【令和８年１０月１日から適用】

装備品等の調達に係る秘密保全対策ガイドライン

令和８年４月

防　衛　省

目　　次

１　目的及び考え方・・・・・・・・・・・・・・・・・・・・・・・・・・１

２　用語の定義・・・・・・・・・・・・・・・・・・・・・・・・・・・・１

３　適用範囲等・・・・・・・・・・・・・・・・・・・・・・・・・・・・２

４　秘密保全規則等の取扱い・・・・・・・・・・・・・・・・・・・・・・３

５　第三者への開示の禁止・・・・・・・・・・・・・・・・・・・・・・・３

６　組織のセキュリティ・・・・・・・・・・・・・・・・・・・・・・・・３

７　特定資料又は特定物件の分類及び管理・・・・・・・・・・・・・・・・３

８　人的セキュリティ・・・・・・・・・・・・・・・・・・・・・・・・・４

９　秘密漏えい等の事故発生時の対応・・・・・・・・・・・・・・・・・・５

１０　物理的及び環境的セキュリティ・・・・・・・・・・・・・・・・・・６

１１　通信及び運用管理・・・・・・・・・・・・・・・・・・・・・・・・８

１２　アクセス制御・・・・・・・・・・・・・・・・・・・・・・・・・１０

１３　検証・改善・・・・・・・・・・・・・・・・・・・・・・・・・・１２

１４　検査及び調査の受入れ・・・・・・・・・・・・・・・・・・・・・１２

１５　適用の特例・・・・・・・・・・・・・・・・・・・・・・・・・・１２

１　目的及び考え方

装備品等の調達に係る秘密保全対策ガイドライン（以下「本ガイドライン」という。）は、乙による秘密（防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律（令和５年法律第５４号）第２７条第１項に規定する装備品等秘密、特定秘密の保護に関する法律（平成２５年法律第１０８号）第３条第１項に規定する特定秘密又は日米相互防衛援助協定等に伴う秘密保護法（昭和２９年法律第１６６号）第１条第３項に規定する特別防衛秘密をいう。以下同じ。）の保全又は保護（以下「秘密保全」という。）を万全ならしめるために、秘密保全特約（装備品等秘密の保全に関する特約条項（装備品等秘密の指定等に関する訓令（令和６年防衛省訓令第１０号。以下「装秘訓令」という。）別記第２号様式の特約条項をいう。以下同じ。）、特定秘密の保護に関する特約条項（特定秘密の保護に関する訓令第３６条第１項に規定する審査基準及び第３７条第２項に規定する特約条項について（防経装第１９０７４号。２６．１２．２４）別紙の付紙第２の特約条項をいう。以下同じ。）若しくは防衛装備庁における特定秘密の保護に関する特約条項（防衛装備庁における特定秘密の保護に関する訓令第３６条第１項に規定する審査基準及び第３７条第２項に規定する特約条項について（装装制第５４号。２７．１０．１）別紙の付紙第２の特約条項をいう。以下同じ。）又は特別防衛秘密の保護に関する特約条項（特別防衛秘密の保護に関する訓令（平成１９年防衛省訓令第３８号）別記第５号様式の特約条項をいう。以下同じ。）若しくは防衛装備庁における特別防衛秘密の保護に関する特約条項（防衛装備庁における特別防衛秘密の保護に関する訓令（平成２７年防衛装備庁訓令第２５号）別記第６号様式の特約条項をいう。以下同じ。）を補足する共通の事項を規定するものである。

乙は、秘密保全規則等（秘密保全特約及び本ガイドラインに基づき作成し甲の確認を受けた秘密の保全に関する規則及び秘密保全実施要領をいう。以下同じ。）に従い、秘密を適正に取り扱わなければならない。

