

---

# 外部サービス利用基準

---

(第 1.1 版)

制定日：令和 4 年 4 月 1 日

改定日：令和 5 年 3 月 31 日

施行日：令和 5 年 4 月 1 日

神戸市

## 改訂履歷

[illegible]

-目次-

1	はじめに	1
1.1	目的	1
1.2	適用範囲	1
1.3	承認者	1
1.4	本文書の位置付け	1
2	外部サービス利用判断基準	2
2.1	機密性2以上の情報を取り扱う場合	2
2.2	機密性2以上の情報を取り扱わない場合	2
2.3	神戸市情報セキュリティ対策基準の適用範囲外における外部サービスの利用	2
2.4	外部サービス利用における留意事項	2
3	外部サービスの利用（機密性2以上の情報を取り扱う場合）	3
3.1	外部サービスの選定条件	3
3.2	外部サービスの選定	3
3.3	外部サービスの利用に係る調達・契約	4
3.4	外部サービスの利用申請及び承認	4
3.5	外部サービスを利用した情報システムの導入・構築時の対策	4
3.5.1	不正なアクセスを防止するためのアクセス制御	4
3.5.2	取り扱う情報の機密性保護のための暗号化	4
3.5.3	開発時におけるセキュリティ対策	5
3.5.4	設計・設定時の誤りの防止	5
3.5.5	外部サービスにおけるユーティリティプログラムに対するセキュリティ対策	5
3.5.6	実施状況の確認・記録	5
3.6	外部サービスを利用した情報システムの運用・保守時の対策	5
3.7	外部サービスを利用した情報システムの更改・廃棄時の対策	6
4	外部サービスの利用（機密性2以上の情報を取り扱わない場合）	7
4.1	外部サービスの選定条件	7
4.2	外部サービスの選定	7
4.3	外部サービスの利用に係る調達・契約	7
5	外部サービスの利用手続き	8
5.1	外部サービスの許可権限者	8
5.1.1	機密性2以上の情報を取り扱う外部サービス	8
5.1.2	機密性2以上の情報を取り扱わない外部サービス	8
5.2	外部サービスの利用申請	8
5.3	委託先等による外部サービスの利用	9
6	外部サービス利用中の取扱い	9
6.1	外部サービス利用基準の確認	9
6.2	是正措置	9
6.3	確認の指示	9

7 外部サービスの利用終了時の取り扱い .....	10
7.1 機密性2以上の情報を取り扱う外部サービスの利用を中止する場合 .....	10
7.2 機密性2以上の情報を取り扱わない外部サービスの利用を中止する場合 .....	10

