一般
投稿論文

個人情報影響評価の有効性評価

坂本 誠[†1]　岡崎 吾哉[†1]　岡本 直子[†1]　川口 晴之[†1]　永野 学[†1]　瀬戸 洋一[†1]

[†1] 産業技術大学院大学

個人情報影響評価（PIA：Personal information Impact Assessment）は，個人情報の収集を伴う情報システムの導入，改修の際に，個人情報漏洩問題の回避あるいは低減を目的として個人情報に関するリスクを「事前」に評価するリスク管理手法である．海外では PIA の実施例は多いが，その有効性を客観的に評価した事例はない．日本で普及させるには，有効性の検証が必要である．評価対象システムの個人情報に関するリスクを構築前に可視化することができるか，システムを適正に構築運用するために PIA 実施依頼組織の個人情報保護意識を向上させることができるかという観点から PIA の評価を行った．個人情報保護意識が約 10% 改善するなど，有効性があるという結果を得た．

1. はじめに

情報化社会において，個人情報は電子化され，消費者が個人の興味・嗜好にあったサービスを享受することができるなどの利便性をもたらす一方，公共機関や企業などに個人情報が大量に蓄積されるようになった．一度漏洩した個人情報を完全に回収することは困難である．したがって，個人情報を扱う情報システムでは，個人情報漏洩の発生を未然に防止することが重要である．個人情報に関する事故の発生を防止するための対策として，たとえば暗号化等の技術的な対策，ISMS（JIS Q 27001:2006），プライバシーマーク（JIS Q 15001:2006）などの運用上の対策があるが，仮に不適切な情報システムが構築された場合，システムの不備を補うための運用コストやシステムを事後的に改修するためのコストなど，追加コストが必要となる．そのため，不適切なシステムが構築されることを事前に防止するための手段として，情報システムの企画，設計段階における対策状況を評価する手法である，個人情報影響評価（PIA：Personal information Impact Assessment，以下 PIA）が注目されている [1].

PIA は個人に関する情報を広く保護の対象とする．ISO 22307 では「プライバシー影響評価（Privacy Impact Assessment）」として表記されるが，「プライバシー」という表記は対象とする情報を限定し得る．本稿では PIA を「個人情報影響評価（Personal information Impact Assessment）」と表記する [2].

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，個人情報に関するリスクを明確にし，ステークホルダへの影響を「事前」に評価し，回避または緩和のための技術的な変更，運用・法制度の整備を促すリスク管理手法である．

PIA を実施することにより，漏洩などの個人情報に関する事故の抑制と対策コストの低減，個人情報保護に関するステークホルダ間の合意形成を行うことができる．

PIA は一部の国で普及しているが，日本では民間利用も含めた PIA 実施に関する根拠法は整備されておらず，一部の試行を除き国内での実施例は少ない [1].「行政手続における特定の個人を識別するための番号の利用等に関する法律」第 15 条において，PIA に相当する「特定個人情報保護評価」が定められているが，同法で規定する「個人付与の番号に関する特定個人情報」の保護が対象であり，現時点で PIA に関する包括的な法的根拠は存在しない [3]．日本において PIA を普及させることが課題であるが，PIA の有効性を明らかにすることはその一助となることが期待される．

PIA の有効性に関し，バイオメトリクスに関する PIA の有効性評価の例があるが，従来の PIA の有効性評価はそれぞれの個別事例における PIA 実施の手順等に関する有効性を評価したものであり，PIA 自身の有効性の評価は報告されていない [4].

PIA 自身の有効性は，PIA 実施の目的から，対象となる情報システムに関するリスクの可視化，リスクに関するステークホルダ間の合意形成の観点から評価することができる．

今回，PIA 自身の有効性を評価するために，個人情報保護に関する組織の成熟度を計測するツールである，米国公認会計士協会・カナダ勅許会計士協会（以下 AICPA/CICA）の Privacy Risk Assessment Tool を参考に有効性評価ツールを開発し，PIA の有効性評価を実施した [5].

本稿では，PIA の有効性に関し，①個人情報に関するリスクの可視化，②個人情報保護に関するステークホル

ダの意識向上の観点から，企画，設計段階にあるシステムに対するPIA実施に際して行った評価について述べる．

本稿は，以下，第2章で個人情報影響評価の概要，第3章で個人情報影響評価の有効性評価の課題，第4章で個人情報影響評価の有効性評価の概要，第5章で実際の有効性評価の測定方法について述べる．

2. 個人情報影響評価

2.1 個人情報影響評価の概要

「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，個人情報に関するリスクを明確にし，個人情報に関する問題によるステークホルダへの影響を「事前」に評価する．個人情報に関する影響を評価するだけでなく，回避または緩和のための技術的な変更，運用・法制度の整備を促すことを目的とするリスク管理手法」である[1].

PIAを実施する目的は，情報システムの個人情報に関する問題を明確にし，効果的な事前対策を実施することによる個人情報に関する事故の抑制，対策コストの低減とステークホルダ間の合意形成にある．

PIAを実施した結果，必要に応じて構築システムに対して仕様の変更を促す．システム稼働前に仕様変更を行うことにより，稼働後の個人情報に関する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損害，システム改修コストを軽減することができる．

また，PIAでは，システム企画書・システム設計書と実際に検出されたリスクとのギャップ，法令・ガイドライン・社内規程・運用規則などの要求事項と実際に検出されたリスクとのギャップを双方向に分析する（図1）．リスク対策計画を評価した結果，検出リスクに対応するリスク対策が計画されていないことが判明した場合，リスク対策の漏れであり，システム企画書・システム設計書などの修正の要求を通じてリスク対策計画の改善を支援する．また，検出リスクに対応する法令・ガイドライン・社内規程・運用規則などの要求事項の完備性を評価する．要求事項におけるリスクの検討漏れを指摘することで，社内規程・運用規則，法令，ガイドラインなどの整備を促す[6].

