調達要求番号：

防衛装備庁仕様書

品件名	次期防衛セキュリティゲートウェイのサービス提供に関する役務（案）	仕様書番号	
		作成年月日	
		改正年月日	
		作成部課等	防衛装備庁長官官房総務官付

1. 総則

1.1 適用範囲

この仕様書は，次期防衛セキュリティゲートウェイ（以下「ＤＳＧ」という。）のサービス提供に関する役務について規定する。

1.2 用語の定義

この仕様書で用いる用語の定義は，**ＪＩＳ　Ｘ　０００１～００３２**によるほか，**表１**のとおりとする。

表１　用語の定義

用語	定義
ＤＳＧ	Ｄｅｆｅｎｓｅ　Ｓｅｃｕｒｉｔｙ　Ｇａｔｅｗａｙ（防衛セキュリティゲートウェイ）の略称。官と民との間で情報共有を可能とする環境を提供する基盤。
ＥＰＰ	Ｅｎｄｐｏｉｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　Ｐｌａｔｆｏｒｍ（エンドポイント保護プラットフォーム）の略称。クライアント端末やサーバ等を，マルウェア感染から保護するソフトウェア。
ＥＤＲ	Ｅｎｄｐｏｉｎｔ　Ｄｅｔｅｃｔｉｏｎ　ａｎｄ　Ｒｅｓｐｏｎｓｅ（エンドポイント検知及び保護）の略称。クライアント端末やサーバ等を常時監視し，不審な挙動を検知するソフトウェア。
ＮＩＳＴ	米国立標準技術研究所。アメリカ商務省に属し，科学技術分野における計測と標準に関する研究を行っており，各種ガイドライン等を発行している。

表 1　用語の定義（続き）

用語	定義
ＮＯＣ	Ｎｅｔｗｏｒｋ　Ｏｐｅｒａｔｉｏｎ　Ｃｅｎｔｅｒの略称。通信ネットワークの可用性と健全性の維持等を目的とした組織。
ＳＯＣ	Ｓｅｃｕｒｉｔｙ　Ｏｐｅｒａｔｉｏｎ　Ｃｅｎｔｅｒの略称。セキュリティインシデントの検出，分析，対応，報告及び防止を目的とした主にセキュリティアナリストから構成される組織。
省ＯＡ	市ヶ谷地区における行政事務の効率化に資するため，内部部局，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，防衛研究所及び防衛装備庁の９機関共同で使用する防衛省ＯＡシステム基盤。
サービス仕様書	ＤＳＧを構成する各サービスについて，提供範囲，ＳＬＡ，稼働率，可用性，復旧目標（ＲＴＯ・ＲＰＯ），セキュリティ要件等，サービスが満たすべき水準及び条件を定義した文書をいう。
サービスカタログ	ＤＳＧが利用者に提供する各サービスの名称，目的，対象利用者及び提供内容を，利用者の視点から一覧化し，分かりやすく示した文書をいう。
緊急時対応計画	緊急時対応計画とは，サービス中断時にサービス，運用及びデータを復旧するための計画であり，代替環境の利用や手作業による業務継続手段を定めるもの。

1.3　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，入札書または見積書の提出時における最新版とする。

