企業、ネットワーク、個人からの３通りの経路がある。このうち、特に、インターネット系システムなどリモート環境へのログインの場合、ネットワークを経由していることから、途中で情報が盗まれる可能性が高くなる（（ｂ）による経路。フィッシング詐欺が代表例）。

個人認証情報の流出経路と技術

流出経路	流出情報	流出原因と対応の方向
a) 企業（管理者） ・　企業内システム（ID 管理、ローカルネットワーク）	企業秘密（個人認証情報を含む）	企業内での管理・アクセス体制の強化（個人認証技術の強化を含む） －内部従業員の不手際 －内部犯行者による犯行　等
b) 企業＝個人間のネットワーク ・　企業系ネットワーク ・　インターネット(オンライン)	個人認証情報	個人認証技術の強化 －フィッシング、スパイウェア等 －盗聴　等
c) 個人（利用者）	個人認証情報	個人の不注意の防止、盗難等の防止 －パスワードメモの流出、盗み見 －コンピュータ上のログ　等

（２）個人認証技術を巡る技術的内容

＜個人認証技術の対応の範囲とその限界＞

一般的に、知識認証など情報のみをもとにした認証に基づく場合において、一旦その認証に係る情報がすべて流出してしまった場合、それが第三者の悪意によるものにせよ、個人の不注意によるものにせよ、一般的にはそれを取り戻すことはできず、被害を完全に防ぐ技術は存在しない[9]。

また、前述の表から分かるとおり、個人認証技術とは関係のない経路で流出する場合も多く、個人認証技術のみによって、認証に係る情報の流出を防止することは不可能であり、したがって、これらのセキュリティの確保にあたっては、技術以外の対応が重要になることに留意する必要がある。

しかしながら、そのような中で、インターネットを通じた個人認証において、これらの情報の流出を可能な限り未然に防ぐ手法が、いくつか技術として考案されている。

インターネット上でのセキュリティ強化に係る個人認証技術

問題	対応する技術
ネットワーク上での盗聴	送受信情報の暗号化（公開鍵基盤（PKI）技術等）
フィッシング等による入力情報の流出	入力情報の多重化（チャレンジ質問、トークンなどの二要素認証等）

これらのうち、どの個人認証の方法を使用するかは、ユーザーの使用しているシステム環境と、サービス提供側のネットワークで必要とされているセキュリティのレベルによって異なる[10]。また、トークンや生体認証デバイスなどはセキュリティの信頼性の向上に繋がるが、これらのデバイスの導入には、コストがかかるという欠点もある[11]。

＜送受信情報（データ）の暗号化（PKI）＞

前述の通り、インターネット系など特にリモート環境でログインを行う場合[12]は、ネットワーク上で流通される情報に関して、第三者による不正アクセス（盗聴）が行われる可能性が高まる。この場合に対して、個人認証に係る情報に限定され

[9] この場合は、一般的には、管理者に連絡して口座等を止めてもらい、その上で、流出先、流出経路等の調査（場合によっては、犯罪調査も含め）などを行うことになる。

[10] http://technet2.microsoft.com/windowsserver/en/library/a1f616bf-3784-4363-8b64-95e90f6903e01033.mspx?mfr=true

[11] http://www.securityfocus.com/infocus/1513

[12] なお、一般的に、ローカル環境におけるログインの際には、第三者による情報への不正アクセスが行われる可能性が低いため、PKI が使用されることは稀である。
http://technet.microsoft.com/en-us/library/cc700808.aspx

るものではないものの、これらの情報が第三者に盗聴され情報が流出しても解読されないようにする手法として、データの暗号化がある。

この暗号化処理を安全かつ円滑に行うためのシステム基盤として、公開鍵基盤（Public Key Infrastructure：PKI）[13]と呼ばれる技術がある。公開鍵基盤（PKI）とは、ある 2 者の間で情報の暗号化を行う際に、暗号化に利用する公開鍵の正当性を、信頼できる第三者（当事者とは異なる）が証明するシステムを指す[14]。一般的には、公開鍵と秘密鍵を利用した暗号化技術が利用され、公開鍵の正当性は、認証機関（Certification Authority：CA）と呼ばれる、信頼できる第三者機関が発行する電子証明書により保証される[15]。

＜入力情報の多重化（チャレンジ質問、トークン等）＞

一方、PKI により暗号化がされていても、フィッシング詐欺[16]の場合には、ID やパスワードなど入力された情報が、そのまま第三者にそのまま流出し、他人によるなりすましがなされることから、PKI を利用した暗号化では対応ができない。また、盗聴、解読されなくとも、各ユーザーのパスワード等が容易に推定されるようであれば、認証の正確性や信頼性は低くなる[17]。

このため、従来の ID・パスワード方式よりも強化された認証方法として、フィッシング等により ID とパスワードが盗まれても、本人になりすますことができないようにするべく、ID・パスワードの入力後、それとは別に、更に本人にしか知りえない情報を認証処理に加えるという手法として、チャレンジ質問や二要素・多要素認証の概念・技術が考案されている。これらは必ずしも目新しいものではないものの、具体的には、以下の通り。

- チャレンジ質問による認証。これは、ID・パスワードの入力に加え、更に、ユーザーがあらかじめ設定した質問に対する答えを入力することを求めることによって認証するものである[18]。したがって、単なるパスワードに加え、更に本人しか知りえない情報を、知識認証として追加するものであると言える。

---

[13] http://technet.microsoft.com/en-us/library/cc700808.aspx
[14] http://www.authenticationworld.com/PKI-Authentication/index.html
[15] なお、PKI が脆弱であるとの指摘もある。
http://www.mozilla.org/projects/security/pki/nss/news/vaudenay-cbc.html
https://www.pki.getronicspinkroccade.nl/website/495/Advisory:+Managed+PKI+Client+Security+Vulnerability+Patch.html
[16] フィッシングとは、本物そっくりのダミーサイト上でユーザーに個人情報を入力させ、情報を獲得するもの。フィッシングサイトにだまされて ID・パスワードを入力してしまうと、ID・パスワード方式のみで認証を行っていたサイトでは、被害を防ぐことができない。
[17] http://www.authenticationworld.com/Password-Authentication/
[18] この秘密の質問の内容は、「はじめてのペットの名前は？」「母親の旧姓は？」「子供の頃住んでいた家の番地は？」などであり、パスワードよりも、第三者には推測しづらい内容としている。

・ トークンが生成するワンタイムパスワード（One Time Password：OTP）による認証。トークンとは、キーホルダー型、USB 型、カード型などのハードウェアであり、管理者側の認証システム先のサーバとシステム上でつながっており、ユーザーから ID・パスワードが入力されると、使い捨てでランダムな数字（OTP）を表示する。ユーザーは、ID・パスワードを入力した後、更に、そのトークン上に表示された OTP を入力して認証を行うことになる。したがって、当該 OTP は、本人しか知りえない情報であり、所有物認証であるとみなされる。

このうち、前者のチャレンジ質問は、ある意味で知識認証（パスワード等）を多重化したものであることから、一要素認証であるとされる一方、後者のトークンについては、知識認証（パスワード）に加え、所有物認証を加えたものであることから、二要素認証[19]であるとされる。特に、トークンを使用した OTP は、パスワード発行企業のセキュリティサーバーのみが知る数学アルゴリズムを使用してランダムに発行されるため、信頼性や安全度は高い[20]。

＜その他の新技術＞

なお、二要素認証での新認証要素としては、指紋、虹彩、顔認証などの生体認証、トークンに注目が集まっているが、最近では、ID、パスワードを入力する際のタイピングの癖で認証を行う技術（BioPassword[21]）なども市場に登場している。また、イギリスのロンドン大学クイーンメアリー校コンピューターサイエンス学部の研究チームも 2005 年、マウスを使用してコンピュータ画面上で署名を行い、その筆跡で認証を行うという技術の開発に成功しており[22]、今後はこれらが新たな認証要素となる可能性もある。

