装装保第４２１０号
令和５年３月１４日
一部改正　装装保第１１７９７号
令和５年６月３０日
一部改正　装装保第１１６９３号
令和７年６月１７日

大臣官房長
各　局　長
施設等機関の長
各幕僚長殿
情報本部長
防衛監察監
各地方防衛局長

防衛装備庁長官
（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（防装庁（事）第１３７号。令和４年３月３１日）第１０項の規定に基づき、別添のとおり定め、令和５年４月１日から適用することとしたので通知する。

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
配布区分：長官官房審議官、各部長、施設等機関の長

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

令和５年３月

防衛装備庁

目次

別記様式第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(回答)
別記様式第７　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内容について(回答)
別記様式第８　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実施結果について(回答)

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に係る監査（以下「情報セキュリティ監査」という。）の実施要領及び情報セキュリティ監査に関する業務（以下「情報セキュリティ監査業務」という。）の協力要領は、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、仕様書等における、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（以下「特約条項」という。）が付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　定義

この実施要領において、用語の定義は、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（防装庁(事)第１３７号。令和４年３月３１日）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（装装保第４２０８号。令和５年３月１４日。以下「細部通知」という。）に定めるところによる。

1.4　情報セキュリティ監査の目的と実施者

⑴　情報セキュリティ監査は、契約に基づき監査対象の防衛関連企業（以下「監査対象企業」という。）の事業所等において取り扱われる保護すべき情報に対する情報セキュリティ対策の実施状況を確認するとともに、その情報セキュリティ対策に不備事項があれば監査対象企業に対して（下請負者の場合は、防衛省と直接契約した監査対象企業を通じて）是正措置を行うよう指導することにより、保護すべき情報の適切な管理に万全を期することを目的とする。

⑵　情報セキュリティ監査は、細部通知別紙の第３項第５号の規定により指定された監査官が実施するものとする。

1.5　情報セキュリティ監査の手順

⑴　情報セキュリティ監査の基本的な手順は、次に掲げるとおりとする。

ア　事前準備

イ　情報セキュリティ基本方針等の確認

ウ　実地監査

エ　指摘事項の改善状況の確認

⑵　前号ウの実地監査及び前号エの指摘事項の改善状況の確認については別

紙第１による。

2.　事前準備

⑴　監査官は、細部通知別紙の第３項第６号の規定による契約担当官等、物別官又は物別室長からの通知により、監査対象企業を把握するとともに、契約書及び仕様書等を入手し、その契約内容を把握する。

⑵　監査官は、情報セキュリティ監査の実施について監査対象企業に連絡するとともに、保護すべき情報の取扱予定等、情報セキュリティ監査に必要な情報を入手し、監査対象企業側の担当者と情報セキュリティ基本方針等の確認及び実地監査の実施時期等について調整する。

3.　情報セキュリティ基本方針等の確認

3.1　情報セキュリティ基本方針等の確認手順

⑴　監査官は、別記様式第１を基準として、情報セキュリティ基本方針等を提出するよう監査対象企業に求めるものとする。ただし、既に確認を受けた情報セキュリティ基本方針等と同一である場合は、別記様式第２を基準として、監査対象企業に届け出るよう求めるものとする。

⑵　前号の規定による提出を受けた監査官の所属する部署等の長（以下「監査官の所属長」という。）は、監査対象企業と調整の上、確認を行い、別記様式第３を基準として、監査対象企業に通知するものとする。

⑶　前２号の規定は、監査対象企業が既に確認を受けた情報セキュリティ基本方針等の全部又は一部を変更する場合について準用する。

⑷　監査官の所属長は、所属する監査官が確認した情報セキュリティ基本方針等について、その確認状況を四半期ごとに取りまとめ、別記様式第４を基準として当該四半期の翌月の２０日までに担当の契約担当官等に報告するとともに、その写しを装備政策部装備保全管理課長に送付するものとする。

3.2　情報セキュリティ基本方針の確認

情報セキュリティ基本方針の確認の適合性は、別紙第２の項目ごとに判定する。

3.3　情報セキュリティ規則の確認

⑴　情報セキュリティ規則の確認の適合性は、別紙第３の項目ごとに判定する。

⑵　監査対象企業が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別紙の装備品等及び役務の調達における情報セキュリ

ティ基準(以下「本基準」という。）に定められた管理策以外の管理策を採用する場合において、当該管理策の有効性が本基準の規定と同等以上であることが合理的に認められるときは、適合と判定するものとする。

⑶　監査対象企業が本基準に規定された項目を適用除外とする場合は、適用除外とする項目及び適用除外とする合理的な理由を確認し、情報セキュリティ規則に明記を求めるものとする。

3.4　情報セキュリティ実施手順の確認

⑴　情報セキュリティ実施手順の適合性は、別紙第４の項目ごとに判定する。

⑵　情報セキュリティ実施手順の確認に当たっては、監査対象企業の近年の情報セキュリティ事故及びサイバー攻撃事案の把握状況等を確認した上で、実施手順の各項目の管理策の必要性及び企業側のリスクの想定をヒアリング等により確認する。

⑶　監査対象企業が、保護システムに係る管理策の全部又は一部を外部の情報セキュリティ対策企業等に委託する場合は、システムセキュリティ実施要領の各項目に対応する管理策がどのように担保されているかを、情報セキュリティ実施手順に規定することを求め、内容を確認する。

⑷　監査対象企業が本基準及びシステムセキュリティ実施要領に定められた管理策以外の管理策を採用する場合において、当該管理策の有効性が本基準及びシステムセキュリティ実施要領の規定と同等以上であることが合理的に認められるときは、適合と判定するものとする。

⑸　監査対象企業が本基準及びシステムセキュリティ実施要領に規定された項目を適用除外とする場合は、適用除外とする項目及び適用除外とする合理的な理由を確認し、情報セキュリティ実施手順に明記を求めるものとする。

4.　情報セキュリティ監査業務に係る協力

4.1　情報セキュリティ監査業務に従事する職員間の協力

⑴　情報セキュリティ監査業務に従事する職員は、相互に協力するとともに、相互の情報交換等により監査技術及び関係知識の共有を図り、職員全体の技量の向上に努めるものとする。

⑵　情報セキュリティ監査業務は、指定された監査官が実施することを原則とし、他の監査官に協力を依頼する場合は、調整により監査結果の提供、実地監査への同行、助言等の協力を求めるものとする。また、同一年度において既に他の監査官が実地監査を実施した監査対象企業の事業所等について

は、当該監査官の実地監査結果を準用することができるものとする。

4.2　防衛省の地方調達契約に係る監査等の調整要領

⑴　防衛省の地方調達（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５条の２に規定する地方調達をいう。以下同じ。）の契約担当官等は、実地監査及び情報セキュリティ基本方針等の確認又は保護すべき情報を下請負者に取り扱わせる場合の申請について、指定した監査官以外の監査官に協力を依頼する必要がある場合は、その理由を明確にし、依頼する監査官の所属長と事前に調整した上、別記様式第５を基準として協力を依頼する。

⑵　前号の規定による依頼を受けた監査官の所属長は、具体的な協力事項及び実施要領等について、依頼元の契約担当官等と調整を実施するものとし、協力の回答をする場合には、別記様式第６を基準として作成し、依頼元の契約担当官等に回答する。

⑶　依頼を受けた監査官の所属長は、実地監査等の協力を実施するに当たり、依頼元の契約担当官等に対し、協力事項に応じ、別記様式第７を基準として回答し、実地監査等を実施した場合は、当該監査等の結果を別記様式第８を基準として回答する。

⑷　第３項において監査対象企業から提出された情報セキュリティ基本方針等の受理及び監査対象企業に対する確認通知並びに監査対象企業への実地監査の実施通知及び結果等の通知は、依頼した契約担当官等が実施する。