なお，引用文書等の定める事項が，この仕様書の内容と異なる場合は，法令等を除き，この仕様書に定める内容が優先する。

1.3.1　引用文書

a)　規格

1)　ＪＩＳ Ｘ ０００１～００３２ 情報処理用語

2)　ＮＩＳＴ　ＳＰ８００－１７１　Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

b)　法令等

1)　著作権法（昭和４５年法律第４８号）

2)　個人情報の保護に関する法律（平成１５年法律第５７号）

3) **知的財産基本法**（平成１４年法律第１２２号）

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）**（防装庁第１３７号。令和５年６月３０日）

5) **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）

6) **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）

7) **政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ）管理基準**

8) **ＩＳＯ９００１　品質マネジメントシステム－要求事項**

9) **ＤＳＰ　Ｚ　９００８　品質管理等共通仕様書**

10) **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。令和６年３月２２日）

11) **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。令和６年３月２５日）

12) **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）

13) **防衛事業適合事業者制度等に関する訓令**（防衛装備庁訓令第１９号。令和７年６月３０日）

14) **防衛事業適合事業者制度等に関する訓令の実施要領について（通知）**（装装保１４８４６号）

15) **環境物品等の調達の推進に関する基本方針**（令和８年２月３日。変更閣議決定）

1.3.2　関連文書

a) **法令等**

1) **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）

2) **防衛省の情報保証に係る訓令**（平成１９年防衛省訓令第１６０号。令和７年３月２４日最終改正）

3) **防衛装備庁の情報保証に関する訓令の運用について（通達）**（装官総第１６５号。令和６年９月２５日）

4) **「防衛省デジタル・ガバメント中長期計画」の決定について（通知）**（防整情第４９８８号。令和４年１２月１２日）

5) **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）

b) **その他**

1) **デジタル社会の実現に向けた重点計画**（令和８年７月２１日。閣議決定）

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

3) **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８年６月１２日。デジタル庁）

4) **政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ）管理基準**（令和８年６月１２日。最終改定）

2. 調達の背景

防衛省は，令和５年度より，防衛省と関連する企業の間で，保護すべき情報（以下「保護情報」という。）を含む多くのデータを安全かつ効率的に共有する通信基盤として，防衛セキュリティゲートウェイ（以下，「ＤＳＧ」という。）のサービス提供を行っている。

ＤＳＧの整備の背景には，特に中小企業など個別の企業にとって，これらの情報を共有するためのセキュアなシステムを自ら整備するには，極めて専門的かつ高度な知識を要するうえ，費用面でも大きな負担となるという事情がある。また，令和５年度以降，防衛産業におけるサイバーセキュリティ体制の強化のため，**ＮＩＳＴ ＳＰ８００－１７１**を参考とした防衛産業サイバーセキュリティ基準への対応が求められている。

現行ＤＳＧの運用を通じ，加入企業及び利用者が増加しており，取り扱う情報やサービスの範囲も拡大していることから，利用者・運用者双方に対して，より一層の利便性の向上が求められている。

こうした状況を踏まえ，現行ＤＳＧサービスは，令和９年度内に次期サービスへの更新を行うことを予定している。更新に当たっては，現行における改善点への対応に加え，政府方針を踏まえたクラウドサービスの活用，官民の業務効率化及び柔軟な働き方への対応を目的として，本役務において次期サービスの提供を行うものである。

具体的には，次期ＤＳＧにおいてクラウドサービスを活用して機能の拡張及び利便性の向上を図りつつ，利用状況に応じて柔軟にリソースを確保できる運用により，リソース及び運用費用を最適化するとともに，各種申請手続の簡略化により官民双方の負担軽減を実現する。あわせて，保護情報を取り扱う「保護情報区画」に加え，これを補完する「業務情報区画」を併設し，暗号鍵を防衛省の管理下に置く鍵管理，ＮＯＣ／ＳＯＣによる監視，オンライン申請，通知機能等の新たなサービス・機能を導入する。これらのサービス・機能は，データ主権を確保する観点から，データの所在を国内リージョンに限定する。これにより，中小企業を含む防衛関連企業に対し，より容易かつ利便性の高い形で機密性・完全性・可用性を確保した情報共有環境を提供し，防衛産業全体のサイバーセキュリティ強化と防衛調達への参画推進を図るものである。

3. 目的等

3.1 整備の目的

次期サービスへの更新に当たり，本役務は，現行ＤＳＧの運用実績及び政府方針を踏まえ，中小企業を含む防衛関連企業に対して，より安全かつ効率的で，かつ利便性の高い情報共有環境を提供することを目的とし，具体的には，以下の内容を実現する。

a) 現行ＤＳＧの改善点への対応
b) クラウドサービスの活用による効率化
c) 利用者の申請負担軽減及び官民の業務効率化
d) 安全かつ効率的な情報共有の継続的提供
e) セキュリティ統制及び監査機能の強化

