研究会報告

ＣＩＡフォーラム研究会報告

『ここから始めるＩＴ監査』Ｑ＆Ａ集

～ＩＴ監査実施のための道しるべ～

研究会No.21－A（システム監査の実施方法サブグループ）

「ＣＩＡフォーラム」は、ＣＩＡ資格保持者の研鑽及び相互交流を目的に活動する、社団法人日本内部監査協会（ＩＩＡ－ＪＡＰＡＮ）の特別研究会である。各研究会は、担当の座長が責任をもって自主的に運営し、研究期間、目標成果を設定し、研究成果を発信している。

この研究報告書は、ＣＩＡフォーラム研究会No.21－Ａが、その活動成果としてとりまとめたものである。報告書に記載された意見やコメントは、研究会の「見解」であり協会の見解を代表するものではなく、協会がこれを保証・賛成・推奨等するものでもない。

はじめに

ＩＴの普及に伴い、現代の企業経営にとって、ＩＴは不可欠のものとなり、ＩＴ監査の重要性が高まっています。更に、近年の個人情報保護法や金融商品取引法等の法制化は、ＩＴ監査を必須のものへと導いています。しかしながら、いざＩＴ監査を実施しようとすると、どこから手をつけたら良いか、何をどのように検証・評価していかねばならないかが、よくわからないというのが、実態ではないでしょうか。

このようなニーズに応えるため、社団法人日本内部監査協会は、ＩＴ監査実施のための「道しるべ」として2007年９月に『ここから始めるＩＴ監査』（同文舘出版㈱）を発刊しました。

当研究会は、2007年12月より、この『ここから始めるＩＴ監査』を、内部監査実務へより効果的に活用するために、本を読んだだけでは理解しにくいことについて、執筆者の方々との質疑応答や研究会メンバー相互のディスカッションにより、疑問点を解消し、ＩＴ監査についての理解を深めてまいりました。本報告書は、研究会での質疑応答やディスカッションを、Ｑ＆Ａの形にまとめたものです。

本報告書を、『ここから始めるＩＴ監査』のサブテキスト的に、ご活用していただくことにより、ＩＴ監査に関心や関わりを持つ、多くの内部監査人の方々のお役に立つことができれば幸いです。

なお、ご多忙のところ、当研究会の運営にご協力をいただいた執筆者の皆様（村田　一様、吉武　一様、金田雅子様、茅野耕治様）に、この場を借りて御礼を申し上げます。

	Q.	A.
第１章　ＩＴ監査とは		
経営とＩＴ	経営目的達成のためにＩＴガバナンスが重要と認識されつつあるが、従来の日本ではＩＴガバナンスの発想がなかったのか？	・ＩＴガバナンスという言葉は米国から伝わっていたが、日本企業の多くではＩＴは専門家の扱うもので、ＩＴに関する経営課題をとらえる概念としてのＩＴガバナンスという発想には至っていなかった。米国ＳＯＸ法の影響で“内部統制”が一般化したその派生で“ＩＴ統制”という言葉も一般化し、ＩＴガバナンスへの認識が高まったと言える。
ＩＴ監査の目的と対象	従来のシステム監査は情報システム部門が主対象だったのか？	・情報システム部門が専門家集団であり、その情報システムに関わる特化した監査としてシステム監査が位置付けされていた。ＩＴガバナンス構築に寄与するために、経営管理層から情報システム部門・各事業部門まで幅広く対象とするＩＴ監査の概念は最近になってからである。
	ＩＴ監査とは、ＩＴ統制の有効性評価と言い換えて良いか？	・ＩＴ監査は、ＩＴガバナンス構築に寄与するという幅広い概念を目指している。広義でのＩＴ統制有効性評価と言えるが、ＩＴ統制監査という言葉が内部統制報告制度に対する狭義の有効性評価として使用されることが多いことから、その目指している内容の区別は重要である。
	ＩＴ監査と、いわゆる従来の日本流システム監査との大きな差異は？	・現在のシステム監査基準では、「組織体のＩＴガバナンスの実現に寄与」と明記されているが、これは2004年の基準作成時に米国の流れを反映させたものである。それ以前のシステム監査は、技術専門家集団に対するシステム技術的監査という考えが中心であり、ＩＴ監査の目指すＩＴガバナンス構築寄与や経営管理層から事業部門までの幅広い監査対象とは異なっていた。
	ＩＴ監査はＣＯＢＩＴ準拠が主流（ディファクトスタンダード）か？	・米国ＩＴガバナンス協会（ＩＴＧＩ）が提唱しているＩＴ統制のフレームワークがＣＯＢＩＴである。ＣＯＢＩＴをベースに、米国ＳＯＸ法の対応のためにＩＴ統制のフレームワークとして“ＣＯＢＩＴ for ＳＯＸ”が発表された。米国でのＳＯＸ法対応を契機として、ＣＯＢＩＴが多くの企業でＩＴ統制のフレームワークとして認知されたことで、ＩＴ統制の監査においてはＣＯＢＩＴ準拠が主流となっている。ただし、ＩＴ統制のフレークワークは、他の機関も提唱しており、日本のシステム管理基準でもＣＯＢＩＴとの対比表を付加することによって適用性を高めているので、監査の目的や監査人の適合性にあった監査基準利用で問題はないものと思われる。
第２章　ＩＴに係るリスクとコントロール		
ＩＴに係るリスク	「ユーザ部門がＩＴ部門へ要求する仕様の枠を超える」とは、どのようなことがあるか？	・次のようなケースが起こり得る。 ユーザ部門の要求機能が間違っていた ユーザ部門の要求機能が不十分であった 法律が新規に制定されたり改正されたりなどの外部の要因により要求機能が変化した 事業モデルを新たに構築したり改訂したりなど内部の要因により要求機能が変化した ・ユーザ部門が軽微と思っている仕様の変更を、力関係の弱い情報システム部門が受けざるを得なくなり、キャパシティオーバー、予算オーバー、納期遅延などを起こしてしまう。