２　用語の定義

本ガイドラインにおいて用語の意義は次のとおりとする。

(1)　情報システムとは、ハードウェア、ソフトウェア、ネットワーク又は記憶媒体で構成されるものであって、これら全体で業務処理を行うものをいう。

(2)　秘密取扱情報システムとは、秘密を取り扱う情報システムをいう。

(3)　パソコンとは、情報システムを構成する端末装置である電子計算機、ネットワークに接続せずに独立して業務処理を行うことのできる電子計算機、計測器又は試験用器材として使用されるものであって各種のデータを保存することのできる電子計算機その他のデータ保存機能を有する電子計算機をいう。

(4)　可搬記憶媒体とは、フロッピーディスク、光磁気ディスク、ＵＳＢメモリ、外付けハードディスクその他のパソコンに挿入又は接続して情報を保存し、当該情報を持ち出すことのできる媒体をいう。

(5)　秘密取扱可搬記憶媒体とは、秘密を取り扱う可搬記憶媒体をいう。

(6)　秘密取扱情報システムメンテナンス等可搬記憶媒体とは、秘密取扱情報システムのメンテナンス等のために使用する可搬記憶媒体をいう。
(7)　携帯型記録機器とは、映像走査機（ハンディスキャナー）、写真機、録音機、ビデオカメラその他の映像記録等の機能を有する機器をいう。
(8)　携帯型情報通信機器とは、携帯電話、携帯情報端末（ＰＤＡ）その他の通話・通信の機能を有する機器をいう。
(9)　特定資料又は特定物件とは、次のいずれかに該当するものをいう。
ア　装備品等秘密の保全に関する特約条項第１条第２項に規定する特定資料又は特定物件
イ　特定秘密の保護に関する特約条項第１条第２項又は防衛装備庁における特定秘密の保護に関する特約条項第１条第２項に規定する特定資料又は特定物件
ウ　特別防衛秘密の保護に関する特約条項第１条第２項又は防衛装備庁における特別防衛秘密の保護に関する特約条項第１条第２項に規定する特定資料又は特定物件
(10)　関係社員とは、職務上特定資料又は特定物件を取り扱う必要があり、乙が秘密保全規則等に基づき指定した者をいう。
(11)　第三者とは、法人又は自然人としての防衛省と直接契約関係にある者以外の全ての者をいい、親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の防衛省と直接契約関係にある者に対して指導、監督、業務支援、助言、監査等を行うものを含む。
(12)　秘密保全施設とは、特定資料又は特定物件が取り扱われ、又は保管されている施設をいう。

３　適用範囲等

(1)　本ガイドラインは、秘密に係る情報の取扱いを対象とする。
(2)　本ガイドラインの適用の対象となる者は、乙において秘密に係る情報に接する全ての者（秘密に係る情報に接する役員（持分会社にあっては従業者を含む。以下同じ。）、管理職員等を含む。）とする。
(3)　秘密に係る情報の取扱いにおいて、パソコン及び携帯型記録機器（以下「パソコン等」という。）を使用する必要のない乙に対しては、パソコン等に係る規定（１０(4)から(9)まで、１０(11)、１１、１２及び１３(1)ア（秘密取扱情報システムに係るものに限る。））は適用しないものとする。この場合、乙は、パソコン等を取り扱わない旨を秘密保全規則等に規定し、甲の確認を受けるものとする。
(4)　本ガイドラインに規定されている事項以外の措置が必要となった場合には、乙は、その都度、甲と協議の上、必要事項を決定するとともに、当該必要事項を秘密保全規則等に加えるものとし、秘密保全規則等に新たに規定したときは、改めて甲の確認を受けるものとする。

4　秘密保全規則等の取扱い

(1)　乙は、本ガイドラインの内容に沿った秘密保全のための要領である秘密保全実施要領を作成し、甲の確認を受けるものとする。

(2)　秘密保全規則等は、甲による確認前に、受注案件を処理する部門責任者又はその上司（以下「部門責任者等」という。）の承認を受けていること。

(3)　乙は、秘密保全規則等を関係社員に確実に周知すること。

5　第三者への開示の禁止

乙は、第三者との契約において乙の保有し、又は知り得た情報を伝達、交換、共有その他提供する約定があるときは、秘密の情報をその対象から除く措置を講じなければならない。

