電力広域的運営推進機関
情報セキュリティ監査業務委託
企画競争仕様書

電力広域的運営推進機関

2019 年 10 月

1　目的

電力広域的運営推進機関（以下、「本機関」という。）の各情報システムにおいて適切な情報セキュリティの管理又は対策が実施されているかについて、第三者の立場から確認及び必要な助言を行い、本機関における情報セキュリティを維持向上させることを目的とする。

2　基本方針

本業務における情報セキュリティ監査は、本機関の重要情報システムに係るセキュリティ対策強化のための体制・制度が機能しているかの検証による監査（以下「**A.マネジメント監査**」という。）と本機関の情報システムに対する疑似的攻撃による監査（以下「**B.ペネトレーションテスト**」という。）の構成で監査を行うこととする。

受託者について、「**A.マネジメント監査**」と「**B.ペネトレーションテスト**」は、それぞれ独立して契約先候補者を選定することとする。

3　業務委託内容

受託者は、以下に示す情報セキュリティ監査業務を、公正かつ客観的な立場で実施すること。なお、監査は助言型監査とする。

監査業務の実施にあたっては、「政府機関の情報セキュリティ対策のための統一基準（平成 30 年度版）（平成 30 年 7 月 25 日策定）」（以下「政府統一基準」という。）、及び本機関が定める情報セキュリティ関連規程(以下「情報セキュリティ関連規程」という。）の内容に基づいた監査を実施すること。

監査実施の結果、不適合の箇所等があった場合、具体的かつ適切な助言をするとともに、不適合となる明確な事由等がある場合は提示すること。

A.　マネジメント監査

本機関の重要システムの実際の運用が、情報セキュリティ関連規程に準拠しているかの確認を行う。具体的には、関連文書の閲覧、被監査部門からのヒアリング調査を行うほか、必要に応じ、情報セキュリティの技術的対策の実施状況についてシステムの目視、事務所内及びデータセンター（１カ所）の観察等を行う。なお、ヒアリング項目（原案）は、本機関から提示することし、具体的な進め方について提案を募集する。

①　対象となる情報セキュリティ関連規程と情報システム（案）

組織全体に係る規程

- 情報管理規程
- 情報システム管理規程
- 情報セキュリティ対策規程

各システム運用細則に関する規程

- 広域機関システム
- スイッチング支援システム

- OA システム
- セキュリティログ監視システム
- 上記の他、電話システムなど設備・機器等に係る小規模な 5 システム

※上記の規程概要は説明会において公開

② 対象となる被監査部門

上記①の 9 システムごとに主管グループのシステム管理者を設置しているため、それぞれシステムごとに 1～2 時間程度のヒアリング調査を必須とする。

③ 本業務の進め方

契約締結後、2020 年 3 月中旬の成果物の納品・検収までの想定する項目は以下のとおりであるが、具体的な進め方について提案を募集する。

- 予備調査
- 監査実施計画書の作成及び被監査部門への通知
- 監査実施
- 監査報告書作成
- 監査報告会の実施
- 成果物納品及び検収

④ 監査報告会

本機関担当者と監査報告書（案）につき討議を行い、完成した監査報告書及び監査報告書概要版をもって情報システム関係者向け報告会の 1 回を開催する。

⑤ 想定する成果物

- 監査実施計画書
- 被監査部門への監査通知書
- 監査調書（監査項目はシステムごと、基本的に前年度のヒアリング項目を準用）
- 監査報告書及び監査報告書概要版
- その他必要と認めたもの

B. ペネトレーションテスト

以下の前年度の実施概要を参考として、診断内容について提案を募集する。

前年度の実施概要

(1) インターネット経由での診断

ルーター、スイッチ、ファイアウォール、サーバや OS、各種サービス等プラットフォームに対する診断を対象とする。

① 対象となる情報システム

- 広域機関システム
- スイッチング支援システム
- OA システム
- セキュリティログ監視システム
- エレクトロニックバンキングシステム

② 対象となるグローバル IP

グローバル IP 数は説明会において、具体的な IP アドレスは受託者のみに公開する。

③ 診断項目

前年度の実施概要は以下のとおりで、DoS ないし DDoS 攻撃耐性診断は対象外としている。

（ア） インターネット側からの攻撃によるサーバへの侵入可否の検証という観点

- ホスト存在確認
- ポートスキャン
- サービス稼働状況確認(バックドア等不要なサービスの確認含む)
- 脆弱性検出
- サーバ(Web/メール/DNS/Proxy など)のセキュリティ設定上の不備確認
- 認証試行

（イ） 侵入できた場合の管理者権限の昇格可否等の検証という観点

- エクスプロイトコード(攻撃コード)を利用したアクセス権限取得、権限昇格可否等の確認
- 脆弱性を組み合わせた複合的な要因での問題検出
- 踏み台としてほかのサーバを攻撃される可能性確認

