

情報セキュリティ監査手続ガイドラインを利用した
監査手続策定の手引

平成 21 年 7 月

経済産業省

はじめに

本文書は、情報セキュリティ監査人(以下、監査人)が「情報セキュリティ監査手続ガイドライン」を用いて監査手続を策定する際の手順について記したガイダンス文書である。

1 情報セキュリティ監査手続ガイドラインを利用した監査手続の策定手順

1.1 事前準備

組織が情報セキュリティ監査を行うには、中長期の監査計画に基づく定期的な監査やサービスの利用者への説明など、個別の目的がある。この目的によって保証型¹や助言型²などの監査のタイプ、管理基準の範囲などが変わる。このため監査手続を策定するためには、監査依頼者に監査の目的を確認し、明確にしておく必要がある。

監査手続を策定するためには、事前に個別情報セキュリティ管理基準³(以下、個別管理基準)を入手する必要がある。個別管理基準は、必ずしもその名の通りの文書でなくてもよく、組織によっては組織の情報セキュリティ関連の規程・ガイドラインの場合もある。

また必要に応じて、次の文書の入手も行う。

- 中長期の監査計画
- 組織図、拠点所在
- 情報システム一覧
- 情報資産一覧
- リスク分析結果
- 組織が重視する外部基準

さらに、次の事項について確認しておかなければならない。

- 監査実施時の制限事項(日時、場所、コスト)
- 監査手続が再実施を含む場合、再実施の実行を許可する責任者

1.2 該当する管理基準の選択

情報セキュリティ監査手続ガイドラインは、情報セキュリティ管理基準のマネジメント基準、管理策基準の管理策(マネジメント基準及び詳細管理策)について監査手続を示しているが、実際の組織で採用されている管理策は、必ずしも情報セキュリティ管理基準と同じではない。このため、内容が似ている管理基準を探し、その監査手続を参考として組織の管理策に適合した監査手続を策定

¹ 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、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。

² 対象事象についての客観的な規準が存在することを前提として、入手した十分かつ適切な証拠に基づきその基準への準拠性について対象事象を評価又は測定し、対象事象と規準とのギャップを検出し、独立の第三者として検出事項及び参考意見として改善提言を行うこと。

³ 組織が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロールを整備し、運用するための基準。また、監査主体が情報セキュリティ監査を行なう上での実際の監査項目。

する必要がある。

1.3 監査手続の選択

次に監査手続を選択する。監査手続で採用される監査技法は下表に示した4種類である。

表1 監査技法

監査技法	定義と説明	補足
質問 (ヒアリング)	<p>マネジメント体制又はコントロールについての整備状況又は運用状況を評価するために、関係者に対して口頭で問い合わせ、説明や回答を求める監査技法</p>	<ul style="list-style-type: none"> 文書による問い合わせを含む 必要に応じて被監査主体の外部委託先への問い合わせも含む 質問結果の食い違いに注意 <ul style="list-style-type: none"> 複数の担当者又は管理者に対するヒアリングで信憑性を高める 他の監査技法と組み合わせて食い違いの原因を明確にする
閲覧 (レビュー)	<p>マネジメント体制又はコントロールについての整備状況又は運用状況を評価するために、規程、手順書、記録(電磁的な記録も含む)等を調べ読む監査技法</p>	<ul style="list-style-type: none"> 職務分掌規程、職務権限規程、情報セキュリティポリシー、情報セキュリティ関連規程、運用手順書、各種申請書類(IDの付与、アクセス権の付与など)、システム上の設定値、システムログなど <ul style="list-style-type: none"> 客観性は高いが、改ざんに注意 複数の文書類の突き合せや、質問との併用が必要。
観察 (視察)	<p>マネジメント体制又はコントロールについての整備状況又は運用状況を評価するために、監査人自らが現場に赴き、目視によって確かめる監査技法</p>	<ul style="list-style-type: none"> 運用担当者が運用手順書に従った操作を実際に行っていることを、監査人自ら直接に把握し、その妥当性や適否を判断する 監査人が目視によって確かめるため、証拠力は強い 厳密には観察した時点のみについての証拠能力しかもたないことに注意 <ul style="list-style-type: none"> 都合の悪い部分は見せていないかもしれない 運用の全てを観察することは困難
再実施	<p>コントロールの運用状況を評価するために、監査人自らが組織体のコントロールを運用し、コントロールの妥当性や適否を確かめる監査技法</p>	<ul style="list-style-type: none"> 例えば、カードによる入室管理が行われている場合、アクセス権が付与されていないカードを利用し、監査人自らがエラーとなることを確かめること等が再実施にあたる 監査人が自ら運用してみるため、証拠力は強い 厳密には再実施を行った時点のみについての証拠能力しかもたないことに注意 <ul style="list-style-type: none"> たまたまそこだけ問題なかったのかもしれない 全てのコントロールを運用してみることは困難

情報セキュリティ監査手続ガイドラインでは、管理策ごとに適切と考えられる監査手続を1つあるいは複数掲げている。複数の監査手続がある場合には、そのすべてを採択するか1つを選択するかは、監査目的の達成のために有効な監査証拠が収集できると考えるかどうかによる。

監査を行うにあたり、組織の情報セキュリティ管理をどういった視点で監査するのかによって、採用する監査技法は自ずと異なってくる。ここで視点とは、情報セキュリティマネジメントの設計、実装、運用のいずれを見るかである。

設計の監査：組織が定めた情報セキュリティ管理の施策が、組織の抱えるリスクに対応したものとなっているかを見る視点であり、情報セキュリティ監査手続ガイドラインの対象とはしていない。