6　組織のセキュリティ

(1)　乙は、秘密保全を確実に実施するための実効性の高い組織を設置するものとする。

(2)　乙は、関係社員以外の役員、管理職員等を含む従業者その他の全ての構成員について、関係社員以外の者は秘密に接してはならず、かつ、職務上の下級者等に対してその提供を要求してはならないことを定めなければならない。

(3)　乙は、秘密の種類を混同することなく、秘密の種類ごとに秘密を管理するとともに、秘密の種類ごとに秘密の管理全般に係る総括的な責任者（特定秘密においては特定秘密の保護に関する業務を管理する者。以下「総括者」という。）を置くこと。ただし、異なる秘密の種類の総括者を同一の者が兼ねることは、妨げない。

(4)　総括者は、秘密保全に係る関係部署及び関係社員の秘密保全に対する責任分担及び役割（秘密保全に係る手続の実施を含む。）を明確に定めること。

(5)　総括者又はその指定する者は、秘密保全規則等の内容及び履行状況を定期的に確認し、不十分な点があると認めるときは、直ちに是正のための必要な措置を講ずること。

7　特定資料又は特定物件の分類及び管理

(1)　総括者は、特定資料又は特定物件の作成、交付、供覧、保管、廃棄等の管理（以下単に「管理」という。）を確実に実施するため、秘密の種類ごと（必要な場合は、これに加え機密、極秘及び秘の区分ごと）に必要な関係簿冊（保管記録、閲覧・貸出記録、検査記録、立入記録等を記載する簿冊をいう。以下同じ。）を整備し、定期的に点検すること。この場合、総括者は、記録内容の改ざんを防止するための適切な管理を行うとともに、関係簿冊は秘密保全の責任がある期間（秘密等の保全又は保護の確保に関する違約金条項の取扱いについて（防経装第３２７０号。１９．３．２９）別添の第２条に規定する乙が秘密等を保全する責任がある期間をいう。）の経過後３年を経過するまでの間保管するものとし、その後、甲の確認を受け、廃棄すること。

また、装備品等秘密の提供を受ける際に交付された装秘訓令第７条第３項に規定する装備品等秘密指定書についても、関係簿冊に準じて管理すること。

(2)　総括者は、特定資料又は特定物件の管理を確実に実施するため、関係社員が従事する管理の作業ごとに、当該関係社員の権限及び義務を定め、並びに他の関係社員による確認、監視等の手順を定めるとともに、関係社員全員に対する教育、監督、検査等を適切かつ確実に行うこと。

８　人的セキュリティ

(1)　部門責任者等は、関係社員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)　乙は、前号における関係社員を指定するに当たっては、甲との契約に違反する行為を求められた場合に、これを拒む権利を実効性をもって法的に保障されない者を当該ふさわしい者と認めてはならない。

(3)　乙は、第１号における関係社員を指定するに当たっては、当該関係社員の指定を行おうとする従業者の同意を得た上で、関係社員名簿（関係社員の氏名、生年月日、所属する部署、役職、国籍等が記載されたものをいう。）を作成し、秘密に係る情報を取り扱わせる前に甲に届け出て同意を得なければならない。これを変更しようとするときも、同様とする。

(4)　乙は、第１号における関係社員を指定するに当たっては、次のア及びイに掲げる場合において、関係社員の指定を行おうとする者に対し、不利益な取扱いをしてはならない。

ア　乙による関係社員の指定の同意を求められた従業者が、当該同意をしない場合

イ　関係社員名簿に記載された従業者について、甲が関係社員の指定の同意をしない場合

(5)　乙は、契約の履行以外の目的で当該関係社員名簿に記載された情報を利用してはならないものとする。

(6)　特定秘密を取り扱う関係社員の指定にあっては、第３号の規定にかかわらず、特定秘密の保護に関する特約条項又は防衛装備庁における特定秘密の保護に関する特約条項に基づき実施するものとする。

