入　札　公　告

本入札に係る落札及び契約締結は、当該業務に係る令和６年度本予算が成立し、予算示達がなされることを条件とするものである。

次のとおり一般競争入札に付します。
なお、本件は、電子調達システム（政府電子調達（GEPS））対象案件である。

令和６年２月９日

支出負担行為担当官
九州防衛局長　江　原　　康　雄
（公印省略）

１　開札日時：令和６年３月１日（金）１１時００分

２　開札場所：〒812-0013　福岡県福岡市博多区博多駅東２丁目 10 番７号
福岡第二合同庁舎　九州防衛局　５階会議室

３　入札に付する事項：
（１）件　　名：九州防衛局ＯＡネットワーク・システムの運用支援役務
（２）契約内容：仕様書のとおり
（３）契約期間：令和６年４月１日（月）から令和７年３月３１日（月）

４　参加資格：
（１）予算決算及び会計令（昭和 22 年勅令第 165 号。以下「予決令」という。）第 70 条及び第 71 条の規定に該当しない者であること。
なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。
（２）令和4・5・6年度全省庁統一資格のうち、「役務の提供等」で「Ｄ」の等級以上に格付され、九州・沖縄地域の競争参加資格を有し、責任をもって履行できる者であること。
（３）適合条件（Ⅰ　セキュリティ関連：Ｐマーク（個人情報）、JISQ27001 若しくは ISO/IEC27001（情報セキュリティ保護）Ⅱ　マネジメント関連：

JISQ9001若しくはISO9001(業務品質管理))を満たす証明書類を提出し、確認を得た者であること。

資料提出期限：令和６年２月２０日（火）正午まで。

（４）防衛省から指名停止の措置を受けている期間中の者でないこと。

（５）暴力団関係業者の排除

ア 都道府県警察から暴力団関係業者として防衛省が発注する工事等から排除するように要請があり、当該状態が継続している有資格業者については、競争参加を認めない。

イ 入札後、契約を締結するまでの間に、都道府県警察から暴力団関係業者として防衛省が発注する工事等から排除するように要請があり、当該状態が継続している有資格業者とは契約を行わない。

（６）入札説明書の交付を受けた者であること。

５　入札方法：

（１）予定価格の制限の範囲内で最低価格をもって有効な入札を行った入札を落札者とする。

（２）落札決定に当たっては、入札書に記載された金額に当該金額の100分の10に相当する額を加算した金額をもって落札価格とするので、入札者は、消費税にかかる課税事業者であるか免税事業者であるかを問わず、見積った契約希望金額の110分の100に相当する金額を入札書に記載すること。

６　入札手続等：

（１）担当部局

〒812-0013　福岡県福岡市博多区博多駅東２丁目10番７号

福岡第二合同庁舎　九州防衛局総務部会計課

（２）本案件は、入札及び資料提出等を電子調達システム（政府電子調達（ＧＥＰＳ）（以下「電子調達システム」という。））で行う案件である。

ただし、電子調達システムにより難い場合は、発注者の承諾を得て紙入札方式に代えるものとする。

なお、紙入札方式の承諾に関しては、九州防衛局総務部会計課へ紙入札方式参加承諾願を提出するものとする。

（３）入札説明書等の交付場所

電子調達システム（電子調達システムURL：https://www.geps.go.jp）より、電子データで交付又は（１）において交付する。

（４）入札説明書等の交付期間

ア 電子調達システムは、公告の日から令和６年２月29日（木）正午まで。

イ 紙入札方式は、公告の日から令和６年２月29日（木）までの平日10時から17時まで。（正午から13時までの間を除く。）ただし、最終日は正午まで。

（５）競争参加資格確認書類の提出

ア 上記４（２）を確認する書類の写しを電子調達システムにより提出すること。ただし、紙入札方式の承諾を得た場合は（１）に持参又は郵送すること。

イ 提出期限は、令和６年２月29日（木）正午まで。なお、紙入札方式による持参の場合は、平日10時から17時まで。（正午から13時までの間を除く。）ただし、最終日は正午まで。郵送の場合は、提出期限までに必着とする。

（６）入札書の提出及び提出期間

ア 入札書の提出は、電子調達システムにより行うこと。ただし、紙入札方式の承諾を得た場合は紙により（１）に持参又は郵送すること。

イ 入札書の提出期限は、令和６年２月29日（木）17時まで。

なお、紙入札方式による持参の場合は、平日10時から17時まで。（正午から13時までの間を除く。）郵送の場合は、提出期限までに必着とする。

７　入札保証金及び契約保証金：免 除

８　入札の無効：４の参加資格のない者の入札及び入札に関する条件に違反した入札は無効とする。

９　契約書作成の要否：要

10　適用する契約条項：役務契約書

装備品等及び役務の調達における情報セキュリティの確保に関する特約条項

情報システムの調達に係るサプライチェーン・リスク対応に関する特約条項

個人情報の取扱いに関する特約条項

談合等の不正行為に関する特約条項

暴力団排除に関する特約条項

11　その他：

（１）端数処理：入札書に記載された金額の100分の10に相当する金額に１円未

満の端数があるときは、その端数を切り捨てるものとし、当該端数処理を切り捨てた後に得られる金額をもって、申込があったものとする。

（２）手続きにおいて使用する言語及び通貨：日本語及び日本国通貨に限る。

（３）詳細は、入札説明書による。

（４）電子調達システムの問い合わせ先：https://www.geps.go.jp

（５）電子調達システムにおいて、システム障害が発生した場合には、日時及び入札方法等を変更する場合がある。

（６）落札者が、１０に掲げる契約条項のほか、中小企業信用保険法第２条第１項に規定する中小企業者である場合は、「債権譲渡制限特約の部分的解除のための特約条項」を別途適用する。

（７）契約締結までに令和６年度の予算（暫定予算含む。）が成立しなかった場合は、契約締結日は予算が成立した日以降とする。また、暫定予算になった場合、全体の契約期間に対する暫定予算の期間分のみの契約とする場合がある。

本書記載事項の詳細及び契約書の閲覧については、九州防衛局総務部会計課会計係に照会のこと。（電話：092－483－8812）

入　札　説　明　書

九州防衛局の「九州防衛局ＯＡネットワーク・システムの運用支援役務」に係る入札公告に基づく入札等については、関係法令に定めるもののほか、この入札説明書によるものとする。

なお、本入札に係る落札及び契約締結は、当該業務に係る令和６年度予算が成立し、予算示達がなされることを条件とするものである。

１　公　告　日：令和６年２月９日（金）

２　契約担当官等：支出負担行為担当官
九州防衛局長　　江原　康雄

３　担 当 部 局：
入札・契約に関すること
〒812－0013
福岡県福岡市博多区博多駅東２丁目 10 番７号
福岡第二合同庁舎
九州防衛局　総務部　会計課　会計係
℡：092－483－8812（内線：335）

仕様書等に関すること
九州防衛局　総務部　総務課　企画係
℡：092－483－8811（内線：316）

４　履 行 内 容 等：
（１）件　　名：九州防衛局ＯＡネットワーク・システムの運用支援役務
（２）契約内容：別添仕様書のとおり
（３）契約期間：令和６年４月１日（月）から令和７年３月 31 日（月）

５　電子調達システムの利用について：
（１）本件は、入札及び資料提出等を電子調達システム（政府電子調達（ＧＥＰＳ）（以下「電子調達システム」という。））で行う案件である。電子調達システムによる場合は、電子認証（ＩＣカード）を取得していること。

なお、電子調達システムによりがたい場合は、別紙様式「紙入札方式参加承諾願」を提出し、発注者の承諾を得ることで紙入札方式に代えるものとする。

（２）紙入札方式参加承諾願の提出

ア 提出期間：公告の日から令和６年２月 20 日（火）正午まで。
なお、持参の場合は、上記期間の土日祝祭日を除く毎日 10 時から 17 時まで。（正午から 13 時までの間を除く。）ただし、最終日は正午まで。

イ 提出場所：上記３に同じ。

ウ 提出方法:持参又は郵送によるものとし､電送によるものは受け付けない。
なお、郵送による場合は、提出期限までに必着とする。

（３）電子調達システムで使用できるＩＣカードは、代表者又は当該入札案件に関する入札･見積権限及び契約締結権限について委任を受けた者のＩＣカードのみである。

（４）電子調達システムにより提出する資料が３MB を超える場合、各資料の提出期間内に持参または郵送をするものとし､電子調達システムとの分割は認めない。また、持参又は郵送する場合は、次の内容を記載した書面を電子調達システムにより送信する。

・持参又は郵送する資料名
・持参又は発送年月日

６　競争参加資格：

（１）予算決算及び会計令（昭和 22 年勅令第 165 号。以下「予決令」という。）第 70 条及び第 71 条の規定に該当しない者であること。
なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

（２）令和４･５･６年度全省庁統一資格のうち、「役務の提供等」で「Ｄ」の等級以上に格付され、九州・沖縄地域の競争参加資格を有し、責任をもって履行できる者であること。

（３）適合条件（Ⅰ　セキュリティ関連：Ｐマーク（個人情報）、JISQ27001 若しくは ISO/IEC27001（情報セキュリティ保護）Ⅱ　マネジメント関連：JISQ9001 若しくは ISO9001(業務品質管理))を満たす証明書類を提出し、確認を得た者であること。

（４）防衛省から指名停止の措置を受けている期間中の者でないこと。

（５）暴力団関係業者の排除

ア　都道府県警察から暴力団関係業者として防衛省が発注する工事等から

排除するように要請があり、当該状態が継続している有資格業者については、競争参加を認めない。

イ　入札後、契約を締結するまでの間に、都道府県警察から暴力団関係業者として防衛省が発注する工事等から排除するように要請があり、当該状態が継続している有資格業者とは契約を行わない。

（６）入札説明書の交付を受けた者であること。

７　仕様書等に対する質問：

（１）仕様書等に対して質問がある場合には、書面（様式は自由）により、次に従い提出すること。

ア　提出期間は公告の日から令和６年２月 20 日（火）正午まで。

なお、持参の場合は、上記期間の土日祝祭日を除く毎日 10 時から 17 時まで。(正午から 13 時までの間を除く。)ただし、最終日は正午まで。

イ　書面は、持参又は郵送によるものとし、電送によるものは受け付けない。

なお、郵送による場合は、提出期限までに必着とする。

（２）（１）の質問に対する回答書は、次のとおり閲覧に供する。

ア　閲覧期間：令和６年２月９日(金)から令和６年２月 29 日（木）まで。

イ　閲覧場所：上記３に同じ

８　競争参加資格の確認等：

（１）本競争の参加希望者は上記６（２）に掲げる競争参加資格を有することを証明するため、次に従い、競争参加資格書類の写し(以下「書類」という。)を提出すること。

ア　電子調達システムによる場合は、公告日から令和６年２月 29 日（木）正午までに電子調達システムにより提出すること。

イ　紙入札方式による場合は、公告日から令和６年２月 29 日（木）正午までに上記３に持参または郵送すること。

なお、持参の場合は、上記期間の土日祝祭日を除く毎日 10 時から 17 時まで。(正午から 13 時までは除く。)ただし、最終日は正午まで。郵送の場合は提出期限までに必着とする。

（２）競争参加資格の確認は、書類をもって行うものとする。

９　開札：

（１）開札日時及び場所

ア　開札日時：令和６年３月１日（金）11 時 00 分

イ　開札場所：九州防衛局　５階会議室

（２）開札は（１）に掲げる日時及び場所において、入札参加者又はその代理人を立ち会わせて行う。ただし、入札参加者又はその代理人が立ち会わない場合は、入札事務に関係のない職員を立ち会わせて行う。

（３）紙入札方式による入札参加者は、開札に立ち会わない場合でも、その者から提出された入札書は有効なものとして取り扱う。

（４）（３）の場合において、再度の入札を行うこととなった時は、再度の入札への参加の意思の有無を電話により確認するものとする。

（５）第１回目の入札において落札者が決定しなかった場合は、再度入札に移行する。

再度入札の日時については、発注者から再度入札通知書を送付するので、パソコンの前でしばらく待機するものとする。開札処理に時間を要する場合は、発注者から開札状況を電子調達システムにより連絡をする。また、紙入札参加者においては（１）の開札場所にて再度入札の日時等を通知する。

10　入札書の提出方法等：

（１）電子調達システム

ア　提出期限：令和６年２月 29 日（木）17 時まで。

イ　提出方法：電子調達システムにより提出を行う。

（２）紙入札方式

ア　提出期限：令和６年２月 29 日（木）17 時まで。

イ　提出場所：上記３に同じ。

ウ　提出方法：入札書を封筒に入れ封緘し、封筒の表に「入札書在中」と朱書きし、入札件名、開札日時及び会社名を記載し、持参又は郵送等（書留郵便等に限る。）すること。なお、郵送による場合は、提出期限までに必着とする。

（３）落札決定に当たっては、入札書に記載された金額に当該金額の 100 分の 10 に相当する額を加算した金額（金額に１円未満の端数があるときは、その端数を切り捨てた金額）をもって落札価格とするので、入札者は、消費税にかかる課税事業者であるか免税事業者であるかを問わず、見積った契約希望金額の 110 分の 100 に相当する金額を入札書に記載すること。また、別紙入札書内訳も併せて提出するものとする。

