仕　様　書

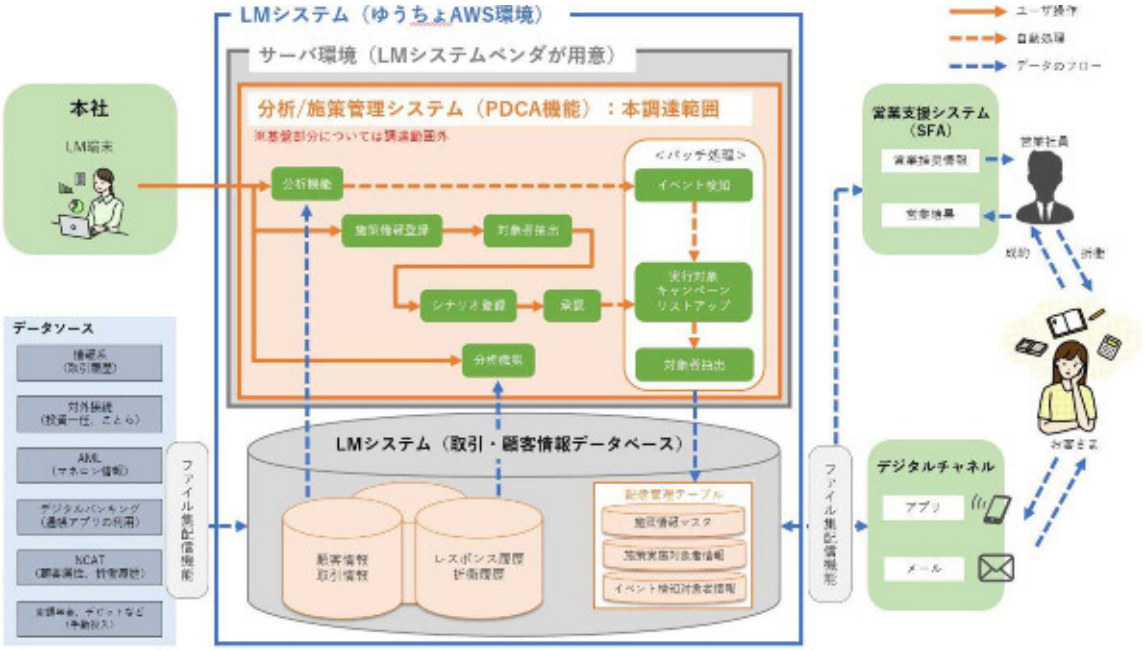
1　件名

マーケティングの高度化に向けた分析と施策管理に関わるツール等の更改
（Implementation and Maintenance of marketing PDCA tool）

2　目的

現行のPDCAツールは、導入から6年（１年間の保守延長対応を含む。）が経ち、2026年1月に更改を迎える。現在、稼働している施策や分析への影響を最小限にしつつ、システム更改を行いたい。

これまで、様々な顧客動向に対する時系列分析や高度な多変量解析等、分析に基づいた効率的な顧客ターゲティングをもとにした、施策を行っており、現在も稼働している施策が数多くあることから、顧客情報のDBは、Teradata Vantageを用い、稼働中の施策や分析への影響を最小限にしつつ、システム構築を行う。さらに、これまで蓄積されてきた分析結果や施策管理についても移行を行い、現行PDCAツールと同等の機能を有する必要がある。



3　本件業務の内容

(1) 要件定義の詳細化/基本設計/詳細設計/開発・単体試験/結合試験/総合試験/データ移行・現新比較

① 施策管理データマートの作成・管理

② 分析ツールの導入・構築

③ 施策管理ツールの導入・構築

④ ①～③を安定稼働させるために必要なインフラの構築依頼書の作成(サーバ/クライアント/ネットワーク等）、運用管理ツール等の導入及びシステム構築(非機能要求グレード）※

※　運用管理ツール等(サーバ監視、ジョブ管理、バックアップ)については、現行LMベンダにてJP1等を用いて対応するが、上記以外に運用管理ツールが必要となる場合は提案すること。また、実際の導入に際しては、営業部門デジタル戦略部リテールマーケティング室（以下「主管担当」という。）と相談の上、決定とする。

(2) 運用・保守/ユーザ研修・操作研修

それぞれの本件業務の内容の詳細については、別紙「仕様書詳細編」（別添及び別紙を含む。）のとおり。

4　本件業務の要件
別紙「仕様書詳細編」（別添を含む。）のとおり。

5　委託期間
契約締結日から2030年12月31日(火)

6　サービス開始日
2026年1月1日(木)

7　構築スケジュール及び作業分界
(1)　構築スケジュール
サービス開始日までのシステム構築スケジュールを、実現性があり、効果的な内容で提示する。
なお、想定している主なシステム構築工程は、要件定義の詳細化/基本設計/詳細設計/開発・単体試験/結合試験/総合試験/データ移行・現新比較/運用・保守/ユーザ研修・操作研修とする。

(2)　作業分界点
会社間（受託者/主管担当/LMシステムベンダ）における責任分界/作業分界点を提案すること。

8　契約形態

項番	作業名称	契約形態	作業分担 ※	
			受託者	主管担当
1	要件定義の詳細化	請負	●	○
2	基本設計	請負	●	△
3	詳細設計	請負	●	△
4	開発・単体試験	請負	●	△
5	結合試験	請負	●	△
6	総合試験	請負	●	△
7	データ移行・現新比較	請負	●	△
8	ユーザ研修・操作研修	準委任	●	○
9	運用・保守・	準委任	●	○

※　凡例　●：作業実施、○：作業支援、△：情報提供・レビュー・管理等
なお、主管担当に記載された「○」、「△」については、「承認」を含む。

9　導入までの想定スケジュール
2023年11月　意見招請公告
2024年４月　公告
2024年６月　提案書提出・契約

10　システム構築イメージ及び構築方針
別紙「仕様書詳細編」のとおり。

11　成果物及び報告物
成果物及び報告物として、別紙「仕様書詳細編」第5章のとおり納入するものとする。

12　納入場所
主管担当が別途指定する場所。

13　その他

(1)　本件業務の内容及び解釈等について、疑義が生じた場合又は特に必要がある場合は、事前に主管担当と協議し、決定・解決することとする。この場合、受託者は当該協議に係る議事録を作成し、主管担当の承認を得なければならない。

(2)　業務従事者に対する作業の指示、労務管理、安全衛生管理等に関する指揮命令は、すべて受託者の責任において行うものとする。

(3)　詳細については、主管担当(TEL 03-3477-2012)の指示によること。

-別紙_仕様書詳細編-

マーケティングの高度化に向けた分析と施策管理に関わるツール等の更改

ゆうちょ銀行

第 １．１ 版

２０２３年１１月

営業部門
デジタル戦略部 リテールマーケティング室

変更履歴

版	変更 年月日	担当者	変更箇所	変更内容	
				新	旧
1	2023/11/6	営業戦略室	初版作成		
1.1	2023/3/29	営業戦略室	4月の部署移動のため 所管部署を修正	営業統括部 営業戦略室	デジタル戦略部 リテールマーケティング室

目次

第1章　はじめに

第1節 用語集

本仕様書において使用する用語と用語の概要は表 1.1.1 のとおり。

表1.1.1　用語集

項番	用語	概要	備考
1	LM システム	ライアビリティ・マネジメントシステムの略。当行口座に関する多くの情報を保有し、ゆうちょ銀行の営業企画・推進管理において重要なシステムである。 ※取引情報等の総容量:108TB	ソフトウェア 現行 Teradata 更改後 Teradata Vantage Cloud Enterprise (バージョン:2.4.3 想定)
2	NCAT システム	ゆうちょ銀行の営業店社員が利用している営業支援システムのこと。	ソフトウェア Salesforce (force.com)
4	PDCA ツール	顧客動向に対する時系列分析や高度な多変量解析等、分析に基づいた効率的な顧客ターゲティングをもとにした、施策管理を行うツール	
5	東 KC	東日本計算センターの略。LM システムのデータ連携用のサーバを置いている。	

第2章　案件概要

第1節 背景と目的

1 背景

ゆうちょ銀行（以下「当行」という。）デジタル戦略部 リテールマーケティング室（以下「主管担当」という。）の所管する分析/施策管理システム（以下「現行 PDCA ツール」という。）の耐用期限到来に伴い、現在、稼働している施策や分析への影響を最小限にしつつ、2026 年 1 月に次のシステムへ更改を行いたい（更改後のシステムを、以下「次期 PDCA ツール」という。）。

2 目的

PDCA ツールについて、現在、稼働している施策や分析への影響を最小限にしつつ、システム更改を行いたい。

これまで、様々な顧客動向に対する時系列分析や高度な多変量解析等、分析に基づいた効率的な顧客ターゲティングをもとにした、施策を行っており、現在も稼働している施策が数多くあることから、顧客情報の DB は、Teradata Vantage を用い、稼働中の施策や分析への影響を最小限にしつつ、システム構築を行う。さらに、これまで蓄積されてきた分析結果や施策管理についても移行を行い、現行 PDCA ツールと同等の機能を有する必要がある。

第2節 目標

上記の目的を果たすため、本案件における目標を以下のとおり定める。

・更改後システムのリリース

2026 年 1 月から使用開始できるよう、稼働中の施策や分析への影響を最小限にしつつ、次期 PDCA ツールを導入する。

第3節 業務の概要

現行 PDCA ツールを用いて、実現している業務の概要について記載する。

1 業務内容

PDCA ツールを用いて様々な顧客動向に対する高度な多変量解析等を行っている。さらに、分析結果に基づいて、NCAT システムへ効率的な顧客ターゲティングをもとにした営業推進情報や、当行アプリに向けたお知らせ/広告配信などを行っている。また、その施策の効果検証も行い、ルール改善や新規イベントの追加等も行っている。

システム更改後も、上記フローを維持しつつ、チャネルの追加等に柔軟に対応できるようにする必要がある。

2 業務フロー

現行の業務フローの概要について、以下に図示する。また、更改後も以下の業務フローを継続できるしなければならない。

図 2.3.1　業務フロー

3 利用者特性

次期PDCAツールの構築に際し、以下の利用者特性に留意して、本件業務の実現方法を提案すること。

【前提条件】

・オンラインサービスの提供時間：　当行営業日 8 時～21 時
・対象ユーザ　　：　当行　本社　営業部門社員
・対象ユーザの人数　　：　現行 60 名　※第 4 章第 3 節に詳細を記載
・使用端末　　：　現行 LM システム専用端末　27 台
　現行の基本スペックは以下のとおり

OS	Windows 10 Pro　(64bit)
チップセット	インテル(R) Q670 チップセット
プロセッサー	Intel(R) Core(TM) i7-13700(16C/2.10GHz/30M)
Intel vPro	Intel vPro Essentials
メモリ	16GB (8GBx2) DDR4 DIMM 3200MT/s
ストレージ	512GB SSD (M.2 NVMe PCIe TLC)
ストレージ2	2nd ストレージなし

※2026 年 1 月に LM システムの更改を行うため、端末スペックは変更可能性あり。

第4節 体制

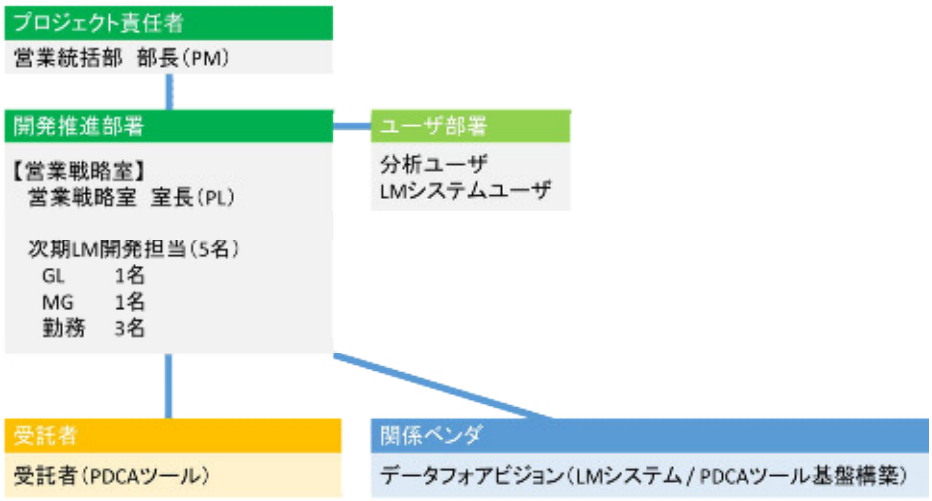
1 実行体制

本件業務はシステムの提供と利用を行う、主管担当に加え、データソースにあたるLMシステムを所掌している関係ベンダ等からなる体制の下推進する。

受託者は本件業務受託後、各工程において受託者名簿を作成し、提出するものとする。監査等の実施のため、当行から提示の要請があった時は、速やかに提示しなければならない。

合わせて、受託者は主管担当からの求めに応じて、関係ベンダに協力するものとする。なお、その際にかかる費用は原則今回調達の運用・保守に係る対価に含むこととするが、内容に応じて別途主管担当との交渉は可能とする。

図 2.4.1　体制図



第5節 スケジュール

1 グランドマスタスケジュール

現在想定するグランドマスタスケジュール（案）は図 2.5.1 のとおり。なお、実際のスケジュールの詳細は、受託者決定後、当該受託者の提案内容も踏まえ、主管担当にて決定する。提案する際には、サービス開始日までのシステム構築スケジュールを、実現性があり、効果的な内容で提案すること。なお、想定している主なシステム構築工程は、要件定義の詳細化/基本設計/詳細設計/開発・単体試験/結合試験/総合試験/データ移行・現新比較/運用・保守/ユーザ研修・操作研修とする。

図 2.5.1　グランドマスタスケジュール（案）

2 主要マイルストーン

本案件における主要マイルストーン（案）は表 2.5.2 のとおり。なお、実際のマイルストーンの詳細は、契約締結後、当該受託者の提案内容も踏まえ、主管担当にて決定する。

表 2.5.2　主要マイルストーン（案）

項番	マイルストーン	時期
1	要件定義の詳細化完了	2024年11月
2	基本設計/詳細設計/開発・単体試験完了	2025年６月
3	結合試験／総合試験完了	2025年11月
4	移行判定	2025年12月
5	サービス開始日	2026年１月

第6節 作業場所

1 開発拠点

顧客情報を確認できる環境を扱う場合には、当行本社 20 階にある LM システム専用室（以下「LM 室」という。）にて作業を行うこと。顧客情報を扱わない場合には、下記要件を満たす拠点であれば、別拠点での開発も可能。なお、LM 専用端末を利用したテスト・構築作業については、スケジュール等を事前に主管担当と調整の上、作業を実施するものとする。

※その際は、別途交付する主管担当におけるセキュリティマニュアルを遵守しなければならない。

ア 建物内への入退室管理、施錠、ユーザ認証等の物理的セキュリティ対策がとられている。また、コンピュータ室・データ保管室の出入口には入退室者を識別、記録する入退室管理設備を設置している。

イ 開発環境（ネットワーク環境含む。）はアクセス権限の管理及びアクセス権限等に応じた適切な ID 管理がされている。また、それに関する社内規程が整備されている。

ウ 開発環境にウイルス対策等のセキュリティ対策が実施され、定義ファイルやパッチ適用が最新状態に維持されている。また USB ポート等からの電子記録媒体への出力規制がなされている。脆弱性などに関する各ソフトウェアへのパッチ適用については、ユーザ部門と協議の上、適用要否を判断する。

エ 開発者による本番環境への誤接続、誤操作、及び担当者以外の操作を防止する仕組みを設ける。

オ プログラム等のサーバへのアップロード端末は開発環境とは別に用意し、本件専用とする。（用意できない場合は主管担当と協議のうえ代替案を提示するものとする。）

カ 情報漏洩等のセキュリティ対策を徹底する。

第7節 プロジェクト管理

1 プロジェクト管理

円滑なプロジェクト推進に向けて品質管理、進捗管理等とプロジェクト管理を行い、サービス開始までの間、以下の会議体に示す報告会を行うものとする。

2 会議体

本案件における会議体案を表 2.7.1 に示す。なお、実際の会議体詳細は、受託者決定後、当該受託者の提案内容も踏まえ、主管担当にて決定する。

表 2.7.1　本案件における会議体（案）

会議名称	開催周期	構成メンバー		取扱事項
		当行	受託者	
要件/仕様検討会	1 回/週	・主管担当	・PM 等	次期 PDCA ツールの詳細な仕様を決定する
進捗状況報告会	1 回/週	・主管担当	・PM	本システムの進捗状況や課題・リスク状況の共有しながら、その対応策を決定する
工程完了兼開始判定会議	工程終了/開始時	・主管担当	・PM ・PL	次工程に移行するに当たっての承認に関わる意思決定をする 当該工程の取組状況や次工程の申し送り事項を共有するとともに、申し送り事項については、その対応方法・時期について検討する
移行判定会議	全工程完了時	・主管担当	・PM	本システムの本格運用・リリースに関わる最終承認をする

