付録第15

単価契約に関する特約条項

（契約金額）

第１条　この契約金額は単価とする。

（契約金額の変更）

第２条　この契約期間中は、契約条項によるほか、原則として契約金額を変更することはできない。

（発注及び納入）

第３条　乙は、甲の発行する発注書等により、指定納期（納入時間・時期）までに指定場所に物品を納入するものとする。

（代金の請求）

第４条　乙は、履行完了段階において確定数量に契約単価を乗じた金額に消費税法（昭和６３年法律第１０８号）に規定する率に基づき計算された消費税額を加えた金額を請求するものとする。

（その他）

第５条　発注予定数量と実際発注数量とに差異が発生した場合であっても、乙は甲に対し、損害賠償を請求することができない。

付録第16

部分払に関する特約条項

（部分払）

第１条　甲は、この特約条項の定めるところに従い、この契約に係る既納部分又は既済部分に対して代金の一部を乙に支払うものとする。

（部分払の支払方法）

第２条　部分払の支払方法（支払回数を含む。以下同じ。）は、別表のとおりとする。

（内訳表の提出）

第３条　乙は、この契約締結後、速やかに前条の支払方法に適合した契約金額の内訳表を作成し、甲の確認を受けるものとする。

２　甲は、前項の内訳表を不適当と認める場合は、これを変更させることができる。

３　前２項の規定は、契約金額を変更した場合における内訳表の変更についても準用する。

（部分払金額）

第４条　甲が部分払として乙に支払う金額は、前条第１項の内訳表に基づいて算定した既納部分又は既済部分に相当する金額とする。ただし、既済部分又は性質上不可分の製造若しくは役務についての契約に係る既済部分に対する部分払の金額は、当該部分に相当する金額の１０分の２の金額を差し引いた金額とする。

２　部分払は、予算の範囲内において行うものとする。

（部分払の請求及び支払）

第５条　部分払の請求及び支払については、契約条項の代金の請求及び支払に関する規定を準用する。

（所有権の移転）

第６条　性質上不可分の製造の既済部分について部分払を行った場合は、その際当該契約物品の所有権は、甲に移転するものとする。

２　前項の規定は、契約物品に係る危険負担及び損害負担について契約条項の定めるところを変更するものではない。

付録第17

売払い物品の解体に関する特約条項

甲（契約担当官）及び乙（契約相手方）は、売払い物品の解体に関して次の特約条項を定める。

（総則）

第１条　乙は、次に掲げる売払い物品については、別に定める解体要領に基づき解体するものとする。

番号	品　　目	型　　式	単 位	数 量	備　　考

（契約金額の内訳）

第２条　前条に掲げる物品に係る契約金額は、〇〇円（消費税及び地方消費税込み）とし、本契約書本文に記載した契約金額の内訳とする。

（所有権の移転）

第３条　第１条に掲げる売払い物品の所有権は、乙が甲に対して解体の完了を届け出て、甲が承認したときをもって甲から乙に移るものとする。

付録第18

中古品の売払いに関する特約条項

甲（契約担当官）及び乙（買受け人）は、中古品の売払いに関して次の特約条項を定める。

（物品の引渡し）

第１条　乙は次に定める期限内に契約代金を完納するとともに、乙の責任と費用負担により契約物品を引き取るものとする。

(1)　契約代金の納入期限　　令和○○年○○月○○日

(2)　物品の引取り期限　　令和○○年○○月○○日

２　乙が契約代金を納入し、契約物品を引き受けたときをもって、甲から乙へ所有権が移転するものとする。

３　乙は、契約物品の引き受けに際して、事故のないように留意するとともに、事故が発生した場合は、乙の責任において処理するものとする。

（担保責任の免除）

第２条　契約物品は現状渡しであり、所有権移転後の使用等に関し、甲は一切の責任を負わないものとする。

２　乙は、契約物品に不具合、隠れたる瑕疵等を発見しても、甲に対して契約代金の減免、損害賠償の請求、又は契約の解除をすることができない。

（法令等に定められた手続）

第３条　契約物品の所有権移転、使用等に関して、法令等により定められた手続がある場合は、乙の責任と費用負担において実施しなければならない。

付録第19

特別防衛秘密の保護に関する特約条項

（乙の一般義務）

第１条　乙（契約業者）は、主たる契約条項に基づく特別防衛秘密の保護に関しては、この特約条項に定めるところにより、秘密保護の万全を期さなければならない。

２　乙は、乙の従業員、再委託を行う場合においてはその相手方（以下「中小受託事業者」という。）その他甲により特別防衛秘密の表示のある特別防衛秘密に属する文書又は図画（以下「特定資料」という。）又は特別防衛秘密の指定のある特別防衛秘密に属する物件（以下「特定物件」という。）を取扱う場所への立ち入りが許可された者の故意又は過失により特別防衛秘密が漏えいしたときであっても、その責任を免れることはできない。

（送達）

第２条　甲は、特定資料又は特定物件を乙に交付するときは、特別防衛秘密及び米国政府の標記を付し、書面又は電磁的記録をもって送達するものとする。

（特定資料の保護措置）

第３条　乙は、主たる契約の説明書、仕様書、計算書、図表等のうち、特定資料を特別防衛秘密の取扱いの業務に従事する者（以下「関係社員」という。）以外の者に供覧してはならない。

２ 乙は、関係社員であっても、作業に必要な限度を超えて特定資料を供覧してはならない。

（特定物件の保護措置）

第４条　乙は、特定物件について、その保管中取扱いの慎重を期して、関係社員以外の者に供覧してはならない。

２　乙は、関係社員であっても、作業に必要な限度を超えて特定物件を供覧してはならない。

（特定資料及び特定物件の複製等）

第５条　乙は、主たる契約に定められている場合を除き、特定資料を複製若しくは製作し、又は特定物件の設計資料、見取図、試験成績表等の複製、製作若しくは写真撮影をする場合は、あらかじめ、甲の許可を得なければならない。

２　乙は、主たる契約又は前項の甲の許可により特定資料の複製若しくは製作又は特定物件の設計資料、見取図、試験成績表等の複製、製作若しくは写真撮影をする場合は、あらかじめ、実施の細部について甲と協議し、甲又は甲の代理者の立会のもと行わなければならない。

３　第１項に規定する特定資料及び特定物件の複製等において完成に至らなかったものは、甲の指示に従い、特別防衛秘密として探知することが困難となるよう、焼却、粉砕、細断、溶解、破壊等の方法により、確実に破棄しなければならない。

（特別防衛秘密の表示等）

第６条　乙は、特定資料又は特定物件を複製又は製作したときは、これらに特別防衛秘密、米国政府、登録番号等の表示を付さなければならない。

（実施報告）

第７条　乙は、特定資料若しくは特定物件を接受、複製、送達、製作若しくは甲からの

指示により破棄したとき、又は第５条に規定する特定物件の設計資料、見取図、試験成績表等の複製、製作若しくは写真撮影をしたときは、速やかに、甲に対し、その旨を書面又は電磁的記録により報告しなければならない。

（立入禁止措置）

第８条　乙は、特定資料又は特定物件が取り扱われている場所について、立入りを禁止しなければならない。

２　前項の規定により立入りを禁止した場合、当該場所を管理する者は、当該場所に立ち入ってはならない旨の掲示その他立入禁止に必要な措置を講じなければならない。

３　乙は、関係社員以外の者を、みだりに第１項に規定する場所に立ち入らせ、又はその付近に必要以上に近づかせてはならない。

４　乙は、関係社員に対しても、作業に必要な限度を超えて、第１項に規定する場所に立ち入らせてはならない。

（秘密保全規則等）

第９条　乙は、社（工場）内における特別防衛秘密の保護を確実に行うため、この特約条項締結の日から１箇月以内（着工の時期が１箇月以内に到来するときは着工の日まで）に特別防衛秘密の保全に関する規則を作成のうえ、甲の確認を受けるものとする。ただし、その規則が既に作成され、甲の確認済みであるときは、特別の指示がない限り、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特別防衛秘密の保全に関する規則を変更するときは、あらかじめ、甲に届出なければならない。

３　第１項の規則には、次の各号に示す事項を明らかにした条項を規定するものとする。

(1)　保管責任者及び取扱者の任命の方法及び責任範囲

(2)　秘密区分の標記の表示方法

(3)　特別防衛秘密の保管及び取扱いのため必要な簿冊の整備

(4)　社（工場）内における立入禁止に関する措置

(5)　特別防衛秘密に属する文書、図画又は物件の製作、複製及び写真撮影に関する手続及び方法

(6)　特別防衛秘密に属する文書、図画又は物件の接受、送達、保管、貸出し、引継ぎ及び返却に関する手続及び取扱方法

(7)　特別防衛秘密の保護状況の検査に関する事項

(8)　非常の場合の措置

(9)　特別防衛秘密の漏えい、紛失、破棄等の事故が発生したときの措置

(10)　その他必要な事項

（特定資料の返却等）

第１０条　乙は、甲が交付した特定資料及び特定物件並びに第５条の規定により複製、製作又は写真撮影をしたすべての資料を契約終了後、直ちに、甲に返却し、又は提出しなければならない。

（検査）

第１１条　乙は、特別防衛秘密の取扱いのため必要な簿冊を整備し、毎月１回以上特別防衛秘密の保護の状況について点検を行い、甲又は甲の代理者の検査を受けなければならない。

２　甲又は甲の代理者は、必要があると認めたときは、前項の検査を行うほか、特別防衛秘密の保護の状況を検査し、又は必要な指示を乙に与えることができる。

（保管状況報告）

第１２条　乙は、毎年６月末日及び１２月末日現在の特定資料及び特定物件の保管の状況を甲に報告しなければならない。

（特定資料又は特定物件を取扱う場所の新設等）

第１３条　乙は、特定資料又は特定物件を取り扱う場所を新設し、又は変更するときは、あらかじめ、甲の確認を受けなければならない。

（事故発生時の措置）

第１４条　乙は、特別防衛秘密の漏えい、紛失、破壊等の事故が発生し、又はそれらの疑い若しくはおそれがあったときは、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。

２　甲は、別に定める秘密保全の確保に関する違約金条項の規定に基づき違約金を請求することができる。

（保全教育）

第１５条　乙は、関係社員に対し、年間計画を立て、保全教育を実施しなければならない。

２　乙は、保全教育を実施する場合は、その内容及び実施方法について、この特約条項締結の日から１箇月以内（着工の時期が１箇月以内に到来するときは、着工の日まで）に甲の確認を受けなければならない。ただし、その内容等が既に甲の確認済みのものであるときは、特別の指示がない限り、届出をすれば足りる。

３　乙は、前項の規定により甲の確認を受けた事項に変更がある場合は、あらかじめ、甲の確認を受けなければならない。

４　乙は、毎年、甲が指示する時期に、保全教育の実施状況を、甲に報告しなければならない。

（再委託）

第１６条　乙は、特定資料の複製若しくは製作又は特定物件の製作、取付け、修理、実験、調査研究、複製等を第三者に再委託させてはならない。ただし、やむを得ず再委託を行う場合は、あらかじめ、甲に対し、再委託の相手方、契約内容、秘密保護の手段等を記載し、又は記録した書面又は電磁的記録を添えて甲の許可を得なければならない

２　前項の規定により、再委託を行う場合において、中小受託事業者は、本省の契約担当官等と秘密保持に関する規程を含む契約を結んでいる者でなければならない。

３　第１項の規定により再委託を行う場合において、物件の輸送、施設の警備その他特別防衛秘密の内容を知り得ないと認められる役務を提供する者については、前項に規定する本省の契約担当官等との契約を要しない。

４　第１項及び第２項の規定は、乙が部外の機関に品質システムの審査を受託する場合に準用する。

５　乙は、第１項に規定する場合を除き、特定資料又は特定物件を第三者に提供してはならない。

（契約の解除）

第１７条　中小受託事業者の責に帰すべき事由により、甲が当該中小受託事業者との契

約を解除する場合は、甲は乙にその旨を通報するものとする。この場合において、甲は乙に対して損害賠償の責を負わないものとする。

２　乙が中小受託事業者との契約を解除する場合は、事前に甲にその旨を通報しなければならない。

３　乙の責めに帰すべき事由により、甲が乙との契約を解除する場合は、甲は乙の中小受託事業者との契約を解除することができる。この場合において、甲は当該中小受託事業者に対して損害賠償の責を負わないものとする。

（特別防衛秘密の取扱いの業務の終了に伴う措置）

第１８条　事故の発生その他の事由（第１０条の規定によるものを除く。）により、甲が乙による特定資料の複製若しくは製作又は特定物件の製作、取付け、修理、実験、調査研究、複製等の一部又は全部をやめさせることが適切であると認めたときは、乙は、速やかに、甲の指示に従い、特定資料又は特定物件の返却、破棄その他の必要な措置を講じなければならない。

付録第20

特定秘密の保護に関する特約条項

（乙の一般義務）

第１条　乙（契約業者）は、主たる契約条項に基づく特定秘密の保護に関しては、この特約条項及び附属する装備品等の調達に係る秘密保全対策ガイドラインの定めるところにより、万全を期さなければならない。

２　乙は、その代表者、代理人、使用人その他の従業者（以下総称して「従業者」という。）、再委託を行う場合においてはその相手方（複数の段階で再委託が行われる場合の当該再委託先を含む、以下同じ。以下「再委託先」という。）の従業者その他特定秘密の保護に関する法律施行令（平成２６年政令第３３６号。以下「令」という。）第１１条第１項第１号の規定に基づき防衛大臣が指名した特定秘密の保護に関する業務を管理する者（以下「特定秘密管理者」という。）が乙の求めにより特定秘密を記録する文書、図画、電磁的記録若しくは物件（以下「特定資料」という。）又は特定秘密を化体する物件及び製造途上にある仕掛品並びにこれらにより構成される物件（以下「特定物件」という。）を取り扱う場所への立入りを許可した者の故意又は過失により特定秘密が漏えいしたときであっても、その責任を免れることはできない。

（交付・保有）

第２条　特定秘密管理者は、特定資料又は特定物件（以下「特定資料等」という。）を乙に保有させ、又は交付するときは、当該特定資料等を乙に保有させ、又は交付する旨を記載し、又は記録した書面又は電磁的記録を添えて、保有させ、又は交付するものとする。

２　前項の交付を行う場合において、当該特定資料等が次の各号に掲げる情報に係るものであるときは、特定秘密管理者は、特定秘密の表示に加え、当該各号に定める表示をするものとする。ただし、既にＮＡＴＯ　ＳＥＣＲＥＴの表示がされているものについては、改めて当該表示をすることを要しない。

(1)　米国秘密軍事情報（秘密軍事情報の保護のための秘密保持の措置に関する日本国政府とアメリカ合衆国政府との間の協定第１条（ａ）に規定する秘密軍事情報であって、アメリカ合衆国政府から受領したものをいう。第２１条第３項第１号において同じ。）米国政府

(2) 北大西洋条約機構秘密情報（北大西洋条約機構から受領した情報又は資料であって、情報及び資料の保護に関する日本国政府と北大西洋条約機構との間の協定第１条（ⅱ）に規定する秘密の指定を受けているものをいう。第２１条第３項第２号において同じ）

ＮＡＴＯ　ＳＥＣＲＥＴ

(3) 仏国秘密情報（情報の保護に関する日本国政府とフランス共和国政府との間の協定第１条（ａ）に規定する秘密情報であって、フランス共和国政府から受領したものをいう。第２１条第３項第３号において同じ。）　仏国政府

(4) 豪州秘密情報（情報の保護に関する日本国政府とオーストラリア政府との間の協定第１条ａに規定する秘密情報であって、オーストラリア政府から受領したものをいう。第２１条第３項第４号において同じ。）　豪州政府

(5) 英国秘密情報（情報の保護に関する日本国政府とグレートブリテン及び北アイルランド連合王国政府との間の協定第１条ａに規定する秘密情報であって、グレートブリテン及び北アイルランド連合王国政府から受領したものをいう。第２１条第３項第５号において同じ。） 英国政府

(6) インド秘密軍事情報（秘密軍事情報の保護のための秘密保持の措置に関する日本国政府とインド共和国政府との間の協定第１条ａに規定する秘密軍事情報であって、インド共和国政府から受領したものをいう。第２１条第３項第６号において同じ。） インド政府

(7) 伊国秘密情報（情報の保護に関する日本国政府とイタリア共和国政府との間の協定第１条ａに規定する秘密情報であって、イタリア共和国政府から受領したものをいう。第２１条第３項第７号において同じ。） 伊国政府

(8) 韓国秘密軍事情報（秘密軍事情報の保護に関する日本国政府と大韓民国政府との間の協定第２条（ａ）に規定する秘密軍事情報であって、大韓民国政府から受領したものをいう。第２１条第３項第８号において同じ。） 韓国政府

(9) 独国秘密情報（情報の保護に関する日本国政府とドイツ連邦共和国政府との間の協定第１条（ａ）に規定する秘密情報であって、ドイツ連邦共和国政府から受領したものをいう。第２１条第３項第９号において同じ。）独国政府

(10) 瑞国秘密情報（防衛装備品及び技術の移転に関する日本国政府とスウェーデン王国政府との間の協定第四条に基づく防衛装備品及び技術に係る情報保護に関する日本国防衛省とスウェーデン王国を代表する国防装備庁との間の取決め第１項に規定する秘密情報であって、スウェーデン王国国防装備庁から受領したものをいう。第２１条第３項第１０号において同じ。）瑞国政府

(11) サウジ秘密情報（防衛協力及び交流の過程で取得される情報の保護に関する日本国政府とサウジアラビア王国国防省との間の取決め第１項ａに規定する秘密情報であって、サウジアラビア王国国防省から受領したものをいう。第２１条第３項第１１号において同じ。）サウジ政府

(12) ＵＡＥ秘密情報（防衛装備品及び技術の移転に関する日本国政府とアラブ首長国連邦政府との間の協定第五条に従って作成される防衛装備品及び技術に係る情報の保護に関する日本国防衛省とアラブ首長国連邦政府との間の取決め第１項３に規定する秘密情報（「محظور」に秘密指定されたものを除く。）であって、アラブ首長国連邦国防省から受領したものをいう。第２１条第３項第１２号において同じ。）ＵＡＥ政府

(13) 宇国秘密情報（情報の保護に関する日本国政府とウクライナ政府との間の協定第１条ａに規定する秘密情報であって、ウクライナ政府から受領したものをいう。第２１条第３項第１３号において同じ。）宇国政府

（乙の秘密保全規則の変更の際の許可等）

第３条　乙は、審査を実施した者の審査を受けた令第１３条に規定する規程（以下「秘密保全規則」という。）並びに特定秘密の保護に関する業務を管理する者（以下「業務管理者」という。）、特定秘密の保護に関する教育の内容及び特定秘密の保護のために必要な施設設備（以下「施設設備」という。）の状況に変更がある場合には、あらかじめ、変更に関する資料の審査を実施した者に提出し、その承認を得なければならない。

