クラウドサービス利用基準

施行日：令和７年４月１日

北九州市

改訂履歴

施行年月日	版番号	改定理由・内容
令和5年4月1日	第1.0版	初版発行（令和5年3月2日決裁、3月29日通知）
令和7年4月1日	第1.1版	総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に伴う改定（令和7年3月3日決裁、3月17日通知）

目次

1　基本的な考え方

（1）目的

クラウドサービス利用基準（以下「本文書」という。）は、本市において、クラウドサービスやウェブ会議サービス等を利用する際の手続きや、利用にあたって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

本文書の適用範囲は、北九州市情報セキュリティ対策基準の適用範囲とする。

2　クラウドサービス利用判断基準

（1）重要情報資産を取り扱う場合

クラウドサービスにおいて機密性の基準第１種又は第２種の情報（以下「重要情報資産」という。）を取り扱う場合は、本文書「3.1 クラウドサービスの選定条件」を満たすクラウド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

クラウド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「4.1 クラウドサービスの選定条件」を満たすクラウドサービスを利用しなければならない。

（3）情報セキュリティ対策基準の適用範囲外におけるクラウドサービスの利用

北九州市情報セキュリティ対策基準の適用範囲外においてクラウドサービスを市民等に利用させる場合には、本文書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。

（4）クラウドサービスを利用する上での留意事項

クラウドサービスの利用に当たっては、情報の管理や処理をクラウド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、適切なクラウド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が考えられる。

① クラウドサービスは、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、クラウドサービス提供者の運用詳細は公開されないためにクラウド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、クラウド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。

② オンプレミスとクラウドサービスの併用やクラウドサービスと他のクラウドサービスの併用等、多様な利用形態があるため、利用者とクラウド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。

③ クラウド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クラウド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。

④ クラウド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。

⑤ サーバ装置等機器の整備環境がクラウド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　クラウドサービスの利用（重要情報資産を取り扱う場合）

3．1　クラウドサービスの選定条件

（1）クラウドサービスの選定条件

所属長は、重要情報資産を取り扱うクラウドサービスを利用する場合には、以下の内容を含む対策をクラウドサービス提供者の選定条件に含めること。

（2）取り扱う情報の格付に応じたセキュリティ要件

所属長は、取り扱う情報の格付に応じて、クラウドサービスのセキュリティ要件としてセキュリティに係る国際規格（ISO/IEC27001）等と同等以上の水準を求めること。

（3）クラウド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

所属長は、クラウド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のほか、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やクラウドサービス提供者等のセキュリティに係る内部統制の保証報告書である SOC 報告書等）から、クラウド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。

（4）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

所属長は、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。

（5）情報が取り扱われる場所等

所属長は、クラウド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クラウド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。）

（6）再委託をする場合

所属長は、クラウドサービス提供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、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に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本市に提供し、本市の承認を受けるよう、クラウドサービス提供者の選定条件に含めること。

（7）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

① 取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件

② 取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

（例：取り扱う情報の可用性区分の格付けに応じて、サービスの中断、終了または変更の際の影響を最小限に抑えるため、システム及びデータのバックアップ計画及び設計を提示し、所属長の承認を得ること。）

（8）セキュリティ対策

① クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における目的外利用の禁止

自組織が取り扱う情報は、クラウドサービス提供者においてクラウドサービスの提供に必要な範囲で利用を認めるものであって、それ以外の目的で利用をさせてはならない。

② クラウド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

③ クラウドサービスの提供に当たり、クラウド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

（例：クラウドサービス提供者が行うクラウド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加えられないための管理体制」が確保されることを求めている。

具体的にクラウドサービス提供者の選定条件に含める内容としては、例えば以下が考えられる。

（ア）クラウドサービスの開発及び運用において、自組織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。

（イ）クラウドサービスに自組織の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、自組織とクラウド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。）

④ クラウドサービス提供者の資本関係・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並びに調達仕様書による施設の場所やリージョンの指定

⑤ 情報セキュリティインシデントへの対処方法

クラウド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、クラウドサービス提供者の選定条件に含めておくとよい。

