[Ⓡ 研究論文]

地方公共団体向け保証型システム監査の適用アプローチ

Approach to Apply the Assuring Type Systems Audit to Local Governments

小宮 弘信　松井 秀雄　金子 力造　田崎 竹雄　浦上 豊蔵　藤野 正純
Hironobu Komiya　Hideo Matsui　Rikizo Kaneko　Takeo Tazaki　Toyozo Urakami　Tadazumi Fujino

特定非営利活動法人　情報システム監査普及機構
NPO Information Systems Audit Diffusion Organization

概　要

筆者等は、過去に保証型システム監査を実施した経験を基に、言明書を用いることで実現可能な保証型システム監査の実施方法について検討を重ねてきた。

一方、個人番号の利用に先立って特定個人情報保護評価制度が開始され、地方公共団体は特定個人情報にまつわるリスクを事前に分析し、リスクを軽減するための適切な措置を講ずることを宣言することとなった。筆者等は、この公開された評価書を言明書と見なし、特定個人情報保護に関する保証型システム監査が可能であると考えた。

本論文では、保証型システム監査の概要と言明書の役割、特定個人情報保護評価における保証型システム監査の可能性及び実施方法や留意すべき事項について述べる。

キーワード：保証型システム監査、言明書、特定個人情報保護評価書、地方公共団体

はじめに

筆者等は、2009 年に中堅企業を対象とする保証型システム監査を実施した。保証型システム監査とは、組織体におけるシステム管理の統制状況を 、独立かつ専門的な立場のシステム監査人が検証又は評価することによって保証を与えるものである。その際利用したのが言明書である。言明書とは、組織の代表が自組織のシステム管理の統制状況の達成レベルについて表明するものをいう。その時の監査では、この言明書に基づいて保証意見を表明することができた。この事例を踏まえ、筆者等は研究グループを立ち上げ、保証型システム監査の実施方法について検討を重ねてきた。その後、当該研究グループは保証型システム監査を広く社会に浸透させるべく、2014 年に NPO として組織化し研究及び普及活動を行っている。

一方、2013 年に「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(以下、「番号法」という)」が公布され、2016 年に特定個人情報の利用が開始された。特定個人情報は、法令により目的外の利用が厳しく制限されており、特に地方公共団体は個人番号利用事務者としてより厳格な管理が求められている。政府では、地方公共団体における特定個人情報保護の管理状況を評価する制度が検討され、2014 年に「特定個人情報保護評価制度」として実施された。

筆者等は、この制度のもと地方公共団体から公表される「特定個人情報保護評価書（以下、「評価書」という)」に着目し、この評価書を言明書と見なし、特定個人情報保護に関する保証型システム監査の実施が可能であると考えた。

公開された評価書について調査を重ねた結果、その内容が自組織のシステム管理の統制状況の達成レベルについて表明されていることから言明書として活用できることが確認できた。そして地方公共団体が利害関係者である地域住民や議会等へ、特定個人情報を取り扱うにあたってリスクを軽減するための適切な措置を講じていることにつ

投稿受理日	2017 年 3 月 28 日
再投稿受理日	2017 年 9 月 6 日
査読完了日	2017 年 11 月 15 日

いて説明責任を果たすためには、この評価書を言明書と見なし、その要求事項に沿った保証型システム監査の実施が、有効であり必要であるとの結論に至った。説明責任を果たす方法としては、他にもISMS等の認証取得や諸制度を活用する方法も考えられる。ただし、いずれもそれぞれの要求事項は、国が定め、個人情報保護委員会が求める特定個人情報保護を目的とした要求事項とは異なる。認証と保証を混同しない様に留意しなければならない[注1]。

本論文では、地方公共団体における特定個人情報保護評価について、保証型システム監査の概要と言明書の役割を踏まえ、保証型システム監査の可能性及び実施方法や留意すべき事項について述べる。

第1章　保証型システム監査とは

1.1　保証型システム監査の可能性

システム監査基準にも示されているように、システム監査には「保証」を与えるものと「助言」を行うものの二つのタイプが存在する[注2]。財団法人日本情報処理開発協会による被監査部門を対象とした平成19年度システム監査普及状況調査によると、実施したシステム監査が「助言型」であったのが89.2%と、「保証型」の18.5%（複数回答あり）を大きく上回った。回答事業体の平均従業員数は3、455人と大企業であり、大企業でも「保証型システム監査」の事例は、きわめて少ないのが実情である[注3]。このように10年前のデータを持ち出さねばならないほど、保証型システム監査に対する調査は行われていないし、保証型システム監査そのものが普及していないと言える。

