

特定個人情報保護評価における課題分析

佐々木 真由美† 阪本 圭† 緑川 和宏† 慎 祥揆† 瀬戸 洋一†

†公立大学法人首都大学東京 産業技術大学院大学
140-0011 東京都品川区 東大井 1 丁目 10-40
seto.yoichi@aait.ac.jp

あらまし 地方自治体などで、マイナンバーを扱うシステムの構築および運用の開始にあたり、番号法で特定個人情報保護評価の実施が義務付けられた。保護評価の目的は、個人のプライバシー等の権利利益の侵害の未然防止と住民の信頼の確保である。2015年度になり、市区町村で保護評価が実施されたが、適正に保護評価が実施されていない評価書があると、関係者より指摘がある。

本稿では、公開された全項目評価書に関し、(1)リスク項目の妥当性、(2)評価書の再利用、および(3)評価モデルの分類について分析した。その結果、例えば、リスク対策については、システムにおける対策の記述はあるが、運用などシステム以外の対策の抜けがある評価書が多数存在した。

The Problem Analysis of Specific Personal Information Protection Assessment

Mayumi Sasaki† Kei Sakamoto† Kazuhiro Midorikawa† Sanggyu Shint† Yoichi Seto†

†Advanced Institute of Industrial Technology
1-10-40 Higashi Ohi, Shinagawa ku, Tokyo 140-0011, JAPAN
seto.yoichi@aait.ac.jp

Abstract Upon construction and launch of a system using the National ID “My Number”, the Local Government is required to implement the Specific Personal Information Protection Assessment based on the National ID Act. The Assessment aims to prevent infringement of personal rights and interests, and secure trust of residents. However, according to a government-related party, the Assessment may not be properly implemented. This paper analyzes the disclosed Assessment Reports in terms of (1) the validity of the risk items, (2) utilization, and (3) omission of assessment subject of the report. In many reports, for example, concerning risk countermeasures, the measures were described for the system, but no measures existed for risk items in operation.

1. はじめに

2015年10月、番号法により、住民にマイナンバーが通知される。マイナンバーを含む個人情報を特定個人情報といい、地方自治体などにおいては、特定個人情報を保有する該当事務に対し、保有前に特定個人情報保護評価(以下、保護評価)の実施が義務付けられた[1]。保護評価は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保を目的とし、地方自治体などが事前に自らリスク評価を行う。

保護評価の実施結果は、評価書として公開されている。しかし、保護評価が適正に実施されていない可能性があるとの指摘もある[2]。

本稿では、自治体が公開した全項目評価書を用い、(1)リスク項目の妥当性、(2)評価書の再利用、(3)評価モデルの分類の3つの観点で分析を行った[3]。

2. 特定個人情報保護評価の概要と課題

特定個人情報保護評価(以下、保護評価)は、しきい値判断により、基礎項目評価、重点項目評価、全項目評価の3つの評価に分類される[1]。しきい値判断は、対象人数と取扱者数、および特定個人情報に関する重大事故の発生有無に影響を受ける。

全項目評価を実施するケースは、他の評価と比較して、多数の特定個人情報を取り扱い、また、多数の者が情報を取り扱うため、特定個人情報の漏えいその他の事故が発生するリスクが高い。したがって、全項目評価書(以下、評価書)は、より詳細で具体的なリスク対策が必要とされる。

本稿では、評価書を対象とし、関係者によって指摘された3つの観点で分析した。

(1) リスク項目の妥当性

自治体などで実施される保護評価は、評価書にあらかじめ記載されたリスク項目に対して、リスク対策の内容を記述する方法で行う。しかし、リスク項目は画一的な記載であり、自治体がリスク対策を検討する際の具体的な水準は明示されていない。このため自治体などで、リスク項目のとらえ方や、対策の粒度に相違があることも考えられる。

(2) 評価書の再利用

自治体の事務の内容は、法律で定義されており、一部の自治体を除けば事務の内容に大きな差異はない。また同一自治体において、先に評価を行った事務の評価書の内容を再利用することも考えられる(例えば、住民基本台帳に関する事務を税に関する事務に再利用するなど)。

(3) 評価モデルの分類

特定個人情報を扱う事務では、情報提供ネットワークシステムを介して情報連携を行うことが可能となる。そのため、自治体などの保護評価の対象範囲は、該当事務から中間サーバー、情報提供ネットワークシステムなどの連携基盤を含めて評価することを求められている。

