

件名：農林水産省本省行政情報システムセキュリティ診断等業務

※ 別添の仕様書は、当該業務における仕様内容の主要な部分を抜粋したものであり、入札にあたっては、必ず別途配布している入札説明書をご確認のうえ、必要な手続きを行っていただくようお願いします。

農林水産省本省行政情報システムセキュリティ診断等業務仕様書

1 目的

本業務の目的は、農林水産省ローカルエリアネットワークの農林水産省本省行政情報システム（以下「本省LANシステム」という。）及びLANパソコン磁気ディスクの情報セキュリティ確保の観点から、セキュリティ診断を実施し、本省LANシステム等における情報セキュリティ対策の状況を把握するものとする。

2 診断対象システム等及び診断実施場所

(1) 診断対象システム等

ア 本省LANシステム

イ 農林水産省大臣官房評価改善課担当者（以下「当省担当者」という。）が指定するパソコン磁気ディスク（1ディスク（200GB相当）。以下「指定磁気ディスク」という。）

(2) 診断実施場所

ア 本省LANシステム

農林水産本省 サーバー室（ドアNo.本152）

イ 指定磁気ディスク

当省担当者から提供する指定磁気ディスクについて、請負者の準備する環境において実施すること。

3 業務内容

(1) 本省LANシステム及び指定磁気ディスクセキュリティ診断計画書の作成

当省が運用・管理する本省LANシステム及び指定磁気ディスクの診断を実施するため、契約締結後速やかに以下の事項を記載したセキュリティ診断計画書を、本省LANシステム、指定磁気ディスク毎に作成すること。

作成に当たっては、具体的な実施方法を立案し、当省担当者と事前に協議を行い承認を得た上で作成すること。

ア セキュリティ診断の目的

イ セキュリティ診断の対象機器

ウ セキュリティ診断の概要

エ セキュリティ診断の実施方法

オ セキュリティ診断の実施時期

カ セキュリティ診断結果の分析方法

キ その他必要な事項

(2) セキュリティ診断の実施

セキュリティ診断計画書に基づき、不正アクセスや外部からの攻撃を未然に防ぐ観点から、不正プログラムの感染経路の推測及び不正プログラムの実行によるファイルやプログラムの改ざん、通信の痕跡、情報の漏えい等にかかる挙動を把握することによりセキュリティ診断を実施すること。

ア 本省LANシステム診断環境

本業務の実施に当たっては、内部セグメントから診断すること。また、ネットワーク環境や運用に影響を与えることなく診断すること。

イ 本省LANシステム診断事項

本省LANシステム診断は、本省LANシステムのコアスイッチ等を通過する全ての通信について、一定期間（最小3日間程度）トラフィックデータを収集・分析し、ネットワーク接続器等の脆弱性等の点検、不正プログラム等に起因する情報漏えいの脅威等を診断すること。

なお、本省LANシステムへ調査・分析のために装置等を設置する必要がある場合は、事前に当省担当者と十分に協議を行った上で実施することとし、本省LANシステムへの影響を最小限に留めるよう、留意すること。

また、装置等の設置に当たっては、請負者の負担で行うこと。

ウ 指定磁気ディスク診断事項

指定磁気ディスク診断は、磁気ディスク内のプログラム全ての命令及びルーチンが意図どおり動作しているか把握すること。

なお、指定磁気ディスク診断に当たっては、作業記録（作業実施日、時間、作業業者氏名等）を以下（3）に定めるセキュリティ診断調書に添付するとともに、不正プログラムの感染経路の推測及び不正プログラムの実行によるファイルやプログラムの改ざん、通信の痕跡、情報の漏えい等にかかる挙動を診断すること。

また、検体（不正プログラム）が発見された場合には、全ての検体のファイル名及び拡張子を明らかにした上で、当省担当者と協議し、解析する検体（1検体）を選定すること。

エ 技術者による手動診断

上記イ及びウの診断は、「6 応札条件」の（3）で示すいずれかの資格を有する者による手動での診断を基本とすること。

オ その他留意事項

診断に際して、本省システムに異常が発生した場合は、その責任を負うとともに、状況や対処方法等について、当省担当者に直ちに報告の上、必要な対処を行うこと。

また、当省担当者と協議の上、当該事案に係る一連の経緯、対処等に加え、原因などについての考察を含めた異常発生報告書を早急に作成し、提出すること。

なお、本省LANシステム診断に当たってサーバー室への入室に際しては、当省担当者の指示に従うこと。

(3) セキュリティ診断調書の作成

セキュリティ診断実施の記録として、以下の事項を記載したセキュリティ診断調書を、本省LANシステム、指定磁気ディスク毎に作成すること。

なお、セキュリティ診断調書には、診断証拠及び関連資料を綴り込むこと。

- ア 表題
- イ セキュリティ診断実施者氏名
- ウ 実施期間
- エ 発見された問題点
- オ 意見
- カ 確認した遵守項目
- キ 確認した対策の内容
- ク サンプルの件数及び抽出方法
- ケ セキュリティ診断方法及び結果
- コ その他必要な事項

(4) セキュリティ診断結果の分析・報告

本診断により把握された欠陥又は脆弱性等が確認された場合は、どのような攻撃を受ける可能性が生じるかを検証するとともに、攻撃に抗する具体的な対処方法の提案及び以下の事項を記載したセキュリティ診断結果報告書を作成すること。

なお、結果の分析方法、報告内容については、事前に当省担当者と協議するとともに、セキュリティ診断結果報告書は、本省LANシステム、指定磁気ディスク毎に文書で整理し当省担当者に報告すること。