（４）入札執行回数は、原則として２回を限度とする。

11　入札保証金及び契約保証金：免　除

12　入札の無効：

（１）次に掲げる入札は無効とする。

ア　本公告において示した競争参加資格のない者のした入札。

イ　本説明書及び入札心得書において示した条件等入札に関する条件に違反した入札。

ウ　入札時点において上記６に掲げる資格のない者のした入札。

（２）（１）の無効の入札を行った者を落札者としていた場合には、落札決定を取り消す。

13　落札者の決定方法：

（１）予定価格の範囲内で、最低価格をもって有効な入札をした者を落札者とする。ただし、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされないおそれがあると認められるとき又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の範囲内の価格をもって入札した他の者のうち最低価格をもって入札した者を落札者とする。

（２）落札となるべき同価の入札をした者が二人以上あるときは、くじへ移行する。くじの実施方法等については、発注者から指示をする。

（３）落札者となるべき者の入札価格が調査基準価格を下回る場合は、低入札価格調査を行うので、落札者となるべき者は、調査に協力をしなければならない。

14　契約書作成の要否等：作成を要する。

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

情報システムの調達に係るサプライチェーン・リスク対応に関する特約条項

個人情報の取扱いに関する特約条項

談合等の不正行為に関する特約条項

暴力団排除に関する特約条項

15　関連情報の窓口：３に同じ。

16　その他：

（１）契約締結日までに令和６年度の予算（暫定予算含む。）が成立しなかった場合は、契約締結日は予算が成立した日以降とする。また、暫定予算

になった場合、全体の契約期間に対する暫定予算の期間分のみの契約とする場合がある。

（２）この一般競争入札に参加を希望する者は、上記６（３）に係る資料の提出及び確認を受けること。公告に記載の提出期限：令和６年２月20日（火）正午までに作成の上、九州防衛局総務部総務課企画係まで郵送、メール又は持参すること。（ＦＡＸは受け付けない。）

（３）契約の手続きにおいて使用する言語及び通貨は、日本語及び日本国通貨に限る。

（４）入札参加者は、入札心得書等を熟読し、入札心得書を遵守すること。

（５）落札者が、１４に掲げる契約条項のほか、中小企業信用保険法第２条第１項に規定する中小企業者である場合は、「債権譲渡制限特約の部分的解除のための特約条項」を別途適用する。

以上

別紙様式

紙入札方式参加承諾願

１．件名：九州防衛局ＯＡネットワーク・システムの運用支援役務

２．電子調達システムでの参加が出来ない理由

上記案件につきましては、電子調達システム対象案件ではありますが、当社においては上記理由により電子調達システムを利用しての入札参加が出来ないため、紙入札方式での参加を承諾いただきますようお願いいたします。

令和　　年　　月　　日

住　　所
商号又は名称
代表者氏名
担当者氏名
連　絡　先

支出負担行為担当官
　九州防衛局長　江原　康雄　　殿

入 札 心 得 書

（目的）

第１条　一般競争（以下「競争」という。）を行う場合における入札その他の取り扱いについては、会計法（昭和22年法律35号）、予算決算及び会計令（昭和22年勅令165号。以下「予決令」という。）、国の物品等又は特定役務の調達手続の特例を定める政令（昭和55年政令300号）、契約事務取扱規則（昭和37年大蔵省令第52号）、国の物品等又は特定役務の調達手続の特例を定める省令（昭和55年大蔵省令第45号）、防衛省所管契約事務取扱細則（平成18年防衛庁訓令第108号）その他の法令に定めるもののほか、この心得書に定めるところによるものとする。

（競争参加の申し出）

第２条　競争に参加しようとする者は、公告、公示又は募集要領（以下「公告等」という。）において指定した期日までに、当該公告等において指定した書類を支出負担行為担当官（会計法第13条第3項に規定する支出負担行為担当官をいう。以下同じ。）に電子調達システムにより提出し、競争参加資格の確認を受けなければならない。ただし、支出負担行為担当官から紙入札での参加の承諾を得た者又は紙入札で参加するよう指示された者（以下「紙入札参加者」という。）は書面により提出することができる。

（入札等）

第３条　仕様書等において同等品による入札参加を認めている場合で、同等品による入札を行おうとする場合には、指示された時期までに支出負担行為担当官へ申請し、承認を得ること。

２　仕様書等において特に指定のない限り、新品による納入とする。

３　入札に参加することができる者（以下「入札参加者」という。）は、支出負担行為担当官から競争参加資格が有ると認められた者又はその代理人のみとする。

４　入札参加者が代理人であるときは、様式１に定める委任状を持参又は郵送（書留郵便に限る。）若しくは託送（書留郵便と同等のものに限る。）（以下「郵送等」という。）等し、入札前までに、支出負担行為担当官に提出しなければならない。ただし、予決令第７１条第１項に該当する者を代理人にとすることはできない。

５　入札参加者又は入札参加者の代理人は、当該入札に対する他の入札参加者の代理をすることができない。

６　入札参加者は、入札説明書、図面、仕様書、契約書案（以下「入札説明書等」という。）を熟覧の上、入札しなければならない。

　なお、入札説明書等に疑義があるときは、入札説明書において指定した期日までに支出負担行為担当官に書面（様式は自由）を持参又は郵送等することにより質問することができる。

７　電子入札参加者は、電子調達システムにおいて入札書を作成し、入札書提出

締切時刻までに、提出しなければならない。また、紙入札参加者は、様式２により入札書を作成し、入札書提出締切時刻までに、公告等において指定した担当部局に提出しなければならない。

８　紙入札参加者は、入札書を郵送等をもって提出することができる。この場合においては、二重封筒とし、入札書及び内訳書を中封筒に入れるものとする。競争参加資格を取得中であった者は、資格審査結果通知書の写しを表封筒と中封筒の間に入れるものとする。表封筒に入札書在中の旨を朱書きし、中封筒に入札件名及び入札日時を記載し、入札書提出締切時刻までに支出負担行為担当官に提出しなければならない。[紙入札参加者は、郵送等により入札書を提出する場合は、発送後速やかに公告等において指定した担当部局に電話連絡するものとする。]

９　入札参加者は、一度提出した入札書の引き替え、変更又は取消しをすることができない。

10　紙入札参加者は、公告等において指定された時刻までに、指定された場所（以下「入札室」という。）に入室し、開札に立ち会うものとする。なお、入札参加者以外の者（本人又はその代理人以外の者）は、入札室に入室できないことがある。

　また、第１回目の開札に立ち会わない場合でも提出された入札書は有効なものとして取り扱うこととするが、再度の入札を行うこととなったときは、再度の入札への参加の意思の有無を電話により確認する。

11　紙入札参加者が、公告において指定された時刻までに入札室に入室しないときは、開札に立ち会う意思がないと認め開札に立ち会わせないものとする。

（入札の辞退）

第４条　入札参加者は、入札執行の完了に至るまでは、いつでも入札を辞退することができる。

２　電子入札参加者は、入札を辞退するときは、入札辞退届を電子調達システムにより提出するものとする。

　紙入札参加者は、入札を辞退するときは、入札辞退届（様式３）を支出負担行為担当官に持参し、若しくは郵送等により提出するものとする。ただし、これによることができない場合は、その旨を明記した入札書を提出するものとする。

３　入札を辞退した者は、これを理由として以後不利益な取扱いを受けるものではない。

（公正な入札の確保）

第５条　入札参加者は、私的独占の禁止及び公正取引の確保に関する法律（昭和22年法律第54条）等に抵触する行為を行ってはならない。

２　入札参加者は、入札に当たっては、競争を制限する目的で他の入札参加者と入札価格又は入札意思についていかなる相談も行わず、独自に入札価格を定めなければならない。

３　入札参加者は、落札者の決定前に、他の入札参加者に対して入札価格を意図

的に開示してはならない。

（入札の取りやめ等）
第６条　入札参加者が連合し、又は不穏の行動をなす等の場合において、入札を公正に執行することができないと認められるときは、当該入札参加者を入札に参加させず、又は入札の執行を延期し、若しくは取りやめることがある。

（入札の無効）
第７条　次の各号の一に該当する入札は、無効とする。
一　入札公告に示した競争参加資格を有しない者のした入札
二　競争参加資格確認資料に虚偽の記載をした者の入札
三　委任状を持参しない代理人のした入札
四　記名を欠く入札（電子調達システムによる場合は、電子認証書を取得していない者のした入札）
五　金額を訂正した入札
六　誤字、脱字等により意思表示が不明瞭である入札
七　明らかに連合によると認められる入札
八　当該入札について他の入札参加者の代理人を兼ね、又は２人以上の代理人をした者のした入札
九　入札において２通以上の入札書を提出した者のした入札
十　その他入札に関する条件に違反した入札
十一　郵送等による入札参加者の未到着の入札

（落札者の決定）
第８条　予決令第79条の規定に基づいて作成された予定価格の制限の範囲内で、最低の価格をもって有効な入札を行った者を落札者とする。ただし、国の支払の原因となる契約のうち予定価格が１，０００万円を超える工事又は製造その他の請負契約について、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされないおそれがあると認められるとき、又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の制限の範囲内の価格をもって入札した他の者のうち最低価格をもって入札した者を落札者とすることがある。
２　予決令第８５条の基準（防衛省所管契約事務取扱細則第２５条第１項（１）に定める基準）に該当する入札を行った者は、支出負担行為担当官の行う調査に協力しなければならない。

（再度入札）
第９条　開札した場合において、落札者がないときは、直ちに再度の入札を行う。
　また、第１回目の開札に立ち会わない場合でも提出された入札書は有効なものとして取り扱うこととするが、再度の入札を行うこととなったときは、再度の入札への参加の意思の有無を電話により確認する。

２　入札を無効とされた者は、再度入札に参加することができない。
３　入札執行回数は、原則として２回を限度とする。
４　各回の入札結果について、落札した場合は落札者名及び落札金額を、落札しなかった場合は最低入札金額を電子調達システムの画面上に表示するとともに、紙入札参加者に対しては入札室において読み上げを行う。
　なお、入札を保留する場合は、電子入札参加者に対しては電子調達システムにより通知するとともに、紙入札参加者に対しては口頭により通知する。
５　再度入札において落札者がないときは、特別な場合を除き、不調とする。

（同価格の入札者が２人以上ある場合の落札者の決定）
第１０条　落札となるべき同価格の入札をした者が２人以上あるときは、直ちに、当該入札をした者にくじを引かせて落札者を決定する。
２　前項の場合において、当該入札をした者のうち、くじを引かない者があるときは、これに代わって入札事務に関係ない職員にくじを引かせる。

（契約書の提出）
第１１条　落札者は、支出負担行為担当官から交付された契約書案に記名し、これを支出負担行為担当官に提出しなければならない。

（入札説明書等）
第１２条　入札説明書等は、積算等の目的以外に使用しないものとする。

（異議の申立）
第１３条　入札をした者は、入札後、この心得書、入札説明書等についての不明を理由として異議を申し立てることができない。

（暴力団排除による誓約）
第１４条　入札参加者は、入札書を提出することにより、様式４による「暴力団排除に関する誓約事項」を承諾したこととなる。
２　前項の誓約事項を許否する者は、競争参加を認めない。
３　第１項の誓約事項の誓約に虚偽があった場合又は誓約に反する事態が生じた場合は、当該入札者が提出した入札書を無効とする。

（不当介入に関する通報・報告の義務）
第１５条　乙は、自ら又は下請負者等が、暴力団、暴力団員、社会運動・政治運動ぼうゴロ等の反社会的勢力から不当要求又は業務妨害等の不当介入（以下「不当介入」という。）を受けた場合は、これを拒否し、又は下請負者等をして、これを拒否させるとともに、速やかに不当介入の事実を様式５により報告するとともに、警察への通報及び捜査上必要な協力を行うものとする。

（その他）
第１６条　契約当事者相互間の信頼関係を損なうような行為を行ってはならない。

２　相手方は「責任あるサプライチェーン等における人権尊重のためのガイドライン」（令和４年９月１３日ビジネスと人権に関する行動計画の実施に係る関係府省庁施策推進・連絡会議決定）を踏まえて人権尊重に取り組むよう努めるものとする。

