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とする。
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、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　ｐ３

第４　情報セキュリティ基本方針等　ｐ３

第５　組織のセキュリティ　ｐ４

第６　保護すべき情報の管理　ｐ５

第７　情報セキュリティ教育及び訓練　ｐ７

第８　物理的及び環境的セキュリティ　ｐ７

第９　保護システムについての管理策　ｐ９

第１０　情報セキュリティ事故等への対応　ｐ９

第１１　情報セキュリティ事故等発生時の対応　ｐ１０

第１２　リスク査定　ｐ１１

第１３　セキュリティ監査　ｐ１１

第１４　防衛省による監査　ｐ１２

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、監査等を行う者を含む。
(12) 保護システムとは、保護すべき情報を取り扱う情報システムをいう。
(13) 保護システム利用者とは、保護すべきデータに接する必要のある者及び保護システムの運用管理業務に従事する者であって、当該データを保存する領域又はその機器に関わる者をいう。
(14) 伝達とは、知識を相手方に伝えることであって、有体物である文書等の送達を伴わないものをいう。
(15) 送達とは、取扱施設の外に所在する者に送り届けることをいい、輸送（社外の事業者との契約に基づき、当該事業者が保護すべき情報を特定の相手方に送達することをいう。以下同じ。）を含む。
(16) 保護すべき文書等とは、保護すべき情報に属する文書（保護すべきデータが保存された可搬記憶媒体を含む。）、図画及び物件をいう。
(17) 可搬記憶媒体とは、パソコン又はその周辺機器に挿入又は接続して情報を保存することができる媒体又は機器のうち可搬型のものをいう。
(18) 情報システムとは、ハードウェア（サーバ、パソコン、モニタ、携帯端末、プリンタ、スキャナ等を含む。以下同じ。）、ソフトウェア（プログラムの集合体をいい、ファームウェアを含む。以下同じ。）、ネットワーク（暗号化により公衆回線に作られる仮想的な専用ネットワークを含む。）又は記憶媒体で構成されるものであって、これら全体で業務処理を行うものをいう。
(19) 悪意のあるコードとは、情報システムが提供する機能を妨害するプログラムの総称であり、コンピュータウイルス及びスパイウェア等をいう。
(20) 情報セキュリティ事象とは、情報セキュリティ事故のおそれ並びに情報セキュリティ事故に至らない情報セキュリティ基本方針等への違反及びそのおそれのある状態をいう。
(21) 情報セキュリティ事故とは、保護すべき情報の漏えい、紛失、破壊等の事故をいう。
(22) 取扱施設とは、保護すべき情報の取扱い及び当該情報に属する文書等の保管を行う場所として、本基準の規定に従って防衛関連企業が指定する建物又は敷地の一部又は全部をいう。
(23) 関係施設とは、取扱施設の外側に隣接する場所であって、本基準の規定に基づき防衛関連企業が指定する建物又は敷地の一部又は全部をいう。

