装装制第９９４号
２７．１０．１
一部改正　装装制第８１号
令和元年５月７日
一部改正　装装保第５３２１号
令和２年４月１日

大臣官房長
防衛大学校長
防衛医科大学校長
防衛研究所長
統合幕僚長
陸上幕僚長　殿
海上幕僚長
航空幕僚長
情報本部長
防衛監察監
各地方防衛局長

防衛装備庁装備政策部長
（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監査実施要領について（通知）

標記について、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７項第２号及び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の措置の細部事項について（装装制第７７号。令和元年５月１日）別紙第４項の規定に基づき、別添のとおり実施要領を定めたので通知する。

添付書類：装備品等及び役務の調達における情報セキュリティ監査実施要領
写送付先：長官官房会計官、長官官房監察監査・評価官、長官官房各装備開発官、長官官房艦船設計官、各部長、施設等機関の長
開示区分：開示
原本保存期間満了時期：２０４６．３．３１

装装制第９９４号別添

装備品等及び役務の調達における情報セキュリティ監査実施要領

平成２７年１０月

防　衛　装　備　庁

目　　次

別紙第１　情報セキュリティ基本方針の判定基準
別紙第２　情報セキュリティ基準の判定基準
別紙第３　情報セキュリティ実施手順の判定基準
別紙第４　実地監査確認項目
別紙第５　地方防衛局等の管轄区域一覧
別紙第６　防衛省の地方調達契約に係る情報セキュリティに関する監査等の協力について

1.　総　則

1．1　通　則

装備品等及び役務の調達における情報セキュリティ基本方針等の確認及び情報セキュリティに関する監査要領並びに防衛省の地方調達契約に係る情報セキュリティに関する監査等の協力依頼の要領は、この実施要領の定めるところによる。

1．2　適用範囲

この実施要領は、仕様書等において「調達における情報セキュリティ基準」が引用されている装備品等及び役務の契約に基づく防衛関連企業の情報セキュリティ対策に適用する。

1．3　用語の意義

この実施要領において、用語の意義は、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）及び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（通知）（装装制第３６９号。２７．１０．１）に定めるところによる。

1．4　監査の目的

情報セキュリティに関する監査は、契約に基づき防衛関連企業の事業所等において取り扱われる保護すべき情報について、防衛関連企業が実施する情報セキュリティ対策が適切に実施され、情報セキュリティが確保されていることを確認するとともに、情報セキュリティ対策に関して不備事項があれば防衛関連企業に対して（下請負者の場合は、契約相手方を通じて）是正措置をとるように指導することにより、保護すべき情報の保全に万全を期すものである。

1．5　監査の手順

情報セキュリティ監査は、次の手順を標準として実施する。

(1)　特約条項に基づき申請され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確認する。

(2)　前項の確認後、特約条項に基づき申請された情報セキュリティ実施手順を確認する。

(3)　契約相手方と調整の上、実地監査の実施計画を作成する。

(4)　実地監査を実施する。

(5)　実地監査の結果に基づき、結果通知書及び監査報告書を作成する。

(6)　実地監査の結果に基づき、必要に応じ是正措置の指導をする。

2.　情報セキュリティ基本方針等の確認

2．1　情報セキュリティ基本方針

情報セキュリティ基本方針は、「調達における情報セキュリティ基準」に基づき、防衛関連企業における情報セキュリティに関する基本的な方針（組織の取組及び組織全体に係る事項等）について規定するものであり、確認に当たっては、別紙第１によりその適合性を確認する。

なお、不適合と認める場合は防衛関連企業に不適合である旨の理由を付して通知し再提出を求める。

2．2　情報セキュリティ基準

(1)　情報セキュリティ基準は、「調達における情報セキュリティ基準」及び情報セキュリティ基本方針に基づき、防衛関連企業における情報セキュリティに関する管理策を規定するものであり、確認に当たっては、別紙第２によりその適合性を確認する。なお、不適合と認める場合は防衛関連企業に不適合である旨の理由を付して通知し再提出を求める。

(2)　情報セキュリティ基準の確認に当たり、「調達における情報セキュリティ基準」に規定された項目のうち、適用除外とする項目がある場合は、適用除外とする項目及び適用除外とする合理的な理由が明記されていることを確認する。

2．3　情報セキュリティ実施手順

(1)　情報セキュリティ実施手順は、情報セキュリティ基準において規定された管理策の具体的な実施手順を規定し、保護すべき情報の管理責任者及び取扱者等により業務マニュアルとして利用されるものであり、確認に当たっては、別紙第３によりその適合性を確認する。なお、不適合と認める場合は防衛関連企業に不適合である旨の理由を付して通知し再提出を求める。