様式１

委　　任　　状

当社は、　　を代理人と定め、下記件名の入札・見積に関する一切の権限を委任します。

記

件　　名：九州防衛局ＯＡネットワーク・システムの運用支援役務

令和　　年　　月　　日

支出負担行為担当官
　九州防衛局長　江原　康雄　　殿

住　　所
商号又は名称
代表者氏名
連　絡　先

様式２

入　札　書

件　　名：九州防衛局ＯＡネットワーク・システムの運用支援役務

入 札 金 額　￥＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

（内訳は、別添入札書金額内訳書のとおり）

上記の金額をもって入札心得書及び入札説明書の条項を承諾のうえ入札します。

令和　　年　　月　　日

支出負担行為担当官
　九州防衛局長　江原　康雄　　殿

住　　所
商号又は名称
代 表 者 氏 名
代 理 人 氏 名
連　絡　先

注：金額、月日等の数字は算用数字で明確に記載すること。

様式３

入　札　辞　退　届

件　　名：　九州防衛局ＯＡネットワーク・システムの運用支援役務

上記件名について、都合により入札を辞退します。

令和　　年　　月　　日

支出負担行為担当官
　九州防衛局長　江原　康雄　　殿

住　　所
商号又は名称
代表者氏名
代理人氏名
連　絡　先

様式4

暴力団排除に関する誓約事項

当社（個人である場合は私、団体である場合は当団体）は、下記1及び2のいずれにも該当しません。また、将来においても該当することはありません。

この誓約が虚偽であり、又はこの誓約に反したことにより、当方が不利益を被ることとなっても、異議は一切申し立てません。

また、官側の求めに応じ、当方の役員名簿（有価証券報告書に記載のもの（生年月日を含む。）。ただし、有価証券報告書を作成していない場合は、役職名、氏名及び生年月日の一覧表）及び登記簿謄本の写しを提出すること並びにこれらの提出書類から確認できる範囲での個人情報を警察に提供することについて同意します。

記

1　契約の相手方として不適当な者

（1）　法人等（個人、法人又は団体をいう。）の役員等（個人である場合はその者、法人である場合は役員又は支店若しくは営業所（常時契約を締結する事務所をいう。）の代表者、団体である場合は代表者、理事等、その他経営に実質的に関与している者をいう。）が、暴力団（暴力団員による不当な行為の防止等に関する法律（平成3年法律第77号）第2条第2号に規定する暴力団をいう。以下同じ）又は暴力団員（同法第2条第6号に規定する暴力団員をいう。以下同じ。）であるとき

（2）　役員等が、自己、自社若しくは第三者の不正の利益を図る目的、又は第三者に損害を加える目的をもって、暴力団又は暴力団員を利用するなどしているとき

（3）　役員等が、暴力団又は暴力団員に対して、資金等を供給し、又は便宜を供与するなど直接的あるいは積極的に暴力団の維持、運営に協力し、若しくは関与しているとき

（4）　役員等が、暴力団又は暴力団員であることを知りながらこれを不当に利用するなどしているとき

（5）　役員等が、暴力団又は暴力団員と社会的に非難されるべき関係を有しているとき

2　契約の相手方として不適当な行為をする者

（1）　暴力的な要求行為を行う者

（2）　法的な責任を超えた不当な要求行為を行う者

（3）　取引に関して脅迫的な言動をし、又は暴力を用いる行為を行う者

（4）　偽計又は威力を用いて支担官等の業務を妨害する行為を行う者

（5）　その他前各号に準ずる行為を行う者

上記事項について、入札書（見積書）の提出をもって誓約いたします。

様式５

令和　　年　　月　　日

支出負担行為担当官

九州防衛局長　江原　　康雄　　殿

住　　所
会 社 名
代表者名
担当者名
連 絡 先

排除対象者による不当介入の概要

貴（支出負担行為担当官名）が発注した公共事業等において排除対象者による不当介入を受けたため、○○警察への通報を行ったことと併せて、下記のとおり報告いたします。

契 約 機 関 等 （部課等名まで記入）	
調達要求番号等	
品 名 ・ 数 量	
契　約　金　額	
不当介入に係る行為者	住所 氏名
発生日時・場所	
不当介入の内容・被害の状況	
警察への通報、捜査上必要な協力についての対応状況	
その他特記事項	

(注)記入要領

1 住所、会社名及び代表者名については、契約書記載の内容とする。

2 「契約機関等」の欄には、当該契約締結の機関名（部課等名まで）を記入する。

3 「調達要求番号等」の欄には、調達要求書記載の「調達要求番号」又は契約書記載の「契約番号」等を記入する。

4 「品名・数量」の欄には、契約書に記載の「品名」又は「件名」等を記入する。

5 「契約金額」の欄には、契約金額及び変更契約をした場合は変更契約金額を記入する。

6 「不当介入に係る行為者」の欄には、（住所、氏名）を記入する。

7 「発生日時・場所」の欄には、不当介入を受けた日時・場所を記入する。

8 「不当介入の内容・被害の状況」の欄には、不当介入を受けた事実内容を詳細に記入する。また、不当介入により被害を受けた場合はその事実内容を詳細に記入する。

9 「警察への通報、捜査上必要な協力についての対応状況」の欄には、通報先の警察名、通報日時、捜査上必要な協力を行った場合はその内容を詳細に記入する。

10 「その他特記事項」の欄には、経緯等を把握するうえで必要な事項があれば記入する。

仕　様　書			
件名	九州防衛局ＯＡネットワーク・システムの運用支援役務	作成年月日	令和 5 年 12 月 26 日
		九州防衛局総務部総務課	

1　総則

1．1　適用範囲

この仕様書は、九州防衛局ＯＡネットワーク・システム（地方防衛局ＯＡネットワーク・システムの借上（北関東・九州）のうち、九州防衛局、長崎防衛支局（大分常駐官事務所を含む。）、熊本防衛支局、佐世保防衛事務所、別府防衛事務所、宮崎防衛事務所及び鹿児島防衛事務所に設置するもの（組織改編等により新たな事務所等に設置した場合を含む。）をいう。）（以下「局ＯＡシステム」という。）の運用支援役務（以下「役務」という。）について適用する。

1．2　目的

本役務は、局ＯＡシステムにおいて動作している装置及び各サービスを安定稼働させると共に、システムの保有する性能を常時最大限発揮させることを目的とする。

1．3　引用文書等

この仕様書に引用する次の文書は、この仕様書に規定する範囲内において、仕様書の一部をなすものであり、入札書又は見積書の提出時における最新版を使用するものとする。

なお、引用文書に定める事項がこの仕様書と相違する場合は、仕様書の定めるところによるものとする。

(1)　防衛省の情報保証に関する訓令（平成 19 年防衛省訓令第 160 号）
(2)　防衛省の情報保証に関する訓令の運用について（通達）（防運情第 9248 号。19.9.20）
(3)　防衛情報通信基盤データ通信網管理運用規則（平成 29 年自衛隊統合達第 15 号）
(4)　取扱い上の注意を要する文書等及び注意電子計算機情報の取扱いについて（通達）（防防調第 4608 号。19.4.27）
(5)　装備品等及び役務の調達における情報セキュリティの確保について（通達）（防装庁（事）第 137 号。4.3.31）
(6)　ＩＴ利用装備品等及びＩＴ利用装備品等関連役務の調達におけるサプライチェーン・リスクへの対応について（通知）（装管調第 807 号。3.1.21）
(7)　情報システムに関する調達に係るサプライチェーン・リスク対応のための措置について（通達）（防装庁（事）第 3 号。31.1.9）
(8)　情報システムに関する調達に係るサプライチェーン・リスク対応のための措置の細部事項について（通知）（装プ武第 188 号。31.1.9）
(9)　個人情報の保護に関する法律（平成 15 年法律第 57 号）
(10)　九州防衛局の情報保証に関する達（平成 19 年九州防衛局達 33 号）
(11)　仕様書「防衛省ＯＡシステム基盤借上（０３換装）」

1．4　一般事項

(1)　契約相手方は、本役務の履行にあたり、業務の意図及び目的を十分理解した上で、仕様書の各要素を満足させなければならない。
(2)　契約相手方は、本役務の履行に係る発注者との連絡調整及び受注者が行う業務全般を統

括する者を定め、総務部総務課に通知するものとする。

(3)　契約相手方は、本役務の契約の履行に当たり、第三者を従事させる必要がある場合は、情報システムの調達に係るサプライチェーン・リスク対応のための措置の細部事項について（通知）（装プ武第 188 号。31.1.9）に定める特約条項を適用する。

(4)　本役務に係る成果物及び類似の派生物（企画等の構想も含む。）における一切の著作権及び所有権は九州防衛局に帰属するものとする。

(5)　契約相手方は、本役務の履行に際し、発注者が保有する資料等で貸与を受ける必要がある場合には、総務部総務課と調整の上、貸与を受けることができるものとする。

(6)　契約相手方は、貸与された資料等がある場合、その取扱いなどに関し、発注者の指定する条件を遵守し、業務の完了後直ちに返却するものとする。

(7)　契約相手方は、本役務の履行上知り得た情報を第三者に漏らしてはならない。また、本役務の履行後においても同様とする。

(8)　契約相手方は、業務関係書類の作成等を行うパソコンについては、情報の流出について万全を期すために、ファイル交換ソフトをインストールしていないものを使用するものとし、第三者を従事させる場合も同様とする。

なお、業務関係書類とは、業務計画書、成果品等のほか、作業従事者名簿等の本支店等で作成する書類の一切を含むものとする。

(9)　契約相手方は、仕様書に関する疑義が生じた場合には、支出負担行為担当官補助者（以下「官補助者」という。）と協議するものとする。

(10)　契約相手方は、以下の資格及び実績の保有状況について、官補助者の確認を得るものとする。資格については、それを証明する書面（認定証など）の写しを提出すること。資格を有しない場合は、各資格に準じている事が確認できる資料を提出すること。

ア　セキュリティ関連資格

(a)　Ｐマーク（個人情報）

(b)　JISQ27001若しくはISO/IEC27001（情報セキュリティ保護）

イ　マネジメント関連資格

JISQ9001若しくはISO9001（業務品質管理）

2　役務に関する要求

2．1　**実施場所、役務期間、役務時間及び人員**

(1)　**実施場所**　実施場所の詳細については、以下のとおり及び支出負担行為担当官（以下「官」という。）が指定する場所とする。

実施場所の名称	住　　所
九州防衛局	福岡市博多区博多駅東２－１０－７福岡第二合同庁舎
長崎防衛支局	長崎市出島町２－２５
熊本防衛支局	熊本市東区東町１－１－１１
大分常駐官事務所	大分市大字里２６２０旭化成㈱大分工場

(2)　**役務期間**

令和６年４月１日から令和７年３月３１日までのうち、月曜日から金曜日までの（祝祭日及び１２月２９日から１月３日までの間を除く。）九州防衛局職員の勤務日を原則とする。

(3) **役務時間**

役務時間は実施場所によって異なり、以下を基準とする。

ただし、夜間、休日、祝祭日等の役務時間外における停電作業対応時や障害発生時、大規模災害発生時等の緊急を要する場合については、その都度官補助者と協議するものとする。

ア　九州防衛局

１日７時間４５分、８時３０分から１７時１５分（１２時から１３時の間を除く。）、月１５５時間を基準とする。

イ　長崎防衛支局

１日７時間４５分、８時３０分から１７時１５分（１２時から１３時の間を除く。）、四半期に１回程度、年３１時間を基準とする。

ウ　熊本防衛支局

１日７時間４５分、８時３０分から１７時１５分（１２時から１３時の間を除く。）、年に８回程度、年６２時間を基準とする。

エ　大分常駐官事務所

１日４時間、１１時から１６時（１２時から１３時の間を除く。）、年に２回程度、年８時間を基準とする。

(4) **人員**

ア　九州防衛局　常駐１名とする。ただし、他の手持ち業務等との関係において履行に必要な業務所要に対応できる態勢にあるものとする。

イ　長崎防衛支局、熊本防衛支局及び大分常駐官事務所　巡回要員１名とする。

２．２　**役務員等**

(1) **役務員**

本役務を実施する者を役務員と呼ぶ（以下、九州防衛局において常駐で役務を実施する者を局役務員、巡回で役務を実施する者を巡回役務員と呼ぶ。）。

(2) **役務員の要件**

役務員は、本役務を実施するにあたって、以下の事項を満たすものとする。

ア　局ＯＡシステムについて、その環境、操作及び運用方法を熟知した上で、作業を行うこと。

イ　引用文書等に挙げる防衛情報通信基盤（以下「ＤＩＩ」という。）等のシステム仕様及び関係規則等について理解でき、かつ、運用に必要な知識を有すること。

ウ　以下に示す能力及び資格のいずれかを有すること。資格については、それを証明する書面の写し、又は資格を保有しない場合は各資格に準じていることが分かる資料を、経験についてはシステム経歴書を提出すること。

(a)　局役務員

情報処理技術者試験（基本情報処理技術者、旧第二種情報処理技術者試験）、又は同等以上と認められる者（ＩＴスキル標準Ｖ３レベル２以上）

(b)　巡回役務員

情報処理技術者試験（IT パスポート）又は同等以上と認められる者（ＩＴスキル標準Ｖ３レベル１以上）

エ　日本国籍を有していること。

(3)　**役務員の申請**

契約相手方は、契約後速やかに本役務に従事する役務員について局ＯＡシステム運用支援作業関係者名簿を作成し、官に提出するものとする。

また、役務員の追加、変更等が生じた場合には、遅滞なく承認を得るものとする。

(4)　**役務員の交代**

官補助者は、本役務を実施するうえで、役務員の技術レベル、資質、態度等が運用支援業務に不適正と認められる場合には、官と協議し、当該不適正事項を契約相手方に提示した上で、役務員の交代を要求することができる。

