内 部 監 査 事 例 集

（情報セキュリティに関する監査）



監　査　室

令和２年１１月５日

目　　次

１．「情報セキュリティに関する監査」の概要
（１）「東北大学における情報セキュリティ対策基本計画」に関する事項・・・・・Ｐ２
（２）個人情報の管理に関する事項・・・・・・・・・・・・・・・・・・・・・・Ｐ３

２．事例等の紹介
（１）留意事項・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・Ｐ４
（２）部局独自の取り組み・・・・・・・・・・・・・・・・・・・・・・・Ｐ５～６
（３）個人情報保護に関する自己点検・・・・・・・・・・・・・・・・・・・・Ｐ７
（４）その他・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・Ｐ８

１．「情報セキュリティに関する監査」の概要

「情報セキュリティに関する監査」は、「平成３０年度内部監査基本計画書」に基づき、平成３０年１０月３０日から１２月５日の期間（部局、法務課）及び平成３１年2月8日から１４日の期間（情報部）に実施した内部監査です。監査の概要は以下のとおりです。

（１）「東北大学における情報セキュリティ対策基本計画」に関する事項

昨今の国立大学法人等における情報セキュリティインシデント発生の急増とその被害が甚大化する傾向にある状況を鑑み、文部科学省から各国立大学法人等に対して平成２８年６月２９日付け「国立大学法人等における情報セキュリティ強化について（通知）」により、「情報セキュリティ対策基本計画」の策定依頼がなされました。

これを受け、本学において必要な情報セキュリティ対策を組織的、計画的に実施するため、「東北大学における情報セキュリティ対策基本計画（平成 28 年度～30 年度）」が策定されたことから、本件監査では、「東北大学における情報セキュリティ対策基本計画」の進捗状況を確認するため、監査を実施しました。

≪監査対象部局等≫
情報部

≪監査項目≫
「東北大学における情報セキュリティ対策基本計画」の進捗状況

（２）個人情報の管理に関する事項

本学が取り扱う個人情報には、学生に関する入試、成績、学生支援等の情報の他、教職員に関する情報、病院で取り扱う診療情報、全学同窓会である萩友会の会員情報や東北大学基金への寄付者に関する情報等、多岐に渡っています。また、専門性や効率性の観点から外部機関へ業務委託がなされる場合も増加しています。

個人情報の不適切な管理により個人情報の漏えい等が発生した場合、個人の権利を侵害するとともに、本学の社会的信用の失墜や各種法人評価への波及等、本学の運営に多大な影響を及ぼすことから、「個人情報の保護に関する法律」及び「独立行政法人等の保有する個人情報の保護に関する法律」等の法令並びに「国立大学法人東北大学個人情報保護規程」等の学内規程に基づき、個人情報を適切に管理する必要があります。

したがって、本件監査では、各部局における保有個人情報の管理状況及び法務課における所掌事項の管理状況を確認するため、監査を実施しました。

≪監査対象部局等≫
教育学研究科・教育学部、工学研究科・工学部、国際文化研究科、流体科学研究所、
災害科学国際研究所、病院、総務企画部社会連携課、教育・学生支援部

≪監査項目≫
（１）個人情報保護管理体制に関する事項
（２）個人情報の取扱いに関する事項
（３）保有個人情報の安全確保上の問題への対応に関する事項

≪監査対象部局等≫
総務企画部法務課

≪監査項目≫
（１）個人情報保護管理体制
（２）個人情報ファイル簿
（３）今後の個人情報保護管理に関する監査

２．事例等の紹介

（１）留意事項

・以下では、平成３０年度に実施した「情報セキュリティに関する監査」において見受けられた事例等を紹介しています。内容については、法令及び学内規程等を参考にして、監査室において判断しています。

・本事例集は、学内の状況を基に作成したものであることから、「取扱注意」及び「学外持出不可」とし、ＷＥＢ上では学内限定とさせていただきます。

・本事例集の内容に関するお問い合わせは、監査室までお願いします。



（２）部局独自の取り組み

部局独自の取り組み事例を２点ご紹介します。

１）情報セキュリティ対策措置の実施

部局の情報ネットワークに情報端末を接続する際、接続利用予定の情報端末の実機を確認し、接続利用申請書記載の情報セキュリティ対策措置が取られていることを確認した上で、接続を許可している。

解　説

当該部局においては、部局の情報ネットワークに接続する際、接続端末が本学で管理する物品か個人所有かに関わらず申請することを義務付け、以下の申請フローを整備していました。

【申請フロー】
① 利用者による接続利用申請書の提出
② 部局技術担当者（補助者）が研究室へ出向く、もしくは利用者に情報端末を持参してもらい、実機を確認
③ 承認の可否を決定
④ （承認の場合）申請承認メールを送付、接続許可リストに追加

情報端末を実際に確認することで、情報セキュリティ対策措置が取られているかを把握することができ、より厳格な管理体制が整備されているという点で、優れた取り組みと思われます。