	Q.	A.
	「リスク発生の可能性を低減するために導入する施策の意思決定（投資判断）の責任はユーザ部門」の場合、施策の内容に妥当性があるかどうかを検証するのもユーザ部門か？	・ＩＴリスクの大きさによっては、全社的なリスク管理部門が妥当性を検証する必要がある。 ・ユーザ部門や情報システム部門とは別の部門が評価していく必要がある。
	監査役監査と内部監査とでは、ＩＴリスクのとらえ方に差があるのか？	・監査役は、取締役の職務の執行を監査する立場から見ているので、ＩＴリスクのとらえ方に特徴がある。 監査役監査では、経営戦略の中に有効なＩＴ戦略を組み込んでいるかを確認することが監査の視点である。 内部監査は、主にＩＴ中期計画と個別ＩＴ計画を適切なプロセスで策定していること、また、ＩＴ開発環境と開発プロセスが適正であることを見る。 ・監査役は、取締役がＩＴについて正しい認識を持っているか、ＢＣＰの手当を執行部門に落としているかをチェックする役目がある。内部監査は、執行部門が取締役から指示された事柄を確実に履行しているかどうかをチェックすることになる。このように２者が連携してＩＴガバナンスの確保を確実にする。
	監査役監査と内部監査の良い関係をもたせるには何が大切か？	・監査役監査では、主として経営戦略と情報戦略の方向性の妥当性や整合性を見る。一方、内部監査では、情報戦略と業務処理統制やＩＴ業務処理統制が整合しているのかを見る。このような役割分担を明確にして総合的な監査になるようにすることが大切である。 ・監査役は能力的にＩＴ監査ができない場合が多いので、内部監査部門に依存することが多くなる。例えば、ＩＴ部門が言ってくる予算の中身、トラブルの中身などについて内部監査部門に説明を求めることがある。このようなことから、内部監査部門に対するニーズが高いと思われる。
	リスク管理部門とユーザ部門におけるＩＴリスクの抽出方法に違いがあるのか？	・リスク管理部門の対象は、全社的なレベルであり、業務部門で行うレベルとは違う。 リスク管理部門では、全社に共通的な法令リスク、共通的な基準（財務報告、環境、安全など）に関係するＩＴリスクが中心である。 ユーザ部門では、業務を遂行するプロセスの各行為におけるすべての脅威がＩＴリスク抽出の対象になる。 ・リスク管理部門は、ビジネスリスクとＩＴリスクを正しく抽出していることを確認する。ユーザ部門は、ビジネスリスクを抽出し、情報システム部門はＩＴリスクを抽出する。
	ＩＴ統制目標として定義されている、 「金融商品取引法の実施基準」 「経済産業省のシステム管理基準」 「日本公認会計士協会のＩＴ委員会報告第３号」 には、内容に大きな違いがあるのか？	・統制の基準、すなわち、有効性、効率性、準拠性、信頼性、可用性、機密性、網羅性などの観点で見ると、統制目標に大きな違いはない。 違いは、基準の利用者（ある専門領域の、システム監査人、ユーザ部門）をそれぞれ想定していることから、対象となる事項が利用者固有のものになっている。 ・ただし、Ｊ－ＳＯＸや日本公認会計士協会の基準では、有効性や効率性を取り上げていない。
	リスク・シナリオを作成するために行うリスクの洗い出し作業は、膨大な作業量にな	・次のように考えることができる。 リスク抽出

	Q.	A.
	るので、何らかの作業基準（粗い抽出基準、粗いリスク評価基準）の設定が必要ではないか？	リスク管理の手順を考えると、リスク管理部門が業務の流れを理解しないままにリスク抽出を行うのは困難である。 各ユーザ部門にリスクの抽出を依頼するとした場合、各部門がＩＴリスクを的確に認識しているとは限らないので、ＩＴリスクだけでなく、すべてのリスクの洗い出しを求めることになる。 この場合、部門によってリスクの洗い出しの精粗があったり、リスク発現時の影響が極めて小さいものがあがったりしがちである。 そこで、影響がある程度大きいものという抽出基準を仮に設ける。
	ＩＴの有効性はどのようにして測るのか？	・ＩＴの有効性とは、ＩＴがその利用目的に適合しているか、あるいはどの程度達成しているかを言う。 利用目的に適合するための要因には、 システムの品質 情報の品質 利用の容易性 有用性の知覚 利用の回数 業務改善の進み具合 就業環境の改善度合い ＩＴへの満足度 経済的な利益 組織の競争力や環境適応力への貢献度 などがあり、これらを総合評価する必要がある。 ・評価の尺度として、ＩＳＡＣＡのVal IT Framework「ＩＴ投資の企業価値ガバナンス」が参考になる。
	ＩＴの有効性を評価する標準的な手順があるか？	・標準的な手順というのはないが、次のようなプロセスになると考える。 情報システムの目的の認識 有効性に係わる評価尺度の選択 評価に必要なデータの存在の認識 情報システム導入前の評価値の入手 情報システム導入後の評価値の入手 導入前と導入後の評価値の比較による有効性の評価
リスクとコントロールの関係	業務処理統制項目の多くがアプリケーションシステムに組み込まれていて自動化されているケースが多いので、その正当性を確かめるために内部監査部門が留意すべきことは何があるか？	・正当性の確認は、開発環境の面と開発プロセス面で考える必要がある。 開発環境面では、ＩＴ業務処理統制項目を考慮した開発環境になっていることを確認すること 開発プロセス面では、企画、基本設計、詳細設計、プログラム製造、テスト、本番稼動のそれぞれの節目において、必要なＩＴ業務処理統制項目がシステムに組み込まれていることを確認すること ・業務処理パッケージについては、日本公認会計士協会のＩＴ委員会報告３号にＱ＆Ａがあり、その中で広く使われているパッケージでカスタマイズせずに使っている場合は特に確認を要しない、そうでない場合はカスタマイズが有効にコントロールされていることを確認することとしている。内部監査部門もこれに準じて判断すれば良い。一般に、パッケージの監査では、入力チェック、

