消防情報管理システム運用管理要綱

消防局警防部指令課

目　　次

第 1 章　　総　則

第 2 章　　管理体制

第 3 章　　情報資産の管理

第 4 章　　機器の導入、変更及び撤去等

第 5 章　　ソフトウェアの導入、変更及び廃棄

第 6 章　　データ等の入出力情報管理

第 7 章　　建物及び関連設備管理

第 8 章　　アカウント管理

第 9 章　　委託先管理

第 10 章　　システム障害対応

第 11 章　　ウィルス対策

第 12 章　　不正アクセス管理

第 13 章　　システム運用

第 14 章　　システム開発及び保守

第 15 章　　ユーザ教育

第 16 章　　災害復旧

第 17 章　　見直し

第１章　総　則

１　趣　旨

この要綱は、別に定めるもののほか、消防情報管理システム（以下「消防 OA」という。）の利用、運用保守、情報セキュリティ及びシステム変更（更新含む）に関し必要な事項を定め、適正かつ安定した運用及び管理を図るものである。

２　適用範囲

この要綱の適用範囲は、消防 OA で取扱う全てのデータ（ドキュメント、ハードコピー、出力したデータ、帳票、アプリケーション、システムログ等)、ネットワーク及びハード機器を対象（以下「情報資産」という。）とする。

３　システム構成

消防 OA を構成するサブシステムは、次のとおりとする。

（１）警防業務システム　：災害活動等に関する情報を取扱うもの
（２）救急業務システム　：救急活動等に関する情報を取扱うもの
（３）予防業務システム　：防火対象物等に関する情報を取扱うもの
（４）危険物業務システム　：危険物施設等に関する情報を取扱うもの
（５）管理業務システム：被服・消防団・車両・マスタデータ等に関する情報を取扱うもの
（６）消防例規等検索システム　：消防例規等に関する情報を取扱うもの
（７）消防 GIS（Geographical information system）　：地図等に関する情報を取扱うもの
（８）消防庁 OL 処理対応システム　：消防庁への統計報告に関する情報を取扱うもの
（９）ネットワークシステム　：消防 OA のネットワーク監理に関する情報を取扱うもの
（10）保安業務システム　：保安施設等に関する情報を取扱うもの

第２章　管理体制

１　運用及び管理のための組織

消防 OA を円滑に運用させるため、消防局に次に掲げる者をおく。

（１）消防 OA 責任者
（２）消防 OA 管理者
（３）消防 OA 所管業務管理者
（４）消防 OA 利用責任者
（５）消防 OA 利用管理者
（６）消防 OA 利用者

２　消防 OA 責任者

消防 OA 責任者とは、システムの運用及び管理の全般を総括する者をいい、次に掲げる業務の責任を有し、警防部指令課長をもって充てる。

（１）情報資産に関すること。
（２）ウィルス対策、不正アクセス等、セキュリティ対策に関すること。
（３）システムの管理体制、保守、構成、機能追加及び開発に関すること。
（４）ハードウェアの導入、変更、配置及び廃棄に関すること。

（５）ソフトウェアの導入、変更及び廃棄に関すること。
（６）関連する施設及び設備に関すること。
（７）管理権限及びユーザアカウントに関すること。
（８）情報セキュリティに係る教育に関すること。
（９）業務委託に関すること。
（10）その他、消防 OA に関すること。

3　消防 OA 管理者

消防 OA 管理者とは、消防 OA 責任者を補佐するとともに、システム全体の維持、管理及び運用を管理する者をいい、警防部指令課情報係の職員をもって充てる。

4　消防 OA 所管業務管理者

消防 OA 所管業務管理者とは、消防 OA で取扱う業務に関わる情報資産、電子計算処理のロジック等の運用及び管理を行う者をいい、業務を所管する所属長をもって充てる。

5　消防 OA 利用責任者

消防 OA 利用責任者とは、各所属内において、次に掲げる業務の責任を有し、所属長をもって充てる。

（１）消防 OA で取扱う情報資産に関すること。
（２）システム障害等に関すること。
（３）消防 OA 機器の管理に関すること。
（４）適正なシステム利用の指導に関すること。
（５）その他、消防 OA に関すること。

6　消防 OA 利用管理者

消防 OA 利用管理者とは、消防 OA 利用責任者を補佐し、適正な新消防 OA の利用に係り所属内の消防 OA 利用者への指導を行うとともに、システムの利用に関する管理を行う者をいい、各所属の庶務（担当）係長をもって充てる。

7　消防 OA 利用者

消防 OA 利用者とは、消防 OA を利用する全ての職員をいう。

第３章　情報資産の管理

1　情報資産

（１）情報資産の管理

消防 OA 管理者は、次に掲げる台帳を整備し、情報資産の追加、変更及び廃棄等があった場合は、その都度台帳を更新し、最新の状態を保つ。

ア　ハードウェア台帳
イ　ソフトウェア台帳
ウ　ファイル・DB 管理台帳
エ　アカウント管理台帳
オ　システムドキュメント台帳

（２）情報資産の監査

消防 OA 責任者は、情報資産について、月に１回以上、各台帳の記載内容と相違がないこ

とを監査する。

監査の結果、情報資産の過不足や各台帳の更新漏れ等があった場合、直ちに原因を調査するとともに必要な措置を行う。

2　情報資産の分類

消防 OA 責任者は、情報資産に関して、川崎市情報セキュリティ対策基準に基づく次の分類にしたがい、機密性、完全性、可用性の評価区分にしたがい分類する。

（1）機密性区分

情報資産について、個人情報等の保護の観点から、許可された者以外が情報の閲覧等をした場合の影響範囲について、情報セキュリティ関連法令等への準拠及び市民生活、行政運営等への影響度から次の区分を明確にする。

なお、「自治体機密性３」は自治体機密性３Ａ、３Ｂ、３Ｃの区分を総じた範囲を指すものとする。

ア　自治体機密性３

（ア）自治体機密性３Ａ

「行政文書の管理に関するガイドライン」（平成２３年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書（国等からの秘密文書扱いの情報提供を受けたもの）

（イ）自治体機密性３Ｂ

漏洩等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産（市民・職員の特定個人情報（マイナンバー情報）、市民・職員の要配慮個人情報）

（ウ）自治体機密性３Ｃ

自治体機密性３Ｂ以上に相当する機密性は要しないが、基本的に公表することを前提としていない行政事務に関する情報で、業務の規模や性質上、取扱いに留意すべき情報資産（市民・職員の個人情報で機密性３Ｂ に該当しないもの、入札予定価格（入札前）など）

イ　自治体機密性２

自治体機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産（法人等に関する情報、職務上の職員情報、審議・検討・協議に関する情報、事務又は事業に関する情報、国の機関等の指示情報など）

