防経装第９２４６号
２１．７．３１
一部改正　防経装第１５５６９号
２３．１２．２８
一部改正　防官文（事）第１８号
２７．１０．１
一部改正　防装庁（事）第１号
令和元年５月７日
一部改正　防装庁（事）第１６５号
令和２年３月３１日

大臣官房長
各局長
施設等機関の長
各幕僚長
情報本部長　殿
技術研究本部長
装備施設本部長
防衛監察監
各地方防衛局長

事務次官
（公印省略）

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（通達）

標記について、下記のとおり定められ、平成２２年４月１日から施行することとされたので、遺漏のないよう措置されたい。

なお、装備品等の調達における情報セキュリティの確保について（防管装第１５８３号。１８．３．６）、装備品等の調達における情報セキュリティの確保に関する特約条項について（防管装第１５８４号。１８．３．６）、「将来ＳＡＭ」関連情報の流出事案に係る関係企業との契約の取扱いについて（防管航第１４９３号。１８．３．２）、「将来ＳＡＭ」関連情報の流出

事案に係る関係企業との契約の取扱いについて（防経シ第９０１５号。１８．９．２２）及び「将来ＳＡＭ」関連情報の流出事案に係る関係企業との契約の取扱いについて（防経装第３２７２号。１９．３．２９）は、平成２２年３月３１日付けをもって廃止することとされたので、併せて通達する。

記

１　目的

この通達は、装備品等及び役務の調達において、防衛関連企業で取り扱われる保護すべき情報の保全のため必要な措置を定めることを目的とする。

２　定義

この通達において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

⑴　保護すべき情報　装備品等及び役務の調達に関する情報のうち、取扱い上の注意を要する文書等及び注意電子計算機情報の取扱いについて（防防調第４６０８号。１９．４．２７）第１に規定する「取扱い上の注意を要する文書等」及び同通達第８に規定する「注意電子計算機情報」並びにこれらの情報を利用して作成される情報をいう。

⑵　情報セキュリティ　保護すべき情報の機密性、完全性及び可用性を維持することをいう。

⑶　機密性　認可されていないものに対して、情報を使用不可又は非公開にする特性をいう。

⑷　完全性　情報の正確さ及び完全さを保護する特性をいう。

⑸　可用性　認可されたものが要求したときに、アクセス及び使用が可能である特性をいう。

⑹　大臣官房長等　装備品等及び役務の調達実施に関する訓令（昭和４９年防衛庁訓令第４号）第２条第２号に規定する大臣官房長等をいう。

⑺　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。

⑻　防衛関連企業　保護すべき情報を取り扱う企業（保護すべき情報を取り扱う下請負者を含む。）をいう。

⑼　下請負者　契約の履行に係る作業に従事するすべての事業者（防衛省と直接契約関係にある者を除く。）をいう。

⑽　第三者　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。

3　仕様書等への引用

大臣官房長等及び防衛装備庁長官は、装備品等及び役務の調達に当たり、保護すべき情報が含まれ、又は含まれることが予想される場合には、仕様書等（仕様書及び仕様書を補足する細部資料をいう。以下同じ。）に別添に定める調達における情報セキュリティ基準（以下「本基準」という。）を引用するものとする。

4　特約条項

契約担当官等は、前項に規定する仕様書等による契約については、別紙の特約条項を適用するものとする。ただし、これにより難い場合は、第１２項の規定により防衛装備庁長官と協議するものとする。

5　取扱者名簿の受領

⑴　契約担当官等は、防衛関連企業が取扱者名簿（保護すべき情報に接する者の氏名、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。以下同じ。）を届け出たときは、調達要求をする者（以下「要求元」という。）に当該名簿に係る必要な措置について照会するものとする。

⑵　要求元は、前号の照会を受けたときは、必要に応じ、防衛装備庁装備政策部装備保全管理官に照会することができる。

⑶　契約担当官等は、第１号及び前号の規定による照会の回答を踏まえ、取扱者名簿を確認するものとする。

⑷　契約担当官等は、防衛関連企業に対し、取扱者名簿に変更があるときは、速やかに、その変更内容を届け出るよう求めるものとする。

6　該当部分の明示

⑴　装備品等及び役務の調達に関係する職員は、防衛関連企業に対し保護すべき情報を交付及び伝達する場合には、保護すべき情報を記録する箇所に、下線を引いて明示する、枠で囲んで明示する又は文頭及び文末に括弧を付して明示する等の措置を採るとともに、保護すべき情報のリスト等を作成し、併せて交付するものとする。

⑵　該当部分の明示に当たっては、行政機関の保有する情報の公開に関する法律（平成１１年法律第４２号）第５条に規定する不開示情報が含まれないことが明らかな部分に対して指定を行わない等、その必要性を十分に検討するものとする。

⑶　防衛関連企業において新たに作成し、又は製作する情報が保護すべき

情報に該当し、契約の目的物に当該情報が含まれる又は含まれることが予想される場合は、当該契約の履行の一環として収集、整理、作成等した一切の情報についても保護すべき情報として指定しなければならない。

⑷　防衛関連企業は、前号の規定により指定した情報のうち、防衛省が保護すべき情報には当たらないと確認した情報があった場合には、当該指定を解除することができる。

7　監査

⑴　契約担当官等は、防衛関連企業の情報セキュリティ基本方針、情報セキュリティ基準及び情報セキュリティ実施手順（本基準第２項第１０号から第１２号までに規定する「情報セキュリティ基本方針」、「情報セキュリティ基準」及び「情報セキュリティ実施手順」をいう。以下同じ。）が本基準に適合しているかについて確認するとともに、情報セキュリティ実施手順に基づく実施状況の監査を実施するものとし、契約履行後においても、必要に応じ、監査を実施するものとする。

⑵　前号に規定する監査の実施要領は、防衛装備庁長官が定めるものとする。

⑶　第１号の規定にかかわらず、契約担当官等は、締結した契約における情報セキュリティに関する監査等（監査及び情報セキュリティ基本方針、情報セキュリティ基準及び情報セキュリティ実施手順の確認をいう。以下同じ。）の実施に当たっては、必要に応じ、防衛装備庁長官及び監査等の対象となる防衛関連企業の事業所、工場等の所在地を管轄区域とする地方防衛局長に協力を依頼するものとする。

⑷　契約担当官等又は地方防衛局長が情報セキュリティに関する監査等を行うに当たっては、第２号に定める実施要領によるものとする。

8　特約条項の特例措置

契約担当官等は、一の装備品等及び役務の調達の計画が複数年度にわたり同一の相手方と契約する計画である場合は、第４項の規定にかかわらず、別紙の特約条項の規定を緩和することができる。

9　普及及び推進

装備品等の調達における情報セキュリティ検討委員会（装備品等の調達における情報セキュリティ検討委員会設置要綱について（防管装第４５０３号。１７．６．６）別紙の第１に規定する委員会をいう。）は、防衛省の装備品等及び役務の調達における情報セキュリティ対策について普及及び推進を図るものとする。

１０　協力

⑴　大臣官房長等及び防衛装備庁長官は、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のため相互に緊密に連携し協力するものとする。

⑵　契約担当官等は、締結した契約における情報セキュリティに関し次に掲げる事項について、必要に応じ、防衛装備庁長官及び監査等の対象となる防衛関連企業の事業所、工場等の所在地を管轄区域とする地方防衛局長に協力を依頼するものとする。