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，プライバシーや個人情報の取り扱いに関してPIA実施依頼組織，個人情報の提供者である個人，マスメディアの三者で議論するための共通の認識を有することができる．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は個人情報に関するリスク評価およびコミュニケーション手段である．

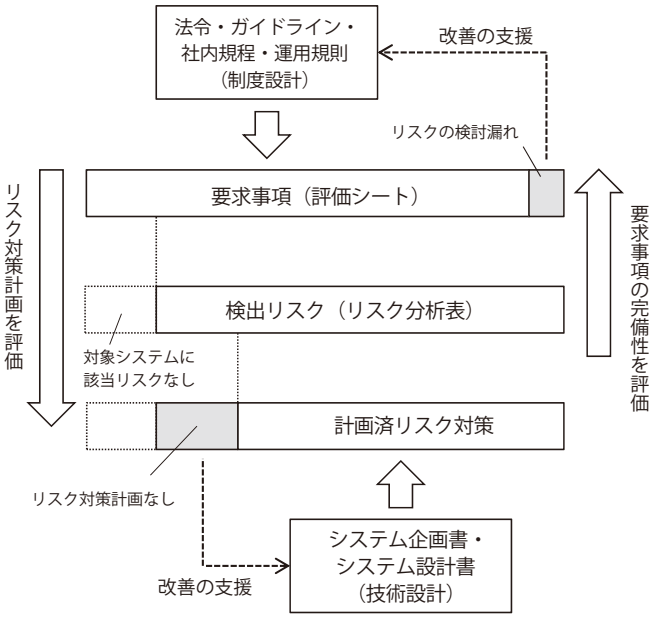


図1 双方向ギャップ分析

ISO 22307 Financial services-Privacy Impact Assessmentは，国際標準化委員会ISO TC 68/SC 7（金融サービス）により2008年4月に発行された個人情報影響評価に関する国際標準規格である[7].

ISO 22307は，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，他の業種にも適用可能である．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．

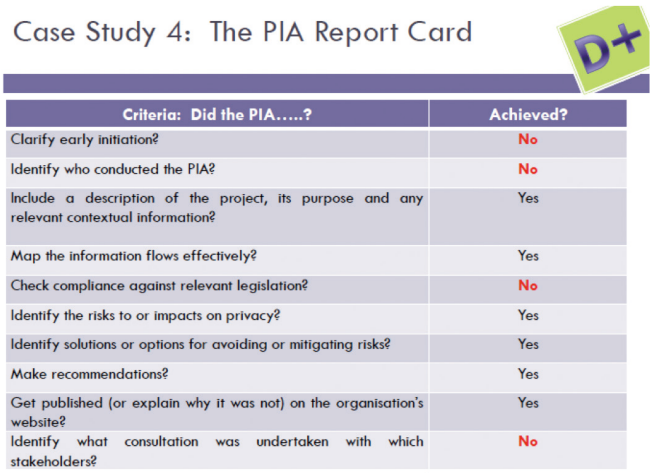
3. 個人情報影響評価有効性評価の課題

PIAの有効性評価の参考となる例として，以下に示す2つの事例がある．

① 個々のPIAの事例に関する有効性評価

PIAの事例に対して，実施手順，結果の有効性を評価している．PIAの責任者が明確であったか，個人情報に対するリスク・影響を特定することができたかなどの評価項目に照らし合わせて，当該PIAの実施手順の有効性評価をA～Dなどのランク付けで行っている．

図2に評価の例を示す[4]．Google社のストリートビューに関するPIAに対する評価例である．個人情報のフローを効果的に特定できたか否か，コンプライアンスのチェックを実施，およびPIAの結果が公開されたか否か



Criteria: Did the PIA.....?	Achieved?
Clarify early initiation?	No
Identify who conducted the PIA?	No
Include a description of the project, its purpose and any relevant contextual information?	Yes
Map the information flows effectively?	Yes
Check compliance against relevant legislation?	No
Identify the risks to or impacts on privacy?	Yes
Identify solutions or options for avoiding or mitigating risks?	Yes
Make recommendations?	Yes
Get published (or explain why it was not) on the organisation's website?	Yes
Identify what consultation was undertaken with which stakeholders?	No

図 2　PIA の手法の有効性評価結果の例 [4)]

などを評価しているが，PIA は有効であるという前提で個別の PIA 事例に対し手順の十分性を評価したものであり，PIA 自身の有効性については言及していない．

② ISMS の有効性評価

JIS Q 27001:2006 の規格項番 4.2.3 b では，当該組織において定期的に ISMS の有効性測定についてレビューをすることを要求している．この場合の有効性とは，管理策の有効性だけでなく，当該組織における ISMS 基本方針と管理目的の達成の度合いを含むが，JIS Q 27001:2006 に規定された内部統制の手法の有効性評価ではない[8],[9]．

①②ともに事例に対する手順の有効性を評価するものであり，PIA や ISMS 自身の有効性，すなわちそれぞれの目的に照らして手法自身が有効であるか否かを評価するものではない．

