調達における情報セキュリティ基準

1　趣旨

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、情報セキュリティ対策を本基準に則り実施するものとする。

なお、従来から情報セキュリティ対策を実施している場合は、本基準に則り、必要に応じ新たに追加又は拡充を実施するものとする。また、本基準において示されている対策について、合理的な理由がある場合は、適用の除外について、防衛省の確認を受けることができる。

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) 「防衛関連企業」とは、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（防経装第９２４６号。２１．７．３１。以下「確保通達」という。）第２項第８号に規定する防衛関連企業をいう。

(2) 「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。

(3) 「保護すべき情報」とは、確保通達第２項第１号に規定する保護すべき情報をいう。

(4) 「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。

(5) 「保護すべきデータ」とは、保護すべき情報に属する電子データをいう。

(6) 「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。

(7) 「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。

(8) 「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。

(9) 「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。

(10) 「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等を定めたものをいう。

(11) 「情報セキュリティ基準」とは、本基準に基づき、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。

(12) 「情報セキュリティ実施手順」とは、情報セキュリティ基準に基づき、防衛関連企業が実施する情報セキュリティ対策の具体的な実現手法を定めたものをいう。

(13) 「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、情報セキュリティ基準及び情報セキュリティ実施手順をいう。

(14) 「下請負者」とは、確保通達第２項第９号に規定する下請負者をいう。

(15) 「第三者」とは、当該装備品等及び役務の調達において、防衛省と直接契約関係に

あるもの以外のものをいう。
(16)「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、破壊等の事故が発生し、又はそれらの疑いがある状態をいう。
(17)「情報セキュリティ事象」とは、情報セキュリティ基本方針等への違反のおそれのある状態及び情報セキュリティ事故につながるおそれのある状態をいう。
(18)「情報システム」とは、ハードウェア、ソフトウェア（プログラムの集合体をいう。）、ネットワーク又は記憶媒体で構成されるものであって、これら全体で業務処理を行うものをいう。
(19)「取扱施設」とは、保護すべき情報の取扱い及び保管を行う施設をいう。
(20)「利用者」とは、情報システムを利用する者をいう。
(21)「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、コンピュータウィルス、トロイの木馬及びスパイウェア等をいう。
(22)「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。
(23)「秘匿化」とは、情報の内容又は情報の存在を隠すことを目的に、情報の変換等を行うことをいう。
(24)「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。
(25)「送達」とは、有体物である文書等を物理的に移動させることをいう。
(26)「電子メール等」とは、メッセージ通信（電子メール、チャット等）及びファイルの送受信（FTP 等）をいう。
(27)「経営者等」とは、経営者又は受注案件を処理する部門責任者をいう。
(28)「管理者権限」とは、情報システムの管理（利用者の登録及び登録削除、利用者のアクセス制御等）をするために付与される権限をいう。

3　対象

(1) 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) 対象者は、防衛関連企業において保護すべき情報に接するすべての者（派遣社員、契約社員、パート及びアルバイト等を含む。以下「取扱者」という。）とする。

4　情報セキュリティ基本方針等の作成

防衛関連企業は、情報セキュリティ基本方針等を作成するものとし、その際及び変更する場合は、本基準との適合性について、防衛省の確認を受けるものとする。

5　情報セキュリティの基本方針等

(1) 情報セキュリティ基本方針及び情報セキュリティ基準

経営者等は、情報セキュリティ基本方針及び情報セキュリティ基準を承認し、保護すべき情報を取り扱う可能性のあるすべての者（取扱者を含む。）に周知しなければならない。また、必要に応じて保護すべき情報を取り扱う下請負者に周知しなければ

ならない。

(2) 情報セキュリティ基本方針等の見直し

経営者等は、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なければならない。※ 6(1)エ 情報セキュリティの実施状況の監査を参照。

6 組織のセキュリティ

(1) 内部組織

ア 情報セキュリティに対する経営者等の責任

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及び情報セキュリティ基本方針等の承認等を通して、組織内における情報セキュリティの確保に努めなければならない。

