

令和7年3月28日

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7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
情-I-034	次期防衛省OAシステム基盤の設計役務（その2）	仕様書のとおり	仕様書のとおり	自：契約締結日 至：令和8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7年5月20日（火）10：30

4. 入札場所 防衛省市ヶ谷庁舎E 2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つて、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04・05・06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し、かつ、令和07・08・09年度競争参加資格（全省庁統一資格）においても同資格を有することが見込まれ、資格決定後、速やかに資格審査結果通知書を提出できる者であること。
 - (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つて、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）の等級にかかわらず、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7年4月15日（火）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	15
	2件	10
	1件	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	15
	7～8人	12
	5～6人	9
	3～4人	6
	1～2人	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	6
	9～10人	5
	7～8人	4
	5～6人	3
	3～4人	2
	1～2人	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つて、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 S B I R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事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、保有個人情報等の取扱いに関する特約条項

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) 契約締結日までに令和7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契約とする場合がある。

(5) 入札に関する条件 仕様書5.1 a)～d)に定める本業務の実施体制並びに仕様書8.2 f) 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7年4月15日（火）12:00。必要に応じ追加資料の提出を求めることがある。）。

(6) 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（前号を除く）を令和7年4月25日（金）12:00までに提出しなければならない。

(7) 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7年5月16日（金）までに、下記担当者必着分を有効とする。

(8) 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。

(9) 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：〇〇〇」 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 中島 電話 03-3268-3111 内線20824

調達仕様書			
件名	次期防衛省OAシステム基盤の設計 役務（その2）	仕様書番号	
		変更年月日	令和 年 月 日
		作成年月日	令和7年3月17日
		作成部署	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、次期防衛省OAシステム基盤の設計役務（その2）について規定する。

1.2 用語の定義

この仕様書で用いる用語の定義は、表1のとおりとする。

表1—用語の定義

用語	定義
防衛省OAシステム基盤	行政事務の合理化・効率化を図るためのLANシステムである防衛省中央OAネットワーク・システムを基本として各業務システム等を集約するために整備する共通基盤。令和6年度にMicrosoft Teams機能の提供開始及び市ヶ谷LANが整備する無線LANへの接続を開始した。
防衛省中央OAネットワーク・システム	市ヶ谷地区において運用している府省内LANシステム
地方防衛局OAネットワーク・システム	地方防衛局において運用している府省内LANシステム
IaaS基盤	防衛省OAシステム基盤に整備する、防衛省内の業務システムの基盤集約を行うためのIaaS（Infrastructure as a Service）基盤
省OA	防衛省OAシステム基盤
現行システム	令和8年9月まで運用する現行の防衛省OAシステム基盤
次期システム	令和8年10月から運用を開始する予定の次期防衛省OAシステム基盤
クラウドサービス	ネットワーク経由でソフトウェアやインフラ等の各種機能が提供され、権限を持った利用者によって自由に設定・管理が可能なサービスを指す。 本紙ではISMAPに登録されたサービスを対象とする
市ヶ谷地区	市ヶ谷駐屯地・基地、政府控室及び各通信所
第1センター	防衛省OAシステム基盤に必要な機器等を設置するデータセンタ
RMF	リスク・マネジメント・フレームワークの略称。防衛省にて実施される、リスク評価・分析及びその結果に対する計画や承認など全般的な業務
SOC	Security Operation Centerの略称 ネットワーク機器、セキュリティ製品及びサーバ類等を24時間365日監視し、セキュリティにおける脅威を検出及び検知し、セキュリティインシデントに対する分析等を行う組織
MOD-1	注意電算機情報及び個人情報電子計算機情報を取り扱う情報システムの保護プロファイル
業務従事者	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

1.3 引用文書等

本仕様書における引用文書は、本仕様書に規定する範囲内において、本仕様書の一部をなすものであり、引用文書に定める項目が本仕様書と相違する場合は、本仕様書を優先する。

なお、引用文書及び関連文書は、入札書又は見積書の提出時における最新版とする。

1.3.1 引用文書

a) 仕様書等

- 1) 防衛省OAシステム基盤借上（03換装）
- 2) 防衛省OAシステム基盤借上（04増設）
- 3) 防衛省OAシステム基盤借上（05端末増設）
- 4) 防衛省OAシステム基盤借上（05増設）
- 5) 防衛省OAシステム基盤借上（06端末増設）
- 6) 防衛省OAシステム基盤借上（06増設）
- 7) 防衛省OAシステム基盤借上（07端末増設）
- 8) 地方防衛局OAネットワーク・システム（北関東・九州）借上
- 9) 地方防衛局OAネットワーク・システム（南関東・沖縄）借上
- 10) 地方防衛局OAネットワーク・システム（東北・中国四国）借上
- 11) 地方防衛局OAネットワーク・システム（北海道・近畿中部）借上

※上記の仕様書に定められる事業者の提出文書も含む

- 12) 防衛省OAシステム基盤基本設計書

b) 法令等

- 1) 個人情報の保護に関する法律（平成15年法律第57号）
- 2) 著作権法（昭和45年法律第53号）
- 3) 「公用文作成の考え方」の周知について（内閣文第1号（令和4年1月11日））
- 4) デジタル・ガバメント推進標準ガイドライン（令和6年5月31日更新）（以下「標準ガイドライン本編」という。）
- 5) 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（令和6年5月31日更新）（以下「標準ガイドライン実践ガイドブック」という。）
- 6) デジタル・ガバメント推進標準ガイドライン解説書（令和6年5月31日更新）（以下「標準ガイドライン解説書」という。）
- 7) 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。）
- 8) 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。平成31年1月9日）
- 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）（装管調第5121号（令和2年3月31日））
- 10) 環境物品等の調達の推進に関する基本方針（変更閣議決定（令和7年1月28日））
- 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基準群（令和5年度版）（以下「統一基準群」という。）

- 12) 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン（デジタル庁（令和4年6月30日））（以下「セキュリティ・バイ・デザイン」という。）

1.3.2 関連文書

a) 仕様書等

- 1) 防衛省OAシステム基盤（設置機材の維持管理）
- 2) 防衛省中央OAネットワーク・システム運用管理役務
- 3) 防衛省OAシステム基盤（設置機材の維持管理）（その2）
- 4) 防衛省OAシステム基盤の運用管理役務
- 5) 防衛省OAシステム基盤のTeams機能の利用に係る導入・維持管理支援役務
- 6) 次期防衛省OAシステム基盤の設計役務

※上記の仕様書に定められる事業者の提出文書も含む

b) 法令等

- 1) 防衛省の情報保証に関する訓令（防衛省訓令第160号（平成19年9月20日））
- 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（平成19年9月20日））
- 3) 防衛情報通信基盤データ通信網管理運用規則（自衛隊統合達第15号（平成29年7月20日））
- 4) 政府機関等の対策基準策定のためのガイドライン（内閣官房 内閣サイバーセキュリティセンター（令和5年7月4日））

c) その他

- 1) 日本産業規格（JIS）（JIS Z 8301）

1.4 別冊

次期防衛省OAシステム基盤の設計役務（その2） 別冊（注意）

1.5 本仕様書における別冊の参照

- a) 本仕様書及び付表における「カタカナ」は、次期防衛省OAシステム基盤の設計役務（その2） 別冊（注意）によるものとする。
- b) 次期防衛省OAシステム基盤の設計役務（その2） 別冊（注意）については、所定の手続きを踏まえた上で防衛省市ヶ谷地区68号館2階において閲覧可能とする。

2. 本調達の概要

省OAは、9機関と共同の部隊（防衛省本省の内部部局、防衛研究所、統合幕僚監部、陸上幕僚監部、海上幕僚監部、航空幕僚監部、情報本部、防衛監察本部、防衛装備庁及び自衛隊サイバー防衛隊）の共同の事業として、約9000台の端末等から構成されるLANシステム及び省内の業務系システムを集約しコストの最適化を目的としたIaaS基盤を構築し、令和3年3月より運用を開始した。

運用開始以降、年度毎にIaaS基盤のリソース増設を行い、地方防衛局の集約を行ってきた。

また、職員の増加に伴う安定的な省OAの利用環境の整備を目的とした端末及びサーバ機器等の増設やMicrosoft 365の導入を行っている。

省OAの令和8年度の換装を行うにあたり、省OAをパブリッククラウドサービスを主としたシステムへ刷新する。また、令和8年度から令和10年度末までに全ての地方防衛局OAネットワーク・システム（以下、「局OA」という。）を段階的に省OAへ統合することを予定している。

そのため、令和8年度の省OA換装においては、オンプレミス環境からクラウドサービスへの移行が発生することが見込まれることから、システムを円滑に移行するための移行設計及び局OA統合を見据え、運用を最適化するための運用設計を行うものである。

