仕様書

システム業務部

Ⅰ．件名

2020 年度 NEDO 情報セキュリティ監査業務

Ⅱ．目的

近時、政府機関や重要インフラ関連企業等に対する標的型サイバー攻撃や IoT 機器の脆弱性を悪用した DDoS 攻撃に加え、各種ランサムウェアの被害など、我が国の国民生活・経済活動を脅かす様々な脅威やインシデントが日々増大する傾向にある。

国立研究開発法人 新エネルギー・産業技術総合開発機構（NEDO。以下「機構」という。）では、技術面・制度面・教育面等様々な観点から情報セキュリティ対策の維持・向上に取り組んでいるところであるが、その対策の実効性や適正性等について、適宜評価する必要がある。

このため、機構の各種規程類の準拠性や妥当性、対象システムの情報セキュリティ対策の実施状況、自己点検の設問及び回答の確認、対象システムの脆弱性診断等について、文書査読、ヒアリング、現地調査及びシステムに対する疑似攻撃（ペネトレーションテスト）等も含め各種監査を実施する。

Ⅲ．業務概要

受託者は、以下の業務を実施すること。

１．セキュリティポリシーの準拠性等の監査（上位規程及び下位規程との準拠性監査を含む。）及び機構の各種規程類に対する見直しの提案

２．対象システムの対策実施状況の監査

３．自己点検の設問の準拠性及び回答の適切性の監査

４．プラットフォーム及び Web アプリケーション等の脆弱性診断（ペネトレーションテストを含む。）

Ⅳ．業務内容

受託者は、以下に示すセキュリティ監査業務を公正かつ客観的な立場で実施すること。なお、監査は助言型監査とする。

監査実施の結果、不適合の箇所等があれば、不適合となる明確な事由等を提示するとともに、具体的な改善策を提案すること。

１．情報セキュリティ関係規程の準拠性監査及び NEDO セキュリティポリシーの見直し提案

以下①、②の情報セキュリティ関係規程に係る準拠性監査を実施すること。

①統一基準と NEDO セキュリティポリシーとの準拠性に関する監査

「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」（以下「統

一基準」という。）に対し、機構が定める「情報セキュリティ管理規程」（以下「管理規程」という。）、「情報セキュリティ対策基準」（以下「対策基準」という。）について、準拠性等の監査を実施すること。なお、ここでは、「管理規程」、「対策基準」の2件を「NEDOセキュリティポリシー」という。

また、監査を実施する際は、上記統一基準以外の「政府機関等の情報セキュリティ対策のための統一規範」、「政府機関等の情報セキュリティ対策の運用等に関する指針」、「府省庁対策基準策定のためのガイドライン」を含めた4つの文書（「統一基準群」と総称する。）及びNEDO情報セキュリティ関係規程等の文書を理解したうえで実施すること（別添1参照）。

なお、実施期間中に統一基準及びNEDOセキュリティポリシーが改定される場合は、対象とする版及び監査方法等について機構の担当職員と協議し、担当職員の指示に従うこと。

②NEDOセキュリティポリシーと実施手順等との準拠性に関する監査

NEDOセキュリティポリシーに対する下記実施手順等について、準拠性等の監査を実施すること。なお、実施手順等として、下記規程を対象とする。

・「情報の格付及び取扱制限の基準並びに格付及び取扱制限を明示等する手順に係る機構達」

③NEDOセキュリティポリシーの見直し提案

準拠性監査の結果から、より効果的な構成や体系など、既存のNEDOセキュリティポリシーの見直しについて提案を行う。

２．対象システムの対策実施状況監査

①監査方法

対象とするシステムに対し、実際のシステムの設計や設定、運用ルール等が、NEDOセキュリティポリシー（及びISMS規格）に準拠しているかの監査を実施すること（準拠性、妥当性）。また、NEDOセキュリティポリシーが統一基準（平成30年度版）をもとに作成したものであることを踏まえ、実施期間中に次期統一基準が改定された場合には、最新の統一基準に準拠していない部分ついての追加対策等の提案を行うこと（「４．プラットフォーム及びWebアプリケーション等の脆弱性診断」についても同様）。

なお、実際の運用状況の把握等については、監査対象として必要な部門（以下「被監査部門」という。）からの聞き取り調査に加え、必要に応じ、情報セキュリティの技術的対策の実施状況についてシステムの目視等を行うこと。

