小牧市医療・介護ネットワーク

「こまきつながるくん連絡帳」

セキュリティポリシー

第１章　総則

（目的）

第１条　このセキュリティポリシーは、小牧市医療・介護ネットワーク「こまきつながるくん連絡帳」（以下「こまきつながるくん連絡帳」という。）の管理運営に関し、そのシステムの運用・管理に関する詳細を規定し、こまきつながるくん連絡帳の安定稼働と効果的な利用支援を目的とする。

（適用範囲）

第２条　このセキュリティポリシーは、こまきつながるくん連絡帳を構成するクラウド設備の管理業務（以下「システム管理業務」という。）並びにこのシステムの利用者（以下「利用者」という。）支援業務及び情報管理業務（以下「システム運用業務」という。）に適用する。

（管理体制）

第３条　こまきつながるくん連絡帳の運用・管理に係る委託契約事業者（以下「契約事業者」という。）は、前条のシステム管理業務及びシステム運用業務に関して責任を持つ「運用管理責任者」を選任するものとする。

２　運用管理責任者は、その配下にシステム管理業務の実施管理を行う「システム管理者」、システム運用業務の実施管理を行う「システム運用者」及びラック等の鍵管理を行う「鍵管理者」を任命するものとする。

３　契約事業者は、前２項により定めた管理体制を小牧市に届出するものとする。

（教育・訓練）

第４条　運用管理責任者は、システム運用業務又はシステム管理業務に携わる要員に対し、次の各号に掲げる事項その他必要な事項について、十分な教育・訓練を実施するものとする。

(1) 業務目的以外でのこまきつながるくん連絡帳へのアクセスを禁止すること。

(2) 自己の保有するパスワードに関し、秘密保持に努めること。

(3) 使用する端末や記録媒体について、第三者に使用されること又は許可なく情報を閲覧されることがないように、離席時には画面ロックする等適切な措置を施すこと。

(4) 異動・退職等により業務を離れる場合は、知り得た情報を秘匿すること。

(5) システムに関する障害、事故等を発見した場合は、速やかに小牧市に報告し、適切な措置を講ずること。

（管理責任）

第５条　情報は、当該情報を作成した利用施設の施設管理者が管理責任を有する。

２　情報の管理及び取扱いは、次の各号のとおりとする。

(1) 情報の利用目的に反する複製や、送付・送信等を行ってはならない。

(2) 業務上必要のない情報を作成してはならない。

(3) 情報の紛失や流出等を防止しなければならない。

(4) 業務以外の目的に情報資産を利用してはならない。

（管理規程などの提示）

第６条　運用管理責任者は、システム管理業務及びシステム運用業務に関係する社内管理規程及び手順を小牧市に提示し、承認を得るものとする。

（準拠する法令・ガイドライン等）

第７条　システム管理業務及びシステム運用業務について、運用管理責任者は、次の各号に掲げる法令及びガイドライン等を遵守するとともに、準拠度チェックリストを小牧市に提示し、承認を得るものとする。

(1) 小牧市が保有する情報資産の機密性、完全性及び可用性（注）を維持するための情報セキュリティ対策を整備するため小牧市情報セキュリティポリシー（平成１５年１０月２１日策定、平成２８年 ３月 ７日改定）

(2) 個人情報の保護に関する法律（平成１５年５月３０日法律第５７号）

(3) ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン１．１版（総務省平成２２年１２月）

(4) ASP・SaaS における情報セキュリティ対策ガイドライン（総務省平成２０年１月３０日）

(5) 医療情報を受託管理する情報処理事業者向けガイドライン（平成２０年７月２４日経済産業省）

(6) クラウドサービス利用のための情報セキュリティマネジメントガイドライン（経済産業省平成２３年４月１日）

２　前項各号のガイドラインの遵守は、次のガイドラインに記述された趣旨を理解したうえで実施する。

(1) 医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン（厚生労働省平成１６年１２月２４日通達、平成２２年９月１７日改正）

