調達要求番号：6KXT1AA0007

陸　上　自　衛　隊　仕　様　書		
サイバー・電磁波集合教育における部外委託教育	仕　様　書　番　号	
	サ教―７	
	作　　成	令 和 ８ 年 ６ 月 ３ 日
	変　　更	
	作成部隊等名	システム通信・サイバー学校サイバー教育部

1　総則

1.1　適用範囲

この仕様書は，陸上自衛隊システム通信・サイバー学校におけるサイバー・電磁波集合教育の最新技術教育（以下，「本教育」という。）に係る役務について必要事項を規定する。

1.2　用語及び定義

この仕様書に用いる用語の定義は，次によるほか，引用文書による。

1.2.1　学生

本役務で実施する最新技術教育を受ける教育対象の者をいう。

1.2.2　講師

学生に対し講義や解説を実施する者をいう。

1.3　引用文書等

1.3.1　引用文書

この仕様書に引用する次の文書は，この仕様書に規定する範囲内において，この仕様書の一部を成すものであり，入札書又は見積書の提出時における最新版とする。ただし，契約締結後，当該文書に改正があった場合は，その適用について別途協議するものとする。

a)　仕様書

ＧＬＴ－ＣＧ－Ｚ０００００１　陸上自衛隊装備品等一般共通仕様書

1.3.2　関連文書

a)　防衛省の情報保証に関する訓令［防衛省訓令第１６０号（１９．９．２０）］

b)　陸上自衛隊の情報保証に関する達［陸上自衛隊達第６１－８号（１９．１２．１７）］

c)　防衛省の情報保証に関する訓令の運用について（通達）

［防運情第９２４８号（１９．９．２０）］

d)　装備品等及び役務の調達における情報セキュリティの確保について（通達）

［防装庁（事）第１３７号（令和４年３月３１日）］

2　業務に関する要求

2.1　役務内容

陸上自衛隊システム通信・サイバー学校サイバー教育部におけるサイバー・電磁波集合教育入校学生等に対して，演習環境を用いたサイバー教育を実施するものとする。

2.2　一般的要求事項

a)　講師による対面の教育（以下，「実習」という。）は，官側が指定する場所にて契約相手方が準備する端末と環境（以下，「実習環境」という。）を用いて実施するものとする。

b) 実習での学習内容等を定着させるため自学自習（以下，「自学自習」という。）を行うものとする。自学自習は，官側が準備する端末からインターネットを利用して実施できるものとし，契約相手方は，実習期間を含めた６カ月間において，自学自習を支援するための環境（以下，「自学自習環境」という。）を用意するものとする。

c) 契約相手方は，教育を実施後に改善事項等を官側と調整の上で取りまとめ，**箇条4**に示す教育成果報告書を官側へ提出する。

2.2.1 全般

a) 教育実施計画書の作成

1) 契約相手方は，契約後速やかに教育実施体制，教育の実施計画等を記載した教育実施計画書を作成し，官側に提出するものとする。
2) 教育実施計画書には，本教育の実施体制及び工程等を含むものとする。
3) 教育実施計画書に変更が必要な場合は，本教育全体に対する影響を調査し，官側に報告するとともに，官側と調整の上，変更を行うものとする。

b) 環境構築

1) 契約相手方は，2.2.5 に示す実習環境を構築するものとする。
2) 契約相手方は，2.2.5 に示す自学自習環境をインターネット上に用意するものとする。
3) 契約相手方は，役務を実施する際に学生が実習環境を利用できるように準備するものとする。
4) 契約相手方は，役務を終了した際に，実習環境を撤収するものとする。

c) 教育資料の作成

契約相手方は，2.4 に示す内容を教育するために必要なテキスト及びマニュアル等の資料を作成するものとする。

d) 実習の統制及び解説

1) 契約相手方は，2.3 に定める内容を学生に教育するために，対面での講義を実施するものとする。
2) 契約相手方は，2.3 項に定める実習において，実習環境の維持管理，対面での実習の統制及び実習後の解説を実施するものとする。
3) 契約相手方は，2.3 項に定める実習において，２名の講師を配置することを基本とする。

