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

2006－DPS－128 (20)
2006－GN－ 61 (20)
2006－EIP－ 33 (20)
2006／9／15

電気通信事業への Privacy Impact Assessment (PIA) の適用に関する一考察

佐藤 亮太† 藤村 明子† 雨宮 俊一† 間形 文彦† 谷口 展郎‡
塩野入 理† 金井 敦†

† 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所
‡ 日本電信電話株式会社 NTT サイバースペース研究所
〒 239-0847 神奈川県横須賀市光の丘 1-1

{sato.ryota,fujimura.akiko,amemiya.shunichi,magata.fumihiko,
taniguchi.noburou,shionoiri.osamu,kanai.atsushi}@lab.ntt.co.jp

あらまし 個人情報漏洩問題などが多発していることにより、企業におけるプライバシ保護の対策の重要性が高まっている。それら問題の特徴からプライバシ保護には事前対策が重要であるといえるが、日本においては確立された事前対策が存在していないという現状がある。本稿では、事前対策の手法として米国、カナダ等で政府の IT システム導入時に実施されているプライバシ影響評価 (PIA) 手法に着目し、PIA 手法の一つのプロセスであるデータフロー分析を既存サービスを対象に実施することによって、PIA 手法の実効性を検証すると共に、その適用可能性についての考察を行なう。

A Consideration on Application of Privacy Impact Assessment (PIA) on Telecommunications Services.

Ryota SATO† Akiko FUJIMURA† Shunichi AMEMIYA†
Fumihiko MAGATA† Noburou TANIGUCHI‡ Osamu SHIONOIRI†
Atsushi KANAI†

†NTT Information Sharing Platform Laboratories, NTT Corporation
‡NTT Cyber Space Laboratories, NTT Corporation
1-1, Hikarino-oka, Yokosuka, 239-0847, Japan

{sato.ryota,fujimura.akiko,amemiya.shunichi,magata.fumihiko,
taniguchi.noburou,shionoiri.osamu,kanai.atsushi}@lab.ntt.co.jp

Abstract Because a leakage of personal information is occured frequently, it is more important to take measures to prevent such leakage for private enterprises. It is important to take preliminary measures to prevent such leakage from the viewpoint of Privacy Protection, but there is not such preliminary measures in Japan. In this paper, we make an introduction of the Privacy Impact Assessment (PIA) method as one of such preliminary protection measures. It is a mandatory process before governmental procurement of IT systems in Canada and the United States to assess the systems with regard to privacy protection. Considering to introduce PIA into private enterprises in Japan, we try to assess a few telecommunications services and examine the possibility of the introduction.

1 はじめに

1.1 個人情報保護法と企業の対応

2005 年 4 月に全面施行された個人情報保護法 [1] により、個人情報保護に関する関心が一気に高まり、連日多くの個人情報漏洩事件が報告されるようになった。このような背景のなか、いくつかの企業ではノート PC の持ち出しを禁止することにより業務効率の低下を引き起こしているなど過敏な反応が見られる一方で、施行から一年経っても問題のある名簿業者は減っていないとの報告もあり、本来、個人情報保護法が目的としていた「個人情報の有用性に配慮しながら、個人の権利利益を保護」が達成されているとは言いがたい状況となっている。また、企業においてはその社会的責任 (CSR:Corporate Social Responsibility) の重要性が近年、強く意識されるようになっているといった背景もあり、特に個人情報がサービス提供

には必須となる企業においては、その個人情報の取り扱いについて法制度を正しく理解し、適切な対応を行なっていくことが今後はますます重要となる。

1.2 電気通信事業におけるプライバシ保護

個人情報がサービス提供に必須となる企業群の一つとして電気通信事業者が挙げられる。電気通信事業者に対しては個別の個人情報保護に関するガイドライン [2] が策定され、より詳細な内容が示されている。また、電気通信サービスを提供する際には、電気通信事業法 [3] に規定されている「通信の秘密の保護」も重要となる。電気通信事業者にとって、個人情報保護や通信の秘密の保護は法律の遵守という観点からだけではなく、ユーザのプライバシ保護という観点からも対応が重要であり、サービスの提供時には十分な対策を施す事が望まれる。

