一般
投稿論文

個人情報影響評価の健診総合システムへの適用

瀬戸 洋一[†1]　渡辺 慎太郎[†2]　高坂 定[†3]　慎 祥揆[†1]

[†1]産業技術大学院大学　[†2]（株）ジュピターテレコム　[†3]（株）メディック総研

健診総合システムのクラウド化が進んでいる．健診総合システムで扱う医療データは機微な個人情報であり取り扱いには注意を要する．漏洩した個人情報を回収することは困難である．また，システムが適正に構築されていない場合，運用時の対策に多大なコストがかかる．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，個人情報の漏洩などの脅威や脆弱性を明確にし，ステークホルダへの影響を事前に評価するリスク管理手法として，個人情報影響評価がある．本稿では，健康診断サービスを事業とする一般財団法人協会が構築を進めている健診総合システムに対して実施した個人情報影響評価の事例を紹介する．

1. はじめに

2010年に「医療情報システムの安全管理に関するガイドライン」が改訂され，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]．このため，総務省，厚生労働省，経済産業省は電子健康記録（EHR : Electronic Health Records）システムおよび個人健康記録（PHR : Personal Health Records）システム構築（総称して健診総合システムと呼ぶ）の実証実験に取り組んでいる．

健診総合システム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．一方で，個人情報の漏洩やデータの改ざんなどの問題が指摘されている[2]．特に医療情報システムでは個人の診療情報という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，個人情報漏洩などの問題への対策が必要である．

海外では，個人情報の漏洩を低減するための手段として，プライバシー影響評価（Privacy Impact Assessment）を活用している[4],[5],[6],[7],[8],[9]．

プライバシー影響評価は，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，個人情報の漏洩などの問題を明確にし，ステークホルダへの影響を事前に評価するリスク管理手法である．

カナダやオーストラリアの政府機関では，個人情報を取り扱う情報システムを構築する際に，社会制度，つまり，プライバシーコミッショナ（Privacy Commissioner）のもと，プライバシー影響評価を実施して個人情報の安全性を事前評価することがシステム構築の予算認可の条件となっている[10]．一方，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条によりプライバシー影響評価の実施を義務付けている[11]．

我が国においても，特定個人情報ファイルを扱う行政機関などに対し，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（通称　番号法）第27条で特定個人情報保護評価の実施，および評価の結果を全項目評価書などにまとめることが義務付けられている．評価書を作成し広く国民の意見を求めた上で，特定個人情報保護委員会による承認後，報告書を公開することになった[7],[12]．

特定個人情報保護評価は，特定個人情報（個人番号を内容に含む個人情報）のみを対象とする事務（運用）を中心に実施する自己評価であり，個人情報を扱うシステムに対し第三者評価として実施するプライバシー影響評価とは異なるものである．

プライバシーは個人情報のうち機微な情報を意味する

が，プライバシー影響評価の対象は，機微な個人情報だけでなく，氏名，性別，住所など一般的な個人情報も対象である．欧米では「プライバシー影響評価」という用語を使っているが，本稿においては，用語の統一のために日本, 韓国で用いている「個人情報影響評価（Personal information Impact Assessment，以下PIAとも表記する）」の用語に統一する[4],[8],[13],[14].

本稿では，健康診断サービスを事業とする一般財団法人協会（以下協会）が構築を進めている健診総合システムに対して実施した個人情報影響評価の事例を紹介する[16]．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実施手順，第4章で事例を述べる．

2. 個人情報影響評価の概要

2.1 個人情報影響評価とは

個人情報影響評価とは，「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（利害関係者）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ことを目的とするリスク管理手法」である[4],[14].

1990年代，個人情報の電子化の進展に伴って情報システムにおける個人情報の漏洩などの問題が顕在化し，個人情報影響評価が検討されはじめた．個人情報影響評価は各国の事情により実施の方法が異なっている．1990年代後半には，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，個人情報影響評価の実施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．カナダ，ニュージーランド，オーストラリアでは，社会制度として個人情報影響評価が実施される一方，米国，韓国では法的に規定し実施している[4],[5],[13],[15].

個人情報影響評価を実施する目的は，個人情報漏洩などの対策コストの低減とステークホルダ間の信頼構築にある．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個人情報漏洩問題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，システム改修費用を低減することができる．また，実施組織が個人情報影響評価報告書を公表することで，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，個人情報影響評価は一種のリスクコミュニケーション手段ともいえる[14].

