仕様書（案）

1. 件名

2027 年度中核人材育成プログラム（IT/OT[1]分野における検知技術・防衛技術・レジリエンス手法等）に関する講習等実施業務

2. 背景・目的

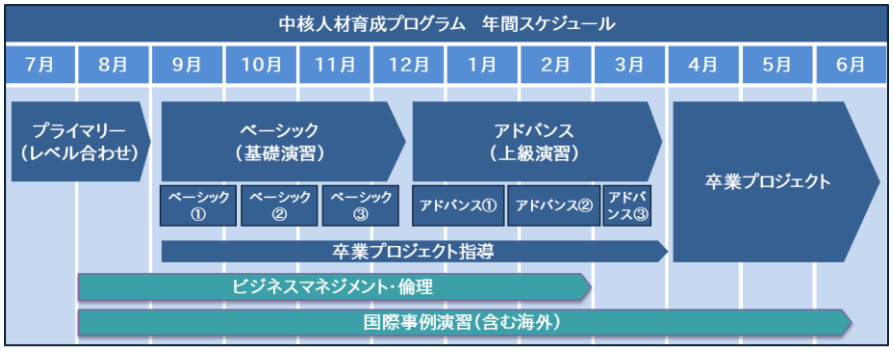
近年、企業や個人の情報を狙ったサイバー攻撃にとどまらず、プラントやインフラの停止を狙い、制御システムまで含めた社会システム全体を標的とするサイバー攻撃のリスクが高まっている。このため、国家として安全・安心な社会を築くために、特に、重要インフラや経済・社会の基盤を支える事業者と国が連携し対策に取り組む必要がある。

プラントやインフラがサイバー攻撃を受けた場合には、それがどのような攻撃であるか把握し、迅速に対処することが重要であるとともに、事業継続性の観点から、サイバー攻撃に備えた準備、復旧計画等について、実践的かつ効果的に学ぶ必要がある。

独立行政法人情報処理推進機構（以下「IPA」という。）では、2017 年に「産業サイバーセキュリティセンター」を設立し、サイバーセキュリティの最新の技術・ノウハウを学ぶとともに、実践的な模擬攻撃を通じた対策立案までを行い、効果的な防御戦略を構築できる人材を育成するとともに、他業界のサイバーセキュリティ責任者や専門家、国内外での人脈を形成することにより、総合的なサイバーセキュリティ戦略立案を担う中核人材の育成を推進する人材育成プログラム（以下「中核人材育成プログラム」という。）を実施している。

中核人材育成プログラムは、以下のコースから構成される。

- プライマリーコース
  7 月初旬頃～8 月末頃の約 2 ヶ月間で IT 基礎（情報システム基礎・情報システムセキュリティ基礎）と OT 基礎（制御システム基礎・制御システムセキュリティ基礎・安全制御基礎）等を習得する
- ベーシックコース
  9 月初旬頃～12 月中旬頃の約 4 ヶ月間で制御システムセキュリティ・IT セキュリティ・BCP 等を演習を通じて網羅的に習得する
- アドバンスコース
  12 月中旬頃～3 月末頃の約 3 ヶ月間でベーシックコースよりも更に実践的な演習を実施し、更なる知見の向上を目指す
- 卒業プロジェクト
  4 月初旬頃～6 月末頃までの期間で、受講者が習得した知識や経験を活かし、個人もしくはグループでテーマを企画立案して実施する
- その他
  上記の技術分野以外にほぼ通年で、ビジネスマネジメント、倫理、国際事例演習によりスキルを習得する。



[1] OT：Operational Technology（制御技術）

OT 固有のセキュリティリスクやサイバー攻撃からの防御手法などの技術的情報は、IT 分野のセキュリティに関する情報と比較して世の中に多く出回っておらず、初めて学習する者も多い。そのため、サイバー攻撃からの防御技術等に関する高度な知識を、限られた期間内で効率よく習得するためには、一貫性をもって学習する必要がある。

本業務では、以下に示す OT 防御技術等分野のプライマリーコース、ベーシックコース、アドバンスコースの講習・演習および卒業プロジェクトテーマへの指導・助言の実施（以下「講習等」という。）の計画及び実施を行うものである。

- 中核人材育成プログラムの中核であるベーシックコース・アドバンスコースにて実施するテクノロジー系講座を十分に理解するために IT および OT 分野の基礎知識や通信プロトコル、セキュリティ対策の基礎知識の習得を目的としたプライマリーコース。
- 制御システム固有のセキュリティリスクやサイバー攻撃の内容、それらサイバー攻撃を防ぐための防御技術に関する知識を習得するベーシックコース。
- ベーシックコースよりも更に実践的な演習を実施し、更なる知見の向上を目指すアドバンスコース。
- ベーシック・アドバンスで習得した知識をもとにサイバーセキュリティに関するテーマを選定し、個人もしくはグループで取り組む卒業プロジェクト。なお、受講者はアドバンスコース期間中から卒業プロジェクトテーマの企画・立案および調査・制作に着手するため、卒業プロジェクトテーマ指導・助言はアドバンスコース期間および卒業プロジェクト期間を通じた対応となる。

3. 中核人材育成プログラム業務内容

3.1. 実施計画書の作成について

契約締結日から 5 営業日程度を目途に、次の(1)～(5)の事項を含む「2027 年度中核人材育成プログラムに関する講習等実施業務（IT/OT 分野における検知技術・防衛技術・レジリエンス手法等)」の実施計画書を作成・提出すること。

(1) 全体の実施スケジュール
(2) 実施予定の概要
  - 実施項目の名称
  - 実施形式
  - 実施場所、など
(3) 実施体制および役割
(4) 常勤講師(予定)の略歴
(5) プロジェクトリーダーの緊急連絡先

