

## 名古屋市外部サービス利用基準

### 1 趣旨

この基準は電子情報の保護を図りつつ、外部サービスの円滑な導入及び一層の活用を図るために、名古屋市情報あんしん条例（平成16年名古屋市条例第41号。以下「あんしん条例」という。）第12条に基づき、外部サービスの利用に当たっての必要な措置等を定めたものである。

なお、この基準における用語の定義、適用範囲、組織体制等は、名古屋市情報セキュリティ対策基準（以下「市対策基準」という。）に準拠する。

### 2 定義

この基準において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

#### (1) 外部サービス

あんしん条例第2条第8号に規定する外部サービスをいう。

#### (2) 外部サービス利用管理者

外部サービスを所管する課等（課、室及び公所等（課を置かないものに限る。）をいう。以下同じ。）の長をいう。

#### (3) 外部サービス提供者

外部サービスを提供する事業者等をいう。

### 3 適用除外

外部サービスの利用に当たって、以下の場合はこの基準の適用を除外する。

#### (1) ソーシャルメディア（名古屋市ソーシャルメディア活用ガイドライン第1項第1号に規定するソーシャルメディアをいう。）の利用に当たって、機密情報を取り扱わない場合

#### (2) 一時的又は専ら試験的な用途のために利用する場合

### 4 関連法規等の遵守

職員は、外部サービスを利用して業務を行う際は、あんしん条例、個人情報の保護に関する法律（平成15年法律第57号）、名古屋市個人情報保護条例（令和4年名古屋市条例第56号）、名古屋市情報セキュリティ基本方針、市対策基準等及びその他の関連する規程を遵守するものとする。

### 5 外部サービス利用管理者の責務

外部サービス利用管理者は、外部サービスを利用する場合は、次の各号に定める内容を実施すること。

- (1) 取り扱う情報資産の分類やこれに応じた取扱制限等を踏まえ、適切な外部サービスを選定すること。
- (2) 運用手順を定め、利用業務、利用目的、取り扱う情報、利用場所等を職員に示すこと。
- (3) 所属における外部サービスの利用状況を把握し、適切に管理すること。
- (4) 外部サービスの約款を継続的に把握し、利用開始の際に求めている情報セキュリティを維持できているか確認すること。

## 6 外部サービスの選定

### (1) 機密情報を取り扱う場合

外部サービスにおいて機密情報を取り扱う場合は、「7 外部サービスの選定要件」を踏まえ、適切な外部サービスを選定しなければならない。

### (2) 機密情報を取り扱わない場合

外部サービスにおいて機密情報を取り扱わない場合は、「7(1) 外部サービスの選定要件」を参考にしつつ、用途に応じた外部サービスを選定しなければならない。

### (3) マイナンバー利用事務系にて利用する場合

マイナンバー利用事務系における外部サービスの利用は原則としてLGWAN-ASPサービスに限られ、当該サービスについてもインターネットと接続されるものは認められない。具体的には、市対策基準「6(1)イ マイナンバー利用事務系における特定通信」及び市管理基準「5(1)イ 特定通信」を満たさなければならない。

## 7 外部サービスの選定要件（機密情報を取り扱う場合）

### (1) 外部サービスの選定要件

外部サービス利用管理者は、外部サービスにおいて機密情報を取り扱う場合は、外部サービスの選定に当たって、以下の要件を約款や協定書、契約書面上等で確認又は合意しなければならない。

#### ア 外部サービス提供者における情報セキュリティガバナンス

- (ア) 取り扱う情報の目的外利用の禁止
- (イ) 情報セキュリティ対策の管理体制
- (ウ) 情報セキュリティインシデントへの対処方法の整備

- (エ) 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（監査受け入れ、認証結果等）及び履行が不十分な場合の対処方法
- (オ) 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
- (カ) サービスレベルの保証
- (キ) 準拠法及び裁判管轄に係るカンントリーリスク

