令和8年1月21日　　支担官第757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。

記

１．入札に付する事項

調達番号	件名	内容	履行場所	履行期限
情-I-070	法令クリアリングシステムの運用（Ｒ７換装）	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１１月３０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８年２月２５日(水)　（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）適合条件を満たすことを証明する書類を期日までに提出し承認を得た者であること。（別紙参照）
（７）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　２月　２日　（月）　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
資料の信頼性確保及び制度調査の実施に関する特約条項
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）入札に関する条件　仕様書3.2 a)～c)に定める本業務の実施体制並びに仕様書10.a)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　２月　４日（水）　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８年　２月　２０日　（金）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）

<u>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</u>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　押川　電話　03-3268-3111　内線20823

別紙

適合条件

１　条件

契約相手方は，会社全体又は業務実施責任者が所属する部門が，以下の条件をすべて満たしていること。

a）過去の受注実績

今年度より過去５年間に防衛省が発注した業務において，ＤＩＩ上又はＤＩＩに連接するインフラ基盤で運用する情報システムの構築整備及び運用に係る役務をそれぞれ完了した実績があること。

b）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。

c）パブリッククラウドに関する業務実績

外部公開用環境に採用するパブリッククラウドを利用したウエブサービスの構築・運用の実績を保有していること。

d）セキュリティガイドラインに係る製品等の提供実績

ＮＩＳＴ　ＳＰ８００－１７１のセキュリティに関する技術的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があること。

e）その他

装備品等及び役務の調達における情報セキュリティ（通達）の添付資料「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」適合者であること。

２　提出書類

１の条件を満たすことが客観的に示されているもの（形式は任意とし、提出書類には、会社名等を表示したうえで綴るものとする。）。

なお、提出書類に関する問い合わせは、提出期限前日の１７時１５分までとする。また、提出した証明書等について、官側が説明を求めたときはこれに応じなければならない。

提出された証明書等を審査の結果、当該案件を履行できると認められた者に限り入札の対象とする。

なお、提出書類については虚偽がないものとする。

３　提出部数

１部

４　提出期限

２月４日（水）１２：００

仕様書		
法令クリアリングシステムの運用（Ｒ７換装）	作成年月日	令和８年１月１４日
	作成課	大臣官房文書課

1　総則

1.1　適用範囲

この仕様書は，大臣官房文書課が行う「法令クリアリングシステムの運用」（以下「本役務」という。）の調達について規定する。

1.2　引用文書等

この仕様書における引用文書は，この仕様書の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，引用文書に定める事項がこの仕様書と相違する場合は，法令等を除き，この仕様書を優先する。なお，引用文書は，入札書又は見積書の提出時における最新版を適用する。

1.2.1　引用文書

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)　**著作権法**（昭和４５年法律第５３号）
3)　**個人情報の保護に関する法律**（平成１５年法律第５７号）
4)　**知的財産基本法**（平成１４年１２月４日法律第１２２号）
5)　**「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））
6)　***デジタル・ガバメント推進標準ガイドライン***（令和７年５月２７日更新））（以下**「*標準ガイドライン本編*」**という。）
7)　***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７年５月２７日更新））（以下**「*標準ガイドライン実践ガイドブック*」**という。）
8)　***デジタル・ガバメント推進標準ガイドライン解説書***（令和７年５月２７日更新））（以下**「*標準ガイドライン解説書*」**という。）
9)　**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）
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。平成３１年１月９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）**（装管調第５１２１号（令和２年３月３１日））
12)　**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。）

b)　**規格**

ＪＩＳ Ｑ ２７００１　情報セキュリティマネジメントシステム（ＩＳＭＳ）
ＪＩＳ Ｘ ０００１：１９９４　情報処理用語－基本用語
ＮＩＳＴ　ＳＰ８００－１７１　**非政府機関情報システムにおけるＣＵＩの保護**

1.2.2　関連文書

a)　**法令等**

1)　**電気用品安全法**（昭和３６年法律第２３４号）
2)　**政府機関の情報セキュリティ対策のための統一管理基準**（情報セキュリティ政策会議）
3)　**政府機関の情報セキュリティ対策のための統一技術基準**（情報セキュリティ対策推進会議）
4)　**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）
5)　**防衛装備庁の情報保証に関する訓令**（平成２７年防衛装備庁訓令１２号）
6)　**防衛省の情報保証に関する訓令の運用について**（防運情第９２４８号。１９．９．２０）
7)　**取扱い上の注意を要する文章等及び注意電子計算機情報の取扱いについて**（防防調第４６０８号。１９．４．２７）
8)　**防衛情報通信基盤データ通信網利用要領について**（統幕指運第４３号。令和３年３月１７日）

9) 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））
10) 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７年度版）
11) 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（防整サ第１４５５０号。令和５年７月３日）
12) 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（防整サ第１４５５１号。令和５年７月３日）

b) 規格
1) ＩＳＯ９００１　品質マネジメントシステムー要求事項
2) ＪＩＳ Ｘ ０００１　情報処理用語－基本用語
3) ＪＩＳ Ｚ ８３０１　規格票の様式及び作成方法

c) 仕様書
ＤＳＰ Ｚ ９００８　品質管理等共通仕様書

d) その他
1) クリアリングシステム用電算機借上（令和元年度，仕様書番号５-０１-００１５）
2) クリアリングシステムの機能維持に係るプログラム改修（平成２６年，仕様書番号 情-Ｉ-０２７）
3) クリアリングシステムの機能維持に係るプログラム改修（令和元年度，仕様書番号 情-Ｉ-０３３）

1.3 用語の定義

この仕様書で使用する用語及び定義は，**表１**に定めるところによる。

表１ー用語の定義

用語	定義
インフラ基盤	防衛省（以下,「官側」という。）がソフト運用のために使用する基盤の総称を指す。
省ＯＡ	防衛省中央ＯＡネットワーク・システムを指す。
省ＯＡ端末	市ヶ谷地区で用いられる省ＯＡに接続して，各種処理を行うための電子計算機
法令クリアリングシステム	防衛省が保有・運用し，省内外にも公開している，防衛省所管法令類に関するデータベースおよび検索ソフトを指す。
現行システム	令和８年１２月までの運用を想定している,現在防衛省で運用されている法令クリアリングシステムを指す。
次期システム	本役務で調達する法令クリアリングシステムを指す。
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。本仕様書では，インフラ基盤のうち「部外データセンターに用意するクラウドサービス」及び「パブリッククラウド上に用意するクラウドサービス」を指す。
市ヶ谷地区	市ヶ谷駐屯地・基地，政府控室及び各通信所
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
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
ＤＩＩ	Defense Information Infrastructure（防衛情報通信基盤）の略名で，自衛隊が共通に使用する音声通信網及びデータ通信網を指す。また，データ通信網に接続を承認された情報システムに必要なサービスを提供するもの
ＷＢＳ	プロジェクトマネジメントで計画を立てる際，プロジェクト全体を細かい作業に分割し，階層構造で表した作業分解図を指す
ＧＯＴＳ	政府機関オフザシェルフ(Government Off-The-Shelf)の略。