3.2. プライマリーコースの計画および実施

3.2.1. 実施対象

社会インフラ及び産業基盤に関連する企業・機関、又はその関連会社からの人材を想定する。

なお、受講者は以下の条件を満たしているものとする。

- 情報処理技術者試験（IT パスポート試験）の合格程度の水準
- 情報システム又は制御システムに関わる 1 年以上の実務経験

また、受講者数は 60 名程度を想定する。

3.2.2. 実施場所

- 東京都文京区本駒込 2-28-8 文京グリーンコートセンターオフィス内
- 東京都千代田区外神田 4 丁目 14-1 秋葉原 UDX 内
- その他 IPA と請負者が協議して合意の上で定めた場所

3.2.3. 実施期間

中核人材育成プログラム実施スケジュールのプライマリーコース期間に受講者全体を対象に講習等を実施する。講習等は IPA が指定する合計約 15 日間とする。(ただし、実施日は

変更される可能性があるため、変更時は速やかに対応できること。）なお、プライマリーコース期間中に夏季休暇を設ける予定であるが、その日程については IPA から別途指定する。

また、プライマリーコース期間中に受講者全体を 2 グループに分割して、1 グループに対して各 2 日間のアクティビティを実施すること。なお、2 日間の内訳は、受講者のベーシックコース受講に向けた準備（模擬施設デモ見学等）及び講師とのコミュニケーション強化を目的としたアクティビティを 1 日、演習施設見学（CSSC 施設を想定）等を 1 日とする。

さらに、全受講者を対象とした演習用 PC 環境（受講者によりそれぞれ Windows 又は Mac の 2 種類 の OS を想定）の構築を最大 2 日間、外部施設見学（CSSC 施設以外）1 日をアレンジし、受講者に解説とともに提供すること。外部施設見学は 1 か所で充足できない場合は、複数施設を同時進行としてもよいこととし IPA と調整して確定すること。

なお、以上の各日程については IPA より別途指定する。

文京グリーンコート施設での講習等の時間は、10：00～17：30 までを基本とし、昼休み休憩(13:15～14:15)及び授業間の休憩時間（15 分×2 回）を除いた 6.0 時間（1 コマ：90 分×4 コマ）で実施する。秋葉原 UDX および演習施設見学（CSSC 施設を想定）での講習等の時間は、昼休み休憩（1 時間）及び授業間休憩（計 30 分）を含む 10:30～18:00 までを基本とする。外部施設見学の時間は IPA と協議により決定する。

3.2.4. 到達目標

- IT 基礎の講習範囲について、情報処理技術者試験の高度試験と情報処理安全確保支援士試験の一部（午前Ⅰ試験）で午前Ⅰ通過者と同等程度の知識を習得すること
- ベーシックコース以降にて制御システムセキュリティを題材にした発展的講義を聴講するため、制御システムに関連する基本的な用語や理論を理解すること
- ベーシックコース以降にて制御システムセキュリティに関する演習を実施するため、制御機器や制御通信ネットワークに関する基礎知識を習得すること
- ベーシックコース以降のアクティブラーニングでの課題解決を自身の力で行うため、制御用コントローラのプログラミングなど、基礎的な技術を身につけること

3.2.5. プライマリーコースの計画

(1) 講習等の計画

以下の要素を必ず取り込み、講習等を実施すること。

【座学・演習】

① IT 基礎

- ✧ 情報システムに関する基礎知識
  - 情報基礎理論
  - ハードウェア（CPU、メモリ）
  - ソフトウェア（アルゴリズム、設計など）
- ✧ ネットワークの基礎
  - TCP/IP、各種プロトコルなど
  - システム及びネットワーク構成
- ✧ UNIX/Linux 入門
  - コマンド
  - ネットワーク構成
- ✧ 情報セキュリティ知識
  - 情報セキュリティ技術
  - 情報セキュリティ管理
- ✧ Python プログラミング

なお、上記の講習等については、IPA 職員が講習等を実施する場合がある。IPA 職員が講習等を実施する場合には、講習等補助要員として講習等に参加し、IPA 職員による講習等の継続が困難である場合には、IPA 職員に代わり講習等を継続すること。IPA 職員による講習等の実施の詳細については後日連絡する。

② OT 基礎
- ✧ 制御システム
  - ・ 背景・歴史
  - ・ 構成（アーキテクチャ・構成機器類等）
  - ・ 制御システムに関連する法制度・政策の紹介
  - ・ 制御システムのセキュリティ脅威、信頼性評価の概要
  - ・ 制御システムセキュリティ対策基礎（代表的な対策の概要、海外動向等）
  - ・ 制御システムセキュリティマネジメント基礎（ビジネスリスクとの関係、計画立案、組織構築、対策効果分析等）
- ✧ 制御工学入門（制御方式の種類、信号・通信理論、分野毎の特徴等）
- ✧ 制御通信プロトコル概論
- ✧ 制御用コントローラプログラミング演習（ラダープログラミング、ST 言語等）

③ その他
- ✧ 演習用 PC 環境の構築
- ✧ 外部施設見学
- ✧ IPA 模擬施設デモ見学

(2) シラバス・時間割・体制図・教材等の作成

シラバス、時間割、体制図および教材等の案を作成し、2027 年 6 月中に IPA に提出すること。詳細な日程は IPA と協議して決定すること。なお、各作成物における記載内容は以下のとおり。

＜シラバス（IPA 指定様式）＞
- ・ 講習等名称と実施概要
- ・ 詳細アジェンダ
- ・ 実施日時と場所
- ・ 予定講師名（外部者の場合は組織・企業名）
- ・ 使用する教材、機材、教科書、その他参考文献、など

＜時間割＞
- ・ 講習等名称
- ・ 実施日時
- ・ 実施場所
- ・ 予定講師名（外部者の場合は組織・企業名）
- ・ 各講習等の実施日程単位のコマ割り、など

＜体制図＞
- ・ 「講師」と「講師補助員」の区分を明示したチーム構成図
- ・ プロジェクトリーダーの氏名
- ・ 予定講師名（外部者の場合は組織・企業名）
- ・ 関連する外部業者名、など

