SAAJ 第175回定例研究会

保証型システム監査の実施方法に関する考察

～特定個人情報保護評価書を活用した保証型システム監査の可能性について～

2018年11月16日（金）

NPO情報システム監査普及機構
保証型システム監査研究会（i研）

発表者：金子力造
共著者：浦上豊蔵、小宮弘信、田崎竹雄、藤野正純、松井秀雄
監修：松田貴典

Agenda

Ⅰ 新システム監査基準に対するパブリックコメント

Ⅱ 保証型システム監査の概要

Ⅲ 特定個人情報保護評価制度での保証型システム監査

Ⅳ 特定個人情報保護評価書を用いた保証型システム監査

Ⅰ．新システム監査基準に対するパブリックコメント

1. パブリックコメント提出の経緯と結果
2. 診断についての意見
3. 利害関係者に対する説明責任についての意見
4. システム監査のニーズについての意見
5. 保証の範囲についての意見
6. 保証型システム監査の取扱についての意見
7. システム監査基準の役割と課題

Ⅰ-1. パブリックコメント提出の経緯と結果

● システム監査基準改訂のパブリックコメントに応募
  – 2002年の改訂から約18年ぶりに見直された内容(案)について、保証型システム監査研究会(i研)のメンバーで意見提出を行った。

「システム監査基準（案）」及び「システム管理基準(案)」に対する意見募集について	
意見募集の対象	•システム監査基準(案) •システム管理基準骨子(案)、システム管理基準(案)
案の公示日～意見受付締切日	公示日：2018年**03月06日**～ 締切日：2018年**03月20日**
問合せ先(所管府省・部局名等)	経済産業省商務情報政策局サイバーセキュリティ課

http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595218007&Mode=0&fromPCMMSTDETAIL=true

意見募集の結果について	
結果概要、提出意見、意見の考慮　結果・理由等	•**別紙1**(システム監査基準(案)について) •**別紙2**(システム管理基準(案)について)
結果の公示日	公示日：2018年**04月20日**
提出意見数	意見者(**19名**)、監査基準(**110件**)、管理基準(**54件**)
(内、研究会メンバー意見)	意見者(　**7名**)、監査基準(**40件**)、管理基準(**14件**) 採択された意見：監査基準(**26件**)、管理基準(**8件**)

http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595218007&Mode=2

改訂では、保証型システム監査について十分言及されていませんでした

Ⅰ-2. 診断についての意見

No.4、No8	監査基準－前文[1]
該当原文	[1] システム監査の意義と目的 　システム監査とは、専門性と客観性を備えた監査人（システム監査人）が、情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証、又は改善のための助言を行い、また、ニーズによっては現状の診断を行う監査の一類型である。
意見理由	・意見内容 　診断は監査の一類型ではない。「システム監査」と「システム診断」という異質な業務をひとつの「システム監査基準」で規律しようとするのは、根本的に矛盾し誤っている。・・・ ・意見内容 「・・・また、ニーズによっては現状の診断を行う監査の一類型である。」 この箇所は、削除すべきである。 ・理由 診断された結果は、監査の一資料として活用することは出来るが、診断そのものは監査ではない。
回答　〇	指摘も踏まえ、診断に関する記載については内容を見直し、削除いたします。

Ⅰ-3. 利害関係者に対する説明責任についての意見

No.11	監査基準－前文[1]
該当原文	[1] システム監査の意義と目的 システム監査は、・・・、組織体の経営活動と業務の効果的な遂行、さらにはそれの変革を支援 的な遂行、さらにはそれの変革を支援 し、組織体の目標達成に寄与することを目的とする。
意見内容	・意見内容 「・・・組織体の目標達成に寄与することを目的とする。」この箇所は、次のように改めるべきである。 「・・・組織体の目標達成に寄与すること、もしくは利害関係者に対する説明責任を果たすことを目的とする。」 ・理由 システム監査の目的は、組織のためだけはなく、利害関係者を守るために重要な役割を担う。社会的にも重要な側面であり、目的から外すべきではない。このことは、システム管理基準（案）5P、1．ITガバナンスの定義にも、「ステークホルダに対する説明責任」として記載されている。
回答　〇	御指摘を踏まえて対応いたします。

システム監査の目的とは？

Ⅰ-4. システム監査のニーズについての意見

No.43	監査基準3　解釈指針1（1）
該当原文	(1) 次のようなニーズに基づいて、システム監査の目的が決定される。 ①例えば、経営陣が・・・、②例えば、経営陣が・・・、③例えば、経営陣が・・・
意見内容	・意見内容 解釈指針に挙げる依頼者の事例に、次のニーズも記載すべきである。 1．システム委託者のニーズ。　委託先の管理レベルによって・・・ 2．システム受託者のニーズ。　システムを受託するに当たって・・・ 3．社会のニーズ。　社会的責任を負う重要インフラや・・・ ・理由 事例は、企業経営者が自組織を評価する場合のニーズに偏っている。 今日のシステム開発においては、自社開発よりも委託、受託による開発も多い。また、本監査基準の前文で、地方公共団体等なども対象としていることから、社会のニーズに対応したシステム監査も想定する必要がある。 自組織の経営に利するという観点だけではなく、外部監査、特に保証型システム監査を活用した組織外部の利害関係者を守るためのニーズもあることに留意すべきである。
回答　〇	御指摘を踏まえて対応いたします。

システム監査のニーズとは？

Ⅰ-5. 保証の範囲についての意見

No.50,51	基準3解釈指針2
該当原文	なお、システム監査のニーズによっては「システム管理基準」又は「情報セキュリティ管理基準」の一部分、あるいは組織体状況に適合するよう適宜選択した項目群を監査上の判断尺度とすることもできる。ただし、システム監査によって保証を行おうとする場合、保証の範囲が限定されることにくわえ、保証の客観性が損なわれる可能性があることに留意する。
意見内容	・意見内容 システム監査によって保証の範囲が限定されるものではない。なぜなら、保証型監査を行う場合、予め保証範囲を特定し、監査依頼者と合意をしているため、監査の結果、合意範囲より監査範囲を絞ることは無いからである。この箇所は、削除すべきである。
回答　×	内部監査を念頭におけば、必ずしもシステム管理基準を監査上の判断尺度として採用される場合ばかりではないと想定されるため、当該趣旨を踏まえ、以下のとおり修文いたします。 「ただし、採用される基準の範囲および性質によっては、保証の範囲が限定されることにくわえ、保証の客観性が損なわれる可能性があることに留意する。」

システム監査における保証とは？

Ⅰ-6. 保証型システム監査の取扱についての意見

No.109	監査基準　その他
該当原文	なし
意見内容	・意見内容 [基準3]の次に、「[基準4]保証型システム監査の実施」を追記する。情報システムの不稼働が、取引先や社会に及ぼすことが考えられる場合には、経営陣は、情報システムの信頼性を高める保証型システム監査の実施をめざさなければならない。このことを基準の内容に記載する。 ・理由 情報システムの高度化と多様化は、劇的に進展しており、システム監査の重要性及びその位置付けを明示的に記述する必要がある。それぞれの基準の説明で、「保証又は助言」という用語を多くの箇所で記述されている。しかし、その表現が、明示的に記載されていない箇所があるため、基準項目の追加、基準内容の追記が必要である。・・・
回答　×	保証型監査だけについて特に記載を行うことは、全体の構成から不適当であるため、原案のとおりとさせていただきます。いただいた御意見については今後の参考とさせていただきます。

Ⅰ-7. システム監査基準の役割と課題

- **システム監査基準の果たすべき役割とは？**
  - ✓ システム監査基準は、システム監査とは何か？誰のために？何のために？ 何を対象に？どのように行うべきか？を明確に定義し、システム監査を実施する者の拠り所となるものでなければなりません。
  - ✓ パブリックコメントに寄せられた様々な意見は、システム監査について真摯に考え、取り組んでおられる方々の考察の集大成です。

パブリックコメントは、公開された基準に比べ注目度は低いが貴重な成果物

- **保証型システム監査の果たすべき役割とは？**
  - ✓ No.47の意見より、「情報システムにまつわるリスクが組織の壁を越えて増大する社会情勢のなかで、利害関係者への説明責任を担保するために、保証型システム監査の担う役割は大きい。システム監査も、言明書を活用した保証型システム監査を検討し、基準に盛り込むべきである。」
  - ✓ No.109の意見より、「保証型システム監査の実施」は、今後のシステム監査で求められることになる。例えば、マイナンバーの保護の監査など・・・」

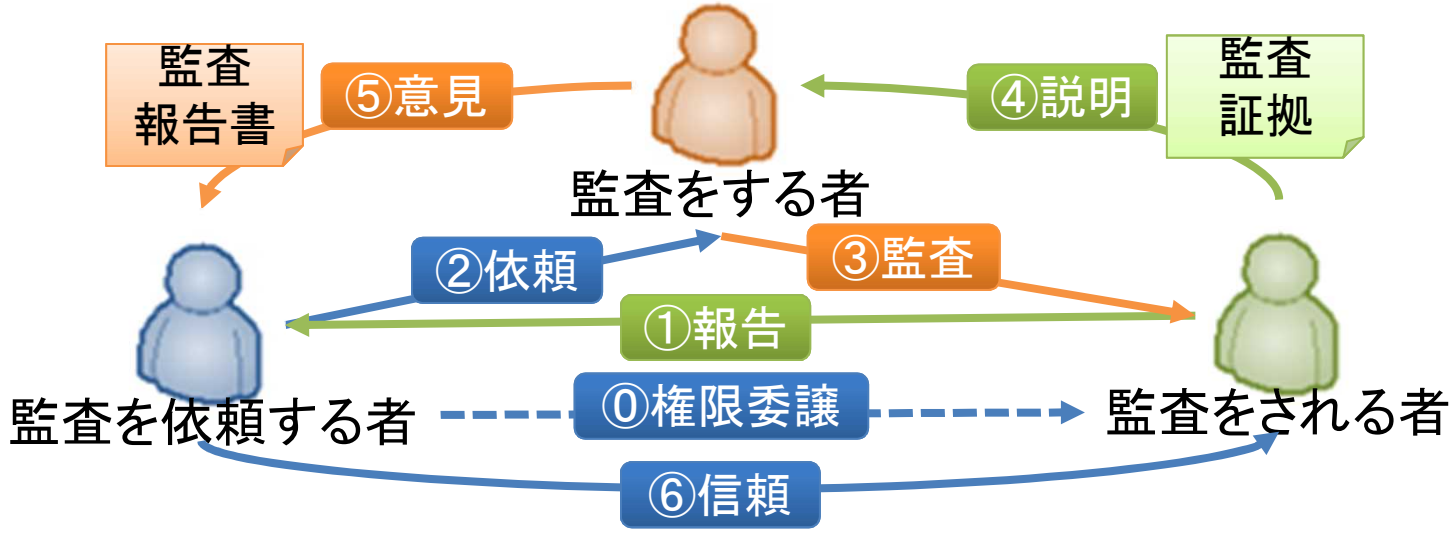
保証型システム監査の概要と特定個人情報保護評価書を活用した
保証型システム監査の可能性について考察します

