情報セキュリティ監査基準
実施基準ガイドライン

Ver1.0

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

1.1　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。

1.2　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側とあらかじめ合意しておく必要がある。

1.3　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、情報セキュリティ監査人にとって、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、被監査側にとっては、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

1.4　「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する。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。

1.5　「情報セキュリティ管理基準」は、JIS X 5080（ISO/IEC 17799）をもとにしており、情報セキュリティに係るマネジメント体制確立のための国際規格と整合性のとれたものとなっている。「情報セキュリティ管理基準」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。

1.6　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、ないしは被監査側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。

1.7　監査の実施に当たって、「情報セキュリティ管理基準」を判断の尺度として用いる場合、情報セキュリティ監査人は、当該基準において管理項目ごとにその管理目的を記述した「目的」、及び管理目的を達成するための統制目標を記述した「コントロール」を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」において「サブコントロール」として記述された事項は、統制目標を具体的に達成するための統制手段の例示を記述しており、被監査側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、管理目的、統制目標自体が不足している、統制目標を達成するために必要な統制手段が不足していると組織体が判断した場合は、管理目的、統制目標、統制手段を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

1.8　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、情報セキュリティ監査人は慎重に検討しなければならない。

1.9 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、経済産業省「システム監査基準」、「情報システム安全対策基準」、「コンピュータウイルス対策基準」、「コンピュータ不正アクセス対策基準」、総務省「情報通信ネットワーク安全・信頼性基準」、警察庁「情報システム安全対策指針」等がある。

1.10　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、内部監査協会（IIA）の「eSAC」、情報システムコントロール協会（ISACA）の「COBIT」、アメリカ公認会計士協会（AICPA）/カナダ勅許会計士協会（CICA）の「Trust 業務原則及び規準」などがある。

1.11 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 1.9 及び 1.10 に限らず、各種公的機関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保証又は助言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

2.1　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。なお、この２つの目的は排他的なものではないため、保証と助言の２つを監査の目的とすることができる。

2.2　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側のニーズによって決定されるが、情報セキュリティ監査人は、監査の実施に先立って、保証を目的とするかあるいは助言を目的とするかについて、監査要請者又は被監査側と調整を重ねておく必要がある。

保証型の監査の意義

2.3　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。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。

助言型の監査の意義

2.4　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。助言型の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保証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情報セキュリティ監査人の意見として表明するものである。

助言型の監査と保証型の監査の選択

2.5　**前提条件の検討**　　組織体が設定し運用すべき情報セキュリティ対策の内容は、事業体の規模、事業戦略、事業の性質、システムの運用環境、法令による規制等によって必ずしも一様ではない。また、情報セキュリティ対策を設定し運用する場合には、その費用対効果、及び通常業務への負荷等を考慮せざるをえない。かかる前提を十分に踏まえた上で、実際に採用されている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。

2.6　**段階的導入の検討**　　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。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。

2.7　**利害関係者の信頼獲得についての検討**　　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。

３．情報セキュリティ監査における成熟度モデルの利用

3.1　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。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。

合理的な範囲での保証又は助言

3.2　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。また、情報セキュリティ対策に係る重大な欠陥等についての助言を行う場合であっても、現に採用されている情報セキュリティ対策に基礎を置いた合理的な範囲での改善提言でなければ意味がない。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。

成熟度レベルに応じた保証又は助言

3.3　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。

3.4　成熟度モデルを利用する場合には、情報セキュリティ監査人は、情報セキュリティ監査の実施に先立って、どのような成熟度モデルを利用するのか、成熟度のレベル分けの判断基準はどのようなものであるのかについて監査依頼者又は被監査側と充分に協議した上で決定することが望ましい。

成熟度モデルの応用局面

3.5　成熟度モデルの利用は監査意見の表明と関連づけたものであるが、主要な管理項目と関連づけて適用することができる。主要な管理項目ごとに、情報セキュリティ対策がどの水準にあるかを成熟度モデルによって判定し、その結果をレーダーチャートなどによって図解することができれば、組織体において採用されている情報セキュリティ対策の全体バランス又は情報セキュリティ対策上の弱点を鮮明にすることができる。リスクに応じた情報セキュリティ監査、又は情報セキュリティ監査の段階的導入を志向する場合には、有効な手法となる。

