仕　様　書

1　業務名

令和元年度情報セキュリティ監査等業務

2　業務目的

広島市立病院機構（以下「本機構」という。）の情報システムの運用管理等において、「広島市立病院機構情報セキュリティポリシー」（以下「ポリシー」という。）等に基づき実施している情報セキュリティ対策について、監査計画に従って、第三者による独立かつ専門的な立場から情報セキュリティ監査を行うとともに、本機構職員を対象とした情報セキュリティ対策に関する研修等を実施し、本機構の情報セキュリティ対策の向上を図る。

3　契約期間

契約締結日から令和２年３月３１日まで

4　業務実施場所

広島市立広島市民病院（広島市中区基町 7-33）
広島市立安佐市民病院（広島市安佐北区可部南二丁目 1-1）
広島市立舟入市民病院（広島市中区舟入幸町 14-11）
広島市立リハビリテーション病院（広島市安佐南区伴南一丁目 39-1）
その他本機構が指定する場所

5　業務内容

（１）情報セキュリティ監査

ポリシー等に基づき、情報セキュリティ対策の改善に関する助言型の情報セキュリティ監査を実施すること。なお、監査日程及び監査項目については、本機構と協議の上、決定すること。

ア　監査対象システム

（ア）本機構が所管又は利用する情報システム
（イ）監査対象は８システムとし、詳細は契約締結後に提示する。

イ　監査適用基準

（ア）広島市立病院機構情報セキュリティポリシー
（イ）監査対象システムの情報セキュリティ実施手順
（ウ）広島市個人情報保護条例（平成１６年広島市条例第４号）
（エ）医療情報システムの安全管理に関するガイドライン
（オ）医療機関における情報セキュリティ等に関する有用な基準等で、本機構と協議の上、採用するもの

ウ　監査評価基準

監査評価基準は次のとおりとする。他の監査評価基準を用いようとする場合は、本機構と協議の上、決定すること。

評価基準	内　容
重大な不適合	情報セキュリティの維持に、問題が発生する可能性が高い状況
軽微な不適合	情報セキュリティの維持に、問題が発生する可能性がある状況
観察事項	情報セキュリティの維持に問題はないが、改善することが望ましい状況
推奨事項	情報セキュリティの維持に特に有効な施策を実施されている状況

エ　監査内容

監査対象のシステムについて、各情報システムの運用管理が、ポリシー等に基づいて適切に実施されているかを監査すること。

オ　監査方法等

（ア）監査実施計画書の作成

監査日程等の決定後、別紙で示す様式に従って、監査実施計画書を作成すること。

（イ）監査チェックリストの作成

監査を効率的かつ効果的に実施するため、事前に監査対象システム所管課及び利用課に確認すべき具体的な項目を記載した、監査チェックリストを作成すること。

（ウ）監査調書の作成

監査対象システム所管課及び利用課から提出される資料の確認、関係者へのヒアリング等を実施し、その内容を取りまとめた監査調書を作成すること。

（エ）意見交換会の実施

監査の結果、発見された問題点について事実誤認がないかなど確認を行うための意見交換会を実施すること。意見交換会終了後は、議事録を作成し速やかに提出すること。

（オ）監査報告書の作成

別紙で示す様式に従って、監査報告書を作成すること。

監査報告書は、監査対象システムに関する脆弱点を網羅した非公開の「詳細版」及び本機構ホームページ公開用の「概要版」を作成すること。

カ　実施スケジュール

契約締結の日から令和２年２月末までとする。

なお、具体的な日程については契約締結後に発注者受注者協議の上、決定するものとする。

キ　その他

(ア）監査対象部署

監査対象部署は、原則、監査対象システムの所管課とするが、運用管理の実態等に応じて、利用課についても監査対象部署とすることがある。

(イ）情報セキュリティポリシーに関する助言

最新版の「医療情報システムの安全管理に関するガイドライン」等、本機構が遵守すべき法令、ガイドライン等に則り、有効かつ効率的なセキュリティ対策を実施できるよう、本機構の情報セキュリティポリシーが規定されているかについても助言を行うこと。

（２）情報セキュリティ研修

本機構職員を対象に、情報セキュリティ対策の必要性や事故事例、ポリシーの概要等に関する情報セキュリティ研修を実施すること。

ア　実施時間及び回数

実施時間：１回当たり約１時間（質疑応答及びアンケート記入時間等約１０分を含む）

回数　　：合計８回

イ　実施場所及び対象人数（予定）

実施場所	実施回数（予定）	対象人数（予定）
広島市立広島市民病院	３回	２００人/回
広島市立安佐市民病院	２回	２００人/回
広島市立舟入市民病院	２回	７０人/回
広島市立リハビリテーション病院	１回	１００人/回

