

情報セキュリティ監査
仕様書

平成 XX 年 YY 月
国立大学法人 A 大学

1. 件名:情報セキュリティ監査

2. 概要

国立大学法人A大学（以下「本学」という。）の情報セキュリティポリシーでは、監査を実施することが決められている。監査には内部監査と外部監査の両方を実施することがセキュリティ向上に有効である。本件は、外部のセキュリティ専門業者により本学のセキュリティ監査を実施し、本学の情報セキュリティの現状分析の参考としその向上に役立てるものである。

3. 要件

- 1) 本学の情報セキュリティ管理が適正に行われているか、情報セキュリティポリシーおよび実施手順を点検し、点検結果を文書で報告すること。文書は電子化されたものと印刷されたものの両方を提出すること。
- 2) 聞き取りにより、情報セキュリティポリシーおよび実施手順の遵守状況を調査すること。調査結果を文書で報告すること。文書は電子化されたものと印刷されたものの両方を提出すること。
- 3) 本学と協議の上監査実施範囲を決定し監査の実施計画書を提出すること。
- 4) 監査実施体制を提示すること。
- 5) 本学と秘密保持契約を締結すること。契約書の詳細は本学と協議の上決定すること。

4. 実施内容

- 1) 聞き取り対象の人数は ○○名以上とすること。
- 2) 聞き取りの対象は、本学職員が決める。
- 3) 聞き取りの実施日は、業務の影響範囲などを勘案した上で本学職員と協議して決定すること。
- 4) 聞き取り内容を録音する場合には、聞き取りの本人から了解を得ること。

5. 請負者に必要な条件

- 1) 監査実施者は、複数の監査人を選任し、監査人のうちの一人を監査責任者とすること。
 - ① 監査責任者は、下記資格のいずれかを取得していること。
 - (ア)ISACA(情報システムコントロール協会)が認定するCISA(公認情報システム監査人)の資格
 - (イ)NPO(日本システム監査人協会)が認定する公認システム監査人の資格
 - (ウ)日本規格協会マネジメントシステム審査員評価登録センターまたは国際審査員登録機構に登録されたISMS 審査員資格
 - ② 監査責任者を補佐する監査人(2名以上)は、それぞれ下記の資格のいずれかを保有していること。
 - (ア)ISACA(情報システムコントロール協会)が認定するCISA(公認情報システム監査人)の資格
 - (イ)NPO(日本システム監査人協会)が認定する公認システム監査人の資格
 - (ウ)独立行政法人情報処理推進機構(旧試験期間:財団法人日本情報処理開発協会)の情報セキュリティアドミニストレータ資格
 - (エ)財団法人日本情報処理開発協会のISMS審査員補資格
- 2) 監査実施者は、経済産業省の「システム監査企業台帳(平成○年度)」または「セキュリティ監査企業台帳(平成○年度)」に登録されていること。
- 3) 監査実施者は、平成○年から△年の期間において情報セキュリティ監査実績を複数(5以上)有すること。特に、国の機関、独立行政法人、あるいは国立大学法人の情報セキュリティ監査を受注した実績を有すること。
- 4) 監査実施者は、本件で発生する作業を外部業者に対して再委託しないこと。

6. 結果報告及び提出物

- 1) 監査に係わる報告書の提出及び改善策の提案について報告会を実施すること。
- 2) 日本語で作成した監査結果報告書
 - ① 電子化された報告書(PDFファイル) 1式
 - ② ファイルリングされた報告書(印刷物) 1式

7. 納期

平成〇〇年 XX 月 XX 日

8. その他

- 1) 本仕様に定められていない点については、本学職員と協議の上、実施細目を決定すること。
- 2) 本監査に必要なもの以外は、本学に持ち込まないこと。
- 3) 本監査する上で請負者の責に帰すべき事由により、本学に損害を与えた場合には、請負者の責任において現状に復すること。また、請負者が被った損害は、本学の責により生じたもの以外は一切の責任を負わないものとする。
- 4) 本監査で作成した一切のものは、すべて本学に帰属するものであり、私権を設定してはならない。