周南市外部サービス利用基準

目次

１　はじめに 1
（１）目的 1
（２）本基準の位置づけ 1
（３）「外部サービス」の定義 1
（４）外部サービス利用の特性 1
２　外部サービスの利用判断基準 3
（１）機密性２以上の情報を取り扱う場合 3
（２）機密性２以上の情報を取り扱わない場合 3
３　外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規定 3
４　外部サービス（機密性２以上の情報を取り扱わない場合）の利用に関する規定 3
５　利用申請の許可権限者への外部サービスの利用申請 4
（１）外部サービス利用申請の許可権限者 4
（２）外部サービスの利用申請 4
６　その他 4

改訂履歴

令和５年９月２０日　策定

１　はじめに

（１）目的

周南市外部サービス利用基準（以下「本基準」という。）は、「周南市情報セキュリティ基本方針」及び「周南市情報セキュリティ対策基準」に基づき、本市において外部サービスを利用する際の判断基準や手続の基本的な事項を定めることを目的とする。

（２）本基準の位置づけ

本基準は、「周南市情報セキュリティ対策基準」で統括情報セキュリティ責任者が整備することとしている以下の事項について定めたものである。

・第８章第２節（１）「外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規定」
・第８章第２節（２）「外部サービス利用判断基準」
・第８章第２節（４）「利用申請の許可権限者への外部サービスの利用申請」
・第８章第３節（１）「外部サービス（機密性２以上の情報を取り扱わない場合）の利用に関する規定」

（３）「外部サービス」の定義

外部サービスとは、本市以外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。

（具体例）

・クラウドサービス（Ｗｅｂ会議サービス、ＳＮＳ（ソーシャルネットワーキングサービス）、検索サービス、翻訳サービス、地図サービス、生成ＡＩ等）
・ホスティングサービス

（４）外部サービス利用の特性

外部サービスの利用にあたっては、情報の管理、処理等をサービス提供者に委ねる外部サービスの特性に鑑み、以下のような留意点があることを踏まえて、適切なサービスの選定を行うこと。

①外部サービスは、そのサービス提供の仕組みの詳細を利用者が知ることがなくても手軽に利用できる半面、運用の詳細は公開されないために利用者にブラックボックスとなっている部分があり、利用者の情報セキュリティ対策の運用において必要な情報（サービス利用者が登録したデータの取り扱い方法等）の確認が困難な場合がある。

②外部サービス提供者が所有するハードウェア（サーバ等）の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者の情報やプログラムをハードウェアで共用することとなるため、情報が漏えいする

リスクを把握、評価することが困難である。

③外部サービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることにより、当該サーバ装置に保存されている情報に対し、現地の政府等による検閲や接収を受ける等のカントリーリスクが存在する。

④サーバ装置等機器の整備環境が外部サービス提供者の都合で急変する場合、サプライチェーンリスク[1]への対策の確認が容易ではない。

⑤オンプレミス[2]と外部サービスの併用や外部サービスと他の外部サービスの併用等、多様な利用形態があるため、利用者と外部サービス提供者との間の責任分界点やサービスレベルの合意が容易ではない場合がある。

⑥外部サービス提供者は、保存した情報を自由に利用することが可能な場合がある。また、約款及び利用規約等でその旨を条件として明示していない場合がある。加えて、外部サービス提供者は、利用者から収集した種々の情報を分析し、利用者の関心事項を把握し得る立場にある。

⑦情報が改ざんされた場合でも、利用形態 （例：無償サービス等、約款によって責任を取らないと明記している場合）によっては外部サービス提供者が一切の責任を負わない場合がある。

⑧保存した情報が誤って消去又は破壊されてしまった場合に、外部サービス提供者が情報の復元に応じない可能性がある。また、復元に応じる場合でも復旧に時間がかかることがある。

⑨利用上の不都合、不利益等が発生しても、サービス提供者が個別の対応には応じない場合が多く、万が一対応を承諾された場合でも、多くの時間を要することがある。

⑩外部サービスの利用開始後であっても、サービス提供者側の都合で、約款及び利用規約の内容が、事前通知等なしで一方的に変更されることがある。

⑪外部サービス提供者の事情等で、予期せぬサービス停止に陥ることがある。また、その際に保存した情報の取扱いは保証されず、損害賠償も行われない場合がある。約款の条項は一般的にサービス提供者に不利益が生じないようになっており、このような利用条件に合意せざるを得ない。また、サービスの復旧についても保証されない場合が多い。