	本仕様書においては防衛省が所有権を有する法令クリアリングシステムのソフトウェアおよびデータベースについて指す。
ＣＯＴＳ	商用オフザシェルフ(Commercial Off-The-Shelf)の略。民需量産品の活用あるいは，民生製品，民生技術をいう。
ＤＳＧ	防衛セキュリティゲートウェイの略。取り扱う保護すべき情報を，防衛省と防衛関連企業の間で，電子データの形で安全かつ効率的に共有することを可能とする通信基盤を指す。
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。

2　本役務の概要

2.1　調達の背景

従前より防衛省職員の利便性向上や，一般国民への説明責任の履行という観点から防衛省で制定された注意区分を有しない訓令及び通達類について公開すべく，これらのデータベースを検索機能付きで運用してきたところである。現行システムについては，省内用と省外用に二つのサーバをＤＩＩ仮想サーバ提供サービスで運用してきたところ，サーバ類のライセンス期限を迎えるという事情，さらにサイバーセキュリティリスクの高まりに伴うリスクへの対応という観点から，より強固なセキュリティ機能を備えた部外のインフラ基盤で運用されるシステムを調達することとなったものである。

2.2　本調達の目的及び期待する効果

法令クリアリングシステムは，防衛省全職員が利用し，職員約２７０，０００名が業務上必要な法令情報を検索できるシステムである。また，防衛省外にも同法令情報等を公開することで，主権者たる国民に対し防衛行政に関する説明責任を果たす一翼を担うシステムであり，本役務については，セキュアで継続的に利用可能なインフラ基盤を調達することで，安定したシステム運用環境の確保とセキュリティ体制の向上を図ることを目的とするものである。

2.3　調達の概要

契約相手方は，法令クリアリングシステムについて，現行システムと同様に防衛省のネットワーク基盤であるＤＩＩ経由で省内から法令情報を閲覧可能とするとともに，省外からの利用者がパブリッククラウドにアクセスすることで法令情報等を閲覧可能なとするために，所要のセキュリティ体制が整備された環境下にあるインフラ基盤（次期システム運用環境）をサービス契約により調達し，官側が現在ＧＯＴＳとして保有する法令クリアリングシステムのソフトウェアを非互換改修した上で，サービス提供されるそれらのインフラ基盤に搭載すること。

2.4　事業スケジュール

本役務に係る事業スケジュールは**図１**のとおり。

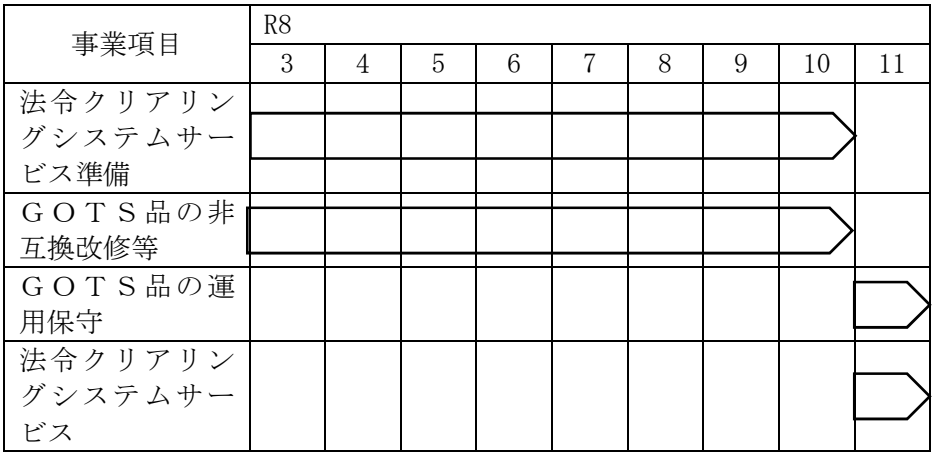

図１－事業スケジュール

2.4.1　運用期間

令和８年１１月１日から令和８年１１月３０日までの期間とする。

3　本役務に関する要求

3.1　事業者の要件

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，以下の要件をすべて満たしていること。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)　過去の受注実績

今年度より過去５年間に防衛省が発注した業務において，ＤＩＩ上又はＤＩＩに連接するインフラ基盤で運用する情報システムの構築整備及び運用に係る役務をそれぞれ完了した実績があること。

b)　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。

c)　パブリッククラウドに関する業務実績

外部公開用環境に採用するパブリッククラウドを利用したウエブサービスの構築・運用の実績を保有していること。

d)　セキュリティガイドラインに係る製品等の提供実績

ＮＩＳＴ　ＳＰ８００－１７１のセキュリティに関する技術的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があること。

e)　その他

装備品等及び役務の調達における情報セキュリティ（通達）の添付資料「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」適合者であること。

3.2　業務従事者の要件

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，官側の承認なく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。

a)　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。）を確保すること

b)　業務従事者が，履行する必要もしくは有用な，または背景となる経歴，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。

c)　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体制にあること。

3.3　役務の実施体制

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，本調達の成功（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)　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。

b)　要員には，①ウエブアプリケーションシステムの構築，②システム運用・保守及び③パブリッククラウドを利用した情報システム整備・運用に関する経験を有する者（複数名で満たすことでも可とする。）を含むこと。

c) 本役務において準備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。

d) 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，２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。

e) 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。

3.4 全般

a) **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）第６条による基本方針を満足すること。

b) 契約の相手方は，**標準ガイドライン本編**の別紙３の１項に基づき，区分等した契約金額の内訳が記載された情報システムの経費区分一覧を契約締結後２週間以内に提出すること。

c) インフラ基盤及び改修後のクリアリングシステムのソフトウェアに関する構成品は，**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**に基づき，情報の漏えい若しくは破壊又は機能の不正な停止，暴走その他の障害等のリスク（未発見の意図せざる脆弱性を除く。）が潜在すると契約の相手方が知り，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が行われていないものでなければならない。

d) インフラ基盤及び改修後のクリアリングシステムのソフトウェアに関する構成品目は，サプライチェーン・リスクへの対応指針によって，製品・サービスにマルウェア等の不正なプログラム及び機器並びに模造品等が組み込まれる等のリスクへの調査が対応可能な製品とする。また，設置後，官側から指示があった場合は，速やかに対象製品の製造元等に関する資料を官側に提出すること。

e) 契約の相手方は，**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**第５条第３項に定められた作業従事者管理報告書（作業従事者名簿の従事者ごとに作業内容の予定と実績を日ごとに記録する報告書）を官側施設で作業を実施する場合，作業実施前及び作業実施後３日以内に官側に提出すること。