## 1 はじめに

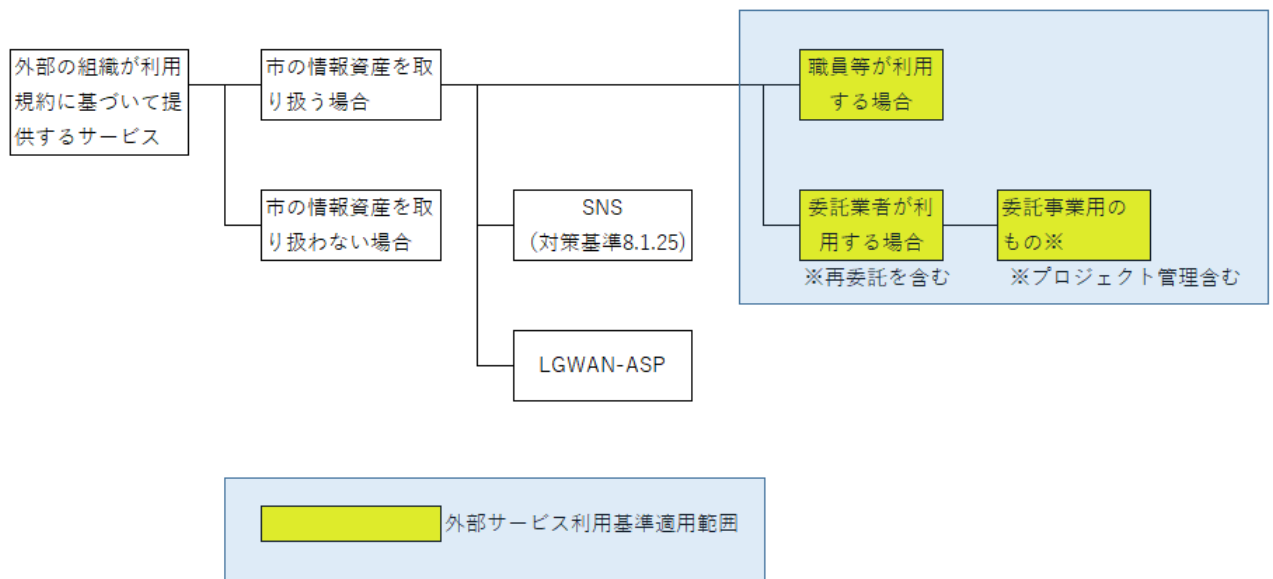
### 1.1 目的

外部サービス利用基準（以下、本文書という）は、神戸市（以下、本市という）において、クラウドサービスや Web 会議サービス等の外部サービス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。

### 1.2 適用範囲

ア 本文書の適用範囲は、神戸市情報セキュリティ対策基準の適用範囲とする。

イ 本文書の適用される外部サービスの範囲は、下記図の網掛けの範囲とする。



### 1.3 承認者

本文書の承認者は、情報セキュリティ最高責任者（以下、「CISO」という。）とする。

### 1.4 本文書の位置付け

本文書は、以下の文書に準拠して記述している。

- ・神戸市情報セキュリティ基本方針
- ・神戸市情報セキュリティ対策基準

## 2 外部サービス利用判断基準

### 2.1 機密性 2 以上の情報を取り扱う場合

外部サービスにおいて機密性 2 以上の情報を取り扱う場合は、本基準「3.1 外部サービスの選定条件」を満たす外部サービスを利用しなければならない。

### 2.2 機密性 2 以上の情報を取り扱わない場合

外部サービスにおいて機密性 2 以上の情報を取り扱わない場合は、本基準「4.1 外部サービスの選定条件」を満たす外部サービスを利用しなければならない。

### 2.3 神戸市情報セキュリティ対策基準の適用範囲外における外部サービスの利用

神戸市情報セキュリティ対策基準の適用範囲外において外部サービスを市民等に利用させる場合には、本基準に準じて適切な外部サービスを選定しなければならない。

### 2.4 外部サービス利用における留意事項

外部サービスの利用に当たっては、情報の管理や処理を外部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、適切な外部サービス提供者を選定することにより外部サービス利用におけるリスクを低減することが考えられる。

ア 外部サービスは、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、外部サービス提供者の運用詳細は公開されないために外部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、外部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。

イ オンプレミスと外部サービスの併用や外部サービスと他の外部サービスの併用等、多様な利用形態があるため、利用者と外部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。

ウ 外部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外部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。

エ 外部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。

オ サーバ装置等機器の整備環境が外部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 外部サービスの利用（機密性 2 以上の情報を取り扱う場合）

#### 3.1 外部サービスの選定条件

情報管理者、業務システム管理者、情報基盤管理者（以下、情報管理者等という。）は機密性 2 以上の情報を取り扱う外部サービスを利用する場合には、別紙「外部サービス要件（機密性 2 以上）」に記載の内容を外部サービスの選定条件に含めなければならない。

#### 3.2 外部サービスの選定

ア 情報管理者等は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスが、本市の情報セキュリティポリシー等を満たしているか否かを評価の上、選定すること。また、必要に応じて外部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等と同等以上の水準を求めること。

イ 情報管理者等は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、外部サービス利用におけるセキュリティ要件を定めること。