２．３　**役務内容**

本役務は、官が貸与する「九州防衛局ＯＡネットワーク・システム運用マニュアル」に基づき、局ＯＡシステムの仕様及び接続形態並びに他の局ＯＡ連接システム（ＤＩＩを含む。）との連接形態を十分に熟知した上で、必要な役務を行う。なお、必要に応じて局ＯＡシステム契約相手方等と連携して作業を行う。対象器材と役務内容の対応及び契約の細部については表１のとおりとする。また、障害発生時等については、その都度協議するものとする。

表１

番号	役務内容	サーバ関係	クライアント関係	ネットワーク関係
1	形態管理	○	○	
2	ソフトウェアのカスタマイズ	○	○	
3	ハードウェア、ソフトウェアの接続又はインストール		○	○
4	障害の内容の確認	○	○	○
5	ヘルプデスク	○	○	○
6	不正アクセスの確認・調査	○	○	
7	ネットワーク運用管理	○	○	○
8	局ＯＡシステムの運用管理	○	○	○
9	ユーザ情報対応	○	○	
10	ホームページの更新	○		
11	職員への連絡業務代行	○	○	○
12	緊急連絡受付	○	○	○
13	府省共通システムとの連接	○	○	○

(1)　**形態管理**

電算機借上の契約相手方から提供されるソフトウェア（修正版等）の登録及び設定を行う。その際、以下の要件を満たすこと。

ア　各装置に搭載されるソフトウェアの仕様を熟知し、事前に動作検証を行った上で作業を行うこと。

イ　本作業に伴う影響を最小限とするよう、システム全体（サーバ、クライアント、ネッ

トワーク機器等）及びシステム運用の仕様並びに局ＯＡ連接システム（ＤＩＩを含む。）との連接仕様を理解し、他機能との関連性、適用順番及び適用時間帯等を検討した上で実施すること。

(2)　**ソフトウェアのカスタマイズ**

必要に応じ局ＯＡシステムのソフトウェアのカスタマイズを行う。その際、以下の要件を満たすこと。

ア　各装置に搭載されるソフトウェアの仕様を熟知し、事前に動作検証を行った上で作業を行うこと。

イ　本作業に伴う影響を最小限とするよう、システム全体（サーバ、クライアント、ネットワーク機器等）及びシステム運用の仕様並びに局ＯＡ連接システム（ＤＩＩを含む。）との連接仕様を理解し、他機能との関連性、適用順番及び適用時間帯等を検討した上で実施すること。

(3)　**ハードウェア（プリンタ等の外付けデバイス）、ソフトウェアの接続又はインストール等**

官の提供するハードウェア（プリンタ等の外付けデバイス）、ソフトウェアについて必要に応じ事前調査及び接続又はインストール等の作業を行う。その際、以下の要件を満たすこと。

ア　各装置のハードウェアの仕様及び搭載されるソフトウェアの仕様を熟知し、事前に動作検証を行った上でハードウェア接続、ソフトウェアインストールを行うこと。

イ　本作業に伴う影響を最小限とするよう、システム全体（サーバ、クライアント、ネットワーク機器等）及びシステム運用の仕様並びに局ＯＡ連接システム（ＤＩＩを含む。）との連接仕様を理解し、他機能との関連性、適用順番及び適用時間帯等を検討した上で実施すること。

ウ　端末の設定変更作業については、ＩＰアドレス体系を熟知し、変更作業を行うことによりネットワーク機能を有する機器の利用に影響を与えないこと。

エ　局ＯＡネットワークに新たなネットワーク機器を接続する場合及び局ＯＡネットワークに接続された機器の故障修理を行う場合、当該機器の情報を確認し、不正接続検知装置に登録すること。

(4)　**障害の内容の確認**

官から障害連絡を受けた際、局ＯＡシステムの障害か使用者の誤操作か、あるいは他の局ＯＡ連接システム（ＤＩＩを含む。）の障害かを切り分けし、局ＯＡシステムの障害の場合は障害原因を特定する。その際、以下の要件を満たすこと。

ア　各装置のハードウェアの仕様及び搭載されるソフトウェアの仕様を熟知した上で、障害内容の確認及び切り分け方式の検討並びに切り分けを速やかに行うこと。

イ　切り分け作業を行うため、利用者の端末の遠隔操作を行う際には、あらかじめ官の了解を得た上で実施すること。

ウ　局ＯＡシステムの障害の場合には、官の指示に従い、局ＯＡシステム契約相手方へ速やかに連絡を行い、連携を図りつつ障害部位を特定すること。他の局ＯＡ連接システムの場合には、速やかに官に報告すること。

エ　障害部位が故障に至らない軽微なものであった場合、状況に応じて定常状態へ復旧及

び改善措置を講じること。

オ　障害復旧後、速やかに局ＯＡシステム障害報告書を提出すること。

カ　使用者の誤操作の場合には、後述の「ヘルプデスク」を行うこと。

(5)　**ヘルプデスク**

局ＯＡシステムの操作、運用についての問い合わせへの対応を行う。その際、以下の要件を満たすこととし、エンドユーザーの問い合わせに対し速やかに対応すること。

ア　各装置のハードウェアの仕様及び搭載されるソフトウェアの操作方法・仕様を熟知し、現状のシステムの形態管理状況及びカスタマイズ状況等を把握した上で行うこと。

イ　局ＯＡシステムの運用（バックアップ運用、ログ運用、夜間処理等）やリソース状況について十分理解した上で行うこと。

(6)　**不正アクセスの確認・調査**

官から局ＯＡネットワーク・システムに対し、不正アクセスの有無について調査の指示を受けた場合又はウィルスを検知した場合には、速やかに調査を行う。その際、以下の要件を満たすこと。

ア　局ＯＡシステムネットワーク構成、ネットワーク機器仕様、局ＯＡ連接システム（ＤＩＩを含む。）の連接仕様を熟知した上で調査を行うこと。

イ　不正アクセスが行われていた場合又はウィルスを検知した場合には、速やかに官に報告すること。また、その原因の特定及び対策を講じること。

ウ　本作業で実施した内容について、速やかに報告書を提出すること。

(7)　**ネットワーク運用管理**

ネットワーク障害による業務への影響を未然に防ぐため、障害の発生の兆候を随時確認するとともに、稼働状況を定期的に照会する。その際、以下の要件を満たすこと。

ア　局ＯＡシステムネットワーク構成、ネットワーク機器仕様、局ＯＡ連接システム（ＤＩＩを含む。）の連接仕様を熟知し、ネットワークの稼働状況を管理すること。

イ　障害の発生の兆候が確認された場合には、速やかに官に報告すること。また、局ＯＡシステム契約相手方へ速やかに連絡を行い、連携を図りつつ障害の原因を特定すること。

ウ　故障に至らない軽微なものであっても、状況に応じて定常状態へ復旧及び改善措置を講じること。

エ　障害復旧後、速やかに局ＯＡシステム障害報告書を提出すること。

オ　主な稼働状況の確認は、以下のネットワークを対象とする。

(a)　局ＯＡシステムで利用する専用回線

(b)　ＤＩＩとの回線

(c)　ネットワーク機器

(8)　**局ＯＡシステムの運用管理**

ハードウェアの動作チェック、イベントログの確認、バックアップシステムの動作確認、バックアップテープの世代管理、バックアップデバイスのクリーニング、サーバのハードディスク容量確認、メール使用量等調査、システム運用スケジュールの変更、セキュリティ情報収集（不正接続検知装置の情報を含む。）、情報漏洩対策機能の運用（登録・変更・削除）、セキュリティ・ホール対策及びウィルス定義ファイルの更新確認を行う。セキュ

リティ・ホール対策については、各装置のハード仕様及び搭載されるソフトウェアの仕様を熟知し、事前に動作検証を行った上で作業を行うこと。

ア　ハードウェアの動作チェックについては、定期的に稼働状況を照会し、異常を検知した場合には、速やかに官に報告すること。また、局ＯＡシステム契約相手方へ速やかに連絡を行い、連携を図りつつ障害の原因を特定すること。

イ　ＣＰＵ、ディスク、メモリ使用率のしきい値超過等、サーバの正常な運転を阻害する事象を発見した場合には、速やかに適切な措置を講じること。

ウ　故障時等のデータ亡失に備え、正常にバックアップが行われるようサーバのバックアップシステムの動作確認を行うこと。バックアップ後のバックアップテープについては、正常にバックアップされたことを確認し、世代管理を行うこと。

エ　バックアップデバイスについては、定期的にクリーニングを行うこと。

オ　サーバのハードディスク容量確認については、サーバの仕様を理解した上で、ハードディスク容量に不足がないか定期的に確認し、必要であれば、ハードディスクの最適化を行うこと。

カ　メール使用量等調査については、電子メール等で利用している機器の仕様を理解した上で、メールの使用量等を定期的に確認すること。

キ　システム運用スケジュールの変更については、システム全体（サーバ、クライアント、ネットワーク機器等）及びシステム運用の仕様並びに局ＯＡ連接システム（ＤＩＩを含む。）との連接仕様を理解した上で、本作業に伴う他機能との関連性、変更順番及び変更時間帯等を検討し、影響を最小限とすること。

ク　セキュリティ・ホール対策及びウィルス定義ファイルの手動更新については、各装置のハード仕様及び搭載されるソフトウェアの仕様を熟知し、事前に動作検証を行った上で作業を行うこと。随時セキュリティ情報の収集に努めること。

(9)　**ユーザ情報対応**

人事異動等に伴うユーザ管理台帳のメンテナンス、ユーザのシステム登録・変更・削除及び端末管理台帳のメンテナンス、身分証ＩＣカードのトークン情報の取得、端末の設定変更及びネットワークケーブルの追加敷設の作業支援並びにサーバ等の設定変更作業を行う。その際、以下の要件を満たすこと。

ア　搭載されるソフトウェアの仕様及びユーザのシステムの登録・変更・削除機能を熟知した上で作業を実施し、作業終了後、動作確認を行うこと。

イ　全国各地方防衛局のユーザ情報の統合を行うにあたり、防衛省ＯＡネットワーク・システム運用役務及び各地方防衛局運用役務と連携を図ること。

ウ　人事異動等により変更が生じる都度、ユーザ管理台帳及び端末管理台帳を常に最新版となるようメンテナンスすること。

エ　端末の設定変更作業については、ＩＰアドレス体系を熟知し、変更作業を行うことによりネットワーク機能を有する機器の利用に影響を与えないこと。

オ　ネットワークケーブルの追加敷設の作業支援については、ネットワーク構成を熟知し、追加敷設することによるサーバ設定への影響を事前に調査し、設定変更後に動作確認を行うこと。

(10)　**ホームページの更新**

イントラネットで公開している局内ホームページの更新作業及びインターネットで使用する局ホームページの掲載データの更新作業の補助を行う。

(11) **職員への連絡業務代行**

システムの運用停止及び端末の設定変更等で利用者と作業日程調整等が必要な場合、局総務部総務課システム担当者及びシステム担当補助者との調整を代行する。

(12) **緊急連絡受付**

システム管理者が緊急と判断した場合、夜間・休日・祝祭日・年末年始についても対応窓口を用意し、受付を実施する。

(13) **府省共通システムとの連接**

府省共通システム（ＡＤＡＭＳⅡ、ＧＩＭＡ等）と局ＯＡシステムの連接等関連業務について、接続試験等検証を実施する。

(14) **その他**

この仕様書に記載されていない事項については、官補助者と協議するものとするが、技術的に当然実施すべき事項については、上記以外の役務作業を行う。

(15) **報告書の提出**

上記役務内容について、下記第３項に掲げる報告及び書類を提出し、官の確認を受ける。

3　提出書類

上記の役務内容について、以下表２に掲げる報告及び書類を提出し、官側の確認を受けるものとする。なお、項目については、必要に応じて変更する場合がある。

表２

書類の名称	必要な項目	提出期限	提出部数	媒体の種別
運用体系図	体系図、連絡先、バックアップ態勢	契約後速やかに	1	電子媒体又は紙媒体
局ＯＡシステム運用支援作業関係者名簿	所属、氏名、役割	契約後速やかに	1	電子媒体又は紙媒体
日々作業内容報告	作業内容及び時間、実施者	毎日の作業終了時	1	電子媒体
局ＯＡシステム運用支援実績（月次）報告書	作業内容、依頼者及び依頼年月日、回答者及び回答年月日、作業時間	該当翌月の末日	1	電子媒体又は紙媒体
局ＯＡシステム障害報告書	障害発生日時、障害の内容及び原因、処置内容及び実施者、復旧日時	障害復旧後可能な限り速やかに	1	電子媒体又は紙媒体
局ＯＡシステム不正アクセス報告書	不正アクセス発生日時、内容、処置内容及び実施者	不正アクセス発生後可能な限り速やかに	1	電子媒体又は紙媒体

局ＯＡシステム利用統計	ネットワークトラフィック、メール使用量、データ容量等	３月末日	１	電子媒体又は紙媒体

※　電子媒体については、九州防衛局ＯＡネットワーク・システム運用管理マニュアルを参照すること。なお、紙媒体については、①古紙パルプ配合率が７０％以上であること。②塗工されていないものについては、白色度７０％程度以下であること。③塗工されているものについては、塗工量が両面で３０g/㎡以下であること。④再利用しにくい加工が施されていないこと。

