

装装保第14846号
令和7年7月31日
一部改正 装装保第25375号
令和7年12月26日
一部改正 装装保第7016号
令和8年3月31日
一部改正 装装保第16671号
令和8年8月6日

長官官房総務官
長官官房人事官
長官官房会計官
長官官房監察監査・評価官
長官官房各装備開発官 殿
長官官房艦船設計官
各部 長
施設等機関の長
各地方防衛局長

防衛装備庁装備政策部長
(公印省略)

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)

標記について、別紙第1から別紙第7までのとおり定めたので通知する。

添付書類：別紙第1～別紙第7

写送付先：陸上幕僚監部指揮通信システム・情報部長、陸上幕僚監部装備計画部長、海上幕僚監部指揮通信情報部長、海上幕僚監部装備計画部長、航空幕僚監部運用支援・情報部長、航空幕僚監部装備計画部長

防衛事業適合事業者制度等に関する訓令の実施要領

第 1 趣旨

この要領は、防衛事業適合事業者制度等に関する訓令（令和 7 年防衛装備庁訓令第 19 号。以下「訓令」という。）第 19 条の規定に基づき、防衛事業適合事業者制度等の実施に関し必要な事項を定めるものとする。

第 2 用語の定義

この要領において用いる用語の意義は、訓令に定めるもののほか、次の各号に定めるところによる。

- (1) 地方防衛局調達部長等 北海道防衛局調達部長、北関東防衛局装備部長、南関東防衛局調達部長、近畿中部防衛局調達部長、中国四国防衛局調達部長、沖縄防衛局調達部長、東海防衛支局長、長崎防衛支局長、東北防衛局郡山防衛事務所長、北関東防衛局宇都宮防衛事務所長、近畿中部防衛局舞鶴防衛事務所長、近畿中部防衛局東海防衛支局岐阜防衛事務所長及び中国四国防衛局玉野防衛事務所長をいう。
- (2) 契約担当官等 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 2 条に規定する契約担当官等をいう。
- (3) 物別官室長等 防衛装備庁における契約事務に関する訓令（平成 27 年防衛装備庁訓令第 34 号）第 2 条第 3 号に規定する物別官室長、長官官房会計官付経理室長及び防衛装備庁の施設等機関の契約担当官等をいう。
- (4) 秘密取扱原因契約 防衛事業適合事業者契約とは別の防衛装備庁と防衛事業適合事業者との間の装備品等の調達又は役務の履行に関する個別の契約であって、当該防衛事業適合事業者が秘密を取り扱う直接の原因となる契約をいう。
- (5) 保護情報取扱原因契約 防衛事業適合事業者契約とは別の防衛装備庁と防衛事業適合事業者との間の装備品等の調達又は役務の履行に関する個別の契約であって、当該防衛事業適合事業者が保護すべき情報を取り扱う直接の原因となる契約をいう。
- (6) 秘密保全対策ガイドライン 装備品等の調達に係る秘密等の保全又は保護の確保について（防経装第 19072 号。26. 12. 24）別添の装備品等の調達に係る秘密保全対策ガイドラインをいう。

第 3 情報保全基準

訓令第 2 条第 6 号に規定する秘密保全基準及び同条第 8 号に規定する保護すべき情報に係る保全基準は、次の各号に掲げる区分に応じ、当該各

号に定めるとおりとする。

- (1) 秘密保全基準 付紙様式第 1－1 から付紙様式第 1－5 までの保全基準兼点検票の項目の欄に掲げる基準（ただし、訓令第 6 条第 1 項の規定に基づく審査においては、付紙様式第 1－1 から付紙様式第 1－4 までの保全基準兼点検票の項目の欄に掲げる基準をいう。）
- (2) 保護すべき情報に係る保全基準 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。以下「情報セキュリティ確保通達」という。）別紙に定める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

第 4 公示の要領

- 1 訓令第 4 条に規定する公示は、防衛装備庁ホームページへ掲載することにより実施するものとし、当該公示に関する事務は、装備政策部装備保全管理課長（以下「装備保全管理課長」という。）が行うものとする。
- 2 訓令第 4 条第 6 号に規定する装備政策部長が必要があると認めた事項は、認証事業者（公示を希望する事業者に限る。）の一覧とする。

第 5 認証の申請及び審査

- 1 装備保全管理課長は、認証を申請する事業者（以下「認証申請事業者」という。）に対し、訓令第 5 条第 1 項に規定する認証申請書等として、付紙様式第 2 の秘密保全体制認証申請書並びに付紙様式第 1－1 から付紙様式第 1－4 までの保全基準兼点検票及び関係書類（事業者の情報保全体制を満たしていることを証明するための書類をいう。以下同じ。）を、地方防衛局調達部長等を経て提出させるものとする。
- 2 装備保全管理課長は、認証申請事業者が防衛事業適合事業者である場合は、前項の認証申請書等として、付紙様式第 2 の秘密保全体制認証申請書のみを、地方防衛局調達部長等を経て提出させるものとする。この場合において、訓令第 6 条第 2 項の規定による現地調査等は、これを省略することができるものとする。
- 3 装備保全管理課長は、認証申請事業者が、併せて秘密の取扱いを前提とする防衛事業適合事業者契約の申込みをする場合は、訓令第 12 条第 1 項に規定する契約申込書等及び前項に規定する認証申請書等を、地方防衛局調達部長等を経て提出させるものとする。この場合において、前項後段の規定を適用するものとする。
- 4 地方防衛局調達部長等は、事業者から前 3 項に規定する書類の提出を受けたときは、当該書類が充足していること及びその内容を確認の上、防衛装備庁長官（装備保全管理課長気付）に進達するものとする。この際、地方防衛局調達部長等は、提出書類のうち付紙様式第 1－1 から付紙様式第

1－4までの内容を精査するものとする。

- 5 装備保全管理課長は、訓令第6条第3項の規定に基づき、付紙様式第3の審査結果の通知又は認証をする場合は、当該審査結果の通知に代えて付紙様式第4の認証通知書を、認証申請事業者に交付するものとする。

第6 認証証明書又は認証マーク

- 1 装備保全管理課長は、認証事業者に対し、訓令第7条第1項に規定する認証証明書として、付紙様式第5による証明書を交付するものとする。
- 2 認証証明書の認証番号の表記は、次の例によるものとし、〔事業者番号〕は、事業者又は事業所ごとに割り振られた番号を、〔延長回数〕は認証の延長回数（認証初回は0）を、それぞれ付すものとする。
認証証明書の認証番号：〔事業者番号〕－〔延長回数〕号
- 3 認証証明書の事業者名の表記は、事業者の希望により事業所名を表すことができるものとする。
- 4 装備保全管理課長は、訓令第7条第1項の規定に基づき、認証証明書を認証事業者に交付する場合において、認証盾を併せて交付することができるものとする。
- 5 訓令第7条第2項に規定する認証マークは、付紙様式第6によるものとする。

第7 認証後の継続的確認

- 1 装備保全管理課長は、訓令第8条第1項の規定に基づき、認証事業者の秘密保全体制が引き続き秘密保全基準を満たしている状態を維持していることを継続的に確認するものとする。この場合において、当該認証事業者を管轄する地方防衛局調達部長等は、当該事業者と調整の上、認証の日から1年ごとに、当該事業者から付紙様式第7の自己点検申告書及び付紙様式第1－1から付紙様式第1－4までの保全基準兼点検票を提出させるものとする。
- 2 前項の書類の提出を受けた地方防衛局調達部長等は、当該書類が充足していること及びその内容を確認の上、装備保全管理課長に進達するとともに、別に定める検査要領により保全検査を行うものとする。
- 3 認証事業者が防衛事業適合事業者である場合の第1項の自己点検申告書等の提出及び前項の保全検査は、これを省略することができるものとする。

第8 認証の取消し

装備保全管理課長は、訓令第9条第1項又は第2項の規定に基づき認証を取り消した場合は、同条第3項の規定に基づき、認証を取り消された

事業者に対し、付紙様式第 8 による認証取消通知書を交付するものとする。

第 9 認証に係る秘密保全体制の変更又は認証の有効期間の延長

- 1 装備保全管理課長は、認証を受けた秘密保全体制の変更を希望する認証事業者に対し、訓令第 10 条第 1 項に規定する申請の書類として、付紙様式第 9 の申請書及び関係書類を、地方防衛局調達部長等を経て提出させるものとする。
- 2 訓令第 10 条第 2 項に規定する秘密保全基準の要件に影響しないことが明らかなものとは、次のアからオまでに掲げる事項とする。
 - ア 事業者名又は事務所等の名称の変更（当該事業者の資本関係に影響のない場合に限る。）
 - イ 本社の所在地の変更
 - ウ 所在地の名称の変更
 - エ 業務の適正化を図るものであって保全水準を低下させることのない秘密保全規則の変更
 - オ その他装備保全管理課長と協議の結果、保全上の影響が生じないと判断された変更
- 3 装備保全管理課長は、認証の有効期間の延長を希望する認証事業者に対し、訓令第 11 条第 2 項又は第 3 項に規定する申請の書類として、付紙様式第 10 の申請書並びに付紙様式第 1－1 から付紙様式第 1－4 までの保全基準兼点検票及び関係書類を、地方防衛局調達部長等を経て提出させるものとする。
- 4 装備保全管理課長は、認証事業者が防衛事業適合事業者である場合は、前項の申請の書類として、付紙様式第 10 の申請書を、地方防衛局調達部長等を経て提出させるものとする。この場合において、訓令第 11 条第 2 項又は第 3 項の規定により準用することとなる訓令第 6 条第 2 項の規定による現地調査等は、これを省略することができるものとする。
- 5 地方防衛局調達部長等は、前各項に規定する書類の提出を受けたときは、第 5 第 4 項の規定に準じて内容を精査するものとする。

第 10 防衛事業適合事業者契約の申込み及び審査

- 1 訓令第 3 条第 1 項第 2 号に規定する別に定める条件は、次の各号に掲げる取り扱う情報の区分に応じ、当該各号に定める情報保全体制とする。
 - (1) 秘密 保全組織、秘密保全規則、教育の体制その他参画を希望する事業の秘密の取扱いの態様に合致した秘密保全体制を整備していること。
 - (2) 保護すべき情報 直近の情報セキュリティ実地監査の結果が良好であること（当該情報セキュリティ実地監査の結果、指摘事項がある場合は

当該指摘事項が是正され、又は改善がなされた場合に限る。）。

- 2 装備保全管理課長は、秘密の取扱いを前提とする防衛事業適合事業者契約の申込みをする事業者に対し、訓令第12条第1項に規定する契約申込書等として、付紙様式第11-1の防衛事業適合事業者契約申込書並びに付紙様式第1-1から付紙様式第1-5までの保全基準兼点検票及び関係書類を、地方防衛局調達部長等を経て提出させるものとする。
- 3 装備保全管理課長は、防衛事業適合事業者契約の申込みをする事業者が認証事業者である場合は、前項の契約申込書等として、付紙様式第11-1の防衛事業適合事業者契約申込書並びに付紙様式第1-5の保全基準兼点検票及び秘密取扱情報システムの体制に係る関係書類を、地方防衛局調達部長等を経て提出させるものとする。この場合において、訓令第13条第2項の規定による現地調査等は、訓令第6条第2項の規定による現地調査等又は第8条第2項の規定による保全検査（指摘事項のない場合に限る。）から3か月を経過していないときは、これを省略することができるものとする。
- 4 装備保全管理課長は、保護すべき情報の取扱いを前提とする防衛事業適合事業者契約の申込みをする事業者が、第1項第2号の条件を満たしている場合は、訓令第12条第1項の契約申込書等として、付紙様式第11-2の防衛事業適合事業者契約申込書のほか、次の各号に掲げる書類を提出させるものとする。この場合において、提出書類に疑義のないときは、訓令第13条第2項の規定による現地調査等は、これを省略することができるものとする。
 - (1) 情報セキュリティ基本方針、規則及び実施手順並びにこれらの書類に係る防衛省からの確認通知の写し
 - (2) システムセキュリティ実装計画及びシステムセキュリティ実装計画に係る防衛省からの確認通知の写し
 - (3) 直近の情報セキュリティ実地監査の結果通知の写し（指摘事項がある場合は、是正措置及び改善状況を証する書類）
- 5 地方防衛局調達部長等は、事業者から前3項に規定する書類の提出を受けたときは、当該書類が充足していること及びその内容を確認の上、防衛装備庁長官（装備保全管理課長気付）に進達するものとする。この際、地方防衛局調達部長等は、提出書類のうち付紙様式第1-1から付紙様式第1-5までの内容を精査するものとする。
- 6 装備保全管理課長は、第2項から第4項までの規定による提出書類及び訓令第13条第2項の規定による地方防衛局調達部長等による現地調査等の結果を踏まえ、情報保全基準への適合性を判断するものとする。
- 7 装備保全管理課長は、訓令第13条第3項の規定に基づき、付紙様式第12の審査結果を、防衛事業適合事業者契約の申込みをした事業者に通知

するものとする。

第 1 1 防衛事業適合事業者契約の締結

- 1 装備保全管理課長は、第 1 0 の審査の結果、適合性を有すると判断された事業者と、訓令第 1 3 条第 3 項に規定する防衛事業適合事業者契約の締結に係る手続を行うものとする。
- 2 前項の場合において、適合性を有すると判断された事業者は、次の各号に掲げる取り扱う情報の区分に応じた契約条項を基準にした防衛事業適合事業者契約を装備保全管理課長と締結するものとし、当該契約が有効である間、当該契約及び次項各号の契約と合わせて、秘密又は保護すべき情報を取り扱うことができる。
 - (1) 秘密 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（装装保第 1 4 8 4 6 号。令和 7 年 7 月 3 1 日。以下「実施要領」という。）別紙第 2 の防衛事業適合事業者契約条項
 - (2) 保護すべき情報 実施要領別紙第 4 の防衛事業適合事業者における保護すべき情報の情報セキュリティの確保に係る契約条項
- 3 契約担当官等は、防衛事業適合事業者契約の下で、秘密取扱原因契約又は保護情報取扱原因契約を締結するときは、次の各号に掲げる契約の区分に応じ、当該各号に定める特約条項を付すものとする。
 - (1) 秘密取扱原因契約 実施要領別紙第 3 の防衛事業適合事業者の秘密の保護に関する特約条項
 - (2) 保護情報取扱原因契約 実施要領別紙第 5 の防衛事業適合事業者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
- 4 前 2 項に規定する契約条項及び特約条項は、防衛事業適合事業者契約の締結に当たり、その基準となる事項を示したものであり、事業者の状況等を踏まえて、当該基準の趣旨を逸脱しない範囲において条項を変更することができるものとする。
- 5 防衛事業適合事業者契約の契約番号の表記は、次の例によるものとし、
〔事業者番号〕は、事業者又は事業所ごとに割り振られた番号を、〔情報取扱区分〕は、契約相手方が取り扱うこととしている情報ごと及び取扱い方法ごとに割り振られた番号を、それぞれ付すものとする。
防衛事業適合事業者契約の契約番号：D C F－〔事業者番号〕－〔情報取扱区分〕－一連番号
- 6 装備保全管理課長は、訓令第 1 3 条第 3 項の規定による契約の締結、訓令第 1 6 条第 1 項の規定による契約の変更及び訓令第 1 7 条第 2 項又は第 3 項の規定による契約の延長をした場合は、その旨を物別官室長等と適宜情報を共有するものとする。

第 1 2 契約後の継続的確認

- 1 装備保全管理課長は、訓令第 1 4 条第 1 項の規定に基づき、防衛事業適合事業者の情報保全体制が引き続き情報保全基準を満たしている状態を維持していることを継続的に確認するものとする。この場合において、当該防衛事業適合事業者を管轄する地方防衛局調達部長等は、当該事業者と調整の上、次の各号に掲げる書類について、当該各号に定める期間に応じ、提出させるものとする。

- (1) 秘密を取り扱う防衛事業適合事業者

- ア 付紙様式第 7 の自己点検申告書及び付紙様式第 1 3 の自己点検票
(月次) 次項の表の起算月から毎月

- イ 付紙様式第 7 の自己点検申告書及び付紙様式第 1 - 1 から付紙様式第 1 - 5 までの保全基準兼点検票並びにリスク査定関係書類 次項の表の起算月から 1 年ごと

- (2) 保護すべき情報を取り扱う防衛事業適合事業者

- 別に定める情報セキュリティ対策実施点検書 契約の日の属する月から 6 か月ごと (基準)

- 2 前項第 1 号の関係書類の提出期間の起算は、次の表の防衛事業適合事業者契約の締結日の属する期間に対応した月から起算するものとする。

防衛事業適合事業者契約の締結日の属する期間	関係書類の提出期間の起算月
4 月 1 日～ 6 月 3 0 日	7 月
7 月 1 日～ 9 月 3 0 日	1 0 月
1 0 月 1 日～ 1 2 月 3 1 日	1 月
1 月 1 日～ 3 月 3 1 日	4 月

- 3 第 1 項第 1 号ア及びイの書類の提出を受けた地方防衛局調達部長等は、秘密を取り扱う防衛事業適合事業者に対し、別に定める検査要領により保全検査を行うものとする。
- 4 第 1 項第 2 号の書類の提出を受けた地方防衛局調達部長等は、保護すべき情報を取り扱う防衛事業適合事業者に対し、別に定める検査要領により、必要に応じて情報セキュリティ実地監査を行うものとする。

第 1 3 契約の解除

装備保全管理課長は、訓令第 1 5 条の規定に基づく契約の解除を行う場合は、事前に契約担当官等と協議を行うものとし、協議の結果、契約を解除することとなった場合は、付紙様式第 1 4 の契約解除通知書を、契

約相手方に送付するものとする。

第 1 4 情報保全体制の変更又は契約期間の延長

- 1 装備保全管理課長は、情報保全体制の変更を希望する防衛事業適合事業者に対し、訓令第 1 6 条第 1 項の申請の書類として、付紙様式第 9 の申請書及び関係書類を、地方防衛局調達部長等を経て提出させるものとする。
- 2 前項の場合において、防衛事業適合事業者が秘密取扱情報システムを変更する場合は、変更後の秘密取扱情報システムのセキュリティ実装計画を、地方防衛局調達部長等を経て提出させるものとする。
- 3 訓令第 1 6 条第 2 項に規定する情報保全基準の要件に影響しないことが明らかなものとは、秘密の取扱いに関する変更については、第 9 第 2 項に掲げる変更事項とし、保護すべき情報の取扱いに関する変更については、これに準じた変更事項とする。
- 4 装備保全管理課長は、防衛事業適合事業者契約の契約期間の延長を希望する防衛事業適合事業者に対し、訓令第 1 7 条第 2 項又は第 3 項の申請の書類として、付紙様式第 1 0 の申請書並びに付紙様式第 1 - 1 から付紙様式第 1 - 5 までの保全基準兼点検票（秘密を取り扱う防衛事業適合事業者に限る。）及び関係書類を、地方防衛局調達部長等を経て提出させるものとする。

第 1 5 秘密保全施設等の管理及び運用

- 1 装備保全管理課長は、防衛事業適合事業者の秘密保全施設等の管理及び運用に関し、当該事業者が次の各号に掲げる事項を行う場合は、当該事業者に対し、別に定める事項を記載した申請を、地方防衛局調達部長等を経て提出させるものとする。
 - (1) 携帯型情報通信又は記録機器の持込み
 - (2) 情報システムの持込み又は設置
- 2 地方防衛局調達部長等は、防衛事業適合事業者から前項に規定する書類の提出を受けたときは、当該書類が充足していること及びその内容を確認の上、装備保全管理課長に送付するものとする。この際、地方防衛局調達部長等は、提出書類の内容を精査するものとする。
- 3 装備保全管理課長は、審査の結果を防衛事業適合事業者に通知するものとする。
- 4 装備保全管理課長は、防衛事業適合事業者が閉鎖区域の構築、設定、変更又は解除を行う場合は、当該事業者に対し、地方防衛局調達部長等を経て申請又は届出をさせるものとする。

第 1 6 装備政策部長の委任を受けた者

訓令第13条第3項、第15条、第16条第1項及び第17条第2項に規定する委任を受けた者は、装備保全管理課長とする。

第17 認証事業者及び秘密を取り扱う防衛事業適合事業者に係る周知要領
装備保全管理課長は、次の各号に掲げる事項について、必要の都度、関係する事業者にも周知するものとする。

- (1) 認証事業者である事実については、公表可能であること。
- (2) 認証の具体的な有効期間、認証を受けた秘密保全施設の使用状況等、現に秘密を取り扱っていることが推測できる内容の公表は控えること。
- (3) 防衛事業適合事業者である事実については、秘密を取り扱う契約を履行中であることが推測できるため、公表を控えること。
- (4) 防衛事業適合事業者が認証事業者である場合は、認証事業者である事実のみ公表可能であること。

第18 認証事業者及び防衛事業適合事業者に係る記録

- 1 装備保全管理課長は、認証及び防衛事業適合事業者契約の締結の状況について、付紙様式第15の認証・防衛事業適合事業者契約整理簿に記録するものとする。
- 2 装備保全管理課長は、前項の認証・防衛事業適合事業者契約整理簿の写しを四半期ごとに、調達管理部調達企画課長及び物別官室長等に提供するものとする。

第19 事業者の教育体制

- 1 装備保全管理課長は、実施要領別紙第6付紙第1の基準2又は基準3に基づき、事業者から教育体制を整備又は維持するために必要な研修に係る申込みを受けた場合は、当該事業者に対して研修を行うものとする。この場合において、当該事業者が認証事業者である場合は、実施要領別紙第6付紙第1中「防衛事業適合事業者」とあるのは「認証事業者」と、「定期的な点検、秘密取扱情報システム」とあるのは「定期的な点検」と、「防衛事業適合事業者契約の申込みをした日から事業者として秘密を取り扱うまで」とあるのは「認証の日から6か月を経過する日まで」と、「秘密取扱情報システム管理者、秘密取扱情報システム担当者、アカウント管理者その他秘密保全組織」とあるのは「その他秘密保全組織」とそれぞれ読み替えて適用するものとする。
- 2 前項の場合において、装備保全管理課長は、事業者に対し、四半期に1回を基準として、次の各号の研修を開催するものとする。
 - (1) 実施要領別紙第6付紙第1の基準2による研修
 - (2) 実施要領別紙第6付紙第1の基準3による研修
- 3 装備保全管理課長は、認証事業者又は防衛事業適合事業者（契約申込書を提出済みの事業者を含む。）に対して研修を実施するに当たっては、付紙様式第16により通知するものとする。

第20 従業者の確認

- 1 物別官室長等は、防衛事業適合事業者契約の下で、秘密取扱原因契約を履行する防衛事業適合事業者に対し、秘密の取扱いの業務を行わせようとする従業者を掲載した関係社員候補者名簿（以下「候補者名簿」という。）及び候補者名簿に掲載される従業者（下請負事業者としての許可を受けようとする防衛事業適合事業者の従業者を含む。以下同じ。）の同意書（写し）を提出させるものとする。この場合において、物別官室長等は、当該候補者名簿に記載される従業者が契約の履行に当たり必要最小限にとどめられていること等について確認をするものとする。
- 2 前項の候補者名簿及び同意書（写し）は、秘密取扱原因契約締結前から契約締結後1か月以内（着工の時期が1か月以内に到来するときは、着工の日まで）に、地方防衛局調達部長等を経て提出させるものとする。
- 3 物別官室長等は、防衛事業適合事業者から提出された候補者名簿の写し及び同意書（写し）を装備保全管理課長に送付するものとし、装備保全管理課長は、必要に応じて関係機関等に照会する等し、これを確認するものとする。
- 4 装備保全管理課長は、秘密取扱原因契約の締結前に防衛事業適合事業者からの従業者の確認に係る申出がある場合は、当該事業者に対し、候補者名簿及び候補者名簿に掲載される従業者の同意書（写し）を提出させることができるものとする。
- 5 前項の規定に基づき候補者名簿及び同意書（写し）の提出を受けた装備保全管理課長は、必要に応じて関係機関等に照会する等し、これを確認するものとする。
- 6 装備保全管理課長は、前2項の手続中に当該事業者から従業者の確認に係る申出を取り消す旨の連絡を受けたときは、当該事業者と調整の上、候補者名簿及び同意書（写し）について返却又は破棄するものとする。
- 7 装備保全管理課長は、第3項又は第5項の規定による確認の結果を別に定める様式により防衛事業適合事業者に通知するとともに、その写しを秘密取扱原因契約を締結している場合にあっては担当する物別官室長等に送付するものとする。この場合において、候補者名簿に掲載された従業者が不適当と認めるときは、その理由を付記するものとする。
- 8 第4項及び第5項の手続後に当該事業者が秘密取扱原因契約を締結した場合は、当該契約を担当する物別官室長等に、候補者名簿及び確認の結果通知の写しを送付するものとする。
- 9 第3項又は第5項の規定による確認の結果、秘密を取り扱うことができるとされた従業者（以下「関係社員」という。）は、関係社員となった日から5年間を上限に秘密を取り扱う資格を有するものとし、この間は、関係社員として、候補者名簿への掲載は簡易の表記によることができるものとする。
- 10 確認を受けた候補者名簿は、関係社員名簿として管理するものとする。
- 11 関係社員名簿の変更
 - (1) 関係社員名簿に掲載された従業者を変更しようとするときは、前各項の規定に準じた手続をとるものとする。
 - (2) 防衛事業適合事業者又は装備保全管理課長は、関係社員としてふさわ

しくないと判断された従業者については、当該関係社員としての指定を取り消すものとする。

- 1 2 候補者名簿及び関係社員名簿並びに同意書の様式は、別に定める。
- 1 3 特定秘密を取り扱う従業者の確認に当たっては、前各項の規定にかかわらず、防衛装備庁における特定秘密の取扱いに関する適性評価の実施に関する訓令（平成27年防衛装備庁訓令第28号）に基づき実施するものとする。

第21 経過措置

- 1 装備保全管理課長は、第5第1項又は第2項の規定にかかわらず、訓令附則第2項に該当する認証申請事業者に対し、訓令第5条第1項に規定する認証申請書等として、付紙様式第2の秘密保全体制認証申請書、過去の審査結果の通知（保全組織、秘密保全規則、教育の体制、秘密保全施設）の写し、付紙様式第1-1の保全基準兼点検票及び保全組織（外国からの影響及び支配の程度に係る部分に限る。）に係る関係書類を、地方防衛局調達部長等を経て提出させるものとする。この場合において、訓令第6条第1項の規定による審査は、本項に基づき提出された認証申請書等に対して行うものとする。
- 2 訓令附則第3項の規定に基づく継続的確認の実施に当たっては、令和10年3月31日までの間は、付紙様式第1-4の保全基準兼点検票に係る確認に関し、特定秘密を取り扱わない秘密保全施設にあっては同票第7（警戒・警報装置）第1項及び第2項に示す基準を、特別防衛秘密を取り扱わない保管庫にあっては同票第7（警戒・警報装置）第6項に示す基準を適用しないことができるものとする。
- 3 装備保全管理課長は、第10第2項又は第3項の規定にかかわらず、訓令附則第4項に該当する防衛事業適合事業者契約の申込みをする事業者に対し、訓令第12条第1項に規定する契約申込書等として、付紙様式第11-1の防衛事業適合事業者契約申込書、付紙様式第1-1の保全基準兼点検票及び保全組織（外国からの影響及び支配の程度に係る部分に限る。）に係る関係書類並びに付紙様式第1-5の保全基準兼点検票及び秘密取扱情報システムの体制に係る関係書類を、地方防衛局調達部長等を経て提出させるものとする。この場合において、訓令第13条第1項の規定による審査は、本項に基づき提出された契約申込書等に対して行うものとし、このうち付紙様式第1-5の保全基準兼点検票に係る審査は、秘密保全対策ガイドラインの基準に照らして行うことができるものとする。
- 4 訓令附則第5項の規定に基づく継続的確認の実施は、第2項の規定に準じて行うものとする。
- 5 装備保全管理課長は、訓令附則第6項に該当する事業者の秘密取扱情報システムに係る訓令第13条第1項の規定による審査の実施に当たっては、秘密保全対策ガイドラインの基準に照らして行うことができるものとし、訓令附則第7項に該当する事業者の秘密取扱情報システムに係る訓令第14条第1項の規定による継続的確認の実施に当たっては、個々の秘密取扱情報システムの換装又は大幅な改修をするまでの間は、当該情報システムに直接関わる付紙様式第1-5の保全基準兼点検票に示す基準は適用

せず、秘密保全対策ガイドラインの基準に照らして行うことができるものとする。

- 6 第19第1項及び第2項に規定する研修を行うに当たっては、当分の間、総括者には、防衛事業適合事業者契約の申込み又は認証の申請の有無にかかわらず、防衛事業適合事業者又は認証事業者の総括者となることが予定されている者（以下「総括者予定者」という。）を含めることができる。この場合において、当該研修を受けた総括者予定者についての総括者の指名に関する基準の適用に当たっては、総括者として研修を受けたものとみなす。
- 7 第19第1項および第2項に規定する研修を行うに当たっては、令和10年3月31日までの間、保全責任者、秘密取扱情報システム管理者、秘密取扱情報システムアカウント管理者その他秘密保全組織を管理する者（以下この項及び次項において「保全責任者等」という。）には、防衛事業適合事業者契約の申込み又は認証の申請を予定している事業者の保全責任者等となることが予定されている者（以下この項及び次項において「保全責任者等予定者」という。）を含めることができる。
- 8 前項の規定により防衛事業適合事業者契約の申込み又は認証の申請を予定している事業者が保全責任者等予定者に実施要領別紙第6付紙第1の基準3第2項第2号に定める研修を受けさせた場合において、当該保全責任者等予定者に1回目の研修を受けさせた日から9か月以内の装備保全管理課長が別に定める日までに防衛事業適合事業者契約の申込み又は認証の申請をしたときは、当該事業者の総括者の氏名に関する基準の運用に当たっては、当該保全責任者等予定者は、保全責任者等として研修を受けたものとみなすことができる。
- 9 令和10年4月1日以降、秘密取扱原因契約及び保護情報取扱原因契約の締結に当たっては、防衛事業適合事業者契約が必須となる制度改正が行われることの周知に努めるものとする。

第22 契約条項は又は特約条項に係る細部事項

- 1 実施要領別紙第2の防衛事業適合事業者契約条項に係る細部事項は、実施要領別紙第6に規定するとおりとする。
- 2 実施要領別紙第5の防衛事業適合事業者における保護すべき情報の情報セキュリティの確保に係る特約条項に係る細部事項は、実施要領別紙第7に規定するとおりとする。

第23 委任規定

この要領の実施に関し必要な細部事項は、装備保全管理課長が定めるものとする。

保全基準兼点検票（保全組織の体制）

事業者名	
点検対象期間	
作成日	
作成者	
確認日	
総括者	

地方防衛局記入欄	
管轄防衛局等	
確認日	
確認者	

防衛装備庁記入欄	
確認日	
確認担当者	
確認日	
確認責任者	

作成要領
・新規申請の場合は、「新規申請」及び詳細を「対応内容」に記載すること（「継続的確認」の記載は不要）
・継続的確認の場合は、「直近の対応日」と「直近の対応内容」に記載した上で、その結果の変更の有無及び詳細を「今回確認」、「対応内容」に記載すること（「新規申請」の記載は不要）
・「今回確認」と「直近の対応内容」に変更がある項目は、「対応内容」に詳細を記載すること。
・対応(提出、実施を含む。以下同じ。)予定の場合は、点検対象期間内の対応予定日を具体的に記載すること。
・回答が困難な項目等がある場合は、その理由を「対応内容」に記載すること。
・各属紙様式を用いて回答する事項について、「今回確認」と「直近の対応内容」に変更がない場合は当該様式の提出は不要

注意事項

意図的な記載漏れや隠べい、虚偽等の回答をした場合、貴社の認証を取り消すほか、悪意を持って虚偽等の回答をし、不当な利益を得た場合には刑法上の罰則が科せられる場合があります。
特に、5 及び 9 については、輸出管理部門、法務部門等に事実確認の上、回答をお願いします。

分 類	番号	項 目	新規申請	継続的確認			対応内容 (回答の詳細などを記載)	判定		備考
				直近の対応日	直近の対応内容	今回確認		担当者	責任者	
第 1 .組織図		組織図について提出すること。								
	1	事業者全体における防衛部門の位置付けを示す組織図を提出しているか。								
	2	防衛省の情報を取り扱う事業部門(以下「防衛部門」という。)の組織編成図を提出しているか。								
第 2 .秘密情報の管理に 係る社内規程		秘密情報の管理に関する規程について定め実施していること。								
	3	コーポレートガバナンスや社内規則等には、防衛省の秘密情報の管理に関するものとは別に、守秘義務等の事業者として遵守する情報の管理に関する内容が含まれているか。								
	4	上記に該当する場合、コーポレートガバナンスや社内規則等から該当部分を抜粋し、提出しているか。								
第 3 .法令の遵守		法令を遵守する体制にあること。								
	5	過去 5 年間に於いて外国為替及び外国貿易法（昭和 2 4 年法律第 2 2 8 号）で規制されている資本取引又は貿易管理に違反した事実があるか。また、同資本取引又は貿易管理に違反した事実の調査中など現在進行中のものはあるか。								
	6	上記に該当する場合、当該事実についての概要が分かる資料を提出しているか。								
	7	5に該当する場合、改善措置を取ったか。								
	8	上記に該当する場合、改善措置についての概要が分かる資料を提出しているか。								
	9	その他、過去 5 年間に事業者として国内法令等に違反した事実があるか。また、違反した事実の調査中など現在進行中のものはあるか。								
	10	上記に該当する場合、当該事実についての概要が分かる資料を提出しているか。								
	11	9に該当する場合、改善措置を取ったか。								
	12	上記に該当する場合、改善措置についての概要が分かる資料を提出しているか。								
第 4 .役員等に係る情報		役員等を介した情報漏えいの懸念が無いこと。								
	13	役員等（取締役、監査役及び代表社員並びに防衛部門の執行責任者という。以下同じ。）が非遵行為を行った際の対応が定められているか。								
	14	上記に該当する場合、該当部分を抜粋し、提出しているか。								
	15	役員等に係る国籍情報、外国事業者等(個人事業主を含む。以下同じ。)の兼任状況及び帰化歴について回答しているか(属紙様式第1を用いて回答すること。)								
	16	外国籍の役員等、外国事業者等を兼任する役員等又は帰化歴がある役員等のいずれかが存在するか。								
	17	上記に該当する場合、当該役員等に防衛省の秘密情報が渡らないことを証明する書類（定款、取締役会決議、コーポレートガバナンス、役員規程、誓約書等）を提出しているか。								
		事業者の財務及び事業の方針の決定に影響を与える外国の者が存在しないこと。								
	18	財務及び事業の方針の決定に影響力を有する者(自社の議決権総数の50%超を有している法人又は個人のほか、別会社を通じて資本を間接的に保有している場合等の実質的に自社の財務及び事業の方針の決定を支配している者をいう。)は存在するか。								

分 類	番号	項 目	新規申請	継続的確認			対応内容 (回答の詳細などを記載)	判定		備考
				直近の対応日	直近の対応内容	今回確認		担当者	責任者	
第 5 .株式所有者等情報	19	上記の回答内容を証明する書類を提出しているか（様式は任意とし、直近の有価証券報告書、大量保有報告書等の既存の会計書類の写しによる回答も可能とする。）。								
	20	18に該当する場合、当該法人又は個人に防衛省の秘密情報が渡らないことを証明する資料（定款、取締役会決議、コーポレートガバナンス、社内規則、確認書等の防衛省の秘密情報の管理に関する規則とは別のもの）を提出しているか(確認書を提出する場合は、属紙様式第5を基本とすること。)。								
	21	発行済株式総数の５％以上又は総資本の５％以上を保有している外国事業者等が存在するか。								
	22	上記に該当する場合、当該外国事業者等に係る情報（外国事業者等の名称、外国事業者等の所在する国、保有株式数、保有割合。個人の場合は氏名、国籍、所属、役職等）について回答しているか(属紙様式第2を用いて回答すること。)。								
	23	自社の主要株主を確認し、発行済株式総数の１０％以上の実質的保有者が分からない状態にあるか。								
	24	上記に該当する場合、その概要（投資会社等の名称、設立準拠法国等、議決権保有割合）について可能な範囲で回答しているか。								
	25	23に該当する場合、実質的保有者として株式総数の５％以上を保有している外国事業者等がいるかについて可能な限り確認を行ったか。								
	26	外国事業者等（本項目においては、子会社を含む。）の発行済株式総数の１０％以上を保有しているか。								
	27	上記に該当する場合、その概要（名称、設立準拠法国等又は国籍、保有株式割合）について可能な範囲で回答しているか(属紙様式第3を用いて回答すること。)。								
	28	26に該当する場合であって、全ての外国事業者等を網羅した回答が困難なときは、自社の防衛部門と契約等を通じて防衛分野に関わる事業を行っている全ての外国事業者等について回答しているか。								
	29	26に該当する場合、当該外国事業者等に対し、防衛省の秘密情報が渡らないことの証明（定款、取締役会決議、コーポレートガバナンス、社内規則、確認書等の防衛省の秘密情報の管理に関する規則とは別のもの）を提出しているか(確認書を提出する場合は、属紙様式第5を基本とすること。)。								
	30	総資本の５％以上の負債を外国事業者等から負っているか。								
	31	上記に該当する場合、その負債の内容、当該外国事業者等の名称等について可能な範囲で回答しているか。								
	32	直近の会計年度において、特定の外国事業者等から総売上上の５％以上又は同一の国又は地域に属する複数の外国事業者等から総売上上の２５％以上を得ているか(直近の会計年度における売上高の総額のうち、同一の国又は地域に属する外国政府(国際機関を含む。)及び外国事業者等との取引に係る売上高が占める割合とする。)。								
	33	上記に該当する場合、その売上内容及び当該外国事業者等に係る情報（名称、設立準拠法国等又は国籍、割合）について回答しているか(属紙様式第4を用いて回答すること。)。								
第 6 .その他の影響	防衛省の機微な情報にアクセスする権限のある者の確認を行うこと。									
	34	指導、監督、業務支援、助言、監査等を通じて、事業者が保有する防衛省の機微な情報(秘密情報及び保護すべき情報)にアクセスする権限のある親会社等（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、監査法人その他自社に対して指導、監督、業務支援、助言、監査等を行う者をいう。以下同じ。）について回答しているか。								
	35	当該親会社等に防衛省の秘密情報を渡さないこと及び当該親会社等が防衛省の秘密情報を渡すよう求めないことを証明する資料（定款、取締役会決議、コーポレートガバナンス、社内規則、確認書等の防衛省の秘密情報の管理に関する規則とは別のもの）を提出しているか(確認書等を提出する場合は、属紙様式第5を基本とすること。)。								
	36	監査法人に防衛省の秘密が提供されないことを証明する書類を提出しているか。								
	37	これまでの質問以外で、自社の財務及び事業の決定に関し、外国事業者等が影響を与える要因がないことを確認しているか。								

総合評価		改善事項に対する措置	
------	--	------------	--

会社の役員等の一覧表

1 貴社について、下記の全ての該当する項目にレ点を入力してください。

☐ 上場会社	☐ 非上場会社	☐ (会社名) の子会社
-------------------------------	--------------------------------	-------------------------------------

2 貴社の取締役、監査役若しくは代表社員及び防衛部門の執行責任者について、下記の項目を記入してください。

	氏 名	役 職	国 籍 等	兼任先等	帰化歴の有無	帰化年月日(※)	元国籍(※)	帰化時の住所(※)
①								
②								
③								
④								
⑤								
⑥								
⑦								

(※)「帰化歴の有無」の欄を「無」と回答した場合、記載は不要

回答が困難な項目等がある場合は、その理由について簡潔に記載してください。

発行済株式総数又は総資本の 5 %以上を保有している外国事業者等

下記の項目を記入してください。

外国事業者等の名称	外国事業者等の所在する国又は地域	保有株式数	保有割合

回答が困難な項目等がある場合は、その理由について簡潔に記載してください。

外国事業者等の発行済株式総数の保有割合

外国事業者等の名称	設立準拠法等又は国籍等	発行済株式総数の保有割合（％）

※「設立準拠法等又は国籍等」の欄には、外国事業者である場合には当該法人の設立に当たって準拠した法令を制定した国又は地域の名称を、個人である場合には当該個人の国籍等を記載してください。

外国事業者等との取引に係る売上高の割合

会計年度	外国政府又は外国事業者等の名称	設立準拠法国等又は国籍等	売上高の割合（％）

※「設立準拠法国等又は国籍等」の欄には、外国政府の場合は当該国の名称を、外国事業者である場合は当該法人の設立に当たって準拠した法令を制定した国又は地域の名称を、個人である場合には当該個人の国籍等を記載してください。

年 月 日

確 認 書

防衛装備庁と特定の契約を締結するに当たり、〇〇〇株式会社（以下「甲」という。）と
〇〇〇株式会社（以下「乙」という。）は、下記の事項を確認します。

記

- 1 甲は、乙に対し、防衛装備庁と乙との間で締結された防衛事業適合事業者契約（以下単
に「防衛事業適合事業者契約」という。）及び秘密取扱原因契約（防衛装備庁と乙の間の
装備品等の調達又は役務の履行に関する契約であって、乙が特定資料等（防衛事業適合事
業者契約に定義する特定資料をいう。以下同じ。）を取り扱う直接の原因となるものをい
う。以下同じ。）に基づいて乙が当該秘密取扱原因契約の履行のために取り扱う特定資料
等について、防衛装備庁が認めた場合を除き、提供等を求めないこと。
- 2 乙は、甲に対し、防衛装備庁が認めた場合を除き、特定資料等の提供等を行わないこと。

以 上

（甲）

〇〇〇株式会社
（親会社・子会社等）

（乙）

〇〇〇株式会社
（防衛装備庁との契約の当事者）

保全基準兼点検票（秘密保全規則）

事業者名	
事業所名	
取り扱う秘密の種類	特別防衛秘密（機密・極秘・秘）・特定秘密・装備品等秘密
点検対象期間	
作成日	
作成者	
確認日	
総括者	

地方防衛局等記入欄	
管轄防衛局等	
確認日	
確認者	

防衛装備庁記入欄	
確認日	
確認担当者	
確認日	
確認責任者	

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第 1. 規則の制定に関する必要事項		規則の制定に関し、以下の項目が規定されていること。							
	1	規則の制定目的が、防衛事業適合事業者契約に基づく秘密の保護に必要な事項を定めることとなっているか。							
	2	規則の適用範囲が秘密を取り扱う全ての行為に及ぶか。							
	3	秘密を取り扱う組織の範囲を定めているか。							
	4	秘密を取り扱う組織の範囲の変更について定めているか。							
	5	取り扱う秘密の種類及び区分を定めているか。							
	6	秘密保全施設の設置の有無を定めているか。							
	7	秘密保全施設を自社で備えない場合、他の事業者の秘密保全施設等の利用の有無を定めているか。							
	8	上記により、他の事業者の秘密保全施設等の利用が有の場合、特定資料等の取扱いの態様に対応した特定資料等を保全する体制を整備しているか。							
	9	秘密情報取扱システムの設置の有無を定めているか。							
	10	秘密取扱情報システムを自社で備えない場合、他の事業者の秘密取扱情報システムの利用の有無を定めているか。							
	11	上記により、他の事業者の秘密取扱情報システムの利用が有の場合、特定資料等の取扱いの態様に対応した特定資料等を保全する体制を整備しているか。							
	12	本規則を適用する防衛省との契約リストを作成し、適宜更新することを定めているか。							
	13	次に掲げる関係法令等が記載されているか。 ・防衛事業適合事業者制度に関する訓令 ・特別防衛秘密の場合（以下 A）、日米相互防衛援助協定等に伴う秘密保護法、日米相互防衛援助協定等に伴う秘密保護法施行令、特別防衛秘密の保護に関する訓令、防衛装備庁における特別防衛秘密の保護に関する訓令 ・特定秘密の場合（以下 B）、特定秘密の保護に関する法律、特定秘密の保護に関する法律施行令、特定秘密の保護に関する訓令、防衛装備庁における特定秘密の保護に関する訓令 ・装備品等秘密を取り扱う場合（以下 C）、防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律、防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律施行令、装備品等秘密の指定等に関する訓令、秘密保全に関する訓令、防衛装備庁における秘密保全に関する訓令							
		以下に記載する用語の定義が、関係法令等に照らして適切に記載されているか。							
		・（A）特別防衛秘密							
		・（B）特定秘密							
		・（C）装備品等秘密							
		・秘密							
		・総括者							
		秘密の管理職員（秘密取扱原因契約に基づいて乙に特定資料等を取り扱わせる意思決定をし、乙における特定資料等の取扱いの状況を管理し、及び監督する防衛省の職員）							
		・（B）適性評価							

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第 1、規則の制定に関する必要事項	14	・防衛事業適合事業者							
		・特定資料							
		・特定物件							
		・特定情報							
		・特定資料等							
		・伝達							
		・秘密業務							
		・関係社員							
		・下請負事業者関係社員							
		・情報システム							
		・秘密取扱情報システム							
		・可搬記憶媒体							
		・携帯型情報通信・記録機器							
		・秘密保全施設							
		・閉鎖区域							
		・制限区域							
		・秘密保全施設等							
		・保管容器							
		・関係簿冊							
		・反古紙							
		外国政府等秘密情報 以下の項目が定義されているか							
		ア 米国秘密軍事情報							
		イ 北大西洋条約機構秘密情報							
		ウ 仏国秘密情報							
		エ 豪州秘密情報							
		オ 英国秘密情報							
		カ インド秘密軍事情報							

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第 1. 規則の制定に関する必要事項		キ 伊国秘密情報							
		ク 韓国秘密軍事情報							
		ケ 独国秘密情報							
		コ 瑞国秘密情報							
		サ サウジ秘密情報							
		シ U A E 秘密情報							
		ス 宇国秘密情報							
第 2. 運用上の注意及び解釈	規則の運用について以下の項目が規定されていること。								
	1	不当な拡張解釈の禁止							
	2	解釈及び運用に疑義が生じた場合の協議							
	3	自社の秘密保全施設等で特定資料等を取り扱う下請負事業者がいる場合の、下請負事業者の秘密保全規則との関係の整理							
第 3. 秘密保全体制の整備及び維持	秘密保全体制の整備及び維持について以下の項目が規定されていること。								
	1	秘密保全体制（総括者、秘密保全組織、外国の影響等の評価、教育体制、秘密保全施設及び秘密取扱情報システム）の整備及び維持について定めているか。							
	2	秘密情報取扱システムを設置する場合、秘密情報取扱システムごとに秘密取扱情報システム実装計画(SSP)を作成し、秘密情報取扱システムで秘密を取り扱う体制を整備することを定めているか。							
	3	防衛省が秘密の区分に応じた要件を変更した場合、防衛省が設定した期間内に対応することを定めているか。							
	4	特定資料の取扱いに対する外国からの影響及び支配の程度について、定期的に評価することを定めているか。							
	5	秘密保全体制（外国からの影響及び支配の程度に係る評価を除く。）を変更する場合は、あらかじめ防衛省の承認を得ることを定めているか。							
第 4. 秘密保全組織及び関係社員の指定及び職務等に関する規定	秘密保全組織及び関係社員について以下の項目が規定されていること。								
	1	秘密保全組織の設定及び改編について							
	2	秘密保全組織の構成について							
	3	秘密保全組織を構成する者の責任分担及び役割について							
	4	総括者の指定及び責任について							
	5	秘密保全規則の違反者に対する懲戒処分について							
	6	関係社員が秘密を取り扱う際の手順の作成について							
	7	保全責任者の指定及び職務について							
	8	保全責任者の補助者の指定について							
	9	関係社員の指定及び解除について							
	10	関係社員としてふさわしい者を指定し、また指定の範囲は必要最小限にとどめることについて							

