別紙１　「ＳＬＡ（Service Level Agreement）項目」

指標の種類	指標名	計算式	単位	目標値	計測方法	計測周期
問い合わせへの一次回答	一次回答の応答時間	応答時刻－問い合わせ受付時刻＜60 分の件数／問い合わせ件数	%	100%	問い合わせ一覧表に受付と応答日時の記録	毎月
セキュリティ対策	セキュリティ事故発生件数	セキュリティ事故発生件数	件	0 件	セキュリティ対策ソフトウェアおよび人手により検知されたセキュリティ事故(防御されたものは除く)の発生件数の集計	毎月
運用業務サービス	サービス提供時間	9:00～18:00 のサービスを提供できなかった日数／営業日数×100	%	0%	勤務実績の提出	毎月
	報告書類の提出期限	期限までに提出した報告書類の件数／報告書類の件数×100	%	100%	提出期日と報告日の比較	都度
ヘルプデスク業務	サービス提供時間	9:00～18:00 のサービスを提供できなかった日数／営業日数×100	%	0%	勤務実績の提出	毎月
障害対応	初動対応の開始	異常の発見から 15 分以内に初動対応を行った障害件数／障害件数×100	%	100%	障害発見日時と初動対応開始日時の障害報告書への記録	毎月
	障害発生の連絡	異常の発見から 1 時間以内に PMDA に連絡した障害件数／障害件数×100	%	100%	障害発見日時と障害発生連絡日時の障害報告書への記録	毎月
	障害報告書の提出期限	期限までに提出した障害報告書の件数／障害報告書の件数×100	%	100%	提出期日と報告日の比較	都度
システム稼働	システム稼働率	(計画サービス時間－計画外サービス停止時間)／計画サービス時間×100 ※1 分未満のサービス停止時間は切り捨て)	%	99.9%	サービス停止開始・終了日時の記録	毎月

別紙２　「作業スケジュール」

別紙2　作業スケジュール

No	セキュリティ対策	実施区分	2025年度 契約月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	実施内容
マイルストン																			
1-1	キックオフ	実施◎	▲																実施計画書に基づくキックオフを実施
1-2	実施計画書の作成	実施◎	実施																契約後2週間以内に運用準備作業に関する実施計画書（運用準備作業）を作成し、PMDAの承認を受ける。
1-3	月次定例	実施◎		▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	
1-4	次年度(新業者)への引継ぎ	実施◎															実施		
運用																			
2-1	インシデント一覧報告（システム障害、情報セキュリティインシデントを含む）	報告○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	「システム運用標準」 ⇒インシデント管理：インシデント一覧による月次報告
2-2	システム変更作業報告 （パッチ適用状況報告を含む）	報告○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	「システム運用標準」 ⇒変更管理：変更作業一覧による月次報告
2-3	特権ID使用状況報告 （台帳を含む）	報告○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	「システム運用標準」 ⇒特権ID管理台帳・特権ID使用管理簿による月次報告
2-4	データ保全（バックアップ）状況の点検	報告○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	「システム運用標準」 ⇒バックアアプと回復：遵守状況の月次報告、机上訓練（任意）
2-5	情報セキュリティ：遵守状況の報告	報告○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	「システム運用標準」 ⇒情報セキュリティ：遵守状況の報告
2-6	脆弱性対策の実施状況の点検	報告○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	⇒情報セキュリティ管理：セキュリティパッチ適用状況の報告 脆弱性に関し関する新着情報、影響度・適用要否、適用予定と実績
権限管理																			
3-1	各業務データアクセス権限再検証	支援△							準備		実施		▲報告			▲報告			不要なアクセス権限の洗い出しと削除。
3-2	ユーザーID棚卸し （各業務システム）	実施◎							準備		実施		▲報告			▲報告			不要IDの洗い出しと削除・無効化。不要なID、権限があれば削除する。
3-3	特権ID検証(棚卸し)	実施◎					準備		実施	▲報告									【システム運用標準】"システム運用管理（要件書）"に基づく運用 ⇒台帳と使用管理簿の相関チェック、使用管理簿とログの相関チェック
3-4	パソコン等搭載ソフトウェアの定期的な調査、不要ソフトウェアの削除	支援△													準備	実施		▲報告	使用するソフトウェア・バージョン、ソフトウェアの利用可否基準を整理し、棚卸を実施する（パソコン更改時に対応し「台帳」を整備する）
点検																			
4-1	情報資産棚卸し・リスク評価	支援△				準備	実施				▲報告								⇒　厚労省のガイドラインに従って実施：「情報資産台帳」「情報資産ライフサイクル確認様式」「リスク評価チェックシート様式」の作成・更新
4-2	パソコン等情報資産棚卸し	支援△													準備	実施		▲報告	台帳と現物との照合（照合結果に基づく「台帳」の作成）
4-3	システム台帳の最新化	支援△							準備		実施		▲報告						⇒資産台帳・管理簿（システム台帳）を更新する。 ⇒ネットワーク機器ソフトウェア資産台帳を更新する。
4-4	ログ取得状況の点検	支援△							準備	実施	▲報告								⇒情報資産の重要度に応じて、監視対象となるイベントを絞り込み、ファイル抽出した上で、セキュリティ違反を示す証跡がないかを定期的に確認する。
4-5	セキュリティヘルスチェック（不正プログラム及び不正な設定変更の有無確認）	支援△					準備	実施	▲報告										
4-6	情報セキュリティ：遵守状況の自己点検	実施○			準備	実施	▲報告												「システム運用標準」 ⇒情報セキュリティ：遵守状況の報告
4-7	情報システム開発・運用資料確認	実施○								準備	実施				▲報告			▲報告	情報システムの開発・運用・保守に必要な各種ドキュメント（各種設計書、手順書等）と実装（システムの構成・設定、プログラム等）が一致していることを確認する。
教育・訓練																			
5-1	システム運用担当者 （サービスデスク）向け研修	受講△							受講										6月に2回開催予定
内部監査																			
6-1	委託先における情報セキュリティ対策の履行状況の確認	受査◎							準備		受査								⇒過去の実施手順を参考に対象システムを選定の上、PMDA内部検査を実施
PMDA監査受査への支援																			
7-1	厚労省・情報セキュリティ監査	支援△							監査支援										
7-2	調達による第3者情報セキュリティ監査	支援△								監査支援									
7-4	監査指摘対応フォロー	支援△		･･･運用フォロー･･･			▲報告	･･･････運用フォロー･･･････					▲報告						「過去の監査対応状況について」に基づく進捗管理、半期毎に報告
オンライン請求受入テストに係る改修等支援																			
8-1	疎通確認テスト	実施◎					実施												マイナポータル、e-Gov等に係る仕様、機能、データパターン等確認
8-2	ユーザビリティテスト	実施◎											実施						テストシナリオの作成、テストデータ等環境準備、軽微改修

別紙３　「業務要件」

業務の時期・時間の定義

	実施時期･期間	実施･提供時間	補足
通年	令和 8 年 4 月 1 日 ～令和 10 年 3 月 31 日 ※業務を行う日（平日）とは、本仕様書で別途定められている業務の他は、行政機関の休日（「行政機関の休日に関する法律」（昭和 63 年法律第 91 号）第 1 条第 1 項に掲げる日をいう。）を除く日とする。	9:00～18:00 ※12:00～13:00 は休憩時間とする。	ただし､本仕様書で別途定めるものの他､緊急作業及び本業務を実施するために必要な作業がある場合は､この限りではない。

運用業務の範囲定義

No	名称	内容
1	【システム監視 － 稼動監視】	本システムのハードウェア、ソフトウェア、ネットワークに対して、以下の稼動状況（パフォーマンス）を監視し、監視実績を記録・管理すること。 ※本システムのハードウェア、ソフトウェア、ネットワークに対し、死活監視、障害監視、エラー出力監視を行い、異常を発見した場合は障害対応手順に沿って対応すること。監視に当たっては事前に PMDA と協議の上､必要に応じてツール等を用いた常時監視の仕組みを構築すること。 (1) ソフトウェア及び開発アプリケーションの稼動状況 (2) ハードウェアの各種状況（性能、容量、故障、縮退） (3) バックアップなどの定期起動ジョブの実行結果 (4) セキュリティアラートの発生状況
2	【システム監視 － ログ監視】	本システムを構成する機器及びソフトウェア上で入手可能なログの管理、監視を行い、必要に応じて外部環境に保管すること。 定期的にログの内容を確認し、異常検知した場合は速やかに総合機構に報告し、問題解決のための対処を行うこと。
3	【システム監視 － 情報セキュリティ監視】	本システムへの不正侵入、不正改ざん検知、ウイルスチェックなど、本システムに関するセキュリティ監視を行うこと。
4	【システム設定・操作 － ジョブ管理】	操作ミスの防止や無人化を目的とした操作の自動化を行う場合、必要となるジョブスケジュールの設定等を行うこと。また、ジョブの登録／変更／削除が必要となる場合には PMDA に提案し、PMDA の了解の下、当該作業を実施すること。
5	【システム設定・操作 － 容量・能力管理】	本システムの性能を計測する指標（CPU 負荷、メモリ使用量、ディスク使用量など）を PMDA と協議の上で確定し、指標データを常時収集し、閾値を超えるなどの異常を発見した場合は障害対応について PMDA に提案し、PMDA の了解の下、当該作業を実施すること。
6	【ヘルプデスク業務 － 問い合わせ対応】	利用者からのシステムに関する問い合わせに対応すること。なお、問い合わせ手段は基本的に電話、電子メールとし、専用のフォーマットを用意し、問

