支担官第９３３号

令和７年１月２７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。

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-KI-017	防衛施設建設情報管理システム運用支援保守業務	仕様書のとおり	仕様書のとおり	自：令和７年２月２７日 至：令和１１年２月２８日

２．入札方式　　一般競争入札（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２月２７日（木）１０：３０

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 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７年２月１３日（木）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3.2（１）～（３）に定める本業務の実施体制並びに仕様書4.2ｆ）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２月１３日（木）１２：００。必要に応じ追加資料の提出を求めることがある。）。

（５）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２月２５日（火）までに、下記担当者必着分を有効とする。

（６）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。

（７）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　黒田　電話　03-3268-3111　内線20822

仕様書			
件名	防衛施設建設情報管理システム運用支援保守業務	作成年月日	令和７年１月１４日
		作成課	整備計画局　建設制度官付

1　総則

1.1　適用範囲

本仕様書は、防衛施設建設情報管理システム（以下「本システム」という。）の運用保守業務（以下「本業務」という。）について規定する。

1.2　用語の定義

本仕様書で使用する用語は**別紙１**のとおりとする。

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なすものであり、入札書または見積書の提出時における最新版を適用するものとする。

なお、引用文書に定める項目が、本仕様書の内容と異なる場合は、本仕様書を優先とする。

（１）法令等

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細部事項について（通知）（装プ武第 188 号。31.1.9）

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。）

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）

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。令和５年７月３日）

デジタル・ガバメント推進標準ガイドライン（２０１８年（平成３０年）３月３０日各府省情報化統括責任者（ＣＩＯ）連絡会議決定）（以下**「標準ガイドライン」**という。）

政府情報システムの整備及び管理に関する標準ガイドライン実務手引書（２０１７年（平成２９年）４月１１日付）（以下**「標準ガイドライン実務手引書」**という。）

デジタル・ガバメント推進標準ガイドライン解説書（２０２３年（令和５年）５月１２

日）（以下**「標準ガイドライン解説書」**という。）

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（２０２３年（令和５年）３月３１日）（以下**「標準ガイドライン実践ガイドブック」**という。）

1.3.2　関連文書

（１）仕様書

防衛施設建設情報管理システムアプリケーション開発業務　調達仕様書

防衛施設建設情報管理システム構築等業務　調達仕様書

防衛施設建設情報管理システム換装業務　調達仕様書

（２）設計書

防衛施設建設情報管理システム換装業務　業務成果品

建設 CALS 用電子納品保管管理システム借上の運用支援保守（平成 25 年度）業務成果品

（３）通達等

防衛省インフラ長寿命化計画（行動計画）について（通達）（防整施（事）第 25 号。27.10.1）

防衛省デジタル・ガバメント中長期計画（２０２２年（令和４年）１２月１２日。防衛省行政情報化推進委員会決定）（以下**“防衛省デジタル・ガバメント中長期計画”**という。）

1.4　調達の背景・目的、期待する効果

平成２５年６月１４日に閣議決定された「日本再興戦略」において、国民生活やあらゆる社会経済活動を支える各種施設をインフラとして幅広く対象とし、戦略的な維持管理・更新等の方向性を示す基本的な計画として、国としての「インフラ長寿化基本計画（基本方針）」がとりまとめられ、この基本計画に基づき、防衛省におけるインフラ長寿命化対策を着実に推進するための方向性を明らかにするため、「防衛省インフラ長寿命化計画（行動計画）」を策定し、取り組みを推進することで維持管理・更新等に係るトータルコストの縮減及び予算の平準化を図ることとした。

日本全国に存在する防衛施設の現状や維持管理・更新に関する情報を省内統一的に運用し、メンテナンスサイクルの構築や維持管理・更新に係るトータルコストの縮減・予算の平準化を実現するため、令和２年度に本システムを整備している。

防衛省情報基盤（DII）の仮想サーバの提供終了に伴い、「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」に示されているクラウド・バイ・デフォルトの原則及び防衛省クラウド整備指針に基づき、情報基盤としてガバメントクラウドを選定し、令和６年度に本システムの換装事業（システム設計・開発、環境構築及びデータ移行等）を実施している。

別紙4　移動端末関連要件

番号	機能	機能詳細
1	運用管理	(1)　端末類のハードウェア情報や、各種アプリケーションのインストール状況を確認できること。また、各種アプリケーションごとのインストール台数、インストール日時、プロダクトID、ライセンス保有状況等の情報が把握できること。 (2)　端末へスクリプトを用いたソフトウェア配布機能を有すること。なお、スクリプトについては、保守契約の範囲で別途費用を発生させず、作成個数に制限無く提供されること。 (3)　IT資産管理台帳として、インストールソフトウェア台帳・ソフトウェアライセンス台帳・ソフトウェア関連部材台帳・ハードウェア台帳の4つの台帳で管理が行えること。 (4)　システム運用の自動化・省力化及びハードウェアの資源管理を支援できること。 (5)　管理コンソール上から、端末を遠隔操作（リモートワイプ等）できること。
2	時刻同期	(1)　端末が正確な時刻を保つような仕組みを有すること。 (2)　※なお、本端末はネットワーク接続不可のため、システム的な対応が困難であれば、運用での代替提案も可とする。
3	セキュリティ対策	(1)　※端末は、持出し先での紛失等による情報漏えいを防止するため、システム領域を含む補助記憶装置全体を秘匿化できること。 (2)　※CALSシステムとの有線LANケーブル又はUSBケーブル経由でのデータやり取りを除き、データの持ち出し行為を原則禁止とし、ネットワーク接続や可搬記憶媒体の利用を制御できること。 (3)　紛失・盗難時の情報漏えい対策（PIN・パスワード管理、リモートワイプ設定）を行うこと。 (4)　デバイス制御（ネットワーク接続制御・外部メディア利用制御　等）を行うこと。 (5)　アプリケーション制御（インストール制御、各種機能の利用・変更制御等）を行うこと。 (6)　資産管理（端末情報管理、セキュリティポリシー管理　等）を行うこと。 (7)　上述の制御について、システム管理者が、課等ごとの管理者権限を有するものに対して、一時的に制御を解除・変更できること。 (8)　端末及びシステム管理者の操作ログを取得すること。 (9)　※暗号化方式には電子政府推奨暗号又は防衛省独自の暗号等を用いること。
4	ログ管理	(1)　以下に示すログを収集し、監査証跡が取得できること。 (ア)※ログオン（成功・失敗）・ログオフ (イ)※ファイル操作ログ（参照・作成・更新・移動・削除） (ウ)※アプリケーション実行ログ（起動・終了） (エ)※可搬記憶媒体接続ログ（デバイス構成変更ログ）

番号	機能	機能詳細
		(オ)※ファイルアクセス (カ)※ウイルス対処ログ (キ)※資産管理ログ(資産管理台帳) (ク)※ユーザ作成・変更・削除ログ(アカウント変更作業履歴) (2) 端末の操作ログについては、ネットワークに接続できない状況でも取得・保存できること。 (3) 端末類のインベントリ情報を収集し、運用管理端末の画面上に収集した情報を一覧表示又は印刷できること。 (4) 収集するログの選択及び追加の権限は、システム管理者のみが有すること。 (5) ログビューアによるログの検索結果からファイルの操作履歴を追跡できること。 (6) ※端末類から収集したログデータは一定期間保管すること。
5	不正接続の防止	(1) ※端末は有線LANケーブル又はUSBケーブル経由でCALSシステムと接続してデータやり取りを行う想定であるが、それ以外の機器(許可されていない機器)の接続を防止する仕組みを有すること。 (2) ※不適合端末(未許可端末やウイルス対策未実施等)を検知する仕組みを有すること。
6	ユーザ認証・ユーザ管理機能	(1) ※端末へのログオンは許可された利用者のみに許可すること(本人認証及びPIN管理)。 (2) 部・課毎にログオン認証可能なグループを指定することが可能であること。 (3) 利用ユーザの管理ができること。また、ユーザの異動等におけるユーザ識別情報や権限の登録・更新ができること。
7	ウイルス対策	(1) ※ウイルス対策ソフトウェアを適用し、ウイルス定義体の更新を行うこと。 (2) 端末のウイルス対策状況の一元管理ができること。
8	ソフトウェア脆弱性対策	(1) ※OSやアプリケーションの脆弱性に対して適用パッチを適用すること。

注1:※は、ネットワークが接続されてなくてもできる作業である。

注2:上記項目は1例とし、移動端末が接続する既設 PC の各システム(省 OA システム、局 OA システム、陸上業務システム等)毎により非機能要件が異なる場合がある。