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第 4. 秘密保全組織 及び関係社員の指定及 び職務等に関する規定	11	防衛省との契約に違反する行為を求められた場合に、これを拒む権利を実行性をもって法的に保証されない者を関係社員として指定することができないことについて							
	12	関係社員の指定についての同意を得ることについて							
	13	関係社員の指定に当たり同意書を取得することについて							
	14	関係社員として指定されることに同意しなかった従業者又は防衛省が関係社員の指定の同意をしなかった従業者に対する、不利益な取扱いの禁止について							
	15	特定秘密を取り扱う関係社員の指名に当たっては、適性評価により特定秘密の取扱いが認められた者から指名し、取り扱う特定秘密の範囲を最小限にすることについて							
	16	特定秘密の取扱いを認められた関係社員が、引き続き特定秘密を取り扱うことの適性を疑われた場合の措置について							
	17	1 6 における必要な措置の報告について							
	18	関係社員候補者名簿の届出及び名簿に登載される従業者の同意書の提出について							
	19	関係社員名簿の変更について							
	20	関係社員名簿の目的外使用の禁止について							
	21	面談等による関係社員の継続的な変化の把握について							
	22	上記における関係社員の事情変化があった場合の報告について							
	23	適格証の作成交付について							
	24	適格証の内容について							
	25	適格証の管理について							
	26	適格証の点検について							
	27	適格証の回収について							
	28	管理責任者及び保全責任者の引継ぎについて							
	29	引継ぎの記録、確認について							
第 5. 秘密情報の取 扱いの範囲等について	秘密情報の取扱いについて、以下の項目が規定されていること。								
	1	第三者による取扱いの禁止について							
	2	関係社員以外の従業者による秘密業務の従事禁止について							
	3	関係社員におけるNeed to knowの厳格な管理							
	4	関係社員の責務及び関係社員相互の伝達の制限について							
	5	防ちようについて							
	6	秘密の漏えい等に係る罰則等の周知について							
	7	秘密の目的外利用の禁止について							

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第 6．関係社員及び 従業員に対する教育の 実施内容及び方法につ いて	関係者員等の教育について、以下の項目が規定されていること。								
	1	保全教育の年間計画について							
	2	保全教育の実施について							
	3	新規の関係社員に対する教育について							
	4	臨時教育について							
	5	取扱終了時教育について							
	6	保全教育の内容等の変更について							
	7	関係社員以外の従業員に対する教育及び記録について							
	8	下請負事業者関係社員への教育及び記録について							
	9	従業員以外の者（保全施設立入りを認められた者）への教育について							
第 7．関係簿冊につい て	関係簿冊について、以下の項目が規定されていること。								
	1	関係簿冊の作成及び管理について							
	2	関係簿冊の改ざん防止について							
	3	関係簿冊の保管期間について							
	4	関係簿冊の廃棄の記録について							
第 8．秘密保全施設 等に関する規定	秘密保全施設等について、以下の項目が規定されていること。（秘密保全施設等を自社で備えない場合（第 1 の 6 ～ 8 参照）は、全て「非該当」とする。）								
	1	秘密保全施設の構築について							
	2	秘密保全施設の新設及び変更時の申請について							
	3	防衛省が規定する要件を満たさない場合の手続について							
	4	秘密保全施設の申請の細部について							
	5	閉鎖区域の構築について（基準を満たさない場合の手続を含む）							
	6	閉鎖区域の構築に係る規則について（設定開始及び設定解除に伴う措置）							
	7	閉鎖区域の設定について							
	8	閉鎖区域の設定期間の変更の届出について							
	9	保全外部区域の設定について							
	10	保全外部区域の立入者名簿について							
	11	保全外部区域の入退管理について							
	12	敷地を保全外部区域に設定した場合の外柵の措置について							

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第 8．秘密保全施設等に関する規定	13	立入制限の掲示について							
	14	関係社員及び立入可能者以外の立入制限について							
	15	特に立入りを必要とする場合について							
	16	秘密保全施設等への立入り時の措置について							
	17	関係社員が立ち入る場合の措置について							
	18	立入可能者が立ち入る場合の措置について							
	19	立入可能者が立ち入る場合の保全措置について							
	20	電子錠の場合の入退管理について							
	21	秘密保全施設等の立入記録の精査及び記録について							
	22	秘密保全施設等の鍵の管理等の細部手続について							
	23	秘密取扱情報システム以外の情報システムの秘密保全施設等への持ち込み禁止について							
	24	秘密取扱情報システム以外の情報システムの持込みが必要となる場合、以下の事項を含めた利用要件について ア 私有の情報システムではないこと。 イ 業務上必要なソフトウェア以外のソフトウェアがインストールされていないこと。 ウ 直前に最新の検知ソフトウェアでフルスキャンしていること。 エ 無線 LAN の機能が無効化されていること。 オ 情報システムの使用後に、秘密取扱情報システムの利用者が秘密のデータが保存されていないことを確認するとともに、当該利用者以外の者が点検すること。 カ 使用日時・使用者・使用目的等を含む記録簿を整備すること。							
	25	上記、情報システムの持込みが必要となった場合について							
	26	秘密保全施設等への携帯型情報通信・記録機器（可搬記憶媒体管理簿に記載されている可搬記憶媒体を除く。）の持込み制限について							
	27	秘密保全施設等への携帯型情報通信・記録機器の持込み制限の掲示について							
第 9．秘密文書等の 接受及び周知等について	28	秘密保全施設等へやむを得ず携帯型情報通信・記録機器を持込む場合の措置について、以下の事項を含めた利用要件の規定について ア 私有の携帯型情報通信・記録機器ではないこと。 イ 業務上必要なソフトウェア以外のソフトウェアがインストールされていないこと。 ウ 直前に最新の検知ソフトウェアでフルスキャンしていること。 エ 無線 LAN の機能が無効化されていること。 オ 携帯型情報通信・記録機器の使用後に、秘密取扱情報システムの利用者が秘密のデータが保存されていないことを確認するとともに、当該利用者以外の者が点検すること。 カ 使用日時・使用者・使用目的等を含む記録簿を整備すること。 キ 携帯型情報通信・記録機器に対するリモートアクセスによる起動及び操作を禁止すること。 ク 携帯型情報通信・記録機器が起動している場合には、外形的に明らかな表示を行うこと。							
	接受について以下の項目が規定されていること。（秘密文書等を接受しないなどの事情のある場合は、当該事情を踏まえた規則とすること。）								
	1	秘密文書等の接受者の制限について							
	2	秘密文書等の接受の報告について							
	3	秘密文書等の保管及び保管簿の作成について							
	装備品等秘密指定書の周知について以下の項目が規定されていること。								
	1	装備品等秘密指定書の周知について							

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第 9．秘密文書等の 接受及び周知等につい て	2	装備品等秘密の延長及び解除の周知について							
	特定秘密の周知について以下の項目が規定されていること。								
	1	特定秘密の指定の周知について							
	2	特定秘密の有効期間満了の通知があった場合の措置							
	3	特定秘密の有効期間延長の通知があった場合の措置							
	4	特定秘密の解除の通知があった場合の措置							
第 1 0．秘密文書等 の保管及び秘密保全施 設等の鍵等の管理につ いて	秘密文書等の保管及び秘密保全施設等のかぎ等の管理について以下の項目が規定されていること。（秘密保全施設等を自社で備えない場合（第 1 の 6 ～ 8 参照）は、全て「非該当」とする。）								
	1	秘密文書等の保管容器への保管について							
	2	秘密を取り扱う可搬記憶媒体の保管について							
	3	秘密文書等が保管容器に保管できない場合の措置について							
	4	秘密文書等の集中保管について							
	5	秘密保全施設等及び保管容器の日々点検について							
	6	文字盤鍵の組み合わせ番号の管理について							
	7	文字盤鍵の組み合わせの変更について							
	8	文字盤鍵の組み合わせの変更の実施者について							
	9	文字盤鍵の組み合わせの変更の記録について							
	10	差し込み式鍵の保管者の制限について							
	11	差し込み式鍵の使用者の制限について							
	12	差し込み式鍵の就業時間外の管理について							
	13	差し込み式鍵を保管する容器の鍵の管理について							
第 1 1．秘密文書等 の閲覧及び秘密情報の 伝達について	秘密文書等の閲覧及び秘密情報の伝達について以下の項目が規定されていること。								
	1	関係社員以外への閲覧・貸出の禁止について							
	2	閲覧・貸出の記録について							
	3	閲覧・貸出場所の制限について							
	4	閲覧・貸出時の保全措置について							
	5	日をまたぐ閲覧・貸出の禁止について							
	6	閲覧・貸出後の確認について							
	7	伝達方法の制限について							

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第 1 1 . 秘密文書等の 閲覧及び秘密情報の 伝達について	8	伝達場所及び伝達時の保全措置について							
	9	特定秘密の伝達の申請について							
	10	特定秘密の伝達の報告について							
	11	特定秘密文書等を用いた伝達について							
第 1 2 . 秘密文書等 の送達について	秘密文書等の送達について以下の項目が規定されていること。(秘密保全施設等を自社で備えない場合（第 1 の 6 ～ 8 参照）は、特段の事情のない限り、全て「非該当」とする。)								
	1	秘密文書等の送達の許可について							
	2	秘密文書等の運搬時の保全措置について							
	3	秘密文書等を運搬容器等により運搬できない場合の措置について							
	4	秘密文書等の封かんについて							
	5	秘密文書等の送達の記録について							
	6	秘密文書等の送達時の保全責任者の責務について							
	7	電気通信による特定秘密の交付について							
第 1 3 . 秘密文書等 の作成等について	秘密文書等の作成等について以下の項目が規定されていること。								
	1	秘密文書等の作成等の申請について							
	2	秘密文書等の作成等の制限について							
	3	秘密文書等の作成が契約履行上認められている場合の措置について							
	4	秘密文書等の作成等の立会について							
	5	秘密文書等の作成等の報告について							
	6	秘密文書等の作成等の保全責任者の責務について							
	7	秘密文書等の作成等の実施記録について							
	8	秘密文書等の作成等時の反故紙について							
	9	完成に至らなかった秘密文書等に関する取扱いの指示を受けたものの報告							
	10	作成等する秘密文書等の指定について							
	11	指定条件変更時の保管簿の措置について							
第 1 4 . 秘密文書等 の表示について	秘密文書等の表示について以下の項目が規定されていること。								
	1	秘密文書等への秘密の種類、区分、一連番号、枚数、指定条件等の表示について							
	2	秘密文書等への外国政府等秘密情報の表示について							
	3	秘密文書等への登録番号等の表示について							

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第 1 4．秘密文書等の表示について	4	秘密文書等への表示場所について							
	5	秘密文書等の表示の色について							
	6	秘密文書等への表示が困難な場合の措置について							
	7	特定秘密の指定期間が満了した場合の表示について							
	8	特定秘密の指定期間が延長された場合の表示について							
	9	秘密等が解除された場合の表示について							
第 1 5．下請負について	下請負について以下の項目が規定されていること。								
	1	下請負の制限について							
	2	秘密業務に係る下請負に該当しない場合について							
	3	下請負の手続について							
	4	下請負先への秘密文書等の伝達及び送達について							
	5	下請負先への秘密文書等の貸与の手続について							
	6	下請負先の検査について							
	7	下請負先の防衛省の保全検査への協力について							
	8	秘密保全施設等において関係社員と協力して秘密取扱業務を行う下請負事業者関係社員がある場合の措置について							
第 1 6．秘密文書等の返却及び廃棄について	秘密文書等の返却及び廃棄について以下の項目が規定されていること。（秘密保全施設等を自社で備えない場合（第 1 の 6 ～ 8 参照）は、特段の事情のない限り、全て「非該当」とする。）								
	1	秘密文書等の速やかな防衛省への返却について							
	2	防衛省の指示による秘密文書等の返却について							
	3	装備品等秘密の指定の有効期間が満了した場合の装備品等秘密文書の防衛省への返却又は提出について							
	4	保全責任者による秘密文書等の返却の記録について							
	5	秘密文書等の廃棄の制限について							
	6	秘密文書等の廃棄方法について							
	7	保全責任者による秘密文書等の廃棄の記録について							
	8	秘密文書等の廃棄の防衛省への報告について							
第 1 7．情報システムについて	情報システムについて以下の項目が規定されていること。（秘密取扱情報システムを自社で備えない場合（第 1 の 9 ～ 1 1 参照）は、全て「非該当」とする。）								
	1	秘密情報を情報システムで取り扱う場合について							
	2	秘密取扱情報システムの利用に関する体制について							
第 1 8．社内点検について	社内点検について以下の項目が規定されていること。								
	1	点検票による社内の毎月の点検について							

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第18．社内点検について	2	特定資料等の保管点検について							
	3	秘密保全規則及び履行状況の点検と見直しについて							
	4	秘密保全を確保するための各種保全措置の検証及びリスク査定の実施について							
	5	防衛省の規則改正の有無の確認と規則への反映について							
	6	秘密文書等の保管状況報告について							
第19．防衛省による保全検査について	防衛省による保全検査について以下の項目が規定されていること。								
	1	防衛省が実施する保全検査への協力について							
	2	防衛省の指導があった場合の措置について							
	3	契約後の防衛省の検査及び調査への協力について							
第20．非常時及び事故時の措置について	非常時及び事故時の措置について以下の項目が規定されていること。								
	1	緊急時の秘密文書等の廃棄について							
	2	緊急時の秘密文書等の廃棄の申請及び報告について							
	3	緊急時の廃棄後速やかに行う報告について							
	4	緊急連絡体制の整備について							
	5	関係社員による保全事故発生時の報告について							
	6	事故発生時の防衛省への速報について							
	7	事故発生時の元請負者への報告について							
	8	連絡系統図の作成と更新について							
	9	事故発生時の対処体制及び対処手順の作成について							
	10	事故発生時の調査内容と報告について							
	11	保全事故の可能性及び懸念についての報告							
	12	事故発生時の保全規則等の見直しについて							
	13	事故発生時の対処訓練の実施と検証について							
第21．雑則について	雑則について以下の項目が規定されていること。								
	1	適合事業者契約終了後の守秘義務について							
	2	規則改正時の申請について							
	3	細部要領への委任について							
	4	様式について本規則と防衛省による指示の競合について							

分 類	番号	項 目	新規申請	継続的な確認	対応条文	対応内容 (項目に対応する条文等を記載する)	判定		備考
							担当者	責任者	
第21. 雑則について	5	社内規則の競合について							
総合判定									

※様式の名称は一般的なものを例示。各社、各事業所等の秘密の取扱状況に応じて変更可とする。

保全基準兼点検票（秘密保全教育の体制）

事業者名	
秘密保全施設の有無 ※認証申請の場合、有と記載	
秘密取扱情報システムの有無	
想定される下請・元請の有無	
点検対象期間 ※新規申請の場合は空欄	
作成日	
作成者	
確認日	
総括者	

地方防衛局等記入欄	
管轄防衛局等	
確認日	
確認者	

防衛装備庁記入欄	
確認日	
確認担当者	
確認日	
確認責任者	

分 類	番号	項 目	新規申請	継続的な確認	対応内容 (左の回答の詳細、教育テキストの記載ページ数などを記載)	判定※		備考
						担当者	責任者	
第 1 . 保全教育体制		毎年定期的に保全教育を行う人的・物的体制を整備している又はこれらを整備することができると認められること。						
	1	秘密保全に関する業務を担当する部署があるか。その体制は明確か。						
	2	秘密保全に関する業務を担当する部署は、現に行われている秘密取扱の業務に照らし、適切か。						
	3	保全教育の年間計画（時期、実施項目（カリキュラム）、場所、教育実施者）を作成しているか。						
	4	保全教育の年間計画では、計画期間における保全教育の狙いが明確になっているか。						
	5	保全教育の年間計画には、計画期間に想定される防衛省の秘密の取扱いに関するリスク評価が反映されているか。						
	6	保全教育の年間計画には、年次教育、取扱前教育及び取扱終了時教育について明記されているか。						
	7	保全教育の年間計画には、どのような場合に臨時教育を行うかが明記されているか。						
	8	保全教育の年間計画は、元請負事業者又は下請負事業者との関係について考慮されているか。						
	9	保全教育の年間計画は、秘密取扱情報システムの利用及び管理について考慮されているか。						
	10	秘密取扱情報システムを備えている場合、当該システムの利用及び管理に関する保全教育体制を整えているか。						
	11	保全教育用のテキストには、【 2 4 ～ 6 4 】のうち必要な教育項目が含まれているか。						
	12	教育実施者は、過去に防衛省又は防衛装備庁の契約担当官等との契約において、保全業務担当者又は管理者として防衛省の秘密を取り扱ったことがあるか。						
	13	教育実施者は、秘密の取扱い経験又は研修の受講を通じて、教育実施者としての識見を備えているか。						
	14	全ての関係社員に対し少なくとも年 1 回保全教育を実施しているか。						
	15	関係社員以外の従業者にに対し、次に掲げる事項を含む教育を実施しているか。 ア 関係社員以外の従業者は特定資料等に接してはならないこと。 イ 役員、管理職員その他の関係社員の職務上の上級者は、関係社員に指定されていない場合には、職務上の下級者である関係社員に対し、自らが特定資料等に接することを求めてはならないこと。						
	16	関係社員以外の従業者にに対し、上記の教育のほか必要であるとしている事項を記載しているか。						
	17	新たに秘密を取り扱う必要がある従業者にに対し、取扱前教育を実施しているか。						
	18	関係社員ではなくなることとなった従業者にに対し、取扱終了時教育を実施しているか。						
	19	従業者に対して行った教育の結果について、記録しているか。						
	20	下請負事業者の関係社員に対し、それぞれが行う特定資料等の取扱いの業務の内容及び態様に応じた教育を実施しているか。						
	21	下請負事業者の関係社員に対して行った教育の結果について、記録しているか。						
	22	従業者及び下請負事業者関係社員のほか、秘密保全施設等への立入りを認めた全ての者に対し、それぞれの責任若しくは役割又は立入りの目的に応じた教育を実施しているか。						
	23	秘密取扱情報システムを備えている場合、当該システムの利用及び管理に関する教育を行っているか。						
第 2 . 保全教育テキスト		秘密に関する法令の内容、秘密の取扱いに関する基本事項、秘密の取扱者としての心得等を的確に習得できること。						
	24	特別防衛秘密／特定秘密／装備品等秘密に関する法律、政令、訓令、事務次官通達その他関係規則の条文の内容、解説が記載されているか。						
	25	秘密保全の必要性（漏えいの国際的、国内的影響）が記載されているか。						
	26	保全教育の意義・重要性（秘密保全意識の涵養を含む。）が記載されているか。						
	27	秘密の漏えい等に係る罰則、懲戒処分、違約金条項等が記載されているか。						
	28	事業者として行う防衛省の秘密を取り扱う業務の範囲を特定し、その内容について記載されているか。						
	29	事業者として行う防衛省の秘密を取り扱う業務の態様を特定し、その内容について記載されているか。						
	30	事業者として行う防衛省の秘密の取り扱う業務の範囲及び態様に応じた秘密保全上のリスクを特定し、その内容について記載されているか。						
	31	取扱業務の範囲及び態様並びに秘密保全上のリスクに照らし、総括者、保全責任者、関係社員等の役割及び責任について記載されているか。						
	32	「need to know の原則」の説明及び確実な履行について記載されているか。						
	33	秘密の保全に関する社内規則を説明した上で、その確実な履行について記載されているか。						
	34	カウンターインテリジェンス及び諸外国の事例を紹介した上で、隙のない勤務と私生活において慎重な行動をとることの重要性について記載されているか。						
	35	上記のほか、事業者として業務上取り扱う情報の保全に関して重視する事項を記載しているか。						

分 類	番号	項 目	新規申請	継続的な確認	対応内容 (左の回答の詳細、教育テキストの記載ページ数などを記載)	判定※		備考
						担当者	責任者	
第2.保全教育テキスト		秘密の提供・保有に関する基本的な原則を習得できること。						
	36	防衛装備庁からの秘密の提供等に係る手続等が記載されているか。						
	37	秘密取扱原因契約が終了したときは特定資料等を防衛装備庁に返却又は提出する必要があることについて記載されているか。						
	38	事業者による秘密の文書、図画及び物件の廃棄は原則として認められないこと及び廃棄が認められている場合について記載されているか。						
		秘密保全施設等の管理に関する知識を習得できること。						
	39	保全外部区域の設定、管理、立入要領が記載されているか。						
	40	閉鎖区域の設定等に関することが記載されているか。						
	41	制限区域の構築等に関することが記載されているか。						
	42	秘密保全施設等の管理、立入制限等に関することが記載されているか。						
	43	秘密保全施設等への機器等の持込み制限等に関することが記載されているか。						
	44	秘密保全施設等への情報システムの持込・設置制限に関することが記載されているか。						
		秘密の供覧・交付等に関する基本的事項を習得できること。						
	45	相手方・必要性に応じて供覧・交付等の可否を判断することが記載されているか。						
		秘密の文書、図画及び物件の登録及び秘密の取扱い状況の記録に関する基本的事項を習得できること。						
	46	関係簿冊の作成・記録・保存要領が記載されているか。						
		秘密の指定、周知等に関する基本的事項を習得できること。						
	47	特定秘密／装備品等秘密の指定、周知等に関することが記載されているか。						
		秘密の文書・物件の作成及び表示に関する基本的事項を習得できること。						
	48	秘密の文書、図画及び物件の作成要領が記載されているか。						
	49	秘密区分ごとの表示・抹消要領が記載されているか。						
		秘密の文書、図画及び物件の運搬、交付、伝達等に関する基本的事項を習得できること。						
	50	秘密の文書、図画及び物件の運搬等の要領が記載されているか。						
	51	秘密の文書、図画及び物件の交付等の要領が記載されているか。						
	52	伝達、送達、閲覧、貸出の要領が記載されているか。						
	53	秘密の文書、図画及び物件の回収、返却の要領が記載されているか。						
		情報システムによる秘密の取扱いに関する基本的事項を習得できること。						
	54	秘密を取り扱う電子計算機等の使用、管理等（悪意のあるソフトウェアへの感染を防止するための対策及び感染した場合の対処手順を含む。）に関することが記載されているか。						
		秘密の文書、図画及び物件の保管に関する基本的事項を習得できること。						
	55	秘密の文書、図画及び物件の保管要領が記載されているか。						
		緊急事態及び事故への備え及び対応に関する基本的事項を習得できること。						
	56	事故に備えることについて記載されているか。						
	57	緊急事態及び事故の発生時の対処要領（各役割ごとの関係社員等の行動、緊急連絡体制、防衛省への報告事項等）が記載されているか。						
		秘密保全体制等の検証及び秘密取扱状況の点検等に関する基本的事項を習得できること。						
	58	秘密保全体制及び秘密の保護措置の検証について記載されているか。						
	59	自己点検の種類、頻度、要領が記載されているか。						
	60	防衛省による保全検査に関することが記載されているか。						
		秘密の取扱業務を伴う下請負に関する基本的事項を習得できること。						
	61	下請負の要領が記載されているか。						
	62	下請負事業者に対する元請負事業者としての責任が記載されているか。						
	63	下請負事業者関係社員に対して元請負事業者が行う教育について記載されているか。						
	64	秘密保全施設等において関係社員と協力して特定資料等の取扱いの業務を行う下請負事業者関係社員があるときの防衛装備庁の許可、下請負事業者との協議、下請負事業者関係社員による秘密取扱業務の管理等について記載されているか。						
第3.教育結果の記録		従業者に対する教育について、その結果を記録していること。						
	65	従業者に対する年次教育の実績を説明してください。						
	66	従業者に対する臨時教育の実績を説明してください。						
	67	従業者に対する取扱前教育の実績を説明してください。						
	68	取扱前教育を受けずに秘密を取り扱った従業者の有無について記載してください。						
	69	従業者に対する取扱い終了後教育の実績を説明してください。						
	70	取扱終了後教育を受けずに離職した従業者の有無について記載してください。						
第4.実施計画の作成		次の年に保全教育を行う人的・物的体制を整備している又はこれらを整備することができると認められること。						
	72	翌年度の実施計画（時期、実施項目、場所、教育実施者）を作成しているか。						
	73	旧年度と翌年度の実施計画に大きな変更（教育内容や教育実施者の変更等）はあるか。						

※ 認証申請又は防衛事業適合事業者契約の申込み時は適合、非適合、非該当から選択するものとし、点検時には良好、要改善、不良から選択するものとする。

総合判定		改善事項に対する措置	
------	--	------------	--

保全基準兼点検票（秘密保全施設、保全外部区域及び保管容器）

事業者名		特別防衛秘密を取り扱うことができる（※変更不可）	地方防衛局等記入欄	防衛装備庁記入欄
事業所名			管轄防衛局等	確認日
秘密保全施設名			確認日	確認担当者
取り扱う秘密の種類			確認者	確認日
施設の用途				確認責任者
保管庫としての用途				
作成日		保管庫として使用できる（※変更不可）		
確認責任者				

(特別防衛秘密を取り扱う場合又は保管庫として使用する場合)									
分 類	番号	項 目	対応状況 (自己評価)	対応内容 (仕様内容を記述した上で、それを確認できる別添資料名を記載)	(別添資料)	現地調査 判定	判定		備考
							担当者	責任者	
第 1. 天井、壁、床		天井について、下欄に掲げる基準を満たしていること。							
	1	厚さ10cm以上の鉄筋コンクリートで堅固に建造されているか。							
		壁について、下欄に掲げる基準を満たしていること。							
	2	厚さ10cm以上の鉄筋コンクリートで堅固に建造されているか。							
	3	床から天井に到達する壁であるか。							
		既存の建造物を改修する場合に、天井又は壁について、上記の基準（1又は2）を満たせないときは、下欄に掲げる基準のいずれかを満たしていること。							
	4	補強コンクリートブロック（厚さ15cm以上。中空部にコンクリートを充填。直径9mm以上の鉄筋を縦40cm以下・横20cm以下の間隔で配筋）で堅固に建造されているか。							
	5	銅板（厚さ3.2mm以上（室内外の両面に配置する場合は、各々1.6mm以上）で堅固に建造されているか。							
	6	その他の不燃性の資材であって、鉄筋コンクリート（厚さ10cm以上）と同等以上の強度を有すると確認されたもので堅固に建造されているか。							
	6.1	同等以上の強度を有すると確認された資材を使用する場合、同等以上の強度を有することが証明できる資料（第三者機関又は資材メーカー等による強度試験結果等）を添付しているか。							
		建築構造上の理由により、天井及び壁について、上記の基準の全部又は一部を満たせないときは、下欄に掲げる基準のいずれかを満たしていること。							
	7	次の措置により、上記の基準（1又は2）と同等以上の保全措置を講じているか。 ・天井として金網（切断困難な強度を有し、溶接又はボルト等により枠に固定されたもの）を張ること。 ・天井からの侵入を警戒する警報装置を設置すること。 ・壁と天井が接続するよう金網（切断困難な強度を有し、溶接又はボルト等により枠に固定されたもの）等を設置すること。							
	8	（格納庫等のように、特に高い天井高であって、壁（間仕切り）が天井まで届かない構造である場合） 代用天井を設置の上、天井と代用天井との間を金網（切断困難な強度を有し、溶接又はボルト等により枠に固定されたもの）で補強しているか。							
	9	（格納庫等のように、特に高い天井高であり、壁（間仕切り）が天井まで届かず、かつ、代用天井を設置できない場合） 壁（間仕切り）を乗り越えて不法侵入できないように特別の措置を講じているか。							
	9.1	不法侵入が困難であることが証明できる資料（実地検証の結果等）を添付しているか。							
		床について、下欄に掲げる基準を満たしていること。							
	10	厚さ10cm以上の鉄筋コンクリートで堅固に建造されているか。							
		床について、上記の基準を満たせない場合に下欄に掲げる基準を満たしていること。							
	11	その他の不燃性の資材であって、鉄筋コンクリート（厚さ10cm以上）と同等以上の強度を有すると確認されたもので堅固に建造されているか。							
	11.1	同等以上の強度を有すると確認された資材を使用する場合、同等以上の強度を有することが証明できる資料（第三者機関又は資材メーカー等による強度試験結果等）を添付しているか。							
第 2. 出入口、搬入口、非常口		出入口、搬入口及び非常口について、下欄に掲げる基準をいずれも満たしていること。							
	1	出入口（搬入口及び非常口を除く。以下同じ。）は1箇所であるか。 （2箇所以上の出入口は、秘密の取扱い上の必要がない限り認められない。）							
	2	搬入口を設置している場合、（1の）出入口では機材等の搬入・搬出ができないからか。							
	3	非常口を設置している場合、施設の面積、構造等の観点から、緊急の事態が発生した際の脱出口のために必要最小限の数か。							
	4	非常口を設置している場合、内側からの開閉のみを可能とする構造か。							
	5	出入口の外側上部に照明装置（常夜灯）を取り付けるなど、出入口に接近する者の監視が容易であるか。							
	6	出入口が開放された際に秘密保全施設の外側から内側を直接見えないようになっているか。（例えば、前室を設けているか。出入口の内側に衝立、カーテン等の外側からの視線を妨げるものを設けているか。）							
	7	搬入口が開放された際に外側から内側を直接見えないようになっているか。直接見えるようになっている場合、搬入口を開放する際に外部からの窃視を防ぐための措置が定められているか。							
第 3. 扉		出入口、搬入口及び非常口の扉について、下欄に掲げる基準をいずれも満たしていること。							
	1	鋼鉄製で、厚さ3. 2mm以上（フラッシュ扉の場合は両面の板が1. 6mm以上）であるか。							
	2	丁番は、内側埋込式であるか。							
	3	丁番が切断された場合でも開放を防止できる構造であるか。							
	4	両開きの扉の場合、扉の合せ目に定規ぶちを取り付けているか。							
	5	扉に覗き窓の機能を必要とする場合は、ドアスコープを取り付けて、内側からのみ覗くことができるものとなっているか。							
第 4. 錠		出入口の錠について、下欄に掲げる基準をいずれも満たしていること。							
	1	差し込み式鍵、生体認証式鍵等による二重施錠方式以上の強度であるか。							
	1.1	差し込み式鍵は、CP認定錠など、対ピッキング性能などが優れており、容易にこじ開けられない強度を有しているか。							
	1.2	生体認証式鍵又は文字盤鍵（交換数1 0 0の3乗以上）以外の鍵である場合、これらと同等以上の強度であることを証明する資料を添付しているか。							
	2	扉の非常開閉装置を取り付けているか。							
		搬入口の錠について、下欄に掲げる基準を満たしていること。							
	3	秘密保全施設の内側からのみ解錠できる構造になっているか。							
	4	上記に該当しない場合、外側の錠は、差し込み式鍵、生体認証式鍵等による二重施錠方式以上の強度であるか。							
	4.1	差し込み式鍵は、容易にこじ開けられない強度を有しているか。							
	4.2	生体認証式鍵又は文字盤鍵（交換数1 0 0の3乗以上）以外の鍵である場合、これらと同等以上の強度であることを証明する資料を添付しているか。							

分 類	番号	項 目	対応状況 (自己評価)	対応内容 (仕様内容を記述した上で、それを確認できる別添資料名を記載)	(別添資料)	現地調査 判定	判定		備考
							担当者	責任者	
第４．錠	非常口の錠について、下欄に掲げる基準を満たしていること。								
	5	秘密保全施設の外側から解錠できない構造になっているか。							
	6	緊急の事態が発生した場合の脱出の容易性を確保した上で、日常的な解錠を回避できる構造になっているか。							
第５．窓	窓について、下欄に掲げる基準を満たしていること。								
	1	無窓であるか							
	上記の基準を満たせない場合、下欄に掲げる資料を用いて秘密保全上の影響がない構造であることを明らかにすること。								
	2	施設における窓の数、位置及び大きさが分かる資料を添付しているか。							
	3	2の資料に、採光、換気等のやむを得ない目的のため必要最小限の数であることが分かる内容が含まれているか。							
	4	2の資料に、鉄格子（日本産業規格、鉄棒直径13mm以上、間隔10cm以下）を堅固に取り付けていることが分かる内容が含まれているか。							
第６．開口部	開口部（ダクト、通風調節装置、天窓、下水溝、トンネル等）について、下欄に掲げる基準をいずれも満たしていること。								
	1	侵入し得る形状の開口部に直径13mm以上の鉄筋を縦及び横に10cm以下の間隔で取り付けているか。							
	2	開口部からの不法侵入、盗み見、盗聴等の侵害に対応するための措置を講じているか。							
第７．警戒・警報装置	警戒・警報装置について、下欄に掲げる基準をいずれも満たしていること。								
	1	出入口の外側に監視カメラを取り付け、入退室の状況が監視できるか。（※）							
	2	搬入口の外側に監視カメラを取り付け、搬出入の状況が監視できるか。（※）							
	3	出入口の扉の開閉を感知する自動の警戒・警報装置を取り付けているか。							
	4	搬入口の扉の開閉を感知する自動の警戒・警報装置を取り付けているか。							
	5	非常口の扉の開閉を感知する自動の警戒・警報装置を取り付けているか。							
	6	秘密保全室内への侵入を感知する自動の警戒・警報装置を取り付けているか。（※）							
	7	警戒・警報装置は、いずれも警備室等と直結し、その配線は容易に切断されないようにし、停電時又は配線切断時にも警報できるか。							
	8	非常時に警備室等外部と通信又は通報ができる機器を取り付けているか。							
9	秘密保全室内を間仕切りした場合、自動の警戒・警報装置（６）及びインターホン等の機器（７）は、間仕切りした部屋ごとに独立して設置されているか。								
第８．境界管理	境界管理について、下欄に掲げる基準をいずれも満たす外柵を設置すること。								
	1	基礎をコンクリートで固定しているか。							
	2	高さ２m以上の金網等を用いて周囲を囲んでいるか。							
	3	上部に有刺鉄線又は赤外線装置等を張り巡らせているか。							
	境界管理について、上記の基準を満たせない場合に下欄に掲げる基準のいずれかを満たしていること。								
	4	上記の基準を満たせない事情及び対象物にかんがみ、境界管理に求められる保全措置（立入制限の実施、警戒・警報装置の設置、警備体制の強化等）を講じているか。							
	4.1	境界を外柵で囲む必要性に乏しい対象物か。							
	4.2	境界は明確に設定されており、管理の措置は明確にされているか。							
	4.2	外柵による境界管理の機能の全部又は一部を補完する措置は十分か。							
	4.3	対象物は、境界と秘密保全施設との間に一定の離隔距離を必要とするか。その場合に、離隔距離は十分か。							
	5	対象物の形状、大きさ、重量などの特性にかんがみ、秘密保全施設が設置された建造物の特性を踏まえ、境界管理に求められる保全措置（立入制限の実施、警戒・警報装置の設置、警備体制の強化等）を講じているか。							
	5.1	対象物は、比較的容易に運搬できる形状、重量か。							
5.2	境界は明確に設定されており、管理の措置は明確にされているか。								
5.3	外柵による境界管理の機能の全部又は一部を補完する措置は十分か。								
第９．保全外部区域	保全外部区域について、下欄に掲げる基準をいずれも満たしていること。								
	1	秘密保全施設の外側に隣接する建物の区画又は敷地のうち必要な範囲を「保全外部区域」として指定していることが配置図等から確認できるか。							
	2	入退者を制限するために、保全外部区域の外側境界に入退口を設置しているか。							
	3	保全外部区域として敷地を指定した場合は、敷地の外周に十分な高さ及び強度のあるフェンス等を設置する等の措置を講じているか（境界管理のために設置された外柵を用いることができる）。							
第１０．保管容器	秘密の種類及び区分に応じた保管容器を準備していること。								
	1 （特別防衛秘密（機密））	三段式文字盤鍵のかかる金庫 ・材質、構造（施錠装置を除く。）等は、日本産業規格S1037に定めるものと同等以上の強度を有しているか。 ・固定式の三段式文字盤鍵と差し込み式錠による二重施錠方式となっているか。 ・ダイヤル及び内蔵式回転板の目盛は、それぞれ100目盛とし、内蔵回転板は、1目盛ごとに任意の番号に調整できる構造で、その実行組み合わせは、100 ³ 以上であるか。 ・触感、音響等による目盛暗探を防止するための構造であるか。							
2 （特別防衛秘密（極秘））	三段式文字盤鍵のかかる鋼鉄製の箱 ・銅板は、日本産業規格G3141に定めるSPCCの標準厚さ1.2mmの銅板を使用した場合に得られる強度以上の強度を有しているか（ただし、棚板、補強板等内部使用銅板は0.8mm以上、裏板は1.0mm以上であるか。）。 ・開き型書庫（両開き書庫及び片開き書庫をいう。）の場合、扉は蝶番が破壊された場合でも扉の開放を防止するための機能を有しているか。 ・施錠装置の内部装置が本体接合部又は本体と扉とのすき間から目視又は触感により探知されないよう金属製覆板を取り付けているか。 ・固定式の三段式文字盤鍵と差し込み式錠による二重施錠方式となっているか。 ・ダイヤル及び内蔵式回転板の目盛は、それぞれ100目盛とし、内蔵回転板は、1目盛ごとに任意の番号に調整できる構造で、その実行組合せは、100 ³ 以上であるか。 ・触感、音響等による目盛暗探を防止するための構造となっているか。								

分 類	番号	項 目	対応状況 (自己評価)	対応内容 (仕様内容を記述した上で、それを確認できる別添資料名を記載)	(別添資料)	現地調査 判定	判定		備考
							担当者	責任者	
第 1 0 . 保管容器	3 (特別防 衛秘密 (秘))	文字盤鍵のかかる銅鉄製の箱 ・本体は、銅板を用いることとし、当該銅板は、日本産業規格G3141に定めるSPCCの標準厚さ0.8mmの銅板を使用した場合に得られる強度以上の強度を有しているか。 ・施錠装置は、文字盤鍵と差し込み式錠による二重施錠方式となっているか。							

備考 1：令和 1 0 年 3 月 3 1 日までの間、特定秘密を取り扱わない秘密保全施設にあっては、第 7（警戒・警報装置）第 1 項及び第 2 項に示す基準を適用しないことができる。
備考 2：令和 1 0 年 3 月 3 1 日までの間、特別防衛秘密を取り扱わない保管庫にあっては、第 7（警戒・警報装置）第 6 項に示す基準を適用しないことができる。

総合判定		改善事項に 対する措置	
------	--	----------------	--

保全基準兼点検票(秘密保全施設、保全外部区域及び保管容器)

事業者名	
事業所名	
秘密保全施設名	
取り扱う秘密の種類	特別防衛秘密を取り扱わない（※変更不可）
施設の用途	
作成日	
確認責任者	

地方防衛局等記入欄
管轄防衛局等
確認日
確認者

防衛装備庁記入欄
確認日
確認担当者
確認日
確認責任者

(特別防衛秘密を取り扱わない場合又は保管庫として使用しない場合)									
分 類	番 号	項 目	対応状況 (自己評価)	対応内容 (仕様内容を記述した上で、それを確認できる別添資料名を記載)	(別添資料)	現地調査 判定	判定		備考
							担当者	責任者	
第1. 天井、壁、床	天井について、下欄に掲げる基準のいずれかを満たしていること。								
	1	頑丈な不燃性の資材（厚さ10cm以上の鉄筋コンクリート、厚さ1.6mm以上の鋼板又は同等の強度を有すると確認されたもの）で堅固に建造されているか。							
	1.1	同等の強度を有すると確認された資材を使用する場合、同等の強度であることを証明できる資料（第三者機関又は資材メーカー等による強度試験結果等）を添付しているか。							
	2	構造上、頑丈な不燃性の資材で堅固に建造できない場合、天井に金網（切断困難な強度を有し、溶接又はボルト等により枠に固定されたもの）を張る、侵入警報装置の設置等で頑丈な不燃性の資材と同等以上の保全措置を講じているか。							
	2.1	同等以上の保全措置となることを説明する資料を添付しているか。							
	壁について、下欄に掲げる基準をいずれも満たしていること。								
	3	頑丈な不燃性の資材（厚さ10cm以上の鉄筋コンクリート、厚さ1.6mm以上の鋼板又は同等の強度を有すると確認されたもの）で堅固に建造されているか。							
	3.1	同等の強度を有すると確認された資材を使用する場合、同等の強度であることを証明できる資料（第三者機関又は資材メーカー等による強度試験結果等）を添付しているか。							
	4	床から天井に到達する壁であるか。							
	天井及び壁について、上記の基準を満たせない場合に下欄に掲げる基準のいずれかを満たしていること。								
	5	（格納庫等のように、特に高い天井高であって、壁（間仕切り）が天井まで届かない構造である場合） 代用天井を設置の上、天井と代用天井との間を金網（切断困難な強度を有し、溶接又はボルト等により枠に固定されたもの）で補強しているか。							
	6	（格納庫等のように、特に高い天井高であり、壁（間仕切り）が天井まで届かず、かつ、代用天井を設置できない場合） 壁（間仕切り）を乗り越えて不法侵入できないように特別の措置を講じているか。							
	6.1	不法侵入が困難であることが証明できる資料（実地検証の結果等）を添付しているか。							
	7	当該施設の天井裏と他の施設の天井裏とが接続している場合には、その境界部を金網等（切断困難な強度を有し、溶接又はボルト等により枠に固定されたもの）の頑丈な不燃性の資材を用いて遮断しているか。							
第2. 出入口、搬入口及び非常口	床について、下欄に掲げる基準を満たしていること。								
	8	頑丈な不燃性の資材（厚さ10cm以上の鉄筋コンクリート、厚さ1.6mm以上の鋼板又は同等の強度を有すると確認されたもの）で堅固に建造されているか。							
	8.1	同等の強度を有すると確認された資材を使用する場合、同等の強度であることを証明できる資料（第三者機関又は資材メーカー等による強度試験結果等）を添付しているか。							
	出入口、搬入口及び非常口について、下欄に掲げる基準をいずれも満たしていること。								
第2. 出入口、搬入口及び非常口	1	出入口（搬入口及び非常口を除く。以下同じ。）は 1 箇所であるか。 （2 箇所以上の出入口は、秘密の取扱い上の必要がない限り認められない。）							
	2	搬入口を設置している場合、（1 の）出入口では機材等の搬入・搬出ができないからか。							
	3	非常口を設置している場合、施設の面積、構造等の観点から、緊急の事態が発生した際の脱出口のために必要最小限の数か。							
	4	非常口を設置している場合、内側からの開閉のみを可能とする構造か。							
	5	出入口の外側上部に照明装置（常夜灯）を取り付けるなど、出入口に接近する者の監視が容易であるか。							
	6	出入口が開放された際に秘密保全施設の外側から内側を直接見えないようになっているか。（例えば、前室を設けているか。出入口の内側に衝立、カーテン等の外側からの視線を妨げるものを設けているか。）							
	7	搬入口が開放された際に外側から内側を直接見えないようになっているか。直接見えるようになっている場合、搬入口を開放する際に外部からの窃視を防ぐための措置が定められているか。							
第3. 扉	出入口、搬入口及び非常口の扉について、下欄に掲げる基準をいずれも満たしていること。								
	1	鋼鉄製又は同等の強度を有すると確認されたものであるか（既存の木造建物等又は既存の建造物の一部を利用して造る出入口又は非常口の扉であって木製等の場合は、鋼板等で補強されているか。）。							
	2	両開きの扉の場合、扉の合せ目に定規ぶちを取り付けているか。							
第3. 扉	3	扉に覗き窓の機能を必要とする場合は、ドアスコープを取り付けて、内側からのみ覗くことができるものとなっているか。							
	出入口の錠について、下欄に掲げる基準をいずれも満たしていること。								
	1	差し込み式錠、生体認証式錠等による二重施錠方式以上の強度であるか。							
第4. 錠	1.1	差し込み式錠は、CP認定錠など、対ピッキング性能などが優れており、容易にこじ開けられない強度を有しているか。							
	1.2	生体認証式錠又は文字盤錠（交換数 1 0 0 の 3 乗以上）以外の錠である場合、これらと同等以上の強度であることを証明する資料を添付しているか。							
	2	扉の非常開閉装置を取り付けているか。							
	搬入口の錠について、下欄に掲げる基準を満たしていること。								
	3	秘密保全施設の内側からのみ解錠できる構造になっているか。							
第4. 錠	4	上記に該当しない場合、外側の錠は、差し込み式錠、生体認証式錠等による二重施錠方式以上の強度であるか。							
	4.1	差し込み式錠は、容易にこじ開けられない強度を有しているか。							
	4.2	生体認証式錠又は文字盤錠（交換数 1 0 0 の 3 乗以上）以外の錠である場合、これらと同等以上の強度であることを証明する資料を添付しているか。							
	非常口の錠について、下欄に掲げる基準を満たしていること。								
第4. 錠	5	秘密保全施設の外側から解錠できない構造になっているか。							
	6	緊急の事態が発生した場合の脱出の容易性を確保した上で、日常的な解錠を回避できる構造になっているか。							

分類	番号	項目	対応状況	対応内容	(別添資料)	現地調査判定	判定		備考	
			(自己評価)	(仕様内容を記述した上で、それを確認できる別添資料名を記載)			担当者	責任者		
第5. 窓	窓について、下欄に掲げる基準を満たしていること。									
	1	無窓であるか								
	上記の基準を満たせない場合、下欄に掲げる資料を用いて秘密保全上の影響がない構造であることを明らかにすること。									
	2	施設における窓の数、位置及び大きさが分かる資料を添付しているか。								
	3	2の資料に、採光、換気等のやむを得ない目的のため必要最小限の数であることがわかる内容が含まれているか。								
	4	2の資料に、鉄格子（日本産業規格、鉄棒直径13mm以上、間隔10cm以下）を堅固に取り付けていることがわかる内容が含まれているか。								
第6. 開口部	開口部（ダクト、通風調節装置、天窓、下水溝、トンネル等）について、下欄に掲げる基準をいずれも満たしていること。									
	1	侵入し得る形状の開口部に金網（切断困難な強度を有し、溶接又はボルト等により枠に固定されたもの）や直径13mm以上の鉄筋を縦及び横に10cm以下の間隔で取り付けられているか。								
	2	開口部からの不法侵入、盗み見、盗聴等の侵害に対応するための措置を講じているか。								
第7. 警戒・警報装置	警戒・警報装置について、下欄に掲げる基準をいずれも満たしていること。									
	1	出入口の外側に監視カメラを取り付け、入退室の状況が監視できるか。（※）								
	2	搬入口の外側に監視カメラを取り付け、搬出入の状況が監視できるか。（※）								
	3	出入口の扉の開閉を感知する自動の警戒・警報装置を取り付けているか。								
	4	搬入口の扉の開閉を感知する自動の警戒・警報装置を取り付けているか。								
	5	非常口の扉の開閉を感知する自動の警戒・警報装置を取り付けているか。								
	6	警戒・警報装置は、いずれも警備室等と直結し、その配線は容易に切断されないようにし、停電時又は配線切断時にも警報できるか。								
第8. 境界	境界管理について、下欄に掲げる基準をいずれも満たす外柵を設置すること。									
	1	基礎をコンクリートで固定しているか。								
	2	高さ2 m以上の高さの金網等を用いて周囲を囲んでいるか。								
	3	上部に有刺鉄線又は赤外線装置等を張り巡らせているか。								
	境界管理について、上記の基準を満たせない場合に下欄に掲げる基準のいずれかを満たしていること。									
	4	上記の基準を満たせない事情及び対象物にかんがみ、境界管理に求められる保安措置（立入制限の実施、警戒・警報装置の設置、警備体制の強化等）を講じているか。								
	4.1	境界を外柵で囲む必要性に乏しい対象物か。								
	4.2	境界は明確に設定されており、管理の措置は明確にされているか。								
	4.2	外柵による境界管理の機能の全部又は一部を補完する措置は十分か。								
	4.3	対象物は、境界と秘密保全施設との間に一定の離隔距離を必要とするか。その場合に、離隔距離は十分か。								
	5	対象物の形状、大きさ、重量などの特性にかんがみ、秘密保全施設が設置された建造物の特性を踏まえ、境界管理に求められる保安措置（立入制限の実施、警戒・警報装置の設置、警備体制の強化等）を講じているか。								
	5.1	対象物は、比較的容易に運搬できる形状、重量か。								
	5.2	境界は明確に設定されており、管理の措置は明確にされているか。								
	5.3	外柵による境界管理の機能の全部又は一部を補完する措置は十分か。								
第9. 保全外部区域	保全外部区域について、下欄に掲げる基準をいずれも満たしていること。									
	1	秘密保全施設の外側に隣接する建物の区画又は敷地のうち必要な範囲を「保全外部区域」として指定していることが配置図等から確認できるか。								
	2	入退者を制限するために、保全外部区域の外側境界に入退口を設置しているか。								
	3	保全外部区域として敷地を指定した場合は、敷地の外周に十分な高さ及び強度のあるフェンス等を設置する等の措置を講じているか（境界管理のために設置された外柵を用いることができる）。								
第10. 保管容器	秘密の種類及び区分に応じた保管容器を準備していること。									
	1 (特定秘密)	三段式文字盤鍵のかかる鋼鉄製の箱 ・鋼板は、日本産業規格G3141に定めるSPCCの標準厚さ1.2mmの鋼板を使用した場合に得られる強度以上の強度を有しているか（ただし、棚板、補強板等内部使用鋼板は0.8mm以上、裏板は1.0mm以上であるか。）。 ・開き型書庫（両開き書庫及び片開き書庫をいう。）の場合、扉は蝶番が破壊された場合でも扉の開放を防止するための機能を有しているか。 ・施錠装置の内部装置が本体接合部又は本体と扉とのすき間から目視又は触感により探知されないよう金属製覆板を取り付けているか。 ・固定式の三段式文字盤鍵と差し込み式錠による二重施錠方式となっているか。 ・ダイヤル及び内蔵式回転板の目盛は、それぞれ100目盛とし、内蔵回転板は、1目盛ごとに任意の番号に調整できる構造で、その実行組合せは、100 ³ 以上であるか。 ・触感、音響等による目盛暗探を防止するための構造となっているか。								
	2 (装備品等秘密)	文字盤鍵のかかる鋼鉄製の箱 ・本体は、鋼板を用いることとし、当該鋼板は、日本産業規格G3141に定めるSPCCの標準厚さ0.8mmの鋼板を使用した場合に得られる強度以上の強度を有しているか。 ・施錠装置は、文字盤鍵と差し込み式錠による二重施錠方式となっているか。								

