広島県水道広域連合企業団
クラウドサービス利用基準

令和８年４月

広島県水道広域連合企業団

広島県水道広域連合企業団 クラウドサービス利用基準

第１ 目的

広島県水道広域連合企業団クラウドサービス利用基準（以下「本基準」という。）は、広島県水道広域連合企業団（以下「水道企業団」という。）が業務においてクラウドサービスを利用する際の判断基準及び遵守すべき事項を定めるものである。本基準は、サービス提供事業者及び業務委託先（以下「事業者」という。）が、水道企業団の情報資産を取扱うにあたり、情報セキュリティ及び業務継続性を確保するための基準を明確にし、適切な管理及び運用を実現することを目的とする。

本基準は、水道企業団が契約・調達・運用又は委託する全てのクラウドサービスに適用するものとする。なお、クラウドサービスにはSaaS、PaaS、IaaSその他同様の技術形態を含むものとする。

なお、本基準の適用範囲は、広島県水道広域連合企業団情報セキュリティポリシー（以下「セキュリティポリシー」という。）を超えるものではない。また本基準で使用する用語の意義は、セキュリティポリシーで使用する用語の例による。

第２ クラウドサービス利用の基本方針

１　水道企業団は、クラウドサービスの導入及び利用に当たっては「クラウド・バイ・デフォルト原則」に基づき、クラウド利用を第一の選択肢とするものとする。ただし、情報資産の重要性、法令上の制約又は技術的要件によりクラウド利用が不適切である場合はこの限りでない。

２　水道企業団及び事業者は、クラウドサービスの利用に際して、情報セキュリティ、個人情報保護、法令遵守、業務継続及び可用性の観点からリスクを評価し、必要な対策を講ずるものとする。

３　サービス提供事業者は、ISO/IEC 27001、ISO/IEC 27017又は27018 及びISMAP等の情報セキュリティに係る第三者認証を取得していることが望ましい。認証を取得していない場合は、同等以上のセキュリティ体制を有することを証明しなければならない。

第３ 情報資産の分類と管理

１　情報資産の分類

水道企業団における情報資産は、機密性を次のとおり分類し、必要に応じて取り扱い制限を行うものとする。

表１　機密性による情報資産の分類

区分	分類基準	対象の例
機密性３Ａ	「行政文書の管理に関するガイドライン」（平成23年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書。	・政策決定に関する重要文書など、極秘性の高い情報
機密性３Ｂ	漏えい等が生じた際に、個人の権	・住民の個人情報を格納するシステ

	利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産。	ムデータ ・マイナンバー等の特定個人情報 ・社会保障、福祉等の業務システム内の個人情報
機密性３Ｃ	機密性３Ｂ以上に相当する機密性は要しないが、基本的に公表を前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産。	・オンライン申請により一時的にインターネット上に保管されるデータ（申請処理の過程で一時的に保管されるデータ） ・文書管理システムの決裁文書として保存されている個人情報 ・施設設計情報や入札予定価格などの非公開情報
機密性２	行政事務で取扱う情報資産のうち、機密性３に相当する機密性は要しないが、直ちに一般に公開することを前提としていない情報資産。	・政策検討に関する情報（公表前の政策案・検討資料など） ・将来公表する予定の文書（白書案など） ・公表された情報以外の、直ちに一般公表されない業務資料や内部資料
機密性１	機密性２又は機密性３の情報資産以外の情報資産。	・ホームページ掲載記事 ・広報誌、パンフレット等

第４ クラウドサービス利用基準

水道企業団の情報資産を取扱うクラウドサービスは、当該情報資産の機密性及び取扱制限に応じて分類し、業務への影響度等を検討した上で、次の区分に従って利用を判断するものとする。

１　機密性２以上の情報を取扱う場合

クラウドサービスにおいて、機密性３Ｂ又は３Ｃの情報を取扱う場合は、本基準「第５ クラウドサービスの利用（機密性２以上の情報を取扱う場合）」を満たすクラウドサービスでなければならない。

