情報セキュリティ監査基準

Ver2.0（案）

前文

情報セキュリティを脅かすリスクが多様化し複雑化している現状に鑑みるとき、情報セキュリティ監査は、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ていることを担保するための有効な手段となる。情報セキュリティ監査は、独立かつ専門的な立場から、組織体の情報セキュリティの状況を検証又は評価して、情報セキュリティの適切性を保証し、又は情報セキュリティの改善に役立つ的確な助言を与えるものだからである。

情報セキュリティ対策は、本来的には、企業、団体、自治体等の組織体の責任において遂行されるべきものであるが、情報セキュリティをマネジメントプロセスに組み込んで構築し運用するためには、管理サイクルの見直しにとって情報セキュリティ監査は不可欠な要素となる。さらに、外部利害関係者との影響関係を視野に入れた IT ガバナンスという観点からも、情報セキュリティ監査のモニタリング機能としての重要性は益々高まってきている。

情報セキュリティ監査基準とは、情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした情報セキュリティ監査人（以下「監査人」という。）の行為規範である。本監査基準は、監査人としての適格性及び監査業務上の遵守事項を規定する「一般基準」、監査計画の立案及び監査手続の適用方法を中心に監査実施上の枠組みを規定する「実施基準」、監査報告に係る留意事項と監査報告書の記載方式を規定する「報告基準」からなっている。

情報セキュリティ監査基準は、組織体の外部者に監査を依頼する情報セキュリティ監査だけでなく、組織体の内部監査部門等が実施する情報セキュリティ監査においても利用できる。さらに、本監査基準は、情報セキュリティにアシュアランスを付与することを目的とした監査であっても、情報セキュリティに対してアドバイザリーを行うことを目的とした監査であっても利用できる。

情報セキュリティ監査の実施に当たっては、組織体における情報セキュリティの適否を判断するための尺度が必要である。情報セキュリティ監査は、本監査基準の姉妹編である情報セキュリティ管理基準及び同基準をもとに策定される個別管理基準を監査上の判断の尺度として用い、監査対象が情報セキュリティ管理基準に準拠しているかどうかという視点で行われることを原則とする。情報セキュリティ管理基準は、国際規格をもとに作成されており、組織体が情報セキュリティを構築し運用するための標準的な対策を提供している。

本監査基準にて用いる「情報セキュリティ」の対象には、組織体が保有する情報のみでなく、サイバーセキュリティの文脈で扱われるサイバー空間としての IT インフラストラク

チャー及び漏えいした場合にプライバシーの侵害となるようなプライバシーに関する情報も含む。一方で、情報セキュリティ管理基準は組織体が保護すべき情報に関するリスクへの管理策を中心に構成されていることから、組織体において情報セキュリティ監査を実施する際には、対処すべきリスクの対象や特徴に応じて適切な基準等を利用ないし併用することも検討すべきである。

情報セキュリティ監査基準 Ver1.0 は平成 15 年に公表されて以来、情報セキュリティ監査制度の普及とともに幅広い分野で活用されている。その一方で監査の目的として示されている「保証の付与」について、「セキュリティインシデントが発生しないことを保証する」という文脈における保証（英語の guarantee に相当）として誤解される事例があることが指摘されるようになった。そこで Ver2.0 への改訂にあたり、これまで「保証」及び「助言」と記載していた箇所について、それぞれ「アシュアランス」及び「アドバイザリー」と表記を改めることとした。表記の変更に伴う意味の変更は生じていないが、用語に馴染みのない読者のため、次項に示す「情報セキュリティ監査の目的」においてそれぞれの定義を示している。

情報セキュリティ監査の目的

情報セキュリティ監査の目的は、組織体としての情報セキュリティに関する取組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管理策の整備、運用状況を、情報セキュリティ管理基準等の判断基準に基づき、監査人が独立かつ専門的な立場から検証又は評価して、もってアシュアランスを与えあるいはアドバイザリーを行うことにある。このとき、アシュアランスとは証拠等の客観的な検証を根拠とした事実認定に基づき信頼性についての意見表明をすることをいい、アドバイザリーとは同様の検証を根拠とした基準不適合の事項に対する改善のための助言を行うことをいう。

情報セキュリティのマネジメントは第一義的には組織体の責任において行われるべきものである。情報セキュリティ監査は、情報セキュリティのマネジメントを行う組織体に対して、管理策が有効に機能していることへのアシュアランス又はアドバイザリーを行うものである。

一般基準

１．目的、権限と責任

情報セキュリティ監査を実施する目的及び対象範囲、並びに監査人の権限と責任は、文書化された規程又は契約書等により明確に定められていなければならない。

なお、情報セキュリティ監査は、情報セキュリティに対する管理策の有効性を対象として行われるものであるが、具体的に設定される監査の目的と監査の対象は監査依頼者の要請に応じたものでなければならない。

２．独立性、客観性と職業倫理

2.1　外観上の独立性

監査人は、情報セキュリティ監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上・経済上、密接な利害関係を有することがあってはならない。

2.2　精神上の独立性

監査人は、情報セキュリティ監査の実施に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。

2.3　職業倫理と誠実性

監査人は、職業倫理に従い、誠実に業務を実施しなければならない。

３．専門能力

監査人は、継続的かつ適切な教育と実務経験を通じて、専門職としての知識及び技能を

維持・向上させなければならない。

４．業務上の義務

4.1　注意義務

監査人は、専門職としての相当な注意をもって業務を実施しなければならない。

4.2　守秘義務

監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、自らの利益のために利用してはならない。

５．品質管理

5.1　情報セキュリティ監査の品質管理

監査人は、監査結果の適正性を確保するために、適切な品質管理を行わなければならない。監査の目的によっては品質を確保するための専門的能力と実務経験を有する品質管理担当者を設定する。

5.2　被監査主体におけるリスクの特徴の考慮

監査人は、監査の実効性を高める観点から、被監査主体におけるリスクの特徴を考慮した監査（リスクベース監査）を行わなければならない。

実施基準

１．監査計画の立案

監査人は、実施する情報セキュリティ監査の目的を有効かつ効率的に達成するために、監査手続の内容、時期及び範囲等について適切と考えられる監査計画を立案しなければならない。監査計画は、事情に応じて適時に修正できるように弾力的に運用しなければならない。

２．監査の実施

2.1　監査証拠の入手と評価

監査人は、監査計画に基づいて、適切かつ慎重に監査手続を実施し、アシュアランス（保証）又はアドバイザリー（助言）についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。

2.2　監査調書の作成と保存

監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければならない。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければならない。

３．監査業務の体制

監査人は、情報セキュリティ監査の目的が有効かつ効率的に達成されるように、適切な監査体制を整え、監査計画の立案から監査報告書の提出及び改善までの監査業務の全体を管理しなければならない。

４．他の専門職の利用

監査人は、情報セキュリティ監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない。他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、及び結果の判断等は、情報セキュリティ監査人の責任において行われなければならない。

報告基準

１．監査報告書の提出と開示

監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。

２．監査報告の根拠

監査人が作成した監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものでなければならない。

３．監査報告書の記載事項

監査報告書には、実施した監査の対象、実施した監査の概要、アシュアランス意見又はアドバイザリー意見、制約又は除外事項、その他特記すべき事項について、監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければならない。

４．監査報告についての責任

監査報告書の記載事項については、監査人がその責任を負わなければならない。