令和７年１２月１９日　　支担官第６８７号

支出負担行為担当官
防衛省大臣官房会計課
会計管理官　平下　一三
（公　印　省　略）

公　　告

下記により入札を実施するので、入札心得及び契約条項等を了承の上、参加されたい。
なお、本入札に係る落札及び契約締結は、当該業務に係る令和８年度本予算が成立し、予算示達がなされることを条件とするものである。

記

１．入札に付する事項

調達番号	件名	内容	履行場所	履行期間
R8-S-0009	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）	仕様書のとおり	仕様書のとおり	自：契約締結日 至：令和９年３月３１日

２．入札方式　　一般競争入札（総合評価落札方式、電子調達システム（政府電子調達（ＧＥＰＳ））対象案件）

３．入札日時　　令和８年３月１３日(金)　（１０：４５）

４．入札場所　　防衛省市ヶ谷庁舎Ｅ２棟３階入札室

５．参加資格　（１）予算決算及び会計令第７０条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。
（２）予算決算及び会計令第７１条の規定に該当しない者であること。
（３）令和07・08・09年度防衛省競争参加資格（全省庁統一資格）「役務の提供等」のＣ等級以上に格付けされ、関東・甲信越地域の競争参加資格を有するもの。
（４）防衛省から「装備品等及び役務の調達に係る指名停止等の要領」に基づく指名停止の措置を受けている期間中の者でないこと。
（５）前号により、現に指名停止を受けている者と資本関係又は人的関係のある者であって、当該者と同種の物品の売買又は製造若しくは役務請負について防衛省と契約を行おうとする者でないこと。
（６）上記（３）の等級かかわらず、防衛省所管契約事務取扱細則（平成１８年防衛庁訓令第１０８号）第１８条第４項各号のいずれかに該当する者（具体的には、以下ア～キのいずれかに該当する者）であること。なお、要件に該当する者で入札に参加しようとするものについては、　令和８年　１月　７日　（水）　１２：００　までに下記ア～キに記載する書類等を防衛省大臣官房会計課契約係へ提出すること。

ア　当該入札に係る物品と同等以上の仕様の物品を製造した実績等を証明できる者

イ　資格審査の統一基準により算定された総合審査数値に以下の技術力の評価の数値を加算した場合に、当該入札に係る等級に相当する数値となる者

項　目	基　準	数　値
入札物品等（訓令第１８条第４項に規定する契約の対象となる物品又は役務をいう。以下同じ）に関連する特許保有件数	３件以上 ２件 １件	15 10 5
入札物品の製造等（訓令第１８条第４項に規定する契約の対象となる物品の製造又は役務の提供等をいう。以下同じ）に携わる技術士資格保有者数	９人以上 ７～８人 ５～６人 ３～４人 １～２人	15 12 9 6 3
入札物品の製造等に携わる技能認定者数（特級、一級、単一級）	11人以上 ９～10人 ７～８人 ５～６人 ３～４人 １～２人	6 5 4 3 2 1

注：１　特許には、海外で取得したものを含む。

２　技術士には、技術士と同等以上の科学技術に関する外国の資格のうち文部科学省令で定めるものを有する者であって、技術士の業務を行うのに必要な相当の知識及び能力を有すると文部科学大臣が認めたものを含む。

ウ　ＳＢＩＲ制度の特定新技術補助金等の交付先中小企業者等であり、当該入札に係る物品又は役務に関する分野における技術力を証明できる者

エ　株式会社産業革新投資機構、独立行政法人中小企業基盤整備機構、株式　会社地域経済活性化支援機構、株式会社農林漁業成長産業化支援機構、株式会社民間資金等活用事業推進機構、官民イノベーションプログラム、株式会社海外需要開拓支援機構、一般社団法人環境不動産普及促進機構における耐震・環境不動産形成促進事業、株式会社日本政策投資銀行における特定投資業務、株式会社海外交通・都市開発事業支援機構、国立研究開発法人科学技術振興機構、株式会社海外通信・放送・郵便事業支援機構、一般社団法人グリーンファイナンス推進機構における地域脱炭素投資促進ファンド事業及び株式会社脱炭素化支援機構の支援対象事業者又は当該支援対象事業者の出資先事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

オ　国立研究開発法人（科学技術・イノベーション創出の活性化に関する法律（平成２０年法律第６３号）第２条第９項に規定する研究開発法人のうち、同法別表第３に掲げるものをいう。）が同法第３４条の６第１項の規定により行う出資のうち、金銭出資の出資先事業者又は当該出資先事業者の出資先事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

カ　国立研究開発法人日本医療研究開発機構による「創薬ベンチャーエコシステム強化事業（ベンチャーキャピタルの認定）」又は国立研究開発法人新エネルギー・産業技術総合開発機構による「研究開発型スタートアップ支援事業（ベンチャーキャピタル等の認定）」において採択された者の出資先事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

キ　グローバルに活躍するスタートアップを創出するための官民による集中プログラム（Ｊ－Ｓｔａｒｔｕｐ又はＪ－Ｓｔａｒｔｕｐ地域版）に選定された事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

６．入札方法　　落札決定に当たっては、入札書に記載された金額に当該金額の１０％に相当する額を加算した額（当該金額に１円未満の端数があるときは、その端数金額を切り捨てるものとする。）をもって落札価格とするので、入札者は、消費税等に係る課税事業者であるか免税業者であるかを問わず、見積もった契約金額の１１０分の１００に相当する金額を入札書に記載すること。

