特定非営利活動法人
日本システム監査人協会報

2011 年 9 月発行
No 127

No. 127（2011 年 9 月　発行）

会報電子版の記事　目次

めだか　【 オフショア開発と日本の開発力 】　　投稿

近年、中国を中心とするオフショア開発は大手企業を中心に益々増加の傾向にある。オフショア開発を発注している、または、受注している組織に対するシステム監査を考えてみると同時にここから見える日本のソフトウエア開発力や国際的な技術者の将来に関する懸念について考えてみたい。オフショア開発を考えるとき、特徴的に必要な視点・観点として両国の文化や言語、距離の克服に対する取り組みが挙げられるが、関連する特徴として両国の文化を理解し日本語が堪能な中国人ブリッジSEの存在がある。私自身、数年来、オフショア開発管理基準の作成に携わってきており、現在2つの中国のオフショア会社の顧問として開発現場の助言を行うほか、某大手企業のオフショア開発のブリッジSE研修の中国での講師経験、中国の東北大学でのオフショア開発に関する1ヶ月間の集中実践開発講座の講師を担当してきた。これらの様々な経験からオフショア開発をとりまく課題と、そこから垣間見える日本のソフトウエア開発力の将来について考えてみたい。

1　オフショア開発の課題

(1)文化・常識の克服

オフショア開発の発注側と受注側はお互い外国の関係にある。日本で常識だと思っても中国では通用しないかもしれない。どちらが良いとか悪いではなく、お互いに誠意をもって丁寧に話し合い、共通の理解を持つことが重要である。ブリッジSEはこの点、相当努力しているが、日本側の理解も非常に重要である。

(2)言語の克服

現在のオフショア開発の橋渡しは日本語が堪能で技術的能力も高い、ブリッジSEが担当している。しかし、日本語の細かい部分は相互理解が難しい場合が少なからず存在する。会話は得意でも日本語の資料作成は苦手な人が多く、このような時は発注側として文章や図表を使い確実に要件や会議記録を伝えることが重要である。

(3)距離の克服

中国は近いと言っても少なくとも半日を要し、内陸の場合は丸1日必要で費用も嵩む。このため、頻繁に顔を合わせての会合はできない。しかし少なくとも最初と中間には現地での打ち合わせを行い、様々な観点でモニタリングを行うことが開発リスクを軽減する視点から肝要であると思われる。

2　中国の会社組織の特徴

中国は法治より人治の色彩が強いと聞くことがあるが私もそのように思う。ルールがあっても運用に大きな幅がある。形式は守るが実態は良く聞かないとわからない面がある。ノウハウは人には溜まるが組織に残ることは少ない。情報伝達する場合、一人ではなく、必要な複数の人に伝えるとか、重要な事項は文書で伝える必要がある。

3　拡大する中国市場と日本人国際技術者の育成

日中オフショア開発のブリッジSEの殆どは中国人である。現在何人いるか不明だが数百人はいると思われ、大学での育成も盛んである。彼らは日本で苦労しながら中国本国でのソフトウエア工場に開発条件を伝え納入まで責任を持つ。当然、システムのキー技術も習得してゆく。 近い将来の巨大な中国ソフトウエア市場に日本は参入できるか？中国文化を理解し中国語を使って仕事を獲得・日中間の調整をして開発を主導できる日本人ブリッジSEやマネージャは存在できるか？これらについて非常に懸念される。オフショア開発の実態を知れば知るほど、少なくともこれらに対応できる人材育成や教育のための企業・大学横断的な仕組みを急ぐ必要がある。（ロン）

（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。）

めだか　【 エンロン和解金 】　投稿

取引の終わった証券会社から簡易書留がきた。

すでに解約した公社債投信にエンロンの社債が組み込まれており、エンロン破綻に伴う集団訴訟手続（クラスアクション）で、和解金が取れたので、当時の償還時受益者に分配する、というのである。

当方の口座は、投信本体は解約してあったが、付属していた普通預金的な口座の解約が遅れており、その残高￥1,519に対し、￥20支払うという内容である。

同封されている案内の中に、Ｑ＆Ａがある。

Ｑ１：当時エンロンの社債を組入れていたのはなぜか。
Ａ：当時、エンロンの社債に対する大手信用格付業者の格付は、投資適格であり、安全性は高いと判断され、利回りなどを考慮の上、組入れられていた。

Ｑ２：エンロン社の経営破綻で損失が出たのか。
Ａ：エンロン社は、2000年度に全米売上高第７位の企業に急成長したが、巨額の不正経理、不正取引に支えられていたことが明るみになり、同社の社債価格が想定外に下落した。当社の公社債投信でも保有していたどう社債を売り、損失計上したことにより、損害が発生した。

Ｑ５：なぜ返金まで約10年もかかったのか。
Ａ：（集団訴訟で和解することになり）2008年9月に裁判所で和解金の分配案が承認され、公社債投信の受託銀行が和解金を受領したが、国内における関係者も多く、返金スキームの確立に時間を要した。

事情はわかったが、￥20受け取るのに、振込先指定書など返送するのも面倒で、問合せ先に電話した。
「￥20受け取るのも面倒だが、受け取らないといったら、そちらは手間がかかるか」と聞けば、「手間はかかりません。この電話で放棄の意思を確認させていただきます」。

エンロンのおかげでＳＯＸ法ができ、あるいは、ビジネスチャンスがふえるかとも考えたが、個人事業主では、お勉強の手間と実入りを比べれば、とうていプラスとはいえない。

思いもかけない和解金の分配も、￥20ではどうにもならない。
エンロンへの悪い印象は、ぬぐえないままなのである。

（左平次）

（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 (5 章)】

榎本 吉伸

(この投稿は 8 月号に掲載したレポートの続きです。)

5. 関連公表文書における保証業務に係る意見等の調査・研究

5.1 **「情報セキュリティ監査研究会報告書」**(経済産業省：2003 年 03 月 26 日)

近年､インターネットの急速な普及および情報システムにおけるセキュリティ対策の不備に起因する様々な問題が生じ、社会的な影響がより深刻なものとなり、いわゆる「情報セキュリティ監査」分野についての制度整備が遅れていることが喫緊の課題として浮上してきた。これにより、2002 年に経済産業省において「情報セキュリティ監査研究会」が設置され､情報セキュリティ監査の普及とそのあり方の検討が行われ､2003.03.26 付けで「情報セキュリティ監査研究会報告書（以下、研究会報告書という。)」として報告された。

この研究会報告書には、別添資料として以下の資料が報告された。

・別添資料 1：情報セキュリティ管理基準（Ver1.0）
・別添資料 2：個別管理基準（監査項目）策定ガイドライン（Ver1.0）
・別添資料 3：電子政府情報セキュリティ管理基準モデル（Ver1.0）
・別添資料 4：情報セキュリティ監査基準（Ver1.0）
・別添資料 5：情報セキュリティ監査基準　実施基準ガイドライン（Ver1.0）
・別添資料 6：情報セキュリティ監査基準　報告基準ガイドライン（Ver1.0）
・別添資料 7：電子政府情報セキュリティ監査基準モデル（Ver1.0）

本レポートでは、別添資料 4、別添資料 5、別添資料 6 について、次項以降で取り上げる。

本研究会報告書においては、検討の背景等、情報セキュリティ監査の全体的な論点はともかくとして、特に「保証型監査の要請」の項に置いて、「保証業務係る監査」について積極的に取り上げている（公表年月日としては、「意見書」より先である)。従って、本レポートでは保証業務等に関連する項を中心として、以下の項目を取り上げる。

①情報セキュリティ監査の対象（システムではなく情報資産）
・情報セキュリティ監査の定義
②多種多様な組織体のニーズに応じた監査制度
・保証と助言（保証型監査の要請等）
・助言型監査から保証型監査へ
③「情報セキュリティ管理基準」策定の考え方
④「情報セキュリティ監査基準」策定の考え方
⑤法的関係についての論点整理（監査を行う主体、被監査主体に関する法的関係）

5.1.1 情報セキュリティ監査の対象（システムではなく情報資産）

研究会報告書には、「情報セキュリティ監査は、情報技術（IT)に関連するいわゆる情報システムのセキュリティだけではなく、より広く「情報資産」（information assets）全体のセキュリティの確保を目的とすることが適当である。」とある。

システム監査との違いを明確にする意図であろう。併せて、ここに「情報セキュリティ監査の定義」を別の項から引用すると、以下の通りである。

「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように､リスクアセスメントに基づく

適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与えあるいは助言を行う活動」と定義されている。

5.1.2 多種多様な組織体のニーズに応じた監査制度

ここでは、保証型監査を論じるべく、その前段階としての助言型監査に触れている。

「保証型監査の要請」として、「情報セキュリティ監査を受けるニーズとしては、まず、第三者（民間企業であれば取引先や顧客、政府関係機関においては国民等）に対して、自らの情報セキュリティ対策についての『お墨付き』を得ることを目的とすることが考えられる。」とあり、情報セキュリティ監査の本来の目的は「保証型監査」であるという基本的スタンスに立っているものと考えられる。このことは後述する、「保証型情報セキュリティ監査概念」（日本セキュリティ監査協会）の報告においても明らかである。

このような前提に立ち、次のように「保証型監査の定義」をしている。

「監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールが監査手続を実施した限りにおいて適切である旨（又は不適切である旨）を伝達する監査の形態を『保証型監査』と呼ぶ。」

引き続き、尚書きで「保証の範囲」を以下のように注記している。

「なお、この場合、『保証』といっても、結果としてインシデントが発生しないという絶対的な保証ではなく、一定の判断の尺度に従って監査手続を行った範囲における合理的な保証となることに留意が必要である。」とある。当然のことである。助言型監査については、本レポートの目的から省略する。

5.1.3 監査基準と管理基準

研究会報告書では、「情報セキュリティ監査の標準的な基準」として行為規範である「情報セキュリティ監査基準」と、この判断の尺度である「情報セキュリティ管理基準」の２つの基準に分け、両者の違いを明確にしている。別段、保証型監査の議論に大きな影響を与えるわけではないが、論点がより明確になると考えられる。

また、情報セキュリティ管理基準については、JIS X 5080:2002を元に作成されているので議論の必要はないが、「成熟度モデル」の項に、以下の記述がある。

「JIS X 5080:2002 をもとに策定する情報セキュリティ管理基準は、その性質上、全てのコントロールとその体系性がベストプラクティスを示したものとなる。したがって、我が国の現状に鑑みるとき、そのベストプラクティスの水準のみを判断の尺度とすると、保証型監査においては肯定型の保証が困難となり、また助言型監査においては指摘する乖離（ギャップ）が大きくなりすぎるという問題点がある。」とあり、ここでは成熟度モデルを各コントロールの達成度評価の尺度（モノサシ）として具体的に活用する考えを提起している。先進的で意欲的な試みであり、大いに賛同したい。

