防衛産業保全マニュアル

(Defense Industrial Security Manual)

2023 年 7 月

防衛装備庁

防衛産業保全マニュアル（DISM）の整備について

我が国を取り巻く安全保障環境は、力による一方的な現状変更やその試み等、一層厳しさを増しており、我が国も防衛力の抜本的な強化が求められています。政府は、昨年末に国家安全保障戦略等の３文書を閣議決定しました。３文書の中で、防衛生産・技術基盤は、装備品のライフサイクルの全てに関与し、装備品と防衛産業は一体不可分であることを踏まえ、防衛産業は、いわば「防衛力そのもの」と位置づけられました。本年６月には、防衛産業に対する様々な支援策等を盛り込んだ防衛生産基盤強化法が国会において成立しました。

他方、防衛産業は、サイバー攻撃を含む諸外国の情報活動などのリスクに晒されています。このような中で、防衛産業は、我が国の防衛上の秘密情報を適切に保護しながら自衛隊の装備品等の開発・生産・維持整備を行い、また、同盟国・同志国等の秘密情報を保護しながら防衛装備・技術協力に参画していく必要があります。防衛産業が、秘密情報を適切に保護すること、つまり「防衛産業保全」は、防衛生産及び防衛装備・技術協力の前提です。

また、防衛産業は、同盟国から導入した先進装備品の生産・維持整備や共同研究開発、防衛装備移転等、ますます国際化が進展しつつあります。これらの防衛産業の国際的な協力は、各国の秘密情報の円滑な共有が必要であり、「国際水準を踏まえた産業保全の強化」が前提となります。

これを踏まえて、本年、防衛装備庁は、参加国間の産業保全に関する手続き等の一定の標準化を図り、国際協力の円滑な実施に資することを目的とする「多国間産業保全ワーキンググループ（Multinational Industrial Security Working Group）」にアジア諸国としてはじめて加入しました。

そして今般、防衛装備庁は、諸外国の産業保全プログラムやその運用マニュアルに相当する「防衛産業保全マニュアル（Defense Industrial Security Manual）」を整備しました。本マニュアルは、防衛産業に適用される秘密情報の保護に係る法令、規則等に基づく防衛産業における情報保護措置を、一元的に整理したものです。

防衛装備庁としては、本マニュアルを国内の防衛産業に普及するとともに、同盟国・同志国等の政府・防衛産業にも共有し、防衛装備・技術協力を含めた防衛生産・技術基盤の強化を図って参ります。

防衛装備庁長官　土本英樹

目　次

本マニュアルは、２０２３年７月１日現在の規則等に基づき作成しました。それ以降の規則改正は反映していませんので、最新の規則等の確認をお願いします。

序章
防衛産業保全について

第１節　防衛産業保全

防衛産業保全とは、防衛省と自衛隊が使用する装備品等の研究開発、調達、補給若しくは装備品等に関する役務の調達に係る契約を締結した事業者（防衛産業）が秘密情報（Classified Information）を取り扱うに当たり、当該秘密情報の保護に必要な保全措置を講じることである。

我が国の防衛産業は、自衛隊の任務遂行に不可欠な装備品等ライフサイクルの各段階を担っており、いわば我が国の防衛力そのものであり、このような装備品等の秘密情報が事業者を通じて漏えいした場合、我が国の安全保障上の影響に加え、我が国に対する諸外国からの信頼喪失など深刻な影響が生じることになる。

また、我が国の防衛産業は、諸外国の情報活動等の脅威にさらされており、その手法はサイバー攻撃、ヒューミント等の多様な手法が想定されることや、事業者の従業者に限らず、秘密情報、システム、施設等の事業者におけるあらゆる資産に触れることのできる者の悪意、自己満足又は無意識により損害を引き起こされてしまう内部脅威などにも十分に留意する必要がある。

防衛産業保全マニュアルにおいては、我が国の防衛力そのものを構成する防衛産業における秘密情報の保護措置に関するルールを規定するものである。

第２節　国際水準を踏まえた防衛産業保全

防衛産業保全は、我が国の防衛の観点から秘匿する必要のある秘密情報を効果的に保護する必要があることと同時に、我が国の防衛産業の強化や国際協力と両立するために国際水準を踏まえた効率的な制度である必要がある。

つまり、防衛産業保全においては、諸外国の情報活動等から秘密情報を保護するための「安全性」を重視すると同時に、産業活動、防衛装備・技術協力等を円滑に実施するため、秘密取扱適格性（Personnel Security Clearance）を有し、かつ、知る必要（Need to know（「情報は知る必要のある者のみに伝え、知る必要のない者には伝えない」という原則））のある者に対して合理的かつ効率的に秘密情報を共有できる「合理性」も確保する必要がある。

このような観点から、防衛産業保全を実施していくにあたっては、先進諸国の間で

一般化している国際的な産業保全のルール、慣行等を踏まえた、「安全性」と「合理性」を同時に実現するルールの確立・運用をめざす。

第３節　防衛産業保全の規則と本マニュアル

防衛産業保全は、第１章で説明する秘密保全制度に基づいて構築されており、その根拠・関連法令は、特定秘密の保護に関する法律（平成２５年法律第１０８号。以下「特定秘密保護法」という。）、日米相互防衛援助協定等に伴う秘密保護法（昭和２９年法律第１６６号。以下「MDA 秘密保護法」という。）及び自衛隊法（昭和２９年法律第１６５号）等と多岐にわたっている。

防衛省・防衛装備庁内の産業保全に関する規則は、これらの複数の法律等を根拠にして、それぞれ対応する規則が制定され、複雑な規則体系となっている。本マニュアルは、防衛産業保全に関する複雑な規則体系を統一的な視点で整理し、可視化するために整備したものである。

また、本マニュアルは、標準的な防衛産業保全に関する措置を記載したものであり、装備品等の秘密情報の重要度等に応じて、追加的な保全措置を講じることは妨げない。

なお、本マニュアルが直接の対象とする範囲は、秘密情報を取り扱う契約の大半を占める防衛装備庁と防衛産業の契約に係る秘密保全である。陸海空自衛隊の整備補給部隊等と防衛産業の契約に係る秘密保全については、本マニュアルに準じて秘密保全措置がとられる。

第１章
秘密制度

第１節　はじめに

防衛省における秘密情報（Classified Information）は、特定秘密保護法に基づく「特定秘密」、MDA 秘密保護法に基づく「特別防衛秘密」、そして自衛隊法等により保護されている「秘」の３つの秘密により構成される（以下、特定秘密、特別防衛秘密及び秘を総称して「秘密情報」という。）。これらは国際的な秘密区分である TOP SECRET、SECRET、CONFIDENTIAL と実質的に同等である秘密区分に分類される。それぞれの対応については、一般的に下記の表のとおり。

防衛省の制度	国際的な秘密区分
特定秘密（機密）／特別防衛秘密（機密）	TOP SECRET
特定秘密／特別防衛秘密（極秘）	SECRET
秘／特別防衛秘密（秘）	CONFIDENTIAL

※ 上記の他、諸外国の「Restricted」の一部や「CUI (Controlled Unclassified Information)」等に相当する非秘密情報（Unclassified Information）であるものの管理を要する情報区分として「注意」及び「部内限り」がある。これらを事業者が取り扱う場合は、特約条項に基づき「保護すべき情報」として、保護措置が講じられる。

なお、特定秘密保護法に基づく「特定秘密」及び MDA 秘密保護法に基づく「特別防衛秘密」の保護は、各行政機関の長に権限・責任が与えられており、防衛省と防衛装備庁は、それぞれの法律の下に、関連する訓令等の関係規則を整備している。

このように、防衛省の秘密情報を取り扱う防衛産業の秘密保全は、上記の複数の法律の下で、複数の部内規則が制定されている体系となっている。

第２節　秘密保護法令

特定秘密保護法は、日本政府内の各省庁の共通の秘密保護制度であり、我が国の安全保障に関する情報のうち特に秘匿することが必要なものについての保護について規定しており、内閣官房が所管している。対象となる情報は、政府が保有する防衛、

外交、特定有害活動（スパイ行為等）の防止、テロリズムの防止に関する情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要であるものを指定しており、当該指定をした特定秘密文書等には「特定秘密」の表示をしなければならないとされている。

次に、「特別防衛秘密」は、日本国とアメリカ合衆国との間の相互防衛援助協定（昭和２９年条約第６号）等に基づき、アメリカ合衆国政府から供与された装備品等の構造又は性能、製作、保管又は修理に関する技術、使用の方法、品目及び数量に係る事項等であって、公になっていないものをいい、MDA 秘密保護法等に基づき秘密区分の指定、運用がなされており、特別防衛秘密文書等には特別防衛秘密に属し、かつ、機密、極秘又は秘のいずれかに区分されている旨の表示をしなければならないとされている。

最後に、「秘」は、防衛大臣又は防衛装備庁長官の定める秘密保全に関する訓令に基づき指定、運用がなされており、自衛隊法等により保護されている。対象となる情報は、国の安全又は利益に関わる事項であって、関係職員以外に知らせてはならないものを「秘」として指定しており、当該指定をした秘文書等には「秘密」の表示をしなければならないとされている。なお、「秘」は、実務上「省秘」や「庁秘」と呼ばれることもある。

第３節　契約に基づく秘密保護

防衛産業において、事業者が秘密情報を取り扱うためには、防衛装備庁と秘密区分に応じた特約条項を付した契約を締結する必要がある。

事業者は、当該契約を締結することにより、秘密保護に関する法令等に基づく義務が課されることとなり、適切な秘密保護措置を講じることとなる。

具体的には、秘密区分に応じた特約条項等に定められた保護措置に関する規定に従い、社内保全規則の作成、保全教育の実施、保全施設の設定、防衛装備庁の定期的な保全検査の受け入れ、システム上での取扱措置等を講じることが要求される。

なお、秘密保護契約は、製造請負契約などの有償契約のみならず、第４章で説明する無償の秘密保護契約も含まれる。

第４節　罰則と違約金

秘密情報の保護について、秘密情報の漏えいに関与した者に対する罰則として、特定秘密保護法、MDA 秘密保護法等の規定により最高１０年の懲役（刑法等の一部を改正する法律（令和４年法律第６７号）の施行日以後は「拘禁刑」となる。）が科される場合がある。

また、防衛装備庁は、事業者に対し社内保全規則に違反した従業者に対して懲戒の手続を備え、かつ、懲戒を確実に履行することを契約書に付属する秘密保全対策ガイドラインにより義務付けている。

更に、秘密情報を取り扱う契約には原則として違約金条項が付されることになっており、事業者が秘密情報を漏えいしたことを防衛装備庁が証明した場合、事業者は契約金額の最大６０％の違約金が科されることとなる。

第５節　秘密情報の取扱いの業務の終了に伴う措置

事業者は契約が終了した後、原則として直ちに防衛装備庁に秘密文書等（「文書」、「物件」及び「当該情報を化体する物件」を含む。）を返却し、又は提出しなければならない。また、事業者が秘密情報を漏えいした場合など、防衛装備庁が事業者に秘密等を取り扱わせることをやめさせることが適切であると認めた場合は、当該事業者に対して秘密文書等の返却その他必要な措置を指示し、当該事業者はその指示に従うことを義務付けている。

第２章
保全に関する入札資格審査（FOCI を含む）

第１節　入札前の確認

秘密情報及び保護すべき情報の取扱いが求められる契約について、入札手続に参加を希望する事業者は、入札に参加する前の段階において、外国の所有、支配、影響（Foreign Ownership Control or Influence：FOCI）の有無を含めて秘密情報を取り扱うのにふさわしい履行体制を確保すること及び履行に必要な情報を取り扱うのにふさわしい契約を履行する業務に従事する従業者を確保することに関し、防衛装備庁の確認を受ける必要がある。

