社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－DPS－128 (6)
2006－GN－ 61 (6)
2006－EIP－ 33 (6)
2006／9／14

ネットワーク社会におけるＩＤ氾濫の課題分析
～ID爆発の問題提起～

斉藤典明、 櫛田達也、 山崎哲朗、 小林透、 金井敦
NTT 情報流通プラットフォーム研究所
〒239-0847 神奈川県横須賀市光の丘1-1

ブロードバンド環境の普及に伴い様々なサービスがオンライン化され、生活に必要な様々な環境がネットワーク上に実現してきている。一方で、ネットワーク社会を背景にした様々な事件や脅威も増加している。そこで本論文では、ネットワーク社会上で様々な社会生活を享受するためのシステム利用とセキュリティの両面のキーとなるIDに着目した。様々な社会システムがネットワークサービス化されるに伴い、ユーザが管理するべきIDが爆発的に増加することにより利用者自身がこれに追随できなくなってくる状態をID爆発と定義し、ここでとり使うべきIDを4つの区分に分類するIDの分類モデルと、その中で発生することが想定される問題を提起する。

The ID Explosion

SAITO Noriaki, KUSHIDA Tatsuya, YAMAZAKI Tetsuro,
KOBAYASHI Toru, KANAI Atsushi
NTT Information-Sharing Labs.
1-1 Hikarinooka Yokosuka-shi, KANAGAWA 239-0847 JAPAN

Many social services which are important for our daily life became available on the network as broadband networks users are increased. On the other hand, several threats which are based on the networks are increasing. Then in this paper, we focused discussion theme to the ID which has an important function as the supply of rights and security for users. We have to manage a lot of IDs as a lot of social service are constructed on the network, and we will be not able to catch up such increasing of IDs. We named such situations the "ID Explosion". Then, the ID categorization model which was classified into four to clarify the structure of the ID Explosion and generated problems under the ID Explosion situation will be described.

1. はじめに

インターネットの普及およびブロードバンド環境の普及に伴い、様々なサービスがオンライン化され、生活に必要な様々な環境がネットワーク上に実現してきている。一方で、ネットワーク社会を背景にした様々な事件や脅威も増加していることが見逃せない。これらの脅威の多くは、ユーザ自身のセキュリティ意識の向上によって改善できるものと考えられるが、一方で、システムの複雑化、関連するシステムの増加にユーザ自身の負担が増加しセキュリティ意識の向上だけでは対処できないという実情もある。

このような実情をより細かく解析するために、ネットワーク社会上で様々な社会生活を享受するためのシステム利用とセキュリティの両面のキーとなるIDに着目した。さら

に、2010年頃に様々な社会システムがネットワークサービス化されるに伴い、ユーザが管理するべきIDが爆発的に増加することにより利用者自身がこれに追随できなくなってくることが予見され、この状態をID爆発と定義し、ここでとり使うべきIDを4つの区分に分類するIDの分類モデルと、その中で発生することが想定される問題を提起する。

2. 社会的背景

2005年度は、4月の個人情報保護法完全施行に始まり、フィッシング詐欺、P2Pソフトウェアによる情報漏えい事件とセキュリティに関する社会動向が非常に大きく揺れた年であった。一方で、2005年はe-Japan計画の終了の年であり、2006年からは2010年に向けたu-Japan計画が総務省から発表された[1]。その中では、"2010年までに①シームレスなユビキタス基盤の整備:国民の100%が高速または超高速を利用可能な社会に、②21世紀の課題解決にICTを利活用:国民の80%がICTは問題解決に役立つと評価する社会に、③ICTの利用環境整備の抜本強化:国民の80%がICTに安心感を得られる社会に"という目標が挙げられており、今後、様々なサービスがネットワーク上で利用可能になる一方でネットワーク社会に対する安全性を高める必要性が述べられている。このことは裏を返すと、ネットワーク社会に対する利便性は向上しているものの不安感は広まっており、更なる発展を遂げるには、現在の不安感を解消せざる終えない状況ともいえる。

また、個人情報保護法では、個人情報として"個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別できることとなるものを含む。)"とあり、システム上のつくりを考慮すると、これはいわゆるIDとそれに関連する属性情報と言い換えることが可能である。つまり、個人情報漏洩事件はID情報の漏洩事件と密接に関係するということができる。

