平成２４年３月８日

内 部 監 査 報 告 書

（監査事項：情報セキュリティに関する監査）

Ⅰ　監査実施の概要

１．監査目的

・個人情報保護に関する適法性の評価
・情報システムにおけるセキュリティ体制に関する整備状況の調査
・情報漏えい案件に関するフォローアップの実施

２．監査対象部局

文学研究科、経済学研究科、工学研究科、薬学研究科、情報科学研究科、サイバーサイエンスセンター、金属材料研究所、流体科学研究所、多元物質科学研究所、教育・学生支援部

計１０部局

３．監査事項

別紙「監査事項一覧（情報セキュリティに関する監査)」のとおり

４．監査実施期間

平成２３年３月１１日
平成２３年６月１６日～平成２３年７月５日

５．主な監査手続

① 個人情報保護規程等に基づく事務処理に関する関係書類の閲覧及び質問
② 情報セキュリティガイドラインに関する遵守状況のアンケート調査
③ 情報漏えい案件発生部局に対する情報漏えい対策に関する質問

Ⅱ　監査結果の要約

１．全般的所見

（１） 個人情報保護に関する適法性の評価

国立大学法人が取り扱う個人情報には、学生に関する入試、成績、経済支援等の情報の他、教職員本人の氏名、住所、生年月日、家族構成や所得情報もあり、情報資産の管理を徹底する必要性が高くなってきている。また、近年では、外部の民間企業への業務委託（外注、アウトソーシング）がなされる場合も増加しており、外注先での安全管理が図られるよう発注者が監督することを委託契約で定める事例も多くなっていることから、「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」等の法律及び「国立大学法人東北大学個人情報保護規程」等の本学学内規程（以下、「法令等」という）に基づき、より一層個人情報の管理を適切に行わなければならない。

このため、各部局において、これらの個人情報の管理が、法令等に基づき適正に行われているかについて監査を実施したところ、一部に不適切事項は見られたものの概ね良好であると判断した。

また、 個人情報保護業務の管理状況において一部改善が必要と思われる点があった。（Ⅲ．２に記載）

（２） 情報システムにおけるセキュリティ体制に関する整備状況の調査

法人化後、本学における情報システムにおいて取り扱う「個人情報及び法人の機密情報等」の取扱いについては、「情報システムセキュリティ対策ガイドライン H17.7.29」や「国立大学法人東北大学個人情報保護規程」等の学内規程により周知されているところである。

このため、各部局に対し情報システムにおけるセキュリティ対策の状況調査として、情報システム担当者に対するアンケート「情報システムセキュリティ対策ガイドラインに関するアンケート」（別添１）を実施し、情報システムにおける暗号化の有無や各端末の認証機能、不正アクセス対策、コンピュータウイルス対策などについて監査を実施したところ、多くの部局においては概ね良好な自己評価が行われており、監査対象部局にてヒアリングを実施した結果からみても、一部に不適切事項は見られたものの概ね良好であると判断した。

なお、ガイドラインは、あくまでも情報セキュリティ対策の目安として定められたものではあるが、個別の項目では、事務用共有ファイルサーバーの管理や暗号化対策、各端末の認証機能の設定等が適切に行われていない傾向が見られるので、各部局の状況に応じて適切な対応を望むものである。

（３） 情報漏えい案件に関するフォローアップの実施

法人化後、本学における個人情報の取扱いについては、「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」が施行されて以降、同法や「国立大学法人東北大学個人情報保護規程」等の学内規程により周知してきたところであるが、平成２２年度において個人情報が保存されたパソコンを持ち出し、盗難または紛失によって個人情報が漏えいした事案が３件発生した。このため、該当部局に対し再発防止対策について監査を実施したところ、一部に不適切事項は見られたものの概ね良好であると判断した。

また、 部局における適切な個人情報の保護を図るための管理状況において一部改善が必要と思われる点があった。（Ⅲ．２に記載）

２．重要事項等

①改善要求を要する指摘事項

該当なし。

②発見事項

該当なし。

③不適切事項　　１２　件

（内訳）

文書の周知について	１　件
個人情報の保管場所について	１　件
情報システムにおける安全の確保について	２　件
ウイルス対応ソフトの導入状況について	２　件
情報システムのバックアップについて	３　件
個人情報の取り扱いの制限について	１　件
情報媒体の廃棄等について	１　件
安全確保上の問題への対応について	１　件

Ⅲ　改善要求等

１．重要事項に対する改善要求

該当なし。

２．本部事務機構等に対する意見

（広報課）

・教育研修の実施について

「東北大学個人情報保護規程」第８条において、総括保護管理者は保有個人情報取り扱い従事者及び保有個人情報を取り扱う情報システム管理者に対し、教育研修を行う必要がある旨規定されているが、実施状況について確認を行ったところ、実施されていなかった。

教育研修は、個人情報保護事務を遂行するための根幹となるものであり、関連する担当課と連携し、規程に定める教育研修を実施する体制を整備することにより、実質的な個人情報管理の強化措置を行うよう総務部広報課に改善を要請する。

・事務担当者に対する個人情報保護マニュアルの作成について

Ⅱ監査結果の要約「全般的所見（１）個人情報保護に関する適法性の評価」に記載のとおり、今回の監査は法令等に基づく適法性について実施した。しかし、法令等は曖昧な表現で記載されている部分が多く、実際に運用するには法令等を補完するマニュアル等の整備が必要となるが、それらのマニュアルが作成されていなかった。

その結果、監査対象部局において、法令等に基づく事務処理の適法性の検証を実施したが、組織的な事務処理が行われていない実態となっている。

従って、速やかに全部局における個人情報保護事務の実態を把握し、関連する担当課と連携しながら個人情報保護マニュアル等を作成することにより、実質的な個人情報の管理強化措置を行う必要があると考えられる。

