別紙

仕様書

1．件名

新規格に則った ISMS 内部監査及び外部審査の支援業務

2．目的

発注者は情報セキュリティマネジメントシステムの国際規格である ISO/IEC27001（以下「ISMS」という。）の認証を 2016 年 12 月に取得し、現在は海外事務所を除く国内全拠点を対象範囲として、ISMS 推進活動を行っている。

2022 年 10 月に ISMS 規格改訂があり、発注者は 2024 年度に移行審査を受審予定である。このため、2023 年度のサーベイランス審査受審後、新規格への移行対応として、必要な ISMS 文書の改訂準備等を行った。

2024 年度に受審する「移行審査」は、初めての対応となり、専門的な知見とノウハウが必要である。本業務は、移行審査に向けて NEDO における PDCA サイクルを基本としたマネジメントシステムを維持するために発生する業務を支援することを目的とする。

なお、発注者は国立研究開発法人として「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（以下、「政府統一基準群」という。）」に準拠した情報セキュリティ管理規程を整備したうえで、ISMS 規格に準拠するための施策を行っている。

3．業務の概要

受注者は、発注者が実施する現在の ISMS 推進活動を支援するとともに、サーベイランス審査及び新規格への移行審査の受審において必要な助言及び作業支援並びに ISMS 推進担当者等への教育を行うこと。

なお、発注者が現在保持している ISMS 認証は以下のとおり。

（1）認証登録番号：IC22J0547

（2）有効期限：2025 年 10 月 31 日

4．履行期限

2024 年 12 月 27 日（金）まで

5．認証対象範囲

2024 年 7 月 1 日時点における、ISMS 認証の対象範囲は以下のとおり。ただし、法令等の改正又は発注者の都合により、業務プロセスの変更、組織改正等が発生した場合は、変更部分に対する審査工数が加算される可能性がある。

（1）審査対象組織

審査対象組織は、発注者のホームページ「組織図」（2024 年 7 月 1 日以降）に示される、海外事務所を除く全ての部門。

（２）審査対象者

「５.（１）審査対象組織」における職員とし、詳細については ISMS 事務局員と調整すること。

（３）審査対象人数

約 1,600 名

（４）審査対象場所

（ａ）本部

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

（ｂ）NEDO 分室

東京都千代田区霞が関一丁目 4 番 2 号　大同生命霞が関ビル

（ｃ）革新蓄電池開発センター

京都府宇治市五ケ庄　京都大学宇治地区キャンパス　先端イノベーション拠点施設 309 号室

６．ISMS 支援業務管理要件

（１）支援業務計画書の作成

受注者は、本業務開始から発生者の 5 営業日以内に「ISMS 支援業務計画書」（案）を作成し、発注者に提出し、発注者の了承を得ること。「ISMS 支援業務計画書」（案）においては、業務責任者、業務管理者、その他各チームの役割、作業分担等を明記した支援体制図及び秘密保持体制の案を包含すること。また、具体的なリスク、課題管理方法を含む支援業務管理要領の案を包含すること。

なお、支援体制には、ISMS 主任審査員、ISMS 審査員又は ISMS 審査員補の資格を持つ要員を 1 名以上含むこと。また、その他の要員は全て、以下の資格のうち 1 つ以上を保持していること。

（ａ）ISMS 主任審査員、ISMS 審査員又は ISMS 審査員補

（ｂ）情報処理安全確保支援士

（ｃ）CISSP

（ｄ）公認情報セキュリティ監査人又は情報セキュリティ監査人補

（ｅ）情報セキュリティスペシャリスト

（ｆ）CompTIA Security＋

（２）会議体等

（ａ）受注者は、月 2 回（原則、第 2 及び第 3 水曜日午後)、全体のとりまとめを行う ISMS 事務局を構成する職員（以下「ISMS 事務局員」という。）との打ち合わせに参加すること。また、当該打合せの議事録を作成すること。議事録は打合せ開催後、1 週間以内に発注者に提出し、発注者の了承を得ること。

