別紙３

クラウドサービス利用判断基準

１　基本的な考え方

（１）目的

クラウドサービス利用判断基準（以下、「基準」とする）は、本市においてガバメントクラウドや LGWAN‐ASP などのサービスを利用する際に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

本基準の適用範囲は、堺市情報セキュリティ対策基準要綱の適用範囲とする。

（３）定義

対象とするクラウドサービス

ガバメントクラウド及びインターネットクラウドサービス、LGWAN‐ASP など事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの（以下、「外部サービス」という）。

２　機密性レベルに応じた基準

情報セキュリティ対策基準要綱に定める自治体機密性３B 及び３C（以下「重要情報資産」という）に該当する情報を対象サービスにおいて取り扱う場合に必要なセキュリティ要件や事業者選定要件を定める。

なお、自治体機密性３A の情報に関しては外部サービスを利用して取り扱うことを禁止する。

（１）重要情報資産を取り扱う場合

外部サービスにおいて重要情報資産を取り扱う場合は、本文書「３．１ サービスの選定条件」を満たすサービスを利用しなければならない。

（２）重要情報資産を取り扱わない場合

外部サービスにおいて重要情報資産を取り扱わない場合は、本文書に準じたサービスを利用しなければならない。庁内環境から外部サービスに持ち出したデータについて、インターネット環境にある端末へのダウンロードは禁止とする。データをダウンロードせざるを得ない場合は、別紙１「利用判断基準別表」②に示す要件に従い取り扱うデータの機密性等に応じた対策を講じること。

（３）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。そこで、適切なサービス提供者を選定することにより以下のようなリスクを低減すること。

（ア）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、サービス提供者の運用詳細は公開されないためサービス利用者にブラックボックスとなっている部分があり、サービス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の入手が困難である。

（イ）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。

（ウ）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。

（エ）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。

（オ）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

3．1サービス等の選定基準

情報システム管理者は、重要情報資産を取り扱う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及び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

（ア）別紙1「利用判断基準別表」に示す対策を講じること。必要に応じて、PIA（特定個人情報保護評価）を実施すること。

（イ）使用する外部サービスは以下のいずれかとする。

・LGWAN-ASP

・ISMAP 及び ISMAP-LIU クラウドサービスリストに掲載されているサービス

・ISMS（ISO/IEC27001、ISO/IEC27017、ISO/IEC27018）認証を受けているサービスについては、サービスの使用目的や使用用途に沿って情報セキュリティ対策が講じられていることを統括情報セキュリティ責任者に示し承認を得ること。

ただし、セキュリティ関連サービス（ウイルス定義ファイルや IP アドレス、URL ドメインリスト等の更新をインターネット経由で提供するサービス）については、更新情報の配信ツールであるため、以下の条件を前提に ISMAP クラウドサービスリスト等に登録されていないクラウドサービスについても、利用を認めるものとする。

・行政文書や行政文書に相当する情報を扱わないこと
・利用するクラウドサービスの接続先の URL を確認の上、当該接続先のみに接続を制限すること
・信頼できる機関が発行した証明書を用いた認証の実施により、サービス提供元の真正性が担保されていること（この対策だけではなく、上記の URL を用いた接続先制限も併せて実施すること）