2.1 本調達の目的及び期待する効果

前述のとおり、省OAはパブリッククラウドサービスを主としたシステムへ刷新し、将来的に局OAを統合することから、移行及び運用についても見直すことで移行と運用の円滑性及び安全性の向上を図る。

2.2 システム構成（概要）

システム構成（概要）はア及びイのとおり。

2.3 システム規模

1) 現行システム

以下の仕様書を参照すること。

- ① 防衛省OAシステム基盤借上（03換装）
- ② 防衛省OAシステム基盤借上（04増設）
- ③ 防衛省OAシステム基盤借上（05端末増設）
- ④ 防衛省OAシステム基盤借上（05増設）
- ⑤ 防衛省OAシステム基盤借上（06端末増設）
- ⑥ 防衛省OAシステム基盤借上（06増設）
- ⑦ 防衛省OAシステム基盤借上（07端末増設）
- ⑧ 防衛省中央OAネットワーク・システム運用管理役務
- ⑨ 防衛省OAシステム基盤の運用管理役務

2) 次期システム

表3のNo. 10で作成される**防衛省OAシステム基盤基本設計書**（以下、「基本設計書」という。）を参照すること。

3) 防衛局OAシステム基盤

以下の仕様書を参照すること。

- ① 地方防衛局OAネットワーク・システム（北関東・九州）借上
- ② 地方防衛局OAネットワーク・システム（南関東・沖縄）借上
- ③ 地方防衛局OAネットワーク・システム（東北・中国四国）借上
- ④ 地方防衛局OAネットワーク・システム（北海道・近畿中部）借上

2.4 契約期間

本調達の契約期間は、契約締結日から令和8年3月31日までとする。

2.5 作業スケジュール

本調達及び関連事業に係る作業スケジュールは**付図4**のとおり。関連事業に関する概要につい

ては、表3を参照すること。

3. 関連調達案件

3.1 関連調達案件の調達単位等

次期システムの設計に係る主な案件名および役割については、表3のとおり。

No. 13～17については現時点での想定となる。

表3－関連調達案件の調達単位等

No.	調達単位	実施予定期間	役割
1	防衛省OAシステム基盤 (設置機材の維持管理)	令和2年7月～ 令和8年2月	第2センターの設置機材の維持管理を実施 ※契約変更により令和12年3月まで延長 と増床を予定(令和8年2月～)
2	防衛省OAシステム基盤 借上(03換装)	令和3年8月～ 令和8年2月	省OAの構築及びハードウェア/ソフトウ ェアの借上を実施
3	防衛省中央OAネットワ ーク・システム運用管理 役務	令和4年3月～ 令和8年2月	省OAの運用管理役務を実施 ※契約変更により端末増設に伴う役務員の 増員を予定(令和7年8月～)
4	防衛省OAシステム基盤 借上(04増設)(以下 「04増設」という。)	令和4年9月～ 令和9年2月	現行システムのIaaS基盤に令和4年度 加入システムを集約するための増設を実施
5	防衛省OAシステム基盤 (設置機材の維持管理) (その2)	令和5年4月～ 令和10年2月	第1センターの設置機材の維持管理を実施 ※契約変更により令和12年3月まで増床 を予定(令和8年3月～)
6	防衛省OAシステム基盤 借上(05増設)(以下 「05増設」という。)	令和5年5月～ 令和10年2月	現行システムのIaaS基盤に令和5年度 加入システムを集約するための増設を実施
7	防衛省OAシステム基盤 運用管理役務	令和5年7月～ 令和8年2月	防衛省OAシステム基盤の借上(05増 設)及び防衛省OAシステム基盤借上(0 5端末増設)として増設する省OAの運用 管理業務を実施
8	防衛省OAシステム基盤 のTeams機能の利用 に係る導入・維持管理支 援役務	令和6年2月～ 令和8年9月	現行システムに対するTeamsの導入・ 維持管理に係る支援を実施
9	防衛省OAシステム基盤 借上(06増設)(以下 「06増設」という。)	令和6年7月～ 令和10年2月	現行システムのIaaS基盤に令和6年度 加入システムを集約するための増設を実施
10	次期防衛省OAシステム 基盤の設計役務	令和6年5月～ 令和7年3月	次期システムに係る設計を実施
11	防衛省OAシステム基盤 のプロジェクト管理支援 役務	令和7年4月～ 令和9年3月	現行及び次期システムに関連する複数事業 のプロジェクト管理支援及び調達支援等 を実施
12	次期防衛省OAシステム 基盤の設計役務(その 2)	令和7年5月～ 令和8年3月	次期システムに係る移行、運用設計を実施
13	防衛省OAシステム基盤 借上(07換装)(以下 「07換装」という。)	令和7年10月 ～ 令和12年9月	次期システムの構築及びハードウェア/ソ フトウェアの借上を実施

(凡例：太枠は本調達案件)

表3－関連調達案件の調達単位等（続き）

No.	調達単位	実施予定期間	役割
14	防衛省OAシステム基盤借上（03換装）（07延長）	令和8年3月～ 令和9年2月	防衛省OAシステム基盤の借上（03換装）で借り上げた現行システム及び北関東・九州局OAのハードウェア/ソフトウェア等の延長
15	防衛省中央OAネットワーク・システム運用管理役務（07延長）	令和8年3月～ 令和8年9月	運用期間を延長した防衛省OAシステム基盤の借上（03換装）の運用管理役務を実施
16	防衛省OAシステムデータ移行支援役務（08移行）	令和8年4月～ 令和8年9月	現行システムから次期省OAへのデータ移行業務を実施
17	防衛省OAシステム基盤の運用管理役務（08運用）	令和8年8月～ 令和12年3月	次期システムの運用管理業務を実施

（凡例：太枠は本調達案件）

3.2 調達案件間の入札制限

相互牽制の観点から、表3のNo. 11の受注業者、及び入札公告時点における前年度及び今年度のデジタル統括アドバイザー業務の契約相手方は、相互に本調達の入札制限の対象とする。

4. 役務の内容

4.1 基本的な留意事項

契約相手方は、作業全般において次に示す事項に留意して作業を進めること。

- a) 現行システム及び次期システムの構成等について、理解した上で作業すること。
- b) 本調達の実施に当たっては、**標準ガイドライン本編**、**標準ガイドライン解説書**及び**標準ガイドライン実践ガイドブック**を参照し、対応すること。
- c) 整備計画局サイバー整備課デジタル化推進班（以下「官側」という。）の指示の下、表3に示す関連調達案件における契約相手方と適宜情報連携を行い、必要に応じて調整を行いながら対応すること。
- d) 提出文書については、想定する記載内容や構成等を整理した骨子を作成の上、事前に官側に提示し、承認を得ること。
- e) **標準ガイドライン**、**リスク管理枠組み（RMF）におけるセキュリティ管理策及びセキュリティ・バイ・デザイン**を基準とし、セキュリティ対策に必要な留意事項を官と協議、決定し対応すること。
- f) 感染症による業務履行に支障を来すことがないように、感染症対策に配慮するとともに予めリスク管理表に対応策について記載すること。

4.2 本役務の計画策定及び状況報告等

4.2.1 作業実施計画書の作成

- a) 契約締結後、速やかに本役務を実施するために必要な作業を洗い出し、作業体制、作業実施計画書を策定し、官側の承認を得ること。また、作業実施計画書に変更が必要な場合は、役務全体に対する影響を調査し、作業実施計画書を変更した上で、官側の承認を得るとともに、作業実施計画書の変更管理を行うこと。

- b) 作業実施計画書には、最低限以下の項目について記述すること。
- 1) 作業概要
 - 2) 作業体制に関する事項
作業実施体制を記載し、統括責任者、業務実施責任者、移行設計チーム責任者、運用設計業務チーム責任者までは担当者の名前を記載し、各役割の責任範囲を明確化すること。
 - 3) スケジュールに関する事項（WBS含む）
スケジュール概要として、各タスクの実施想定時期、主要なマイルストーンを記載すること。
 - 4) 成果物に関する事項
各提出文書について、途中成果物及び最終成果物の想定される提出年月、文書に記載する内容について概要を記載すること。
 - 5) 設計手法等

