電力広域的運営推進機関
2023 年度ペネトレーションテスト業務委託
入札仕様書

電力広域的運営推進機関

2023 年 9 月

1. 目的

ネットワークに接続されているコンピュータに対するサイバー攻撃は増加傾向にあり、その手口が巧妙化している状況において、電力広域的運営推進機関（以下、「本機関」という。）の情報システムにつき、適切なセキュリティ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. 業務委託内容

ネットワークに接続されている本機関の情報システムに対して、最新の技術を駆使して侵入を試みることで、システムにセキュリティ上の脆弱性が存在するかどうかにつき、インターネット経由による脆弱性診断、Web アプリケーション診断及びオンサイトでの無線 LAN の脆弱性診断を行う。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。

(1) インターネット経由による脆弱性診断

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。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専門家による手作業での検査を実施すること。

① 対象となる情報システム

- 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
- セキュリティログ監視システム
- 容量市場システム
- FIT 納付金・交付金管理システム
- 入札システム
- 再エネ業務統合システム
- 財務会計システム
- インターネット HP

② 対象となる IP 数

IP 数　90 個（前年度実績による予定）

※具体的な IP アドレスは受託者のみに公開する。

データセンター利用：４システム

クラウドサービス利用：６システム

③ 診断項目

以下のとおりとし、DoS ないし 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。

(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　等

(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　等

(2) Web アプリケーション診断

① 対象

- 本機関 Web サイト（http://www.occto.or.jp/）

② 診断項目（例）

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。

- ユーザ認証に関する項目
- コンテンツアクセス承認に関わる項目
- クライアントを対象とした攻撃に関する項目
- コマンド実行に関する項目
- 情報取得に関する項目
- アプリケーション機能の悪用に関する項目　等

※「安全なウェブサイトの作り方」（独立行政法人情報処理推進機構）のウェブアプリケーションのセキュリティ実装に記載されている SQL インジェクション、OS コマンド・インジェクション やクロスサイト・スクリプティング 等の 11 種類の脆弱性を参照のこと。

(3) 無線 LAN の脆弱性診断

本機関事務所に診断機材を持ち込み、不正 AP 検出及び正規 AP への侵入可否判定により無線 LAN の脆弱性を診断する。

① 対象となる無線 LAN（前年度実績）

- 新豊洲事務所（新豊洲駅直結・フロア面積 2,615 ㎡）…無線 AP 数 8AP
- 第 2 事務所（東京駅直結・フロア面積 842.58 ㎡）…無線 AP 数 8AP

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。

3. 業務実施期間（予定）

業務実施期間は、契約締結後、2024 年 2 月 28 日（水）（予定）までの成果物納品の見込みで、契約期間として 2024 年 2 月末日を予定（詳細は契約締結時に決定することとする。）

4. 本業務の進め方

(1) 実施計画

契約締結から納品期日までの期間で、受託者により最適なスケジュールを提案し、本機関担当者と合意すること。

特に、受託者側の対応キャパシティを考慮する必要があることから、受託者と本機関担当者とで診断内容、診断実施日、時間帯を調整すること。

(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。

(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) 監査報告会

本機関の情報システム関係者向け報告会の 1 回を開催する。

5. 納入物（予定）

下記の予定する納入物は、編集可能なファイル形式（ワード、エクセル等）で作成し、電子媒体（DVD-R）及び印刷物 1 部により提出する。

- 監査実施計画書
- （被監査部署宛て）監査通知書
- 監査報告書（指摘事項一覧を含む）
- 監査報告書（概要版）
- その他本業務において作成した資料のうち必要と認めたもの

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) 再委託は原則として禁止とするが、もしも業務遂行上、再委託が必要となる場合は、本機関の定める再委託申請書に基づき、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) 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) 本業務に関する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