	Q.	A.
		自動計算、自動仕分けが有効にコントロールされていることを想定しているので、ドキュメントを調べてきちんと書かれているか、説明を受けるかをしなくてはならない。すなわち、米国ＳＯＸ法でいう、要求、実装、テスト結果をきちんと追う必要がある。
	自社開発システムプロセスにおける業務処理統制項目の確認の手段として、プログラム仕様書、プログラム単体テスト仕様書、テスト結果の正当性を確認するための事前準備として何が必要か？	・ＩＴ業務処理統制項目について、プログラム仕様書、プログラム単体仕様書のどこに反映されているかを容易に確認できるようにインデックス付けをシステム開発部門に要請しておく。 ・プログラムの目的に合致していることを各ドキュメントやテスト結果を精査することが必要である。プログラムの目的を果たすためには、業務処理が正しくなされていること、ＩＴを使った統制項目があり、これらが有効に作り込まれていることをチェックするのだが、すべてのプログラムを調べると労力がかかりすぎるので、実際にはサンプリングして確認することになる。
第３章　ＩＴ監査の実施方法		
ＩＴ監査実施のための環境	ＩＴに係るリスクに対するコントロールの存在を示す各種記録やドキュメントは具体的にどのようなものか？　例示してもらえないか？	・定期的な点検や事故の報告、ヘルプデスクの記録、ログ、ログ分析等である。
	ＩＴ監査人の育成は、どのようなパターンを推奨するか？	・ＩＴ監査を内部監査人が、システム部門の応援を得て実施することから始める。一緒にＩＴ監査をしながら、徐々に内部監査人がＩＴ監査のスキルを身につけていくパターンを推奨する。
ＩＴ監査のプロセス	監査実施／評価対象の範囲については、どのタイミングで検討するのか？	・初回のＩＴ監査か、継続的ＩＴ監査であるのかによって異なることが考えられる。また対象についても人、組織、プロセス（業務）等により違いがあり、更に監査対象のＩＴ（システム）内容によりそれぞれ違いがあるので、一概にはこのタイミングでということは言えない。
	Ｊ－ＳＯＸ対応のＩＴ統制（全社統制／ＩＴ全般統制）評価方針との整合性・関連性について検討する必要はあるか？	・この検討は、まずどこが（誰が）行うのか、という観点からその必要性を考えることがポイントであり、米国ＳＯＸ法対応を例にとるならば、その対応部門としては「ミドル」部門が受け皿になってきているケースが多いようである。日本の場合には内部監査部門がＪ－ＳＯＸ対応部門として受け皿になるかどうか、は議論が分かれている。 ＩＴ監査はＪ－ＳＯＸ上のＩＴ統制評価方針を考慮する必要があるが、こうしたＪ－ＳＯＸ、業務監査、ＩＴ監査それぞれの立ち位置が異なれば調整が必要になる。
	リスク評価の最新とは、直近の評価のことを示すのか？	・一番手前で行われたリスク評価を示すので、それが例えば１年前であれば、「最新」ということになる。リスク評価のタイミングに依存するものである。
	中長期監査計画の「取締役会等の承認」を得る目的は、経営資源の確保以外にはどのようなものがあるか？	・ＩＴ監査実施上、１）アクセス権限　２）ＩＴ監査対象組織（子会社を含む）へのアクセス　３）クリティカルなシステムを監査対象とする　等のケースで事前に取締役会の承認を得る必要がある。
	「当該年度……」とは、通常の会計期である期間を示していると考えて良いか？	・通常の会計期を示している。

	Q.	A.
	通常の内部監査計画と比較して、ＩＴ監査計画策定上の特徴とはどのようなものか？(特に短期監査計画上)	・監査対象自体がＩＴという特性を持つので、そこに通常の内部監査計画との違いや特徴がＩＴ監査計画策定上、特に短期監査計画の内容に現れることがある。例えばＩＴ開発プロセスの各段階に合わせて、必要項目についての適時監査を実施する計画などがある。
	監査対象にもよるが、予備調査にかける日数は平均何日くらいか？	・監査対象（ＩＴ全般統制、情報セキュリティ監査、ＩＴ業務処理統制、開発段階のＩＴ監査等）により、予備調査にかける日数がまちまちなので､一概には言えない。大切なことは予備調査としてどこまでヒアリングするか、会社として決めておく必要がある。予備調査の範囲が、本調査でのヒアリング範囲に影響を与える。なお、実務的には予備調査と本調査での、一部の質問の重複は致し方ない側面がある。
	財務会計処理システムを監査対象とした場合、Ｊ－ＳＯＸにおけるＩＴ業務処理統制との関連はどうなるのか？（リスクとコントロールは？）	・かなり重複する部分があると思われる。ただし、Ｊ－ＳＯＸにおけるＩＴ業務処理統制と一般的なＩＴ監査におけるＩＴ業務処理統制は、その監査範囲が違うことに注意する。
	基準、あるべき姿とは、具体的にはどのようなものか？　基準のよりどころとなるものは何かあるのか？	・システム管理基準や、ＣＯＢＩＴ等の汎用的な規範を基に、各会社や各組織のＩＴ成熟度に呼応した作成したシステム開発・保守・運用等の各種基準やあるべき姿をいう。大切なことは、絶対的な最終目標である基準を設定するのではなく、あくまで各組織の個性に合わせて設定する必要がある。
	図表３－11　40「本番データ貸出に関する依頼書及び取扱手順」は、どのようなケースに発生するのか？	・開発した（修正の場合もある）アプリケーションを試験する段階で、より現実的な試験を実施するという名目で本番データを使用する場合がある。また、障害を調査する際に、本番環境に直接アクセスできないため、試験環境又は開発環境に本番データをコピーして調査する場合もある。 一般的に、本番環境に比べて、試験環境又は開発環境はセキュリティが甘く、より多くの人がアクセス可能なため、機密性の面でリスクがある。 そのため、本番データの貸出は最小限とし、正当な依頼書に基づいて貸出され、使用中は本番環境と同様にアクセス制限され、試験・調査の終了時には確実に消去される等の手順が定められている必要がある。 一般的には、生の本番データを貸出すのではなく、個人情報等をマスク処理したテストデータに変換して貸出す場合が多い。
	図表３－11　68「プロジェクトの評価」についてのＩＴ監査について、多くの日本企業で実際に行っているのか。もし、そうであれば業種はどのような企業か？	・プロジェクトの絶対的な評価手法と言えるものはなく、評価自体非常に難しい。しかしながら、次のプロジェクトを成功に導くためには、過去のプロジェクトの実績が正直に残っていることが必要である。その点から、最低限プロジェクトの記録が正確に残っていることが必要ではないだろうか。そのような記録が残っていないような場合、同じような失敗を繰り返すリスクがある。
	図表３－11　78「本番データ修正に関する記録」とは、ＤＢＭＳのユーティティＰＧＭを使用して実施するデータ修正か（関連データの修正が実施されない可能性あ	・本番データは一連のアプリケーションで処理されて初めて整合性を維持できる。ユーティリティプログラムを使用したデータ修正は、例外処理であり、データの不整合を招きやすい。