・教職員に対する個人情報取り扱いマニュアルの作成について

学生の個人情報は、事務職員ばかりでなく教員も取り扱うことが多いため、監査対象部局における教員に対する個人情報の管理に係る対応状況について監査したところ、多くの部局で教員に対する組織的な対応が行われていなかった。平成２２年度に発生した情報漏えい案件は全て教員によるものであり、個人情報の取り扱い並びにモバイル機器や記録メディアの取り扱いについては、早急に関連する担当課等と連携し、具体的な指示を行う必要があると思われる。

また、現在の法令等の内容は具体性に欠けており、教職員による個人情報の適切な管理ができない状態となっている。このままこの状態を放置するならば今後も情報の漏えい等が発生する可能性があり、当該部局のみならず、このような不適切な状態を放置した本部事務機構の責任は免れることはできない。

これらの問題を解決するためには、教職員に対する個人情報取り扱いマニュアルを作成することにより実質的な個人情報の管理強化措置を行う必要があると考えられる。

・個人情報漏えいに対する再発防止策のフォローアップについて

平成２２年度において、個人情報が保存されたモバイルパソコン等を持ち出し、盗難または紛失によって個人情報が漏えいした事案が３件発生した。このため、該当部局である経済学研究科及び工学研究科に対し再発防止対策がどのように策定され、実施されているか監査を実施したところ、震災等の影響もあると思われるが、具体的な対応策について策定は行っていたものの、実行されていない状態となっていた。個人情報の漏えい対策は、再発防止策を策定するだけではなく、策定した防止策をどこまで実行するかが重要である。個人情報保護事務を所掌する広報課において、再発防止策を提出させるだけではなく、定期的な報告書や自己評価を求めその実態を把握するなど、適切なチェック体制を構築し、特に対応が遅れている項目があれば適切に指導を行うなど、その防止策が有効に機能しているかを確認する必要があると思われる。

・個人情報保護事務に関する自己点検について

「東北大学個人情報保護規程」第３０条は、個人情報保護担当者による自己点検について定めていることから、平成２２年度の実施状況を監査したところ、実施している部局は皆無であった。本来、同規程では保護担当者による自己点検を義務付けているが、実態として、例年広報課からの依頼に基づき実施されているのが現状であったため、平成２２年度において同課が実施依頼を行わなかったことが原因と考えられる。この件については、早急に自己点検の実施を行うよう各部局等に指示をお願いしたい。

また、この自己点検は、本来個人情報保護事務について自ら点検を行い、改善する必要のある項目については自主的に改善することを目的に行っているはずである。しかし、今回監査対象部局に対しこの件についてヒアリングを行ったところ、多くの部局で自己点検は実施するものの、改善行為を行っていないことが判明した。その責任は、当該部局にもあるが、自己点検票の提出を受けても、部局に対し指導助言等を行わない広報課の業務体制にも問題があることは明白である。ついては、自己点検に対する評価制度を導入し、監査責任者に対し報告を行うなど業務の改善が必要と思われる。

３．優れた取り組みについて

各部局における優れた取り組みとして以下の事例があった。これらの事例については、今後監査室の web ページや内部監査事例集等を通じて学内に公開する予定である。

- 学内のネットワーク利用者に対し、ネットワークの利用方法や注意点等を記載した「ネットワーク利用の手引き」を作成し、利用者に対して周知していた。

- 学内のネットワーク利用者に対し、講習会を開催し、ネットワークの利用方法や注意事項等を周知していた。

別紙

監査事項一覧（情報セキュリティに関する監査）

１．個人情報の保護について

- 保護担当者が選任されているか？
- 教員、事務等の区分毎にどのような管理を行っているか？
- 総括保護管理者等が実施している教育研修に職員が参加しているか？
- 保有個人情報の取扱担当者を必要最小限に限定しているか？
- 保有個人情報を、複製、送信、記録媒体の外部への送付及び持ち出しの場合の手続きはどのようになっているか？
- 情報媒体の管理が適正に行われているか？
- 個人情報の廃棄の処理が適正に行われているか？
- 利用及び保管等の取り扱いの状況について記録してあるか？
- 保有個人情報の取り扱いに係る業務を外部に委託する場合、個人情報に係る取り扱いについて書面により取り交わしているか？
- 個人情報ファイル簿を適正に管理しているか？
- 個人情報保護担当者による自己点検を行っているか？

２．情報漏えいについて

- 漏えい等の発生から報告まで迅速に報告がなされたかどうか？
- 漏えい等が発生した場合、再発防止策を策定し、実効性のある防止策を行っているか？

３．情報システムにおける情報セキュリティについて

- 情報システムの管理はどのような管理体制になっているか？
- 保有個人情報の秘匿性等その内容に応じてアクセス制御のために必要な措置を講じているか？
- 保有個人情報の秘匿性等その内容に応じて、当該保有個人情報へのアクセス記録を定期に又は随時に分析するために必要な措置を講じていますか？
- 保有個人情報を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講じていますか？
- コンピュータウイルスによる保有個人情報の漏えい、滅失又はき損の防止のため、コンピュータウイルスの感染防止等に必要な措置を講じていますか？
- 保有個人情報の秘匿性等その内容に応じて、その暗号化のために必要な措置を講じていますか？
- 保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要

な措置を講じていますか？

- 端末の盗難又は紛失による情報漏えいを防ぐため、端末の固定、執務室の施錠等の必要な措置を講じていますか？
- 保有個人情報を取り扱う基幹的なサーバ等の機器を設置する室等に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講じていますか？
- 災害等に備え、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講じていますか？