②監査対象システム

(a) 「情報基盤サービス」※

(b) 「統合人事システム」

※（a）「情報基盤サービス」は2020年11月に更新予定のシステムであるため、監査の

実施については、安定稼働後の 2021 年 1 月以降の実施とする。

３．自己点検の確認

機構が実施する情報セキュリティ自己点検について、設問の準拠性や役職員からの回答の適正性等の監査を行うこと。具体的な内容は、対象の補足率、設問の規程類への準拠性、回答率の状況や各回答の適正性に加え、必要により、自己点検の実施方法に係る改善方法の提案等を含むものとする。

なお、個別回答の確認等は、回答者全数のサンプリングでも良いが、結果の有意性や代表性等を考慮し分析すること。

４．プラットフォーム及び Web アプリケーション等の脆弱性診断

プラットフォーム及び Web アプリケーション等に対する脆弱性診断を実施すること。

脆弱性診断に係る計画書を作成する場合には、実施日時、実施者、プラットフォーム及び Web アプリケーション等の対象範囲、診断手法、診断項目等を含めること。

結果報告書を作成する場合には、上記計画書の内容を踏まえ、得られた診断結果、予見されるリスクや問題点、具体的な回避策や改善策等を含め、簡潔に結果をまとめること。

なお、診断を実施する場合には、「ツール診断」、「手動診断」を適宜組み合わせ、最適な診断方法とすること。また、現行業務への影響を極力最小化するよう実施方法、実施時間等を考慮し、効率的に診断を実施すること。仮に影響が予見される場合には、予め担当職員に説明し了解を得ること。

仮に、重大な脆弱性が発見された場合は、機構による対処を踏まえ、再度診断を実施すること。再度診断を実施する場合は、実施方法、実施範囲、実施時期等を担当職員と調整すること。

①プラットフォームに対する脆弱性診断

プラットフォーム（サーバ、ネットワーク機器等）に対し、機構外部（インターネット側）及び機構内部またはデータセンター（内部セグメント側）からの探査活動（Portscan、IPscan 等）を含めた疑似攻撃（ペネトレーションテスト等）を行うことにより、対象とするプラットフォームに問題がないか、脆弱性診断を実施すること。

診断対象は「別添２」のシステムとし、診断項目は「別添３」を対象に実施すること。なお、必要に応じ、受託者にて診断項目を変更・追加しても良い。

②Web アプリケーションに対する脆弱性診断

診断対象とする Web アプリケーションに対し、機構外部（インターネット側）及び機構内部またはデータセンター（内部セグメント側）からの疑似攻撃等を実施することにより、脆弱性診断を実施すること。

診断対象は「別添４」の Web アプリケーションとし、診断項目は「別添５」を対象に実施すること。なお、必要に応じ、受託者にて診断項目を変更・追加しても良い。

Ⅴ．監査手順

上記「Ⅳ．業務内容」で記述したセキュリティ監査業務の実施に当たっては、基本的に以下の手順にて監査を進めることとし、関連文書の調査、被監査部門からのヒアリング調査を行うほか、必要に応じ、情報セキュリティの技術的対策の実施状況についてシステムの目視等を行うこと。

また、「Ⅳ．4．プラットフォーム及びWebアプリケーション等の脆弱性診断」についても、下記実施手順等に準じ、適切な計画策定、診断実施、結果報告等を行うこと。

なお、より効率的かつ効果的な実施手順等がある場合は、その実施手順等を担当職員と協議したうえで、実施すること。

１．監査計画書

受託者は、各監査手順の実施日程及び監査の概要等を定めた監査計画書を採択決定後NEDOの指示する日から2週間以内に作成し、担当職員の了承を得ること。

２．予備調査

予備調査として、以下の調査を行うこと。

①統一基準群、NEDOセキュリティポリシー及び実施手順等の内容を把握する。

②機構内（本部、海外事務所等）の組織体制や業務内容、システム構成等の内容を把握する。

③対象システムの概要を把握し、必要により設計書、運用ルール、マニュアルや手順書等を把握する。

④脆弱性診断を実施するにあたり、事前に疎通確認等を行い、状況により監査実施場所や監査方法を適宜提案する。

３．監査手続書

監査手続書を作成し、監査手法の決定、被監査対象の選定、本調査実施スケジュール等の調整を行う。なお、監査手続書には次の項目を含むこと。監査手続書の提出期限は、担当職員と調整し決定すること。