(2) 医療情報システムの安全管理に関するガイドライン第４．２版（厚生労働省平成２５年１０月）

（資産台帳の整備、管理）

第８条　契約事業者は、こまきつながるくん連絡帳を構成するクラウド設備に関係する情報資産を確実に保護し、その情報セキュリティ（機密性、完全性及び可用性（注）。以下同じ。）を確保することを目的に、そのクラウド設備を構成するハードウェア、ソフトウェアについて資産台帳を整備管理するものとする。

（注）国際標準化機構（ＩＳＯ）が定めるもの（ＩＳＯ４９８－２：１９８９）

機密性（confidentiality）：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること

完全性（integrite）：情報及び処理の方法の正確さ及び完全である状態を安全防護すること

可用性（availability）：許可された利用者が必要な時に情報にアクセスできることを確実にすること

第２章　物理的及び環境的セキュリティ

（クラウド設備の設置場所）

第９条　こまきつながるくん連絡帳を構成するクラウド設備は、医療情報等を処理保管する重要機器が含まれることから、次の各号に掲げる条件を満たすセキュリティ区画に設置するものとする。

(1) 一般的な事務室との共用又は隣接を避けていること。

(2) 管理区域は原則として地階又は１階に設けず、危険物保管場所、火気施設、水道設備等のリスクの大きい場所から離れていること。

(3) 設置場所の表示は最小限にとどめていること。

(4) 出入り口は原則１か所とし、施錠設備を設けていること。

(5) 窓を設けることを避け、設ける場合は強化ガラスの使用などの対策をしていること。

(6) 防犯カメラ、侵入報知器等の防犯設備を設置していること。

(7) コピー機、ＦＡＸなど情報の複写、送信のための設備を設置していないこと。

(8) 外部の施設を利用する場合は、他組織の機器から隔離し、施錠できるようにしていること。

(9) 管理区域内の機器、記録媒体等に影響を与えない消防用設備を設置すること。

（設置場所の運用）

第１０条　センター設置場所の運用は、次の各号のとおりとする。

(1) クラウド設備設置室及びこまきつながるくん連絡帳用に隔離されたスペースは、不在時には施錠すること。

(2) クラウド設備設置室への入室は、認証装置等により特定のものに制限すること。

(3) 入室制限を受けている者の入室に対しては、運用管理責任者が許可し、入室可能な者が同伴すること。

(4) 入退室履歴を記録すること。

(5) クラウド設備設置室内では許可なしに撮影、録音をしないこと。

(6) クラウド設備設置室内には、必要なもの以外を置かないこと。

(7) こまきつながるくん連絡帳用に隔離されたスペースの鍵は鍵管理者が管理すること。

（電源設備の点検）

第１１条　システム管理者は、電源設備の点検作業のため、年１回１日間（２４時間）商用電源供給とするものとする。なお、システム管理者は予め点検をしようとする３か月前までに点検日程等について小牧市と協議するものとする。

第３章　システム運用業務とそのセキュリティ

（システム運用業務）

第１２条　こまきつながるくん連絡帳に関するシステム運用業務については、利用者等の的確な管理と利便性の向上を図ることを目的とし、次の各号に掲げる業務をシステム運用業務とする。（図１）