ウ 情報管理者等は、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すること。

エ 情報管理者等は、必要となる条項（インシデントの報告義務、損害賠償等）が契約や利用規約に盛り込まれているか確認するとともに、必要に応じて契約及びサービスレベルを保証させるための SLA を締結する。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を取得するなどレベルに応じた適切な対策を実施する。

外部サービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関する外部サービス事業者の定める条件に鑑み、その規約内容が本市によって受容可能か判断する。

なお、必要となる条項が盛り込まれていない外部サービスでは原則として機密性 2 以上の情報を取り扱うことはできないが、外部サービス提供者との間に規約等に優先する特約を締結するなど、必要となる条項を実質的に担保することで機密性 2 以上の情報の取り扱いを可能とすることも考えられる。

オ 外部サービスの利用規約等では損害賠償について上限が設けられるなど、本市にとって不利になる条件が盛り込まれている場合があるので十分検討のうえ判断すること。

カ 情報管理者等は、外部サービス事業者と情報セキュリティに関する役割及び責任の分担について確認すること。

キ 情報管理者等は、情報セキュリティに配慮した開発・構築及び運用・保守の手順及び実践内容について、外部サービス事業者から必要な情報が得られることを、契約の前に確認すること。

### 3.3 外部サービスの利用に係る調達・契約

- ア 情報管理者等は、外部サービスを調達する場合は、3.1 外部サービスの選定条件を調達仕様に含めること。
- イ 情報管理者等は、外部サービスを調達する場合は、外部サービス提供者及び外部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。

### 3.4 外部サービスの利用申請及び承認

- ア 情報管理者等は、外部サービスを利用する場合には、情報セキュリティ管理者へ外部サービスの利用申請を行うこと。
- イ 情報セキュリティ管理者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定する。
- ウ 情報セキュリティ管理者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、申請者に通知するとともに、申請者を外部サービス管理者に指名する。

### 3.5 外部サービスを利用した情報システムの導入・構築時の対策

外部サービス管理者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部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行うこと。

#### 3.5.1 不正なアクセスを防止するためのアクセス制御

- ア 外部サービス提供者が付与又は外部サービス利用者が登録する識別コードを、作成から廃棄に至るまで、ライフサイクルで管理すること。
- イ 外部サービスを利用する際に使用するネットワークに対して、サービスごとにアクセスを制御すること。
- ウ 管理者特権を保有する外部サービス利用者に対し、強固な認証技術を利用すること。
- エ 外部サービス提供者が提供する主体認証情報が適切に管理されていること。
- オ 外部サービス上に保存する情報や外部サービスの機能に対してアクセス制御ができること。
- カ 外部サービス利用者による外部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ができること。
- キ 外部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が実施されていること。
- ク インターネット等の外部の通信回線から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場合、適切なセキュリティ対策が実施されていること。

#### 3.5.2 取り扱う情報の機密性保護のための暗号化

- ア 外部サービス内及び通信経路全般において暗号化が行われていること。
- イ 利用する情報システムに係る法令や規則を遵守する暗号化方式となっていること。

### 3.5.3 開発時におけるセキュリティ対策

- ア 外部サービス提供者へセキュリティを保つための開発手順等の情報を要求し、それを活用すること。
- イ 外部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、そのソフトウェアの外部サービス上におけるライセンス管理を行うこと。

### 3.5.4 設計・設定時の誤りの防止

- ア 外部サービス提供者へ設計、構築における知見等の情報を要求し、それを活用すること
- イ 設定の誤りを見いだすための対策をとること。
- ウ ネットワーク設計において、セキュリティ要件の異なるネットワーク間の通信を監視すること。
- エ 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を監視し、将来の予測を行うこと。
- オ 利用する外部サービス上で可用性 2 の情報を取り扱う場合は、可用性を考慮した設計とすること。
- カ 外部サービス内における時刻同期の方法を確認すること。