別紙3_サービスレベル要求書

大項目	中項目	内容	対応時間／頻度
システム監視業務		・本システムの異常を自動で検知・通報する仕組み等の利用あるいはガバメントクラウドが提供するシステム監視運用サービスを利用し、障害の早期発見と正常稼働の担保に努めること。	平日9:00～18:00／週1回
	死活監視	・本システムの異常通知がないかを監視する。	平日9:00～18:00／日1回
	閾値監視	・サーバのCPU、メモリ、ディスク等の閾値を超える利用が無いかを監視する。	平日9:00～18:00／日1回
	サービス、プロセス監視	・サービス、プロセスに異常が無い事を監視する。	平日9:00～18:00／日1回
	バックアップ監視	・バックアップ処理にて異常が無い事を監視する。	平日9:00～18:00／週1回
	ウイルス対策監視	・ウイルススキャンに異常通知が無いかを監視する。 ・ウイルスパターンファイルの更新確認する。	平日9:00～18:00／週1回
	ログ監視	・サーバのイベントログに異常が無いことを監視する。 ・イベントログを保存する。	平日9:00～18:00／週1回
ヘルプデスク業務		・本システムの利用に関連し、官・民からの各種問い合わせに対応すること。 ・問い合わせ対象は本システム及び補助ツール（施設点検用アプリケーション、電子納品物作成支援ツール、電子納品保管管理データ登録支援ツール）も含む。	受付：24時間365日 対応：平日9:00～17:00
	電話、電子メールによる質問受付・回答	・問い合わせに必要な電話回線（1回線以上）及び電子メールアドレス（1つ以上）を準備すること。 ・利用者への周知やHPの変更作業等を実施すること。	平日9:00～17:00 回答期限は原則、受付翌平日17:00まで
	官の利用者に対するクライアント端末設定等の支援	・契約相手方の責任で回答が不可能な問い合わせがあった場合は、速やかに官側に連絡すること。 ・ヘルプデスク業務を実施する場所及び使用する機器類はヘルプデスク業務専用とし、契約相手方が準備すること。	平日9:00～17:00
	利用者に対するシステム基本操作支援		平日9:00～17:00
	ヘルプデスク受付回答状況の報告		日次
運用支援業務		本システムを運用する上で、以下の各種業務支援を実施すること。	受付：24時間365日 対応：平日9:00～18:00 （12:00～13:00は休憩） ※上記時間外での対応あり
	①業務運用支援作業		
	データ登録支援	・データの新規登録作業は原則職員が実施。職員から支援依頼があった場合に対応すること。	必要都度
	データ削除支援	・文書保存期限を過ぎたデータについて官側担当者に確認した上でデータ削除を支援すること。	必要都度
	登録データ更新支援	・以下データの更新作業を支援すること。 防衛施設建設情報管理システムにおける所属局、所属機関、所属基地、駐屯地等、名称、住所、所在地（緯度・経度）、電話番号、施設ID、既存の施設区分（庁舎、隊舎）、既存の施設面積、新規及び既存又、非正規に登録された電子納品データ ・工事・業務名称完成年月日等の基本情報の入力を行うこと。	必要都度
	②システム保全作業		
	アプリケーションプログラムのパッチ等適用作業	・アプリケーション及びソフトウェアの修正モジュール、セキュリティパッチ等の適用作業を行うこと。実施にあたっては契約相手方が用意する環境にて検証を行い、官の承認後に本番適用を行うこと。	必要都度
	構成情報管理	・アプリケーションプログラム、ソフトウェア、ガバメントクラウドのプラットフォーム環境（AWSサービス）、ネットワーク構成（GSS G-Net含む）等の構成管理を実施すること。	構成変更都度
	情報提供	・本システムの構成品や運用に関するセキュリティ脆弱性に係る情報について、情報提供すること。	必要都度
	ソフトウェア等の運用保守業務	・別契約「防衛施設建設情報管理システム換装業務」で調達するソフトウェアに対して保守を実施すること。	対応：平日9:00～18:00 （12:00～13:00は休憩） ※緊急時は上記時間外での対応について官と協議すること。
	③その他作業		
	データ抽出作業等	・官が指定する各種条件でのデータ抽出、本システムの運用上不要となったデータの削除等を実施すること。	年間約10件
	システム改修を伴わない設定変更作業	・本システムに対する設定変更等の軽微な作業を実施すること。	年間約3件
	FAQの作成	・本システムの利用における頻出問い合わせ等をFAQとして整理すること。	必要都度
	防衛施設建設情報管理システムの最適化検討に関する技術支援	・本システムに係る関係者（DII、内部部局等、ガバメントクラウド関係機関等）との調整及び検討に対し、情報提供等の支援を実施すること。	年間約1件
障害対応・保守手配業務			
	アプリケーションプログラムに関する障害対応	・別契約「防衛施設建設情報管理システム換装業務」で作成するアプリケーション等に対し、不具合を検知・受付した際、対応を実施すること。	対応：平日9:00～18:00 （12:00～13:00は休憩） ※緊急時は上記時間外での対応について官と協議すること。
	ソフトウェア製品及びプラットフォーム環境に関する障害対応	・別契約「防衛施設建設情報管理システム」で調達するソフトウェア製品及びプラットフォーム環境に対し、不具合を検知・受付した際、対応を実施すること。	対応：平日9:00～18:00 （12:00～13:00は休憩） ※緊急時は上記時間外での対応について官と協議すること。
	タブレット端末に関する対応	・本システムにて利用する移動端末に対し、不具合を検知・受付した際、官が指定する作業場所（市ヶ谷敷地内に限る）にて対応を実施すること。 ・障害の原因がソフトウェア（官側のソフトウェアを除く）やハードウェアの設定にある場合、ソフトウェアの再インストール、再設定を行い速やかに障害から回復させること。 ・記憶装置を有する機器を廃棄、返却又は修理などのために官側の施設から持ち出す場合、データ消去（※）を実施すること。 ※記憶装置の記憶域全体をソフトウェアなどによって重ね書き（無意味な文字・数字。記号を含む）を2回以上実施すること、もしくは官側の立ち合いで消磁又は破壊すること。 ・本システムを利用可能とするための作業（※）を実施すること。必要な情報は官側から提供するものとする。 ※ハードウェア、OSなどの設定及び施設点検用タブレットアプリケーションツールのインストール、設定、利用環境に応じたネットワーク設定及び動作確認	必要都度
	省既存環境等に関する障害対応	省既存環境及びガバメントクラウド環境との連携が必要な場合、協力して対応にあたること。	必要都度
	パッチ提供	本システムを構成するソフトウェアにおいて、ソフトウェアの脆弱性対応等のため修正プログラム（以下「パッチ」という）をソフトウェアの製造元が発表した場合、契約相手方は速やかに当該製造元からパッチを入手し、官側に提供すること。	必要都度
	その他作業	他省庁の動向調査を行い、必要に応じて本システム関連文書の改訂支援を行うこと。	必要都度
情報提供業務			

	防衛施設建設情報管理システムホームページの運用	・契約相手方は別契約「防衛施設建設情報管理システム換装業務」にて防衛省職員向けに作成したウェブサイトを利用してFAQ、運営スケジュール、稼働状況及び緊急連絡先等を公開すること。 ・ホームページの内容を随時更新し、最新の状態を維持すること。緊急の連絡事項がある場合、官側に報告するとともにホームページに当該情報を掲載すること。 ・ホームページのアドレス変更等が発生する場合、新しいホームページアドレスを案内する等、利用者が継続利用するための支援を実施すること。	必要都度
次期システムへの更改支援業務			
	データ移行支援	業務引継に伴いデータ移行が発生する場合、移行に必要なデータを汎用的なデータ形式（CSV等）に加工し、無償で提供すること。またファイル・データレイアウト等の資料を提供し、誠意をもって協力すること。なお、国際基準等に則る標準的なレイアウトに対応する業務については、標準的なレイアウトでのデータ提供を行うこと。	必要都度
	システム終了対応支援	本契約終了時、本システムの停止、撤去、廃棄に係る作業を行うこと。	システム終了時
その他業務			
	RMFに係る支援業務	官からの要望に基づき、必要に応じてRMFに係る支援を実施すること。	必要都度
	ガバクラ調整に係る支援業務	官からの要望に基づき、必要に応じてガバクラ利用に係る各種支援作業を実施すること。 ・リソース増減の申請、設定作業等の申請等	必要都度

別紙２　システム構成環境等

1　概要

「防衛施設建設情報管理システム（以下、「本システム」という。）は、DII 部内オープン系ネットワーク及び政府共通ネットワーク(GSS)を経由しガバメントクラウドに接続し、ガバメントクラウドの情報基盤及び提供サービスを利用する。また、本システムの利用端末には、既存の省 OA 端末等を利用する。

なお、本システムは本省（市ヶ谷）のみならず、各拠点（各地方防衛局（地方防衛支局、防衛事務所含む)、各陸上自衛隊、各海上自衛隊、各航空自衛隊、防衛大、防衛医大、各通信所、各試験場等）の職員もアクセス可能である。