Ⅱ．保証型システム監査の概要

1. 監査とは？
2. 新システム監査基準におけるシステム監査の定義と目的
3. 旧システム監査基準が示す保証型システム監査と助言型システム監査
4. 新システム監査基準が示す保証型システム監査と助言型システム監査
5. 保証型システム監査における言明書
6. 保証型システム監査における監査報告書
7. 保証型システム監査のニーズ
8. 保証型システム監査の四分類について
9. 経営者主導方式
10. 委託者主導方式
11. 受託者主導方式
12. 社会主導方式
13. 保証型システム監査の実施手順

Ⅱ-1. 監査とは？

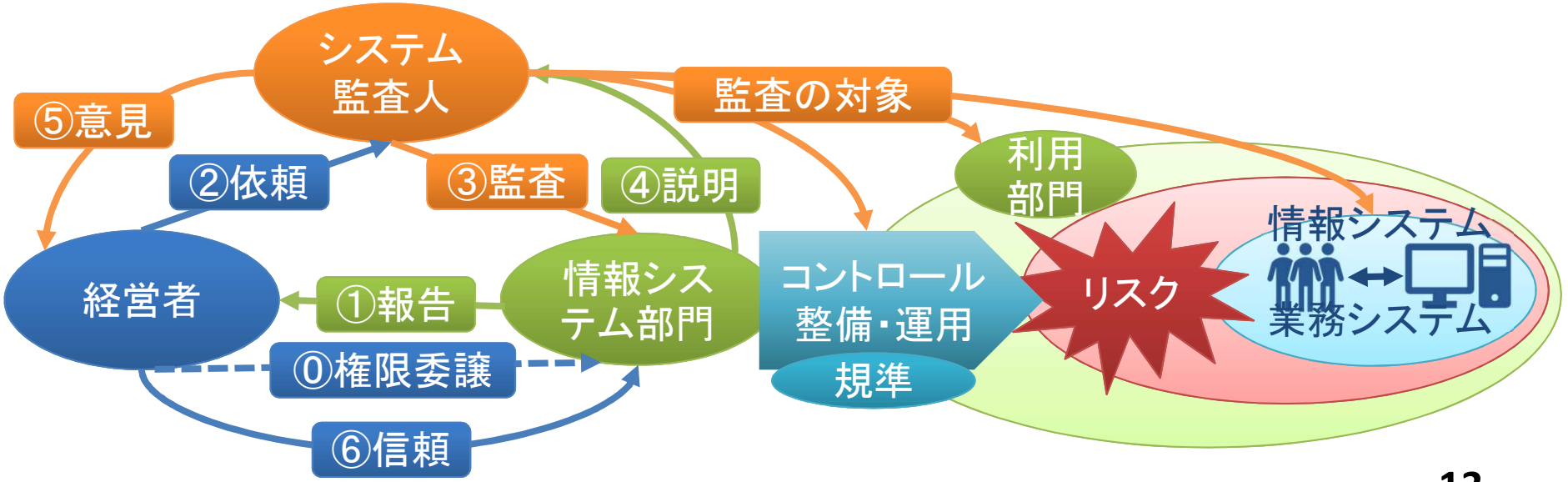
- 監査の三者関係
  - ✓ 監査は、監査を依頼する者（依頼者）、監査をされる者（被監査組織）、監査をするもの（監査人）の三者があって初めて成立する。
  - ✓ 三者はお互いに独立しており、その役割を兼ねることは出来ない。
  - ✓ 監査とは、監査人が依頼者の要請に応じ、監査対象について情報を収集分析し評価した結果をもとに、独立した第三者の意見として依頼者に報告する行為である。



- そもそも監査は、その行為が保証 でなければならない。
  - ✓ 監査でいう「保証」は、**assurance**であって**guarantee**ではない。
  - ✓ 監査人は、監査報告書の中で**意見表明**という形で保証する。

Ⅱ-2. 新システム監査基準におけるシステム監査の定義と目的

前 文	[1]システム監査の意義と目的
定義	システム監査とは、専門性と客観性を備えたシステム監査人が、一定の基準に基づいて情報システムを総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査の一類型である。
目的	システム監査は、情報システムにまつわるリスク（以下「情報システムリスク」という。）に適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすことを目的とする。



Ⅱ-3. 旧システム監査基準が示す保証型システム監査と助言型システム監査

旧システム監査基準　Ⅰ．前文より抜粋

	組織内部の利害	組織外部の利害
背景	情報システムは、経営戦略を実現するための組織体の重要なインフラストラクチャとなっている。	情報システムがネットワーク化されることにより、社会の重要なインフラストラクチャとなって来ている。
課題	リスクを適切にコントロールすることが組織体における重要な経営課題となっている。	情報システムに係わる利害関係者は、組織体内にとどまらず、社会へと広がっている。
効果	システム監査の実施は、組織体のITガバナンスの実現に寄与することができる。	システム監査の実施は、利害関係者に対する説明責任を果たすことにつながる。
目的	情報システムが、組織体の経営方針及び戦略目標の実現に寄与するため。	情報システムが、外部に報告する情報の信頼性を保つように機能するため。
手段	情報システムの改善のための助言を行うことを目的とした監査も利用できる。	情報システムに保証を付与することを目的とした監査であっても利用出来る。

	助言型	保証型
目的	助言型監査は主に組織内部の改善目的として定義された。判断規準に照らし問題点を指摘し改善を促す。	保証型監査は主に利害関係者を守るため、もしくは判断の材料として定義された。判断規準に照らし適切であることを保証する。
言明書	必ずしも必要ではない	必要
監査意見	改善勧告、助言等	保証意見（肯定意見・否定意見）

当初はIT統制の成熟度が低く、保証型が難しかったため
助言型が主になっていたと考えられる。

Ⅱ-4. 新システム監査基準が示す保証型システム監査と助言型システム監査

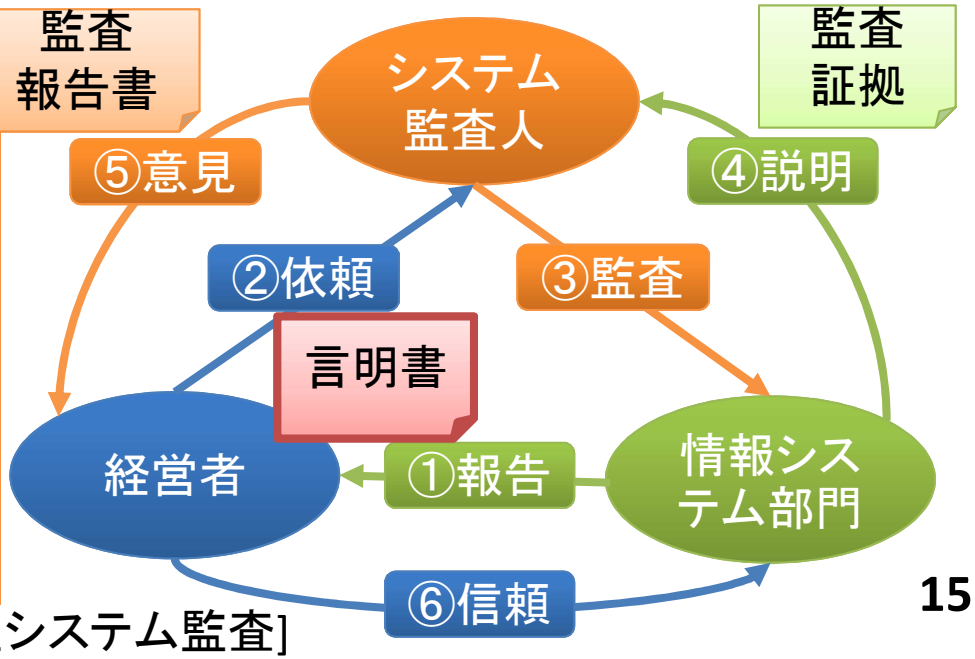
新システム監査基準 【基準3】[解釈指針]1.より抜粋

1.(1)	例えば、次のようなニーズに基づいて、システム監査の目的が決定される。
①保証を目的とした	経営陣が、取引先等からの信頼を得るために、経営者による**言明書**の範囲内で、自組織の情報システムのマネジメントが有効に機能していることのお墨付きを得たいというニーズをもっている場合、「システム管理基準」に照らして情報システムのマネジメントの状況を評価・検証しもって保証を目的としたシステム監査が行われる。
②助言を目的とした	経営陣が、自組織のシステム開発管理に重大な不備があるのではないかと不安に思っており、もし不備があればそれを指摘してもらい、改善の具体的な方策を知りたいというニーズをもっている場合、「システム管理基準」に照らして現状のシステム開発管理の状況を評価・検証し、指摘事項とともに改善提案を行う、助言を目的としたシステム監査が行われる。

システム監査人による監査意見

【肯定意見】
「監査した範囲で、言明書に記載された内容は妥当である」
と肯定する意見表明

【否定意見】
「監査した結果、言明書に指摘事項がある」
と否定する意見表明



[保証型システム監査]

Ⅱ-5. 保証型システム監査における言明書

- 組織のIT統制状況に関する自己評価を表明したもの
  - ✓ 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。

○○○システムの情報セキュリティ管理に関する言明書（サンプル）		
○○○○○　殿 20○○年○○月○○日　責任者名		
言明文	当社は、○○○の基準に準拠した○○○をもとに、下記の範囲で○○○システムの情報セキュリティ管理について適切な管理策を整備、実施している。	
対象システムに関して整備、実施している管理策		
統制内容	1. 情報セキュリティ管理ルールを策定している	(1)情報システム部門長は、サイバー攻撃への対処策を策定している。 →証拠
	2. アクセス管理を行っている	(1)運用管理者は、○○○データへのアクセスコントロール及びモニタリングを、実施している。 (2)運用管理者は、・・・を行っている。 →証拠
	3. ログ管理を行っている	(1)運用管理者は、○○○ログを取得し、定期的に分析している。 →証拠

Ⅱ-6. 保証型システムにおける監査報告書

- 監査意見の対象は、言明された内容である。
  - ✓ 保証の範囲は、①依頼者との合意に基づき、②監査の対象、③判断の尺度、④監査の目的、⑤監査した期間、⑥監査した結果の範囲に限定される。監査意見は、未来の事象や状態を保証するものではない。

システム監査報告書（サンプル）

監査意見

我々は、①貴社との依頼内容の合意に基づき、独立した第三者でありかつ専門家であるシステム監査人として、貴社から提示された②言明書を対象とし、③〇〇〇を判断の規準としてシステム監査を実施した。当監査の目的は、提示された④言明書の妥当性について監査し、監査意見を表明することにある。