連携基盤では、他行政機関のシステム間でデータの連携を行う。しかし、事務を担当する職員が、意識せずに利用する連携基盤などは、保護評価の対象から見落とされる可能性がある。

3. 課題の分析

3.1 リスク項目の妥当性

3.1.1 目的

保護評価では、リスク評価に関する手順書が存在しないため、評価の実施は、自治体に委ねられている。また、評価を実施する担当者の専門性も要求されていないため、リスク評価の適正な実施が困難な可能性があり、実態を調査した。

分析対象の評価書は、リスク分析を網羅的に実施している全項目評価書とした。分析を実施した時点(2015年6月10日)では、221件の評価書が特定個人情報保護委員会から公開されている[3]。分析には、同一事務、「住民基本台帳に関する事務」に対する評価書を対象とした。分析対象とする自治体の地域は、偏りが無いよう日本各地の市区町村から選んだ。分析件数は、当時公開されてい

る対象事務の評価書(80件)の約10%に相当する9件とした。自治体の評価書との比較対象として国から提示されている記載要領を用いた。

3.1.2 方法

評価書のうち住民基本台帳ファイルに関する「Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策」の各リスク項目について、システムとシステム以外(運用)に対する対策に区分した評価基準を作成する。その上で作成した評価基準と、分析対象となる自治体の評価書と比較を行う。リスク評価は、システムとシステム以外(運用)では異なる脅威と脆弱性があるので、分けて対応する必要がある[4]。

比較した結果は、表1にしたがって指数化し、各リスク項目に対する対応に関して過不足を確認する。

表1 リスク対応の評価区分

評価結果	評価指数
評価基準で示しているリスク対応を充足している。または評価基準に記載のリスク対応に加えて、更なる対応を記載している。	3
評価基準で示しているリスク対応の一部のみ記載している。(評価基準で示す以外のリスク対応を記載しているが、評価基準で示しているリスク対応を充足していない場合も含む)	2
評価基準で示しているリスク対応を記載していない。	1
評価基準ではリスク対応を示していない。(例えば運用のみのリスク対応で問題がなく、システムでのリスク対応が存在しないケース)	- (評価対象外)

『(別添)特定個人情報に関する安全管理措置(事業者編)』に示す安全対策基準に従い、各リスク項目に対して実施すべきリスク対応を、システムでの対応と運用での対応(システム外)に区分して、評価基準を作成した[5]。表2に作成した評価基準の一部を示す。

表2 評価基準

リスク	措置の目的	システムで対応する措置	運用(システム外)で対応する措置
特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く)			
目的外の入手が行われるリスク	対象者以外の情報入手を防止する	1. アクセス可能な端末を制限する 2. 操作可能な職員を制限する 3. 個人単位の操作ログ取得する	1 個人情報収集に際して組織としてのポリシーを明確にしている(条例等) 2. 届出/申請内容や本人確認書類に基づく本人確認を行う 3. 届出とシステム入力内容に齟齬がないか照合を行う
	必要な情報以外の情報入手を防止する	1. 必要な情報以外は取得できないよう、インタフェース上定められている 2. 必要な情報以外はシステム上登録できないようにしている 3. 入手可能な業務・システムをシステム的に限定している	1. 個人情報収集に際して組織としてのポリシーを明確にしている(条件等) 2. 書式として必要な項目以外は記入できないよう、限定している 3. 記載例を提示し、必要な情報以外は記入されないようにしている

3. 1. 3 結果と考察

(1)システム

表3は、自治体におけるシステムのリスク対応に関する評価指数の分布と全項目の平均値を示す。評価基準で示したリスク対応を一切記載していない場合の評価指数が1ポイントである。自治体で実施した全49項目の評価指数の平均値が1ポイントに近い場合は、適切な評価が実施されていない可能性が高い。また、2ポイント以上のものは、適正なリスク評価を実施していることを示す。しかし、例え2に近い値であっても、リスク項目によっては適正なリスク対応ができていない可能性がある。

表3 リスク対応状況（システム）

全49項目	システム				評価指数 (全項目平均)
	3	2	1	0	
A市	7	12	5	25	2.08
B市	11	10	5	23	2.23
C市	7	12	6	24	2.04
D区	11	8	8	22	2.11
E市	9	13	3	24	2.24
F市	10	13	1	25	2.38
G市	11	12	1	25	2.42
H市	5	16	3	25	2.08
I区	24	0	0	25	3.00

(2)運用(システム外)