No	名称	内容
		合せ内容や処置内容を漏らさず記録すること。また、システム及び機器の障害に関する問い合わせについては原因の調査を実施し、PMDA 担当者に連絡すること。その際は、解決のための対応策も提案すること。保守サービスや各種メーカーへの問合せ時には窓口となって情報を集約すること。
7	【運用管理】	システム運用上の業務プロセスを定めた「業務フロー及び手順書」について、次のシステム運用業務について作成･更新するものとする。 (ｱ)問合せ管理プロセス　(ｲ)インシデント管理プロセス　(ｳ)変更管理プロセス　(ｴ)リリース管理プロセス　(ｵ)構成管理プロセス　(ｶ)問題管理プロセス　(ｷ)各定期点検プロセス　(ｸ)リスク管理プロセス　(ｹ)課題管理プロセス　(ｺ)情報セキュリティ管理プロセス。 変更管理及びリリース管理に伴うハードウェア、ソフトウェア等の資源の版数管理、原本管理を行うこと。本業務の改修案件に限らず、対象システムに対する全ての変更について構成管理を行うこと。
8	【ユーザー管理】	(ア) PMDA から提出されるユーザ登録・削除依頼に基づき、OS 上、及びアプリケーション上のユーザを登録・削除すること。作業内容はすべて作業ログとして蓄積し、PMDA に報告すること。(随時／適宜) (イ) システムを構成する機器やアプリケーション等のユーザ管理 システムを構成する機器やアプリケーション、リモートアクセス機器及びリモートアクセスユーザを管理の対象とすること。 (ウ) アクセス権限管理 管理対象となる各種ユーザのアクセス権限の管理を行うこと。
9	【サービスレベル管理】	別紙１　「ＳＬＡ（Service Level Agreement）項目」参照 運用業務については、受託者とＰＭＤＡとの間で協議の上、ＳＬＡ（Service Level Agreement）を締結する。サービスレベル評価項目と要求水準については、別紙１「ＳＬＡ項目」を参照すること。ただし、サービスレベル評価項目と要求水準については、協議の上、見直すこととする。
１０	【バックアップ/リカバリ】	重大な障害が発生し、復旧が必要になる場合に備え、運用手順としてバックアップ並びにリカバリ計画及び手順を確立し、それに基づき実行すること。
		バックアップデータのリカバリを行う必要があると考えられる場合には、PMDA の判断に従いリカバリ手順に沿って作業すること。
１１	【各種データ管理】	定期的に取得が必要な運用データ、各種帳票・レポート類、各システムの設定データ等のデータ管理。
		(1) 必要データの保存と削除 定期的に夜間バッチ処理により生成される結果データ、操作履歴等の蓄積データに関しては、データを定期的に再利用可能な形式で別媒体に保存した後にデータベースから削除を行うこと。
		(2) データ保守 業務アプリケーションに起因する障害復旧に伴い、過去のデータを含め、不整合データの存在が明らかになった場合、不整合データの修正箇所の特定、報告を行い、PMDA と協議の上、修正、削除の実施、確認、記録業務への対応を行うこと。また関連文書検索用紐付けデータのデータベースへの一括登

No	名称	内容
		録、更には登録された紐付けデータに不整合等が判明した場合には、その修復も行うこと。
		(3) データ集計 PMDA の指示により、データベースからの条件指定によるデータ検索、抽出、集計を行うこと。(月 4 回程度)
１２	【データベース運用支援】	データベースの性能劣化を防止するため、テーブル再構成やインデックス再構成等の性能劣化防止作業を計画し、PMDA の承認を得た上で定期的に実施すること。
１３	【住基ネット関連運用支援】	住基ネットに係るシステムについて、適宜以下について対応すること。 (1) 市町村コードマスタファイルの更新 (2) 画面制御情報の設定 (3) 本人確認端末の追加 (4) 情報提供業務メニュー画面における初期表示の設定変更 (5) 情報提供サーバにおけるユーザパスワード変更に伴う対応 (6) 耐タンパー装置の抜き取り/接続 (7) 定期点検（日常点検、定期点検、バックアップ装置のクリーニング等） (8) 情報提供サーバ/本人確認端末/その他ハードウェアやソフトウェアに係るアップデート (9) 法定停電等におけるシステム停止/起動 (10)操作ログ検証のための救済システムデータの抽出 (11)障害発生時の復旧作業
１４	【ファイルサーバ棚卸】	救済システム内に構築されているファイルサーバについては、一時的な利用を想定したものであるため、半年に一回の頻度で棚卸を行い、最終更新日が半年以上前のファイルについては担当課に移動を依頼すること。 共有フォルダ配下のファイルを取得するバッチファイルが配置され、タスクスケジューラによって定期実行され、最終更新日とパスを含む情報を出力するようになっているが、現状は整形が必要である。(上位フォルダ単位でのファイル分割、半年経過前の情報の削除等) PMDA の指示を踏まえて処理を効率化するようバッチファイルを修正すると共に、運用手順書を新規作成すること。
１５	【その他】	定期的（概ね年 2 回）に実施される新霞が関ビル電気設備のための停電に対応すること。

保守業務の範囲定義

No	名称	内容
1	【システム設定・操作 - 設定変更】	ハードウェア、OS、ミドルウェア等を正常に稼動させるために設定の変更が必要となる場合にはPMDAに提案し、PMDAの了解の下、当該作業を実施すること。
2	【ソフトウェア保守 - ソフトウェア更新】	運用対象システムのソフトウェア資源について、以下の作業を実施する。なお、(3)～(6)に係る、公表されている脆弱性情報を漏れなく把握すること。ソフトウェアの更新作業については、PMDA と協議の上、検証テストや事前のバックアップ（スナップショット取得等）を実施の上で本番環境に反映させること。
		(1) パッチの提供に関する情報及び 脆弱性情報の収集 当システムを構成する全てのソフトウェアについて、ソフトウェアベンダからのパッチ（不具合修正を目的とするパッチ、脆弱性対策を目的とするセキュリティパッチの両方を含む。）の提供情報及び脆弱性に関する情報を継続的に収集すること。
		(2) 脆弱性対応計画の作成 脆弱性情報又はセキュリティパッチの提供に関する情報を入手した場合、当該脆弱性への対応又は当該セキュリティパッチの適用に関する計画を脆弱性対応計画」（案）として取りまとめ、PMDAの承認を得ること。脆弱性対応計画」（案）は、以下の内容を含むこと。 ・対策の必要性 ・対策方法又は対策方法が存在しない場合の一時的な回避方法 ・対策方法又は回避方法が情報システムに与える影響 ・直ちにはパッチ適用できないと判断される場合のリスクと当面の回避策（案） ・対策の実施予定 ・テストの必要性 ・テストの方法 ・テストの実施予定 ・テストの合格基準 ・本番環境への適用手順とスケジュール
		(3) 業務アプリケーションへのパッチの定期適用 業務アプリケーションプログラムへのパッチの適用を定期的に適用する計画を作成し、PMDAの承認の上で適用を実施すること。
		(4) 業務アプリケーションへのパッチの緊急適用 業務アプリケーションプログラムへのパッチを緊急適用する計画を作成し、PMDAの承認の上で適用を実施すること。
		(5) OS・ミドルウェアの不具合修正の適用 特定ミドル保守業者又はその他の機器保守業者から提供される修正版の OS・ミドルウェアの不具合修正資源を適用する計画を作成し、PMDA の承認を得た上で適用を実施すること。
		(6) ウィルスパターンファイルの更新 本システムに導入されているアンチウィルスソフトウェアのうち、パターンファイルの自動更新が行われていないものについては、1日ごとにウィルスパターンファイル資源を適用すること。

No	名称	内容
3	【ハードウェア保守】	ハードウェア及びファームウェアの不具合、ファームウェア更新等のハードウェア保守に関してサーバ等の保守業者と協力し、分担の役割に応じて対応すること。作業の分担において抜け、漏れが出ないよう充分留意し、最終的な対応は本件受注業者の責任において実施すること。別紙　運用監視・保守方針と役割分担を参照。
4	【不具合修正、軽微な改修】	運用を継続するにあたって、業務の効率化、利便性の向上に資するために、PMDAの指示の下、検索条件及び検索処理の修正、小規模ツール、文書管理システムに関連した文書の保存方法といった軽微なプログラム改修・システム構成の変更を実施すること。必要な設計書及び業務フローの改訂・作成及びプログラム入替え作業も含むものとする。（年間100人日程度※の作業とする。）
5	【オンライン請求受入テストに係る改修等支援】	デジタル庁によるマイナポータル/汎用電子申請サービス/e-Gov 審査支援サービス（以下、「外部サービス」という）側の改修が完了した後、外部サービス側の環境（テスト環境含む）とPMDAの検証環境を利用して、オンライン請求に係る一気通貫のテストを実施する。 （外部サービスを含む全体像については下図を参照） 一気通貫テストの開始時期について、デジタル庁とスケジュール調整を行うこと。デジタル庁に確認の上、改修完了に先行して実施可能なテスト範囲があれば順次着手すること。 一気通貫のテストに当たっては、アプリによる認証にあたりスマートフォンの利用が必須であることから、以下の要領でスマートフォンを準備すること。 台数：14台（iPhone 7台、Android 7台） 利用場所：PMDA拠点内 OS： 　iPhone：iOS 16以降 　Android：Android 11以上 Android端末のメーカー：Google Pixel その他：グローバルIPアドレスを1つに絞って通信できること また、スマートフォンの初期セットアップにあわせて、アプリの利用申請、インストール作業やテストに使用するために必要となる各種設定作業を実施すること。 一気通貫テストについては受託者主体の「①疎通確認テスト（システム観点での構成やデータ入出力に係るテスト）」と PMDA 主体の「②ユーザビリティテスト（業務観点でのテスト）」を想定しており、それぞれ以下について対応すること。 ① 疎通確認テスト ● 外部サービスが手順書通り利用できるか確認すること ● e-Gov 審査支援サービスからダウンロードする全手続き分の請求データについて以下を確認すること

