マイナンバー制度でのリスク対策と監査

－自治体等の特定個人情報保護評価をモデルにして－

平成27年11月20日

システム監査学会常任理事
大阪成蹊大学名誉教授
松田　貴典

マイナンバー制度の確立

「行政手続きにおける特定の個人を識別するための番号の利用に関する法律（番号法）」に基づく社会保障・税番号制度（通称、マイナンバー制度）は、平成27年10月5日から施行され、平成28年1月1日に運用開始される。番号法では、住民票を有するすべての人に12桁の個人番号（マイナンバー）を付して、効率的に情報を管理し、複数の機関に存在する個人の情報が同一人の情報であることを確認する社会基盤として活用される。

改正番号法及び改正個人情報保護法が平成27年9月3日に成立。
平成28年1月1日より、①特定個人情報保護委員会を改組し、個人情報保護委員会を新設、関連する定めを個人情報委員会に移行、②社会保障、税、災害対策の分野での活用から、金融や医療の分野に利用範囲を拡大する等
平成29年ごろに、①個人情報の定義の明確化でグレーゾーンを解決し、「匿名加工情報」について自由活用を認め、②5000人要件の撤廃で、小規模取扱事業者へも法が適用される等

期待される効果

- 一つ目は、「**公平・公正な社会の実現**」

  所得や他の行政サービスの受給状況を把握し、負担を不当に免れることや給付を不正に受けることを防止するとともに、本当に困っている人をきめ細かに支援を行えるようにする。

- 二つ目は、「**国民の利便性の向上**」

  添付書類の削減などを行い、行政手続きを簡素化し、国民の負担を軽減する。また、行政機関や地方公共団体等が持っている自分の情報を確認したり、さまざまなサービスのお知らせを受け取るようにする。

- 三つ目は、「**行政の効率化**」

  行政機関や地方公共団体等で、さまざまな情報の照合、転記、入力などを要している時間や労力を大幅に削減する。複数の業務間の連携が進み、作業の重複等などの無駄を削減する。

懸念されていること

マイナンバーが個人にとっては、
- 国家による**個人情報の一元管理**されるのではないか
- 個人情報の**不正追跡・突合・財産等の権利侵害**となるのではないか
- 個人情報の漏えい、滅失、毀損、不正使用等による**プライバシーの侵害**につながるのではないか等

個人番号（カード）の活用にあたっては、
- 個人番号（カード）を何に使うのか
- 個人番号（カード）をどのように管理（保管）するのか等

企業や事業体にとって
- 従業者の個人番号の**収集**をどのようにすればいいのか
- 集めた個人番号をどのように**管理**すればいいのか

リスク対策の不考慮や個人情報の漏えいが企業や事業体にとっては
- 行政や企業等の戦略目標達成へ**失策**につながる
- 企業価値や**ブラント価値、レピュテーション**の低下となる
- **社会的責任（CSR，GSR）**が問われることになる

特定個人情報保護評価の実際

評価の意義とリスク対策

特定個人情報保護評価の意義

1. **事前対応**によるプライバシー等の権利利益の侵害の**未然防止**
2. 諸外国で採用されている**PIA**（Privacy Impact Assessment：プライバシー影響評価）に相当
3. 行政機関や地方公共団体等は、特定個人情報保護評価書に、**個人のプライバシー等の権利利益を侵害するリスクを自ら分析し、対策を講じて保護に十分であると「宣言」**
4. 特定個人情報ファイルの取扱いプロセスにおけるリスク対策が厳格に求められており、**リスク対策の内容が詳細に且つ具体的**に記載

そこで、先行する特定個人情報保護評価でのリスク対策の監査及び自己点検は、**「マイナンバー制度でのリスク対策と監査」の実務研究に最適なモデル**である

特定個人情報評価の概要

① 特定個人情報ファイル【注】の取扱いに対して厳しい法規制の強化を図る
② 技術面では特定個人情報の提供は原則として情報提供ネットワークシステムを使用して行う
③ 制度面では、特定個人情報保護委員会による監視・監督の強化
④ 個人情報の漏えい、滅失、毀損や不正使用による個人のプライバシー等の権利侵害を未然に防止する目的として、事前のリスク分析とその軽減措置として「特定個人情報保護評価」を原則義務付けた

