保証型システム監査を可能にするアプローチ

発表者：松井秀雄
共著者：金子力造、小宮弘信、田崎竹雄、藤野正純（50 音順）

1. 保証型システム監査とは

1.1 システム監査の分類

システム監査基準（平成１６年改訂版）では、システム監査の目的が次のように定義されている。「システム監査の目的は、組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、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、保証を与えあるいは助言を行い、もってＩＴガバナンスの実現に寄与することにある」

この定義からも明らかなように、システム監査には「保証」を与えるものと「助言」を与えるものの２つのタイプが存在する。 しかし、システム監査の歴史が始まって以来、「助言」を与えるタイプのものが多く実施されてきたが、「保証」を与えるタイプの事例は少ないのが実情である。

1.2 保証型システム監査では何を「保証」するのか

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自体に対して絶対的な保証を与えるような監査意見を表明する事は極めて困難であり、システム監査人にとってリスクが大きいと思われる。

現実解として次のような状況を設定すれば、保証型システム監査が可能と考えられる。

イ．監査対象組織のＩＴ統制状況に関する「言明書」が当該組織の代表者から表明されること

ロ．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

1.3 保証型システム監査の難しさ

イ．「助言型」より強く求められる監査要点の網羅性

助言型システム監査においても改善勧告を行う論点の網羅性は求められるが、「保証意見の表明」という結論から考えると、保証型システム監査の方が網羅性をより強く求められる。

ロ．可監査性と言明書の十分性

まず、被監査主体がシステム監査可能な状態であることが前提となる。

保証型システム監査を行う際に検討対象となる「言明書」の論点が狭小で、監査目的やシステム管理基準等から考えて本来カバーすべき論点の相当部分が欠落していた場

合、十分な論点を具備した「言明書」を被監査組織から提示してもらうよう働きかける必要がある。

ハ．組織規模や業界毎の特性への配慮

一般的に組織規模の大小や業種・業界によってＩＴ統制への取り組みに温度差がある事は周知の事である。システム監査人としては、監査対象組織の組織規模や業界特性に照らし合わせた上で「保証意見」表明の可否を判断する必要がある。ただその際、システム監査人は組織規模や業界特性に応じて判断をした「根拠」を示さなければならない。

二．軽微な瑕疵がある場合の保証意見表明

保証型システム監査を目指して監査を行う過程で、瑕疵が見つかった場合、「保証意見」表明の可否を監査人チーム内で検討する必要がある。その際、瑕疵部分の重要度や影響度を評価・文書化しておき、監査人として説明責任を果たせるように備えなければならない。

1.4　保証型システム監査は誰が行うのか

保証型システム監査では、保証型監査意見が被監査組織の外に向かって使われる事が多い事から、保証意見が「所詮身内の意見」と見なされないよう、組織外の監査人により実施するのが妥当である。

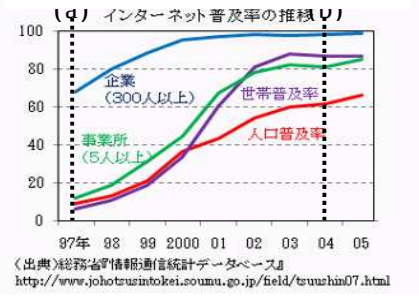
2.　保証型システム監査の必要性とその背景

2.1　保証型システム監査が導入された背景

システム監査基準に「保証型」が導入された主因として、1990 年代以降、情報システムが組織の「内部」及び「外部」に与える影響が急速に拡大したことが背景として上げられる。情報システムは、業務の効率化の為だけではなく、経営戦略を実現するための重要な基盤となった。またインターネット社会の進展で組織間のシステムが相互に依存するようになり、システムのリスクは組織の枠を越え、取引先や顧客、社会全体にまで影響を与えるようになった。これらの要因により情報システムが適切に管理されていることについて、ステークホルダー（広義・狭義）への説明責任がより増大したと言える。システム監査基準は、以上の環境変化を踏まえ 2004 年に改訂された。

[図 1]

※ ｼｽﾃﾑ監査基準は(a)1997 年一部改訂 (b)2004 年に現基準に改訂された



〈出典〉総務省「情報通信統計データベース」
http://www.johotsusintokei.soumu.go.jp/field/tsuushin07.html

