別紙５

情報セキュリティ要求仕様

1. 情報セキュリティ対策のサービスレベルに関する事項

・情報セキュリティ対策のサービスレベルを保証するための措置を講ずること
＜委託先に求めるサービスレベル（例）＞
(1) 使用するソフトウェアのセキュリティ修正の提供後にこれを適用するまでの期間
(2) 外部からの攻撃等の異常を検知してから当省に報告するまでの時間

2. 情報セキュリティを確保するための体制の整備

2.1. 事業者に求める資格等

・本調達に係る業務を行おうとする事業者又はその部門において、情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価制度に基づくＩＳＭＳ認証又はこれと同等の認証を取得していること

・本調達に係る業務を行おうとする事業者又はその部門は、情報セキュリティ対策ベンチマークを実施し、その結果を提示すること

2.2. 作業要員に求める資格等

・本調達に係る業務を行う事業者は、当該業務の実施において情報セキュリティを確保するための体制を整備すること。なお、本案件に従事する者には、以下のいずれかの資格を有する者を含めること
＜作業要員に求める資格（例）＞
(1) 情報セキュリティスペシャリスト
(2) 公認情報システムセキュリティ専門家(CISSP)
(3) 公認情報セキュリティマネージャー(CISM)
(4) 公認情報セキュリティ監査人(CAIS)
(5) 公認情報システム監査人(CISA)

3. 外部委託する業務以外の情報資産の保全

・委託先に庁舎内で業務を行わせる等、委託先が当省が保有する他の情報資産にアクセスし得る環境で業務を行わせる場合に、当該他の情報資産へのアクセスの禁止及びその保全は委託先が当然守るべき事項であること

4. 運用・保守・点検における情報セキュリティ対策の実施

4.1. 運用・監視

4.1.1. サーバ

（サーバ装置）

・多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、利用を認めるソフトウェア及び禁止するソフトウェアをバージョンを含め提案すること。また、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直すための提案を行うこと

(1) ソフトウェアベンダ等のサポート状況

(2) ソフトウェアと外部との通信の有無及び通信する場合はその通信内容

(3) インストール時に同時にインストールされる他のソフトウェア

(4) その他、ソフトウェアの利用に伴う情報セキュリティリスク

・通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための措置を講ずること

・サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること

・所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には、当省に報告し改善を図ること。なお、当該サーバ装置の構成やソフトウェアの状態を定期的に確認する場合は、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること

・サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、サーバ装置への無許可のアクセス等の不正な行為を監視するため、以下の措置を講ずること

(1) アクセスログ等を定期的に確認すること

(2) 不正プログラム対策ソフトウェアを利用すること

(3) ファイル完全性チェックツールを利用すること

(4) CPU、メモリ、ディスク I/O 等のシステム状態を確認すること

・要安定情報を取り扱うサーバ装置については、運用状態を復元するため、以下の措置を講ずること

(1) サーバ装置の運用に必要なソフトウェアの原本を別に用意しておくこ

と

(2) 定期的なバックアップを実施すること

(3) サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施すること

(4) バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施すること

（ウェブ）

・ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること

5. セキュリティの検証と妥当性確認

・本調達に係る業務を行う事業者は、セキュリティの検証と妥当性確認を行うための専門家による開発者による設計や実装作業の適正性を確認すること

・本調達に係る業務を行う事業者は、コード検査ツール等の利用により、正確かつ効率的なセキュリティの検証と妥当性確認を行うこと

・本調達に係る業務を行う事業者は、セキュリティの検証と妥当性確認を実施すること

・第三者による脆弱性検査を実施しない場合には、実施しない理由を明確にすること

・本調達に係る業務を行う事業者は、第三者による脆弱性検査を実施すること

6. セキュリティ機能の装備

6.1. ログの取得・管理

6.1.1. 構成要素（共通）

・情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。

・情報システムの特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め、管理すること

(1) 事象の主体（人物又は機器等）を示す識別コード

(2) 識別コードの発行等の管理記録
(3) 情報システムの操作記録
(4) 事象の種類
(5) 事象の対象
(6) 正確な日付及び時刻
(7) 試みられたアクセスに関わる情報
(8) 電子メールのヘッダ情報及び送信内容
(9) 通信パケットの内容
(10) 操作する者、監視する者、保守する者等への通知の内容

