情報セキュリティ監査基準
実施基準ガイドライン

Ver2.0（案）

本ガイドラインは、「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、及び情報セキュリティ監査実施上の手順について示したものである。

Ⅰ．情報セキュリティ監査実施上の前提事項

１．情報セキュリティ監査における準拠規範

情報セキュリティ監査の実施に当たっては、監査対象が情報セキュリティ対策に係る一定の条件を満たしているか否か、あるいは情報セキュリティ対策の実施状況が適切であるか否かについて検証、評価する際の拠り所とすべき判断の尺度が必要となる。

情報セキュリティ監査の実施に当たって用いる判断の尺度は、基本的には、監査の目的又は監査契約によって決定される。情報セキュリティ監査人（以下「監査人」という。）は、監査の実施に先立って、監査上の判断の尺度とすべき基準等を監査依頼者又は被監査主体とあらかじめ合意しておく必要がある。

情報セキュリティ監査の実施に当たって監査上の判断の尺度を明確にしておくことは、監査人にとって、監査手続と監査意見表明の基礎を確立することになる。一方、被監査主体にとっては、採用すべき情報セキュリティ対策の枠組みを決定し、情報セキュリティ対策運用上の焦点が絞りやすくなる。

「情報セキュリティ管理基準」による監査

「情報セキュリティ監査基準」に従った監査においては、本監査基準と姉妹編をなす「情報セキュリティ管理基準」を監査上の判断の尺度として用いることを原則としている。ただし、情報セキュリティ監査の要請又は目的によって、「情報セキュリティ管理基準」以外の適切な管理基準等を、監査上の判断の尺度として用いることもできる（次項「その他の管理基準等による監査」参照）。

「情報セキュリティ管理基準」は、ISO/IEC 27014 に基づくガバナンス基準、JIS Q 27001 に基づくマネジメント基準及び JIS Q 27002 に基づく管理策基準により構成され、情報セキュリティに係るマネジメント体制の確立及び運用のための国際規格と整合のとれたものとなっている。ガバナンス基準は、組織体のガバナンスのうち情報セキュリティに関する目的とプロセスを構成する要素に対応した判断の尺度であり、全ての要素が適切に整備され運用されていない限り、ガバナンスが適切に行われているとは言えない。また、マネジメント基準は組織としてのマネジメントサイクルの構成要素に対応した判断の尺度であり、ガバナンスと同様にすべての要素が適切に運用され整備されていることが必須である。一方、管理策基準は、情報資産を保護するために、情報セキュリティ対策の水準を設定し運用する際の標準的な管理項目を規定し、最善実務慣行として示したものであるから、当該管理基準を基礎として、組織体において必要な項目を追加し、あるいは該当しない項目を

削除して活用することができる。

情報セキュリティ監査の目的を充分に達成するためには、「情報セキュリティ管理基準」の趣旨及び枠組みを尊重し、当該基準のすべての項目について監査の対象とすることが望ましい。ただし、情報セキュリティ監査の要請又は目的、ないしは被監査主体の特性又はリスクの程度等を考慮して、当該管理基準の一部の管理項目（例えば、外部委託契約に係る管理項目等）を監査の対象とすることができる。その場合には、情報セキュリティ監査の対象として選択された管理項目が、監査の対象として選択されなかった他の管理項目と有機的に結びついてはじめて有効に機能することもある点に留意しなければならない。

監査の実施に当たって、「情報セキュリティ管理基準」の管理策基準を用いる場合、監査人は、当該基準における「管理策」をその「目的」を踏まえて判断尺度の枠組みとして用いることになる。「情報セキュリティ管理基準」の管理策基準において「詳細管理策」として記述された事項は、管理策の目的を具体的に達成するための手段の例示を記述しており、被監査主体のリスク等を考慮して監査手続を具体的に実施する局面で適宜取捨選択すべき事項であることに留意する。また、管理策基準に規定された詳細管理策のみでは情報セキュリティ対策が不十分であると組織体が判断した場合は、管理策の目的を具体的に達成するための手段を詳細管理策として適宜追加することが必要となることに留意する。

