プライバシー影響評価の健康診断総合システムへの適用

渡辺 慎太郎† 鶴田 亜由美† 前島 肇†
前田 武志† 瀬戸 洋一† 高橋 祐司‡

†産業技術大学院大学
〒140-0011 東京都品川区東大井 1-10-40
a1157sw@aiit.ac.jp

‡財団法人全日本労働福祉協会
〒143-0016 東京都大田区大森北 1-18-18

あらまし 医療情報システムが扱うデータは機微な個人情報であり，システム構築に際してプライバシーへの配慮が課題となり，リスクアセスメントが必要となる．プライバシー影響評価（以下PIA）は，個人情報提供者のプライバシーへの影響をシステム稼働前に事前に評価することにより，プライバシーリスクを低減させる手法である．今回，健康診断総合EHR（Electronic Health Record）システムのクラウド化にあたり，基本設計におけるPIAを実施した．これにより，事前にリスクを可視化し，ステークホルダー間で共有化するなどの有効性を確認できた．

Applied to the Electric Health Record System of Privacy Impact Assessment

Shintaro Watanabe† Ayumi Tsuruta† Hajime Maejima†
Takeshi Maeda† Yoichi Seto† Yuji Takahashi‡

†Advanced Institute of Industrial Technology
1-chome 10-40, Higashi-Ooi, Shinagawa-ku, Tokyo 140-0011, JAPAN
a1157sw@aiit.ac.jp

‡All Japan Labour Welfare Foundation
1-chome 18-18, Omori-kita, Ota-ku, Tokyo 143-0016, JAPAN

Abstract A Privacy Impact Assessment (PIA) is a systematic technique to review privacy risks of pre-launched systems, conducted to ensure personal information protection. In the project we performed a PIA on the primary design documents of an Electronic Health Record system. The system handles personal health records based on a cloud computing platform that may raise some security issues. We obtained the results such as an effective risk sharing between stakeholders.

1　はじめに

厚生労働省ガイドラインの 2010 年改訂によって民間のデータセンター事業者が医療機関保有データの外部保存を受託できるようになり，我が国でも医療情報システムにおいてクラウドコンピューティングの利用が可能となった[1].

総務省，厚生労働省，経済産業省が電子健康記録（EHR）・個人健康記録（PHR）システム構築の実証実験に取り組んでいる．EHR/PHR の導入は重複検査の回避を通じて個人や保険者に身体的負荷の軽減や医療費の削減をもたらし，医療機関には患者情報共有による安全性の向上をもたらすなど，その利点が確認されている[2].

一方で，プライバシーやセキュリティに関する懸念が指摘されている．特に医療情報システムでは個人の健康情報という極めて機微な情報を取り扱うため，懸念は通常の情報システムよりも大きい.

クラウドコンピューティングを推進するベンダーの中には，クラウドサービスによってデータを外部に保管する行為を企業が資金を銀行に預けることになぞらえて説明し，安全性を主張する企業もある[3].

しかし，個人情報は貨幣と異なり取り替えが利かない．また，一度漏洩した個人情報を取り戻すことは事実上不可能である．したがって，クラウドコンピューティング内で個人情報を扱う場合にも，プライバシー保護の対策が必要である.

海外では，個人情報の漏洩を未然に防止するための有効な手段として，プライバシー影響評価（Privacy Impact Assessment，以下 PIA）が注目されている[4]．PIA は，個人情報の収集を伴う情報システムの導入あるいは改修にあたり，プライバシーリスクを明確にし，プライバシー問題によるステークホルダーへの影響を事前に評価するリスク管理手法である[5].

カナダやオーストラリアの政府機関・州政府では，個人情報を取り扱う情報システムを構築する際に，プライバシーコミッショナー（Privacy Commissioner）の下，PIA を実施して個人情報の安全性を事前評価することが予算認可の条件となっている．米国では，個人情報を扱う行政システムの構築において，電子政府法第 208 条により PIA の実施が義務づけられている[6].

我が国においても，いわゆるマイナンバー法案の第 15 条において，行政機関等が特定個人情報保護評価を実施し，広く国民の意見を求めた上で評価書を作成し，個人番号情報保護委員会による承認を受けたのち報告書を公開するとされており，「特定個人情報保護評価」が PIA に相当する.

本発表では，財団法人全日本労働福祉協会が構築を進めている健康診断総合システムに対して実施した PIA に関して報告を行う.