７．入札保証金及び契約保証金　　免　除

８．入札の無効　　５の参加資格のない者のした入札または入札に関する条件に反した入札は無効とする。

９．契約書作成の要否　　要

10．適用する契約条項　　役務等契約条項、談合等の不正行為に関する特約条項、
暴力団排除に関する特約条項、
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
情報システムの調達に係るサプライチェーン・リスク対応に関する特約条項

11．その他
（１）細部入札要領については別途配布する「一般競争入札の案内について」（以下、入札案内）のとおり。
（２）入札案内受領の際、資格審査結果通知書（全省庁統一資格）の写しを提示すること。
（３）原則、現に指名停止を受けている者の下請負については認めないものとする。ただし、真にやむを得ない事由を防衛省が認めた場合には、この限りではない。
（４）入札に関する条件　仕様書3.3.2 e)～f)に定める本業務の実施体制並びに
仕様書6.6.1 b) 1)～3) に定める契約の履行体制に関する資料を提出し、
適合すると認められること
（提出期限：令和８年　１月　９日（金）　１２：００　必要に応じ追加資料の提出を求めることがある。）。
（４）この一般競争（総合評価落札方式）に参加を希望するものは、応札資料作成要領に定める提出物を　令和８年　１月　２８日（水）　１２：００　までに提出しなければならない。

（５）契約締結日までに令和８年度予算（暫定予算を含む。）が成立しなかった場合は、契約締結日は本予算が成立した日以降とする。また、暫定予算となった場合、全体の契約期間に対する暫定予算の期間分のみの契約とする場合がある。
（６）本案件は、府省共通の「電子調達システム」（https://www.p-portal.go.jp）を利用した応札及び入開札手続により実施するものとする。ただし、電子調達システムによりがたい者は、「紙」による入札書等の提出も可とするが、郵便入札については、 令和８年　３月 １１日 （水）までに、下記担当者必着分を有効とする。
（７）落札者が、１０に掲げる契約条項のほか、中小企業信用保険法第２条第１項に規定する中小企業者である場合は、「債権譲渡制限特約の部分的解除のための特約条項」を別途適用する。
（８）入札案内の交付場所、契約条項を示す場所及び問合せ先
〒162-8801　東京都新宿区市谷本村町５－１　（庁舎Ａ棟10階）※顔写真付の身分証明書を持参すること。
受付時間　９：３０～１８：１５（１２：００～１３：００までの間を除く）

また、入札案内のメール配布を希望する者は、以下のとおりメールを送信すること。
メールアドレス：naikyoku_chotatsu_mailmagazine@ext.mod.go.jp
メール件名　　：「件名：○○○」　入札案内送信依頼
添付ファイル　：資格審査結果通知書（全省庁統一資格）の写し
防衛省大臣官房会計課契約係　河野　電話　03-3268-3111　内線20822

仕様書			
件　名	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）	作成年月日	令和７年１２月５日
		仕様書番号	
		整備計画局サイバー整備課	

1. 総則

1.1　適用範囲

この仕様書は、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（申請・計画）（以下「本役務」という。）について規定する。

1.2　用語の定義

本仕様書における用語は、各関連文書に規定するもののほか、次に掲げるとおりとする。

a)　リスク管理枠組み　Risk Management Framework（以下「ＲＭＦ」という。）のことを指し、情報システムのセキュリティに対するリスクの管理を適切に行うための枠組みをいう。

1.3　引用文書等

この仕様書に引用する以下の文書は、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、役務開始時における最新版を適用するものとする。なお、引用文書が定める事項がこの仕様書の内容と異なる場合は、この仕様書の内容を優先する。ただし、原文が日本語以外の言語かつ日本語訳文があるものであって、原文と日本語訳文に差異がある場合は原文を優先するものとする。

a)　引用文書

1)　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）（以下「訓令」という。）

2)　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）（以下「運用通達」という。）

3)　リスク管理枠組み（ＲＭＦ）におけるセキュリティ管理策（令和 5 年 7 月 3 日情報保証統括責任者）（以下「セキュリティ管理策」という。）

4)　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）（以下「情報セキュリティ通達」という。）

5)　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）

6)　環境物品等の調達の推進に関する基本方針（令和 7 年 1 月 28 日閣議決定）

7)　NIST SP 800-37 Rev.2

8)　NIST SP 800-53 Rev.5

b)　関連文書

1)　情報システムにおけるリスク管理枠組み（ＲＭＦ）実施要領（令和 6 年 11 月 20 日情報保証統括責任者）

2)　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）

3)　IT 利用装備品等及び IT 利用装備品等関連役務の調達におけるサプライチェーン・リスクへの対応について（通知）（装管調第 807 号。令和 3 年 1 月 21 日）

4)　IT 利用装備品等及び IT 利用装備品等関連役務の調達におけるサプライチェーン・リスクへの対応に関する事務処理要領ついて（通知）（装管調第 808 号。令和 3 年 1 月 21 日）