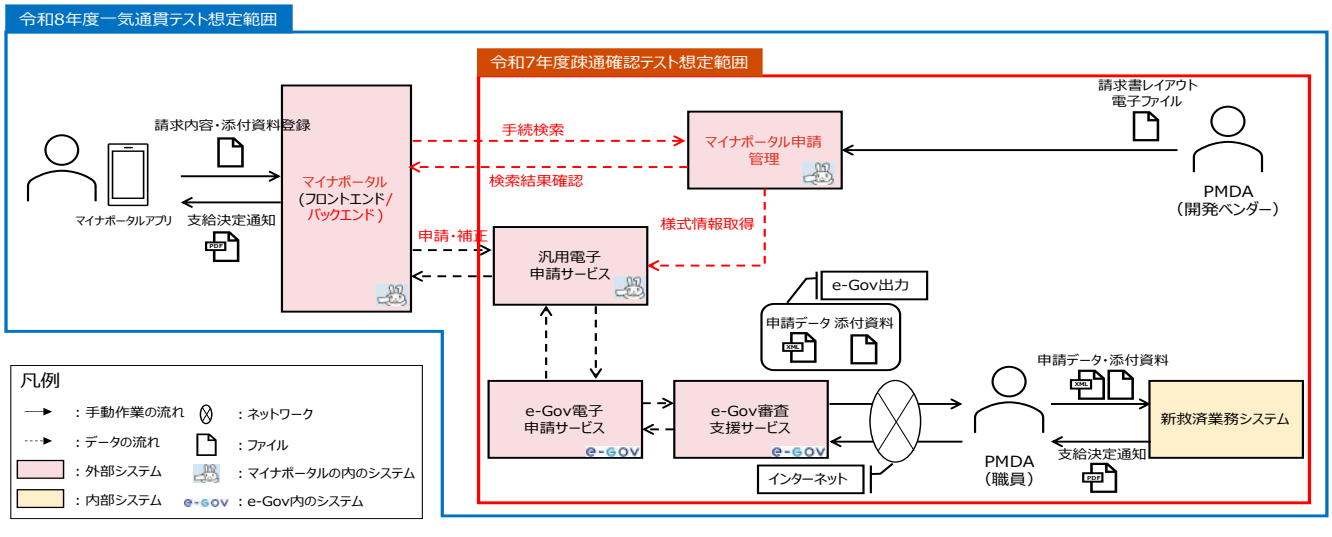
No	名称	内容
		➢ パラメータシート通り様式が設定されていること ➢ zip ファイルの構成（フォルダ/ファイル構成、形式等）が想定通りであること ➢ XML ファイルのデータ構造が想定通りであること ➢ 本システムへの取込み後、問題なく DB 登録、画面/帳票出力できること ※想定仕様については PMDA よりご連絡する予定 ● 決定通知を e-Gov 審査支援サービスを通してアップロードし、マイナポータルで閲覧できることを確認すること ● 全手続きにおいて外部サービス側と本システムとでデータパターン（最大値/最小値、単一/複数の選択肢、チェックボックス、日付、ブランクフォームの値等）を洗い出し、問題なく入出力できることを確認すること ※上記に係るテストシナリオ及びテストデータ、テスト環境について作成/準備すること ※PMDA 環境におけるファイルのアップロード/ダウンロードについては受託者では対応できないため、PMDA 職員に依頼すること ※受託者によるテストにあたっては、J-LIS からテスト用のマイナンバーカード借用すること。手続に数カ月かかる可能性があるため、PMDA に確認の上、契約次第すぐに借用に係る手続を進めること。 ② ユーザビリティテスト ● 令和 7 年度受入テストのテストシナリオをもとに、ユーザビリティテストで必要なテストシナリオを作成すること ● 令和 7 年度以降、政府共通基盤側の仕様変更等が発生した場合には、必要に応じて該当箇所を含むテストシナリオを追加すること ● 必要に応じてテストデータや環境を準備すること ● テスト担当者（ユーザー）からの問合せに対応すること 上記の一気通貫テストの結果、外部サービスの設定変更等が必要となった場合は、PMDA の指示の下、設定変更又は変更支援をすること。この変更により e-Gov 審査支援サービスから出力される XML 等のデータが変更されるかを確認し、変更される場合は当該変更を受けて XML データ取込み機能等において既存システムの改修が必要かどうか確認すること。 既存システムの改修が必要な場合は軽微なプログラム改修を実施すること。 必要に応じて設計書の作成・改訂及びプログラム入替え作業を実施すること。 当該変更を受けて既存の手順書（PMDA 向け、請求者向け）や請求者向け動画を修正する必要があれば対応すること。 本件に関連して、必要に応じて QA 管理表等を作成の上、直接外部関係者（デジタル庁等）とコミュニケーションをすること。 本件についてはタイムリーな対応を求めることから、担当者を本案件専用にア

No	名称	内容
		サインすること。 （本タスク全般として 60 人日程度※の作業とする。）

※ ローコード基盤であることを考慮し、画面や帳票の文言修正、レイアウトの変更等、軽微なメンテナンス作業は通常保守作業として、保守作業工数消費対象作業に含まないこととする。業務ロジックの追加・変更を伴う改修は保守作業工数を消費することとする。

※別途、改修案件が調達された場合、当該受注業者との連携、調整を密にし、当該受注業者による改修作業が円滑に進むよう支援をすること。その際にはソースプログラムのデグレード等が発生しないよう、構成管理に留意すること。本システムの開発方法に適合させること。

図　外部サービスを含む全体像



別紙4

システム運用管理基準

2018 年 7 月

独立行政法人　医薬品医療機器総合機構

【資料の見方】

✧　システム運用業務を「１２の領域」に分けている。
それぞれの業務プロセスは、標準化対象外。各情報システムの体制･特性･リスク等により、最適なプロセスを設計し、運用する。

✧　システム運用の標準化（要件）は、システム運用者（委託先）から PMDA への報告（情報提供も含む）を統一することにある。

- 当資料においては「標準化」のタイトル等にて報告を記載している。
- 標準化（要件）は、「報告書式を統一する領域」と「報告内容を統一（書式任意）」の 2 タイプに分かれる。
- 「報告書式を統一する領域」は、インシデント管理、変更管理、アクセス権管理の領域となっている。

改訂履歴

改訂日	改訂理由
2018 年 6 月 8 日	初版発行
2018 年 7 月 20 日	情報セキュリティ遵守状況報告内容を追記

1. はじめに

1．1　目的

独立行政法人医薬品医療機器総合機構（PMDA：Pharmaceuticals and Medical Devices Agency）（以下、「機構」という。）が調達し、又は、開発した情報システムの運用管理を確実かつ円滑に行い、利用者が要求するサービス品質を、安定的、継続的かつ効率的に提供するために、情報システムの運用管理に関する業務内容を明確化・標準化するために定めるものである。

1．2　対象範囲

機構が調達し、又は開発・構築した全ての情報システムの運用保守を担当する組織（情報システムの運用保守業務を外部委託する場合における委託先事業者を含む）に適用する。

1．3　適用の考え方

システム運用管理業務は、既に開発・構築しサービスイン（本番稼動）している情報システムの運用・保守業務の実行と管理に係る業務を対象とする。

情報システムの運用・保守を外部委託する場合は、本資料をもとに委託先事業者において、当該情報システムの種類・規模・用途を踏まえた適切な運用手順を策定のうえ、運用サービスを提供するものとする。

1．4　用語の定義

本要領で使用する用語は情報システムの「ITIL（IT Infrastructure Library）」のガイドラインを踏まえた運用プロセス定義に準拠するものとする。

1．5　準拠および関連文書

上位規程　：「情報セキュリティポリシー」
関連文書　：「情報システム管理利用規程」

2. システム運用管理業務の概要

機構においては情報システムの運用保守を外部委託している状況を踏まえ、運用管理に必要なプロセスのあるべき姿から主要なプロセスを運用管理業務として選定し、以下の12の管理業務について、明確化・標準化を行う。

管理業務	概要
問合せ管理 （サービスデスク）	システムの利用者からの問合せ窓口として、利用者からの各種問合せについて一括受付することにより 問合せに対する早期回答、障害対応への早期エスカレーションを図るとともに、ユーザからの要望を適切に吸い上げる。
インシデント管理	問い合わせに含まれるインシデント、あるいはハードウェア、アプリケーションなどからのインシデント発生の警告／報告を受け、サービスの中断を最小限に抑えながら、可能な限り迅速に通常サービスを回復するよう努める。
問題管理 （再発防止策）	障害（インシデント）の根本的な原因となっている不具合が、ビジネスに与える悪影響を最小化するため、問題を分析し抜本的解決策や回避策を立案する。
変更管理 （課題管理）	情報システムに対する変更の許可と実装を確実に行うための管理をいう。本番環境に対する変更要求を適正な要領で評価・承認を行い、標準化された変更方法、手順が実施されることを確実にする。また、変更による影響とリスクを最小化し、障害を未然に防止することで、サービス品質の維持・向上に努める。 なお、本要領においては、変更要求の必要性、効果、リスクなど変更の妥当性の評価と承認（変更管理）に加えて、本番環境に対してどのような準備・実行・見直しを行って変更を加えるかの決定（リリース管理）を含めるものとする。
構成管理	情報システムを構成する物理資源・論理資源とその環境を常に把握するための管理をいう。運用・保守業務やそのサービスに含まれる全てのIT資産や構成を明確にし、正確な構成情報と関連文書を提供することで、他のサービスマネジメント・プロセス（インシデント管理、問題管理、変更管理、情報セキュリティ管理等）に信頼できる管理基盤を提供する。
運行管理 （稼動管理）	情報システム全体を予定通り安定的に稼動させるために、システムのスケジュール、稼働監視、オペレーションなど一連の運行を管理する。 ・スケジュール管理 ・オペレーション管理（定型業務、非定型業務） ・稼動監視　・障害対応　・ジョブ運用　・媒体管理 ・本番システム導入・移行時の支援　等

