支担官第１８０号

令和７年６月１２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-I-041	情報システムの脆弱性対策支援役務	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1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７年7月１８日（金）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７年６月２５日（水）１２：００までに、下記ア～キに記載する書類等を防衛省大臣官房会計課契約係へ提出すること。

ア　当該入札に係る物品と同等以上の仕様の物品を製造した実績等を証明できる者

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

項　目	基　準	数　値
入札物品等（訓令第１８条第４項に規定する契約の対象となる物品又は役務をいう。以下同じ）に関連する特許保有件数	３件以上	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、
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）この一般競争に参加を希望するものは、適合条件を満たすことを証明する書類を令和７年６月２６日（木）１４：００までに提出しなければならない。

（５）入札に関する条件　仕様書4.1 a)～e)に定める本役務の実施体制並びに仕様書5.1 a)～e) 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６月２６日（木）１４：００。必要に応じ追加資料の提出を求めることがある。）。

（６）本案件は、府省共通の「電子調達システム」（https://www.p-portal.go.jp）を利用した応札及び入開札手続により実施するものとする。ただし、電子調達システムによりがたい者は、「紙」による入札書等の提出も可とするが、郵便入札については、<u>令和７年7月１６日（水）</u>までに、下記担当者必着分を有効とする。

（７）落札者が、１０に掲げる契約条項のほか、中小企業信用保険法第２条第１項に規定する中小企業者である場合は、「債権譲渡制限特約の部分的解除のための特約条項」を別途適用する。

（８）入札案内の交付場所、契約条項を示す場所及び問合せ先

〒162-8801　東京都新宿区市谷本村町５－１　（庁舎A棟10階）※顔写真付の身分証明書を持参すること。

受付時間　９：３０～１８：１５（１２：００～１３：００までの間を除く）

<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すること。</u>

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　河野　電話　03-3268-3111　内線20822

別紙

適合条件

1　条件

応札者は、次の条件を満たしていること。

a)　契約相手方は、委託先を含め、以下の要件を満たす体制を確保し、本役務を実施できる業務実施体制を整えること。

b)　経済産業省が定める「情報セキュリティサービス基準」に適合する企業を記載した「情報セキュリティサービス基準適合サービスリスト」(うちペネトレーションテスト（侵入試験）サービスまたは脆弱性診断サービス）に登録されている事業者を含めること。

c)　業務従事者の資格等

業務従事者の資格等の要件については、以下のとおりとする。

1)　総括責任者

①　過去５年間において、情報システムに係るプロジェクトマネジメント業務の責任者としての経験を有すること。

②　以下のいずれかの資格を有しているか又は資格を有することと同等以上の技術を保持していることが証明できること。

・ＰＭＰ（プロジェクトマネジメント・プロフェッショナル）
・ 情報処理技術者試験（プロジェクトマネージャ）
・ 情報処理安全確保支援士
・ CISSP (Certified Information Systems Security Professional)

2)　侵入試験の業務従事者

(1)　侵入試験責任者

①　中央省庁向けペネトレーションテスト業務または脆弱性診断の経験年数を５年以上有し、かつペネトレーションテストまたは脆弱性診断の責任者としての経験を有すること。

②　以下のいずれかの資格を有しているか、又は資格を有することと同等以上の技術を保持していることが証明できること。

・ 情報処理安全確保支援士
・ CISSP (Certified Information Systems Security Professional)
・ OSCP (Offensive Security Certified Professional)

(2)　侵入試験作業従事者

①　作業従事者２名以上とすること（うち少なくとも１名は、３年以上の中央省庁向けペネトレーションテストまたは脆弱性診断の経験を有すること。)。

②　作業従事者のうち、少なくとも１名以上は、以下のいずれかの資格を有しているか、又は資格を有することと同等以上の技術を保持していることが証明できること。

・ 情報処理安全確保支援士
・ CISSP（Certified Information Systems Security Professional）
・ OSCP（Offensive Security Certified Professional）
・ GIAC Penetration Tester
・ GIAC Exploit Researcher and Advanced Penetration Tester