＜教材等＞
- ・ 講習等で使用を予定するテキスト教材

(3) 教材等の準備

講習等実施に用いる教材を準備すること。なお、教材は原則として請負者が著作権を有するものを含めること。不足分については、国内外の第三者が著作権を有するものを利用してもよいし、新たに作成してもよい。ただし、第三者が著作権を有するものを利用する場合には、利用した箇所に引用表記を行うなど、第三者が著作権者であることを明示すること。

IPA が講習等実施前に教材の確認を求めた場合には、速やかに応じること。

3.2.6. プライマリーコースの実施

(1) 講習等の実施

講習等では以下を実施すること。

- 3.2.5 で計画した講習等を受講者に対して実施する。
- 講習等に対する受講者からの質疑に対応する。
- プライマリーコースの講習等終了時に受講者に対して習熟度を確認する。

(2) 受講者へのフォロー

- プライマリーコースの講習等終了時に受講者に対して、自己診断などにより講習前後の知識や技能の習熟度を確認すること。
- 習熟度評価結果や IPA が受講者から週次で受領する状況報告などにより、3.2.4 到達目標の基準に対して、理解が及んでいない受講者が確認できた場合、個別もしくは全体的にフォローを実施すること。ただし、特段の事情が無く受講者自身の責（無断欠席など）に起因する場合は除く。なお、フォローを実施する日程等は IPA と調整すること。
- 習熟度の確認方法及び設定した基準は、IPA の承認を得ること。

(3) 実施報告書の作成

講習等終了後に「2027 年度中核人材育成プログラムのプライマリーコースに関する実施報告書（IT/OT 分野における検知技術・防衛技術・レジリエンス手法等)」を、「7.1 納入期限と納入物件」に記載の日程までに IPA に提出して承認を得ること。

また、同報告書は次の事項を含むこと。

- 講習等全体の実施結果まとめ
  - ① 実施目的
  - ② 到達目標
  - ③ 講習等の実施概要（シラバス、時間割、体制図）
  - ④ 実施した講習等の内容が分かる資料（フォロー時の講習等も含む）
  - ⑤ 各講習等で受講者から出た主な質問、など
  - ⑥ 仕様書の各要件を満たしていることを確認した結果(チェックリスト)、など
- 習熟度評価方法に基づく確認結果
- プライマリーコースの講習等実施にて感じた問題点およびその改善案

3.3. ベーシックコースの計画および実施

3.3.1. 実施対象

対象とする受講者は合計で 60 名程度とするが、受講者全体を 3 つのクラスに分けて実施するため、1 クラス 20 名程度への講習等の実施となる。なお、受講者は 2027 年度中核人材育成プログラムのプライマリーコースで実施した講習等内容を理解しているものとする。

3.3.2. 実施場所

- 東京都文京区本駒込 2-28-8 文京グリーンコートセンターオフィス内
- 東京都千代田区外神田 4 丁目 14-1 秋葉原 UDX 内
- その他 IPA と請負者が協議して合意の上で定めた場所

3.3.3. 実施期間

受講者を 3 つのクラスに分けて講習等を行うため、ベーシックコース期間中の 2027 年 9 月初旬頃から 2027 年 12 月中旬頃までの間に 1 回あたり約 20 日間の講習等を 3 回実施する。

講習等の時間は 10：30～18：00 までを基本とし、昼休み休憩(12:00～13:00)と授業間の休憩時間（15 分×2 回）を除いた 6.0 時間（1 コマ：90 分×4 コマ）にて実施する。

なお、講習等は演習中心での実施が想定されるため、講習等時間については事前に IPA と協議した上で変更可能とする。

講習等実施場所が IPA の施設外である場合、受講者が講習等使用機材を利用した自習を行うことを考慮し、講習等終了後に施設利用時間の延長に対応できる体制を整えること。

3.3.4. 到達目標

- 制御システムが直面する脅威に対応する代表的攻撃パターンを把握し、システムのどの部分がリスクを含んでいるか解析出来る能力を身に着けること
- 産業系システムへのサイバー攻撃に対する有効な防御策の基礎知識と実装技術を有し、システムへの適応案を作成することが出来ること
- セキュリティインシデントの発生時、実際に何が起こるか、何を行うべきかについて、実体験に裏付けられた知識と経験を有し、関係者に対して冷静な指示を出せること
- 攻撃解析技術についての基礎技術を習得して、影響範囲の特定、安全を考慮した事業継続優先事項の判断、適切な手順に沿ったフォレンジックの指示といった、より実践的な技術を学ぶための準備が出来ていること

3.3.5. ベーシックコースの計画

3.3.5.1. 講習等の計画

以下の要素を必ず取り込み、講習等を実施すること。

【座学・演習・アクティブラーニング】

- 制御システムセキュリティ概論
- 攻撃モニタリング・攻撃体験
- パケットキャプチャ
- 防御技術紹介・適用
- フォレンジック入門
- 防御技術
- 攻撃回避手法
- 成果報告・ディスカッション

3.3.5.2. シラバス・時間割・体制図・教材等の作成

シラバス、時間割および体制図の案を作成し、2027 年 8 月 6 日(金)までに IPA に提出すること。なお、各作成物における記載内容は以下のとおり。

＜シラバス（IPA 指定様式）＞

講習等名称と実施概要

- 実施日時と場所
- 詳細アジェンダ
- 予定講師名（外部者の場合は組織・企業名）
- 使用する教材、機材、教科書、その他参考文献、など

＜時間割＞

- 講習等名称
- 実施日時
- 実施場所
- 予定講師名（外部者の場合は組織・企業名）
- 各講習等の実施日程単位のコマ割り、など

＜体制図＞

- 「講師」と「講師補助員」の区分を明示したチーム構成図
- プロジェクトリーダーの氏名
- 予定講師名（外部者の場合は組織・企業名）
- 関連する外部業者名、など

3.3.5.3. 評価方法の設計について

ベーシックコースにおける受講者の受講結果の評価方法を設計する。評価方法は、以下に示す方法でも良いし、独自に考案した方法でも良いが、採用した方法は採用理由と

共に 2027 年 8 月 6 日(金)までに IPA に報告して承認を得ること。

- 筆記テスト等を実施した結果で評価する方法
- 講習等を実施した技能結果を客観的に評価する方法
- 受講者に予め提示した評価軸に対して講習等開始時と期間終了後とで自己申告させて評価する方法
- 講習等開始時に受講者が自ら定めた目標に対し、その達成率を自己申告させて評価する方法