2.2.2 実施時期等

実習時期等は，次によるものとする。また，実習での学習内容を定着させるため，自学自習の支援期間を設けるものとし，細部日程は，官側との調整による。

a) 実　習

令和８年８月３日（月）から同年９月９日（水）（８月８日（土）～１６日（日）、２２日（土）、２３日（日）、２９日（土）、３０日（日）、９月５日（土）、６日（日）を除く。）の２３日間とする。

b) 自学自習の支援

令和８年８月１日から１月３１日の間

2.2.3 教育対象人数

７名（基準）とする。

2.2.4 実習実施場所

契約相手方は，陸上自衛隊システム通信・サイバー学校等が駐屯する久里浜駐屯地の敷地内において，官の指定する教場を用いて実習を実施するものとする。

2.2.5　実習及び自学自習環境

a)　実習期間に使用する環境は，次によるものとする。

1)　学生１人１台の実習を実施するための端末（以下，「実習用端末」という。）を利用できること。

2)　実習用端末を用いて実習を滞りなく実施できる数量のモバイルルーターを利用できること。

3)　実習班内の情報及びデータ共有のため，チャット等のコミュニケーションサービスが利用できること。

4)　契約相手方は，実習環境を安定的に維持できるものとする。

b)　自学自習環境は，次によるものとする。

1)　端末については，官側で用意するものとする。

2)　インターネット回線については，官側で用意するものとする。

3)　仮想環境上のシステムを操作しながら課題に取り組む，ハンズオン形式の問題（CTF 形式を含む）を中心とすること。当該問題は，単なる閲覧・説明に留まらず，受講者自身が手を動かして攻撃・検証等を行う形式であること。

4)　演習中の操作ログをシステム上で解析し，ユーザー毎のスキルレベルや特性に合った問題をシステム側で自動判別できること。

5)　自学自習環境にはＷｅｂブラウザ上でアクセスできること。

6)　演習問題並びに解説は，日本語を母語とする者が作成した，日本語として自然で理解しやすい文章で提供されること。なお，外国語で作成された文書を機械翻訳ソフト等により日本語化したものの提供は認めない。

7)　計画停止を除き，２４時間３６５日利用可能な環境を用意すること。

8)　官の担当者が学生の学習状況を確認できる機能を有すること。

9)　生成ＡＩチャットボットを活用し，問題を解くうえでの補助となる情報を提供する機能を有すること。

2.3　実習内容

実習内容は官側と調整の上，2.3.1及び2.3.2に定める要領で構成するものとする。また，教育水準は，ＩＰＡ（情報処理推進機構）の定めるＩＴスキルレベル標準のレベル３程度とする。

2.3.1　実習項目

a)　**プラットフォーム脆弱性診断（基準）**

Ｎｍａｐを利用したサーバへのスキャンやリモートプロトコルの脆弱性検証手法，ツールを利用した自動診断を学び，診断結果に基づくレポート作成演習を実施するものとする。

b)　**ＷＥＢアプリ脆弱性診断（基準）**

Ｗｅｂアプリケーションを構成する要素やセキュリティ技術，代表的な脆弱性検証方法を学び，Ｗｅｂアプリケーションに対するペネトレーション演習を実施するものとする。

c)　**ペネトレーションテスト（基準）**

Ｌｉｎｕｘ,Ｗｉｎｄｏｗｓに対する初期侵入，権限昇格，横展開，永続化といったペネトレーションの一連の流れとテクニックを学ぶものとする。

d)　**マルウェアの挙動と攻撃シナリオ（基準）**

Ｗｉｎｄｏｗｓ上で動作するマルウェアの挙動について，マルウェアが悪用するＷｉｎｄｏｗｓの機能の学習やマルウェアの攻撃シナリオ策定演習を通し理解を深められるものとする。

e)　**インシデントハンドリング（座学/演習）**

インシデントハンドリングに必要なサイバーセキュリティの基礎知識，セキュリティ機器の概要，インシデントハンドリングフローおよび対応手法について学ぶものとする。インシデントハンドリングに関連する知識や手順について講義形式で学習し，インシデントの分析および対応に必要な知識を習得するものとする。
また，そのうち1日については，セキュリティツールを使用した実践演習として，セキュリティ機器に記録されたインシデントログの分析を行い，タイムラインの作成，インシデントの対応方針の決定および対応実施を行うものとする。