2　プライバシー影響評価の概要

2.1　プライバシー影響評価とは

PIA とは，個人情報の収集を伴うシステムの導入や改修の際に，プライバシー問題を回避・低減するために，プライバシーへの影響を「事前」に評価するリスク管理手法である.

1990 年代，個人情報の電子化の進展に伴って情報システムのプライバシー問題が顕在化し，PIA が検討されはじめた．90 年第後半には，カナダ，ニュージーランド，オーストラリアが先行して導入している．また米国やカナダなど，PIA の遂行が行政機関における予算承認プロセスに組み込まれている国も存在する[7].

PIA を実施する目的は，コスト低減とステークホルダー間の信頼構築にある。

PIA では，実施結果を踏まえ，必要に応じて構築システムに対して仕様の変更を促す．システム稼働前に変更を行うことにより，稼働後のプライバシー問題発覚による稼動停止や，それに伴って発生するビジネス上のリスク，システム改修費用を軽減することができる[8].

また，実施組織が PIA 報告書を公表することで，プライバシーや個人情報の取り扱いに関し

て実施組織，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 は一種のリスクコミュニケーション手段である．

2.2 国際標準 ISO 22307

ISO 22307 Financial services - Privacy Impact Assessment は，国際標準化委員会 ISO TC68/SC7（金融サービス）により 2008 年 4 月に発行されたプライバシー影響評価に関する国際標準規格である[9]．プライバシー保護の目的では金融業界に限定していないため，他の業種にも適用することができる．

ISO 22307 は，①PIA 計画，②PIA 評価，③PIA 報告，④十分な専門知識，⑤独立性と公共性の程度，⑥対象システムの意思決定時の利用の 6 項目を PIA 実施における要求事項としている．このうち，前 3 者が PIA の実施手順に相当し，後 3 者が実施体制に相当する．以下に概要を示す．

①PIA 計画： 適用範囲の定義，実施者に必要な専門知識分野の特定，適用される法令や規格の特定，対象システムの調査を行い，実施計画書を作成する．

②PIA 評価： PIA 計画で定義した PIA の実施対象範囲について，プライバシーリスクを洗い出し，指摘事項とその指摘事項に対する推奨案を作成する．この作業は，プライバシーに関する専門知識を持ったメンバーが行う．

③PIA 報告： 対象システムについて関係者間でレビューを行うため，評価，分析した事項と必要であれば提案事項を文書化する．

④十分な専門知識： PIA 実施プロジェクトのメンバーに対して，法律分野，IT インフラストラクチャ，業務プロセスに関する十分な専門知識を要求する．

⑤独立性と公共性： PIA の実施者に対して，対象システムに関する利害関係者に対し独立性と公共性を保ち，中立性を確保するよう要求する．

⑥対象システムの意思決定： PIA 実施結果をリスク対策時の対象システムの意思決定時に利用するよう要求する[10]．

2.3 PIA ハンドブック，実施マニュアル

諸外国の公的機関が発行した PIA ハンドブックを比較・検討した上で，我が国において PIA を実施する上での課題として，

① 立的な立場で助言・勧告する組織の不在
② PIA の実施を義務づけ，体制を規定した法令の不在
③ マニュアルの未整備

の 3 点を掲げ，ISO 22307 に準拠しつつ我が国の社会制度の特性を考慮したハンドブックとマニュアルを既に開発した[11]．

ハンドブックは，ステークホルダーが PIA の目的と実施の範囲および効果を事前に理解し，円滑に PIA を実施するために利用する，PIA の意義と方法論とを記述した解説書である．

一方，マニュアルは PIA の実施者が参照するものであり，プロジェクトの立ち上げから終結までの実施手順について記載されている．標準化された手続きに則ることにより，実施者の能力によって評価結果に偏りを発生させないことを目的とする．

3 健康情報とプライバシーリスク

3.1 個人健康情報のプライバシー

個人情報保護法では，データベース化されている個人情報に対して適正な安全管理措置を求めているが，個人情報の重要度や機微性に関する規定は行われていない．一方，「個人情報保護マネジメントシステム－要求事項（JIS Q 15001：2006）」では，思想，信条，宗教，人種，民族，本籍地，身体・精神障害，犯罪歴などを機微な個人情報と定義している．