5)　国等による環境物品等の調達の推進等に関する法律（平成 12 年法律第 100 号）

6) 著作権法（昭和 45 年法律第 48 号）
7) IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ（平成 30 年 12 月 10 日関係省庁申合せ）
8) デジタル・ガバメント推進標準ガイドライン（2025 年（令和 7 年）5 月 27 日デジタル社会推進会議幹事会決定）
9) 防衛省における標準ガイドラインの適用について（平成 27 年 3 月 31 日防衛省行政情報化推進委員会決定）
10) サイバーセキュリティ戦略（令和 3 年 9 月 28 日閣議決定）
11) 政府機関等のサイバーセキュリティ対策のための統一規範（令和 7 年 6 月 27 日サイバーセキュリティ戦略本部決定）
12) 政府機関等のサイバーセキュリティ対策のための統一基準（令和 7 年度版）（令和 7 年 6 月 27 日サイバーセキュリティ戦略本部）
13) 政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）（令和 7 年 7 月 1 日サイバーセキュリティ戦略本部）
14) 政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書（令和 7 年 7 月内閣官房国家サイバー統括室）
15) NIST SP 800-18 Rev.1
16) NIST SP 800-30 Rev.1
17) NIST SP 800-39
18) NIST SP 800-53A Rev.5
19) NIST SP 800-137
20) FIPS 199
21) FIPS 200
22) CNSSI No.1253
23) DoDI 8510.01

2. 役務に関する要求

2.1 役務の目的

防衛省・自衛隊においては、米国のセキュリティ基準を参考に防衛省の情報保証訓令等の改正を行い令和５年度からＲＭＦを導入し、全省的に情報システムのライフサイクル全般を通じたセキュリティ強化の取り組みを進めている。情報システム情報保証責任者が実施する運用承認の申請業務やリスク分析・評価の計画・実施業務は、ＲＭＦの考え方に基づき実施することとなるが、その業務を行うにあたってはＲＭＦに係る専門的な知見が必要となる。そこで、本役務は、防衛省全体として本制度の統一的な運用を確保し、業務が遅滞なく円滑に遂行できるようにするため情報システム情報保証責任者が実施する業務の支援を行うことを目的とする。

2.2 実施場所、役務期間

2.2.1 実施場所

防衛省市ヶ谷地区及び防衛省・自衛隊並びに防衛装備庁の所在地又は契約相手方の執務場所とする。

2.2.2 役務期間

契約締結日から令和９年３月３１日（水）までとする。

2.3 役務実施スケジュール

本役務の実施スケジュール（基準）を**図－１**に示す。

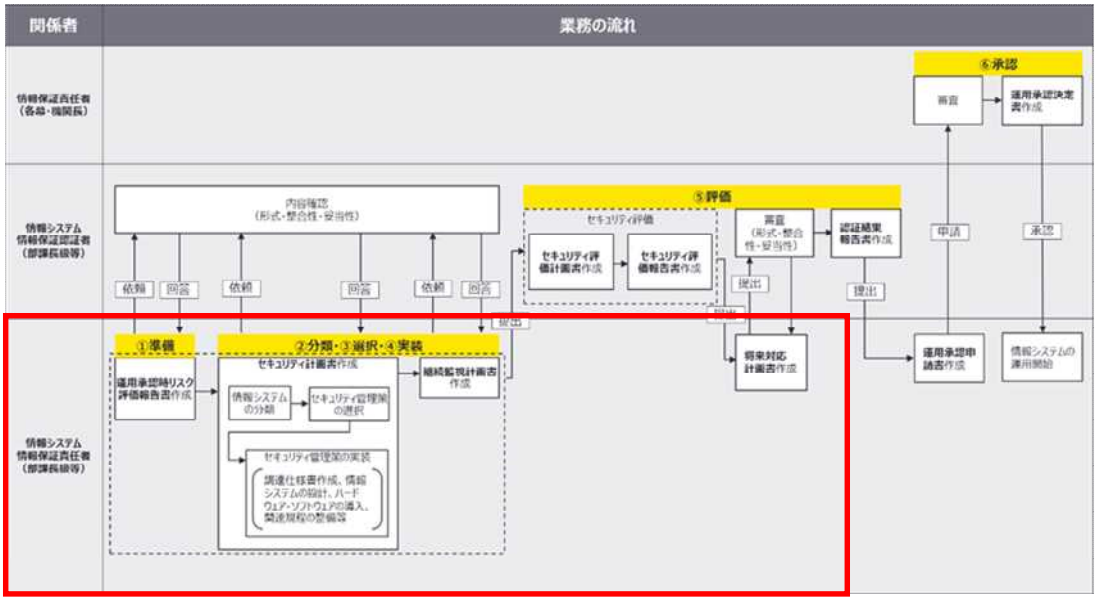
図-１　役務実施スケジュール（基準）

	１／四半期			２／四半期			３／四半期			４／四半期		
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
実施計画書作成												
役務員への教育												
対象情報システムの把握												
運用承認に係る支援												
リスク分析・評価支援												
脆弱性検査に係る支援												
継続監視に係る支援												