5.　情報セキュリティ監査等の教育及び指導

⑴　監査官の所属長は、所属する情報セキュリティ監査業務に従事する職員の監査技術及び関連知識の向上を図るために必要な教育を適時実施するものとする。

⑵　装備政策部長は、情報セキュリティ監査業務に従事する職員の監査技術の向上及び均一化を図るための教育を定期的に実施するものとする。

⑶　装備政策部長は、情報セキュリティ監査業務に従事する職員の実施する情報セキュリティ監査業務に関し、必要に応じて、監査実施要領の指導及び監査実施状況の確認を関係職員に行わせるものとする。

別紙第１

情報セキュリティ監査の実地監査等の実施要領

令和５年３月

防衛装備庁

目次

1.　目的

この要領は、情報セキュリティ監査の実地監査及び指摘事項の改善状況の確認に必要な事項を定めることを目的とする。

2.　実地監査の区分及び手法

2.1　実地監査の区分

情報セキュリティ監査の実地監査は、次の区分により実施するものとする。

⑴　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別紙の装備品等及び役務の調達における情報セキュリティ基準（以下「本基準」という。）による運用開始後又はシステムセキュリティ実装計画確認後に、本基準に基づく監査を初めて受ける防衛関連企業に対して実施する監査

⑵　維持監査

初回監査の翌年度以降、年１回以上定期的に特約条項の遵守状況及び情報セキュリティ基本方針等の有効性及び遵守状況を確認する監査

2.2　実地監査手法

実地監査は、次の手法を組み合わせて、情報セキュリティ規則及び情報セキュリティ実施手順の遵守状況を確認するものとする。

⑴　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

⑵　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

⑶　質問による確認：総括者、管理者、取扱者、保護システム管理者及び担当者、保護シテム利用者等の職務に関する認識及び知識、保護すべき情報及び保護システムの取扱状況等

⑷　観察による確認：取扱施設等の指定、設備の管理状況、機器の設置状況等

⑸　試行による確認：入退管理装置、保護システムへのアクセス制限等の機能等

3.　実地監査計画等の作成及び送付

3.1　実地監査計画の作成

⑴　監査官の所属長は、実地監査の目的を有効かつ効率的に達成するため、毎年度当初、装備政策部装備保全管理課長と調整の上、履行中の契約等に係る実地監査計画を作成するほか、次に掲げる場合には実地監査計画を作成し、付紙第１号様式を基準として担当の契約担当官等、物別官又は物別室長に

報告するとともに、その写しを装備政策部装備保全管理課長に送付するものとする。

ア　細部通知第３項第６号の規定による契約担当官等、物別官又は物別室長からの通知を受領した場合

イ　監査対象企業の情報セキュリティ対策に関して、実地監査の必要があると認めた場合

ウ　既に報告した実地監査計画の内容を変更する場合

⑵　実地監査計画は、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監査対象企業の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。

⑶　実地監査計画は、契約の内容及び履行過程、保護すべき情報の取扱状況等を考慮し、実地監査の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実地監査項目等を考慮して適切な監査期間を設定する。

⑷　実地監査の項目は、付紙第２号様式を基準として、次の監査区分に基づく項目を対象とする。

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又は不良の指摘をした項目及びその他保護すべき情報の取扱状況等に応じた必要な項目（システムセキュリティ実施要領に関する項目は省略不可）とする。

ウ　従来から実施している情報セキュリティ対策に新たな項目を追加、あるいは項目を変更又は削除した場合は、該当する項目は必須とする。

3.2　実地監査通知

⑴　監査官の所属長は、監査対象企業と調整した上で、付紙第３号様式を基準として、監査対象契約、監査対象事業所名、実地監査の実施期間及び監査官等を監査対象企業に通知するとともに、その写しを契約担当官等、物別官又は物別室長及び装備保全管理課長に送付するものとする。

⑵　前号に規定する調整により管轄の区域外に所在する事業所等の実地監査が必要と認める場合には、事前調整の上、付紙第４号様式を基準として作成し、関係書類を添えて当該事業所等の所在地を管轄する監査官の所属長に前号の通知をするものとする。

⑶　前号の依頼を受けた監査官の所属長は、所属の監査官に実地監査を行わせ、その結果を付紙第５号様式を基準として依頼を行った監査官の所属長に通知するものとする。

4.　実地監査の実施

4.1　保護すべき情報の取扱状況の把握

監査官は、実地監査の開始に当たり、監査対象企業の担当者から契約履行の状況を聴取し、保護すべき情報が取り扱われる過程を確認し、各過程における情報セキュリティ上のリスクの有無を検討する。また、保護対象の情報資産の特定について、監査対象企業の担当者と防衛省の認識の齟齬について確認するものとする。

4.2　実地監査における留意事項

⑴　監査官は、実地監査計画に基づき、付紙第２号様式「情報セキュリティ実地監査確認書」に定める項目ごとに監査対象企業の担当者の立会いの下、情報セキュリティ対策の実施状況を確認及び評価する。

⑵　監査対象企業が前号に定める確認項目以外の管理策を採用している場合及び、当該管理策の有効性が情報セキュリティ基本方針等の規定と同等以上であることが合理的に確認できる場合は、適合と判定するものとする。

⑶　監査対象企業における保護すべき情報の取扱状況等に応じて実地監査を複数回に分割して実施する場合は、監査項目を適宜分割し、限られた期間内に効果的、効率的な監査の実施に努めるものとする。また、監査対象企業の保護すべき情報の取扱状況に応じて、適宜項目を追加して確認するものとする。

4.3　実地監査結果の確認

⑴　監査官は、実地監査の際に不備事項を認めた場合は、監査対象企業の立会者に対し、その場で指摘の内容及び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、監査対象企業に対して総合評価及び指摘事項等を講評し確認を得るものとする。

⑵　実地監査結果の評価及び指摘事項について監査対象企業と見解の相違がある場合は、その場の評価を保留とし、後日、協議を行うものとする。協議においては、保護すべき情報の漏えい、紛失、改ざん等、想定されるリスクの回避、低減等に効果のある管理策であるか否かを基準として再度判定するものとする。

5.　実地監査結果の報告書等の作成及び送付

5.1　実地監査調書の作成と保管

⑴　実地監査の実施内容の記録として、付紙第２号様式を基準として監査項

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、監査対象企業の立会者名、指導した是正措置、その他一連の実地監査事項の詳細な記録を監査調書として作成し保管する。

⑵　実地監査調書は事業所等ごとに取りまとめ、文書で保管する場合は施錠したロッカー等に、データで保存する場合は暗号化等により、必要な期間保存又は保管するものとする。

5.2　評価

監査官は、実地監査結果について、下表の「項目別評価基準」及び「総合評価基準」に基づき確認項目ごとの評価と総合評価を実施する。なお、評価に当たっては、保護すべき情報の漏えい、紛失、改ざん等の想定されるリスクを回避、低減等する効果のある管理策か否かを基準として評価するものとする。

【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) 軽微な指導事項(記録の一部記入漏れ、誤記等)はあるが、即時に訂正が確認でき、項目全体として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) 定められた情報セキュリティ対策が保護すべき情報の取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えい又は流出につながるおそれがある状態。 (3) 定められた情報セキュリティ対策が保護すべき情報の取扱いの現状と符合せず、管理策の全面的な見直しが必要である。

【総合評価基準】

評　価	基　準
良　好	「良好」又は軽微な「要改善」項目がある場合
要改善	「要改善」又は他の対策で補填可能な「不良」がある場合
不　良	情報漏えい等につながる致命的な「不良」項目がある場合

5.3　実地監査結果通知の作成及び送付

監査官の所属長は、実地監査終了後、実地監査調書を基に監査結果をまとめ、付紙第６号様式を基準として実地監査結果通知を作成し、監査対象企業に送付するとともに、その写しを装備政策部装備保全管理課長に送付する。通知には、実施した監査の概要、実地監査結果の総合評価等を記載し、指摘事項がある場合は、付紙第６号の２様式を基準として項目別に簡潔に記載し、是正措置を要求する。