経済的損失レベル(y)				
	3	口座番号＆暗証番号. クレジットカード番号＆カード有効期限. 銀行のアカウント＆パスワード	遺言書	前科前歴. 犯罪歴. ブラックリスト
	2	パスポート情報. 購入記録. ISP のアカウント＆パスワード. 口座番号のみ. 銀行のアカウントのみ	年収・年収区分. 資産. 建物. 土地. 残高. 借金. 所得. 借入記録	
	1	氏名. 住所. 生年月日. 性別. 金融機関名. 住民票コード. メールアドレス. 健康保険証番号. 年金証書番号. 免許証番号. 社員番号. 会員番号. 電話番号. ハンドル名. 健康保険証情報. 年金証書情報. 介護保険証情報. 会社名. 学校名. 役職. 職業. 職種. 身長. 体重. 血液型. 身体特性. 写真(肖像). 音声. 声紋. 体力診断. ISP のアカウントのみ.	健康診断. 心理テスト. 性格判断. 妊娠経験. 手術歴. 看護記録. 検査記録. 身体障害者手帳. DNA. 病歴. 治療法. 指紋. レセプト. スリーサイズ. 人種. 地方なまり. 国籍. 趣味. 特技. 嗜好. 民族. 日記. 賞罰. 職歴. 学歴. 成績. 試験得点. メール内容. 位置情報	加盟政党. 政治的見解. 加盟労働組合. 信条. 思想. 宗教. 信仰. 本籍. 病状. カルテ. 認知症. 身体障害. 知的障害. 精神的障害. 保有感染症. 性癖. 性生活
		1	2	3
				精神的苦痛レベル(x)

図 1 シンプル EP 図

個人情報の機微性については，NPO 日本ネットワークセキュリティ協会のシンプル EP (Economic-Privacy)図が指針になる[12].

図 1 に示すように，同図は情報の機微性を経済的損失と精神的苦痛との 2 つの軸から分類している. 個人の健康情報については，漏洩時における精神的苦痛レベルが 2～3 と高く評価されており，厳重な取り扱いが求められる.

また，業務によって固有な機微情報の定義が行われている場合がある. たとえば健康診断業務について，厚生労働省労働基準局長通達(平成 16 年 10 月 29 日)は一部の感染症や遺伝情報を事業者が労働者から取得すべきでない情報としている。

3.2 個人健康情報と情報セキュリティ

個人の健康情報では，情報セキュリティにおける機密性の優先度が相対的に低下することがある. たとえば救急医療のように，人の生命に関わる場合である. 個人情報保護法においても，生命，身体，財産の保護のために必要があり本人の同意を得ることが困難な場合には，本人の同意なく個人情報を第三者へ提供することが認められている.

医療情報システムにおいても，個人健康情報については機密性と同等以上に完全性や可用性が重要な要素となる場合がある. 住所や氏名が一部正確さを欠いても本人の生命が危険に冒されることは考えにくいが，誤った医療データに基づく診療は医療事故に直結するからである.

可用性については，事業継続と密接に関わる問題である. 一般の事業者であれば休業を余儀なくされるような大災害が発生した際にも，医療機関の事業継続は必須である[13].

以上のように，健康情報のプライバシーリスクは，個人情報の漏洩だけでなく，毀損や滅失も含まれる.

4 プライバシー影響評価の適用

4.1 健診総合システムの概要

全日本労働福祉協会が構築を進めている健康診断システムに対して PIA を実施した.