・取得したログに対する不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定めること。また、ログが取得できなくなった場合の対処方法についても定めること

・悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。また、ログ情報をソフトウェア等により集計し、時系列で表示し報告書を作成する等の作業を自動化する機能を設け、ログを効率的かつ確実に点検、分析及び報告すること

・標的型攻撃に関する措置として、攻撃の初期段階からの経緯を確認する必要があるため、ログは1年間以上保存すること

・情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること

6.1.2. サーバ
（データベース）
・行政事務を遂行するに当たって不必要なデータの操作を検知できるよう、以下の措置を講ずること
(1) 一定数以上のデータの取得に関するログを記録し、警告を発すること
(2) データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発すること

6.1.3. ネットワーク
（リモートアクセス環境）

・VPN 回線を整備してリモートアクセス環境を構築する場合は、主体認証ログの取得及び管理を実施すること

6.2. 不正プログラム対策

6.2.1. 構成要素（共通）

・想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を講ずること

・不正プログラム対策ソフトウェア等及びその定義ファイルは、常に最新のものが利用可能となるような構成とすること。また、不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと

・不正プログラム対策の実施を徹底するため、不正プログラム対策に関する以下の状況を報告すること

(1) 不正プログラム対策ソフトウェア等の導入状況

(2) 不正プログラム対策ソフトウェア等の定義ファイルの更新状況

6.2.2. アプリケーション

（アプリケーションコンテンツ）

・提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下の措置を講ずること

(1) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること

(2) 外部委託により作成したアプリケーションプログラムを提供する場合には、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること

・提供するアプリケーション・コンテンツにおいて、省外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認すること。なお、必要があって当該機能を含める場合は、省外へのアクセスが情報セキュリティ上安全なものであることを確認すること

・提供するアプリケーション・コンテンツに、本来のサービス提供に必要のない省外へのアクセスを自動的に発生させる機能を含めないこと

6.3. 標的型攻撃対策

6.3.1. 構成要素（共通）

・標的型攻撃による組織内部への侵入を低減するため、サーバ装置及び端末について、以下の措置を講ずること

(1) 不要なサービスの機能を削除又は停止すること

(2) 不審なプログラムが実行されないよう設定すること

(3) パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限すること

・USB メモリ等の外部電磁的記録媒体を利用した、組織内部への侵入を低減するため、以下の措置を講ずること

(1) 製造元、製造過程が不明なもの、持ち主がわからないものなど、出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させないよう、接続する外部電磁的記録媒体を事前に特定しておくこと

(2) 外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査すること

(3) サーバ装置及び端末について、自動再生（オートラン）機能を無効化すること

・内部に侵入した攻撃の侵入範囲の拡大の困難度を上げるため、端末の管理者権限アカウントについて、以下の措置を講ずること

(1) 不要な管理者権限アカウントを削除すること

(2) 管理者権限アカウントのパスワードは、容易に推測できないものに設定すること

・情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下の措置を実施すること

(1) 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定し、インターネットに直接接続しないこと

(2) 認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した措置を講ずること

・ 重点的に守るべき業務・情報を取り扱う情報システムについては、高度サイバー攻撃対処のためのリスク評価等のガイドラインに従って、措置を講ずること

6.4. 納入成果物に関する確認・認証取得等

・ 本調達に係る情報システムにおいて取り扱う情報の保護を目的として、ISO/IEC 15408 に基づき必要なセキュリティ機能を設計し、実装すること。当該設計において策定するセキュリティ設計仕様書(ST: Security Target)について ST 確認を受け、その結果を提出すること

・ 本調達に係る情報システムを構成するソフトウェアについて、取り扱う情報の保護を目的とするセキュリティ機能について、ISO/IEC15408 に基づく認証を取得していること

・ 本調達に係る情報システムを構成する機器等について、取り扱う情報の保護を目的とするセキュリティ機能について、ISO/IEC15408 に基づく認証を取得していること