5.4　実地監査報告書の作成及び送付

⑴　監査官は、実地監査終了後、実地監査調書を基に監査結果をまとめ、付紙第７号様式を基準として実地監査報告書を作成する。報告書の作成に当たっては、監査対象企業の情報セキュリティ対策の状況の把握に留意し、監査対象企業の事業所等ごとに監査概要、監査項目、実地監査結果及び評価、指摘事項、所見等を簡潔に記載する。

⑵　監査官の所属長は、所属する監査官の実地監査の実施状況を四半期ごとにとりまとめた報告書を付紙第８号様式を基準として作成し、前号の実地監査報告書を添付して当該四半期の翌月２０日までに担当の契約担当官等、物別官又は物別室長に送付するとともに、その写しを装備政策部装備保全管理課長に送付するものとする。

6.　指摘事項の是正指導

⑴　監査官は、実地監査において「要改善」及び他の対策で補填可能な「不良」の評価に当たる指摘事項がある場合は、監査対象企業に対して、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、次回の監査時において確認する。なお、次回の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。

⑵　実地監査において情報漏えい等につながる致命的な「不良」評価に当たる指摘事項がある場合は、監査対象企業に対して、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。

7.　下請負者に対する監査

⑴　下請負者に対する監査は、特約条項に基づき、防衛省と直接契約した監査対象企業が確認した下請負者の情報セキュリティ対策確認書を届け出させ、

監査官がその内容を確認するものとし、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又は保護すべき情報の取扱経験が浅いなど）に実施する。

⑵　下請負者の監査の確認内容は、原則として監査対象企業の定めた情報セキュリティ基本方針等に則り、下請負者における適切な取扱いに必要な事項とする。

⑶　下請負者を実地監査する場合は、あらかじめ監査対象企業と調整の上、監査対象企業を通じて監査の対象、実地監査項目等を通知し、監査対象企業の立会いの下、監査対象企業の監査等の手順に準じて実施する。

⑷　下請負者の監査対象事業所が管轄区域外の場合は、第３項を準用して当該事業所等を管轄する地方防衛局等へ下請負者に対する実地監査を依頼するものとする。なお、下請負者に対する監査を実施する場合は、原則として監査対象企業の立会いの下、行うものとする。

⑸　下請負者に対する実地監査の結果、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、監査対象企業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、第６項を準用して改善状況を確認する。

付紙第１号様式(第 3.1 関係)

文 書 番 号
発簡年月日

(契約担当官等、物別官、物別室長)
殿

(監査官の所属長)

情報セキュリティ監査の実地監査計画について(報告)

標記について、次のとおり計画・変更したので報告する。

令和　　年度　　情報セキュリティ監査計画書(第　　回)

番号	契約相手方 監査対象事業所名	監査区分	実施時期	監査実施項目	備　考

写送付先：装備政策部装備保全管理課長

付紙第２号様式(第3.1関係)

情報セキュリティ実地監査確認書

番号	対応条項	項目 情報セキュリティ基準	評価	確認者	確認日	備考
1	共通	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に従い『情報セキュリティ基本方針（基本方針）』、『情報セキュリティ規則（規則）』、『情報セキュリティ実施手順（実施手順）』が作成されていること。				
2	第4	『情報セキュリティ基本方針等』の作成・周知について ①定めた手順に従い、情報セキュリティ基本方針等の定期的な見直しを行っていること。（適切/有効/妥当性の維持） ②定めた手順に従い、情報セキュリティ基本方針等を変更した場合は、経営者等の承認、防衛省の確認、取扱者への周知を適切に行っていること。 ③定めた手順に従い、情報セキュリティ実施手順を社外の者にみだりに公開しないよう適切に管理していること。				
3	第5	組織のセキュリティについて ①定めた手順に従い、情報セキュリティ体制を構築するとともに各職責を明示化し、情報セキュリティ管理策が適切に実施されていること。 ②定めた手順に従い、保護すべき情報を取り扱う下請負者の防衛省からの承認、下請負者の情報セキュリティの実施状況を確認していること。				
4	第6	保護すべき情報の管理について ①定めた手順に従い、保護すべき情報の授受、作成、制作、複製（バックアップを含む。）、閲覧、持ち出し、送達、返却、提出、廃棄を実施するとともに関係記録を保管又は保存していること。 ②防衛関連企業の情報を公開する場合は、定めた手順に従い、保護すべき情報が含まれていないことを確認していること。				
5	第7	情報セキュリティ教育及び訓練について ①定めた手順に従い、定期的及び必要な場合に教育及び訓練を実施し、取扱者の意識及び能力向上を行っていること。 ②同教育に関する計画、実施記録等を作成し、保管又は保存していること。				
6	第8	物理的及び環境的セキュリティについて 定めた手順に従い、物理的及び環境的セキュリティ管理策を実施していること。 （例：取扱施設等、入退管理機器、保護システム、保管された保護すべき情報の指定、管理等）				
7	第9	保護システムの管理策の運用ルールを定めていること。				
8	第10 11	情報セキュリティ事故等への対処及び対応について ①情報セキュリティ事故等対処計画を定め、事故発生時における適切な処置の実施と、報告要領等を明確化し、取扱者等に周知していること。 ②情報セキュリティ事故等対処計画に基づく事故等対処テストを定期的に実施し、その記録を保管又は保存していること。				

9	第12	リスク査定について ①リスク査定に関する手順を定め、保護すべき情報に関するリスクの特定、分析、評価を定期的に実施し、その結果を定められた者に周知していること。 ②リスク査定の分析結果、その対処に関する記録を保管又は保存していること。				
10	第13	セキュリティ監査について ①定めた手順に従い、セキュリティ監査を計画的に実施し、その結果を定められた者に周知し、改善等の適切な措置を行っていること。 ②セキュリティ監査の計画、結果等の文書を作成し、保管又は保存していること。				
11	第14	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（施設への立入り、監査官による書類の閲覧等）を行っていること。				
		システムセキュリティ実施要領				
1	第2	システムセキュリティ実装計画について 定めた手順に従い、『システムセキュリティ実装計画書』が作成、変更、承認、周知、及び保管又は保存され、防衛省の確認を受けていること。				
2	第3	構成管理について ①定めた手順に従い、保護システムのベースライン構成設定を定め、設定されていること。 ②定めた手順に従い、保護システムの構成設定目録が適切に作成・変更され、構成設定に関する記録が適切に保管及び保存されていること。				
3	第４	保護システムの基本的防御について ①定めた手順に従い、保護システムの領域（範囲）が明確にされていること。 ②定めた手順に従い、保護システムの操作手順書が作成、変更、周知されていること。 ③定めた手順に従い、保護すべきデータが適切に暗号化されていること。 ④定めた手順に従い、暗号鍵の管理が適切に行われていること。 ⑤定めた手順に従い、保護システムへのソフトウェアインストール、アップデートが行われていること。 ⑥定めた手順に従い、保護システムにおけるアプリケーションの権限管理が適切に行われていること。 ⑦定めた手順に従い、仮想化システムに対して物理システム同様、各種管理策が取られていること。 ⑧定めた手順に従い、保護システムと外部システムとの接続及びその使用が制限されていること。				
4	第５	アクセス制御について ①定めた手順に従い、保護すべきデータ及び保護システムに対する物理的・論理的なアクセス制御が適切に行われていること。 ②定めた手順に従い、アカウント管理者が指定され、アカウント管理(設定、変更、削除等)が適切に行われていること。 ③定めた手順に従い、保護システムへのログオン管理が適切に行われていること。 ④定めた手順に従い、保護システムのユーザーセッション管理が適切に行われていること。 ⑤定めた手順に従い、保護システムへのリモートアクセスが適切に行われていること。特に、リモートアクセス時の通信経路が暗号化されていること。				
5	第６	識別及び認証について 定めた手順に従い、保護システムの識別及び認証が適切に行われていること。また、多要素認証が導入されていること。				

