放送大学学園情報セキュリティ監査仕様書

1. 目的

本業務は、放送大学学園（以下「学園」という。）が実施している情報セキュリティ管理が、学園の基準に基づいて適切に実施されているか否かを、第三者による独立かつ専門的な立場から検証・評価することにより、学園の情報セキュリティ管理上の課題とそれに対する改善策を明確にすることで、情報セキュリティ水準の一層の向上を図る。

2. 期間

平成２８年１月１２日から平成２８年３月３１日まで

3. 業務の内容

3.1 監査実施計画書の作成

監査の実施体制、監査項目毎の実施スケジュール及び実施手順書を監査実施計画書として作成すること。

3.2 監査項目

1) 各所属における情報セキュリティポリシーの遵守状況の調査（現地調査）
2) 教職員等の情報セキュリティポリシーの理解度、意識の傾向の調査（教職員アンケート）

3.3 調査報告書の作成

各調査結果について、調査報告書を作成すること。

3.4 最終報告書の作成及び監査報告会の開催

一連の調査内容及び調査結果をとりまとめ、報告書を作成し、監査報告会を開催すること。

4. 監査の実施方法等

4.1 監査の基準

次の基準（以下「ポリシー等」という。）を基に、監査チェックシートを作成し、これに基づく助言型の監査を実施すること。

【必須とする基準】

(1) 放送大学学園情報セキュリティポリシー（別紙 1. 基本方針）
(2) 放送大学学園情報セキュリティガイドライン利用者用　契約後本学より提供
(3) 放送大学学園情報資産管理表　契約後本学より提供

【参考とする基準】

(1) 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）（総務省） http://www.soumu.go.jp/main_content/000348656.pdf

(2) 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）（総務省） http://www.soumu.go.jp/main_content/000348657.pdf

(3) 情報セキュリティ監査基準及び同実施基準ガイドライン
（経済産業省）http://www.meti.go.jp/policy/netsecurity/isaudit.html

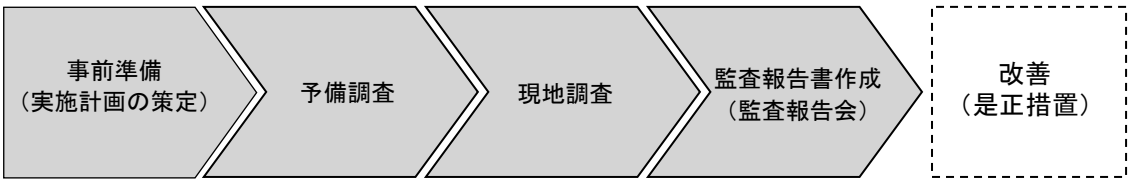
(4) 上記のほか、情報セキュリティ監査に有用な基準等は、学園と協議のうえ採用すること。

4.2 監査の対象範囲と実施方法等

4.2.1 現地調査

学園本部、学習センターにおいてポリシー等の遵守状況を確認するために、学園が指定する所属に赴き、教職員に対するインタビュー及び執務室内の巡視により調査を実施すること。

現地調査は以下に示した流れで実施する。



① 事前準備（実施計画の策定）

本学園の情報セキュリティに関する文書の閲覧、全体的な情報セキュリティの状況把握、監査日程の調整等を行い、監査実施計画書（本計画書）を作成すること。

② 予備調査

ポリシー等の内容確認等概要調査の監査チェックリストの作成を行い、各所属長を対象とする自記式アンケートで概要調査を行うこと。

③ 現地調査

ポリシー等の遵守状況を確認するために、本学園が指定する所属に赴き、職員に対するインタビュー及び執務室内の巡視により調査を実施すること。

監査の重点項目を以下に示す。

【調査技法】

インタビュー	対象所属の管理者・担当者への質問による口頭での確認
閲覧	文書・記録等の閲覧による確認
観察	執務室等の視察（目視）による観察（職員等へのインタビューを含む。）
再実施	監査人立ち会いの下、実際に職員等が操作を行うことによる確認

【調査対象者】

現地調査は、学園本部１７課・室、「社会と産業コース」所属の専任教員（最大 10 名）、千葉学習センター、福岡学習センター、大阪学習センター、群馬学習センターの計２２所属で実施すること。調査にかかる交通費等は本入札に含めること。調査時間は 10 時～12 時、13 時～15 時、15 時～17 時の 2 時間程度で終了するスケジュールで実施すること。実施日程や内容等詳細については契約締結後打ち合わせにて決定する。

対象者	住所
学園本部１７課・室	千葉県千葉市美浜区若葉 2-11
「社会と産業コース」所属専任教員（最大 10 名）	千葉県千葉市美浜区若葉 2-11
千葉学習センター	千葉県千葉市美浜区若葉 2-11
群馬学習センター	群馬県前橋市若宮町 1-13-2
大阪学習センター	大阪府大阪市天王寺区南河堀町 4－88
福岡学習センター	福岡県春日市春日公園 6-1