2.2 国際標準 ISO 22307

ISO 22307（Financial services - Privacy Impact Assessment）は，ISO　TC 68/SC 7（金融サービス）により開発され，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[17].

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，ほかの業種にも適用することができる．

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

①計画

影響評価の適用範囲の定義，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．

②評価

計画で定義した影響評価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．

③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，評価事項を文書化する．

④十分な専門知識

実施プロジェクトのメンバに対して，法律分野，システム技術，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

実施プロジェクトのメンバに対して，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，中立を確保するよう要求する．

⑥対象システムの意思決定時の利用

実施結果をシステム構築や改築時の意思決定に利用する．

個人情報影響評価を実施する諸外国では，国際標準の要求事項に適合し，各国の社会制度に合わせたガイドライン（実施手順書）を整備している．

日本において，国際標準であるISO 22307に従い開発した実施手順を第3章で述べる[18].

	プロジェクト計画①	評価準備②	個人情報リスクの識別③	個人情報リスクの分析④	個人情報リスクの評価⑤	報告⑥
評価手順	1. 実施体制の整備	1. 評価関連資料の収集	1. 個人情報の識別	1. 影響度の評価	1. 必要なリスク対応の検討	1. 報告書の作成
	2. 対象範囲の確定	2. 対象システムの分析	2. リスクシナリオの識別	2. 発生可能性の評価	2. 個人情報保護評価	
	3. 参照法令や規格, ガイドライン, 社内規程, 契約類の特定	3. データフローの分析	3. 既存または計画済み対策の識別			
	4. 実施計画書の作成	4. 評価シートの作成				
成果物	・実施計画書⑦	・システム分析書 ・データフロー分析書 ・評価シート⑧	・個人情報管理台帳 ・リスク分析表	・リスク分析表	・リスク分析表 ・評価シート⑨	・個人情報保護評価報告書⑩

図 1　個人情報影響評価の実施手順

3. 個人情報影響評価の実施手順

3.1　個人情報影響評価の実施手順

図 1 に個人情報影響評価の手順を示す．手順は ISO 22307 に準じて詳細化するが，リスク分析の具体的な方法については，ISO 22307 の規格で記載されていないため，3.2 節で述べる分析方法を開発した [18],[19],[20].

(1) プロジェクト計画

プロジェクト計画フェーズでは，予備評価の実施および実施計画書を作成する（図 1 の①．以下図 1 は省略）．

本評価の実施計画を策定するために予備評価を実施し，扱う情報，システム構成などの基本情報を収集する．これらの情報をもとに，プロジェクトを推進する実施体制，影響評価の対象範囲，参照すべき法令や規格あるいはガイドライン，組織の内部規則を特定する．また，実施スケジュールおよび評価チームの体制について実施計画書にまとめる（⑦）．

(2) 評価準備

評価に必要な設計資料などを収集し，システム構成の分析，個人情報に関するデータフロー分析を実施する（②）．

また，管轄省庁の指定するガイドラインや個人情報保護に関する法令，組織内規則などをもとに評価の基準となる評価シートを作成する（⑧）．

(3) 影響評価の実施

影響評価は，リスクの識別（③），リスクの分析（④），リスクの評価（⑤）の手順で実施する．実際の評価は，評価シートをチェックすることにより影響評価を行う（⑨）．影響評価を実施するにあたり，システム分析およびデータフロー分析，および既存の対策などを理解した上でチェックする．

(4) 報告

個人情報影響評価報告書を作成し公開する（⑥）．

評価チームは，リスクに関する影響評価の結果をもとに，個人情報影響評価報告書を作成する（⑩）．報告書は，情報セキュリティ監査報告書の構成に準拠し，通常 3 つの区分で構成する [21],[22].

A）導入区分
- 目的
- 期間，スケジュール
- 適用範囲
- 体制（評価チーム, 実施依頼責任者）

B）概要区分
- 対象システムに関する記述（システム構成，取り扱う個人情報など）
- リスク評価実施手順およびリスク評価基準
- 実施にあたり使用した専門知識

C）意見区分
- 対象システムが計画する安全管理措置に対する評価
- 法令やガイドライン，組織内規程の整備などに関する評価

評価チームは，実施依頼組織の責任者に個人情報影響評価報告書を提出する．実施依頼組織に対し報告を行い，システム設計書における個人情報に関する問題の有無を指摘し，是正に関する助言を行う．報告後，実施依頼組織の責任者は，個人情報の取り扱いに関する責任者であるチーフプライバシーコミッショナ（Chief Privacy Commissioner，組織によっては，Chief Privacy Officer）の助言を受け個人情報影響評価報告書を承認し，正式に公開する．

3.2　個人情報影響評価におけるリスク分析手法

第 2 章で述べたように個人情報影響評価とは，「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．また，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．したがって，技術，法制度両方に関する問題を是正する必要がある [14],[16],[23].