イ 外部サービスにおける情報セキュリティ対策

- (ア) ログインに関わる適切な認証機能の提供
- (イ) 適切なアクセス制限機能の提供
- (ウ) 保存データの漏えい等に備えた対策
- (エ) 通信データの盗聴、改ざん等に備えた対策
- (オ) 不正アクセスを監視、検知、防止等する適切な対策
- (カ) メンテナンス・障害等による停止時の適切な対応（冗長化、連絡体制、バックアップ等）の整備及び情報提供方法の確認
- (キ) 監査や侵害時の証拠調査を適切に行うログ管理等の対策
- (ク) 不正プログラムに備えた対策
- (ケ) 記録媒体の更改時及びサービス利用終了時等におけるデータ廃棄・回収方法の適切な実施及び担保方法

ウ 利用者側（自組織側）における情報セキュリティ運用

- (ア) 責任分界点の把握
- (イ) 利用環境における情報セキュリティ設定の適切な運用
- (ウ) 終了時等のデータ廃棄に係る記録の実施
- (エ) 利用者に対する教育

(2) 外部認証等の取り扱い

次の各号のいずれかに該当する外部サービスは、「7(1) 外部サービスの選定要件」の内、「ア 外部サービス提供者における情報セキュリティガバナンス」の(ア)～(カ)、及び「イ 外部サービスにおける情報セキュリティ対策」の(ア)～(ケ)の内容について、十分な管理体制が敷かれているものとみなすことができる。ただし、その場合であっても、利用者側（自組織側）が講じるべき情報セキュリティ要件に係る内容もあるため、必要な情報を適宜把握しなければならない。

ア 外部サービスがLGWAN-ASPに登録されている

イ 外部サービスがISMAPクラウドサービスリストに登録されている

ウ 外部サービス提供者が、クラウドサービス提供事業者としてISMS認証（ISO/IEC 27017）を取得しており、その対象範囲に外部サービスを含んでいる

エ 外部サービス提供者が、ISMS認証（ISO/IEC 27018）を取得しており、その対象範囲に外部サービスを含んでいる

(3) 選定時の特例

約款による外部サービス等、「7(1) 外部サービスの選定要件」を満たすことができない外部サービスの場合、原則として機密情報を取り扱うことはできないが、以下に該当する場合は取り扱うことができるものとする。ただし、いずれの場合も通信データの適切な暗号化が担保される外部サービスを選定しなければならない。

ア 外部サービス上に機密情報を保存せず、適切な保護措置を講じる場合

イ Web会議サービス利用手順(別紙1)に沿ってWeb会議サービスを利用する場合

8 外部サービス利用申請

外部サービス利用管理者は、機密情報を取り扱う外部サービスの利用を開始するときは、原則として利用開始前に電子情報保護副統括管理者に様式（別紙2）による申請を行い、承認を受ける必要がある。情報セキュリティの対策が異なる複数の機能を含んだ外部サービスを利用する場合は、その機能ごとに名称を分けて報告を行うものとする。

附 則

- 1 この基準は、令和 4年 4月 1日から施行する。
- 2 この基準の第 7項から第11項までの規定は、この基準の施行日以降に外部サービスの利用の選定を開始する場合について適用する。
- 3 施行日前に選定を開始又は終了している外部サービスについては、契約等の更新時にこの基準の第 7項から第12項までの規定を適用する。

附 則

この基準は、令和 5年 4月 1日から施行する。

附 則

この基準は、令和 6年 4月 1日から施行する。

附 則

この基準は、令和 7年 7月 1日から施行する。

## Web会議サービス利用手順

### 1 趣旨

職員がWeb会議を適切に利用するための利用手順を定める。

### 2 定義

Web会議サービスとは、事業者等がインターネット上で提供するWeb会議サービスをいう。

### 3 セキュリティ対策

- (1) 本市がWeb会議を主催する場合は、会議に無関係の者が参加できないよう、次のような対策を講じること。
  - ア 会議室にアクセスするためのパスワード等を可能な限り設定する。  
Teamsのゲスト参加（URLによる参加）等、パスワードが設定できない場合は、URLが関係者外に漏れないよう管理を徹底する。
  - イ 会議の参加者に会議室にアクセスするためのURL及び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。
  - ウ 待機室を設けて参加者と確認できたものだけを会議室に入室させる。
  - エ 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。
- (2) 本市がWeb会議を主催する場合で、機密情報等を取扱う可能性のある場合は、可能な限りエンドツーエンドの暗号化を行うこと。
- (3) 本市がWeb会議を主催する場合で、機密情報等を取扱う場合は、Web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、エンドツーエンド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。
- (4) 音声を取扱う場合は、ヘッドホンを使用する、個室で実施するなど、内容が周囲に漏れないよう注意すること。
- (5) Web会議サービスで参加者と資料共有をする場合は、画面録画をされたり、参加者以外の者が意図せず閲覧する可能性もあるため、参加者に十分注意を促すとともに、そのリスクを理解した上で行うこと。