※「必要な項目」は、官側指示により必要に応じ適宜追加・削除する。

4　検査

検査は、第３項の提出書類に基づき官補助者の確認によるものとする。

5　情報の保全等

契約相手方は、本契約の履行にあたっては、以下の事項について遵守すること。

知り得た保護情報の取扱いに当たっては、「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（通達）（防装庁（事）第 137 号(4.3.31)」に基づき、適切に管理するものとする。細部については以下のとおりとする。

番号	保護すべき情報	具体的な保護すべき情報
１	ネットワーク構成	ネットワーク構成全般
２	インターフェイス（アドレス、プロトコル等）仕様	ＩＰアドレス
３	セキュリティ（ファイヤーウォール等）仕様	ファイヤーウォール設定値
		不正接続検知装置設定値
		セキュリティパッチ適用状況
		管理者パスワード
４	設置場所等の施設情報（設置部隊及び数量を含む）	端末機器配置図
		ネットワーク配線図
５	個人に関する情報	ユーザ情報

6　資料の貸与

以下の資料を貸与する。取扱いについては、十分注意するものとし、原則として官が指定した役務席から持ち出してはならない。また、本資料より知り得た情報を第三者に漏らしてはならない。なお、本役務の履行後においても同様とする。

局ＯＡシステム契約相手方からの指示により仕様に変更等が生じた場合には、随時修正を行い、常に最新の状態にすること。

・仕様書「防衛省ＯＡシステム基盤借上（０３換装)」
・システム構成書
・システム設定書
・システム取扱い説明書（システム管理者等マニュアル）
・構成品取扱説明書（ユーザマニュアル）

7　その他

7．１　官有設備等の貸与

契約相手方は、官の設備及び器材等の貸与を受けることができるほか、必要に応じてその他の官有設備等の貸与を受けることができるものとする。

７．２　官側における支援

契約相手方は、この契約の履行にあたって、官側の支援が必要な場合には、支援を得ることができるものとする。

７．３　個人情報の取扱い

個人情報の取扱いについては、「個人情報の保護に関する法律（平成 15 年法律第 57 号)」及び契約約款の条項を遵守すること。

７．４　役務等に関する要求

本役務の実施にあたり、契約の相手方（下請負者、再委託先等を含む。）は、契約物品（役務対象物品又は寄託品を含み、ソフトウェアその他の電子計算機情報を含む。）又は官給品等（契約相手方が当該契約の履行のために防衛省から支給され、又は貸与される材料、部品、機器、治工具、測定具等（ソフトウェアその他の電子計算機情報を含む。）について、情報の漏えい若しくは破壊又は障害等のリスク（未発見の意図せざる脆弱性を除く。）が潜在すると知り、又は知り得べきソースコード、プログラム、電子部品、機器等の埋込み又は組込みその他官の意図せざる変更を行わず、かつ、そのために必要な相応の管理を行うものとする。

紙応札者が落札した場合

役 務 契 約 書（案）

１　件　　名：九州防衛局ＯＡネットワーク・システムの運用支援役務

２　契約内容：仕様書のとおり

３　契約場所：仕様書のとおり

４　契約期間：令和６年４月１日から令和７年３月 31 日

５　契約金額：￥　　．―
（うち消費税及び地方消費税の額￥　．―）
月額：￥　　．―
（うち消費税及び地方消費税の額￥　．―）

６　契約保証金：免　除

７　支払方法：毎月払

８　特約条項：有

発注者　支出負担行為担当官 九州防衛局長　江原　康雄（以下「甲」という。）と、受注者　　（以下「乙」という。）は、九州防衛局ＯＡネットワーク・システムの運用支援役務について、次に定める条項により契約を締結し、その証しとして本書２通を作成し、当事者が記名押印のうえ各自１通を保有する。

令和 ６ 年　　月　　日

甲　　福岡県福岡市博多区博多駅東２丁目 10 番７号
支出負担行為担当官
九州防衛局長　　江　原　　康　雄

乙

（信義則）
第１条　甲及び乙は、信義を重んじ、契約に基づき債務を誠実に履行しなければならない。

（総則）
第２条　乙は、この契約の基づき、履行期限までに履行場所において、契約に係る役務を提供し、甲は役務の対価として代金を支払う。
２　乙は、契約期間中、局ＯＡを安定稼働させると共にシステムの最大能力を常時発揮させなければならない。

（権利義務の譲渡の禁止）
第３条　乙は、債務の履行を第三者に引き受けさせ、又は契約から生ずる権利若しくは義務を第三者に譲渡し、承継せしめ若しくは担保に供してはならない。ただし、書面による甲の事前の承認を得たときはこの限りではない。

（一括委任又は一括請負禁止）
第４条　乙は、この契約の履行について、業務の全部又はその主たる部分を一括して第三者に委任し、若しくは請け負わせてはならない。ただし、あらかじめ乙の申請を甲が承認した場合は、この限りではない。
２　前項の場合及び軽微な業務を除き、乙が業務の一部を第三者に委任し、若しくは請け負わせるには、あらかじめ甲に通知しなければならない。
３　乙は、第１項又は第２項により委任若しくは請け負わせた者から更に第三者に委任若しくは請負が行われる場合には、あらかじめ甲に通知しなければならない。
４　乙は、第１項の承認を得た場合又は、第２項及び第３項の通知を行った場合であっても、受任者、下請負者又はそれらの被用者（以下「受任者等」という。）の行為につき、甲に対して一切の責任を負うものとする。

（秘密の保持）
第５条　乙は、債務の履行に際して知り得た秘密及び個人情報（以下「知り得た秘密」という。）を第三者に漏らし、提供し、又は利用してはならない。
２　乙は、使用人の身元並びに作業場における風紀、衛生及び規律の維持について一切の責任を負う。
３　乙は、業務の処理に当たって守るべき事項を定め、乙の使用人に対し明示しなければならない。
４　乙は、知り得た秘密の漏えい等の防止のため、適切な措置をとらなければな

らない。
5　乙は、個人情報を複製する場合、あらかじめ書面により甲の承認を受けなければならない。
6　乙は、個人情報に関し、善良なる管理者の注意を持って債務を履行する目的の範囲外での利用をしてはならない。
7　乙は、個人情報の管理につき、定期的に検査を行う。また、甲は、特に必要と認めた場合は、乙に対し、個人情報の管理状況に関し質問し、資料の提出を求め、又はその職員の乙の事業所等の関係場所に立入調査させることができる。
8　乙は、甲が適当でないと認めた使用人を使用することができない。
9　債務の履行に関し事故等が発生した場合、乙は、速やかに、その内容を甲に報告するものとする。

（報告及び検査）
第６条　乙は、各月の末日に、その月の初日から末日までの役務の提供が終了したときは、その旨を速やかに甲に報告しなければならない。
2　甲は、前項の報告を受けた日から起算して 10 日以内に、検査を命じた職員（以下「検査官」という。）に検査させる。

（再検査）
第７条　乙は、前条第２項の検査に合格しないものがあるときは、遅滞なく手直しをし、速やかに甲に報告しなければならない。この場合において手直しに要する費用は、乙が負担するものとする。
2　甲は、前項の報告を受けた日から起算して 10 日以内に検査官に再検査をさせる。

（請求及び支払）
第８条　乙は、甲の検査に合格したとき又は再検査に合格したときは、代金の支払いを甲に請求するものとし、甲は、請求書を受理した日から 30 日（以下「約定期間」という。）以内に支払うものとする。
2　甲の責めに帰すべき事由により代金の支払が遅れた場合においては、約定期間が満了する日の翌日から支払をする日までの日数に応じ、未支払金額に対し約定期間満了の日の翌日時点における財務省告示による政府契約の支払遅延利息の率を乗じて計算した額を遅延利息として乙に支払わなければならない。ただし、甲が約定期間内に支払をしないことが天災地変等やむを得ない事由の発生によるときは、当該事由の継続する期間の日数は、遅延利息を支払

う日数に算入しない。

（事情変更の場合の契約内容の変更）

第９条　甲及び乙は、経済情勢の変動、天災地変の発生、関係法令の制定又は改廃その他この契約の締結の際、予測できなかった著しい事情の変更が生じたことにより債務を履行することが不適当と認められるときは協議を行い、契約の内容を変更することができる。

２　第１項のほか甲が必要であると認めるときは協議を行い、契約の内容を変更することができる。

３　第１項及び第２項における契約の内容の変更は、書面により行う。

（履行遅滞における遅延損害金）

第 10 条　乙が、自らの責めに帰すべき事由により甲の指定する期限までに役務を完了することができないときは、遅滞日数に応じ、遅滞分に相当する代金に対し、１日につき０．１％の率を乗じて計算した金額を遅延損害金として甲に支払わなければならない。

（甲の解除権）

第 11 条　甲は、次の各号のいずれかに該当するときは、この契約を解除し、契約金額の 10 分の 1 に相当する額を違約金として徴収することができる。

一　乙が本契約を履行しないとき又は履行の見込みがないと認めたとき。

二　乙が債務の履行を拒絶する意思を明確に表示したとき。

三　債務の履行に際し、乙又は乙の使用人が不正行為又は不当行為を行ったとき。

四　乙が、この契約の条項に違反したとき。

五　契約期間中、乙の信用の状態が著しく低下し、債務の履行ができないと甲が認めたとき。

２　甲は、前項各号に掲げる場合のほか、自己の都合により契約を解除することができる。ただし、甲は、契約を解除する日の 30 日前までに書面により乙に予告しなければならない。

（賠償金等の徴収）

第 12 条　乙は、この契約に基づく賠償金、損害金又は違約金（以下、「賠償金等」という。）は、甲の発する納入告知書に基づき、納入告知書に定める期日（以下「納付期限」という。）までに支払わなければならない。

２　甲は、乙が賠償金等を納付期限までに支払わないときは、納付期限の翌日か

ら賠償金等の支払のあった日までの日数に応じ、未支払金額に対し遅延が生じた時点における財務省告示による国の債権の管理等に関する法律施行令第29 条第一項本文に規定する財務大臣が定める率の率を乗じて計算した金額を遅延利息として徴収する。ただし、乙が納付期限までに支払わないことが天災地変等やむを得ない事由の発生によるときは、当該事由が継続する期間の日数は、遅延利息を支払う日数に算入しない。

（乙の解除権）

第 13 条　乙は、乙の責めに帰することができない事由により履行できないときは、契約を解除することができる。

（代金の部分支払）

第 14 条　第 11 条又は前条の規定により契約が解除される前に、役務の提供のうちすでに行われたものがあるときは、乙は、その部分に相当する代金の支払を請求することができる。この場合において、その期間が１月に満たないときは、日数に応じた日割計算によって算定（１円未満の端数は切り捨てる。）するものとする。

２　第６条から第８条までの規定は、前項の規定により代金の支払を請求する場合について準用する。この場合において、第６条第１項中「各月」とあるのは「この契約が解除される日の属する月」と「末日まで」とあるのは「この契約が解除される日まで」と読み替えるものとする。

（損害賠償責任）

第 15 条　第 11 条の規定に基づき甲が契約を解除したことにより乙が損害を受けたときは、甲は損害を賠償しなければならない。

２　乙が債務を履行するに際し、使用人が甲又は第三者に損害を与えたときは、乙は、甲又は第三者に対して使用人の行為（不作為を含む）から生ずる損害を賠償するものとする。ただし、甲の受けた損害のうち自己の責めに帰すべき事由により生じたものがあるときは、甲は、損害賠償の損害賠償の額を減額することができる。

（合意管轄）

第 16 条　この契約に関する訴訟については、福岡地方裁判所を管轄裁判所とする。

（その他）

第17条　この契約に定めのない事項及び契約に関して生じた疑義は、甲、乙が協議して解決する。

２　この契約においては、乙は「責任あるサプライチェーン等における人権尊重のためのガイドライン」（令和４年９月１３日ビジネスと人権に関する行動計画の実施に係る関係府省庁施策推進・連絡会議決定）を踏まえて人権尊重に取り組むよう努めるものとする。

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

（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。

（下請負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、下請負者（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。

（下請負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、保護すべき情報を下請負者に取り扱わせる必要が生じた場合には、当該下請負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、下請負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、原則として下請負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、乙の下請負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、甲が行う乙の下請負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、乙又は乙の下請負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、防衛装備庁長官と協議を行ったうえで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（防経装９２４６号。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　ｐ２

第２　定義　ｐ２

第３　対象　ｐ５

第４　情報セキュリティ基本方針等　ｐ５

第５　組織のセキュリティ　ｐ５

第６　保護すべき情報の管理　ｐ８

第７　情報セキュリティ教育及び訓練　ｐ１１

第８　物理的及び環境的セキュリティ　ｐ１２

第９　保護システムについての管理　ｐ１５

第１０　情報セキュリティ事故等への対応　ｐ１５

第１１　情報セキュリティ事故等発生時の対応　ｐ１７

第１２　リスク査定　ｐ１８

第１３　セキュリティ監査等　ｐ１９

第１４　防衛省による監査　ｐ２０

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) 下請負者とは、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、監査等を行うものを含む。
(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。この場合において、当該者が、自らが保護すべき情報に接しているとの認識の有無を問わない。）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、防衛省の確認を受けるのとする。