本システムのシステム構成イメージは図１のとおり。

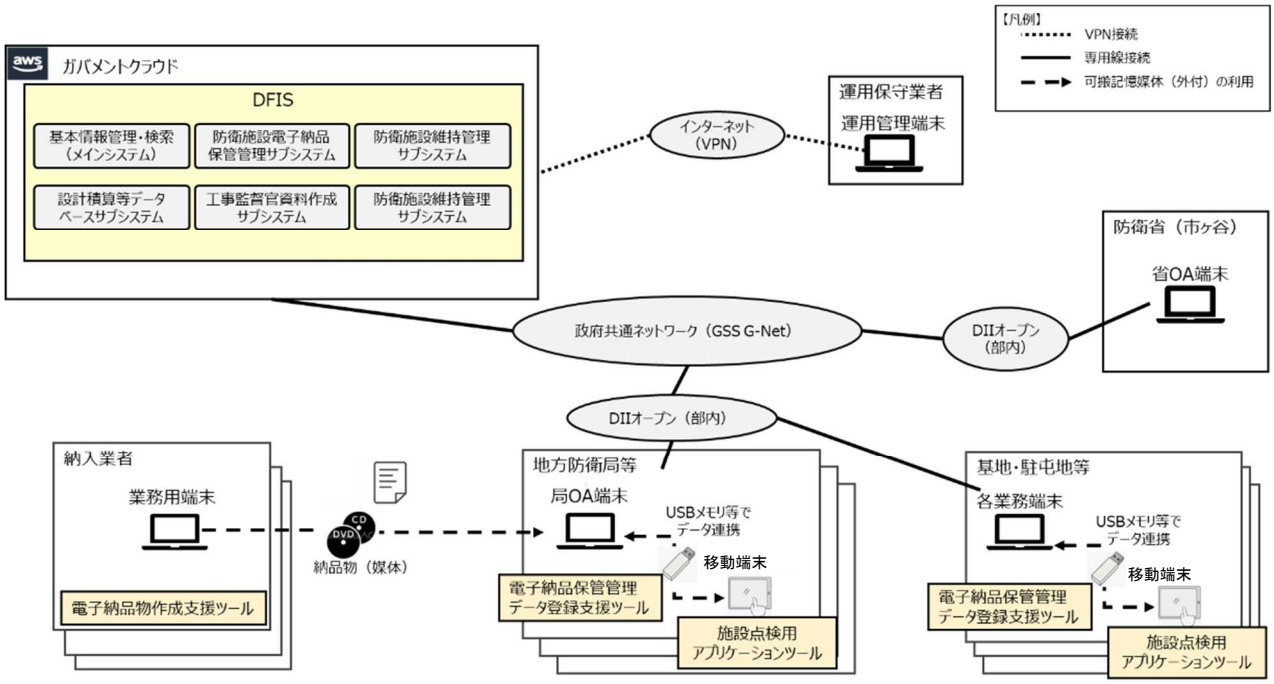


図１　システム構成イメージ

2　役割分担

2.1　作業・責任分担の基本

本システムの稼働にあたっては、ガバメントクラウドを管理するＣＳＰ及び省既存環境保守業者、利用システムの運用保守事業者が協力して作業に当たる必要がある。各環境における作業・責任分担の基本については、ガバメントクラウド等の各種ガイドライン及び、省既存環境の提供範囲等に基づき対応を実施する。

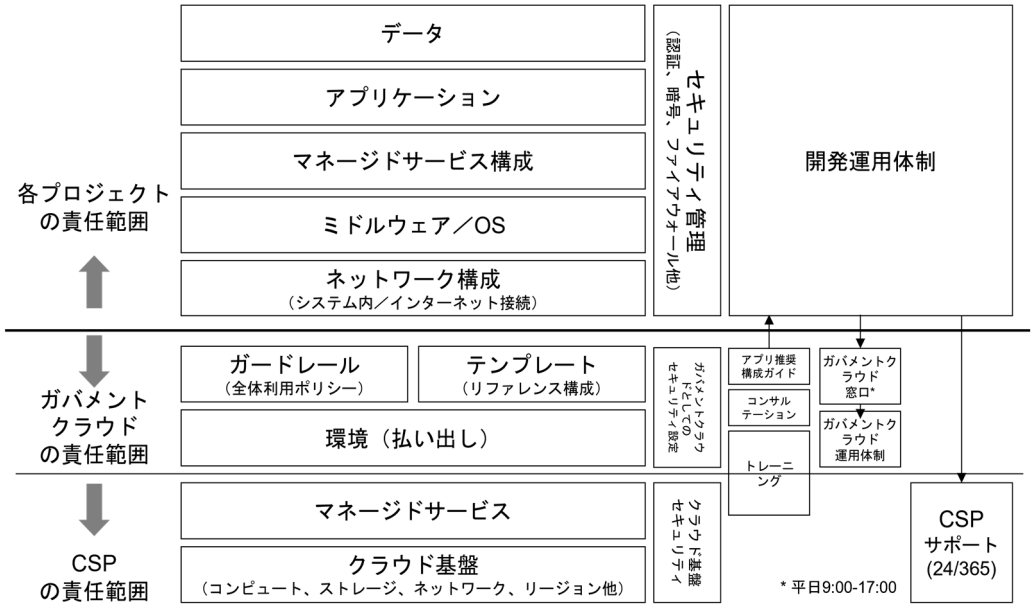


図２　ガバメントクラウドにおける責任範囲

（ガバメントクラウド　手続き概要(5.3 版)　1.7 責任分解点より）

表１　本システムにおける責任分担・作業役割分担

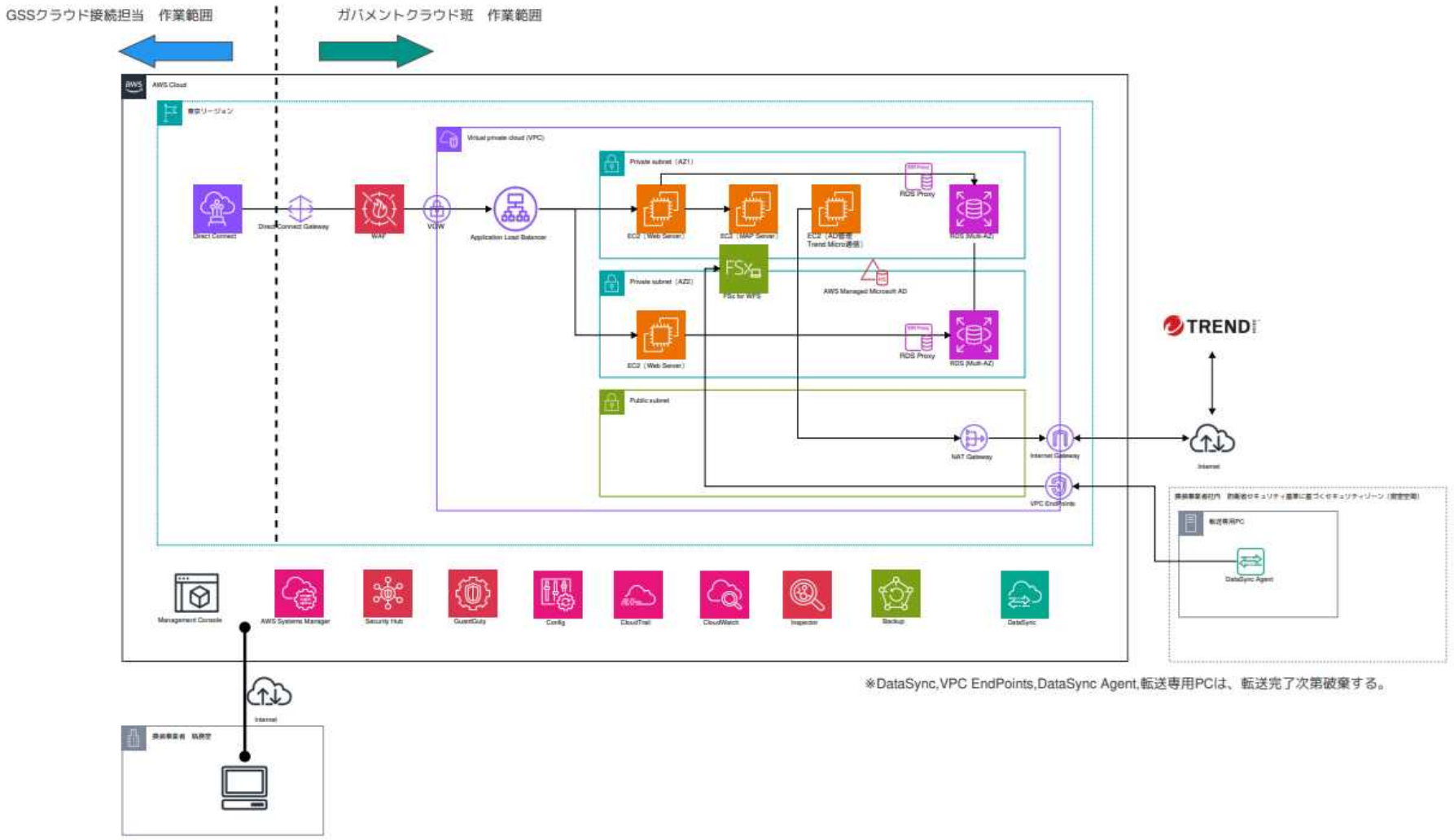
利用拠点	対応範囲	担当
ガバメントクラウド	DFIS データ	運用保守支援事業者
	DFIS アプリケーション	運用保守支援事業者
	ミドルウェア／OS	運用保守支援事業者
	内部 NW	運用保守支援事業者/CSP
	設備環境	デジタル庁(CSP)
	クラウド基盤	デジタル庁(CSP)
政府共通ネットワーク(GSS)		デジタル庁（GSS　G-ne t ）
DII 部内オープンネットワーク		防衛省(統合幕僚監部)
防衛省内	省 OA 端末等	省 OA 端末等保守事業者
	移動端末	各部隊等
納入業者拠点	業務用端末	納入業者
ネットワーク(VPN)		運用保守支援事業者/ISP
運用保守事業者拠点	運用保守用端末	運用保守支援事業者

