調達における情報セキュリティ基準

この基準は、調達における情報セキュリティ基本方針に示す防衛情報資産に関する情報セキュリティ対策に適用することを目的とし、防衛省として特に重視し実施することを求める項目を示すものである。

【前提となる要求条件】

１．受注企業は、調達における情報セキュリティ基本方針に示す防衛情報資産を保護するために十分であるべく、従来から実施している情報セキュリティ対策に加えて、本基準により新たに追加又は拡充すべき情報セキュリティ対策を実施すること。

２．受注企業は、防衛省との契約に基づく情報セキュリティ対策要求事項への適合の客観的証拠を示すため、情報セキュリティ対策の手順を文書化し、対策の実施状況を記録するとともに、それらの管理も実施すること。これら情報セキュリティ対策にかかる各種ドキュメントの作成に際しては、ＪＩＳ　Ｘ　５０８０　を参考とすること。

３．受注企業は、防衛省による情報セキュリティ対策に関する監査について、要求があれば受け入れること。

（注）１．以下に示す【基準】の［補足説明］は、なるべく受注企業の情報セキュリティ対策として、取り入れることを希望するものではあるが、その判断は、企業の裁量に任せるものである。ただし、2.4 の［補足説明］(1)及び 8.2 の［補足説明］(1)は、必須とする。

２．この基準においては、調達における情報セキュリティ基本方針の４（１）の⑨に関する規定は設けないこととする。

【基準】

１．セキュリティ基本方針

1.1 基本方針文書は、経営者によって承認され、適当な手段で、全従業員に公表し、通知すること。

［補足説明］

(1) 経営者とは、受注案件を処理する部門責任者を示す（以下の文書中も同様）。

(2) 受注案件を処理する当該部門に有効な明文化された基本方針文書を持つ。

1.2 基本方針には、定められた見直し手続に従って基本方針の維持及び見直しに責任をもつ者が存在すること。

２．組織のセキュリティ

2.1 セキュリティを主導するための明りょうな方向付け及び経営者による目に見える形での支持を確実にするために、運営委員会を設置すること。

［補足説明］

(1) 運営委員会は適切な責任分担及び十分な資源配分によって組織内におけるセキュリティを促進すること。

2.2 個々の資産の保護に対する責任及び特定のセキュリティ手続の実施に対する責任を、明確に定めること。

［補足説明］

(1) 情報若しくはサービスの無認可の変更又は誤用の可能性を小さくするために、職務若しくは責任領域の管理又は実行の分離を考慮する。

［手順等の例示］

(1) 当該契約における情報システムの管理者を定め、アクセス制御管理を実施する。

2.3 情報セキュリティ基本方針の実施を、他者が見直すこと。

［補足説明］

(1) 他者が見直すとは、被監査者から独立した者（部外者を含む。）が行う内部監査のことである。

2.4 情報システム、ネットワーク及び／又はデスクトップ環境についての、マネジメント及び統制の全部又は一部を外部委託する組織のセキュリティ要求事項は、当事者間で合意される契約書に記述すること。

［補足説明］

(1) 外部委託（最下層までの下請負企業を含む。）に求めるセキュリティ要求事項として守秘義務を含める。

(2) 情報処理施設の管理のために外部の請負業者を利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れる。

(3) （外部委託による装置の保守整備の場合）装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく実施する。

３．資産の分類及び管理

3.1 情報システムそれぞれに関連づけてすべての重要な資産について目録を作成し、維持すること。

［手順等の例示］

⑴ 官側が貸与した文書及び作成された書類等を分類（社外秘等に区分）し、台帳等に登録する。

3.2 組織が採用した分類体系に従って情報のラベル付け及び取扱いをするための、一連の手順を定めること。

［補足説明］

⑴ 情報の分類及び関連する保護管理策では、情報を共有又は制限する業務上の必要、及びこのような必要から起こる業務上の影響（例えば、情報への認可されていないアクセス又は情報の損傷）を考慮に入れておく。

⑵ 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立する。

⑶ 認可されていないアクセスから情報システムに関する文書を保護する。

⑷ 運用システム（情報システム）でのソフトウェアの実行を管理する。

⑸ 試験データを保護し、管理する。

⑹ プログラムソースライブラリへのアクセスに対しては、厳しい管理を維持する。

⑺ システム監査ツール、すなわち、ソフトウェア又はデータファイルへのアクセスは、誤用又は悪用を防止するために、保護を行う。

［手順等の例示］

⑴ 情報資産を分類するための基準について明文規定を作成する。

４．人的セキュリティ

4.1 従業員は、雇用条件の一部として、秘密保持契約書又は守秘義務契約書に署名すること。

［補足説明］

⑴ 雇用条件には、情報セキュリティに対する従業員の責任を記述する。

⑵ 組織のセキュリティ基本方針及び手順に違反した従業員に対する、正式な懲戒手続を備える。

4.2 組織の基本方針及び手順について、組織のすべての従業員及び関係するならば外部利用者を適切に教育し、並びに定期的に更新教育を行うこと。

［補足説明］

(1) 情報セキュリティに関する教育として、次の［手順等の例示］に掲げる項目に関する教育も含めて実施する。

［手順等の例示］

(1) 情報サービスの利用者に対して、システム若しくはサービスのセキュリティの弱点、又はそれらへの脅威に気づいた場合若しくは疑いをもった場合は、注意を払い、かつ報告するよう要求する。