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下請負者

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下請負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下請負者との間で契約し、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、当該下請負者において情報セキュリティが確保されることを確認した後、防衛省に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。

(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。

(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、保護システムにおける保護すべきデータの閲覧については、システムログの記録により代用することができる。

(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。

(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。

(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、保護すべき情報の取扱施設に加え、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。

エ　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。

オ　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等により、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。

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に対する保護システムの対処能力の有効性を検証し、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号及び第２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、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有効性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有効性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有効性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及び監査官による書類の閲覧等への協力）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　ｐ２２

第２　システムセキュリティ実装計画書　ｐ２２

第３　構成管理　ｐ２３

第４　保護システムの基本的防御　ｐ２５

第５　アクセス制御　ｐ２７

第６　識別及び認証　ｐ３０

第７　通信制御　ｐ３２

第８　システム監視　ｐ３４

第９　システムログ　ｐ３６

第１０　脆弱性スキャン　ｐ３８

第１１　バックアップ　ｐ３８

第１２　システムメンテナンス等　ｐ３９

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、セキュリティ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、数字及び特殊文字をそれぞれ１文字以上使用した１４文字以上であり、容易に推測されないものであること。

(ｲ) 定められた期間以内に変更すること。

(ｳ) 世代にわたって同じパスワードを使用しないこと。

(ｴ) 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下請負者を含む。）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。

情報システムの調達に係るサプライチェーン・リスク対応に関する特約条項

甲及び乙は、防衛省が行う情報システム（ハードウェア、ソフトウェア、ネットワーク、記録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。以下同じ。）の調達に係るサプライチェーン・リスク（当該情報システム及びその構成品等のサプライチェーンにおいて、不正プログラムの埋込み、情報の窃取、不正機能の組込み等が行われるリスクをいう。以下同じ。）への対策に関し、次の特約条項を定める。

（意図せざる変更が加えられないための管理体制）

第１条　乙は、この契約の履行において、本情報システム（この契約において全部又は一部を設計、構築･製造、運用･保守又は廃棄（賃貸借によるものを含む。）する情報システムをいう。以下同じ。）に防衛省の意図しない変更や情報の窃取等が行われないことを保証する管理を、再委託（再々委託以降の委託を含む。なお、市場に流通するカタログ製品の購入は、再委託に含まれない。以下同じ。）先を含め、この特約条項の定めるところにより、一貫した品質管理体制の下で行わなければならない。ただし、第三者に再委託しても情報システムの内容を知り得ないことが明らかな場合並びに第三者に再委託してもマルウェア等の不正なプログラム及び機器が組み込まれる等のリスクがないことが明らかである製造請負を再委託する場合は、この限りではない。

２　乙は、防衛省の意図しない変更や要機密性情報の窃取等が行われないことを保証するための具体的な管理手順その他の品質保証体制を証明する書面（品質管理体制の責任者及び品質保証の各担当者がアクセス可能な範囲等を示した管理体制図を含めることを必須とする。）を甲に提出しなければならない。第三者機関による品質保証体制を証明する書面等が提出可能な場合には、当該書面等を合わせて提出するものとする。

３　乙は、本情報システムに防衛省の意図しない変更が行われるなど不正が見つかったときに、追跡調査や立入検査等、防衛省と連携して原因を調査し、排除するための手順及び体制（防衛省の情報システムの運用・保守業務を行う契約にあっては、当該運用・保守業務において乙及び再委託先が行う作業履歴を記録し、防衛省の求めに応じてこれらを防衛省に提出する手順及び体制を含めることを必須とする。）を整備し、当該手順及び体制を示した書面を甲に提出しなければならない。

４　乙は、この契約の一部を再委託する場合には、前項により、防衛省と乙が連携して行う追跡調査や立入検査等を再委託先が受け入れるよう、あらかじめ再委託先と約

定しておかなければならない。なお、追跡調査や立入検査等において防衛省が必要と判断した場合には、この契約の履行に従事する再委託先の従業員の情報を確認するため、これに協力する旨を再委託先との約定に含めなければならない。

5　乙は、サプライチェーン・リスクを低減する対策として、情報システムの設計、製造・構築、運用・保守、廃棄の各工程における不正行為の有無について定期的及び必要に応じて監査を行うとともに、この契約により甲に納入する製品に対して意図しない変更が行われるリスクを回避するための試験を行わなければならない。当該試験の項目は、情報セキュリティ技術の趨勢、対象の情報システムの特性等を踏まえ、乙において適切に設定し、少なくとも以下の６項目については必ず実施しなければならない。

(1) 環境設定されたパラメータの再確認

(2) 製造中に利用したアカウントの削除の確認

(3) ウイルスチェック

(4) 不要なソフトウェアパッケージの削除の確認

(5) 使用ソフトウェアのバージョン管理の確認

(6) ソフトウェアのインストール手順書（インストールソフトウェアの名称及び設定パラメータ内容から成る手順書をいう。）の完成度の確認

6　乙は、前項の試験に関し、実施要領を作成し、甲の確認を得た後、提出しなければならない。ただし、既に甲の確認を得た実施要領と同一である場合には、特別な指示が無い限り、届出をすれば足りる。

7　乙は、この契約の全部を一括して、第三者に再委託してはならない。また、この契約の履行における総合的な企画及び判断並びに業務遂行管理部分を第三者に再委託してはならない。ただし、この契約の適正な履行を確保するために必要な範囲において、この契約の一部（総合的な企画及び判断並びに業務遂行管理部分を除く。）を第三者に再委託する場合には、乙は、主たる契約条項の下請負に関する規定の定めるところにより、必要な手続きを実施しなければならない。

8　前項の規定は、乙が再委託先を変更する場合その他の事由により、届出を行った内容等を変更する場合に準用する。

9　乙は、再委託先に提供する情報は必要最低限の範囲とし、提供された情報を第三者に漏洩することを防止するため、再委託先において適切な管理を行う旨を再委託先との約定に含めなければならない。

10　乙は、この契約の一部を第三者に負わせる場合においても、この契約により乙の義務とされていることにつきその責めを免れない。

11　乙は、この契約の一部の再委託に当たり、再委託先においてこの特約条項に定める義務が確実に履行されるため必要な事項を、再委託先と約定しなければならない。

（委託先の資本関係・役員の情報等に関する情報提供）

第２条　乙は、この契約の履行に従事する従業員（契約社員、派遣社員等の雇用形態を問わず、この契約の履行に従事する全ての従業員をいう。以下同じ。）を必要最低限の範囲に限るものとし、以下の情報を書面により甲に届け出なければならない（送付も可とする。）。

(1) 乙の資本関係及び役員の情報

(2) この契約に係る各工程の実施場所（防衛省及び防衛省以外のそれぞれの場所）

(3) この契約の履行に従事する従業員の氏名、所属、役職、専門性（特に、情報セキュリティに係る資格、研修実績、情報セキュリティ業務での経験年数）

(4) この契約の履行に従事する従業員の国籍（雇用対策法（昭和４１年法律第１３２号）第２８条第１項に基づき事業主が厚生労働大臣に届け出る事項として、雇用対策法施行規則（昭和４１年労働省令第２３号）第１０条第１項第３号に規定される国籍の属する国等をいう。以下同じ。）の割合

(5) 情報システムに関する代表的な契約実績（防衛省及び防衛省以外とのそれぞれの契約実績）

２　前項の規定は、乙がこの契約の履行に従事する従業員を変更する場合にも準用する。

３　乙は、この契約の一部を再委託する場合、再委託業務に従事する従業員を必要最低限に限ることを再委託先と約定するとともに、以下の情報を書面により甲に届け出なければならない（送付も可とする。）。

(1) 再委託先の資本関係及び役員の情報

(2) 再委託業務の実施場所（防衛省及び防衛省以外のそれぞれの場所）

(3) 再委託業務に従事する従業員の氏名、所属、役職、専門性（特に、情報セキュリティに係る資格、研修実績、情報セキュリティ業務での経験年数）

(4) 再委託業務に従事する従業員の国籍の割合

(5) 情報システムに関する代表的な契約実績（防衛省又は防衛省以外との契約実績）

４　前項の規定は、乙が再委託先を変更する場合又は再委託先が再委託業務に従事する従業員を変更する場合にも準用する。

（サプライチェーン・リスクに係る監査の受入れ等）

第３条　乙は第１条第３項に定める防衛省が行う追跡調査や立入検査等を受け入れなければならない。なお、追跡調査や立入検査等において防衛省が必要と判断した場合には、この契約の履行に従事する従業員の情報を確認するため、これに協力しなければならない。

２　乙は、再委託先に対し、定期的及び必要に応じて再委託先におけるサプライチェーン・リスク対応についての実施状況について監査を行うものとする。

（機器等の調達）

第４条　乙は、この契約により甲に納入する「IT 製品の調達におけるセキュリティ要件リスト」（経済産業省）に掲載される機器等（以下「機器等」という。）には、Common Criteria（ISO/IEC 15408)の評価保証レベル（EAL）４以上の製品を努めて使用しなければならない。機器等に当該基準を満たす製品の使用が困難な場合は、使用を予定している機器等と当該基準の比較表を作成し、甲の確認を得た後、安全性及び信頼性の高い製品を使用するものとする。ただし、使用を予定している機器等と当該基準の比較表の確認に当たり、既に甲の確認を得た比較表と同一である場合は、特別な指示がない限り、届出をすれば足りる。

２　乙は、第２条第３項に掲げるもののほか、機器等の製造を再委託先に請け負わせる場合、再委託先にこれらの製品に対して意図しない変更が行われるリスクを回避するための試験を行わせなければならない。当該試験の項目は、情報セキュリティ技術の趨勢、対象の情報システムの特性等を踏まえ、乙が再委託先と調整して適切に設定し、少なくとも以下の６項目については必ず実施しなければならない。

(1) 環境設定されたパラメータの再確認

(2) 製造中に利用したアカウントの削除の確認

(3) ウイルスチェック

(4) 不要なソフトウェアパッケージの削除の確認

(5) 使用ソフトウェアのバージョン管理の確認

(6) ソフトウェアのインストール手順書（インストールソフトウェアの名称及び設定パラメータ内容から成る手順書をいう。）の完成度の確認

３　乙は、前項の試験に関し、再委託先に実施要領を作成させ、甲の確認を得た後、提出しなければならない。ただし、既に甲の確認を得た実施要領と同一である場合は、特別な指示が無い限り、届け出をすれば足りる。

４　乙は、機器等の調達におけるトレーサビリティを確保するため、乙の製造する機器等について製造工程の履歴を記録する管理体制を整備し、機器等を構成する主要部品について製造事業者、製造事業者の国籍、製造国に関する情報（以下「トレーサビリティ情報」という。）を把握しなければならない。また、乙は、当該管理体制に以下の項目を含めなければならない。

(1) 機器等に対して不正な変更が加えられないための体制

(2) 不正な変更が加えられていないことを検査する体制

(3) 機器等の設計から部品検査、製造、完成検査に至る工程を一貫した品質保証体制の下で、不正な変更が行われないことを保証する体制

５　乙が機器等の製造を再委託先に請け負わせる場合にも、前項の規定を準用するものとする。

６　乙は、前２項の規定による管理体制を証明する資料を甲に提出しなければならない。また、甲の求めに応じ、トレーサビリティ情報を甲に提出しなければならない。

（防衛省施設において作業を実施する場合の届出）

第５条

乙は、この契約の履行のため、納入先部隊等の防衛省施設（艦艇を含む。）において作業（情報システムの内容を知り得ないことが明らかである役務を除く。）を行う場合には、あらかじめ、作業従事者名簿（当該作業に従事する者の会社名及び氏名を一覧にした名簿をいう。以下同じ。）を書面により甲に提出又は送付し、甲の確認を得なければならない。

２　甲は、前項により乙から提出された作業従事者名簿について、第２条第１項及び第２条第３項により乙があらかじめ届け出ている従業員であることが確認できた場合には、名簿の写しに確認年月日及び確認者名又は部署の長の了解を得た上で確認部署名を記入し、乙に送付又は手交する。

３　乙は、納入先部隊等の防衛省施設（艦艇を含む。）における作業に当たり、作業従事者名簿の写しに作業従事者管理報告書（作業従事者名簿の従事者ごとに作業内容の予定と実績を日ごとに記録する報告書）を添付し、この契約の受領検査官又は使用責任者（会計法（昭和２２年法律第３５号）第２９条の１１第２項の補助者として甲が乙に通知した者をいう。）に書面により届け出なければならない（送付も可とする。）。納入に先立ち部隊等で現地技術確認試験等を行う場合には、受領検査官又は使用責任者に代えて、甲が乙に指定する当該部隊等に所属する者（作業確認者）に届出（送付も可とする。）を行うこととする。