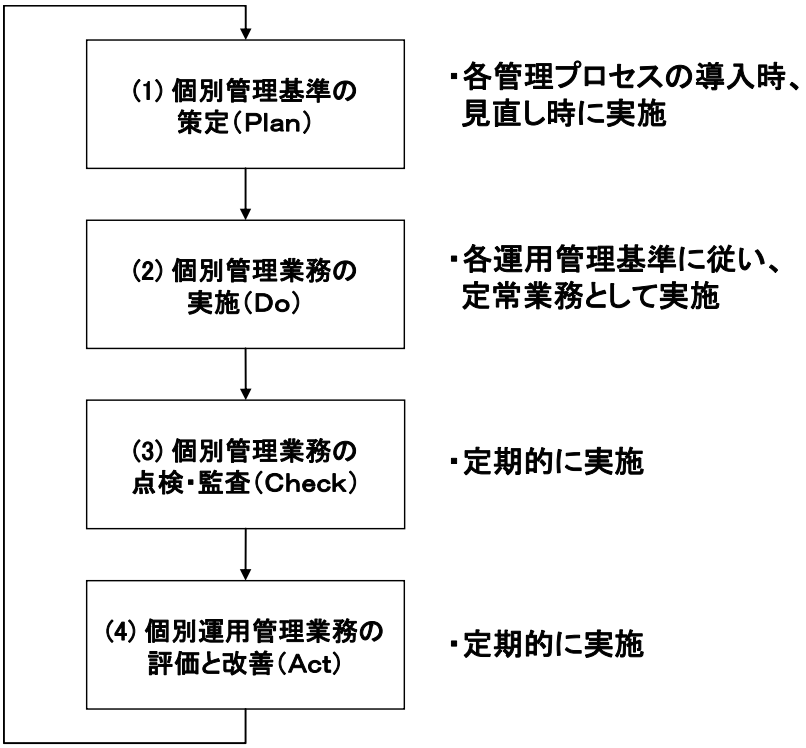
管理業務	概要
バックアップと 回復管理	必要なバックアップを定期的に取得、管理し、障害が発生した場合は、速やかな回復ができるよう、回復要件に基づき必要な回復手順、仕組みを計画、作成、維持する。
情報セキュリティ管理	情報セキュリティポリシーに規定されたセキュリティ対策を実施するために必要な管理要件に基づき、情報セキュリティ管理要領・手順等を作成し、情報セキュリティ管理を行う。
アクセス権管理	アクセス方針を定め、アクセス制御の仕組みを構築・維持し、システム・アカウントの申請受付け・登録・変更・削除など管理業務を行う。 ・アプリケーション・システムのアカウント ・サーバのOSアカウント ・DBMSアカウント ・運用支援システムのアカウント ・各種特権アカウント　等
キャパシティ管理	サービス提供に必要となるシステム資源の利用状況の測定・監視を実施し、現在の業務要求（既存の提供サービス量）と将来の業務要求（要求される提供サービス量）とを把握した上で、システム資源がコスト効率よく供給されるように調整・改善策の立案を行う。
可用性管理	ITインフラストラクチャーを整備し、それをサポートするITサービス部門の能力を最適化させることで、ビジネス部門に対して、費用対効果が高いITサービスを持続して提供する。 可用性管理の活動は、既存のITサービスの可用性を日常的に監視・管理する「リアクティブ」なプロセスと、リスク分析や可用性計画の策定や可用性設計基準などの作成を行う「プロアクティブ」なプロセスに分けられる。
サービスレベル管理	「サービスレベル合意書」で定める各種サービスレベル値の達成、維持作業として、管理項目に対する実績データの収集、分析、評価、及び改善策を策定する。 また、運用管理業務における報告データを収集、管理し、月次にユーザへの報告を実施する。

3. 運用管理業務の基本プロセス

（運用管理業務プロセスのPDCAマネジメントサイクル）

他のマネジメント・システムと同様に、運用管理業務プロセスも手順書等を策定して終わりではなく、実際に手順書等に準拠した運用を実施し、定期的に又はシステムの変更やメンバーの入れ替わりなどに合わせて都度、管理プロセスを見直し、必要に応じて改善・是正を行う必要がある。

そのために、運用管理業務プロセスに、個別管理要領の「策定（Plan）」、「実施（Do）」、「点検・監査（Check）」、「評価と改善（Act）」の４つの基本プロセスからなるPDCAマネジメントサイクルを導入し、継続的改善を実施することが重要である。



各基本プロセスの概要は、以下のとおりである。

（1） 個別管理要領の策定 （Plan）
各運用管理業務の実施方針、実施範囲、管理プロセス、業務の管理指標等を含めた管理要領書ならびに管理手順を定める。

（2） 個別管理業務の実施 （Do）
各運用管理業務の実作業を行うとともに、業務遂行に必要な関連情報の蓄積、実績情報の収集保管、およびに評価指標の実績測定を行う。

（3） 個別管理業務の点検・監査 （Check）
各運用管理業務に対し、個別運用管理要領に遵守した運用がなされているか定期的に点検・監査を行い、その結果を分析･評価する。

（4） 個別運用管理業務の評価と改善 （Act）
各運用管理業務に対する評価指標に対する実績管理を行うと共に、品質向上に向けた改善計画を立案し、改善実施を行う。

4. システム運用管理業務の明確化・標準化

4. 1 問合せ管理

(1) 目的

ユーザ及び各業務プロセスオーナからの問合せや依頼に対する受付窓口を一元化することで、各業務の利用ユーザの業務効率性を向上させる。

(2) 業務の概要

問合せ対応では、問合せの受付、クローズ、一次回答、管理プロセスの評価・改善の一連のプロセスを実施する。

(3) 管理対象

本番システム環境で稼動している全てのシステムに係る以下の問合せについて対応する。

- アプリケーション仕様、操作、機能、内容に関する問合せ
- ハードウェア／ソフトウェアに関する問合せ
- 要望
- アプリケーション修繕に対する依頼
- その他の依頼作業

(4) 業務の管理指標＆標準化

問合せ対応業務を評価するための評価指標として以下を定義し、定期的(月次)報告を行う。

①問合せ発生件数(日次集計・月次集計を含む)
②問合せ区分別件数
③問合せ一次回答期限遵守率
④問合せ完了率(一定期間経過後(10 営業日経過後)の完了率)

※報告内容は、各システムの状況に応じて変更しても構わない。

【補足】

問合せにより「システム障害」「セキュリティインシデント」が発覚した場合は、該当問合せは一次回答にてクローズとし、その後は「インシデント管理」にて対応する。

問合せにより「変更」実施が必要となった場合は、対応予定日を回答することでクローズとし、その後は「変更管理(課題管理)」にて対応する。

４．２ インシデント管理

(1) 目的

インシデント管理は、ユーザからの問合せ・連絡、あるいはオペレータや監視システム等によるインシデントの検知を受け、ITサービスの中断を最小限に抑えながら、可能な限り迅速に正常なサービスを回復することを目的とする。

(2) 業務の概要

①インシデントの定義

インシデントとは、ユーザや監視システム等の検知により判明したハードウェアやソフトウェアに関する一般的な障害（システム・ダウン、バグによるアプリケーションの機能停止等）だけでなく、ユーザが日常の操作手順によってITサービスを利用する上で支障がある事象はすべてインシデントに包含される。

【注】このインシデントには、情報セキュリティインシデント（不正アクセス・マルウェア検知等）を含む。

また、まだITサービスに影響を与えていない構成アイテムの障害もインシデントとして扱う。

例えば、(i) 二重化されたデータベース・システムの一方がダウンした場合で、まだサービス自体が正常に稼働している場合、(ii) 本番環境のバックアップを検証環境にリストアできない場合、これらをインシデントとして扱う。

②インシデント管理の主な活動

インシデント管理は、インシデントの 4 つのライフサイクル（発見－判別－回復－解決）の内、発見－判別－回復（解決）までをカバーする。（再発防止については、次節の「問題管理」で扱う。）

インシデント管理のプロセスでは、主に次の活動を実施する。

- ・インシデントの検知
- ・インシデントの記録
- ・インシデントの通知
- ・インシデントの分類
- ・インシデントの優先度付け
- ・インシデントの初期診断
- ・エスカレーション
- ・インシデントの調査と診断
- ・復旧(解決)策の実施
- ・インシデントのクローズ

(3) 管理対象

本番システム環境で稼動している全てのシステムのインシデントを管理対象とする。

(4) 業務の管理指標

インシデント管理の管理業務を評価するための評価指標として以下を定義し、定期的(月次)報告を行う。

① 当月インシデント発生件数（総件数、障害ランク別・原因別・システム別件数・解決責任部門別）

② 優先度又は緊急度毎に分類されたインシデントの解決までに要した時間（平均時間）
③ ステータス（記録済み、対応中、クローズ済み等）毎のインシデントの内訳
④ 長期間（発生から１カ月以上）未解決のインシデントの件数と理由および業務影響
⑤ 新規に発生したインシデントの件数とその傾向
⑥ ユーザのトレーニングなど、ITテクノロジーに関連しないで解決されたインシデントの件数
⑦ 解決に要したコスト
⑧ インシデント発生件数の削減率（対前年比）

(5) 標準化

インシデント管理は、機構標準書式を適用する。

①インシデント発生(判明)時

インシデントごとに個票を起票する。この個票は「機構標準書式」を使用する。

※添付「インシデント報告書（ひな型）」を使用する。また「インシデント一覧記載要領」を参照し、対応すること。

※各情報システムの状況等によって、一部改修して使用しても構わない。ただし、必須項目の変更・削除は認めない。

②定期的(月次)報告時

インシデントごとの個票を集計表に転記のうえ報告する。この集計表は「機構標準書式」を使用する。

※添付「インシデント一覧」を使用する。

４．３ 問題管理（再発防止策）

(1) 目的

サービスの信頼性を維持・向上するためには、システムの利用・運用上発生した問題（障害を引き起こす根本的な原因）を確実に解決し、同一障害・類似障害の再発防止のための是正を実施することを目的とする。

