D2401 情報セキュリティ監査規程

国立情報学研究所 学術研究プラットフォーム運営・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委員会

**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  D2401 | 文書番号の変更のみ | － |
| 2022年12月28日  D2401 | 統一基準（令和3年度版）の改訂への対応 | 高等教育機関における情報セキュリティポリシー推進委員会事務局 |
| 2024年3月26日  D2401 | 統一基準（令和5年度版）の改訂への対応 | 高等教育機関における情報セキュリティポリシー推進委員会事務局 |

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。

解説：情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。本学において実施する情報セキュリティ監査は、業務や情報システムへの理解度が高く、効率的に監査の深掘りができ、組織の情報セキュリティ対策の改善に係るPDCAサイクルを円滑に機能させるためにも重要である。  
また、監査の結果で明らかになった課題を踏まえ、また、監査の結果で明らかになった課題を踏まえ、全学総括責任者は、部局総括責任者に指示し、必要な対策を講じさせることが重要である。

D2401-01 （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の遵守状況が監査の実施を通じて確認され、明らかになった問題点が改善されるようにすることを目的とする。

D2401-02　（適用範囲）

第二条　この規程は、本学及び関係機関において実施するすべての情報セキュリティ監査に適用する。

D2401-03 （用語）

第三条　この規程において用いる用語は、本学が定める「D1001 情報セキュリティ対策基本規程」及び「D2101 情報セキュリティ対策基準」において定めるところによる。

D2401-04　（監査実施計画の策定）（政府機関統一基準の対応項番2.3.2(1), 2.3.2(1)-1,2）

第四条　情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定めること。

解説：「対策推進計画に基づき監査実施計画を定める」について  
情報セキュリティ対策基準第七条に規定する対策推進計画には、監査の基本的な方針として、重点とする監査の対象及び目標（今年度の監査でどのような部分を重視するかを明確にする）・監査の実施時期・監査業務の管理体制等を簡潔に記載することを想定している。監査の基本的な方針の案は、情報セキュリティ監査責任者が作成することを想定している。また、情報セキュリティ監査責任者は、対策推進計画に基づき、個別の監査実施計画を策定し、監査を実施する。被監査部門に対しては、監査実施機関、監査実施者の氏名、監査対象者を含む事項を、情報セキュリティ監査責任者より事前通知し、監査の内容や範囲をあらかじめ明確化しておくことが望ましい。  
なお、内閣官房内閣サイバーセキュリティセンターが公表している「情報セキュリティ監査実施手順の策定手引書」は、監査実施計画の策定における考え方や計画に含めるべき内容等を具体的に示しており、これを参考に計画を策定するとよい。この他にも、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」等にも詳細が説明されているので、併せて参考にするとよい。  
参考：内閣官房内閣サイバーセキュリティセンター「情報セキュリティ監査実施手順の策定手引書」  
（https://www.nisc.go.jp/active/general/pdf/SecurityAuditManual.pdf）  
参考：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」  
（ https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS\_Audit\_Annex05.p df）

２　情報セキュリティ監査責任者は、対策推進計画に基づき、以下を例とする監査実施計画を策定すること。

注意：本項における規定内容は例示にとどまり、以下の各号のいずれも満たさない形での運用も可能となる。よって本項による統制を有効に機能させるために次のような修正を行うことが考えられる。  
① 必須とすべき内容に絞った上で「例とする」を「含む」に改める。  
② 「ただし、第○号及び第○号は必須とする。」のような但し書きを追記する。