(1) ユーザー管理　利用者識別番号（以下「ユーザーＩＤ」という。）及び暗証番号（以下「パスワード」という。）の付与とその登録・変更・削除

(2) ポータル管理　ポータルサイト情報の登録・変更・削除

(3) 本番データの臨時使用　こまきつながるくん連絡帳の本番データの提供

(4) 問い合わせ対応　利用者等の問い合わせ対応

(5)その他　システム運用に関する事項

（ユーザー管理）

第１３条　小牧市は、施設管理者からの依頼により利用者のユーザーＩＤ利用停止並びに新たなユーザーＩＤ及びパスワードの付与をする場合、次の各号に示すとおり実施する。

(1) 利用者の追加に際しては、ユーザーＩＤ及びパスワードのコード要件に適合するユーザ

ーＩＤ及びパスワードの決定及び登録を行い、そのユーザーＩＤ及びパスワードを、施設管理者に封書で知らせるものとする。

(2) 利用者の削除に際しては、その依頼に対して速やかに削除するものとする。

(3) 利用者の変更に際しては、前２号の処理を行うものとする。

(4) 利用者に関する付随情報については、当該利用者の本人確認を確実に実施したうえで、依頼に応じて変更するものとする。

（ポータル管理）

第１４条　システム運用者は、小牧市からポータルサイト情報の変更要求があったとき、次の各号に示すとおり実施する。

(1) ポータルサイト中に登録されている情報構成の変更など表示画面の設計を要する場合は、その設計について、小牧市と協議するものとする。

(2) 表示画面の設計が不要で内容変更のみの場合は、その要求に対し、速やかに対応するものとする。

(3) 新規追加情報又は更新情報については、ポータルサイトトップページで新規情報又は既存情報の更新が明記されるよう併せて変更するものとする。

（データの臨時使用）

第１５条　データを臨時使用する者は、データ使用許可申請書（様式第１）を小牧市に提出しなければならない。

２　小牧市は、前項の申請書を受理したときは、その内容について適正かどうか審査を行い、データ使用許可決定・却下通知書（様式第２）により、申請者に決定又は却下を通知するものとする。

３　システム運用者は、前項のデータ使用許可決定通知書が提示されたとき、次の各号に示すとおり実施する。

(1) 使用するデータに個人情報が含まれる場合は、個人を特定できないように加工し出力する。

(2) 提供にあたって集計などの情報処理が必要なときは、その処理を行う。

(3) 提供方法は、紙又はデータとし、その送付先は当該申請者とする。

（問い合わせ対応）

第１６条　契約事業者は、月曜日から金曜日（祝祭日と、１２月２９日から１月３日までは除く）までの午前９時から午後５時まで、利用者からの次の各号に掲げる内容に対応できる体

制（ヘルプデスク）を整えるものとする。

(1) システム利用開始時の問い合わせ

(2) システム仕様に関する問い合わせ

(3) システム概要に関する問い合わせ

(4) システム利用に関する問い合わせ

(5) 参加医療施設等の案内

(6) ユーザー情報の問い合わせ

(7) 障害対応・復旧時間の問い合わせなど

なお、システム運用者は、それぞれの問い合わせとその対応について記録するものとする。

第４章　システム管理業務とそのセキュリティ

（システム管理業務）

第１７条　こまきつながるくん連絡帳に関するシステム管理業務については、こまきつながるくん連絡帳を構成するクラウド設備システムに関係する情報資産を確実に保護し、その情報セキュリティ（機密性、完全性及び可用性）を確保することを目的とし、次の各号に掲げる業務をシステム管理業務とする。（図２）

(1) トラブル対応　セキュリティ上の問題、事故・故障等への対応

(2) セキュリティ区画の管理　セキュリティ区画の入退管理と施錠管理

(3) 受け入れ　こまきつながるくん連絡帳の開発・構築・改修後のシステムの受け入れ

(4) 維持管理　こまきつながるくん連絡帳のハードウェア、ソフトウェアの維持管理

(5) データ・バックアップ　システムデータ、アプリケーションデータのバックアップ

(6) 運転監視　こまきつながるくん連絡帳の運転、操作及び稼働監視

(7) その他　システム管理に関する事項

（トラブル対応）

第１８条　システム管理者は、システム管理業務の中でシステムの異常を発見した場合、システム運用者から不具合の連絡を受けた場合又はシステム運用中の情報漏えい事故が発生した場合、次の各号に示すとおり対応し、システム障害・情報漏えい事故報告書（様式第３）にその内容を記録し、小牧市へ提出するものとする。小牧市は、当該報告を受けた際、必要に応じてその旨を小牧市在宅医療・介護連携推進協議会（以下「協議会」という。）に報告し、協議会は事故防止の対策を協議するものとする。

