大阪府立大学情報セキュリティ監査
業務委託仕様書

1. 業務名

大阪府立大学情報セキュリティ監査業務

2. 監査目的

本業務は、本学が定める情報セキュリティポリシーに基づき実施している、情報資産管理、情報システムの保守・運用手順の整備等の情報セキュリティ対策について基準等に準拠して適切に実施されているかを点検評価することで、第三者による独立かつ専門的な立場から本学が抱える情報セキュリティの問題点を明らかにし、本学の情報セキュリティ対策の向上につなげることを目的とする。

3. 委託期間

契約締結の日～平成 31 年 1 月 31 日（木）

4. 監査対象

監査室、理事長室、広報課、総合企画課、総務・施設課、人事課、財務課、
研究推進課、国際・地域連携課、学術情報課

	キャンパス	所属長	実務担当者	その他
監査室	中百舌鳥 C	1	1	1
広報課		1	3	7
総合企画課		2	4	7
総務・施設課		2	7	１５
人事課		1	7	２２
財務課		1	１０	２７
研究推進課		2	5	５７
国際・地域連携課		2	3	9
	なんばセンター	0	1	6
学術情報課	中百舌鳥 C	3	5	１７

（平成 30 年 4 月現在・人数などは変更する可能性がある）

5. 委託内容

本業務は助言型監査とし、本学が施行している「情報格付け取扱手順」及び各組織が作成している「情報セキュリティに関する業務実施手順書」（以下「両手順書」という）の運用監査について当該業務委託を実施するものとする。

具体的には、両手順書に沿った業務運用状況を監査するための項目を抽出し、職員へのアンケートやヒアリング、現地調査等により、業務で取り扱う情報資産が適正に運用・管理されているか、専門的視点から監査する。

(1) 監査実施計画書の作成

情報セキュリティ監査について、目的、対象、場所、方法、実施スケジュール、監査チームの構成、作業者、その他必要な手順等を具体的に記載した監査実施計画書を作成すること。

その際、監査を実施する上で大学側が行う作業等について明示すること。また、内容について本学の承認を得ること。

(2) 予備調査の実施

「情報格付け取扱手順」及び「情報セキュリティに関する業務実施手順書」から事前に調査すべき項目を抽出し、アンケート調査票を作成すること。アンケート調査票は、情報セキュリティに関する専門知識を持たない者でも内容を明確に理解できるものとし、選択式を中心に、必要に応じて記述式を用いるものとする。その際、アンケート調査の項目は平成 29 年度の調査票に準じることとし、規定改正などが生じた部分についてのみ修正するものとする。

監査対象者数等は 4. に記載の通りである。また、アンケート項目について本学の承認を得ること。

なお、アンケート調査票の対象者への送付と回収は、本学が行う。

(3) 予備調査報告書の作成

(2)の予備調査の結果をもとに、予備調査報告書を作成し、提出すること。その際、フォーマットなどは平成 29 年度の予備調査報告書に準じることとする。予備調査報告書は、対象組織別及び全体まとめを含むものとし、その内容について本学の承認を得ること。

なお、対象組織別の予備調査報告書は、(4)のヒアリング及び現地調査に先立ち、4. に記載の所属長及び実務担当者に提供することを前提とする。

(4) ヒアリング及び現地調査の実施

ヒアリング形式で質問を行うほか、業務を行っている現場や文書・記録等の確認を実施し、両手順書に基づいた情報セキュリティ対策の遵守状況を把握する。その際に必要となる資料があれば、必要部数を準備すること。

ヒアリング内容は(3)の予備調査の結果から、特にヒアリング及び現地調査により把握

する必要があると認められる項目とし、ヒアリング項目について本学の承認を得ること。その上で、ヒアリング及び現地調査を主体的に実施すること。

なお、ヒアリング及び現地調査は平日 9 時半から 17 時の間に行うものとし、日程調整と場所の確保は本学が行う。

(5) 監査報告書の作成

(3)の予備調査の結果、及び(4)のヒアリング及び現地調査で実施した各検証をもとに、監査報告書を作成し、提出すること。その際、フォーマットなどは平成 29 年度の監査報告書に準じることとする。監査報告書は、対象 10 組織別及び全体まとめの合計 11 種を作成し、内容について本学の承認を得ること。

監査報告書には検証結果を記述するとともに、問題点とした部分についてはその根拠と緊急度の区別を記載すること。併せて、具体的な改善方法を提案するとともに、それを実施することによる効果を記載すること。その際、できるだけ専門用語の使用を避け、情報セキュリティに関する知識を持たない者でも内容を明確に理解できるものとすること。

また、監査結果を踏まえ、両手順書そのものに関する改善点があれば、その点についても監査報告書に具体的に記載すること。

(6) 監査報告会の開催

4．に記載の所属長に対し、監査報告書の内容について、質疑応答を交えて分かりやすく詳細に口頭説明を行うこと。その際、監査報告会の内容及び資料について本学の承認を得た上で、必要部数を準備すること。

