

システム運用管理規程

改廃履歴

Rev	改 廃 内 容	実 施 日	作 成 者	承 認 日
1. 0	初版	2005/04/01	情報セキュリティ委員会事務局	2005/03/30
1. 1	第7条（6）①重要ファイルを修正	2006/01/20	情報セキュリティ委員会事務局	2006/01/17
1. 2	第3条「情報システム管理責任者は、・・・」追記 第3条（2）⑨⑩を追記 第5条～第11条 情報システム管理責任者を削除	2006/11/01	情報システム管理責任者	2006/11/01
1. 3	第16条に2項追加（プログラムリリース） 第18条に2項追加（データパッチ）	2007/01/10	情報システム管理責任者	2007/01/16
1. 4	第19条 改廃の決裁 社長→副社長	2008/10/30	情報システム管理責任者	2008/10/29
1. 5	第12条、14条、第15条の計画書作成部門を明確化した。 第16条、18条のシステムの変更・保守部門を明確化した。	2009/07/21	情報システム管理責任者	2009/07/13
1. 6	関連規程および第7条に記述の情報セキュリティポリシー対策基準を情報セキュリティ対策規程に変更。	2010/01/16	情報システム管理責任者	2010/02/16
1. 7	規程作成細則実施に伴う書式変更	2010/04/01	情報システム管理責任者	2010/03/04
1. 8	第19条 条文の削除	2010/08/31	情報システム管理責任者	2010/09/16
2. 0	C S I R T設置に伴う変更	2016/09/01	情報セキュリティ委員会事務局	2016/09/01

関連規程

情報セキュリティ対策規程：情報セキュリティ委員会



本規程（システム運用管理規程）：運用部門の長



アクセス制御管理規程：運用部門の長



ネットワーク管理規程：運用部門の長

目次

第 1 章 総則	1
第 1 条 目的	
第 2 条 適用範囲	
第 3 条 実施者	
第 2 章 システムの運用及び管理	2
第 4 条 システム運用計画	
第 5 条 マニュアル整備	
第 6 条 オペレーション管理	
第 7 条 ファイル管理	
第 8 条 機器・設備管理	
第 9 条 アクセス管理	
第 10 条 リソース管理	
第 11 条 障害管理	
第 3 章 システムの受入	4
第 12 条 新システムの導入	
第 13 条 セキュリティ要件	
第 14 条 受入テスト	
第 15 条 移行	
第 4 章 システムの変更・保守	5
第 16 条 システム変更・保守	
第 17 条 不具合及びセキュリティホール情報の収集	
第 18 条 パッチの適用	

システム運用管理規程

規程番号 5002-0000-00-規

制 定 日 2005年 4月 1日

改 正 日 2016年 9月 1日

第1章 総 則

(目的)

- 第 1 条 本規程は当社におけるシステムの信頼性・安全性・効率性に資するべく、関係者が遵守すべきシステム運用、システム管理の基本を定める。
ただし、本規程に定めのない事項が発生した場合には運用部門の長の指示に従うものとする。

(適用範囲)

- 第 2 条 本規程の対象範囲はシステム運用、システム管理に関わる業務とする。

(実施者)

- 第 3 条 運用部門の長は、当社の情報システムの運用管理について統括する。情報システム運用の実施者は、運用管理業務、システム管理業務、及びオペレーション業務に関するすべての従業員と外部委託先要員をいう。
また、システム運用の実施者は、その役割によって運用管理責任者とシステム管理担当者とオペレータに区分けする。

(1) 運用管理責任者（各情報システムを運用する部門の責任者）

運用管理責任者は、運用業務の円滑な推進を図るために、次の運用管理業務を行う。

- ①運用計画の策定
- ②運用状況の確認
- ③要員管理
- ④費用管理
- ⑤運用評価

(2) システム管理担当者（各情報システムを運用する部門の担当者）

システム管理担当者は、担当する情報システムについて、運用業務の円滑な推進を図るために、次のシステム管理業務を行う。

- ①マニュアル整備
- ②オペレーション管理
- ③ファイル管理
- ④機器・設備管理
- ⑤アクセス管理
- ⑥リソース管理
- ⑦障害管理
- ⑧安全対策
- ⑨システムの受入管理
- ⑩システムの変更・保守管理

(3) オペレータ

オペレータは運用計画、オペレーション指示書、オペレーションマニュアルに基づきオペレーション業務を行う。

第2章 システムの運用及び管理

(システム運用計画)

第 4 条 システム運用の各業務を安定的に遂行するために運用計画を策定し、文書にとりまとめる。

- (1) 年間運用計画（年間運用スケジュール）
- (2) 月次運用計画（月次運用スケジュール）
- (3) 日次運用計画（日次運用スケジュール）
- (4) 要員計画（オペレータスケジュール）
- (5) システムメンテナンス計画（システムメンテナンススケジュール）
- (6) 予算計画（外注人件費、システム保守費、備品・消耗品等）
- (7) 教育訓練計画

