特定非営利活動法人
日本システム監査人協会報

2011 年 10 月発行
No 128

No. 128（2011 年 10 月　発行）

会報電子版の記事　目次

めだか　【 めだか　どじょう 】　　**投稿**

「どじょう」が人気だそうである。
鍋物ではない。どじょうを使った「どじょうすくい」は、忘年会のかくし芸、ひょうきんなだけでなく、疲れた人を励ます伝統芸能のひとつで、コミュニケーションを円滑にする現代の手段だと思う。
毎回恒例の人形を型どった名物饅頭も発売された様子。

一方で、日本システム監査人協会の会報誌には「めだか」コラムがあり、すでに１年以上の人気記事として読者の認知度も高まり、評価もあがってきたようである。英語圏の社会では、good eye, expert eye, excellent eye であり、日常的にもよく使われる表現である。他人の目で評価するAuditが普及する背景でもある。近視眼や目がくもっていては正しい姿は見えず、色眼鏡をかけていては勘違いしてしまう。
システム監査には、第三者の立場で客観的な評価をして、よりよい状態に改善、改革を後押しするという役割がある。目利き、目高が重要で、善くない現象、障害や事故が発生した状況の原因を示唆し、方向をしめす役割と責任は大きい。
さらに今や、システム監査の対象を情報システムの企画開発運用など、従来のソフト開発に限定する必要は薄い。ツールとしてのIT活用の広がりは、業務の仕組み、情報を処理し活用するシステムという仕組みにまで広がり、目高の見識を生かす場面は、経済活動のほとんどの分野に展開できる。

「どじょう」、「めだか」は、魚という分類では主役ではない。しかし、どじょうすくい、土鍋、システム監査、業務改革という分野に絞れば、主役として活動できる土俵はある。
使う場所、タイミング、活用方法が適切であれば、活性化、鑑識の役割が活きて来る。
焦点を絞って役割を果たし、誰もが納得し評価される成果を積み上げること。
評価が高まり賛同者も増えれば、活動も活発になり、経済循環が加速し規模も大きくなる。
そのためには、情報を発信して、めだかの存在や活動を伝える工夫が必要である。

限られた予算、人員を投入して復興、再生、再興という役割が必要な今、めだかの人材は、もと情報発信して姿を見せると、役に立つ場面が現れるのではないだろうか。
システム監査人としての個人の活動を支援するためには、システム監査人のブランドつくりが必要で、このめだかコラムや情報発信型会報のスタイルは、従来の活動記録保存という役割に加え、情報発信拠点としてもっと活用できるのではないか、と思う。
情報化社会はどんどん変化、発展している。システム監査人として、新しい技術、新しい使い方に取り組み習熟して、新しい視点、目線を加え、付加価値を高める目利きの役割を果たし続けたい。

（展望明日）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

投稿

■　【保証業務に係る公表文書の調査研究と保証型システム監査の一考察（6 章)】

榎本　吉伸

（この投稿は 8 月号と 9 月号に掲載したレポートの続きです。）

6. 保証型システム監査のフレームワーク

本章の目的は、意見書・研究報告書等の保証業務に係る公表文書を十分に理解した上で、保証型システム監査のフレームワークを一つのモデルとして明確にすることである。既に見てきたように、保証業務に係るシステム監査について制度として必要な監査基準や監査手続等の基本的要件は十分に議論が尽くされていると考える。従って、本レポートの主題は既に議論されてきた保証型システム監査の要件を一つのフレームワークとしてまとめることである。今後必要なのは、保証型システム監査の豊富な実績の積み重ねとその成果としての社会への普及、浸透であろう。

本レポートでは「保証型システム監査に係るフレームワーク」について、システム監査で信頼と実績のある経済産業省「システム監査基準」に準拠して、既に見てきた保証業務に係る議論を整理すると共に、特に保証業務に係るシステム監査の担保要件等について重点的に追補し、これを定義し明確化する。

結論から先に述べると、保証型システム監査で特に重点を置くべき論点は、保証を担保する 5 つの要件のうち、「適合する基準」と「適切で十分な証拠」の 2 項であると筆者は考える。それぞれ、次章と本章で考察する。

6.1 システム監査の定義（システム監査基準「Ⅰ前文」、「Ⅱシステム監査の目的」に準じる）

6.1.1 システム監査の目的

システム監査の目的は、「システム監査基準」に準じ、下記の通りとする。

> 6.1.1　**システム監査の目的**
>
> **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。**

この目的の定義で、第 1 義的な目的は、「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」であり、第 2 義的な目的は、「保証を与えあるいは助言を行う」ことである。そして最終目的は「IT ガバナンスの実現に寄与すること」である。システム監査に係る者は、この最終目的を忘れてはならない。

IT ガバナンスの実現に寄与するためには、システム監査が制度として、また組織体のマネジメントシステムとして日常の経営活動に組み込まれていることが必須要件である。また、ここでは「保証を与えあるいは助言を行い」と、助言型システム監査での準用を考慮して保証と助言のいずれをもカバーする旨の定義とする。尚、システム管理基準については「システム監査の実施に当たっては、組織体における情報システムに係るリスクに対するコントロールの適否を判断するための基準が必要である。システム監査は、本監査基準の姉妹編であるシステム管理基準を監査上の評価基準として用い、監査対象がシステム管理基準に準拠しているかどう

かという視点で行われることを原則とする。」とし、システム監査における評価基準としてのシステム管理基準の役割を明確にする。これは保証型システム監査においても同様であるが「適合する基準」としての十分な議論が必要であると考える。

6.1.2 コントロールを適切に整備・運用されているかを検証又は評価するための目標

次に、前項で定義した第 1 義的な目的である「コントロールを適切に整備・運用されているかを検証又は評価するための目標」は、保証業務の要件として重要な論点となる。組織体が情報システムに係るリスクに対するコントロールを適切に整備・運用されているかを検証又は評価するための目標（注記：本レポートでは、コントロール目的ではなく「コントロール目標」という用語を使う）として、次の 4 項目がある。

・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貢献するため （以下、「戦略性」と言う）

・情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため （以下、「安全性／有効性／効率性」と言う）

・情報システムが、内部又は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（以下、「信頼性」と言う）

・情報システムが、関連法令、契約又は内部規程等に準拠するようにするため（以下、「遵守性」と言う）

尚、本レポートでは情報セキュリティ監査の目標である機密性・安全性・可用性も上記の安全性および信頼性に含まれると考える。

ここでは保証業務を議論する観点から、上記の 4 つのコントロール目標を以下のように分類して定義する。

6.1.2 コントロールを適切に整備・運用するための目標（以下、「コントロール目標」という）

①情報提供に係る IT システムの戦略性

②情報提供に係る IT システムの有効性および効率性

③情報提供に係る IT システムの安全性および信頼性

④情報提供に係る IT システムの遵守性

この定義では、システム監査基準のコントロール目標の区分とは異なり、“安全性”は内容分類により信頼性と同一のグルーピングとする。これらのコントロールの目標は、システム管理基準に記載の各コントロールの属性情報である。ここで筆者は保証型システム監査の対象と上記コントロール目標には、次のような傾向があると考える。

一般的に戦略性、有効性、効率性を監査対象とする保証型システム監査の実施は、保証という言葉の定義から考えて、第三者からの依頼は少ないものと考える。例えば、情報システムの戦略性、有効性、効率性については、経営者（主題に責任を負う者）が自社（自身）のために助言型システム監査を要請することがあっても、「当該情報システムの戦略性」について第三者が保証型システム監査を要請することはあまり考えられない。これに対して、安全性、信頼性、遵守性については、「保証」の定義に馴染む目標である。

7 章では、保証業務とコントロール目標の関係を論ずるべく、経済産業省「システム管理基準」の各コントロールについて、該当する上記のコントロール目標を考察する。

6.2 保証型システム監査のフレームワークにおける保証業務の要件

保証型システム監査のフレームワークにおいて、保証業務の定義および保証業務を担保する要件は以下の通りである。

6.2.1 保証業務の定義

保証型システム監査のフレームワークにおける保証業務の定義は、意見書に準じて、以下の通りとする。

> 6.2.1 **保証業務の定義**
>
> **保証業務とは、主題に責任を負う者が一定の基準によって当該主題を評価又は測定した結果を表明する情報（以下、「主題情報」という。）について、または当該主題それ自体について、それらに対する想定利用者の信頼の程度を高めるために、業務実施者が自ら入手した証拠に基づき基準に照らして判断した結果を結論として報告する業務をいう。**