2 プライバシ影響評価

個人情報漏洩事件を中心に、プライバシに関わる事件が多く顕在化していることは上述の通りである。近年のプライバシに関わる事件においては、その賠償金額もさることながら、電子データとして漏洩が起こるため被害者の数が非常に多くなることが特徴的である。例えば、1999 年京都府宇治市において、住民基本台帳に記された住所、氏名生年月日などの個人情報が漏洩した事件においては、原告 3 人に対して 1 人当たり 1 万 5 千円の賠償金を支払う事が命じられている [4]。この際の全情報漏洩件数は約 22 万人分と報告されており、もし、被害者となった約 22 万人全てに賠償金を支払う事になれば、その合計は約 33 億円にも及ぶ計算となる。つまり、漏洩した側には多大な経済的損害が発生可能性があるということがいえる。また、電子データとして個人情報が漏洩した場合、実質的にはそれを完全に回収することが不可能であり、被害者にとっての精神的、経済的苦痛が永続的に続く事が懸念される。

このように、「多大な経済的被害が発生する可能性」と「問題発生後の修復の困難性」という 2 つの特徴より、プライバシ問題はそれを起こさないための事前の対策が重要であるといえる。そして、そのプライバシ保護のための事前対策としてプライバシ影響評価（Privacy Impact Assessment 以下 PIA）[5] が提案されている。

2.1 PIA の現状

PIA は、カナダやアメリカの電子政府・自治体において、IT システムを導入もしくは大幅な変更を加える際に、事前にプライバシ影響評価を行い、その結果をシステムの設計に反映させ、さらに導入後の運用状態を把握し、サービスへの反映までを考慮したアセスメント手法である。カナダでは、1983 年に施行されたプライバシ法によって、政府機関が新規の IT システムを導入するにあたり、PIA の実施が義務付けられており [6]、同様に、アメリカにおいても 2002 年に施行された電子政府法において、PIA を行うことが義務付けられている [7]。

日本の総務省では「住民のプライバシーの保護に関する新しい考え方と電子自治体におけるそのシステム的な担保の仕組みについての研究会」を主催し [8]、そこで PIA を取り上げ、日本の実情に応じて PIA の考え方を実践的に組み入れていくことが有効であると結論付けている。

2.2 PIA の全体的な枠組み

PIA はカナダやアメリカを始めとする国々で実践されているが、統一されたフォーマットはなく、それぞれが独自のフォーマットを用いている。そこで、本稿では総務省の研究会でも取り上げられているカナダにおける PIA を例に、そこで紹介されている PIA のフォーマット（以下、既存フォーマット）を基本にして、PIA の全体的な枠組みについて分析を行なう。

既存フォーマットには、対象 IT システムについてのプライバシ影響評価を行なうプロセスが記されている。このプロセスは、図 1 に示したように、大きく分けて 4 つのステップに分けて考える事ができる [9]。

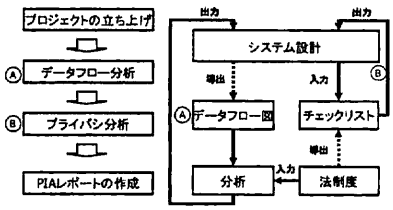

図 1: PIA の 4 つのステップ

最初のステップである「プロジェクトの立ち上げ」においては、当該システムの概要の記述や法制度の観点からのプライバシ保護要件の抽出などを行い、プロジェクトの体制構築・整備を行なう。