(マニュアル整備)

第 5 条 システムを正確かつ安全に運用するため、通常時の各種運用手順を標準化したマニュアルを整備する。また、障害による影響を極小化し早期復旧させるため、障害時の操作手順を明確化したマニュアルを整備する。

(1) マニュアルの標準化

マニュアルは、システム運用の効率性を高め、信頼性を保持するために不可欠なものであることを認識し、記載内容の正確性を十分確認するとともに、標準化された操作手順及び適切な障害対策を記載する。

(2) マニュアル変更・修正

① マニュアルは、オペレーションミス等のトラブルを誘発したり効率の低下を防ぐために、現行のシステムに常に適合したものとする。

② システム変更やシステム運用部門の環境変化に応じて順次改訂する。

(3) マニュアルの保管管理方法

システム運用に必要なマニュアルは、改ざん・不正使用等を防止するため、その保管管理は適正に行う。

(オペレーション管理)

第 6 条 システムの不正使用を防止するとともに、システム運用の円滑化を図るため、オペレーションについての依頼、承認、実行、記録、結果確認等の管理を行う。

(1) オペレーション依頼・承認

コンピュータシステムの不正使用を防止するため、オペレーションの依頼・承認は、オペレーション依頼書等の文書を用いて行う。

(2) オペレーション確認

オペレーションの正確性・正当性を確保するため、オペレーション実行状況を確認するとともに、依頼したオペレーションの記録を残す。

(3) 例外処理

コンピュータの不正使用防止、及び運用業務の円滑化を図るため、例外処理の取扱管理は以下とする。

① 例外処理依頼は、すべて文書により運用部門の責任者の承認を得た後に行う。

② 例外処理は、必要なもののみに限定する。

③ 運用部門の責任者は、例外処理の状況を確認する。

(ファイル管理)

第 7 条 ファイルの不正使用・改ざん・紛失等を防止するため、ファイルの授受・廃棄・複写・保管は「情報セキュリティ対策規程」及び「情報資産取扱規程」の定めに従い行う。

また、ファイルの破損、障害等の発生に備えてバックアップを確保する。

(1) ファイル受渡し

磁気媒体（テープ・CD・MO・フロッピーディスク等）により、外部とデータ授受を行う場合、データ漏えいを防止するため、受渡し方法を定めておく。

(2) ファイル廃棄

ファイルの廃棄においては、誤消去、データ漏えい等を防止するため、ファイル管理簿による保存期間、ファイルの機密度に応じた廃棄方法等を明確にする。

(3) ファイル複写

無断複写等によるデータ漏えいを防止するため、コピーが必要な場合は、情報の重要度に応じた手続きの上、例外処理として扱い、コピーファイルの授受、廃棄についても結果を確認する。

(4) ファイル保存期間

ファイルの誤消去を防止するため、ファイルの重要度に応じ、保存期間を明確にする。

(5) ファイル在庫管理

ファイルの不正使用、紛失等を防止するため、ファイル管理簿等により定期的に棚卸しを行い、在庫管理を徹底する。

(6) バックアップ取得

① 個人情報等厳秘情報および事業継続上の重要ファイルに破損・障害等が発生した場合、早期に回復するためにファイルのバックアップを取得し、保管管理方法を明確にすること。

② バックアップを取得するにあたっては、適切な世代管理レベル（二世代前・三世代前まで等）を設定する。また、その際の作業に従事する要員についても予め限定し、保存する媒体を規定し、その手順書を作成する。

③ 回復に要する時間及びその間の影響を考慮して、取得間隔を定める。

(7) ファイル保管場所

① ファイルの不正使用、紛失等を防止するとともに、障害時・災害時の復旧のため、マシン室・保管庫等定められた場所にファイルを保管する。

② 火災や地震等の災害に備えて、重要なファイルは分散保管や遠隔地保管する。

(8) ファイル修正管理

障害等により、ファイルに不整合が生じ、修正が必要になった場合には、修正作業の依頼、承認の手続を明確にし、結果の確認・検証を行う。また、その作業結果を保存する。

（機器・設備管理）

第 8 条 システム運用を円滑に実施するため、汎用機、サーバ、端末、ネットワーク機器等のハードウェア類、並びに電源、空調、監視等の設備類の管理、保守を行う。

(1) 管理方法

① 各機器・設備類の管理責任者を明確に定める。

② 各機器・設備類は情報資産台帳に記載して管理する。

③ 各機器・設備類の操作手順書を備える。

④ 各機器・設備類の障害発生時の迅速な復旧のために保守体制を明確にする。

(2) 保守方法

① 各機器・設備類を長時間停止した場合の再稼働に当たっては、保守点検を実施する。

② 代替機等常時稼働しない設備は、正常稼働することを定期的に確認する。

- ③メーカー側保守体制、責任者、担当者の氏名・電話番号・保守担当範囲を明確にする。
- ④保守作業の結果を報告書として受領し、分析・評価を行う。
- ⑤保守作業には当該システムのシステム管理担当者が立会いを行う。