3.2 整備の効果

本役務の実施により，前項に掲げる目的に対応して，次の効果が得られる。

a) 現行ＤＳＧの改善点への対応により，加入・利用の増加に応じた利便性の高い利用環境が提供され，利用者・運用者双方の満足度及び生産性が向上する。

b) クラウドサービスの活用による効率化により，利用状況に応じて柔軟にリソースを確保できる運用により，リソース及び運用費用が最適化される。

c) 利用者の申請負担軽減及び職員の業務効率化により，主に利用者が用いるオンライン申請の自動化・可視化を通じて，利用者側の入力負担及び審査担当者の業務負荷低減が期待されるとともに，処理リードタイムの短縮が実現される。

d) 安全かつ効率的な情報共有の継続的提供により，保護情報区画を主たる区画とし，業務情報区画を併設する二区画構成とすることで，機密性区分に応じた適切な情報の取扱いが可能となり，防衛関連企業が利用しやすいセキュアな情報共有環境を提供することで，防衛産業サイバーセキュリティ基準等への対応を支援する。

e) 統制の強化により，暗号鍵の防衛省管理下での運用，ＮＯＣ／ＳＯＣによる監視及びログ・監査情報の提供を通じて，防衛省側による統制の強化が図られる。また，区画別の可用性設計により，災害又は障害の発生時にも業務の継続が可能となる。

4. 事業の内容

4.1 整備の概要

次期ＤＳＧでは，防衛省と防衛関連企業の間で安全なデータ共有が可能となるネットワーク機能及び関連サービスを，パブリッククラウドを前提とした利用状況に応じて柔軟にリソースを確保できる構成により提供する。これらの機能及びサービスは，保護情報区画を主たる区画とし，業務情報区画を併設する二区画構成として，外部からの不正アクセスや意図しない情報漏えいを未然に防止できるよう，ＮＩＳＴ基準に準拠したセキュリティ環境を条件とするとともに，ＮＯＣ／ＳＯＣによる２４時間３６５日の監視を行い，インシデント対応及び復旧サポートを行うものとする。

4.1.1 情報区画の構成

次期ＤＳＧは，保護情報区画を主たる区画とし，業務情報区画を併設する二区画構成とする。両区画の構成は次のとおりとする。

a) **保護情報区画**

保護すべき情報を取り扱う区画であり，パブリッククラウド上に，防衛領域として物理的又は論理的に分離した環境として構築する。接続は閉域網（広域イーサネット又はモバイル閉域網）によることとし，可用性は可用性ゾーン（ＡＺ）冗長及び複数リージョンにわたる冗長（マルチＡＺ及びマルチリージョン）により確保する。

b) **業務情報区画**

保護すべき情報未満の情報を取り扱う区画であり，パブリッククラウド上に構築する。企業側からの接続はインターネット経由とし，ブラウザベースのクライアントレスＶＰＮにより利用する。可用性は可用性ゾーン冗長（マルチＡＺ）を基本とする。

4.1.2　次期ＤＳＧに係る事業スケジュール

次期ＤＳＧに係る事業スケジュールは，**図１**のとおりとする。本役務による次期ＤＳＧサービスの提供に加え，次年度以降，次期ＤＳＧにおいて追加のサービスを提供する関連事業の実施を想定している。契約相手方は，これらの追加サービスの提供が円滑に行えるよう，必要な連携を図るものとする。