f) ログ解析

ＬｉｎｕｘやＷｉｎｄｏｗｓのイベントログおよび通信ログ，ＩＤＳやＥｌａｓｔｉｃ ＳＩＥＭといったセキュリティ製品ログの解析を学ぶものとする。

2.3.2 実習後の教育成果報告書の作成

実習後１カ月以内に,以下の内容を含んだ教育成果報告書を作成する。

a) 各学生の各科目におけるスキルレベルの定量的評価

定量的評価とは,演習の正答率や演習中に実施した理解度テストの評点を以て評価すること。

b) 各学生のテクニカルスキルにおける定性的評価

学生の強み,弱みとなるテクニカルスキルに関して,講師による講評を記載すること。

c) 各学生のコンセプチュアルスキルにおける定性的評価

学生の演習時の取り組み姿勢（周囲とのかかわり方や発言量）,自学自習環境への取り組みの様子に関して,講師による講評を記載すること。

2.4 自学自習内容

2.2.5に定める環境を用意すると共に，2.4.1に定める自学自習項目を含めた演習問題を提供するものとし，細部は官側との調整による。

2.4.1 自学自習項目

a) ＩＴ基礎

Ｌｉｎｕｘコマンド操作，Ｗｉｎｄｏｗｓコマンド操作，リモートプロトコルの操作，Ｗｅｂサーバの仕組みなど，サイバーセキュリティの基礎となるＩＴ知識を学ぶ内容の問題を提供すること。

b) ペネトレーションテスト

偵察，初期侵入，内部横展開，権限昇格の一連の動きを体験できる内容の問題を提供すること。

c) Ｗｅｂアプリケーション脆弱性診断

ＸＳＳ，ＳＱＬインジェクション，ディレクトリトラバーサル，アクセス制御不備などの代表的なＷｅｂアプリケーションの脆弱性検証や，やられサイトへの攻撃検証可能な内容の問題を提供すること。

d) プラットフォーム脆弱性診断

ＳＳＨ，ＦＴＰ，ＤＮＳ，ＳＭＢなどのリモートプロトコルが稼働しているサーバに対しNmapを用いたスキャンの実践やエクスプロイトを利用した侵入を行う内容を含んだ問題を提供すること。

e) インシデントハンドリング（ログ解析）

ログファイルを解析し，攻撃活動の痕跡を特定する内容の問題を提供すること。

2.5 実施体制

2.5.1　実施体制

契約相手方は，本役務の実施に当たって次の体制を確保し，これを変更する場合には，事前に官側と協議するものとする。

a)　履行に必要な情報を取り扱うにふさわしい契約を履行する業務に従事する個人（以下，「個人従事者」という。）であること。

b)　契約相手方は，ＩＳＯ／ＩＥＣ ２７００１（ＩＳＭＳ）を取得していること。

c)　契約相手方は，日本語で資料の作成及び教育が実施できること。

d)　契約相手方は，経済産業省が定める「情報セキュリティサービス基準適合サービスリスト」に登録されている事業者を含めること。

e)　契約相手方は，過去３年以内で２０営業日以上連続して実施した研修を５回以上提供した実績を有する事業者を含めること。

f)　個人従事者は、教育実施体制に以下のいずれかの資格を有する者を１名以上含むこと。なお，同一人がすべての資格を有することを求めるものではない。

1)　情報処理安全確保支援士

2)　ＣＩＳＳＰ

3　情報保証及び秘密保全

3.1　契約相手方は，本契約の履行により直接又は間接を問わず知り得た事項の管理に万全を期すとともに，それらの部外での利用，公表等を防衛省の許可なく行ってはならない。

3.2　契約相手方は，役務作業で生じた各種資料等については，部外での利用，公表等を防衛省の許可なく行ってはならない。

3.3　契約相手方の責任に起因する情報の漏洩等により損害が発生した場合は，それに伴う弁済等の措置はすべて契約相手方が負担することとする。

3.4　この項目については，契約期間の終了後においても同様とする。

4　提出資料

提出資料は**表1**によるものとし，提出前に官側の確認を受けるものとする。

表1－提出資料

番号	提出資料	提出方式	数量	提出時期	提出先
1	実施計画書	電子媒体	１部	契約後，速やかに	サイバー教育部
2	実施体制表				
3	自学自習環境用マニュアル				
4	テキスト			各実習科目終了後	
5	教育成果報告書			終了後，１カ月(基準)	
6	実施完了報告書			契約完了までに	

5　その他

5.1　官側における支援

契約相手方は，官側の支援を必要とする場合，官側と協議の上，次の支援を受けることができる。

a)　役務に必要な官側資料等の貸与又は閲覧等

b)　役務に必要な官側施設及び機器の使用

c)　役務に必要な官側の人員による支援

d)　その他官側が必要と認めたもの

5.2　施設の立ち入り

契約相手方は，施設の立入（輸送車両の操縦手の立入含む。）については，官側の指定する申請手続きを実施し，原則として対面教育開始前日までに所要の立入申請を完了し，許可を得るものとする。

5.3　仕様書に関する疑義

契約相手方は，この仕様書の内容に関し疑義を生じた場合は，速やかに契約担当官等に対し疑義の解決又は意見の調整を得るものとする。

5.4　制限事項

教育の内容，実施要領及び教育状況等の情報共有に関しては，下請業者を含む関係者のみに限定するものとする。

.