第１号議案

情報セキュリティ監査業務委託の実施について（案）

2019 年度情報セキュリティ対策推進計画に基づき実施する情報セキュリティ監査について監査業務を外部に委託する。

１．業務の目的

本機関の情報システムにつ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、第三者である専門家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．調　達

（１）対象

A.　重要システムに係るマネジメント監査（以下「マネジメント監査」という。）
　　重要システムにおける情報セキュリティ施策等の運用状況を監査する。

B.　ペネトレーションテスト
　　疑似攻撃等によりネットワークの脆弱性を監査する。

なお、「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、企画提案を受け付けて契約先候補者を決定する。

（２）調達方式

会計規程第２２条第１項第４号による企画競争とする。

（３）調達スケジュール（予定）

2019 年 10 月 9 日（水）	公告（本理事会後速やかに実施）
2019 年 10 月 16 日（水）	説明会
2019 年 10 月 21 日（月）	企画競争に関する問合せ締切
2019 年 10 月 24 日（木）	問合せに対する回答公表
2019 年 10 月 31 日（木）	企画書等提出締切
2019 年 11 月 13 日（水）	契約先候補者決定

（４）詳細仕様

別紙２　企画競争仕様書のとおり。

３．契約先候補者の決定

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より、契約先候補者を選考し、その決定及び契約の締結について、別途、理事会で議決する。

４．企画競争とする理由

昨今、情報システムに対するサイバー攻撃は増加かつ巧妙化しているなかで、情報セキ

ュリティ監査につき、 IPA（独立行政法人情報処理推進機構）の情報セキュリティサービス基準適合サービスリストにて公開されているサービスも多様化しており、最新の動向に関する専門的な知見が必要である。

また、近年の情報セキュリティ監査業界の要員不足等により、本機関で定めた入札仕様では対応できずに応札者が少なくなり、入札が困難になる可能性がある。そのため公平かつ競争性がある調達のため、応募者の専門的な知見・経験に基づく創意工夫のある企画提案を受ける企画競争によることとする。

【参　考】

会計規程

（随意契約）

第２２条　本機関の契約が次の各号の一に該当する場合には、前２条の規定にかかわらず、随意契約の方法によることができる。

（１）　契約の性質又は目的が競争入札を許さないとき。

（２）　緊急の必要により競争入札に付する時間がないとき。

（３）　競争入札に付することが不利と認められるとき。

（４）　企画競争によって契約先候補者を選定したとき。

（５）　公募(入札可能性調査）を行った結果、応募者が単独であるとき。

（６）　前各号に規定する場合のほか、予定価格が少額のとき又はその他本機関の事業運営上特に必要があるとき。

【添付資料】

別紙１　企画競争説明書

別紙２　企画競争仕様書

以　上

別紙 1

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
企画競争説明書

電力広域的運営推進機関

2019 年 10 月

1　業務名

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

A.マネジメント監査

B.ペネトレーションテスト

2　調達方式

企画競争方式で行う。

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。企画競争参加者は、下記のいずれか又は両方の企画書・見積書等を提出することとし、本機関において、公正な基準及び方法により、契約先候補者を選考する。

A.マネジメント監査

B.ペネトレーションテスト

3　参加方法

3.1　参加資格

(1)　平成 31・32・33 年度又は令和元・2・3 年度の競争参加資格（全省庁統一資格）の「役務の提供等」において、C等級以上に格付けされており、関東・甲信越地域の資格を有する者であること。

(2)　説明会に参加した者であること。

(3)　各省各庁から指名停止又は一般競争入札資格停止若しくは営業停止を受けていない者であること。

(4)　予算決算及び会計令(昭和 22 年勅令第 165 号)第 70 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

(5)　予算決算及び会計令第 71 条の規定に該当しない者であること。

(6)　会社更生法（平成 14 年法律第 154 号）に基づく更生手続開始の申立て又は民事再生法（平成 11 年法律第 225 号）に基づく再生手続開始の申立てがなされている者でないこと（但し、会社更生法に基づく更生手続開始の申立て又は民事再生法に基づく再生手続開始の申立てがなされている者で、手続開始の決定後、競争参加資格の再認定を受けている者を除く。）。

(7)　自己、自社若しくはその役員等（注 1）が、暴力団員による不当な行為の防止等に関する法律第 2 条に定める暴力団、暴力団員又はその他反社会的勢力（注 2）でない者であること。

（注 1）取締役、監査役、執行役、支店長、理事等、その他経営に実質的に関与している者。

（注 2）暴力団準構成員、総会屋等、社会運動等標ぼうゴロ又は特殊知能暴力集団、暴力団又は暴力団員と社会的に非難されるべき関係を有する者、暴力団員でなくなった時から 5 年を経過しない者等、その他これに準じる者。

(8)　破壊活動防止法に定めるところの破壊的団体およびその構成員でない者であること。

(9)　平成 30 年度「情報セキュリティ監査企業台帳（2019 年 3 月 8 日版)」又は（独）情報処理推進機構がホームページにおいて公表している「情報セキュリティサービス基準適合サービスリスト」のいずれかに記載されている者であること。