ただ現段階では、以下の成熟度モデルの３例を示すのみに留めている。

①Security Self-Assessment Guide For IT Systems（NIST）のIT セキュリティアセスメントフレームワークのモデル

②Cobit Ver.3 の成熟度モデル

③SSE-CMM 2.0(ISO/IEC 21827)の成熟度モデル

この利用については、後述の「平成 20 年 情報セキュリティ監査制度利用促進事業実施報告書」（日本セキュ

リティ監査協会）に詳しい。

保証型監査に関して、これ以上突っ込んだ具体的な議論は、各別添資料に委ねられている。

5.1.4 法的関係についての論点整理（監査を行う主体、被監査主体に関する法的関係）

保証型監査においては、法的責任問題が重要となる。それを意図して、法的関係についての論点整理が述べられているので、抜粋して紹介する。

①監査を行う主体に関する法的関係

情報セキュリティ監査を行う主体に対しては、a. 被監査主体に対する法的責任、b. 監査結果を信頼した第三者に対する法的責任が発生する可能性がある。

a. 被監査主体に対する法的責任

「監査を行う主体は、監査の依頼者である被監査主体に対する契約上の責任と、不法行為責任を負う可能性がある。このうち、契約上の責任を明確にするためには、①契約の書面化、②契約における監査の判断の尺度の具体化が有益であると考えられる。」とある。保証型監査において、特にこれらが重要である所以である。

b. 監査結果を信頼した第三者に対する法的責任

この問題は、「抽象的には論じ得ず、被監査主体、監査を行う主体及び第三者の関係なども踏まえて具体的に確定していくほかにないものと考えられる。」とある通り難しい問題であるが、これについても前項同様、「契約内容の明確化」および「監査における判断の尺度の具体化による保証内容の明確化」が重要であろう。

②被監査主体に関する法的関係

「情報セキュリティ監査を利用した情報セキュリティマネジメントの確立は、訴訟リスクを軽減する可能性があると考えられる。」とあり、情報セキュリティマネジメント確立が責任の軽減に貢献する可能性に言及している。卓見である。

5.2 **「情報セキュリティ監査基準（Ver1.0）」**（経済産業省：5.1 の別添資料 4）

情報セキュリティ監査研究会報告書の別添資料である「情報セキュリティ監査基準（Ver1.0）」では、システム監査基準（2004.01.08 改訂版。以下、同じ）と同様に、目的等で「保証」と「助言」を併せて対象範囲としている。内容については、「システム監査基準」とほとんど差異はなく、保証業務に固有の記載もない（システム監査基準が後付で改定された）。

尚、情報セキュリティ監査における基準は、システム管理基準と同様、監査基準に併せて別添資料 1 の「情報セキュリティ管理基準」を使うことは、周知の通りである。

5.3 **「情報セキュリティ監査基準　実施基準ガイドライン（Ver1.0）」**（同 5.1 の別添資料 5）

本ガイドライン（以下、「実施基準ガイドライン」という。）は、「情報セキュリティ監査基準」のうち「実施基準」に係る基本的な考え方を踏まえ、特に留意すべき事項、および情報セキュリティ監査実施上の手順について示されたものである。

実施基準ガイドラインでは、保証業務についての記載があるので紹介する。

尚、保証業務に関する記載以外の事項は既知の内容としてここでは取りあげない。

＜Ⅰ．情報セキュリティ監査実施上の前提事項＞

5.3.1 「情報セキュリティ監査の目的」としての保証型監査

「Ⅰ．情報セキュリティ監査実施上の前提事項」の「2.1 情報セキュリティ監査の目的設定」では「情報セキュリティ監査の実施に当たっては、監査の目的があらかじめ設定されていなければならない。」とあり、「情報セキュリティ監査には、組織体が採用している情報セキュリティ対策の適切性に対して一定の保証を付与することを目的とする監査（保証型の監査という）と、情報セキュリティ対策の改善に役立つ助言を行うことを目的とする監査（助言型の監査という）がある。」とある。

①保証型の監査の意義（研究会報告書に同じ）

次に「実施基準ガイドライン 2.3 保証型の監査の意義」で保証型監査の定義が示されている。すなわち「保証型の監査とは、監査対象たる情報セキュリティのマネジメント又はコントロールが、監査手続を実施した限りにおいて適切である旨（又は不適切である旨）を監査意見として表明する形態の監査をいう。」

さらに「保証型の監査の結論として表明される保証意見は、情報セキュリティ監査人が「情報セキュリティ監査基準」に従って監査手続を行った範囲内での請合いであって、かつ当該監査手続が慎重な注意のもとで実施されたことを前提として付与される保証であることに留意する」と、合理的保証であることを明言している。

②助言型監査の意義

実施基準ガイドライン「2.4 助言型監査の意義」より、保証型監査と区別して理解する目的で定義を引用する。

「助言型の監査とは、情報セキュリティのマネジメント又はコントロールの改善を目的として、監査対象の情報セキュリティ対策上の欠陥及び懸念事項等の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を監査意見として表明する形態の監査をいう」

5.3.2 助言型の監査と保証型の監査の選択

①前提条件の検討

実施基準ガイドラインでは、「2.5 前提条件の検討」で、監査を実施する際に保証型／助言型を選択する要件として、「組織体が採用し運用している情報セキュリティ対策の内容と水準を考慮して、助言型の監査とするか、保証型の監査とするか、あるいは併用型の監査とするかの決定は慎重に行われるべきである。」とある。この決定は業務依頼者が行うものであり、客観的に決められるべきものではない。ここでは「保証型／助言型を選択する要件」として、「組織体が採用し運用している情報セキュリティ対策の内容と水準」により、必ずしも保証型が選択できるものではないことを言っている。「保証」できる水準でない場合や次項の段階的導入を考慮すべき場合を言う。

②段階的導入の検討

次に実施基準ガイドライン「2.6 段階的導入の検討」で、「情報セキュリティ対策は、環境条件の変化に応じて、段階的に内容の向上を図ることが現実的であることから、情報セキュリティ監査をそのためのモニタリング機能として位置づけることも有益である。その場合、助言型の監査から手掛け、被監査側の情報セキュリティ対策が一定水準に達した段階で保証型の監査に切り替えるという方策が考えられる」とあり、さらに「なお、保証型の監査では、継続して情報セキュリティ監査を受けることによってはじめて効果が得られることに留意する」とある。ここで何を言わんとしているのかはよく分からない。

③利害関係者の信頼獲得についての検討

さらに実施基準ガイドライン「2.7 利害関係者の信頼獲得についての検討」では、「不特定多数の利害関係者が関与する公共性の高い事業又はシステム等、あるいは不特定多数の利害関係者の情報を取扱う場合であっ

て高い機密性の確保が要求される事業又はシステム等については、保証型の監査を定期的に（例えば、1 年ごと）利用し、その監査の結果を開示することによって利害関係者の信頼を得ることが望ましい。」とある。保証型監査の定期的な実施と監査結果の開示を示唆している。

5.3.3 情報セキュリティ監査における成熟度モデルの利用

①「異なった保証水準の付与又は段階的な保証の付与」に関して

実施基準ガイドライン 3 項では「成熟度モデルの利用」について詳しく紹介されている。同 3.1 項では、「情報セキュリティ監査においては、監査対象の範囲又は実施すべき監査手続の内容等によって、異なった保証水準の付与又は段階的な保証の付与が可能であり、さらに情報セキュリティ対策上の欠陥等に係る検出事項及び改善提言の内容においても差異を付けることが可能である」とある。

この「異なった保証水準の付与」における異なった水準とはどのように決めるのか。成熟度モデルのレベルを示していると思われるが、監査対象組織により、またコントロール毎にレベルを変えた場合、その評価の一般性あるいは他の監査との比較公平性はどのように考えれば良いのか。また合理的保証業務としての水準とは如何なる相関関係があるのか。具体的にどのレベルであれば保証業務の水準として適正なのか、議論すべき点は残る。

異なった保証水準を「実施した監査手続ごとに設定した水準（ここではコントロール毎に予め定めた目標レベル）での保証」と考えてよいのであれば話は簡単である。実施した監査手続とその評価結果を明確に監査報告書に記載すればよいのである。

筆者も、ISMS 認証取得の内部監査を経験した際に、ISMS ではコントロールの運用状況評価におけるサンプリング試査で、評価するサンプル数が定められていないことが奇異に感じられた経験がある。またコントロールの保証水準として、例えば、コントロールとして「パスワードは定期的に変更すること」とある場合、評価尺度として「定期的に」とは月に一回なのか、年に一回なのかが明確で無い。尺度の程度で評価の水準が決まる。評価尺度となるコントロールの適切な水準が定められていないのである。この件については保証型業務では極めて重要な要件と考えるので、後述する筆者の考え方を述べる際に言及する。

本項では、さらに「現に採用されている情報セキュリティ対策又は採用すべき情報セキュリティ対策の内容は組織体において異なり、一律の固定的水準を前提とした情報セキュリティ監査を行うことが現実的でない場合がある」とある。保証型システム監査において、組織体で採用している情報セキュリティ対策の水準に応じた保証をすればよいのであれば、基準とは評価尺度には関係せずコントロール項目を列挙したものに過ぎないことになる。

②合理的な範囲での保証又は助言

次に「3.2 合理的な範囲での保証又は助言」では、「情報セキュリティ対策の適否について保証を付与する限りは、監査報告書の利用者がその保証水準に合理的な範囲で信頼を置き、情報セキュリティ監査人にとっては監査責任を全うできるだけの保証水準が要求される」とある。この「監査報告書の利用者が合理的な範囲で信頼を置く保証水準」の水準と、前項の「異なった保証水準の付与」の水準とは一致するのであろうか。

さらにここでは、「情報セキュリティ対策の成熟度に応じた監査を行うことによって、保証型の監査においては保証の水準を明確にでき、助言型の監査においては段階的な情報セキュリティ対策の導入を推進することができる」とあり、成熟度レベルに応じた監査を行うことにより成熟度に応じた水準の保証を行うことを勧めている。

以上から、情報セキュリティ監査基準において合理的保証業務とは、当該組織体の情報セキュリティ対策の

実施レベルに応じた監査手続による評価で良いと言うことなのか。

③成熟度レベルに応じた保証又は助言

成熟度レベルの利用の項では、「3.3 成熟度レベルに応じた保証又は助言」で、「情報セキュリティ対策の成熟度モデルとは、組織体における情報セキュリティ対策を段階的に向上させることを目的に、組織体が設定又は運用する情報セキュリティ対策の実施水準を区別する考え方である。通例、組織体が設定又は運用する情報セキュリティ対策の実施水準を 5 段階にレベル分けすることが多い」。例えば、レベル 1 での実施水準を保証することが、保証業務と言えるのか。成熟度モデルの利用の場合は、そのモデルと保証水準レベルの明確化が重要である。

＜Ⅱ．情報セキュリティ監査の実施手順＞

5.3.4 実施すべき監査手続の概要

本ガイドライン「Ⅱ．情報セキュリティ監査の実施手順」では、「2.7 監査実施計画の立案」において、「情報セキュリティ監査人は、監査の基本的な方針に基づいて、実施すべき監査手続についての詳細な計画として、次の事項を立案する」として、立案事項の 4 項目に以下の記載がある。

・実施すべき監査手続の概要（必要に応じて、監査要点、実施すべき監査手続の種類、監査手続実施の時期、及び**試査**の範囲を含む（ゴシック体、筆者））

ここで特筆すべきは、「試査の範囲」と証拠入手手続の技法として“試査”が取り挙げられていることである。重要なことで、記憶に留めておいていただきたい。

5.3.5 監査手続の実施（監査証拠の入手と評価）

「3. 監査手続の実施」の 3.1 項で、「保証型の監査であれ助言型の監査であれ、情報セキュリティ監査人は、自らの監査意見を裏付けるに十分かつ適切な監査証拠を入手しなければならない。監査証拠は、保証意見又は助言意見の根拠となるものであるから、その時の状況に応じてもっとも適切な監査手続を選択適用した結果得られたものでなければならない」とあり、特に保証型と助言型で区別をしていない。

