付紙第４

秘密取扱情報システムに関する特約条項

（適用範囲）

第１条　秘密を情報システムで取り扱う場合には、この特約の定めを適用する。

２　この特約の定めに基づいて執られる措置は、主たる契約条項の定めに基づいて執られる措置と整合的に行われなければならない。

（定義）

第２条　この特約において次の各号に掲げる用語の意義は、それぞれ当該各号に定めるとおりとする。

⑴　ユーザーセッション　秘密取扱情報システム利用者が実行するそれぞれのアプリケーションの論理的な経路をいう。

⑵　ホワイトリスト　秘密取扱情報システムにインストールし、及び実行することが認められたソフトウェアのリストをいう。

⑶　構成設定　秘密取扱情報システムの構成要素（情報システムを構成するハードウェア、ソフトウェア、ネットワーク及び記憶媒体をいう。以下同じ。）の種類、バージョン等及び当該構成要素の機能の決定並びに構成要素の動作等を制御する設定値を決定することをいう。

⑷　サプライチェーン・リスク　秘密取扱情報システムに関する調達に際し、秘密取扱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。

⑸　電子政府推奨暗号等　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。

（組織のセキュリティ）

第３条　乙は、秘密を秘密取扱情報システムで取り扱うための体制を整備し、これを維持しなければならない。

２　乙は、秘密取扱情報システム利用者以外の者に秘密取扱情報システムを利用させてはならない。

３　主たる契約条項の定め及びこの特約の定めに基づいて秘密取扱情報システムに関して執られる措置については、秘密取扱情報システムを利用した秘密

の取扱いのため必要な範囲において、関係社員その他の従業者に徹底するものとする。この場合において、秘密取扱情報システムに関する情報の供覧の範囲を必要最小限の範囲にとどめ、秘密取扱情報システムの管理及び運用に関する文書を適切に保護しなければならない。

4　乙は、その秘密保全施設等において関係社員と協力して乙のために特定資料等の取扱いの業務を行う下請負事業者関係社員に対し、秘密取扱情報システムの利用を認めることができる。この場合においては、主たる契約条項の定めに従って行う下請負事業者との間の協議に下請負事業者関係社員による秘密取扱情報システムの利用に関することを含めなければならない。

5　前項の場合における第３項の規定の適用については、「関係社員その他の従業者」とあるのは、「関係社員その他の従業者及び乙の秘密保全施設等において関係社員と協力して乙のために特定資料等の取扱いの業務を行う下請負事業者関係社員」とする。

（体制）

第４条　乙は、秘密取扱情報システムごとに秘密取扱情報システム利用者を指定しなければならない。秘密取扱情報システム利用者は、関係社員の中から、乙が当該秘密取扱情報システムを用いて特定資料等の取扱いの業務を行う上で必要最小限の範囲で指定するものとする。

2　乙は、秘密取扱情報システムごとに秘密取扱情報システム管理者（秘密取扱情報システムの運用管理に責任を負う管理者をいう。以下同じ。）を指定しなければならない。秘密取扱情報システム管理者は、当該秘密取扱情報システムの秘密取扱情報システム利用者の中から、ふさわしいと認める者を指定するものとする。

3　乙は、秘密取扱情報システムごとに秘密取扱情報システム担当者（秘密取扱情報システム管理者の業務遂行を補助する者をいう。以下同じ。）を指定しなければならない。秘密取扱情報システム担当者は、当該秘密取扱情報システムの秘密取扱情報システム利用者の中から、ふさわしいと認める者を指定するものとする。

4　乙は、秘密取扱情報システムごとにアカウント管理者（秘密取扱情報システムへ論理的にアクセスするための権利の設定、変更、削除等の管理を行う者をいう。以下同じ。）を指定しなければならない。アカウント管理者は、秘密取扱情報システムの秘密取扱情報システム担当者の中から、ふさわしいと認める者を指定するものとする。