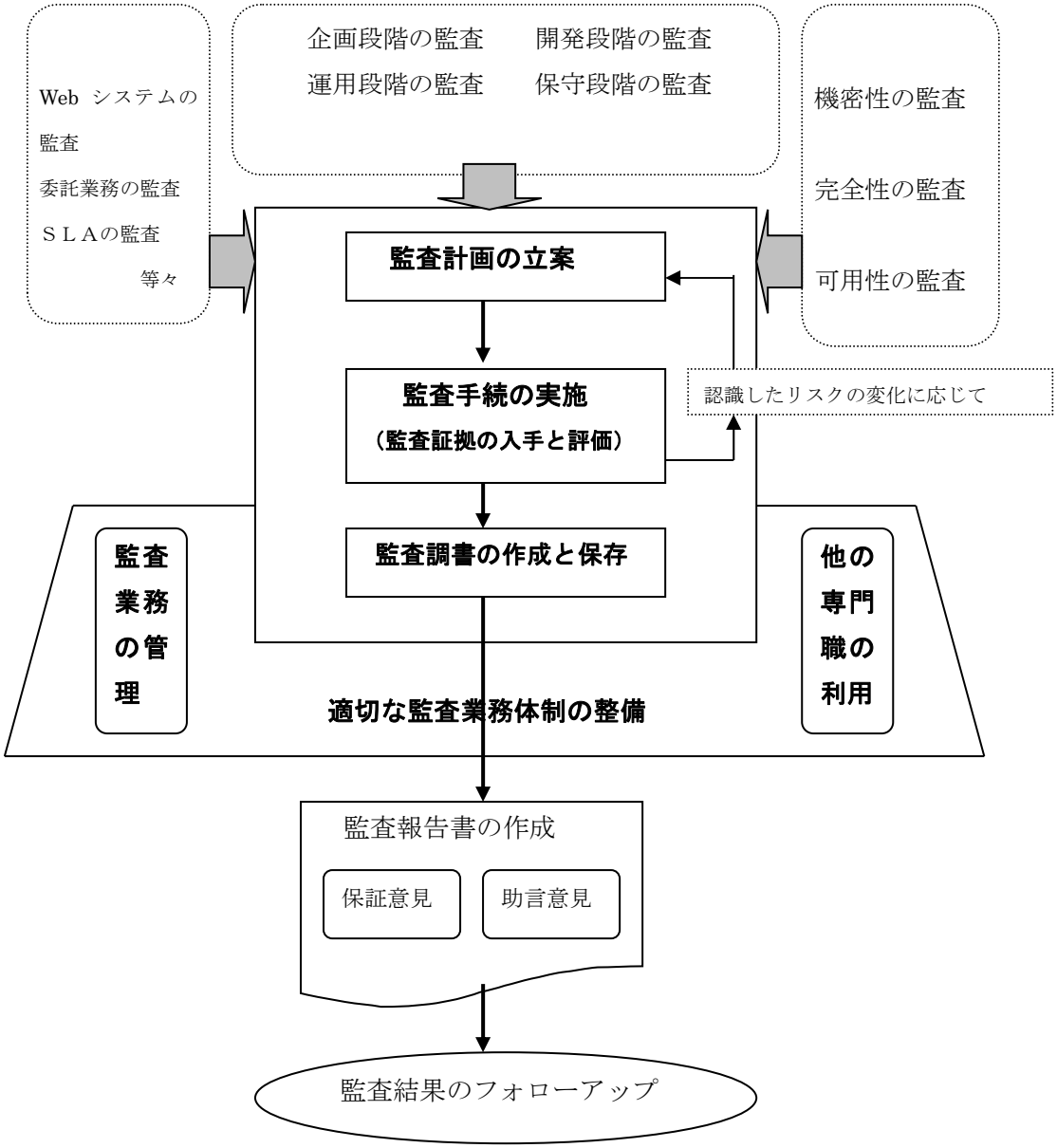
3.6　成熟度モデルは、被監査側が作成した自己評価表において反映させることができる。