なお、監査報告会は 12 月上旬の平日 9 時半から 17 時の間に行うものとし、日程調整と場所の確保は本学が行う。

(7) 相談対応

ヒアリング、現地調査、及び監査報告会の際に、情報セキュリティに関する問題等についての相談を受けた場合は、適切に対応すること。

6. 監査成果物の内容、納期、納品方法等

(1) 監査成果物の内容

下記の監査成果物を、印刷物（A4 判簡易製本）及び電子媒体（CD-ROM）により、必要数提出すること。なお、電子媒体におけるデータの形式は Word、Excel、PowerPoint、PDF を基本とし、それ以外のデータ形式を用いる場合は別途相談すること。

・監査成果物：監査実施計画書、アンケート調査票、予備調査報告書、ヒアリング調査票（現地調査含む）、監査報告書（11 種）、監査報告会資料

・提出物数　：印刷物は各 2 部、電子媒体は 1 枚

(2)　最終納期

平成 31 年 1 月 31 日（木）

(3)　納品先

大阪府堺市中区学園町 1 番 1 号

大阪府立大学学術情報課情報システム室

7. 適用基準

(1)　政府等が示す基準

・地方公共団体における情報セキュリティ監査に関するガイドライン
（平成 27 年 3 月版）

・地方公共団体における情報セキュリティポリシーに関するガイドライン
(平成 27 年 3 月版)

・上記のほか委託期間において情報セキュリティに関し有用な基準等で、委託者と協議して採用するもの。

(2)　規程文書

・大阪府立大学情報格付け取扱手順（平成 30 年 4 月 1 日施行）

・情報セキュリティに関する業務実施手順書（各課・事務所において策定・施行）

(3)　その他、本業務に関して必要と思われる基準

8. 監査人の要件

①　監査責任者、監査人、監査補助者、アドバイザ等で構成される監査チームを編成すること。

②　監査チームは、本業務の実施に当たり、必要十分な人員で編成すること。

③　監査チームは、次に掲げる知識及び技能を備えていること。

・情報セキュリティ監査の実施に関する知識及び技能

・情報セキュリティに係るリスクのマネジメントに関する知識及び技能

・ISMS 認証取得のマネジメントに関する知識及び技能

・情報セキュリティの技術に関する知識及び技能

・その他の関連知識及び技能（プロジェクト管理、文書作成等）

④　監査チームには、財団法人日本情報処理開発協会 ISMS ユーザーズガイド(JISQ27001:2014(ISO/IEC27001:2013)対応)「表 7-2 力量と関連する資格」で明らかにされている資格の要件を備えた専門家が 1 人以上含まれていること。

⑤　監査チームには、監査の効率と品質の保持のため次のいずれかの実績（実務経験）を有する専門家が 1 人以上含まれていること。

・公的機関又は地方公共団体における情報セキュリティ監査

・公的機関又は地方公共団体における情報セキュリティに関するコンサルティング
・情報セキュリティポリシーの作成(支援を含む)

⑥　監査チームの構成員が、監査対象における情報資産の管理並びに当該情報資産に関する各種ネットワーク及び情報システムの企画、開発、運用、保守等について関わっていないこと。

⑦　本学が監査人の要件を満たしていないと判断し人員交代の要請を行った場合は、速やかに対応すること。

9. 委託業務の実施方法

業務の実施にあたっては以下の方法により行うものとする。

①　契約締結後、受託者は 14 日以内に監査項目および監査内容、実施スケジュール等を記載した監査実施計画書を提出し、大学及び受託者の協議により委託業務の詳細内容及び各作業の実施時期を決定するものとする。

②　7.の適用基準及びその他の説明のために引用又は参照する資料については、信頼しうる配布元から受託者が自らの負担で入手すること。

③　スケジュールに基づいた業務の進捗状況について、大学の求めに応じ、随時委託作業の報告や委託内容に関する資料の提出を行うこと。

④　大学の求めに応じ、大学との打合せを実施すること。また、その際の議事録も含め、すべての打合せにおいて議事録を作成すること。なお、議事録については、各打合せ終了後 7 日以内に提出するものとする。

⑤　その他必要な事項については、大学及び受託者による協議の上決定する。

10. その他

①　受託者は、この契約に関して知り得た秘密を漏らしてはならない。この契約終了後も同様とする。

②　受託者は、この契約に基づく業務を処理するために大学から提供された資料等を、大学の承諾なく複写及び複製してはならない。また、契約終了後は、速やかに大学に返却しなければならない。なお、提供された資料のうち、個人情報保護に係るものは、施錠した保管庫等で保管する等、適切に管理しなければならない。

③　本業務に必要な機器類の調達、通信費等は、本契約に含めるものとする。

④　受託者は、この契約に関して保護すべき情報を取り扱った担当者の所属・氏名等の一覧を大学に提出すること。

以上