ア　保護すべき情報の第三者に対する開示の申請に関すること。

イ　下請負者を使用する場合の届出に関すること。

ウ　事故発生時の調査に関すること。

１１　適用除外

この通達の規定は、防衛省が直接又は輸入業者を通じて外国から行う装備品等及び役務の調達（日本国とアメリカ合衆国との間の相互防衛援助協定に基づく有償援助による装備品等及び役務の調達を含む。）には適用しない。

１２　協議

大臣官房長等は、この通達に定める事項の実施に当たり疑義が生じた場合には、その都度、防衛装備庁長官と協議するものとする。

１３　その他

本通達の実施に関し必要な細部事項は、防衛装備庁長官が別に定めるものとする。

添付書類：別紙

調達における情報セキュリティ基準

別紙

装備品等及び役務の調達における情報セキュリティの確保に関する特約条項

（情報セキュリティ基本方針等の確認）

第１条　乙は、契約締結後、速やかに、仕様書等（仕様書及び仕様書を補足する細部資料をいう。以下同じ。）に定めるところにより、情報セキュリティ基本方針及び情報セキュリティ基準（甲の定める「調達における情報セキュリティ基準」（以下「本基準」という。）第２項第１０号及び第１１号に規定する「情報セキュリティ基本方針」及び「情報セキュリティ基準」をいう。以下同じ。）を作成し、甲の定める本基準に適合していることについて甲の確認を受けなければならない。ただし、既に甲の確認を受けた情報セキュリティ基本方針及び情報セキュリティ基準と同一である場合は、特別な指示がない限り、届出をすれば足りる。

２　乙は、前項により甲の確認を受けた情報セキュリティ基本方針及び情報セキュリティ基準を変更しようとするときは、あらかじめ、当該変更部分が甲の定める本基準に適合していることについて甲の確認を受けなければならない。

３　乙は、甲の確認を受けた情報セキュリティ基本方針及び情報セキュリティ基準に基づき、情報セキュリティ実施手順（本基準第２項第１２号に規定する「情報セキュリティ実施手順」をいう。以下同じ。）を作成し、甲の定める本基準に適合していることについて甲の確認を受けなければならない。ただし、既に甲の確認を受けた情報セキュリティ実施手順と同一である場合は、特別な指示がない限り、届出をすれば足りる。

４　第２項の規定は、情報セキュリティ実施手順を変更する場合に準用する。

５　甲は、乙に対して情報セキュリティ基本方針、情報セキュリティ基準及び情報セキュリティ実施手順並びにそれらが引用している文書の提出、貸出、又は閲覧を求めることができる。

（保護すべき情報の取扱い）

第２条　乙は、前条において甲の確認を受けた情報セキュリティ基本方針、情報セキュリティ基準及び情報セキュリティ実施手順に基づき、この契約に関する保護すべき情報（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（防経装第９２４６号。２１．７．３１）第２項第１号に規定する「保護すべき情報」をいう。以下同じ。）を取り扱わなければならない。

（保護すべき情報の漏えい等に関する乙の責任）

第３条　乙は、乙の従業員又は下請負者（契約の履行に係る作業に従事するすべての事業者（乙を除く。）をいう。）の故意又は過失により保護すべき情報の漏えい、紛失、破壊等の事故があったときであっても、契約上の責任を免れることはできない。

（開示の申請及び届出）

第４条　乙は、やむを得ず保護すべき情報を第三者に開示する場合には、あらかじめ、開示先において情報セキュリティが確保されることを付紙様式に定める確認事項により確認した上、書面により甲の許可を受けなければならない。

２　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、保護すべき情報をその対象から除く措置を講

じなければならない。
３　乙は、契約の履行に当たり、保護すべき情報を下請負者に取り扱わせる場合には、あらかじめ、付紙様式に定める確認事項によって、当該下請負者において情報セキュリティが確保されることを確認し、その結果を甲に届け出なければならない。ただし、輸送その他の保護すべき情報を知り得ないと乙が認める業務を請け負わせる場合は、この限りではない。
４　第１項及び前項の規定は、乙が保護すべき情報を開示した第三者及び下請負者について準用する。この場合において、当該第三者及び下請負者は、乙を経由して甲の承認を受けなければならない。

（監査）
第５条　甲は、仕様書等に定める情報セキュリティ対策に関する監査を行うことができる。
２　甲は、前項に規定する監査を行うため、甲の指名する者を乙の事業所、工場その他の関係場所に派遣することができる。
３　甲は、第１項に規定する監査の結果、乙の情報セキュリティ対策が情報セキュリティ基本方針等（本基準第２項第１３号に規定する「情報セキュリティ基本方針等」をいう。以下同じ。）を満たしていないと認められる場合は、その是正のため必要な措置を講じるよう求めることができる。
４　乙は、前項の規定による甲の求めがあったときは、速やかに、その是正措置を講じなければならない。
５　前各項の規定は、乙の下請負者について準用する。ただし、第３項に規定する甲が行う是正のための求めについては、乙に対し直接行うものとする。
６　乙は、甲が乙の下請負者に対し監査を行うときは、甲の求めに応じ、必要な協力をしなければならない。

（事故等発生時の措置）
第６条　乙は、保護すべき情報の漏えい、紛失、破壊等の事故が発生したときは、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、その後速やかにその詳細を甲に報告しなければならない。
２　次に掲げる場合において、乙は、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、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。
⑴　保護すべき情報が保存されたサーバ又はパソコン（以下「サーバ等」という。）に悪意のあるコード（情報システムが提供する機能を妨害するプログラムの総称であり、コンピュータウイルス及びスパイウェア等をいう。以下同じ。）への感染又は不正アクセスが認められた場合
⑵　保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染が認められた場合
３　第１項に規定する事故について、それらの疑い又は事故につながるおそれのある場合は、乙は、適切な措置を講じるとともに、速やかに、その詳細を甲に報告しなければならない。
４　前３項に規定する報告のほか、保護すべき情報の漏えい、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、乙は、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速やかに甲に報告しなければならない。
５　前各項に規定する報告を受けた甲による調査については、前条の規定を準用する。
６　乙は、第１項に規定する事故がこの契約及び関連する装備品等の運用に与える影

響等について調査し、その措置について甲と協議しなければならない。
７　第１項に規定する事故が乙の責めに帰すべき事由によるものである場合には、前項に規定する協議の結果、とられる措置に必要な費用は、乙の負担とする。
８　前項の規定は、甲の損害賠償請求権を制限するものではない。

（契約の解除）
第７条　甲は、乙の責めに帰すべき事由により前条第１項に規定する事故が発生し、この契約の目的を達することができなくなった場合は、この契約の全部又は一部を解除することができる。
２　前項の場合においては、主たる契約条項の契約の解除に関する規定を準用する。

（契約履行後における乙の義務等）
第８条　第２条、第３条、第５条及び第６条の規定は、契約履行後においても準用する。ただし、当該情報が保護すべき情報でなくなった場合は、この限りでない。
２　甲は、本基準第７項第２号イの規定による契約終了後における乙に対する保護すべき情報の返却、提出等の指示のほか、業務に支障が生じるおそれがない場合は、乙に保護すべき情報の破棄を求めることができる。
３　乙は、前項の求めがあった場合において、保護すべき情報を引き続き保有する必要があるときは、その理由を添えて甲に協議を求めることができる。