２　乙は、毎年、審査を実施した者が指示する時期に、令第１３条に従って講じた措置の内容を、報告しなければならない。（業務管理者の責任）

第４条　乙は、業務管理者に、特定秘密の表示その他の特定秘密の保護を適切に管理するための措置を講じさせなければならない。

（従業者に対する特定秘密の保護に関する教育）

第５条　　乙は、従業者に対し特定秘密の保護に必要な知識の習得及び意識の高揚を図るための教育を実施しなければならない。

２　　乙は、新たに特定秘密の取扱いの業務を行うこととされている従業者に対する前項の教育については、当該特定秘密の取扱いの業務を行う前に実施しなければならない。

３　乙は、第１項の教育を特定秘密の取扱いの業務を行う従業者が少なくとも年１回受講できるよう実施しなければならない。ただし、必要な場合は、当該教育を臨時に実施することを妨げない。

（従業者の範囲の決定）

第６条　乙は、秘密保全規則等に基づき、特定秘密の取扱いの業務を行う従業者の範囲を決定するに当たっては、従業者個人単位で行い、その範囲は当該特定秘密を知得させる必要性を考慮して最小限にとどめなければならない。

２　乙は、前項で決定した従業者の範囲を、この特約条項締結後、特定秘密を取り扱わせる前に、特定秘密管理者に報告しなければならない。

３　乙は、第１項の従業者の範囲を変更するときは、あらかじめ、特定秘密管理者に報告しなければならない。

（適正評価の事務）

第７条　乙は、その従業者について、防衛大臣が行う適性評価（特定秘密の保護に関する法律（平成２５年法律第１０８号。以下「法」という。）第１２条第１号の適性評価をいう。以下同じ。）に関し、属紙「適性評価に関する特約条項」に規定する事務を行うものとする。

（従業者への周知）

第８条　乙は、特定資料等の交付若しくは特定秘密の伝達を受けたとき又は特定秘密を保有するときは、当該特定秘密を取り扱う従業者にその旨を周知しなければならない。

（特定資料等の保護措置）

第９条　乙は、特定資料等を当該特定秘密を取り扱う従業者以外の者に供覧してはならない。

２　乙は、当該特定秘密を取り扱う従業者であっても、作業に必要な限度を超えて特定資料等を供覧してはならない。

３　乙は、主たる契約に別途定められている場合を除き、特定資料等を作成しようとするときは、あらかじめ、特定秘密管理者の許可を得なければならない。

４　　前項の場合、乙は、実施の細部について特定秘密管理者と協議し、特定秘密管理者又はその指名する者の立会いのもと行わなければならない。

５　　乙は、特定資料等を作成したときは速やかにその旨を特定秘密管理者に書面又は電磁的記録により報告するとともに、特定秘密管理者より必要な指示を受けるものとする。

６　乙は、特定資料等の作成において完成に至らなかったものについては、特定秘密管理者の指示に従い、特定秘密管理者に引き渡し、又は特定秘密として指定された情報を探知することができないよう、焼却、粉砕、細断、溶解、破壊等の復元不可能な方法により、確実に廃棄しなければならない。

（再委託先への交付及び伝達の承認）

第１０条　乙は、特定資料等の交付、又は特定秘密の伝達を、甲との間における法第５条第４項又は法第８条第１項に規定する契約（以下「保全契約」という。）を締結した再委託先であって、当該保全契約に基づき当該特定秘密を保有することができ、又は交付を受けることができる者（以下「特定秘密取扱事業者」という。）以外の者に行ってはならない。

２　乙は、特定秘密取扱事業者に特定資料等を交付し、又は特定秘密を伝達するときは、特定秘密管理者の承認を得るものとする。

３　前項の規定に基づき交付する特定資料等を返却させる場合には、乙は、交付の際に、特定秘密管理者の指示を受け、業務管理者に当該特定資料等の返却の時期を明示させるものとする。

（運搬の方法）

第１１条　特定資料等を運搬するときは、乙は、当該特定秘密の取扱いの業務を行う従業者の中から指名した従業者に携行させるものとする。

２　乙は、前項の規定により運搬することができないとき又は運搬することが不適当であるときの運搬の方法については、特定秘密管理者の指示に従うものとする。

（交付の方法）

第１２条　乙は、特定資料等を交付するときは、受領書等に、名宛人又はその指名する者　（第１０条第２項の承認を受けた特定秘密取扱事業者の従業者であって、当該特定秘密を取り扱う者に限る。）の受領印の押印を受けるなど、受領の記録を残すものとする。

２ 特定資料等は、郵送により交付してはならない。

（文書及び図画の封かん等）

第１３条　乙は、特定秘密である情報を記録する文書若しくは図画を運搬し、又は交付するときは、それを外部から見ることができないように封筒若しくは包装を二重にして封かんするものとする。

（物件の包装等）

第１４条　乙は、特定秘密である情報を記録する物件、又は特定物件を運搬し、又は交付するときは、窃取、破壊、盗見等の危険を防止するため、運搬容器に収納し、施錠するなどの措置を講ずるものとする。

（電気通信による交付）

第１５条　乙は、特定資料（物件を除く。）を電気通信の方法により交付するときは、暗号措置等必要な措置を講ずるものとする。ただし、インターネットを介した電子メール又はストレージ　サービスを利用しての交付はしてはならない。

（特定資料等の接受）

第１６条　乙は、封かんされている特定秘密である情報を記録する文書若しくは図画は、名宛人又はその指名する従業者（当該特定秘密を取り扱う者に限る。）でなければ開封させてはならない。

（伝達の方法）
第１７条　乙は、特定秘密を伝達するときは、その旨を明らかにするとともに、当該特定秘密の内容を筆記することを差し控えるよう伝えるなど、その保護につき注意を促すための必要な措置を講ずるものとする。
２　　乙は、特定秘密の伝達を電話で行ってはならない。
３　　乙は、特定秘密を伝達する場合には、盗聴等の防止に努めるものとする。
（特定秘密を取り扱うために使用する電子計算機の使用の制限等）
第１８条　特定秘密である情報を記録する電磁的記録の取扱いに当たっては、乙はこれをスタンドアローンの電子計算機又はインターネットに接続していない電子計算機であって、かつ特定秘密を取り扱う従業者のみがアクセスできる措置が講じられたものとして、業務管理者が認めたもので取り扱わなければならない。
２　　乙は、特定秘密である情報を記録する電磁的記録を前項の電子計算機で取り扱うときは、当該電磁的記録の電磁的記録媒体への書き出し及び印刷の記録を保存しなければならない。
３　　乙は、特定秘密を取り扱う従業者が特定秘密である情報を記録する電磁的記録を可搬記憶媒体に記録する場合は、パスワード設定又は暗号化措置による秘匿措置を講じさせなければならない。ただし、当該措置を講ずることにより主たる契約の履行に著しい支障が生じる恐れがあり、当該措置を講じないことについて特定秘密管理者の承認を受けた場合はこの限りではない。
（特定資料及び特定物件の保管）
第１９条　特定資料の保管に当たっては、乙は、三段式文字盤鍵のかかる金庫若しくは鋼鉄製の箱又はこれらに準じる強度を有する保管容器にこれを保管しなければならない。
２　　乙は、特定秘密である情報を記録する電磁的記録を記録する電子計算機には、その盗難、紛失等を防止するため、当該電子計算機の端末をワイヤで固定する等の必要な物理的措置を講ずるものとする。
３　第１項の規定は、特定秘密である情報を記録する可搬型記憶媒体に準用する。
４　乙は、特定物件については、第１項及び第２項の規定を準用し、保管しなければならない。ただし、特定物件の形状等により、当該措置によることができない場合は、特定秘密管理者と協議し、適切と認める措置により保管するものとする。
（その保管のための施設設備）
第２０条　乙は、前条に定めるもののほか、特定資料等を保護するための施設設備について、間仕切りの設置、裁断機の設置等特定秘密の保護に必要な措置を講じなければならない。
（特定秘密の表示等）
第２１条　乙は、特定秘密を保有するとき、自ら特定資料等を作成したとき又は特定秘密の伝達を受けたときは、当該特定秘密又は特定資料等について、法第３条第２項各号のいずれかに掲げる措置を講じなければならない。
２　前項の場合において、乙は、法第３条第２項第１号に掲げる措置を講ずる際に、特定秘密管理者から別に指示のある場合は、その表示をしなければならない。
３　第１項の場合において、当該特定資料等が次の各号に掲げる情報に係るものであるときは、乙は、前２項の表示に加え、当該各号に定める表示をしなければならない。

ただし、既にＮＡＴＯ　ＳＥＣＲＥＴの表示がされているものについては、改めて当該表示をすることを要しない。

(1)　米国秘密軍事情報米国政府
(2)　北大西洋条約機構秘密情報　ＮＡＴＯ　ＳＥＣＲＥＴ
(3)　仏国秘密情報仏国政府
(4)　豪州秘密情報豪州政府
(5)　英国秘密情報英国政府
(6)　インド秘密軍事情報インド政府
(7)　伊国秘密情報 伊国政府
(8)　韓国秘密軍事情報 韓国政府
(9)　独国秘密情報　独国政府
(10)　瑞国秘密情報　瑞国政府
(11)　サウジ秘密情報　サウジ政府
(12)　ＵＡＥ秘密情報　ＵＡＥ政府
(13)　宇国秘密情報　宇国政府

（指定の有効期間の満了に伴う措置）

第２２条　乙は、特定秘密管理者から令第７条第１項第２号の規定に基づく特定秘密の指定の有効期間が満了した旨の通知を受けたときは、当該指定に係る特定資料等であったものについて、特定秘密の表示に赤色の二重線を付すことその他これに準ずる方法によりこれを抹消した上で、令第７条第２項に規定する指定有効期間満了表示をしなければならない。

２　前項の場合において、乙は、法第３条第２項第２号に掲げる措置を受けた者に対し、当該指定の有効期間が満了した旨を記載した書面の交付（当該書面の作成に代えて電磁的記録の作成がされている場合にあっては、当該電磁的記録の電子情報処理組織（当該交付をすべき者の使用に係る電子計算機（入出力装置を含む。以下同じ。）と当該交付を受けるべき者の使用に係る電子計算機とを電気通信回線で接続した電子情報処理組織をいう。）を使用する方法による提供。以下同じ。）により通知しなければならない。

３　第１項の場合において、乙は、当該指定の有効期間が満了した旨を当該指定に係る情報を取り扱う従業者（当該指定の有効期間の満了について前項の通知を受けた者を除く。）に周知しなければならない。

４　前２項、次条及び第２４条の通知又は周知（以下「通知等」という。）を書面に代えて電磁的記録で行う場合には、当該通知等の相手方が通知等の内容を確実に確認し、これに基づき適格な保護措置が講じられることを担保するため、電子メールの開封確認機能を利用し通知等の相手方の電子メール開封を確認すること、通知等の相手方に通知等の内容を確認した旨の折り返しの連絡を求めることその他の必要な措置を講ずるものとする。

（指定の有効期間の延長に伴う措置）

第２３条　乙は、特定秘密管理者から令第８条第１号の規定に基づく特定秘密の指定の有効期間を延長した旨の通知を受けたときは、法第３条第２項第２号に掲げる措置を受けた者に対し、当該指定の有効期間が延長された旨及び延長後の当該指定の有効期間が満了する年月日を書面の交付により通知しなければならない。

２　前項の場合において、乙は、当該指定の有効期間が延長された旨及び延長後の当該指定の有効期間が満了する年月日を当該指定に係る情報を取り扱う従業者（当該指定の有効期間の延長について前項の通知を受けた者を除く。）に周知しなければならない。

（指定の解除に伴う措置）

第２４条　乙は、特定秘密管理者から令第１０条第１項第２号の規定に基づく特定秘密の指定が解除された旨の通知を受けたときは、当該指定に係る特定資料等であったものについて、特定秘密の表示に赤色の二重線を付すことその他これに準ずる方法によりこれを抹消した上で、令第１０条第２項に規定する指定解除表示をしなければならない。

２　前項の場合において、乙は、法第３条第２項第２号に掲げる措置を受けた者に対し、当該指定が解除された旨及びその年月日を書面により通知しなければならない。

３　第１項の場合において、乙は、当該指定が解除された旨及びその年月日を当該指定に係る情報を取り扱う従業者（当該指定の解除について前項の通知を受けた者を除く。）に周知しなければならない。

（登録及び管理）

第２５条　乙は、特定秘密を保有したとき、特定資料等の交付若しくは特定秘密の伝達を受けたとき又は自ら特定資料等を作成したときは、速やかに、その旨を帳簿に登録しなければならない。

２　乙は、特定資料等の貸出し、回収、返却又は廃棄を行ったときは、速やかに、その旨を帳簿に登録しなければならない。

３　乙は、第２２条から前条までの措置を講じたときは、速やかにその旨を帳簿に登録しなければならない。

（実施報告）

第２６条　乙は、特定資料等を接受、作成、送達又は廃棄（第３２条の規定により廃棄した場合を除く。）したときは、速やかに、特定秘密管理者に対し、その旨を書面又は電磁的記録により報告しなければならない。

２　前項に規定する報告は、作成した特定資料等、又は作成において完成に至らなかった特定資料等であって、特定秘密管理者の指示を受けたものの取扱いを含めて行うものとする。

（立入制限措置等）

第２７条　乙は、特定資料等が取り扱われている場所について、当該特定資料等を取り扱う従業者、第１０条第２項の承認を受けた特定秘密取扱事業者の従業者であって当該特定秘密を取り扱う者及び甲と保全契約を締結した他の事業者の従業者であって、乙の求めに応じ特定秘密管理者が許可した者（以下「特定秘密取扱事業者の従業者等」という。）以外の立入りを禁止しなければならない。

２　前項の規定により立入りを禁止した場合、当該場所を管理する者は、当該場所に立ち入ってはならない旨の掲示その他立入禁止に必要な措置を講じなければならない。

３　第１項の場所を新設し、又は変更したときは、当該施設において特定秘密の取扱いを開始する前に、特定秘密管理者の承認を得なければならない。

４　乙は、当該特定秘密を取り扱う従業者及び特定秘密取扱事業者の従業者等以外の者を、みだりに第１項に規定する場所に立ち入らせ、又はその付近に必要以上に近づか

せてはならない。
５　乙は、当該特定秘密を取り扱う従業者及び特定秘密取扱事業者の従業者等に対しても、作業に必要な限度を超えて、第１項に規定する場所に立ち入らせてはならない。
（携帯型情報通信・記録機器の持込制限）
第２８条　乙は、携帯型情報通信・記録機器の特定資料等が取り扱われている場所への持込みを禁止しなければならない。
２　　やむを得ず持込みが必要となった場合には、乙は、特定秘密管理者の事前の承諾を得た上で、持ち込む携帯型情報通信・記録機器について、インストールされているソフトウェアを確認するなど特定秘密の漏えいを防止するための措置を講じなければならない。
（特定資料等の返却等）
第２９条　乙は、特定秘密管理者が交付した特定資料等及び当該特定資料等に関し作成したすべての特定資料等を主たる契約が終了（契約解除の場合も含む。）した後直ちに特定秘密管理者に返却し、又は提出しなければならない。ただし、特定秘密管理者が特定資料等の廃棄又は保持を認めた場合はこの限りではない。
（検査）
第３０条　乙は、特定秘密の取扱いの業務を管理するため必要な帳簿を整備し、毎月１回以上特定秘密の取扱いの状況について検査を行い、特定秘密管理者に結果を報告しなければならない。
２　　特定秘密管理者は、前項に規定する報告を受けるほか、乙の特定秘密の取扱い状況について自ら調査する必要があると認めるときは、特定秘密管理者が別に指定する職員に検査及び指導を行わせることができる。
３　　乙は、特定秘密管理者が乙の再委託先に対し、検査等を行うときは、特定秘密管理者の求めに応じ、必要な協力をしなければならない。
（特定資料等の取扱いの記録）
第３１条　乙は、業務管理者に、特定資料等の閲覧その他取扱いの経過を明確にするため、特定資料等を取り扱った従業者の氏名、日時、その他特定秘密管理者が指示した事項の記録を保存させるものとする。
（緊急事態に際しての廃棄）
第３２条　乙は、特定資料等の奪取その他特定秘密の漏えいのおそれがある緊急の事態に際し、その漏えいを防止するため他に適当な手段がないと認められる場合は、特定秘密として指定された情報を探知することができないよう、焼却、粉砕、細断、溶解、破壊等の復元不可能な方法により、当該特定資料等を廃棄しなければならない。
２　乙は、前項の規定に基づき、特定資料等を廃棄する場合には、あらかじめ特定秘密管理者を通じて防衛大臣の承認を得なければならない。ただし、その手段がない場合又はそのいとまがない場合は、廃棄後速やかにその旨を特定秘密管理者を通じて防衛大臣に報告しなければならない。
３　前項ただし書きに規定する報告は、特定資料等の奪取その他特定秘密の漏えいのおそれがある緊急の事態に際し、廃棄した特定資料等の概要、その漏えいを防止するため他に適当な手段がないと認められる場合に該当する理由及び廃棄に当たって用いた方法を書面又は電磁的記録により報告するものとする。
（事故発生時等の措置）

第３３条　乙は、特定秘密の漏えい、特定資料等の紛失、破壊等の事故が発生したとき（ それらの疑い又はおそれがあるときを含む。）、又はこの規則に定める秘密保護のための措置に抵触するような事態が発生したときは、直ちに事故の内容に応じた適切な措置を講ずるとともに、把握し得る限りの全ての内容を特定秘密管理者に報告しなければならない。

２　乙は、前項に規定する報告後、事故の原因のほか、特定秘密管理者から指示があった事項について詳細な調査を行い、速やかにその結果を特定秘密管理者に報告しなければならない。

（違約金の請求）

第３４条　甲は、別に定める秘密等の保全又は保護の確保に関する違約金条項の規定に基づき違約金を請求することができる。

（関連資料等の保存）

第３５条　乙は、秘密等の保全又は保護の確保に関する違約金条項の規定に基づき違約金を請求できる期間が満了するまでの間は、主たる契約、帳簿等、特定秘密の保護や取扱いに関する資料等を保存しなければならない。

（再委託の禁止）

第３６条　乙は、特定秘密の取扱いに係る業務（物件の輸送、施設の警備その他の役務であって、特定秘密の内容を知り得ないと認められるものを除く。）を第三者に再委託してはならない。ただし、やむを得ず再委託を行う場合は、あらかじめ、甲に対し、再委託の相手方、契約内容、取り扱わせる特定秘密を特定する事項、特定秘密の保護の手段等を記した書面又は電磁的記録を添えて、甲の許可を得なければならない。

２　前項の規定により再委託を行う場合において、再委託先は、特定秘密取扱事業者でなければならない。

３　乙は、第１項の規定により再委託を行う場合、再委託先による特定秘密及び特定資料等の適切な取扱いを確保するため、当該再委託先の作成する秘密保全規則等、再委託先における特定秘密を取り扱う従業者の名簿、その他特定秘密及び特定資料等の秘密保全のための措置の実施状況等を確認しなければならない。

４　前３項の規定は、乙が外部の機関に特定資料の閲覧が必要な品質システムの審査を委託する場合に準用する。

５　　乙は、再委託先と再委託の契約を締結し、又は契約の内容を変更したときは、再委託先に対し再委託の契約書の写しを甲に提出するよう指導しなければならない。ただし、乙が当該再委託の契約書の写しを甲に提出した場合はこの限りではない。

（保全契約の解除等）

第３７条　甲は、乙が本特約の規定に違反したときは、催告を要さずに本契約の一部又は全部を直ちに解除することができる。この場合において、甲は乙及び再委託先に対して損害賠償の責を負わないものとする。