(24) システムログとは、情報システムにおける動作履歴に関する記録をいう。
(25) 取扱施設等とは、取扱施設及び関係施設をいう。
(26) ベースライン構成設定とは、保護システムとシステムコンポーネントの構成の把握並びに保護システムの更新及び変更時のベース(基準)となる構成設定をいう。
(27) ブラックリストとは、保護システムにインストール又は保護システムで実行してはならないソフトウェアのリストをいう。
(28) ホワイトリストとは、保護システムにインストール及び保護システムで実行してもよいソフトウェアのリストをいう。
(29) 保護すべきデータとは、保護すべき情報が電子的な状態にあるものをいう。
(30) 構成設定とは、情報システムを構成する構成要素（ハードウェア、ソフウェア、ネットワーク及び記憶媒体）の機種、バージョン等及び当該構成要素の機能並びに動作等を制御する設定値を決定することをいう。
(31) リプレイ攻撃とは、利用者の確認に用いられる認証データの通信を盗聴し得られたデータをそのまま用いてその利用者になりすます方式をいう。
(32) モバイルコードとは、インターネット等のネットワークを通じて、自動的にダウンロード及び実行されるプログラムをいう。
(33) 外部ネットワークとは、インターネットその他の防衛関連企業によって管理されないネットワークをいう。
(34) 機密性とは、認可されていないものに対して、情報を使用不可又は非公開にする特性をいう。
(35) 完全性とは、情報の正確さ及び完全さを保護する特性をいう。
(36) 電子政府推奨暗号等とは、電子政府推奨暗号リストに記載されている暗号等又は電子政府推奨暗号選定の際の評価方法により評価した場合に電子政府推奨暗号と同等以上の解読困難な強度を有する秘匿化の手段をいう。
(37) 管理者権限とは、情報システムの管理（情報システム利用者の登録、削除、及びアクセス制御等）を行うために付与される権限をいう。
(38) 外部システムとは、防衛関連企業によって管理されないシステム（クラウドサービス事業者によるクラウドサービス、及び請負業者の情報システム等を含む。）をいう。
(39) ユーザセッションとは、保護システム利用者が実行する各アプリケーションの論理的な経路をいう。
(40) タイムスタンプとは、電子データの取得、作成等を行った時刻に関する情報をいう。
(41) 可用性とは、認可されたものが要求したときに、アクセス及び使用が可能である特性をいう。

第３　対象

１　対象とする情報

対象とする情報は、防衛関連企業において取り扱われる保護すべき情報とする。

２　対象者

対象者は、防衛関連企業において保護すべき情報に接する全ての者（保護すべき情報に接する役員（持分会社にあっては社員を含む。）、管理職員、派遣社員、契約社員、パート、アルバイト等を含む。）とする。

第４　情報セキュリティ基本方針等

１　情報セキュリティ基本方針等の作成及び変更

(1)　防衛関連企業は、本基準の内容に沿った情報セキュリティ基本方針等を作成し、経営者等の承認を得るものとする。
(2)　防衛関連企業は、情報セキュリティ基本方針等を適切、有効及び妥当なものとするため、定期的な見直しを実施するとともに、情報セキュリティに係る重大な変化及び情報セキュリティ事故が発生した場合は、その都度見直しを実施し、必要に応じて情報セキュリティ基本方針等を変更し、経営者等の承認を得るものとする。
(3)　防衛関連企業は、情報セキュリティ基本方針等を作成又は変更する場合は、本基準との適合性に関する防衛省の確認を受けるものとする。

２　情報セキュリティ基本方針等の周知等

(1)　保護すべき情報の管理全般に係る総括的な責任を負う者（以下「総括者」という。）は、情報セキュリティ基本方針等を取扱者に周知するものとする。

(2)　防衛関連企業は、情報セキュリティ実施手順を社外の者（契約に関係する防衛省の職員を除く。）にみだりに公開しないよう適切に管理するものとする。

第５　組織のセキュリティ

１　経営者等の職責

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

２　経営者等及び取扱者の責務

(1)　取扱者の指定等

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

(ｱ)　在職中及び離職後において、業務上知り得た保護すべき情報を、第三者に漏えいしないこと（以下「守秘義務」という。）。

(ｲ)　守秘義務に違反した場合に法律上の責任を負うこと。

(ｳ)　守秘義務の内容を理解し、かつ、承諾すること。

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

(ｱ)　総括者

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

ウ　経営者等は、防衛省との契約に違反する行為を求められた場合に、これを拒む権利を実効性をもって法的に保障されない者を取扱者にふさわしい者として認めてはならない。

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

オ　管理者は、取扱者の退職、異動、職務内容の変更などの理由により、保護すべき情報にアクセスする必要がなくなった場合は、取扱者名簿を更新するとともに、当該取扱者との面談等により、守秘義務を再確認するものとする。

(2)　保護システム利用者の指定等

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

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

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

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

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

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

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

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

(3)　情報セキュリティの確保

ア　経営者等は、情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当て、情報セキュリティ基本方針等の承認等を通して、自社における情報セキュリティの確保に努めるものとする。また、組織内において、取扱者以外の役員、管理職員等を含む従業員、その他の全ての構成員に対して、取扱者以外の者は保護すべき情報に接してはならず、かつ、職務上の下級者等に対してその提供を要求してはならないことを定めるも