さらに、一連のフィッシング詐欺では、銀行口座のID窃盗の危機が問題となった。金融庁発表の資料[2]の中にはインターネットバンキングにおける銀行口座に対するリスクとして、ID／PW(PW＝PassWord 以下PWと略す)の不適切な管理によるID窃盗、PCなどの盗難によるID窃盗、フィッシングサイト・スパイウェア・キーロガーなどによるID利用中におけるID窃盗、PWの再交付時を狙ったID窃盗が挙げられている。このようなID窃盗に対して、米国では消費者の20%以上が、カナダでは消費者の9%がID窃盗の被害にあっているといわれている報告[3]もあり、日本社会においても今後さらに問題が拡大し、大きな社会問題に発展することも予想される。また、米国においてはID漏洩に対する脅威とID活用に関するトレードオフも問題になっている[4]。

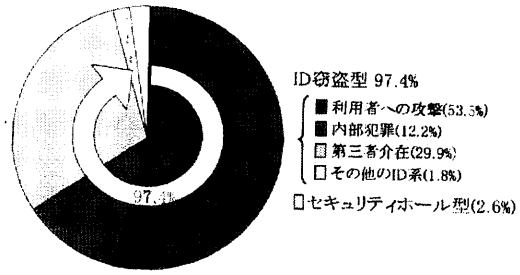

図1. 不正アクセスの動向

さて、日本においては警察庁発表の資料[5]によれば、2005年の不正アクセスの検挙件数は271件報告されている。このデータについて少し整理すると次のようになる。全体の不正アクセスの検挙件数の271件に対して、セキュリティホールへの攻撃が7件(2.6%)、ID窃盗型が264件(97.4%)であり、ほとんどがIDに関する脅威である。ID窃盗型を細分化すると、利用者に対する攻撃が145件(53.5%)、ID管理者などの内部犯罪が33件(12.2%)、第三者介在によるものが81件(29.9%)、その他のID系が5件(1.8%)となっている(図1)。(注:原資料に対する本資料での対応は、"識別符号窃用型"を"ID窃盗型"に、"利用者用のパスワードの設定・管理の甘さに付け込んだもの"、"言葉巧みに利用権者から聞き出した又はのぞき見たもの"、"スパウイウェア等のプログラムを使用して識別符号を入手したもの"、"フィッシングサイトにより入手したもの"を"利用者に対する攻撃"とし、"識別符号を知り得る立場にあった元従業員や知人等によるもの"を"内部犯罪"とし、"他人から購入したもの"、"共犯者等から入手したもの"を"第三者介在"としてある。)

このようなID窃盗に対して、経済産業省の"コンピュータ不正アクセス対策基準"[6]では、ユーザサイドにおけるID／PW管理では"パスワードは随時変更すること"などの9項目を遵守するように推奨されている。そして、これと同様のことが様々なシステムでのID管理で推奨されているのが実情である。このガイドラインが遵守できれば、ID窃盗は大幅に削減できるかも知れない。しかしながら、一人当たりのID／PWの数が増加していることや、複雑なPWを記憶し続けることは人間の記憶力の限界を超えており、このガイドラインを守ることは現時点で非常に困難であることは、誰もが体感的に

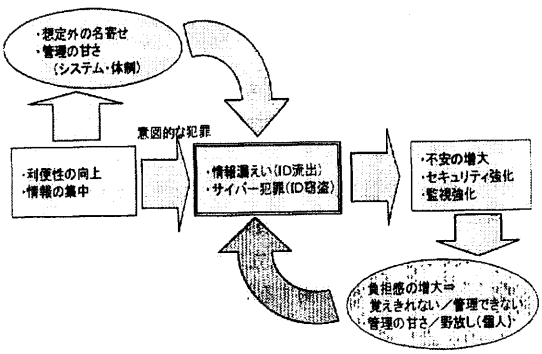

図2. ID管理の脆弱性の構造

知っていることである[7]。

人間系の入らないシステムのセキュリティを確保するには、システムを強化することに比例して強化可能であるが、ユーザという人間系を考慮した場合、セキュリティを強化するために、例えばルールを強化してゆくなど、守れないような方法を前提としたセキュリティの強化では、かえってセキュリティの脆弱性を生み出すことになる(図2)。今後、IDの増加に伴い、このようなセキュリティの強化が返って脆弱性を生み出すような問題が大きくなることが予想される。そこで、本論文では、このIDの増加に伴い人間の対応が追随できなくなってしまった状態を*ID爆発(ID Explosion)*と定義する。