付紙様式

情報セキュリティ対策実施確認書

1　下請負者名又は開示先事業者名等

(1) 事業者名：

(2) 対象部門等名：

(3) 請負又は開示予定年月日：

(4) 業務の実施予定場所※：

※（請負事業者又は開示先事業者の業務の実施予定場所を記入）

2　防衛省による情報セキュリティ実地監査の受査状況

(1) 下請負者又は開示先事業者

ア　監査年月日：

イ　監査結果：

ウ　監査結果の文書番号及び年月日：

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

ア　監査年月日：

イ　監査結果：

ウ　監査結果の文書番号及び年月日：

3　下請負者又は開示先事業者に対する確認事項（上記２における監査年月日が請負年月日の属する年度又はその前年度の場合は、下線を引いた事項を除き確認を省略することができる。）

番号	確認事項	実施／未実施	実施状況の確認方法　又は　未実施の理由
1	**5(1)情報セキュリティ基本方針及び情報セキュリティ基準** ・保護すべき情報を取り扱う可能性のある全ての者に周知することを定めていること。 ・必要に応じて下請負者へ周知することを定めていること。		
2	**5(2)情報セキュリティ基本方針等の見直し** ・情報セキュリティ基本方針等を定期的並びに重大な変化及び事故が発生した場合、見直しを実施し、必要に応じて変更することを定めていること。		
3	**6(1)ア　情報セキュリティに対する経営者等の責任** ・経営者等が情報セキュリティ基本方針等を承認することを定めていること。 ・取扱者以外の役員（持分会社にあっては社員を含む。以下同じ。）、管理職員等を含む従業員その他の全ての構成員について、取扱者以外の者は保護すべき情報に接してはならないことを定めていること。 ・職務上の下級者等に対して、保護すべき情報の提供を要求してはならないことを定めていること。		
4	**6(1)イ　責任の割当て** ・総括責任者を置くことを定めていること。 ・管理責任者を置くことを定めていること。		
5	**6(1)ウ　守秘義務** ・取扱者との間で守秘義務を定めた契約又は合意をすることを定めていること。 ・定期的並びに状況の変化及び事故が発生した場合、要求事項の見直しを実施し、必要に応じて修正することを定めていること。		
6	**6(1)エ　情報セキュリティの実施状況の監査** ・情報セキュリティの実施状況について、定期的及び重大な変化が発生した場合、監査を実施し、必要に応じて是正措置をとることを定めていること。 ・定期的及び重大な変化が発生した場合において、監査を適切に実施していること。 ・監査の実施に関し、その結果を保存していること。 ・監査の結果、必要な是正措置が適切にとられていること。		
7	**6(2)　保護すべき情報を取り扱う下請負者** ・保護すべき情報を請け負わせる場合には、契約上の義務に本基準に基づいた実施を含めるとともに、確認を実施し、防衛省へ届け出ることを定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法　又は　未実施の理由
8	**6(3)ア　第三者への開示の禁止** ・第三者（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。以下同じ。）への開示又は漏えいをしてはならないことを定めていること。 ・保有し、又は知り得た情報を第三者との契約において伝達、交換、共有その他提供する約定があるときは、保護すべき情報をその対象から除く措置を定めていること。 ・やむを得ない場合は、あらかじめ書面による防衛省の許可を得ることを定めていること。		
9	**6(3)イ　第三者に関係したリスクの管理** ・第三者の取扱施設への立入りを許可する場合、リスクを明確にした上対策を定めていること。		
10	**6(3)ウ　第三者に対する立入りの許可** ・第三者へ立入りを許可する場合の手順を定めていること。		
11	**7(1)　分類の指針** ・保護すべき情報を明確に分類できる分類体系を定めていること。		
12	**7(2)ア　保護すべき情報の目録** ・目録の作成及び維持することを定めていること。 ・目録が適切に維持されていること。		
13	**7(2)イ　取扱いの管理策** ・取扱施設で取り扱うことを定めていること。 ・接受等を記録することを定めていること。 ・個人が所有する情報システム及び可搬記憶媒体で取り扱ってはならないことを定めていること。 ・（やむを得ない場合）事前に防衛省の許可を得る手続を定めていること。 ・防衛省の指示に従い、返却、提出、破棄等必要な措置をとることを定めていること。 ・防衛省から、保護すべき情報の破棄を求められた場合であって、当該情報を引き続き保有する必要がある場合には、その理由を添えて、発注者(防衛省との直接契約関係にある防衛関連企業をいう。以下同じ。)を経由して防衛省(調達要求元)に協議を求めることができることを定めていること。 ・接受等が適切に記録されていること。		
14	**7(2)ウ　保護すべき情報の保管等** ・保護すべき情報は、施錠したロッカー等において保管することを定めていること。 ・ロッカー等の鍵を適切に管理（無断での使用を防止）することを定めていること。 ・施錠したロッカー等において保管していること。 ・ロッカー等の鍵を適切に管理していること。		
15	**7(2)エ　保護すべき情報の持ち出し** ・持ち出しに伴うリスクを回避することができると判断する場合の判断基準を定めていること。 ・持ち出しする場合は記録することを定めていること。 ・持ち出しを記録していること。		
16	**7(2)オ　保護すべき情報の破棄** ・復元できない方法による破棄を定めていること。 ・破棄したことを記録することを定めていること。 ・破棄を記録していること。		
17	**7(2)カ　該当部分の明示** ・保護すべき情報を作成、製作又は複製した場合、保護すべき情報である旨の表示を行うことを定めていること。 ・契約の目的物が保護すべき情報を含むものである場合には、当該契約の履行の一環として収集、整理、作成等した一切の情報について、防衛省が当該情報を保護すべき情報には当たらないと確認するまでは、保護すべき情報として取り扱うことを定めていること。 ・防衛関連企業は、保護すべき情報の指定を解除する必要がある場合には、その理由を添えて、発注者を経由して防衛省（調達要求元）に協議を求めることができることを定めていること。 ・保護すべき情報を記録する箇所を明示する及び明示の方法を定めていること。 ・適切に表示及び明示されていること。		
18	**8(1)　経営者等の責任** ・経営者等は取扱者の指定の範囲を必要最小限とするとともに、ふさわしいと認める者を充て、情報セキュリティ基本方針等を遵守させることを定めていること。 ・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ないことを定めていること。		
19	**8(2)　取扱者名簿** ・取扱者名簿を作成し、又は更新したときは、発注者を経由して各取扱者について防衛省に届け出て同意を得ることを定めていること。 ・取扱者名簿には、取扱者の氏名、生年月日、所属する部署、役職、国籍等が記載されていること。 ・取扱者名簿には、保護すべき情報に接する全ての者（保護すべき情報に接する役員（持分会社にあっては社員を含む。以下同じ。）、管理職員、派遣社員、契約社員、パート、アルバイト等を含む。この場合において、当該者が、自らが保護すべき情報に接しているとの認識の有無を問わない。）が記載されていること。		
20	**8(3)　情報セキュリティ教育及び訓練** ・定期的な教育及び訓練の実施を定めていること。 ・定期的に行う教育には、組織の方針、取扱手順、関連する法令その他なりすましメール等による悪意のあるコード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等に関する内容が含まれていること。 ・定期的に教育及び訓練を実施していること。 ・教育及び訓練の実施状況を記録し、保管していること。		

