

別添2 情報セキュリティ

第1 セキュリティ要求

1. 基本的な考え方

本稿は情報セキュリティにおける様々なパターンを想定した本市の基本的な考え方を示した資料であり、本件調達仕様書を補足するものとなっている。システム構成形態により要不要があるため、必要な事項を参照の上、要件定義時に協議を行うものとする。

なお、本資料のセキュリティ要求に基づき履行状況等についてドキュメントの提出を要求する場合がある。

基本的には自身が持つシステムの脆弱性を内部点検・外部点検等で把握の上、予防的統制として内外の脅威に対してどのように対応するのか、日常的な対策はどうするのか、発見的統制としてインシデント発生時にどのように対応するのかを明らかにすること。

2. 情報セキュリティインシデントへの対処

- (1) 受注者は情報セキュリティインシデントを認知した場合には、後述の対処手順又は本市の指示若しくは是正要求に従って、適切に対処すること。
- (2) 受注者は、本市から応急措置の実施及び復旧に係る指示又は是正要求を受けた場合は、当該指示又は是正要求を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として取りまとめ、本市に報告すること。

3. 情報セキュリティの管理に係るドキュメントの提出

- (1) 受注者は、本業務及び情報セキュリティ管理の履行可能性を証明するため、本業務で取扱う情報等の特性を十分に踏まえ、以下のドキュメントを提出すること。

ア WBS 手法(小日程計画)を用いて、作業工程ごとに必要なアクティビティを分類・定義し、アクティビティごとに必要となる作業量を記載するとともに、それを実現するためのスケジュール及び体制等を含むスケジュール

イ 情報セキュリティ管理計画書

- (2) 受注者は「情報セキュリティ管理計画書」について、要件定義工程終了までに以下の要素を含むドキュメントを整備し、本市に提出の上、開発段階から情報セキュリティ対策を実施すること。

表題	規定内容
①目的外利用の禁止	本業務で知りえた情報の目的外利用を禁止すること。
②従業員の管理体制	本業務の実施に当たり、受注者又はその従業員、本業務の役務の内容の一部を再委託する先、若しくはその他の者による意図せざる不正な変更が情報システムのハードウェアやソフトウェア等に加えられないための管理体制が整備されていること。
③組織の管理体制	受注者の資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性(情報セキュリティに係る資格・研修実績等)・

	実績及び国籍に関する情報提供を行うこと。
④情報セキュリティインシデントへの対処	情報セキュリティインシデントへの対処方法が確立されていること。
⑤履行状況の報告	情報セキュリティ対策その他の契約の履行状況を定期的に確認し、本市へ報告すること。
⑥情報セキュリティ対策の改善	情報セキュリティ対策の履行が不十分である場合、速やかに改善策を提出し、本市の承認を受けた上で実施すること。
⑦本市の情報セキュリティ監査	本市が求めた場合に、速やかに本市の情報セキュリティ監査を受けること。
⑧可用性の担保	本業務において、可用性2情報（行政事務で取り扱う情報資産のうち滅失、紛失又は当該情報資産が利用不可能であることにより住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産。以下同じ。）を取り扱うなど、本市が可用性を確保する必要があると認めた場合は、サービスレベルの保証を行うこと。
⑨再委託先への措置・監督義務	本業務を再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように情報セキュリティ管理計画書に記載された措置の実施を担保すること。
⑩可用性情報の受領手順	本市から可用性2情報を受領する場合は、本市が指示する情報セキュリティに配慮した受領方法にて行うこと。
⑪可用性情報の廃棄手順	本市から受領した可用性2情報が不要になった場合は、本市の指示に従い、これを確実に返却、又は抹消し、書面（廃棄履歴管理簿）にて報告すること。
⑫情報セキュリティインシデントの報告	本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は速やかに本市に報告すること。

4. 情報資産管理標準シートの整備・維持

- (1) 受注者は、別添3 運用・保守「10.システム構成管理」に掲げる事項について記載した情報資産管理標準シートを、設計工程終了までに、本市に提出すること。
- (2) 受注者は、情報システムの現況確認支援として、次に掲げる事項について実施すること。