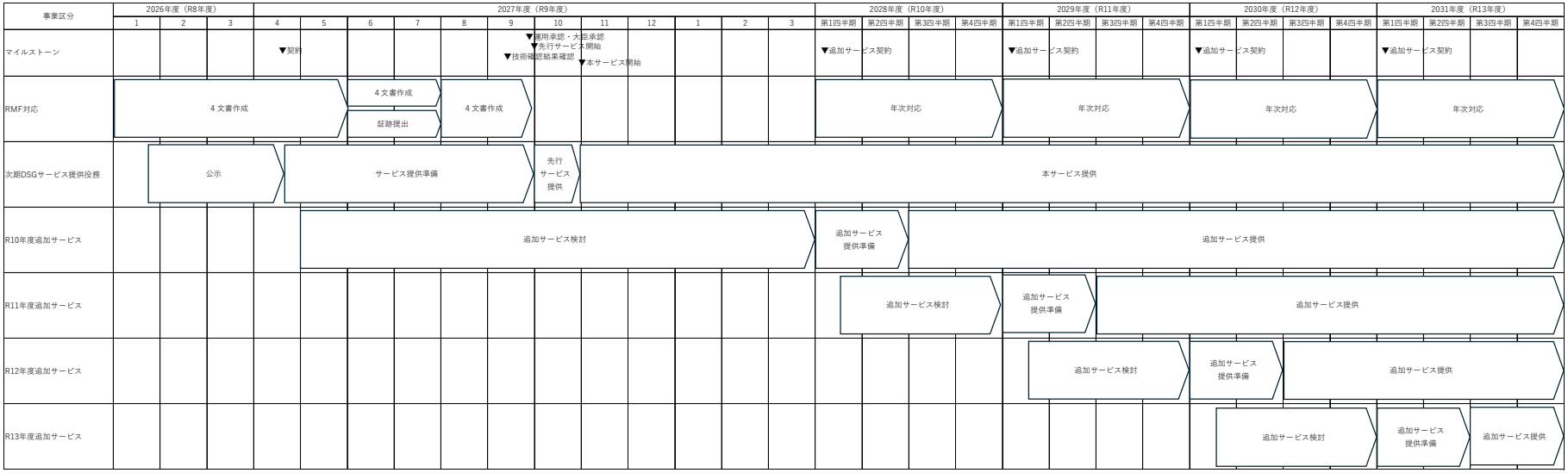

図１　事業スケジュール（予定）

4.2　サービス提供に係る基本要件

a)　サービス構成

次期ＤＳＧの構成は，パブリッククラウド上に構築する保護情報区画及び業務情報区画の二区画，ＮＯＣ／ＳＯＣによる監視機能，データの管理・保全を行うストレージ及びバックアップ機能，並びにこれらを接続する通信設備を用いてサービス提供する。保護情報区画は，防衛情報通信基盤（ＤＩＩ）及び閉域網（広域イーサネット又はモバイル閉域網）と接続し，業務情報区画は，インターネットを介したブラウザベースのクライアントレスＶＰＮにより接続することで，官と民との間で情報共有が可能な環境を提供する。

b)　環境の信頼性

上記の構成において，採用するパブリッククラウドサービスは，政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ）に登録されたものとし，データの所在は国内リージョンに限定する。ネットワークは，保護情報区画では閉域網を用い，適切な暗号化により安全性の高い通信を確保する。また，暗号鍵は防衛省の管理下に置くものとし，可用性ゾーン（ＡＺ）冗長及び複数リージョンにわたる冗長により，高い可用性を確保する。

c)　データセンターの設置環境

クラウドサービスのデータセンターは，活断層等の地理的リスクを考慮して設置されたものであること。情報資産の保管及び障害・災害発生時の退避先(バックアップ・災害復旧先)は，全て日本国内のリージョンとし，事業継続性を確保するため，地理的に十分離隔した異なるリージョン及び可能な限り異なる電力供給系統に立地すること。

d)　ＮＯＣ／ＳＯＣの設置環境

ＮＯＣ／ＳＯＣは，官との連携が可能な国内の拠点に設置すること。運用の継続性を確保するため，官が別途定める目標復旧時間（ＲＴＯ）を満たすよう，主たる拠点の障害時にも運用を継続できる冗長化した拠点を国内に確保すること。

e)　中立性

1)　導入するハードウェア，ソフトウェア等の構成要素は，標準化団体（ＩＥＥＥ，ＪＩＳＣ等）が規定または推奨する各種業界標準に準拠すること。

2)　次々期サービス移行の際に，移行の妨げや特定の装置や本サービスに依存することを防止する為，原則として本サービス内のデータ形式はＸＭＬ，ＣＳＶ等の標準的な形式で取り出すことができるものとすること。

3)　特定の事業者や製品に依存することなく，他者に引き継ぐことが可能なサービス構成であること。

4.3　提供するサービス

次期ＤＳＧでは，利用者に直接提供する利用者向けサービスと，これらを支えるサービスを提供する。利用者向けサービスでは，区画共通において，現行の各サービスの対象範囲を拡大するとともに，新たに通知・ポータルサービスを提供して利便性の向上を図る。保護情報区画においては，防衛省内システム等の構築及び運用に必要な環境を利用可能とするインフラ提供

サービスを新たに提供し，業務情報区画においては，官民双方の業務効率化を図るため新たにオンライン申請サービスを提供する。また，サービス提供管理，セキュリティサービス，アカウント管理サービス及び端末管理サービスにより，次期ＤＳＧ全体の統制及びセキュリティの担保を行う。なお，各サービスの詳細は「**5.3 提供サービス**」に示す。