※納入業者端末については、運用保守支援業務の対象外

3　システム構成

3.1　ガバメントクラウド環境

3.1.1　環境構成



3.1.2 構成詳細

AWS Pricing Calculator より引用

リージョン	説明	サービス	設定の概要
アジアパシフィック（東京）	WEB サーバー（r5n,8cpu,64gb）2 台	Amazon EC2	テナンシー（共有インスタンス），オペレーティングシステム（Windows Server），Workload（Consistent，Number of instances：2），高度な EC2 インスタンス（r5n.2xlarge），Pricing strategy（On-Demand Utilization：100 %Utilized/Month），モニタリングを有効にする（disabled），EBS ストレージ量（300 GB），DT Inbound：Not selected（0 TB per month），DT Outbound：Not selected（0 TB per month），DT Intra-Region：（0 TB per month）
アジアパシフィック（東京）	MAP サーバー（r5n,4cpu,32gn）1 台	Amazon EC2	テナンシー（共有インスタンス），オペレーティングシステム（Windows Server），Workload（Consistent，Number of instances：1），高度な EC2 インスタンス（r5n.xlarge），Pricing strategy（On-Demand Utilization：100 %Utilized/Month），モニタリングを有効にする（disabled），EBS ストレージ量（2400 GB），DT Inbound：Not selected（0 TB per month），DT Outbound：Not selected（0 TB per month），DT Intra-Region：（0 TB per month）
アジアパシフィック（東京）	ストレージ（FSx）マルチ AZ、30TB、バックアップ（30TB）	Amazon FSx for Windows File Server	希望するストレージ容量（30 TB），バックアップストレージ（0 TB），必要な合計スループット（200 MBps），プロビジョンド SSD IOPS（自動）
アジアパシフィック（東京）	DB（サーバレス）マルチ、1 台	Amazon RDS for SQL server	各 RDS インスタンスのストレージ（汎用 SSD（gp3）），ストレージ量（2500 GB），ノード（1），インスタンスタイプ（db.m5.4xlarge），使用状況（オンデマンドのみ）（100 %Utilized/Month），価格モデル（OnDemand），デプロイオプション（Multi-AZ），ライセンス（License included），データベース版（Standard），追加のバックアップストレージ（0 TB），汎用 SSD（gp3）- IOPS（3000），汎用 SSD（gp3）- スループット（125 MiBps）

リージョン	説明	サービス	設定の概要
アジアパシフィック（東京）	VPC	Network Address Translation (NAT) Gateway	NAT ゲートウェイの数 (1)
アジアパシフィック（東京）	VPC	AWS PrivateLink	AWS リージョンあたりの VPC インターフェイスエンドポイントの数 (6)
アジアパシフィック（東京）	Config	AWS Config	記録された継続的な設定項目の数 (100), 設定ルール評価の数 (100)
アジアパシフィック（東京）	Cloud Trai	AWS CloudTrail	管理イベントの単位（百万), 書き込み管理の証跡 (3), 読み込み管理の証跡 (3), データイベントの単位（百万), S3 証跡 (3), Lambda 証跡 (3), Insights イベントの単位（百万), Insight イベントを伴う証跡 (3), 書き込み管理イベント (1 /月), 読み込み管理イベント (1 /月), Lambda データイベント (1 /月), 分析された書き込み管理イベントの数 (1 /月), S3 オペレーション (1 /月)
アジアパシフィック（東京）	GuardDuty	Amazon GuardDuty	EC2 VPC フローログ分析 (1 GB per 月), EC2 DNS クエリログ分析 (1 GB per 月), EBS ボリュームデータスキャン分析 (2000 GB per 月), Lambda VPC フローログ分析 (0 GB per 月), RDS プロビジョンドインスタンス vCPU (1 /月), Aurora Serverless v2 インスタンス ACU (0 /月)
アジアパシフィック（東京）	Security Hub	AWS Security Hub	アカウント数 (5), アカウントごとのセキュリティチェックの数 (100), アカウントごとの検出結果の取り込み数 (500)

リージョン	説明	サービス	設定の概要
アジアパシフィック（東京）	Direct Connect	AWS Direct Connect	ポート数 (4)，ロケーション (AT Tokyo Chuo Data Center, Tokyo, JPN)，ポートタイプ (Hosted)，ポート容量 (100M)，データ転送（送信）(1 TB)，データ転送（受信、無料）(1 TB)
アジアパシフィック（東京）	CloudWatch	Amazon CloudWatch	メトリクスの数（詳細メトリクスとカスタムメトリクスを含む）(10)，GetMetricData: リクエストされたメトリクスの数 (20000)，GetMetricWidgetImage: リクエストされたメトリクスの数 (20000)，その他の API リクエストの数 (20000)，Canary の実行回数 (30000)
アジアパシフィック（東京）	ActiveDirectry	AWS Directory Service	ディレクトリの合計数 (1)，追加ドメインコントローラーの合計数 (0)，エディション (Standard)，共有されるディレクトリの数 (0)，各ディレクトリを共有する追加アカウントの数 (0)，共有ディレクトリのエディション (Standard)
アジアパシフィック（東京）	Amazon Inspector	Amazon Inspector	1 か月あたりにスキャンされた EC2 インスタンスの平均*数 (4)
アジアパシフィック（東京）	AD 管理用の Windows	Amazon EC2	テナンシー (共有インスタンス)，オペレーティングシステム (Windows Server)，Workload (Consistent, Number of instances: 1)，高度な EC2 インスタンス (t3.xlarge)，Pricing strategy (On-Demand Utilization: 100 %Utilized/Month)，モニタリングを有効にする (disabled)，EBS ストレージ量 (200 GB)，DT Inbound: Not selected (0 TB per month)，DT Outbound: Not selected (0 TB per month)，DT Intra-Region: (0 TB per month)

リージョン	説明	サービス	設定の概要
アジアパシフィック（東京）	Firewall	AWS Web Application Firewall (WAF)	ウェブ ACL ごとに追加するルールの数（5 /月），使用されたウェブアクセスコントロールリスト（ウェブ ACL）の数（3 /月），ウェブ ACL ごとのルールグループの数（1 /月），各ルールグループ内のルールの数（10 /月），ウェブ ACL ごとのマネージドルールグループの数（10 /月）
アジアパシフィック（東京）	AP サーバーの Application Load Balancer	Application Load Balancer	Application Load Balancer の数（1）
アジアパシフィック（東京）	データ移行ツール	AWS DataSync	AWS DataSync がコピーしたデータの合計量（月あたり）（17 TB）
アジアパシフィック（東京）	EBS RDS FSx Backup	FSX Backup	バックアップされるプライマリデータの量（17 TB），プライマリデータの推定される毎年の増加率（%）（0.02），プライマリデータの推定される日単位の変化率（%）（0.002），日単位のバックアップウォームリテンション期間（30 日数）
アジアパシフィック（東京）	EBS RDS FSx Backup	RDS Backup	バックアップされるプライマリデータの量（100 GB），プライマリデータの推定される毎年の増加率（%）（0.02），プライマリデータの推定される日単位の変化率（%）（0.002），継続的なバックアップウォームリテンション期間（7 日数），日単位のバックアップウォームリテンション期間（30 日数）
アジアパシフィック（東京）	EBS RDS FSx Backup	EBS Backup	バックアップされるプライマリデータの量（2000 GB），プライマリデータの推定される毎年の増加率（%）（0.02），プライマリデータの推定される日単位の変化率（%）（0.002），日単位のバックアップウォームリテンション期間（7 日数），月単位のバックアップコールドリテンション期間（6 月）