備考 1：秘密の取扱いに関する契約申込書等を提出した日の前日までに秘密保全施設としての構造等が適当であると認められた秘密保全施設については、第 7（警戒・警報装置）第 1 項及び第 2 項に示す項目を除き、上記の各項目に示す基準を満たしているとなすことができる。

備考 2：令和 1 0 年 3 月 3 1 日までの間、特定秘密を取り扱わない秘密保全施設にあつては、第 7（警戒・警報装置）第 1 項及び第 2 項に示す基準を適用しないことができる。

総合判定		改善事項に対する措置	
------	--	------------	--

項目	番号 ※ 1	保全基準	経過措置等 該当項目 ※ 2	対応状況 （自己評 価）※ 3	対応文書 （秘密保全規則、 システム実装計画、 その他の文書）	対応内容 （規定を抜粋又は要約）	直近の対応 （確認）日	（地方局） 現地調査 判定※ 4	（装備庁） 判定※ 4		備考	
									担当者	責任者		
第 1 0 . 構成管理	秘密取扱情報システム管理者は、セキュリティエンジニアリングの原則の適用について、以下のことを定め、実施していること。											
	1	秘密取扱情報システムを設計、開発、導入及び変更する場合には、セキュリティエンジニアリングの原則（情報システムの企画から設計、開発、運用に至るまでの全ての工程において、セキュリティを確保する方策をいう。）により実施しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者）	該当									
	秘密取扱情報システム管理者は、構成設定等について、以下のことを定め、実施していること。											
	②	構成設定目録は、秘密保全規則等と整合的であり、秘密取扱情報システムの構成要素の機能（秘密取扱情報システムに実装されるポート、プロトコル及びサービスを含む。）及び動作（ソフトウェアによるものを含む。）を業務遂行上の必要最小限に制限しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	③	構成設定を実施する手順を作成しているか。	該当									
	④	秘密取扱情報システムの構成要素は、構成設定を実施する手順及び構成設定目録に従って、秘密取扱情報システム管理者が設定しているか。	該当									
	⑤	構成設定を実施するための物理的・論理的なアクセス権限は、当該アクセス権限を付与された業務を行うべき者に限るなど、必要最小限の範囲に限定しているか。										
	秘密取扱情報システム管理者は、構成設定目録の変更等についての手順を作成し、以下のことを定め、実施していること。											
	⑥	構成設定目録の内容を定期的（スタンドアロン方式でない場合（複数の端末を接続してネットワークを構成する場合）には 3 か月に 1 回以上を基準）に点検しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	⑦	点検により不備が判明した場合、及びぜい弱性に対処し、又は業務上必要な機能の変更に伴い秘密取扱情報システムの構成要素の構成設定を変更した場合には、構成設定目録を変更しているか。										
	⑧	構成設定を変更する場合及び特段の事情により特別（例外的）な構成設定を行う場合には、当該構成設定が秘密保全規則等に反しないことを確認するとともに、秘密取扱情報システムのセキュリティに及ぼす影響を事前に分析し、問題が無いことを確認した上で実施しているか。										
第 1 1 . 情報システムの基本的防御	秘密取扱情報システム管理者は、ホワイトリストについて、以下のことを定め、実施していること。											
	⑨	ホワイトリストを、個別の構成要素ごとに、及び業務上使用するソフトウェアを網羅して作成し、定期的（1 年に 1 回以上を基準）に、及び秘密取扱情報システムに変更が生じた場合など必要と認める場合に精査し、更新しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）	該当									
	⑩	秘密取扱情報システムは、ホワイトリストに掲載されたソフトウェアのみをインストールし、及び実行することが可能となるように設定されているか。	該当									
第 1 1 . 情報システムの基本的防御	秘密取扱情報システム管理者は、秘密取扱情報システムの構成設定及びデータ管理について、以下の基本的事項を定め、実施していること。											
	①	秘密取扱情報システムのネットワークは、秘密保全施設等内において有線により構成要素が配線接続されているか（他の情報システム又は秘密取扱情報システムが設置された秘密保全施設等の外部との通信は、完全に遮断されているか）。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	②	秘密取扱情報システムは、無線 LAN の機能が無効化されていること又は無線 LAN の機能を有していないことを確認したか。										
	③	メンテナンス等による一時的な接続を除き、秘密取扱情報システム以外の情報システムとの接続は禁止されているか。										
	④	秘密取扱情報システムに内蔵する記憶媒体に、秘密のデータを保存していないか（秘密のデータは秘密可搬記憶媒体にのみ保存しているか。）。										
	秘密取扱情報システム管理者は、秘密取扱情報システムの操作手順書について、以下のことを定め、実施していること。											
	⑤	秘密取扱情報システム利用者による不適切な操作がセキュリティに悪影響を及ぼすことを防ぐため、秘密取扱情報システムの利用に当たっての手順、セキュリティ上遵守すべき事項等を明記した操作手順書を作成しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	⑥	操作手順書には、パスワード設定に関する以下の項目を含んでいるか。 ア 利用者にパスワードの変更手順を理解させること。 イ 利用者にパスワードの変更を実施させること。 ウ パスワードは、推測されにくいものとする。 エ 利用者が画面上の表示を確認しつつ設定することのできる機能を有すること。 オ ログオン及びユーザーセッションに関すること。										
	⑦	操作手順書は、秘密取扱情報システム利用者が秘密取扱情報システムを利用する際に参照することが可能な状態になっているか。										
	秘密取扱情報システム管理者は、その他の基本的防御対策について、以下のことを定め、実施していること。											
	⑧	秘密取扱情報システムにソフトウェアをインストール又はアップデートする場合は、あらかじめその有効性や副作用の可能性を分析及び評価し、必要かつセキュリティ上適切と認められる場合に限り実施しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
⑨	セキュリティ上のアップデートが必要な場合は、アップデートが利用可能となつてから定められた期間内（スタンドアロン方式でない場合（複数の端末を接続してネットワークを構成する場合）には 1 か月を基準）にアップデートしているか。											
⑩	秘密取扱情報システムの機能を、システムの管理者用機能と利用者用機能を分離しているか。											
⑪	管理者権限を持たない秘密取扱情報システム利用者による管理者用機能の不正利用を防ぐための防止策を講じているか（管理者権限以外での読み取り・実行を不可能とする設定）。	該当										
⑫	仮想化技術を利用して複数の仮想コンピュータを構築する場合は、当該仮想コンピュータ間で不正な又は意図しない移動やデータリソースへのアクセスを防止する措置及び対策をしているか。	該当 S A										

項目	番号 ※ 1	保全基準	経過措置等 該当項目 ※ 2	対応状況 （自己評 価）※ 3	対応文書 （秘密保全規則、 システム実装計画、 その他の文書）	対応内容 （規定を抜粋又は要約）	直近の対応 （確認）日	(地方局) 現地調査 判定※ 4	(裝備庁) 判定※ 4		備考	
									担当者	責任者		
第 1 4 . システム 監視	秘密取扱情報システム管理者は、システム監視について、以下のことを定め、実施していること。											
	①	秘密取扱情報システムにおける不正なアクセス及び変更、アカウント及び権限の不正な使用、不正な通信並びに悪意のあるコード等（以下「不正なアクセス等」という。）の検知のため、秘密取扱情報システムの構成設定に応じ、必要な情報の収集を行うための機器の設置、ソフトウェアのインストール等を実施し、又は他の方法により、以下の事項について秘密取扱情報システムの運用状況の監視（以下「システム監視」という。）を実施しているか。（なお、ウは、スタンドアロン方式でない場合（複数の端末を接続してネットワークを構成する場合）に限り要する。） ア 不正な相手方又は方法等によるアクセス イ 権限（利用者権限、管理者権限）の不正な使用 ウ 秘密取扱情報システム内部の不正な操作による不正な通信 エ 悪意のあるコードの秘密取扱情報システムへの侵入 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	②	内部の兆候、外的な状況変化に関する情報を収集・分析し、システム監視体制や監視範囲を適切に見直しているか。										
	秘密取扱情報システム管理者は、システム監視の実施方法について、以下のことを定め、実施していること。											
	③	悪意のあるコードの侵入の監視は、秘密取扱情報システムを構成するサーバ及びパソコンにおける悪意のあるコードを検知するためのソフトウェア（以下「検知ソフトウェア」という。）をインストールしているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	④	検知ソフトウェアとして、未知の脅威にも対応できるよう、ヒューリスティックエンジン等の高度な手法を活用可能なソフトウェアをインストールしているか。	該当 S A									
	⑤	検知ソフトウェア又はウイルス定義ファイルのアップデート版が提供された場合において、有効性や副作用の可能性を分析及び評価し、アップデートを実施することが必要かつ適切と認められるときは、定められた期間（ 1 か月以内を基準）にアップデートを行っているか。										
	⑥	悪意のあるコードを検知するため、秘密取扱情報システムに対する検知ソフトウェアによるフルスキャンを定期的（スタンドアロン方式でない場合（複数の端末を接続してネットワークを構成する場合）には 1 週間に 1 回以上を基準）に実施しているか。										
	⑦	一定の期間（スタンドアロン方式でない場合（複数の端末を接続してネットワークを構成する場合）には 1 週間以上を基準）電源の切断された状態にある秘密取扱情報システム及び秘密可搬記憶媒体については、再度の電源投入時にフルスキャンを実施しているか。										
	⑧	検知ソフトウェアにより、秘密取扱情報システムにおけるファイルのダウンロード、開封及び実行の都度、当該ファイルに対し、悪意のあるコードを検知するためのリアルタイムスキャンをしているか。										
	秘密取扱情報システム管理者は、不正なアクセス等を検知した際の対応について、以下のことを定め、実施していること。											
	⑨	検知ソフトウェアにより悪意のあるコードを検知した場合は、検知ソフトウェアによる誤検知の可能性を検証した上でブロック、隔離、若しくは削除又はそれらを組み合わせた措置を実施しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者）										
	秘密取扱情報システム管理者は、システム監視により取得した情報の利用及び保管について、以下のことを定め、実施していること。											
	⑩	システム監視により取得した情報を事故等への対処などに利用するものとし、秘密取扱情報システム管理者は、取得した情報を確認、承認し、関係部署等に通知しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	⑪	システム監視により取得した情報を文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存しているか。										
第 1 5 . システム ログ	秘密取扱情報システム管理者は、システムログの取得及び分析について、以下のことを定め、実施していること。											
	①	秘密取扱情報システムにおける不正な操作や通信を探知するため、以下の事項に係る記録をシステム上で自動的に取得しているか。 ア 秘密のデータへの動作の内容 （ファイルの作成・編集・削除、印刷、秘密可搬記憶媒体への書き出し等） イ 秘密取扱情報システム利用者ごとの操作内容 （利用者ID、ログオン及びログオフの日時、アクセス者の端末ID、アクセスされたファイル及び使用されたプログラム等） （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	②	上記のほか、秘密取扱情報システムの特性に応じ、秘密取扱情報システムにおける不正な操作や通知を探知するために必要となるシステムログの内容を検討し、その取得に係る対象及び方法が含まれているか。	該当 S A									
	③	システムログの取得に失敗した場合は、秘密取扱情報システム上に記録され、秘密取扱情報システム担当者等に対しアラートを発しているか。	該当 S A									
	④	システムログの内容並びにその取得に係る対象及び方法は、定期的（ 1 年に 1 回以上）に、及びシステムログの取得に失敗した場合その他必要と認められた場合に精査し、必要に応じて変更しているか。										
	⑤	定期的（スタンドアロン方式でない場合（複数の端末を接続してネットワークを構成する場合）には 1 週間に 1 回以上）にシステムログの分析を実施するものとし、分析を行う場合は、秘密取扱情報システム構成要素から取得したシステムログを集約し、全体的かつ横断的に分析しているか（反復継続性に乏しい特異な事象、秘密取扱情報システム利用者による異常な操作、システムの異常な挙動等の有無、過去の事故等との類似性等）。	該当									
	⑥	システムログの分析を行った場合は、その結果を記録したシステムログ分析結果記録簿（付紙様式第33（基準））を作成し、速やかに総括者その他必要な者に報告しているか。										
	⑦	システムログの分析に係る結果を記録した文書の作成においては、システムログの内容（時刻の順序を含む。）が変更できない措置が講じられているか。	該当 S A									
	⑧	システムログを取得するツールを、不正なアクセス、改ざん、削除等から保護しているか。										
	秘密取扱情報システム管理者は、システムログの管理について、以下のことを定め、実施していること。											
	⑨	システムログの取得及び分析に関わる秘密取扱情報システムの設定を行うために必要なアクセス権限を、必要な者に限定して付与しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	⑩	システムログ及びその分析の結果の記録は、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、秘密取扱情報システム管理者及び秘密取扱情報システム担当者以外にアクセスされないように設定するとともに、5 年間保管又は保存しているか。										
	秘密取扱情報システム管理者は、システムログにタイムスタンプを付与する要領について、以下のことを定め、実施していること。											
	⑪	システムログに対し、秘密取扱情報システムの内部におけるシステムクロックを利用して、タイムスタンプ（日本標準時（JST）を基準とし、これにより難しい場合は協定世界時（UTC）又はグリニッジ標準時（GMT）を基準とした時刻表記で統一）を付与しているか。利用するシステムクロックの時刻補正を行っているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。）	該当									
第 1 6 . ぜい弱 性スキャン等	秘密取扱情報システム管理者は、ぜい弱性スキャンについて、以下のことを定め、実施していること。											
	①	秘密取扱情報システム全体に対するぜい弱性スキャンを定期的（スタンドアロン方式でない場合（複数の端末を接続してネットワークを構成する場合）には 1 か月に 1 回以上）に実施し、その結果を分析しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）	該当									
	②	社内からの情報に加え、専門的な外部機関（以下単に「外部機関」という。）が発信するぜい弱性情報等に係る注意喚起及び助言等の情報を継続的に収集し、当該ぜい弱性が秘密取扱情報システムに対し影響を与える可能性があると認められる場合に、秘密取扱情報システム全体に対し当該ぜい弱性に係るぜい弱性スキャンを実施し、その結果を分析しているか。	該当									
	③	ぜい弱性スキャンの分析の結果を記載したぜい弱性スキャン分析結果記録簿（付紙様式第34（基準））を作成しているか。	該当									
	秘密取扱情報システム管理者は、ぜい弱性スキャンの分析結果等の利用について、以下のことを定め、実施していること。											
	④	自社における秘密取扱情報システム以外の情報システムにおけるぜい弱性の発見及び修正等に資するため、ぜい弱性スキャン結果の分析など脆弱性の発見に資する情報を自社の必要な者及び組織に共有しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）	該当									
	⑤	外部機関から収集した情報に基づき、秘密取扱情報システム担当者、秘密取扱情報システム利用者等に対し、注意喚起及び助言をしているか。	該当									
⑥	ぜい弱性が特定された場合は、秘密取扱情報システムぜい弱性対処記録（付紙様式第22（基準））を作成し、定められた期間内（ 1 か月を基準）に対処しているか。	該当										

項目	番号 ※ 1	保全基準	経過措置等 該当項目 ※ 2	対応状況 (自己評 価) ※ 3	対応文書 (秘密保全規則、 システム実装計画、 その他の文書)	対応内容 (規定を抜粋又は要約)	直近の対応 (確認) 日	(地方局) 現地調査 判定 ※ 4	(装備庁) 判定 ※ 4		備考	
									担当者	責任者		
第 1 7 . バックアップ	秘密取扱情報システム管理者は、秘密取扱情報システムのシステムログに関するバックアップの手順において、以下のことを定め、実施していること。											
	①	秘密取扱情報システムのシステムログ（事故等の分析に必要なシステムデータを含む。）のバックアップに関する手順を定めているか（バックアップデータを利用した復旧手順を含むこと）。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）	該当 S A									
	②	システムログのバックアップに関する手順は、以下の事項が考慮されているか。 ア 定期的（1 か月に 1 回以上）に実施すること。 イ バックアップデータは、システムの復旧、事故等に伴うシステムログの分析等に際して利用されることを考慮した期間保存されること。 ウ バックアップは、自社が定めた秘密取扱情報システムの目標復旧時間に対応した頻度で行うこと。 エ バックアップされたデータの機密性、完全性及び可用性を確保すること（バックアップデータを保管する拠点や場所を保護していること。）。	該当 S A									
	③	システムログのバックアップに関する手順に従い、定期的にバックアップを実施し、バックアップ実施等記録簿（付紙様式第35（基準））を作成しているか。	該当 S A									
第 1 8 . メンテナンス等	秘密取扱情報システム管理者は、メンテナンス等計画について、以下のことを定め、実施していること。											
	①	秘密取扱情報システムのメンテナンス等（保守、点検、診断、修理、整備及びアップグレードを含む。以下同じ。）の実施のため、以下の事項を定めた計画（以下「メンテナンス等計画」（付紙様式第36（基準））という。）を作成しているか。 ア メンテナンス等を実施する人員 イ メンテナンス等の対象（ソフトウェア、ハードウェア及びファームウェアを含む。） ウ メンテナンス等の内容（メンテナンス等に使用される機器及びツールを含む。やむを得ず持ち出す場合は、秘密の漏えいを防止するための措置を講じること。） エ その他メンテナンス等に必要な事項（メンテナンス等の実施及び記録に規定する措置を実施するために必要な事項） （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	②	メンテナンス等計画に従い、秘密取扱情報システムのメンテナンス等を定期的に、及びその必要が認められたときに行っているか。										
	秘密取扱情報システム管理者は、メンテナンス等の実施について、以下のことを定め、実施していること。											
	③	メンテナンス等を実施する前に、メンテナンス等により影響を受けることが予測される事象についてのセキュリティ対策を実施しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）										
	④	メンテナンス等の実施者について、秘密取扱情報システム利用者の中から、業務の遂行上必要最小限度の範囲であることを確認した上で指定しているか。										
	⑤	秘密取扱情報システム利用者以外の者（外部委託）によるメンテナンス等の実施は、原則として禁止し、やむを得ず外部委託しなければならない場合には、総括者は、少なくとも以下の事項を講じているか。 ア 外部委託を受ける者との間において、秘密保全のために必要な契約を締結すること等により、秘密保全上の注意点及び要求事項を明示的に義務付けること。 イ 外部委託を受ける者は、防衛省が、秘密取扱情報システムが設置されている秘密保全施設への立入りを事前に許可した者に限ること。 ウ 外部委託を受ける者によるメンテナンス等に当たっては、秘密取扱情報システムから秘密のデータを消去した後に行わせることとするほか、秘密保全施設内において管理されている他の秘密に接することのないよう措置を講じること。										
	⑥	メンテナンス等の監督について、以下の措置を講じているか。 ア 秘密取扱情報システム利用者の中から技術的な知見を有する者を監督者として指定していること。 イ 監督者をメンテナンスの場に立ち合わせ、メンテナンス等の実施状況を監督させていること。 ウ 監督者に監督結果、秘密保全上の注意点及び要求事項の順守状況等について速やかに報告させていること。										
	⑦	メンテナンス等の実施に当たり、以下の措置を講じているか。 ア メンテナンス等を実施する人員が秘密取扱情報システムにアクセスする際に、ログオン時と同様の多要素認証を求めること。 イ 秘密取扱情報システム管理者が承認した適切な検査されたツール（診断ツールやテストプログラムが保存された記憶媒体を含む。）のみ使用させること。 ウ メンテナンス等計画に記載された機器のみメンテナンス等に使用させること。	該当 S A									
	⑧	秘密取扱情報システムのメンテナンス等を実施した後に、当該セキュリティ対策がメンテナンス等の実施前と同様に適切に機能していることを確認しているか。										
	秘密取扱情報システム管理者は、メンテナンス等の記録について、以下のことを定め、実施していること。											
	⑨	監督者は、メンテナンス等を実施した日時、人員の名簿（国籍等を記載）、実施の対象及び内容をメンテナンス等実施記録（付紙様式第37（基準））により作成し、秘密取扱情報システム管理者の確認を得ているか。 （実施者：監督者、承認者：秘密取扱情報システム管理者）										
	⑩	メンテナンス等の記録は、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、5年間保管又は保存しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者）										
第 1 9 . サプライチェーン・リスク	秘密取扱情報システム管理者は、サプライチェーン・リスクについて、以下のことを定め、実施していること。											
	1	秘密取扱情報システムの構成要素及び可搬記憶媒体に関するサプライチェーン・リスクを管理するための方針、サプライチェーン・リスク管理計画及びサプライチェーン・リスクに関する管理策を実施するための実施手順（以下、本項目において「方針等」という。）を作成し、必要に応じて更新しているか。 （実施者：秘密取扱情報システム担当者、承認者：総括者）	該当									
	②	秘密取扱情報システムを整備し、及び可搬記憶媒体を調達するに当たっては、方針等に基づき、その構成要素のサプライチェーン・リスクを予防、特定、弱点等による被害又は影響を極限しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）	該当									
	③	方針等に基づき選定した秘密取扱情報システムの構成要素について、必要な来歴を作成及び更新し、そのサプライチェーン・リスクを予防、特定し、弱点等による被害又は影響を極限する措置を講じているか。	該当									
総合判定												

※ 1 ○で囲んだ番号は情報システムごとに点検するものを表し、○で囲んでない番号は事業所ごとに点検するものを表している。

※ 2 (1)「該当」：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（装装保第 14846 号。令和 7 年 7 月 31 日）別紙第 1 第 2 1 第 5 項の規定の適用を受ける事業者については、継続的な確認の実施を行うに当たり、該当する保全基準を適用しないことができる。

(2)「S A」：スタンドアロン方式の情報システム（複数の端末を接続してネットワークを構成する場合をいう。）については、該当する保全基準を適用しないことができる。

※ 3 防衛事業適合事業者契約の申込み時は、原則として、「対応済、対応予定、一部対応（代替策）、対応困難（代替策）、非該当、その他」から選択するものとし、点検時には、「実施済、未実施、その他」から選択するものとする。

「対応予定」については、対応する時期が定まっている場合が該当する。この場合には、対応する時期を明記するものとする。

「一部対応（代替策）」については、該当する保全基準の一部を満たせない場合が該当する。

「対応困難(代替策)」については、試験、計測、解析又は性能評価を目的に専用に整備された秘密取扱情報システムであって、その仕様上、該当する保全基準の実装が著しく困難であるか、著しく非合理的であるものが該当する。これらの場合には、その理由を示し、当該保全基準を実装しないことにより生じ得るリスクを特定し、当該保全措置を講じないことに対する代替策を講じ又は代替策の考え方を示した上で、代替策の妥当性について調整するものとする。

「非該当」については、秘密取扱情報システムにおいて実際に取り扱われる秘密のデータの取扱いの特性上、該当する保全基準を適用できないことが自明である場合をいう。

「その他」については、具体的な状況を明記するものとする。

※ 4 防衛事業適合事業者契約の申込み時は、原則として、「適合、条件付適合、不適合、非該当」から選択するものとし、点検時には「良好、要改善、不良」から選択するものとする。

保全基準兼点検票（秘密取扱情報システム）（拡張管理策（第 1 1 条第 3 項及び第 1 3 条第 5 項関係））

点検対象期間											
点検日											
事業者名											
システム名称											
作成日											
作成者											
確認日											
総括者											

地方防衛局等記入欄		防衛装備庁記入欄	
管轄防衛局等		確認日	
確認日		確認担当者	
確認者		確認日	
		確認責任者	

項目	番号 ※ 1	保全基準	対応状況 （自己評価）※ 2	対応文書 （秘密保全規則、 システム実装計画、 その他の文書）	対応内容 （規定を抜粋又は要約）	直近の対応 （確認）日	(地方局) 現地調査 判定※ 3	(装備庁) 判定※ 3		備考
								担当者	責任者	
第 1．秘密保全 規則等の取扱い	－									
第 2．組織のセキュリティ	－									
第 3．人的セキュリティ	総括者は、秘密情報セキュリティ教育及び訓練について、以下のことを定め、実施していること。									
	1	教育及び訓練は、秘密取扱情報システムに適用するセキュリティ管理策を理解するために十分な専門性（①不審な通信及び異常動作、②最新のサイバー攻撃に関する内容、③緊急時対応計画における自身の役割、④現実にも即した事故等訓練）のある内容であるか。 （①及び②については、外部委託により実施することを含む。） （実施者：秘密取扱情報システム管理者、承認者：総括者。以下、本項目において同じ。）								
	2	秘密取扱情報システム管理者及び秘密取扱情報システム担当者に対し、消火設備（消火器、屋内消火栓、スプリンクラー等）、空気調和設備（自動制御設備、換気設備、排煙設備等）、電気通信設備（動力設備、幹線設備、構内配電設備、構内情報通信網設備等）の非常時の使用方法に関する教育（例：消火器の使用手法、扉の緊急解放法等）を定期的（１年に１回以上を基準）に実施しているか。								
	総括者は、秘密のデータの管理について、以下のことを定め、実施していること。									
第 4．秘密のデータの分類及び管理	1	防衛関連の情報をホームページ、刊行物、ソーシャルネットワーキングサービスに公開する場合には、公開に先立って、当該情報の中に秘密のデータが含まれていないことを確認しているか。また、公開済みの情報に注意を払い、インターネット上に秘密のデータが流出していないことを常続的に確認しているか。 （実施者：秘密取扱情報システム管理者、承認者：総括者。以下、本項目において同じ。）								
	秘密取扱情報システム管理者は、秘密のデータ及びサーバの廃棄について、以下のことを定め、実施していること。									
	②	秘密のデータを廃棄する場合には、秘密のデータが復元できない状態（データ消去ソフトウェアによる消去を実施し、データ復元ソフトウェアを使用してデータが検出されない状態をいう。以下、本項目において同じ。）であることを点検した上で、記録しているか。								
	③	秘密のデータの廃棄の状況について、秘密のデータを復元できない状態とし、又は秘密のデータを廃棄した者とは別の者が点検しているか。								
	④	サーバを廃棄する場合には、秘密のデータが復元できない状態であることを点検した上で、サーバを物理的に破壊し、その旨を記録しているか。								
	⑤	サーバを再利用していないか（秘密のデータの取扱いが終わった時点で、秘密保全規則等に基づき確実に廃棄しているか）。								
	⑥	サーバの廃棄の点検の記録は、廃棄を実施した者の氏名、所属及び所在等、実施時刻並びに実施完了の証明となる資料（署名等）について、記載又は添付し、保管しているか。								
	⑦	サーバの廃棄の状況について、秘密のデータを復元できない状態とし、又はサーバを破壊した者とは別の者が点検しているか。								
	8	意図したとおり秘密のデータが復元できない状態になることを確実に実施するため、定められた頻度（１年に１回以上を基準）で、データ消去ソフトウェア、データ復元ソフトウェア及び廃棄の手順を確認しているか。								
第 5．物理的及び環境的セキュリティ	秘密取扱情報システム管理者は、秘密取扱情報システムに対する物理的セキュリティ対策について、以下のことを定め、実施していること。									
	①	秘密のデータは、暗号化した上でサーバに保管しているか（秘密可搬記憶媒体で保管することが適切な秘密のデータを除く。）。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）								
	②	パソコンは、秘密のデータの保管に関して最小限の機能だけを持つ端末（例：シンクライアント端末）としているか。								
	③	サーバは、秘密の種類及び区分に応じた保管容器と同等以上の機能及び構造を有するサーバラックにより保護しているか。								
	④	秘密保全施設等内のケーブル（電気ケーブル、光ケーブル、LANケーブル）は、偶発的な損傷、中断、物理的な改ざんを防止するため、他のケーブルから明確に区別した上で、建物の構造（床下配線）、配線ダクト等により保護しているか。								
	⑤	同一の建造物であって秘密保全施設等を跨ぐ場合のケーブル（電気ケーブル、光ケーブル、LANケーブル）は、偶発的な損傷、中断、物理的な改ざんを防止するため、他のケーブルから明確に区別した上で、建物の構造（通信管路）又は金属製の配線ダクト（穴なしタイプ）により保護しているか。								
	⑥	同一敷地内の建造物を跨ぐケーブルについては、他のケーブルから明確に区別した上で、以下の全ての保護措置を実施しているか。なお、周辺の建造物の規模・形状、周辺の地形・障害物等により、当該保護措置の基準を満たせない場合には、同等以上の保護措置を講ずること。 ア 電磁的な情報漏えいに対する保護措置を実施していること（例：光ケーブル） イ 通信管路又は金属製の配線ダクト（穴なしタイプ）による保護措置を実施していること ウ 地下に埋設していること								
	⑦	鍵のかかる配電盤や配線盤を使用しているか。								
	⑧	無停電電源装置は、鍵のかかるラックに入れているか。								
	⑨	サーバに無停電電源装置を据え付けているか。								
	⑩	停電時又は電力途絶時に点灯し、秘密保全施設等内の非常口及び避難経路を照明する非常用自動照明を整備しているか。								
	⑪	サーバが設置されている秘密保全施設等については、停電時にも無停電電源装置等の予備電源により動作する火災検知及び消火システムを整備しているか。								
	⑫	サーバを設置している秘密保全施設等内の温度、湿度、空気清浄度等の環境管理基準を定めているか。								
	⑬	秘密保全施設等内の環境管理基準の適合状況を継続的に確認しているか。								
	⑭	サーバに書及ぼすおそれのある環境の変動を防ぐために、サーバが設置されている秘密保全施設等については、自動的な環境制御機器（温度、湿度等を検知し、その値に応じて自動で冷却・加湿・換気等を行う機器をいう。）を導入しているか。								
	⑮	水の流れを遮断するための主遮水弁（バルブ）を秘密取扱情報システム管理者及び秘密取扱情報システム担当者に周知し、消火設備や上下水道の故障による水漏れから秘密取扱情報システムを保護しているか。								
	⑯	秘密取扱情報システム管理者が定める秘密取扱情報システム構成要素（例：サーバ、パソコン、ネットワーク装置、セキュリティ装置等）については、秘密取扱情報システムであることを標示しているか。								
⑰	出力機能を有する秘密取扱情報システム構成要素（プリンター等）については、不正な出力を防止するため、利用者認証等の機能を実装しているか。									

項目	番号 ※ 1	保全基準	対応状況 (自己評価) ※ 2	対応文書 (秘密保全規則、 システム実装計画、 その他の文書)	対応内容 (規定を抜粋又は要約)	直近の対 応(確認) 日	(地方局) 現地調査 判定※ 3	(整備庁) 判定※ 3	備考
第 6. 秘密のデータの漏えい等の事故等発生時の対応	総括者は、秘密のデータの漏えい等に関する事故等発生時への対応について、以下のことを定め、実施していること。								
	①	シーサート（CSIRT）を設置し、及び維持しているか（外部からのリモート対応不可）。 （実施者：秘密取扱情報システム管理者、承認者：総括者。以下、本項目において同じ。）							
	②	セキュリティオペレーションセンター（SOC）を設置し、及び維持しているか（外部からのリモート対応不可）。							
	3	事故等対処手順と業務継続計画との整合性を確保しているか。							
	④	自社が導入しているセキュリティツール（フォレンジックツール、構成管理ツール、資産管理ツール、I A M ツール（識別及びアクセス管理ツール）、システム監視ツール、システムログ取得分析ツール、ぜい弱性スキャンツール、メンテナンスツール等）により、事故等対処の支援（ユーザー支援含む。）を自動化しているか。							
	⑤	事故等対処に当たり、秘密取扱情報システムの構成要素のサプライチェーンに関わるぜい弱性が確認された場合は、当該サプライチェーンを構成する事業者に当該ぜい弱性を共有しているか。							
	6	ヘルプデスク等を設置し、秘密取扱情報システム利用者に対して、事故等に関する必要な情報を提供しているか。							
	7	事故等の対処に当たり、必要に応じて専門的な外部機関を含めた調査・分析ができるよう準備しているか。							
	⑧	セキュリティツールからの検知に加えて、自ら能動的に秘密取扱情報システムに脅威が存在することを前提として、専門的な知識やセキュリティツールを活用・分析して潜在的な脅威、事故等を洗い出す活動（脅威ハンティング）を継続的に実施しているか（外部からのリモート対応不可）。							
	⑨	事故等の発見時及び検知時の報告に当たり、自動化された仕組みを使用し、2 4 時間 3 6 5 日、関係者に通知する体制をとっているか。							
	総括者は、秘密取扱情報システムの可用性を維持するための緊急時対応計画について、以下のことを定め、実施していること。								
	⑩	秘密取扱情報システム障害時の対応を適切に実施するため、以下の事項を含めた緊急時対応計画を整備しているか。 ア 対象となる秘密取扱情報システム・業務の範囲（重要度分析の結果を反映） イ 復旧目標、復旧優先順位及び復旧の評価指標 ウ 緊急時対応の役割、職責及びこれを割り当てられた個人及びその連絡先 エ 秘密取扱情報システムに妨害、侵害又は障害が発生したとしても必要不可欠な業務を継続するための方策 オ 秘密取扱情報システムを完全に復旧させるための方策 カ 緊急時対応計画の共有範囲及び要領 （実施者：秘密取扱情報システム管理者、承認者：総括者。以下、本項目において同じ。）							
	⑪	緊急時対応計画は、定期的（1 年に 1 回以上を基準）に、及び組織体制や秘密取扱情報システムに変更が生じるなど必要と認める場合には、内容を精査し、必要に応じ、更新しているか。							
	⑫	緊急時対応計画は、関係者に周知しているか。							
	⑬	緊急時対応時に実施した措置から学んだ教訓を踏まえ、教育及び訓練に反映しているか。							
	⑭	緊急時対応計画の複製は、業務上の必要最小限とし、報告先を管理した上で、必要な保全措置を行っているか。							
第 7. リスク査定	総括者は、リスク査定について以下のことを定め、実施していること。								
	①	リスク査定を行う項目を設定するに当たっては、拡張管理策(1-5-2)第 1 0（構成管理）②で実施する重要度分析の結果（重要な秘密取扱情報システム構成要素及び機能を特定）を考慮しているか。 （実施者：秘密取扱情報システム管理者、承認者：総括者。以下、本項目において同じ。）							
	2	外部に存在するサイバー攻撃に関する脅威を継続的に把握し、必要に応じて、速やかにリスク査定を実施することにより、脅威環境を判断しているか。							
第 8. 点検	－								
第 9. 秘密取扱情報システムセキュリティ実装計画	総括者は、秘密取扱情報システムセキュリティ実装計画及び行動規則の作成等について、以下のことを定め、実施していること。								
	①	秘密取扱情報システムを使用した業務内容及び秘密取扱情報システムにおける秘密のデータの流れを正確に反映したデータフロー図を作成するため、データフロー制御に関する方針（以下「データフロー制御方針」という。）を策定し、運用するとともに、必要に応じて更新しているか。 また、データフロー制御方針は秘密取扱情報システムセキュリティ実装計画に含まれるものとする。 （実施者：秘密取扱情報システム管理者、承認者：総括者。以下、本項目において同じ。）							
	2	秘密取扱情報システムを取り扱うに当たって、秘密取扱情報システム利用者に求められる責任及び期待される行動を規定した規則（以下「行動規則」という。）を作成し、定期的（1 年に 1 回以上を基準）に、及び必要と認める場合に、当該行動規則を精査し、更新しているか。							
	3	秘密取扱情報システムへのアクセスを許可する前に、秘密取扱情報システム利用者に対して、行動規則を理解し順守することに同意する旨の確認を得ているか。また、行動規則が更新された場合には、改めて秘密取扱情報システム利用者から同意を得ているか。							

項目	番号 ※ 1	保全基準	対応状況 （自己評価） ※ 2	対応文書 （秘密保全規則、 システム実装計画、 その他の文書）	対応内容 （規定を抜粋又は要約）	直近の対応 （確認）日	（地方局） 現地調査 判定※ 3	（整備庁） 判定※ 3	備考	
第 1 0 . 構成管理	秘密取扱情報システム管理者は、構成設定等について、以下のことを定め、実施していること。									
	①	秘密取扱情報システム構成要素の構成設定を一元管理するとともに、以下の項目を適切に統合制御するため、構成管理ツール等を導入しているか。 ア 構成設定の変更を行う場合のアクセス制御 イ 管理者権限を有するアカウントの権限の細分化・制御 ウ 構成設定目録の維持 エ 秘密のデータの保存場所の識別・追跡・特定（D L Pによる属性・内容スキャンを実施） オ 必要な世代数分の過去の構成設定の値の保持（2世代を基準） （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）								
	②	秘密取扱情報システムの構成設定の変更を行う場合は、試験環境（仮想環境、夜間等のメンテナンス時等）であらかじめその有効性や副作用の可能性を分析及び評価しているか。								
	③	暗号化技術が、構成管理の対象として適切に管理されているか。								
	④	不正な構成設定の変更が行われた場合に、当該変更を自動的に検知する機能を実装しているか。								
	⑤	ソフトウェアのライブラリ内のプログラムに関して、当該プログラムの内容を変更する管理者権限を制御する機能を実装しているか。								
	秘密取扱情報システム管理者は、秘密取扱情報システム構成要素であるソフトウェア等について、以下のことを定め、実施していること。									
	⑥	ソフトウェアプログラムの秘密取扱情報システム上での実行は、「例外による許可を除き全て拒否（deny-all, permit-by-exception）」とするとともに、秘密取扱情報システム構成要素に関して、定められた頻度（1年に1回以上を基準）で確認を実施しているか。								
	⑦	秘密取扱情報システムに対する不正な機器の接続やソフトウェアのインストールを検知し、アラートを発出するために、資産管理ツールを導入しているか。								
	⑧	オープンソースソフトウェア（OSS）を利用する場合には、以下の使用基準を定めているか。 ア コードの検証ができないバイナリのみ提供しているOSSは拒否 イ 定期的な更新がなされていないOSSは拒否								
	⑨	ソフトウェアのインストールは、管理者権限を付与されたアカウントでのみ実施する機能を実装しているか。								
	10	契約上の取決め及び著作権法に従いソフトウェアを使用し、当該使用状況を確認しているか。								
	⑪	外部の権威ある認証局により認証された証明書を用いた電子署名が付与されていない、又は電子署名が検証されていないソフトウェアについては、そのインストールを防止しているか。								
	秘密取扱情報システム管理者は、重要度分析の実施について、以下のことを定め、実施していること。									
	⑫	リスク宣定の実施（拡張管理策(1-5-2)第7（リスク宣定）①）及び緊急時対応計画の作成（拡張管理策(1-5-2)第6（秘密のデータの漏えい等の事故等発生時の対応）②）に当たっては、秘密取扱情報システム構成要素に関する重要度分析を行い、重要な秘密取扱情報システム構成要素及び機能を特定しているか。								
第 1 1 . 情報システムの基本的防御	秘密取扱情報システム管理者は、基本的防御対策について、以下のことを定め、実施していること。									
	①	秘密取扱情報システムにソフトウェアをインストールし、又はアップデートする場合には、運用環境に移行する前に独立した試験環境（仮想環境含む。）であらかじめその有効性や副作用の可能性を分析及び評価し、必要かつセキュリティ上適切と認められる場合に限り実施しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）								
	②	秘密取扱情報システムのソフトウェアをインストールし、又はアップデートした場合には、影響を受ける管理策が適切に実装され、意図したとおりに機能していることを検証しているか。								
	③	秘密取扱情報システムは、セキュリティ以外の機能がセキュリティ機能に対して影響を与えないように論理的な領域を分離しているか。								
	④	暗号化を実施する場合には、最新の電子政府推奨暗号又はこれと同等の強度の暗号を使用しているか。								
	⑤	秘密取扱情報システム構成要素に障害が発生した場合には、秘密取扱情報システム内の情報（例：障害原因の特定、及び秘密取扱情報システムの中断を最小限に抑えて運用を再開するために必要な情報）を保持しつつ、あらかじめ定められた既知の安全な状態（例：認証機能が停止した場合には、ユーザーログインを不許可にする。暗号機器が故障した場合には、データの通信を停止する。）に遷移することにより、障害状態の継続による影響を最小限に防止しているか。								
	⑥	秘密取扱情報システムで使用する暗号鍵は、ハードウェアセキュリティモジュールやTPM等により安全に保護されているか。								
	⑦	秘密取扱情報システムは、隠ぺい及び誤導に関する機能（例：ポート番号のランダム化）を実装しているか。								
	⑧	秘密取扱情報システムの管理措置にランダム性を導入するため、特定の日常的な管理措置（例：スキャン頻度、パッチ適用スケジュール、ぜい弱性スキャンのタイミング）を異なる日時・時間に行っているか。								
	⑨	秘密取扱情報システムの冗長性を高めるため、秘密取扱情報システム管理者が定める秘密取扱情報システムによる業務処理や秘密取扱情報システム構成要素を、論理的な領域又は複数の物理的な場所に分散しているか（例：負荷分散型クラスター）。								
	⑩	冗長性を満たすように構築した秘密取扱情報システム構成要素について、必要な同期が行われているか。								
	⑪	秘密取扱情報システム構成要素を運用するに当たり、プロセスを分離するか、プロセスごとにアドレス空間（仮想アドレス空間を含む。）を割り当てているか。								
	⑫	外部から持ち込まれたデータは、隔離された環境又はサンドボックス環境で安全に確認しているか。								
	⑬	適用可能なアップデートが秘密取扱情報システムにインストールされているかどうかについて、自動アップデートチェック機能（例：パッチ管理ツール、脆弱性スキャンツール）により、定められた基準（四半期に1回以上を基準）で確認しているか。								
	⑭	秘密取扱情報システムのアップデートを実施した場合には、アップデートする前のバージョン（運用上不要となる全てのソフトウェアを対象とする。以下「旧バージョン」という。）が削除されたことを確認しているか。なお、旧バージョンを残す場合には、ソフトウェアのアップデートを行う前に実施する分析及び評価の段階で、あらかじめ削除対象外として整理しているか。								
⑮	秘密取扱情報システムに保存している情報については、秘密取扱情報システム管理者が定めた期間で削除しているか。									

項目	番号 ※ 1	保全基準	対応状況 (自己評価) ※ 2	対応文書 (秘密保全規則、 システム実装計画、 その他の文書)	対応内容 (規定を抜粋又は要約)	直近の対 応(確認) 日	(地方局) 現地調査 判定※ 3	(整備庁) 判定※ 3	備考
第 1 2 . アクセス 制御		秘密取扱情報システム管理者は、アカウント管理について、以下のことを定め、実施していること。							
	①	アカウントの設定、変更、削除等が実行されたことを把握するための自動化されたアカウント管理支援機能を実装しているか。 (実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。)							
	②	臨時アカウントや緊急アカウント等の一時的に使用することを目的としたアカウントは、一定期間（7 2 時間以内を基準）経過後に、自動的に削除又は無効化される機能を実装しているか。							
	③	アカウントの設定、変更、削除等を行った場合には、自動的に監査を行う機能を実装しているか。							
	④	管理者権限を付与されたアカウントについて、定期的に役割及び使用条件を見直しているか。							
	⑤	共有アカウントやグループアカウント等の複数の者が利用するアカウントは、原則として禁止するものとし、以下の条件を満たす場合のみ許可しているか。 ア 業務上の必要性 イ 利用期間・利用者・利用範囲の明確化 ウ 責任の所在の明確化 エ システムログの取得等 オ 個人としての認証が実施された後に当該アカウントへのアクセスを許可する機能を実装していること。							
	⑥	管理者権限の実行に関して、2 名以上による承認が必要となる機能又は手順を設定しているか（秘密のデータの削除、管理者権限を有するアカウントの設定等）。							
	⑦	分類及びラベル付けされた秘密のデータのデータフローを制御するフィルタリング機能を実装しているか。							
	⑧	データフロー制御に従わない通信は、不審な通信としてすべてネットワーク監視・防護により遮断しているか。							
	⑨	秘密取扱情報システム利用者が実行するソフトウェアのプロセスが、自身の権限よりも高い管理者権限で実行されることを防止する機能を実装しているか。							
	⑩	同時セッションの数を制限する機能を実装しているか。また、最大同時セッション数は、秘密取扱情報システム管理者が定める最小限に設定されているか。							
	⑪	ユーザーセッションが終了した際に、秘密取扱情報システム利用者に対して、ログアウトの通知を表示することを実装しているか。							
	⑫	識別又は認証がなされずに秘密取扱情報システムを実行する行為については、原則として禁止し、その必要が生じた場合には、秘密取扱情報システム管理者が事前に承認しているか。							
	⑬	セキュリティ属性（秘密の区分、作成者、所有者・管理者、アクセス権限、分類ラベル、作成日、改訂履歴等）をメタデータとして秘密のデータに関連付け（例：データ分類ツール）、当該データの処理・伝送時にもその状態を維持するとともに、定められた頻度（9 0 日を基準）でセキュリティ属性の妥当性を見直しているか。							
	⑭	メタデータが改ざんされないように維持する機能を実装し、定められた頻度で完全性を検証しているか。							
	⑮	秘密のデータを保管するサーバ等への不正なデータマイニングに対して、検知及び防止する機能を実装しているか（クエリ制限、監視・検知）。							
	⑯	必要に応じて、アカウントの使用条件（特定の曜日、時刻、使用時間等）を定めているか。							
	⑰	秘密取扱情報システム管理者は、秘密取扱情報システム管理者が定める重大なリスク（損害を与えるためにアクセス権限を悪用すること、攻撃者により損害を与えるための手段として利用されること等）をもたらす可能性のある挙動をする秘密取扱情報システム利用者を発見した場合には、当該秘密取扱情報システム利用者のアカウントを速やかに無効化（3 0 分以内を基準）しているか。							
第 1 3 . 識別及 び認証		秘密取扱情報システム管理者は、秘密取扱情報システムの識別及び認証等について、以下のことを定め、実施していること。							
	①	多要素認証の実装に当たっては、認証要素の一つはアクセス先の秘密取扱情報システムから分離された機器により提供されているか（例：ハードウェアトークン、バイオメトリクス等）。 (実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。)							
	②	多要素認証の際にIDカードを使用する場合には、自社において秘密取扱情報システムを使用することができると認めたIDカードであることを確認する機能を実装しているか。							
	③	秘密取扱情報システム構成要素同士が双方向認証を行う場合には、暗号技術により一意に識別・認証しているか（サーバがルートCAとして発行したデジタル証明書により確認（証明書失効リスト含む。））。							
	④	秘密取扱情報システム構成要素に対して、動的にアドレスを割り当てているか。動的アドレスを割り当てると当たっては、リース情報（IPアドレス、MACアドレス、リース開始・終了時刻、リース期間（2 4 時間）、ID・ホスト名等）を標準化するとともに、当該リース情報を監査しているか。							
	⑤	秘密取扱情報システム管理者があらかじめ定めたサーバにおいて、識別子の一意性を確保しつつ、秘密取扱情報システム利用者、秘密取扱情報システム構成要素及びサービスの属性を集中管理しているか。							
	⑥	パスワードによる認証に関して、脆弱なパスワードのリストを整備し、定められた頻度（四半期に1 回以上を基準）で更新しているか。							
	⑦	秘密取扱情報システム利用者がパスワードを設定するときには、脆弱なパスワードのリストに該当していないことを自動的に確認する機能を実装しているか。							
	⑧	基本的な管理策(1-5-1)第1 3（識別及び認証）⑨に示すパスワードの要件を満たすことを求める機能を実装しているか。							
	⑨	基本的な管理策(1-5-1)第1 3（識別及び認証）⑩に示す保存・伝送方式としてハッシュ化を使用する場合には、ハッシュからパスワードを特定する攻撃への対策を講じているか（1 6 バイト以上のソルトを付加している等）。							
	⑩	秘密取扱情報システムの設置時に、初期の認証情報を変更しているか。							
	11	2 以上の秘密取扱情報システムを利用する秘密取扱情報システム利用者に対して、当該秘密取扱情報システムの間でパスワードの使いまわしを禁止しているか。							
	⑫	キャッシュされた認証情報は一定期間経過後に、自動的に無効化又は削除しているか。							
	⑬	IAMツール（識別及びアクセス管理ツール）を実装しているか。							
	⑭	秘密取扱情報システムにインストールされるデジタル証明書に関する情報は、一元的に管理し、その有効期限等については、定められた頻度（1 年に1 回以上を基準）で確認及び見直ししているか。							
	⑮	認証手段の発行に当たっては、秘密取扱情報システム管理者が指名する登録実施者の面前で、対面により実施しているか。							