我々の意見としては、⑤20xx年xx月xx日～20xx年xx月xx日の本社〇〇〇システムの情報セキュリティ管理について下記の⑥監査した結果により、「言明書」の事項は、言明されたとおり整備、運用されており妥当であると認める。

実施した監査手続きと監査結果

項番	統制項目	言明された管理策	実施した監査手続き	指摘
1	（省略）	（省略）	（省略）	―
2	ログ管理を行っている	(1)運用管理者は、〇〇〇ログを取得し、定期的に分析している。	インタビュー 実施記録閲覧	無し

言明された内容を保証している

Ⅱ-7．保証型システム監査のニーズ

- 利害関係者及び依頼者の視点から見たニーズ
  - ✓ 保証型監査のニーズを利害関係者及び依頼者の視点で分類すると、以下の4つが考えられる。

利害関係者	依頼者	保証型システム監査のニーズ
①経営者のニーズ	経営者	情報システム部門からの報告の妥当性を外部評価によって担保したい、保証というお墨付きをもらって安心したい。
②委託者のニーズ	委託者	受託者の管理レベルによって大きな損害を被る可能性があり、その管理レベルが自社の望むレベルであるか判断する材料として、第三者の評価が欲しい。
③受託者のニーズ	受託者	システムを受託するに当たって、委託者が受託者の管理レベルを重視するようになり、受託者の管理は委託者の要求を満たしている旨を宣言したい。
④社会のニーズ	経営者	社会的責任を負う重要インフラや多数の生命・財産に影響を及ぼす分野において、不特定多数の利害関係者に向けて、自組織の管理レベルを判断してもらう材料として公開したい。

ニーズに対応した保証型システム監査のあり方を考える必要がある

Ⅱ-8. 保証型システム監査の四分類について

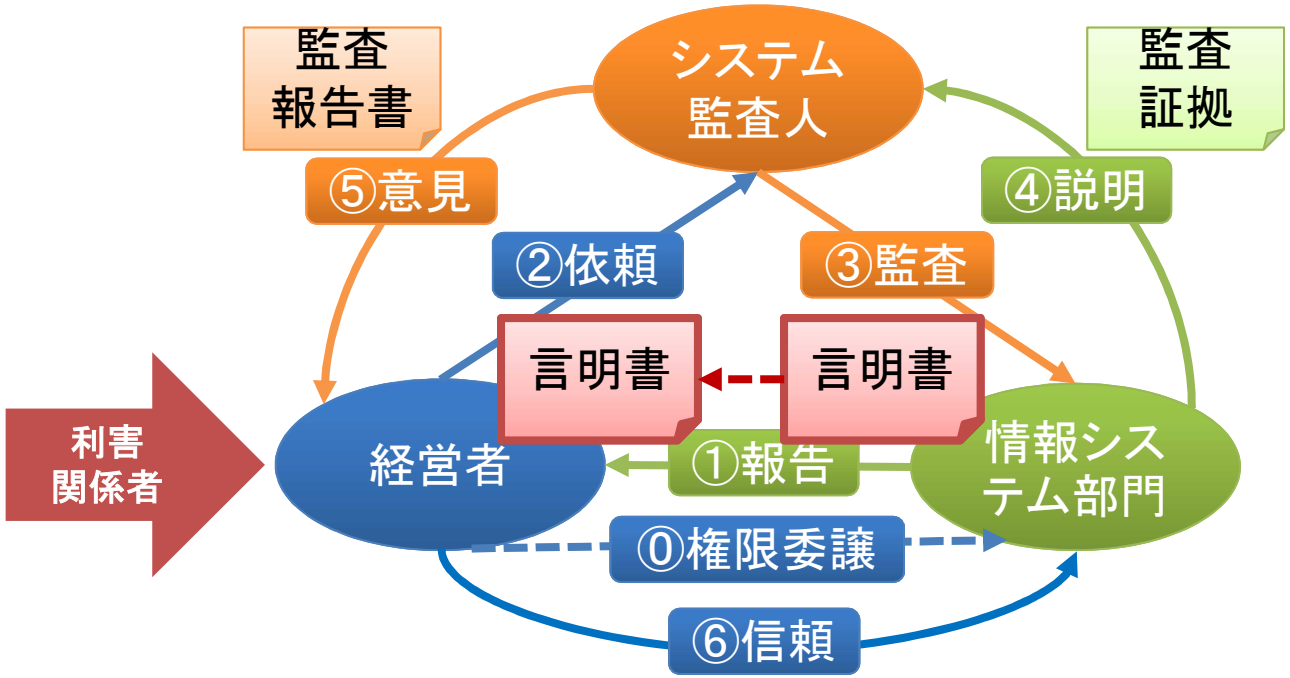
- 依頼者の目的から行った分類
  - ✓ 誰が、何の目的で保証型システム監査を依頼するのかを考えることで、どのような保証型システム監査があり得るのかが明らかにできる。
  - ✓ この視点で分類すると、次の四分類となる。

分 類	依頼者	監査結果の利用目的	言明書作成	被監査組織
①経営者主導方式	経営者	経営者が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情報システム部門が作成する	自組織
②委託者主導方式	委託者	委託者が受託者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
③受託者主導方式	受託者	受託者が委託者の要求する管理レベルを満たしていることを宣言するため	委託者の要求レベルで受託者が作成する	受託者
④社会主導方式	経営者	不特定多数の利害関係者へ、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

各方式によって目的や関係者の役割が異なる

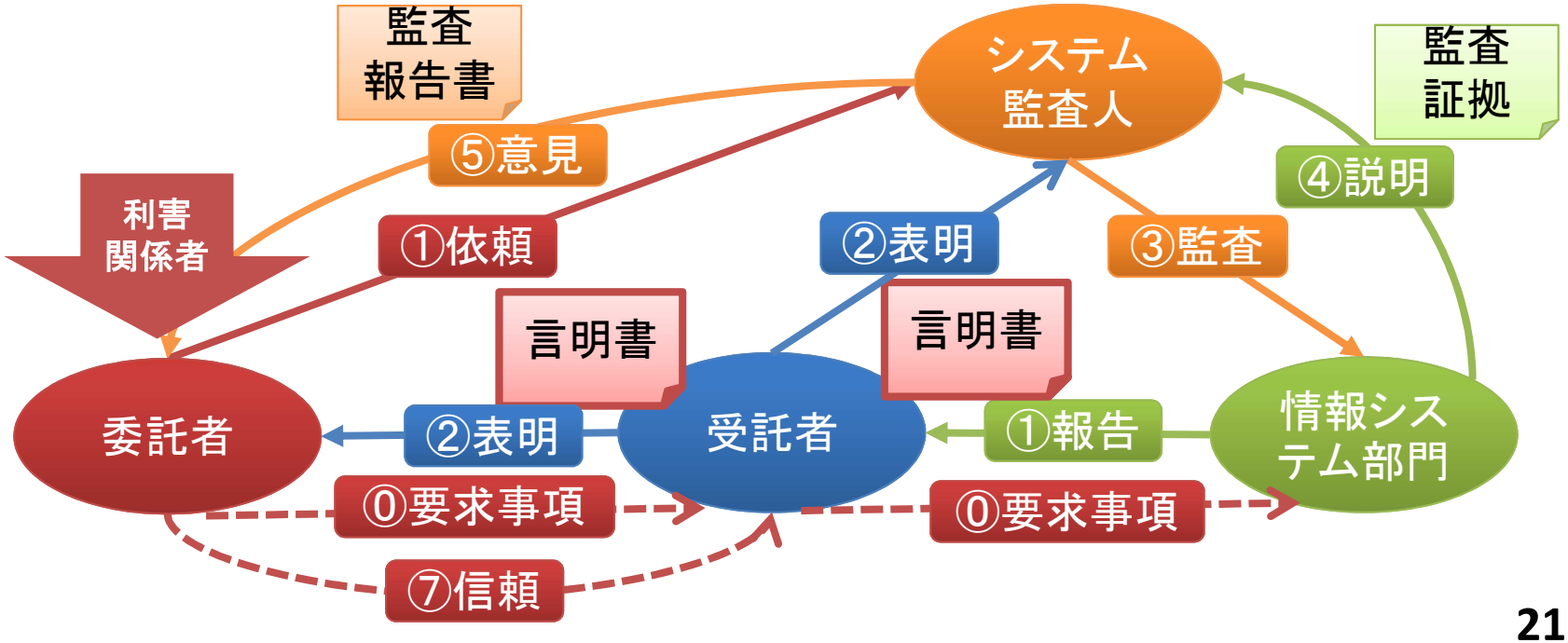
Ⅱ-9. 経営者主導方式

- 経営者が自組織の統制状況を確認するため
  - ✓ 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者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。監査報告書は自組織で利用されるべきものである。



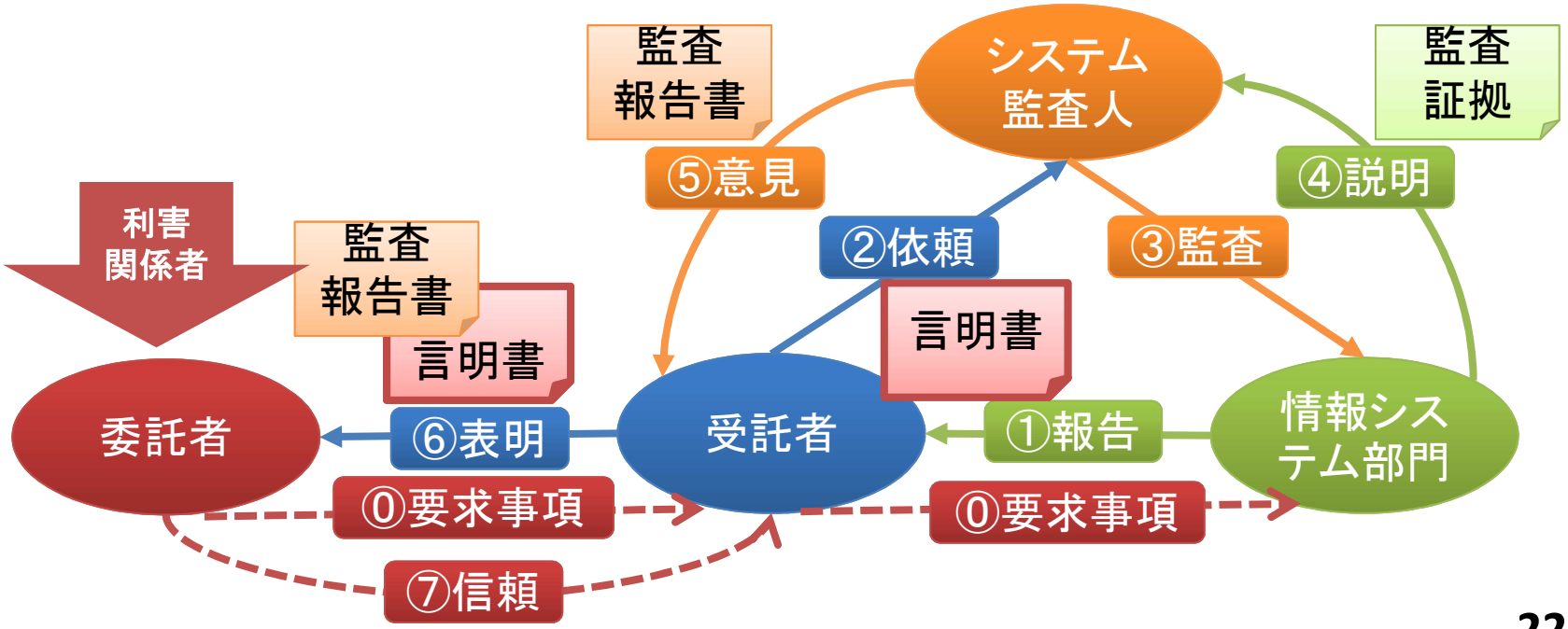
Ⅱ-10. 委託者主導方式

- 委託者が受託者の統制状況を確認するため
  - ✓ 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。