### 3.5.5 外部サービスにおけるユーティリティプログラムに対するセキュリティ対策

ユーティリティプログラムには、アプリケーションや OS の設定を変更するものがあるため、利用するユーティリティプログラムの使用を確認し、外部サービスの動作に悪影響を及ぼさないようにすること。

### 3.5.6 実施状況の確認・記録

外部サービス管理者は、3.5 外部サービスを利用した情報システムの導入・構築時の対策に規定されている内容について、外部サービス事業者に情報を求め、実施状況を確認・記録すること。

## 3.6 外部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 業務システム管理者、情報基盤管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部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を規定すること。
  - ア 外部サービス利用方針の規定
  - イ 外部サービス利用に必要な教育
  - ウ 取り扱う資産の管理
  - エ 不正アクセスを防止するためのアクセス制御
  - オ 取り扱う情報の機密性保護のための暗号化
  - カ 外部サービス内の通信の制御
  - キ 設計・設定時の誤りの防止
  - ク 外部サービスを利用した情報システムの事業継続

ケ 設計・設定変更時の情報や変更履歴の管理

- ② 業務システム管理者、情報基盤管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。
- ③ 業務システム管理者、情報基盤管理者は、前各項において定める規定に対し、外部サービス事業者に情報を求め、運用・保守時に実施状況を定期的に確認・記録すること。

### 3.7 外部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 業務システム管理者、情報基盤管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。
  - ア 外部サービスの利用・終了時における対策
  - イ 外部サービスで取り扱った情報の廃棄
  - ウ 外部サービスの利用のために作成したアカウントの廃棄
- ② 外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。
- ③ 外部サービス管理者は、外部サービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

## 4 外部サービスの利用（機密性 2 以上の情報を取り扱わない場合）

### 4.1 外部サービスの選定条件

情報管理者等は機密性 2 以上の情報を取り扱わない外部サービスを利用する場合には、別紙「外部サービス要件（機密性 1）」に記載の内容を満たす外部サービスを選定しなければならない。

### 4.2 外部サービスの選定

ア 情報管理者等は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスが、本市の情報セキュリティポリシー等を満たしているか否かを評価の上、選定すること。また、必要に応じて外部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等と同等以上の水準を求めること。

イ 情報管理者等は、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すること。

ウ 情報管理者等は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、外部サービス利用におけるセキュリティ要件を定めること。

エ 情報管理者等は、必要となる条項（インシデントの報告義務、損害賠償等）が契約や利用規約に盛り込まれているか確認するとともに、必要に応じて契約及びサービスレベルを保証させるための SLA を締結する。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を取得するなどレベルに応じた適切な対策を実施する。外部サービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関する外部サービス事業者の定める条件に鑑み、その規約内容が本市によって受容可能か判断する。

なお、必要となる条項が盛り込まれていない外部サービスは原則として利用できないが、外部サービス提供者と規約等に優先する特約を締結するなど、必要となる条項を実質的に担保することで外部サービスの利用を可能にすることも考えられる。

オ 外部サービスの利用規約等では損害賠償について上限が設けられるなど、本市にとって不利になる条件が盛り込まれている場合があるので十分検討のうえ判断すること。

カ 情報管理者等は、外部サービス事業者と情報セキュリティに関する役割及び責任の分担について確認すること。

### 4.3 外部サービスの利用に係る調達・契約

ア 情報管理者等は、外部サービスを調達する場合は、4.1 外部サービス提供者の選定条件を調達仕様に含めること。

イ 情報管理者等は、外部サービスを調達する場合は、外部サービス提供者及び外部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。