一般的なシステム監査は，規則で定めた要求事項をシステムが満たすかどうかを一方向的に評価する．これに対し，規則自体の評価を合わせて行う点が個人情報影響評価の特徴である．

しかし，具体的なリスク分析の方法は ISO 22307 や各

国のガイドラインでも明記していない．

このため，個人情報リスクの識別（③）と分析（④）を行い，制度設計と技術設計を同時に評価する手法として，図2に示す双方向ギャップ分析と呼ぶリスクアセスメント手法を開発した[14],[16],[20].

(1) 要求事項の適合性評価

評価対象システムの技術設計文書（システム企画書や設計書など）が要求事項を満たしているか否かを確認する．また，技術設計文書で計画されている安全管理措置（管理策）がどのリスクと関連しているのかを明らかにする．

表1は，要求事項への適合性評価における判定パターンを示す．

ある要求事項に関して，該当するリスクが検出され，安全管理措置が十分に計画されていれば問題ない（判定パターン（i））．また，リスクアセスメントによってリスクが検出されない場合（判定パターン（iv)），安全管理措置は不要である．

リスクが検出されているにもかかわらず，安全管理措置が計画されていないか不十分な場合(判定パターン(ii))には，技術設計に不備があると判定する．また，該当するリスクが検出されずに安全管理措置がとられている場合（判定パターン（iii））には，個人情報の漏洩などプライバシー上の問題は存在しないが，対策にかかる費用が正当化できるかどうかを別途検証する必要がある．

(2) 要求事項の妥当性評価

要求事項の妥当性評価では，検出したリスクに関して要求事項が網羅されているかどうかを確認する．

対象システムが保有するリスクに関して要求事項が存在しない場合には，要求事項の不備を検証した上で，法令や規則を整備し，運用においてリスク緩和策を講ずるなどの勧告を行い，制度設計の改善を行う．

一例として，「暗号化方式の規定」が挙げられる．暗号方式は医療情報システムの安全管理に関するガイドラインに規定されていない．このため，ベンダ（システム開発チーム）に一任されている．つまり，システムのリスク分析を実施した結果，暗号の方式や鍵管理に関するリスクが見つかるが，医療機関の運用ルールには鍵管理などが明確に規定されていないという問題がある．

暗号化は，システムのセキュリティ機能を決定する重要な因子であり，ベンダへ一任する事項ではない．システム構築・運用者が明確な意思をもって決定すべき要求事項である．電子政府推奨暗号リストなどを参照し，具体的な仕様を示す必要がある．

このように，リスクアセスメントを適切に位置付けることで，個人情報影響評価の定義である制度・運用・技術面の変更を促すことが可能になる．

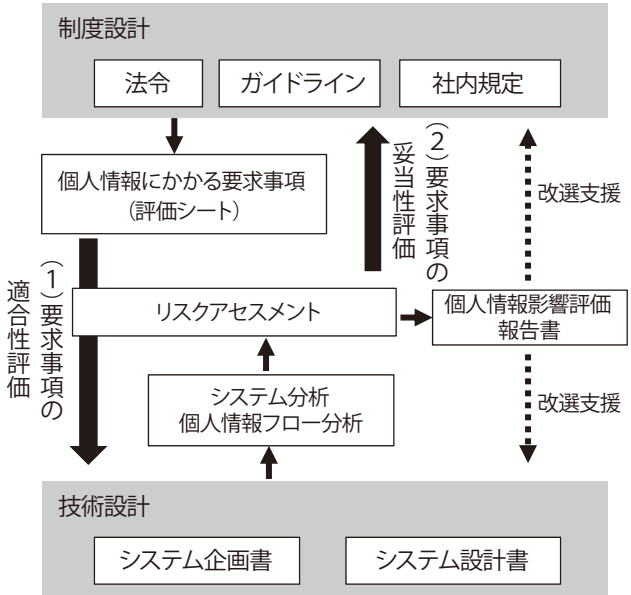

図2　双方向ギャップ分析

表1　要求事項への適合性判定パターン

No.	リスク	安全管理措置	判定
(i)	検出	十分	問題なし
(ii)	検出	なし・不十分	技術設計に不備
(iii)	未検出	あり	費用正当化必要
(iv)	未検出	なし	問題なし

