

将来を見据えた国民ID構築のための提言

Proposal for establishing a national ID scheme - from the viewpoint of security, privacy and architecture

個人情報保護研究会 国民IDのあり方検討会
山崎文明、畑野元、三谷洋、小泉雄介、原岡望、
芦田勝、林隆臣、川口元、小林健、力利則

要旨

行政サービスの向上、業務の効率化、諸外国に追いつくことなどを目的に、日本においても国民ID構築の検討が進んでいる。本研究では、セキュリティとプライバシーへの対応や新しい技術の採用の必要性について論述し、将来を見据えた国民ID構築のための提言を行う。本研究の提言も含め十分な議論を尽くし、新しい技術を駆使したセキュリティとプライバシーのバランスの取れた先進的な国民ID構築を希望する。

キーワード

国民ID、セキュリティ、プライバシー、アーキテクチャ、マスターID、トランザクションID、ID付番

1. 本研究の目的と問題提起

本稿では、現在、政府等が検討を進めている国民IDについて、将来を見据えて十分な議論を尽くしたうえで制度作りや方式設計を進めるべきであるという提言を行う。

国民IDの構築の目的として、国や地方自治体等の行政サービスの利便性の向上、業務の効率化、電子政府の構築に関する安全な社会の形成等が挙げられている。これらの目的から実施範囲と実現時期、予算等を踏まえた議論がなされている。具体的な実現手段は諸外国の既存の方式を参考にしている。

しかし本来、制度作りや方式設計においては、セキュリティやプライバシーに関する議論を尽くし、国民IDの実現時期をにらみ、将来にわたって有効な技術を取り入れるように検討する必要がある。国民IDの取り組みに先進的な国では国民IDにカードや顔写真を使用する時代は過ぎ、新しい技術を駆使しようとしている。既存の方式を使って国民IDを構築したのでは、セキュリティやプライバシーの問題が生じる可能性があり、諸外国が新しい技術を駆使した方式でさらに先をいくことになる。

現在の日本で国民IDに関して議論が不足していると考えられる事項は次の3点である。

第1の点は、セキュリティに関する議論である。漏えい防止の検討はされてはいるが、恒久的なマスターIDと日常的に使われるトランザクションIDの識別について十分な議論が行われていない。さらに国民IDが短期的に大量に漏えいした際にIDの再付番をどのように行うかが検討されていない。セキュリティが万全であ

るという前提に立つのではなく、リスクを想定した検討を進めなければならない。

第2の点は、プライバシーに関する議論である。まず名寄せの問題がある。行政サービス間で同じIDが使用されると、容易に名寄せが可能となるリスクが発生する。さらに今後の課題として、自分で自分をどう証明するかという議論も必要である。今はIDと顔写真が貼付された証明書やカードが本人認証に使われているが、身分証にIDや顔写真を貼付することの必要性や、顔写真で本人を確実に照合できるのかという検討も必要である。各国の導入例のうち現在最も先進的といえるシンガポールの方式では、IDや顔写真のない金属の棒による認証方式を使うことによって、セキュリティ対策、プライバシー保護と本人認証のレベルを引き上げることが検討されている。

第3の点は、国民IDを実現するアーキテクチャに関する議論である。国民IDの導入の先駆者である豪州では、方式や制度の問題を解決するために1986年、2006年、2009年と3回にわたって方式設計を見直して新技術を導入し、将来も見直しを行っていくとしている。他国がすでに利用している方式であっても、安全面、制度面、運用面の検討、将来にわたる有効性の確認等を十分に行わなければならない。技術立国を標榜する日本の重要施策として先進的な国民IDの導入が図られるように議論を尽くす必要がある。

以上の3点が本稿での主な問題提起である。現在検討が進んでいる国民ID構築において、本稿で取り上げた事項も含め十分な議論を尽くして進めることが重要である。

本稿の構成は次のとおりである。第1章での目的と問題提起に続き、第2章で国民ID構築の背景と経緯、第3章でID付番の代表的な方式のメリットとデメリットを検討する。それらの議論に基づき、第4章で国民IDに関するセキュリティとプライバシーに関する課題の整理を行い、第5章で先進事例も踏まえて新しいアーキテクチャを提言する。最後に第6章で今回の問題提起と提言に関して議論すべき事項も含めてまとめる。