(2) 業務の概要

本番サービスに影響を与えた障害を分析し、それらの共通の根本原因を取り除く是正策を実施するまでの一連のプロセスを管理する。 問題管理(再発防止)では、以下を実施する。

- ・問題の傾向分析と課題点の抽出
- ・是正策の検討
- ・是正策の実施

(3) 管理対象

本番システム環境で稼動している全てのシステムの問題を管理対象とする。

(4) 業務の管理指標＆標準化

問題管理(再発防止)業務を評価するための評価指標として以下を定義し、定期的(月次)報告を行う。

① 再発防止策が策定された問題件数（総件数、障害ランク別・原因別・システム別件数・解決責任部門別）
② ステータス（記録済み、対応中、クローズ済み等）毎の再発防止策の内訳
③ 再発防止に要したコスト
④ 長期間（策定から１カ月以上）未実施の再発防止策件数と理由
⑤ 再発防止の実施率（対前年比）

※報告内容は、各システムの状況に応じて変更しても構わない。

４．４ 変更管理

(1) 目的

サービスの信頼性を維持・向上するためには、システムに対する変更について、その妥当性を検証し、変更によるユーザへの影響を最小限にすることが重要である。 変更管理プロセスは、システムに対する変更を一元的に管理することを目的とする。

(2) 業務の概要

変更管理では、変更の申請から変更内容の審査、変更の承認または却下、変更の実施、変更実施結果の報告までの一連のプロセスを管理する。

緊急の場合、対応を優先し所定のプロセスを適宜省略することを可能とするが、事後的に対応できるものについては、事後速やかに対応することとする。

(3) 管理対象

運用チームが運用し本番サービスを提供するシステムのすべて又はその一部に対して影響を与えるすべての変更を管理対象とする。

本番環境	構成要素（主な要素）
ハードウェア	CPU、DASD・DISK、サーバ、ワークステーション、周辺装置
システム・ソフトウェア	OS、サブシステム、サーバ及びワークステーション OS
ミドルウェア	DBMS、ネットワーク OS
アプリケーション・ソフトウェア	ソース、モジュール、シェル、JCL
ネットワーク・ハードウェア	スイッチ、ルータ、ブリッジ
ネットワーク・サービス	基幹ネットワーク、LAN、インターネット　等
データ	データベース及びファイル内のデータ（に対する直接修正）

(4) 業務の管理指標

変更管理業務を評価するための評価指標として以下を定義する。

① 変更実施件数（総件数、領域別・原因別・システム別件数・解決責任部門別）
② 変更の実装が失敗した件数
③ 変更のバックログの件数
④ 予定期間でクローズされなかった変更の件数
⑤ 変更が原因で発生した変更の件数
⑥ 緊急の変更の件数

※具体的にどの管理指標をどう用いるかについては、今後調整の上確定する。
以下同様。

(5) 標準化

変更管理は、機構標準書式を適用する。

①変更案件発生時

課題管理表に記入し、変更管理のステイタス（未着手（対応予定日記入）～着手(対応中)～完了）を管理する。

※課題管理表の書式は、各情報システムの任意とする。

②変更実施着手時

変更の着手ごとに個票を起票する。この個票は「機構標準書式」を使用する。

※添付「変更作業申請書（ひな型）」を使用する。

※各情報システムの状況等によって、一部改修して使用しても構わない。ただし、PMDA側の確認・承認欄の削除は認めない。

※個票は、「単純な定常作業」に関しては使用しなくても良い。

- 「単純な定常作業」は、各システムにて定義する。
- ただし、定期的（月次）報告には、記載する。

※個票は委託先にて保管し、監査等にて提示要求があった場合は、速やかに提示できるよう対応する

③定期的(月次)報告時

変更実施ごとの個票を集計表に転記のうえ報告する。この集計表は「機構標準書式」を使用する。

※添付「変更作業一覧」を使用する。また「変更作業一覧記載要領」を参照し、対応すること。

※「単純な定常作業」に関しては、「変更作業一覧」の「変更申請」欄及び「完了確認」欄に関する内容を記入し、報告する。

４．５ 構成管理

(1) 目的

システムの構成要素（構成情報）を正確に把握し、常に最新状態にあることを保証する事で、他の運用管理プロセス（障害管理や変更管理等）に対して必要な構成情報を提供できるようにする。

(2) 業務の概要

構成管理では、ITサービス開始時より構成情報を一元管理し、他の運用管理プロセスから最新の構成情報を参照可能にする。

本管理プロセスの開始前に、立案した計画に沿って対象とするITサービスやITコンポーネントの範囲、詳細度のポリシーを策定し、開始時のベースラインを把握する。 次に、構成情報の収集と分類を行ったうえで構成情報を参照可能な状態に維持する。

本管理プロセスの開始後は、変更管理プロセスと連携し、構成情報が常に最新状態として維持されるようにコントロールを行う。 また、定期的に構成情報の点検を行うことにより、課題や問題点を洗い出し、評価・改善を行う。

(3) 管理対象

構成管理が対象とする構成情報は以下の通りとする。

カテゴリー	管理対象の種類
システム運用管理	各種管理プロセス定義書、手順書、依頼書、CI一覧
システム運用	・ハードウェア、ネットワーク・ハードウェアの一覧、構成図 ・ネットワーク・サービス （WAN、インターネット等)の一覧、構成図 ・システム運用各種手順書（障害対応手順書等）
システム保守	・システム・ソフトウェア、ミドルウェアの一覧、構成図 ・アプリケーション・ソフトウェア(ライブラリ、データ、環境設定情報)
ハウジング	環境設備 （空調設備、電源設備、配線室、配線、管理室)の一覧、構成図
アプリケーション保守	・設計ドキュメント、プログラムソース ・アプリケーション保守用各種手順書（定型作業手順書等）

(4) 業務の管理指標

構成管理業務を評価するための評価指標として以下を定義する。

① 承認されていない構成の件数

② 不正確な構成情報が原因で失敗した変更及び発生した障害の件数

③ CI（管理対象の項目数）の正確さ率

・構成アイテムの管理情報と実態（H/W、S/W、M/W、機器）との整合性の確認

(5) 標準化

機構では、「システム管理台帳」による管理を実施している。

システム管理台帳の更新(点検)を定期的に実施するため、機構の指示により更新情報を提示すること。

４．６ 運行管理

(1) 目的

運行管理の目的は、開発部門より引き継いだ業務アプリケーション・システムを、あらかじめ定められた運行計画に基づき、定められた手順に従ってシステム運用を行うことにより、システム運用の品質の維持・向上を図ることにある。

(2) 業務の概要

運用引継ぎから、システムのスケジュール計画、稼働監視、オペレーションなど一連の運行を管理する。 以下のサブプロセスから構成される。

① 運用引継ぎ
② 運用スケジュールの計画・管理
③ オペレーション実施
④ 稼動監視と障害対応（一次対応）
⑤ ジョブ実行管理
⑥ 帳票管理
⑦ 報告管理

(3) 管理対象

本番システム環境で稼動している全てのシステムの運行を管理対象とする。

日次で目視監視している業務のうち、メール通知機能を利用した監視ツールに設定することができる業務があれば、機構に提案し了承を得ることで設定可能とする。

(4) 業務の管理指標

運行管理業務を評価するための評価指標として以下を定義する。

① 重要バッチ処理終了時間遵守率
② 重要帳票の配布時間遵守率
③ システムの運行業務に起因した障害の発生件数
・プログラム・JCL等の本番移送のミス、ジョブのスケジュール誤り、操作ミス、監視項目の見落とし／発見遅延、等。
④ 非定型依頼業務の実施件数と正常終了率

４．７ バックアップと回復管理

(1) 目的

障害発生時等において、速やかに正確な回復処置が行えるようにバックアップの取得・リストアの手順を明確にし、安定したサービスの提供を図る。

(2) 業務の概要

アプリケーションオーナーとのサービスレベルまたは管理目標の合意に基づき、システムの回復要件に見合ったバックアップ・リストア方針を定め、バックアップ対象の選定、手順の明確化を実施する。

日常運用においては、バックアップ取得、バックアップ媒体の保管を行う。

また、定期的に、バックアップ・リストア実績報告を行い、バックアップ・リストアにおける体制、役割、手順の見直しを図る。

(3) 管理対象

本番システム環境で稼動している全てのシステムのバックアップとリストアを管理対象とする。

本要領の適用システムに関するOS、データベース、テーブル類、ユーザデータなどのバックアップ計画、バックアップ取得、バックアップ媒体の保管、リストア実施および定期的な実績報告の手続きを対象とする。

(4) 業務の管理指標

バックアップと回復管理業務を評価するための評価指標として以下を定義する。

① 当月で計画された定期バックアップの内、バックアップに失敗した件数と理由。
② 当月実施されたリストア件数と内訳（障害対応、調査目的、帳票再作成・出力等）。
③ 当月実施されたリストアの内、リストアに失敗した件数と理由。

(5) 標準化

〇定期的なバックアップが取得されていることを報告する（月次）（書式任意）

〇機構では、「リストアの机上訓練」を定期的に実施することを推奨している。

各情報システムにおいては、必要に応じて定期的な訓練実施を行い、結果報告を行う。

４．８ 情報セキュリティ管理

(1) 目的

情報セキュリティ管理は、「情報セキュリティ規程」に定める情報セキュリティの管理要領に則り、情報システムのセキュリティを維持・管理し、情報資産を適切に保護することを目的とする。