3. ID分類モデル

ネットワークの社会インフラとしての利用シーンの増加とID／PWの増加に伴い、IDにまつわる様々な問題が生じているが、ここで、今回の検討で対象とするIDについて整理しておく。ここでは、IDの一連の利用シーンを想定して、IDの生成、IDを活用するためのIDへの意味付け、IDの活用、IDの活用後の4つのフェーズに分類した(表1)。

・カテゴリ1：IDとしての基本的な識別子としての役割のものである。ここでは、特に何かの利用目的を考えずに、対象を一意に識別するための識別子としてのIDである。表中で例示したIDは、意味や利用目的を述べない範囲での識別子の役割としてのIDである。識別子としてのIDなので、名前やメールアドレスのように所有者本人以外が使うこともある。

・カテゴリ2：IDに対する存在、能力、権利を示すためのものである。ここでは、識別子として識別されたIDに意味や利用目的などの属性情報を設定したIDである。これは、権限などの所有者だけが使う排他的なものであり、パスワード設定や認証デバイスの所有や証書により対処者と権限の明記などにより第三者からの利用が守られるものである。より具体的な例として、サービスに対する利用権利という観点ではID、PWからなるアカウントがここに入る。

・カテゴリ3：権利の行使に用いるIDのことで、特に認証（認可）のことである。ここでは、あらかじめ設定された権利情報に基づき権利を行使する場合である。具体的には、認証において、あらかじめシステムに設定されているアカウントとしてのIDと、利用の際に用いる入力手したやデバイスに格納されているIDとの照合がおこなわれるが、この後者の認証の際に発生するIDのことである。

・カテゴリ4：IDの使用によって生じるIDのことである。ここでは、IDの利用後に残るID自身のコピーや、回数情報や統計情報などのように新たに発生する情報自身に価値や権利がありこれらに対して新たに付与される場合に生じるIDのことである。

上記の区分について、社員番号を例に説明をする。カテゴリ1のIDは、社員を識別するために用いる番号のことで、この段階のIDは誰にどのIDを付与したという割り当てが管理されていれば良く、これに対する実態がなくても良い。社員番号を用いて、社員サービス用のOAシステムのアカウントや、社員番号を記載した社員証／入館証を作成すると、アカウントという2次的なIDが生成される。（社員証は、単純に社員を識別するためだけの番号のメモであればカテゴリ1の位置づけになるが、社員証には社員を識別するという目的のほかに社員番号に対する属性が記載されているのでカテゴリ2として区分した。）このようなアカウントが設定されているOAシステムにログインするとき（あるいはビルに入館するとき）、システムのプロンプトに入力したIDとサーバに設定されているIDの照合を行うことによって認証をおこなうが、このような利用の際に入力するIDをカテゴリ3のIDとする。（認証・認可とは、入力したIDとサーバに設定されているIDの照合であるというスタンスである。）OAシステムにログインすると、その記録がログファイルにIDが記載されるが、このログファイルに残るIDがカテゴリ4のIDである。

4. ID爆発の問題提起

IDの増加に伴い、人間の対応が追随できなくなってしまった状態をID爆発と定義したが、実際にどのような問題があるのかを先の表中にまとめた。問題については、大きく分けて、現在すでにある問題がID爆発によりさらに大きくなる問題と、現在はない（あまり問題視さ

れていない）がID爆発により新たに発生する問題の2つに区分し、IDの4つのカテゴリごとに想定される問題の例を挙げた。以下にそれぞれについて述べる。

(1) 問題領域【I】

ここでの問題は、様々な種類、大量のIDが増加することに関し、特に、ID体系に機縁する問題である。もし、全世界のすべてのものに対するIDの付与基準や付与体系が過不足なく統一されていれば問題にはならないが、そのようなことは現実問題としてできないことから、それぞれの団体で発行されたIDが氾濫することになる。そして、今回のID爆発のそもそもの発端となる。