（その他）

第６条　この特約条項各条の規定により、乙が甲又は防衛省に提出する資料、書面等の名称及び提出時期については、この特約条項の別表による。

２　別表に掲げる資料、書面等により甲に報告された内容について、サプライチェーン・リスクが懸念され、これを低減するための措置を講じる必要があると認められる場合に、甲は乙に是正を求めることがあり、乙は相当の理由があると認められるときを除きこれに応じなければならない。

３　甲は、乙の責めに帰すべき事由により、本情報システムに防衛省の意図しない変更が行われるなど不正が見つかり、この契約の目的が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。

４　前項の場合においては、主たる契約の解除に関する規定を準用する。

別表

情報システムの調達におけるサプライチェーン・リスク対応に関する特約条項に基づき提出する資料、書面等の提出時期
（第６条関係）

番号	名　称	条番号	資料、書面等の内容	提出時期	様式
1	管理手順及び品質保証体制（意図しない変更及び情報の窃取等の保証）	第1条第2項	防衛省の意図しない変更や情報の窃取等が行われないことを保証するための具体的な管理手順その他の品質保証体制を証明する書面（品質管理体制の責任者及び品質保証の各担当者がアクセス可能な範囲等を示した管理体制図を含めることを必須とする。）	契約の締結後遅滞なく	任意
2	不正発見時の追跡調査及び立入検査等の手順及び体制（原因調査及び排除）	第1条第3項	防衛省の意図しない変更が行われるなど不正が見つかったときに、追跡調査や立入検査等、防衛省と連携して原因を調査し、排除するための手順及び体制（防衛省の情報システムの運用・保守業務を行う契約にあっては、当該運用・保守業務において乙及び再委託先が行う作業履歴を記録し、防衛省の求めに応じてこれらを防衛省に提出する手順及び体制を含めることを必須とする。）	契約の締結後遅滞なく	任意
3	製品に対して意図しない変更が行われるリスクを回避するための試験実施要領	第1条第6項	乙が納入する製品に対して意図しない変更が行われるリスクを回避するための試験実施要領が記載された書面	試験実施前まで	任意
4	再委託業務に従事させる場合の届出書	第1条第7項	再委託の相手方の商号又は名称及び住所並びに再委託する業務の範囲、再委託の必要性について記載した書面	主たる契約条項の定めによる。	主たる契約条項の定めによる。
5	委託業務従事者届出書	第2条第1項	乙の資本関係等、作業従事者の氏名等及び情報システムに関する代表的な契約実績が記載された書面	委託先において業務を行う前まで	付紙様式第１
6	委託業務従事者届出書（変更）	第2条第2項	乙が本契約の履行に従事する従業員を変更する場合の届出	従業員を変更する前まで	付紙様式第１
7	再委託業務に従事させる場合の届出書	第2条第3項	再委託先の資本関係等、作業従事者の氏名等及び情報システムに関する代表的な契約実績が記載された書面	再委託先において、業務を行う前まで	付紙様式第２
8	再委託業務に従事させる場合の届出書（変更）	第2条第4項	乙が再委託先を変更する場合又は再委託先が再委託業務に従事する従業員を変更する場合の届出	再委託先又は再委託先が従事者を変更する前まで	付紙様式第２
9	使用を予定している機器等とCommon Criteria（ISO/IEC 15408)の比較表	第4条第1項	機器等にCommon Criteria（ISO/IEC 15408）レベル４を満たす製品の使用が困難な場合は、使用を予定している機器等と当該基準の比較表	当該製品を使用する前まで	任意
10	製品に対して意図しない変更が行われるリスクを回避するための試験実施要領	第4条第3項	再委託先が納入する製品に対して意図しない変更が行われるリスクを回避するための試験実施要領が記載された書面	試験実施前まで	任意
11	製造工程の履歴を記録する管理体制	第4条第6項	機器等の調達におけるトレーサビリティを確保するため、乙の製造する機器等について製造工程の履歴を記録する管理体制を証明する書類	契約の締結後遅滞なく （再委託する場合） 再委託先において、業務を行う前まで	任意
12	トレーサビリティ情報（機器等を構成する主要部品）	第4条第6項	機器等を構成する主要部品について製造事業者、製造事業者の国籍、製造国に関するトレーサビリティ情報が記載された書面	甲から求めがあった場合は速やかに	任意
13	作業従事者名簿届出書（追加）	第5条第1項	納入先部隊等での作業を実施する場合の作業従事者名簿	納入先部隊等での作業開始前	付紙様式第３
14	作業従事者管理報告書	第5条第3項	作業従事者管理報告書	納入先部隊等での作業開始前	付紙様式第４

付紙様式第１

委託業務従事者届出書（変更）

年　　月　　日

所　属
官　職
氏　名　　殿

住　　所
会 社 名
代表者名

下記契約に関して、情報システムの調達におけるサプライチェーン・リスク対応に関する特約条項第〇条の規定に基づき、下記のとおり届け出ます。

記

調 達 要 求 番 号 ……
認証（契約）番号・年月日 ……
品　名　・　数　量 ……

１　事業者

番号	資本関係	役員	業務実施場所	住所・ 電話番号	業務範囲

２　作業従事者

番号	所属・役職	氏名	専門性 （情報ｾｷｭﾘﾃｨに係る資格・研修実績・経験年数）

３　国籍

番号	国名	作業従事者数（名）	割合（%）

４　情報システムに関する代表的な契約実績

番号	契約相手方	契約システム名	契約年度

注１：契約の締結後、遅滞なく本様式で届け出ること。この場合、件名の（変更）を横線で消去すること。

注２：変更がある場合は、変更する旨を本様式により作業に従事する前までに、届け出ること。

付紙様式第２

再委託業務に従事させる場合の届出書（変更）

年　　月　　日

所　属
官　職
氏　名　　殿

住　　所
会 社 名
代表者名

下記契約に関して、情報システムの調達におけるサプライチェーン・リスク対応に関する特約条項第〇条の規定に基づき、下記のとおり届け出ます。

記

調 達 要 求 番 号 ……
認証（契約）番号・年月日 ……
品　名　・　数　量 ……

１　事業者名：

番号	資本関係	役員	業務実施場所	住所・ 電話番号	業務範囲

２　作業従事者

番号	所属・役職	氏名	専門性 （情報ｾｷｭﾘﾃｨに係る資格・研修実績・経験年数）

３　国籍

番号	国名	作業従事者数（名）	割合（%）

４　情報システムに関する代表的な契約実績

番号	契約相手方	契約システム名	契約年度

注１：再委託先において委託業務を行う前までに本様式で届け出ること。この場合、件名の（変更）を横線で消去すること。
注２：業務範囲については、いずれの会社（事業者）の下請業務か分かるよう、かつ、簡潔に記載すること。
注３：変更がある場合は、変更する旨を本様式により作業に従事する前までに、届け出ること。

付紙様式第３

作業従事者名簿届出書（追加）

年　　月　　日

所　属
官　職
氏　名　　殿

住　　所
会 社 名
代表者名

下記契約に関して、情報システムの調達におけるサプライチェーン・リスク対応に関する特約条項第〇条の規定に基づき、下記のとおり届け出ます。

記

調　達　要　求　番　号　……
認証（契約）番号・年月日　……
品　名　・　数　量　……

作業従事者名簿

番号	会社名（事業者名）	氏　　名

注１：納入先部隊等での作業開始前までに本様式で届け出ること。この場合、件名の（追加）を横線で消去すること。
注２：追加のあった場合は、速やかに追加した旨を本様式で届け出ること。

付紙様式第４

作　業　従　事　者　管　理　報　告　書

調　達　要　求　番　号　……
認証（契約）番号・年月日　……
品　名　・　数　量　……

（会社名　　）　　年　月　日

氏　名	作　業　内　容	
	予　定	実　績

注１：作業内容については、予定欄は契約相手方が、実績欄は受領検査官等が記入する。
注２：本届出書の提出時において、日々の作業内容の決定が困難な場合には、予定欄は作業開始前までに記入するものとする。

上記のとおり確認した。

年　月　日

所　属
官　職
氏　名

個人情報の取扱いに関する特約条項

甲及び乙は、個人情報の取扱いに関し、次の特約条項を定める。

1　乙は、善良な管理者の注意をもって委託業務を行うものとする。

2　乙は、個人情報の漏えい等の防止のため、適切な措置をとらなければならない。

3　乙は、この契約の履行に際し知得した秘密を第三者に漏らし、又は利用してはならない。

4　乙は、委託業務の全部又は一部を第三者に請け負わせる場合には、あらかじめ、書面により甲の承認を受けなければならない。

5　乙は、委託業務に係る個人情報を他の目的で利用してはならない。また、当該情報を第三者へ提供してはならない。

6　乙は、個人情報を複製する場合には、あらかじめ、書面により甲の承認を受けなければならない。

7　乙は、個人情報の管理につき、定期的に検査を行う。また、甲は、特に必要と認めた場合には、乙に対し、個人情報の管理状況に関し質問し、資料の提出を求め、又はその職員に乙の工場等の関係場所に立入調査をさせることができる。

8　委託業務に係る個人情報に関する事故等が発生した場合には、乙は、速やかに、その内容を甲に報告する。

9　甲は、乙が正当な理由なくこの契約の全部又は一部を履行しない場合には、この契約の全部又は一部を解除することができる。

談合等の不正行為に関する特約条項

甲及び乙は、談合等の不正行為に関し、次の特約条項を定める。

（談合等の不正行為に係る解除）

第１条　甲は、この契約に関して、次の各号の一に該当するときは、契約の全部又は一部を解除することができる。

一　公正取引委員会が、乙又は乙の代理人に対して私的独占の禁止及び公正取引の確保に関する法律（昭和２２年法律第５４号。以下「独占禁止法」という。）第７条又は第８条の２（同法第８条第１号若しくは第２号に該当する行為の場合に限る。）の規定による排除措置命令を行ったとき、同法第７条の２第１項（同法第８条の３において読み替えて準用する場合を含む。）の規定による課徴金の納付命令を行ったとき、又は同法第７条の４第７項若しくは第７条の７第３項の規定による課徴金の納付を命じない旨の通知を行ったとき。

二　乙又は乙の代理人（乙又は乙の代理人が法人の場合にあっては、その役員又は使用人）が刑法（明治４０年法律第４５号）第９６条の６若しくは第１９８条又は独占禁止法第８９条第１項の規定による刑の容疑により公訴を提起されたとき。

２　乙は、この契約に関して、乙又は乙の代理人が独占禁止法第７条の４第７項又は第７条の７第３項の規定による通知を受けた場合には、速やかに、当該通知文書の写しを甲に提出しなければならない。

（談合等の不正行為に係る違約金）

第２条　乙は、この契約に関して、次の各号の一に該当するときは、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、契約金額の１０分の１に相当する額を違約金として甲が指定する期日までに支払わなければならない。

一　公正取引委員会が、乙又は乙の代理人に対して独占禁止法第７条又は第８条の２（同法第８条第１項若しくは第２号に該当する行為の場合に限る。）の規定による排除措置命令を行い、当該排除措置命令が確定したとき。

二　公正取引委員会が、乙又は乙の代理人に対して独占禁止法第７条の２第１項（同法第８条の３において読み替えて準用する場合を含む。）の規定による課徴金の納付命令を行い、当該納付命令が確定したとき。

三　公正取引委員会が、乙又は乙の代理人に対して独占禁止法第７条の４第７項又は第７条の７第３項の規定による課徴金の納付を命じない旨の通知を行ったとき。

四　乙又は乙の代理人（乙又は乙の代理人が法人の場合にあっては、その役員又は使用人）が刑法第９６条の６若しくは第１９８条又は独占禁止法第８９条第

１項の規定による刑が確定したとき。

２　乙は、前項第４号に規定する場合に該当し、かつ次の各号の一に該当するときは、前項の契約金額の１０分の１に相当する額のほか、契約金額の１００分の５に相当する額を違約金として甲が指定する期日までに支払わなければならない。

一　公正取引委員会が、乙又は乙の代理人に対して独占禁止法第７条の２第１項及び第７条の３の規定による納付命令を行い、当該納付命令が確定したとき。

二　当該刑の確定において、乙が違反行為の首謀者であることが明らかになったとき。

三　乙が甲に対し、独占禁止法等に抵触する行為を行っていない旨の誓約書を提出しているとき。

３　乙は、契約の履行を理由として、前２項の違約金を免れることができない。

４　第１項及び第２項の規定は、甲に生じた実際の損害の額が違約金の額を超過する場合において、甲がその超過分の損害につき賠償を請求することを妨げない。

暴力団排除に関する特約条項

甲及び乙は、暴力団排除に関し、次の特約条項を定める。

（属性に基づく契約解除）

第１条　甲は、警視庁又は道府県警察本部の暴力団排除対策を主管とする課の長（以下「暴力団対策主管課長」という。）への照会、又は暴力団対策主管課長からの通知により、乙が次の各号の一に該当すると認められたときは、本契約を解除することができる。

（１）　法人等（個人、法人又は団体をいう。）の役員等（個人である場合はその者、法人である場合は役員又は支店若しくは営業所（常時契約を締結する事務所をいう。）の代表者、団体である場合は代表者、理事等、その他経営に実質的に関与している者をいう。）が、暴力団（暴力団員による不当な行為の防止等に関する法律（平成３年法律第77号）第２条第２号に規定する暴力団をいう。以下同じ）又は暴力団員（同法第２条第６号に規定する暴力団員をいう。以下同じ。）であるとき