6	第７	通信の制御について 定めた手順に従い、モバイルコード、VoIP、オフィス機器等の通信機能の利用が適切に制限されていること。				
7	第８	システム監視について 定めた手順に従い、保護システムの内部及び外部境界に対する以下の項目の監視が適切に行われ、関連記録が適切に保管又は保存されていること。 ①不正な相手方又は方法等によるアクセス。 ②権限（管理者権限を含む。）の不正な使用。 ③内部及び外部との不正な通信。 ④悪意のあるコードの侵入。				
8	第９	システムログについて 定めた手順に従い、保護システムのシステムログが適切に取得、分析、保存又は保管されていること。				
9	第１０	脆弱性スキャンについて ①定めた手順に従い、保護システムの脆弱性スキャンが適切に実施され、その分析結果の利用も適切に行われていること。 ②定めた手順に従い、脆弱性スキャンの実施に関する記録(脆弱性スキャンの分析結果等)が保管又は保存されていること。				
10	第１１	バックアップについて 定めた手順に従い、保護システムのサーバ及びパソコンに保存している全ての保護すべきデータ及び保護システムにおけるシステムデータについて、定期的にバックアップが行われ、当該データが適切に管理されていること。				
11	第１２	システムメンテナンスについて ①システムメンテナンス等計画が作成され、同計画に基づきシステムメンテナンスが適切に実施されていること。 ②定めた手順に従い、システムメンテナンスに係る記録が保管又は保存されていること。				
12	第2 1 (2)、第2 2、第4 2 (1)、第5 1 (2) (3)	各種書類の作成・変更について、承認プロセスが定められ機能していること。				
13	第3 2 (1)、第3 3	保護システムの各種設定・設定変更について、承認プロセスが定められ機能していること。				
14	第2 3、第2 5、第3 4、第5 2 (1)、第12 3	定めた手順に従い、各種書類・データ（記録文書データ含）の保管・保存が適切に行われている。また、必要がある場合は防衛省に提出していること。				
留意事項（１）上記項目は、事業所等の特性に応じて必要な項目を追加して規定する。 （２）上記項目のうち、適用除外とする項目については、その理由を明記する。			総合評価			【コメント】

付紙第３号様式(第 3.2 関係)

文 書 番 号
発簡年月日

(監査対象企業)

殿

(監査官の所属長)

情報セキュリティ対策に関する実地監査の実施について(通知)

下記の契約に係る「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」第５条に規定する情報セキュリティ対策に関する実地監査を実施しますので通知します。

記

１　調達要求番号：
２　契約品名・認証番号又は契約番号(年月日)、納期：
３　事業所名(所在地)：
４　監査対象部門(所在地)：
５　監査官名：
６　監査実施期間：

写送付先：契約担当官等、物別官、物別室長、装備政策部装備保全管理課長

付紙第４号様式(第 3.2 関係)

管轄区域外(監査対象事業所・下請負者)実地監査依頼書

文 書 番 号
発簡年月日

(依頼先の監査官の所属長)
殿

(依頼元の監査官の所属長)

貴管管轄区域にある(監査対象事務所・下請負者)について、次の事項に関する実地監査を行われたく依頼する。

実地監査項目

備 考

添付書類：情報セキュリティ基本方針等
保護すべき情報のリスト

付紙第５号様式(第 3.2 関係)

管轄区域外（監査対象事業所・下請負者）実地監査結果通知書

文 書 番 号
発簡年月日

(依頼元の監査官の所属長)
殿

(依頼先の監査官の所属長)

(依頼文書番号等)により依頼のあった、(監査対象事業所・下請負者)に係る実地監査を実施したので、次のとおりその結果を通知する。

監査項目及び結果

備 考

添付書類：実地監査報告書、指摘事項通知（指摘事項がある場合）
情報セキュリティ基本方針等、保護すべき情報のリスト（返却）

付紙第６号様式(第 5.3 関係)

文 書 番 号
発簡年月日

(監査対象企業)

殿

(監査官の所属長)

情報セキュリティ実地監査結果について（通知）

標記について、下記のとおり通知します。
(要改善の場合)
なお、指摘事項については、速やかに是正の上、報告してください。
(不良の場合)
なお、指摘事項については、速やかに是正の上、再度監査を受けてください。

記

１　監査実施日または期間：
２　監査対象事業所等名：
３　監査区分：(初回監査・維持監査)
４　監査結果：(　良　好・ 要改善 ・不　良　)
監査指摘事項の内訳は、別紙のとおりです。(結果が要改善又は不良の場合)
５　監査実施者：
６　調達要求番号：

添付書類：(別紙として「指摘事項通知書」を添付する。(指摘がある場合))
写送付先：装備政策部装備保全管理課長

付紙第６号の２様式(第 5.3 関係)

別紙

指 摘 事 項 通 知 書

監査対象企業名：
監査対象事業所等名：

番号	情報セキュリティ 監査確認書の項目	指 摘 事 項	備 考

付紙第７号様式(第5.4関係)

情報セキュリティ実地監査報告書

監査対象企業 監査対象事業所等名	
同上所在地	
監査対象企業の立会者名 (所属・役職等)	
調達要求番号 契約品名 納　期	
保護すべき情報の取扱い状況(予定を含む)	文書・物件保管、文書作成・複製、文書閲覧、物件作成、 プログラム等の製作・複製、その他(　　)
情報セキュリティ基本方針等の確認年月日	
監査区分(前回監査日)	初回監査・維持監査(年月日)
監査結果	(記載例) 情報セキュリティ規則及び実施手順の遵守状況等について監査した。 監査実施項目：　　項目 監査別評価　：良　好　　件 要改善　　件 不　良　　件 (指摘事項の内訳は、別紙のとおり。)
所見等	
監査実施年月日(期間) 情報セキュリティ 監査官名	令和　　年　　月　　日 所属 氏名

添付書類：(別紙として「指摘事項通知書」を添付する。(指摘がある場合))

付紙第８号様式(第 5.4 関係)

文 書 番 号
発簡年月日

(契約担当官等、物別官、物別室長)
殿

(監査官の所属長)

情報セキュリティ監査の実地監査の実施状況について(報告)

標記について、次のとおり実施したので報告する。

実地監査実施状況
(令和　年度　第　／四半期分)

監査実施日 又は期間	契約相手方 監査対象事業所等名	調達要求番号 契約品名	監査対象契約 通知書番号	備 考

添付書類：情報セキュリティ実施監査報告書
写送付先：装備政策部装備保全管理課長

別紙第2(第3.2関係)

情報セキュリティ基本方針の判定基準

大項	中項	基本方針の項目	判定※	確認者	確認日	備考
1		目　的				
	1	防衛省との契約に基づく保護すべき情報に関して、情報セキュリティの確保を目的としている。				基本方針が保護すべき情報に特化されている場合
	2	防衛省との契約に基づく保護すべき情報に関して、情報セキュリティを確保することが包含されている。				民生部門と基本方針が共通化されている場合
2		基本方針の役割と位置付け				
	1	前項の目的を実現するための活動の指針であり、情報セキュリティ対策に関する最も基本的な方針を示す規定であることを定めている。				
3		経営陣の承認				
	1	経営陣の承認と責任のもと組織の情報セキュリティ対策に取り組むことを定めている。				
4		適用対象範囲				
	1	防衛省との契約に基づく保護すべき情報を対象としている。				基本方針が保護すべき情報に特化されている場合
		防衛省との契約に基づく保護すべき情報が対象に含まれている。				民生部門と基本方針が共通化されている場合
	2	防衛省との契約に基づく保護すべき情報を取り扱う可能性のある全ての者を対象としている。				基本方針が保護すべき情報に特化されている場合
		防衛省との契約に基づく保護すべき情報を取り扱う可能性のある全ての者（防衛部門に所属する全ての者）が対象に含まれている。				民生部門と基本方針が共通化されている場合
5		情報セキュリティに関する取組み				
	1	防衛省の定める「装備品等及び役務の調達における情報セキュリティ基準」に基づき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。				民生部門と基本方針が共通化されている場合で、各項目の内容を包含している場合も適合とする。
	2	情報セキュリティ対策を実施するための組織を構築し運用することを定めている。				
	3	情報セキュリティ基本方針を頂点として、情報セキュリティ規則、情報セキュリティ実施手順その他必要な規程により情報セキュリティに関する体系を作成することを定めている。				
留意事項 既に契約相手方で基本方針が規定されている場合、同様の内容であれば項目名、順番にかかわらず適合とする。			総合判定			【コメント】

