別添

IT セキュリティに関する開発等の業務における要項

● 開発等用機器及びソフトウェア

JST・受注者側の機器と費用負担

JST 内でシステム開発等の業務を行うために必要な機器及びソフトウェアは JST より貸与する。

JST 以外の場所でシステム開発等の業務を行うために必要な機器及びソフトウェアは受注者が用意することを基本とする。

開発等の業務のために必要となる特殊なソフトウェア等詳細は別途受注者と協議する。

● その他の前提条件

守秘義務

受注者は、本業務の内容及び本業務に関連して開示を受けた又は知り得た相手方の技術的若しくは事業運営に係る一切の情報（以下「機密情報」という）につき最大限の注意をもって秘密を保持し、事前に JST の書面による承諾を受けることなく、本業務の目的外で使用し、又は第三者に開示・漏えいしてはならない。なお、受注者は、自社の従業員を含む本業務に従事する関係者（以下、単に関係者と略す）にのみ機密情報を開示するものとし、本業務に関与しない者には、いかなる手段においても一切機密情報を開示し又は使用させてはならない。また、本件の実施完了後は、本件に関する情報を返却又は確実に破棄すること。

個人情報の取扱い

業務の実施にあたっては、個人情報の保護に関する法令や規範を遵守するとともに、個人情報の保護の重要性を認識し、個人の権利又は利益を侵害することのないよう、個人情報の取扱いを適正に行うこと。

● **情報セキュリティ管理**

受注者は、以下の情報セキュリティ管理事項を遵守すること。

1. **要求事項**

- JST の「情報システムに関する情報セキュリティ対策ガイドライン（委託先用）」「JST ソフトウェア品質管理ガイドライン」に準拠し、システム開発等の業務を実施すること。
- JST の情報セキュリティポリシーに則り、当該システムの「セキュリティ管理手順」を作成し、JST 承認のもと、適宜修正・更新を行うこと。
- 情報データの管理台帳を作成し、情報データのライフサイクルをトレースすること。二次配布が必要な場合、事前に JST に申請し、承認を得たうえで、当該データのライフサイクルについてもトレースすること。
- セキュリティ管理責任者を設定し、責任・権限を明確化すること。
- 管理対象を明確化し、重要性に応じた管理方法を定めること。
- 本基準を逸脱する場合、その内容、理由、代替方法、当該方法でセキュリティを担保する理由等について記録として残し（管理台帳に記入等）、JST に申請し、承認を受けること。

2. **プログラム等の脆弱性対策**

- 開発プログラムの既知の脆弱性は解消しておくため、IPA の「安全なウェブサイトの作り方」等を参考に対応すること。特に、パスワード入力時に、エラーメッセージによって ID 等の存在が確認できないようにしておくこと。納品物として、「安全なウェブサイトの作り方」チェック済みのリストを添付すること。
- 納品前には脆弱性診断を行い、問題のないことを確認しておくこと。その診断結果も納品すること。脆弱性の確認範囲は、IPA だけでなく、JPCERT/CC、US-CERT、各ベンダーサイト等もチェックしておくこと。

- 設計書の内容を考慮したセキュリティ実施手順を踏襲すること。場合によっては、ツールの導入を検討すること。

＜対策例＞

- SQL インジェクション脆弱性
- OS コマンドインジェクション脆弱性
- ディレクトリトラバーサル脆弱性
- セッション管理の脆弱性
- アクセス制御欠如と認可処理欠如の脆弱性
- クロスサイトスクリプティング脆弱性
- クロスサイトリクエストフォージェリ脆弱性
- クリックジャッキング脆弱性
- HTTP ヘッダインジェクション脆弱性
- 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
- パラメータ書換え検査
- エラーページ検証
- CRLF インジェクション検査

- メールヘッダインジェクション脆弱性
- eval インジェクション脆弱性
- レースコンディション脆弱性
- メールアドレス収集ロボット等の対策
- 改ざん対策
- パス名パラメータの未チェック
- 認証検査
- ファイル拡張子検査
- 隠れ URL の検索
- その他ウェブアプリケーション固有の問題の検査
- メールの第三者中継検査
- その他

・ プログラムデバッグのためにソースコードに入れたコメント行、テストプリント文、ワークファイル、あるいは、不要なサンプルファイル等は削除しておくこと。
・ 各パッケージ・機器等の既定値の ID・パスワードは変更しておくこと。
・ 改ざん検知のため、情報が更新されるファイルの保存先については、設計時に JST と調整すること。