3.5 基本的留意事項

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) 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。

b) 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。

3.6 本役務の計画策定及び状況報告等

a) 契約締結後，２週間以内に本役務を実施するために必要な作業を洗い出し，作業体制を策定し，作業実施計画書について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，変更部分について官側に報告し，承認を得ること。

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，各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) コミュニケーション管理

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。

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。

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。

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) 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。

3.7 調達における報告・調整会議の主催

a) 契約相手方は，作業の状況について，隔週を基準とし報告会議・調整会議を開催すること。ただし，官側がこれを要しないと判断した場合はこの限りではない。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) 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。

3.8 システムと利用者の端末との連携に関する条件

官側のクリアリングシステム利用者が省ＯＡの端末から利用することを前提とする。

4 サービスに関する要求

契約相手方は，データセンター内及びパブリッククラウド上に，本項で定める基準を満たしたサービスを提供すること。

なお，パブリッククラウドについては，政府が定める政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program：ISMAP）の認定を受けたものであること。

4.1 運用開始に伴うシステム移行

システム移行においては，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時期について検討の上，官側と協議すること。

4.2 インフラ概要及び構成

システム概要は，**図２及び表２**を基準とする。

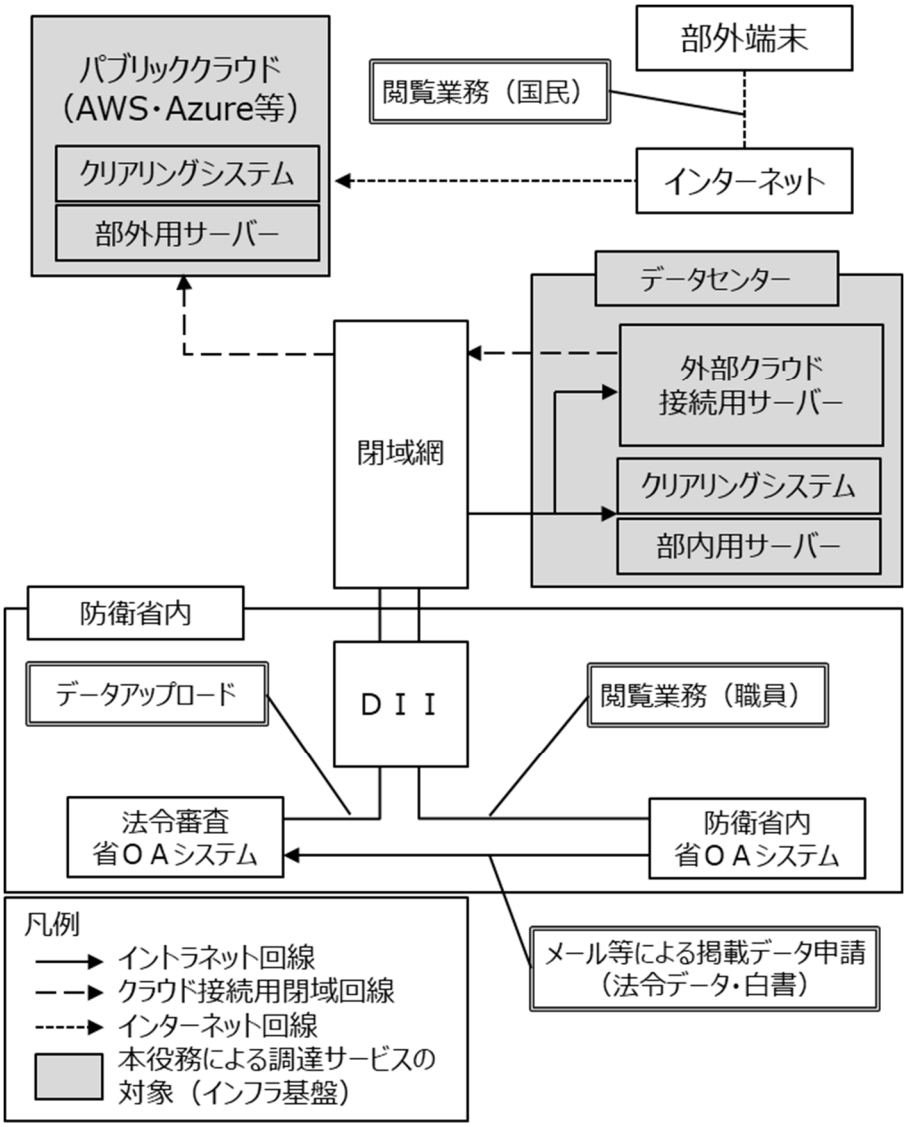

図２－業務・システムの概要図

表２－主要な業務と業務概要

法令検索業務	本システムにおいて，法令データベースへのアクセスを通じた防衛省の規則類に関する検索，データ閲覧，データダウンロード
防衛白書検索業務	本システムにおいて，法令データベースへのアクセスを通じた防衛白書に関する年度ごとの検索，データ閲覧，データダウンロード
掲載法令データの掲載	本システムにおいて，検索機能を通じ検索できる形式での法令データファイルの掲載作業
防衛白書の掲載	本システムにおいて，検索機能を通じ検索できる形式での防衛白書データの掲載作業

4.3　提供サービスに要求する事項

本システムは，契約相手方から提供されるサービスにより整備・運用されるものとする。

提供サービスに要求する事項については，**別冊**のとおりとする。

4.4 サービス準備に関する要求

契約相手方は上記のほか，インフラ基盤（**図２**に示すパブリッククラウド及びデータセンターを指す。）の利用に伴い付随して発生する以下の作業について，運用開始までに実施すること。

a)　パブリッククラウド上のクラウドサービスの準備

パブリッククラウド上に，インターネットからのアクセス用に仮想サーバを用意し，契約相手方が提供するデータセンターと閉域ネットワークで接続したうえで，部内系のデータセンターに実装する法令クリアリングシステムのデータベースと同様のデータベースをインターネットから閲覧可能な環境を準備すること。