ウ　実施内容

研修は、各会場とも同一内容とし、原則、次に掲げる項目で構成することとするが、他にも推奨される研修項目がある場合は、本機構と協議の上、決定すること。

（ア）情報セキュリティ対策の必要性

（イ）情報セキュリティ事故の事例（日本年金機構、医療機関の事例を含めること）

（ウ）サイバー攻撃の手口（標的型攻撃メール等）

（エ）最新の情報セキュリティ技術（医療機関の事例を含めること）

（オ）ポリシーの概要等

エ　研修テキスト等の作成

（ア）研修テキスト及び研修アンケートを作成の上、本機構の承認を得ること。

（イ）研修アンケートは、情報セキュリティに対する理解度チェック及び研修についての質問等とすること。

（ウ）研修テキスト及び研修アンケートは、必要部数を印刷し、研修実施日に持参すること。

オ　実施方法

（ア）研修は、集合研修とする。

（イ）研修アンケートは、集計を行い、その結果を本機構に提出すること。

カ　研修用機材等

（ア）講師が研修に使用するパソコン、プロジェクタは、受注者において準備し、スクリーン、マイク及び電源等は本機構が準備する。

（イ）研修会場の設営等に協力すること。

キ　実施スケジュール

契約締結の日から令和２年３月末までの開院日とする。

研修は診療時間外に行うため、研修の開始時刻は１７時～１９時を予定し、各実施場所にお

いて複数回実施する場合は、原則として、別日程とする。
　具体的なスケジュールについては契約締結後に発注者受注者協議の上、決定するものとする。

ク　その他
　集合研修に参加できない職員が、後日、研修内容を学習するため、本機構職員が集合研修時の講義内容のビデオ撮影を行う。撮影した映像及び研修テキスト（以下「研修教材」という。）の取り扱いは、以下のとおりとする。
・　研修教材を本機構の院内ネットワーク上の共有フォルダに保存し、職員が自席の端末を使用して研修教材を閲覧する。
・　研修教材は契約期間内のみ利用することとし、本機構の職員のみが閲覧する。
・　研修教材の複製及び外部への持ち出しを行わないよう、職員に周知徹底する。
・　研修教材の編集・加工・二次利用を行う場合は、事前に本機構と受注者で協議を行う。

6　委託業務実施計画書の作成等
（1）委託業務実施計画書の作成
ア　業務開始に当たり、契約締結日から１０日以内に委託業務実施計画書を作成し、本機構の承認を得ること。
イ　委託業務実施計画書は、別紙で示す様式に従って作成すること。
ウ　委託業務実施計画書を変更する必要があるときは、本機構の承認を得た上で変更し、変更後の委託業務実施計画書を提出すること。
エ　委託業務実施計画書には、後記７に示す業務履行体制（資格、実績等）を確認できる書類を添付すること。

（2）委託業務実施報告書の作成
　すべての業務が完了したときには、委託業務実施報告書を作成し提出すること。

（3）本機構からの資料等の提供
ア　業務の実施に当たり必要となる資料及び電子データを、本機構が妥当と判断する範囲内で提供する。
イ　本機構が提供した資料及び電子データは、業務を実施する目的のためにのみ用いることができる。
ウ　本機構が提供した資料及び電子データは、本機構の許可なく複写又は複製してはならない。
エ　本機構が提供した資料及び電子データは、適切に保管すること。
オ　本機構が提供した資料（本機構の許可を得て複写・複製したものも含む。）は、業務終了後に本機構へ返却すること。
カ　本機構が提供した電子データ（本機構の許可を得て複写・複製したものも含む。）は、業務終了後に消去すること。

（4）成果物の作成
　成果物については、その内容等について本機構と協議の上、作成すること。
　また、成果物の作成に当たって、各課等に対する調査が必要となる場合は、本機構と協議の上、必要に応じて調査票等の資料を作成すること。