本協会は，巡回健診や施設健診などの健康

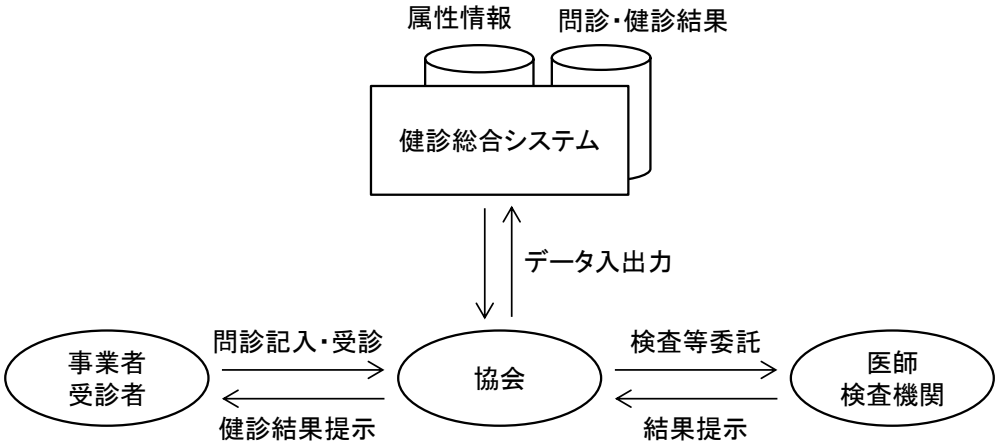

図 2　個人情報のフロー概略図

診断を中核的な事業とする団体であり，事業者・受診者へのサービス向上などを目的として，全拠点のコード・マスターの統一とデータベースの一元管理を基本方針とした健診総合システムの構築を，システム保有コスト圧縮のためクラウドコンピューティング上に行うことを決定した.

図 2 に，業務における個人情報フローの一部を示す．受診者は受診時，予め氏名などが印字された問診票に心身の状況や既往歴などを記入し，健康診断を受診する．協会は，検査の一部を医師や検査機関に委託する．収集したデータをシステムに入力し，判定結果を出力して受診者に返却する.

健診総合システムで取り扱う受診者の個人情報は，氏名・性別・生年月日・所属組織などの属性情報と，問診票への記載内容や測定データ，検査データ，判定データを含む問診・健診結果情報とに大別される.

健診総合システムが取り扱う個人情報の中には機微なものも含まれるため，クラウドコンピューティング基盤への移行にあたってはプライバシーリスクを評価する必要がある．基本設計段階において PIA を実施することで，事前にプライバシーリスクを可視化しリスクの回避・低減を図った.

4.2　プライバシー影響評価の実施

まず，ハンドブックを利用し，PIA の目的や手順，工程を共有化するため，PIA 実施者と依頼者（協会職員など）でプロジェクトキックオフミーティングを実施した.

PIA の具体的な実施は，マニュアルを利用した.

予備評価では，個人情報の取り扱いの有無や規模を確認し，PIA 実施の要否を判定する．健診総合システムで取り扱う個人情報（属性情報ならびに健診結果情報）とその規模（年間約 80 万件）から，クラウド環境下で適切に構築運用されない場合，個人情報が漏洩するリスクが想定される．従って，同システムに対して，PIA を実施し事前にプライバシーリスクの評価を行うことが必要であると判定した.

PIA の実施には，「簡易 PIA」と「詳細 PIA」とがある．両者の違いは，評価基準を個別に策定するか否かにある．簡易 PIA では評価基準に所定のものを使用し，チェックリストの形式でテンプレート化された評価シートに基づいて評価作業を行う．一方，詳細 PIA では，対象システムのリスク分析から評価基準を策定した上で，評価を実施する.

いずれを採用するかは，費用，個人情報保護の重要性，公共性，開発段階などを考慮し，PIA 依頼者と実施者とで相談のうえ決定する.