【注】 特定個人情報とは、個人番号を含む個人情報。特定個人情報ファイルとは、個人番号を内容に含む個人情報ファイル又はデータベースのこと

特定個人情報保護評価は、特定個人情報ファイルの取り扱う事務の

① 対象人数
② 従業者(委託先を含む)にうち特定個人情報ファイルを取扱う者の数
③ 特定個人情報に関する過去1年間の重大事故発生の有無に基づき
④ 特定個人情報ファイルを保有する前に、特定個人情報保護評価を実施し基礎項目評価と重点項目評価又は全項目評価の実施を判断(しきい値判断)
⑤ その結果を「特定個人情報保護評価書」に記載し公表する

【特定個人情報評価書の記載事項】

Ⅰ　基本情報
Ⅱ　特定個人情報ファイルの概要
　1．名称
　2．基本情報
　3．特定個人情報の入手・使用
　4．特定個人情報ファイルの委託
　5．特定個人情報ファイルの提供・移転
　　（委託を伴うものを除く）
　6．特定個人情報の保管・消去
Ⅲ　特定個人情報ファイル取扱いプロセスにおける
　リスク対策
　1．特定個人情報ファイル名
　2．特定個人情報の入手
　　（情報提供ネットワークを通じた入手を除く）
　3．特定個人情報の使用
　4．特定個人情報ファイルの取り扱いの委託
　5．特定個人情報の提供・移転
　　（委託や情報提供ネットワークを通じた提供を除く）
　6．情報提供ネットワークシステムとの接続
　7．特定個人情報の保管・消去
Ⅳ　その他のリスク対策
　1．監査
　2．従業者に対する教育・啓発
　3．その他のリスク対策
Ⅴ　開示請求、問合せ
　1．特定個人情報の開示・訂正・利用停止請求
　2．特定個人情報ファイルの取扱いに関する問合せ
Ⅵ　評価実施手続き

【事例】

特定個人情報保護評価書（全項目評価書）

評価書番号	評価書名
1	後期高齢者医療制度関係事務　全項目評価書

個人のプライバシー等の権利利益の保護の宣言

奈良県後期高齢者医療広域連合は、後期高齢者医療制度関係事務における特定個人情報ファイルの取扱いに当たり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項	―

評価実施機関名

奈良県後期高齢者医療広域連合

特定個人情報保護委員会　承認日　【行政機関等のみ】

公表日

［平成26年4月　様式4］

「奈良県後期高齢者医療制度関係事務」の表紙
- 個人のプライバシー等の権利利益の保護の宣言
- 公表日：平成27年7月30日

出典：http://nara-kouiki.jp/images/about_us/joho/zenkoumoku_hyoukasho.pdf

特定個人情報保護評価の実施主体

■　**特定個人情報保護評価の実施主体**

○行政機関の長

○地方公共団体の長その他の機関

○独立行政法人等

○地方独立行政法人

○地方公共団体情報システム機構並びに番号法１９条第７号に規定する情報照会者及び情報提供者

■　**特定個人情報を保有しようとしている者及び保有している者**であり、情報提供ネットワークシステムを使用するか否かに関わらず、その公的性格に鑑み、実施が義務付けられている

■　これら以外の者である事業者は、主に源泉徴収義務等のために個人番号を取り扱うことが予定されているが、事業目的で個人番号を利用するものでないとして、実施の義務付けはされていない。但し、**情報提供ネットワークシステムを使用した情報連携を行う事業者は、事業のために個人番号を取り扱うものであり、番号制度への関与の程度も深い**などの理由により、特定個人情報保護評価の実施が義務付けられている