⑫保存した情報の取扱いが保証されず、一旦記録された情報の確実な消去は困難である。

---

[1] 企業等が製品やサービスを提供するために依存している関連会社などに起因するセキュリティ上のリスク

[2] サーバ、ソフトウェア等の情報システムを、自分が管理する施設内に設置して運用する形態

２　外部サービスの利用判断基準

（１）機密性２以上の情報を取り扱う場合

外部サービスにおいて機密性２以上の情報を取り扱う場合、本基準「３　外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規定」を満たす外部サービスを利用すること。

（２）機密性２以上の情報を取り扱わない場合

外部サービスにおいて機密性２以上の情報を取り扱わない場合、本基準「４　外部サービス（機密性２以上の情報を取り扱わない場合）の利用に関する規定」を満たす外部サービスを利用すること。

３　外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規定

情報セキュリティ管理者は、機密性２以上の情報を取り扱う外部サービスを利用する場合、別紙「外部サービス要件一覧」にまとめた要件を基に、必要な事項を外部サービスの選定条件とすること。なお、任意としている項目については、要件を満たしていないことの影響を考慮して、サービスを選定すること。

①セキュリティに係る国際規格等の資格・認証の取得

②情報セキュリティ対策の実施

③サービスの中断や終了時に円滑に業務を移行するための対策

④情報セキュリティ監査の受入れ

⑤サービスレベルの保証

⑥本市の情報を取り扱う場所及び契約に定める準拠法・裁判管轄

⑦サービス提供者がその役務内容を一部再委託する場合の、サービス提供者の　選定条件で求める内容の担保、及び再委託先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の提供

⑧外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティの確保

４　外部サービス（機密性２以上の情報を取り扱わない場合）の利用に関する規定

情報セキュリティ管理者は、機密性２以上の情報を取り扱わない外部サービスを利用する場合には、本基準「１　はじめに（４）外部サービス利用の特性」に記載した留意点等から生じるリスクを受容するか、又はそれをリスク低減するための措置を講ずることが可能であるかを十分検討した上で、必要な選定条件を定め、利用を決定すること。

５　利用申請の許可権限者への外部サービスの利用申請

（１）外部サービス利用申請の許可権限者

情報システム管理者を外部サービス利用申請の許可権限者とする。

（２）外部サービスの利用申請

外部サービスの利用にあたっては、周南市職務権限規程（平成１５年４月２１日規程第５号）別表第２の定めるところにより、事前に審査、利用承認を受けること。業者決定後、下記手順により利用申請を行うこと。

①情報セキュリティ管理者は、外部サービスを利用する場合には、利用申請の許可権限者と事前協議した上で、利用申請の許可権限者に外部サービスの利用申請を行うこと。

②利用申請の許可権限者は、外部サービスの利用申請を審査し、可否を決定すること。

③利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして、以下の内容を外部サービス利用台帳に登録すること。また、期間の延長や廃止等変更がある場合は、更新すること。

（ア）外部サービスの名称（必要に応じて機能名までを含む）

（イ）外部サービス提供者の名称

（ウ）利用目的（業務内容）

（エ）取り扱う情報の格付

（オ）利用期間

（カ）利用申請者（所属・氏名）

（キ）利用者の範囲（自組織の関係者内に限る、部局内に限る など）

６　その他

情報セキュリティ管理者は、本基準に定める内容のほか、取り扱う情報資産やサービス等の内容を考慮して、個別に適切な選定条件を定めること。

附　則

この利用基準は、令和５年９月２０日から施行する。

別紙「外部サービス要件一覧」

＜必須／推奨／任意について＞
必須：満たす必要がある要件
推奨：満たすべきだが、代替サービスが他にない場合等に満たさないことを許容できる要件
任意：必須ではないが、満たさない場合の影響を考慮する必要がある要件