①件名、作成日、監査責任者名

②監査実施予定日、監査実施予定場所及び監査予定項目

③被監査部門名

④監査詳細項目、必要資料名及び監査手法

４．本調査

監査手続書に基づき、必要な監査を実施する。

５．監査調書

監査調書の作成に当たっては、担当職員との協議を行い作成すること。なお、監査調書には次の項目を含むこと。

①件名、作成日、監査責任者名

②監査実施日、監査実施場所及び監査項目
③被監査部門名及び被監査部門対応者
④監査詳細項目、監査資料名、監査手法及び監査結果（課題の有無及び内容）
⑤検出事項とその影響度、改善提言の有無及び内容
⑥所見

６．監査報告書作成及び報告会開催

監査報告書の作成に当たっては、担当職員との協議を行い作成すること。なお、監査報告書には次の項目を含むこと。また、監査報告書を要約した概要版を作成すること。

①監査内容について

監査項目、監査方法及び監査実施状況（被監査部門、監査実施場所、監査実施日及び被監査部門対応者名）

②監査結果について

被監査部門の現状、監査結果の詳細、指摘事項、想定されるリスク及び改善提言

③指摘事項の根拠となる資料

なお、監査報告書の提出に先んじて、NEDO 情報セキュリティ監査責任者及び担当職員等を対象とした報告会を開催すること。報告会の開催時期や内容については、担当職員と調整し実施すること。

Ⅵ．実施期間

NEDO の指定する日から 2021 年 3 月 18 日（木）まで

Ⅶ．予算額

1,450 万円以内（税込）

Ⅷ．納入物品

１．監査計画書	書面正副各 1 部、電子媒体 1 部
２．監査手続書	書面正副各 1 部、電子媒体 1 部
３．監査調書	書面正副各 1 部、電子媒体 1 部
４．監査報告書	書面正副各 1 部、電子媒体 1 部
５．監査報告書概要	書面正副各 1 部、電子媒体 1 部

納入物品のうち、書面は、A4 判又は A3 判（A3 判を用いる場合は、折り込んで A4 判に収まる形態とすること。）とし、電子媒体は、Microsoft Office Professional Plus 2013 でレイアウトの崩れ無く読み取れるよう作成されたファイル、及び当該ファイルを Adobe Acrobat Reader DC で読み取れる形式に変換したファイルを、CD-R 又は DVD-R に格納し納入すること。なお、電子媒体の表面には、件名及び納入年月日を明記したラベルを貼り付けること。

Ⅸ．納入場所

国立研究開発法人 新エネルギー・産業技術総合開発機構 システム業務部

Ⅹ．その他

１．契約期間中及び契約期間終了後において、本業務により知り得た機構の関連文書や対象システムの情報等については、受託者が適切に管理し、いかなる場合においても他者には漏えいしないこと。また、他の目的に使用しないこと。

２.監査の実施に当たっては、あらかじめ監査人を登録し、担当職員の了承を得ること。

３．受託者は、担当職員及び被監査部門の担当者と日本語でコミュニケーションが可能で、かつ、良好な関係が保てること。

４．受託者は、監査の実施者として、事実の認定、影響度の判断、意見の表明等を行う場合は、公正・普遍の態度を保持すること。

５．監査の実施に際し、緊急に対応を要する事項が明らかになったときは、直ちに口頭をもって担当職員に報告し、後日、書面による報告を行うこと。なお、報告に基づく対応については、担当職員の指示に従うこと。

６．監査の実施に際しては、被監査部門に対し、業務の実施手順、システムの運用方法等について直接指揮・命令を行わないこと。

７．監査の実施に際しては、被監査部門の業務に支障を来さないよう十分留意のうえ実施すること。

８．監査責任者は、監査計画に基づく進ちょく状況について常に把握し、担当職員からの問合せに対し、迅速に対応できるようにすること。

９．受託者は、本業務の遂行において、機構の情報セキュリティが侵害され又はその恐れがあると判断される場合には、速やかに担当職員に報告を行い、原因究明及びその対処方法等について担当職員と協議し対処すること。

10．受託者は、情報の受け渡し等について、次の項目を遵守すること。

①受託者は、貸与された紙媒体や電子媒体の取扱いに十分注意を払うとともに、機構内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に担当職員の許可を得ること。

なお、機器の持込みを許可された場合であっても、担当職員の許可なく情報を複製してはならない。また、複製を許可された場合でも、作業終了後には、持ち込んだ機器から複製した情報が電子計算機等から消去されていることを担当職員が確認で