※会議の都度、速やかに、受託者において議事録を作成し主管担当の承認を受けること。

第3章　委託概要

第1節 基本方針・実施施策

第 2 章第 2 節の目標を達成するための基本方針及び実施施策を以下に記載する。

＜基本方針及び実施施策＞

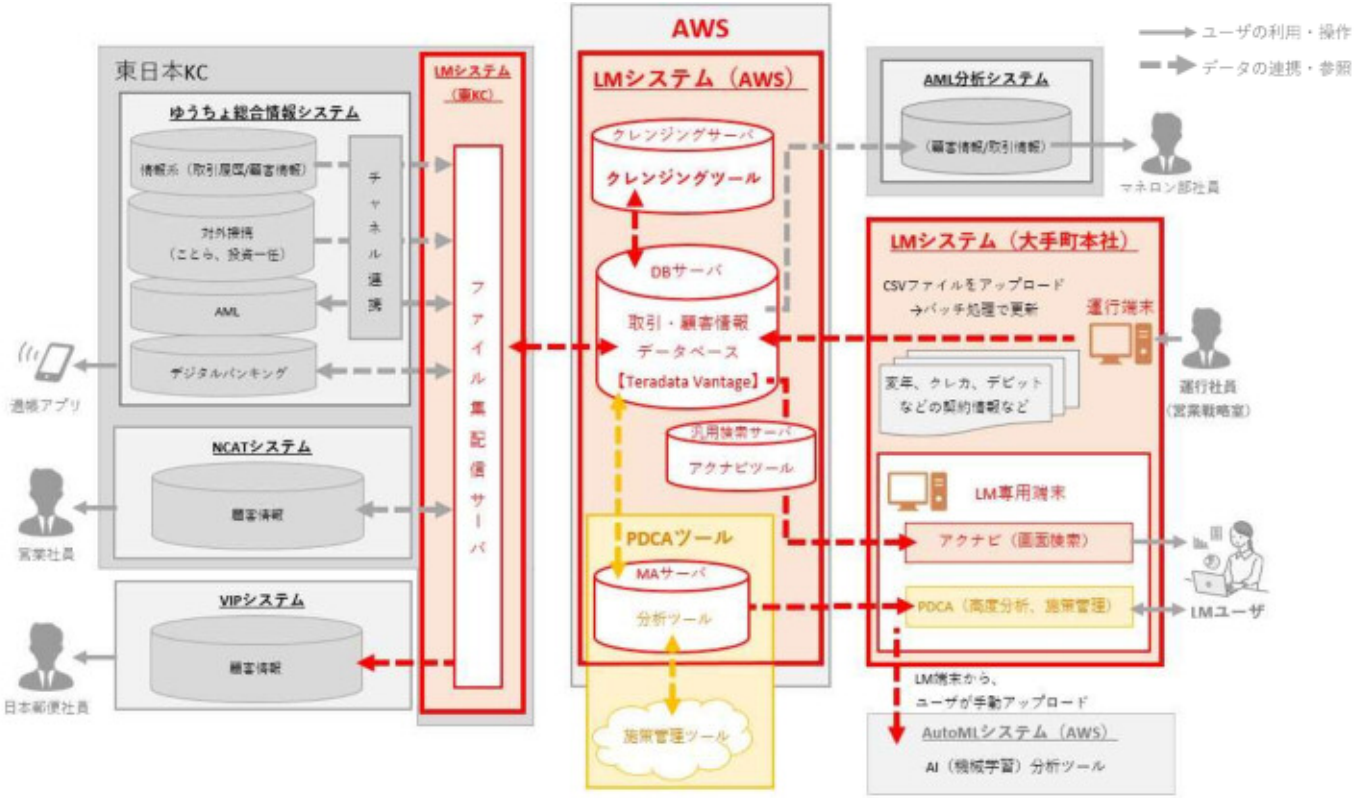
- LM システムが、クラウド上へ移行されるのに伴って、現行からシステム構成が変更されるため、それに合わせて更改対応を行う。その際、プログラムに手を入れるのは最小限にし、移行リスクを抑えて実施するものとする。
- 本案件は PDCA ツールのソフトウエアのみ調達対象とし、サーバ構築、LM 専用端末、運行端末、東 KC と AWS 東京リージョン間､AWS 東京リージョンと当行本社間の回線の調達に関しては別調達となる。
- LM システムの更改に伴い次期 PDCA ツールの対応が必要となった場合、主管担当や関係ベンダ等と協議、協力して対処すること。関係ベンダ側への質疑応答は主管担当にて取り次ぐ。
- 受託者/主管担当/関係ベンダにおける責任分界/作業分界点を提案するものとする。
  なお、受託者が別の外部事業者の提供する機能を使用してサービス提供をする場合、外部事業者が対応可能な責任範囲やサービスレベルについて要件を満たす製品/サービスを選択していなければならない。特に障害や保守対応におけるそれぞれの責任範囲やサービスレベルを明確にし、要件を満たしていなければならない。
- データソースは、LM システムを用いなければならない。
- 基盤は別途調達となるため、必要なスペック等を、契約後速やかに提示するものとする。
- 採用するパッケージ等市販の製品・部品、SaaS サービスは、以下の内容を考慮の上、継続的に拡張可能な仕組みとして設計・開発を実施するものとする。
  1. 独自の変更を最小限に止め、更改やバージョンアップの対応容易性を確保すること
  2. 先進的技術の採用にあたっては、短命化リスクのない、将来的な普及の見込みがあるものにすること
  3. 陳腐化・老朽化した技術や製品・ツール、SaaS サービス等の採用はしないこと
  4. 導入するシステムの利用期間以上にサポート期間があるものを採用すること
- 現行機能と同等で、顧客動向に対する高度な多変量解析、分析に基づいた効率的な顧客ターゲティングが行えるようにするものとする。また、現行資産は全て移行対象とし、次期 PDCA ツールでも正常に動くことを保証するものとする。
- ルールベースでイベント（顧客の大口入金、大口出金など）を検知し、セールスリードを NCAT システムに自動配信を行うため、検知したイベントと営業支援情報を LM システム向けに配信する。その際、条件の修正や新規施策の追加は、容易に可能とする。
- 将来的には、顧客コミュニケーション基盤としてマーケティング施策の実行を自動化する MA（マーケティングオートメーション）ツール・製品を整備し、マーケティングシナリオ（カスタマージャーニー）に基づいた、顧客へのアプローチの実施、各出力チャネルへの配信制御を行えるようにするものとする。
- 本システムで収集・分析した結果は、各配信チャネル（メール、SNS、SMS、アプリプッシュ通知、SalesforceFSC、WEB 接客ツール等）へ直接配信もしくは配信基盤と連携可能とする。ただし現在構築されていないチャネルもあるため、可能な限り、柔軟にチャネルを追加可能な構成となるよう考慮すること。
- 他社の特許等の権利を侵害しないものとすること。
- システム全体として当行セキュリティーポリシー及び FISC 等に準拠した個人情報保護を含め堅牢なシステム構築を行うものとする。

第2節 システム化の範囲

1 システム構成図

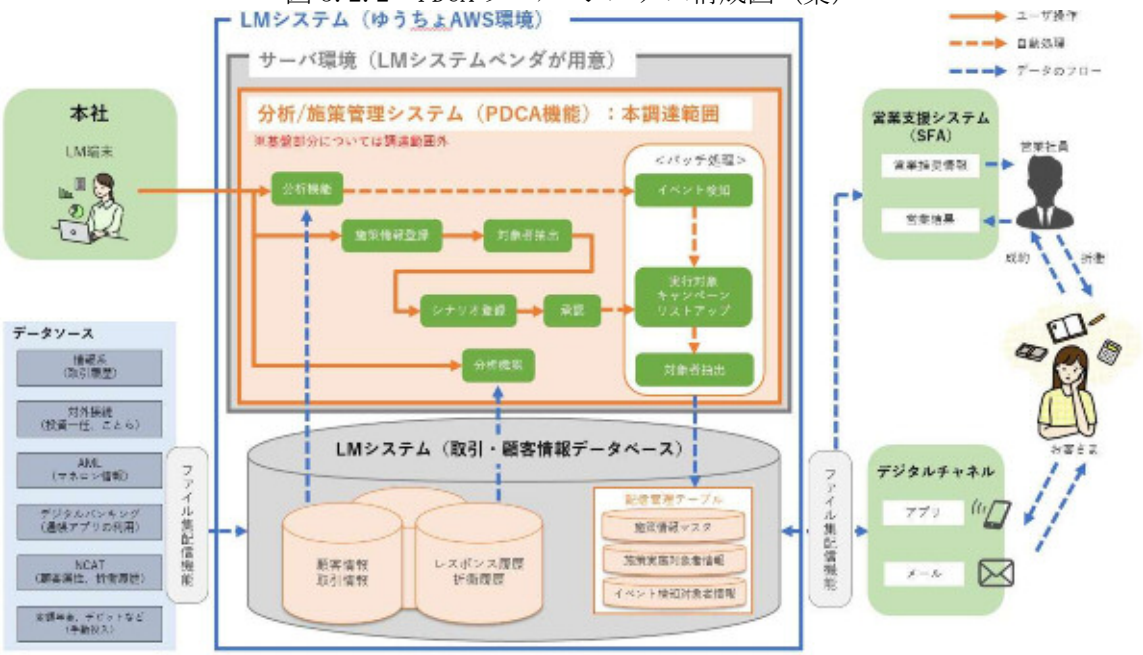
LM システム全体のシステム構成図を図 3.2.1 に示す。なお、本案件は PDCA ツールのソフトウエアのみ調達対象とし、サーバ構築、LM 専用端末、運行端末、東 KC と AWS 東京リージョン間、AWS 東京リージョンと当行本社間の回線の調達に関しては別調達となる。（黄色で記載した部分が本案件の調達範囲）

図 3.2.1　LM システム更改全体のシステム構成図



また、全体のシステム構成図のうち、本案件におけるシステム構成案を図 3.2.2 に示す。

図 3.2.2　PDCA ツール システム構成図（案）



2 システム構築における作業分界点

システム構築における作業分界点は以下のとおり。

（１）基盤は別途調達※となるため、必要なスペック等を、契約締結後、速やかに主管担当に提示するものとする。また、ユーザーデータ領域は、21TB（1 人当たり 0.5TB 程度）確保すること。

（２）LM システムに対する開発は別途調達となる。
LM 専用端末については、25 年 11 月ごろから LM 専用端末で更改後 PDCA ツールを使えるように設定作業を行うこと。（新端末 16 台、継続利用端末 11 台の予定）

（３）総合試験（日廻し運用）、研修あたっては、現行 LM システムベンダ及び NCAT システムベンダによる環境提供のもと、作業を実施すること。

※別途調達範囲は以下を想定。なお、実際の作業分界については主管担当と相談する。

・サーバの環境構築
・サーバ構築に伴う各種ネットワーク機器の構築／試験

第3節 委託期間及びサービス開始日

・委託期間：契約締結日から 2030 年 12 月 31 日（火）
・サービス開始日：2026 年 1 月 1 日（木）を予定

第4章　機能要件

第1節 共通事項

1 基本方針

- 次期 PDCA ツールの構築に当たっては、十分な実績があり、安全でかつ陳腐化しない技術を採用することを基本とする。
- オープン系サーバの OS は Redhat Linux 又は Windows を採用することを原則とする。左記以外とする場合は主管担当に報告の上、その依頼に従うこととする。
- 次期 PDCA ツール構築に用いるソフトウェア（OS、ユーティリティ、ミドルウェア、業務ソフトウェア）は、2030 年 12 月 31 日まで適切な保守サービスが受けられなければならない。
- 次期 PDCA ツールの運用期間終了までに保守サービス期間が満了する製品は、原則提案に含めないこと。ただし、提供製品が市場にない等のやむを得ない理由により、保守期限が調達時点で未定の製品を導入する場合は、PDCA ツールの提供するサービスに影響がないことを保証するとともに、主管担当と協議とする。
- 採用するパッケージ等市販の製品・部品、SaaS サービスは、第 3 章　第 1 節の記載に従い採用する。

LM 専用端末の画面 UI は WEB ブラウザインターフェースを利用すること。ただし WEB ブラウザインターフェースではない機能については、その妥当性を説明できれば、利用も可とする。

2 基本機能・役割

本案件において構築する主な基本機能は以下の 3 点。

表 4.1.1

No	機能	主な用途・役割
1	分析機能	・GUI またはコーディングによる統計処理、条件抽出などの汎用分析 ・分析結果をデータだけではなく、表・グラフ形式でも還元可能 ・外部データの取込、及び分析結果のエクスポートを画面上で実行
2	イベント検知機能	・GUI によるイベントロジックの事前分析・開発 ・イベント検知ロジックの生成・実装 ・画面上でバッチ処理登録を行うことによりイベント検知を定期実行
3	施策シナリオ管理機能	・施策シナリオ（誰に、いつ、何を、どのチャネル）の設計・実装 ・各種チャネルシステムへのリストの自動連携（日次/週次/月次/指定の営業日ごと/随時など） ・施策情報、ターゲットリストの一元管理

第2節 機能要件

本案件における機能要件は、以下のとおり。

1 システム要件

(1) 分析ツール機能要件

顧客分析を行うために必要な、以下の機能要件を満たすものとする。

表 4.2.1 分析ツール機能要件

No	機能観点	機能要件
1	LM システムへのダイレクトアクセス	LM システムにダイレクトにアクセスし、顧客を検索、条件抽出、データ加工、分析などが行えること。また、Teradata を単なるデータソースとするのではなく、以下の No.2～8 の機能を実行する際に、可能な限り処理エンジンとして有効活用すること。（一般的に In-Database 処理と言われる内容に相当）
2	LM システムの参照設定	LM システムのバッチ処理で作成されるテーブルについて、直接参照可能な設定を行うこと。ただし、ユーザが各々作るテーブル（加工領域）は参照対象外とする。また、LM システムは年４回、1 回あたり平均で 30 テーブルを前提とし、テーブルの項目追加や新規テーブル作成の開発を行うため、その都度柔軟に対応できるように、検討すること。
3	複数のデータソースへの対応	分析対象のデータソースとして、Teradata だけでなく、複数の RDBMS、SAS、Hadoop、各種ファイル形式（CSV、Excel、Access など）、外部データなど、幅広く対応できること。 （幅広いデータソースから、一旦、Teradata にデータを取込む機能でも可）
4	検索・集計処理	LM システム上のデータに対して、店番、顧客属性、取引明細等、多様な条件の組み合わせで複雑な検索・条件抽出ができること。 また、様々なキーを軸としつつ、要約統計量の算出（頻度、平均値、中央値、標準偏差、最小値、最大値等）及び軸を組み合わせた表分析（クロス集計）を実行できること。
5	ユーザーデータ加工処理	分析プロセスで新たに必要となるデータの作成にあたり、各種テーブルの横結合（JOIN）、縦結合（UNION）、集計、条件文による値の置換（CASE 式）、転置（縦横変換）、ランク化、データ項目間の数値演算や文字列処理等、分析の為のデータ準備作業ができること。
6	大容量・高速データハンドリング	LM システムにダイレクトにアクセスし、ユーザーデータ加工や新規ユーザテーブル作成処理を、高速に行えること。この際に、LM システムからデータダウンロードをせずに、Teradata 上でデータ加工処理を完結させる技術を有すること。また、LM システム外で作成したデータがある場合には、LM システム内に新規ユーザテーブルとして高速に書き戻し（作成・更新・削除）を可能とすること。 ※LM システムにある大容量データをもとに、高速にデータ加工する技術要素が必要不可欠

No	機能観点	機能要件
7	統計解析処理	一元度数表や分割表などの記述統計、t 検定などの分散分析、相関分析や回帰分析などの多変量解析、生存時間分析など、各種統計解析処理を実行できること。
8	データ加工・分析プロセスの可視化・共有	データ加工・分析プロセスのフローをアイコン等で表示し、可視化する等、作成者以外のユーザが処理内容を理解できること。また、複数ユーザ間でフローを共有できること。
9	ユーザビリティ	上記の No.1～8 の機能は、基本的にドラッグ＆ドロップ等の GUI 操作で実行できること。また、ユーザ操作画面はすべて日本語化されていること。
10	移行資産の互換性	現行 PDCA ツールの分析機能（SAS Enterprise Guide 7.15）で作成された資産について、次期 PDCA ツールに移行すること。また、その互換性を担保すること。

(2) 施策管理ツール機能要件

施策管理・自動実行を行うために必要な、以下の機能要件を満たすものとする。

表 4.2.2 施策管理ツール機能要件

観点	No	機能観点	機能要件
施策管理・自動実行	1	施策の一元管理	顧客アプローチを行う全施策・全シナリオについて一元的に管理する機能を有すること。
	2	施策の作成・更新・複製・削除	施策を作成・更新・複製・削除できること。特にオペレーションミス防止の観点から、過去実施した施策を複製し、抽出条件を修正することで新規施策を作成できる機能を有すること。
	3	施策の概要情報の登録・更新	施策に関する概要情報を柔軟にカスタマイズし、登録・更新可能であること。また、それら施策情報を LM システムに格納可能であること。 例）施策名、対象者の概要、施策分類、商品・サービス、実施チャネル、施策優先度、施策開始日（終了日）
	4	施策の一覧表示・検索	登録した施策を一覧表示し、必要に応じて施策の概要情報の各項目、施策の実施状況(ステータス）などで検索、照会できること。また、どの施策が実行中なのかを把握できること。
	5	分析ツールとの連動	全顧客のセグメンテーション結果、全顧客の購買スコアの予測結果等、各顧客の分析結果を、キャンペーン対象者の選出基準として施策管理ツールで利用できること。
	7	施策の顧客アプローチシナリオの定義	「施策の対象者抽出・除外」、「チャネル」、「コンテンツ」、「施策の実施期間」、「施策の自動実行登録」、後述する「マルチステップル、マルチチャネル」等のシナリオ設定を実施できること（タブによる複数画面でも可、ステップ毎に別のキャンペーンになって分断されるのは不可）
	8	施策対象者リストの作成	施策対象者のリストを作成するにあたり、施策 ID やその施策の内容、チャネル側への指示等（例：推奨商材やトークスクリプト情報など）、リストに追加する情報を柔軟にカスタマイズできること。

観点	No	機能観点	機能要件
	9	施策の実行スケジューリング	施策を手動、もしくは自動で実行できるようスケジュール登録（日次/週次/月次/任意の営業日ごと）し自動実行ができること。LM システムの標準スケジューラー（JP1：Automatic Job Management System3）と連携できること。
	10	マルチステップ､マルチチャネル	重点顧客に接触した後のフォローアップ､成約した顧客への架電等、施策に対する反応情報に応じて再アクションを取る場合（マルチステップ）に、顧客を再リスト化し、セグメントの特長に応じた施策実施チャネルへの割り当てを行える（マルチチャネル）こと。また、顧客それぞれの反応タイミングにあわせてフォローアップができること。
	11	権限管理	施策の閲覧・作成・承認などの権限をユーザ/グループ単位に柔軟に定義できること。また、ユーザごとに使用できるデータを制限する機能があること。
	12	施策の承認･ワークフロー	施策実施や顧客アプローチシナリオの設定内容が適切であることをダブルチェックするための承認・ワークフロー機能を有し、承認された施策のみ実行が可能な仕組みであること。 また、承認者が承認後に申請者が施策の設定内容を改変できないような仕組みを有すること。
	13	LM システムでのデータ一元管理	施策マスタや施策実施履歴、イベント履歴、顧客へのコンタクト履歴や顧客レスポンス履歴など、施策管理に関するすべての恒久データを LM システムで一元管理できること。
	14	イベント閾値算出	入金系イベントであれば「【××円以上の入金】をイベント発生とみなし、クロスセルを実施」等、イベント指標とイベント抽出条件を詳細に定めるために、イベント発生と成約率の関係を分析した上で、最終的なイベントの閾値（【××円】）を決定できること。
	15	時間イベント	「定期満期まで 60 日」、「住宅ローン借り入れ後 5 年経過」、「誕生日」等、特定時点に到ったタイミングの顧客を検知できること。
	16	属性変更イベント	「住所変更」、「公共料金、給振りの追加」、「金融商品の新規口座開設」等、顧客属性、取引属性に変更のあった顧客を検知できること。
	17	動態変化イベント	「××円以上の入出金」という単純な条件だけでなく、「その顧客の過去の平均に加えばらつき等の各種統計量を考慮した際の異常値と考えられる入出金」、「口座の休眠化」等、取引の動きに急激な変化のあった顧客を検知できること。
	18	イベント検知自動化と施策管理ツール連携	イベント条件に該当する顧客を自動検知し、検知された顧客を施策管理ツールにシームレスに連携しキャンペーン対象としてリスト抽出できること。

観点	No	機能観点	機能要件
	19	施策の対象者の条件抽出	LM システムにダイレクトにアクセスし、顧客属性情報だけでなく、取引実績（例：過去 1 年間で普通口座の残高増が〇万以上など）、顧客分析結果（例：「リスク許容派セグメント」等）など複数の条件の組み合わせ（AND/OR)による対象者抽出を設定できること。過去の施策履歴を参照し、日次での差分抽出ができることを必須とする。 また、以下の３つのカテゴリーの抽出条件を組み合わせた抽出ができること ①ルール抽出 ・事前に定義したルールに基づく条件抽出 ・ルールを作成・保存・複写する権限をユーザ単位で設定 ②個別抽出 ・ユーザが施策の都度設定（ルール化されない条件での抽出） ③イベント検知連携 ・イベント設計・検知機能との連携によるリスト抽出
	20	推奨商品割当最適化	各イベントと商品成約の関連性の分析結果を踏まえて特定の商品成約確度の高い顧客を検知できること。 （例） 投資信託の成約確率が XX%以上 等
	21	施策の対象者(セグメント）の除外条件	以下の３つのカテゴリーの除外条件を組み合わせたセグメント抽出ができること。 ①必須除外 ・事前に定義したルールに基づく条件を除外 ・システムで強制適用する顧客コンタクトポリシー ・ユーザは変更不可 例）貸金系施策は 6 か月に 1 回、E メールは 1 週間で 1 回まで等 ②ルール除外 ・事前に定義したルールに基づく条件を除外 ・ルールを作成・保存・複写する権限をユーザ単位で設定 ③個別除外 ・ユーザが施策の都度設定（ルール化されない条件での抽出）
	22	施策横断での除外制御	各施策横断で対象者リストを照合し、同一種類の施策の二重実行、もしくは同一チャネルからの施策の二重実行が発生しないよう不要な顧客をリストから除外し、除外履歴を LM システムに保管できること。横断的なポリシーの変更などがユーザ自身でできること。 例）営業からの重複架電やダイレクトメールの二重送付の防止
	23	チャネルキャパシティ制御	営業やコールセンターなどの人的チャネルでこなせない数の顧客が割り当てられないように設定ができ、施策横断でチャネルのキャパシティが制御できること。キャパシティをオーバーした顧客が対象者として抽出された場合は、人的チャネル以外のチャネルに自動的にカスケードできること。
	24	大容量･高速データハンドリング	セグメント抽出・除外やリスト作成、各履歴管理の処理を、高速に行えること。この際に、LM システムからデータダウンロードをせずに、Teradata 上で処理を完結させる技術を有すること。（部分的に Teradata の外で処理する部分があっても良いが、該当箇所の処理内容と影響について明示すること） LM システムにある大容量データをもとに、高速にセグメント抽出・除外し、リスト作成や履歴管理する技術要素が必要不可欠