本レポートでは主題情報についてのみならず、主題それ自体についてのシステム監査（直接方式）も含める。

保証業務の定義は概ね意見書の定義に準じるが、「合意された手続」を含め、本レポートでは次のように分類し、「名称」も以下のようにすることを提案したい。

分　類	名　称	意見書等の分類
保証業務に係るシステム監査	システム監査 （JASA の利用者合意方式、被監査主体合意方式も含む）	監査 レビュー
助言業務に係るシステム監査	システムコンサルティング （あるいはシステム診断）	合意された手続 財務諸表等の調製等

ここで、システム監査とは「保証業務に係る業務」に限定し、助言型は監査と呼ばず、システムコンサルティングと称し区別を明確にしたい（但し、本レポートでの表現は混乱を避けるため、従来どおり「保証型システム監査」および「助言型システム監査」という）。

尚、この分類では、意見書の定義にある「主題に責任を持つ者が唯一の想定利用者である場合（JASA の監査主体合意方式）」や「合意された手続」等については、意見書と異なる。

今回の新システム監査基準の改定では、情報セキュリティ監査基準に続き、従来の助言型監査に加えて保証型監査を導入し、利害関係者への監査結果の報告も視野に入れている点が特徴で、システム監査の社会的役割を強化したものある。しかし、システム監査基準解説書（平成 16 年度改訂版。以下、「解説書」という）には、「保証型監査では、『いつ、誰が、どのような判断尺度で、何を、どのように評価した』といった点が明確にされた監査実施結果でなければ説得力はない」とあるが、これは助言型監査でも同様ではないか。

6.2.2 「保証型システム監査」の保証を担保する要件

6.2.2 「保証型システム監査」の保証を担保する要件

保証型システム監査における「保証」を担保する要件は、以下の 5 項目とする。

①三当事者

②主題／主題情報

③適合する評価基準

④適切かつ十分な証拠

⑤監査報告書

保証型システム監査における「保証」を担保する要件は、以下の 5 項目とする。

①三当事者

保証業務を成立させる当事者として、業務実施者（監査人）、主題に責任を負う者（一般に保証業務依頼者と同じ場合が多いが、異なる場合もある）および想定利用者の三当事者の存在が必要である。

②主題あるいは主題情報

主題の要件は以下の通り。

・説明可能であること（意見書では、「識別可能のであること」とある。）

・一定の規準に基づいて首尾一貫した評価又は測定を行うことができること

・業務実施者が主題情報に対する保証を得るために十分かつ適切な証拠を収集することができること

ここに、主題情報とは、主題に関して監査対象とするコントロール目標の評価を示す情報。例えば主題が IT システムでコントロール目標が信頼性の場合、主題情報は当該 IT システムの信頼性を示す情報である。本レポートでは、保証型システム監査においても主題あるいは主題情報を監査対象とする。

③適合する評価基準

主題に責任を負う者が主題情報を作成する場合及び業務実施者が結論を報告する場合に主題を評価又は測定するための一定の規準で、以下の５項目を満たすもの（詳細は、意見書による）。

・目的適合性

・完全性

・信頼性

・中立性

・理解可能性

意見書でのこの規準の定義は大変有効である。これをベースに、より保証業務に係る監査に適合する基準要件の議論が必要である。特に戦略性や有効性、効率性のコントロール目標を監査対象とする基準として、適切な基準を選択するのは難しい。7章で考える。

④適切かつ十分な証拠

保証業務を担保できる客観的に適切かつ十分な証拠。

この「保証業務を担保できる客観的に適切かつ十分な」が本レポートで議論すべき最重要事項で、後述する。

⑤監査報告書

監査報告書は、保証要件を満たす記載内容を一般用語で簡潔に記述することが肝要である。後述する。

6.2.3 保証型システム監査とコントロール目標

ここに前項の各コントロール目標に対して、上記の保証要件の具体例を示す。

コントロール目標	当事者	主題	主題情報の例	基準
①戦略性	・業務実施者 ・主に主題に責任を負う者（＝想定利用者）	・情報システムに係る戦略的業務	・IT 戦略計画書および達成評価	戦略性を測定／評価可能な基準
②有効性／効率性	・業務実施者 ・主に主題に責任を負う者（＝想定利用者）	・情報システムに係る運用・開発業務	・IT 開発計画の目標 ・IT 開発／運用等効率性指標	・有効性を測定／評価可能な基準 ・効率性を測定／評価可能な基準
③信頼性／安全性	・業務実施者 ・主題に責任を負う者 ・想定利用者	・情報システムに係る業務全般	当該業務の信頼性／安全性に関する経営者の主張	・システム管理基準 ・FISC ガイドライン等
④遵守性	・業務実施者 ・主題に責任を負う者 ・想定利用者	・法令／規程等により遵守すべき規準が明確な業務	・当該業務の法令／規程等遵守に関する経営者の主張	・金融検査マニュアル等各基準類

この表からも判断できるように、コントロール目標を①戦略性、②有効性／効率性とする監査では、保証業務に係る当事者において想定利用者が主題に責任を負う者であることが多いと考えられるが、意見書の定義では、主題に責任を負う者が唯一の利用者（例えば、経営者等）である場合は、保証業務の範囲には含まれないとする。しかし、自分で自分の管理する情報システムの保証を得たいと考える場合もある。第三者である想定利用者が主題に責任を負う企業の戦略性や有効性／効率性の評価を必要とすることは実際上それほど多くの機会はない。従って、戦略性や有効性／効率性の評価はシステムコンサルティングや内部監査による助言型システム監査案件となることが実務上多いと言える。

一方、コントロール目標が③信頼性／安全性、④遵守性のシステム監査においては、一般的に第三者の想定利用者を含めた三当事者が存在するが故に、保証型システム監査が容易に成立すると考えられる。

6.2.4 評価基準としての「保証型システム管理基準」

上記③項の「適合する評価基準」として提供される保証型システム管理基準の議論において重要な論点は、保証業務における監査対象として戦略性や有効性／効率性のコントロール目標に対して保証業務が成立するか（具体的な案件が発生するか)、成立するとすればその管理基準は適切かどうかであると考える。参考までに、ＩＴ実務指針に挙げられているコントロール目標の具体例は「信頼性等」とのみ記載。考えすぎか。

この議論では、戦略性や有効性／効率性を評価する基準として、利用する基準が保証業務に適合するか否かが重要であり、保証型システム管理基準としての検討が望まれる。

尚、本レポートでは「システム管理基準」に対して経済産業省が示す「判断の尺度」と言う用語は使わないで、用語として「評価基準」を使う（現状の管理基準であるコントロール一覧表に、“尺度”という言葉は適さないと考える)。

ここでは尺度と言う用語は“モノサシ”と同様で別の意味で用いたい。すなわち、本レポートでは「尺度」とはコントロールを評価する際の「モノサシ（達成度、割合、回数等)」とし、その指標としての目標値（具体的な達成値）が必要と考える。成熟度モデルで言えば成熟度レベルを示す。例えば、先に挙げた情報セキュリティにおけるコントロール例である「パスワードの定期的な変更」においては、その評価の尺度（モノサシ）はパスワードの変更回数で、その目標値として１回／月か１回／年かを定め、それを判断の尺度とし運用状況の評価を行ことが必要と考える。

現存するシステム管理基準に、評価の尺度（モノサシ）と指標までを含めた基準は存在しない。また、この具体的な評価尺度の指標は、業種や業態、とくに企業規模に合わせて設定する必要がある。

成熟度モデルを利用したコントロール評価は、成熟度レベルそのものを評価の尺度（モノサシ）とし、指標としてその定めた成熟度レベルに対する達成度を評価するため、評価の尺度（モノサシ）と指標が標準的に定められているので、一般的に理解が得やすい。

6.2.5 本レポートでの「情報セキュリティ監査」の考え方

前章で「情報セキュリティ監査」の公表文書について触れてきたが、本レポートでは「システム監査と情報セキュリティ監査の違い」については本質論ではないので議論しない。両者は監査する対象や範囲、すなわち具体的な IT コントロール（評価基準の項目）が異なるだけで監査としての基本的な手続（監査基準の範疇）は変わりないと考える。経済産業省公表のシステム監査基準と情報セキュリティ監査基準とは、内容がほぼ同じであることからも明確である。

解説書には、「システム監査は、情報システムのライフサイクルを通じて実施する総合的な監査であるのに対して、情報セキュリティ監査は、情報セキュリティに特化した監査である」とある。本レポートでは、システム監査として議論する。

