令和 7 年度 J-PARC センター情報セキュリティ検査・訓練作業

仕様書

目次

1. 件名

令和 7 年度 J-PARC センター情報セキュリティ検査・訓練作業

2. 目的及び概要

国立研究開発法人日本原子力研究開発機構(以下、JAEA という)と、大学共同利用機関法人高エネルギー加速器研究機構(以下、KEK という)は J-PARC センターを設置し、大強度陽子加速器施設(J-PARC)の運営、利用及び施設整備に関する業務を共同で行っている。

J-PARC センター職員等が基幹ネットワーク等を利用する上で必要となる情報セキュリティ対策の啓発の一環として、令和 7 年度 J-PARC センター情報セキュリティ検査・訓練（以下、検査・訓練という）を実施する。

この検査・訓練では、J-PARC センターの情報セキュリティ管理及び対策における現状分析と啓発、今後のレベル向上に資することを目的として、J-PARC センター職員等を対象とした標的型攻撃メール訓練を実施する。

本仕様書は、当該作業を受注者に請負わせる為の仕様について定めたものである

3. 納期

令和 8 年 2 月 20 日(金)

4. 作業内容

4.1. 準備

(1). 契約締結後の書類提出

受注者は、契約締結後速やかに以下の書類を作成し、情報システムセクション検査・訓練チーム（以下、検査・訓練チームという）へ提出すること。なお、これらの書類内容について検査・訓練チームと十分協議の上、作成にあたること。

- 委任又は下請負届
- 総括責任者届
- 請負体制表
- 従事者名簿
- 検査・訓練実施計画書
- 作業工程表
- 個人情報管理体制図

(2). 打合せの実施・議事録の提出

a. 打合せ

受注者は、契約締結後速やかに検査・訓練チームとの打合せの場を設定すること。検査・訓練チームとの打合せでは、標的型攻撃メール訓練についての方法、

判断基準、実施方針等の確認を行うこと。なお、打合せ実施場所は JAEA 原子力科学研究所を予定とするが、やむを得ない理由がある場合は Web 会議等のリモートで行うことがある。また、打合せ時の資料は、打合せ 2 日前（土日祝日を除いた平日の稼働日）までに検査・訓練チームへ提出すること。

b. 議事録

受注者は、打合せや協議において決定した内容について都度速やかに議事録(Word)を作成し、メール添付で検査・訓練チームへ提出すること。

(3). 問い合わせへの対応・連絡先の明確化

a. 問い合わせへの対応

受注者は、検査・訓練チームからの問い合わせには速やかに(問い合わせを知覚した翌営業日までに)応答すること。

b. 連絡先の明確化

受注者は、当該作業の主担当者と副担当者を設け、その連絡先として、メールアドレス、電話番号を検査・訓練実施体制表に記載すること。

4.2. 標的型攻撃メール訓練

メール受信ドメインは複数(JAEA、KEK、J-PARC センター等)あり、それぞれのネットワークで 1 つ以上のセキュリティ装置が独立に運用されている。これらを踏まえ、受注者は以下を実施すること。

(1). 標的型攻撃メール訓練の実施

標的型攻撃メール訓練（以下、訓練という）として、以下方針のもと、対象者(以下、訓練対象者という)のメールアドレスに対し、添付ファイル型、URL 型、混合型(添付ファイル型＋URL 型)の内、いずれかの訓練用擬似攻撃メール(以下、訓練メールという)を送信し、訓練メールの添付ファイル開封又は訓練メール本文等に記載されている URL にアクセスした職員等(以下、訓練開封者という)を分析・集計及び同定すること。

a. 対象者（訓練対象者）

対象：J-PARC センター職員等を対象とする。

人数：検査・訓練チームが指定する約 600 名

b. 実施回数

・訓練は計 2 回(第 1 回訓練、第 2 回訓練)行う。

c. 実施日時

・各回の訓練実施日時はそれぞれ検査･訓練チームが指定する日時とする。
・第 1 回訓練と第 2 回訓練の実施間隔は 1 ヵ月程度とする。

d. 訓練に使用するメールと注意喚起用コンテンツ
・後述の、訓練メールの作成・提案・提出、注意喚起用コンテンツの作成・提案・提出を経て決定した訓練メールと注意喚起用コンテンツを使用すること。
・訓練メールによっては、訓練メール毎の訓練メール本文内への訓練対象者名記載に対応すること。
・第 1 回訓練と第 2 回訓練ではそれぞれ異なる訓練メールを使用すること。