例えば、管理項目ごとに、該当しない（0）、整備していない（1）、整備している（2）、運用している（3）、継続的に改善されている（4）に分けて被監査側に記入してもらうことによって、情報セキュリティ監査人は情報セキュリティ対策上の弱点を容易に把握することができ、又被監査側において情報セキュリティ対策に対する認識を高めてもらうことができる。なお、情報セキュリティ監査人は、当該被監査側が作成した自己評価表への回答及びその適正性を被監査部門の長又は必要に応じて組織体の長が認めた旨を記載した文書（適正言明書という）を入手し、当該適正言明書を監査意見表明の対象とすることができる。

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

1.1　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。



1.2　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とするため、監査調書として記録しなければならない。

1.3　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、情報セキュリティ監査人は、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

2.1　情報セキュリティ監査人は、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、監査の基本的な方針を立案し、それに基づいて、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。

2.2　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

2.3　情報セキュリティ監査人は、監査の基本的な方針として、次の事項を立案する。

・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、200X 年 X 月 X 日から 200X 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

2.4　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。

2.5　内部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。

2.6　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

2.7　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。

・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

2.8　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。

2.9　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

2.10　情報セキュリティ監査人は、監査計画の立案に役立たせるため、リスクアセスメントを実施することが望ましい。監査計画立案段階におけるリスクアセスメントは、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、リスクアセスメントの結果を実施すべき監査手続に反映させることによって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。

2.11 被監査側においてリスクアセスメントが行われている場合、情報セキュリティ監査人は、リスクアセスメントの適切性を確かめた上で、被監査側によって実施されたリスクアセスメントの結果を監査計画の立案に活用することができる。被監査側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、情報セキュリティ監査人は、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コントロール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。

2.12 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、その結果をもとに情報セキュリティ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、情報セキュリティ監査人は、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。

2.13 被監査側で情報セキュリティに係るリスクアセスメントが行われていない場合又はリスクアセスメントが不適切である場合には、必要に応じて情報セキュリティ監査人がリスクアセスメントを行う必要がある。助言型の監査において、被監査側によるリスクアセスメントが行われていない場合又はリスクアセスメントが不適切な場合には、当該事実、及び情報セキュリティ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コントロール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）

3.1　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。

3.2　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、脆弱性スキャン、システム侵入テストなどの方法を通じて入手される。しかし、情報セキュリティ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。情報セキュリティ監査人は、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。

3.3　情報セキュリティ監査人は、入手した監査証拠の必要性と十分性の判断に当たって、被監査側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。

3.4　情報セキュリティ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。被監査側が現に採用しているコントロール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コントロールが必要とされ、逆にリスクが低い場合にはそれに対応したコントロールとなる。

４．監査調書の作成と保存

4.1　情報セキュリティ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。

4.2　監査調書とは、情報セキュリティ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。情報セキュリティ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、被監査側から提

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。

4.3　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、情報セキュリティ監査人が正当な注意を払って監査業務を遂行したことの証左となることがある。

4.4　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情報セキュリティ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。

4.5　監査調書は、情報セキュリティ監査終了後も相当の期間、整理保存しておく必要がある。監査調書には被監査側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。外部の情報セキュリティ監査人に保証型監査を依頼した場合においては、監査調書は、監査人の所有に属することに留意すること。

５．適切な監査業務の体制整備

5.1　情報セキュリティ監査人は、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。

5.2　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。

5.3　情報セキュリティ監査が監査チームによって実施される場合には、適切な職務の分担に配慮し、監査担当者間における相互チェックが機能するような体制を整えることが望ましい。

5.4　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ことが望ましい。

5.5　十分かつ適切な監査証拠を入手するために、情報セキュリティ監査人が必要と認めた場合には、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情報セキュリティ監査人にあることに留意しなければならない。