（２）　役員等が、自己、自社若しくは第三者の不正の利益を図る目的、又は第三者に損害を加える目的をもって、暴力団又は暴力団員を利用するなどしているとき

（３）　役員等が、暴力団又は暴力団員に対して、資金等を供給し、又は便宜を供与するなど直接的あるいは積極的に暴力団の維持、運営に協力し、若しくは関与しているとき

（４）　役員等が、暴力団又は暴力団員であることを知りながらこれを不当に利用するなどしているとき

（５）　役員等が、暴力団又は暴力団員と社会的に非難されるべき関係を有しているとき

２　乙は、甲から求めがあった場合、乙の役員名簿（有価証券報告書に記載のもの（生年月日を含む。）。ただし、有価証券報告書を作成していない場合は、役職名、氏名及び生年月日の一覧表とする。）及び登記簿謄本の写しを提出するとともに、これらの提出書類から確認できる範囲での個人情報を警察に提供することについて同意するものとする。

（行為に基づく契約解除）

第２条　甲は、乙が自ら又は第三者を利用して次の各号の一に該当する行為をした場合は、本契約を解除することができる。

（１）　暴力的な要求行為

（２）　法的な責任を超えた不当な要求行為

（３）　取引に関して脅迫的な言動をし、又は暴力を用いる行為

（４）　偽計又は威力を用いて支担官等の業務を妨害する行為

（５）　その他前各号に準ずる行為

（暴力団排除に関する表明及び確約）
第３条　乙は、前２条各号のいずれにも該当しないことを表明し、かつ、将来にわたっても該当しないことを確約する。
２　乙は、前２条各号の一に該当する者（以下「排除対象者」という。）を下請負者等（下請負者（再下請負以降の全ての下請負者を含む。）、受任者(再委任以降の全ての受任者を含む。）及び下請負者又は受任者が当該契約に関して個別に契約する場合の当該契約の相手方をいう。以下同じ。）としないことを確約する。

（下請負者等に関する契約解除）
第４条　乙は、契約後に下請負者等が排除対象者であることが判明したときは、直ちに当該下請負者等との契約を解除し、又は下請負者等に対し契約を解除させるようにしなければならない。
２　甲は、乙が下請負者等が排除対象者であることを知りながら契約し、若しくは下請負者等の契約を承認したとき、又は正当な理由がないのに前項の規定に反して当該下請負者等との契約を解除せず、若しくは下請負者等に対し契約を解除させるための措置を講じないときは、本契約を解除することができる。

（損害賠償等）
第５条　甲は、第１条、第２条及び前条第２項の規定により本契約を解除した場合は、これにより乙に生じた損害について、何ら賠償ないし補償することは要しない。
２　乙は、甲が第１条、第２条及び前条第２項の規定により本契約を解除した場合において、甲に損害が生じたときは、その損害を賠償するものとする。
３　甲は、第１条、第２条及び前条第２項の規定によりこの契約の全部又は一部を解除した場合は、代金（一部解除の場合は、解除部分に相当する代金）の１０パーセントの金額を乙から違約金として徴収するものとする。
４　前項の規定は、甲に生じた実際の損害の額が違約金の額を超過する場合において、甲がその超過分の損害につき賠償を請求することを妨げない。

（不当介入に関する通報・報告）
第６条　乙は、自ら又は下請負者等が、暴力団、暴力団員、社会運動・政治運動標ぼうゴロ等の反社会的勢力から不当要求又は業務妨害等の不当介入（以下「不当介入」という。）を受けた場合は、これを拒否し、又は下請負者等をして、これを拒否させるとともに、速やかに不当介入の事実を甲に報告するとともに、警察への通報及び捜査上必要な協力を行うものとする。

債権譲渡制限特約の部分的解除のための特約条項

甲及び乙は、債権譲渡制限特約の部分的解除に関し、次の特約条項を定める。

（債権譲渡制限特約の部分的解除）

第１条　契約条項第〇条の規定にかかわらず、乙が中小企業者（中小企業信用保険法（昭和２５年法律第２６４号）第２条第１項に規定する者をいう。以下同じ。）である場合には、乙が流動資産担保融資保証制度を利用することが可能なときに限り、乙は、信用保証協会及び中小企業信用保険法施行令（昭和２５年政令第３５０号）第１条の２に規定する金融機関に対し、甲に対する売掛債権を譲渡することができる。

２　前項の規定に基づいて売掛債権の譲渡を行った場合には、甲の対価の支払による弁済の効力は、甲が予算決算及び会計令（昭和２２年勅令第１６５号）第４２条の２の規定に基づき、センター支出官に対して支出の通知を行った時点で効力を生ずるものとする。

３　前項の規定は、甲が、前渡資金から乙に対価を支払う場合には適用しない。

（譲渡可能な売掛債権）

第２条　前条第１項の規定により乙が譲渡することのできる売掛債権は、乙が当該売掛債権を譲渡しようとする時点において、乙が反対給付の履行を完了していることを甲が受領検査調書や納品書などにより確認しており、かつ、その金額が確定しているものとする。

（部分払、前金払又は概算払との関係）

第３条　乙は、第１条第１項の規定により売掛債権を譲渡しようとする時点において、既に甲からこの契約に係る代金の部分払、前金払又は概算払を受けている場合には、確定した契約金額と、既に支払を受けている金額との差額のみ譲渡することができる。

（承諾申請及び通知の様式）

第４条　乙は、甲に対し売掛債権の譲渡の承諾申請又は通知を行う場合には、承諾申請は様式１により、通知は様式２により行わなければならない。

（承諾の様式）

第５条　甲は、乙からの債権譲渡の承諾申請について承諾する場合には、譲渡の対象となる売掛債権が第２条に規定する要件を満たすことを確認の上、様式１に定めた事項を遵守することを条件として承諾するものとする。

（甲の権利及び利益）

第６条　甲及び乙は、乙の売掛債権譲渡が、契約不適合責任に係る権利、債務不履行等による契約の解除権、期限の利益、部分払、前金払又は概算払による債務の一部消滅、契約条項に基づく契約金額の変更その他契約内容の将来の変更、その他この契約に基づき甲が有する権利及び利益に一切の影響を及ぼさないよう、必要な措置を講じなければならない。

２　乙は、甲に対する売掛債権を譲渡しようとする場合には、あらかじめ信用保証協会及び金融機関に対し、原契約条項及びこの特約条項の内容を説明しなければならない。

（様式１）

債権譲渡承諾申請書

年　　月　　日

支出負担行為担当官　殿

住　所：
譲渡人：（甲）　　○○株式会社
代表者：
担当者：
連絡先：

住　所：
譲渡人：（乙）株式会社○○銀行
代表者：
担当者：
連絡先：

住　所：
譲渡人：（丙）○○信用保証協会
代表者：
担当者：
連絡先：

○○株式会社（以下「甲」という。）は、下記の○○契約条項第○条の規定に基づいて貴殿より○年○月○日に契約の履行の確認を受けました。つきましては、「債権譲渡承諾書」による貴殿の承諾がなされることを前提として、甲が○○契約に基づく代金債権（以下「譲渡対象債権」という。）を株式会社○○銀行（以下「乙」という。）及び○○信用保証協会（以下「丙」という。）に譲渡し、乙及び丙が譲渡対象債権を準共有として譲り受けたいので、「債権譲渡制限特約の部分的解除のための特約条項」第１条及び第４条の規定に基づき、貴殿の承認を得たく申請します。

その際、甲、乙及び丙は、下記の点につき、予め承諾していることを申し添えます。

１．譲渡対象債権に係る乙及び丙への支払については、従前どおり○○契約条項第○項第○号の規定に基づき、契約物品（又は役務）全体の完成、納入及びその確認を条件としてなされること。
２．乙及び丙は第三者に譲渡対象債権を再譲渡し、これに質権を設定し、又はその他譲渡対象債権の帰属並びに行使を阻害する行為を行わないこと。
３．国に対しては、譲渡対象債権に係る○○契約条項（当該契約条項に基づく変更契約を含む。）以外の責任は求めないこと、同契約条項に規定される甲の契約不適合責任については、従前どおり甲が継続して負担するものであること、及び債権譲渡に要する信用保証料、金利その他一切の費用については甲の負担であって、国に負担を求めることはないこと。
４．本件申請の内容について、直接確認することがあること。

また、同契約条項に基づく代金は、乙及び丙が指定する下記の口座にお振り込み下さい。

記

１．貴殿と甲との間で締結された　年　月　日付○○契約
(1)　調達要求番号
(2)　契 約 品 名
(3)　納　　期
(4)　認 証 番 号

２．譲渡債権の額
(1)　契約代金額　　金　　円
(2)　前払金等既受領済額　金　　円
(3)　差引譲渡対象債権額　金　　円

３．乙及び丙が指定する口座の表示
フリガナ　フリガナ
○○銀行○○支店・口座の種類
フリガナ
口座人名義○○・口座番号○○○○

注：本承諾申請書は必要に応じて修正することを妨げないが、「予め承諾している事項」の内容は修正してはならない。

○○○第○○○○号
年　　月　　日

債権譲渡承諾書

住　所：
譲渡人：（甲）　　○○株式会社
代表者：

住　所：
譲渡人：（乙）株式会社○○銀行
代表者：

住　所：
譲渡人：（丙）○○信用保証協会
代表者：

上記申請につき、○○契約に基づく譲渡対象債権の乙及び丙への譲渡については、下記の事項を甲、乙及び丙が遵守することを条件として、「債権譲渡制限特約の部分的解除のための特約条項第５条」の規定に基づき承諾します。

記

１．本承諾によって、○○契約（当該契約条項に基づく変更契約を含む。）に規定する国の権利及び利益には何ら変更がなく、また甲の本契約上の責任は一切軽減されるものではないこと。

２．乙及び丙は第三者に譲渡対象債権を再譲渡し、これに質権を設定し、又はその他譲渡対象債権の帰属並びに行使を阻害する行為を行わないこと。

３．国による代金の支払は、○○契約条項第○条の規定に基づき行われるものであること。

支出負担行為担当官

確認日付欄

（お問い合わせ先）
担当：
電話：

注：担当官は、本承諾書について修正が必要な場合には、適宜修正して差し支えない。

（様式２）
［内容証明郵便等の民法施行法第５条の規定による証書］

債権譲渡通知書

支出負担行為担当官　殿

住　所：
譲渡人：（甲）　　○○株式会社
代表者：
担当者：
連絡先：

住　所：
譲渡人：（乙）株式会社○○銀行
代表者：
担当者：
連絡先：

住　所：
譲渡人：（丙）○○信用保証協会
代表者：
担当者：
連絡先：

○○株式会社（以下「甲」という。）は、下記の○○契約条項第○条の規定に基づいて貴殿より○年○月○日に契約の履行の確認を受け【［準確定契約及び概算契約の場合は記述］、かつ○年○月○日に契約金額が確定し】ました。よって、甲が○○契約に基づく代金債権（以下「譲渡対象債権」という。）を株式会社○○銀行（以下乙」という。）及び○○信用保証協会（以下「丙」という。）に譲渡し、乙及び丙が譲渡対象債権を準共有として譲り受けました。つきましては、「債権譲渡制限特約の部分的解除のための特約条項」第１条及び第４条の規定に基づき、本書をもってご通知申し上げます。

その際、甲、乙及び丙は、下記の点につき、予め承諾していることを申し添えます。

１．譲渡対象債権に係る乙及び丙への支払については、従前どおり○○契約条項第○項第○号の規定に基づき、契約物品（又は役務）全体の完成、納入及びその確認を条件としてなされること。
２．乙及び丙は第三者に譲渡対象債権を再譲渡し、これに質権を設定し、又はその他譲渡対象債権の帰属並びに行使を阻害する行為を行わないこと。
３．国に対しては、譲渡対象債権に係る○○契約条項（当該契約条項に基づく変更契約を含む。）以外の責任は求めないこと、同契約条項に規定される甲の契約不適合責任については、従前どおり甲が継続して負担するものであること、及び債権譲渡に要する信用保証料、金利その他一切の費用については甲の負担であって、国に負担を求めることはないこと。
４．本件通知の内容について、直接確認することがあること。

また、同契約条項に基づく代金は、乙及び丙が指定する下記の口座にお振り込み下さい。

記

１．貴殿と甲との間で締結された　年　月　日付○○契約
(1)　調達要求番号
(2)　契 約 品 名
(3)　納　　期
(4)　認 証 番 号

２．譲渡債権の額
(1)　契約代金額　　金　　円
(2)　前払金等既受領済額　金　　円
(3)　差引譲渡対象債権額　金　　円

３．乙及び丙が指定する口座の表示
○○銀行（フリガナ）○○支店（フリガナ）・口座の種類
口座人名義（フリガナ）○○・口座番号○○○○

注：本通知は必要に応じて修正することを妨げないが、契約履行の確認日に係る部分及び契約金額の確定日に係る部分並びに「予め承諾している事項」の内容は修正してはならない。