２　再委託先の責に帰すべき事由により、甲が当該再委託先との保全契約を解除する場合は、甲は乙にその旨を通報するものとする。この場合において、甲は乙に対して損害賠償の責を負わないものとする。

３　乙が再委託先との契約を解除する場合は、事前に甲にその旨を通報しなければならない。

属　紙

適性評価に関する特約条項

（候補者名簿の提出）

第１条　乙は、その従業者に特定秘密を取り扱わせるため防衛大臣による適性評価を実施する必要があると認めるときは、その者の氏名、生年月日、所属する部署、役職名及び法第１２条第１項各号のうち該当する号その他参考となる事項を記載し、又は記録した名簿を作成し、これを特定秘密管理者に提出しなければならない。

２　　乙は、前項の名簿に記載し、又は記録した事項に変更があるときは、速やかに特定秘密管理者に通知しなければならない。

（適性評価の実施に関する協力）

第２条　乙は、評価対象者について照会があった場合に必要な報告を行うこと、評価対象者及びその上司等に対する面接等の実施に便宜を図ることなど、防衛大臣が実施する適性評価に必要な協力を行わなければならない。

（適性評価結果等通知書その他の文書の管理）

第３条　乙は、適性評価の結果が記された文書その他適性評価の実施に当たり特定秘密管理者に送付し、又は特定秘密管理者から送付された文書の管理を、次の各号に定めるところにより行わなければならない。

(1) 漏えい又は滅失の防止その他安全管理のための措置を厳格に行うこと。

(2) 用済後速やかに廃棄し、適性評価の結果適性があると認められた旨特定秘密管理者が通知した文書は送付日から５年、その他の文書は送付日から１年を超えて保存しないこと。

（評価結果その他の個人情報の目的外利用の禁止）

第４条　乙は、評価対象者が適性評価の実施に同意をしなかった事実、適性評価の結果適正がないと認められた事実その他適性評価に関し特定秘密管理者から通知される個人情報を、法令に基づく場合を除き、特定秘密の保護以外の目的のために利用し、又は第三者に提供してはならない。

（特定秘密の取扱業務の停止）

第５条　乙は、適性評価の結果適性があると認められた従業者であって、現に特定秘密を取り扱っている者又は新たに特定秘密を取り扱わせようとしている者について、特定秘密管理者から、新たな適性評価の結果として、適正がないと認められた旨通知があったときは、直ちに、当該従業者が特定秘密を取り扱わないよう措置しなければならない。特定秘密管理者から、法第１２条第１項第３号の規定に該当するため、適性に疑義がある旨通知されたときも同様とする。

（事後の事情の変化に関する報告）

第６条　乙は、過去５年以内に適性評価の結果適性があると認められた従業者であって、現に特定秘密を取り扱っている者又は新たに特定秘密を取り扱わせようとしている者について、教育等を通じて「特定秘密の保護に関する誓約書」に基づく申出を徹底させるとともに、面談等の機会を活用し、次に掲げる事情が職務の内外を問わず生じていないかどうかの確認を行い、状況の変化の継続的な把握に努めなければならない。

(1) 外国籍の者と結婚した場合その他外国との関係に大きな変化があったこと。

(2) 罪を犯して検挙されたこと。
(3) 懲戒処分の対象となる行為をしたこと。
(4) 情報の取扱いに関する規則に違反したこと。
(5) 違法な薬物の所持、使用等薬物の違法又は不適切な取扱いを行ったこと。
(6) 自己の行為の是非を判別し、若しくはその判別に従って行動する能力を失わせ、又は著しく低下させる症状を呈していると疑われる状況に陥ったこと。
(7) 飲酒により、けんか等の対人トラブルを引き起こしたり、業務上の支障を生じさせたりしたこと。
(8) 裁判所から給与の差押命令が送達されるなど経済的な問題を抱えていると疑われる状況に陥ったこと。
(9) 上記のほか、特定秘密を漏らすおそれがないと認めることについて疑義が生じたこと。

２　乙は、前項各号に掲げる事情があると認めた場合には、速やかに特定秘密管理者に報告しなければならない。

（従業者が派遣労働者である場合の措置）

第７条　乙は、乙の指揮命令の下に労働する派遣労働者（労働者派遣事業の適正な運用の確保及び派遣労働者の保護等に関する法律（昭和６０年法律第８８号）第２条第２号に規定する派遣労働者をいう。）である従業者について、第１条の名簿に登載する場合には、同条に定める事項のほか、次に掲げる事項を当該名簿に記載し、又は記録するとともに、当該従業者を雇用する事業主に対し、当該名簿に登載した旨を通知しなければならない。
(1) 派遣労働者である旨
(2) 当該従業者についての予定している業務内容

２　　乙は、乙の指揮命令の下に労働する派遣労働者である従業員について、特定秘密管理者から次に掲げる事項を通知された場合には、当該通知の内容を書面により、当該従業者を雇用する事業主に通知しなければならない。
(1) 適性評価実施責任者に提出する名簿に登載しないこと。
(2) 適性評価を実施することについて防衛大臣の承認が得られたこと、又は得られなかったこと。
(3) 当該従業者が適性評価の実施についての同意をしなかったことにより適性評価が実施されなかったこと。
(4) 当該従業者が同意を取り下げたことにより適性評価の手続が中止されたこと。
(5) 適性評価の結果
(6) 当該従業者が法第１２条第１項第３号の規定に該当するため、適性に疑義があること。

３　乙は、過去５年以内に適性評価の結果適性があると認められた従業者であって、現に特定秘密を取り扱っている者又は新たに特定秘密を取り扱わせようとしている者が乙の指揮命令の下に労働する派遣労働者である場合には、当該従業者を雇用する事業主が当該従業者について第６条の事情があると認めたときに、乙に確実に報告をさせる必要な措置を講じなければならない。

４　乙は、乙の指揮命令の下に労働する派遣労働者を雇用する事業主に対し、第１項又は第２項の通知をしたときは、当該通知をした文書について、これが第３条の規定に

準じて適切に管理されるよう、必要な措置を講じなければならない。

5　乙は、評価対象者が派遣労働者である従業者の場合には、当該従業者を雇用する事業主に対し、当該従業者が適性評価の実施に同意をしなかった事実、適性評価の結果適性がないと認められた事実その他適性評価に関し乙を経由して特定秘密管理者から通知される個人情報を、法令に基づく場合を除き、特定秘密の保護以外の目的のために利用し、又は第三者に提供しないよう必要な措置を講じなければならない。

（契約履行後における乙の義務）

第８条　第３条、第４条並びに前条第４項及び第５項の規定は、契約履行後においても準用する。

付録第21

装備品等秘密の保全に関する特約条項

（乙の一般義務）

第１条　乙（契約業者）は、主たる契約条項に基づく装備品等秘密の保全に関しては、この特約条項及び附属する装備品等の調達に係る秘密保全対策ガイドライン（第９条第１項において単に「ガイドライン」という。）に定めるところにより装備品等秘密保全の万全を期さなければならない。

２　乙は、乙の従業員、再委託を行う場合においてはその相手方（以下「中小受託事業者」という。）その他甲により装備品等秘密の表示のある秘密に属する文書又は図画（以下「特定資料」という。）又は装備品等秘密の表示のある秘密に属する物件（以下「特定物件」という。）を取扱う場所への立ち入りが許可された者の故意又は過失により秘密が漏えいしたときであっても、その責任を免れることはできない。

（送達）

第２条　甲は、特定資料又は特定物件を乙に交付するときは、当該特定資料又は当該特定物件に装備品等秘密の表示を付すとともに、当該特定資料又は当該特定物件に装備品等秘密指定書（当該特定資料又は当該特定物件において装備品等秘密を記録し、又は化体する部分を特定するために必要な事項を記載した書面。以下同じ。）を添えて、送達するものとする。

２　前項の場合において、当該特定資料又は当該特定物件が次の各号に掲げる情報に該当するときは、甲は、装備品等秘密の表示に加え、当該各号に定める表示を付すものとする。ただし、既にＮＡＴＯ　ＣＯＮＦＩＤＥＮＴＩＡＬ又はＮＡＴＯ　ＲＥＳＴＲＩＣＴＥＤの表示が付されているものについては、改めて当該表示を付すことを要しない。

(1)　米国秘密軍事情報（秘密軍事情報の保護のための秘密保持の措置に関する日本国政府とアメリカ合衆国政府との間の協定第１条（ａ）に規定する秘密軍事情報であって、アメリカ合衆国政府から受領したものをいう。第６条第２項第１号において同じ。）米国政府

(2)　北大西洋条約機構秘密情報（北大西洋条約機構から受領した情報又は資料であって、情報及び資料の保護に関する日本国政府と北大西洋条約機構との間の協定第１条（ⅱ）に規定する秘密の指定を受けているものをいう。第６条第２項第２号において同じ。）　ＮＡＴＯ　ＣＯＮＦＩＤＥＮＴＩＡＬ又はＮＡＴＯ　ＲＥＳＴＲＩＣＴＥＤ

(3)　仏国秘密情報（情報の保護に関する日本国政府とフランス共和国政府との間の協定第１条（ａ）に規定する秘密情報であって、フランス共和国政府から受領したものをいう。第６条第２項第３号において同じ。）仏国政府

(4)　豪州秘密情報（情報の保護に関する日本国政府とオーストラリア政府との間の協定第１条ａに規定する秘密情報であって、オーストラリア政府から受領したものをいう。第６条第２項第４号において同じ。）豪州政府

(5)　英国秘密情報（情報の保護に関する日本国政府とグレートブリテン及び北アイルランド連合王国政府との間の協定第１条ａに規定する秘密情報であって、グレートブリテン及び北アイルランド連合王国政府から受領したものをいう。第６条第２項第５

号において同じ。）英国政府

(6)　インド秘密軍事情報（秘密軍事情報の保護のための秘密保持の措置に関する日本国政府とインド共和国政府との間の協定第１条ａに規定する秘密軍事情報であって、インド共和国政府から受領したものをいう。第６条第２項第６号において同じ。）インド政府

(7)　伊国秘密情報（情報の保護に関する日本国政府とイタリア共和国政府との間の協定第１条ａに規定する秘密情報であって、イタリア共和国政府から受領したものをいう。第６条第２項第７号において同じ。）伊国政府

(8)　韓国秘密軍事情報（秘密軍事情報の保護に関する日本国政府と大韓民国政府との間の協定第２条（ａ）に規定する秘密軍事情報であって、大韓民国政府から受領したものをいう。第６条第２項第８号において同じ。）韓国政府

(9)　独国秘密情報（情報の保護に関する日本国政府とドイツ連邦共和国政府との間の協定第１条（ａ）に規定する秘密情報であって、ドイツ連邦共和国政府から受領したものをいう。第６条第２項第９号において同じ。）独国政府

(10)　瑞国秘密情報（防衛装備品及び技術の移転に関する日本国政府とスウェーデン王国政府との間の協定第四条に基づく防衛装備品及び技術に係る情報保護に関する日本国防衛省とスウェーデン王国を代表する国防装備庁との間の取決め第1項に規定する秘密情報であって、スウェーデン王国政府から受領したものをいう。第６条第２項第１０号において同じ。）瑞国政府

(11)　サウジ秘密情報（防衛協力及び交流の過程で取得される情報の保護に関する日本国国防省とサウジアラビア王国国防省との間の取決め第１項ａに規定する秘密情報であって、サウジアラビア王国国防省から受領したものをいう。第６条第２項第１１号において同じ。）　サウジ政府

(12)　ＵＡＥ秘密情報（防衛装備品及び技術の移転に関する日本国政府とアラブ首長国連邦政府との間の協定第五条に従って作成される防衛装備品及び技術に係る情報の保護に関する日本国防衛省とアラブ首長国連邦国防省との間の取決め第１項３に規定する秘密情報（「محظور」に秘密指定されたものを 除く。）であって、アラブ首長国連邦国防省から受領したものをいう。第６条第２項第１２号において同じ。）　ＵＡＥ政府

(13)　宇国秘密情報（情報の保護に関する日本国政府とウクライナ政府との間の協定第１条ａに規定する秘密情報であって、ウクライナ政府から受領したものをいう。第６条第２項第１３号において同じ。）　宇国政府

（特定資料の保全措置）

第３条　乙は、主たる契約の説明書、仕様書、計算書、図表等のうち、特定資料を防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律（令和５年法律第５４号）第２７条第３項の規定により防衛大臣に報告した装備品等秘密の取扱いの業務に従事する者（以下「関係社員」という。）以外の者に供覧してはならない。

２　乙は、関係社員であっても、作業に必要な限度を超えて特定資料を供覧してはならない。

（特定物件の保全措置）

第４条　乙は、特定物件について、その保管中取扱いの慎重を期して、関係社員以外の者に供覧してはならない。

２　乙は、関係社員であっても、作業に必要な限度を超えて特定物件を供覧してはならない。

（特定資料及び特定物件の複製等）

第５条　乙は、主たる契約に定められている場合を除き、特定資料を複製若しくは製作し、又は特定物件の設計資料、見取図、試験成績表等の複製、製作若しくは写真撮影をする場合は、あらかじめ、甲の許可を得なければならない。

２　乙は、主たる契約又は前項の甲の許可により特定資料の複製若しくは製作又は特定物件の設 計資料、見取図、試験成績表等の複製、製作若しくは写真撮影をする場合は、あらかじめ、実施の細部について甲と協議し、甲又は甲の代理者の立会の下行わなければならない。

３　第１項に規定する特定資料及び特定物件の複製等において完成に至らなかったものは、甲の指示に従い、装備品等秘密として探知することが困難となるよう、焼却、粉砕、細断、溶解、破壊等の方法により、確実に破棄しなければならない。

（装備品等秘密の表示等）

第６条　乙は、特定資料又は特定物件を複製又は製作し、甲からの指示があったときは、甲又はその指定する者の立会いの下、これらに装備品等秘密及び登録番号等の表示を付さなければならない。ただし、甲又はその指定する者の許可を受けたときはこの限りではない。

２　前項の場合において、当該特定資料又は当該特定物件が次の各号に掲げる情報に該当するときは、乙は、装備品等秘密、登録番号等の表示に加え、当該各号に定める表示を付さなければならない。ただし、既にＮＡＴＯ　ＣＯＮＦＩＤＥＮＴＩＡＬ又はＮＡＴＯ　ＲＥＳＴＲＩＣＴＥＤの表示が付されているものについては、改めて当該表示を付すことを要しない。

(1)　米国秘密軍事情報　米国政府
(2)　北大西洋条約機構秘密情報　ＮＡＴＯ　ＣＯＮＦＩＤＥＮＴＩＡＬ又はＮＡＴＯ　ＲＥＳＴＲＩＣＴＥＤ
(3)　仏国秘密情報　仏国政府
(4)　豪州秘密情報　豪州政府
(5)　英国秘密情報　英国政府
(6)　インド秘密軍事情報　インド政府
(7)　伊国秘密情報　伊国政府
(8)　韓国秘密軍事情報　韓国政府
(9)　独国秘密情報　独国政府
(10)　瑞国秘密情報　瑞国政府
(11)　サウジ秘密情報 サウジ政府
(12)　ＵＡＥ秘密情報 ＵＡＥ政府
(13)　宇国秘密情報 宇国政府

（実施報告）

第７条　乙は、特定資料若しくは特定物件を接受、複製、送達、製作若しくは甲からの指示により破棄したとき、又は第５条に規定する特定物件の設計資料、見取図、試験成績表等を複製、製作若しくは写真撮影をしたときは、速やかに、甲に対し、その旨を書面又は電磁的記録により報告しなければならない。

（立入禁止措置）
第８条　乙は、特定資料又は特定物件が取り扱われている場所について、立入りを禁止しなければならない。
２　前項の規定により立入りを禁止した場合、当該場所を管理する者は、当該場所に立ち入ってはならない旨の掲示その他立入禁止に必要な措置を講じなければならない。
３　乙は、関係社員以外の者を、みだりに第１項に規定する場所に立ち入らせ、又はその付近に必要以上に近づかせてはならない。
４　乙は、関係社員に対しても、作業に必要な限度を超えて、第１項に規定する場所に立ち入らせてはならない。
（秘密保全規則等）
第９条　乙は、社（工場）内における装備品等秘密の保全を確実に行うため、この特約条項締結の日から１箇月以内（着工の時期が１箇月以内に到来するときは、着工の日まで）にガイドラインに基づき、装備品等秘密の保全に関する規則及び装備品等秘密保全実施要領（以下「装備品等秘密保全規則等」という。）を作成の上、甲の確認を受けるものとする。ただし、装備品等秘密保全規則等が既に作成され、甲の確認済みのものであるときは、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装備品等秘密保全規則等を変更するときは、あらかじめ、甲に届出なければならない。
（特定資料の返却等）
第１０条　乙は、甲が送達した特定資料及び特定物件並びに第５条の規定により複製、製作又は写真撮影をした全ての資料を契約終了後、直ちに、甲に返却し、又は提出しなければならない。
２　乙は、契約履行中であっても、装備品等秘密指定書に示されている装備品等秘密の指定の有効期間が満了した場合は、直ちに、当該資料を甲に返却し、又は提出しなければならない。
（検査）
第１１条　乙は、装備品等秘密の取扱いのため必要な簿冊を整備し、原則として、毎月１回以上装備品等秘密の保全状況について点検を行い、甲又は甲の代理者の検査を受けなければならない。
２　甲又は甲の代理者は、必要があると認めたときは、前項の検査を行うほか、装備品等秘密の保全の状況を検査し、又は必要な指示を乙に与えることができる。
（保管状況報告）
第１２条　乙は、毎年６月末日及び１２月末日現在の特定資料及び特定物件の保管の状況を甲に報告しなければならない。
（特定資料又は特定物件を取扱う場所の新設等）
第１３条　乙は、特定資料又は特定物件を取り扱う場所を新設し、又は変更するときは、あらかじめ、甲の確認を受けなければならない。
（事故発生時の措置）
第１４条　乙は、装備品等秘密の漏えい、紛失、破壊等の事故が発生し、又はそれらの疑い若しくはおそれがあったときは、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。
２　甲は、別に定める秘密等の保全又は保護の確保に関する違約金条項（第２３号）の

規定に基づき違約金を請求することができる。

（保全教育）

第１５条　乙は、関係社員に対し、年間計画を立て、保全教育を実施しなければならない。

２　乙は、保全教育を実施する場合は、その内容及び実施方法について、この特約条項締結の日から１箇月以内（着工の時期が１箇月以内に到来するときは、着工の日まで）に甲の確認を受けなければならない。ただし、その内容等が既に甲の確認済みのものであるときは、特別の指示がない限り、届出をすれば足りる。

３　乙は、前項の規定により甲の確認を受けた事項に変更がある場合には、あらかじめ、甲の確認を受けなければならない。

４　乙は、毎年、甲が指示する時期に、保全教育の実施状況を、甲に報告しなければならない。

（再委託）

第１６条　乙は、特定資料の複製若しくは製作又は特定物件の製作、取付け、修理、実験、調査研究、複製等を第三者に再委託させてはならない。ただし、やむを得ず再委託を行う場合は、あらかじめ、甲に対し、再委託の相手方、契約内容、装備品等秘密保全の手段等を記した書面又は電磁的記録を添え、甲の許可を得なければならない。