項目	番号 ※ 1	保全基準	対応状況 (自己評価) ※ 2	対応文書 (秘密保全規則、 システム実装計画、 その他の文書)	対応内容 (規定を抜粋又は要約)	直近の対応 (確認) 日	(地方局) 現地調査 判定※ 3	(整備庁) 判定※ 3	備考
第 1 4 . 通信の 制御		秘密取扱情報システム管理者は、通信の制御について、以下のことを定め、実施していること。							
	①	秘密取扱情報システムの通信を制御するための方針（目的、対象範囲、関係者の権限・責任、通信制御に当たっての基本的事項をいう。）（以下「通信制御方針」という。）及び秘密取扱情報システムの通信の制御に関する管理策の実装を促進するための実施手順（以下、本項目において「方針等」という。）を作成しているか。なお、通信制御方針は秘密取扱情報システムセキュリティ実装計画に含まれるものとする。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）							
	②	方針等を定期的（１年に１回以上を基準）に、及び秘密取扱情報システムに変更が生じるなど必要と認める場合に精査し、必要に応じ、更新しているか。							
	③	方針等は、データフロー制御方針との整合性を考慮しているか。							
	④	方針等は、関係者に周知しているか。							
	⑤	秘密のデータの通信を行う場合には、当該データを自動的に暗号化するとともに、当該データを転送する通信経路を暗号化しているか。ただし、漏えいのおそれがないと認められる秘密保全施設等内において、送配線（有線）等で通信が行われる場合は、この限りでない。							
	⑥	秘密取扱情報システム内で境界を設けている場合には、秘密取扱情報システム管理者が定める秘密取扱情報システム構成要素（ホスト型のセキュリティ製品を導入できる全ての構成要素）に対してホスト型の境界防護の仕組み（例：HIDS、HIPS）を導入しているか。							
	⑦	秘密取扱情報システムを構成する機器のうちセキュリティツール（フォレンジックツール、構成管理ツール、資産管理ツール、ＩＡＭツール（識別及びアクセス管理ツール）、システム監視ツール、システムログ取得分析ツール、ぜい弱性スキャンツール、メンテナンスツール等）については、採用している分析手法を保護するため、物理的に又は論理的に分離したサブネットワーク上に構成しているか。							
	⑧	使用していない物理ポートは、無効化又は封印しているか。							
	⑨	ネットワーク経由の特権アクセスは、アクセス制御及び監査のための専用の管理インターフェース（例：ジャンプサーバ、VLANによる分離等）を経由することにより経路を制限しているか。							
	⑩	秘密取扱情報システム構成要素の境界を業務内容に応じて論理的に又は物理的に隔離しているか。また、論理的に隔離する場合には、当該境界に境界防護の仕組み（例：F/W）を導入し、サブネットワークを構築しているか。							
	⑪	秘密のデータを伝送する場合の暗号化及び復号に当たっては、一時ファイルの機密性・完全性を確保し、また、一時ファイルが不要となった時点で速やかに消去しているか。							
	⑫	秘密取扱情報システムを利用した通信のセッション終了時又は当該セッションが、非アクティブ状態で定められた期間（15分を基準）を経過した場合は、当該セッションに関連するネットワーク接続を全て終了させているか。							
	⑬	秘密取扱情報システム内で暗号技術を使用するに当たっては、暗号鍵の生成、配付、保管、アクセス及び廃棄（以下「生成等」という。）に関する生成等要件を作成し、当該生成等要件に基づき暗号鍵を作成し、及び管理しているか。							
	⑭	通信セッションの真正性を保護するため、電子証明書等の方法により、通信先が意図した相手であることを確保しているか（例：サーバとパソコン端末）。							
	⑮	秘密取扱情報システムのログアウト時又はセッションの終了時には、当該セッションに係る識別子を無効化しているか。							
	⑯	通信セッションごとに、秘密取扱情報システム管理者が定めるランダム性の要件を満たす情報（文字列等）を含む、一意なセッション識別子を生成しているか。また、他の情報システムが生成したセッション識別子は認識しないようにしているか。							
	⑰	ネットワーク上に外部の悪意のあるコードの識別を行うための装置（例：NIDS、NIPS）を設置し、監視しているか。							
第 1 5 . システム 監視		秘密取扱情報システム管理者は、システム監視について、以下のことを定め、実施していること。							
	①	不正な通信に対するシステム監視を実施する場合は、基本的な管理策(1-5-1)第 1 4（システム監視）①に加えて、認可又は承認されていないソフトウェア（サービス指向アーキテクチャのサービス含む。）に関する監視を実施しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）							
	②	システム監視において、認可又は承認されていないサービスを発見した場合には、基本的な管理策(1-5-1)第 1 4（システム監視）⑨に準じて対応しているか。							
	③	システム監視を実施する場合は、システム上の挙動を常時監視するとともに、システムログの分析結果を利用しているか。							
	④	セキュリティツールを連携させ、システム監視ツールは秘密取扱情報システム全体にわたるシステム監視（システムログの関連付けを含む。）が可能となっているか。							
		秘密取扱情報システム管理者は、システム監視の実施方法について、以下のことを定め、実施していること。							
	⑤	システム監視ツールは、システムログ取得分析ツール（例：SIEM）による準リアルタイム分析が可能となるよう整備されているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）							
	⑥	システム監視に当たっては、機密性保護と可視性維持の均衡を図りながら、システム監視ツールにより通信の内容を確認できるようにしているか。							
	⑦	管理者権限を付与されたアカウント（権限の一部を付与されたアカウントを含む。）に対して、追加的なシステム監視を実施しているか。							
	⑧	ホスト型のシステム監視ツール（例：EDR）により、システム監視を実施しているか。							
	9	サイバー攻撃に関する脅威情報を継続的に把握し、秘密取扱情報システム管理者、秘密取扱情報システム担当者に報告しているか。							
	⑩	システム監視ツールにより、主要なネットワークトラフィックを可視化するとともに、ネットワーク上の信号が途絶した場合には、自動的にデータの転送を停止し、アラートを発出しているか。							
	⑪	ソフトウェアに対する不正な変更を検知するための完全性の検証を以下の条件で実施しているか。 ア サーバ上のソフトウェア ソフトウェアの実行及び変更時 イ 端末上のソフトウェア ネットワーク接続時							
	⑫	秘密取扱情報システムの起動に当たって、ファームウェアの保護（例：更新時のデジタル署名、書き込み保護）及びブートプロセスの完全性を検証するための機能（例：Secure Boot）を実装しているか。							
	⑬	ブートプロセスの完全性を検証する秘密取扱情報システム構成要素（例：サーバ、端末の特定）を定め、当該秘密取扱情報システム構成要素の完全性を秘密取扱情報システム管理者が定める期間や条件で検証しているか。							
	⑭	ブートプロセスが正常に機能しなかったとき起動するフェイルオーバー機能（稼働中のシステムが意図せずに停止した場合に、自動的に待機システムに切り替わる仕組み）を実装しているか。							
	⑮	秘密取扱情報システム管理者が定める情報源（例：人事記録）によりリスクが高まっていることが確認された者のアカウントは停止しているか。							
	⑯	悪意のあるコードを検知するため、可搬記憶媒体を秘密取扱情報システムに接続する前に、検知ソフトウェアによるフルスキャンを実施しているか。							
		秘密取扱情報システム管理者は、不正なアクセス等を検知した際の対応について、以下のことを定め、実施していること。							
	⑰	システム監視により不正なアクセス等を検知した場合は、秘密取扱情報システム管理者、秘密取扱情報システム担当者等に応じたアラートを発出しているか。 （実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。以下、本項目において同じ。）							
	⑱	検知ソフトウェアにより悪意のあるコードを検知した場合は、基本的な管理策(1-5-1)第 1 4（システム監視）⑨を実施するとともに、悪意のあるコードの特性や動作を分析し、必要に応じて事故等対処手順に準じて対応しているか。							

項目	番号 ※ 1	保全基準	対応状況 (自己評価) ※ 2	対応文書 (秘密保全規則、 システム実装計画、 その他の文書)	対応内容 (規定を抜粋又は要約)	直近の対 応(確認) 日	(地方局) 現地調査 判定※ 3	(整備庁) 判定※ 3	備考
第 1 6 . システム ログ		秘密取扱情報システム管理者は、システムログの取得及び分析について、以下のことを定め、実施していること。							
	①	システムログの情報を追加することができる機能を実装しているか。 (実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。 以下、本項目において同じ。)							
	②	システムログを保存するサーバの記憶領域に対して、必要な容量を割り当てているか。							
	③	システムログの容量が不足する可能性がある場合には、代替ストレージをあらかじめ用意し、当該代替ストレージに転送されるようにしているか。							
	④	システムログを保存するサーバの記憶領域の使用割合が、定められた基準（システムログの最大記憶容量の 7 5 %を基準）を超えた場合には、秘密取扱情報システム担当者等に対しアラームを発する機能を実装しているか。							
	⑤	システムログの取得及び分析ツール（以下「システムログ取得分析ツール」という。） (例：SIEM) を実装しているか。							
	⑥	否認防止の対象となる行為（例：ファイル操作、電子メール等の送受信等）に関して、秘密取扱情報システム利用者又は当該秘密取扱情報システム利用者の代わりに動作するプロセスが実施したシステムログを取得しているか。							
	⑦	システムログ取得分析ツールによるシステムログの分析結果と当該システムログ取得分析ツールにより取得することができないシステムログ（例：システムログ取得分析ツールと直接できないセキュリティツール、秘密取扱施設への入退室の記録から取得した情報等）とを関連付けて分析しているか。							
	⑧	システムログへのアクセス権限は、秘密取扱情報システム管理者及び秘密取扱情報システム担当者に限定して付与するとともに、当該アクセス権限を読み取り専用に制限しているか。							
	⑨	システムログ取得分析ツールを、不正なアクセス、改ざん、削除等から保護しているか。							
	⑩	長期間保存されたシステムログが、必要な時に速やかに検索することができる措置を実施しているか（システムログへのメタデータの付与、保存形式の標準化等）。							
	⑪	タイムスタンプ間の関係について時間順序を確保するため、時差の許容範囲を定めるとともに、当該時差内の状態を維持しているか（例：サーバのReal Time Clockを基準に時刻を配信し、定期的に手動補正。）。							
	⑫	秘密取扱情報システムのログイン時に、自動的に、特定の条件（例：ブートプロセス開始時、ユーザの異常な行動の検知時）でセッション監査を行う機能（例：特定のユーザのキー操作の監視、ファイル転送の記録・確認することができる機能）が稼働しているか。							
第 1 7 . ぜい弱 性スキャン等		秘密取扱情報システム管理者は、ぜい弱性スキャンについて、以下のことを定め、実施していること。							
	①	ぜい弱性スキャンツールを実装しているか。 (実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。 以下、本項目において同じ。)							
	②	定期的（1 か月に 1 回以上を基準）なぜい弱性スキャンを実施する前に、ぜい弱性スキャンツールを最新の状態に更新しているか。							
	③	ぜい弱性スキャンは、管理者権限を付与されたアカウントにより実施しているか。							
第 1 8 . バック アップ		秘密取扱情報システム管理者は、秘密取扱情報システムの秘密のデータに関するバックアップの手順について、以下のことを定め、実施していること。							
	①	基本的な管理策(1-5-1)第 1 7（バックアップ）②・③の規定にかかわらず、秘密取扱情報システムに関するデータ（秘密のデータ、システムログ、システムデータを含む全ての情報）について、定期的（1 週間に 1 回以上を基準）にバックアップし、「バックアップ実施等記録簿」（付紙様式第 3 5（基準））により速やかに総括者、秘密取扱情報システム管理者その他必要者に報告しているか。また、バックアップしたデータの取扱いについて、基本的な管理策(1-5-1)第 1 7（バックアップ）②の規定に従っているか。 (実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者、 以下、本項目において同じ。)							
	②	秘密のデータの完全性を検証するため、秘密のデータの一部をランダムにサンプリングした上で、定期的（1 か月に 1 回以上を基準）に、バックアップされた秘密のデータの可用性を試験的に確認しているか。							
	③	バックアップされたデータは、秘密のデータの保存領域とは論理的に異なる領域に保存し、また、暗号化の機能を実装しているか。							
第 1 9 . メンテ ンス等		秘密取扱情報システム管理者は、メンテナンス等の実施について、以下のことを定め、実施していること。							
	①	メンテナンス等に使用される機器は、施錠したロッカー等により保管しているか。 (実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。 以下、本項目において同じ。)							
	②	メンテナンス等に使用される機器をやむを得ず秘密保全施設等の外に持ち出す必要がある場合には、当該機器に秘密のデータが保管されていないことを確認するとともに、当該持出について、秘密取扱情報システム管理者の許可を受けているか。							
	③	メンテナンス等に使用される機器を再利用していないか（メンテナンスの対象となる秘密取扱情報システムを廃棄した時点等で確実に廃棄しているか）。							
	④	メンテナンス等の実施に際しては、あらかじめ付与された特別なアカウントのみにより行われ、当該アカウントによる実施内容が全て記録される機能が実装されているか。							
	⑤	メンテナンス等の実施の監督に当たっては、システムログ（秘密取扱情報システムで定めているシステムログと同じ内容）を取得し、及びその分析を実施しているか。							
	⑥	基本的な管理策(1-5-1)第 1 8（メンテナンス等）①に規定するメンテナンス等計画の承認を行う際には、メンテナンス等に使用される機器及びツールにインストールされているソフトウェアが最新（更新ファイルの真正性含む。）となっていることを確認しているか。							
	⑦	秘密取扱情報システムを秘密保全施設等の外に持ち出す必要がある場合（非ローカルメンテナンス等）には、秘密取扱情報システム管理者は、システムメンテナンス等計画による承認を得るとともに、あらかじめ秘密取扱情報システムに記録された秘密のデータを削除し、又は移動させ、秘密のデータが復元できない状態（データ消去ソフトウェアによる消去を実施し、データ復元ソフトウェアを使用してもデータが検出されない状態をいう。）にするなど必要な措置を講じ、同計画にその旨を記載しているか。							
	⑧	監督者は、秘密取扱情報システムのメンテナンス等を実施する者と共に現場に所在して、非ローカルメンテナンス等の実施の状況を監督しているか。							
	⑨	非ローカルメンテナンス等の実施の状況の監督に当たっては、システムログ（秘密取扱情報システムで定めているシステムログと同じ内容）の取得及び分析を実施しているか（結果報告は、通常のメンテナンスと同様に実施する。）。							
	⑩	秘密取扱情報システムに障害が発生した場合には、適時にメンテナンス等を実施するため、メンテナンス等に必要な役務や部品を取得するための計画を作成し、必要に応じて更新しているか。							
	⑪	秘密取扱情報システム構成要素ごとの平均故障時間（MTTF）及び代替の秘密取扱情報システム構成要素の取得予定時期（MTTFから取得時期を設定すること）を定めているか。							
	⑫	平均故障時間（MTTF）に基づき、代替の秘密取扱情報システム構成要素を取得し、予備整備を行っているか。							

項目	番号 ※ 1	保全基準	対応状況 (自己評価) ※ 2	対応文書 (秘密保全規則、 システム実装計画、 その他の文書)	対応内容 (規定を抜粋又は要約)	直近の対応 (確認) 日	(地方局) 現地調査 判定※ 3	(整備庁) 判定※ 3	備考
第 2 0 . サプライ チェーン・リスク	総括者は、サプライチェーン・リスクについて、以下のことを定め、実施していること。								
	1	サプライチェーン・リスクに関する管理策を適正に実施するために、秘密取次情報システム管理者が定める職員で構成されるサプライチェーン・リスク管理(SCRM)チームを設置しているか。 (実施者：秘密取次情報システム管理者、承認者：総括者。以下、本項目において同じ。)							
	2	サプライチェーン・リスクを考慮して、秘密取次情報システム構成要素の供給源を多様化しているか。							
	秘密取次情報システム管理者は、サプライチェーン・リスクについて、以下のことを定め、実施していること。								
	3	秘密取次情報システム構成要素の選定、受入、変更又はアップデートの前に、秘密取次情報システム管理者が定める必要な評価（例：試験環境（仮想環境含む。）におけるウイルスチェック、ぜい弱性の確認、環境設定されたパラメータの再確認、製造中に利用されたアカウントの削除等の安全性の確認を含む分析及び評価）を実施しているか。 (実施者：秘密取次情報システム担当者、承認者：秘密取次情報システム管理者。以下、本項目において同じ。※) ※調達部門や資材部門等のサプライヤーとの窓口部門と協力することを妨げるものではないが、窓口部門が各項目を実施する場合には、実施者及び承認者は、その実施内容の適正性を確認し、承認すること。							
	4	秘密取次情報システム管理者は、定期的（１年に１回以上を基準）に、及び必要があると認められる場合に、サプライヤーに関するサプライチェーン・リスクを評価し、必要に応じて、サプライヤーを変更するよう努めているか。							
	5	サプライチェーン・リスクに関する事故等が発生した場合又はぜい弱性が発見された場合には、サプライヤーから当該事項が通知される合意を締結するよう努めているか。							
	6	秘密取次情報システム構成要素について、耐タンパ性を確保するためのTPM・HSMの導入、偽造防止サービスを提供している製品の選定、メンテナンス等の実施時の構成管理に努めるなど、ライフサイクル全般を通じて改ざん対策を行っているか。							
	7	改ざんを検知するため、定期的（１年に１回以上を基準）に、及び必要があると認められた場合に、秘密取次情報システム構成要素を検査しているか。							
	8	基本的な管理策(1-5-1)第３（人的セキュリティ）３に規定する教育及び訓練に、秘密取次情報システム構成要素の偽造品対策に関する内容を含めているか。							
第 2 1 . 秘密取 次情報システムの 調達	総括者は、サプライヤーに対するサプライチェーン・リスクの適用（フローダウン）について、以下のことを定め、実施していること。								
	9	秘密取次情報システムのライフサイクル全般（設計、開発、導入、廃棄に至るまでの全ての工程）に参画するサプライヤーに対して、サプライチェーン・リスクに関する管理策を適用するよう努めているか。							
	総括者は、秘密取次情報システムの調達について、以下のことを定め、実施していること。								
	1	秘密取次情報システム構成要素の調達に関する方針及び秘密取次情報システム構成要素の調達を実施するための実施手順（以下、本項目において「方針等」という。）を作成しているか。 (実施者：秘密取次情報システム管理者、承認者：総括者。以下、本項目において同じ。)							
	2	方針等を定期的（１年に１回以上を基準）に、及び秘密取次情報システムに変更が生じた場合など必要と認める場合に精査し、必要に応じ更新しているか。							
	秘密取次情報システム管理者は、秘密取次情報システムの調達の実施について、以下のことを定め、実施していること。								
	3	秘密取次情報システムの開発ライフサイクル全般に関するセキュリティ対策文書を作成・更新し、実施しているか（設計・開発・運用工程におけるセキュリティ対策は、以下を基準として実施）。 ア システム要件に応じたセキュリティ基本方針（目標、品質管理体制、適用／準拠する規格（ISO/IEC 15048）） イ リスク分析の実施 ウ セキュリティ要件の決定（必要な機能の特定、不必要に高いリスクをもたらす機能の使用の回避又は最小化を含む。） エ セキュリティ設計／構築手順書の作成 オ セキュアなプログラミングガイド文書の作成 カ セキュアなシステム基盤構築（秘密取次情報システム構成要素の購入・統合・パラメータの設定等） キ セキュアなプログラミング（ＡＩを利用してコーディングする場合、人間によるレビューを必ず実施すること） ク 本番移行前のぜい弱性検査 ケ 運用後のぜい弱性検査 コ セキュアな運用手順書（管理者用／利用者用）							
	4	秘密取次情報システムのライフサイクル全般を通じて、秘密取次情報システムの運用前の環境（開発環境、テスト環境及び統合環境）を適切に管理しているか。							
	5	運用、保守段階における秘密取次情報システムの更新計画（秘密取次情報システムの変更を含む。）を作成・更新しているか。							
	6	秘密取次情報システムの構成要素には、Common Criteria(ISO/IEC 15408) の評価保証レベル(EAL) 4 以上の製品又は同等品を努めて使用しているか。							

項目	番号 ※ 1	保全基準	対応状況 (自己評価) ※ 2	対応文書 (秘密保全規則、 システム実装計画、 その他の文書)	対応内容 (規定を抜粋又は要約)	直近の対 応(確認) 日	(地方局) 現地調査 判定※ 3	(整備庁) 判定※ 3	備考
第 2 1 . 秘密取 扱情報システムの 調達		秘密取扱情報システム管理者は、セキュリティエンジニアリングの原則の適用について、以下のことを定め、実施していること。							
	7	秘密取扱情報システムの基本的な管理策(1-5-1)第 1 0 (構成管理) 1 に規定するセキュリティエンジニアリングの原則に、以下の原則を含めているか。 ア 明確な抽象化(clear abstractions) イ 共通の仕組みの最小化(least common mechanism) ウ モジュール化及び階層化(modularity and layering) エ 部分的に整序された依存関係(partially ordered dependencies) オ 効率的に媒介されるアクセス(efficiently mediated access) カ 最小共有(minimized sharing) キ 複雑性低減(reduced complexity) ク 保守拡張性(secure evolvability) ケ 信頼できる構成品(trusted components) コ 階層型信頼(hierarchical trust) (実施者：秘密取扱情報システム担当者、承認者：秘密取扱情報システム管理者。 以下、本項目において同じ。)							
	8	秘密取扱情報システムの基本的な管理策(1-5-1)第 1 0 (構成管理) 1 に規定するセキュリティエンジニアリングの原則に、以下の原則を含めているか(続き)。 サ 逆改ざん閾値(inverse modification threshold) シ 階層型保護(hierarchical protection) ス 最小セキュリティ要素(minimized security elements) セ 最小権限(least privilege) ソ 根拠のある許可(predicate permission) タ 自立信頼性(self-reliant trustworthiness) チ 安全な分散型構成(secure distributed composition) ツ 信頼できる通信経路(trusted communications channels) テ 継続的保護(continuous protection) ト 安全なメタデータ管理(secure metadata management)							
	9	秘密取扱情報システムの基本的な管理策(1-5-1)第 1 0 (構成管理) 1 に規定するセキュリティエンジニアリングの原則に、以下の原則を含めているか(続き)。 ナ 自己分析(self-analysis) ニ 責任追跡性及び追跡可能性(accountability and traceability) ヌ 安全な初期設定(secure default) ネ 安全な障害及び復旧(secure failure and recovery) ノ 経済的なセキュリティ(economic security) ハ 性能セキュリティ(performance security) ヒ 人的要因を考慮したセキュリティ(human factored security) フ 許容可能なセキュリティ(acceptable security) ヘ 再現可能な文書化された手順 ホ 手順の厳密性 マ 安全な情報システム変更 ミ 十分な文書化							
	⑩	秘密取扱情報システム構成要素の設計・開発・運用を委託する場合には、基本的な管理策(1-5-1)第 1 0 (構成管理) 1 及び拡張管理策(1-5-2)第 2 1 (秘密取扱情報システムの調達) 7 ～ 9 に規定するセキュリティエンジニアリングの原則を求めるよう努めているか。							
	⑪	秘密取扱情報システム構成要素の設計・開発・運用を委託する場合には、基本的な管理策(1-5-1)第 1 0 (構成管理) 及び拡張管理策(1-5-2)第 2 1 0 (構成管理) で規定している構成管理を求めるとともに、秘密取扱情報システム管理者が定める頻度で、当該構成管理の実施状況の報告を求めるよう努めているか。							
	⑫	秘密取扱情報システムの開発を委託する場合には、ソフトウェア及びハードウェアの完全性の検証を求めるよう努めているか。							
	⑬	秘密取扱情報システムの開発を委託する場合には、システム開発ライフサイクルにおける設計段階後の全ての段階において、以下の事項を求めるよう努めているか。 ア 継続的なセキュリティ管理策の実装状況の評価するための計画を作成し、実施すること。 イ 必要な深度、範囲、頻度で、単体テスト、結合テスト、システムテスト等を実施すること。 ウ 評価計画実施及びテスト結果を作成すること。 エ 検証可能な欠陥修正プロセスを実施すること。 オ ぜい弱性分析を実施すること。 カ 重要度分析を実施すること。							
	⑭	秘密取扱情報システムの開発を委託する場合には、静的コード解析等の実施を求めるよう努めているか。							
	⑮	秘密取扱情報システムの開発を委託する場合には、以下の開発プロセスを求めるよう努めているか。 ア セキュリティ要件に明示的に対応すること イ 開発プロセスで使用する規格及びツールを特定すること ウ 開発プロセスで使用する具体的なツールのオプション及びツールの設定を定めること エ 開発で使用するプロセス又はツールに対する変更の完全性を確保すること							
	⑯	秘密取扱情報システムの開発を委託する場合には、当該委託の成果物を適切に使用することができるようにするための教育を実施しているか。							
	⑰	秘密取扱情報システムの開発を委託する場合には、必要とされるセキュリティの機能並びに物理的及び論理的な秘密取扱情報システム構成要素に対するセキュリティ管理策の割当を委託するためのセキュリティ設計書を求めているか。							
	⑱	秘密取扱情報システム構成要素に対するサポートが終了した場合には、当該秘密取扱情報システム構成要素を速やかに交換しているか。							
総合判定									

- ※ 1 ○で囲んだ番号は情報システムごとに点検するものを表し、○で囲んでない番号は事業所ごとに点検するものを表している。
- ※ 2 防衛事業適合事業者契約の申込み時は、原則として、「対応済、対応予定、一部対応(代替策)、対応困難(代替策)、非該当」から選択するものとし、点検時には、「実施済、未実施、その他」を記載するものとする。
- 「対応予定」については、対応する時期が定まっている場合が該当する。この場合には、対応する時期を明記するものとする。(※ 4)
- 「一部対応(代替策)」、「対応困難(代替策)」については、該当する保全基準の一部又は全部を満たせない場合が該当する。これらの場合には、その理由を示し、当該保全基準を実装しないことにより生じ得るリスクを特定し、当該保全措置を講じないことに対する代替策を講じ又は代替策の考え方を示した上で、代替策の妥当性について調整するものとする。
- 「非該当」については、秘密取扱情報システムにおいて実際に取り扱われる秘密のデータの取扱いの特性上、該当する保全基準を適用できないことが自明である場合をいう。
- 「その他」については、具体的な状況を明記するものとする。
- ※ 3 防衛事業適合事業者契約の申込み時は、原則として、「適合、条件付適合、不適合、非該当」から選択するものとし、点検時には「良好、要改善、不良」から選択するものとする。
- ※ 4 秘密取扱情報システムへの実装に時間を要する等の理由により直ちに適用することができない保全基準がある場合には、その理由及び拡張管理策(1-5-2)に従った取扱いを行うことができる合理的な時期を示した将来対応計画を作成し、付紙様式第 1 - 5 - 2 に将来対応計画書を添付するものとする。

秘密保全体制認証申請書

年 月 日

防衛装備庁長官 殿
(装備政策部装備保全管理課長気付)
(地方防衛局調達部長等経由)

所 在 地
事業者名
代表者名

秘密保全体制の認証について、属紙第 1 及び属紙第 2 の内容を承諾しましたので、保全基準兼点検票及び下記の関係書類を添えて申請します。

記

(関係書類)

- 1 申請条件を満たしていることを証明する書類
- 2 組織の体制
 - (1) 総括者（保全の総括責任者）の指名
役 職：
氏 名：
指名基準：基準 1、基準 2、基準 3（いずれかに○をしてください。）
 - (2) 総括者の指名に当たって、選択した指名基準を満たしていることを証明する書類及び総括者の経歴
 - (3) 保全の責任者（総括者、保全責任者等）の役割及び役職を明記した書類
 - (4) 事業者全体の中の防衛部門の位置付けが分かる組織図
 - (5) 防衛部門の組織編成図
 - (6) 付紙様式第 1－1 の回答を証明する書類
- 3 秘密保全規則
 - (1) 秘密保全規則案
 - (2) 懲戒手続等が規定された社内規則
- 4 教育の体制

- (1) 教育実施計画及び教育テキスト
- (2) 直近の保全教育の実施状況

5 秘密保全施設

- (1) 構造（設計）図、カタログ等
- (2) 建築（改修）中の写真
- (3) 基準と同等以上であることを証明する書類

（その他調整事項）

6 認証する場合に交付する認証証明書の宛名の希望

事業者名／事業所名／別途調整 （いずれかに○をしてください。）

7 防衛装備庁のホームページ（認証事業者リスト一覧）への掲載

希望する / 希望しない （いずれかに○をしてください。）

- 添付書類：
- 1 保全基準兼点検票（保全組織の体制）
 - 2 保全基準兼点検票（秘密保全規則）
 - 3 保全基準兼点検票（秘密保全教育の体制）
 - 4 保全基準兼点検票（秘密保全施設、保全外部区域及び保管容器）
 - 5 関係書類

【申請に当たっての留意事項】

- 1の「証明する書類」として、以下のいずれかの書類を提出してください。
 - (1) 秘密取扱原因契約に係る契約書（鑑）の写し
 - (2) 防衛装備庁との契約に係る契約書（鑑）の写し3件分
- 2(1)の「指名基準」について、属紙第2の基準2又は基準3に該当する場合には、防衛装備庁が実施する研修を修了してください。
- 2(6)の「証明する書類」として、以下の書類を参考に、該当箇所の書類を添付してください。
定款、取締役会決議書、コーポレートガバナンス、役員規程、情報管理規定、有価証券報告書、大量保有報告書、その他参考となる書類
- 5(3)の「証明する書類」として、保全基準に相当する代替措置を講じる場合に、これを証明する書類を提出してください。
- 防衛事業適合事業者制度等に関する訓令（令和7年防衛装備庁訓令第19号）附則第2項に該当する事業者として、既に秘密を取り扱う契約を通じて秘密保全体制を整備している事業者が本申請を行う場合は、以下の書類により申請することができます。
 - (1) 本申請書
 - (2) 付紙様式第1－1及び本申請書の2に掲げる書類
 - (3) 本申請書の3、4及び5に係る過去の審査結果の通知の写し
- 防衛事業適合事業者が認証申請する場合は、本申請の本文を「秘密保全体制の認証について、属紙第1及び属紙第2の内容を承諾しましたので、防衛事業適合事業者として、下記のとおり申請します。」とした上で、記書き部分に「（その他調整事項）」のみを記載して申請することができます。

認証申請に当たっての承諾事項

（秘密の保全体制の維持）

第 1 認証を受けた秘密の保全体制について、認証の有効期間内においては、認証を受けた時点と同じ適切な保全体制を維持すること。

（秘密の保全体制の変更）

第 2 認証を受けた秘密の保全体制について、変更のある場合は、真にやむを得ない事情のある場合を除き、事前に防衛装備庁又は地方防衛局に申請すること。

（防衛装備庁による保全教育の受講）

第 3 教育の体制が不十分と判断された場合には、保全教育の実施者に対して、年 1 回以上、防衛装備庁による保全教育を受けさせること。

（保全基準兼点検票の提出）

第 4 別に定める要領により正確な保全基準兼点検票を防衛装備庁に提出すること。

（現地調査等の受入）

第 5 認証を受けた情報保全体制について、別に定めるところにより防衛装備庁若しくは地方防衛局の現地調査等又は保全検査を受け入れ、是正措置等を求められた場合は、適切な措置を講じること。

（認証取消後の措置）

第 6 認証の取消を受けた場合は、認証証明書を返納し、認証マークの使用を終了すること。

（その他事項）

第 7 その他調整事項が生じた場合は、防衛装備庁装備政策部装備保全管理課と協議すること。

総括者の指名に関する細部審査基準

認証申請する事業者は、総括者を指名するに当たっては、以下の第 1 から第 3 までの基準のいずれかを満たすことができる者とする。

第 1 基準 1

- 1 総括者は、認証事業者の契約代理人、防衛事業に関する事業本部長又は工場長その他の認証事業者の経営責任者又は防衛事業の執行責任者として、認証事業者及びその下請負事業者に対し、秘密の保全についての権限を行使できること。
- 2 総括者は、過去 10 年の間、2 年以上継続して、通算 3 年以上にわたり防衛産業において該当する秘密区分を含む防衛省の秘密を取り扱った実務経験があること。
- 3 総括者は、リスク評価、従業員への教育、秘密保全施設等の管理、定期的な点検、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置について熟知しており、日常的な秘密の取扱いについて関係社員に対する指導を行うことができること。

第 2 基準 2

- 1 総括者は、認証事業者の契約代理人、防衛事業に関する事業本部長又は工場長その他の認証事業者の経営責任者又は防衛事業の執行責任者として、認証事業者及びその下請負事業者に対し、秘密の保全についての権限を行使できること。
- 2 第 1 の 2 及び 3 を満たすことができない場合には、以下の措置を講じること。
 - (1) 保全責任者その他秘密保全組織を管理する者であって、総括者を支える者として過去 10 年の間に通算 5 年以上にわたり防衛産業において該当する秘密区分を含む防衛省の秘密を取り扱った実務経験があり、リスク評価、従業員への教育、秘密保全施設等の管理、定期的な点検、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置について熟知している者を配置すること。
 - (2) 総括者は、認証の日から 6 か月を経過する日までに、リスク評価、従業員

への教育、秘密保全施設等の管理、定期的な点検、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置についての防衛装備庁の研修を修了すること。

第3 基準3

- 1 総括者は、認証事業者の契約代理人、防衛事業に関する事業本部長又は工場長その他の認証事業者の経営責任者又は防衛事業の執行責任者として、認証事業者及びその下請負事業者に対し、秘密の保全についての権限を行使できること。
- 2 第2の2(1)を満たすことができない場合には、以下の措置を講じること。
 - (1) 総括者は、認証の日から6か月を経過する日までに、リスク評価、従業員への教育、秘密保全施設等の管理、定期的な点検、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置についての防衛装備庁の研修を修了すること。
 - (2) 保全責任者その他秘密保全組織を管理する者は、認証の日から6か月を経過する日までに1回及びその後は3か月に1回の頻度により合計4回、リスク評価、従業員への教育、秘密保全施設等の管理、定期的な点検、下請負事業者との関係並びに事故対応を含め、日常的な秘密の取扱いに関する保全措置についての防衛装備庁の研修を修了すること。

付紙様式第3

発 簡 番 号

発 簡 年 月 日

(事 業 者) 殿

防衛装備庁装備政策部長

○ ○ ○ ○

認証審査の結果について（通知）

標記について、 年 月 日付で貴社から申請のあった認証に係る審査の結果、
[認証する／下記のとおり認証しない]こととなった旨、通知します。

[以下は、認証しない場合に記載]

記

認証しない理由等：

写送付先：地方防衛局調達部長等

発 簡 番 号
発 簡 年 月 日

(事 業 者) 殿

防衛装備庁装備政策部長

○ ○ ○ ○

認 証 通 知 書

標記について、 年 月 日付で申請のあった貴社の秘密保全体制について、
下記のとおり防衛装備庁の秘密保全基準を満たしていることを認証します。

記

- 1 認証番号：
- 2 認証を受けた事業所名及び所在地
事業所名：
所 在 地：
- 3 秘密保全施設の数及び内訳：
- 4 認証の有効期間： 年 月 日から5年間
- 5 取り扱うことのできる秘密情報の種類：
- 6 その他事項
認証事業者であることは公表可能ですが、現に秘密を取り扱っていることが
推測できる内容の公表は控えてください。

写送付先：地方防衛局調達部長等、契約担当官等

[事業者番号] - [延長回数]号

防衛事業
認証事業者DEFENSE
CLEARED
FACILITIES防衛事業認証事業者
認証証明書*Certificate of Defense Cleared Facilities*

殿

貴社の情報管理体制は、防衛装備庁の秘密保全基準を
満たしていることを認証します。

*This is to certify that your information security is
granted for the security standards by ATLA.*

**ATLA**Acquisition, Technology &
Logistics Agency

年 月 日

防衛装備庁長官





- 備考 1 認証マークは、認証事業者の秘密保全体制が防衛装備庁の秘密保全基準を満たしていることを証するものであり、当該認証事業者のみが使用できる。
- 2 大きさは、適宜とする。
- 3 認証を取り消された事業者は、認証マークの使用を直ちに終了すること。

自己点検申告書

年 月 日

防衛装備庁装備政策部長 殿
(地方防衛局調達部長等経由)

所 在 地
事業者名
代表者名

秘密保全体制について、下記のとおり点検したので申告します。

記

- 1 前回点検時からの変更の有無 有 / 無
- 2 懸念事項の有無 有 / 無
- 3 懸念事項の内容(「無」の場合は記載不要)
- 4 点検時期
- 5 その他事項

添付書類：[自己点検票（月次）、保全基準兼点検票]

発 簡 番 号

発 簡 年 月 日

(事 業 者) 殿

防衛装備庁装備政策部長

○ ○ ○ ○

認 証 取 消 通 知 書

標記について、 年 月 日付で貴社に交付した認証について、これを取り消します。なお、下記の認証番号の認証証明書を速やかに防衛装備庁装備政策部装備保全管理課に返却するとともに、認証マークを使用している場合はその使用を終了してください。

記

1 取消しをする認証番号：

2 取消理由：

写送付先：地方防衛局調達部長等、契約担当官等

年 月 日

防衛装備庁装備政策部長 殿
(地方防衛局調達部長等経由)

所 在 地
事業者名
代表者名

秘密保全体制／情報保全体制の変更について（申請）

標記について、 年 月 日付で防衛装備庁[から認証を受けた秘密保全体制
／と締結した防衛事業適合事業者契約の対象となる情報保全体制]の変更を予定
しているため、下記のとおり申請します。

記

1 変更の内容

2 変更予定時期

3 その他事項

添付書類： 1 保全基準兼点検票
2 関係書類

防衛装備庁装備政策部長 殿
(地方防衛局調達部長等経由)

所 在 地
事業者名
代表者名

保護すべき情報の取扱に関する情報保全体制の変更について (申請)

標記について、下記のとおり申請します。

記

- 1 変更を希望する防衛事業適合事業者契約番号
D C F -
- 2 変更の内容
- 3 変更する関係書類
【情報セキュリティ基本方針／情報セキュリティ規則／情報セキュリティ実施
手順／システムセキュリティ実装計画書】
- 4 変更予定時期
- 5 その他事項

添付書類：変更する関係書類

年 月 日

防衛装備庁装備政策部長 殿
(地方防衛局調達部長等経由)

所 在 地
事業者名
代表者名

[認証／防衛事業適合事業者契約] の延長について (申請)

標記について、 年 月 日付で防衛装備庁 [から受けた認証／と締結した防衛事業適合事業者契約] の延長を希望するため、下記のとおり申請します。

記

1 延長を希望する[認証番号／防衛事業適合事業者契約番号] :

2 その他事項

添付書類 : 1 保全基準兼点検票
2 関係書類

年 月 日

防衛装備庁装備政策部長 殿
(地方防衛局調達部長等経由)

所 在 地
事業者名
代表者名

保護すべき情報に関する防衛事業適合事業者契約の延長について
(申請)

標記について、下記のとおり申請します。

記

- 1 延長を希望する防衛事業適合事業者契約番号
- 2 関係書類
 - (1)直近の情報セキュリティ実地監査の結果通知の写し
 - (2)直近の情報セキュリティ対策実施点検書の写し
- 3 その他事項

添付書類：関係書類

防衛事業適合事業者契約申込書

年 月 日

防衛装備庁長官 殿
(装備政策部装備保全管理課長気付)
(地方防衛局調達部長等経由)

所 在 地
事業者名
代表者名

秘密情報の取扱いに係る防衛事業適合事業者契約について、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（装装保第 1 4 8 4 6 号。令和 7 年 7 月 3 1 日）別紙第 2 の契約条項により締結したく、保全基準兼点検票及び下記の関係書類を添えて申し込みます。

記

- 1 防衛事業に参画する意思： 有 / 無（どちらかに○をしてください。）
- 2 参画を希望する事業の概要：
- 3 契約締結者の確認
乙（契約当事者）として契約を締結する当事者名：
- 4 組織の体制
 - (1) 総括者（保全の総括責任者）の指名
役 職：
氏 名：
指名基準：基準 1、基準 2、基準 3（いずれかに○をしてください。）
 - (2) 総括者の指名に当たって、選択した指名基準を満たしていることを証明する書類及び総括者の経歴
 - (3) 保全の責任者（総括者、保全責任者等）の役割及び役職を明記した書類
 - (4) 事業者全体の中の防衛部門の位置付けが分かる組織図
 - (5) 防衛部門の組織編成図
 - (6) 付紙様式第 1 - 1 の回答を証明する書類

5 秘密保全規則

- (1) 秘密保全規則案
- (2) 懲戒手続等が規定された社内規則

6 教育の体制

- (1) 教育実施計画及び教育テキスト
- (2) 直近の保全教育の実施状況

7 秘密保全施設

- (1) 構造（設計）図、カタログ等
- (2) 建築（改修）中の写真
- (3) 基準と同等以上であることを証明する書類

8 秘密取扱情報システム

- (1) 秘密取扱情報システム体制
- (2) 秘密取扱情報システムセキュリティ実装計画

- 添付書類：
- 1 保全基準兼点検票（保全組織の体制）
 - 2 保全基準兼点検票（秘密保全規則）
 - 3 保全基準兼点検票（秘密保全教育の体制）
 - 4 保全基準兼点検票（秘密保全施設、保全外部区域及び保管容器）
 - 5 保全基準兼点検票（秘密取扱情報システム）
 - 6 関係書類

【申込みに当たっての留意事項】

- 4 (1)の「指名基準」について、属紙第2の基準2又は基準3に該当する場合には、防衛装備庁が実施する研修を修了してください。
- 4 (6)の「証明する書類」として、以下の書類を参考に、該当箇所の書類を添付してください。
定款、取締役会決議書、コーポレートガバナンス、役員規程、情報管理規定、有価証券報告書、大量保有報告書、その他参考となる書類
- 5 (3)の「証明する書類」として、保全基準に相当する代替措置を講じる場合に、これを証明する書類を提出してください。
- 秘密保全施設又は秘密取扱情報システムを備えない防衛事業適合事業者となることを希望して本申込みを行う場合は、本申込書の7又は8について、単に「希望しない」と記載してください。
- 防衛事業適合事業者制度等に関する訓令(令和7年防衛装備庁訓令第19号)附則第4項に該当する事業者として、既に秘密を取り扱う契約を通じて秘密保全体制を整備している事業者が本申込みを行う場合は、以下の書類により申請することができます。
 - (1) 本申込書
 - (2) 付紙様式第1－1及び本申込書の4に掲げる書類
 - (3) 本申込書の5、6及び7に係る過去の審査結果の通知の写し
 - (4) 付紙様式第1－5及び8に掲げる書類
- 認証事業者が申込みをする場合は、以下の書類により申込みをすることができます。
 - (1) 本申込書
 - (2) 付紙様式第1－5及び関係書類

総括者の指名に関する細部審査基準

防衛事業適合事業者契約の申込みをする事業者は、総括者を指名するに当たっては、以下の第1から第3までの基準のいずれかを満たすことができる者とする。

第1 基準1

- 1 総括者は、防衛事業適合事業者の契約代理人、防衛事業に関する事業本部長又は工場長その他の防衛事業適合事業者の経営責任者又は防衛事業の執行責任者として、防衛事業適合事業者及びその下請負事業者に対し、秘密の保全についての権限を行使できること。
- 2 総括者は、過去10年の間、2年以上継続して、通算3年以上にわたり防衛産業において該当する秘密区分を含む防衛省の秘密を取り扱った実務経験があること。
- 3 総括者は、リスク評価、従業員への教育、秘密保全施設等の管理、定期的な点検、秘密取扱情報システム、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置について熟知しており、日常的な秘密の取扱いについて関係社員に対する指導を行うことができること。

第2 基準2

- 1 総括者は、防衛事業適合事業者の契約代理人、防衛事業に関する事業本部長又は工場長その他の防衛事業適合事業者の経営責任者又は防衛事業の執行責任者として、防衛事業適合事業者及びその下請負事業者に対し、秘密の保全についての権限を行使できること。
- 2 第1の2及び3を満たすことができない場合には、以下の措置を講じること。
 - (1) 保全責任者その他秘密保全組織を管理する者であって、総括者を支える者として過去10年の間に通算5年以上にわたり防衛産業において該当する秘密区分を含む防衛省の秘密を取り扱った実務経験があり、リスク評価、従業員への教育、秘密保全施設等の管理、定期的な点検、秘密取扱情報システム、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置について熟知している者を配置すること。

- (2) 総括者は、防衛事業適合事業者契約の申込みをした日から事業者として秘密を取り扱うまでに、リスク評価、従業者への教育、秘密保全施設等の管理、定期的な点検、秘密取扱情報システム、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置についての防衛装備庁の研修を修了すること。

第3 基準3

- 1 総括者は、防衛事業適合事業者の契約代理人、防衛事業に関する事業本部長又は工場長その他の防衛事業適合事業者の経営責任者又は防衛事業の執行責任者として、防衛事業適合事業者及びその下請負事業者に対し、秘密の保全についての権限を行使できること。
- 2 第2の2(1)を満たすことができない場合には、以下の措置を講じること。
 - (1) 総括者は、防衛事業適合事業者契約の申込みをした日から事業者として秘密を取り扱うまでに、リスク評価、従業者への教育、秘密保全施設等の管理、定期的な点検、秘密取扱情報システム、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置についての防衛装備庁の研修を修了すること。
 - (2) 保全責任者、秘密取扱情報システム管理者、秘密取扱情報システム担当者、アカウント管理者その他秘密保全組織を管理する者は、防衛事業適合事業者契約の申込みをした日から事業者として秘密を取り扱うまでに1回及びその後は3か月に1回の頻度により合計4回、リスク評価、従業者への教育、秘密保全施設等の管理、定期的な点検、秘密取扱情報システム、下請負事業者との関係並びに事故対応を含め、日常的な秘密の取扱いに関する保全措置についての防衛装備庁の研修を修了すること。

防衛事業適合事業者契約申込書

年 月 日

防衛装備庁長官 殿
(装備政策部装備保全管理課長気付)
(地方防衛局調達部長等経由)

所 在 地
事業者名
代表者名

防衛装備庁と保護すべき情報の取扱いに係る防衛事業適合事業者契約の締結を申し込みます。なお、本申込みに係る契約条件は、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（装装保第 1 4 8 4 6 号。令和 7 年 7 月 3 1 日）別紙第 4 及び第 5 による契約条項に従うものとし、下記の事項に関する関係書類を提出します。

記

- 1 防衛事業に参画する意思の確認
防衛事業に参画する意思 有 / 無 （どちらかに○をしてください。）
- 2 参画を希望する事業の概要
- 3 契約締結者の確認
乙（契約当事者）として契約を締結する当事者名
- 4 関係書類
 - (1) 情報セキュリティ基本方針
 - (2) 情報セキュリティ規則
 - (3) 情報セキュリティ実施手順
 - (4) システムセキュリティ実装計画書
 - (5) 上記 4 つに係る防衛省からの確認通知の写し
 - (6) 直近の情報セキュリティ実地監査の結果通知の写し

添付書類： 関係書類

発 簡 番 号
発 簡 年 月 日

(事 業 者) 殿

防衛装備庁装備政策部長

○ ○ ○ ○

防衛事業適合事業者契約に係る審査の結果について（通知）

貴社からの防衛事業適合事業者契約申込書（ 年 月 日付）に係る標記について、下記のとおり通知します。

〔特定秘密も対象の場合〕 なお、特定秘密の保護に関する法律（平成 2 5 年法律第 1 0 8 号）第 5 条 4 項に規定する基準に適合すると認めましたことを合わせて通知します。）

記

- 1 申込内容について、 承諾する（契約する） / 承諾しない（契約しない）
- 2 防衛事業適合事業者契約番号：
- 3 契約の対象となる情報（秘密の種類・区分又は保護すべき情報）：
- 4 秘密保全施設の有無：
- 5 秘密取扱情報システムの有無：
- 6 承諾しない場合の理由等：

