第４補給処公示第２２６号
令和５年８月３０日

分任支出負担行為担当官
航空自衛隊第４補給処調達部長
藤本　芳信

契約条項の一部改正について

１　「代金の確定に関する特約条項（支払限度）」別紙様式２中「別紙様式２」を「別紙様式第２」に改めました。
２　「代金の確定に関する特約条項（中途見直し条項付支払限度）」別紙様式２中「別紙様式２」を「別紙様式第２」に改めました。
３　「代金の確定に関する特約条項（概算）」中「別紙　　を「別紙様式第１」に、
別紙様式第１」
別紙様式２中「別紙様式２」を「別紙様式第２」に改めました。
４　「代金の確定に関する特約条項（中途見直し条項付概算）」別紙様式２中「別紙様式２」を「別紙様式第２」に改めました。
５　「日米了解事項覚書に関する特約条項」中「日本国防衛庁」を「日本国防衛省」に改めました。
６　「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」を別表のとおり一部改めました。

添付書類：別表

別表

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の一部改正表

改正前	改正後
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	**装備品等及び役務の調達における情報セキュリティの確保に関する特約条項**
第５条 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。	第５条 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とする。
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**	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**
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 (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。	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 (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は、本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。
第５　組織のセキュリティ ２　経営者等及び取扱者の責務 (3) 情報セキュリティの確保 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。 ４　第三者 (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５　組織のセキュリティ ２　経営者等及び取扱者の責務 (3) 情報セキュリティの確保 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。 ４　第三者 (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は、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 ４　保護すべき情報の持ち出し及び送達 (3) 持ち出し及び送達の際の表示 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。	第６　保護すべき情報の管理 ４　保護すべき情報の持ち出し及び送達 (3) 持ち出し及び送達の際の表示 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。
第８　物理的及び環境的セキュリティ	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。 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。） 4　保護システムに対する物理的セキュリティ対策 (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 (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。	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５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。 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「入退管理機器」という。） 4　保護システムに対する物理的セキュリティ対策 (4) その他の保護システムに対する管理策については、第９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 (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１１　情報セキュリティ事故等発生時の対応 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。	第１１　情報セキュリティ事故等発生時の対応 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、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。
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** 第３　構成管理 2　ベースライン構成設定等 (3) 構成設定の方法 イ　アクセス権限の特定等 (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。 (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。	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** 第３　構成管理 2　ベースライン構成設定等 (3) 構成設定の方法 イ　アクセス権限の特定等 (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、当該アクセス権限を使用することがふさわしい者に限り使用させることとする。 (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。	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、イに規定するブラックリスト又はウ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。
第６　識別及び認証 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。 (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。 (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。 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。	第６　識別及び認証 １　識別及び認証等の実施 (1) 識別の実施 ア　アカウント管理者は、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。 (2) 認証の実施 ア　アカウント管理者は、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。 (3) パスワードによる認証の実施 ア　アカウント管理者は、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。 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、他の者が容易に復号できない方式を用いて保存又は伝送するものとする。
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 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。	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 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、取得困難である場合は、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、ウに規定する措置を行うものとする。

(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。 第１０　脆弱性スキャン等 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。 (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１２　システムメンテナンス等 ２　システムメンテナンス等の実施 (4) システムメンテナンス等の監督等 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。	(2) システムログの分析 ア　保護システム担当者は、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。 第１０　脆弱性スキャン等 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の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。 (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とする。 第１２　システムメンテナンス等 ２　システムメンテナンス等の実施 (4) システムメンテナンス等の監督等 イ　アにより指定された監督者は、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。