3） 脆弱性工程管理の業務従事者

（1） 脆弱性工程管理責任者

① 過去３年間において、情報システムに係るプロジェクトマネジメント業務の責任者としての経験を有すること。

② 以下のいずれかの資格を有しているか又は資格を有することと同等以上の技術を保持していることが証明できること。

・PMP（プロジェクトマネジメントプロフェッショナル）
・情報処理技術者試験（プロジェクトマネージャ）

（2） その他の役務員

以下の資格等のうち，いずれかを有する者を１名有すること。

・ 情報処理安全確保支援士
・ CISSP（Certified Information Systems Security Professional）

4） 教育支援の業務従事者

作業従事者のうち、少なくとも１名以上は、以下のいずれかの資格を有しているか、又は資格を有することと同等以上の技術を保持していることが証明できること。

・ 情報処理安全確保支援士
・ CISSP（Certified Information Systems Security Professional）

２ 提出書類の形式等については以下のとおりとする。

a） 書類の形式

形式は任意とし、提出書類には、会社名等を表示するとともに、社印を押印のうえ、上記書類順で綴るものとする。

b） 提出部数

各１部

c） 提出期限

令和７年６月２６日（木） １４：００まで

d） 虚偽がないものとする。

e） 書類提出後、官側から細部補足資料等及び社内監査を求める場合がある。

f） 提出書類に関する問い合わせは、提出期限の前日の１７時１５分までとする。

調達要求番号：

<table>
<tr><td colspan="4">調達仕様書</td></tr>
<tr><td rowspan="4">件　名</td><td rowspan="4">情報システムの脆弱性対策支援役務</td><td>仕様書番号</td><td></td></tr>
<tr><td>変更年月日</td><td>令和　年　月　日</td></tr>
<tr><td>作成年月日</td><td>令和７年５月　日</td></tr>
<tr><td>作成部署</td><td>整備計画局サイバー整備課</td></tr>
</table>

1.　総則

1.1　適用範囲

この仕様書は，情報システムの脆弱性対策支援役務（以下「本役務」という。）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，この仕様書に用いる用語の定義は，ＪＩＳ Ｘ ０００１～ＪＩＳ Ｘ ００３２，ＩＥＥＥ規格，ＩＥＴＦ標準勧告，ＩＴＵ－Ｔ勧告，ＩＳＯ規格，政府情報システムにおける脆弱性診断導入ガイドライン, 情報セキュリティサービス基準によるものとする。

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)　政府情報システムにおける脆弱性診断導入ガイドライン（令和６年１月３１日）
b)　情報セキュリティサービス基準（令和５年３月３０日）
c)　個人情報の保護に関する法律（平成１５年法律第５７号）
d)　著作権法（昭和４５年法律第４８号）
e)　「公用文作成の考え方」の周知について（令和４年１月１１日内閣文第１号）
f)　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。）
g)　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（防装庁（事）第３号３１．１．９）
h)　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（平成３１年１月９日））

1.3.2　関連文書

a)　**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）

1.4　別冊

情報システムの脆弱性対策支援役務**（注意）**

1.5　本仕様書における別冊の参照

a)　本仕様書における**カタカナ**は，情報システムの脆弱性対策支援役務 別冊によるものとする。

b)　情報システムの脆弱性対策支援役務 別冊については，所定の手続きを踏まえた上で防衛省市ヶ谷庁舎６８号館２階において閲覧可能とする。

2.　調達案件の概要

情報システムが抱える各種脆弱性および設定の不備を根底から対策するため、脆弱性・設定不備の発見、原因分析、対策の指導、修正確認及び関係者への教育の一連の活動を実施するものである。