インターネットからの閲覧にあたって，本システムの部内系に部外用サーバを更新するための外部クラウド接続用サーバを設けて間接的に部外用サーバをメンテナンス可能な構成とすること。概要については**図２**による。また，契約相手方はパブリッククラウドに必要なセキュリティ対策（ファイアウォール等）も併せて実装すること。

b) データセンター内へのクラウドサービスの準備

省ＯＡ端末から，法令クリアリングシステムの部内用サーバへの接続（閲覧，データアップロード用）を可能とすること。概要については**図２**による。また，契約相手方はデータセンターに必要なセキュリティ対策（ファイアウォール等）も併せて実装すること

c) サーバ証明書の準備

ＳＳＬサーバ証明書の取得に必要な情報を官側に提示し，証明書発行に関する支援を実施すること。また，ＳＳＬサーバ証明書が発行され次第，ソフトウェア導入時にサーバに設定すること。

d) ＤＩＩオープン系との接続

契約相手方が提供するデータセンターについて，ＤＩＩのオープン系と接続できるよう，閉域網を提供するとともに，官は設定変更等について適宜ＤＩＩと調整することから，契約相手方はそれに必要な情報提供を適宜実施すること。

e) サーバ及びクラウドへの搭載

運用に当たって使用するインフラ基盤に，**5.** に求める改修後のＧＯＴＳを搭載すること。

f) データベースのインポート

ソフトウェアに紐づく，法令データについて，現行システムで使用しているデータベースをインポートし，ソフトウェアの検索タグと紐づけを実施すること。なお，法令データについてはインポート時における最新版とし，差し替えデータが官側から提供された際は，インポート時に提供されたデータに差し替えること。

5　ＧＯＴＳ品の非互換改修に関する要求

5.1　改修概要

当該サービスにクリアリングシステムのソフトウェアを搭載するにあたり，必要となる非互換改修について実施するものとする。

5.2　改修の内容

契約相手方は，契約後，運用開始前までに**表３**に定める内容の改修を実施し，当該サービスに搭載すること。

表３－改修作業項目

改修作業項目	改修作業概要
サービスに対応するための非互換改修	当該サービスにソフトウェアを搭載するにあたり，支障なく運用するための非互換改修※を実施すること。なお，改修時は，4.2 に定める業務に必要な機能を損なってはならない。
ＤＩＩオープン系との接続に伴う改修	当該サービスとＤＩＩのオープン系が接続されることに伴い，クリアリングシステムへの法令データのアップロード等の作業について，省ＯＡ端末からの作業が可能であるかを検証し，必要に応じて適合するためのソフトウェア改修を行うこと。

※　非互換改修にあたっては，ＧＯＴＳの中に含まれるソフトウェアについて更新が必要な場合はライセンス等を取得の上，適切に最新版に更新すること。

5.3　特別の留意事項

a)　ソフトウェアの非互換改修については，当該サービスにおいて，異常なく動作するよう調整に万全を期すこと。

b)　改修後のソフトウェアを当該サービスに搭載したのち，異常なく検索画面が表示され，データの更新機能，法令データへのアクセス機能が動作するかについて最終点検を実施すること。

5.4　改修後のプログラムの関係資料の作成

改修後のＧＯＴＳについて，基本設計書，詳細設計書，プログラム設計書及びプログラムを作成し，官側に提出すること。

5.5　改修後のユーザマニュアルの作成

改修後の法令クリアリングシステムについて，省ＯＡ端末からのアップロードによる運用開始に伴い，データアップロード作業に関する操作手順書について作成し，提出すること。

また，本業務の実施によって既存の本システム操作手順書（運用管理要領及び運用監視マニュアル）に変更が発生する場合には，変更箇所について官側と確認の上，必要な修正を実施すること。

6　ＧＯＴＳ品の運用保守に関する要求

6.1　保守条件

保守期間は，システムの運用期間に準ずること。

6.2　保守体制

ＧＯＴＳソフトウェアサポートに係る保守体制は次による。

1)　ＧＯＴＳソフトウェアごとの技術情報提供

2)　ＧＯＴＳソフトウェアの不具合発生時の状況分析及び障害の切り分けに並びに対処

6.3　保守実施項目

契約の相手方は，当該サービスが常時目的の機能を完全に発揮しうる状態を維持するため，適時適切な保守の提供を行うものとし，保守実施項目は次による。

a)　障害が発生し，クリアリングシステムの運用に影響が出る場合は，障害発生時から１営業日を基準として復旧に努めるものとする。

b)　契約の相手方は，交通事情又は天候などによる例外を除き，通常，障害発生時の電話連絡から速やかに要員の派遣を行い，復旧に当たるものとする。

c)　クリアリングシステムの運用のために使用するソフトウェアに対する機能，操作方法，設定方法及び運用中に発生した問題及び障害に対し，電話，電子メール等の手段を用いて対応するものとする。

d)　障害発生時の対応については，契約相手方の通常の営業日・営業時間に基づく。

7　品質管理

a)　品質管理は，b)による。また，**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**に基づき，b)のサプライチェーン・リスクへの対応を行うこと。

b) 当該サービスの構成品は，障害等リスクが潜在すると契約の相手方が知り，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側の意図せざる変更が行われない相応の管理その他の契約の相手方（下請負者，再委託先等含む。）による適正な品質管理の下で製作されたものであって，その品質を保証されたものでなければならない。

8 貸付品

応札希望者及び契約相手方は，**表４**に示す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。

表４－貸付／閲覧品

番号	名称	数量	媒体	貸付等期間	貸付等場所
1	クリアリングシステム　詳細設計書	1	電子	令和８年 11 月 30 日まで	大臣官房文書課
2	クリアリングシステム　プログラム設計書	1	電子		
3	クリアリングシステム　プログラム	1	電子		
4	クリアリングシステム　運用管理要領	1	電子		
5	クリアリングシステム　運用監視マニュアル	1	電子		

9 提出物等

9.1 提出物

契約相手方は，**表５**に示す提出物を，提出時期までに提出し官側の承認を得ること。

また，令和８年１１月３０日までに，追記不可の処置を実施後，最終版を提出するものとする。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，官側と相談の上，合意した期間内に該当箇所を修正し，官側の承認を得ること。