4.2.2 作業実施要領書の作成

- a) 契約締結後、速やかに設計業務の管理方法、手順及び遵守事項等について定めた作業実施要領書を作成し、作業開始前に官側の承認を得ること。
- b) 作業実施要領書には、最低限以下の項目について記述すること。
- 1) コミュニケーション管理
 - ① 会議体の一覧を記載し、各会議体の目的及び開催頻度について記載すること。
 - ② 会議において作成する議事録の様式、提出期限について記載すること。
 - ③ コミュニケーション手段として、官との窓口を明確化し、平日日勤帯において常時連絡可能な電子メールアドレス及び電話番号を記載すること。
 - 2) 体制管理
メンバーの追加、離任などの変更が発生する場合、体制図および作業者名簿を更新して提出する旨、明記すること。
 - 3) 工程管理
 - ① 管理方法、管理項目、管理手法について記載すること。
 - ② 進捗状況を定義し、遅延や遅延の可能性が発生するタスクが可視化されるようにすること。
 - ③ 進捗遅延時の対処について、遅延の度合い、後続タスクへの影響を加味した対処を明確に記載すること。
 - 4) 品質管理
 - ① 品質管理方針と品質管理基準を設定し、品質管理の具体的な方法を明示すること。
 - ② プロジェクトの品質管理として、フェーズ単位でのレビューおよび定点でのレビューについて、実施目的および実施時期を記載すること。
 - ③ 文書の品質管理として、官へレビューを依頼および文書を提出する際には、社内で作成した「レビュー等実施記録等」を同時に提示する旨、記載すること。
 - ④ レビュープロセスを明確化し、レビューイ、レビューアを行う役割をプロセス単位で記載すること。

- ⑤ レビュー種別と観点を記載し、品質を担保するうえで十分な管理措置を行っていることを記載すること。
 - ⑥ 各提出文書において、対象となるレビュー種別がわかるマトリクス表を記載すること。
- 5) リスク管理

リスク管理表を作成し、管理項目、管理手法、官とのリスク共有について、作成したリスク管理表を、リスクの大小にかかわらず進捗報告会議で官へ報告する旨を記載すること。
 - 6) 課題管理

課題管理表を作成し、管理項目、管理手法、官との課題共有について、作成した課題管理表は、進捗報告会議で官へ報告する旨を記載すること。
 - 7) 文書構成管理

対象文書と別紙等の関連文書について一覧化して記載すること。また、版数管理を行い、最新状態及び修正内容の管理を行うこと。
 - 8) 変更管理

管理方法、管理フローについて記載すること。
 - 9) 情報セキュリティ対策

方針、保護すべき情報の取り扱い、防衛省内における事業者資産の取り扱いについて記載すること。

4.2.3 業務従事者名簿の作成

各種作業を実施する業務従事者について、契約締結後、速やかに業務従事者名簿を作成し、官側に報告、承認を得ること。また、業務従事者に異動、退職、長期休暇等が生じ、業務従事者の追加、変更等が必要となった場合には、十分な時間的余裕をもって後任の業務従事者に確実に引継ぎを実施するとともに、再度業務従事者名簿を作成し、官側に報告、承認を得ること。なお、官側が業務従事者の要件を満たさないと判断した場合についても同様とする。

4.3 設計全般

- a) 4.4.5及び4.5.5で示された要件を満たすための設計等について、官側と調整し、決定すること。また、調整に当たっては、契約相手方の推奨する設計等について積極的に提案すること。

なお、設計漏れが発覚した場合は、速やかに官側と協議の上、対応すること。
- b) 基本設計書を基に必要な移行及び運用について設計を行うこと。
- c) 移行及び運用設計において、基本設計書の修正が必要となった場合、変更内容について借上事業者及び官側の了承を得たうえで、変更管理に基づき管理するとともに修正を行うこと。
- d) 官側から要請された次期システムに関連する会議に参加し、官側への必要な助言等を行うとともに、必要に応じて議事録及び会議資料の作成を支援すること。ただし、他事業者が主催する会議体においては前述の対象外とする。
- e) 災害対策環境（以下「災対環境」という。）について、付表1を基準とし設計に反映すること。

- f) 移行及び運用設計の内容について、官側及び各機関等と調整し承認を得ること。
- g) 表3のNo.11の省OAのプロジェクト管理支援役務の受注業者（以下「工程管理事業者」という。）が作成するデータ移行役務及び運用役務の調達仕様書を作成するにあたり必要になると想定される情報を途中成果物として提供すること。また、情報提供後に更新等が発生した場合は必要に応じて更新情報を提供すること。
- 1) データ移行役務に関する情報は令和7年11月30日まで
- 2) 運用役務に関する情報は令和8年2月28日まで

4.4 移行設計

4.4.1 作業範囲

設計範囲は省OA及び局OAを含む移行対象となるデータの選定、移行方式及びシステム切り替え方針の決定とする。

4.4.2 データ移行対象

- a) 次期システムでユーザが必要とするデータ移行対象は下表を想定している。設計を進めるうへで変更する場合は官側と協議し適宜対象を変更すること。また、システムに関するデータ移行の対象は設計を進める上で検討すること。

表4ーデータ移行対象

No.	移行元機能名	移行対象データ	留意事項
1	ユーザ管理機能	アカウントデータ セキュリティグループ グループポリシー	4.4.5a)b)c) 項の要件に留意して移行設計を行うこと。
2	ファイル共有機能	ファイルデータ	
3	部内系端末	ローカルデータ	ユーザの負荷を極小にする手法を検討すること。
4	部外系仮想端末	ローカルデータ	ユーザの負荷を極小にする手法を検討すること。
5	ユーザー支援サイト	サイトデータ	移行先に応じて必要なデータを検討すること。

- b) データ移行設計の対象となるシステムは以下を想定している。
- 1) 現行システム
- 2) 北関東・九州局OA
- 3) 南関東・沖縄局OA
- 4) 北海道・近中局OA
- 5) 東北・中四国局OA

4.4.3 システム移行

システム移行においては以下について検討すること。

- a) 現行システムとの並行稼働及び次期システムへの切り替えについて検討すること。
- b) 第2センターに引き込んでいるDII網へ接続する回線のネットワーク経路切り替えに関する検討をすること。

- c) 現行システム撤去後、ラック本数の削減のために、隣接ラックへの05増設機器移設を検討すること。

4.4.4 防衛省OAシステム基盤移行計画書案の作成

- a) 移行役務事業者が円滑に移行作業を実施するため、防衛省OAシステム基盤移行計画書案（以下、「移行計画書案」という。）を作成し官側の承認を得ること。
- b) 移行計画書案については以下の項目を最低限とし、その他必要な項目は追加すること。
 - 1) 移行対象データ
 - 2) 移行対象となるデータの保存場所、データの種類等
 - 3) 移行対象データ量
 - 4) 移行方式（移行段階のシステム構成含む。）
 - 5) 移行元及び移行先の情報
 - 6) 移行環境及び方式
 - 7) データ移行に係る時間（目安）

4.4.5 移行設計において考慮すべき事項

- a) 移行については表4の移行対象データ全てではなく、必要なデータのみを整理、抽出し、不要なデータは移行対象外とすること。整理、抽出は必要に応じて現行システムの運用役務事業者及び保守役務事業者と連携して行うこと。
- b) 現行システムで利用されているアカウントデータを整理し、移行対象を選定のうえ、移行方針を検討すること。
- c) 管理者アカウント、サービスアカウント等の特権アカウントを移行する場合は、パスワード変更を行う等、セキュリティリスクを低減する方法を検討すること。
- d) 04増設の管理機能は次期システムの管理機能を利用する設計とすること。また、04増設の撤去後不要なデータを残さない設計とすること。
- e) システム移行についてはア～ウを参照した上で、システム移行対象を検討すること。
- f) 移行に当たり、構築開始からシステム切替までの過渡期となるシステム構成の設計を含むこと。また、現行システム及びユーザへの影響を極限とし、円滑に移行可能な構成及び方法を検討すること。
- g) 04増設、05増設及び06増設を07換装で導入するネットワーク機器へ収容することを前提とした移行設計を行うこと。また、04増設、05増設及び06増設を撤去する際、撤去対象以外の基盤への影響を極限とする設計とすること。
- h) 移行設計にあたり、次期システムで導入される各機器の仕様及び設計について必要に応じて、同年度に別途調達する防衛省OAシステム基盤借上（07換装）の事業者と認識を合わせること。

4.5 運用設計

4.5.1 作業範囲

- a) 範囲は、附表及び基本設計書に記載される機能を基に設計を行うこと。
- b) 各地方防衛局に配置する現地役務員の可否を検討し、官側の承認を得ること。

- c) 各地方防衛局に現地役務員の配置が必要と判断される場合、現地役務員を配置することを前提とした運用設計を行うこと。
- d) 現地役務員の配置を前提とした場合、現地役務と中央（市ヶ谷地区）役務員の責任分界を明確にすること。