本稿では，PIA 自身の有効性評価として，PIA というリスク管理手法がその目的に照らして有効であるか否かという観点で評価する．

厳密に PIA 自身の有効性を評価するには，PIA を実施したケースと実施しないケースでシステムを構築し，PIA の目的であるプライバシー問題発生の回避可能性を測定する必要がある．しかし，まったく同一のシステムを複数の手段で構築することは現実的ではなく，この評価を実施することは困難である．そこで，PIA の目的に着目して，下記の 2 点を評価軸とした[10]．

① 個人情報に対するリスク（プライバシーリスク）の可視化

PIA を実施することで明らかになった，評価基準（評価シート）に対する適合・不適合の状況の評価．PIA の目的の 1 つに個人情報漏洩問題の回避または緩和のための影響評価がある．つまり，PIA を実施することで個人情報漏洩リスクを可視化することができたかを評価する．

② 個人情報保護意識の改善

PIA 実施依頼組織の個人情報保護意識の改善度合いの評価．PIA の目的の 1 つにリスクに関するステークホルダ間の合意形成がある．この目的達成に必要な PIA 実施依頼組織の個人情報保護意識を改善することができたかを評価する．

4. 有効性評価方法の提案

第 3 章で述べたように PIA 有効性評価のために，個人情報に対するリスクの可視化，ステークホルダ間の個人情報保護意識の改善の度合いを評価した．以下に詳述する．

4.1 個人情報漏洩リスク（プライバシーリスク）の可視化の測定

PIA を実施することにより，対象システムにおける個人情報のライフサイクルの局面ごとに個人情報に対するリスク分析を行うことができる．

PIA の実施にあたり，対象システムに関連する法令，規格，組織内規定などの要求事項を基に評価基準である評価シートを作成し，当該システムの法令等の要求事項に対する適合性を評価する．表 1 に健診総合システムにおける評価項目と指摘事項の例を示す[11]．

また，システムの対象とする業務における個人情報のデータフロー，システムの機能・構成・運用等の観点からリスク分析を行い，システムの不備を検出する．検出された不備と評価シートの差分は，法令・規格・組織内規定などの要求事項の不足を表す．PIA は対象システムにおけるリスクの識別分析のみならず，要求事項の不足を識別することができる．要求事項の不足の例として，医療機関向けに実施した PIA において，厚生労働省の医療情報システムの安全管理ガイドライン第 4.2 版では医療情報の暗号化を要求しているが，その暗号化の方式・強度などについては具体的な基準が定められていないことなどの指摘がある．

表 1　評価項目と指摘事項の例

評価項目	評価結果・指摘事項
評価対象システムにて，取得しようとする個人情報について，個人情報か否か特定する手続き，手順が定められているか．また，評価対象組織における個人情報の範囲について，定期的に現実と乖離が発生していないかを確認，改訂する手続き，手順が定められているか．	個人情報の特定に関しては，基本設計段階から明記されておくべきであり，それが基本設計書に含まれないのは問題である． 指摘事項：個人情報の定義や定義改訂の手続きや手順を定めること．

表1の例では，評価対象システムは，設計者の観点で個人情報保護の対策が考慮されていたが，コンプライアンスの観点で，個人情報の特定に関する手続き，手順の検討が不十分であるという不適合が見つかった．これはPIA実施依頼組織で見落されていたリスクである．

評価対象システムは，以下のとおり，病院など公共性の高い民間分野のシステムとした[6],[11],[12].

① Webベース監視サービス

自動車に搭載したカメラによって，映像情報を収集し，仮想空間を構築するシステム．個人の顔や生活風景も含まれる．

② バイオメトリック認証システム

指紋，顔，静脈等のバイオメトリック情報を使ったユーザ認証を必要とするアプリケーションに対し，バイオメトリック情報の管理・照合機能を提供するシステムである．

③ Webベース求人サイト

就職目的の学生の登録データおよび求人参加企業のデータを管理し，学生情報および企業情報の検索照合機能を提供することを目的としているWebサイトであり，クラウドコンピューティングを活用している．

④ クラウド対応健診総合システム

健診事業者における，健康診断にかかる受診者情報，健診結果情報，請求情報を一元的に管理するシステムであり，プライベートクラウド上に構築される．

⑤ 総合病院病院情報システム

350床規模の総合病院における電子カルテ，医事システムであり，既存システムの更新事案である．

4.2　個人情報保護意識の改善の測定

個人情報保護意識の改善を測定するために，PIA実施依頼組織に対し，PIA開始時および終了時に個人情報保護意識を測定した．

4.2.1　個人情報保護意識調査の検討

ステークホルダの個人情報保護意識を，以下に対する理解度について着目し測定した．

① 評価対象組織における個人情報保護に関する取り組みの重要度

② 評価対象組織における個人情報保護に関する取り組みの達成度

前者は個人情報保護に関する取り組みの重要度に対する認識を測ることで，意識を直接的に測定するものである．後者はこれまで知り得なかった評価対象組織の個人情報保護に関する取り組み状況を深く認識する，もしくは，組織の構成員の意識が改善した結果組織の個人情報保護に関する取り組みの達成度が改善するという点で，間接的に「意識」を測定するものである．

日本におけるPIAは各組織の任意の取り組みである．PIAの結果は公開されないことも考えられるため，ステークホルダはPIA実施依頼組織の役職員とした．

個人情報保護意識の調査の手法として，AICPA/CICAのPrivacy Risk Assessment Tool（以下PRA Tool）を参考に，日本におけるPIA有効性評価ツールを開発した[5]．PRA Toolは，AICPA/CICAが策定し米国およびカナダで利用されている「一般に公正妥当と認められたプライバシー原則」（Generally Accepted Privacy Principles，以下GAPP）に基づいたアンケート形式で自組織の個人情報保護に対する取り組みの成熟度を評価するツールである．

このツールは，GAPPの10原則に基づく73の評価項目を設定し，「Likelihood of a Control Failure（統制失敗の可能性）」「Business Impact（ビジネスへの影響）」「Effort/Cost to Mitigate（軽減に要する労力／コスト）」の3つの評価軸で評価する．評価の基準には，情報システムコントロール協会（ISACA）が策定したIT管理のベストプラクティスであるCOBIT Version 4.1で定義された成熟度モデルが使用され，表2に示すとおり，3段階の尺度が用いられている[5],[13].