写送付先：地方防衛局調達部長等、契約担当官等

- 注：1 審査の結果、防衛事業適合事業者契約申込みが承諾された場合は、実際に秘密又は保護すべき情報を取り扱う直接の原因となる調達等の契約を締結する前に、防衛事業適合事業者契約を締結すること。
- 2 第3項には、防衛事業適合事業者契約の下で取り扱う情報（「特別防衛秘密（機密・極秘・秘）」、「特定秘密」、「装備品等秘密」又は「保護すべき情報」の別）を記載すること。
- 3 第4項及び第5項については、秘密に係る防衛事業適合事業者契約の申込みの場合に記載すること。

自己点検票（月次）

点検対象期間	
点検日	
事業者名	
作成日	
作成者	
確認日	
総括者	

地方防衛局等記入欄		防衛装備庁記入欄	
管轄防衛局等		確認日	
確認日		確認担当者	
確認者			

※事業者の形態に応じて別葉で作成すること

分 類	番 号	項 目	対応内容	対応内容の詳細 (件数、人数、管理の状況等を記載)	判定	備考
第1. 秘密取扱原因契約及び秘密文書等の継続保有		秘密取扱原因契約の状況				
	1	前回の月次点検時から秘密取扱原因契約の履行状況に変動があるか。ある場合、秘密取扱原因契約の一覧表が最新の内容であることを確認したか。				
		秘密文書等の継続保有の状況				
	2	秘密取扱原因契約の終了後も継続して保有している秘密文書等はあるか。ある場合、当該秘密文書等を継続保有する合理性があるか。				
第2. 秘密文書等の管理状況		前回の月次点検時から特定資料又は特定物件の保管状況に変動があるか。ある場合、保管簿を適切に更新したか。				
	3	特別防衛秘密文書等（機密）				
		特別防衛秘密文書等（極秘）				
		特別防衛秘密文書等（秘）				
	4	特定秘密文書等				
	5	装備品等秘密文書等				
		保有している秘密文書等の保管簿における件数は何件か。				
	6	特別防衛秘密文書等（機密）				
		特別防衛秘密文書等（極秘）				
		特別防衛秘密文書等（秘）				
	7	特定秘密文書等				
	8	装備品等秘密文書等				
		保有している秘密文書等の実物（保管の状況を別紙に記入する。）の件数は秘密文書等保管簿と一致しているか。				
	9	特別防衛秘密文書等（機密）				
		特別防衛秘密文書等（極秘）				
		特別防衛秘密文書等（秘）				
	10	特定秘密文書等				
	11	装備品等秘密文書等				
		前回の月次点検時から今回の点検時までの間に、秘密文書等の製作又は複製を行ったか。行った場合、秘密文書等複製等実施記録簿に記載したか。				
	12	特別防衛秘密文書等（機密）				
		特別防衛秘密文書等（極秘）				
		特別防衛秘密文書等（秘）				
	13	特定秘密文書等				
	14	装備品等秘密文書等				
		前回の月次点検時から今回の点検時までの間に、秘密文書等の反故紙の破棄／廃棄を行ったか。行った場合、反故紙廃棄簿に記載したか。				
	15	特別防衛秘密文書等（機密）				
		特別防衛秘密文書等（極秘）				
		特別防衛秘密文書等（秘）				
	16	特定秘密文書等				
	17	装備品等秘密文書等				
		前回の月次点検時から今回の点検時までの間に、関係簿冊の廃棄を行ったか。行った場合、関係簿冊廃棄記録簿に記載したか。				
18	特別防衛秘密					
19	特定秘密					
20	装備品等秘密					
	前回の月次点検時から今回の点検時までの間に、秘密文書等の閲覧を行ったか。行った場合、閲覧簿に記載したか。					
21	特別防衛秘密文書等（機密）					
	特別防衛秘密文書等（極秘）					
	特別防衛秘密文書等（秘）					
22	特定秘密文書等					
23	装備品等秘密文書等					

分 類	番号	項 目	対応内容	対応内容の詳細 (件数、人数、管理の状況等を記載)	判定	備考
第 2 ． 秘密文書等の管理状況		前回の月次点検時から今回の点検時までの間に、秘密文書等の貸出を行ったか。行った場合、貸出簿に記載したか				
	24	特別防衛秘密文書等（機密）				
		特別防衛秘密文書等（極秘）				
		特別防衛秘密文書等（秘）				
	25	特定秘密文書等				
	26	装備品等秘密文書等				
		前回の月次点検時から今回の点検時までの間に、保管容器の文字盤鍵の組合せ番号を変更したか。変更した場合、文字盤鍵組合せ番号変更記録簿に記載したか。				
	27	特別防衛秘密文書等				
	28	特定秘密文書等				
	29	装備品等秘密文書等				
		前回の月次点検時から今回の点検時までの間に、管理責任者又は保全責任者を変更したか。変更した場合、引継確認簿に記載したか。				
	30	特別防衛秘密				
	31	特定秘密				
	32	装備品等秘密				
		前回の月次点検時から今回の点検時までの間に、下請負事業者関係社員に特定資料等を取り扱わせたか。取り扱わせした場合、その記録を簿冊に適切に記載したか。				
	33	特別防衛秘密				
	34	特定秘密				
	35	装備品等秘密				
第 3 ． 施設の管理状況		保全外部区域の立入者の管理状況				
	36	保全外部区域の立入について、立ち入る必要のない者が立ち入ることができないよう措置されているか。				
		秘密保全施設の立入者の管理状況				
	37	秘密保全施設への立入りの状況を記録しているか。				
	38	立入記録簿に記載された立入者について、関係社員名簿その他の名簿に照らして適合しているか。				
		秘密保全施設の管理状況（代替措置を含む）				
	39	境界に前回の月次点検時には確認されなかった異常はないか。				
	40	出入口等の扉に前回の月次点検時には確認されなかった外傷がないか。				
	41	出入口等の扉の錠に前回の月次点検時には確認されなかった異常はないか。				
	42	警報装置に異常はないか。				
	43	監視カメラの動作に異常はないか。				
	44	鍵及び暗証番号の管理は適切に行われているか。				
	45	必要に応じて、扉の暗証番号の変更を行っているか（毎年 1 回以上、管理責任者の交代、漏えいの疑いがあった場合など）。				
	46	立入可能者以外の者が秘密保全施設等に立ち入ってはならない旨の掲示、立入可能者以外の者を必要以上に当該秘密保全施設等の付近に近付けない措置その他必要な措置を講じているか。				
	47	携帯型情報通信・記録機器の持込み禁止（防衛装備庁の事前の許可を受けたものを除く。）の掲示がされているか。				
	48	人の異動等に伴うカード認証のデータの更新が行われているか。				
		閉鎖区域の管理状況				
	49	境界に前回の月次点検時には確認されなかった異常はないか。				
	50	閉鎖区域の出入口等の扉に前回の月次点検時には確認されなかった外傷がないか。				
	51	閉鎖区域の出入口等の扉の錠に前回の月次点検時には確認されなかった異常はないか。				
	52	警報装置に異常はないか。				
	53	監視カメラの動作に異常はないか。				
	54	鍵及び暗証番号の管理は適切に行われているか。				
	55	必要に応じて、扉の暗証番号の変更を行っているか（毎年 1 回以上、管理責任者の交代、漏えいの疑いがあった場合など）。				
	56	立入可能者以外の者が秘密保全施設等に立ち入ってはならない旨の掲示、立入可能者以外の者を必要以上に当該秘密保全施設等の付近に近付けない措置その他必要な措置を講じているか。				
	57	携帯型情報通信・記録機器の持込み禁止（防衛装備庁の事前の許可を受けたものを除く。）の掲示がされているか。				
	58	人の異動等に伴うカード認証のデータの更新が行われているか。				

分 類	番号	項 目	対応内容	対応内容の詳細 (件数、人数、管理の状況等を記載)	判定	備考
第 3 . 施設の管理状況	保管容器の管理状況					
	59	扉及び鍵の動作に異常はないか。				
	60	鍵及び暗証番号の管理は適切に行われているか。				
	61	必要に応じて、扉の暗証番号の変更を行っているか（毎年 1 回以上、管理責任者の交代、漏えいの疑いがあった場合など）。				
第 4 . 関係社員の管理状況	前回の月次点検時から今回の点検時までの間に、関係社員の指定又は解除状況に変更があったか。場合、指定・解除簿を更新したか。					
	62	特別防衛秘密				
	63	特定秘密				
	64	装備品等秘密				
	秘密文書等の取扱いが必要な社員のうち、必要最小限の者が関係社員として指定／指名されているか。					
	65	特別防衛秘密				
	66	特定秘密				
	67	装備品等秘密				
	特定秘密取扱者に指名された社員は適性評価を保有しているか（有効期間が切れていないか）。					
	68	特定秘密				
	退職者が、関係社員として指定／指名されていないか。					
	69	特別防衛秘密				
	70	特定秘密				
	71	装備品等秘密				
	異動により、秘密文書等の取扱いができなくなった者が関係社員として指定／指名されていないか。					
	72	特別防衛秘密				
	73	特定秘密				
	74	装備品等秘密				
	適格証等の交付・回収を遅滞なく行っているか。					
	75	特別防衛秘密				
	76	特定秘密				
	77	装備品等秘密				
	適格証明書管理簿を適切に記載しているか。					
	78	特別防衛秘密				
	79	特定秘密				
	80	装備品等秘密				
第 5 . 教育の実施状況	81	前回の月次点検時から今回の点検時までの間に、新たに関係社員等（関係社員及び下請負事業者関係社員（この自己点検を行う事業者の秘密保全施設等に立ち入って秘密を取り扱う者に限る。83、86、89及び91において同じ。）をいう。）になった従業員がいたか。				
	上記に該当する場合、新たに関係社員等になった従業員に対して、取扱開始前に、取扱前教育を行ったか。					
	82	関係社員				
	83	下請負事業者関係社員				
	84	前回の月次点検時から今回の点検時までの間に、保全教育の年間計画に記載した臨時教育を行う場合の状況が生じたか。				
	上記に該当する場合、臨時教育を行ったか。					
	85	関係社員				
	86	下請負事業者関係社員				
	87	前回の月次点検時から今回の点検時までの間に、関係社員ではなくなることとなった従業員がいたか。				
	上記に該当する場合、当該者に取扱終了時教育を行ったか。					
	88	関係社員				
	89	下請負事業者関係社員				
	前回の月次点検時から今回の点検時までの間に、年間計画に記載した年次教育を行ったか。					
	90	関係社員				
	91	下請負事業者関係社員				
	関係社員以外の従業員への教育を行ったか。					
	92	関係社員以外の従業員				
	93	秘密の保全に関して、社内で適切な指導を行っているか。				
	94	関係社員に対して、守秘義務の自覚について指導を行っているか。				

分 類	番号	項 目	対応内容	対応内容の詳細 (件数、人数、管理の状況等を記載)	判定	備考
第 6．秘密取扱情報システムの使用状況		秘密取扱情報システムを適切に取り扱ったか。				
	95	秘密のデータは、秘密取扱情報システムに保存していないか。				
	96	秘密取扱情報システム以外の情報システムを、無断で設置していないか。				
	97	登録している携帯型情報通信・記録機器以外の機器を、無断で持ち込んでいないか。				
	98	秘密取扱情報システムのネットワークは、秘密保全施設内において有線により接続されているか（他の情報システム又は秘密取扱情報システムが設置された秘密保全施設等の外部との通信は、完全に遮断されているか）。				
第 7．その他の管理・実施状況	99	その他指導又は改善の指示をした事項はあるか。				
			総合判定		改善事項に対する措置	

自己点検票（月次）別紙

- 1 点検対象期間：
2 異常の有無：有・無（いずれかに○）

秘密文書等の保管の状況

(1) 装備品等秘密

区分	摘要	A	B					C					保管数	
		前回検査時の 保管数	増加要因					減少要因					A + B - C	指定前
			供与	複製	製作	接受	小計	返却／提出	解除	破棄	送達	その他 ()	小計	
	件 数	0					0						0	
	部 数	0					0						0	
備 考														

- 注：1 A～C各欄には、既に官から秘密に指定されているものを計上する。
2 保管数の指定前のものについては、その名称を備考欄に記載する。
3 文書及び図画（電磁的記録を含む。）と物件とをそれぞれ別葉で作成する。
4 B欄の「供与」には、官から貸与された文書等の数を計上する。同じく「接受」には、下請負者（又は元請負者）から送達された文書等の数を計上する。
5 C欄の「返却／提出」には、官に返却した文書等及び契約において製作又は複製した文書等で官に提出したものの数を計上する。同じく「送達」には、下請負者（又は元請負者）に送達した文書等の数を計上する。
6 C欄の「その他（）」には、紛失等の事故により減少した文書等の数を計上し、（）内に事故の事由を記載する。

(2) 特別防衛秘密

区分	摘要	A	B					C					保管数	
		前回検査時の 保管数	増加要因					減少要因					A + B - C	指定前
			供与	複製	製作	接受	小計	返却／提出	解除	破棄	送達	その他 ()	小計	
機 密	件 数	0					0						0	0
	部 数	0					0						0	0
極 密	件 数	0					0						0	0
	部 数	0					0						0	0
秘	件 数	0					0						0	0
	部 数	0					0						0	0
計	件 数	0	0	0	0	0	0	0	0	0	0	0	0	0
	部 数	0	0	0	0	0	0	0	0	0	0	0	0	0
備 考														

- 注：1 A～C各欄には、既に官から特別防衛秘密に指定されているものを計上する。
2 保管数の指定前のものについては、その名称を備考欄に記載する。
3 文書及び図画（電磁的記録を含む。）と物件とをそれぞれ別葉で作成する。
4 B欄の「供与」には、官から貸与された文書等の数を計上する。同じく「接受」には、下請負者（又は元請負者）から送達された文書等の数を計上する。
5 C欄の「返却／提出」には、官に返却した文書等及び契約において製作又は複製した文書等で官に提出したものの数を計上する。同じく「送達」には、下請負者（又は元請負者）に送達した文書等の数を計上する。
6 C欄の「その他（）」には、紛失等の事故により減少した文書等の数を計上し、（）内に事故の事由を記載する。

(3) 特定秘密

区分	摘要	A	B					C					保管数	
		前回検査時の 保管数	増加要因					減少要因					A + B - C	
			供与	複製	製作	接受	小計	返却／提出	解除	破棄	送達	その他 ()	小計	
機 密	件 数	0					0						0	0
	部 数	0					0						0	0
備 考														

- 注：1 B欄の「供与」には、官から貸与された文書等の数を計上する。同じく「接受」には、下請負者（又は元請負者）から送達された文書等の数を計上する。
2 C欄の「返却／提出」には、官に返却した文書等及び契約において製作又は複製した文書等で官に提出したものの数を計上する。同じく「送達」には、下請負者（又は元請負者）に送達した文書等の数を計上する。
3 C欄の「その他（）」には、紛失等の事故により減少した文書等の数を計上し、（）内に事故の事由を記載する。

付紙様式第14-1

発 簡 番 号

発 簡 年 月 日

(事 業 者) 殿

防衛装備庁装備政策部長

○ ○ ○ ○

契 約 解 除 通 知 書

標記について、 年 月 日付で貴社と締結した防衛事業適合事業者契約を解除します。

記

1 防衛事業適合事業者契約番号：

2 解除理由：

写送付先：地方防衛局調達部長等、契約担当官等

発 簡 番 号

発 簡 年 月 日

(事 業 者) 殿

防衛装備庁装備政策部長

○ ○ ○ ○

契 約 解 除 通 知 書

標記について、防衛事業適合事業者における保護すべき情報の情報セキュリティの確保に係る契約書第 5 条第 1 項【第 1 号／第 2 号／第 3 号／第 4 号】の規定に基づき、下記のとおり 年 月 日付で貴社と締結した防衛事業適合事業者契約を解除します。

記

- 1 防衛事業適合事業者契約番号：
- 2 解除理由：
(第 5 条第 1 項の各号から適用する内容を具体的に記述)

写送付先：地方防衛局調達部長等、契約担当官等

認証・防衛事業適合事業者契約整理簿

No	事業者（事業所）名	保全施設	情報取扱区分	認証年月日	認証番号	防衛事業適合事業者契約年月日	防衛事業適合事業者契約番号	備 考

備考 1：認証事業者の取消し又は防衛事業適合事業者契約の解除があった場合は、その旨を備考欄に記載すること。

2：認証又は防衛事業適合事業者契約の延長のあった場合は、それぞれ認証年月日又は防衛事業適合事業者契約年月日の欄に追記すること。

付紙様式第 16

発 簡 番 号

発 簡 年 月 日

(事 業 者) 殿

防衛装備庁装備政策部装備保全管理課長

○ ○ ○ ○

事業者に対する研修の実施について（通知）

標記について、防衛装備庁において以下のとおり研修を実施しますので、御参加ください。

記

1 日 時 :

2 対象者 :

3 備 考 :

別紙第 2

防衛事業適合事業者契約条項

防衛装備庁装備政策部装備保全管理課長 [氏名]（以下「甲」という。）及び[事業者名] [役職名] [氏名]（以下「乙」という。）は、防衛装備庁が定める手続による乙の申込みに基づき、秘密（日米相互防衛援助協定等に伴う秘密保護法（昭和 29 年法律第 166 号）第 1 条第 3 項に規定する特別防衛秘密、特定秘密の保護に関する法律（平成 25 年法律第 108 号。以下「特秘法」という。）第 3 条第 1 項に規定する特定秘密又は防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律（令和 5 年法律第 54 号）第 27 条第 1 項に規定する装備品等秘密をいう。以下同じ。）の保全又は保護に係る防衛事業適合事業者契約を締結する。

第 1 章 総則

（契約の目的）

第 1 条 乙は、この契約書に定めるところに従い、特定資料等を保護するものとする。

2 乙は、この契約を締結し、この契約が有効である間、防衛事業適合事業者として、秘密取扱原因契約及びこの契約に基づいて、秘密取扱原因契約の履行のために必要となる特定資料等を取り扱うことができる。

（定義）

第 2 条 この契約において次の各号に掲げる用語の意義は、それぞれ当該各号に定めるとおりとする。

- (1) 秘密取扱原因契約 この契約とは別の防衛装備庁と乙の間の装備品等の調達又は役務の履行に関する契約であって、乙が特定資料等を取り扱う直接の原因となるものをいう。
- (2) 特定資料 秘密取扱原因契約に基づいて乙に交付され、若しくは伝達され、又は乙が秘密取扱原因契約に基づいて保有し、受領し、若しくは作成した秘密に該当する文書、図画若しくは電磁的記録又は特定情報を記録する物件をいう。
- (3) 特定物件 秘密取扱原因契約に基づいて乙に交付され、又は乙が秘密取扱原因契約に基づいて保有し、受領し、若しくは作成した秘密に該当する物件、作成途上にあるその仕掛品又はこれらにより構成される物件をいう。

- (4) 特定情報 秘密取扱原因契約に基づいて乙が知得した秘密に該当する情報をいう。
- (5) 特定資料等 特定資料、特定物件又は特定情報をいう。
- (6) 関係社員 乙の従業者であって、秘密取扱原因契約及びこの契約に基づいて特定資料等の取扱いが認められた者をいう。
- (7) 下請負事業者関係社員 下請負事業者の従業者であって、秘密取扱原因契約及びこの契約に基づいて特定資料等の取扱いが認められた者をいう。
- (8) 秘密保全施設 特定資料等を情報漏えいの蓋然性の極めて低い環境で安全に取り扱い、又は嚴重に保管するため、不法な侵入、秘密の窃取等を防止し、入退室を管理し、不審な立入りを検知するなどの秘密を保全するための機能を備えた乙が管理する施設であって、特定資料等を常続的に取り扱う施設として甲の承認を得たものをいう。
- (9) 閉鎖区域 特定資料等を情報漏えいの蓋然性の極めて低い環境で安全に取り扱うため、不法な侵入、秘密の窃取等を防止し、入退室を管理し、不審な立入りを検知するなどの秘密を保全するための機能を備えた乙が管理する区域であって、短期的に特定資料等を取り扱う区域として甲の承認を得たものをいう。
- (10) 制限区域 特定資料等を情報漏えいの蓋然性の極めて低い環境で安全に取り扱うため、不法な侵入、秘密の窃取等を防止し、区域への入退を管理し、不審な立入りを検知するなどの秘密を保全するための機能を備えた乙が管理する区域であって、当該区域を管理する者の常続的な監督及び監視の下、一時的に特定資料等を取り扱う区域として甲の承認を得たものをいう。
- (11) 秘密保全施設等 秘密保全施設、閉鎖区域又は制限区域をいう。
- (12) 装備政策部長 防衛装備庁装備政策部長をいう。
- (13) 管轄防衛局等 乙が所在する地域を管轄する地方防衛局、地方防衛局地方防衛支局、地方防衛局地方防衛事務所又は地方防衛局地方防衛支局地方防衛事務所をいう。
- (14) 秘密の管理職員 秘密取扱原因契約に基づいて乙に特定資料等を取り扱わせる意思決定をし、乙における特定資料等の取扱いの状況を管理し、及び監督する防衛装備庁の職員であって、特定資料等が特別防衛秘密である場合にあっては秘密取扱原因契約の契約担当官等（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2条に規定する契約担当官等をいう。以下同じ。）を、特定資料等が特定秘密である場合にあっては防衛装備庁における特定秘密の保護に関する訓令（平成27年防衛装備庁訓令第27号）第3条に規定する特定秘密管理者を、特定資料等が装備品

等秘密である場合にあっては装備品等秘密の指定等に関する訓令（令和 6 年防衛省訓令第 10 号）第 2 条第 2 号に規定する契約締結者をいう。

- (15) 情報システム 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。
- (16) 秘密取扱情報システム 秘密を取り扱う情報システムをいう。
- (17) 秘密取扱情報システムセキュリティ実装計画（SSP） 情報システムが秘密取扱情報システムに求められる基準を満たしていることを証明する資料一式であって、ホワイトリスト、構成設定目録、操作手順書、アクセス制御方針、携帯型情報通信・記録機器の利用に係る要件、秘密取扱情報システムのセキュリティを確保するための組織体制、秘密取扱情報システムのネットワーク構成図及び秘密のデータのデータフロー図から構成されるものをいう。
- (18) 可搬記憶媒体 防衛省の情報保証に関する訓令第 2 条第 5 号に規定する可搬記憶媒体をいう。
- (19) 携帯型情報通信・記録機器 携帯電話、携帯情報端末、映像走査機器（ハンディスキャナー）、写真機、録音機その他の通話、記録等の機能を有する容易に携行できる機器をいう。
- (20) 秘密取扱情報システム利用者 秘密取扱情報システムを利用することが認められた者をいう。

（防衛事業適合事業者の一般義務）

- 第 3 条 乙は、その従業者、下請負事業者の従業者（下請負を行う場合に限る。以下同じ。）又は乙が秘密保全施設等への立入りを認めた者（甲の職員又は乙若しくは下請負事業者の従業者を除く。）の故意又は過失により乙が管理する秘密が漏えいしたときは、その責任を負うものとする。
- 2 乙は、総括者を配置しなければならない。総括者は、乙において特定資料等の保護に関する業務の全般を総括する責任者であり、特定資料等の取扱いの業務の全般を管理するものとする。
 - 3 乙は、特定資料等の保護及び取扱いに関し、次の各号に掲げる事項を含め、その従業者が遵守すべきことを明確にしなければならない。
 - (1) 関係社員以外の乙の従業者は、特定資料等に接してはならないこと。
 - (2) 役員、管理職員その他の関係社員の職務上の上級者であって、関係社員でない者は、職務上の下級者である関係社員に対し、自らが特定資料等に接することを求めてはならないこと。
 - 4 乙は、特定資料等の取扱いに関する法令又は秘密保全規則（秘密保全規則とあわせて秘密保全実施要領を定めている場合はこれを含む。以下同じ。）

に違反した従業者に対する正式な懲戒手続を備えなければならない、かつ、懲戒を確実に実施しなければならない。

(譲渡等の禁止)

第4条 乙は、防衛事業適合事業者としての立場を第三者に譲渡し、又は貸与してはならない。

(無償契約)

第5条 この契約は、甲乙間に、この契約を原因とした金銭のやり取りを生じさせるものではない。

2 前項の規定は、秘密取扱原因契約に基づき、この契約の履行に係る違約金その他の金銭のやり取りを定めることを排除するものではない。

(適用範囲)

第6条 この契約は、甲乙間でこの契約が適用されることを確認した特定資料等に適用する。

2 前項の規定を実施するため、甲及び乙は、この契約の適用を受ける秘密取扱原因契約を網羅したリストを作成し、装備政策部長が別に定めるところにより、定期的に更新するものとする。

3 この契約に基づいて特定資料等を取り扱うことのできる乙の組織の範囲は、付紙第1に示すとおりとする。

4 付紙第1に示す乙の組織の範囲に変更があった場合には、乙は、これを更新するため、甲にこの契約の変更を申し入れなければならない。ただし、当該変更が軽微なものであって、甲乙間において、変更の前後における当該乙の組織の範囲について疑義が生じないことが確認されたときは、乙は、変更後の組織の範囲を甲に届け出ることによりこれを更新することができる。

(取り扱う秘密の区分)

第7条 乙が取り扱うことのできる秘密の区分は、＜特別防衛秘密、特定秘密及び装備品等秘密＞(注)とする。

(注) この契約の対象となる秘密の区分を選ぶ。

2 乙が特別防衛秘密、特定秘密又は装備品等秘密のいずれかを取り扱わない場合におけるこの契約の適用に当たっては、下表の左欄に掲げる取り扱わない秘密の区分に応じ同表の右欄に掲げる適用されない条項を適用しない。

取り扱わない秘密の区分	適用されない条項
-------------	----------

特別防衛秘密	第 1 8 条第 2 項、第 2 6 条第 2 項、 第 4 6 条及び第 5 2 条第 5 項
特定秘密	第 1 8 条第 3 項、第 2 6 条第 3 項、 第 4 4 条、第 4 7 条から第 5 0 条ま で、第 5 2 条第 5 項、第 5 4 条、第 5 6 条及び第 6 0 条第 2 項
装備品等秘密	第 2 6 条第 4 項、第 2 7 条第 3 項及 び第 5 1 条

第 2 章 秘密保全体制

第 1 節 秘密保全体制の整備・維持

(秘密保全体制の整備・維持)

第 8 条 乙は、この契約の締結に先立ち、取り扱う秘密の区分に応じて装備政策部長が別に定める要件に従い、総括者の指名、保全責任者の配置その他防衛事業適合事業者であるための秘密保全組織を整え、外国からの影響及び支配の程度を評価し、秘密保全規則を定め、関係社員に対する教育の体制を整え、及び教育を実施し、秘密保全施設及び秘密取扱情報システムを構築するなど、乙において特定資料等を保全する体制を整備しなければならない。

2 乙は、秘密取扱情報システムを構築する場合には、秘密取扱情報システム管理者の配置その他秘密取扱情報システムで取り扱う特定資料等を保全するための組織を整え、秘密取扱情報システムセキュリティ実装計画（SSP）を定め、秘密取扱情報システム利用者に対する教育の体制を整え、及び教育を実施するなど、秘密取扱情報システムにおいて特定資料等を保全する体制を整備しなければならない。

3 前 2 項の規定にかかわらず、乙は、自己の秘密保全施設又は秘密取扱情報システムを整備せずに防衛事業適合事業者となることを希望するときは、秘密保全施設又は秘密取扱情報システムを備えない限定的な防衛事業適合事業者となることができる。この場合におけるこの契約の適用に当たっては、下表の左欄に掲げる整備しない特定資料等を保全する体制の区分に応じ同表の右欄に掲げる適用されない条項を適用しない。

整備しない特定資料等を保全する体制の区分	適用されない条項
秘密保全施設	第 1 2 条第 4 号（乙の秘密保全施設等に係る部分に限る。）、第 2 0 条第 4 項、第 2 1 条第 1 項（乙の保全施設等に立ち入る者に対する教育に

	限る。）、第22条第6項、第25条、第4章第1節、第43条第1項（下請負事業者関係社員に関するものに限る。）、第57条第3項、第60条、第66条第2項第1号及び第69条
秘密取扱情報システム	第59条

- 4 乙は、前項の規定により秘密保全施設又は秘密取扱情報システムを備えない限定的な防衛事業適合事業者となる場合において、その従業者に、他の防衛事業適合事業者又は特定資料等の取扱いが認められた事業者の秘密保全施設内において、又はこれらの事業者の秘密取扱情報システムを利用して、特定資料等を取り扱わせようとするときは、かかる特定資料等の取扱いの態様に対応した特定資料等を保全する体制を整備しなければならない。
- 5 この契約に基づいて特定資料等を取り扱うことのできる乙の秘密保全施設及び秘密取扱情報システムは、付紙第2に示すとおりとする。
- 6 付紙第2に示す乙の秘密保全施設及び秘密取扱情報システムに変更があった場合には、乙は、これを更新するため、甲にこの契約の変更を申し入れなければならない。ただし、当該変更が軽微なものであって、甲乙間において、変更の前後における当該乙の組織の範囲について疑義が生じないことが確認されたときは、乙は、変更後の組織の範囲を甲に届け出ることによりこれを更新することができる。
- 7 乙は、この契約が有効である間、第1項から第4項までの規定により整備した特定資料等を保全する体制を継続して維持しなければならない。
- 8 甲は、情報の保護に係る法令の改廃、諸外国と締結し、又は署名した情報の保護に関する協定又は取決めの改廃その他情報の保護に関して防衛事業適合事業者を取り巻く環境に変動があったときは、第1項から第3項までに定める秘密の区分に応じた要件を変更することができる。この場合においては、変更後の要件を乙に適用するまでに、原則として、1年を超えない経過措置を設け、乙に及ぼす影響を緩和するものとする。

（新たな秘密保全施設及び秘密取扱情報システムの構築）

- 第9条 乙は、この契約の締結後、この契約が有効である間に新たに秘密保全施設又は秘密取扱情報システムを構築する必要がある場合には、装備政策部長が別に定めるところにより甲の承認を得て、前条第1項又は第2項に定める秘密の区分に応じた要件に合致したものを構築しなければならない。

- 2 前項の規定により新たに秘密保全施設又は秘密取扱情報システムを構築する場合において、前条第1項及び第2項に定める秘密の区分に応じた要件を満たすことのできないやむを得ない事由があるときは、乙は、当該秘密保全施設又は秘密取扱情報システムにおいて取り扱う特定の特定資料等に関して予想される秘密の保全上の脅威を明らかにした上で、同項に定める秘密の区分に応じた要件と実質的に同等と認められる当該特定の特定資料等を保全する体制を甲に提案し、その承認を得た上で、当該特定の特定資料等に限った秘密保全施設又は秘密取扱情報システムを構築することができる。

(特別な秘密保全体制)

第10条 甲は、特定資料等の保護措置に関する外国政府からの要請その他の事由により、第8条第1項及び第2項に規定する要件では特定の特定資料等を保全する体制が十分ではないと認める特段の事由がある場合には、乙に対し、これらの規定による特定資料等を保全する体制に加え、当該特定の特定資料等を保全するための特別な秘密保全体制を構築し、これを維持するよう求めることができる。

- 2 前項の規定による特別な秘密保全体制の構築及び維持は、この契約の特約に基づき実施するものとする。

(秘密保全体制の変更)

第11条 乙は、前3条の規定に基づき構築した秘密保全体制（外国からの影響及び支配の程度に係る評価を除く。）を変更する必要があると認めた場合には、あらかじめ、管轄防衛局等を経由して甲の承認を得なければならない。

第2節 総括者

(総括者)

第12条 乙は、総括者に、次の各号に掲げる事項その他防衛事業適合事業者として取り扱う特定資料等を秘密の区分ごとに適切に保護するための措置を講じさせなければならない。

- (1) 特定資料等を取り扱うために必要な知識を自ら取得し、これを維持すること。
- (2) 保全責任者その他の総括者の下で日常的に特定資料等の保護に関する業務に従事する者に必要な知識を取得させ、及びこれを維持させること。
- (3) 特定資料等を取り扱う乙の関係部署の長並びに関係社員の責任及び役割を明確にすること。

- (4) 関係社員及び乙の秘密保全施設等において特定資料等を取り扱う全ての者に対して秘密保全規則を遵守させること。

第3節 関係社員

(従業者の範囲の決定)

第13条 乙は、秘密の区分に応じた手続に従い、秘密の区分ごとに特定資料等の取扱いの業務を行わせようとする従業者の範囲を決定するものとする。

2 前項の規定により特定資料等の取扱いの業務を行わせようとする従業者の範囲を決定するに当たっては、特定資料等の取扱いの業務を行うことに同意しない従業者を当該範囲に含めてはならない。

3 第1項の規定により決定する特定資料等の取扱いの業務を行わせようとする従業者の範囲は、特定資料等を取り扱うことがふさわしいと認められた従業者の中から、その責任及び役割を明確にし、秘密を知得させる必要性を考慮して最小限にとどめなければならない。

4 乙は、その従業者について特定資料等を取り扱うことがふさわしいと認めるに当たっては、防衛装備庁との契約又はこの契約に違反する行為を求められた場合にこれを拒む権利を実効性をもって法的に保障されない者を認めてはならない。

(関係社員候補者名簿)

第14条 乙は、前条の規定により従業者の範囲を決定するときは、秘密取扱原因契約ごとに、秘密の区分に応じた関係社員候補者名簿（装備政策部長が別に定める様式に関係社員の氏名、生年月日、所属する部署、役職、国籍等を記載した名簿をいう。以下同じ。）を作成しなければならない。

2 乙は、前項の規定により関係社員候補者名簿を作成するときは、従業者を関係社員候補者名簿に掲載すること、人的クリアランスに関する確認を行うこと等について、当該従業者の同意を得なければならない。

3 乙は、前2項の規定により作成した関係社員候補者名簿に掲載された従業者に特定資料等の取扱いの業務を行わせることについて、甲の同意を得なければならない。

4 乙は、前項に規定する甲の同意を得るまでは、関係社員候補者名簿に掲載された従業者に特定資料等の取扱いの業務を行わせてはならない。

(関係社員名簿)

第15条 乙は、前条第3項に規定する甲の同意を得たときは、特定資料等の取扱いの業務から離れた後を含め、特定資料等の取扱いの業務を通じて知得

した秘密を保全する責任があること等について、甲の同意を得た従業者の同意を得なければならない。

- 2 前条第3項に規定する甲の同意及び前項に規定する甲の同意を得た従業者の同意のいずれも得られた従業者が掲載された名簿を関係社員名簿とする。
- 3 乙は、関係社員名簿に掲載された従業者を変更しようとするときは、前条及び第1項に規定する手続をとらなければならない。

(従業者の範囲の決定に係る禁止事項)

第16条 乙は、前2条の規定による関係社員候補者名簿又は関係社員名簿の作成に関し、次の各号に掲げる者に人事上その他の不利益な取扱いをしてはならない。

- (1) 特定資料等の取扱いの業務を行うことに同意しなかった従業者
 - (2) 関係社員候補者名簿に掲載された従業者のうち甲の同意が得られなかった者
- 2 乙は、関係社員候補者名簿又は関係社員名簿に掲載された情報をこの契約を履行する目的以外のために利用してはならない。

(従業者からの同意書)

第17条 第14条第2項の規定に基づく従業者の同意及び第15条第1項の規定に基づく甲の同意を得た従業者の同意については、次の各号に掲げる秘密の区分に応じ、当該各号に定める同意書を得るものとする。

- (1) 特別防衛秘密又は装備品等秘密 装備政策部長が別に定める同意書
 - (2) 特定秘密 適性評価（特秘法第12条第1号の適性評価をいう。以下同じ。）に関して別に定められた同意書
- 2 同一の従業者が複数の秘密取扱原因契約に関して特定資料等の取扱いの業務に従事しようとする場合の前項第1号の同意書の取得については、一の秘密取扱原因契約に係る同号の同意書を取得したときは、その他の秘密取扱原因契約に係る同号の同意書の取得を省略することができる。ただし、同意書の記載内容に変更があった場合、同意書を出した従業者が関係社員となつてから一定の期間を経た場合その他の装備政策部長が別に定める場合にあつては、この限りでない。

(人的クリアランスの事務)

第18条 乙は、この契約に基づいて甲が乙の従業者に対して行う人的クリアランスの確認に関する事務に協力するものとする。

- 2 乙は、特定特別防衛秘密（防衛大臣又は防衛装備庁長官が特別の保護を要するものとして指定した特別防衛秘密をいう。）を取り扱う従業者の人的クリアランスの確認に関し、甲又は秘密の管理職員の指示するところにより事務を行うものとする。
- 3 乙は、特定秘密を取り扱う従業者について、防衛装備庁長官が行う適性評価に関し、付紙第3に規定する事務を行うものとする。

第4節 外国からの影響及び支配

（外国からの影響及び支配）

第19条 乙は、乙における特定資料等の取扱いに対する外国からの影響及び支配の程度について、装備政策部長が別に定めるところに従い、定期的に評価しなければならない。

第5節 秘密保全規則

（規則）

第20条 秘密保全規則は、この契約の内容を反映したものでなければならない。

- 2 乙は、特定資料等の取扱いの業務の管理を行う従業者の管理の業務ごとに当該従業者の責任及び役割を定め、及び他の特定資料等の取扱いの業務を行う関係社員による確認、監視等の手順を定め、全ての関係社員に乙の監督が及ぶようにしなければならない。
- 3 乙は、秘密保全規則が確実に履行されるよう、関係社員及び関係社員以外の従業者に対し、その内容を周知するなど、それぞれの従業者の責任及び役割に応じた措置を講じなければならない。
- 4 前項に規定する措置を講じるに当たり、乙の秘密保全施設等において特定資料等の取扱いの業務を行う下請負事業者関係社員があるときは、当該下請負事業者関係社員に適用される下請負事業者の秘密保全規則との関係を整理しなければならない。

第6節 教育

（教育の計画）

第21条 乙は、その従業者、下請負事業者関係社員（下請負を行う場合に限る。）及び乙の秘密保全施設等に立ち入る者に対し、定期的に、及び臨時に特定資料等の取扱に関する教育を行うものとし、このため、年度の教育計画その他特定資料等に係る秘密の保全に関する教育の計画を定めなければならない。

2 前項に規定する教育の計画は、総括者が定めるものとする。

(関係社員及び下請負事業者関係社員に対する教育)

第22条 乙は、関係社員に対し、特定資料等の保護に必要な知識の習得及び意識の高揚を図るための教育を実施しなければならない。この教育には、次の各号に掲げる事項を含むものとする。

- (1) 秘密保全の重要性及び意義（秘密保全意識の醸成を含む。）に関すること。
 - (2) 「need to knowの原則」（「情報は知る必要がある者にのみ伝え、知る必要のない者には伝えない」という原則）を確実に履行すること。
 - (3) 情報保全に関する組織内の規則を確実に履行すること。
 - (4) 隙のない勤務と私生活において慎重に行動すること。
 - (5) 悪意のあるソフトウェアへの感染（特に可搬記憶媒体を介した感染）、内部不正等を防止するための対策及び感染した場合の対処手順に関すること。
 - (6) 業務上の役割と責任に応じて行動すること。
 - (7) 前各号に掲げる事項のほか、秘密保全規則その他の乙において業務上取り扱う情報の保全に関すること。
- 2 関係社員に対する教育は、取扱前教育（新たに関係社員になった従業員に対する教育をいう。次項において同じ。）、年次教育、臨時教育及び取扱終了時教育（関係社員ではなくなることとなった従業員に対する教育をいう。第5項において同じ。）とする。
- 3 乙は、取扱前教育について、新たに関係社員となった従業員が特定資料等の取扱いの業務を行う前に実施しなければならない。
- 4 乙は、年次教育について、関係社員が少なくとも年1回受講できるよう計画的に実施しなければならない。ただし、計画にない教育を行う必要が認められた場合は、随時のタイミングで臨時教育を実施するものとする。
- 5 乙は、取扱終了時教育について、関係社員ではなくなることとなった従業員に対して、当該者による特定資料等の取扱いの業務の終了後速やかに行わなければならない。
- 6 乙は、乙の秘密保全施設等において特定資料等の取扱いの業務を行う下請負事業者関係社員があるときは、当該下請負事業者関係社員に対し、当該下請負事業者関係社員による特定資料等の取扱いの業務の内容及び態様に応じ、前各項の規定に準じた教育を行わなければならない。

(関係社員以外の従業員への教育)

第23条 乙は、関係社員以外の従業者に対し、次の各号に掲げる事項を徹底しなければならない。

- (1) 関係社員以外の従業者は特定資料等に接してはならないこと。
- (2) 役員、管理職員その他の関係社員の職務上の上級者は、関係社員に指定されていない場合には、職務上の下級者である関係社員に対し、自らが特定資料等に接することを求めてはならないこと。
- (3) 前2号に掲げる事項のほか乙における特定資料等の取扱いの業務を管理する上で必要なこと。

(従業者等への教育の記録)

第24条 乙は、前2条の規定により従業者及び下請負事業者関係社員（乙の秘密保全施設等において特定資料等の取扱いの業務を行う下請負事業者関係社員がある場合に限る。）に対して行った教育の結果について、記録しなければならない。

(秘密保全施設等に立ち入る者への教育)

第25条 乙は、乙の秘密保全施設等への立入りを認めた乙の従業者以外の者に対し、それぞれの責任若しくは役割又は立入りの目的に応じた教育を行わなければならない。

第3章 秘密の提供及び返却

(交付・保有)

第26条 秘密取扱原因契約に関して行われる乙に対する特定資料等の提供（乙に特定資料等を保有させ、伝達し、又は交付することをいう。以下同じ。）は、秘密の管理職員又はその指定した者を通じて行うものとする。

- 2 前項の場合において、特別防衛秘密である特定資料等を提供するときは、秘密の管理職員又はその指定した者は、秘密区分（機密、極秘又は秘の別）及び米国政府の表示を確認するものとする。
- 3 第1項の場合において、特定秘密である特定資料等を提供するときは、当該特定資料等を乙に提供する旨を記載し、又は記録した文書又は電磁的記録を添えて行うものとする。
- 4 第1項の場合において、装備品等秘密である特定資料等を提供するときは、装備品等秘密指定書（当該特定資料等において装備品等秘密を記録し、又は化体する部分を特定するために必要な事項を記載した書面をいう。以下同じ。）を添えて行うものとする。

- 5 甲は、第1項の規定により特定資料等の交付を行う場合には、交付する特定資料等に係る秘密に該当する区分を示す表示その他の装備政策部長が別に定める表示を付すものとする。ただし、表示を付すことが困難な場合においては、この限りでない。

(返却)

第27条 乙は、秘密取扱原因契約の契約期間が終了（契約の解除に伴う契約期間の終了の場合を含む。）したときは、当該秘密取扱原因契約に関して交付を受けた特定資料等及び当該特定資料等に関して作成した全ての特定資料等について、秘密の管理職員又はその指定した者に直ちに返却し、又は提出しなければならない。

- 2 前項の場合において、秘密の管理職員又はその指定した者が、乙による特定資料等の廃棄又は引き続きの保有を認め、又はかかる旨の指示をしたときは、当該秘密の管理職員又はその指定した者の指示に従うものとする。

- 3 前2項の規定にかかわらず、装備品等秘密指定書に示された装備品等秘密の指定の有効期間が満了した場合には、乙は、当該装備品等秘密指定書に係る特定資料等を直ちに甲に返却し、又は提出しなければならない。

(廃棄)

第28条 乙は、この契約に定められた場合を除き、特定資料等を廃棄してはならない。

第4章 保護措置

第1節 秘密保全施設等の管理

(保全外部区域)

第29条 乙は、保全外部区域（秘密保全施設への不正な立入りを防止するため、秘密保全施設の外側に隣接する建物又は敷地であつて、立入りを管理すべき区画として指定したものをいう。以下同じ。）を設け、及びその外側境界に入退口を設置しなければならない。

- 2 乙は、保全外部区域への立入りを許可する者の名簿を作成し、保全外部区域への立入りを管理しなければならない。当該名簿は、定期的に、及び必要に応じて見直すものとする。

(閉鎖区域の構築)

第30条 乙は、閉鎖区域において特定資料等を取り扱う必要が生じた場合には、第7条に定める秘密の区分に応じた要件に合致したものを構築した上

で、当該閉鎖区域の設定に係る手続を定めた秘密保全規則の改正案を添えて、第9条の新たな秘密保全施設の構築の規定に準じて、甲の承認を得なければならない。

- 2 前項の規定により閉鎖区域を構築する場合において、第8条第1項に定める秘密の区分に応じた要件を満たすことのできないやむを得ない事由があるときは、乙は、当該閉鎖区域において取り扱う特定の特定資料等に関して予想される秘密の保全上の脅威を明らかにした上で、同項に定める秘密の区分に応じた要件と実質的に同等と認められる当該特定の特定資料等を保全する体制を甲に提案し、その承認を得た上で、当該特定の特定資料等に限った閉鎖区域を構築することができる。

(閉鎖区域の設定)

第31条 乙は、閉鎖区域において特定資料等を取り扱う場合には、あらかじめ、当該閉鎖区域を使用する目的、期間を定め、装備政策部長が別に定めるところにより、当該閉鎖区域を設定する旨を甲に届け出なければならない。この場合において、閉鎖区域の設定の期間は、防衛省に引き渡される建造中の艦船内に構築される閉鎖区域を除き、3か月を超えることはできない。

- 2 乙は、閉鎖区域を設定しようとするときは、当該閉鎖区域における特定資料等の取扱いに先立って、次の各号に掲げる事項を点検しなければならない。
 - (1) 当該閉鎖区域が引き続き前条第1項の規定により甲の承認を得た要件又は同条第2項の規定により甲の承認を得た体制を満たすこと。
 - (2) 当該閉鎖区域に不法な侵入、秘密の窃取等を可能とし、又はそれらを容易にする機能を有する機器が設置されていないこと。
 - (3) 当該閉鎖区域において、閉鎖区域の設定の期間を通じて、この章に定める保護措置が確実に執られること。
- 3 乙は、閉鎖区域の設定を解除したとき（第1項の規定により届け出た設定の期間を満了した場合を含む。）は、装備政策部長が別に定めるところにより、その旨を甲に届け出なければならない。
- 4 乙は、第1項の規定により届け出た内容を変更しようとするときは、その旨の届出を甲に対して行わなければならない。

(制限区域の承認)

第32条 乙は、制限区域において特定資料等を取り扱う必要が生じた場合には、当該制限区域において取り扱う特定の特定資料等に関して予想される秘密の保全上の脅威を明らかにし、及び当該制限区域を使用する目的、場所、

時間等を勘案した上で、管理者の配置、境界の設定、区域の監督及び監視、立入りの制限、管理規則その他秘密の保全上の対応策を定めなければならない。

- 2 乙は、前項の秘密の保全上の対応策について、装備政策部長が別に定めるところにより、制限区域における特定の特定資料等の取扱いの必要性、当該制限区域における特定資料等の取扱いに伴い予想される秘密の保全上の脅威及び乙による当該制限区域の妥当性の詳細について、秘密の管理職員の確認を得た上で、甲の承認を得なければならない。
- 3 制限区域に配置される管理者及び当該管理者の業務を一時的に代行する者は、甲が実施する研修を修了した者でなければならない。

(制限区域の設定)

第33条 乙は、制限区域を設定しようとするときは、当該制限区域における特定資料等の取扱いに先立って、次の各号に掲げる事項を点検しなければならない。

- (1) 当該制限区域において前条第2項の規定により甲の承認を得た秘密の保全上の対応策が執られること。
- (2) 当該制限区域に不法な侵入、秘密の窃取等を可能とし、又はそれらを容易にする機能を有する機器が設置されていないこと。
- (3) 当該制限区域において、制限区域の設定の時間を通じて、この章に定める保護措置が確実に執られること。
- 2 制限区域を設定し、及び使用できる時間は、当該制限区域が設定された乙が管理する場所の通常の業務時間の範囲内でなければならない。
- 3 制限区域において特定資料等が取り扱われているときは、当該制限区域を管理する者は、当該制限区域における特定資料等の取扱いの業務に立ち会い、並びに当該制限区域を常続的に監督し、及び監視し、当該制限区域における秘密の保全に専従しなければならない。
- 4 制限区域を特定資料等の保管の目的で使用してはならない。

(保全外部区域の立入管理)

第34条 乙は、保全外部区域について、立ち入る必要がない者の立入りを認めてはならない。

(立入制限措置等)

第35条 乙は、秘密保全施設等について、特定資料等を取り扱うことのできる関係社員又は下請負事業者関係社員（下請負を行う場合に限る。）及び甲又は甲の指定した者が立入りを許可した者（次項において「立入可能者」という。）以外の者の立入りを禁止しなければならない。