きる方法で証明すること。
②受託者は、貸与された紙媒体や電子媒体を担当職員の許可なく機構外に持ち出し、これを複製してはならない。また、複製を許可された場合でも、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明すること。
③受託者は、本業務を終了又は契約解除する場合には、担当職員から貸与された紙媒体や電子媒体を速やかに担当職員に返却すること。その際、必ず担当職員の確認を受けること。

11. 受託者は、脆弱性診断の実施について、以下の項目を遵守すること。
①受託者は、機構の対象システムのネットワーク構成や運用上の規則・習慣等について、十分理解したうえで、与えられた環境下において診断業務を実施すること。なお、対象システムの運用に影響を与えないよう十分留意すること。
②診断業務に必要な脆弱性診断ツールの調達・導入や、診断業務をかかる通信費等一切の費用は、受託者の負担とする。
③機構内のシステムに装置やソフトウェア等を導入する必要がある場合は、事前に担当職員と協議を行ったうえで実施することとし、機構内のシステムへ与える影響を最小限に留めるよう十分留意すること。
④受託者は、本業務を実施する目的でシステム設定等を変更する場合は、事前に担当職員の了解を得るとともに、設定等を変更した場合は、業務終了後に現状を回復し、担当職員にその報告を行うこと。
⑤診断業務の実施に際し、機構内のシステムに異常の発生又はその恐れがあると判断される場合には、その状況や対処方法等について、速やかに担当職員に報告を行い、必要な対処を行うこと。また、当該事案に至る経緯や原因、対処などの考察も含め報告書を提出すること。

12. 受託者が受託業務の一部を再委託する場合は、再委託者は、受託者と同様、本仕様に記載の情報の取扱等情報セキュリティを遵守することとし、別途提出する体制図に再委託の内容（再委託者名、再委託業務等）を明記すること。

13. 受託者は、業務実施に際して発生した不明な点は、担当職員に確認のうえ、その指示に従うこと。

14. 本仕様書に定める事項については、随時ＮＥＤＯと調整の上実施する。また、本仕様書に定めなき事項については、ＮＥＤＯと実施者が協議の上で決定することとする。

（別添１）

準拠性等監査に関連する文書体系（Ⅳ.１.関係）

【NEDO 情報セキュリティ関係規程等】

	名称
1	情報セキュリティ基本方針
2	情報セキュリティ管理規程
3	情報セキュリティ対策基準
4	情報の格付及び取扱制限の基準並びに格付け及び取扱制限を明示等する手順に係る機構達
5	情報システム運用管理規程
6	情報システムの運用及び管理に関するガイドライン
7	海外事務所における情報セキュリティガイドライン
8	その他マニュアル及び手順書関連

※上記資料は、契約締結後、受託者に提供する。

※上記資料は大凡 150 ページ程度。

【NISC 統一基準群より】

	名称
1	政府機関等の情報セキュリティ対策のための統一規範
2	政府機関等の情報セキュリティ対策の運用等に関する指針
3	政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）
4	政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）

※以下の Web サイトより参照。

https://www.nisc.go.jp/materials/index.html

（別添２）

対策実施状況監査の対象システム概要（Ⅳ.２.関係）

(a) 「情報基盤サービス」

NEDO の役職員が日常業務で使用するシンクライアント PC、IP 電話、スマートフォン、複合機、ネットワーク等のオフィス機器とメールやオフィスソフトから構成される ICT 環境を一括して提供するサービス。

(b) 「統合人事システム」

「統合人事システム」は、人事・給与・勤務・研修等を管理するシステム。

※基本的に、プラットフォームに対する脆弱性診断の対象システムと同一とする（Ⅳ.４.①関係）。

※(a)、(b)の関連文書については、大凡 500 ページ程度。

（別添３）

プラットフォームに対する脆弱性診断項目（Ⅳ.４.①関係）

	診断項目	診断内容
1	ポートスキャン	対象機器で稼働している各ホストのOSや、動作しているサービスについて、ポートの稼動状態にかかる情報を確認する。
2	バナー情報取得	稼動しているポートからバナー情報を収集し、OS種別やサービスのソフトウェア名、バージョン等を特定する。
3	パスワード・認証	各ホストで動作しているサービス等から、システムに登録されているユーザ情報（ユーザID）を収集する。稼動しているサービス情報を基に、ソフトウェアの不備や設定の不備等による情報漏えいの可能性等を確認する。
4	DNSキャッシュポイズニングチェック	DNSサーバ関連ソフトウェアが最新であるか、コンテンツサーバの再帰問い合わせ動作が無効になっているか等、脆弱性の有無を診断する。
5	既知の脆弱性検証	各ホスト上の接続可能なサービスに対し、脆弱性診断ツール等を用い、ホスト上の脆弱性（ソフトウェアの不備、設定の不備、推測可能なパスワード等）の情報を収集する。