表題	内容
①現況確認作業（棚卸）	受注者は、年1回、本市の指示に基づき、情報資産管理標準シートと情報システムの現況との突合・確認（以下「現況確認」という。）を実施すること。
②差異の特定と解消	受注者は、現況確認の結果、情報資産管理標準シートと情報システムの現況との間の差異がみられる場合は、運用計画に定める変更管理方法に従い、差異を解消すること。

③ライセンス承諾の確認	受注者は、現況確認の結果、ライセンス許諾条件に合致しない状況が認められる場合は、当該条件への適合可否、条件等を調査の上本市に報告すること。
④サポート切れのソフトウェア	受注者は、現況確認の結果、サポート切れのソフトウェア製品の使用が明らかとなった場合は、当該製品の更新の可否、更新した場合の影響の有無等を調査の上、本市に報告すること。

5. 情報システムの情報セキュリティに係る技術ドキュメントの整備

- (1) 受注者は、情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連の情報セキュリティに係る技術ドキュメントを整備すること。(※システム構成管理関係のドキュメントと一部重複するが、ここでは情報セキュリティ関係の資料一式として整備を行うこととする。重複する部分は同じ内容で構わない。)

表題	内容
①ハードウェア情報	情報システムを構成するサーバ装置及び端末関連情報
②通信回線等情報	情報システムを構成する通信回線及び通信回線装置関連情報 ・通信回線及び通信回線装置を管理する職員を特定する情報 ・通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン ・通信回線及び通信回線装置の仕様書又は設計書 ・通信回線の構成 ・通信回線装置におけるアクセス制御の設定 ・通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応
③情報セキュリティ水準の維持手順	情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順 ・サーバ装置及び端末のセキュリティの維持に関する手順 ・通信回線を介して提供するサービスのセキュリティの維持に関する手順 ・通信回線及び通信回線装置のセキュリティの維持に関する手順
④情報セキュリティインシデントの対処手順	情報セキュリティインシデントを認知した際の対処手順
⑤情報システムの利用者の特定	サーバ装置及び端末を管理する職員及び利用者を特定する情報
⑥ソフトウェアの種類及びバージョン	サーバ装置及び端末の機種並びに利用しているソフトウェアの種類及びバージョン
⑦第三者ソフトウェア及びFOSSの利用状況	サーバ装置及び端末で利用するソフトウェアを動作させるために用いられる他のソフトウェアであって、以下を含むものの種類及びバ

	ーション ・動的リンクライブラリ等、ソフトウェア実行時に読み込まれて使用されるもの ・フレームワーク等、ソフトウェアを実行するための実行環境となるもの ・プラグイン等、ソフトウェアの機能を拡張するもの ・静的リンクライブラリ等、本市がソフトウェアを開発する際に当該ソフトウェアに組み込まれるもの ・インストーラー作成ソフトウェア等、本市がソフトウェアを開発する際に開発を支援するために使用するもの
--	---

6. 機器等の調達に係る情報セキュリティの確保

本業務において、本市にサーバ装置、端末、通信回線装置、複合機、特定用途機器、外部電磁的記録媒体、ソフトウェア等(以下「機器等」という。)を納品、賃貸借等をする場合、受注者は、以下の措置を講ずること。

表題	内容
①製造工程における有害物の混入の回避	納入する機器等の製造工程において、受注者及び本市が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。
②構成機器の不正変更の認知	機器等に対して不正な変更があった場合に識別できる構成管理体制を確立していること。また、不正な変更が発見された場合に、本市と受託者が連携して原因を調査・排除できる体制とすること。
③セキュリティ診断	脆弱性検査等のテストが実施されている機器等を採用し、そのテストの結果が確認できること。
④第三者の評価	コモンクライテリア(ISO/IEC 15408)に基づく認証を取得している機器等を採用することが望ましい。なお、当該認証を取得している場合は、証明書等の写し(もしくは説明資料)を提出すること。
⑤納品物の情報セキュリティに関する品質保証シート	機器等の納品時に、以下の事項を書面で報告すること。 ・セキュリティ要件の実装状況(セキュリティ要件に係る試験の実施手順及び結果) ・機器等に不正プログラムが混入していないこと(最新の定義ファイル等を適用した不正プログラム対策ソフトウェア等によるスキャン結果、内部監査等により不正な変更が加えられていないことを確認した結果等)