3.1.3 サービス解説

サービス名	解説
Amazon EC2	Amazon EC2（Elastic Compute Cloud）は、Amazon Web Services（AWS）が提供するスケーラブルな仮想サーバー（インスタンス）を利用できるサービス。ユーザーはこのサービスを使って、インターネット上でサーバーを立ち上げ、アプリケーションのホスティングや処理、開発、テストなどを行うことができる。EC2 は非常に柔軟性が高く、オンデマンドでリソースを利用できるため、負荷の変動に応じてサーバーをスケールアップやスケールダウンすることが可能。
Amazon FSx for Windows File Server	Amazon FSx for Windows File Server は、Amazon Web Services（AWS）が提供する、完全マネージド型の Windows 向けファイルストレージサービス。Windows Server で動作するファイルシステムをクラウド上で提供し、Windows ベースのアプリケーションやサービスに必要なファイル共有機能を簡単に実現できる。
Amazon RDS for SQL server	Amazon RDS for SQL Server（リレーショナル・データベース・サービス・フォー・エスキュー・エル・サーバー）は、Amazon Web Services（AWS）が提供するマネージド型のリレーショナルデータベースサービスで、Microsoft SQL Server をクラウド環境で使用できるようにしたもの。これにより、ユーザーは SQL Server のデータベースをオンプレミスで運用する場合のように、インフラのセットアップや管理を行うことなく、スケーラブルで高可用性のデータベースを簡単に運用できる。
Network Address Translation（NAT）Gateway	Network Address Translation（NAT）Gateway は、AWS（Amazon Web Services）が提供する、プライベートサブネット内にあるインスタンスがインターネットと通信できるようにするためのマネージドサービス。NAT Gateway は、プライベート IP アドレスを持つインスタンスが、インターネット上のリソースにアクセスするために、パブリック IP アドレスを一時的に利用する仕組み。
AWS PrivateLink	AWS PrivateLink は、AWS が提供するサービスで、ユーザーが AWS サービスや VPC（Virtual Private Cloud）内のリソースに対して、プライベートな接続を提供するもの。これにより、インターネットを経由せずに、安全で低遅延の通信を可能にする。特に、セキュリティやデータ保護が重要なケースで非常に役立つ。

サービス名	解説
AWS Config	AWS Config は、AWS のリソース設定を記録し、監査やコンプライアンスのチェックを行うためのマネージドサービス。AWS Config を使うことで、AWS 環境内で設定されたリソースの構成を把握し、その変更を追跡・管理できる。
AWS CloudTrail	AWS CloudTrail は、AWS アカウント内でのユーザーおよびサービスのアクティビティを記録し、監査、セキュリティの分析、およびトラブルシューティングに役立つログを提供するマネージドサービス。CloudTrail は AWS リソースに対するすべての API 呼び出し（AWS Management Console、AWS CLI、AWS SDK、その他の AWS サービスからの呼び出しを含む）をキャプチャする。
Amazon GuardDuty	Amazon GuardDuty は、AWS 環境の脅威検出サービスであり、継続的にセキュリティ監視を行い、潜在的な不正アクティビティや異常な振る舞いを検出する。GuardDuty は、機械学習、異常検知技術、AWS の脅威インテリジェンスフィードを活用して、脅威を識別し、アラートを生成する。
AWS Security Hub	AWS Security Hub は、AWS アカウント全体でのセキュリティ状況を統合的に可視化し、管理するためのセキュリティサービス。Security Hub は、複数の AWS セキュリティサービス（Amazon GuardDuty、Amazon Inspector、AWS Config など）や、サードパーティ製セキュリティツールからのセキュリティ検出結果を集約・統合し、統一されたダッシュボードでセキュリティリスクを一元管理することができる。
AWS Direct Connect	AWS Direct Connect は、オンプレミスのデータセンター、オフィス、またはコロケーション環境と AWS クラウドを直接接続する専用ネットワークサービス。これにより、インターネットを介さずに AWS にアクセスでき、帯域幅の高い、安定した低レイテンシのネットワーク接続が提供される。
Amazon CloudWatch	Amazon CloudWatch は、AWS のモニタリングおよび管理サービスで、AWS リソースやアプリケーションの運用データを収集、分析、可視化するために使用される。これにより、システムのパフォーマンスを最適化し、運用上の問題を迅速に検出して対応することができる。
AWS Directory Service	AWS Directory Service は、クラウドベースでディレクトリに関するサービスを提供し、Microsoft Active Directory (AD) やその他のディレクトリ依存アプリケーションを AWS 上で管理するためのサービス。これにより、企業はディレクトリ管理や認証を容易に行うことができ、AWS 環境とオンプレミス環境との統合も可能になる。

サービス名	解説
Amazon Inspector	Amazon Inspector は、AWS 上のアプリケーションを自動的に評価し、セキュリティの脆弱性やベストプラクティスへの準拠状況を検査するサービス。これにより、セキュリティリスクを早期に特定し、修正するための推奨事項を提供する。
AWS Web Application Firewall (WAF)	AWS Web Application Firewall (WAF) は、ウェブアプリケーションを保護するためのセキュリティサービスで、一般的なウェブ攻撃や悪意のあるトラフィックからアプリケーションを防御する。AWS WAF は、アプリケーションの可用性を確保しながら、セキュリティとパフォーマンスを向上させることができる。
Application Load Balancer	Application Load Balancer (ALB) は、AWS の Elastic Load Balancing サービスの一部であり、アプリケーションレベル (OSI モデルのレイヤー7) でトラフィックを分散するためのロードバランサー。ALB は、複雑なトラフィックのルーティングや、HTTP/HTTPS リクエストに基づいた高度なルール設定が可能で、ウェブアプリケーションに特化したトラフィック管理機能を提供する。
AWS DataSync	AWS DataSync は、データの転送を簡素化し、迅速に行うためのマネージドサービス。オンプレミスのストレージシステムと Amazon S3、Amazon EFS、Amazon FSx などの AWS ストレージサービス間でのデータ転送を効率化することができる。DataSync は、データ移行、バックアップ、データの複製など、さまざまなユースケースに対応している。
FSX Backup	Amazon FSx Backup は、AWS の Amazon FSx サービスに関連するバックアップ機能で、Amazon FSx for Windows File Server および Amazon FSx for Lustre に対して、データのバックアップとリストアを行うためのマネージドサービス。FSx Backup を使用することで、データの保護、災害復旧、データ保持のニーズに応じた柔軟なバックアップソリューションを実現できる。
RDS Backup	Amazon RDS Backup は、Amazon Relational Database Service (RDS) のデータベースインスタンスに対するバックアップ機能を提供する。RDS は、データベースの管理を簡素化するためのマネージドサービスで、バックアップやリカバリのオプションを組み込むことで、データの保護と可用性を向上させる。
EBS Backup	Amazon EBS Backup は、Amazon Elastic Block Store (EBS) ボリュームに対してバックアップ機能を提供するサービス。EBS は、Amazon EC2 インスタンスに接続して使用するブロックストレージであり、データの耐久性と可用性を確保するために行う機能。

3.2 省 OA 端末等

省 OA 端末等とは、以下の端末の総称である。

- 防衛省・市ヶ谷地区の行政事務用システムの利用端末「省 OA 端末」
- 地方防衛局の行政事務用システムの利用端末「局 OA 端末」
- 各部隊の行政事務用システムの利用端末「部隊 OA 端末」
- 各機関の行政事務省システムの利用端末「機関 OA 端末」

別紙１_用語の定義

項番	用語	意味
1	防衛施設建設情報管理システム	防衛施設の現状や維持管理・更新等に関する情報を防衛省内統一的に運用し、メンテナンスサイクルの構築や維持管理・更新等に係るトータルコストの縮減・予算の平準化を実現するため、これらの情報を防衛省全体で共有できる情報基盤として整備したシステムをいい、①防衛施設電子納品保管管理サブシステム、②防衛施設維持管理サブシステム、③設計積算等データベースサブシステム、④工事監督官資料作成サブシステムの４つのサブシステムからなる。以下「**ＤＦＩＳ**」という。
2	ＤＩＩ	防衛省・自衛隊のコンピューター・システム等を収容し、体系的に構築される超高速・大容量の共通ネットワークをいう。Defence Information Infrastructure（防衛情報通信基盤）の略字。
3	省 OA 端末、局 OA 端末、部隊端末、機関端末等	本システムの利用者用端末をいう。
4	ガバメントクラウド	「デジタル社会の実現に向けた重点計画」等の政府方針に基づき、デジタル庁が提供する複数のクラウドサービスの利用環境をいう。
5	ＡＷＳ	AWS（Amazon Web Services）は、Amazon Web Service, Inc.が提供するクラウドコンピューティングを活用したサービスをいう。
6	ＣＳＰ	クラウドサービスプロバイダの略称であり、クラウドサービスを提供する事業者をいう。
7	ＧＳＳ	ガバメントソリューションサービスの略称であり、デジタル庁が提供する、政府共通の標準的な業務実施環境をいう。
8	リスク管理枠組み	“Risk Management Framework”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。以下「**RMF**」という。
9	サプライチェーン・リスク	情報システム※に関する調達に際し、当該情報システム及びその構成品等のサプライチェーンにおいて、不正プログラムの埋込み、情報の窃取、不正機能の組込み等が行われるリスクをいう。 ※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）第２条第２号に規定する情報システムをいう。