4. 健診総合システムへの個人情報影響評価の実施

4.1 対象システムの概要

対象システムの分析を行う評価チーム（大学）は医療関係者ではない（大学院の教員と学生）．このため，評価の前に，健診総合システムへの学習や理解を深めた．

健診総合システムを構築運用する協会は，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し，健診結果報告書作成までの時間を短縮することにより，事業所・受診者へのサービス向上，およびシステム保有コストの圧縮を目的として，プライベートクラウド上に健診総合システムを構築することを決定した．

以下にシステム概要を示す．

(1) システム機能

図3に示すように，健康診断業務に関する情報（健康診断の結果や請求情報，健診スタッフの勤務状況やスケジュールなど）を，一括管理し，インターネット回線を

用いて複数の拠点（協会支社）や診断先（医師，検査機関）にて使用できるようにする．

(2) システム運用者およびサービス利用者

システム運用者は，開発担当，業務担当，健診スタッフ，医師，診療所スタッフであり，サービス利用者は健診を受ける受診者である．レコード（データ）数は延べ400万人分（約80万人分／年×5年）である．

4.2 プロジェクト計画

健診総合システムについて，学生たちの理解が深まった後，実際の個人情報影響評価の手順に従い，影響評価の適用範囲，作業期間の見積もり，必要な専門知識の特定および，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，および，実施体制の編成を行った．この結果をプロジェクト計画段階に相当する実施計画書として作成した．

(1) 影響評価の実施体制

図4に示す実施体制を構築した．評価チームは，システム構築運用組織（協会）と影響評価を実施する組織（大学）との合同で設置した．

評価チームのメンバは，

- 個人情報影響評価に関する技量
- 個人情報保護法に関する知識
- 情報セキュリティに関する技量
- 情報システムに関する知識．たとえば，クラウドコンピューティング技術，データベース技術，ネットワーク技術，システム設計に関する技量
- 健診業務に関する知識

を有する人材で構成される．

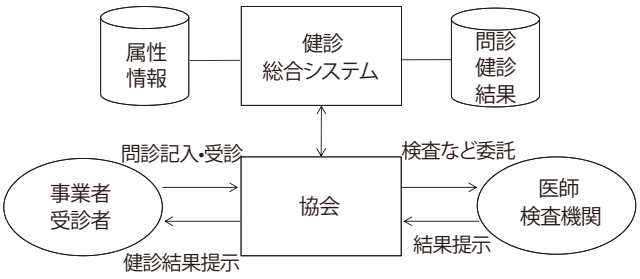

図3 システムと運用の概要

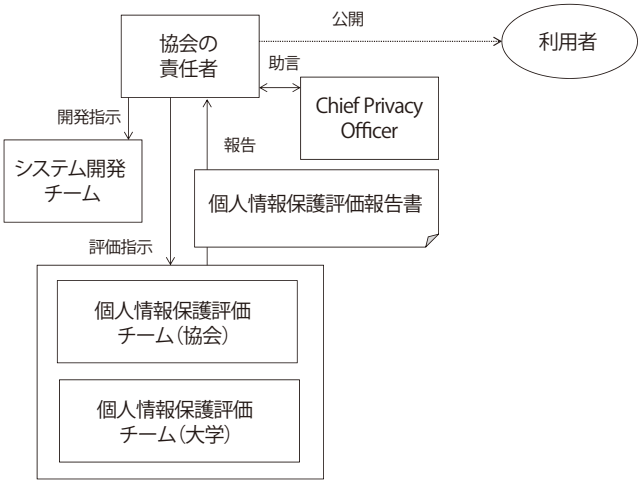

図4 個人情報影響評価の実施体制図

評価にかかった主な人的資源は，4人×5カ月=20人月（総計720時間）である．実作業の対応は，教員1名と学生3名，週9時間／人程度の対応であった．学生は個人情報影響評価に関する知識を学習しながら対応した．