のとする。

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

ウ　経営者等は、情報セキュリティ基本方針等に違反した取扱者に対する対処方針及び懲戒手続を定め、違反が生じた場合には、当該対処方針及び懲戒手続に基づき対処するものとする。

エ　経営者等は、前２号に規定する者、その他の責任の割当てについて、当該責任を業務の遂行上必要最小限度に分割して割り当て、同一の取扱者に広範な責任を持たせてはならない。ただし、総括者及び管理者については、兼任させることができるものとする。

３　保護すべき情報を取り扱う下請負者

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

１　保護すべき情報の分類

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

２　保護すべき情報の目録の作成等

(1)　目録の作成

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

(2)　目録の更新

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

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

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

(ｳ)　保護すべき情報の送達、返却、提出又は廃棄

イ　目録には、接受等を行った者の氏名、所属、所在等を記載するものとする。

ただし、保護すべき情報の取扱いに関するシステムログの記録により代用する場合は、アカウントの識別子を記載するものとする。

(3)　目録等の保管

管理者は、保護すべき情報の目録は、不正なアクセス、改ざん、盗難等から保護するため、文書により保存する場合は、施錠したロッカー等（第８第５項第２号の規定により鍵及び解錠キーを厳格に管理するものとする。以下同じ。）により、データで保存する場合には、暗号化により必要な期間保管又は保存するものとする。

３　保護すべき文書等の表示等

(1)　保護すべき文書等への表示

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

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

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

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

(2)　その他の表示

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

4　保護すべき情報の持ち出し及び送達

(1)　持ち出し及び送達の方法

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

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

(2)　送達することができる者の制限

管理者は、保護すべき情報を持ち出し及び送達することができる者を業務の遂行上必要最小限度に制限するものとする。

(3)　持ち出し及び送達の際の表示

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

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

5　保護システムにおける可搬記憶媒体の使用制限

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

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

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

(3)　個人の所有する又は所有者若しくは管理者が明確でない可搬記憶媒体を保護システムにおいて使用しないこと。

(4)　保護システムにおいて可搬記憶媒体を使用することができる者を業務の遂行上必要最小限度に制限すること。

(5)　可搬記憶媒体の使用が、第１号に規定する目録に従って実施されることを確保するため、保護すべきデータの可搬記憶媒体への複製をソフトウェアにより制御する等の技術上の措置を講じること。

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

6　保護すべき情報を記録した媒体の廃棄又は再利用

(1)　保護すべき文書等（この号において、保護すべきデータを除く。）の廃棄

防衛関連企業は、保護すべき文書等を廃棄する場合は、裁断等確実な方法により廃棄し、保護すべき文書等が復元できない状態であることを点検したうえで、その旨を記録するものとする。

(2)　可搬記憶媒体の廃棄又は再利用

防衛関連企業は、保護すべきデータの保存に利用した可搬記憶媒体を廃棄する場合は、保護

すべきデータが復元できない状態であることを点検したうえで、可搬記憶媒体を物理的に破壊し、その旨を記録するものとする。また、再利用する場合は、保護すべきデータが復元できない状態であることを点検した後に実施するものとする。

(3)　保護システムの廃棄又は再利用

防衛関連企業は、保護システムを廃棄する場合は、保護すべきデータが復元できない状態であることを点検したうえで、記憶媒体を物理的に破壊し、その旨を記録するものとする。また、再利用する場合は、保護すべきデータが復元できない状態であることを点検した後に実施するものとする。