(2)　情報セキュリティ実施手順の確認に当たっては、次の各事項に留意して実施する。

ア　雛形や他社のコピーではなく、自社の組織又は部門の特性、契約履行の内容に応じた実施手順であること。

イ　保護すべき情報の取り扱い状況に応じた具体的な実施手順であること。

ウ　保護すべき情報の取り扱い者が理解しやすく、普及が容易で錯誤を起こし難い平易な記述であること。

3.　実地監査

3．1　監査の区分

実地監査は、次の監査区分に分類して実施する。

(1)　初回監査

「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」が適用された契約を初めて締結し、これに基づく監査を初めて受ける防衛関連企業に対し実施する監査

(2)　維持監査

初回監査の翌年度以降、定期的に情報セキュリティ基本方針等の有効性及び情報セキュリティ実施手順の遵守状況を確認する監査

(3)　更新監査

初回監査又は維持監査の対象となる契約履行後、１年以上当該特約条項の適用のある契約締結がなく、実地監査を受けていない防衛関連企業が、再度当該特約条項の適用のある契約を締結した後に実施する監査

3．2　監査実施計画の作成

(1)　実地監査の実施に先立ち、実地監査の目的を有効かつ効率的に達成するために監査実施時期、監査項目、監査手法等を検討し監査実施計画を作成する。

(2)　監査実施計画は、契約の締結後、契約の履行状況等を考慮し、保護すべき情報を管理している事業所等ごとに作成する。ただし、情報セキュリティ対策が複数の事業所等にまたがり実施されている場合は、一括して計画することができる。

(3)　監査実施については、契約履行状況及び保護すべき情報の取扱い状況等を勘案して適切な時期及び年間実施回数（年１回以上）を設定し、事業所等の規模及び監査実施項目等を考慮して適切な監査期間を設定する。

(4)　監査項目は、別紙第４の実地監査確認項目を基準として、次の監査区分に基づく項目及び防衛関連企業が従来から実施している情報セキュリティ対策に新たに追加又は拡充した項目から選択する。

ア　初回監査では、原則として全項目とする。

イ　維持監査では、前回の監査で要改善の指摘をした項目及びその他保護すべき情報の取扱い状況等に応じた必要な項目とする。

ウ　更新監査では、前回の監査からの経過年数等の状況に応じて必要な項目とし、前回の監査から３年以上経過している場合においては、初回監査と同様の項目とする。

3．3　監査実施通知

監査の実施に先立ち、あらかじめ監査実施日時、実施内容等の細部について契約相手方と調整した上、監査対象契約、監査対象事業所等名、監査実施期間、監査実

施者等を契約相手方に通知する。

3．4　監査手法

実地監査は、監査実施計画に基づき、次の手法を組み合わせて、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遵守状況を確認する。

(1)　目視による確認：保護すべき情報（文書、データ等）の保管状況等の確認
(2)　閲覧による確認：教育実施記録、社内点検記録、関連文書、関係簿冊等の確認
(3)　質問による確認：管理責任者、取扱者に対する知識、認識、取扱い状況等の確認
(4)　観察による確認：関連施設、設備の管理状況、機器の設置状況等の確認
(5)　試行による確認：入退管理装置、システムへのアクセス制限等の機能確認

3．4．1 取扱い状況の把握

監査の実施に当たり、契約履行における防衛関連企業の保護すべき情報の取扱い状況（予定を含む）、保護すべき情報の動きなど業務の流れを把握する。

3．4．2 監査の実施

監査に当たっては、監査実施計画に基づき、別紙第４により項目ごとに契約相手方の立会いの下、情報セキュリティ対策の実施状況を確認する。また、契約相手方の保護すべき情報の取扱い状況に応じて、適宜項目を追加して確認する。なお、限られた期間内に効果的、効率的に監査が実施できるように、監査手法、サンプリング、精査（全数確認）を有効に組み合わせて監査を実施する。

3．4．3 監査結果の確認

監査実施の際に不備事項を認めた場合は、契約相手方の立会者に対してその場で指摘の内容、不備とする理由を説明し、不備事実の確認を得る。また、監査日程の最終日に監査結果を総括し、契約相手方に対して総合評価及び指摘事項等を講評し確認を得る。なお、監査結果の評価及び指摘事項について、契約相手方と見解の相違がある場合は保留とし、別途協議する。