その他の管理基準等による監査

情報セキュリティ監査において、「情報セキュリティ管理基準」以外の管理基準を用いる場合には、監査の目的等に照らして、管理基準としての体系性、標準性、適用可能性等について、監査人は慎重に検討しなければならない。

情報セキュリティ対策に係る管理項目を含む管理基準等で政府機関が公表している国内基準には、内閣サイバーセキュリティ戦略本部「政府機関等のサイバーセキュリティ対策のための統一基準群」、内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省「政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準」、経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」、「システム管理基準」等がある。

情報セキュリティ対策に係る管理項目を含むその他の管理基準等で国際的に認知度が高いものに、米国国立標準技術研究所（NIST）の「The NIST Cybersecurity Framework」、情報システムコントロール協会（ISACA）の「COBIT」、米国 Center for Internet Security の「CIS Controls」などがある。

情報セキュリティ監査における監査上の判断の尺度として、上記に限らず、各種公的機関、業界団体又は監査サービス会社等で作成した管理基準等、あるいは組織体が独自に定めた管理規定（情報セキュリティ基本方針を含む）、CPS（認証局運用規程）、SLA（サービス水準合意書）等を用いることを妨げるものではない。ただし、組織体が定めた情報セキュリティ基本方針、CPS、SLA 等については、当該規定類の適切性に係るアドバイザリ

一又はアシュアランスが情報セキュリティ監査の目的とされることもあり得る点に留意する。

２．情報セキュリティ監査の目的設定

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。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アシュアランス[1]を付与することを目的とする監査（アシュアランス型監査という）と、情報セキュリティ対策の改善に役立つアドバイザリー[2]を行うことを目的とする監査（アドバイザリー型監査という）がある。

なお、この２つの目的は排他的なものではないため、アシュアランスとアドバイザリーの２つを監査の目的とすることができる。

情報セキュリティ監査の目的は、基本的には監査依頼者又は被監査主体のニーズによって決定されるが、監査人は、監査の実施に先立って、アシュアランスを目的とするかあるいはアドバイザリーを目的とするかについて、監査依頼者又は被監査主体との間で決定しておく必要がある。

アシュアランス型監査

アシュアランス型監査は、本来的には監査対象たる組織体の情報セキュリティに関するガバナンス、マネジメント又は管理策が監査手続を実施した限りにおいて適切であるとして監査人がアシュアランスを付与するものである。しかしながら、特に外部監査の場合、組織体の実態に対してアシュアランスを付与するためには網羅的な検証が必要となるなど時間・リソース・費用の観点で現実的ではない。そこで現実的な実施方法として、監査対象の情報セキュリティに責任を有するトップマネジメントが、自らの情報セキュリティ対策が適切に整備され運用されているとの主張（具体的な対策に関する説明を含む）を言明として提示し、監査人は監査手続を実施した限りにおいての、言明の内容と事実との乖離の有無を表明する形態の監査が行われている（これを言明方式の監査という）。

アシュアランス型監査の結論として表明される意見は、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監査意見の表明であって、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アシュアランスであり、当該意見に一切の誤りがないという絶対的な保証ではないことに留意する。特に、被監査主体である組織体において、「インシデントが発生しないことを保証する」という誤解が生じることがないよう、監査の実施に先立って十分な理解を得るよう努めることが望ましい。

また、監査人と監査報告書利用者の間における、監査リスク受容の程度についての合意

---

[1] 評価に対して証拠等の客観的な検証を根拠として信頼性を付与することをいう。
[2] 証拠等の客観的な検証を根拠として評価をもとに助言を行うことをいう。

の形態により、アシュアランスの水準が異なる可能性があることにも留意する。

アドバイザリー型監査

アドバイザリー型監査とは、情報セキュリティのマネジメント又は管理策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検出事項と併せて監査意見として表明する形態の監査をいう。アドバイザリー型監査の結論として表明される助言意見は、情報セキュリティ対策に対して一定のアシュアランスを付与するものではなく、改善を要すると判断した事項を監査人の意見（アドバイザリー）として表明するものである。