2.2　システム監査基準の改訂による保証型監査の位置づけ

現基準では、以下の２つの要素が付加され、前文で２つに分けて表現されている。

イ．組織内部の利害：経営戦略の実現とガバナンスの構築に寄与することを付加し、組織内部の目的を拡大した。

ロ．組織外部の利害：組織外へ与える影響と利害関係者の利害を守るため、又利害関係者が判断の材料として利用することを想定した表現を付加した。

【システム監査基準「Ⅰ．前文」より、抜粋・要約】　　[表 1]

ｲ. 組織内部の利害について	ﾛ. 組織外部の利害について
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。
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も組織体内にとどまらず、社会へと広がっている。
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。
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。
情報システムが、内部規程等に準拠するようにするため。	情報システムが、関連法令、契約に準拠するようにするため。
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であっても利用できる。	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。

助言型監査は主に組織内部の改善目的として、保証型監査は主に組織外部の利害関係者を守るため、もしくは判断の材料として利用することを想定して改訂されたと思われる。

2.3　保証型システム監査のニーズについて

保証型監査を依頼する側の視点でそのニーズを分類すると、以下の４つが考えられる。

イ．経営者のニーズ：システムが経営戦略に合致しているか確認したい、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もしくはPRしたいなどがある。

ロ．システム委託者のニーズ：委託先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などがある。

ハ．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、委託元が委託先の管理レベルを重視するようになり、委託元に自社のシステム管理レベルを判断してもらう材料として開示したいなどがある。

ニ．社会のニーズ：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。

システム監査人としては、依頼者の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。

3. 保証型システム監査と助言型システム監査

3.1 助言型システム監査

助言型システム監査は、被監査組織と監査人が合意した評価基準に基づいて、監査対象の情報システムのコントロール状況について調査を行い、問題がある事項、不十分と思われる事項を検出し、必要に応じてその検出事項に対応した改善勧告を行う監査である。その監査結果は主に内部目的に利用される。

3.2 保証型システム監査

保証型システム監査は、被監査監組織の代表者から提示された言明書の内容に基づき、監査対象である情報システムのコントロール状況が、一定の判断基準により監査手続を実施した限りにおいて適切であることを監査意見として表明する監査である。その監査結果は、内部目的にも利用されるが、主に被監査組織を取り巻く利害関係者向けの外部目的に利用される。

3.3 保証型システム監査の手順

監査の手順について、保証型システム監査と助言型システム監査に大きな違いはなく、判断の尺度となるシステム監査基準、システム管理基準その他の基準なども同じものを使う。しかし、被監査組織のレベルによっては保証型システム監査が成立するとは限らない。このことから、保証型システム監査の手順において、以下のような特徴がある。

・被監査組織の可監査性や成熟度について、保証型システム監査が可能であるかを検討した結果、保証型システム監査は不可能であると判断した場合
→依頼元に対して助言型システム監査の実施を勧奨することもありえる
・可監査性に欠ける、つまり言明書に沿った監査証拠の存在が認められない場合
→整備する時間をとった後に監査を行うことなども検討する
・監査を実施し、検出事項を抽出・分析した結果、監査人の合意意見形成時点で、保証意見を出すことについて最終的に合意を得られなかった場合
→その時点で助言型システム監査に切り替えることもありえる

助言型システム監査と保証型システム監査の主な相違点 [表 2]

	助言型システム監査	保証型システム監査
言明書	必ずしも必要ではない	必要
監査目的	判断規準に照らし問題点を指摘し改善を促す	判断規準に照らし適切であることを保証する
可監査性要求レベル	低い	高い
成熟度レベル	低～中程度で効果的	中～高程度で効果的
報告内容	改善勧告	保証意見

4. 保証型システム監査の分類定義

保証型情報セキュリティ監査では、後述のとおり監査手続きを誰が合意するかによって、３つに分類している。しかしこれらの分類では「誰からの依頼か」、「依頼者の監査目的は何か」など分かり難い所があり、また利害関係者が監査結果を利用する場合だけを想定し、自社内での利用については明記されていない。

そこで誰が、何の目的で依頼するのかを考えると、次の４分類が考えられる。

①経営者主導方式では経営者が自組織の情報システムの管理レベルを把握したい
②委託者主導方式では委託者が委託先の情報システムの管理レベルを把握したい
③受託者主導方式では受託者が委託元に自組織の情報システムの管理レベルを報告したい
④社会主導方式では広く社会に自組織の情報システムの管理レベルを表明したい