番号	確認事項	実施／未実施	実施状況の確認方法　又は　未実施の理由
21	**8(4)　違反者への対処方針** ・情報セキュリティ基本方針等に違反した取扱者に対する対処方針及び手続を定めていること。		
22	**8(5)　取扱者の責任** ・在職中及び離職後においても、知り得た保護すべき情報を第三者に漏えいしてはならないことを定めていること。		
23	**8(6)　保護すべき情報の返却** ・保護すべき情報に接する必要が無くなった場合は、管理者へ返却することを定めていること。 ・保護すべき情報は、管理者へ返却されていること。		
24	**9(1)ア　取扱施設の指定** ・取扱施設を定めていること。		
25	**9(1)イ　物理的セキュリティ境界** ・物理的セキュリティ境界を用いることを定めていること。		
26	**9(1)ウ　物理的入退管理策** ・取扱施設への立入りは、許可された者だけに制限することを定めていること。 ・第三者の立入りを記録することを定めていること。 ・立入記録の保管を定めていること。 ・第三者の立入りを記録し、保管していること。		
27	**9(1)エ　取扱施設での作業** ・機密性に配慮し作業することを定めていること。 ・通信機器及び記録装置を利用する場合は、経営者等の許可を得ること定めていること。		
28	**9(2)ア　保護システムの設置及び保護** ・保護システムへの保護措置を実施することを定めていること。 ・保護システムへ保護措置が実施されていること。		
29	**9(2)イ　保護システムの持ち出し** ・持ち出しに伴うリスクを回避することができると判断する場合の基準を定めていること。 ・持ち出しする場合は記録することを定めていること。 ・持ち出しを記録していること。		
30	**9(2)ウ　保護システムの保守及び点検** ・第三者による保守及び点検を行う場合は、必要な処置を実施することを定めていること。 ・第三者による保守及び点検時において、必要な処置が実施されていること。		
31	**9(2)エ　保護システムの破棄又は再利用** ・保護すべきデータが復元できない状態であることを点検し、物理的に破壊したのち、破棄し、その旨を記録することを定めていること。 ・復元できない状態であることを点検した後、再利用することを定めていること。 ・破棄を記録していること。		
32	**10(1)　操作手順書** ・操作手順書を整備し、維持することを定めていること。 ・操作手順書には、 ①可搬記憶媒体へ保存時の手順②可搬記憶媒体及び保護システムの破棄又は再利用の手順③電子メール等での伝達の手順④セキュリティに配慮したログオン手順についての記述又は引用がなされていること。		
33	**10(2)　悪意のあるコードからの保護** ・保護システムを最新の状態に更新されたウィルス対策ソフト等を用いて、少なくとも週１回以上フルスキャンを行うことなどにより、悪意のあるコードから保護することを定めていること。（なお、１週間以上電源の切られた状態にあるサーバ又はパソコンについては、再度の電源投入時に当該処置を行うことで可。） ・ウイルス対策ソフト等を最新の状態に更新していること。 ・保護システムをウイルス対策ソフト等により、少なくとも週１回以上フルスキャンしていること。（１週間以上電源の切られた状態にあるサーバ及びパソコンについては、再度の電源投入時に当該処置を行うことで可。）		
34	**10(3)　保護システムのバックアップの管理** ・可搬記憶媒体へのバックアップを実施する場合、調達における情報セキュリティ基準7(2) 及び10(4) に添った取扱いをすることを定めていること。		
35	**10(4)ア　可搬記憶媒体の管理** ・保護すべき情報を保存した可搬記憶媒体を施錠したロッカー等により集中保管することを定めていること。 ・ロッカー等の鍵を適切に管理することを定めていること。 ・保護すべき情報とそれ以外を容易に区別できる処置をすることを定めていること。 ・施錠したロッカー等において集中保管していること。 ・ロッカー等の鍵を適切に管理していること。 ・保護すべき情報とそれ以外を容易に区別できる処置がされていること。		
36	**10(4)イ　可搬記憶媒体への保存** ・可搬記憶媒体へ保存する場合、暗号技術を用いることを定めていること。		
37	**10(4)ウ　可搬記憶媒体の破棄又は再利用** ・保護すべきデータが復元できない状態であることを点検し、物理的に破壊したのち、破棄し、その旨を記録することを定めていること。 ・復元できない状態であることを点検した後、再利用することを定めていること。 ・破棄を記録していること。		

番号	確認事項	実施／未実施	実施状況の確認方法　又は　未実施の理由
38	**１０(5)ア　保護すべき情報の伝達** ・伝達に伴うリスクから保護できると判断する場合の基準を定めていること。		
39	**１０(5)イ　伝達及び送達に関する合意** ・保護すべき伝達及び送達は、守秘義務を定めた契約又は合意した相手に対してのみ行うことを定めていること。		
40	**１０(5)ウ　送達中の管理策** ・保護すべき文書等を送達する場合、許可されていないアクセス及び不正使用等から保護する方法を定めていること。		
41	**１０(5)エ　保護すべきデータの伝達** ・保護すべきデータを伝達する場合には、保護すべきデータが既に暗号技術を用いて保存されている、通信事業者の回線区間に暗号技術を用いる又は電子メール等に暗号技術を用いることのいずれかによって、保護すべきデータを保護しなければならないことを定めている。（漏えいのおそれのない取扱施設内で有線での伝達をする場合を除く。）。 ・電子メール等による伝達など、暗号技術を用いるに当たって個人の操作を要するものについて、その旨の教育を行うなど、確実な実施のための方策がとられていること。		
42	**１０(6)　外部からの接続** ・外部からの接続を許可する場合は、利用者の認証を行い、及び暗号技術を用いることを定めていること。		
43	**１０(7)　電子政府推奨暗号等の利用** ・暗号技術を用いる場合には、電子政府推奨暗号等を用いることを定めていること。 ・やむを得ず電子政府推奨暗号等を使用できない場合は、その他の秘匿化技術を用いることを定めていること。		
44	**１０(8)　ソフトウェアの導入管理** ・導入するソフトウェアの安全性を確認することを定めていること。		
45	**１０(9)　システムユーティリティの使用** ・システムユーティリティの使用を制限することを定めていること。		
46	**１０(10)　技術的脆弱性の管理** ・脆弱性に関する情報を取得すること及び適切に対処することを定めていること。		
47	**１０(11)ア　監査ログ取得** ・利用者の保護すべき情報へのアクセス及び例外処理を記録した監査ログを取得することを定めていること。		
48	**１０(11)イ　監査ログの保管** ・取得した監査ログを記録のあった日から少なくとも３か月以上保存するとともに、定期的に点検することを定めていること。 ・監査ログを記録のあった日から３か月以上保存していること。		
49	**１０(11)ウ　監査ログの保護** ・監査ログを改ざん及び許可されていないアクセスから保護することを定めていること。		
50	**１０(11)エ　クロックの同期** ・保護システム及びネットワークを通じて保護システムにアクセス可能な情報システムの日付及び時刻を定期的に合わせることを定めていること。		
51	**１０(11)オ　保護すべきデータの監視** ・保護システムが共有ネットワーク（インターネット等）へ物理的に接続されている場合は、共有ネットワークを通じた保護すべきデータの社外漏えいを未然に防止することを可能とする常時監視を行わなければならない。 ・保護すべきデータが、共有ネットワークを通じて社外へ漏えいすることを未然に防止することを可能とする常時監視を行っていること。		
52	**１１(1)　アクセス制御方針** ・職務内容に応じて、保護すべき情報、取扱施設及び保護システムへのアクセス制御方針を定めていること。 ・定期的並びに重大な変化及び事故が発生した場合、見直しを実施し、必要に応じて修正することを定めていること。		
53	**１１(2)ア　利用者の登録管理** ・保護システムの利用者の登録及び登録削除をすることを定めていること。		
54	**１１(2)イ　パスワードの割当て** ・初期又は仮パスワードは、容易に推測されないものとするとともに、機密性を配慮した方法で配布することを定めていること（パスワードより強固な手段を併用又は採用している場合はこの限りでない。）。		
55	**１１(2)ウ　管理者権限の管理** ・管理者権限の利用は必要最低限とすることを定めていること。		
56	**１１(2)エ　アクセス権の見直し** ・保護システムの利用者のアクセス権の割当てを定期的及び必要に応じて見直すことを定めていること。		
57	**１１(3)ア　パスワードの利用** ・保護システムの利用者は、容易に推測されないパスワードを選択しなければならないことを定めていること（パスワードより強固な手段を併用又は採用している場合はこの限りでない。）。		
58	**１１(3)イ　無人状態にある保護システム対策** ・保護システムが無人状態に置かれる場合、機密性を配慮した措置を実施することを定めていること。 ・無人状態にある保護システムへ機密性を配慮した措置が実施されていること。		