（３）個人認証を取り巻く産業構造

①インターネット上での個人認証を巡る産業構造

＜インターネットでの個人認証を利用する企業＞

このような個人認証技術を、インターネットでのビジネスに利用して活用する企業としては、以下の種類がある。

・ 銀行、クレジット会社等の金融機関（インターネットバンキングサービス等）

[19] 二要素認証・多要素認証とは、所有物、知識、生体に係る 3 種類の認証要素のうち、2 つ以上の要素を利用した認証方法を指す。

[20] http://www.authenticationworld.com/Token-Authentication/

[21] 個人認証システムの開発、製品販売、同分野でのコンサルティング業務を行う AdmitOne Security 社による。http://www.admitonesecurity.com/products_kda.asp

[22] http://www.dcs.qmul.ac.uk/~pmco/biometricsummary.pdf

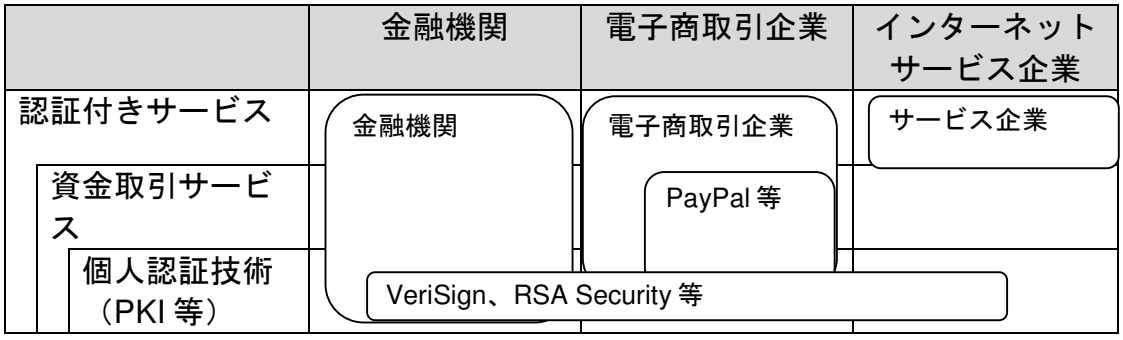
・　電子商取引を行う各種企業（インターネット・ショッピング業者など）
・　インターネットサービス企業（電子メールサービスのプロバイダを含む）

これらの企業においては、それぞれ求められるセキュリティ基準に従って、顧客保護の観点から、信頼性の高い個人認証システムを導入する必要がある。その際、特に、金融機関や電子商取引事業者においては、個人認証に係る情報の漏洩が事業者・ユーザーの双方にとっての金銭的被害に直結することから、一般的には、これらの企業において、より信頼性の高い認証を行うことが求められる。このような理由から、インターネットサービス提供事業や電子メールプロバイダーと比較して、インターネット上で金銭取引を行う企業の場合は、より信頼性・安全性の高い認証システムを導入しているのが一般的である。

なお、電子商取引（特に、小規模企業）企業の一部においては、金銭取引自体が自らのビジネスのコアではないため、個人認証を含む資金取引全体に金銭取引に係る専門サービスである PayPal などの企業に、任せる場合がある。

PayPal は、1998 年に創立したインターネット決済仲介会社であり、2002 年に大手インターネットショッピングサイト eBay に買収されている。PayPal のユーザーはインターネットショッピングの際、PayPal で開設したアカウントを通じて支払いを行う[23]。現在、同システムのユーザー数は全世界に 1 億 6,400 万人、2007 年 6 月の時点での年間取引額は 110 億ドルである。

インターネットを利用した個人認証技術を巡る産業構造[24]



②認証関連ビジネスの動向

＜インターネットインフラ（PKI：認証サービス）＞

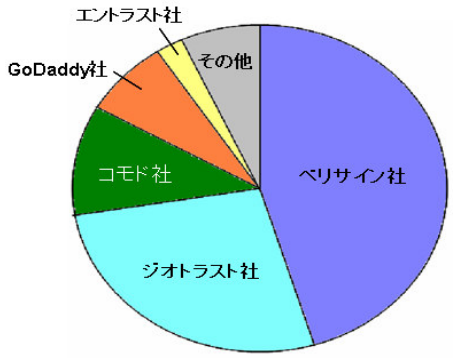
[23] https://www.paypal.com/us/cgi-bin/webscr?cmd=_home-general&nav=0
なお、PayPal を利用することにより、ユーザーは、不必要にクレジット情報を開示する必要もなく、また、クレジット会社と契約のない小企業（個人を含む）も確実にかつ容易に支払を受けることが可能となる。

[24] なお、PayPal は、PKI に関しては、VeriSign 社の発行する電子証明書を利用しており、また、トークンに関しても、VeriSign 社のものを利用している。

これらの個人認証を含むインターネット系のサービスを提供するにあたって、当該個人認証技術は、これらの上記の企業が独自に技術を開発している訳ではない。特に、PKI については、取引の当事者から独立した信頼できる第三者による認証インフラであることから、PKI の提供を専門的に提供するサービス市場が構築されている。

2006 年 6 月に発表された市場調査の結果によると、主要な電子証明書である SSL 証明書発行市場のうち、VeriSign 社は約 45%の市場シェアを獲得しており、また、同年 7 月、同社は市場シェア第 2 位の Geotrust 社を買収している[25]ことから、現在、VeriSign 社の市場シェア合計は 70%近くと、ほぼ独占状態である。

SSL 証明書発行企業の市場シェア（2006 年 6 月）[26]



VeriSign 社（カリフォルニア州）は、1995 年に、RSASecurity 社（マサチューセッツ州）の認証部門が独立する形で創業した企業であり、1998 年に NASDAQ に株式公開をしている。同社は、2007 年の売上は 1496 百万ドルであり[27]、現在、世界 15 カ国に法人拠点を持ち、世界 38 ヶ所で販売拠点を展開している。

同社は、サーバ証明書や認証システム、暗号化など、主にセキュリティに関する製品・サービスで知られている[28]が、その中心となるのが PKI に関連する商品で

[25] http://news.cnet.com/2110-7355_3-6073234.html

[26]出典：http://news.netcraft.com/archives/2007/10/26/netcraft_ssl_survey.html

[27] 同社 10K より。https://investor.verisign.com/annuals.cfm
http://files.shareholder.com/downloads/VRSN/397102870x0x190141/a65a1902-eb6f-414a-b64b-347ea5b59bd0/VeriSign_2007AR.pdf
なお、1496 百万ドルのうち、インターネットでの PKI 認証を含むインターネットサービスグループが 917 百万ドル、コミュニケーションサービスグループが 579 百万ドルとなっており、近年、後者は減少傾向にあるが、前者は増加傾向にある。

[28] なお、企業向け以外に、同社による個人認証向けの電子証明書としては、e メール用セキュア ID、アクロバット用マイ・クレデンシャルの 2 種類がある。セキュア ID は、メールの内容が改ざんされていないことを証明する電子証明書で、マイ・クレデンシャルは、作成されたアクロバットファイルが改ざんされていないことを証明する電子証明書である。

あり、また、同社は、政府機関と取引する外部機関に対して有効な電子証明書を、国防総省から CA として認定を受けて、発行している[29]。

＜二要素認証等に係るベンダ＞

トークンなどに係る二要素認証については、多くのベンダがサービスを提供している[30]が、この中で、RSA Security 社が、二要素認証を含む認証分野でのシェア 70%を獲得しているとされる[31]。

RSA Security（マサチューセッツ州）は、1986 年に RSA Data Security として設立され、暗号などの事業に取り組んでいたが、上記 VeriSign 社を独立させた後は、いくつかの売買収の後、2006 年に EMC 社に買収され、現在は、EMC 社のセキュリティ部門としての位置付けになっている。2007 年の同社のセキュリティ部門の売上は、525 百万ドルであり、同部門は、Fortune 500 の 90%以上の企業を顧客に持っている[32]。同社は、主として金融機関向けにビジネスを展開しており、後述する FFIEC のガイドラインの制定に伴い、金融機関向けの売上が急増し、世界全体で 3500 以上の金融機関が利用にするに到っているとされる[33]。

なお、上記の VeriSign 社は、PKI だけでなく、トークンの提供も行っている。このトークンを購入したユーザーは、同社のトークン・ネットワーク対応ウェブサイトにて、所有するトークンの登録を行う。トークンの登録は利用ウェブサイトごとに行うが、1 つのトークンで複数のウェブサイトへの登録が可能であり[34]、また、インターネット関連企業に比較的多くサービスを提供している。