- 2 乙は、立入可能者以外の者が秘密保全施設等に立ち入ってはならない旨の掲示、立入可能者以外の者を必要以上に当該秘密保全施設等の付近に近付けない措置その他同項の措置を実施するために必要な措置を講じなければならない。

（携帯型情報通信・記録機器の持込制限）

第36条 乙は、秘密保全施設等への携帯型情報通信・記録機器の持込みを禁止しなければならない。

- 2 前項の規定にかかわらず、やむを得ず秘密保全施設等に携帯型情報通信・記録機器の持込みが必要となった場合には、乙は、甲の事前の許可を得た上で持ち込むことができる。この場合においては、乙は、持ち込む携帯型情報通信・記録機器について、装備政策部長が別に定める措置を講じなければならない。

（情報システムの持込・設置制限）

第37条 乙は、秘密保全施設等に情報システムを持ち込み、又は設置する場合には、甲の許可を得なければならない。

- 2 前項の許可を得て情報システムを持ち込む場合には、乙は、装備政策部長が別に定める措置を講じなければならない。
- 3 第1項の許可を得て情報システムを設置する場合には、乙は、秘密取扱情報システムに準じた保全措置を講じなければならない。

（秘密保全施設等の運用管理）

第38条 乙は、装備政策部長が別に定めるところにより、秘密保全施設等への立入りの状況を記録し、不審な立入りがいないかどうか当該記録を定期的に精査し、その結果を記録しなければならない。

- 2 乙は、秘密保全施設等に立ち入る者（次項において「立入者」という。）に対し、当該秘密保全施設等への立入りが許可された者であることを外形的に証する識別証（バッジ等）を着用させなければならない。
- 3 乙は、秘密保全施設等を運用し、及び管理するために必要な細部の手続を定め、実施しなければならない。当該手続には、次の各号に掲げる措置を含めるものとする。

- (1) 秘密保全施設等の鍵の管理に関すること（物理鍵を用いる場合にあっては、保管、接受等に関すること。暗証番号鍵を用いる場合にあっては、共有、更新等に関すること。電子鍵を用いる場合にあっては、発行、回収等に関すること。）。
 - (2) 秘密保全施設等の警備に関すること。
 - (3) 立入者が着用する識別証（バッジ等）の発行等に関すること。
 - (4) 立入りの概況の記録（立入者の所属、氏名、立入目的、入退室の日時等）の取得に関すること（電子的に取得する場合を含む。）。
 - (5) 立入りの概況の記録の精査に関すること。
 - (6) その他秘密保全施設等の運用及び管理のために必要なこと。
- 4 乙は、第1項の記録の内容が改ざんされないよう措置した上で、装備政策部長が別に定める期間、同項の記録を保管しなければならない。保管期間の経過後の当該記録の廃棄に当たっては、あらかじめ甲の確認を受けるものとする。

第2節 供覧及び交付等の範囲

（供覧）

- 第39条 乙は、特定資料等を当該特定資料等の関係社員以外の者に供覧してはならない。
- 2 乙は、特定資料等の関係社員であっても、現に当該特定資料等について取り扱う必要のない従業者に当該特定資料等を供覧してはならない。

（第三者への交付及び伝達の禁止）

- 第40条 乙は、特定資料等について、次条に規定する場合その他の秘密の管理職員の許可を得た場合を除き、第三者に提供してはならない。

（下請負事業者への交付及び伝達）

- 第41条 乙は、秘密取扱原因契約の履行のためやむを得ず下請負事業者に特定資料等を取り扱わせる場合であって、当該下請負事業者が当該特定資料等を取り扱うことができることについての秘密の管理職員の許可をあらかじめ得たときは、当該下請負事業者に当該特定資料等を交付し、又は伝達することができる。

第3節 登録及び記録

（登録及び管理）

第42条 乙は、特定資料等の管理の現況について、装備政策部長が別に定めるところにより、秘密文書等保管簿その他の帳簿に登録しなければならない。

2 前項の帳簿は、秘密の種類ごとに（必要な場合は、これに加え、機密、極秘及び秘の区分ごとに）整備するものとし、指定の状況、作成、交付、供覧、保管、貸出、回収、返却、廃棄等の状況を記録するものとする。

3 乙は、第1項の帳簿の内容が改ざんされないよう措置した上で、装備政策部長が別に定める期間、同項の帳簿を保存しなければならない。保存期間の経過後の当該帳簿の廃棄に当たっては、あらかじめ甲の確認を受けるものとする。

（取扱いの記録）

第43条 乙は、特定資料等の閲覧その他関係社員及び下請負事業者関係社員（乙の秘密保全施設等において関係社員と協力して乙のために特定資料等の取扱いの業務を行う下請負事業者関係社員がある場合に限る。次項において同じ。）による特定資料等の取扱いの経過について、装備政策部長が別に定めるところにより、閲覧・貸出記録簿その他の帳簿に登録しなければならない。

2 前項の帳簿は、秘密の種類ごとに（必要な場合は、これに加え、機密、極秘及び秘の区分ごとに）整備するものとし、特定資料等を取り扱った関係社員及び下請負事業者関係社員の氏名、日時、その他秘密の管理職員が指示した事項を記録するものとする。

3 乙は、第1項の帳簿の内容が改ざんされないよう措置した上で、装備政策部長が別に定める期間、同項の帳簿を保存しなければならない。保存期間の経過後の当該帳簿の廃棄に当たっては、あらかじめ甲の確認を受けるものとする。

第4節 特定秘密の周知

（特定秘密を取り扱う従業者への周知）

第44条 乙は、特定秘密である特定資料若しくは特定物件の交付を受け、特定秘密の伝達を受け、又は特定秘密を保有したときは、これらを取り扱う従業者にその旨を周知しなければならない。

第5節 作成

（作成）

第45条 乙は、特定資料又は特定物件を作成（複製及び製作を含む。以下同じ。）しようとする場合には、あらかじめ、秘密の管理職員の許可を得なければならない。ただし、秘密取扱原因契約に特定資料又は特定物件の作成に係る定めのあるときは、当該定めに従うものとする。

2 前項の規定により特定資料又は特定物件を作成する場合には、乙は、これらを作成する方法の細部について、秘密の管理職員と協議し、秘密の管理職員又はその指名する者の立会いの下に行わなければならない。

3 乙は、特定資料又は特定物件を作成したときは、速やかにその旨を秘密の管理職員に書面又は電磁的記録により報告し、必要な指示を受けるものとする。

4 乙は、特定資料又は特定物件の作成に際して完成に至らなかったものがあるときは、秘密の管理職員の指示に従い、これを秘密の管理職員に引き渡し、又は秘密を探知することができないよう、焼却、粉碎、細断、溶解、破壊等の復元不可能な方法により、確実に廃棄しなければならない。

第6節 表示等

（特別防衛秘密の表示等）

第46条 乙は、特別防衛秘密である特定資料又は特定物件を作成したときは、これらに特別防衛秘密、秘密区分、米国政府、登録番号、一連番号、枚数及び指定条件の表示を付さなければならない。この場合において、特定資料（物件を除く。）を作成したときは、文書又は図画の各頁の中央に当該文書又は図面に固有の数字又は組織名等の表示を付すものとする。

2 前項後段の規定にかかわらず、秘密の管理職員から別に指示のあるときは、当該指示に従った表示をしなければならない。

（特定秘密の表示等）

第47条 乙は、特定秘密を保有し、自ら特定秘密である特定資料又は特定物件を作成し、又は特定秘密の伝達を受けたときは、当該特定秘密、特定資料又は特定物件について特秘法第3条第2項各号のいずれかに掲げる措置を講じなければならない。

2 前項の規定に従い特秘法第3条第2項第1号に掲げる措置を講ずる場合においては、乙は、特定秘密その他装備政策部長が別に定める表示を付すものとする。

3 前項の場合において、秘密の管理職員から別に指示のあるときは、当該指示に従った表示をしなければならない。

(特定秘密の指定の有効期間の満了に伴う措置)

第48条 乙は、秘密の管理職員から特定秘密の保護に関する法律施行令（平成26年政令第336号。以下「特秘令」という。）第7条第1項第2号の規定に基づく特定秘密の指定の有効期間が満了した旨の通知を受けたときは、当該指定に係る特定資料又は特定物件であったものについて、特定秘密の表示に赤色の二重線を付すことその他これに準ずる方法によりこれを抹消した上で、特秘令第7条第2項に規定する指定有効期間満了表示をしなければならない。

- 2 前項の場合において、乙は、特秘法第3条第2項第2号に掲げる措置を受けた者に対し、当該指定の有効期間が満了した旨を記載した書面の交付（当該書面の作成に代えて電磁的記録の作成がされている場合にあっては、当該電磁的記録の電子情報処理組織（当該交付をすべき者の使用に係る電子計算機（入出力装置を含む。この項において同じ。）と当該交付を受けるべき者の使用に係る電子計算機とを電気通信回線で接続した電子情報処理組織をいう。）を使用する方法による提供をいう。以下次条及び第50条において同じ。）により通知しなければならない。
- 3 第1項の場合において、乙は、当該指定の有効期間が満了した旨を当該指定に係る情報を取り扱う従業者（当該指定の有効期間の満了について前項の通知を受けた者を除く。）に周知しなければならない。
- 4 前2項、次条及び第50条の通知又は周知（以下この項において「通知等」という。）を書面に代えて電磁的記録で行う場合には、電子メールの開封確認機能を利用し通知等の相手方の電子メール開封を確認すること、通知等の相手方に通知等の内容を確認した旨の折り返しの連絡を求めることその他の通知等の相手方が通知等の内容を実に確認し、これに基づき適格な保護措置が講じられることを担保するための措置を講ずるものとする。

(特定秘密の指定の有効期間の延長に伴う措置)

第49条 乙は、秘密の管理職員から特秘令第8条第1号の規定に基づく特定秘密の指定の有効期間を延長した旨の通知を受けたときは、特秘法第3条第2項第2号に掲げる措置を受けた者に対し、当該指定の有効期間が延長された旨及び延長後の当該指定の有効期間が満了する年月日を書面の交付により通知しなければならない。

- 2 前項の場合において、乙は、当該指定の有効期間が延長された旨及び延長後の当該指定の有効期間が満了する年月日を当該指定に係る情報を取り扱う従業者（当該指定の有効期間の延長について前項の通知を受けた者を除く。）に周知しなければならない。

(特定秘密の指定の解除に伴う措置)

第50条 乙は、秘密の管理職員から特秘令第10条第1項第2号の規定に基づく特定秘密の指定が解除された旨の通知を受けたときは、当該指定に係る特定資料又は特定物件であったものについて、特定秘密の表示に赤色の二重線を付すことその他これに準ずる方法によりこれを抹消した上で、特秘令第10条第2項に規定する指定解除表示をしなければならない。

2 前項の場合において、乙は、特秘法第3条第2項第2号に掲げる措置を受けた者に対し、当該指定が解除された旨及びその年月日を書面の交付により通知しなければならない。

3 第1項の場合において、乙は、当該指定が解除された旨及びその年月日を当該指定に係る情報を取り扱う従業者（当該指定の解除について前項の通知を受けた者を除く。）に周知しなければならない。

(装備品等秘密の表示等)

第51条 乙は、装備品等秘密である特定資料又は特定物件を作成し、秘密の管理職員からの指示があったときは、これらに装備品等秘密、登録番号その他装備政策部長が別に定める表示を付さなければならない。ただし、秘密の管理職員又はその指定する者の許可を受けたときは、この限りでない。

第7節 運搬、交付、伝達等

(運搬等)

第52条 乙は、特定資料又は特定物件を運搬するときは、当該特定資料又は秘密物件を取り扱うことができる関係社員の中から指名した従業者に携行させなければならない。この場合において、特定資料又は特定物件が特別防衛秘密又は特定秘密であるときは、複数名の関係社員で運搬しなければならない。

2 乙は、特定資料又は特定物件を封筒若しくは包装によりこん包して運搬し、又は輸送し、若しくは郵送するとき（書留による郵送に限る。以下同じ。）は、これらが窃取され、破壊され、又は盗み見られるなどの危険を防止するため、こん包を二重にした上で、これらを封かんしなければならない。

3 乙は、前項の規定によることのできない特定資料又は特定物件を運搬し、又は輸送し、若しくは郵送するときは、これらが窃取され、破壊され、盗み見られるなどの危険を防止するため、これらを運搬容器に収納し、施錠するなどの措置を講じなければならない。

- 4 乙は、前3項の規定により運搬することができないとき又は運搬することが不適当であるときの運搬の方法については、秘密の管理職員の指示に従うものとする。
- 5 特別防衛秘密又は特定秘密である特定資料及び特定物件は、郵送してはならない。

(交付)

第53条 乙は、特定資料又は特定物件を交付するときは、名宛人又はその指名する者（当該特定資料又は特定物件を取り扱うことができる者に限る。）に対して行わなければならない。この場合において、交付をしたときは、受領書等に名宛人又はその指名する者の受領印の押印を受けるなど、受領の記録を残すものとする。

(電気通信による特定秘密の交付)

第54条 乙は、特定秘密に該当する特定資料（物件を除く。）を電気通信の方法により交付するときは、暗号措置その他の秘密の管理職員が必要と認める措置を講じなければならない。ただし、特に認められた場合を除き、インターネットを介した電子メール又はストレージサービスを利用しての交付をしてはならない。

(接受)

第55条 乙は、封かんされている特定資料又は特定物件については、名宛人又はその指名する関係社員（当該特定資料又は特定物件を取り扱うことができる者に限る。）でなければ開封させてはならない。

(特定秘密の伝達)

第56条 乙は、特定秘密を伝達するときは、その旨を明らかにするとともに、当該特定秘密の内容を筆記することを差し控えるよう伝えるなど、その保護につき注意を促すための必要な措置を講ずるものとする。

- 2 乙は、特定秘密の伝達を電話で行ってはならない。
- 3 乙は、特定秘密を伝達するときは、盗聴等を防止するものとする。

(下請負事業者への交付又は伝達)

第57条 この節の規定の適用に当たり、特定資料等の交付又は伝達の相手方が下請負事業者である場合には、乙は、あらかじめ、秘密の管理職員の承認を得なければならない。

- 2 前項に規定する場合であつて、交付する特定資料又は特定物件を一定の期限又は条件を満たしたときに返却させる必要があるときは、乙は、秘密の管理職員の指示を受け、当該特定資料又は特定物件の返却の時期を明示した上で交付するものとする。
- 3 第1項の承認を得た場合において、乙の秘密保全施設等において関係社員と協力して乙のために特定資料等の取扱いの業務を行う下請負事業者関係社員があるときの当該下請負事業者関係社員に対する特定資料等の伝達については、関係社員に対する特定資料等の伝達とみなすものとする。

第8節 保護措置に関する報告

(実施報告)

- 第58条 乙は、特定資料又は特定物件を接受し、作成し、送達し又は秘密の管理職員からの指示により廃棄したときは、速やかに、秘密の管理職員に対し、その旨を書面又は電磁的記録により報告しなければならない。
- 2 前項に規定する報告は、作成した特定資料若しくは特定物件、又は作成において完成に至らなかった特定資料若しくは特定物件であつて、秘密の管理職員の指示を受けたものの取扱いを含めて行うものとする。

第9節 情報システム

(情報システムの使用)

- 第59条 乙は、秘密を情報システムで取り扱う場合には、付紙第4に定めるところにより、秘密取扱情報システムを使用しなければならない。

第10節 保管

(保管)

- 第60条 乙は、特定資料又は特定物件を保管する場合には、甲の承認を得た保管容器に保管しなければならない。
- 2 特定秘密である情報を記録する可搬型記憶媒体の保管は、前項の規定に従って行うものとする。
 - 3 第1項の規定にかかわらず、その形状等により同項の規定により保管できない特定物件については、保管庫である秘密保全施設の中で、又は甲が適切と認める方法により保管するものとする。

第5章 緊急事態及び事故

(緊急事態に際しての廃棄)

第61条 乙は、特定資料等の奪取その他秘密の漏えいのおそれがある緊急の事態に際し、その漏えいを防止するため他に適当な手段がないと認められる場合には、特定資料等を探知することができないよう、焼却、粉碎、細断、溶解、破壊等の復元不可能な方法により、当該特定資料又は特定物件を廃棄しなければならない。

2 乙は、前項の規定に基づき、特定資料又は特定物件を廃棄する場合には、あらかじめ秘密の管理職員を通じて防衛装備庁長官の承認を得なければならない。ただし、その手段がない場合又はそのいとまがない場合は、廃棄後速やかにその旨を秘密の管理職員を通じて防衛装備庁長官に報告するものとする。

3 前項ただし書に規定する報告は、特定資料等の奪取その他秘密の漏えいのおそれがある緊急の事態の状況、廃棄した特定資料又は特定物件の概要、同項ただし書の規定を適用した理由及び廃棄に当たって用いた方法を書面又は電磁的記録により行うものとする。

(事故への備え)

第62条 乙は、特定資料等の漏えい、紛失、破壊等の事故が発生した場合の対処の責任者、当該責任者で行う対処手順その他事故への対処体制を整えなければならない。

2 乙は、前項の対処体制の有効性を確認するため、定期的に事故の発生に備えた訓練を実施しなければならない。

(事故等の発生時等の措置)

第63条 乙は、特定資料等の漏えい、紛失、破壊等の事故が発生したとき又はこの契約に定める特定資料等の保護措置に抵触するような事態が発生したときは、直ちに、発生した事故又は事態（以下この条及び次条において「事故等」という。）の内容に応じた適切な措置を講ずるとともに、装備政策部長が別に定める要領に基づき、秘密の管理職員及び装備保全管理課長にその時点で把握できた事故等に関する情報を報告しなければならない。

2 乙は、前項に規定する報告をした後、事故等が発生した原因、事故等に関して収集した証拠、秘密の管理職員から指示があった事項を詳細に調査し、その結果を秘密の管理職員に速やかに報告しなければならない。

3 乙は、第1項に規定する報告のほか、秘密の漏えい、紛失、破壊等の事故が発生した可能性又は将来発生する懸念についての情報を把握した場合は、直ちに、甲に報告するものとする。

(教訓の反映)

第64条 乙は、事故等への対処の結果を踏まえて新たに採用した特定資料等の保護措置について、秘密保全規則に反映しなければならない。

第6章 検証・検査・点検

(検証)

第65条 乙は、特定資料等を保全する体制及び特定資料等の保護措置の実施の状況について、定期的に検証しなければならない。

2 前項の検証に当たっては、次の各号に掲げる事項を考慮したリスク査定（起こり得る脅威を想定した上で、その影響の程度を分析し、及び想定された脅威への対策の妥当性を評価することをいう。次条において同じ。）を実施するものとする。

- (1) 特定資料等の保護に対して起こり得る脅威についての想定
- (2) 特定資料等に対して不正なアクセスを行おうとする者（潜在的に存在するものを含む。）についての想定
- (3) 特定資料等への不正なアクセスとして想定される行為の態様
- (4) 前号の行為が行われた場合の保全体制及び保護措置のぜい弱性の程度
- (5) 特定資料等が不正に開示され又は使用され、改ざんされ、破壊等された場合に生じる被害の程度
- (6) 特定資料等の取扱いの業務に関し、特定資料等の取扱いの業務を行う組織内に存在する脅威（潜在的に存在するものを含む。）の想定
- (7) 特定資料等の取扱いの業務に関し、特定資料等の取扱いの業務を行う組織の外部（乙の組織の内外を問わない。）に存在する脅威（潜在的に存在するものを含む。）の想定

3 乙は、第1項の検証を行った場合において、その保全体制又は保護措置を改善する必要性を認めたときは、検証結果に応じた改善を行わなければならない。

(防衛事業適合事業者による点検)

第66条 乙は、装備政策部長が別に定めるところにより、毎月1回以上、特定資料等の保護措置の実施の状況についての点検を行い、管轄防衛局等にその結果を報告しなければならない。

2 乙は、装備政策部長が別に定めるところにより、1年に1回以上、保全組織の体制その他の秘密保全体制についての点検を行い、リスクを査定し、管轄防衛局等にその結果を報告しなければならない。

(甲による実地検査・調査)

第67条 乙は、前条各項の規定による点検の結果の報告に基づいて、甲又はその指定した者が行う実地の検査を受けなければならない。

2 甲又はその指定した者は、前項に規定する実地の検査の結果を踏まえ、乙による特定資料等の保護措置の実施の状況について更に検査する必要があると認めたときは、乙の秘密保全の体制及び特定資料等の保護措置の実施の状況を調査し、及び必要な指導を行うことができる。

3 乙は、前2項の規定により甲又はその指定した者が行う検査又は調査に協力しなければならない。

4 秘密取扱原因契約の履行に当たり、秘密の管理職員が必要と判断して行う検査又は調査は、第1項及び第2項に基づき行う検査又は調査として行うことができるものとする。この場合において「甲」とあるのは「秘密の管理職員」と読み替えるものとする。

第7章 下請負

(下請負の禁止)

第68条 特定資料等の取扱いに係る業務は、原則として、下請負をしてはならない。

2 前項の規定は、特定資料又は特定物件の輸送、秘密保全施設等の警備その他の役務の提供であつて、当該役務を提供する者が当該役務の提供を通じて、秘密を直接取り扱うことがなく、秘密の内容を知ることができないよう措置されている業務については、適用しない。

3 第8条第3項の規定により秘密保全施設を備えない限定的な防衛事業適合事業者となった事業者については、下請負を認めない。ただし、秘密取扱原因契約の履行のため、装備政策部長が別に定めるところにより、乙の下請負事業者が付紙第2に示す当該下請負事業者の秘密保全施設等又は防衛省の施設において特定資料等を取り扱う場合は、この限りでない。

(下請負の手続)

第69条 前条の規定にかかわらず、乙は、やむを得ず下請負を行う必要があると認めた場合には、秘密取扱原因契約に定めるところにより、秘密取扱原因契約の秘密の管理職員の許可を得なければならない。この場合において、乙の秘密保全施設等において関係社員と協力して乙のために特定資料等の取扱いの業務を行う下請負事業者関係社員があるときは、その旨を明らかにして許可を得るものとする。

- 2 前項の許可を得た場合において、乙の秘密保全施設等において関係社員と協力して乙のために特定資料等の取扱いの業務を行う下請負事業者関係社員があるときは、乙は、同項の許可に係る下請負事業者との間で、当該下請負事業者関係社員による乙の秘密保全施設等における特定資料等の取扱いの業務の管理について協議し、その結果を甲に届け出なければならない。当該協議は、当該下請負事業者関係社員が乙の秘密保全施設等において行う特定資料等の取扱いの業務の内容及び態様に応じたものとしなければならない。

(秘密の管理職員による下請負事業者に対する検査への協力)

第70条 乙は、秘密の管理職員又はその指定した者が、乙の下請負事業者に対し、乙が下請負をした特定資料等の取扱いに係る業務についての検査又は調査を行うときは、秘密の管理職員又はその指定した者の求めに応じ、必要な協力をしなければならない。

第8章 雑則

(契約期間)

第71条 この契約の契約期間は、契約を締結した日から5年間とする。

(契約の延長)

第72条 乙は、この契約の延長を希望する場合には、この契約の残余の期間が6か月となる日から3か月となる日までに、取り扱う秘密の区分に応じて装備政策部長が別に定める要件を満たしていることを証する書類と共に、契約の延長を申請するものとする。

(甲による契約の解除等)

第73条 甲は、乙がこの契約に基づく保護の対象となる秘密を現に取り扱っておらず、当分の間この契約に基づく保護の対象となる秘密を取り扱うことが想定されない場合には、この契約を解除するため、乙と協議することができる。

- 2 甲は、乙がこの契約の規定に違反したときは、この契約の全部又は一部を催告することなく解除することができる。この場合において、甲は、乙及び乙の下請負事業者に対して損害賠償の責を負わないものとする。

(乙による契約の解除)

第74条 乙は、この契約に基づく保護の対象となる秘密を現に取り扱っておらず、当分の間この契約に基づく保護の対象となる秘密を取り扱うことが想

定されない場合には、この契約を解除するため、甲と協議することができる。

(契約の変更)

第75条 甲及び乙は、この契約が満了するまでの間において、この契約に定める内容を変更する必要があると認めた場合は、当該変更について協議するものとする。

(事情の変更)

第76条 甲及び乙は、この契約の締結後、天災地変、法令の制定又は改廃、その他の著しい事情の変更により、この契約に定める内容が不当となり、当該内容を変更する必要があると認めた場合は、当該変更について協議するものとする。

(契約終了後の適用)

第77条 この契約に基づいて乙が現に取り扱った特定資料等に係る秘密を保護する義務は、この契約の終了後も当該特定資料等に係る秘密の指定が解除されるまでの間、継続する。

2 乙は、この契約の終了後においても、秘密保全上調査をする必要があると秘密の管理職員が認めた場合には、第67条又は第70条の規定に準じてこれらの者が行う調査を受け入れ、必要な協力をしなければならない。

(協議)

第78条 甲及び乙は、この契約に関し紛争又は疑義が生じた場合は、その都度協議して解決するものとする。

(裁判管轄)

第79条 この契約は、日本国内法に準拠する。

2 この契約に関する訴えは、東京地方裁判所の管轄に属するものとする。

上記契約の締結を証するため、契約書2通を作成し、双方記名押印の上、各1通を保有するものとする。

令和 年 月 日

甲 防衛装備庁装備政策部
装備保全管理課長 [氏名] 印

乙 [住所]
[事業者名]
[役職名] [氏名] 印

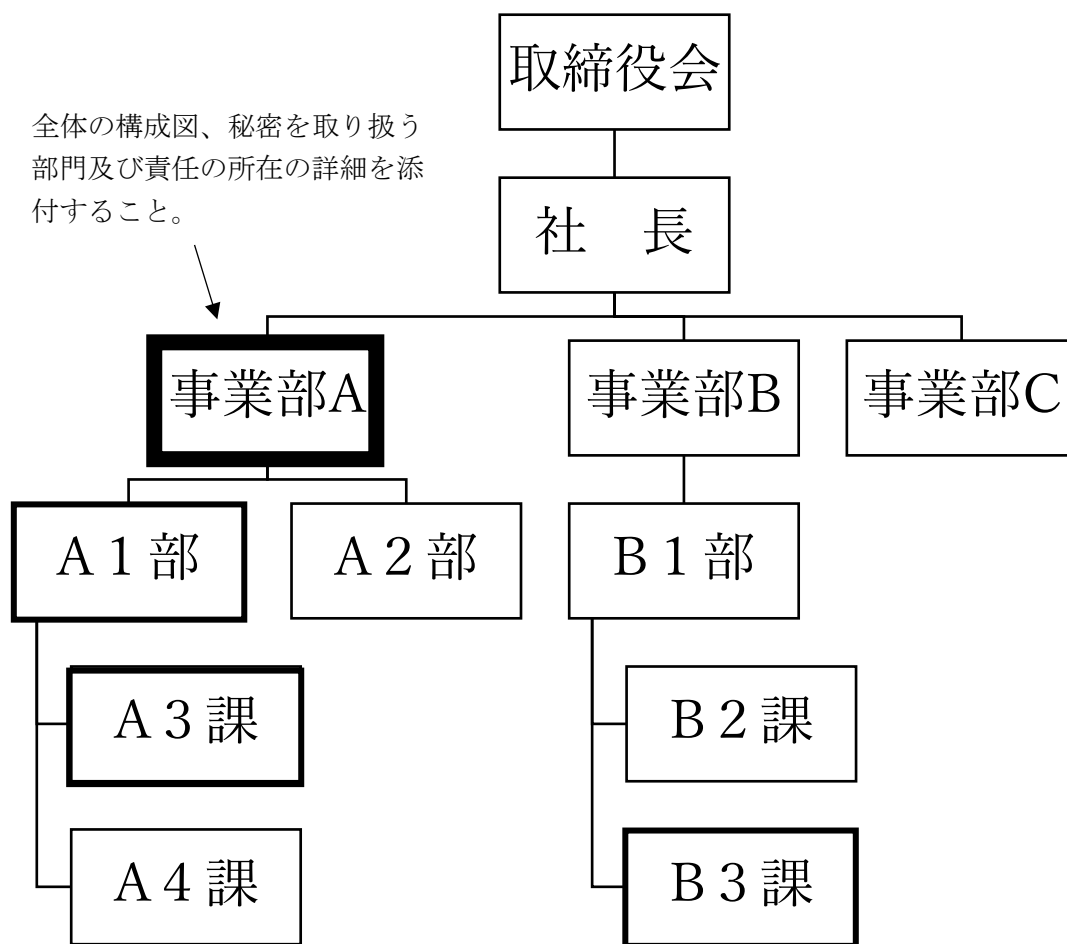
特定資料等を取り扱うことのできる乙の組織の範囲について（記載例 1）

1. 関係部署

- （例 1） ○○事業本部○○部
○○事業本部××支社
○○事業本部◇◇製作所
（例 2） ◇◇製作所□□工場

2. 社内における関係部署の位置付け（組織図※の添付）

（複数の事業部間で関係部署が混合している場合）



※ 事業者全体の組織構成図及び秘密を取り扱う部門の詳細な組織構成図を添付すること。また、複数の部門又は工場において、関係部署が混合している場合には、該当する部署及び責任の所在を特定すること。

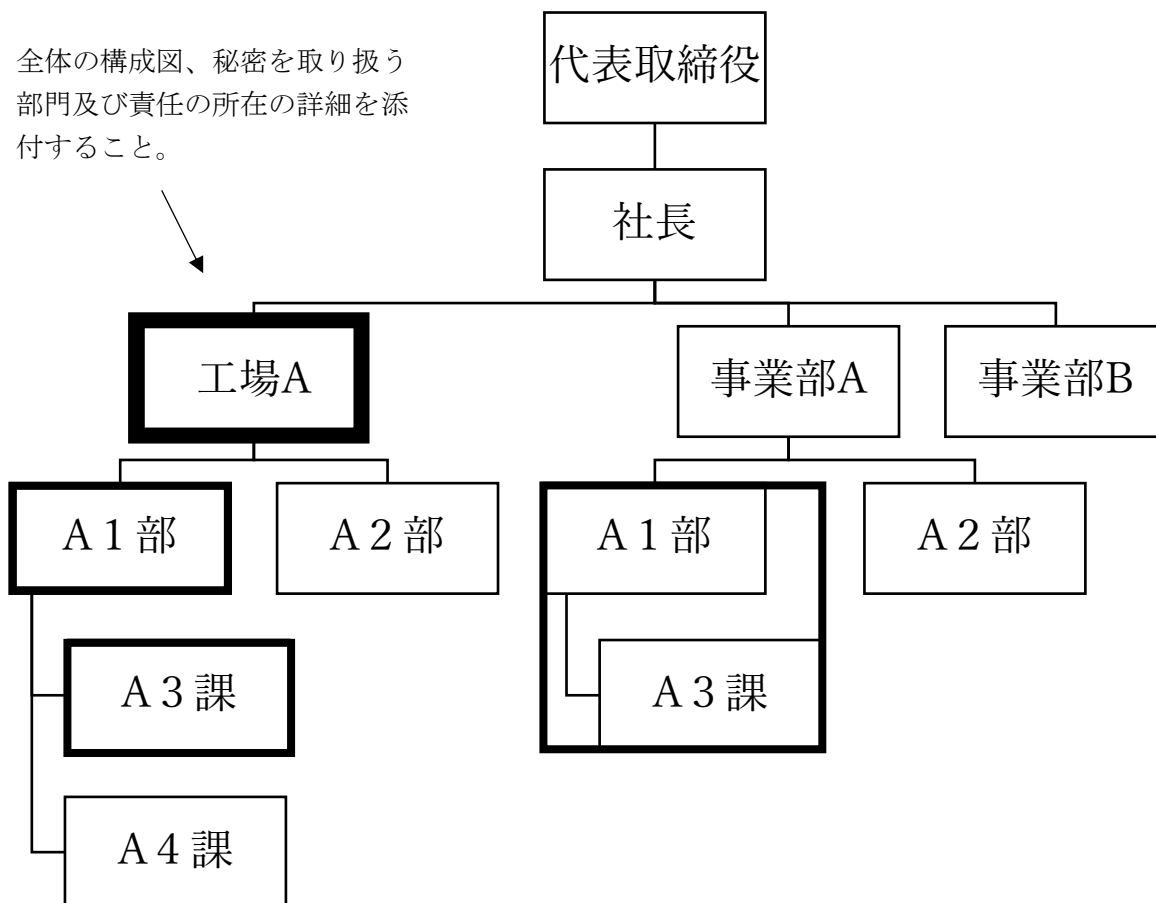
特定資料等を取り扱うことのできる乙の組織の範囲について（記載例 2）

1. 関係部署

- （例 1） ○○事業本部○○部
○○事業本部××支社
○○事業本部◇◇製作所
（例 2） ◇◇製作所□□工場

2. 社内における関係部署の位置付け（組織図※の添付）

（複数の事業部又は工場間で関係部署が混合している場合）



※ 事業者全体の組織構成図及び秘密を取り扱う部門の詳細な組織構成図を添付すること。また、複数の部門又は工場において、関係部署が混合している場合には、該当する部署及び責任の所在を特定すること。

秘密保全施設及び秘密取扱情報システム一覧

項目	詳細	
秘密保全施設	＜乙の全ての秘密保全施設を記載する。＞	
	他の事業者の秘密保全施設等の利用の有無	有・無
	乙の秘密保全施設がない場合の下請負事業者の秘密保全施設等	＜下請負事業者の該当する秘密保全施設等を記載する。＞
秘密取扱情報システム	＜乙の全ての秘密取扱情報システムを記載する。＞	
	他の事業者の秘密取扱情報システムの利用の有無	有・無

適性評価に関する特約条項

(候補者名簿の提出等)

- 第1条 乙は、その従業者に特定秘密を取り扱わせるため防衛装備庁長官による適性評価を実施する必要があると認めるときは、その者の氏名、生年月日、所属する部署、役職名及び法第12条第1項各号のうち該当する号その他参考となる事項を記載し、又は記録した名簿を作成し、これを特定秘密管理者に提出しなければならない。
- 2 乙は、前項の名簿に記載し、又は記録した事項に変更があるときは、速やかに特定秘密管理者に通知しなければならない。
- 3 乙は、適性評価の結果適性があると認められた従業者であって、特定秘密を取り扱わせる場合は、関係社員名簿に掲載し、これを特定秘密管理者及び甲に提出しなければならない。

(適性評価の実施に関する協力)

- 第2条 乙は、評価対象者について照会があった場合に必要な報告を行うこと、評価対象者及びその上司等に対する面接等の実施に便宜を図ることなど、防衛装備庁長官が実施する適性評価に必要な協力を行わなければならない。

(適性評価結果等通知書その他の文書の管理)

- 第3条 乙は、適性評価の結果が記された文書その他適性評価の実施に当たり特定秘密管理者に送付し、又は特定秘密管理者から送付された文書の管理を、次の各号に定めるところにより行わなければならない。
- (1) 漏えい又は滅失の防止その他安全管理のための措置を厳格に行うこと。
- (2) 用済後速やかに廃棄し、適性評価の結果適性があると認められた旨特定秘密管理者が通知した文書は送付日から5年、その他の文書は送付日から1年を超えて保存しないこと。

(評価結果その他の個人情報の目的外利用の禁止)

- 第4条 乙は、評価対象者が適性評価の実施に同意をしなかった事実、適性評価の結果適性がないと認められた事実その他適性評価に関し特定秘密管理者から通知される個人情報を、法令に基づく場合を除き、特定秘密の保護以外の目的のために利用し、又は第三者に提供してはならない。

(特定秘密の取扱業務の停止)

第5条 乙は、適性評価の結果適性があると認められた従業者であって、現に特定秘密を取り扱っている者又は新たに特定秘密を取り扱わせようとしている者について、特定秘密管理者から、新たな適性評価の結果として、適性がないと認められた旨通知があったときは、直ちに、当該従業者が特定秘密を取り扱わないよう措置しなければならない。特定秘密管理者から、法第12条第1項第3号の規定に該当するため、適性に疑義がある旨通知されたときも同様とする。

(事後の事情の変化に関する報告)

第6条 乙は、過去5年以内に適性評価の結果適性があると認められた従業者であって、現に特定秘密を取り扱っている者又は新たに特定秘密を取り扱わせようとしている者について、教育等を通じて「特定秘密の保護に関する誓約書」に基づく申出を徹底させるとともに、面談等の機会を活用し、次に掲げる事情が職務の内外を問わず生じていないかどうかの確認を年1回以上行い、状況の変化の継続的な把握に努めなければならない。

- (1) 外国籍の者と結婚した場合その他外国との関係に大きな変化があったこと。
- (2) 罪を犯して検挙されたこと。
- (3) 懲戒処分の対象となる行為をしたこと。
- (4) 情報の取扱いに関する規則に違反したこと。
- (5) 違法な薬物の所持、使用等薬物の違法又は不適切な取扱いを行ったこと。
- (6) 自己の行為の是非を判別し、若しくはその判別に従って行動する能力を失わせ、又は著しく低下させる症状を呈していると疑われる状況に陥ったこと。
- (7) 飲酒により、けんか等の対人トラブルを引き起こしたり、業務上の支障を生じさせたりしたこと。
- (8) 裁判所から給与の差押命令が送達されるなど経済的な問題を抱えていると疑われる状況に陥ったこと。
- (9) 上記のほか、特定秘密を漏らすおそれがないと認めることについて疑義が生じたこと。

2 乙は、前項各号に掲げる事情があると認めた場合には、速やかに特定秘密管理者に報告しなければならない。

(従業者が派遣労働者である場合の措置)

第7条 乙は、乙の指揮命令の下に労働する派遣労働者（労働者派遣事業の適正な運用の確保及び派遣労働者の保護等に関する法律（昭和60年法律第88号）第2条第2号に規定する派遣労働者をいう。）である従業者について、第1条の名簿に登載する場合には、同条に定める事項のほか、次に掲げる事項を当該名簿に記載し、又は記録するとともに、当該従業者を雇用する事業主に対し、当該名簿に登載した旨を通知しなければならない。

(1) 派遣労働者である旨

(2) 当該従業者についての予定している業務内容

2 乙は、乙の指揮命令の下に労働する派遣労働者である従業者について、特定秘密管理者から次に掲げる事項を通知された場合には、当該通知の内容を書面により、当該従業者を雇用する事業主に通知しなければならない。

(1) 適性評価実施責任者に提出する名簿に登載しないこと。

(2) 適性評価を実施することについて防衛装備庁長官の承認が得られたこと、又は得られなかったこと。

(3) 当該従業者が適性評価の実施についての同意をしなかったことにより適性評価が実施されなかったこと。

(4) 当該従業者が同意を取り下げたことにより適性評価の手続が中止されたこと。

(5) 適性評価の結果。

(6) 当該従業者が法第12条第1項第3号の規定に該当するため、適性に疑義があること。

3 乙は、過去5年以内に適性評価の結果適性があると認められた従業者であって、現に特定秘密を取り扱っている者又は新たに特定秘密を取り扱わせようとしている者が乙の指揮命令の下に労働する派遣労働者である場合には、当該従業者を雇用する事業主が当該従業者について第6条の事情があると認めたときに、乙に確実に報告をさせる必要な措置を講じなければならない。

4 乙は、乙の指揮命令の下に労働する派遣労働者を雇用する事業主に対し、第1項又は第2項の通知をしたときは、当該通知をした文書について、これが第3条の規定に準じて適切に管理されるよう、必要な措置を講じなければならない。

5 乙は、評価対象者が派遣労働者である従業者の場合には、当該従業者を雇用する事業主に対し、当該従業者が適性評価の実施に同意をしなかった事実、適性評価の結果適性がないと認められた事実その他適性評価に関し乙を経由して特定秘密管理者から通知される個人情報を、法令に基づく場合を除

き、特定秘密の保護以外の目的のために利用し、又は第三者に提供しないよう必要な措置を講じなければならない。

(契約履行後における乙の義務)

第8条 第3条、第4条並びに前条第4項及び第5項の規定は、契約履行後においても準用する。

秘密取扱情報システムに関する特約条項

(適用範囲)

第 1 条 秘密を情報システムで取り扱う場合には、この特約の定めを適用する。

2 この特約の定めに基づいて執られる措置は、主たる契約条項の定めに基づいて執られる措置と整合的に行われなければならない。

(定義)

第 2 条 この特約において次の各号に掲げる用語の意義は、それぞれ当該各号に定めるとおりとする。

- (1) ユーザーセッション 秘密取扱情報システム利用者が実行するそれぞれのアプリケーションの論理的な経路をいう。
- (2) ホワイトリスト 秘密取扱情報システムにインストールし、及び実行することが認められたソフトウェアのリストをいう。
- (3) 構成設定 秘密取扱情報システムの構成要素（情報システムを構成するハードウェア、ソフトウェア、ネットワーク及び記憶媒体をいう。以下同じ。）の種類、バージョン等及び当該構成要素の機能の決定並びに構成要素の動作等を制御する設定値を決定することをいう。
- (4) サプライチェーン・リスク 秘密取扱情報システムに関する調達に際し、秘密取扱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。
- (5) 電子政府推奨暗号等 電子政府推奨暗号リストに記載されている暗号等又は電子政府推奨暗号選定の際の評価方法により評価した場合に電子政府推奨暗号と同等以上の解読困難な強度を有する秘匿化の手段をいう。

(組織のセキュリティ)

第 3 条 乙は、秘密を秘密取扱情報システムで取り扱うための体制を整備し、これを維持しなければならない。

2 乙は、秘密取扱情報システム利用者以外の者に秘密取扱情報システムを利用させてはならない。

3 主たる契約条項の定め及びこの特約の定めに基づいて秘密取扱情報システムに関して執られる措置については、秘密取扱情報システムを利用した秘密

の取扱いのため必要な範囲において、関係社員その他の従業者に徹底するものとする。この場合において、秘密取扱情報システムに関する情報の供覧の範囲を必要最小限の範囲にとどめ、秘密取扱情報システムの管理及び運用に関する文書を適切に保護しなければならない。

- 4 乙は、その秘密保全施設等において関係社員と協力して乙のために特定資料等の取扱いの業務を行う下請負事業者関係社員に対し、秘密取扱情報システムの利用を認めることができる。この場合においては、主たる契約条項の定めに従って行う下請負事業者との間の協議に下請負事業者関係社員による秘密取扱情報システムの利用に関することを含めなければならない。
- 5 前項の場合における第3項の規定の適用については、「関係社員その他の従業者」とあるのは、「関係社員その他の従業者及び乙の秘密保全施設等において関係社員と協力して乙のために特定資料等の取扱いの業務を行う下請負事業者関係社員」とする。

(体制)

- 第4条 乙は、秘密取扱情報システムごとに秘密取扱情報システム利用者を指定しなければならない。秘密取扱情報システム利用者は、関係社員の中から、乙が当該秘密取扱情報システムを用いて特定資料等の取扱いの業務を行う上で必要最小限の範囲で指定するものとする。
- 2 乙は、秘密取扱情報システムごとに秘密取扱情報システム管理者（秘密取扱情報システムの運用管理に責任を負う管理者をいう。以下同じ。）を指定しなければならない。秘密取扱情報システム管理者は、当該秘密取扱情報システムの秘密取扱情報システム利用者の中から、ふさわしいと認める者を指定するものとする。
 - 3 乙は、秘密取扱情報システムごとに秘密取扱情報システム担当者（秘密取扱情報システム管理者の業務遂行を補助する者をいう。以下同じ。）を指定しなければならない。秘密取扱情報システム担当者は、当該秘密取扱情報システムの秘密取扱情報システム利用者の中から、ふさわしいと認める者を指定するものとする。
 - 4 乙は、秘密取扱情報システムごとにアカウント管理者（秘密取扱情報システムへ論理的にアクセスするための権利の設定、変更、削除等の管理を行う者をいう。以下同じ。）を指定しなければならない。アカウント管理者は、秘密取扱情報システムの秘密取扱情報システム担当者の中から、ふさわしいと認める者を指定するものとする。

- 5 秘密取扱情報システム管理者は、秘密取扱情報システムの適正な管理に影響がないと判断される場合には、秘密取扱情報システム担当者及びアカウント管理者を兼ねることができる。
- 6 秘密取扱情報システム担当者は、秘密取扱情報システムの適正な管理に影響がないと判断される場合には、アカウント管理者を兼ねることができる。
- 7 前条第4項の場合における第1項の規定の適用については、「関係社員」とあるのは、「関係社員及び乙の秘密保全施設等において関係社員と協力して乙のために特定資料等の取扱いの業務を行う下請負事業者関係社員」とする。この場合において、第2項から第4項までの規定にかかわらず、下請負事業者関係社員である秘密取扱情報システム利用者を秘密取扱情報システム管理者、秘密取扱情報システム担当者又はアカウント管理者に指定してはならない。
- 8 前各項の規定による指定（新たな指定により元々の指定を解除する場合を含む。）は、装備政策部長が別に定めるところにより行うものとする。

（同意書）

- 第5条 乙は、秘密取扱情報システム利用者を指定した場合には、秘密取扱情報システムの利用は監視され、利用履歴が記録されること等について、当該秘密取扱情報システム利用者の同意を得なければならない。
- 2 前項の同意は、装備政策部長が別に定めるところにより行うものとする。

（総括者）

- 第6条 乙は、総括者に、次の各号に掲げる事項その他秘密取扱情報システムにおける特定資料及び秘密取扱情報システムに係る特定物件の取扱いに関して必要な措置を講じさせなければならない。
- (1) 秘密取扱情報システムの管理及び運用が秘密保全規則等の下で的確に行われることを確保すること。
 - (2) 秘密取扱情報システムを管理し、及び運用する組織のセキュリティを整備すること。
 - (3) 秘密取扱情報システム利用者に対する教育を行うこと。
 - (4) 秘密取扱情報システム及び可搬記憶媒体の廃棄を承認し、その実施を監督すること。
 - (5) 事故への対処体制を整備し、及び事故等に対応し、並びにぜい弱性への対処を監督すること。
 - (6) リスク査定を監督すること。
 - (7) 点検の実施要領を承認し、及び点検の実施を監督すること。

- (8) 秘密取扱情報システムセキュリティ実装計画（SSP）を承認し、その実施を監督すること。

（秘密取扱情報システム管理者）

第7条 乙は、秘密取扱情報システム管理者に、次の各号に掲げる事項その他秘密取扱情報システムの管理のために必要な措置を講じさせなければならない。

- (1) 電磁的記録である秘密（以下「秘密のデータ」という。）を分類し、及び管理すること。
- (2) 物理的セキュリティ対策の実施を監督すること。
- (3) 可搬記憶媒体を管理すること。
- (4) 秘密取扱情報システム及び可搬記憶媒体の廃棄を申請し、及びこれらを廃棄すること。
- (5) ぜい弱性対処記録及びぜい弱性スキャン分析結果記録簿を承認し、並びにぜい弱性に対処すること。
- (6) リスク査定を実施すること。
- (7) 点検の実施要領を作成し、及び点検を実施すること。
- (8) 秘密取扱情報システムセキュリティ実装計画（SSP）を作成し、これにのっとりた措置を執ること。
- (9) セキュリティエンジニアリングの原則を承認すること。
- (10) 構成設定を監督し、証明するための目録を承認し、及び構成管理の実施を監督すること。
- (11) 基本的な防御対策の実施を監督すること。
- (12) アクセス制御方針を承認し、その実施を監督すること。
- (13) アカウント管理計画（秘密取扱情報システム利用者のアカウントを管理する計画をいう。以下同じ。）を承認し、アカウント（秘密取扱情報システムに論理的にアクセスするための権利をいう。以下同じ。）の管理を監督すること。
- (14) ログオン及びユーザーセッションの管理を監督すること。
- (15) 識別管理簿（アカウント及び秘密取扱情報システムを構成する機器を識別するために付与した識別子を管理するための帳簿をいう。以下同じ。）を承認し、識別及び認証を監督すること。
- (16) 秘密保全施設等における通信の制御を監督すること。
- (17) 運用状況の監視及び対応を監督すること。
- (18) システムログの取得及び分析を監督すること。
- (19) システムログのバックアップ等を監督すること。

- (20) システムメンテナンス等計画を承認し、その実施を監督すること。
- (21) 構成要素に関するサプライチェーン・リスクを管理すること。

(秘密取扱情報システム担当者)