6.3 一般規準

6.3.1 システム監査実施の目的と責任の明確化

システム監査基準には、「システム監査を実施する目的及び対象範囲、並びにシステム監査人の権限と責任は、文書化された規程、または契約書等により明確に定められていなければならない。」とある。このことは監査において基本的な事項であり、既に学んだ他の公表文書でも同じである。特に保証型システム監査（外部監査人による監査）では、契約書等での明確な規定は重要である。また、関連事項として、主題情報としての確認書や言明書等の有無の議論が挙げられる。

①監査目的

監査目的では、特に既述の「コントロール目標」のいずれを目的とするのかを、明確にすることが重要である。目標により監査手続等に違いが生じる。

②監査対象範囲

保証型システム監査では、監査対象範囲の選択は、保証を得るに重要な要素となる。監査計画や監査契約書で明確にしなければならない。情報セキュリティ監査基準では保証目的を達成するためには、情報セキュリティ管理基準の全コントロール項目を監査対象とすることが望ましいとするが、保証型システム監査では、例えば、あるシステムについて、システム管理基準の「企画業務」等、一部のコントロール分野での監査も可能である。必ずしも全分野、全コントロールが必須要件ではない。従って、主題に責任を負う者（経営者等）は、システム監査の中長期計画において、コントロール分野の網羅性を十分に意識した監査対象範囲を計画し、利用者に十分な信頼を得る必要がある。また、報告書の利用者はその旨を十分に理解した上で、監査結果を活用

することが肝要である。

③保証型システム監査における監査人の権限と責任

意見書には、「主題に責任を負う者が自己の責任において主題情報を想定利用者に提示しない場合に、業務実施者が、主題それ自体について一定の規準によって評価又は測定した結果を結論として表明する保証業務があるが、この場合においても、業務実施者は、主題それ自体に対する責任を負うものではなく、主題それ自体の信頼の程度を高めることに責任を負う（保証業務の分類①）」。また「業務実施者は、保証業務について要請される要件及び保証業務の実施に関する基準に準拠して適切に業務を行わなかった場合には責任を負う（保証業務実施の前提③）」とある。

これは監査目標としたコントロールの適切な実施における評価または測定結果に対する責任論であり、主題における実際の不備や事故の発生そのものに対する責任を負うものではない。そのような責任は外部の業務実施者に負える訳がなく、当然であろう。

6.3.2 システム監査人の独立性、客観性と職業倫理

保証業務おいては、システム監査人の独立性は特に重要である。

①外観上の独立性／客観性（「システム監査基準」に同じ）

システム監査人は、システム監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない。

解説者には、「独立性の本質は精神上の独立性であるが、外観上の独立性が損なわれると、精神上の独立性が損なわれているとの嫌疑がもたれるため、外観上の独立性を維持することが重要である」とある。

②精神上の独立性／客観性（「システム監査基準」に同じ）

システム監査人は、システム監査の実施に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。

③職業倫理と誠実性（「システム監査基準」に同じ）

システム監査人は、職業倫理に従い、誠実に業務を実施しなければならない。

解説書には、「監査報告書の信頼性を担保するためには、システム監査人が高い品格とともに高度な人格、すなわち、倫理観、誠実性、責任感、正義感等を有することが必要である」と更に説明がある。職業倫理には、業務委嘱懇請の禁止、成功報酬の禁止、信用失墜行為の禁止等が紹介されている。

6.3.3 専門能力（省略）

6.3.4 業務上の義務

業務上の義務には、研究報告と同様に「職業的専門家としての猜疑心」の記載を望みたい。システム監査基準には、その解説書の「精神上の独立性」に記載がある。

①注意義務（「システム監査基準」に同じ）

システム監査人は、専門職としての相当な注意をもって業務を実施しなければならない。

解説書には、「システム監査人に求められる正当な注意義務は、民法（第 644 条）に規定される善良なる管理者しての注意義務（善管注意義務）に相当するものと考えられる」とあり、その上で「システム監査人は専門的な能力があることが想定されるため、システム監査人に求められる善管注意義務は一般のそれよりも高いものとなる」とある。

②守秘義務（省略）

③職業的猜疑心

研究報告では、「主題情報に重要な虚偽表示が含まれていないかどうかについて判断するための十分かつ適

切な証拠を入手することができるように、職業的専門家としての懐疑心を保持し、保証業務を計画し実施する。」と職業的猜疑心の必要性を説く。

6.3.5 品質管理（省略）

以上の一般基準各項は、保証型システム監査では更に厳守されるべき事項であろう。

6.4 実施基準

6.4.1 監査計画の立案

「システム監査人は、実施するシステム監査の目的を有効かつ効率的に達成するために、監査手続の内容、時期及び範囲等について、適切な監査計画を立案しなければならない。監査計画は、事情に応じて適時に修正できるように弾力的に運用しなければならない。」（システム監査基準）

①中長期計画、短期、個別

監査計画は、中長期計画から短期計画、個別計画へとブレークダウンし、監査対象範囲の網羅性を図らなければならない。

②監査の基準

保証業務に係るシステム監査の個別計画では、「適切な基準」を明確にせねばならない。有効性や効率性のコントロール目標に対する基準は、特に慎重を要する。基準には大きく次の２通りある。

・既に取り挙げてきた公的機関による公表基準（例、システム管理基準）

・各企業で作成された企業固有の基準（公的基準を参考にしたものも含む）

有効性や効率性を目標とするシステム監査では後者の基準により実施されるケースがあるが、これは第三者への保証には必ずしも十分ではない場合がある。例えば、近年 IT 投資の有効性・効率性評価において評価手法として注目され始めている「IT ポートフォリオ評価」などが公正妥当な評価基準として広く社会に浸透すれば、第三者を想定利用者とする有効性・効率性評価の保証型システム監査の管理基準として十分活用できるであろう。

③監査対象期間に対する考え方

保証型システム監査については、保証する対象期間が議論になる。保証期間をどこに限定するのかである。一般的には、ある一時点か定められた期間である。ある個別計画の監査対象期間を定める場合は、中長期計画および短期計画で監査対象や監査項目等について全体的に網羅性を考慮して決める必要がある。また、この場合は後述するサンプリング試査のサンプリング期間を考慮する必要がある。

監査対象期間に関して、保証型システム監査の議論で“システム監査では、会計監査のように過去の一定期間の保証では経営者に満足されず、「では、今後も安心できるのか？」との質問に答えなければ評価されない”という意見がある。しかし、この質問に答えるのは不可能であり、どのような保証型監査でも未来を保証はできない。

保証型システム監査における対象期間の問題（将来の保証に関する問題）については、過去から一定期間の組織体制や仕組みの安全性／信頼性等の保証の上に、その継続性および環境変化への対応性を判断することで、想定利用者は、近未来の保証を自らの責任で想定することになる。

6.4.2 監査の手順（情報セキュリティ監査基準には、この項なし。）

システム監査基準には「システム監査は、監査計画に基づき、監査の実施として予備調査、本調査及び評価・結論の手順により実施しなければならない」とある。手順そのものについては、保証型システム監査と一般のシステム監査とは差異はないが、その監査手順における監査手続（方法論）に違いがあると考える。特に保証型システム監査では、本調査における監査証拠の入手および評価に厳格な対応を要求されると考える。適切かつ十分な監査証拠および証拠から判断できる事実に基づく論理的で体系的な評価が要求されるであろう。

①予備調査

予備調査の目的と調査内容については、システム監査基準に詳しい記載はない。日本システム監査人協会編『情報システム監査実践マニュアル』には「監査対象の業務およびシステムの実態を把握し、その後の本調査の円滑に実施することを目的とする」とあり、調査内容として「調査内容は、監査対象に信頼性、安全性、効率性、有効性を確保するためのコントロールが整備されているか（コントロールの整備状況)」であり、調査方法として「コントロールに関する資料収集、関係者へのインタビュー、アンケート調査などにより調査を行う」とある。

しかしながら、監査の手順として予備調査はシステム監査個別計画策定後に行うとある。個別計画では、監査項目まで明らかにするのが一般的だが、外部監査人が監査の実施を請け負った場合、個別計画が与件か個別計画から考えるかで予備調査の目的や内容が違ってくる。このことは、主題情報としての言明書に対する監査（監査項目が言明書で与件）か、主題そのものの監査（監査項目の洗い出しも監査対象となる）かにも関係する。

ケースによっては、個別計画作成（監査対象／監査項目の明確化）のために事前調査（予備調査以前の調査）が必要となる場合もある。

本レポートでは、保証型システム監査としては、監査対象案件の個別計画（監査目的／監査対象）が明確であり、従って予備調査の主要な目的は、監査項目（コントロール）の選択およびそのコントロールの整備状況把握と定義する。実務上は、案件における与件（個別計画書の有無等）の程度により予備調査の内容、タイミング等の考慮が必要である。