4.4 防衛省と防衛関連企業の整備担当範囲

次期ＤＳＧの整備担当範囲は，防衛省（契約相手方を含む。）及び防衛関連企業の二者について，次のとおりとする。

a） 防衛省（契約相手方を含む）

ＤＳＧの情報管理・監視に係る要件の提示及び国有財産（施設・電力等）の提供を行うとともに，サービス提供事業者において，パブリッククラウド上の保護情報区画及び業務情報区画の基盤，ＤＳＧ側の通信基盤，並びに各サービスの構築・整備を担当する。

b） 防衛関連企業

防衛関連企業は，防衛産業サイバーセキュリティ基準に従い，ＤＳＧの利用に必要な企業側端末及び接続用スイッチ等の利用者用情報通信機材，並びに利用区画への立入制限・入退管理に係る設備を整備する。

4.5 防衛省と防衛関連企業の運用上の責任

次期ＤＳＧの運用上の責任は，防衛省（契約相手方を含む。）及び防衛関連企業の二者について，次のとおりとする。責任分担の詳細は**別紙１**「責任分担表」による。

a） 防衛省（契約相手方を含む）

運用方針の決定，情報セキュリティ事故発生時のリスク査定及び対応方針の承認，利用者のセキュリティ確認・承認並びに監査の実施を行う。また，サービス提供事業者において，ＤＳＧ全体の監視（ＮＯＣ／ＳＯＣ），インシデントの検知・初動対応・復旧，アカウント・鍵管理の運用，ログ・監査情報の提供並びにヘルプデスク運用を行う。

b） 防衛関連企業（加入企業）

防衛関連企業は，防衛産業サイバーセキュリティ基準に従い，ＤＳＧの利用区画への立入り状況の常時把握，入退室の状況管理及び確認並びに官への報告，企業側端末の適切な管理を行う。

5. 役務に関する要求

5.1 役務の実施体制

契約相手方は，本件の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。

また，契約相手方は，統括責任者，業務実施責任者及び各チームリーダを含む実施体制図を提出すること。統括責任者及び業務実施責任者は，プロジェクトマネージャ（ＰＭＰ等）又は情報処理安全確保支援士のいずれかの資格を有する者，若しくはこれらと同等以上の知識及び経験を有する者とする。

a） 業務従事者への要求

1) 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

「業務従事者」という。）を確認すること

2) 前記 1)の業務従事者が本契約を履行するために必要な経験，資格，業績等を有すること

3) 上記 1)の業務従事者が，前記 2)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

4) 前記 3)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

b) **提供実績に関する要求**

契約相手方は，**ＮＩＳＴ　ＳＰ８００－１７１**に規定するセキュリティ要件を満たす機能を有する製品又はサービスを提供した実績を有すること。実績を証する書面を求められた場合は，提出できること。

5.2 役務実施計画書の作成

契約相手方は，役務実施計画書を作成し，事前に調達要求元の確認を得て，提出するものとする。

5.3 提供サービス

ＤＳＧが提供するサービスは，**表２**のとおりとする。各サービスの提供内容の詳細は**別紙２**「技術要件詳細」に，予定数量は**別紙３**「予定数量」による。

表２　提供サービス

番号	サービス名	区画	内容
1	サービス提供管理	共通	サービス維持等
2	ファイル共有サービス	共通	保護すべき情報等のファイル共有
3	アカウント管理サービス	共通	アカウント管理，多要素認証等
4	セキュリティサービス	共通	ＮＯＣ／ＳＯＣ，ＥＰＰ／ＥＤＲ， マルウェア対策，ＦＷ／ＷＡＦ， 脅威検知，脆弱性管理等
5	ヘルプデスクサービス	共通	問い合わせ・申請・障害対応
6	加入支援サービス	共通	加入申請受付・対応，回線工事支援
7	ログ・監査情報提供 サービス	共通	情報セキュリティ基準対応等に必要なログ・監査情報の提供
8	インフラ提供サービス	保護情報	ＩａａＳ提供
9	コミュニケーション サービス	保護情報	チャット，Ｗｅｂ会議
１０	端末管理サービス	保護情報	ポリシー制御等
１１	オンライン申請サービス	業務情報	各種申請の自動化

