乙訓福祉施設事務組合外部サービスを利用する利用基準

１　基本的な考え方

（１）目的

この基準は、乙訓福祉施設事務組合（以下「本組合」という。）においてクラウドサービスやウェブ会議サービス等の外部サービス（以下「外部サービス」という。）を利用する際の手続や、利用に当たって必要なセキュリティ対策等の基本的な事項を定めることを目的とする。

（２）適用範囲及び用語

この基準の適用範囲及び用語の意義は、乙訓福祉施設事務組合情報セキュリティポリシーの適用範囲とする。

２　外部サービス利用判断基準

（１）　自治体機密性２以上の情報資産を取り扱う場合

外部サービスにおいて自治体機密性２以上の情報を取り扱う場合は、３．１外部サービスの選定条件を満たす外部サービスを利用しなければならない。

（２）　自治体機密性２以上の情報資産を取り扱わない場合

外部サービスにおいて自治体機密性２以上の情報資産を取り扱わない場合は、４．１外部サービスの選定条件を満たす外部サービスを利用しなければならない。

（３）　乙訓福祉施設事務組合情報セキュリティポリシーの適用範囲外における外部サービスの利用

乙訓福祉施設事務組合情報セキュリティポリシーの適用範囲外において外部サービスを住民等に利用させる場合は、この基準に準じて適切な外部サービスを選定しなければならない。

（４）　外部サービスを利用する上での留意事項

外部サービスの利用に当たっては、情報の管理や処理を外部サービス提供者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなる。外部サービスを利用する目的、利用する業務の範囲を明確化した上で、適切な外部サービス提供者を選定し、次のリスクの低減を図る。

①　情報の管理や処理を外部サービス提供者に委ねるため、その情報の適正な取り扱いの確認が容易ではない。外部サービス提供者の運用詳細等が公開されない場合は、利用者が情報セキュリティ対策を行うことが困難となる。

②　オンプレミス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。

③　外部サービス提供者が所有する資源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一つの外部サービス基盤で共用することとなるため、情報が漏えいするリスクが存在する。

④　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るカントリーリスクが存在する。

⑤　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・リスクへの対策の確認が容易ではない。

３　外部サービスの利用（自治体機密性２以上の情報資産を取り扱う場合）

３．１　外部サービスの選定条件

情報セキュリティ責任者は、自治体機密性２以上の情報資産を取り扱う外部サービスを利用する場合は、以下の内容を含む対策を外部サービス提供者の選定条件に含めること。

（１）　外部サービスのセキュリティ要件

情報セキュリティ責任者は、外部サービスのセキュリティ要件としてセキュリティに係る国際規格（ＩＳＯ／ＩＥＣ２７００１及びＩＳＯ／ＩＥＣ２７０１７）等と同等以上の水準を求めること。

（２）　外部サービス提供者の信頼性が十分であることの総合的・客観的な評価・判断

情報セキュリティ責任者は、外部サービスに対する情報セキュリティ監査による報告書の内容、各種の認定、認証制度の適用状況等（例：ＩＳＭＳ認証の国際規格、ＩＳＭＡＰの管理基準を満たしていることや外部サービス提供者等のセキュリティに係る内部統制の保証報告書であるＳＯＣ報告書等）から、外部サービス及び当該サービスの委託先（再委託を含む。）の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

（３）　流通経路全般にわたるセキュリティの適切な確保のためのセキュリティ要件

情報セキュリティ責任者は、外部サービス部分を含む情報の流通経路全般にわたるセキュリティ対策を実施する必要がある。システムの重要度に応じて求められる自治体可用性のレベル等（稼働率、目標復旧時間、バックアップの保管方法等）を調達の際に仕様書に具体的に盛り込まなければならない。

（４）　情報が取り扱われる場所等

情報セキュリティ責任者は、外部サービスの利用を通じて本組合が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクがある外部サービス提供者を選定してはならない。（例：データセンター及び外部サービスを提供するリージョン（国・地域）を日本国内に限定する。）