5.4**「情報セキュリティ監査基準　報告基準ガイドライン（Ver1.0）」**（同 5.1 の別添資料 6）

上記の実施基準ガイドラインに続き、「情報セキュリティ監査基準」の報告基準に係る基本的な考え方を踏まえ、監査報告書の雛形を示したガイドラインである（以下、「報告基準ガイドライン」という）。

保証型システム監査の内容を報告基準において具体的に示した意欲的な試みである。

5.4.1 監査報告書の意味と記載事項

①監査報告書の定義（省略）

②監査報告書の記載事項

監査報告書の記載事項は、次の記載区分によって構成されると整理されており、意見区分には「保証意見」も対象として記載され、次項でさらに保証型監査報告書について触れている。

・導入区分（実施した監査の対象等を記載する）
・概要区分（実施した監査の内容等を記載する）
・意見区分（保証意見又は助言意見を記載する）

・特記区分（必要に応じてその他特記すべき事項を記載する）

③監査意見の種別

監査意見の種別では、保証型の監査報告書に関する記載があり、以下のように説明されている。

・情報セキュリティ監査報告書は、情報セキュリティ監査の目的又は契約の内容によって、保証型の監査報告書（保証報告書という）が作成される場合と、助言型の監査報告書（助言報告書という）が作成される場合がある。

・１通の情報セキュリティ監査報告書において、保証意見を記載した後で、助言意見を記載することもある。

5.4.2 助言報告書作成上の留意事項（一部記載）

①助言意見の表明方法

助言意見の表明方法の 3 項目には、以下の記載がある。

「助言意見は、情報セキュリティ監査報告書の内部利用を前提とした場合に有効な意見表明方式である」。

5.4.3 助言報告書の雛形（省略）

5.4.4 保証報告書作成上の留意事項

①保証意見の表明方法

助言意見の表明方法と同様に保証意見の表明方法の 2 項目には、以下の記載がある。

「保証意見は、情報セキュリティ監査報告書の内部利用を前提とした場合にも有効な意見表明方式であるが、監査報告書の外部開示を前提とした場合には原則としてこの意見表明方式による」。保証意見はあまり内部利用では行われないと筆者は考えるが、如何なものか。また本来、内部利用のために行った監査の保証意見を外部利用することは適切でない。

②保証意見の類別

保証意見の類別では、以下の通り具体的な保証意見が紹介されており保証報告書作成の理解に役立つ。

・肯定意見

情報セキュリティ対策の全てに重大な欠陥がなく、適切である旨の保証。

・限定付肯定意見

情報セキュリティ対策の一部に欠陥があるか、又は情報セキュリティ監査人が必要と認めた監査手続が制約されたがその部分を除けば適切である旨の保証。

・否定意見

情報セキュリティ対策に重大な欠陥があり、情報セキュリティ管理状況が全体として適切とはいえない旨の保証。

さらに、本項の２項目には限定付肯定意見、否定意見について次の記載がある。

「限定付肯定意見及び否定意見は、情報セキュリティ対策に無視し得ない欠陥があることを監査意見として表明することになる。このことから情報セキュリティ監査報告書の外部開示を想定した場合には、必ずしも現実的でない」。契約が許されるなら、引き続き紹介されている次の示唆が現実的には有効であろう。「情報セキュリティ監査報告書の外部開示が想定される場合であって、肯定意見の表明が困難であると判断されるときは、助言型の監査に切り替えるか、又は一定期間をおいて被監査側による改善が図られた段階で監査に着手することが望ましい」

つづいて３項目には、「情報セキュリティ監査人が必要と認めた監査手続が制約され、保証意見の合理的な根拠を得ることができなかった場合には、保証意見を述べてはならない」とある。当然である。

5.4.5 保証報告書の雛形

①肯定意見の雛形

肯定意見の場合、本ガイドラインで報告書名は「情報セキュリティ監査報告書」とある。

ＩＴ実務指針では、同じセキュリティに関する検証についての合理的保証業務を対象としているが「独立した監査法人（公認会計士）の検証報告書」とあり、監査報告書でなかったことは既に述べた。立場の違いか。日本公認会計士協会の明確な説明が欲しい。

情報セキュリティ監査報告書（例）の主文の重要な箇所を紹介する。

「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。監査は、情報セキュリティに関わるリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づいて適切なコントロールが採用されているか否かについて検討し評価している。採用した監査手続は、われわれが必要と認めたものを適用しており、監査の結果として意見表明のための合理的な根拠を得たと確信している。われわれの意見によれば、200ｘ年ｘ月ｘ日から 200ｘ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」

尚、報告書の記載形式はＩＴ実務指針に詳しいが、ここでは以下の 2 方式が紹介されている。

・直接報告方式（主題そのものについて表明する方式）

上記の情報セキュリティ監査報告書（例）で、情報セキュリティ対策の実施状況について、直接、監査意見を表明するときには、「情報セキュリティ対策の実施状況について」と記載する。これを直接報告方式という。すなわち、主題そのものについて直接、監査意見を表明する方式をいう。

・言明方式（主題情報に基づく方式）

一方、直接報告方式に対して「言明方式」とは、主題情報である確認書（「適正言明書」ともいう。）を入手して、当該確認書について監査人が意見を表明する方法をいう。この場合は、「被監査側が作成した自己評価表に対する担当部門の責任者（又は組織体の長）による適正言明書が、情報セキュリティ管理基準に準拠しているか否かについて」と記載する。

尚、追記として「言明方式の方が、通例、意見表明に関わる情報セキュリティ監査人の責任を明確にしやすい」とある。

②限定付意見等の雛形

限定付意見には、次の 2 つの場合がある。

・情報セキュリティ対策の重要な欠陥等に基づく限定

・監査人が必要と認めた監査手続の制約に基づく限定

また、該当する欠陥等の重大さに鑑みて情報セキュリティ管理状況が全体として適切とは判断できないときには否定意見を表明する。

③合意に基づく監査手続とその結果のみを報告する方式の雛形

経済産業省から公表された基準関連では、本情報セキュリティ監査基準報告基準ガイドラインのみ、意見書等でいう「合意された手続」についての記載がある。

その定義は、本ガイドラインでは「外部監査人による監査において、選択適用すべき検証手続を監査依頼者と協議の上で決定し、それに対する結論のみを報告する業務」となる。

さらに「この報告書は、監査人としての保証を付与するものではない」旨、及び「この報告書は、外部の不特定の関係者に開示されることを前提としていない」旨を明記しなければならないのは、意見書等と同じである。尚、雛形の報告書名が「監査人による報告書」とあり、監査報告書ではなく“監査”の記載がないのは、筆者の考え過ぎか。

5.5 「システム監査基準」（経済産業省：2004 年 01 月 08 日改訂）

経済産業省が 2004 年度に改訂した「システム監査基準」（以下、「システム監査基準」という。）では、その前文に以下のように保証業務について言及している。

「Ⅰ前文　本基準は、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、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」とある。

また、「Ⅱ．システム監査の目的」には、「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」とあり、これ以降の関連する項でも同様に保証業務と助言業務の両方について併記している。特に保証業務の定義等、保証業務に固有のテーマを取り上げた記述は無い。

これは、経済産業省より新しく「情報セキュリティ監査基準（2003.03.26）」が公表されたことに併せてシステム監査基準も改定されたことによる。

このシステム監査基準については、次章で「保証型システム監査のフレーム」を議論する際に、システム監査基準に準じて詳しく見る。

尚、「システム管理基準」にも保証業務に関することは言及されていない。併せて、システム管理基準についても保証業務に係る観点から後述する。

5.6 情報セキュリティ監査制度利用促進事業実施報告書における「第 1 編 第 4 部 社会的合意方式における監査業務実施基準の検討」

（日本セキュリティ監査協会：2009 年 03 月 31 日）

日本セキュリティ監査協会（以下、「JASA」という。）は、「平成 20 年 情報セキュリティ監査制度利用促進事業実施報告書（以下、「実施報告書」という。）」をホームページ上に掲載している。

本実施報告書は、意見書や研究報告等のこれまでの監査の枠組みから離れて、情報セキュリティ監査に係る新たな枠組みの研究を行っている挑戦的で意欲的な試みである。

実施報告書では、第１編から第４編まで、以下の報告が行われている。

第１編　保証型監査促進プロジェクト報告
- 第１部　民間企業における保証型情報セキュリティ監査パイロット監査報告
- 第２部　サプライチェーンにおける保証型情報セキュリティ監査の活用
- 第３部　地方公共団体に於ける監査手続作成のための脅威対策表および利用ガイド
  ＜附録＞脅威対策表
- 第４部　社会的合意方式における監査業務実施基準の検討

第２編　情報セキュリティ管理基準
- 第１部　情報セキュリティ監査における監査手続策定ガイドライン（次項 5.7）
- 第２部　国際規格への成果展開などの標準化活動

第３編　普及促進部会
第４編　調査研究部会
　第１部　情報セキュリティ監査を取り巻く基準等に関する動向の調査
　第２部　情報セキュリティ監査制度に係る基準の枠組み検討結果
　本レポートでは、特に保証業務に係る情報セキュリティ監査を取り上げた報告書「第１編 第４部 社会的合意方式における監査業務実施基準の検討（以下、「報告書」という。)」についてのみ論ずる。

5.6.1 社会的合意方式
　報告書のタイトルは、「社会的合意方式における監査業務実施基準の検討」と“社会的合意方式”に限定されているが、JASA では、社会的合意方式に併せて、利用者合意方式、被監査主体合意方式の３方式の監査業務が検討されている。
まずこれら３方式の定義を、JASA のホームページより抜粋して明らかにしておこう。
①社会的合意方式
　「情報セキュリティ管理基準や監査基準に沿い、監査テーマに関して監査意見を表明するに十分な手続きをふみ、その結果をすべての利害関係者たり得る利用者に報告する方式」を社会的合意方式と呼ぶ。意見書等で言う「保証業務に係る監査」と同義である。
②利用者合意方式
　「被監査主体の情報セキュリティ対策に直接の利害関係を持ち、その適否や有効性に特定の期待や要求水準を示している監査報告書の利用者（１次利用者）が、監査人が採用する監査手続きの十分性について、暗黙または明示的に合意している場合の保証型監査」を利用者合意方式と呼ぶ。「利用者が監査手続の十分性について合意していること」が要件である。意見書等では「合意された手続」に分類されている業務である。
③被監査主体合意方式
　「被監査主体が、利害関係者に向けて説明するために、特定の監査テーマを定め、その監査手続きを監査人と相談し合意の上で定める場合で、かつ、監査テーマと監査手続きについて監査報告書の利用者の確認がある場合の保証型監査」を被監査主体合意方式という。「監査手続の十分性について被監査主体と合意され、利用者の確認がある」ことが要件である。
　被監査主体合意方式は、利用者合意方式との違いが少し分かり難いが、企業が業務の一部を他の企業に外部委託する場合が、これが適用される典型的なパターンであるという。委託元企業が利用者、委託先企業が被監査主体となるが、被監査主体合意方式は、委託先が自ら、委託元から求められている情報セキュリティ対策の実施状況につき保証を得たい場合で、利用者である委託元企業に監査手続等の了解（確認）を得て行う場合を言う。
　いずれも保証業務に係る三当事者間の関係が少し異なるだけで、意見書の分類では、利用者合意方式、被監査主体合意方式は「合意された手続」となるが、情報セキュリティ監査では、このような当事者間の関係は十分に具体性があり、「合意された手続」も「監査」と呼ぶことに賛同したい。