２　前項の規定により再委託を行う場合において、中小受託事業者は、防衛省の契約担当官等と装備品等秘密の保全に関する規定を含む契約を結んでいる者でなければならない。

３　第１項の規定により再委託を行う場合において、物件の輸送、施設の警備その他装備品等秘密の内容を知り得ないと認められる役務を提供する者については、前項に規定する本省の契約担当官等との契約を要しない。

４　第１項及び第２項の規定は、乙が部外の機関に品質システムの審査を委託する場合に準用する。

５　乙は、第１項に規定する場合を除き、特定資料又は特定物件を第三者に提供してはならない。

（契約の解除）

第１７条　中小受託事業者の責に帰すべき事由により、甲が当該中小受託事業者との契約を解除する場合は、甲は乙にその旨を通報するものとする。この場合において、甲は乙に対して損害賠償の責を負わないものとする。

２　乙が中小受託事業者との契約を解除する場合は、事前に甲にその旨を通報しなければならない。

３　乙の責に帰すべき事由により、甲が乙との契約を解除する場合は、甲は乙の中小受託事業者との契約を解除することができる。この場合において、甲は当該中小受託事業者に対して損害賠償の責を負わないものとする。

（装備品等秘密の取扱いの業務の終了に伴う措置等）

第１８条　事故の発生その他の事由（第１０条の規定によるものを除く。）により、甲が乙による特定資料の複製若しくは製作又は特定物件の製作、取付け、修理、実験、調査研究、複製等の一部又は全部をやめさせることが適切であると認めたときは、乙は、速やかに、甲の指示に従い、特定資料又は特定物件の返却、廃棄その他の必要な措置を講じなければならない。

付録第22

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（防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律（令和５年法律第５４号）第２７条第１項に規定する装備品等秘密、特定秘密の保護に関する法律（平成２５年法律第１０８号）第３条第１項に規定する特定秘密又は日米相互防衛援助協定等に伴う秘密保護法（昭和２９年法律第１６６号）第１条第３項に規定する特別防衛秘密をいう。以下同じ。）の保全又は保護（以下「秘密保全」という。）を万全ならしめるために、秘密保全特約（装備品等秘密の保全に関する特約条項（装備品等秘密の指定等に関する訓令（令和６年防衛省訓令第１０号。以下「装秘訓令」という。）別記第２号様式の特約条項をいう。以下同じ。）、特定秘密の保護に関する特約条項（特定秘密の保護に関する訓令第３６条第１項に規定する審査基準及び第３７条第２項に規定する特約条項について（防経装第１９０７４号。２６．１２．２４）別紙の付紙第２の特約条項をいう。以下同じ。）若しくは防衛装備庁における特定秘密の保護に関する特約条項（防衛装備庁における特定秘密の保護に関する訓令第３６条第１項に規定する審査基準及び第３７条第２項に規定する特約条項について（装装制第５４号。２７．１０．１）別紙の付紙第２の特約条項をいう。以下同じ。）又は特別防衛秘密の保護に関する特約条項（特別防衛秘密の保護に関する訓令（平成１９年防衛省訓令第３８号）別記第５号様式の特約条項をいう。以下同じ。）若しくは防衛装備庁における特別防衛秘密の保護に関する特約条項（防衛装備庁における特別防衛秘密の保護に関する訓令（平成２７年防衛装備庁訓令第２５号）別記第６号様式の特約条項をいう。以下同じ。）をいう。以下同じ。）を補足する共通の事項を規定するものである。乙は、秘密保全規則等（秘密保全特約及び本ガイドラインに基づき作成し甲の確認を受けた秘密の保全に関する規則及び秘密保全実施要領をいう。以下同じ。）に従い、秘密を適正に取り扱わなければならない。

２　用語の定義

本ガイドラインにおいて用語の意義は次のとおりとする。

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

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

(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。

⑹　特定資料又は特定物件とは、次のいずれかに該当するものをいう。
ア　装備品等秘密の保全に関する特約条項第１条第２項に規定する特定資料又は特定物件
イ　特定秘密の保護に関する特約条項第１条第２項又は防衛装備庁における特定秘密の保護に関する特約条項第１条第２項に規定する特定資料又は特定物件
ウ　特別防衛秘密の保護に関する特約条項第１条第２項又は防衛装備庁における特別防衛秘密の保護に関する特約条項第１条第２項に規定する特定資料又は特定物件
⑺　関係社員とは、職務上特定資料又は特定物件を取り扱う必要があり、乙が秘密保全規則等に基づき指定した者をいう。
⑻　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。
⑼　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
⑴　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。
⑵　本ガイドラインの適用の対象となる者は、乙において秘密に係る情報に接する全ての者（秘密に係る情報に接する役員（持分会社にあっては従業者を含む。以下同じ。）、管理職員等を含む。この場合において、当該者が、自らが秘密に係る情報に接しているとの認識の有無を問わない。）とする。
⑶　秘密に係る情報の取扱いにおいて、パソコン及び携帯型記録機器（以下「パソコン等」という。）を使用する必要のない乙に対しては、パソコン等に係る規定（第８⑹オ、第１０⑷から⑼まで、第１１及び第１２）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。
⑷　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
⑴　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。
⑵　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。
⑶　乙は、秘密保全規則等を関係社員に確実に周知すること。

５　第三者への開示の禁止
乙は、第三者との契約において乙の保有し、又は知り得た情報を伝達、交換、共有

その他提供する約定があるときは、秘密の情報をその対象から除く措置を講じなければならない。

6　組織のセキュリティ

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

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

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

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

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

7　特定資料又は特定物件の分類及び管理

(1)　総括者は、特定資料又は特定物件の作成、交付、供覧、保管、廃棄等の管理（以下単に「管理」という。）を確実に実施するため、秘密の種類ごと（必要な場合は、これに加え機密、極秘及び秘の区分ごと）に必要な関係簿冊（保管記録、閲覧・貸出記録、検査記録、立入記録等を記載する簿冊をいう。以下同じ。）を整備し、定期的に点検すること。この場合、総括者は、記録内容の改ざんを防止するための適切な管理を行うとともに、関係簿冊を秘密保全の責任がある期間（秘密等の保全又は保護の確保に関する違約金条項の取扱いについて（防経装第３２７０号。１９．３．２９）別添の第２条に規定する乙が秘密等を保全する責任がある期間をいう。）の経過後３年を経過するまでの間保管するものとし、その後、甲の確認を受け、廃棄すること。また、装備品等秘密の提供を受ける際に交付された装秘訓令第７条第３項に規定する装備品等秘密指定書についても、関係簿冊に準じて管理すること。

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

8　人的セキュリティ

(1)　部門責任者等は、関係社員の指定の範囲を必要最小限とするとともに、ふさわしい者を充て、秘密保全規則等を遵守させなければならない。

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

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

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

ア　乙による関係社員の指定の同意を求められた従業者が、当該同意をしない場合

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

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

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

(7)　部門責任者等は、次のア及びイに掲げる措置を確実に講ずること。

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

イ　関係社員の秘密保全に関する責任を明確にし、在職中及び離職後における秘密保全に係る取扱いについて、同意書を提出させること。また、当該同意書には、当該関係社員が秘密を漏えいした場合の当該関係社員の民事上の責任に係る規定を含めること。

(8)　総括者は、秘密保全の重要性及び保全に関する社内規則（秘密保全規則等を含む。ウにおいて同じ。）の内容について、関係社員に対し、次のアからカまでに掲げる内容を含む教育及び訓練を新たに関係社員に指定された者が秘密を取り扱う前等の必要な都度及び定期的に行い、その結果を甲に届け出ること。また、関係社員以外の全ての従業者に対して、定期的に必要な範囲について教育を行い、その結果を記録するものとする。

ア　秘密保全の重要性及び意義（秘密保全意識のかん養を含む。）

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

ウ　保全に関する社内規則の確実な履行

エ　隙のない勤務と私生活における慎重な行動

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

カ　ア～オまでに掲げる事項の他、関係社員の役割と責任に応じて必要となる事項

9　秘密漏えい等の事故発生時の対応

(1)　事故発生時の報告

ア　乙は、秘密の漏えい、紛失、破壊等の事故（それらの疑い又はおそれがあるときを含む。以下同じ。）が発生したときは、適切な措置を講じるとともに、直ち

に把握し得る限りの全ての内容を甲に報告し、その後速やかにその詳細を甲に報告しなければならない。

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

(2)　報告要領の作成

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

(3)　事故発生時の対処等

ア　対処体制及び手順

総括者は、秘密の漏えい、紛失、破壊等の事故発生時の対処体制、当該対処体制における責任者及び対処手順を定めるものとする。

イ　証拠の収集

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

ウ　秘密保全規則等への反映

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

(4)　対処訓練の実施

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

１０　物理的及び環境的セキュリティ

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

(2)　総括者は、秘密保全施設の外側に隣接する建物又は敷地のうち必要な範囲を「保全外部区域」として指定し、秘密保全施設への不正な立入りを防止するため、次のアからウに掲げる措置を講じるものとする。

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

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

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

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

ア　秘密保全施設内における秘密保全を強化するために、総括者は、次の(ｱ)か

ら(ｴ)までに掲げる内容を含む秘密保全の措置を講じること。

(ｱ)　関係社員その他甲により立入りを許可された者（第１１(8)イに基づき甲が秘密保全施設への立入りを許可した外部委託を受ける者を含む。）以外の者を立ち入らせない。

(ｲ)　秘密保全施設の錠として、電子錠を利用する場合は、入退の記録を電子的に取得すること。この場合、電子的記録をもってイに規定する記録簿に代えることができるものとする。

(ｳ)　秘密保全施設への立入りの記録を定期的に精査し、記録すること。

(ｴ)　総括者は、秘密保全施設の鍵の保管及び接受、秘密保全施設の警備その他秘密保全施設における秘密保全を強化するため必要な細部の手続を定めること。

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

(4)　総括者は、秘密を取り扱うパソコン等の設置に当たっては、次のアからカまでに掲げる項目の情報システム実装計画を作成し、必要に応じ更新すること。この際、設置場所における危険性を十分配慮して設置し、必要な保護措置を講じること。

ア　秘密を取り扱う情報システムを構成する構成要素の構成設定に係る現状を正確に確認及び証明するための目録

イ　第１１(1)に規定する操作手順書

ウ　第１２(1)に規定するアクセス制御方針

エ　秘密のデータのデータフロー図

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

カ　その他必要な事項

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

(6)　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。

(7)　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。

(8)　総括者は、⑷の規定により設置したパソコン等以外のパソコン等及び携帯型情報通信機器については、秘密保全施設への持込みを原則として禁止すること。ただし、新設等のため、やむを得ず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。

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

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

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

１１　通信及び運用管理

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

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

(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、原則として禁止すること。

(5)　総括者は、情報システムのメンテナンス等（保守、点検、診断、修理、整備及びアップデートを含む。以下同じ。）を定期的及び必要に応じて行うため、次のアからエまでに掲げる項目を含むシステムメンテナンス等計画を作成し、当該計画に基づき、メンテナンス等を実施するものとする。

ア　メンテナンス等を実施する人員

イ　メンテナンス等の対象（情報システムにおけるソフトウェア、ハードウェア及びファームウェアを含む。）

ウ　メンテナンス等の内容（メンテナンス等に使用される機器及びツールを含む。）

エ　その他メンテナンス等に必要な事項

(6)　総括者又はその指定する者は、前号のシステムメンテナンス等計画に基づきメンテナンス等の作業を行っている間、立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。

(7)　総括者又はその指定する者は、メンテナンス等を実施した日時、人員の名簿（国籍等を記載）、実施の対象及び内容等を記録すること。

(8)　秘密保全施設内で使用する情報システムのメンテナンス等に関する外部委託は、原則として禁止する。ただし、やむを得ず外部委託をしなければならない場合には、総括者は、少なくとも次のアからウまでに掲げる措置を講ずること。

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メンテナンス等に当たっては、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じること。

(9)　総括者は、装備品等秘密の保全に関する特約条項第５条第１項、特定秘密の保護に関する特約条項第９条第３項若しくは防衛装備庁における特定秘密の保護に関する特約条項第９条第３項又は特別防衛秘密の保護に関する特約条項第５条第１項若しくは防衛装備庁における特別防衛秘密の保護に関する特約条項第５条第１項に規定する特定資料、特定図面等及び特定物件の複製等について、電子情報としてこれを行う場合には、可搬記憶媒体以外への保存を禁止すること。

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

ア　可搬記憶媒体を使用するときは、総括者又はその指定する者がその都度許可を与えること。

イ　可搬記憶媒体の貸出・返却に関する記録を残すこと。

ウ　可搬記憶媒体に情報を記録するときは、秘匿すること。

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

オ　可搬記憶媒体の内容の複製及び破棄手順に関すること。

１２　アクセス制御

(1)　総括者は、秘密保全施設内において情報システムを使用する場合には、関係社員が取り扱うことができる秘密の種類及び関係社員の役職等に応じた情報システムの利用可能機能等をアクセス制御方針として規定することにより、アクセス制御を行うこと。なお、アクセス制御方針は、次のアからエまでに掲げる項目を含めるものとする。

ア　アカウント管理者（アカウントの設定、変更及び削除等を行う者）の指定
イ　利用者ごとに業務遂行上必要最小限度の機能及び権限となるようアカウントを管理すること。
ウ　秘密保全施設内に設置する情報システムを構成する機器に対する識別及び情報システム利用者の認証に関すること。なお、情報システム利用者の認証は、多要素認証等の方法により情報システム利用者が特定されるよう設定すること。
エ　その他必要な事項

(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ほか、定期的な見直しを実施するとともに、速やかに見直しに応じた利用者としての登録及び登録の削除を行うこと。

(3)　総括者は、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。なお、パスワード設定においては、次のアからオまでに掲げる内容を含む必要な措置を講じ、その内容を第１１(1)に規定する操作手順書に記載すること。
ア　利用者にパスワードの変更手順を理解させること。
イ　利用者にパスワードの変更を実施させること。
ウ　パスワードは、推測されにくいものとし、定期的に変更すること。
エ　利用者が画面上の表示を確認しつつ設定することのできる機能を有すること。
オ　ログオン及びユーザセッションに関すること。

(6)　総括者は、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。

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

１３　検証・改善

(1)　総括者は、秘密保全に万全を期すため、秘密保全に係る社内の文書類、組織、秘密の管理状況及び教育内容等の秘密保全を確保するための各種措置等について不断の検証を行い、状況に応じて必要な改善を行うこと。また、検証に際して、次のア及びイに掲げる事項を考慮したリスク査定を実施すること。

ア　特定資料又は特定資料及び情報システムへの不正なアクセス、開示、使用、改ざん、破壊等が及ぼす被害、脅威及び脆弱性の程度

イ　特定資料又は特定物件を取り扱う部署の内部のほか、秘密保全に影響を及ぼす恐れがあると認める範囲内で、自社の別の部署及び外部の組織(情報システムの保守を請け負う業者等を含む。)におけるリスクを特定、分析及び評価

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

１４　検査及び調査の受入れ

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

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

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

１５　適用の特例

(1)　乙は、自らが保有する設備等の改修に時間を要する等の理由により直ちに本ガイドラインに従って秘密を取り扱うことが困難な場合は、その理由及び本ガイドラインに従った取り扱いを行うことができる時期について、甲に申請するものとする。

(2)　乙は、前項の規定により甲に申請をした場合は、本ガイドラインに従って秘密を取り扱うために必要な設備等の改修等に関する事業計画をあわせて甲に提出するものとする。ただし、他の契約によりすでに甲が確認済みの事業計画がある場合には、特別の指示がない限り、届出をすれば足りる。

(3)　前号の事業計画の納期は、令和１０年３月３１日を超えてはならない。

(4)　甲は、(2)の規定により提出された事業計画を確認し、これを適当と認めたときは、その旨を乙に通知するものとする。

(5)　乙は、前号の通知を受けた場合には、甲が適当と認めた事業計画が完了するまでの間は、この通達による改正前の「装備品等の調達に係る秘密保全対策ガイドライン」の規定を適用することができる。

付録第23

秘密等の保全又は保護の確保に関する違約金条項

第１条　乙は、防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律（令和５年法律第５４号）第２７条第１項に規定する「装備品等秘密」、特定秘密の保護に関する法律（平成２５年法律第１０８号）第３条第１項に規定する「特定秘密」又は日米相互防衛援助協定等に伴う秘密保護法（昭和２９年法律第１６６号）第１条第３項に規定する「特別防衛秘密」（以下「秘密等」という。）であって、装備品等秘密の保全に関する特約条項（装備品等秘密の指定等に関する訓令（令和６年防衛省訓令第１０号）第８条１項に規定する装備品等秘密の保全に関する規定をいう。）、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。）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言う。）に基づき乙が保全又は保護すべきものを当該秘密等に接する権限のない者に漏えい（以下単に「漏えい」という。）したことを甲が証明した場合は、甲が契約の全部又は一部を解除するか否かにかかわらず、次の各号に掲げる基準に従い、甲が指定する期間内に違約金を支払わなければならない。ただし、乙が、当該秘密等の漏えいについて、自己の責に帰すべからざる事由により生じたことを証明したときは、この限りでない。

(1)　漏えいした秘密等の区分に応じて、それぞれ次に掲げる金額

ア　「装備品等秘密」のときは、契約金額の１００分の５

イ　「特定秘密」のときは、契約金額の１００分の７．５

ウ　「特別防衛秘密」のときは、契約金額の１００分の１０

(2)　次のアからウまでの事由に該当する場合には、前号に掲げる金額に、それぞれ当該アからウまでに掲げる金額を加算

ア　秘密等の漏えいが乙の故意又は重大な過失によると認められるときは、前号に掲げる金額と同額

イ　乙が甲に対し、秘密等の漏えいの事実を直ちに報告しなかったときは、前号に掲げる金額に１００分の５０を乗じた金額

ウ　乙が甲に対し、秘密等の漏えいに関し虚偽の報告をしたときは、前号に掲げる金額に１００分の５０を乗じた金額

(3)　乙が、過去１０年以内に秘密等を漏えい（当該漏えいが本契約に係るものであるか、甲乙間の他の契約に係るものであるかを問わない。）し、甲により第１号のいずれかに該当するものとして違約金を請求されていた場合においては、今回漏えいした秘密等の区分に応じて同号に掲げる金額と同額を加算

(4)　前号に規定する場合における当該過去の秘密等の漏えいが第２号に掲げる加算事由のいずれかに該当するとされた場合であって、今回の秘密等の漏えいが当該加算事由と同一の事由に該当するときは、前号に掲げる金額の加算に加えて、当該加算事由に応じて第２号に掲げる金額と同額を加算

(5)　秘密等の漏えいが、第２号のイ又はウに掲げる事由に該当せず、かつ、乙の極めて軽微な過失によると認められるときは、第１号、第３号及び前号の規定

にかかわらず、契約金額の１００分の５以内で甲が定める金額

２　乙が複数の秘密等を一の行為において漏えいした場合は、漏えいした各秘密等について算出した違約金の額の最高額をもって違約金の額とする。

３　乙が甲との間の複数の契約において保全又は保護すべきものとされている秘密等を漏えいした場合において、いずれの契約の履行における漏えいか乙が証明できないときは、当該秘密等が漏えいした疑いがある各契約について算出した違約金の額の最高額をもって違約金の額とする。