(7)　部門責任者等は、次のア及びイに掲げる措置を確実に講ずること。

ア　秘密保全規則等に違反した者に対する正式な懲戒手続を備え、かつ懲戒を確実に履行すること。

イ　関係社員の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取扱いについて、同意書を提出させること。また、当該同意書には、当該関係社員が秘密を漏えいした場合の当該関係社員の民事上の責任に係る規定を含めること。

(8)　総括者は、秘密保全の重要性及び保全に関する社内規則（秘密保全規則等を含む。ウにおいて同じ。）の内容について、関係社員に対し、次のアからカまでに掲げる内容を含む教育及び訓練を新たに関係社員に指定された者が秘密

を取り扱う前等の必要な都度及び定期的に行い、その結果を甲に届け出ること。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について教育を行い、その結果を記録するものとする。

ア　秘密保全の重要性及び意義（秘密保全意識のかん養を含む。）

イ　「need to know の原則」（「情報は知る必要がある者にのみ伝え、知る必要のない者には伝えない」という原則）の確実な履行

ウ　保全に関する社内規則の確実な履行

エ　隙のない勤務と私生活における慎重な行動

オ　悪意のあるソフトウェアへの感染（特に可搬記憶媒体を介した感染）、内部不正等を防止するための対策及び感染した場合の対処手順

カ　ア～オまでに掲げる事項のほか、関係社員の役割と責任に応じて必要となる事項

9　秘密漏えい等の事故発生時の対応

(1)　事故発生時の報告

ア　乙は、秘密の漏えい、紛失、破壊等の事故（それらの疑い又はおそれがあるときを含む。以下同じ。）が発生したときは、適切な措置を講じるとともに、直ちに把握し得る限りの全ての内容を甲に報告し、その後速やかにその詳細を甲に報告しなければならない。

イ　乙は、アに規定する報告のほか、秘密の漏えい、紛失、破壊等の事故が発生した可能性又は将来発生する懸念について、乙の内部又は外部から指摘があったときは、直ちに当該可能性又は懸念の真偽を含む把握し得る限りの全ての背景及び事実関係の詳細を甲に報告しなければならない。

(2)　報告要領の作成

総括者は、前号に規定する報告を迅速かつ的確に行うための報告要領を定めるとともに、当該報告をするに当たっての責任者、連絡担当者等を明らかにした連絡系統図を作成し、異動等があった場合は、速やかにこれを更新するものとする。

(3)　事故発生時の対処等

ア　対処体制及び手順

総括者は、秘密の漏えい、紛失、破壊等の事故が発生した場合の対処体制として、次の(ｱ)から(ｵ)までに掲げる事項を整備するとともに、当該対処体制における責任者及び対処手順を定めるものとする。

(ｱ)　事故への対処の準備、発見及び検知時の報告、監視及び分析、被害及び影響の抑制並びに局限、証拠の保存及び原因の究明並びに復旧までの各段階における対処体制（秘密取扱情報システムを原因とする事故にあっては、その対処体制を含む。）、責任及び手順を含めること。

(ｲ)　事故への対処に関する必要な情報の提供等を行う問い合わせ窓口等を設置し、関係社員に周知すること。

(ｳ)　事故の原因を特定するに足る記録を取得するとともに、デジタルフォレ

ンジック技術の利用等により事故への対処のために必要な情報を収集及び分析すること。

(ｴ)　秘密取扱情報システム及び秘密取扱情報システムに関係する情報システムの分析及び精査を行い、当該情報システム内の構成要素、データ、アカウント等の中から、悪意のあるソフトウェアへの感染又は不正アクセスなどの事故が発生した原因を特定すること。

(ｵ)　情報システムの脆弱性が発見又は検知された場合は、適切な対処を行うとともに、当該脆弱性を修正すること。

イ　証拠の収集

乙は、秘密の漏えい、紛失、破壊等の事故が発生した場合には、これらに関する証拠を収集し、速やかに甲へ提出しなければならない。

ウ　秘密保全規則等への反映

乙は、秘密の漏えい、紛失、破壊等の事故の対処において実施した事項について、秘密保全規則等の見直しに反映し、秘密保全規則等に新たに規定するときは、甲の確認を受けるものとする。