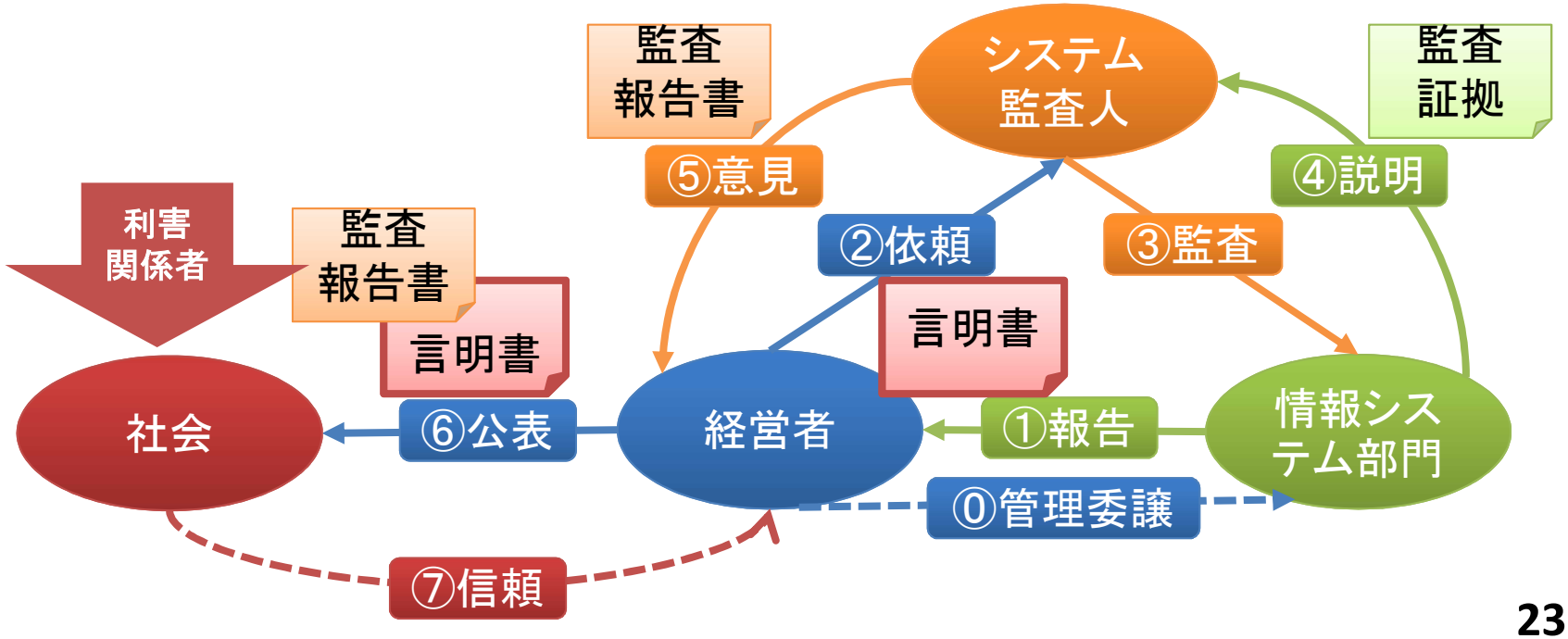
Ⅱ-11. 受託者主導方式

- 受託者が自らの統制状況を委託者へ表明するため
  - ✓ 受託者主導方式とは、受託者が委託者の要求を満たしていることを受託者自身が宣言するために行う監査である。
  - ✓ 受託者は委託者の要求を言明書として表し、委託者と合意を得る必要がある。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。
  - ✓ 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。

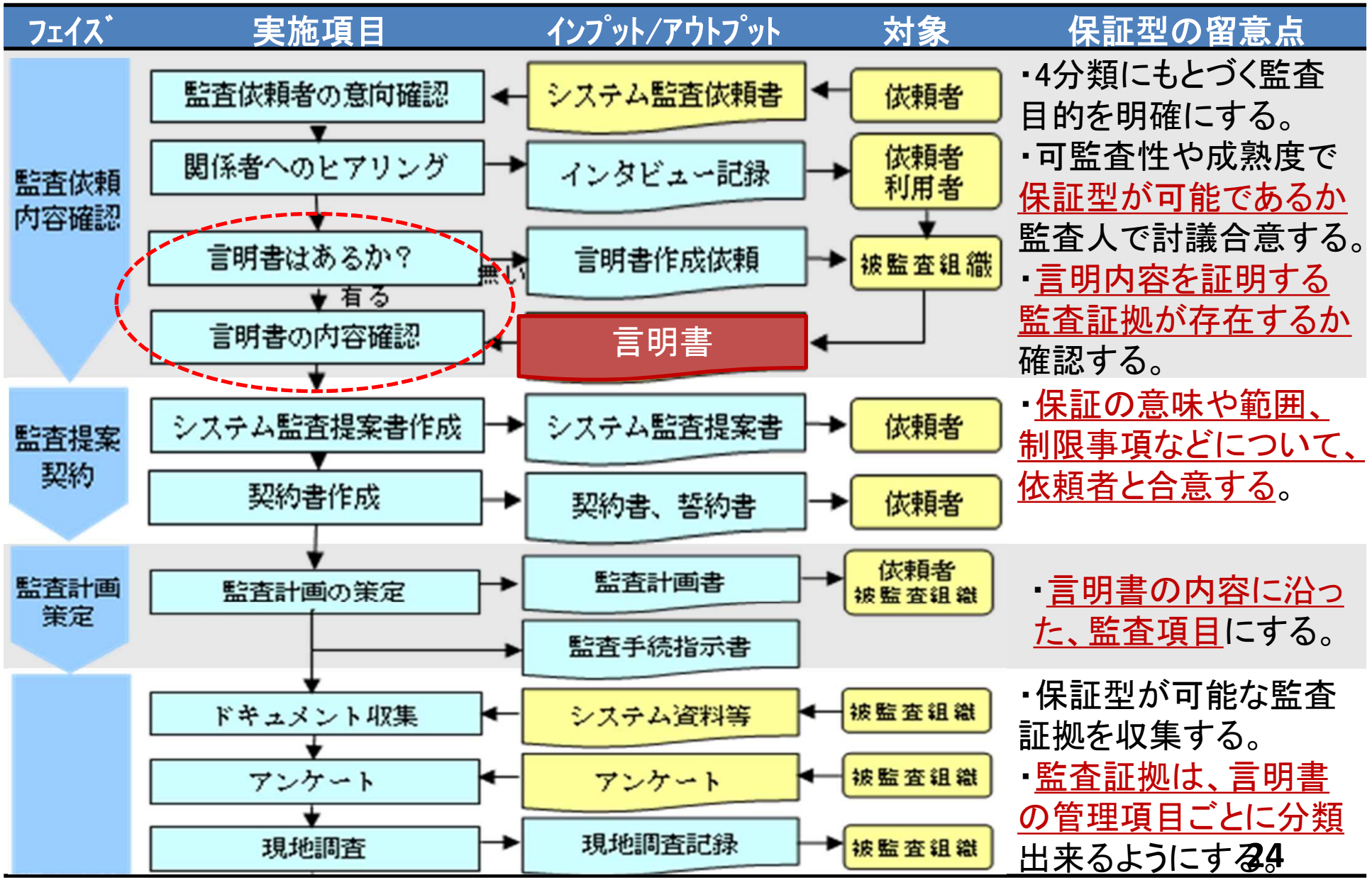


Ⅱ-12. 社会主導方式

- 不特定多数の利害関係者へ説明責任を果たすため
  - ✓ 社会主導方式とは、社会の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表明するために行う監査である。
  - ✓ 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、ホームページ等を利用して、社会に公表されることもある。



Ⅱ-13. 保証型システム監査の実施手順

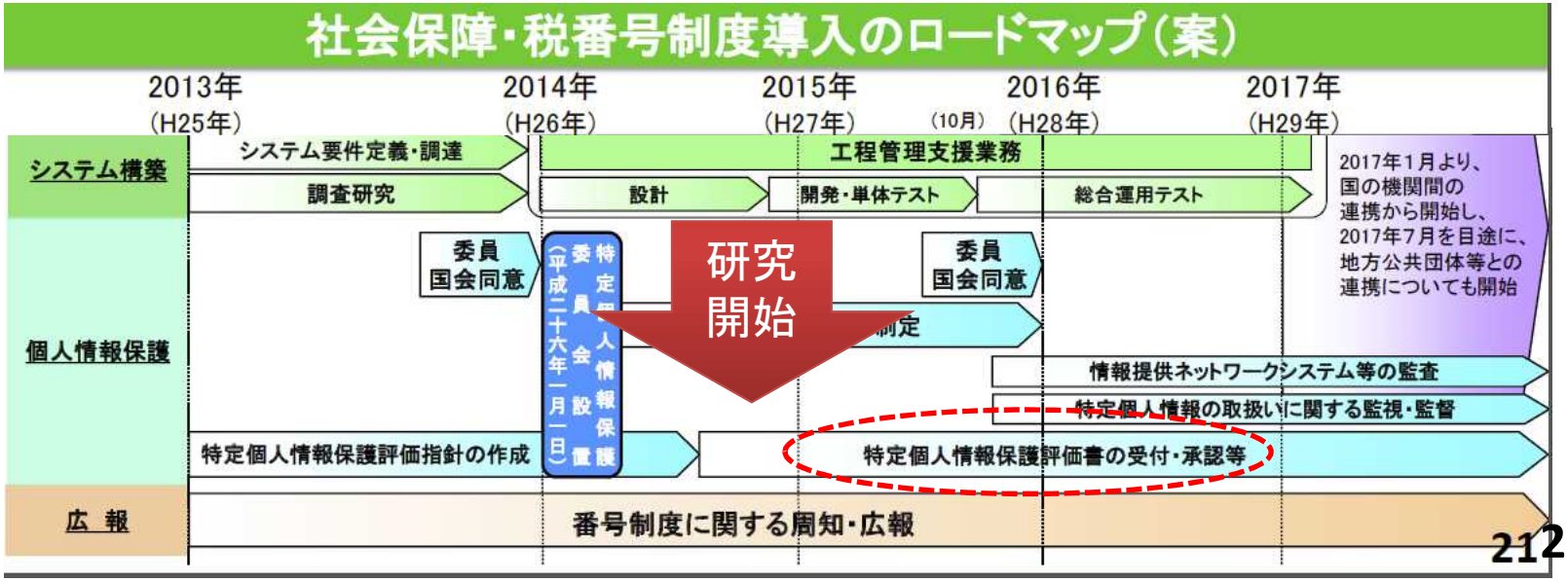


Ⅲ. 特定個人情報保護評価制度での保証型システム監査

1. 特定個人情報保護評価制度が開始された経緯
2. 特定個人情報保護法評価書とは
3. 全項目評価書の構成
4. 公開された管理内容の事例
5. 特定個人情報保護評価制度に関する指針
6. 特定個人情報保護法評価書の公開状況
7. 地方公共団体における保証型システム監査の必要性