2.1　本業務期間

本業務の実施期間は，契約締結日から令和８年１月３０日（金）までとする。

2.2　事業スケジュール

本役務の事業スケジュールは**図 1** を基準とする。

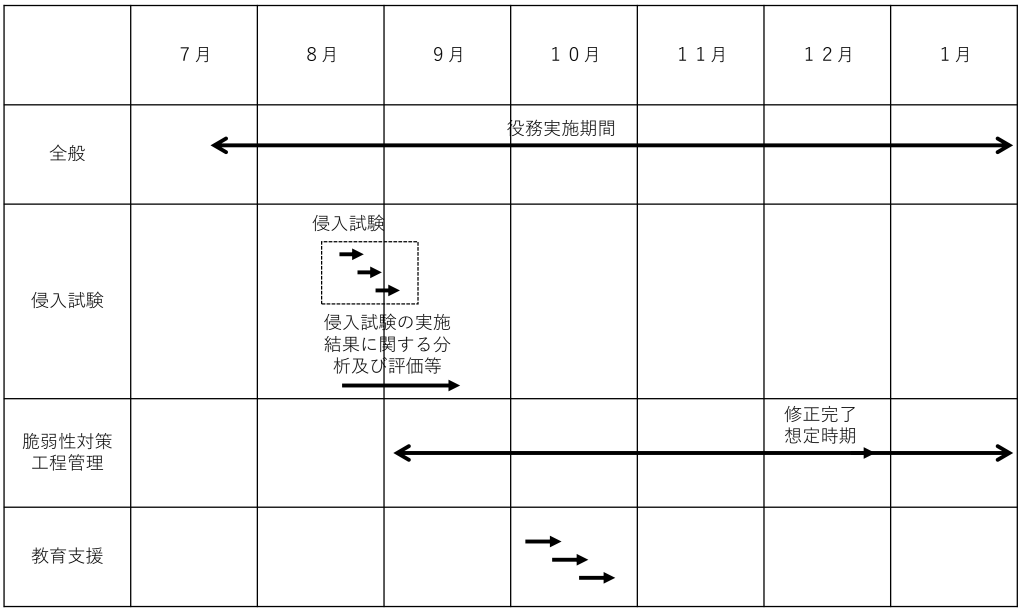

図１　事業スケジュール

2.3　対象システム

本役務の対象とする情報システムの概要は**表 1** を基準とする。

表１　対象システム

<table>
<tr><th>対象システム</th><th>ユーザ数</th><th>概要</th><th>対象ホスト
（ＩＰ数）</th><th>所在地域</th></tr>
<tr><td>研究開発支援システム</td><td>約１３００</td><td rowspan="3">・Active Directoryを中心としたOA環境を提供
・DIIが提供する部外系ネットワークに接続するためのVDI環境をユーザに提供</td><td>２５</td><td>市ヶ谷地区</td></tr>
<tr><td>北関東防衛局OAネットワークシステム</td><td>約６００</td><td>２５</td><td>北関東地区</td></tr>
<tr><td>東北防衛局OAネットワーク・システム</td><td>約６００</td><td>２５</td><td>東北地区</td></tr>
</table>

※ＤＩＩ：防衛情報通信基盤

2.4　役務実施場所

a)　本役務に係る作業場所は，**表２**を基準とすること。

表２　作業場所

役務内容	作業場所
侵入試験	準備にかかる作業場所は契約相手方が用意するものとし、侵入試験本番時の作業実施場所は、各情報システムの所在地を基準とし、官側の指定する場所とする。
脆弱性対策 工程管理	準備にかかる作業場所は契約相手方が用意するものとし、進捗報告会は防衛省市ヶ谷地区からのリモート開催または対面とする。
教育支援	準備にかかる作業場所は契約相手方が用意するものとし、教育本番時の実施場所は防衛省市ヶ谷地区からのリモート開催または対面とする。

3.　役務の内容

3.1　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)　**政府情報システムにおける脆弱性診断導入ガイドライン**を参照し対応することを基準とする。

b)　対象システムの担当者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。

3.2　作業実施計画書の作成

契約相手方は本役務の実施にあたり、以下の内容を含む作業実施計画書を作成し官側の承認を得る事。

a)　作業概要

b)　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，導入業務実施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。