5.4 付随作業

ＤＳＧのサービスを提供するに当たって，付随する関連作業を行うこと。

5.5 実績レポートの提出

a) 契約相手方は，リソース使用量の日次推移及びこれに基づく従量課金の実績を月次で提出すること。これにより，運用及び費用が実際の使用量に即していることを官が確認できるようにすること。なお，月末時点等の値のみをもって実績とせず，期間中の使用量の推移を実績の根拠とすること。

b) **別紙３**「予定数量」に示す予定数量は，調達仕様書作成時での想定量を示しており，確定した利用数量ではない。

5.6 サービス移行時の支援

契約相手方は，本役務の終了に伴う次々期サービスへの移行に際し，次の支援を行うこと。

a) 官の指示に基づき，移行の検討に係る事業者に対する支援（現行構成・データ・運用に関する情報提供等）を実施すること。

b) 官の指示に基づき，データ抽出の支援（対象データの特定，抽出方式の検討，抽出作業への協力等）を行うこと。

c) 官の指示に基づき，前記 a)及び上記 b)に付帯する作業を行うこと。

6. 運用期間

ＤＳＧの運用期間は，令和９年１１月１日から令和１４年３月３１日までを予定し，詳細は官と協議して確定する。現行ＤＳＧからの移行は，現行サービスに影響を与えないよう，区画又はサービス単位による段階的な移行とし，一定の並行運用期間を確保する。次期ＤＳＧの先行サービス開始は，切替えの１か月前を目途とする。

また，次期ＤＳＧの本サービス開始に当たっては，契約相手方は，先行サービスの開始前までに，**別紙２**「技術要件詳細」への適合を示す「技術要件確認結果報告書」を提出して官の合意を得るものとし，官の運用承認，並行運用による確認及び修正内容の合意を経た後，官の承認を得て本サービスの運用を開始すること。

7. サービス提供に関する要求事項

次期ＤＳＧのサービス提供に関する要求事項は，次の各号のよるものとする。

7.1 ＤＳＧの利用におけるセキュリティ対策

a) 契約相手方は，**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）**（以下「情報セキュリティ通達」という。）における添付書類「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おける特約条項」，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」及び付紙「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システムセキュリティ実施要領」に基づき，サービスを提供すること。

b) 防衛省で定めるＲＭＦについて，「**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）**」に基づき，以下の支援を行うこと。

1) 官と協議の上，ＲＭＦで導出されるセキュリティ管理策について，必要な措置を講ずること

2) 官と協議の上，ＲＭＦにおけるセキュリティ管理策の実装状況を示す設計書，試験結果，設定証跡，監査資料等の証跡を提出すること

c) 保護対象データについては，クラウドサービス事業者等が単独で復号できず，防衛省側が復号の可否を統制できる鍵管理を採用すること。暗号鍵の生成，保管，利用，更新，停止，失効及び利用履歴の管理は防衛省の管理下で行うこと。暗号方式は電子政府推奨

暗号リスト等に基づくものとする。

d) データの所在は国内リージョンに限定し，国外移転を行わないこと。クラウド利用時のデータ所在，管理主体及び監査条件について，防衛省側が必要な統制を確認できること。

e) 企業側保有端末の記憶媒体全体の暗号化（ＢｉｔＬｏｃｋｅｒ等）を前提とし，当該暗号化に用いる鍵は企業側の管理とすること。

f) ＮＯＣ／ＳＯＣによる監視，ＥＰＰ／ＥＤＲ，マルウェア対策及び脆弱性管理（仮想パッチを含む）を２４時間３６５日体制で提供すること。

g) 契約に関与する者以外に対しては，保護すべき情報の内容及びファイル名を表示させないこと。また，契約等の単位でアクセスを制御し，他の契約等の情報と混在させないこと。なお，企業側端末内に保存されたデータの物理的な削除は必須としないが，前記のアクセス制御を確実に担保すること。

h) ＤＳＧを構成するサービスに係るアクセスログ等の証跡を保存し，官からの要求があった場合は提供すること。

i) ＤＳＧを構成するサービスにおける脆弱性対策の実施内容を官が確認できること。

j) ＤＳＧを構成するサービス上で取り扱う情報について，機密性及び完全性を確保するためのアクセス制御，暗号化及び暗号鍵の保護並びに管理を確実に行うこと。

7.2 サービスの提供条件及び契約終了時の措置

a) ＤＳＧを構成するサービスにおいて個人情報又は保護情報が取り扱われる場合には，当該サービスの契約に定める準拠法に従い，裁判管轄は国内に限ること。

b) ＤＳＧを構成するサービスの廃止，サービス内容の変更等に伴い契約を終了する場合は，他のサービス等に円滑に移行できるよう，十分な期間をもって事前（サービス廃止等の２年以上前が望ましい。）に官に通知すること。