Ⅲ-1．特定個人情報保護評価制度が開始された経緯

- この制度は、地方公共団体等において特定個人情報にまつわるリスクを軽減し、国民・住民の信頼の確保することを目的に開始された。
  - ✓ 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た。
  - ✓ 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。実施は義務づけられている。

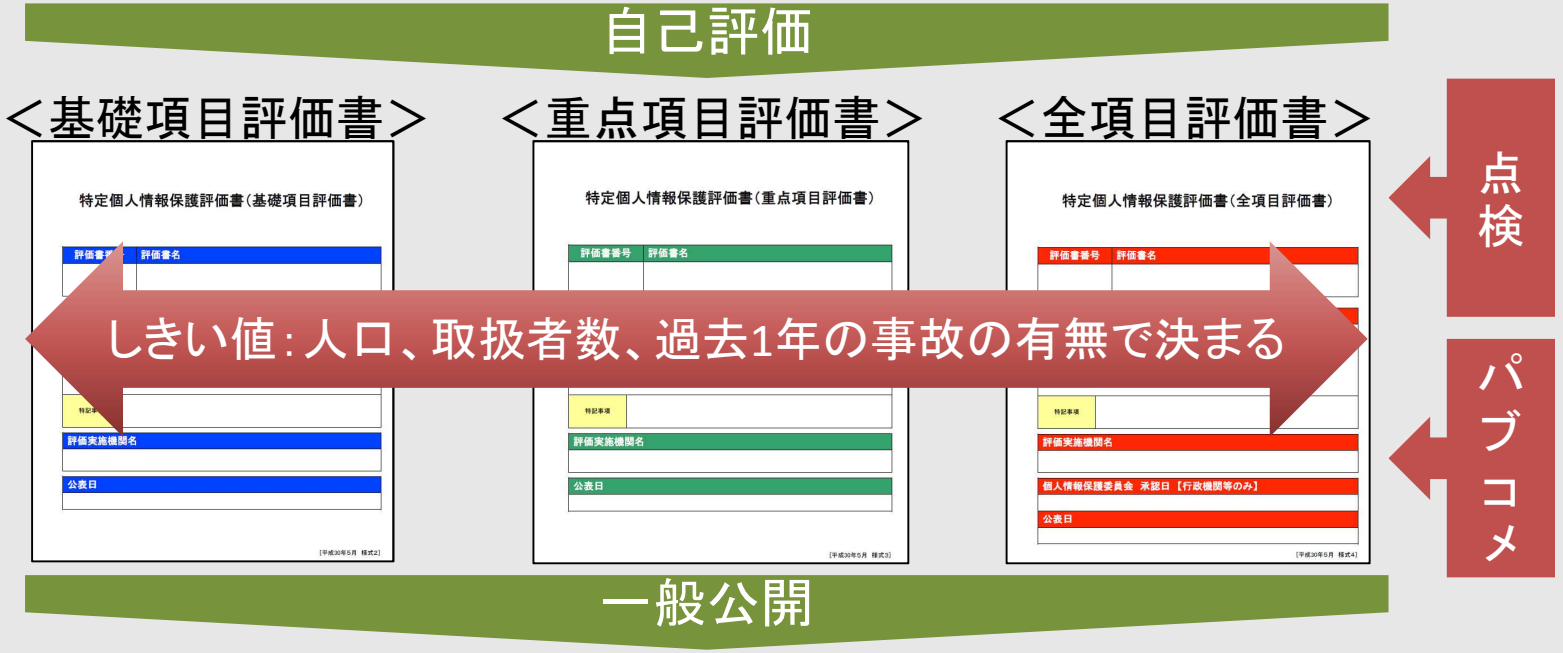


Ⅲ-2. 特定個人情報保護法評価書とは

特定個人情報保護法評価書

地方公共団体等が、特定個人情報にまつわるリスクを自ら分析し、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もの

- 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
- 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
- 「全項目評価書」については、パブリックコメントを求め、指摘があれば対応する
- 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



Ⅲ-3. 全項目評価書の構成

● 評価書は、特定個人情報のライフサイクルに沿って構成されている。

【表紙】個人のプライバシー等の権利利益の保護の宣言、Ⅰ基本情報	
Ⅱ特定個人情報のファイルの概要	Ⅲ　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
1．特定個人情報ファイル名 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取扱いの委託 5．特定個人情報の提供・移転 6．特定個人情報の保管・消去 7．備考	1．特定個人情報ファイル名 2．特定個人情報の入手 3．特定個人情報の使用 4．特定個人情報ファイルの取扱いの委託 5．特定個人情報の提供・移転 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	Ⅴ開示請求、問合せ Ⅵ評価実施手続
1．監査（①自己点検、②監査） 2．従業者に対する教育・啓発 3．その他のリスク対策	

Ⅲ-4. 公開された管理内容の事例

茨木市　約28万人

リスク2： 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		
ユーザ認証の管理	［　行っている　］	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	・指静脈認証による操作者認証を行う。	

神戸市　約153万人

リスク2： 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		
ユーザ認証の管理	［　行っている　］	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	・システムを利用する必要がある職員を特定し、職員証等の操作者個別のICカード及びパスワードによ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、そのユーザがシステム上で利用可能な機能を制限することで不正使用が行えない対策を実施している。 ・パスワードの前回の変更から一定期間経過後に、システムが自動的にパスワード変更を求め、変更しなければ使用できない仕組みとしている。	

相模原市　約72万人

リスク2： 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		
ユーザ認証の管理	［　行っている　］	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	＜住民記録システムにおける措置＞ ・ICカードによる認証を実施しており、認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで不正利用が行えない対策を実施することとする。 ・利用できる端末をシステムで管理することにより、不要な端末からの利用ができないような制限を実施する。また、端末を管理するシステムにアクセスできる権限を制限する。 ・住民記録システムを稼動するLANでは、ファイアウォールにより外部からの侵入を防御する。 ＜共通基盤システムにおける措置＞ ・共通基盤システムでは、ユーザIDによる識別とパスワードによる認証を実施することとしており、、認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、不正利用が行えない対策を実施することとする。 ・共通基盤システムでは、システムの利用できる端末をシステムで管理することにより、不要な端末からの利用ができないような対策を実施することとする。 ・共通基盤システムでは、パスワードの適性のチェック、有効期限の管理を行い、3ヶ月に1度、不適切なパスワードの利用の禁止や有効期限切れのパスワードの失効を実施することとする。	

Ⅲ-5. 特定個人情報保護評価制度に関する指針等

個人情報保護委員会　特定個人情報保護評価　（制度概要）

地方公共団体等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。

https://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(行政機関等･地方公共団体等編)

地方公共団体等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。

https://www.ppc.go.jp/files/pdf/my_number_guideline_gyosei-chihou.pdf

特定個人情報保護評価指針（平成二十六年特定個人情報保護委員会告示第四号）

特定個人情報保護評価制度の意義、実施手続き、審査、承認の過程が記載されている。

https://www.ppc.go.jp/files/pdf/PIA_shishin.pdf

特定個人情報保護評価指針の解説

問合せの多い事項について、事務局が回答した事例等のうち、参考となる要旨を記載したもの。実際の記載要領が、別添付１～別添付４まで公開されている

https://www.ppc.go.jp/files/pdf/kaisetsu_shishin.pdf

別添５：特定個人情報保護評価指針第10（２）に定める審査の観点の主な考慮事項

個人情報保護委員会が審査する際の、適合性及び妥当性の2つについて、審査の観点における主な考慮事項を記載している

必要条件　十分条件

https://www.ppc.go.jp/files/pdf/kaisetsu_shishin.pdf

Ⅲ-6. 特定個人情報保護法評価書の公開状況

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（個人情報保護委員会）

マイナンバー保護評価WEBにおいて公表されている機関数及び評価書数は次表のとおり。
2018年6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565件に及んでいる。