国民が自らの問題として考えるとともに、政府等での検討においても議論を尽くし、将来を見据えた国民IDの礎を築いていただきたい。

2. 国民IDの検討経緯と状況

日本社会の直面している課題には、少子高齢化の進行による就労世代の税負担増加、社会保障費の増大、国の歳入・歳出の不均衡、国の借金の増加などがある。「年金保険料を払っても将来もらえない」「納税の仕組みが不公平だ」「税金を使う行政の無駄、非効率性の解消が先だ」といった不満が上がる。これに対し、政府等は、納税管理または社会保障制度の健全化等の名目で、国民IDの導入を前提とした検討を進めている。

2.1 国民IDとは

国民IDは、次のように定義できる[1]。なお、IDに関する制度、IDを記録して本人に渡す形態を示す場合もある。

- ・社会基盤の運営、利活用に供し、行政サービス等を利用する際等に個人を識別する
- ・日本国民等^{*1}のほぼ全員に、統一的に日本国から強制的に付番される
- ・他人のIDと重複しない
- ・英数字等から構成される
- ・法の定める目的と範囲で利用できる

国民IDは関連する個々の番号のベースとなるため、マスターIDと呼ばれることもある。これに対して、行政ごとにマスターIDとの対応付けがなされた、分野別に利用するトランザクションIDがある(図1)。

どのような用途、範囲にするかについても次のような側面が検討されている。

- ・社会基盤の内部処理に利用される側面(バックオフィス連携)
- ・社会基盤と個人のインターフェイスに利用される側面(ポータビリティ等)
- ・私人間で利用する側面(民間活用)

*1 出生後すべての国民に付与するか、一定年齢以上にするか、外国在住の国民、国籍を有しない人、住民票コードを有しない人、日本在住の外国籍の人等、どの範囲で付与するか等についても検討する必要がある。

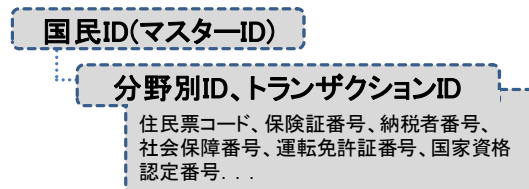


図1. 国民IDに関連する番号

2.2 付番とIDの検討課題

日本の政府の検討ではマスターIDを新規に付番するか、既存の分野別番号等を法令等によってマスターIDとするかといった選択肢も挙げられている。日本においてどのような番号が国民ID(マスターID)になるかは次のような懸念もあり、流動的な状況にある。

- ・納税者番号は取引の相手方に明示するが、住民票コードはできるだけ露出しないようにするなど秘匿性に差異がある。
- ・運転免許証番号などは年齢や取得条件に制限があり、住民票コードもすべての住民に付番されているわけではない。
- ・住基カード等が身分証明に使用できない場面もある(番号や本人写真の貼付の有無など)。

2.3 政策の検討状況

さらに行政サービスにおける負担と受益のバランスに関する意識が高まり、このバランスの適正化を図るうえで、国民IDによって国民一人ひとりを識別して行政が管理する必要があるという論調に変わってきている(表1)。

表1. 国民IDをめぐる政府・民間の動き

分類	主体	アクション
政府・省庁	民主党	2009年7月27日 マニフェスト2009「所得の把握を確実にを行うために、 税と社会保障制度共通の番号制度 を導入する」
	政府税制調査会	2009年12月22日 平成22年度税制改正大綱「 社会保障・税共通の番号制度 の導入を進める」
	国家戦略室	2010年2月8日～ 社会保障・税に関わる番号制度に関する検討会 開催
	IT戦略本部(内閣官房IT担当室)	2010年5月11日「新たな情報通信技術戦略」 「 社会保障・税の共通番号 の検討と整合性を図りつつ、個人情報保護を確保し府省・地方自治体間のデータ連携を可能とする電子行政の共通基盤として、2013年までに 国民ID制度 を導入する」
経済産業界・メディア	社会生産性本部	2009年1月28日 提言「国民の安心を担保する仕組みを構築し、 「JAPAN-ID」の早期実現 を」
	日経新聞	2009年2月1日 社説「 社会保障・納税者番号の実現へ踏み出せ 」
	日本経団連	2009年11月17日 提言「ICTの利活用による新たな政府の構築に向けて」(税・社会保障共通の番号制度)

2.4 国民IDに対するプライバシー問題

日本では従来から行政分野別に多様な番号を使用している。住民票コード、基礎年金番号、保険証番号、運転免許証番号、パスポート番号、印鑑登録番号など、1人に10個以上の番号が付されている。政府や経済界には国民IDを導入する意向があり、これまで何度も番号制度の導入が検討されてきた。住民票コードは当初「各省庁統一個人コード」という名称で1968年から検討が開始されている。納税者番号は1979年から、社会保障番号も2001年から検討がなされている。