3．4．4 監査調書の作成と保管

監査実施内容の記録として、別紙第４により監査項目ごとの確認方法及び実施状況、評価、指摘した不備事項の詳細、契約相手方立会者名、指導した是正措置、その他一連の監査実施事項の詳細な記録を監査調書として作成し保管する。なお、監査調書は事業所等ごとに取りまとめ、監査報告書の根拠資料として鍵のかかる書庫で保管する等、適切に管理する。

3．5　評価

防衛関連企業の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遵守状況について、確認した項目ごとにその実施状況を評価する。

3．5．1 評価の基準

情報セキュリティ実施手順の項目ごとの評価基準は、次による。

［項目別評価基準］

評　価	基　準
良　好	(1) 情報セキュリティ対策が、良好かつ適切に実施されている。 (2) 軽微な指摘事項（記録の一部記入漏れ、誤記等）はあるが、即時に是正が確認でき、項目全体としては良好に実施されている。
要改善	(1) 定められた情報セキュリティ対策を実施しているが、一部未実施の部分がある、又は実施している内容に不十分な部分がある。 (2) 定めた情報セキュリティ対策が保護すべき情報の取り扱いの現状と符合しない部分があり、管理策の一部見直しが必要。
不　良	(1) 定められた情報セキュリティ対策を全く実施していない。 (2) 定められた情報セキュリティ対策を実施しているが、実施の内容が不十分で、保護すべき情報の漏洩又は流出に直ちに繋がるおそれがある状態。 (3) 定めた情報セキュリティ対策が保護すべき情報の取り扱いの現状と符合せず、管理策の全面的な見直しが必要。

3．6　監査結果の通知

実地監査終了後、監査調書を元に監査結果をまとめ、監査結果を契約相手方に通知する。通知には、実施した監査の概要、監査結果の総合評価等を記載し、指摘事項がある場合は、項目別に簡潔に記載し是正措置を要求する。

なお、結果通知に記載する総合評価基準は、次による。

［総合評価基準］

評　価	基　準
良　好	「要改善」、「不良」評価の項目がない。
要改善	「不良」評価の項目がなく、「要改善」の項目がある。
不　良	「不良」評価の項目がある。

3．7　監査実施報告書の作成

実地監査終了後、監査調書を元に監査結果をまとめ、監査報告書を作成する。作成に当たっては、防衛関連企業の情報セキュリティ対策の状況が明瞭に把握できるように作成するものとし、監査対象事業所等ごとに監査の概要、監査項目、監査結果及び評価、指摘事項、所見等を簡潔に記載する。

3．8　指摘事項の是正指導

(1)　実地監査において「要改善」評価にあたる指摘事項がある場合は、契約相手方に対して、速やかに是正措置をとるように指導し、その改善状況を報告させ次回監査時に確認する。なお、次回監査時に改善が確認できない場合は、早急に是正措置をとらせるとともに、再監査により改善状況を確認する。

(2)　実地監査において「不良」評価にあたる指摘事項がある場合は、契約相手方に対して、その場で直ちに対策を講じるように指導し、早急に是正措置をとらせるとともに、再監査により改善状況を確認する。

3．9　下請負者に対する監査

(1)　下請負者に対する監査は、特約条項に基づき契約相手方が届出た情報セキュリティ対策実施確認書を確認し、必要と認める場合（保護すべき情報を多量に保管している、頻繁に保護すべき情報の移動を行う、保護すべき情報の取扱い経験が浅いなど。）に実施する。

(2)　下請負監査を実施する場合は、あらかじめ契約相手方と調整の上、監査の対象、監査実施項目等を通知し、契約相手方に対する監査等の手順に準じて実施する。また、下請負者の監査対象事業所が日本国外の場合は、別紙第５に示す管轄区域に所在する契約相手方を担当する地方防衛調達部長等が下請負監査を実施するものとする。なお、原則として契約相手方の立会いの下、実施する。

(3)　下請負者に対する監査の結果、情報セキュリティ対策に不備があると認められる場合は、契約相手方を通じて是正措置を要求し、その改善状況を報告させるとともに、3.8 項を準用し改善状況を確認する。

4.　防衛省の地方調達契約に係る協力

4．1　情報セキュリティ基本方針等の確認の協力依頼

防衛省の地方調達の契約担当官等は、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の実施に当たり、協力を依頼する必要がある場合には、その理由を明確にし、別紙第５に示す地方防衛局調達部長等と事前に調整した上、別紙第６により協力を依頼する。

なお、契約相手方から提出された確認申請書の受理及び適合、不適合の判定並びに契約相手方に対する確認通知は、当該契約担当官等が実施する。

4．2　情報セキュリティに関する監査の協力依頼

防衛省の地方調達の契約担当官等は、締結した契約における情報セキュリティに関する監査の実施に当たり、協力を依頼する必要がある場合には、その理由を明確にし、別紙第５に示す地方防衛局調達部長等と事前に調整した上、別紙第６により協力を依頼する。