e. 実施環境
・訓練の実施に必要な機器、環境等(Web サーバ、メールサーバ、インターネット接続環境、ドメイン名、注意喚起用コンテンツ等)は受注者が用意すること。
・用意(取得)するドメイン名は検査・訓練チームと調整して決定すること。

f. 事前テスト
訓練の事前テストを実施すること。事前テストは、事前テスト対象者メールアドレス（JAEA、KEK、J-PARC センター等の複数のドメインがある）に訓練で使用する訓練メールと同様のテストメールを送信し、メール到達性、訓練開封者の同定に必要な個人を識別するためのパラメータ、アクセス元ネットワークを識別するためのパラメータ等が検知確認用サーバのログに記録されることを確認すること。
また、事前テスト対象者による添付ファイル開封又は URL へのアクセスについて、検知確認用サーバのログを分析した上、検査・訓練チームにそのログと分析結果を提供し、開封判定について検査・訓練チームと協議の上、開封判定を決定すること。
また、訓練メール送信元メールサーバの送信条件(制約)があればその情報を検査・訓練チームに提供すること。
なお、事前テスト対象者(複数名：JAEA、KEK、J-PARC センター等)は検査・訓練チームが指定する。

g. 訓練実施結果の検証と訓練開封者の同定
訓練対象者による添付ファイル開封又は URL へのアクセスについて、検知確認用サーバのログを分析した上、検査・訓練チームにそのログと分析結果を提供

し、開封判定について検査・訓練チームと検証の上、訓練開封者を同定すること。

h. 訓練開封者の集計及び統計処理

訓練開封者の同定結果に基づき、集計及び統計処理を行うこと。訓練開封者数・未開封者数の内訳（第1回訓練のみ開封、第2回訓練のみ開封、全ての回で開封、全ての回で未開封）や開封率等の集計及び統計処理については、訓練回別、所属母組織別、ディビジョン別、セクション別、ドメイン別、集計期間中の期日別などを想定すること。

i. 訓練実施に際しての注意事項

・訓練実施時間について

JAEA/KEKの勤務時間内(09:00～17:30)に訓練メールの送信を完了すること。

・訓練メール送信方法について

インターネット側から、訓練対象者メールアドレスドメイン(JAEA、KEK、J-PARCセンター等)毎に並列で、1通/分の間隔で送信すること。

・送信数制限について

プロバイダ等の制限で同一メールアドレスからの送信数が制限される場合には同一ドメイン名の予備メールアドレスから訓練対象者メールアドレス宛に送信し、前述の勤務時間内に訓練メールの送信を完了すること。

・連絡/相談窓口について

訓練実施期間中における連絡/相談窓口を用意すること。

・開始連絡と終了連絡について

訓練メールの送信を開始する前には、検査・訓練チームへ開始連絡を行うこと。同様に、訓練メールの送信がすべて完了した際には検査・訓練チームへ終了連絡を行うこと。

(2). 検査・訓練実施体制表の提出

a. 作成・提案・提出

訓練の実施における以下①の案を作成し、第1回訓練の実施3週間前までには検査・訓練チームへ提案・提出すること。また、当該案について検査・訓練チームと協議の上、第1回訓練の実施2週間前までには以下①を完成させ、検査・訓練チームへ提出すること。

①検査・訓練実施体制表（標的型攻撃メール訓練）

(3). 検査・訓練実施要領書の提出

a. 作成・提案・提出

訓練の実施における以下①の案を作成し、第 1 回訓練の実施 3 週間前までには検査・訓練チームへ提案・提出すること。また、当該案について検査・訓練チームと協議の上、第 1 回訓練の実施 2 週間前までには以下①を完成させ、検査・訓練チームへ提出すること。