「データフロー分析」においては、当該システムの業務プロセス図を基に、そこに流通する個人情報を可視化することによりデータフロー図の作成を行なう。その際には、プライバシ測定基準とよばれる観点より当該システムで利用されている個人情報、その取り扱い状況、懸案事項について明らかにする [11]。プライバシ測定基準に関しては、第 3.3.1 節において実際の分析を行ないながら詳しく説明をする。さらに、明らかになった懸案事項に対しては、関連する法制度から個別に分析を行い、そこからの要請をシステムの設計に反映させる。

続く「プライバシ分析」においては、「プロジェクトの立ち上げ」のステップで検討された法制度の観点からプライバシ保護要件を反映させた PIA チェックリスト [12] に従って、当該システムが抱えているプライバシに関する問題を網羅的に明らかにし、その影響や対策についての分析が行なわれる。この PIA

チェックリストについては必ずしも全てに完全に対応する必要なく、当該システムに割り当てられた資産やその目的に応じて、どの程度対策を打つかを把握する事が肝要である。ここで明らかになった対策については、当該システムへ反映し、その変化を含めて最初のステップから分析を繰り返すことになる。

最後の「PIA レポートの作成」においては、アセスメント結果をまとめて公表する。当該システムについてのアセスメント内容について、全ての対象となるユーザに理解できる形で開示することによって、ユーザへの説明責任を果たすと共に、ユーザとの積極的なコミュニケーションを図るためのツールとしても利用される。このように、ユーザの反応も組み入れられるプロセスを設けることによって、例えば、後にユーザの心理的な反発から大きなシステム変更を余儀なくされるようなリスクといったものも軽減する事が可能となる。

2.3 PIA 実施における政府と電気通信事業者との比較

行政機関において PIA が利用されてきた大きな理由としては、行政のために国民や住民は選択の余地なく個人情報の提供を行なわなければならないことが挙げられる [13]。一方で、民間企業が個人情報の提供先の場合には、ユーザが自らの意思で情報をコントロールすればよいため、行政機関が提供先である場合に比べてプライバシ保護対策の必要性が小さいと見ることもできる。しかしながら、例えば電話のように人々の LifeLine として電気通信サービスを提供する場合には、行政サービスと同様にプライバシ保護を積極的に行なう事が重要であろう。

以上の観点から、本稿においては、日本の電気通信事業への PIA の適用可能性を探ることにより、プライバシアセスメント普及によるプライバシ保護の在り方について模索する。具体的には、既存の電気通信サービスやこれから想定されるサービスを PIA の対象とし、PIA においてプライバシに関する分析を行なう実質的な第一ステップであるデータフロー分析を行なうことによって、PIA の実行性の検証と今後の課題などについての考察を行なう。

3 PIA の適用

3.1 発信電話番号通知サービスについて

既存の電気通信サービスとして、本稿では発信電話番号通知サービス（以下、発番通知サービス）を取り上げることにする。この発番通知サービスは、1997 年にサービスを開始するにあたり、NTT が有識者を集めて発信電話番号利用サービスアセスメント研究会（以下、アセスメント研究会）を開催し [14]、そこに内在するプライバシ問題と対策について十分な議論がなされたという経緯がある。そこで、このサービスに対してデータフロー分析を実施する事により、過去の議論によって挙げられたプライバシ問題等が導出されるかを確認する。

3.2 アセスメント研究会による議論

発番通知サービスは、当時社会問題となっていた迷惑電話により侵害されていた「着信者のプライバシ」の保護対策として導入が検討された。そして、アセスメント研究会における議論により、発番通知サービスが導入される事による 2 つのプライバシ問題が提起された。

- 発信者のプライバシ
  発信者番号が相手に通知されることによる、発信者の匿名性が侵害される問題。
- 目的外利用に関するプライバシ
  着信者がデータを蓄積して、発信者が意図しない目的で収集、利用される問題。

さらに、これらの解決策として以下の機能を備えることも提案された。

- ブロッキング機能
  発信者のプライバシと目的外利用に関するプライバシの保護のための機能で、通話前に 184 を付けると通知されない機能（per call blocking）や回線毎に通知されない機能（per line blocking）のこと。