また誰が、何の目的で監査をするのかを考える事は、「どこまで保証するのか」、「何を保証するのか」を明らかにする事につながる。①では経営者の要求に対して、自組織の情報システムの管理はどこまで応えられているかを保証。②では委託者の要求に対して、委託先がどこまで応えられているかを保証。③では委託元の要求に対して、受託者側がどこまで応えられているかを保証。④では広く認められた基準に対して、情報システムの管理がどこまで出来ているかを保証することになる。

そこで重要になって来るのが言明書である。それぞれの要求が具体的な管理レベルとして明記され、監査で保証を与えるだけの根拠となる証拠を入手できるような要求事項となっていなければならない。

【保証型システム監査の 4 分類】 [表 3]

分類	依頼者	言明書作成	被監査人	利用者	監査結果の利用目的
①経営者主導方式	経営者	自社が考える独自なレベルで CIO が作成する	自組織	経営者	自社の管理レベルの評価
②委託者主導方式	委託者	委託者の要求レベルで委託先が作成する	委託先	委託者	委託先の管理レベルの評価
③受託者主導方式	受託者	委託者の要求レベルで受託先が作成する	受託先	委託者	委託元へ管理レベルの報告
④社会主導方式	経営者	一般に周知な高レベルの基準で依頼企業が作成する	自組織	社会	一般企業や社会に対して、自社の管理レベルの表明

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、経営者の要求レベル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企業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社内に留め、利用されるべきものである。

②委託者主導方式

委託者主導方式とは委託元の要求に対して、委託先がどの程度対応できているかを監査する方式である。委託先は委託元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。監査人は言明書通りに委託先が対応しているかを監査する。そして監査報告書は委託元が利用する限定的なものである。また委託先が保証型監査を行える状態かどうかを予備調査する必要がある。

③受託者主導方式

受託者主導方式とは委託元の要求に対して、受託先が対応できていることを表明する方式である。受託先は委託元の要求を言明書として表し、委託元と合意を得る必要がある。また委託元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。そして監査人は言明書通りに受託先が対応しているかを監査する。そして監査報告書は委託先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元に対して、二次利用されることも想定される。

④社会主導方式

社会主導方式とは一般企業や市民から信頼を得るために、自社のシステム管理レベルを広く表明する方式である。現状は法定化された基準がないため、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。しかしこの方式を広めていくためには、成熟度レベルを同規模企業と比較して、監査意見を表明したり、特化した部分のみを監査したりと工夫が必要である。

5. 類似するその他の保証型監査

5.1 保証型情報セキュリティ監査

保証型情報セキュリティ監査には①被監査主体合意方式、②利用者合意方式、③社会的合意方式の 3 方式がある。これは監査人が必要な監査手続きを、だれが合意するかによって分類されている。

被監査主体合意方式は実施する監査手続きを被監査主体が合意する方式である。そして利用者が提示した管理手続きが被監査主体において有効に機能しているかどうかを監査する。利用者合意方式は実施する監査手続きを利用者が合意する方式である。データセンターへの運用委託やＡＳＰ利用などの場合、被監査主体の業務の流れや情報システムについての詳細を利用者が分からず、利用者は具体的な要求事項の形で委託先に求める事ができない。そこで被監査主体が具体的な管理手続きを約束することで利用者の期待に応えようとするものである。社会的合意方式は社会的に合意された監査手続きを使用する方式である。この場合は業界などの実務実態を反映した管理手続きを定めることが必要である。

保証型情報セキュリティ監査の分類表 [表 4]

	被監査主体合意方式	利用者合意方式	社会的合意方式
監査手続き	被監査主体の合意 利用者の確認	利用者の合意	社会的に合意
管理手続き	利用者の管理手続き	被監査主体の管理手続き 利用者が合意	社会的に合意された管理手続き
情報セキュリティ・マネジメント	利用者が主導	被監査主体が主導	被監査主体が主導
事例	個人情報の処理など重要な情報の作業を外部委託	データセンター、ASP 利用 一般的な業務委託	電子商取引、 自治体の情報サービス