①検査・訓練実施要領書（標的型攻撃メール訓練）

b. 作成にあたっての注意事項

検査・訓練実施要領書（標的型攻撃メール訓練）には以下を含めること。

・概要（実施目的、概要等）
・実施体制（実施担当者に関する情報等）
・実施期間
・実施方法（訓練環境、訓練方法、開封判定基準、集計期間等）
・実施対象（訓練対象者数、訓練メール送信数、送信成功数、不達数）
・訓練メール内容（送信元メールアドレス、送信元メールアドレス表示名、メール件名、メール本文、添付ファイル有無、気付きポイント等）
・注意喚起用コンテンツ

(4). 訓練メールの作成

a. 作成・提案・提出

第 1 回訓練、第 2 回訓練それぞれで使用する訓練メールを作成すること。

また、訓練メールの提案資料として以下①を作成し、第 1 回訓練の実施 10 週間前までには検査・訓練チームへ提案・提出すること。また、当該案について検査・訓練チームと協議の上、第 1 回訓練の実施 4 週間前までには訓練メールと以下①を完成させ、検査・訓練チームへ提出すること。

①訓練メール（第 1 回訓練、第 2 回訓練）

b. 提案資料及び訓練メール作成にあたっての注意事項

・添付ファイル型、URL 型、混合型（添付ファイル型＋URL 型）等のそれぞれで 3 件程度ずつ案を作成すること。
・各案には、送信元メールアドレスドメイン、送信元メールアドレス、送信元メールアドレス表示名、メール件名、メール本文、添付ファイル内容等も含めること。
・第 1 回訓練と第 2 回訓練ではそれぞれ異なる訓練メールを使用すること。
・第 1 回訓練と第 2 回訓練ではそれぞれ別のドメインを使用すること。

・各案には推奨理由を付けること。

(5). 注意喚起用コンテンツの作成

a. 作成・提案・提出

第 1 回訓練、第 2 回訓練それぞれで使用する注意喚起用コンテンツ(添付ファイル、URL アクセス先)を作成すること。

また、注意喚起用コンテンツの提案資料として以下①②を作成し、第 1 回訓練の実施 4 週間前までには検査・訓練チームへ提案・提出すること。また、当該案について検査・訓練チームと協議の上、第 1 回訓練の実施 2 週間前までには注意喚起用コンテンツと以下①②を完成させ、検査・訓練チームへ提出すること。

①注意喚起用コンテンツ（第 1 回訓練）

②注意喚起用コンテンツ（第 2 回訓練）

b. 提案資料及び注意喚起用コンテンツ作成にあたっての注意事項

・添付ファイル型で使用する注意喚起用コンテンツのファイル形式は、Microsoft Word(docx)、Excel(xlsx)又は PDF のいずれかとすること。

・マクロ付きファイルは不可とする。

(6). 訓練開封者への訓練メール解説資料の作成

a. 作成・提案・提出

第 1 回訓練、第 2 回訓練それぞれの訓練開封者へ注意喚起を行うための訓練メール解説資料を作成すること。

また、解説資料の提案資料として以下①②の案を作成し、第 1 回訓練の実施 4 週間前までには検査・訓練チームへ提案・提出すること。

また、当該案について検査・訓練チームと協議の上、第 1 回訓練の実施 2 週間前までには解説資料と以下①②を完成させ、検査・訓練チームへ提出すること。

①訓練開封者への訓練メール解説資料（第 1 回訓練）

②訓練開封者への訓練メール解説資料（第 2 回訓練）

b. 提案資料及び訓練開封者への訓練メール解説資料作成にあたっての注意事項

・第 1 回訓練、第 2 回訓練それぞれの訓練メール内容に沿った解説資料とすること。

(7). 検査・訓練結果報告書の提出

a. 作成・提案・提出

訓練結果をまとめた以下①の案を作成し、訓練終了後速やかに検査・訓練チー

ムへ提案・提出すること。また、当該案について検査・訓練チームと協議の上、後述の検査・訓練チームに対する結果報告会の実施 1 週間前までには以下①を完成させ、検査・訓練チームへ提出すること。