（例：対処方法

（ア） 復旧を優先する場合は、クラウドサービスの利用を一時的に停止するための手順を規定すること。

（イ） 業務継続を優先する場合は、クラウドサービスの利用を継続した上で情報セキュリティインシデントに対処する手順を規定すること。

（ウ）情報セキュリティインシデントに係るクラウドサービス提供者と自組織間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。）

⑥ 情報セキュリティ対策その他の契約の履行状況の確認方法

⑦ 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

⑧ 情報セキュリティ監査の受入れ

（9）その他要件

① 情報の取扱手順

（ア）格付及び取扱制限の明示等、運搬又は送信、消去等の情報の取扱いに関して、クラウドサービス提供者においても自組織の対策基準に定める内容と同等の取扱いが行われるよう、あらかじめクラウドサービス提供者と合意しておくことが重要である。

（イ）情報システムの利用等において目的外の不必要なアクセスが行われる可能性も考慮し、クラウドサービス提供者における情報の取扱状況を適宜把握することが重要である。

（ウ）クラウドサービス提供者において、業務委託、他のクラウドサービス等を用いてクラウドサービスを提供することが考えられる場合は、北九州市情報セキュリティ対策基準「8.1.業務委託」及び本文書 3 クラウドサービスの利用（情報重要情報資産を取り扱う場合）の規定をクラウドサービス提供者においても遵守させるよう仕様書等に規定し、クラウドサービス提供者とあらかじめ合意しておくことが望ましい。

② クラウドサービスに係るアクセスログ等の証跡の保存

ログは 1 年間以上保存することが望ましい。なお、記憶媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する。

③ クラウドサービス提供者による情報の管理・保管

（ア）利用者はクラウド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。

（イ）クラウド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クラウドサービス提供者に確認の上、合意しておくこと。

④ 情報開示請求に対する開示項目や範囲

（ア）事前に自組織とクラウドサービス提供者が協議の上、クラウド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。

（イ）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　クラウドサービスの利用に係る調達・契約

① 所属長は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件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、クラウド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 所属長は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

３．３　クラウドサービスを利用した情報システムの導入・構築時の対策

① 所属長は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を実施すること。

（ア）不正なアクセスを防止するためのアクセス制御

・クラウドサービスを利用する際にクラウドサービス提供者が付与又はクラウドサービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理

・クラウドサービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御

・クラウドサービスを利用する情報システムの管理者特権を保有するクラウドサービス利用者に対する強固な認証技術の利用

・クラウドサービス提供者が提供する主体認証情報の管理機能が要求事項を満たすことの確認

・クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できることの確認

・クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作の特定と誤操作の抑制

・クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施

・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にクラウド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と認める場合の

適切なセキュリティ対策の実施
・クラウドサービスが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うための必要なログの管理

（イ）取り扱う情報の機密性保護のための暗号化
・クラウドサービス内及び通信経路全般における暗号化の確認
・利用する情報システムに係る法令や規則に対する暗号化方式の遵守度合い

（ウ）開発時におけるセキュリティ対策
・情報システムの構築においてクラウドサービスを利用する場合のクラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用
・情報システムの構築において、クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合の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

（エ）設計・設定時の誤りの防止
・クラウドサービス上に情報システムを構築する際のクラウドサービス提供者への設計、構築における知見等の情報の要求とその活用
・クラウドサービス上に情報システムを構築する際の設定の誤りを見いだすための対策
・クラウドサービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視
・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についての監視と将来の予測
・利用するクラウドサービスの可用性に応じた設計を考慮する。
・クラウドサービス内における時刻同期の方法の確認

② 所属長は、情報システムにおいてクラウドサービスを利用する際には、台帳及び関連文書に記録又は記載しなければならない。なお、台帳に記録又は記載した場合は、システム管理部門へ報告しなければならない。