保証型システム監査が普及しない理由として、被監査組織の情報システム自体やそのガバナンスに関する整備状況や運用状況に対して、システム監査人が絶対的な保証を与えるような監査意見を表明する事は、被監査組織がどのようにリスク対策を行ってもリスクはゼロにはならないという事から極めて困難なためである。保証した後で何らかのトラブルが発生した場合、保証したことに対する賠償問題などシステム監査人にとってリスクが大きい。そのためシステム監査人は、IT統制全般に対する絶対的な保証を行うのではなく、入手した監査証拠を評価した範囲で保証を行うのである。

保証型監査を実施するために、入手する監査証拠の範囲を決めるための基となるのが、被監査組織の代表者から表明される当該組織のIT統制状況に関する「言明書」である。

言明書があってこそ、システム監査人は監査対象組織の統制状況がその言明書に記載されているレベルに達しているかを監査し、達成していると判断した時に保証を与える監査意見を表明することができる。

言明書とは、IT統制のための要求項目（要求レベル）が、どのようにコントロールされているか（管理レベル）を具体的に記述し、責任者がその要求に対する達成度合を「言明」として表明した文書である。

1.2　保証型システム監査の四分類

誰が、何の目的で保証型システム監査を依頼するのかを考えることで、どのような保証型システム監査があり得るのかが明らかにできる。この視点で分類すると、次の四分類となる。

①経営者主導方式

経営者主導方式とは経営者の要求に対して、現場では、どの程度対応できているかを監査する方式である。この時、経営者の要求に対して、管理・統制が出来ている旨を言明書という形式で明確に表明することが重要である。そして言明書通りに依頼組織の情報システムが整備、運用されているかを監査する。この方式の監査報告書は自組織に留め、利用されるべきものである。

図表1　保証型システム監査の四分類

分　類	依頼者	監査結果の利用目的	言明書作成	被監査組織
経営者主導方式	経営者	自組織の管理レベルを評価するため	自組織が考える独自なレベルでCIOが作成する	自組織
委託者主導方式	委託者	委託先の管理レベルを評価するため	委託者の要求レベルで受託者が作成する	受託者
受託者主導方式	受託者	委託元へ管理レベルを報告するため	委託者の要求レベルで受託者が作成する	受託者
社会主導方式	経営者	取引先や社会に対して、自組織の管理レベルを表明するため	一般に周知な高レベルの基準で依頼者が作成する	自組織

②委託者主導方式

委託者主導方式とは委託者の要求に対して、受託者がどの程度対応できているかを監査する方式である。受託者は委託者の要求に対してどのように対応しているかを言明書として表明する。システム監査人は言明書通りに受託者が対応しているかを監査する。監査報告書は委託者が利用する限定的なものである。また受託者の可監査性が前提となる。

③受託者主導方式

受託者主導方式とは委託者の要求に対して、受託者がどの程度対応できているかを監査する方式であり、その監査結果を持って受託者が委託者の要求に対して対応できていることを表明するものである。受託者は委託者の要求への対応を言明書として表し、委託者と合意を得る必要がある。また委託者から具体的な要求が出されない場合は、システム管理基準などを使い、関係者と具体的な要求に落とし込む必要がある。そしてシステム監査人は言明書通りに受託者が対応しているかを監査する。監査報告書は委託者に報告する限定的なものであるが、同じような要求レベルの複数の委託者に対して、二次利用されることも想定される。

④社会主導方式

社会主導方式とは様々なステークホルダーから信頼を得るために、自組織のシステム管理レベルを広く表明するため、監査依頼組織がどの程度システム管理を行えているかを監査する方式である。現状は法定化された基準がないため、システム監査人が保証意見を表明するには監査リスクを考え、高い管理レベルが必要となる。依頼者は独自の管理基準かまたは一般に認知されているシステム管理基準などを基に言明書を作成し、その言明書通りにシステムを運営しているかを監査する。監査報告書は言明書と共に社会に対して、ホームページ等を利用して公表される。

本論文で提案した方法に準拠すれば、保証型システム監査は実行可能であり、監査チームが異なっても監査意見はほぼ同じになる。保証型システム監査を実行するための要件は、① 被監査組織が監査可能な体制にあること、②「言明書」がシステム管理基準等からみて本来カバーすべき論点を相当程度カバーしていること、③監査チームが、被監査組織の規模や業態の特性に対応できる知識と経験を持った複数のシステム監査人で構成されていること、④システム監査人は、被監査組織から独立した第三者であることである。

