

# マルチステークホルダープロセスにおける プライバシー影響評価の考察

浦田有佳里<sup>†1</sup> 下村憲輔<sup>†1</sup> 白石敬典<sup>†1</sup> 田娟<sup>†1</sup> 中原道智<sup>†1</sup> 瀬戸洋一<sup>†1</sup>

**概要:** 個人情報の収集を伴うシステムを構築する際、プライバシー保護には、プライバシー影響評価 (Privacy Impact Assessment) を事前に実施することが有効である。PIAの目的は、公共の利益を確保し、個人のプライバシーを守ると共に、ステークホルダー間の信頼関係を確保することにある。カナダや米国では行政システムを構築する際、PIAの実施を法的に義務付けている。日本で実効性をもって実施するには、理論的な裏付けが必要である。本稿では、PIAが、ユーザープライバシーを尊重するプライバシーバイデザインの考え方、およびステークホルダー間の対話による合意形成を行うマルチステークホルダープロセスより構成されることを考察する。

**キーワード:** ISO31000, プライバシー影響評価, プライバシーバイデザイン, マルチステークホルダープロセス, リスク評価

## A Study of Privacy Impact Assessment in the Multi-Stakeholder Process

Yukari Urata<sup>†1</sup> Kensuke Shimomura<sup>†1</sup> Keisuke Shiraishi<sup>†1</sup> Tian Juan<sup>†1</sup>  
Michitomo Nakahara<sup>†1</sup> Yoichi Seto<sup>†1</sup>

**Abstract:** When building a system that uses personal information, the privacy protection, it's effective to implement Privacy Impact Assessment in advance for risk mitigation. The purpose of PIA is to ensure the public benefit, together with protecting the individual's privacy right, and to ensure the trust relationship between the stakeholders. In constructing the administrative system in Canada and the United States is obliged to legal implementation of the PIA. To conduct it in Japan with the system, There is a need for theoretical support. In this paper, PIA is, consider the concept of Privacy by Design that respects user privacy, and to be composed of Multi-Stakeholder Process to carry out the consensus interactive between the stakeholders.

**Keywords:** ISO31000, Multi-Stakeholder Process, Privacy by Design, Privacy Impact Assessment, Risk Assessment

### 1. はじめに

個人情報の保護を強化すると同時に適正な利活用を目的に、2015年個人情報保護法が改正された。これにより匿名化情報や要配慮個人情報が利用できるようになった[1]。要配慮個人情報、つまりプライバシーに関する情報の扱いには、より注意を要し、リスク評価が強化される方向にある[2]。

個人情報が国境を越え、プライバシーの定義を各国で合わせる必要があり、国際標準規格 ISO/IEC29100 (プライバシーフレームワーク (プライバシー保護の枠組みと原則)) が発行され、プライバシーの定義と原則が規定された[3]。

個人情報を扱うシステムを構築する場合、事前リスク評価の重要性が高まり、諸外国ではプライバシー影響評価 (Privacy Impact Assessment, PIA) が実施されている[4]。日本でもマイナンバー制度の導入により類似の特定個人情報保護評価が実施された[5]。

日本で本格的にPIAを実施するためには、リスク評価ガイドラインの開発や第三者機関の設置が必要である。ガイドラインおよび個人情報保護委員会が整備され、PIAを実施する環境は整った[6][7]。

PIAは、リスクの可視化・軽減、関係者によるリスク

コミュニケーション (関係者の合意形成) が目的と言われている[6]。リスクの可視化・軽減に関しては、リスク評価の目的やその基準の明確化が必要である。

リスクコミュニケーションプロセスとして、行政機関では、異なる立場の意見を調整するマルチステークホルダープロセス (Multi-Stakeholder Process, MSP) が導入されている[8]。

MSPのプライバシー保護に関する事例として、オーストラリアにおけるスマートメータ導入に関わるPIAがある。ビクトリア州産業省が主催し、クラウド利用のビジネスチャンスと課題・消費者等に対する配慮の有り方について検討した。プライバシーリスクを特定、評価し、対処方策を策定した[9]。本事例は、PIAをリスク評価にツールとして利用したもので、MSPとPIAの理論的な構成について考察したものではない。

プライバシーリスク対策を実現するには、PIA, ISO31000, ISO/IEC29100, プライバシーバイデザイン, MSPなどの原則や手法の理解が必要である。