ウ　自治体機密性１

自治体機密性２、３以外の情報資産

※機密性区分の自治体機密性２、３は、川崎市情報公開条例第８条に規定する不開示情報に相当する情報が該当する。

（2）完全性区分

情報資産について、破壊や改ざん等の意図しない情報の不備が発生することによる影響範囲について、市民生活、業務運営等への影響度から次の区分を明確にする。

ア　自治体完全性２

改ざん、誤びゅう又は破損により、 住民の権利が侵害される又は行政事務の的確な遂

行に支障（軽微なものを除く）を及ぼすおそれがある情報資産

イ　自治体完全性１

自治体完全性２の情報資産以外の情報資産

（３）可用性区分

情報資産について、許可された利用者が必要な時に情報及び情報システムを利用できない状況になった場合の影響範囲について、市民生活、行政運営等への影響度から次の区分を明確にする。

ア　自治体可用性２

滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く）を及ぼすおそれのある情報資産

イ　自治体可用性１

自治体可用性２の情報資産以外の情報資産

３　評価結果による見直し

消防 OA 責任者は、評価結果を踏まえ、川崎市情報セキュリティ対策基準に基づく見直しを行い、必要に応じて改訂を行う。

４　消防 OA の私的利用の禁止等

（１）消防 OA は業務目的にのみ利用し、個人の興味本位等の私的な利用をしてはならない。

（２）消防 OA に対して、不正に侵入する行為又は試みる行為（なりすまし等）をしてはならない。

（３）業務以外の目的では、情報資産の複写、保存、転送及び閲覧をしてはならない。

第４章　機器の導入、変更、撤去等

１　対　象

情報資産のうち、主電子計算装置及び周辺装置等の機器（以下「消防 OA 機器」という。）を対象とする。

２　企　画

消防 OA 責任者は、消防 OA 機器の導入及び変更を計画するにあたり、次の事項を実施する。

（１）消防 OA 機器に係る諸元、機器構成、ネットワーク等について検討し、基礎的な設計を行うこと。

（２）導入及び変更する消防 OA 機器が本市既設ネットワークに接続する場合には、総務企画局デジタル化施策推進室と必要な調整を行うこと。

（３）導入する OA 機器の配置場所について、庁舎管理者等と次の事項を調整すること

ア　設置場所（空きスペースの有無、コンセント等配線の有無）

イ　消費電力量と設置場所の総電力量

ウ　OA 機器の発熱量と設置場所の空調設備の能力

３　調　達

消防 OA 責任者は、消防 OA 機器を調達するにあたり、別に定められた調達に係る手続に従うとともに、次の事項を盛り込んだ調達仕様書を作成する。

（1）情報セキュリティ対策事項
（2）保守体制及び障害発生時の対応体制事項
（3）調達 OA 機器の製造元に対する要求事項（ISO9001、ISO15408、ISO27001 等の規格取得条件）

> ISO9001 とは、概して製品の品質保証と顧客満足及び改善を含む組織の管理まで踏み込んだ品質マネジメントシステムの要求事項を規定した国際標準規格のこと。
> ISO15408 とは、概して情報技術セキュリティの観点から、情報技術に関連した製品およびインターネットシステムが適切に設計され、その設計が過不足なく実装されていることを客観的に評価・保証するために必要な各種事項を規定した国際標準規格のこと。
> ISO27001 とは、概して情報資産と事業継続保護マネジメントのための事実上の国際標準規格のことで、「情報セキュリティマネジメントシステム」（ISMS）の要求事項を定義しています。

4　作　業

消防 OA 責任者は、消防 OA 機器の導入、変更及び撤去を行うにあたり、次の事項を実施する。

（1）対象となる庁舎管理者と次の事項を調整する。
　ア　作業日時
　イ　作業者（本局職員以外の者が実施する場合には必要に応じて「作業者名簿」を作成すること）
　ウ　作業内容（「導入（変更・撤去）OA 機器一覧」を作成すること）
　エ　作業者の持ち込む資器材
（2）消防 OA 利用責任者は、次の事項を行う。
　ア　あらかじめ提出されている作業者名簿と作業者の照合
　イ　作業者の入庁確認（作業者名簿が存する場合は、それとの照合）
　ウ　作業内容の確認及び立会い
　エ　作業者の持ち込む資機材の確認（本市の所有物が混入していないこと等）
　オ　作業者の退庁確認
（3）施錠されたラックに格納されている OA 機器の変更を行う場合は、消防 OA 責任者が本要綱第 7 章に規定されている鍵の運用を行う。
（4）消防 OA 責任者は、作業完了後に作業完了報告書を作成する。なお、委託により本局職員以外の者が作業した場合で、必要な内容が記載された書面が存する場合は、それをもって作業完了報告に替えることができる。
（5）消防 OA 責任者は、作業完了後に導入及び変更した OA 機器について、ハードウェア台帳を更新する。

5　廃　棄

消防 OA 責任者は、OA 機器の廃棄又は撤去にあたり、次の事項を実施する。

（1）ハードディスク及び可搬媒体は、専用ソフトによるデータ消去または粉砕による物理的な破壊を行う。
（2）データ消去または物理的破壊を委託先やリース会社に実施させる場合は、確実に実施されたことを証明する文書を取得する。

（3）管理番号等が付されたラベルは、確実に処分する。

6　事故対応

消防 OA 責任者は、OA 機器の導入、変更、廃棄等の作業において問題や事故が発生した場合、次の事項を行う。

（1）消防 OA 責任者は、問題や事故を認知した場合、直ちにその状況把握を行い、作業の継続または中断を判断する。

（2）消防 OA 責任者は、発生した問題や事故ついて、その原因を調査するとともにその対応策を検討する。

（3）消防 OA 責任者は、発生した問題や事故について、今後も発生する可能性があるものについては、対処方針を定めるとともに必要に応じて本要綱の見直しを行う。

第５章　ソフトウェアの導入、変更及び廃棄

1　対　象

消防 OA を構成するソフトウェアを対象とする。

2　ソフトウェアの導入、変更の企画及び調達

ソフトウェアの導入及び変更を計画するにあたり、次の事項を実施する。

（1）消防 OA 所管業務管理者は、関係法令及び業務の情勢と消防 OA との適応について留意し、消防 OA の実効性を確保する。

（2）消防 OA 所管業務管理者は、所管する業務に係る消防 OA での運営又は取扱い等において、該当サブシステムの改修等を要すると認められる場合、消防 OA 責任者へその旨を通知する。

（3）消防 OA 責任者は、消防 OA 管理者とともに消防 OA の改修について、システムの改修の妥当性、実効性、費用対効果等の総合的な考察を踏まえ、その実施について消防 OA 所管業務責任者と協議する。

