

別紙3 セキュリティ要件

No	大区分	小区分	内容
1	外部サービス提供者の選定基準		日本の法令の範囲内で運用できるサービスであること。また、日本国内の裁判所を合意管轄裁判所とすること。
2	外部サービス提供者の選定基準		個人情報や住民の生命・財産に関わる情報、その他、非公開情報のデータが保存されるデータセンターは日本国内にあること。
3	外部サービス提供者の選定基準		利用する外部サービスのリージョンを日本国内に限定すること。
4	外部サービス提供者の選定基準		業務の重要度に応じたSLA(稼働率、目標復旧時間、目標復旧ポイント、バックアップの頻度・範囲・世代・保管方法等)、インシデント報告義務及び情報セキュリティ対策の履行が不十分な場合の対処(追完、損害賠償等)等、必要となる条項を盛り込んだ契約が締結可能なこと。
5	外部サービス提供者の選定基準		外部サービスの終了又は変更時における事前の通知について以下を例とする取り決めが可能なこと。当該外部サービスの終了又は変更の際に1ヶ月前までにメール・文章等所定の方法で事前に告知すること。
6	外部サービス提供者の選定基準		外部サービスの中断や終了時等に円滑に業務を移行することが可能なこと。その際は、移行方法が提示され、標準化されたデータ形式やインターフェースが使用可能であること。
7	外部サービス提供者の選定基準		外部サービス提供者による情報資産の利用は、外部サービスの提供に必要な範囲で認めるものであり、それ以外の目的で本市の情報資産の利用は認めない。
8	外部サービス提供者の選定基準		外部サービス提供者における情報セキュリティ対策が確実に実施されること。公開資料や監査報告書(又は内部監査報告書・事業者の報告資料)等から上記内容(セキュリティ対策の実施内容・管理体制)を示すことが可能なこと。
9	外部サービス提供者の選定基準		外部サービスの開発及び運用が本市の意図しない変更が行われない一貫した品質保証体制の下でなされていること。意図しない変更とは非公開設定が説明なく、公開設定になることや本市が保存するデータが意図せず書き換えられることを想定しており、機能追加等はこれに含まれない。
10	外部サービス提供者の選定基準		<p>情報セキュリティインシデントの対処について以下を例とする内容を調達仕様を含められること。</p> <p>情報セキュリティインシデントが発生した際に、外部サービス提供者と連絡がつかない、営業時間外の対応が不可能等の状況にならないこと。また、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に情報セキュリティインシデント発生時に以下の対応を行うこと。</p> <p>①外部サービス提供者が情報セキュリティインシデントを検知した際は、速やかに本市に報告を行うこと。</p> <p>②情報セキュリティインシデントが発生した際に、運用状況・影響範囲調査等、事案解決のために積極的に調査を行うこと。</p> <p>③情報セキュリティインシデント発生後、可及的速やかに調査・報告を実施すること。なお、情報セキュリティインシデントの疑いに対する連絡を受けた場合も同様に調査に着手すること。</p> <p>④当該事案の原因特定のため、各種システムログを取得すること。また、取得したログの分析に必要な情報を提供すること。</p> <p>⑤調査の結果、サービス停止等の措置が必要な場合は、市担当者に報告した上で速やかにその対応を行い、インシデント収束後、速やかに復旧を行うこと。</p> <p>⑥調査の結果、ファームウェア・ソフトウェア等のバージョンアップ等が必要となった場合は、速やかに対応すること。</p>
11	外部サービス提供者の選定基準		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契約の履行状況の確認方法を盛り込んだ契約が締結可能なこと。
12	外部サービス提供者の選定基準		外部サービス提供者により、利用規約、各種設定の変更について、以下を例とする取り決めが可能なこと。当該サービスの利用規約については、1ヶ月前までに、各種設定の変更については7日前までにメール・文章等所定の方法で事前に告知すること。
13	外部サービス提供者の選定基準		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ていること。
14	外部サービス提供者の選定基準		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次をはじめとした情報を本市に提供可能であること。 <ul style="list-style-type: none"> ・再委託先事業者情報 ・再委託内容 ・再委託先の情報セキュリティ責任者 ・再委託先の個人情報管理者 ・再委託先の従事者の情報 <p style="text-align: right;">等</p>

No	大区分	小区分	内容
