

農林水産省行政情報システム等監視業務仕様書

I 目的

農林水産省行政情報システム（以下「本省LANシステム」という）のサーバー等を外部からの不正アクセスや破壊行為等の攻撃から守るために、24時間365日の有人による監視を実施する。

II 監視対象

監視対象は、バリアセグメント及び下記機器とする。

- 1 ファイアウォール (FortiGate-30B) 2台
- 2 不正アクセス監視機器 (Proventia GX4004V2) 1台
- 3 本省LANシステム監視対象サーバー等群 (別紙1参照)

III 履行期間

平成24年4月1日から平成25年3月31日まで

IV 業務内容

本調達に係る業務遂行に必要な作業及び経費のすべては、本業務に含むものとする。

1 監視業務全般

- (1) 監視により、新たな脅威が発見された場合は、対処方法及び運用方法について、大臣官房統計部管理課情報室（以下「担当部署」という。）及び別途調達する本省LANシステム等運用支援業者（以下「運用支援業者」という。契約締結後、別途提示する。）に、速やかに連絡すること。
- (2) 監視ソフトウェアがバージョンアップした場合は、バージョンアップにより、追加されたルールを新規に追加すること。
- (3) 担当部署及び運用支援業者からの電子メール、電話、FAX等による緊急連絡、質問事項及び相談事項には、速やかに対応すること。
- (4) 有人による監視を24時間365日行うこと。
- (5) 連絡対応は、日本語で行うこと。

2 ファイアウォール監視

インターネット接続用ファイアウォールを対象としたファイアウォール監視を行うこと。

なお、監視内容は以下のとおりである。

(1) 担当部署の指示に従い、監視方法を取り決め、ファイアウォールの監視を行うこと。

(2) 一定時間間隔でファイアウォール機器の死活監視を行うこと。

また、ファイアウォール機器の停止が検出された場合、担当部署及び運用支援業者に速やかに連絡すること。

なお、連絡方法については、別途、担当部署から指示する。

(3) 一定時間間隔及び日次でファイアウォールサービスの起動確認を行うこと。

また、ファイアウォールサービスダウンが検出された場合は、対処方法及び運用方法について担当部署及び運用支援業者に速やかに連絡すること。

(4) 一定時間間隔でファイアウォールのCPU使用率データを収集すること。

(5) 日次でファイアウォールのシステムファイルの改ざん監視を行うこと。

また、改ざんが検出された場合には、担当部署及び運用支援業者に速やかに連絡すること。

(6) ファイアウォールのログを受注者側で管理すること。

なお、ログは最低90日間保管すること。

また、担当部署の要請があった際には、即時に提供ができること。

(7) ネットワーク型侵入検知と連携し、不正アクセスに対する対処を行うこと。

3 ファイアウォール監視報告

ファイアウォール監視に関する以下の(1)～(4)を記載した「監視／侵入検知レポート」を日次作成し、それらを月次ごとに集計したものを報告書として月次報告会で担当部署へ報告すること。

なお、担当部署が必要と認めた場合は、随時、報告会を実施し内容の説明を行うこと。

また、セキュリティレベル向上のため運用上の改善の必要が生じた際には随時提案を行い、担当部署の承認を得た上で改善を行うこと。

(1) ファイアウォール稼動状況、障害通知状況、稼動監視状況、アクセスポリシー変更結果、パッチ状況等の監視状況。

(2) アップダウンチェック、ファイアウォールモジュール動作監視、ファイアウォールポリシーロード監視、ファイアウォール機器のファイル改ざんの監視及びCPU使用率。

- (3) アクセスポリシー変更作業の内容。
- (4) 受信プロトコル利用状況、送信プロトコル利用状況、Dropイベント発生状況、上位内部メール送信先及び上位外部メール送信先。

4 ネットワーク型侵入検知・防御

不正アクセス監視機器、バリアセグメントを対象とした不正アクセスの監視を行うこと。

なお、監視業務内容は以下のとおりである。

- (1) 担当部署と協議し、監視方法（監視点の設定、パケットのロギング、接続の切断、担当部署及び運用支援業者への連絡方法等）を決定し、不正アクセスの監視を行うこと。