なお、監査の実施に係る契約相手方への監査実施通知及び監査結果等の通知は、当該契約担当官等が実施する。

4．3　その他の事項に関する協力依頼

防衛省の地方調達の契約担当官等は、締結した契約における情報セキュリティに関する次の事項について、協力を依頼する必要がある場合には、その理由を明確にし、別紙第５に示す地方防衛局調達部長等と事前に調整した上、別紙第６により協力を依頼する。

(1)　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

(2)　下請負者を使用する場合の届出に関すること

(3)　事故発生時の調査に関すること

なお、各事項に係る契約相手方からの申請、届出等の受理、承認又は確認等の判定、契約相手方への通知等の手続きは、当該契約担当官等が実施する。

4．4　防衛省の地方調達の契約担当官等への協力

地方防衛局調達部長等は、防衛省の地方調達の契約担当官等から管轄区域内に所在する防衛関連企業の事業所、工場等に関し、防衛省の地方調達契約に係る情報セキュリティ監査等に関する協力の依頼があった場合には、当該契約担当官等と調整するものとする。なお、調整要領については、別に定める。

5.　その他

装備政策部装備保全管理官は、この実施要領の実施のための細部事項について定めることができる。

別紙第３

情報セキュリティ実施手順の判定基準

調達における情報セキュリティ基準		判定の目安			備考
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	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。			
			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について、経営者等の承認を得る手順を定めていること。	
			2	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ついて、保護すべき情報を取り扱う可能性のある全ての者（派遣社員、契約社員、パート、アルバイト等を含む。）に周知する方法を定めていること。	
			3	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することを定めていること。	
5(2)	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。			
			1	基本方針等を見直す時期及び実施責任者又は実施担当部署を定めていること。	
			2	基本方針等を見直す作業手順、承認手順等を定めていること。	
			3	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発生時の見直し手順を定めていること。	
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。			
			1	経営者等が情報セキュリティ組織における最高責任者として、直接承認又は確認する事項及び手順を定めていること。	
			2	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ないようにする要領、かつ、職務上の下級者等に対してその提供に係る要求をさせないようにする要領を定めていること。	
6(1)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。			
			1	保護すべき情報の管理全般に係る総括的な責任者として、総括者を定めていること。	
			2	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を定めていること。	合理的理由があれば一つの役職者が兼務してもよい。
			3	総括者及び管理者の指定及び指定解除の手順、要領を定めていること。	

調達における情報セキュリティ基準		判定の目安			備考
6(1)ウ	守秘義務	防衛関連企業は、8(5) 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。			
			1	防衛関連企業と取扱者の間で、情報セキュリティに関する守秘義務について具体的な義務の内容を定めていること。（内容に取扱者でなくなった場合及び離職後も守秘義務が継続することを定めていること。）	
			2	守秘義務に関する誓約書又は合意書の様式を定め、あらかじめ取扱者から提出を受けることを定めていること。	
			3	守秘義務の要求事項について、要求内容の見直し時期及び手順を定めていること。	
			4	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の見直し手順を定めていること。	
6(1)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、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。			
			1	保護すべき情報の取り扱い状況に関する監査の実施時期及び実施手順を定めていること。	
			2	独立した監査部門又は被監査部門以外に所属する者が監査を実施することを定めていること。	
			3	監査の実施の結果に対して、経営者等への報告、是正措置の実施等の手順を定めていること。	
			4	監査の実施から是正措置の確認までの一連の記録、経営者等への報告記録等の保存方法を定めていること。	
			5	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の監査実施手順を定めていること。	
6(2)	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、この限りではない。			
			1	下請負者との契約の内容に、下請負者が防衛省の定める「調達における情報セキュリティ基準」に基づく情報セキュリティ対策を実施することを定めていること。	
			2	下請負者に対する防衛省が定める確認事項の確認実施要領及び防衛省への届け出要領（下請負者の場合は、契約相手方を通じて届け出る。）を定めていること。	
6(3)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。			
			1	第三者に保護すべき情報を開示する際の承認手続きを定めていること。	
			2	やむを得ず第三者へ開示する場合の承認権者をあらかじめ定めていること。	
			3	第三者へ開示する場合の防衛省への許可申請手順を定めていること。（下請負者の場合は、契約相手方を通じて許可を受ける。）	