(4)　対処訓練の実施

総括者は、前号で作成した事故発生時の対処体制及び手順の有効性を確認するため、定期的に対処訓練を実施し、その結果を検証するものとする。この場合、その検証結果等を記録するものとする。

１０　物理的及び環境的セキュリティ

(1)　総括者は、秘密保全施設への関係社員以外の者の立入りを制限するとともに、秘密保全施設は、不正な立入りができない構造にすること。

(2)　総括者は、秘密保全施設の外側に隣接する建物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、秘密保全施設への不正な立入りを防止するため、次のアからウまでに掲げる措置を講じるものとする。

ア　保全外部区域への立入りを厳格に管理するため、立入を許可する者の名簿を作成し、定期的及び必要に応じて更新する等必要な措置を講じること。

イ　保全外部区域の外側境界に入退口を設置し、必要な管理措置により入退者を制限すること。

ウ　保全外部区域に敷地を指定した場合は、十分な高さ及び強度のあるフェンス等を設置するなど必要な措置を講じること。この際、秘密保全施設の外柵と共用する場合は、高さ等について秘密保全施設の基準を満たすこと。

(3)　総括者は、秘密保全施設への関係社員以外の者の立入りを制限するため、次のア及びイに掲げる入退室管理を確実に行うこと。

ア　秘密保全施設内における秘密保全を強化するために、総括者は、次の(ｱ)から(ｴ)までに掲げる内容を含む秘密保全の措置を講じること。

(ｱ)　関係社員その他甲により立入りを許可された者（１１(9)イに基づき甲が秘密保全施設への立入りを許可した外部委託を受ける者を含む。）以外の者を立ち入らせない。

(ｲ)　秘密保全施設の錠として、電子錠を利用する場合は、入退の記録を電子的に取得すること。この場合、電子的記録をもってイに規定する記録簿に代えることができるものとする。
(ｳ)　秘密保全施設への立入りの記録を定期的に精査し、記録すること。
(ｴ)　総括者は、秘密保全施設の鍵の保管及び接受、秘密保全施設の警備その他秘密保全施設における秘密保全を強化するため必要な細部の手続を定めること。

イ　総括者は、関係社員その他甲により立入りを許可された者が秘密保全施設に立ち入るときは、その者に所属、氏名、立入り目的その他の所要事項を記録簿に記載させるとともに、バッジ等を着用させ、立入りを管理すること。

(4)　総括者は、秘密を取り扱うパソコン等の設置に当たっては、次のアからクまでに掲げる項目の秘密取扱情報システム実装計画を作成し、甲の確認を受けること。

ア　秘密取扱情報システムのセキュリティを確保するための組織体制図（総括者等の秘密取扱情報システムのセキュリティに責任を有する者の具体的な責任の内容及び範囲を記載するものとする。）

イ　秘密取扱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

ウ　秘密取扱情報システムの構成図

エ　秘密のデータのデータフロー図

オ　１１(1)に規定する操作手順書

カ　１１(3)に規定するリスト

キ　１２(1)に規定するアクセス制御方針

ク　その他必要な事項

(5)　総括者は、秘密を取り扱うパソコン等を設置する際、設置場所における危険性を十分配慮して設置し、必要な保護措置を講じること。

(6)　総括者は、秘密取扱情報システム実装計画を定期的に確認し、当該秘密取扱情報システム実装計画を更新した場合は、甲に届け出るものとする。ただし、当該秘密取扱情報システム全体を更新する場合は、改めて甲の確認を受けるものとする。

(7)　総括者は、秘密に係る業務のために使用するパソコン等を秘密保全施設内に常設し、原則としてその持出しを禁止し、不正な持出し等を防止するため、必要な措置を講じること。ただし、保守等のため、やむを得ず持ち出さなければならない場合には、総括者は、パソコン等に記録されている秘密の漏えいを防止するための措置を講じること。この場合、総括者は、総括者又はその指定する者を含む複数の者が措置状況等を確認し、かつ、総括者又はその指定する者が持出しに関する記録簿に所要事項を記録した場合に限り、持出しを許可すること。