3. 開発等の業務に伴うセキュリティ管理実施内容

基本は JST の情報セキュリティポリシーに準ずるが、特に下記事項について確実な管理を行うこと。システムの開発等の業務でサーバにアクセスするパソコンについては、JST に承認された場合を除き、Web 閲覧及びメールの利用は禁止する(アップデートを除く)。

(1) LAN／パソコン管理

・ 本業務で使用する受注者の LAN／パソコン環境は、ファイアウォール、ウイルス対策、Web フィルター、使用者認証等のセキュリティ対策を実施すること。作業開始時に LAN／パソコン環境について示した図及び運用手順を JST に提出し、承認を得ること。JST から、現場確認を求められた場合は、それに速やかに応じること。
・ 受注者の作業環境と JST 間のネットワークについて、JST の指示に従い、セキュリティを確保すること。
・ 本業務の実施に必要な最低限のパソコンを接続し、またパソコンは他の業務と兼用しないこと。
・ 作業の開始前に、本業務で使用するパソコンが既にウイルス等に感染していないことを確認すること。
・ 本業務で使用するパソコンは管理台帳で管理すること。
・ 本業務で使用するパソコンにインストールされているソフトウェアを管理台帳に全て記入すること。また、新しくソフトウェアをインストールするときは、JST に申請し承認を得ること。
・ 本業務で使用するパソコンに業務に必要のないソフトウェアのインストール、私的使用は禁止すること。
・ 本業務で使用するパソコン、及び、同一ネットワーク上に接続されているパソコンにアンチウイルス等インストールされているソフトウェア及び OS のアップデートは、動作保証の範囲内で毎日実施すること。また、アップデート方法について管理台帳に記入し、自動アップデートでない場合は、アップデート実施の日時、内容等の記録を管理台帳に残すこと。

・ 本業務でノートパソコンを使用する場合は、盗難の防止策を施すこと。
・ パソコンを一定時間使わない時は自動ロックすること。

(2) 開発用サーバの管理

・ 本業務で使用する受注者の開発用サーバ環境は、他の業務とは独立した LAN 環境が望ましい。
・ 開発用サーバへのログインについては、ID・パスワード等によるアクセス管理を行い、セキュリティ管理責任者が認めた者以外の操作を禁止すること。

(3) 可搬型外部記憶媒体(USB メモリ、スマホ、SD カード、DVD 等)への書き込み制限について

・ 可搬型外部記憶媒体の管理台帳を作成し、管理責任者を任命すること。
・ 管理責任者は、可搬型外部記憶媒体を施錠したキャビネット等で保管すること。
・ 関係者への貸し出し、返却に当たって、貸し出し管理簿に、貸し出し(返却)日時、貸し出し者、可搬型外部記憶媒体の識別 No を記載すること。
・ 私用の可搬型外部記憶媒体の使用は禁止すること。
・ 不要な可搬型外部記憶媒体は廃棄すること。
・ USB メモリは、パスワードや強制暗号化つき USB メモリとすること。
・ 月 1 回棚卸しを行うこと。
・ 業務上必要のない外部記憶媒体は取り外すこと。
・ 業務上必要のないプリンターは取り外すこと。
・ 外部記憶媒体への接続制限又は接続された場合のログを取得すること。
・ 可搬型外部記憶媒体への書き出しを制限、若しくは書き出しのログを取得すること。

(4) 外部とのデータ授受(メール、媒体等)

・ 本業務、及び、承認されたパソコン／開発用サーバの利用にあたり、可搬型外部記憶媒体の使用は禁止する。ただし業務上不可欠な場合に限り①JST の承認を受けること、②可搬型外部記憶媒体自体又はデータにパスワードを設定すること、を条件として使用を認める。使用範囲は承認を受けた業務及びパソコンのみとし、使用後は当該データを削除すること。
・ 本業務で外部と授受するデータは、授受手順を明確化し、JST に申請し、承認を得たうえで作業を実施すること。
・ それ以外のデータ授受が発生したときは、JST の承認を受けること。対象データは事前に必ずウイルスチェックを行うこと。
・ データの授受にあたっては、データ暗号化、パスワード設定等のセキュリティ対策を施こすこと。
・ 本業務、及び、承認されたパソコン／開発用サーバの利用にあたり、業務以外でのデータの授受は禁止する。