3.3.6. ベーシックコースの実施

3.3.6.1. 講習等の実施

講習等では以下を実施すること。

- 3.3.5 で計画した講習等を受講者に対して実施する
- 講習等に対する受講者からの質疑に対応する
- ベーシックコースの講習等終了時に受講者に対して習熟度を確認する
- 講習等実施場所が IPA の保有する施設外の場合、受講者毎の入退室時間を記録する
- ペネトレーション手法に関しては、プログラム等による演習ツール等を用いた複数の攻撃方法を行う内容とすること。なお、演習に使用する演習ツールプログラム等は、IPA が保有する演習用模擬システムや個人演習環境の環境変化に柔軟に対応できるプログラム等とし、請負者が準備して演習等を行う

3.3.6.2. 講習等使用機材

講習等の実施では以下の条件を満たす機材を準備すること。
なお、下記については制御システムに対する攻撃／防御における初級から中級レベルの講習等が実施できる模擬システムであること。

- 重要インフラ分野や主要産業で利用される制御システム（ビル管理システム／監視カメラシステム／ガスプラント／電力送配電システム／FA 組立システム等）に関する複数の模擬システム
- ペネトレーションテストの実践やセキュリティ対策実装時の効果が検証できる制御システムに関する模擬システム
- 制御システムにおける一般的なアーキテクチャ（コントローラ・HMI・ネットワーク機能）を備えた制御システムに関する模擬システム
- サイバー攻撃を受けた際にプラントへの影響をわかりやすくするための機能を備えた制御システムに関する模擬システム

3.3.6.3. 実施報告書の作成

講習等終了時において、「2027 年度中核人材育成プログラムのベーシックコースに関する実施報告書（IT/OT 分野における検知技術・防衛技術・レジリエンス手法等）」を、「7.1 納入期限と納入物件」に記載の日程までに IPA に提出して承認を得ること。
また、同報告書は次の事項を含むこと。

- 講習等の実施結果のまとめ
  - ① 実施目的
  - ② 到達目標
  - ③ 講習等の実施概要（シラバス、時間割、体制図）
  - ④ 実施した講習等の内容が分かる資料（追加講習等も含む）
  - ⑤ 各講習等で受講者から出た主な質問
  - ⑥ 仕様書の各要件を満たしていることを確認した結果(チェックリスト)、など
- 3.3.5.3 で定めた受講者評価方法に基づく確認結果
- IPA の施設外で講習等を実施した場合の入退室記録
- ベーシックコースの講習等実施にて感じた問題点およびその改善案

3.4. アドバンスコースの設計及び実施について

3.4.1. 実施対象

2027年度産業サイバーセキュリティセンター中核人材育成プログラムに参加する60名程度の受講者のうち、前半及び後半で「OT 防御技術・ペネトレーション手法クラス」へ配属された、それぞれで最大 30 名程度の受講者を対象とする。

なお、受講者は以下の基礎知識を習得しているものとする。

- 制御システムにおけるインシデント対応手順
- インシデント発生を想定した BCP/BCM の企画立案手法
- 制御システムの管理に必要となる安全性や可用性の確保の方法
- サイバー攻撃手法を習得する意義を正しく理解できるモラル
- サイバー攻撃の脅威となる代表的な攻撃パターンや解析に関する方法
- 代表的なサイバー攻撃への適切な防御に関する知識や実装に関する方法

3.4.2. 実施場所

(1) 東京都千代田区外神田 4 丁目 14-1 秋葉原 UDX 内
(2) 東京都文京区本駒込 2-28-8 文京グリーンコートセンターオフィス内
(3) その他 IPA と請負者が協議して合意の上で定めた場所

3.4.3. 実施期間

2027 年 12 月中旬頃から 2028 年 3 月末頃の約 3 ヶ月間のうち、前半及び後半で、それぞれ IPA の指定する 20 日間以上の演習等を実施すること。また、受講者の希望を踏まえ、6 日間程度の追加講義を実施すること。なお、演習等の実施日程は、後日 IPA から指定する。

また、演習等は 90 分×4 コマ（計 6.0 時間/日）構成として、昼休み休憩（1 時間）及び授業間休憩（計 30 分）を含む 10:30～18:00 までを基本として実施する。なお、演習等の内容がハンズオン中心になることが想定されるため、演習等を担当する講師の裁量により各講習の開始及び終了時間の変更は行ってよい。

3.4.4. 到達目標

卒業プロジェクトを実行するために必要となる能力･知識の習得を目標とする。なお、これら目標の具体的な内容は受講者自らに設定させることとする。

設定する目標の一例を以下に示す。

- 制御システム等に想定外の異常が発生した際に自ら考え対処して解決する能力
- 制御システムへのサイバー攻撃に対して以下の手法等により対処する能力
  - ① コンピュータプログラミング対策
  - ② フォレンジック解析
  - ③ ネットワーク（セグメントセキュリティ）対策
  - ④ システム検知対策

3.4.5. アドバンスコースの設計

3.4.5.1. シラバス・時間割・体制図の作成について

アドバンスコースで行う演習等のシラバス・時間割・体制図、および講習コンテンツ（案）を作成し、2027 年 11 月 19 日(金)までに IPA に提出して承認を得ること。

なお、以下の内容を含めること。また、前半及び後半で演習等の内容や実施場所等が大きく異なる場合は、その旨が分かるように記載すること。

アドバンスコースで行う演習等は、ベーシックコースまでの受講者の技術レベル、取組状況、セキュリティ動向などを踏まえて設計すること。それに伴い、以下の内容に関して実施計画書から大きな変更が生じる場合は IPA と協議すること。