５　秘密取扱情報システム管理者は、秘密取扱情報システムの適正な管理に影響がないと判断される場合には、秘密取扱情報システム担当者及びアカウント管理者を兼ねることができる。
６　秘密取扱情報システム担当者は、秘密取扱情報システムの適正な管理に影響がないと判断される場合には、アカウント管理者を兼ねることができる。
７　前条第４項の場合における第１項の規定の適用については、「関係社員」とあるのは、「関係社員及び乙の秘密保全施設等において関係社員と協力して乙のために特定資料等の取扱いの業務を行う下請負事業者関係社員」とする。この場合において、第２項から第４項までの規定にかかわらず、下請負事業者関係社員である秘密取扱情報システム利用者を秘密取扱情報システム管理者、秘密取扱情報システム担当者又はアカウント管理者に指定してはならない。
８　前各項の規定による指定（新たな指定により元々の指定を解除する場合を含む。）は、装備政策部長が別に定めるところにより行うものとする。

（同意書）
第５条　乙は、秘密取扱情報システム利用者を指定した場合には、秘密取扱情報システムの利用は監視され、利用履歴が記録されること等について、当該秘密取扱情報システム利用者の同意を得なければならない。
２　前項の同意は、装備政策部長が別に定めるところにより行うものとする。

（総括者）
第６条　乙は、総括者に、次の各号に掲げる事項その他秘密取扱情報システムにおける特定資料及び秘密取扱情報システムに係る特定物件の取扱いに関して必要な措置を講じさせなければならない。
⑴　秘密取扱情報システムの管理及び運用が秘密保全規則等の下で的確に行われることを確保すること。
⑵　秘密取扱情報システムを管理し、及び運用する組織のセキュリティを整備すること。
⑶　秘密取扱情報システム利用者に対する教育を行うこと。
⑷　秘密取扱情報システム及び可搬記憶媒体の廃棄を承認し、その実施を監督すること。
⑸　事故への対処体制を整備し、及び事故等に対応し、並びにぜい弱性への対処を監督すること。
⑹　リスク査定を監督すること。
⑺　点検の実施要領を承認し、及び点検の実施を監督すること。

⑻　秘密取扱情報システムセキュリティ実装計画（ＳＳＰ）を承認し、その実施を監督すること。

（秘密取扱情報システム管理者）

第７条　乙は、秘密取扱情報システム管理者に、次の各号に掲げる事項その他秘密取扱情報システムの管理のために必要な措置を講じさせなければならない。

⑴　電磁的記録である秘密（以下「秘密のデータ」という。）を分類し、及び管理すること。

⑵　物理的セキュリティ対策の実施を監督すること。

⑶　可搬記憶媒体を管理すること。

⑷　秘密取扱情報システム及び可搬記憶媒体の廃棄を申請し、及びこれらを廃棄すること。

⑸　ぜい弱性対処記録及びぜい弱性スキャン分析結果記録簿を承認し、並びにぜい弱性に対処すること。

⑹　リスク査定を実施すること。

⑺　点検の実施要領を作成し、及び点検を実施すること。

⑻　秘密取扱情報システムセキュリティ実装計画（ＳＳＰ）を作成し、これにのっとった措置を執ること。

⑼　セキュリティエンジニアリングの原則を承認すること。

⑽　構成設定を監督し、証明するための目録を承認し、及び構成管理の実施を監督すること。

⑾　基本的な防御対策の実施を監督すること。

⑿　アクセス制御方針を承認し、その実施を監督すること。

⒀　アカウント管理計画（秘密取扱情報システム利用者のアカウントを管理する計画をいう。以下同じ。）を承認し、アカウント（秘密取扱情報システムに論理的にアクセスするための権利をいう。以下同じ。）の管理を監督すること。

⒁　ログオン及びユーザーセッションの管理を監督すること。

⒂　識別管理簿（アカウント及び秘密取扱情報システムを構成する機器を識別するために付与した識別子を管理するための帳簿をいう。以下同じ。）を承認し、識別及び認証を監督すること。