（平成30年6月30日現在）

機関情報		評価書情報			
公表者区分	公表機関数	評価書数	評価書種別		
			基礎	重点	全項目
行政機関の長	8 機関	16	8	0	8
地方公共団体の長その他の機関	2,190 機関	31,471	29,494	1,412	565
独立行政法人等	26 機関	32	24	1	7
地方独立行政法人	1 機関	1	1	0	0
地方公共団体情報システム機構	1 機関	1	0	0	1
情報連携を行う事業者	636 機関	835	707	48	80
合計	2,862 機関	32,356	30,234	1,461	661

https://www.ppc.go.jp/mynumber/information/2018/20180705/

- 個人情報保護委員会　マイナンバー保護評価WEB（公表された評価書を検索）

https://www.ppc.go.jp/mynumber/evaluationSearch/

Ⅲ-7．地方公共団体における保証型システム監査の必要性

- 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。

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（総務省）

✓ 助言型監査と保証型監査について次の記述がある。

- 「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、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。

http://www.soumu.go.jp/main_content/000348657.pdf

地方公共団体で保証型システム監査の実施が求められている

Ⅳ. 特定個人情報保護評価書を用いた保証型システム監査

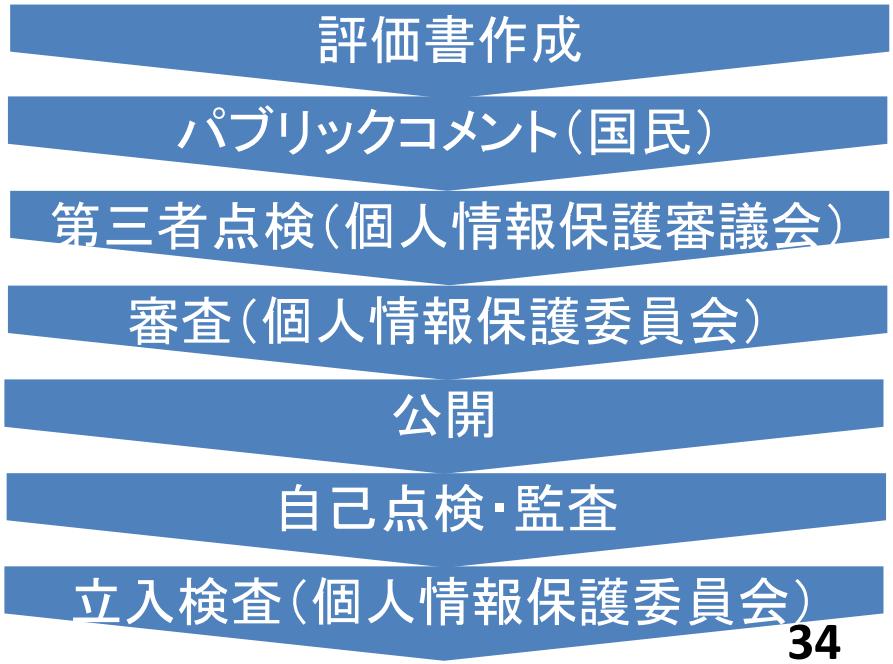
1. 評価書を用いた保証型システム監査の目的
2. 評価書を言明書と見なす方法
3. 地方公共団体向け保証型システム監査の関係者
4. K市の評価書に対するパブリックコメント
5. 評価書記載のポイント
6. 特定個人情報保護に関する管理規準（案）
7. 評価書を用いた保証型システム監査のフロー
8. 依頼内容確認フェーズのポイント
9. 監査提案・契約フェーズのポイント
10. 監査計画・調査実施フェーズのポイント
11. 検出事項分析フェーズのポイント
12. 監査報告フェーズのポイント
13. 評価書を活用した保証型システム監査の必要性

Ⅳ-1．評価書を用いた保証型システム監査の目的

- 地方公共団体の説明責任とは？
  - ✓ 地方公共団体は、特定個人情報の照会・提供を情報提供ネットワークシステムを通じて行っている。
  - ✓ 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。
  - ✓ 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ることにより説明責任を担保することに繋がる。

個人情報保護委員会への報告が義務付けられる場合である「重大な事態」とは、漏えいした特定個人情報に係る本人の数が100人を超える事態をいう

＜定期的な立入検査＞
- 平成28年度計画5件
- 平成29年度計画8件
- 平成30年度計画50件



Ⅳ-2. 評価書を言明書と見なす方法

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]

リスク2：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			
ユーザ認証の管理	［　行っている　］	＜選択肢＞ 1）行っている	2）行っていない
具体的な管理方法	・システムを利用する必要がある職員を特定し、職員証等の操作者個別のICカード及びパスワードによ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、そのユーザがシステム上で利用可能な機能を制限することで不正使用が行えない対策を実施している。 ・パスワードの前回の変更から一定期間経過後に、システムが自動的にパスワード変更を求め、変更しなければ使用できない仕組みとしている。		
アクセス権限の発効・失効の管理	［　行っている　］	＜選択肢＞ 1）行っている	2）行っていない
具体的な管理方法	職員異動等で権限の発効・失効の必要が生じた場合、所属長よりシステムを管理する所属に申請を行い、システムを管理する所属の所属長の決裁を経て、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	［　行っている　］	＜選択肢＞ 1）行っている	2）行っていない
具体的な管理方法	・アクセス権限表のファイルを直接システムに読み込み、アクセス権限及び操作権限の更新を行う自動処理を組み込むことにより、管理しているアクセス権限と、システムに登録されている権限が一致するようにしている。 ・異動が生じた場合には速やかに手続きを行うよう運用マニュアルに定めるとともに、不要なアクセス権限が付与されていないか、所属長が定期的にチェックを行っている。		
特定個人情報の使用の記録	［　記録を残している　］	＜選択肢＞ 1）記録を残している	2）記録を残していない
具体的な方法	・システムで特定個人情報が表示される画面を表示した際に、日時、対象者、操作者の記録を磁気ディスクに保存している。保存された記録は、一定期間保管している。 ・記録された情報を元に、定期的に内部監査を行っている。		
その他の措置の内容	－		
リスクへの対策は十分か	［　十分である　］	＜選択肢＞ 1）特に力を入れている 3）課題が残されている	2）十分である

＜言明書＞

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	

言明

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	神戸市　住民基本台帳事務　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

神戸市は，住民基本台帳事務における特定個人情報ファイルの取扱いにあたり，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

神戸市長

特定個人情報保護委員会　承認日【行政機関等のみ】

公

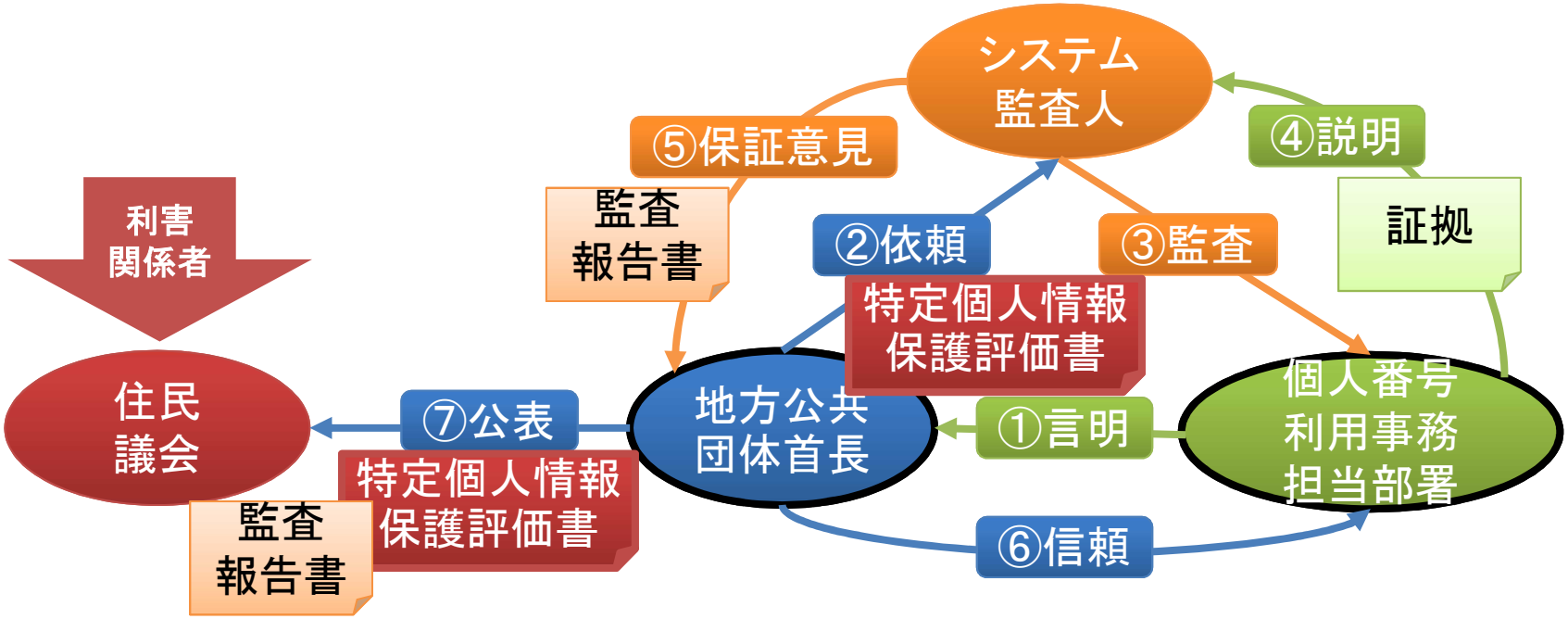
［平成26年4月　様式4］

言明

組織の長

Ⅳ-3. 地方公共団体向け保証型システム監査の関係者

- 地域社会への説明責任を担保するため
  - 保証型システム監査には4つの分類がある事を述べたが、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（個人番号利用事務担当部署）・システム監査人の三者の役割を整理した図を示す。



当初公開された評価書には、記載に問題のあるものも見られた。

Ⅳ-4. 神戸市の評価書に対するパブリックコメント

- 神戸市のパブリックコメントに応募
  - 神戸市の住民基本台帳に関する全項目評価書について、保証型システム監査研究会（i研）のメンバーで意見提出を行った。

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	
対象	•「特定個人情報保護評価書（全項目評価書）」
案の公示日～意見受付締切日	公示日：2014年12月8日～ 締切日：2015年1月9日
PIA提出意見及び回答	提出意見（111項目）、内採用（58項目）

http://www.city.kobe.lg.jp/information/public/comment/gyoute/060shimin/PIA_ikenbosyukekka.html

該当	意見	意見の理由	意見に対する回答	
Ⅲ-7-リスク1-⑤ 物理的対策	耐震対策についても記述する。	地震対策についての記述が無いため。	修正を加えます。「サーバを格納しているラックには、耐震補強を実施している。」	○
	「・バックアップ媒体は，施錠できる保管庫に保管している。」・・・＞施錠以外に、遠隔地保管を考慮していない	コンピュータ・センターと同一場所にバックアップ媒体を保管していると、共倒れになるリスクがある	下記のとおり修正を加えます。「バックアップ媒体は、耐震・耐火機能を満たした区画に設置した保管庫に保管するほか、遠隔地での保管も実施している。」	○

管理策に対する指摘と改善提案を行った

Ⅳ-5. 評価書記載のポイント

全項目評価書記載ポイント集

公開されている特定個人情報保護評価書の中から全項目評価書について、各自治体が実際に作成・更新する際のヒントになる指摘事項をとりまとめた。改善点や記載事例についても併せて提示している。

- 記載ポイント集 - Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策
- 記載ポイント集 - Ⅳその他のリスク対策

http://j-aisa.jp/research/27/

特定個人情報保護評価書(全項目評価書)記載ポイント集 - Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策

全項目評価書の記載ポイント集(2016. 1. 16改訂)