(2) 業務の概要

情報セキュリティ管理プロセスは、企業のリスク管理活動の一環として、ITサービス及びサービスマネジメント活動におけるすべての情報のセキュリティを、首尾一貫した方針に基づき効果的に管理する。

具体的には、情報セキュリティ規程に則って、適切にセキュリティ管理策が導入され、維持されていることを確実にするために、セキュリティ管理計画の維持・管理、セキュリティ対策の導入時の確認・レビューを行う。

また、導入されたセキュリティ管理策が適切に運用されているかを定期的に点検するとともに、コンプライアンス等の観点からのシステム監査の実施対応をおこなう。

(3) 管理対象

ITサービス及びサービスマネジメント活動におけるすべての情報セキュリティの管理を対象とする。

(4) 業務の管理指標

情報セキュリティ管理業務を評価するための評価指標として以下を定義する。

① 情報セキュリティ違反・事件・事故の発生件数とその内容
② 発生した情報セキュリティ違反・事件・事故への対策の実施状況
③ 情報セキュリティ監査（内部・外部）及び自己点検で検出された不適合の件数
④ 前回の情報セキュリティ監査及び自己点検で検出された不適合の是正状況

(5) 標準化

①情報セキュリティ遵守状況の報告＜次ページ参照＞

- 情報セキュリティを遵守していることを定期的(月次)にて報告すること
- 合わせて委託会社における自己点検を定期的(年 2 回程度)に実施し、点検結果を報告すること。
  （点検内容は委託会社の任意項目で実施）

②情報セキュリティパッチの適用

- 仕様書の記載内容にしたがって情報セキュリティパッチの適用を実施し、定期的(月次)に報告すること

【補足説明】

情報セキュリティ遵守状況の報告は、以下の内容を確認し、報告すること

① 情報の目的外利用の禁止

② 情報セキュリティ対策の実施および管理体制（プロジェクト計画書記載内容の遵守）
※委託先において実施するセキュリティ研修や委託先の情報セキュリティポリシー遵守のため取組み内容を含む
※責任者による情報セキュリティの履行状況の確認を含む

③ 体制変更の場合の速やかな報告

④ 体制に記載された者以外が委託業務にアクセスできない（していない）ことの確認
※発生した場合は、すぐに検知でき、報告される

~~⑤~~ 要員の所属・専門性（資格や研修実績）・実績および国籍に関する情報提供
※変更があれば、その都度情報提供される。

⑥ 秘密保持契約（誓約書）の提出（要員全員が提出）
※委託業務を離れた者の一定期間の機密遵守を含む
※体制変更があった場合の追加提出も含む

⑦ 情報セキュリティインシデントへの対処方法の明確化され、要員に周知されている

⑧ 再委託がある場合は、上記内容を再委託先においても遵守していることが確認されている

４．９ アクセス権管理

(1) 目的

システムを利用するユーザ・アカウントを保護するため、及び、なりすましによる不正ログインの可能性を低減するために、ユーザ・アカウントを役割権限別に分類した上で管理方法を取決めてセキュリティレベルを維持する。

(2) 業務の概要

システムを利用するサーバ OS、ミドルウェア、アプリケーション・ソフトウェア、及びネットワーク機器のアカウントを対象にアクセス権の管理を行う。

(3) 管理対象

本番システム環境での全てのアカウント（社外の取引先等に提供しているアカウントを含む）のアクセス権を管理対象とする。

本番環境	アクセス権管理の対象
システム・ソフトウェア	OS ユーザID
ミドルウェア	DBMSユーザID、ジョブスケジューラ・ユーザID、他
アプリケーション・ソフトウェア	アプリケーション・ユーザID
ネットワーク機器	各ネットワーク機器の管理者用ID

(4) 業務の管理指標

アクセス権管理業務を評価するための評価指標として以下を定義する。

① 期間内に発生したユーザID登録・変更・削除の件数
② 特権（高権限）ユーザID別の貸出し件数と用途
③ アカウントおよびアクセス権の定期棚卸しで、発見された不備項目
④ 不適切／不正なアクセス権限の設定によって発生したインシデントの件数
⑤ アクセス権限の再設定が必要となったインシデントの件数
⑥ 間違ったアクセス権限の設定によって提供不能になったサービスの件数
⑦ 間違ったアクセス権限の設定によって生じた不正アクセスの件数

(5) 標準化

特権（高権限）IDについて、以下の管理を行う。

①特権ID(システムID)台帳の作成

※添付「特権ID管理台帳」を使用する。

※各情報システムの状況等によって、一部改修して使用しても構わない。ただし、項目の削除は認めない。

※監査等にて提示要求があった場合は、速やかに提示できるよう保管する

②特権ID(システムID)使用管理簿の作成（またはログ抽出）

※添付「特権 ID 使用管理簿」を使用する。

※各情報システムの状況等によって、一部改修して使用しても構わない。ただし、項目の削除は認めない。

※ログイン・ログアウトのログ(または画面コピー)を必ず保管（または添付）し、監査等にて提示要求があった場合は、速やかに提示できるよう保管する

③定期(月次)報告

特権ID(システムID)台帳ならびに特権ID(システムID)使用状況を、定期(月次)報告する。

(ログまたは画面コピーは、月次報告不要)

④特権ID棚卸し

特権IDの棚卸しを定期的(年 2 回程度)に実施し、報告を行う。(報告書式任意)

棚卸し点検内容は以下の通り

〇台帳は、本当に使用する者を登録しているか?(体制図と一致しているか?)

・チームから外れた者が削除されずに残っていないか?

・使用予定がない者が登録されていないか?

〇台帳と使用管理簿の相関は一致しているか?

〇使用管理簿とログ(または画面コピー)保管の相関は一致しているか?

4．10　キャパシティ管理

(1)　目的

キャパシティ管理の目的は、ビジネスが必要とするときに、必要なキャパシティを適正なコストで提供することである。 すなわち、

① ビジネスの需要に対する供給

ビジネスの変化に合わせて、ITサービスの対応にもスピードが要求される。 キャパシティ管理は、現在から将来にわたるビジネス需要・要件に合わせて、ITインフラストラクチャーのキャパシティを最大限に活用できるようにすることを目的とする。

② キャパシティに対するコスト

一方、必要以上のキャパシティを確保すると購入や運用のための費用が膨らみ、ビジネスの観点からコストを正当化できない。 キャパシティを最適化し、費用対効果が高いITサービスを提供することもキャパシティ管理の目的である

(2)　業務の概要

このプロセスは、次の3つのサブプロセスから構成される。

① ビジネスキャパシティ管理

ITサービスに対する将来のビジネス需要・要件を収集・検討し、それによって、ITサービスのキャパシティを確実に実装させるための計画の立案、予算化、構築がタイムリーに実施されるようにする。

② サービスキャパシティ管理

実際のサービスの利用と稼働のパターン、山と谷を理解して、運用中のITサービスのパフォーマンスを監視し、それによって、SLAの目標値を達成し、ITサービスを要求どおりに機能させる。

③ コンポーネントキャパシティ管理

ITインフラストラクチャーの個々のコンポーネントのパフォーマンスとキャパシティ、使用状況を監視し、それによって、SLAの目標値を達成・維持するために、コンポーネントの利用を最適化する。

(3)　管理対象

本要領の適用システムにおけるハードウェア、ソフトウェア、ネットワーク、アプリケーション、及び人的リソースを対象とする。

(4)　業務の管理指標

キャパシティ管理業務を評価するための評価指標として以下を定義する。

① CPU、ディスク、メモリ、ネットワーク容量などの閾値に対する需要の割合
② ITサービスのパフォーマンス不足に起因するSLA違反やインシデントの発生件数
③ ITコンポーネントのパフォーマンス不足に起因するSLA違反やインシデントの発生件数
④ 正規の購入計画に含まれていなかった、パフォーマンスの問題解決のために急きょ行った購入の数又は金額

４．１１　可用性管理

(1)　目的

可用性管理の目的は、ビジネス部門に対して、費用対効果が高いITサービスを持続して提供することであり、そのためにITインフラストラクチャーを整備し、それをサポートするITサービス部門の能力を最適化させる。

(2)　業務の概要

可用性管理の活動は大きく、1）可用性要件の把握、2）可用性の設計、及び3）可用性の改善活動の3つに分けられる。

具体的には、以下の可用性管理の3要素の目標値を設定し、設定した可用性のレベルを達成・維持・向上させることである。

① 可用性

可用性とは、ITサービスが必要なときに使用できる割合のことで、一般的には稼働率という指標を用いて表される。

稼働率（%）＝（サービス提供時間－停止時間）÷サービス提供時間

② 信頼性

提供されるITサービスにおける、不具合の発生しにくさ／故障しずらさを表す。

平均故障間隔＝（使用可能な時間－総停止時間）÷（サービス中断の回数－1）

③ 保守性

ITサービスが停止又は品質低下した際に、いかに早く復旧できるかを示す指標。

平均修理時間＝修理時間の合計÷サービス中断の回数

可用性について極めて重要なことは、ユーザの求めるシステムの可用性レベルをどのように達成するかについて、システム設計時に真剣に検討し、システム構築時に実現し、システムの運用において継続的に改善することである。

(3)　管理対象

本基準の適用システムにおけるハードウェア、ソフトウェア、ネットワーク、及びアプリケーションを対象とする。

(4)　業務の管理指標

可用性管理業務を評価するための評価指標として以下を定義する。

① 可用性の割合
② 平均故障間隔
③ 平均修理時間
④ サービスの中断回数
⑤ 定期的なリスク分析、及びレビューの完了の件数

４．１２　サービスレベル管理

(1)　目的

ユーザニーズを満足する適正なサービスレベルおよび管理指標を設定し、これを実績管理することにより質の高いサービスの提供を図る。

(2)　業務の概要

サービスレベルおよび各個別管理業務での管理指標の実績データを定期的に把握し、サービスレベル指標と実績の差異や傾向を継続的に分析することにより、改善策を立案し実施する。