- (2) 攻撃の種類単位ごとに詳細にルールを定義すること

- (3) 一定時間間隔で不正アクセス監視機器の死活監視を行うこと。

また、不正アクセス監視機器の停止が検出された場合、対処方法及び運用方法について担当部署及び運用支援業者に、速やかに連絡すること。

- (4) 一定時間間隔及び日次で不正アクセス監視サービス（プロセス）の起動確認を行うこと。

また、不正アクセス監視サービス（プロセス）ダウンが検出された場合は、対処方法及び運用方法について、担当部署及び運用支援業者に速やかに連絡すること。

- (5) 日次で擬似的なアタックを行い、不正アクセス監視機器が正常に動作しているか確認すること。

- (6) 一定時間間隔及び日次で不正アクセス監視機器のディスク使用率の確認を行うこと。

- (7) 一定時間間隔で不正アクセス監視機器のCPU使用率データを収集すること。

- (8) 運用状況に合わせてイベント監視ポリシーのチューニングを行うこと。

- (9) 不正アクセス監視のログを受注者側で管理すること。

なお、ログは最低90日間保管すること。

また、担当部署の要請があった際には、即時に提供ができること。

- (10) ファイアウォール監視と連携し、不正アクセスに対する対処を行うこと。

- (11) 不正アクセス防御装置で利用しているソフトウェアのバージョンアップ又はシグネチャーの追加等があった場合に、追加等されたシグネチャーの内容に応じて、不正アクセスレベル設定、防御設定等について、担当部署に提案を行い、承認を得た上、設定変更作業を行うこと。

5 ネットワーク型侵入検知報告

ネットワーク型侵入検知に関する以下の報告を月次で行うこと。

なお、Webサーバーに対する攻撃があった場合は、攻撃日時、攻撃元、攻撃の種類、攻撃を受けたサーバー名称等の情報を担当部署及び運用支援業者に速やかに報告を行うほか、担当部署が必要と認めた場合、随時、報告会を実施し内容の説明を行うこと。

また、セキュリティレベル向上のため運用上の改善の必要が生じた際には随時、担当部署に提案を行い、承認を得た上で改善を行うこと。

- (1) 不正アクセスに関する通知日時、不正アクセス検出日時、イベント名。
- (2) 検出した不正アクセスに関するイベント名、イベント発生日時、発信先IPアドレス・ポート番号、送信元IPアドレス、プロトコル番号。
- (3) 検出した不正アクセスの傾向。
- (4) アップダウンチェック、不正アクセス監視モジュール動作監視、不正アクセス監視コンフィグレーション管理、ディスク使用率、CPU使用率。
- (5) コンフィグレーション変更作業内容。
- (6) 不正アクセスの影響度合。

なお、不正アクセスの対処方法については、担当部署と協議し決定すること。

6 本省LANシステム監視対象サーバ等群の監視

別紙1の「本省LANシステム監視対象サーバ等群一覧」について、一定時間間隔の監視を行うものとする。

なお、各サーバにおける監視時間間隔においては、別途、担当部署から指示する。

また、サーバの停止等が検出された場合、担当部署及び運用支援業者へ、速やかに連絡すること。

(1) Webサーバ

Ping及びサービスポートの死活監視を行うこと。

なお、本省、水産庁及び林野庁のサイトへの攻撃予告等があった場合は、担当部署から別途指示する。

(2) ノーツ（メール）サーバ

メール送受信の確認を夜間（19:00～翌日9:00）の間に全てのメールサーバで行うこと。

(3) ネットワーク機器及びその他サーバ

Ping及びサービスポートの死活監視を行うこと。

7 オペレータによる監視

監視に当たっては、オペレータによる監視を行い、緊急対応を行う際は、速やかに担当部署及び運用支援業者に連絡し、対処方法（暫定的対処を含む）を示すこと。

8 日別ネットワーク型不正アクセス検知レポート

不正アクセス監視機器へ導入しているネットワーク型不正アクセス検知用ソフトウェアの機能を使用し、攻撃レポートをメールにて翌日午前中までに報告すること。

なお、攻撃レポートにおける対応は以下のとおりとする。

(1) 不正アクセス監視機器で収集した攻撃を集計し、攻撃内容を担当部署へメールによる日次報告をする。

(2) 報告内容はサマリ情報と詳細情報とする。

なお、サマリ情報は、検出された攻撃シグネチャの件数を危険レベル（高、中、低）で表示する。

(3) 詳細情報については検出された攻撃の詳細情報を危険度レベル（高、中、低）ごとに表示するとともに、名称、件数、時刻、送信元アドレス、宛先アドレスとポート、シグネチャごとの付加情報とする。