(2) ソフトウェアの誤動作を報告する手順を確立する。

(3) 組織は、通常の勤務時間内及び時間外の情報への許可されていないアクセス、情報の消失及び損傷のリスクを軽減するために、クリアデスク（使用していない書類や媒体をキャビネット等に収納し、机上に放置しないこと）及びクリアスクリーン（不正な操作や盗み見を防止するため、離席時には、パソコン等をログオフするか、画面・キーボードロック等の保護機能を使用すること）方針を持ち、実行する。

(4) 音声、映像の通信設備、ファクシミリ及びカメラ付携帯電話を使用して行われる情報交換を保護するために、適切な手順及び管理策をもつ。

4.3 セキュリティ事件・事故は、適切な連絡経路を通して、できるだけ速やかに報告すること。

［補足説明］

(1) セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理の責任及び手順を確立する。

５．物理的及び環境的セキュリティ

5.1 組織は、情報処理設備を含む領域を保護するために、幾つかのセキュリティ境界を利用すること。

［補足説明］

(1) セキュリティが保たれた領域のセキュリティを強化するために、その領域での作業のための管理策及び指針を追加する。

5.2 認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によってセキュリティの保たれた領域を保護すること。

［手順等の例示］

(1) 来訪者等について来訪目的、立入範囲等を簿冊、バッチ等で管理する。

(2) 設計、製造施設へアクセスする者を、規則に基づいて、入退管理装置の運用、簿冊へ

の記入によりアクセス制御する。

5.3 装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置し又は保護すること。

［補足説明］

(1) 設計製造に使用するサーバをセキュリティ区画に設置し、端末の盗難について対策を施す。

(2) 無人運転の装置の利用者は、無人運転の装置が適切な保護対策を備えていることを確実にする。

5.4 所有権に関係なく、組織の敷地外で情報処理のために装置を使用する場合は、管理者が認可すること。

［補足説明］

(1) 装置とは、情報処理のためのパソコン等の機器のほか、印刷された紙なども含む。

5.5 取扱いに慎重を要する情報を保持する記憶装置の処分、修理或いは再使用の前に、標準の削除機能を用いるよりも物理的に破壊するか、又は確実に上書きして情報漏洩を防止すること。

６．通信及び運用管理

6.1 セキュリティ個別方針によって明確化した操作手順は、文書化して維持していくこと。

［手順等の例示］

(1) 設計・製造に使用する情報システムの管理・運用規則（操作手順等）は、利用者の常時参照を可能とする。

6.2 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること。

［手順等の例示］

(1) フリーソフトウェア等の使用は、管理し、検査する。

6.3 ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること。

［手順等の例示］

(1) 少なくともインターネットとの接続点にファイアウォールを設置する。

6.4 コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書の管理手順があること。

［手順等の例示］

(1) 付属媒体の作成、複製及び破棄について明文規定を作成する。

(2) 利用者に、付属媒体の取扱いに関する作業手順を理解させる。

6.5 媒体が不要となった場合は、安全、かつ、確実に処分すること。

6.6 電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること。

［補足説明］

(1) 電子メールの使用について明文規定を作成する。

［手順等の例示］

(1) 利用者に電子メールに関する作業手順を理解させる。

７．アクセス制御

7.1 アクセス制御についての業務上の要求事項を定義し、文書化すること。

［補足説明］

(1) 情報及びサービスへのアクセスは文書化したアクセス制御方針の内容に従って制限すること。

(2) 遠隔地からの利用者のアクセスには、認証を行う。

(3) 遠隔コンピュータシステムへの接続には、認証を行う。

(4) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に基づき行う。

(5) ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にする。

(6) 支援要員を含め、業務用システムの利用者は、既定のアクセス制御方針に従い、個々の業務用ソフトウェアの要求事項に基づき、また、組織のアクセス制御方針に合わせて、情報及び業務用システム機能へのアクセスを許されること。

［手順等の例示］

(1) フォルダまたはディレクトリに対してアクセス制御を設定する。

7.2 複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセ

スを許可するための、正規の利用者登録及び登録削除の手続があること。

［補足説明］

(1) データ及び情報サービスへのアクセスに対する有効な管理を維持するため、経営者は、利用者のアクセス権を見直す正規の手順を、定期的に実施する。

［手順等の例示］

(1) 利用者に対して、システム管理者より制限されたアクセス権限を割り当てる。

7.3 特権の割当て及び使用は、制限し、管理すること。

7.4 パスワードの割当ては、正規の管理手続によって統制すること。

7.5 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと。

［手順等の例示］

(1) 利用者にログインパスワードの変更手順を理解させる。

(2) 利用者にログインパスワードの変更を実施させる。

7.6 ネットワークを介したサービスへのアクセスは、利用者に対して使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること。