表５－提出物

No.	文書名	部数	提出時期	備考
1	経費区分一覧	１部	契約締結後２週間以内	3.4b による。
2	作業従事者管理報告書	１部	作業実施前及び作業実施後３日以内	3.4e による。ただし，防衛省内で作業を要する場合に限る。
3	作業実施計画書	１部	契約締結後２週間以内	3.6a による。
4	基本設計書	１部	システム運用開始前まで	5.4 による。
5	詳細設計書	１部	システム運用開始前まで	5.4 による。
6	プログラム設計書	１部	システム運用開始前まで	5.4 による。
7	プログラム	１部	システム運用開始前まで	5.4 による。
8	ユーザマニュアル	１部	システム運用開始前まで	5.5 による。
9	運用管理要領	１部	システム運用開始前まで	5.5 による。
10	運用監視マニュアル	１部	システム運用開始前まで	5.5 による。
11	サービス完了報告書	１部	サービス完了後速やかに	4 による。
12	サービス準備完了報告書	１部	サービス準備完了後速やかに	4 による。
13	改修作業完了報告書	１部	作業完了後速やかに	5 による。
14	運用保守役務完了報告書	１部	役務完了後速やかに	6 による。

備考：提出媒体は全て電子媒体とする

9.2 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，**ＪＩＳ Ｘ ０００１：１９９４**情報処理用語－基本用語の規定に準拠すること。
d) 提出文書は電子媒体により作成し，**表５**に示す提出部数を提出すること。
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。
f) 電子媒体による提出について，一太郎 Government，Microsoft Word，同 Excel，同 PowerPoint 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。

9.3 提出場所

提出文書は，原則として以下の場所に直接提出，電子メールまたはＤＳＧによる提出とする。

（提出先）

〒162-8801 東京都新宿区市谷本村町５－１　防衛省大臣官房文書課法令審査

10 情報保全

情報の保全は，次による。

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

3) 官が書面により個別に許可した場合を除き，契約相手方に係る親会社，地域統括会社，ブランド・ライセンサー，フランチャイザー，コンサルタントその他の契約相手方に対して指導，監督，業務支援，助言，監査等を行う者を含む一切の契約相手方以外の者に対して伝達又は漏えいされないことを保障する履行体制

b) 契約相手方は第三者を従事させる場合を含め，サプライチェーン・リスクに対応し，**情報システムに関する調達に係るサプライチェーン・リスク対応のための措置について（通達）**及び**情報システムに関する調達に係るサプライチェーン・リスク対応のための措置の細部事項について（通知）**に定める特約条項並びに**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）**に基づき行うものとするほか，官の指示に従うものとする。

c) 上記 a)の保護すべき情報の細部については，**表６**のとおりとする。

表６－保護情報

番号	保護すべき情報	保護すべき情報の詳細
1	ネットワーク構成	ネットワーク構成，配線図
2	インターフェイス（アドレス，プロトコル等）仕様	ＩＰアドレス
3	セキュリティ（ファイアーウォール等）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
		管理者パスワード

11 立入禁止場所等への立入

契約の相手方は，この契約の履行に当たり，立入禁止区域への立入が必要な場合には，官側が定める規則等に従い，事前に立入申請を行うこと。

12 官側の支援

契約の相手方は，この契約の履行に当たり，次の事項について官側の支援を必要とする場合には，事前に官側と調整の上，無償で官側の支援を受けることができる。

a) 現地における機器等の搬入時の立会，保管場所の提供，搬入器材の保管
b) 現地における電力，用水，スペース等の使用
c) 官側施設及び構内回線の利用
d) 官側の保有する関連器材の使用
e) 機能確認に関する事前調整及び現地確認時の支援
f) その他，契約履行に必要な事項

13 著作権その他の権利

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（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技術資料を含む。以下同じ。）を除く。）についての著作権（**著作権法第２７条**及び**第２８条**に規定する権利を含む。）を官に譲渡し，著作者人格権を行使しないこと。また，当該著作物の著作者が契約の相手方以外の者であるときは，当該著作者が著作者人格権を行使しないよう必要な措置をとること。

b) 官側は，この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き，この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（当該資料のうち契約相手方の指定するものの複製を除く。）することができること。

c) 官側は，契約の相手方から，上記 a)により官側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こと。

d) 前記 c)にかかわらず，契約の相手方は，防衛省の使用に供する目的で，上記 a)より官側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こと。

e) 契約の相手方は，この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こと。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こと。

f) 官側及び契約の相手方は，知的財産権の権利の帰属等に関し，疑義が生じた場合には，その都度協議して解決すること。

g) 契約の相手方は，本契約の履行により得られた知的財産，上記 a)に規定する契約の相手方の固有の技術資料及び上記 b)に規定する契約相手方の指定するものについて，知的財産の概要，権利，帰属，実施権等の設定可否等について知的財産管理報告書を作成し，提出すること。

14 個人情報の保護

a) 「個人情報」とは，本契約に基づき契約の相手方が取り扱う氏名，年齢，その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができるものを含む。）をいう。

b) 個人情報の保護に関する法律（平成１５年法律第５７号）を遵守すること。

c) 個人情報の保護の重要性を認識し，本契約の履行にあたっては個人の権利を侵害することのないよう，個人情報を適正に取り扱わなければならない。

d) 本契約に関して知り得た個人情報を，本契約を遂行する目的以外に使用してはならず，また，他に漏洩してはならない。本契約が終了し，または解除された後においても同様とする。

15 再委託

再委託は，次に掲げるとおりとする。

a) 契約の相手方は，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) 契約の相手方は，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，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，契約締結後やむをえ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，上記 b)又は c)により再委託を行う場合には，契約の相手方が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，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業務を実施させる場合は，全ての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，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**に定める特約条項に基づき必要な手続を実施すること。

16 仕様書の疑義

この仕様書にお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。

17　ＲＭＦ審査プロセスへの対応協力

契約相手方は，システムの運用開始に先立ち，運用承認取得に向けたＲＭＦ審査プロセスにおいて，当該審査役務を受諾した側から，システム構成等の情報提供を求められた場合，官側の回答作成に必要な情報を提供するものとする。

別冊

提供サービスに要求する事項

調達件名：法令クリアリングシステムの運用（Ｒ７換装）

サービス一覧

サービス名	内容
法令クリアリングシステムサービス（部外）	**別紙１**及び**別紙２**に示す基本事項の対応を含む、法令クリアリングシステムサービス（部外）の提供の際に必要な項目は以下のとおりとする。 ・　コンピュート ・　ネットワーク・回線 ・　システム運用管理 ・　セキュリティ（全般） ・　ＳＯＣ機能
法令クリアリングシステムサービス（部内）	**別紙１**及び**別紙３**に示す基本事項の対応を含む、法令クリアリングシステムサービス（部内）の提供の際に必要な項目は以下のとおりとする。 ・　コンピュート ・　ネットワーク・回線 ・　システム運用管理 ・　セキュリティ（全般） ・　ＳＯＣ機能 ・　データセンター