（５）　再委託をする場合

情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、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、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、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を本組合に提供し、本組合の承認を受けるよう、外部サービス提供者の選定条件に含めること。

（６）　外部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

情報セキュリティ責任者は、取り扱う情報の自治体可用性区分に応じて、サービスの中断、終了又は変更の際の影響を最小限に抑えることができるよう次の要件を含めたシステム並びにデータのバックアップ計画及び設計を外部サービス提供者に求めなければならない。

①　取り扱う情報の自治体可用性区分の格付けに応じた、サービス中断時の復旧要件

②　取り扱う情報の自治体可用性区分の格付けに応じた、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

（７）　セキュリティ対策

情報セキュリティ責任者は、次のセキュリティ対策を外部サービス提供者に求め、対応できることを外部サービス提供者の選定条件に含めること。

①　外部サービスの利用を通じて本組合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の禁止（例：本組合で取り扱う情報は、外部サービス提供者において外部サービスの提供に必要な範囲で利用を認めるものであって、それ以外の目的で利用をさせてはならない。）

②　外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制の提示

③　外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先その他の者によって、本組合の意図しない変更が加えられないための管理体制の提示

（例：具体的に外部サービス提供者の選定条件に含める内容としては、例えば以下が考えられる。

（ア）　外部サービスの開発及び運用において、本組合の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。

（イ）　外部サービスに本組合の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、本組合と外部サービス提供者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。また、当該体制が書類等で確認できること。）

④　外部サービス提供者の資本関係、役員等の情報及び外部サービス提供に従事する者の所属の提示

（例：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並びに調達仕様書による施設の場所やリージョン（国・地域）の提示）

⑤　情報セキュリティインシデントへの対処方法

外部サービス提供者において発生した情報セキュリティインシデントによる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）の提示

（例：対処方法

（ア）　復旧を優先する場合は、外部サービスの利用を一時的に停止するための手順を規定する。

（イ）　業務継続を優先する場合は、外部サービスの利用を継続した上で情報セキュリティインシデントに対処する手順を規定する。

（ウ）　情報セキュリティインシデントに係る外部サービス提供者と本組合間の情報エスカレーション方法やそのタイミングについて規定する。）

⑥　脅威に対する外部サービス提供者の情報セキュリティ対策（なりすまし、情報漏えい、情報の改ざん、否認防止、権限昇格への対応、サービス拒否・停止等）の実施状況やその他の契約の履行状況の確認方法の提示

⑦　情報セキュリティ対策の履行が不十分な場合の対処方法の提示

３．２　外部サービスの利用に係る調達・契約

①　情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。また、調達仕様の内容を契約に含める際、外部サービス提供者との情報セキュリティに関する役割及び責任の範囲が明確になっていることを確認すること。

②　情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

３．３　外部サービスを利用した情報システムの導入・構築時の対策

情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、次の事項を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を実施すること。

（１）　アクセス制御に関する事項

・　外部サービスを利用する際に外部サービス提供者が付与又は外部サービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管

理

- 外部サービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御
- 外部サービスを利用する情報システムの管理者特権を保有する外部サービス利用者に対する強固な認証技術の利用
- 外部サービス利用者による外部サービスに多大な影響を与える操作の特定と誤操作の抑制
- 外部サービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施
- インターネット等の外部の通信回線から庁内通信回線を経由せずに外部サービス上に構築した情報システムにログインすることの要否の判断及び情報システムへのログインを認める場合の適切なセキュリティ対策の実施

（２） 暗号化に関する事項

取り扱う情報の自治体機密性に応じた保護のための適切な暗号化処理を実施する。（例：外部サービス内及び通信経路全般における暗号化、利用する情報システムに係る法令や規則に対する暗号化方式の遵守度合い）