①検査・訓練結果報告書（標的型攻撃メール訓練）

b. 作成にあたっての注意事項

検査・訓練結果報告書（標的型攻撃メール訓練）には以下を含めること。

・概要（実施目的、概要等）
・実施体制（実施担当者に関する情報等）
・実施期間
・実施方法（訓練環境、訓練方法、開封判定基準、集計期間等）
・実施対象（訓練対象者数、訓練メール送信数、送信成功数、不達数）
・訓練メール内容（送信元メールアドレス、送信元メールアドレス表示名、メール件名、メール本文、添付ファイル有無、気付きポイント等）
・注意喚起用コンテンツ
・訓練結果（訓練開封者数や開封率等の集計及び統計結果とその傾向と分析）
・訓練結果に対する分析や改善点についての提言等

4.3. 報告会

(1). 検査・訓練チームに対する結果報告会

受注者は、検査・訓練チームに対し、検査・訓練結果報告書を用いた詳細な報告(約 1 時間)を実施すること。開催場所は JAEA 原子力科学研究所を予定とするが、やむを得ない理由がある場合は Web 会議等のリモートで行うことがある。実施有無も含めて検査・訓練チームへ確認を行うこと。

5. 作業に必要な資格等

作業に必要な資格等を以下に示す。なお、資格要件説明資料は A4 用紙 20 枚程度で作成すること。

(1).受注者は ISO 9001 取得又は ISO9001 取得相当の管理を実施していること。
(2).受注者は ISO 27001 取得又は JIS_Q 27001 を取得していること。
(3).受注者は独立行政法人情報処理推進機構(IPA)公開「情報セキュリティサービス基準適合サービスリスト」の「脆弱性診断サービス」に登録されていること。
(4).受注者は特定非営利活動法人 日本セキュリティ監査協会(JASA)公開「情報セキュリティサービス台帳」の「脆弱性診断サービス」に登録されていること。
(5).受注者は訓練の訓練従事者を選任し、訓練従事者のうちの一人を訓練責任者とすること。(訓練責任者と訓練従事者は兼任しても良い)

(6). 訓練責任者は、訓練従事者の指揮命令、監督を行うこと。

(7). 訓練従事者は、標的型攻撃メール訓練作業及び分析資料作成の経験又は知識を有すること。

(8). 訓練従事者は、訓練対象者自身による添付ファイル開封、URL のアクセスについてのログ分析に関する経験又は知識を有すること。

6. 提出書類

提出書類について、注意事項、提出場所、提出書類を以下に示す。受注者は以下のとおり提出すること。

[注意事項]

全般：*1 *2 *3 *4 *5

個別：*6 *7 *8 *9

[提出場所]

JAEA　原子力科学研究所　情報システムセンター建家　11 号室

[提出書類]

(1). 委任又は下請負届

契約締結後速やかに　　1 部

(2). 総括責任者届

契約締結後速やかに　　1 部

(3). 請負体制表

契約締結後速やかに　　1 部 *6

(4). 従事者名簿

契約締結後速やかに　　1 部

(5). 検査・訓練実施計画書

契約締結後速やかに　　1 部

(6). 作業工程表

契約締結後速やかに　　1 部

(7). 個人情報管理体制図

契約締結後速やかに　　1 部 *7

(8). 検査・訓練実施体制表（標的型攻撃メール訓練）

第 1 回訓練の実施 2 週間前までに　1 部

(9). 検査・訓練実施要領書（標的型攻撃メール訓練）

第 1 回訓練の実施 2 週間前までに　1 部

(10). 検査・訓練結果報告書（標的型攻撃メール訓練）

報告会の実施 1 週間前までに　　1 部 *8

(11). 議事録

会合後速やかに　　1部

(12). その他の書類

必要に応じて速やかに　　1部 *9

*1：納品に際して、本仕様書「10. 検査員及び監督員」に示す一般検査が行われることを前提とし、納品図書を直接持参のうえ納品手続きにあたること。

*2：提出書類一式をA4サイズのファイルに収め、納品図書とすること。この納品図書のファイル表面には、本契約件名、JAEA契約番号、納入年月、受注者名（会社名）が印字されたラベルシールを貼り、納品図書であることが容易に判別できるようにすること。なお、納品図書のファイル表面に貼るラベルシールは、色は無地とし、ラベルライター等の機械を使用して作成したものであること（手書きのラベルシールは禁止とする)。同様に、納品図書ファイルの背には、本契約件名、受注者名（会社名）等のラベルシールを貼ること。