今回評価で用いたPIAでは，個人情報保護法に加えOECD Guidelines（以下OECD8原則），業界ごとのガイドラインや評価対象組織の社内規程などを考慮して評価項目を決定する．GAPPの10原則，OECD8原則，個人情報保護法の枠組みは整合している．

以下に，提案方式を説明する．

4.2.2　PIA有効性評価ツールの提案

PRA Toolは個人情報保護に関する組織の成熟度を計測するものである．PRA Toolをステークホルダ個々人の意

表2　PRA Toolにおける評価尺度の例

スコア	特性
2＝低リスク	成熟度レベル5―最適化されている 成熟度レベル4―管理され計測可能 ・実効性のある内部統制とリスク管理環境が実施されている
5＝中リスク	成熟度レベル3―手続きが確立されている ・プライバシー管理が，実行され，十分に文書化されている
8＝高リスク	成熟度レベル2―反復可能だが直観に頼る 成熟度レベル1―初期的・場当たり的 成熟度レベル0―管理不在 ・プライバシー管理は行われているが，文書化されていない

識の計測に利用するためには，質問の分かりやすさ向上と評価軸の変更が必要である．そこで質問は，個人情報保護に関する専門知識がなくとも回答できるように平易な表現とした．また，回答者の職種や担当業務を制限しない質問項目とした．さらにシステムに対する評価を行うため，技術的な質問項目を追加した．

表3にPRA Toolの質問項目と作成した質問項目の対比例，**表4**に作成した質問項目の一覧を示す．質問に対する回答の選択肢は，**表5**に示す評価指針を用いた．意識を測る評価軸と尺度への対応は，**表6**に示す「重要度」「達成度」という2つの評価軸で5段階の尺度を用いた．リスクの軽減に要するコストに関しては，PIA実施依頼組織内で回答者が限定されることから，PRA Toolで用いられているコストに関する評価軸は採用しなかった．

「重要度」「達成度」の2つの評価軸はすべての質問項目に対して設定した．表5に回答者に提示した評価の指針を示す．

「重要度」に関して，各質問項目は，個人情報保護に寄与する取り組みを示している．重要度の認識が高まれば，個人情報保護意識が改善したものと考えることができる．

「達成度」は，PIAの過程で組織が個人情報保護の取り組みを強化したことにより値が改善した場合，ステークホルダ個々人の意識が改善した結果達成度が改善したと考えることができる．

PIA実施の結果，これまで認識の少なかった取り組み状況を深く認識したという場合，達成度が改善する場合，低下する場合のいずれも生じ得る．達成度の値に変化が生じたことにより個人情報保護意識が改善したものと考えることができる．

以上のように，さまざまな業務担当者に対して個人情報保護に関する意識の調査が可能なPIA有効性評価ツールを開発した．

5. 有効性評価の結果

5.1 評価の実施と結果

5.1.1 個人情報に対するリスクの可視化の測定

表3　PRA Toolと PIA 有効性評価ツールの質問項目対比例

PRA Tool	PIA 有効性評価ツール
Resources are provided by the entity to implement and support its privacy policies. （プライバシーポリシーを実施，支援するためのリソースは，事業体から提供されている）	プライバシーポリシーを遵守するにあたり，業務量が増加する場合は要員を補強する等，必要な要員が確保されていますか？