- ア 報告書の名称
- イ 報告書の日付
- ウ 報告書の宛先
- エ セキュリティ診断者の署名、又は記名押印
- オ セキュリティ診断実施期間
- カ セキュリティ診断の基準
- キ 総合的所見
- ク 問題に対する対処方法の提案
- ケ 添付資料
- コ その他必要な事項

(5) セキュリティ診断結果の報告

セキュリティ診断調書及びセキュリティ診断結果報告書を提出後、統括情報セキュリティ責任者（大臣官房評価改善課長）及び当省担当者に対して概要を報告すること。

なお、開催日時、報告内容などの詳細については、事前に当省担当者と協議した上で、農林水産省本省内会議室で行うこと。

4 履行期間及び診断報告書等の提出期限

(1) 履行期間

履行期間は、平成24年3月30日（金）までとする。

なお、セキュリティ診断結果の報告については、平成24年3月28日（水）までに実施すること。

(2) 診断報告書等の提出期限及び提出先

請負者は、平成24年3月30日（金）までに下記提出先に診断業務に関するセキュリティ診断結果報告書及び関連資料について、印刷物及び電子ファイルにてそれぞれ一式を提出すること。

【提出先】

農林水産省大臣官房評価改善課情報セキュリティ対策班（本館6階ドアNo.651）

5 作業実施に関する条件

(1) 請負者は、本業務の実施に当たっては、本業務に従事する者の所属、氏名、有する資格、担当する業務の内容・業務実施体制、情報管理体制及び連絡先を明確に示す体制図を記載した書面及び実施スケジュールを、契約締結後5日以内（「行政機関の休日に関する法律」第1条第1項に定める日を除く。）に、当省担当者に提出し承認を得ること。

(2) 請負者は、本業務に関連した資料等（電子データ、電子データを記録した記録媒体・装置、印刷物等の紙媒体を含む。）を持ち帰る必要が生じた場合には、当省担当者へ資料等の名称、使用目的及び数量等を記載した書面を提出し、事前に当省担当者の承認を得ること。また、本業務終了後、速やかに返却すること。

(3) 請負者は、本業務に関連した資料等（電子データ、電子データを記録した記録媒体・装置、印刷物等の紙媒体を含む）を複製し、省外に持ち出す必要が生じた場合には、当省担当者へ資料等の名称、使用目的、複製方法、数量及び使用後の廃棄方法を記載した書面を提出し、事前に当省担当者の承認を得た上で複製すること。

また、複製した資料等については、本業務終了後、速やかに復元又は判読できない方法を用いて確実に廃棄すること。

(4) 請負者は、本業務に関連して入手した資料と業務上知り得た個人情報を含む全ての情報について、本業務の実施中及び終了後においても機密保持のために十分な体制・設備により厳重に管理し、紛失や盗難等による情報漏えいを確実に防止すること。

なお、情報の管理状況の検査に関する事項等を記載した書面を提出すること。

(5) 請負者は、本業務に関連して入手した資料と業務上知り得た個人情報を含む全ての情報については、第三者に開示してはならない。

(6) 請負者は、本業務に関連して入手した資料と業務上知り得た個人情報を含む全ての情報が紛失や盗難等による第三者への情報漏えいの発生又は、そのおそれがある場合は、直ちに当省担当者へ報告すること。

また、直ちに事実調査を行い、漏えいした情報の内容、原因、再発防止策等について記載した書面を提出すること。

(7) 請負者は、本業務の実施に際して、当省関係施設及び敷地内に立ち入る場合、当省及び関係機関が別途定める諸規則等手続きに従い、許可された区域以外へ立ち入らないこと。

また、立ち入りに際しては、常に社員証等の身分証明書を携帯し、ネームプレートや腕章等を着用すること。

(8) 請負者は、本業務に関連して入手した資料と業務上知り得た個人情報を含む全ての情報の取扱いに関しては、本業務に関わる再請負先を含む全ての要員に法令、本仕様書に定める事項等を遵守させるとともに、その指導及び監督を行わなければならない。

(9) 請負者は、最新の脆弱性情報について収集し、検証・調査研究しているチームを内部に常時保有し、業務を行うこと。

6 応札者の条件

応札者は、次に掲げる条件を全て満たしていること。

(1) 財団法人日本情報処理開発協会の情報セキュリティマネジメントシステム (ISMS) 認証基準 (JIS Q 27001:2006 (ISO/IEC 27001:2005)) による ISMS 認証取得事業者、財団法人日本情報処理開発協会のプライバシーマーク使用許諾事業者のいずれかに適合している組織であること。

(2) 過去においてシステムのセキュリティ診断業務に関する業務を請け負った実績があること。

(3) 本業務の従事者には、以下のいずれかの資格を有する者を含めること。

ア 公認情報システムセキュリティプロフェッショナル (CISSP)

イ 日本行政情報セキュリティプロフェッショナル認定資格 (JGISP)

ウ Guidance Software社の認定資格 (EnCase Certified Examiner (EnCE))

エ AccessData社の認定資格 (AccessData Certified Examiner (ACE))

(4) 情報の漏洩等の防止及びセキュリティ確保のため、情報の取り扱い及びセキュリティ

確保に関する体制マニュアル等を備えていること。

7 疑義等の照会

本仕様書について疑義等のある場合、任意様式にて質問書を作成し、提出すること。
なお、質問書に対する回答は適宜行う。