7. 情報システムの要件定義における情報セキュリティの確保

受注者は本業務の要件定義工程において、以下の措置を講ずること。

- (1) 開発する情報システムが運用される際に想定される脅威の分析結果並びに当該情報システムにおいて取り扱う情報の格付及び取扱制限に応じて、情報システムに組み込む認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件を適切に策定し、本業務の成果物に明記すること。
- (2) 情報システム運用時に情報セキュリティ確保のために必要となる管理機能を本業務の成果物に明記すること。
- (3) 情報セキュリティインシデントの発生を監視するために必要な機能について、以下を例とする機能を本業務の成果物に明記すること。

表題	機能例
①外部からの不正侵入監視機能	通信回線で接続している箇所における外部からの不正アクセスを監視する機能
②外部への情報漏洩監視機能	不正プログラム感染や踏み台に利用されること等による本市外への不正な通信を監視する機能
③挙動監視	端末等の組織内ネットワークの末端に位置する機器及びサーバ装置において不正プログラムの挙動を監視する機能
④物理端末の不正操作の監視	端末への外部電磁的記録媒体の挿入を監視する機能
⑤サーバの不正操作の監視	サーバ装置等の機器の動作を監視する機能

- (4) 開発する情報システムに関連する脆弱性への対策が実施されるよう、以下を含む対策を本業務の成果物に明記すること。

表題	対策例
①脆弱なソフトウェアの組み込み	既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。
②開発時の情報セキュリティ対策	開発時に情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針を定めること。
③脆弱性への継続的な改善	セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。

8. 情報システムの運用・保守における情報セキュリティの確保

本業務において、情報システムの運用・保守について、受注者は、以下の措置を講ずること。

- (1) 情報システムに実装されたセキュリティ機能を適切に運用するため、以下を実施すること。

表題	措置内容
①運用環境条件との整合	情報システムの運用環境に課せられるべき条件の整備

性の確認	
②監視・連絡	情報システムのセキュリティ監視を行う場合の監視手順や連絡方法
③保守作業時の情報セキュリティ対策	情報システムの保守における情報セキュリティ対策
④運用中の情報セキュリティ対策	運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策

- (2) 情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、本市に速やかに報告すること。
- (3) 本業務において、情報システムのセキュリティ監視について、受注者は、以下の内容を含む監視手順を定め、適切に監視運用すること。
- ① 監視するイベントの種類
 - ② 監視体制
 - ③ 監視状況の報告手順
 - ④ 情報セキュリティインシデントの可能性がある事象を認知した場合の報告手順
 - ⑤ 監視運用における情報の取扱い(機密性の確保)
- (4) 本業務において、運用中の情報システムに脆弱性が存在することを発見した場合、受注者は、速やかに担当部署に報告し、運用・保守要件に従って脆弱性の対策を行うこと。
- (5) 受注者は、情報システムにおいて取り扱う情報について、アクセス制御の設定など、情報システムに実装されたセキュリティ機能が適切に運用されていることを定期的に確認すること。
- (6) 受注者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

9. 情報システムの更改・廃棄における情報セキュリティの確保

本業務において、情報システムの更改又は廃棄を行う場合、受注者は、当該情報システムに保存されている情報について、以下の措置を講ずること。

- (1) 情報システム更改時の情報の移行作業における情報セキュリティ対策
- (2) 情報システム廃棄時の不要な情報の抹消

10. 情報システムの構成要素別の情報セキュリティ対策

受注者は、アプリケーションプログラムの作成等における情報セキュリティの確保として、以下を含む情報セキュリティ対策を実施すること。

- (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) 作成するアプリケーションプログラムに不正プログラムを含まないこと。
- (3) 作成するアプリケーションプログラムに脆弱性を含まないこと。
- (4) 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコン

テンツを提供しないこと。

- (5) 電子証明書等を用いた署名等、作成するアプリケーション・コンテンツの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がある場合には、それをアプリケーション・コンテンツの提供先に与えること。また、電子署名を採用する場合、政府認証基盤(GPKI)等の利用が可能であれば、政府認証基盤により発行された証明書を用いて電子署名を施すこと。
- (6) 作成するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制する等、情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないように、提供方式を定めてアプリケーション・コンテンツを開発すること。
- (7) サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供される等、サービス利用に当たって必須ではない機能がアプリケーション・コンテンツに組み込まれることがないように開発すること。
- (8) 提供されるアプリケーション・コンテンツに、外部のサーバ等へ自動的にアクセスが発生する等、仕様に無い機能が組み込まれていないことを確認すること。必要があつて当該機能を含める場合は、外部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。

11. ウェブサーバの導入・運用における情報セキュリティの確保

受注者は、ウェブサーバの導入・運用における情報セキュリティの確保として、以下を含む情報セキュリティ対策を実施すること。

- (1) ウェブサーバの管理や設定において、情報セキュリティ確保のための対策を講ずること。
- (2) サービスの提供に必要な情報が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。
- (3) LGWAN-ASP で利用するシステムの場合は、lg.jp 等で終わる LGWAN ネットワーク内で使用できるドメイン名を情報システムにおいて使用すること。
- (4) ウェブアプリケーションの開発において、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、以下を含む脆弱性への対策を講ずること。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。

代表的な脆弱性の例

表題	攻撃例
① SQL インジェクション脆弱性	受け付ける SQL 文の組み立て・解釈方法に問題がある場合、攻撃によってデータベースの不正利用が可能となること。
② OS コマンドインジェクション脆弱性	ウェブアプリケーションが、外部からの攻撃により、ウェブサーバの OS コマンドを不正に実行されてしまうこと。
③ ディレクトリトラバーサル脆弱性	ウェブアプリケーションが外部からのパラメータとしてウェブサーバ内のファイル名を直接指定している場合に、攻撃者に任意のファイルを指定され、ウェブアプリケーションが意図しない処理を行ってしまうこと。
④ セッション管理の脆弱	ウェブアプリケーションのセッション ID を取得して、その利用者に

性	なりすましてアクセスされてしまうこと。
⑤ アクセス制御欠如と認可処理欠如の脆弱性	画面やメニュー等の設定不備による悪用が可能となること。
⑥ クロスサイトスクリプティング脆弱性	ウェブページの脆弱性につけこみ不正スクリプトを埋め込み、第三者に攻撃をすること。
⑦ クロスサイトリクエストフォージェリ脆弱性	利用者が何も知らずに攻撃用 Web ページにアクセスすることで、不正なリクエストが第三者に送信されること。
⑧ クリックジャッキング脆弱性	細工された外部サイトを閲覧し操作することにより、利用者が誤操作し、意図しない機能を実行させられること。
⑨ メールヘッダイnjekション脆弱性	フォームなどに備え付けのメールを送信する機能に対して、入力データを改ざんすることで、メールの送信先を変更できること。
⑩ HTTP ヘッダイnjekション脆弱性	Web ブラウザが Web サーバに対して送信する HTTP リクエストに、改行コードを含む不正な文字列を紛れ込ませることで、Web サーバからの HTTP レスポンスを改ざんする。レスポンス内容に任意のヘッダフィールドを追加したり、任意のボディを作成できること。
⑪ eval インjeksiン脆弱性	与えられた文字列をスクリプトのソースとして解釈できることにより不正なコードが実行できること。
⑫ レースコンディション脆弱性	処理の競合により、同時に排他制御が行われていない変数について上書きが発生し、予期せぬ値に変化すること。
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	異常なデータをプログラムに送り込むことで、メモリの領域を超えて領域外のメモリを上書きし、動作が不安定になる、意図しないコードを実行できること。