表4　PIA 有効性評価ツールの質問項目一覧

1. マネジメント	
問1	貴組織のプライバシーポリシー（個人情報の取り扱い方針について明文化されたもの）は以下の事項を定めていますか？ ・プライバシーポリシー公開の取り扱い ・個人情報提供・収集について本人の選択や同意 ・個人情報の収集，利用・保存・廃棄，アクセス，開示 ・個人情報にかかるセキュリティ，品質およびモニタリング・改善 プライバシーポリシーが定められていない場合1を選択してください．
問2	プライバシーポリシーとプライバシーポリシーが履行されない場合の影響についてすべての役員・職員に対して少なくとも年1回（プライバシーポリシーが変更された場合は，ただちに），周知していますか？
問3	プライバシーポリシーの制定，管理，更新を行う責任部署を定めて周知していますか？
問4	プライバシーポリシーと関連手続きの制定，変更について，マネジメント（経営層）の承認を得ていますか？
問5	プライバシーポリシーと関連手続きについて，関係法令・諸規制との適合性を最低年1回（関係法令・諸規制が変更された場合，その都度）確認していますか？
問6	個人情報の分類，センシティブな個人情報の該当有無，関連手続きとシステム，および関与する第三者を明確にしていますか？
問7	個人情報に関する新たなリスクの存在やリスクの変化を少なくとも年1回確認し，リスク対応策の見直しを行っていますか？
問8	役員・職員は，プライバシーポリシーと内部規程等との整合性を検証し，問題がある場合は修正をする機会を与えられていますか？
問9	個人情報にかかる手続き・仕組みが新たに制定されたり変更される場合，プライバシーポリシーに従い個人情報が保護されることを確認していますか？
問10	プライバシーにかかる事故，法令や内部規程違反等の管理手続きを制定し，適用していますか？
問11	プライバシーポリシーを遵守するにあたり，業務量が増加する場合は要員を補強する等，必要な要員が確保されていますか？
問12	個人情報管理担当職員は，その職務に就くために必要な専門的教育を受けていますか？
問13	プライバシーポリシーと関連する個人情報の取り扱いについて，社内教育プログラムや担当職員向け研修を行っていますか？
問14	事業分野ごとの個人情報保護に関する法令やガイドランなどの変更に応じて，プライバシーポリシーや内部規定を更新していますか？
2. 通知・公表	
問15	プライバシーポリシーの中で，次の項目について本人に対して通知・公表すると述べていますか？ ①目的，②選択・同意，③収集，④利用・保存・廃棄，⑤アクセス　⑥開示，⑦セキュリティ，⑧品質，⑨モニタリング・改善
問16	個人情報を本人ではなく第三者から収集する場合は，その情報源を明記していますか？
問17	個人情報の収集時やプライバシーポリシーの変更時，個人情報を他の目的で使用する前に，本人に対して通知や公表を行っていますか？
問18	プライバシーポリシーでは，対象となる組織と事業活動が明確になっていますか？
問19	プライバシーポリシーは，分かりやすく明確に書かれていますか？
3. 選択と同意	
問20	プライバシーポリシーでは，個人情報の提供・利用・開示に関して本人に選択権があること，かつ本人から同意を得る必要があることを述べていますか？
問21	法令に基づく例外を除き，個人情報の収集・利用・開示に関して本人に選択権があることを本人に伝えていますか？

問22	個人情報の提供や利用への同意を拒否したり取り下げた場合に本人にどのような影響がおよぶか, 本人に伝えていますか？
問23	個人情報の収集時に，本人の同意をとっていますか？　同意を取る際に本人が選択した内容は確実に履行されていますか？
問24	個人情報を当初の目的外で利用する際や利用目的を変更する場合に，本人の同意を得ていますか？
問25	法令で特に定められている場合を除き，センシティブな個人情報を収集・利用・開示する場合には，明示的な同意を本人から直接得ていますか？
問26	個人のコンピュータや電子機器を通じて個人情報を送受信する場合，事前に本人の同意を得ていますか？
4. 収集	
問27	プライバシーポリシーでは，個人情報の収集に関して述べていますか？
問28	個人情報の収集は公表した目的に限定して行われることを，本人に知らせていますか？
問29	収集する個人情報の形式や方法（クッキーなどのトラッキング技術を含む）を文書化し，通知していますか？
問30	収集する個人情報は，公表された目的において必要な範囲に限定していますか？
問31	個人情報を収集する手法が公正かつ適法であることを経営層は確認していますか？
問32	第三者から収集した個人情報が，公正で合法的な方法で収集した情報源であることを経営層は確認していますか？
問33	利用する個人情報に新規情報を追加する場合に，本人に知らせていますか？
5. 利用, 保存と廃棄	
問34	プライバシーポリシーでは，個人情報の利用，保存，廃棄について述べていますか？
問35	個人情報は同意を得た目的にのみ利用すること，目的の実現に必要な期間あるいは法令が要請する期限を超えて保存しないこと，廃棄にあたっては遺失・誤使用・不正アクセスを防止する方法を用いることを，本人に通知していますか？
問36	法令に基づく例外を除いて，個人情報は通知や公表内容で定めた目的にのみ使用し，その利用にあたって本人の同意を得ていますか？
問37	個人情報は，法令に基づく例外を除いて，定められた目的の実現に必要な期間を超えて保存しないようにしていますか？
問38	保存期間を超えた個人情報は，遺失・誤使用・不正アクセスが防げるような方法を用いて，匿名化または破棄，廃棄していますか？
6. アクセス	
問39	プライバシーポリシーでは，自身の個人情報にアクセスできる機会を提供すると述べていますか？
問40	自身の個人情報を確認，更新，訂正するための方法を，本人に知らせていますか？
問41	事業者が保有する個人情報に自身の記録が含まれるかどうか，本人は確かめられますか？
問42	個人情報へのアクセス請求を受けた場合，請求者の本人確認をしていますか？
問43	分かりやすい書式，妥当な期間，妥当な費用で，個人情報を本人に提供していますか？
問44	自身の個人情報へのアクセス要請を否認する場合，その理由や法的根拠とともに，異議申し立てを行う権利について，書面にて通知していますか？
問45	本人の要請に基づいて個人情報の更新，訂正を行っていますか？
問46	個人情報の修正要請を否認する場合，理由と不服申し立ての方法について，本人へ書面にて通知していますか？
7. 第三者提供	
問47	プライバシーポリシーでは，個人情報の第三者提供に関して述べていますか？
問48	法令に基づく例外を除き，個人情報の第三者への提供は通知・公表された目的に限定し，本人の同意を得た上で行われることを，本人に通知していますか？
問49	プライバシーポリシーや個人情報取扱に関する諸規程について，提供先の第三者に通知していますか？
問50	個人情報の取り扱いを第三者に委託する場合，プライバシーポリシーや関連する諸規定に従って，委託契約を交わしていますか？
問51	個人情報を新しい目的や目的外利用のために第三者に提供する場合には，事前に本人からの同意を得ていますか？
問52	第三者が個人情報を不正に利用した場合，是正措置が取れるようになっていますか？
8. プライバシーのセキュリティ	
問53	プライバシーポリシーにおいて情報セキュリティが述べられていますか？
問54	個人情報を保護するため予防策を講じられていることを本人に通知していますか？
問55	セキュリティ対策が策定され，承認され，実施されていますか？ （「セキュリティ対策」は, 遺失, 誤使用, 不正アクセス, 公開, 毀損，滅失から個人情報を保護するための，組織的・人的・技術的・物理的な安全措置を含みます）
問56	個人情報へアクセスする際，論理的アクセス制御がされていますか？（論理的アクセスとは本人認証などを言います）
問57	個人情報へアクセスする際，物理的アクセス制御がされていますか？（物理的アクセス制御とはサーバルームが施錠してあるなどを言います）
問58	自然災害や想定外事故によって，個人情報が漏洩することに対する予防策を講じていますか？
問59	個人情報を送付する場合，送付途中で情報の漏洩が起こらないように対策を取っていますか？（システム部門の方はネットワーク利用の場合など，情報の暗号化をしていますか？事務職の方は書類を送る場合など，目隠しシールなどを用いて透けて見えないようにしていますか？）
問60	可搬型メディア（USB メモリ, CD-ROM など）や機器（ノート PC など）に保存された個人情報について，不正アクセスから保護されていますか？
問61	個人情報の取り扱いについて, 管理上（取扱手順や対応など), 技術上（暗号化など），物理上（書類の送り方など）の安全性について, 少なくとも 1 年に 1 回は確認を行っていますか？
問62	システム開発やシステムテストにおいて個人情報の利用を禁じていますか？（ただし，当該情報が匿名化その他の手法で保護されている場合は除きます）
9. 品質	
問63	プライバシーポリシーに個人情報の品質について述べられていますか？（ここでいう品質とは，情報が正確であること，完全であること，利用目的にかなっていること，情報の収集方法や保管方法が適切であること等を言います）
問64	貴組織では，本人に対して正確な個人情報を提供してもらうように，掲示や書面を用いて依頼していますか？
問65	収集・保管されている個人情報は，その利用目的にかなう正確かつ必要十分な情報ですか？
問66	利用目的範囲外の個人情報を収集・保管していませんか？
10. モニタリングと改善	
問67	プライバシーポリシーに，プライバシーポリシーの改訂・改善のための手続きが明記されていますか？
問68	個人情報提供者から照会，クレーム，異議申し立てがあった場合，その対応窓口の所在や，連絡先を明記していますか？
問69	個人情報提供者からの照会，クレーム，異議申し立てに対応する手順が定められていますか？
問70	個々のクレームについて対処した結果を書面で当事者へ通知していますか？
問71	プライバシーポリシーおよび法令・内部規定，サービスレベル契約およびその他契約事項の遵守状況を検証し，結果を経営層へ書面で報告してしますか？
問72	プライバシーポリシーおよび関連手続きを遵守していない場合，適宜，是正措置を行っていますか？
問73	リスク評価に基づき，個人情報の管理についての監視を継続的に行い，適宜，是正措置を行っていますか？