保証型システム監査でも不適正意見を表明する場合もありうる。保証意見を表明できない場合には助言型システム監査に移行し、保証型システム監査で適正意見が表明できるように被監査組織に助言することもある。

第２章 地方公共団体の特定個人情報保護評価における保証型システム監査の必要性とその背景

番号法が施行されたことにより、特定個人情報を取り扱う地方公共団体を取り巻く環境がどのように変化し、保証型システム監査の必要性がどのように増しているのかを以下に述べる。なお、システム監査では「信頼性」「安全性」「有効性」等の観点から監査をおこなうが、情報の取り扱いにおける「安全性」は「情報セキュリティ」に関連する事から、本論文で言うシステム監査は情報セキュリティを包含する。

2.1 特定個人情報保護評価制度の開始

特定個人情報保護評価制度は、特定個人情報ファイルを保有する国の行政機関や地方公共団体が、個人のプライバシー等の権利利益に与える影響を予測した上で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分析し、そのようなリスクを軽減するための適切な措置を講ずることを宣言するものであり、2015 年に日本全国の地方公共団体がこの評価書を作成した。

この評価の実施手順は、個人情報保護委員会により次のとおり決められている。

①扱う対象人数の規模に応じて評価項目の詳細度を「基礎項目評価」「基礎項目評価＋重点項目評価」「基礎項目評価＋全項目評価」の３種類の選択肢から決定する

②詳細度に応じて定められた項目について自己評価を行う

③人口規模が大きい地方公共団体が作成する「全項目評価書」については、パブリックコメントを求め、指摘があればその対応を行う
（筆者等は近畿圏にある政令市に対して評価書のパブリックコメントを送り、同市が指摘事項を受け止めて評価書が改定された例がある）

④各地方公共団体は、評価結果を個人情報保護委員会に提出し、一般に公開する（ただし、公開の際、情報セキュリティ上のリスクになる部分は除く）

この制度の目的は、個人のプライバシー等の権利利益の侵害の未然防止及び国民・住民の信頼の確保である。しかし、地方公共団体は地域住民の信頼を確保するために、自組織内で行った評価とパブリックコメントへの対応だけで、地域住民の信頼を得られるとは考え難い。住民からの信頼を高めるために、個人情報保護分野の専門家による保証意見を添えて公表する取り組みを追加すべきである。ここに、保証型システム監査を実施する意義がある。

2.2　特定個人情報保護評価書と保証型システム監査における言明書の関係

保証型システム監査でシステム監査人が保証意見を述べる対象は「組織長の言明書」であるが、筆者等の調査では、適切な言明書を用意できていない組織が多かった。しかし、2015 年に日本全国の地方公共団体において作成された「特定個人情報保護評価書」を、「保証型システム監査」の前提となる「言明書」に相当するものと考えると、「保証型システム監査」を受ける根幹的な条件の一つが整った。「特定個人情報保護評価書」と保証型システム監査の「言明書」の主要項目の対応関係を図表２に示す。

2.3　サイバー・テロ等の増加傾向を踏まえた総務省の動向と地方公共団体に求められる対応

標的型攻撃メールなどのサイバー・テロにより機密情報が盗まれる事案が増加しており、地方公共団体は個人番号利用事務で扱う個人情報の安全

図表２　特定個人情報保護評価書を保証型システム監査の言明書と見なす場合の対応図
＜特定個人情報保護評価書＞（K 市 全項目評価書 住民基本台帳事務 P42 より抜粋）[1]

想定されるリスク	統制のための要求項目	統制の具体的記述	責任者が表明した達成度合
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	ユーザー認証の管理を行っている	・システムを利用する必要がある…認証を行っている ・認証後は利用機能の認可機能により…行っている ・パスワードの前回の変更から…仕組みとしている	リスク対策は十分である
	アクセス権限の発効・失効の管理を行っている	・職員異動等で権限の発効・失効の必要が生じた場合…システム管理担当者が権限の発効及び失効を行っている	
	アクセス権限の管理を行っている	・アクセス権限表のファイルを…ようにしている ・異動が生じた場合には…チェックを行っている	
	特定個人情報の使用の記録を残している	・システムで…一定期間保管している ・記録された情報を元に…を行っている	