(4)　廃棄又は再利用前の点検

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

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

7　保護すべき文書等の防衛省への返却等

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

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

8　保護すべき文書等の作成等の手順

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

9　防衛関連の情報を公開する場合の措置

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

第７　情報セキュリティ教育及び訓練

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

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

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

(3)　情報セキュリティ基本方針等の確実な履行

(4)　公私における慎重な行動

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

(6)　前号に掲げる事項のほか、情報セキュリティ事故等への対処のために必要な事

(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。

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「入退管理機器」という。）

ウ　保護システム

エ　保管された保護すべき文書等

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

2　取扱施設等に対する物理的セキュリティ対策

(1)　取扱施設等の指定

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

イ　経営者等は、取扱施設内に保護システム（保護すべき情報の保存又は当該情報へのアクセスを可能とする機器に限る。第４項において同じ。）を設置し、当該施設内で保護すべき情報を取り扱うものとする。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(5)　立入りが許可されていない者による取扱施設への立入りは、管理責任者が承認した場合に限り許可することとし、管理責任者の指定した者が同行して監視するとともに、第２号ウ又はエの措置を行うものとする。
(6)　取扱施設等が自然災害等の非常事態により使用できない場合は、経営者等が指定する取扱施設等を代替する施設において、総括者が当該事態の状況を踏まえつつ、取扱者のみが当該保護すべき情報に接することができるようにするために必要な物理的セキュリティ対策を講じることで、保護すべき情報を扱うことができる。

３　入退管理機器に対する物理的セキュリティ対策

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

(1)　入退管理機器の現状を記録した目録を作成し保管するものとし、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により必要な期間保管すること。
(2)　前号に規定する目録は、定期的に、及び入退管理機器の変更など必要があると認める場合には、その都度精査し、必要に応じ更新すること。
(3)　入退管理機器として暗証番号等を併用する場合は、定期的に、及び当該暗証番号等を配布されていた者が、異動等により取扱施設等への立ち入り権限を失うなど必要があると認める場合には、その都度当該暗証番号等を変更すること。
(4)　入退管理機器として錠を併用する場合は、鍵の紛失など必要があると認める場合に、当該錠を変更すること。

４　保護システムに対する物理的セキュリティ対策

(1)　保護システム管理者は、保護システムを構成するハードウェア及び記憶媒体について、不正な移動、持ち出し等を防止するため、必要な措置を講じるものとする。
(2)　保護システムの取扱施設外への持ち出しは、保護システム管理者が管理責任者と調整の上許可することとし、当該持ち出しを行う者が保護システム利用者でない場合は、保護システム管理者の指定する保護システム利用者が同行して監視し、記録するものとする。
(3)　保護システムに接続された送配線は、関係施設において破壊、情報窃取を防止又は検知できる物理的セキュリティ対策を講じるものとする。
(4)　その他の保護システムに対する管理策については、第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

(1)　保護すべき情報の保管

ア　保護すべき情報を文書等により保管する場合は、取扱施設内の施錠したロッカー等に保管するものとする。
イ　保護すべきデータを保護システムに保存する場合は、第４項第１号に定める措置を行うものとする。

(2)　鍵等の管理

第１号に規定するロッカー等の鍵を保管するのは、管理者（保護システムに関連する場合にあっては保護システム管理者を含む。以下本号において同じ。）及び管理者が指定した者のみとし、それ以外の者により解錠されることがないよう厳格に管理するものとする。

第９　保護システムについての管理策

１　防衛関連企業は、自社の保有又は使用する保護システムに、保護すべき情報を適切に取り扱うために必要と認める情報セキュリティ対策を講じるものとする。
２　防衛関連企業は、前項の規定に基づき情報セキュリティ対策を講じる際は、本基準及び付紙に規定する管理策を盛り込んだ情報セキュリティ実施手順を定めるものとする。

第１０　情報セキュリティ事故等への対応

１　情報セキュリティ事故等対処計画の策定

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

ア　事故等への対処の準備
イ　事故等の発見及び検知時の報告・連絡要領

ウ　事故等の監視（システム監視を含む。）及び分析
エ　事故等による被害及び影響の抑制並びに局限
オ　事故等に係る証拠の保存及び原因の究明
カ　事故等からの復旧（復旧に要する時間の目標を含む。）