※判定は「適合」、「不適合」、「除外」を記載。

別紙第3(第3.3関係)

情報セキュリティ規則の判定基準

項目	対応条項	確認項目（防衛省確認事項）	判定※	確認者	確認日	備考
	第4	**情報セキュリティ基本方針等**				
1	第4　1	情報セキュリティ基本方針等の作成及び変更について、以下のことを定めていること。				
2		① 情報セキュリティ基本方針等の、本基準に沿った作成・変更				
3		② 情報セキュリティ基本方針等の、経営者等による承認				
4		③ 情報セキュリティ基本方針等の、作成・見直し及び変更の手順 （情報セキュリティに係る重大な変化及び事故発生時、内容変更時、防衛省の確認等を定期的に実施）				
5	第4　2	情報セキュリティ基本方針等の周知等について以下のことを定めていること。				
6		①取扱者への周知（情報セキュリティ基本方針等）				
7		②情報セキュリティ実施手順の管理要領（社外の者にみだりに公開しないように適切な管理）				
8	**第5**	**組織のセキュリティ**				
9	第5　1、2	経営者等及び取扱者の責務について以下のことを定めていること。				
10	第5　2(1)	①経営者等が自社の情報セキュリティの最高かつ最終的な権限及び責任を有すること。				
11		②経営者等が保護すべき情報の取扱者を指定すること及びその条件(守秘義務の合意、ふさわしい者等)				
12		③経営者等による保護すべき情報に係る総括者及び管理者の指定				
13		④保護すべき情報の取扱者名簿の作成及び変更要領 （管理者による作成及び更新、防衛省への届出、取扱者でなくなる者への守秘義務の確認）				
14	第5　2(2)	保護システム利用者の指定等について以下のことを定めていること。				
15		①経営者等が保護システム利用者を指定すること及びその条件（書面による同意）				
16		②経営者等による保護システム管理者及び保護システム担当者の指定				
17		③保護システム管理者による保護システム利用者名簿の作成及び更新				
18	第5　2(3)	情報セキュリティの確保について以下のことを定めていること。				
19		①取扱者以外の者は保護すべき情報に接してはならない。				
20		②職務上の下級者に対して保護すべき情報の提供を要求してはならない。				

21		③全ての従業員に対し情報セキュリティ事故等を発見又は検知した場合の報告義務及び全ての従業員の義務の履行				
22		④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措置(対処方針、懲戒手続及びそれらに基づく対処等)を定めていること				
23	第5　3	保護すべき情報を取扱う下請負者について以下のことを定めていること。				
24		① 契約上の義務に本基準に基づいた保護すべき情報の取扱いの実施を包含				
25		② 防衛省が定める確認事項に基づく下請負者の確認の実施及び防衛省への届出				
26	第5　4	第三者について以下のことを定めていること。				
27		① 防衛省の許可なく保護すべき情報を第三者に取り扱わせない。				
28		② 第三者との契約において自社の保有又は知り得た情報を伝達、交換、共有、提供する約定がある場合は、約定の対象から保護すべき情報を除く				
29		③ 保護すべき情報の第三者への開示についての手順				
30	**第6**	**保護すべき情報の管理**				
31	第6　2	保護すべき情報の目録の作成等について以下のことを定めていること。				
32		① 保護すべき情報の管理状況を記載した目録の作成及び作成要領（保護すべき情報の名、保管した場所等）				
33		②保護すべき情報の管理状況を記載した目録の更新要領（接受等があった場合に更新、接受者の氏名、所属、所在等の記載）				
34		③ 保護すべき情報の管理状況を記載した目録の保管要領（文書の場合：施錠したロッカー等、データの場合：暗号化、保存又は保管期間）				
35	第6　3	保護すべき文書等の表示等について以下のことを定めていること。				
36		① 保護すべき文書等（文書と可搬記録媒体）への表示及び、保護すべき情報が記載された箇所の明示をする。				
37		② 保護すべき情報を封筒又はコンテナ等の容器に保管する場合の表示及びその要領				
38	第6　4	保護すべき情報の持ち出し及び送達の方法について以下のことを定めていること。				
39		①持ち出し及び送達を行う場合の手順 a 管理者の許可 b 施錠等により物理的に保護された容器に格納して輸送 c 送達することができる者を業務の遂行上必要最小限度に制限 d 送達する場合の容器に対する表示方法 e 当該情報を受け取る者に直接手交（郵便の場合は書留）				
40	第6　5	保護システムにおける可搬記憶媒体等の使用制限について以下のことを定めていること。				
41		①使用できる可搬記憶媒体の目録の作成及び更新要領 (可搬記憶媒体ごとの使用用途、更新する場合、使用者名簿等)				
42		②個人が所有若しくは管理者が明確でない可搬記憶媒体の保護システムでの使用禁止				
43		③可搬記憶媒体を使用できる者を業務上必要最小限度				

44		④保護すべきデータの可搬記憶媒体への複製をソフトウェアにより制御する等の技術的措置				
45		⑤可搬記憶媒体を保護システム以外の情報システムへの接続を制限 (接続を行う場合の手順)				
46	第6　6	保護すべき情報を記録した媒体の廃棄又は再利用について以下のことを定めていること。				
47		① 保護すべき文書等、保護すべきデータを保存した可搬記憶媒体及び保護システムを廃棄する場合の措置及び手順				
48		② 可搬記憶媒体及び保護システムを再利用する場合の措置及び手順				
49		③ 破棄及び再利用する場合の点検についての措置及び手順(点検の記録要領、実施者の指定手順等)				
50	第6　7	保護すべき文書等の防衛省への返却等について、以下のことを定めていること。				
51		① 契約履行後、防衛省の指示に従い保護すべき文書等に行う措置及び手順				
52		② 保護すべき文書等を引き続き保有する必要がある場合の措置及び手順				
53	第6　8	保護すべき情報の作成等及びその持ち出し、送達、返却及び破棄に係る手順を定めていること。				
54	第6　9	防衛関連の情報を公開する場合の措置及び手順(保護すべき情報の有無の確認)について定めていること。				
55	**第7**	**情報セキュリティ教育及び訓練について以下のことを定めていること。**				
56		①取扱者に対する教育及び訓練の実施要領 a 実施の時期：定期的(１年に１回以上)、新たに取扱者を指定する場合等 b 内容等：技術的・専門的事項、職務に関する事項、部外の知見の利用 c 教育実施者：経営者等、総括者、管理者、保護システム管理者、外部の識者				
57		②教育及び訓練の具体的な実施計画				
58		③教育及び訓練の実施状況の記録及び保管又は保存要領				