c)　スケジュールに関する事項

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。

3.3　作業実施要領書の作成

契約相手方は本役務の実施にあたり、以下の内容を含む作業実施要領書を作成し官側の承認を得ること。

a)　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および電話番号を記載すること。

b)　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。

c)　工程管理

1)　工程管理に関する体制について，各役割の責任範囲を明確化して記載すること。

2)　管理方法，管理項目，管理手法について記載すること。

3)　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。

4)　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。

d)　品質管理

1)　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。

2) 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。

3) 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。

4) 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。

5) 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。

e) 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。

f) 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。

g) 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

3.4 ペネトレーションテスト（以下「侵入試験」という。）

a) 契約相手方は以下の侵入試験に係る実施内容を2.3項に示す対象システム毎に実施すること。

b) 侵入試験実施計画書の作成

1) 契約相手方は、侵入試験実施計画書、事前説明会資料、ヒアリングシート（テンプレート）及び個別実施計画書（テンプレート）を作成し、官側の承認を得ること。

2) 侵入試験実施計画書には、以下の事項を含むこと。

- 全体スケジュール
- 事前説明会及びヒアリング内容
- 侵入試験方法（使用する機材やツール等の内容を含む。）
- 侵入試験の実施完了条件
- 侵入試験の実施結果に関する分析、評価方法及び評価観点
- 本業務に係る管理者及び作業従事者に関する役割及び氏名を含む体制図
- 管理者及び作業従事者の所属、氏名及び経歴の一覧表

3) 期限

侵入試験実施計画書案は契約締結日からおおむね１週間以内、事前説明会資料案、ヒアリングシート（テンプレート）案及び個別実施計画書（テンプレート）案は契約締結日からおおむね２週間以内に提出し、別途官側の承認を得ること。

3.4.1 侵入試験の全般事項

a) 事前説明会の実施

1) 契約相手方は、対象システムの担当者に対する事前説明会の時期について調整すること。

2) 事前説明会は、原則として対象システムごとに１回開催することとし、リモートでの開催も含め官側又は対象システムの担当者の指定する場所で実施すること。

3) 契約相手方は、事前説明会において、事前説明会資料に基づき、侵入試験日程、調査内容、依頼事項（調査において必要な情報を収集するためのヒアリングシートの記入を含む。）及び調査実施における注意点等について説明すること。ヒアリングシートには、以下の事項を含むこと。

- 対象システムの概要
- システム利用形態
- インターネット接続状況
- インターネット以外の対象システム外ネットワークの接続状況
- OS 及びサーバ用途
- 事前ポートスキャン等や侵入試験の実施時における連絡先及び連絡方法
- Web アプリケーションを監視対象とする侵入防御装置やウェブアプリケーションファイアウォールの有無

b) ヒアリングの実施

1) 契約相手方は、対象システムの情報システム情報保証責任者補助者（以下「対象システムの担当者」という。）に対するヒアリングの時期について調整すること。

2) 契約相手方は、回答されたヒアリングシートに基づき、対面または遠隔での打合せにより、対象システムに係る聴取を対象システムの担当者に対して行うこと。

3) ヒアリングにおける侵入試験対象のホストの選定では、契約相手方のこれまでの経験や知見を活用し、効果的かつ効率的な調査が実施できるよう、必要な資料（例えば、ネットワーク構成図等）の閲覧や確認、助言等を行うこと。

4) 契約相手方は、対象システムにおいて必要となる事前準備及び確認事項（例えば、バックアップの取得や、通信監視を委託している事業者をはじめとする関係先への連絡、調査実施時においてサービス障害等が発生した場合の技術的な対応、必要に応じた復旧支援態勢等）について説明すること。

c) 侵入試験の実施方針

その他の侵入経路、侵入方法を試み侵入試験の実施期間内に可能な限り網羅的な試験を行うこと

3.4.2 個別実施計画書の作成

契約相手方は、対象システムごとに、以下の事項を含めた個別実施計画書を作成すること。

- 侵入試験の概要
- 侵入試験の実施方法（攻撃方法、使用するツール等の内容を含む。）
- 侵入シナリオ
- 侵入試験期間中の作業スケジュール
- 管理者及び侵入試験に従事する作業従事者の役割、所属、氏名の一覧表
- 事前説明会及びヒアリング等で決定した事項のうち、調査実施に当たり共有すべき事項