３．個人認証技術を巡るセキュリティの現状と政府の動き

（１）個人認証技術を巡るセキュリティの現状

インターネット利用の普及に伴い、個人情報の盗難・なりすまし犯罪など、情報の信頼性や機密性に関連する問題も数多く発生している[35]。しかしながら、全体のセキュリティを巡る問題の中で、個人認証技術の不備が、大きな割合を占めている訳では必ずしもないが、相対的重要性は、着実に増加しつつある。

---

[29] http://www.verisign.com/authentication/government-authentication/eca-certificates/index.html
なお、DODの認定を受けているCAは、VeriSign社に加え、Operational Resource Consultant社、IdenTrust社の３社のみ。

[30] 具体的には、RSA Security 社、VeriSign 社、Entrust 社、Aladdin Knowledge Systems 社、Cryptomathic 社、Vasco 社　など。

[31] https://info.rsasecurity.com/2007Am/webcast/070327ESG/webcast_slides.pdf　p27

[32] http://japan.rsa.com/node.aspx?id=1003

[33] http://journal.mycom.co.jp/news/2007/04/25/003/

[34] https://idprotect.verisign.com/learnmoredemo.v

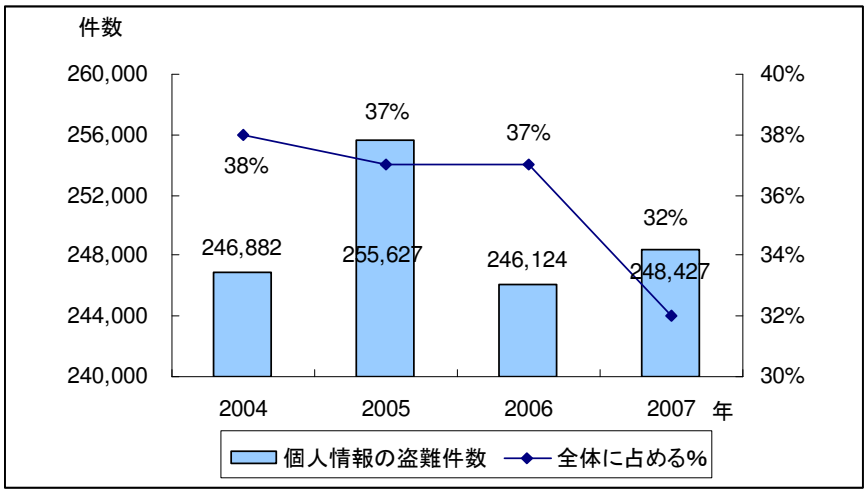
[35] USA Today, “Technology cuts down on Web resistrations; OpenID lets consumers have only one user name and password,” March 16 2008, Obtained via Nexis.

①消費者から見た被害の状況

＜消費者詐欺に係る苦情に対する個人情報の盗難、なりすまし＞

2007 年に米国連邦取引委員会（Federal Trade Commission：FTC）に寄せられた消費者詐欺（Consumer fraud）に係る苦情のうち、約 32%（24.8 万件）が、個人情報の盗難・なりすまし犯罪に関するものであった[36]。件数は増減を繰り返しているが、苦情全体に対するその割合は、2004 年以降僅かながらも減少傾向にある。

個人情報の盗難・なりすまし犯罪に関する苦情件数と全体に占める割合[37]



ただし、この中で、ID 窃盗・詐欺におけるインターネットを通じたものの割合は、必ずしも多いものではない。金融サービス企業を主なクライアントに持つリサーチ・コンサルティング企業である Javelin Strategy & Research（カリフォルニア州プレザンプトン）が 2008 年 2 月に発表した調査結果によると、2007 年に発生した ID 窃盗で原因が明らかになっているケース（全体の 35%）のうち、ハッキングやウィルス、スパイウェアなどを含む、インターネット上での活動が原因とされるものは全体の 12%となっている[38]。なお、ID 窃盗による 2007 年の被

[36] それ以外には、自宅への訪問販売、カタログ販売、インターネットを介した販売（オークションなども含む）、ローン詐欺などが含まれる。
USA Today, “Technology cuts down on Web resistrations; OpenID lets consumers have only one user name and password,” March 16 2008, Obtained via Nexis.

[37] 出典：Federal Trade Commission の情報をもとに作成。
FTC, “Consumer Fraud and Identity Theft Complaint Data,”（FY 2006and 2007）
http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2007.pdf
http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2006.pdf

[38] 一方、財布やクレジットカード・デビットカードの紛失や盗難が原因とされるケースは全体の 33%、その他、窃盗された郵便物や友人知人などの顔見知りによる ID 盗難を含めたオフライン全体での盗難は、全体の 81%に上っている。

害総額（インターネット以外のものも含む）は前年の 493 億ドルから約 450 億ドルへ、平均損失額は前年の 5,920 ドルから 5,574 ドルへ、被害者数も前年の 840 万人から 810 万人へと減少している[39]。

＜フィッシング詐欺の動向＞

このようなインターネットを通じた個人認証関連情報の盗難のうち、フィッシング詐欺については、若干増加傾向にある。

調査会社である Gartner が 2007 年 12 月に発表した調査[40]によると、2007 年 8 月までの 1 年間でフィッシング詐欺によって金銭的被害を被った被害者の数は、前年の 230 万人から 360 万人と増加し、フィッシング詐欺による年間被害額は、2006 年の 23 億ドルから 32 億ドルに増加した[41]（ただし、1 件あたりの平均被害額は、前年の 1244 ドルから、886 ドルに減少）。なお、計 360 万人の被害者のうち、160 万人が損失額の 64%を、犯罪者側あるいは企業側から取り戻すことができたとされる。

②企業側から見た被害の動向

＜企業におけるサイバー犯罪被害＞

他方、消費者からではなく、企業から見たサイバー犯罪による被害額から見た場合、一般的には減少傾向にあるとともに、特に個人認証関連の情報による被害は、むしろインターネットを通じた流出というよりは、内部従業員の不手際や内部犯行者によるものが大半である。

米コンピュータ・セキュリティ研究所（Computer Security Institute：CSI）と FBI が企業・組織を対象に毎年行っている共同調査（2007 年 9 月発表）[42]によると、これまで減少傾向にあったサイバー犯罪の被害額平均は、2006 年には、35.4 万ドルと増加傾向に転じた[43]。回答企業が経験した代表的なサイバー犯罪の種類

---

[39] Javelin Strategy & Research, “2008 Identity Fraud Survey Report,” February 2008.
http://www.idsafety.net/803.R_2008%20Identity%20Fraud%20Survey%20Report_Consumer%20Version.pdf
http://blog.trustedid.com/?p=551

[40] http://www.gartner.com/it/page.jsp?id=565125
http://www.itmedia.co.jp/enterprise/articles/0712/18/news017.html、
http://www.computerworld.jp/news/sec/91809.html

[41] なお、同社が過去に行った同様の調査では、2004 年のフィッシング詐欺による平均被害額は 257 ドル、2004 年 6 月から 2005 年 5 月にかけてのフィッシング詐欺における被害者数は 120 万人、被害総額は 9 億 2,900 ドルであったとされる。したがって、フィッシング詐欺については、引き続き増加傾向にある。
http://www.gartner.com/it/page.jsp?id=498245
http://www.gartner.com/press_releases/asset_129754_11.html

[42] http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

[43] 2003 年は、52.5 万ドル、2004 年は 20.4 万ドル、2005 年は 16.7 万ドルと減少していた。
http://itpro.nikkeibp.co.jp/article/COLUMN/20060731/244732/
http://itpro.nikkeibp.co.jp/article/USNEWS/20060714/243466/

（複数回答）としては、「内部犯行者によるネットワークへの不正アクセス」が 59%、「ウィルス攻撃」が 52%、「ノート PC・モバイルの損失･盗難」が 50%、「フィッシング詐欺」が 27%[44]「情報への不正アクセス」が 25%となっており、その他、「パスワードの漏洩」（10%）、「知的財産の盗難」（8%）なども見受けられた。なお同調査では、今後 2 年間での最大の懸念事項として、データ保護やフィッシング対策、アイデンティティ・アクセス管理などが上がっている。