項番	規定番号	区分	要件	必須／推奨／任意	適用状況
1	①	セキュリティ評価制度	利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））への登録が行われていること。	推奨	
2		資格・認証（国際規格） ※アプリケーション 提供事業者	サービス提供を行う組織（アプリケーション提供事業者）が、ISO/IEC 27001認証の取得もしくは同等の取扱いを行うこと。	任意	
3		プライバシーマーク ※アプリケーション 提供事業者	サービス提供を行う組織（アプリケーション提供事業者）が、Pマーク（プライバシーマーク）を取得していること。	任意	
4		資格・認証（国際規格） ※クラウドサービス プロバイダー	サービス提供を行う組織（クラウドサービスプロバイダー）が、ISO/IEC 27001認証を取得していること。	推奨	
5			サービス提供を行う組織（クラウドサービスプロバイダー）が、ISO/IEC 27017認証を取得していること。	推奨	
6			サービス提供を行う組織（クラウドサービスプロバイダー）が、ISO/IEC 27018認証を取得していること。	任意	
7		プライバシーマーク ※クラウドサービス プロバイダー	サービス提供を行う組織（クラウドサービスプロバイダー）が、Pマーク（プライバシーマーク）を取得していること。	任意	
8		データセンター要件	データセンターは、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設備とすること。	推奨	
9	②	情報セキュリティ対策	サービス提供業務の遂行のために提供する情報（契約等の手続に付随して外部サービス事業者が知りうる利用者情報等）を、サービス提供業務の遂行目的外で利用しないこと。情報の目的外利用の禁止に対する遵守（義務）の表明をすること。	必須	
10			サービス提供を行う組織若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制について提示すること。	必須	
11			サービス提供事業の事務所、運用場所（地域（リージョン）が特定できるようにすること）を情報提供すること。提供にあたっては文書にて内容を確約すること。	必須	
12			情報セキュリティインシデントが発生した場合に、被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について提示すること。	必須	
13			障害や情報セキュリティインシデントの発生、監査結果等によって、情報セキュリティ対策の履行が不十分であると認められた場合の対処（改善の実施等）方法について提示すること。	必須	
14	③	外部サービス終了時	次期サービスへ移行するためのデータ提供が可能なこと。	必須	
15			データを消去する際に、データを復元できないように電子的に完全に消去又は廃棄すること。また、データを消去又は廃棄した証明書を提示すること。	必須	
16	④	セキュリティ監査	第三者による情報セキュリティ監査の受入れが行われていること。	任意	
17	⑤	SLA（Service Level Agreement）	サービスレベルの保証が定められていること。 （例：サービス提供時間、稼働率、バックアップの取得頻度、問合せへの応答時間　など）	任意	
18		データの所在・適用法と裁判管轄	サービス上のユーザ所有データ（バックアップデータを含む。）の所在地が日本国内に限定できること。	推奨	

項番	規定番号	区分	要件	必須／推奨／任意	適用状況
19	⑥		準拠法、裁判管轄を国内に指定できること。	推奨	
20			市が登録したデータは、本市に確実に提供でき、提供後のデータの所有権・管理権は、市が保有すること。また、市が登録したデータは、本契約に明示的に定められているところを除き、本市の承諾なく、利用できないものとすること。	必須	
21	⑦	再委託	サービス提供を行う組織が本市の情報を取り扱うに際して、その取り扱いを再委託していない、または、再委託する場合に事前に通知または公開すること。	必須	
22	⑧	データ暗号化	機密性の高いデータについて、暗号化等によって蓄積・伝送データを保護できること。	必須	
23		ログ取得	外部サービス上におけるアクセスログ等の証跡に係る保存期間について、一定期間の保存が可能であること。その手法について提示すること。	必須	
24		脆弱性対策	外部サービス上の脆弱性を発見する方法があり、実施可能であること。その手法について提示すること。	必須	
25		不正アクセス対策	通信内容を監視する等により、不正アクセスや不正侵入を検知及び通知できること。	必須	
26		機器停止	機器に異常があった場合、検知できること。 また、機器を死活監視し、停止した場合、検知できること。	必須	
27		データ取扱い時の権限管理	データの取り扱いについて、権限管理及びアクセス制御ができること。	必須	
28		保守端末	保守端末は、認証管理、持出管理、施錠管理、ログ管理等によりセキュリティを確保していること。	必須	