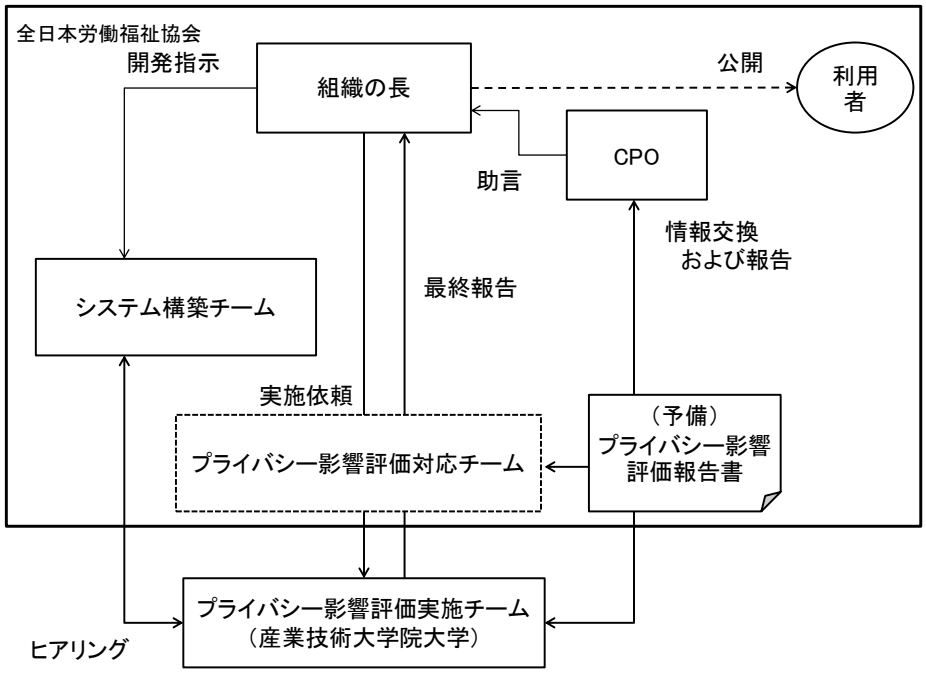

図 3 PIA 実施体制図

今回は詳細 PIA を採用した.

PIA の実施においては，依頼者が公的機関か民間機関かで評価の位置づけが異なる. 公的機関の場合は，システム構築における予算執行許可などに関係する保証型評価となり，監査的な位置づけになる. 一方民間機関の場合は，プライバシーリスクを低減するコンサルティングを行う助言型評価となる.

全日本労働福祉協会は，主たる業務である健康診断事業が高い公共性を有しているが民間機関であるため，助言型評価を基本とした PIA を実施した.

本プロジェクトの体制を図 3 に示す.

以下，PIA の作業を具体的に述べる.

⑴ 予備評価

協会より提供された基本設計書をもとに必要に応じて聞き取りを行い，健診総合システムの概要，保有する個人情報の種別，ならびに情報のフローを調査し，PIA 実施の要否を判定した. また，詳細 PIA の実施を決定するとともに作業工数の見積もりを行った.

⑵ PIA 実施計画の作成

PIA の適用範囲，作業期間の見積もり，必要な専門知識の特定及び，健診総合システムに適用される法令やガイドラインの調査，また，実施体制の決定，PIA 実施者の編成を行った. この結果を PIA 実施計画書として作成した.

⑶ システム分析，個人情報フロー分析

基本設計書に加えて業務フローの提供を協会より受け，対象システムのハードウェアおよびネットワーク要件を確認するとともに，業務における個人情報の取得・利用・保管・廃棄までの個人情報フロー分析を実施した.

⑷ リスク分析

PIA の評価基準を策定するために，リスク分析を実施した. 情報資産の資産価値を数値化し，その資産価値と脆弱性，脅威をもとにリスクの程度を数値化することでリスクを可視化した.

⑸ 評価基準の策定

協会の事業内容，個人情報の保有件数，対象システムの目的，機能，クラウドコンピューティングに関連するリスク，上記のリスク分析結果を考慮の上，遵守すべき法律・ガイドラインをもとに，評価基準を策定した. それぞれの評価基準は，質問項目という形で評価シートにまとめ

られる.

質問項目は OECD のプライバシー8 原則の分類に合わせ，計 37 の項目で構成した. 評価シートの作成に使用した法律，ガイドライン等は，以下のとおりである.

- 個人情報の保護に関する法律（平成十五年五月三十日 法律第五十七号）
- プライバシー保護と個人データの国際流通についてのガイドライン 経済協力開発機構
- 医療情報システムの安全管理に関するガイドライン（第 4.1 版） 厚生労働省
- クラウドサービス利用のための情報セキュリティガイドライン 経済産業省

⑹ PIA 評価実施

評価シートの各質問項目について，基本設計書に照らして評価を行い，適合・不適合・評価不能（評価時点では未確定のものなど）を判定した. 基本設計書からでは確認できない部分に関しては，聞き取り調査や実地調査によって補った.

評価結果のうち，不適合の項目に対しては指摘事項を記載し，改善すべきものとしている. 適合・評価不能の項目に対しては，その一部について推奨事項を記載し，プライバシー保護の観点から実施が望ましい施策を記載している.

⑺ 報告書の作成とレビュー

評価結果をまとめ，PIA 報告書として発行し，CPO に提出した.

PIA 報告会を実施し，評価結果を説明すると同時に改善案を提示した.

4.3 評価結果

評価結果を，マニュアルに準じて以下のような項目で表現した.

⑴指摘事項

3 つの区分で指摘した.

- 開示すべき重要な不備： 個人情報漏洩に直接関与する事象であり，発生する可能性が高い
- 不備： 個人情報漏洩に直接関与する事象であるが，発生する可能性が低い
- 軽微な不備： 個人情報漏洩に直接関与しない事象

⑵推奨事項

基本設計段階の評価では該当しないものの以降の段階で顕在化しうる問題に対して，事前に助言可能な項目を推奨事項として明示した.

