仕様書

1　業務の目的、対象及び実施期間

(1) 目的

インターネットサービスを行っているサーバ等に対して内部セグメント側からの擬似的な攻撃等による検査を実施し、セキュリティホールの有無を診断するとともに必要な対策を検討・提示する。

(2) 対象

委託者が管理している図書館システムのDMZ上のサーバとする。

（実施対象IPアドレスを指定し、年間2 IPアドレス・オンサイト実施とする。）

No.	診断対象機器
1	Web蔵書検索用サーバ
2	Mail/DNS履歴管理サーバ

(3) 診断対象サーバの場所

データセンター（浜松市内）

(4) 実施期間

本業務の実施期間は、概ね次に示すとおりとするが、委託者と受託者で調整のうえ日程を定めることとする。

業務項目	9月	10月	11月	12月	1月	2月	3月
セキュリティ診断	▲ 日程調整 診断内容確認	▲ セキュリティ診断	▲ 診断報告		▲ 再診断	▲ 再診断報告	

2　実施項目

以下のとおり、セキュリティホール検査、検査結果の分析・評価、対策方法検討・提示を行うこと。

(1) セキュリティホール検査

ア　受託者が保有する検査ツールを用い、内部セグメント側から検査を行う。

イ　受託者は検査の開始前、終了後には委託者の担当者へ開始、終了の旨を連絡することとする。

(2) 検査結果の分析・評価

ア　実施した試験項目に対して脆弱性の有無、その程度及びサービスへの影響について分析を行う。

イ　発見された脆弱点について関連情報を収集する。

ウ　検査結果に対する評価を行う。

(3) 対策方法検討・提示

ア　発見された脆弱点の改善方法、対処方法の検討を行い、委託者に提案する。

イ　対処方法について即時に実施できない場合の暫定的な対応方法があるときは、その方法も委託者

に提案する。

３　業務着手時の届出

受託者は、本業務着手時に次の通知書等を委託者に提出することとする。

(1) 技術者の選任通知（任意様式）
　受託業務を担当する技術者全員の氏名、経験業務種別（ソフトウェア開発 SE、ネットワーク運用管理等）及び経験年数等を記載する。また、検査を実施する技術者においては、「６　業務実施内容」の(1)クに示す保有資格も明示すること。

(2) 業務実施計画表（任意様式）
　「２　実施項目」に示す各業務について、概略工程及び詳細工程を記載する。なお、契約書第７条第１号に定める「業務予定表」に同様の内容が記載されている場合、本計画表の提出は省略できる。

４　成果品

(1) 本業務の成果品として、「セキュリティ診断検査結果報告書（任意様式）」を提出すること。詳細は次のとおりとする。

ア　媒体及び数量
　データファイル（DVD または CD-ROM）、印刷出力各１式

イ　内容
　以下に示す項目とする。
(ｱ) 検査概要
(ｲ) 検査対象サーバ（名称、IP アドレス）
(ｳ) 検査結果及び総合評価
(ｴ) 検査結果詳細（分析結果）
(ｵ) 対策方法

(2) 報告書・成果品等納品形式

ア　受託者が委託者に対して提出する報告書、ドキュメント類の体裁は、原則としてＡ４判縦又は横とし、文字方向は横書きとする。見やすさに配慮し、適宜Ａ３判を用いてもよいが、Ａ４サイズに折り込んで製本することとする。

イ　受託者が委託者に対して提出する報告書、ドキュメント類のうち、データファイルで提出するものについては、テキスト形式又は Word、Excel、PowerPoint 等の MS-Office で利用可能な形式で作成するものとする。

ウ　本業務の成果品には次の各項目を表記することとする。
(ｱ) 受託業務名
(ｲ) 成果品品目名
(ｳ) 成果品納入年月
(ｴ) 版数（1.0 版 など）
(ｵ) 「著作権者：浜松市」の表記

５　業務実施形態

受託者は、セキュリティ検査実施中に検査対象サーバ及びその他のサーバとこれらが提供しているサービスに影響を及ぼすことのないよう十分に注意して行うこと。また、影響が認められた場合において、実

施中の検査を中断できる体制を確保すること。

６　業務実施内容

(1) 下記の内容を網羅した、セキュリティホール検査を実施することとする。

ア　TCP フルポートスキャンを実施すること。

イ　検出したオープンポートに対してはバナー情報の取得を実施すること。

ウ　Web蔵書検索用サーバにおいて外部にWebサービスを提供するために開放している全ポートに対し、システムの情報が取得できるページが存在していないかを検査すること。(システムに不要なコンテンツや、公開されている Web ページ以外のリンクが存在していないページを含む)