## 5 外部サービスの利用手続き

### 5.1 外部サービスの許可権限者

#### 5.1.1 機密性2以上の情報を取り扱う外部サービス

機密性2以上の情報を取り扱う外部サービスを利用する場合は、情報セキュリティ管理者を外部サービスの許可権限者とする。

#### 5.1.2 機密性2以上の情報を取り扱わない外部サービス

機密性2以上の情報を取り扱わない外部サービスを利用する場合は、当該外部サービスを取り扱う情報管理者等を外部サービスの許可権限者とする。

### 5.2 外部サービスの利用申請

#### 5.2.1 機密性2以上の情報を取り扱う外部サービスを利用する場合

- ① 情報管理者は、外部サービスを利用する際、情報セキュリティ管理者に利用申請する。利用申請時には、別紙「外部サービス要件（機密性2以上）」を提出すること。
- ② 情報セキュリティ管理者は申請内容を確認し、問題がなければ承認する。
- ③ 情報セキュリティ管理者は申請者に結果を通知し、承認時は申請者を外部サービス管理者に指名する。
- ④ 承認後、外部サービス管理者は情報システム台帳に登録を行う。
- ⑤ 情報セキュリティ管理者にて以下の内容をサービス利用状況に登録する。
  - ア 外部サービスの名称
  - イ 外部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、部局内に限る等）
  - ク 外部サービス管理者（所属役職）
- ⑥ 外部サービス利用のための公用アカウントを作成すること。私用アカウントでの外部サービス利用は禁止する。

#### 5.2.2 機密性2以上の情報を取り扱わない外部サービスを利用する場合

- ① 情報管理者等は、別紙「外部サービス要件（機密性1）」により外部サービスの利用について問題がないか確認する。
- ② 問題がなければ、情報管理者等にて利用を承認し、自らが外部サービス管理者となる。
- ③ 承認後、外部サービス管理者が情報システム台帳へ登録する。
- ④ 外部サービス利用のための公用アカウントを作成すること。私的なアカウントでの外部サービス利用は禁止する。

### 5.3 委託先等による外部サービスの利用

情報管理者等は、委託先や指定管理者等、本市の業務の一部を担っているものが、外部サービスを利用する場合には、それらの事業者から別紙「外部サービス要件（機密性2以上）または「外部サービス要件（機密性1）」を提出させ、情報管理者等が要件適合を確認するものとする。

## 6 外部サービス利用中の取扱い

### 6.1 外部サービス利用基準の確認

外部サービス管理者は外部サービスの利用規約やシステム構成等に変更があった際には、利用している外部サービスが本利用基準に適合しているか確認しなければならない。また、外部サービスにおいてインシデントが発生した際には、あらためて利用基準に適合しているか確認しなければならない。

### 6.2 是正措置

外部サービス管理者は外部サービスが本利用基準に適合しない場合には、適合するように外部サービスの取り扱いについては是正しなければならない。是正できない場合には速やかに外部サービスの利用を中止しなければならない。

### 6.3 確認の指示

情報セキュリティ管理者は、外部サービスにおける脆弱性や情報セキュリティインシデントの情報を得た際、または必要に応じて外部サービス管理者に対して本利用基準に適合しているかを確認させることができる。この場合、外部サービス管理者は速やかに利用基準に適合しているか確認を行い、その結果について情報セキュリティ管理者に報告しなければならない。

## 7 外部サービスの利用終了時の取り扱い

### 7.1 機密性2以上の情報を取り扱う外部サービスの利用を中止する場合

- ① 外部サービス管理者は、情報セキュリティ管理者に利用中止を申請する。
- ② 外部サービス管理者は、情報システム台帳の状態を稼働中から廃止済みに変更する。
- ③ 情報セキュリティ管理者はサービス利用状況を更新する。
- ④ 外部サービス管理者は、外部サービスで取り扱った情報を廃棄する。
- ⑤ 外部サービス管理者は、外部サービスの利用のために作成したアカウントを廃棄する。
- ⑥ 外部サービス管理者は、④⑤において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録する。

### 7.2 機密性2以上の情報を取り扱わない外部サービスの利用を中止する場合

外部サービス管理者は、情報システム台帳の状態を稼働中から廃止済みに変更する。