(5) データの持ち出し

・ データを持ち出すノートパソコン(媒体を含む)がある場合は、JST に申請し、承認を受けること。その際、データ暗号化、パスワード設定等のセキュリティ対策を施すこと。

・ 個人情報については理由の如何に関わらず持ち出しを禁止する。
・ 調査・解析等でも、ログ情報は海外に開示しないこと。海外での調査・分析が必要な場合は、JST の了承を得ること。

(6) テストデータの利用

・ 開発等の作業においては、テストデータの利用を原則とすること。
・ 業務上やむを得ずテストデータに本番データを使用する場合は、JST に申請し、必要最小限のデータの提供を受けること。また、データの保護対策を実施すること。

(7) 遠隔操作端末管理

・ 本業務の実施にあたり、サーバを遠隔操作で使用することを JST が承認した場合、端末操作権限の付与・取り消しについて管理を行い、セキュリティ管理責任者が認めた者以外の操作を禁止すること。
・ 接続できるネットワークを限定するための IP アドレス制限を行い、通信路は暗号化すること。

(8) ID／パスワード管理

・ 管理者権限で管理者権限の必要のない作業を行わないこと。
・ 管理者権限のあるアカウントを利用した作業の記録を残すこと。
・ 本業務で使用する操作端末ごとに管理者名及び使用者名、それらの利用権限、担当作業内容及び ID を管理台帳に記入し、JST の承認を受けること。変更（追加、内容の変更、削除）はルールに基づき管理台帳で管理し、JST に報告すること。定期的に、内容の精査を行い、不要な ID は速やかに削除し結果を報告すること。ID は個人ごとに付与し、関係者の変更時に同一 ID の引継ぎは行わないこと。
・ 本業務で使用するパスワードは 13 文字以上、英小文字、英大文字、数字、記号の複合（少なくとも 3 種類以上）であること。ただし、13 文字以上のパスワードが設定できないシステムにおいては、8 文字以上、英小文字、英大文字、数字、記号の複合（少なくとも 3 種類以上）であることとし、原則 90 日毎に更新し、更新した場合はその旨を管理台帳に記入すること。
・ 本業務で使用する ID の複数の使用者による共有は原則禁止する。システム的に実現が不可能であるときは、共有する ID の使用記録を残すこと。作業担当者の変更があった場合は、必ずパスワードの変更を行うこと。
・ 本業務で使用するパスワードを操作端末に記憶させないこと。

(9) 要員管理

・ 関係者に対して、セキュリティに関する教育を実施し、管理台帳に記録すること。
・ 一時的な応援要員についても、作業開始前に教育を実施すること。

(10) 設備・場所

・ 受注者の作業を実施する場所は、何らかの入退室管理機能を備えること。
・ 本業務の実施する施設・場所が、JST 以外の業務と共用の場合は、パーティション等で区分し関係者以外の立ち入りを禁止すること。

(11) セキュリティカード管理(貸与された場合)

- JST から貸与する入退室用セキュリティカードは、台帳等により適切に管理すること。
- 不要になったセキュリティカードは JST へ返却すること。
- 万一、セキュリティカードを紛失した場合は、速やかに JST へ報告すること。
- いかなる場合もセキュリティカードの第三者への貸与は禁止とする。

(12) 納品物

- 電子ファイル等については、納品時点における最新版コンピュータウイルス検索用パターンファイル(DAT ファイル、定義ファイル、シグネチャ)を実装したコンピュータウイルス検知ソフトウェアを用いて、コンピュータウイルス混入についてチェックを行い、納品物の健全性を確保すること。

(13) 貸与品

- 貸与品は、責任者を定めて適切に管理し、紛失や破損の無い様に留意すること。また、本件作業が完了次第、全ての貸与品を速やかに返却すること。

(14) その他

- 管理対象のドキュメント、媒体等は、管理台帳により管理すること。また、施錠したキャビネット等に保管すること。
- JST のサーバ室に入室する際には、記名等、入室記録のための手順に従うこと。
- JST 内及び関係場所においては、許可された場所以外に立ち入らないこと。
- 情報セキュリティインシデントの発生や兆候を発見した場合は、JST に速やかに報告すること。
- JST でセキュリティ監査が実施される際には、JST の要請に応じてセキュリティ監査対応を行うこと。監査で指摘されたことは誠意をもって対応すること。(本件の対応のために多大な工数が必要な場合は、別途調整する。)

4. その他

前述の要件を満足しない場合は、その代替方法を検討・提案し、JST の承認を受けること。