機密性３Ａの情報については、クラウドサービスの利用は不可とする。

２　機密性２以上の情報を取扱わない場合

クラウドサービスにおいて、機密性２以上の情報を取扱わない場合は、本基準「第６ クラウドサービスの利用（機密性２以上の情報を取扱わない場合）」を満たすクラウドサービスでなければならない。

３　情報セキュリティポリシーの適用範囲外におけるクラウドサービスの利用

情報セキュリティポリシーの適用範囲外において、クラウドサービスを住民等に利用させる場合には、本基準に準じて適切なクラウドサービスを選定しなければならない。

第５ クラウドサービスの選定（機密性２以上の情報を取扱う場合）

サービス提供事業者は、クラウドサービス（民間事業者が提供するものに限らず、水道企業団が自ら提供するもの等を含む。以下同じ。）における情報の機密性、完全性及び可用性を確保するため、次の要件を満たさなければならない。

１　取扱う情報の格付に応じたサービス選定及びセキュリティ要件

ア　委託業務の遂行において利用するクラウドサービスは、原則として次の事項を満たすものでなければならない。

イ　受注者は、取扱う情報資産の可用性区分に応じて、利用するクラウドサービスが、次の事項に対応可能であることを提示すること。

(ｱ)　クラウド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及びデータ移行の可否

(ｲ)　クラウドサービスの中断時の復旧目標及び復旧手順

ウ　受注者は、情報セキュリティマネジメントシステム（ISMS）適合性評価制度の認証（ISO/IEC 27001）を取得していること。なお、取得していない場合は、これと同等の情報セキュリティ管理体制を整備していること。また、受注者は、取扱う情報資産の機密性区分及び取扱い制限を踏まえ、利用するクラウドサービスが、以下の内容を含む情報セキュリティ対策を実施していること。

(ｱ)　機密性２または３Ｃの情報を取扱う場合、ＩＳＭＳ（ISO/IEC 27001）を取得していることに加え、ＩＳＭＡＰクラウドサービスリスト若しくはＩＳＭＡＰ－ＬＩＵクラウドサービスリスト に登録されていること、又はサービス提供事業者（クラウドサービスプロバイダ）が、クラウドサービスにおける情報セキュリティ認証 （ISO/IEC 27017）を取得していること。

(ｲ)　機密性３Ｂの情報を取扱う場合、ＩＳＭＳ（ISO/IEC 27001）を取得していることに加え、ＩＳＭＡＰクラウドサービスリストに登録されていること、又はサービス提供事業者（クラウドサービスプロバイダ）が、クラウドサービスにおける情報セキュリティ認証（ISO/IEC 27017 及び ISO/IEC 27018）を取得していること。

(ｳ)　機密性３Ａの情報は、クラウドサービスで取り扱わないこと。

(ｴ)　クラウドサービスで機密性３Ｃ以上の情報を扱う場合は、機密性保護のため暗号化すること。また、サービス利用終了後には情報を消去すること。

(ｵ)　クラウドサービスの利用終了後等に、クラウドサービスで取り扱った情報を消去する場合には、利用者が暗号鍵を削除するなどの簡易的かつ確実な対応により、保存した情報を復元困難とする機能を有すること。また、受注者及びサービス提供事業者が削除を実施する場合は、その履行を証明する書面（データ消去証明書等）を提出できること。

(ｶ)　ＩＳＭＡＰクラウドサービスリスト等に未登録のサービスを利用する場合、ＩＳＭＡＰ認証の代替として、以下いずれかの方法によりＩＳＭＡＰ認証が求めるセキュリティ水準と同等以上であることを示すことで、水道企業団の承認を得ることができる。

a　サービス提供事業者が提示する、情報セキュリティ監査による報告書の確認。

b　サービス提供事業者が、水道企業団が指定する「別紙_クラウドサービス要件確認」に回答し、提出することによる ISMAP 認証管理基準への適合確認。

(ｷ)　「情報セキュリティ監査による報告書」は、独立した第三者機関により評価された監査報告書が代替となり得る。監査報告書の例として、米国公認会計士協会（AICPA）が定める、SOC2（Service Organization Control 2）Type2 レポート。もしくは、Cloud Security Alliance（CSA）が提供する STAR Level 2 認証等が挙げられる。