また、当該機能についてプログラムを開発する必要がある場合は、担当部署と協議し、受注者の責任及び負担で開発を行うこと。

V 機器等導入に関する事項

1 ネットワーク型不正アクセス検知用ソフトウェア、機器類等の運用等については、担当部署の指示に従うこと。

2 本業務に伴い、既存機器類に設定変更が生じる場合は、担当部署と事前に協議を行うこと。

また、既存機器類の設定作業の費用は受注者で負担すること。

3 監視は当省以外のセキュリティが確保されている建屋（監視センター）から監視用として専用線を整備し行うこと。

なお、当省環境に接続するに当たって必要な機材等について受注者が用意し、その場合の費用は受注者で負担すること。

また、接続する際には暗号化、アクセス制御などのセキュリティ対策を実施すること。

4 シグネチャ別の対処方法等の具体的監視内容について提案を行い、担当部署と協議の上、サービス開始時までには不備の無い体制を確立すること。

VI 成果物

成果物として、以下の1～3を納品すること。

なお、本業務において、開発及び改修を行ったソフトウェアが生じた場合は、以下の4～7を納品すること。

- 1 報告書（月次） 1式
- 2 リアルタイム監視サービス体制詳細説明書 1式
- 3 上記1、2を収録した電子媒体 1式
- 4 ソフトウェア設計書 1式
- 5 ソースコード 1式
- 6 操作説明書 1式
- 7 上記4～6を収録した電子媒体 1式

Ⅶ 成果物の納入期限

- 1 「Ⅳ 成果物」の1は、毎月の月次報告会で担当部署へ提出すること。
- 2 「Ⅳ 成果物」の2は契約締結後5日（行政機関の休日（行政機関の休日に関する法律（昭和63年法律第91号）第1条第1項に掲げる日をいう。）を除く。）以内に担当部署へ提出し、承認を得ること。
- 3 「Ⅳ 成果物」の3については本業務完了後、担当部署へ提出すること。
- 4 「Ⅳ 成果物」の4～7はその業務が完了次第、速やかに担当部署へ提出すること。

なお、監視業務において発生した各報告に係る報告書については、業務完了後、当該年度分をファイリングし担当部署へ提出すること。

Ⅷ 成果物の権利帰属

この契約により作成される成果物の著作権等の取扱いは、次に定めるところによる。

- 1 受注者は、著作権法（昭和45年法律第48号）第21条（複製権）、第26条の3（貸与権）、第27条（翻訳権・翻案権等）及び第28条（二次的著作物の利用に関する原作者の権利）に規定する権利を、発注者に無償で譲渡する。
- 2 発注者は、著作権法第20条（同一性保持権）第2項第3号又は第4号に該当しない場合においても、その使用のために当該成果物を改変し、また、任意の著作者名で任意に公表することができるものとする。
- 3 受注者は、発注者の書面による事前の同意を得なければ、著作権法第18条（公表権）及び第19条（氏名表示権）を行使できないものとする。
- 4 第三者が権利を有する著作物（以下「既存著作物」という。）を使用し

て成果物を作成する場合は、発注者が特に使用を指示した場合を除いて、受注者が必要な費用の負担及び使用許諾契約に係る一切の手続きを行うこと。この場合、受注者はその手続きの内容について事前に発注者の承認を得ることとし、発注者は既存著作物についてその許諾要件の範囲内で使用するものとする。

なお、業務の実施に関し、第三者との間に著作権に係る権利侵害の紛争が生じた場合は、その原因が専ら発注者の責めに帰す場合を除き、受注者の責任及び負担において一切を処理すること。この場合、発注者は係る紛争等の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講じるものとする。