12. データベースの導入・運用における情報セキュリティの確保

受注者は、データベースの導入・運用における情報セキュリティの確保として、以下を含む情報セキュリティ対策を実施すること。

- (1) データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。
- (2) 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。
- (3) データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できる対策を講ずること。(例 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)
- (4) データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作への防止措置を講ずること。
- (5) データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をすること。

13. クラウドサービスの利用における情報セキュリティの確保

受注者は、クラウドサービスにおける情報セキュリティの確保として、以下を含む情報セキュリティ対策

を実施すること。

- (1) クラウドサービスのデータセンター(バックアップセンターを含む。)は国内に限ること。障害発生時の情報資産の退避先等、いかなる理由があっても日本国外に持ち出すことは禁止する。
- (2) クラウドサービスの廃止、サービス内容の変更等に伴いクラウドセンターを変更する場合は、他のクラウドサービス等に円滑に移行できるよう、十分な期間をもって事前(サービス廃止等の1年以上前が望ましい。)に本市へ通知すること。また、サービス中断時の復旧目標時間を本市へ通知すること。
- (3) 契約を終了する場合、クラウドサービス上に保存された本市のデータについて、CSV ファイルなどの汎用性のあるデータ形式に変換して提供するとともに、クラウドサービス上において復元できないよう抹消し、その結果を本市に書面で報告すること。
- (4) クラウドサービスに係るアクセスログ等の証跡を保存し、本市からの要求があった場合は提供すること。なお、証跡は1年間以上保存することが望ましい。
- (5) インターネット回線とクラウド基盤との接続点の通信を監視すること。
- (6) クラウドサービスに係る業務の一部がクラウドサービス事業者以外の事業者により外部委託されている場合は、当該クラウドサービス事業者以外の事業者についても再委託に関する事項の措置を講ずること。
- (7) クラウドサービスにおける脆弱性対策の実施内容を本市が確認できること。
- (8) クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替等の対策が講じられていること。また、クラウドサービスに障害が発生した場合の復旧時点目標(RPO)等の指標を提示すること。なお、冗長化やバックアップデータを取り扱う場合は、データセンターを地理的に離れた複数の地域に設置するなどの災害対策が講じられていること。
- (9) クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。
- (10) クラウドサービスの利用者が、自らの意思によりクラウドサービス上で取り扱う情報を確実に抹消できること。
- (11) 本業務において、クラウドサービスに係る情報について、要件定義終了までに開示項目や範囲を明記した資料を提出すること。
- (12) 本市に対して、クラウドサービスに係る機密性の高い情報を開示する場合は、本市において、当該情報を審査又は本業務以外の目的で利用しないよう適切に取り扱うため、必要に応じて当該情報に取扱制限を明記するなどの措置を講ずること。
- (13) ISO/IEC27001 又はそれに基づく認証を取得しているクラウドサービスを採用すること。また、当該認証の証明書等の写し(若しくは第三者が確認できる説明資料)を提出すること。
- (14) クラウドサービスの情報セキュリティ水準を証明する以下のいずれかの証明書等の写し(若しくは第三者が確認できる説明資料)を提出すること。
 - ① ISO/IEC27017 又は ISMS クラウドセキュリティ認証制度に基づく認証
 - ② セキュリティに係る内部統制の保証報告書(SOC 報告書(Service Organization Control Report))
 - ③ 情報セキュリティ監査により対策の有効性が適切であることを証明する報告書(クラウド情報セキュリティ監査制度に基づく CS マークが付された CS 証明書等)
 - ④ 政府情報システムのためのセキュリティ評価制度(ISMAP)に基づく認証

- ⑤ 金融機関等コンピュータシステムの安全対策基準(FISC)に基づく認証
- ⑥ 特定非営利活動法人日本セキュリティ監査協会(JASA)に基づく認証のうちゴールド(適合監査)