■　評価の実施が義務付けされない事業者は実施が望ましい

１．特定個人情報取扱いプロセスにおけるリスク対策

１．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）

①目的外の入手が行われるリスク
②不適切な方法で入手が行われるリスク
③入手した特定個人情報が不正確であるリスク
④入手の際に特定個人情報が漏えい・紛失するリスク
⑤その他のリスク

２．特定個人情報の使用

①目的を超えた紐付け、事務に必要ない情報との紐付け
②権限のない（元職員、アクセス権限のない職員等）によって不正に使用されるリスク
③従業者が事務外で使用するリスク
④特定個人情報ファイルが不正に複製されるリスク

３．特定個人情報ファイルの取扱いの委託

①委託先による特定個人情報の不正入手・不正な使用に関するリスク
②委託先による特定個人情報の不正な提供に関するリスク
③委託先による特定個人情報の保管・消去に関するリスク
④委託契約終了後の不正な使用に関するリスク
⑤再委託に関するリスク

4．特定個人情報の提供・移転（情報提供ネットワークシステムを通じた提供を除く）

①不正な提供・移転が行われるリスク
②不適切な方法で提供・移転が行われるリスク
③誤った情報を提供・移転してしまうリスク

5．情報提供ネットネットワークシステムとの接続

①目的外の入手がおこなわれるリスク
②安全が保たれない方法によって入手が行われるリスク
③入手した特定個人情報が不正確であるリスク
④入手の際に特定個人情報が漏えい・紛失するリスク
⑤不正な提供が行われるリスク
その他

6．特定個人情報の保管・消去

①特定個人情報の漏えい・滅失・毀損のリスク
②特定個人情報が古いまま保管されるリスク
③特定個人情報が消去されずにいつまでも存在するリスク

２．その他のリスク対策

１．監査（自己点検、監査、従業者に対する教育・啓発）

事例研究

リスク対策項目と管理基準例
（調査自治体等の記載事例を含む）

特定個人情報保護の監査にあたって

1. 基準の見直しが必須
   評価書に記載されている①特定個人情報ファイルの取扱いプロセスにおけるリスク対策及び②その他のリスク対策に着眼して、基準（主に管理基準）の見直しを実施する
   また、関連法令や社会規範、情報技術の進展にともなって配慮すべきサブコントロールや管理策基準についても見直しが必要である
2. 個人情報保護の監査基準や管理基準をもたない組織体等では、業務活動や環境等に配慮して独自の基準の策定が必要である
3. コンプライアンスの監査も必要
   特定個人情報の取扱いについて罰則が強化され、法人にも適用される
   例えば、◎個人番号事務等に従事する者（していた者）が正当な理由なく、特定個人情報ファイルの不正な提供（第67条）、◎不正な利益を図る盗用した場合（第68条）、◎業務に関する秘密を漏えい又は盗用した場合（第69条）、◎人を欺き、人に暴行を加え人を脅迫し、又は財物の窃盗、施設への侵入、不正アクセス等により個人番号を取得した場合（第70条）等、罰則が強化されるとともに、罰則によっては人のみならず法人にも適用される

評価書のリスク対策での管理基準例（一部）

調査自治体等での評価書のリスク対策事例からみた管理基準例
調査対象自治体等：千葉県柏市、兵庫県神戸市、大阪府堺市、奈良市、奈良県後期高齢者医療連合ほか

リスク項目内容	管理基準例（事例を含む）
目的外の入手が行われるリスク ・事務をするうえで必要な者以外が入手しないようにする対策 ・必要なもの以外の特定個人情報を入手しないようにする対策	・住民からの届出書等の記載ミスを防止する対策をとる ・他部署からの情報照会等では、別の個人と間違いのないように、一意性を確保するように確認を行う
入手の際に特定個人情報が漏えい・紛失リスク 情報の安全確保の観点から、情報漏えい・紛失のリスク軽減の措置	・入力画面や書類が関係者以外から見えないように配慮する ・届出書等の書類使用期間中は、処理が終われば厳重に保管する。また、メモ等は、使用後、高性能シュレッダーや焼却等にて復元不能の方法で廃棄する