15	外部サービス提供者の選定基準		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から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し、判断可能なこと。認定・認証制度の例は以下のとおり。 ① ISO/IEC 27017 ② ISMAP管理基準を満たすこと ③ ISMAPクラウドサービスリスト ④ SOC報告書
16	導入・構築時の対策	アクセス制御に関する事項	業務の特性及び取り扱う情報に応じて以下を例とする接続制御が可能なこと。 ●インターネット接続系業務 ・インターネット接続可(接続可能な端末の限定) ・インターネット接続可
17	導入・構築時の対策	アクセス制御に関する事項	不正なアクセスを防止するためのアイデンティティ管理(アカウントの発行や削除等のメンテナンス)とアクセス制御(外部サービスに保存される情報や外部サービスの機能ごとにアクセスする権限のない職員がアクセスできないように制限)を実施すること。
18	導入・構築時の対策	アクセス制御に関する事項	システム管理者等の特権アカウントが外部サービスに接続する際は、強化された認証技術(多要素認証等)を用いること。
19	導入・構築時の対策	アクセス制御に関する事項	外部サービスに影響を与える操作(サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除・外部サービス利用の終了手順・バックアップ及び復旧等)について、誤操作を抑制するための手順書の作成や誤操作を認識可能なアラート等を実装する等の対策を行うこと。
20	導入・構築時の対策	アクセス制御に関する事項	外部サービス上で構成される仮想マシンに対して適切なセキュリティ対策(必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策、ログ取得等の実施)を行うこと。 SaaSを利用する場合は、これらの対応が、外部サービス提供事業者側でされていること。
21	導入・構築時の対策	アクセス制御に関する事項	庁内通信回線を経由せずに外部サービスを利用する場合は、多要素主体認証方式やデバイス認証による接続端末制限等の対策を行うこと。(リモートから外部サービスにインターネットで直接接続するようなケースが有る場合のみ該当)
22	導入・構築時の対策	暗号化に関する事項	取り扱う情報の機密性に応じた保護のための適切な暗号アルゴリズム(CRYPTRECにより安全性及び実装性能が確認された「電子政府推奨暗号リスト」)を用いた暗号化処理(情報が保存されている場合、情報が通信され転送されている場合等フローに応じた暗号化)を行うこと。
23	導入・構築時の対策	設計・設定及び開発に関する事項	外部サービスログについて以下を例とする取り決めが可能なこと。 外部サービスに係るログ等の証跡の保存、取得及び提供が可能であり、ログは1ヶ月間以上保存すること。また、改ざん防止等のログ等に関する保護が実施されていること。
24	導入・構築時の対策	設計・設定及び開発に関する事項	当該外部サービスの標準的な監視機能で取得できない監査及びデジタルフォレンジックに必要な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)について、市の求めにより提供可能であること。
25	導入・構築時の対策	設計・設定及び開発に関する事項	外部サービス内において確実に時刻同期を行い、取得するログの時刻、タイムゾーンを統一すること。
26	導入・構築時の対策	設計・設定及び開発に関する事項	設計・設定時の誤りの防止の対応として、以下を例とする対策を行うこと。 ・外部サービス提供者による設定の実施 ・外部サービス提供者からの推奨される設定情報の入手 ・外部サービス提供者による設定内容のレビュー ・外部サービス提供者が提供するセキュリティ設定・監視ツールの利用 ・設定権限を与える外部サービス利用者の限定
27	導入・構築時の対策	設計・設定及び開発に関する事項	セキュリティを保つための開発手順やフレームワーク等の情報が活用されていること。
28	導入・構築時の対策	設計・設定及び開発に関する事項	外部サービス上に構成された情報システムと他の外部サービス利用者のネットワークやサブネット間等の異なるネットワーク間の通信(トラフィック)を監視すること。 (SaaSの場合は対象外)
29	導入・構築時の対策	設計・設定及び開発に関する事項	業務継続を考慮し、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(移植容易性)について、必要に応じて外部サービス提供者に報告を求めることが可能であること。
30	導入・構築時の対策	設計・設定及び開発に関する事項	冗長構成や冗長回線等の実装により可用性を十分に考慮した設計となっていること。
31	導入・構築時の対策	設計・設定及び開発に関する事項	パスワードの管理機能について以下の機能を備えている。 ・長さ10文字以上の制限 ・英大文字、英小文字、記号及び数字を含める制限 ・過去に使用したパスワードを利用できないように制御 ・パスワードをハッシュ化した状態で保存する機能