また、入札に参加を希望する事業者は、入札前に次節に記述する書面の提出が必要である。

第２節　保全体制を確認するための提出書類

防衛装備庁は、前節で記述した理由により、入札日以前に提出期限を区切って、次に掲げる資料の提出を要求する。

１．契約の履行に関わる者の一覧表（氏名、役職、経歴、学歴、母語、国籍等）

２．資格のない従業者（取締役員等を含む。）が秘密情報にアクセスすることを禁じる社内規則（秘密契約を履行する事業者の組織の物理的又は組織的な分離及び資格のない者による不正アクセスの効果的な排除を含む。）

３．事業者に対し潜在的影響力を持つ外国を含む親会社又は他の事業者との契約関係及び資本関係

４．上記３で述べた親会社又は他の事業者に機微情報（秘密情報及び保護すべき情報）を共有しない証明

第３節　保全上の懸念が生じた場合の措置

防衛装備庁は、入札を希望する事業者から提出された資料に基づき、当該事業者の外国との関係、保全体制について、要求事項に適合しているか確認する。

防衛装備庁は、要求事項に適合しないと判断した場合は、保全体制を確立するために必要な規則の整備等の対応措置を講じさせる。これにより、当該事業者は要求事項に適合する必要がある。

仮に、要求事項に適合することが確認できない場合、当該事業者は、入札に参加することは認められない。

また、事業者は、第２節において提出した内容に変化が生じた場合は、契約履行途上においても再度、速やかに必要な書類等を提出しなければならない。

第３章
事業者秘密取扱適格性（Facility Security Clearance）

第１節　事業者秘密取扱適格性の申請

事業者が、秘密情報を取り扱うためには、事業者秘密取扱適格性(Facility Security Clearance：FSC)が認定されることが必要である。事業者秘密取扱適格性を認められた事業者を「秘密取扱適格事業者」という。

秘密情報の取扱いを希望する事業者は、事業者が所在する場所を管轄する地方防衛局を経由して、防衛装備庁へ申請を行い、同庁（装備保全管理課）の審査を受けた後、秘密取扱適格事業者と認定される。この申請は、原則として参加を希望する入札公告がなされた後に行うことができる。

事業者は、地方防衛局を通じて防衛装備庁（装備保全管理課）と事前調整を行うことができる。

なお、特定秘密については、法令に基づき、秘密取扱適格事業者のことを「適合事業者」といい、秘密取扱適格性の申請先は防衛装備庁装備政策部長となる。

また、事業者は、特定秘密、特別防衛秘密又は秘ごとにそれぞれ申請を行う必要がある。

第２節　申請内容

本節は、事業者が事業者秘密取扱適格性の申請において必要となる申請内容を規定する。

事業者が申請する必要がある内容は、総括者、秘密保全規則等、保全教育及び秘密保全施設である。

１．総括者（Facility Security Officer: FSO）

事業者秘密取扱適格性を申請する事業者は、秘密区分ごとに防衛装備庁が指定する保全措置を行う全責任を負う総括者を指名する必要がある。なお、特定秘密の総括者は、業務管理者という。

⑴　総括者の資格

総括者は、事業者秘密取扱適格性（FSC）を有する事業者の従業者であるとともに、当該事業者において取り扱う秘密区分に応じた秘密取扱適格性（PSC）を有することが必要である。また、総括者は、秘密の保護に関する業務を適切に行うために、防衛装備庁により承認された資料を用いた教育や自身の経験から得ら

れた必要な知識を有していることが必要である。さらに総括者は、防衛装備庁との契約の履行に関する事務を統括し、当該事業者における秘密の保護に関する業務の管理につき職責を全うできることが要求される。

⑵　総括者の職務

総括者の主な職責は以下のとおり。

・　秘密情報を取り扱う従業者を知る必要性（Need to know）に基づき選抜・配置すること。
・　当該従業者に保全教育を実施し、社内保全規則を遵守させること。
・　秘密保全施設における保護措置を講じること。
・　秘密情報を取り扱う情報システムに保護措置を講じること。
・　自己点検を行い必要な場合は是正措置を講じること。
・　地方防衛局が実施する保全検査に協力すること。

⑶　秘密保全組織

総括者は、秘密保全を確実に実施するため、実効性の高い秘密保全組織を設置し、社内の秘密保全を実施することが求められる。

そのため、総括者は、直接秘密情報を取り扱う設計・製造等を実施する部署に秘密保全組織を構築するほか、総括者を直接補佐し、社内の保全規則の作成や保全教育を実施し、社内監査を実施する専属の部署を設置する必要がある。

総括者は、直接秘密情報を取扱い設計・製造等を実施する部署等に、次に掲げる役職者として、第５章で説明する秘密取扱適格性（PSC）を有する者の中から任命する必要がある。

ア　管理責任者

管理責任者は、保全責任者を通じて取扱者を監督する。

イ　保全責任者

保全責任者は、取扱者を監督し、秘密情報を管理するための事務作業を実施する。

ウ　保全責任者代理（必要に応じ任命）

保全責任者代理は、保全責任者の不在時にその職務を代行する。

エ　取扱者

取扱者は、秘密情報に関わる作業（設計及び製造等）を実施する。

２．秘密保全規則等

事業者秘密取扱適格性を申請する事業者は、秘密保全規則及び秘密保全実施要領を作成することが義務付けられる（以下、秘密保全規則と秘密保全実施要領を総称して、「秘密保全規則等」という。）。

秘密保全規則等に事業者が記載すべき内容の詳細は、秘密情報の取扱いを含む契約の特約条項に添付され、その一部を構成する防衛装備庁の規則（保全に関する規則及び秘密保全対策ガイドライン）により規定される。

秘密保全規則に記載すべき主な項目は以下のとおり。

⑴　規則の制定に関する必要事項
⑵　秘密情報の取扱いに関する規則の不当な拡張解釈の禁止に関する規定
⑶　規則の解釈又は運用について疑義が生じた場合の協議に関する事項
⑷　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
⑸　秘密の保全等に関する規定
⑹　接受、保管、貸出及び閲覧等に関する規定
⑺　伝達、送達等に関する規定
⑻　保全状況検査、報告等に関する規定
⑼　複製、製作、写真撮影及び秘密情報の表示に関する規定
⑽　秘密情報の指定等に関する規定
⑾　下請負先の保全措置に関する規定
⑿　秘密保全施設等に関する規定
⒀　秘密文書等の返却及び廃棄に関する規定
⒁　非常時及び事故等発生時の対策及び報告等に関する規定
⒂　秘密保全規則の細部取扱いに関する規定

また、秘密保全対策ガイドラインに定めるところによる、事業者が作成する秘密保全実施要領の主な項目は以下のとおり。

⑴　目的及び考え方
⑵　用語の定義
⑶　適用範囲等
⑷　秘密保全規則等の取扱い
⑸　第三者への開示の禁止
⑹　組織のセキュリティ

⑺　特定資料又は特定物件の分類及び管理
⑻　人的セキュリティ
⑼　秘密漏えい等の事故発生時の対応
⑽　物理的及び環境的セキュリティ
⑾　通信及び運用管理
⑿　アクセス制御
⒀　検証・改善
⒁　検査及び調査の受入れ

3．保全教育

事業者秘密取扱適格性を申請する事業者は、関係社員（第5章に記載する秘密取扱適格性を有し、かつ知る必要性（Need to know）があるとして総括者が指定し、防衛装備庁の確認を得た従業者）に対し秘密情報に関する法令の内容、秘密文書等の取扱いの手続その他秘密情報の保全又は保護に必要な措置に関する知識を的確に習得できる保全教育を実施することが義務付けられる。

そのため、次の項目について作成し、申請する必要がある（具体的な内容は、第6章で説明する。）。

⑴　毎年定期的に保全教育を実施する人的・物的体制を整備していること、又はこれらを整備することができると認められること。
⑵　「保全教育用テキスト」の内容は秘密情報の保全又は保護に必要な内容であること。
⑶　講師が専門知識を有する者であること。

4．秘密保全施設

事業者秘密取扱適格性を申請する事業者は、契約を遂行するため秘密文書等を接受する場合は、秘密保全施設等を設置することが必要となる。これは、接受した秘密文書等が窃取や窃見されないようにすることが目的である。

事業者は、秘密保全施設を設置する場合、当該秘密保全施設の図面等（秘密保全施設の位置、構造等を詳細に記載したもので、その他必要な付属書類を含む。）を申請書に添付して提出し、許可を得る必要がある。

申請後、許可が得られるまでの間に、地方防衛局の保全検査官による現地調査が実施されるため、事業者はその調査に協力することが義務付けられる。

なお、秘密を取り扱う場所が官側施設のみである場合や元請事業者等の他所の秘

密保全施設で行う場合は、自社で秘密情報を取り扱わないため、秘密保全施設を設置する必要はない。

秘密保全施設の具体的な構造基準は、第１０章第２節で説明する。

第３節　審査及び結果の通知

前節の申請について、防衛装備庁における審査により、適当であると認められた場合は、防衛装備庁から申請した事業者に対し、秘密取扱適格事業者への認定の審査結果が文書で通知される。

この通知文書の発簡番号及び発簡日付は、その後の手続で必要となるため、事業者は適切に保管する必要がある。

第４節　変更について

秘密取扱適格事業者の認定を受けた事業者が、認定の前提となった規則等を変更するときは、改めて変更申請をする必要がある。特に、保全施設を変更する場合は、工事の着工前に、防衛装備庁による変更の承認を得る必要がある。

ただし、変更の理由が次に掲げる理由である場合は、申請によらず届出を提出すれば足りる。届出による変更の場合は、防衛装備庁からの許可を受けることは不要である。

⑴　防衛省又は防衛装備庁の訓令、通達等の改正等に基づく変更

⑵　事業所、部署、役職等の名称のみの変更

⑶　秘密の保全措置に影響を与えない変更

なお、会社の合併等若しくは事業所の統合又は移転の場合は、新規の申請又は変更の申請が必要となる。

第５節　新たな契約における手続について

事業者は、新たに締結する秘密情報を取り扱う契約において、既存の契約を通じて防衛装備庁から既に確認を受けた秘密保全規則等、教育資料及び秘密保全施設を使用する場合、あらためて申請する必要はなく、審査結果の通知の発簡番号及び発簡日付を届出れば足りる。

第６節　秘密保全施設の解除について

事業者は、防衛装備庁が確認した秘密保全施設を今後使用する見込みがない等の理由がある場合は、秘密保全施設指定の解除の届出をすることが認められている。

なお、一度解除した秘密保全施設を再度使用する場合は、あらためて申請をすることが必要となる。

第７節　秘密保全規則の見直しについて

事業者は、秘密保全に万全を期すため、秘密保全に係る社内の文書類、組織、秘密の管理状況、教育内容等の秘密保全を確保するための各種保護措置等について不断の検証を行い、状況に応じて必要な改善を行うことが必要となる。

なお、状況に変化が生じ、秘密保全規則等の見直しを行う際には、本章第４節に基づく規則等の変更の手続をとる必要がある。

第４章
秘密保護契約

第１節　保全措置の義務

第１章第３節で記述したように、防衛産業保全制度では、事業者は秘密保護に関する特約条項を付した製造請負等の契約に基づいて保全措置を行う義務を負うことになる。従って、契約日をもって保全措置が義務付けられる。