また、必要に応じて、消防局情報化推進委員会設置要綱に規定する消防局情報化推進委員会において審議する。

（4）消防 OA 管理者は、ソフトウェアを調製するにあたり、仕様書に次の事項を盛り込む。

ア　情報セキュリティ対策事項

イ　保守体制、障害発生時の対応体制についての要求事項

ウ　調達ソフトウェアの製造元に対する要求事項（ISO9001、ISO15408、ISO27001 等の規格取得条件）

3　ソフトウェアの導入、変更及び廃棄前の検証

消防 OA 管理者は、ソフトウェアの導入、変更及び廃棄前に次の事項を実施する。

（1）疑似本番環境を備え、ソフトウェアが正常稼動すること及びシステムへの影響がないことを確認すること。

（2）導入及び変更にあたっては、ウィルス汚染について必ずチェックし、ウィルス感染していないことの確認をすること。

（3）不測の障害に備え、データのバックアップを行うとともにリカバリ方法を施すこと。

（4）検証する際の使用データは、原則、実データを使用しないこと。ただし、やむを得ず実

データでの検証が必要な場合は、そのデータから個人を特定できないように個人情報（特に氏名、住所等の属性情報）に係る部分を抹消又はマスキング処理により無意味なデータに変換し、検証後はデータを確実に廃棄すること。

4　作業、変更、廃棄及び事故対応

消防 OA 責任者は、ソフトウェアの導入、変更及び撤去を行う際の作業、廃棄及び事故対応について、「本要綱第 4 章」に準じて実施する。

また、消防 OA 管理者は、作業完了後に導入、変更及び撤去したソフトウェアについて、ソフトウェア台帳を更新する。

第６章　データ等の入出力情報管理

1　対　象

情報資産のうち、ホストサーバ内のハードディスクに格納されたデータ及び国、県等、外部組織が所管するシステムとネットワークを介して送受信したデータを対象とする（以下「消防 OA データ」と言う）。また、消防 OA データは、次のとおり区分する。

（1）システム運用関係データ

ア　システムを稼動させる基本プログラムデータ

イ　消防 OA プログラムデータ

ウ　入力、図面及び帳票様式データ

エ　電子計算処理記録データ

オ　操作記録データ

カ　システム運用に係るバックアップデータ

（2）業務運用関係データ

ア　入力、変更及び削除したデータ

イ　消防 OA からエクスポート（排出）した Excel、DocuWorks 等の電子データ

ウ　エクスポート後、加工したデータ

2　消防 OA データの保管

（1）保管場所の指定

消防 OA データは、消防 OA 利用責任者が指定した場所に保管するものとし、保管場所は常に整理整頓を行い、磁気媒体の紛失、遺失、混入が生じることがないようにしなければならない。

（2）電子媒体での保管

消防 OA 管理者及び消防 OA 利用管理者は、消防 OA データを磁気媒体で保管する場合、ファイル･DB 管理台帳を作成し、施錠可能なキャビネット等で厳重に保管する。この場合、システム運用関係データについては消防局総合庁舎第 2 電算室とする。

また、保管しているデータは、月に 1 回、ファイル・DB 管理台帳と照合し、消防 OA 責任者又は消防 OA 利用責任者の点検を受ける。

（3）保管期限

消防 OA 利用責任者は、消防 OA データの重要度と照らし、必要に応じて保管期限を定める。

（4）廃棄

廃棄する消防 OA データ又は保管期限を定めた消防 OA データで期限が経過したものについて、次の方法により廃棄または消去を行う。

ア　廃棄対象が紙の場合

・ シュレッダー等による裁断
・ 焼却処理

イ　廃棄対象が電子媒体の場合

・ 保存されたファイルの削除
・ データ消去ツールを使用したデータの完全消去
・ 電子媒体自体の裁断、焼却等、物理的破壊

ウ　廃棄を業者等に委託する場合

・ 委託業者等に引渡す前に、廃棄対象となる電子媒体及び紙の数量及びデータ内容（項目）の控え
・ 委託業者等からの廃棄証明の受領

3　消防 OA データの持ち出し

消防 OA データは、庁外へ持ち出してはならない。

ただし、庁外へ持ち出すことが業務に有用な場合、又は庁外へ持ち出さなければ業務上支障を来たす場合で、システム運用関係データについては消防 OA 責任者、業務運用関係データについては、消防 OA 所管業務管理者又は消防 OA 利用責任者が必要と認めた場合はこの限りでない。この場合、システム運用関係データの取扱いは、消防 OA 管理者とする。

4　システム運用関係データの引渡し等

システム運用関係データを本局職員以外の者へ引渡す又は授受する場合（以下「引渡し等」と言う。）について、次の事項を遵守する。

（1）データ送受書の作成

消防 OA 管理者は、システム運用関係データの引渡し等を行う場合、次の事項が記載されたデータ送受書を作成し、消防 OA 責任者の承認を得る。

・ 引渡し等の日
・ 使途及び相手方
・ データ内容（項目）
・ 容（数）量
・ 媒体の種類
・ 返還の有無及び期間
・ その他必要な事項

（2）引渡し等の場所

引渡し等の場所は、消防局総合庁舎第 2 電算室とする。

（3）送致等

消防 OA 管理者は、データ送受書の写しを相手側の情報管理を行う責任者へ提出するとともに「データ送受書」の内容と相違が無いことの確認印を得る。

また、庁舎外にデータ及び帳票を持ち出す場合は、施錠可能な鞄やケースに収容して移送

するものとする。

5　消防 OA データの紛失時等の対応

消防 OA 利用者等は、消防 OA データの紛失、盗難等の可能性が確認された場合、直ちに消防 OA 利用管理者及び消防 OA 利用責任者に報告する。

消防 OA 利用責任者は、状況把握を行いつつ消防 OA 責任者に報告する。

消防 OA 責任者は、紛失、盗難等の可能性が確認された情報の機密性区分が自治体機密性３の場合、統括情報セキュリティ管理者（消防局情報セキュリティマニュアル第１章２に基づき「庶務課長」）に報告する。

その他の機密性区分である場合は、事実関係を確認した後、業務への影響範囲及び要因の特定を行い、再発防止策の検討を行う。

第７章　建物及び関連設備管理

1　対 象

（1）　消防 OA サーバを設置している部屋、バックアップデータ及び消防 OA 管理用 PC が配置されている部屋（以下「消防 OA マシンエリア」という。）

（2）消防 OA 等を取扱う執務室（以下「消防 OA 執務エリア」という。）

2　消防 OA マシンエリアの入退室管理

消防 OA マシンエリアへ入室できる者は、消防 OA 責任者及び消防 OA 管理者とする。

ただし、消防 OA 責任者及び消防 OA 管理者がシステム運用上必要と認める行為を行う者（以下「入室許可者」という）はこの限りではない。この場合、消防 OA 責任者及び消防 OA 管理者は、次の手順により入退室管理を行う。

