令和８年度ＩＴ人材育成研修

仕　様　書

１．件名

IT人材育成研修　一式

２．背景及び目的

独立行政法人国立高等専門学校機構（以下「機構」という。）において、情報システム及び情報ネットワーク（以下「情報システム等」という。）は、教育及び業務における基幹系システムとして非常に重要な役割を担っており、また、情報システム等を支える人材の確保及び育成は、機構としての重要かつ喫緊な課題となっている。

ついては、全国立51高等専門学校（以下「高専」という。）及び機構本部の情報システム等の運用管理に携わる者の専門的知識や技術力の向上を図ることを目的とした研修を実施することとし、この研修の実施に関する業務を委託するものである。

３．研修実施計画書の提出について

① 本仕様書に記載する研修実施要件に基づき、「研修実施計画書（記載内容に、教育項目・日程計画・教育形式・教育内容・講師・機材仕様を含む）」を作成し提出すること。
② 研修実施計画書の内容に基づいて技術審査を行う。
③ 技術審査において、本仕様書の要求要件を満たしていないと判断された場合は不合格となる。また、記述内容が不明確である場合や説明が不十分な場合などにより、十分な技術審査が行えないと判断された場合は、要求要件を満たしていないものとみなす。
④ 研修実施計画書には、当該計画書の内容に関する照会先を明記すること。
⑤ 提出された内容等について、問い合わせやヒアリングを行うことがあるので、これに対応すること。
⑥ 研修実施計画書は日本語で作成すること。

４．契約期間

契約開始日～令和9年2月末日まで

５．研修実施要件

（１） 研修内容

別紙「サイバーセキュリティ研修」に示す内容の研修を実施すること。

（２） 受講者人数

60名程度

※最大受講者を32名とする研修を、2回に分けて実施

（３） 事前課題

① 受講者に対し、集合研修の内容をスムーズに理解するにあたり必要な知識を習得するための事前課題を課すこと。なお、事前課題には30分程度で実施可能な自習学習資料を含めるものとする。

② 事前課題については、1回目の集合研修実施4週間前までに電子データで機構に納品すること。

③ 受講者への事前課題の展開は、機構担当者を通じて行うものとする。

（４）集合研修

① 必要な座学を実施しつつ、実習や実機に触れる演習に重きを置いたものとすること。

② 演習はグループワーク形式とし、機構が指定するグループ名簿に基づいてグループ分けを行うこと。

③ 研修内容、実施体制、機材、課題、テキスト等は、全受講者同一とすること。

④ 適宜、質疑応答・休憩の時間を設けること。

⑤ 研修は1回につき連続する平日２日間で行うものとし、1回目は1月26日（火）から1月28日（木）まで、2回目は2月2日（火）から2月4日（木）まで実施すること。

⑥ 開催時間は、9時30分～17時30分または10時～18時とすること。

⑦ 実施日程は、落札後に機構担当者と協議の上、決定するものとする。

⑧ 開催場所は、最寄り駅から徒歩10分以内に到着する会場を用意すること。また、最寄り駅は、東京駅または品川駅から電車移動にて30分以内に到着する駅とすること。

⑨ 各研修は、同一建物内にて行うこと。

⑩ 1名以上の講師により行うこと。また、予定する講師は、情報処理安全確保支援士の資格を有し、別紙「サイバーセキュリティ研修」に示す内容に類似する研修について、官公庁又は独立行政法人を対象として、過去3年以内に業務として行った経験を有すること（研修実施計画書にて、予定している講師が前述の要件を満たしていることを示すこと）。なお、落札後の講師の交代は、やむを得ない場合を除き原則認めないものとする。

⑪ 機構担当者と協議の上、受講者全員に対してアンケートを実施し、その結果を機構にも

提供すること。アンケート内容については、機構と事前に協議すること。

（５）機材

① 研修に必要な機材やツール、ネットワーク環境等を用意すること。また、演習用端末を受講者数分（1名につき1台）＋予備1台を用意すること。

② 上記①以外に、研修の実施に必要な機材を用意すること。

（６）テキスト

① 研修内容のテキストを作成し、1回目の集合研修実施4週間前までに電子データで納品し、1回目の集合研修実施日前日（以下、「期日」という。）までに機構の承認を得ること（承認が得られない場合、期日までに承認が得られるよう、機構のフィードバックを元に適宜修正を行うこと）。

② 集合研修当日に、資料として紙媒体で受講者全員に配付（持ち帰り可能）すること。また、併せて予備1部を用意すること。

③ 受講者に配付された紙媒体のテキストについては、受講者所属の高専内において、関係者複数名で閲覧が可能であること。

６．機密保持

① 本業務により知り得た全ての情報について守秘義務を負うものとし、これを第三者に漏らさないこと。また、他の目的に使用しないこと。

② 本業務により知り得た情報については、契約期間はもとより、契約終了後においても第三者に漏らしてはならない。

③ 正当な理由があってやむを得ず第三者に開示する場合、事前に機構の許可を得ること。また、情報の厳重な管理を実施すること。

④ 機構が提供した資料は、 原則として全て複製禁止とすること。研修の業務上やむを得ず複製する場合は、機構の許可を得なければならず、この場合にあっても使用終了後はその複製を機構に返納又は焼却・消去する等適切な措置をとり、機密を保持すること。

７．損害賠償

受注者が本契約に違反して、機構本部が損害を被った場合には、機構本部は受注者に対して契約金額を上限として損害賠償を請求し、かつ、両者協議の上、機構本部が適当と考える必要な措置をとることを請求できる権利を有するものとする。

８．納入成果物

（１）事前課題

1回目の集合研修実施4週間前までに、電子データで納品すること。

（２）テキスト

1回目の集合研修実施4週間前までに電子データで納品し、内容について期日までに機構の承認を得ること。

（３）研修実施報告書

2回目の集合研修実施後速やかに、研修実施報告書（記載項目に、アンケート結果・教育項目・日程・教育形式・教育内容・講師を含む）を、電子データで提出すること。

９．その他

本調達の履行について疑義が生じたとき、又は本調達に伴い機構と締結する契約書に定めのない事項については、機構及び受注者双方で協議の上決定すること。

別　紙

■研修内容「サイバーセキュリティ研修」

【概要】

ハンズオン形式でセキュリティに関する研修を行う。

【受講者】

各高専・機構本部事務局において、日常的にネットワークシステムの維持管理を行っている教職員を想定する。IP アドレスやネットワーク機器ならびにこれに関する概念に対し、基礎知識を有していることを前提とする。

【研修項目】

・DMZ 攻撃演習

DMZ サーバ経由で機密情報の漏えいが発生したインシデントを想定し、侵入経路及び攻撃手法の特定並びに封じ込めを実施する。調査対象 OS の構成は、Windows 及び Linux をそれぞれ50％とする。

シナリオ形式（サイバーレンジ）による研修とし、ログからインシデントの原因を特定する形式とする。

【目標】

各高専に於いて以下の作業ができるようになること。

・高専機構の情報セキュリティインシデント対応チーム、上司、ベンダー等と適切に情報共有し、インシデント発生時に、検知・連絡受付→トリアージ→インシデントレスポンス→報告・公表→事後対応等の一連の対応を自らすすんで行うことができる。

・パソコン、サーバ、ネットワーク機器等のログを監査できる、もしくは監査作業の内容を把握できる。