それでは、なぜ日本では国民IDが導入されてこなかったのか。それは、住基ネット・住民票コードに代表される国民総背番号制への強い反対運動などのためである。住基ネットそのものは1994年から検討が開始されていた。当初は住民票コードの各行政分野や民間分野での利用も想定されていたが、市民団体やマスコミなどの批判を受けて、住基ネット・住民票コードの利用目的を「住民の居住関係の確認」に限定するという制約が課され、民間利用は禁止された。国民ID導入にあたっては、このような住民のプライバシー上の不安を払拭することが大きな課題といえる。

2.5 本人確認の強化の必要性

国民IDの導入にあたっては、国民IDの発行時の本人確認の強化も重要な課題となる。たとえば、本人確認の手段として最も普及している運転免許証については、次の方法で本人に気付かれずに不正に取得できるというリスクも存在する。

- ①Aさんの健康保険証等、写真付きでない本人確認書類を不正に入手する。
- ②この書類を本人確認に使用してAさんの住民票の写しを不正取得する。
- ③健康保険証、住民票写しを本人確認に使用してAさん名義の運転免許証を不正に取得する。
- ④健康保険証等をAさんに返却する。

運転免許証はそれだけで本人確認書類とする場合が多いため、免許証を不正取得した後は、それを足掛かりに預金口座の不正開設等を連鎖的に行うことが可能となってしまう。このような「不正な信用の連鎖」が発生することのないように、国民IDに関しては発行時に厳密な本人確認を行うことが必要となる。

3. ID付番の代表的な方式

国民ID実現の目的は、行政の効率化、ワン

ストップ化などの国民利便性の向上である。検討過程においては、万が一の情報漏えい時のリスク評価、その際の再付番の方法なども重要な課題である。本章では、ID付番の方法としてフラットモデル、セパレートモデル、およびセクトラルモデルを取り上げ、諸外国の導入事例に基づいてメリット、デメリットを概説する。

3.1 フラットモデル

複数の行政機関で個人識別番号を共通で利用する方式である。エストニアで国民IDの付番方法として採用されており、国民一人ひとりに付番された番号を、納税、年金、医療保険等複数の行政分野で利用するものである。この方式は、分野別番号・行政サービスの統合、ワンストップ化が容易である。しかし、1つの行政機関のデータベースから情報が漏えいした場合、国民IDをすべて再付番する必要が発生する。不正利用や漏えい時のデータマッチングのリスクも高い[1]。

3.2 フラットモデル(符号化モデル)

フィンランドもフラットモデルを採用しているが、国民IDをそのまま使用するのではなく符号化した値を用いる。この方式は、各行政機関が保有する個人データを分野間で連携して使う、いわゆるワンストップ化が可能である。個別データベースから情報漏えいがあった場合でも国民ID自体を再付番する必要はない。しかし不正利用や漏えい時のデータマッチングのリスクは高い[1]。

3.3 セパレートモデル

分野ごとに個人識別番号を付番し、番号間に関連性をもたせない方式である。この方式は、不正利用や情報漏えい時のデータマッチングのリスクが低い。しかし、分野をまたぐ個人データの利用は難しい。

このモデルに該当するドイツでは、1970年代に、住民登録等の行政事務の効率化を目的に個人識別番号の導入が提案されたが、連邦憲法裁判所が「行政機関は国民の生活を管理監視するようなデータの持ち方をしてはならない」とし、分野横断的な個人識別番号を違憲としたことにより廃案になった[1]。2009年からHealth Cardが発行されるなど各種ICカードの発行が計画されているが、一方では2005年に「共通eCard戦略」が発表されており、各種ICカードの機能を電子IDカードに統合する計画もある。電子IDカードは2010年11月から発行され、電子政府や電子商取引などインターネット上で個人を認証するツールとしても使用される。電子IDカードのシリアル番号が券面に付されるが、これはカードの発行管理にのみ使用される。このシリアル番号を他のカード等との共通番

号として使用することは法律により禁止されている。

3.4 セパレートモデル(変換テーブル式)

分野別番号を1つのデータベース(ID変換テーブル)で関連付ける方式である。データベース上の情報へのアクセス記録を本人が閲覧できる。3.3で述べたセパレートモデルと分野別番号の仕組みは同じように見えるが、分野別識別番号の不正利用・情報漏えい時のデータマッチングのリスクは低くない。データベース上で個人を識別する番号が漏えいした場合は、すべての分野別番号が漏えいしてしまうリスクが高い。この方式は日本での採用候補となっているが、本稿で挙げた方式の中ではリスクが高い方式だといえる。