4.5.2 SOC業務の検討

次期システムにおけるSOC業務について以下を基準に検討し、運用計画書及び運用業務フローに反映すること。なお、自衛隊サイバー防衛隊とのSOC業務の責任分界点については、官側で設定する調整会議に同席のうえ、調整に資する資料作成及び質疑応答の対応を行うとともに、調整結果を運用計画書及び運用業務フローに反映すること。

a) 監視と検知

- 1) 24時間365日のリアルタイム監視
ネットワーク、サーバー、エンドポイント、クラウド環境などのセキュリティログやイベント等、継続的に監視すべき異常な活動や潜在的な脅威について検討すること。
- 2) 脅威インテリジェンスの活用
既知の脅威だけでなく、新たな脅威にも迅速に対応するための、最新の脅威情報や脆弱性情報の収集、分析方法の検討及び監視システムへ適用に関する手法を検討すること。
- 3) アラートのトリアージ
検知される大量のセキュリティアラートから、真に脅威と識別するための判断基準、優先順位及び対応フローを検討すること。
- 4) 脅威情報の管理
他部署、他組織から受領した脅威情報を監視システムへ適用する運用フローについて検討すること。

b) インシデント対応

- 1) インシデントの分析と調査
セキュリティインシデントが発生した際の原因、影響範囲、攻撃者のTTPS（戦術、技術、手順）等の調査・分析手法及び対応策について検討すること。また、検討の結果官の所掌判断される範囲については、官への支援内容について検討すること。
- 2) インシデントの封じ込めと駆除
被害拡大の防止措置を迅速に対応するため、感染システムやネットワーク隔離、マルウェアの駆除及び脆弱性の修正等の手法及び対応順序について検討すること。
- 3) 復旧と再発防止
被害を受けたシステムに対する復旧の支援範囲を検討すること。また、再発防止ため、インシデントの原因となった脆弱性及びセキュリティ対策の改善方法について対応プロセスを検討すること。

c) 脆弱性管理

- 1) 脆弱性スキャンの実施
潜在的なセキュリティリスクを特定するため、定期的なネットワーク及びシステムの脆弱性をスキャンする対象範囲及び分析観点について検討すること。

- 2) 脆弱性の評価と優先順位付け
特定された脆弱性の危険度や影響範囲を評価するための評価基準及び修正の優先度の基準について検討すること。
- 3) 脆弱性の修正支援
脆弱性修正のためのパッチ適用や設定変更のため、システム管理者への支援範囲を検討すること。
- d) **セキュリティ意識向上**
 - 1) セキュリティ教育
セキュリティ意識の向上を図るため、省OAユーザ（職員）向けのセキュリティ教育や訓練の手法及び頻度等について検討すること。
 - 2) セキュリティポリシーの策定と遵守
組織全体のセキュリティポリシーを策定し、その遵守状況を監視すること。
- e) **レポートと改善**
 - 1) インシデントレポート
インシデントに関する官側への報告内容（インシデント発生時の状況、対応内容、改善策等）について検討すること。
 - 2) セキュリティ体制の改善
セキュリティレベル向上のため、セキュリティ体制の評価基準及び評価頻度について検討すること。
 - 3) ログのレビュー
定期的なログのレビュー及び分析の対象範囲及び観点について検討すること。
 - 4) I o C の記録及び提供
システム内で発見された脅威情報 I o C (I n d i c a t o r o f C o m p r o m i z e) の管理項目、共有方法及び共有先について検討すること。

4.5.3 運用業務フロー図の作成

- a) 運用計画書に記載した業務毎のフローを作成し、官側の承認を得ること。
- b) 運用業務フロー図には、誰がどの作業を行うか等が可視化されるように作成すること。

4.5.4 防衛省OAシステム基盤運用計画書の作成

- a) **留意事項**
 - 1) **付表 1** 及び基本設計書に記載される機能に関する運用を網羅し、運用対象、体制、定常時の業務等を設計し、防衛省OAシステム基盤運用計画書を作成した上で、官側の承認を得ること。
 - 2) リスク管理枠組み（RMF）において次期システムに求められるセキュリティ管理策を網羅的に運用設計に取り入れること。
- b) 防衛省OAシステム基盤運用計画書（以下、「運用計画書」という。）は、以下の項目について記載すること。また、設計に応じて必要な項目を追加する場合は官側と協議すること。
 - 1) 運用管理対象（構成品目単位）

2) 運用業務一覧

運用業務一覧は、以下の項目について記載すること

- ① 業務名
- ② 業務概要
- ③ 運用形態

運用形態（オンサイト，リモート等），運用環境（通常環境，災対環境）等

- ④ 業務頻度（日次，月次，四半期，半期，年次及び随時等）
- ⑤ 担当者（主担当者，支援者，保守事業者及び関連事業者等）
- ⑥ 不定期作業

3) SLA（Service Level Agreement）案

4) 稼働報告（月次報告，年次報告等）

5) 運用業務実施スケジュール案

定期作業の実施スケジュール等を示した運用作業実施スケジュール案を作成し，官側の承認を得ること。

6) 成果物に関する事項

運用役務にて作成する成果物を記載すること。

7) 運用作業の条件（実施可能な時間帯，業務影響等）

4.5.5 運用設計において考慮すべき事項

- a) 運用について，付表 1 の業務内容を基準とした設計内容とすること。
- b) 現行システムにおける運用課題を調査・整理し，対策を設計に盛り込むこと。
- c) 各局OAが今後，省OAに統合されることを踏まえ，拡張性を考慮した設計とすること。
- d) 官品モバイル端末の利用機能に関する運用における，官品モバイル端末事業者側との責任分界点及び対応範囲について明確化すること。
- e) 端末は個人と紐付けて管理を行う方法，課室に紐付ける機器と管理方法を検討し，運用計画書に反映させること。
- f) 運用設計にあたり，次期システムで導入される各機器の仕様及び設計について必要に応じて，同年度に別途調達する防衛省OAシステム基盤借上（07換装）の事業者と認識を合わせること。

4.6 設計役務における報告・調整会議の主催

- a) 契約相手方は，設計作業の状況について，週次で報告会議・調整会議を開催すること。また，会議の実施要領については，別途官側と調整すること。なお，官側の要求又は臨時に開催の必要が生じた場合についても開催すること。
- b) 契約相手方は，設計の内容の調整，承認を得るために官側及び各機関等と設計調整会議を開催すること。また，設計調整会議の開催回数及び対象者については官側と相談の上，必要に応じて開催すること。
- c) 開催した会議については，議事録を作成することとし，開催から3営業日以内に官側に提出し，承認を得ること。

5. 本役務の実施に伴うプロジェクト実施体制の整備

5.1 全般

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) 業務従事者を確保すること。
- b) a)の業務従事者が5.4に示す要件を満たすこと。
- c) a)の業務従事者が、b)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。
- d) c)の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。

5.2 事業者の要件

5.2.1 一般事項

本役務を担当するに当たり、会社全体又は業務実施責任者が所属する部門が、以下のいずれかの要件を満たしていること。資格については、それを証明する書面（認定証等）の写しを提出すること。

- a) 情報セキュリティに係る公的認証
ISMS認証（JISQ27001（ISO/IEC27001））を保有していること。
- b) 委託実績
 - 1) 中央省庁又は地方自治体において、端末5000台規模以上のLANシステムの運用及び移行の受託実績を有すること。
 - 2) 中央省庁又は地方自治体における業務システム等を集約することを目的とした共通的な基盤の設計・開発及び運用の受託実績を有すること。
 - 3) 中央省庁又は地方自治体におけるLANシステムにおいて、運用及び移行の受託実績を直近5年以内にそれぞれ1件以上有すること。

5.3 実施体制について

契約相手方の体制は、以下に示す条件を満たすこと。なお、作業体制全般、特に、統括責任者、業務実施責任者については、本調達成功（予定どおりの設計、品質の担保）に向け、積極的・主体的な業務の推進や提案等を求める。

- a) 本役務においてスケジュールに遅延の兆候が発生した場合、官側に報告し、速やかにスケジュールの見直しを行うとともに体制の増強等を含めた対策案を提示し、官側に承認を得ること。
- b) 本役務において業務履行に支障を来す問題が発生することが見込まれる場合、官側及び工程管理事業者の支援を要請し、体制の増強等を含めた対策案を検討すること。また、必要に応じ官側に報告、承認を得ること。
- c) 本役務において業務履行に支障を来す問題が発生した場合、早急に官側及び工程管理事業者へ報告し工程管理事業者の支援を得て、体制の増強等を含めた是正案を提示し官側の承認を得ること。
- d) 本調達において、納品成果物の品質を管理する品質管理責任者を定めること。