＜金融機関における被害＞

そのような中で、金融機関においては、インターネットを通じた個人認証情報の流出は、重要な課題となりつつある。

Gartner 社（2008 年 6 月）の調べ[45]によると、銀行の詐欺の中では、電子資金取引に際する個人情報の盗難が、トップとされる。また、FDIC（米国預金保険機構）が、2008 年 2 月にまとめた事故報告書によると、2007 年第 2 四半期に起こった、5000 ドル以上の被害を被った金融機関への非権限アクセス事件は全部で 536 件、こうした非権限アクセスによる金融機関の被害は増大している[46]。

このような中、上記 Gartner 社の調査によると、米国の金融機関が不正取引防止[47]のために行っている取り組みのうち、1 位はオンライン上での不正取引の発見であるが、それに次いで 2 番目に投資額の多いものは、オンライン取引における本人認証であり、今後、不正取引防止と本人認証[48]の強化に費やされる出費額は、2008 年と 2009 年には更に増加するとの見込みとしている。

（２）連邦政府における個人認証技術を巡る取組み

このような中、連邦政府は、インターネット利用の促進の観点から、従来から、個人認証技術に関し、民間企業と連携して当該技術の開発を進めるとともに、連邦政府あるいは金融機関向けのガイドライン等を発行してきている。以下に、連邦政府による取り組みの例を挙げた。

①米国国立標準研究所（NIST）：政府機関を中心とした導入

＜1990 年代の動き＞

[44] 今回から、新たに調査に追加されている。
[45] 米国の 50 銀行による、詐欺行為への対応策と顧客認証手段に関する調査。
http://www.gartner.com/it/page.jsp?id=721009
[46] http://headlines.yahoo.co.jp/hl?a=20080805-00000011-vgb-secu
[47] オンラインかそうでないかを問わない。
[48] オンライン･オフラインを問わない。

インターネット上での個人認証技術に関しては、米国国立標準研究所（National Institute of Standards and Technology：NIST）が、1990 年代前半とかなり早い段階から、スマートカードやトークンなどを使用した認証システム導入の必要性を指摘するとともに[49]、主に各種政府機関に対し、インターネット上で情報を取り扱う際のセキュリティ・ガイドラインを発行している。その中で、個人認証の他にも、情報の暗号化や、有効な個人認証の方法の１つとしてのトークンの利用を挙げており、また、これらのガイドラインは、ビジネス用にも参考にされている[50]。

また、このようなガイドライン等の発行と併せて、NIST は、PKI やトークンなどの技術の開発を、民間企業と共同で行っており[51]、これらの技術は、国防総省を含む連邦政府の各省庁において先進的に導入されている。

＜2000 年代の動き＞

2002 年 12 月に制定された「連邦情報セキュリティマネジメント法（FISMA：Federal Information Security Management Act of 2002）により、各種政府機関及び連邦政府機関から業務委託を受けている民間企業は、情報セキュリティを強化するためプログラムを策定、実施することが義務付けられるとともに、NIST に対して、そのための規格やガイドラインの策定、開発が義務付けられた。

そのような中で、個人認証に関する政府の取り組みとしては以下の 2 つが挙げられる。

・ 「連邦政府機関向けの電子認証にかかわるガイダンス（E-Authentication Guidance for Federal Agencies：2003 年[52]）」これは、1998 年政府ペーパーワーク削減法に基づき、行政予算管理局（Office of Management and Budget：OMB）が 2003 年 12 月に発表したものであり、各連邦機関が導入すべき認証レベルを決定するための手引きとして、個人認証を必要とする電子取引が失敗

[49]例えば、NIST は、1994 年の広報の中で、オンライン上での認証には、情報漏えいの可能性がついて回ることを指摘し、より強力な認証方法として、ワンタイムパスワードを紹介している。
http://csrc.nist.gov/publications/nistbul/csl93-07.txt
http://csrc.nist.gov/publications/nistbul/csl94-05.txt

[50] 政府機関に対する認証強化の提言の例としては、以下のようなものが挙げられる。
NIST, “HCFA INTERNET SECURITY POLICY,” November 24, 1998,
http://csrc.nist.gov/groups/SMA/fasp/documents/policy_procedure/internet_policy.pdf
http://www.ocio.usda.gov/directives/doc/DR3140-002.htm
これは、連邦医療財政局（Health Care Financing Administration：HCFA）でのインターネットの利用の拡大を受け、NIST が、同機関が管理する個人情報をインターネット上で送受信する際のガイドラインを定めたものである

[51] 具体的には、例えば、1996年には、PKIに関しては、VeriSign社を含む10社との共同研究を発表している。
http://www.nist.gov/public_affairs/releases/n96-24.htm
http://www.imc.org/imc-pfl/mail-archive/msg00068.html

[52] http://eap.projectliberty.org/docs/E-Auth_Guidance_final_12-16-03.pdf

した際のリスクを特定、4 つの認証レベルを設定し、リスクと認証レベルの相関関係を明確化している。

・ 「電子的認証に関するガイドライン（Electronic Authentication Guideline：2006 年[53]）」これは、2006 年 4 月に、上記ガイダンスを踏まえて、NIST が発行したものであり、前文書で定義された各レベルで使用することが許可されている認証システムを決定している。詳細は以下の通り。

認証レベルと使用可能な認証システム

認証の種類	レベル 1	レベル 2	レベル 3	レベル 4
ID 及びパスワード	○	○		
OTP 生成トークン	○	○	○	
コンピュータに保存された暗号鍵[54]	○	○	○	
ハードウェアに保存された暗号鍵[55]	○	○	○	○

これらのガイドラインは、原則として、連邦政府機関職員がリモート環境から政府のシステムへのログインを行う際の手引きであるが、これらで示された技術は、官との連携する民間事業や、ベンダを通じて、民間企業にも普及されていくことになる。

②連邦金融機関調査委員会（FFIEC）：民間金融機関での取り組みの推進

一方、連邦政府による、民間企業向けに対する取り組みとしては、連邦金融機関調査委員会（Federal Financial Institutions Examination Council：FFIEC）が、2005 年 10 月に、特にインターネットバンキングを提供する金融機関に対して、ガイドライン「Authentication in an Internet Banking Environment」を発行している[56]。この 2005 年のガイドラインは、それ以降、顧客の情報保護に関する法制度と技術が変化したことや、近年インターネット上での詐欺や個人情報の盗難が増加していること、当時と比較して高性能な認証システムが開発されたことなどを受け、発行されたものである。

このガイドラインの中では、口座詐欺や個人情報の盗難は、一要素認証システムのセキュリティの脆弱さに起因するとの指摘し、そのため、インターネットバンキングサービスを提供する金融機関に対し、インターネット取引のリスクに見合ったセキュリティ・認証システムとしての二要素認証の導入を促し、具体的に

[53] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
[54] 通常、この鍵の起動にはパスワードの入力が必要となる。
[55] この鍵の起動には、パスワードもしくは生体情報の入力が必要となる。
[56] なお、FFIEC は 2001 年にも同タイトルのガイドラインを発表している。また、同ガイドラインは、FFIEC が 2002 年 12 月に発行した、「Information Technology Examination Handbook」とも連動している。

は、同委員会を構成する 5 連邦機関[57]の管轄下にある全ての金融機関に対し、2006 年 12 月末までに例外なく二要素認証システムを導入するよう求めている[58][59]。

その上で、リスクアセスメント、顧客認証、監視・通達、顧客意識の向上などをいかにして行うべきかを解説している。（Appendix では、チャレンジ質問、トークン、生体認証など様々な認証方法を紹介している。）

③その他の連邦政府の動き（罰則の強化など）

上記のようなガイドライン以外においても、連邦政府においては、個人認証に関しては、近年 ID 窃盗に関して、罰則を強化するなどの対策に取り組んでいる。

具体的には、2004 年 7 月、ブッシュ大統領は、ID 窃盗罰則強化法に署名している[60]。また 2006 年 5 月 10 日、ブッシュ大統領の大統領命令により、司法長官と FTC 長官を議長とする Identity Theft Task Force が設立され、同タスクフォースは 2007 年 4 月、ID 窃盗対策戦略計画（COMBATING IDENTITY THEFT： A Strategic Plan）を発表した[61]。同計画では、以下のような戦略を打ち立てている。