観点	No	機能観点	機能要件
	25	施策の対象者(セグメント）の検証	設定した抽出・除外条件の正しさを検証するために、その時点での対象者件数の把握、抽出や除外に使用した項目の統計情報や、対象者リストを出力し、リストが適切に抽出されていることをユーザ自身が確認できること。
	26	施策の非対象者(コントロールグループ)	施策の対象者（セグメント）から、効果検証を行うための非対象者（コントロールグループ）を件数や比率を指定し作成することで、モニタリング･効果検証機能での両者の比較評価に活用できること。
	27	ユーザビリティ	上記の No.1～26 の機能は、基本的にドラッグ＆ドロップ等の GUI 操作で実行できること。また、ユーザ操作画面はすべて日本語化されていること。 GUI で操作できない機能については別途記載すること。
チャネル	1	実施チャネル	施策を実施するチャネルは、当行の NCAT システムと通帳アプリ（FANSHIP を使ったお知らせ配信）とし、現システム同様、日次ファイル連携による連携方式とする。 また、それぞれのチャネルに対して、以下の情報を配信できること。 ・「イベント情報」、「推奨アクション（推奨商品）」など顧客を理解する情報及びそれらの詳細情報（イベント発生条件やトークスクリプト）
	2	新規チャネルの追加	26.1 リリース以降、上記のチャネルに加え、ダイレクト契約者に向けたメール配信も行えるようにする施策を検討中のため、実施チャネルの追加に柔軟に対応できる設計とすること。 なお、本機能は今回の調達範囲外とする。
マスタ	1	施策管理データマートの作成・管理	施策管理に必要な以下の情報を LM システム内にテーブルを作成するための仕様・設計情報を明示すること。 （イベント検知履歴、施策マスタ、施策実施履歴、チャネル I/F 情報、施策除外履歴など）

(3) 拡張性機能要件

以下の機能要件を満たすものとする。なお、可能な限り今回提案するパッケージの拡張機能で提案すること。異なるパッケージ製品（別製品）の場合は、今回提案するパッケージとの連携方法を明示すること。また、拡張要件は本件業務に含まない。

表 4.2.3 拡張性機能要件

No	機能観点	機能要件
1	チャネル拡張性	施策を実施するチャネルは、将来的には、当行のホームページやインターネットバンキング、アプリへのコンテンツ出し分け配信及び SMS 等への拡張を検討している。それらのチャネルへの拡張性を有すること。
2	マルチチャネルでのシナリオ一元管理	上記すべてのチャネルでの施策や顧客アプローチシナリオを一元管理し、それらデータを LM システムで一元管理できる拡張性を有すること。
3	マルチチャネルでのデータ一元管理	将来的に、上記すべてのチャネルでの施策の対象者抽出や顧客のコンタクト/レスポンス履歴データを、データを原則 2 重持ちすることなく当行 LM システムにダイレクトアクセスし、LM システムで一元管理できる拡張性を有すること。なお、最低限のデータ重複を可能とするが、変更・削除等のデータ改修は一元的に実施できること。

No	機能観点	機能要件
4	リアルタイムの施策実行	Web やアプリにおける顧客の行動を捉え、リアルタイム（行動発生から数秒程度を目標）に各配信チャネルへ配信を可能とすること。 また、各チャネルを横断したコミュニケーションを可能とすること。
5	パーソナライズ	Web やアプリにおける顧客の行動履歴等から、顧客の嗜好を分析し、パーソナライズコンテンツを配信すること。

2 運用・保守委託要件

受託者は、本システムの安定的な稼働を確保するため、システム運行管理及びシステム運行管理に必要な各種サービスを実施する。

(1) 本件業務の内容等

受託者は、システムの保守として、以下のサービスを提供するものとする。

① システム利用等に関するユーザ問合せ窓口を設置する。
② 障害対応（原因調査、対応方針検討、障害履歴管理等）。
③ 不具合対応、リリース前テスト・ライブラリ管理。
④ 機能拡張、仕様変更に関する相談・サポート（機能拡張、仕様変更に関する作業は含まず）サービスイン後に追加開発等が発生する場合は、今回調達範囲外とし、別途契約更等で対応するが、その際、受託者は主管担当の依頼に応じて追加開発に係る費用明細を速やかに作成、提供する。
⑤ パッケージソフトのバージョンアップ対応を実施する。なお、バージョンアップに係る作業費用等、バーションアップに関する総費用は今回調達範囲に含むものとし、対応可能な範囲を提案とするものとする。なお、対応可能な範囲を超える対応回数、対応規模であった場合は、内容に応じて別途主管担当と調整できるものとする。また、実際のバージョンアップに関しては主管担当と協議の上実施する。
⑥ スクラッチ開発が発生する場合は、スクラッチでの開発範囲に対する保守内容（作業/頻度等）を提案すること。なお、スクラッチ開発部分の保守に要する費用は本契約金額に含むものとする。
⑦ LM システムは年４回ほど、テーブルの項目追加や新規テーブル作成の開発を行うため、その都度、LM システムの参照設定を行うこと。合わせて、自動実行している分析に影響がないか調査も行い、懸念事項がある場合には主管担当へ報告する。
⑧ ゴールデンウィークや正月など、上流システムから LM システムへのデータ連携が停止されるタイミングがあるため、LM の追いつき処理に合わせて、追いつき対応を行う。
⑨ システムリソース、サービスリソース両者のリソース状況を監視の上、管理する。なお、SaaS の場合サービス提供側の仕様に準拠するものとする。監視において、サービス提供に影響を与えうる異常を検知した場合には、速やかに主管担当へ報告を実施しなければならない。
⑩ システムの構成要素(当行提供サービスに使用する OS や WEB アプリケーション等)の製品名、バージョン、サポート期限（EOL。製品提供元のサポート等提供期限）について、管理台帳を作成し、最新の状態となるよう EOL 情報の取得及び台帳の都度更新を行うとともに、最低年次で更新漏れがないこと、及び、原則として EOL 到来製品の使用がないことを確認すること（原則、委託期間中を通じて保守サービスの提供される製品を使用すること。ただし、やむを得ない事由により継続使用する場合は、継続使用によるリスクも考慮の上、受託者社内基準に従い継続して利用できることの判断が責任者によりされていること）。

主管担当より上記の管理台帳について提出の依頼があった場合、受託者は速やかに管理台帳を提出、もしくは EOL 管理作業について適切に実施していることを示す証明書等の提出を行うこと。証明書等を提出する場合は、当行所定の様式に従うこと。

(2) 保守サービス提供時間帯等

受託者は以下の時間帯における保守サービスを提供すること。

① 原則営業日の９時から１８時とし、電話及びメールでの問合せ対応とする。
② 受託者は、主管担当等からの障害発生報告等により、障害等発生の事実を確認した場合は、主管担当の依頼により速やかに復旧修理を実施すること。
③ 受託者からの申し入れにより、新たに作業等を行う必要が生じた場合の料金は本契約金額に含まれるものとする。
④ 上記①に示すサービス提供時間以外に受託者がサービスを提供する場合、及び主管担当からの申入れにより受託者が新たに作業等を行う必要が生じた場合の料金は、本契約金額に含まれないものとし、主管担当と受託者はその金額について別途協議するものとする。

(3) 保守等報告

受託者は、本契約に基づいて保守等の実施状況を、月次運用・保守報告書（様式適宜）を作成し、月１回主管担当あてに提出すること。

第3節 非機能要件

1 非機能要件

(1) 基本方針

以下の（2）～（4）要件を満たすように設計を行うこと。ただし、基本的にはLMシステムの性能に準拠する。記載されている観点以外の部分については、仕様書詳細編「別添１_非機能要求グレード」に示す。

(2) 規模・性能要件

以下の利用者数、業務量等に耐えうる業務効率を損なわないオンライン画面処理を確保すること。

・ 規模要件

ア 利用者数・拠点数

PCの利用者数は、以下のとおり。次期PDCAツール稼動時(2026年度)より、5年間の利用に耐えうる利用者数を想定して設計すること。(小数点第一位四捨五入)

表4.3.1-1 利用者数（単位：人 ※最終的に1.5倍となる想定）

利用者	2026年度 (現行と同等)	2030年度 (見込み)
システム運行担当者（内 承認者）	15 (5)	15 (5)
分析・施策実行担当者	45	75
合計	60	90

拠点は、本社の1拠点を考えている。

イ 需要予測（顧客規模・業務処理量）

参考として、各配信チャネルの需要予測（顧客規模・業務処理量）を以下に示す。業務処理量について、2026年度の稼動後5年間の増加を想定すること。

表4.3.1-2 各配信チャネルの需要予測(2023年10月時点)

No	分類	2023年度 (実績)	2026年度 (見込み)	2030年度 (見込み)	備考

1	渉外社員	渉外社員 約 2,000 人 対象顧客 1,500 万人	―	―	
2	通帳アプリ	会員数 約 900 万人	会員数 約 1,089 万人	会員数 約 1,595 万人	中期経営計画の目標 KPI(2025 年度 1,000 万人)より、前年比の 10%会員数増加を想定
3	ゆうちょダイレクトのメール	約 1,000 万人	―	―	

ウ　アクティブ顧客数

当行のアクティブ顧客数は、以下のとおりとなる。

表 4.3.1-3　アクティブ顧客数（単位：千万人）

顧客数	2021 年	2022 年	2023 年	2030 年見込
アクティブ顧客	7.05	7.04	6.97	6.7
全量(解約･休眠を除く)	10.08	10.06	10.04	9.9

・　性能要件

ア　バッチ処理

登録されているバッチ処理のボリュームによるが、現行のバッチ処理を移行した場合 LM システムのバッチ処理後、2 時間以内で完了する（5：00～8：00 で完了する）ことを目標とする。なお、オンラインサービス提供時間は、8:00～21:00 を予定している。

イ　オンラインの性能

LM システムのデータベース上の約 1 億件の顧客マスタ（155 変数、約 2,000Byte）のインプットデータを対象とした場合、以下の表 4.3.2 に示す分析処理ごとの同時操作数と性能目標を満たすハードウェアを導入するために、必要な機器のスペックについて契約締結後速やかに提出すること。また、画面レスポンスタイムは指定しないが、業務に支障をきたさないレベルの性能は保証すること。

表 4.3.2 分析ツールの性能要件

No	処理	備考
1	データ加工・集計	顧客マスタの全件を読み込み、SQL にて 6 つの量的変数の集計を行う ・同時操作数 5, 性能目標 30 分
2	要約統計量の作成	2 つのカテゴリー変数の各カテゴリー値の組み合わせごとに 4 つの量的変数 を分析対象として要約統計量を算出する ・同時操作数 5, 性能目標 30 分
3	一元度数表の作成	カテゴリー変数 1 つ使用し、一元度数表を作成する。 ・同時操作数 5, 性能目標 30 分

(3) 可用性・信頼性要件

基本的には、LM システムに準拠することとなるが、以下の点を目標とすること

・ 可用性

- 稼働率(計画停止時間を除いた月当たりの運用時間を測定し、稼働比率で示した値)は、99%以上を目標とする。
  なお、SaaS の稼働率については、サービス提供側の稼働率に準拠するものとするが、上記目標とする。
- 運用時間（サービスを提供する時間帯を示す。ただし、計画停止時間は、含まない）は、24 時間 365 日とし、オンラインサービス提供時間は、当行営業日 8:00-21:00 とすること。

※計画停止時間とは、GW や年始などの上流システムが停止する時間をいう。

- データ処理要求をシステムで受け付けてからの処理応答時間については、システムの特性、業務内容等を鑑み、提案すること。
- 特定の配信チャネル、入力チャネルに障害が起こった際、他配信チャネルは、通常通り配信が継続できるように、配信チャネル間の独立性を確保できるようにすること。
- 定期的に計画されている保守に伴うシステム停止予定通知について、システムの特性、運用保守体制・業務内容等を鑑み、効率且つ有効な事前連絡方法（事前通知のタイミング／方法の記述を含む）及び通知期限等を提案すること。
- 他システムとの連携含め、障害にはアラートを送出し、システム運用担当者に通知可能なシステムであること。サービスに影響する障害発生時の、システムの特性、運用保守体制・業務内容等を鑑み、通知プロセスと連絡通知時間について確認すること、又は要件を提示すること。
- 障害が発生した場合、障害発生から本格復旧までの間、その後も適宜、対応状況（発生時刻/復旧時刻、障害内容、障害原因、復旧作業内容・措置、再発防止策等）を主管担当へ報告すること。

・ 復旧時間

- 障害時の回復時間を短縮し業務への影響を少なくするための考慮を行うこと。
- 重大障害等によりシステムの早期復旧が不可能な事態が発生した場合に、業務を続行するために、自動且つ定期的に実施できるバックアップの仕組みを備え、バックアップデータの早急な提示が可能な代替措置(CSV、Excel 等データ形式の提示含む)を提案すること。
- システム障害が発生してからサービスが復旧するまでに要する目標時間として、24 時間程度とする。目標復旧地点としては、1 営業日前の時点まで復旧する。なお、SaaS の場合サービス提供側の復旧時間に準拠するものとするが、上記目標とすること。

2 セキュリティ要件

セキュリティ対策としては、受託者が最新の情報セキュリティ対策を収集し、金融機関として有効な対策については、主管担当と協議の上、設計・開発すること。なお、本システムに必要となる対策の具体的な範囲、実施内容等については、契約締結後、当行による承認を経て決定するものとする。なお、SaaS の場合サービス提供側の仕様に準拠するものとし、以下に記載されている対応が難しい場合には、同等のセキュリティが担保できる代替案を主管担当へ提示し、協議の上対応するものとする。

(1) 機密性担保

機密性を担保するために適切なセキュリティ対策がなされていること。

(2) セキュリティ診断

ア セキュリティ診断

受託者は、本契約で構築するシステムがセキュリティ要件を満たしている事について、原則、別添４「診断企業要件」に記載する要件を満たす第三者によるセキュリティ診断（WEB アプリケ

ーション診断、ネットワーク診断等）を実施し、実施結果（修正対処後の再診断含む。）をサービス開始前までに主管担当に報告し、承認を得ること。

セキュリティ診断は、サービス開始前に加え、最低１年に１回程度定期的に実施し、機能追加等の変更が行われた際にも当該機能のサービス開始前までに診断及び必要に応じた修正を実施し、実施結果を主管担当に報告し、承認を得ること。なお、診断対象の変更により費用が変動するため、セキュリティ診断を実施する都度、別途見積りとし、今回の調達では、サービス開始前のセキュリティ診断のみを対象とする。

セキュリティ診断の実施にあたっては、システムの仕様に応じ必要な診断項目や検証パターン数、実施方法等が異なるため、リクエスト数やデータフロー等の仕様が確定した後、診断の項目及び実施方法について主管担当に説明し、承認を得ること。また、診断の項目については別添５「セキュリティ診断実施項目」を満たすこと。

セキュリティ診断において重大な脆弱性が判明した場合、又は、主管担当が問題と認識した場合は、原則サービス開始前に修正及び再診断を実施し、当該脆弱性が解消されたことを示す再診断結果等を主管担当に報告し、承認を得ること。

当行の責任範囲においては、上記のとおりセキュリティ診断を実施すること。

なお、クラウド（ASP）業者の責任範囲においては、当行のためにセキュリティ診断を実施できない場合、報告書等（別添６「各種証明書」）によりセキュリティ診断の実施を主管担当へ報告すること。

報告書等の提出が難しい場合は、セキュリティ診断実施と同等のセキュリティを担保していることを証明する書類（SOC2 レポート、PCIDSS 準拠証明書等）を主管担当に提出することにより、代替を可とする。

イ ファイアウォールの設定検証

当行の資産としてファイアウォール（同機能を持つ UTM 等も含む。）を設置した際は、実際のファイアウォールの設定値(コンフィギュレーションリスト・アクセスコントロールリスト等)が設計書（設定値を記載したドキュメント）どおりになっていることを定期的（四半期ごと）に検証し、前年度の結果を取りまとめて年に一度、4 月末までに報告すること。また、当行用のファイアウォールの設定値もしくは設計書を修正した際は、その都度、当行に修正内容を報告すること。

当行の資産でないファイアウォール（同機能を持つ UTM 等も含む。）を設置した際は、当行へのサービス提供にあたり、サービス利用時に経由する通信経路上にあるファイアウォールについて、受託者は設計書どおりに設定されていることを定期的(年 1 回以上)に確認し、証跡もしくは報告書等（別添６「各種証明書」）により確認結果を当行へ報告すること。

報告書等の提出が難しい場合は、当行が求めるセキュリティ水準と同等のセキュリティを担保していることを証明する書類（SOC2 レポート、PCIDSS 準拠証明書等）を主管担当に提出することにより、代替を可とする。

(3) IT 資産情報

受託者は、当行資産として導入する機器・ソフトウェアがある場合、主管担当より別途提示するフォーマットに従い、サービスインの 3 か月前を目途に、該当機器の IT 資産情報を記入し、提出すること。具体的な提出時期は、主管担当の決定に従うこと。なお、別途提示するフォーマットのイメージは別添７「IT 資産情報ヒアリングシート」のとおり。

受託者は、上記で提出した資料について、主管担当からの依頼に従い、適宜記載内容の修正を行うこと。また、サービスイン後に機器変更、もしくは使用するソフトウェアの変更等、IT 資産情報に変更が生じる場合は、速やかに主管担当に報告するとともに、別途提示するフォーマットに記入し、提出すること。

(4) アクセス・利用制限

システム利用者を識別するための認証を実施すること。今回調達範囲において、一般ユーザとは別にアクセス権限の違う管理ユーザを作成可能なこと(アカウント作成､パスワード設定等を可能とする ID)。

故意または過失によるファイルの破損、または不正アクセスからデータを保護するため、重要なファイルについては、ソフトウェアによるアクセス制御機能を設けること。

アカウントロック及び営業時間外のアクセス試行等を検知した場合、当該ログを取得し、１年間保管すること。

通常使用する時間帯以外はアクセスを停止（遮断）すること。なお、「通常使用する時間帯」についてはシステムの特性、業務内容等を鑑み別途、主管担当と調整すること。

各サーバにおいて、特権 ID（OS 及び DB の管理者権限（root/admin 等権限））の使用履歴（成功時及び失敗時）を取得し１年間保管すること。

各サーバまたは認証ログを管理するサーバにおいて、アクセスログを取得し、１年間保管すること。

保守運用員、当行社員によるシステムへのアクセスにおいて、認証に一定回数失敗した場合のアカウントロック機能を実装すること。

ユーザが操作したログを取得できること。また、不正アクセスを早期に発見するため、アクセスの失敗及び不正アクセスを監視する機能を設けること｡アクセスの失敗を監視する機能として、業務アプリケーションに以下のものを設けること。

1. アクセス履歴※を取得し監査証跡として 1 年間保管する機能。
2. 連続した何回かのアクセスの失敗に対しては、アカウントロック等を行う機能。
3. ログオンしたまま一定時間操作が行われない場合のセッションタイムアウト機能。

※アクセス履歴とは次のような履歴を指す。

①ログインとログオフ状況(時刻、ID など)
②不正なアクセス要求(時刻、ID)
③システムによって失効とされた ID
④システムにログインしたまま一定時間操作が行われず、強制的にログオフされた ID
⑤特権 ID の利用履歴（成功時及び失敗時）
⑥厳秘、機密情報の閲覧・取得（DL 含む）及び持出した記録

なお、上記 1～3 についてはクラウド（ASP）サービスの機能に実装されていない場合、当行と協議の上、運用での対応も含めた同等レベルの代替案を提示し承認を得ること。

