鎌倉市外部サービス利用基準

令和6年（2024 年）5月 23 日作成

目次

内容

１　目的 ..... - 3 -

２　対象者 ..... - 3 -

３ 用語の定義 ..... - 3 -

４　 外部サービス利用判断基準 ..... - 5 -

５　 外部サービス選定基準 ..... - 7 -

６ 外部サービスの利用手続き ..... - 7 -

1　目的

本書は、鎌倉市情報セキュリティ対策基準8．2（1）及び8．3（1）で定める、外部サービスの利用の際の判断の基準や手続き、利用にあたっての必要なセキュリティ対策等を規定するものである。

本書で定める内容以外のセキュリティ対策等については、鎌倉市情報セキュリティポリシーに定める。

2　対象者

本基準の適用範囲は、鎌倉市情報セキュリティポリシーで定める適用範囲に準じる。

3　用語説明

（1） 外部サービス：クラウドサービスプラットフォーム上に、ソフトウェア等を搭載し、インターネットや、LGWAN 経由で提供される情報システムの機能やサービス。本基準内では、オンライン会議システム及び SNS は含まない。

（2） ISO/IEC 27001：情報セキュリティマネジメントシステム（ISMS）に関する国際規格。情報の機密性・完全性・可用性の 3 つをバランスよくマネジメントし、情報を有効活用するための組織の枠組みを示す。

（3） ISO/IEC 27017：クラウドサービスに関する情報セキュリティ管理策のガイドライン規格。情報セキュリティ全般に関するマネジメントシステム規格である ISO/IEC 27001 の取り組みを ISO/IEC 27017 で強化することで、クラウドサービスにも対応した情報セキュリティ管理体制を構築することができる。

（4） ISMAP：政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録し、各政府機関は原則、安全性が評価され「登録簿」に掲載されたサービスから調達をおこなうことで、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度。

（5） LGWAN-ASP:民間企業等が ASP（アプリケーションサービスプロバイダ）として、LGWAN を通じて、サービス利用者である地方公共団体に各種行政事務サービスを提供するもの。

その他の用語については、鎌倉市情報セキュリティポリシーに準じる。

【参考】

機密性による情報資産の分類

分類	分類基準
機密性3	行政事務で取り扱う情報資産のうち、鎌倉市情報公開条例第6条の各号に相当する機密性を要する情報資産
機密性2	行政事務で取り扱う情報資産のうち、鎌倉市情報

	公開条例第6条の各号に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産
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

役割名称とその役割

名称	役割
最高情報セキュリティ責任者 (CISO:ChiefInformation Security Officer)	**ア** 情報セキュリティの確保についての事項を所管する副市長を CISO とする。CISO は、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。 **イ** CISO は、情報セキュリティインシデントに対処するための体制(CSIRT:Computer Security Incident Response Team、以下「CSIRT」という。)を整備し、役割を明確化する。
統括情報セキュリティ責任者	**ア** 情報セキュリティの確保についての事項を所管する部長を CISO 直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISO を補佐しなければならない。 **イ** 統括情報セキュリティ責任者は、本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。 **ウ** 統括情報セキュリティ責任者は、本市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。 **エ** 統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報セキュリティ担当者、統括情報システム責任者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。 **オ** 統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。 **カ** 統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報セキュリティ担当者、統括情報システム責任者、情報システム管理者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。 **キ** 統括情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、回復のための対策を講じなければならない。 **ク** 統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課

	題及び問題点を含む運用状況を適時に把握し、必要に応じてCISO に
統括情報システム責任者	**ア** 情報セキュリティの確保についての事項を所管する課長を 統括情報システム責任者とする。統括情報システム責任者は、統括情報セキュリティ責任者を補佐しなければならない。 **イ** 統括情報システム責任者は、本市の共通的なネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。 **ウ** 統括情報システム責任者は、本市の共通的なネットワークにおける情報セキュリティ対策に関す る権限及び責任を有する。 **エ** 統括情報セキュリティ責任者は、本市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。
情報セキュリティ責任者	**ア** 内部の部の長、行政委員会事務局の長及び消防長を情報セキュリティ責任者とする。 **イ** 情報セキュリティ責任者は、当該部等の情報セキュリティ対策に関する統括的な権限及び責任を有する。 **ウ** 情報セキュリティ責任者は、その所管する部等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。 **エ** 情報セキュリティ責任者は、その所管する部等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員等に対する教育、訓練、助言及び指示を行う。
情報セキュリティ管理者	**ア** 内部の部の課長、内部の部の出張所等出先機関の長、行政委員会事務局の課長及び消防本部の課長を情報セキュリティ管理者とする。 **イ** 情報セキュリティ管理者は、その所管する課等の情報セキュリティ対策に関する権限及び責任を有する。 **ウ** 情報セキュリティ管理者は、その所掌する課室等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者、統括情報システム責任者、統括情報セキュリティ責任者及び CISO へ速やかに報告を行い、指示を仰がなければならない。