一　監査の目的（例：情報セキュリティ対策の実際の運用が情報セキュリティ関係規程に準拠していること等）

二　監査の対象（例：監査の対象となる組織、情報システム、業務等）

解説：「監査の対象」について  
監査の対象を検討する際は、以下の情報を参考に検討することが考えられる。  
・学内で発生した情報セキュリティインシデントの再発防止・教訓  
・本学における教育の実施状況に関する分析・評価結果  
・本学における自己点検結果の分析・評価結果  
・過去の情報セキュリティ監査の結果  
・外部の勉強会や研修で得られた知見  
・最新の脅威動向に関する情報  
また、監査の対象例と監査の対象に合わせた監査内容例は以下のとおりであり、本学の実情に応じて検討すること。  
・情報セキュリティ対策推進体制を監査対象とした場合  
全学総括責任者や全学実施責任者等が担う役割を対象に、情報セキュリティ関係規程の運用が適切に行われていることを確認する。  
対策基準に統一基準を満たすための適切な事項が定められていることを確認する。  
運用規程及び実施手順が対策基準に準拠していることを確認する。  
・特定の業務を監査対象とした場合  
業務に関与する部門、取り扱う情報、使用する情報システムについて、業務手順の観点から情報セキュリティ関係規程の運用が適切に行われていることを確認する。  
・特定の部門を監査対象とした場合  
部門で取り扱う情報、利用する情報システムについて、当該部門の利用者等により情報セキュリティ関係規程の運用が適切に行われていることを確認する。  
・特定の情報システムを監査対象とした場合  
情報システムの情報セキュリティ対策について、情報セキュリティ関係規程で規定されている情報セキュリティ対策が講じられていること、及び実際に運用されていることを確認する。  
・特定の情報セキュリティ対策を監査範囲とした場合  
最新のサイバーセキュリティに関する脅威動向、インシデント事例、様々な情報セキュリティ技術の普及等を踏まえ、以下に示す例のように、セキュリティリスクの高い範囲に監査を限定し、複数の情報システムへ監査を同時に実施する。  
-情報システム関連文書の整備状況  
-インターネットに接続する認証機能での多要素主体認証の導入  
-アクセス制御機能の適切な運用  
-管理者権限を持つ主体の識別コード及び主体認証情報に関する管理  
-ソフトウェアに関する脆弱性対策の実施  
-情報システムの情報セキュリティに影響する各種設定情報  
-不正アクセスへの対策状況

三　監査の方法（例：情報セキュリティ対策の運用状況を検証するため、査閲、点検、観察、ヒアリング等を行う。監査の基準は、ポリシー及びそれに基づく規程等とする）

解説：「監査の方法」について  
監査を実施するに当たっての監査技法の例を以下に示す。監査対象や監査テーマに応じて効果的な技法を実施することで監査品質を向上できるが、監査の作業負荷に留意することが必要である。  
・監査対象の組織の利用者等への質問（ヒアリング）  
・記録文書等やシステム設定等の査閲（レビュー）  
・執務室、サーバ室等の観察（視察）  
・監査人自らが監査対象の組織で実施される運用を試行することによる情報セキュリティ対策の運用状況の評価（再実施）  
・情報システムに対する脆弱性診断又はペネトレーションテスト  
更に、必要に応じて、サーバ、端末、通信回線装置等の機器、クラウド環境を含む情報システムの情報セキュリティに関する設定情報の確認、ログ出力状況の確認などを確認することも考えられる。

四　監査の実施体制（例：監査責任者、監査実施者の所属、氏名）

五　監査の実施時期（例：対象ごとの実施時期）

３　情報セキュリティ監査責任者は、組織内における監査遂行能力が不足している場合等においては、学外の者に監査の一部を請け負わせること。

解説：「学外の者に監査の一部を請け負わせる」について  
情報セキュリティ監査責任者は、監査を実施するに当たり、学内に情報セキュリティ監査実施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することが重要である。また、監査業務を外部事業者に請け負わせることは、業務委託に該当することから、関連する規定にも留意する必要がある。また、情報セキュリティ監査人資格者の業務への関与等を考慮することが望ましい。加えて、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を記載した「情報セキュリティサービス基準適合サービスリスト」（うちセキュリティ監査サービスに係る部分）を活用することも考えられる。  
参考：経済産業省「情報セキュリティサービス基準」  
（https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun.pdf）  
参考：独立行政法人情報処理推進機構（IPA）「情報セキュリティサービス基準適合サービスリスト」  
（https://www.ipa.go.jp/security/it-service/service\_list.html）

４　情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施が必要な場合には、追加の監査実施計画を定めること。