外部審査にて発生した課題及び不適合の対応及び規格改訂対応における課題等についても、この打ち合わせにて、報告、検討をすること。

なお、本打ち合わせは、部門内の ISMS 推進担当となる職員（以下「ISMS 推進担当者」という。）が出席する「ISMS 推進 WG」の議事等について事前に調整を行う場でもある。

（ｂ）発注者から要請がある場合、受注者は発注者が開催する会議体へ参加すること。

（３）その他 ISMS 支援業務管理要件

（ａ）電子メールを本支援業務で使用する場合は、電子メールを識別するため、ISMS 支援業務計画書でメール送受信ルールを規定すること。電子メールを利用して電子ファイルを送付又は受領する場合は、パスワードにより暗号化した圧縮形式のファイル（ZIP）又は発注者が用意するファイル転送用ストレージサービス（PrimeDrive）を用いること。パスワードについては発注者と協議のうえ別途決定すること。また、電話によるコミュニケーションについては、別途電子メール又は文書を用いて決定事項等を記録し、共有すること。

（ｂ）送付又は受領した資料等については授受管理表を作成すること。業務終了後は受領した資料等を確実に消去又は廃棄し、発注者に報告すること。

７．業務内容

（１）支援業務計画書の策定

受注者は、「ISMS 支援業務計画書」（案）を作成し、発注者の了承を得ること。計画内容には、発注者が作成した ISMS 推進計画に沿って作業時期及び工数（目安）を記載すること。計画書の詳細については、「６．（１）支援業務計画書の作成」を参照のこと。

（２）ISMS 文書及び関連する規程、法令等の把握

受注者は、発注者が現在までに整備した ISMS 活動に係る文書を確認し、必要な助言及び作業支援を行うための情報を収集、整理すること。また、発注者は公的機関として、内閣サイバーセキュリティセンターが発行する「政府統一基準群」に準拠する情報セキュリティ関連規程を整備する必要があり、ISMS 文書は規程類の細則として整備していることを踏まえ、政府統一基準群及び関連する法令等についても、内容を把握すること。

（３）ISMS 内部監査員研修の資料の準備並びに講師

ISMS 内部監査員候補者に対して、内部監査員として必要な力量を得ることを目的とした集合形式の研修資料（講師用原稿を含む）を作成し、受注者は講師を務めること。研修は基礎編及び応用編（各 1.5 時間）の 2 部構成とし、基礎編は合計 3 回、応用編は合計 5 回実施すること。実施時期は発注者と協議すること。

内部監査員研修は 2024 年 8 月の実施を予定している。

（４）ISMS 内部監査実施に関する助言及び作業支援

受注者は、発注者が計画する ISMS 内部監査（年 1 回）において、監査計画に対する助言、監査で使用するチェックシート改訂等の作業支援、監査員として全ての監査への参加及び監査結果に対する助言を行うこと。また、監査終了後に実施する「ISMS 内部監査報告会」の資料作成に対し助言を行い、ISMS 事務局員の作業支援を行うこと。なお、ISMS 内部監査は以下の実施内容を予定している。

（ａ）国内拠点 19 部門及び ISMS 事務局の計 20 部門を対象とする。

（ｂ）監査にかかる時間は以下を想定している。

ISMS 事務局及び情報システムを管轄する部門…3.0 時間

「５．（４）審査対象場所」に示す（ｂ）及び（ｃ）…1.5 時間

その他の部門…2.0 時間

（ｃ）2024 年 9 月に実施を予定。

（ｄ）同時に最大 2 部門実施し、午前午後 1 部門ずつ、1 日最大 4 部門実施可能とする。

（5）ISMS 外部審査に関する助言及び作業支援

受注者は、発注者が ISMS 審査登録機関から審査を受ける際にオブザーバーとし全ての審査に同席し、審査内容の記録、指摘内容への助言と、審査準備等の作業支援を行うこと。なお、現時点で審査登録機関と合意している ISMS 審査の計画は、概ね以下のとおり。