基本事項（続き）

サービス基本事項（全般）

項番	項目	要件
1	サービス全般	契約後速やかに，本件の役務の実施計画書（基本事項に示す各項目に適合することを示す内容を含むものとする。）を提出し、法令クリアリングシステムシステムサービス運用開始前に官側の承認を得ること。
2	サービス全般	法令クリアリングシステムサービスの廃止，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１年以上前が望ましい。）に防衛省へ通知できること。
3	サービス全般	構成するサービスの契約を終了する場合は，サービス上に保存されたデータを保証すること。
4	法令順守	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。
5	サポート	各サービスの運用状況・障害情報を通知又は確認できること。
6	拡張性	官側の求めにより，提供サービスの追加又は提供サービスの変更が生じる場合，契約相手方は官側と協議の上，原則としてこれを受け入れることができること。

各種サービスの技術要件詳細

法令クリアリングシステムサービス（部外）要件

項番	項目	要件
1	コンピュート	仮想マシンは現行システム運用されているデータについて，インターネットを介して提供できること。
2	コンピュート	仮想マシンは現行データの公開情報を管理できること。
3	コンピュート	ＣＰＵのコア数は１サーバあたり８コアを基準として提供し、利用状況に応じて追加できること。
4	コンピュート	メモリサイズは１サーバあたり１０GBを基準として提供し、利用状況に応じて追加できること。
5	コンピュート	サーバのシステム領域とデータ保存領域を併せて、１サーバあたり６７５GB以上のディスクを搭載して提供すること。
6	コンピュート	WEBサーバ機能を有すること。
7	コンピュート	官側が現在ＧＯＴＳとして保有する法令クリアリングシステムのソフトウェアを非互換改修したアプリケーションが利用できること。
8	コンピュート	文書検索処理が３件/秒以上実行できること。
9	コンピュート	文書閲覧処理が３件/秒以上実行できること。
10	コンピュート	パブリッククラウド上に，インターネットからのアクセス用に仮想サーバを用意し，使用するインフラ基盤と接続し，アクセス体制を準備すること
11	ネットワーク・回線	一度構成したネットワークは，後からアドレス空間を拡張したり，ネットワークを付け足したり変更できること。
12	ネットワーク・回線	ＳＮＭＰｖ２／ｖ３，ＳＳＨｖ２，ｆｔｐの利用ができること。
13	ネットワーク・回線	サーバーへのトラフィックの負荷分散ができること。
14	ネットワーク・回線	ラウンドロビン方式及び最小コネクション数方式での負荷分散ができること。
15	ネットワーク・回線	同一通信元からの通信を常に同一サーバーに振り分けができること。
16	ネットワーク・回線	サーバーの死活監視を行い，未応答サーバーを負荷分散の対象外へ処理できること。
17	ネットワーク・回線	負荷分散対象の通信をリクエスト数の制御ができること。
18	ネットワーク・回線	ＨＴＴＰＳにより通信の秘匿化ができること。
19	ネットワーク・回線	秘匿化通信に利用するサーバー証明書の登録・更新ができること。
20	システム運用管理	ログによる状況の確認及び設定変更の管理ができること。
21	システム運用管理	装置状況の通知やログ情報の転送ができること。
22	システム運用管理	コネクションのログを受信及び蓄積し，ログの検索及び閲覧ができること。
23	システム運用管理	設定に基づいてＩＰパケット通信の許可又は遮断ができること。
24	システム運用管理	ＩＰｖ４パケットの経路制御ができること。
25	システム運用管理	ログ情報を他の装置に転送できること。
26	システム運用管理	検知した不正な通信の状況や情報を解析装置にログとして送付ができること。
27	システム運用管理	各装置のリソース状況をモニタリングできること。
28	システム運用管理	リソースの項目に閾値を設定し，閾値を超えた場合，アラート通知すること。
29	システム運用管理	仮想マシンを作成し，必要なリソースを割り当てることができること。
30	システム運用管理	仮想マシンの性能情報が閾値を超過した際にＳＮＭＰトラップで通知できること。
31	セキュリティ	ＳＳＬサーバ証明書の取得に必要な情報を官側に提示し，証明書発行に関する支援を実施すること。
32	セキュリティ	ウイルス対策機能を利用できること。
33	セキュリティ	スケジュール設定による自動更新又は手動更新によって，最新のシグネチャに更新できること。
34	セキュリティ	保護対象装置の資源（システムファイルやデータ）及び可搬記憶媒体に対し，リアルタイム検知，又は自動及び手動での定時スキャンを行い，パターンマッチングによるウイルスの検知ができること。
35	セキュリティ	保護対象装置をチェックした結果や検出した情報を管理サーバーに収集し，表示できること。
36	セキュリティ	悪意のあるプログラムの動作の抑制ができること。
37	セキュリティ	セキュリティベンダーから最新のシグネチャを取得し，最新の状態に更新できること。
38	セキュリティ	ＥＤＲ機能を用いて，マルウェア等の感染，侵入の検出ができること。
39	セキュリティ	ＥＤＲ機能を用いて，感染した端末の隔離ができること。
40	セキュリティ	ＥＤＲ機能を用いて，保護対象の機器のイベント情報を収集し，セキュリティインシデントにつながる振る舞いの検出ができること。
41	セキュリティ	振る舞い検知を含むアンチウイルス製品を提供できること。
42	セキュリティ	セキュリティアラートとセキュリティ状況を管理者アカウントで包括的に確認できること。
43	セキュリティ	ファイアウォールについては設定情報を管理サーバーで一元管理できること。
44	セキュリティ	ファイアウォールについてはＧＵＩを使用した設定変更ができること。
45	セキュリティ	管理サーバーからファイアウォール装置に対して設定を投入できること。
46	セキュリティ	WAF(Web Application Firewall)の機能を利用できること。
47	SOC機能	セキュリティインシデントの検出、分析、対応、報告及び防止を実施すること。
48	SOC機能	防衛関連事業専用のＳＯＣ体制としたサービスであること。
49	SOC機能	法令クリアリングシステムサービスにて使用されるサーバー向けに，各装置のパッチ適用状況の管理ができること。
50	SOC機能	法令クリアリングシステムサービスにて使用されるサーバー向けにネットワーク上のセキュリティ製品（ＦＷ・ＩＰＳ・ＩＤＳ等）の運用ができること。
51	SOC機能	法令クリアリングシステムサービスにて使用されるサーバー向けに，エンドポイントセキュリティ製品（ＥＰＰ・ＥＤＲ）の運用ができること。
52	SOC機能	官側の指示に基づきＳＯＣで収集したログをエンドユーザーに提供できること。
53	SOC機能	法令クリアリングシステムサービスにて使用するサーバ上のソフトウェアの脆弱性情報を取得・管理し，脆弱性を検知できること。
54	SOC機能	攻撃者の脅威情報等については，一般公開されている情報を利活用し，品質の向上に利用すること。なお，本事業で検知した攻撃者等の脅威情報について，再利用や注意喚起のための公開を行う場合は利用者が特定されない形に加工すること。