- e) 作業要員は本仕様書に示す要件を円滑に遂行できる能力を有すること。
- f) 官側において、要員の交代の必要があると判断したときは、1週間前までに契約相手方に通知の上、交代させるものとする。
- g) 要員の変更に際しては、いずれの要因においても十分な引継ぎ期間を設けるなど、業務を円滑に持続できるように十分な配慮を行うこと。
- h) 契約相手方は、常に作業要員の服装、勤務態度、風紀及び衛生等について万全の監督を行うこと。
- i) 作業要員は、業務実施場所の整理整頓を随時行い、作業環境の整備に努めること。

5.4 業務従事者の要件

5.4.1 一般事項

本役務の実施に当たり、以下に定める業務従事者を配置するとともに、各業務従事者に求める要件を満たす者を従事させること。なお、各責任者は第三者に委任、又は請け負わせることはできないものとする。

5.4.2 統括責任者

- a) 本調達の仕事全体を統括し、各要員を管理すること。
- b) 業務進行上の問題が生じた場合又は官側の要求に応じ、業務実施責任者へのヒアリングを行うとともに、問題が生じた原因及び原因に対する改善策を官側に報告し承認を得ること。
- c) 中央省庁、独立行政法人又は地方自治体における情報システムの設計・構築及び運用・保守業務において業務実施責任者以上（業務実施責任者補佐等、同等の経歴を含む。）としての経験が5年以上あり、設計・構築及び運用・保守業務に関する経験を5年以上有すること。
- d) 中央省庁、独立行政法人又は地方自治体における端末5000台規模以上のLANシステム、かつRMFで求められるセキュリティ対策を施したシステム又は、MOD-1以上のセキュリティ対策を施したシステムについての移行設計及び運用設計又は運用役務及び移行役務に、業務実施責任者以上として携わった実績を有すること。
- e) 以下のいずれかの資格を有すること。
 - 1) PMP (Project Management Professional)
 - 2) 情報処理技術者試験 (プロジェクトマネージャ)

5.4.3 業務実施責任者

- a) 本調達の設計業務に係る仕事全体を統括し、各要員を管理すること。
- b) 中央省庁、独立行政法人又は地方自治体における情報システムの設計・構築及び運用・保守業務において、業務実施責任者以上（業務実施責任者補佐等、同等の経歴を含む。）としての経験が5年以上有すること。
- c) 統一基準群に定める機密性2情報以上の情報を取り扱うシステムの設計業務において、業務実施責任者（業務実施責任者補佐等、同等の経歴を含む。）としての実績を有すること。
- d) 業務期間中は、本調達に係る仕事に専任すること。

- e) 以下のいずれかの資格を有すること。
 - 1) PMP (Project Management Professional)
 - 2) 情報処理技術者試験 (プロジェクトマネージャ)
 - 3) 「ITスキル標準 (Ver 3.0)」のプロジェクトマネジメント (専門分野: 指定しない, 達成度指標: レベル5以上)

5.4.4 移行設計チーム

移行設計チームの体制に, 以下の業務経験を有する要員を配置すること。

- a) オンプレミスからIaaS又はPaaSへのファイル共有ストレージの移行経験
- b) Microsoft Active Directory Domain Serviceの移行経験
- c) Entra ID (旧Azure AD) とMicrosoft Active Directory Domain Service間の連携の設計経験

5.4.5 チーム責任者 (移行設計)

- a) 担当するチーム全体を管理監督すること。
- b) 情報システムの移行設計又は移行業務においてチーム責任者以上の経験が5件以上の経験を有すること。なお, 中央省庁, 独立行政法人又は地方自治体における端末5000台規模以上のLANシステムに係る移行業務経験を1件以上含むこと。
- c) 業務期間中は, 本職務に専任すること。

5.4.6 移行設計担当者

- a) LANシステムの移行業務経験を有する要員を配置すること。
- b) オンプレミスファイル共有ストレージからIaaS又はPaaSへデータ移行業務経験を有する要員を配置すること。
- c) 移行設計業務経験を有すること。
- d) 業務期間中は, 当該担当者のうち8割以上を本職務の専任とすることが望ましい。

5.4.7 運用設計チーム

運用設計チームの体制に, 以下の業務経験を有する要員を配置すること。

- a) 以下の業務経験を有する要員を配置すること。
 - 1) Entra ID (旧Azure AD) の運用経験
 - 2) Microsoft 365の運用経験
- b) 以下のいずれかの資格を有する要員を配置すること。
 - 1) 情報処理技術者 (ITサービスマネージャー)
 - 2) ITIL (Expert以上)
- c) 以下のいずれかの資格を有する要員を配置すること。
 - 1) 情報処理技術者 (情報処理安全確保支援士)
 - 2) セキュリティプロフェッショナル認定資格制度 (CISSP)
 - 3) 情報処理技術者 (情報セキュリティスペシャリスト)
- d) 以下の資格のうち1)又は2)を有する要員を配置すること。

- 1) AWS Certified Solution Architect Associate
- 2) Azure Administrator Associate
- e) ITIL foundation以上の資格を有する要員を配置すること。

5.4.8 チーム責任者（運用設計）

- a) 担当するチーム全体を管理監督すること。
- b) 情報システムの運用設計又は運用業務においてチーム責任者以上の経験が3年以上あり、運用設計又は運用業務に関する5年以上の経験を有すること。
- c) 中央省庁、独立行政法人又は地方自治体における端末5000台規模以上のLANシステムについての運用設計業務経験を有すること。
- d) 業務期間中は、本職務に専任すること。

5.4.9 運用設計担当者

- a) LANシステムの運用設計・運用業務経験を有する要員を配置すること。
- b) 運用計画書（運用設計書を含む）作成、業務フロー作成の業務経験の実績を有すること。
- c) 業務期間中は、当該担当者のうち8割以上を本職務の専任とすることが望ましい。

5.5 第三者の従事

契約相手方は、本職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（調達）**に定める特約条項を適用すること。

6. 提出文書の範囲、提出期限等

6.1 提出文書

表6に示す文書は、提出時期までに電子メール等の手段により提出し官側の承認を得ること。また、令和8年3月31日までに、可能な限り1枚のCD-R又はDVD-Rにまとめ、追記不可の処置を実施後、提出するものとする。また、作業の実施に当たり、当該文書の記載事項に疑義が生じた場合、速やかに該当箇所を修正し、官側の承認を得ること。

表6－提出文書

No.	文書名	部数	提出時期
1	作業実施計画書	電子媒体：1部	契約締結後速やかに
2	作業実施要領書	電子媒体：1部	契約締結後速やかに
3	業務従事者名簿	電子媒体：1部	契約締結後速やかに 役員変更があった場合その都度速やかに
4	防衛省OAシステム基盤移行計画書案	電子媒体：1部	最終成果物の提出時期は令和8年3月末とし、 途中成果物の提出時期は令和7年9月末とする。
5	防衛省OAシステム基盤運用計画書	電子媒体：1部	最終成果物の提出時期は令和8年3月末とし、 途中成果物の提出時期は令和7年9月末とする。
6	運用作業実施スケジュール案	電子媒体：1部	最終成果物の提出時期は令和8年3月末とし、 途中成果物の提出時期は令和7年9月末とする。
7	運用業務フロー図	電子媒体：1部	最終成果物の提出時期は令和8年3月末とし、 途中成果物の提出時期は令和7年9月末とする。
8	議事録	電子媒体：1部	開催から3営業日以内

6.2 提出方法

- a) 提出文書は、全て日本語で作成すること。ただし、英字で表記することが一般的な文言については、英字で表記することができるものとする。
- b) 用字・用語・記述符号の表記については、「**公用文作成の考え方**」の周知についてに準拠すること。
- c) 情報処理に関する用語の表記については、原則、**日本産業規格（JIS）**の規定に準拠すること。
- d) 提出文書は電子媒体（CD-R又はDVD-R等）により作成し、表6に示す提出部数を提出すること。また、電子媒体はウイルスチェックを実施した上で、追記不可の処置を施し提出するものとする。
- e) 提出文書の用紙のサイズは、原則として日本産業規格A列4番とするが、必要に応じて日本産業規格A列3番を使用すること。また、修正時等に差し替えが可能なようにバインダ方式とすること。
- f) 電子媒体による提出について、一太郎Government9、Microsoft Word 2019、同Excel 2019、同PowerPoint 2019で読み込み可能な形式及びPDF形式で作成し、提出すること。ただし、官側が他の形式による提出を求める場合は、調整の上、これに応じること。なお、契約相手方側で他の形式を用いて

提出する必要があるファイルがある場合は、官側と調整すること。

- g) 提出後、官側において改変が可能となるよう、図表等の元データも併せて提出すること。
- h) 提出文書の作成に当たって、特別なツールを使用する必要がある場合は、事前に官側の承認を得ること。