5.2 委託業務における 18 号監査（日本公認会計士協会監査基準委員会報告書第 18 号）

財務情報に重大な影響を与える業務を外部に委託する場合において、委託会社はその委託業務についても内部統制の有効性を評価する必要がある。このとき委託会社監査人が直接委託業務の内部統制の有効性について監査することは、非常に負荷が高くその業務において他の委託先の重要情報を取り扱っている場合もあり、現実的に困難である。

そこで委託会社監査人は、受託会社に対して、当該業務の内部統制の有効性に関する監査の実施及び監査報告書の作成（18 号報告書）を依頼し入手することで、その報告書を基に評価・監査を実施できる。

受託会社にとっても、個々の顧客企業からの評価・監査を受けなくて済むという負荷軽減のメリットがあるとともに、この報告書を必要に応じて委託先に提供可能であることは、顧客サービスの一つとして有益である。

5.3 Trust サービス

Trust サービスとは、Trust サービスの原則と規準 [注 1] に従い、AICPA/CICA からライセンスを与えられた Trust サービス検証責任者によって実施される検証業務である。

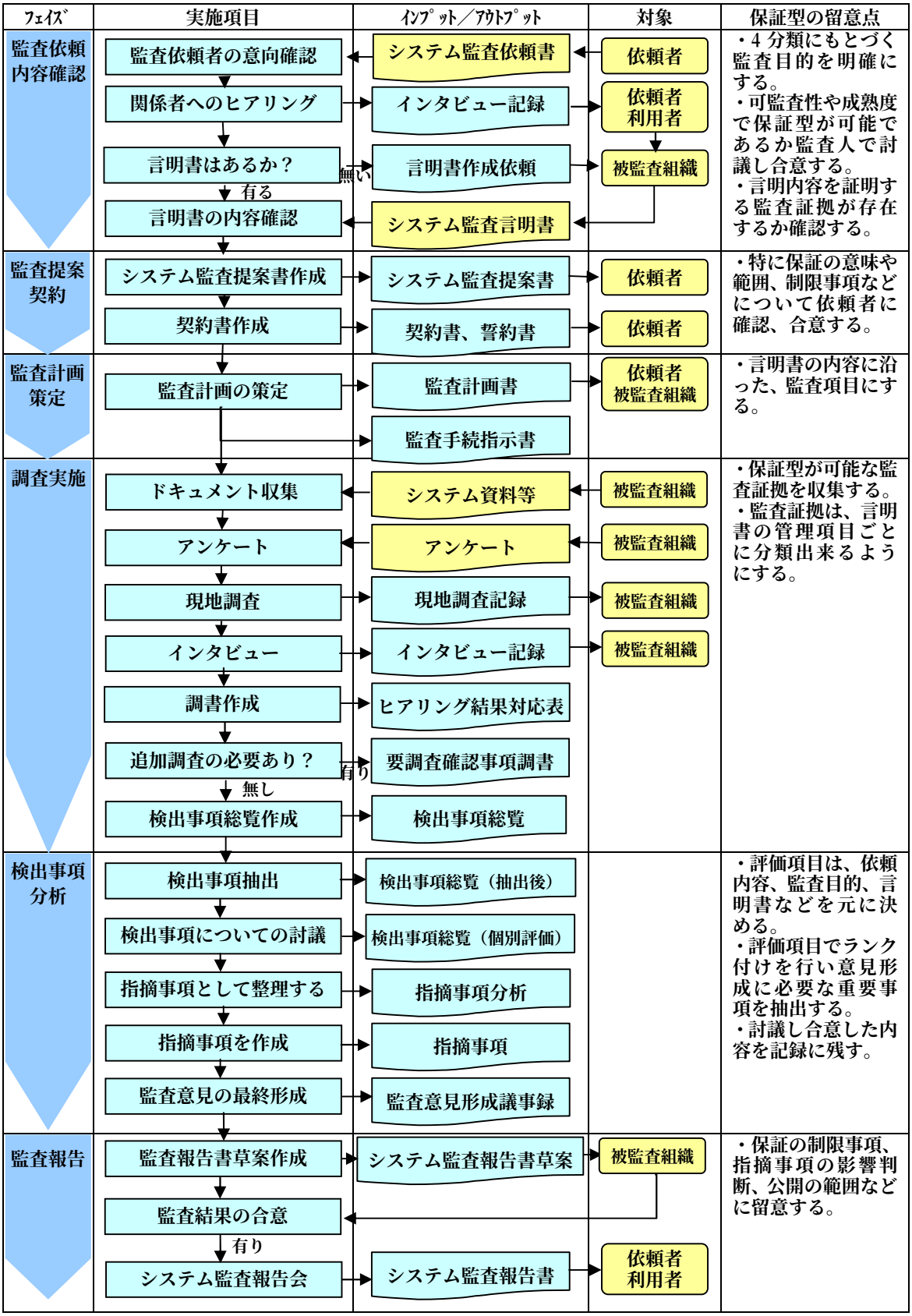
ここに言う検証業務とは、保証基準 [注 2] における「合理的保証」業務をいい、「限定的保証」は採用されない。合意された手続業務及び助言業務を含むので、保証型システム監査より広範囲をカバーし、対象とする内部統制が、情報システムの信頼性等かインターネットを介した電子商取引の安全性かで ”SysTrust ” と “ WebTrust ” という二つの認定シールを持つ。