⒃　秘密保全施設等における通信の制御を監督すること。

⒄　運用状況の監視及び対応を監督すること。

⒅　システムログの取得及び分析を監督すること。

⒆　システムログのバックアップ等を監督すること。

⑳　システムメンテナンス等計画を承認し、その実施を監督すること。
㉑　構成要素に関するサプライチェーン・リスクを管理すること。

（秘密取扱情報システム担当者）
第８条　乙は、秘密取扱情報システム担当者に、次の各号に掲げる事項その他秘密取扱情報システム管理者の業務遂行を補助するために必要な措置を講じさせなければならない。
⑴　物理的セキュリティ対策を行うこと。
⑵　可搬記憶媒体を管理する簿冊（以下「可搬記憶媒体管理簿」という。）を作成し、可搬記憶媒体の点検をすること。
⑶　セキュリティエンジニアリングの原則を適用すること。
⑷　構成設定の状況を把握し、これを証明するための目録を作成し、及び構成管理を行うこと。
⑸　基本的な防御対策を行うこと。
⑹　アクセス制御方針を作成し、アクセスを制御すること。
⑺　秘密保全施設等における通信を制御すること。
⑻　運用状況の監視を行い、及びその結果に対応すること。
⑼　システムログを取得し、及びその分析を行うこと。
⑽　ぜい弱性対処記録及びぜい弱性スキャン分析結果記録簿を作成すること。
⑾　システムログのバックアップ等を行うこと。
⑿　システムメンテナンス等計画を作成し、メンテナンス等を行うこと。
⒀　その他秘密取扱情報システム管理者から命じられたこと。

（アカウント管理者）
第９条　乙は、アカウント管理者に、次の各号に掲げる事項その他秘密取扱情報システムのアカウントの管理のために必要な措置を講じさせなければならない。
⑴　アカウント管理計画を作成し、秘密取扱情報システムのアカウントの管理を行うこと。
⑵　ログオン及びユーザーセッションを管理すること。
⑶　識別管理簿を作成し、識別及び認証を行うこと。
⑷　その他秘密取扱情報システム管理者から命じられたこと。

（秘密取扱情報システム利用者への教育）

第１０条　乙は、秘密取扱情報システム利用者に対し、その職責及び利用する秘密取扱情報システムに応じた技術的及び専門的な教育を行わなければならない。
２　前項の規定の実施に当たっては、主たる契約条項に定める教育と整合的に行うものとする。

（秘密取扱情報システムの設置）
第１１条　乙は、秘密取扱情報システムを秘密保全施設等の内部に設置し、秘密取扱情報システムセキュリティ実装計画（ＳＳＰ）に従って管理し、及び運用しなければならない。
２　秘密取扱情報システムは、有線により構成要素が配線接続されなければならず、他の情報システム又は秘密取扱情報システムが設置された秘密保全施設等の外部との通信は、完全に遮断されなければならない。
３　前項の規定にかかわらず、その構成要素が複数の秘密保全施設等の内部に設置される秘密取扱情報システムであって、秘密保全施設等の間を有線接続されるものとして防衛装備庁が定める基準を満たす秘密取扱情報システムは、複数の秘密保全施設等の構成要素の間で通信を行うことができる。
４　秘密取扱情報システムに接続できる可搬記憶媒体は、当該秘密取扱情報システムが設置された秘密保全施設等から持ち出してはならない。ただし、特定資料等を当該秘密保全施設等の外にある者への交付のため、秘密保全施設等の外部への持出しの許可を得た可搬記憶媒体は、この限りでない。

（秘密取扱情報システムセキュリティ実装計画（ＳＳＰ）の更新）
第１２条　乙は、秘密取扱情報システムセキュリティ実装計画（ＳＳＰ）を定期的に見直し、その内容を常に最新のものに更新しなければならない。
２　乙は、秘密取扱情報システムセキュリティ実装計画（ＳＳＰ）を変更した場合には、甲に届け出なければならない。
３　乙は、サプライチェーン・リスクに留意して構成要素を選定するものとする。
４　乙は、甲から秘密取扱情報システムセキュリティ実装計画（ＳＳＰ）を見直すよう求められたときは、これに応じなければならない。