● 侵入試験の実施における手続きの流れに沿って実施内容の観点を取りまとめた調査観点を作成し、個別実施計画書に含めること。調査観点を**表３**に示す。

表３　侵入試験の実施における調査観点

No.	調査観点		備考
1	システム情報及び脆弱性情報等の収集	・ネットワーク情報の収集 ・システム情報の収集 ・脆弱性情報の収集 ・ユーザ、アカウント情報の収集 ・ファイルサーバの探索 ・認証情報の検索	自動スキャン、ネットワーク診断に加えて手動での情報収集を行う事
2	対象ホストへの侵入可否の調査及び分析	・OS 及びミドルウェアその他のシステム上に内在する脆弱性の調査 ・対象ホストが提供するサービス（意図せず公開しているサービスを含む）の設定不備の調査 ・アクセス制御不備の調査 ・ユーザ、アカウント情報の調査 ・プロダクト固有のデフォルトユーザ情報の調査	
3	侵入可能な攻撃の実行	No.１及び No.２で得られた情報を利用した攻撃の実行	自動的な攻撃に加えて手動での攻撃試行行う事
4	侵入後の活動目的達成	・一般ユーザから管理者への権限昇格の実行 ・侵入に成功したホストと同様の手法で他ホストへの侵入 ・侵入に成功したホストを踏み台にした他ホストへの侵入 ・インターネットアクセスへの試行 ・システム内部の情報獲得	自動的な攻撃に加えて手動での攻撃試行行う事

3.4.3　侵入試験の実施

a) 契約相手方は、承認が得られた個別実施計画書及び以下の事項に基づき侵入試験を実施すること。
b) 侵入試験の実施は３日～４日間実施すること。
c) 侵入試験の時間帯は、原則、平日の午前10時から午後５時30分の間とする。ただし、対象システムの担当者等が上記以外の日時を希望した場合は、官側及び対象システムの担当者と調整の上、体制を整備すること。
d) 侵入試験実施期間の各日の作業開始前及び終了後には、官側及び対象システムの担当者に原則としてメールにて報告すること。ただし、作業場所等の理由によりメールを送信できない

場合には、電話にて報告すること。

e) 作業中は対象システムのサービスを停止させ、又は阻害していないか常に状況を確認すること。

f) 対象システムについて、サービスを停止させ、又は阻害した場合は、直ちに作業を中止し、官側及び対象システムの担当者へ報告すること。具体的な報告基準は、以下のとおり。

- 侵入試験を実施した結果、対象システムの全部又は一部の機能やサービスについて、利用者視点での何らかの影響が発生したことを認識した場合(サービス停止、無応答、性能劣化等)
- 上記に示した事象が軽微なものであっても、当該事象を対象システムの担当者が認識するに至った場合また、サービス復旧の際に協力を求められた場合には、官側及び対象システムの担当者の指示に従うこと。なお、中止した調査の再開については、対象システムの担当者と再開に伴う影響を含め、十分に調整し、サービスへの影響が生じない対策を講じること。

g) 対象システムに侵入できた場合、官側が契約締結後に提示する様式(個別結果一覧)により、検出した問題点を整理し、侵入試験実施期間終了後、５開庁日以内に官側に提出すること。

h) 侵入試験には、官側又は対象システムの担当者が立ち会うことがある。

i) 官側又は対象システムの担当者からの指示又は問合せに速やかに対応できるよう体制を整備すること。

j) 対象システムの拠点で侵入試験を行い、端末の持込み及び接続並びにログ情報の持ち出しに当たって、対象システムの担当者に対して申請書の提出等が必要な場合、官側又は対象システムの担当者の指示に従うこと。

k) プログラム、生成プロセス、生成ファイル及びその他の侵入試験中に対象システムに加えた影響は、残留させないよう適切に処理すること。なお、契約相手方のみで残留物の除去処理が出来ない場合にあっては、侵入試験実施期間終了後直ちに官側及び対象システムの担当者に報告した上で、対象システムに残留物の除去処理を依頼すること。

l) 侵入試験後のヒアリング

1) 契約相手方は侵入試験によって検出された問題点に関連する対象システムの運用手順・方法、使用ツール、運用・管理プロセス、保守手順・方法など運用管理保守に関するヒアリングを対象システムの担当者、管理者、運用事業者、保守事業者に対して行うものとする。

2) ヒアリングに当たっては、侵入試験後ヒアリングシートを作成し事前に官側の承認を得る事。

3.4.4　侵入試験の実施結果に関する分析及び評価等

a) 対象システムごとの個別調査結果報告書兼対応計画書の作成

1) 記載内容

契約相手方は、侵入試験によって検出された問題点及び侵入試験後のヒアリング結果から対象システムのセキュリティ対策の実施状況の分析及び評価を行い、その結果として以下の項目を含めた個別調査結果報告書兼対応計画書及び解説書を作成し、官側の承認を得るこ