第２節　入札前の秘密文書の閲覧

装備品等の調達に係る入札等のため、当該入札等に参加しようとする事業者に対し、製造請負契約等の契約が成立する以前においても、秘密情報を含む仕様書等を開示することを許可する場合がある。

具体的には、秘密情報を含む仕様書の入札前の閲覧（閲覧内容の記録は許可されない。）は、事業者が、誓約書に秘密保全規則等を添付して提出し、防衛装備庁の許可を受けることにより可能となる。この誓約書は、秘密保護契約の一種であり、保全措置を講じることを義務付ける法的効果を有するものであり、仮に、当該秘密情報の漏えいが発生した場合は、民事上の責任が発生する。

また、秘密情報を閲覧できる事業者は、防衛装備庁が知る必要性（Need to know）により判断し、当該事業者は事業者秘密取扱適格性（FSC）を有し、閲覧する個人は秘密取扱適格性（PSC）を有する必要がある。これらの適格性を有しない事業者は、防衛装備庁に対して、第３章及び第５章の申請手続を行わなければならない。

第３節　製造請負等を伴わない無償の秘密保護契約

第２節の入札前の閲覧の他にも、防衛装備庁との製造請負等の契約が無い事業者が、防衛省・防衛装備庁の秘密情報を「知る必要性」がある場合は、防衛装備庁は、製造請負等を伴わない無償の秘密保護契約を締結して、当該事業者に秘密情報を取り扱わせることができる。ここでいう「無償」とは、防衛装備庁が事業者に対して契約の対価として金銭を支払うことはないという意味である。

この無償の秘密保護契約は、締結した事業者に対し保全措置を講じることを義務付ける効果を有するものであり、仮に、当該秘密情報の漏えいが発生した場合は、秘密区分に応じて刑事上、民事上の責任が発生する。また、秘密情報を取り扱う事業者については、防衛装備庁が知る必要性（Need to know）により判断し、当該事業者は事

業者秘密取扱適格性（FSC）を有し、秘密情報を取り扱う個人は秘密取扱適格性（PSC）を有する必要がある。これらの適格性を有しない事業者は、防衛装備庁に対して、第３章及び第５章の申請手続を行わなければならない。

第 5 章
秘密取扱適格性（Personnel Security Clearance）

第 1 節　秘密取扱適格性とは

秘密情報を取り扱う個人は、取り扱う秘密区分に応じた秘密取扱適格性（Personnel Security Clearance: PSC）を保有していることが必要である。秘密取扱適格性は、秘密情報を取り扱う契約の締結後に付与手続がとられる。

この秘密取扱適格性は、我が国が諸外国等と締結する情報保護協定において規定している、政府職員及び事業者の従業者が秘密情報にアクセスする際に必要となる「秘密情報取扱資格（Personnel Security Clearance）」と同一のものである。

秘密取扱適格事業者の従業者について、防衛装備庁における確認のプロセスを経て、秘密情報を取り扱わせるにふさわしい者として秘密取扱適格性を付与される。

個別の契約において、秘密情報にアクセスするには、秘密取扱適格性と、当該契約において秘密情報を取り扱う必要性（Need to know）が確認され、当該秘密情報の取扱いを許可された者として関係社員として名簿に登録される必要がある。

第 2 節　秘密取扱適格性の取得手続

秘密情報を取り扱う事業者の従業者に対する秘密取扱適格性の付与は、秘密保全対策ガイドラインに基づき、秘密情報を取り扱う契約が締結された後に、秘密情報を取り扱う必要がある従業者を記載する関係社員の名簿を作成する過程で行われる。

総括者は、当該契約に係る秘密情報を取り扱う必要がある従業者を関係社員の候補として選抜し、秘密取扱適格性を取得する手続をとらせる。

特定秘密を取り扱う従業者に対しては、特定秘密保護法及び特定秘密の指定及びその解除並びに適性評価の実施に関し統一的な運用を図るための基準（平成 26 年 10 月 14 日閣議決定。以下「運用基準」という。）に基づいて、特定秘密の秘密取扱適格性を付与するプロセスである適性評価を実施する。

適性評価の手続においては、特定秘密保護法及び運用基準に従って、特定秘密を取り扱う必要のある従業者が、質問票に必要な情報を記載した上で防衛装備庁に提出し、防衛装備庁（装備保全管理課）は適性評価を実施し、結果を当該従業者に通知する。

適性評価により適性を認められた従業者は、特定秘密の秘密取扱適格性を取得し、これを取り扱う必要性が確認された後、当該契約の関係社員名簿に記載されることと

なる。

特別防衛秘密及び秘を取り扱う契約においては、総括者が作成した関係社員の候補を記載した名簿に、候補となる従業者個人の特性等の情報を付した上で防衛装備庁に提出する。防衛装備庁は、提出された個人の情報に基づき、必要に応じて事業者を通じて追加情報の提出を求め、当該従業者の秘密取扱適格性の付与について判断する。

第３節　秘密取扱適格性の有効性

既存の契約により、有効な秘密区分に応じた秘密取扱適格性を得ている従業者は、同一の秘密区分の秘密情報を取り扱うことができるほか、新たな契約に携わる必要があると総括者が判断した場合は、防衛装備庁の確認を経た後に、新たな契約の関係社員名簿に掲載することが可能である。

また、総括者は、一度、秘密取扱適格性が付与され関係社員と認められた従業者であっても、人事面談等の機会を活用し、秘密情報を取り扱うにふさわしくない事情が職務の内外を問わず生じていないかどうかの確認を行わなければならない。秘密取扱適格性を付与された従業者は、自身における状況の変化を報告する義務を負う。

総括者は、保全教育において当該義務について従業者に認識させなければならない。また、一年に一度、従業者の上司により実施される人事面談等の機会を通じ、従業者個人の状況を継続的に把握し、当該事情が生じていることを把握した場合は防衛装備庁へ報告しなければならない。

第４節　関係社員の誓約

総括者は、関係社員が秘密情報を取り扱う前に、これを漏えいした場合の、秘密区分に応じた刑事及び民事上の責任に係る規定を含め、秘密保全に関する責任を明確にし、在職中及び離職後における秘密保全に係る誓約書を提出させることが義務付けられている。

従業者が秘密情報を取り扱う業務に従事することを望まない場合は、関係社員に指定することはできず、既に関係社員に指定している場合は、除外する必要がある。

第６章
保全教育の実施

第１節　秘密情報を取り扱う前の教育

総括者は、前章において説明した関係社員名簿について、防衛装備庁による確認を受けた後、関係社員に実際の秘密情報を取り扱わせる前に、第３章第２節第３項に基づき作成した保全教育用テキストに基づき、保全教育を受講させなければならない。

これは、契約履行中、採用、異動等により新たに関係社員に指定された者についても同様である。

第２節　定期的な教育及び訓練

総括者は、年に１回の保全教育を全関係社員に受講させなければならない。これは、前節の教育も含めて最低年に１回実施しなければならない。また、関係社員以外の全ての従業者に対して、定期的に必要な範囲の教育を行うこととされている。

また、その教育内容に基づいた訓練を事業所単位で実施しなければならない。

第３節　教育及び訓練の内容

総括者は、教育の実施について、次に掲げる全ての項目を実施しなければならない。

⑴　秘密情報に関する法律、政令、訓令、通達その他関係規則の条文及びその解説
⑵　秘密保全の必要性（漏えいによる国際的、国内的影響を含む。）
⑶　保全教育の意義・重要性
⑷　関係社員の役割及び責任
⑸　非常事態発生時の対処要領
⑹　秘密情報の取扱要領（接受、作成、伝達、閲覧、引継要領、検査要領、下請負要領等）
⑺　立入禁止区域の設定、管理、立入要領
⑻　電子計算機情報の保全要領
⑼　情報保全対策（諸外国の事例、カウンターインテリジェンスを含む。）
⑽　社内規則の確実な履行、隙のない勤務と私生活における慎重な行動
⑾　その他の留意事項（関係社員自身の状況の変化の自発的な報告を含む。）

また、教育においては座学に加え、実地による訓練（非常事態発生時の対処訓練等）を実施する必要がある。地方防衛局は、事業者における保全教育用テキストを防衛装備庁が規定する基準に基づき作成させる。事業者は、当該保全教育用テキストについて、地方防衛局を通じ防衛装備庁による承認を受けなければならない。

なお、防衛装備庁は、カウンターインテリジェンスを含む教育資料の提供等により事業者における教育の支援を実施する。

第４節　教育の記録

総括者は、本章第１節及び第２節に基づき実施した教育及び訓練について、その記録を残すほか、特約条項に基づき教育の実施状況を防衛装備庁に報告しなければならない。地方防衛局は、教育及び訓練の実施状況を保全検査において確認する。

第７章
秘密文書等の接受

第１節　秘密文書等の貸付申請

事業者は、契約締結後、前章までに記載した条件を満たした後、仕様書に記載のある貸付文書に関する秘密文書等の貸付申請を行うことができる。なお、申請先は、防衛装備庁となる。

貸付申請を受けた防衛装備庁は、秘密文書等を保有している機関等と調整の上、回答を行う。

第２節　接受

事業者は、秘密文書等の接受について、指定された関係社員に接受させなければならない。具体的には以下の手続を行う。

⑴　事業者が、秘密文書等を防衛装備庁から接受する際に、防衛装備庁から受領する秘密文書等と送付書の内容に相違がないか確認する。

⑵　その上で、事業者は受領書を防衛装備庁に提出する。

⑶　防衛装備庁は、当該事業者に貸し出した秘密文書等について、管理簿に記載する。

⑷　事業者は、当該秘密文書等を、自社の秘密保全施設まで持ち帰り、管理簿に記載する。

⑸　事業者は、接受した秘密文書等を自社の秘密保全施設内に運搬した後、保全責任者が秘密文書等と送付書を照合するなど異常の有無を確認した上で、防衛装備庁へ接受の報告をする。

第３節　秘密文書等の運搬

前節で接受した秘密文書等は、接受した関係社員が事業者の秘密保全施設まで運搬する必要がある。特定秘密及び特別防衛秘密の場合は、２名以上で行う必要がある。

秘密文書等は、当該秘密文書等の秘密区分が表示された不透明の封筒に封かんし、さらに、その封筒を、秘密区分が識別できるような表示をしていない封筒に封かんしなければならない。輸送する間は、この２重封筒を施錠することのできる運搬容器（外側から内側を視認できない物に限る。）を用いて携行する必要がある。

上記により難い場合は、あらかじめ防衛装備庁の許可を得て、他の方法によること

ができる。

なお、秘密文書等を事業者の保全施設以外の場所（下請負事業者の秘密保全施設等）へ送達する場合は、仕様書等に記載がない限り、防衛装備庁の事前の許可が必要となる。

第４節　秘密物件の輸送

事業者が、秘密物件を輸送する場合において、秘密物件の寸法や重量、その他の性質により封筒の使用が不可能なときは、漏えいを防止するよう包装を厳重にする等の措置を講じなければならない。

また、寸法や重量、その他物理的な性質により民間輸送業者を使用する必要がある場合、事業者は防衛装備庁の許可を得なければならない。

この際、秘密物件が梱包され、その秘密情報の内容を知り得ない状態で民間輸送業者に引き渡される場合は、民間輸送業者は秘密情報を取り扱わない。この場合、輸送の際は、事業者の関係社員を同行させる必要がある。これは、事故等で梱包が破損し秘密物件が暴露した場合に対処する必要があるためである。