（続き１）

リスク項目内容	管理基準例（事例を含む）
入手した特定個人情報が不正確であるリスク ・入手の際の本人確認の措置の内容 本人から個人番号の提供を受ける時、番号カードの提示もしくは身分証明書の提示を受ける等、厳格な本人確認をする（番号法１６条） ・個人番号の真正性確認の措置の内容 入手した個人番号が本人の個人番号で間違いないことの確認の方法 ・特定個人情報の正確性確保の措置の内容 入手した情報の正確性を保つための方法	・窓口の受付の際には、本人であることの間違いない書類・方法で本人確認を行う ・本人番号カードもしくは身分証明書にて本人確認を行う ・システムへの入力では、入力者とチェック者を別人にて行う ・転入届を受付ける際には、転出証明書を確認し、真正性に疑問がある場合には、転出地に確認をとる

その他のリスク	・スクリーンセーバーを利用して、長時間にわたり本人確認画面の表示をさせない ・統合端末を来訪者から見えない位置に置いて作業する

（続き２）

目的を超えた紐付け、事務に必要のない情報との紐付け ・宛名システム等における措置 ・事務を使用するその他のシステム措置。例えば、評価対象の事務に必要ない者の個人番号にアクセスできないような対策	・システム間で相互にアクセスできないようなシステム設計に行う ・市町村クライアントサーバーと統合、宛名システム間との接続を行わない ・個人番号へのアクセスは、アクセス許可をえた場合にかぎり可能にする
権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク ・ユーザ認証管理 ・アクセス権限の発行・失効の管理 ・発行管理：事務上必要なユーザについてのみＩＤ等を発行する手段 ・権限者を不必要に増やさないための手段 ・失効管理：事務範囲の変更、異動、休職、退職等、アクセスする必要がなくなったユーザ権限の失効手段 ・アクセス権限の管理 ・特定個人情報の使用の記録	・アクセス権限の発行・失効管理は適切に実施する。また、ユーザＩＤ・パスワードの付与の権限、対象者、使用記録等の確認を行う ・自動的にパスワード変更を要求し、パスワードの長期間使用を防止する ・生体認証により操作者の認証 ・退職・異動等による登録・抹消手続きを連携

（続き３）

特定個人情報ファイルが不正に複製されるリスク 　番号法は特定個人情報を作成できる範囲を限定している。不正に複製しない対策	・複製する端末を限定し、事前の許可申請を行い、承認をえるようにする ・ＵＳＢやＤＶＤ等の外部記憶装置にはアクセスできないように制限をかける ・外部媒体への複製は、権限者が行う
特定個人情報ファイルの取扱いの委託 ・委託先による特定個人情報の不正入手・不正な使用に関するリスク ・委託先による特定個人情報の不正な提供に関するリスク ・委託先による特定個人情報の保管 ・消去に関するリスク ・委託契約終了後の不正な使用等に関するリスク ・再委託に関するリスク	・業者選定にあたっては、過去の委託実績や履行状況を確認する ・委託先で特定個人情報ファイルを使用した業務の従事者、従事時間を記録させて、提出することを契約する ・システムの品質管理等の目的で、外部に特定個人情報ファイルが必要となった場合には、ダミーデータに変換する ・特定個人情報ファイルを取扱う保守業務では、遠隔保守はさせない ・特定個人情報の消去が必要になった場合には、記録媒体については返還させ、紙媒体の場合には、復元できないような方法（焼却、溶解処理等）で実施する