合わせて、アクセス履歴を定期的にチェックしてサービス利用者が正当なアクセスなのかどうかを調査すること。不正アクセスの拡大防止のため、対応策、復旧手順を明確にするとともに、不正アクセスが発生した場合は、原因を分析・主管担当へ報告した後、主管担当の承認のもと再発防止策を講ずること。

監査証跡、オペレーション記録、運転記録等は、改ざん及び不正アクセスを防ぐために、正当なアクセス権限者以外のものから以下のいずれかの方法により適切に保護すること。

・暗号化して保管する。
・ 書換え不能メディアに記録し、保護された場所に保管する。
・ネットワーク経由の不正アクセスや改ざんを防止するために､オフライン媒体に記録する。

また、クラウドサービスのアクセス権限設定に関する仕様変更や変更時には、設定内容の妥当性を確認し主管担当あて事前に通知すること。

(5) データの秘匿

別途調達するシステム基盤において、暗号化を実施するため、影響を及ぼさないこと。また、PDCA ツール内のすべてのデータにおいて、秘匿のため暗号化を実施すること。暗号化方式は CRYPTREC 暗号リスト（電子政府推奨暗号リスト）及び TLS 暗号設定ガイドラインで推奨される方式による暗号化に準拠していること。

(6) ネットワーク対策

不正な通信を遮断するための制御やアクセス元の制限を実施すること（例：ファイアウォールや IP アドレス制限等）。外部ネットワークからの不正侵入があった場合は、直ちに当行へ通知すること。

また、次期 PDCA ツール側の機能を利用し、ネットワーク対策を講じる場合は、以下の要件も併せて満たすこと。

1. 外部ネットワークからのアクセス経路は、不正アクセスを防止するため、ファイアウォール等で不要なポートを閉塞する等必要最小限にするとともに、ネットワーク構成情報を適切に管理すること。
2. 外部ネットワークと接続する場合は、接続部分の不正侵入防止のため、入口対策を講ずること。合わせて、侵入したウイルスの検知、バックドアの構築防止、機密情報の流出防止等を目的とした出口対策(通信ログ､イベントログ等の分析による､不適切な通信の検知･遮断 等)を講ずること。
3. 外部ネットワークからの不正侵入の防止と早期発見のため、内部ネットワークへのアクセスを監視し、アクセス履歴のチェックを行うこと。

(7) マルウェア対策

マルウェア（ウィルス、ワーム、ボット等）の感染を防止するため、ウイルス対策ツール等の仕組みを導入すること。対策を実施する場合には、ウイルス定義ファイルの更新方法やタイミングについても検討し、システム全体に対して緊急度の高いセキュリティパッチ（ウイルス定義ファイルを含む）に関しては、即座に適用すること。適用を検討する際には、システム全体への影響を確認し、パッチ運用の可否を判断すること。

ウイルス対策ツール（本体、及びウィルス定義ファイル）が更新されていることを定期的に確認し、確認結果を定期的に管理台帳に記録し、管理すること。

なお、ウイルス定義ファイルの更新頻度及び台帳更新頻度は、ウイルス対策ツールの更新方法（自動／手動）によって、以下のア、イ以上の頻度で対応すること。

ア　自動の場合

【更新頻度】サーバ：月次、　端末：週次

【台帳更新】サーバ・端末：月次

イ　手動の場合

【更新頻度】サーバ・端末：月次

【台帳更新】サーバ・端末：更新の都度

また、主管担当より上記の管理台帳について提出の依頼があった場合、受託者は速やかに管理台帳を提出、もしくは上記について適切に実施していることを示す証明書等の提出を行うこと。証明書等を提出する場合は、当行所定の様式に従うこと。

(8) 脆弱性管理

受託者が詳細化された要件定義書に定める仕様を満たす、もしくは、サービスを提供するために納品/提供した機器及び製品を網羅的に把握し､情報の収集及びセキュリティパッチファイルの取得を継続的に行うこと。

システム全体に対して緊急度の高いセキュリティパッチに関しては、即座に適用すること。適用を検討する際には、システム全体への影響を確認し、パッチ運用の可否を判断すること。

取得したセキュリティパッチファイル、パッチ適用状況等を一覧管理する台帳等を作成し、四半期の頻度で更新を行い、主管担当に報告を行うこと。※更新の都度報告できない場合には、当行からの求めに応じ、作成した台帳等を開示すること。

主管担当より上記の管理台帳について提出の依頼があった場合、受託者は速やかに管理台帳を提出、もしくはセキュリティパッチ管理作業について適切に実施していることを示す証明書等の提出を行うこと。証明書等を提出する場合は、当行所定の様式に従うこと。

当行からの脆弱性管理に関する問い合わせに応じること。

(9) サイバーインシデント対応手順

以下のサイバーインシデントが発生した場合に備え、次期 PDCA ツールの開始までに当行で整備する対応手順の策定の支援を実施すること。

1. 攻撃予告発生
2. DoS 攻撃発生
3. 不正アクセスの発生
4. コンピュータウイルス感染発生
5. サイバー攻撃による社外秘以上の情報漏えい発生

サイバーインシデントに係る当行からの対応手順に関する問い合わせに応じること。

(10) Web 対策

セキュアコーディング、Web サーバの設定等による対策の強化を実施すること。

(11) 一時データファイルに対するセキュリティ対策

システム処理中に重要なデータを含む一時データファイルが生成される場合、重要なデータの漏洩を防止するため、利用状況に応じ不要となった時点で自動消去すること。

(12) 暗号鍵に関わる機能

電子化された共通鍵、秘密鍵を蓄積する IC カード等の機器、媒体あるいはそれに含まれるソフトウェアには、共通鍵、秘密鍵を保護する機能を具備すること。また、システム上に生成される一時データは不要となった時点で自動消去すること。

(13) 不正アクセス対策

ソフトウェアには、脆弱性が発見される可能性があるため、使用しない機能は停止、あるいは使用を制限すること。また、使用予定のないソフトウェアは搭載しないこと。

(14) パスワードによる対策

別途調達するシステム基盤において、設定されるパスワードでのログインとするか、ツールごとにパスワード等を設定する場合については、以下のとおり推測されにくいもののみ許容するよう、システム的に制御すること。

ア　英大文字／英小文字／数字／記号のうち最低 3 つを組み合わせること
イ　8 桁以上

また、初期設定されるパスワード等については、初回ログイン時にパスワード変更を実施させるよう、システム的に制御すること。

(15) バックアップ

別途調達するシステム基盤の要件に準拠するが、次期 PDCA ツール側の機能を利用する場合は、以下の要件も併せて満たすこと。

ア　バックアップの保管管理方法を明確にすること。
イ　業務継続上重要なデータについては、定期的なバックアップを実施し、本番環境から切り離した環境に保管する等ランサムウェア感染を考慮したバックアップを実施すること。

第5章 作業概要

第1節 開発期間（要件定義の詳細化～総合試験）

1 目標と基本方針

開発期間は総合試験完了を目指し、作業を遂行すること。事前に開発フェーズの作業内容及び成果物を定め、その進行状況を以下に示す工程終了時をチェックポイントとし、各チェックポイントにおいて、主管担当の承認をもって後続工程へ移ること。

- （チェックポイント 1）要件定義の詳細化終了時
- （チェックポイント 2）基本設計終了時
- （チェックポイント 3）詳細設計/構築/製造終了時
- （チェックポイント 4）総合試験終了時（移行判定）

また、工程の進行を阻害するリスク・課題を軽減・解決するため、プロジェクト管理体制(PMO)を構築して進行状況をモニタリングし、適切な対策を適時に実行する。

なお、本案件で作成した各種成果物及び作業プロセスに対しては、あらかじめ定めた品質管理計画に基づき品質評価を実施する。

2 工程の作業と終了基準

各工程の主な作業、終了基準は表 5.1.1 のとおり。

表 5.1.1　各工程における作業と終了基準

工程	作業(主要)	終了基準(主要)
要件定義の詳細化／基本設計	・業務要件及び技術要件に対する実現方法を各種要領に基づき定義する。	・ 成果物一覧に定義された成果物がすべて作成されている ・ 各工程の成果物と整合性が確保されている ・ 品質管理計画に基づき、品質確認対象がすべて品質確認され、かつ指摘事項に対する対応策が実施されている ・ 品質確認が適切なプロセスと参加者によって担保されている ・ 各成果物の内容について、関係者間で合意されている ・ 各成果物が所定のレビュープロセスを経て、承認者により承認されている ・ 残課題が存在し、次工程へ申し送りする場合は、その理由とアクションが具体化されている
	【システム設計】 ・要件定義書（詳細編）の作成	・ 詳細化された要件定義書の作成、レビューが完了している。
	【試験方針】 ・試験方針・計画の策定	・ 試験方針及び試験要件が関係者間で合意されている
詳細設計／開発	・基本設計にて定義した設計を実現する内部処理に関する詳細設計を実施 ・詳細設計にて定義した設計を実現する実装を実施 ・各設計に基づき、機能単体の試験を実施	・ 当該工程のすべての作業が完了していること ・ 前工程にて作成された成果物と本工程の成果物の整合性が確保されていること ・ 残課題が対応されていること ・ 残課題が存在し次工程へ申送りする場合は、その理由とアクションが具体化されていること ・ 品質管理計画に基づき、品質確認対象がすべて品質確認され、かつ指摘事項に対する対応策が実施されている ・ 品質確認が適切なプロセスと参加者によって担保されている
結合試験／総合試験	・業務機能が設計条件に適合しており、業務要件・非機能要件を満たしていることを、疑似環境等を使った実運用に近い形態で確認する。	・ すべての試験シナリオが実施されている ・ 試験シナリオ結果がすべて正しい。ただし、故障対応等が未済で結果確認ができないものについては、対応計画が立てられ内容が妥当である ・ 試験結果のレビューが適切なプロセスと参加者によって実施されている ・ 品質管理計画に基づき、品質確認対象がすべて品質確認され、かつ指摘事項に対する対応策が実施されている ・ 品質確認が適切なプロセスと参加者によって担保されている

3 成果物

受託者は以下のとおり、納入する。なお、納入方法は手交とし、また、成果物は電子媒体とする。なお、様式等納入に必要となる事項の詳細は主管担当と事前に調整し、承認を得る。

表 5.1.2　成果物

工程	成果物名	媒体	納入/作業完了期限
要件定義の詳細化	プロジェクト管理計画書	電子媒体	契約締結後2か月以内
	情報管理計画書		契約締結後2か月以内
	要件定義書(詳細編)		2024年11月30日
基本設計	システム開発設計書(基本設計編)		2025年1月31日
詳細設計/開発・単体試験	システム開発設計書(詳細設計編)		2025年6月30日
	システム等構成図		2026年1月31日
結合試験	結合試験仕様書		2025年11月30日
	結合試験結果報告書		2025年11月30日
総合試験	総合試験仕様書		2025年11月30日
	総合試験結果報告書		2025年11月30日
	上記※ファイルを記録した CD-R 等	CD-R等2部	2026年1月31日
	ソフトウェア一式	電子媒体	2026年1月31日

※プロジェクト管理計画書からユーザマニュアルまでを示す。

4 作業方針

(1) 基本設計・詳細設計作業方針

- 以下の後続工程開始時において、受託者は、前工程で必要な成果物を作成の上、主管担当に提示し、承認を経て、後続工程の作業を実施する。

  - ✓ 基本設計開始時
  - ✓ 詳細設計開始時

- 設計作業環境、作業場所等は、本受託者の負担と責任において用意する。
- 作業は、現行業務利用している他のシステム関係者、本システムと並行して構築している他システム関係者等と連携して行う。
- 後続工程で設計結果の変更が発生した場合は、その対応方針について、主管担当と協議する。

(2) 開発作業方針

- 受託者は、主管担当に対して、開発工程作業の開始、進捗等を随時、報告する。
- 開発期間中、設計内容の見直しが発生した場合は、設計工程における成果物に対して影響範囲を分析の上、修正作業を実施し、主管担当に修正した成果物名や修正内容等、報告する。
- 詳細設計の内容や要件の追加、修正等が開発工程に発生した場合、開発規模や範囲等を分析し、主管担当に報告、協議の上、極力、開発モジュールの修正・見直し対応できるようにする。

(3) 結合試験/総合試験作業方針

ア 共通

- 試験作業は、機能、性能、運用、セキュリティ等の評価を行い、本システムの設計・開発内容の妥当性を確認することを目的とし、具体的な評価項目については、主管担当に確認・承認を得ることとする。
- 試験作業には本システム以外のシステムとの接続試験を含むこととする。
- テスト環境での事前評価と総合試験内にて本番環境での受入試験を行うこととする。
- 定期的に進捗報告を行うとともに、問題発生時においては、随時報告を行う。なお、各試験の実施途中において、主管担当がそれまでのテスト結果の報告を求めた場合は、これに従わなければならない。
- 各試験終了時に、実施内容、品質評価結果及び次工程への申し送り事項等について取り纏めたテスト結果報告書を作成し、試験結果についての証跡及びテストに使用したツール等を提出することとする。
- 試験に使用したテストデータ、ユーザ ID 等を、テスト完了時において完全に削除し、本受託者において当該情報を保持しないことを制約する旨の書類を総合試験の試験結果報告書に含め、主管担当に提出する。

イ 試験データ

- テスト環境での試験データは、原則として受託者が用意すること。ただし、移行作業後の総合試験については、本番データ相当を用いることとする。
- 試験データ管理は、受託者が責任を持って行うこととする。なお、試験データの内容、種類等は、試験工程ごとの試験結果報告書に記載することとする。
- 試験において、本番データを使用する場合は、その取扱い等については、主管担当の指定に従うこととする。また、他システムからの本番データが必要となる場合は、主管担当がマスキングした情報を提供するが、本システムから本番データを取得する場合は、受託者がデータをマスキングすることとする。

ウ テスト環境要件

- 開発工程における各種モジュールの単体、結合試験に必要な機器等は、受託者の負担と責任において用意することとする。

・　総合試験（受入試験含む）を実施する環境については、原則として、稼働前の本番環境を効果的に利用することとする。

エ　総合試験（検収）

・　総合試験は、主管担当が主体となって行うが、受託者は、総合試験時、主管担当の求めに応じて総合試験をサポートするための体制を確保することとする。
・　総合試験で必要な試験データについては、受託者が主管担当からの依頼内容を基に用意することとする。
・　総合試験で確認された障害について、主管担当からの依頼により解析を行い、原因及び対策方針案を提示することとする。
・　上記にて主管担当が決定した対応方針に従い、プログラム及びドキュメント等を修正する。

第2節 移行期間

1 目標と基本方針

移行期間は 2026 年 1 月のサービス開始を目指し、作業を遂行する。
移行対象のデータは以下のとおり。

表 5.2.1　移行対象データ

No	種類	ファイル数	備考
1	イベント検知プログラム （施策対象者を検知するEGプログラム）	約60	
2	EGのプロジェクトファイル	約4,500	45ユーザ×100ファイルを想定
3	SASデータセット	約2,210	

2 工程の作業と終了基準

各工程の主な作業、終了基準は表 5.2.2 のとおり。

表 5.2.2　移行期間における作業と終了基準

期間	作業(主要)	終了基準(主要)
移行計画・準備	・要件定義の詳細化にて定義した移行方針を基に、具体的な移行計画を策定 ・計画済みの移行、準備を推進	・当該工程のすべての作業が完了していること ・スコープ、スケジュール、体制について関係者間で合意されていること ・計画書が所定のレビュープロセスを経て、プロジェクトマネージャにより承認されていること ・成果物が所定のレビュープロセスを経て、プロジェクトマネージャにより承認されていること
移行リハーサル	・移行用データ登録作業を計画し、必要回数のリハーサルを実施	・当該工程のすべての作業が完了していること
コンティンジェンシープラン策定	・システム導入における緊急時に関わる対応計画を策定	・当該工程のすべての作業が完了していること ・成果物が所定の規程に準じていること ・災害時の復旧手順が具体化されていること ・コンティンジェンシープランが所定のレビュープロセスを経て、プロジェクトマネージャにより承認されていること
移行	・移行リハーサルにて妥当性が確認された移行手順に基づき移行作業を実施	・予定した作業がすべて正常に完了していること
サービスイン （運用開始）	・業務運営状況の監視 ・システム運用状況の監視	・移行終了後、所定の期間において業務・システムの運用が顧客サービス・経営に大きな影響を与えていないこと

3 成果物

移行期間の成果物は表 5.2.3 のとおり。

表 5.2.3　移行期間における主な成果物

工程	成果物名	備考	媒体	納入/作業完了期限
データ移行	移行計画書		電子媒体	2025年12月31日
	データ移行計画書			2025 年 12 月 31 日
	移行テスト仕様書兼結果報告書	上記計画書に基づき本受託者が準備した環境で移行に関わるツールや方法論についての検証項目、検証結果について取り纏めた文書		2025 年 12 月 31 日
	移行リハーサル手順書			2025 年 12 月 31 日
	移行リハーサル結果報告書			2025 年 12 月 31 日
	本番移行手順書			2025 年 12 月 31 日
	本番移行完了報告書	完了基準に基づき、当該作業が完了していることを報告する文書		2026 年 1 月 31 日
現新比較	現新比較結果報告書	完了基準に基づき、当該作業が完了していることを報告する文書		2025 年 12 月 31 日
	上記※ファイルを記録したCD-R等		CD-R 等 2 部	2026 年 1 月 31 日

※移行計画書から現新比較結果報告書まで

4 作業方針

ア　移行作業方針

- 上記「3　成果物」内の各種計画書作成時に移行対象となるシステム環境や移行対象テーブル、データ等を特定の上、その移行方式、スケジュール、体制等を取り纏め、主管担当に報告する。
- 移行元システムからのデータの移行作業に関わる移行リハーサル及び本番稼働のためのシステム移行作業は、原則として平日以外で実施することとして移行計画を策定する。スケジュールの制約等により、平日も必要となる場合は、主管担当と協議の上、計画を策定する
- 移行元システムからのデータ移行作業は、受託者が、移行元システムの受託者の協力の下、移行システム（データ移行を実施するツール、仕組み等）を利用し、実施すること。
- 移行作業に当たっては、進捗管理及び障害管理を行い、移行作業に係る管理責任を負うものとする。なお、移行元システムからのデータの抽出作業は、事前に、主管担当、移行元システムの受託者と協議の上、役割分担を定義の上、当該役割分担に基づき、データ抽出作業を実施すること。
- 移行の際に、移行元システム、あるいは他システム等に影響があると想定される場合には、事前に主管担当及び移行元システム、他システム等の管理責任者に連絡すること。なお、他システムに係る業者との調整が必要となる場合は、主管担当を通じて実施すること。その際、調整内容について、事前に主管担当と協議すること。
- 移行のために、主管担当の作業が必要なる場合は、作業内容を整理した文書を作成、説明の上、実施すること。
- 移行作業のために機器等の追加が必要な場合は、受託者が用意すること。また、作業終了後は、当該機器を撤去すること。
- 移行作業中に障害が発生した場合には、速やかに原因究明にあたるとともに、計画書、作業手順書等に従い、切り戻し作業を行い、主管担当の承認を得て、必要な障害対処作業を本受託者の責任と負担により実施すること。

第3節 保守・運用期間

1 目標と基本方針

保守･運用期間は 2026 年 1 月の運用開始及びその後の安定運用を目指し､作業を遂行すること｡(2026 年 1 月 1 日から 2030 年 12 月 31 日まで)

2 工程と作業の終了基準

保守・運用期間の主な作業、終了基準は表 5.3.1 のとおり。

表 5.3.1　保守・運用期間における作業と終了基準

期間	作業(主要)	終了基準(主要)
運用マニュアル等 引継ぎ文書の作成	・　運用マニュアルの作成 ・　システム操作・利用マニュアルの作成	・　運用マニュアル等の引継ぎ文書が全量作成されていること
教育・研修	・　業務担当者へのシステム操作に関わる教育・研修の実施 ・　システム運用担当者へのシステム運用業務、オペレーションに関わる教育・研修の実施	・　教育・研修項目、当該項目に該当するシステム操作方法について、期間中、業務担当者、システム運用担当者へ実操作を含めた説明会、演習が完了していること