（1）消防 OA マシンエリアへ入室する者に入退室記録簿を起票させる。

（2）起票の確認後、入室許可を示す名札を手渡し、着用させる。

（3）入室許可者が作業を行うために持ち込む機材、OA 機器、可搬媒体等の確認を行い、情報セキュリティ上好ましくない物品については持ち込ませない。

（4）入室許可者の作業を監視し、情報セキュリティ上危険であると判断される行為があった場合には、直ちに作業の中止を求める。

（5）入室許可者の作業終了次第、入退室記録簿を起票させるとともに入室許可を示す名札を返納させ、マシン室から退室させる。

3　消防 OA 執務エリアの入退室管理

消防 OA 執務エリアへ入室できる者は、消防職員とする。ただし、消防 OA 利用責任者が業務上必要と認めた場合はこの限りではない。

4　消防 OA マシンエリア管理

消防 OA マシンエリアは施錠管理された部屋であることとし、必要に応じて取扱う情報が機密性、完全性及び可用性の区分の何れか一つでも２以上に該当するものは、施錠可能なラック等により管理を行う。

ラックのカギの管理は、消防 OA 責任者又は消防 OA 管理者とする。また、カギの使用機会は、機器及びソフトウェアの導入、変更及び廃棄作業等のラックを開放する必要がある場合に限定する。

5　消防 OA マシンエリアの環境管理

消防 OA 責任者は、次の事項について、消防 OA マシンエリアの環境管理を実施する。

（1）空調管理

OA 機器の稼動に適した空調環境（概ね、温度は 22～26℃、湿度は 40～46%）であることを確保する。

（2）電源管理

消防 OA マシンエリアの供給電力と設置している全ての OA 機器の電力使用量とを照らし、安定稼働に適した電力余力があることを確保する。

また、停電時における無停電装置等への切換えにあたっても電力不足によるシステム障害が発生しないような対策を講じる。

（3）耐震管理

OA 機器は、ボルトによる直止め、耐震ラック等により、地震発生時の倒壊の対処を講じることとする。また、電源ケーブル及び LAN ケーブル等は、切断等が発生しないように保護カバー設置する。

（4）消火設備等の管理

消防 OA マシンエリアの消火設備等について、適切に管理する。

（5）鍵の管理

業務エリアの全ての鍵が適切に施錠できることを適宜確認する。

（6）その他

原則、次の事項を禁止する。

- 消防 OA 以外の OA 機器、備品、その他付帯設備への触手
- 火気の使用
- 飲食
- 通信機器

第８章　アカウント管理

1　対　象

消防 OA のアカウントを対象とする。

2　管理者用 ID

（1）管理者用 ID

管理者用 ID とは、消防 OA を導入した際に各サーバに設定した特殊な ID を指し、消防 OA 責任者及び消防 OA 管理者（以下「管理 ID 資格者」と言う。）に割り当てる。

また、管理 ID 資格者は、必要な業務の管理上、管理 ID 資格者の代行として作業を行う必要があると認めた場合、一時的な ID を割り当てることができることとする。この場合、業務権限の割り当ては必要最小限に留めることとする。

（2）ID 管理

管理者用 ID の利用期間は１年とする。

この期限を越えて管理 ID 資格者の職にある場合は、新規の ID を割り当てるとともに従前の ID を抹消する。また、利用期間内であっても、異動等により管理 ID 資格者が変更し

た場合、その者の ID を抹消し、新規の ID を割り当てるものとする。

また、パスワードの有効期間は 3 箇月に設定し、その都度更新する。

（3）利用範囲

管理者用 ID の利用は、バッチジョブ実行管理、ソフトウェア管理、アカウント管理、障害対応、バックアップ等の必要な場合にのみに限定する。

3　利用者用 ID

（1）アクセス制御ポリシー

消防 OA 利用の適正なアクセス制御管理を行うため、消防 OA のメニュー、機能、登録・修正・削除・参照等の入力権限と役職、部署、担当業務等とを照らし、消防 OA 利用者等のシステム利用範囲（以下「消防 OA ロール」という。）について、アクセス制御に係るポリシーを定めて管理することとし、消防 OA 責任者の専管事項とする。

また、消防 OA ロールは、運用及び管理上変更が必要であると認められる場合に限り、期間を限定し例外措置を認めることとする。

（2）アクセス制御

ア　人事異動時の措置

消防 OA ロールは、消防 OA 利用者等に人事異動が生じた場合、発令日の午前 8 時 0 分をもって更新することを基本とする。また、これに係る設定作業は、消防 OA 管理者が行う。

イ　消防 OA ロールの例外措置

消防 OA ロールは、消防 OA 所管業務管理者が業務処理上の事由により、消防 OA ロールの変更が必要であると認められる場合で、消防 OA 責任者が承認した場合に限り、一次的に消防 OA を変更できることとする。この場合の手順は、次のとおりとする。

（ア）消防 OA 所管業務管理者は、利用資格申請書（様式 1）を消防 OA 責任者に申請する。

（イ）消防 OA 管理者は、アクセス制御ポリシーと照らし、消防 OA ロールの割当て変　更の妥当性を勘案し、割当て変更の可否を判断する。

（ウ）消防 OA ロールの割当て変更が認められた場合、その判断結果に基づき消防 OA 管理者が設定の変更作業を行う。

（エ）消防 OA 責任者は、利用資格申請書（様式 1）に作業結果を補記するとともに、その写しを消防 OA 所管業務管理者へ送付するとともに、利用資格申請書（様式 1）を保管する。

4　その他の ID の管理

オペレーティングシステム及びアプリケーションに登録されている共有用、テスト用の ID は、消防 OA 管理者が管理することとし、不要な ID は削除もしくは権限の取り消しを行う。

5　定期的なアカウント管理

消防 OA 管理者は、次の事項についてアカント管理作業を行い消防 OA 責任者へ報告する。

（1）人事異動発令時

ア　システムに登録されている全ての ID について、アカウント管理台帳を作成する。

イ　利用者 ID については、利用資格申請書（様式 1）とアカウント管理台帳とを照合する。

この場合、利用資格申請書（様式 1）のない ID、もしくは不適切な設定となっている ID

については、利用資格停止を行う。

（2）年度末

ア　アカウントは ID 別にログイン回数一覧を作成する。

イ　ログイン回数より、次に該当するケースを抽出する。

・ 年間を通じてログインを行った形跡のない ID

・ 他の ID と比較して特出した利用のある ID

・ 勤務時間外等に過度なログイン形跡が確認された ID

第９章　委託先管理

１　委託先の選定

（1）委託先の選定

消防 OA 責任者は、消防 OA が保有する情報及び消防 OA の開発、運用、保守及びデータ処理に係る業務の一部または全部を外部に委託する場合、情報漏えい等を防止するため、次の事項を実施するとともに別に定められた委託先選定に係る手続等を遵守する。