3.5 セクトラルモデル

セクトラルモデルはオーストリアで利用されている方式である。この方式の個人識別番号は、大きく3階層に分かれて付番される。最初に、連邦内務省が各自治体から集めたCRR番号(中央住民登録簿番号)を発行し、データ保護委員会がCRR番号に基づきソースPIN(秘匿番号)を発行する。次にデータ保護委員会がソースPINから分野別番号(ssPIN)を発行する。分野別番号は税制、社会、教育などの行政分野ごとに保存・管理されている。当該行政分野以外で利用、保存することは禁止されている。また、分野別番号からソースPINが判明しないように、不可逆性を確保している。

電子行政サービスのICカードには、ソースPINが保存されているが、各行政分野ではソースPINから変換された分野別番号を利用している。このため、セクトラルモデルでは、個人識別番号と分野別番号が直接結びつかず、「国民総背番号制」の批判も生じにくい。また、各分野別番号はデータ保護委員会を介して他の分野別番号との紐付けが可能である。運用方法もカードには1つの番号を記録するのみで良く、カードへの番号の追加・変更などの必要がない。しかし、各行政分野の分野別番号を体系的に付番する際の運用負荷がかかる[1]。

4. セキュリティとプライバシーからみた課題

システムの情報漏えい防止策を検討するうえで、ID付番の設計が重要な要素となる。ID付番を設計する場合、セキュリティとプライバシーという2つの側面から検討する必要がある。

4.1 マスターIDとトランザクションIDの識別

IDには、ほぼ恒久的に変更されない「マスターID」と、日常的に使用され情報漏えいや悪用

が確認された場合に容易に変更できる「トランザクションID」の2種類がある。セキュリティ面からまず検討すべき点は、マスターIDとトランザクションIDの識別である。次に、容易に再付番できるものをトランザクションIDとする必要がある。

複数の病院間で患者情報を共有しようと計画されている地域医療情報の連携を検討する議論に患者IDとして運転免許証番号を候補に挙げている例があるが、運転免許証番号は容易に変更できるものではない。運転免許証番号が日常的に患者IDとして使用された結果、悪意のある第三者に知られることで不正利用された場合、ただちに運転免許証番号を変更することは困難である。本人の希望があれば変更できるとされている住民票コードも各自治体に配布されている番号枠が少ないことや住基カードを書き換えるには役所へ出頭しなければならないことを考えると容易に変更できるとはいえずトランザクションIDとしての使用には向いていない。何をもってマスターIDとし、何をもってトランザクションIDとするか、十分な議論が必要である。電子政府として先進的なシンガポールでは、指紋に代表される生体情報をマスターIDに使用することが検討されている。

4.2 再付番方法

セキュリティ要件として次に検討すべき点は、データ漏えい時の再付番方法である。IDが漏えいした場合、悪用された痕跡が発見されなくとも、悪用されることを想定して、短期間でIDの再付番ができる方策を検討しておく必要がある。次のような検討が必要である。

第1に漏えい件数を極力少なくすること、第2にできるだけ多くのID発行窓口を用意して短期間でIDを再付番できる体制を確保することである。漏えい件数を極力少なくするためにはデータをセグメント化(分割)する必要がある。ID発行窓口は、仮に年間1000万人規模の発行能力を用意しても日本の人口規模を考慮すると再付番と発行に10年以上の年月が必要となり、現実的ではない。先に紹介したシンガポールでは、銀行をはじめとする金融機関にID発行窓口業務を委ねることが検討されている。

4.3 名寄せ防止によるプライバシーの確保

プライバシーの面からは容易にデータのマッチングが行えないことを保証する必要がある。すべての行政サービスに同じIDが使用される場合、名寄せが容易になるためプライバシーの侵害につながるなどの批判がある。諸外国をみても行政、医療情報、税務情報における名寄せへの懸念を払拭する制度作りがなされている。たとえばドイツでは2009年から税務識別

番号(納税者 ID)の利用を開始したが、税務への利用に限定している[2]。

こうした批判に応えるためには、行政サービスごとに異なった ID を使用し、容易に名寄せできない仕組みが望まれるが、行政サービスの受給者である国民としては、複数の ID を使い分ける煩わしさが生じる。また、名寄せができないことを悪用して行政サービスの不正受給を行う者を摘発するためには、本人の同意がある場合または、第三者機関の審査など特定の条件を満たした場合のみ名寄せを可能とする仕組みが必要である。国民 ID は、こうした相反する要件を同時に満たす必要がある。