5.6.2 情報セキュリティ監査の本来の目的
　報告書の前文 2.項に、「また、情報セキュリティ監査業務は保証業務として実施されることが本来の目的であり、一般に「助言型」監査と呼ばれる業務は、いわば最終目的に至る過渡期におけるフェイズととらえられる。したがって本情報セキュリティ監査業務実施基準では、特に言及しない限り情報セキュリティ監査は、保

証業務としてそれを意味する。」とある。“情報セキュリティ監査業務は保証業務として実施されることが本来の目的”とある。情報セキュリティ監査の監査目標が機密性・安全性・可用性であるが故に、この言明は容易である。システム監査における有効性・効率性の目標を考える場合、必ずしも保証だけが目的ではないと言える。

5.6.3 情報セキュリティ監査業務の意義および性格

①情報セキュリティ監査業務の定義

情報セキュリティ監査業務の定義として、「情報セキュリティ監査業務は、情報セキュリティの管理状況の適切性について、それに責任を負う被監査主体責任者等が提示した言明書について、情報セキュリティ監査人が一定の基準に照らしてその記述の適正性について保証業務としての総合結論を表明する業務である。」とあり、前文の通り保証業務を前提としている。

②監査の基準

別段、保証業務に固有の説明はない。

③言明書の内容

ここでは言明書の内容について明らかにされている。

「言明書には、監査対象の範囲、および情報セキュリティ管理・統制の整備、運用状況について被監査主体責任者が、上記「(4) 監査の基準」への準拠状況を評価した結果が、記述される。」

被監査主体責任者が、情報セキュリティ管理・統制の整備、運用状況について自ら評価した結果を「言明書」として要求している。監査は言明書に対して行われる。

尚、既に紹介した「報告基準ガイドライン」では直接報告方式の紹介があるが、上記の定義にも「それに責任を負う被監査主体責任者等が提示した言明書について、…」とあるように、JASA では「言明書方式」が前提と理解して良いのか、判断を迷う点である。

5.6.4 情報セキュリティ監査業務

①情報セキュリティ監査業務プロセス

本項では、「言明書に記載される被監査主体責任者による評価は、情報セキュリティ管理基準および本情報セキュリティ監査業務実施基準に規定する評価基準に対する状況がレベル数値によって示される。」とあり、評価が「レベル数値」により行うとある。次項で評価数値レベルの説明がある。

②言明書（被監査主体責任者）の評価の指針および監査人の評価の指針

本報告書では、評価の指針として「評価数値レベル」により行うとあり、JASA 独自の考えを展開している。評価の方法論がより論理的となり、更に普及推進に努力を望みたい。

・評価数値レベル（保証型監査としては重要と考えるので全文抜粋）

「情報セキュリティ管理基準の「マネジメント基準」および「管理策基準」の各規定への準拠の程度を下記の数値レベルで評価し、言明書「責任者の評価」数値とする」とあり、下記の数値レベルが提示されている（参考：FISC成熟度モデル）。

a. マネジメント基準の評価数値レベル

1：非公式に実施されているが文書化されていない。

2：文書化されているが、運用が十分でない。

3：文書化され、運用されている。

b. 管理策基準の評価数値レベル

1：公式な文書化は不十分である。

2：公式に文書化されているが、組織全体として策定されていない。

3：組織全体として文書化され導入［筆者注記：運用？］されている。

4：運用され、モニタリングされている。

5：運用され、不備等について有機的なフィードバック・改善がなされている。

ここでは、マネジメント基準の評価数値レベルと管理策基準のそれが、なぜ異なるのか理由が詳しく説明されていない。また整備状況の評価と運用状況の評価が渾然一体となった成熟度モデルである。文書化は整備状況評価の範囲で、運用・モニタリング・改善等は運用状況評価の範囲と考えるが、いかがであろうか。但し、内部統制監査のように、整備状況の評価と運用状況の評価を２段階のステップで行うべきかどうかは議論が必要である。

・監査手続上の留意事項

更に監査手続上の留意事項として、「各評価項目の監査に当たっては、統計的サンプリング等、保証業務として適切な技法により実施する。」とあり、保証業務として適切な技法の実例として「統計的サンプリング等」を挙げている。

上記の成熟度モデルによる評価と統計的サンプリングとの関連についての説明はない。

③情報セキュリティ監査報告書（省略）

④言明書

ここでも言明書について「監査人は、言明書を入手しその謄本を監査報告書に綴りこむ。」とあり、記載項目には以下の 5 項が挙げられている。

・監査対象となる管理状況

・監査対象の範囲・期間及び評価結果に関する記述

・情報セキュリティに関する管理及び管理状況並びにその評価に対する責任

・言明書の作成責任

・言明書の作成に関する責任者による記名捺印

更に、被監査主体責任者の評価として「情報セキュリティ管理基準の「マネジメント基準」および「管理策基準」の各基準の項目毎に、「２．(2)①評価数値レベル」に基づき被監査主体責任者が評価した結果の評価数値レベルを記載する。」

⑤被監査主体責任者の確認書

JASAでは、言明書のみならず確認書の入手も前提としている。「監査人は、被監査主体責任者から言明書に関する責任及び必要と判断した事項を記載した書面を「確認書」として入手する。」。

これは、2003年4月の内閣府令第28号（企業内容等の開示に関する内閣府令等の一部を改正する内閣府令）では、有価証券報告書の提出に際して「代表者による適正性の確認書」を添付することを求めるようになったことを参考にしているものと考えられる。

5.6.5 報告書等の例示

①情報セキュリティ監査報告書の例示

例示の主文から、重要な事項を引用記載する。

・私たちの責任は、独立の立場から「言明書」に対する結論を報告することにある。

・私たちは、監査の結果として結論を報告するための合理的な基礎を得たと判断している。

・「言明書」の記載が、合理的保証を提供するためにすべての重要な点において適正に表示されているものと認める。
・私たちの結論から将来を予想することにはリスクがある。
②言明書の例示
　例示は以下の通り。
・主文（一部引用）
　「私たちは、平成×年×月×日から平成×年×月×日までの期間における、○○株式会社の○○○システムの情報セキュリティに関する管理状況について、「情報セキュリティ査業務実施基準」（平成×年×月×日 日本セキュリティ監査協会）に従って評価し作成した「監査対象の範囲」及び「被監査主体責任者の評価」は以下のとおりです。
・監査対象の範囲（省略）
・被監査主体責任者の評価
　被監査主体責任者の評価では、マネジメント基準と管理策基準別に、コントロール項目番号、評価項目（コントロール）、責任者評価が表で示されている。責任者評価は「評価数値レベル」の数値が記載されている。
③被監査主体責任者の確認書の例示
　例示の主文から、重要事項を引用する。
・○○○○システムの情報セキュリティの管理状況の維持及び「言明書」の作成についての責任は、○○株式会社の責任者にあります。
・言明書に記載した○○株式会社の○○○○システムの情報セキュリティの管理状況の評価は、「情報セキュリティ監査実施基準」 に従って正しく表示しております。
　以上、JASAによる「情報セキュリティ監査制度利用促進事業実施報告書」の一部を紹介したが、第1編から第4編までを含めると膨大な資料となり、極めて革新的で意欲的な試みである。実施メンバーに敬意を表したい。

5.7 **「情報セキュリティ監査手続ガイドライン」**（経済産業省：2009 年 7 月）

　本ガイドラインは、情報セキュリティ管理基準（2008 年改正版）を用いて監査を実施する組織、監査を受ける組織、および内部監査の実施を検討している組織に対して、具体的な監査の手続を与える監査手続ガイドライン（以下、監査手続ガイドライン）である。
前項の実施報告書の成果として、平成 21 年 7 月に経済産業省より公示されたものである。
　本ガイドラインには、情報セキュリティ管理基準の全てのコントロールに対して、
　・主たる監査対象　　・監査技法
　・監査手続　　・留意点
の 4 項が A3 プリントで約 90 頁（A4 プリントでは、字が小さくて読めない）ものボリュームで紹介されており、実施マニュアルともいえる。

5.7.1 情報セキュリティ監査手続ガイドラインの概説

　概説には、保証型監査についての記載があるが、特に保証業務を重点的に意図した記載ではないように感ずる。参考に挙げる。
「情報セキュリティ監査人（以下、監査人）が監査を行う場合、監査計画を立案し監査依

頼者と同意しておくことが必要である。監査依頼者は多くの場合、組織全体、監査部門あるいは情報セキュリティ管理部門の長である。利用者合意方式の保証型監査では監査報告書の利用者がこれに該当する。」（傍線筆者）。

ここに、利用者合意方式とは「監査報告書の利用者が、被監査主体の情報セキュリティ対策に直接の利害関係を持ち、その適否や有効性に特定の期待や要求水準を満たしている場合に、監査人が利用者の期待している水準を満たしているかどうかを監査する方式。監査人は、1 次利用者の期待する情報セキュリティ確保の要求水準を満たすかどうかを確認するに十分な監査手続を実施し、その結果を 1 次利用者に報告する。」とある。また、保証型監査とは「保証型の監査とは、監査対象たる情報セキュリティのマネジメント又はコントロールが、監査手続を実施した限りにおいて適切である旨（又は不適切である旨）を監査意見として表明する形態の監査を指す。保証型の監査の結論として表明される保証意見は、情報セキュリティ監査人が「情報セュリティ監査基準」に従って監査手続を行った範囲内で、監査手続が実施されたことを前提として付与される保証であり、「インシデントが発生しない」ことを保証するのではなく、「基準」に照らし適切であるか否かを保証するものである。」。

5.7.2 情報セキュリティ監査手続ガイドラインの記載 4 項目

ガイドラインの項目には、上記の「主たる監査対象」、「監査技法」、「監査手続」、「留意点」の 4 項目が説明されている。

そのうち「監査技法」については、一般的な監査技法である「質問」、「閲覧」、「観察」、「再実施」の 4 監査技法が紹介されているが、保証型監査固有の監査技法としての特筆はない。

5.8 IT 委員会研究報告第 39 号「情報セキュリティ検証業務」

（日本公認会計士協会：2010 年 05 月 18 日）

2010 年 05 月 18 日に日本公認会計士協会より公表された IT 委員会研究報告第 39 号「情報セキュリティ検証業務」（以下、「IT39 号」という。）は、既に公表されたＩＴに係る保証業務についての一般的な指針である「ＩＴ実務指針（ＩＴ委員会報告第 5 号）」を前提としている。

その上で、「情報セキュリティ」の分野に限った合理的保証水準による保証業務としての検証業務についての研究報告書である。監査業務ではなく“検証業務”と呼ぶのは、「ＩＴ実務指針（ＩＴ委員会報告第 5 号）」に同じである。重要なポイントのみ考察する。

5.8.1　情報セキュリティ検証業務における評価指針等

IT39 号において保証業務に係る要件等は、ＩＴ実務指針をベースにしている。

①評価水準

「Ⅲ 情報セキュリティ検証業務における留意点」で述べられている 1.評価指針の「評価水準」は、既に触れた「5.6　情報セキュリティ監査制度利用促進事業実施報告書における／第 1 編 第 4 部 社会的合意方式における監査業務実施基準の検討」における評価水準からの引用である。