4　外部サービス利用判断基準

(1) 情報資産の取り扱いを許可する場所について

情報セキュリティ管理者は、外部サービスを利用する場合には、外部サービスの利用を通じて本市が

取り扱う情報資産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踏まえ、情報の取り扱いを許可する場所について、機密性による情報資産分類により、原則、次の条件を含めなければならない。

ア　機密性2以上の情報を取り扱う場合

日本国内にあるデータセンターかつ国内法の適用範囲であること。

イ　機密性1の情報のみを取り扱う場合

裁判管轄の問題等のリスクを踏まえ決定すること。

(2)　外部サービスの選定について

情報セキュリティ管理者は、外部サービスを選定する際は、次の条件を考慮し、選定を行わなければならない。

ア　機密性2以上の情報を取り扱う場合

ISMAP(政府情報システムのためのセキュリティ評価制度)の登録があるクラウドサービスであること、もしくは、LGWAN-ASP 上に構築された(扱うデータの保存が LGWAN-ASP 上にある)クラウドサービスであることが望ましい。

この他の場合には、ISO 認証(27001、27017)や日本セキュリティ監査協会のクラウド情報セキュリティ監査制度等の各種認証制度への適合条件を参考に当該サービスの信頼性が十分であることを総合的・客観的に評価し、選定を行い、また、アクセス制御(適切な認証方法、IP アドレス等による特定の場所や装置からの接続を認証する方法等によるアクセス制御ができることなど)、暗号化(暗号技術検討会及び関連委員会(CRYPTREC)により安全性及び実装性能が確認された「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)に記載されている方法による暗号化」)及びバックアップ・復旧・定期訓練(不測の事態に事業を継続するために必要なバックアップ、復旧、定期訓練等の手順を定め、実施することなど)等のセキュリティ要件について、確認し、選定を行うこと。

イ　機密性1の情報のみを取り扱う場合

必要に応じて前項の内容への適合状況を参考に選定すること。

(3)　外部サービス利用中止における取り扱いについて

情報セキュリティ管理者は、外部サービス利用の中断時や外部サービス提供の終了時における対応として、次の条件を選定条件に含めなければならない。

ア　機密性2以上の情報を取り扱う場合

（ア） サービスの中断・終了時にデータ返却がされること。又は自らデータ取得ができること。

（イ） サービスの中断・終了時にシステム等に保存されているデータを復元不可能な状態にして削除・廃棄できること。 また、確実に廃棄され、復元不可能な状態となったことの確認が証明書等により可能であること。

（ウ） 事前に一定期間の告知期間を設けるなどサービス終了に当たっての取り決めがあること。

イ 機密性1の情報のみを取り扱う場合

必要に応じて前項の内容への適合状況を参考に選定すること。

5 外部サービス提供者の選定基準

情報セキュリティ管理者は、外部サービス提供者を選定する際は、次の条件を選定条件に含めなければならない。

(1) 機密性2以上の情報を取り扱う場合

ISO/IEC 27001（情報セキュリティマネジメントシステム）や ISO/IEC 27017（クラウドサービスセキュリティ）及びこれらと同等以上であると認められるの国際規格の認証を取得していること。これらの認証を取得していない場合は、外部サービス提供者における情報セキュリティ対策の適切な整備・運用及び管理体制の確保について、第三者による監査報告書等により、確認できること。

(2) 機密性1の情報のみを取り扱う場合

前項の内容に適合することが望ましい。

6 外部サービスの利用手続き

情報セキュリティ管理者は、外部サービスの利用にあたっては、以下の内容を確認・実施しなければならない。

(1) 利用しようとする外部サービスが、鎌倉市情報セキュリティポリシー及び本基準に記載の要件を充足するかの確認を行う。

(2) 利用しようとする外部サービスの導入について、デジタル戦略課に導入の事前相談を行う。

(3) 導入する外部サービスの内容により、情報システム審査会での審査・承認を受ける必要があるため、これらに必要な手続きを行う。

(4) その他必要な調整や申請等の作業を行う。