イ 責任の割当て

防衛関連企業は、保護すべき情報に係るすべての情報セキュリティの責任を明確にするため、保護すべき情報の管理全般に係る総括的な責任者及び保護すべき情報と関連する資産ごとに、それぞれ管理責任者（以下「管理者」という。）を指定しなければならない。

ウ 守秘義務

防衛関連企業は、８(4) に基づき取扱者に要求する事項を特定したのち、取扱者との間で守秘義務を定めた契約又は合意をしなければならない。また、要求事項の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状況の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、見直しを実施した上、必要に応じて要求事項を修正しなければならない。

エ 情報セキュリティの実施状況の監査

防衛関連企業は、情報セキュリティの実施状況について、定期的及び情報セキュリティの実施に係る重大な変化が発生した場合には、監査を実施し、その結果を保存しなければならない。また、必要に応じて是正措置をとらなければならない。

(2) 保護すべき情報を取り扱う下請負者

防衛関連企業は、当該契約の履行に当たり、保護すべき情報を取り扱う業務を請け負わせる場合、本基準に基づく情報セキュリティ対策の実施を当該下請負者との間で契約し、当該業務を始める前に、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、防衛省に届け出なければならない。ただし、輸送その他の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。

(3) 第三者

ア 第三者への開示の禁止

防衛関連企業は、第三者（保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に保護すべき情報を開示又は漏えいしてはならない。やむを得ず保護すべき情報を第三者（保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に開示しようとする場合には、あらかじめ、書面により防衛省の許可を受けなければならない。

イ　第三者に関係したリスクの管理

防衛関連企業は、第三者に取扱施設への立入りを許可する場合、想定されるリスクを明確にした上、対策を定めなければならない。

ウ　第三者に対する立入りの許可

防衛関連企業は、定めた対策が満たされた場合を除き、取扱施設に対する第三者の立入りを許可してはならない。

7　保護すべき情報の管理

(1) 分類の指針

防衛関連企業は、保護すべき情報を明確に分類することができる情報の分類体系を定めなければならない。

(2) 保護すべき情報の取扱い

ア　保護すべき情報の目録

防衛関連企業は、保護すべき情報の現状（保管場所等）が分かる目録を作成し、維持しなければならない。

イ　取扱いの管理策

防衛関連企業は、保護すべき情報を取扱施設において取り扱うとともに、保護すべき情報を接受、作成、製作、複製、持ち出し（貸出を含む。）及び破棄する場合は、記録しなければならない。

なお、保護すべき情報を個人が所有する情報システム及び可搬記憶媒体において取り扱ってはならず、やむを得ない場合は、事前に防衛省の許可を得なければならない。また、契約終了後は、防衛省の指示に従い、返却、提出等必要な措置をとらなければならない。

ウ　保護すべき情報の保管

防衛関連企業は、保護すべき情報を施錠したロッカー等に保管し、その鍵を適切に管理しなければならない。

エ　保護すべき情報の持ち出し

防衛関連企業は、経営者等が持ち出しに伴うリスクを回避することができると判断した場合を除き、保護すべき情報を取扱施設外に持ち出してはならない。

なお、持ち出しをする場合は、記録するものとする。

オ　保護すべき情報の破棄

防衛関連企業は、接受、作成、製作又は複製した保護すべき情報を破棄する場合は、復元できないように裁断等確実な方法により破棄し、その旨を記録するものとする。

なお、保護すべきデータを保存した可搬記憶媒体を破棄する場合は、10(4) ウに

基づき破棄するものとする。

カ　該当部分の明示

防衛関連企業は、保護すべき情報を作成、製作又は複製した場合は、保護すべき情報である旨の表示を行うものとする。その際、保護すべき情報を記録する箇所に、下線を引いて明示する、枠で囲んで明示する又は文頭及び文末に括弧を付して明示する等の措置をしなければならない。

