（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 年度情報システムの脆弱性診断業務

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「発注者」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、情報システムに対する脆弱性の対策状況を確認するため本業務を実施する。

Ⅲ．業務概要

受注者は、以下の業務を実施すること。

・Web アプリケーションの脆弱性診断

Ⅳ．業務内容

受注者は、以下に示す脆弱性診断業務を公正かつ客観的な立場で実施すること。

診断実施の結果、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。

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、Web アプリケーション等の対象範囲、診断手法及び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、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及び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、事前に発注者に説明し了承を得ること。

また、重大な脆弱性が発見された場合は、発注者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、実施範囲及び実施時期等を発注者と調整すること。

１．Web 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、発注者の外部（インターネット側）及び発注者の内部又はデータセンター（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１」の Web アプリケーションとし、診断項目は「別添２」をベースに、診断対象において必要と思われる項目を含むこと。なお、発注者が「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」に準拠した情報セキュリティ対策を行う必要があることを考慮し、受注者にて診断項目を変更・追加しても良い。診断項目を変更・追加する場合は、事前に発注者に説明し、了承を得ること。

Ⅴ．診断手順

「Ⅳ．業務内容」で記述した業務の実施にあたっては、以下の手順に沿って、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、その実施手順等を発注者と協議したうえで、実施すること。

１．全体計画書の作成

受注者は、診断全体のスケジュール及び診断の概要等を定めた全体計画書を、発注者の指示する日から 2 週間以内に作成し、発注者の了承を得ること。

２．予備調査

予備調査として、以下の調査を行うこと。

①診断対象とする Web アプリケーションの概要を把握し、脆弱性診断に必要な情報の収集を効率的に行うため、ヒアリングシート等を作成、提供すること。

②脆弱性診断を実施するにあたり、Web アプリケーション担当側から要望があった場合は、説明会等を実施する。また、事前に疎通確認等を行い、状況により診断実施場所や診断方法を適宜提案すること。

３．診断実施計画書の作成

診断実施計画書を作成し、診断手法の決定、診断対象の選定、診断の実施スケジュール等の調整を行うこと。なお、診断実施計画書には次の項目を含むこと。診断実施計画書の提出期限は、発注者と調整し決定すること。

①件名、作成日、実施責任者名

②診断実施予定日、診断査実施予定場所及び診断予定項目

③診断を受ける Web アプリケーション名

④診断詳細項目及び診断手法等

⑤診断結果の判定基準

４．診断の実施

診断実施計画書に基づき、必要な診断を実施すること。

５．診断結果報告書の作成

診断結果報告書の作成に当たっては、発注者との協議を行い作成すること。なお、診

断結果報告書には次の項目を含むこと。

①件名、作成日、実施責任者名

②診断実施日、診断実施場所及び診断項目

③診断を受ける Web アプリケーション名及び対応者

④診断詳細項目、診断手法等及び診断結果

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

また、診断結果報告書の概要版を作成すること。概要版は幹部向けの報告書となるため、出来るだけ平易な表現を用い、図・表・グラフなどで視覚的に理解しやすいものとすること。

Ⅵ. 履行期間

契約締結日から 2025 年 2 月 28 日（金）まで

Ⅶ. 納入物

項番	名称	形式・数量	納入期限
1	全体計画書	書面各 1 部、電子媒体 1 部	発注者の指定する日
2	診断実施計画書	書面各 1 部、電子媒体 1 部	発注者の指定する日
3	診断結果報告書	書面各 1 部、電子媒体 1 部	2025 年 2 月 28 日
4	診断結果報告書概要	書面各 1 部、電子媒体 1 部	2025 年 2 月 28 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。

Ⅷ. 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

Ⅸ. 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、発注者に対し「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、発注者の同意を得ること。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、作成等を行った一切の情報が、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、あらかじめ発注者へ届出を行い、同意を得ること。

２．履行完了後の情報の取扱い

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。

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発注者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．受注者は、発注者及び被診断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。

３．診断の実施に際し、緊急に対応を要する事項が明らかになったときは、直ちに口頭で発注者に報告し、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、発注者の指示に従うこと。

４．実施責任者は、全体計画書に基づく進ちょく状況について常に把握し、発注者からの問合せに対し、迅速に対応できるようにすること。

５．受注者は、本業務の遂行において、発注者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、速やかに発注者に報告を行い、原因究明及びその対処方法等について発注者と協議し対処すること。

６．受注者は、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、発注者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、事前に発注者の許可を得ること。

なお、機器の持込みを許可された場合であっても、発注者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発注者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発注者の許可なく発注者外に持ち出し、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発注者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、発注者から貸与された紙媒体や電子媒体を速やかに発注者に返却すること。その際、必ず発注者の確認を受けること。

7．受注者は、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受注者は、発注者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、診断業務にかかる通信費等一切の費用は、受注者の負担とする。

③発注者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、事前に発注者と協議を行ったうえで実施することとし、発注者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受注者は、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、事前に発注者の了承を得るとともに、設定等を変更した場合は、業務終了後に原状回復し、発注者にその報告を行うこと。

⑤診断業務の実施に際し、発注者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､速やかに発注者に報告を行い、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。

⑥対象システム側の受け入れ態勢が整わない等、直接受注者が診断業務を遂行できない場合は、発注者と協議の上、対応を決定すること。

8．受注者が発注者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、下請負業務等）を明記すること。

9．受注者は、業務実施に際して発生した不明な点は、発注者に確認のうえ、その指示に従うこと。

10. 受注者は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。

11. 本仕様書に定める事項については、随時発注者と調整の上実施すること。また、本仕様書に定めなき事項については、発注者と受注者が協議の上で決定することとする。

12. 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）

Webアプリケーションに対する脆弱性診断の対象Webページ

No	システム名	全体 ページ数	備考
1	NEDOホームページ	10,000	公開
2	アンケート・イベントシステム	2	公開
3	成果フォローアップ（追跡調査）Web化システム	1	公開
4	アンケートシステム（管理画面）	15	イントラ
5	審査システム（管理画面）	1	イントラ
6	審査システム（審査委員側画面）	1	公開
7	ＰＭＳ外部申請システム	1	公開
8	ピアレビュア（審査委員側画面）	1	公開
9	ピアレビュア（管理画面）	1	イントラ
	合計	10,023	

※ページ数は大凡の数であり、診断実施のタイミングにより増減有り

（別添２）

Webアプリケーションに対する脆弱性診断項目

	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、Web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、Web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	Webページへの出力処理に問題がある場合、その Web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 Web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 Web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	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

	可制御の欠落	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