5. アーキテクチャからみた課題

アーキテクチャの視点からは ID 付番の設計に求められる要件の実装を検討していくことが重要である。第 4 章で挙げたとおり、「マスターID とトランザクション ID の識別」、「再付番への対応」、「名寄せの防止」を実現するための方式や技術が求められる要素となる。

すでに、諸外国で国民 ID の実装が行われているケースも見受けられるが、第 3 章の事例にもあるとおり、フラットモデルやセパレートモデルでは、この要件を満たしていない。

第 5 章では、ID 付番の設計に求められる要件を満たすことが可能であると思われる新しい技術や方式を取り上げ、検討を行う。

5.1 要件を満たす方式について

セクショナルモデル等で実装が行われている方式に加え、要件を満たすことのできる方式として、次の 3 つを取り上げる。

- ・ダイナミック ID
- ・OpenID
- ・トークナイゼーション

(1) ダイナミック ID[3]

ダイナミック ID は、複数のサーバとの認証を個々のサーバが有する静的な ID を用いて行うのではなく、動的な ID を振り出して行う方式である。動的な ID の振り出しについては、ID とパスワード、スマートカード等による 2 要素認証の仕組みを採用している。この方式では、認証時に、ユーザは ID をスマートカードに入力し、スマートカード内に格納された情報を元にしたハッシュ値を計算して動的な ID を生成し、認証サーバへログインメッセージとして送信する。ユーザと認証サーバ間はハッシュ化された値でのみの認証となるため、動的な ID が経路上で漏えいしても個人を特定することができない。本人のマスターID は、スマートカードに格納されるだけでネットワーク上へは流れず、アプリケーションへのログインは、動的に生成されたトランザクション ID により行わ

れる。また、トランザクション ID は毎回動的に生成されるため、万が一漏えいしても、再付番の必要がない。トランザクション ID により名寄せを行うこともできない。ただし、動的に生成した ID をアプリケーションへ連携させるためのリモートシステムが必要となり、運用負荷などの課題が懸念される。

(2) OpenID[4]

OpenID は、OpenID Foundation により策定された仕様に基づき構築された OP (OpenID Provider) により運営されている。OpenID は分散方式であり、OP の承認や認証を行う機関はない。OpenID では OP が発行する URL 形式の ID を用いて、OpenID と連携しているサイト RP (Relying Party) へのシングルサインオンを可能にする仕組みを提供している。ユーザは、利用する OP を自由に選択できる。複数の RP の ID を覚える必要がなく、管理を OP に任せることにより、セキュリティと利便性を享受することができる。RP への認証時、認証は OP で行われ、OP の認証に用いられるマスターID は、RP には渡されず、認証を行った OP から、URL 形式の ID が渡される。さらに、ユーザがどのサイトにどのような情報を提供するかを決めることができるため、ユーザが意図しないデータのマッチングが行われにくい。ただし、信頼できる OP の選択や、登録された ID の管理をユーザが個人の責任で行う必要がある。

(3) トークナイゼーション[5]

マスターID とトランザクション ID の組み合わせに用いられる方式をトークナイゼーション (Tokenization) という (図 2)。マスターID を無意味な数列 (トークン) に置き換えて、トランザクション ID を生成する技法である。トークン化された情報は、暗号化と同様に、データが漏えいしても個人を特定できない。システム的にはデータベースの構造変更や画面表示の変更が不要で導入が容易であることから、データベースの暗号化が求められているシステムで広く普及している。