具体的な例として、番号不足、汚染ID、付与方法の混乱、架空ID、期限切れIDなどの問題が挙げられる。番号不足は、IPアドレス問題のように、当初考えていたID体系が飽和してしまう問題である。汚染IDは、例えば電話番号のように一定のアドレス資源を使いまわしている場合、現在の利用者が以前の利用者の影響を受けてしまう問題である。付与方法の混乱は、IDの発行主が自由にIDを発行し、これをローカルで使っている場合は問題ないが、他との連携で活用しようとすると不整合や混乱が発生する問題である。架空IDは、今手元にあるIDが正規のIDかわからないことによって生じる問題である。期限切れIDも同様である。

(2) 問題領域【II】

ここでの問題は、これまで想定していなかったものへのIDの付与や、これまで想定もしていなかった特性をもつIDの出現により、便利になる反面新たに発生する問題のことである。

(3) 問題領域【III】

ここでの問題は、IDに関連づけられる権利の設定や権利の証明に関する問題であり、言い換えるとIDの管理に関する問題である。ID管理に関しては、立場は2つあり、一つはIDの発行主体におけるIDの管理と、もう一つは利用者としてのIDの管理の問題である。今回は特に利用者の立場に立った検討であるため、ここでは利用者の立場に関する問題を中心にリストアップしてみる。

具体的な例として、覚えきれない、管理しきれない、かさばる、埋もれてしまう、関連がわからない、変更が困難などの問題が挙げられる。覚えきれないについては、会員番号、メールアドレス、パスワードが多すぎる、複雑すぎるなどの理由により覚えきれないという問題である。管理しきれないについては、パスワードの更新や、日々の履歴のチェックなどの管理がIDが多すぎることによって追随できなくなる問題である。かさばるについては、会員証やポイントカード、クレジットカードなどが財布の中でかさばる問題である。埋もれてしまうについては、特に利用頻度の少ないIDやIDの証書がどこかにしまい見つけるのが困難になってしまう問題である。関連がわからないは、あるIDは他のIDの存在が前提になっている場合があり、このようなID相互の関連がある場合、IDが増えてゆくことによりどのIDとどのIDが関連するのかがわからなくなる問題である。変更が困難は、IDの利用者が変更をしようと思っても、ID

表1. IDの類別とID爆発の課題

	定義	例	ID爆発	
			現在の延長上の問題	新たな問題
カテゴリ1	識別子としてのID。 ヒト、モノ、コンテンツ、トコロ、コト、サービス、トキなどディジタル世界で扱うあらゆるものを識別するために発生するID。 自分に対するIDであるが他人に教えることもある。 （メールアドレス、名前など）	名前、社員番号、シリアル番号、ファイル名、URL、住所、経度緯度、組織名、電話番号、時刻、ucodeなど	【I】 ・番号不足 ・汚染ID ・付与方法の混乱 ・架空ID ・期限切れID	【II】 ・想定外対象へのIDの発行 ・想定外特性のID （事後決定型、プローブ、ダミー、バイナリー形式など）
カテゴリ2	存在、能力、権利を示すためのID。 IDとPWの対によるアカウントや、IDを記載した証書や、PWだけのシステムを含む。 （※PW：パスワード）	戸籍、住民票、社員証、学生証、免許証、メールアカウント、ソフトウェアのライセンス、コンテンツのライセンス、各種サービスのアカウントなど	【III】 ・覚えきれない ・管理しきれない ・かさばる ・埋もれてしまう ・関連がわからない ・IDの階層化	【IV】 ・新たな権利形態 （場所、コンテンツなどの対象や、家族利用などの利用者に対してなど）
カテゴリ3	権利の行使、認証するためのID。 ICカードのようにIDなどが埋め込まれているものを含む。	システムへログインのための手入力のID、予約番号、引き換え券、郵便受けのパスワード、家の鍵、ICカード入館証など	【V】 ・頻度/シーンの増加 ・使いわけの煩雑さ ・不正アクセス	【VI】 ・想定外の相互連携
カテゴリ4	IDの使用によって生じるID。	履歴上のID、申し込み記録	【VII】 ・必要以上の名寄せ ・プライバシー問題 ・目的外利用	【VIII】 ・履歴に対する権利 ・誤識別/想定外の名寄せ ・IDの価値生成