(ｸ)　クラウドサービスを提供する情報処理設備が収容されているデータセンターが設置されている独立した地域（リージョン）が原則として国内であること。

(ｹ)　ただし、データの保存性、災害対策等からバックアップ用のデータセンターが海外であることが望ましい場合、又は争訟リスク等を踏まえた上で海外にあることが特に問題ないと認められる場合はこの限りではない。

(ｺ)　法的措置が必要なトラブル対応等を考慮し、クラウドサービスの契約に定める準拠法が原則として国内法のみであること。

(ｻ)　国の行政機関が提供するシステム（ガバメントクラウド等）を利用する場合は、別途、水道企業団が指定する事項を遵守すること。

(ｼ)　不正アクセスを防止するためのアクセス制御を実施すること。

(ｽ)　管理権限（特権 ID 等）を用いて、クラウドサービスにアクセスする際は、多要素認証を用いて認証すること。

(ｾ)　クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（ＳＬＡ）において定めること。

(ｿ)　クラウドサービスに保存される情報の利用終了後の取り扱いを定めること。

(ﾀ)　クラウドサービスの利用を通じて水道企業団が取扱う情報のサービス提供事業者における目的外利用の禁止。

(ﾁ)　サービス提供事業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整備。

(ﾂ)　クラウドサービスの提供に当たり、サービス提供事業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、水道企業団の意図しない変更が加えられないための管理体制の整備。

(ﾃ)　サービス提供事業者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・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。

(ﾄ)　情報セキュリティインシデントへの対処方法を確立していること。

(ﾅ)　情報セキュリティ対策その他の契約の履行状況を確認できること。

(ニ)　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を確立していること。

(ヌ)　水道企業団内システムと外部のアプリケーションを連携する場合や、複数のクラウドサービスを連携して用いる場合、ＣＳＶやＡＰＩ連携等を使用する際のユーザアプリケーションやデバイスの範囲は最小限に限定し、ＣＳＶやＡＰＩ接続等の認証やログ管理など不正な操作を防止するために必要な保護やアクセス制御を実施すること。

(ネ)　生成 AI（文章、画像、プログラム等を生成できる AI モデル）又は生成 AI を利用したサービス（以下「生成 AI 等」という。）を利用する場合、入力した情報が AI 等の学習に利用されない設定が担保されていること。

(ノ)　機密性３Ａ（秘密文書相当）の情報は、生成 AI 等で取り扱わないこと。また、生成 AI 等を利用して作成した成果物については、その旨を明示する機能や運用が可能であること。

(ハ)　受注者は、クラウド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が適切に確保されるよう、情報の流通経路全般を見渡した形で、上記(ア)～(ノ)の事項について検討し、必要な措置を講じること。

表２　機密性区分と第三者認証の対応

機密性	クラウド利用可否	必須条件１（共通）	必須条件２（いずれか）
３Ａ	❌利用不可	---	---
３Ｂ	✅利用可能	ISMS（ISO/IEC 27001）取得	以下のいずれか： ・ISMAPクラウドサービスリスト登録 ・ISO/IEC 27017 & ISO/IEC 27018取得
３Ｃ又は２	✅利用可能	ISMS（ISO/IEC 27001）取得	以下のいずれか： ・ISMAPクラウドサービスリスト登録 ・ISMAP-LIUクラウドサービスリスト登録 ・ISO/IEC 27017取得