３．リスクの特徴に基づく監査目標設定の考え方

情報セキュリティ監査を有効かつ効率的に行うためには、リスクの特徴に基づいた監査を実施する必要がある。この場合、アシュアランス型監査とアドバイザリー型監査とではアプローチの方法が異なる。以下にアドバイザリー型、次いでアシュアランス型の順で監査目標設定の考え方を示す。

アドバイザリー型監査における目標設定

アドバイザリー型監査では、リスクベース監査を行うことが望ましい。リスクベース監査は、被監査主体のリスクの特徴に基づき、重大と判断されるリスクに対応した管理策の有効性評価に監査資源を集中することで、限られた期間と資源でより的確な監査結果が得られる。

具体的には、被監査主体において適切なリスク評価が行われ、リスクと管理策が体系的に結びついている場合、多数の管理策のうち、重大と判断されるリスクへの対策としての効果が大きいと判断されるいくつかの管理策（以下「鍵となる管理策」という。）を特定することができる。この鍵となる管理策が有効でない場合には、組織体の情報セキュリティ対策に重大な瑕疵があり、他の管理策が例え有効であっても、リスクが極めて大きい。一方、鍵となる管理策が有効であれば、他の管理策に多少の問題があっても、その影響は軽微といえる。

組織が情報セキュリティ対策を網羅的に評価したい場合や、被監査主体のリスク評価及びその結果に基づく管理策の選定プロセスに十分な信頼度がない場合には、管理策基準に基づくチェックリストによる監査を実施する。組織がリスク管理目標を明確に設定している場合には、当該目標に基づくチェックリストを作成することが望ましい。

アシュアランス型監査における目標設定

アシュアランス型監査の場合でも、リスクベース監査の考え方を採用することはできる。ただし、被監査主体が実施したリスク評価及びそれに基づく管理策の選定のプロセスにつ

いて、外部の監査人が有効であるとの意見を述べるには、相当の監査資源を投入する必要が生じるため、現実的ではない。むしろ、鍵となる管理策を含む比較的リスクが大きいと被監査主体と合意できる範囲を監査対象として限定し、管理策の有効性について意見表明を行うことが望ましい。

アシュアランス型監査では、監査人が監査報告書利用者と監査リスク受容の程度を実施する監査手続としてあらかじめ合意をする。合意の形態として、利用者合意方式と社会的合意方式の次の二つの方式がある。目標設定は、いずれの形態を採用するかを関係者間で明確に合意した上で行うべきである。

利用者合意方式は、監査人が監査報告書利用者と明示的に、あるいは暗黙に監査手続について合意する方式である。合意した監査対象に対して、合意した監査手続に基づく監査を実施することで、監査報告書のリスクを監査人と報告書利用者が共有する。この場合には、報告書のリスクについて理解が必須であり、リスクを理解している者に監査報告書の配付・閲覧を制限する。