管理措置を今まで以上に厳格に行う必要がある。また、その管理状態を地域住民に公表する必要がある。この流れを示すものとして2017年1月4日付日本経済新聞(朝刊)に次の記事が掲載された。

「総務省は地方公共団体の職員による不正会計や情報漏洩などを防ぐ体制づくりを地方公共団体の首長に義務づける。上場企業が導入している「内部統制」によるリスク管理を参考にし、基本方針や実施計画などをつくるよう求める。地方行政への住民の信頼を高める狙いだ。 ＜中略＞ 基本方針と実施計画に基づいて首長は人事体制の見直しや業務プロセスの改善を進め、1年に1回、内部統制状況評価報告書も作成する。報告書は地方公共団体が設置している監査委員の監査を受け、議会にも提出し、住民の代表である議会によるチェックを定期的に受けられるようにする。」

この動向を受けて、地方公共団体は情報漏洩などを防ぐ統制環境を整備し、その状況を評価する報告書を作成し、専門的知見を備えた第三者によるチェックを受ける体制をとるべきであり、住民の信頼を高めるために保証型システム監査を受けて監査意見を公開する必要がある。

総務省から2015年3月に出された「地方公共団体における情報セキュリティ監査に関するガイドライン」に次の記述がある。「786 の市区町村(45.1%)が情報セキュリティ監査を実施しているが、今後もさらに多くの地方公共団体で情報セキュリティ監査が実施されるよう、推進していく必要がある。」と記載されている。

助言型監査と保証型監査については次の記述がある。

「 外部監査の形態には、当該地方公共団体に対し、情報セキュリティ対策の改善の方向性を助言することを目的とする助言型監査と、住民や議会等に対し、情報セキュリティの水準を保証することを目的とする保証型監査がある。どちらの型の外部監査を行うかは地方公共団体の判断次第であるが、一般的には、情報セキュリティ対策の向上を図るため、最初は継続的な内部監査と併せて助言型監査を行い、必要に応じて保証型監査を行うことが考えられる。」

この記述から、総務省は地方公共団体に対して情報セキュリティ対策に関する外部監査を推奨しており、当初は助言型監査から始めて成熟度が上がった時点で保証型監査を行う方向性が示されている。

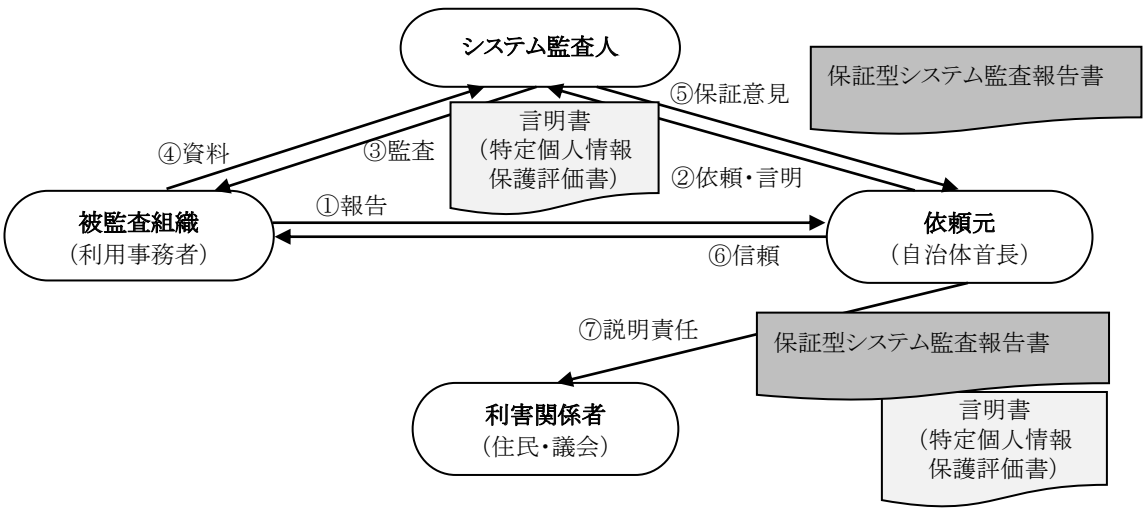
2.4 地方公共団体向け保証型システム監査の関係者

保証型システム監査には4つの分類がある事を第1章で述べたが、地方公共団体における保証型システム監査は地域社会に対して自組織の管理レベルを表明するものであるので「社会主導方式」に該当する。