（秘密のデータの管理）
第１３条　乙は、秘密のデータを他の電磁的記録から明確に区別し、秘密保全施設等内で管理しなければならない。

２　前項の規定の実施に当たっては、秘密のデータの管理に関する帳簿を作成するものとする。
３　秘密のデータは、当該秘密取扱情報システムで使用することが認められた可搬記憶媒体に保存しなければならない。
４　秘密のデータは、秘密取扱情報システムの記憶媒体に保存してはならない。
５　前２項の規定にかかわらず、その記憶媒体に秘密のデータを保存するものとして防衛装備庁が定める基準を満たす秘密取扱システムは、その記憶媒体に秘密のデータを保存することができる。

（可搬記憶媒体の管理）
第１４条　乙は、秘密取扱情報システムで可搬記憶媒体を使用する場合には、次の各号に定める事項その他可搬記憶媒体の管理のために必要な事項を定めなければならない。
⑴　可搬記憶媒体管理簿を作成すること。
⑵　可搬記憶媒体の状況及び可搬記憶媒体管理簿の内容を定期的に点検すること。
⑶　可搬記憶媒体を使用できる者を必要最小限に制限すること。
⑷　可搬記憶媒体の使用は秘密取扱情報システム管理者が許可すること。
⑸　可搬記憶媒体に秘密のデータを記録する場合には、強固な暗号鍵を用い、最新の電子政府推奨暗号等により暗号化し、暗号鍵を厳格に管理すること。

２　乙は、可搬記憶媒体管理簿に記載されていない可搬記憶媒体の秘密取扱情報システムへの接続を拒否する設定にしなければならない。
３　乙は、可搬記憶媒体を廃棄する場合には、これを秘密のデータが復元できないよう物理的に破壊しなければならない。なお、一の秘密取扱情報システムで使用された可搬記憶媒体を他の情報システムで再利用してはならない。
４　可搬記憶媒体管理簿は、装備政策部長が別に定めるところにより作成するものとする。

（アクセス制御）
第１５条　乙は、アカウント管理計画を作成し、これに従って、秘密取扱情報システム利用者の職責に応じた必要最小限の権限を付与し、アカウントの利用を管理しなければならない。付与したアカウントは、定期に及び必要に応じて、見直すものとする。

２　乙は、秘密取扱情報システムへのログオン及びユーザーセッションを管理し、秘密取扱情報システムの不正な利用を防止しなければならない。
３　アカウント管理計画は、装備政策部長が別に定めるところにより作成するものとする。

（識別及び認証）
第１６条　乙は、識別管理簿を作成しなければならない。
２　乙は、秘密取扱情報システムで用いられる識別子及び認証子を厳格に管理し、多要素認証を含め、秘密取扱情報システムで用いられる認証が厳正に行われるよう措置しなければならない。
３　識別管理簿は、装備政策部長が別に定めるところにより作成するものとする。

（システム監視）
第１７条　乙は、秘密取扱情報システムに対する不正なアクセス、利用者権限等の不正な使用、不正な通信、悪意のあるコードの侵入等を検知するため、秘密取扱情報システムの運用の状況を監視しなければならない。
２　乙は、前項の規定による監視の結果を記録し、組織横断的な対策に取り組むものとする。

（システムログの取得・分析、バックアップ）
第１８条　乙は、不正な操作又は通信を探知するため、秘密取扱情報システムについて、秘密のデータの取扱いに関する記録、秘密取扱情報システム利用者ごとの操作の記録その他秘密取扱情報システムの操作、入出力、通信等の記録を自動的に取得しなければならない。
２　乙は、前項の規定により取得した記録について、定期的に分析しなければならない。分析に当たっては、全体的かつ横断的にシステムログを精査するものとし、反復継続性に乏しい特異な事象、秘密取扱情報システム利用者による異常な操作、システムの異常な挙動等の有無を判断しなければならない。
３　乙は、第１項の規定により取得したシステムログについて、定期的にバックアップし、その機密性、完全性及び可用性を確保しなければならない。
４　乙は、第１項及び第２項の規定によるシステムログの分析の結果を記録しなければならない。