２）部局独自の研修会等の実施

① 部局のコンピュータ実習室を授業以外で利用しようとする学生に対し、情報セキュリティ等を内容とする利用前講習会を実施している。

② 部局における新任教職員向け研修において、情報セキュリティに関する講義を実施している。

③ 情報ネットワーク講習会を各研究室の教員（情報ネットワーク管理者）及び学生代表に対して実施し、参加した当該教員及び学生が各研究室構成員に水平展開する体制を構築している。

解　説

上記①について、当該部局においては、部局のコンピュータ実習室に設置された情報ネットワークを授業以外で利用しようとする学生に対し、利用時のルールや個人情報保護等を内容に含んだ利用前講習会を実施していました。

また、上記②について、当該部局においては、新任教職員向け研修の中で、情報セキュリティに関する講義を実施していました。

情報セキュリティインシデントの発生を防止するためには、構成員一人一人が情報セキュリティに対する意識を持つことが重要と考えられることから、利用前講習会や講義の実施による教職員・学生への意識付けは、優れた取り組みと思われます。

上記③について、当該部局においては、情報ネットワーク講習会を各研究室の教員（情報ネットワーク管理者）と学生代表に対して実施していました。また、講習会に参加した教員及び学生が各研究室構成員に内容を伝達する体制が構築されていました。

研究室単位で情報を共有することで、組織としての情報セキュリティに対する意識向上が期待できると考えられる点で、優れた取り組みと思われます。

（３）個人情報保護に関する自己点検

個人情報保護管理体制に関する監査事項として、国立大学法人東北大学個人情報保護規程（以下「規程」という。）第 32 条及び国立大学法人東北大学個人情報保護細則（以下「細則」という。）第 10 条（令和元年５月２０日改正により、現在は第９条）に規定のある「個人情報保護に関する自己点検」の実施状況を確認したところ、複数部局において点検が実施されていませんでした。

解　　説

自己点検について

情報セキュリティ対策は、大学の構成員一人一人が守るべきルールを遵守し、必要な知識の習得を確実に行うことで、実効性が担保されるものです。

加えて、学内規則等に準拠した運用を行っているか等の観点から定期に点検することで、構成員（個人）や所属する部局（組織）の情報セキュリティ対策の水準を確認することができます。

点検結果を踏まえ、部局の管理者（個人情報保護管理者）が必要と認めるときは、その結果を個人情報総括保護責任者に報告し（規程第 32 条）、個人情報総括保護責任者又は個人情報保護管理者は、必要に応じて保有個人情報の適切な管理のための措置について、見直し等を講ずるものとされています（規程第 33 条）。

本件監査においては、個人情報保護に関する自己点検を実施していない部局が見受けられました。また、点検を実施している部局においても、点検の内容等を模索しながら実施している状況が確認されました。

監査結果を受け、内部監査報告書の「本部事務機構に対する意見」として、総務企画部法務・コンプライアンス課に対し、規程第 32 条で求められている個人情報保護に関する自己点検の内容について、改めて各部局に例示する等の対応を要請しました。

その後、所掌課から令和元年６月 27 日付け総法文「「個人情報ファイル簿」の作成・更新及び保有個人情報の管理状況の点検実施について（依頼）」において、「保有個人情報の管理状況点検シート」による点検実施の依頼がありました。

各部局等の事務部においても点検を実施いただいたかと思います。本点検の趣旨をご理解いただき、今後もご協力いただけますと幸いです。

（４）その他

本学は、新しい日常（New Normal）を見据え、教育、研究、社会との共創、さらには業務全般のオンライン化を進め、ポストコロナの新たな時代への社会変革を先導する大学を目指しています。

令和２年６月１日には「東北大学オンライン事務化」が宣言されました。今後、オンライン活用の機会は、さらに増加することが考えられます。

オンラインの活用により、業務効率の向上や多様なライフスタイルに合わせた働き方改革の推進等が見込まれる一方、個人もしくは所属する組織で管理する情報端末を使用することにより、情報端末の紛失や個人情報漏えいの発生といったリスクが予想されます。

高度化するサイバー犯罪や詐欺、個人の不注意による個人情報の漏えい等の情報セキュリティインシデントを防止するためには、各自がセキュリティ対策を確実に実施する必要があります。加えて、先述の「点検→（必要に応じて）改善」のサイクルの実行や、情報セキュリティに関する最新情報の積極的な把握、毎年実施されている「情報セキュリティ・個人情報保護教育」（e ラーニング）の受講による自身の知識・理解度の確認を通じて、一人一人が情報セキュリティに対する意識を持ち続けることが重要と考えられます。

情報を取り巻く環境が日々変化する中、社会動向や学内の動きに注目いただきつつ、本事例集が業務の一助となれば幸いです。

【東北大学監査室】
TEL：022-217-5680
E-mail：kansa@grp.tohoku.ac.jp