特定個人情報保護評価書(全項目評価書)			審査の観点					
	項目名	記載要領 別添4	審査の番号			考慮事項	指摘事項	改善点／事例
	1.特定個人情報ファイル名	・このシートで記載する特定個人情報ファイルの名称を記載してください。リスク対策が共通する複数の特定個人情報 ファイルについてまとめて記載することができます。その場合は、このシートで記載する全ての特定個人情報ファイルの 名称を記載してください。 ・その際、「I 3.特定個人情報ファイル名」で記載した通し番号とともに記載してください。	(9) (10) (11)			特定個人情報ファイルを取り扱うプロセスにおいて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、特定個人情報保護評価の対象となる事務の実態に基づき、特定しているか。 特定されたリスクを軽減するために講ずべき措置についての記載は具体的か。 記載されたリスクを軽減させるための措置は、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・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	評価書に安全対策用語のみが記載され、具体的内容の記載が求められているが、具体的な記述がされていないものがある。 リスクに対する措置の内容について、リスクを防止するためのコントロールが正しく書けていない場合がある。(努力目標を記載している事例がある)	主語を明確にし、具体的な対応を記述して、市民にもどのような対策が講じられているのか分かるような記述とする。 市町村におけるセキュリティ対策基準やデータ保護管理規程などを盛り込んで、どのような対策を行っているのか、分かり易く記述する。
	2.特	リスク1: 目的外の入手が行われるリスク	(11)	③		特定個人情報の入手について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。		
		対象者以外の情報の入手を防止するための措置の内容	(11)	③	24	評価対象の事務を遂行する上で必要な者以外の者の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。	直接入手のみを記述し、他市町村からの入手について言及していない場合がある。 「防止に努める」などの事例では、防止対策が十分であると判断することが出来ない。 「対象者以外の入手が出来ない仕組みとなっている」などの記載事例があり、具体的な記述となっていない。	住民からの入手、他部署からの入手、他市町村からの入手(情報提供ネットワークシステムを介しない入手)など入手方法の違いごとに、対象者以外の情報を入手しないように分けて記述する。 「防止する」等の明確な表現で記述する。 「○○ネットワークからの入手では、対象者以外の情報がシステムでフィルタリングされ、対象者のみの情報が受け渡される仕組みとなっている」等、具体的な仕組みの内容を記載する。
		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	(11)	③	25	事務を遂行する上で必要な情報以外の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。	直接入手のみを記述し、他市町村からの入手について言及していない場合がある。 「不必要な情報が入手出来ない仕組みとなっている」などの記載事例があり、具体的な記述となって	入手方法ごとに不必要な情報を入手しないように対策を講じる旨を記述する。 「○○ネットワークからの入手では、目的外の項目が除外されて受け渡される仕組みとなっている」等、具体

評価書が言明書として活用できるよう、参考資料として作成した

Ⅳ-6. 特定個人情報保護に関する管理規準（案）

特定個人情報保護のシステム管理規準（案）

本管理規準は、自治体及び地方公共団体（以後、「自治体等」と言う）における「特定個人情報の取扱いプロセスにおけるリスク対策と管理規準」をモデル事例として示したものである。

自治体等においては、本管理規準の基づき、特定個人情報の適正は保護が実施されなければならない。その上で求められるリスク対策が適正に実施されているかどうか、「システム監査」を実施することが重要となる。

http://j-aisa.jp/research/109/

Ⅰ　特定個人情報の取扱いプロセスにおけるリスク対策の管理規準モデル・事例

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）の管理

1.1　目的外の入手が行われるリスク

1.1.1　住民からの届出書等の記載ミスを防止する対策を講じること

・住民異動届出での記載内容のミス防止するため書式、記載方法の見本を提示している。

1.1.2　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こと

・他部署からの入手では、氏名、生年月日、性別を伝え、別人と間違いのないように一意性を確保するとともに、疑問があるときには通知元に必ず確認をしている。

1.1.3　届出から仮入力、照合、確定までのプロセスにおいてのミスを無くす対策を講じること

・届出人が記載した届出書と転出証明書を照合し、一意性が疑問ある時には転出市町村へ問合せや市町村ＣＳでの確認を行う。

1.1.4　住基ネットから目的外の情報が入手できない対策を講じること

適切な統制を整備してもらうよう、参考資料として作成した

Ⅳ-7．評価書を用いた保証型システム監査のフロー

すでに言明書が存在し公開されている前提でスタートする

Ⅳ-8. 依頼内容確認フェーズのポイント

1. 意向確認と事前情報の収集、可監査性の判断まで

①依頼者（組織の責任者）が、特定個人情報保護評価書に対するシステム監査を打診する。

②監査人は、依頼者に保証の意味や範囲、制限事項について説明・確認を行い、合意する。

③監査人は、依頼者に事前インタビューを実施する。

④監査人は、評価書に基づいて監査要点を整理し、言明を担保する証拠の存在を確認する。

⑤監査人は、③及び④から、保証型システム監査が可能であるかチームで討議し合意する。

Ⅳ-9. 監査提案・契約フェーズのポイント

2. システム監査の提案から契約まで

①監査人は、依頼者に監査の内容、範囲（取扱プロセスの全部か、一部か）、実施手順、成果物や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。

②監査人は、依頼者に保証の意味や範囲、監査人の責任限定、監査結果の公開の範囲など制限事項について説明し依頼者と合意を得る。

③①及②を基に契約書を作成する。監査人及び依頼者は、監査契約を締結する。

④監査人は、必要に応じて秘密保持の覚書、倫理規定、宣誓書なども準備する。

Ⅳ-10. 監査計画・調査実施フェーズのポイント

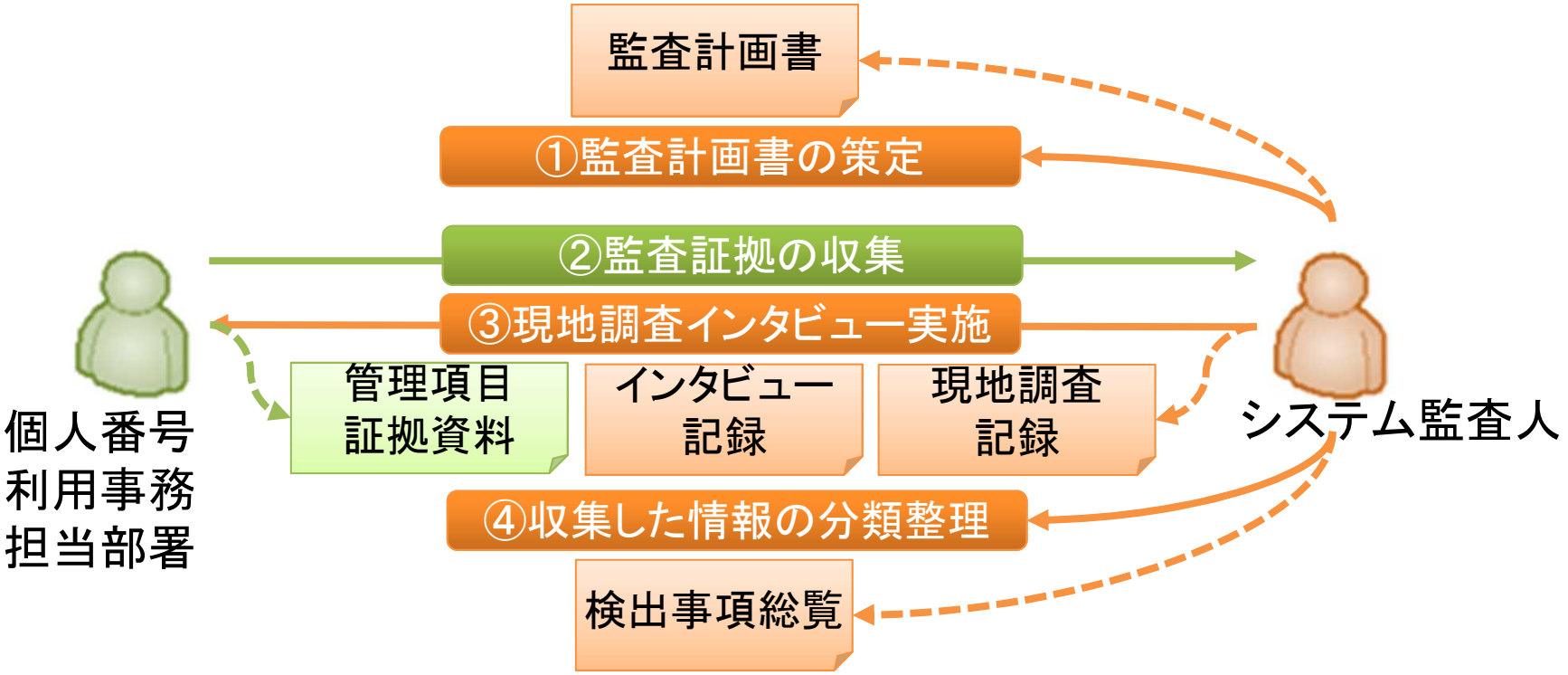
3. システム監査計画の作成から調査実施まで

①監査人は、提案内容及び評価書の内容に沿った監査要点を基に監査計画を策定する。

②監査人は、評価書の管理項目に紐付いた資料を収集する。

③監査人は、現地調査及び被監査部門に対するインタビューを実施する。

④監査人は、②及び③の結果を評価書の監査要点ごとに分類整理する。



Ⅳ-11. 検出事項分析フェーズのポイント

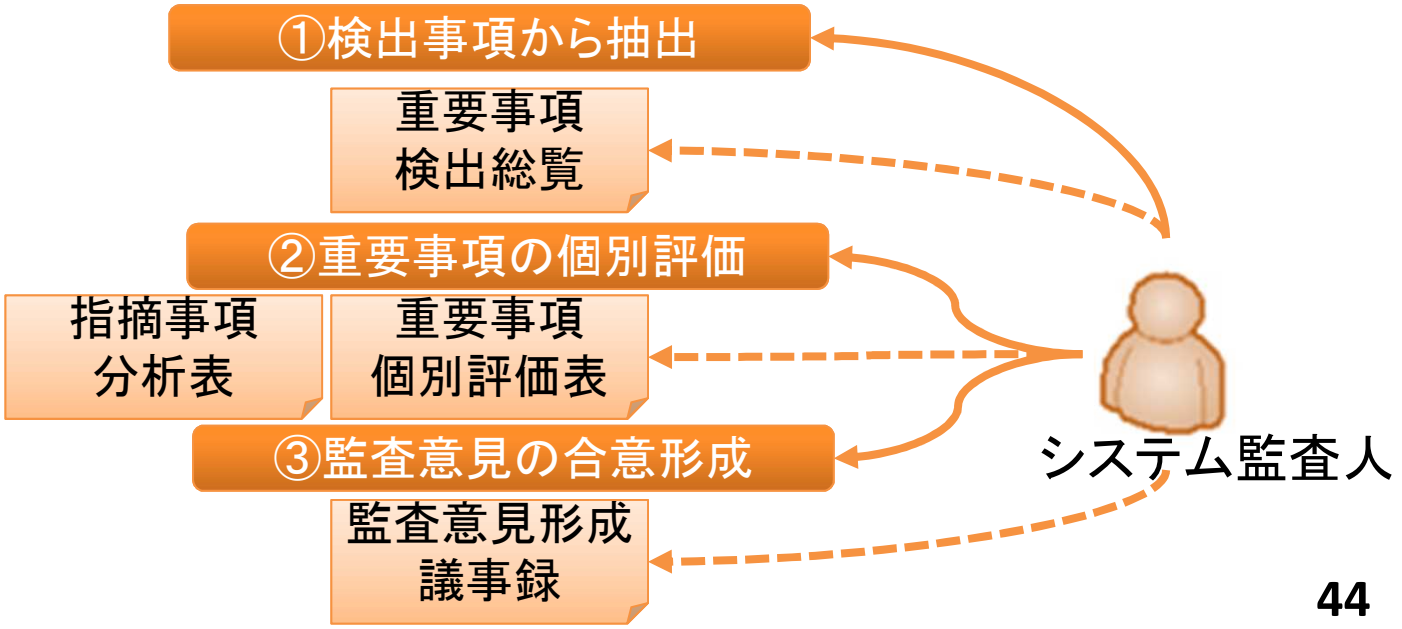
4. 検出事項の分析と監査意見の合意形成

①監査人は、調査実施フェーズでまとめた検出事項から監査目的を基にランク付けを行い監査意見形成に必要な重要事項を抽出する。

②抽出した重要事項について、個別に評価を行う。

③言明書（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。「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。