（続き４）

不正な提供・移転が行われるリスク ・どの職員がどの特定個人情報の提供又は移転をしたのか記録	・特定個人情報の提供・移転についてはあらかじめ仕様にて取り決めを行い ・システムの提供ログを保管して公訴時効となる７年間分を保存する ・提供・移転したネットワークの通信ログを記録し管理者による定期的なチェックを行う
誤った情報を提供・移転してしまうリスク **誤った相手に提供・移転してしまうリスク**	・情報提供する相手ごとに連携データの種別と、ＩＤ・パスワードを設定し、認証行為を行って誤送信をしないようにする ・連携データごとにデータの種別を、通信相手ごとにIDとパスワードによる認証を行う
安全が保たれない方法によって入手が行われるリスク	・他団体等との接続は、回線を専用回線、ＶＰＮ等で分離し固定する ・情報提供ネットワークシステムとのインタフェースにはフィルタリング機能、ＶＰＮ機能を実装し、通信を暗号化する ・離席時には必ずログアウトして、成りすましによる操作の防止をする

（続き５）

物理的対策 　特定個人情報の漏えい、滅失、毀損を防ぐための対策。例えば、特定個人情報が保有されているサーバーの設置場所に監視カメラを設置するなど方法により入退出者を管理することや、サーバー設置場所、端末設置場所、記録媒体・紙媒体の保管場所について施錠管理がなされていること	・特定個人情報を保有する場所は、物理的に堅牢で、地震、火災、洪水等の自然災害から適切に保護する ・特定個人情報を保有する部屋への入退出は、許可された職員のみに制限する ・特定個人情報を保有する場所は、情報保護の重要度（秘密レベル）に対応した物理的対策を行い、十分に保護機能を維持する
技術的対策 　特定個人情報の漏えい、滅失、毀損を防ぐための対策。例えば、ウイルス対策ソフトを導入することや、不正アクセス対策を実施すること	・特定個人情報を保有するサーバーや端末には、ウイルス対策ソフトを導入し、常に最新の定義ファイルの自動更新をする ・通信ネットワークシステムにはＵＴＭ（総合脅威管理）装置を導入し、総合的に通信ネットワーク脅威から保護する ・特定個人情報を保有するシステムでは、情報保護するための技術的対策は十分に保護機能を維持する

（続き６）

バックアップ 特定個人情報ファイルの滅失、毀損が発生した場合に復元できるように、バックアップを保管すること	・データバックアップは、特定個人情報ファイルが事故、災害等で滅失、毀損しても復元できるように、世代管理のもとで保管する ・データバックアップには、自動送信によるバックアップ、ミラー化によるバックアップをする、また、脅威の種類別による復元を可能にする

消去手順 ・保管期間を経過した特定個人情報を消去する手順が定められていること ・定められている場合は、特定個人情報を適切な時に安全かつ確実に消去できる手続き・体制がとられていること ・誤って消去すべきでない情報まで消去しないこと ・消去しなければならない情報の全部又は一部が消去されないまま残されていないこと	・保管期間を過ぎた特定個人情報の印刷物、資料、媒体等について廃棄・消去する場合には復元ができないように、紙媒体では高性能シュレッダーや焼却、溶解処理などを行い、電磁的記録媒体では復元不可能な物理的破壊等 ・外部の廃棄事業者に廃棄、消去を委託する場合に、職員の立ち合いのもとで行うか、廃棄業者から「廃棄証明書」等を受領する ・紙の異動届書等は保管期間ごとにわけて鍵付保管庫で保管し、保管期間を過ぎたものについては溶解処理を行う