（３） 設計・設定及び開発に関する事項

- 外部サービスの利用の企画、要件の確認の段階から想定される脅威やリスクに対するセキュリティ対策の実施（例：開発手順等の情報を要求、外部サービス上に他ベンダが提供するソフトウェア等を導入する場合の当該ソフトウェアの外部サービス上におけるライセンス規定）
- 外部サービス内における時刻同期の方法の確認
- 設計・設定時の誤りの防止の対応として、設計書や設定の知見等の情報の要求（例：設計書や設定のレビューやクラウドサービスのフレームワークとの比較）
- 外部サービス上に情報システムを構築する際の設定の誤りを見出すための対策
- 外部サービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視
- 利用する外部サービス上の情報システムが利用するデータ容量や稼働性能についての監視や業務継続に向けた報告
- 利用する外部サービス上で自治体可用性に応じた設計を確認

３．４　外部サービスを利用した情報システムの運用・保守時の対策

① 情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、次の事項を含む外部サービスを利用して情報システムを運用する際のセキュ

リティ対策に留意すること。

（ア）　運用・保守時における利用方針に関する事項

・　責任分界点を意識した外部サービスの利用

・　利用承認を受けていない外部サービスの利用禁止

・　外部サービス提供者に対する定期的なサービスの提供状態の確認

・　利用する外部サービスに係る情報セキュリティインシデント発生時の連絡体制

（イ）　運用・保守時における教育に関する事項

・　外部サービス利用のための規定及び手順について定め、利用者に周知

・　外部サービス利用に係る情報セキュリティリスクとリスク対応について利用者に周知

・　外部サービス利用に関する適用法令や関連する規制等について利用者に周知

（ウ）　運用・保守時における資産管理に関する事項

・　外部サービス上で利用するＩＴ資産の適切な管理

・　外部サービス上に保存する情報に対する適切な格付・取扱制限の明示

・　外部サービスの機能に対する脆弱性対策について、外部サービス利用者の責任範囲の明確化と対策の実施

（エ）　運用・保守時におけるアクセス制御に関する事項

・　管理者権限を外部サービス利用者へ割り当てる場合のアクセス管理と操作ログの取得

・　外部サービス利用者に割り当てたアクセス権限に対する定期的な見直し

・　外部サービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限

・　利用する外部サービスの不正利用の監視

（オ）　運用・保守時における暗号化に関する事項

・　外部サービス上に保存するデータに対する暗号化に用いる仕組みや鍵の管理方法について確認

・　鍵管理機能を外部サービス提供者が提供するものを利用する場合、鍵管理手順と鍵の種類の情報を確認

・　鍵管理機能を外部サービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報を確認

（カ）　運用・保守時における外部サービス内の通信に関する事項

・　利用する外部サービスのネットワーク基盤が他のネットワークと分離されていることの確認

（キ）　運用・保守時における設計・設定に関する事項

・　外部サービスの設定を変更する場合の設定の誤りを防止するための対策

・　外部サービス利用者が行う可能性のある重要操作の手順書の作成
・　利用する外部サービスの仮想マシンのネットワークが他の利用者のネットワークと分離されていることを外部サービス提供者の開示している情報等で確認する。

（ク）　運用・保守時における事業継続に関する事項

・　不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施
・　自治体可用性２の情報を外部サービスで取り扱う場合の十分な自治体可用性の担保、復旧に係る手順の策定と定期的な訓練の実施
・　外部サービス提供者からの変更通知の内容確認と復旧手順の確認
・　外部サービスで利用しているデータ容量、性能等の監視

（ケ）　運用・保守時におけるインシデント対応に関する事項

・　利用者が、外部サービスにおける情報セキュリティインシデントや情報の目的外利用等を認知した場合、情報セキュリティ責任者へ報告する。
・　情報セキュリティ責任者は、利用者からインシデント報告を受けた場合の対応手順を定める。

３．５　外部サービスを利用した情報システムの更改・廃棄時の対策

情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、次の事項を含む外部サービスの利用を終了する際のセキュリティ対策を実施すること。