＜シラバス＞

- 講習等名称と実施概要
- 詳細アジェンダ

・　実施日時と場所
・　予定講師名（外部者の場合は組織・企業名）
・　使用する教材、機材、教科書、その他参考文献、など

＜時間割＞
・　講習等名称
・　実施日時
・　実施場所
・　予定講師名（外部者の場合は組織・企業名）
・　各講習等の実施日程単位のコマ割り、など

＜体制図＞
・　「講師」と「講師補助員」の区分を明示したチーム構成図
・　プロジェクトリーダーの氏名
・　予定講師名（外部者の場合は組織・企業名）
・　関連する外部業者名、など

＜講習コンテンツ（案）＞
・　目的、および概要
・　機器リスト（機器分類、用途、購入予定額など）、など

3.4.5.2. 演習等の設計

以下内容を満たす演習等を設計すること。

・　受講者 5～6 名程度で構成するグループもしくは受講者所属企業が属する業界別に構成するグループにて実施可能な内容とすること
・　演習用模擬システム及び個人演習環境[2]を活用した内容とすること。なお、演習用模擬システムは以下 10 システム等を想定する
  - 鉄鋼圧延システム
  - 機械製造システム
  - 鉄道運行管理システム
  - スマートグリッド・発電システム
  - 施設管理システム
  - 車載システム
  - 熱資源活用制御システム
  - FA システム
  - ガスプラントシステム
  - 変電所システム
・　実際に製品として販売されている機器類を利用して、受講者が属する業界に準ずる環境にて、制御システム機器に共通して存在するリスク／特定の制御システム機器にのみ存在するリスクを学習することができる内容とし、各システムおよびそのシステムへの攻撃手法、防御・検知手法に精通あるいは、以下の点に対する深い知識を持つ講師および講師補助が演習を実施すること
  - ネットワークセキュリティ
  - ロボットセキュリティ、制御システムセキュリティ
  - フォレンジック解析
  - セキュリティマネジメント
  - ペネトレーションテスト
・　受講者がハンズオンにて制御システムへのサイバー攻撃からの防御手法やペネトレーション手法に関して実践的な経験を得ることができる内容とすること
・　ペネトレーション手法に関しては、プログラム等による演習ツール等を用いた複数の攻撃方法を行う内容とすること。なお、演習に使用する演習ツールプログラム等は、IPA が保有する演習用模擬システムや個人演習環境の変化に柔軟に対応できるプログラム等とし、請負者が準備して演習等を行うこと

[2] 個人演習環境：UDX 施設内で用意されている PLC＋HMI＋ネットワーク機器で構成される最小の演習環境

・ 演習等は受講者自らが課題を検討し、確認し、考察し、対処することができる内容とすること

3.4.5.3. 演習環境の構築

・ 演習実施に必要となる電子工作機器などの消耗品類も必要となるため、演習を実施するために必要十分であり、且つ経済的合理性を考慮した数量を併せて準備すること
・ 演習環境の構築のために準備する機器について、IPA と協議の上で以下項目を含むリスト作成して提出すること（日程詳細は「7.1 納入期限と納入物件」を参照）
  ① 機器分類
  ② メーカー名称
  ③ 製品名（型番）
  ④ 購入個数／台数
  ⑤ 搬入予定日
  ⑥ 購入単価（税込） 、など
・ カリキュラムの実施において上記以外に構築する必要性がある環境がある場合には、その内容や構築数量について IPA と協議すること
・ 環境構築はアドバンスコースの開始日を目途に完了すること。但し、メーカーの在庫不足などにて納期が遅れる等の場合には、納入の時期や台数について IPA と協議すること

3.4.5.4. 受講者評価方法の設計

アドバンスコース期間終了時における受講者の受講結果の評価方法を設計する。評価方法は、以下に示す方法でもよいし、独自に考案した方法でもよいが、採用した方法は採用理由と共に 2027 年 11 月 19 日(金)までに IPA に報告して承認を得ること。

・ 受講者に予め提示した評価軸に対して講習等開始時と期間終了後とで自己申告させて評価する方法
・ 講習等開始時に受講者が自ら定めた目標に対し、その達成率を自己申告させて評価する方法

3.4.6. アドバンスコースの実施

3.4.5.1 で作成したシラバス・時間割に基づき演習等を実施すること。なお、演習等の実施内容には以下の作業が含まれる。

・ アドバンスコース演習等の進行及び受講者への演習等指導
・ 演習等で受講者から挙がった質疑への対応
・ 事前に受講者が設定した目標に対する達成度状況の確認
・ 目標未達の可能性がある受講者へのフォロー、補習の実施

3.4.7. 実施報告書の作成

(1) 実施報告書の名称

実施報告書は以下の名称にて作成すること。

「2027 年度中核人材育成プログラムのアドバンスコースに関する実施報告書（IT/OT 分野における検知技術・防衛技術・レジリエンス手法等)」

(2) 実施報告書の内容

実施報告書には以下の内容を含めること。

・ 演習等全体の実施結果まとめ
  ① 実施目的
  ② 達成目標
  ③ 演習等の実施概要（シラバス、時間割、担当講師名）
  ④ 実施した演習等の内容が分かる資料（補習等も含む）
  ⑤ 各演習等で受講者から出た主な質問 、など
・ 3.4.5.4 で定めた受講者評価方法に基づく確認結果

・　アドバンスコースの演習等実施にて感じた問題点及びその改善案

(3) 実施報告書の提出期限

「7.1 納入期限と納入物件」に記載の日程までに IPA に提出して承認を得ること。

3.5. 卒業プロジェクトについて

3.5.1. 実施対象

中核人材育成プログラムの卒業プロジェクトテーマのうち、「IT/OT 分野における検知技術・防衛技術・レジリエンス手法等」の担当講師を主担当もしくは副担当として指名したテーマを推進する受講者を対象とする。なお、担当する受講者数については、主とする実施場所に収容できる受講者数を考慮し、主担当とするテーマに属する受講者 40 名前後とするが、超過する場合には調整を行う。

なお、担当するテーマを推進する受講者はアドバンスコースにて「IT/OT 分野における検知技術・防衛技術・レジリエンス手法クラス」に配属された受講者だけではなく、同クラスに配属された受講者を 2 名以上含むグループに所属する受講者も含む。