（ウ）本市が示す以下の接続方法により接続すること。（参考資料「クラウドサービスの取扱いについて」を参照）

① ローカルブレイクアウト方式

接続する外部サービスの利用方法及び制御機能に応じて次のとおり対策を講じて接続すること。

〇認証・ウイルス定義体の取得のみの場合、下表１の A の〇に該当する対策を実施すること。

クラウドサービス利用の構成

（１）アプリケーションを利用するためのライセンスの認証・認可でクラウドサービスにアクセスする

（２）各団体専用領域（テナント）を保有しない

（３）Web 会議システム、メールなどのアプリケーションを利用しない

〇ファイルを庁内に取り込まない場合、下表１の B の〇に該当する対策を実施すること。

クラウドサービス利用の構成

（１）Web 会議システム、団体外の組織を自テナントの Web 会議に招待し、会議を行うが LGWAN 接続系にファイルのダウンロードは制限する

※ 外部団体のテナントにアクセスする場合(外部団体から招待された Web 会議に参加し、ファイル交換をする等）は、インターネット接続系の端末からアクセスする。

（２）団体外の組織とファイル管理システムを通じ、ファイルの共有を行うが、LGWAN 接続系にファイルのダウンロードは制限する

（３）メール、団体外の組織からのメール受信あり

〇外部とファイル送受信を行い内部に取り込む場合、下表１の C の〇に該当する対策を実施すること。

クラウドサービス利用の構成

（１）Web 会議システム、団体外の組織を自テナントの Web 会議に招待し、会議を行う

※ 外部団体のテナントにアクセスする場合(外部団体から招待された Web 会

議に参加し、（2）ファイル交換をする等）は、インターネット接続系の端末からアクセス

（3）団体外の組織と Web 会議システムを通じ、ファイルの共有を行う

（4）団体外の組織とファイル管理システムを通じ、ファイルの共有を行う

（5）メール、団体外の組織からのメール受信あり

表 1

A	B	C	セキュリティ対策	概要
	○		クラウドサービスからファイルダウンロード制限	クラウドサービス上から業務端末へのファイルダウンロードを制限する。
○	○	○	接続先のクラウドサービスの証明書による認証	接続先のクラウドサービスが本物であるか否か、正当性を確認する。
○	○	○	マルウェア対策ソフト	パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN 接続系に配置する端末、業務サーバで対応すること。
○	○	○	パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消す LGWAN 接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線 AP で対応すること。
○	○	○	接続先制限	LGWAN 接続系から外部へのアクセス先を LGWAN-ASP 及び利用が許可されたクラウドサービスのみに限定する。
	○	○	ローカルブレイクアウトテナントアクセス制御	利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限する。
	○	○	メール無害化/ファイル無害化	ファイルからテキストのみを抽出、ファイルを画像 PDF に変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN 接続系にインターネットからファイルを取り込むこと。なお、本対策におけるファイル無害化とは、インターネットメールに添付されたファイルの無害化を指す。
○	○	○	権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する。LGWAN 接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、LGWAN 接続系のスイッチ・無線 AP で対応すること。
	○	○	アクセス制御	不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認証・認可に基づき、アクセスの許可または拒否を行う。LGWAN 接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線 AP で対応すること。
	○	○	IDS/IPS	ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。
○	○	○	DDoS 対策	サービス不能攻撃の一つである DDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS 対策機器の導入や DDoS 対策サービスの利用によって、高負荷攻撃への耐性を向上させる。負荷分散装置（ロードバランサ）による耐性向上を含む。
○	○	○	通信路暗号化	通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとすること。

② インターネットパソコン方式

インターネット環境にある端末からクラウドサービスを使用して、重要情報資産を取り扱うことは、原則禁止とする。ただし、次のいずれかに該当する場合は、別紙 1 に示す安全管理措置を講じることに合わせて、想定し得るセキュリティリスクについて対応していることを証明し、統括情報セキュリティ責任者の承認を得ること。なお、これまでに堺市個人情報保護審議会の承認を得て導入しており、引き続き利用するものについては、リプレイス時に実施方法を見直すこと。

〇業務に必要な機能がインターネットクラウドのみで提供されていること。

〇外部事業者との情報共有、ファイル共有方法として実現方法が限られること。

③ LGWAN‐ASP 利用方式

④ ガバメントクラウド方式

（2）サービス及びサービス提供者の選定基準

（ア）基本方針

① 事業者は外部サービスに関する情報セキュリティについての基本的な方針を定めた文書（情報セキュリティポリシー等）を作成すること。

② 外部サービスは本市の情報セキュリティポリシーに従った利用が可能であること。

③ 外部サービスに関する情報セキュリティ対策についての具体的な対策を定めた資料を作成し、本市に提供すること。

（イ）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

情報システム管理者は、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：ISO/IEC 27017 によるクラウドサービス分野における ISMS 認証の国際規格、また、ISMAP の管理基準を満たすことの確認や ISMAP クラウドサービスリスト等）から、外部サービス及び当該サービスの委託先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。

① 情報セキュリティに関するルールの遵守について定期的に監査を受け、その監査人が発行する監査結果を本市に報告すること。または、外部機関による情報セキュリティ監査の結果を報告し、本市の承認を得ること。

（ウ）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

情報システム管理者は、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など）を十分に検討し、調達の際に、検討した結果を調達仕様書に具体的に盛り込まなければならない。また、必

要となる条項（インシデントの報告義務、損害賠償等）を盛り込んだ契約を締結するほか、必要に応じてサービスレベルを保証させるための SLA や SLO についても検討する。特に、バックアップについては、契約において、各業務システムの重要度を勘案した適切なバックアップレベルを設定し、別途のバックアップの取得など、レベルに応じた適切な対策を実施することが重要である。

① 業務実施方法、サービスの提供に関する重大な変更が生じる場合は予め本市に報告し、同意を得ること。

② サービス品質保証 （SLA：Service Level Agreement）を定め、本市の合意を得ること。

（エ）情報が取り扱われる場所等

情報システム管理者は、外部サービスの利用を通じて本市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を評価して外部サービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。