の発行主体との合意が困難であったり、そのIDに様々な権利が関連づけられおり、これらを変更するのに手間がかかるような問題である。

(4) 問題領域【IV】

ここでの問題は、これまで想定していなかったようなIDに対する権利などが新たに発生する問題である。例えば現在、場所やダウンロードしたコンテンツなどには権利的な問題があるが、ネットワーク上では制御できない状態である。これが今後ネットワークから制御できるようになると、IDとセットで権利を管理する仕組みが必要になることが予想される。このとき、利用者本人だけでなく、現在あいまいな権利関係となっているような家族関係や友人間での私的な利用(コピー)についても、IDとセットになることによって明示的になり、社会的なインフラとしてIDと権利を管理する仕組み必要になるであろう。

(5) 問題領域【V】

ここでの問題は、IDによって利用可能になった権利などに対して実際に利用するに際に生じる問題である。大きな方向性として、認証連携や認証デバイス、生体認証などの活用によりユーザの負担感を軽減する流れと、本人確認性を確実にするために二要素認証を用いたり、権限を細分化し多段階に細かく認証してゆくなどより複雑化する流れがある。そのため、利便性と安全性のトレードオフをうまくバランスさせることが重要となる。

具体的な例として、頻度／シーンの増加、使い分けの煩雑さ、不正アクセスなどに関する問題がある。頻度の増加は、例えば、受付けら居室までスルーで通れたものがIC入館カードの出現により建物の区分ごとにICカード認証をするようなイメージであり、認証が簡単になることによりこれまで以上に認証の回数やシーンが増加することである。使い分けの煩雑さは、同じサービスに対するIDがあったとしても立場(例えば、業務かプライベートか)によって使い分けが発生する場合である。不正アクセスは、本来アクセスしてはいけない人がアクセスする問題である。特にシステム側にとっては、単純には不正使用のIDと正規使用のIDの区別がつかないため今後大きな問題になることも予想される。

(6) 問題領域【VI】

ここでの問題は、IDを利用するにあたってこれまで考えても見なかった不都合が生じる問題である。例えば、現在検討がされているリバティアライアンス型のシングルサインオンでは、xSP側の連携によって利便性を向上させる方式があるが、xSPの連携スキームが時には利用者にとって不都合が生じる組み合わせが発生する危険性も考えられる。他にも、住民基本台帳のデータが他のシステムで利用されるなど、制度面での利便性向上が、利用者の危険性となり、利用者の個人的な努力で回避するのが困難な状況も生じかねない。

(7) 問題領域【VII】

ここでの問題は、IDの利用によって生じるIDに対する権利や価値に関する問題である。

具体的な例として、必要以上の名寄せ、プライバシー、目的外利用などに関する問題がある。これは、いくつかのIDデータを活用すると本人性だけでなく、本人の生活環境などがわかってしまうような場合である。このような情報が契機となって迷惑メール問題や不当な与信などのようなプライバシーに関する問題がある。

(8) 問題領域【VIII】

ここでの問題は、IDの利用によって生じたIDに対してこれまで想定されていなかった権利の発生などに関する問題である。例えば、現在、監視カメラに移っている本人写真に対する取り扱いはセンシティブな問題を含んでいる。これと同様に履歴残っているIDの記録に関しても開示の可否を含めて今後大きな問題になる可能性がある。また、マーケティングにおいては履歴のデータからのマイニングによって見込み顧客の抽出などをおこなっているが、抽出結果が妥当な場合はプライバシー問題があるが、もしこれらの抽出結果が誤っている場合でも問題を含んでいる場合がある。特に誤抽出によって利用者へ不利益をもたらせる場合は大きな社会問題になりかねない。(アメリカなどではすでに実際に起きているという報告もある。[4]) さらに、IDの利用、特に多くの人の利用によってIDに対して価値が生じる場合がある。例えば、多くの人が訪問することにより場所に対しては"人気の場所"という情報(価値)(コンテンツであれば視聴率)が生じる場合がある。このようなIDの利用によって生じる価値情報の取り扱いについても今後議論して整理する必要があるであろう。

5. ID爆発の考察

これらのID爆発に機縁する問題についてここでは利用者への影響(脅威)について考察する。

(1) カテゴリ1(【I】と【II】):IDには、システムや組織から一方的に与えられた場合と、利用者自身が申請する場合がある。すべてのIDが機械的に付与された番号であり公平感があれば利用者はそれほど意識することなく利用可能であり、大きな影響はないと思われる。しかしながら、メールアドレスや名前のように、自分を表すためのIDであったり、他人からの利用が想定されるIDについては、覚えやすさやフレンドリーさも重要な要素