6.5. 主体認証機能

6.5.1. 構成要素（共通）

・ 情報システムへ情報へのアクセスを管理するため、主体を特定し、それが正当な主体であることを検証するため、以下を例とする主体認証方式を決定し、主体の識別及び主体認証を行う機能を設けること
  (1) 知識（パスワード等、利用者本人のみが知り得る情報）による認証
  (2) 所有（電子証明書を格納する IC カード、ワンタイムパスワード生成器当、利用者本人のみが所有する機器等）による認証
  (3) 生体（指紋や静脈等、本人の生体的な特徴）による認証

・ 情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。）すること

・ 単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与しないこと

・ 主体認証を行う情報システムにおいて、主体認証情報が第三者に対して明らかにならないよう、以下の機能を設けること

(1) 送信又は保存時の主体認証情報の暗号化機能
(2) 主体認証情報へのアクセス制限機能

・ 主体認証を行う情報システムにおいて、主体認証情報を他の主体に不正に利用され、又は利用されるおそれを認識した場合の措置として、以下の機能を設けること
(1) 特定の識別コードによる認証を停止する機能
(2) 主体認証情報の再設定を利用者に要求する機能

・ 主体認証を行う情報システムにおいて、利用者に主体認証情報の定期的な変更を求めるため、以下の機能を設けること
(1) 主体認証情報の定期更新を促す機能
(2) 主体認証情報の定期更新の有無を確認する機能
(3) 主体認証情報の定期的な変更を行わなければ、情報システムの利用を継続させない機能

・ 識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう促すこと

・ 主体認証情報の不正な利用を防止するため、主体が情報システムを利用する必要がなくなった場合には、以下の措置を講ずること。また、主体への識別コードの付与に関する記録を消去する場合には、当省による事前の許可を得ること
(1) 主体の識別コードを無効にすること
(2) 主体に交付した主体認証情報格納装置を返還させること
(3) 無効化した識別コードの他の主体への新たな発行を禁止すること

・ 主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずること

・ 知識（パスワード）による認証を用いる場合は、辞書攻撃等によるパスワード解析への耐性を考慮し、パスワード規則（文字種、組合せ、桁数等）のパスワード設定条件を利用者に守らせる機能を設けること

・ 知識（パスワード）による認証を用いる場合は、他の情報システムで利用し

ている主体認証情報を設定しないよう主体に注意を促すこと

・ 共用識別コードを付与する場合は、利用者を特定できる仕組みを設けること（共用識別コードでログインする前に個別の識別コードでログインが必要となる機能等）

・ 共用識別コードを付与する場合は、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること

6.5.2. サーバ

（ウェブ）

・ ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行うこと

・ ウェブコンテンツの編集作業を担当する主体を限定するため、OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除すること

（電子メール）

・ 電子メールクライアントから電子メールサーバへの電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証機能を導入すること

・ 電子メールのなりすましを防止するため、以下の措置を講ずること

(1) SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting & Conformance）等の送信ドメイン認証技術による送信側の措置を行うこと

(2) SPF、DKIM、 DMARC 等の送信ドメイン認証技術による受信側の措置を行うこと

(3) S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名の技術を利用すること

6.5.3. ネットワーク

（リモートアクセス環境）

・ VPN 回線を整備してリモートアクセス環境を構築する場合は、以下の措置を講ずること

(1) 通信を行う端末の識別又は認証
(2) 利用者の認証

・VPN 回線を整備してリモートアクセス環境を構築する場合は、利用開始及び利用停止時の申請手続を整備し、運用すること

6.6. サービス不能攻撃対策
6.6.1. 構成要素（共通）
・ サービス不能攻撃に対抗するため、サーバ装置、端末及び通信回線装置について、以下を例とする措置を講ずること
(1) パケットフィルタリング機能
(2) 3-way handshake 時のタイムアウトの短縮
(3) 各種 Flood 攻撃への防御
(4) アプリケーションゲートウェイ機能

・ サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限する等の機能を設けること

・ サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段を確保すること

・ サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限する等の機能を設けること

・ サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段を確保すること

・ サーバ装置、端末及び通信回線装置に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合は、サービス不能攻撃に対抗するため、以下を例とする措置を講ずること
(1) インターネットに接続している通信回線の提供元となる事業者が別途提供する、サービス不能攻撃に係る通信の遮断等の措置を講ずること