*3：JAEAの指定書式が存在する場合は、その書式に準じ作成し提出すること。

*4：文書・図表などの表現が稚拙ではなく、簡潔・平易な日本語で記載すること。

*5：原則、Word又はExcelで作成にあたること。これ以外のツールを使用する際は当セクション担当者にあらかじめ確認の上、協議し取り決めること。

*6：請負体制表には、「資本関係・役員の情報、事業の実施場所、事業従事者の所属・専門性（情報セキュリティに係る資格・研修等)・実績及び国籍」について記載すること。

*7：個人情報管理体制図には、個人情報を安全に取扱うための組織体制が整備されていることを確認できる体制図を記載すること。また、個人情報の漏えい等安全確保の上で問題となる事案の発生又は発生するおそれがあることを知ったときに対応する責任者を記載し、当機構への連絡体制を記載すること。また、個人情報を取り扱うことを許可された作業従事者以外の者が当該個人情報にアクセスすることができないようになっているか、施錠状況や個人情報へのアクセス制限の設定状況について記載すること。

*8：納品図書のファイルに収めた印刷物と同一内容の電子データ（該当書類完成時のツール版（Word/Excel）とPDF版）を記録媒体（CD-ROM又はDVD-ROM）に保存し、この記録媒体を納品図書のファイルに収めること。この記録媒体の表面には、本契約件名、JAEA契約番号、納入年月、受注者名（会社名)、保存された電子データの名称等を印字し、納品物の一部であることが判るようにすること（手書きは禁止とする)。また、この記録媒体を納品図書のファイルに収める際は、穴あきタイプの不織布ケース等を用いて納品図書のファイルに収納する等、当該納品図書のファイルと物理的に分離しないよう努めること。

*9：JAEA担当者又は当セクション担当者と受注者でその都度協議し取り決める。

7. 貸与品

なし。

8. 作業実施期間

契約締結後～令和８年２月において実施する。ただし、各種実験機器の試験稼働時期と重なる可能性もある為、詳細な実施時期については別途協議の上決定する。

9. 検収条件

本仕様書『4.　作業内容』に定める作業の実施と確認、本仕様書『6.　提出書類』に定める書類提出及び納品図書の納品と確認、並びに JAEA が本仕様書の定める業務が実施されたと認めた時を以て業務完了とする。

10. 検査員及び監督員

検査員

(1). 一般検査　管財担当課長

監督員

(1). 現場確認　J-PARC センター　情報システムセクション　セクション員

11. 協議

本仕様書に関してあるいは、記載の事項及び記載のない事項について疑義が発生した場合は、JAEA 及び受注者双方の協議の上対処するものとする。

12. 守秘義務

受注者は、本作業を実施することにより取得した本作業に関する各データ、技術情報、成果その他のすべての資料及び情報を J-PARC センター外に持ち出して発表もしくは公開することはできない。また、特定の第三者に提供することはできない。

13. 情報セキュリティの強化

情報セキュリティの強化について、別紙「情報セキュリティ強化に係る特約条項」に定められたとおりとする。

14. グリーン購入法の推進

(1). 本契約において、グリーン購入法（国等による環境物品等の調達の推進等に関する法律）に適用する環境物品（事務用品、ＯＡ機器等）が発生する場合は、これを採用するものとする。