参考までに、FISC ガイドラインでは予備調査は事前の文書調査と解せるが、如何。FISC には整備状況の把握は本調査で行う旨の記載がある。

②監査手続の作成

予備調査の結果、抽出されたコントロールのチェック項目の明確化、監査手続書（監査担当者、監査手法等）作成等の監査手続の具体化を行い、本調査に挑む。

③本調査

本調査では、作成した監査手続を具体的に実施し、コントロール運用状況の把握および評価を行うための監査証拠の入手が主目的である。いわゆる「運用状況の評価」である。

本レポートでは、保証型システム監査におけるコントロールの運用状況評価は、サンプリング試査によることとする。

④評価・結論

予備調査・本調査で入手した十分かつ適切な証拠に基づき判断・評価をし、結論に導く。

保証型システム監査の評価においては、入手した証拠に基づく事実からのみ厳密に結論が導かれるべきである。

6.4.3 監査の実施

①監査証拠の入手と評価

システム監査基準には「システム監査人は適切かつ慎重に監査手続を実施し、保証又は助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない」としか記載がなく、助言業務と比較して、保証業務としての十分かつ適切な監査証拠についての具体的な記載は無い。

・十分かつ適切な監査証拠と合理的な評価とは

監査証拠とは、「監査基準委員会報告書第31号　監査証拠」（公認会計士協会）によれば、以下の通りである。システム監査においても同様である。併せて、十分かつ適切な監査証拠および監査証拠の証明力についても紹介する。

監査証拠	監査証拠は、監査人が監査意見を形成するに足る合理的な基礎を得るために利用するすべての情報である。
十分かつ適切な監査証拠	十分性は、監査証拠の量の問題である。適切性とは、監査証拠の質の問題、すなわち、取引、勘定残高及び開示に関連する経営者の主張を裏付けたり、又は虚偽の表示を発見するために入手した監査証拠の適合性と証明力である。
監査証拠の証明力	・企業から独立した情報源から入手した監査証拠は、企業から入手した監査証拠より証明力が強い。 ・企業から入手した監査証拠は、内部統制が有効なときには証明力が強い。 ・ 監査人が直接入手した監査証拠（例えば、内部統制の運用についての観察により入手した監査証拠）は、間接的又は推測によって入手する監査証拠（例えば、内部統制の運用についての質問により入手した監査証拠）よりも、証明力が強い。 ・ 監査証拠は、紙媒体、電子媒体又はその他の媒体であろうと、文書化されたものの方が、証明力が強い（例えば、議事録は、会議の後の口頭による議事説明よりも証明力がある。）。 ・ 原本によって提供された監査証拠は、コピーやファックスによって提供された監査証拠よりも、証明力が強い。

・監査結果の評価

監査結果の評価は、監査調書をもとに監査証拠を十分に検討して、事実に基づき監査人が自ら行う。その評価結果である結論に至る具体的方法論には定まったものはなく、結果やレベルは当該監査人の能力次第である。

評価について、前出『情報システム監査実践マニュアル』には、「3.3 評価結論」で、以下の説明がなされている。

「・評価・結論は、予備調査・本調査を通して収集した監査証拠を整理・分析し、監査テーマについての監査対象のコントロール（注記：監査項目）の状況を評価することである。

・評価・結論は、監査報告の内容を決める重要な段階であり、システム監査人の分析力・判断力が問われる段階である。

・評価を行うに当たっては、評価結果を定量化して示すことが、監査の客観性という観点からも、組織体の長に監査結果を明確に示すという観点からも有効である。」

また「ここでは、定量化評価の手順と評価方法の例を紹介する」と有り、「（1）評価の手順、（2）評価方法

の例、（3）評価を行う上での留意点」が示され、「（2）評価方法の例」として定量化方法である「減点法、加点法、星取表法」が説明され、少し詳しい手順、方法が示されている。しかし、特に保証型システム監査に対して適切で合理的な評価方法としての紹介ではないが、定量化評価は重要な論点である。

②コントロール評価の方法

・保証型システム監査における「評価」の考え方

保証型システム監査における評価方法

システム監査人は適切かつ慎重に監査手続を実施し、保証業務に係る監査結果を裏付けるのに客観的で十分かつ適切な監査証拠を入手し、以下の通り評価しなければならない。

・コントロールの評価は成熟度モデルにより行うことが望ましい

・コントロールの運用状況評価においては可能な限り“試査”により行う

・コントロールごとに評価の尺度（モノサシ）と指標（目標値）を定めることが望ましい

・成熟度モデル評価方式

保証型システム監査におけるコントロールの評価では、成熟度モデルの達成指標（成熟度レベル）を予め被監査主体と協議の上、成熟度モデル評価方式で行うことが望ましい。この際、成熟度モデルについては Cobit モデルあるいは FISC モデルを参考にしたい。

・整備状況評価および運用状況評価の 2 段階評価方式

成熟度モデル評価方式を使用しない場合は、整備状況評価と運用状況評価の 2 段階方式で評価することを薦める。成熟度レベルの定義には整備状況と運用状況が同一レベルに混在しているので、整備状況評価と運用状況評価の 2 段階評価で行うことはできない。2 段階評価の場合、整備状況評価においては、コントロールの有無とその適切性を評価する。運用状況評価では監査時点あるいは監査対象期間におけるコントロールの運用における有効性評価である。

いずれの場合も、運用の有効性評価は基本的に「試査」により評価することが望ましい。

また、2 段階方式ではコントロールのごとに評価の尺度（モノサシ）と指標を定めることが必要である。

尚、成熟度モデルと試査との関連は、成熟度モデルの目標レベル（例えば、「レベル 3：コントロールは適切に運用されている。」）に対する“適切な運用”の達成評価を行う際に、サンプリング試査による評価を行う方法が考えられる。

③内部統制のサンプリング試査における「25 件のサンプル件数」

ここで実務上、試査の方法として参考としたいのは、内部統制の評価で活用された「サンプリング試査」である。保証型システム監査での一般的に公正妥当な評価方法と考える。

内部統制の実施基準「Ⅲ　財務報告に係る内部統制の監査」には、外部監査人が運用状況評価を実施する際には、「例えば日常反復継続する取引について、統計上の正規分布を前提とすると、90%の信頼度を得るには、評価対象となる統制上の要点ごとに少なくとも 25 件のサンプルが必要になる」と記載されている。

この実施基準の「90%の信頼性を得るには、25 件のサンプルが必要」ということは、確率論を利用した統計的手法によるもので、公認会計士協会の「財務報告に係る内部統制の監査に関する実務上の取扱い（公開草案）」では、以下のように説明されている。

「統計的サンプリングにおいては、母集団の誤謬率についての結論を出すためのサンプリングとして、属性サンプリングが用いられる。つまり、金額ではなく、特定の属性の有無を判定することになるため、結果は率（%）で表される。内部統制監査の実施基準４．(2)①ロ．ａに例示されている 25 件のサンプル数は、許容誤謬率が

9%、サンプリングリスクが 10%（信頼度が 90%）、予想誤謬率が 0%であるならば、下記に例示した表に従って示される（AICPA : Audit and Accounting Guide-AUDIT SAMPLING より。文言一部修正）。ただし、当該統計的サンプリングの考え方に従い、テストの結果、内部統制からの逸脱が生じた場合や信頼度を向上させる場合はサンプルの件数は増大することに留意が必要である（次表、参照）。」

【運用評価手続のための統計的サンプル数】

（下線筆者）		許容誤謬率								
		2%	3%	4%	5%	6%	7%	8%	9%	10%
予想誤謬率	0.00	114	76	57	45	38	32	28	25	22
	0.50	194	129	96	77	64	55	48	42	38
	1.00	*	176	96	77	64	55	48	42	38
	1.50	*	*	132	105	64	55	48	42	38
	2.00	*	*	198	132	88	75	48	42	38
	2.50	*	*	*	158	110	75	65	58	38
	3.00	*	*	*	*	132	94	65	58	52
	3.50	*	*	*	*	194	113	82	73	52
	4.00	*	*	*	*	*	149	98	73	65
	5.00	*	*	*	*	*	*	160	115	78
	6.00	*	*	*	*	*	*	*	182	116
	7.00	*	*	*	*	*	*	*	*	199

結論として、保証型システム監査におけるコントロール項目ごとの評価を内部統制監査における「サンプリング試査」で行うことは、保証型システム監査の評価結果を利用する第三者にとって理論的でかつ納得のできる評価方法と考える。

ただ、サンプリング試査はコントロール個々の評価に使用されるもので、総合評価ではレーダーチャートによる表現等で新しい経営手法を活用した科学的で体系的な総合評価方式の開発が望まれる。