(2) サービス不能攻撃の影響を排除又は低減するための専用の対策装置の導入
(3) サーバ装置、端末及び通信回線装置及び通信回線の冗長化

・ サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定の上、監視方法及び監視記録の保存期間を定め、保管すること

6.6.2. サーバ
（サーバ装置）
・ 障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについては、将来の見通しも考慮し以下の措置を講ずること
(1) 負荷分散装置、DNS ラウンドロビン方式等による負荷分散
(2) 同一システムを２系統で構成することによる冗長化

6.7. 権限管理
6.7.1. 構成要素（共通）
・ 主体の識別コード及び主体認証情報が、第三者等によって窃取された際の被害を最小化するため、以下の措置を講ずること
(1) 業務上必要な場合の限定付与
(2) 必要最小限の権限付与
(3) 管理者権限更新のための専用端末の整備

・ 管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること

6.7.2. サーバ
（データベース）
・ データベースに対する内部不正を防止するため、データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講ずること

6.8. 暗号化・電子署名
6.8.1. 構成要素（共通）
・ 情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利

用した安全なプロトコル及びその運用方法等について、以下の措置を講ずること

(1) 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とし、 複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とすること

(2) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択すること

(3) 暗号化された情報の復号又は電子署名の付与に用いる鍵は、耐タンパ性を有する暗号モジュールへの格納すること

(4) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮すること

(5) 行政事務従事者が暗号化及び電子署名に使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用すること

(6) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること

(7) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること

(8) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること

・ 電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、政府認証基盤の発行する電子証明書を使用すること

・ 署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下を例とする方法により、当該情報の提供を可能とすること

(1) 信頼できる機関による電子証明書の提供

(2) 厚生労働省の窓口での電子証明書の提供

6.8.2. アプリケーション

（アプリケーションコンテンツ）

・ 文書ファイル等のコンテンツの提供において、当該コンテンツが改ざん等なく真正なものであることを確認できる手段がない場合は、「https://」で始まるURLのウェブページから文書ファイル等のコンテンツをダウンロードできるように提供すること

・ 改ざん等がなく真正なものであることを確認できる手段の提供として電子証明書を用いた署名を用いるとき、政府認証基盤（GPKI）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと

6.8.3. サーバ

（データベース）

・ データベースに格納されているデータに対して暗号化を実施すること。また、バックアップデータやトランザクションデータ等についても暗号化を実施すること

・ 鍵に利用するアルゴリズムに対する脆弱性が発見された際には、定められた鍵の管理手順等に従い、速やかに十分な強度の鍵にてデータベースの再暗号化をすること。その際には、古い世代の鍵で暗号化されたバックアップデータとの紐付けも管理すること

・ データベースに機密性3情報を含むデータを格納する場合は、適切にデータを暗号化すること。また、復号に用いる鍵は、データベースとは別の専用装置等に保存の上、定められた鍵の管理手順に従い管理すること

（ウェブ）

・ 通信時の盗聴による第三者への情報の漏えいの防止及び正当なウェブサーバであることを利用者が確認できるようにするため、以下の措置を講ずること

(1) TLS（SSL）機能を適切に用いること

(2) TLS（SSL）機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証

できる認証局（証明書発行機関）により発行された電子証明書を用いること

(3) 暗号技術検討会及び関連委員会（CRYPTREC）により作成された「SSL/TLS暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定すること

6.8.4. ネットワーク

（リモートアクセス環境）

・VPN 回線を整備してリモートアクセス環境を構築する場合は、通信内容の暗号化を実施すること

6.9. アクセス制御

6.9.1. 構成要素（共通）

・情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、利用者やそのグループ属性に基づくアクセス制御の機能を設けること