本稿では、PIAとこれらの技術との関係を考察する。本稿の構成は、2章でプライバシーバイデザインなどプライバシー対策の基本的な手法、3章ではMSPにおけるPIAの

<sup>†1</sup> 公立大学法人首都大学東京 産業技術大学院大学  
Advanced Institute of Industrial Technology

構成について考察を述べる。

## 2. プライバシー対策の基本的な手法

プライバシー対策の基本的な考え方としてプライバシーバイデザインがあり、プライバシーバイデザインの考えが適正に実装されているか確認する手法がPIAである。

### 2.1 プライバシーバイデザイン

プライバシーバイデザイン(計画的なプライバシー対策)(Privacy by Design, PbD)は、カナダオンタリオ州情報&プライバシーコミッショナーの Ann Cavoukian 博士が 1990 年代に提唱した [10]。

PbD の定義は、「プライバシー侵害のリスクを低減するため、システムの開発においてプロアクティブ (proactive 事前) にプライバシー対策を考慮するというコンセプトであり、企画から保守段階までのシステムライフサイクルで一貫した取り組みを行うこと」である。

図 1 は、PbD のコンセプトである 7 つの原則を示す。

PbD は情報技術だけでなく、組織や社会基盤も適用対象としている。また、アプリケーションにプライバシー強化技術 (Privacy Enhancing Technologies) を組み込み、組織のプライバシーリスクの低減対策を行うことが必要と主張している。

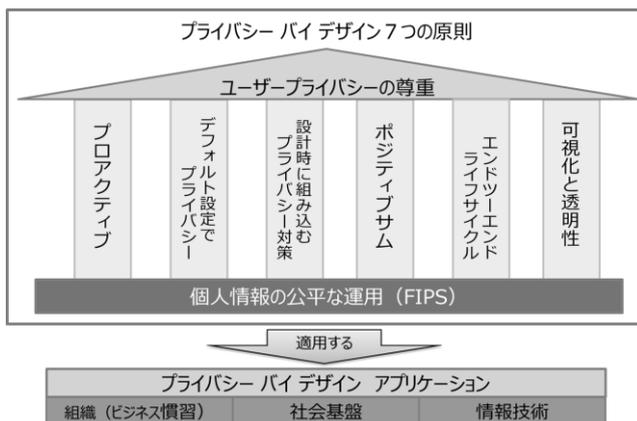


図 1 プライバシーバイデザインの 7 つの原則

PbD は、個人情報の公正な運用についての原則 (Fair Information Practices, FIPs) に則りシステムを構築することを勧めている。FIPs とは、個人情報を扱うシステムの設計開発に関する技術や個人情報に関する公正な運用についての原則をいう。

従来、社会の安全性を確保するには、セキュリティを強化し、ある程度のプライバシーの侵害は仕方がないという考え方が多かったが、PbD では、セキュリティとプライバシー両方の安全性を成立させるポジティブサムを基本としている。つまり、ポジティブサムとは、システム構築に際してプロアクティブ (事前) にビジネスプロセスにプライバシー対策とセキュリティ対策を両立し実装することである。

PbD のコンセプトが適正に実現されたか確認する手法が PIA である。個人情報を扱うシステムの構築にあたって、構築前に実施するプライバシーリスク評価により計画改善を図ることを目的としている。これにより、IT システムにおけるリスク回避や、個人情報を提供する個人や関

心のある世論への説明責任を実施することができる。

なお、PbD の 7 つの原則は、国際標準 ISO/IEC29100 (プライバシーフレームワーク (プライバシー保護の枠組みと原則)) では 11 原則となっている。詳細は 3.2 節で説明する。

### 2.2 プライバシー影響評価

プライバシー影響評価 (Privacy Impact Assessment, PIA) の定義は、以下のとおりである [4] [6]。

「個人情報の取得を伴うシステムの導入または改修にあたり、プライバシーへの影響を「事前」に評価し、その回避または緩和のために「法制度」・「運用的」・「技術的」な変更を促す一連のプロセスである。」

PIA の目的は、単にシステムのリスクを評価し、技術的な対策を実施するだけでなく、新しいシステムを構築、運用する上での前提条件である法制度、社内規定、業界ガイドラインなどに関係するリスク要因を明確にすることである。

PIA はリスクマネジメント手法のひとつであり、リスクマネジメント規格の国際標準である ISO 31000:2009 (リスクマネジメント-原則および指針) を基に PIA の手順を構成することができる。PIA の評価を実施する組織 (PIA 評価実施組織) は、図 2 に示す手順で PIA を実施する。