民間輸送業者が秘密物件を梱包する等により秘密情報に接する可能性がある場合は、民間輸送業者は秘密取扱適格事業者である必要がある。この場合、民間輸送業者の関係社員が輸送を行うのであれば、事業者の関係社員が輸送の際に同行する必要はない。

第５節　秘密文書等の保管

事業者が、秘密文書等を受領した場合は、自社の秘密保全施設内にある保管容器に保管しなければならない。

また、事業者の保全責任者は、可能な限り秘密文書等を集中保管する必要がある。

なお、秘密物件で、保管容器に格納できない場合等は、保管庫に保管する必要がある。

秘密保全施設、保管庫、保管容器の基準は、第１０章第２節で説明する。

第６節　秘密文書等の共用

事業者が、現に自社の秘密保全施設内に保管している秘密文書等を、他の契約で使用する必要がある場合、共用の手続をとることができる。この手続は、できる限り秘密文書等の複製物を増やさず、同じ秘密文書を複数の契約で使用する必要がある場合は、共用して用いた方が秘密保全に資するとの考えに基づいている。

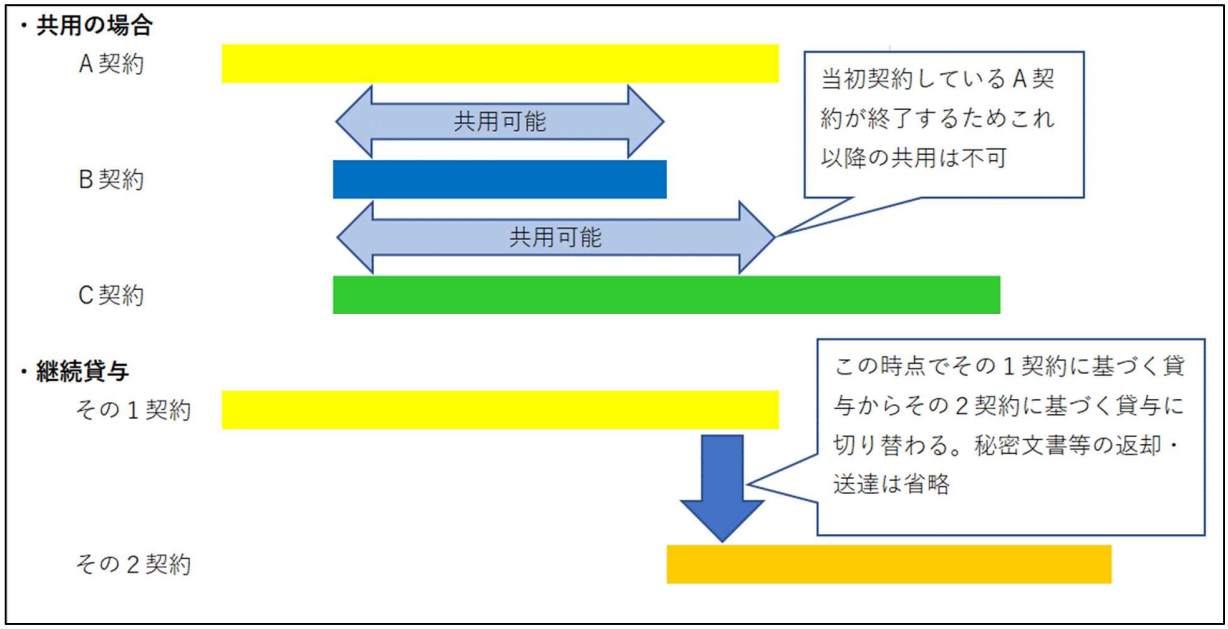
共用は、事業者からの申請を受けた防衛装備庁が、当該秘密文書等の管理者等と調整を実施し同意を得た場合のみ実施することができる。なお、この共用手続は、当初契約の履行期間内のみでしか実施することができない。

第７節　秘密文書等の継続貸与

事業者が、例えば同一事業のその１、その２契約や毎年ほぼ同一内容の契約（量産及び機体定期修理等）を結んでいる場合など、継続貸与の手続をすることにより、当初の契約終了後に秘密文書等を防衛装備庁へ返却又は提出せずに、引き続き使用することができる。

これは、手続のためだけに事業者の秘密保全施設から秘密文書等を運搬することは秘密保全上リスクがあるため、このリスクを減らすために規定されているものである。

【共用と継続貸与の比較】



第８章
秘密文書等の閲覧・貸出

第１節　秘密文書等の閲覧

事業者は、特定の事業における秘密情報を取り扱う従業者について、防衛装備庁により承認された事業ごとの関係社員名簿に記載しなければならない。

事業者は、自社の秘密保全施設内で保管している秘密文書等を関係社員に閲覧させる場合、閲覧をしようとする者が当該秘密情報を取り扱うことのできる関係社員（秘密取扱適格性を有し、知る必要性があり、当該秘密情報の取扱いが許可された従業者）であること及び契約履行上、閲覧の必要があることを確認しなければならない。

この際、当該閲覧する関係社員に対して、閲覧記録簿に必要事項を記載させるとともに、事業者の保全責任者が前述の確認を行い、確認した旨を閲覧記録簿に記載する必要がある。

また、閲覧は、秘密文書等が保管されている秘密保全施設内で行わなければならない。それ以外の秘密保全施設で閲覧する場合は、次節の貸出の手続を併せて行う必要がある。

なお、下請負事業者等自社以外の関係社員に閲覧させる場合も、本節の手続が必要となる。

第２節　秘密文書等の貸出

事業者は、自社の秘密保全施設内で保管している秘密文書等を保管している秘密保全施設以外の秘密保全施設に持ち出す必要がある場合、貸出の手続を行わなければならない。

事業者は、文書等を関係社員に貸し出す場合、貸出を受ける者が当該秘密文書等を取り扱うことのできる関係社員であること及び契約履行上、貸出の必要があることを確認しなければならない。

この際、当該貸出を受ける関係社員に対して、貸出記録簿に必要事項を記載させるとともに、事業者の保全責任者が前述の確認を行い、確認した旨を貸出記録簿に記載する必要がある。

なお、下請負事業者等自社以外の関係社員に貸出する場合も、本節の手続が必要になる。

第３節　秘密情報の伝達

事業者は、関係社員同士が秘密を伝達する場合は、秘密保全施設内で行わせる必要があるほか、その始めと終わりに伝達する内容が秘密情報であることを明らかにするとともに、筆記又は録音を禁止する等必要な措置を講じなくてはならない。

また、事業者は、関係社員が、秘密保全施設以外の公共交通機関や公共の場での会話又は電話などで、秘密情報へ言及することを禁止するよう徹底する必要がある。

第９章
秘密文書等の作成及び表示

第１節　作成の申請及び登録番号の付与

事業者は、秘密文書等を作成又は複製（以下「作成等」という。）しようとするときは、防衛装備庁にあらかじめ申請し、許可を得なければならない。この際、秘密文書等の作成等の範囲及び数量は必要最小限度にしなければならない。

ただし、契約書の仕様書に秘密文書等の作成等の記載がある場合は、あらかじめ許可を得ていることになるため申請は不要である。

また、事業者は防衛装備庁に作成等した秘密文書等に記載する登録番号等の付与を受けなければならない。

第２節　作成時の官側の立会

事業者は、秘密文書等を作成等する場合は、秘密保全施設内で実施しなければならないほか、防衛装備庁（地方防衛局の保全専門官等）の立会が必要となる。そのため、作成等する場合は事前に官側とよく調整する必要がある。

第３節　作成中の取扱い

事業者は、作成等の途中の文書等で、その作成等の完了後、秘密に指定されることが予想される文書等については、秘密文書等と同等に取り扱わなければなければならない。

また、分析等に時間がかかるなどの理由で、秘密文書等の作成に長時間かかる場合であって、官側による指示があるときには、作成中の段階での前節の防衛装備庁（地方防衛局の保全専門官等）の立会は不要である。

ただし、最終的に秘密文書等の作成を終える段階では、前節の防衛装備庁（地方防衛局の保全専門官等）の立会が必要となる。

第４節　秘密区分の表示

事業者は、作成等した秘密文書等に、秘密区分に応じた表示を行わなければならない。

表示は、「特定秘密」、「特別防衛秘密（機密）」、「特別防衛秘密（極秘）」、「特別防衛

秘密（秘）」、「秘」のいずれかになる。どの表示を行うかは、仕様書又は官側の指示に従って行うこととなる。

秘密文書等の場合は、秘密を記載しているページに加え、表紙及び裏表紙のそれぞれ右上及び左下に赤色で表示する必要がある。また、何が秘密情報なのかを明示した表示を行う必要がある。例えば、文書の一部分であれば下線部を引く又は○や□で囲うなど、挿絵、写真、図又は表などの場合は外周を赤枠で囲うなど、表内が秘密であることを明記する等の記載が必要である。

秘密物件の場合は、適宜の場所に記載する必要がある。また、秘密文書等又は秘密物件への表示が物理的に不可能な場合は、秘密区分の通知書類を、取り扱う関係社員等に交付又は閲覧させて周知する必要がある。

なお、当該秘密情報が外国政府由来の場合、秘密区分の表示に加え、当該外国政府の表示も併せて行う必要がある。

第５節　登録番号及び一連番号等の表示

事業者は、本章第１節で指示を受けた登録番号、一連番号、枚数及び指定条件を、文書であれば表紙左上に、それ以外の場合は適宜の場所に表示する必要がある。

特定秘密の場合は、上記に加え、特定秘密の指定の整理番号を表示する必要がある。

登録番号により、当該秘密を指定した部署又は当該秘密文書の作成に責任を負う部署が明らかになる。

第６節　秘密区分等の表示の変更

事業者は、防衛装備庁から書面による指示があった場合は、秘密区分及び指定条件（以下この節において「秘密区分等」という。）の表示の変更を行わなければならない。

また、防衛装備庁の秘密文書等の管理者の判断により、秘密区分等の表示の変更を秘密文書等の管理者で行うために、秘密文書等の返却を指示した場合は、その指示に従い秘密文書等を防衛装備庁へ返却しなければならない。

第７節　秘密文書等の作成途上の反古紙等の廃棄

事業者は、秘密文書等の作成等のために一時的に作成した反古紙等で、実質的に当該秘密の内容を含むものは、これらが探知され、又は収集されることのないよう注意

し、廃棄及び保管について、秘密に準じた取扱いをするものとする。

　なお、廃棄に当たっては、秘密文書等を廃棄する方法と同様に秘密情報の内容を推測されないように実施しなければならない。

第１０章
秘密保全施設

第１節　秘密保全施設

事業者は、秘密情報を取り扱う際には、秘密保全施設で取り扱わなければならない。また、秘密保全施設とは、秘密文書等を保管容器に格納する秘密保全施設のほか、機能試験等で秘密情報を取り扱うため期間を定めて設定する閉鎖区域、秘密物件が保管容器に保管できない場合に設置する保管庫又は金庫室を総称するものである。

第２節 秘密保全施設の構造基準

秘密物件を保護するための秘密保全施設の構造基準は、以下のとおり。

また、閉鎖区域の構造基準は、秘密保全施設の構造基準を基本的に準用するが、同等以上の保護措置をとることで代替措置を講じることができる。代替措置については、施設の特色により個別に検討する必要があり、防衛装備庁の承認を受けなければならない。

１．天井、壁、床

原則として、鉄筋コンクリート又は頑丈な不燃性の資材で堅固に建造する必要がある。また、天井裏が他の部屋の天井裏と接続している場合は、その境界部を金網等の頑丈な不燃性の資材を用いて遮断しなければならない。