表7は，過去に実施したPIAの事例である[6],[10],[11],[12]．評価シートの項目数，評価基準に対する不適合を表す指摘事項の数を示す．

5.1.2　個人情報保護意識の改善の測定

第4章に記載した健診総合システムのPIA事例に対して，提案したPIA有効性評価ツールを用い，PIA実施依頼組織の本部，支部を対象に，PIA開始時と終了時の2回，個人情報保護意識を調査した．調査対象者は9名である．同様に，病院情報システムに関するPIA事例に対して，PIA実施依頼組織の個人情報保護意識を調査した．調査対象者は6名である．

(1) 個人情報保護意識の改善

図3に検診総合システムおよび病院情報システムにおける「重要度」の測定結果を示す．各回答者の質問項目に対する評点の領域ごとの平均値を集計した．PIA実施の開始時と終了時を比較すると，健診総合システムのPIA，病院情報システムのPIAとも評価ツールの全領域について「重要度」の認識が高くなっている．改善幅は平均で10.4%である．

また，健診総合システムのPIAでは，評価対象組織は本部のほかに支部が存在した．表8はそれぞれの平均値の差である．PIA終了時の本部と支部の差が縮小していることより，PIAを実施することでPIA実施依頼組織内での意識の乖離が縮小したことも判明した．

PIAを実施することで，PIA実施依頼組織内での個人情報保護意識の改善効果が判明した．

(2) プライバシー対応の達成度向上

図4に検診総合システムおよび病院情報システムにおける「達成度」の測定結果を示す．各回答者の質問項目に対する評点の領域ごとの平均値を集計した．PIA実施

表5　回答者に提示した評価の指針

回答項目	評価の指針（評価の目安）
重要度	PIA実施依頼組織に対して 5：きわめて重要 4：重要度が高い 3：重要度が中 2：重要度が低い 1：まったく重要でない
達成度	PIA実施依頼組織における体制やプロセスに対して 5：自ら実践している．または，熟知しており他人を指導することができる 4：よく知っている 3：一応知っている 2：よく知らない 1：まったく知らない

表6　評価軸と尺度

回答項目	尺度		
	5～4	3	2～1
PIA実施依頼組織および事業に対する重要度	大	中	小
体制やプロセス確立の達成度	管理されている	ある程度実現できる	実現できない

表7　PIAの実施結果

システム	評価項目数	指摘事項数
Webベース監視サービス	29	22
バイオメトリック認証システム	36	25
Webベース求人サイト	43	6
クラウド対応健診総合システム	37	6
総合病院病院情報システム	41	1