3.5.2. 実施場所

(1) 東京都千代田区外神田 4-14-1 秋葉原 UDX 内

(2) 東京都文京区本駒込 2-28-8 文京グリーンコートセンターオフィス内

(3) その他 IPA と請負者が協議して合意の上で定めた場所

3.5.3. 実施期間

2028 年 4 月初旬頃から 6 月までの IPA の指定する日程（57 日間程度）での実施とする。

3.5.4. 到達目標

プライマリーコースからアドバンスコースまでの期間で学習した内容を活用し、受講者自らが立案した産業サイバーセキュリティに関するテーマについて個人もしくはグループで取り組み、6 月中旬頃に受講者派遣元企業が参加して実施する報告会において 20 分～30 分程度のテーマ報告、10 分程度の質疑応答に対応できること。

3.5.5. 実施内容

受講者からの質疑について、「IT/OT 分野における検知技術・防衛技術・レジリエンス手法等」の側面から応答すると共に、主担当もしくは副担当として指名された卒業プロジェクトテーマについて助言・指導を行うこと。プロジェクト期間中、最大１０プロジェクトに対して助言・指導対応にあたることができ、講師は毎日２名以上指導に当たることのできる体制を整え、適宜、アドバンスコース同様に模擬システム、および攻撃・防御手法に精通した講師の助言・指導を得られるように調整を行うこと。また、卒業プロジェクトの遂行にあたって電子工作機器などの消耗品類も必要となる場合、演習を実施するために必要十分であり、且つ経済的合理性を考慮した数量を併せて準備すること。

なお、主担当・副担当では以下に示す役割の違いがある。

【主担当】

① 卒業プロジェクト中間報告会において、担当するテーマ報告の場に出席して司会進行を務める。

② 卒業プロジェクト最終報告会において、担当するテーマ報告の場に出席して司会進行を務める。

③ 卒業プロジェクト最終報告会における担当するテーマの報告結果を踏まえて、テーマの評定・講評を行い、その結果を IPA に報告する。

【副担当】

④ 卒業プロジェクト中間報告会において、担当するテーマ報告の場に出席する。（ＴＶ会議システム等を通じた間接参加も可とする。）

⑤ 卒業プロジェクト最終報告会において、担当するテーマ報告の場に出席する。

3.5.6. 実施報告書の作成

(1) 実施報告書の名称

実施報告書は以下の名称にて作成すること。

「2027 年度中核人材育成プログラムの卒業プロジェクトに関する実施報告書（IT/OT 分野における検知技術・防衛技術・レジリエンス手法等)」

(2) 実施報告書の内容

実施報告書には以下の内容を含めること。

- 主担当として携わった卒業プロジェクトテーマの概要
  （内容については、受講者からプロジェクト概要を収集してまとめる等、具体的なとりまとめ方法は任意とする）
- 主担当として携わった卒業プロジェクトのテーマに対する評定・講評結果
  （評定･講評はテーマに携わった受講者の人数に拠らず､一律でテーマ単位に行う）
- 受講者への助言・指導の状況
- 卒業プロジェクト期間の助言・指導を通じて得た示唆・問題点・改善点
- その他、仕様書の要件を満たしていることを確認した結果、など

(3) 実施報告書の提出期限

「7.1 納入期限と納入物件」に記載の日程までに IPA に提出して承認を得ること。

3.5.7. その他

講習等以外の以下イベントについて、卒業プロジェクトを直接担当した講師の何れかが出席すること。なお､卒業プロジェクトの中間及び最終報告会については､別途､参加日程の調整を行う。

- 卒業プロジェクト中間報告会　[卒業プロジェクト期間の 3 日間程度]を想定
- 卒業プロジェクト最終報告会　[卒業プロジェクト期間の 6 日間程度]を想定
- 中核人材育成プログラム修了式典　[2028 年 6 月下旬の 1 日]を想定

3.6. その他

- 2027 年 7 月 1 日（木）に実施予定である受講者の中核人材育成プログラム開講の式典に、講師のいずれかが出席すること。なお、式典のタイムスケジュールについては IPA から別途通知するものとする。また、講師が出席できない場合は事前に IPA と協議すること。
- 2027 年 8 月下旬前後に実施を予定するベーシックコースオリエンテーションに、講師のいずれかが出席すること。なお、日程については事前に IPA と講師の間で調整を行うものとするが、講師が出席できない場合は IPA と協議すること。
- アドバンスコースにおいて、受講者が 3.4.5.2 で示した IPA が保有する演習用模擬システム以外の PA[3]系の演習用模擬システムなどでの演習実施を希望する場合、5 日間程度を目途に実施すること。
- 講習等実施場所が IPA の施設外である場合、受講者が講習等使用機材を利用した自習を行うことを考慮し、講習等終了後に施設利用時間の延長に対応できる体制を整えること。

4. 実施体制に関する要件

本業務を実施するにあたっては、次の実績及び要件を満たすこと。

4.1. 組織としての要件

- 業務の役割を定めた実働可能な人数が確保できること
- 組織として適切な管理・バックアップ体制が整えられること
- 模擬システム等を活用したサイバーセキュリティ演習を、重要インフラ事業者を対象に提供した実績を持つこと

[3] PA：Process Automation

- 産業系システムに関するシステムインテグレーションや保守の能力を有し、演習実施前後の演習用模擬システム等の設定やメンテナンスが可能であること
- 制御システム分野において、演習用テストベッド等の構築や運営の経験を有すること
- 本件の計画業務実施時に、実際の制御機器を用いた検証を実施可能な環境を有すること
- 産業系システム機器に関する保守技術を持った人材を有し、演習実施前後の模擬システムの設定等の作業を行えるティーチングアシスタント等を提供可能であること
- ネットワークトラフィック生成機能など演習に活用可能な支援ツールを有すること
- 制御システムに関連する規格の国際標準化活動に従事した実績があること
- 日本国籍を有する実施要員のみで実施体制を構築すること
- 本件にあたって、作成・変更・修正される教材等に第三者が権利を有する著作物が含まれる場合、請負者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うことが可能であること。この場合は事前に当機構に報告し、承認を得ること。
- 本件にあたって、第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争の原因が専ら当機構の責めに帰す場合を除き、請負者の責任、負担において一切を処理することが可能であること。この場合、当機構は係る紛争の事実を知ったときは、請負者に通知し、必要な範囲で訴訟上の防衛を請負者にゆだねる等の協力措置を講ずる。なお、請負者の著作又は一般に公開されている著作について、引用する場合は出典を明示するとともに、請負者の責任において著作者等の承認を得るものとし、当機構に提出する際は、その旨併せて報告するものとする。