②記述書

監査対象は、明確な記載はないが主題情報を記載した「経営者の記述書」と考えられる。

③評価の方法

特筆すべきは、「1.評価指針／（2）規準間の整合性と評価の方法について」では、コントロールの評価において「各評価項目の評点の評価に当たっては、原則として統計的サンプリング等合理的な方法により実施す

る。」とあり、サンプリング試査で行うことの具体的な記載がある。

④検証報告書に記載の重要な固有の限界情報

また「3.情報セキュリティ検証報告書の形式と記載事項」には、「⑬規準に照らして主題を評価又は測定する場合の重要な固有の限界情報」に次の記載がある。「セキュリティ検証報告書の想定利用者が、当該業務の固有の限界について、十分に理解していないため、検証報告書上で明示的に記載することが適切と判断される場合には、有効性に関する過去の評価が将来期間には及ばないということを記載する。」と、将来における保証ができないことを明記している。

5.8.2　情報セキュリティ評価基準

IT39号の「Ⅳ 情報セキュリティ評価基準」では情報セキュリティ管理基準が明確にされており、経済産業省公表の「情報セキュリティ管理基準：平成20年改正版（以下、「20年版管理基準」という。）」あるいは、その前提となる「ISO/IEC27001:2005 ISMS要求事項（JIS Q 27001:2006））」をベースにほぼ同様の管理策（コントロールのこと）から構成されている。

20 年版管理基準はマネジメント基準と管理策基準とから構成されており、各々IT39 号では管理規準とコントロール規準となっている。

①管理規準（「マネジメント基準」）

IT39 号の管理規準には、20 年版管理基準（実際には、前出の「情報セキュリティ監査手続ガイドライン」）の管理策基準（例えば、項番 1.1.1）のレベルまで記載され、次のコントロール規準と記載項目のレベルをあわせてある。

ただ、管理策基準の項目には項番 1.1、項番 1.1.1 の両レベルで若干違い（多寡）がある。

尚、20 年版管理基準のマネジメント基準では、項番 1.1 レベルまでしか記載がないが、「情報セキュリティ監査手続ガイドライン」には項番 1.1.1 までの記載がある。

②コントロール規準

IT39 号のコントロール規準では、管理策基準（例えば、項番 1.1.1）のレベルまでで、20 年版管理基準の詳細管理策の項番 1.1.1.1 レベル（実際には「情報セキュリティ監査手続ガイドライン」に記載）までの取扱いは無い。

尚、コントロールの記載文章は、いずれも「・・・しているか。」とあり、実務上の評価が容易な文章になっている。

以上のことから、保証業務に係る監査で重要な「評価方法（ここでは、評価指針）」と「管理基準」が既に公表されている基準をベースにした引用に近い内容であり、IT39 号はあまり新しく参考とすべき点のない報告書である。

5.9 **「金融機関等のシステム監査指針（第 3 版）」**

（財団法人金融情報システムセンター：2007 年 3 月）

「金融機関等のシステム監査指針」についての役割は、本指針（以下、FISC ガイドライン）に特に記載は無いが、エグゼクティブサマリー（経営者のためのガイド）の第 1 項「システム監査の目的」で明らかである。「情報システムを活用した信頼できる金融サービスの提供」を目的とした、経営者視点によりシステム監査を行うべく開発されたシステム監査ガイドラインであり、システム監査の分野では実績もあり、権威あるガイドラインである。

ここにエグゼクティブサマリー「システム監査の目的」およびシステム監査基準に該当する「第 1 部フレームワーク」から保証業務に関連する記載を抜粋して紹介する。
尚、本レポートの目的から、システム監査に係る一般的な記載内容は紙面の都合上から省略する。また、経済産業省公表の「システム管理基準」に相当する評価基準は、FISC ガイドラインでは「第 2 部チェックポイント集」で用意されているが、ここで詳細は触れない。

5.9.1 エグゼクティブサマリー
① システム監査の目的
「金融機関等の経営者は、情報システムの安定的な運用を図る仕組みを構築し、信頼できる金融サービスを提供することが求められている。情報システムを安定的に運用するためには、全社的なリスク管理体制を構築し、当該管理体制を踏まえて情報システムに係る内部統制（以下「IT コントロール」という）を整備し、その継続的な運用をシステム監査によって担保するという仕組みが必要とされる」（傍点筆者）。
ここに、「情報システムに係る内部統制の整備」と明言されているのは卓見である。その上で、全社的なリスク管理体制を踏まえた情報システムに係る内部統制の整備・運用を“担保するための仕組み”がシステム監査であると提言されている。担保は“保証”と言葉を変えてよいと判断するのは筆者の独断であろうか。
②システム監査の役割
次に、システム監査の役割では、まず「情報システムの安全性、信頼性、遵守性の確保を目的として行われる」を取り上げている。情報システムのオペレーショナルミスや不正行為が、業務中断、決済不能、風評等の金融機関等におけるオペレーショナル・リスクに波及する可能性を孕んでおり、「経営者は、損失に結びつくリスクに対して適切な IT コントロールが設定され、継続して運用されているかどうかを、システム監査によって確かめておく必要がある。」とシステム監査の役割を明確にされている。
更に、「あわせて、金融機関等にとって、情報システムの戦略的な活用は、経営戦略の実現、及び業務プロセスの改善にとって不可欠なものである」とあり、「このような観点からするシステム監査は、情報システムの有効性、効率性の確保を目的として行われる」と有効性（戦略性含む）および効率性について追記されている。
尚、システム管理基準に相当する第 2 部の「チェックポイント集」では、IT コントロールは要点項目／大項目／小項目で整理されており、169 項目の小項目単位に、監査の着眼点である 5 つのコントロール目標「有効性、効率性、信頼性、安全性、遵守性」の識別がされている。さらに小項目ごとにリスクとコントロールが明記され、そのコントロールの評価チェックポイントが挙げられている。
このコントロール目標と基準との関連は重要であるが、例えば、経済産業省「システム管理基準」ではその関連付けは成されていない。本レポートの「7 章 保証型システム監査に係るシステム管理基準の考察」で詳しく見る。

5.9.2 システム監査の概念（FISC ガイドライン「第 1 部 フレームワーク」第 I 章）
①システム監査の意義
FISC ガイドラインでは、システム監査の定義で、次のように保証業務に触れている。
FISC ガイドラインでいうシステム監査とは、「情報システムの有効性、効率性、信頼性、安全性、及び遵守性を達成できるよう、情報システムリスクを把握し、情報システムに係るコントロールが適切かつ効果的であることを、被監査部門から組織的に独立したシステム監査人が検証し、その結果を保証意見又は助言勧告としてとりまとめ、経営者に報告する監査」をいう。

②システム監査の 2 つの職能

FISC ガイドラインでは、システム監査の職能として保証と改善を挙げている。「システム監査の職能をどのように見るかについては、大別して次の 2 つがある。保証職能(assurance function)と改善職能(improvement function)である」と。保証職能について見る。

a. システム監査の保証職能

システム監査の保証職能とは、「監査対象をある判断の尺度に照らして「適切である」「重大な問題は見当たらなかった」という旨のお墨付きを与える職能」（傍点筆者）をいう。

したがって、もし情報システムに重大な欠陥があれば、それは否定的保証ということになる。また一部を除いて問題なしとする旨の限定付の保証もある。

また FISC ガイドラインでは、保証職能の例として「経営管理への寄与を目的としたシステム監査における保証職能は、例えば、開発から運用への切り替え局面でゴーサインを出す場合の判断材料として監査によって付与される保証という職能を利用することができる。また、業務部門において自己診断や自己評価を行ったうえで、さらにその信憑性を高めるために保証職能を利用することもできる」と紹介する。

更に、保証要件として職業的懐疑心と十分かつ適切な監査証拠を 2 点挙げる。「保証の付与という職能をシステム監査に期待する考え方によれば、監査人には批判的なものの見方と態度が要求され、保証を裏付けるために質的にも量的にも十分かつ適切な監査証拠の入手が重視されなければならない」。

この項の末尾には、合理的な保証であることの説明がされている「なお、ここで保証といってもそれは絶対的な保証ではありえない。それは、監査資源には限りがあること、保証の対象範囲を明確に限定することが困難であること、監査証拠の入手と評価の局面において事実認定だけでなく監査人の価値判断を伴わざるをえないこと等の理由から、絶対かつ完全な保証を望むべくもなく、またそれを期待してはならない。システム監査によって付与される保証は、あくまでも合理的な保証(reasonable assurance)にすぎないのである」。

5.9.3 情報システムに係るコントロールとシステム監査

①情報システムの目的から見た機能要件

FISC ガイドラインでは、「情報システムの目的は、情報提供と業務処理という役割を通じて経営戦略を支援し、もって経営目的の達成に資することにある」とも定義されている。続いて、情報システムがこの役割を適切に果たすために備えていなければならない 5 つの機能要件として「有効性、効率性、信頼性、安全性、遵守性」を挙げ、各々について紹介している。これら情報システムが備えていなければならない 5 機能要件は、「コントロール目標」とも言い換えることもでき、システム監査実施の観点からは「監査の着眼点」であり、システム監査人が立証すべき「監査目標」であるともいう。

この情報システムの 5 機能要件（コントロール目標、監査目標）は、FISC ガイドラインではシステム監査の役割として挙げられているが、「保証業務に係るシステム監査の目標となり得るか」という論点（7 章で議論）で重要なので、全項引用して紹介する。

a. 情報システムの有効性（筆者注記：有効性には「戦略性」を含むと考えられる）

有効性とは、「情報システムが経営方針または経営戦略の策定及び実現に対して効果的な情報や業務処理機能を提供していること。これには例えば目的適合性、適時性、有用性、あるいは利便性等が含まれる」という。

この目標に対する評価基準は、目的適合性の場合「明確な経営目標や戦略目標に対する効果的な情報や業務処理機能の提供の実績有無あるいは目標達成度」であると考えられる。

b. 情報システムの効率性

効率性とは、「情報システムによる情報やサービスの提供が、生産性や経済性の高い方法で行われていること。これには資源の効率的活用だけでなく、将来的な拡張性や、他システムとの連携の柔軟性等も含まれる」という。

効率性という目標に対する評価基準は、まず当該コントロールに関する測定可能な効率性の判断基準となる尺度（モノサシ）と指標が必要である。また、具体的に効率性をコントロール目標とするITコントロールが適合する規準であるかどうかは十分に確認する必要がある。

c. 情報システムの信頼性

信頼性とは、「情報システムが提供する情報やサービスが、信頼できるものであること。これには、情報システムに期待される情報やサービスを情報システムが確実に提供しているということが含まれ、また結果やプロセスの堅確性や正確性等が含まれる。」という。

信頼性をコントロール目標とする評価基準は一般的である。ＩＴ実務指針（4.2 ITに係る保証業務の概要）では、具体的な保証業務として「ITに係る○○○の信頼性等に関する評価」と信頼性に重きを置いている。

d. 情報システムの安全性

安全性とは、「情報システムが災害・障害・犯罪・不正行為、その他の脅威から保護されていること。これには、機密性(重要な情報が非権限者に知られることがないように保護されていること)、完全性(不正や障害等により情報の一貫性が失われることがないよう保護されていること)、可用性(必要とされる情報が必要なときに利用可能であり、また必要な資源の継続的使用が確保されていること)等が含まれる」という。

