仕　様　書

		調達要求番号	図電情処７
件名	数量	備　考	
防衛大学校共同利用電子計算機システムのセキュリティ調査役務	１式		

1　総則

(1)　適用範囲

この仕様書は、防衛大学校共同利用電子計算機システムのセキュリティ調査役務（以下、「本役務」という。）について適用する。

(2)　用語の定義

この仕様書で用いる用語の定義は、JIS X 0001～JIS X 0032によるほか、引用文書等による。

(3)　引用文書等

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なすものであり、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。

ア　引用文書

(ｱ)　法令等

防衛省の情報保証に関する訓令（平成19年防衛省訓令第160号）

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）

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263号（5.6.30）（以下「情報セキュリティ通達」という。）

情報システムに関する調達に係るサプライチェーン・リスク対応のための措置について（通達）防装庁（事）第３号（31.1.9）

情報システムに関する調達に係るサプライチェーン・リスク対応のための措置の細部事項について（通知）装プ武第188号（31.1.9）

(ｲ)　規格

ISO 9001 品質マネジメントシステム－要求事項

ISO 27001 情報セキュリティマネジメントシステム

JIS X 0001～JIS X 0032 情報処理用語

(ｳ)　仕様書

6-06-2003-341A-A-0009　防衛大学校共同利用電子計算機システム借上（06換装）仕様書（契約年月日：令和６年７月２日）（以下「現行システム」という。）

イ　関連文書

(ｱ)　法令等

著作権法（昭和45年法律第48号）

知的財産基本法（平成14年法律第122号）

リスク管理枠組み（RMF）におけるセキュリティ管理策について（通知）防整サ第14550号（5.7.3）

デジタル・ガバメント推進標準ガイドライン（2026年（令和8）6月12日　デジタル社会推進会議幹事会決定）

デジタル・ガバメント推進標準ガイドライン解説書（2026年（令和8）6月12日　デジタル庁）

デジタル・ガバメント推進標準ガイドライン実践ガイドブック（2026年（令和8年）6月12日付）

SINETネットワークサービスガイドライン（令和5年11月1日改定）

(ｲ)　技術資料

6-06-2003-341A-A-0009　防衛大学校共同利用電子計算機システム借上（06換装）（契約年月日：令和6年7月2日）要件定義書

図電情処4　セキュリティ監視支援役務（契約年月日：令和5年6月12日）

2　一般事項

契約相手方は、本役務の履行にあたり、本仕様書に記載する事項の全てを行わなければならない。

3　役務に関する要求

(1)　概　要

本役務は、防衛大学校共同利用電子計算機システムにおけるセキュリティ課題等の調査、抽出を行い、セキュリティ課題等に対する改善策の調査及び検討を行うものである。

(2)　役務内容

役務の内容は次のとおりとする。

ア　実施計画書の作成

契約相手方は、契約締結後、速やかに実施計画書を作成すること。実施計画書には、作業概要、作業体制、スケジュール、会議体、進捗管理、コミュニケーション管理、情報セキュリティ等を含めること。

実施計画書は、実施計画説明会において官側に説明し、官側の同意を得た後、1部を提出すること。

イ　セキュリティ検討

契約相手方は、表1のセキュリティ検討を実施すること。

表1　セキュリティ検討

番号	項目	内容
1	現行システムの用途、利用形態、接続先等の整理	官側が提供する情報を基に、現行システムの教研系システム（SINET）、研究系システム（WIDE）、事務系システム（DII部内）及び事務系システム（DII部外）（以下、「サブシステム」

		という。）が保有する機能、機能毎の利用者、用途、利用形態、連接するシステム・ネットワーク、接続方法等を調査し、セキュリティ検討の前提情報として整理する。
2	現行システムのセキュリティ課題等の調査及び抽出	番号１を基にサブシステム毎にセキュリティ対策状況等を調査し、現行システムにおけるセキュリティ上の課題やリスクを抽出する。
3	外部提供サービスの活用におけるセキュリティ課題等の調査及び抽出	番号１の結果を踏まえ、サブシステム毎或いは機能毎に外部提供サービスを活用する場合に想定されるセキュリティ上の課題やリスクを抽出する。
4	セキュリティ課題等に対する改善策の検討	番号２及び番号３で抽出したセキュリティ課題等への改善策（案）を検討する。
5	外部提供サービスのセキュリティ検討	代表的な外部提供サービス（複数）について、セキュリティ機能、利用方式、責任分界方式、監査ログ管理等の観点から比較検討を行う。
6	セキュリティ等の影響度及び費用対効果の検討	官側において集約するシステム利用者要望及び課題並びに番号１～５までの調査、検討結果を踏まえて対応すべき課題について、対応する場合の影響度及び費用対効果を整理し、優先順位付けの支援を行う。なお、検討に当たっては、広く浸透している分析手法やビジネスフレームワーク等を用いて、客観性及び透明性を確保すること。