	Q.	A.
	り）？　それとも、特別にアプリケーションＰＧＭを作成して、そのＰＧＭによる修正か？	そのため、本番データ修正は厳密に管理されなければならない。場合によっては、開発者まで問合せて、隠れた制約事項がないか確認が必要なことも考えられる。 そもそも、手動でデータの整合性をとらなければいけないようなシステムは望ましくなく、最低でも不整合を検出する仕組み、できればある程度自動的に不整合を解決する機能を持つべきである。
	ＩＴ監査において、ＣＡＡＴｓを実際に使用している企業はあるのか？　どの程度のスキルが必要なのか？	・金融機関等で実際に使用している事例は見受けられるが、一般事業会社で使用されている事例は、まだ少ないと考えられる。
	監査モジュール法は、常時継続的監査活動であり、またユーザ管理業務の側面からは、常時継続的事後統制とも言えるか。	・そのとおりである。監査モジュール法を導入すると異常値のモニタリング業務がユーザ側で実施できることになる。
	ＩＴ監査における運用状況検証と実証性検証との関係は、財務諸表監査における「運用評価手続」と「実証手続」との関係と同義か？　ＩＴ監査における実証性検証とは、どのようなことを意味するのか？ i.e.）設定したコントロールが適切か否か直接的に検証する？	・そもそも財務諸表監査における実証手続は、期末の財務諸表残高に対する経営者のアサーション（例えば、売掛金の実在性等）を直接的に検証するために監査証拠を入手することである。運用評価手続によって運用状況が良好と判断された場合、実証手続の範囲は狭くなる。一方、運用状況が良好でないと判断された場合、実証手続の範囲は広くなる。全く良好でない場合、試査による検証が実施できず精査する必要がある。 ・このような財務諸表監査における運用評価手続と実証手続の関係はＩＴ監査においては明確には見られない。ＩＴ監査における実証性検証は、実際に運用状況が有効であるということを、発生したインシデントから遡って直接的に検証することである。例えば、システム運用が設計どおりきちんと運用されていても、システム障害が発生したとする。この場合、システム障害が発生した真の原因を追究することにより、より効果的なＩＴ統制が再設計されることになる。
	Ｊ－ＳＯＸにおいては、そもそも実証性検証という概念は存在するのか？	・Ｊ－ＳＯＸの対象は、あくまで会社の財務報告に係る内部統制の整備・運用状況を評価することにある。よって、Ｊ－ＳＯＸにおいては実証性検証という概念は存在しない。なお、評価の結果、重要な欠陥が存在し、その欠陥が財務諸表に与える影響額を見積もった後に、財務諸表監査において実証性検証の監査範囲を広くしたり、より証拠力の高い監査証拠の入手が必要になるといった､内部統制監査と財務諸表監査との連携は必要となる。ただし、この連携はあくまでも外部監査人である監査法人に求められるものであり、会社が、実際にこの連携を行うものではない。
	日常のモニタリング状況と結果を年次報告書に記載しているケースは多いのか（経営陣へのアピールになる）？	・それほど、多くないと考えられる。実際に企業においてどのような種類のモニタリング状況を、どの程度のレベルまで記載するのか、他社事例を収集したい。また、この記載をすることによって、経営者に何をアピールするのか明確にするべきである。
	ＩＴ監査以外の通常の内部監査と同一の報告書に記載すると考えて良いか？	・実際行ったＩＴ監査のボリュームによる。通常の業務プロセス監査と同じくらいのボリュームであれば各々、独立させて記載することもある。
	継続的に監視するプロセスについて、ＩＴ	・通常の業務プロセス監査と違い、ＩＴ監査においては

	Q.	A.
	監査におけるフォローアップ・プロセスに特有なポイントは何か？	そのフォローアップ・プロセスが比較的長期にわたるため、モニタリング、是正アクション、フォローアップ監査を効果的に組み合わせる必要がある。いずれにせよＰＤＣＡサイクルをきちんとまわすことが大切である。また、助言やファシリテーション等で支援する場合の留意事項として、あくまで意思決定権限は被監査部門にあるということである。将来の監査実施のために独立性はきちんと確保しておく必要がある。
	他社ではどの程度徹底してフォローアップ監査を実施しているか？　例えば、フォローアップ状況を示す根拠資料の入手のみか、もしくは資料入手＋インタビューを実施するか、あるいは現場に赴きフォローアップ結果の運用状況を検証すべくサンプリングで検証を行うか？　等々	・会社によって様々である。内部監査で発見された指摘事項ができるだけきちんと改善されるようにするために、一定期間ごとに取締役会への報告会を行うと良い。特に取締役会のメンバーに社外取締役の方がいると、社長を含め社内取締役への内部監査での指摘事項に対して積極的な改善への牽制につながる。
第４章　ＩＴ監査実施上の要点		
システム・ライフサイクルに沿った監査	システム・ライフサイクルに沿った視点で情報システムの正常な稼動の確保を支援していくには、内部監査のアシュアランス機能とコンサルティング機能の、どちらの機能を発揮すれば良いか？	・これは、経営者のニーズによって決まる。内部監査部門と経営者の意思疎通の中で、そのニーズを的確にとらえ、アシュアランスを求められているのか、コンサルティングを求められているのかを見極めていくべきであり、その結果を監査計画として反映させて、監査を実施する。
	企画・開発段階におけるプロジェクト・マネジメントの適切性監査のメリット及び実施に向けて想定される障害は？	・メリット：当段階の監査での指摘・改善は、運用・保守段階での指摘・改善に比較して、コストを低くおさえることができる。 プロジェクトは初めが肝心であり、企画段階でプロジェクトの初めから終りまでの間にどのようなことが起こるのか想像（リスク評価）して、対応策を検討するといったことに時間をかけることが、結果的にプロジェクトを効率的に終わらせることになる。監査としては、プロジェクトの計画の妥当性(適切なステップを踏んでいるか)の重要性をプロジェクトメンバーに認識してもらう、またはその認識があるか確認し、プロジェクトとしてやるべきことの実施を促すことが重要である。 ・障害：企画・開発段階では内容が固まっていないことが多いので、監査のタイミングが難しいし、具体的な指摘が困難である。また、往々にして企画段階でユーザの意図が適切に反映されない、システム開発側との行き違いがみられる。ユーザ目線で監査することが重要ではないか。
	財務報告に係る内部統制報告制度で要請されるＩＴの統制の設計は、システム・ライフサイクルのどの段階で考慮するべきか？	・言うまでもないことであるが、企画段階で設計に盛り込まれることとなる。多くの事業会社では、ＩＴの統制の思想が欠けていたようであり､当制度の実施によって、徐々に改善が進んでいくものと思われる。
	企画段階において、費用対効果の妥当性監査を実施する際のポイントは？	・システム開発の効果測定は、明確な基準がないこともあって、難しい面がある。最近では、ValＩＴという投資効果測定の理論が出ているので、参考にすると良い。 ・費用については、費用見積りのプロセスをチェックする、過去のプロジェクトとの比較をする等で妥当性をみていくことが重要である。また、コンサルタント等の