- PIA 計画作成  
評価対象のシステム範囲、PIA 体制、スケジュールを記載する。
- 対象システム分析  
システム構成図、システムフロー、システム要件を分析する。
- プライバシーリスク識別  
個人情報の識別は、個人が特定できる情報について、識別する。リスクシナリオの識別では、システム構成図やシステムフローなどにより、リスクを特定する。
- プライバシーリスク分析  
リスクが発生した場合のシステムや業務への影響度を明確にする。発生可能性の評価では、リスクの発生可能性をあらかじめ設定しておく。
- プライバシーリスク評価  
必要なリスク対応検討として、個人情報に関する法令やガイドライン・社内規定などから抽出した要求事項を評価シート (チェックリスト) としてまとめる。評価項目は ISO/IEC29100 の 11 原則を用いる。

PIA では、評価シートを基準とし、対象システムの企画書・設計書から個人情報フロー等を分析して、システムの設計が基準を満たすか否かの評価、および、リスクの影響度を評価する。

- プライバシーリスク対応  
対策が必要なリスクに対策をたてる。
- PIA および対応 プロセスの記録  
評価結果を基にプライバシーリスクの特定と対策方法についてまとめる。つまり、PIA 報告書を作成し、制度面や技術面における改善を助言する。

この手順を通して、各手順に必要な監査及びモニタリング、コミュニケーションや協議が実施される。また、PIA の実施によって、稼働後のプライバシー問題の発覚による稼働停止や、それに伴って発生するビジネス上のリスク、システム改修コストを軽減することができる。従って PIA は、システム開発の早い段階で実施することが望ましい。

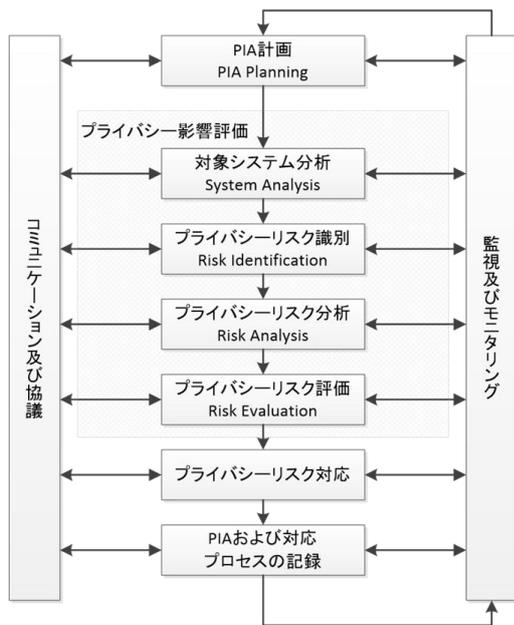


図 2 PIA 実施手順の概要

図3に示すようにシステムを構築運用する組織(以下PIA実施依頼組織)がPIA報告書を公表することで、個人情報の取り扱いに関してPIA実施依頼組織、個人、マスメディアの三者で議論する共通の土俵を提供することができる。組織が個人の権利保護に留意している姿勢を関係者に示すことにもなる。すなわち、PIAはプライバシーリスクに関するリスクコミュニケーション手段としても有効である。

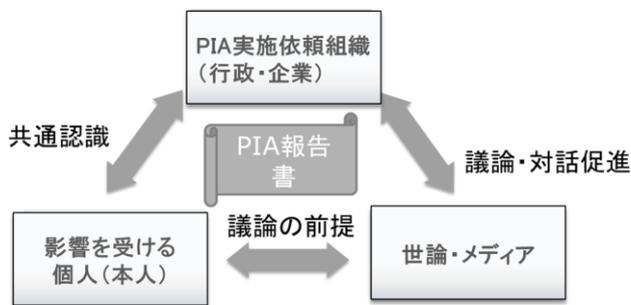


図 3 PIA 報告書とステークホルダー間のリスク共有

したがって、PIAの要点は以下の2点にある。

- システムに対し構築前に事前にプライバシー(個人情報漏洩)リスクの可視化・軽減を行う。
- PIAの評価結果は、意思決定者が利用だけでなく、データ提供主体者などのステークホルダーが意見を交換し、合意形成の手段を得るために実施する。

### 3. マルチステークホルダープロセスにおけるプライバシー影響評価の検討

PbDはプライバシー保護の基本的な考え方を示し、適正に実現しているかはPIAにより確認できる。マルチステー

クホルダーのプライバシー分野での適用事例がPIAといえる。本章では、PIAとマルチステークホルダープロセスの関係を明確にする。

#### 3.1 マルチステークホルダープロセス

マルチステークホルダープロセス(Multi-Stakeholder Process, MSP)とは、行政、企業、市民、有識者などの関係者が対等な立場で参画し、オープンなプロセスにより課題解決、ルール策定などを行う方法である[8]。