２．間仕切り

扉を開けたときに内側が視認できる場合は、衝立若しくはカーテン等を設置しなければならない。

３．出入口

出入口は、原則１カ所とする必要があり、出入口の扉の上部に停電時にも機能する照明装置（常夜灯）を設置しなければならない。なお、機材の搬入・搬出ができない場合は、別途、搬入口を設けることができる。

また、脱出口が必要な場合は、内側からの開閉を可能とする措置を講じた非常口を設けることができる。

4．扉及び錠

出入口、搬入口、非常口の扉は、原則として鋼鉄製である必要がある。また、両開きの場合は、扉の合せ目に定規縁が必要である。

また、覗き窓を必要とする場合は、内側からのみ覗くことができるようにする必要がある。

出入口及び搬入口は、三段式文字盤かぎ（交換数１００の３乗以上）及び差し込み式かぎ等による二重施錠方式、又はそれ以上の保護措置を講じる必要がある。例えば、三段式文字盤かぎに代えて静脈認証の電子錠にする等の要領がある。

なお、非常時にすぐに脱出できるようにするため出入口には非常開閉装置が必要である。

5．窓

原則として、設置できない。ただし、窓を設置する場合又は施設の構造上窓が設置されている場合には必要最小限にとどめて、鉄格子（日本産業規格、鉄棒直径１３ｍｍ以上、間隔１０ｃｍ以下）を設置する必要がある。また、窓ガラスは、金網入り不透明なものとするか、不透明なものになるような措置を講じる必要がある。

6．開口部

ダクト、通風調節装置、天窓、下水溝、トンネル等の開口部は、大きさ、形状から不法侵入、盗見又は盗聴のおそれがある場合には、金網を取り付けるか鉄格子（日本産業規格、鉄棒直径１３ｍｍ以上、間隔１０ｃｍ以下）を取り付けなければならない。

7．警報装置

停電時でも作動する扉の開閉及び侵入を感知する自動の警報装置を警備室等に直結して取り付けなければならない。この際、配線は容易に切断されないように留意するとともに、配線切断時は、配線が切断された旨の警報を発するようにする必要がある。

8．外柵

外部から秘密保全施設への不法侵入を防止し得るように基礎をコンクリートで

固定し、対象物に応じ、高さ２ｍ以上の強度の金網等を用いて周囲を囲み、その上部には有刺鉄線、赤外線装置等を取り付ける必要がある。

この外柵は、秘密保全施設の建物又は秘密保全施設の建物が含まれる事業所等の敷地全体の周りのどちらかに設置しなければならない。

また、秘密情報を保全するための代替措置を講じた場合は、外柵を設置しないことができる。代替措置の内容については、施設の特色を踏まえ個別に検討し、防衛装備庁の承認を受けなければならない。

９．保管容器

秘密文書等は、秘密の種類及び区分に応じて、特定秘密は三段式文字盤かぎとさし込み式かぎを併用した金庫又は鋼鉄製の箱、特別防衛秘密及び秘は三段式文字盤かぎのかかる金庫又は鋼鉄製の箱にそれぞれ保管する必要がある。

容器の外側には、秘密文書等の保管容器として承認されていることがわかるような表示はできない。

１０．「保全外部区域」の設置

秘密保全施設への不正な立入を阻止するため、秘密保全施設の外側に「保全外部区域」を指定し、その区域への立入を厳格に管理する必要がある。

第３節 秘密保全施設の管理

事業者は、秘密保全施設を適切に管理するため、次に掲げる措置を実施する必要がある。

１．秘密保全施設の営業日における点検

事業者は、全ての秘密資料及び秘密保全施設が適切に保全されていることを確実にするために、営業日ごとに保管場所に異状が無いか確認を実施しなければならない。

２．秘密保全施設及び保管容器の鍵の管理

秘密保全施設及び保管容器の鍵は、勤務時間中は、総括者の許可を受けた者によって確実に管理し、勤務時間外については、警備員室等に設置された鍵保管容器等

で保管する必要がある。

また、鍵保管容器の鍵は、総括者の許可を受けた者によって確実に管理する必要がある。

なお、鍵の管理又は使用者は、必要最小限度としなければならない。

総括者は、潜在的なリスクを低減させるため、以下の例を含む適切な措置を講じるよう努めなければならない。

・マスターキーの作成を禁止すること
・鍵の複製に係る手続の確立
・保管されている秘密文書等と同等の保護を鍵に対して与えること
・定期的な鍵の監査
・鍵の管理者の変更時における鍵の全数確認

3．保管容器の暗証番号の管理

保管容器に暗証番号を付与できる場合、その暗証番号は、必要最小限の総括者の許可を受けた関係社員が管理する必要がある。なお、保管容器の暗証番号を管理する関係社員と保管容器の鍵を管理する関係社員は、同一の関係社員とすることはできない。

これは、単独で秘密文書等を窃取又は盗見することを防止するためである。

暗証番号は、少なくとも年に1回及び次に掲げる場合に該当するときは変更する。

⑴　保管容器として最初に使用するとき。
⑵　暗証番号を知る関係社員が退職又は異動するとき。
⑶　暗証番号の漏えい又は漏えいの疑いがあるとき。

4．秘密保全施設の保守管理

秘密保全施設で保守管理を行うために関係社員以外の者が立ち入る際は、第１２章の立入手続を事前に行う必要がある。

第１１章
秘密を取り扱う情報システム

第１節 情報システムに関する規定

秘密情報の作成又は取扱いに使用する事業者の情報システムは、秘密情報を漏えいしないように、適切に管理しなければならない。

情報システムの主な規定は、次のとおりである。

１．人的セキュリティについて
２．物理的及び環境的セキュリティについて
３．通信及び運用管理について
４．アクセス制御について
５．検証・改善について

第２節 人的セキュリティ

１．情報システムの利用者

事業者は、秘密情報を取り扱うシステムの利用者の指定の範囲を必要最小限とするとともに、ふさわしい者を充て、秘密保全規則等を遵守させなければならない。

２．悪意のあるソフトウェアへの感染防止対策等の教育について

事業者は、可搬記憶媒体を介して悪意のあるソフトウェアが感染するリスクがあることを関係社員に認知させ、情報システムに適切なセキュリティ対策が講じられるように定期的に必要な範囲について教育を行い、その結果を記録しなければならない。

第３節 物理的及び環境的セキュリティ

１．情報システム実装計画書

事業者は、秘密情報を情報システムで取り扱う場合は、情報システム実装計画書（以下「実装計画書」という。）を作成し、必要に応じ更新しなくてはならない。

実装計画書には、次に掲げる項目を記載することが必要である。なお、この実装計画書は、毎月の保全検査の対象となる。

⑴　秘密情報を取り扱う情報システムを構成する構成要素の構成設定に係る現状を正確に確認及び証明するための目録

秘密情報を取り扱う情報システムを構成するハードウェア、ソフトウェア、ネットワーク及び記憶媒体の機種、バージョン等の現状を正確に確認及び証明するために目録を作成しなければならない。

⑵　操作手順

事業者は、秘密保全施設内で使用する情報システムに関する操作手順を作成し、情報システムを取り扱う関係社員が常時参照できるように整備する必要がある。

⑶　アクセス制御方針

事業者は、関係社員が取り扱うことができる秘密情報の種類及び関係社員の役職等に応じた情報システムの利用可能機能等をアクセス制御方針として規定しなければならない。

⑷　秘密情報のデータのデータフロー図

事業者は、秘密情報を取り扱う情報システム内で秘密情報のデータのデータフロー図を作成しなければならない。このデータフロー図は、秘密データが立入禁止区域外にでないかを確認することを目的として作成するものである。

⑸　秘密情報を取り扱う情報システムのセキュリティを確保するための組織体制図

事業者は、秘密情報を取り扱う情報システムのセキュリティに責任を有する者を確認できるようにするため、具体的な責任の内容及びその範囲を記載する組織体制図を作成する必要がある。

⑹　その他必要な事項

⑴～⑸で作成した資料において、情報システムのネットワーク内の秘密データが保全施設外に出ていないかについて確認できない場合は、追加で資料を作成する必要がある。

２．情報システムの持ち出しについて

秘密情報を取り扱う情報システムは、原則として秘密保全施設に常設し、持ち出

しを禁止するとともに、不正な持ち出しを防止するために必要な措置を講じなければならない。例えば、情報システムの修理や処分するためにやむを得ず秘密保全施設から持ち出すときは、記憶媒体を物理的に破壊する等秘密情報の漏えいを防止するための措置が必要である。

情報システムの不正な持ち出しを防止するための具体的措置としては、情報システムをセキュリティワイヤで固定するほか、秘密保全施設で修理する際は総括者が指定する関係社員が監視するなどの措置をとらなければならない。

また、秘密情報の漏えいを防止するには事業者の業務内容等の実情・実態に即した保護措置を講じていくことが重要であり、例えば秘密保全施設の出入りの際に必要に応じて所持品検査を実施すること等の対策が必要になる。

3．秘密保全施設への情報システムの持込みについて

秘密保全施設には、常設している情報システム以外の携帯型通信機器等の持込みを原則として禁止しなければならない。やむを得ず持ち込む場合は、秘密情報の漏えいを防止する措置を講じ、記録簿に所要事項を記録し、持ち込む携帯型通信機器が私有品でないことを確認した上で、総括者が許可する必要がある。

第4節 通信及び運用管理

1．通信について

秘密情報を取り扱う情報システムは、スタンドアローンとして使用するか、ネットワークに接続する場合は、秘密保全施設内において有線で配線接続する場合に限り構築でき、秘密保全施設外のいかなるものとも原則として接続してはならない。また、保全区画内においてワイヤレスネットワーク接続（ワイヤレスキーボード、ワイヤレスマウス等）の使用は禁止しなければならない。

2．情報システムにインストールするソフトウェアについて

秘密情報を取り扱う情報システムには、業務に必要なソフトウェアのみ使用し、悪意あるソフトウェアから秘密情報を保護するため、最新のウィルス対策ソフト等を用いて、悪意あるソフトウェアを検知するなどの対策を行わなければならない。

3．情報システムのメンテナンス等について

事業者は秘密情報を取り扱う情報システムのメンテナンス等（保守、点検、診断、修理、整備及びアップデートを含む。）を定期的及び必要に応じ実施するため、メン

テナンス等計画を作成し、その計画に基づきメンテナンス等を実施する必要がある。メンテナンス等計画には、メンテナンス等を実施する人員、対象、内容、その他必要な事項等を含める必要がある。

実際にメンテナンス等を実施する際は、総括者又はその指定する関係社員が、立会い及び必要な監視を行うとともに、メンテナンス等を実施した日時、人員の名簿、実施の対象及び内容を記録しなければならない。

4．情報システムのメンテナンス等の外部委託について

秘密情報を取り扱う情報システムのメンテナンス等を秘密取扱適格事業者以外への外部委託は原則として禁止している。やむを得ず秘密取扱適格事業者以外への外部委託をしなければならない場合は、外部委託先に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、秘密保全施設への立入りは事前に地方防衛局が許可した者に限ること、外部委託先が秘密情報に接触することがないように措置する対策を講じなければならない。

5．可搬記憶媒体の取扱いについて

事業者は、秘密情報を電子情報として取り扱う場合、原則として可搬記憶媒体へ保存しなければならない。

事業者は、可搬記憶媒体の取扱いに関する管理手順を作成し、関係する関係社員へ周知する必要がある。管理手順には、可搬記憶媒体を関係社員が使用する場合は、総括者又はその指定する者がその都度許可を与えること、貸出・返却に関する記録を残すこと、可搬記憶媒体へ情報を保存する場合は、電子政府推奨暗号等を使用して秘匿し、その暗号鍵は厳格に管理すること、可搬記憶媒体の内容の複製及び破棄手順に関することを記載しなければならない。