	Q.	A.
		（外部）専門家の見積りであっても、全幅の信頼をおくことなく、その妥当性をチェックするべきである。
	監査での指摘に対して、被監査部門が従わない場合があるが、どのように対応すると良いか？	・自社（のシステム開発で）の失敗事例を集めておき、指摘事項に適したリスク事例を提示し、被監査部門による適切なリスク対応を促すことで理解が深まり、監査指摘事項の採用率アップにつながっていく。監査指摘事項の具体性が重要である。
	システム開発を外部委託している場合のシステム・ライフサイクル監査の留意点は？	・企画フェーズでは、外部委託及び委託先選定の妥当性をチェックする。 ・開発フェーズでは、進捗管理が単に委託先からの報告書をファイルしているだけ、予定より遅れていることが報告されているのに委託元として対応していない等おざなり（丸投げ）になっていないか妥当性をチェックする。
	システム開発の外部委託先を直接監査する場合の留意点は何か？	・直接、外部委託先を監査する場合には、まず委託先との契約書に条項を盛り込んで、監査実施の根拠とする。監査の具体的手法としては、情報システム部門の外部委託先ヒアリングに帯同して監査を実施する等が考えられる。
	システム開発の外部委託は、委託先の再委託、再々委託等が実態として多くみられるが、どこまでを監査の対象・範囲とするべきか？	・例えば、再々委託先まで把握しようとすると、その数は膨大なものとなり、管理は困難である。実務上は、委託元として委託先が再委託する場合には、必ず報告をもらうようになっており、その管理が適切になされているかをチェックすれば良いのではないか。
	テストが適切に行われているかをチェックするには、どのような手法があるか？	・一例として、システム・バグ件数とテスト件数の関連性の分析的手続（グラフ化してモニタリング等）を実施して、異常値等チェックする。テストは品質確保の重要な局面であるが、始めに結論ありき（問題なし）のテストが、プロジェクトの納期や費用等の問題で行われがちであるので、その点に注意してみることである。
	システム開発プロジェクトを評価するに当たっての指標には、具体的にどのようなものがあるか？	・システム部門が実施するシステム実現機能のユーザ満足度調査結果（例：４段階評価） ・ユーザからの問合せ、照会内容及び件数 ・システム障害の発生件数 ・予算と実績の比較、分析 がある。特に予実比をしっかりと実施して、今後の糧となる経験値が蓄えられているかをチェックする。
	保守担当者は、運用担当者と職務分離が必要とあるが、人員不足等で分離できない場合、どのような統制をしけば良いか（職務分掌に代わる代替的な統制とは）？	・担当者のローテーション ・強制休暇や長期出張の制度化 ・システム変更の場合には、必ず上長の承認をとる ・運用担当者が本番環境にアクセスできる場合は、アクセスログを収集しモニタリングできるようにして、上長等の第三者によるチェックを実施する ・内部監査の実施頻度を上げる 等を代替統制として検討すると良い。
	企画フェーズのユーザによる成果物の検収条件とは、具体的に何か？	・各段階での成果物（設計書・テスト結果報告書・ユーザマニュアル等）から、どの時点でどの成果物をユーザに提示し、検収を受けるかを明確にし、企画段階で決定することである。
	開発フェーズのサービス・イン判定基準、	・サービス・インとはカット・オーバーとも言われ、そ

	Q.	A.
	判定プロセスとは、どのようなものか？	の判定基準は、開発したシステムを本格稼動（本番環境）に移行するための判断基準である。具体的には、バグは解消しているか、操作マニュアルは作成されているか、必要なユーザ教育は完了しているか等である。 ・サービス・イン判定プロセスは、基準に基づく確認が適切に実施されているか、あらかじめ定められた承認権限者が判定しているか等がチェックポイントとなる。
情報セキュリティ監査	コラム「情報セキュリティ監査制度」の４）では、「保証型監査」と「助言型監査」と書かれている。内部監査人協会（ＩＩＡ）内部監査の専門職的実施の国際基準で定義されたAssurance Services とConsulting Servicesとは異なる概念と考えるべきか？同じく、冒頭の７頁にも記載された「アシュアランス」と「コンサルティング」との関係はどうか？	・異なった独立の概念として考えるべきである。
	③評価・監査：「グラフを利用した成熟度モデル例」では、情報セキュリティ監査の項目以外にも、次章の事業継続計画等も入っているが、あくまでもこれらは例示ということで理解して良いか？	例示である。経済産業省の「情報セキュリティ管理基準Ver1.0」を参考にしている。ただし、『事業継続管理』が『事業継続計画』になっているが、意図はない。 「情報セキュリティ管理基準Ver1.0」は、平成21年１月31日廃止である。代わって、平成20年改正版が公表されている。参考まで。
	③評価・監査：網掛け部分「情報セキュリティ監査で参考として使用する成熟度モデル」で３つのモデルが示されている。そのレベルが４－５段階だが、その区分数が近い理由は何かあるのか？　また、並べた意味は横方向の記載は同一、又は、近いという意味なのか、単にレベルの強弱を示すものであって、特に横の関連性はないのか？	・ＣＯＢＩＴがこれらの原型であり、そこから派生したモデルなので、ほぼ同系のモデルである。
	⑷迄に説明されてきた体制整備ではなく、この⑸と「⑹アクセス・コントロール」とあわせて個別に情報セキュリティ項目が記載されている。次の⑹アクセス・コントロールとあわせて、なぜここに個別に記載されているのか？　仮に重要であるとすると、重要監査項目として整理した方がわかりやすくないか？	・初めてのＩＴ監査ということで、初心者としても重要な項目を敢えて取り上げている。
	情報セキュリティとは、大きく分ければ、＜マネジメント態勢＞と＜安全対策及びアクセス・コントロール＞と見て良いのか？　例えば、㈶金融情報システムセンター（ＦＩＳＣ）にあるような、機密情報管理、コンピュータウィルス等の不正プログラム対策、顧客データ保護、ネットワークセキュリティは含まれないのか？	・この項目も初心者向けなので、重要な項目とした。もちろんあげられた項目も重要ではある。
事業継続管理	ＢＣＭとリスクマネジメントの関係は？	・リスクマネジメントの過程で洗い出されたリスクのうち、事業中断に関わるリスクに対する組織的な統制活動がＢＣＭだといえる。すなわち、ＢＣＭはリスクマネジメントの一側面である。