④保証型システム監査における評価尺度（モノサシ）および指標の明確化

既に触れてきたが、保証型システム監査における評価方法においては、評価基準としてのコントロール（現システム管理基準）内容の記載だけでなく、実際に評価する際の具体的な尺度（モノサシ）と指標が必要と考える。成熟度モデルによる評価の場合は、そのコントロールの尺度に対する成熟度モデルのレベル（目標値）の達成評価を行う方法が望ましい。保証型システム監査では、コントロール各々の評価尺度（モノサシ）とその指標（目標値）を明確にして、その指標に対する達成度で客観的に評価する方法を確立すべきと考える。

この評価尺度および指標は、監査計画立案における監査手続詳細を決める際に、予め被監査主体の現状の規定・ルール等を考慮の上、十分に協議して定めることが望ましい。

参考として、IPA（情報処理推進機構）から公表された「定量的セキュリティ測定手法および支援ツールの開発」の調査報告書／別冊「定量的セキュリティ測定ガイドライン」を紹介する。当ガイドラインでは、個々のコントロールに対して各々定量的尺度（割合、回数、時間、期間等）とその指標（目標値／例えば、100%の割合）が定められている。画期的な試みである。システム監査に携わる者が、学ばねばならないガイドラインである。

⑤監査調書の作成と保存（省略）

6.4.4 監査業務の体制（「システム監査基準」に準じる）

6.4.5 他の専門職の利用（「システム監査基準」に準じる）

6.4.6 情報セキュリティ監査

システム監査基準には「情報セキュリティ監査については、原則として、情報セキュリティ管理基準を活用することが望ましい。」とある。当然である。

6.5 報告基準

監査報告、監査報告書は研究報告に例示も含め詳しい。これを参考とすべきである。しかし報告書例が会計監査をベースにしているため、「経営者の記述書が、・・・適正に表示しているものと認める」（積極的形式／肯定的結論／主題情報に基づく方式）とか「・・・適正に表示していないものと認める」（積極的形式／否定的結論／主題情報に基づく方式）のように、保証の文言がストレートではない。これに関しては「6.5.3 監査報告書の記載事項」で詳しく見る。

報告で重要なことは、正式報告に際して行われる事前の「事実誤認の確認」は、保証型システム監査ではより一層慎重に行う必要がある。

6.5.1 監査報告書の提出と開示

システム監査基準には「システム監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、システム監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。」とある。

保証型システム監査では、開示されることが前提のため、開示方法等に十分考慮する必要があることは言うまでもない。

6.5.2 監査報告の根拠（省略）

6.5.3 監査報告書の記載事項

①研究報告「b.積極的形式／直接報告方式」における文例

研究報告におけるb.積極的形式／直接報告方式の場合の文例は「当監査法人は、○○株式会社が、○○○○の評価規準に基づいて、平成×年×月×日から平成×年×月×日までの期間において、○○株式会社の○○○システムがセキュリティに関する合理的保証を提供するための有効な○○○○をすべての重要な点において維持しているものと認める。」（報告書の独立した監査法人の検証報告書）とあり、“保証する”とは書かれていない。

②報告基準ガイドラインの情報セキュリティ監査報告書（例）の主文

一方、報告基準ガイドラインの情報セキュリティ監査報告書（例）の主文は、「われわれの監査は、情報セキュリティ監査基準に準拠して行われた。（中略）われわれの意見によれば、200 x 年 x 月 x 日から 200 x 年 x 月 x 日までの期間に係る XXX を対象とした情報セキュリティ対策の実施状況は、情報セキュリティ管理基準に照らして適切であると認める。」（5.5.5 保証報告書の雛形①肯定意見の雛形）で、「適切であると認める」とあり、“保証する”とは書かれていない。いずれも想定利用者である第三者には隔靴掻痒の感がある。

報告結果の保証内容が違うのであればやむを得ないが、「維持しているものと認める／適切であると認める⇒保証する」であるならば、保証型システム監査の監査報告書では、「・・・を保証する」とか「・・・を除き、保証する」等、一般者にも容易に理解できる表現を使いたい。

6.5.4 監査報告についての責任（省略）

6.5.5 監査報告に基づく改善指導（フォローアップ）

保証型監査では、改善指導およびフォローアップまでは言及しないのが一般的である。しかし本レポートでは、保証型システム監査では、可能ならば報告内容に「指摘事項／改善事項」を付け加えることを推奨したい。それこそが想定利用者（経営者等）に望まれる生きた報告事項であると考える。保証業務と改善の指摘とは異なる領域の業務だと限定的に考えることはない。保証のためのシステム監査業務を行っている過程で問題があれば、その改善事項は指摘できるはずである。

フォローアップまで行うことは独立性に問題があるとの指摘もあるが、改善事項が適切に行われているかどうかの結果フォローであれば問題はないと考える。

6.6 助言型システム監査、システムコンサルティング業務および合意された手続

意見書によれば、保証型システム監査は保証業務として位置づけられるが、助言型システム監査はその範囲外であることが明らかである。また、システムコンサルティング業務が保証型でないことは無論のことである。

この際、本章の最初に述べたように、保証業務に係る案件は「監査」と呼び、それ以外の助言型業務は「コンサルティング」と呼ぶことで統一してはどうだろうか。

再掲するが、意見書では「保証業務の定義に合致しない業務」として、特に以下の４業務を挙げ、保証業務の要件を明確にしている。

①業務実施者が、主題に責任を負う者又は特定の利用者との間で合意された手続に基づき発見した事項のみを報告する業務（「合意された手続」という。）

②財務情報の作成及び作成への関与を行う業務（「財務諸表等の調製」という。）

③主題に責任を負う者の経営又税務上の判断に関わる助言や調査等を行う業務

④税務申告書の作成及び納税者の代理を行う業務

①はシステム監査（情報セキュリティ監査（JASA）では監査業務）に分類。②、③、④は、コンサルティング業務と言える。

この章の最後に、「（表. 2）保証業務における“保証”を担保する主要項目まとめ」を添付する。“保証”を担保する主要項目について各公表文書と本レポートの比較を行った。

（表. 2）保証業務における“保証”を担保する主要項目まとめ（経産省「システム監査基準」の項目記載順）

比較項目 （必要な重要項目のみ）	意見書	研究報告	ＩＴ実務指針	情報セキュリティ監査	本 レポート
【前文、監査の目的】					
監査の目的	想定利用者の信頼の程度を高めるため	同左	同左	マネジメントプロセスの有効な運用	IT ガバナンスへの寄与（ステークホルダーの観点含む）
監査対象業務	内部統制など財務情報以外の事項を対象とした業務も含めた幅広い財務諸表	財務情報 内部統制 コンプライアンス 環境 成果 （IT 関連の記載無し）	・IT に係るシステム ・IT に係る内部統制 ・IT に係る経営戦略・経営管理 ・IT に係る委託・受託業務 ・IT に係る情報 ・その他 IT に係る事項	情報セキュリティに係るリスクのマネジメント又はコントロール ・IT に係るシステム ・IT に係る情報	情報システム（あるいは IT)に係る業務
コントロールの目標	・財務諸表監査／信頼性 ・内部統制／有効性 ・レビュー業務／信頼性 （「二 保証業務の意味」より）	・信頼性 ・有効性 ・コンプライアンス検証業務等／遵守性 （「２.保証業務の概要」より）	IT に関する信頼性等	・機密性 ・安全性 ・可用性	・戦略性 ・有効性／効率性 ・信頼性／安全性 ・遵守性
【保証業務の要件】					
当事者	・業務実施者 ・主題に責任を負う者 ・想定利用者	同左	同左	同左	同左
主題／主題情報	主題／主題情報	同左	同左	原則主題情報（言明書）	主題／主題情報

比較項目 （必要な重要項目のみ）	意見書	研究報告	ＩＴ実務指針	情報セキュリティ監査	本レポート
・確認書	特に記載無し	確認書 （確認書が入手できない場合は、限定付き結論か、結論を表明しないことを検討）	確認書 （同左）	確認書	問わない
適合する基準	具体的な基準例無し	・会計基準 ・内部統制基準等	同左	情報セキュリティ管理基準	システム管理基準他
適切かつ十分な証拠	適切かつ十分な証拠	同左	同左	同左	同左
監査報告書	監査報告書	同左	同左	同左	同左
【一般基準】（略）	―	―	―	―	―
【実施基準】					
・監査証拠の入手と評価 （監査証拠収集手続）	特に記載無し	原則として試査	原則として試査	試査：情報セキュリティ監査基準実施基準ガイドラインに記載	原則として試査
【報告基準】					
報告書の名称	保証報告書	検証報告書	検証報告書	監査報告書	監査報告書
監査報告についての責任	主題そのものに対する責任ではない	（同左）	（同左）	（同左）	（同左）
監査報告に基づく改善指導（フォローアップ）	－	－	－	保証型には改善事項の記載なし	保証型にも改善事項の記載が重要と考える