本業務では、ガバメントクラウド上で稼働する本システムにおいて障害等を予防しサービスを安定的に継続させることを目的とし、サービスの安定的な継続を期待する。

1.5 業務・システムの概要

本システムに係る業務の概要は、**図１**による。電子納品保管管理業務は、防衛省建設工事の電子成果品を登録・検索・閲覧することをいう。設計積算業務は、各地方防衛局等で実施した防衛施設に関する設計・積算等情報を登録することをいう。防衛施設維持管理業務は、防衛施設の維持管理等に関する点検計画の作成、コスト管理等を行うことをいう。工事監督官資料作成業務は、防衛省建設工事の実施に必要な書類をシステム上で入力・帳票化することをいう。

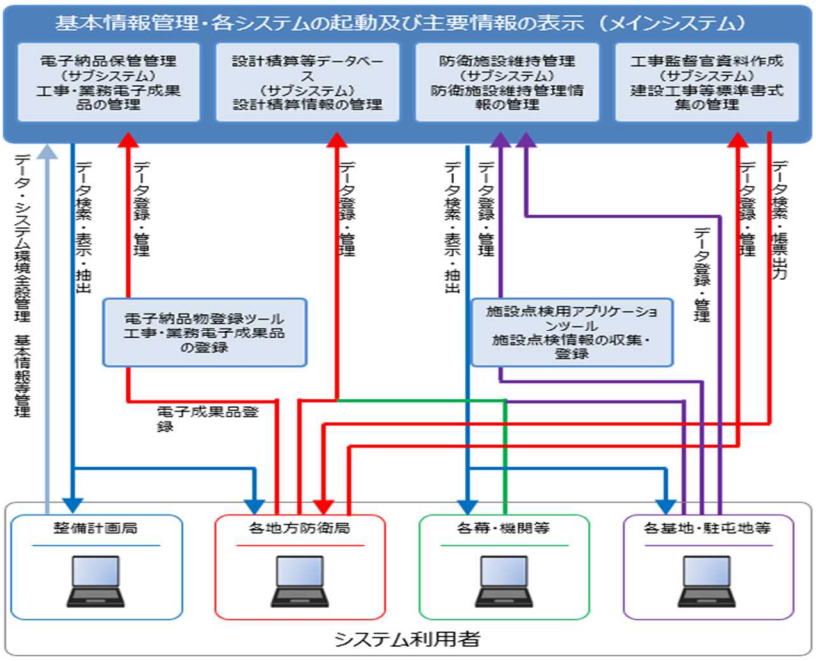


図１　業務及びシステムの概要

1.6 事業スケジュール

本業務及び関連事業に係る作業スケジュール（案）は、下図のとおりとする。

年度		6	7	8	9	１０	１１
次期システム ※ガバメントクラウド１段階目 ※令和１１年２月末まで	換装業務	⟷					
	運用支援保守業務		⟷	⟷	⟷	⟷	

図２　事業スケジュール（案）

1.7 調達案件及び関連調達案件の調達単位

本調達及び関連調達に係る調達単位は、下表のとおりとする。

表１　調達単位

No.	実施内容	実施期間	事業内容
1	換装業務	令和6年9月～令和7年2月28日	ガバメントクラウドへの本システムの換装
2	運用支援保守業務	令和7年3月～令和11年2月28日	本システムの運用及び保守支援に係る業務 ※本業務

2 本業務に関する要求

2.1 要求事項等

2.1.1 一般的要求事項

本システムの情報セキュリティ対策は「**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)**」及び「**情報システムにおけるリスク管理枠組み（ＲＭＦ）実施要領等について（通知）別添（注意**)」を基準とし、本システムのセキュリティ管理策を踏まえて、運用保守体制を整備すること。

2.1.2 システムの概要

防衛施設建設情報管理システムの概要は**図１**のとおりである。なお、本システムはDII部内オープン系ネットワーク及び政府共通ネットワーク(GSS)を経由しガバメントクラウドに接続し、ガバメントクラウドの情報基盤及び提供サービスを利用する。また、本システムの利用端末には、既存の省OA端末等を利用する。システム構成環境については、別紙２を参照のこと。

2.1.3 契約条件

契約期間は、契約締結日から令和11年2月28日までとする。なお、本システムの本稼働開始は令和7年3月1日を予定している。

2.2 作業の内容

契約相手方に求める業務を以下に示す。なお、各種業務における満たすべき内容については**別紙３**に示す業務品質レベルを確保すること。

2.2.1 共通事項

（1）業務実施計画の作成

契約相手方は、本業務を実施するに当たり、本契約締結後速やかに以下の内容を含む業務実施計画書を作成し、官の確認を受けること。また、業務遂行に関して課題が発生した場合は、速やかに官に報告し、対応方針について協議すること。

（ア）業務概要（目的・目標、範囲）
（イ）実施体制
（ウ）関連事業契約相手方からの引継計画
（エ）業務提供開始までの準備計画
（オ）コミュニケーション管理（会議体、報告書管理等）
（カ）全体スケジュール
（キ）品質管理
（ク）課題管理
（ケ）システム構成管理・変更管理
（コ）情報セキュリティ対策（運用保守における情報セキュリティインシデント対策等）

（２）運用保守計画の作成

契約相手方は、本業務を実施するに当たり、本書に定める運用保守業務に係る計画書を作成し、官の確認を受けること。

（３）運用保守要領の作成

契約相手方は、本業務を実施するに当たり、運用保守のセキュリティ対策に係る運用保守要領を作成し、官の承認を受けること。

（４）報告

運用保守状況を報告すること。（報告内容・方法、頻度等は運用保守計画書に記載するものとし、ガバメントクラウドのダッシュボードにて報告可能なものは利用を前提とする。）

（ア）稼働監視報告書（月次）
（イ）ヘルプデスク業務報告書（日次）
（ウ）業務報告書（システム技術支援、ヘルプデスク、情報提供、稼働監視業務）（月次）

（５）省既存環境側との連携

本システムは省既存環境・サービス及びガバメントクラウド環境・サービスを利用するため、本業務にあたってはそれらの運用保守相手方と連携・協力すること。

（ア）省既存環境・サービス

ＤＩＩ

（イ）ガバメントクラウド環境・サービス

AWS 各種サービス、GSS G-Net

（６）実施体制等

本業務を実施するために必要な人員について体制を整備すること。業務繁忙期（主に毎年３～４月）における業務量増加にも支障なく対応できるよう留意すること。

2.2.2 システム監視業務

本システムが問題なく利用できるよう、システム障害・異常等の監視を行うこと。

（１）死活監視

本システムの異常通知がないかを監視すること。

（２）閾値監視

サーバの CPU、メモリ、ディスク等の閾値を超える利用が無いかを監視すること。

（３）サービス、プロセス監視

サービス、プロセスに異常が無い事を監視すること。

（４）バックアップ監視

バックアップ処理にて異常が無い事を監視すること。

（５）ウイルス対策監視

（ア）ウイルススキャンに異常通知が無いかを監視すること。

（イ）併せて、ウイルスパターンファイルの更新確認すること。

（６）ログ監視

（ア）サーバのイベントログに異常が無いことを監視すること。

（イ）イベントログを保存すること。

2.2.3 ヘルプデスク業務

本システムの利用に関連し、官・民からの各種問い合わせに対応すること。

（１）電話、電子メールによる質問受付・回答

（２）官の利用者に対するクライアントパソコン設定等の支援

（３）利用者に対するシステム基本操作支援

（４）ヘルプデスク受付回答状況の報告

2.2.4 運用支援業務

本システムを運用する上での各種支援業務作業等を実施すること。

（１）業務運用支援作業

（ア）データ登録支援

データの新規登録作業は原則職員が実施。職員から支援依頼があった場合に対応すること。

（イ）データ削除支援

文書保存期限を過ぎたデータについて官側担当者に確認した上でデータ削除を支援すること。

（ウ）登録データ更新支援

① 以下のデータの更新作業を支援すること。

防衛施設建設情報管理システムにおける所属局、所属機関、所属基地、駐屯地等、名称、住所、所在地（緯度・経度）、電話番号、施設 ID、既存の施設区分（庁舎、隊舎）、既存の施設面積、新規及び既存又、非正規に登録された電子納品データ