- ID 窃盗のターゲットとなりやすい社会保障番号（SSN）をむやみに政府機関が使用しない。
- 民間企業が収集し保管する個人データへの保護プロセスと、情報漏洩が発生した場合の被害者への通知方法について、全国規模の基準を設ける。
- ID 窃盗防止、探知、保護対策について、政府機関が消費者、企業、公的機関を教育する大規模なキャンペーンを実施する。

---

[57] 連邦準備制度、連邦預金保険会社、全米信用組合管理局、通貨監督庁、金融監督局の 5 連邦機関。

[58] FFIEC, “Authentication in an Internet Banking Environment,” http://www.ffiec.gov/pdf/authentication_guidance.pdf

具体的には、以下の点をポイントとしている。

- 5 連邦機関としては、ハイリスクの取引に関しては、一要素認証では不十分であると考える。実際、アカウント詐欺や個人情報の盗難は、一要素認証の結果として生じていることが多い。
- したがって、リスク評価に基づき一要素認証では不十分と判断される分野において、金融機関は、それらのリスクを低減するべく、多要素認証、多層化（Layered）セキュリティ、もしくは他の手法を導入するべきである。
- 具体的には、金融機関は、定期的に、以下のことを行うべきである。
  - 自らの情報セキュリティプログラムにおいて、①インターネットサービス・製品に係るリスクの特定と評価、②リスクを低減させるための行動措置の明確化、③顧客の認識を高めるための措置と評価、を確保すること。
  - 必要あれば、技術の進化、顧客情報の機密性、情報に係る内外からの脅威等を踏まえて、この情報セキュリティプログラムを適宜更新すること。
  - 実際に、適切なリスク軽減プログラムの導入を実行すること。

[59] http://www.csialliance.org/publications/csia_whitepapers/CSIA_FFIEC_Get_Facts_November_2006.pdf

[60] http://journal.mycom.co.jp/news/2004/07/16/007.html

[61] http://www.idtheft.gov/reports/StrategicPlan.pdf、http://www.ftc.gov/opa/2007/04/idtheft.shtm、http://www.itmedia.co.jp/news/articles/0704/25/news015.html

・　「National Identity Theft Law Enforcement Center」を設置し、法的機関が互いに協力してより効率よく情報を共有、捜査に当たる。

また、その後、司法省（DOJ）の支援の下、ID 窃盗に対する罰則を更に強化する法案[62]が上院で成立している（2007 年 10 月[63]、2008 年 7 月[64]）。

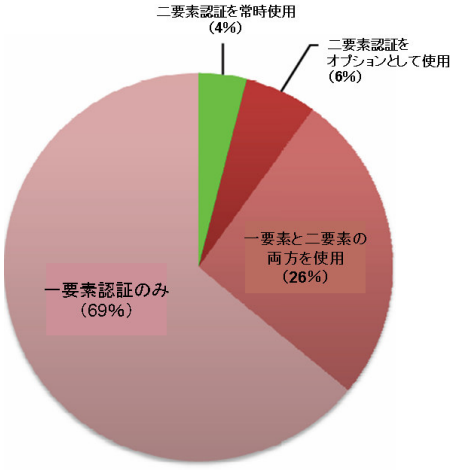
４．個人認証システムを巡る産業界の動き

（１）金融機関、電子商取引企業における動き

①金融機関における動き

前述のとおり、FFIEC は、2005 年のガイドラインにより、インターネットバンキングを提供する金融機関に対し、2006 年 12 月末までに例外なく二要素認証システムを導入するよう求めていた。また、Network World 誌は、2008 年の注目技術の１つとして二要素認証を選出している[65]。

インターネットバンキングを提供する金融機関が導入している認証システム[66]



[62] Identity Theft Enforcement and Restitution Act of 2007（S. 2168）
[63] http://arstechnica.com/news.ars/post/20071017-identity-theft-bill-would-allow-consumers-to-seek-restitution.html
http://www.govtrack.us/congress/bill.xpd?bill=s110-2168
[64] http://leahy.senate.gov/press/200807/073108a.html
[65] http://www.networkworld.com/research/2008/011408-8-techs-authentication.html?fsrc=rss-security
[66]出典：Sestus Data Company

しかしながら、Sestus Data Company による 2007 年の調査（上図）[67]によると、二要素認証はスタンダードとして、徐々に定着し始めているようではあるものの、全顧客向けに導入している金融機関は僅か 4%であり、一部でも導入している機関は 36%にしか過ぎない。一方、調査対象 100 金融機関中、67 機関が、チャレンジ質問による個人認証を行っている。

このような意味で、各金融機関は、二要素に対応するかどうかは別にして、ID とパスワード以外の本人にしか知りえない情報の入力を、認証プロセスに含めるといった方向に動いているのは間違いないとは考えられるものの、その手法については、かなり柔軟な対応を行っているものと評価できる[68]。

これは、金融機関にとって、そもそも、セキュリティの強化に関しては、自らが受ける金銭的被害[69]に加え、個人情報の盗難などで顧客が被害を被り、企業の信頼が失われるのを避け、顧客からの信頼を高めることなどが、導入の動機として挙げられる。一方で、顧客にとって利用しやすいシステムでなければ、顧客離れが起きる可能性もあり、その中で、コスト面も踏まえつつ、各社が最も望ましいと判断されるものがそれぞれ試行錯誤の中で多様なシステムが導入されつつあるものと考えられる。

各金融機関の多重認証に向けた取り組み（本稿の事例）

金融機関名	要素数	2 要素目の種類	ID・パスワード以外に必要な情報
Citibank（法人顧客等）	2	トークン（OTP）	OTP
（普通顧客）	1	N/A	N/A
Bank of America	2	携帯電話（OTP）	サイトキー[70]、OTP、チャレンジ質問**
Capital One	2*	トークン（OTP）	チャレンジ問題**
American Bank	1	N/A	アクセスコード、OTP*
ING ダイレクト	1	N/A	チャレンジ質問、イメージ及びフレーズ

* 希望者のみの利用

** 登録したコンピューター以外からのアクセス時のみ必要

[67] Sestus Data Company, “Trends in U.S. Multi-Factor Non-Compliance,” June 21 2007, http://www.phishcops.com/docs/Trends_in_MFA_NonCompliance.pdf

[68] http://www.nri.co.jp/opinion/it_solution/2007/pdf/IT20070909.pdf

[69] 現時点で、責任論に関しては、ケースバイケースになる。たとえば Bank of America の場合、インターネットバンキングにおいて、顧客の許可なく取引が行われた場合、顧客に対して免責額ゼロを保障しています。一方、Citibank は免責額に関しては言及していないものの、問題解決に向け、無料で調査を行うなどしている模様。

[70] ING ダイレクトの「イメージ」と機能・役割的に同じ。

＜チャレンジ質問による認証＞

チャレンジ質問を採用している事例として、世界的に展開しているインターネットバンクである、ING ダイレクトがあげられる。同社のシステムにログインする場合、ユーザーは ID を入力して最初の認証を行った後、あらかじめ登録したチャレンジ質問の回答を 2 つ入力して更なる認証をうける。

ING ダイレクトへのログインの流れ[71]

最後のステップでは、登録時に各ユーザーが選択したイメージとフレーズを確認し、この 2 つが正しければ、パスワードを入力してログインを完了する。イメージ及びフレーズは、ユーザーと ING ダイレクトしか知りえない情報であるため、この 2 つが正しい限り、そのページがダミーである心配はない[72]。

CapitalOne 社のインターネットバンキングサービスの場合は、通常の認証は ID・パスワードの入力のみで行うものの、その顧客の通常のログイン様式とは異なる方法でログインが行われる場合にのみチャレンジ質問を利用している。具体的には、インターネットバンキングのページ上で複数のチャレンジ質問の中から 3 つを選択し、その答えを事前に登録しておく。この質問は、顧客が普段インターネット取引を行うコンピュータとは違うコンピュータからログインを行う場合などに出題され、利用者は ID・パスワードに加えてこのチャレンジ質問の回答を入力しなければならない。質問とその回答はインターネットバンキングページで変

[71] 出典：ING ダイレクトホームページ http://home.ingdirect.com/
[72] https://home.ingdirect.com/privacy/privacy_security.asp?s=newsecurityfeature