（ア）　外部サービスの利用終了時における対策に関する事項

・　外部サービスの利用を終了する場合の移行計画書又は終了計画書の作成
・　移行計画書又は終了計画書の外部サービス利用者への事前通知

（イ）　外部サービスで取り扱った情報の廃棄に関する事項

・　情報の廃棄方法の確認

（ウ）　外部サービスの利用のために作成したアカウントの廃棄に関する事項

・　作成された外部サービス利用者アカウントの削除
・　利用した管理者アカウントの削除・返却と再利用の確認
・　外部サービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

４　外部サービスの利用（自治体機密性２以上の情報資産を取り扱わない場合）

４．１　外部サービスの選定条件

統括情報セキュリティ責任者又は情報セキュリティ責任者は、自治体機密性２以上の情報資産を取り扱わない外部サービスを利用する場合には、以下の内容を含む対策

を外部サービス提供者の選定条件に含めること。

（１）　外部サービスを利用可能な業務の範囲

統括情報セキュリティ責任者又は情報セキュリティ責任者は、次のようなリスクを受容し、又は低減するための措置を講ずることが可能であることを検討した上で、許可する業務の範囲を決定すること。また、許可をする場合には、外部サービスを利用する目的、利用する業務の範囲を明確化し、適切な外部サービス提供者を選定すること。

（ア）　外部サービス提供者は、保存された情報を自由に利用することが可能である。また、約款、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。

（イ）　情報が改ざんされた場合でも、利用形態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。

（ウ）　突然サービス停止に陥ることがある。また、その際に預け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。

（エ）　保存された情報が誤って消去され、又は破壊されてしまった場合に、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。

（オ）　約款及び利用規約の内容が、外部サービス提供者側の都合で利用開始後事前通知等無しで一方的に変更されることがある。

（カ）　情報の取扱いが保証されず、一度記録された情報の確実な消去は困難である。

（キ）　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、その対応には時間を要することが多い。

（ク）　外部サービスで提供される情報が国外で保存・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、現地の政府等による検閲や接収を受ける可能性がある。

（２）　外部サービスの利用の留意点

情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱わない前提で外部サービスを業務に利用する場合は、次のことに留意すること。

①　サービス利用中の安全管理に係る運用手順

（ア）　サービス機能の設定（情報の公開範囲等）に関する定期的な内容確認

（イ）　情報の滅失、破壊等に備えたバックアップの取得

（ウ）　利用者への定期的な注意喚起（禁止されている自治体機密性２以上の情報資産の取扱いの有無の確認等）

②　情報セキュリティインシデント発生時の連絡体制

４．２　外部サービスの利用における対策の実施

情報セキュリティ責任者は、利用しているサービスの約款その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で自治体機密性２以上の情報資産を取り扱わない場合の外部サービスの利用を申請すること。

５　外部サービスの利用手続

５．１　外部サービスの許可権限者

外部サービスを利用する場合は、統括情報セキュリティ責任者を外部サービスの許可権限者とする。

５．２　外部サービスの利用申請

（１）　情報セキュリティ責任者は、外部サービスを利用する場合には、統括情報セキュリティ責任者へ外部サービスの利用申請を行うこと。

（２）　統括情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

（３）　統括情報セキュリティ責任者は、外部サービスの利用申請を承認したときは、承認済外部サービスとして記録し、申請を行った情報セキュリティ責任者を外部サービス管理者に指名すること。

（４）　統括情報セキュリティ責任者は、次の内容を承認済外部サービス台帳に登録すること。

①　外部サービスの名称（必要に応じて機能名までを含む。）

②　外部サービス提供者の名称

③　利用目的（業務内容）

④　取り扱う情報の格付け（自治体機密性２以上等）

⑤　利用期間

⑥　利用申請者（所属・氏名）

⑦　利用者の範囲（本組合の関係者内に限る、部局内に限る等）

⑧　外部サービス管理者（所属・補職名）

（５）　外部サービスの利用を終了するときは、当該外部サービスを利用している情報セキュリティ責任者は、統括情報セキュリティ責任者に利用終了の報告をすること。

附　則

この基準は、令和８年４月１日から施行する。