4.3 対象システム

個人情報影響評価の対象とする医療機関は診療部門，検査部門などの多くの部門から構成され，その部門に対応した情報システムが存在する．

医療機関のシステムの中核をなす電子カルテシステムと医事会計システムを影響評価の対象範囲とする（表2参照）．また，病診連携システムは外部病院連携を行っているが，病診連携システムと電子カルテシステム間での情報の受け渡し部分までを対象範囲とし，外部連携機能については対象範囲外とする．今回の評価対象であるクラウド化基本設計書に記述されたシステム構成の確認，および個人情報の取得，利用，保管，破棄までのデータフロー分析を実施した．

4.4 評価準備

(1) 評価関連資料の収集

評価資料として，適用法令や規格，対象システム関連文書，実施組織の内部ポリシー文書などを収集した．一例を挙げると以下のとおりである．

①組織外文書

- 医療情報システムの安全管理に関するガイドライン（厚生労働省発行）
- 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（経済産業省発行）

表2 評価対象システム一覧

NO	システム名	使用目的
1	電子カルテシステム	診療録・オーダ・看護支援
2	医事会計システム	医事請求・会計・レセプト・DPC（Diagnosis Procedure Combination: 診断群分類．包括評価による定額払いに使用）
3	文書管理システム（Yahgee）	文書の作成支援・管理
4	病診連携システム（C@RNA）	地域医療施設との診療予約連携
5	シンクライアントシステム	シンクライアントおよびサーバ

②組織内

- 就業規則
- システム概念図，データモデル図など

(2) 対象システムの分析

表2に評価対象のシステム一覧を示す．対象システムの分析システム構成をネットワーク，ハードウェア，ソフトウェアと分類し，脅威を意図的なものと偶発的なものとに分けて整理した．たとえば，ネットワークで意図的脅威として盗聴，不正侵入，偶発的な脅威として通信輻輳，故障などがある．

(3) データフローの分析

健診総合システムの構成，運用などに関する詳細を把握し，個人情報フロー，業務分析書を作成した．

受診時において，健診総合システムより受診票・問診票が出力され，受診者に渡される．受診者にて受診票・問診票が記入され，協会に提出し健診を受診する．

検体の検査は検査会社へ委託し，レントゲンの読影・判定については医師に依頼する．それぞれの検査結果や判定および問診情報は健診結果として，健診総合システムに登録される．

健診終了後，健診結果報告書・一覧表が健診総合システムより出力され，協会を介して事業所・受診者に渡される．

4.5 リスク識別と分析

システム構成，および個人情報フローをもとに個人情報リスクを分析する．システムが取り扱う個人情報データは，氏名連絡票の入出力など，複数人の個人情報を取り扱う業務が多く，紛失・流出した際に与える影響が大きいことが推測される．また，データのシステム入力時に誤入力や取り違いが発生する可能性のある業務が見られ，正確性が重視される健診データは，誤入力，取り違いを発生させない取り組みが必要である．協会では健診結果という機微な情報を取り扱うため，個人情報の適切な管理が強く要請される．

4.6 リスク評価

適用法令および規格をもとに，リスク評価項目をチェックリストとする評価シートを作成した[1],[24],[25]．評価シートは，OECD（経済協力開発機構）で，個人情報保護の基本となるガイドライン「OECD8原則」に準拠して大分類し，各項目に関し具体的なチェック項目を中分類，小分類といった階層的な構成で37項目を作成した．表3に評価項目の概要を示す．

図5に評価シートの例を示す．記載項目は，以下の通

表 3　評価項目の概要

	大項目	中項目	項目数
1	目的明確化の原則	利用目的の特定，個人情報の特定，機微情報	3
2	利用制限の原則	第三者提供，目的外利用の同意，利用目的の変更，個人情報の共同利用	5
3	収集の原則	本人の同意	1
4	データ内容の原則	データの正確性	1
5	安全の原則	プライバシー保護機構，脆弱性対策，データの消去，識別認証，通信の保護，アクセス制御，監査，安全管理措置，システム関係者の管理，その他運用体制の整備	22
6	公開の原則	個人情報保護方針	1
7	個人参加の原則	個人情報の開示，個人情報の内容の訂正，個人情報の利用の停止，第三者提供の停止	4