更することが可能だが、利用者は、チャレンジ質問を登録しないと、インターネットバンキングサービスを利用できないようになっている[73]。

＜二要素認証：トークンの利用＞

トークン利用による認証システムを導入している例としては、テキサス州に拠点を置く American Bank が挙げられる。同行は FFIEC によるガイダンスの発表を受け、2005 年 7 月にトークンを使った二要素認証の導入を発表、一般顧客とビジネス顧客の希望者に対し、RSA セキュリティ社の提供する SecurID と呼ばれるトークンを無料で配布している[74]。SecurID の機能は VeriSign 社のものと同様であるが、同銀行のインターネットバンキングのみで使用可能としており、同銀行にクローズドなシステムとしていることが特徴である[75]。（これに対し、前述の通り、インターネットサービスで多く利用されている VeriSign 社のトークンでは、複数のサイトで利用可能としている。）

また、CitiBank は、法人顧客と Private Banking サービスを利用している特別顧客にはトークンを配布して二要素認証を行う一方、一般顧客へのインターネットバンキングサービスでは従来通りの ID・パスワードのみの一要素認証を行っており、大口顧客と一般顧客の差別化を図っている[76]。

＜二要素認証にかかる新技術：携帯電話の利用、PhoneFactor など＞

Bank of America は、インターネット取引の際、トークンの代わりに、携帯電話を利用した SafePass システムを導入している。これは、ユーザーが ID・パスワードを入力すると、トークンの変りに、ユーザーが登録した携帯電話に 6 桁の OTP を送信し、その OTP をもとにして二要素認証を行うものである。なお、同社の OTP の有効期間は他企業のものと比較して短く、10 分となっている[77]。

また、これ以外にも、携帯電話を使用したインターネットでの認証に係る新しい技術として、Positive Networks 社による「PhoneFactor」が挙げられる。

PhoneFactor は、企業、一般ユーザーに認証サービスを提供しているが、このうち、企業向けサービスでは、携帯・固定の区別なしにどの電話からでも認証を行えるシステムを、一般ユーザーに対しては、登録した携帯電話で認証を行えるサービスを提供している。いずれの場合も、ユーザーはまず、ID・パスワードを使用してログインを行う。その後、登録した電話（固定もしくは携帯）に着信が

---

[73] http://www.capitalone.com/bank/services/online/multifactor_authentication.php

[74] トークンの利用を希望しない顧客に対しては、ING ダイレクト社同様、チャレンジ質問による認証を行っている。

[75] すなわち、American Bank で使われる SecurID を他サイトで使用することは出来ず、同様に、他サイトで使用している SecurID も、American Bank へのログインには使用できない。
http://www.pcbanker.com/CustServ/securIDinfo.asp

[76] http://www.citibank.com/us/citibusiness/securitytoken3.htm
http://www.citi.com/privatebank/client/index.htm

[77] http://www.bankofamerica.com/privacy/index.cfm?template=learn_about_safepass

入り、電話端末の＃キーを押すことで認証が完了する[78]。先述の Bank of America の場合と似たシステムだが、OTP を入力しなくて良い分、利便性は高い。なお、同システムは、OpenID[79]による SSO システムとも連動している。

②金融機関以外のインターネットサービスにおけるトークンの利用

インターネット決済仲介会社である PayPal の年間取引額（2007 年 6 月時点）は 110 億ドルであったが、このうち 0.3%に当たる 3,520 万ドルはフィッシング詐欺などの不正取引で使用された額であった[80]。

このため、PayPal は、2007 年 6 月、それまでの ID・パスワードによる一要素認証に加え、Paypal Security Key[81]の使用による二要素認証システムを試験的に導入している[82]。これは、トークンを購入[83]したユーザーは、サインインの際に、ID・パスワードに加え、当該トークンに表示される OTP を入力するものであるが[84]、同製品は、VeriSign 社のトークンのシステム[85]を利用している[86]。

（２）インターネットサービス会社における動き

①シングルサインオン連携に向けた取り組み（概要）

個人認証技術に関しては、セキュリティ強化の方向のみに動いている訳ではない。特に、近年のインターネットサービスの勃興により、今後益々、個人が自らの情報を、インターネットを通じて管理する方向にある。これらのインターネットサービス企業を見ると、金融機関ほどセキュリティの強化に動いているところはほとんど見られず、むしろサイト間の連携によりも、ユーザーの利便性を強化する動きが特徴的と言える。

---

[78] http://www.phonefactor.com/how-it-works/white-paper
[79] OpenID については次章を参照。
[80] http://www.infoworld.com/article/07/06/15/paypal-using-verisign-tokens_1.html
[81] 同製品は税・送料込みで 5ドル。現在のところ、PayPal Security Key が導入されているのは米国のみで、実際の利用者数などは明らかにされていない。
[82] http://www.infoworld.com/article/07/06/15/paypal-using-verisign-tokens_1.html
[83] VeriSign 社の HP によると、定価は 30 ドルである。PayPal は任意の顧客に対して実質無料でトークンを配布しており、購入費の 5ドルは、トークンの送料に充当されている。
[84] http://investor.ebay.com/releasedetail.cfm?ReleaseID=249263
[85] 同製品は日本国内では「ユニファイドオーセンティフィケーション（AU）」の製品名で展開。
http://www.verisign.com/authentication/individual-authentication/index.html
[86] http://investor.ebay.com/releasedetail.cfm?ReleaseID=249263

確かに、チャレンジ質問や二要素認証の導入などにより、個別入力におけるネットワーク上のセキュリティレベルは向上する。しかしながら、全体でみると、

- アカウントごとに、異なる数多くのパスワードを記憶するのはわずらわしく、かつ、このため個人レベルでのパスワードの管理も雑にならざるを得なくなる。
- また、アカウントの作成に当たっては、個人情報の入力が必要な場合が多いため、各社・サービス毎にアカウントを作成すればするほど、多数の個人情報を入力しなければならず、結果として、個人情報が漏洩する可能性も高くなる。

という問題をはらんでおり、このような観点から、現在、各プロバイダやウェブサービス提供企業は、複数の企業間で連携して、相互に運用可能なシングルサインインシステム（SSO）システムや連携認証システムの構築など、ユーザーの利便性強化に向けた取り組みを行っている。

なお、このような連携は、企業から見た場合、必ずしも全ての企業にとって同一のメリットがある訳ではない。一般的には、利用者の少ないサイトから見た場合、連携をすることは、他のサイトからユーザーを取り込むための施策として位置付けられるが、既に多くの利用者を有するサイトから見ると、むしろ自らのユーザーが他のサービスに流出する懸念が大きくなる。

以下においては、2000 年以降におけるこのような SSO 連携に向けた取り組みとして、2001 年に設立された Liberty Alliance と大手ソフトウェアベンダである Microsoft の動き、そして、インターネットサービスが進展する中、2007 年 6 月に発足した OpenID Federation を巡る動き等について、紹介する。

連携認証普及を目的とする異業種組織[87]

名称	設立時期	.理事会メンバー	参加者数	主な活動内容
Liberty Alliance	2001 年 9 月	AOL, BT, France Telecom, NTT, CA, Novell, Intel, Oracle, Sun Microsystems	150 企業・組織	インターネットにおけるセキュリティ、アイデンティティ問題の解決を目的。その一環として、連携認証システム構築のための研究。
OpenID Federation	2007 年 6 月	Google, IBM, Microsoft, VeriSign, Yahoo	30 社、1 万サイト[88]	SSO システム、OpenID を提供。 対応サイト数が増加中。
Information Card Foundation	2008 年 6 月	Equifax, Microsoft, Oracle, PayPal, Novell, Google	30 企業・組織	インターネット上での電子 ID インフラの構築と、利用促進が目的

[87]出典:各種資料を基に作成

[88] OpenID 発行プロバイダ数は約 30、OpenID 対応サイトは約 1 万となっている。

②2000 年前半の動き（Liberty Alliance と Microsoft）

＜Liberty Alliance の設立経緯と Microsoft＞

2001 年 9 月に約 30 企業が合同で立ち上げた Liberty Alliance （Liberty Alliance Project）は、セキュリティ、アイデンティティ問題の解決を目指して設立された非営利団体である。同団体はその活動の中で、参加ベンダ間のシステムに互換性を持たせ、世界規模の連携型認証システムの構築も目指している。