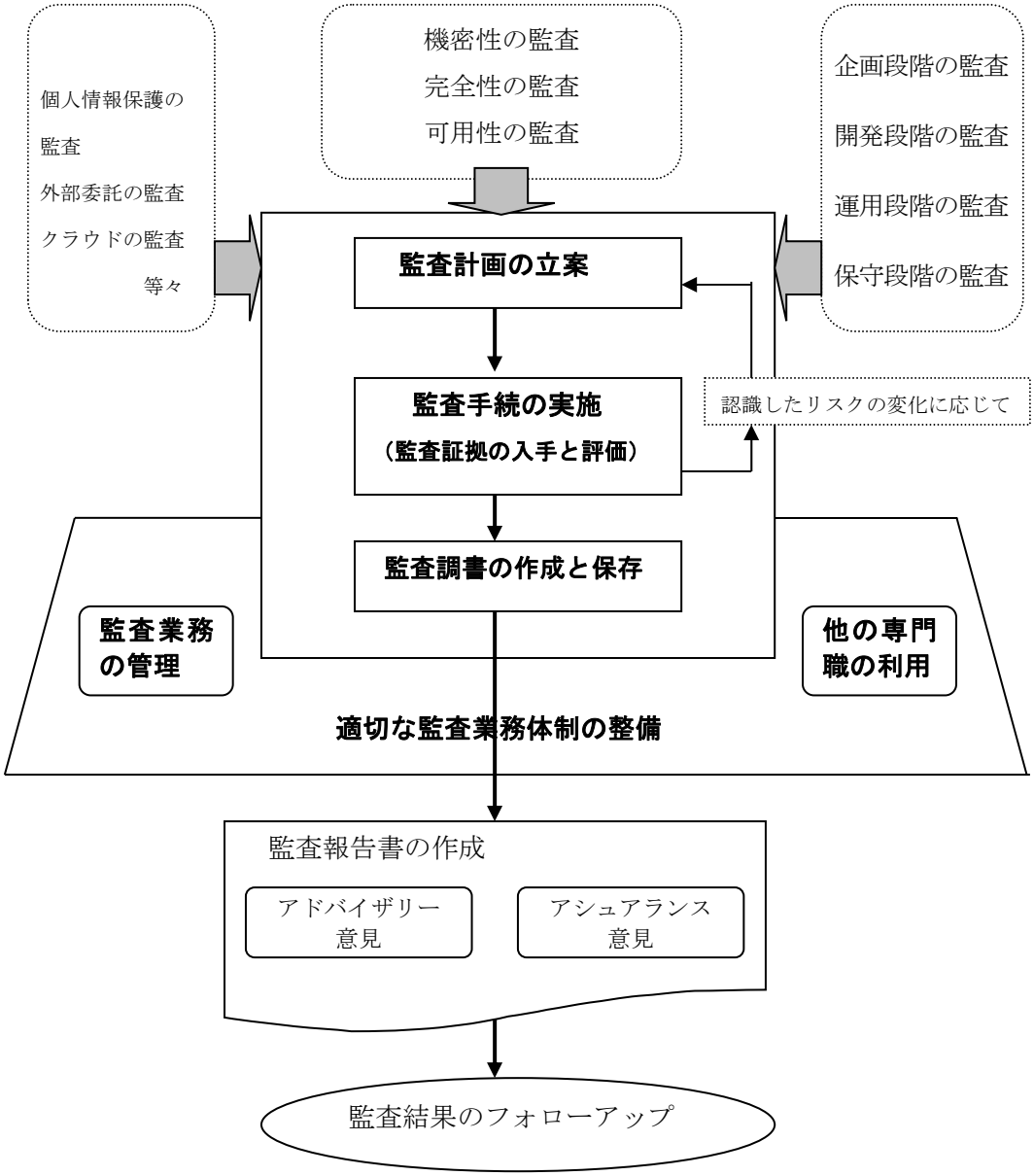
社会的合意方式は、社会的に合意された監査手続を行うものである。また、監査報告書は一般に公開される。監査人は実施する監査手続が社会的に合意されていることを確認し、監査目標を設定する必要がある。

なお、リスクベース監査の考え方で示した鍵となる管理策の考え方は、監査リスク（監査人が誤った意見を表明するリスク）の評価や重大性の判定の参考として用いることができる。

Ⅱ．情報セキュリティ監査の実施手順

１．監査実施のフレームワーク

情報セキュリティ監査実施上の全体像を図示すれば次のようになる。図中、太字は「情報セキュリティ監査基準」「実施基準」で規定している箇所である。情報セキュリティ監査は、その目的又は実施形態を問わず、監査計画の立案、監査手続の実施（監査証拠の入手と評価)、監査報告書の作成を経て実施される。