健診総合システム基本設計におけるPIA評価シート

文書番号：AIIT-0xx_yyyymmdd　　産業技術大学院大学 2012/mm/dd

No	中項目	評価項目	回答	評価結果		指摘・推奨事項	参照資料
<1> 目的明確化の原則							
1	利用目的の特定	評価対象システムにて、取得・利用される個人情報の目的は特定されているか。	参照資料からは、利用目的を特定する文言が確認できない。	個人情報の利用目的は、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：利用目的を特定する文言を基本設計書に盛り込むこと。	文書番号：001_20120318「システム概要」
2	個人情報の特定	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、C福祉協会における個人情報の範囲について、定期的に現実（法律改訂等）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。	参照資料からは、個人情報の定義に関する文言が確認できない。	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。	文書番号：001_20120318「システム概要」
3	機微情報	評価対象システムにて、法令に基づく業務以外で以下の特定の機微な個人情報の取得を行っていないか。 a) 思想、信条及び宗教に関する事項。 b) 人種、民族、門地、本籍地、身体・精神障害、犯罪歴、その他社会的差別の原因となる事項。 c) 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項。 d) 集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項。 e) 保健医療(3)及び性生活。 ※感染症、精神疾患に係わる情報、病名、検査結果、受診科、障害度、介護度などの情報。	機微情報の定義については、厚生労働省平成16.10.29基発第1029009号通達において「HIV感染症やB型肝炎等」の感染症や「色覚検査等の遺伝情報」と定められている。参照資料においては、当該検査以外の「感染症・メンタルヘルス」等の結果について事業主には通知しないことを定めている。	上位文書において機微な情報が特定され、取り扱いが定められているため、問題ない。	○		平成16.10.29基発第1029009号通達「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針について」 文書番号019_20120728「健康情報の取り扱いについてのお知らせ」
<2> 利用制限の原則							
4	第三者提供	評価対象システムにて、個人情報を第三者へ提供することを想定しているか。想定している場合、その利用目的が特定されているか。	閲覧資料からは、対象システムが個人情報を第三者へ提供する業務が確認できない。	個人情報の第三者への提供は想定されておらず、問題ない。	○		文書番号：001_20120318「システム概要」
5	目的外利用の同意	評価対象システムにて、C福祉協会が、個人情報の取得・利用目的を超えて利用する場合、本人の同意を得る手続き、手順が定められているか。	参照資料からは、本来の目的を超えて取得・利用することは想定されておらず、定められていない。	本来の目的を超えて取得・利用することは想定されていないので、現時点では問題ない。	○	推奨事項： 今後の業務拡大の可能性を鑑み、手続き・手順を定めておくこと。	文書番号：001_20120318「システム概要」
6	利用目的の変更	評価対象システムにて、取得・利用する個人情報の利用目的を変更する場合、変更前後の利用目的の妥当性(合理的な範囲を超えていないか)を確認する手続き、手順が定められているか。	参照資料からは、利用目的の変更は想定されておらず、定められていない。	利用目的の変更は想定されていないので、現時点では問題ない。	○	推奨事項： 今後の業務拡大の可能性を鑑み、手続き・手順を定めておくこと。	文書番号：001_20120318「システム概要」
7		評価対象システムにて、取得・利用する個人情報の利用目的を変更する場合、本人に通知、または公表する手続き、手順が定められて	参照資料からは、利用目的の変更は想定されておらず、定められていない。	利用目的の変更は想定されていないので、現時点では問題ない。	○	推奨事項： 今後の業務拡大の可能性を鑑み、手続	文書番号：001_20120318「システム概要」

図 5　評価シートの例

りである．

①評価項目：対象システムに対する要求事項を記入

②回答：評価項目に対する実態を記入

③評価結果：評価結果の要点を記入．結果は，○（適合），×（不適合），△（評価不能），－（評価対象外）の4段階で記入

④指摘・推奨事項：評価結果が適合または評価不能の場合，推奨意見を記入（任意），不適合の場合，問題点を記入

⑤査閲資料：評価の証拠とした資料やヒアリング結果を記入

4.7　報告

評価シートの各評価項目について，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．

評価区分には，情報セキュリティ監査で用いる三区分（重要な不備，不備，軽微な不備）を採用した．区分の詳細を表4に示す．

健診総合システムのクラウド化に対する個人情報影響評価を，37の評価項目に関して実施した．評価の結果，軽微な不備を6件検出した．

- 重要な不備　　0件
- 不備　　0件
- 軽微な不備　　6件

表5は，検出した「軽微な不備」の内容，つまり，評価シートより指摘事項に該当する指摘項目，および指摘理由を示す．

提起した推奨内容は22項目あった．以下の3つに分類される．

第1は，基本設計段階では未確定である項目が挙げられる．たとえば，クラウド事業者の選定に関して，推奨事項を記した．

第2は，純粋に技術的な項目である．識別認証において多要素認証を推奨，および個人情報の開示・訂正・停止に関し，出力理由の記録，追記型の記録，保存記録に関する匿名化，などの推奨事項を記した．