・利用者やそのグループ属性に基づくアクセス制御のほか、必要に応じて以下の措置を実施すること

(1) 利用時間や利用時間帯によるアクセス制御

(2) 同一主体による複数アクセスの禁止

(3) ネットワークセグメントの分割によるアクセス制御

6.9.2. アプリケーション

（アプリケーションコンテンツ）

・省外向けに提供するウェブサイト等が実際の厚生労働省提供のものであることを利用者が確認できるように、政府ドメイン名を情報システムにおいて使用すること

・利用者が検索サイト等を経由して厚生労働省のウェブサイトになりすました不正なウェブサイトへ誘導されないよう、省外向けに提供するウェブサイトに対して、以下の検索エンジン最適化措置（SEO 対策）を講ずること

(1) クローラからのアクセスを排除しないこと

(2) cookie 機能を無効に設定したブラウザでも正常に閲覧可能とすること

(3) 適切なタイトルを設定すること

(4) 不適切な誘導を行わないこと

・省外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、不審なサイトへのアクセスを防止するための措置を講ずること

6.9.3. サーバ

（サーバ装置）

・要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するため、以下の措置を講ずること

(1) 要保護情報を取り扱うサーバ装置については、クラス２以上の要管理措置区域に設置すること

(2) 施錠可能なサーバラックに設置して施錠すること

(3) 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定すること

(4) 一定時間操作が無いと自動的にスクリーンロックするよう設定すること

（データベース）

・データベースに対する内部不正を防止するため、管理者アカウントを適切に管理すること。なお、必要に応じて、情報システムの管理者とデータベースの管理者は別にすること

・データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しないこと

・データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること

（ウェブ）

・ウェブコンテンツの編集作業を担当する主体を限定するため、ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えないこと

・公開してはならない又は無意味なウェブコンテンツが公開されないよう管理するため、以下の措置を講ずること

(1) 公開を想定していないファイルをウェブ公開用ディレクトリに置かないこと
(2) 初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除すること

・ウェブコンテンツの編集作業に用いる端末を限定するため、以下の措置を講ずること
(1) ウェブコンテンツの更新の際は、専用の端末を使用して行うこと
(2) ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限すること

（電子メール）
・電子メールサーバが電子メールの不正な中継を行わないように設定すること

6.9.4. ネットワーク
（リモートアクセス環境）
・VPN 回線を整備してリモートアクセス環境を構築する場合は、以下の措置を講ずること
(1) リモートアクセスにおいて利用可能な公衆通信網の制限
(2) アクセス可能な情報システムの制限
(3) リモートアクセス中の他の通信回線との接続禁止

6.10. ＩＰｖ６通信回線
6.10.1. ネットワーク
（情報システムへのＩＰｖ６技術）
・IPv6 Ready Logo Program に基づく Phase-2 準拠製品であること

・IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること
(1) グローバル IP アドレスによる直接の到達性における脅威
(2) IPv6 通信環境の設定不備等に起因する不正アクセスの脅威
(3) IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生
(4) アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

・自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずること

7. 製品のサポート期間の確認

・情報システムの構築等又は運用・保守・点検の際に導入する製品（ソフトウェア及びハードウェア）については、当該情報システムのライフサイクルにおけるサポート（部品、セキュリティパッチの提供等）が継続される製品を導入すること。サポートライフサイクルポリシーが事前に公表されていない製品を導入する場合は、サポートが継続して行われるよう計画を提出すること。なお、後継製品に更新する場合の費用は本調達に含むものとすること

8. 脆弱性対策の実施

8.1. ソフトウェア脆弱性対策

8.1.1. 構成要素（共通）

・サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての措置を行い、対象となるソフトウェアについて、サポートサービスを提供すること

・対象となるソフトウェアの脆弱性情報を適宜報告すること

(1) 脆弱性の原因
(2) 影響範囲
(3) 対策方法
(4) 脆弱性を悪用する不正プログラムの流通状況

・サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアのバージョン、脆弱性対策の状況等を定期的に報告すること

・サポート期間を過ぎたソフトウェアを利用する場合は、ソースの内容を熟知しており、かつ迅速に内容を改編できる適切なサポートサービスを提供できる体制を整備すること

・公開された脆弱性の情報がない段階において、その他、端末及び通信回線装置上で採り得る措置の有無について調査を行い、当該措置が有る場合は実施す

ること

・サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等の可否を判断するため、以下の内容を報告すること
(1) 対策の必要性
(2) 対策方法
(3) 対策方法が存在しない場合又は対策が完了するまでの期間に対する一時的な回避方法
(4) 対策方法又は回避方法が情報システムに与える影響
(5) 対策の実施予定
(6) 対策試験の必要性
(7) 対策試験の方法
(8) 対策試験の実施予定