第8条 乙は、秘密取扱情報システム担当者に、次の各号に掲げる事項その他秘密取扱情報システム管理者の業務遂行を補助するために必要な措置を講じさせなければならない。

- (1) 物理的セキュリティ対策を行うこと。
- (2) 可搬記憶媒体を管理する簿冊（以下「可搬記憶媒体管理簿」という。）を作成し、可搬記憶媒体の点検をすること。
- (3) セキュリティエンジニアリングの原則を適用すること。
- (4) 構成設定の状況を把握し、これを証明するための目録を作成し、及び構成管理を行うこと。
- (5) 基本的な防御対策を行うこと。
- (6) アクセス制御方針を作成し、アクセスを制御すること。
- (7) 秘密保全施設等における通信を制御すること。
- (8) 運用状況の監視を行い、及びその結果に対応すること。
- (9) システムログを取得し、及びその分析を行うこと。
- (10) ぜい弱性対処記録及びぜい弱性スキャン分析結果記録簿を作成すること。
- (11) システムログのバックアップ等を行うこと。
- (12) システムメンテナンス等計画を作成し、メンテナンス等を行うこと。
- (13) その他秘密取扱情報システム管理者から命じられたこと。

(アカウント管理者)

第9条 乙は、アカウント管理者に、次の各号に掲げる事項その他秘密取扱情報システムのアカウントの管理のために必要な措置を講じさせなければならない。

- (1) アカウント管理計画を作成し、秘密取扱情報システムのアカウントの管理を行うこと。
- (2) ログオン及びユーザーセッションを管理すること。
- (3) 識別管理簿を作成し、識別及び認証を行うこと。
- (4) その他秘密取扱情報システム管理者から命じられたこと。

(秘密取扱情報システム利用者への教育)

第10条 乙は、秘密取扱情報システム利用者に対し、その職責及び利用する秘密取扱情報システムに応じた技術的及び専門的な教育を行わなければならない。

2 前項の規定の実施に当たっては、主たる契約条項に定める教育と整合的に行うものとする。

(秘密取扱情報システムの設置)

第11条 乙は、秘密取扱情報システムを秘密保全施設等の内部に設置し、秘密取扱情報システムセキュリティ実装計画（SSP）に従って管理し、及び運用しなければならない。

2 秘密取扱情報システムは、有線により構成要素が配線接続されなければならない。他の情報システム又は秘密取扱情報システムが設置された秘密保全施設等の外部との通信は、完全に遮断されなければならない。

3 前項の規定にかかわらず、その構成要素が複数の秘密保全施設等の内部に設置される秘密取扱情報システムであって、秘密保全施設等の間を有線接続されるものとして防衛装備庁が定める基準を満たす秘密取扱情報システムは、複数の秘密保全施設等の構成要素の間で通信を行うことができる。

4 秘密取扱情報システムに接続できる可搬記憶媒体は、当該秘密取扱情報システムが設置された秘密保全施設等から持ち出してはならない。ただし、特定資料等を当該秘密保全施設等の外にある者への交付のため、秘密保全施設等の外部への持出しの許可を得た可搬記憶媒体は、この限りでない。

(秘密取扱情報システムセキュリティ実装計画（SSP）の更新)

第12条 乙は、秘密取扱情報システムセキュリティ実装計画（SSP）を定期的に見直し、その内容を常に最新のものに更新しなければならない。

2 乙は、秘密取扱情報システムセキュリティ実装計画（SSP）を変更した場合には、甲に届け出なければならない。

3 乙は、サプライチェーン・リスクに留意して構成要素を選定するものとする。

4 乙は、甲から秘密取扱情報システムセキュリティ実装計画（SSP）を見直すよう求められたときは、これに応じなければならない。

(秘密のデータの管理)

第13条 乙は、秘密のデータを他の電磁的記録から明確に区別し、秘密保全施設等内で管理しなければならない。

- 2 前項の規定の実施に当たっては、秘密のデータの管理に関する帳簿を作成するものとする。
- 3 秘密のデータは、当該秘密取扱情報システムで使用することが認められた可搬記憶媒体に保存しなければならない。
- 4 秘密のデータは、秘密取扱情報システムの記憶媒体に保存してはならない。
- 5 前2項の規定にかかわらず、その記憶媒体に秘密のデータを保存するものとして防衛装備庁が定める基準を満たす秘密取扱システムは、その記憶媒体に秘密のデータを保存することができる。

(可搬記憶媒体の管理)

第14条 乙は、秘密取扱情報システムで可搬記憶媒体を使用する場合には、次の各号に定める事項その他可搬記憶媒体の管理のために必要な事項を定めなければならない。

- (1) 可搬記憶媒体管理簿を作成すること。
 - (2) 可搬記憶媒体の状況及び可搬記憶媒体管理簿の内容を定期的に点検すること。
 - (3) 可搬記憶媒体を使用できる者を必要最小限に制限すること。
 - (4) 可搬記憶媒体の使用は秘密取扱情報システム管理者が許可すること。
 - (5) 可搬記憶媒体に秘密のデータを記録する場合には、強固な暗号鍵を用い、最新の電子政府推奨暗号等により暗号化し、暗号鍵を厳格に管理すること。
-
- 2 乙は、可搬記憶媒体管理簿に記載されていない可搬記憶媒体の秘密取扱情報システムへの接続を拒否する設定にしなければならない。
 - 3 乙は、可搬記憶媒体を廃棄する場合には、これを秘密のデータが復元できないよう物理的に破壊しなければならない。なお、一の秘密取扱情報システムで使用された可搬記憶媒体を他の情報システムで再利用してはならない。
 - 4 可搬記憶媒体管理簿は、装備政策部長が別に定めるところにより作成するものとする。

(アクセス制御)

第15条 乙は、アカウント管理計画を作成し、これに従って、秘密取扱情報システム利用者の職責に応じた必要最小限の権限を付与し、アカウントの利用を管理しなければならない。付与したアカウントは、定期に及び必要に応じて、見直すものとする。

- 2 乙は、秘密取扱情報システムへのログオン及びユーザーセッションを管理し、秘密取扱情報システムの不正な利用を防止しなければならない。
- 3 アカウント管理計画は、装備政策部長が別に定めるところにより作成するものとする。

(識別及び認証)

- 第16条 乙は、識別管理簿を作成しなければならない。
- 2 乙は、秘密取扱情報システムで用いられる識別子及び認証子を厳格に管理し、多要素認証を含め、秘密取扱情報システムで用いられる認証が厳正に行われるよう措置しなければならない。
 - 3 識別管理簿は、装備政策部長が別に定めるところにより作成するものとする。

(システム監視)

- 第17条 乙は、秘密取扱情報システムに対する不正なアクセス、利用者権限等の不正な使用、不正な通信、悪意のあるコードの侵入等を検知するため、秘密取扱情報システムの運用の状況を監視しなければならない。
- 2 乙は、前項の規定による監視の結果を記録し、組織横断的な対策に取り組むものとする。

(システムログの取得・分析、バックアップ)

- 第18条 乙は、不正な操作又は通信を探知するため、秘密取扱情報システムについて、秘密のデータの取扱いに関する記録、秘密取扱情報システム利用者ごとの操作の記録その他秘密取扱情報システムの操作、入出力、通信等の記録を自動的に取得しなければならない。
- 2 乙は、前項の規定により取得した記録について、定期的に分析しなければならない。分析に当たっては、全体的かつ横断的にシステムログを精査するものとし、反復継続性に乏しい特異な事象、秘密取扱情報システム利用者による異常な操作、システムの異常な挙動等の有無を判断しなければならない。
 - 3 乙は、第1項の規定により取得したシステムログについて、定期的にバックアップし、その機密性、完全性及び可用性を確保しなければならない。
 - 4 乙は、第1項及び第2項の規定によるシステムログの分析の結果を記録しなければならない。

(ぜい弱性スキャン)

第19条 乙は、秘密取扱情報システムについて潜在的に懸念される脅威を探知するため、定期に及び必要に応じて、秘密取扱情報システムのぜい弱性スキャンを行い、その結果を分析しなければならない。

2 前項の分析は、情報システムを巡る脅威に関する最新の動向に係る技術的な知見を踏まえて行うものとする。

3 乙は、前2項の規定によるぜい弱性スキャンの結果を記録し、組織横断的な対策に取り組むものとする。

(ぜい弱性対処)

第20条 乙は、秘密取扱情報システムにぜい弱性が発見され、又は検知された場合の対処の責任者及び当該責任者の下で行う対処手順を整えなければならない。

2 乙は、発見され、又は検知されたぜい弱性を速やかに修正し、又は対策を講じなければならない。

(リスク査定及び点検)

第21条 乙は、秘密取扱情報システムにおける特定資料の取扱い及び秘密取扱情報システムに係る特定物件の取扱いに関するリスク査定を実施しなければならない。

2 乙は、秘密取扱情報システムにおける特定資料の取扱い及び秘密取扱情報システムに係る特定物件の取扱いについて定期的に点検を行わなければならない。

3 前2項の規定によりリスク査定又は点検を行うに当たっては、主たる契約条項に定める措置と整合的に行うものとする。

4 第1項又は第2項の規定によりリスク査定又は点検を行った場合において、改善事項が判明したときは、速やかに措置しなければならない。

(メンテナンス等)

第22条 乙は、定期的にかつ計画的に、秘密取扱情報システムの保守、点検、診断、修理、整備、アップグレードその他の秘密取扱情報システムのメンテナンス等を行わなければならない。

2 前項のメンテナンス等は、原則として、秘密取扱情報システム利用者のうちふさわしい者として指定されたものを行うものとし、秘密の保全のための措置を講じるものとする。

3 乙は、前2項の規定によるメンテナンス等の状況を記録しなければならない。

(秘密取扱情報システムの廃棄)

第23条 乙は、秘密取扱情報システムを廃棄する場合には、秘密のデータが復元できないよう、記憶媒体を物理的に破壊しなければならない。

2 秘密取扱情報システムは、その全部又は一部を他の目的の情報システムとして再利用してはならない。

3 秘密取扱情報システムの廃棄は、総括者が監督するものとする。

4 前2項の規定の実施に当たっては、装備政策部長が別に定めるところにより記録するものとする。

(事故)

第24条 乙は、特定資料等の漏えい、紛失、破壊等の事故が秘密取扱情報システムの利用に伴って発生した場合の対処の責任者、当該責任者の下で行う対処手順その他事故への対処体制を整えなければならない。

2 前項の事故への対処体制を整えるに当たり、乙は、秘密取扱情報システムの特性に応じた証跡を収集するものとする。

3 事故への対処体制を整え、及び事故等に対応するに当たっては、主たる契約条項に定める措置と整合的に行うものとする。

(取扱いの記録)

第25条 乙は、秘密取扱情報システムの取扱いについては、装備政策部長が別に定めるところにより、帳簿に記録しなければならない。この場合において、乙は、当該帳簿の内容が改ざんされないよう措置しなければならない。

2 乙は、前項の帳簿の内容が改ざんされないよう措置した上で、装備政策部長が別に定める期間、同項の帳簿を保管しなければならない。保管期間の経過後の当該帳簿の廃棄に当たっては、あらかじめ甲の確認を受けるものとする。

(その他)

第26条 この特約条項の実施の細部については、別に防衛装備庁装備政策部長が定めるところによるものとする。

別紙第 3

防衛事業適合事業者の秘密の保護に関する特約条項

(乙の一般義務)

第 1 条 乙（契約業者）は、主たる契約条項に基づき乙が取り扱う秘密（防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律（令和 5 年法律第 5 4 号）第 2 7 条第 1 項に規定する装備品等秘密、特定秘密の保護に関する法律（平成 2 5 年法律第 1 0 8 号）第 3 条第 1 項に規定する特定秘密又は日米相互防衛援助協定等に伴う秘密保護法（昭和 2 9 年法律第 1 6 6 号）第 1 条第 3 項に規定する特別防衛秘密をいう。以下同じ。）の保護に関し、この特約条項及び防衛事業適合事業者契約（防衛事業適合事業者制度等に関する訓令（令和 7 年防衛装備庁訓令第 1 9 号）第 1 3 条第 3 項に定める契約をいう。以下同じ。）に定めるところにより、万全を期さなければならない。

2 乙は、その従業者、下請負を行う場合においては下請負事業者の従業者又は乙が防衛事業適合事業者契約に規定する秘密保全施設等への立入りを認めた者（防衛省の職員又は乙若しくは下請負事業者の従業者を除く。）の故意又は過失によりこの契約の履行のために取り扱う秘密が漏えいしたときであっても、その責任を免れることはできない。

(秘密の取扱い)

第 2 条 乙は、防衛事業適合事業者契約の定めるところに従い、この契約の履行のために取り扱う秘密を保護しなければならない。

(違約金の請求)

第 3 条 甲（秘密の管理職員）は、付紙「秘密の保全又は保護の確保に関する違約金条項」の規定に基づき違約金を請求することができる。

(下請負の禁止)

第 4 条 乙は、秘密の取扱いに係る業務（物件の輸送、施設の警備その他役務であって、秘密の内容を知り得ないと認められるものを除く。）を第三者に下請負してはならない。ただし、やむを得ず下請負を行う場合は、あらかじめ、甲に対し、下請負の相手方、契約内容、取り扱わせる秘密を特定する事項、特定資料等（秘密を記録する文書、図画、電磁的記録若しくは物件又は秘密を化体する物件及び製造途上にある仕掛品並びにこれらにより構成される物件をいう。以下同じ。）の保護の手段等を記した書面又は電磁的記録を

添えて、甲の許可を得なければならない。

- 2 前項の規定により下請負を行う場合において、下請負事業者は、防衛事業適合事業者契約又は保全契約（装備品等秘密の保全に関する特約条項（装備品等秘密の指定等に関する訓令（令和6年防衛省訓令第10号）別記第2号様式の特約条項をいう。）、防衛装備庁における特定秘密の保護に関する特約条項（防衛装備庁における特定秘密の保護に関する訓令第36条第1項に規定する審査基準及び第37条第2項に規定する特約条項について（装装制第54号。27. 10. 1）別紙の付紙第2の特約条項をいう。）又は防衛装備庁における特別防衛秘密の保護に関する特約条項（防衛装備庁における特別防衛秘密の保護に関する訓令（平成27年防衛装備庁訓令第25号）別記第6号様式の特約条項をいう。）をいう。以下同じ。）を締結した者であつて、当該防衛事業適合事業者契約又は保全契約に基づき、特定資料等を保有することができ、又は交付を受けることができるもの（以下「秘密取扱事業者」という。）でなければならない。
- 3 乙は、第1項の規定により秘密取扱事業者である下請事業者の下請負を行わせる場合には、当該下請負事業者による特定資料等の適切な取扱いを確保するため、当該下請負事業者の作成する秘密保全規則等、下請負事業者における秘密を取り扱う従業者の名簿その他特定資料等の秘密保全のための措置の実施状況等を確認しなければならない。
- 4 乙は、下請負事業者と下請負の契約を締結し、又は締結した下請負の契約の内容を変更した場合には、当該下請負事業者に対し、当該下請負の契約書の写しを甲に提出するよう指導しなければならない。ただし、乙が当該下請負の契約書の写しを甲に提出した場合はこの限りでない。

（保全契約の解除等）

- 第5条 甲は、乙がこの特約条項の規定に違反した場合には、この契約の全部又は一部を催告することなく解除することができる。この場合において、甲は、乙及び下請負事業者に対して損害賠償の責を負わないものとする。
- 2 甲は、下請負事業者の責に帰すべき事由により当該下請負事業者との防衛事業適合事業者契約又は保全契約を解除した場合には、その旨を乙に通報するものとする。この場合において、甲は、乙に対して損害賠償の責を負わないものとする。
 - 3 乙が下請負先との契約を解除するときは、その旨を甲に事前に通報しなければならない。

秘密の保全又は保護の確保に関する違約金条項

第1条 乙は、秘密（防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律（令和5年法律第54号）第27条第1項に規定する装備品等秘密、特定秘密の保護に関する法律（平成25年法律第108号）第3条第1項に規定する特定秘密又は日米相互防衛援助協定等に伴う秘密保護法（昭和29年法律第166号）第1条第3項に規定する特別防衛秘密をいう。以下同じ。）であって、防衛事業適合事業者の秘密の保護に関する特約条項（防衛事業適合事業者制度等に関する訓令（令和7年防衛装備庁訓令第19号。以下「防衛事業適合事業者訓令」という。）第13条第4項に規定する契約条項をいう。）に基づき乙が保全又は保護すべきものを当該秘密に接する権限のない者に漏えい（以下単に「漏えい」という。）したことを甲が証明した場合は、甲が契約の全部又は一部を解除するか否かにかかわらず、次の各号に掲げる基準に従い、甲が指定する期間内に違約金を支払わなければならない。ただし、乙が、当該秘密の漏えいについて、自己の責に帰すべからざる事由により生じたことを証明したときは、この限りでない。

- (1) 漏えいした秘密の区分に応じて、それぞれ次に掲げる金額
 - ア 「装備品等秘密」のときは、契約金額の100分の5
 - イ 「特定秘密」のときは、契約金額の100分の7.5
 - ウ 「特別防衛秘密」のときは、契約金額の100分の10
- (2) 次のアからウまでの事由に該当する場合には、前号に掲げる金額に、それぞれ当該アからウまでに掲げる金額を加算
 - ア 秘密の漏えいが乙の故意又は重大な過失によると認められるときは、前号に掲げる金額と同額
 - イ 乙が甲に対し、秘密の漏えいの事実を直ちに報告しなかったときは、前号に掲げる金額に100分の50を乗じた金額
 - ウ 乙が甲に対し、秘密の漏えいに関し虚偽の報告をしたときは、前号に掲げる金額に100分の50を乗じた金額
- (3) 乙が、過去10年以内に秘密を漏えい（当該漏えいが本契約に係るものであるか、甲乙間の他の契約に係るものであるかを問わない。）し、甲により第1号のいずれかに該当するものとして違約金を請求されていた場合においては、今回漏えいした秘密の区分に応じて同号に掲げる金額と同額を加算
- (4) 前号に規定する場合における当該過去の秘密の漏えいが第2号に掲げる加算事由のいずれかに該当するとされた場合であって、今回の秘密の漏えい

いが当該加算事由と同一の事由に該当するときは、前号に掲げる金額の加算に加えて、当該加算事由に応じて第2号に掲げる金額と同額を加算

- (5) 秘密の漏えいが、第2号のイ又はウに掲げる事由に該当せず、かつ、乙の極めて軽微な過失によると認められるときは、第1号、第3号及び前号の規定にかかわらず、契約金額の100分の5以内で甲が定める金額
- 2 乙が複数の秘密を一の行為において漏えいした場合は、漏えいした各秘密について算出した違約金の額の最高額をもって違約金の額とする。
- 3 乙が甲との間の複数の契約において保全又は保護すべきものとされている秘密を漏えいした場合において、いずれの契約の履行における漏えいか乙が証明できないときは、当該秘密が漏えいした疑いがある各契約について算出した違約金の額の最高額をもって違約金の額とする。
- 4 乙が違約金を甲の指定する期間内に支払わない場合は、乙は、当該期間を経過した日から支払いをする日までの日数に応じ、当該期間を経過した日における法定利率により計算した額の延納利息を甲に支払わなければならない。

第2条 乙が秘密を保全又は保護する責任がある期間は、乙が甲から秘密を指定した旨の通知を受けたときから、当該秘密の指定にかかる期間（甲が当該期間を延長する旨乙に通知した場合は、当該延長後の期間）が終了するまで、又は甲が秘密の指定を解除するまでとする。ただし、甲が乙に秘密を提供する場合は、当該秘密を乙が受領したときからとする。

- 2 前項に定める乙が秘密を保全又は保護する責任がある期間に乙が秘密を漏えいしたときは、当該期間又は当該期間経過後3年を経過するまでの間、甲は、乙に対して前条の規定に基づく違約金を請求できるものとする。
- 3 本違約金条項が付されている契約が終了し、又は解除された場合であっても、第1項に定める乙が秘密を保全又は保護する責任がある期間及び前項の規定に基づき甲が乙に対して違約金を請求できる期間は、本違約金条項は、なおその効力を有するものとする。

第3条 乙が本違約金条項が付されている契約の履行のために下請負事業者の下請負を行った場合の違約金の請求要領は、次の各号に定めるところによる。

- (1) 当該下請負事業者の故意又は過失により秘密が漏えいしたときは、甲は、乙と当該下請負事業者の間で締結された下請負契約の額を基礎として、前2条の規定に準じて算定した額の違約金を乙に請求することができる。

- (2) 前号の場合において、乙は、本違約金条項が付されている契約の当事者として、甲に対する違約金の支払義務を負う。
- (3) 前号の規定は、乙が同号の規定に従って甲に対する違約金を支払った場合において、乙が当該違約金相当額の全部又は一部を当該下請負事業者に求償することを妨げるものではない。
- (4) 乙が前号の規定により当該下請負事業者に対して求償する場合には、乙が当該下請負事業者を選定し、監督する立場にあることを踏まえ、乙と当該下請負事業者間において、漏えいの態様、過失の程度、経営への影響等を総合的に勘案し、合理的な範囲内の負担割合について、双方誠実に協議して定めるものとする。この場合において、乙は、製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（昭和31年法律第120号）等の関係法規を遵守し、不当に当該下請負事業者の利益を害してはならない。
- (5) 前各号の規定にかかわらず、甲、乙及び当該下請負事業者の間で締結された既存の特約条項に基づく三者間契約による違約金条項が適用される場合は、当該三者間契約による要領を優先するものとする。

第4条 本違約金条項の規定は、これに基づく違約金とは別に甲がその損害につき乙に対し賠償を請求することを妨げない。

別紙第 4

防衛事業適合事業者における保護すべき情報の情報セキュリティの確保
に係る契約書

適合事業者契約番号 [適合事業者契約番号]

契 約 相 手 方 乙 : [事業者名]

事 務 所 等 名 [保護すべき情報を取り扱う事務所等の名称]

防衛事業適合事業者における保護すべき情報の情報セキュリティの確保に係る契約

防衛装備庁装備政策部装備保全管理課長 [氏名]（以下「甲」という。）及び [事業者名] [役職名] [氏名]（以下「乙」という。）は、甲の定める手続による乙の申し込みに基づき、保護すべき情報（装備品等及び役務の調達に関する情報のうち、乙に保護を求める情報として、防衛省（防衛装備庁を含む。以下同じ。）が指定したものをいう。以下同じ。）の情報セキュリティの確保に係る防衛事業適合事業者契約を締結する。

（目的）

第1条 この契約は、[保護すべき情報を取り扱う事務所等の名称]において、乙が取り扱う保護すべき情報の情報セキュリティを確保するため、甲及び乙の間に締結するものである。

（情報セキュリティの確保）

第2条 乙は、この契約の履行に当たっては、この条項に定めるもののほか、防衛事業適合事業者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が付されている装備品等及び役務の契約（契約相手方の下請負者として保護すべき情報を取り扱う場合を含む。）（以下「情セキ特約付契約」という。）に基づく乙の情報セキュリティ対策を確実に実施するものとする。

（情報セキュリティ基本方針等）

第3条 乙は、保護すべき情報を取り扱うに当たり、保護すべき情報を取り扱うことの業務環境等を考慮の上、別紙（甲の定める「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」（以下「本基準」という。））に従って、必要な措置をとらなくてはならない。

<情報システムで保護すべき情報を取り扱う場合>

2 乙は、前項を実施するため、別添（本基準に従い乙が作成し、防衛省が確認した情報セキュリティ基本方針、情報セキュリティ規則及び情報セキュリティ実施手順（以下「情報セキュリティ基本方針等」という。））を適切に維持し、これを管理しなければならない。

<紙媒体のみで保護すべき情報を取り扱う場合>

2 乙は、前項を実施するため、紙媒体のみで保護すべき情報を取り扱うこととし、別添（本基準に従い乙が作成し、防衛省が確認した情報セキュリティ基本方針及び情報セキュリティ規則（以下「情報セキュリティ基本方針等」という。））を適切に維持し、これを管理しなければならない。

3 乙は、情報セキュリティ基本方針等のうち、内容の全部又は一部を変更しよ

うとするときは、甲の定める申請又は届出の手続をとらなければならない。

(監査)

第4条 甲又は甲の依頼を受けた者（この条において「甲」という。）は、乙においてこの契約及び情セキ特約付契約の条項の定めに従い保護すべき情報の取扱いが行われているかにつき、監査を行うものとする。

2 乙は、情報セキュリティ対策の実施状況について、甲の定める要領により定期的に点検を行い、管轄する地方防衛局にその結果を申告しなければならない。

3 甲は、第1項に規定する監査を実地で行うため、甲の指名する者を乙の事業所、工場その他の関係場所に派遣することができる。

4 甲は、第1項に規定する監査の結果、乙において情報セキュリティ基本方針等に従い保護すべき情報の取扱いが行われていないと認める場合には、その是正のため必要な措置を講じるよう求めることができる。

5 乙は、前項の規定により是正のため甲から必要な措置を講じるよう求めがあった場合には、速やかに必要な措置を講じなければならない。

(契約の解除)

第5条 甲は、乙がこの契約に定める義務に違反した場合、又は次に掲げる事項に該当する場合は、この契約を解除することができる。

(1) 乙が存在しなくなったとき。

(2) 乙が、第4条第4項の措置を所要の期間内に講じなかったとき。

(3) 乙が、不正な手段により、この契約又は他の防衛事業適合事業者契約を締結したことが判明したとき。

(4) 乙が、正当な理由がなくて、契約締結日から3年を経過しても、情セキ特約付契約に係る競争入札に参加しなかったとき、随意契約に応じなかったとき、又は保護すべき情報の取扱いがなかったとき。

2 甲は、乙が情セキ特約付契約を現に履行しておらず、当分の間情セキ特約付契約を履行することが想定されない場合は、この契約を解除するため、乙と協議することができる。

3 乙は、情セキ特約付契約を現に履行しておらず、当分の間情セキ特約付契約を履行することが想定されない場合は、この契約を解除するため、甲と協議することができる。

(契約期間)

第6条 この契約の契約期間は、契約を締結した日から5年間とする。

2 乙は、前項に規定する契約期間の延長を希望する場合には、この契約の残余の期間が6か月前から3か月前までの間に、甲の定める手続に基づき、契約期間の延長を申請するものとする。

- 3 前項の規定による延長の期間は、5 年を上限とする。
- 4 前項の規定は、複数回の延長を排除するものではない。

(代金)

第7条 この契約は、甲乙間に、この契約を原因とした金銭のやり取りを生じさせるものではない。

- 2 前項の規定は、情セキ特約付契約に基づき、この契約の履行に係る違約金その他の金銭のやり取りを定めることを排除するものではない。
- 3 第1項の規定は、防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律（令和5年法律第54号）に基づき、防衛省が、この契約の履行に係る財政上の措置をとることを排除するものではない。

(その他)

第8条 乙は、防衛事業適合事業者であることを装備品等、包装容器、表紙又は送り状等に表示するとき、若しくは保護すべき情報を取り扱う事務所等であることをその事務所等の表示板等に表示するときは、不当な、又は著しく誇大な表示を行ってはならない。

- 2 乙は、甲の同意なく、この契約によって知り得た情報を第三者に開示又は漏えいし、若しくは防衛省との契約の履行以外の目的に使用してはならない。
- 3 前項の規定は、この契約の終了後において準用する。
- 4 乙は、この契約に基づき発生した権利義務を第三者に譲渡し、又は貸与してはならない。
- 5 甲及び乙は、この契約が満了するまでの間において、この契約に定める内容を変更する必要があると認める場合は、当該変更について協議するものとする。
- 6 甲及び乙は、この契約に関し紛争又は疑義が生じた場合は、その都度、協議して解決するものとする。

(裁判管轄)

第9条 この契約は、日本国内法に準拠する。

- 2 この契約に関する訴えは、東京地方裁判所の管轄に属するものとする。

上記契約の締結を証するため、契約書 2 通を作成し、甲及び乙が記名、押印の上、各 1 通を保有する。

令和 年 月 日

甲 防衛装備庁装備政策部
装備保全管理課長 [氏名] 印

乙 [住所]
[事業者名]
[役職名] [氏名] 印

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

＜情報システムで保護すべき情報を取り扱う場合＞

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

情報セキュリティ基本方針

情報セキュリティ規則

＜情報システムで保護すべき情報を取り扱う場合＞

情報セキュリティ実施手順

別紙第5

防衛事業適合事業者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

(保護すべき情報の取扱い)

第1条 乙は、この特約条項が付された契約（以下「本契約」という。）を履行するに際しては、この特約条項及び保護すべき情報（装備品等及び役務の調達に関する情報のうち、乙に保護を求める情報として、防衛省（防衛装備庁を含む。）が指定したものをいう。以下同じ。）の情報セキュリティの確保について防衛装備庁と締結した防衛事業適合事業者契約（以下「適合事業者契約」という。）の定めるところに従い、本契約において甲が指定した保護すべき情報（以下「本契約保護情報」という。）を取り扱わなければならない。

(下請負事業者に対する指導監督)

第2条 乙は、本契約を履行するに当たり、この特約条項を適切に履行する義務を負い、下請負事業者（本契約の履行に係る作業に従事する全ての事業者（乙を除く。）をいう。以下同じ。）に対して、適切な指導・監督を行わなければならない。

(下請負事業者に本契約保護情報を取り扱わせる際の手続及び第三者開示の禁止)

第3条 乙は、本契約を履行するに当たり、適合事業者契約を締結していない下請負事業者（以下「未適合下請負事業者」という。）に本契約保護情報を取り扱わせる必要が生じた場合には、当該未適合下請負事業者において情報セキュリティが確保されるよう、防衛装備庁装備政策部長（以下「装備政策部長」という。）が別に定めるところにより、本契約保護情報の適切な取扱いに必要な事項を確認しなければならない。

2 乙は、装備政策部長が別に定めるところにより、前項の下請負事業者に本契約保護情報を取り扱わせることについて、同項の規定により確認した内容を添えて、甲の承認を得なければならない。

3 甲は、前項の規定により申請のあった内容を直接確認する必要があると認めた場合には、乙に、その旨を申し入れるものとする。

4 乙は、甲から前項の申し入れがあった場合には、必要な協力を行うものとする。

5 乙は、本契約を履行するに当たり、適合事業者契約を締結している下請負事業者（以下「適合下請負事業者」という。）に本契約保護情報を取り扱わせる必要が生じた場合には、当該適合下請負事業者が適合事業者契約に基づき地

方防衛局に申告した情報セキュリティ対策実施点検書により、当該適合下請負事業者が本契約保護情報の適切な取扱いに必要な事項を備えていることを確認しなければならない。

- 6 乙は、装備政策部長が別に定めるところにより、前項の規定により確認した内容を書面により甲に届出しなければならない。
- 7 乙は、原則として、下請負事業者を除く第三者（甲と直接契約関係にある者以外の全ての者をいう。以下同じ。）に本契約保護情報を開示してはならない。ただし、本契約の履行上又は公益上特に当該第三者に開示する必要があると認められる場合には、装備政策部長が別に定めるところにより、その都度、甲と協議するものとする。
- 8 乙は、第三者との契約（本契約及び適合事業者契約以外の全ての契約をいう。この項において同じ。）において、乙が保有し、又は知り得た情報を伝達、交換、共有等を行う約定があるときは、本契約保護情報をその約定の対象から除くよう、当該第三者との契約を変更する等の措置を講じなければならない。

（未適合下請負事業者に対する監査）

- 第4条 甲は、未適合下請負事業者に対して直接監査を行う必要があると認めた場合には、乙に、その旨を申し入れるものとする。
- 2 乙は、甲から前項の申し入れがあった場合には、必要な協力をしなければならない。
 - 3 甲は、第1項に規定する監査を行うため、甲の指名する者を当該未適合下請負事業者の事業所、工場その他の関係場所に派遣することができる。
 - 4 甲は、第1項に規定する監査の結果、当該未適合下請負事業者において第2条に規定する乙の指導・監督に基づいて作成した情報セキュリティ基本方針等に従い本契約保護情報の取扱いが行われていないと認めた場合には、その是正のため必要な措置を講じるよう求めることができる。
 - 5 甲は、前項の規定により同項の未適合下請負事業者には是正のため必要な措置を講じるよう求めるときは、乙を通じて求めるものとする。

（事故発生時の措置）

- 第5条 乙は、事故等（情報セキュリティ事故及び情報セキュリティ事象に該当するものをいう。以下同じ。）が発生したときは、適合事業者契約に付属する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、同基準に従い乙が作成した情報セキュリティ基本方針及び情報セキュリティ規則に定めるところにより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甲に報告しなければならない。
- 2 乙は、前項に規定する事故等が本契約の履行及び関連する装備品等の運用に与える影響等について調査し、その措置について甲と協議しなければならない。

ない。

- 3 前項の協議の結果、事故等が乙の責めに帰すべき事由によるものである場合には、その措置に必要な費用は、乙の負担とする。
- 4 前項の規定は、甲の損害賠償請求権を制限するものではない。

(契約の解除)

第6条 甲は、乙の責めに帰すべき理由により事故等が発生し、本契約の目的を達することができなくなった場合又は適合事業者契約が解除された場合には、本契約の全部又は一部を解除することができる。

- 2 前項の場合においては、本契約の解除に関する規定を準用する。

(本契約履行後における乙の義務等)

第7条 第1条、第2条及び第5条の規定は、本契約の履行後において、乙又は乙の下請負事業者が本契約保護情報を取り扱う場合について準用する。

- 2 第4条の規定は、本契約の履行後において、未適合下請負事業者が本契約保護情報を取り扱う場合について準用する。
- 3 本契約の履行後において、当該本契約保護情報が保護すべき情報ではなくなった場合には、前2項の規定を適用しない。
- 4 甲は、本契約の終了後において、甲から乙に対して交付し、又は伝達した本契約保護情報（以下「交付保護情報」という。）の返却、乙又は乙の下請負事業者が作成し、又は製作した本契約保護情報（以下「作成保護情報」という。）の提出等の指示のほか、業務に支障が生じるおそれがない場合には、乙に本契約保護情報の破棄を求めることができる。
- 5 乙は、前項の指示又は求めがあった場合において、交付保護情報を引き続き保有する必要があるときは、その理由を添えて甲に協議を求めることができる。
- 6 乙は、第4項の指示又は求めがあった場合において、作成保護情報を引き続き保有する必要があるときは、当該作成保護情報の名称及び保有期間を甲に届け出て確認を得るものとする。
- 7 乙は、前2項の規定により本契約保護情報の保有が認められた場合において、当該本契約保護情報の取扱者名簿に変更があるときは、その変更内容を甲の求める届出先に届け出て確認を得るものとする。

防衛事業適合事業者契約の契約条項に係る細部事項

第 1 秘密取扱原因契約のリスト（第 6 条関係）

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（装装保第 1 4 8 4 6 号。令和 7 年 7 月 3 1 日。以下「実施要領」という。）別紙第 2 防衛事業適合事業者契約条項（以下「契約条項」という。）第 6 条第 2 項に規定する秘密取扱原因契約を網羅したリストの更新は、毎年 6 月末及び 1 2 月末時点を基準として行うものとする。

第 2 秘密保全体制の整備・維持（第 8 条関係）

- 1 契約条項第 8 条第 1 項に規定する装備政策部長が別に定める要件は、実施要領別紙第 1 付紙様式第 1－1 から付紙様式第 1－5 までの各情報保全体制に係る保全基準兼点検票の項目の欄に掲げる項目とする。
- 2 契約条項第 8 条第 1 項に規定する総括者の指名に関する基準は、付紙第 1 に掲げる細部審査基準とする。

第 3 新たな秘密保全施設及び秘密取扱情報システムの構築（第 9 条関係）

契約条項第 9 条第 1 項の規定による手続において、乙は、実施要領別紙第 1 第 1 4 第 1 項から第 3 項までの規定に基づき、新たな秘密保全施設及び秘密取扱情報システムの内容が保全基準を満たしていることを甲から承認されなければならない。

第 4 関係社員候補者名簿（第 1 4 条関係）

- 1 契約条項第 1 4 条第 1 項に規定する装備政策部長が別に定める様式は、付紙様式第 1 とし、甲は、確認した結果を付紙様式第 2 により、乙に通知するものとする。
- 2 関係社員候補者名簿に記載する従業者の掲載基準は、付紙第 2 のとおりとする。

第 5 従業者からの同意書（第 1 7 条関係）

- 1 契約条項第 1 7 条第 1 項第 1 号に規定する装備政策部長が別に定める同意書の様式は、付紙様式第 3 とする。
- 2 契約条項第 1 7 条第 2 項に規定する一定の期間は、関係社員となった日から 5 年間とし、同項ただし書の装備政策部長が別に定める場合は、次の各号に掲げる場合とする。
 - (1) 関係社員名簿に記載した内容に変更がある場合
 - (2) 引き続き関係社員とすることに疑いを生じさせる事情がある場合
 - (3) その他甲が必要と判断した場合

第 6 人的クリアランスの事務（第 1 8 条関係）

乙は、特定秘密を取り扱う従業者の確認に関し、実施要領別紙第2付紙第3適性評価に関する特約条項に基づき、必要な措置を講ずるものとする。

第7 外国からの影響及び支配（第19条関係）

契約条項第19条に規定する外国からの影響及び支配の程度に関し、乙は、実施要領別紙第1付紙様式第1-1の保全基準兼点検票に掲げる事項に照らし、外国からの影響及び支配の有無について自己点検を行い、甲の確認を受けるものとする。

第8 交付・保有（第26条関係）

1 契約条項第26条第5項に規定する装備政策部長が別に定める表示は、次の各号に掲げる表示等とする。

(1) 特定資料等が次の各号に掲げる情報に係るものであるときは、当該各号に定める表示。ただし、既にNATO SECRETの表示がされているものについては、改めて当該表示をすることを要しない。

ア 秘密軍事情報（秘密軍事情報の保護のための秘密保持の措置に関する日本国政府とアメリカ合衆国政府との間の協定第1条(a)に規定する秘密軍事情報であって、アメリカ合衆国政府から受領したものをいう。） 米国政府

イ 北大西洋条約機構秘密情報（北大西洋条約機構から受領した情報又は資料であって、情報及び資料の保護に関する日本政府と北大西洋条約機構との間の協定第1条(ii)に規定する秘密の指定を受けているものをいう。） NATO SECRET

ウ 仏国秘密情報（情報の保護に関する日本国政府とフランス共和国政府との間の協定第1条(a)に規定する秘密情報であって、フランス共和国政府から受領したものをいう。） 仏国政府

エ 豪州秘密情報（情報の保護に関する日本国政府とオーストラリア政府との間の協定第1条aに規定する秘密情報であって、オーストラリア政府から受領したものをいう。） 豪州政府

オ 英国秘密情報（情報の保護に関する日本国政府とグレートブリテン及び北アイルランド連合王国政府との間の協定第1条aに規定する秘密情報であって、グレートブリテン及び北アイルランド連合王国政府から受領したものをいう。） 英国政府

カ インド秘密軍事情報（秘密軍事情報の保護のための秘密保持の措置に関する日本政府とインド共和国政府との間の協定第1条aに規定する秘密軍事情報であって、インド共和国政府から受領したものをいう。） インド政府

キ 伊国秘密情報（情報の保護に関する日本国政府とイタリア共和国政府との間の協定第1条aに規定する秘密情報であって、イタリア共和国政府から受領したものをいう。） 伊国政府

ク 韓国秘密軍事情報（秘密軍事情報の保護に関する日本国政府と大韓民国政府との間の協定第2条(a)に規定する秘密軍事情報であって、大韓民国政府から受領したものをいう。） 韓国政府

ケ 独国秘密情報（情報の保護に関する日本国政府とドイツ連邦共和国政府との間の協定第1条(a)に規定する秘密情報であって、ドイツ連邦共和国政府から受領したもの） 独国政府

コ 瑞国秘密情報（防衛装備品及び技術の移転に関する日本国政府とスウェーデン王国政府との間の協定第四条に基づく防衛装備品及び技術に係る情報保護に関する日本国防衛省とスウェーデン王国を代表する国防装備庁との間の取決め第1項に規定する秘密情報であって、スウェーデン王国国防装備庁から受領したもの） 瑞国政府

サ サウジ秘密情報（防衛協力及び交流の過程で取得される情報の保護に関する日本国防衛省とサウジアラビア王国国防省との間の取決め第1項aに規定する秘密情報であって、サウジアラビア王国国防省から受領したもの） サウジ政府

シ UAE秘密情報（防衛装備品及び技術の移転に関する日本国政府とアラブ首長国連邦政府との間の協定第五条に従って作成される防衛装備品及び技術に係る情報の保護に関する日本国防衛省とアラブ首長国連邦国防省との間の取決め第1項第3に規定する秘密情報（「محظور」に秘密指定されたものを除く。）であって、アラブ首長国連邦国防省から受領したもの） UAE政府

ス 宇国秘密情報（情報の保護に関する日本国政府と政府との間の協定第1条aに規定する秘密情報であって、ウクライナ政府から受領したもの）

(2) 特定資料等の各項の中央に当該文書、図画又は電磁的記録固有の数字又は組織名等を大判のスタンプによる表示又はこれに準ずる方法によって記載し、又は記録する等の所要の措置を講ずるものとする。

2 特定秘密である特定資料等を提供する場合において、契約条項第26条第5項ただし書の表示を付することが困難なときは、付紙様式第4により周知するものとする。

第9 閉鎖区域の構築・設定（第30条・第31条関係）

1 契約条項第30条第1項の規定により閉鎖区域を構築するに当たっては、乙は、付紙様式第5により甲に申請するものとする。

2 前項の規定により構築した閉鎖区域を変更しようとする場合は、乙は、同項の規定に準じて甲に申請するものとする。

3 契約条項第31条第1項の規定により閉鎖区域において特定資料等を取り扱う場合は、あらかじめ、乙は、当該閉鎖区域の名称、確認番号及び当該閉鎖区域を使用する秘密取扱原因契約並びに設定期間（始期年月日及び終期年月日）を、付紙様式第6により甲に届け出るものとする。

4 前項の規定により届け出た内容を変更しようとする場合は、乙は、同項の規定に準じて甲に届け出るものとする。

5 契約条項第31条第3項の規定により閉鎖区域の設定を解除した場合は、乙は、当該閉鎖区域の実施期間（始期年月日及び終期年月日）、保護措置の実施状況、異常の有無等を甲に届け出るものとする。

第10 携帯型情報通信・記録機器の持込制限（第36条関係）

- 1 契約条項第36条第2項に規定する装備政策部長が別に定める措置は、次の各号に掲げる措置を基準とする。
 - (1) 私有の携帯型情報通信・記録機器ではないこと。
 - (2) 業務上必要なソフトウェア以外のソフトウェアがインストールされていないこと。
 - (3) 直前に最新の検知ソフトウェアでフルスキャンしていること。
 - (4) 無線LANの機能が無効化されていること。
 - (5) 携帯型情報通信・記録機器の使用後に、秘密取扱情報システムの利用者が秘密のデータが保存されていないことを確認するとともに、当該利用者以外の者が点検すること。
 - (6) 使用日時・使用者・使用目的等を含む記録簿を整備すること。
 - (7) 携帯型情報通信・記録機器に対するリモートアクセスによる起動及び操作を禁止すること。
- 2 乙は、携帯型情報通信・記録機器を秘密保全施設等に持ち込もうとする場合は、その目的、作業内容、持ち込み期間（始期年月日及び終期年月日）、取り扱う特定資料等の名称、秘密の種類及び区分（「特定特別防衛秘密（機密・極秘・秘）」、「特別防衛秘密（機密・極秘・秘）」、「特定秘密」又は「装備品等秘密」）のほか、前項に規定する基準を満たすことを証する文書を添えて甲に申請するものとする。この際、乙は、一の秘密取扱原因契約に基づき携帯型情報通信・記録機器を秘密保全施設等に持ち込もうとする回数が複数に及ぶ場合は、包括的に申請することができる。

第11 情報システムの持ち込み・設置制限（第37条関係）

- 1 契約条項第37条第2項に規定する装備政策部長が別に定める措置は、次の各号に掲げる措置を基準とする。
 - (1) 私有の情報システムではないこと。
 - (2) 業務上必要なソフトウェア以外のソフトウェアがインストールされていないこと。
 - (3) 直前に最新の検知ソフトウェアでフルスキャンしていること。
 - (4) 無線LANの機能が無効化されていること。
 - (5) 情報システムの使用後に、秘密取扱情報システムの利用者が秘密のデータが保存されていないことを確認するとともに、当該利用者以外の者が点検すること。
 - (6) 使用日時・使用者・使用目的等を含む記録簿を整備すること。
- 2 乙は、情報システムを秘密保全施設等に持ち込もうとする場合は、その目的、作業内容、持ち込み期間（始期年月日及び終期年月日）、取り扱う特定資料等の名称、秘密の種類及び区分（「特定特別防衛秘密（機密・極秘・秘）」、「特別防衛秘密（機密・極秘・秘）」、「特定秘密」又は「装備品等秘密」）のほか、前項に規定する基準を満たすことを証する文書を添えて甲に申請するものとする。この場合において、乙は、秘密取扱原因契約に基づき情報システムを秘密保全施設等に持ち込もうとする回数が複数に及ぶときは、包括的に申請することができる。

第 1 2 秘密保全施設等の運用管理（第 3 8 条関係）

- 1 契約条項第 3 8 条第 1 項の規定に基づき、秘密保全施設等への立入りの状況を記録するため、乙は、立入者の所属、氏名、立入目的、その他の所要の事項について、付紙様式第 7 による立入記録簿に記載するものとする。
- 2 契約条項第 3 8 条第 4 項に規定する装備政策部長が別に定める期間は、法令その他別段の定めのある場合を除き、当該記録を作成した日の翌年度から起算して 5 年間を基本とする。

第 1 3 登録及び管理（第 4 2 条関係）

- 1 契約条項第 4 2 条第 1 項の規定に基づき、特定資料等の管理の現況を把握するため、乙は、次の各号に掲げる帳簿について、当該各号による様式を基準として、特定資料等を登録及び管理するものとする。
 - (1) 秘密文書等保管簿（装備品等秘密／特別防衛秘密） 付紙様式第 8 - 1
 - (2) 秘密文書等保管簿（特定秘密） 付紙様式第 8 - 2
 - (3) 秘密文書等複製等実施記録簿 付紙様式第 9
 - (4) 指定・解除簿（装備品等秘密／特別防衛秘密） 付紙様式第 1 0 - 1
 - (5) 指定・解除簿（特定秘密） 付紙様式第 1 0 - 2
 - (6) 反故紙破棄／廃棄簿 付紙様式第 1 1
 - (7) 関係簿冊廃棄記録簿 付紙様式第 1 2
- 2 契約条項第 4 2 条第 3 項に規定する装備政策部長が別に定める期間は、法令その他別段の定めのある場合を除き、秘密取扱原因契約の終了した日の翌年度から起算して 5 年間を基本とする。

第 1 4 取扱いの記録（第 4 3 条関係）

- 1 契約条項第 4 3 条第 1 項の規定に基づき、特定資料等の閲覧その他関係社員及び下請負事業者関係社員による特定資料等の取扱いの経過を把握するため、乙は、次の各号に掲げる帳簿について、当該各号による様式を基準として必要な事項を記録し、これを管理するものとする。
 - (1) 秘密文書等閲覧簿 付紙様式第 1 3
 - (2) 秘密文書等貸出簿 付紙様式第 1 4
 - (3) 文字盤鍵組合せ番号変更記録簿 付紙様式第 1 5
 - (4) 適格証明書管理簿 付紙様式第 1 6
 - (5) 引継確認簿 付紙様式第 1 7
- 2 契約条項第 4 3 条第 3 項に規定する甲が別に定める期間は、法令その他別段の定めのある場合を除き、当該記録を作成した日の翌年度から起算して 5 年間を基本とする。

第 1 5 特定秘密の表示等（第 4 7 条関係）

契約条項第 4 7 条第 2 項に規定する装備政策部長が別に定める表示は、次の各号に掲げる表示とする。

- (1) 特定秘密資料等が次の各号に掲げる情報であるときは、当該各号に定める表示。ただし、既に N A T O S E C R E T の表示がされているも

のについては、改めて当該表示をすることを要しない。

- ア 秘密軍事情報 米国政府
- イ 北大西洋条約機構秘密情報 N A T O S E C R E T
- ウ 仏国秘密情報 仏国政府
- エ 豪州秘密情報 豪州政府
- オ 英国秘密情報 英国政府
- カ インド秘密軍事情報 インド政府
- キ 伊国秘密情報 伊国政府
- ク 韓国秘密軍事情報 韓国政府
- ケ 独国秘密情報 独国政府
- コ 瑞国秘密情報 瑞国政府
- サ サウジ秘密情報 サウジ政府
- シ U A E 秘密情報 U A E 政府
- ス 宇国秘密情報 宇国政府