番号	確認事項	実施／未実施	実施状況の確認方法　又は　未実施の理由
59	**１１(4)ア　機能の制限** ・保護システムの利用者の職務内容に応じて、利用できる機能を制限することを定めていること。		
60	**１１(4)イ　ネットワークの接続制御** ・保護システムを共有ネットワークへ接続する場合、接続に伴うリスクから保護することを定めていること（FW設置など）。		
61	**１１(5)ア　セキュリティに配慮したログオン手順** ・保護システムの利用者は、セキュリティに配慮した手順でログオンすることを定めていること。 ・セキュリティに配慮した手順でログオンしていること。		
62	**１１(5)イ　利用者の識別及び認証** ・保護システムの利用者ごとに一意な識別子（ユーザーID、ユーザー名等）を保有させることを定めていること。		
63	**１１(5)ウ　パスワード管理システム** ・保護システムは、パスワードの不正使用を防止する機能を有さなければならないことを定めていること。		
64	**１２(1)、(2)　情報セキュリティの事故等の報告** ・情報セキュリティ事故等に関する下記のそれぞれの事項について、発注者（防衛省との直接契約関係にある防衛関連企業をいう。以下同じ。）への報告要領を定めているとともに、当該報告要領に以下のことが規定されていること。 ①　情報セキュリティ事故が発生したときは、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、その後速やかにその詳細を発注者に報告しなければならない。 ②　ア）保護すべき情報が保存されたサーバ又はパソコン（以下「サーバ等」という。）に悪意のあるコードへの感染又は不正アクセスが認められた場合、及びイ）保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染が認められた場合において、適切な措置を講じるとともに、直ちに把握し得る限りの全ての内容を、その後速やかにその詳細を発注者に報告しなければならない。 ③　情報セキュリティ事故の疑い又は事故につながるおそれのある場合は、適切な措置を講じるとともに、速やかに、その詳細を発注者に報告しなければならない。 ④　前記①から③までに規定する報告のほか、保護すべき情報の漏えい、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防衛関連企業の内部又は外部から指摘があったときは、防衛関連企業は、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速やかに防衛省に報告しなければならない。 ・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している（異動等のあった場合には更新している）とともに、直ちに発注者に報告する場合の責任者及び連絡担当者を明示していること。		
65	**１２(3)ア　対処体制及び手順** ・情報セキュリティ事故（情報セキュリティ事故の疑いのある場合を含む。以下同じ。）及び事象に対処するため、対処体制、責任及び手順を定めていること。		
66	**１２(3)イ　証拠の収集** ・情報セキュリティ事故が発生した場合（保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染が認められた場合を含む。）、証拠を収集し、速やかに発注者を経由して防衛省へ提出することを定めていること。		
67	**１２(3)ウ　情報セキュリティ基本方針等への反映** ・情報セキュリティ基本方針等の見直しに、情報セキュリティ事故及び事象を反映することを定めていること。		
68	**１３(1)ア　遵守状況の確認** ・管理者の責任の範囲において、情報セキュリティ基本方針等の遵守状況の確認を定めていること。		
69	**１３(1)イ　技術的遵守の確認** ・保護システムの管理者の責任の範囲において、情報セキュリティ基本方針等への技術的遵守状況を確認することを定めていること。		
70	**１３(2)　情報セキュリティの記録** ・保護すべき情報に係る重要な記録の保管期間を定めていること。 ・重要な記録は、施錠したロッカー等において保管又は暗号技術を用いる等厳密に保護することを定めていること。 ・適切に鍵を管理することを定めていること。 ・重要な記録は、施錠したロッカー等において保管又は暗号技術を用いる等厳密に保護されていること。 ・適切に鍵が管理されていること。		
71	**１３(3)　監査ツールの管理** ・保護システムの監査に用いるツールは、悪用を防止するため、必要最低限の使用にとどめることを定めていること。		

確認年月日：

確認者（企業名、所属、役職、氏名）：　　印

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

調達における情報セキュリティ基準

1　趣旨

調達における情報セキュリティ基準（以下「本基準」という。）は、装備品等及び役務の調達に係る企業において当該調達に係る保護すべき情報の適切な管理を目指し、防衛省として求める対策を定めるものであり、当該企業は、情報セキュリティ対策を本基準に則り実施するものとする。

なお、従来から情報セキュリティ対策を実施している場合は、本基準に則り、必要に応じ新たに追加又は拡充を実施するものとする。また、本基準において示されている対策について、合理的な理由がある場合は、適用の除外について、防衛省の確認を受けることができる。

2　定義

本基準において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

⑴ 「防衛関連企業」とは、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（防経装第９２４６号。２１．７．３１。以下「確保通達」という。）第２項第８号に規定する防衛関連企業をいう。

⑵ 「可搬記憶媒体」とは、パソコン又はその周辺機器に挿入又は接続して情報を保存することができる媒体又は機器のうち、可搬型のものをいう。

⑶ 「保護すべき情報」とは、確保通達第２項第１号に規定する保護すべき情報をいう。

⑷ 「保護すべき文書等」とは、保護すべき情報に属する文書（保護すべきデータが保存された可搬記憶媒体を含む。）、図画及び物件をいう。

⑸ 「保護すべきデータ」とは、保護すべき情報に属する電子データをいう。

⑹ 「情報セキュリティ」とは、保護すべき情報の機密性、完全性及び可用性を維持することをいう。

⑺ 「機密性」とは、認可されていないものに対して、情報を使用不可又は非公開にする特性をいう。

⑻ 「完全性」とは、情報の正確さ及び完全さを保護する特性をいう。

⑼ 「可用性」とは、認可されたものが要求したときに、アクセス及び使用が可能である特性をいう。

⑽ 「情報セキュリティ基本方針」とは、本基準に基づき、防衛関連企業が情報セキュリティへの取組の方針等を定めたものをいう。

⑾ 「情報セキュリティ基準」とは、本基準に基づき、防衛関連企業が実施する情報セキュリティ対策について定めたものをいう。

⑿ 「情報セキュリティ実施手順」とは、情報セキュリティ基準に基づき、防衛関連企業が実施する情報セキュリティ対策の具体的な実現手法を定めたものをいう。

⒀ 「情報セキュリティ基本方針等」とは、情報セキュリティ基本方針、情報セキュリティ基準及び情報セキュリティ実施手順をいう。

⒁ 「下請負者」とは、確保通達第２項第９号に規定する下請負者をいう。

⒂ 「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。

⑯ 「情報セキュリティ事故」とは、保護すべき情報の漏えい、紛失、破壊等の事故をいう。

⑰ 「情報セキュリティ事象」とは、情報セキュリティ基本方針等への違反のおそれのある状態及び情報セキュリティ事故につながるおそれのある状態をいう。

⑱ 「情報システム」とは、ハードウェア、ソフトウェア（プログラムの集合体をいう。）、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。