(8)　総括者は、秘密に係る業務のために使用するパソコン等として、無線ＬＡＮの機能が内蔵されているものの使用を禁止すること。

(9)　総括者は、秘密保全施設内に常設するパソコン及び記憶媒体のうち固定可能なものにあってはセキュリティワイヤなどにより固定の上、これを施錠することとし、又は固定することが困難なものにあってはロッカー等に保管の上、これを施錠すること。この場合、セキュリティワイヤ又はロッカー等の鍵は、総括者又はその指定する者が、その許可なく使用されることのないよう適切に管理すること。

(10)　総括者は、(4)の規定により設置したパソコン等以外のパソコン等及び携帯型情報通信機器については、秘密保全施設への持込みを原則として禁止すること。ただし、新設等のため、やむを得ず当該パソコン等又は携帯型情報通信機器の持込みが必要となった場合には、総括者は、次のアからカまでに掲げる要件を満たすことを確認した上で、事前に甲の許可を受けること。

ア　私有のパソコン等又は携帯型情報通信機器ではないこと。

イ　１１(3)のリストにないソフトウェアがインストールされていないこと。

ウ　無線ＬＡＮの機能を無効化すること。

エ　直前に悪意のあるソフトウェアを検知するための最新のソフトウェアでフルスキャンする体制にあること。

オ　パソコン等又は携帯型情報通信機器を使用して持ち出す際に、秘密のデータが保存されていないことを利用者が確認するとともに、総括者又は総括者が指定する者が点検する体制にあること。

カ　利用日時、利用者及び利用目的等を含む記録簿を整備する体制にあること。

(11)　秘密に係る業務に使用したパソコン等を処分又は修理するときは、次のア及びイに掲げる措置を実施すること。

ア　パソコン等は物理的に破壊し、又はいかなる方法においても記録又は保存された内容を再現することができない状態にし、秘密の漏えいを防止すること。

イ　処分又は修理に当たっては、総括者又はその指定する者が必ず監督し、その実施状況を記録すること。この場合、総括者の指定する者が当該監督を行ったときは、総括者に速やかに当該実施状況を報告すること。

１１　通信及び運用管理

(1)　総括者は、秘密保全施設内で使用するパソコン等に関する操作手順書を作成し、関係社員が常時参照できるようにすること。

(2)　総括者は、悪意のあるソフトウェアから秘密を保護するため、関係社員にそれぞれのパソコン等に対応する適切な最新のウィルス対策ソフトウェア等を用いて当該ソフトウェアを検出させ、及び検出時にその事実を適切に認知させるための対策を講じるとともに、当該ソフトウェアが認知された場合は、削除する等の措置を講じるとともに、その経緯を記録すること。特に、可搬記憶媒体については、少なくとも週１回以上当該措置を講じること。ただし、１週間以上使用されていない可搬記憶媒体については、使用する直前に当該措置を講じるものとする。

(3)　総括者は、秘密取扱情報システムにインストールできるソフトウェアのリストを作成し、当該リストにないソフトウェアが秘密取扱情報システムにインストールされていないか確認すること。
(4)　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配線接続した場合に限り構築できるものとし、当該有線については、破壊又は情報窃取を防止できる措置を講じること。
(5)　秘密取扱情報システムのネットワークは、秘密保全施設外への接続は、原則として禁止すること。
(6)　総括者は、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、整備及びアップデートを含む。以下同じ。）を定期的及び必要に応じて行うため、次のアからエまでに掲げる項目を含むシステムメンテナンス等計画を作成し、当該計画に基づき、メンテナンス等を実施するものとする。
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（秘密取扱情報システムにおけるソフトウェア、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。）
エ　その他メンテナンス等に必要な事項
(7)　総括者又はその指定する者は、前号のシステムメンテナンス等計画に基づきメンテナンス等の作業を行っている間、立会い及び必要な監視を行うこと。この場合において、総括者の指定する者が立会い、又は必要な監視を行ったときは、総括者の指定する者は、総括者に対し速やかに秘密保全上の注意点及び要求事項の遵守状況等について報告すること。
(8)　総括者又はその指定する者は、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等を記録すること。
(9)　秘密取扱情報システムのメンテナンス等に関する外部委託は、原則として禁止する。ただし、やむを得ず外部委託をしなければならない場合には、総括者は、少なくとも次のアからウまでに掲げる措置を講じること。
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、甲が、当該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、当該秘密取扱情報システムから秘密に係る情報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触することのないよう措置を講じること。
(10)　総括者は、装備品等秘密の保全に関する特約条項第５条第１項、特定秘密の保護に関する特約条項第９条第３項若しくは防衛装備庁における特定秘密の保護に関する特約条項第９条第３項又は特別防衛秘密の保護に関する特約条