3.3 既存サービスに対するデータフロー分析

ここでは実際に発番通知サービスの業務プロセス図を基にして、データフロー分析を実行する。今回はアセスメント研究会の議論に合わせて、発信者や着信者といったエンティティに注目したデータフロー図を作成する。また、データフロー分析においては、当該システムにおける特徴的な処理、例えばサービスオーダー処理、通常接続処理、明細・料金処理といったもの毎に、データフロー図を切り分けて作成することも可能である [15]。

エンティティを視点として通常接続処理に注目した当該システム全体の大きな情報の流れを図 2 に示す。これより、発信者、着信者の電話番号が当該システム上を移動していることがわかる。

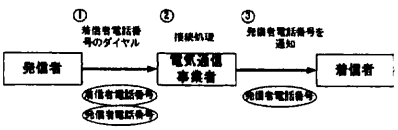

図 2: 発番通知サービスにおけるデータフロー図

3.3.1 プライバシ測定基準と分析

上記データフロー図をもとに分析を行う際には、第 2.2 節で述べたように、以下のようなプライバシ測定基準を用いた分析を行なう。

- 個人の特定性
  一つの情報から個人が特定される事を防ぐため、当該システム上で情報がどこへ移動したかを分析する。
- データの結合性
  複数の操作によって得られた情報をつき合わせて個人を特定される事を防ぐため、複数の情報が相互にリンクされたり、参照状態にあるかを分析する。
- システムにおける観察容易性
  当該システムの操作の記録などから個人を特定される事を防ぐため、その情報が誰に、どの程度アクセスされ、使用されるかを分析する。

「個人の特定性」の観点からは、発信者の電話番号が電気通信事業者、着信者へと移動していることから、それぞれ「通信事業者に電話番号が渡る事」に関する懸案事項と「着信者に電話番号が渡る事」による懸案事項の 2 つが分析対象として挙げられる。

また、「データの結合性」の観点からは、発信者と着信者の電話番号が電気通信事業者において結合しており、これに関する懸案事項を挙げるべきであるが、紙面の都合上、詳細な分析は省略する。

なお、「システムにおける観察容易性」の観点についてであるが、今回のデータフロー図においては通信事業者側におけるデータの蓄積等の処理を対象外としたため検討外となる。

3.3.2 法制度の観点からの分析

次に、プライバシ測定基準によって挙げられた 2 つの懸案事項に対して、関連する法制度の観点から分析を行なう。なお、発番通知サービスの議論が行われた 1997 年とプライバシ保護要件を同じくするため、当時の法制度に準ずることとし、2005 年に施行された個人情報保護法等は対象としない。

「通信事業者に電話番号が渡る事」についての分析

ここでは、憲法や電気通信事業法に示されている通信の秘密と、電気通信事業における個人情報保護に関するガイドライン [16] と、いわゆる OECD の 8 原則 [17] の「収集制限の原則」、「目的明確化の原則」がプライバシ保護要件である。通信の秘密については、電気通信事業者の正当業務行為として、役務の提供上必要な範囲において電話番号等の接続情報を知ることが認められている [18]。ただし、個人情報保護の観点から、個人情報は事業の提供に必要とされる一定期間が過ぎた場合は、遅滞なく消去せねばならない。以上から、電話番号に関する保管期間を定め、情報を破棄する仕組みを備える必要があることわかる。

「着信者に電話番号が渡る事」についての分析

通信の秘密、電気通信事業における個人情報保護に関するガイドライン、OECD の 8 原則の「利用制限の原則」がプライバシ保護要件である。これらの観点により、この懸案事項はさらに「電話番号が着信者に知られることによる問題」と「その着信者が電話番号をデータベース化して利用される問題」に分けられる。