日本でも個人情報の活用推進により、行政や事業者は持続的に事業を運営するため、市民やメディアなどから信頼を得て進める必要がある。

図4に示すように、一部の関係者だけが前進しようとする他の利害関係者からの反対で引っ張り戻される。お互いの信頼関係を構築し、ステークホルダー全体で前進することが必要であり、相互利益の尊重と信頼関係の構築がMSPの重要なポイントである。

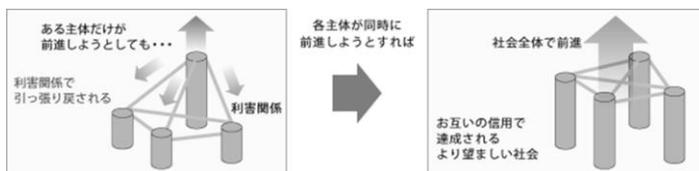


図 4 マルチステークホルダープロセスの考え方

内閣府が発表したMSPの報告書では以下のように記載されている[11]。

#### (1) 定義

MSPは、「平等代表制を有する3主体以上のステークホルダー間における、意思決定、合意形成、もしくはそれに準ずる意志疎通のプロセス。」と定義される。ステークホルダーの平等代表制とは、MSPにおけるあらゆるコミュニケーションにおいて、各ステークホルダーが対等な立場で参加し、自らの意見を平等に表明できることであり、また、相互に説明責任を負うことである。意思決定や合意形成は、政策決定から共通認識の形成、実践的な取組実施に向けての合意、ステークホルダー間のパートナーシップやネットワーク形成に至るまでを幅広く含むものである[11]。

#### (2) 背景

MSPは主に80年代後半から90年代にかけての“持続可能な発展”に関わる議論の中で登場した。1987年に開催された環境と開発に関する世界委員会(通称ブルントラント委員会)報告書「われら共通の未来(Our Common Future)」及び1992年の環境と開発に関する国連会議採択文書「アジェンダ21」では、持続可能な発展を達成するためには、様々なステークホルダー(MSP)が政策決定に関する情報へアクセスし、政策決定へ参加する制度を保障することが不可欠である旨が述べられている[12]。

MSPは環境問題への適用を最初に行ったが、現在では、

環境問題以外の事案にも活用され、情報共有やルール策定、利害調整が行われている [13].

### (3) 手順

図 5 に MSP の手順を示す。

- ① 課題の抽出：課題を抽出し、MSP の実施を判断する。
- ② 準備：リスクの抽出と評価指標の作成。専門家の意見の取り込みなどを行う。
- ③ ステークホルダーの招集：本事案に関係するステークホルダーの招集。市民やメディア、NPO の参加。
- ④ 合意形成：ステークホルダー全員が同じ情報を共有し、対等な立場で対話し、合意形成する。

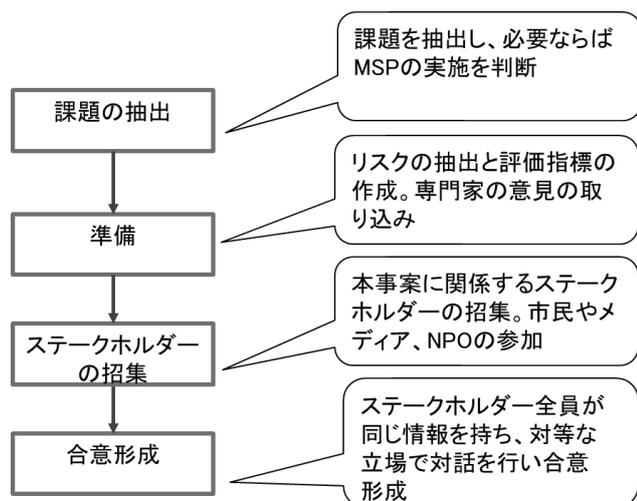


図 5 MSP 手順

### 3.2 PIA と PbD と MSP の関係

図 2 に示したように、ISO31000 をベースとした PIA の手順は、リスクマネジメントプロセスだけではなく、コミュニケーション・協議および監視・モニタリングが重要である。