c) ＤＳＧを構成するサービスの契約を終了する場合，官と協議の上，サービス上に保存されたデータを保証すること。

d) 官に対して，ＤＳＧを構成するサービスに係る機密性の高い情報を開示する場合は，官において，当該情報を審査又は本業務以外の目的で利用しないよう適切に取り扱うため，必要に応じて当該情報に取扱制限を明記するなどの措置を講じること。

e) ＤＳＧのサービス利用以外の方法で保管データを提供する場合は，当該データの機密性を確保するための保護手段を講じること。

f) 提供サービスの追加・変更が生じる場合，官と協議の上，原則受け入れられること。

7.3 サービスの可用性及び事業継続

ＤＳＧを構成するサービスの可用性を保証するための十分な冗長性，障害時の円滑な切り替え等の対策が講じられていること。

8. 監査の実施

契約相手方は，**情報セキュリティ通達**における添付書類「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おける特約条項」，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，官が実施する監査の受け入れが可能であること。監査の際，契約の相手方は，官の求めに応じ，本役務に関連する情報を開示すること。

9. その他の指示

9.1 情報保全

a) 契約相手方は，官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，**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借置の細部事項について（通知）**，別添情報システムに関する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。

c) 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。）の取扱いに当たっては，**情報セキュリティ通達**における添付書類「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) 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
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

d) 上記 a)から c)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，保護情報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) 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に報告すること。

f) 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。

g) 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，契約相手方は官の求めに応じ，協議を行い，必要な対策を講

じること。

h) 装備政策部長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装備政策部長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。

i) 立入禁止場所等において保守作業若しくは搬入調整作業等を実施するに当たっては，各部隊等所定の立入申請書により過去に立ち入りの実績がある場合は作業の 2 週間前までに，実績がない場合は契約後速やかに提出し，許可を得ること。

j) 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，官と協議の上，その指示に従うこと。

k) 契約相手方は，官から貸付けを受けた文書及び電子データについては，当該役務終了時に官に返却すること。また，提供を受けた文書及び電子データについては，当該役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。

l) 本契約に係る情報及び情報システム以外の官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。

m) 契約相手方は，ＤＳＧにおいて，情報セキュリティが侵害され又は侵害されるおそれが発生した場合には，直ちに官に報告すること。

n) 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が認めた場合は，官の求めに応じ協議を行い，官と合意の上で，改善を図ること。

9.2 知的財産権の帰属

知的財産権の帰属は，次による。

9.2.1 著作権

a) 契約相手方は，契約書又は仕様書の定めるところにより官に提出された著作物（**著作権法**第１０条第１項第９号で規定されるプログラムの著作物を除く。）に関する全ての著作権（同法第２７条及び第２８条に規定する権利を含む。）を，納入と同時に官に譲渡し，また，契約相手方は著作者人格権を行使せず，契約相手方は第三者に著作者人格権を行使させない。ただし，契約相手方の固有の技術資料（契約相手方が第三者から提供を受けたものを含む。）に係る著作権及び著作者人格権についてはこの限りでない。

b) 提出書類等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。

c) 本業務の提出書類等に関し，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。

d) 官は，本契約の履行中及び終了後５年間は，契約書又は仕様書の定めるところにより官に提出された契約相手方の固有の技術資料につき，本契約に関して官が行う監督，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，

契約相手方の固有の技術資料に係る著作物を，官の内部において複製，翻訳及び翻案することができる。ただし，当該技術資料のうち契約相手方の指定するものを除く。

e) 官は，契約相手方から，上記 a)により官が譲渡を受けた著作権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。官は，本契約の履行中及び終了後５年間は，契約書又は仕様書の定めるところにより官に提出された，提出書類等に組み込まれた契約相手方がすでに著作権を保有しているもの（以下，「固有の著作物」という。）につき，本契約に関して官が行う監督，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，固有の著作物を，内部において複製，翻訳及び翻案することができる。ただし，固有の著作物のうち契約相手方の指定するものを除く。

f) 前記 e)にかかわらず，契約相手方は，官の使用に供する目的で，上記 a)により官が譲渡を受けた著作権に係る著作物を複製し，翻訳し又は翻案することができる。

g) 契約相手方は，知る限りにおいて，仕様書で定める事項の遂行に当たり実施した又は留意すべき特許権，実用新案権又は意匠権（出願中を含む。）を報告する。また，契約相手方は，官に提出した技術資料に含まれている契約相手方の固有の技術資料の記載箇所及び上項 d)ただし書きの指定について，官に報告する。以上の報告は，知的財産管理報告書を作成し，官に提出して行うものとする。