調達における情報セキュリティ基準		判定の目安			備考
6(3)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。			
			1	第三者が取扱施設へ立ち入る場合におけるリスクを明確にした上、立入り統制要領を定めていること。	
6(3)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。			
			1	第三者の取扱施設への立入り許可手続きを定めていること。	
			2	第三者の立入許可記録の保存要領を定めていること。	
7(1)	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。			
			1	保護すべき情報を明確に識別できる、情報資産の分類体系又は分類方法を定めていること。	
7(2)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。			
			1	保護すべき情報の目録の作成及び保管、管理要領を定めていること。	
7(2)イ	取扱いの管理策	(ｱ) 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。 (ｲ) 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。 (ｳ) 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。 (ｴ) 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。			
			1	保護すべき情報の取扱施設における取扱い要領を定めていること。	
			2	保護すべき情報の接受、送達、作成、製作、複製、持ち出し（貸出を含む。）及び破棄の記録要領を定めていること。	
			3	やむを得ず、保護すべき情報を個人が所有する情報システム、パソコン、可搬記憶媒体、その他の機器等で取り扱う場合の許可手順を定めていること。	
			4	やむを得ず、保護すべき情報を個人が所有する情報システム、パソコン、可搬記憶媒体、その他の機器等で取り扱う場合の防衛省への許可手続きを定めていること。	
			5	契約修了後の保護すべき情報の防衛省への返却、提出、破棄等の手順を定めていること。	
			6	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、その理由を添えて防衛省（調達要求元）に協議を求めることができる手順を定めていること。	

調達における情報セキュリティ基準		判定の目安			備考
7(2)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。 ※10(7)電子政府推奨暗号等の利用を参照			
			1	施錠できるロッカー等における保護すべき情報の保管要領を定めていること。	
			2	保護すべき情報を保管するロッカー等の鍵の管理要領を定めていること。	
			3	保護すべき情報を保護すべきデータとして保存し、暗号技術を用いる場合（可搬記憶媒体に保存する場合、10(4)イに基づき保存するものとする。）、暗号技術の利用手順及び記録要領を定めていること。	
			4	保護すべき情報を暗号技術を用いずに保護すべきデータとして保存する場合、暗号技術にかわる手段により保護すべきデータを保護する要領を定めていること。	
7(2)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。			
			1	保護すべき情報の持ち出し許可権者及び持ち出しに伴うリスクを回避できると判断する場合の判断基準を定めていること。	
			2	正当な理由により社外へ持ち出す際の持ち出し手続き及び記録要領を定めていること。	
7(2)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。			
			1	保護すべき情報を破棄する場合の具体的な手順、方法を定めていること。	
			2	保護すべき情報を破棄した場合の記録要領を定めていること。	
7(2)カ	該当部分の明示	(ｱ) 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。 (ｲ) 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。			
			1	保護すべき情報を作成、製作又は複製した場合の表示及び明示方法を定めていること。	
			2	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、防衛省が当該情報が保護すべき情報に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手順を定めていること。	
			3	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、その理由を添えて防衛省（調達要求元）に協議を求めることができる手順を定めていること。	

調達における情報セキュリティ基準		判定の目安		備考
8(1)	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にするとともに、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。		
		1	取扱者の指定基準を規定していること。	
		2	取扱者の指定基準中に「保護すべき情報の取扱者の指定の範囲を必要最小限にするとともに、ふさわしいと認める者を充てること及び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」旨の規定を定めていること。	
		3	取扱者の指定手続き及び承認者を定めていること。	
		4	経営者等が取扱者に情報セキュリティ基本方針等を遵守させる方法を定めていること。	
8(2)	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。		
		1	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る手順を定めていること。	
		2	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、上記と同様の措置をとる手順を定めていること。	
8(3)	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。		
		1	取扱者に対する教育及び訓練の時期、頻度（少なくとも年１回以上）、内容等(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を含む。)を定めていること。	
		2	教育及び訓練の具体的な実施計画を定めていること。	
		3	教育及び訓練の実施者及び実施要領を定めていること。	
		4	教育及び訓練の有効性（理解度）の確認要領を定めていること。	
		5	教育及び訓練の実施状況について、記録要領及び少なくとも翌年度末まで保管する保管要領を定めていること。	
		6	新たに保護すべき情報を取り扱う者に対する教育及び訓練は、保護すべき情報へのアクセスを認可する前に実施することを定めていること。	
8(4)	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きを定めなければならない。		
		1	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手続きを具体的に定めていること。	
8(5)	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。		
		1	取扱者への周知要領を定めていること。	