（５）議事録等の作成

ア　協議等を行う際は、本機構、受注者とも協議事項を事前に連絡すること。

イ　協議後は、別紙で示す様式に従って議事録を作成し速やかに提出すること。

ウ　協議等において生じた検討課題については、議事録とは別に、別紙で示す様式に従って課題管理表を作成すること。

（６）報告等

受注者は、作業スケジュールに十分配慮した上で業務に当たることとし、本機構と密接に連絡を行い、適宜業務の進捗状況を報告すること。

7　業務履行体制

（１）情報セキュリティ監査の実施に当たっては、監査責任者、監査人、監査補助者等で構成する監査チームを編成すること。

（２）監査責任者及び監査人は、次に掲げるいずれかの資格を有する者とする。

ア　システム監査技術者

イ　公認情報システム監査人（ＣＩＳＡ）

ウ　公認システム監査人

エ　ＩＳＭＳ主任審査員

オ　ＩＳＭＳ審査員

カ　公認情報セキュリティ主任監査人

キ　公認情報セキュリティ監査人

（３）監査チームには、監査の効率と品質の保持のため、病床数２００以上の医療機関における次のいずれかの実績（実務経験）を有する者を１人以上含むこと。

ア　情報セキュリティ監査

イ　情報セキュリティに関するコンサルティング

ウ　情報セキュリティポリシーの作成に関するコンサルティング（支援を含む。）

（４）監査チームの構成員は、監査対象となる情報システムの企画、開発、運用、保守等に関わっていない者とする。

（５）監査チームの構成員には、外部人材を含めないこと。

（６）情報セキュリティ研修の講師は、前記（２）に掲げるいずれかの資格を有する者で、平成２５年４月以降、国、地方公共団体又は企業（自社を除く。）において情報セキュリティに関する研修等の講師を務めた経験を有する者とすること。

講師の人選（外部有識者の招聘も可とする。）については、本機構と協議の上、決定すること。

8　情報セキュリティ対策

（１）業務の実施に当たっては、ポリシーに定める事項を遵守すること。

（2）成果物の作成に当たっては、コンピュータウィルス対策など十分なセキュリティ対策が施された環境で行うこと。

（3）業務の従事者が本機構の施設内で業務を実施するときは、名前札や身分証明書を着用させること。

（4）本機構は、受注者に対し、本機構の情報の保護管理に関する実施状況を調査し、又は報告を求めることができるものとする。

9　提出物及び成果物等

（1）提出物、成果物の作成及び納品期限

本機構に提出する、委託業務実施計画書、委託業務実施報告書、議事録（以下「提出物」という。）のほか、業務の成果物として下表の物を提出すること。

なお、成果物は、本機構と協議の上、分割又は統合して提出することも可とする。

成果物の名称		納品期限
情報セキュリティ監査		
	監査実施計画書	監査日程等の決定後１０日以内
	監査チェックリスト	監査日程等の決定後２０日以内
	監査調書	各監査対象システムの監査終了後１０日以内
	意見交換会議事録	意見交換会の終了後５日以内
	監査報告書（概要版・詳細版）	意見交換会終了後１０日以内
情報セキュリティ研修		
	研修テキスト	研修実施日２０日前
	研修アンケート	研修実施日２０日前
	研修アンケート集計結果	研修終了後１４日以内

（2）提出物、成果物の形態、部数等

ア　使用言語

提出物及び成果物は、日本語で表記すること。

イ　部数

提出物及び成果物は、紙（成果物については、ホチキス留め等の簡易製本を行うこと。）及び電子データをそれぞれ2部提出すること。

ウ　紙の形態

提出物及び成果物は、原則としてＡ４用紙とするが、やむを得ない場合はＡ３用紙も可とする。ただし、Ａ３用紙を使用する場合は、必ずＡ４用紙と同じ大きさでかつ見開きしやすいよう、折りたたむこと。

エ　電子データの形式

提出物及び成果物は、Ｗｏｒｄ、Ｅｘｃｅｌ又はＰｏｗｅｒＰｏｉｎｔのいずれかの形式で加工可能な電子データにて提出すること。

なお、研修テキストはＰｏｗｅｒＰｏｉｎｔとする。

オ　記録媒体

電子データは、ＣＤ－Ｒ等本機構が指定する記録媒体にて提出すること。

（3）著作権の帰属

提出物、成果物及びこれらに付随する資料の著作権（第２７条及び第２８条の権利を含む。）は、すべて本機構に帰属するものとし、書面による本機構の承諾を受けないで他に公表、譲渡、貸与又は使用してはならない。ただし、受注者が従前から保有する著作権は受注者に留保されるものとし、本機構は、業務の目的の範囲内で自由に利用できるものとする。

10 その他

業務の実施に当たり、本仕様書に疑義が生じたとき、又は、本仕様書に記載のない事項については、本機構と協議の上、決定すること。