（続き７）その他リスク対策

自己点検 　評価書に記載したとおりに運用されていること。 　その他特定個人情報ファイルの取扱いの適正性について評価を担当する部署自らが、自己点検を行うこと	・チェックリストは管理者用（管理的視点で記載）と担当者用（現場担当視点で記載）を作成し、その回答結果の差異をもとに問題点を洗い出し、実施すべき改善対策を明らかにして、効果的な自己点検を実施する ・実情に合わせた自己点検シートを作成し、年１回、職員による自己点検を実施する
監査 ・監査を行うか否か ・評価実施機関内の内部監査／外部の第三者による監査の別 ・監査事項 ・監査の頻度・方法 ・監査の責任者・監査実施体制 ・監査結果をどのように活用するか	・年度別監査計画を策定し特定個人情報保護の監査を実施する －評価書の記載事項と運用実態 －個人情報保護に関する規定、体制整備 －物理的及び組織・人的セキュリティ －アクセス制御、－通信及び運用管理 －アクセス管理、－システム開発及び保守 ・組織内部での監査のみならず、第三者の外部監査人による監査を実施する ・自組織の特定個人情報保護の監査基準及び管理基準を策定し、一定の保護の保証（合理的保証）がえられる「保証型監査」を実施する

（続き８）

従業者に対する教育・啓発 ・特定個人情報を取扱う従業者等に対して、特定個人情報の安全管理が図られるよう、教育・啓発活動について記載すること ・違反行為者への措置 違反行為を行った従業者等に対してどのような措置を講じるのか記載する	・特定個人情報を取扱う従業者等に対して、定期的に情報セキュリティに関する教育・研修を実施する ・特定個人情報を取扱う委託先の従業者に対して、定期的に情報セキュリティに関する教育・研修を実施する ・管理者は朝礼や現場の会議にて、日頃から特定個人情報保護について注意・喚起する ・特定個人情報の漏えいや無断持ち出し等の違反行為を行った従業者等に対する処罰規程を定める
その他のリスク対策	・トップを委員長とする「情報セキュリティ委員会」を設置して、定期的委員会の開催のもとで以下の問題対策検討を実施する －特定個人情報保護での問題と対策の検討 －リスク対策実施上での問題点と改善策の検討 －法や規程等の通達等の情報共有 －情報セキュリティ教育・啓発について －その他、情報セキュリティに関する諸問題への対応

特定個人情報保護の監査はどうあるべきか

■特定個人情報保護評価では、厳格な個人情報保護を求めており、自己点検を含めた監査の実施を**義務化**する
■管理基準の実効性を評価する
※実効性とは「管理基準が遵守されて、それが徹底的に実施され、特定個人情報の保護が有効に機能していること」
■特定個人情報保護評価書には、個人のプライバシー等の権利利益を保護する取組みを「**宣言**」しており、その運用が適正に実施されていることを**合理的保証**する「**保証型監査**」を実施する
■年に一度は、外部監査人による監査を実施する
■「ガバナンスと戦略目標の実現」に寄与する監査をめざすこと
個人情報の漏えいや紛失は、**社会的責任（ＳＲ）**を問われるばかりでなく、**レピューテーション**を急降下させることになる

■　目指すは「**セキュリティ文化の醸成**」である
それは、「情報セキュリティに対する認識を、組織のトップから現場まで高めるために、トップを委員長とする「**情報セキュリティ委員会**」を設置し、定期的な教育・啓発に加えて、日頃の業務活動の中から教育・指導をおこない、組織の中に「**セキュリティ文化の醸成**」を図ることである

参考・引用文献

発表内容の詳細は、特別寄稿「マイナンバー制度でのリスク対策と監査　ー自治体等における特定個人情報保護評価をモデルにしてー」　月刊監査研究　２０１５年１０月号に掲載している

- 「マイナンバー社会保障・税番号制度」　内閣官房ホームページ
  http://www.cas.go.jp/jp/seisaku/bangoseido/gaiyou.html
- 「特定個人情報保護評価指針」　特定個人情報保護委員会　平成26年4月20日
  http://www.ppc.go.jp/enforcement/assessment/
- 「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」特定個人情報保護委員会　平成26年12月11日
  http://www.ppc.go.jp/files/pdf/261211guideline2.pdf
- 「特定個人情報保護評価書（全項目評価書）」記載要領　特定個人情報護評価委員会ホームページ
  http://www.ppc.go.jp/enforcement/assessment/description/
- 松田貴典著　「ビジネス情報の法とセキュリティ」　白桃書房　2005