(3)　管理対象

IT 部門が提供するすべての IT サービスに関するサービスレベルおよび各個別管理業務での管理指標を管理対象とする。

(4)　業務の管理指標

サービスレベル管理業務を評価するための評価指標として以下を定義する。

①「サービスレベル合意書」の各サービスレベル項目の達成率

②各個別管理業務での管理指標の達成率

(5)　標準化

サービスレベル管理業務を定期的(月次)に報告する。

①「サービスレベル合意書」の各サービスレベル項目の達成率

②各個別管理業務での管理指標の達成率

以上

別紙5 情報セキュリティ対策の運用要件

情報システムの運用・保守の業務遂行にあたっては、調達・構築時に決定した情報セキュリティ要件が適切に運用されるように、人的な運用体制を整備するとともに、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を確実に実施すること。

対策区分	対策方針	対策要件	運用要件	定期点検
侵害対策 （AT：Attack）	通信回線対策 （AT-1）	通信経路の分離 （AT-1-1）	不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。ネットワーク構成情報と実際の設定を照合し、所定の要件通りに設定されていることを定期的に確認すること。	セキュリティヘルスチェック（構成管理資料の原本と実際の設定状況を目視にて突合せチェックすることにより各種セキュリティ設定の不正変更の有無をチェックする）と合わせて実施し報告すること。
		不正通信の遮断 （AT-1-2）	通信に不正プログラムが含まれていることを検知したときに、その通信をネットワークから遮断すること。	
		通信のなりすまし防止　（AT-1-3）	通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能について、有効に機能していることを定期的に確認すること。	セキュリティヘルスチェック（構成管理資料の原本と実際の設定状況を目視にて突合せチェックすることにより各種セキュリティ設定の不正変更の有無をチェックする）と合わせて実施し報告すること。
		サービス不能化の防止　（AT-1-4）	サービス不能攻撃を受けているかを監視できるよう、稼動中か否かの状態把握や、システムの構成要素に対する負荷を定量的(CPU 使用率、プロセス数、ディスク I/O 量、ネットワークトラフィック量等)に把握すること。監視方法はシステムの特性に応じて適切な方法を選択すること。	
	不正プログラム対策 （AT-2）	不正プログラムの感染防止　（AT-2-1）	不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施すること。	
		不正プログラム対策の管理　（AT-2-2）	不正プログラム対策ソフトウェア等の定義ファイルの更新状況を把握し、不正プログラム対策ソフトウェア等が常に有効に機能するよう必要な対処を行うこと。	

	セキュリティホール対策（AT-3）	運用時の脆弱性対策　（AT-3-2）	情報システムを構成するソフトウェア及びハードウェアのバージョン等を把握して、製品ベンダや脆弱性情報提供サイト等を通じて脆弱性の有無及び対策の状況を定期的に確認すること。脆弱性情報を確認した場合は情報システムへの影響を考慮した上でセキュリティパッチの適用等必要な対策を実施すること。 対策が適用されるまでの間にセキュリティ侵害が懸念される場合には、当該情報システムの停止やネットワーク環境の見直し等情報セキュリティを確保するための運用面での対策を講ずること。	脆弱性対策の実施状況は、月次で報告すること。
不正監視・追跡 （AU: Audit）	ログ管理（AU-1）	ログの蓄積・管理（AU-1-1）	情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログ（システムへのログオンや資源へのアクセスのロギング等）を取得すること。	ログが所定の要件通り、取得・蓄積されていることを確認すること。（年１回以上）
		ログの保護　（AU-1-2）	取得・蓄積されたログが不正な改ざんや削除が行われないようログの格納ファイルのアクセス権を制限する等必要な対策を講じること。	取得・蓄積されたログが不正な改ざんや削除が行われていなことを確認すること。（年１回以上）
		時刻の正確性確保（AU-1-3）	システム内の機器の時刻同期の状況を確認すること。	
	不正監視（AU-2）	侵入検知　（AU-2-1）	不正行為に迅速に対処するため、通信回線を介して所属するＰＭＤＡ外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知した場合は通信の遮断等必要な対処を行うこと。	
アクセス・利用制限（AC: Access）	主体認証（AC-1）	主体認証　（AC-1-1）	主体認証情報（ＩＤ、パスワード）は不正に読み取りできないよう保護すること。	
	アカウント管理（AC-2）	ライフサイクル管理　（AC-2-1）	主体が用いるアカウント（識別コード、主体認証情報、権限等）は、主体の担当業務に必要な範囲において設定すること。 また、アカウント管理（登録、更新、停止、削除等）の作業内容は記録し、証跡を保管すること。 アカウント棚卸を定期的に実施し、不要なアカウントを削除すること。	アカウント棚卸を定期的（年１回以上）に実施すること。
		アクセス権管理（AC-2-2）	主体が用いるアカウント（識別コード、主体認証情報、権限等）は、主体の担当業務に必要な範囲において設定すること。また、アカウント管理（登録、更新、停止、削除等）の作業内容は記録し、証跡を保管すること。 権限の再検証を定期的に実施し、不要な権限を削除すること。	ユーザーＩＤの棚卸と合わせて実施すること。

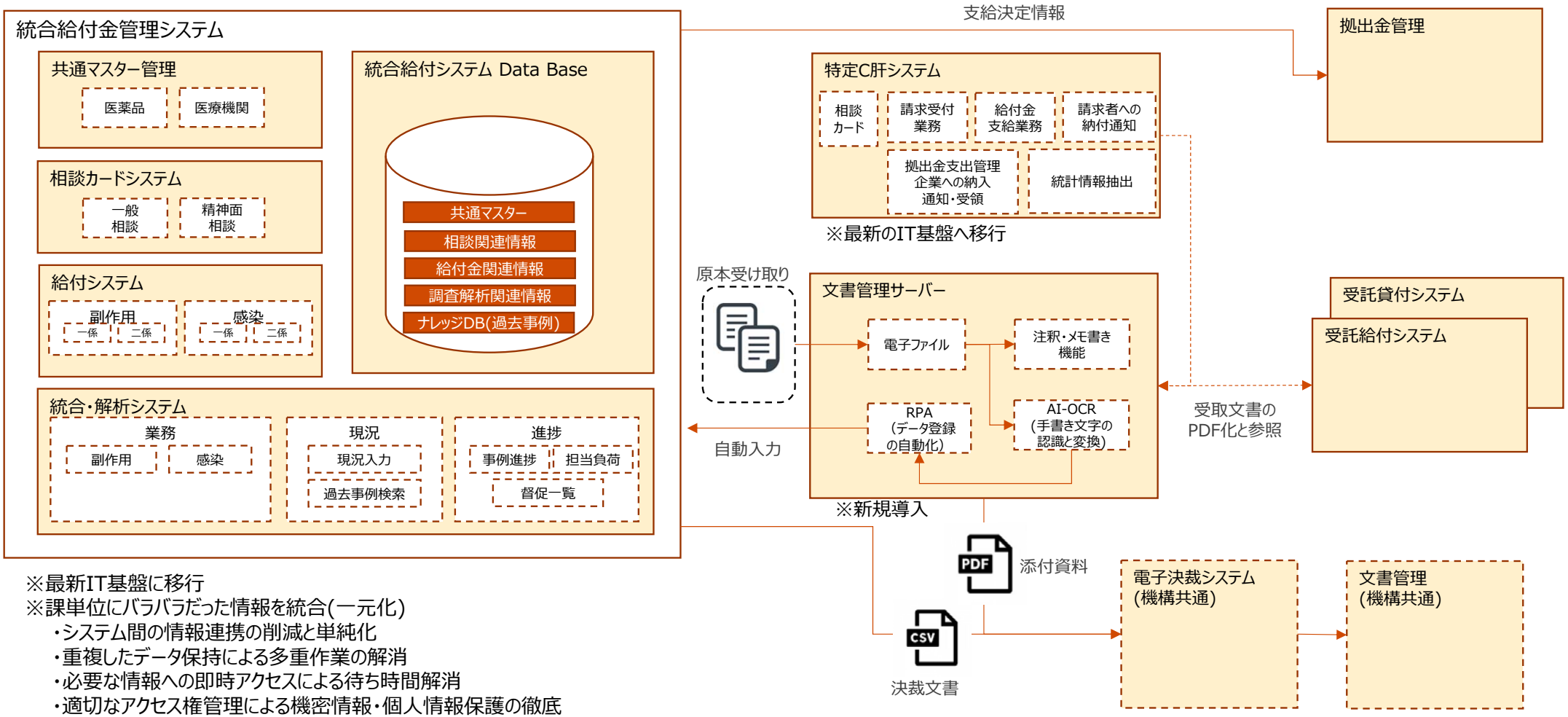
		管理者権限の保護（AC-2-3）	システム特権を付与されたアカウント及び使用者を特定し、アカウントの使用状況を記録し、アカウントの不正使用がないことを定常的に確認すること。	管理状況を「特権ＩＤ台帳」及び「特権ＩＤ使用管理簿」により、月次で報告すること。
データ保護（PR: Protect）	機密性・完全性の確保（PR-1）	通信経路上の盗聴防止 （PR-1-1）	通信回線に対する盗聴行為による情報の漏えいを防止するため、通信回線を暗号化する機能について、有効に機能していることを定期的に確認すること。	セキュリティヘルスチェック（各種セキュリティ設定の不正変更の有無、および不正操作の痕跡の有無の確認）と合わせて実施し報告すること。
		保存情報の機密性確保 （PR-1-2）	情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限すること。構成情報と実際の設定を照合し、所定の要件通りに設定されていることを定期的に確認すること。 また、業務データへのアクセス権限の付与状況を点検し、不要なアクセス権限が付与されていないことを確認すること。	ユーザーＩＤの棚卸と合わせて実施すること。
		業務データへのアクセス管理	情報の格付の見直し及び再決定が行われた際や、当該情報システムに係る職員等の異動や職制変更等が生じた際には、情報に対するアクセス制御の設定や職務に応じて与えられている情報システム上の権限が適切に変更されていることを確認すること。	ユーザーＩＤの棚卸と合わせて実施すること。
		受託者によるアクセス	受託者は受託した業務以外の情報へアクセスしないこと。	情報セキュリティ遵守状況は月次で報告すること。
物理対策（PH: Physical）	情報窃取・侵入対策（PH-1）	情報の物理的保護（PH-1-1）	受託者の管理区域において、受託者がＰＭＤＡより提供された情報を格納する機器は、情報の漏えいを防止するため、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。	情報セキュリティ遵守状況は月次で報告すること。
		侵入の物理的対策（PH-1-2）	受託者の管理区域において、受託者がＰＭＤＡより提供された情報を格納する機器は、物理的な手段によるセキュリティ侵害に対抗するため、外部からの侵入対策が講じられた場所に設置すること。	情報セキュリティ遵守状況は月次で報告すること。
		入退室管理の履行	ＰＭＤＡが管理するサーバ室、事務室等の管理区域への入退出については、ＰＭＤＡ入退室管理規程を遵守すること。 ＰＭＤＡの管理区域内での作業は、原則として、ＰＭＤＡ職員の立会いのもとで行うこと。	