Trust サービス検証責任者（公認会計士）は、企業の情報システムに採用された内部統制の手続が、経営者の記述書に記載された方針に基づき、かつ、Trust サービスの規準に準拠していることを確かめる。

AICPA/CICA が、原則と規準から検証手続の方法、及び報告書の形式まで一貫して提供し開発しており、経営者は、特定された原則および規準を使用してシステムの信頼性について言明し、同一の規準により Trust サービス検証責任者が検証し保証する。規準に合致しない場合は保証しないので、保証型監査というよりも認証に近い。

6. 保証型システム監査の実施手順

6.1 実施フロー例と保証型の留意点 [図 2]



6.2　監査意見合意形成のプロセス

システム監査人は、以下のようなプロセスで監査証拠の分析を行い、合意することによって保証意見を表明することが可能であると考える。

イ．検出事項総覧の作成

収集した検出事項を言明書の管理項目ごとに整理し、複数の評価項目を設ける。

評価項目及びレベルは、監査テーマ、言明された管理レベル、保証型監査の４分類による目的などを勘案して決める。

ロ．検出事項総覧の抽出

監査人が分担して、それぞれの検出事項の評価項目（重要度、影響度、可能性など）によるランク付けを行い、あらかじめ合意したレベルで問題となる検出事項だけを抽出する。抽出した検出事項それぞれに想定されるリスクと監査人の意見を付加する。

ハ．検出事項についての合意

抽出された検出事項の評価内容、意見について、監査人全員で討議し合意する。

ニ．指摘事項として整理する

合意された検出事項について監査要点ごとに、言明された管理策との関連や問題点、影響の軽微なども含め監査人の意見を付加し指摘事項として取りまとめる。

ホ．監査意見形成

指摘事項について、4 分類に応じた目的と言明書に記載されているレベル及び、組織規模や業界特性を勘案し保証意見が出せるかどうか監査人全員で討議し合意形成を行う。監査意見形成議事録として記録する。

7.　まとめ

これまで実施されたシステム監査では「助言型」が多く、「保証型」は圧倒的に少ない。その理由の一つとして、監査人側に「何を保証するのか？」、「保証を与えた後に瑕疵が判明した場合のリスクを負えるのか？」といった不安がある様に思われる。

当論文は、そこを突破するアプローチとして、こうすれば保証型システム監査を実施できるのではないかという可能性を示すべく、過去に保証型システム監査を経験したメンバー有志 5 名が約 2 年間検討してきた成果を纏めたものである。

数少ない経験事例をもとに検討したものであるため、まだまだ不備な点もあろうかと思われる。　今後諸賢の経験事例や知見が得られれば、改善を図って行きたい。

[注 1] Trust サービスの原則と規準；The AICPA/CICA Trust Services Principles and Criteria

[注 2] 保証基準；International Standards on Assurance Engagements 3000：国際保証業務基準第 3000 号

[添付資料]　言明書のサンプル

【タイプ 1　経営者主導方式　言明書 例】

XXXX システム監査人 殿

平成XX年XX月XX日
株式会社 XXXX 取締役社長 XX XX

当社システム監査対象システムに対するIT統制状況の言明

当社(組織)は、システム監査対象システムに対する下記のIT統制目標を設定し、
手続き文書を制定し、同業同規模の企業に遜色ないレベルで運用している。
なお、監査対象システムは次のシステムである。
① XXXシステム