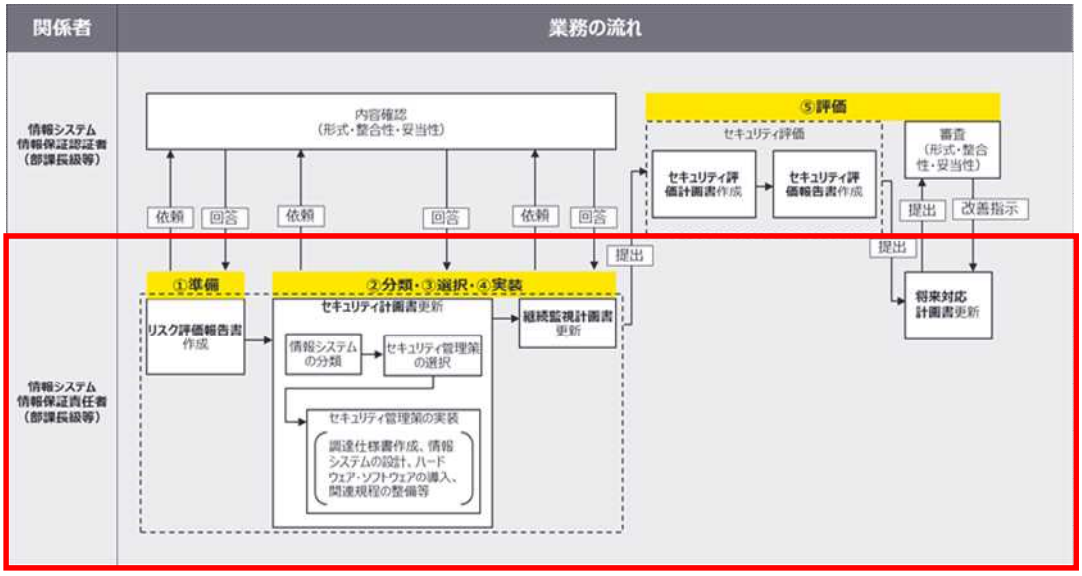
2.4　各業務の実施フロー

ＲＭＦで実施する各業務の実施フローを**図－２**から**図－４**までに示す。
なお、本役務による支援の対象範囲は赤枠内の業務とする。

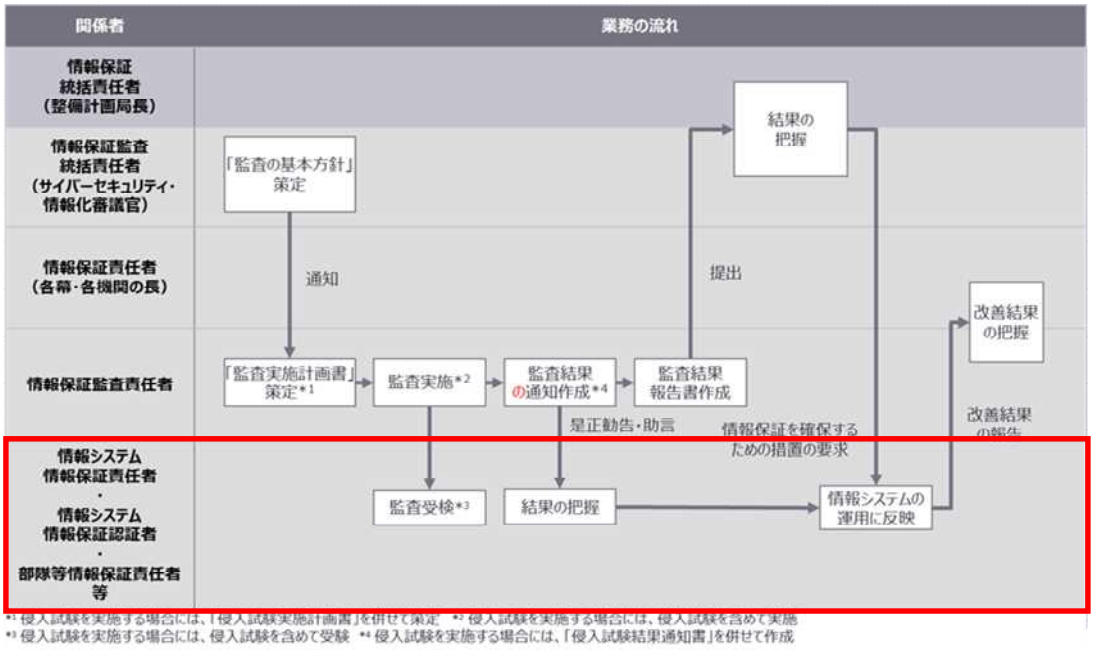
図－２　運用承認業務フロー



図－３　リスク分析・評価業務フロー



図－４　監査業務フロー



2.5　対象システム数

本役務の各業務において支援の対象となるシステム数は令和７年１１月１日時点で概ね**表１**のとおり。なお、対象システム数は**表１**に対して変動する可能性がある。

表１　対象システム数

項　目		システム数
運用承認支援		642
リスク分析・評価支援	リスク評価報告書（簡易版）	1,217
	リスク評価報告書（携帯電話版）	30
	リスク評価報告書（後続評価）	336
継続監視結果支援		336
脆弱性検査結果対応支援（机上試験を含む）		270
監査支援		90
侵入試験支援（机上試験を含む）		22
合　計		2,943

2.6　役務実施事項

2.6.1　実施計画書等の作成

2.6.1.1　実施計画書の作成

本契約の締結後、契約相手方は、前期役務事業者が作成した引継ぎ資料を踏まえ、本役務を実施するために必要な作業の洗い出しを行い、実施計画書を作成し、官側と協議の上、提出すること。

2.6.1.2　実施体制表の作成

本契約の締結後、契約相手方は、本役務を実施するための体制整備を行い、実施体制表を作成し、官側と協議の上、提出すること。また、実施体制に変更が生じる場合は、遅滞なく官側と協議を行い、変更後の実施体制表を提出すること。なお、運用承認業務及び情報保証監査業務の公平性を確保するため情報システム情報保証認証者及び情報保証監査責任者との客観性・公平性を担保する体制とすること。