⑲ 「保護システム」とは、保護すべき情報を取り扱う情報システムをいう。

⑳ 「取扱施設」とは、保護すべき情報の取扱い及び保管を行う施設をいう。

㉑ 「利用者」とは、情報システムを利用する者をいう。

㉒ 「悪意のあるコード」とは、情報システムが提供する機能を妨害するプログラムの総称であり、コンピュータウィルス、スパイウェア等をいう。

㉓ 「電子政府推奨暗号等」とは、電子政府推奨暗号リストに記載されている暗号等又は電子政府推奨暗号選定の際の評価方法により評価した場合に電子政府推奨暗号と同等以上の解読困難な強度を有する秘匿化の手段をいう。

㉔ 「秘匿化」とは、情報の内容又は情報の存在を隠すことを目的に、情報の変換等を行うことをいう。

㉕ 「伝達」とは、知識を相手方に伝えることであって、有体物である文書等の送達を伴わないものをいう。

㉖ 「送達」とは、有体物である文書等を物理的に移動させることをいう。

㉗ 「電子メール等」とは、電子メールの送受信、ファイルの共有及びファイルの送受信をいう。

㉘ 「経営者等」とは、経営者又は受注案件を処理する部門責任者をいう。

㉙ 「管理者権限」とは、情報システムの管理（利用者の登録及び登録削除、利用者のアクセス制御等）をするために付与される権限をいう。

3　対象

⑴　対象とする情報は、防衛関連企業において取り扱われる保護すべき情報とする。

⑵　対象者は、防衛関連企業において保護すべき情報に接する全ての者（保護すべき情報に接する役員（持分会社にあっては社員を含む。以下同じ。）、管理職員、派遣社員、契約社員、パート、アルバイト等を含む。この場合において、当該者が、自らが保護すべき情報に接しているとの認識の有無を問わない。以下「取扱者」という。）とする。

4　情報セキュリティ基本方針等の作成

防衛関連企業は、情報セキュリティ基本方針等を作成するものとし、その際及び変更する場合は、本基準との適合性について、防衛省の確認を受けるものとする。

5　情報セキュリティの基本方針等

⑴　情報セキュリティ基本方針及び情報セキュリティ基準

経営者等は、情報セキュリティ基本方針及び情報セキュリティ基準を承認し、保護すべき情報を取り扱う可能性のあるすべての者（取扱者を含む。）に周知しなければならない。また、必要に応じて保護すべき情報を取り扱う下請負者に周知しなければならない。

⑵　情報セキュリティ基本方針等の見直し

経営者等は、情報セキュリティ基本方針等を適切、有効及び妥当なものとするため、定期的な見直しを実施するとともに、情報セキュリティに係る重大な変化及び情報セキュリティ事故が発生した場合は、その都度、見直しを実施し、必要に応じて情報セキュリティ基本方針等を変更しなければならない。※６⑴エ 情報セキュリティの実施状況の監査を参照。

6　組織のセキュリティ

⑴　内部組織

ア　情報セキュリティに対する経営者等の責任

経営者等は、情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当て及び情報セキュリティ基本方針等の承認等を通して、組織内における情報セキュリティの確保に努めるものとし、組織内において、取扱者以外の役員、管理職員等を含む従業員その他の全ての構成員について、取扱者以外の者は保護すべき情報に接してはならず、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。

イ　責任の割当て

防衛関連企業は、保護すべき情報に係るすべての情報セキュリティの責任を明確にするため、保護すべき情報の管理全般に係る総括的な責任者及び保護すべき情報と関連する資産ごとに、それぞれ管理責任者（以下「管理者」という。）を指定しなければならない。

ウ　守秘義務

防衛関連企業は、８⑸に基づき取扱者に要求する事項を特定したのち、取扱者との間で守秘義務を定めた契約又は合意をするものとし、要求事項の定期的な見直しを実施するとともに、情報セキュリティに係る状況の変化及び情報セキュリティ事故が発生した場合は、その都度、見直しを実施した上、必要に応じて要求事項を修正しなければならない。

エ　情報セキュリティの実施状況の監査

防衛関連企業は、情報セキュリティの実施状況について、定期的及び情報セキュリティの実施に係る重大な変化が発生した場合には、監査を実施し、その結果を保存しなければならない。また、必要に応じて是正措置をとらなければならない。

⑵　保護すべき情報を取り扱う下請負者

防衛関連企業は、当該契約の履行に当たり、保護すべき情報を取り扱う業務を下請

負者に請け負わせる場合、本基準に基づく情報セキュリティ対策の実施を当該下請負者との間で契約し、当該業務を始める前に、防衛省が定める確認事項に基づき、当該下請負者において情報セキュリティが確保されることを確認した後、防衛省に届け出なければならない。ただし、輸送その他の保護すべき情報を知り得ないと防衛関連企業が認める業務を請け負わせる場合は、この限りでない。

⑶　第三者

ア　第三者への開示の禁止

防衛関連企業は、第三者（保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に保護すべき情報を開示又は漏えいしてはならない。やむを得ず保護すべき情報を第三者（保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に開示しようとする場合には、あらかじめ、書面により防衛省の許可を受けなければならない。

イ　第三者に関係したリスクの管理

防衛関連企業は、第三者に取扱施設への立入りを許可する場合、想定されるリスクを明確にした上、対策を定めなければならない。

ウ　第三者に対する立入りの許可

防衛関連企業は、定めた対策が満たされた場合を除き、取扱施設に対する第三者の立入りを許可してはならない。

7　保護すべき情報の管理

⑴　分類の指針

防衛関連企業は、保護すべき情報を明確に分類することができる情報の分類体系を定めなければならない。

⑵　保護すべき情報の取扱い

ア　保護すべき情報の目録

防衛関連企業は、保護すべき情報の現状（保管場所等）が分かる目録を作成し、維持しなければならない。

イ　取扱いの管理策

⑺　防衛関連企業は、保護すべき情報を取扱施設において取り扱うとともに、保護すべき情報を接受、作成、製作、複製、持ち出し（貸出を含む。）及び破棄する場合は、記録しなければならない。

⑴　防衛関連企業は、保護すべき情報を個人が所有する情報システム及び可搬記憶媒体において取り扱ってはならず、やむを得ない場合は、事前に防衛省の許可を得なければならない。

⑼　防衛関連企業は、契約終了後、防衛省の指示に従い、保護すべき情報の返却、提出等必要な措置をとらなければならない。

⑽　防衛関連企業は、契約終了後、防衛省から保護すべき情報の破棄を求められた場合であって、当該情報を引き続き保有する必要があるときは、その理由を添えて防衛省に協議を求めることができる。

ウ　保護すべき情報の保管等

防衛関連企業は、保護すべき情報を施錠したロッカー等に保管し、その鍵を適切に管理しなければならない。

また、保護すべき情報を保護すべきデータとして保存する場合には、暗号技術を用いることを推奨する。※１０⑺ 電子政府推奨暗号等の利用を参照

エ　保護すべき情報の持ち出し

防衛関連企業は、経営者等が持ち出しに伴うリスクを回避することができると判断した場合を除き、保護すべき情報を取扱施設外に持ち出してはならない。

なお、持ち出しをする場合は、記録するものとする。

オ　保護すべき情報の破棄

防衛関連企業は、接受、作成、製作又は複製した保護すべき情報を破棄する場合は、復元できないように裁断等確実な方法により破棄し、その旨を記録するものとする。

なお、保護すべきデータを保存した可搬記憶媒体を破棄する場合は、10(4) ウに基づき破棄するものとする。

カ　該当部分の明示

⑺ 防衛関連企業は、保護すべき情報を作成、製作又は複製した場合は、下線若しくは枠囲みによる明示又は文頭及び文末に括弧を付すことによる明示等の措置を行うものとする。