9.2.2 権利義務の帰属等

a) 契約相手方は，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**（平成１４年法律第１２２号）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。

b) 契約相手方が，前記 a)の必要な措置を講じなかったことにより官が損害を受けた場合は，官は，契約相手方に対してその賠償を請求することができる。

c) 本契約において作成した情報は，官の所有に属するものとする。

9.3 再委託

再委託する場合においては，**デジタル・ガバメント推進標準ガイドライン**に基づき，次の事項を遵守するものとする。

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及び報告徴収，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，官の承認を受けなければならない。

d) 契約相手方は，上記 b)又は前記 c)により再委託を行う場合には，契約相手方が官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「**9.1 情報保全**」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) 上記 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，官側と協議したうえで，**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）**に定める特約条項に基づき必要な手続を実施するものとする。

9.4 提出書類

提出書類は，**表**による。また，作業の実施に当たり，当該文書の記載事項に変更が生じた場合は，速やかに該当箇所を修正し，官の確認後，提出すること。なお，月次報告書及び年次報告書に記載する項目は，技術要件一覧に定める内容を含むこととする。また，利用者マニュアル，サービス仕様書及びサービスカタログについては，先行サービスの開始前までに提出し，官の合意を得ること。

表３　提出書類

番号	文書名	提出時期	数量 電子媒体	提出先	備考
１	役務実施計画書	契約後 速やかに	１部	防衛装備庁情報システム管理室	**別紙２**の各項目に適合していることが記載されたもの及び本件の役務の実施計画
２	サービス 提供体制表	契約後 速やかに	１部		「**5.1 役務の実施体制**」に定める実施体制及び提供実績を示したもの
３	実績レポート	実績確定後 速やかに	１部		毎月の利用数量及び利用料金の確定後，利用実績を示すもの
４	月次報告書	毎月	１部		当月のサービス提供状況・利用実績・インシデント等を記載したもの
５	年次報告書	毎年度末	１部		当該年度のサービス提供状況・実績・改善提案等を記載したもの
６	サービス仕様書	先行サービス 開始前	１部		「**1.2 用語の定義**」の「サービス仕様書」に定めるもの
７	インシデント 報告書	発生後 速やかに	１部		セキュリティインシデント等の発生・対応・再発防止策を記載したもの
８	技術要件確認結果 報告書	先行サービス 開始前	１部		**別紙２**「技術要件詳細」への適合を示したもの
９	利用者マニュアル	先行サービス 開始前	１部		利用者がＤＳＧの各サービスを利用するための操作手順等を記載したもの
１０	サービスカタログ	先行サービス 開始前	１部		「**1.2 用語の定義**」の「サービスカタログ」に定めるもの
１１	緊急時対応計画	作成及び修正後 速やかに	１部		「**1.2 用語の定義**」の「緊急時対応計画」に定めるもの

9.5　貸付文書等

契約の相手方は，サービスの提供に必要と認める官の保有する文書等について，官と協議の上，無償で借受け又は閲覧することができる。

9.6　官側の支援

9.6.1　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，官が認める範囲内において，次に示す支援を無償で使用することができる。

a)　防衛省内における搬入器材の保管

b)　防衛省内における電力，水，スペース等の使用

c)　防衛省内における施設の利用

d)　防衛省内における官の保有する関連器材の使用

e)　防衛省内の回線

f)　機能確認に関する事前調整及び現地確認時の支援

g)　その他，契約履行に必要な事項

9.6.2　国有財産の使用制限

a)　契約相手方は，「**9.6.1　国有財産の利用**」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，あらかじめ官と協議した上で，官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，上記 **a)** 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。

10　その他特記事項

a)　ＤＳＧのサービス提供に当たり，官の指示に従うとともに，細部にわたり官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)　官の情報が含まれるハードディスク及び機器等については，契約終了等において，官の情報を消去するため，物理的な破壊等により使用不能な状態とすることができること。その際，読み取り不可能にしたことが確認できる証明書を提出すること。

c)　引用文書及び関連文書を閲覧する必要が生じた場合は，官と協議すること。

d)　この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)　提出書類等は，**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。