障害対策（事業継続対応）（DA: Damage）	構成管理（DA-1）	システムの構成管理 （DA-1-1）	情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を実際のシステム構成と合致するように維持・管理すること。	変更作業時の構成管理資料の更新については、「変更作業一覧」により、月次で報告すること。
	可用性確保（DA-2）	システムの可用性確保 （DA-2-1） 情報のバックアップの取得	システム及びデータの保全が確実に実施されるため、システム及びデータのバックアップが所定の要件通りに取得されていることを定期的に確認すること。 また、回復手順について机上訓練を実施し、バックアップや回復手順が適切に機能することを確認する。	バックアップの実施状況は、月次で報告すること。 バックアップによるリストア等回復手順については、 机上訓練を年１回以上実施すること。
サプライチェーン・リスク対策（SC: Supply Chain）	情報システムの構築等の外部委託における対策（SC-1）	委託先において不正プログラム等が組み込まれることへの対策（SC-1-1）	情報システムの運用保守において、ＰＭＤＡが意図しない変更や機密情報の窃取等が行われないことを保証するため、構成管理・変更管理を適切に実施すること。	変更管理の状況は「変更作業一覧」により、月次で報告すること。

救済システムの構成（オンライン化含まず）

別紙6

○2024年に給付システム、統合・解析システム、相談カードシステムを対象に、稼働プラットフォームの再構築、ＤＢ統合、機能追加を実施。
併せて、特定C肝システムを対象に稼働プラットフォームの再構築を実施。



※最新IT基盤に移行
※課単位にバラバラだった情報を統合(一元化)
- ・システム間の情報連携の削減と単純化
- ・重複したデータ保持による多重作業の解消
- ・必要な情報への即時アクセスによる待ち時間解消
- ・適切なアクセス権管理による機密情報・個人情報保護の徹底

別紙7 ハードウェア一覧 （詳細構成は資料閲覧時にシステム設計書を確認すること）

システムコード	ハードウェア種別	製造元（ベンダー名）	ハードウェア		物理・仮想区分
			機器名称	システムモデル（型番・型式）	
HI-000	SVR	DELL	文書管理DBサーバ(本番)	PowerEdge R750ラック	物理
HI-000	SVR	DELL	文書管理DBサーバ(待機)	PowerEdge R750ラック	物理
HI-000	SVR	–	ライフサイクル管理サーバ	–	仮想
HI-000	SVR	–	ローコード開発基盤サーバ(開発機)	–	仮想
HI-000	SVR	–	ローコード開発基盤サーバ(検証機)	–	仮想
HI-000	SVR	–	ローコード開発基盤サーバ(本番機)	–	仮想
HI-000	SVR	–	文書管理サーバ	–	仮想
HI-000	SVR	–	バックアップ管理サーバ	–	仮想
HI-000	SVR	–	ログ管理サーバ	–	仮想
HI-000	SVR	–	運用管理サーバ	–	仮想

別紙7 ソフトウェア一覧 （詳細構成は資料閲覧時にシステム設計書を確認すること）

システムコード	製造元（ベンダー名）	ソフトウェア		
		ソフトウェア名称	エディション	バージョン
HI-000	Microsoft	Windows Server	Standard	2022
HI-000		Windows Server	Datacenter	2022
HI-000		SQL Server	Standerd	2022
HI-000			Express Edition	2019
HI-000		Microsoft Internet Information Services(IIS)	–	10.0.20348.1
HI-000		Microsoft .NET Framework	–	4.8
HI-000		Microsoft Build Tools	–	2015
HI-000		.NET Core	–	2.1
HI-000		Microsoft Visual C++ 2015 Redistributable Update 3	–	2015
HI-000		OpenSSL	–	3.1.0
HI-000	Oracle	Oracle Database	Standard Edition	19c
HI-000		OpenJDK	–	uild 11.0.17+8)
HI-000	PostgreSQL	PostgreSQL	–	–
HI-000	Apache	Apache Tomcat	–	8.5.84
HI-000	ゾーホージャパン	Op Manager	Professional Edition	12.7.198
HI-000	Arcserve	Arcserve UDP エージェント	–	9.0.6034
HI-000		Arcserve UDP コンソール	–	9.0.6034
HI-000		Arcserve UDP 復旧ポイントサーバ（RPS）	–	9.x
HI-000	infosense	Logstorage コンソール	–	9.1.0
HI-000		Logstorage LogGate	–	9.1.0
HI-000		Logstorage Agent ※ログ収集機能	–	9.1.0
HI-000		Logstorage SecureBatchTransfer（SBT） ※ログ収集機能	–	9.1.0
HI-000	ウィングアーク1ST	invoiceAgent 文書管理	rise（オンプレミス版）	10.9.1.2
HI-000	Outsystems	Outsystems	Standard Edition	11.27

別紙7 ソフトウェア一覧 （詳細構成は資料閲覧時にシステム設計書を確認すること）

システムコード	製造元（ベンダー名）	ソフトウェア		
		ソフトウェア名称	エディション	バージョン
HI-000	Trend Micro	Trend Micro Deep Security Agent ウイルス対策	-	20.0

別紙7 主なソフトウェア構成 （詳細構成は資料閲覧時にシステム設計書を確認すること）

	リモートデスクトップサーバ	DB	開発言語	フレームワーク
給付システム	Windows Server Datacenter 2022	SQL Server Standerd 2022	Outsystems 11.27(Standard Edition)	-
統合解析システム	Windows Server Datacenter 2022	SQL Server Standerd 2022	Outsystems 11.27(Standard Edition)	-
拠出金システム	Windows Server Datacenter 2022	SQL Server Standerd 2022	Outsystems 11.27(Standard Edition)	-

別紙８

資料閲覧について

1. 閲覧対象物

   健康被害救済業務システムに係る関連資料

2. 閲覧場所

   独立行政法人 医薬品医療機器総合機構内

3. 閲覧期間

   令和８年１月23日（金）から令和８年２月10日（火）までの平日（10:00～17:00）

4. 閲覧上の注意

   (1) 閲覧に際しては、5.閲覧連絡先に電話にて連絡し、社名・連絡先・人数等を登録すること。なお、3.閲覧期間の後半は閲覧場所を確保できなくなる場合があるので、早めに閲覧希望日時を登録すること。

   (2) 閲覧前に別紙様式に基づき秘密保持誓約書を作成し、捺印の上総合機構に提出すること。

   (3) 一回あたりの閲覧時間は１時間程度とする。閲覧回数は原則制限しない。

   (4) 閲覧時に個々の内容に関する質問に応じることはできない。

5. 閲覧連絡先

   独立行政法人　医薬品医療機器総合機構　健康被害救済部

   企画管理課　布施

   電話：03（3506）9460

別紙様式

独立行政法人医薬品医療機器総合機構　御中

秘密保持誓約書

貴機構における一般競争入札公告（健康被害救済業務システムの運用支援業務（以下「本件業務」という。）について、＿＿＿＿＿＿＿＿＿＿＿＿（以下「弊社」という。）が応札するため、現行システムを参照するにあたり、次の事項を遵守することを誓約いたします。

記

１．弊社は、媒体及び手段を問わずに貴機構から開示もしくは提供された貴機構の秘密情報（以下「本件秘密情報」という。）を、本件業務応札のため必要な者を除く第三者に対して開示しません。ただし以下のものについては秘密情報に含みません。

(1) 弊社が貴機構より開示を受けた時点で既に公知であったもの
(2) 弊社が貴機構より開示を受けた時点で既に所有していたもの
(3) 弊社が貴機構より開示を受けた後に弊社の責によらずに公知となったもの
(4) 弊社が正当な権利を有する第三者から守秘義務を負わずに適法に入手したもの
(5) 法令または裁判所の命令により開示を義務付けられたもの

２．弊社は、本件業務応札のために必要な者がそれ以外の者に秘密情報を開示しないよう、厳正な措置を講じます。

３．弊社は、本件秘密情報を本件業務のみを目的として使用するものとし、他の目的には一切使用いたしません。

４．弊社は、本件秘密情報を複写または複製いたしません。

５．弊社が本誓約書の内容に違反したことにより本件秘密情報が漏洩し、貴機構に損害が発生した場合には、貴機構に対してその損害を賠償いたします。
なお、賠償額については、貴機構と弊社にて別途協議して定めるものとします。

６．本誓約書は、本件業務終了後も本件秘密情報が機密性を失う日まで有効に存続することを確認します。

以上

年　　月　　日　　部長印

住　　所

社　　名

部 署 名

担当者氏名