⑴ 防衛関連企業は、契約の目的物が保護すべき情報を含むものである場合には、当該契約の履行の一環として収集、整理、作成等した一切の情報について、防衛省が当該情報を保護すべき情報には当たらないと確認するまでは、保護すべき情報として取り扱わなければならない。ただし、保護すべき情報の指定を解除する必要がある場合には、その理由を添えて防衛省に協議を求めることができる。

8　人的セキュリティ

⑴　経営者等の責任

経営者等は、保護すべき情報の取扱者の指定の範囲を必要最小限とするとともに、ふさわしいと認める者を充て、情報セキュリティ基本方針等を遵守させなければならない。また、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。

⑵　取扱者名簿

防衛関連企業は、取扱者名簿（取扱者の氏名、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。以下同じ。）を作成又は更新し、その都度、保護すべき情報を取り扱う前に防衛省に届け出て同意を得なければならない。また、防衛関連企業は、下請負者及び保護すべき情報を開示する第三者の取扱者名簿についても、同様の措置をとらなければならない。

⑶　情報セキュリティ教育及び訓練

防衛関連企業は、取扱者の職務に関連する組織の方針、手順、関連する法令その他なりすましメール等による悪意のあるコード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等について、教育及び訓練を定期的に実施するとともに、その状

況を記録し、少なくとも翌年度末まで保管しなければならない。

⑷　違反者への対処方針

防衛関連企業は、情報セキュリティ基本方針等に違反した取扱者に対する対処方針及び手続を定めなければならない。

⑸　取扱者の責任

取扱者は、在職中及び離職後において、契約の履行において知り得た保護すべき情報を第三者（保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に漏えいしてはならない。

⑹　保護すべき情報の返却

防衛関連企業は、取扱者の雇用契約の終了又は取扱者との契約合意内容の変更に伴い、保護すべき情報に接する必要がなくなった場合には、取扱者が保有する保護すべき情報を管理者へ返却させなければならない。

9　物理的及び環境的セキュリティ

⑴　取扱施設

ア　取扱施設の指定

防衛関連企業は、保護すべき情報の取扱施設を明確に定めなければならない。

イ　物理的セキュリティ境界

防衛関連企業は､保護すべき情報及び保護システムのある区域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いなければならない。

ウ　物理的入退管理策

防衛関連企業は、取扱施設への立入りを適切な入退管理策により許可された者だけに制限するとともに、取扱施設への第三者の立入りを記録し、保管しなければならない。※１３⑵ 情報セキュリティの記録を参照

エ　取扱施設での作業

防衛関連企業は、保護すべき情報に係る作業は、機密性に配慮しなければならない。また、取扱施設において通信機器（携帯電話等）及び記録装置（ボイスレコーダ及びデジカメ等）を経営者等の許可無く利用してはならない。

⑵　保護システムの物理的保全対策

ア　保護システムの設置及び保護

防衛関連企業は、保護システムを設置する場合、不正なアクセス及び盗難等から保護するため、施錠できるラック等に設置又はワイヤーで固定する等の措置をとらなければならない。

イ　保護システムの持ち出し

防衛関連企業は、経営者等が持ち出しに伴うリスクを回避することができると判断した場合を除き、保護システムを取扱施設外に持ち出してはならない。

なお、持ち出しをする場合は、記録するものとする。

ウ　保護システムの保守及び点検

防衛関連企業は、第三者による保護システムの保守及び点検を行う場合、必要に

応じて、保護すべき情報を復元できない状態にする、又は取り外す等の処置を実施しなければならない。

エ　保護システムの破棄又は再利用

防衛関連企業は、保護システムを破棄する場合は、保護すべきデータが復元できない状態であることを点検した上、記憶媒体を物理的に破壊した後、破棄し、その旨を記録しなければならない。また、再利用する場合は、保護すべきデータが復元できない状態であることを点検した後でなければ再利用してはならない。

１０　通信及び運用管理

⑴　操作手順書

防衛関連企業は、保護システムの操作手順書を整備し、維持するとともに、利用者が利用可能な状態にしなければならない。

⑵　悪意のあるコードからの保護

防衛関連企業は、保護システムを最新の状態に更新されたウィルス対策ソフトウェア等を用いて、少なくとも週１回以上フルスキャンを行うことなどにより、悪意のあるコードから保護しなければならない。なお、１週間以上電源の切られた状態にあるサーバ又はパソコン（以下「サーバ等」という。）については、再度の電源投入時に当該処置を行うものとする。

⑶　保護システムのバックアップの管理

防衛関連企業は、保護システムを可搬記憶媒体にバックアップする場合、可搬記憶媒体は7⑵及び次号に沿った取扱いを行わなければならない。

⑷　可搬記憶媒体の取扱い

ア　可搬記憶媒体の管理

防衛関連企業は、保護すべきデータを保存した可搬記憶媒体を施錠したロッカー等において集中保管し、適切に鍵を管理しなければならない。また、可搬記憶媒体は、保護すべき情報とそれ以外を容易に区別できる処置をしなければならない。※７⑵ 保護すべき情報の取扱いを参照

イ　可搬記憶媒体への保存

防衛関連企業は、保護すべきデータを可搬記憶媒体に保存する場合、暗号技術を用いなければならない。ただし、防衛省への納入又は提出物件等である場合には、防衛省の指示に従うものとする。※１０⑺ 電子政府推奨暗号等の利用を参照

ウ　可搬記憶媒体の破棄又は再利用

防衛関連企業は、保護すべきデータの保存に利用した可搬記憶媒体を破棄する場合、保護すべきデータが復元できない状態であることを点検した上、可搬記憶媒体を物理的に破壊した後、破棄し、その旨を記録しなければならない。また、再利用する場合は、保護すべきデータが復元できない状態であることを点検した後でなければ再利用してはならない。

⑸　情報の伝達及び送達

ア　保護すべき情報の伝達

防衛関連企業は、通信機器（携帯電話等）を用いて保護すべき情報を伝達する場

合、伝達に伴うリスクを経営者等が判断の上、必要に応じそのリスクから保護しなければならない。

イ　伝達及び送達に関する合意

防衛関連企業は、保護すべき情報を伝達及び送達する場合には、守秘義務を定めた契約又は合意した相手に対してのみ行われなければならない。

ウ　送達中の管理策

防衛関連企業は、保護すべき文書等を送達する場合には、送達途中において、許可されていないアクセス及び不正使用等から保護しなければならない。

エ　保護すべきデータの伝達

防衛関連企業は、保護すべきデータを伝達する場合には、保護すべきデータが既に暗号技術を用いて保存され、通信事業者の回線区間に暗号技術を用い、又は電子メール等に暗号技術を用いることのいずれかによって、保護すべきデータを保護しなければならない。ただし、漏えいのおそれがないと認められる取扱施設内において、有線で伝達が行われる場合は、この限りでない。※１０⑺ 電子政府推奨暗号等の利用を参照

⑹　外部からの接続

防衛関連企業は、保護システムに外部から接続（モバイルコンピューティング及びテレワーキング等）を許可する場合は、利用者の認証を行うとともに、暗号技術を用いなければならない。※１０⑺ 電子政府推奨暗号等の利用を参照