② 工事・業務名称完成年月日等の基本情報の入力を行うこと。

（2）システム保全作業

（ア）アプリケーションプログラムのパッチ等適用作業

アプリケーション及びソフトウェアの修正モジュール、セキュリティパッチ等の適用作業を行うこと。実施にあたっては契約相手方が用意する環境にて検証を行い、官の承認後に本番環境へ適用を行うこと。

（イ）構成情報管理

アプリケーションプログラム、ソフトウェア、ガバメントクラウドのプラットフォーム環境（AWS サービス）、ネットワーク構成（GSS G-Net 含む）等の構成管理を実施すること。

（ウ）情報提供

本システムの構成品や運用に関するセキュリティ脆弱性に係る情報について、情報提供すること。

（エ）ソフトウェア等の運用保守業務

別契約「防衛施設建設情報管理システム換装業務」で調達するソフトウェアに対して保守を実施すること。

（3）その他作業

（ア）データ抽出作業等

官が指定する各種条件でのデータ抽出、本システムの運用上不要となったデータの削除等を実施すること。

（イ）システム改修を伴わない設定変更作業

本システムに対する設定変更等の軽微な作業を実施すること。

（ウ）FAQ の作成

本システムの利用における頻出問い合わせ等を FAQ として整理すること。

（エ）防衛施設建設情報管理システムの最適化検討に関する技術支援

本システムに係る関係者（DII、内部部局等、ガバメントクラウド関係機関等）との調整及び検討に対し、情報提供等の支援を実施すること。

2.2.5 障害対応・保守手配業務

本システム及び本システムの運用における障害を検知した場合、必要な対応作業・保守手配等を実施すること。

（1）アプリケーションプログラムに関する障害対応

システム内のアプリケーション等に対し、不具合を検知・受付した際、対応を実施すること。

（2）ソフトウェア製品及びハードウェアに関する障害対応

別契約「防衛施設建設情報管理システム換装業務」で調達するソフトウェア製品及びプラットフォーム環境に対し、不具合を検知・受付した際、対応を実施すること。

（3）移動端末に関する障害対応

（ア）本システムにて利用する移動端末（**別紙４**参照）に対し、不具合を検知・受付した際、官が指定する作業場所（市ヶ谷敷地内に限る）にて対応を実施すること。

（イ）障害の原因がソフトウェア（官側のソフトウェアを除く）やハードウェアの設定にある場合、ソフトウェアの再インストール、再設定を行い速やかに障害から回復させること。

（ウ）記憶装置を有する機器を廃棄、返却又は修理などのために官側の施設から持ち出す場合、データ消去（※）を実施すること。

※記憶装置の記憶域全体をソフトウェアなどによって重ね書き（無意味な文字・数字。記号を含む）を2回以上実施すること、もしくは官側の立ち合いで消磁又は破壊すること。

（エ）本システムを利用可能とするための作業（※）を実施すること。必要な情報は官側から提供するものとする。

※ハードウェア、OS及び施設点検用タブレットアプリケーションツールの再インストール、再設定

（4）省既存環境に関する障害対応

省既存環境及びガバメントクラウド環境との連携が必要な場合、協力して対応にあたること。

（5）パッチ提供

本システムを構成するソフトウェアにおいて、ソフトウェアの脆弱性対応等のため修正プログラム（以下「パッチ」という）をソフトウェアの製造元が発表した場合、契約相手方は速やかに当該製造元からパッチを入手し、官側に提供すること。

（6）その他作業

他省庁の動向調査を行い、必要に応じて本システム関連文書の改訂支援を行うこと。

2.2.6 情報提供業務

（１）防衛施設建設情報管理システムホームページの運用

（ア）契約相手方は別契約「防衛施設建設情報管理システム換装業務」にて防衛省職員向けに作成したウェブサイトを利用して FAQ、運営スケジュール、稼働状況及び緊急連絡先等を公開すること。

（イ）ホームページの内容を随時更新し、最新の状態を維持すること。緊急の連絡事項がある場合、官側に報告するとともにホームページに当該情報を掲載すること。

（ウ）ホームページのアドレス変更等が発生する場合、新しいホームページアドレスを案内する等、利用者が継続利用するための支援を実施すること。

2.2.7 次期システムへの更改支援業務

契約相手方は、本契約の履行期間の満了、全部若しくは一部の解除、又はその他の契約の終了事由の如何を問わず、本契約が終了となる場合には、契約相手方は官の指示のもと、本契約終了日までに官が継続して業務を遂行できるような必要な措置を講じ、他のシステム等に移行する作業の支援を行うこと。

（１）データ移行支援

業務引継に伴いデータ移行が発生する場合、移行に必要なデータを汎用的なデータ形式（CSV 等）に加工し、無償で提供すること。またファイル・データレイアウト等の資料を提供し、誠意をもって協力すること。なお、国際基準等に則る標準的なレイアウトに対応する業務については、標準的なレイアウトでのデータ提供を行うこと。

（２）システム終了対応支援

本契約終了時、本システムの停止、撤去、廃棄に係る作業を行うこと。

2.2.8 その他業務

契約相手方は、官からの要望に基づき、必要に応じて以下の支援を実施すること。

（１）RMF に係る支援業務

官からの要望に基づき、必要に応じて RMF に係る支援を実施すること。

（２）カバメントクラウドに関する調整に係る支援業務

官からの要望に基づき、必要に応じてガバメントクラウドの利用に係る各種支援作業を実施すること。

１）リソース増減の申請

２）設定作業等の申請等

3 作業実施体制

契約相手方は、「2.2　作業の内容」の契約相手方に求める業務を実施するために必要な人員を確保し、次により、必要な作業実施体制を確立、維持し、適切な場所等において作業を実施すること。

3.1　役務員の選任・管理等

（１）統括役務員の選任

契約相手方は、役務期間を通じて次に掲げる作業体制の統括に従事させる統括役務員１名以上を選任するものとする。

なお、契約期間満了前に、やむを得ない事情で変更する場合も同様とする。

ア　本業務の業務全般の統括

イ　「5.1　提出書類等」に掲げる報告書等に関する官への報告

ウ　役務員に対する監督及び指導

エ　本業務に関する官との連絡及び調整

オ　本業務に関する官からの要望への対応

カ　インシデントの進捗管理

キ　その他官の指示に基づく作業

（２）役務従事者名簿の提出

契約相手方は、本業務に従事する役務員について、役務従事者名簿を作成し、官の確認を受けるものとする。役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。また、ガバメントクラウド環境にアクセスする役務員は明示し、官の承認を得ること。

（３）役務員の交代

ア　官は、本業務を実施する上で、役務員の技術レベル、資質及び態度等が本業務を遂行するうえで不適正と認められる場合、当該不適正事項を契約相手方に提示した上で、役務員の交代を要求することができる。

イ　契約相手方は、上項（ア）の官の要求に対し、役務員の交代等により速やかに対応すること。

ウ　契約相手方は、役務員が事故、病気、公共交通の遅延等により勤務できない状況である場合は、当該役務員と同等の技術レベルを有した役務員に交代することにより速やかに対応すること。ただし、ガバメントクラウド環境にアクセスする役務員の交代は官の承認を得ること。

（４）役務員の管理

統括役務員は、一般役務員の技術レベルを管理し、役務員の技術レベルを維持又は向上すること。

（５）役務員の変更の届出

契約相手方は、役務員に異動、退職、長期休暇等が生じ、役務員の追加、変更等が必要となった場合は、十分な時間的余裕をもって官に報告し、承認を得るものとする。

3.2 作業役務員に求める資格等の要件

各役務員は、本業務を実施するに当たっては、次の事項を満たすものとする。

（１）各役務員共通の要件

日本国籍を有していること。

（２）統括役務員は類似のシステム運用保守業務において、要員管理を遂行するとともに、チームをリードして目的を遂行できる立場での勤務経験を 5 年以上有していること。また、役務従事者は、類似のシステム運用保守業務にシステムエンジニアとして従事した経験を 3 年以上有していること。

（３）役務従事者は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。

3.3 作業場所等

作業場所については、防衛省市ヶ谷地区及び官が指定する場所とする。指定場所においては官の立入検査を受けること。

作業実施場所は、原則として、平日 8 時 30 分から 18 時 15 分までの利用とする。ただし、業務繁忙期等を考慮し、利用時間の延長等が必要な場合は、官との協議とする。

また、本業務実施にあたり、各局・各基地での作業が発生する場合も、官との協議とする。

なお、各役務員の作業実施場所における作業については、以下のとおりとする。

（１）本業務に係るデータや情報は作業場所内でのみ利用が許される。契約相手方は入退室管理等の厳格な情報保護に努めること。

（２）本作業を行う作業用端末は本業務専用のものとし、契約相手方が用意すること。作業用端末においては USB メモリや CD-R 等の記録媒体・可搬媒体等の利用を厳格に管理すること。なお、本業務終了時には、本業務専用端末上のデータを消去し、消去証明書を官に提出すること。