（例：データセンターは日本国内とする。日本国内の裁判所（必要に応じて地方公共団体の所在地を管轄する裁判所）を合意管轄裁判所として規定する。）

① 情報資産は、日本国の法律が及ぶ範囲に設置すること。

（オ）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

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を示すこと。

① 外部サービスの開発及び運用において、本市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。

② 外部サービスに本市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、本市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。

③ 利用者が快適に利用するために必要なリソースの容量・能力を確保すること。利用において必要な監視機能を確認するとともに、監視により業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めること。

（カ）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）について明確に示すこと。

① 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市へ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こと。
② 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示すこと。
③ 外部サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）ができること。稼働停止を検知した場合は、本市に速報できること。
④ 外部サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）ができること。障害を検知した場合は、本市に速報できること。
⑤ 外部サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器等の稼働停止、障害、パフォーマンス低下等について、本市に詳細を報告すること。
⑥ 情報セキュリティインシデントを検知した場合、検知した内容、被害状況、対応予定等、本市が必要とする情報を、本市に速報すること。
⑦ 検知した情報セキュリティインシデントを速やかに調査し、調査結果の詳細を本市に報告すること。

（キ）その他要件
① 外部サービス提供者による情報の管理・保管
・外部サービス提供者による情報の管理・保管方法について事前に把握すること。
・外部サービス提供者が情報の管理・保管を他の事業者へ委託する場合、当該事業者における情報セキュリティ水準や情報の取扱方法に関して外部サービス提供者に確認の上、合意しておくこと。
② 情報開示請求に対する開示項目や範囲
・事前に自組織と外部サービス提供者が協議の上、外部サービス提供者が提供する内容の項目や範囲を契約において明記すること。
・対象情報の機密性が高い場合、両者間で秘密保持契約（NDA：Non-Disclosure Agreement）を締結するなど必要な措置を講じた上で取得すること。

３．２ 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
外部サービス利用の終了に関する内容について、以下のとおり確認すること。
① 外部サービスの利用を終了する際に、本市が求める他の外部サービス等への情報資産の移行方法を示し対応可能であること。例）CSV 等でデータを出力すること
② 外部サービス利用終了時は、作成したアカウントやサービスで取り扱った情報について複製を含む全ての情報資産の再利用が不可能な方法での削除及びその証明書の提出をすること。※外部サービスの利用を終了する場合は必ず記載すること。
③ 利用する情報資産（機器等）を交換または処分（廃棄）する場合の取り扱いが、本市

情報資産の漏えいが発生しない方法であることを予め本市に示すこと。

３．３ 外部サービスの利用に係る調達・契約

（１）情報システム管理者は、外部サービスを調達する場合は、サービス及びサービス提供者の選定基準を調達仕様に含めること。
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）情報システム管理者は、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締結までに確認すること。

別紙１

以下に示す①外部サービス共通の対策を講じてください。またインターネット環境からサービスを使用する場合は②インターネットパソコン方式の対策も講じてください。

①外部サービス共通

No.	区分	要件概要
1	技術的セキュリティ	外部サービスの停止により市民サービスに多大な影響を与える場合は、外部サービスを安定して利用するために必要な冗長化対策を講じること。
2	技術的セキュリティ	利用する時刻の同期が確実に行われるための対策を講じること。
3	技術的セキュリティ	外部サービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的脆弱性に関する情報（OS、その他ミドルウェア等を含めたソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。
4	技術的セキュリティ	アクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。 認証方法…ID/PWの設定、生体認証及び多要素認証【推奨】、特定の拠点…IPアドレスの制限、クライアント証明書【推奨】
5	技術的セキュリティ	パスワードを認証要素とする場合は、パスワードの桁数、文字種等、複雑性をシステム側で制御できること。
6	技術的セキュリティ	情報資産へのアクセス履歴、機器への操作履歴、サービスの利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）などを取得し、【本市が求める期間（１年以上を記載）】保存すること。履歴を改ざんされないような対策を講じること。
7	技術的セキュリティ	本市の監査及びデジタルフォレンジックに必要となる外部サービス事業者の環境内で生成されるログ等の情報（デジタル証拠）をインシデントが起こった際などに本市の求めに応じて速やかに提供すること。
8	技術的セキュリティ	不正プログラムへの対策を確実に実施すること。（複数の外部サービスを組み合わせて構成する場合において、他の外部サービスが不正プログラムへの対策を実施している場合を除く。ただし、その場合は他の外部サービスが実施する対策に協力すること。）
9	技術的セキュリティ	外部ネットワーク及び内部ネットワークからの不正アクセスを防止する措置を講じること。 例）ファイアウォール又はリバースプロキシの導入
10	技術的セキュリティ	本市の指定するバックアップの頻度、バックアップデータの保存期間、バックアップデータからのリカバリー方法を実施すること。 バックアップの頻度や保存期間について本市の指定する範囲と異なる変更を行う場合はあらかじめ本市の承諾を得ること。
11	技術的セキュリティ	庁内環境から外部に持ち出したデータについて、インターネット環境にある端末等へのダウンロードを禁止すること。 ただし、やむを得ずダウンロードする際は②の端末要件を満たすこと。なお、指定管理者や委託事業者がデータをダウンロードする必要がある場合は、②の端末要件を満たした上で、持ち出すデータの内容を限定し、事前に情報システム管理者の承認を得ること。
12	技術的セキュリティ	特定個人番号を含むデータについて本市と外部サービス環境を接続する際、LGWAN回線またはガバメントクラウド専用線を使用すること。
13	技術的セキュリティ	特定個人番号を含むデータについては、インターネット環境にある端末等へのダウンロードを制限すること。