3 報告物

保守・運用期間の報告物は表 5.3.2 のとおり。

表 5.3.2　保守・運用期間における主な報告物

工程	報告物名	備考	媒体	提出期限
研修	教育研修計画書	教育研修を実施する上での目的や方針、スケジュール（カリキュラム含む）や体制、教育研修環境等を記載した文書	電子媒体	2026年1月31日
研修	教育研修教材	教育研修を実施する際の教材	電子媒体	2026年1月31日
	システム操作マニュアル	業務担当者が本システムを操作する際、利用する操作マニュアル		2026年1月31日
運用・保守	運用マニュアル	システム運用・保守作業を実施する上でのサービス内容や手順を取り纏めた文書		2026年1月31日
	月次運用・保守報告書	サービス開始後、月次		当月分を翌月10日まで ※履行期限　2031年1月31日

4 作業方針

ア　システム運用・保守方針

(ｱ) 基本方針

本システム稼働時において、システム運用･保守に必要な機能を設計するとともに、運用・保守業務の自動化等を効率的に遂行するための効果的な機能を提案し、主管担当と協議の上、設計・開発に取り込むこと。

また、リリース後の機能強化開発に対して、短期間で開発できるように、設計・開発段階で変更容易性を考慮すること。

システム運用･保守期間中の業務担当者からの機能追加､修正､削除等の要求に対しては、主管担当が当該各要件について対応緊急度を識別した上で、取り纏めを行い、取り纏めた内容に基づき、本運用・保守受託者と変更する機能の内容や他機能システムへの影響範囲、コスト、スケジュール等を協議、対応判断を行った上で対応を実施すること。

(ｲ) システムの運用スケジュール

本システムの運用スケジュールとしては、原則、以下のスケジュールとする。また、ユーザによる画面操作については、下記運用スケジュールの期間において、可能な状態を維持すること。ただし、業務繁忙期等により夜間バッチ処理が下記運用スケジュール内に完了しない場合は、バッチ処理完了後に利用開始とする。

表 5.3.4 運用スケジュール

項番	サービス	処理区分	スケジュール
1	オンラインサービス	登録・更新・参照	営業日 8:00　～　21:00
2	バッチ処理サービス	登録・更新	LM システムのバッチ終了後から 2 時間以内で完了すること。（5:00～8:00 を想定。）

(ｳ) 問い合わせ対応

- 主管担当からの問合せ窓口を設置すること。
- その際、電話、電子メール等を用意し、本システムにて整備した機器（システム環境、製品・ツール類等）やサービスに関する問い合わせに対応すること。
- 問合せ窓口は、日本国内に設置し、日本語で対応可能とすること。
- 電話応対は、主管担当営業日の 9 時から 18 時まで受付し、対応すること。
- 電子メールは、24 時間受付を行い、受付時間外に受信した問合せへの回答は、翌営業日に対応すること。
- 問合せ者やその内容等の情報漏洩・紛失を防ぐ対策を行うこと。
- 問題への対応、依頼等を適切に行える体制を整えるとともに、応対者については、必要な人数の確保及び教育を実施し、運用･保守業務に支障を生じさせないようにすること。

(ｴ) システム運用・保守方針

■ **月次報告**

- 月次報告は、運用・保守レベルの維持管理を行うことを目的としている。
- 受託者は、「月次運用・保守報告書」を作成し、主管担当に報告すること。
- 報告内容に基づき、実態の評価、問題対応結果の評価及び実施対策の評価を行う。
  また、報告内容に基づき、再発防止策の検討、作業計画、予防施策等の検討を行うこと。
- 「月次運用・保守報告書」の内容は、概ね以下のとおりとする
  - 実績報告
  - 問題対応結果の報告
  - 再発防止策
  - 作業計画
  - 予防施策
  - 課題管理状況
  - アクセスログに基づいて許可されていないアクセスの分析及び報告
  - アカウントロックや時間外のアクセス試行等の不正なアクセスの分析報告

■ **アプリケーションソフトウェア保守**

- 本システムで納入するすべてのアプリケーションソフトウェアを保守対象とすること。
- 日本語で対応できるものとすること。
- アプリケーションソフトウェアの潜在的な不具合やセキュリティ上の不具合があった場合は、主管担当に報告の上、依頼内容に従い、不具合対応する修正プログラムの適用を行うこと。
- アプリケーションソフトウェアに障害があった場合、受託者、メーカー、サービサー等の保守担当者による障害箇所の特定、原因調査、復旧作業の切り分けを実施し、速やか

に報告の上、依頼内容に従い、復旧対応するとともに、動作確認によって正常に動作することを保証すること。
- システム運用・保守期間中のアプリケーションソフトウェアのバージョンアップが発生した場合は、主管担当にバージョンアップの内容と影響範囲を報告の上、バージョンアップ実施要否判断を協議し、主管担当の依頼に従い実施すること。
- システム運用・保守期間中のパフォーマンス向上及び機能変更要望が発生した場合は、主管担当と協議の上、対応方法等を検討すること。

イ　教育・研修方針

(ｱ) 基本方針

更改後のシステム運行担当者、業務担当者の作業が滞りなく行えるよう、研修等を実施すること（想定は以下の表 5.3.4 のとおり）。なお、研修の環境は原則総合試験環境とし、研修内容、実施スケジュールについては主管担当と協議の上決定すること。

。主管担当から、本社営業部門の各ユーザへ研修を行うため、研修等の訓練に要する文書の作成支援を行うこと。

表 5.3.4-1　システム運行担当者向け研修内容（予定）

No	項目	内容
1	実施期間	総合試験期間中
2	実施場所	主管担当　執務室（大手町本社　20 階）
3	実施内容	・ユーザ登録/削除（実機） ・ユーザ共有領域の利用状況の確認（実機） ・ユーザ共有領域のテーブルの削除（実機） ・施策の実行登録/削除（実機） ・バッチ処理状況の確認（実機） など ※運行上必要になりそうな研修があれば、適宜提案すること。
4	訓練対象者	・主管担当　担当者 5 名程度

表 5.3.4-2　業務担当者向け研修内容（予定）

No	項目	内容
1	実施期間	総合試験期間中
2	実施場所	主管担当　執務室（大手町本社　20 階）
3	実施内容	・現行 PDCA ツールから変更があった UI や機能の研修（座学） ・施策管理ツール習得研修（実機） など ※必要になりそうな研修があれば、適宜提案すること。
4	訓練対象者	・主管担当　業務担当者 7 名程度

第6章　その他

第1節 その他留意事項

・受託者は、データの取扱いについて、契約書に別紙２として添付する「情報保護・管理要領」を遵守すること。なお、受託者は、本件業務の全部又は一部を第三者に再委託する場合は、事前に社内取扱規程等の書類を主管担当へ提出し、主管担当の承認を得た上で受託した作業を実施すること。
・受託者は、受託者が何らかの理由により当該作業を継続できなくなった場合に備え、サービス継続のためのコンティンジェンシープランを作成し、主管担当の承認を得ること。
・受託者は主管担当からの求めに応じて、他ベンダに協力すること。なお、その際にかかる費用は原則今回調達の運用・保守に係る対価に含むこととするが、内容に応じて別途主管担当との交渉は可能とする。
・追加開発等が発生する場合は、本件業務の範囲外とし、別途契約変更等で対応するが、その際、受託者は主管担当の依頼に応じて追加開発に係る見積やスケジュール等を速やかに作成、提供すること。
・追加開発の検討にあたり、開発工程への吸収時期の調整、吸収時期別の生産性の調整等、受託者はこの協議に応じること。
・追加開発、仕様変更等に関しては、詳細見積とその根拠を提示すること。
・追加開発等における単価は、原則、当初調達に係る見積書記載の金額を上限とする。
・本仕様書記載の要件（受託者から提案される要件を含む。）以外に追加要件及び仕様変更等が発生した場合の作業工数単価（以下「単価」という。）については、入札時の単価は使用せず、以下の考え方に基づき、当行及び受託者で調整することとする。

ア　当行の他システム開発を現に受託している場合

他のシステム開発で使用している単価を適用することを基本とする。ただし、受託しているシステムが今回提案するシステムと性質が大きく異なる場合を除く。

なお、複数のシステム開発を受託している場合は、類似のシステムの単価を適用することを基本とする。

イ　当行の他システム開発を現に受託していない場合

当行におけるシステム開発のうち、類似のシステム開発の単価を基本とする。

なお、単価が合意できない場合は、当行からの申し出により、当行が第三者に委託することを認めるものとし、第三者がシステム開発等を行うための引き継ぎに協力するものとする。その場合の引き継ぎ作業については別途契約するものとし、その工数は提案の工数には含まず、引き継ぎ作業の単価は別途協議する。

また、単価の調整に併せて、開発生産性の調整も行うこととする。

・使用しているツール等がサービス提供を終了する場合は６か月以上前に主管担当のＥメールアドレス宛てにメールで通知すること。
・本契約を終了する際、次期システムの開発・保守を引継ぎ、又は、後継システムの開発を担う第三者に対し、引継ぎの情報提供、資料開示、照会に対する回答、など協力作業を行うこと。（当該第三者に対する協力作業については、当行からの要請に基づき契約変更等で対応することとし、本件業務範囲には含めない。）
・当行監査部門が必要と認めるときは、監査を受けること。
・クラウド事業者に対する立入監査・モニタリング態勢を整備すること。なお、立入監査やモニタリングが実施できない場合は、第三者監査等の報告書を主管部へ提出すること。その場合は、検証項目が十分であることを確認するため、事前に主管担当の承認を得ること。
・成果物の納入場所は、主管担当が別途指定する場所、条件によること。
・本件業務の内容及び解釈等について、疑義が生じた場合又は特に必要がある場合は、事前に主管担当と協議し、決定・解決すること。この場合、協議後速やかに、受託者は当該協議に係る議事録を作成し、主管担当の承認を得ること。
・業務従事者に対する作業の指示、労務管理、安全衛生管理等に関する指揮命令は、すべて受託者の責任において行うものとする。
・詳細については、主管担当(TEL03-3477-2012)の指定によること。

第2節 提案方法

(1) 提案方法

提案方法は、以下を参照すること。

・別添２　提案書作成要領

・別添３　提案書評価基準

(2) 更なる改善提案

本契約の見積り金額の範囲内で本仕様書に記載した要件よりも優れた機能又はサービスの提供が可能なものがあれば適宜の様式に記入し、提案書に添付すること。

見積り金額には含まれないが将来的な機能拡張に関して優れた提案があれば適宜の様式に記入し、提案書に添付すること。

第3節 受託者に求める要件

受託者は、開発規模が本契約と同等程度であり、本契約で提案するシステム構成に類似する構成での実績を有する方が望ましい。

1 受託企業に求める要件

「別紙５　適合証明書」に示す条件を満たすこと。適合証明書に記名・押印したものを提案書に添付して提出すること。

2 プロジェクトメンバーに求める要件

- プロジェクトメンバーのマネジャー・リーダー・サブリーダーは、国内金融機関において、分析/施策管理システムの導入・開発・設計に関して、プロジェクトを完遂した者もしくは同等の経験、知識を有している者とすること。
- プロジェクトメンバーのメンバークラスは、分析/施策管理システムの導入・開発・設計に関して、充分な経験、知識を有している者とすること。
- 日本語で十分な意思疎通を行うことが出来ること。
- 本システムと関連するシステム開発者及び関連部署と円滑な共同作業が出来ること。

第4節 主管担当

本案件の主管担当は以下のとおり。

担　当：株式会社ゆうちょ銀行 営業部門 デジタル戦略部 リテールマーケティング室
所在地：〒100-8793　東京都千代田区大手町二丁目３番１号（大手町プレイスウエストタワー 20F）
電　話：03-3477-2012
Email：jouhoukatsuyousuisin.ii@jp-bank.jp