４　乙が違約金を甲の指定する期間内に支払わない場合は、乙は、当該期間を経過した日から支払いをする日までの日数に応じ、当該期間を経過した日における法廷利率により計算した額の延納利息を甲に支払わなければならない。

第２条　乙が秘密等を保全又は保護する責任がある期間は、乙が甲から秘密等を指定した旨の通知を受けたときから、当該秘密等の指定にかかる期間（甲が当該期間を延長する旨乙に通知した場合は、当該延長後の期間）が終了するまで、又は甲が秘密等の指定を解除するまでとする。ただし、甲が乙に秘密等を提供する場合は、当該秘密等を乙が受領したときからとする。

２　前項に定める乙が秘密等を保全又は保護する責任がある期間に乙が秘密等を漏えいしたときは、当該期間又は当該期間経過後３年を経過するまでの間、甲は、乙に対して前条による違約金を請求できるものとする。

３　本違約金条項が付されている契約が終了し、又は解除された場合であっても、第１項に定める乙が秘密等を保全又は保護する責任がある期間及び前項により甲が乙に対して違約金を請求できる期間は、本違約金条項は、なおその効力を有するものとする。

第３条　本違約金条項の規定は、これによる違約金とは別に甲がその損害につき乙に対し賠償を請求することを妨げない。

付録第24

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

（保護すべき情報の取扱い）

第１条　乙は、この特約条項が付された契約を履行するに際しては、この特約条項の定めるところに従い、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、乙に保護を求める情報として、甲が指定したものをいう。以下同じ。）を取り扱わなければならない。

（情報セキュリティ基本方針等）

第２条　乙は、保護すべき情報を取り扱うに当たり、保護すべき情報を取り扱う乙の業務環境等を考慮の上、別紙（甲の定める「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」（以下「本基準」という。））に従って、必要な措置をとらなくてはならない。

２　乙は、前項を実施するため、本基準に従い、情報セキュリティ基本方針を、本基準及び情報セキュリティ基本方針に従い、情報セキュリティ規則を、本基準及びシステムセキュリティ実施要領に従い、情報セキュリティ実施手順を作成しなければならない。

３　乙は、前項の規定により作成した情報セキュリティ基本方針等について、甲の確認を受けなければならない。ただし、他の契約により既に甲の確認を受けているものと同一のものである場合は、その旨を甲に届出をすれば足りる。

４　乙は、甲の確認を受けた基本方針等のうち、内容の全部又は一部を変更しようとするときは、あらかじめ、その内容が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。

（中小受託事業者に対する指導監督）

第３条　乙は、本特約条項が付された契約を履行するに当たり、これを適切に履行する義務を負い、中小受託事業者（契約の履行に係る作業に従事する全ての事業者（乙を除く。）をいう。以下同じ。）に対して、適切な指導・監督を行わなければならない。

（中小受託事業者等に保護すべき情報を取り扱わせる際の手続等）

第４条　乙は、契約の履行に当たり、保護すべき情報を中小受託事業者に取り扱わせる必要が生じた場合には、当該中小受託事業者において情報セキュリティが確保されるよう、甲の定めるところにより、適切な取扱いに必要な事項を確認しなければならない。

２　乙は、前項により確認した内容を書面により甲に届出するとともに、中小受託事業者に保護すべき情報を取り扱わせることについて申請し、甲の承認を得なければならない。

３　乙は、第三者（甲と直接契約関係にある者以外の全ての者をいう。以下同じ。）との契約（この特約条項が付された契約以外の契約をいう。この項において同じ。）において、乙が保有し、又は知り得た情報を伝達、交換、共有等を行う約定があるときは、保護すべき情報をその約定の対象から除くよう、当該第三者との契約を変更する等の措置を講じなければならない。

４　甲は、第２項の規定により申請のあった内容を直接確認する必要があると認めた場合には、乙に、その旨を申し入れるものとする。

５　乙は、甲から前項の申し入れがあった場合には、必要な協力を行うものとす

る。

6　乙は、原則として中小受託事業者を除く第三者に保護すべき情報を開示してはならない。ただし、契約の履行上又は公益上特に当該第三者に開示する必要があると認められる場合には、その都度、甲と協議するものとする。

（監査）

第５条　甲は、乙においてこの特約条項の定めに従い保護すべき情報の取扱いが行われているかにつき、監査を行うものとする。

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、乙においてこの特約条項の定めに基づいて作成した情報セキュリティ基本方針等に従い保護すべき情報の取扱いが行われていないと認める場合には、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、前項の規定により是正のため甲から必要な措置を講じるよう求めがあった場合には、速やかに必要な措置を講じなければならない。

5　甲は、乙の中小受託事業者に対して直接監査を行う必要があると認めた場合には、乙に、その旨を申し入れるものする。

6　乙は、甲から前項の申し入れがあった場合には、必要な協力をしなければならない。

7　第１項から第４項までの規定は、甲が行う乙の中小受託事業者に対する監査について準用する。ただし、甲は、第３項の規定に準じて、是正のため必要な措置を講じるよう求めるに際しては、乙を通じて求めるものとする。

（事故等発生時の措置）

第６条　乙は、本基準に従って定めた情報セキュリティ規則において、事故等（当該規則において情報セキュリティ事故及び情報セキュリティ事象に該当するものをいう。以下同じ。）が発生したときは、本基準に定めるところにより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　乙は、前項に規定する事故等がこの契約の履行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。

3　前項の協議の結果、事故等が乙の責めに帰すべき事由によるものである場合には、その措置に必要な費用は、乙の負担とする。

4　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事故等が発生し、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１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、乙又は乙の中小受託事業者が保護すべき情報を取り扱う場合について準用する。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、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、前項の指示又は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。

（適用の特例）

第９条　乙は、自らが保有する設備等の改修に時間を要する等の理由により直ちに本基準に従って保護すべき情報を取り扱うことが困難な場合は、その理由及び別紙に従った取扱いを行うことができる時期について、甲に申請しなければならない。

２　乙は、前項の規定により甲に申請をした場合は、本基準に従って保護すべき情報を取り扱うために必要な設備等の改修等に関する事業計画を速やかに甲に提出しなければならない。ただし、他の契約により、既に甲に対して事業計画を提出している場合には、その旨を甲に届け出るものとする。

３　前項の事業計画の終期は、令和１０年３月３１日を超えてはならない。

４　甲は、第２項の規定により提出された事業計画（第２項ただし書の規定により届出があった場合には、その内容）を確認し、これを適当と認めたときは、その旨を乙に通知するものとする。

５　乙は、前項の通知を受けた場合には、甲が適当と認めた事業計画が完了するまでの間は、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）９２４６号。令和４年３月３１日）２１．７．３１）の規定を適用することができる。

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基準

目　次

第１　趣旨

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。）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、本基準に則り情報セキュリティ対策を実施するものとする。

第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。

(1)　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。
(2)　保護すべき情報とは、装備品等及び役務の調達に関する情報のうち、防衛省が企業に保護を求める情報として指定したものをいう。
(3)　防衛関連企業とは、保護すべき情報を取り扱う契約相手方企業(団体及び個人を含む。）をいう。
(4)　取扱者とは、保護すべき情報を取り扱う者として、経営者等が指定した者をいう。
(5)　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、情報セキュリティ規則及び情報セキュリティ実施手順をいう。
(6)　経営者等とは、防衛関連企業の経営者又は受注案件を処理する部門責任者をいう。
(7)　中小受託事業者とは、契約の履行に係る作業に従事する全ての事業者（防衛省と直接契約関係にある者を除く。）をいう。
(8)　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を定めたものをいう。
(9)　情報セキュリティ規則とは、本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。
(10)　情報セキュリティ実施手順とは、本基準及びシステムセキュリティ実施要領に基づき、防衛関連企業が保有又は使用する保護システムに対する管理策を定めたものをいう。
(11)　第三者とは、法人又は自然人としての防衛省と直接契約関係にある者以外の全ての者をいい、親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の防衛省と直接契約関係にある者に対して指導、監督、業務支援、助言、監査等を行う者を含む。
(12)　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。
(13)　保護システム利用者とは、保護すべきデータに接する必要のある者及び保護システムの運用管理業務に従事する者であって、当該データを保存する領域又はその機器に関わる者をいう。
(14)　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。
(15)　送達とは、取扱施設の外に所在する者に送り届けることをいい、輸送（社外の事業者との契約に基づき、当該事業者が保護すべき情報を特定の相手方に送達することをいう。以下同じ。）を含む。
(16)　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。
(17)　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。
(18)　情報システムとは、ハードウェア（サーバ、パソコン、モニタ、携帯端末、プリンタ、スキャナ等を含む。以下同じ。）、ソフトウェア（プログラムの集合体をいい、ファームウェアを含む。以下同じ。）、ネットワーク（暗号化により公衆回線に作られる仮想的な専用ネットワークを含む。）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)　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、コンピュータウイルス及びスパイウェア等をいう。
(20)　情報セキュリティ事象とは、情報セキュリティ事故のおそれ並びに情報セキュリティ事故に至らない情報セキュリティ基本方針等への違反及びそのおそれのある状態をいう。
(21)　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。
(22)　取扱施設とは、保護すべき情報の取扱い及び当該情報に属する文書等の保管を行う場所として、本基準の規定に従って防衛関連企業が指定する建物又は敷地の一部又は全部をいう。
(23)　関係施設とは、取扱施設の外側に隣接する場所であって、本基準の規定に基づき防衛関連企業が指定する建物又は敷地の一部又は全部をいう。
(24)　システムログとは、情報システムにおける動作履歴に関する記録をいう。
(25)　取扱施設等とは、取扱施設及び関係施設をいう。
(26)　ベースライン構成設定とは、保護システムとシステムコンポーネントの構成の把握並びに保護システムの更新及び変更時のベース(基準)となる構成設定をい

う。
(27)　ブラックリストとは、保護システムにインストール又は保護システムで実行してはならないソフトウェアのリストをいう。
(28)　ホワイトリストとは、保護システムにインストール及び保護システムで実行してもよいソフトウェアのリストをいう。
(29)　保護すべきデータとは、保護すべき情報が電子的な状態にあるものをいう。
(30)　構成設定とは、情報システムを構成する構成要素（ハードウェア、ソフウェア、ネットワーク及び記憶媒体）の機種、バージョン等及び当該構成要素の機能並びに動作等を制御する設定値を決定することをいう。
(31)　リプレイ攻撃とは、利用者の確認に用いられる認証データの通信を盗聴し得られたデータをそのまま用いてその利用者になりすます方式をいう。
(32)　モバイルコードとは、インターネット等のネットワークを通じて、自動的にダウンロード及び実行されるプログラムをいう。
(33)　外部ネットワークとは、インターネットその他の防衛関連企業によって管理されないネットワークをいう。
(34)　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。
(35)　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。
(36)　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。
(37)　管理者権限とは、情報システムの管理（情報システム利用者の登録、削除、及びアクセス制御等）を行うために付与される権限をいう。
(38)　外部システムとは、防衛関連企業によって管理されないシステム（クラウドサービス事業者によるクラウドサービス、及び請負業者の情報システム等を含む。）をいう。
(39)　ユーザセッションとは、保護システム利用者が実行する各アプリケーションの論理的な経路をいう。
(40)　タイムスタンプとは、電子データの取得、作成等を行った時刻に関する情報をいう。
(41)　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。

第３　対象

１　対象とする情報

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。

２　対象者

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。）、管理職員、派遣社員、契約社員、パート、アルバイト等を含む。）とする。

第４　情報セキュリティ基本方針等

１　情報セキュリティ基本方針等の作成及び変更

(1)　防衛関連企業は、本基準の内容に沿った情報セキュリティ基本方針等を作成し、経営者等の承認を得るものとする。
(2)　防衛関連企業は、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、経営者等の承認を得るものとする。
(3)　防衛関連企業は、情報セキュリティ基本方針等を作成又は変更する場合、本基準との適合性に関する防衛省の確認を受けるものとする。

2　情報セキュリティ基本方針等の周知等

(1)　保護すべき情報の管理全般に係る総括的な責任を負う者（以下「総括者」という。）は、情報セキュリティ基本方針等を取扱者に周知するものとする。
(2)　防衛関連企業は、情報セキュリティ実施手順を社外の者（契約に関係する防衛省の職員を除く。）にみだりに公開しないよう適切に管理するものとする。

第５　組織のセキュリティ

1　経営者等の職責

経営者等は自社の情報セキュリティに係る最高かつ最終的な権限及び責任を有するものとする。

2　経営者等及び取扱者の責務

(1)　取扱者の指定等

ア　経営者等は、取扱者の指定の範囲を業務の遂行上必要最小限度に制限するとともに、次に掲げる事項に合意した者の中からふさわしい者を取扱者に指定するものとする。

(ｱ)　在職中及び離職後において、業務上知り得た保護すべき情報を、第三者に漏えいしないこと（以下「守秘義務」という）。
(ｲ)　守秘義務に違反した場合に法律上の責任を負うこと。
(ｳ)　守秘義務の内容を理解し、かつ、承諾すること。

イ　経営者等は、保護すべき情報に係る全ての情報セキュリティの責任を明確にするため、取扱者のうち、ふさわしいと認める者を次に掲げる者に指定するものとする。

(ｱ)　総括者
(ｲ)　保護すべき情報及びこれに関連する資産ごとに、それぞれ管理責任を負う者（以下「管理者」という。）

ウ　経営者等は、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取扱者にふさわしい者として認めてはならない。

エ　管理者は、取扱者として指定した個人の氏名、生年月日、所属する部署、役職及び国籍等を記載したリスト(以下「取扱者名簿」という。)を作成又は更新し、取扱者に保護すべき情報を取り扱わせる前に、防衛省に届け出なければならない。なお、保護すべき情報の取扱いの開始については、防衛省の指示によるものとする。

オ　管理者は、取扱者の退職、異動、職務内容の変更などの理由により、保護すべき情報にアクセスする必要がなくなった場合は、取扱者名簿を更新する

とともに、当該取扱者との面談等により、守秘義務を再確認するものとする。

(2)　保護システム利用者の指定等

ア　経営者等は、保護システム利用者を指定するものとし、その指定の範囲を業務の遂行上必要最小限度に制限するものとする。その際、次に掲げる事項に関し書面による同意を事前に得るものとする。なお、保護システムの利用により、当該利用に対する常時監視、履歴の記録及び監査について同意したものとみなす。

(ｱ)　ログオンする情報システムが、保護すべきデータを取り扱うための保護システムであること。

(ｲ)　保護システムの利用は常時監視されるとともに、利用履歴が記録され、監査の対象となること。

(ｳ)　保護システムを不正に使用した場合に法律上の責任を問われる可能性があること。

イ　経営者等は、保護システムに係る全ての情報セキュリティの責任を明確にするため、保護システム利用者のうち、ふさわしいと認める者を次に掲げる者に指定するものとする。

(ｱ)　保護システムの運用管理に責任を負う者（以下「保護システム管理者」という。）

(ｲ)　保護システム管理者の業務遂行を補佐する者（以下「保護システム担当者」という。）

ウ　保護システム管理者は、アに規定する保護システム利用者の名簿（以下「保護システム利用者名簿」という。）を作成するものとし、保護システム利用者の退職、異動及び職務内容の変更などの理由により、保護システムを利用する必要がなくなった場合は、保護システム利用者名簿を更新するものとする。

(3)　情報セキュリティの確保

ア　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、情報セキュリティ基本方針等の承認等を通して、自社における情報セキュリティの確保に努めるものとする。また、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対して、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るものとする。

イ　経営者等は、全ての従業員に対し、情報セキュリティ事故等（情報セキュリティ事故及び情報セキュリティ事象をいう。以下同じ。）を発見又は検知した場合は、管理者（保護システムに係る情報セキュリティ事故等にあっては、保護システム管理者又は保護システム担当者を含む。）に直ちに報告するよう義務付け、全ての従業員は、その義務を果たすものとする。

ウ　経営者等は、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懲戒手続を定め、違反が生じた場合には、当該対処方針及び懲戒手続に基づき対処するものとする。

エ　経営者等は、前２号に規定する者、その他の責任の割当てについて、当該責任を業務の遂行上必要最小限度に分割して割り当て、同一の取扱者に広範

な責任を持たせてはならない。ただし、総括者及び管理者については、兼任させることができるものとする。

3　保護すべき情報を取り扱う中小受託事業者

防衛関連企業は、契約の履行に当たり、保護すべき情報を取り扱う業務を中小受託事業者に請け負わせる場合は、本基準に規定する措置の実施を当該中小受託事業者との間で契約し、当該業務を開始する前に、防衛省が定める確認事項に基づき、当該中小受託事業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、防衛省に申請することとする。ただし、輸送その他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。

4　第三者

(1)　第三者の保護すべき情報の取扱い

防衛関連企業は、防衛省の許可を受けずに第三者に保護すべき情報を取り扱わせてはならない。

(2)　第三者との約定からの保護すべき情報の除外

防衛関連企業は、第三者との契約において防衛関連企業の保有又は知り得た情報を伝達、交換、共有又は提供する約定がある場合、約定の対象とする情報から保護すべき情報を除くものとする。ただし、事前に防衛省の許可を得た場合は、この限りでない。

第6　保護すべき情報の管理

1　保護すべき情報の分類

防衛関連企業は、保護すべき情報を他の情報から明確に区別できるよう適切に分類し、厳格に管理するものとする。

2　保護すべき情報の目録の作成等

(1)　目録の作成

管理者は、保護すべき情報を保管した場所、保存した保護システム、可搬記憶媒体等、保護すべき情報の管理状況を記載した目録を作成するものとする。なお、目録の作成は、保護すべき情報の取扱いに関するシステムログの記録により代用することができるものとする。

(2)　目録の更新

ア　管理者は、下記の（ｱ）から（ｳ）までに掲げる措置（以下「接受等」という。）を実施する場合は、保護すべき情報の目録を更新するものとする。なお、目録の更新は、保護すべき情報の取扱いに関するシステムログの記録により代用することができるものとする。

(ｱ)　保護すべき情報の接受、作成、製作又は複製（バックアップを含む。以下同じ。）

(ｲ)　保護すべき情報の閲覧又は持ち出し（取扱施設の外に持ち出すことをいい、貸出を含む。以下同じ。）

(ｳ)　保護すべき情報の送達、返却、提出又は廃棄

イ　目録には、接受等を行った者の氏名、所属、所在等を記載するものとする。ただし、保護すべき情報の取扱いに関するシステムログの記録により代用する場合は、アカウントの識別子を記載するものとする。

(3)　目録等の保管

管理者は、保護すべき情報の目録は、不正なアクセス、改ざん、盗難等から保

護するため、文書により保存する場合は、施錠したロッカー等（第８第５項第２号の規定により鍵及び解錠キーを厳格に管理するものとする。以下同じ。）により、データで保存する場合には、暗号化により必要な期間保管又は保存するものとする。

