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
入札仕様書

電力広域的運営推進機関

平成 28 年 9 月

1　目的

電力広域的運営推進機関（以下「本機関」という。）の各組織及び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

本入札における情報セキュリティ監査は、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「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「ペネトレーションテスト」という。）の 2 本立てで監査を行うこととする。

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 28 年度版）（平成 28 年 8 月 31 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。）の内容を理解したうえで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。

3.1　マネジメント監査

3.1.1 政府統一基準と情報セキュリティ関連規程との準拠性に関する監査

情報セキュリティ関連規程が政府統一基準に準拠していることの確認を行う。

3.1.1.1 対象となる情報セキュリティ関連規程

(1)情報管理規程

情報管理体制、情報区分について定めた規程である。

(2)情報セキュリティ対策規程

情報システム全体において具体的なセキュリティ対策について定めた規程である。

(3)OA システムの運用細則に関する規程

役職員が日常業務で利用するメール、ファイルサーバ、イントラネット等を提供する OA システムに関して個別具体的な運用を定めた規程である。

(4)スイッチング支援システムの運用細則に関する規程

本機関の会員に提供しているスイッチング支援システムに関して個別具体的な運用を定めた規程である。

(5)EB システムの運用細則に関する規程

銀行が提供するオンラインバンキングシステムの利用に関して個別具体的な運用を定めた規程である。（１０月以降施行予定）

3.1.2 情報セキュリティ関連規程と被監査部門の運用との準拠性に関する監査

本機関の被監査部門における実際の運用が、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、関連文書の調査、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、事務所内の観察等を行う。

3.1.2.1 対象となる被監査部門

以下の部門ごとに情報管理責任者(計 6 名)を設置しているため、それぞれ 2 時間程度のヒアリング調査は必須とする。

(1)総務部

(2)企画部

(3)計画部

(4)運用部

(5)紛争解決対応室

(6)監査室

3.1.2.2 対象となる情報システム

以下のシステムごとにシステム管理者(兼務があるため計 2 名)を設置しているため、それぞれ 2 時間程度のヒアリング調査は必須とする。

(1)OA システム

(2)スイッチング支援システム

(3)EB システム

3.2　ペネトレーションテスト

3.2.1 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し、SQL インジェクションなどに代表される Web アプリケーション診断は対象外とする。ツールによる診断に加えて、診断の網羅性や精度を向上させるためにセキュリティ有識者による手作業での検査を実施すること。