ここでの安全性は情報セキュリティの目標でもある。また安全性は信頼性に含まれると判断することも可能で、保証業務のコントロール目標としては妥当である。

e. 情報システムの遵守性

最後の遵守性とは、「情報システム及びそれに関連する業務プロセスが、法令、規制、あるいは当該金融機関等の方針及び手続き等を遵守していること。また、情報システム及びそれに関連する業務プロセスにこれらの規制情報を遵守する仕組みが組み込まれていること。この要件は、上記 a から d と同列なものではなく、それらの前提として位置づけられる関係にある」という。

当該目標に対する「評価基準」としては、遵守すべき法令や規則、社内規程等が考えられる。

以上、上記各機能要件の記載で、当該目標に対する「評価基準」に関する記述は筆者による追記である。これらのコントロール目標に対する評価基準は、次章の保証型システム監査のフレームワークについて考える際に参考となる。

5.9.4 システム監査の新たな対応

FISC ガイドラインでは、新たな対応として「成熟度モデル」と「自己評価」を取り上げている。

①成熟度モデルの展開

この成熟度モデルは CMM（ソフトウェア開発プロセスの能力評価のために開発されたモデル）を情報システムに係るコントロールの評価に応用しようとするものである。

FISC ガイドラインには、例として以下の５レベル表示を示している。

・レベル１

最低限のコントロールが場当たり的に実施されている。したがって、組織としてのコントロールの基準や標準が全く確立されていない。

・レベル２

必要なコントロールが計画され、その結果が追跡され、点検されている。組織としてのコントロールの基準や標準が一部確立されている。

・レベル３

コントロールのプロセスが、組織全体として、標準化、文書化され、周知されたうえで、それに従って運用されている。

・レベル４

コントロールのプロセスが、標準化された手続きに従っているかを監視することが可能であり、場合によっては、定量的な測定も可能である。標準化された手続きからの逸脱があった場合には、適切かつ適時な是正ができる。

・レベル５

コントロールのプロセスは、組織全体として、継続的に改善され、コントロールは常にベストプラクティスの水準にある。コントロールの自動化も十分に進み、情報システムの品質改善につながっている。

この例示で見れば、「レベル２」でコントロールの水準としては問題ないと考えられる。レベル３では、組織全体としての「標準化」、「文書化」が要求されているが、これらはコントロールの適切性自体の評価結果を左右しない。

ここで言えるのは、システム監査の評価手続において、成熟度モデルは評価基準ではなく（評価基準としてはシステム管理基準等に示された IT コントロールがある）、筆者の言う「評価の尺度（モノサシ）」に該当すると考える（次章 6.2 参照）。

②コントロール自己評価の活用

FISC ガイドラインで自己評価とは、「情報システムに係るコントロールが適切に機能していることを、情報システムの整備と運用に直接的な責任を有する情報システム部門又はユーザー部門が、自らの判断と責任において評価することを、コントロールの自己評価（self assessment）という。」と言う。更に尚書きで「なお、このコントロールの自己評価をシステム監査で利用しようとする場合に注意しなければならないことは、自己評価の結果はあくまでも「自己申告」にすぎず、したがってシステム監査人は、その結果をそのまま監査証拠として採用することはできないことである」とある。当然である。

5.9.5 システム監査の実施（FISC ガイドライン「第 1 部 フレームワーク」第Ⅱ章）

①予備調査

FISC ガイドラインでは、予備調査は「監査手続を具体化させることを目的に、被監査部門からの資料収集等により監査対象の概要を把握する。予備調査を実施するなかで当該監査対象に関してのリスク評価を行い、重点的に監査すべき事項を見極める」とあり、文書調査と言える。

②監査手続書の作成

FISC ガイドラインでは、監査手続を具体化するために「監査手続書」を作成する。チェックポイント集を前提に手続は明確である。主要な手続は以下の通りである。

・監査項目の明確化（第 1 段階）

手続の第 1 段階は、監査目的に従って、監査対象ごとに主要な監査項目を決定する。

更に「ここでいう監査対象は、「チェックポイント集」の各要点項目における「大項目」におおむね相当し、監査項目は「小項目」におおむね相当する」と具体的で例示もある。

・チェックポイントの設定（第 2 段階）

手続の第 2 段階は、上記で設定した監査項目（小項目）ごとにチェックポイント集よりチェックポイントを設定する。

・監査手続の具体化（第 3 段階）

手続の第 3 段階は、チェックポイントごとに「何を、誰に対して、どのようにして確認するか等の監査手順を可能な限り具体化した監査手続を検討し、監査手続書としてとりまとめる」。情報セキュリティ監査手続ガイドラインには、情報セキュリティ管理基準の全てのコントロールに対して、主たる監査対象、監査技法、監査手続、留意点が一覧表でまとめられている。参考となる。

③本調査／検証手続の実施

監査手続とは「監査対象における情報システムリスクのコントロールが適切かつ効果的であり、実際に遵守され運用されているかどうかについて、事実に基づいた確証的な監査証拠で裏付けて確認してゆくプロセスである。」とあり、次の 2 段階で行う。

a. コントロールの必要性／妥当性の検証（整備状況の確認／検証）

第 1 段階は「監査対象における情報システムリスクに対して、手続きや組織体制等のコントロールが必要かどうかを、まず確認する」。コントロールの必要性検証である。次に、「コントロールを具体化した組織体制や手続き等が、妥当で（筆者変更：「必要」を「妥当」に変更。必要性の検証は終わっている）かつ十分かどうかを検証する。例えば手続きや組織体制等は、重大な情報システムリスクをカバーしているか、法令･規制や自社の方針等に沿っているか、あるいは他業務との関係も含めて内容は適時に見直され改訂されているか等、その妥当性を検証する」。以上が必要なコントロールの整備状況の検証である。

b. コントロールの遵守性の検証（運用状況の検証）

設定されたコントロールが妥当であると判断された場合、「これが定められたとおりに実際に運用されているかどうか、また十分に効果を発揮しているかどうかを検証する」。運用状況の評価である。

c. 監査証拠の入手

監査証拠の入手は、「コントロールの整備状況(必要性と妥当性)及び運用状況について、システム監査人が必要と認めた監査手続を慎重に実施し、十分かつ適切な監査証拠を入手する」とある。

更に、監査証拠を入手するためのテストの例として以下の３つが挙げられている。

・テストデータを用いた処理ロジックの検証

・システム設定値出力リストと設計書上の定義情報の突合による検証

・侵入テストによる脆弱性の検証

この FISC ガイドラインの例示では、IT コントロール（いわゆる内部統制でいうシステム的コントロール）に係る一般的な証拠入手方法の記載で、保証業務に係るシステム監査に特有の監査証拠入手に関する記載、例えば“試査”等についての記述はない。

尚、「監査調書の作成」については省略。

④評価・結論

評価・結論に至る過程は保証業務に係る監査報告では重要である。FISC ガイドラインには「監査調書の内容を分析し、明らかにされた問題点が重要であるか（指摘事項に値するか）、またそれは改善を要する事項か（改善案を提示するか）どうかを総合的に検討・判定し、監査意見の基礎を固める」とあり、特に保証、助言の記載は無い。

a. 問題点の摘出（指摘事項）

評価・結論における問題点の指摘は、「監査調書に記録されたシステム監査人の所見や発見事項、当該事実

を裏づける証拠資料等については、被監査部門との間で事実確認を行うなど、十分かつ適切な監査証拠に基づいて、システム監査人の判断としなければならない」とあり、一般的な「指摘事項内容の例」として、以下を挙げている。

・発見した事実の内容

・指摘の根拠

指摘の根拠として、「問題点と判断した事実はどのような監査証拠に基づいているか」を記載する。

・準拠標準、手続き等

指摘した問題点に関して、「どの標準(システム開発・運用規程、セキュリティポリシーやスタンダード等)を充足していないか、どの手続きに反しているか等、システム監査人が準拠性の判断に用いた標準、手続き等」を明確にする。

・影響

結果として「発生する可能性のあるリスクの内容、潜在的な影響度、範囲など」の影響を記述する。

・問題点の重大性

問題点の重大性の判断は、総合評価に大きく影響するが、「以上を総合的に判断し、当該事実の重大性を判定する」とあり、内部統制における「重要な欠陥」の判断基準（例えば、連結税引前利益については、概ねその５％程度とすることが考えられるが、・・・(実施基準より)）のような、具体的な判断の尺度が欲しい。

b. 改善提案（以下、省略）

⑤監査報告

監査報告書の記載事項例として、「システム監査の結果」の記載は以下の通りである。

・総評（総合的な意見）

・監査項目別（小項目）

保証業務に限らず監査報告書には、総評のみが書かれる。監査項目別は別紙添付資料である。

以上、見てきたようにFISCガイドラインにも、特に保証業務に係るシステム監査に固有の記載は少ない。

5.10 **「金融検査に関する基本指針」**（金融庁：2005.07.01）

金融庁から公表された「金融検査に関する基本指針」（以下、「基本指針」という）は、金融機関等の業務の適切性確保のための検査等に関する基準であり、検査等の実施に当たっての基本的考え方を示す。システム監査おけるシステム監査基準に当たる位置づけである。

併せて公表されている「金融検査マニュアル（預金等受入金融機関に係る検査マニュアル)」には、システム管理基準に相当するコントロール内容が、「オペレーショナル・リスク管理体制の確認検査用チェックリスト」別紙2で「システムリスク管理態勢の整備・確立状況」としてA4で15ページ程度示されている。

ここでは、金融庁及び財務局における検査部局の立場で実施する際の基本指針であるために「検査／検証」という言葉が使われ、“保証”と言う観点からの議論はない。

但し、金融庁等の立場からの検査という意味から、一般者は限りなく“保証”に近いレベルを推測する。参考までに関連する箇所を一部抜粋して紹介する。

5.10.1 検査等の実施に当たっての基本的考え方

基本的考え方の第1項に、検査部局の使命が明確にされている。その使命は「金融庁及び財務局における検査部局の使命は、銀行法等が求める金融機関の業務の健全性及び適切性の確保のため、立入検査の手法を中心

に活用しつつ、各金融機関の法令等遵守態勢、各種リスク管理態勢等を検証し、その問題点を指摘するとともに、金融機関の認識を確認することである」と明記されている。
検査の目的は、「金融機関の業務の健全性及び適切性の確保」のためであり、「問題点を指摘するとともに、金融機関の認識を確認すること」であるという。

この使命を効果的に果たすための対応として、第2項に「金融機関のリスクをみつめ、その問題点について、金融機関等に対して有効な形で警告を発することが我々の役割である。その作業は、事実を的確に把握し、客観的に問題点を示したうえで金融機関の主張を十分に聴取し、その理解や認識を確認するプロセス（ 以下「双方向の議論」という。） を経たものである必要がある。」とある。ここからは改善型監査と考えるべきであろう。

基本的考え方では、検査等における「基本原則」が示されており、参考までに簡単に紹介する。
①利用者視点の原則
「検査等の実施に当たっては、預金者等一般の利用者及び国民経済の立場に立ち、その利益が保護されることを第一の目的とし、各金融機関の経営実態を検証しなければならない。」とある。
②補強性の原則
「検査等は、自己責任原則に基づく金融機関自身の内部管理及び会計監査人等による厳正な外部監査を前提としつつ、「市場による規律」などを補強するものである。適切な内部管理ができているかどうかの説明責任はあくまで金融機関自身にあり、検査部局は、これを検証する立場にある。」ここでは外部監査を前提とした補強であり、検証であることが明記されている。
③効率性の原則
「重要性の観点を配慮しつつ、メリハリを持った的確な指摘に努める必要がある」
④実効性の原則
「検査等は、金融機関における業務の健全性及び適切性の確保につながるように実施される必要がある」
⑤プロセス・チェックの原則
「検査等の実施に当たっては、原則として、各金融機関の法令等遵守態勢、各種リスク管理態勢に関して、そのプロセス・チェックに重点を置いた検証を行わなければならない」