	Q.	A.
	一般的には、ＢＣＭはリスクマネジメントの一環として実施するのか？　それとも、ＢＣＭは単独で実施するべきか？	・あるべき論でいえば、ＢＣＭはリスクマネジメントの一側面なので、ＢＣＭをリスクマネジメントと切り離して単独で実施するのは望ましくないといえる。しかし、実際に態勢を整える段階では、ＢＣＭをリスクマネジメントと切り離す組織が多いのではないだろうか。
	ＢＣＭはＩＴ関係だけ取り出して単独で実施する方が効果的か？　それとも、ＢＣＭはあくまでも範囲を限定せず全社的に行うべきか？	・これもあるべき論でいえば、ＩＴだけを切り離して単独でＢＣＭを実施するべきではない。歴史的にＩＴ関係のＢＣＭは先行しているので、ＢＣＭといえばＩＴとなりがちだが、あくまでも業務継続のためのＩＴである。ただし、監査の観点でＩＴだけを対象とすることはあり得る。
	ＢＣＭに関わる「脅威」としては、どのようなものが考えられるか？	・事故災害（火災等）、自然災害（地震・台風等）、人的災害（テロ・不正利用等）、感染症（新型インフルエンザ等）、技術的災害（停電・コンピュータ障害・ネットワーク障害等）、社会インフラの障害（電気・水道・公共交通機関等の停止等）などが考えられる。取引先の倒産なども考えられる。
	コンティンジェンシープランの説明にいう、「Recoverabilityを確保する対応策」としての「脅威発生に備えた事前準備」とはどのようなものが考えられるか？	・「Recoverabilityを確保する対応策」としての「脅威発生に備えた事前準備」としては、例えばバックアップシステムの用意、安全在庫の確保、食料の備蓄、要員の訓練などが考えられる。
	「拠点」はロケーションのみで判断すべきか？　すなわち、 ①ロケーションが独立していればすべて別拠点 ②同一ロケーションであれば、業務内容が異なる組織でも同一拠点か？	・「拠点」の判断はロケーションが基本であるが、業務内容によっても別拠点とする方が良い場合がある。ただし、後者は組織の規模、責任体制等が影響する。 つまり、①は別拠点とほぼ言い切れるが、②は条件によって変わる。
	ビジネス影響度分析に使用する指標としては、損失予想金額のほかにどのようなものがあるか？	定量的な評価項目としては、 ・業務停止に伴い発生する違約金の額 ・業務停止の影響を受けるユーザ数・取引先数 ・ロストする在庫量　等 定性的な評価項目としては、 ・社会的な評判や信用の失墜 ・従業員の士気低下 ・社会全体に与える影響　等 がある。
	導入フェーズにおいて、「外部機関との必要な情報の共有も重要である」とあるが、これは、どのようなことを想定しているのか？	・「外部機関」とは、主に外部の業務委託先を想定している。「外部機関との必要な情報の共有も重要である」の趣旨は、外部の業務委託先ともＢＣＰを共有しなければＢＣＭ態勢は機能しない、ということである。
	リスク評価手順は、必ず業務の洗い出しから始めるのか？　脅威を先に仮定する方が考えやすいと思われるが。 また、わが国の代表的なガイドラインである、日本銀行「金融機関における業務継続体制の整備について」（2003年）、内閣府「事業継続ガイドライン第一版」（2005年）でも潜在的脅威を特定することから始めている。	・ＢＣＭの理論からすれば業務の洗い出しから始めることになる。しかし、業務を先に特定し、後から脅威の洗い出しを行うと、複数の脅威が想定される可能性があるが、だからといって、それら複数の脅威に対して一度に対応策を作ることは容易ではない。そのため、実務的には脅威を先に特定するケースが多くなると思われる。ただし、リスク・シナリオを作成する段階では、脅威が複合的に発生した場合を想定しなければならない。 現実的には、脅威として地震と感染症を想定してＢＣＭ態勢を構築するケースが多くなると思われる。

	Q.	A.
	「通常時の（ＢＣＭ）組織体制」と「脅威顕在化時の（ＢＣＭ）組織体制」が異なるのは、例えばどのようなケースか？	・「通常時の（ＢＣＭ）組織体制」はＢＣＭを有効に運営するための体制、「脅威顕在化時の（ＢＣＭ）組織体制」は情報や指揮・命令を速やかに伝達させるための体制である。ＢＣＰの方針策定、ビジネス影響度分析、コンティンジェンシープランの策定・テスト等を統括する部署と脅威発生時の対策本部（コンティンジェンシープランの発動判断責任者を長とする）とが異なるケースである。例えば、前者をリスク管理部門、後者を総務部門とするケースである。
	脅威が複数特定された場合、ＢＣＰやコンティンジェンシープランは脅威ごとに作成するのか？　それともすべての脅威が複合的に発生したと想定して１つに集約するのか？	・例えば、脅威が地震と感染症では組織が受ける影響、とるべき対応策はそれぞれ異なると考えられる。効果的なＢＣＰ・コンティンジェンシープランとするためには、それらを脅威ごとに作成するべきである。 なお、日本銀行「金融機関における業務継続体制の整備について」（2003年）に、ＢＣＰは「少数のシナリオ（被災シナリオ）に基づき策定することが重要である」とあるのは、現実的に、すべてのプランが一度に作成できるわけではないので、まずは少数の重大な脅威を想定してひととおり作成してしまうことが重要である、という意味もあるのではないか。
	コンティンジェンシープランは「対応手順を示した文書の総称」としながら、ＢＣＭ関連文書の説明の中で各手順書と同格に併記されているのはなぜか？	・正しくは以下のとおり。 誤：ＢＣＭ関連文書（ＢＣＰの方針、コンティンジェンシープラン、初期対応手順書、暫定対応手順書、本格復旧手順書等） ↓ 正：ＢＣＭ関連文書（ＢＣＰの方針、コンティンジェンシープラン（初期対応手順書、暫定対応手順書、本格復旧手順書等）等）
	ＢＣＭ関連文書の説明には、Availabilityを確保する対応策に関する文書についての言及がないが、そのような文書は存在しないのか？	・そのようなことはない。ＢＣＭ関連文書にはＢＣＰそのものが含まれるので、当然Availabilityを確保する対応策に関する文書も含まれる。
	ＢＣＭに対する監査の基準はあるか？	・ＢＣＭに対する監査の基準というものは存在しないが、ＢＣＭ自体の基準（ガイドライン）の裏返しということがいえるので、それらを利用することが可能である。ＢＣＭの基準・ガイドラインには、海外のものとしては、英国で2006年に発効したBS25999等、日本のものとしては、日本銀行が2003年に公表した指針「金融機関における業務継続体制の整備について」等がある。
第５章　ネットワーク・システム監査実施上の要点		
ネットワーク・システムの仕組みと構成要素	しっかりした管理体制とは、どのようなものか？	・『ここから始めるＩＴ監査』の181頁重点チェックポイントに記載されているので参照されたい。
	ネットワークの規模、質等で標準的管理体制なるものがあるのか？	・標準的な管理体制なるものは特にないが、各企業が自社のシステムや業務について、リスク評価を行い、その結果に対して適切な管理体制を構築することが大切。
	安全かつ経済的に高い信頼性とは、どの程度の費用をネットワーク維持費用にかければ良いのか？	・売上や収益に対して何％かければ良いというものではなく、ネットワーク管理者が自社のネットワークを評価して、必要な費用を見積もることが大切。内部監査としては、その申請が妥当かどうかを評価する。