(アクセス管理)

- 第 9 条 システムを構成する機器及び運用上必要なファイルなど各種資源に対する不正使用、破壊、改ざん等を防止するため、端末等からアクセスする際のアクセス制御管理を行う。
- (1) アクセス制御について
システムやファイルに対するアクセス制御方針およびアクセス権限者の管理については「アクセス制御管理規程」に定める。
 - (2) ネットワークの管理について
ネットワークの管理、およびネットワークの利用にかかる手続き等は「ネットワーク管理規程」に定める。

(リソース管理)

- 第 10 条 システムの安定稼働を確保するため、システム稼働上での性能データを収拾・監視し、そのデータを分析することにより、運用計画・サービスレベルと合致しているか評価を行う。また、問題点があった場合や将来予測に対して対応が必要な場合には速やかに検討作業を行い、機器設備の増設、システムの更改計画を策定する。

(障害管理)

- 第 11 条 障害が発生した場合の早期発見、早期復旧、局所化、並びに障害の未然防止、再発防止を実現するために障害管理を行う。
- (1) 障害監視
システムの重要度や回復に必要な時間から監視対象を明確にし、その監視内容、監視方法を手順化する。
 - (2) 障害対応体制
障害が発生した場合の連絡体制や障害対策体制を整備し、周知徹底する。障害対策体制では障害のレベルに応じて障害対策会議の設置を行う体制とする。
 - (3) 復旧作業
障害の原因を速やかに把握し、定められた復旧手順により復旧作業を実施する。
 - (4) 障害記録・報告
発生した障害について障害報告書を作成し、システム運用部門の責任者および関係者へ報告する。
 - (5) 未然防止、再発防止
障害の再発防止のため、障害記録をもとに障害の傾向や根本原因を分析し、問題点・課題を明確化し、対応策を検討する。

第3章 システムの受入

(新システムの導入)

- 第 12 条 新規にシステムを導入する場合は、システム開発部門またはパッケージ導入部門（以下、システム開発部門という）は、システム導入計画書を作成し、当該システムを運用する部門の承認を得る。なお、当該計画書には次の項目を含める。
- (1) システムの目的
 - (2) システムの機能概要

- (3) システムの機器構成（含む、ネットワーク構成）
- (4) システムの利用者
- (5) セキュリティ対策（冗長性）
- (6) 導入スケジュール

（セキュリティ要件）

第 13 条 新規にシステムを導入する場合は、次のセキュリティ要件を考慮し、適切なセキュリティ対策を講じる。

- (1) システムの利用者を特定し、利用権限者を認証するシステム機能を搭載する。
- (2) 端末からシステムへのアクセスについて適切な経路を設定する。
- (3) システムのデータファイル、DBには適切なアクセス権限を設定する。
- (4) システムのプログラム、ユーティリティの使用は一般利用者から保護する。
- (5) システムの利用にかかる重要なログは採取したのち一定期間安全に保管する。
- (6) システムファイル、DBファイル等重要なファイルについてバックアップ機能を設定する。
- (7) システムサービス運用時間帯を定め、運用時間帯以外はサービスを停止する。

（受入テスト）

第 14 条 新規にシステムを導入する場合は、システム開発部門の協力の下、重要なシステム、大規模なシステムについては受入テストを実施する。

（移行）

第 15 条 新規にシステムを導入するにあたって、移行処理を伴う場合、システム開発部門は、事前に移行計画書（移行手順書）を作成する。

第4章 システムの変更・保守

（システム変更・保守）

第 16 条 システムの安定稼働、改竄防止の為、システム変更・保守は次のとおり実施する。

- (1) システムに重大な変更及び運用変更がある場合、当該システム開発部門は、事前にシステム更改計画書を作成する。また、変更後のシステムに沿った運用項目・手順を再定義し、運用関係者に再教育する。
システム更改計画書はシステム導入計画書（第 12 条にて定義）による。
- (2) システム保守によりプログラムを本番環境へリリースする場合、各業務のリリース手順に従い、保守担当責任者および当該システムを運用する部門の承認を得る。

（不具合及びセキュリティホール情報の収集）

第 17 条 オペレーティングシステム等の基本ソフトウェア及びパッケージソフトウェアの不具合及びセキュリティホールに関する情報及びパッチ情報を収集する。また、当該システムにとって重大、緊急な情報は、速やかに運用管理責任者へ報告する。

（パッチの適用）

第 18 条 システムの安定稼働、改竄防止の為、パッチの適用は次のとおり実施する。

- (1) システムのパッチは重大・緊急なものについてシステムへ適用する。当該システム開発部門は、パッチ適用による業務への影響を調査し、必要に応じてパッチ適用テストを実施する。
- (2) システム保守によりデータパッチを実施する場合、各業務のパッチ手順に従い、システム開発部門責任者および当該システムを運用する部門の承認を得る。