運用実施要領

[プロジェクト名]

第 n.n版

改訂履歴

|  |  |  |  |
| --- | --- | --- | --- |
| 版数 | 改訂日付 | 改訂者 | 改訂内容 |
| n.n | 2021年3月30日 | XXXX | ・資料間の不整合の修正 |

変更履歴

|  |  |  |  |
| --- | --- | --- | --- |
| 履歴ID | 更新日付 | 更新者 | 更新内容 |
| n.n.rn | yyyy年mm月dd日 |  |  |

目次

[第１章 はじめに 5](#_Toc67247380)

[第２章 コミュニケーション管理 6](#_Toc67247381)

[１． 運用に携わる事業者、関係事業者との合意形成手続等 6](#_Toc67247382)

[２． 運用事業者が参加すべき会議等 6](#_Toc67247383)

[３． インシデント発生時の連絡手段、報告要領等 6](#_Toc67247384)

[第３章 体制管理 7](#_Toc67247385)

[第４章 作業管理 8](#_Toc67247386)

[第５章 リスク管理 10](#_Toc67247387)

[第６章 課題管理 11](#_Toc67247388)

[第７章 システム構成管理 12](#_Toc67247389)

[第８章 変更管理 14](#_Toc67247390)

[第９章 情報セキュリティ対策 16](#_Toc67247391)

## はじめに

［本ドキュメントが対象とするプロジェクト・業務・情報システムの概要を記載する。なお、以降のフォーマットはサンプルとして提供するものであり、情報システムの特性、プロジェクトの内容等に応じて適宜カスタマイズして使用すること。］

## コミュニケーション管理

［運用に携わる事業者、関係事業者との合意形成手続や運用事業者が参加すべき会議、開催頻度・議事録等の管理の記載方法を次に示す。］

### 運用に携わる事業者、関係事業者との合意形成手続等

［プロジェクト管理要領の「コミュニケーション管理」注）も踏まえて、運用に携わる事業者、関係事業者等との合意形成に関する手続、連絡調整に関する方法や手順、頻度、議事録の管理等について記載する。特に議事録については、ＰＪＭＯが議事録の正確性を確認し、修正することができる旨の記載に加えて、議事録の内容を確認し確定するプロセスについても記載する。

注）標準ガイドライン解説書「第３編第２章２．2)イ コミュニケーション管理」参照。

### 運用事業者が参加すべき会議等

［プロジェクト管理要領の「コミュニケーション管理」の記載事項、提案書を踏まえ、以下に示す例を参考に、運用事業者が参加すべき会議やその開催頻度、主催者、参加者、議事録の作成主体等について記載する。

参加者の定義に当たっては、会議目的に合わせて確認・検討・判断に必要な関係者を網羅的に定義することが重要であるが、必要以上に多数とした場合には、参加者の負荷が高まる、開催日程調整が困難になる、会議において会議目的外の検討が行われる等のリスクが高まる点に留意すること。］

|  |  |  |
| --- | --- | --- |
| 会議体名称 | 会議目的 | 開催頻度 |
| 定期運用会議 | 運用作業実績、リスク、課題等の確認 | 毎月等 |
| 運用業務年間評価会議 | 年間の運用作業実績の確認、改善策の検討 | 年次 |
| 対策検討会議 | 障害対応、再発防止策の検討 | 障害発生時等 |
| その他調整会議※ | 他の情報システムの運用作業との調整 | 適宜 |

※複数の情報システムを統合的に運用する場合や政府共通プラットフォームを利用する場合等

### インシデント発生時の連絡手段、報告要領等

［インシデント発生時の連絡窓口や情報共有プロセス、報告様式やタイミング等を記載する。］

## 体制管理

［調達仕様書で示した作業の実施体制注１）を基に、提案書を踏まえ、作業体制の説明及び作業要員変更時の報告・承認方法を記載する。

作業体制の記載に当たっては、チーム及び作業要員数、作業要員に求める資格要件を記載し、各チームが適正な作業体制を確保できていることが確認できるようにする。

運用業務を行う上での作業体制注２）の変更時の報告・承認方法の記載に当たっては、実施のタイミング、報告方法（報告内容、報告先、様式）、承認方法（承認時の確認事項、承認プロセス、承認結果の通知方法、様式等）等を記載し、作業要員の変更が、迅速で、かつ、業務遂行に悪影響を与えない形で実施でき、常に最新の作業体制情報（作業要員に求める資格要件の充足状況を含む。）を確認できるようにする。］