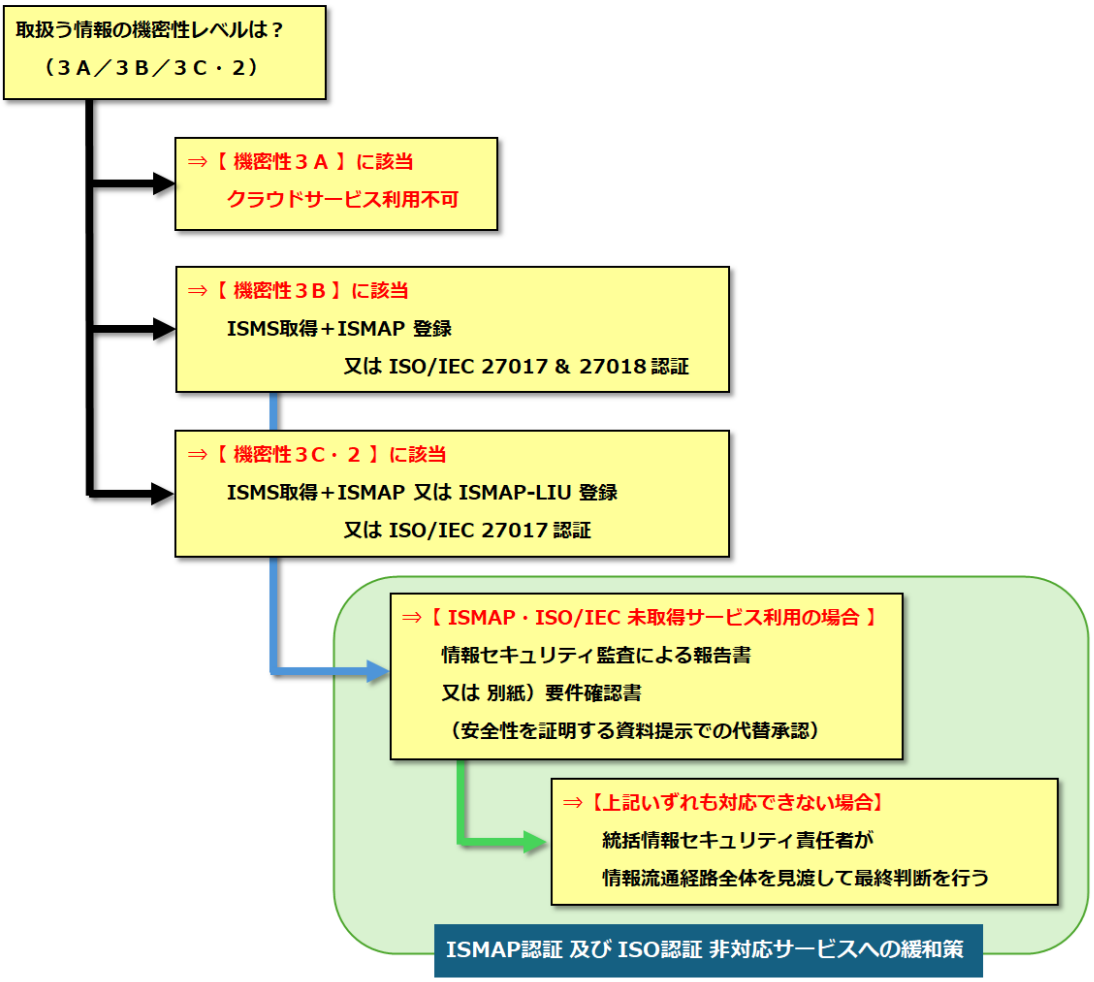

図１　情報資産の機密性による情報セキュリティ認証判定フロー

エ　受注者は、クラウド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を提示すること。

オ　受注者は、取扱う情報の格付等を勘案し、水道企業団が必要と認める場合は、以下の内容に対応すること。

(ｱ)　情報セキュリティ監査の受入れ

(ｲ)　サービスレベルの保証

カ　受注者は、利用するクラウドサービスにおいて、国内法以外の法令及び規制が適用されるリスクがある場合は、データが取り扱われる場所（国・地域）及び契約に定める準拠法・裁判管轄を提示すること。

キ　受注者は、サービス提供事業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水道企業団に提供し承認を受けること。

第６ クラウドサービスの選定（機密性２以上の情報を取扱わない場合）

受注者は、機密性２以上の情報を取扱わない業務においてクラウドサービスを利用する場合は、利用するサービスの約款、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選定すること。

第７ 委任

本基準は、社会情勢、法令改正及び技術動向の変化に応じて、必要に応じて改定を行うものとする。また、本基準に定めるもののほか、必要な事項は別に定める。

附　則

本基準は、令和８年４月１日から施行する。