ウ　成果報告書の作成

契約相手方は、前記（2）イの検討結果として、成果報告書を作成すること。

成果報告書は、成果報告会において官側に説明し、官側の同意を得た後、１部を提出すること。

エ　役務期間

契約締結日から令和９年３月１９日までとする。

オ　役務実施場所

契約相手方の事業所及び官側の指定する場所とする。

4　役務の実施体制

(1)　契約相手方の要件

契約相手方の要件は、次による。

ア　契約の相手方は、日本国内に本社を有すること。

イ　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「役務従事者」という。）を確保できること。

ウ　防衛省において、プロジェクト管理業務及び官側の業務に係る技術支援の元請けとしての契

約実績を有すること。

エ　防衛省において、情報システムの整備における企画から予算要求、調達の工程業務に係る教材作成及び教育実施の元請けとしての契約実績を有すること。

オ　防衛省において、外部提供サービス移行に係る支援業務の元請けとしての契約実績を有すること。

カ　防衛省において、体系的に構築されたネットワークへの加入に係る支援業務の元請けとしての契約実績を有すること。

キ　防衛省におけるリスク管理枠組みに係る支援業務の元請けとしての契約実績を有すること。

ク　品質管理体制について、ISO9001の認証を取得していること。

ケ　情報セキュリティ体制について、ISO27001又はこれと同等の認証を取得していること。

コ　現行システムの技術資料等を利用できる知見を有すること。

(2)　役務従事者

契約相手方は、契約締結後速やかに、以下の要件を満たす役務従事者名簿を作成し、官側に提出すること。また、役務従事者の中から実施責任者を１名指定すること。

役務従事者の要件は、次による。

ア　実施責任者は、以下の資格のいずれか又は同等の能力（防衛省の情報システムに関連したプロジェクトに直近８年以内に３件以上従事した経験・実績、又は防衛省のプロジェクトに通算８年以上従事した経験等）を有すること。

(ｱ)　情報処理技術者試験（プロジェクトマネージャ）

(ｲ)　Project Management Professional

イ　全役務従事者（実施責任者を含む。）を通じて、以下の全ての資格を有すること。

(ｱ)　Certified Information Systems Security Professional (CISSP)

(ｲ)　Certified Information Systems Auditor (CISA)

(ｳ)　情報処理安全確保支援士

(ｴ)　AWS Certified Solutions Architect - Professional

(ｵ)　Google Cloud Professional Cloud Architect

(ｶ)　Microsoft Certified: Azure Solutions Architect Expert

5　提出書類

提出書類は表２による。

表２　提出書類

番号	名称	数量	提出時期	提出先	備考
1	役務従事者名簿	１部	契約締結後、速やかに	防衛大学校	電子データ
2	実施計画書	１部	契約締結後、速やかに	防衛大学校	電子データ
3	成果報告書	１部	納期までに	防衛大学校	電子データ

6　成果物の帰属

成果物の権利の帰属はすべて官側のものとし、契約相手方は、官側が承諾した場合を除き、成果物を公表してはならない。

7　貸付図書

契約相手方は、官側と調整することにより、必要な資料を無償で貸与を受けることができるものとする。ただし、官側が保有する資料の貸与を受けた場合、取り扱いに留意し、法令及び関連規則等に従い、官側が指定する条件を遵守するものとする。

8　情報保証

防衛省の情報保証に関する訓令及び防衛省の情報保証に関する訓令の運用について（通達）を適用するものとする。

9　情報保全

契約相手方は、本契約の履行に際し知り得た保護すべき情報（情報セキュリティ通達第２項第１号に規定する情報をいう。）その他の非公知の情報（以下「保護すべき情報等」という。）の取り扱いに当たっては、情報セキュリティ通達における添付資料「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関する特約条項」及び別紙「装備品等及び役務の調達における情報セキュリティ基準」に基づき（保護すべき情報に該当しない非公知の情報にあっては、これらに準じて）、適切に管理するものとする。この際、特に、保護すべき情報等の取扱いについては、次の履行体制を確保し、これを変更した場合には、遅滞なく官に通知するものとする。

(1)　契約を履行する一環として契約相手方が収集、整理、作成等した情報が、官側が保護を要さないと確認するまでは保護すべき情報（情報セキュリティ通達第５項第４号の規定に基づく解除をしようとする場合に、同号に規定する確認を行うまでは保護すべき情報として取り扱うものとする。）として取り扱われることを保障する履行体制

(2)　官の同意を得て指定した取扱者以外の者に取り扱わせないことを保障する履行体制

(3)　官が書面により個別に許可した場合を除き、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障する履行体制

(4)　保護すべき情報については、情報セキュリティ指定書による。

10　第三者に係る取り扱い

(1)　契約相手方が自己以外の第三者を当該契約の遂行上、業務に従事させる場合は、情報システムに関する調達に係るサプライチェーン・リスク対応のための措置について（通達）及び情報システムに関する調達に係るサプライチェーン・リスク対応のための措置の細部事項について（通知）に基づく特約条項によるもののほか、官側の指示に従うものとする。

(2)　契約相手方は、本契約の履行に当たり知り得た知識を第三者に漏えい又は他に転用してはなら

ない。

11　入札制限

本役務の遂行にあたり、公正性確保、利益相反防止、相互牽制作用等の確保及び役務内容の重複を避けるための観点から、契約の相手方は、次の事項に該当する事業者（子会社、親会社又は実質的に支配関係にあると認められる事業者を含む。）であってはならない。

(1)　防衛大学校共同利用電子計算機システムに係る借上・保守業務、データ移行業務及び運用支援業務の各受託事業者

(2)　防衛省の各機関共同事業であるリスク管理枠組みの円滑な運用を確保するための運用支援及び教育支援役務、リスク管理枠組みの統一的な制度運用を確保するための支援役務（申請・計画）又はリスク管理枠組みの統一的な制度運用を確保するための支援役務（認証・監査）の受託事業者

12　その他

本仕様書に記載のない事項が発生した場合は、両者の協議により決定する。