59	**第8**	**物理的及び環境的セキュリティ**				
60	第8　1	物理的セキュリティ対策の方針において以下のことを定めていること。				
61		①取扱施設等、入退管理機器、保護システム及び保管された保護すべき文書等に対する物理的セキュリティ対策の方針の作成				
62		②物理的セキュリティ対策の方針の作成並びに精査及び修正する要領				
63	第8　2	取扱施設等に対する物理的セキュリティ対策について以下のことを定めていること。				
64		①取扱施設及び関係施設の指定				
65		②取扱施設内での保護システムの設置及び保護すべき情報の取扱い				
66		③取扱施設等立入名簿の作成・更新要領（管理責任者が作成、保護システム管理者の同意、取扱施設等の立入許可者を業務上必要最小限の範囲とし証明書を発行する、定期的な見直し及び更新等）				
67		④取扱施設と関係施設の境界に入退口の設置及び入退者を入退管理機器又は警備員等による管理				
68		⑤関係施設の外側境界に入退口の設置及び入退者の制限				
69		⑥取扱施設への入退をIDカードにより管理する場合の要領 （入退記録の取得、記録の見直し等）				
70		⑦取扱施設への入退を警備員等により管理する場合の要領 （入退記録簿の記載内容、記録の見直し等）				
71		⑧敷地を取扱施設等に指定した場合のフェンス等の措置及び手順				
72		⑨取扱施設の入退をICカードのみで管理する場合の必要な措置の要領				
73		⑩取扱施設に携帯電話、デジタルカメラ、ボイスレコーダー等を持ち込む場合の手順				
74		⑪保管又は保存要領は、契約履行後1年間を目安				
75	第8　3	入退管理機器に対する物理的セキュリティ対策について以下のことを定めていること。				
76		①入退管理機器の現状を記録した目録の作成（入退機器の名称、導入年月、責任者等）及び更新(修理及び責任者の変更等)並びに保存又は保管の要領				
77		②入退管理機器として暗証番号を併用する場合の措置				
78		③入退管理機器として鍵を併用する場合の措置				
79	第8　4	保護システムに対する物理的セキュリティ対策について以下のことを定めていること。				
80		①保護システムを構成するハードウェア及び記憶媒体への不正な移動及び持ち出しを防止する措置（施錠できるラック等に設置、ワイヤーでの固定等）				

81		②保護システムの持ち出しについての措置及び手順(許可権者、持ち出し者が保護システム利用者以外の場合等)				
82		③保護システムに接続された送配線に対する措置（たやすく切断されない措置：カバー等の設置)				
83	第8　5	保管された保護すべき情報に対する物理的セキュリティ対策について以下のことを定めていること。				
84		①保護すべき情報を文書及び可搬記憶媒体並びに保護システムに保管又は保存する場合の措置及び手順				
85		②保護すべき情報を保管しているロッカー等の鍵の措置及び手順				
86	**第9**	**保護システムの管理策について以下のことを定めていること。**				
87		①自社の保有又は使用する保護システムに必要と認める情報セキュリティ対策の実施				
88		②本基準及びシステムセキュリティ実施要領から必要な管理策を盛り込んだ情報セキュリティ実施手順の作成				
89	**第10**	**情報セキュリティ事故等への対応**				
90	第10　1	情報セキュリティ事故等対処計画について以下のことを定めていること。				
91		①事故等の各段階（平素、事故等発見時、事故等の監視及び分析、被害及び影響の抑制並びに局限、事故等の証拠の保存及び原因の究明、事故等からの復旧）に対処し得る体制、責任及び手順				
92		②ヘルプデスクの設置及び実施手順				
93		③デジタルフォレンジック技術の利用等による必要な情報の収集及び分析並びにその手順				
94		④自社のネットワークにおける全ての情報システムの分析及び精査並びにその手順				
95		⑤事故等への対処により取得した情報等を記録した文書の作成及び保管要領				
96		⑥当該対処の教訓を情報セキュリティ教育及び訓練等への反映				
97	第10　2	情報セキュリティ事故等対処テストについて以下のことを定めていること。				
98		①情報セキュリティ事故等対処テストの実施要領				
99		②対処テストの結果を記録した文書の作成・保管要領				

100	**第11**	**情報セキュリティ事故等発生時の対応**				
101	第11　1	情報セキュリティ事故等発生時の対応について以下のことを定めていること。				
102		①情報セキュリティ事故等を発見又は検知した場合の措置及び手順（発見又は検知した従業員が管理者、保護システム管理者に報告、管理者の情報セキュリティ事故等対処計画による対処、当該事故等の内容及び結果並びに対処により取得した情報等の文書を作成、総括者に報告）				
103		②保護システムの脆弱性を発見又は検知した場合の措置及び手順（発見した保護システム利用者が保護システム管理者に報告、同管理者が適切な措置の実施、脆弱性の内容、改善又は修正の方法を記載した文書を作成し総括者に報告）				
104		③　①及び②で作成した文書の保存又は保管要領				
105		④改善又は修正の手順（情報セキュリティ事故等対処計画に定められた期間内に実施、困難な場合は是正計画を作成し、同計画に定められた期間内に実施、防衛省に報告）				
106		⑤保護システムの脆弱性を修正する場合の手順（リスク査定の実施、脆弱性情報データベース等の活用、脆弱性が重大な影響を及ぼす場合に可能な限り速やかに修正を実施）				
107	第11　2	防衛省への報告について以下のことを定めていること。				
108		①情報セキュリティ事故等を発見又は検知した場合の防衛省への報告要領 a 直ちに把握し得る限りの情報 b その後、速やかにその詳細 c 報告の責任者等を明記した連絡系統図等				
109		②事故等の詳細な報告要領 定められた期間までにその原因、影響、初期的な対処状況				
110	**第12**	**リスク査定について以下のことを定めていること。**				
111		①リスク査定の実施要領 a 実施時期：定期的又は必要と認められた場合 b 査定対象 c 結果を記載した文書の作成及び周知				
112		②リスク査定の結果を記録した文書の保管又は保存手順 a 施錠したロッカー等（データで保存する場合には、暗号化） b 保管又は保存期間				
113		③リスク査定の評価基準及び手順				
114	**第13**	**セキュリティ監査**				
115	第13　1	セキュリティ監査計画の作成等について以下のことを定めていること。				
116		①監査部門の設置及び同部門の構成 （原則として最低1名は監査を受ける部署以外の取扱者を配置）				

117		②監査部門によるセキュリティ監査計画の作成及び経営者等の承認				
118		③監査に関与する者への保護システムに対するアクセス権の付与				
119		④監査部門への必要な情報の提供				
120	第13　2	セキュリティ監査の実施要領を作成し、以下のことを定めていること。				
121		①実施時期：1年に１回以上又は必要な場合				
122		②リスクの特定、分析及び評価法等				
123	第13　3	セキュリティ監査結果の報告等について以下のことを定めていること。				
124		①セキュリティ監査結果の作成及び周知の実施要領 a 作成内容 b 提出期限 c 周知者				
125		②監査部門から改善提案が出された場合の措置及び手順 a 当該部署と監査部門との協議 b 改善策の決定及び実施並びに完了予定時期 c 是正計画の作成及び是正完了時期、防衛省への報告				
126		③セキュリティ監査実施計画、セキュリティ監査結果記録文書等の保管又は保存要領				

留意事項（１）上記項目は、事業所等の特性に応じて必要な項目を追加して規定する。 （２）上記項目のうち、適用除外とする項目については、その理由を明記する。	総合判定		【コメント】

※判定は「適合」、「不適合」、「除外」を記載。

別紙第4(第3.4関係)