第5節 添付資料一覧

(1) 別添

別添１　非機能要求グレード

別添２　提案書作成要領

別添３　提案書評価基準
別添４　診断企業条件
別添５　セキュリティ診断実施内容
別添６　各種証明書
別添７　IT 資産情報ヒアリングシート

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	運用コストへの影響	備考	LMシステム	PDCAツール	PDCAツール補足	LMシステム補足事項 （凡例） －：補足事項無	社会的影響が殆ど無いシステム 選択レベル	社会的影響が殆ど無いシステム 選択時の条件	社会的影響が限定されるシステム 選択レベル	社会的影響が限定されるシステム 選択時の条件	社会的影響が極めて大きいシステム 選択レベル	社会的影響が極めて大きいシステム 選択時の条件
A.1.1.1	可用性	継続性	運用スケジュール	システムの稼働時間や停止運用に関する情報。	○	○	運用時間（通常）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止		【重複項目】 C.1.1.1、運用時間は、システムの可用性の実現レベルを表す項目であると共に、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 運用時間は、オンライン／バッチを含みシステムが稼動している時間帯を指す。 【レベル】 （）内の時間は各レベルの一例を示したもので、レベル選定の条件とはしていない。規定無しは、固定のサービス時間が存在しないことを示し、基本的にシステムは停止していて、必要に応じてユーザがシステムを起動するようなケースを想定している（例．障害発生に備えた予備システム、開発・検証用システム等）。定時内や夜間のみ停止は、一般的な業務形態を想定したもので、業務が稼動する時間帯が異なるシステムにおいては、時間帯をスライドさせるなどの読替えが必要である。停止有りとは、システムを停止しなければならないQoS時間帯ではなく、システムを停止できる可能性のある時間帯を指す。24時間無停止は、オンライン業務が稼動していない時間にバッチを稼動させる必要があり、システムを停止することができないようなケースも含まれる。	3	3			2	夜間のみ停止（9時～21時）	夜間に実施する業務はなく、システムを停止可能。 [－] 運用時間をもっと限って業務を稼働させる場合 [+] 24時間無停止やリブート処理等の短時間の停止のみを考える場合	4	若干の停止有り（9時～翌朝8時55分）	24時間無停止での運用は必要ないが、極力システムの稼働は継続させる。 [－] 夜間のアクセスは認めないなど、長時間運用を停止する場合 [+] 24時間無停止で運用する場合	5	24時間無停止	システムを停止できる時間帯が存在しない。 [－] 1日のスケジュールで定期的に運用を停止する時間帯が存在する場合
A.1.1.2					○	○	運用時間（特定日）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止		【重複項目】 C.1.1.2、運用時間は、システムの可用性の実現レベルを表す項目であると共に、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 特定日とは、休日/祝祭日や月末月初など通常の運用スケジュールとは異なるスケジュールを定義している日のことを指す。特定日が複数存在する場合は、それぞれにおいてレベル値を整合する必要がある（例：「月～金はLevel2だが、土日はLevel0」、「通常はLevel5だが、毎月1日にリブートをするためその日はLevel3」など）。 また、ユーザの休日だけでなく、ベンダの休日についても特定日として認識し、運用保守体制等を整合すること。	2	2			0	規定無し	通常と異なる運用時間となる特定日は存在しない。 [+] 休日にバックアップ運用を行うなど、通常とは異なる運用時間となる特定日が存在する場合	2	夜間のみ停止（9時～21時）	週末はバックアップ運用のみのため、夜間は停止する。 [－] 週末運用するバックアップやバッチ処理などが存在せず、土休日は運用を停止する場合 [+] 休日出勤する社員の業務に必要なため、土休日も運用する場合	5	24時間無停止	システムを停止できる時間帯が存在しない。 [－] 定期的に運用を停止する日が存在する場合
A.1.1.3					○	○	計画停止の有無	計画停止有り（運用スケジュールの変更可）	計画停止有り（運用スケジュールの変更不可）	計画停止無し				○	【重複項目】 C.2.1.1、計画停止の有無は、システムの可用性の実現レベルを表す項目であると共に、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【運用コストへの影響】 計画停止が"有り"の場合、事前のバックアップや、システム構成に応じた手順準備など、運用時のコストがかさむ。	0	0			0	計画停止有り（運用スケジュールの変更可）	事前の合意があれば、停止は可能。 [+] 運用時間外での停止だけで対応可能な場合	1	計画停止有り（運用スケジュールの変更不可）	24時間無停止での運用は必要ない。停止可能な時間が存在し、計画的な停止は可能。 [－] 運用スケジュールとしては停止可能な時間帯は存在しないが、事前の調整で停止が可能な場合 [+] 24時間無停止が要求される場合	2	計画停止無し	システムを停止できる時間帯が存在しない。 [－] 運用スケジュールとして停止可能な時間帯が存在し、計画停止の必要性がある場合
A.1.2.1			業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。		○	対象業務範囲	内部向けバッチ系業務	内部向けオンライン系業務	内部向け全業務	外部向けバッチ系業務	外部向けオンライン系業務	全ての業務		【メトリクス】 ここでの対象業務範囲とは、稼働率を算出する際の対象範囲を指す。	3	3		－	2	内部向け全業務	内部向けの業務が主要業務であり、内部向け全業務が稼働していることがシステム稼働の条件となる。	3	外部向けバッチ系業務	外部とのバッチ的な処理で業務が主要業務であり、内部向けの業務および外部とのバッチ的な業務が	4	外部向けオンライン系業務	外部とのリアルタイムでの処理が主要業務であり、外部向けオンライン業務が稼働していることがシステ
A.1.2.2						○	サービス切替時間	24時間以上	24時間未満	2時間未満	60分未満	10分未満	60秒未満	○	【メトリクス】 サービス切替時間とは、想定できる障害（例えばハードウェアの故障等により業務が一時的中断するケースなど）に対して、対策を施すこと（例えばクラスタ構成でのサーバの切替えなど）により、業務再開までに要する時間を指す。 【運用コストへの影響】 中断を許容する時間が長くなれば、復旧対策としてはシステムでの自動化から人員による手動での対処に比重が移るため、運用コストへの影響が出てくる。	1	1		※ なお、AWSの切り替え時間に関しては、AWS側の切り替え時間に準拠するものとするが、レベル1以上を目標とすること。	1	24時間未満	外部向けの業務はなく、1日程度の中断であれば許容できる。 [－] 障害時の対策を必要としない場合 [+] サービス切替の影響がある場合（影響度に応じて中断を許容できる時間を検討する）	3	60分未満	外部とのオンラインでの業務はあるが、数十分の停止までは許容可能。 [+] オンライン業務においてサービス切替の影響がある場合（影響度に応じて中断を許容できる時間を検討する）	5	60秒未満	リアルタイム性が要求されるため、システム停止時は瞬時の復旧が必要となる。 [－] 業務の停止が1時間以内であれば許容できる場合
A.1.2.3						○	業務継続の要求度	障害時の業務停止を許容する	単一障害時は業務停止を許容せず、処理を継続させる	二重障害時でもサービス切替時間の規定内で継続する					【メトリクス】 業務継続の要求度とは、発生する障害に対して、どこまで業務を継続させる必要があるかを示す考え方の尺度を示している。 システムを構成する機器や部位には、単一障害点SPOF（Single Point Of Failure）が多数存在し、システム停止となるリスクを多く含んでいる。これらのSPOFを許容するか、冗長化などの対策で継続性をどこまで確保するかが要求の分かれ目となる。	1	1		または、稼働率99%を満たすことを前提に障害時の業務停止を許容する。 ※ただし、回線をベストエフォート回線とする場合は回線起因による障害は対象外とする。	1	単一障害時は業務停止を許容せず、処理を継続させる	障害時の業務停止の許容時間に合わせる。 [－] リスクを認識した上、障害発生時の業務停止を許容できる場合 [+] コスト増を考慮した上で二重障害による業務停止を防止する必要がある場合	2	二重障害時でもサービス切替時間の規定内で継続する	障害時の業務停止の許容時間に合わせる。 [－] リスクを認識した上、二重障害での業務停止を許容できる場合	2	二重障害時でもサービス切替時間の規定内で継続する	二重障害でも業務継続が前提となる。
A.1.3.1			目標復旧水準（業務停止時）	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標。		○	RPO（目標復旧地点）	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+アーカイブからの復旧）				【メトリクス】 RLOで業務の復旧までを指定している場合、該当する業務のデータの復旧までが対象であり、業務再開の整合性の確認は別途必要となる。 【レベル3】 障害発生時点とは、障害が発生する直前のトランザクションなどの処理が完了している時点のことを指し、障害発生時点まで復旧するためには、発生直前の完了した処理のジャーナログが保証されていることが前提となる。またジャーナルログをアーカイブすることで、障害発生までの任意の時点への復旧に対応することを想定している。	2	2		24時間以内に1営業日前の状態へ復旧することを目標とする。 ※ なお、AWSに関しては、AWS側に準拠するが、レベル2以上を目標とすること。	1	5営業日前の時点（週次バックアップからの復旧）	データの損失は許容できないため、週次のバックアップからの復旧とする。 [－] データを持たず、復旧が不要な場合 [+] 日次のバックアップからの復旧でないと、データ損失の影響が大きい場合	3	障害発生時点（日次バックアップ+アーカイブからの復旧）	データの損失は許容できないため、障害発生時点までの復旧が原則。 [－] データの損失がある程度許容できる場合（復旧対象とするデータ（日次、週次）によりレベルを選定）	3	障害発生時点（日次バックアップ+アーカイブからの復旧）	データの損失は許容できないため、障害発生時点までの復旧が原則。
A.1.3.2						○	RTO（目標復旧時間）	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内			【メトリクス】 サービス切替時間（A.1.2.2）での復旧時間と異なり、RTOでの復旧時間は、業務の継続対策を実施していない（業務停止となる）ケースでの障害での復旧時間を指している。 RLOで業務の復旧までを指定している場合、該当する業務のデータの復旧までが対象であり、業務再開の整合性の確認は別途必要となる。	1	1		24時間以内に1営業日前の状態へ復旧することを目標とする。 ※ なお、AWSの復旧時間に関しては、AWS側の復旧時間に準拠するが、レベル1以上を目標とすること。	1	1営業日以内	目標復旧地点を考慮し、システムの規模から判断する。 [－] 業務停止の影響が小さい場合 [+] 業務停止の影響が大きい場合	2	12時間以内	目標復旧地点を考慮し、システムの規模から判断する。 [－] 業務停止の影響が小さい場合 [+] 業務停止の影響が大きい場合	4	2時間以内	なるべく早く復旧する。
A.1.3.3						○	RLO（目標復旧レベル）	システムの復旧	特定業務のみ	全ての業務					【メトリクス】 業務停止を伴う障害が発生した際、何を復旧の対象とするかのレベルを示す。 【レベル0】 システムの復旧は、ハードウェアの復旧だけでなくデータのリストアまでを対象とする。 【レベル1】 特定業務とは、例えばA.1.2.1対象業務範囲で定義する継続性が要求される業務などを指す。	0	0		－	1	特定業務のみ	主要な業務のみを対象とすることができる。 [+] 業務毎に影響を切り離せない場合	2	全ての業務	全ての業務が稼働していないと影響がある。 [－] 影響を切り離せる業務がある場合	2	全ての業務	全ての業務が稼働していないと影響がある。 [－] 影響を切り離せる業務がある場合
A.1.4.1			目標復旧水準（大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標。 大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、システムに甚大な被害が発生するか、電力などのライフラインの停止により、システムをそのまま現状に修復するのが困難な状態となる災害をいう。		○	システム再開目標	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開		【メトリクス】 大規模災害とは、RPO、RTO、RLOなどの細かな要求までは確定せず、システム再開目標として大まかな復旧時間を設定する。目標復旧レベルについては、業務停止時の目標復旧水準を参考とする。	1	1		－	1	数ヶ月以内に再開	データの損失はある程度許容でき、週次のバックアップからの復旧とする。 [－] データを持たず、復旧が不要な場合 [+] 業務停止の影響が大きい場合	3	一週間以内に再開	大規模災害時は、保管するデータからの復旧により業務を再開する。 [－] 代替機器の調達や、復旧体制の準備に時間がかかる場合 [+] 業務停止の影響が大きく、DRサイトによる早急な復旧が必要な場合	4	3日以内に再開	ライフラインの復旧を考慮し、システムとして最大限の回復に努める。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合
A.1.5.1			稼働率	明示された利用条件の下で、システムが要求されたサービスを提供できる割合。 明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。		○	稼働率	95%以下	95%	99%	99.9%	99.99%	99.999%		【レベル】 24時間365日の稼働の場合、1年間で業務が中断する時間の合計は、それぞれ以下の通りとなる。 95%・・・・・・・・・18.3日 99%・・・・・・・・・87.6時間 99.9%・・・・・・・ 8.76時間 99.99%・・・・・・ 52.6分 99.999%・・・・・ 5.26分 また1日8時間で週5日稼働のシステムではサービス切替時間と稼働率の関係は以下の通りとなる。 週に1時間・・・・97.5% 月に1時間・・・・99.4% 年に1時間・・・・99.95%	2	2		稼働率99%を目標とする。 ※ なお、AWSの稼働率に関しては、AWS側の稼働率に準拠するが、レベル2以上を目標とすること。	2	99%	1年間で数時間程度の停止を許容。 備考に記載した稼働率での目安となる稼働時間を参考にして決定する。	4	99.99%	1年間で1時間程度の停止を許容。	5	99.999%	1年間で数分程度の停止までしか許容できない。
A.2.1.1		耐障害性	サーバ	サーバで発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	特定のサーバで冗長化	全てのサーバで冗長化					【メトリクス】 冗長化における機器、コンポーネントは、冗長化の単位を表し、機器は筐体を複数用意することによる冗長化、コンポーネントは筐体を構成する部品（ディスク、電源、FAN、ネットワークカード等）を複数用意することによる冗長化を指す。 また、仮想化技術の適用により、同一ハードウェア上にサーバ機能を集約させることで、冗長化に必要なハードウェア所要量を削減することも可能である。いずれにしても、ハードウェア上で実現される業務継続性の要求を満たすよう機器の冗長化を検討する必要がある。 【レベル1】 特定のサーバで冗長化とは、システムを構成するサーバの種別（DBサーバやAPサーバ、監視サーバなど）で冗長化の対応を分けることを意味する。 また要求としてサーバの単位ではなく、業務や機能の単位で冗長化を指定する場合、それを実装するサーバを想定してレベルを設定する。	2	0	PDCAツールはシングル構成のため。	－										
A.2.1.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化					【レベル1】 サーバを構成するコンポーネントとして、内蔵ディスクや、電源、FANなどを必要に応じて冗長化することを想定している（例えば内蔵ディスクのミラー化や、ネットワークIFカードの2重化など）。	1	1		※ なお、対象がクラウドサービスである場合、責任共有モデルに基づき、クラウドサービス提供事業者の責任範囲であれば保証の対象外とするが、レベル1以上を目標とすること。										
A.2.2.1			端末	端末で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	共用の予備端末を設置	業務や用途毎に予備端末を設置						1	LM準拠	ハードウェア関連はLMシステム準拠。								
A.2.2.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化					【レベル1】 端末を構成するコンポーネントとして、内蔵ディスクや、電源、FANなどを必要に応じて冗長化することを想定している（例えば内蔵ディスクのRAID構成など）。	0	LM準拠	ハードウェア関連はLMシステム準拠。								
A.2.3.1			ネットワーク機器	ルータやスイッチなどネットワークを構成する機器で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	特定の機器のみ冗長化	全ての機器を冗長化					【レベル1】 特定の機器のみとは、ネットワークを構成するルータやスイッチの内、冗長化したサーバを収容するスイッチなどを想定している。	2	LM準拠	ハードウェア関連はLMシステム準拠。	または、稼働率を満たす冗長化構成を提案すること。 ※ なお、対象がクラウドサービスである場合、責任共有モデルに基づき、クラウドサービス提供事業者の責任範囲であれば保証の対象外とするが、レベル2以上を目標とすること。										
A.2.3.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化					【レベル1】 ネットワーク機器を構成するコンポーネントとして、電源やCPU、FANなどを必要に応じて冗長化することを想定している。	2	LM準拠	ハードウェア関連はLMシステム準拠。	または、稼働率を満たす冗長化構成を提案すること。 ※ なお、対象がクラウドサービスである場合、責任共有モデルに基づき、クラウドサービス提供事業者の責任範囲であれば保証の対象外とするが、レベル2以上を目標とすること。										
A.2.4.1			ネットワーク	ネットワークの信頼性を向上させるための要求。			回線の冗長化	冗長化しない	一部冗長化	全て冗長化する					【メトリクス】 回線の冗長化とは、ネットワークを構成する伝送路（例えばLANケーブルなど）を物理的に複数用意し、一方の伝送路で障害が発生しても他方での通信が可能な状態にすること。 【レベル1】 一部冗長化とは、基幹のネットワークのみ冗長化するケースや、業務データの流れるセグメントなどを想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－										
A.2.4.2							経路の冗長化	冗長化しない	一部冗長化	全て冗長化する					【メトリクス】 経路の冗長化とは、ネットワーク内でデータを送受信する対象間で、データの流れる順序（経由するルータの順序）を複数設定することで、ある区間で障害が発生しても、他の経路で迂回し通信を可能な状態にすること。 【レベル1】 一部冗長化とは、基幹のネットワークのみ冗長化するケースや、業務データの流れるセグメントなどを想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－										
A.2.4.3							セグメント分割	分割しない	サブシステム単位で分割	用途に応じて分割					【レベル2】 用途とは、監視やバックアップなどの管理系の用途から、オンライン、バッチなどの業務別の用途を示している。 サブシステム単位で分割したなかで、更に用途に応じてセグメントを分割することを想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	※ なお、対象がクラウドサービスである場合、責任共有モデルに基づき、クラウドサービス提供事業者の責任範囲であれば保証の対象外とするが、レベル1以上を目標とすること。										
A.2.5.1			ストレージ	ディスクアレイなどの外部記憶装置で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	特定の機器のみ冗長化	全ての機器を冗長化					【メトリクス】 NAS、iSCSI対応の装置を含む。 ただしNASやiSCSIはLANなどのネットワークに接続して利用するため、NASやiSCSIの接続環境の耐障害性対策は小項目A.2.4ネットワークに含まれる。 【レベル1】 特定の機器のみとは、導入するストレージ装置に格納するデータの重要度に応じて、耐障害性の要求が装置毎に異なる場合を想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	端末は対象外とするが、それ以外は1とする。										
A.2.5.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化					【レベル1】 ストレージを構成するコンポーネントとして、ディスクを除く、CPUや電源、FAN、インターフェースなどを必要に応じて冗長化することを想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	端末は対象外とするが、それ以外は1とする。 ※ なお、対象がクラウドサービスである場合、責任共有モデルに基づき、クラウドサービス提供事業者の責任範囲であれば保証の対象外とするが、レベル1以上を目標とすること。										
A.2.5.3							冗長化（ディスク）	非冗長構成	単一冗長	多重冗長					【レベル1】 単一冗長とは、単一箇所の障害であれば、サービス継続可能な冗長構成のことである。 【レベル2】 多重冗長とは、同時に複数の箇所が障害の状態となっても、サービス継続可能な冗長構成のことである。	2	LM準拠	ハードウェア関連はLMシステム準拠。	※ なお、対象がクラウドサービスである場合、責任共有モデルに基づき、クラウドサービス提供事業者の責任範囲であれば保証の対象外とするが、レベル1以上を目標とすること。										
A.2.6.1			データ	データの保護に対しての考え方。	○		バックアップ方式	バックアップ無し	オフラインバックアップ	オンラインバックアップ	オフラインバックアップ+オンラインバックアップ				【重複項目】 C.1.2.1、バックアップ方式は、バックアップ運用設計を行う上で考慮する必要があり、運用・保守性と重複項目としている。 【レベル】 オフラインバックアップとは、システム（あるいはその一部）を停止させてバックアップを行う方式、オンラインバックアップとはシステムを停止せず稼働中の状態でバックアップを行う方式を指す。	2	LM準拠	ハードウェア関連はLMシステム準拠。	－										
A.2.6.2					○		データ復旧範囲	復旧不要	一部の必要なデータのみ復旧	システム内の全データを復旧					【重複項目】 C.1.2.1、可用性ではデータをどこまで保全するかという観点で、運用ではデータをどこまで復旧させるかという観点で本項目が必要となり、重複項目としている。 【レベル1】 一部の必要なデータとは、業務継続性の要求を満たすために必要となるようなデータを想定している。	2	LM準拠	ハードウェア関連はLMシステム準拠。	－										
A.2.6.3							データインテグリティ	エラー検出無し	エラー検出のみ	エラー検出＆再試行	データの完全性を保障（エラー検出＆訂正）				【メトリクス】 データに対して操作が正しく行えること、操作に対して期待した品質が得られること、またデータへの変更が検知可能であることなどを物理レベルで保証する。 【レベル】 仕組みの実装は、製品、業務アプリケーションによる検出を含む。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－										
A.3.1.1		災害対策	システム	地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすための要求。			復旧方針	復旧しない	限定された構成でシステムを再構築	同一の構成でシステムを再構築	限定された構成をDRサイトで構築	同一の構成をDRサイトで構築			【メトリクス】 大規模災害のための代替の機器として、どこに何が必要かを決める項目。 【レベル】 レベル1および3の限定された構成とは、復旧する目標に応じて必要となる構成（例えば、冗長化の構成は省くなど）を意味する。 レベル2および4の同一の構成とは、復旧後も復旧前と同じサービスレベルを維持するため、本番環境と同一のシステム構成を必要とすることを意味する。 レベル1および2のシステムを再構築を選択する場合、被災後の再構築までを契約の範囲として考えるのではなく、被災したサイトあるいは共用センターなどの設備を利用して、あくまでシステムを再構築する方針とすることを要求するものである。 一方レベル3および4のDRサイトで構築は、指定されたDRサイトに復旧用のシステムを構築するところまでを含む。	1	0		－										