4.2. 講師としての要件

- 制御システム・制御セキュリティ領域における防御技術やペネトレーション等に関する知識を有しており、当該分野に関する講義・演習経験者であること
- 重要インフラを題材とした産業システムのサイバーセキュリティに関する研修の提供実績を持つこと(年間 100 名程度以上)
- NIST SP 800-82、IEC 62443-2-1 などをはじめとする制御システムのセキュリティ対策規格に関する知識を有すること
- 電力・鉄道・ビルなど重要インフラの各分野のシステムに固有の制御プロトコルに関して網羅的な知識を有すること
- Stuxnet 型攻撃など制御システムに対する高度なペネトレーション手法、SIEM や計測機器を活用した実践的なフォレンジック技術について最先端の知見を有すること
- 情報システムと制御システムが接続された近代的な産業システムを対象としたサイバーセキュリティの知識を有すること
- 制御システムに対するペネトレーションテストの実施、状況の分析、防御技術の考案といった作業を実施できる能力と経験を有すること
- 非 IP 環境でのペネトレーションテストに関する演習等の講師経験があること
- 制御システムに対する高度なペネトレーション手法、SIEM や計測機器を活用した実践的なフォレンジック技術について最先端の知見を有し、それら手法を用いた演習等の講師経験があること

5. 留意事項

- 講師の旅費及び必要な機材の運搬費は請負者が負担すること。
- 請負者は、講習等の教材等を請負者の責任において本業務内で準備すること。
- 受講者が IPA の施設で講習等に使用するパソコン、インターネットアクセス回線及びマイク・プロジェクター等の設備及び演習等使用機材は IPA 又は受講者で用

意する。それ以外の機材については、請負者の費用負担で用意すること。また、講習等を行う前に必要な事前セッティングは請負者の費用負担で行うこと。

- 請負者は、本業務で使用する資料及び教材等に関し、国内外の第三者が保有する知的財産権を侵害しないことを保証すること。また、権利侵害の紛争が生じた場合（私的交渉、仲裁を含み、法的訴訟に限らない。）、請負者の費用と責任負担において、その紛争を処理解決するものとし、IPA に対し一切の負担及び損害を被らせないこと。
- 本業務内で作成する資料、ドキュメント類については、IPA 産業サイバーセキュリティセンターで定めた作成ドキュメントの共有範囲に従い表示を行うこと。作成ドキュメントの共有範囲の表示については、IPA から契約締結後に開示する。
- 定期的に IPA との進捗状況報告ミーティングを実施して、発生する課題やリスクの整理、それらの解決を図るものとし、日程及び進捗の確認方法は IPA と協議すること。本仕様書の記載内容を大きく超える実施時間への対応や受講生人数への対応が発生する見込みがある場合、費用等や運営体制について IPA と協議すること。
- 天災など、IPA および請負者の責に帰さない事由により講習等が中止となった場合、その補習の実施等について IPA と協議すること。
- 本仕様書に記載されていない事項や不明な点がある場合には、IPA と協議すること。
- 本業務では IPA と請負者の双方の秘密情報を取り扱う可能性があるため、秘密情報を取り扱う場合は、別途、秘密保持契約を締結すること。

6. セキュリティ要件

本業務では、IPA と請負者は双方以下のセキュリティ要件を遵守するものとする。

(1) 本業務のために提供された情報は、本業務の目的以外に利用しないこと。

(2) 本業務において開示された資料や情報は、秘密の保持および紛失・滅失対策に留意し、管理の責任を負うこと。

(3) 情報セキュリティを確保するための体制を定め、確認を求めた場合には速やかに報告すること。

(4) 本業務の遂行において情報セキュリティが侵害され、又はそのおそれがある場合には、速やかに必要な措置を講ずるとともに報告を行うこと。また、必要に応じて双方で協議すること。

(5) 本業務に関する情報セキュリティ対策の履行状況の確認を求められた場合には、速やかに報告すること。なお、必要に応じて事前に通知を行った上で本業務に関する情報セキュリティ対策の実施状況確認のための調査を行う場合がある。

(6) 本業務の一部を第三者に再委託する場合、第三者に請け負わせることにより生ずる脅威に対して、本要件に基づく情報セキュリティ対策が十分に確保されるか確認し、必要に応じて措置を講じること。

(7) 本業務完了又は契約解除等により、提供した紙媒体及び電子媒体（複製を含む。）が不要になった場合には、速やかに返却、もしくは破砕、溶解及び焼却等の方法により情報を復元困難かつ判読不能な方法で抹消すること。

(8) 情報管理体制

① 受注者は本事業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「情報セキュリティを確保するための体制を定めた書面（情報管理体制図」」及び「情報取扱者名簿」（氏名、住所、生年月日、所属部署、役職等が記載されたもの）を契約前に提出し、担当部門の同意を得ること。（住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当部門から求められた場合は速やかに提出すること。）なお、情報取扱者名簿は、委託業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。

（確保すべき履行体制）

契約を履行する一環として契約相手方が収集、整理、作成等した一切の情報が、ＩＰＡ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。
　ＩＰＡが個別に承認した場合を除き、契約相手方に係る親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の契約相手方に対して指導、監督、業務支援、助言、監査等を行う者を含む一切の契約相手方以外の者に対して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 本事業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ものとする。ただし、担当部門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、予め担当部門へ届出を行い、同意を得なければならない。