・実施時期：11 月 18 日（月）～11 月 22 日（金）

・審査工数：５日間　×　審査員 2～３名（サーベイランス審査）

・審査場所：「５．（４）審査対象場所」に記載のとおり。

・審査対象：本部、NEDO 分室及び革新蓄電池開発センターを予定。

（6）課題・不適合等発生時の助言及び作業支援

受注者は、内部監査及び外部審査にて発生した課題及び不適合の対応において、原因分析及び是正処置等に対する助言を行い、ISMS 事務局員の作業支援を行うこと。

（7）発注者の ISMS 推進活動の今後の活動に向けた助言の提供

専門家としての観点から発注者の ISMS 推進活動における、今後考慮すべき点、改訂すべきルール、ISMS 推進活動全体に対する懸念等と、それに対する対策案としての助言があれば提示すること。

（8）支援業務実施報告書の作成

受注者は、本業務の内容をまとめた「ISMS 支援業務実施報告書」を作成し、発注者に報告し、発注者の了承を得ること。

８．納入成果物等

（1）納入成果物及び納入期限

以下の「表 1　納入成果物一覧」に示す提出書類一式を作成し、納入すること。

表 1　納入成果物一覧

項番	納入成果物	掲載場所	納入期限
1	ISMS 支援業務計画書	７．（１）支援業務計画書の策定	発注者が別途指示する。
2	ISMS 内部監査員研修資料	７．（３）ISMS 内部監査員研修の資料の準備並びに講師	発注者が別途指示する。
3	ISMS 支援業務実施報告書	７．（８）支援業務実施報告書の作成	2024 年 12 月 27 日
4	業務完了報告書	10.　業務完了報告書	2024 年 12 月 27 日
5	議事録	６．（２）(a)	打合せ終了後 1 週間以内

（2）納入方法

納入成果物を納入する際は以下の条件を満たすこと。

（ａ）全ての納入成果物は、書面及び電子媒体を各 1 部納入すること。

（ｂ）全ての納入成果物は、日本語で記載すること。ただし、固有名詞については日本語以外での記載も可とする。また、専門用語には説明を付すこと。

（ｃ）書面は A4 判（A3 判を用いる場合は、織り込んで A4 判に収まる形態）とすること。

（ｄ）電子媒体に保存するデータの形式は、PDF 形式及び Microsoft365 で扱える形式とすること。

（３）納入場所

郵便番号 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　システム業務部

９．情報管理体制等

（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、発注者に対し「情報取扱者名簿」（氏名、所属部署、役職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、発注者の同意を得ること。また、個人住所、生年月日、パスポート番号については、発注者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、作成等した一切の情報が、発注者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、発注者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、予め発注者へ届出を行い、同意を得ること。

（４）発注者が提供した資料又は発注者が指定した資料の取扱い（返却・削除等）については、発注者の指示に従うこと。

１０．業務完了報告書

受注者は全ての業務が完了したときは、業務完了報告を 2024 年 12 月 27 日までに通知すること。併せて授受管理表に基づき、受領した資料等を確実に消去又は廃棄し、発注者に報告すること。

１１．その他

（１）受注者は、本件の遂行にあたり、情報に対する不正アクセス、情報漏えい及び改ざんを防止するため、機密性、完全性及び可用性の観点で対策を行うこと。

（２）受注者は発注者の情報セキュリティ管理規程等を遵守すること。

（３）支援業務に伴い発生する交通費、印刷費、通信費等については本調達の範囲内とすること。

（４）発注者の職員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。

（５）本業務の実施に際しては、発注者の関係部門の通常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。

（６）受注者が適格請求書発行事業者である場合、発注者に対し適格請求書を交付すること。

（7）本業務の実施にあたり、疑義を生じた場合又は本仕様書に記載のない事項については、発注者と協議のうえ解決すること。

（8）発注者は 2024 年 7 月に、大規模な組織改編を予定している。このため、組織改編後に、新たな部、室にて、リスク評価を行うこととしている。前年度までの体制とは、異なることに留意のこと。