	Q.	A.
	クライアントサーバ型とインターネット型では、安全性、効率性、経済性、利便性でどのような違いがあるのか？	・クライアントサーバ型は社内ネットワークを中心に利用する場合には、安全性・効率性の面で効果がある。 ・インターネット型は世界中のサーバとつながるオープンなネットワークで非常に利便性があり、経済的にも費用が安いというメリットがあるが、安全性には、問題がある。
	現在はどの仕組みが多く採用されているのか？	・インターネット型である。
	ＯＳＩ参照モデルがＴＣＰ／ＩＰとの普及競争に負けた理由は何か？	・ＴＣＰ／ＩＰモデルの方が階層も少なく利用しやすかった。
	専用線か公衆網を選択する場合は、何を基準にしたら良いものか？	・専用線を選択する場合は、支店とか関連会社等、同一の地点と大量のデータのやり取りをする場合には効果がある。現在はインターネットの普及があり公衆網の選択が多い。
	料金の決定はどのような方法で計算するのか？	・ＮＴＴ等の通信会社が定額か、従量制かで独自の計算方法で課金している。
	最大４台で設置を制限している理由は何か？	・リピータやハブを使ってケーブル長さを延長して、最大４台（５台でもいける場合あり）までに制限しているのは、延長することにより、性能が下がり通信ができない状態になるためである。
	外からのアクセスを制限する制御は、ルータはソフトウェアで、Ｌ３スィッチはその部分をハードウェア化で処理しているとあるが、どちらも、ソフトウェアでもハードウェアでもできるということか？	・どちらでもできる。
	電子メールは、送信はＳＭＴＰ、受信はＰＯＰ３で通信しているが、送信と受信でなぜ分かれているのか？	・送信は単にメールを出すだけの機能、受信はメールの分配、保存等の多種の機能が必要なので、ＳＭＴＰは送信、ＰＯＰ３は受信専用の通信規約を使用している。
	許可されているＨＴＴＰ通信に紛れている悪意ある内容を止めることができない場合、次善の策はあるのか？	・アプリケーション側に脆弱性がなければ、悪意ある内容が紛れていても問題ないことになるが、後から脆弱性が発見されることもあるため、次善の策としてWeb Application Firewall（ＷＡＦ）を導入し、悪意ある内容を検出した際には遮断する。ＩＤＳ／ＩＰＳもＷＡＦも通信を監視し、不正な通信を警告・遮断するものだが、ＩＤＳ／ＩＰＳが不正な通信手段・パターンを監視するのに対して、ＷＡＦはＨＴＴＰ通信の中の入力値等の内容を監視する点で性格が異なる。
	プロキシサーバはどのネットワークにも設置してあるものか？	・どのネットワークにも必ず入っているとは言えないが、大部分のネットワークにはキャッシュ機能を使用するため、設置されている。
	不正検出型、異常検出型、ホスト型、ネットワーク型とあるが、組み合わせで相性の善し悪しはあるのか？	・組み合わせでの相性の善し悪しというものではなく、検知の仕組みで不正検出型ＩＤＳ・異常検出型ＩＤＳの２つに分類され、ＩＤＳの設置場所により、監視するコンピュータにインストールして使うホスト型と、ネットワークに接続し、監視するネットワーク型に分類される。
	ＩＤＳを拡張するとは、具体的にはどういうことか？	・ネットワーク型のＩＰＳはＩＤＳの機能を拡張し、登録された不正な通信を検出した時に、パケットを破棄したり、通信を遮断したりするもの。

	Q.	A.
	管理者が想定する許可された通信パターンとは、どのような、又はどのくらいの数のパターンをいうのか？	・許可された通信パターンの方が多いため、一般的には許可されない不正な通信パターンを検出する（ネガティブモデル）。不正な通信パターンには特徴があり、この特性値を基に検出する。この特性値の設定は管理者が手動で行うのではなく、ＷＡＦのメーカーが「シグネチャ」として供給している。ウイルス対策ソフトのパターンファイルのようなものである。そのため、最新のパターンに更新していないと検出できないことになる。ＩＤＳ／ＩＰＳやＷＡＦは所詮機械なので、誤検出が発生する（正当な通信が不正として誤って検出されてしまう）。誤検出か否かを判定するのは、最終的には人間になる。そのため、これらの機器は、導入費用だけでなく、監視や維持のためのランニング・コストが結構かかるため、注意が必要である。
	アプリケーションによる暗号化と、伝送経路自体の暗号化のどちらかを使用する決め手は何か？	・伝送路を流れる通信をすべて固定的に暗号化するのであれば、伝送路自体の暗号化を選択する。暗号化には処理の手間がかかるため、伝送路のパフォーマンスは低下する。そのため、暗号化通信がわずかであれば、アプリケーションによる暗号化を選択する。一般的に、インターネット上の通信では、アプリケーションによる暗号化（ＳＳＬ等）が行われている。
	ここの説明のＲＡＩＤやリダンダント電源はフェールソフトよりフェールオーバーとして捉える必要があるとの考えもあるが、 ・フェールセーフ⇒システムを安全に停止させる ・フェールソフト⇒故障部分を切り離して、処理を継続する ・フェールオーバー⇒バックアップ と言い換えて良いか？	・クラスタ構成のサーバなどで、稼動系から待機系へ切り替わること。 再び、待機系から稼動系へ切り替わる（戻る）ことをフェイル・バックという。
	個人情報保護法との関係は？　個人情報の不正入手以外にどのような脅威が想定されるか？	・企業の営業を妨害するなどの脅威が考えられる。
	「システム管理者の防御措置の努力義務」⇒どのような責任を問われるのか？	・特段、具体的に問われることはない。
	ネットワークの帯域を枯渇させるというのはどのような状況か？　ファイアウォールで外部ネットワークを遮断するだけでは不十分か。ＩＰＳを導入した場合の相対的な費用対効果は？	・帯域が枯渇するとは、通信量が限界値を超え、通信処理待ちが発生した状況である。故意に不要な通信を生み出して、通信を妨害することが、インターネットのようなオープンネットワークでは可能である。 ファイアウォールで外部ネットワークと区画することは意味があるが、ファイアウォールで許可している通信の不正なパターンは、ＩＤＳ／ＩＰＳで遮断する必要がある。
	通常のファイアウォールとの違いは何か？「ＷＡＮ」と「ＬＡＮ」の関係は？	・社内と社外の区別という理解。社外から社内アドレスのなりすましを早期に発見することが必要。
	送信元ＩＰアドレス「欄」を有効に書き換えることは比較的容易か？	・容易である。
	バッファ・オーバーラン事象が発生してしまう体系とは？	・古い世代のものとしては、COBOL、Fortranなどの言語があげられる。