2.6.2　進捗管理

作業全体及び各業務の進捗を把握できる進捗管理表を作成し、本役務の進捗状況、内容等について管理を行い、月１回を基準として官側に報告すること。

2.6.3　ＲＭＦに係る役務員への教育

役務従事者が防衛省の情報保証関連規則及びＲＭＦ関連業務に係る理解を深めることができる教育資料の作成を行い、官側と協議の上、役務員に教育を実施すること。

2.6.4　対象情報システムの把握

契約相手方は、本役務を実施する上で必要となる対象情報システムについての情報を把握するための方法について官側と協議の上、対象情報システムについての情報を把握すること。

2.6.5　運用承認に係る支援

2.6.5.1　運用承認時リスク評価報告書の作成に係る支援

官側が運用承認を取得する際に運用承認時リスク評価報告書を用いて実施するリスク分析・評価において、次のa)及びb）についての支援を行うこと。

a)　リスク分析・評価の準備に係る支援

1)　リスク分析・評価を実施する上での想定や制限の特定作業

官側が行うリスク分析・評価を実施する上での想定や制限の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

2)　情報源の特定作業

官側が行う記述的情報（例えば、情報システムで採用される技術や、その情報システムが運用される環境、他の情報システムとの接続、共通インフラ・サービスに対する依存などに関する説明）、脅威、脆弱性や影響に関する情報源の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

b) **リスク分析・評価の実施に係る支援**

1) **脅威源の特定作業**

官側が行う懸念される脅威源、脅威源の特徴の特定・分析作業において、特に情報セキュリティの観点から脅威源の妥当性等について専門的な知見による官側への助言等の支援を行うこと。

2) **脅威事象の特定作業**

官側が行う起こり得る脅威事象及び事象間の相互関係性等の特定作業において、特に複数の脅威源が単一の脅威事象を引き起こす場合、単一の脅威源が複数の脅威事象を引き起こす場合などの観点から専門的な知見による官側への助言等の支援を行うこと。

3) **脆弱性と素因的条件の特定作業**

官側が行う特定した脅威源と、その脅威源によりもたらされる可能性のある脅威事象に対して当該システムにどのような脆弱性があるか、どの程度脆弱であるかの分析作業において、専門的な知見による官側への助言等の支援を行うこと。

4) **リスクと関連するセキュリティ管理策の特定**

官側が行う脅威源・脅威事象及び脆弱性・素因的条件に対応するセキュリティ管理策の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

5) **発生可能性の特定作業**

官側が行う脅威事象の発生可能性と負の影響を及ぼす可能性等の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

6) **影響の特定作業**

官側が行う負の影響の特定及び重大さの分析作業において、専門的な知見による官側への助言等の支援を行うこと。

2.6.5.2 **セキュリティ計画書の作成に係る支援**

a) **情報システムのセキュリティ管理策の選択及び実装方法の特定に係る支援**

リスク分析・評価の結果及びセキュリティ分類に基づいて官側が行うセキュリティ管理策の選択及びセキュリティ管理策の実装方法の特定作業において、専門的知見による官側への助言等の支援を行うこと。

2.6.5.3 **継続監視計画書の作成に係る支援**

a) **継続監視の実施要領の策定に係る支援**

1) **データをサンプリングする範囲の設定作業**

官側が行うデータをサンプリングする際の管理策、評価方法、評価対象の名称の設定作業において、専門的知見による官側への助言等の支援を行うこと。

2) **継続監視のための指標と監視頻度の設定**

官側が行うリスクを評価、管理するための管理策の評価に用いる指標の決定、そのリスク許容度、指標の監視頻度の設定作業において、専門的知見による官側への助言等の支援を行うこと。

3) **継続監視で得られた情報の収集方法の設定作業**

官側が行う情報の収集方法、保管方法、分析方法等の設定作業において、専門的知見による官側への助言等の支援を行うこと。

2.6.5.4 **将来対応計画書の作成に係る支援**

セキュリティ評価計画書に基づき情報システム情報保証認証者が行ったセキュリティ管理策の分析・評価で確認された未準拠のセキュリティ管理策についての対策及び計画の策定

作業において、専門的知見による官側への助言等の支援を行うこと。

2.6.6　継続監視計画書に基づく分析・評価に係る支援

1)　継続監視から得られた結果の分析に係る支援

監視から得られた結果がリスク許容度の範囲内にあるか、また、脆弱性が組織全体／任務・業務プロセス／情報システムに与える潜在的な影響等の観点から官側が行う分析作業において、専門的知見による官側への助言等の支援を行うこと。

2)　セキュリティ管理策の有効性の評価に係る支援

官側が行う継続監視の分析結果に基づくセキュリティ管理策の有効性の評価作業において、専門的知見による官側への助言等の支援を行うこと。

2.6.7　リスク分析・評価に係る支援

2.6.7.1　リスク評価報告書（簡易版）の作成に係る支援

リスク評価報告書（簡易版）を用いて官側が行うリスク分析・評価において、次の a)及び b）についての支援を行うこと。

a)　リスク分析・評価の準備に係る支援

1)　リスク分析・評価を実施する上での想定や制限の特定作業

官側が行うリスク分析・評価を実施する上での想定や制限の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

2)　情報源の特定作業

官側が行う記述的情報（例えば、情報システムで採用される技術や、その情報システムが運用される環境、他の情報システムとの接続、共通インフラ・サービスに対する依存などに関する説明)、脅威、脆弱性や影響に関する情報源の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

b)　リスク分析・評価の実施に係る支援

1)　脅威源の特定作業

官側が行う懸念される脅威源、脅威源の特徴の特定・分析作業において、特に情報セキュリティの観点から脅威源の妥当性等について専門的な知見による官側への助言等の支援を行うこと。