(1) システムの異常、不具合の状況及び情報漏えいの状況を確認し、小牧市に連絡する。

(2) 事案が発生し、情報資産の防護のためにネットワークの切断がやむを得ない場合は、ネ

ットワークを切断する措置を講ずる。

(3) 事案が発生し、情報資産の防護のために情報システムの停止がやむを得ない場合は、情報システムを停止する。

(4) 事案にかかる情報システムのアクセス記録及び現状を保存する。

(5) 原因を分析し、その復旧のため関係箇所（メーカー、ベンダー、システム構築箇所など）と連係し、早期復旧に努める。また、情報漏えい事故については、被害規模の確認をするとともに、今後の対処予定の検討をする。

(6) 利用者等の利用に影響が及ぶ場合は、状況に応じてポータルサイトサービスへの掲載及び電話・FAX・E-mail 等により状況、復旧予定、今後の対処予定などを報告する。（図３）

(7) 事案に対処した経過を記録する。

(8) 事案にかかる証拠保全の実施を完了するとともに、再発防止の暫定処置を検討する。

(9) 再発防止の暫定措置を講じた後、復旧を行う。

(10) システム管理業務の一環で対応できない再発防止策が必要と思われる場合は、その内容を整理し小牧市に報告する。

（セキュリティ区画管理）

第１９条　システム管理者は、こまきつながるくん連絡帳の維持管理等に伴って直接当該クラウド設備に対する作業を実施する必要がある場合、次の各号に掲げる事項を遵守するものとする。

(1) こまきつながるくん連絡帳を構成するクラウド設備設置室への入退管理ルールに従うこと。

(2) ラックは常時施錠し、作業に当たっては鍵管理者による鍵の貸し出し許可を受けること。

(3) 鍵の管理は、鍵管理者が実施すること。

（受け入れ）

第２０条　システム管理者は、システムを新規に受け入れる場合又は改善後に受け入れる場合、次の各号に掲げる事項を実施するものとする。

(1) システム管理業務として規定された業務の具体的な実施方法又はその変更事項の確認

(2) 受け入れるシステムが仕様どおり稼働することの確認又は改善の場合は既存システムへの悪影響がないことの確認

(3) 受け入れる資産台帳（ハードウェア、ソフトウェア、アプリケーションプログラム等）の整備

(4) 受け入れるシステムについて、システムファイルのバックアップの確保

（維持管理）

第２１条　システム管理者は、受け入れたシステムのハードウェア及びソフトウェアに対する維持管理を、次の各号に示すとおり実施するものとする。

(1) ハードウェアに対しては、メーカーの指示に従い定期的な再起動等の維持管理を行い記録する。

(2) ソフトウェアに対しては、メーカー等からの指示に従い、バグ対応やセキュリティホール対応等の維持管理を行い記録する。

(3) ソフトウェアの維持管理を実施したときは、システムファイルのバックアップを確保する。

(4) システムデータについては、第２０条に規定した受け入れ時及び変更時にバックアップを取り、５年間保管するものとする。

（データの処分）

第２２条　システム管理者は、システムデータを処分する場合は、記録媒体の初期化、破壊、専用ソフトウェアによる消去等データを復元できないよう確実な方法で処分し、システム運用者に消去証明を提出する。

（データ・バックアップ）

第２３条　システム管理者は、システム内にて一時保管している利用者の複製診療情報（以下「アプリケーションデータ」という。）について、データ・バックアップ処理を次の各号に示すとおり実施するものとする。

(1) 利用者が、こまきつながるくん連絡帳のシステム内へアプリケーションデータを発信した日から起算して５年間の保管に万全を期すために、毎日及び毎月定められた日時に自動データ・バックアップ処理を行う。

(2) 自動データ・バックアップ作業を行う日時については、予め小牧市の承認を受けるものとする。小牧市からの承認後、毎日及び毎月のデータ・バックアップの日時をポータルサービスにより予め利用者に公開するものとする。

