別紙第１３

装備品等の調達に係る秘密保全対策ガイドライン

平成２６年１２月

防　　衛　　省

目　　次

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（秘密保全に関する訓令（平成１９年防衛省訓令第３６号）第２条第１項に規定する秘密、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（秘密の保全に関する特約条項（秘密保全に関する訓令（平成１９年防衛省訓令第３６号）第２９条第１項に規定する秘密の保全に関する規定をいう。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（平成２６年防衛省訓令第６４号）第３７条第１項に規定する特約条項をいう。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）第２７条第１項に規定する秘密保持に関する規定をいう。以下同じ。）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)　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。

(3)　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。

(4)　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。

(5)　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。

(6)　特定資料又は特定物件とは、秘密の保全に関する特約条項第１条第２項、特

定秘密の保護に関する特約条項第１条第２項又は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をいう。

(7)　外部委託とは、情報システムに関する保守等の業務の一部又は全部を第三者に請け負わせることをいう。

(8)　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)　秘密に係る情報の取扱いにおいて、パソコン、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（第５(5)、第７(3)オ、第８(3)から(8)まで、第９及び第１０）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。

(3)　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、秘密保全規則等を秘密の取扱いの業務に従事する者（以下「関係社員」という。）に確実に周知すること。

５　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こと。

(2)　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。

(3)　総括者は、秘密保全に係る関係部署及び従業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。

(4)　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。

(5)　秘密保全施設内で使用する情報システムに関する外部委託は、原則として禁止する。ただし、保守等のため、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エまでに掲げる措置を講ずること。

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保守等に当たっては、当該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ずること。

エ　総括者又はその指定する者は、外部委託を受けた者が保守等の作業を行っている間、立ち会い、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ち会い、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外部委託を受けた者の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。

６　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「作成等」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。以下この号において同じ。）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、関係簿冊を秘密保全の責任がある期間（秘密等の保全又は保護に関する違約金条項第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。）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。

(2)　総括者は、特定資料又は特定物件の作成等を確実に実施するため、関係社員が従事する作成等の作業ごとに、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。

7　人的セキュリティ

(1)　部門責任者等は、秘密を取り扱うのにふさわしい者をもって充てること。

(2)　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誓約を文書で行わせること。また、当該文書には、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。

(3)　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、関係社員その他の従業員全てに対し、次のアからオまでに掲げる内容を含む教育を定期的に行い、その結果を甲に届け出ること。

ア　秘密保全の重要性、意義（秘密保全意識の涵養を含む。）

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（特に記憶媒体を介した感染）を防止するための対策及び感染した場合の対処手順

(4)　総括者は、秘密の漏えい、紛失、破壊等の事故に対して、迅速、効果的及び整然とした対処を確実に行うこと。この場合、総括者又はその指定する者は、適切な連絡経路を通じて、直ちに把握し得る限りの全ての内容を甲に報告するとともに、その後速やかにその詳細を報告することとし、そのため、総括者は、必要な手順を作成すること。なお、手順には、報告に当たっての責任者及び連絡担当者等を明らかにした連絡系統図を作成することとし、異動等のあった場合にはこれを更新すること。

8　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）及び（イ）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（第５項（５）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)　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。

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。

(3)　総括者は、パソコン等の設置に当たっては、設置場所における危険性を十分配慮して設置し、及び保護すること。

(4)　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すること。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、持ち出しを許可すること。

(5)　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。

(6)　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。

(7)　総括者は、(3)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の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、やむを得ずパソコン等の持込みが必要となった場合には、総括者は、持込むパソコン等について、インストールされているソフトウェア等を確認するなど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が持込みに関する記録簿に所要事項を記録し、かつ、持ち込むパソコン等が私有品ではないことを確認した場合に限り、持込みを許可すること。

(8)　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。

９　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を文書化し、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ずること。特に、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ずること。ただし、１週間以上使用されていない記憶媒体については、使用する直前に当該措置を講ずるものとする。

(3)　総括者は、業務に必要なソフトウェアの使用状況を確認するとともに、必要のないソフトウェアのインストールをさせないこと。

(4)　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、秘密保全施設外への接続は、いかなる場合も禁止すること。

(5)　総括者は、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項に規定する特定資料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、記憶媒体以外への保存を禁止すること。

(6)　総括者は、次のアからエまでに掲げる内容を含む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　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。

イ　記憶媒体の貸出・返却に関する記録を残すこと。

ウ　記憶媒体に情報を記録するときは、秘匿すること。

エ　記憶媒体の内容の複製及び破棄手順に関すること。

１０　アクセス制御

(1)　総括者は、秘密保全施設内において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、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規定することにより、アクセス制御を行うこと。

(2)　総括者は、関係社員による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とともに、そのほか定期的な見直しを実施すること。

(3)　総括者は、情報システムの操作性を改善するためのソフトウェアの使用を制限するとともに、情報システムの使用状況の記録等に必要なソフトウェア又はデータの誤用又は悪用を防止するため、総括者が(2)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、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、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。パスワード設定においては、次のアからエまでに掲げる内容を含む必要な措置を講じること。

ア　利用者にパスワードの変更手順を理解させる。

イ　利用者にパスワードの変更を実施させる。

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。

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。

(6)　総括者は、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に、以下の事項に留意し、情報システムの使用状況を記録し、保存すること。

ア　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。

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、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。

１１　検証・改善

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、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。