(9) 業務従事者の経歴

業務従事者の経歴（氏名、所属、役職、学歴、職歴、業務経験、研修実績その他の経歴、専門的知識その他の知見、母語及び外国語能力、国籍等がわかる資料）を提出すること。

※経歴提出のない業務従事者の人件費は計上不可。

(10) 履行完了後の情報の取扱い

ＩＰＡから提供した資料又はＩＰＡが指定した資料の取扱い（返却・削除等）については、担当職員の指示に従うこと。業務日誌を始めとする経理処理に関する資料については適切に保管すること。

(11) 情報管理に対する社内規則等（社内規則がない場合には代わりとなるもの）を提出すること。

(12) 本業務内でクラウドサービスを利用する場合、利活用する情報属性に応じたセキュリティ対策要件を考慮して選定すること。

7. 納入物件関連事項

以下の納入期限までに納入物件を納入すること。

7.1. 納入期限と納入物件

納入は、中間、最終の 2 回とする。

【中間納入】

- 納入期限：2028 年 3 月 31 日（金）
- 納入物件：
  - 「2027 年度中核人材育成プログラムのプライマリーコースに関する実施報告書（IT/OT 分野における検知技術・防衛技術・レジリエンス手法等）」
  - 「2027 年度中核人材育成プログラムのベーシックコースに関する実施報告書（OIT/OT 分野における検知技術・防衛技術・レジリエンス手法等）」

【最終納入】

- 納入期限： 2028 年 7 月 20 日（木）
- 納入物件：
  - 「2027 年度中核人材育成プログラムのアドバンスコースに関する実施報告書（IT/OT 分野における検知技術・防衛技術・レジリエンス手法等）」
  - 「2027 年度中核人材育成プログラムの卒業プロジェクトに関する実施報告書（IT/OT 分野における検知技術・防衛技術・レジリエンス手法等）」
  - 「アドバンスコースの演習等及び卒業プロジェクトの実施にあたり準備した機器類一式リスト及び現品写真等」
  - 「アドバンスコースの演習等及び卒業プロジェクトの実施にあたり準備した機器類一式」

機器類一式を除き、これらの電子データを収めた電子記録媒体（光学メディア等）を納入することとし、検収用としてそれぞれ紙媒体 1 部を提出すること。

7.2. 納入場所

〒113-6591
東京都文京区本駒込 2－28－8 文京グリーンコートセンターオフィス 17F
独立行政法人情報処理推進機構
産業サイバーセキュリティセンター事業部人材育成グループ

「アドバンスコースの演習等及び卒業プロジェクトの実施にあたり準備した機器類一式」については、
東京都千代田区外神田 4 丁目 14-1 秋葉原 UDX N20 階 DE

8. 検収条件

本仕様書の要件を満たした上で本仕様に定めるすべての業務が実施され、かつ納入物件に不足・不備がないこと。

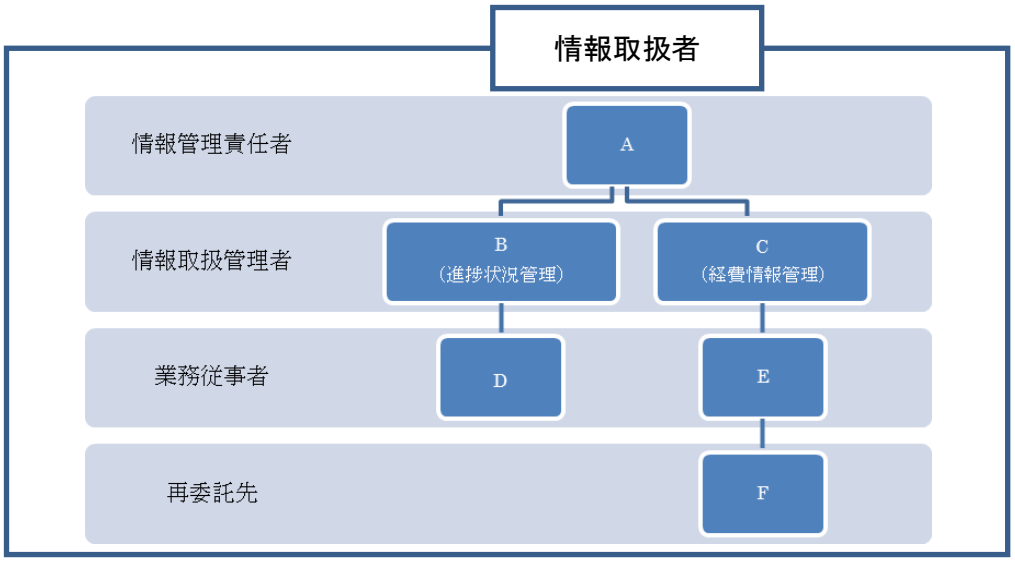
以上

【添付資料】

- 別紙1.情報管理体制図

※情報管理体制図に記載すべき事項

a. 本業務の遂行に当たって保護すべき情報を取り扱うすべての者。（再委託先も含む。）
b. 本業務の遂行のため最低限必要な範囲で情報取扱者を設定し記載すること。



- 別紙 2. 情報取扱者名簿

※情報取扱者名簿に記載すべき事項等

a. 受注者としての情報取扱の全ての責任を有する者。必ず明記すること。
b. 本業務の遂行にあたって主に保護すべき情報を取り扱う者ではないが、本業務の進捗状況などの管理を行うもので、保護すべき情報を取り扱う可能性のある者。
c. 本業務の遂行にあたって保護すべき情報を取り扱う可能性のある者。
d. 日本国籍を有する者及び法務大臣から永住の許可を受けた者（入管特例法の「特別永住者」を除く。）以外の者は、パスポート番号等及び国籍を記載。

情報取扱者名簿

		氏名	個人住所（注）	生年月日（注）	所属部署	役職	d.パスポート番号及び国籍（注）
a.情報管理責任者	A						
b.情報取扱管理者	B						
	C						
c.業務従事者	D						
	E						
再委託先	F						

（注）個人住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当部門から求められた場合は速やかに提出すること。