(3) 毎月１回のデータ・バックアップ作業時については、こまきつながるくん連絡帳のすべて又はその一部のサービスを停止することができるものとする。また、システム停止を伴う作業が発生する場合は、その内容を予めポータルサービスにより利用者に公開するものとする。

（運転・監視）

第２４条　システム管理者は、受け入れたシステムの運転操作（起動停止など）及びシステムの稼働監視（生死監視など）を次の各号に示すとおり実施するものとする。

(1) システムの運転操作は自動運転とする。ただし、こまきつながるくん連絡帳のシステム内からアプリケーションデータの削除処理及びシステムの異常等によりシステム停止を要する場合は、手動運転操作とする。

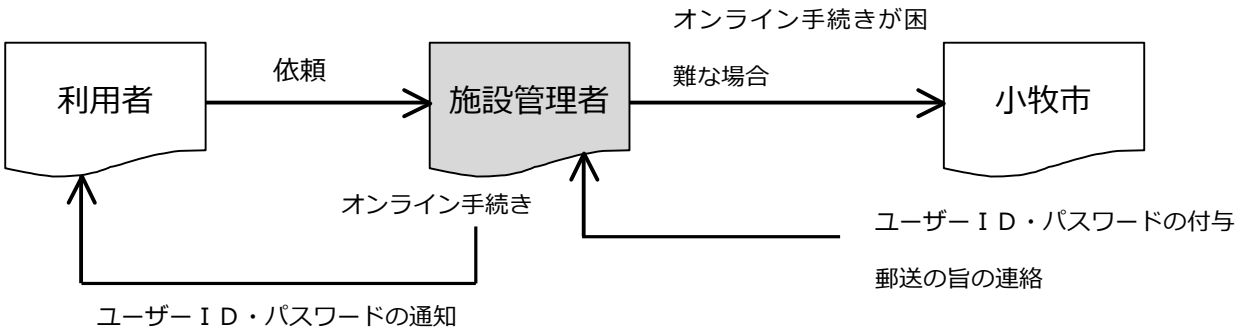
(2) ネットワーク監視プログラム等による５分毎のハードウェアの生死監視、１５分毎のシステムアプリケーションの応答監視及びファイア・ウォールのアクセス・ログ確認によるシステムの稼動監視を定期的なチェックとする。