8　人的セキュリティ

(1) 経営者等の責任

経営者等は、保護すべき情報の取扱者を必要最低限とするとともに、ふさわしいと認める者を充てなければならない。また、情報セキュリティ基本方針等を取扱者に遵守させなければならない。

(2) 情報セキュリティ教育及び訓練

防衛関連企業は、取扱者の職務に関連する組織の方針及び手順並びに関連する法令等について、教育及び訓練を定期的に実施しなければならない。

(3) 違反者への対処方針

防衛関連企業は、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手続を定めなければならない。

(4) 取扱者の責任

取扱者は、在職中及び離職後において、契約の履行において知り得た保護すべき情報を第三者（保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に漏えいしてはならない。

(5) 保護すべき情報の返却

防衛関連企業は、取扱者の雇用契約の終了又は取扱者との契約合意内容の変更に伴い、保護すべき情報に接する必要がなくなった場合には、取扱者が保有する保護すべき情報を管理者へ返却させなければならない。

9　物理的及び環境的セキュリティ

(1) 取扱施設

ア　取扱施設の指定

防衛関連企業は、保護すべき情報の取扱施設を明確に定めなければならない。

イ　物理的セキュリティ境界

防衛関連企業は、保護すべき情報及び保護すべき情報を取り扱う情報システム（以下「保護システム」という。）のある区域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いなければならない。

ウ　物理的入退管理策

防衛関連企業は、取扱施設への立入りを適切な入退管理策により許可された者だけに制限するとともに、取扱施設への第三者の立入りを記録し、保管しなければならない。※13(2) 情報セキュリティの記録を参照

エ　取扱施設での作業

防衛関連企業は、保護すべき情報に係る作業は、機密性に配慮しなければならない。また、取扱施設において通信機器（携帯電話等）及び記録装置（ボイスレコーダ及びデジカメ等）を経営者等の許可無く利用してはならない。

(2) 保護システムの物理的保全対策

ア　保護システムの設置及び保護

防衛関連企業は、保護システムを設置する場合、不正なアクセス及び盗難等から保護するため、施錠できるラック等に設置又はワイヤーで固定する等の措置をとらなければならない。

イ　保護システムの持ち出し

防衛関連企業は、経営者等が持ち出しに伴うリスクを回避することができると判断した場合を除き、保護システムを取扱施設外に持ち出してはならない。

なお、持ち出しをする場合は、記録するものとする。

ウ　保護システムの保守及び点検

防衛関連企業は、第三者による保護システムの保守及び点検を行う場合、必要に応じて、保護すべき情報を復元できない状態にする、又は取り外す等の処置を実施しなければならない。

エ　保護システムの破棄又は再利用

防衛関連企業は、保護システムを破棄する場合は、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上、記憶媒体を物理的に破壊した後、破棄し、その旨を記録しなければならない。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でなければ再利用してはならない。

１０　通信及び運用管理

(1) 操作手順書

防衛関連企業は、保護システムの操作手順書を整備し、維持するとともに、利用者が利用可能な状態にしなければならない。

(2) 悪意のあるコードからの保護

防衛関連企業は、保護システムをウィルス対策ソフトウェア等により悪意のあるコードから保護しなければならない。

(3) 保護システムのバックアップの管理

防衛関連企業は、保護システムを可搬記憶媒体にバックアップする場合、可搬記憶媒体は7(2)及び次号に沿った取扱いを行わなければならない。

(4) 可搬記憶媒体の取扱い

ア　可搬記憶媒体の管理

防衛関連企業は、保護すべきデータを保存した可搬記憶媒体を施錠したロッカー等において集中保管し、適切に鍵を管理しなければならない。また、可搬記憶媒体は、保護すべき情報とそれ以外を容易に区別できる処置をしなければならない。※7(2)保護すべき情報の取扱いを参照