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

ア　保護システム管理者の下にヘルプデスク等を設置し、保護システム利用者に対し、情報セキュリティ事故等に関する必要な情報の提供等を行うこと。
イ　情報セキュリティ事故等の詳細を把握するため、デジタルフォレンジック技術の利用等により必要な情報を収集及び分析すること。
ウ　保護システムを含め、自社のネットワークにおけるすべての情報システムの分析及び精査（システムログの取得及び分析を含む。）を行い、当該情報システム内の構成要素、データ及びアカウント等の中から、悪意のあるコードへの感染又は不正アクセスなどの情報セキュリティ事故等が発生した原因を特定すること。
エ　情報セキュリティ事故等への対処の要領及び結果（当該事故等に対する分析及び原因究明等の結果を含む。）並びに当該対処により取得した情報等を記録した文書の作成及び保管に関すること。
オ　情報セキュリティ事故等への対処において収集した情報の分析結果を踏まえ、当該対処に係る教訓を取りまとめ、情報セキュリティ教育及び訓練、情報セキュリティ事故等対処計画及び情報セキュリティ事故等対処テストの内容に反映させること。

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

2　情報セキュリティ事故等への対処テスト

(1)　防衛関連企業は、情報セキュリティ事故等対処計画の有効性を検証し、潜在的な弱点又は欠陥を発見するため、情報セキュリティ事故等対処テストを第７第１項の規定による訓練に含めるなど、定期的に実施するものとする。

(2)　前号に規定する情報セキュリティ事故等対処テストを実施した場合は、当該テストの結果を記録した文書を作成し、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存するものとする。

第１１　情報セキュリティ事故等発生時の対応

1　情報セキュリティ事故等を発見又は検知した場合の処置

(1)　全ての従業員は、情報セキュリティ事故等を発見又は検知した場合は、速やかに管理者（保護システムに係る場合は保護システム管理者）に報告するものとし、管理者は情報セキュリティ事故等対処計画に基づき適切に対処するとともに、その内容及び結果（当該事故等に対する分析及び原因究明等の結果を含む。）並びに当該対処により取得した情報等を記録した文書を作成し、総括者に報告するものとする。

(2)　保護システム利用者が保護システムの脆弱性を発見又は探知した場合は、速やかに保護システム管理者に報告するものとし、保護システム管理者は、適切な対処を行うとともに、その内容、修正方法を記載した文書を作成し、総括者に報告するものとする。

(3)　保護システム管理者は、前２号の規定により作成した文書は、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、契約履行後においても必要な期間保管又は保存するものとする。

(4)　総括者は、第１号及び第２号による情報セキュリティ事故等対処計画に基づく対処を行う場合は、同計画に定められた期間内に行うものとする。

　なお、当該期間までの改善又は修正が困難と認める場合は、是正計画を作成し、同計画に定められた期間内に修正を実施するとともに防衛省に報告するものとする

(5)　防衛関連企業は、保護システムの脆弱性に係る修正を実施する場合は、第１２に規定するリスク査定の結果及び公開されている脆弱性情報データベース等を活用するものとし、当該脆弱性が保護システムのセキュリティに重大な影響を及ぼす場合には、可能な限り速やかに修正を実施するものとする。

2　防衛省への報告

(1)　総括者は、前項第１号に掲げる情報セキュリティ事故等の報告を受けた場合は、適切な措置

を講じるとともに、直ちに把握し得る限りの全ての内容を、その後速やかにその詳細を防衛省（契約担当官等又は防衛装備庁長官が別に定めた部署の職員。以下同じ。）に報告するものとする。

(2)　総括者は、前号のほか、防衛関連企業の内部又は外部から情報セキュリティ事故等が発生した可能性又は将来発生する懸念の指摘があった場合は、当該可能性又は懸念の真偽を含む把握し得る限りの全ての背景及び事実関係の詳細を速やかに防衛省に報告するものとする。

(3)　総括者は、前２号に規定する防衛省への報告については、それぞれ責任者及び連絡担当者等を明示した連絡系統図を含む報告要領を定め、責任者及び連絡担当者等に異動等があった場合にはこれを更新するものとする。