(3) 前２号の業務に必要な運転手順書は、システム管理者がいつでも参照できるよう常備するものとする。

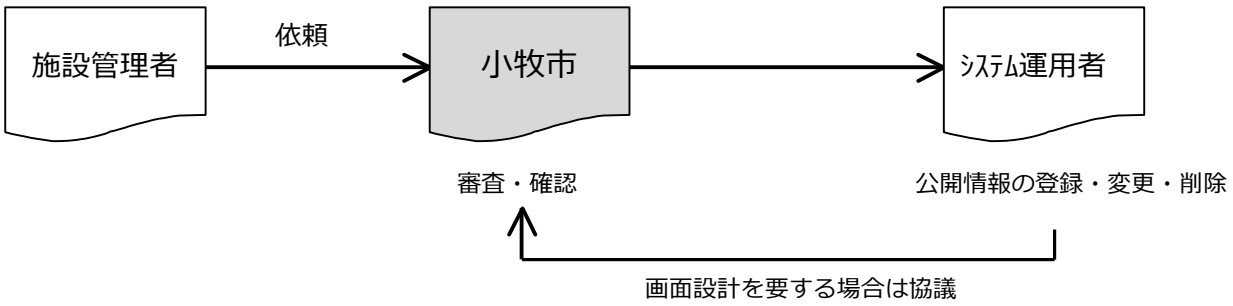
（図１）

システム運用業務

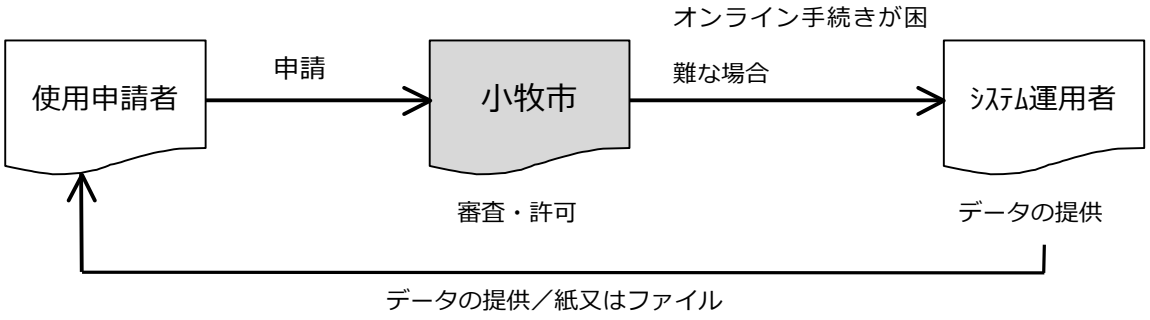
1　ユーザーＩＤ及びパスワードの付与とその登録・変更・削除



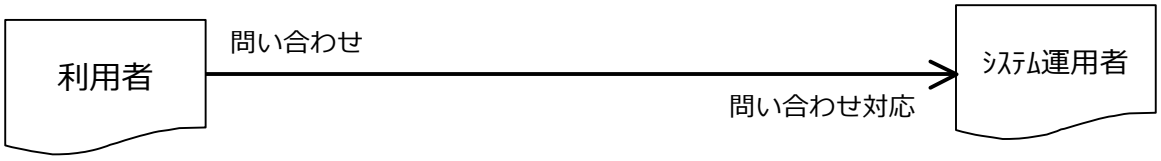
2　ポータルサイト情報の登録・変更・削除（ポータル管理）



3　データの臨時使用



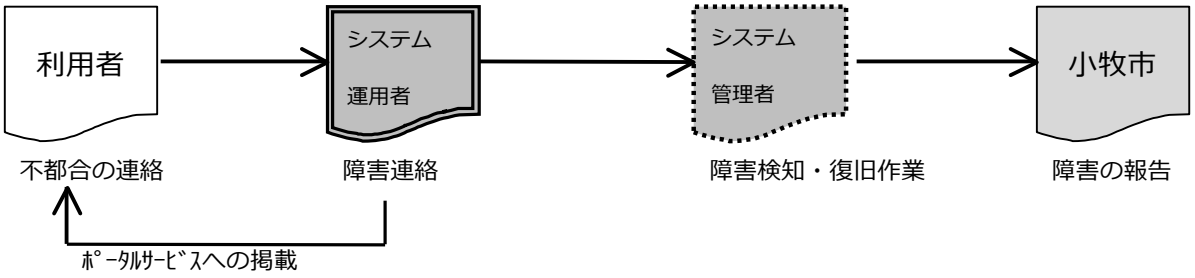