第5節 アクセス制御

1．アクセス制御方針の作成

事業者は、情報システムのアカウント管理者（アカウントの設定、変更及び削除等を行う者）を指定すること、情報システムの利用者ごとに業務遂行上必要最小限度の機能及び権限となるようアカウントを管理すること、情報システムを構成する機器の識別及び情報システム利用者の認証に関することを定めたアクセス制御方針を作成しなければならない。

２．利用者ＩＤの設定

事業者は、情報システムを取り扱う関係社員ごとに利用者ＩＤを保有させ、関係社員自身でパスワードを設定させる必要がある。これは、次項で説明する情報システムの使用状況を記録する際、各利用者を識別するためである。

上記に加え、ログオン試行回数の上限を設定し、それを超える回数を失敗した場合は自動的にロックし、一定時間再試行できないように設定するとともに、非アクティブ状態であり続ける上限時間を定め、それを超える場合にはユーザセッションをロックするように設定する必要がある。

３．情報システムの使用状況の記録

事業者は、情報システムの不正使用や不適切な運用のチェックなど、問題が発生したときの調査及びアクセス制御の監視を補うため、情報システムの使用状況を記録し、保存する必要がある。この記録は、少なくとも利用者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並びに使用されたプログラム、情報システム及びデータへのアクセスの成否を含み、定期的及び必要に応じて点検しなければならない。

第６節 検証・改善

事業者は、秘密保全に万全を期すため、秘密情報を取り扱う情報システムに係る文書類、組織、秘密情報の管理状況、教育内容等について、定期的な検証を行い、状況に応じて必要な改善を行わなくてはならない。

この検証において、秘密文書等及び秘密を取り扱う情報システムへの不正なアクセス、開示、使用、改ざん、破壊等が及ぼす被害、脅威及び脆弱性の程度、秘密を取り扱う部署の内部のほか、秘密保全に影響を及ぼすおそれがあると認める範囲で、事業者の別の部署及び外部の組織（情報システムの保守を外部委託する業者等を含む。）におけるリスクを特定、分析及び評価を考慮したリスク査定を実施する必要がある。

なお、このリスク査定を実施した場合は、その結果を記録する必要がある。

第１２章
立入手続及び会議

第１節　立入手続

本章は、事業者の秘密保全施設に、事業者の関係社員及び管轄する地方防衛局の保全検査官以外の者が立ち入る場合について、説明する。

本章の手続は、立入者が秘密取扱適格性を有する者であるか及び立入りの必要性を確認することにより、秘密取扱適格性を有する者以外の者が秘密に接することを防止すること及び秘密取扱適格性を有しない立入者に対して実施する保護措置について確認することにより、秘密情報の漏えいを防止することを目的としている。

外国からの訪問に関する手続は、第１７章で説明する。

第２節　秘密情報を取り扱うための立入

秘密情報を取り扱うための立入の回数は、必要最小限にとどめる必要がある。事業者は、秘密保全施設へ関係社員以外の者を立ち入らせる前に、管轄する地方防衛局の許可を得る必要があり、政府職員及び他の事業者の関係社員ごとに立入手続が規定されている。

秘密を取り扱うための立入者は、知る必要性（Need to know）の確認が必要となり、政府職員については秘密取扱立入通知書の通知によって、他の事業者の関係社員については契約及び秘密取扱立入許可申請書により確認される。

１．政府職員の訪問の許可

訪問する政府職員の管理者によって発行される秘密取扱立入通知書が、地方防衛局を経由して受入先の事業者に通知される。当該通知書は、以下の情報が含まれる。

⑴　管理者の官職及び氏名（承認権者は所属部課等の長）
⑵　立入期日
⑶　立入者の氏名及び身分証明書番号
⑷　立入目的（知る必要性）
⑸　立入者が取り扱い得る秘密の種類及び範囲（秘密取扱適格性及び当該秘密の取扱許可）
⑹　立入先で開示される秘密情報の範囲

2．他の事業者の関係社員に対する立入許可

受入側の事業者は、秘密取扱立入許可申請書を管轄する地方防衛局に提出する必要がある。当該許可申請書に記載しなければならない情報は、前項の規定と同じである。申請者は受入側の事業者の総括者とし、訪問前までに管轄する地方防衛局からの許可を得る必要がある。

3．長期間の立入許可

地方防衛局は、必要な場合に常時立入許可書を発行することができ、有効期間は1年未満となる。事業者と地方防衛局は、この許可書の有効期限が切れていないか定期的に確認をしなければならない。また、常時立入許可書を受けた者は、人事異動などで使用の必要がなくなった場合は速やかに当該許可書を発行した地方防衛局に申し出なければならない。

第3節　秘密情報を取り扱わない立入

事業者は、秘密保全施設、秘密保全施設内の器材等の維持管理や、消防点検等の法令の規定等により秘密取扱適格性を有しない者を秘密保全施設へ立ち入らせる必要がある場合は、管轄する地方防衛局へ立入許可申請書を提出し、訪問前までに地方防衛局の許可を得る必要がある。

この場合、保全責任者又は保全責任者が指定した関係社員を立ち会わせ、秘密情報の漏えい等の防止に必要な保護措置（秘密文書等を保管容器に格納又は他の秘密保全施設へ移動、被覆等）を講じる必要がある。

なお、許可申請書には以下の項目を記載しなければならない。

⑴　立入先の秘密保全施設名
⑵　立入期日
⑶　立入者の氏名及び身分証明書番号
⑷　立入目的
⑸　立入先で取り扱われている秘密の種類
⑹　立入時の秘密保護措置

第４節　緊急時の立入

緊急を要する業務等で真にやむを得ないと認められる場合は、適切な秘密保護措置を講じた上で、事後に必要な手続を実施することを条件に、事業者の秘密保全施設への立入について管轄する地方防衛局から許可される場合がある。

この許可は、真にやむを得ないと認められた場合のみ認められる手続であり、法令等に根拠がある場合などに限定して実施する必要がある。

第５節　会議

本節における説明は、秘密情報を取り扱う会議の時のみ実施する措置ではなく、秘密保全施設で必要となる保護措置のうち、特に留意すべき措置を特記し、秘密情報の漏えいを防止することを目的としている。

なお、秘密情報の取り扱いを伴う会議は、防衛装備庁との契約の履行を目的に行われるものを想定している。

事業者は、契約に基づき、会議の実施を求められることがあるが、このような秘密情報の取扱いを伴う会議は、必要最小限にとどめる必要がある。

１．参加者及び実施場所

秘密情報を取り扱う会議に参加できる者は、秘密取扱適格性を有し、会議の実施に必要な事業者の従業者及び政府職員であり、会議の目的のために必要最小限の参加範囲に限定する必要がある。

また、会議は、事業者の承認済の秘密保全施設又は政府の秘密取扱施設で行うほか、取り扱う秘密情報の範囲は、会議の目的に関連するものに限定しなければならない。

なお、参加者が秘密取扱適格性を有するかどうか及び知る必要性（Need to know）を有しているかについては、事業者の秘密保全施設で実施する場合は、第２節で説明した秘密取扱立入通知書及び秘密取扱立入許可申請書により確認され、防衛装備庁の秘密取扱施設で行う場合は、防衛装備庁の主催者（管理者）が確認することとなる。

２．伝達時の措置

第８章第３節で説明したとおり、秘密情報を口頭で伝達する場合は、その始めと

終わりに伝達する内容が秘密であることを明らかにするとともに、筆記及び録音を禁止する等必要な措置を講じる必要がある。

3．配布資料

秘密情報が含まれる資料を配布するために複製しなくてはならない場合は、仕様書に記載がない限り事前に防衛装備庁に複製の許可を得る必要がある。また、それぞれの資料に一連番号を表示する必要がある。

秘密情報が含まれる資料は会議後回収することを原則とし、事業者以外の参加者に配布した資料を回収しない場合は、防衛装備庁に事前に許可を得た上で、送達の手続をとる必要がある。

第１３章
下請負契約

第１節　下請負について

秘密情報の取扱いを含む下請負契約は、原則として認められない。ただし、特段の事情がある場合は、以下の条件により許可する場合がある。

・当該下請負事業者が事業者秘密取扱適格性（FSC）を認定されていること。

・防衛装備庁と元請事業者と下請負事業者との三者間で、秘密保護契約（以下「三者間契約」という。）が締結されていること。

下請負事業者は、秘密取扱適格事業者であるほか、元請事業者に課されている義務と同様の義務を課されることになる。

第２節　元請事業者の責任

元請事業者が、下請負事業者に秘密情報を開示する又は下請負事業者に秘密情報を取り扱わせる前に、元請事業者は以下の事項を実施する必要がある。

（下請負契約締結前）

⑴　防衛装備庁に対して下請負契約を締結する旨の申請書を提出する必要がある
当該申請書には以下の項目を記載しなければならない。

・下請負事業者名

・下請負業務内容の詳細

・下請負事業者が取り扱う秘密情報の範囲

・下請負事業者が行う情報保全措置

⑵　下請負事業者に対して、防衛装備庁との三者間契約の締結に向けた手続を始めるよう要請しなければならない。

⑶　提出した申請書について防衛装備庁から許可を得る必要がある。

（下請負契約締結後）

⑷　定期的に下請負事業者の検査を行わなければならない（地方防衛局はこれとは

別に定期検査を実施する。)。

⑸　下請負事業者に秘密情報を送付する場合は、防衛装備庁に申請し、許可を得なければならない。なお、この場合、原則として、防衛装備庁から直接、下請負事業者に秘密文書等を送付する。

第３節　三者間契約

三者間契約には、次の項目を含む。

なお、三者間契約の効力は、元請事業者による下請負申請が許可された場合に発生することになる。

⑴　下請負事業者は、元請事業者と同様に秘密の保全を確実に実施すること。

⑵　下請負事業者は、自らの過失により秘密情報を漏えいした場合、元請事業者との下請負契約にかかる契約金額に対して違約金条項に定める違約金を支払うこと。

⑶　下請負事業者が取り扱う秘密情報の範囲

⑷　下請負契約の途中解除

・下請負事業者の帰責事由により防衛装備庁が下請負事業者との保全契約を契約途中で解除する場合には、防衛装備庁は元請事業者に対して契約の途中解除を通告すること。
・下請負事業者の帰責事由により、元請事業者が下請負契約を契約途中で解除する場合は、元請事業者はあらかじめ防衛装備庁に通知しなくてはならないこと。
・元請事業者の帰責事由により、防衛装備庁が元請契約を契約途中で解除する場合は、防衛装備庁は、元請事業者と下請負事業者との三者間の契約を解除できること。

第４節　下請負契約の終了

元請事業者は、下請負契約を終了する場合、原則として三者間契約も終了することになるため、下請負事業者に対して、当該下請負事業者が所有している秘密文書等を

原則として全て防衛装備庁に返却又は提出させなければならない。当該秘密文書等が元請事業者から下請負事業者に対して提供されたものである場合には、当該元請事業者に対して返却又は提出させるものとする。

なお、下請負事業者は、三者間契約が終了した場合でも、三者間契約中に知得した秘密情報を漏えいすることは認められない。

第５節　下請負事業者への秘密物件等の輸送

第２節第５項において、原則として、防衛装備庁から直接下請負事業者に秘密文書等を送付するとあるが、防衛装備庁の許可があれば、元請事業者から下請負事業者、下請負事業者から元請事業者へ秘密物件等を輸送することができる。