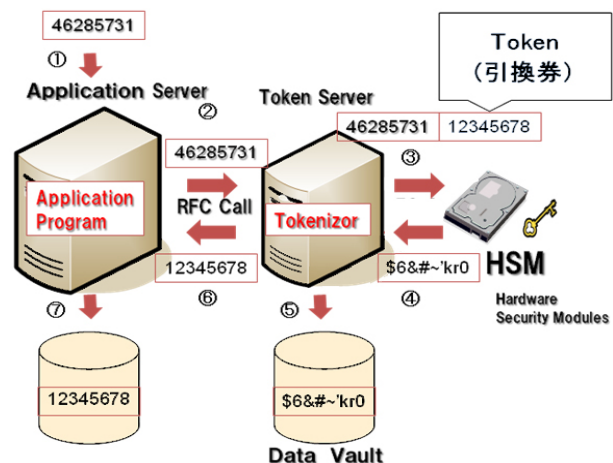


図 2. トークナイゼーション

5.2 実現に向けた課題

ID 付番の設計に求められる要件の実現に加え、個人情報オンラインでやりとりする際に、個人情報が漏えいしても第三者が悪用できない仕組みを併せて実装することが必要である。具体的には、認証を行う際に必要とされる情報やパスワードが、認証の度に異なるものとする方式を採用することが考えられる。この方式により、ID やパスワードをワンタイム化することで、情報の漏えいに関するリスクを低減できる。これまでのセキュリティ対策は、情報漏えいを起こさない仕組みに注力していたが、ここではID とパスワードが漏えいしても、第三者が入手したパスワードはすでに利用できないものとなっており、入手したID とパスワードを不正使用すること自体を防止する具体策となる。

現状では、日本でもオンラインバンキングの本人認証方法等でワンタイムパスワードのトークンの配布が行われている。また、すでに実現されている方式であるセクショナルモデルでは、生涯不変なマスターID から共通鍵暗号方式またはトークナイゼーションで生成されたトランザクションID が日常のID として使用されている。セクター単位で大量のID が情報漏えいする可能性はあるが、漏えいした際には、アーカイブされたトランザクションID と新たに付番されたID とをマージして新たなID を生成することで、漏えいしたID を無効にすることができる。暗号化されてアーカイブされているトランザクションID の使用に際して、暗号鍵を管理する第三者機関の承認の下に使用が許される。このような仕組みが導入されることで情報漏えい事故が起こっても被害者が出ない「情報漏えいに強いシステム」が構築される。情報漏えいを起こさない仕組み作りが重要であることはいままでのまではないが、さらに、情報漏えい事故を起こしても被害者を出さない仕組み作りが今後の課題である。

6. まとめ

本稿は、現在、具体的な検討が進んでいる国民ID 構築に関して、議論を尽くして進めるべきである3点の事項（セキュリティ・プライバシー・アーキテクチャ）について問題提起と提言を行った。この3点以外にも、国民ID の民間利用による財源の確保など議論を尽くすべき事項は多い。

国民ID はあくまで国民自身のためのインフラ投資であり、高齢化、高度医療体制の充実といった点など社会保障制度全体の強化につながる点にも十分配慮したものでなければならぬ[6]。第1章で述べた豪州の議会を中心とする国民的議論の経緯[7]などにおいても、①付与対象者やその強制付与の範囲、②ID データベースの登録項目や認証媒体の保有情報の内容、③中央管理システムの保管データやネットワークへのアクセス権の明確化、④民間部門のID 利用の限定方法、⑤登録情報への本人の開示請求・修正権等が具体的に論議されている。

国民ID 構築は、日本が将来に向けて技術力や法制整備、方式設計等に関する先進国となり得るか、安全でより便利な社会を築けるかを左右するものであるといっても過言ではない。拙速に進めるのではなく、十分な議論を尽くすことが必要である。

参考文献

- [1] 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1月
- [2]<<http://www.cao.go.jp/zeicho/siryou/pdf/sg5kai5-2.pdf>>、<<http://www.pruefzifferberechnung.de/Identifikationsnummer.shtml>>、<http://bundesrecht.juris.de/ao_1977/index.html>、2010年5月28日アクセス
- [3]<<http://www.waset.org/journals/waset/v59/v59-34.pdf>>、<<http://jglobal.jst.go.jp/public/20090422/200902284913940300>>、<<http://jdream2.jst.go.jp/jdream/action/JD71001Disp?APP=jdream&action=reflink&origin=JGLOBAL&version=1.0&lang-japanese&db=JSTPlus&doc=08A1078117&fullink=no&md5=872ef55ddf3345f4954f32a1ec594f9>>、2010年5月28日アクセス
- [4]<<http://openid-foundation-japan.github.com/openid-authentication.html>>、2010年5月28日アクセス
- [5]<http://www.netone.co.jp/solution/security/colum/colum_103.html>、2010年5月28日アクセス
- [6] ID の多機能化を国民に説明している例。フィンランドの“Electronic Identity and Certificates”の解説サイト。<<http://www.vaestorekisterikeskus.fi/vrk/home.nsf/www/electronicidentity>>、2010年5月28日アクセス
- [7]<http://austlii.edu.au/~graham/publications/2010/CyberLPC_submission2.pdf>、2010年5月28日アクセス