表4は、自治体における運用のリスク対応に関する評価指数の分布と全項目の平均値を示す。システムと比較して評価指数が低い。これはリスク対策についてシステムでのリスク対応のみが記載され、運用での対応が記載されていない自治体が多いことが原因である。

システムにおける分析と同様に、評価基準で示したリスク対応を一切記載していない場合の評価指数が1ポイントであることから、自治体で実施した全49項目の評価指数の平均値が1ポイントに近い場合は適切な評価が実施されていない可能性が高い。また、2ポイント以上のものは、適正なリスク評価を実施していることを示す。しかし、例え2に近い値であっても、項目によっては適正なリスク対応が実施できていない可能性がある。

表4 リスク対応状況（運用）

全49項目	運用				評価指数 (全項目平均)
	3	2	1	0	
A市	11	17	7	14	2.11
B市	12	21	2	14	2.29
C市	9	16	11	13	1.94
D市	12	12	12	13	2.00
E市	8	17	11	13	1.92
F市	12	14	10	13	2.06
G市	8	16	12	13	1.89
H市	11	13	12	13	1.97
I区	36	0	0	13	3.00

分析の結果、複数の自治体でリスク項目に対してシステムと運用を混在して評価を行っており、適正なリスク対応ができていない可能性があることが判明した。自治体におけるリスク評価は、評価ガイドラインが存在しないために、自治体間でリスク項目のとらえ方と記述の粒度に相違がある。

保護評価で、適正なリスク評価を行うには、リスク評価ガイドラインの整備が不可欠である。

3. 2 評価書の再利用

3. 2. 1 目的

自治体が公表した評価書と、総務省が例示した「住民基本台帳に関する事務に関する特定個人情報保護評価書記載要領(案)」(以下、記載要領)の項目を比較することにより類似度を明確にする[3][6].

3. 2. 2 方法

分析対象は、3. 1. 1 節で選定した評価書の本人確認情報ファイルとする。「Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策」について、評価書と記載要領とが一致する文字数を数え、その比率を算出する。表 5 にしたがって、指数化する。

表 5 一致評価指数

一致率 (%)	一致評価指数
不一致	0
25%未満	1
25%以上～50%未満	2
50%以上～75%未満	3
75%以上～	4

具体的には、以下の 2 点について分析する。

- (1) 自治体毎の一致評価指数： 評価書の措置の記載内容と記載要領の同箇所を確認し、自治体単位で、リスク項目ごとの一致評価指数を求め、全 34 項目の平均値を比較した。
- (2) 一致評価指数の高い項目： リスク項目ごとに一致評価指数を比較し、一致評価指数の高い項目を確認した。

3. 2. 3 結果と考察

表 6 は項目毎一致評価指数表の例の一部を示す。項目毎一致評価指数表は、リスク項目ごとに、各自治体の一致評価指数と全自治体(分析対象)の平均値を示す。

表 6 項目毎一致評価指数表

1. 特定個人情報ファイル名										
(2) 本人確認情報ファイル	A市	B市	C市	D区	E市	F市	G市	H市	I区	評価平均
2. 特定個人情報の入手 (情報提供ネットワークシステムを通じた入手を除く。)										
リスク 1 : 目的外の入手が行われるリスク										
対象者以外の情報の入手を防止するための措置の内容	4	4	4	4	4	4	4	4	1	3.7
必要な情報以外を入手することを防止するための措置の内容	4	4	4	4	4	4	4	4	4	4.0
リスク 2 : 不適切な方法で入手が行われるリスク										
リスクに対する措置の内容	4	4	4	4	4	4	4	4	3	3.9

(1)自治体毎の一致評価指数

表 7 は自治体毎一致状況を示す。自治体毎一致状況では、記載要領と評価書の同箇所を比較し、類似性を一致評価指数化し、自治体ごとの平均値を比較した。表 5 に示すように平均評価指数が 2 を超えるものは、一致率が 50%を超える。したがって、平均評価指数が 2 を超えるものは、再利用し

た可能性がある。平均評価指数が2を超える自治体は、6自治体であった。

表7 自治体毎一致状況

項目数 34	A市	B市	C市	D区	E市	F市	G市	H市	I区	平均
平均評価指数	2.54	2.82	1.77	3.23	2.03	2.23	2.40	1.97	1.69	2.30

(2)一致評価指数の高い項目

各自治体が共通して再利用した可能性が高い項目は、「目的外の入手が行われるリスク」、「不適切な方法で入手が行われるリスク」などがある。これらは、番号法の導入により新たに措置が必要となった項目である。また記載要領には、法律の番号が誤って記されているリスク項目がある。9件の評価書のうち誤った番号をそのまま誤記した評価書は、7件であった。