解説：第２項「追加の監査実施計画を定める」について  
学内外において注目すべき情報セキュリティインシデントが発生した場合は、本学の実態を把握するため、追加的な監査を行い、必要な措置を講ずることが想定される。また、情報セキュリティ対策の実施内容に大きな変更が生じた場合は、その対策の実施状況を把握するために追加で監査を行うことも考えられる。このように、情報セキュリティ監査責任者は、対策推進計画に基づき策定した監査実施計画以外の事項についても、必要に応じて監査実施内容に含めることを考慮する必要がある。

D2401-06　（監査の実施）（政府機関統一基準の対応項番2.3.2(2), 2.3.2(2)-1）

第六条　情報セキュリティ監査責任者は、監査実施計画に基づき、監査の実施を監査実施者に指示し、結果を監査報告書として全学総括責任者に報告すること。

解説：「監査報告書」について  
監査報告書の作成に際しては、根拠となる監査調書を適切に作成することが必要である。監査調書とは、情報セキュリティ監査実施者が行った監査業務の実施記録であって、監査報告書に記載する監査意見の根拠となるべき監査証拠、その他関連資料等をつづり込んだものをいう。情報セキュリティ監査実施者自らが直接に入手した資料や試験の結果、被監査部門側から提出された資料のほか、場合によっては外部の第三者から入手した資料等を含むことがある。  
監査の結果は、監査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する必要がある。監査報告書には、実際の運用状況が情報セキュリティ関係規程に準拠して行われているかなどの結果を記載する。さらに、監査の過程において、情報セキュリティ対策の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。反対に組織として推奨すべき優れた取組等がある場合には、それらを組織全体に広めるなどの助言・提案があってもよい。

２　情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者から選定し、情報セキュリティ監査実施者に指名すること。

解説：「被監査部門から独立した者」について  
情報セキュリティ監査実施者には、監査人としての独立性及び客観性を有することが求められる。例えば、情報システムを監査する場合に、当該情報システムの構築をした者や運用を行っている者が監査をしてはならない。また、情報の取り扱われ方に関する監査を行う場合には、当該情報を取り扱う者はその監査をしないこととする。

３　情報セキュリティ監査責任者は、以下の事項を全て含む監査の実施を監査実施者に指示すること。

一　対策基準に政府機関統一基準を満たすための適切な事項が定められていること

解説：「政府機関統一基準を満たすための適切な事項が定められていること」について  
政府機関統一基準1.1(1)において、「情報セキュリティ対策の項目ごとに機関等が遵守すべき事項（以下「遵守事項」という。）を規定する」とされており、また、「政府機関等の対策基準策定のためのガイドライン」（以下、「策定ガイドライン」という。）の1.1(1)「本ガイドラインの目的」において、「統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）を例示するとともに、対策基準の策定及び実施に際しての考え方等を解説するものである。」とされており、策定ガイドラインの1.1(5)「対策基準の策定手順」において、「本ガイドラインに規定される基本対策事項は、遵守事項を満たすためにとるべき基本的な対策事項の例示であり、遵守事項に対応するものであるため、機関等は基本対策事項に例示される対策又はこれと同等以上の対策を講じる必要がある。」とされている。これらの記述から、本条で定める「政府機関統一基準を満たすための適切な事項が定められていること」について監査する際は、政府機関統一基準に準拠するサンプル規程集の規定事項及び解説の記載についても参照した上で監査を実施する必要がある。  
対策基準に、政府機関統一基準を満たすための適切な事項が定められているか否かを判断する際には、本学における組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性を踏まえ、必要な事項が対策基準に盛り込まれているか否かを確認する必要がある。このため、対策基準の策定に当たり、対策基準に各事項を盛り込んだ理由や対策基準策定ガイドラインの基本対策事項との関係等について記録を残しておくと、監査の際に有用である。

二　実施手順がポリシー及びそれに基づく規程等に準拠していること

三　被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること

解説：「実際の運用」について  
被監査部門の職員等に対する質問や記録文書の査閲、執務室等の観察、機器の設定状況の点検等の方法により、運用の準拠性を確認する。また、必要に応じて、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も求められる。例えば、監査対象によってはソフトウェアやウェブアプリケーション等の情報システムに関連する脆弱性の検査、情報システムに対する侵入検査といった方法によっても確認することができる。  
なお、監査実施者が監査過程で情報セキュリティの向上につながる対策等の監査以外の行為を行った場合には、その行為に対する別途の監査が必要となる可能性がある。したがって、情報セキュリティ監査責任者は、情報セキュリティ対策の向上になり得る行為や、作業を効率的に行うことにつながる行為であるとしても、監査以外の行為を監査実施計画の中に取り込むべきではない。