(10) 前年度の情報セキュリティ監査の実績として、官公庁・自治体等に対する助言型監査の実績が 1 件以上あること。

(11) 監査の第三者性を担保するため、本機関の「OA システム」、「スイッチング支援システム」、「広域機関システム」及び「セキュリティログ監視システム」に関わる業務（企画、設計、開発、構築、運用、保守又は支援のいずれかに関する業務）の受注者、または受注者の関係事業者及び関係会社等ではないこと。

(12) 監査人のうち 1 名を監査責任者とし、監査責任者は以下の資格のいずれかを保持していること。

（ア） 特定非営利活動法人日本セキュリティ監査協会（JASA）が認定する公認情報セキュリティ主任監査人又は公認情報セキュリティ監査人

（イ） 経済産業大臣が認定するシステム監査技術者

（ウ） 特定非営利活動法人日本システム監査人協会(SAAJ)が認定する公認システム監査人（CSA）

（エ） 情報システムコントロール協会(ISACA)が認定する公認情報システム監査人(CISA)

3.2　説明会の実施

下記日時で説明会を実施する。企画競争の応募を希望する者は参加すること。

日　　時：2019 年 10 月 16 日（水）15 時 30 分～（60 分程度）

場　　所：東京都江東区豊洲 6-2-15 電力広域的運営推進機関

参加資格：上記 3.1 の資格を満たす者

そ の 他：

- 応募を希望する事業者は必ず参加すること(不参加の場合は応募できないものとする)
- 参加人数は各社 2 名までとする
- 受付にて名刺を 1 枚提出すること

3.3　提出方法

2019 年 10 月 31 日（木）15 時必着で以下書類を郵送または持参すること。

(1)　提出書類

- 企画提案書　2 部
  （表紙に「A.マネジメント監査」又は「B.ペネトレーションテスト」を明記すること。両方に提出しようとする場合は、「A.マネジメント監査」と「B.ペネトレーションテスト」を別冊で提出すること。）
- 見積書（別途密封すること）
- 全省庁統一資格 資格審査結果通知書(写)

- 契約書(案)
- 適合証明書
- 上記内容を納めた電子ファイル（PDF 等）を保存した電子媒体（DVD-R）等

(2) 提出先

〒135‐0061

東京都江東区豊洲 6-2-15

電力広域的運営推進機関　総務部経理グループ「情報セキュリティ監査業務委託」

3.4 保証金及び契約保証金

免除

3.5 契約先候補者の決定

予算上限価格の範囲内で、公正な基準及び方法により、「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。なお、その決定後に、実施しようとする業務に合致するため契約先候補者と協議を行うことができるものとし、その協議に基づき仕様等の内容を変更した場合は、再度見積書等を再提出することとする。

3.6 結果の通知

2019 年 11 月 15 日（金）までに、企画競争参加者に対して結果を通知する。

3.7 入札の無効

3.1 に示した参加資格のいずれかを欠く者のした入札、入札までに不渡手形または不渡小切手を出す等、履行能力を認められない者が行った入札、提出資料に虚偽の記載をした者のした入札及び入札に関する条件に違反した場合は無効とする。

4 業務委託期間

契約締結の日から 2020 年 3 月 31 日（火）までを契約期間（案）とする。

5 納入物（予定）

（ア） 監査実施計画書

（イ） 監査通知書

（ウ） 監査調書

（エ） 監査報告書

（オ） 監査報告書概要

（カ） その他必要と認めたもの

6 完了期限(納入物の提出期限)

2020 年 3 月 27 日(金)予定

7　検収条件

納入物の検査合格(納入物の内容が本契約の内容に適合していると判断された場合)をもって、検収とする。

8　支払条件

契約代金は、検収後、翌月末日までに支払うものとする。

9　見積条件

- 見積金額には本契約の履行に関して必要な一切の費用を含めること
- 見積書には提案金額の総額および内訳(職位別・作業単位別等のそれぞれの工数がわかるようにすること。）を必ず記載すること
- 見積書には記名押印のうえ提出すること

※尚、必要に応じて見積金額の算定根拠を明示していただく場合があります。

10　秘密保持及び個人情報の保護

本調達に際して知り得た広域機関の業務上、技術上の秘密及び情報（個人に関する情報含む）を目的外使用しないこと。また、第三者に漏えいしないこと。

11　特記事項

（1）　本説明書及び仕様書に記載されている事項について不明な点は、2019 年 10 月 21 日（月）17 時までに下記問い合わせ先へ電子メールで問い合わせることとする。問い合わせへの回答は、2019 年 10 月 24 日（木）までに本機関ウェブサイトの本件公告上に開示する。

問い合わせ先：keiyaku@occto.or.jp

ウェブサイト　：トップ＞調達情報

（2）　本説明書に記載のない事項及び疑義については、協議のうえ決定することとする。

（3）　結果については、契約先候補者との契約締結後、原則として、契約相手方、契約締結日及び契約金額等の契約の概要を公表することとする。

以上

別紙２

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