クラウドサービスの利用において必要となるセキュリティ要件

1.1　クラウドサービスを利用した情報システムの導入・構築時のセキュリティ対策に関する事項

＜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ィンティティ管理（ID のプロビジョニングから廃棄まで）とアクセス制御を実装する。
- システム管理者等の特権アカウントがクラウド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）を用いる。
- クラウドサービスに影響を与える操作の特定と誤操作を抑制するために、手順書の作成や誤操作を認識可能なアラート等の実装を考慮する。
- クラウド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を行う。
- 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を行う。（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）

＜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。

＜設計・設定及び開発に関する事項＞

- クラウド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を検討し、その検討結果を踏まえ、設計・開発におけるセキュリティ対策を行う。また、クラウドサービスで取得可能なログの種類、範囲等を確認し、必要となるログの取得機能を実装する。
- クラウドサービス内における時刻同期の方法について確認し、取得するログの時刻、タイムゾーンを統一する。
- 設計・設定時の誤りの防止の対応として、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などを行う。
- 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を活用する。

- クラウドサービス上に他ベンダーが提供するソフトウェア等を導入する場合は、そのソフトウェアのクラウドサービス上におけるライセンス規定を確認する。
- クラウドサービス上に構成された情報システムと他のクラウド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。
- 利用するクラウド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、必要に応じてクラウドサービス提供者に報告を求め、業務が継続できるよう考慮する。
- クラウドサービスを利用する業務において必要となる可用性（冗長構成や冗長回線等の実装）を考慮した設計になっているか確認を行う。

＜その他＞

- 日本の裁判管轄、法令が適用されること。海外への機密情報の流出リスクを考慮し、クラウドサービスを提供するリージョン（国・地域）を国内に指定すること。国内のクラウドサービスにおいて、利用者のデータが、海外に保存されないか確認を行う。
- クラウドサービス提供者が、利用者の情報資産へ目的外のアクセスや利用を行わないように定められているか確認を行う。
- 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について、規定されているか確認を行う。

1.2　クラウドサービスを利用した情報システムの運用・保守時のセキュリティ対策に関する事項

＜運用・保守時における利用方針に関する事項＞

- クラウドサービス提供者と責任分界点について確認し、リスクの受容可否を判断する。
- 利用承認を受けていないクラウドサービスは利用しない。
- クラウドサービス提供者に対して定期的にサービスのサービスレベルを確認する。
- 利用するクラウド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クラウドサービス提供者との責任分担や連絡体制を明確にする。

＜運用・保守時における教育に関する事項＞

- 利用するクラウドサービスの手順書（操作手引書）を定め、利用者に周知する。
- 利用するクラウドサービスにおけ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共有をはかる。

- 利用するクラウドサービスに関する適用法令や関連する規制等がある場合は、利用者に周知する。

＜運用・保守時における資産管理に関する事項＞

- クラウドサービス上で利用する IT 資産が脆弱性による影響を受ける場合に備え、利用者側の責任範囲を明確にしておく。
- クラウドサービス上に情報を保存する場合は、個人情報の有無、機微性の高低等の情報に対する格付・取扱制限等が把握できるようにする。

＜運用・保守時におけるアクセス制御に関する事項＞

- システム管理者特権を割り当てる場合のアクセス管理（4.5 アクセス制御参照）と操作に関するログを取得する。
- クラウドサービスの各利用者に割り当てたアクセス権限に対して、定期的な見直し（異動時、退職時等の確認）を行う。
- クラウド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は、その機能の確認と利用できる者を制限する。
- 利用するクラウドサービスの不正な利用を監視（例：業務時間外の利用等をクラウドサービスに対するアクセスログで確認）する。

＜運用・保守時における暗号化に関する事項＞

- クラウドサービスに情報資産（データ）を保存する場合、暗号化の仕組みや暗号化に使用する鍵の管理方法について確認をする。
- 鍵管理機能をクラウドサービス提供者が提供するものを利用する場合、リスクがないか確認する。
- 鍵管理機能をクラウド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関する内容を確認し、リスクがないか確認する。

＜運用・保守時におけるクラウドサービス内の通信に関する事項＞

- 利用するクラウド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をクラウドサービス提供者の開示している情報等で確認する。

＜運用・保守時における設計・設定に関する事項＞

- クラウドサービスの設定を変更する場合、設定の誤りを防止するための対策（グローバルなセキュリティのガイドラインやフレームワークとの差異の確認等）を行う。
- 利用者が行う重要な操作に関する手順書を作成する。
- 利用するクラウド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クラウドサービス提供者の開示している情報等で確認する。

- クラウドサービス提供者により、利用規約、各種設定が変更された場合の変更内容の確認方法や連絡方法を定めることを確認する。

＜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を実施（クラウドサービス提供者が提供する機能を利用する場合は、その実施の確認）する。
- クラウドサービスが、業務に必要な可用性を満たしたものになっているか確認をする。また、復旧に係る手順の策定と定期的な訓練を実施する。
- クラウドサービス提供者からの設定やバージョン等の変更の確認方法と利用するクラウドサービス上のシステムに影響があった場合を想定し、復旧手順について確認する。
- クラウドサービスで利用しているデータの容量、性能等を監視し、クラウドサービスまたは、クラウドサービス上のシステムへの影響について把握する。

＜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、クラウド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、クラウドサービス管理者へ報告を行う。
- クラウドサービス管理者が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。

1.3　クラウドサービスを利用した情報システムの更改・廃棄時のセキュリティ対策に関する事項

＜クラウドサービスの利用終了時における対策に関する事項＞

- クラウドサービスの利用を終了する場合は、移行計画書又は終了計画書を作成する。
- クラウドサービスの利用終了による業務影響が無いように、利用者に対して利用終了の予定時期を事前に知らせる。

＜クラウドサービスで取り扱った情報の廃棄に関する事項＞

- 取り扱う情報の機密性に応じて、廃棄方法を決定する。

＜クラウド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＞

- 作成したクラウドサービス利用者の各アカウントを削除する。
- 利用したシステム管理者特権アカウントを削除（又は返却）する。
- クラウド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がある場合は、関連情報（資格情報等）含めて廃棄する。