D2401-08　（監査結果に応じた対処）（政府機関統一基準の対応項番2.3.2(3)）

第八条　全学総括責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を全学実施責任者及び部局総括責任者に指示すること。

解説：「指摘事項に対する改善計画の策定等を全学実施責任者及び部局総括責任者に指示」について  
情報システムに対する指摘事項の場合には、部局技術責任者等が指摘事項に対する改善計画の策定等を実施する場合があるので、指摘事項へ対応する範囲に留意し、本条第２項及び第３項でも同様に留意すること。  
なお、指摘事項へ対応する範囲に留意すべき事項は以下が考えられる。  
・部局技術責任者が担当する情報システムでの改善だけでなく、本学の対策基準や運用規程等の見直しが発生する場合には、全学実施責任者や部局総括責任者において改善計画を個別に策定する必要がある。  
・学内で横断的に改善が必要な事項、又は自らが担当する組織のまとまりに特有な改善が必要な事項では、運用規程等の見直しが発生した場合、所管する情報システムで対応が必要となる。また、D2101（情報セキュリティ対策基準）第九十八条に基づき、部局技術責任者が情報システムの情報セキュリティ対策の見直しを行い、その措置結果を全学実施責任者へ報告を行う場合、改善を実施するために複数の関係者が関与するため、責任分界を改善計画で明確にする必要がある。

２　全学実施責任者は、全学総括責任者からの改善の指示のうち、学内で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を全学総括責任者に報告すること。また、措置が完了していない改善計画は、定期的に進捗状況を全学総括責任者に報告すること。

解説：「学内で横断的に改善が必要な事項」について  
監査報告書に記載される改善が必要な事項の内容によっては、監査を受けた部門以外の部門においても同種の課題や問題が存在している可能性がある。また、学内で共通的に使用している情報システムに対する改善が必要な事項については、監査を受けた部門のみで対処することが困難であると同時に、情報システムの利用部門全体に係る改善が必要な事項となる可能性がある。このような、組織全体として改善が必要な事項が確認された場合は、全学実施責任者がその対策に係る事務を統括することが求められる。  
なお、改善を指示されていない事項であっても、監査によって得られた教訓等を被監査組織以外にも展開し、組織全体で監査の教訓を対策に生かすことを考慮することも、組織全体の情報セキュリティを強化するために重要な取組である。

解説：「必要な措置を行った上で改善計画を策定」について  
改善が必要な事項の中には、緊急の措置が必要なものが存在する可能性があることから、そのような事項が確認された場合は、直ちに措置を行い、その結果を報告する必要がある。情報システムの機能改修を伴う措置等、即時の実施が困難と考えられるものについては、情報セキュリティに係るリスクを軽減させるための暫定的な措置を講ずるなどの対応を行うとともに、情報システムの改善計画を策定し、暫定的な措置の実施結果と併せて報告する必要がある。

３　部局総括責任者は、全学総括責任者からの改善の指示のうち、自らが担当する組織のまとまりに特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を全学総括責任者に報告すること。

解説：「自らが担当する組織のまとまりに特有な改善が必要な事項」について  
第１項により、全学総括責任者から指示を受けた改善すべき事項のうち、第２項における「学内で横断的に改善が必要な事項」を除いたものを指している。

解説：「必要な措置を行った上で改善計画を策定」について  
改善が必要な事項の中には、緊急の措置が必要なものが存在する可能性があることから、そのような事項が確認された場合は、直ちに措置を行い、その結果を報告する必要がある。情報システムの機能改修を伴う措置等、即時の実施が困難と考えられるものについては、情報セキュリティに係るリスクを軽減させるための暫定的な措置を講ずるなどの対応を行うとともに、情報システムの改善計画を策定し、暫定的な措置の実施結果と併せて報告する必要がある。