C2401 情報セキュリティ監査規程

国立情報学研究所 学術情報ネットワーク運営・連携本部  
高等教育機関における情報セキュリティポリシー推進部会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年2月15日  A2401 | 新規作成（監査規程） | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2007年10月31日  A2401 | 「情報セキュリティ監査規程」に文書名変更 | － |
| 2013年7月5日  B2401 | 文書番号の変更のみ | － |
| 2015年10月9日  C2401 | 文書番号の変更のみ | － |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

C2401-01 （目的）

第一条　独立性を有する者による情報セキュリティ監査の実施基準を定めることにより、本学ポリシー、実施規程、及びそれに基づく手順が確実に遵守され、問題点が改善されることを目的とする。

C2401-02 （監査計画の策定）

第二条　情報セキュリティ監査責任者は、年度情報セキュリティ監査計画を策定し、全学総括責任者の承認を得る。

解説：監査の基本的な方針として、年度情報セキュリティ監査計画を策定し、承認を受けることを求める事項である。年度情報セキュリティ監査計画には、次の事項が含まれる。

・重点とする監査対象及び監査目標（情報漏えい防止、不正アクセス防止など）

・監査実施期間

・監査業務の管理体制

・外部委託による監査の必要性及び範囲

・監査予算

なお、以前実施した監査結果で明らかになった課題及び問題点の改善状況について、監査を実施する場合には、年度情報セキュリティ監査計画に盛り込む。

C2401-03 （情報セキュリティ監査の実施に関する指示）

第三条　全学総括責任者は、年度情報セキュリティ監査計画に従って、情報セキュリティ監査責任者に対して、監査の実施を指示する。

２　全学総括責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合、情報セキュリティ監査責任者に対して、年度情報セキュリティ監査計画で計画された事案以外の監査の実施を指示する。

解説：年度情報セキュリティ監査計画において実施する監査以外に、本学内、本学外における事案の発生の状況又は情報セキュリティ対策の実施についての重大な変化が生じた場合に、必要に応じて臨機応変に監査を実施することを求める事項である。

なお、本学内において甚大な情報セキュリティ侵害が発生した場合であって、その侵害の規模や影響度をかんがみ、より客観性・独立性が求められるときは、外部組織による監査を検討することが求められる。

C2401-04 （個別の監査業務における監査実施計画の策定）

第四条　情報セキュリティ監査責任者は、年度情報セキュリティ監査計画及び情報セキュリティの状況の変化に応じた監査の実施指示に基づき、個別の監査業務ごとの監査実施計画を策定する。

解説：監査の基本的な方針に基づいて、実施すべき監査についての詳細な計画を策定することを求める事項である。監査実施計画には、次の事項が含まれる。(経済産業省 情報セキュリティ監査基準 実施基準ガイドラインVer1.0 等を参考)

・監査の実施時期

・監査の実施場

・監査の実施担当者及び割当て

・準拠性監査（ポリシー及び実施規程に基づく手順に準拠した手続が実施されていることを確認する監査）のほか、必要に応じて妥当性監査（実施している手続が有効なセキュリティ対策であることを確認する監査）を行うかについての方針

・実施すべき監査の概要（監査要点、実施すべき監査の種類及び試査の範囲を含む。）

・監査の進捗管理手段又は体制

C2401-05 （情報セキュリティ監査を実施する者の要件）

第五条　情報セキュリティ監査責任者は、監査を実施する場合には、被監査部門から独立した情報セキュリティ監査を実施する者に対して、監査の実施を依頼する。

解説：情報セキュリティ監査を実施する者に監査人としての独立性及び客観性を有することを求める事項である。情報システムを監査する場合には、当該情報システムの構築又は開発をした者は、その監査をしないこととする。また、情報資産の運用状況に関する監査を行う場合には、当該情報資産を運用している者はその監査をしないこととする。

２　情報セキュリティ監査責任者は、必要に応じて、本学外の者に監査の一部を請け負わせる。

解説：情報セキュリティ監査を実施する者は、監査を実施するに当たり、必要に応じて監査対象システムの詳細情報を有する組織、本学内の情報システム部門又は外部専門家の支援を受けることを求める事項である。