注１）標準ガイドライン解説書「第３編第６章３．1)オ 作業の実施体制・方法に関する事項」参照。

注２）標準ガイドライン解説書「第３編第９章１．2)イ 作業体制に関する事項」参照。

## 作業管理

［運用状況の月次報告において、運用作業実績や情報システムの構成や運転状況、サービスレベルの達成状況等の運用事業者から報告を求める内容についても記載する。報告を求める具体的な内容の例を以下に示す。

また、情報システムの運用・保守中に発生した問題やインシデントの管理方法についても記載する。問題やインシデントについては、運用事業者において一元管理するため、保守事業者が問題やインシデントを検知した際には、問題やインシデントの内容等の情報について迅速に報告させ、確実にそれらの情報を把握する旨を記載する。問題やインシデントの管理における運用事業者、保守事業者等の役割分担を明確にするため、以下に示す図を参考に、問題・インシデント管理のフローも記載する。

問題やインシデントのうち、プロジェクト全体で管理すべきリスクや課題については、標準ガイドライン解説書「第３編第９章１．3)エ リスク管理」及び同「第３編第９章１．3)オ 課題管理」に記載する手順等に従い対応する旨を記載する。］

|  |  |
| --- | --- |
| 報告項目 | 内容 |
| 作業実績状況 | * 運用作業の集計結果（実施件数、工数実績、総作業時間等） * 運用作業の一覧（作業内容、担当者、発生日、完了日等） * 作業実績状況を踏まえた改善提案　等 |
| サービスレベルの達成状況 | 「運用計画」の附属文書として作成した「監視項目」について報告を求める。また、目標値に満たない項目がある場合には、要因分析結果の報告や改善策の提案も求める。  例：   * 稼働率（ハードウェア、ソフトウェア、ネットワーク等） * 応答時間 * 応答時間達成率 * スループット * バッチ処理完了時間遵守率 * 定時バックアップ率 * 障害復旧時間　等 |
| 情報システムの構成と運転状況 | 「運用計画」の附属文書として作成した「監視項目」について報告を求める。また、目標値に満たない項目がある場合には、要因分析結果の報告や改善策の提案も求める。  例：   * 情報システム利用状況（アクセス件数、利用件数、ＣＰＵ使用率、メモリ空き容量、ＨＤＤ空き容量等） * 情報システム構成情報（ソフトウェアライセンス数、構成変更件数等） * セキュリティ状況（アカウントロック検知数、不正アクセス件数、ウイルス検知数、不正侵入検知数等）　等 |
| 情報システムの定期点検状況 | * 定期点検の実施有無 * ログ解析結果　等 |
| 情報システムの利用者サポート、教育・訓練状況 | * ヘルプデスク稼働状況（問合せ件数、一次回答率等） * コールセンタ稼働状況（問合せ件数、一次回答率等） * 操作研修実施状況（研修実施回数、研修受講率等）　等 |
| リスク・課題の把握・対応状況 | * リスク・課題の一覧 * リスク・課題の発生理由、対応状況　等 |
| 問題・インシデントの把握・対応状況 | * 発生した問題・インシデントの一覧 * 問題・インシデントの発生理由、対応状況　等 |
| 業務実施指標の証跡 | * 電子決裁件数 * 一連の業務に要した処理時間　等 |

ダイアグラム, 概略図

自動的に生成された説明

## リスク管理

［運用事業者に対して運用上のリスクの提示を求める際の手順や報告様式について記載する。なお、運用事業者との間でリスクの報告に用いる様式は、原則として標準ガイドライン実践ガイドブック第３編第２章別紙「プロジェクト管理要領\_別紙２-Ａ０１\_リスク分析の検討事項」の様式を参考にして作成する。この際、これまでの工程におけるリスク対応の結果を確認した上で、想定されるリスクやリスクの顕在化要因等を見直し、運用に係るリスクを網羅的に整理する。

運用事業者から報告を受けた運用上のリスクについて、プロジェクト全体で管理すべきリスクとして整理する際には、運用の範囲内で対応可能なものが含まれていないか否かを確認する。

また、リスク管理における運用事業者、保守事業者等の役割分担を明確にするため、以下に示す図を参考とし、リスク管理のフローを記載する。］

ダイアグラム

自動的に生成された説明

## 課題管理

［運用事業者に対して運用上の課題の提示を求める際の手順や報告様式について記載する。なお、運用事業者との間で課題の報告に用いる様式は、原則として標準ガイドライン実践ガイドブック第３編第２章別紙「プロジェクト管理要領\_別紙２－Ａ０２\_課題管理の書式例」の様式を参考にして作成する。

運用事業者から報告を受けた運用上の課題について、プロジェクト全体で管理すべき課題として整理する際には、運用の範囲内で対応可能なものが含まれていないか否かを確認する。