	Q.	A.
	「ハッシュ値」という考え方は、入力データの正確性を検証するために合計値を当てる場合などの数値もこれに相当するか？	・いわゆる、メッセージダイジェストとして理解すれば良い。
	スパイウェアは悪用されるだけか？	・原則、そのとおり。例外的に通信の状況を把握する市場調査的な使用目的もある。
	フィッシングとファーミングの相違点は？	・ファーミングは、フィッシングよりもより広範囲、より悪質であることが特徴。
	クロスサイトという言葉の意味は？	・攻撃を受ける閲覧者がサイトを跨るという意味。
	ソーシャルエンジニアリングとは？	・肩越しにパスワードを盗み見るような行為 ・初歩研修では「ゴミ箱」をあさるといったことが言われる。
ネットワーク・システム監査の要点	一般的なＩＴ監査では、第５章に記載されている脅威や脆弱性に対し、どの程度の備えがあれば良しとするのか？	・すべての脅威・脆弱性に対処するには、莫大な費用がかかり、経済的ではない。自社のＩＴ環境に重大な影響（対策費を超える損害の発生が見込まれる）を及ぼす恐れのある脅威・脆弱性に対して、優先的、集中的に対応するのが良い。したがって、チェックポイントのすべてを完璧に満たしている必要はなく、チェックポイントを当てた時に、重大なリスクが放置されていなければ良いのではないだろうか。
	ＩＴ監査人として第５章に記載されている事象の知識はどの程度必要とされているか？	・一般的なＩＴ監査人が理解すべき事象としてはかなり専門性が高いと思われる。
	ネットワーク管理者が定められ、そこに情報が集約され、適切な判断を下せる体制とはどのようなレベルをイメージすれば良いのか？	・よくある悪い例が、技術的な専門領域に当たるため、ネットワーク担当者に特権を与えて、作業を任せ切りにしていることである。 軽微な変更等もあり、すべてをネットワーク管理者が承認していては機動性に欠け、必要な対応に遅れが生じることも考えられるため、作業はネットワーク担当者が実施するが、ネットワーク管理者がすべての情報を把握できる必要がある。ネットワーク担当者には、ネットワーク管理者に作業内容を的確に説明する責任がある。 具体的な監査手続としては、体制図を確認し、その中でネットワーク管理者の役割と責任が定められ、それが個人に割り当てられていること、ネットワークの運用に係わる報告事項がネットワーク管理者が出席した会議等で報告されていること、等を文書・記録などから外形的に確認することになると思われる。
	ネットワークに関する教育・研修についてベストプラクティスのようなものはないか？	・実際にネットワーク設定等の操作を実習するのがベストと考える。 小規模なものでは、自宅のＰＣをインターネットに接続することである。社内のネットワークの運用に携われば、日々の障害対応を通して障害切り分け等の手順を学ぶことができる。 ただ、監査人としては、自らすべて調査する責任を負うのではなく、ネットワーク管理者に詳細を説明してもらい、対策の妥当性というよりは、そもそも想定されるリスクに対して対策が講じられているか（例えば、ネットワーク診断等を受けているかなど）を評価すれば、最低限の役目を果たしていると考える。したがって、ネット

	Q.	A.
		ワーク管理者がリスクは存在しない旨、明確に表明しているのであれば、明らかな反論がない限り、それを信用するしかないと思う。
	十分な強度を有する暗号化技術にはどのようなものがあるのか？	・日本では、「電子政府推奨暗号リスト」が公開されている。 現在広く使われている暗号方式のＳＨＡ－１及びＲＳＡ1024については、安全性の低下（危殆化）が指摘されており、より安全な暗号方式へ移行させる必要がある。 米国政府標準暗号では、2010年までにＳＨＡ－１をより強力な暗号方式に切り替えるとしている。
	ネットワーク故障対応時の訓練の具体的な例は？	・「回線の切り換え」、「ネットワーク機器の切り換え」が主な訓練項目になると思う。自動切り換えになっているものも多いと思われるが、切り換え時間を含めて想定どおりに切り換わることを、実際に確認しておくことが重要である。
	監査部門でセキュリティを評価する際、どのくらいのスキルが必要か？（過去のＩＴ部門の経験並びに身につけるべき知識）	・情報セキュリティに関するベストプラクティスは、はっきりしているため（ＩＳＯ27002）、この知識を身につけておくべきである。具体的には、ＩＳＭＳ内部監査員、可能であればＩＳＭＳ審査員のトレーニングを受けているのが望ましいと考える。ただし、ＩＳＯ27002の管理策の趣旨を理解するためには、ベースとなるＩＴに関する知識が必要になる。（逆に言えば、具体的にリスクを想定できるレベルとして、趣旨が理解できれば十分なレベルと考える） ちなみに、情報セキュリティ人材については、ＩＳＥＰＡ（情報セキュリティ教育事業者連絡会）で議論の最中である。
おわりに		
個人情報保護法	「個人情報保護監査」における組織の「個人情報取扱事業者」としての対応の切り口である「技術的措置」及び「物理的措置」について、情報セキュリティ監査との棲み分けをどのようにするか？	・情報セキュリティ監査の手法を応用して、個人情報保護監査における「技術的措置」及び「物理的措置」の対応状況の監査を実施する。
継続的監査	継続的監査の実施状況についての事例等があるか？	・継続的監査はＩＴを駆使した監査手法の１つであるが、データの収集方法、収集したデータの分析、評価するためのパラメータの設定等、費用対効果を含め十分に浸透していないのが実態と思われる。
	被監査部門による継続的点検と監査部門による継続的監査との相関関係は？	・被監査部門の点検状況の濃淡により、監査部門の監査の濃淡を決定することになる。すなわち、被監査部門において十分な自己点検が行われていない業務については、監査を実施することにより内部統制の有効状況を検証するという、それぞれを補完する関係にある。

『ここから始めるＩＴ監査』執筆者　（順不同・敬称略）

氏　名	所　　属	担　当
村田　一	オリックス株式会社　監査部副部長	第１章、第２章
吉武　一	株式会社りそな銀行　内部監査部アドバイザー	第３章、おわりに
金田　雅子	株式会社三菱東京ＵＦＪ銀行　監査部上席調査役	第４章
茅野　耕治	ＮＴＴデータ・セキュリティ株式会社　コンサルティング部課長	第５章

＜ＣＩＡフォーラム研究会No.21－Ａ（システム監査の実施方法サブグループ）メンバー＞

（順不同・敬称略）

	氏　名	所　　属	担　当
座長	矢島　博之	キリンホールディングス株式会社　経営監査部主幹	第３章、まとめ
	上本　美紀	株式会社トーマツ環境品質研究所　コンサルティング本部シニアコンサルタント	
	榎本　竜矢	株式会社三井住友銀行　業務監査部グループ長	第５章
	大塚　哲夫	株式会社アーバネットコーポレーション　内部監査室室長	第５章
	香川　正数	三菱化学株式会社　監査室部長代理	第５章
	烏谷　弘一	株式会社電通国際情報サービス　監査室シニアプロジェクトディレクター	第１章
	北島　貴三夫	株式会社ＩＨＩ　監査室室長	第２章
	佐藤　亜紀	株式会社京三製作所　内部監査室主任	
	佐土原　勉	ソニーライフ・エイゴン・プランニング株式会社　内部監査部統括課長	おわりに
	瀬野　毅	富士通株式会社　経営監査部リスクマネージャー	
	生川　治	ウォルト・ディズニー・ジャパン株式会社　シニア・マネジャー	第３章
	新江　誠	富士重工業株式会社　監査部主査	第４章
	細川　宗治	三協・立山ホールディングス株式会社　経理部	第３章
	松田　幸一	アキレス株式会社　監査部参事補	第４章
	門田　広志	日本興亜損害保険株式会社　業務監査部	
	吉岡　三隆	さくらカード株式会社　監査部次長	第４章
	吉武　一	株式会社りそな銀行　内部監査部アドバイザー	