組織内に監査を実施する者が不足している場合又は監査遂行能力が不足している場合には、監査業務（内部監査）を外部事業者に請け負わせることを検討すべきである。その委託先の選定に当たっては、被監査部門との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮し、外部委託に関する対策基準に従うこと。また、情報セキュリティ監査企業台帳に登録されている企業や情報セキュリティ監査人資格者の業務への関与などを考慮することが望ましい。

C2401-06 （情報セキュリティ監査の実施）

第六条　情報セキュリティ監査を実施する者は、情報セキュリティ監査責任者の指示に基づき、監査実施計画に従って監査を実施する。

２　情報セキュリティ監査を実施する者は、実施手順が作成されている場合には、それらが本ポリシーに準拠しているか否かを確認する。

３　情報セキュリティ監査を実施する者は、被監査部門における実際の運用が本ポリシー及び実施規程に基づく手順に準拠しているか否かを確認する。

解説：３項は、被監査部門における実際の運用が、ポリシー及び実施規程に基づく手順に準拠して実施されているか否かの確認を求める事項である。監査に当たっては、必要に応じて、自己点検記録の査閲、機器の設定状況の点検等により、被監査部門において実施されている情報セキュリティ対策が有効に機能しているか否かを確認することが求められる。

４　情報セキュリティ監査を実施する者は、監査調書を作成し、あらかじめ定められた期間保存する。

解説：監査意見表明の根拠となる監査調書を適切に作成し、保存することを求める事項である。監査調書とは、情報セキュリティ監査を実施する者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を実施する者自らが直接に入手した資料やテスト結果だけでなく、被監査部門側から提出された資料等を含み、場合によっては組織の外部の第三者から入手した資料等を含むことがある。

５　情報セキュリティ監査責任者は、監査調書に基づき監査報告書を作成し、全学総括責任者へ提出する。

解説：監査結果を報告書として文書化した上で、全学総括責任者へ確実に提出をすること求める事項である。なお、本監査は、実際の運用状況がポリシー及び実施規程に基づく手順に準拠して行われているか等、準拠性の監査を意図したものであるが、監査の過程において、遵守内容の妥当性に関連して改善すべき課題及び問題点が検出された場合には、この検出事項や助言提案を監査報告書に含めることが望ましい。

C2401-07 （情報セキュリティ監査結果に対する対応）

第七条　全学総括責任者は、監査報告書の内容を踏まえ、被監査部門の部局総括責任者に対して、指摘事案に対する対応の実施を指示する。

解説：監査報告書において指摘された課題及び問題点に対する改善を図るため、全学総括責任者へ被監査部門の部局総括責任者に対する対応実施の指示を求める事項である。

２　全学総括責任者は、監査報告書の内容を踏まえ、監査を受けた部門以外の部門においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、他の部局の部局総括責任者に対しても、同種の課題及び問題点の有無を確認するように指示する。

解説：監査報告書において指摘された課題及び問題点が、他の監査対象にも同種の課題及び問題点として存在する可能性が高い場合又は同種の課題及び問題点の存在を緊急に確認する必要性が高い場合には、想定される他の監査対象についても同様に調査を実施する必要がある。そのため、全学総括責任者から部局総括責任者に対する確認の指示を求める事項である。

３　部局総括責任者は、監査報告書に基づいて全学総括責任者から改善を指示された事案について、対応計画を作成し、報告する。

解説：監査報告書に基づいて全学総括責任者から改善を指示された事案について、対応計画の作成及び報告を求める事項である。監査報告書において指摘された課題及び問題点の改善が困難であることについて正当な理由がある場合には、リスク軽減策を示した上で、達成することが可能な対応目標を提示することが重要である。また、その課題及び問題点が人為によるものである場合には、部局総括責任者は、提示された対応目標を情報セキュリティ対策の教育方法や教育施策に反映することが必要である。

４　全学総括責任者は、監査の結果を踏まえ、本ポリシー及び実施規程に基づく既存の手順の妥当性を評価し、必要に応じてその見直しを指示する。

解説：情報セキュリティ監査責任者から報告された監査報告書において、遵守内容の妥当性に関連した改善指摘を受けた場合には、ポリシー及び実施規程に基づく既存の手順の更新を検討することを求める事項である。検討の結果、ポリシー及び実施規程に基づく手順の更新を行わない場合には、その理由について明確化すること。