２０２５年3月２８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

「東北大学におけるサイバーセキュリティ対策等基本計画」の実施状況の検証

２．監査対象部局

情報部

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

２０２５年2月２８日から２０２５年3月１３日

５．主な監査手続

「東北大学におけるサイバーセキュリティ対策等基本計画」の実施状況に関する質問及び関係書類の査閲

Ⅱ．監査結果の要約

１．全般的所見

国立大学法人等におけるサイバーセキュリティ対策等の継続的な取り組みを行うこと及び大学等の保有する多岐にわたる情報資産を新たな脅威等から守ることを目的とし、文部科学省から各国立大学法人等に対して、令和４年６月２２日付４文科高第３６７号「大学等におけるサイバーセキュリティ対策等の継続的な取り組みについて（通知）」が発出され、「サイバーセキュリティ対策等基本計画」（以下、「対策基本計画」という。）の改訂依頼がなされた。本学では当該通知を受け、セキュリティインシデント発生の防止やインシデント発生時の影響範囲を最小限に止めること等を目的として、既存の対策等基本計画を改定し、２０２２（令和４）年１０月～２０２５（令和７）年３月までを対象期間とした対策基本計画を策定した。

対策基本計画では①リスクへの対応認識と確認と体制の構築、②リスクの特定と評価、③リスクへの対策、④外注や共同研究、重要プロジェクトにかかるリスク管理、⑤インシデントの緊急体制と復旧体制の整備、⑥脅威動向や脆弱性情報取集、監視、侵入の特定などの運用について、及び⑦技術的、オペレーション等の監査について、を個別方針とし、個別取組の実施時期を示した工程表が併せて策定された。

また、本学では、２００８（平成２０）年度から全学の情報基盤インフラの維持及び整備にかかる計画を策定し、その計画実施に必要となる経費は全学的基盤経費により安定的に確保しているが、対策基本計画の実施に必要となる経費についても、現行の情報基盤整備計画を必要に応じて見直し確保していくものとされている。

２０２２（令和４）年１０月～２０２５（令和７）年３月までを対象期間とした対策基本計画が適切に実施されているかについて監査を実施したところ、適切に対策基本計画に沿った進捗が図られていると判断した。

なお、サイバーセキュリティ対策は新技術の進展や新たな脅威の登場により対応しなければいけない内容が増加する一方、メール誤送信や情報の意図せぬ公開などの単純な人為的ミスも懸念されるため、今後も引き続き、組織的、継続的なサイバーセキュティ対策の強化すること及びその実行のための予算の確保が重要であることを併せて付記する。

２．指摘事項

ア）改善事項

該当なし

イ）注意事項

該当なし

３．その他

特になし

Ⅲ．改善要求等

該当なし

別紙

監査事項一覧（情報セキュリティに関する監査）

１．リスク管理体制の構築についての実施状況の検証

リスクへの対応認識と確認と体制の構築

・ポリシーや対策推進計画、管理規定の策定
・管理体制の構築
・リスク対策にかかる予算、資源

２．リスクの特定についての実施状況の検証

リスクの特定と評価

・大きなリスクの対象となりうる情報の確認
・大きなリスクの特定
・情報機器の洗い出し

３．リスク対策の実施状況の検証

リスクへの対策

・守るべき情報の保護
・情報機器の脆弱性対応
・災害等などのリスク対策
・構成員へのセキュリティ意識の徹底

４．サプライチェーンリスクへの対応についての実施状況の検証

外注や共同研究、重要プロジェクトにかかるリスク管理

５．インシデント対応体制の構築についての実施状況の検証

インシデントの緊急体制と復旧体制の整備

６．セキュリティ運用の実施についての実施状況の検証

脅威動向や脆弱性情報取集、監視、侵入の特定などの運用について

７．監査等での運用チェックについての実施状況の検証

技術的、オペレーション等の監査について