ア　委託作業で取扱う情報及び消防 OA について、「本要綱第３章 情報資産の分類及び管理」に従って、評価を行うこと。

イ　機密性区分の評価結果に基づき、機密性を確実に保持するための対策を委託要件として記述すること。

（2）委託先選定の基準

消防 OA 責任者は、情報資産の分類を考慮して、次の基準により委託先を選定する。

ア　委託先における情報管理に係る基本方針、実施体制及び取扱規程の整備状況

イ　委託先における情報の取扱状況の点検及び監査に係る規程の整備状況

ウ　委託先における外部委託に係る規程の整備状況

エ　実績等に基づく委託先の情報管理上の社会的信用度

オ　委託先の経営の健全性

カ　委託先の技術及び対応力

キ　公的認証の取得状況（プライバシーマーク、ISMS 等）

プライバシーマークとは、概して日本工業規格「JIS Q 15001 個人情報保護マネジメントシステムの要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を財団法人日本情報処理開発協会（JIPDEC）が認定し、その旨を示したシンボルマークのこと。
ISMS とは、情報セキュリティマネジメントシステムのことで、概して個別の問題毎に対する技術対策の他に組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、適切な資源配分を行いシステムを運用することで、組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し又は改善すること。

（3）委託契約

消防 OA 責任者は、次の事項を契約書類に含めるとともに別に定められた委託契約に　係る手続に従う。

ア　委託作業項目

イ　責任範囲、連絡体制

ウ　提供されるサービスに関する履行基準（サービスレベル）
エ　再委託禁止
オ　情報資産等の取扱い
カ　立ち入り検査等の委託契約遵守状況の確認を求める行為
キ　作業指示の証拠となる書類の種類と保管責任
ク　作業進捗に係る定期報告の方法と報告内容
ケ　システム障害及び災害発生時の対応、復旧方法
コ　その他の関連する管理義務

（4）誓約書

消防 OA 責任者は、自治体機密性３に相当する委託業務を行う業者からは、作業者の一覧が記載された機密保持に係る誓約書を受領する。

2　委託業務の点検

（1）委託契約事項の遵守状況確認

消防 OA 責任者は、外部委託先からの定期報告により、委託契約事項が遵守されていることを確認する。

（2）事故発生時の原因調査

消防 OA 責任者は、委託作業に係る情報の漏えい・紛失・毀損・消失等の情報セキュリティに関する事故が発生した場合、その原因を調査する。

この場合、原因調査の結果に基づき、次の対策を行う。

ア　委託先に対する再発防止策の実施要請とその内容を含んだ文書
イ　損害賠償等の請求
ウ　委託先管理体制の強化

第１０章　システム障害対応

1　システム障害発生時の対応

（1）システム障害の備え

消防 OA 責任者は、システム障害の発生（システムの停止、異常作動等のシステム要因事項のみならず、システム利用時における情報漏えい、ウィルス感染等の 2 次的な要因事項も含む）に備え、次の事項について連絡体制及び対処手順をあらかじめ定める。

ア　消防 OA のプログラム不備、運用作業上のミス等による消防 OA の誤作動、停止等
イ　電源異常、天災による機器損壊等によるシステムの停止または故障
ウ　消防 OA 障害対策後の動作確認

（2）システム障害発生時の対応

消防 OA 利用者等は、システム障害が発生したと思われる場合、原因の究明に必要となる現状の情報を可能な範囲で保存するとともに速やかに消防 OA ヘルプデスクへ連絡する。また、必要に応じて消防 OA 利用管理者に報告する。

消防 OA 利用管理者は、消防 OA 利用責任者に報告する。

消防 OA ヘルプデスクは、消防 OA 管理者に報告するとともにシステム保守委託業者と協力して障害の原因究明及び復旧作業を実施する。

消防 OA 管理者は、システム保守委託業者から次の事項を聴取し、消防 OA 責任者に状況を報告するとともに必要に応じて消防 OA 利用者等へ連絡する。

ア　システム障害の発生原因

イ　復旧の方策

ウ　復旧に要する時間、復旧予定時間及びシステム利用開始予定時間

エ　復旧にあたるバックアップデータの使用要否

※「別図」参照

2　大規模なシステム障害の判断と対応

（1）障害規模の判断

消防 OA 責任者は、大規模なシステム障害に発展する懸念があるものとして、次の基準により判断する。

ア　可用性区分において、自治体可用性２と判定される消防 OA

イ　可用性区分にて自治体可用性１と判定されている消防 OA のうち、障害の影響範囲が庁内の広域に渡るシステム

ウ　障害復旧に必要とされる時間が 24 時間を超えるもの

（2）大規模なシステム障害の対応

消防 OA 責任者は、大規模なシステム障害が発生したと判断した場合、その状況を「本要綱第 16 章 災害復旧」に基づき、統括情報セキュリティ管理者（消防局情報セキュリティマニュアル第１章２に基づき「庶務課長」）に報告し、障害の復旧に対応する。

3　システム障害復旧後の事後作業

消防 OA 責任者は、システム障害記録書を作成するとともに再発防止処置を検討し、必要な対策を実施する。

第１１章　ウィルス対策

1　ウィルス対策ソフトの導入

（1）主計算機のウィルス対策ソフト

消防 OA 責任者は、サーバ等の主計算機に対し、次の要件を満たすウィルス対策ソフトを導入する。

ア　消防 OA 機器に対してコピーされた全てのファイルからウィルスを検出する機能

イ　１日１回定期的に消防 OA 機器に格納される全てのファイルからウィルスを検出する機能

ウ　読込または書込を予定している可搬媒体に保存される全てのファイルからウィルスを検出する機能

エ　検出されたウィルスを駆除または隔離する機能

オ　ウィルスが検出された場合、管理者に通知する機能

カ　検出されたウィルスの出所の追跡に必要な情報をログとして記録する機能

キ　ウィルス対策ソフト及びパターンファイルを自動更新する機能

2　主計算機のウィルス対策管理

消防 OA 責任者は、ウィルス対策管理を徹底するため、次の事項を徹底させる。

（1）消防 OA 責任者は、消防 OA 利用者等に対し、ウィルス感染時の連絡及び報告体制を周知しなければならない。

（2）消防 OA 責任者は、ウィルス感染時の症状について調査し、消防 OA 利用者等に周知しなければならない。

（3）ウィルス感染が発覚した情報機器は、本市ネットワークから切り離し、ウィルスの感染拡大を防止する。

3　主計算機の定期的なログの収集

消防 OA 責任者は、月 1 回主計算機からウィルス検出ログを収集し、ウィルス対策ソフトが有効に機能していることを確認する。

また、ウィルスログが収集された場合は、ウィルスの種類等から進入経路を特定するとともに対応策を検討する。

4　大規模なウィルス感染時の対応

（1）ウィルスの検出

消防 OA 責任者は、ウィルスが検出された場合、次の事項について、確認する。

ア　同一のネットワークセグメントで複数のウィルスが検出されていないか。

イ　異なるネットワークセグメントで同一種のウィルスが検出されていないか。

（2）ウィルス感染の連絡

消防 OA 責任者は、全庁的なウィルス感染危険があると判断される場合、ウィルスが検出された消防 OA とネットワーク接続している全ての消防 OA を所管する部署に対して、次の事項を連絡及び調整する。