（ぜい弱性スキャン）

第１９条　乙は、秘密取扱情報システムについて潜在的に懸念される脅威を探知するため、定期に及び必要に応じて、秘密取扱情報システムのぜい弱性スキャンを行い、その結果を分析しなければならない。
２　前項の分析は、情報システムを巡る脅威に関する最新の動向に係る技術的な知見を踏まえて行うものとする。
３　乙は、前２項の規定によるぜい弱性スキャンの結果を記録し、組織横断的な対策に取り組むものとする。

（ぜい弱性対処）
第２０条　乙は、秘密取扱情報システムにぜい弱性が発見され、又は検知された場合の対処の責任者及び当該責任者の下で行う対処手順を整えなければならない。
２　乙は、発見され、又は検知されたぜい弱性を速やかに修正し、又は対策を講じなければならない。

（リスク査定及び点検）
第２１条　乙は、秘密取扱情報システムにおける特定資料の取扱い及び秘密取扱情報システムに係る特定物件の取扱いに関するリスク査定を実施しなければならない。
２　乙は、秘密取扱情報システムにおける特定資料の取扱い及び秘密取扱情報システムに係る特定物件の取扱いについて定期的に点検を行わなければならない。
３　前２項の規定によりリスク査定又は点検を行うに当たっては、主たる契約条項に定める措置と整合的に行うものとする。
４　第１項又は第２項の規定によりリスク査定又は点検を行った場合において、改善事項が判明したときは、速やかに措置しなければならない。

（メンテナンス等）
第２２条　乙は、定期的にかつ計画的に、秘密取扱情報システムの保守、点検、診断、修理、整備、アップグレードその他の秘密取扱情報システムのメンテナンス等を行わなければならない。
２　前項のメンテナンス等は、原則として、秘密取扱情報システム利用者のうちふさわしい者として指定されたものが行うものとし、秘密の保全のための措置を講じるものとする。
３　乙は、前２項の規定によるメンテナンス等の状況を記録しなければならない。

（秘密取扱情報システムの廃棄）

第２３条　乙は、秘密取扱情報システムを廃棄する場合には、秘密のデータが復元できないよう、記憶媒体を物理的に破壊しなければならない。

２　秘密取扱情報システムは、その全部又は一部を他の目的の情報システムとして再利用してはならない。

３　秘密取扱情報システムの廃棄は、総括者が監督するものとする。

４　前２項の規定の実施に当たっては、装備政策部長が別に定めるところにより記録するものとする。

（事故）

第２４条　乙は、特定資料等の漏えい、紛失、破壊等の事故が秘密取扱情報システムの利用に伴って発生した場合の対処の責任者、当該責任者の下で行う対処手順その他事故への対処体制を整えなければならない。

２　前項の事故への対処体制を整えるに当たり、乙は、秘密取扱情報システムの特性に応じた証跡を収集するものとする。

３　事故への対処体制を整え、及び事故等に対応するに当たっては、主たる契約条項に定める措置と整合的に行うものとする。

（取扱いの記録）

第２５条　乙は、秘密取扱情報システムの取扱いについては、装備政策部長が別に定めるところにより、帳簿に記録しなければならない。この場合において、乙は、当該帳簿の内容が改ざんされないよう措置しなければならない。

２　乙は、前項の帳簿の内容が改ざんされないよう措置した上で、装備政策部長が別に定める期間、同項の帳簿を保管しなければならない。保管期間の経過後の当該帳簿の廃棄に当たっては、あらかじめ甲の確認を受けるものとする。

（その他）

第２６条　この特約条項の実施の細部については、別に防衛装備庁装備政策部長が定めるところによるものとする。