各種サービスの技術要件詳細

法令クリアリングシステムサービス（部内）要件

項番	項目	要件
1	コンピュート	仮想マシンは現行データの公開情報を管理できること。
2	コンピュート	ＣＰＵのコア数は１サーバあたり８コアを基準として提供し、利用状況に応じて追加できること。
3	コンピュート	メモリサイズは１サーバあたり１０GBを基準として提供し、利用状況に応じて追加できること。
4	コンピュート	サーバのシステム領域とデータ保存領域を併せて、１サーバあたり６７５GB以上のディスクを搭載して提供すること。
5	コンピュート	WEBサーバ機能を有すること。
6	コンピュート	文書検索処理が３件/秒以上実行できること。
7	コンピュート	文書閲覧処理が３件/秒以上実行できること。
8	コンピュート	官側が現在ＧＯＴＳとして保有する法令クリアリングシステムのソフトウェアを非互換改修したアプリケーションが利用できること。
9	ネットワーク・回線	省OA端末から，法令クリアリングシステムへの接続（閲覧，データアップロード用）が可能であること。
10	ネットワーク・回線	一度構成したネットワークは，後からアドレス空間を拡張したり，ネットワークを付け足したり変更できること。
11	ネットワーク・回線	ＳＮＭＰｖ２／ｖ３，ＳＳＨｖ2，ｆｔｐの利用ができること。
12	ネットワーク・回線	サーバーへのトラフィックの負荷分散ができること。
13	ネットワーク・回線	ラウンドロビン方式及び最小コネクション数方式での負荷分散ができること。
14	ネットワーク・回線	同一通信元からの通信を常に同一サーバーに振り分けができること。
15	ネットワーク・回線	サーバーの死活監視を行い，未応答サーバーを負荷分散の対象外へ処理できること。
16	ネットワーク・回線	負荷分散対象の通信に対して，帯域制御ができること。
17	ネットワーク・回線	ＨＴＴＰＳにより通信の秘匿化ができること。
18	ネットワーク・回線	秘匿化通信に利用するサーバー証明書の登録・更新ができること。
19	ネットワーク・回線	暗号化スイートの設定ができること。
20	システム運用管理	ログによる状況の確認及び設定変更の管理ができること。
21	システム運用管理	装置状況の通知やログ情報の転送ができること。
22	システム運用管理	分散の対象となるレコード情報について，ＤＮＳサーバーの代わりに返答ができること。
23	システム運用管理	コネクションのログを受信及び蓄積し，ログの検索及び閲覧ができること。
24	システム運用管理	送信元及び送信先のＩＰアドレス，ポート番号を条件としてフィルタリングルールの作成ができること。
25	システム運用管理	設定に基づいてＩＰパケット通信の許可又は遮断ができること。
26	システム運用管理	ＩＰｖ４パケットの経路制御ができること。
27	システム運用管理	ログ情報を他の装置に転送できること。
28	システム運用管理	検知した不正な通信の状況や情報を解析装置にログとして送付ができること。
29	システム運用管理	各装置のリソース状況をモニタリングできること。
30	システム運用管理	リソースの項目に閾値を設定し，閾値を超えた場合，アラート通知すること。
31	システム運用管理	仮想マシンを作成し，必要なリソースを割り当てることができること。
32	システム運用管理	仮想マシンを他の仮想化ホストサーバーへ無停止で移動できること。
33	システム運用管理	負荷に応じて仮想マシンの配置を無停止で自動的に変更できること。
34	システム運用管理	仮想マシンの性能情報が閾値を超過した際にＳＮＭＰトラップで通知できること。
35	システム運用管理	構成する装置の操作ができること。
36	セキュリティ	ＳＳＬサーバ証明書の取得に必要な情報を官側に提示し，証明書発行に関する支援を実施すること。
37	セキュリティ	ウイルス対策機能を利用できること。
38	セキュリティ	スケジュール設定による自動更新又は手動更新によって，最新のシグネチャに更新できること。
39	セキュリティ	保護対象装置の資源（システムファイルやデータ）及び可搬記憶媒体に対し，リアルタイム検知，又は自動及び手動での定時スキャンを行い，パターンマッチングによるウイルスの検知ができること。
40	セキュリティ	保護対象装置をチェックした結果や検出した情報を管理サーバーに収集し，表示できること。
41	セキュリティ	保護対象装置にエージェントを導入することで，ＩＰアドレス及びプロトコル，ポート番号等による通信制御ができること。
42	セキュリティ	悪意のあるプログラムの動作の抑制ができること。
43	セキュリティ	保護対象装置に対してエージェントをインストール後，管理サーバーから必要なソフトウェア資源の配布ができること。
44	セキュリティ	セキュリティベンダーから最新のシグネチャを取得し，最新の状態に更新できること。
45	セキュリティ	ＥＤＲ機能を用いて，マルウェア等の感染，侵入の検出ができること。
46	セキュリティ	ＥＤＲ機能を用いて，感染した端末の隔離ができること。
47	セキュリティ	ＥＤＲ機能を用いて，保護対象の機器のイベント情報を収集し，セキュリティインシデントにつながる振る舞いの検出ができること。
48	セキュリティ	定期的にアンチウイルス製品の定義ファイルを更新できること。
49	セキュリティ	振る舞い検知を含むアンチウイルス製品を提供できること。
50	セキュリティ	セキュリティアラートとセキュリティ状況を管理者アカウントで包括的に確認できること。
51	セキュリティ	ファイアウォールについては設定情報を管理サーバーで一元管理できること。
52	セキュリティ	ファイアウォールについてはＧＵＩを使用した設定変更ができること。
53	セキュリティ	管理サーバーからファイアウォール装置に対して設定を投入できること。
54	セキュリティ	WAF(Web Application Firewall)の機能を利用できること。
55	データセンター	データセンター及び回線の提供は，災害対策基本法及び武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律において，指定公共機関である事業者であること。
56	データセンター	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ていること。
57	データセンター	事業継続性を確保するため，各データセンターは異なる大陸プレート及び異なる電力会社管内に立地していること。
58	データセンター	情報資産を日本国内に保管できること。
59	データセンター	障害発生時の情報資産の退避先を全て日本国内にできること。
60	データセンター	運用系の情報資産を全て日本国内に保管できること。
61	データセンター	防衛省専用区画として整備できること。
62	データセンター	防衛省専用区画に立入する際は，機器借上事業者等が申請を行い，官側がそれを承認した者のみを立入させる機能を提供可能とし，立入記録の管理ができること。
63	データセンター	建物（設置スペースも含む。）の入館申請管理は，Ｗｅｂ等システムにより実施できること。
64	データセンター	通用門や敷地出入口は，有人警備による確認及びセキュリティシステムを設置できること。
65	データセンター	建物のアクセス管理は，役務員やＩＣカード又は生体認証等による確認を必要とすること。
66	データセンター	設置スペースの設置する区画への立入者を，当該フロアへのアクセス権を有する者に限定できること。
67	データセンター	建物の避難経路に対して，平常時における侵入防止対策を講じることができること。
68	データセンター	敷地出入口，建物及びフロアは，監視カメラの記録及びモニタリングを実施できること。