調達における情報セキュリティ基準		判定の目安			備考
8(6)	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。			
			1	取扱者が所有する保護すべき情報の管理者への返却要領を定めていること。	
9(1)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。			
			1	保護すべき情報を取扱う施設の指定要領を定めていること。	
9(1)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。			
			1	保護すべき情報及び保護システムのある取扱施設は、関係者以外が容易に立ち入れない構造とすることを定めていること。	周囲を壁で囲まれた閉鎖空間等
			2	保護すべき情報及び保護システムのある取扱施設の出入口について、セキュリティ対策を規定していること。	施錠、有人受付、監視カメラ、警報装置等
9(1)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。※13（2）情報セキュリティの記録を参照			
			1	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明記していること。	
			2	取扱施設への第三者の立入りの記録要領及び記録の保管要領を定めていること。	
			3	取扱施設への立入を許可された第三者を識別するための立入許可証等の着用を定めていること。	
9(1)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、デジカメ等）を経営者等の許可なく利用してはならない。			
			1	取扱施設における保護すべき情報に係る作業の実施に当たっては、情報の流出、漏洩等に十分配慮することを定めていること。	
			2	取扱施設においては、通信機器及び記録装置の利用は事前に管理者が許可した場合を除き、利用してはならない事を定めていること。	
			3	通信機器及び記録装置を利用する場合の許可手続きを定めていること。	
9(2)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。			
			1	保護システムを設置する場合の保護すべき情報の流出、漏洩のリスクを十分に配慮した具体的対策を定めていること。	
9(2)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。			
			1	事前に経営者等が許可した場合を除き、取扱施設外への持ち出しを禁止することを定めていること。	
			2	持ち出しのリスクから保護できると判断する場合の判断基準を定めていること。	
			3	経営者等の許可を得て保護システムを取扱い施設外へ持ち出す場合の手続きを定めていること。	
			4	保護システムの持ち出し記録について、記録要領を定めていること。	

調達における情報セキュリティ基準		判定の目安			備考
9(2)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出来ない状態にする、又は取り外す等の処置を実施しなければならない。			
			1	第三者により保護システムを保守及び点検する場合、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の実施手順を定めていること。	
			2	第三者が保護システムの保守及び点検を実施する際に、保護策がとられていることを管理責任者が確認する手順を定めていること。	
9(2)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。			
			1	保護システムを破棄する場合及び再利用する場合の保護すべきデータが復元出来ないことを点検する手順を定めていること。	
			2	保護すべき情報が復元できない状態であることの点検を管理者が確認する手順を定めていること。	
			3	保護システムを破棄又は再利用する場合の実施記録について、管理者の確認記録を含め記録することを定めていること。	
10(1)	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。			
			1	保護システムの操作手順書の維持管理要領を定めていること。	
10(2)	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ー又はパソコン（以下「サーバー等」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。			
			1	保護システムのセキュリティパッチの適用及びウィルス対策ソフトウェアを最新の状態（ウィルス定義ファイル及びスキャンエンジンの更新など。）に維持する手順を定めていること。	
			2	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、週１回以上のフルスキャンの実施要領を定め、当該実施要領には保護システムのフルスキャンの実施とともにその実施状況を確認する手順を定めていること。ただし、１週間以上電源の切られた状態にあるサーバー等については、再度の電源投入時に最新の状態に更新されたウィルス対策ソフトウェアを用いてフルスキャンを行う手順を定めていること。	
			3	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ない場合は、最新の状態に更新されたウィルス対策ソフトウェアを用いて、１か月に１回以上のフルスキャンを行う実施要領を定めていること。ただし、１か月以上使用されていない保護システムについては、使用する直前にフルスキャンを行う実施要領を定めていること。	
			4	保護システムにおいて、可搬記憶媒体を使用する場合は、使用する直前に最新の状態に更新されたウィルス対策ソフトウェアを用いて、可搬記憶媒体に保存されているデータのスキャンを行う手順を定めていること。	

