（別紙）

仕様書

国立研究開発法人新エネルギー・産業技術総合開発機構

Ⅰ．件名

2024 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（以下「NEDO」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、NEDO の各種規程類の準拠性及び情報システムのセキュリティ対策実施状況を確認するため本業務を実施する。

Ⅲ．用語の定義

本仕様書で使用する用語の定義は以下のとおり。

・統一基準群とは、サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 26 条第１項第２号に基づきサイバーセキュリティ戦略本部が定める「政府機関等のサイバーセキュリティ対策のための統一基準群」をいう。
・管理規程とは、NEDO が定める「情報セキュリティ管理規程」をいう。
・対策基準とは、NEDO が定める「情報セキュリティ対策基準」をいう。
・情報セキュリティ関係規程とは、管理規程及び対策基準並びにこれらに基づく実施手順等をいう。

Ⅳ．業務概要

受注者は、以下の業務を実施すること。

１．　情報セキュリティ関係規程の準拠性等の監査（上位規程及び下位規程との準拠性監査を含む。）及び、必要な場合は見直しの提案

Ⅴ．業務内容

受注者は、以下に示す情報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（監査対象の情報セキュリティ上の問題点を指摘した上で、改善提案を行う監査形態）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見直しの提案

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統一基準群と NEDO 情報セキュリティ関係規程との準拠性に関する監査

最新版の統一基準群に対し、NEDO が定める管理規程及び対策基準について、準拠性等の監査を実施すること。

また、統一基準群の改訂（2023 年 7 月 4 日決定）に伴い、情報セキュリティ管理規程・対策基準については 2024 年 3 月 31 日付で管理規程及び対策基準を改訂しているが、政府機関等の対策基準策定のためのガイドライン（2024 年 7 月 24 日一部改定）については未対応であるため、情報セキュリティ関係規程の改訂が必要と思われる箇所があった場合は、改訂案を示すこと。

なお、監査を実施する際は、情報セキュリティ関係規程を理解したうえで実施することとし（別添 1 参照）、具体的な監査方法等については、NEDO 担当職員（以下「担当職員」という。）と協議し、担当職員の指示に従うこと。

②管理規程及び対策基準と実施手順等との準拠性に関する監査

管理規程及び対策基準に対し、実施手順等の準拠性等の監査を実施すること。

なお、以下の実施手順等を対象とする。

・「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」
・外部サービス利用の申請ルール

Ⅵ. 監査手順

「Ⅳ. 業務内容」で記述した情報セキュリティ監査業務の実施にあたっては、基本的に以下の手順にて監査を進めることとし、関連文書の調査及び被監査部門からのヒアリング調査を行うこと。

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. 監査計画書の作成

受注者は、監査全体のスケジュール及び監査の概要等を定めた監査計画書を、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、情報セキュリティ関係規程の内容を把握する。
②NEDO 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. 監査手続書の作成

監査手続書を作成し、監査手法の決定、被監査対象の選定、本調査の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こと。

５．監査調書の作成

監査調書の作成にあたっては、担当職員と協議を行い作成すること。なお、監査調書には以下の項目を含むこと。

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あたっては、担当職員と協議を行い作成すること。なお、監査報告書には以下の項目を含むこと。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、統一基準改訂に伴う情報セキュリティ関係規程の改訂提案等
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 の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。

Ⅶ．履行期間

契約締結日から 2025 年 3 月 14 日（金）まで

Ⅷ．納入物

項番	名称	形式・数量	納入期限
1	監査計画書	書面 1 部、電子媒体 1 部	NEDO の指定する日
2	監査手続書	書面 1 部、電子媒体 1 部	NEDO の指定する日
3	監査調書	書面 1 部、電子媒体 1 部	2025 年 3 月 14 日
4	監査報告書	書面 1 部、電子媒体 1 部	2025 年 3 月 14 日
5	監査報告書概要	書面 1 部、電子媒体 1 部	2025 年 3 月 14 日

納入物のうち、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 Office365 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

〒212-8554
神奈川県川崎市幸区大宮町 1310 番　ミューザ川崎セントラルタワー
国立研究開発法人新エネルギー・産業技術総合開発機構 法務部

Ⅹ．情報管理について

１．情報管理体制

① 受注者は、本業務で知り得た情報を適切に管理するため、次の履行体制を確保し、NEDO に対し「情報取扱者名簿」（氏名、所属部署、役職、国籍等が記載されたもの）及び「情報管理体制図」（情報セキュリティを確保するための体制を定めた書面）を契約前に提出し、NEDO の同意を得ること。また、情報取扱者の個人住所、生年月日、パスポート番号を NEDO から求められた場合は、速やかに提出すること。
なお、情報取扱者は、本業務の遂行のために最低限必要な範囲で設定すること。

（確保すべき履行体制）

契約を履行する一環として受注者が収集、整理、作成等を行った一切の情報が、NEDO が保護を要さないと確認するまでは、情報取扱者名簿に記載のある者以外に伝達又は漏えいされないことを保証する履行体制を有していること。

② 本業務で知り得た一切の情報について、情報取扱者以外の者に開示又は漏えいしてはならない。ただし、NEDO の承認を得た場合はこの限りではない。

③ ①の情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、あらかじめ NEDO へ届出を行い、同意を得ること。

２．履行完了後の情報の取扱い

NEDO が提供した資料又は NEDO が指定した資料の取扱い（返却・削除等）については、

NEDO の指示に従うこと。

XI．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 NEDO の関連文書や対象システムの情報等については、受注者が適切に管理し、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．受注者は、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．受注者は、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、直ちに口頭で担当職員に報告し、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．受注者は、本業務の遂行において、NEDO 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．受注者は、情報の受け渡し等について、以下の項目を遵守すること。

①受注者は、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、NEDO 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受注者は、貸与された紙媒体や電子媒体を担当職員の許可なく NEDO 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受注者は、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．受注者が NEDO の承認を得て本業務の一部を第三者に請け負わせる場合は、その第三

者は、受注者と同様、本仕様に記載の情報の取扱い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下請負の内容（下請負人名、下請負業務等）を明記すること。

12. 受注者は、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。

12. 受注者は適格請求書発行事業者である場合、NEDO に対し適格請求書を交付すること。

13. 本仕様書に定める事項については、随時担当職員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、担当職員と受注者が協議の上で決定することとする。

14. 本業務は、本仕様書及び受注者が入札時に提出した提案書に基づき実施すること。

（別添１）

準拠性等監査に関連する文書体系（Ｖ．１．関係）

【情報セキュリティ関係規程】

	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	外部サービス利用の申請ルール
6	情報システム運用管理規程
7	情報システムの運用及び管理に関するガイドライン
8	その他マニュアル及び手順書関連

※以上の資料は、契約締結後、受注者に提供する。

※以上の資料は大凡 150 ページ程度。

【NISC 統一基準群より】

	名称
1	政府機関等のサイバーセキュリティ対策のための統一規範
2	政府機関等のサイバーセキュリティ対策のための統一基準（令和 5 年度版）
3	政府機関等の対策基準策定のためのガイドライン（令和 5 年度版） （令和 6 年 7 月 24 日一部改定）

※以下の Web サイトより参照。

https://www.nisc.go.jp/policy/group/general/kijun.html