なお、輸送に関しては、第７章第４節に従わなければならない。

第１４章
保全検査

第１節　関係簿冊

総括者は、秘密情報の接受、閲覧、作成、保管、提出、廃棄等を確実に実施し、また確実に実施したことを証明するため、以下のとおり必要な関係簿冊を整備しなければならない。

・保管記録（件名、文書番号及び受領年月日等）
・閲覧・貸出記録（閲覧・貸出年月日、閲覧・貸出者等）
・秘密保全施設への立入記録（施設への立入者、適格証番号、施設内における業務内容、入退出時間等）
・検査記録（事業者による社内検査記録等）

総括者は、関係簿冊を秘密保全の責任のある期間（秘密情報の指定期間若しくは指定の解除）の経過後３年を経過するまでの間保管しなければならない。

第２節　事業者による社内検査

総括者は、少なくとも月に一回は社内検査を行う必要がある。社内検査の対象は、前節の関係簿冊の点検のほか、事業者でとられる全ての秘密保全措置となる。

総括者は、社内検査の結果を記録し、保管しなければならない。

第３節　地方防衛局による保全検査

事業者は、前節の社内検査の終了後に、月に１回管轄する地方防衛局の職員による保全検査を受検しなければならない。

また、事業者は、地方防衛局が行う保全検査に協力する必要がある。保全検査は、事業所ごとに実施し、地方防衛局の職員は、管轄する事業者全てを検査するため、あらかじめ受検日程について事業者と調整し、事業者は地方防衛局が行う保全検査の前までに前節の社内検査を終える必要がある。

また、これに加え防衛装備庁が必要と判断すれば、臨時で保全検査を実施することもある。

主要な検査項目は、次のとおりであり、すべての秘密保全措置が対象となる。

・秘密情報の取扱状況（作成、複写、伝達、廃棄等）
・秘密情報の帳簿への記録
・施設（立入手続等を含む）
・情報システムの使用履歴
・関係社員名簿
・保全教育の実施
・事業者の社内検査の結果
・下請負事業者の管理監督（下請負がある場合）

また、検査は次の３つの評価区分に従って評価される。

・良　好：全ての保全措置が要求基準に基づき適切に実施されている。
・要改善：全体として適切な保全措置がとられているが、軽微な修正を必要とする項目がある。
・不　良：不適切な保全措置がとられており、保全措置を完全にするため見直しが必要である。

なお、通常、地方防衛局は、防衛装備庁に対して四半期ごとに検査結果を通知するが、「不良」事項が見つかった場合は、速やかに防衛装備庁に通知する必要がある。

この場合、事業者は指摘された事項を解決する是正計画を作成し、実施しなければならない。地方防衛局は事業者の是正計画を確認し、その是正計画の実行の確認を行うとともに、必要に応じて指導を行う。当該是正計画の実行期限は地方防衛局により提示され、又は当該事業者及び地方防衛局との協議により決定される。

第４節　保管状況報告

事業者は、前２節の社内検査及び保全検査のほか、原則６月末及び１２月末時点の秘密文書等の保管状況を防衛装備庁に報告する必要がある。

この保管状況の報告は、防衛省で統一した時期に実施している報告にあわせて実施されている。

第５節　特定秘密の取扱いに係る基準適合性報告

適合事業者は、特定秘密の保護に関する法律施行令（平成２６年政令第３３６号）第１３条に従って講じた措置の内容を毎年４月末までに、防衛装備庁装備政策部長宛に提出しなければならない。

第１５章
事故発生等の報告及び措置

第１節　事故等発生時の措置

事業者は、秘密文書等を紛失した場合、秘密情報が漏えい若しくは破壊された場合又はそれらの疑い若しくはおそれがある場合、あるいは事業者が所持を認められていない秘密物件等を受領又は発見した場合は、直ちに適切な措置を講じる必要がある。

秘密情報の漏えい等の「疑い若しくはおそれがある場合」には、従業者等による不正、許可を得ない秘密情報の取扱いやアクセス又は関係社員による総括者が許可しない外国政府関係者等との接触を含む。

事業者は、これらを発見した場合は、直ちにその事実の確認を行い、かつ、秘密情報の保護に必要な措置を講じて事故等の拡大防止に努めるとともに、その段階で把握しうる全ての内容を防衛装備庁（装備保全管理課）及び管轄する地方防衛局の双方へ報告することが義務付けられている。

秘密情報の保護に必要な措置とは、秘密保全施設を含む建物の封鎖、総括者の指示を受けて秘密文書等を一時的に安全な場所への移動、不正に受領した秘密文書等の防衛装備庁（装備保全管理課）への提出等があげられる。

事業者は、報告後、遅滞なく次に掲げる項目を詳細に調査し、調査結果に所見及び対策を添えた調査報告書を契約担当官等に提出しなければならない。

・事故が発生した日時及び場所並びに事故等の当事者の氏名及び職務
・事故等に係る秘密文書等の件名、登録番号、一連番号、数量及び内容
・事故等の原因及び経緯
・事故等が及ぼす影響
・事故等に対して講じた措置
・その他参考となるべき事項

なお、事業者は、上記の事故等が犯罪行為に該当する場合、速やかに警察に通報する必要がある。

第２節　緊急連絡体制

事業者は、前節で説明した非常時及び事故等発生時に備えて速やかに連絡できる体制を維持するために、緊急時の連絡経路を整備し、関係社員に周知しなければならな

い。

防衛装備庁の窓口は、装備政策部装備保全管理課及び地方防衛局となり、その連絡先は次のとおり。

・事故等の連絡先

防衛装備庁装備政策部装備保全管理課

電話：０３－３２６８－３１１１　内線　２１０４３～２１０４５

（夜間については、契約後に通知する夜間緊急窓口に連絡する。）

各防衛局の連絡先は付録に記載する。

第３節　非常時の措置

事業者は、秘密情報の漏えいのおそれがある緊急の事態に際し、その漏えいを防止するために他に適当な手段がないと認められる場合は、焼却、粉砕、細断、溶解、破壊等の復元不可能な方法により、秘密文書等を廃棄することができる。

この場合、あらかじめ防衛装備庁（特定秘密の場合は防衛装備庁（調達事業部長）を通じて防衛大臣又は防衛装備庁長官）の承認が必要になるが、その手段がない場合又はそのいとまがない場合は、廃棄後速やかに報告する必要がある。

第４節　公益通報窓口

事業者の役員及び従業者（退任及び退職した者を含む。）は、秘密情報の取扱いについて、防衛装備庁の職員又は防衛装備庁の契約先事業者で防衛装備庁との契約事業に従事している従業者が、法令違反行為又は法令違反行為が生じるおそれがあるときは、防衛装備庁の公益通報窓口に通報することができる。

事業者は、自社の従業者が公益通報を行ったことを理由として解雇したり、不利益な取扱いを行うことは禁止されている。

公益通報を行う場合は、公益通報者の所属、氏名及び連絡先、通報対象事実（いつ、だれが、どこで、どのように法令違反行為を行ったか等）、通報対象事実の根拠となる法令名をできる限り明らかにして、メール、郵送又は電話により、以下に記載する窓口に通報することができる。

ただし、秘密情報の内容を通報することは認められない。

・通報窓口の連絡先

メール：atla-koeki-tsuho@atla.mod.go.jp

郵　送：〒１６２－８８７０　東京都新宿区市谷本村町５－１
防衛装備庁長官官房監察監査・評価官
公益通報窓口

電　話：０３－３２６８－３１１１　内線　３５８４１・３５８４３

第１６章
秘密文書等の返却及び廃棄

第１節　秘密文書等の返却・提出

事業者は、秘密情報を取り扱う契約において、秘密文書等を使用する必要がなくなった場合、速やかに秘密文書等を返却しなければならない。

契約に基づき作成又は複製した秘密文書等も、仕様書で定められた提出先に提出する必要がある。

なお、契約履行中であっても、防衛装備庁の指示があった場合は、秘密文書等を返却又は提出しなければならない。

また、契約解除になった場合も、事業者は、秘密文書等を速やかに返却又は提出しなければならない。

事業者は、この返却及び提出について、記録に残し、防衛装備庁へ報告する必要がある。

第２節　秘密文書等の廃棄

事業者は、原則として貸与を受けた秘密文書等は返却し、作成又は複製した秘密文書等は提出しなければならないが、防衛装備庁の指示があった場合のみ秘密文書等を廃棄することができる。

秘密文書等を廃棄する際は、防衛装備庁の指示に従い、総括者により指定された関係社員を最低１名以上立会させ、焼却、粉砕、細断、溶解、破壊等の方法により、秘密として探知されないように確実に廃棄しなければならない。

なお、事業者は、廃棄について記録に残し、防衛装備庁へ報告する必要がある。

第１７章
国際的な事業に関連する保全措置

本章では、国際的な事業に関連する秘密情報の管理について説明する。

我が国の事業者が、諸外国の政府及び事業者との間において、秘密情報を「安全」かつ「合理的」に共有できることは、防衛装備・技術協力の基盤である。

第１節　適用される国内法令及び二国間の保全枠組

国際的な事業に関連する秘密情報の外国政府又は外国事業者との共有は、秘密情報の保護に関する国内法令及び国際的な枠組の適用を受ける。

また、我が国の秘密情報は原則として、相手国政府との間における秘密情報の保護に係る協定の締結又は相手国の当局との間における取決めの署名が行われるまで相手国に開示されない。

我が国の防衛関連の事業者にも適用され得る、他国との間の情報保護のための枠組みとしては、相手国と交換する安全保障に係る秘密情報の保護措置について定めた秘密情報保護協定、相手国と交換する秘密軍事情報の保護措置について定めた秘密軍事情報保護協定及び防衛当局間における情報保護取決めがある。

なお、他国との間における秘密情報保護枠組は、相手国との関係等により非公表とするものもある。

第２節　外国の利害関係者に対する秘密情報の開示

外国政府又は外国事業者に対して秘密情報を開示するにあたっては、秘密情報の保護に関する国内法令及び関連する防衛装備庁の規則に従い、防衛装備庁長官の許可が必要となる。

なお、秘密情報を含む物件及び技術の外国への提供については、秘密情報の保護に関する法令等による規制が適用されることに加え、外国為替及び外国貿易法（昭和２４年法律第２２８号）による輸出許可を受けることが必要である。

第３節　外国政府の秘密情報

１．外国政府の秘密情報の受領

我が国の秘密保護法令及び我が国と外国政府との間で締結している秘密情報保護協定等において、外国政府の秘密情報を日本の事業者に取り扱わせる際には、日本政府を経由することを前提としている。これは、日本の事業者は、日本政府と当該事業者との秘密保護契約（第４章）に基づき秘密情報を保護する義務が課されるためである。

また、防衛装備・技術協力等（日本の防衛関連事業者が外国の政府又は事業者により実施される事業に参画する場合等）の目的のために、日本の事業者が外国政府の秘密情報を受領する必要が生じた場合には、防衛装備庁との間で秘密保護契約を締結することにより、当該外国政府の秘密情報の保護について法的義務を負った上でこれを受領することが可能となる。その際、当該事業者は、事業者秘密取扱適格性(FSC)を取得している必要がある。