個人情報を扱うシステムは利用する側と個人情報を提供する個人とで、利害関係が発生する。利害関係に関して、立場の異なるステークホルダーとの合意形成が重要である。

図 6 に示すように、リスクを可視化し合意形成するのが PIA である。合意形成には MSP のプロセスが有効である。また、PIA を実施する際、評価の基準は、PbD のプライバシーに関する 7 つの原則（具体的に利用するのは ISO/IEC29100 の 11 原則）を評価の大項目とする。

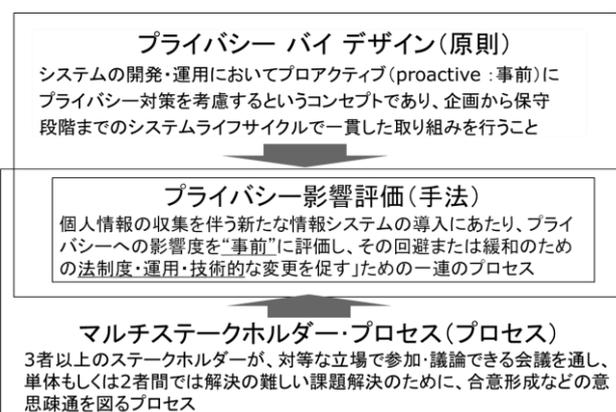


図 6 プライバシー影響評価と MSP と PbD の関係

#### (1) PbD 原則を利用した基準

図 7 に示す監視・モニタリングを行うためには、評価の基準が必要である。2.1 節で述べたように PbD の 7 つの原則が基準となる。現在は、国際標準規格 ISO/IEC29100 が発行されている。このため、評価項目として、表 1 に示す ISO/IEC29100 の 11 原則を利用する [3].

表 1 ISO/IEC29100 の 11 原則

1. 同意及び選択 (Consent and choice)
2. 目的の正当性及び明確化 (Purpose legitimacy and specification)
3. 収集制限 (Collection limitation)
4. データの最小化 (Data minimization)
5. 利用、保持、及び開示の制限 (Use, retention and disclosure limitation)
6. 正確性及び品質 (Accuracy and quality)
7. 公開性、透明性、及び通知 (Openness, transparency and notice)
8. 個人参加とアクセス (Individual participation and access)
9. 責任 (Accountability)
10. 情報セキュリティ (Information security)
11. プライバシーコンプライアンス (Privacy compliance)

#### (2) MSP を利用した合意形成プロセス

図 7 に示すステークホルダー間の協議・コミュニケーションには、図 5 で述べた MSP の手順を利用する。

利害関係が異なる立場のステークホルダー間のコミュニケーションのためには、適正な情報の提供が必要である。PIA 報告書を用いることによりステークホルダー間で情報を共有し、協議、合意形成を行うことができる。

例えば、一つの事例として大阪ステーションの監視カメラの実証実験で生じたように、カメラシステムを設置運用する側は、エリアの安全性確保を考えている。

一方、個人は必要以上にプライバシーを侵害されると受け取る [14].

設置すれば個人の安全性が確保できるにもかかわらず、プライバシーへの過剰な反応のため安全性を放棄するような行動になる。事前に PIA を実施し、適正な情報共有を行い協議する必要があったと考えられる。これは、双方にメリットがあるにも関わらず、適正なコミュニケーションが取れず、関係者の安全性確保とプライバシー侵害の明確な評価や合意形成ができなかった事例である。

### (3) PIA プロセスから見た PbD および MSP

図 7 に ISO31000 による PIA のプロセスから PbD および MSP の関係を示す。リスクマネジメントには監視・モニタリングとコミュニケーション・協議がプロセスを通して必要になってくる。監査及びモニタリングには、ISO/IEC29100 の 11 原則 (PbD のプライバシー7原則) を適用することにより客観性・透明性を持った評価ができる。また、コミュニケーション及び協議に関しては、MSP による利害関係の異なるステークホルダー同士が適正な情報を共有し、対等な立場で協議することにより合意形成が行われる。