2)　脅威事象の特定作業

官側が行う起こり得る脅威事象及び事象間の相互関係性等の特定作業において、特に複数の脅威源が単一の脅威事象を引き起こす場合、単一の脅威源が複数の脅威事象を引き起こす場合などの観点から専門的な知見による官側への助言等の支援を行うこと。

3)　脆弱性と素因的条件の特定作業

官側が行う特定した脅威源と、その脅威源によりもたらされる可能性のある脅威事象に対して当該システムにどのような脆弱性があるか、どの程度脆弱であるかの分析作業において、専門的な知見による官側への助言等の支援を行うこと。

4)　リスクと関連するセキュリティ管理策の特定

官側が行う脅威源・脅威事象及び脆弱性・素因的条件に対応するセキュリティ管理策の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

5)　発生可能性の特定作業

官側が行う脅威事象の発生可能性と負の影響を及ぼす可能性等の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

6)　影響の特定作業

官側が行う負の影響の特定及び重大さの分析作業において、専門的な知見による官側への助言等の支援を行うこと。

2.6.7.2　リスク評価報告書（携帯電話版）の作成に係る支援

携帯電話（スマートフォン含む）に対してリスク評価報告書（携帯電話版）を用いて官側

が実施するリスク分析・評価において、専門的な知見による官側への助言等の支援を行うこと。

2.6.7.3　リスク評価報告書を用いて実施するリスク分析・評価

2.6.7.3.1　リスク評価報告書の作成に係る支援

リスク評価報告書を用いて官側が実施するリスク分析・評価において、次のa)及びb）についての支援を行うこと。

a)　リスク分析・評価の準備に係る支援

1)　リスク分析・評価を実施する上での想定や制限の特定作業

官側が行うリスク分析・評価を実施する上での想定や制限の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

2)　情報源の特定作業

官側が行う記述的情報（例えば、情報システムで採用される技術や、その情報システムが運用される環境、他の情報システムとの接続、共通インフラ・サービスに対する依存などに関する説明)、脅威、脆弱性や影響に関する情報源の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

b)　リスク分析・評価の実施に係る支援

1)　脅威源の特定作業

官側が行う懸念される脅威源、脅威源の特徴の特定・分析作業において、特に情報セキュリティの観点から脅威源の妥当性等について専門的な知見による官側への助言等の支援を行うこと。

2)　脅威事象の特定作業

官側が行う起こり得る脅威事象及び事象間の相互関係性等の特定作業において、特に複数の脅威源が単一の脅威事象を引き起こす場合、単一の脅威源が複数の脅威事象を引き起こす場合などの観点から専門的な知見による官側への助言等の支援を行うこと。

3)　脆弱性と素因的条件の特定作業

官側が行う特定した脅威源と、その脅威源によりもたらされる可能性のある脅威事象に対して当該システムにどのような脆弱性があるか、どの程度脆弱であるかの分析作業において、専門的な知見による官側への助言等の支援を行うこと。

4)　リスクと関連するセキュリティ管理策の特定

官側が行う脅威源・脅威事象及び脆弱性・素因的条件に対応するセキュリティ管理策の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

5)　発生可能性の特定作業

官側が行う脅威事象の発生可能性と負の影響を及ぼす可能性等の特定作業において、専門的な知見による官側への助言等の支援を行うこと。

6)　影響の特定作業

官側が行う負の影響の特定及び重大さの分析作業において、専門的な知見による官側への助言等の支援を行うこと。

2.6.7.3.2　セキュリティ計画書、継続監視計画書及び将来対応計画書の更新に係る支援

リスク評価報告書を用いて実施されたリスク分析・評価の結果を受けて官側が実施するセキュリティ計画書、継続監視計画書及び将来対応計画書の更新作業において、専門的な知見による官側への助言等の支援を行うこと。

2.6.8　脆弱性検査に係る支援

2.6.8.1　脆弱性検査の実施

対象システムのネットワークに関する情報、対象システムのシステム構成、設計等に関する情報等について収集を行い脆弱性検査を実施すること。また、その結果について分析を行い官側に報告すること。

2.6.8.2　脆弱性検査の結果を踏まえた将来対応計画書の作成に係る支援

脆弱性検査の結果を踏まえて官側が実施する将来対応計画書の作成作業において、専門的な知見による官側への助言等の支援を行うこと。

2.6.8.3　脆弱性検査の机上調査に係る支援

スタンドアロン型の情報システム、ＯＴ／ＩＯＴシステム及びＩＰアドレスが付与されていない機器で構成されている情報システムのうち、官側が必要と認める情報システムに対する机上調査等による脆弱性検査を行うこと。

2.6.9　監査の結果に基づく是正勧告・助言への対応に係る支援

情報保証監査責任者が行った情報システムに対する監査の結果、不良評価と判定された項目について、是正勧告・助言に基づき官側が行う改善策の検討作業において、専門的知見による官側への助言等の支援を行うこと。

2.6.10　侵入試験の結果に基づく是正勧告・助言への対応に係る支援

情報保証監査責任者が行った侵入試験の結果、洗い出された問題点等について、是正勧告・助言に基づき官側が行う改善策の検討作業において、専門的知見による官側への助言等の支援を行うこと。

