

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 1 0 %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 1 0 %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 2 5 %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、その売上上の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１４．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１５．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１６．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１７．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９～１１参照）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１８．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		毎年度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100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100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 2 m 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 1 0. 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。								
第4. 錠	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。								
第7. 警戒・警報装置	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。								
	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。								
第8. 境界	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。								
	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)	(装備庁)		備考	
								現地調査 判定 ※ 4	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、及びせい弱性に対処し、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、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書を作成し、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 秘	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 1 4 - 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があった場合は、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：