調達における情報セキュリティ基準		判定の目安		備考
10(3)	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7(2)及び次号に沿った取扱いを行わなければならない。		
		1	保護システム内の保護すべきデータを可搬記憶媒体にバックアップする際、保護すべき情報が保存されている場合は、保護すべき情報の取り扱いと同様の保管及び取扱いの手順を実施することを定めていること。	
10(4)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。※7(2)保護すべき情報の取扱いを参照		
		1	保護すべきデータを保存した可搬記憶媒体の保管要領、保管するロッカー等の鍵の管理要領を定めていること。	
		2	可搬記憶媒体は、保護すべき情報とそれ以外とを容易に区別できる表示要領を定めていること。	
10(4)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。		
		1	保護すべきデータを可搬記憶媒体に保存する際の暗号技術を用いる手順を定めていること。	
10(4)ウ	可搬記憶媒体の破棄及び再利用	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。		
		1	保護すべき情報を取扱った可搬記憶媒体を破棄又は再利用する場合の保護すべきデータを復元出来ない状態にする手順及び点検の手順を定めていること。	
		2	保護すべきデータが保存されていないこと及び復元出来ない状態であることを管理者が確認する手順を定めていること。	
		3	可搬記憶媒体を破棄又は再利用する場合の実施記録について、点検及び管理者の確認を含めて記録要領を定めていること。	
10(5)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。		
		1	通信機器を用いて保護すべき情報を伝達する場合のセキュリティ対策実施要領を定めていること。	
		2	通信機器を用いて保護すべき情報を伝達する場合のセキュリティ対策について、管理者の承認又は確認手順を定めていること。	
		3	通信機器を用いて保護すべき情報を伝達した場合の記録について、管理者の承認又は確認の記録を含め記録することを定めていること。	
10(5)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。		
		1	保護すべき情報の伝達及び送達する相手との守秘義務を定めた契約又は合意手順を定めていること。	

調達における情報セキュリティ基準		判定の目安			備考
10(5)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。			
			1	保護すべき情報を送達する場合の送達手順を定めていること。	
			2	保護すべき情報を送達する場合の送達記録について、記録要領を定めていること。	
10(5)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。※10(7)電子政府推奨暗号等の利用を参照			
			1	保護すべきデータを伝達する場合、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する手順を定めていること。	
			2	保護すべきデータを伝達する場合、伝達の記録要領を定めていること。	
			3	保護すべきデータを伝達する場合、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、この限りではないことを定めていること。	
10(6)	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。※10(7)電子政府推奨暗号等の利用を参照			
			1	保護システムに外部から接続を許可する場合の利用者の認証手順を定めていること。	
			2	保護システムに外部から接続を許可する場合の暗号技術を用いた接続手順を定めていること。	
10(7)	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。			
			1	暗号技術を用いる場合の電子政府推奨暗号等又はその他の秘匿化技術等の利用手順を定めていること。	
10(8)	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。			
			1	ソフトウェアの導入について、ソフトウェアの安全性の確認要領を定めていること。	
			2	保護システムへソフトウェアを導入する場合の許可権者及び許可手続きを定めていること。	
10(9)	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。			
			1	システムユーティリティの機能を使用できる者は、あらかじめ指定された管理者又は特定の取扱者のみに限定することを定めていること。	
10(10)	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。			
			1	技術的脆弱性に関する情報について、取得方法及び対処要領を定めていること。	
			2	技術的脆弱性への対策を実施する者（管理責任者又は特定の取扱者）を定めていること。	
10(11)ア	監査ログの取得	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。			
			1	利用者（管理者も含む）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の取得要領を定めていること。	

調達における情報セキュリティ基準		判定の目安			備考
10(11) 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。			
			1	取得した監査ログを記録のあった日から少なくとも３か月以上保存することを定めていること。	
			2	取得した監査ログを記録のあった日から１か月以内に点検を行う実施要領を定めていること。	
			3	取得した監査ログを施錠したロッカー等において保管又はアクセス制御等により厳重に保護するとともに、適切に鍵を管理することを定めていること。	
			4	監査ログを保存する目的が、保護すべき情報の流出、漏洩等の事案が発生した際に確認する証拠とすることを定めていること。	
10(11) 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。			
			1	取得した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ための対策を定めていること。	
10(11) 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。			
			1	保護システムにおける監査証跡を正確なものとするため、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時刻合わせを実施する手順を定めていること。	
10(11) 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、共有ネットワーク等を通じて、保護すべきデータの社外漏えいを未然に防止できることを可能とする常時監視を行わなければならない。			
			1	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、保護すべきデータの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の実施要領を定めていること。	
			2	常時監視中、異常が発見された場合の対処及び報告の実施要領を定めていること。 また、対処及び報告に当たっての責任者、担当者等を定めていること。	
11(1)	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。			
			1	取扱者及び利用者の職務に応じたアクセス制御方針に基づく実施手順を定めていること。	
			2	アクセス制御方針の見直す手順を定めていること。	