（別添４）

脆弱性診断の対象 Web ページ（Web アプリケーション）（Ⅳ.４.②関係）

No	システム名	全体 ページ数	備考
1	NEDO ホームページ	19,100	公開
2	アンケート集計システム	2	公開
3	事前評価者 HP ピアレビュアシステム	25	公開
4	風況マップシステム	10	公開
5	日射量データベース閲覧システム	5	公開
6	洋上風況マップシステム	10	公開
7	成果フォローアップ（追跡調査）Web 化システム	1	公開
8	研究成果管理システム	40	公開
9	ピアレビュアシステム（管理画面）	60	イントラ
10	アンケートシステム（管理画面）	15	イントラ
11	PMS 外部申請システム	1	公開
	合計	19,269	

※ページ数は大凡の数であり、監査実施のタイミングにより増減有り

（別添５）

Web アプリケーションに対する脆弱性診断項目（Ⅳ.４.②関係）

	診断項目	診断内容
1	SQL インジェクション	SQL 文の組み立て方法に問題がある場合、攻撃者によってデータベースの不正利用をまねく可能性があるため、この脆弱性に関する診断を行う。
2	OS コマンド・インジェクション	外部からの攻撃により、ウェブサーバの OS コマンドを不正に実行されてしまう問題がないか診断を行う。
3	ディレクトリ・トラバーサル	ファイル名指定の実装に問題がある場合、ウェブアプリケーションが意図しない処理を行ってしまう可能性があるため、この脆弱性の診断を行う。
4	セッション管理の不備	セッション ID の発行や管理に不備がある場合、利用者になりすましアクセスされてしまう可能性があるため、この脆弱性にかかる診断を行う。
5	クロスサイト・スクリプティング	ウェブページへの出力処理に問題がある場合、そのウェブページにスクリプト等を埋め込まれてしまう等の問題があるため、この脆弱性にかかる診断を行う。
6	クロスサイト・リクエスト・フォージェリ	利用者が意図したリクエストを識別する仕組みを持たないウェブサイトは、悪意のある人が用意した罠により、利用者が予期しない処理を実行させられてしまう可能性があるため、この脆弱性にかかる診断を行う。
7	HTTP ヘッダ・インジェクション	HTTP レスポンスヘッダの出力処理に問題がある場合、攻撃者は、レスポンス内容に任意のヘッダフィールドを追加し、また、複数のレスポンスを作り出すような攻撃を仕掛ける場合があるため、この脆弱性にかかる診断を行う。
8	メールヘッダ・インジェクション	メール送信機能を持つウェブアプリケーションに問題がある場合、管理者が設定した固定のメールアドレスではない宛先にメールを送信され、迷惑メールの送信に悪用される可能性があるため、この脆弱性にかかる診断を行う。
9	クリックジャッキング	細工された外部サイトを閲覧し操作することにより、利用者が誤操作し、意図しない機能を実行させられる可能性があるため、この脆弱性にかかる診断を行う。
10	バッファオーバーフロー	プログラムが入力されたデータを適切に扱わない場合、プログラムが確保したメモリの領域を超えて領域外のメモリを上書きされ、意図しないコードを実行してしまう可能性があるため、この脆弱性にかかる診断を行う。
11	アクセス制御や認可制御の欠落	不適切な設計により生じる、アクセス制御や認可制御等の機能欠落に伴う脆弱性について診断を行う。

12	改行コードインジェクション	Web サーバのレスポンスヘッダやメールヘッダに不正なヘッダの追加・本文の改ざんが可能かどうかを診断する。
13	Cookieの扱い	Cookieの設定項目に対し、その属性や内容について診断する。
14	認証回避	ログイン画面以降のURLに直接アクセスし、認証を回避することが可能かどうかを診断する。
15	SSL 証明書の不備	SSL 証明書を利用している場合、その属性や内容等の適正性にかかる診断を行う。

（注）「安全なウェブサイトの作り方（改訂第 7 版）」（独立行政法人情報処理推進機構）を参考に作成。
https://www.ipa.go.jp/security/vuln/websecurity.html