ただし、要配慮個人情報及び特定個人情報（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第2条第8項に規定する特定個人情報をいう。）については、チャットへの書き込みや資料共有などのWeb会議サービス上へ情報を保存する機能を使用しないこと。

- (6) 会議録音・録画データ、共有資料、チャット等の会議データがクラウド上に存在する場合には、クラウド上からの削除を実施すること。
- (7) 機密情報及び個人情報保護のために、意図しない映り込みや音声の漏えいを避けるよう、参加者端末の場所、映像の背景に配慮すること。

外部サービス利用申請書		様式
		令和 <input type="text"/> 年 <input type="text"/> 月 <input type="text"/> 日
電子情報保護副統括管理者 宛 (総務局行政DX推進部長)		
	外部サービス 利用管理者	<input type="text"/>
<p>外部サービスの利用について、名古屋市外部サービス利用基準に基づき、別紙のとおり、選定要件を満たすことを確認しましたので、下記の通り申請します。</p> <p>記</p>		
1	外部サービス及び提供者の名称	
	外部サービス名称	<input type="text"/>
	外部サービス提供者	<input type="text"/>
2	サービス概要（参考資料別添可）	<input type="text"/>
3	サービスを利用して行う業務	<input type="text"/>
4	取り扱う情報資産の分類	<input type="text"/>
5	申請区分	<input type="text"/>
6	サービス利用期間（契約期間）	<input type="text"/> ~ <input type="text"/>
7	担当者及び連絡先	
	担当者	<input type="text"/>
	メール	<input type="text"/>

## 外部サービス利用申請書 別紙

外部サービス名称		記入日			
外部サービス提供者名称		利用部署			
区分	選定要件	要否	適用状況	備考	
1 認証等の取得状況					
<p>いずれかに該当した場合、「ア 外部サービス提供者における情報セキュリティガバナンス」の(ア)～(カ)、及び「イ 外部サービスにおける情報セキュリティ対策」(ア)～(ケ)(ウの一部を除く)は省略可能です。  ※緑網掛け部分(カントリーリスクと利用者側における情報セキュリティ運用)は残るので注意してください。</p>					
①	LGWAN-ASP	外部サービスがLGWAN-ASP に登録されている。	-		
②	ISMAP	外部サービスがISMAPクラウドサービスリストに登録されている。	-		
③	ISO/IEC 27017	外部サービス提供者が、クラウドサービス提供事業者としてISMS認証(ISO/IEC 27017)を取得しており、その対象範囲に外部サービスを含んでいる。	-		
④	ISO/IEC 27018	外部サービス提供者が、ISMS認証(ISO/IEC 27018)を取得しており、その対象範囲に外部サービスを含んでいる。	-		
2 外部サービス選定要件					
ア 外部サービス提供者におけるセキュリティガバナンス					
(ア)	目的外利用	利用者の取り扱い情報(契約等の手続に付随して外部サービス事業者が知りうる利用者情報等も含む)を、サービス提供業務の遂行目的外で利用しないこと。情報の目的外利用の禁止に対する遵守(義務)の表明をすること。	必須※		
(イ)	管理体制	組織として情報セキュリティ対策の管理体制を構築していること。サービス提供を行う組織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について提示すること。	必須		
(ウ)	インシデント対応	情報セキュリティインシデントが発生した場合に、被害を最小限に食い止めるための対応方法(対応手順、責任分界、対応体制等)について整備していること。	必須		
(エ)	監査等・改善	情報セキュリティ管理状況その他契約の履行状況を確認する方法(監査の受け入れ、外部監査・認証機関等による報告・認証結果等の公表等)が提示されていること。 障害や情報セキュリティインシデントの発生、監査結果等によって、情報セキュリティ対策の履行が不十分であると認められた場合の対応(改善の実施等)方法について提示されていること。	必須		
(オ)	サービス移行	サービス中断時等の復旧要件・データ移行方法等の検討に必要な情報(目標復旧時間、バックアップサイトへのアクセス手段等)を確保できること。	任意		
(カ)	SLA	サービスレベルの保証が定められていること。	任意		
(キ)	データの所在・適用法と裁判管轄(カントリーリスク)	サービス上のユーザ所有データ(バックアップデータを含む。)の所在地が日本国内に限定できること。	必須		
		準拠法、裁判管轄を国内に指定できること。	必須		
		市が登録したデータは、本市に確実に提供でき、提供後のデータの所有権・管理権は、市が保有すること。また、市が登録したデータは、本契約に明示的に定められているところを除き、本市の承諾なく、利用できないものとする。	必須		
イ 外部サービスにおけるセキュリティ対策					
(ア)	利用者認証	利用者のログインに関して適切な本人確認が実施できること。 管理者として保守・更新等に係るアクセスをする場合は、不正接続を防止するため認証を徹底すること。(例：ワンタイムパスワードの併用、多要素認証、電子証明書、接続元IP制限等)	必須		
(イ)	アクセス制御	データ又は保存領域(アカウント、階層構造等)において、適切な権限管理及びアクセス制御機能が提供されていること。 (自組織内において、配下の利用者のデータアクセス権限が異なる人員が複数人存在する場合は「任意」ではなく「必須」として扱う。)	任意 (一部必須)		
(ウ)	保存データ保護	機密情報について、暗号化によって適切に保存データを保護できること。	任意 (一部必須)		
		法令による要求がある場合や緊急の場合を除いて、外部サービス事業者による機密情報へのアクセスを行わないこととなっていること。 (「ISMAPクラウドサービスリスト」への登録がされている外部サービスは省略可能)	任意 (一部必須)		
(エ)	通信データ保護	機密情報について、暗号化によって適切に蓄積・伝送データを保護できること。	必須		
(オ)	不正アクセス対策	通信内容を監視するなど、不正アクセスや不正侵入を検知、防止等する対策を講じていること。	必須		