現在の参加団体数は 150 近くで、その内訳は、IT、金融、通信、メディア、製造など様々な分野の民間企業に加え、米国防総省などの政府機関や大学などの教育機関も含まれる（なお、日本企業からは NTT、NHK、NEC などが参加[89]）。現在の理事会メンバーは、AOL、BT、France Telecom、NTT、CA、Novell、Intel、Oracle、Sun Microsystems であり、そのような意味で、AOL を除き、通信メーカーとハード・ソフトウェアベンダが中心となっていることが特徴であると言える。

この Liberty Alliance は、当時 Microsoft 社の進めていた自社の SSO システムである Passport 構想への対抗であるといわれる[90]。すなわち、巨大ソフトウェア企業に対して、他のソフトウェア、ハードウェアベンダが対抗したという構図であると言える。実際に、現時点においても、Microsoft 社は、Liberty Alliance には参加していない。

＜Liberty Alliance の取り組みとその後＞

Liberty Alliance では、その一部として、SSO 技術の開発とその標準化の策定や、ガイドラインの策定に向けた取り組みを行ってきている。具体的には、参加組織は、エキスパート・グループ（EG）もしくはスペシャル・インタレスト・グループ（SIG）に所属し、プライバシーやインターネット上での ID 問題の解決に向けた活動を行っている[91]。

同団体はより強力で信頼性の高い認証システムの構築に向け、個人認証分野に力を入れており、特に 2005 年以降は、現在の認証システムの欠点として、現存の様々な認証システムが相互に運用可能でない点を指摘し、解決策の提案に努めてきている[92]。

---

[89] http://www.projectliberty.org/liberty/membership/current_members

[90] http://e-words.jp/w/Liberty20Alliance.html
http://www.atmarkit.co.jp/news/200205/01/passport.html
http://www.atmarkit.co.jp/news/200311/14/liberty.html

[91] 具体的には、EG としては、アイデンティティ・アシュランス EG、ビジネスおよびマネジメント EG、技術 EG、公共政策 EG、また、SIG としては、アイデンティティ・アシュランス SIG、e ガバメント SIG、強力な認証 SIG、日本 SIG、健康アイデンティティ管理 SIG が設置されている。
出典：Liberty Alliance Project ホームページの情報を基に作成

[92] http://www.projectliberty.org/liberty/strategic_initiatives/strong_authentication

しかし、同団体での取り組みは参加企業間の話し合いに終わっており、認証システムの相互運用性に向けた具体的な成果はほとんどあがっていないようである[93][94]。

一方、3 億 8,000 万人以上のユーザー数を誇る Microsoft 社は、独自の個人認証システムとして Windows Live ID（旧 Passport Service）を提供しており、一般ユーザーは、Windows Live ID とパスワードを使用してサインインを行う。Windows Live ID では、同システムだけではなく、同社の Passport Service でサポートされている外部ウェブサイトへのサインインも可能である[95]。

2007～2008 年、このサービスに加え、同社は、自社が提供するウェブサイト以外でも Windows Live ID を使用してウェブ認証、委任認証、クライアント認証を行えるようにするための、3 種類のソフトウェア開発キット（SDK）も発表した[96]。同キットを使用して開発されたウェブサイトが増加すれば、1 つの ID・パスワードでネットワーク内の全てのサイトにログインできる、シングルサインオン（SSO）システムの構築が可能になる。今回発表されたキットは Java、Python など 6 つのプログラミング言語に対応している[97]。

（２）OpenID と ICF の動き

①OpenID

＜Open ID とは＞

OpenID Federation は、SSO システムである OpenID と、OpenID コミュニティの発展を目指し、2007 年 6 月に発足した非営利団体である。

OpenID とは、オープン型の ID システムであり、ユーザーはこの ID を作成することで、OpenID に対応している他ウェブサイトにも、OpenID でサインインすることが出来るようになるため、いくつもの ID やパスワードを作成・記憶する必要

---

[93]最新の動きとしては、2008 年 6 月、Identity Assurance Framework（IAF）の初バージョンと、Identity Governance Framework（IGF）のドラフトを発表した。IAF では 4 段階のアイデンティティ保証レベルが設定された他、ビジネスルールやアイデンティティ供給者がユーザーの信頼を獲得するために必要な条件、また、供給者がその条件を満たしているかを判断するための方法論などが盛り込まれている。IGF は Liberty Alliance と Oracle 社が共同で作成した、企業レベルでのアイデンティティ管理に関する枠組みである。なお、両文書は共に、Liberty Alliance のホームページからダウンロード可能。
http://www.projectliberty.org/resource_center/specifications/liberty_alliance_identity_assurance_framework_iaf_1_1_specification （IAF）
http://www.projectliberty.org/resource_center/specifications/igf_1_0_specs （IGF）

[94] http://www.projectliberty.org/strategic_initiatives/identity_assurance

[95] http://dev.live.com/liveid/

[96] http://dev.live.com/liveid/

[97] http://www.infoworld.com/article/07/08/17/Microsoft-takes-another-try-at-single-sign-on_1.html

がなくなる。また、OpenID に対応の各サイトでアカウントを新設する際、認証は OpenID を通して行われるため、ユーザーは必要以上に個人情報を開示せずに済み、ユーザー自身による個人情報管理能力が強化されるというメリットもある。このため、OpenID はユーザー中心の ID システムであると言える[98]。

具体的に、OpenID の入手方法には、以下の 2 通りがある。

① ユーザーは、OpenID プロバイダーを通して OpenID の発行を受ける。OpenID プロバイダーは現在約 30 社となっており、その中には、VeriSign 社も含まれている[99]。これにより、ユーザーは、OpenID 対応サイトのいずれにおいても、当該単一の OpenID を利用してログインすることが可能となる。現在、OpenID 対応サイトは、1 万サイトに達する。

② このうち、特定の OpenID 対応サイトにおいては、ユーザーは、OpenID の発行を受けなくとも、当該サイトでのアカウントを OpenID に変換し利用が可能となっている。現在、数は多くはないものの、AOL や Google が提供するブログサービス「Blogger」などが対象となっている。これらのサイトの OpenID では URL がユーザー名となる点が特徴であり、このため、ウェブサイト・ブログオーナーは、所有するサイトの URL を OpenID アカウントに変換して使用することも出来る[100]。

OpenID 発行企業[101]

①OpenID 発行企業（例）	ClaimID	myOpenID	Verisign Personal Identity Provider	
②ユーザーが元々所有している ID を OpenID としてそのまま転用できるサイト	AOL LiveJournal Vox	Blogger Orange Yahoo	Flickr SmugMug WordPress.com	LiveDoor Technorati
	myID.net	myVidoop		

＜Open ID への各企業の参加に係る経緯＞

この OpenID を運営する OpenID Foundation の企業理事会メンバーとして、2008 年 2 月に、Google、IBM、Microsoft、Yahoo!、Verisign が新たに参加した。

---

[98] OpenID Press Release, “Technology Leaders Join OpenID Foundation to Promote Open Identity Managers on the Web,” February 7 2008, Accessible on http://openid.net/foundation/

[99] USA Today, “Technology cuts down on Web resistrations; OpenID lets consumers have only one user name and password,” March 16 2008, Obtained via Nexis.

[100] OpenID Press Release, ibid.
たとえば、AOL のアカウント保有者の場合、OpenID は「openid.aol.com/**screenname**」に、Google が提供するブログサービス「Blogger」の場合は、「**blogname**.blogspot.com」のようになる。
http://openid.net/get/
なお、Yahoo の場合、そのサイトでのアカウント名を OpenID としてそのまま利用できないため、OpenID サイトへサインインする際に Yahoo にリダイレクトされ、そこでログインを行った後、元のサイトに再びリダイレクトされる仕組みになっている。

[101] http://openid.net/get/

このような主要なインターネット、IT 関連企業が積極的な参加を示したことが、本プロジェクトへの参加社数拡大の大きな要因であると考えられる。

この OpenID は、もともと、2005 年に、Six Apart 社のチーフ・アーキテクトであった Brad Fitzpatrick 氏のアイデアに基づき、その後同社や VeriSign、JanRain、Sxip Identity 等中小ベンチャーの技術者等がアイデアと技術を持ち寄り開発した技術である[102]。

このような中、大手企業としては、Microsoft 社が、2007 年 2 月というかなり早い時期に支援を宣言している[103]。同社は、2007 年 2 月に、上記 3 社と共同作業を発表しているが、これは、Open ID と、同社の ID プラットフォームである Windows CardSpace との相互運用可能性を図ろうとするものであり、そのような意味で、インターネットサービス会社としてではなく、ソフトウェアの観点からの連携であった[104]。