分析の結果、再利用の可能性のある評価書は、9自治体中6自治体であった。項目ごとにみると、番号法の導入により新たに設定したリスク項目は、再利用の可能性が高い。しかし、評価書の記述様式が、画一的であるため、再利用していなくても、結果的に記述内容が類似してしまう可能性がある。一方で、評価の効率化のために、記述例の再利用は、有効でもある。再利用に対しては、適切なリスク評価を実施しているか確認することが、第三者点検の責務であり、点検委員会(特定個人情報保護委員会)が適正に機能すれば、再利用に問題があるか否か確認できる。

3.3 評価モデルの分類

3.3.1 目的

マイナンバー制度において、自治体では、他の行政機関と情報連携し業務を進める。情報連携は、新設する中間サーバーおよび情報提供ネットワークシステム(以下、情報提供NS)で行う。

特定個人情報保護評価の対象範囲は、図1に示すように、4つのモデルに表せる。図1の赤枠は評価の範囲を示し、緑のボックスは特定個人情報の正本・副本DBを示す。

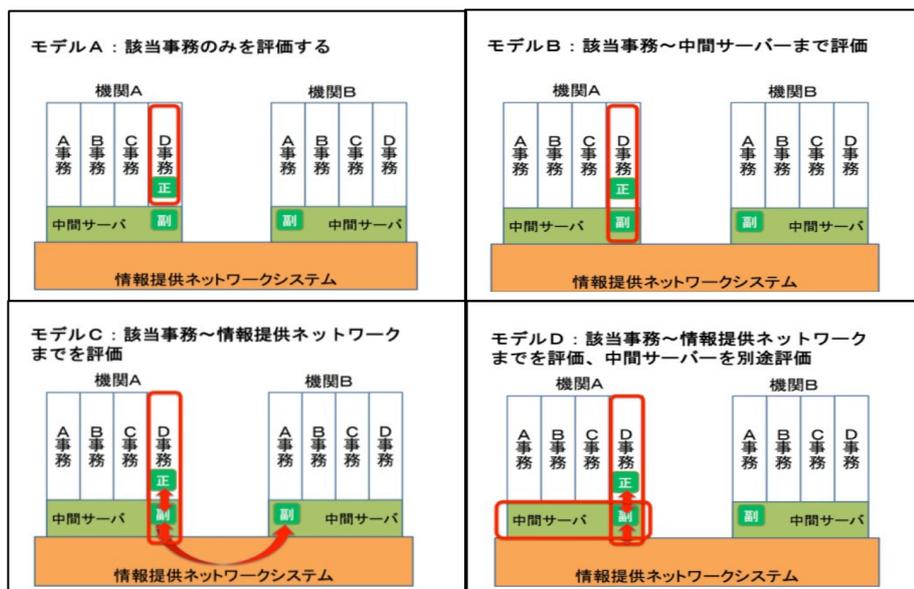


図1 評価モデル

モデルA: 該当事務のみを評価するモデル

モデルB: 該当事務から中間サーバーを含めて評価するモデル

モデルC: 該当事務から中間サーバー, 情報提供 NS を含めて評価するモデル

モデルD: 該当事務から情報提供 NS を評価し中間サーバーを別途評価するモデル

自治体の評価書を分析することで, どのモデルに分類されるか調査した.

3. 3. 2 方法

表 8 は, 自治体の評価書のモデル分類を示す.

表 8 評価書のモデル分類

モデル	対象と範囲	自治体	コメント
A	担当事務のみ	-	中間サーバーなどを評価対象としない. 評価内容としては問題ある.
B	担当事務~中間サーバー	C 市	自治体の中では, 早い時期(平成 26 年 11 月)に評価書を公表している.
C	担当事務~中間サーバー~ 情報提供ネットワーク	E 市, D 区, F 市 A 市, B 市, G 市 H 市	当初, モデル A の自治体が多かったが, 特定個人情報保護委員会から指摘され, モデル C に是正した.
D	担当事務~情報提供ネット ワーク/中間サーバー	I 区	事務システムの評価と中間サーバーの評価を別紙にて提出している.

初期に提出された評価書は, モデル A が多数あったと国より発表された. 評価書において, 市町村 CS(コミュニケーションサーバー)および中間サーバーについて評価していないと指摘があり, 再評価を助言された.