記

カテゴリー	項　目	統 制 目 標 ＜例＞
システムの開発・保守	開発・保守手続き	適切な開発・保守手続きを定め、周知している
	手続きの遵守	定めた開発・保守手続きどおり実施している
システムの運用・管理	運用手続き	適切な運用手続きを定め、周知している
	手続きの遵守	定めた運用手続きどおり実施している
システムの安全性確保	安全確保の手続き	安全確保のための適切な手続きを定め、周知している
	手続きの遵守	定めた運用手続きどおり実施している
外部委託先管理	外部委託先を選定する手続きを定めている	外部委託先を選定する適切な手続きを定め、周知している
	手続きの遵守	定めた選定手続きどおり実施している

【タイプ２　委託者主導方式　言明書　例】

『X 社様の機密情報を取り扱う受託業務の情報セキュリティ管理手続に関する言明』

○○○　監査人　殿

２０１２年４月２６日
Y株式会社ＣＩＯ
○○○○

当社は、X社様から業務を受託するにあたり、X社様が指定する機密情報を共有することとなる。当社における該当情報の取扱い、管理及び業務全般について、X 社様からの要請事項である「お取引様向け　情報セキュリティ基準」に基づき、以下の通り情報セキュリティ管理策を設定し、実施していることをここに言明する。

情報セキュリティに関する要請事項	実施している情報セキュリティ管理策
情報セキュリティを組織的に進められる体制を構築する。	情報セキュリティ管理についての組織体制を構築している。
	情報セキュリティに関するルールを制定し、文書化している。
	組織内の情報セキュリティ実施項目について、責任者および関連する役割と責任を明確化している。
機密管理が必要な情報を特定し、機密管理に必要な管理ルールを実施する。	X 社が指定した機密情報及びこれを利用して創出した機密情報を明確にしている。
	機密情報の受け渡しに関する管理ルールを制定している。
	職場でのアクセス管理を実施している。
	情報資産の持ち出し、持ち込みに関する管理ルールを制定している。
	IT システムのアクセス管理を実施している。
	IT システム（含む PC）の設置及び廃棄に関する管理ルールを制定している。
	不正プログラムやウイルスに対する管理ルールを制定する。
	事業継続確保のためのバックアップに関する管理ルールを制定する。
機密保持の誓約等、情報漏洩を防止する人的な対策を実施する。	情報セキュリティに関する教育・訓練を実施している。
	従業員等との機密保持誓約を締結している。
情報セキュリティ関連の事故が発生した場合の対応を明確化し実施する。	事故報告・対応体制を確立している。
	事故対応マニュアルを作成している。
	再発防止策を策定し、実施している。
組織的な改善活動が実施できるように、情報セキュリティの PDCA を実施する。	情報セキュリティ対策が正しく実施されているかを見直す為に、自己点検を実施している。
	自己点検結果に基づく改善活動のための体制を構築している。

※なお具体的な管理策については、X社様作成「お取引先様向け　情報セキュリティ構築マニュアル」を参考に当社の状況に合わせ、適切な管理策を設定した。

【タイプ３　受託者主導方式　言明書　例】

『ソフトウェア開発における基本遵守事項に関する言明』

２０１２年ＸＸ月ＸＸ日

（委託元）ＸＸＸＸＸＸＸＸＸＸ社　経営者　殿　　（委託先）情報統括責任者

ＸＸＸＸＸＸＸＸＸＸ社様から２０１１年４月から２０１２年３月までの間、販売管理システムの開発を受託し、販売管理システムの開発にあたっては委託元様からの要求事項である「ソフトウェア開発に対する基本遵守事項」を守り、ソフトウェア開発を行ったことをここに言明する。詳細については以下の通りである。

