電力広域的運営推進機関
ペネトレーションテストによる情報システムの
セキュリティ診断
入札仕様書

電力広域的運営推進機関

平成 27 年 12 月

1　概要

1.1　目的

本仕様書は、電力広域的運営推進機関（以下、「広域機関」）の情報システムに対して、情報セキュリティ確保の観点からペネトレーションテストによるセキュリティ診断を実施し、情報セキュリティ対策の状況を把握することを目的とする。

1.2　基本方針

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、侵入できた場合の管理者権限の昇格可否の検証を基本方針とする。

2　診断対象

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。

対象となるグローバル IP 数 ： 別紙のとおり※入札説明会に参加した者に対してのみ公開する

3　業務委託内容

受託者は以下に従いセキュリティ診断を実施すること。

3.1　診断計画

① 一部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、受託者と広域機関とで診断内容をすり合わせし、IP アドレスごとに診断実施日と時間帯を調整する。

3.2　診断実施

① 診断は 2 月の初旬から 2 月 23 日(火)の平日日中帯のいずれかで実施すること。なお、2 月 22 日(月)および 2 月 23 日(火)の 2 日間のみ診断可能な IP アドレスがある。

② インターネット側からリモートで診断を実施すること。オンサイト診断は実施しない。

③ 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。

④ 主な診断項目は以下の通り。なお、大量にパケットを送り付けてシステムの耐性を確認する

DoS 攻撃診断は対象外とする。

(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

3.3 (必要に応じて)緊急速報の提出

① 診断中に危険度が高い脆弱性で早急な対応が必要な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。

② 緊急速報は診断後翌営業日以内を目標に送信すること。

3.4 診断結果報告書の作成と提出

① 診断結果を分析し、診断結果報告書の取りまとめを行う。

② 診断結果報告書には「発見された脆弱性、脆弱性詳細、リスク、具体的な対策案」を記載すること。

③ 診断結果報告書は診断完了後 1、2 週間以内を目標にメールにて提出すること。結果報告会は不要とする。

3.5 診断結果に対する問い合わせ対応

① 診断結果報告書に対して、広域機関から内容の確認等、問い合わせをすることがある。そのため、診断結果報告書を送付してから 1 か月以上、問い合わせ対応期間を設けること。

② 問い合わせは、電話もしくはメールでの対応とする。

4 その他

① 本業務に必要な診断機器、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、診断に必要な作業場所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