調達における情報セキュリティ基準		判定の目安			備考
11(2)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。			
			1	保護システムを利用する取扱者について、常時適切なアクセス権を付与されるように、利用者登録及び削除の手順を定めていること。	
11(2)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。			
			1	保護システム利用のための取扱者へのパスワードの割り当て方法及び配布要領を定めていること。	
11(2)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。			
			1	保護システムの管理者権限の付与要領及び利用規定を定めていること。	
11(2)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。			
			1	保護システムに関するアクセス権の割当ての見直し要領を定めていること。	
11(3)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。			
			1	パスワードの選択要領及び変更する期間を定めていること。	
11(3)イ	無人状態にある情報システム対策	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。			
			1	保護システムの設置された取扱施設が無人状態になる場合の機密性を考慮したセキュリティ対策の実施要領を定めていること。	
11(4)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。			
			1	保護システム利用者の職務内容に応じて、利用できる機能を制限する手順を定めていること。	
11(4)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。			
			1	保護システムから共有ネットワークへの接続について、アクセス制御方針に基づいた実施要領を定めていること。	
			2	保護システムから共有ネットワークへの接続に伴うリスクから保護するため、セキュリティ対策の実施要領を定めていること。	

調達における情報セキュリティ基準		判定の目安			備考
11(5)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。			
			1	保護システムを利用する場合のセキュリティを配慮したログオン手順を定めていること。	
11(5)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。			
			1	保護システムの利用者ごとに特定のユーザーID、ユーザー名等を割当てる手順を定めていること。	
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（パスワードの定期的な変更を利用者に促す機能又は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。			
			1	保護システムの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促す機能又はパスワードの再使用を防止する機能等）の具体的機能及び機能の実施手順を定めていること。	
12(1) (2)	情報セキュリティ事故等の報告及び報告要領	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へ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。 防衛関連企業は、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。			

調達における情報セキュリティ基準			判定の目安		備考
			1	情報セキュリティ事故が発生した場合、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、防衛省に報告するための報告要領を定めていること。（下請負者の場合は、契約相手方を通じて報告すること。）	
			2	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、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、防衛省に報告するための報告要領を定めていること。（下請負者の場合は、契約相手方を通じて報告すること。）	
			3	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、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、防衛省に報告するための報告要領を定めていること（下請負者の場合は、契約相手方を通じて報告すること。）	
			4	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するための報告要領を定めていること（下請負者の場合は、契約相手方を通じて報告すること。）	
			5	上記１から４までの報告後、速やかにその詳細を防衛省に報告するための報告要領を定めていること。（下請負者の場合は、契約相手方を通じて報告すること。）	
			6	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、その詳細を防衛省に報告するための報告要領を定めていること。（下請負者の場合は、契約相手方を通じて報告すること。）	
			7	上記１から６までの報告について、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するとともに、異動等のあった場合にはこれを更新する要領を定めていること。	
			8	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ことを定めていること。	
12(3)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。			
			1	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への対処体制、責任及び手順を定めていること。	
			2	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への対処手順（連絡手順、被害の拡大防止、証拠の保存、原因究明等）を定めていること。	

調達における情報セキュリティ基準		判定の目安			備考
12(3)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(1)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。			
			1	情報セキュリティ事故、その疑いのある場合及び12(1)イ(ｱ)の場合に関連する証拠を収集する具体的手順を定めていること。	
			2	上記において、収集した証拠を速やかに防衛省に提出する手順を定めていること。（下請負者の場合は、契約相手方を通じて提出する。）	
12(3)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。			
			1	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する手順を定めていること。	
13(1)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。			
			1	情報セキュリティ基本方針等の遵守状況に関して、点検の頻度、実施要領を定めていること。	
			2	不適切な事項を認めた場合、是正措置の手順を定めていること。	
			3	保護すべき情報の保管及び取扱いに係る管理者が、その保管状況及び取扱い状況について常に把握し、異常のないことを確認する手順を定めていること。	
13(1)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。			
			1	保護システムの利用に係る技術的遵守状況を確認する手順を定めていること。	
			2	不適切な事項を認めた場合の是正措置の手順を定めていること。	
13(2)	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重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。			
			1	保護すべき情報の保管及び取扱いに係る記録の具体的な保管手順並びに鍵の管理手順を定めていること。	
13(3)	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。			
			1	保護システムの監査に用いるツールの使用を必要最低限とするための使用要領を定めていること。	
13(4)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。			
			1	防衛省の実施する情報セキュリティ対策に関する監査の受査要領を定めていること。	
13(4)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ち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。			
			1	防衛省の実施する情報セキュリティ対策に関する監査に対する協力要領を定めていること。	

留意事項
（１）実施手順の項目は、事業所等の特性等に応じて必要な項目を追加して規定するものとする。
（２）実施手順の項目のうち、適用除外とする項目については、その理由を明記するものとする。