ア　ウィルス感染発生状況の確認

イ　ネットワーク接続の一時停止の要否

（3）ウィルス感染の報告

消防 OA 責任者は、ウィルス感染の状況を「本要綱第 16 章 災害復旧」に基づき、統括情報セキュリティ管理者(消防局情報セキュリティマニュアル第１章２に基づき「庶務課長」)へ報告する。

（4）消防 OA 責任者の対応

消防 OA 責任者は、総務企画局デジタル化施策推進室の協力を得て、次の対応を行わなければならない。

ア　ウィルスが検出されたネットワークセグメントを特定すること。

イ　特定されたネットワークセグメント内の端末機をネートワークから切り離し、感染防止措置を行うこと。

ウ　特定されたネットワークセグメントの実地調査を行い、ウィルス発生源を特定すること。

エ　ウィルス対応策を実施すること。

オ　ウィルス発生に関する原因と対応策を取りまとめ、消防局情報セキュリティマニュアルに基づき、統括情報セキュリティ管理者（消防局情報セキュリティマニュアル第１章２に基づき「庶務課長」）に報告する。

5　ウィルス感染における事後処理

（1）改ざん及び破壊状況の調査

消防 OA 責任者は、検出されたウィルスの情報に基づき、データ及び消防 OA に対して、改ざん及び破壊がないか調査を行う。

データ及び消防 OA の改ざん及び破壊が確認された場合は、「本要綱第 10 章 システム障害対応」にしたがい、復旧を行う。

（2）データ漏えい状況の調査

消防 OA 責任者は、検出されたウィルスの情報に基づき、バックドア機能（不正侵入したネットワークに対し再侵入できるように設けられた侵入口）による外部への情報漏えいがないか調査を行う。

情報漏えいが確認された場合は、情報漏えいしたデータファイルを特定し、ファイル・DB 管理台帳にある機密性区分を確認し、被害状況を消防局情報セキュリティマニュアルに基づき統括情報セキュリティ管理者（消防局情報セキュリティマニュアル第１章２に基づき「庶務課長」）に報告する。

（3）見直し

消防 OA 責任者は、本要綱が有効に機能していることを確認するとともに、必要に応じて、本要綱の見直しを行う。

第１２章　不正アクセス管理

1　不正アクセス回避のための措置と対応

（1）アクセスログの確認

消防 OA 責任者は、不正アクセスを回避するため、次の事項について、適宜ログを確認する。

ア　連続したアクセス（認証）の失敗

イ　大量のデータ送信

ウ　特権ユーザに割り当てられた処理の試行

エ　連続したポートスキャン

（2）不正アクセスの兆候があった場合の対応

消防 OA 責任者は、不正アクセスの兆候があると判断される行為が検知された場合、係る全てのログを保存するとともにその対応として一時的にネットワークの停止を実施するか否かの判断を行う。また、必要に応じて、不正アクセス対策の強化を図る。

2　不正アクセスの痕跡確認と対応

（1）不正アクセスの痕跡確認

消防 OA 責任者は、不正アクセスの痕跡を把握するため、次の事項について、適宜ログを確認する。

ア　通常では使用が許可されないユーザ ID によるログイン

イ　通常では使用が許可されないプロトコル及びサービスの起動

ウ　その他、通常では検知されることのないログ内容

（2）不正アクセスへの対応

消防 OA 責任者は、不正アクセスの痕跡を発見した場合、当該ネットワークセグメントに

接続される機器について、次の事項の確認を行う。

ア　データの改ざん及び破壊の可能性

イ　消防 OA の改ざん及び破壊の可能性

ウ　データの持ち出しの可能性

（3）不正アクセスに係る関係書類の作成

消防 OA 責任者は、係る全てのログの保存、データの改ざん・破壊・持ち出し状況等必要な項目を記載した関係書類を作成する。

（4）不正アクセスに係る被害の報告

消防 OA 責任者は、ファイル・ＤＢ管理台帳と照合して、持ち出されたデータの機密性区分を確認し、被害状況を消防局情報セキュリティマニュアルに基づき統括情報セキュリティ管理者（消防局情報セキュリティマニュアル第１章２に基づき「庶務課長」）に報告する。

（5）再侵入防止措置

消防 OA 責任者は、不正アクセスの原因を調査し、再侵入を防止するための処置を行う。また、再侵入防止措置までの間、物理的にネットワークを切り離しておく。

3　不正アクセスにおける事後処理

消防 OA 責任者は、ファイアウォールの確認を実施するとともに、必要に応じた改善を実施する。

第１３章　システム運用

1　ジョブスケジュールの作成

（1）ジョブスケジュールの作成

消防 OA 責任者は、次のジョブスケジュールを作成する。

ア　年間スケジュール表

イ　当日スケジュール表

（2）連絡及び調整

消防 OA 責任者は、関連部署又は保守業者等（以下「関連部署等」という。）と連携して業務を実施する必要がある場合、ジョブスケジュールについて調整を行う。

2　オペレーション指示書等の作成

（1）オペレーション指示書等の作成

消防 OA 責任者は、当日スケジュール表にしたがい、オペレーション指示書を作成する。また、作業を行うにあたり、可搬媒体や帳票等の入出力情報が伴う場合は、バッチ処理入出力情報一覧を作成する。

（2）オペレーションの実施

オペレーションは消防 OA 管理者が実施するものとし、消防 OA 管理者はオペレーション指示書及びバッチ処理入出力情報一覧にしたがい、バッチジョブなどのオペレーションを行う。

オペレーションを実施している際、オペレーション指示書に定めのない状況が発生した場合には、消防 OA 責任者に報告し、指示を受ける。

3　オペレーションの確認

（1）オペレーションの確認

消防 OA 管理者は、オペレーション指示書に基づき、作業内容が確実かつ適切にオペレーションが実施されたことを確認する。

（2）オペレーションミスが確認された場合

消防 OA 責任者は、作業漏れ等のオペレーションミスが確認された場合、必要に応じて、関連部署等と連絡及び調整の上、事後対応について指示を行う。

（3）特例処理の実施及び確認

消防 OA 管理者は、ジョブスケジュールに無い特例処理を行う必要が生じた場合、消防 OA 責任者に報告するとともにオペレーション指示書の備考欄に該当事項を起票する。