4　利用者への問い合わせ対応



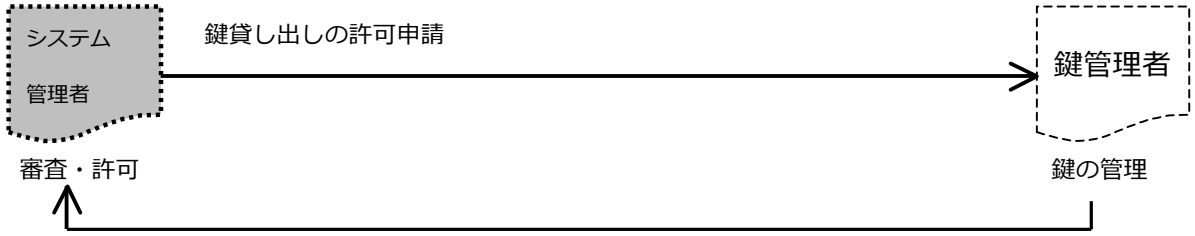
（図２）

システム管理業務

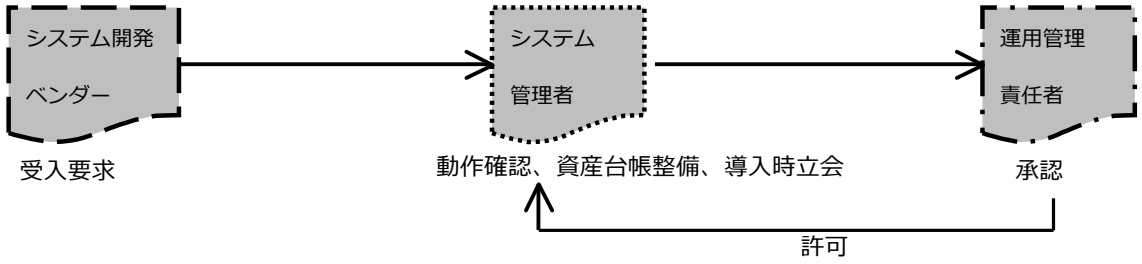
1　セキュリティ上の問題、事故・故障等への対応



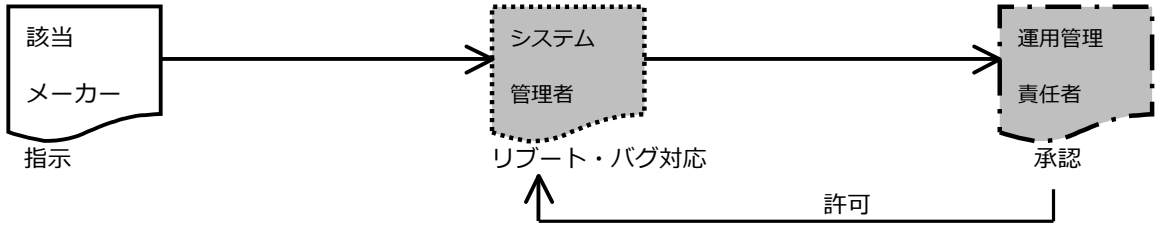
2　セキュリティ区画の管理



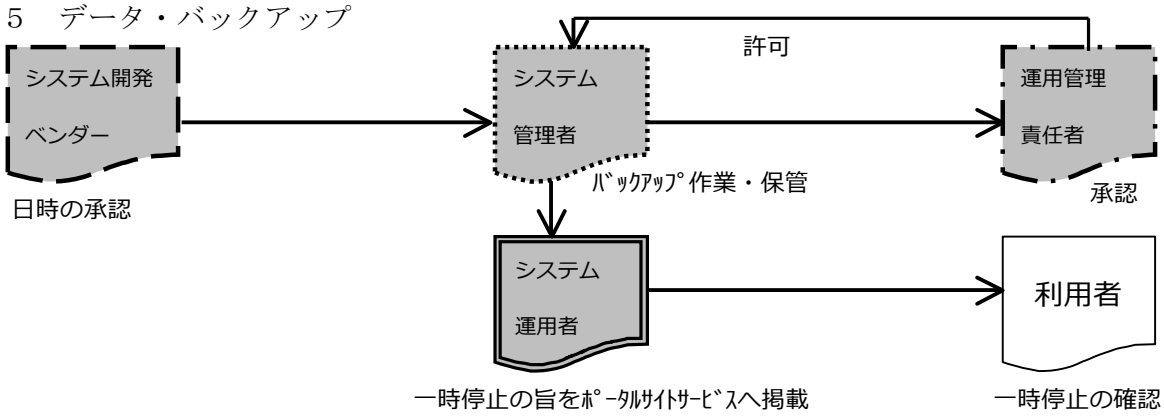
3　新たなシステムの受け入れ



4　維持管理



5　データ・バックアップ



（図３）

障害・情報漏えい事故時などの連絡体制図