③ 所属長は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備又は確認しなければならない。

（ア）クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

（イ）クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

（ウ）利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

④ 所属長は、第一項において定める項目に対し、構築時に納品物等を通じて実施状況を確認すること。

３．４　クラウドサービスを利用した情報システムの運用・保守時の対策

① 所属長は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策に留意す

ること。

（ア）クラウドサービス利用方針

・責任分界点を意識したクラウドサービスの利用

・利用承認を受けていないクラウドサービスの利用禁止

・クラウドサービス提供者に対する定期的なサービスの提供状態の確認

・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連絡体制

（イ）クラウドサービス利用に必要な教育

・クラウドサービス利用のための規定及び手順について

・クラウドサービス利用に係る情報セキュリティリスクとリスク対応について

・クラウドサービス利用に関する適用法令や関連する規制等について

（ウ）取り扱う資産の管理

・クラウドサービス上で利用する IT 資産の適切な管理

・クラウドサービス上に保存する情報に対する適切な格付・取扱制限の明示

・クラウドサービスの機能に対する脆弱性対策について、クラウドサービス利用者の責任範囲の明確化と対策の実施

（エ）不正アクセスを防止するためのアクセス制御

・管理者権限をクラウドサービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録

・クラウドサービス利用者に割り当てたアクセス権限に対する定期的な見直し

・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の機能の確認と利用者の制限

・利用するクラウドサービスの不正利用の監視

（オ）取り扱う情報の機密性保護のための暗号化

・暗号化に用いる鍵の管理者と鍵の保管場所

・鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価

・鍵管理機能をクラウドサービス提供者が提供する場合の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情報の要求とリスク評価

（カ）クラウドサービス内の通信の制御

・利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていることの確認

（キ）設計・設定時の誤りの防止

・クラウドサービスの設定を変更する場合の設定の誤りを防止するための対策

・クラウドサービス利用者が行う可能性のある重要操作の手順書の作成と監督者の指導の下での実施

（ク）クラウドサービスを利用した情報システムの事業継続

・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の確実な実施（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）

・可用性の基準第１種及び第２種の情報をクラウドサービスで取り扱う場合の十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施
・クラウドサービス提供者からの変更通知の内容確認と復旧手順の確認
・クラウドサービスで利用しているデータ容量、性能等の監視

② 所属長は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、台帳及び関連文書を更新又は修正しなければならない。なお、台帳を更新又は修正した場合は、システム管理部門へ報告しなければならない。

③ 所属長は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

④ 所属長は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスで発生したインシデントを認知した際は「北九州市情報セキュリティ事故に関する対応要綱」に準じて対応すること。

⑤ 所属長は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認すること。

３．５　クラウドサービスを利用した情報システムの更改・廃棄時の対策

① 所属長は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスの利用を終了する際のセキュリティ対策を実施すること。

（ア）クラウドサービスの利用終了時における対策
・クラウドサービスの利用を終了する場合の移行計画書又は終了計画書の作成
・移行計画書又は終了計画書のクラウドサービス利用者への事前通知

（イ）クラウドサービスで取り扱った情報の廃棄
・情報の廃棄方法

（ウ）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
・作成されたクラウドサービス利用者アカウントの削除
・利用した管理者アカウントの削除・返却と再利用の確認
・クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

② 所属長は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認し記録を残すこと。

4　クラウドサービスの利用（重要情報資産を取り扱わない場合）

4．1　クラウドサービスの選定条件

（1）クラウドサービスの選定条件

所属長は、重要情報資産を取り扱わないクラウドサービスを利用する場合には、以下の内容を含む対策をクラウドサービス提供者の選定条件に含めること。

（2）クラウドサービスを利用可能な業務の範囲

所属長は、以下のようなリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、許可する業務の範囲を決定すること。

検討すべきリスクの例

（ア）クラウドサービス提供者は、保存された情報を自由に利用することが可能である。また、約款、利用規約等でその旨を条件として明示していない場合がある。加えて、クラウドサービス提供者は、利用者から収集した種々の情報を分析し、利用者の関心事項を把握し得る立場にある。

（イ）情報が改ざんされた場合でも、利用形態によってはクラウドサービス提供者が一切の責任を負わない場合がある。

（ウ）クラウドサービス提供者が海外のデータセンター等にサーバ装置を設置してサービスを提供している場合は、当該サーバ装置に保存されている情報に対し、現地の法令等が適用され、現地の政府等による検閲や接収を受ける可能性がある。