④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。



Ⅳ-12. 監査報告フェーズのポイント

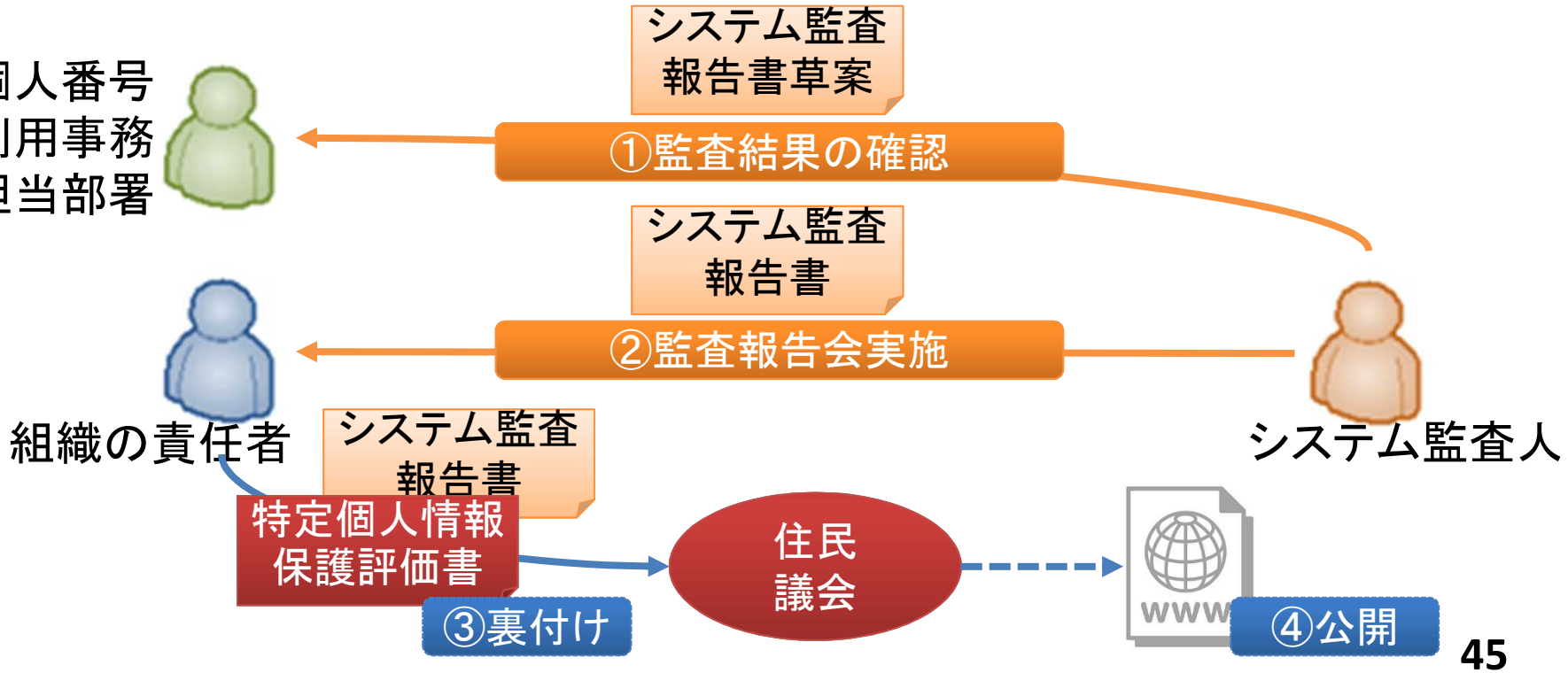
5. 被監査組織との確認から依頼者への報告まで

①監査人は、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。

②監査人は、監査報告会を実施し、システム監査報告書を依頼者に提出、報告する。

③依頼者は、必要に応じ、議会や各種委員会、住民等への説明の裏付けとする。

④依頼者は、場合によってはシステム監査結果をウェッブ等で公開する。



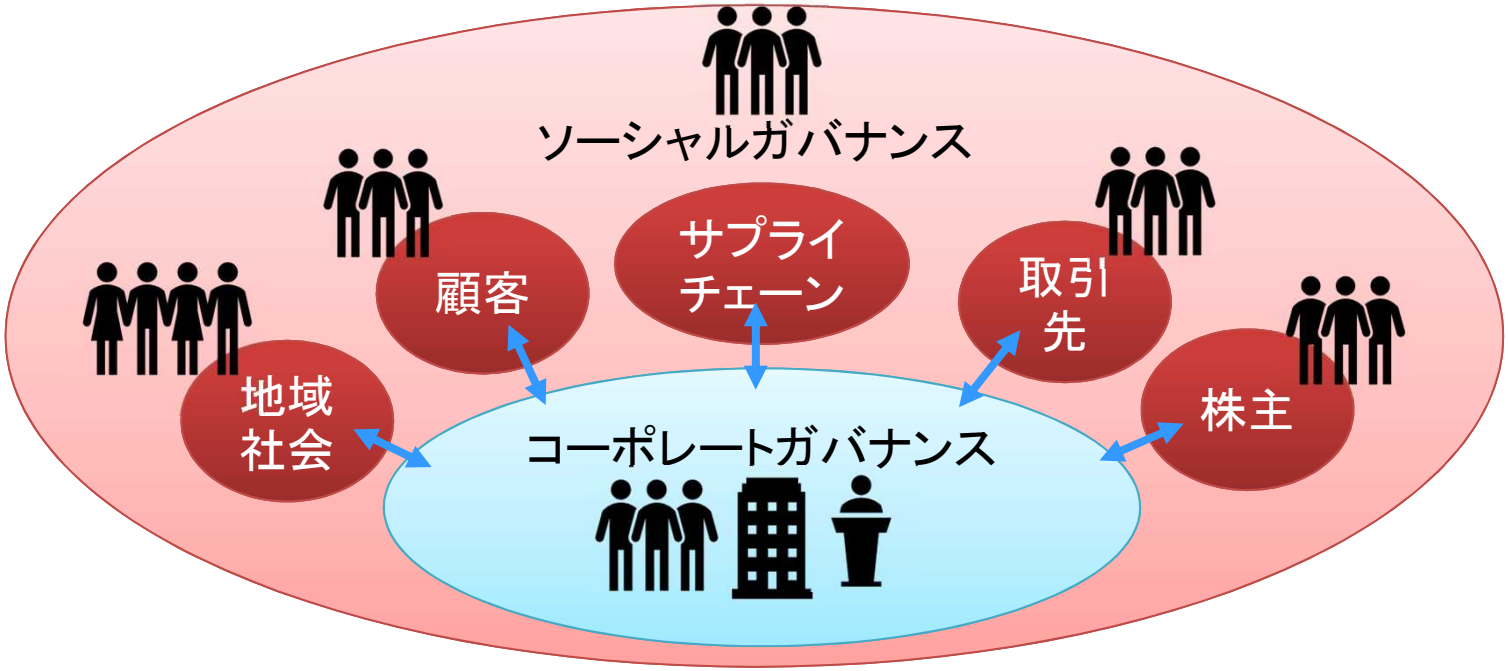
Ⅳ-13. 評価書を活用した保証型システム監査の必要性

● 地方公共団体等におけるシステム監査

- ✓ 多数の地方公共団体で、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ができる。
- ✓ 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。
- ✓ 特定個人情報保護に関する評価書を言明書と見なし、保証型システム監査を実施することは十分可能であると考える。
- ✓ まず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認知してもらうことが今後の課題である。

ソーシャルガバナンス

- 外部評価の重要性について
  - ✓ 組織のコントロールに対する組織内部による評価機能は、一定の改善効果はあるが、限界もある。
  - ✓ 昨今、企業・行政などで様々な不祥事が続くのは、経営に利するという観点が、特定の利害関係者優先、組織の存続、規模拡大、利益重視など、「組織に利する」「経営者に利する」と曲解されることに起因する。
  - ✓ 組織の利害のみでシステム監査を考えるのではなく、様々な利害関係者の視点に立つシステム監査こそ、今後必要とされるのではないだろうか。



【参考文献・リンク】

参考文献・リンク

- SAAJ日本システム監査人協会　近畿支部創設25 周年記念研究大会　論文（2013年07月）
  - 「保証型システム監査を可能にするアプローチ」　松井秀雄、金子力造、小宮弘信、田崎竹雄

http://www.saajk.org/wordpress/wp-content/uploads/saaj_20130706_thesis06.pdf

- JSSAシステム監査学会　設立30周年記念　特別号－第31巻第1号　論文（2018年2月）（※会員限定）
  - 「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」
    小宮弘信、松井秀雄、金子力造、田崎竹雄、浦上豊蔵、藤野正純

https://www.sysaudit.gr.jp/members/ronbun/201803/2017Journal_article_j-aisa.pdf

- 総務省　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

http://www.soumu.go.jp/denshijiti/jyouhou_kansa/index.html

- マイナンバーを適切に取り扱うためのポイント～検査結果を踏まえて～

https://www.ppc.go.jp/files/pdf/mynumber_point.pdf

- 地方公共団体等における監査のためのチェックリスト～マイナンバーの適正な取扱いのために～

https://www.ppc.go.jp/files/pdf/check_list.pdf

- 地方公共団体等における特定個人情報等取扱要領等

https://www.ppc.go.jp/files/pdf/chihou_youryou.pdf

ご清聴ありがとうございました。