項番	大項目	中項目	小項目	小項目説明	最重要項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	LMシステム	PDCAツール	PDCAツール補足	LMシステム補足事項 （凡例） －：補足事項無	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム	
								0	1	2	3	4	5							選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件
A.3.2.1			外部保管データ	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管するなどの要求。			保管場所分散度	外部保管しない	1カ所	1カ所（遠隔地）	2カ所（遠隔地）					1	0		－						
A.3.2.2							保管方法	媒体による保管	同一サイト内の別ストレージへのバックアップ	DRサイトへのリモートバックアップ						1	0		－						
A.3.3.1			付帯設備	各種災害に対するシステムの付帯設備での要求。			災害対策範囲	対策を実施しない	特定の対策を実施する	想定する全ての対策を実施する					【メトリクス】 付帯設備については、システム環境・エコロジーにおいてF.4.1.1の耐震震度、F.4.4.4の停電対策で、災害対策の一部として要求を具体化している。 【レベル】 想定する災害対策としては、以下が考えられる。 ・地震対策 ・瞬電・停電対策 ・火災対策 ・漏電対策 ・雷対策 ・水害対策 ・電界・磁界対策	0	0								
A.4.1.1		回復性	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力。	○		復旧作業	復旧不要	復旧用製品は使用しない手作業の復旧	復旧用製品による復旧	復旧用製品＋業務アプリケーションによる復旧				【重複項目】 C.3.1.1。復旧作業は、可用性と運用・保守性に共通して含まれている。運用・保守性では、復旧目標の運用への影響という観点でその作業を確認するが、可用性は、それを実現するための手段として確認する。 【レベル】 自作ツールを利用するケースは手作業に含む。 復旧用製品とは、バックアップ・リカバリを行う製品を指す。復旧用製品による復旧を行う場合、どこまで自動化するか（自動リカバリー機能充足率など）を定義するケースもあるが、可用性としては、復旧用製品を使用するかしないかでギャップが発生するため、この観点でレベルを検討する。	1	1		－						
A.4.1.2						○	代替業務運用の範囲	無し	一部の業務について代替業務運用が必要	全部の業務について代替業務運用が必要					【重複項目】 C.3.1.2。復旧作業は、可用性と運用・保守性に共通して含まれている。運用・保守性では、復旧目標の運用への影響という観点でその作業を確認するが、可用性は、それを実現するための手段として確認する。 【メトリクス】 代替業務運用とは、障害によりシステムが復旧不可能となった場合に、代替業務でカバーすることが可能な運用手段（代替機あるいは人手による運用）を指す。	0	0		災対環境までは求めないが当行に業務影響を与えない範囲で可用性を担保すること。						
A.4.2.1			可用性確認	可用性として要求された項目をどこまで確認するかの範囲。		○	確認範囲	実施しない。または単純な障害の範囲	業務を継続できる障害の範囲	業務停止となる障害のうち一部の範囲	業務停止となる障害の全ての範囲				【レベル】 レベル2および3の確認範囲には、レベル1で定義した内容を含む。	1	1		－	1	業務を継続できる障害の範囲 業務停止となる障害が発生しても、復旧方法が自明であり、確認の必要がない場合。 [－] 障害時の対策を考慮しない場合 [+] 業務停止となる障害が発生した際、その復旧方法を事前に確認しておく必要がある場合	2	業務停止となる障害のうち一部の範囲 業務停止となる障害に対しての対策を確認する必要があるが、リスクの高い障害や、障害の種類により確認を限定することが可能な場合。 [－] 業務停止となる障害による影響が極めて少ないと判断できる場合 [+] 障害の種類や発生リスクを考慮せず、可能な範囲で確認が必要な場合	3	業務停止となる障害の全ての範囲	業務停止による影響が極めて大きく、考えられる障害に対して事前に確認が必要な場合。 [－] 障害の種類や発生リスクにより、システムへの影響を限定できる場合
B.1.1.1	性能・拡張性	業務処理量	通常時の業務量	性能・拡張性に影響を与える業務量。 該当システムの稼働時を想定し、合意する。 それぞれのメトリクスに於いて、単一の値だけでなく、前提となる時間帯や季節の特性なども考慮する。	○	○	ユーザ数	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用					【重複項目】 F.2.1.1。ユーザ数は性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもあるため、性能・拡張性とシステム環境・エコロジーの両方に含まれている。 【レベル】 前提となる数値が決められない場合は、類似システムなどを参考に仮の値でも良いので決めておくことが必要。	0	0		－	0	特定ユーザのみ 部門内利用などでユーザが特定できる場合を想定。 [+] ユーザを特定できない場合	1	上限が決まっている あらかじめ一定の上限値を設定する場合を想定。 [－] 特定のユーザのみ使用することを合意できた場合	2	不特定多数のユーザが利用 国民全体がアクセスする可能性があるような場合を想定。 [－] 一定の上限値を設定することが可能な場合
B.1.1.2						○	同時アクセス数	特定利用者の限られたアクセスのみ	同時アクセスの上限が決まっている	不特定多数のアクセス有り					【メトリクス】 同時アクセス数とは、ある時点でシステムにアクセスしているユーザ数のことである。	0	0		－	0	特定利用者の限られたアクセスのみ 登録ユーザから想定する。	1	同時アクセスの上限が決まっている システムに対してどのようなピークモデルを想定しているか確認する。	2	不特定多数のアクセス有り システムに対してどのようなピークモデルを想定しているか確認する。
B.1.1.3						○	データ量	全ての データ量が明確である	主要な データ量のみが明確である						【レベル1】 主要なデータ量とは、システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、マスター系テーブルやまなランザクションデータの一次保存分などがある。 主要なデータ量しか決まっていない場合、後工程に於いて、検討漏れデータの出現などによるディスク追加などが発生するリスクがある。	1	1	・MCIF DBデータ総量は108TB(最大テーブル5.3TB) ・顧客数約1億人、アプローチ対象顧客数は0.8億人 ・MCIF DB上でのデータ保管期間は概ね37ヶ月分を保持 ・取引履歴テーブルの	－	0	全ての データ量が明確である 要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	0	全ての データ量が明確である 要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	0	全ての データ量が明確である 要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合
B.1.1.4						○	オンラインリクエスト件数	処理毎にリクエスト件数が明確である	主な処理のリクエスト件数のみが明確である						【メトリクス】 オンラインリクエスト件数は単位時間を明らかにして確認する。 【レベル1】 主な処理とはシステムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民情報システムの転入・転出処理やネットショッピングシステムの決済処理などがある。 主なリクエスト件数しか決まっていない場合、後工程に於いて、検討漏れリクエストの出現などによるサーバ能力不足などのリスクがある。	1	1		－	0	処理毎にリクエスト件数が明確である 要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数が把握できていない場合	0	処理毎にリクエスト件数が明確である 要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数が把握できていない場合	0	処理毎にリクエスト件数が明確である 要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数が把握できていない場合
B.1.1.5						○	バッチ処理件数	処理単位毎に処理件数が決まっている	主な処理の処理件数が決まっている						【メトリクス】 バッチ処理件数は単位時間を明らかにして確認する。要件定義時には主な処理（特に該当システムでクリティカルとなる処理）では処理件数のおおよその目安は決まっているはずであり、それを元に性能や拡張性の検討を進める。要件定義時に明確になっていない場合は、確定度合も含め、想定しておく。 【レベル1】 主な処理とはシステムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。 主なバッチ処理件数しか決まっていない場合、後工程に於いて、検討漏れ処理の出現などによるサーバ能力不足などのリスクがある。	1	1		－	0	処理単位毎に処理件数が決まっている 要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	0	処理単位毎に処理件数が決まっている 要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	0	処理単位毎に処理件数が決まっている 要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合
B.1.1.6							業務機能数	業務機能が整理されている	確定した業務機能一覧が作成されている	業務機能一覧はあるが、確定していない					【メトリクス】 要件定義時には業務機能一覧はレベルの差があっても決まっているはずであり、それを元に性能や拡張性の検討を進める。要件定義時に明確になっていない場合は、確定度合も含め、想定しておく。	1	1		－						
B.1.2.1			業務量増大度	システム稼動開始からライフサイクル終了までの間で、開始時点と業務量が最大になる時点の業務量の倍率。 必要に応じ、開始日の平均値や、開始後の定常状態との比較を行う場合もある。		○	ユーザ数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	3	3		増大時にも仕様書に記載のサービスレベルを落とさないこと。 なお、拡張時の料金は過度に高額にならないようにすること。	0	1倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [+] 利用者の増加が見込まれる場合	1	1.2倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [－] 利用者が固定されている場合 [+] 利用者の増加が見込まれる場合	1	1.2倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [－] 利用者が固定されている場合 [+] 利用者の増加が見込まれる場合
B.1.2.2						○	同時アクセス数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	3	3		増大時にも仕様書に記載のサービスレベルを落とさないこと。 なお、拡張時の料金は過度に高額にならないようにすること。	0	1倍	システムのピークモデルがユーザ数の増によってどのように変わると考えているかを確認する。 [+] 利用者の増加が見込まれる場合	1	1.2倍	システムのピークモデルがユーザ数の増によってどのように変わると考えているかを確認する。 [－] 利用者が固定されている場合やユーザの増加とアクセスユーザの増加がリンクしない場合 [+] 利用者の増加が見込まれる場合	1	1.2倍	システムのピークモデルがユーザ数の増によってどのように変わると考えているかを確認する。 [－] 利用者が固定されている場合やユーザの増加とアクセスユーザの増加がリンクしない場合 [+] 利用者の増加が見込まれる場合
B.1.2.3						○	データ量増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	2	2		増大時にも仕様書に記載のサービスレベルを落とさないこと。 なお、拡張時の料金は過度に高額にならないようにすること。	0	1倍	業務のトレンドによってシステムで扱うデータ量がどの程度増加するかを確認する。 [+] 段階的稼働や、マスター蓄積システムの場合	1	1.2倍	業務のトレンドによってシステムで扱うデータ量がどの程度増加するかを確認する。 [－] データを蓄積しないゲートウェイシステムの場合 [+] 段階的稼働や、マスター蓄積システムの場合	1	1.2倍	業務のトレンドによってシステムで扱うデータ量がどの程度増加するかを確認。 [－] データを蓄積しないゲートウェイシステムの場合 [+] 段階的稼働や、マスター蓄積システムの場合
B.1.2.4						○	オンラインリクエスト件数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【メトリクス】 オンラインリクエスト件数は単位時間を明らかにして確認する。 【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	2	2		増大時にも仕様書に記載のサービスレベルを落とさないこと。 なお、拡張時の料金は過度に高額にならないようにすること。	0	1倍	システムの制約となるリクエスト数の見通しを確認する。	1	1.2倍	システムの制約となるリクエスト数の見通しを確認する。	1	1.2倍	システムの制約となるリクエスト数の見通しを確認する。
B.1.2.5						○	バッチ処理件数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【メトリクス】 バッチ処理件数は単位時間を明らかにして確認する。 【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	2	2		増大時にも仕様書に記載のサービスレベルを落とさないこと。 なお、拡張時の料金は過度に高額にならないようにすること。	0	1倍	システムの制約となる処理件数を確認する。	1	1.2倍	システムの制約となる処理件数を確認する。	1	1.2倍	システムの制約となる処理件数を確認する。
B.1.2.6							業務機能数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 業務機能数増大率を評価する際は、機能の粒度（1機能あたりの見積規模、サービス範囲など）は具体的数値を示すことが望ましい。 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	2	2		増大時にも仕様書に記載のサービスレベルを落とさないこと。 なお、拡張時の料金は過度に高額にならないようにすること。									
B.1.3.1			保管期間	システムが参照するデータのうち、OSやミドルウェアのログなどのシステム基盤が利用するデータに対する保管が必要な期間。 必要に応じて、データの種別毎に定める。		○	保管期間	6ヶ月	1年	3年	5年	10年以上有期	永久保管		【レベル】 対象が複数あり、それぞれの保管期間が異なる場合は、それぞれの対象データについて決めること。 【レベル0】 保管期間の制約が短い場合は6ヶ月で代用する。	2	2		－	1	1年 毎年データを更新していく想定。 [－] 保管データがほとんど無い場合 [+] ディスク容量に余裕がある場合	3	5年 税制などの対応で保管期間が規定されているという想定。 [－] 参照期間が限られていて、バックアップ媒体に吸い上げることが可能な場合 [+] ディスク容量に余裕がある場合	4	10年以上有期 エンドユーザに保証している外部要件などで、保管期間が決められていると想定。 [－] 参照期間が限られていて、バックアップ媒体に吸い上げることが可能な場合 [+] ディスク容量に余裕がある場合
B.1.3.2				保管対象のデータを選択する際には、対象範囲についても決めておく。			対象範囲	オンラインで参照できる範囲	アーカイブまで含める						【メトリクス】 保管対象のデータを配置する場所を決める。保管場所によっては参照するための手間がかかる場合がある。また、バックアップの取得方法などへの配慮が必要になる。	1	1		－						
B.2.1.1		性能目標値	オンラインレスポンス	オンラインシステム利用時に要求されるレスポンス。 システム化する対象業務の特性をふまえ、どの程度のレスポンスが必要かについて確認する。ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に順守率を決める。具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。 （例：Webシステムの参照系/更新系/一覧系など）		○	通常時レスポンス順守率	順守率を定めない	60%	80%	90%	95%	99%以上		【レベル】 具体的な目標値や約束値がある場合、各処理の順守率を規定する。 レベルに示した順守率はおおまかな目安を示しており、具体的にはレスポンスと順守率について数値で合意する必要がある。	0	0		－	0	順守率を定めない トランザクションの量が少ない場合、または多い場合でもユーザに対する利用制限などが可能な場合を想定。 [+] 性能低下が、システムの評価低下につながる場合	3	90% 管理対象とする処理の中で、通常時のトランザクション数の90%が目標値を達成できれば良いと想定。 [－] 遅くても、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、システムの評価低下につながる場合	5	99%以上 管理対象とする処理の中で、通常時のトランザクション数の99%が目標値を達成できれば良いと想定。 [－] 遅くても、処理出来れば良い場合。または代替手段がある場合
B.2.1.2						○	ピーク時レスポンス順守率	順守率を定めない	60%	80%	90%	95%	99%以上		【レベル】 具体的な目標値や約束値がある場合、各処理の順守率を規定する。 レベルに示した順守率はおおまかな目安を示しており、具体的にはレスポンスと順守率について数値で合意する必要がある。	0	0		高負荷時においてはゆうちょ銀行と協議の上、決定	0	順守率を定めない トランザクションの量が少ない場合、または多い場合でもユーザに対する利用制限などが可能な場合を想定。 [+] 性能低下が、システムの評価低下につながる場合	2	80% 管理対象とする処理の中で、ピーク時のトランザクション数の80%が目標値を達成できれば良いと想定。 [－] 遅くとも、処理出来れば良い場合、または代替手段がある場合 [+] 性能低下が、システムの評価低下につながる場合	4	95% 管理対象とする処理の中で、ピーク時のトランザクション数の95%が目標値を達成できれば良いと想定。 [－] 遅くとも、処理出来れば良いか代替手段がある場合 [+] 性能低下が、システムの評価低下につながる場合
B.2.1.3							縮退時レスポンス順守率	縮退をしない	60%	80%	90%	95%	99%以上		【レベル】 具体的な目標値や約束値がある場合、各処理の順守率を規定する。 レベルに示した順守率はおおまかな目安を示しており、具体的にはレスポンスと順守率について数値で合意する必要がある。	0	0		－						
B.2.2.1			バッチレスポンス（ターンアラウンドタイム）	バッチシステム利用時に要求されるレスポンス。 システム化する対象業務の特性をふまえ、どの程度のレスポンス（ターンアラウンドタイム）が必要かについて確認する。更に、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に順守率を決める、具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。 （例：日次処理/月次処理/年次処理など）		○	通常時レスポンス順守度合い	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる					【レベル1】 所定の時間には再実行は含まない。	1	1		－	0	順守度合いを定めない 比較的小規模のデータしかないため、バッチのレスポンス順守度に関しては特に規定しないと想定。	2	再実行の余裕が確保できる 管理対象とする処理の中で、通常時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 [－] 再実行をしない場合または代替手段がある場合	2	再実行の余裕が確保できる 管理対象とする処理の中で、通常時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 [－] 再実行をしない場合または代替手段がある場合
B.2.2.2						○	ピーク時レスポンス順守度合い	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる					【レベル1】 所定の時間には再実行は含まない。	0	0		高負荷時においてはゆうちょ銀行と協議の上、決定	0	順守度合いを定めない 比較的小規模のデータしかないため、バッチのレスポンス順守度に関しては特に規定しないと想定。	2	再実行の余裕が確保できる 管理対象とする処理の中で、ピーク時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 ピーク時に余裕が無くなる場合にはサーバ増設や処理の分割などを考慮する必要がある。 [－] 再実行をしない場合または代替手段がある場合	2	再実行の余裕が確保できる 管理対象とする処理の中で、ピーク時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良い想定。 ピーク時に余裕が無くなる場合にはサーバ増設や処理の分割などを考慮する必要がある。 [－] 再実行をしない場合または代替手段がある場合
B.2.2.3							縮退時レスポンス順守度合い	縮退をしない	所定の時間内に収まる	再実行の余裕が確保できる					【レベル1】 所定の時間には再実行は含まない。	0	0		－						
B.2.3.1			オンラインスループット	オンラインシステム利用時に要求されるスループット。 システム化する対象業務の特性をふまえ、単位時間にどれだけの量の作業ができるかを確認する。更に、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に処理余裕率を決める、具体的な数値は特定の機能またはシステム分類毎に決めておくこと			通常時処理余裕率	1倍（余裕無し）	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 ここでの余裕率は、システム全体で処理できるトランザクション量を示す。例えば、レベル3（2倍）であれば、2倍のトランザクションを処理できることを言う。 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	1	1		－						
B.2.3.2							ピーク時処理余裕率	1倍（余裕無し）	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 ここでの余裕率は、システム全体で処理できるトランザクション量を示す。例えば、レベル3（2倍）であれば、2倍のトランザクションを処理できることを言う。 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	0	0		高負荷時においてはゆうちょ銀行と協議の上、決定						
B.2.3.3							縮退時処理余裕率	縮退をしない	通常時の1/2の処理が出来る	通常時と同様に処理が出来る						0	0		－						
B.2.4.1			バッチスループット	バッチシステム利用時に要求されるスループット。 システム化する対象業務の特性をふまえ、どの程度のスループットを確保すべきか確認する。更に、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に処理余裕率を決める、具体的な数値は特定の機能またはシステム分類毎に決めておくこと			通常時処理余裕率	1倍（余裕無し）	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	1	1		－						
B.2.4.2							ピーク時処理余裕率	1倍（余裕無し）	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	0	0		高負荷時においてはゆうちょ銀行と協議の上、決定						
B.2.4.3							縮退時処理余裕率	縮退をしない	通常時の1/2の処理が出来る	通常時と同様に処理が出来る						0	0		－						
B.2.5.1			帳票印刷能力	帳票印刷に要求されるスループット。 業務で必要な帳票の出力時期や枚数を考慮し、どの程度のスループットが必要かを確認する。 更に、ピーク特性や、			通常時印刷余裕率	1倍（余裕無し）	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	－			－						
B.2.5.2							ピーク時印刷余裕率	1倍（余裕無し）	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	－			－						