前者の問題は、通信に関与する当事者間における通信の秘密の問題である。発信者、着信者それぞれが相手に対して主張する秘密であるため、発信者が着信者に電話番号が知られることを認める意思表示があればよい。つまり、この問題は第 3.2 節で述べた「発信者のプライバシ」と同様の問題であり、PIA のアセスメントからもアセスメント研究会と同様の問題を導き出されうることが明らかとなった。また、その解決策の一つとして「ブロッキング機能」による意思表示の仕組みが必要であるといえる。

また、後者の問題は、OECD の 8 原則の中の「利用制限の原則」に従うと、電話番号情報に関しても発信者の意図しない形での情報収集は避けねばならない事になる。これは第 3.2 節で述べた「目的外利用に関するプライバシ」と同様の問題であり、その一つの解決策として「ブロッキング機能」が必要といえる。

3.4 既存サービスへの PIA 実施結果からの考察

上述のように、発番通知サービスに対して PIA のデータフロー分析を行なった結果、アセスメント研究会における結論を導出し得ることが示された。加えて、通信事業者に対して、当該システムにおける電話番号の保存期間についての提案も行なう事ができた。当然のことながら、アセスメント研究会の結論を知った状態でアセスメントを行なっていることになるが、データフロー分析のスキームに従い、系統立った分析を行なう事によって、有識者を多く集め議論を行なう代わりに、効率よくプライバシ保護対策を実施できる可能性が示唆されたということができる。

3.5 仮想サービスに対するデータフロー分析

本節では、以下に述べる IPv6 網を用いた仮想の電気通信に関するサービスに対してデータフロー分析を実施する事によって、当該サービスに関するプライバシ問題の提起を行なうと共に、PIA の実効性についてのさらなる検証を進める。

アセスメント対象となる仮想サービスは IPv6 網上における IP 電話の発番通知サービスであり、当該システム構成は、複数事業者間とのやり取りは無く、さらに、SIP サーバによる処理など通信事業者側で

行う処理については簡単のため対象外とする。今回は、IPアドレスの取り扱いの責任が最も曖昧となる通信の当事者と事業者間の問題に着目し、また、通信の当事者端末の機能を考慮して、電話機端末には電話番号のみが表示され、ホームゲートウェイ（以降はHGWと呼ぶ）は通信相手のIPアドレスが通知される事を前提条件とする。

図3に当該システム全体の情報の流れを示す。

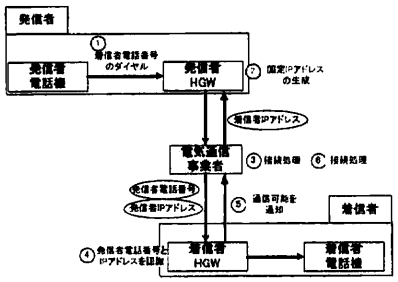

図3: IP電話の発番通知サービスにおけるデータフロー図

3.5.1 プライバシ測定基準からの分析

「個人の特定性」の観点から、通信事業者に発信者や着信者の電話番号やIPアドレスが渡っており、着信者は発信者の電話番号とIPアドレスを知る事が可能であることが分かる。これらより、「通信事業者に電話番号やIPアドレスが渡る事」に関する懸案事項と「着信者に電話番号やIPアドレスが渡る事」に関する懸案事項の2つが挙げられる。さらに、通信が確立した場合には発信者側に着信者のIPアドレスが移動していることが分かる。これにより、「発信者にIPアドレスが渡る事」に関する懸案事項も挙げることができる。

また、「データの結合性」の観点からは、着信者側における2つの情報の結合に着目すると、「発信者の電話番号とIPアドレスが結びつく事に関する懸案事項」が挙げられる。

なお、「システムにおける観察容易性」の観点についてであるが、今回のデータフロー図においては通信事業者側におけるデータの蓄積等の処理を対象外としたため検討外となる。