・脆弱性対策を実施する場合には、少なくとも以下の事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。また、対策状況の報告間隔は可能な限り短縮すること
(1) 実施日
(2) 実施内容
(3) 実施者

・セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイルは、信頼できる方法で入手すること

・適用するサーバ装置、端末及び回線装置上で利用するソフトウェアについて、予め検証環境を準備するなどして、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響範囲を事前に確認すること

8.1.2. サーバ
（データベース）
・データベースにアクセスする機器上で動作するプログラムに対して、SQL インジェクションの脆弱性を排除すること

・データベースにアクセスする機器上で動作するプログラムに対して、SQL イン

ジェクションの脆弱性を排除するため、以下を例とする措置を講ずること
(1) ウェブアプリケーションファイアウォールの導入
(2) データベースファイアウォールの導入

（ウェブ）
・ウェブサーバの管理や設定において、不要な機能の停止又は制限等の以下の措置を実施すること
(1) CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とすること
(2) ディレクトリインデックスの表示を禁止すること
(3) ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限すること
(4) ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持すること

・既知の種類のウェブアプリケーションの脆弱性を排除するため、以下を含むウェブアプリケーションの脆弱性を排除する措置を講ずること。また、運用時においても、これらの措置に漏れが無いか定期的に確認し、措置に漏れがある状態が確認された場合は対処を行うこと
(1) SQL インジェクション脆弱性
(2) OS コマンドインジェクション脆弱性
(3) ディレクトリトラバーサル脆弱性
(4) セッション管理の脆弱性
(5) アクセス制御欠如と認可処理欠如の脆弱性
(6) クロスサイトスクリプティング脆弱性
(7) クロスサイトリクエストフォージェリ脆弱性
(8) クリックジャッキング脆弱性
(9) メールヘッダインジェクション脆弱性
(10) HTTP ヘッダインジェクション脆弱性
(11) eval インジェクション脆弱性
(12) レースコンディション脆弱性
(13) バッファオーバーフロー及び整数オーバーフロー脆弱性

9. 情報セキュリティ対策の履行状況の報告
・本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託先は、当省に対して定期的に報告を行うこと

＜履行状況を確認するための委託先による定期報告（例）＞

(1) 本調達仕様において求める情報セキュリティ対策の実績

(2) 委託先における情報の秘密保持等に係る管理状況

10. 情報セキュリティ対策の履行が不十分であると思われる場合の対処

・本調達に係る業務の遂行において、委託先における情報セキュリティ対策の履行が不十分である可能性を委託元が認める場合には、委託先の責任者は、委託元の求めに応じこれと協議を行い、合意した対応を採ることとする

11. 情報セキュリティ対策の遵守方法及び管理体制等に関する確認書の提出

・調達仕様で示された情報システムに装備すべきセキュリティ機能に関する要求事項が確実に履行されるよう、機能の詳細及び実装方法について、確認書等（又は契約の付属書）を作成し提出すること

・調達した機器等に不正な変更が見つかったときに、追跡調査や立入検査等、当省と調達先が連携して原因を調査・排除できる体制を整備していること。

12. 情報セキュリティ監査の実施

・当省が求めた場合に、速やかに情報セキュリティ監査を受け入れること。

13. 情報セキュリティが侵害された場合の対処

・本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、速やかに委託元に報告の上、委託事業を一時中断するなど、必要な措置を講じた上で、契約に基づく対処を実施すること。これに該当する場合には、以下の事象を含む。

(1) 委託先に提供し、又は委託先によるアクセスを認める厚生労働省の情報の外部への漏えい及び目的外利用

(2) 委託先の者による厚生労働省のその他の情報へのアクセス

・本調達に係る業務の遂行において委託先に提供し、又は委託先によるアクセスを認める情報について外部への漏えい、目的外利用等、情報セキュリティ侵害が起き又はそのおそれがある場合には、速やかにこれを委託元に報告すること