5.10.2 検査等の実施手続等
①検証
実施手続の検証の項には、「被検査金融機関との間における「双方向の議論」が重要であることを十分に認識し、相手の説明及び意見をよく聞くとともに、当方の考え方を伝える場合には、その根拠等も添えて説明しなければならない」とあり、詳細な実施手続の記載は無い。
②実地調査
実地調査では「必要に応じて、検査官が、被検査金融機関の役職員が現に業務を行っている施設、資料保管場所等に直接赴き、原資料等を適宜抽出・閲覧等を行いつつ、業務運営について調査（ 以下「実地調査」という。） を実施する」とある。
実地調査は「検査の効果的な実施の観点から、原則として、無予告とする」とある。金融庁による検査（監査）の特質であろう。
③検査モニター
基本指針では「本基本指針の適切な運用を確保し、検査マニュアルの機械的・画一的な運用を防止する等の

観点から、必要に応じ、検査局・財務局幹部が被検査金融機関より直接、意見を聴取する（ 以下「オンサイト検査モニター」という。）」と、検査マニュアルの機械的・画一的な運用を防止している。

以上、検査者の立場から、その基本指針に保証業務に係る事項がないのは妥当であろう。

5.11 「金融検査マニュアル（預金等受入金融機関に係る検査マニュアル）」

（金融庁：2009.05）

基本指針に基づき公表された「金融検査マニュアル（預金等受入金融機関に係る検査マニュアル）」（以下、「金融検査マニュアル」という）は、「検査官が、金融機関を検査する際に用いる手引書として位置付けられるものであり、…」とある。

システム管理基準に該当する監査項目（コントロール）としてチェック項目を記載したマニュアルである。

5.11.1 検査の実施における配慮点

本金融検査マニュアルの「はじめに」には、「当該基本指針において示された金融検査の基本的考え方を踏まえた適切な検査を実施するため、検査官は、金融機関に対する検査の実施にあたり、特に以下の点に配意する必要がある。」とあり、5項目の配慮点が挙げられている。参考に項目のみ列挙する。

①重要なリスクに焦点をあてた検証（「ﾘｽｸ・ﾌｫｰｶｽ、ﾌｫﾜｰﾄﾞ・ﾙｯｷﾝｸﾞ」ｱﾌﾟﾛｰﾁ）
②問題の本質的な改善につながる深度ある原因分析・解明
③問題点の指摘と適切な取組の評価、静的・動的な実態の検証
④指摘や評定根拠の明示、改善を検討すべき事項の明確化
⑤検証結果に対する真の理解（「納得感」）

5.11.2 金融検査マニュアルにより検査を行うに際しての留意事項

本項には、チェックリストの項目説明として、以下の記載がある。

「チェック項目の語尾が『しているか』又は『なっているか』とあるのは、特にことわりのない限り、当該金融機関が達成していることを前提として検証すべき項目である」。

また「一方、チェック項目の語尾が『望ましい』とあるのは、特にことわりのない限り、金融機関に対してベスト・プラクティスとして期待される項目である」。

さらに「一方、チェック項目において『例えば』として着眼項目を列記してあるのは、全ての内容を字義どおり達成することを求めるものではなく、当該金融機関の業務の規模・特性等に応じて実質的な機能達成のための必要性を判断すべき例示項目である」。

5.11.3 チェックリスト

以上の前書きに続いて、具体的なチェックリストが 10 項目（A4－316 頁）に亘ってまとめられている。参考までに 2～3 のチェックリスト項目名を紹介する。

・経営管理（ガバナンス）態勢－基本的要素－の確認検査用チェックリスト
・法令等遵守態勢の確認検査用チェックリスト
・信用リスク管理態勢の確認検査用チェックリスト
・オペレーショナル・リスク管理態勢の確認検査用チェックリスト

当チェックリストで構成を紹介すると、以下の 3 部構成となっている。

Ⅰ．経営陣によるオペレーショナル・リスクの総合的な管理態勢の整備・確立状況
Ⅱ．管理者によるオペレーショナル・リスクの総合的な管理態勢の整備・確立状況
Ⅲ．個別の問題点

この「Ⅲ．個別の問題点」の第 5 項に「システムリスク管理態勢については、別紙 2 参照」とあり、上記と同様に、以下の３部構成で IT コントロールについて記載されている。

Ⅰ．経営陣によるシステムリスク管理態勢の整備・確立状況
Ⅱ．管理者によるシステムリスク管理態勢の整備・確立状況
Ⅲ．個別の問題点

①経営陣によるシステムリスク管理態勢の整備・確立状況

この項では経営陣の立場から、経営陣が果たすべき役割と負うべき責任が記載されている。またその「検証ポイント」では、システムリスクが定義されているので紹介する。

「システムリスクとは、コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い金融機関が損失を被るリスク、さらにコンピュータが不正に使用されることにより金融機関が損失を被るリスクをいう。」。これから分かるように、システムリスクとして主に信頼性／安全性に係るコントロール目標が重視されている。

以下に、経営陣が果たすべき役割の項目を参考に挙げておく。

・適正なシステムリスク管理態勢の整備・確立に向けた方針の策定
・システムリスク管理に関する内部規程、組織体制の整備
・システムリスク管理の評価、改善活動

②管理者によるシステムリスク管理態勢の整備・確立状況

本項では、管理者及びシステムリスク管理部門が果たすべき役割と負うべき責任について検査官が検証するためのチェック項目を記載している。以下に、項目のみ挙げる。

・管理者の役割・責任（システムリスク管理規程の整備・周知、内容。組織体制の整備）
・システムリスク管理部門の役割・責任（システムリスクの評価、モニタリング、見直し）

③個別の問題点

本項においては、「システムリスク管理の実態に即した個別具体的な問題点について検査官が検証するためのチェック項目」を記載している。同様にチェック項目を挙げる。

・情報セキュリティ管理
・システム企画・開発・運用管理等
・防犯、防災、バックアップ、不正利用防止
・預金口座の名寄せ
・システム関係の業務委託先の検証
・システム統合に係るリスク管理態勢

第4項の「預金口座の名寄せ」は金融機関固有のテーマで、他はシステム管理基準と差異はない。また、保証業務に関連する記載は特に無い。

尚、最後の項のシステム統合に係るリスク管理の検証については、「システム統合リスク管理態勢の確認検査用チェックリスト」(平成14年12月26日付検第567号)に基づき行うとある。

以上で、保証業務に係る公表文書の調査・研究を終える。

研究会報告　【第 164 回月例研究会受講報告】

会員番号 0902　**宮下重美**

・テーマ　　クラウドサービス利用のための情報セキュリティマネジメントガイドラインについて
・日、場所　　2011 年 7 月 20 日（水）、御茶ノ水　総評会館
・講師　　経済産業省 商務情報政策局 情報セキュリティ政策室 佐藤明男 氏

Ⅰ. はじめに

経済産業省で策定した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」について解説いただいた。その要旨は次のとおりである。

本ガイドラインは、クラウドサービス利用における情報セキュリティ管理の確立、導入、運用、監視、見直し、維持及び改善のための実施の手引を提供するものである。JIS Q 27002:2006 が示す実施の手引を、クラウドサービス利用時に適用するため、考え方、留意点についてまとめている。

2010 年 10 月初旬独ベルリンで開催された国際標準化会議 ISO／IEC JTC1／SC 27 において、
本ガイドラインに基づく日本提案（SC27N9044）が採択され、新たなプロジェクトとして開始されている。

Ⅱ. 講演主旨

1. クラウドに関する政策

クラウドコンピューティングは低コストで大量の情報処理がタイムリーに実施できるため、今日、各産業界、公共機関、利用者から大きな期待が寄せられている。このクラウドの政策対応として信頼性向上、安全性向上、高速化の技術開発をはかりながら、医療分野、交通分野、データ基盤分野、社会基盤分野の実証事業を進め、データ利活用による新産業創出などの工程を推進してきている。

情報セキュリティに関しても、「システムの構築、運用、利用のためのガイドライン」の策定と体制整備を進めてきた。本講演で、このマネジメントガイドラインを発表する。

2. クラウドに関する利用者の意識

国内企業の情報漏えいインシデント件数は年々増大しており、世界的には大規模な情報漏えい事故が増加している。この中で、今後,クラウドコンピューティング環境に移行することにより,情報漏えいが更に増大するのではないかとの懸念がある。

最近のウェブアンケート（500人対象）の調査によると、“クラウドのセキュリテイ対策(情報漏えい対策等)が十分かどうか分からない“との懸念が多い。また、情報セキュリティに関する情報を含め、クラウドサービスの利用を検討するために十分な情報がクラウド事業者から開示されていない状況にある。

一方、別の調査によれば、クラウドサービス利用におけるセキュリテイ対策のニーズとして、クラウドサービス事業者に対し、ISMS、Pマークの認証・取得の要望も多い。

3. クラウドのセキュリティ上の脅威

クラウドの脅威を示すインシデント件数は36件があり、攻撃以外のインシデントは約70%、各種攻撃が約30%となっている（2009.3～2010.7 IPA調査）。また、脆弱性の代表例としては「仮想化製品」が殆どであり、続いて、データベ

ースが僅かとなっている(NVD.NIST.IPA調査)。

4. クラウドサービス利用のための情報セキュリティマネジメントガイドライン

このガイドラインは、経済産業省が「クラウドセキュリティ管理基準策定TF（座長：工学院大学・大木栄二郎教授）」を設置し、平成22年7月から10月にかけて、議論・策定した。

http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html

（1）ガイドラインの概要

＜目的＞

このガイドラインを情報セキュリティ管理、及び情報セキュリティ監査に活用することにより、クラウド利用者とクラウド事業者における信頼関係の強化に役立てることを目的としている。

＜適用範囲＞

このガイドラインは,組織事業の基礎を成す情報資産の多くを、外部組織であるクラウド事業者が提供するクラウドサービスに委ねようとする組織が、「JIS Q 27002(実践のための規範)」に規定している管理目的を達成するための管理策を実施しようとする場合を想定している。

＜特徴＞

・全面的にクラウドサービスを利用する際の「JIS Q 27002（実践のための規範）」の管理目的達成という究極的な状況を想定することにより、クラウドサービスの利用において変化するシステム環境、責任の所在、事故や事象の判断基準を明確にする。

・クラウドサービスを全面的に利用することにより生ずるリスクの変化に対応するため、「JIS Q 27002（実践のための規範）」の管理策に、「クラウド利用者のための実施の手引」と「クラウド事業者の実施が望まれる事項」を追加している。

（2）クラウドサービス利用に関わる管理策の選定と利用

・クラウド利用者が「JIS Q 27001（要求事項）」による情報セキュリティマネジメントシステム（ISMS）のPDCAモデルを使用する際に、このガイドラインが示す「クラウドサービス利用のための管理策の実施の手引き」を利用すれば、マネジメントシステムを維持しながら、クラウドサービスを利用した適切な情報セキュリティ管理が容易に行えるようになっている。