2.6.11　情報システム間の接続及び外部サービスの利用に係る支援

2.6.11.1　情報システム間の接続に係る支援

訓令第２１条第２項第３号に示す特別な理由があるとして情報システムを他の情報システム又はネットワークと接続を行う場合、官側が行う起こりうる脅威事象及び脅威事象に対応するセキュリティ管理策の特定作業において、専門的な知見による官側への助言等の支援を行うこと。なお、対象となる情報システム数については、最大５システムを想定している。

2.6.11.2　外部サービスの利用に係る支援

運用通達第３第１０項第２号に示す外部サービスを調達する際に、官側が行う必要なセキュリティ管理策の選択及び実装方法の特定作業において、専門的知見による官側への助言等の支援を行うこと。なお、対象となる情報システム数については、最大５システムを想定している。

3. 契約相手方の要件等

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、事前に官と協議するものとする。

3.1 契約相手方の要件

a) NIST SP 800-37 Rev.2 及び NIST SP 800-53 Rev.5 の知見を有していること。

b) 令和５年３月３１日に改正された訓令第２６条、同訓令第２７条の２及び同訓令第５２条の規定に基づく情報システムの運用承認、リスク分析・評価及び監査（監査の結果に基づく対応含む。）のいずれかの支援業務の実績を有すること。

c) 表１に示す規模の情報システム数に対して NIST SP 800-37 Rev.2 及び NIST SP 800-53 Rev.5 を踏まえたリスクマネジメントの業務（支援を含む。）に主たる契約者として従事した実績を有すること。

d) ISMS(ISO/IEC27001)の認証を取得していること。

e) 過去５年以内に、政府機関、重要インフラ事業者等におけるプロジェクトのコンサルティング等の業務に１年以上従事した実績を有すること。

f) 以下のいずれかの要件を満たすこと。

1) 政府機関、重要インフラ事業者等におけるリスクマネジメントシステムの業務に従事した実績を有していること。

2) COBIT、CMMI 等のプロセスモデルに従った制度構築、運用、アセスメントを実施した経験が２年以上あること。

g) 契約相手方は、業務の過程において官側から指示された事項については、迅速かつ的確に実施するものとする。
h) 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、速やかに支出負担行為担当官等と協議し、その指示に従うものとする。

3.2 役務員の要件

a) 契約の履行に必要な業務に従事する者、かつ、履行中に知り得た情報の保全を確実に行うことができる者（以下「業務従事者」という。）を確保すること。
b) **本役務を統括する責任者となる業務従事者**
1) 令和５年３月３１日に改正された訓令第２６条、同訓令第２７条の２及び同訓令第５２条の規定に基づく情報システムの運用承認、リスク分析・評価及び監査（監査の結果に基づく対応含む。）のいずれかの支援の業務に責任者又は責任者に準ずる立場で従事した実績を有すること。
2) 表１に示す規模の情報システム数に対して NIST SP 800-37 Rev.2 及び NIST SP 800-53 Rev.5 を踏まえたリスクマネジメントの業務（支援を含む。）に責任者又は責任者に準ずる立場で従事した実績を有すること。
3) 以下のいずれかの資格または同等以上の能力を有すること。
・ ＰＭＰ（プロジェクトマネジメント・プロフェッショナル）
・ 情報処理技術者試験（プロジェクトマネージャ）
・ 技術士（情報工学部門）又は技術士（総合技術監理部門のうち情報工学を選択科目とした者）
c) **主任者、チームリーダー等となる業務従事者**
1) NIST SP 800-37 Rev.2 及び NIST SP 800-53 Rev.5 の知見を有していること。
2) 令和５年３月３１日に改正された訓令第２６条、同訓令第２７条の２及び同訓令第５２条の規定に基づく情報システムの運用承認、リスク分析・評価及び監査（監査の結果に基づく対応含む。）のいずれかの支援の業務に責任者又は責任者に準ずる立場として従事した経験を有すること。
3) 以下のいずれかの資格又は同等以上の能力を有すること。
・ CISSP
・ CIA、CISA 又は CRISC
・ 情報処理安全確保支援士、システム監査技術者又は公認情報セキュリティ監査人（CAIS）
・ 技術士（情報工学部門）又は技術士（総合技術監理部門のうち情報工学を選択科目とした者）
・ ISMS 主任審査員
d) **本役務の実務を担当する業務従事者**
1) NIST SP 800-37 Rev.2 及び NIST SP 800-53 Rev.5 の知見を有する者を複数人含めること。
2) 令和５年３月３１日に改正された訓令第２６条、同訓令第２７条の２及び同訓令第５２条の規定に基づく情報システムの運用承認、リスク分析・評価及び監査（監査の結果に基づく対応含む。）のいずれかの支援の業務経験を有する者を複数人含めること。
3) 以下のいずれかの経験を有する者を複数人含めること。
・ 政府機関、重要インフラ事業者等における情報セキュリティ又は情報システムに関連する監査の業務に従事した経験を有すること。
・ 政府機関、重要インフラ事業者等における情報システムのリスク分析の業務に従事した経験を有すること。
・ 監査結果をもとに改善計画を策定し、情報システム又は業務の改善に２年以上従事

した経験があること。
・ COBIT、CMMI 等のプロセスモデルに従った制度構築、運用又は改善活動において、対象となる組織に対する支援に２年以上従事した経験があること。

e) 原則として全ての業務従事者（再委託先を含む。）は、日本国籍を有していること。

f) 上記の業務従事者は、それぞれに掲げるもののほか、履行に必要若しくは有用な、又は背景となる経歴、知見、資格、語学（母語及び外国語能力）、文化的背景（国籍等）、業績等を有すること。また、業務従事者が他の手持ち業務等との関係において履行に必要な業務所要に対応できる態勢にあること。