(2). 本仕様に定める提出図書（納入印刷物）については、グリーン購入法の基本方針に定める「紙類」の基準を満たしたものであること。

15. 適用法規・規則等

本契約の作業などにあたっては、以下の法令等を必要に応じて適用とする。

(1). 労働基準法

(2). 労働安全衛生法

(3). JAEA/KEK 及び J-PARC センター諸規定

(4). その他、関連諸法令、基準

16. 特記事項

(1). 受注者は、本作業にかかわる各個別業務の全部又は一部を、第三者へ委任もしくは下請負を行う場合、資本関係・役員の情報、事前に JAEA の了解をとり、委任先又は下請負先に対して JAEA の守秘義務契約条項を網羅した守秘義務契約等を結び、その写を JAEA に提出すること。

(2). 受注者は、本作業に必要なもの以外は J-PARC センターに持ち込まないこと。

(3). 受注者は、本作業実施に当たっては情報セキュリティ規程類について特に留意し、これを遵守すること。また、情報セキュリティ規程類に基づく J-PARC センターの指示に従うこと。

(4). 受注者は、本作業に係る情報について、災害、紛失、破壊、改ざん、き損、漏えい、コンピュータウィルスによる被害、不正利用、不正アクセス、その他の事故等、これらの発生又は生ずるおそれがあることを知った場合は、ただちに J-PARC センターに報告し、指示に従うものとする。本契約終了後においても、同様とする。

(5). 受注者は、情報セキュリティ等の重要な情報を知り得る立場にある為、個人情報の取り扱いについてその保護の重要性を認識し、個人の権利、利益を侵害することのないよう以下を遵守すること。

a. 本作業に係る者を特定し、それ以外の者に作業をさせてはならない。

b. 本作業に係る情報について、適切に管理すること。情報システムに於いて扱う場合には適切なアクセス制限を行い、ウィルス対策、P2P ソフトの不使用等適切な情報セキュリティ対策を実施すること。

c. 本作業を処理するために、提供されたあるいは自らが収集又は作成した個人情報が記録された資料等（USB などの電磁的記録を含む）の取扱いは以下①及び②とする。

①複製又は複写してはならない。複製又は複写する必要がある場合には、J-PARC センターに対して、その範囲・数量等を書面により通知して承諾を得なければならない。

②本契約終了後速やかに、J-PARC センターに返還し、又は引き渡すものとする。ただし、J-PARC センターが別に指示したときは当該方法による。

(6). 本作業で作成した一切のものは、すべて当機構に帰属するものであり、私権を設定してはならない。ただし、あらかじめ書面により当機構の承認を受けた場合はこの限りではない。

(7). 受注者は、本契約の履行に関して第三者に身体的又は財産的損害を与えた場合、これにより生じた損害賠償の責めを負うものとする。

(8). 受注者は、本作業をする上で受注者の責めに帰すべき事由により当機構に損害を与えた場合には、受注者の責任において現状に復すること。また、受注者が被った損害が当機構の責により生じたもの以外は、当機構は一切の責任を負わないものとする。
(9). 受注者は、従事者に関して労基法、労安法その他法令上の責任並びに従事者の規律秩序及び風紀の維持に関する責任を全て負うとともに、これらコンプライアンスに関する必要な社内教育を事前に行うものとする。
(10). 受注者は、当機構が原子力の研究・開発を行う機関であるため、高い技術力及び高い信頼性を社会に求められていることを認識し、当機構の規程等を遵守するとともに安全性に配慮し業務を遂行し得る能力を有する者を従事させること。
(11). 当機構内への入退域及び物品、車両等の搬出入に当たっては、当機構所定の手続きを遵守すること。
(12). 受注者は、異常事態等が発生した場合、当機構の指示に従い行動するものとする。また、本契約に基づく作業等を起因として異常事態等が発生した場合、受注者がその原因分析や対策検討を行い、主体的に改善するとともに、受注者による原因分析や対策検討の結果について当機構の確認を受けること。
(13). 受注者は、機構が伝染性の疾病（新型インフルエンザ等）に対する対策を目的として行動計画等の対処方針を定めた場合は、これに協力するものとする。
(14). 受注者は、本仕様書の各項目に従わないことにより生じた、機構の損害及びその他の損害についてすべての責任を負うものとする。

以上