・クラウドサービスを提供するクラウド事業者は、このガイドランが示す「クラウド事業者の実施が望まれる事項」を利用すれば、クラウド利用者に対して適切に管理された情報セキュリティサービスを提供することが出来る。

・上記の2項によるクラウド利用者と事業者の両者の管理策によって、双方の責任が明確化し、情報セキュリティガバナンス及び情報セキュリティマネジメントの実施が可能となる。

（3）ガイドラインの構成内容

・このガイドラインの箇条5～15は、「JIS Q 27002（実践のための規範）」と対応している。
このため、「JIS Q 27002（実践のための規範）」の管理策を実施するための補足として活用できる。

・参考として、「付属書A：クラウドサービス利用に係るリスク」を「付属書B：クラウドサービス利用におけるリスクアセスメントの実施例」を示している。

（4）ガイドラインにおける実施事項のイメージ（例）

XX. X YYYYYY ← ガイドラインの箇条と実施事項

＜目的と管理策＞

目的と管理策は,情報セキュリティ管理における目的が変更されないように「JIS Q 27002(実践のための規範)」をそのまま引用している。それぞれの実施項目の必要性や背景などを理解するため、又、情報セキュリティ監査に利用

する場合にも目的を明確にするために利用できる。

＜クラウド利用者のための実施の手引＞

クラウドサービス利用において、クラウド利用者が実施する管理策を支持し、管理目的を満たすための情報を提供する。この手引にはすべての場合に適していないものもあるため,他の方法でその管理策を実施する方がより適切な場合もある。

＜クラウド事業者の実施が望まれる事項＞

クラウドサービス利用において、クラウド事業者の協力が必要となる管理策については、クラウド利用者が実施する管理策を支持し、管理目的を満たすために、クラウド事業者の実施が望まれる事項に係る情報を提供する。

＜クラウドサービスの関連情報＞

クラウドサービス利用において考慮が必要と思われる関連情報（関連するクラウドサービスの種類、利用環境又は利用技術に関する情報など）を提供する。

（注1）クラウド固有の事項がない場合は、それぞれの項目は記載しないこととした

（注2）これらガイドラインの内容については、クラウド障害事例に対応させ検証している。

(5)クラウド事業者のサプライチェーンについての考え方

・クラウドサービスにおいては、laaS、PaaS 及び SaaSそれぞれが関連しあってサプライチェーンを形成し、クラウドサービス全体を提供することがある。

・このガイドラインにおいては、クラウドサービスを供給する側が利用する側に回ることで、サービスの供給と利用の連鎖が形成される。

・「クラウド利用者のための実施の手引」を自らの組織に活用できるだけでなく,「クラウド事業者の実施が望まれる事項」を自らが利用するクラウドサービスの供給者に対して要請し,サプライチェーンを形成するクラウド事業者の情報セキュリティマネジメントに活用することも出来る。

(6)本ガイドラインの情報セキュリテイ監査への活用

本ガイドラインの実施項目を、情報セキュリティ監査の枠組みで利用することにより、クラウド利用者及びクラウド事業者間の信頼関係を構築することが可能である。なお、監査人はクラウド事業者からのクラウド利用者への言明（コミットメント）を保証する、こととなる。

5. 国際規格化

(1)国際規格化の経緯

・日本から Cloud computing services における情報セキュリティマネジメントとして、SC27／WGlのBerlin会議(2010.10)で、このガイドランを提案した。

・Cloud computing services におけるSecurity and Privacy プロジェクトのStudy periodを開始した。

・これは、情報セキュリティマネジメント分野での日本初のプロジェクトであり、SC27／WGlのRapporteurは、山崎哲教授（工学院大学）である。

(2)本ガイドラインと海外の関連基準との関係

・本ガイドラインは、クラウド利用者向けにISO／IEC 27002を補完する位置づけである。

・米国CSAのガイドラインはクラウド事業者向けの管理策であり、広い意味で利用者にも有用な管理策が追加されている。

・FedRAMPは、米国政府にとってのクラウドコンピューティング認証プログラムであり、調達時の具体的な仕様要件である。

・ENISAのガイドラインは、クラウドコンピューティングにおけるリスク評価を実施し、優先的に講じるべき管理策を参照するものである。

(3) 日本企業にとってのメリット

・本ガイドラインは、ISO／IEC27001 Annex に準拠して作成している。このため

→目次等の構成を合わせ、管理目的等は、ISO／IEC27001 Annex をそのまま準用している。

→全面的にクラウドサービスを利用する際の管理目的達成という究極的状況を想定している。

→差分のみの適用も可能であり、また、情報セキュリテイ監査に活用できるため、クラウド環境におけるセキュリテイ確保、コストが削減できる。

・ISMS(ISO／IEC27001)の取得は日本が世界の取得数の半数以上を占める。このため

→既にISMSを多数取得している我が国企業にとつては、現状のISMS(ISO／IEC27001)に準拠した基準ができる方が有利になる。

・以上から、このガイドランは“クラウドセキユリテイの不安を払拭し、安全なクラウド利用”と“クラウト時代における情報セキュリテイ監査制度の導入”を可能とするものである。

Ⅲ.主な質疑応答

(1)利用者の立場にたった本ガイドラインは評価したい。しかし、情報セキュリティ監査への活用の課題として、無条件に「クラウド事業者の言明を第三者の監査人が保証する」ことは実態的に難しいのではないか。保証という形態も取れないかもしれない。

→ご意見のとおりであり、その主旨は理解できる。

(2)データセンタ、データが海外にある場合の取扱はどうなるのか。提供事業者が詳細を開示しない場合はどうするのか。

→ガイドラインp66「15.1.1 適用法令の識別」にまとめているので参照されたい。

導入利用者としても、提供事業者のコミットメントを確認する必要がある。

(3)クラウド事業者がサービス提供にあたり再委託する場合があるがどう扱うのか。

→典型的な例は、「クラウド事業者のサプライチェーン」で説明したものが該当する。

具体的には、SaaS利用者からみて次の関係になる。

SaaS利用者　→ SaaS事業者A　→　PaaS事業者B　→ IaaS事業者C

(PaaS利用者)　(IaaS利用者)

事業者B、C は再委託先などとなる。

それぞれの事業者に対し、クラウドサービス利用者、提供者の立場における業務分担・責任分担を明確にする必要がある。このガイドラインでは「クラウド利用者のための実施の手引」と「クラウド事業者の実施が望まれる事項」としてまとめているので、参照されたい。

Ⅳ. 感想

大きな流れであるクラウド利用に関して、情報セキュリティ上の不安が利用者、事業者共に強い。しかし、このガイドラインは、クラウドの利用者サイドに立って、「クラウド利用者のための実施の手引」と「クラウド事業者の実施が望まれる事項」を取りまとめたものであり、画期的なガイドランである。これらをベースにした国際標準化を注視しつつ、クラウドの一層の活用とシステム監査への適用を進めたい。

注目情報（9/1～9/30）

■　【IPA は「セキュリティ要件確認支援ツール」を公開（2011/8/17）に注目 】

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）技術本部セキュリティセンターは、8 月 17 日（水）、情報システムの機能・サービスに応じたセキュリティ要件(*1)定義を容易にすることを目的とした「セキュリティ要件確認支援ツール」を IPA のウェブサイトで公開している。

セキュリティに詳しくない情報システム担当者が、情報システムの持つリスク等を考慮してセキュリティ要件を定義することを容易できるようにしたツールであるとのこと。

詳細は　→ https://isec-sras.ipa.go.jp/

■　【クラウド監査　新基準で対応　日経コンピュータ記事（2011/8/18 号）に注目　】

日経コンピュータ 2011.8.18 号で次に次の記事が掲載されていました。

「IIJ や NEC、クラウドサービス監査に着手　新基準への対応で顧客を開拓」

【要約】

IIJ と NEC は 2013 年 3 月までに監査を受けることを表明　NTT コムウェアは準備中とのこと。

SAS70（Statement on Auditing Standard No.70)の適用期間が 2011 年 6 月 15 日で切れる。これに変わる物が SOC(Service Organization Controls)がある。　SOC 詳細は　→ http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx

SOC1(ISAE3402,SSAE16 など)
　J-SOX など財務報告に関する内部統制の整備、運用状況を保証
　会計関連アプリケーションを稼働させる IaaS PaaS が対象
SOC2(AICPA GUIDE など)
　主に企業向けのサービスを対象にコンプライアンス、情報セキュリティ
　などの観点から内部統制の整備・運用状況を保証
　CRM などの顧客情報や取引情報を扱う SaaS が対象
SOC3(Web Trust, SysTrust など)
　主に個人向けのサービスを対象にコンプライアンス、情報セキュリティ
　などの観点から内部統制の整備・運用状況を保証
　決済機能を提供する SaaS や、個人向けのストレージサービスが対象　　と掲載されていました。

以上

全国のイベント・セミナー情報

■【 東京・月例研究会 】

【 9月の月例研究会 】

開催日時　：9月28日（水） 午後6時半から8時半
場所　　：総評会館2階大会議室
講演テーマ：「FISC 安全対策基準の改訂について」（仮題）
講演者　　：公益財団法人　金融情報システムセンター
　　監査安全部　総括主任研究員　松宮伸行　氏

【 10 月の月例研究会(予定) 】

開催日時　：10月28日（水） 午後6時半から8時半
場所　　：総評会館2階大会議室
講演テーマ：「BCMS 適合性評価制度について」（仮称）
講演者　　：一般財団法人日本情報経済社会推進協会
　　情報マネジメント推進センター　副センター長　高取　敏夫　氏

■【近畿支部　システム監査実践セミナー２日間コース】

日本システム監査人協会近畿支部では、システム監査人の実務能力の維持・向上のため「システム監査実践セミナー（2日間コース）」を開催し、ご参加の皆様にもご好評をいただいています。 システム監査を実際に行う機会が少ない現状において、模擬的に体験できる機会を皆様にご提供することを目的としています。システム監査技術者や公認システム監査人を目指されている方、システム監査の実務経験をする機会のない方、システム監査に興味をお持ちの方，内部監査ご担当になられた方など、この機会を利用してシステム監査の実際を体験し、システム監査能力と知識の向上を図りませんか。システム監査に興味をお持ちの方であれば，会員・非会員を問わず参加大歓迎です。

開催　平成 23 年 9 月 23 日（金:祝日）13:00～21:00 ＜1 泊 2 日＞
　　平成 23 年 9 月 24 日（土） 9:00～16:30

詳細は当協会HP（http://www.saaj.or.jp/shibu/kinki/kenkyukai127.html）をご参照ください。

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)

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

□■SAAJ 会報編集担当から連絡（http://www.skansanin.com/saaj/）

会報記事の公開サイトを情報発信サイトとしてリニューアルしています。お気づきになりましたか。
さらに、これまでは会報への投稿者に、記念品として図書券(薄謝)を進呈しておりましたが、全国の投稿者への配布事務が煩雑なため、スムーズに配布できておりませんでしたので、見直しをすすめています。
会報を電子化、月次発行し、個別記事への関心も高まっていることから、今後は、アワード方式とし、全員ではなく、年間で人気のあった記事の投稿者へ、ちょっとうれしい(多めの)謝礼方式に切り替える予定です。

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、またはファイル添付(1MB 未満)するだけです。
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。

■ 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、および購読/解除の申請は、購読申請・解除フォームに申し込んでください。
【お問い合わせ】【購読/解除】　http://www.skansanin.com/saaj/　の SAAJ 会報問い合わせフォーム

■□■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）