e）読出し専用以外のアクセスは、システムファイルの隔離された複製に対してだけ許可し、それらの複製は、監査が完了した時点で削除するか、又は監査の文書化の要求によってそのようなファイルを保存する義務があるときは、適切に保護する。
f）監査ツールの実行など、特別又は追加の処理に関する要求を特定し、合意する。
g）監査におけるテストがシステムの可用性に影響する可能性がある場合、こうしたテストは営業時間外に実施する。
h）監査及びテストを目的とする全てのアクセスを監視し、ログをとる。

○経済産業省告示第百二十五号

情報セキュリティ監査基準（令和七年改正版）を次のように定め、令和七年八月二十九日から適用する。なお、平成十五年経済産業省告示第百十四号は、令和七年八月二十八日限り廃止する。

令和七年八月二十九日　　経済産業大臣　武藤　容治

情報セキュリティ監査基準（令和７年改正版）

主旨

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。そこで令和７年改正版への改正にあたり、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。

Ⅰ．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を表明することをいい、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指摘と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。

Ⅱ．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。