6.3 提出場所

提出文書は、原則として以下の場所に提出すること。ただし官側が別途指定する場合はこの限りではない。

(提出先)

〒162-8801 東京都新宿区市谷本村町5-1

防衛省整備計画局サイバー整備課デジタル化推進班

7. 作業場所

- a) 本調達に係る作業は、官側の指定する場所（都内）、契約相手方が用意する場所で行うこと。
- b) 作業環境（事務機器、備品及び消耗品等）は、契約相手方が用意すること。
- c) 調整や会議の打ち合わせの実施等は原則防衛省市ヶ谷地区、官側の指定する場所（都内）で行うこと。

8. 個人情報保護及び秘密保全等

8.1 個人情報保護

- a) 契約相手方は、官側から提供された個人情報及び業務上知り得た個人情報について、**個人情報の保護に関する法律**に基づき、適切な管理を行わなくてはならない。また、当該個人情報については、本業務以外の目的のために利用してはならない。
- b) 契約相手方は、本業務の実施に伴い知り得た保護情報の取扱いに当たっては、**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）**に基づき、保護すべき情報（以下「保護情報」という。）を適切に管理するものとし、その効力はこの契約終了後も継続するものとする。また、保護情報は、省内実施場所でのみ取り扱うものとし、持ち出す場合は必要な措置、手続きを講ずるものとする。
- c) 契約相手方は、**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の細部事項について（通知）**別添「情報システムの調達におけるサプライチェーン・リスク対応に関する特約条項」に基づき、サプライチェーン・リスク対応を実施すること。
- d) a)からc)のほか、官側は契約相手方に対し、本業務の適正かつ確実な実施を確保するために必要な範囲で、秘密を適正に取り扱うための措置を採るべきことを指示することができるものとする。
- e) 契約相手方は、本業務の契約の履行に必要であると官側が承認した場合を除き、情報を役務事務所以外の省外に持ち出してはならない。
- f) 契約相手方は、本業務の契約の履行に必要であると官側が承認した場合を除き、外部から省内実施場所へデータを持込んではいない。
- g) 本業務の実施において情報セキュリティが侵害され、又はその恐れがある場合には、適切

な措置を講じるとともに、直ちに把握し得る限りの全ての内容を、その後速やかにその詳細を官側に報告すること。

- h) 本業務の実施における情報セキュリティ対策の履行状況について、官側から実績の報告を求めた場合には、速やかに提出すること。
- i) 本業務の実施において、契約相手方における情報セキュリティ対策の履行が不十分であると認められる場合には、契約相手方は官側の求めに応じ、協議を行い、必要な対策を講じること。

8.2 秘密保全

- a) 官側が定める立入禁止の掲示がある場所及び官側が定める立入制限場所等（以下「立入禁止場所等」という。）へ立ち入る技術員等は、当該立入禁止場所等への立入手続等に関する達又は、官側等又はその指定した者が定める手続に従い、立ち入りを許可された者でなければならない。
- b) 契約相手方は、官側から貸付けを受けた文書及び電子データについては、当該業務終了時に官側に返却すること。また、提供を受けた文書及び電子データについては、当該業務終了前までに消去又は廃棄して、速やかにその旨を書面で報告すること。
- c) 本契約に係る情報及び情報システム以外の官側が所管する情報及び情報システムに不要なアクセスを実施しないこと。
- d) 立入禁止場所等への携帯電話、パソコン及び可搬記憶媒体の持込みについては、官側と協議の上、その指示に従うこと。
- e) 業務の遂行において契約相手方の情報セキュリティ対策の履行が不十分であると官側が認めた場合は、官側の求めに応じ協議を行い、官側と合意の上で、改善を図ること。
- f) 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をとること。
 - 2) 官側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をとること。
 - 3) 官側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をとること。

- g) 契約相手方は、知り得た保護情報の取扱いにあたっては、**情報セキュリティ通達**に基づき、**工**に示す保護すべき情報を適切に管理するものとする。

9. 提出書類の取扱い

9.1 知的財産権の帰属

9.1.1 著作権

- a) 提出文書に関する著作権は、官側に帰属するものとする。また、契約相手方は、防衛省が承認した場合を除き、提出文書に関する著作者人格権を行使しないものとする。
- b) a)に関わらず、提出文書に契約相手方が既に著作権を保有しているものが組み込まれている場合は、契約相手方が既に著作権を保有しているものの著作権についてのみ、契約相手方に帰属する。
- c) 契約相手方は、本業務の提出文書に関し、**著作権法**第27条及び第28条を含む著作権の全てを官側に無償で譲渡するものとする。
- d) 提出文書に第三者が権利を有する著作物が含まれる場合には、契約相手方が当該著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続きを行うものとする。
- e) a)及びc)において、官側は納入された著作物を自ら利用するために必要と認められる範囲で、翻案、翻訳、複製及び貸与することができるものとする。
- f) 本業務の提出文書等に関し、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官側の責めに帰す場合を除き、契約相手方の責任と負担において一切を処理すること。この場合において、官側は当該紛争の事実を知ったときは、契約相手方に必要な範囲で訴訟上の対応を契約相手方に委ねるなどの協力措置を求めるものとする。

9.1.2 権利義務の帰属等

- a) 本業務の実施が第三者の特許権、著作権その他の権利と抵触する場合は、契約相手方は、その責任において、必要な措置を講じなくてはならない。
- b) 契約相手方は、本業務の実施状況を第三者に提供し、又は公表しようとする場合は、あらかじめ、官側の承認を受けなければならない。
- c) 省内実施場所で生成した情報は、防衛省の所有に属するものとする。

10. 再委託

- a) 契約相手方は、本業務の実施に当たり、その全部を一括して再委託してはならない。
- b) 契約相手方は、本業務の実施に当たり、その一部について再委託を行う場合には、再委託先の事業者名、再委託先に委託する業務の範囲、再委託を行うことの合理性及び必要性、再委託先の履行能力並びに報告徴収、個人情報の管理その他運営管理の方法（以下「再委託先名等」という。）について記載した文書を提出し、官側の承認を受けなければならない。
- c) 契約相手方は、契約締結後やむを得ない事情により再委託を行う場合には、再委託先名等を明らかにした上で、官側の承認を受けなければならない。
- d) 契約相手方は、b)又はc)により再委託を行う場合には、契約相手方が官側に対して負う義

務を適切に履行するため、再委託先の事業者に対し8.に掲げる事項について、必要な措置を講じさせるとともに、再委託先から必要な報告を聴取しなければならない。

- e) b)又はc)に基づき再委託先の事業者に義務を実施させる場合は、全て契約相手方の責任において行うものとし、再委託先の事業者の責に帰すべき事由については、契約相手方の責に帰すべき事由とみなして契約相手方が責任を負うものとする。
- f) 契約相手方は、本業務の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は、情報システムの調達におけるサプライチェーン・リスク対応に関する特約条項に基づき必要な手続きを実施する。

11. 資料の貸与

契約相手方は、本役務の実施に当たり必要な官側の保有する資料等について、官側の許可を得た上で、閲覧又は貸与を受けることができる。官側が保有する資料の閲覧又は貸与を受ける場合は、取扱いに留意し、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こと。

12. 官側の支援

12.1 国有財産の利用

契約相手方は、本契約の履行に当たって必要な場合、官側が認める範囲内において、次に示す官側の支援を無償で使用することができる。

- a) 現地調査（現行システムの確認）に関する事項
- b) 本役務場所における搬入器材の保管
- c) 本役務場所における電力、水、スペース等の使用
- d) 本役務場所における施設の利用
- e) 本役務場所における官側の保有する関連器材の使用
- f) 本役務場所の回線
- g) 機能確認に関する事前調整及び現地確認時の支援
- h) その他、官側が認めた必要な事項

12.2 国有財産の使用制限

- a) 契約相手方は、12.1で示す国有財産について、本業務の実施及び実施に付随する業務以外の目的で使用し、又は利用してはならない。
- b) 契約相手方は、あらかじめ官側と協議した上で、官側の業務に支障を来さない範囲内において、施設内に本業務の実施に必要な設備等を持ち込むことができる。
- c) 契約相手方は、b)で設備等を設置した場合は、設備等の使用を終了又は中止した後、直ちに必要な原状回復を行う。
- d) 契約相手方は、既存の建築物、工作物等に汚損、損傷（機器の故障等を含む。以下同じ。）等を与えないよう十分に注意し、損傷が生じるおそれがある場合は、養生を行うものとする。損傷が生じた場合は、契約相手方の責任と負担において速やかに復旧しなければならない。