⑺　電子政府推奨暗号等の利用

防衛関連企業は、暗号技術を用いる場合、電子政府推奨暗号等を用いなければならない。

なお、電子政府推奨暗号等を用いる事が困難な場合は、その他の秘匿化技術を用いる等により保護すべき情報を保護しなければならない。

⑻　ソフトウェアの導入管理

防衛関連企業は、保護システムへソフトウェアを導入する場合、当該システムの管理者等によりソフトウェアの安全性が確認された場合を除き、許可してはならない。

⑼　システムユーティリティの使用

防衛関連企業は、保護システムにおいてオペレーティングシステム及びソフトウェアによる制御を無効にすることができるシステムユーティリティの使用を制限しなければならない。

⑽　技術的脆弱性の管理

防衛関連企業は、技術的脆弱性に関する情報について時期を失せず取得し、経営者等が判断の上、適切に対処しなければならない。

⑾　監視

ア　監査ログ取得

防衛関連企業は、保護システムにおいて、保護すべき情報へのアクセス及び例外処理を記録した監査ログを取得しなければならない。

イ　監査ログの保管

防衛関連企業は、取得した監査ログを記録のあった日から少なくとも３か月以上

保存するとともに、定期的に点検しなければならない。

ウ　監査ログの保護

防衛関連企業は、監査ログを改ざん及び許可されていないアクセスから保護しなければならない。

エ　クロックの同期

防衛関連企業は、保護システム及びネットワークを通じて保護システムにアクセス可能な情報システムの日付及び時刻を手動等により定期的に合わせなければならない。

オ　保護すべきデータの監視

防衛関連企業は、保護システムが共有ネットワーク（インターネット等）へ物理的に接続されている場合は、共有ネットワークを通じて、保護すべきデータの社外漏えいを未然に防止することを可能とする常時監視を行わなければならない。

１１　アクセス制御

⑴　アクセス制御方針

防衛関連企業は、保護すべき情報、取扱施設及び保護システムへのアクセスについて、取扱者及び利用者の職務内容に応じて、アクセス制限方針を作成しなければならない。また、アクセス制御方針は定期的に見直しを実施するとともに、情報セキュリティに係る重大な変化及び情報セキュリティ事故が発生した場合には、その都度、見直しを実施し、必要に応じてアクセス制御方針を修正しなければならない。

⑵　利用者の管理

ア　利用者の登録管理

防衛関連企業は、取扱者による保護システム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、保護システムの利用者としての登録及び登録の削除をしなければならない。

イ　パスワードの割当て

防衛関連企業は、保護システムの利用者に対して初期又は仮パスワードを割り当てる場合、容易に推測されないパスワードを割り当てるものとし、機密性に配慮した方法で配布するものとする。なお、パスワードより強固な手段（生体認証等）を採用又は併用している場合は、本項目の適用を除外することができる。

ウ　管理者権限の管理

保護システムの管理者権限は、必要最低限の利用にとどめなければならない。

エ　アクセス権の見直し

防衛関連企業は､保護システムの利用者に対するアクセス権の割当てについては、定期的及び必要に応じて見直しを実施しなければならない。

⑶　利用者の責任

ア　パスワードの利用

防衛関連企業は、容易に推測されないパスワードを保護システムの利用者に選択させるとともに、定期的に変更させなければならない。

なお､パスワードより強固な手段（生体認証等）を採用又は併用している場合は、

本項目の適用を除外することができる。

イ　無人状態にある保護システム対策

防衛関連企業は、保護システムが無人状態に置かれる場合、機密性を配慮した措置をとらなければならない。

⑷　ネットワークのアクセス制御

ア　機能の制限

防衛関連企業は、保護システムの利用者の職務内容に応じて、利用できる機能を制限し提供しなければならない。

イ　ネットワークの接続制御

防衛関連企業は、保護システムの共有ネットワーク（インターネット等）への接続については、アクセス制御方針に基づいて実施するとともに、接続に伴うリスクから保護しなければならない。

⑸　オペレーティングシステムのアクセス制御

ア　セキュリティに配慮したログオン手順

防衛関連企業は、利用者が保護システムを利用する場合、セキュリティを配慮した手順により、ログオンさせなければならない。

イ　利用者の識別及び認証

防衛関連企業は、保護システムの利用者ごとに一意な識別子（ユーザーID、ユーザー名等）を保有させなければならない。

ウ　パスワード管理システム

保護システムは、パスワードの不正使用を防止する機能（パスワードの定期的な変更を利用者に促す機能、パスワードの再使用を防止する機能等）を有さなければならない。

１２　情報セキュリティ事故等の管理

⑴　情報セキュリティ事故等の報告

ア　防衛関連企業は、情報セキュリティ事故が発生したときは、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、その後速やかにその詳細を防衛省に報告しなければならない。

イ　次に掲げる場合において、防衛関連企業は、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、その後速やかにその詳細を防衛省に報告しなければならない。

(ｱ) 保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染又は不正アクセスが認められた場合

(ｲ) 保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染が認められた場合

ウ　情報セキュリティ事故の疑い又は事故につながるおそれのある場合は、防衛関連企業は、適切な措置を講じるとともに、速やかに、その詳細を防衛省に報告しなければならない。

エ　前記アからウまでに規定する報告のほか、保護すべき情報の漏えい、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防衛関連企業の内部又は外部から指摘があったときは、防衛関連企業は、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速やかに防衛省に報告しなければならない。

⑵　情報セキュリティ事故等の報告要領

防衛関連企業は、⑴アからエまでの規定による報告について、それぞれ防衛省への報告要領を定めなければならない。また、報告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報告要領の策定時に作成し、異動等のあった場合にはこれを更新するものとする。

特に、連絡系統図には、直ちに防衛省へ報告する場合の責任者及び連絡担当者を明示するものとする。

⑶　情報セキュリティ事故等の対処等

ア　対処体制及び手順

防衛関連企業は、情報セキュリティ事故、その疑いのある場合及び情報セキュリティ事象に対処するため、対処体制、責任及び手順を定めなければならない。

イ　証拠の収集

防衛関連企業は、情報セキュリティ事故が発生した場合、その疑いのある場合及び⑴イ(ｱ)の場合証拠を収集し速やかに防衛省へ提出しなければならない。

ウ　情報セキュリティ基本方針等への反映

防衛関連企業は、発生した情報セキュリティ事故、その疑いのある場合及び情報セキュリティ事象を、情報セキュリティ基本方針等の見直し等に反映しなければならない。

１３　遵守状況等

⑴　遵守の確認等

ア　遵守状況の確認

防衛関連企業は、管理者の責任の範囲において、情報セキュリティ基本方針等の遵守状況を確認させなければならない。

イ　技術的遵守の確認

防衛関連企業は、保護システムの管理者の責任の範囲において、情報セキュリティ基本方針等への技術的遵守状況を確認させなければならない。

⑵　情報セキュリティの記録

防衛関連企業は、保護すべき情報に係る重要な記録（複製記録、持ち出し記録及び監査記録等）の保管期間（少なくとも契約履行後１年間）を定めた上、施錠したロッカー等において保管又は暗号技術を用いる等厳密に保護するとともに、適切に鍵を管理しなければならない。

⑶　監査ツールの管理

防衛関連企業は、保護システムの監査に用いるツールについて、悪用を防止するため必要最低限の使用にとどめなければならない。

⑷　防衛省による監査

ア　監査の受入

防衛関連企業は、防衛省による情報セキュリティ対策に関する監査の要求があった場合には、これを受け入れなければならない。

イ　監査への協力

防衛関連企業は、防衛省が監査を実施する場合、防衛省の求めに応じ必要な協力（監査官の取扱施設への立入り及び監査官による書類の閲覧等への協力）をしなければならない。