保証型システム監査の関係者として、依頼元(地方公共団体首長)・被監査組織(個人番号利用事務者)・システム監査人の三者の役割を整理して図表3に示す。

地方公共団体は、他の地方公共団体との情報連携により個人番号利用事務を行っている。地方公共団体は個人番号利用事務の処理に必要な特定個人情報を、情報照会者として特定個人情報の提供を受け、また情報提供者として、他の地方公共団体の求めに応じ特定個人情報の提供を行う。これらの特定個人情報の照会・提供は情報提供ネット

図表3 特定個人情報保護評価における保証型システム監査の関係図(社会主導方式)



ワークシステムを通じて行われ、地方公共団体の情報システムで処理される。情報提供ネットワークシステム及び地方公共団体の情報システムの安全性及び信頼性は確保されなければならない。

このように組織間での情報連携が頻繁に行われることになるため、各地方公共団体において情報システムの管理レベルに大きな差があることは、漏洩等のリスク増大につながる。

以上述べてきたように、住民の信頼を高めるため地方公共団体は個人情報の管理状況について社会主導型の保証型システム監査を受けて保証意見を公開する必要性が高まっている。

第３章　保証型システム監査の実施方法

3.1　保証型システム監査の目的と対象

本研究における保証型システム監査は「番号法」に基づいて、地方公共団体で個人番号が適正に取扱われている事を表明した「特定個人情報保護評価書」を対象とする。地方公共団体が行う特定個人情報保護評価の妥当性を監査し、意見表明することを目的とするものである。

システム監査の対象は「評価書」に記載されている内容に限定する。その対象は情報システムのみでは無く、マニュアルによる個人番号の取扱いと誤謬による処理誤り、そしてコンピュータ処理に係わる情報漏洩等の業務上のリスクに対する統制であることに留意する。すなわち特定個人情報を扱う業務のリスクを軽減するための統制が整備され、機能しているかを監査し意見表明する。

3.2　保証型システム監査実施の規準と指針

保証型システム監査実施にあたって、システム監査人が拠り所とする「規準[注4]」が必要である。筆者等は、公開されている特定個人情報保護評価指針および地方公共団体が作成した特定個人情報全項目評価書を調査し、「特定個人情報保護のリスク対策とシステム管理規準」[2]と「全項目評価書記載ポイント集」[3]を作成した。

「特定個人情報保護のリスク対策とシステム管理規準」は、自治体及び地方公共団体が作成し公表した全項目評価書を基に、地方公共団体が統制として実施すべきリスク対策を対象にして、重要な管理規準を例示したものである。地方公共団体における特定個人情報保護に関する管理規定として活用することを目的としている。具体的には、特定個人情報の「入手」「使用」「委託」「提供・移転」「ネットワーク接続」「保管・消去」等の取扱いプロセス毎にリスクとそのリスク対策の要件を管理規準として例示した。また、その他のリスク対策として、「自己点検」「教育・啓発」「監査」について管理規準を例示した。

「全項目評価書記載ポイント集」は、地方公共団体が行った特定個人情報保護評価に対する意見募集で公開された特定個人情報保護評価書（全項目評価書）を分析し、記載ポイント集として当研究でとりまとめを行ったものである。全項目評価書の各リスク項目に記載された統制内容に対してシステム監査の視点から指摘事項を述べ、その具体的な改善点および事例を記載した。地方公共団体における特定個人情報保護に関する業務での具体的な統制として参照することができる。

筆者等は、「特定個人情報保護のリスク対策とシステム管理規準」と「全項目評価書記載ポイント集」を特定個人情報保護統制の保証の判断規準として活用することを提案する。また、これらを参照して具体的な取組を被監査部門に対して改善提案することも可能である。

個人情報保護委員会が公表している指針や解説には以下のものがある。

①特定個人情報保護評価指針第 10(2) に定める審査の観点[4]
行政機関等から個人情報保護委員会に提出された全項目評価書を審査し、承認する際、適合性及び妥当性の２つの観点から審査を行うと定めている。

②特定個人情報保護評価指針第 10(2) に定める審査の観点における主な考慮事項[5]
特定個人情報保護評価指針に定める審査の観点に基づき、指針に定める実施手続等に適合した特定個人情報保護評価を実施しているか (適合性)、特定個人情報保護評価の内容は指針に定める特定個人情報保護評価の目的等に照らし妥当と認められるか (妥当性) 等を審査するため、指針に定める審査の観点に加え、審査の観点における主な考慮事項を記載している。