（エ）突然サービス停止に陥ることがある。また、その際に預けた情報の取扱いは保証されず、損害賠償も行われない場合がある。約款の条項は一般的にサービス提供者に不利益が生じないようになっており、このような利用条件に合意せざるを得ない。また、サービスの復旧についても保証されない場合が多い。

（オ）保存された情報が誤って消去又は破壊されてしまった場合に、サービス提供者が情報の復元に応じない可能性がある。また、復元に応じる場合でも復旧に時間がかかることがある。

（カ）約款及び利用規約の内容が、クラウドサービス提供者側の都合で利用開始後事前通知等無しで一方的に変更されることがある。

（キ）情報の取扱いが保証されず、一旦記録された情報の確実な消去は困難である。

（ク）利用上の不都合、不利益等が発生しても、サービス提供者が個別の対応には応じない場合が多く、万が一対応を承諾された場合でも、その対応には時間を要することが多い。

（3）クラウドサービスの利用の留意点

所属長は、重要情報資産を取り扱わない前提でクラウドサービスを業務に利用する場合は、以下のことに留意すること。

① サービス利用中の安全管理に係る運用手順

（ア）サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認

（イ）情報の滅失、破壊等に備えたバックアップの取得

（ウ）利用者への定期的な注意喚起（禁止されている重要情報資産の取扱いの有無の確認等）

② 情報セキュリティインシデント発生時の連絡体制

４．２　クラウドサービスの利用における対策の実施

職員等は、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重要情報資産を取り扱わない場合のクラウドサービスの利用を申請すること。また、所属長は、当該クラウドサービスの利用において適切な措置を講ずること。

5　クラウドサービスの利用手続き

5．1　クラウドサービスの許可権限者

（1）重要情報資産を取り扱うクラウドサービス

重要情報資産を取り扱うクラウドサービスを利用する場合は、CISO をクラウドサービスの許可権限者とする。

（2）重要情報資産を取り扱わないクラウドサービス

重要情報資産を取り扱わないクラウドサービスを利用する場合は、所属長をクラウドサービスの許可権限者とする。

5．2　クラウドサービスの利用申請

（1）重要情報資産を取り扱うクラウドサービスを利用する場合

① 所属長は、クラウドサービスを利用する場合には、CISO へクラウドサービスの利用申請を行うこと。

クラウドサービスの中には複数のサービス（機能）を含んだものが存在する。含まれる個々のサービス（機能）において情報セキュリティの対策が異なる場合は、個々のサービスに分割して申請が必要である。

② CISO は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定すること。

③ CISO は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名すること。

④ 所属長は、CISO が承認したクラウドサービスについて、以下の内容を台帳に登録すること。

（ア）クラウドサービスの名称（必要に応じて機能名までを含む）
（イ）クラウドサービス提供者の名称
（ウ）利用目的（業務内容）
（エ）取り扱う情報の格付
（オ）利用期間
（カ）利用申請者（所属・氏名）
（キ）利用者の範囲（自組織の関係者内に限る、部局内に限る など）。
（ク）クラウドサービス管理者（所属・補職名）
（ケ）その他必要な項目

（2）重要情報資産を取り扱わないクラウドサービスを利用する場合

① 職員は、クラウドサービスを利用する場合には、所属長へクラウドサービスの利用申請を行うこと。

② 所属長は、職員等によるクラウドサービスの利用申請について問題がないか確認のうえ、利用の可否を決定することとし、利用を可とする場合は自らがクラウドサービス管理者となる。

③ 利用を可としたクラウドサービスは、常に最新のクラウドサービスの利用状況を把握できるように台帳（重要情報資産を取り扱わない場合）に下記の項目を入力すること。入力内容に変更があった場合は、随時修正すること。

（ア）クラウドサービスの名称（必要に応じて機能名までを含む）
（イ）クラウドサービス提供者の名称
（ウ）利用目的（業務内容）
（エ）取り扱う情報の格付
（オ）利用期間
（カ）利用申請者（所属・氏名）
（キ）利用者の範囲（自組織の関係者内に限る、部局内に限る など）。
（ク）クラウドサービス管理者（所属・補職名）
（ケ）その他必要な項目