と。対応計画書については対象システムの担当者が対応計画を記載できる様式を用意すること。

2) 調査の内容

・ 調査で用いた調査実施手順及び方法並びに侵入シナリオ

・ 対象システムについて調査を実施した範囲

3) 調査結果

・ 検出した問題点の内容及び危険度のレベルの一覧

・ 検出した問題点を再現する方法

・ 検出した問題点及び侵入試験後のヒアリング内容を分析した結果で得られる原因と対策方法。なお、根本的な対策方法が、期間及びコスト等の面から早期の実施が現実的に困難と思われる場合は、暫定的な対策についても併せて示すこと。

4) 問合せ窓口

問合せ対応連絡先（メールアドレス及び電話番号）

3.4.5 個別調査結果報告会の開催

a) 契約相手方は、対象システムごとに、官側及び対象システムの担当者等と調整の上、個別調査結果報告会を開催し、個別調査結果報告書兼対応計画書に基づき実行可能かつ具体的な対策方法について報告すること。

3.5 脆弱性対策工程管理

契約相手方は対象システム毎に作成した個別調査結果報告書兼対応計画書を基に修正のための工程管理を実施すること。

a) 工程管理支援

1) 対象システムの担当者等が作成する、対応計画書及びWBSの妥当性を評価し必要に応じて指摘するとともに対応計画及びWBSを確定させること。

2) 進捗報告会において、成果物及びタスクの状況を確認し、進捗状況を管理すること。

3) 進捗報告会（リモート又は対面で週１回を基準）に参加して進捗を確認し遅延への対応案を検討して対象システムの担当者及び官側に報告を行う事。

4) 進捗報告会の議事録（様式適宜）を作成し開催後３日を基準に対象システムの担当者等及び官側に提出すること。

b) 技術的支援

1) 根本的対策、緩和策、適切な運用方法について助言を行い、それが確実に実施されるように対象システムの担当者等を指導する事、運用上の理由及びその他の理由から実施できない場合はその理由の妥当性について評価し対象システムの担当者及び官側に報告を行うこと。

2) 対象システムの担当者が計画する対応方法・手順などの妥当性について確認し必要に応じて指摘すること。

3) 対象システムの担当者が検出された問題点を確認できる方法及び修正を確認できる方法を提供すること。

4) 管理者アカウントの管理に必要なツールとしてパスワードマネージャーを各システムに提

供し本役務終了後も使用可能とすること。

なお、提供機能、提供方法については官と協議のうえ決定すること。

3.6　教育支援

a)　契約相手方は対象システムの情報システム情報保証責任者及び情報システム情報保証責任者補助者向けの教育を実施すること。

b)　教育にあたり**3.4.4項**の分析、評価結果から運用上の推奨事項、効率的なセキュリティ対策、現状構成で実施可能な対策方法を案出して教育資料に反映させること。

c)　教育の実施形式

1)　対面開催（各情報システム毎１回）

2)　省内ポータルサイトでの教育資料、教育用動画、確認テストの公開

d)　作成資料

1)　教育スライド（対面開催、資料提供用）

2)　教育用動画資料

3)　確認テスト

e)　教育内容

侵入試験結果を参考に**表４**の内容を含めて必要な項目を官側と調整のうえ選定するものとし、運用役務事業者、保守事業者を監督及び指導をする立場として知っておくべき内容とチェック方法について教育内容を構成すること。