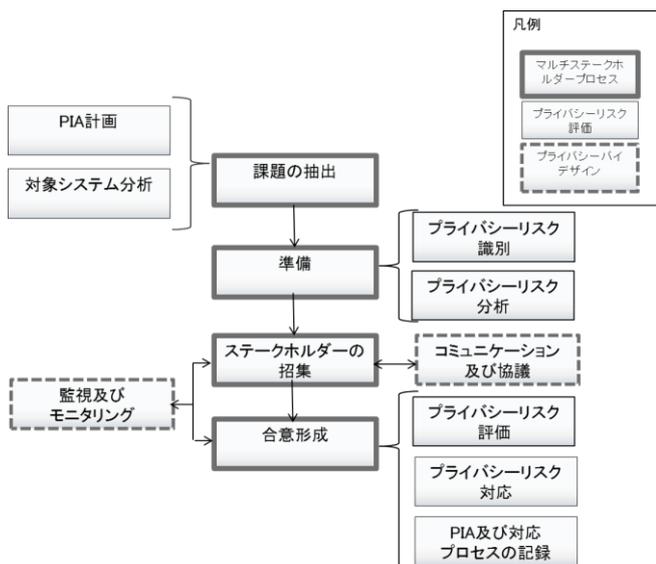


図 7 PIA と MSP と PbD の関係

## 4. おわりに

プライバシーバイデザイン PbD の原則およびマルチステークホルダープロセス MSP を分析し、プライバシー影響評価 PIA がどのような考え方をベースに構築され、プロセスが構成されているかを考察した。

PIA の評価基準に対する確認プロセス (監査・モニタリング) に対し、ISO/IEC29100 の 11 原則 (PbD の 7 原則) をベースにすることが有効であることが判明した。また、PIA のコミュニケーションプロセスは、PbD の可視化と透明性の具体化であり、そのプロセスは MSP の合意形成のプロセスと同様であることが判明した。つまり、PIA は、PbD

と MSP とをベースに成り立っている評価プロセスと言える。

個人情報を収集・保管・利用する行政機関や民間企業におけるシステムにおいて、すでに利用している MSP をベースとする PIA は採用が容易であり、今後、適正な社会コストで個人のプライバシー保護するために、PIA が広く必要されることを期待する。

## 参考文献

- [1] 個人情報保護委員会： 個人情報保護とは、  
<http://www.ppc.go.jp/personal/general/>.
- [2] 個人情報保護委員会： 特定個人情報保護評価、  
<http://www.ppc.go.jp/enforcement/assessment/>.
- [3] ISO/IEC29100: 2011,  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=45123](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123).
- [4] 瀬戸洋一： サイバーセキュリティとプライバシー問題 プライバシーバイデザインとプライバシー影響評価。電子情報通信学会総合大会, 2016年3月16日
- [5] 内閣官房： 特定個人情報保護評価、  
[http://www.cas.go.jp/jp/seisaku/bangoseido/kojin\\_joho/](http://www.cas.go.jp/jp/seisaku/bangoseido/kojin_joho/).
- [6] 瀬戸洋一： 実践的プライバシーリスク評価技法 実践的プライバシーリスク評価技法：プライバシーバイデザインと個人情報影響評価。近代科学社, 2014年
- [7] 個人情報保護委員会： <http://www.ppc.go.jp/>.
- [8] パーソナルデータ利活用に関するマルチステークホルダー・プロセスの実施方法等の調査事業、  
[http://www.meti.go.jp/committee/kenkyukai/shoujo/personal\\_data/pdf/report\\_01\\_01.pdf](http://www.meti.go.jp/committee/kenkyukai/shoujo/personal_data/pdf/report_01_01.pdf).
- [9] マルチステークホルダーの役割と設計、  
[http://innovation-nippon.jp/reports/2013StudyReport\\_MSHP.pdf](http://innovation-nippon.jp/reports/2013StudyReport_MSHP.pdf).
- [10] アン・カブキアン, 堀部/政男, JIPDEC 訳： プライバシー・バイ・デザイン, 日経 BP, 2012年
- [11] 内閣府. マルチステークホルダープロセスの定義と類型.  
<http://www5.cao.go.jp/npc/sustainability/concept/definition.html>.
- [12] 新時代のマルチステークホルダープロセスとソーシャルイノベーション,  
[http://www.murc.jp/english/think\\_tank/quarterly\\_journal/qj1003\\_07.pdf](http://www.murc.jp/english/think_tank/quarterly_journal/qj1003_07.pdf).
- [13] プライバシーに関わる標準化の動向,  
[https://www.nri.com/jp/event/mediaforum/2014/pdf/forum207\\_1.pdf](https://www.nri.com/jp/event/mediaforum/2014/pdf/forum207_1.pdf).
- [14] 映像センサー使用大規模実証実験検討委員会： 調査報告書 2014年 (平成 26年) 10月20日,  
<https://www.nict.go.jp/nrh/iinkai/report.pdf>.

URL は 2016 年 8 月 4 日に確認