【項目別内訳】

分類	遵守事項	実施状況
開発業務	情報システムの信頼性・安全性水準の達成を確実なものにするシステムライフサイクルプロセスを確立し、文書化すること。	共通フレーム 2007 及び ISO/IEC 20000 を参照し、ライフサイクルプロセスを確立し、文書化した。
	企画・開発から保守・運用に至る各プロセスにおける役割分担及び責任権限等を明確化し、合意すること。	共通フレーム 2007 を参照し、個々のプロセスに関する双方の役割・責任を文書化し、合意した。
	具体的な機能要件及びその実現性並びに実現・運用コスト等について明確化及び文書化し、合意すること。	情報システム利用者及び情報システム供給者協力の下、発注仕様に基づき具体的な機能要件を明確化及び文書化した。
	非機能要件の実現に向けた利用者・供給者間で合意すること。	JIS X 0129 で定められた品質に関する特性を参考に非機能要件を抽出し、文書化した。
	情報システムの開発にかかる価格の見積値を、その算出根拠を説明すること。	価格の算出根拠の一つとして、ファンクションポイント法 3 等を活用した工数見積りを実施した。
	情報システムの大規模化及び複雑化を極力抑える設計を心がけること。	標準に基づいた通信プロトコル、データフォーマット等を採用した。
	情報システムの設計に当たり、フェイルセーフ 4 の観点から、各種障害に対して発生時の業務・サービスへの影響の防止及び最小化に努めること。	システム構成要素や機能の二重化・多重化等を設計に織り込んだ。
	各種ユーザインタフェイス等の設計に当たり、フールプルーフ 5 の観点から、誤操作等の防止に努めること。	画面設計において、誤操作の防止に配慮した部品配置及び画面遷移等を行った。
	情報システムに求められる信頼性・安全性の水準に応じたテスト及びレビューを行い、当該システムの機能要件及び非機能要件に対する適合性の確認に努めること。	情報システム利用者による仕様適合性の確認及び実環境における利用可能性の確認に向け、情報システム利用者の協力によるテスト及び試行等を実施した。
保守・運用業務	保守・運用に関する体制等を利用者・供給者間で合意すること。	運用保守体制図及び運用フロー図を作成し、合意した。

【タイプ４　社会主導方式　言明書　例】

K市被災者支援システムの災害対策に関する言明書

○○○○○　監査人　殿

平成○○年○○月○○日
K市情報センターCIO○○○

本市では、東日本大震災によって地方自治体が被った甚大な被害と住民サービスへの影響に鑑み、災害時の対策としてBCPの構築、整備を進めている。その中で危機管理下における情報システムの果たす役割と重要性は高く、情報センターでは特に災害時に速やかな住民支援サービスの実施につなげるため、平成23年4月1日より「被災者支援システム」に重点を置いて災害対策を行ってきた。

私たちはシステム管理基準に準拠し下記の範囲で対象システムに対する適切な管理策を整備、実施していることを言明する。

１．目的

災害時に速やかな住民支援サービスの実施につなげるため。

対象システムの復旧目標を、災害時から遅くとも２週間以内とする。

２．対象範囲

（1）対象場所

K市庁舎情報センター内

（2）対象情報システム

K市被災者支援システム・・・大規模災害時の被災者情報管理システム。

（住民基本情報、災害統計処理、各種申請処理、文書管理など）

３．対象システムに関して整備、実施した管理策

項番	分類	管理策
1	リスク分析	大規模災害のリスク及び対象システムに与える影響範囲を明確している。
2		対象システムの停止により、市民が被る損失を分析している。
3		業務の回復許容時間及び優先順位を定めている。
4	災害時対応計画	リスク分析の結果に基づき、K市のBCPと整合性をとった災害時対応計画を策定した。
5		災害時対応計画は、組織体の長である市長が承認した。
6		災害時対応計画の実現可能性を検討した。
7		災害時対応計画の中で、職員の教育訓練の方針を明確にしている。
8		災害時対応計画は、情報センター内だけでなく全市各部署に周知徹底している。
9		災害時対応計画は、必要に応じて見直す。
10	バックアップ	被災者支援システムが必要とするデータ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めている。
11		情報センターの責任者は、上記バックアップ方法及び手順を検証している。
12	代替処理・復旧	情報センターでは、復旧までの代替処理手続き及び体制を定め、検証している。
13		情報センターでは、復旧手続き及び体制を定め、検証している。

※なお詳細な管理策については、総務省「地方公共団体におけるICT部門の事業継続計画（BCP）策定に関するガイドライン」を参考に本市の状況に合わせて整備した。

参照：①システム管理基準を参考
②X社作成「お取引先様向け情報セキュリティ構築マニュアル」を参考
③情報システムの信頼性向上に関するガイドラインを参考
④地方公共団体におけるICT部門の事業継続計画（BCP）策定に関するガイドライン」を参考