その後、2007 年 2 月に AOL が利用することを発表しているが、大手のインターネット企業として、Google が支援を発表したことが大きい。Google は、2007 年 12 月に、ブログサイトである Blogger において、Open ID のサポートを開始した。Google 内部で、本 Open ID に主導的役割を果たしたのは、前述の元 SixApart 社の元社員で同年 8 月に Google に転職した Brad Fitzpatrick 氏であると言われる[105]。なお、その後、2008 年 1 月に Yahoo!が参加している。

＜現状と課題＞

現在、OpenID 対応サイトは 1 万件近くに増加[106]しており、現在、1 億 6,000 万以上の OpenID が発行されている[107]。OpenID 対応サイトの中には Yahoo! や AOL、Wikipedia など、ユーザー数の多いサイトも含まれており、2008 年 7 月末には、登録 ID 数 5 億人の人気ソーシャルネットワーキングサイト（SNS）である MySpace も、OpenID への参加を表明、OpenID の今後の拡大が期待されている。これらのサイトにログインする際は、ユーザーは一度 OpenID にリダイレクトされて認証を受け、認証終了後に再び、元のサイトに戻される。

しかしながら、少なくとも現時点で、大手である Google や Microsoft が全面的に自社サイトを OpenID 対応にしている訳ではない。Google 社は各種の自社サービス間で SSO を導入しており、また、YouTube など買収した企業と自社サービ

---

[102] http://www.atmarkit.co.jp/news/analysis/200704/23/openid.html

[103] なお、大手では、その直前の 2007 年 1 月に、セキュリティソフト企業の Symantec が、支援を表明している。

[104] なお、ソフトウェア系大手企業としては、2007 年 5 月には、Sun Microsystems が連携を発表している。

[105] http://jp.techcrunch.com/archives/google-trialling-openid-with-blogger-may-offer-openids-to-users/

[106] http://openid.net/where/

[107] http://openid.net/what/

スの SSO の連携にも積極的に取り組んでいる[108]が、少なくとも、現時点では、OpenID に関しては、Blogger のサイトに限定しており、また、Microsoft は、2008 年 6 月、同社が OpenID を支援すると宣言して 16 ヶ月後に初めて、同社の医療プラットフォームである Health Vault で Open ID を使えるようにした[109]。

なお、セキュリティ企業から見た場合、VeriSign は、自社の PKI、トークン等を OpenID に組み込むことができるようなサービスを提供し、OpenID が容易に使えるよう取り組んでいる[110]。

また、同システムでは、セキュリティ面、プライバシー面での問題が解決されていないとの批判も見受けられる。IT やコンピューター関係のブログ、”A Consuming Experience”によると、OpenID の最大の長所である SSO の利便性は、セキュリティ面での欠点にもなりうる。つまり、もし OpenID とそのパスワードが盗まれた場合、OpenID でログインできる全てのサイトにおいて、盗まれた OpenID が悪用される可能性が高い。このため、OpenID 自身はそのシステムを「ユーザー中心」と謳っているものの、実際のところユーザーは、OpenID プロバイダーに情報管理のほぼ全てを頼らざるを得ない状況である。また、OpenID はフィッシングに対して脆弱であるとの指摘も見受けられる[111]。

②The Information Card Foundation（ICF）

連携型認証システムに関する団体の中で最も新しいと思われるのは、2008 年 6 月に Equifax 社、Microsoft 社、Oracle 社、PayPal、Novell 社、Google 社の 6 社が中心となり、その他 IT 関係企業 9 社が参加して発足させた、The Information Card Foundation（ICF）である。

ICF は、インターネット上での電子 ID インフラの構築と、その利用促進を目的とした活動を行う非営利団体であり、同団体は、Information Card（I-Card）の普及を目的としている。I-Card とは、免許証やビデオショップの会員証など、実際の生活で使用する身分証明書や会員証の電子版である。現在、同組織のメンバーは 30 個人・団体にまで拡大している[112]。

---

[108] https://www.google.com/accounts/ServiceLogin?service=youtube&continue=http://www.youtube.com/signup&passive=true/

[109] http://jp.techcrunch.com/archives/20080623microsofts-first-step-in-accepting-openid-signons-healthvault/

[110] http://jp.techcrunch.com/archives/20080820verisigns-personal-identity-portal-is-half-way-to-password-bliss/

[111] A Consuming Experience, “OpenID: Intro & How to for Non-techies,” April 3 2008, Obtained via Nexis.

[112] http://informationcard.net/index.php?page=members

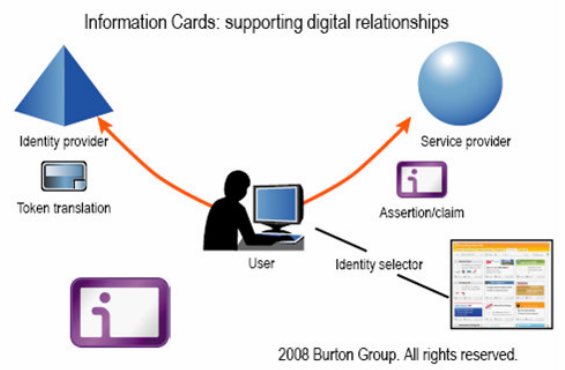
ICF 参加企業[113]

運営会員	Equifax	Google	Microsoft
	Novell	Oracle	PayPal
スポンサー会員	Backgroundchecks.com	Gemalto	Idology
	IP Commerce	Parity	Ping Identity
	Privo	Wave	
普通会員	Arcot Systems	Aristotle	A.T.E. Software
	CORISECIO	Crypto-Pro	Eduserv
	Figlo	FuGen Systems	Fun Communications
	ooTao	Wisekey S.A.	WSO2
協力会員	Fraunhofer Institute FOKUS	ETRI	Liberty Alliance

ユーザーは、ID やパスワードなどの情報を入力した I-Card を自分で作成できるほか、信用できる第三者機関（銀行など）などの I-Card プロバイダに個人情報を提供し、デジタル身分証明書としての I-Card の提供を受けることも可能である。この I-Card は、コンピュータのデスクトップや携帯端末に設置された Identity Selector と呼ばれるインターネット上の電子財布内に収納される。

実際に、各ウェブサイトのアカウントにログインする際は、ユーザーは Identity Selector 内の I-Card をクリックするだけでログインできる。このため、各ウェブサイトで ID やパスワードの入力を行わなくても良く、また、情報に変更があった場合は、I-Card システム上で情報の更新を行うと、I-Card 全てが連動して一括で更新される仕組みになっているため、各アカウントで更新を行う手間が省ける[114]。

I-Card 使用の流れ[115]



[113] http://informationcard.net/members 個人メンバーは省略。
[114] http://informationcard.net/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=3&cntnt01returnid=15
[115] 出典：http://informationcard.net/uploads/images/ICFgraphic.pdf

したがって、I-Card を使用したシステムは SSO を可能にするばかりでなく、インターネットで様々な個人情報を入力する方式とは根本的に異なるため、フィッシング詐欺などの被害に遭う可能性が低くなるという点が同システムの魅力の 1 つとして挙げられる。さらに、ユーザー、ID プロバイダー（銀行など、信用できる第三者機関）、利用先のウェブサイトの 3 者がリアルタイムで同期化し、暗号化した情報のやり取りを行うため、高い信頼性も期待されている[116]。

同団体はまだ発足して間もないため、これ以上の情報はまだ公開されていないが、2008 年 2 月に開催された情報セキュリティに関するシンポジウムである RSA Conference では、約 50 社が I-Card システムに関するディスカッションに参加、また、2008 年末までにかけても同様のイベントが予定されている[117]。さらに、Liberty Alliance や OpenID Foundation など、相互運用可能な連帯認証システムの普及に向けた取り組みを行う他組織とも協力体制を構築、または、今後の構築を予定している。

このレポートに対するご質問、ご意見、ご要望がありましたら、tagui_ichikawa@jetro.go.jp までお願いします。

[116] http://news.cnet.com/8301-10789_3-9975122-57.html
[117] http://news.cnet.com/8301-10789_3-9975122-57.html