③特定個人情報の適正な取扱いに関するガイドライン (行政機関等・地方公共団体等編)[6]
個人番号を取り扱う行政機関及び独立行政法人等、並びに地方公共団体及び地方独立行政法人が特定個人情報の適正な取扱いを確保するための具体的な指針を定めている。

3.3 地方公共団体向け保証型システム監査の実施手順

3.3.1 全体実施手順（提案～計画～監査～報告）

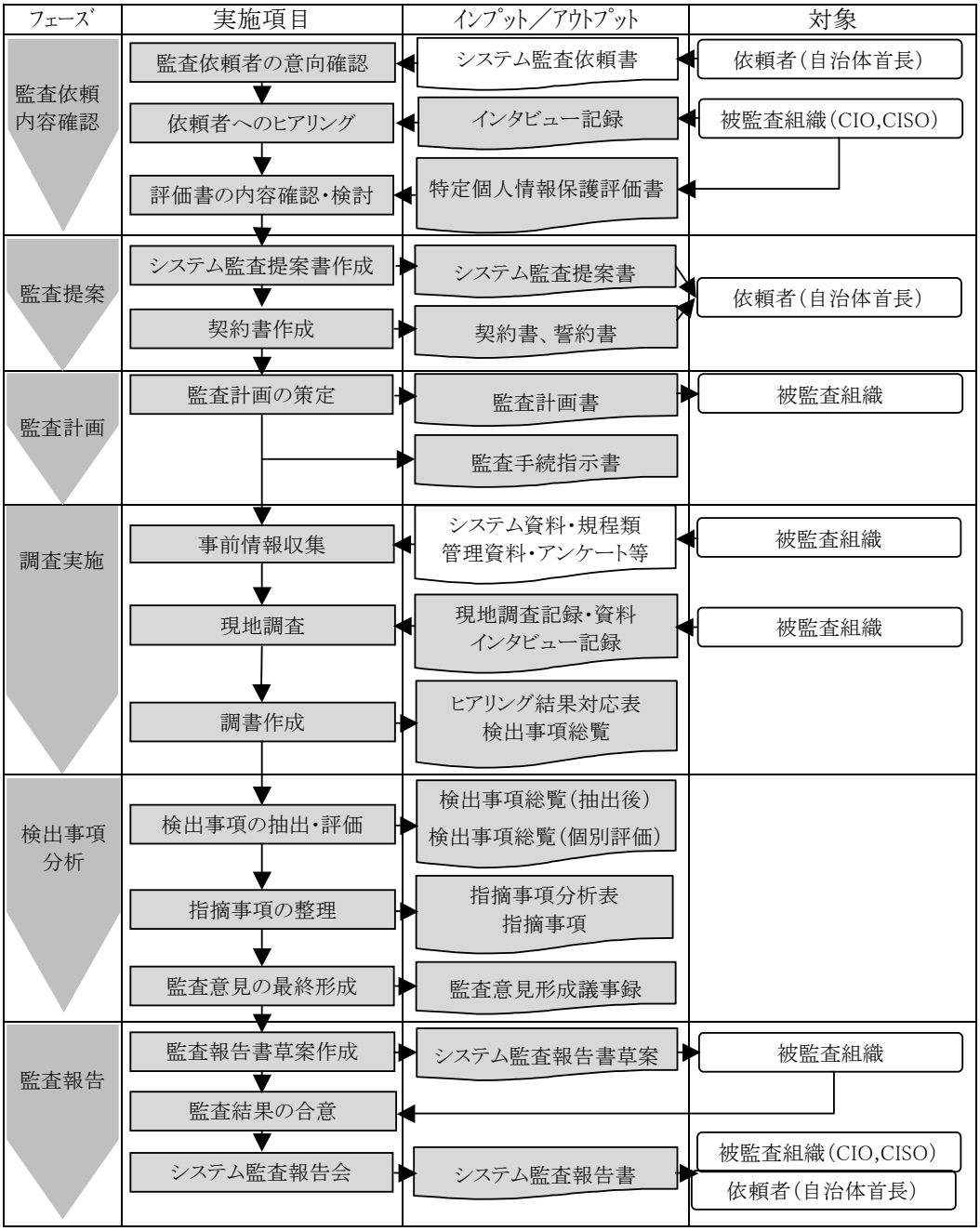
保証型システム監査の監査提案から監査計画、実施、報告までの全体フローを図表４に示す。システム監査のフェーズ毎に実施項目、インプット／アウトプット情報及び実施対象を示した。