表４　教育内容

設定上の改善事項	具体的方策	NIST SP800 における対策
認証情報（ID、パスワード）が記載されたファイルの保護	認証情報（ID、パスワード）が記載されたファイルを保管する場合はパスワードを設定する。	・SC-13 暗号化保護 ・SC-28 情報の暗号化保護
強度の低いパスワードの改善	桁数が短い、キーボードの配列の利用、簡単な文字列の利用及び ID とパスワードが同じなどの脆弱なパスワードは設定しないものとする。	・IA-5 認証情報管理 ・IA-2 認証 ・IA-2 認証
パスワードの使いまわし	管理者パスワードやネットワーク機器の管理パスワードを同じものを設定しない。	・IA-5 認証情報管理
DNS ゾーン転送の制限	DNS サーバの DNS ゾーン転送を許可しない設定にする。	・SC-20 DNS セキュリティ ・AC-4 情報フロー強制
SSH の認証方式の改善	SSH でリモートでアクセスする際の認証方式を多要素認証や、クライアント証明書を必須とする。	・IA-2 認証 ・IA-5 認証情報管理 ・SC-13 暗号化保護
適切なアクセス制御の導入	管理者しかアクセスしないネットワーク機器やサーバへのアクセスを制御する	・AC-3 アクセス強制 ・AC-6 権限分離 ・AC-17 リモートアクセス

表４　教育内容（続き）

設定上の改善事項	具体的方策	NIST SP800 における対策
証明書サーバの設定修正	・Active Directory 証明書サービスにおいて Web Enrollment Role サービスを停止またはアクセスできる端末を限定する ・Active Directory 証明書サービスエンタープライズ認証局（Certificate Authority ：CA）で、脆弱な設定の証明書テンプレートを利用しない	・AC-17 リモートアクセス ・SC-7 境界防護 ・CM-7 最小機能
SPN アカウントの適正な管理	サービスプリンシパル名に関連したドメイン管理者アカウントの適正な管理。	・AC-2 アカウント管理 ・AC-5 権限の分離 ・AC-6 最小特権 ・AC-17 リモートアクセス
古いバージョンのプロトコル使用	例：古いバージョンの SNNP のバージョンを利用しない。	・CM-7 最小機能 ・SC-12 暗号化保 ・CA-7 継続的モニタリング
不要な機能の停止	デフォルトで起動している使用しないアプリケーション・サービスなどを停止する。	・CM-7 最小機能 ・CM-6 設定変更管理 ・SA-14 システムおよび通信保護
脆弱なアプリケーション・サービスのアップデート	使用しているアプリケーション・サービスのバージョンを管理して必要に応じてアップデートを実施する。	・CM-3 構成変更管理 ・CM-5 構成の検証 ・CM-8 情報システムコンポーネントの管理 ・SI-2 ソフトウェア、ファームウェア、情報のアップデート
SCAP の効果的な活用	SCAP の必要性、SCAP の要素、SCAP の活用プロセス、結果レポートの読み解き	全般

4.　本役務の実施体制

4.1　作業実施体制

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，業務実施責任者については，本役務の成功（予定どおりの稼働，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)　本役務に関して統括を行う責任者（以下「統括責任者」という。）を配置し、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。

b)　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。

c)　業務従事者が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)　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。

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

4.2　契約相手方及び要員等に求める資格等の要件

契約相手方は、委託先を含め、以下の要件を満たす体制を確保し、本役務を実施できる業務実施体制を整えること。

a)　経済産業省が定める「**情報セキュリティサービス基準**」に適合する企業を記載した「情報セキュリティサービス基準適合サービスリスト」（うちペネトレーションテスト（侵入試験）サービスまたは脆弱性診断サービス）に登録されている事業者を含めること。

b)　業務従事者の資格等

業務従事者の資格等の要件については、以下のとおりとする。

1)　総括責任者

①　過去５年間において、情報システムに係るプロジェクトマネジメント業務の責任者としての経験を有すること。

②　以下のいずれかの資格を有しているか又は資格を有することと同等以上の技術を保持していることが証明できること。

・ＰＭＰ（プロジェクトマネジメント・プロフェッショナル）

・　情報処理技術者試験（プロジェクトマネージャ）

・　情報処理安全確保支援士

・　CISSP（Certified Information Systems Security Professional）

2)　侵入試験の業務従事者

(1)　侵入試験責任者

①　中央省庁向けペネトレーションテスト業務または脆弱性診断の経験年数を５年以上有し、かつペネトレーションテストまたは脆弱性診断の責任者としての経験を有すること。

②以下のいずれかの資格を有しているか、又は資格を有することと同等以上の技術を保持していることが証明できること。

・ 情報処理安全確保支援士
・ CISSP（Certified Information Systems Security Professional）
・ OSCP（Offensive Security Certified Professional）