また、課題管理における運用事業者、保守事業者等の役割分担を明確にするため、以下に示す図を参考とし、課題管理のフローを記載する。］

ダイアグラム, 概略図

自動的に生成された説明

## システム構成管理

［運用事業者に対して管理を求める対象とする情報システムを構成するハードウェアやソフトウェア製品、ネットワーク等の各資産における管理項目を記載する。また、保守事業者が情報システムの構成を変更した際には、変更内容等の情報について迅速に報告させ、確実にそれら情報を更新する旨を記載する。また、ハードウェア、ソフトウェアの構成について個別に管理するだけでなく、稼働環境の確認やライセンス管理の観点からもソフトウェアがどのハードウェアに紐づいているかについても明らかにできる関連図についても記載する。情報システムを構成する各資産における管理項目の例を以下に示す。］

|  |  |
| --- | --- |
| 資産 | 管理項目（例） |
| ハードウェア | 管理番号、分類、メーカ、品番、シリアル番号、数量、購入日、廃棄日、設置場所、ＯＳ、バージョン、実装メモリ、ディスク容量、保守サポート期限　等 |
| ソフトウェア製品 | 管理番号、分類、名称、バージョン、数量、購入日、廃棄日、契約ライセンス数、使用済ライセンス数、媒体保管場所、保守サポート期限　等 |
| アプリケーションプログラム | 管理番号、分類、名称、バージョン、取得日、最新更新日、廃棄日、媒体保管場所　等 |
| ネットワーク | 管理番号、分類（アクセス回線、中継回線）、ネットワーク種類、帯域、設置拠点、契約開始日、契約終了日　等 |
| 外部サービス | 管理番号、サービス分類、名称、契約開始日、契約終了日　等 |
| 施設・区域 | 管理番号、分類、名称、場所　等 |
| 公開ドメイン | 管理番号、分類、名称、ドメイン数、作成日、終了日　等 |
| その他 | 証明書有効期限　等 |

［また、システム構成管理として管理すべきドキュメントを記載する。

（システム構成管理において管理すべきドキュメントの例）

* ハードウェア構成図
* ソフトウェア構成図
* ハードウェアとソフトウェアの関連図
* ネットワーク接続構成図
* ネットワーク機器構成図
* 建物図面、電源や信号ケーブル等の配線図　等

さらに、システム構成管理における運用事業者、保守事業者等の役割分担を明確にするため、以下に示す図を参考とし、システム構成管理のフローを記載する。］

ダイアグラム

自動的に生成された説明

## 変更管理

［運用により発生する変更内容について、管理対象、変更手順、管理手法等を記載する。管理対象としては、次の例を参考に、運用業務における変更管理の対象とすべき資料等を特定し、記載する。なお、変更管理の対象となるものは、承認等に基づき確定した状態にあるものであり、承認前等で内容が流動的であるものは含めない点に留意する。

特に、ソフトウェアの保守により変更が発生する場合には、運用業務における変更管理（本番環境への適用履歴管理）と保守業務における変更管理（修正プログラムによるソフトウェアの変更履歴管理）は個別に行うが、それぞれの事業者における変更内容は一意に特定できる情報によりひも付けて確認できる必要がある。そのため、ソフトウェアの保守事業者が仕様書、設計書等を変更した際には、運用事業者が変更内容等の情報について報告を受け、確実にそれら情報の把握及び管理を行う旨を記載する。

（管理対象の例）

* 運用要件定義書
* 設計書
* 調達仕様書
* 運用計画とその附属文書（確定版）
* 運用実施要領（確定版）
* 作業手順書（確定版）
* マニュアル（確定版）
* ソースコード 等

また、変更管理における運用事業者、保守事業者等の役割分担を明確にするため、以下に示す図を参考とし、変更管理のフローを記載する。］

ダイアグラム

自動的に生成された説明

## 情報セキュリティ対策

［要件定義の情報セキュリティに関する事項注１）及び調達仕様書における情報セキュリティに係る内容注２）に基づき、情報セキュリティ確保のための管理項目やその内容について記載する。なお、各管理項目における具体的な手順等は、作業手順書として別途作成する。特に、異常検知時の報告所要時間やログの点検間隔等、定量的に記載できるものは定量的に記載することが望ましい。

注１）標準ガイドライン解説書「第３編第５章２．1)ウj) 情報セキュリティに関する事項」参照。

注２）標準ガイドライン解説書「第３編第６章３．1)カ 作業の実施に当たっての遵守事項」参照。

（情報セキュリティ確保のための管理項目の例）

* 情報・データ管理（情報・データの授受、廃棄等の管理）
* アクセス管理（主体認証情報管理、アクセス権限管理等）
* 不正アクセス監視
* ログ管理、ログ分析
* 脆弱性対策等の情報セキュリティ対策の実施状況の管理 等

以上