情報セキュリティ実施手順の判定基準

項目	対応条項	確認項目（防衛省確認事項）	判定※	確認者	確認日	備考
	第2	**システムセキュリティ実装計画書**				
1		システムセキュリティ実装計画書の作成等について以下のことを定めていること。				
2		①システムセキュリティ実装計画書の作成及びその手順 a 作成者：保護システム管理者 b 承認権者：経営者等 c 記載又は添付項目 d 定期的な確認 e 変更時の措置				
3		②システムセキュリティ実装計画書の保存等及びその手順 a 保存責任者：保護システム管理者 b 保管又は保存方法及び場所 c 保管又は保存期間				
4		③システムセキュリティ実装計画書の周知及びその手順 a 周知の責任者：保護システム管理者 b システム管理業務に従事する者、その他の周知可能な者				
5	**第3**	**管理構成**				
6	第3 1	セキュリティエンジニアリングの原則				
7		保護システムの設計、開発、導入及び変更する場合にセキュリティエンジニアリングの原則を適用することを定めていること。				
8	第3 2	ベースライン構成設定について以下のことを定めていること。				
9		①ベースライン構成設定の決定の方針(情報セキュリティ基本方針等に基づく措置が実施可能、保護システムのセキュリティ確保等)及び手順（システム管理者が定め、総括者の承認等)				
10		②構成設定を実施する手順(ソフトウェアの導入、アクセス権限、必要最小限の機能)				
11		③構成設定の精査（定期的又は必要とする場合)				
12		④ブラックリスト又はホワイトリストの作成等及び更新要領				
13	第3 3	ベースライン構成設定の変更等の手順を作成し、以下のことを定めていること。				
14		①変更及び特別の構成設定を行うことができる条件				
15		②実施者及び承認権者⇒実施者：保護システム管理者、承認者：総括者				
16		③セキュリティ上の影響の分析等				
17	第3 4	構成設定に係る記録及び保存について以下のこと定めていること。				
18		①構成設定目録の作成及び更新の手順(構成要素に係る現状を確認・証明、構成要素ごとに責任者を記載、定期的な精査により更新)				

19		②構成設定に係る記録（構成設定の決定、変更、構成設定の実施を記載）				
20		③　①及び②の保存及び保管の要領				
21	**第４**	**保護システムの基本的防御**				
22	第4 1	保護システムにおける保護すべき情報を扱う領域、イントラネット、外部ネットワークとの境界に物理的又は論理的に制御可能な措置を行うことを定めていること。				
23	第4 2	保護システムの操作手順書について以下のことを定めていること。				
24		①保護システムの操作手順書の作成				
25		②同手順書の作成及び周知の要領				
26	第4 3	保護すべきデータの暗号化について以下のことを定めていること。				
27		①保護すべきデータを保護システム及び可搬記憶媒体に保存する場合の暗号化要領				
28		②データの暗号化は電子政府奨励暗号等を使用				
29		③暗号鍵の管理要領				
30	第4 4	その他の基本的防御対策について以下のことを定めていること。				
31		①保護システムにソフトウェアのインストール及びアップデートする場合の措置及び手順				
32		②保護システムにおけるアプリケーション等の機能の分離（管理者用・利用者用）				
33		③管理者用機能の不正利用の防止策				
34		④仮想化技術を利用する場合の措置及び対策				
35		⑤保護システムを外部システムに接続する場合の措置及び対策				
36	**第5**	**アクセス制御**				
37	第5 1	アクセス制御方針について以下のことを定めていること。				
38		①作成の目的（保護すべきデータ又は保護システムの論理的アクセスを制御）				
39		②作成者及び承認者（作成：保護システム管理者、承認：総括者）				
40		③アクセス権限を有するものを業務上必要最小限度に指定				
41		④見直し及び修正の要領				
42	第5 2(1)	アカウント管理について以下のことを定めていること。				
43		①アカウント管理者の指定(保護システム管理者が指定)				
44		②アカウント管理者の業務（アカウント利用者を必要最小限度、管理者権限の分離、利用者ごとに管理し利用状況を記録、利用者のアクセス権限を変更又は失効させる場合の措置、管理者権限の使用制限）				
45	第5 2(2)	ログオンの管理について以下のことを定めていること。				
46		①保護システムへのログオンを連続して失敗した場合の措置(自動ロック及び定められた期間内は再試行不能な設定)				
47		②保護システムにログオンする場合の留意事項(パソコン画面に不正なログオン試行に有用な情報を表示させない等)				
48	第5 2(3)	保護システムにログオンしたユーザセッションの管理について以下のことを定めていること。				

49		①ユーザセッションロックの実行（非アクティブ状態であり続ける上限時間を超えた場合、利用者が保護システムの置かれた席から離席する場合）				
50		②ユーザセッションロック時のパソコンのディスプレイの保護（スクリーンセーバ等）				
51		③ユーザセッションロックの解除(利用者に多要素認証)				
52		④利用者がログオフを要求した場合の措置（自動的にユーザセッションを終了、利用者が継続実行を設定した以外のソフトウェアプログラムを終了）				
53	第5 2(4)	保護システムのリモートアクセス管理について以下のことを定めていること。				
54		①リモートアクセス利用の手順(保護システム管理者の承認)				
55		②リモートアクセス利用時の措置（必要最小限度に制限、保護システムのリモートアクセスに係る通信の暗号化、アクセス制御ポイントの管理(自動監視・制御)、スプリットトンネリングの禁止、管理者権限の使用の原則禁止）				
56	**第6**	**識別及び認証**				
57	第6 1	保護システムの識別及び認証等について以下のことを定めていること。				
58		①識別を実施する場合の措置及び手順（アカウント及び保護システム構成機器への識別子の付与、識別子の保護システムでの有効化、識別子の再使用、使用されていない識別子、管理者権限）				
59		②認証を実施する場合の措置及び手順(ログオン時の多要素認証、リモートアクセス、管理者権限)				
60		③パスワードにより認証する場合の措置及び手順（パスワードの付与、初期パスワード、パスワードの要件、パスワードの保存又は伝送、作成したパスワードの忘失）				
61	第6 2	その他の認証子による認証について、適切な機器等を使用するための措置及び手順（機器等の紛失又は破損等による交換を含む。）を定めていること。				
62	**第7**	**通信の制御**				
63	第7 1	通信の制御について以下の措置及び手順を定めていること。				
64		①保護システムと外部ネットワークとの通信を行う場合				
65		②不特定多数の者がアクセス可能なウェブサーバ等を保有する場合				
66		③リモートアクセスを実施する場合				
67	第7 2	通信データ及び通信セッションの保護について以下の措置及び手順を定めていること。				
68		①保護すべきデータを通信する場合(セキュリティの確保、業務上必要最小限度、保護システム以外の情報システムとの通信は防衛省の許可、データ又は転送する通信経路の暗号化)				
69		②保護システムを利用した通信のセッションの保護(セッション終了時等における関連するネットワーク接続の全ての終了、保護システムと外部ネットワークの通信は電子証明書等の利用)				
70	第7 3	通信機能の利用制限について以下のことを定めていること。				
71		①保護システムにおけるモバイルコードの利用手順(許容条件、保護システム管理者の承認)				
72		②保護システムにおけるVoIP技術の利用手順（許容条件、保護システム管理者の承認）				

73		③保護システムに接続されたオフィス機器の利用手順(利用要件、保護システム以外からのアクセスによる起動及び操作の制限、起動している場合の措置、保護システム管理者の承認)				
74	**第8**	**システム監視**				
75	第8 1	システム監視実施について以下のことを定めていること。				
76		①保護システムの内部及び外部境界に対するシステム監視				
77		②監視事項(不正な相手方又は方法等によるアクセス、権限(管理者権限を含む)の不正な使用、内部及び外部との不正な通信、悪意のあるコードの侵入)				
78	第8 2	システム監視の実施方法について以下のことを定めていること。				
79		①システム監視の共通事項（システム上での挙動を常時監視、不正なアクセスを探知した場合の措置、システム監視のレベルを上げる等の措置)				
80		②不正な通信に対するシステム監視（保護システムの内部及び外部との間における双方向の通信トラフィック、不正なローカル接続、ネットワーク接続、リモート接続、リモートアクセスを常時監視)				
81		③悪意のあるコードの検知要領(パターンマッチング手法やヒューリスティックエンジン等の高度な手法を活用可能なソフトウェアのインストール及びアップデート、保護システムに対する定期的なフルスキャン、ファイルに対するリアルタイムスキャン)				
82	第8 3	不当なアクセス又は悪意あるコードを検知した場合の対応について以下のことを定めていること。				
83		①誤検知の可能性の検証				
84		②検知された悪意のあるコードを含むファイル等のブロック、隔離、削除等				
85	第8 4	システム監視により取得した情報の利用及び保管について以下のことを定めていること。				
86		①情報の利用及び通知要領（情報セキュリティ事故等の対処、関係部署への通知)				
87		②情報の保管要領等（施錠したロッカー等又は暗号化、定められた期間)				
88	**第9**	**システムログ**				
89	第9 1	システムログの取得及び分析について以下のことを定めていること。				
90		①取得するシステムログの内容(保護すべきデータへの動作の内容及び保護システム利用者毎の操作内容等並びに取得するログ内容について保護システム管理者の承認)。				
91		②取得する方法(保護システム上で自動的に取得、取得に失敗した場合の措置、定期的な精査及び変更)。				
92		③システムログの分析要領（定期的な分析、分析方法は保護システム管理者が承認、保護システムに報告生成機能、分析結果の文書化、総括者及び保護システム管理者等に報告)				
93	第9 2	システムログの管理について以下のことを定めていること。				
94		①システムログの取得及び分析に関わる保護システムの設定を行うためのアクセス権の付与				
95		②システムログ及び分析結果を記録した文書の保管要領（暗号化又施錠したロッカー等、必要な期間、定期的な確認)				