監査計画は、監査を有効かつ効率的に実施する観点から、監査の基本的な方針と、実施すべき監査手続を立案する。監査手続は、監査計画に基づいて、十分かつ適切な監査証拠を入手し評価するために実施される。かかる監査実施の過程は、監査報告書作成の基礎であるため、監査調書として記録しなければならない。

情報セキュリティ監査を有効かつ効率的に実施するために立案される監査計画、及びそれに基づいて行われる監査手続は、適切な監査業務体制の確立によって担保される。したがって、監査人は、監査業務の全体が適切に管理できるような体制を整え、必要に応じて他の専門職の利用を考慮しなければならない。

２．監査計画の立案

情報セキュリティ監査を有効かつ効率的に実施するために、情報セキュリティ監査の基本的な方針に基づいて、実施すべき監査手続を具体的に決定し、必要な監査体制を整えなければならない。

情報セキュリティに係るリスクは常に変動するため、監査計画は、適切なリスクアセスメントの結果を反映していることが望ましい。また、監査計画は、リスクの変動に応じて適時に修正されなければならない。

監査基本計画の立案

監査の基本的な方針として、次の事項を立案する。

- 監査方法の種類（アシュアランス型、アドバイザリー型）
- 監査対象とする範囲（例えば、外部委託）
- 監査対象とする期間又は期日（例えば、20XX 年 X 月 X 日から 20XX 年 X 月 X 日）
- 監査対象とする段階（例えば、運用段階）
- 監査対象に係る監査目標（例えば、機密性）
- 監査業務の管理体制
- 他の専門職の利用の必要性と範囲

監査の基本的な方針は、監査基本計画書として文書化する必要がある。内部監査として情報セキュリティ監査を実施する際には、監査基本計画書は、原則として年度計画として作成されるが、必要に応じて、長期計画、中期計画、及び年度計画に分けて策定する。

内部目的の監査としての情報セキュリティ監査は、長・中期的な監査計画のもとで継続的あるいは定期的に実施することが肝要である。情報セキュリティ監査の実施を外部に委託する場合であっても、長・中期的な基本計画に基づいて監査契約を締結すべきである。情報セキュリティに係る脅威は、それが原因となってさまざまな事業活動上のリスクとして派生することがあるため、情報セキュリティ監査の基本的な方針は、通常の業務監査との連携を視野に入れて立案することが望ましい。

監査実施計画の立案

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。

・監査手続の実施時期
・監査手続の実施場所
・監査手続の実施担当者及びその割当て
・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）
・監査手続の進捗管理手段又は体制

実施すべき監査手続の詳細な計画は、監査実施計画書として文書化する必要がある。実施すべき監査手続の重複又は脱漏を防ぐため、いつ、どこで、誰が、どのような監査手続を実施するかを体系的に立案し、あわせて監査手続の進捗管理を行うための手段又は体制を計画に織り込んでおくことが肝要である。

内部監査を実施する場合においては、監査依頼者（通常は内部監査部門の長）が情報セキュリティ監査計画を承認することが必要となる。

監査計画立案における監査対象のリスクアセスメント

監査人は、監査計画立案段階において、監査対象における情報セキュリティに係るリスクを監査人として把握する必要がある。このため、被監査主体の協力を得て、リスク情報の収集と評価を行うことが考えられる。

情報セキュリティに係るリスク情報の収集と評価に当たっては、関連する事業又は業務部門の関係者を一同に会した組織横断的なワークショップ形式による自由な討議又は自己評価が効果的で効率的な場合がある。この手法は、RSA（Risk Self Assessment）又は CSA（Control Self Assessment）と呼ばれることがある。これには、被監査側にリスク自己評価表を配布し記入を求め、その結果をもとに監査人が必要なヒアリング等を組み合わせる簡便法も含まれる。RSA を有効に活用すれば、監査人は、情報セキュリティに係るリスクを網羅的に把握でき、かつリスクの派生を見極めることができる。リスク自己評価表の記入を求める場合には、現状を正確に、客観的に記入できるように、質問項目の内容、記入環境に留意すること。なお、RSA には、情報セキュリティに係るリスク情報を組織体全体で共有することができ、また関係部署への教育的効果などの付随的効果も期待できる。