実装の監査：情報セキュリティの対策が、組織の定める通りに実装されているかを監査する視点で、この場合、組織的・人的な対策の実装については、監査の対象は管理手続、手順、文書様式となり、監査技法は閲覧(レビュー)が主となる。また、技術的・物理的な対策については、監査の対象は情報システムの設計書や

設定となり、監査技法は閲覧(レビュー)、観察(視察)が主となる。いずれの場合も対象によっては質問(ヒアリング)や再実施も採用される。

運用の監査：情報セキュリティ対策が、組織の定める通りに運用されているかを監査する視点で、この場合、監査の対象は台帳などの記録やシステムのログとなり、監査技法は閲覧(レビュー)、観察(視察)、質問(ヒアリング)、再実施が適宜選択される。

監査の目的によっては、情報セキュリティ監査手続ガイドラインに掲げる監査手続のいずれも適当ではない、あるいは個別管理基準が情報セキュリティ管理基準(平成20年改正版)と異なるため対応する管理基準自体が情報セキュリティ監査手続ガイドラインに存在しない場合も想定される。このような場合には、独自に監査手続を策定する必要がある。

情報セキュリティ監査手続ガイドラインでは、監査対象や組織について一般的な名称で記しているため、個別の組織の状況に応じて監査対象の文書、記録類、システムについて、実際の組織で用いられている名称に改める必要がある。この作業のためには、1.1 で入手した文書が有用である。

1.4 証拠の量の決定

監査人が収集する監査証拠は、被監査主体が個別管理基準通りに実装、運用していることについて、監査人が十分な心証を得るに足るものでなければならない。このためには監査証拠の質と量に注意が必要である。監査証拠の質については、1.3 で示した監査手続(監査技法)の選択及び監査対象の範囲の選択に依存する。一方、監査証拠の量については情報セキュリティ監査手続ガイドラインでは述べていない。収集すべき監査証拠の量は、監査の目的、個別管理基準の具体的な実装や運用方法、監査対象の状況によって自ずと異なってくる。一人の管理者に質問するだけで十分である場合もあれば、複数の管理者への質問が必要な場合もある。また1拠点だけの視察で十分と判断できる場合もあれば、全拠点についての視察が必要となる場合もある。

コスト(監査人、被監査主体双方の労力)を考慮しつつ、十分な量の監査証拠を収集すべきである。

1.5 監査手続の順序の決定

監査手続を実施するためには、特に突合による網羅性を検証するような場合に事前の調査が必要なものもある。また、質問(ヒアリング)対象者にはまとめて質問する、同一の場所への視察の項目はまとめて行うなど、被監査組織の人員の労力も念頭に入れた効率のよい監査手続を計画しなければならない。

有効な監査証拠を効率よく収集する監査手続のために、事前調査も含めどのような順序で情報や証拠の入手を行うかも検討する必要がある。例えば、新入社員への情報セキュリティ教育の実施状況を監査する場合、事前に監査対象期間に入社した社員のリストを入手しておく必要がある。また退職者の情報システム利用権限の抹消状況を監査する場合には、事前に監査対象期間の退職

者リストを入手しておく必要がある。これらのリストは通常、人事部門が保有しており、それぞれの監査項目ごとに都度人事部門からリストを取り寄せるのではなくまとめて依頼すべきである。

2 監査手続策定における留意事項

2.1 厳密性が求められる場合の監査手続

保証型監査で運用が言明どおりに行われていることを求められる場合など、厳密性が求められる場合は、対象となる詳細管理策について①当該管理策が対象とする資産や主体が明確に定義されていること、②管理策を実施するための手順が明確であること、③管理策が実装され、更に運用されていることを示す記録があること、④その記録が検証され、更に適切に保管されていること、の4つの要件を満たす必要がある。監査手続はこの要件ごとに策定する。情報セキュリティ監査手続ガイドラインにおいて記述している監査手続は、主にこのうち③及び④に関わるものである。①や②の記述がない項目の場合、その詳細管理策の前提となる定義や手順(上記①及び②)について、マネジメント基準あるいは他の詳細管理策に対応する項目を参照して、監査手続を策定する。

2.2 適切な監査技法の選択

監査においては、対象範囲のすべてについて同じ深さの監査手続を用いる必要はない。誤った監査意見を述べる可能性の高い対象(監査リスクの高い対象)に重点を置いて監査技法を選択することが望ましい。すなわち、監査リスクの高い対象に対しては閲覧(レビュー)や質問(ヒアリング)に加えて、工数がかかる観察(視察)や再実施などを組み合わせ、監査リスクが低い対象には比較的工数がかからない閲覧(レビュー)や質問(ヒアリング)を多用するようにするとよい。監査目的に合わせて、現実的なコスト(時間、費用)で実施可能な監査とすべきである。

情報システムの設定を確認する場合には、閲覧(レビュー)と観察(視察)のいずれかの監査技法が用いられることが多い。すなわち、被監査主体にその設定ファイルを紙媒体に印刷文書を準備してもらい確認する場合(閲覧(レビュー))と、現場に赴いて情報システムの画面に表示依頼を行い、表示されたものを確認する場合(観察(視察))である。

監査証拠が改ざん又はねつ造される可能性は、一般的に閲覧(レビュー)の方が高いと考えられるが、多くの情報システムの設定を観察(視察)によって確認するためにすべての現場に出向くのはコストがかかり、結果として他の監査手続で十分な証拠を収集することができないこともあり得る。このため、証拠が改ざん又はねつ造されるリスクが許容できると判断する場合には、閲覧(レビュー)による監査手続を選択することもあり得る。この場合には、情報セキュリティ監査手続ガイドラインで「観察(視察)」による監査手続としてあっても、「閲覧(レビュー)」と読み替えて、監査手続を策定する。

なお、予備調査及びリスクアセスメントの結果は、監査リスクの観点から適切な監査技法を選択するために有用である。