３　保護すべき文書等の表示等

(1)　保護すべき文書等への表示

管理者は、保護すべき文書等を作成、製作、収集、整理又は複製（以下「作成等」という。）した場合は、次に掲げる措置を講じるものとする。

ア　当該文書等が保護すべき情報を含む旨の表示を行うこととし、当該表示は、文書の表紙右上に記載する等、容易に判別可能なものとすること。

イ　当該文書等の中で、保護すべき情報が記録された箇所に、下線を引く、枠で囲む、文頭及び文末に括弧を付す等により明示すること。

ウ　当該文書等のうち、保護すべきデータが保存された可搬記憶媒体についても、保護すべきデータを含む旨を外形的に表示すること。

(2)　その他の表示

管理者は、封筒又はコンテナ等の容器に保護すべき文書等を格納して保管する場合は、当該封筒、ファイル、コンテナ等の容器の中に保護すべき情報が存在する旨を表示するものとする。

４　保護すべき情報の持ち出し及び送達

(1)　持ち出し及び送達の方法

ア　保護すべき情報の持ち出し及び送達を行う場合は、管理者の許可を得るものとする。

イ　保護すべき情報を持ち出し又は送達する場合は、施錠等により物理的に保護された容器に格納するものとする。

(2)　送達することができる者の制限

管理者は、保護すべき情報を持ち出し及び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するものとする。

(3)　持ち出し及び送達の際の表示

ア　保護すべき情報を持ち出し又は送達する場合は、封筒、コンテナ等の容器に、その中に保護すべき情報が含まれる旨を表示しないものとする。

イ　保護すべき情報の送達は、当該情報を受け取ることができる者の氏名等を相手にあらかじめ明示し、直接の手交（郵送の場合にあっては、書留）により、必ずその者によって受け取られるようにするものとする。

５　保護システムにおける可搬記憶媒体の使用制限管理者は、保護システムにおいて可搬記憶媒体を使用する場合は、次の各号に掲げる措置を講じるものとする。

(1)　使用できる可搬記憶媒体及びその用途などを記載した目録を作成し、保護システム管理者の承認を得ること。なお、目録の作成は、保護すべき情報の取扱いに関するシステムログの記録により代用することができるものとする。

(2)　前号に規定する目録は、定期的に、及び保護システムにおいて使用できる可搬記憶媒体、その用途等に変更があった場合など必要があると認められる場合にはその都度精査し、必要に応じ、更新すること。なお、目録の更新は、保護すべき情報の取扱いに関するシステムログの記録により代用することができるものとする。

(3)　個人の所有する又は所有者若しくは管理者が明確でない可搬記憶媒体を保護

システムにおいて使用しないこと。

(4)　保護システムにおいて可搬記憶媒体を使用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すること。

(5)　可搬記憶媒体の使用が、第１号に規定する目録に従って実施されることを確保するため、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上の措置を講じること。

(6)　第１号の規定により承認を得た可搬記憶媒体の保護システム以外の情報システムへの接続を制限すること。

6　保護すべき情報を記録した媒体の廃棄又は再利用

(1)　保護すべき文書等（この号において、保護すべきデータを除く。）の廃棄防衛関連企業は、保護すべき文書等を廃棄する場合は、裁断等確実な方法により廃棄し、保護すべき文書等が復元できない状態であることを点検したうえで、その旨を記録するものとする。

(2)　可搬記憶媒体の廃棄又は再利用

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廃棄する場合は、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うえで、可搬記憶媒体を物理的に破壊し、その旨を記録するものとする。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に実施するものとする。

(3)　保護システムの廃棄又は再利用

防衛関連企業は、保護システムを廃棄する場合は、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うえで、記憶媒体を物理的に破壊し、その旨を記録するものとする。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に実施するものとする。

(4)　廃棄又は再利用前の点検

ア　管理者は、前各号における点検の記録は、廃棄又はデータ消去を実施した者の氏名、所属及び所在等、実施時刻並びに実施完了の証明となる資料（署名等）について記載又は添付し、文書により保管するものとする。

イ　前各号における点検を実施する者は、廃棄又はデータを復元できなくした者とは別の者を充てるものとする。

7　保護すべき文書等の防衛省への返却等

(1)　管理者は、契約履行後、防衛省の指示に従い、保護すべき文書等の返却、提出、破棄など必要な措置を講じるものとする。

(2)　防衛関連企業は、契約履行後、当該文書等を引き続き保有する必要がある場合は、その理由を添えて防衛省に協議を求めるものとする。

8　保護すべき文書等の作成等の手順

管理者は、保護すべき文書等の作成等及びその持ち出し、送達、返却及び廃棄に係る手順を定めるものとする。

9　防衛関連の情報を公開する場合の措置

防衛関連企業は、ホームページへの掲載、その他の方法により自社の情報を公開する場合は、当該情報の中に保護すべき情報が含まれていないことを確認するものとする。

第７　情報セキュリティ教育及び訓練

１　防衛関連企業は、取扱者に対し、次の各号に掲げる事項を含む教育及び訓練を１年に１回以上行うものとする。なお、教育及び訓練については、専門性の高い教育項目を含め、外部の知見を活用するなど適切に実施するものとする。

(1)　情報セキュリティの重要性及び意義（情報セキュリティ意識のかん養を含む。）

(2)　「need to knowの原則」（「情報は知る必要がある者のみに伝え、知る必要ない者には伝えない」という原則）の確実な履行

(3)　情報セキュリティ基本方針等の確実な履行

(4)　公私における慎重な行動

(5)　悪意のあるコードへの感染、内部不正、情報セキュリティ事象及び同事故等への対処手順

(6)　前号に掲げる事項のほか、情報セキュリティ事故等への対処のために必要な事項(7)　第１号から第６号までに掲げる事項のほか、取扱者の役割と責任に応じて必要となる技術的及び専門的な事項

２　経営者等は、総括者、管理者、保護システム管理者、保護システム担当者に対しては、前項に掲げる事項に加え、それぞれの職責等に関する教育を行うものとする。３管理者は、新たな取扱者の指定、取扱者の異動及び職務内容の変更、保護システムの変更が生じる場合その他必要があると判断する場合に、第１項に規定する教育及び訓練を行うものとする。

４　管理者は、前各項に規定する教育及び訓練の実施に係る状況を記録した文書を作成し保管するものとし、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間が経過するまで保管又は保存するものとする。

第８　物理的及び環境的セキュリティ

１　物理的セキュリティ対策の方針

(1)　管理責任者(取扱施設等の物理的セキュリティに責任を有する者で、管理者の中から総括者が指定した者をいう。以下同じ。)は、次に掲げる施設及び情報システム等に対する物理的セキュリティを確保するため、第２項から第４項までに掲げる事項に係る物理的セキュリティの対策の方針を作成するものとする。

ア　取扱施設及び関係施設

イ　取扱施設等の入退を管理するための鍵及び電子錠等の機器（以下「入退機器」という。）

ウ　保護システム

エ　保管された保護すべき文書等

(2)　管理責任者は、情報セキュリティ事故など物理的な情報セキュリティに重大な影響を及ぼす事象が発生した場合は、物理的セキュリティ対策の方針を精査し、必要に応じて修正を行うものとする。

２　取扱施設等に対する物理的セキュリティ対策

(1)　取扱施設等の指定

ア　経営者等は、自社のセキュリティ水準を維持する物理的範囲を画定するため、取扱施設に加え、関係施設を指定するものとする。

イ　経営者等は、取扱施設内に保護システム（保護すべき情報の保存又は当

該情報へのアクセスを可能とする機器に限る。第４項において同じ。）を設置し、当該施設内で保護すべき情報を取り扱うものとする。

ウ　管理責任者は、取扱施設等、取扱施設等に講じた物理的セキュリティ対策及び入退管理機器の設置状況について図面等により管理するものとする。

エ　管理責任者は、取扱施設等への立ち入り許可に関する手順を作成し、許可した者の名簿（以下「取扱施設等立入名簿」という。）を作成し、保護システム管理者の同意を得ることとする。

オ　管理責任者は、取扱施設等立入名簿に基づき取扱施設等への立ち入りを許可する証明書を発行するものとし、当該立ち入りを許可する者については、業務の遂行上必要最小限に制限するものとする。

カ　管理責任者は、取扱施設等立入名簿を定期的に見直し、必要に応じて更新するものとする。

(2)　管理責任者は、取扱施設等に対する物理的セキュリティ対策を確保するため、次に掲げる措置を実施するものとする。

ア　取扱施設と関係施設の境界に入退口を設置し、入退管理機器又は警備員、受付係その他管理責任者が指定した者（以下「警備員等」という。）により、入退する者が当該入退を許可された者であることを管理（識別及び認証を含む。以下この号において同じ。）すること。

イ　関係施設の外側境界に入退口を設置し、必要な管理措置により入退者を制限すること。

ウ　取扱施設への入退をＩＤカード（ 社員証、身分証明書その他入退する者の個人識別が可能なものをいう。以下同じ。）により管理する場合は、当該入退の記録を電子的に取得すること。

エ　取扱施設への入退を警備員等により管理する場合は、必要に応じて入退する者の所属、氏名、入退の時間等所要の事項を記録簿に記載すること。

オ　ウ及びエの規定により取得した記録は、定期的に、及び保護すべき情報等への不正なアクセスの発見に資するなど必要と認められる場合には、その都度精査すること。

カ　取扱施設等において敷地を指定した場合は、十分な高さ及び強度のあるフェンス等を設置するなど必要な措置を講じること。

キ　取扱施設の入退をＩＣカード（一時的に貸与した入退カード、複数の者が共用するカードその他入退する者の個人識別ができないものをいう。）のみで管理する場合は、当該施設の境界を警備員等、センサー装置又は監視カメラによる監視など必要な措置を講じること。

ク　取扱施設においては、当該施設の画像、動画、音声等の情報の収集・通信が可能な機器（携帯電話、デジタルカメラ、ボイスレコーダー等）の利用（持ち込みを含む。）を制限すること。

(3)　警備員等は、第２号オの規定により入退に係る記録を精査した場合は、その結果を記録した文書を作成し、管理責任者に報告するものとする。

(4)　管理責任者は、第２号ウ及びエに規定する入退に係る記録並びに前号に規定する当該記録を精査した結果を記録した文書を保管するものとし、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により契約履行後においても必要な期間保管又は保存するものと

する。

(5)　立入りが許可されていない者による取扱施設への立入りは、管理責任者が承認した場合に限り許可することとし、管理責任者の指定した者が同行して監視するとともに、第２号ウ又はエの措置を行うものとする。

(6)　取扱施設等が自然災害等の非常事態により使用できない場合は、経営者等が指定する取扱施設等を代替する施設において、総括者が当該事態の状況を踏まえつつ、取扱者のみが当該保護すべき情報に接することができるようにするために必要な物理的セキュリティ対策を講じることで、保護すべき情報を扱うことができる。

３　入退管理機器に対する物理的セキュリティ対策

管理責任者は、入退管理機器に対する不正なアクセス等を防止及び検知するため、以下の措置を講じるものとする。

(1)　入退管理機器の現状を記録した目録を作成し保管するものとし、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により必要な期間保管すること。

(2)　前号に規定する目録は、定期的に、及び入退管理機器の変更など必要があると認める場合には、その都度精査し、必要に応じ更新すること。

(3)　入退管理機器として暗証番号等を併用する場合は、定期的に、及び当該暗証番号等を配布されていた者が、異動等により取扱施設等への立ち入り権限を失うなど必要があると認める場合には、その都度当該暗証番号等を変更すること。

(4)　入退管理機器として錠を併用する場合は、鍵の紛失など必要があると認める場合に、当該錠を変更すること。

４　保護システムに対する物理的セキュリティ対策

(1)　保護システム管理者は、保護システムを構成するハードウェア及び記憶媒体について、不正な移動、持ち出し等を防止するため、必要な措置を講じるものとする。

(2)　保護システムの取扱施設外への持ち出しは、保護システム管理者が管理責任者と調整の上許可することとし、当該持ち出しを行う者が保護システム利用者でない場合は、保護システム管理者の指定する保護システム利用者が同行して監視し、記録するものとする。

(3)　保護システムに接続された送配線は、関係施設において破壊、情報窃取を防止又は検知できる物理的セキュリティ対策を講じるものとする。

(4)　その他の保護システムに対する管理策については、第８に定めるところによるものとする。

５　保管された保護すべき情報の物理的セキュリティ対策

(1)　保護すべき情報の保管

ア　保護すべき情報を文書等により保管する場合は、取扱施設内の施錠したロッカー等に保管するものとする。

イ　保護すべきデータを保護システムに保存する場合は、第４項第１号に定める措置を行うものとする。

(2)　鍵等の管理

第１号に規定するロッカー等の鍵を保管するのは、管理者（保護システムに関連する場合にあっては、保護システム管理者を含む。以下本号において同

じ。）及び管理者が指定した者のみとし、それ以外の者により解錠されることがないよう厳格に管理するものとする。

第９　保護システムについての管理策

１　防衛関連企業は、自社の保有又は使用する保護システムに、保護すべき情報を適切に取り扱うために必要と認める情報セキュリティ対策を講じるものとする。

２　防衛関連企業は、前項の規定に基づき情報セキュリティ対策を講じる際は、本基準及び付紙に規定する管理策を盛り込んだ情報セキュリティ実施手順を定めるものとする。

第１０　情報セキュリティ事故等への対応

１　情報セキュリティ事故等対処計画の策定

(1)　経営者等は、情報セキュリティ事故及び情報セキュリティ事象（以下「事故等」という。）の発生に備え、情報セキュリティ事故等対処計画を定めるものとし、総括者は、次に掲げる事故等対処の各段階に対処し得る体制、責任及び手順を定めるものとする。

ア　事故等への対処の準備

イ　事故等の発見及び検知時の報告・連絡要領

ウ　事故等の監視（システム監視を含む。）及び分析

エ　事故等による被害及び影響の抑制並びに局限

オ　事故等に係る証拠の保存及び原因の究明

カ　事故等からの復旧（復旧に要する時間の目標を含む。）

(2)　情報セキュリティ事故等対処計画においては、前号の規定による対処体制等のほか、次に掲げる事項についての措置を定めるものとする。

ア　保護システム管理者の下にヘルプデスク等を設置し、保護システム利用者に対し、情報セキュリティ事故等に関する必要な情報の提供等を行うこと。

イ　情報セキュリティ事故等の詳細を把握するため、デジタルフォレンジック技術の利用等により必要な情報を収集及び分析すること。

ウ　保護システムを含め、自社のネットワークにおけるすべての情報システムの分析及び精査（システムログの取得及び分析を含む。）を行い、当該情報システム内の構成要素、データ及びアカウント等の中から、悪意のあるコードへの感染又は不正アクセスなどの情報セキュリティ事故等が発生した原因を特定すること。

エ　情報セキュリティ事故等への対処の要領及び結果（当該事故等に対する分析及び原因究明等の結果を含む。）並びに当該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に関すること。

オ　情報セキュリティ事故等への対処において収集した情報の分析結果を踏まえ、当該対処に係る教訓を取りまとめ、情報セキュリティ教育及び訓練、情報セキュリティ事故等対処計画及び情報セキュリティ事故等対処テストの内容に反映させること。

(3)　事業継続計画を策定している場合は、当該計画と情報セキュリティ事故等対処計画との整合性を確保するものとする。

２　情報セキュリティ事故等への対処テスト

(1)　防衛関連企業は、情報セキュリティ事故等対処計画の有効性を検証し、潜在的な弱点又は欠陥を発見するため、情報セキュリティ事故等対処テストを第７第１項の規定による訓練に含めるなど、定期的に実施するものとする。
(2)　前号に規定する情報セキュリティ事故等対処テストを実施した場合は、当該テストの結果を記録した文書を作成し、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存するものとする。

第１１　情報セキュリティ事故等発生時の対応

１　情報セキュリティ事故等を発見又は検知した場合の処置

(1)　全ての従業員は、情報セキュリティ事故等を発見又は検知した場合は、速やかに管理者（保護システムに係る場合は保護システム管理者）に報告するものとし、管理者は情報セキュリティ事故等対処計画に基づき適切に対処するとともに、その内容及び結果（当該事故等に対する分析及び原因究明等の結果を含む。）並びに当該対処により取得した情報等を記録した文書を作成し、総括者に報告するものとする。
(2)　保護システム利用者が保護システムの脆弱性を発見又は探知した場合は、速やかに保護システム管理者に報告するものとし、保護システム管理者は、適切な対処を行うとともに、その内容、修正方法を記載した文書を作成し、総括者に報告するものとする。
(3)　保護システム管理者は、前２号の規定により作成した文書は、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、契約履行後においても必要な期間保管又は保存するものとする。
(4)　総括者は、第１号及び第２号による情報セキュリティ事故等対処計画に基づく対処を行う場合は、同計画に定められた期間内に行うものとする。
なお、当該期間までの改善又は修正が困難と認める場合は、是正計画を作成し、同計画に定められた期間内に修正を実施するとともに防衛省に報告するものとする。
(5)　防衛関連企業は、保護システムの脆弱性に係る修正を実施する場合は、第１２に規定するリスク査定の結果及び公開されている脆弱性情報データベース等を活用するものとし、当該脆弱性が保護システムのセキュリティに重大な影響を及ぼす場合には、可能な限り速やかに修正を実施するものとする。

２　防衛省への報告

(1)　総括者は、前項第１号に掲げる情報セキュリティ事故等の報告を受けた場合は、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(契約担当官等又は防衛装備庁長官が別に定めた部署の職員。以下同じ。)に報告するものとする。
(2)　総括者は、前号のほか、防衛関連企業の内部又は外部から情報セキュリティ事故等が発生した可能性又は将来発生する懸念の指摘があった場合は、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ものとする。
(3)　総括者は、前２号に規定する防衛省への報告については、それぞれ責任者及び連絡担当者等を明示した連絡系統図を含む報告要領を定め、責任者及び

連絡担当者等に異動等があった場合にはこれを更新するものとする。

(4)　総括者は、第１号の規定による情報セキュリティ事故等の詳細の防衛省への報告は、情報セキュリティ事故等対処計画に定められた期間までに、それらの原因（当該情報セキュリティ事故等の原因となった悪意のあるコード等の検体を取得している場合には、当該検体を含む。）及び影響並びにそれらに対する初期的な対処状況について報告するものとする。

第１２　リスク査定

１　総括者は、保護すべき情報に関連するリスクを特定、分析及び評価するため定期的に、自社の情報セキュリティに重大な変化が生じた場合など必要と認められた場合はその都度、リスク査定を実施するものとする。

２　総括者は、前項に規定するリスク査定を実施した場合は、速やかにその結果を記録した文書を作成し、当該文書を経営者等、管理者、保護システム管理者及び保護システム担当者その他の業務の遂行上必要と認める者に周知するものとする。

３　総括者は、前項に規定するリスク査定結果を記録した文書について、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存するものとする。

４　総括者は、第１項に規定するリスク査定を実施する場合は、保護すべき情報及び保護システムへの不正なアクセス、開示、使用、改ざん及び破壊等が及ぼす被害、脅威及び脆弱性の程度を複合的に評価するものとする。

５　総括者は、前各項の規定によりリスク査定を実施する場合は、保護すべき情報を取り扱う部署の内部のほか、保護すべき情報の保護に影響を及ぼすおそれがあると認める範囲内で、自社の別の部署又は外部の組織（情報システムの運用を請け負う業者等を含む。）におけるリスクを特定、分析及び評価するものとする。

第１３　セキュリティ監査

１　セキュリティ監査計画の作成等

(1)　防衛関連企業は、情報セキュリティ基本方針等に基づく措置の実施状況の確認及びその措置が継続的に有効であることの評価を客観的に行うため、監査部門を設置し、同部門には原則として最低１名は監査を受ける部署以外の者を含むものとする。この場合において、セキュリティ監査の項目が保護すべき情報に関する事項である場合は、当該保護すべき情報の取扱者を含むものとする。