- 5 使用する画像、デザイン、表現等に関して他者の著作権を侵害する行為に十分配慮し、これを行わないこと。

IX 知的財産等

- 1 受注者は本契約に関して発注者が開示した情報（公知の情報を除く。以下同じ）及び契約履行課程で生じた納入成果物に関する情報を本契約の目的以外に使用又は第三者に開示若しくは漏えいしてはならないものとし、そのために必要な措置を講ずること。（本件において知り得た事項については外部に漏らさぬこと。）
- 2 本契約履行課程で生じた納入成果物に関しての著作権等の取扱いは、次に定めるところによること。
 - (1) 受注者は著作権法（昭和45年法律第48号）第21条（複製権）、第26条の2（貸与権）、第27条（翻訳権・翻案権等）及び第28条（二次著作物の利用に関する原作者の権利）に規定する権利を発注者に無償で譲渡すること。
 - (2) 発注者は著作権法第20条（同一性保持権）第2項、第3項又は第4項に該当しない場合においても、その使用のために仕様書等で指定する物件（以下「契約目的物」という。）を改変し、また、任意の著作者名で任意に公表することができるものとする。
 - (3) 受注者は発注者の書面による事前の同意を得なければ、著作権法第18条（公表権）及び第19条（氏名表示権）を行使することができないこと。
- 3 納入成果物に第三者が権利を有する著作物（以下「既存著作物」という。）が含まれる場合は、発注者が特に使用を指示した場合を除き、当該著作物の使用に必要な費用の負担及び使用許諾契約に係る一切の手続きを行うこと。この場合、受注者は当該契約等の内容について事前に発注者の承認を

得ることとし、受注者は既存著作物について当該許諾要件の範囲内で使用するものとする。

なお、本仕様に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争の原因が専ら発注者の責めに帰す場合を除き、受注者の責任、負担において一切を処理すること。この場合、発注者は係る紛争等の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講じるものとする。

X 個人情報の扱い

- 1 本業務の作業を派遣労働者に行わせる場合は、労働者派遣契約書に秘密保持義務など個人情報の適正な取扱いに関する事項を明記し、作業実施前に教育を実施し、認識を徹底させること。
- 2 個人情報を複製する際には、事前に担当部署の許可を得ること。なお、複製の実施は必要最小限とし、複製が不要となり次第、その内容が絶対に復元できないように破棄・消去を実施すること。
なお、受注者は廃棄作業が適切に行われた事を確認し、その保証をすること。
- 3 受注者は、本業務を履行する上で個人情報（生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。以下同じ。）の漏えい等安全確保の上で問題となる事案を把握した場合には、直ちに被害拡大の防止等のために必要な措置を講ずるとともに、担当部署に事案が発生した旨、被害状況、復旧等の措置及び本人への対応等について直ちに報告すること。
- 4 個人情報の取扱いにおいて適正な取扱いが行われなかった場合は、本業務の契約解除の措置を受けるものとする。

X I 情報セキュリティの確保

- 1 業務遂行に当たっては、「政府機関の情報セキュリティ対策のための統一管理基準」、「政府機関の情報セキュリティ対策のための統一技術基準」、「農林水産省における情報セキュリティ対策基準」及び別紙2「情報セキュリティに係る遵守事項」について遵守すること。
- 2 本業務を行うに当たって情報管理責任者を明確に定め、責任者の所属、氏名等を記載した管理体制を書面にて提出すること。

なお、情報管理責任者と個人情報取扱責任者が同一の場合には、その旨を記載すること。

3 本業務の受注、施行に当たって知り得た全ての事項については、契約期間中はもとより、契約終了後においても外部に漏らしてはならない。秘密保全に関することは、担当部署の指示に従うこと。

4 本業務の受注、施行に従事する全ての者と個別に退職後も有効な守秘義務契約を締結すること。

5 本業務において知り得た情報の漏えい等の事案が発生した際には、担当部署に電話、口頭等による報告を行うとともに、書面にて提出すること。

なお、事案の発生後は事態の収拾及び拡大防止の措置を迅速かつ適切に行うこと。

また、受注者以外の作業も含め、対処に係る費用は全て受注者が負担すること。

6 受注者環境に本業務に必要な情報以外を保持することのないよう、不要になった情報は適宜、担当部署に返却を行うこと。

7 使用するソフトウェアについては、既知のセキュリティホールに対するセキュリティ対策を行うこと。

X II その他

本仕様書に含めない事項については、担当部署と必要に応じて打ち合わせを行うこと。

X III 疑義等の照会

本仕様書について疑義等のある場合は、「農林水産省行政情報システム監視業務の提案に係る質問書」（様式任意）を作成し担当部署へ提出すること。

なお、質問書に対する回答は適宜行う。

また、本省LANシステムの設計書の閲覧する場合には、本業務の公告期間中に限り、閲覧をする日の3日（行政機関の休日を除く。）前の10:00～17:00の間に担当部署へ連絡し、担当部署が指示する日時及び場所においてのみ可能とする。