3.5.2 法制度の観点からの分析

当該システムに対する関連法制度としては、本稿の第3.3.2節で用いた法制度に加えて、2005年に施行された個人情報保護法を新たに考慮せねばならない。

ここで、各懸案事項の分析に入る前に、IPアドレスの取り扱いについて述べておく。電話番号は電話帳などにより個人を特定されうるため個人情報と一般的に考えられている一方で、IPアドレスの扱いに関しては議論の余地がある。個人情報保護法第2条によると、個人情報とは特定の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することができるもの、という旨の定義がされている。

今回の対象としているIPv6網においては、IPアドレスを払い出す機能の一つにステートレスアドレス自動生成がある。これは、IPv6のホスト（図3では電話機）が、MACアドレスを利用して自動的にIPアドレスを生成する機能である。この場合、異なるIPアドレスであっても、そこに含まれるMACアドレスにより、同一の端末からの通信であるという情報が漏れる。そして、このIPアドレスが何らかの形で実社会の個人を特定できる情報と結び付く場合は、これも個人情報として扱われなければならない。したがって、そのような状況下では、IPアドレスも電話番号と同等に個人情報保護法の範囲内で議論されるべきである、ということが言える。

「通信事業者と着信者に電話番号やIPアドレスが渡る事」についての分析

憲法や電気通信事業法と個人情報保護法をプライバシ保護要件とする。ここでの分析においては、IPアドレスを電話番号と同じ個人情報として扱う事で、本稿の第3.3.2節で行なった分析と同じ議論が可能である。さらに、個人情報保護法第19条のデータの内容の正確性の確保や、第3条に記述のある自己情報コントロール権に基づいた個人情報保護の要件からも「電話番号に関する取り扱いについての仕組み」や「ブロッキング機能」の必要性を導出することができる。

「発信者にIPアドレスが渡る事」についての分析

ここでのプライバシ保護要件も上記の懸案事項と同じである。着信者側にもIPアドレスの通知を選択できるようにする、もしくはIPアドレスの通知が不必要であるならば、それを着信者には知らせないような機能が必要といえる。

「発信者の電話番号とIPアドレスが結びつく事」についての分析

電話番号が個人情報であれば、電話番号と結びついたIPアドレスも個人情報とみなされるため、法的な両者の取り扱いは同等となる。また、当該システム上においては、通信の当事者は相手のIPアドレスをHGWにて知る事ができる。従って、発信者がそのIPアドレスを知らせる、知らせないの選択ができる仕組みを整える必要がある事が導かれる。

3.6 仮想サービスへのPIA実施結果からの考察

上述のように、当該システムにおいては、IPアドレスに関しても発信者の意思を反映させる仕組みの必要性が導かれた。その具体的な仕組みの一つとしては、同一のMACアドレスを含む複数IPアドレス間のリンクを断つ仕組みを通信事業者側に導入することが挙げられる。

また、本稿の第3.3.2節で明からかにされた電話番号に関する取り扱いについての仕組みやブロッキング機能に対する、個人情報保護法を考慮した現在の法体系における妥当性も確認された。

さらに、当該サービスの特有の問題として、着信者のIPアドレスが発信者に知られてしまうという新たなプライバシ問題も発見され、HGWにはIPアドレスを通知しない機能などが求められることが分かった。

4 まとめと今後の展開

本稿においては、プライバシ保護に関する事前対策としてPIAに着目し、その概要について述べ、電気通信サービスへの適用について考察した。発番通知サービスとIP電話における発番通知サービスについて実際にPIAの一つのステップであるデータフロー分析を実施することにより、いくつかのプライバシ問題の提案を行ない、データフロー分析の実効性検証を行なった。

今回はデータフロー分析のみを実行したため、PIAのプロセス全体が有効であると結論付ける事はできない。プライバシ保護という観点からは、当該システムのプライバシ問題についての特定と対策を行える事は必要であるが、そのプライバシ保護対策の正当性についてユーザとの共通理解を醸成することが重要である。つまり、PIAレポートの作成と公開により、当該システムのユーザとのコミュニケーションを図るプロセスまで実施する事でPIAプロセス全体の有効性を議論する事が可能となる。