（３）作業場所への契約相手方の自社支給端末の持ち込み・利用については、事前に官の承認を得ること。ただし、自社支給端末で本業務に係るデータや情報を扱うことは禁止とする。

（４）問い合わせに必要な電話回線（1 回線以上）及び電子メールアドレス（1 つ以上）を契約相手方が用意すること。

4 情報の保全

4.1 個人情報及び保護情報

a) 契約相手方は、防衛省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、**情報システムの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)項からc)項のほか、官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防衛省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防衛省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ならない。

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防衛省に報告すること。

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、防衛省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、契約相手方は防衛省の求めに応じ、協議を行い、必要な対策を講じること。

4.2 秘密保全

a) 官房長等又はその指定した者が定める立入禁止の掲示がある場所及び部隊等の長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、官房長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、防衛省から貸付けを受けた文書及び電子データについては、当該業務終了時に防衛省へ返却すること。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防衛省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、防衛省と協議の上、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防衛省が認めた場合は、防衛省の求めに応じ協議を行い、防衛省と合意の上で、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、遅滞なく防衛省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) 防衛省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) 防衛省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

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、「**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、適切に管理する。保護すべき情報は、**表２**のとおりとする。

表２　保護すべき情報

保護すべき情報	保護すべき情報の例
ネットワーク・システム情報	IP アドレス、設計書類、システム構成図及びネットワーク構成図並びにユーザ情報（ID・パスワード、アカウント情報及び職員属性情報）
各種ファイルデータ	グループウェアデータ、ファイルサーバデータ、イントラ Web コンテンツ、各端末類のローカルデータ及びセキュリティバックアップログ
セキュリティ仕様	ファイアーウォール設定値、セキュリティパッチ適用状況及び管理者パスワード

5　その他

5.1　提出書類等

本契約で作成する提出物について、官の承認を得た上で、提出期限までに提出すること。提出物については、以下の「提出物一覧」に示す提出物及び提出期限を基本とするが、より良い提案がある場合は、業務実施計画書に具体的に定め、官の承認を得ること。

（1）提出書類

本契約相手方は、**表３**に示す提出書類について指定された提出時期に指定された数量を官側に提出しなければならない。

表３　提出書類

番号	書類名	提出時期	数量 単位	媒体	提出先
1	業務実施計画書	契約後速やかに	1式	紙	整備計画局 建設制度官
			1式	電子	
2	運用保守計画書	契約後速やかに	1式	紙	
			1式	電子	
3	運用保守要領	契約後速やかに	1式	紙	
			1式	電子	
4	役務従事者名簿	契約後速やかに	1式	紙	
			1式	電子	
5	業務引継書	納期まで	1式	紙	
			1式	電子	

（2）納入品

契約相手方は、**表４**に示す納入品について、契約の完了時に検査を受けなければならない。

表４　納入品

番号	書類名	提出時期	数量 単位	媒体	納入場所
1	稼働監視報告書	令和７年３月１日以降毎月初旬	１式	電子	整備計画局建設制度官
2	ヘルプデスク業務日次報告書	令和７年３月１日以降業務終了後毎日	１式	電子	
3	業務報告書（システム技術支援、ヘルプデスク、情報提供、稼働監視業務）	毎年度末	１式	紙	
			１式	電子	

※１･･･紙媒体で納入する計画書等は、Ａ４版縦、横書きとする。

※２･･･電子媒体は、書き換え不可のＣＤ－Ｒ又はＤＶＤ－Ｒを使用するものとする。

（3）貸付品

表５に示すほか、官側が必要と認めた資料を官側と調整の上、契約担当官等に申請し、無償で貸付を受けることができる。

表５　貸付品

番号	書類名	数量 単位	秘密区分	貸付 期間	貸付・返却場所
1	防衛施設建設情報管理システム換装業務　業務成果品	１式	注意	契約相手方の申請後速やかに ～ 納期まで	整備計画局建設制度官
2	情報システムにおけるリスク管理枠組み（ＲＭＦ）実施要領等について（通知）添付書類２～４	１式	注意		

5.2　知的財産権の帰属

著作権等の知的財産の取扱いは，次による。

a) 契約の相手方は，契約書又は仕様書等の定めるところにより官側に提出された著作物についての著作者人格権（**著作権法**第１８条から第２０条までの権利をいう。）を行使しないものとする。また，本契約の一部又は全部を再委託した第三者についても同様とする。ただし，契約の相手方の固有の技術資料（契約の相手方が第三者から提供を受けたものを含む。以下同じ。）についてはその限りではない。

b) 契約の相手方は，契約書又は仕様書等の定めるところにより官側に提出された著作物について，全ての著作権（**著作権法**第２７条及び２８条の権利を含む。）を官側に譲渡しなければならない。ただし，契約の相手方の固有の技術資料については，その限りではない。

c) 契約の相手方は，官側の使用に供する目的で，b)項により官側が譲渡を受けた著作物を複製し，翻訳し又は翻案することができる。官側は，契約の相手方からb)項により官側が譲渡を受けた著作物の利用の許諾を求められた場合には，特に支障がない限りこれを許諾するものとし，必要な事項は協議して定めるものとする。

d) 官側は，本契約の履行中及び終了後５年間は，契約書又は仕様書等の定めるところにより官側に提出された契約の相手方の固有の技術資料について，本契約に関して防衛省（防衛装備庁を含む。以下同じ。）が行う監督，検査，調査，試験若しくはその結果の評価その他これに類する業務のため必要がある場合は，その内容を防衛省の内部において利用し及び複製（当該技術資料のうち契約の相手方の指定するものの複製を除く。）することができる。

e) 契約の相手方は，本契約の履行に当たり，第三者の有する知的財産権（**知的財産基本法**第２条第２項に規定する知的財産権をいう。以下同じ。）又は技術上の知識に関し第三者が契約の相手方に対して有する契約上の権利を侵害することのないよう必要な措置を講ずるものとする。契約の相手方が，前文の必要な措置を講じなかったことにより官側が損害を受けた場合は，官側は契約の相手方に対してその賠償を請求することができる。

5.3　再委託

再委託は，次による。

a) 契約の相手方は，本契約の履行に当たり，その全部を一括して再委託してはならない。

b) 契約の相手方は，本契約の履行に当たり，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，契約担当官等の承認を受けなければならない。

c) 契約の相手方は，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，契約担当官等の承認を受けなければならない。

d) 契約の相手方は，上項b)又はc)により再委託を行う場合には，契約の相手方が防衛省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“**４　情報の保全**”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) 上項b)又はc)に基づき再委託先の事業者に業務を実施させる場合は，全て契約の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，契約の相手方の責に帰すべき事由とみなして契約の相手方が責任を負うものとする。

f) 契約の相手方は，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。

5.4 官側の支援

本件の履行に当たって、次の事項について官側の支援を必要とする場合には官側と調整し、無償で官側の支援を受けることができる。

（1）官側の保有する資料などの閲覧に関する事項

（2）官側の保有する施設（電力、用水などを含む。）、設備、機器の使用及び操作に関する事項

（3）その他、契約相手方が契約履行上必要とし、官側と協議の上、官側が必要と認めた事項

5.5 仕様書の疑義

契約相手方は、本仕様書に疑義が生じた場合には、速やかに官側と協議するものとする。

6 附属書

次に示す付図及び別紙は，この仕様書の一部をなすものとする。

別紙１　用語の定義

別紙２　システム構成環境等

別紙３　サービスレベル要求書

別紙４　移動端末関連要件

情報セキュリティ指定書	発簡番号	
	調達要求番号	－
	調達要求年月日	令和７年１月　日
	作成部課	整備計画局建設制度官
	作成年月	令和７年１月１４日
品　　名	防衛施設建設情報管理システム運用支援保守業務	
仕様書番号	―	

１　保護すべき情報の管理

契約相手方は、この契約の履行に当たり知り得た保護すべき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（防装庁（事）第１３７号。令和４年３月３１日）別添の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の規定に基づき、適切に管理するものとする

２　保護すべき情報として指定された情報

表１

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	備考
1	ネットワーク・システム情報	IP アドレス、設計書類、システム構成図及びネットワーク構成図並びにユーザ情報（ID・パスワード、アカウント情報及び職員属性情報）	運用保守用端末での取り扱いは除く	
2	各種ファイルデータ	グループウェアデータ、ファイルサーバデータ、イントラ Web コンテンツ、各端末類のローカルデータ及びセキュリティバックアップログ	運用保守用端末での取り扱いは除く	
3	セキュリティ仕様	ファイアーウォール設定値、セキュリティパッチ適用状況及び管理者パスワード	運用保守用端末での取り扱いは除く	