4. 役務従事者の申請

契約相手方は、本役務に従事する者について、役務関係者名簿（氏名、国籍、所属、主たる担当業務及び主たる作業場所）を契約後速やかに作成し、支出負担行為担当官に提出して承認を得るものとする。また、本役務に従事する者の追加又は変更が生じた場合には、遅滞なく支出負担行為担当官の承認を得るものとする。

5. 次期役務事業者への引き継ぎ資料の作成

契約相手方は、次期役務事業者が遅滞なく円滑に官側の支援を行うことができるよう引継ぎ資料の作成を行い、官側と協議の上、提出すること。

6. 情報の保全

6.1 契約を履行する一環として収集、整理、作成等を実施して得られた情報の取扱い

a) 契約相手方は、業務関係書類の作成等を会社で行う場合、使用するパソコンについては、情報の流出について万全を期すため、ファイル交換ソフトをインストールしないものを使用するとともに、ウイルス対策ソフトをインストールした上で、ウイルス定義ファイルを常に最新のものとすること。また、役務員等が個人で所有しているパソコンを使用してはならない。なお、第三者を従事させる場合も同様とする。

b) 契約相手方は、この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、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) 発注者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) 発注者が書面により個別に許可した場合を除き、受注者に係る親会社、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受注者に対して指導、監督、業務支援、助言、監査等を行う者を含む一切の受注者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

c) 保護すべき情報については**表２**のとおりとする。

表２－保護すべき情報

番号	保護すべき情報	保護すべき情報の詳細	企業で取り扱う際の留意事項
1	情報システムの設計に関する情報	－	官側との調整時、提出書類の作成時に明らか又は類推できる場合は保護の対象とする。
2	情報システムの機能・性能に関する情報	－	
3	情報システムの構成に関する情報	－	
4	情報システムの設定に関する情報	－	
5	情報システムの運用に関する情報	－	
6	情報システムのセキュリティポリシーに関する情報	－	
7	情報システムの脆弱性検査、侵入試験及び監査に関する情報	－	
8	「対外厳秘」、「注意」、「記入後注意」（情報を記入したものに限る）、「部内限り」、「非開示」、「一部開示」、「部分開示」、「一部非開示」、「機密性２」が記載された情報	－	
9	「受注者限り」との条件で発注者から提供を受ける情報	－	
１０	契約を履行する過程で発生する番号１から番号９までのいずれかの情報を含む情報	－	

7. 提出書類

契約相手方は、**表３**に示す書類を提出し、要求元の承認を得ること。

表３　提出書類の一覧

番号	書類の名称	部数	提出期限	媒体
1	実施計画書	1	契約締結日から１か月以内	電子媒体１部
2	実施体制表	1	契約締結日から１か月以内	
3	役務関係者名簿	1	契約締結後速やかに	
4	役務実施報告書（月報）	1	翌月７営業日まで	
5	役務実施報告書（最終報告）	1	令和９年３月３１日まで	
6	次期役務事業者への引継ぎ資料	1	令和９年３月１９日まで	

8. 貸付品

a) 本契約の遂行に当たり必要となる官の保有する文書等について官と調整の上、無償で貸付け又は閲覧することができる。貸付場所は、官が指定する場所とし、貸付期間は、契約期間中とする。

b) 契約相手方は、官の保有する資料の貸与を受ける場合はその取扱いに留意し、法令、関連規則等に従い、官が指定する条件を遵守すること。

9. 官側の支援

契約相手方は、役務の実施に当たり官側の支援を必要とする場合には、官側と調整の上、次の事項について無償で支援を受けることができる。

a) 立入りに関する事項

b) 事務室、机、椅子、パソコン、内線電話、水及び電気

c) その他、官側が必要と認めた事項

10. 検査

本仕様書に基づき、整備計画局サイバー整備課支出負担行為担当官補助者が実施する。

11. その他

a) 本役務により作成した成果物に関する所有権及び著作権は、防衛省に帰属するものとする。

b) 契約相手方は、本役務契約の履行に当たり、第三者を従事させる必要がある場合には、「**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）**」に定める特約条項を適用する。

c) 各機関の長が定めた立入禁止場所に立ち入る場合は、各機関の立入手続に従い所要の手続を実施するものとする。

d) 本役務において使用する物品等は、「**環境物品等の調達の推進に関する基本方針**」の基準を満たすものであること。ただし、基本方針の改定があった場合には、これに従うものとする。

e) 本役務の入札に参加する者又は本役務に第三者として従事する者は、運用承認、リスク分析・評価及び情報保証に関する監査業務の公平性・客観性を担保するため、「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)」への入札参加を制限する。また、「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)」に第三者として従事することについても同様に制限する。

f) 本仕様書に基づき支援対象となった情報システムの支援完了後の運用、セキュリティ及び保守における不備については、契約相手方の責任は問わない。
g) 本役務の実施にあたり、契約の相手方（下請負者、再委託先を含む。）は、取り扱う情報システム等について、情報の漏えい若しくは破壊又は障害等のリスク（未発見の意図せざる脆弱性を除く。）が潜在すると知り、又は知り得べきソースコード、プログラム、電子部品、機器等の埋込み又は組込みその他官の意図せざる変更を行わず、かつ、そのために必要な相応の管理を行うものとする。
h) 本仕様書に疑義が生じた場合は、速やかに支出負担行為担当官等と協議し、その指示に従うものとする。