②インターネットパソコン方式(原則禁止)
（インターネット環境にあるパソコンについて以下のセキュリティ対策を講じること。ただし、インターネット仮想パソコンを使用する場合を除く。）

No.	区分	要件概要
1	技術的セキュリティ	外部サービスや内部システムに接続する専用端末（以下、専用端末とする）として、電子メール機能など外部に情報を送付する機能を原則禁止する。 外部記録媒体を使用したデータ持ち出しは厳格に制限する。
2	技術的セキュリティ	許可された専用端末のみ外部サービスに接続できる。
3	技術的セキュリティ	専用端末にログインできる職員を管理する。
4	技術的セキュリティ	ログイン時に使用するパスワードは初期設定のまま使用せず、また安易に推測可能なものを使用しない。
5	技術的セキュリティ	専用端末は有線ケーブルを用いて接続を行い、事務室外への持ち出しを禁止する。
6	技術的セキュリティ	不要なソフトウェアのインストールを禁止する。
7	技術的セキュリティ	専用端末に資産管理ソフトを導入して、操作ログの取得及び保存をする。
8	技術的セキュリティ	専用端末のOS等のアップデートやネットワーク機器のソフトウェア等に脆弱性を残さないように、更新ファイルやパッチ等を適用する。
9	技術的セキュリティ	専用端末の不正プログラム対策として、ウイルス対策ソフトの更新や定期スキャン等を行う。
10	技術的セキュリティ	専用端末に業務と無関係もしくは不要なデータのダウンロードを禁止する。（人的セキュリティ対策を含む）
11	技術的セキュリティ	専用端末に無操作時の画面ロック及びスクリーンセーバー機能を設定する。
12	技術的セキュリティ	専用端末を一定時間操作しない場合、自動的にログオフする。（人的セキュリティ対策を含む）
13	技術的セキュリティ	ハードディスクの暗号化機能を有する端末を許可端末とする。
14	技術的セキュリティ	（複数台でネットワークを組む際は）ファイアウォールを設置するなど外部からのアクセスを制限するほか、ネットワークの通信ログを取得及び保存する。
15	技術的セキュリティ	専用端末内に格納するデータをは必要最小限とし不必要なデータは定期的に消去する。（人的セキュリティ対策を含む） データの格納はできる限り庁内LAN環境において行うなどインターネット環境で保存しないこと。
16	技術的セキュリティ	暗号化通信（SSL通信）を使用した接続とする。
17	技術的セキュリティ	インターネット端末内にバックアップデータを残さないこと。外部サービス等でバックアップを取得、保存すること。
18	技術的セキュリティ	専用端末からやむを得ずデータを持ち出しを行う場合には、事前に承認を得てその記録を残すこと。（人的セキュリティ対策を含む）
19	技術的セキュリティ	専用端末及び外部記録媒体を廃棄する時は物理的に破壊するなど内部データを再度読み込みができない状態で廃棄する。
20	技術的セキュリティ	データを記録した外部記録媒体は使用後に初期化する。（人的セキュリティ対策を含む）
21	技術的セキュリティ	外部記録媒体（USBメモリ等）の所在や使用状況の管理、使用の制限を実施する。（人的セキュリティ対策を含む）
22	技術的セキュリティ	暗号化機能及びウイルス対策機能を有する外部記録媒体を使用する。