［補足説明］

(1) 利用者に、遠隔地からのアクセスに関する作業手順を理解させる。

(2) 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止する。

(3) ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話のような移動型計算処理の設備を用いるとき、業務情報のセキュリティが危険にさらされないような防御を確実に実施するために、正式な方針を整え、適切な管理策を採用しなければならない。

(4) 遠隔地作業を認可し、管理するための個別方針、手順及び標準類を策定することを考慮すること。

［手順等の例示］

(1) 遠隔地からネットワーク経由で設計製造に使用する情報システムへアクセスする場合の手順について明文規定を作成する。

(2) 移動型計算処理の設備の運用について簿冊等により管理する。

7.7 すべての利用者（技術支援要員、例えば、オペレータ、ネットワーク管理者、システムプログラマ、データベース管理者）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（利用者ＩＤ）を保有すること。

7.8 質のよいパスワードであることを確実にするために、パスワード管理システムは有効な対話的機能を提供すること。

7.9 システムユーティリティの使用を制限し、厳しく管理すること。

7.10 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること。

［補足説明］

(1) 情報処理設備の使用状況を監視する手順を確立する。

(2) 監視の結果は定期的に見直すこと。

(3) システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること。

(4) 情報処理施設の使用には管理者の認可を要するものとし、そのような施設の誤用を防ぐための管理策を用いる。

８．システムの開発及び保守

8.1 組織の情報を保護するための暗号による管理策の使用について、個別方針を定めること。

［補足説明］

(1) 取扱いに慎重を要する又は重要な情報の機密性を保護するために、暗号化すること。

(2) 電子文書の真正性及び完全性を保護するために、ディジタル署名を用いる。

(3) 事象又は動作が起こったか起こらなかったかについての紛争の解決が必要である場合には、否認防止サービスを用いる。

(4) 一連の合意された標準類、手順及び方法に基づくかぎ管理システムを、暗号技術の利用を支援するために用いる。

8.2 外部委託によるソフトウェア開発をセキュリティの保たれたものとするために、管理策を用いること。

［補足説明］

(1) 外部委託（最下層までの下請負企業を含む。）に対する管理策として守秘義務を含める。

［手順等の例示］

(1) 請負会社・派遣会社との間で守秘義務を含めたセキュリティ対策を明記した契約をする。

９．適合性

9.1 組織の重要な記録は、消失、破壊及び改ざんから保護されること。

［補足説明］

⑴ 内部監査記録は、保管期間（例：１年間）を定め、安全に保管する。

9.2 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること。

［補足説明］

⑴ 組織内の全ての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするため、定期的な見直しを考慮すること。

⑵ 新しいシステム又は既存のシステムの改善に関する業務上の要求事項には、管理策についての要求事項を明確にする。

9.3 情報システムは、技術的なセキュリティ実行標準と適合していることを定期的に検査すること。

【用語の解説】

情報セキュリティ対策

情報の機密性、完全性及び可用性を維持するための具体的方法・手段のこと。

デスクトップ環境

X Window System のようなウィンドウシステムにおいて、ユーザーインタフェースやメニュー、各ウィンドウを統一して表現するための規格や仕様のこと。

プログラムソースライブラリ

よく利用されると思われるプログラムソースをまとめたファイルのこと。

システム監査

コンピュータシステムの有効性と効率、信頼性、安全性などを第三者が総合的に点検、評価し、関係者に対して助言や勧告などを行うこと。

更新教育

教育内容の変更の有無に拘わらず、既に教育実施済みの組織のすべての従業員及び関係するならば外部利用者に対し、改めて教育を行うこと。

セキュリティ境界

外壁、カードで制御した入口、又は有人の受付といった障壁を形成することによる保護すべき領域とそうでないものとの境目のこと。

セキュリティ個別方針

組織全体の管理を対象とするのではなく、個別の事業部あるいはプロジェクトの管理を対象とするセキュリティ方針のこと。

フリーソフトウェア

ソフトウェアの開発者が無料で提供し、自由に使用できるソフトウェアの総称のこと。

ファイアウォール

IP 接続された LAN などのネットワーク上に設置する、ハッカーやクラッカーからの侵入や破壊を未然に防ぐためのしくみのこと。

フォルダ

Windows や MacOS で、ファイルやプログラムなどを保存しておく入れ物のこと。

ディレクトリ

ファイルを管理する登録簿のこと。またはファイルを階層構造で管理するための概念のこと。

セキュリティ慣行

情報の機密性、完全性及び可用性の維持のため、習慣（又は常識）として行われていること。

システムユーティリティ

OS やアプリケーションの機能や操作性を改善するためのソフトウェアの総称のこと。

セキュリティ実行標準

ハードウェア及びソフトウェアの管理策を記述した基準のこと。