69	データセンター	敷地及び建物におけるセキュリティシステム及び監視カメラの記録を実施できること。
70	データセンター	本設備に設置された機器等を維持する機器借上事業者について，必要がある際は２４時間連続して滞在できる環境を提供できること。
71	データセンター	データセンターは，セキュリティ管理方法を具体的に定めた文書を整備し，評価と改訂ができること。及びセキュリティ管理体制を整備できること。
72	データセンター	データセンターは，本設備を早期復旧させるための体制を整備し，復旧作業・支援人員の確保等ができること。
73	データセンター	全てのデータセンターはデータセンターファシリティスタンダードの基準において全項目でティア３以上に準拠していること。
74	データセンター	建物構造が震度６強に耐えうる耐震又は免震等の構造を備えていること。
75	データセンター	設置スペースのフリーアクセスは，最大加速度５００ｇａｌ以上に耐えること。ただし，免震構造の場合は，建物もしくは免震装置・床が当該加速度以上に耐えること。
76	データセンター	免震ピットには，「積層ゴム支承」，「直動転がり支承」及び「特殊ダンパー」等の免震装置を複数設置していること。
77	データセンター	ＰＭＬ（Ｐｒｏｂａｂｌｅ　Ｍａｘｉｍｕｍ　Ｌｏｓｓ。地震リスク分析による予想最大損失率）による評価が１０％以下であること。
78	データセンター	地震による内装（間仕切壁，天井，照明器具等）の落下・破損の防止措置を講ずること。
79	データセンター	二重床は，耐震補強とすること。又は，免震構造等により地震の揺れを建物に伝わり難くする措置を講じていること。
80	データセンター	電源設備及び空調設備には耐震措置を講ずること。
81	データセンター	ラックは耐震固定を実施すること。
82	データセンター	地震の際に機器等に影響を与えないよう，機器等及び什器等に対して耐震措置を講ずること。
83	データセンター	データセンターの建物は，建築基準法の耐火建築基準（第２条第９号の２）に規定する耐火性能を有すること。
84	データセンター	設置スペース，電気室，無停電電源装置は防火区画であること。
85	データセンター	消防法に定められた自動火災報知設備を有すること。
86	データセンター	消火設備はオゾン層破壊係数がゼロであるガス系消火設備として，サイレンサーを設置していること。
87	データセンター	設置スペースのあるサーバールームは，外部から内部が見通せない構造とし，防衛省以外のサーバーが設置されない専用の部屋とすること。
88	データセンター	設置スペースの天井高は，フリーアクセス床を除いて２，４００mm以上であること。
89	データセンター	１ラック当たりの供給電力は，６ＫＶＡ以上(実効４ＫＶＡ以上)であること。
90	データセンター	搬入口から設置スペースまで機器が搬入できるルートが確保（貨物用エレベーターを含む。）できること。
91	データセンター	必要に応じて当該区画の拡張ができること。
92	データセンター	データセンター事業者で用意するラックのみ，棚板及びブランクパネルは求めに応じて無償で提供できること。
93	データセンター	ラック及びサーバールームの個別鍵（ＩＣカード含む。）は，データセンター事業者が管理するものとし，官側及び関連する他契約の事業者の入館時に当該鍵を貸与できること。
94	データセンター	設置スペースにおけるセキュリティシステム及び監視カメラの記録とモニタリングの実施ができること。
95	データセンター	設置スペースへの入退室記録（関係者限り）は，官側からの求めに応じ提供できること。
96	データセンター	設置スペース内に官側監視カメラの持ち込み及び設置ができること。
97	データセンター	受電設備は法定点検時も完全無停止であること。
98	データセンター	燃料の備蓄量は，無供給で４８時間以上連続運転ができること。
99	データセンター	非常用発電機の燃料が優先的に供給を受けられる契約を燃料供給会社と締結していること。
100	データセンター	無停電電源設備の停電補償時間は，非常用発電機が安定した電力を供給するまでの間，かつ１０分以上であること。
101	SOC機能	セキュリティインシデントの検出、分析、対応、報告及び防止を実施すること
102	SOC機能	防衛関連事業専用のＳＯＣ体制としたサービスであること。
103	SOC機能	法令クリアリングシステムサービスにて使用されるサーバー向けに，各装置のパッチ適用状況の管理ができること。
104	SOC機能	法令クリアリングシステムサービスにて使用されるサーバー向けにネットワーク上のセキュリティ製品（ＦＷ・ＩＰＳ・ＩＤＳ等）の運用ができること。
105	SOC機能	法令クリアリングシステムサービスにて使用されるサーバー向けに，エンドポイントセキュリティ製品（ＥＰＰ・ＥＤＲ）の運用ができること。
106	SOC機能	官側の指示に基づきＳＯＣで収集したログをエンドユーザーに提供できること。
107	SOC機能	法令クリアリングシステムサービスにて使用するサーバ上のソフトウェアの脆弱性情報を取得・管理をし，脆弱性を検知できること。
108	SOC機能	攻撃者の脅威情報等については，一般公開されている情報を利活用し，品質の向上に利用すること。なお，本事業で検知した攻撃者等の脅威情報について，再利用や注意喚起のための公開を行う場合は利用者が特定されない形に加工すること。

別記様式第１（第２項関係）

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	－
	作　成　部　課	大臣官房文書課法令審査
	作　成　年　月	令和８年１月１４日
品　名	法令クリアリングシステムの運用（Ｒ７換装）	
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

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
ネットワーク構成	ネットワーク構成，配線図	契約の履行の一環として収集、整理、作成等した情報についての適切な管理
インターフェイス（アドレス，プロトコル等）仕様	ＩＰアドレス	
セキュリティ（ファイアーウォール等）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，管理者パスワード	

３　特記事項

なし。