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

第１２　リスク査定

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

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

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

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

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

第１３　セキュリティ監査

１　セキュリティ監査計画の作成等

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

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

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

イ　セキュリティ監査を実施する日程

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

(3)　前号アの規定によりセキュリティ監査に関与する者に対する保護すべき情報及び保護システムに対するアクセス権限について、総括者は当該セキュリティ監査の遂行上必要な権限を付与するものとする。

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

２　セキュリティ監査の実施

総括者は、１年に１回以上及び自社の情報セキュリティに重大な変化が生じた場合など必要と認めた場合に、監査部門に、前項に規定するセキュリティ監査計画に基づくセキュリティ監査（

情報セキュリティ基本方針等に基づく措置が継続的に有効であることの評価を含む。）を実施させるものとする。

3　セキュリティ監査結果の報告等

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

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

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

イ　アに規定する問題点がある場合は、その改善提案

ウ　イに規定する改善提案を踏まえた改善策の実施に必要な期間

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

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

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

第１４　防衛省による監査

1　監査の受入

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

2　監査への協力

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

付紙

装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領

目　次

第１　趣旨　ｐ１４

第２　システムセキュリティ実装計画書　ｐ１４

第３　構成管理　ｐ１４

第４　保護システムの基本的防御　ｐ１６

第５　アクセス制御　ｐ１７

第６　識別及び認証　ｐ１８

第７　通信制御　ｐ１９

第８　システム監視　ｐ２０

第９　システムログ　ｐ２１

第１０　脆弱性スキャン等　ｐ２２

第１１　バックアップ　ｐ２３

第１２　システムメンテナンス等　ｐ２３

第１　趣旨

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

第２　システムセキュリティ実装計画書

１　システムセキュリティ実装計画書の作成

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

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

ア　第３第２項第１号に規定するベースライン構成設定

イ　第３第２項第５号に規定するブラックリスト又はホワイトリスト

ウ　第３第４項第１号に規定する構成設定目録

エ　第４第２項第１号に規定する操作手順書

オ　第５第１項第１号に規定するアクセス制御方針

カ　第７第３項第１号及び第２号に規定する保護システムにおけるモバイルコード及びＶｏＩＰ技術の利用に係る要件

キ　第７第３項第３号に規定する保護システムにおける各種のオフィス機器の利用に係る要件

ク　保護システムのセキュリティを確保するための組織体制図（経営者等、総括者及び保護システム管理者、その他保護システムのセキュリティに責任を有する者の具体的な責任の内容及び範囲を記載するものとする。）

ケ　保護システムのネットワーク構成図

コ　保護すべきデータのデータフロー図

２　システムセキュリティ実装計画書の定期的な確認

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

３　システムセキュリティ実装計画書の保存等

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

４　システムセキュリティ実装計画書の周知

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

５　システムセキュリティ実装計画書の防衛省への提出等

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

第３　構成管理

１　セキュリティエンジニアリングの原則の適用

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

２　ベースライン構成設定等

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

ア　情報セキュリティ基本方針等に基づく措置が実施可能なものであること。

イ　保護システムのセキュリティを確保するものであること。

ウ　保護システム構成要素の機能及び動作を業務の遂行上必要な最小限度に制限するものであること。

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

(3)　構成設定の方法

ア　保護システム管理者は、保護システム構成要素の構成設定を適切に制御するための手順を定めるとともに総括者の承認を得て、同手順に基づきソフトウェアの導入等を行うものとする。

イ　アクセス権限の特定等

(ｱ)　保護システム構成要素の構成設定を行うための物理的及び論理的なアクセス権限は、当該構成設定を行うために必要な最小限度の範囲に限定するものとする。

(ｲ)　(ｱ)に規定する論理的なアクセス権限は、構成設定を安全に実施する能力を有し、かつ、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。

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ものとする。

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、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。

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　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。

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　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。

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　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。

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

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

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

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

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

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。

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、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。

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。

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。

(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とする。

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。

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。