さらに、監査人は被監査主体によるリスクアセスメントの実施状況を確認することが望ましい。監査リスク（監査人が誤った意見を表明することにより被る恐れのある損害）は、被監査主体に係るリスクと監査人に係るリスクで合成される。会計監査のように長年の蓄積を得た監査においては、監査リスクの大きさを定量的に評価することが可能であり、このような評価に基づいて最適な監査手続を設計できる。一方情報セキュリティ監査におい

ては、情報セキュリティに関わるリスクの大小比較が可能な場合はあっても、その数量的な把握や比較が困難な場合が多いため、同様の設計は不可能である。そこで、監査リスクにつながる３種類のリスク、すなわち被監査主体に係るリスクである固有リスク（統制がない状態における情報セキュリティリスク）及び統制リスク（組織の統制が効かないことにより生じるリスク）、さらに監査人に係る発見リスク（統制の有効性を正しく発見できないことにより生じるリスク）を対象に、監査手続を通じてそれぞれのリスクを可能な範囲で的確に検出できるかを検討することが考えられる。これは、重要な監査対象の戦略的決定にとって有益であるばかりでなく、必要なリソースの配分を適切に調整することで、全体としてメリハリのある監査を期待でき、もって監査目的を有効かつ効率的に達成することにつながる。

被監査主体におけるリスクアセスメントの適切性の判定に当たって、監査人は、リスクアセスメント手法の厳密性を検証するのではなく、リスク・マッピング等の工夫によって、リスクアセスメントの結果が管理策と関連づけられたものであることを確かめておくことが重要である。

なお、アドバイザリー型監査においては、被監査主体におけるリスクアセスメントの適切性、及び監査人によるリスクアセスメントの結果とそれに応じたマネジメント又は管理策の整備及び運用に対する助言が重要な指摘事項となることがある。

３．監査手続の実施（監査証拠の入手と評価）

アシュアランス型監査であれアドバイザリー型監査であれ、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するための監査手続を実施しなければならない。監査証拠は、アシュアランス意見又はアドバイザリー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。

監査証拠は、関連書類の閲覧及び査閲、担当者へのヒアリング、現場への往査及び視察、システムテストへの立会、テストデータによる検証及び跡付け、脆弱性診断、ペネトレーションテストなどの方法を通じて入手される。しかし、監査人が入手した資料等がそのまま監査証拠となるわけではない。監査人は、当該資料等の入手源泉及び入手時の状況等を勘案して、監査証拠として採用するか否か、それが有する信用性及び証明力の程度を慎重に判断し、その結果等を明らかにしなければならない。近年では、監査人が現場で往査することなく、通信ネットワークを介して観察を行うリモート監査や、専用の機器を用いた自動収集なども利用されることから、これらにより得られた監査証拠の扱いについても考慮する必要がある。

監査人は、入手した監査証拠の必要性と十分性の判断に当たって、被監査主体から提出された資料、監査人自ら入手した資料、監査人自ら行ったテスト結果等を総合的に勘案して、相互に矛盾があるか否か、異常性を示す兆候があるか否かを評価しなければならない。

監査人が入手した監査証拠の評価に当たっては、リスクアセスメントの結果との関連づけが考慮されることが望ましい。被監査主体が現に採用している管理策が適切であるか否かの判断は、リスクに応じたものでなければならない。リスクが相対的に高い場合にはより強力な管理策が必要とされ、逆にリスクが低い場合にはそれに対応した管理策となる。管理策が適切でないと判断した場合には、監査の目的や設定した目標の達成に対する影響の重要性や広範性を判断する。アシュアランス型監査において総合的な意見が求められる場合は、表明する意見の類別について、慎重に判断を行う。