しかしながら、海外でPIAが実施されてきた背景には政府が法により実施を義務付けるなどの強制力が働いていた事実があり、企業においてPIAの実施を想定する場合には、導入や実施に関わるコストに対する効果を明確に示す必要がある。コストの面では、企業におけるサービス企画、開発、提供の段階でPIAを導入することにより、例えば開発スピードの減少やユーザ対応に関わる費用の増大などが想定される。これに対して、今回行なったデータフロー分析の結果により、プライバシ保護対策が系統的に効率よく行なえる可能性がある事を示唆し、PIA導入に対する効果を実践的に示す事ができた。今後は、PIAのデータフロー分析以外のステップの有効性の検証などを含め、企業おけるPIAによるプライバシ保護対策の適用可能性について検討していく予定である。

参考文献

[1] 首相官邸 (2003) "個人情報の保護に関する法律" http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html

[2] 総務省 (2004) "電気通信事業における個人情報保護に関するガイドライン" http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/denki.pdf

[3] 総務省 (1984) "電気通信事業法" http://law.e-gov.go.jp/htmldata/S59/S59HO086.html

[4] "宇治市住民基本台帳データ漏洩事件" 大阪高裁平成13年12月25日判決、平成13年(ネ)第1165号

[5] Roger Clarke(2004) "A History of Privacy Impact Assessments" http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist.html

[6] 株式会社ネオテニー編 (2003) "カナダにおけるプライバシー" http://joi.ito.com/privacyreport/Contents_Distilled/JapaneseSection/Canada_J_p06-72.pdf

[7] Office of Management and Budget(2005) "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" http://www.whitehouse.gov/omb/memoranda/m03-22.html

[8] 総務省 (2004) "住民のプライバシーの保護に関する新しい考え方と電子自治体におけるそのシステム的な担保の仕組みについての研究会" http://www.soumu.go.jp/denshijiti/jyumin_p.html

[9] 田中一郎, "環境影響評価手法を応用するプライバシー影響評価,"Cyber Security Management August 2005 vol.6 Number70, 2005

[10] Tresuary Board of Canada Secretariat"Privacy Impact Assessment Audit Guide" http://www.tbs-sct.gc.ca/ia-vi/policies-politiques/pia-efvp/pia-efvp_e.asp

[11] 総務省 (2004) "電子政府・電子自治体のためのプライバシー影響評価" http://www.soumu.go.jp/denshijiti/pdf/jyumin_p_s2.pdf

[12] 佐藤亮太, 藤村明子, 雨宮俊一, 間形文彦, 塩野入理, 金井敦, "プライバシ影響評価 (PIA) 手法の日本への導入に関する一考察," コンピュータセキュリティシンポジウム 2005(CSS2005), pp.115-120, 2005

[13] 田中一郎, "個人情報保護の事前対策を促す「プライバシー影響評価」とは," 日経BPガバメントテクノロジー, 2006 http://itpro.nikkeibp.co.jp/article/govtech/20060302/231523/

[14] 堀部政男, "発信電話番号表示とプライバシー," NTT出版, 1998

[15] E-government Unit of State Services Commission in New Zealand, "Authentication for e-government: Privacy Impact Assessment report," 2003, http://www.e.govt.nz/archive/services/authentication/authent-pia-200312/listing_archives

[16] 総務省, "電気通信事業における個人情報保護に関するガイドライン," 1998, http://www.soumu.go.jp/joho_tsusin/whatsnew/guideline_privacy_1.html

[17] 総務省, "OECD理事会勧告8原則," 1980, http://www.soumu.go.jp/gyoukan/kanri/oecd8198009.html

[18] 岡村久道, 新保史生 "電子ネットワークと個人情報保護" 現代産業選書, 2002年