第１４章　システム開発及び保守

１　システム開発（改修等含む）

（1）システム開発の企画

消防 OA 管理者は、社会の情勢と消防 OA との適応について留意するとともに、消防 OA の実効性を確保するため、必要に応じて新規システム開発を企画する。

システム開発の立案にあたっては、次の事項について精査する。

ア　システムで取扱う情報を明らかにし、本要綱第３章により、情報の機密性、完全性及び可用性を評価する。

イ　評価結果に基づき、次に掲げる情報セキュリティ要件を明らかにする。

- 消防 OA の運用及び管理に関する要件
- 消防 OA の設置場所に関する要件
- バックアップ方式、機器の二重化等の障害対策に関する要件
- 操作者等の認証方式、アクセス制御方式等の要件
- 消防 OA の操作及び利用に関する教育研修に関する要件
- 準拠すべき法律、制度に関する要件

ウ　自治体機密性３の情報については、暗号化技術を適用する。

（2）開発業者の調達

消防 OA 責任者は、開発業者を調達するにあたり、次の事項を実施する。

ア　別に定められた調達に係る手続に従うとともに、調達仕様書に次の事項を盛り込む。

- 企画時に定めた情報セキュリティ要件
- 保守体制及び障害発生時の対応体制についての要求事項
- 消防 OA 開発における情報セキュリティ上、有用な規格取得条件

イ　必要に応じて、調達仕様書の内容について、総務企画局デジタル化施策推進室と調整を行う。

ウ　機器の調達及びソフトウェアの調達を行う場合は、本実施要綱第４章及び第５章を遵守する。

（3）システム開発

消防 OA 責任者は、設計、開発、テスト（以降「システム開発」という。）を行うにあたり、業務上必要な機能とともに、次の情報セキュリティ機能について、機密性、完全性及び

可用性に関する評価結果に基づき、実装する。また、情報セキュリティ対策上の機能の実現において、本市情報基盤を活用する場合は総務企画局デジタル化施策推進室と調整を行う。

- 認証機能及びアクセス制御機能
- プログラム改ざん機能
- 不正アクセス監視機能
- 端末識別機能
- ログ取得機能
- バックアップ取得機能及びリカバリ機能
- なりすまし防止機能

3　システム保守

（1）保守要件検討

消防 OA 責任者は、次の事項に基づき、システム保守要件の検討を実施する。

ア　システム保守を行うことによる既存機能への影響を十分に分析する。

イ　システム保守を行うことにより、他システム（他部署が所管するシステム）に提供しているデータに影響がある場合、その影響について調整を図る。

（2）保守プログラム開発

消防 OA 責任者は、次の事項により、保守プログラム開発を実施する。

ア　プログラム変更内容を記録したドキュメントとして、「プログラム変更仕様書」を作成し、その内容に基づき、開発を進める。

イ　保守プログラムのテストは、本番環境と同様のソフトウェア、プログラムが稼動しているテスト環境にて実施し、保守対象プログラム以外に影響が発生しないことを確認する。

ウ　保守プログラムのテストには、ダミーデータを使用し、他システムへ影響が発生しないことを確認する。

エ　保守プログラムの本番移行については、本要綱第５章にしたがい実施する。

4　その他

（1）開発環境の管理

消防 OA 責任者は、次の事項により、システム開発環境の管理を実施する。

ア　開発用機器は、本番用機器とは別に用意する。ただし、ソフトウェアの設定によって、主計算機を別にした場合と同等の安全対策が実現できる場合は、同一の機器の使用を許可する。

イ　開発用機器を本市既存ネットワークへ接続することを禁止する。

ウ　本番環境で使用するデータを開発の用途で使用することを禁止する。

エ　開発用機器を本番環境に移行する場合、次の事項により実施する。

- システムの稼動に不要なライブラリ、テストプログラム、テストデータ、開発ツールは、削除する。
- システム開発に使用した開発者用ＩＤ及びテスト用ユーザＩＤは、抹消する。

（2）開発ドキュメント管理

消防 OA 責任者は、次の事項により開発ドキュメントの管理を実施する。

ア　開発ドキュメントは、消防局総合庁舎第２電算室に保管し、システムドキュメント台帳

を作成する。

イ　システム改修を行った場合、プログラム仕様変更の履歴について、システムドキュメント台帳に記録する。

5　情報収集

（1）情報収集

消防 OA 責任者は、消防 OA が使用しているソフトウェア等について、次の情報の収集に努める。

ア　セキュリティホール、バグ等の情報

イ　パッチプログラム等の配布に関する情報

ウ　保守停止に関する情報

（2）対応の検討

消防 OA 責任者は、収集した情報について、システム保守業者を交えて対応策の必要性及び対応を実施しない場合のリスクを検討し、システム保守作業に反映する。

第１５章　ユーザ教育

1　教育の主旨

消防 OA 責任者、消防 OA 所管業務管理者及び消防 OA 利用責任者は、消防 OA 利用者等に対し、情報を適切に管理する義務（情報保全義務）を遵守させ、情報及び消防 OA の適切な操作及び取扱いにおける事故や不正な行為の発生を防止するため、適宜実施する。

2　教育の計画

（1）計画の内容

ア　教育内容

イ　教育方法

ウ　教育対象部署及び対象者

エ　実施スケジュール

（2）教育計画の策定にあたっての留意点

ア　教育内容

・　実施手順等の理解を深める情報

・ 他自治体や企業等で発生している情報セキュリティに関する事故のうち、情報利用者に対して周知する必要のある情報

・ その他、消防 OA 情報利用者等に対して周知する必要のある情報

イ　教育方法

教育内容に基づき、最も短期間かつ効果的な教育方法とする。

（3）教育対象部署及び対象者

教育内容に基づき、最も効果的な対象部署及び対象者を選定する。

第１６章　災害復旧

1　災害発生時の対応

（１）災害発生の報告

消防 OA 責任者は、市民生活や行政運営に影響を及ぼし、全庁的な対応が必要とされる次の事象が発生した場合、速やかに災害発生の事実とその状況を消防局情報セキュリティマニュアルに基づき統括情報セキュリティ管理者（消防局情報セキュリティマニュアル第１章２に基づき「庶務課長」）に報告する。

ア　大規模なシステム障害による消防 OA の停止

イ　大規模なウィルス感染

ウ　地震、火災等による消防 OA の停止

２　災害復旧の対応

（１）災害復旧の対応

消防 OA 責任者は、消防局情報セキュリティマニュアルに基づき統括情報セキュリティ管理者（消防局情報セキュリティマニュアル第１章２に基づき「庶務課長」）の指示を受け、次の事項について必要な対応を講じる。