モデル B を採用した C 市は, 他の自治体に先行して保護評価を実施し, 早期に評価書を公表(平成 26 年 11 月)した. ただし, 例えば「...構築する予定」など, 安全管理措置の内容に具体性が欠ける記述があり, 中間サーバーの評価は不足がある. 情報提供 NS の運営は平成 29 年である. 他の自治体との連携は住基ネットワークの利用に留め, 当初, 情報提供 NS とは連携しないシステムを構築, 評価を実施する自治体はモデル B になる.

モデル C は, 特定個人情報保護委員会が推奨するモデルであり, 分析対象とした評価書の多くはこのモデルに相当する[1][7]. ただし, 具体的な安全管理措置に関し懸念がある. 例えば, 情報提供 NS へのアクセスを許可された者は, 自治体の首長であり, 適切な担当者のみへのアクセスを保証しなくてはならない. この場合アクセス制御は, バイオメトリック認証が適切であるが, この措置をとっている自治体はない.

I 区は, モデル D で, 事務と中間サーバーを分けて保護評価を実施している. 他の事務の保護評価を実施する場合において, 共通システムの保護評価の実施を省略することを目的としている.

3. 3. 3 結果と考察

(1) 評価対象に関し

当初, 情報提供 NW と連携を行わない自治体は, モデル B である. 情報提供 NW と情報連携を行う自治体は, モデル C である. ただし, 安全管理措置を適正に実施する必要がある. モデル D は, 現状の保護評価では, 連携基盤である中間サーバーや情報提供 NW に対し十分なりリスク評価が行えない可能性がある.

国の発表によれば, 市町村 CS および中間サーバーが評価対象から抜けていると指摘があった. しかし, 特定個人情報保護委員会は先行して, 種々の観点で評価のポイントを考察していることより, 本来, 留意事項は事前に公開されることが望ましい.

(2)リスク評価の適正化に関し

事務システムはパッケージされた製品が多く、中間サーバーや情報提供 NS の詳細仕様について、自治体職員がその技術的仕様を熟知することは困難である。また、システムと運用におけるリスクは発生原因、対策も基本的に異なるため、両者は分離してリスク評価をするべきである。

4. おわりに

地方自治体などにおいて、番号法により規定された特定個人情報保護評価が実施された。しかし、評価が適正に実施されていない可能性があるとの指摘があり、公開された評価書を対象としてリスク評価の実施状況を分析した。

その結果、リスク対策については、例えば、記録やルールに対して、システムにおける対策の記述はあるが、運用などシステム以外の対策は抜けている評価書が多数存在した。また、評価の対象について事務を評価するとしているが、実際には、システムへの知見が不足すると評価対象であるシステムやファイルを見落とす可能性があることが判明した。

これらの課題の対策として、リスク評価ガイドラインの提示、および評価結果を適正に監査する自治体対応の第三者点検組織の整備が必要であることが判明した。

謝辞 本研究は、産業技術大学院大学の Project Based Learning において実施された。PBLを進める上で、メンバーである黒沢裕太氏、沖村星児氏、馬小飛氏の協力を得た。ここに感謝の意を表します。

参考文献

- [1] 特定個人情報保護委員会： 特定個人情報保護評価指針の解説，平成 26 年 4 月 20 日（平成 26 年 11 月 11 日改正） <http://www.ppc.go.jp/files/pdf/explanation.pdf>
- [2] マイナンバー制度を揺るがす不適切な特定個人情報保護評価，pp. 6-10，日経コンピュータ，2015. 5. 14 号
- [3] 特定個人情報保護委員会： マイナンバー保護評価 Web <http://www.ppc.go.jp/mynumber/evaluationSearch/>
- [4] 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. 6
- [5] 特定個人情報保護委員会： （別添）特定個人情報に関する安全管理措置（事業者編），平成 26 年 12 月 11 日 [http:// www.ppc.go.jp/files/pdf/261211guideline2.pdf](http://www.ppc.go.jp/files/pdf/261211guideline2.pdf)
- [6] 住民基本台帳に関する事務に関する特定個人情報保護評価書記載要領（案） <http://www.ppc.go.jp/files/pdf/260624siryo1.pdf>
- [7] 特定個人情報保護委員会： 第 33 回特定個人情報委員会 議事概要 [http:// www.ppc.go.jp/files/pdf/261118gaiyou.pdf](http://www.ppc.go.jp/files/pdf/261118gaiyou.pdf)