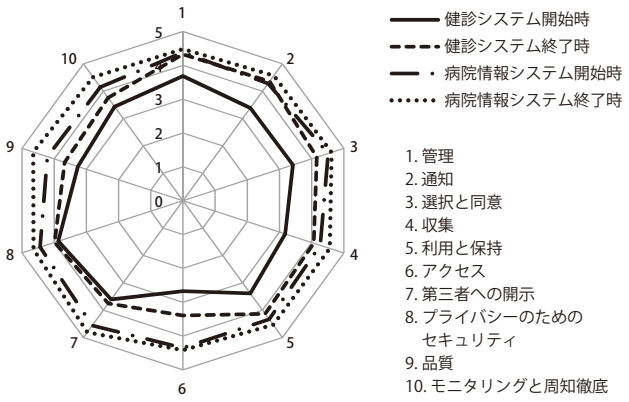


図3　重要度

表8　本部と支部の乖離幅（健診システム）

評価項目	達成度			重要度		
	4月	9月	比較	4月	9月	比較
1. 管理	0.51	0.42	0.09	0.14	0.28	−0.14
2. 通知	0.88	0.83	0.05	0.30	0.53	−0.23
3. 選択と同意	0.79	0.24	0.55	0.48	0.03	0.45
4. 収集	0.18	0.58	−0.40	0.09	0.09	0.00
5. 利用と保持	0.61	0.49	0.12	0.70	0.48	0.22
6. アクセス	0.92	0.73	0.19	0.45	0.22	0.23
7. 第三者への開示	0.24	0.28	−0.04	0.74	0.07	0.67
8. プライバシーのためのセキュリティ	0.17	0.04	0.13	0.08	0.39	−0.31
9. 品質	0.19	0.14	0.05	0.57	0.10	0.47
10. モニタリングと周知徹底	0.38	0.30	0.08	0.05	0.34	−0.29
総計	**0.49**	**0.27**	**0.22**	**0.24**	**0.08**	**0.16**

の開始時と終了時を比較すると，評価ツールの全領域について「達成度」の認識が高くなっている．改善幅の平均は20.3%であった．特に，重要度が高いと評価された項目（健診総合システムにおいては，1．管理，8．プライバシーのためのセキュリティ，病院情報システムにおいては7．第三者への開示，9．品質）についての改善幅が大きい．

5.2　考察

(1) 個人情報に対するリスクの可視化の測定

第1章で述べたとおり，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，個人情報に関するリスクを明確にし，ステークホルダへの影響を「事前」に評価し，回避または緩和のための技術的な変更，運用・法制度の整備を促すリスク管理手法である．

PIAを実施することによって，実施依頼組織において見落とされていたリスクを明らかにすることができれば，PIAの目的の一部を達成することができる．評価対象システムに関するリスクの可視化有無を測定することでPIAの有効性を確認することができる．

過去に実施したPIAの事例では，それぞれ指摘事項が検出されている（表7）．指摘事項数が最小1件から最大25件と差が大きい．それぞれの事例の評価対象システムの規模・種類，構築対象組織等はまちまちである．指摘事項数の差は，評価対象システムの規模・種類，評価対象組織におけるシステムの企画・設計能力の違いによって生じたものと考えることができる．リスクの可視化の観点ではPIAは有効であるといえる．

(2) 個人情報保護意識の改善の測定

第3章で述べたとおり，PIAの目的の1つにリスクに関するステークホルダ間の合意形成がある．合意形成のために必要なPIA実施依頼組織の個人情報保護意識を測定することでPIAの目的の一部の達成状況を測定することができる．

第4章で述べたとおり，提案したPIA有効性評価ツールによる評価はPIAの開始時と終了時に実施している．PIA実施に際しては，ヒアリング，中間報告などを実施し，PIA実施依頼組織の役職員に対してPIA実施依頼組織の個人情報保護に関する取り組み状況を明らかにしている．

前項で述べたとおり，「重要度」の値は平均で10.4%，「達成度」の値は平均で20.3%改善している．個人情報保護意識の観点でもPIAは有効であるということがいえる．

なお，本ツールにおける「達成度」の評価は，PIA開始前後で評価対象組織における個人情報保護に関する取り組みの達成度が改善した場合と，評価対象組織の達成度は変化せず，アンケート回答者の達成度に関する認識が変化した場合の区別をすることができない．

また，PIAの目的に照らし，個人情報に対するリスク（プライバシーリスク）の可視化と個人情報保護意識の改善の2点の評価軸を設定したが，評価軸が必要十分であるかの検証はできていない．今後改善が必要である．

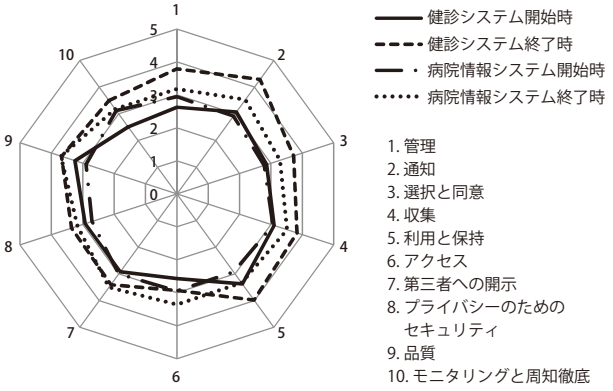


図4　達成度

6. おわりに

本稿では，PIAが，リスク評価の手段であることに着目し，個人情報に関するリスクの可視化とステークホルダの個人情報保護意識の改善の２つの観点から評価を行った．

その結果，個人情報に関するリスクの可視化については，PIAを実施することによりPIA実施依頼組織で見落とされていたリスクを明らかにすることができた．また，ステークホルダの個人情報保護意識の改善については，PIA実施の開始時と終了時で「重要度」「達成度」のいずれの評価軸においても個人情報保護意識が改善したとの結果を得た．以上よりPIAの実施効果を実証することができた．