研究会、セミナー開催報告、支部報告

■ 【第 165 回月例研究会受講報告】

会員番号 328 勝田敦彦

・テーマ　医療情報システムの安全管理のための 3 制度について
～医療情報の利活用のために何をすべきか！～
・日、場所　2011 年 8 月 24 日（水)、御茶ノ水　総評会館
・講師　一般社団法人医療情報安全管理監査人協会　相澤　直行　氏氏

1．　講演内容

今回の講演は以下の内容で行われた。

（1） 医療情報システムの安全管理のために
（2） 医療情報システム安全管理評価制度
（3） 医療情報システム監査人試験制度
（4） 公認医療情報システム監査人認定制度

2．　講演の概要

（1） 医療情報システムの安全管理のために

医療情報については、個人情報の中でも機微情報が多く含まれているが、以前は紙による処理が多かったこともあり、医療情報の取り扱いについて、問題になることは少なかった。しかし、平成 11 年（1999）4 月の「電子保存に関する 3 局長通知」以降、医療情報の電子媒体による保管が認められ、その後医療情報の外部保管も認められ、また医療情報システムの進展に伴い医療情報に関する事故も増加してきた。

このような状況を踏まえ、厚生労働省としても、注意喚起の通知をいくつか発出するに至っている。

医療情報の多くは、個人情報に該当するため個人情報保護法により保護されるが、医療情報を扱う医療機関は民間のものと公的なものがあることから、その設立基盤の違いにより適用される法律が異なることに注意する必要がある。

医療分野における研究分野以外（一般）の個人情報保護ガイドラインは、4 つあるが、基本的なガイドラインは「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン（局長通達)」と「医療情報システムの安全管理に関するガイドライン（局長通達)」である。

前者は、医療機関が行う個人情報の適正な取り扱いの確保に関する活動を支援するための指針である。このガイドラインでは医療・介護分野の特質を踏まえ、要求レベルを引き上げている。この中で、医療機関等において、医療情報システムを導入したり、診療情報の外部保管を行う場合には、「医療情報システムの安全管理に関するガイドライン」によると規定されている。

後者は、電子保存に関するガイドラインおよび医療・介護関連機関における個人情報保護のための情報システム運用管理を対象としたガイドラインとなっている。

当該安全管理ガイドラインは第 1 版が平成 17 年（2005）3 月に策定されて以降、第 2 版から第 4.1 版（平成 22 年（2010）2 月）まで、ほぼ毎年改訂されている。

なお、当該安全管理ガイドラインは医療情報システムの利用者である全ての医療機関に対するガイドラインであるとともに、医療情報を受託管理する情報処理事業者、および医療情報を取り扱う ASP・SaaS 事業者に対するガイドラインでもある。

また、当該安全管理ガイドラインは iMISCA のホームページからもダウンロード可能である。
http://misca.jp/index.php?ダウンロード

（2） 医療情報システム安全管理評価制度

（財）医療情報システム開発センター（MEDIS-DC）は昭和 49 年（1974）7 月に、医療のシステム化推進のため厚生労働省、経済産業省共管の財団法人として設立された。

当該センターの主な事業としては、「標準化」、「導入支援」、「医療情報の安全管理」、「その他」がある。そして「医療情報の安全管理」の具体的な内容として、「保健医療福祉分野のプライバシーマークの付与認定審査」、「医療情報システム安全管理評価制度（PREMISS）」、「医療情報システム監査人試験制度」がある。

「医療情報システム安全管理評価制度（PREMISS）」とは、「医療情報システムの安全管理に関するガイドライン」への準拠生を第三者が客観的に評価する制度であり、2011 年 8 月現在 4 医療機関が評価を受けている。

当該 4 件の評価における共通課題の一つとして、「医療情報システムに対する監査が未実施」が挙げられ、定期的な情報システムの監査を実施できる体制整備と人材育成が求められている。

（3） 医療情報システム監査人試験制度

当該試験制度は、医療情報システム安全管理評価結果における課題である「定期的な情報システムの監査を実施できる体制整備と人材育成」に対処するため、一般財団法人医療情報システム開発センターが実施主体となって実施する試験制度である。

当該試験は、保健医療福祉分野のシステム内部監査に関わる人（医療機関等の職員、ベンダの社員等）を対象としており、当該試験の出題範囲は以下の通りである。

・第一科目（医療情報システムに関する知識）
・第二科目（監査に関する知識）
・第三科目（法律、ガイドラインに関する知識）

また、当該試験制度には免除制度があり、医療情報技師については第一科目（医療情報システムに関する知識）が、システム監査技術者、専門監査人（CMAIS,CMAPP,CMAAS）、公認システム監査人（CSA,ASA）、公認情報システム監査人（CISA）、公認情報セキュリティ監査人（CAIS）については第二科目（監査に関する知識）が免除されている。

当該試験は第 1 回が 2011 年 6 月 19 日に実施された。試験結果の概要は以下の通り。

・受験者数 308 人、合格者数 142 人、合格率 46.1%
・合格者の勤務先では保険医療福祉施設 28%、教育研究機関 3%、企業 67%、行政機関・他 2%
・当該試験の対策講座として「到達度確認講習会」があるが、当該講習を受講した人の合格率は 57.4%であるのに対し、未受講者の合格率は 37.2%に留まった。
・科目免除と合格率の関係では、「免除科目なし」：31.1%、「第一科目免除」：56.2%、「第二科目免除」：25.5%、「第一・第二科目免除」：64.3%となっており、医療情報技師の資格保有者の合格

率が高い一方、監査資格保有者の合格率が低くなっている。

（4） 公認医療情報システム監査人（MISCA）認定制度

当該制度は医療情報システムの監査が出来る人を認定する制度として、一般社団法人医療情報安全管理監査人協会（iMISCA：2011 年 4 月 1 日設立）が実施主体となって行われる認定制度である。

公認医療情報システム監査人（MISCA）の認定要件は以下の通り。

① MISCA 補（3 年毎の更新）

・医療情報システム監査人試験に合格していること

・医療情報システム監査人としての行動を約束できること（倫理規程への誓約）

② MISCA（3 年毎の更新）

・MISCA 補の認定を受けていること（同時申請も可）

・所定の監査実績があること

・所定の保健医療福祉分野における実務経験があること

・面接（初回のみ）

③ 認定登録の特典

・認定・登録カードの発行（写真付き）

・ 協会のホームページで認定番号・氏名の公表（任意）

・監査人専用メーリングリストへの登録

・MISCA 資格保有のメリットは以下の通りである。

① 医療機関等のメリット

・医療情報システムの仕様を理解し、システムの安全性を自ら評価できる。

・医療情報システムの安全管理状況を定期的に把握することにより、安心して医療情報の利活用が可能となる。

② ベンダーのメリット

・自社が提供する医療情報システムやサービスのガイドラインへの準拠性を客観的に説明することが可能となり、差異化を図れる。

・提供後は、定期監査により、医療機関等に客観的な監査報告が可能となる。

③ 個人のメリット

・医療機関従事者は、自組織の監査を担当・実施することにより、より職務・職歴の幅が広がり、現在担当している職務に関する技術・知見が高まる。

・ベンダー勤務者は、自社が関連する医療情報システム開発時の監査を担当することにより、より職務・職歴の幅が広がり、現在担当している職務に関する技術・知見が高まる。

・自分が所属する組織では医療情報システムに関係していない場合、iMISCA に登録することにより、医療情報システム監査の支援・実施依頼を受けて監査を実施・支援できる。

3． 質疑・応答

講演終了後、活発な質疑・応答があった。その中から、システム監査人の立場から重要と思われるものは以下のとおり。

（質問１）:公認医療情報システム監査人認定制度は､医療機関内の職員をターゲットとしているのか。

（回答１）: 当該制度は、医療機関等に内部監査を広めていくことを第一義としており、ベンダーを牽

制するという観点からも医療機関内の職員が内部監査を担当することが一番望ましいと考えている。

（質問２）:「公認医療情報システム監査人（MISCA)」の認定条件として、「所定の保険医療福祉分野における実務経験があること」があるが、ベンダー勤務者等、保険医療機関に勤務していない人は、この条件をどのようにクリアーしたらよいのか。