エ　取得したバナー情報を元に影響のあるセキュリティホールについて机上調査を行い、最新のセキュリティホールを報告すること。

オ　市販のセキュリティ検査ツール（Nessus と同等品）を用いて検査を実施すること。

カ　市販のセキュリティ検査ツールを用いた検査だけでなく、以下の検査作業を行うことで、検査範囲／精度の向上を行うこと。
(ｱ) ネットワーク系コマンド等による検査
(ｲ) 各種スクリプト等による検査
(ｳ) 独自ツールによる検査
(ｴ) 実際の攻撃コードを送信し、疑似攻撃では確認できない脆弱性を検査すること。
(ｵ) セキュリティ専門技術者の手作業による検査・分析等

キ　検査ツールによる結果は必ず専門技術者による手動アクセス等で確認し、誤検知を除外すること。

ク　各工程において、「情報処理安全確保支援士（登録セキスペ)」(国家資格）の資格を保有する者が最低１名従事すること。

(2) セキュリティホール検査項目については、25,000 項目以上とし、かつ下記のセキュリティホール検査項目を網羅すること。

ア　電子メール検査
　電子メールサービスのセキュリティホール、アカウント取得の可否、メールを不正に中継できるかどうか等についての検査

イ　DNS 検査
　DNS のセキュリティホールや、バージョン返却の有無、ゾーン情報の転送を無制限に行っていないか等についての検査

ウ　WWW 検査
　WWW サービスのセキュリティホール、脆弱性のある CGI／モジュールが含まれていないか等についての検査

エ　FTP 検査
　FTP サービスのセキュリティホール、Anonymous、FTP サーバの設定不備等についての検査

オ　NFS 検査
　NFS により共有されているディレクトリがないか等についての検査

カ　RPC 検査

RPC プログラムが動作していないか等についての検査

キ　SNMP 検査
SNMP のセキュリティホールや、情報取得の可否等についての検査

ク　OS 検査
OS の脆弱性、設定不備等についての検査

ケ　バックドア検査
不正利用される裏口（バックドア）がないかどうかについての検査

コ　アカウント検査
脆弱なアカウント／パスワードが設定されていないかどうかについての検査

サ　Expoit 検査
Expoit コードを送信し、shell を取得可能かについての検査

シ　強制ブラウジング検査
公開エリアのファイルやディレクトリが閲覧可能かについての検査

(3) セキュリティ診断検査の結果レポートは、下記の項目に基づき作成すること。

ア　セキュリティ診断終了後、脆弱性の脅威とその対策案をまとめた資料（報告書）を作成すること。専門的な知識がない場合でも理解しやすいように工夫した資料（報告書）も作成すること。

イ　セキュリティホールの危険度でレベルが分類され、優先度が容易に判断できる様にすること。

ウ　グラフ等を使用した統計情報を記載すること。

エ　対策方法はコマンドラインレベルで詳細に記載すること。

オ　報告する脆弱性は、それが脆弱性であると判断した根拠データ（通信ログ等）を報告書に記載すること。

カ　解析中、危険度の高いセキュリティホールが判明した場合、先行して脅威の概要と対策案を速報として報告すること。

キ　報告書記載の内容については、報告会後１か月間、メールや電話によるサポートを行うこと。

7　会議

(1) 主催
浜松市立中央図書館とする。

(2) 開催時期
原則として、セキュリティ診断結果報告会、再診断結果報告会の 2 回開催とするが、委託者と受託者の協議を必要とする事項が発生した場合は、委託者又は受託者から相手に申し出て臨時の会議を開催できるものとする。また、セキュリティ診断において、脅威が検出されなかった場合等、委託者が会議を行う必要が無いと判断した場合は開催せず、書面による報告をもって報告会が完了したものとみなすことができる。

(3) 開催場所
原則として、浜松市立中央図書館又は中央図書館関係施設とする。ただし、委託者と受託者の双方の合意によりリモート会議システム等を利用する場合はこの限りではない。

(4) 開催目的
セキュリティ診断業務の報告を行い、必要な対策を検討・提示する。

(5) 出席対象
原則として、委託業務実施担当者、受託者の業務責任者及び技術者の代表者とする。(図書館システム構築・保守業者も出席し、3者で実施する)

(6) その他
報告する際は、セキュリティに関する専門的な知識がなくても理解しやすいように工夫し、報告すること。

８　受託者の選任技術者の交替

委託者は、受託者が「３　業務着手時の届出」(1)に基づき選任した本業務の担当技術者について、本業務を遂行する上で不適切と判断した場合は、書面をもって受託者に当該技術者の交替を要請することができるものとする。

９　問題・課題処理等

業務実施期間中に発生した問題・課題・質問等の処理は、次により実施することとする。

(1) 委託者受託者間での連絡は文書またはE-Mailをもって行うこととする。ただし、緊急の場合はこの限りではない。

(2) 必要に応じて管理番号等を付与し、これを管理することとする。

１０　疑義

契約書及び仕様書等に記載されていない事項及び疑義が生じた場合は、委託者と受託者とが協議して定めるものとする。