謝辞　本研究は産業技術大学院大学のProject Based Learning（PBL）における教育研究活動で実施された．PBLのメンバである渡辺慎太郎，前島　肇，鶴田亜由美，高坂　定，各氏の協力を得た．ここに感謝の意を表します．

参考文献

1) 瀬戸洋一, 六川浩明, 新保史生, 村上康二郎, 伊瀬洋昭:プライバシー影響評価 PIA と個人情報保護，中央経済社 (2010).
2) 産業技術大学院大学：個人情報影響評価　事例集，http://aiit.ac.jp/master_program/isa/professor/y_seto.html（2014 年 4 月 28 日現在）
3) 高坂　定，石田　茂，横山　完，他：各国におけるプライバシー影響評価とハンドブックの整備に関する分析，日本セキュリティ・マネジメント学会誌，Vol.27, No.1, pp.17-26 (2013).
4) Wadhwa, K. : SAPIENT Project : Supporting Fundamental Rights, Privacy and Ethics in Smart Surveillance Technologies, Biometrics 2011 (2011).
5) 米国公認会計士協会・カナダ勅許会計士協会：AICPA/CICA Privacy Assessment Tool, http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/gen-accepted-privacy-principles/item10727.zip (2014 年 4 月 28 日現在)
6) 前島　肇，瀬戸洋一，他：プライバシー影響評価におけるリスクアセスメントの検討，情報処理学会第 75 回全国大会講演論文集, Vol.2013, No.1, pp.603-605 (2013).
7) ISO 22307 Financial Services – Privacy Impact Assessment (2008).
8) 日本工業規格 JIS Q 27001：2006 ―情報セキュリティマネジメントシステム―要求事項 (2006).
9) 羽生田和正，他：情報セキュリティのためのリスク分析・評価，日科技連 (2008).
10) 鶴田亜由美，瀬戸洋一，他 : プライバシー影響評価の有効性評価に関する一考察，SCIS2013 (2013).
11) 渡辺慎太郎，瀬戸洋一，他：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，情報処理学会コンピュータセキュリティシンポジウム 2012 論文集，Vol2012, No.3, pp331-338 (2012).
12) 岡本直子，瀬戸洋一，他：An Implementation Status of Personal information Impact Assessment in Japan, The 41st Conference of the KIPS (Korea Information Processing Society), Vol.20, No.2, (2013).
13) 情報システムコントロール協会：COBIT Version 4.1 (2007).
14) 特定個人情報保護委員会：特定個人情報保護評価指針 (2014).
15) 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).
16) 石田　茂，瀬戸洋一，他：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).
17) 韓国インターネット振興院 著，岡本直子，他（翻訳）：個人情報影響評価実施ガイド個人情報影響評価実施事例集，http://aiit.ac.jp/master_program/isa/professor/pdf/y_seto_shiryo13.zip (2014 年 4 月 28 日現在)
18) 産業技術大学院大学：プライバシー影響評価ハンドブック，http://aiit.ac.jp/master_program/isa/professor/pdf/y_seto_shiryo09.zip (2014 年 4 月 28 日現在).
19) 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― JIS Q 27001:2006（ISO/IEC 27001:2005） 対応―，http://www.isms.jipdec.jp/doc/JIP-ISMS114-21.pdf (2014 年 4 月 28 日現在).

坂本 誠（非会員）a1221ms@aiit.ac.jp
2014 年産業技術大学院大学産業技術研究科情報アーキテクチャ専攻修了（情報システム学修士），（株）ベラ代表，一般財団法人日本情報経済社会推進協会嘱託研究員.

岡崎 吾哉（非会員）a1208mo@aiit.ac.jp
2014 年産業技術大学院大学産業技術研究科情報アーキテクチャ専攻修了（情報システム学修士), 1994 年青年海外協力隊（理数科教師），1997 年情報数理研究所，2011 年フリーエンジニア.

岡本 直子（非会員）a1246no@aiit.ac.jp
2014 年産業技術大学院大学産業技術研究科情報アーキテクチャ専攻修了（情報システム学修士）. 2012 年韓国外国語大学英語学部通訳翻訳学科卒業.（株）ケイト・スペード ジャパン IT シニアマネージャー.

川口 晴之（非会員）a0818hk@aiit.ac.jp
2014 年産業技術大学院大学産業技術研究科情報アーキテクチャ専攻修了（情報システム学修士）. 1991 年川崎市立井田病院放射線診断科勤務，診療放射線技師.

永野 学（非会員）a1141sn@aiit.ac.jp
2014 年産業技術大学院大学産業技術研究科情報アーキテクチャ専攻修了（情報システム学修士），1994 年より学校法人聖学院教職員（理科，情報）.

瀬戸 洋一（正会員）seto.yoichi@aiit.ac.jp
1979 年慶應義塾大学大学院修士課程修了（電気工学専攻），同年（株）日立製作所入社, 2006 年より産業技術大学院大学教授. リスクマネジメント，個人認証技術の教育研究に従事. 工学博士（慶応義塾大学），技術士（情報工学）.

投稿受付：2014 年 5 月 1 日
採録決定：2015 年 7 月 31 日
編集担当：大島浩太（埼玉工業大学）

本論文は特集「プライバシーフレンドリーステム」への投稿論文です.