No	大区分	小区分	内容
32	導入・構築時の対策	設計・設定及び開発に関する事項	一定回数続けてログインに失敗した場合に、ログイン不能にするアカウントロック機能を有していること。
33	運用・保守時の対策	アクセス制御に関する事項	パスワードなどの認証情報の割り当てが外部サービス提供者側で実施される場合、以下を例とする管理手順が実施されること。 ・パスワードは、他者に知られないように管理しなければならない。 ・パスワードを秘密にし、パスワードの照会等には一切応じてはならない。 ・パスワードは十分な長さとし、文字列は想像しにくいもの(アルファベットの大小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)にしなければならない。 ・パスワードが流出したおそれがある場合には、速やかに報告し、パスワードを変更しなければならない。 ・サーバ、ネットワーク機器、パソコン及びモバイル端末等にパスワードを記憶させてはならない。
34	運用・保守時の対策	資産管理に関する事項	当該外部サービスに関連する脆弱性情報の提供を行うこと。また、外部サービス提供者の責任範囲で発生した脆弱性対応が迅速に行われること。
35	運用・保守時の対策	アクセス制御に関する事項	管理者権限を割り当てる場合のアクセス管理と操作に関するログの取得が行われること。また、管理者権限を持つ者の操作等について、すべて記録し、保存できること。
36	運用・保守時の対策	アクセス制御に関する事項	外部サービスのリソース(ネットワーク、仮想マシン等)の設定を変更するユーティリティプログラムが存在する場合、利用者を制限できること。
37	運用・保守時の対策	アクセス制御に関する事項	外部サービスの不正な利用を監視可能であること。 (例:業務時間外の利用等を外部サービスに対するアクセスログで確認)
38	運用・保守時の対策	暗号化に関する事項	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、鍵の生成から廃棄に至るまでのライフサイクルにおける仕組みにリスク(鍵が窃取される可能性や鍵生成アルゴリズムの危殆化の可能性等)がないこと。
39	運用・保守時の対策	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利用者のネットワークや通信と分離されていること及び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。 SaaSの場合は、他の利用者が市のデータにアクセスできないよう確実な制御を行っていること。
40	運用・保守時の対策	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、以下を例とする設定の誤りを防止するための対策を行うこと。 ・外部サービス提供者による設定の実施 ・外部サービス提供者からの推奨される設定情報の入手 ・外部サービス提供者による設定内容のレビュー ・外部サービス提供者が提供するセキュリティ設定・監視ツールの利用 ・設定権限を与える外部サービス利用者の限定 ・追加機能に対する初期設定や追加機能により影響を受ける設定の確認
41	運用・保守時の対策	事業継続に関する事項	バックアップ頻度、範囲、実施手順、復旧手順等、外部サービスが業務に必要な可用性を満たしたものになっていること。また、復旧に係る手順の策定と定期的な訓練を実施すること。
42	運用・保守時の対策	事業継続に関する事項	利用する外部サービスで使用済みのデータ容量やサービスの性能について監視を行い、想定された容量・性能内で運用していることを確認できること。
43	更改・廃棄時の対策	外部サービスで取り扱った情報の廃棄に関する事項	外部サービスの利用終了時に、外部サービスで取り扱った業務に関わる全ての情報が、外部サービス基盤上から確実に削除可能であること。なお、削除する対象はバックアップ等により複製されたものにも及ぶ点に注意すること。 削除にあたっては、情報資産を暗号化した鍵(暗号鍵)を削除するなどにより、復元困難な状態としなければならない。
44	更改・廃棄時の対策	外部サービスで取り扱った情報の廃棄に関する事項	外部サービスの基盤となる装置等の処分についてセキュリティを確保した対応が行われること。
45	更改・廃棄時の対策	外部サービスで取り扱った情報の廃棄に関する事項	外部サービスの基盤の処分の確認にあたり、外部サービス提供者が利用者に提供可能な第三者による監査報告書や認証等を取得していること。
46	更改・廃棄時の対策	外部サービスで取り扱った情報の廃棄に関する事項	外部サービスの利用終了時に、情報の廃棄の実施報告書を提出すること。
47	更改・廃棄時の対策	外部サービスで取り扱った情報の廃棄に関する事項	外部サービス利用者の各アカウント以外に特殊なアカウント(ストレージアカウントなど)がある場合は、関連情報(資格情報等)含めて廃棄可能であること。