6　ウェブ会議サービスを適切に利用するための利用手順

6.1　利用にあたって

（1）職員等は、本市の定める利用手順に従い、ウェブ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

6.2　ウェブ会議サービスの利用時の対策

（1）職員等は、ウェブ会議サービスの利用に当たり、以下の情報セキュリティ対策を実施する必要がある。

① 原則として、自組織から支給された端末（各所属で導入した端末を含む。）を利用すること。

② 利用するウェブ会議サービスのソフトウェアが、最新の状態であることを確認すること。

③ 重要情報資産を取り扱う場合は、可能な限りエンドツーエンド（E2E）の暗号化を行うこと。

④ 重要情報資産を取り扱う場合は、ウェブ会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、E2E の暗号化を利用できなくなる機能を可能な限り使用しないこと。

⑤ 音声を扱う場合は、ヘッドホンを使用するなど、内容が周囲に漏れないよう注意すること。

（2）職員等は、ウェブ会議を主催する場合、会議に無関係の者が参加できないよう以下の情報セキュリティ対策を講ずる必要がある。

① 会議室にアクセスするためのパスワード等をかける。

② 会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知する。

③ 待機室を設けて参加者と確認できた者だけを会議室に入室させる。

④ なりすましや入れ替わりが疑われるなどの不審な参加者を会議室から退室させる。

6.3　留意事項

（1）ウェブ会議サービスを利用する場合、ウェブ会議サービスのソフトウェアで録画等を防止する設定を行っていても、ビデオカメラで撮影されれば会議内容は保存されるため、会議内容は会議の参加者に保存されることを前提として、会議で取り扱う情報を確認する必要がある。

（2）ウェブ会議サービスでは音声・映像、参加者のメールアドレス等の属性等様々な個

人情報を取り扱うことが考えられるため、ウェブ会議に招待される場合は、重要情報資産を含んだチャットへの書き込みや資料共有を行わないなど、情報を保存させないような利用を考慮する必要がある。

（3）ウェブ会議サービスは、音声、映像、共有資料、チャット、録画・録音データ等、多種のデータを扱うため、これらのデータがどこに格納されるかは、情報漏えいリスクに大きく影響する。そのため、主催者は使用するウェブ会議サービスがクラウドサービス、オンプレミスのいずれかを、まず確認することが必要である。

クラウドサービスの場合、負荷分散のため海外のデータセンターが利用されることがある。データセンターが置かれた国によっては、政府が法に基づきデータを強制収用するリスクがある。どの国のデータセンターを使用するかは通常契約で決められるが、無料サービスでは契約プロセスを通さないため、本件は特に注意が必要である。

クラウド上に録画・録音データを保存する場合には、復元不可能な形で完全削除ができるか（セキュアデリート機能の有無）の確認も重要である。

6.4　機密性別のウェブ会議の開催例

（1）重要情報資産を取り扱う会議

① 音声データ等の会議データのクラウド上での復号は、会議の機密性の観点から、いかなる形であれ許されないと判断した。ウェブ会議サービスの資料共有、録画機能は使用せず、音声・映像交換およびチャット機能のみを使用することとした。資料の共有は安全な形でメール添付ファイルとして事前配布し、それを参照する形とした。

② ウェブ会議サービスは E2E の暗号化ができる製品を使用することとした。また、国内データセンターのみを使用する契約とした。

③ 会議パスワードを設定、待機室機能を有効とし、会議パスワードは会議案内メールとは別経路で組織外参加者に安全に届けることとした。また、組織外参加者については会議実施時に声、顔での確認を必ず実施することにした。

（2）重要情報資産を取り扱わない事前申し込みを必要とする講習会

① 会議資料、会議の内容とも機密性は低いため、ウェブ会議サービスは全機能（音声・映像交換、資料共有、チャット等）を使用することとし、データの所在（海外・国内等）にはこだわらなかった。

② 参加者端末、サーバ間の通信が安全であることを確認した。

③ 参加人数が多いため、参加者事前登録の機能を使用し、参加者の事前確認をするとともに、会議の URL は参加者のみに届け、会議実施時の参加者確認は担当をアサインし実施した。