（回答２）:現時点では、医療情報技師の資格取得により当該条件の代替を考えている。

４．　所感

今回の講演を聴いた感想は以下の通りである。

まず、現在では殆どの業務がシステムに依存しており、システムなしには業務を遂行することが難しい状況になっている。そのことからシステムを監査し、システムの信頼性、安全性、効率性、有効性を確保することが益々求められる時代になってきている。しかし、システム監査を適切に実施するためには、システムや監査に関する知識・技量だけでは不十分であり、監査対象の業務に関する知識も求められる。

そのことから、システム監査学会では専門監査人制度を立ち上げ、分野毎の専門監査人を認定している。今回の「公認医療情報システム監査人（MISCA）制度」もその延長にあると考えられる。一人の監査人が全ての業務分野を適切に監査することは難しく、今後専門分野に熟達した監査人の認定が進展していくことと思われる。

次に、「公認医療情報システム監査人（MISCA）制度」に関する疑問である。本制度は講師の説明の通り、医療機関等における内部監査人を育成することを第一義としている。そして、当該システム監査人としては医療情報技師を想定しているとのことであった。しかし、医療情報技師は医療機関内において、情報システムの企画・導入・運用・保守・外部委託管理等を中心に担当している職員と想定される。つまり、正にシステム監査を受ける立場の人である。その人が、システム監査人となって自医療機関等のシステムを監査することは自己監査となってしまうのではなかろうか。このことに関する論理的な整理が必要と思われる。

＜係りより＞

今回は会員の勝田敦彦氏に報告記事をお願いしました。この記事を相澤直行氏に確認いただいた際に、上記所感に対して以下のコメントをいただきました。

＜疑問に対する考え方＞

一般的な病院では、医療情報システムの導入から運用・保守までベンダーに頼っている現状がある。安全管理ガイドラインの対象は、導入、運用だけでなく、利用、保守及び廃棄に関わる人又は組織まで対象としていることから、監査対象は広く、システム部門に止まらない(各診療科におけるシステムの運用状況も含む)。従って、医療情報技師が内部監査を実施することについては、ベンダーへの牽制となることもあり自己監査となる以上にメリットがあると考えている（自己監査は、システム部門は他の部門の職員が監査することにより回避できる)。もし、ベンダーを使わず自病院で開発したシステムであるなら、外部監査である「医療情報システム安全管理評価制度(PREMISS)」を併用することが望まれる(審査事例あり)。

■　【近畿支部主催　「事例に学ぶ課題解決セミナー（半日コース）」開催報告】

近畿支部　　吉谷尚雄

セミナーは７月２３日１３：００～１６：５５まで、ＪＲ大阪駅から徒歩１０分の距離にある「毎日インテシオ」３階の「常翔学園大阪センター」で計画通りに開催されました。
プログラムは広瀬克之講師、是松徹講師及び三橋潤講師により、受講生８名に対して実施されました。
広瀬講師：「事例講義：大手電機メーカの統合システム構築の障害」（課題解決の進め方について詳細な講義がありました。）それを受けて是松講師：「簡易演習：医療機器メーカの統合システム構築工程の障害」（簡易演習を実施し、現場の人に話を聞くことの重要性を強調しました。）　最後に三橋講師：「講義（まとめ）：リスク管理とシステム監査」（発生した事象からリスク管理として何が足りなかったのかを見出し、再発防止につなげる「システム監査」を解説しました。）

会場の「常翔学園大阪センター」は教育施設として明るく清潔でＡＶ設備も完備し、快適な環境でセミナーは計画通りに実施されました。セミナー受講生に記入して頂いたアンケート結果から、全体として良い評価を得ることができました。アンケートの自由意見欄では、「受講者同士や講師とのディスカッションの要素も欲しい」、「日々行っているリスク管理とは視点が異なる・・・」などの意見があり、今後の課題も得ることができました。

以上

注目情報（10/1～10/31）

■【IPA は、組織の重要情報の窃取を目的としたサイバー攻撃に関する注意を喚起】（IPA 2011/9/20 発表）

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、9 月 20 日（火）、組織における知財や個人情報を狙ったサイバー攻撃事件が目立っており、昨今も攻撃を受けていた事件が報道されたことを受け、組織のシステム管理者に対し、広く対策の徹底を呼びかけるため、注意喚起を発した。

近年、組織の知財情報や個人情報等の窃取を目的とした攻撃が増加している。サイバー攻撃は、公開されているサーバーへの攻撃だけではなく、特定企業や公的機関を狙い、ソフトウェアの脆弱（ぜいじゃく）性を悪用し、複数の攻撃を組合せ、人間の心理・行動の隙を突く手法を用い、対応が難しいサイバー攻撃（IPA ではこのような攻撃を「新しいタイプの攻撃」 と呼ぶ）が問題になっている。 「新しいタイプの攻撃」は、端末がウイルスに感染してしまうと、組織内に拡散するだけでなく、攻撃者との通信によるウイルスの機能増強や、組織内の情報探査を行い、それらの情報を攻撃者へ送信したりする。場合によっては、組織の活動に関わる秘密情報や設計図などの知財情報などが攻撃者に窃取されてしまう。

組織のネットワーク管理者は、早期発見の備え、事後対応など、トータルなセキュリティ対策を徹底し、また、不正アクセスや侵入、ウイルス感染の検知時は、IPA へ早急に届出てほしい。

詳細は　→ http://www.ipa.go.jp/about/press/20110920.html

■【「サイバーインテリジェンス情報共有ネットワーク」を構築】（警察庁 2011/9/21 発表）

警察庁は、「標的型メール攻撃事案の把握状況について」と題して以下の発表を行った。

警察では、情報窃取の標的となるおそれのある全国約4,000の事業者等と「サイバーインテリジェンス情報共有ネットワーク」を構築し、標的型メール攻撃等の情報窃取を企図したとみられるサイバー攻撃事案に係る情報を集約し、これらの情報を総合的に分析して事業者等に対する注意喚起を実施。

このネットワーク等を通じた情報収集により、震災後、「地震情報」、「被ばくに関する知識」、「計画停電」等の震災や原発事故に関する情報の提供を装った標的型メールが我が国の民間企業等に合計500件以上送付されていることを把握。

詳細は　→　http://www.npa.go.jp/keibi/biki5/hyotekigata.pdf

〈標的型メールの特徴〉　ＩＰＡの記事による　→　http://www.ipa.go.jp/about/press/20100602.html

① メールの受信者が信頼することを狙った、官公庁をかたる送信元と署名
② 宛先は業務用メーリングリスト
③ メーリングリストの用途に合わない件名
④ 添付ファイルは PDF ファイル（実態は Adobe Reader に存在する脆弱性を利用し攻撃を実行するマルウェア）
⑤ 件名と結びつかない本文

全国のイベント・セミナー情報

■ 【東京・月例研究会】

【１０月の月例研究会】

開催日時　：２０１１年１０月２８日（金）１８時３０分から２０時３０分
場所　：御茶ノ水　総評会館２階大会議室
講演テーマ　：「BCMS 適合性評価制度の現況と ISO 化の進展」
講演者　：一般社団法人日本情報経済社会推進協会
情報マネジメントセンター 副センター長 高取敏夫 氏

【１１月の月例研究会】

開催日時　：２０１１年１１月２４日（木）１８時３０分から２０時３０分
場所　：御茶ノ水　総評会館２階大会議室
講演テーマ　：「サイバー犯罪の現状と警察庁の取組み」（仮題）
講演者　：警察庁生活安全局情報技術犯罪対策課
専門官 人見友章 氏

■ 【システム監査実務セミナー４日間コース】

日本システム監査人協会では、設立目的のひとつである「システム監査人の実務能力の維持・向上」のため、毎年数回、セミナーを開催しています。

今回ご案内するセミナーは、COSO-ERM モデルが提唱する、企業のリスク低減を図るためのシステム監査を目指す、「システム監査実務セミナー」（４日間コース　１泊２日２回）です。

企業の経営戦略及び業務の有効性と効率性の向上を図るためには、情報システムの活用が必須であり、その評価・改善を進めるためには、システム監査を実施することが有効です。

これまで実施されてきた業務監査（システム監査）では、現場の業務評価の視点を重視した監査が多く見受けられています。

今後は、コーポレートガバナンス、内部統制の面から、業務評価の視点に加えて、経営リスクに対する業務システムの有効性、効率性、安全性の向上の観点からの評価・改善提案が重要になってきます。

本セミナーは、当協会のシステム監査事例研究会で実施した、「システム監査サービス」の実際の監査事例を教材として、ロールプレイを中心とした演習ベースのきわめて実践的なコースで、全社的リスクマネジメントの枠組み（①経営戦略への貢献、②業務の有効性と効率性、③報告の信頼性、④関連法規の遵守）に ついてよりよく理解し、経営に役立つシステムの実現に資するシステム監査の方策を理解・修得することを目標にしております。