第3は，運用に関する項目である．目標未達リスクの管理，システムでの役割と職責とのマッピングの整備，定期的な監査，および継続的な教育に関し推奨事項を記した．

上記の評価結果は，システム設計自体の問題というより，クラウドコンピューティングという新しい技術を導入したことによる，組織のルールなどが未整備な軽微な指摘事項といえる．個人情報影響評価では，システム的な個人情報漏洩リスク分析のほか，双方向ギャップ分析によるリスク分析手法を用いることにより，組織ルールなど基本設計時に考慮すべき制度的な課題も事前に洗い出せることが特徴である．

また，個人情報影響評価プロジェクトをシステム構築運用組織と評価チームと協力して実施することにより，組織の個人情報保護意識が高まるなどの効果を認めることができた[26]．

以上の評価結果を個人情報影響評価報告書としてまとめ，協会内の責任者および個人情報保護に関する責任者チーフプライバシーオフィサに提出した．個人情報影響評価報告書の是正内容はシステム運用時までに是正されることになった．

表4　評価区分

評価区分	区分説明
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である

表5　軽微な不備の一覧

指摘項目（中項目）	指摘理由
利用目的の特定	個人情報取得の利用目的が査閲文書に記されていない
個人情報の特定	個人情報の定義や，定義改訂の手続き・手順が査閲文書に記されていない
本人の同意	個人情報の取得にあたり，本人の同意を得ることが査閲資料から確認できない
データの正確性	データ訂正の手続きや手順を定めた文書が存在しない
訂正	過去の健診結果内容に関して訂正を行わない運用である一方，システム的には変更が可能である
停止	個人情報に関して保管期限を定めた文書が存在しない

5. まとめ

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に対して，個人情報影響評価を実施した．その結果，以下の結果を得た．

(1) 設計は適正に行われているが，新しいシステムを運用する組織のルールが準備されていないなど制度的な課題を明確化できた．

(2) 個人情報影響評価をシステム構築運用組織と評価チームと協力して進めることにより，組織の個人情報保護意識が高まるなどの効果を認めることができた．

(3) 実施手順を用いて対応した．初めて影響評価を実施する者であっても，この実施手順によって効率的に実施することができることが実証された．

個人情報影響評価の事例はまだ少ない．開発した実施手順をもとに，いろいろな分野の事例を増やし，効果を検証することが重要である．

謝辞　今回，匿名扱いとなったが，個人情報影響評価の実施の機会を与えていただいた健診総合システムを運用する一般財団法人協会および評価の実施に協力いただいた協会職員に感謝します．また，実施ガイドラインの開発には，産業技術大学院大学の大学院生であった，岡崎吾哉，岡本直子，川口晴之，坂本　誠，鶴田亜由美，永野　学，前島　肇各位の協力があった．