イ　可搬記憶媒体への保存

防衛関連企業は、保護すべきデータを可搬記憶媒体に保存する場合、暗号技術を用いなければならない。ただし、防衛省への納入又は提出物件等である場合には、防衛省の指示に従うものとする。※10(7) 電子政府推奨暗号等の利用を参照

ウ　可搬記憶媒体の破棄又は再利用

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破棄する場合、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上、可搬記憶媒体を物理的に破壊した後、破棄し、その旨を記録しなければならない。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でなければ再利用してはならない。

(5) 情報の伝達及び送達

ア　保護すべき情報の伝達

防衛関連企業は、通信機器（携帯電話等）を用いて保護すべき情報を伝達する場合、伝達に伴うリスクを経営者等が判断の上、必要に応じそのリスクから保護しなければならない。

イ　伝達及び送達に関する合意

防衛関連企業は、保護すべき情報を伝達及び送達する場合には、守秘義務を定めた契約又は合意した相手に対してのみ行われなければならない。

ウ　送達中の管理策

防衛関連企業は、保護すべき文書等を送達する場合には、送達途中において、許可されていないアクセス及び不正使用等から保護しなければならない。

エ　電子メール等による伝達

防衛関連企業は、電子メール等において保護すべきデータを伝達する場合、暗号技術を用いて保護すべきデータを保護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、有線で伝達が行われる場合は、この限りでない。※10(7) 電子政府推奨暗号等の利用を参照

(6) 外部からの接続

防衛関連企業は、保護システムに外部から接続（モバイルコンピューティング及びテレワーキング等）を許可する場合は、利用者の認証を行うとともに、暗号技術を用いなければならない。※10(7) 電子政府推奨暗号等の利用を参照

(7) 電子政府推奨暗号等の利用

防衛関連企業は、暗号技術を用いる場合、電子政府推奨暗号等を用いなければならない。

なお、電子政府推奨暗号等を用いる事が困難な場合は、その他の秘匿化技術を用いる等により保護すべき情報を保護しなければならない。

(8) ソフトウェアの導入管理

防衛関連企業は、保護システムへソフトウェアを導入する場合、当該システムの管理者等によりソフトウェアの安全性が確認された場合を除き、許可してはならない。

(9) システムユーティリティの使用

防衛関連企業は、保護システムにおいてオペレーティングシステム及びソフトウェアによる制御を無効にすることができるシステムユーティリティの使用を制限しなけ

ればならない。

(10)　技術的脆弱性の管理

防衛関連企業は、技術的脆弱性に関する情報について時期を失せず取得し、経営者等が判断の上、適切に対処しなければならない。

(11)　監視

ア　監査ログ取得

防衛関連企業は、保護システムにおいて、利用者の保護すべき情報へのアクセス及び例外処理を記録した監査ログを取得しなければならない。

イ　監査ログの保管

防衛関連企業は、取得した監査ログを一定期間保存するとともに、定期的に点検しなければならない。※13(2) 情報セキュリティの記録を参照

ウ　監査ログの保護

防衛関連企業は、監査ログを改ざん及び許可されていないアクセスから保護しなければならない。

エ　クロックの同期

防衛関連企業は、保護システム及びネットワークを通じて保護システムにアクセス可能な情報システムの日付及び時刻を手動等により定期的に合わせなければならない。

１１　アクセス制御

(1) アクセス制御方針

防衛関連企業は、保護すべき情報、取扱施設及び保護システムへのアクセスについて、取扱者及び利用者の職務内容に応じて、アクセス制限方針を作成しなければならない。また、アクセス制御方針は定期的に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しなければならない。

(2) 利用者の管理

ア　利用者の登録管理

防衛関連企業は、取扱者による保護システムへのアクセスを許可し、適切なアクセス権を付与するため、保護システムの利用者としての登録及び登録の削除をしなければならない。

イ　パスワードの割当て

防衛関連企業は、保護システムの利用者に対して初期又は仮パスワードを割り当てる場合、容易に推測されないパスワードを割り当てるものとし、機密性に配慮した方法で配布するものとする。なお、パスワードより強固な手段（生体認証等）を採用又は併用している場合は、本項目の適用を除外することができる。