なお、外国政府の秘密情報を受領する必要がある日本の事業者が、防衛装備庁との間において、防衛省に納入する装備品の製造請負契約等を締結する予定がない場合であっても、当該事業者は、第４章３節で説明した無償の秘密保護契約を防衛装備庁と締結することにより、当該外国政府の秘密情報の保護について法的に義務を負った上で、これを受領することが可能となる。無償の秘密保護契約に関する問い合わせは防衛装備庁（装備保全管理課）が受け付ける。

２．外国政府の秘密情報の取扱い

外国政府から受領した秘密情報は、当該外国政府による秘密区分に係る表示を維持した上で、日本において相当する秘密区分及び提供国の表示について、防衛装備庁が定めた様式により原則として赤色で付すこととしている。

なお、外国政府の中には、日本に直接対応するもののない四番目の秘密区分として「Restricted」等の区分を設けているものもある。これらは、二国間の情報保護協定等による相手国政府からの通知等に従って、秘密情報である「秘」として保護する場合と、管理された非秘密情報（Controlled Unclassified Information）である保護すべき情報（注意及び部内限り）として保護される場合がある。

また、外国政府から受領した秘密情報は、情報保護協定等の規定に従い、当該情報の提供国政府の書面による事前の許可を得た場合を除いて、第三者に開示することはできない。

第４節　国際共同プロジェクトに関する秘密保全

防衛装備庁の各部署（長官官房各開発官及び各研究所等）は、国際的な共同プロジェクトの実施にあたり、防衛装備庁（装備保全管理課）の承認を得て、当該プロジェクトに係る保全要領（Project Security Instruction, 以下「PSI」という。）を相手国の担当部署との間に作成する。

PSI は、共同プロジェクト参加国の異なる保全規則を調整し、共同プロジェクトを円滑に実施するための情報保全の実施要領である。

両国の政府職員及び事業者は、当該プロジェクトを PSI の規定により実施する。

PSI の標準的な項目は以下のとおりであるが、必要に応じ追加の要件を適用してもよい。

・導入及び用語の定義（目的、権限、責任、適用範囲）
・保全に関する指示（秘密情報への接触、国際的な送付、表示、管理すべき非秘密情報の保護の手続、秘密区分、漏えい及び違反）
・プログラム情報（共同プログラムにおいて提供・生成・使用されるあらゆる情報）の開示（第三者への開示、会議等での開示、一般への公表、展示会での開示等にかかる指示）
・国際訪問
・下請負
・クリアランスを有する施設の一覧
・共同プログラムの終了又は事業者の契約終了時における保全に関する計画
・保全教育・保全意識の向上

第５節　事業者による外国との間における秘密情報の送付

外国との間における秘密情報の送付は、政府間の経路を通じて行われる。これは、日本の秘密保護法令において、秘密情報は日本政府を通じて外国政府及び日本の事業者に提供する枠組となっていること等を背景にしている。

他方、防衛装備・技術協力等においては、政府間の直接の送付のみならず、日本及び外国の事業者間において秘密情報を物理的又は電子的に送付し、迅速に共有することが不可欠な場合がある。

このような場合、日本政府及び相手国政府との間に事前の了解があり、かつ日本の

秘密保護法令と整合的な運用を確保できる場合には、事業者による秘密情報の送付が可能となる。例えば、特定秘密に関しては、以下の条件を満たすことにより、事業者間の秘密情報の送付が日本政府を通じて日本の事業者及び外国政府への提供の範囲内と解釈でき可能となる。

⑴　秘密情報の確実な保護措置のために必要な事項に関する防衛装備・技術協力等を行う相手国政府との間の確認

⑵　秘密情報の送付に関する防衛省から適合事業者に対する事前の指示又は許可

⑶　事業者から防衛省へのその後の情報共有（日本政府による確実な特定秘密情報の管理・把握）

その上で秘密情報の送付の可否及び個別具体的な手続については、当該国との情報保護協定等の規定等を含む個別の事情を踏まえて検討する必要がある。特定秘密以外の秘密情報に関するものを含め、所要が発生した場合の問い合わせは、防衛装備庁（装備保全管理課）が受け付ける。

第６節　外国からの訪問及び外国人による立入の制限

本節においては、外国人による秘密情報へのアクセスを必要とする、事業者の秘密保全施設への訪問の手続について説明する。

⑴　訪問の申請手続

訪問に関する具体的な手続については、本マニュアルに規定するもの（外国人の訪問申請（Request For Visit，以下「RFV」という。）（付録２））が原則である。他方、PSI 等の両国間の書面による合意により、代替となる訪問要領を個別に定めることは妨げない。

⑵　訪問の申請手続

外国人による訪問の申請手続は以下のとおり。

①　外国政府は、政府間経路（通常は当該国の大使館）を通じて、防衛装備庁（装備保全管理課）に対して、RFV を提出。

②　防衛装備庁は、当該外国人のセキュリティ・クリアランス及び秘密保全施設の訪問に関して知る必要性（Need to know）等を確認し、結果及び RFV を地方防衛局に通知。

③　地方防衛局において、当該訪問の可否を決定し、訪問先事業者に通知。

⑶　RFV の種類

外国人による訪問には次の３つの種類がある。

①　１回限りの訪問：特定の目的のための単発かつ短期間（通常３０日以内）の訪問のこと。訪問の期間は、訪問者の秘密取扱適格性（PSC）の有効期間を超えることはない。

②　継続訪問：特定の期間、特定の目的のために特定の場所に継続的に行う１年以内の訪問を指す。訪問の期間は、訪問者の秘密取扱適格性（PSC）の有効期間を超えることはない。

③　緊急訪問：⑷に示す申請期限を満たすことができず、訪問ができない場合に重大な影響が生じることが合理的に予測される場合に許可される１回限りの訪問。緊急訪問を申請する場合、訪問先との間で当該訪問に関して事前調整を行い、防衛装備庁に対し訪問の正当性を示す必要がある。

⑷　RFV の申請期限

RFV は、1 回限りの訪問又は継続訪問の最初の開始日の２０営業日前までに申請しなければならない。

⑸　RFV の修正

①　すでに承認された、あるいは保留中の RFV について、変更が必要な場合、修正した RFV を提出しなければならない。

②　ただし訪問の種類及び緊急訪問で申請した内容は、修正手続によって変更することはできない。

③　修正内容の反映は、防衛装備庁（装備保全管理課）に RFV が届いた日から５営業日必要である。

（付録１）　問い合わせ先等

● 本マニュアルについての問い合わせ先

防衛装備庁　装備政策部　装備保全管理課

（住所）〒１６２－８８７０

東京都新宿区市谷本村町５－１

（電話）０３－３２６８－３１１１　内線　２１０４３～２１０４５

（メールアドレス）：hozen-manual@ext.atla.mod.go.jp

●事故等発生時の連絡先

防衛装備庁　装備政策部　装備保全管理課

（住所）〒１６２－８８７０

東京都新宿区市谷本村町５－１

（電話）０３－３２６８－３１１１　内線　２１０４３～２１０４５

（休日夜間の緊急電話先）　契約後に通知する。

各地方防衛局の連絡先

組織等名	部署名	電話番号（直通）
北海道防衛局	調達部調達計画課	011-272-7512
東北防衛局	郡山防衛事務所	024-961-7681
北関東防衛局	装備部装備企画課	03-3908-5121
	宇都宮防衛事務所	028-638-1384
南関東防衛局	調達部装備課	045-641-4741
近畿中部防衛局	調達部装備課	06-6949-6472
	舞鶴防衛事務所	0773-62-0305
東海防衛支局	装　備　課	052-952-8281
	岐阜防衛事務所	058-383-5935
中国四国防衛局	調達部装備課	082-223-8014
	玉野防衛事務所	0863-21-3724
長崎防衛支局	総　務　課	095-825-5303
沖縄防衛局	調達部調達計画課	098-921-8131

（付録２） RFV の標準的なフォーマット

All fields must be completed and the form communicated via Government-to-Government

REQUEST FOR VISIT

TO: _____

(Country/international organisation name)

1. TYPE OF VISIT REQUEST	**2. TYPE OF INFORMATION/ MATERIAL OR SITE ACCESS**	**3. SUMMARY**
☐ One-time ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Agency/Facility For an amendment, insert the NSA/DSA original RFV Reference No._____	☐ CONFIDENTIAL or above ☐ Access to security facilities without access to classified information/ material	No. of sites: _____ No. of visitors: _____

4. ADMINISTRATIVE DATA:

Requestor: To: ATLA, Japan Ministry of Defense	NSA/DSA RFV Reference No._____ Date *(dd/mm/yyyy)*: _____/_____/_____

5. REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

☐ Military ☐ Government ☐ Industry ☐ Other

If other, specify: _____

NAME:

POSTAL ADDRESS:
E-MAIL ADDRESS:
FAX NO:
TELEPHONE NO:

6. GOVERNMENT AGENCY(IES) , ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED - *(Annex 1 to be completed)*

7. DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. TYPE OF INITIATIVE *(Select one from each column)*:

☐ Government initiative	☐ Initiated by requesting agency or facility
☐ Commercial initiative	☐ By invitation of the facility to be visited

9. IS THE VISIT PERTINENT TO:

☐ Specific equipment or weapon system
☐ Foreign military sales or export licence
☐ A programme or agreement
☐ A defence acquisition process
☐ Other

Specification of the selected subject:

10. SUBJECT TO BE DISCUSSED/JUSTIFICATION/PURPOSE *(To include details of host Government/Project Authority and solicitation/contract number if known and any other relevant information. Abbreviations should be avoided)*:

11. ANTICIPATED HIGHEST LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:

☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐ Other

If other, specify: _____

12. PARTICULARS OF VISITOR(S) - *(Annex 2 to be completed)*

13. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE
(dd/mm/yyyy): _____/_____/_____

15. REQUESTING NATIONAL SECURITY AUTHORITY / DESIGNATED SECURITY AUTHORITY:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE
(dd/mm/yyyy): _____/_____/_____

16. REMARKS *(Mandatory justification required in case of an emergency visit)*:

ANNEX 1 to RFV FORM

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

1. ☐ Military ☐ Government ☐ Industry ☐ Other

If other, specify: _____

NAME:
ADDRESS:
TELEPHONE NO:
FAX NO:

NAME OF POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

NAME OF SECURITY OFFICER OR
SECONDARY POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

2. ☐ Military ☐ Government ☐ Industry ☐ Other

If other, specify: _____

NAME:
ADDRESS:
TELEPHONE NO:
FAX NO:

NAME OF POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

NAME OF SECURITY OFFICER OR
SECONDARY POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

3. ☐ Military ☐ Government ☐ Industry ☐ Other

If other, specify: _____

NAME:
ADDRESS:
TELEPHONE NO:
FAX NO:

NAME OF POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

NAME OF SECURITY OFFICER OR
SECONDARY POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

4. ☐ Military ☐ Government ☐ Industry ☐ Other

If other, specify: _____

NAME:
ADDRESS:
TELEPHONE NO:
FAX NO:

NAME OF POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

NAME OF SECURITY OFFICER OR
SECONDARY POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

(Continue as required)

ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)

1. ☐ Military ☐ Defence Public Servant ☐ Government

☐ Industry/Embedded Contractor ☐ Other (Specify: _____)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

2. ☐ Military ☐ Defence Public Servant ☐ Government

☐ Industry/Embedded Contractor ☐ Other (Specify: _____)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

3. ☐ Military ☐ Defence Public Servant ☐ Government

☐ Industry/Embedded Contractor ☐ Other (Specify: _____)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

4. ☐ Military ☐ Defence Public Servant ☐ Government

☐ Industry/Embedded Contractor ☐ Other (Specify: _____)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

(Continue as required)