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) 総務省：平成 24 年版情報通信白書 (2012)．
3) Metz, C. : We' re Like a Bank for Your Data, Google, Wired (2012)．http://www.wired.com/2012/05/google-apps-iso/ (2016 年 3 月現在)
4) 瀬戸洋一 他：プライバシー影響評価 PIA と個人情報保護，中央経済社 (2010)．
5) Wright, D. and Hert, P. D. : Privacy Impact Assessment, Second Edition, Springer Verlag (2012)．
6) 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)．
7) 瀬戸洋一 (監修)：自治体のための特定個人情報保護評価実践ガイドライン，ぎょうせい (2015)．
8) シン・ヨンジン (著)，瀬戸洋一・JIPDEC (監訳)：情報化社会の個人情報保護と影響評価，頸草書房 (2014)．
9) 韓国行政安全部・KISA (韓国インターネット振興院)：個人情報保護評価遂行ガイド (2012)．
10) カナダにおける PIA ガイドライン，http://www.cio.gov.bc.ca/cio/priv_leg/foippa/pia/pia_index.page (2016 年 3 月現在)
11) 米国における PIA ガイドライン, http://www.gsa.gov/portal/content/102237 (2016 年 3 月現在)
12) 日本における特定個人情報保護評価指針，http://www.ppc.go.jp/enforcement/assessment/ (2016 年 3 月現在)
13) 岡本直子，岡崎吾哉，川口晴之，坂本　誠，永野　学，慎　祥揆，瀬戸洋一：韓国における個人情報保護評価の制度と実施状況，日本セキュリティ・マネジメント学会誌，第 29 巻，第 1 号，pp.17-26 (2015)．
14) 瀬戸洋一:実践的プライバシーリスク評価技法，近代科学社 (2014)．
15) シン・ヨンジン (著)，瀬戸洋一・JIPDEC (監訳)：情報化社会の個人情報保護と影響評価，頸草書房 (2014)．
16) 渡辺慎太郎，瀬戸洋一 ほか：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，CSS2012 (2012)．
17) ISO 22307 Financial Services — Privacy Impact Assessment (2008)．
18) 永野　学，岡本直子，瀬戸洋一，岡崎吾哉，川口晴之，坂本　誠：個人情報保護評価ガイドラインの開発，日本セキュティ・マネジメント学会誌，第 29 巻，第 1 号，pp.3-16 (2015)．
19) 瀬戸洋一：個人情報保護評価 PIA の考え方と実施手順―プライバシーバイデザインとしての PIA ―，法とコンピューティング学会第 3 回小グループ研究会 (2013)．
20) 前島　肇，瀬戸洋一 他：プライバシー影響評価実施におけるリスクアセスメントの検討，情報処理学会 (2013)．
21) 情報セキュリティ監査基準 報告基準ガイドライン Ver.1.0, http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex06.pdf (2016 年 3 月現在)
22) システム監査と情報セキュリティ監査の違い Q&A，http://www.saaj.or.jp/team_for10years/QandA10_201002.pdf (2016 年 3 月現在)
23) 瀬戸洋一：スマートシティにおけるプライバシー影響評価の適用，IEEJ Tran.EIS, IEEJ Transactions on Electronics, Information and Systems , Vol.133, No.7, pp.1427-1435 (2013)．
24) 個人情報保護マネジメントシステム―要求事項，JIS Q 15001, http://www.meti.go.jp/policy/it_policy/privacy/jis_shian.pdf (2016 年 3 月現在)
25) 医療分野の個人情報影響評価の資料，http://aiit.ac.jp/master_program/isa/professor/y_seto.html (2016 年 3 月現在)
26) 坂本　誠，岡崎吾哉，岡本直子，川口晴之，永野　学，瀬戸洋一：個人情報影響評価の有効性評価，情報処理学会デジタルプラクティス，Vol.7, No.1, pp.52-60 (2016)．

瀬戸 洋一（正会員）seto.yoichi@aiit.ac.jp
1979 年慶應義塾大学大学院工学研究科博士前期課程修了，同年（株）日立製作所入社，システム開発研究所にて，画像処理技術，地理情報処理技術，情報セキュリティ技術の研究開発に従事．セキュリティ研究センター副センター長，セキュリティビジネスセンタセンター長，主管研究員歴任後，2006 年より産業技術大学院大学教授．プライバシー保護技術の教育研究に従事．工学博士．

渡辺 慎太郎（正会員）watanabeshint@jupiter.jcom.co.jp
一橋大学経済学部卒業，産業技術大学院大学修了（情報アーキテクチャ専攻）．（株）ジュピターテレコム サイバーセキュリティ推進部アシスタントマネージャー．産業技術大学院大学認定登録講師．CISA，CISSP．

高坂 定（正会員）s.takasaka@medical-ict.com
医療 IT コンサルタント．（株）メディック総研．（一社）保健医療福祉情報システム工業会 国際標準化／国内標準化委員会委員．日本 HL7 協会 情報教育委員会委員長．日本医療情報学会会員．

慎 祥揆（正会員）shin@aiit.ac.jp
2009 年慶應義塾大学大学院工学研究科開放環境科学専攻博士後期課程単位取得後退学，2010 年から 2011 年まで慶應義塾大学理工学部准訪問研究員歴任．2011 年より産業技術大学院大学助教．データマイニング，e ラーニング，プライバシー，モバイルデータ処理に関する研究に従事．工学博士．

投稿受付：2014 年 4 月 9 日
採録決定：2015 年 11 月 30 日
編集担当：板倉真由美（日本マイクロソフト（株））

本論文は，特集「プライバシーフレンドリーシステム」(Vol.6, No.1) への投稿論文です．