13. その他特記事項

- a) 本役務の推進に当たり、官側の指示に従うとともに、細部にわたり官側と密接な連絡を保ち、作業が良好、かつ安全に実施できるよう努めること。

- b) 契約相手方は、本役務契約の履行に当たり、第三者に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（調達）**に定める特約条項を適用する。
- c) 引用文書及び関連文書を閲覧する必要がある場合は、官側と協議すること。
- d) 本仕様書について疑義を生じた場合は、速やかに契約担当官側等と協議すること。
- e) 各機関等の長が定めた立入禁止場所等に立ち入る場合は、各機関等の立入手続に従い手続を実施するものとする。
- f) 6. に示す提出文書が、**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。

付表1_役務作業項目及び概要

凡例：○（主体）△（支援・連携）

No.	大項目	中項目	小項目	概要	本業務	備考	
1	サービスデスク	ヘルプデスク	省OA利用者対応窓口	省OA利用者及び局OA運用役務員からの問合せ及び各種依頼の受付	○	省OAの操作及び運用について、電話又はメールによる問合せに対する対応。各種問題切り分けに関するシステムエンジニア等への作業依頼を含む。障害等の受付は、項番7による。	
2				問合せ等内容の記録	○	問合せ等内容は、電子的に記録し、システム管理者及び役務員の情報共有を可能とする。	
3			システム利用方法問合せ対応	対応が容易又は既出の問合せに対する回答	○	パスワードの初期化等の定型的な問合せに対し、電話又は遠隔操作で対応する。	
4				官給ソフトウェアに関する問合せに対する回答	○	必要に応じてソフトウェア提供元へ確認し、回答する。	
5			申請等の受付業務の対応	各機関等からのシステム変更、異動等の申請について、申請の受付、対応及び申請情報の管理	○		
6			障害等の受付業務の対応	省OA利用者、防衛研究所電算機システム利用者及び局OA運用役務員からの障害通知の受付	○	障害内容の確認に関するシステムエンジニア等への作業依頼を含む。	
7				D I I に起因する省OA利用者からの障害通知の受付	○	一次切り分け後のD I I への問い合わせも含む	
8			現地対応	各局において、問合せ及び各種依頼への対応について、必要に応じた現地対応の実施	○		
9	ホームページ（防衛省内向け）の更新	ホームページ（防衛省内向け）管理	省OAに関するホームページ（防衛省内向け）登録、更新及び削除	○	掲載するコンテンツについてホームページ（防衛省内向け）にアップロード等を実施する。また、軽微な改修及び更新（日付や画像の更新、誤字脱字の修正）等を実施する。		
10				頻出する問合せ等内容及び回答の掲示	○	F A Q を作成し、更新してホームページ（防衛省内向け）に掲載する。	
11	I Cカード（ログオン専用I Cカード）	I Cカード管理	I Cカード利用登録（新規省OA利用者、臨時カード等）	○			
12				I Cカード利用停止の処置（紛失時）	○		
13				I Cカード忘失事の臨時I Cカード割り当て、パスワード初期化作業	○		
14	アクセス権管理	ファイルサーバのアクセス権管理	ファイルサーバにおける各フォルダのアクセス権設定状況の調査	○	年1回を基準に実施する。		
15				アクセス権調査結果の集計及びシステム管理者への報告	○		
16	防衛省携帯	アカウント情報提供	防衛省携帯のアカウント申請により、A D からアカウント情報を抽出し、管理元のD I I に提供	○			
17		端末及びアカウント情報登録及び設定	防衛省携帯のアカウント申請により、防衛省携帯及びアカウント情報をIntuneに登録し、防衛省携帯を設定	○			
18		デバイス管理	防衛省携帯の紛失時にリモートロック、リモートデータ削除等を実施	○			
19	障害管理	障害内容の確認	障害対応	障害の一次切り分け	○	サービスデスク等からの連絡による障害通知への対応を含む。必要に応じて、第2センターへの切替えの必要性についてシステム管理者に通報。	
20					D I I 提供サービスに関する障害の一次切り分け	○	
21					I a a S 基盤の障害対応	△	システム管理者を通じて、システム保守契約相手方及び加入システム管理者へ速やかに連絡するとともに、連携を図りつつ必要な支援を行う。
22				加入システムの障害対応	△	加入システム管理者からの依頼に応じて、I a a S 基盤のシステムログ等を確認して情報連携する。	
23				加入システム管理者からの依頼に応じて、第2センターへの切替えを実施	△	第2センターへの切替えにおいて、加入システム側及びシステム保守契約相手方が実施する作業に必要な支援を行う。	
24				加入システム管理者からの依頼に応じて、第1センターへの切戻しを実施	△	第1センターへの切戻しにおいて、加入システム側及びシステム保守契約相手方が実施する作業に必要な支援を行う。	
25				軽微な障害からの復旧	○	借上保守による対応が不要なもの（端末類の再セットアップ、システム保守役務契約相手方への障害の連絡及びシステム保守役務契約相手方による端末修理時の立会対応の対応等）を対象とする。	
26				保守窓口	障害内容の記録管理	○	
27					障害箇所調査	△	障害が発生しているハードウェア又はソフトウェアを特定する。電話又はメールにより対応する。

付表1_役務作業項目及び概要

凡例：○（主体）△（支援・連携）

No.	大項目	中項目	小項目	概要	本業務	備考
28		保守対応	ハードウェア修理	復旧方法の検討及び復旧スケジュールの設定	△	システム保守役務契約相手方の修理等の作業支援をする。
29			ハードウェア障害復旧	障害対応に伴うシステムの再起動	○	必要に応じて第2センターから切戻しを含む
30			ソフトウェア障害復旧	障害復旧後の動作確認	○	
31			データ復旧	障害対応等報告書の作成及び提出	△	システム保守役務契約相手方が作成する障害対応等報告書を確認する。
32	問題管理	省OAの問題管理	システム管理者に対する技術支援	システム借上契約相手方が導入したハードウェア、借上ソフトウェア、官給ソフトウェア及び官品ソフトウェアに関するシステム管理者からの問合せ及び要望事項への対応	△	
33					△	
34			大規模災害等の非常時訓練における対応	システム管理者が実施するシステム継続訓練等におけるシステムの正常性確認、復旧手順の確認等の技術的な支援を行う。また、非常時におけるシステム復旧要領の作成及びシステム管理者への技術支援を行う。	○	システム継続訓練等は年3回程度実施する。
35		加入システムからの要望・問い合わせ対応	加入システム支援	加入システムにおける変更作業において、実施可否の検討及び加入システム管理者における作業に対して必要な支援を実施	○	以下の作業等を想定 ・加入システムで設置した物理サーバ構成変更（クラスター設定等） ・各加入システム内のネットワーク構成変更 ・テナント内仮想サーバのリソース割当て変更
36			要望・問い合わせに対する基盤側作業	省OAの管理者側でしか対応できない要望等に対する実施可否の検討及び作業を実施	○	以下の作業等を想定 ・加入システムに割り当てたテナントのリソースプール変更
37	変更管理	形態管理	借上ソフトウェア及び官給ソフトウェア修正版適用（OSを含む。）	適用する借上ソフトウェア及び官給ソフトウェア修正版の選定	○	借上ソフトウェアに関する情報は、システム保守役務契約相手方が提供し、選定においても同契約相手方の支援を受ける。また、適用手順は、防衛省が貸与するシステム管理者マニュアルに従う。
38				適用実施計画の作成及びシステム管理者との調整	○	
39				検証の実施	○	
40				借上ソフトウェア及び官給ソフトウェア修正版の適用設定及び実施	○	
41	リリース管理	省OAの運用管理	ウイルス定義体適用管理	適用するウイルス定義体の選定及び検証	○	サーバ及び端末類を対象にウイルス定義体の適用を行う（1日1回を基準）。
42				定義体の配布設定及び実施	○	
43			セキュリティパッチ適用（OS）	適用するOSセキュリティパッチの選定	○	サーバ及び端末類を対象とし、月1回以上実施する（臨時更新を含む。）。
44				適用実施計画の作成及びシステム管理者との調整	○	選定においてはシステム保守役務契約相手方の支援を受けるものとし、適用手順は、防衛省が貸与するシステム管理者マニュアルに従う。
45				検証の実施	○	
46				OSセキュリティパッチの適用設定及び実施	○	
47			省OA利用者管理	新規の省OA利用者の登録	○	
48			省OA利用者データ修正	既存の省OA利用者の登録内容変更及び削除	○	身分証ICカード、ICカード立入証の忘失時の対応、パスワード忘失時のリセット対応及びDIIサービス利用申請を含む。
49			S/MIMEメール情報管理	S/MIMEメール利用者の登録及び削除	○	
50				公開鍵及び秘密鍵の登録	○	
51	個人端末管理	個人端末設置場所変更に伴う個人端末の設定変更	○	設定変更手順は、防衛省が貸与するシステム管理者マニュアルに従う。		
52	プリンタ類管理	プリンタ類設置場所変更に伴うプリンタ類の設定変更	○			
53	個人端末管理	貸出に伴う個人端末の設定	○			
54		個人端末の貸出及び個人端末貸出台帳の更新	○			
55		個人端末の返却時の受領、設定初期化等の実施	○			
56	端末類マスタの更新	適用すべき差分セキュリティパッチ、追加ソフトウェア等の選定	○	各機関等の端末類マスタを対象とし、年1回を基準に実施し、年間の運用状況を考慮して選定する。		
57		端末類マスタの更新作業の実施	○			
58	H/W、S/Wの接続又はインストール等	官品ソフトウェアインストール	事前動作検証及び手順確認	○	運用管理端末又は予備機で検証する。	
59			インストールに伴う設定変更	○	通信ポートの開放等を実施する。	
60			インストール対象の端末類におけるソフトウェアインストールの実施	○		
61			周辺機器の接続	事前動作検証及び手順確認	○	運用管理端末及び予備機で検証する。
62			ハードウェア接続に伴うデバイス接続の許可設定	○	設定手順は、予め手順化されたものに従う。	