ア　災害復旧中の業務運用方法に対する質疑応答対応

イ　外部機関や市民からの問合せ対応

ウ　災害復旧作業完了時の稼動確認項目の検討

エ　災害復旧作業状況の管理

オ　災害復旧作業上にて発生する課題、問題に対する対応指示

（２）災害復旧状況の確認

消防 OA 責任者は、災害復旧作業の完了した段階で、消防 OA 所管業務管理者に稼動確認試験を依頼する。

消防 OA 所管業務管理者は、稼動確認試験を実施後、消防 OA を利用した業務再開可否を判断するとともに、消防 OA 責任者へその旨を通知する。

（３）業務再開の報告

消防 OA 責任者は、消防 OA 所管業務管理者の通知を踏まえ、業務再開が可能であると判断した場合に消防局情報セキュリティマニュアルに基づき統括情報セキュリティ管理者（消防局情報セキュリティマニュアル第１章２に基づき「庶務課長」）に業務再開可能の報告を行う。

（４）業務再開

消防 OA 責任者は、消防局情報セキュリティマニュアルに基づき統括情報セキュリティ管理者（消防局情報セキュリティマニュアル第１章２に基づき「庶務課長」）の指示を受けて、業務を再開する。

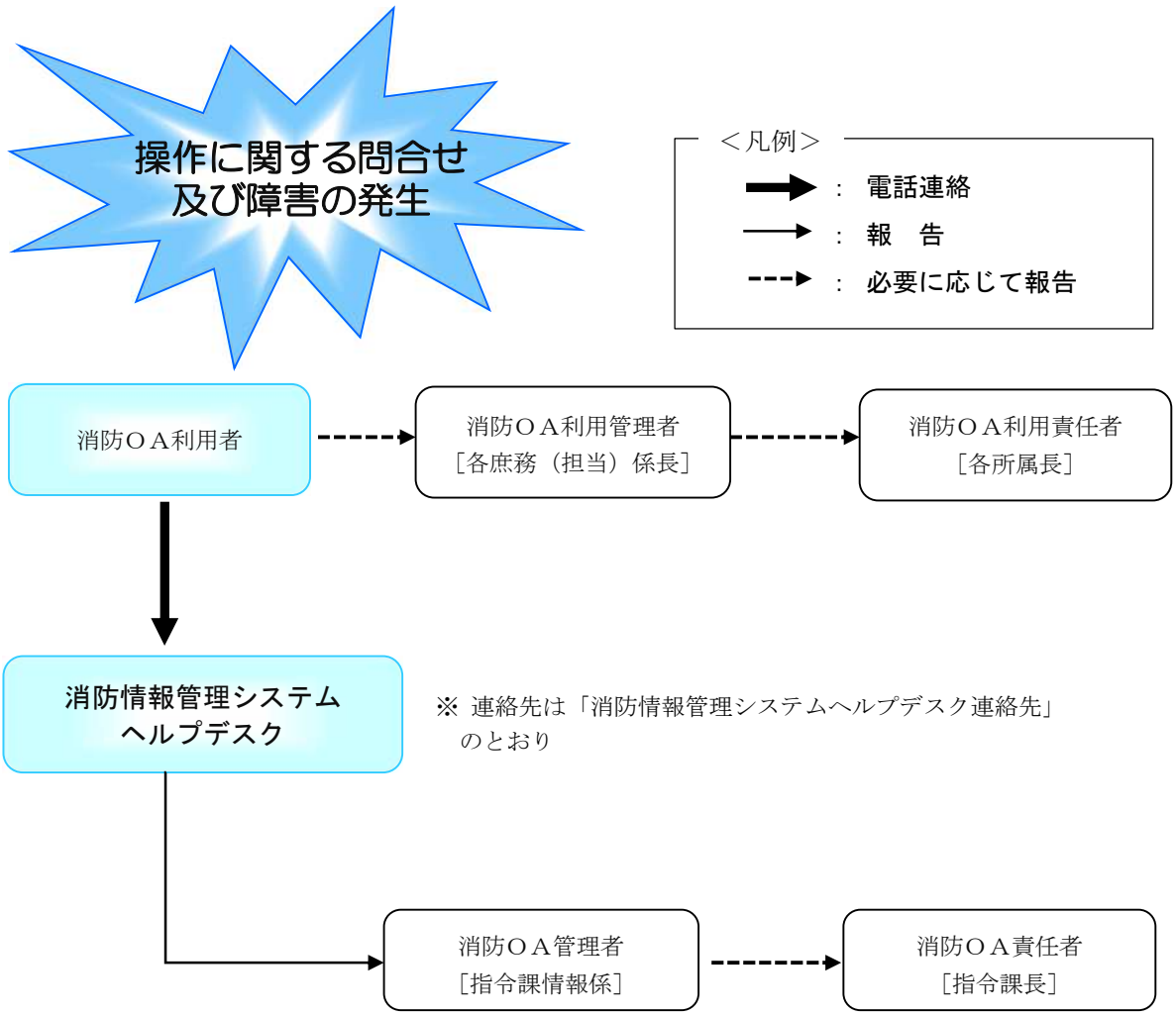
第１７章　点検による見直しと改善

消防 OA 責任者は、消防 OA の利用、運用保守、情報セキュリティ及びシステム開発に関し、適正な運用及び管理を図るため、必要に応じて本要綱の改正を検討する。

改正履歴

施行年月日	文書番号
平成 19 年 12 月 28 日	19 川消庶第 2339 号
平成 20 年 10 月 20 日	20 川消庶第 1591 号
平成 21 年 4 月 1 日	21 川消指第 199 号
平成 27 年 5 月 25 日	27 川消指第 370 号
令和 07 年 12 月 8 日	7 川消指第 1290 号
令和 08 年 11 月 13 日	8 川消指第 1312 号

別　図　（第 10 章　システム障害対応）



【 消防情報管理システムヘルプデスク連絡先 】

取 扱 業 務	開 設 時 間	連 絡 先
各サブシステムの 操作に関すること	（平日） 9：00 ～ 17：00	０８０－２５６３－０１１９ （川崎消防ヘルプデスク・日立 SRC）
障害に関すること	24 時間	

様式１

○○川消○第○○○○号
令和○○年○○月○○日

消防ＯＡ責任者　様
（指令課長）

消防ＯＡ所管業務管理者
（該当所属長）

消防OA利用資格申請書

≪ 消防OAロール変更該当者 ≫

所　　属		階　　級	
職員コード		氏　　名	

≪ 利用（希望）開始日等 ≫

利用開始	年　　月　　日	利用終了	年　　月　　日

≪ 変更申請事項 ≫

利用サブシステム名称	
利用業務名称	

≪ 理　由 ≫

≪ その他特記事項 ≫

≪ 登録結果 ≫

処理日付	年　　月　　日	登録実施者	
ロール名称	変更前	変更後	
個別権限設置事項	変更前	変更後	

≪ 連絡事項 ≫

拒否事由	○アクセスポリシー不適合　　○その他

※エクセルファイルで消防ＯＡ責任者に申請