(カ)	メンテナンス・障害時 対処	メンテナンスや障害等、サービスの停止が発生した場合における対処として、サブサイト等の冗長化対応、データのバックアップと復旧方法の整備、及び利用者に対する情報提供方法が確立されている。	任意		
(キ)	ログ管理	外部サービスに係るアクセスログが適切に取得・管理され、侵害発生時に証拠調査等の対応が適切に実施できること。 利用者側が外部サービス提供者に侵害発生時に調査に必要なログを要求できる、調査ツールがある、又は調査を要求することが可能であること。	必須		
(ク)	不正プログラム対策	マルウェア対策を適切に講じていること。	必須		
(ケ)	データ廃棄	データを復元できないように消去を行い、データを消去・廃棄を適切に行った証明書を提示すること。 証明書の発行ができない場合、約款において適切なデータ消去処理を宣言し、かつ、外部サービス提供者がデータ消去の規定を含むISMS認証(ISO/IEC 27001)もしくは同等以上の措置・認証(OSゴールドマークやSOC報告書等)を受けていること。	必須		
ウ 利用者側(自組織側)におけるセキュリティ運用					
(ア)	責任分界点の把握	外部サービス提供者が示す、利用者側におけるセキュリティ保護に関する安全管理に責任を負うべき内容を把握すること。	必須		
(イ)	セキュリティ運用	ウ(ア)責任分界点の把握で判明したセキュリティ設定を適切に設定し、運用すること。(アカウント認証の管理、暗号鍵の適切な運用等)	必須		
(ウ)	データ廃棄記録	利用終了時等に適切にアカウント及びデータ廃棄のプロセス(自組織側において実施するプロセスがある場合)を実施し、その記録を残すこと。	必須		
その他					
	サービスの利用環境	タブレット端末・スマートフォン等を用いて外部サービスを利用する場合は、情報セキュリティ対策基準・管理基準に定めるモバイル端末に求められるセキュリティ要件を満たし、端末の紛失・盗難等に適切な対応を行うとともに、利用者によるデータへのアクセス制限を厳格に実施すること。	任意 (一部必須)		