項第５条第１項若しくは防衛装備庁における特別防衛秘密の保護に関する特約条項第５条第１項に規定する特定資料、特定図面等及び特定物件の複製等について、電子情報としてこれを行う場合には、可搬記憶媒体以外への保存を禁止すること。

(11)　総括者は、次のアからクまでに掲げる内容を含む可搬記憶媒体の取扱いに関する管理手順を作成し、関係社員に周知すること。

ア　秘密取扱可搬記憶媒体については、秘密取扱情報システム以外の情報システムへの接続を禁止すること。

イ　秘密取扱可搬記憶媒体を使用するときは、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。

ウ　秘密取扱可搬記憶媒体の貸出・返却に関する記録を残すこと。

エ　秘密取扱可搬記憶媒体に情報を記録するときは、秘匿すること。

オ　暗号については、電子政府推奨暗号等を使用するものとし、暗号鍵の厳格な管理方法に関すること。

カ　秘密取扱情報システムで取り扱うデータについては、データの記録をソフトウェアにより制御する等の技術上の措置を講じることにより、秘密取扱可搬記憶媒体以外の可搬記憶媒体への記録を原則として禁止すること。
ただし、秘密取扱情報システムの使用状況を記録する際は総括者の許可を得た場合のみ秘密取扱可搬記憶媒体以外の可搬記憶媒体を使用することができる。

キ　秘密取扱情報システムメンテナンス等可搬記憶媒体については、メンテナンスに係るデータを記録する場合のみ秘密取扱情報システム以外の情報システムに挿入又は接続することができる。

ク　秘密取扱可搬記憶媒体の内容の複製及び破棄手順に関すること。

１２　アクセス制御

(1)　総括者は、秘密保全施設内において秘密取扱情報システムを使用する場合には、関係社員が取り扱うことができる秘密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することにより、アクセス制御を行うこと。なお、アクセス制御方針は、次のアからオまでに掲げる項目を含めるものとする。

ア　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）の指定

イ　管理者用機能と利用者用機能を分離すること。

ウ　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。

エ　秘密取扱情報システムを構成する機器に対する識別及び情報システム利用者の認証に関すること。なお、秘密取扱情報システム利用者の認証は、多要素認証等の方法により秘密取扱情報システム利用者が特定されるよう設定すること。

オ　その他必要な事項

(2)　総括者は、関係社員による秘密取扱情報システムの利用可能機能へのアクセスを許可し、適切なアクセス権を付与するため、利用者としての登録及び登録の削除を行うこと。また、アクセスに対する有効な管理を維持するため、人事異動等の際においてはアクセス権の見直しを実施するほか、定期的な見直しを実施するとともに、速やかに見直しに応じた利用者としての登録及び登録の削除を行うこと。

(3)　総括者は、１１(3)に規定するリストにないソフトウェアの使用を制限するとともに、総括者が前号の規定により許可する関係社員以外の者がアクセスすることのないようアクセス権を厳格に管理すること。