(2)　監査部門は、次に掲げる事項を記載したセキュリティ監査計画を作成し、総括者を通じて経営者等の承認を得るものとする。

ア　セキュリティ監査に関与する者の氏名、所属する部署、役職、権限、責任の内容等

イ　セキュリティ監査を実施する日程

ウ　情報セキュリティ基本方針等に基づく措置に係る実施状況の確認及びその 措置が継続的に有効であることの評価を行うための手順及び方法

(3)　前号アの規定によりセキュリティ監査に関与する者に対する保護すべき情報及び保護システムに対するアクセス権限について、総括者は当該セキュリ

ティ監査の遂行上必要な権限を付与するものとする。

(4)　総括者は、セキュリティ監査を適切に実施するために必要な情報を監査部門に提供し、その情報を利用及び分析させるものとする。

2　セキュリティ監査の実施

総括者は、１年に１回以上及び自社の情報セキュリティに重大な変化が生じた場合など必要と認めた場合に、監査部門に、前項に規定するセキュリティ監査計画に基づくセキュリティ監査（ 情報セキュリティ基本方針等に基づく措置が継続的に有効であることの評価を含む。）を実施させるものとする。

3　セキュリティ監査結果の報告等

(1)　総括者は、監査部門に、セキュリティ監査終了後、速やかにその結果を記録した文書を作成及び提出させ、当該文書を経営者等、管理者、保護システム管理者及び保護システム担当者その他の業務の遂行上必要と認める者に周知するものとする。

(2)　総括者は、前号に規定するセキュリティ監査の結果を記録した文書には次に掲げる事項を明記させるものとする。

ア　情報セキュリティ基本方針等に基づく措置の実施状況及びその措置が継続的に有効であることに係る問題点の有無及びその内容

イ　アに規定する問題点がある場合は、その改善提案

ウ　イに規定する改善提案を踏まえた改善策の実施に必要な期間

(3)　総括者は、前号イの規定により監査部門から改善提案が示された場合は、当該措置を実施する部門と監査部門との間で協議させたうえで改善策を決定し、同協議で定められた期間までに当該改善策を実施するものとする。

(4)　前号に規定する改善策が監査部門との協議の結果、定められた期間内に実施することが困難と認められた場合には、総括者は速やかに是正計画を作成し、同計画に定められた期間内に当該改善策を実施するとともに防衛省に報告するものとする。

(5)　総括者は、セキュリティ監査計画、セキュリティ監査の結果を記録した文書その他のセキュリティ監査に係る重要な文書は、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存するものとする。

第１４　防衛省による監査

1　監査の受入

防衛関連企業は、防衛省によるセキュリティ対策に関する監査の要求があった場合は、これを受け入れるものとする。

2　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は、防衛省の求めに応じ必要な協力（監査官の取扱施設等への立入り、監査官による書類の閲覧、保護すべき情報の取扱いに関するシステムログの記録の確認等への協力）を行うものとする。

付紙

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システムセキュリティ実施要領

目　次

第１　趣旨

この要領は、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。）第９に基づき装備品等及び役務の調達における情報システムのセキュリティの確保に関して必要な事項を定めることを目的とする。

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

(1)　防衛関連企業は、自社の保有又は使用する保護システムについて、本基準に規定する措置を適切に実施し、本基準に適合していることを証明する資料として、システムセキュリティ実装計画書を作成するものとする。

(2)　システムセキュリティ実装計画書には、自社の保有又は使用する保護システムに関する次に掲げる文書等を記載又は添付するものとし、同計画は保護システム管理者が作成し、総括者を通じて経営者等の承認を得るものとする。

ア　第３第２項第１号に規定するベースライン構成設定
イ　第３第２項第５号に規定するブラックリスト又はホワイトリスト
ウ　第３第４項第１号に規定する構成設定目録
エ　第４第２項第１号に規定する操作手順書
オ　第５第１項第１号に規定するアクセス制御方針
カ　第７第３項第１号及び第２号に規定する保護システムにおけるモバイルコード及びＶｏＩＰ技術の利用に係る要件
キ　第７第３項第３号に規定する保護システムにおける各種のオフィス機器の利用に係る要件
ク　保護システムのセキュリティを確保するための組織体制図（経営者等、総括者及び保護システム管理者、その他保護システムのセキュリティに責任を有する者の具体的な責任の内容及び範囲を記載するものとする。）

ケ　保護システムのネットワーク構成図
コ　保護すべきデータのデータフロー図

2　システムセキュリティ実装計画書の定期的な確認

保護システム管理者は、保護システムの現状を正確に把握するためシステムセキュリティ実装計画書の内容を定期的に確認することとし、変更する場合は、第１項第２号により、総括者を通じて経営者等の承認を得るものとする。

3　システムセキュリティ実装計画書の保存等

保護システム管理者は、システムセキュリティ実装計画書を文書により保管する場合は施錠したロッカー等により、データで保存する場合には、暗号化により、少なくとも必要な期間保管又は保存するものとする。

4　システムセキュリティ実装計画書の周知

保護システム管理者は、システムセキュリティ実装計画書を作成又は変更した場合は、これを周知するとともに、システム管理業務に従事する者以外にシステムセキュリティ実装計画書（ 操作手順書を除く。）を配布又は閲覧させないものとする。

5　システムセキュリティ実装計画書の防衛省への提出等

システムセキュリティ実装計画書を作成した場合及び防衛省からの求めがあった場合は、同計画書について防衛省の確認を受けるものとする。

第３　構成管理

1　セキュリティエンジニアリングの原則の適用

防衛関連企業は、保護システムの設計、開発、導入及び変更する場合において、セキュリティエンジニアリングの原則（情報システムの企画から設計、開発、運用に至るまでの全ての工程において、セキュリティを確保する方策をいう。）を適用するものとする。

2　ベースライン構成設定等

(1)　保護システム管理者は、保護システムを構成するハードウェア、ソフトウェア、記憶媒体及びネットワーク（以下「保護システム構成要素」という。）について、次に掲げる要件を満たすために必要なベースライン構成設定を定め総括者の承認を得るものとする。

ア　情報セキュリティ基本方針等に基づく措置が実施可能なものであること。
イ　保護システムのセキュリティを確保するものであること。
ウ　保護システム構成要素の機能及び動作を業務の遂行上必要な最小限度に制限するものであること。

(2)　保護システム構成要素の構成設定は、ベースライン構成設定に従って保護システム管理者が設定するものとする。

(3)　構成設定の方法

ア　保護システム管理者は、保護システム構成要素の構成設定を適切に制御するための手順を定めるとともに総括者の承認を得て、同手順に基づきソフトウェアの導入等を行うものとする。
イ　アクセス権限の特定等
(ｱ)　保護システム構成要素の構成設定を行うための物理的及び論理的なアクセス権限は、当該構成設定を行うために必要な最小限度の範囲に限定するものとする。

(ｲ)　(ｱ)に規定する論理的なアクセス権限は、構成設定を安全に実施する能力を有し、かつ、に限り使用させることとする。

ウ　必要最小限度の機能等の設定

保護システム構成要素の構成設定は、当該保護システム構成要素の機能等（ポート、プロトコル及びサービスを含む。）及びプログラムのうち、安全でないもの及び必要不可欠な最小限を超えるものを無効化し、その実行を防止するものとする。

(4)　構成設定の精査

保護システム管理者は、定期的に、及び保護システム構成要素の構成設定を新たに実施した場合など必要と認める場合には、保護システム構成要素の構成設定の状況を精査し、ベースライン構成設定に従っていることを確認するものとする。

(5)　ブラックリスト又はホワイトリストの作成等

ア　保護システム管理者は、ベースライン構成設定に基づき、個別の保護システム構成要素ごとに、ブラックリスト又はホワイトリストを作成するものとする。その際、保護システム管理業務従事者とそれ以外の保護システム利用者で業務上使用するソフトウェアに違いがある場合は、それぞれに向けたリストを作成することができるものする。

イ　保護システム管理者は、ブラックリストを作成した場合は、保護システムが当該ブラックリストに掲載されたソフトウェアをインストール又は実行することが不可能となるように設定するものとする。

ウ　保護システム管理者は、ホワイトリストを作成した場合は、保護システムが当該ホワイトリストに掲載されたソフトウェアのみをインストール及び実行することが可能となるように設定するものとする。

エ　保護システム管理者は、定期的に、及び保護システム構成要素に変更が生じた場合など必要と認める場合には、アに規定するブラックリスト又はイに規定するホワイトリストを精査し、必要に応じ、当該リストを更新するものとする。

3　ベースライン構成設定等の変更等

(1)　保護システム管理者は、保護システム構成要素に係る脆弱性の発見及び修正並びに業務上必要な機能の変化等が生じた場合には、総括者の承認を得て、ベースライン構成設定を変更するものとする。

(2)　保護システム管理者は、個々の保護システム構成要素において、ベースライン構成設定に従うことが不可能又は著しく合理性を欠く等の事情があると認めた場合に、総括者の承認を得て、特別の構成設定を行うものとする。

(3)　保護システム管理者は、第１号の規定によりベースライン構成設定を変更する場合及び前号の規定により特別の構成設定を行う場合は、当該構成設定が保護システムのセキュリティに及ぼす影響を分析した上で、実施するものとする。

4　構成設定に係る記録及び保存等

(1)　構成設定目録

ア　目録の作成

(ｱ)　保護システム管理者は、保護システム構成要素の構成設定に係る現状を正確に確認及び証明するための目録（以下「構成設定目録」とい

う。）を作成するものとする。

(ｲ)　構成設定目録には、個々の保護システム構成要素ごとに、保護システム管理者が指定した構成設定に責任を有する者の氏名、連絡先等を明記するものとする。

イ　目録の更新

(ｱ)　保護システム管理者は、保護システム構成要素の構成設定の現状に変化が生じた場合（保護システムにおけるソフトウェアのインストール及びアップデートを行った場合を含む。）は、構成設定目録を更新するものとする。

(ｲ)　構成設定目録の内容を定期的に精査し、現状が正確に記載されていない場合は、速やかに目録を更新するものとする。

(2)　構成設定に係る記録

保護システム管理者は、ベースライン構成設定の決定及び変更並びに保護システム構成要素構成設定の実施を記録した文書を作成するものとする。

(3)　目録等の保存等

防衛関連企業は、構成設定目録及び前号により作成した文書を、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存するものとする。

第４　保護システムの基本的防御

１　保護システムの領域の確定

防衛関連企業は、保護システム（保護すべき情報の保存又は当該情報へのアクセスを可能とする機器に限る。以下同じ。）における保護すべき情報を取り扱う領域を定め、イントラネット及び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ものとする。

２　保護システムの操作手順書の策定

(1)　保護システム管理者は、保護システム利用者による不適切な操作がセキュリティに悪影響を及ぼすことを防ぐため、保護システムの利用に当たっての手順及びセキュリティ上遵守すべき事項等を明記した操作手順書を作成し、総括者の承認を得るものとする。

(2)　前号に規定する操作手順書は、保護システム利用者が保護システムを使用する際に参照することができる状態にするものとする。

３　保護すべきデータの暗号化

(1)　暗号化

ア　防衛関連企業が保護システムに保護すべきデータを保存する場合は、当該データの機密性及び完全性を維持するため、当該データを暗号化するものとする。

イ　保護すべきデータを可搬記憶媒体に保存する場合は、当該データの機密性及び完全性を維持するため、当該データを暗号化するものとする。ただし、別に防衛省の指示がある場合には、その指示に従うものとする。

(2)　暗号化の方法

防衛関連企業が保護すべきデータの暗号化など保護システムにおいて使用する暗号は、電子政府推奨暗号等を使用するものとする。ただし、別に防衛省が指示する暗号がある場合は、その指示に従うものとする。

(3)　暗号鍵の管理

防衛関連企業は、前号に規定する暗号の暗号鍵を、自社の管理要領により厳格に管理するものとする。

4　その他

(1)　ソフトウェアのインストール及びアップデートの制限等

ア　防衛関連企業が保護システムにおいてソフトウェアのインストール又はアップデートを行う場合は、保護システム管理者は、あらかじめその有効性や副作用の可能性等を分析及び評価し、必要かつセキュリティ上適切と認められる場合に限り実施するものとする。

イ　アに規定する分析及び評価によりソフトウェアのアップデート（パッチ及びアンチウイルスシグネチャを含む。）を実施することが必要かつセキュリティ上適切と認めた場合は、当該ソフトウェアのアップデートが利用可能となってから速やかに実施するものとする。

(2)　管理者用機能と利用者用機能の分離

保護システム管理者は、保護システムにおけるアプリケーション等の機能は、管理者用機能と利用者用機能を分離するものとする。

(3)　管理者用機能の不正利用防止

保護システム管理者は、管理者権限を持たない保護システム利用者による管理者用機能の不正利用を防ぐため、アクセス制限や構成設定の実施などの対策を講じるものとする。

(4)　仮想化技術の利用時の対策

保護システム管理者は、保護システムを構成するハードウェア又はソフトウェアにおいて、仮想化技術を利用して複数の仮想コンピュータを構築する場合は、当該仮想コンピュータ間でデータの不正な又は意図しない移動を防止する対策を講じるものとする。

(5)　外部システムとの接続制限

保護システム管理者は、保護システムを外部システムと接続する場合は、当該接続及びその使用に係る安全性を検証し、保護システムと外部システムとの接続及びその使用を管理又は制限するものとする。

第５　アクセス制御

１　アクセス制御方針

(1)　防衛関連企業は、保護すべきデータ及び保護システムに対する論理的なアクセス（保護システムへのログオン及び保護システムの個々の機能へのアクセスを含む。以下同じ。）の制御を実施するために必要な措置を定めたアクセス制御方針を作成するものとする。

(2)　アクセス制御方針は、保護システム管理者が作成し、総括者の承認を得るものとし、作成に当たっては、保護すべきデータ及び保護システムに対する論理的なアクセス権を有する者を業務の遂行上必要最小限度となるように定めるものとする。

(3)　保護システム管理者は、アクセス制御方針を定期的に、及び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するものとし、修正した場合は前号により総括者の承認を得るものとする。

２　アクセス制御方針に基づく管理策

防衛関連企業は、アクセス制御方針に基づき、以下の管理策を行うものとする。

(1)　アカウントの管理

ア　保護システム管理者は、保護システムへ論理的にアクセスするための権利（以下「アカウント」という。）について、保護システム担当者のうち、アカウントの設定、変更、削除等（以下「アカウントの管理」という。）を行う者としてふさわしい者（以下「アカウント管理者」という。）をアカウント管理者に指定するものとする。

イ　アカウント管理者は、業務の遂行上必要最小限度の機能及び権限となるよう、アカウントの管理を計画し、保護システム管理者の承認を得て実施するものとする。その際、保護システム管理者、保護システム担当者、その他の者ごとに適切なアカウントの範囲を区別し、付与する者は必要最小限度に制限するものとする。

ウ　アカウント管理者は、保護システム利用者ごとにアカウントの管理を実施するものとし、アカウントの利用状況（利用者名及び利用開始日時）を記録するものとする。

エ　保護システム利用者の退職、異動及び職務内容の変更などの事由がある場合は、当該保護システム利用者のアクセス権限を変更又は失効させるものとし、アカウント管理者は、事由の発生から定められた時間内に保護システム管理者の承認を得て必要なアカウントの管理を行うものとする。なお、これにより難い場合には、当該時間以内に、アクセス権の失効のみ実施するものとする。

オ　エの規定により保護システム利用者のアクセス権限を変更又は失効させる場合は、アカウント管理者は、次に掲げる措置を講じるものとする。

(ｱ)　保護システム利用者の失効するアクセス権限に関連する識別子（アカウントにあってはユーザＩＤをいい、保護システムを構成する機器にあってはホスト名等をいう。以下同じ。）及び認証子を無効化させること。

(ｲ)　当該保護システム利用者の失効するアクセス権限に関連する鍵、ＩＤカード等証明証及びトークン等に加え、保護システムの操作手順書等を返納させること。

(ｳ)　アカウント失効日時等の記録を行うこと。

カ　保護システム管理者及び保護システム担当者が使用するアカウントなど管理者権限の一部を付与されたアカウントについては、当該権限を使用する必要がある場合にのみ使用させるものとする。

(2)　ログオンの管理

ア　ログオン試行保護システム管理者は、保護システムへのログオン試行時に連続して失敗できる上限を定め、それを超えた場合には、当該ログオン試行を行ったアカウントを自動的にロックし、当該ロック時から定められた時間が経過するまで保護システムに対するログオンの再試行が行えないよう設定するものとする。

イ　保護システム利用者が保護システムにログオン試行を行う場合は、パソコンの画面上に不正なログオン試行に有用な情報を表示させないものとする。

(3)　ユーザセッションの管理

保護システム管理者は、保護システムにログオンした保護システム利用者のユーザセッションについて、次に掲げる方法により管理を行うものとする。

ア　非アクティブ状態であり続ける時間の上限を設定し、それを超えた場合は、当該ユーザセッションをロックすること。

イ　保護システム利用者が保護システムの置かれた席から離席する際には、当該ユーザセッションをロックさせること。

ウ　当該ユーザセッションをロックした場合の不正なアクセス及びデータの閲覧等を防止するため、パソコンのディスプレイの全面をスクリーンセーバ等により保護すること。

エ　当該ユーザセッションのロックを解除するために、保護システム利用者に対し、第６第１項第２号アに規定する多要素認証を行わせること。

オ　保護システム利用者が、保護システム上でログオフを要求した場合は、自動的に当該ユーザセッションを終了させること。

カ　当該ユーザセッションを終了させる場合には、保護システム利用者が継続実行を設定した計算処理プログラム等を除き、すべてのソフトウェアプログラムを終了させること。

(4)　リモートアクセスの管理

ア　保護システム管理者は、保護システムへのリモートアクセスの利用を業務の遂行上必要最小限度に制限するとともに、事前に承認するものとする。

イ　アの規定によりリモートアクセスを利用する場合は、当該アクセスを通じた通信を適切に保護するため、保護システム管理者は、次に掲げる措置を実施するものとする。

(ｱ)　保護システムへのリモートアクセスに係る通信を暗号化すること。

(ｲ)　リモートアクセス等を受ける保護システムの境界（プロキシサーバ及びバーチャル・プライベート・ネットワーク（ＶＰＮ）サーバ等をいう。）を必要最小限度に制限すること。

(ｳ)　保護システムへのリモートアクセスを利用している場合は、同時に当該リモートアクセスに利用するものとは異なる通信経路を利用しないこと。

ウ　保護システムへのリモートアクセスを利用している際の管理者権限の使用は、事前に保護システム管理者が承認した場合を除き、禁止するものとする。

第６　識別及び認証

防衛関連企業は、保護システムにおける識別及び認証について、アクセス制御方針に基づき、以下の管理策を行うものとする。

１　識別及び認証等の実施

(1)　識別の実施

ア　保護システム管理者は、アカウント及び保護システムを構成する機器（サーバ、パソコン及び周辺機器を含む。ウにおいて同じ。）に対し、識別可能な識別子を付与し、保護システム管理者が承認をするものとする。