- (2) 特定資料等の各項の中央に当該文書、図画又は電磁的記録固有の数字又は組織名等を大判のスタンプによる表示

第 1 6 装備品等秘密の表示等（第 5 1 条関係）

契約条項第 5 1 条に規定する装備政策部長が別に定める表示は、特定資料又は特定物件が次の各号に掲げる情報である場合の当該各号に定める表示とする。ただし、既に N A T O S E C R E T の表示がされているものについては、改めて当該表示をすることを要しない。

- (1) 秘密軍事情報 米国政府
- (2) 北大西洋条約機構秘密情報 N A T O S E C R E T
- (3) 仏国秘密情報 仏国政府
- (4) 豪州秘密情報 豪州政府
- (5) 英国秘密情報 英国政府
- (6) インド秘密軍事情報 インド政府
- (7) 伊国秘密情報 伊国政府
- (8) 韓国秘密軍事情報 韓国政府
- (9) 独国秘密情報 独国政府
- (10) 瑞国秘密情報 瑞国政府
- (11) サウジ秘密情報 サウジ政府
- (12) U A E 秘密情報 U A E 政府
- (13) 宇国秘密情報 宇国政府

第 1 7 防衛事業適合事業者による点検（第 6 6 条関係）

- 1 契約条項第 6 6 条各項の規定に基づき、乙は、次の各号に掲げる書類について、当該各号に定める期間に応じ、甲に提出するものとする。

- (1) 実施要領別紙第 1 付紙様式第 7 の自己点検申告書及び同付紙様式第 1 3 の自己点検票（月次） 次項の表の起算月から毎月
- (2) 実施要領別紙第 1 付紙様式第 7 の自己点検申告書及び同付紙様式第 1 ー 1 から同付紙様式第 1 ー 5 までの保全基準兼点検票並びにリスク査定関係書類 次項の表の起算月から 1 年ごと

- 2 前項各号の関係書類の提出期間の起算は、次の表の防衛事業適合事業者契約の締結日の属する期間に対応した月から起算するものとする。

防衛事業適合事業者契約の締結日の属する期間	関係書類の提出期間の起算月
4月1日～6月30日	7月
7月1日～9月30日	10月
10月1日～12月31日	1月
1月1日～3月31日	4月

第18 秘密保全施設を備えない限定的な防衛事業適合事業者に係る下請負の禁止の例外（第68条関係）

契約条項第68条第3項に規定する装備政策部長が別に定める場合は、乙が秘密保全施設を備えずに下請負事業者の秘密保全施設又は防衛省の施設において当該下請負事業者に特定資料等を取り扱わせる必要性及び合理性が存在することが認められた場合であって、次の各号に掲げる要件を全て満たしたときとする。

- (1) 契約条項第69条第1項の規定により、同項の秘密の管理職員の許可を得ていること。
- (2) 乙の秘密保全規則に当該下請負事業者による特定資料等の取扱いの管理について規定されており、乙にこれを実施する態勢が整っていること。
- (3) 乙が、当該下請負事業者による特定資料等の取扱いに関し、当該下請負事業者との契約に従い、当該下請負事業者と同等の注意義務を負うこと。
- (4) 乙による特定資料等の取扱いは、秘密の管理職員が承認した範囲であること。

第19 契約の延長（第72条関係）

契約条項第72条に規定する装備政策部長が別に定める要件として、乙は、実施要領別紙第1付紙様式第10の契約延長の申請書及び同付紙様式第1-1から同付紙様式第1-5までの保全基準兼点検票を提出するものとする。

第20 情報システムに関する記録（情報システム特約条項第4条、第5条、第14条、第15条、第16条、第23条、第25条関係）

- 1 実施要領別紙第2付紙第4の秘密取扱情報システムに関する特約条項（以下「情報システム特約条項」という。）の規定による秘密取扱情報システムに関する記録を把握するため、乙は、次の各号に掲げる帳簿について、当該各号による様式を基準として記録するものとする。

- (1) 秘密取扱情報システム利用者指定・解除簿 付紙様式第18
- (2) 秘密取扱情報システム利用に当たっての同意書 付紙様式第19
- (3) 可搬記憶媒体管理簿 付紙様式第20

- (4) 秘密取扱情報システム管理簿 付紙様式第 2 1
 - (5) 秘密取扱情報システムぜい弱性対処記録 付紙様式第 2 2
 - (6) ホワイトリスト 付紙様式第 2 3
 - (7) 構成設定目録 付紙様式第 2 4
 - (8) 操作手順書 付紙様式第 2 5
 - (9) アクセス制御方針 付紙様式第 2 6
 - (10) 携帯型情報通信・記録機器の利用に係る要件 付紙様式第 2 7
 - (11) 秘密取扱情報システムのセキュリティを確保するための組織体制 付紙様式第 2 8－1、2 8－2
 - (12) ネットワーク構成図 付紙様式第 2 9
 - (13) データフロー図 付紙様式第 3 0
 - (14) アカウント管理計画 付紙様式第 3 1
 - (15) 識別子管理簿 付紙様式第 3 2
 - (16) システムログ分析結果記録簿 付紙様式第 3 3
 - (17) ぜい弱性スキャン分析結果記録簿 付紙様式第 3 4
 - (18) バックアップ実施等記録簿 付紙様式第 3 5
 - (19) メンテナンス等計画 付紙様式第 3 6
 - (20) メンテナンス等実施記録 付紙様式第 3 7
- 2 情報システム特約条項第 2 5 条第 2 項に規定する装備政策部長が別に定める期間は、法令その他別段の定めのある場合を除き、当該記録を作成した日の翌年度から起算して 5 年間を基本とする。

第 2 1 秘密取扱情報システム実装計画の届出（情報システム特約条項第 1 2 条関係）
秘密取扱情報システム実装計画を変更した場合は、乙は、付紙様式第 3 8 による様式を基準として届け出るものとする。

総括者の指名に関する細部審査基準

乙は、総括者を指名するに当たっては、以下の第 1 から第 3 までの基準のいずれかを満たすことができる者とする。

第 1 基準 1

- 1 総括者は、防衛事業適合事業者の契約代理人、防衛事業に関する事業本部長又は工場長その他の防衛事業適合事業者の経営責任者又は防衛事業の執行責任者として、防衛事業適合事業者及びその下請負事業者に対し、秘密の保全についての権限を行使できること。
- 2 総括者は、過去 10 年の間、2 年以上継続して、通算 3 年以上にわたり防衛産業において該当する秘密区分を含む防衛省の秘密を取り扱った実務経験があること。
- 3 総括者は、リスク評価、従業員への教育、秘密保全施設等の管理、定期的な点検、秘密取扱情報システム、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置について熟知しており、日常的な秘密の取扱いについて関係社員に対する指導を行うことができること。

第 2 基準 2

- 1 総括者は、防衛事業適合事業者の契約代理人、防衛事業に関する事業本部長又は工場長その他の防衛事業適合事業者の経営責任者又は防衛事業の執行責任者として、防衛事業適合事業者及びその下請負事業者に対し、秘密の保全についての権限を行使できること。
- 2 第 1 の 2 及び 3 を満たすことができない場合には、以下の措置を講じること。
 - (1) 保全責任者その他秘密保全組織を管理する者であって、総括者を支える者として過去 10 年の間に通算 5 年以上にわたり防衛産業において該当する秘密区分を含む防衛省の秘密を取り扱った実務経験があり、リスク評価、従業員への教育、秘密保全施設等の管理、定期的な点検、秘密取扱情報システム、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取

扱いに関する措置について熟知している者を配置すること。

- (2) 総括者は、防衛事業適合事業者契約の申込みをした日から事業者として秘密を取り扱うまでに、リスク評価、従業者への教育、秘密保全施設等の管理、定期的な点検、秘密取扱情報システム、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置についての防衛装備庁の研修を修了すること。

第3 基準3

- 1 総括者は、防衛事業適合事業者の契約代理人、防衛事業に関する事業本部長又は工場長その他の防衛事業適合事業者の経営責任者又は防衛事業の執行責任者として、防衛事業適合事業者及びその下請負事業者に対し、秘密の保全についての権限を行使できること。
- 2 第2の2(1)を満たすことができない場合には、以下の措置を講じること。
 - (1) 総括者は、防衛事業適合事業者契約の申込みをした日から事業者として秘密を取り扱うまでに、リスク評価、従業者への教育、秘密保全施設等の管理、定期的な点検、秘密取扱情報システム、下請負事業者との関係及び事故対応を含め、年次及び月次の秘密の取扱いに関する措置についての防衛装備庁の研修を修了すること。
 - (2) 保全責任者、秘密取扱情報システム管理者、秘密取扱情報システム担当者、アカウント管理者その他秘密保全組織を管理する者は、防衛事業適合事業者契約の申込みをした日から事業者として秘密を取り扱うまでに1回及びその後は3か月に1回の頻度により合計4回、リスク評価、従業者への教育、秘密保全施設等の管理、定期的な点検、秘密取扱情報システム、下請負事業者との関係及び事故対応を含め、日常的な秘密の取扱いに関する保全措置についての防衛装備庁の研修を修了すること。

関係社員候補者名簿の作成基準

防衛事業適合事業者は、契約条項第 14 条に基づく関係社員候補者名簿作成の際の従業者（以下「候補者」という。）の掲載に当たっては、以下の点に留意するものとする。

- (1) 候補者には、人格、素行、勤務状況等を総合的に勘案し、秘密を取り扱う業務に従事する者としてふさわしい者を充て、その範囲は最小限とすること。
- (2) 候補者の指定に当たっては、従業者の同意を得た上で確認を行い、確認の過程で得た個人情報の取扱いについては目的外の使用をしないこと。
- (3) 候補者の指定に当たっては、次表に掲げる掲載基準を参考に確認するものとし、従業者との面談や公的証明書等により確認するとともに、契約の履行中においても継続的に把握すること。
- (4) 関係社員候補者名簿又は関係社員名簿に掲載された従業者の情報に変更のあった場合は、改めて申告するよう従業者に注意喚起すること。
- (5) 関係社員候補者名簿の記載事項に関し、装備保全管理課長から改めて確認を求められた場合は速やかに対応をすること。
- (6) 従業者が、別の契約で確認を受けた関係社員名簿が有効期間内にある場合は、氏名、当該確認通知の発簡番号及び発簡年月日の記入をもってこれに代えることができる。

掲載基準	判定の目安
1 秘密の漏えいのおそれがないことの確認として、人格、素行、勤務状況等を踏まえ、ふさわしい者であることの総合的な確認が行われていること。また、防衛装備庁との契約に違反する行為を求められた場合に、これを拒む権利を実効性をもって法的に保障されない者に該当しない者であることの確認が行われていること。	関係社員候補者名簿に次に掲げる事項が漏れなく記載されており、事業者におけるこれらの確認方法及び確認した事実が明確になっていること。 (1) 候補者に指定された者の氏名 (2) 生年月日 (3) 所属する部署 (4) 役職 (5) 勤務状況等（人格、素行を含む。） (6) 国籍
2 候補者の範囲は必要最小限にとどめられていること。	各候補者の従事する秘密業務の内容が明確になっていること。

付紙様式第 1

発 簡 番 号

発 簡 年 月 日

契 約 担 当 官 等 殿
(地方防衛局調達部長等 経由)

所 在 地
事業者名
代表者名

関係社員候補者名簿の提出について

標記について、属紙のとおり同意を得たく提出します。

1 調達要求番号

2 件名

添付書類：属紙

注 意

(特に厳重な取扱いを要する)

契約担当官等名	確認年月日

関係社員 候補者 名簿

番号	(ふりがな) 氏 名	関係社員 としての役職	関係社員 としての業務内容	生年月日	部署・役職	勤務状況等	国 籍	確認 結果	備 考

- ※1 名簿に所定の事項を記載した後は、「個人情報」の表示を併記する。
- ※2 備考欄には、防衛事業適合事業者において確認結果の根拠となった資料名等又は確認の方法等を記載するほか、その他懸念される事項等があればその旨記載する。
- ※3 関係社員の候補者が、既に確認を受けている関係社員（当初の確認から5年以内の者に限る。）である場合は、氏名、関係社員としての役職、関係社員としての業務内容のほか、備考欄に「確認済み」及び確認通知の発簡番号・発簡年月日を記載するものとする。
- ※4 契約担当官等は、関係社員の候補者の範囲について確認後、確認年月日を記載するものとする。
- ※5 装備保全管理課長は、関係社員候補者の確認を行った後、表題中「候補者」の部分有二重線で抹消するほか、同意を得られなかった候補者については二重線で抹消する。
- ※6 関係社員候補者名簿に記載された情報は、関係社員としての確認手続のみに使用し、目的外の利用を禁止するとともに適切に管理しなければならない。

付紙様式第2

発 簡 番 号

発 簡 年 月 日

(防衛事業適合事業者) 殿

防衛装備庁装備政策部

装備保全管理課長

関係社員候補者名簿について（通知）

〔防衛事業適合事業者からの届出文書番号（発簡年月日）〕により届出された標記について、【適当であると認めた／不適当であると認めた】ので通知します。

〔不適当であると認めた理由：（※）〕

※ 不適当であると認めた場合に、その理由を具体的に記載する。

写送付先：契約担当官等、地方防衛局調達部長等

年 月 日

同 意 書

(事業者名)

宛

私は、秘密を取り扱う業務に従事するに当たって、関係社員候補者名簿へ掲載され、秘密を取り扱う者としてふさわしい者であることの確認のために必要な事項を防衛省に報告し、防衛省がこの確認のため必要な場合はこれに協力することについて同意します。

また、私は、関係社員名簿に掲載された場合、秘密を取り扱うに当たり、在職中及び離職後において、秘密（特別防衛秘密/装備品等秘密）を故意に漏えい等したときには、関係法律により罰せられることがあること及び民事上の責任を問われることがあることを理解し、秘密を取り扱う業務に従事することに同意します。

現 住 所 :

氏 名 :

生 年 月 日 :

※本同意書は、防衛省の確認を受け、関係社員とされた日から起算して
5年間有効

付紙様式第 4

発 簡 番 号

發簡年月日

防衛裝備庁裝備政策部

裝備保全管理課長

特定秘密に係る指定書

その性質上、次の文書等には「特定秘密」の表示が行われていないが、特定秘密文書等に該当する。

[illegible]

付紙様式第 5

発 簡 番 号

発 簡 年 月 日

防衛装備庁装備政策部装備保全管理課長 殿

(防衛事業適合事業者)

閉鎖区域の[構築／変更]に係る確認について (申請)

標記について、([構築／変更]の理由を記載) のため、申請します。

添付書類： 1 秘密保全規則の改正案

2 保全基準兼点検票 (付紙様式第 1 - 4) 及び関係書類

写送付先：申請者である防衛事業適合事業者を管轄する地方防衛局調達
部長等

発 簡 番 号
発 簡 年 月 日

防衛装備庁装備政策部装備保全管理課長 殿

(防衛事業適合事業者)

閉鎖区域の[設定／期間の変更]について (届出)

標記について、下記のとおり届出ます。

記

- 1 閉鎖区域の確認番号
- 2 閉鎖区域の名称
- 3 秘密取扱原因契約
- 4 設定期間

写送付先：申請者である防衛事業適合事業者を管轄する地方防衛局調達
部長等

- 注：1 第1項には、構築の際に防衛装備庁から確認を受けたときの通知文書番号及び発簡年月日を記載すること。
- 2 第4項には、始期年月日及び終期年月日を記載すること。設定期間の変更の場合には、変更前及び変更後のそれぞれについて、始期年月日及び終期年月日を記載すること。

立 入 記 録 簿

秘密保全施設等の名称：_____

年月日	立入時刻	退出時刻	所 属	氏 名	目 的	適格証明書 の 番 号	本人確認欄	保全責任者 確認欄	備 考
	:	:							
	:	:							
	:	:							
	:	:							
	:	:							

※ 関係社員以外の立入可能者の場合は、「適格証明書の番号」欄には、当該立入可能者の身分証明書等の番号を記載させる。

【装備品等秘密文書等／特別防衛秘密文書等】保管簿

番号	登録番号	一連番号	指定条件	件 名	接 受		
					年月日	受領者 確認欄	保全責任者 確認欄

付紙様式第 8－1 （ 2 ／ 2 ）

複製等				送 達				破 棄			備 考
年月日	実施者 確認欄	立会官 確認欄	保全責任者 確認欄	年月日	送達先	受領者 確認欄	保全責任者 確認欄	年月日	実施者 確認欄	保全責任者 確認欄	

※ 1 文書と物件は、別葉の保管簿で管理する。

※ 2 【装備品等秘密文書等／特別防衛秘密文書等】を送達又は破棄し、若しくは指定が解除された場合は、当該【装備品等秘密文書等／特別防衛秘密文書等】の管理情報を記録する行の全体を赤色の二重線等で抹消する。

※ 3 【装備品等秘密／特別防衛秘密】に指定される前の文書等については、備考欄に【指定前装備品等秘密／指定前特別防衛秘密】と記載する。その後、防衛省により【装備品等秘密／特別防衛秘密】に指定された場合は、登録番号等の管理情報を記載するとともに、備考欄の【指定前装備品等秘密／指定前特別防衛秘密】の記載を赤色の二重線等で抹消する。

特定秘密文書等保管簿

番号	登録番号 及び一連番号	保存期間	特定秘密の指定		件 名	接 受		
			整理番号	有効期間が 満了する年月日		年月日	受領者 確認欄	保全責任者 確認欄

付紙様式第 8－2 （ 2 ／ 2 ）

作成（複製を含む。）				送 達				廃 棄			備 考
年月日	実施者 確認欄	立会官 確認欄	保全責任者 確認欄	年月日	送達先	受領者 確認欄	保全責任者 確認欄	年月日	実施者 確認欄	保全責任者 確認欄	

※ 1 文書と物件は、別葉の保管簿で管理する。

※ 2 特定秘密文書等を送達、廃棄し、又は特定秘密の指定の有効期間が満了し、若しくは特定秘密の指定が解除された場合は、当該特定秘密文書等の管理情報を記録する行の全体を赤色の二重線等で抹消する。

※ 3 特定秘密の指定の有効期間が延長された場合は、特定秘密の指定の有効期間が満了する年月日欄に延長後の指定の有効期間が満了する年月日を追記する（それまでの指定の有効期間が満了する年月日は赤色の二重線等で抹消する。）。

【装備品等秘密文書等複製等／特別防衛秘密文書等複製等／特定秘密文書等作成】実施記録簿

実 施 年 月 日	調達要求番号	複製又は 製作の別	件 名	登録番号	一連番号	数量	保管場所	実施者 確認欄	保全責任者 確認欄	備 考

※ 文書と物件は、別葉で管理する。

指定・解除簿（【装備品等秘密／特別防衛秘密】）

番号	所 属	氏 名	役 職	指 定			解 除			備 考
				年月日	本人確認欄	総括者 確認欄	年月日	本人確認欄	総括者 確認欄	

※ 1 役職欄には、秘密保全組織上の役職を記載する。

※ 2 解除する場合は、その理由（例：契約終了、人事異動、退職等）を備考欄に記載する。

指定・解除簿（特定秘密）

番号	所 属	氏 名	役 職	適性評価 年 月 日	指 名			解 除			備 考
				適性評価 有効期間	年 月 日	本人 確 認 欄	業 務 管 理 者 確 認 欄	年 月 日	本人 確 認 欄	業 務 管 理 者 確 認 欄	

※ 1 役職欄には、秘密保全組織上の役職を記載する。

※ 2 解除する場合は、その理由（例：契約終了、人事異動、退職等）を備考欄に記載する。

反古紙【破棄／廃棄】簿

[illegible]

関係簿冊廃棄記録簿（【装備品等秘密／特別防衛秘密／特定秘密】）

[illegible]

【裝備品等秘密文書等／特別防衛秘密文書等／特定秘密文書等】閱覽簿

[illegible]

【裝備品等秘密文書等／特別防衛秘密文書等／特定秘密文書等】貸出簿

[illegible]

【裝備品等秘密保全／特別防衛秘密保護／特定秘密保護】適格証明書管理簿

[illegible]

引継確認簿（【装備品等秘密／特別防衛秘密／特定秘密】）

引継年月日	保管数量		異状の有無	（※１）管理責任者／保全責任者		（※２）管理責任者		備考
	文書	物件		所属・氏名	確認欄	確認年月日	確認欄	
				（旧）				
				（新）				
				（旧）				
				（新）				
				（旧）				
				（新）				

※１ 所要に応じ、いずれかを選択して記載する。

※２ 保全責任者の引継確認簿の場合に設ける。

秘密取扱情報システム利用者指定・解除簿

番号	所 属	氏 名	役 職	指 定			解 除			備 考
				年月日	本人 確認欄	総括者 確認欄	年月日	本人 確認欄	総括者 確認欄	

※ 解除する場合は、その理由（例：契約終了、人事異動、退職等）を備考欄に記載する。

年 月 日

秘密取扱情報システム利用に当たっての同意書

(事業者名)

宛

私は、秘密取扱情報システム利用者として、次の事項内容を理解し、同システムを適切に利用することに同意します。

- 1 利用する情報システムが、秘密のデータを取り扱うための秘密取扱情報システムであること。
- 2 秘密取扱情報システムの利用は常時監視されるとともに、利用の履歴が記録され、検査の対象となること。
- 3 秘密取扱情報システムを不正に使用した場合は、法律上の責任を問われる可能性があること。

現 住 所 :

氏 名 :

生 年 月 日 :

※本同意書は、書名から 5 年間有効

可搬記憶媒体管理簿

1 管理番号等

管理番号	
媒体の種類	
品名／形式番号	

2 登録・廃棄

区分	年月日	秘密取扱情報システム 担当者	秘密取扱情報システム 管理者	データの 消去	復元でき ない状態 の点検	廃棄
登録						
廃棄				※1	※2、3	※4

※1 データ消去を実施した者の氏名、所属、実施時刻を記入し、署名する。

※2 データ消去を実施した者とは異なる者が、保護すべきデータが復元できない状態であることを点検する。

※3 点検した者の氏名、所属、実施日を記入し、署名する。

※4 廃棄を実施した者の氏名、所属、実施時刻を記入し、署名する。なお、廃棄は、データ消去実施者が兼ねることができる。

3 使用用途

番号	年月日	内 容	暗号化の 有無※5	秘密取扱情報シ ステム担当者	秘密取扱情報シ ステム管理者
1					
2					

※5 可搬記憶媒体に情報を記録するときは、暗号化すること。また、政府推奨暗号等を使用すること。

4 接続可能システム

番号	年月日	秘密取扱情報システム又は 情報システムの名称	秘密取扱情報シ ステム担当者	秘密取扱情報シ ステム管理者
1				
2				
3				

5 使用可能者

番号	年月日	所属	役職	氏名	秘密取扱情報システム担当者	秘密取扱情報システム管理者
1						
2						
3						
4						

6 使用履歴

番号	年月日	使用用途 番号	接続可能 システム番号	使用可能者 番号	秘密取扱情報システム担当者	秘密取扱情報システム管理者
1						
2						
3						
4						

7 確認履歴

年月日	秘密取扱情報システム担当者	秘密取扱情報システム管理者	備 考

8 秘密取扱情報システム以外の情報システムへの接続

年月日	秘密取扱情報システム担当者	秘密取扱情報システム管理者	備考（接続した情報システムなど）

秘密取扱情報システム管理簿

1 管理番号等

管理番号	
品名／形式番号	

2 登録・廃棄

区分	年月日	秘密取扱情報システム 担当者	秘密取扱情報システム 管理者	データの 消去	復元でき ない状態 の点検	廃棄
登録						
廃棄				※1	※2、3	※4

- ※1 データ消去を実施した者の氏名、所属、実施時刻を記入し、署名する。
- ※2 データ消去を実施した者とは異なる者が、保護すべきデータが復元できない状態であることを点検する。
- ※3 点検した者の氏名、所属、実施日を記入し、署名する。
- ※4 廃棄を実施した者の氏名、所属、実施時刻を記入し、署名する。なお、廃棄は、データ消去実施者が兼ねることができる。

秘密取扱情報システムぜい弱性対処記録

秘密取扱情報 システム管理番号	
発見日時	
発見者	
発見又は探知された ぜい弱性	
システムへの影響	
修正方法	
修正日	
修正実施者	
使用パッチ、 適用更新プログラム	
修正結果への評価等	

※ぜい弱性診断を実施した場合、診断結果等を添付する。

(秘密取扱情報システム管理番号)

ホワイトリスト

パソコン名又は機器名：

番号	名称	エディション	バージョン	提供元	適用区分	備考
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

(秘密取扱情報システム管理番号)

構成設定目録

構成要素：(ハードウェア／ソフトウェア／記憶媒体／ネットワーク)

No.	対象項目	要求事項	機能名称	設定項目	設定値	設定値の説明 (変更した理由を追記)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

(秘密取扱情報システム管理番号)

操作手順書

1. はじめに

- (1) 目的
- (2) 事前準備
- (3) 留意事項

2. 操作手順

- (1) 端末起動
- (2) ログイン

(以降は機器に応じて記載)

(秘密取扱情報システム管理番号)

アクセス制御方針

1. 秘密取扱情報システムのアクセス制御
(システム管理者とシステム利用者の区分)
2. 必要最小限度の原則
3. アカウント管理
 - (1) アカウント作成
 - (2) アカウントの発行管理
 - (3) アカウントによるデータアクセス管理
4. ログオン及びユーザーセッションの管理
5. リモートアクセスの禁止

携帯型情報通信・記録機器の利用に係る要件

1. 目的

2. 対象

3. 利用要件

(1) 基本方針

(2) 技術要件

(3) 運用要件

(秘密取扱情報システム管理番号)

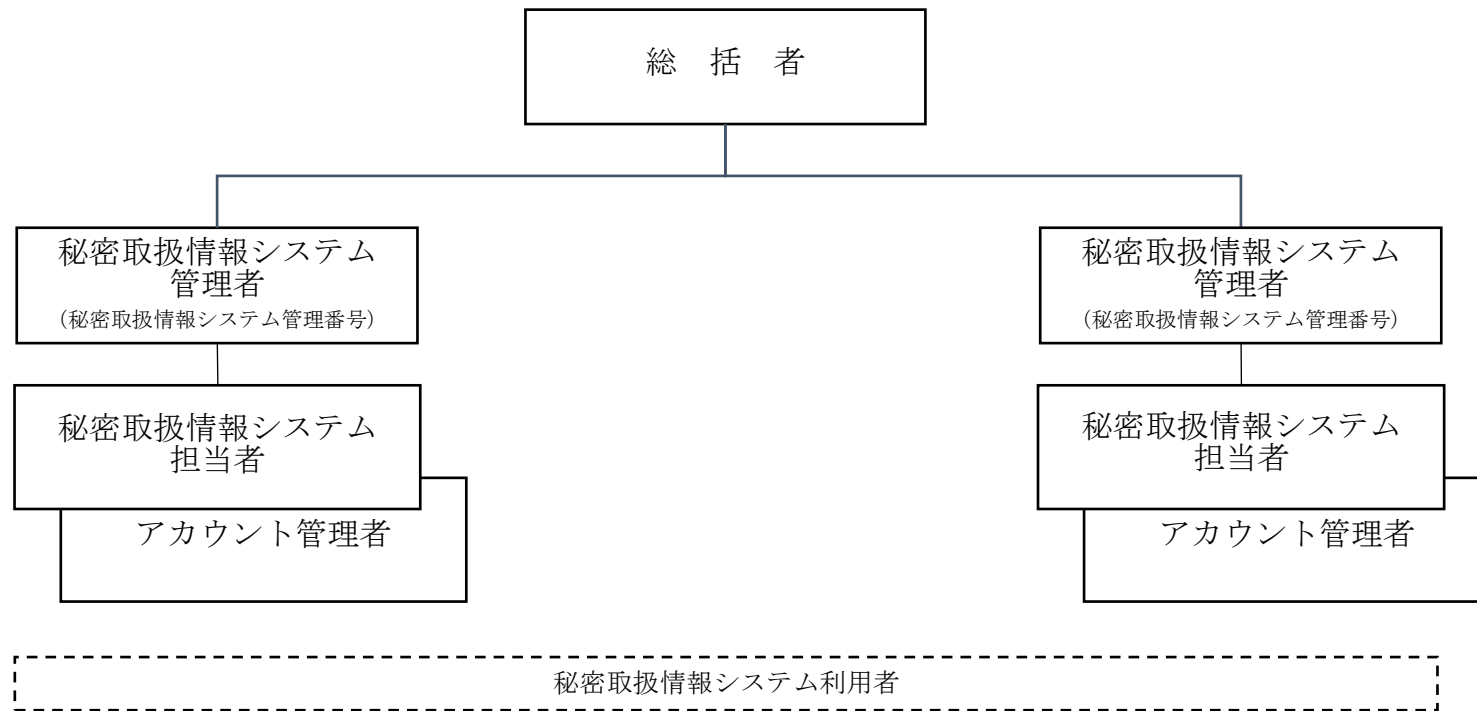
秘密取扱情報システムのセキュリティを確保するための組織体制（人員）

年 月 日現在

No.	保全体制における役職	所属	役職	氏名	着任日	秘密取扱情報システム （管理者、一般利用者の別）	責任及び役割
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

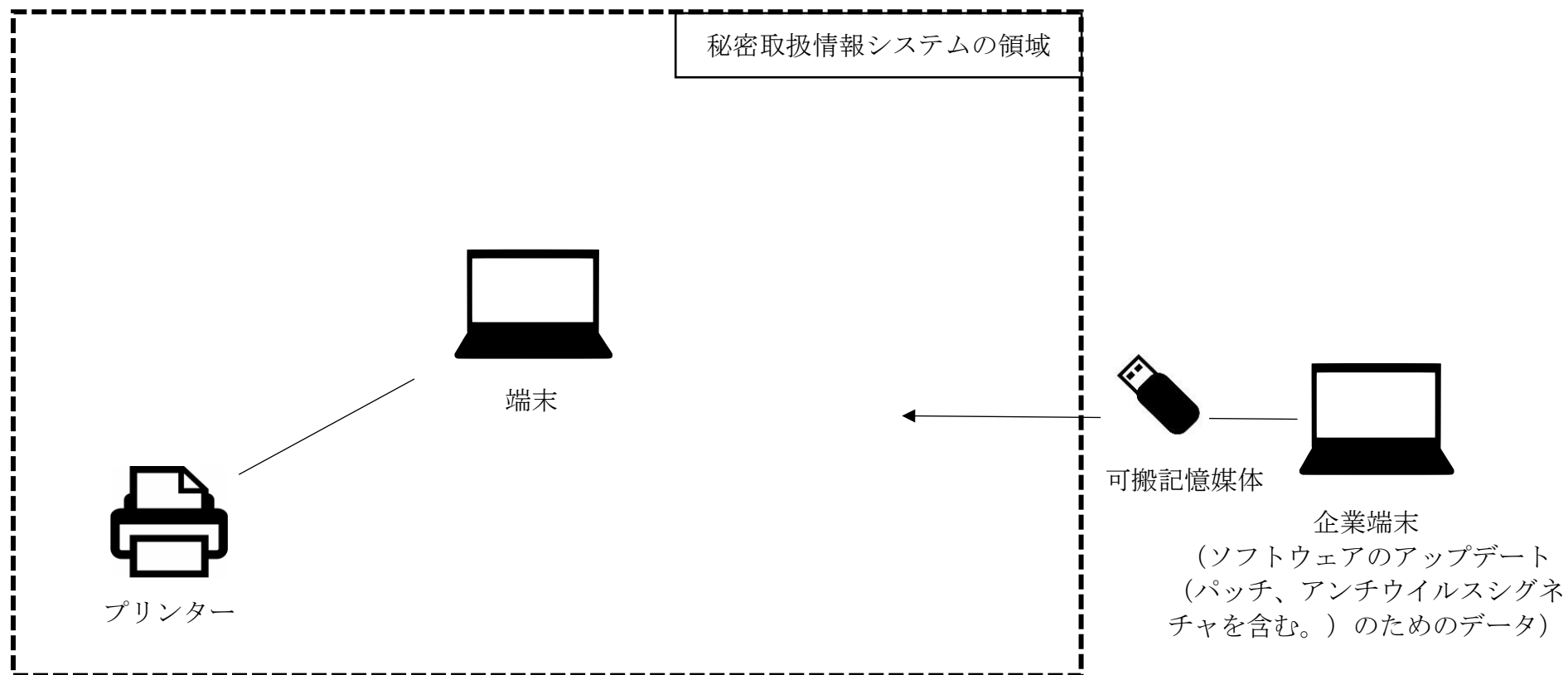
秘密取扱情報システムのセキュリティを確保するための組織体制（体制図）

年 月 日現在



(秘密取扱情報システム管理番号)

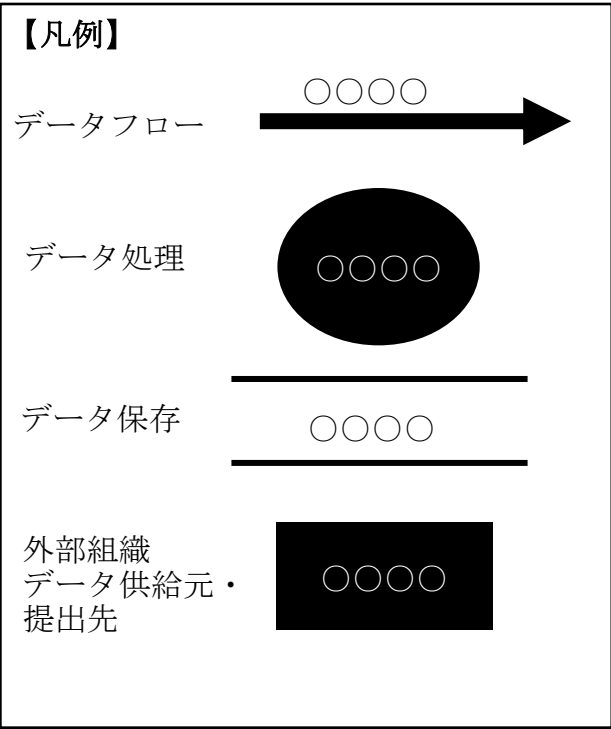
ネットワーク構成図



(秘密取扱情報システム管理番号)

データフロー図

業務概要	備考



(秘密取扱情報システム管理番号)

アカウント管理計画

1 目 的

2 アカウント区分及び利用可能権限

区 分※	利用可能権限	備 考

※役職名等は、秘密保全組織上の役職を記載する。

3 設定要領

識別子管理簿

（秘密取扱情報システム管理番号）

1 秘密取扱情報システム利用者

整理 番号	所属	氏 名	役職名等	識別子(ID)	設定日	秘密取扱シス テム管理者	失効日時	秘密取扱シス テム管理者	備 考

※役職名等は、社内における役職及び秘密保全組織上の役職を記載する。

(秘密取扱情報システム管理番号)

2 秘密取扱情報システム構成要素：品名又はホスト名：〇〇〇 (一件一葉で作成)

整理 番号	資産管理番号	識別子(ID)	利用者	設定日	秘密取扱シス テム管理者	失効日時	秘密取扱シス テム管理者	備 考

※ 1：1 年間以上使用されなかった識別子は無効化すること。

※ 2：無効化した識別子は再利用しないこと（2 年間）。

システムログ分析結果記録簿

(秘密取扱情報システム管理番号)

分析日	アラート件数			不審な挙動		秘密取扱情報 システム管理者	総括者
	低	中	高	概 要	対処必要性		

添付分析結果：

ぜい弱性スキャン分析結果記録簿

(秘密取扱情報システム管理番号)

年月 日	区 分	ぜい弱性スキャン結果		脆弱性の特定	処置方針	秘密取扱情報 システム管理者	総括者
		概要	詳細				

バックアップ実施等記録簿

(秘密取扱情報システム管理番号)

[illegible]

メンテナンス等計画

- 1 実施年月日
- 2 実施場所
- 3 秘密取扱情報システム管理番号
- 4 対象機器
- 5 作業区分（どちらかを○で囲む）
定期 ・ 臨時
- 6 実施者
 - (1) 監督者
 - (2) メンテナンス人員（秘密取扱システム利用者以外の場合はその旨を明記）
- 7 メンテナンス等の内容
 - (1) 実施概要、手順等
 - (2) メンテナンス等に使用する機器、ツール等
- 8 その他（メンテナンス等に付帯する作業について記載）

(秘密取扱情報システム管理番号)

メンテナンス等実施記録

実 施 日 時		
実 施 場 所		
対 象 機 器		
作 業 区 分		
実 施 者	監 督 者	
	メンテナンス人員※	
内 容	実施概要、手順等	
	メンテナンス等に使用した機器、ツール等	
その他		

※メンテナンス人員が指定された秘密取扱情報システム利用者以外の場合、事業者の名称及び所在、人員の名簿（国籍等を含む。）を記入する。

付紙様式第 38

発 簡 番 号

発 簡 年 月 日

防衛装備庁装備政策部装備保全管理課長 殿
(地方防衛局調達部長等 経由)

所 在 地

事業者名

代表者名

秘密取扱情報システムセキュリティ実装計画について

標記について、別添のとおり届け出ます。

記

- 1 防衛事業適合事業者契約年月日：
- 2 防衛事業適合事業者契約番号：

添付書類：秘密取扱情報システムセキュリティ実装計画

防衛事業適合事業者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に係る細部事項

第1 未適合下請負事業者による保護すべき情報の取扱いの確認（第3条第1項関係）

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（装装保第14846号。令和7年7月31日。以下「実施要領」という。）別紙第5防衛事業適合事業者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（以下「特約条項」という。）第3条第1項に規定する保護すべき情報の適切な取扱いに必要な事項の確認は、付紙様式第1の情報セキュリティ対策実施確認書により行うものとする。

第2 未適合下請負事業者による保護すべき情報の取扱いに関する承認（第3条第2項関係）

特約条項第3条第2項に規定する未適合下請負事業者による保護すべき情報の取扱いに関する承認の申請は、付紙様式第2により、乙に対する監査の協力の依頼を受けた地方防衛局調達部長等を経由して行うものとする。

第3 適合下請負事業者による保護すべき情報の取扱いの届出（第3条第6項関係）

特約条項第3条第6項に規定する適合下請負事業者による保護すべき情報の取扱いの届出は、付紙様式第3により、乙に対する監査の協力の依頼を受けた地方防衛局調達部長等を経由して行うものとする。

第4 保護すべき情報の第三者への開示に関する協議（第3条第7項関係）

特約条項第3条第7項に規定する保護すべき情報の第三者への開示に関する協議は、付紙様式第4により、当該第三者に関する情報、当該第三者が当該保護すべき情報を取り扱う理由、当該第三者がとる保全措置等を説明して行うものとする。

情報セキュリティ対策実施確認書

1 下請負事業者名又は開示先事業者名等

- (1) 事業者名：
- (2) 対象部門等名：
- (3) 請負又は開示予定年月日：
- (4) 業務の実施予定場所※：
※（下請負事業者又は開示先事業者の業務の実施予定場所を記入）

2 防衛省による情報セキュリティ実地監査の受査状況

※（本項目は該当無しの場合は省略可）

(1) 下請負事業者又は開示先事業者

- ア 監査年月日：
- イ 監査結果：
- ウ 監査結果の文書番号及び年月日：

(2) 下請負事業者又は開示先事業者の業務実施場所を管理する事業者（2（1）の下請負事業者又は開示先事業者と同じ場合は省略可）

- ア 監査年月日：
- イ 監査結果：
- ウ 監査結果の文書番号及び年月日：

3 下請負事業者又は開示先事業者に対する確認事項

番号	確認事項	評価	実施状況の確認方法 又は未実施の理由
情報セキュリティ基準			
1	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に従い『情報セキュリティ基本方針（基本方針）』、『情報セキュリティ規則（規則）』、『情報セキュリティ実施手順（実施手順）』が作成されていること。		
2	『情報セキュリティ基本方針等』の作成・周知について ①定めた手順に従い、情報セキュリティ基本方針等の定期的な見直しを行っていること。（適切/有効/妥当性の維持） ②定めた手順に従い、情報セキュリティ基本方針等を作成・変更した場合は、経営者等の承認、取扱者への周知を適切に行っていること。 ③定めた手順に従い、情報セキュリティ実施手順を社外の者にみだりに公開しないよう適切に管理していること。		
3	組織のセキュリティについて ①定めた手順に従い、情報セキュリティ体制を構築するとともに各職責を明示化し、情報セキュリティ管理策が適切に実施されていること。 ②定めた手順に従い、保護すべき情報を取り扱う下請負事業者の防衛省への届出、下請負者の情報セキュリティの確保状況を確認していること。		
4	保護すべき情報の管理について ①定めた手順に従い、保護すべき情報の授受、作成、制作、複製（バックアップ含む）、閲覧、持ち出し、返却、提出、廃棄を実施するとともに関係記録を保管又は保存していること。 ②防衛関連の情報を公開する場合は、定めた手順に従い、保護すべき情報が含まれていないことを確認していること。		
5	情報セキュリティ教育及び訓練について ①定めた手順に従い、定期的及び必要な場合に教育及び訓練を実施し、取扱者の意識及び能力向上を行っていること。 ②同教育に関する計画、実施記録等を作成し、保管又は保存していること。		
6	物理的および環境的セキュリティについて 定めた手順に従い、物理的及び環境的セキュリティ管理策を実施していること。 （例：取扱施設等、入退室管理機器、保護システム、保管された保護すべき情報の指定、管理等）		
7	保護システムの管理策の運用ルールを定めていること。		

8	情報セキュリティ事故等への対処及び対応について ①情報セキュリティ事故等対処計画を定め、事故等発生時に適切な処置の実施と、報告要領等を明確化し、取扱者等に周知していること。 ②情報セキュリティ事故等対処計画に基づく事故等対処テストを定期的の実施し、その記録を保管又は保存していること。		
9	リスク査定について ①リスク査定に関する手順を定め、保護すべき情報に関するリスクを特定、分析、評価を定期的の実施し、その結果を定められた者に周知していること。 ②リスク査定の分析結果、その対処に関する記録を保管又は保存していること。		
10	セキュリティ監査について ①定めた手順に従い、セキュリティ監査を計画的に実施し、その結果を定められた者に周知し、改善等の適切な措置を行っていること。 ②セキュリティ監査の計画、結果等の文書を作成し、保管又は保存していること。		
11	防衛省が監査を実施する場合、防衛省の求めに応じ必要な協力（施設への立入り、監査官による書類の閲覧等）を行うこととされていること。		
システムセキュリティ実施要領			
1	システムセキュリティ実装計画について 定めた手順に従い、『システムセキュリティ実装計画書』が作成、変更、承認、周知、及び保管又は保存されていること。		
2	構成管理について ①定めた手順に従い、保護システムのベースライン構成設定を定め、設定されていること。 ②定めた手順に従い、保護システムの構成設定目録が適切に作成・変更され、構成設定に関する記録が適切に保管及び保存されていること。		
3	保護システムの基本的防御について ①定めた手順に従い、保護システムの領域（範囲）が明確にされていること。 ②定めた手順に従い、保護システムの操作手順書が作成、変更、周知されていること。 ③定めた手順に従い、保護すべきデータが適切に暗号化されていること。 ④定めた手順に従い、暗号鍵の管理が適切に行われていること。 ⑤定めた手順に従い、保護システムへのソフトウェアインストール、アップデートが行われていること。 ⑥定めた手順に従い、保護システムにおけるアプリケーションの権限管理が適切に行われていること。 ⑦定めた手順に従い、仮想化システムに対して物理システム同様、各種管理策が取られていること。 ⑧定めた手順に従い、保護システムと外部システムとの接続及びその使用が制限されていること。		

4	アクセス制御について ①定めた手順に従い、保護すべきデータ及び保護システムに対する物理的・論理的なアクセス制御が適切に行われていること。 ②定めた手順に従い、アカウント管理者が指定され、アカウント管理(設定、変更、削除等)が適切に行われていること。 ③定めた手順に従い、保護システムへのログオン管理が適切に行われていること。 ④定めた手順に従い、保護システムの通信セッション管理が適切に行われていること。 ⑤定めた手順に従い、保護システムへのリモートアクセスが適切に行われていること。特に、リモートアクセス時の通信経路が暗号化されていること。		
5	識別及び認証について 定めた手順に従い、保護システムの識別及び認証が適切に行われていること。また、多要素認証が導入されていること。		
6	通信の制御について 定めた手順に従い、モバイルコード、VoIP、オフィス機器等の通信機能の利用が適切に制限されていること。		
7	システム監視について 定めた手順に従い、保護システムの内部及び外部境界に対する以下の項目の監視が適切に行われ、関連記録が適切に保管又は保存されていること。 ①不正な相手方又は方法等によるアクセス。 ②権限（管理者権限を含む。）の不正な使用。 ③内部及び外部との不正な通信。 ④悪意のあるコードの侵入。		
8	システムログについて 定めた手順に従い、保護システムのシステムログが適切に取得、分析、保存又は保管されていること。		
9	脆弱性スキャンについて ①定めた手順に従い、保護システムの脆弱性スキャンが適切に実施され、その分析結果に基づく措置が行われていること。 ②定めた手順に従い、脆弱性スキャンの実施に関する記録(脆弱性スキャンの分析結果等)が保管又は保存されていること。		
10	バックアップについて 定めた手順に従い、保護システムのサーバ及びパソコンに保存している全ての保護すべきデータ及び保護システムにおけるシステムデータについて、定期的にバックアップが行われ、当該データが適切に管理されていること。		

11	システムメンテナンスについて ①システムメンテナンス等計画が作成され、同計画に基づきシステムメンテナンスが適切に実施されていること。 ②定めた手順に従い、システムメンテナンスに係る記録が保管又は保存されていること。		
12	各種書類の作成・変更について、承認プロセスが定められ機能していること。		
13	保護システムの各種設定・設定変更について、承認プロセスが定められ機能していること。		
14	定めた手順に従い、各種書類・データ（記録文書データを含む）の保管・保存が適切に行われていること。また、必要がある場合は防衛省に提出していること。		
確認年月日：令和 年 月 日 確認者（企業名、所属、役職、氏名）：		総合評価	【コメント】

注：未実施の理由については、実施する必要が無いと認められる合理的な理由を記すこと。

「評価」、「総合評価」の項目については、装備品等及び役務の調達における情報セキュリティ監査実施要領について（装装保第4210号。令和5年3月14日）別紙第1に準じて記載するものとする。

文 書 番 号

発簡年月日

(契約担当官等)

殿

(地方防衛局調達部長等経由)

(防衛事業適合事業者)

未適合下請負事業者に保護すべき情報を取り扱わせる申請について

下記契約に係る「防衛事業適合事業者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」第3条第2項の規定に基づき、下記のとおり別添を添えて申請します。

記

1 取扱い先

会社名（事業者名）：

代表者名：

住所・電話番号：

業務の範囲：

2 取扱い理由

3 対象となる保護すべき情報

(1) 関連契約調達要求番号、契約品名、認証番号又は契約番号(年月日)、納期

(2) 保護すべき情報のリスト

4 取扱い先の保全措置

添付書類：1 情報セキュリティ対策実施確認書

2 (未適合下請負者における情報セキュリティ確保の確認結果を示す資料)

文 書 番 号

発簡年月日

(契約担当官等)

殿

((担当の監査官)経由)

(防衛事業適合事業者)

適合下請負者に保護すべき情報を取り扱わせる届出について

下記契約に係る「防衛事業適合事業者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」(以下「特約条項」という。)第3条第2項の規定に基づき確認したところ適切でしたので、特約条項第3条第4項の規定に基づき、下記のとおり別添を添えて届け出ます。

記

1 取扱い先

会社名(事業者名):

防衛事業適合事業者契約番号:

代表者名 :

住所・電話番号 :

業務の範囲 :

2 取扱い理由

3 対象となる保護すべき情報

(1) 関連契約調達要求番号、契約品名、認証番号又は契約番号(年月日)、納期

(2) 保護すべき情報のリスト

4 取扱い先の保全措置

添付書類: 適合下請負者の情報セキュリティ対策実施点検書

(契約担当官等)

殿

(防衛事業適合事業者)

第三者に保護すべき情報を開示する協議について

下記契約に係る「防衛事業適合事業者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」(以下「特約条項」という。)第 3 条第 7 項の規定に基づき、下記の第三者に保護すべき情報を取り扱わせたく協議します。

記

1 取扱い先 (第三者)

会社名 (事業者名) :

代表者名 :

住所・電話番号 :

業務の範囲 :

2 取扱い理由

3 対象となる保護すべき情報

(1) 関連契約調達要求番号、契約品名、認証番号又は契約番号(年月日)、納期

(2) 保護すべき情報のリスト

4 取扱い先 (第三者) がとる保全措置