3.2.1.1 対象となる情報システムとグローバル IP

別紙のとおり。※入札説明会で配布する。

3.2.1.2 診断項目

以下の通りとし、DDoS 攻撃耐性診断は対象外とする。なお、必要に応じて受託者にて診断項目を追加してもかまわない。

(イ)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

(ロ)侵入できた場合の管理者権限の昇格可否の検証という観点

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

3.2.2 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。

3.2.2.1 対象となる無線 LAN

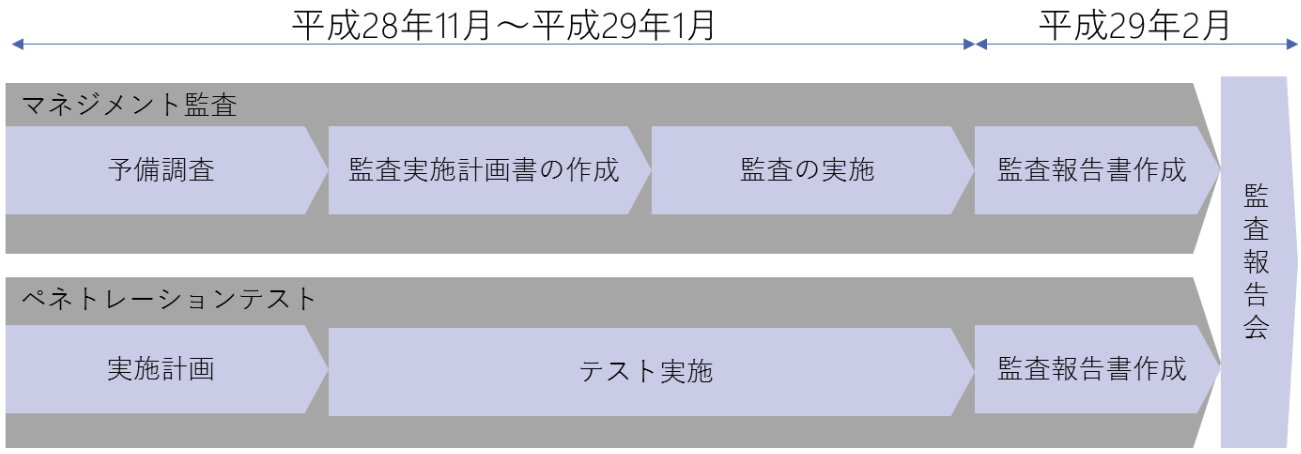
別紙のとおり。※入札説明会で配布する。

3.2.2.2 診断項目

フロア内の不正 AP 検出、正規 AP への侵入可否判定を行う。

4 進め方

「3 業務委託内容」にて記述した業務については、以下図の進め方に従うこととする。



4.1 マネジメント監査

4.1.1 予備調査

以下の通り予備調査を行い、監査計画作成の準備を行う。

(1)政府統一基準、情報セキュリティ関連規程の内容を把握する。

(2)本機関の組織体制やシステム構成等の内容を把握する。

(3)対象システムの概要を把握し、必要により設計書、運用ルール等を把握する。

4.1.2 監査実施計画書の作成

本機関担当者と打ち合わせを行い、以下の項目を含む監査実施計画書を作成する。

(1)監査目的

(2)監査対象

(3)被監査部門、その責任者及び担当者

(4)監査手法

(5)監査の判断の尺度とする基準

(6)監査実施概要

(7)監査実施責任者及び実施担当者の体制

(8)監査実施スケジュール

(9)監査実施場所

(10)その他必要と思われる項目

また、被監査部門に監査の実施内容、スケジュール、準備事項等を事前に通知するため、必要事項を記載した監査通知書を作成する。

4.1.3 監査の実施

監査実施計画書に従い、必要な監査を実施し監査調書を作成する。監査調書には次の項目を含むこと。

(1)件名、作成日、監査責任者名

(2)監査実施日、監査実施場所及び監査項目

(3)被監査部門名及び被監査部門対応者

(4)監査詳細項目、監査資料名、監査手法及び監査結果（課題の有無及び内容）

(5)検出事項とその影響度

(6)所見

4.1.4 監査報告書作成

実施した監査に関する全ての事項について、正確かつ漏れなく必要な事項を整然と分かるように工夫して結果を取りまとめ、以下の事項を含む監査報告書を作成すること。また、監査報告書の概要版も作成すること。

(1)監査実施期間

(2)監査対象範囲

(3)監査の基準

(4)総合的所見

(5)監査意見

(6)不適合となった個所に関する想定されるリスク及び具体的な助言

(7)遵守事項の整備状況の妥当性及び運用状況の準拠性に関する監査を実施した旨及びその結果

4.2　ペネトレーションテスト

4.2.1 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。

4.2.2 テスト実施

マネジメント監査と並行して平日日中帯に実施することとする。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送信すること。緊急速報は診断後翌営業日以内を目標に送信すること。

4.2.3 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作成すること。また、監査報告書の概要版も作成すること。

(1)発見された脆弱性

(2)脆弱性詳細

(3)リスク

(4)具体的な対策案

4.3　監査報告会

本機関の役員向け報告会及び担当者向け報告会の 2 つを開催する。

前者は監査報告書の概要版に基づいて行うこととし、10 分程度にまとめること。

後者の日程は本機関の担当者と調整する。

5　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 本業務について、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、本入札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