イ　アに規定する識別子を当該保護システムにおいて有効化する場合は、機密性に配慮した方法で設定するものとする。

ウ　アに規定する識別子を他のアカウント及び保護システムを構成する機器に

対し再使用してはならない。ただし、当該識別子の使用を終えた日から定められた期間を経過した場合にはこの限りでない。

エ　アに規定する識別子が保護システムにおいて定められた期間以上使用されなかった場合は、当該識別子を無効化するものとする。

オ　保護システム利用者の代理として動作するプロセスを識別するものとする。

(2)　認証の実施

ア　保護システム管理者は、保護システム利用者が第５第２項第１号の規定により付与されたアカウントで保護システムにログオンする場合は、本人だけが知る要素（以下「知識要素」という。）、本人だけが所有する要素（以下「所持要素」という。）及び本人の持つ生体的要素（以下「生体要素」という。）のうち複数の異なる要素を保持すると認められた者のみを許可（以下「多要素認証」という。）するものとする。

イ　保護システム利用者が保護システムに対し、リモートアクセスによりログオンする場合は、アに規定する多要素認証をリプレイ攻撃に耐性のある方式で行うものとする。

ウ　アに規定するログオンを認証する場合は、当該ログオンに使用される機器が、前号アの規定により識別子を付与された機器であることを識別するものとする。

エ　保護システム利用者の代理として動作するプロセスが保護システムに対しアクセスする場合は、当該プロセスが前号オの規定により識別されたプロセスであることを認証するものとする。

(3)　パスワードによる認証の実施

ア　保護システム管理者は、第１号アに規定するアカウントのユーザＩＤに係る初期パスワードを保護システム利用者に割り当てる場合は、容易に推測されず、かつ、アカウントごとに異なるパスワードを割り当てるものとする。

イ　アに規定する初期パスワードを保護システム利用者に配布する場合は、機密性に配慮した方法により行うものとする。

ウ　保護システム利用者が初期パスワードを使用した認証により保護システムにログオンした場合は、直ちに当該パスワードを変更させるものとする。

エ　保護システム利用者が作成又は変更するアカウントのユーザＩＤに係るパスワードは、次に掲げる要件を満たすものとする。

(ｱ)　大文字英字、小文字英字、数字及び特殊文字のうち３種類以上使用した１０文字以上であり、容易に推測されないものであること。

(ｲ)　紙等への記載又は記憶媒体への保存（オに規定する場合を除く。）が行われていないこと。

(ｳ)　定められた期間以内に変更すること。

(ｴ)　世代にわたって同じパスワードを使用しないこと。

(ｵ)　紙等への記載又は記憶媒体への保存（オに規定する場合を除く。）が行われていないこと。

オ　保護システムへのログオンに使用されるパスワードを認証するため、当該保護システム内において保存又は伝送する必要があるパスワード情報

は、他の者が容易に複合できない方式を用いて保存又は伝送するものとする。

カ　保護システム利用者が作成したパスワードを忘失した場合は、当該パスワードを無効化するとともに、当該保護システム利用者に対し、アの規定により初期のパスワードを配布するものとする。

2　識別及び認証におけるその他の留意事項

(1)　保護システム管理者は、その他の認証子による認証について、適切な機器等（ＩＤカード、ＩＤカードリーダー、トークン及び生体認証機器を含む。以下同じ。）を使用することにより、十分な強度を確保するものとする。

(2)　保護システム管理者は、前号に規定する機器等は、不正なアクセス等から保護するため、厳格に管理するものとする。

(3)　保護システム管理者は、第１号に規定する機器等を紛失又は破損等により交換する場合は、保護システムにおいて、当該機器等による認証を無効化するものとする。

第７　通信制御

1　通信の制御

(1)　防衛関連企業が保護システムと外部ネットワークとの通信を行う場合は、プロキシサーバ、インターフェイス（ゲートウェイ、ルーター及びファイアウォール等）を設置し、必ず当該機器を経由する通信を行うものとし、当該機器は許可された通信以外は拒否するよう設定するものとする。

(2)　インターネットなど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は、当該ウェブサーバ等を含むサブネットワークを設置するものとし、リモートアクセスを実施する場合には、リモートアクセスを管理するインターフェイスを設置するものとする。

2　通信データ及び通信セッションの保護

(1)　保護すべき情報の通信制限

ア　防衛関連企業が保護すべきデータの通信を行う場合は、セキュリティが確保され、かつ、業務の遂行上必要最小限度の範囲に制限するものとし、防衛省からの許可を得た場合を除き、保護システム以外の情報システムとの間における保護すべきデータの通信を行わないものとする。

イ　保護すべきデータの通信を行う場合は、第４第３項第１号の規定により暗号化されたデータにより行うか、当該データを転送する通信経路を暗号化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、送配線（有線）等により通信が行われる場合は、この限りでない。

(2)　通信セッションの保護

ア　保護システムを利用した通信のセッションの終了時又は当該セッションが非アクティブ状態で定められた期間を経過した場合は、当該セッションに関連するネットワーク接続を全て終了させるものとする。

イ　保護システムと外部ネットワークにおける通信のセッションにおいては、なりすましによる攻撃等を防止するため、電子証明書等の方法により、通信先が意図した相手であることを確保するものとする。

3　通信機能の利用制限

(1)　モバイルコード

ア　保護システム管理者は、モバイルコードが悪意のある者により利用されたときの保護システムに与える被害を考慮し、保護システムにおける利用の要件を定めるものとする。

イ　保護システムにおけるモバイルコードの利用は、アに規定する利用の要件を満たす場合に限り許可することとし、当該許可については、保護システム管理者が承認をするものとする。

(2)　ＩＰネットワークによる音声伝達技術（以下「ＶｏＩＰ技術」という。）

ア　保護システム管理者は、ＶｏＩＰ技術が悪意のある者により利用された場合の保護システムに与える被害を考慮(通話内容の改ざん及び漏えい等を防ぐための通信経路の暗号化を含む。)した、保護システムにおける利用の要件を定めるものとする。

イ　保護システム管理者は、保護システムにおけるＶｏＩＰ技術は、アに規定する利用の要件を満たす場合に限り許可することとし、当該許可に当たっては、保護システム管理者が承認をするものとする。

(3)　オフィス機器

ア　保護システム管理者は、保護システムに接続された電子ホワイトボード、ネットワークカメラ等の各種のオフィス機器等が悪意のある者により利用された場合の保護システムに与える被害を考慮し、次に掲げる事項を含めた保護システムにおける利用要件を定めるものとする。

(ｱ)　当該機器に対するリモートアクセスによる起動及び操作を禁止すること。

(ｲ)　当該機器が起動している場合には、外形的に明らかな表示を行うこと。

イ　保護システム管理者は、保護システムに接続されたオフィス機器等の利用は、当該利用の都度、アに規定する利用の要件を満たす場合に限り許可することとし、当該許可に当たっては、保護システム管理者が承認をするものとする。

第８　システム監視

１　システム監視の実施

防衛関連企業は、保護システムにおける不正なアクセス及び変更、アカウント及び権限の不正な使用、不正な通信並びに悪意のあるコード等（以下「不正なアクセス等」という。）の検知に必要な情報の収集を行うための機器の設置、ソフトウェアのインストール等を実施し、次に掲げる事項について保護システムの内部及び外部境界に対する監視（以下「システム監視」という。）を実施するものとする。

(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

２　システム監視の実施方法

(1)　システム監視の実施に係る共通事項

ア　防衛関連企業がシステム監視を実施する場合は、システム上の挙動を常時監視するとともに、第９第１項の規定により作成されたシステムログの分析

結果を利用するものとする。

イ　システム監視により不正なアクセス等を検知した場合は、保護システム管理者及び保護システム担当者にアラートが発せられるよう、保護システムを設定するものとする。

ウ　保護システムに対する不正なアクセス等のリスクの増大又はその兆候等が認められる場合には、必要に応じ、システム監視のレベルを引き上げるものとする。

(2)　システム及び通信の監視方法

ア　防衛関連企業が第１項第３号に掲げる不正な通信に対するシステム監視を実施する場合は、次に掲げる事項に対する常時監視を行うものとする。

(ｱ)　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

(ｲ)　不正なローカル接続、ネットワーク接続、リモート接続及びリモートアクセス

イ　悪意のあるコードの検知

(ｱ)　第１項第４号に掲げる悪意のあるコードの侵入の監視は、保護システムを構成するサーバ及びパソコンにおける悪意のあるコードを検知するためのソフトウェア（以下「検知ソフトウェア」という。）として、ウイルス定義を用いたパターンマッチング手法のほか、未知の脅威に対応するための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をインストールするものとする。

(ｲ)　ウイルス定義及び検知ソフトウェアのアップデート版が提供された場合において、第４第４項第１号に規定する分析及び評価によりそれらのアップデートを実施することが必要かつ適切と認められるときは、速やかにアップデートを行うものとする。

(ｳ)　悪意のあるコードを検知するため、保護システムに対する検知ソフトウェアによるフルスキャンを定期的に実施するものとする。なお、一定の期間以上電源の切断された状態にあるサーバ又はパソコン等については、再度の電源投入時に当該処置を実施するものとする。

(ｴ)　検知ソフトウェアにより、保護システムにおけるファイルのダウンロード、開封及び実行等の都度、当該ファイルに対し、悪意のあるコードを検知するためのリアルタイムスキャンを実施するものとする。

３　不正なアクセス等を検知した際の対応

保護システム管理者が第２項第１号イに規定するアラートを受けた場合又は検知ソフトウェアにより悪意のあるコードを検知した場合は、検知ソフトウェアによる誤検知の可能性を検証し、その結果を踏まえ、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、隔離若しくは削除又はそれらを適切に組み合わせた措置を実施するものとする。

４　システム監視により取得した情報の利用及び保管

(1)　防衛関連企業は、システム監視により取得した情報を情報セキュリティ事故等への対処などに利用するものとし、保護システム管理者は、取得した情報を関係部署等に通知するものとする。

(2)　システム監視により取得した情報に対する不正なアクセス、改ざん及び消去等を防ぐため、当該取得した情報は、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管

又は保存するものとする。

第９　システムログ

１　システムログの取得及び分析

(1)　システムログの取得

ア　防衛関連企業は、保護システムにおける不正な操作や通信を探知するため、次に掲げる事項に係る記録をシステム上で自動的に取得するものとする。

(ｱ)　保護すべきデータへの動作の内容

(ｲ)　保護システム利用者ごとの操作内容

イ　保護システム担当者はアに規定するシステムログのほか、保護システムにおける不正な操作や通信を探知するために必要となるシステムログの内容並びにその取得に係る対象及び方法を決定し、保護システム管理者の承認を得るものとする。

ウ　ア及びイに規定するシステムログの内容並びにその取得に係る対象及び方法は、保護システムにおいて取得可能であることを事前に検証するものとし、生成困難である場合は、当該保護システムにおいて実施可能な監視手法の再設計を検討するものとする。

エ　システムエラー等によりシステムログの取得に失敗する場合に備え、当該失敗の影響の低減及び復旧等に係る対策をあらかじめ定めるものとし、取得に失敗した場合は、保護システム担当者等必要な者に対しアラートを発するとともに、ウに規定するの措置を行うものとする。

オ　ア及びイに規定するシステムログの内容並びにその取得に係る対象及び方法は、定期的に精査し、必要に応じて変更するものとする。

(2)　システムログの分析

ア　保護システム管理者は、定期的にシステムログの分析を実施するものとし、分析を行う場合は、保護システム構成要素から取得したシステムログを集約し、全体的かつ横断的な分析を行うものとする。

イ　システムログの分析の方法は、次に掲げる要件を考慮して選択し、保護システム管理者の承認を得るものとする。

(ｱ)　異常と認められる状況の発見に資すること。

(ｲ)　過去の情報セキュリティ事故等との類似性等の発見に資すること。

ウ　システムログの分析及び分析結果の報告をサポートするため、保護システムに報告書生成機能を持たせるものとする。

エ　システムログの分析を行った場合は、その結果を記録した文書を作成し、速やかに総括者及び保護システム管理者その他必要な者に報告するものとする。

オ　エに規定するシステムログの分析に係る結果を記録した文書の作成においては、システムログの内容（時刻の順序を含む。）を変更しないものとする。

２　システムログの管理

(1)　保護システム管理者は、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に必要なアクセス権限を、必要な者に限定して付与するものとする。

(2)　システムログ及びその分析の結果の記録は、文書等の場合は、施錠したロッカー等により、電子データを保護システムに保存する場合は、保護システム管理者及び保護システム担当者以外にアクセスされないよう設定することにより、必要な期間保存又は保管するものとする。

(3)　保護システム管理者は、前号の規定により保存又は保管しているシステムログについて、定期的に改ざん又は削除等が行われていないか確認するものとする。

3　システムログに付与するタイムスタンプ

(1)　保護システム管理者は、システムログに対し、保護システムの内部におけるシステムクロックを使用して、タイムスタンプを付与するものとする。

(2)　システムログのタイムスタンプは、日本標準時（ＪＳＴ）を基準とした時刻表記で統一するものとする。これにより難い場合は、協定世界時（ＵＴＣ）又はグリニッジ標準時（GMT）を基準とした時刻表記で統一するものとする。

(3)　タイムスタンプに使用するシステムクロックの同期は、保護システムに外部の権威ある機関が運営するＮＴＰサーバ等から得られる日付及び時刻と同期する機能を持たせるものとする。

4　システムログを取得するツールの保護

保護システム管理者は、システムログを取得するツールを、不正なアクセス、改ざん又は削除から保護するものとする。

第１０　脆弱性スキャン等

１　脆弱性スキャンの実施

(1)　保護システム管理者は、保護システム全体に対する脆弱性スキャンを定期的に行い、その結果を分析するものとする。

(2)　保護システム管理者は、社内からの脆弱性情報に加え、情報セキュリティに係る専門的な外部機関（以下「情報セキュリティ機関」という。）が発信する脆弱性情報等セキュリティに係る注意喚起及び助言等の情報を継続的に収集するものとし、当該脆弱性が保護システムに対し影響を与える可能性があると認められる場合に、保護システム全体に対し当該脆弱性に係る脆弱性スキャンを実施し、その結果を分析するものとする。

(3)　保護システム管理者は、前２号による分析の結果を記載した文書を作成するものとし、脆弱性が特定された場合は、本基準第１１第１項第４号及び第２項第１号の措置を行うものとする。

２　分析結果等の利用

(1)　保護システム管理者は、自社における保護システム以外の情報システムにおける脆弱性の発見及び修正等に資するため、脆弱性スキャン結果の分析など脆弱性発見に資する情報を自社の必要な者及び組織に共有するものとする。

(2)　保護システム管理者は、社内又は前項第２号の情報セキュリティ機関から収集した情報に基づき、保護システム担当者、保護システム利用者（保護システムを利用する中小受託事業者を含む。）等に対し、適切なセキュリティに係る注意喚起及び助言等を行うものとする。

(3)　保護システム管理者は、前２号により脆弱性が特定された場合は、定められた時間内に特定された脆弱性を修正するものする。

第１１　バックアップ

１　保護システム管理者は、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（防衛省が提供した保護すべきデータを除く。）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を行うものとする。

２　前項の規定によりバックアップされたデータは、少なくとも次回のバックアップの完了まで保存するものとする。

３　バックアップは、自社が定めた保護システムの目標復旧時間に応じた頻度で行うものとする。

４　保護システム管理者は、第１項の規定によりバックアップされたデータの機密性、完全性及び可用性を保護するものとする。

５　保護システム管理者は、バックアップに関する手順を定めるものとする。

第１２　システムメンテナンス等

１　システムメンテナンス等の計画

(1)　保護システム管理者は、保護システムのメンテナンス等（保守、点検、診断、修理、整備及びアップグレードを含む。以下同じ。）を定期的に、及び必要な場合にはその都度行うものとする。

(2)　保護システム管理者は、次に掲げる事項を定めた計画（以下「システムメンテナンス等計画」という。）を管理責任者と調整の上作成し、総括者の承認を得るものとする。

ア　メンテナンス等を実施する人員

イ　メンテナンス等の対象（保護システムにおけるソフトウェア、ハードウェア及びファームウェアを含む。）

ウ　メンテナンス等の内容（メンテナンス等に使用される機器及びツールを含む。）

エ　アからウまでに掲げるほか、第２項及び第３項に規定する措置を実施するために必要な事項

(3)　保護システムを取り外す場合、取扱施設の外に持ち出す必要がある場合又は保護システム等に対しネットワークを経由したメンテナンス等（以下「リモートメンテナンス等」という。）を実施する必要がある場合は、保護システム管理者は、前号による承認を得るとともに、あらかじめ当該保護システム等に記録された保護すべき情報を削除又は移動させるなど必要な措置を講じ、システムテナンス等計画にその旨を記載するものとする。

２　システムメンテナンス等の実施

保護システム管理者は、システムメンテナンス等計画に従って、保護システムのメンテナンス等を実施するものとする。

(1)　人員の指定

ア　保護システム管理者は、保護システムのメンテナンス等を実施することができる人員を保護システム利用者のうちから業務の遂行上必要最小限度に制限したうえで、指定するものとする。

イ　保護システム利用者以外の者によるメンテナンス等を実施する必要がある場合は、保護システム管理者が前項第２号による承認を得て実施させる

」

ものとし、メンテナンス等の完了後、直ちに当該人員による保護システム及び取扱施設へのアクセスを含むメンテナンス等への関与を終了させるものとする。

(2)　ツールの検査

保護システムのメンテナンス等の実施に当たっては、保護システム管理者が承認した適切な検査されたツール（診断ツールやテストプログラムが保存された記憶媒体を含む。）のみを使用させるものとする。

(3)　システムへのアクセスの認証等

ア　保護システムのメンテナンス等を実施する人員が保護システムにアクセスする必要がある場合は、当該人員に対し多要素認証を求めるものとする。

イ　保護システムのメンテナンス等に使用する機器は、システムメンテナンス等計画に記載された機器と同一であることを識別するものとする。

(4)　システムメンテナンス等の監督等

ア　保護システムのメンテナンス等を実施する場合は、保護システム管理者は保護システム利用者の中から技術的な知見を有する者を監督者として指定し、監督結果を管理責任者及び保護システム管理者に速やかに報告させるものとする。

イ　アにより指名された監督者は、保護システムのメンテナンス等を実施する者とともに現場に所在（リモートメンテナンス等の場合はネットワークを経由）して、メンテナンス等の実施状況を監督するものとする。

ウ　システムメンテナンス等の実施状況の監督に当たっては、第９に規定するシステムログの取得及び分析を実施するものとする。

(5)　保護システム管理者は、保護システムのメンテナンス等を実施する前に、メンテナンス等により影響を受けることが予測される事象についてのセキュリティ対策を実施し、メンテナンス等の終了後、当該セキュリティ対策がメンテナンス等の実施前と同様に適切に機能していることを確認するものとする。

３　システムメンテナンス等の記録

(1)　前項第４号アにより指定された監督者は、メンテナンス等を実施した日時、事業者の名称及び所在、人員の名簿（国籍等を記載）、実施の対象及び内容等の記録を文書により作成し、管理責任者及び保護システム管理者の確認を得るものとする。

(2)　前号に規定するシステムメンテナンス等の結果を記録した文書を、文書により保存する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存するものとする。