表１　現地調査のタイムスケジュール案

No.	実施事項	主な実施内容	実施時間例
1	監査開始会議	所属側の対応者の確認、タイムスケジュールの確認等を行うこと。	10:00～10:10（10 分）
2	インタビュー・閲覧	監査チェックリストに基づき、ポリシー等の遵守状況を確認すること。 必要に応じて文書及び記録類の閲覧を行う。	10:10～11:00（50 分）
3	観察	監査チェックリストに基づき、執務室内等の観察、職員等へのインタビューを行うこと。	11:00～11:15（15 分）
4	検出事項等の整理	説明用に内容の整理を行うこと。	11:15～11:45（30 分）
5	監査終了会議	対象者への説明を行うとともに、意見交換を行うこと。	11:45～12:00（15 分）
			計 2 時間

【調査の重点項目】

ア）情報資産の管理

情報資産の管理について、以下の事項を調査すること。

1.　重要度に応じた分類がされているか。
2.　重要度の高い情報を保存した記録媒体に識別が付されているか。
3.　重要度の高い情報について、台帳管理がされているか。
4.　重要度の高い情報の持ち出し、閲覧、配布等を行う場合、定められた手続きに則って行われているか。
5.　重要度の高い情報等の管理文書が適切に保管されているか。
6.　重要度の高い情報の記録媒体の保管や廃棄が適切に行われているか。

7. 教務情報システム等で出力した学生の個人情報に関して、保管や廃棄が適切に行われているか。

イ）情報機器の管理

独自購入のパソコンの持ち込み、持ち出しについて、以下の事項を調査すること。

1. 持ち込み、持ち出しにあたり情報資産管理者の承認を得るなど、定められた手続きを経ているか。
2. 現在有効なコンピュータウイルス対策ソフトが導入され、最新のパターンファイルを適用しているか。
3. 最新版のセキュリティパッチ適用など、セキュリティホール対策がとられているか。
4. ファイル共有ソフト等、情報セキュリティ事故の危険を誘発するソフトウェアがインストールされていないか。
5. その他、情報セキュリティ上の問題はないか。

所属で管理するＵＳＢメモリ等の記録媒体（個人所有のものを除く。）の管理について、以下の事項を調査すること。

1. 台帳管理されているか。
2. 記録媒体は施錠保管されているか。
3. 重要度の高い情報の持ち出しを行う場合、定められた手続きに則って行われているか。

【評価基準】

○：適合	適用基準に準拠した運用（情報セキュリティ対策の実施）が確実に行われていること（適切性）を確認できた。
△：観察事項	適用基準に準拠した運用（情報セキュリティ対策の実施）が行われているが、想定されるリスクへの対応が適切とはいえない。
×：不適合	（重大事項） 適用基準に準拠した運用（情報セキュリティ対策の実施）が行われていないことが明白であり、リスクが顕在化する可能性が高い、又はリスクが顕在化した場合の影響が大きいため、早急な対処が必要である。 （軽微事項） 適用基準に準拠した運用（情報セキュリティ対策の実施）が行われていないがリスクが顕在化する可能性は低い、又はリスクが顕在化しても影響は小さいものの対処が必要である。
N/A：非該当	当該監査項目が該当しない。

※ここに記述されていない詳細な部分については監査人の判断により追加する。詳細は契約後打ち合わせにて調整する。

④ 調査報告書の作成

調査報告書は、各所属別の詳細結果を記述した「調査報告書（詳細版）」と、学園全体の傾向を記述した「調査報告書（概要版）」を作成すること。

報告書の作成にあたっては、総括を記載するなどして全体の流れを理解しやすくするとともに、

問題点（不適合事項）に対しては、現状把握や問題点の指摘のみにとどまらず、具体的かつ有効な解決策の提示を行うこと。なお、「調査報告書（概要版）」については学園担当者と合意を得るため、素案の段階で記述内容の確認を学園担当者へ依頼し報告書を作成すること。

⑤ 監査報告会

学園担当者との合意を得た調査報告書を作成し、その内容について監査報告会で報告を行うこと。監査報告会の日程については３月末を予定している。

4.2.2 職員アンケート

教職員のポリシー等、情報セキュリティに関しての理解度、意識に関して質問を行い、集計・分析を行うこと。

① 事前準備

【調査対象者】

学園教職員（本部、学習センター、常勤教員）約 1,000 名

【調査内容】

教職員のポリシー等、情報セキュリティに関しての理解度、意識に関して質問を行い、集計・分析を行うこと。アンケート項目は、30 項目程度とし、項目は、学園の担当者と打ち合わせを行い決定すること。質問に当たっては専門用語の使用は極力控え、わかりやすく平易な表現を用いること。

【調査方法】

電子メールあるいは Web ページ等で対象者に行うこと。調査期間は二週間を予定している。詳細は別途協議のうえ決定する。

② 集計・分析

アンケート調査の回収については、督促を行い対象者の期限内に 2/3 以上を目標とする。

③ 調査報告書の作成

教職員の情報セキュリティポリシーの理解度、意識の傾向を分析したものを調査報告書として作成すること。報告書は専門用語の使用は極力控え、わかりやすく平易な表現を用いること。素案の段階で記述内容の確認を学園担当者へ依頼し報告書を作成すること。