４．監査調書の作成と保存

監査人が実施した監査手続の結果と、監査手続に関連して入手した資料等は、監査の結論に至った経過がわかるように監査調書として作成し、情報漏えいや紛失等を考慮し、適切に保管しなければならない。

監査調書とは、監査人が行った監査業務の実施記録であって、監査意見表明の根拠となるべき監査証拠、その他関連資料等を綴り込んだものをいう。監査人自身が直接に入手した資料やテスト結果だけでなく、被監査主体から提出された資料等を含み、場合によっては組織体外部の第三者から入手した資料等を含むことがある。

監査調書は、主として監査意見の根拠とするために作成されるが、それ以外にも次回以降の情報セキュリティ監査を合理的に実施するための資料として役立ち、また監査の品質管理の手段としても役立つ。さらには、監査人が正当な注意義務を果たして監査業務を遂行したことの証左となることがある。

監査調書はさまざまな目的に役立つことから、監査調書の作成に当たっては、正確かつ漏れなく必要な事項を綴り込まなければならず、適当な参照符号等を整備して監査人が監査の結論に至った経過が秩序整然と分かるように工夫しなければならない。

監査調書は監査人の所有に属することから、情報セキュリティ監査終了後も相当の期間、監査人の責任のもとで整理保存しておく必要がある。監査調書には被監査主体の機密事項が含まれていることから、保管場所や保管責任者の特定等、監査調書の保管には慎重な注意が求められる。

５．適切な監査業務の体制整備

監査人は、監査計画の立案、監査手続の実施、監査証拠の入手と評価、監査報告書の作成、監査報告に基づくフォローアップからなる一連の監査業務の遂行において、監査業務を効率的に実施し、かつ重要な問題点の見落とし等監査業務上の瑕疵が生じないよう、監査業務の全体を管理しなければならない。

監査業務は、少ないコストで、最大限の効果が期待できるよう実施されるべきであるが、そのためには監査業務の品質確保が最も重要な要件となる。監査業務の品質管理は、適切な監査計画の立案、監査マニュアルの整備、及び監査調書のレビュー等を通じてなされる。

よって実施体制の検討に際しては監査担当者間の適切な職務の分担に配慮し、相互チェックが機能するような体制を整えるとともに、監査チームから独立した品質管理者が品質管理を行えるようにする。

監査計画の立案段階において想定しなかった状況変化（リスクの変化を含む)、すなわち経営方針の変更、事業プロセスの変更、情報システムの新規開発、突発事象の発生等にも柔軟に対応できるように、必要な措置等を講じておく。

十分かつ適切な監査証拠を入手するために、監査人が必要と認めた場合には、情報処理安全確保支援士、システム監査技術者、ネットワークスペシャリスト、システムアナリスト、ビジネスコンサルタント、技術士、弁護士、公認会計士等の専門職の支援を仰ぐことを考慮すべきである。なお、当該専門職からのアドバイスや監査手続の補助又は代行があっても、監査の結果についての責任は監査人にあることに留意しなければならない。

監査リスクによっては、専門的能力と実務経験を有する審査担当を設定し、監査計画、監査手続、監査報告に対して情報セキュリティ監査に対して客観的な立場から重要な判断及び結論についての評価を実施する。

６．アシュアランス型監査を行う場合の品質管理システム

アシュアランス型監査を行う監査人は、法人個人を問わず一定の監査品質を維持するための品質管理体制を含む品質管理システムを設ける必要がある。品質管理システムの中には次のような事項が含まれる。

- 独立性の維持方法
- 専門能力の維持するための研修
- 契約締結方法
- 審査担当の要否を含む個別業務の品質維持方法
- 品質管理システムの有効性のモニタリング方法