付表1_役務作業項目及び概要

凡例：○（主体）△（支援・連携）

No.	大項目	中項目	小項目	概要	本業務	備考
63				ハードウェア接続の実施	○	
64			官品ソフトウェア修正 版適用	官品ソフトウェア修正版適用の検討及び検証	○	
65			【ソフトウェア改良版 の提供】	適用スケジュールの設定	○	
66				官品ソフトウェア修正版適用の実施	○	
67				官品ソフトウェア修正版適用後の動作確認の実施	○	
68			NAS（システム管理 者指定）管理	システム管理者が指定するNASの接続並びにアク セス権の付与及び削除	○	
69			ネットワーク管理	ネットワーク機器の設定変更	○	端末類、プリンタ類の設置場所変更等に伴う作業を行 う。
70				ネットワークケーブルの敷設作業の支援	○	端末類、プリンタ類の設置場所変更等に伴う作業を行 う。
71	構成管理	省OAの運用管理	省OA利用者管理	省OA利用者管理台帳の更新	○	アクセス権の管理を含む。
72			端末類管理	省OA提供機能の物品管理機能である物品管理ツ ールによる端末類等管理台帳の更新	○	IPアドレス管理、MACアドレス管理並びに端末類 及びプリンタ類の状態、消耗品在庫、設置状況及びソ フトウェアのバージョン管理を行う。
73			周辺機器の接続	省OA提供機能の物品管理機能である物品管理ツ ールによる端末類等管理台帳の更新	○	周辺機器の接続情報を管理する。
74			情報資産管理標準シ ート等の管理	情報資産管理標準シート等の作成及び更新	○	登録の発生及び変更の都度実施する。
75		H/W、S/Wの接続又はイ ンストール等	官品ソフトウェアのイ ンストール	省OA提供機能の物品管理機能である物品管理ツ ールによるインストール実施後の端末類等管理台帳の 更新	○	ソフトウェアのインストール情報を管理する。
76			官給ソフトウェアイン ストール	省OA提供機能の物品管理機能である物品管理ツ ールによるインストール実施後の端末類等管理台帳の 更新	○	ソフトウェアのインストール情報を管理する。
77	保全管理	省OAの保全管理	死活監視	サーバ及びネットワーク機器の死活を監視	○	
78			リソース監視	CPU、メモリ、ストレージの使用率及び使用量を監視	○	
79			トラフィック監視	ネットワークトラフィックを監視	○	
80			サービス監視	サービス提供状況を監視	○	
81			日常点検	各種ログの確認による、エラー及びセキュリティイ ンシデントチェック	○	イベントログの確認、不正アクセス、ウイルス検出状 況の確認等を実施する。
82				トラフィック情報の定期的な取得、分析及び管理	○	月1回を基準に実施する。
83				プリンタ類の定期的な使用状況調査及び報告	○	印刷枚数の確認を月1回を基準に実施する。
84			停電時の点検	計画停電後におけるネットワークスイッチの復電及 び導通確認	○	休日で年10回程度点検する（1回につき1棟程度実 施。ただし、うち1回は全棟が対象）。
85			定期バックアップ	自動運用状況の確認	○	
86				バックアップテープの世代管理	○	バックアップテープの交換作業を含む。
87				バックアップデバイスのクリーニング	○	
88				バックアップ取得スケジュールの変更	○	設定変更手順は、防衛省が貸与するシステム管理者マ ニュアルに従う。システム管理者から変更の指示が あった場合を含む。
89			任意バックアップ/リ ストア	バックアップ/リストアスケジュールの調整と設定	○	依頼に応じて行う任意ファイルのバックアップ/リス トアを実施する。
90				バックアップ/リストアスケジュールの実行	○	依頼に応じて行う任意ファイルのバックアップ/リス トアを実施する。
91	セキュリティ管理	セキュリティインシデ ント管理	セキュリティ監視	リアルタイム脅威分析	○	分析手法のチューニングを含む。
92				予防措置	○	収集した脅威情報及び脆弱性情報から予防的措置を実 施する。
93				脆弱性情報の収集	○	構成品の脆弱性情報を収集する。
94				セキュリティ監視状況の報告	○	脅威分析情報、脆弱性情報及び予防措置内容につい て、定期的な報告を実施する。 また、必要性に応じて、適宜報告を実施する。
95			セキュリティインシデ ント対応	該当する省OA利用者への連絡	○	LANケーブル抜線の依頼を含む。
96				セキュリティインシデント発生時の調査及び対応	○	省OA利用者への聞き取り確認、完全スキャン実施依 頼及びウイルス定義ファイルの更新確認を含む。
97				セキュリティインシデント発生報告書の作成及び報 告	○	システム管理者へ報告する。
98			セキュリティ改善支援	各取得ログの統計及びセキュリティリスクの分析	○	各取得ログ（防衛省が取得したログを含む。）を分析 し、セキュリティホールが判明した場合のシステム管 理者への提案及び対策の実施を含む。
99	システム利用状況 報告	システム利用状況報告	利用状況調査	機器構成や定期的に取得した性能状況レポートをも とに、システム利用状況を分析	○	四半期に1回を基準に実施する。
100			利用状況報告	システム利用状況報告書を作成し、利用状況を報告	○	報告者は、統括役務員及び副統括役務員とする。 報告はシステム管理者との報告会でを行う。

付表1_役務作業項目及び概要

凡例：○（主体）△（支援・連携）

No.	大項目	中項目	小項目	概 要	本業務	備 考
101	役務実施報告	システム利用状況報告 (IaaS基盤)	IaaS基盤利用状況 調査	05増設で構築された各装置において、機器構成や 定期的に取得した性能状況レポートをもとに、シス テム利用状況を分析	○	四半期に1回を基準に実施する。
102			IaaS基盤利用状況 報告	システム利用状況報告書(IaaS基盤)を作成 し、利用状況を報告	○	報告者は、統括役員とする。報告はシステム管理者 との報告会で行う。
103		RMF対応	継続監視計画	RMFの継続監視計画書に定められた確認内容につい て、定期的な確認を行い、エビデンスを提示	○	四半期に1回を基準に実施する。
104		役務実施報告	運用状況報告	役務実施日報を作成し、運用状況を報告	○	報告者は、統括役員及び副統括役員とし、報告は メールで行う。
105		役務実施週報を作成し、運用状況を報告	○	報告者は、統括役員及び副統括役員とする。 報告はシステム管理者との報告会で行う(週1回30 分程度)。なお、省OAのテレビ会議システムを利用 して報告できるものとする。		
106	役務実施月報を作成し、運用状況を報告	○	報告者は、統括役員及び副統括役員とする。 報告はシステム管理者及び各機関等担当者との報告会 で行う(月1回1時間程度)。なお、省OAのテレビ 会議システムを利用して報告できるものとする。			
107	役務実施年間報告書を作成し、運用状況を報告	○	報告者は、統括役員及び副統括役員とする。 なお、省OAのテレビ会議システムを利用して報告で きるものとする。			
108	継続的な運用改善	運用改善案の提案	利便性、セキュリティ、官の負荷軽減、運用業務の 効率化等の観点から運用改善案の提案を実施	○	監視項目、業務フロー等の見直しを年に1回を基準に 実施する。	