④ 監査報告会

学園担当者との合意を得た調査報告書を作成し、その内容について監査報告会で報告を行うこと。監査報告会の日程については３月末を予定している。

4. スケジュール案

	分類	１月			２月			３月		
現地調査	事前準備		●	●	●					
	予備調査			●	●					
	現地調査					●	●			
	監査報告書作成					●	●	●		
アンケート	事前準備		●	●						
	アンケート作成			●						
	アンケート実施				●	●				
	集計・分析						●	●		
	監査報告書作成							●		
共通	監査報告会								●	

5. 成果物

成果物は次のとおりとし、Ａ４判縦（必要に応じＡ３判横のページの挿入も可）で横書きとし、紙媒体で２部提出すること。

また、紙媒体のほかに、Microsoft Word 2013、Excel 2013 のいずれかの記録形式で確認可能な電子媒体（ＣＤ－Ｒ等）で正副各１部提出すること。

なお、電子媒体については、最新のパターンファイルによりウイルスチェックを実施したうえで提出すること。

(1) 監査実施計画書

(2) 最終報告書（本編及び概要版を作成すること。）

・所属別現地調査報告書（２１所属）

・アンケート報告書

・監査報告書（概要版）

6. 従事者の要件

監査を行う者は、監査対象となるシステム等と利害関係を有しない中立的な立場にあり、かつ情報セキュリティ監査業務に精通した者が行うこと。さらに、監査の実施にあたっては、学園の情報セキュリティポリシー等の詳細情報を公開する必要があるため、秘密保持の面で信頼性の高い業者でなければならないことから、次のすべての条件を満たすこととする。

(1) 監査従事者の中に、過去 10 年以内に学園に在職していた者、学園で運用しているシステムの設計、構築、運用及び保守にかかる業務に携わった者が含まれていないこと。

(2) 秘密保持に関する社内規則が定められており、社員との守秘義務契約を締結していること。

(3) 監査従事者のうち、監査業務全体を指揮し管理する役割を担う監査責任者は、公認情報セキュリティ監査人を取得し、10 年以上の情報セキュリティ監査業務経験を有する者を充て応札時にこれを証明すること。

(4) 監査従事者のうち、監査業務担当者、5 年以上の情報セキュリティ監査業務経験を有する者を充て応札時にこれを証明すること。

7. 作業時間

現地調査やインタビュー等、学園内で行う作業については、原則として学園の勤務時間内（国民の祝日を除く月～金曜日の９時００分～１７時４５分）に行うものとする。
その他、具体的な作業日時等については、学園との協議のうえ決定すること。

8. 再委託

原則として業務の再委託は認めないが、高度な専門性を有する業務の一部を再委託することが必要である場合は、あらかじめ書面により学園の承諾を得てこれを行うことができる。
なお、再委託を行う場合、再委託先事業者も本仕様書で規定する項目を遵守するよう再委託先との契約書中に明記すること。

9. 守秘義務等

本業務に従事する事業者（再委託先の事業者を含む）は、業務中に知り得た情報を、業務の実施に必要な範囲内においてのみ利用するものとし、情報漏えい防止のため、取扱いに十分留意するとともに、これを第三者に漏らしてはならない。これは契約終了後も同様とする。
また、業務上取り扱うデータについては、業務に必要な範囲内においてのみ利用するものとし、これを所定の場所以外に持ち出してはならない。
その他、本業務に係る契約書の特記事項に記載された重要情報の取扱い等に関する規定については、これを遵守しなければならない。

10. 受託者負担

(1) 作業に必要な機器、ツール、消耗品等は、受託者において用意し、これらを学園のネットワークに設置、導入する場合は、事前に書面により学園と協議し、作業終了後は原状に復すること。
(2) 業務に必要な交通費用等は受託者の負担とすること。
(3) 作業の実施中にシステムに障害を発生させた場合は、速やかに学園に連絡するとともに速やかに原状に復する支援を行うこと。
(4) 受託者は業務の執行にあたり、故意又は過失により学園又は第三者に損害を与えた場合は、損害賠償の責任を負うものとする。また、業務終了後に学園又は第三者に損害を与えたことが発覚した場合も同様とする。

11. 著作権

(1) 成果物の所有権・著作権等は、学園より受託者へ契約金額が完済されたときに受託者より学園に移転する。なお、成果物に受託者独自のノウハウ、アイデア、ツール、分析アプローチ、テンプレート等を使用して報告書を作成した場合、それらに該当する著作権の移転は含まれない。
(2) 成果物に第三者が権利を有する著作権が含まれている場合は、受託者は当該著作権の使用に関する負担金の一切の手続きを行い、第三者の著作権その他の権利を侵害してはならない。

12. その他

本仕様書に示す業務内容等は主要事項を定めたものであり、明記していない事項についても業務として当然行うべき事項については本仕様に含まれるものとする。また、定めのない事項については、必要に応じて学園と協議のうえ決定することとする。

以上