になる。しかしながら、これらはユーザへは不便という程度であり脅威とまではならないと予測される。

(2) カテゴリ2 (【III】と【IV】) : 不正アクセスの原因がユーザ自身のID管理の不適切さや、IDの再発行のタイミングを狙ったID流出が非常に多いことから、このカテゴリでの問題の放置は非常に大きな脅威となりうる。特にIDが増加するとユーザによる管理の限界が真っ先に影響が生じ、この課題に対する対策として技術的な対策だけでなく法律・制度面での対策の両面が必要になると予測される。特に技術的な対策は、守れない対策ではなく守れる範囲での対策指針が必要になると考えられる。例えば、多種多様なIDを一律原則どおり管理するには限界があり、IDの重要度と利用頻度に応じた適切な管理方法が考えられる。また、IDの利用においては、匿名性と実名性のバランスが必要となり、同一目的でも特性の異なるIDを階層化してバランスを保って用いるような方法も必要であろう。このようなIDの階層化の是非の検討やIDの管理指針が今後必要となるであろう (図4)。

(3) カテゴリ3 (【V】と【VI】) : ここでは、例えユーザがきちんとID管理をしていたとしても、システム側のゆるい認証によって、誤って重要なシステムを第三者に利用させてしまうようなことが脅威になる。特にユーザにとっては非常に大きな脅威である。

(4) カテゴリ4 (【VII】と【VIII】) : 現在、履歴を直接利用するというシーンは、マーケティング支援やディジタルフォレンジックの領域であり、それほど多くないと考えられる。また、これらの領域ではすでにプライバシーの問題についても慎重に取り扱いがされている。しかしながら、プライバシー以外でも非常に大きな脅威が潜んでおり、欧米では履歴解析のミスにより犯罪者ではない人が犯罪者扱いされてしまう事例や、最近の日本における社会保険庁の年金問題 (支払い履歴が消えている) のような事例がある。

6. おわりに

本論文では、ネットワーク社会上で様々な社会生活を享受するためのシステム利用とセキュリティの両面のキーとなるIDに着目し、IDが爆発的に増加することにより利用者自身がこれに追随できなくなってくる状態をID爆発と定義し、ここでとり使うべきIDを4つの区分に分類するIDの分類モデルと、その中で発生することが想定される問題を提起した。

今後の課題は、これらの問題を解決するための技術として、ID爆発により大量かつ複雑化するID間の関係を

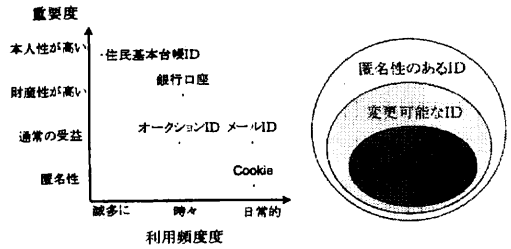

図4.IDの位置づけの例

解きほぐしIDにまつわる情報をユーザ主導で管理・利用する技術の研究を進めており、次の3つの要件を満たせる技術の実現を提案してゆく予定である。

・IDの状況がわかり統廃合などがしやすくなる。(可視化、利便性向上)

・IDが安全に管理されていることがわかる。(安全性向上、監査。)

・存在、関係、所有、権利、契約、行動などを証明、立証できる。

[文　献]

[1]"u-Japan政策 ～2010年ユビキタスネット社会の実現に向けて～",
ユビキタスネット社会の実現に向けた政策懇談会,総務省.
http://www.soumu.go.jp/s-news/2004/pdf/041217_7_bt2_all.pdf

[2]"情報セキュリティに関する検討会の概要について",
金融庁.
http://www.fsa.go.jp/singi/infosec_ken/20060713.html

[3]" 8. 日本におけるID窃盗の実態 ", IT+PLUS, NIKKEI NET.
http://it.nikkei.co.jp/security/column/drwestin.aspx?n=MMITca023020012006&cp=1

[4]"プロファイリング・ビジネス",Robert O'Harrow著, 中谷訳, 日経BP社,2005.

[5]"不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況", 警察庁.
http://www.npa.go.jp/cyber/statics/h17/h17_06.html

[6]"コンピュータ不正アクセス対策基準",経済産業省.
http://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm

[7]"「すべて違うID・パスワードを利用」1割以下、増え続けるログインサービス",デイリーリサーチ 2006/08/08号.
http://japan.internet.com/research/20060808/1.html