(2) 侵入試験作業従事者

① 作業従事者２名以上とすること（うち少なくとも１名は、３年以上の中央省庁向けペネトレーションテストまたは脆弱性診断の経験を有すること。）。

② 作業従事者のうち、少なくとも１名以上は、以下のいずれかの資格を有しているか、又は資格を有することと同等以上の技術を保持していることが証明できること。

・ 情報処理安全確保支援士
・ CISSP（Certified Information Systems Security Professional）
・ OSCP（Offensive Security Certified Professional）
・ GIAC Penetration Tester
・ GIAC Exploit Researcher and Advanced Penetration Tester

3) 脆弱性対策工程管理の業務従事者

(1) 脆弱性対策工程管理責任者

① 過去３年間において、情報システムに係るプロジェクトマネジメント業務の責任者としての経験を有すること。

② 以下のいずれかの資格を有しているか又は資格を有することと同等以上の技術を保持していることが証明できること。

・PMP（プロジェクトマネジメントプロフェッショナル）
・情報処理技術者試験（プロジェクトマネージャ）

(2) その他の役務員

以下の資格等のうち，いずれかを有する者を１名有すること。

・ 情報処理安全確保支援士
・ CISSP（Certified Information Systems Security Professional）

4) 教育支援の業務従事者

作業従事者のうち、少なくとも１名以上は、以下のいずれかの資格を有しているか、又は資格を有することと同等以上の技術を保持していることが証明できること。

・ 情報処理安全確保支援士
・ CISSP（Certified Information Systems Security Professional）

4.3 提出文書の範囲，提出期限等

4.3.1 提出文書

表５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，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５　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 役務員変更があった場合その都度速やかに
４	侵入試験実施計画書	電子媒体：１部	契約締結後２週間以内
５	事前説明会資料	電子媒体：１部	契約締結後２週間以内
６	ヒアリングシート（テンプレート）及び個別実施計画書（テンプレート）	電子媒体：１部	契約締結後２週間以内
７	個別実施計画書	電子媒体：１部	ヒアリングシート提供後２週間以内
８	個別調査結果報告書兼対応計画書	電子媒体：１部	侵入試験後５週間以内
９	解説書	電子媒体：１部	侵入試験後５週間以内
１０	情報システム情報保証責任者・補助者教育資料	電子媒体：１部	侵入試験後１０週間以内
１１	教育用動画資料	電子媒体：１部	侵入試験後１０週間以内
１２	確認テスト	電子媒体：１部	侵入試験後１０週間以内
１３	議事録	電子媒体：１部	開催から３営業日以内

4.3.2　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) 提出文書は電磁的記録媒体（ＣD-Ｒ又はＤＶＤ－Ｒ等）により作成し，**表５**に示す提出部数を提出すること。また，電磁的記録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) 電磁的記録媒体による提出について，一太郎Ｇｏｖｅｒｍｅｎｔ４，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。

4.3.3 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リスクマネジメント班

5. 個人情報保護及び秘密保全等

5.1 情報の保全

契約相手方は，本役務の契約の履行に当たっては，次の事項について遵守すること。

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，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）における別紙「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。なお，細部については，**表６**のとおりとする。

表６　保護情報

別冊$\boxed{ア}$のとおりとする。

b) 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

c) 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
d) 官が書面により個別に許可し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
e) 契約相手方は，本役務の契約の履行に必要な場合を除き，端末類から部外に対して電子メールを送信してはならない。

5.2 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) b)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。

5.3 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。

g) 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。

h) 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。

i) 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。

j) 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，保護すべき情報を適切に管理するものとする。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，$\boxed{\text{ア}}$に示す保護すべき情報を適切に管理するものとする。

6.　提出書類の取扱い

6.1　知的財産権の帰属

6.1.1　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。

6.1.2 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。

7. 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5. 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。

8.　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。

9.　官側の支援

9.1　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

9.2　国有財産の使用制限

a)　契約相手方は，**9.1** 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。

10.　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)　引用文書及び関連文書を閲覧する必要が生じた場合は，官側と協議すること。
c)　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。
d)　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。
e)　**4.3.1** 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。