なお、本セミナーを受講した後、事後課題を提出頂き、その内容が適切であると判断された場合には、当協会が認定する公認システム監査人の認定に必要なシステム監査実務を 1 年間経験したものとみなされます。

本セミナーは、IT コーディネータ協会の「専門知識研修コース」(5.5 ポイント相当)に認定されています。

1. 日程及び会場

平成 24 年 1 月 21 日(土)～22 日(日)

平成 24 年 2 月 4 日(土)～5 日(日)　　＜1 泊２日２回＞

どちらか一方のみの参加は不可

※　原則として、宿泊必須となりますが、事情により宿泊が難しい場合は、ご相談ください。

時間：土曜は 10:00～21:00、日曜は 09:00～15:00

（進行状況により若干の変更が生じる場合があります。）

会場：　晴海グランドホテル

〒104-0053 東京都中央区晴海 3-8-1

電話番号： 03-3533-7111

（最寄り駅　都営地下鉄大江戸線勝どき駅下車徒歩８分）

2. 費用　　168,000 円（日本システム監査人協会会員）

189,000 円（一般）

（費用には、主教材費・宿泊費・食事代・消費税が含まれます。）

3. 副教材

情報システム監査実践マニュアル(第 2 版)　森北出版社　5,460 円

お近くの書店等にてご購入ください。

※工業調査会版の同名書をお持ちの場合は、内容は変わりませんので、新たに購入する必要はありません。

4. 受講していただきたい方

情報処理技術者(システム監査)資格保有者もしくは同等の知識を有する方、または内部監査、システム監査の経験がある方

（上記条件に当てはまらない方は、お問合せください）

1)　企業・官公庁にお勤めの方

：監査部門（内部監査部・室、内部統制部・室、監査役室など）の方

：業務改善部門（企画部・室、事務管理部・室、など）の方

：経営戦略・予実算管理部門（企画部・室、総務部、経理部など）の方

2)　教育・研究者の方

：経営学の部門で教育・研究に携わっている方

：情報学の部門で教育・研究に携わっている方

3)　個人の方

：システム監査の実際を体験してみたい方

：システム監査技術者試験には合格したもののシステム監査参加機会のない方

：公認システム監査人の資格認定を目指している方

：CISA を取得したもののシステム監査参加機会のない方

：監査業務への異動、転職を目指されている方

6. 募集人員　　定員２０名（最小催行人員１０名）

7. 受講申し込み方法

以下の URL からお申し込みください。

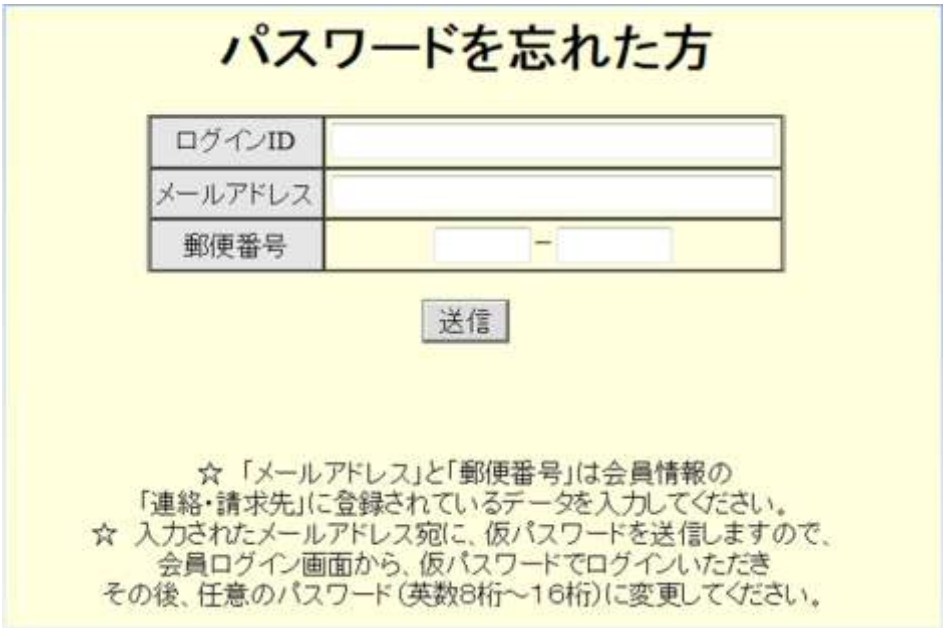
http://www.saaj.or.jp/kenkyu/jitsumuseminar19.html

事務局からのお知らせ【会員サイトへのログイン】　2011.9.23

§ 会員は、協会ホームページから会員サイトにログインして、
ご自分の情報を変更することができます。

URL：https://www.saaj.or.jp/members_site/KaiinStart

§ パスワードを忘れた方は、以下のページに進んでください。



§ 会員サイトでは、理事会議事録の閲覧などができます。

§ 会員情報変更画面で、会費納入日やCSA/ASA更新日の確認などができます。
（入会年月日は工事中で、表示されない場合があります。）
この画面で、住所変更、所属変更、メールアドレスの変更などができます。

以上

（SAAJ事務局）

■□■ ＳＡＡＪ会報編集担当より　お知らせ

会員の皆様からの、投稿を募集しております。分類は次の通りです。

１．めだか　　（Word の投稿用テンプレートを利用してください。会報サイトからダウンロードできます）
２．会員投稿　（Word の投稿用テンプレートを利用してください）
３．会報投稿論文 （論文投稿規程があります）

これらは、いつでも募集しております。 気楽に投稿ください。
特に新しく会員となられた方（個人、法人）は、システム監査への想いやこれまで活動されてきた内容で、
システム監査にとどまらず、IT 化社会の健全な発展を応援できるような内容であれば歓迎いたします。

次の投稿用アドレスに、テキスト文章を直接送信、または Word ファイルで添付していただくだけです。
投稿用アドレス：saaj-kaihoh ☆ yahoogroups.jp （☆は投稿時には＠に変換してください）

会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

■□■ 会報の記事に直接コメントを投稿できます

会報の記事は、
1）PDF ファイルの全体を、URL（http://www.skansanin.com/saaj/）へアクセスして、画面で見る
2）PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る
3）会報 URL（http://www.skansanin.com/saaj/）の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。
もっと突っ込んだ、便利な利用法はご存知でしょうか。

気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。。
コメント記入、投稿の方法は、動画で紹介していますので、参考にしてください。
（http://www.skansanin.com/saaj/ の記事、「コメントを投稿される方へ」 ）

■□■ 会報投稿記事２０１１アワード開催のお知らせ　（予告）

会報では、会報記事の投稿者に図書カードを配布しておりましたが、配布事務の負荷が大きいため、

年間アワードの方式に変更を計画しています。

つきましては、正式な実施要領は12月号で案内しますが、次の通り、会員の投票形式により、受賞記事を選んでいただく方式とさせていただきます。アワードの実施に伴い、従来の図書カード配布方式は、なくなります。

対象投稿記事

2011 年会報アワード　:2011/1-12 までの会報に掲載された記事を選定の対象とします

アワードの種類:

SAAJ めだか賞、

論文賞、

奨励賞　など、3点を選定し、記念品を贈呈する予定。

選定方法　:

投票機関を定め、投票用のツールを案内します。

投票には、SAAJ の会員が1票を投票できます。期間内に投票された投票を単純集計して判定します。

会員は、候補記事の中から、受賞にふさわしいと思う記事を選んで、期日内に投票いただきます。

得票数の多い記事をアワードの対象とします。

投票期間:

12/1 より 12/31　の 23:59 まで(予定)

会員限定記事

【本部・理事会議事録】(会員サイトから閲覧ください。パスワードが必要です)

■発行：　NPO 法人　日本システム監査人協会　会報編集部

〒103-0025　東京都中央区日本橋茅場町２－８－８共同ビル６F

■ご質問は、下記のお問い合わせフォームよりお願いします。

【お問い合わせ】　http://www.saaj.or.jp/toiawase/

■送付停止は、購読申請・解除フォームに申し込んでください。

【送付停止】　http://www.skansanin.com/saaj/

■□■ＳＡＡＪ会報担当

編集： 竹下和孝、仲　厚吉、安部晃生、成 楽秀、桜井由美子、清水恵子、山田 隆、片岡 学、

木村陽一、藤野明夫　　投稿用アドレス：saaj-kaihoh☆yahoogroups.jp（☆は安全対策）