筆者等は先行研究において、保証型システム監査の実施手順では監査計画の策定に入る前に「監査依頼内容の確認フェーズ」や「監査提案フェーズ」が必要であるとした。言明書の有無、言明内容に沿う監査証拠の有無などを確認することにより、保証型システム監査の実施について合意することができ、監査計画の策定に進めるからである。これは被監査組織が地方公共団体の場合も同様である。

3.3.2 監査依頼内容確認～監査提案～監査計画策定フェーズのポイント

このフェーズにおいて、まず依頼者とシステム監査人の間で保証の意味や範囲、制限事項について確認を行い、合意をすることが重要である。

図表４　地方公共団体向け保証型システム監査の実施手順



システム監査人は、言明書に基づいて監査要点を整理する。被監査部門に対してヒアリング等の予備調査を行い、言明書を担保する監査証拠となる文書類が存在するかを確認する。その結果、被監査部門の整備状況やIT統制の成熟度を考慮して保証型システム監査が可能であるかシステム監査人で討議し合意する。

保証型システム監査が可能であると合意した場合、依頼内容、監査の範囲、監査実施手順、監査スケジュール、成果物、見積金額等を記載したシステム監査提案書を作成し提出する。監査契約の締結後、言明書の内容に沿った監査要点を基に監査計画を策定する。

3.3.3 調査実施フェーズのポイント

このフェーズでは、システム監査人は現地調査でインタビューを行い、曖昧な回答はその内容を確認するとともに、保証意見の表明を可能にする監査証拠を収集する。

言明書を監査要点にブレークダウンし、それに基づいて監査証拠を収集する。監査証拠は、規定、規準、業務手順書等の文書やインタビュー、業務実施状況の観察記録などであり、調書としてまとめる。収集した監査証拠は、言明書の監査要点ごとに分類し整理する。

3.3.4 検出事項分析フェーズのポイント

システム監査人は、調査実施フェーズでまとめた検出事項から重要と思われるものについて評価を行う。評価項目は、監査目的、言明書を基に定め、その評価項目でランク付けを行い、指摘事項など監査意見形成に影響を与えると思われる重要事項を抽出する。

評価書には、リスク対策として「特に力を入れている」「できている」「十分である」などの自己評価が記載されている。筆者等が作成した「全項目評価書記載ポイント集」には各評価項目に具体的な統制事例を示している。この事例を参照することで自己評価の妥当性を判定し、被監査組織の統制目標レベルの設定が可能となり、監査意見の形成の一助とすることができる。

これらの討議及び合意内容は監査意見形成議事録として記録に残す。

3.3.5 監査報告フェーズのポイント

監査意見を監査報告書にまとめるにあたり、監査報告書草案の時点で被監査組織に対して事実誤認等がないか確認を取る。監査報告会を実施して地方公共団体の首長に報告し、システム監査報告書として依頼者に提出を行う。システム監査結果は、関係部門に周知し業務上のリスクを認識してもらい、継続的な改善を現場に定着させ、リスクをより低減させるように活用を図ることを伝える。

依頼者である地方公共団体は必要に応じ住民にシステム監査結果を公開する。

3.4 その他の留意点

保証型システム監査では、被監査部門のリスクが言明書に示された範囲、方法で担保されていることを意見表明し保証する。しかし、言明書の保証のみでは依頼者である首長の満足は得られないと考える。従来の助言型監査と同様に、業務上のリスクの強弱を診断し、弱いところを強化する提案を監査の付加価値として提供することは有益である。提案内容は、被監査組織の成熟度を勘案し、現場が実施しやすい改善を自らの取組で導入することを推進するものでなければならない。この監査意見が地方公共団体の業務改善に貢献する。

おわりに

2017年1月末現在で、地方公共団体の長、その他の機関から公開された全項目評価書は551件に及んでいる[7]。全国の地方公共団体で、統一の管理項目によりリスクを分析し、適切な対策を講じていると宣言することは画期的なことである。しかし、現状では評価書がようやく作成されたばかりであり、広く監査が実施されるまでには至っていない。また組織内部の自己点検や内部監査だけでは、評価書の実効性を評価するには不十分である。独立かつ専門的な立場のシステム監査人が、実際の運用状況について検証評価する外部監査によってこそ、リスクに対するコントロールが適切に整備・運用されていることが一定の条件において担保され、地方公共団体首長が住民や議会などの利害関係者に対する説明責任を果たすことにつながる。この事が、地方公共団体向けシステム監査の中でも、特に保証型システム監査を行う動機となり、地方公共団体における特定個人情報保護につながる。