(4)　総括者は、秘密取扱情報システムの使用状況の記録の編集など、操作に関する権利の割当てを制限し、関係社員のアクセス権を厳格に管理すること。

(5)　総括者は、責任の所在を明確にするために、秘密取扱情報システムを使用するすべての者に、各個人ごとの利用者ＩＤ（以下単に「利用者ＩＤ」という。）を保有させるとともに、パスワード設定をさせること。なお、パスワード設定においては、次のアからカまでに掲げる内容を含む必要な措置を講じ、その内容を１１(1)に規定する操作手順書に記載すること。

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し、定期的に変更すること。

エ　パスワードを亡失した場合の初期パスワードの配布に関すること。

オ　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。

カ　ログオン及びユーザセッションに関すること。

(6)　総括者は、秘密取扱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に、次のアからウまでに掲げる事項に留意し、秘密取扱情報システムの使用状況を記録し、保存すること。

ア　秘密取扱情報システムの使用状況の記録は、定期的に、及び必要に応じて点検すること。なお、点検結果の作成に当たっては、記録の内容（時系列の順序を含む。）を変更しないこと。

イ　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、秘密取扱情報システム及びデータへのアクセスの成否を記録すること。

ウ　記録及び記録を取得するツールを、不正なアクセス、改ざん又は削除から保護すること。

(7)　総括者は、必要に応じ、秘密取扱情報システムのパソコンの識別及び利用者の認証を適切に実施すること。

１３　検証・改善

(1)　総括者は、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、

秘密の管理状況及び教育内容等の秘密保全を確保するための各種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。
また、検証に際して、次のア及びイに掲げる事項を考慮したリスク査定を実施すること。
ア　特定資料又は特定物件及び秘密取扱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
イ　特定資料又は特定物件を取り扱う部署の内部のほか、秘密保全に影響を及ぼす恐れがあると認める範囲内で、自社の別の部署及び外部の組織（情報システムの保守を請け負う業者等を含む。）におけるリスクの特定、分析及び評価

(2)　総括者は、前号に規定された検証を実施した場合は、その結果を記録すること。

１４　検査及び調査の受入れ

(1)　乙は、関係簿冊及び秘密保全施設を含め、原則として、毎月１回以上秘密の保全状況について点検を行い、甲又は甲の代理者の検査を受けなければならない。

(2)　甲又は甲の代理者は、必要があると認めたときは、前号の検査を行うほか、秘密の保全の状況を検査し、又は必要な指示を乙に与えることができる。

(3)　乙は、契約履行後においても、秘密保全上必要があると甲が認めた場合は、甲又は甲の代理者の求めに応じ、甲又は甲の代理者が実施する検査及び調査を受け入れ、必要な協力をしなければならない。

１５　適用の特例

(1)　令和８年１０月１日以後の秘密を取り扱う契約（以下「適用日後契約」という。）において、乙が令和８年１０月１日以前の秘密を取り扱う契約（以下「適用日前契約」という。）において使用した秘密取扱情報システム（以下「旧秘密取扱情報システム」という。）を引き続き使用する場合であって、乙が当該旧秘密取扱情報システムに係る秘密取扱情報システム実装計画を既に作成し保全検査において確認されている場合は、令和１３年１月１日までの間は、改正後の１０(4)ウ及びカ、(6)、１１（3）及び(11)ア、カ及びキ並びに１２(3)及び(6)ア及びウまでの規定は適用しないものとする。

(2)　乙は、適用日前契約と適用日後契約が重複して適用される場合、適用日前契約についても、改正後の９(3)ア(ｱ)から(ｵ)まで、１０(10)アからカまで、並びに１２(1)イ及び(5)エの規定を適用するものとする。

(3)　乙は、第１号の規定において令和１３年１０月１日まで適用しないものとされた改正後の規定を適用しようとする場合は、１０(4)の規定に基づき秘密取扱情報システム実装計画を作成し、甲の確認を受けるものとする。

(4)　第１号の規定にかかわらず、乙は、特定の環境を維持する等のやむを得ない理由により、令和１３年１０月１日以後も、旧秘密取扱情報システムに改正後

の規定を適用できない場合は、適用できない規定及びその理由を明らかにした上で、甲の承認を得ることで引き続き当該規定を適用しないことができる。