96	第9 3	システムログにタイムスタンプを付与する要領（日本標準時、システムクロックの同期方法）を定めていること。				
97	第9 4	システムログを取得するツールの保護要領(不正なアクセス、改ざん又は削除に対する論理及び物理的対策)を定めていること。				
98	**第10**	**脆弱性スキャン等**				
99	第10 1	脆弱性スキャンについて以下のことを定めていること。				
100		①脆弱性スキャンの実施手順（定期的又は専門的な外部機関が発信する脆弱性情報等が保護システムに対して影響を与える可能性がある場合、保護システム全体に脆弱性スキャンを実施）				
101		②脆弱性スキャンの分析結果の文書化				
102		③脆弱性が特定された場合の措置(定められた時間内に必要な改善又は修正、防衛省への報告)				
103	第10 2	脆弱性スキャンの分析結果について以下のことを定めていること。				
104		①分析結果の周知				
105		②情報セキュリティ機関から収集した資料に基づく注意喚起				
106		③脆弱性が特定された場合の対処要領				
107	**第11**	**バックアップ**				
108		バックアップの手順において以下のことを定めていること。				
109		①バックアップの対象(全ての保護すべきデータ及び必要なシステムデータ)				
110		②バックアップの保存期間及び頻度				
111		③バックアップデータの保護対策(保管拠点の保護等)				
112	**第12**	**システムメンテナンス等**				
113	第12 1	システムメンテナンス等計画について以下のことを定めていること。				
114		①システムメンテナンスの実施時期（定期的及び必要な場合）				
115		②システムメンテナンスの実施者、対象及び内容				
116		③保護システムの取外し、取扱施設外への持ち出し、リモートメンテナンス時の措置及び手順				
117	第12 2	システムメンテナンス等の実施について以下のことを定めていること。				
118		①メンテナンス要員の指定要領(保護システム利用者が行う場合、保護システム利用者以外が行う場合)				
119		②メンテナンスツールの検査要領(保護システム管理者の承認)				
120		③保護システムへのアクセスの認証等(メンテナンス実施者に多要素認証、使用する機器の識別)				
121		④システムメンテナンスの監督等(監督者の指定、監督結果の報告)				
122		⑤セキュリティ対策（メンテナンス等の実施前のセキュリティ対策の実施、メンテナンス等の終了後の機能の確認）				
123	第12 3	システムメンテナンスの記録について以下のことを定めていること				
124		①システムメンテナンスの監督者による記録及び承認等の要領				
125		②システムメンテナンスを記録した文書の保管要領				

留意事項（1）上記項目は、事業所等の特性に応じて必要な項目を追加して規定する。 （2）上記項目のうち、適用除外とする項目については、その理由を明記する。	総合判定		【コメント】

※判定は「適合」、「不適合」、「除外」を記載。

別記様式第１（第 3.1 関係）

文 書 番 号
発簡年月日

（監査官の所属長）
殿

（監査対象企業）

情報セキュリティ基本方針、情報セキュリティ規則及び情報セキュリティ実施手順の確認について

下記契約に係る「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」第２条第３項の規定に基づき確認されたく提出します。

記

１　調達要求番号
２　契約品名
３　認証番号又は契約番号（年月日）
４　納期
５　監査対象事業所名（所在地）
６　監査対象部門（所在地）

添付書類：１　情報セキュリティ基本方針
２　情報セキュリティ規則
３　情報セキュリティ実施手順

別記様式第２（第 3.1 関係）

文 書 番 号
発簡年月日

（監査官の所属長）
殿

（監査対象企業）

情報セキュリティ基本方針、情報セキュリティ規則及び情報セキュリティ実施手順について（届出）

下記契約に係る「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」第２条第２項に規定する情報セキュリティ基本方針、情報セキュリティ規則及び情報セキュリティ実施手順については、既に確認を受けておりますので、同条第３項の規定に基づき届け出ます。

記

１　調達要求番号
２　契約品名
３　認証番号又は契約番号(年月日)
４　納期
５　監査対象事業所名(所在地)
６　監査対象部門(所在地)
７　確認通知番号(年月日)

別記様式第３（第 3.1 関係）

文 書 番 号
発簡年月日

（監査対象企業）
殿

（監査官の所属長）

情報セキュリティ基本方針、情報セキュリティ規則及び情報セキュリティ実施手順の確認について（通知）

（申請文書番号）により提出された標記の件について、確認しましたので通知します。

別記様式第４（第 3.1 関係）

文 書 番 号
発簡年月日

（契約担当官等、物別官、物別室長）
殿

（監査官の所属長）

情報セキュリティ基本方針、情報セキュリティ規則、情報セキュリティ実施手順確認状況報告書
（令和　年度　第　／四半期分）

番号	①事業所等名称	②監査対象契約	③確認通知
1			
2			
3			
4			
5			

①監査対象契約通知等の契約相手方名（監査対象事業所）
②監査対象契約通知等の文書番号（発簡年月日）、当該契約の認証番号又は契約番号
③地方防衛局調達部長等からの確認通知文書番号（発簡年月日）

写送付先：装備政策部装備保全管理課長

別記様式第５（第 4.2 関係）

文 書 番 号
発簡年月日

（監査官の所属長）
殿

（防衛省の地方調達の契約担当官等）

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（依頼）

標記について、下記のとおり依頼する。

記

１　契約の概要（契約件名、契約年月日、納期、契約相手方、監査対象事業所等及び所在地）：
２　協力を依頼する内容（項目、範囲、時期等）：
３　協力を依頼する理由：

添付書類：契約書（写）等
　　保護すべき情報のリスト

別記様式第６（第 4.2 関係）

文 書 番 号
発簡年月日

（防衛省の地方調達の契約担当官等）
殿

（監査官の所属長）

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
（回答）

標記について、下記のとおり回答する。

記

１　監査等の協力の可否:可・否
２　協力実施の条件：
（又は否とする理由）：
３　その他：

関連文書：（監査等の協力依頼文書番号、日付）

別記様式第７（第 4.2 関係）

文 書 番 号
発簡年月日

（防衛省の地方調達の契約担当官等）
殿

（監査官の所属長）

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内容について（回答）

標記について、下記のとおり回答する。

記

（記載例）
１　実施事項：
２　監査対象企業、事業所等名：
３　監査実施日又は期間：
４　監査同行者又は実施者：
５　その他：

関連文書：（監査等の協力依頼文書番号、日付）

別記様式第８（第 4.2 関係）

文 書 番 号
発簡年月日

（防衛省の地方調達の契約担当官等）
殿

（監査官の所属長）

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実施結果について(回答)

標記について、下記のとおり回答する。

記

（記載例）
１　実施事項：
２　実施結果：

関連文書：（監査等の協力依頼文書番号、日付）
添付書類：情報セキュリティ実地監査報告書、指摘事項通知書等
情報セキュリティ基本方針等(返却)