さらに実効性のある監査を可能とする為には、評価書が適切に記載されていなければならない。公開された複数の評価書を調査した所、内容が曖

味で具体性を欠くものがあった。

記載内容の問題点として、まず全体として用語が統一されていない事、矛盾した記載がある事、さらに具体的な管理方法の記載で抽象的な表現、例えば「適切に行う」「可能な限り」「定期的に行う」など管理レベルを評価できない内容が見られた。これらの問題点を踏まえ、筆者等は、K 市から公開された評価書に対し、改善提言としてパブリックコメントを提出した。その結果、指摘した事項 111 項目に対し 58 項目が評価され改訂された。その内容は、K 市の住民基本台帳事務の特定個人情報保護評価書にかかる意見募集結果の中で「PIA 提出意見及び回答」として公開されている[8]。

このように、各地方公共団体で評価書が言明書として活用できるようレベルアップする必要がある。その上で、保証型システム監査の必要性と有効性を広く社会に認知してもらうことが今後の課題として挙げられる。筆者等の研究は、その為の具体的な監査手順を整理し、システム監査人が保証型システム監査を積極的に実施できる手立てを明らかにしていくことを目標としている。

【注記】

1. 保証行為であるところの「監査」と類似する用語との異同は以下の通りである。
「証明」は、他の者の行為やその結果についての事実の有無を証拠立てて明らかにすることであり、監査のように相対的ではない。「認証」は、ある者の行為の結果を、審査人が特定の規準にどの程度合致しているかを判定し、格付けし結果を公表することであり、監査のように総合判断はしない。「検査」は、個々の品質等の良否を判定して合否を表明するものであり、意見表明ではない。
2. システム監査基準（平成 16 年改訂版）Ⅱシステム監査の目的
3. システム監査を保証型監査で実施すべきか否かの意識調査について、「保証型監査で実施すべき」であるとの回答は 22.8% 、一方「保証型監査で実施すべきと思わない」は 24.1％と多くなっている。また「わからない」も 50.0％と多く、問題の難しさが浮き彫りになった。更に回答事業体の平均従業員数が 3、455 人と大企業であり、中堅・中小企業も含めると保証型システム監査を行った事業体の比率は、もっと少ないと考えられる。
4. 「規準」（criteria）とは、何らかの判定をするためのきまり・判断手段をいう。何らかの行為のもととなるきまり「基準」（standard）と異なることに留意する。

【参考文献】

1. K 市 ; 特定個人情報保護評価書の公表より No.01 住民基本台帳事務　全項目評価書 http://www.city.kobe.lg.jp/information/project/innovation/mynumber/img/01_zen_juuminkihon-konbini.pdf、参照日（2017 年 3 月 1 日）
2. 特定非営利活動法人情報システム監査普及機構 ; 特定個人情報保護のリスク対策とシステム管理規準、http://j-aisa.jp/、参照日（2017 年 3 月 1 日）
3. 特定非営利活動法人情報システム監査普及機構 ; 全項目評価書記載ポイント集、http://j-aisa.jp/、参照日（2017 年 3 月 1 日）
4. 個人情報保護委員会 ; 特定個人情報保護評価指針、平成 28 年 1 月 1 日、https://www.ppc.go.jp/files/pdf/20160101_shishin.pdf、参照日（2017 年 3 月 1 日）
5. 個人情報保護委員会 ; 特定個人情報保護評価指針第 10(2) に定める審査の観点における主な考慮事項、平成 26 年 8 月 26 日、http://www.ppc.go.jp/files/pdf/141111shinsakouryo.pdf、参照日 (2017 年 3 月 1 日)
6. 個人情報保護委員会 ; 特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）、平成 28 年 4 月 1 日 (改正)、http://www.ppc.go.jp/files/pdf/261218guideline.pdf、参照日（2017 年 3 月 1 日）
7. 個人情報保護委員会 ; 評価実施機関における特定個人情報保護評価書の公表の状況、平成 29 年 1 月 31 日 https://www.ppc.go.jp/files/pdf/290203_mynumber_public.pdf、参照日 (2017 年 3 月 1 日)
8. K 市 ; 住民基本台帳事務の特定個人情報保護評価書にかかる意見募集結果「PIA 提出意見及び回答」http://www.city.kobe.lg.jp/information/public/comment/gyoute/060shimin/iken.pdf、参照日（2017 年 3 月 1 日）