ウ　管理者権限の管理

保護システムの管理者権限は、必要最低限の利用にとどめなければならない。

エ　アクセス権の見直し

防衛関連企業は、保護システムの利用者に対するアクセス権の割当てについて

は、定期的及び必要に応じて見直しを実施しなければならない。

(3) 利用者の責任

ア　パスワードの利用

防衛関連企業は、容易に推測されないパスワードを保護システムの利用者に選択させるとともに、定期的に変更させなければならない。

なお、パスワードより強固な手段（生体認証等）を採用又は併用している場合は、本項目の適用を除外することができる。

イ　無人状態にある保護システム対策

防衛関連企業は、保護システムが無人状態に置かれる場合、機密性を配慮した措置をとらなければならない。

(4) ネットワークのアクセス制御

ア　機能の制限

防衛関連企業は、保護システムの利用者の職務内容に応じて、利用できる機能を制限し提供しなければならない。

イ　ネットワークの接続制御

防衛関連企業は、保護システムの共有ネットワーク（インターネット等）への接続については、アクセス制御方針に基づいて実施するとともに、接続に伴うリスクから保護しなければならない。

(5) オペレーティングシステムのアクセス制御

ア　セキュリティに配慮したログオン手順

防衛関連企業は、利用者が保護システムを利用する場合、セキュリティを配慮した手順により、ログオンさせなければならない。

イ　利用者の識別及び認証

防衛関連企業は、保護システムの利用者ごとに一意な識別子（ユーザーID、ユーザー名等）を保有させなければならない。

ウ　パスワード管理システム

保護システムは、パスワードの不正使用を防止する機能（パスワードの定期的な変更を利用者に促す機能又はパスワードの再使用を防止する機能等）を有さなければならない。

１２　情報セキュリティ事故等の管理

(1) 情報セキュリティの事故の報告

防衛関連企業は、情報セキュリティ事故が発生した場合、速やかに防衛省へ報告しなければならない。また、情報セキュリティ事故が発生した場合の防衛省への報告要領を定めておかなければならない。

(2) 情報セキュリティ事故等の対処等

ア　対処体制及び手順

防衛関連企業は、情報セキュリティ事故及び事象に対処するため、対処体制、責任及び手順を定めなければならない。

イ　証拠の収集

防衛関連企業は、情報セキュリティ事故が発生した場合、証拠を収集し速やかに防衛省へ提出しなければならない。

ウ　情報セキュリティ基本方針等への反映

防衛関連企業は、発生した情報セキュリティ事故及び事象を、情報セキュリティ基本方針等の見直し等に反映しなければならない。

１３　遵守状況等

(1) 遵守の確認等

ア　遵守状況の確認

防衛関連企業は、管理者の責任の範囲において、情報セキュリティ基本方針等の遵守状況を確認させなければならない。

イ　技術的遵守の確認

防衛関連企業は、保護システムの管理者の責任の範囲において、情報セキュリティ基本方針等への技術的遵守状況を確認させなければならない。

(2) 情報セキュリティの記録

防衛関連企業は、保護すべき情報に係る重要な記録（複製記録、持ち出し記録及び監査記録等）の保管期間（少なくとも契約履行後１年間）を定めた上、施錠したロッカー等において保管又は暗号技術を用いる等厳密に保護するとともに、適切に鍵を管理しなければならない。

(3) 監査ツールの管理

防衛関連企業は、保護システムの監査に用いるツールについて、悪用を防止するため必要最低限の使用にとどめなければならない。

(4) 防衛省による監査

ア　監査の受入

防衛関連企業は、防衛省による情報セキュリティ対策に関する監査の要求があった場合には、これを受け入れなければならない。

イ　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、防衛省の求めに応じ必要な協力（監査官の取扱施設への立入り及び監査官による書類の閲覧等への協力）をしなければならない。