外部サービス利用におけるセキュリティ要件

この要件は、藤沢市（以下「委託者」という。）と事業者（以下「受託者」という。）が締結する契約（以下「本契約」という。）において、本契約に係る個人情報を取り扱うに当たり、受託者が外部サービスを利用する際に従うべき基準を明示するものです。

1　情報を取り扱う場所について

（1）情報の取扱い場所は国内かつ国内法の適用範囲のみを可能とすること。

（2）日本データセンター協会が制定するデータセンターファシリティスタンダードのティア3相当の基準を満たした環境とすること。

2　外部サービス提供者について

（1）原則として、情報セキュリティマネジメントシステム（ISO/IEC 27001）やクラウドサービスセキュリティ（ISO/IEC 27017）等の国際規格の認証を取得していること。

（2）委託者が登録したデータは、委託者に確実に提供でき、提供後のデータの所有権・管理権は、委託者が保有すること。また、外部サービスの利用を通じて委託者が取り扱う情報の外部サービス提供者における目的外利用を禁止すること。

（3）外部サービス提供者における情報セキュリティ対策の適切な整備・運用及び管理体制を確保すること。

（4）外部サービスの提供内容について、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、委託者の意図しない変更が加えられないことを確認できる管理体制を確保すること。

（5）外部サービス提供者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築及び発生した情報セキュリティインシデントへの対処方法を策定すること。

（6）外部サービスの情報セキュリティの確保における外部サービス提供者及び利用者の役割及び責任範囲を明確化すること。

（7）情報セキュリティ監査の受入れが可能なこと。

（8）外部サービス提供者がその役務の一部で再委託を行ったり、他社のサービスを利用したりする場合は、これ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、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、委託者の求めに応じて再委託先やサービス利用先等の情報セキュリティ対策の実施状況を確認するために必要な情報を委託者に提供し、委託者の承認を受けること。

（9）外部サービス事業者が利用する機器等を廃棄する際は、セキュリティを確保した対応を行うこと。

3　外部サービスについて

(1)原則として、ISMAP(政府情報システムのためのセキュリティ評価制度)やクラウド情報セキュリティ監査制度等の各種認証を取得していること。

(2)外部サービスに係るアクセスログ等の証跡を保存すること。なお、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点から、証跡は原則1年間以上保存すること。

(3)ファイアウォール等を導入するなどして必要な通信だけを許可するよう設定すること。また、利用する外部サービスとセキュリティ要件の異なるネットワーク間との接続点の通信の監視や、必要に応じて死活監視による機器の停止を検知すること。

(4)不正アクセス対策として、IP アドレスやクライアント証明書などによるアクセス制御を実施すること。

(5)外部サービスにログインする際は、原則として個人ごとにIDを設け、パスワードは十分な長さ(8文字以上推奨)とし、文字列は想像しにくいもの(アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等)設定できること。

(6)外部サービス上で取り扱う情報の改ざん、漏洩を防ぐための暗号化及び暗号鍵の保護並びに管理を確実に行うこと。暗号化を用いる場合は、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」に記載されている方法を採用すること。なお、利用する鍵長については、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致した鍵長を用いること。

(7)業務の性質に応じて冗長化を検討する。冗長化を行う場合は、地理的に離れた複数の地域に設置するなどの災害対策を講じること。

(8)外部サービスの中断や終了時に際し、円滑に業務を移行するための対策として、サービス中断時の復旧要件や、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法等の対策を実施すること。

(9)外部サービスの契約を終了する場合、外部サービス上に保存されたデータについて、CSVデータなどの汎用性のあるデータ形式に変換して提供すること。また、外部サービス上において復元できないようデータを抹消し、証明書を提出すること。

(10)外部サービスを構築するサーバに等にはマルウェア対策を実施すること。

(11)外部サービス提供者が、保守等のため外部サービスに接続する場合は、接続する端末を特定し、アクセス制御や通信の暗号化などの不正アクセス対策を実施すること。また、マルウェア対策を実施すること。

(12)業務の性質に応じてバックアップの必要性を検討すること。外部サービス事業者のバックアップ機能を利用する場合、外部サービス事業者にバックアップ機能の仕様を要求し、その仕様を確認すること。また、その機能の仕様が委託者の求める要求事項を満たすことを確認すること。外部サービス事業者からバックアップ機

能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行うこと。また、バックアップデータは当該システムとは切り離された環境や上書き不可能な環境に保存するなどのランサムウェア対策を実施すること。

(13)外部サービスの構成要素の全てについて、脆弱性が発見され対応パッチが公開された際は、原則として1週間以内に適応させること。1週間以内に対応できない場合は、適応時期や適応までの暫定対応を検討し、委託者の承認を得ること。

（以下余白）