(2) オンサイトでの診断

本機関の新豊洲事務所に診断機材を持ち込み、無線 LAN の脆弱性を診断する。

① 対象となる無線 LAN（前年度実績）

- 本機関の新豊洲事務所（1 カ所）
- 無線アクセスポイント数　14 台

② 診断項目

- フロア内の不正アクセスポイント検出、正規アクセスポイントへの侵入可否判定

(3) ペネトレーションテスト実施における留意点

① 実施計画

稼働中のシステムに対する診断を含むこと、また受託者側の対応キャパシティも考慮する必要があることから、受託者と本機関の担当者とで診断内容、診断実施日、時間帯を調整する。

② テスト実施

平日日中帯に実施する。なお、実施中に危険度が高い脆弱性で早急な対応が必要と思われる個所が発見された場合、緊急速報として、発見された脆弱性と推奨する対策を簡単にまとめたものをメールで、診断後翌営業日以内を目標に送信すること。

③ 監査報告書作成

テストの結果を分析し､以下の事項を含む監査報告書を及び監査報告書の概要版を作成する。

④ 監査報告会

本機関担当者と監査報告書（案）につき討議を行い、完成した監査報告書及び監査報告書概要版をもって情報システム関係者向け報告会の 1 回を開催する。

⑤　想定する成果物

- 監査実施計画書
- 監査報告書及び監査報告書概要版
- その他必要と認めたもの

4　期　間

業務の実施期間は、契約締結後、2020 年 3 月 27 日（金）（予定）の成果物の納品・検収の見込みであるが、契約期間として 2020 年 3 月末日を予定（詳細は契約締結時に決定することとする。）

5　企画提案の選考

(1)　選考方法

企画提案の選考にあたり、本機関監査室長が指名する 3 名以上の者をもって構成する選考会議において、(3)の選考基準に従って契約先候補者を選考する。

(2)　予算規模

下記を上限（消費税込）とする。

A. マネジメント監査　：　9,000,000 円

B. ペネトレーションテスト　：　7,000,000 円

なお、最終的な業務内容、契約金額等については、契約先候補者と本機関と調整の上で決定する。

(3)　選考基準

以下の選考基準に従って総合的な評価を行う。なお、企画書等の提出期限後に、必要に応じてヒアリングを実施する場合がある。

①　「企画競争説明書」に記載する応募資格を満たしているか。

②　企画提案の内容が本業務の目的に合致しているか。

③　業務の実施方法や実施スケジュールが妥当か。

④　業務の実施方法等について、本業務の成果を高めつつ、合理的･効率的な提案となっているか。

⑤　本業務に係る知見・経験を有しているか。

⑥　本業務を遂行するため必要十分な実施体制をとっているか。

⑦　本業務の作業内容に照らして合理的・効率的に工数が算出されているか。

⑧　その他必要な項目

(4)　契約先候補者の決定

上記の選考の結果、「A.マネジメント監査」と「B.ペネトレーションテスト」は、それぞれ独立して契約先候補者を選定し、企画書等を提出した企画競争参加者に通知する。なお、契約先候補者の決定後、契約先候補者の提出した企画書等の内容について、実施しようとする業務の趣旨に合致するよう、契約先候補者と協議を行い、修正する場合がある。その場合、企画に係る見積額に変更が生じるときは、見積書等の再提出を依頼することがある。

6　秘密情報の保護

本委託業務に関連して開示する機関の秘密情報の適正な情報管理を維持するため、本機関の情報セキュリティ関連規程を遵守し、情報セキュリティを確保するものとする。特に下記の点に留意すること。

(1) 本委託業務の開始時に、業務に係る情報セキュリティ対策の遵守方法及び管理体制について、本機関担当者に書面で提出すること。

(2) 本機関から秘密情報を提供された場合には、当該情報の機密性の格付けに応じて適切に取り扱われるための措置を講ずること。

(3) 本機関の情報セキュリティ関連規程の履行が不十分と見なされるとき又は受託者において委託業務に係る情報セキュリティ事故が発生したときは、必要に応じて本機関の行う情報セキュリティ監査を受け入れること。

(4) 本機関から提供された秘密情報が業務終了等により不要になった場合には、確実に返却し又は廃棄すること。

(5) 再委託することとなる場合は、再委託先にも上記と同様の制限を課して契約すること。

7　その他

(1) 本業務のペネトレーションテストに必要な診断機器、診断ツール類、設定費用、インターネット回線通信費等は本契約に含めるものとする。

(2) 本業務の本機関担当者との討議、被監査部門のインタビュー及びオンサイト診断は、本機関の新豊洲事務所で実施し、その他作業に必要な作業場所や作業端末等は受託者にて確保するものとする。

(3) 本仕様書に記載の事項は、本企画競争のために限り使用することとし、目的外使用や第三者への漏えいをしないこと。

(4) この仕様書に定めのない事項について必要のある時は、委託者と受託者が都度協議し、決定するものとする。

以　上