4.4 PIA フレームワークの有効性評価

PIA 実施フレームワークに関し，下記の効果を確認した.

⑴ PIA ハンドブックおよび実施マニュアル

ハンドブックを用いることで，PIA の依頼者である全日本労働福祉協会が PIA の効果や手順に関し理解することにより，実施体制を整備，及び必要な情報の公開などの協力関係を構築でき，PIA を円滑に進めることができた.

実施マニュアルは，適用範囲を民間分野におけるクラウドマイグレーションと規定している. 今回対象としたシステムは個人健康情報を取り扱う公共性の高い分野ではあったが，マニュアルに従うことで PIA を支障なく進めることが可能であった.

検討すべき事項としては下記がある. 指摘事項における重要度の区分について，現行では情報セキュリティの 3 要素（機密性・完全性・可用性）のうち機密性（個人情報の漏洩）のみを基準としている. しかし，第 3 節のとおり完全性や可用性の欠如（個人情報の毀損や滅失）が事業に重大な影響を与えるシステムも存在するため，これらを基準に含めることを考慮すべきである.

⑵ PIA 実施の効果

基本設計段階におけるデータの収集から破棄までに至る処理に関して，プライバシーリスクの可視化が行なえた.

協会は，プライバシーリスクを網羅的に可視化することで，対策コストや後続段階への反映事項の明確化などを事前に把握することができた. PIA での指摘事項の半数以上は，本稿執筆時点で既に改善されている. また，共有化し

たリスクを元に，運用段階での管理策を議論・検討することができた.

クラウドコンピューティングのマイグレーションは協会にとっても初めての事例であり，本 PIA は今後のシステム導入においても参考にできるものである.

5　まとめ

国際標準 ISO 22307 に準拠した PIA ハンドブックならびに実施マニュアルに従い，全日本労働福祉協会がクラウドコンピューティング基盤に構築する健診総合システムの基本設計書に対して詳細 PIA を実施し，評価を行った. その結果，プライバシーリスクを可視化し共有することにより，効率的にプライバシー保護対策の提言を行うことができた.

また，実施においてハンドブックやマニュアルの利用が有効であることを確認した.

謝辞:

今回の PIA 実施にあたり，株式会社メディック総研の高坂定氏には，健診システムや医療関係のコンプライアンス上の留意点など助言をいただいた.

参考文献

[1] 厚生労働省:医療情報システムの安全管理に関するガイドライン　第 4.1 版, 2010.2

[2] 総務省:平成 24 年版情報通信白書, 2012.7

[3] Cade Metz:Google: 'We're Like a Bank for Your Data', Wired, 2012.5 http://www.wired.com/wiredenterprise/2201/05/google-apps-iso/

[4] David Wright, Paul De Hert: Privacy Impact Assessment, Second Edition, Springer Verlag, 2012.8

[5] 瀬戸洋一ほか:プライバシー影響評価 PIA と個人情報保護，中央経済社, 2010.3

[6] 星野あい，瀬戸洋一ほか:グループウェアシステムのクラウド化基本設計に対するプライバシー影響評価　実施とその効果 SCIS2011, 2011.1

[7] 瀬戸洋一:プライバシー影響評価のアセスメント手法に関する調査研究，産学戦略的研究フォーラム, 2007

[8] 石田茂，瀬戸洋一ほか:日本におけるプライバシー影響評価の実施に関する提案, ISEC, 2011.11

[9] ISO22307 Financial services—Privacy impact assessment, 2008.5

[10] 高坂定，石田茂，横山完，瀬戸洋一:プライバシー影響評価実施における社会制度の相違を考慮したハンドブックの開発, SCIS2012, 2012.1

[11] 石田茂，高坂定，横山完，瀬戸洋一:日本におけるプライバシー影響評価の実施に関する提案，信学技報, 2011.11

[12] NPO 日本ネットワークセキュリティ協会: 2010 年度情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～, 2011.7

[13] 財団法人日本情報処理開発協会:医療機関向け ISMS ユーザーズガイドーJIS Q 27001:2006（ISO/IEC 27001:2005）対応ー, 2008.5

註）過去の PIA 報告書やハンドブック，実施マニュアルについては，次の URL からダウンロードすることができる.

http://aiit.ac.jp/master_program/isa/professor/y_seto.html