項番	大項目	中項目	小項目	小項目説明	最低限必要項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	運用コストへの影響	備考	LMシステム	PDCAツール	PDCAツール補足	LMシステム補足事項 （凡例） －：補足事項無	社会的影響が殆ど無いシステム 選択レベル	社会的影響が殆ど無いシステム 選択時の条件	社会的影響が限定されるシステム 選択レベル	社会的影響が限定されるシステム 選択時の条件	社会的影響が極めて大きいシステム 選択レベル	社会的影響が極めて大きいシステム 選択時の条件
B.2.5.3				障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に余裕率を決める。具体的な数値は特定の帳票や			縮退時印刷余裕率	縮退をしない	通常時の1/2の印刷が出来る	通常時と同様に印刷が出来る						－		－							
B.3.1.1		リソース拡張性	CPU拡張性	CPUの拡張性を確認するための項目。 CPU利用率は、将来の業務量の増加に備え、どれだけCPUに余裕をもたせておくかを確認するための項目。 CPU拡張性は、物理的もしくは仮想的に、どれだけCPUを拡張できるように しておくかを確認するための項目。 CPUの専有の有無に		○	CPU利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			○	【メトリクス】 CPU利用率は単位時間に、実行中のプログラムがCPUを使用している割合を示している。単位時間をどの程度にするか、また、動作するプログラムの特性によって数値は大きく異なる。 【レベル】 レベルに示した利用率はおおまかな目安を示しており、具体的な数値で合意する必要がある。 【運用コストへの影響】	1	1		－	0	80%以上	システムが過剰設備となっていないという想定。 [+] 近い将来利用者が増える予定がある場合	1	50%以上 80%未満	業務量の増加に備え、余裕を持たせている状態を想定。 [－] 性能・拡張性より低コストであることを優先する場合 [+] 近い将来利用者が増える予定がある場合	1	50%以上 80%未満	業務量の増加に備え、余裕を持たせている状態を想定。 [－] 性能・拡張性より低コストであることを優先する場合 [+] 近い将来利用者が増える予定がある場合
B.3.1.2						○	CPU拡張性	1倍（拡張要求なし）	1.5倍の拡張が可能	2倍の拡張が可能	4倍の拡張が可能	8倍以上の拡張が可能		○	【運用コストへの影響】 CPU拡張性がない場合、機器自体の増設や、環境や契約の変更が必要になる場合がある。	1	1		クラウドサービスを利用する場合、クラウドサービスの特性により考慮不要	0	1倍（拡張要求なし）	部門内限定の利用であり、CPUの拡張が不要な場合	1	1.5倍の拡張が可能	2～3年後のシステム拡張に備え、CPU増設を可能にしたと想定。	1	1.5倍の拡張が可能	2～3年後のシステム拡張に備え、CPU増設を可能にしたと想定。
B.3.2.1			メモリ拡張性	メモリの拡張性を確認するための項目。 メモリ利用率は、将来の業務量の増加に備え、どれだけメモリに余裕をもたせておくかを確認するための項目。 メモリ拡張性は、物理的もしくは仮想的に、どれだけメモリを拡張できるようにしておくかを確認するための項目。 メモリの専有の有無		○	メモリ利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			○	【メトリクス】 メモリ利用率は単位時間に、実行中のプログラムがメモリを使用している割合を示している。単位時間をどの程度にするか、また、動作するプログラムの特性によって数値は大きく異なる。 【レベル】 レベルに示した利用率はおおまかな目安を示しており、具体的な数値で合意する必要がある。 【運用コストへの影響】	1	1		－	0	80%以上	システムが過剰設備となっていないという想定。 [+] 近い将来利用者が増える予定がある場合	1	50%以上 80%未満	業務量の増加に備え、余裕を持たせている状態を想定。 [－] 性能・拡張性より低コストであることを優先する場合 [+] 近い将来利用者が増える予定がある場合	1	50%以上 80%未満	業務量の増加に備え、余裕を持たせている状態を想定。 [－] 性能・拡張性より低コストであることを優先する場合 [+] 近い将来利用者が増える予定がある場合
B.3.2.2						○	メモリ拡張性	1倍（拡張要求なし）	1.5倍の拡張が可能	2倍の拡張が可能	4倍の拡張が可能	8倍以上の拡張が可能		○	【運用コストへの影響】 メモリ拡張性がない場合、機器自体の増設や、環境や契約の変更が必要になる場合がある。	1	1		クラウドサービスを利用する場合、クラウドサービスの特性により考慮不要	0	1倍（拡張要求なし）	部門内限定の利用であり、メモリの拡張が不要な場合	1	1.5倍の拡張が可能	2～3年後のシステム拡張に備え、メモリ増設を可能にしたと想定。	1	1.5倍の拡張が可能	2～3年後のシステム拡張に備え、メモリ増設を可能にしたと想定。
B.3.3.1			ディスク拡張性	ディスクの拡張性を確認するための項目。 ディスク利用率は、将来の業務量の増加に備え、どれだけディスクに余裕をもたせておくかを確認するための項目。			ディスク利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			○	【レベル】 レベルに示した利用率はおおまかな目安を示しており、具体的な数値で合意する必要がある。 【運用コストへの影響】 ディスクに空きが無い場合、単純増加ファイルの監視等が必要になる。	1	1		－									
B.3.3.2				ディスク拡張性は、物理的もしくは仮想的に、どれだけディスクを拡張できるようにし			ディスク拡張性	1倍（拡張要求なし）	1.5倍の拡張が可能	2倍の拡張が可能	4倍の拡張が可能	8倍以上の拡張が可能		○	【運用コストへの影響】 ディスク拡張性がない場合、機器自体の増設や、環境や契約の変更が必要になる場合がある。	1	1		クラウドサービスを利用する場合、クラウドサービスの特性により考慮不要									
B.3.4.1			ネットワーク	システムで使用するネットワーク環境の拡張性に関する項目。 既存のネットワーク機器を活用する場合は既存ネットワークの要件を確認するために利用する。 ネットワークの帯域については「B.4.1 帯域保証機能の有無」で確認する。			ネットワーク機器設置範囲	無し	フロア内のLAN	同一拠点（ビル）内のLAN	社内複数拠点間の接続（LAN、WAN）	社外拠点との接続			4	4		P-NET利用の場合は対象外とする。								
B.3.5.1			サーバ処理能力増強	サーバ処理能力増強方法に関する項目。 将来の業務量増大に備える方法（スケールアップ/スケールアウト）をあらかじめ考慮しておくこと。どちらの方法を選択するかはシステムの特徴によって使い分けることが必要。 スケールアップは、より処理能力の大きなサーバとの入れ替えを行うことで処理能力の増強を行う。			スケールアップ	スケールアップを行わない	一部のサーバのみを対象	複数のサーバを対象				【メトリクス】 あらかじめ余剰リソースを用意しておくことで速やかにスケールアップを行う等、スケールアップの迅速性についても検討する。 また、スケールアップしている状態は、コスト増に繋がる場合があるため、必要に応じてスケールダウンの迅速性についても考慮する。 【レベル1】 オンライントランザクション処理のような更新系の割合が多いシステムでアプリケーションサーバをスケールアップする場合を想定。 【レベル2】 レベル1に加え、DBサーバのスケールアップを追加する場合を想定。	2	2		取り扱うデータ量及びユーザ数の変動に対応できることを想定								
B.3.5.2				スケールアップは同等のサーバを複数台用意し、サーバ1台数を増やすことで処理能力の増強を行う。			スケールアウト	スケールアウトを行わない	一部のサーバのみを対象	複数のサーバを対象					【メトリクス】 スケールアップと同様、スケールアウトの迅速性についても検討する。 また、必要に応じて、スケールインの迅速性についても検討する。 【レベル1】 Webサーバと負荷分散装置などフロント部分を複数台用意する場合を想定。 【レベル2】 レベル1に加え、バックエンドのサーバを複数台用意する場合を想定。	2	0	PDCAツールはシングル構成であり、原則スケールアップで対応。	取り扱うデータ量及びユーザ数の変動に対応できることを想定							
B.4.1.1		性能品質保証	帯域保証機能の有無	ネットワークのサービス品質を保証する機能の導入要否およびその程度。 伝送遅延時間、パケット損失率、帯域幅をなんらかの仕組みで決めているかを示す。回線の帯域が保証されていない場合性能悪化につながることがある。			帯域保証の設定	無し	プロトコル単位で設定	各サーバ毎に設定	アプリケーションのエンドツーエンドで検証・保証					1	0	PDCAツール側での帯域保証設定は不要。	P-NET利用の場合は対象外とする。							
B.4.1.2			HWリソース専有の有無	サーバのリソース（CPUやメモリ）を専有するか、共有するかを示す。HWリソースを他のサーバと共有する場合、他のサーバの影響を受けて、性能悪化につながることがある。			HWリソース専有の設定	無し（共有）	有り（専有）						0	0		－								
B.4.2.1			性能テスト	構築したシステムが当初/ライフサイクルに渡っての性能を発揮できるかのテストの測定頻度と範囲。			測定頻度	測定しない	構築当初に測定	運用中、必要時に測定可能	運用中、定常的に測定					2	2		－								
B.4.2.2							確認範囲	確認しない	一部の機能について、目標値を満たしていることを確認	全ての機能について、目標値を満たしていることを確認						1	1		－								
B.4.3.1			スパイク負荷対応	通常時の負荷と比較して、非常に大きな負荷が短時間に現れることを指す。業務量の想定されたピークを超えた状態。 特にB2Cシステムなどクライアント数を制限できないシステムで発生する。システムの処理上限を超えることが多いため、Sorry動作を実装し対策する場合が多い。			トランザクション保護	トランザクション保護は不要である	同時トランザクション数の制限機能	同時トランザクション数の制限機能に加え、Sorry動作	独立したSorry動作を行うサーバの設置				0	0		－								
C.1.1.1	運用・保守性	通常運用	運用時間	システム運用を行う時間、利用者やシステム管理者に対してサービスを提供するために、システムを稼動させ、オンライン処理やバッチ処理を実行している時間帯のこと。	○	○	運用時間（通常）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止		【重複項目】 A.1.1.1、運用時間（通常）は、システムの可用性の実現レベルを表す項目でもあるため、重複項目となっている。 【メトリクス】 運用時間は、オンライン/バッチを含みシステムが稼動している時間帯を指す。 【レベル】 （）内の時間は各レベルの一例を示したもので、レベル選定の条件とはしていない。規定無しは、固定のサービス時間が存在しないことを示し、基本的にシステムは停止していて、必要に応じてユーザがシステムを起動するようなケースを想定している（例：障害発生に備えた予備システム、開発・検証用システム等）。定時内や夜間のみ停止は、一般的な業務形態を想定したもので、業務が稼動する時間帯が異なるシステムにおいては、時間帯をスライドさせるなどの読替えが必要である。停止有りとは、システムを停止しなければならない時間帯ではなく、システムを停止できる可能性のある時間帯を指す。24時間無停止は、オンライン業務が稼動していない時間にバッチを稼動させる必要があり、システムを停止することができないようなケースも含まれる。	3	3		－	2	夜間のみ停止（9時～21時）	夜間に実施する業務はなく、システムを停止可能。 [－] 運用時間をもっと限って業務を稼働させる場合 [+] 24時間無停止やリブート処理等の短時間の停止のみを考える場合	4	若干の停止有り（9時～翌朝8時55分）	24時間無停止での運用は必要ないが、極力システムの稼働は継続させる。 [－] 夜間のアクセスは認めないなど、長時間運用を停止する場合 [+] 24時間無停止で運用する場合	5	24時間無停止	システムを停止できる時間帯が存在しない。 [－] 1日のスケジュールで定期的に運用を停止する時間帯が存在する場合
C.1.1.2					○	○	運用時間（特定日）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止		【重複項目】 A.1.1.2、運用時間（特定日）は、システムの可用性の実現レベルを表す項目でもあるため、重複項目となっている。 【メトリクス】 特定日とは、休日/祝祭日や月末月初など通常の運用スケジュールとは異なるスケジュールを定義している日のことを指す。特定日が複数存在する場合は、それぞれにおいてレベル値を整合する必要がある（例：「月～金はレベル2だが、土日はレベル0」、「通常はレベル5だが、毎月1日にリブートをするためその日はレベル3」など）。 また、ユーザの休日だけでなく、ベンダの休日についても特定日として認識し、運用保守体制等を整合すること。	2	2		－	0	規定無し	通常と異なる運用時間となる特定日は存在しない。 [+] 休日にバックアップ運用を行うなど、通常とは異なる運用時間となる特定日が存在する場合	2	夜間のみ停止（9時～21時）	週末はバックアップ運用のみのため、夜間は停止する。 [－] 週末運用するバックアップやバッチ処理などが存在せず、土休日は運用を停止する場合 [+] 休日出勤する社員の業務に必要なため、土休日も運用する場合	5	24時間無停止	システムを停止できる時間帯が存在しない。 [－] 定期的に運用を停止する日が存在する場合
C.1.2.1			バックアップ	システムが利用するデータのバックアップに関する項目。		○	データ復旧範囲	復旧不要	一部の必要なデータのみ復旧	システム内の全データを復旧					【重複項目】 A.2.6.2、可用性ではデータをどこまで保全するかという観点で、運用ではデータをどこまで復旧させるかという観点で本項目が必要となり、重複項目としている。 【メトリクス】 システムを障害から復旧するためには、データバックアップ以外に、OSやアプリケーションの設定ファイル等を保管するシステムバックアップも必要となることが考えられる。システムバックアップの取得方法や保管方法についても、同時に検討すべきである。 【レベル1】 一部の必要なデータとは、業務継続性の要求を満たすために必要となるようなデータを想定している。	2	LM準拠	ハードウェア関連はLMシステム準拠。	－							
C.1.2.2						○	外部データの利用可否	全データの復旧に利用できる	一部のデータ復旧に利用できる	外部データは利用できない					【メトリクス】 外部データとは、当該システムの範囲外に存在するシステムの保有するデータを指す（開発対象のシステムと連携する既存システムなど）。外部データによりシステムのデータが復旧可能な場合、システムにおいてバックアップ設計を行う必要性が減るため、検討の優先度やレベルを下げて考えることができる。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－	1	一部のデータ復旧に利用できる	他システムから必要なデータを修復することができるため、バックアップによってシステムの全データを復旧しなくてもよいことを想定。 [－] 外部に同じデータを持つシステムが存在するため、バックアップを取得しなくても本システムの全データを復旧できるような場合	2	外部データは利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [－] 外部に同じデータを持つシステムが存在するため、本システムに障害が発生した際には、そちらからデータを持ってきてシステムを復旧できるような場合	2	外部データは利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [－] 外部に同じデータを持つシステムが存在するため、本システムに障害が発生した際には、そちらからデータを持ってきてシステムを復旧できるような場合
C.1.2.3						○	バックアップ利用範囲	バックアップを取得しない	障害発生時のデータ損失防止	ユーザエラーからの回復	データの長期保存（アーカイブ）				【メトリクス】 マルウェア等によるデータ損失への備えや、監査のためのログの退避など、セキュリティ観点のバックアップも考慮すること。 【レベル2】 ユーザエラーからの回復の場合、システムとしては正常に完了してしまった処理を元に戻さなければならないため、複数世代のバックアップの管理や時間指定回復（Point in Time Recovery）等の機能が必要となる場合が考えられる。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－	1	障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [－] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 復旧時点（RPO）が固定ではなく、障害の内容に応じて時間指定で復旧する必要がある場合	2	ユーザエラーからの回復	管理者の作業ミスなどによって発生したデータ損失について6回復できることを保証したい。 [－] 管理者の作業ミスによる復旧は管理者が作業前に個別にデータ保全作業を実施することで担保することとし、バックアップによる回復は必要としない場合 [+] データ損失からの回復だけでなく、過去データの保存用途に用いる場合	3	データの長期保存（アーカイブ）	内部統制対応の要件に基づき、データの履歴を保存する必要がある。 [－] バックアップはデータ損失からの回復に対する用途にのみ使用する場合
C.1.2.4						○	バックアップ自動化の範囲	全ステップを手動で行う	一部のステップを手動で行う	全ステップを自動で行う				○	【メトリクス】 バックアップ運用には、 ・スケジュールに基づくジョブ起動 ・バックアップ対象の選択 ・バックアップ先の選択 ・ファイル転送 などといった作業ステップが存在する。 【運用コストへの影響】 バックアップ運用の自動化を実現するためには、ハードウェア・ソフトウェアに対する投資が必要となり導入コストは増大する。しかし、運用中におけるバックアップ作業をユーザが実施する必要がなくなるため、その分運用コストは減少すると考えられる。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－	0	全ステップを手動で行う	バックアップに関するオペレーションはスケジュール管理も含めて基本的に手動で実行する。 [+] バックアップに関する管理者のオペレーションを削減したい場合	1	一部のステップを手動で行う	バックアップに関するオペレーションはバックアップ管理のソフトウェアを導入して自動化するが、一部の作業（特定のコマンド実行、テープ交換等）は手動にて実施する必要がある。 [－] 管理者が全てのステップを手動で実行する場合 [+] バックアップ運用の全てのステップを自動で行いたい場合	2	全ステップを自動で行う	バックアップに関するオペレーション（スケジュール管理、メディア管理、ジョブ実行等）に関して、管理ソフトウェアを導入して自動で行うことを想定。 [－] 管理者が手動でバックアップを実行する場合
C.1.2.5						○	バックアップ取得間隔	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ			4	LM準拠	ハードウェア関連はLMシステム準拠。	－	1	システム構成の変更時など、任意のタイミング	バックアップから復旧する必要のあるマスターデータ等は、運用中ほとんど更新されることがないため、定期的にではなく、マスターデータ更新時にバックアップを取得することを想定。 [+] バックアップから復旧する必要のあるデータがトランザクショナルなデータで運用中随時更新されるようなものである場合	4	日次で取得	全体バックアップは週次で取得する。しかし、RPO要件である、1日前の状態に戻すためには、毎日差分バックアップを取得しなければならないことを想定。 [－] RPOの要件が[－]される場合 [+] RPOの要件が[+]される場合や、複数世代を確保してバックアップの可用性を高めたい場合	5	同期バックアップ	RTOの要件を満たすため、更新内容をバックアップサイトへ転送し、障害発生時にすぐに運用が可能なDRサイトを構成することを想定。 [－] 障害発生時にバックアップからのリカバリ作業のため運用の停止が許されるような場合
C.1.2.6						○	バックアップ保存期間	バックアップを保存しない	1年未満	3年	5年	10年以上有限	永久保存		【メトリクス】 主に可用性の観点で実施されるバックアップの世代管理とは別に、ここではデータ保全という観点でバックアップデータの保存期間を検討する。	3	LM準拠	ハードウェア関連はLMシステム準拠。	－	0	バックアップを保存しない	バックアップデータは障害復旧用途にのみ利用されるものであり、データ保存の用途には使用しないことを想定。 [+] バックアップをデータアーカイブの用途に利用するような場合	2	3年	社内規定でデータの更新履歴を3年間保持しなければならないことを想定。 [－] 保管先容量の制限で3年分をシステム上に保持できない場合 [+] 社内外の規定が変更されて保存期間が延長されることが想定される場合	4	10年以上有限	10年間のデータ保存が法律で規定されているような場合を想定。 [－] 保存先容量の制限で10年分をシステム上に保持できない場合 [+] 保存先容量に制限がなく、永続的にデータを保管しなければならない場合
C.1.2.7						○	バックアップ方式	バックアップ無し	オフラインバックアップ	オンラインバックアップ	オフラインバックアップ+オンラインバックアップ				【重複項目】 A.2.6.1、バックアップ方式は、システムを停止するかどうかの検討が含まれるため、可用性の観点でも考慮する必要があり、重複項目となっている。 【レベル】 オフラインバックアップとは、システム（あるいはその一部）を停止させてバックアップを行う方式。オンラインバックアップとはシステムを停止せず稼働中の状態でバックアップを行う方式を指す。	2	LM準拠	ハードウェア関連はLMシステム準拠。	－							
C.1.3.1		運用監視	システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目。 セキュリティ監視については本項目には含めない。「E.1 不正監視」で別途検討すること。			○	監視情報	監視を行わない	死活監視を行う	エラー監視を行う	エラー監視（トレース情報を含む）を行う	リソース監視を行う	パフォーマンス監視を行う	○	【メトリクス】 監視とは情報収集を行った結果に応じて適切な宛先に発報することを意味する。本項目は、監視対象としてどのような情報を発信するべきかを決定することを目的としている。また、監視情報の発報先については、「C.4.5.2 監視システムの有無」で確認すること。 【レベル】 死活監視とは、対象のステータスがオンラインの状態にあるかオフラインの状態にあるかを判断する監視のこと。 エラー監視とは、対象が出力するログ等にエラー出力が含まれているかどうかを判断する監視のこと。トレース情報を含む場合は、どのモジュールでエラーが発生しているのか詳細についても判断することができる。 リソース監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいてCPUやメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視のこと。 パフォーマンス監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスクI/O、ネットワーク転送等の応答時間やスループットについて判断する監視のこと。 【運用コストへの影響】 エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が	4	LM準拠	ハードウェア関連はLMシステム準拠。	－	2	エラー監視を行う	管理者がすぐにシステムにアクセスして障害状況を調査することができるため、バックアップによってシステムの全データを復旧しなくても、ある程度障害箇所が判断できるようにする必要がある場合	3	エラー監視（トレース情報を含む）を行う	夜間の障害時にも、管理者に状況を通知し、すぐ対処が必要なのかどうかを判断するため、詳細なエラー情報まで監視を行うことを想定。 [－] 障害時は管理者がすぐにシステムにアクセスできるため、詳細なエラー情報まで監視する必要がない場合 [+] エラー情報だけでなく、リソース使用状況も監視して、障害発生を未然に防ぎたい場合	4	リソース監視を行う	CPU使用率やスワップの発生状況等に対して閾値を設定し、サービスレベル低下の予兆を監視して、システムの拡張計画や運用スケジュールの検討を行うことを想定。 [－] 障害の発生を検知して管理者への対応を促すのみで良い場合 [+] 業務アプリケーションの応答時間やスループットなど、より厳密にシステムのサービスレベルを評価したいような場合

項番	大項目	中項目	小項目	小項目説明	最低限必要な項目	重要な項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	運用コストへの影響	備考	LMシステム	PDCAツール	PDCAツール補足	LMシステム補足事項 （凡例） －：補足事項無	社会的影響が殆ど無いシステム 選択レベル	社会的影響が殆ど無いシステム 選択時の条件	社会的影響が限定されるシステム 選択レベル	社会的影響が限定されるシステム 選択時の条件	社会的影響が極めて大きいシステム 選択レベル	社会的影響が極めて大きいシステム 選択時の条件
C.1.3.2						○	監視間隔	監視を行わない	不定期監視（手動監視）	定期監視（1日間隔）	定期監視（数時間間隔）	リアルタイム監視（分間隔）	リアルタイム監視（秒間隔）			4	LM準拠	ハードウェア関連はLMシステム準拠。	－	1	不定期監視（手動監視） 必要に応じて管理者が手動確認をするため、診断間隔は不定期となることを想定。 [+] 手動確認ではなく、システムに監視をさせて必要に応じて管理者に通知をさせたい場合	4	リアルタイム監視（分間隔） 障害を検知するまでの時間がかかってしまうが、システムに対する監視情報収集のコストを低くすることを優先し、分間隔での監視とすることを想定。 [－] 障害の検知はアプリケーションの機能で実装し、システム基盤としての監視としては定期的な運用状況のレポートのみでよいような場合 [+] 障害検知までの時間を短縮したいような場合	5	リアルタイム監視（秒間隔） 障害発生時にはすぐに検知して対処に移れるように、秒間隔での監視を行うことを想定。 [－] 監視情報の収集がアプリケーションのパフォーマンスに影響するリスクを回避するため、監視間隔を広げるような場合
C.1.3.3							システムレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 システムレベルの監視とは、業務アプリケーションも含め、そのシステムを構成する複数のサーバ等の状態確認結果から、システムとして機能する状態にあるかどうかを判断するものである。バックアップの監視やジョブの監視などが該当する。 【レベル】 監視を行う場合には、システムレベルについての監視情報と監視間隔を個別に確認する必要がある。システムが提供するいくつかの機能のうち、重要度の高い一部の機能のみを対象に監視を行うことを想定している。	2	LM準拠	ハードウェア関連はLMシステム準拠。	－						
C.1.3.4							プロセスレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 プロセスレベルの監視とは、アプリケーションやミドルウェア等のプロセスが正しく機能しているかどうかを判断するものである。主にOSコマンドによるプロセスの情報（死活、CPU使用率、メモリ使用率など）を監視するものを想定している。 【レベル】 監視を行う場合は、プロセスレベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上で稼動する複数のプロセス（アプリケーションおよびミドルウェア）のうち、重要度の高い一部のプロセスのみを対象に監視を行うことを想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－						
C.1.3.5							データベースレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 データベースレベルの監視とは、DBMSの機能として提供される情報を確認し、正しく機能しているかを判断するものである。ログ出力内容やパラメータ値、ステータス情報、領域使用率等の監視を想定している。 【レベル】 監視を行う場合は、データベースレベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上で稼動する複数のデータベースのうち、重要度の高い一部のデータベースのみを対象に監視を行うことを想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－						
C.1.3.6							ストレージレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 ストレージレベルの監視とは、ディスクアレイ等の外部記憶装置に関して、状態を確認し、正しく機能しているかを判断するものである。OSコマンドによって確認できるディスク使用率等の他、ファームウェアが出力するログ情報などの監視を想定している。 【レベル】 監視を行う場合は、ストレージレベルについての監視情報と監視間隔を個別に確認する必要がある。 レベル1の一部とは、システムに接続される複数のストレージのうち、重要度の高い一部のストレージのみを対象に監視を行うことを想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－						
C.1.3.7							サーバ（ノード）レベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 サーバ（ノード）レベルの監視とは、対象のサーバがOSレベルで正しく機能しているかを判断するものである。ハートビート監視などが該当する。 【レベル】 監視を行う場合は、サーバ（ノード）レベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上に存在する複数のサーバ（ノード）のうち、重要度の高い一部のサーバのみを対象に監視を行うことを想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－						
C.1.3.8							端末/ネットワーク機器レベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 端末/ネットワーク機器レベルの監視とは、クライアント端末やルータ等のネットワーク機器に関して、状態を確認し、正しく機能しているかを判断するものである。ハートビート監視の他、個別のファームウェア等が出力する情報に基づく監視などを想定している。 【レベル】 監視を行う場合は、端末/ネットワーク機器レベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上に存在する複数の端末/ネットワーク機器のうち、重要度の高い一部の端末/ネットワーク機器のみを対象に監視を行うことを想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－						
C.1.3.9							ネットワーク・パケットレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 ネットワーク・パケットレベルの監視とは、ネットワーク上を流れるパケットの情報を確認し、正しく機能しているかを判断するものである。パケットロスやネットワーク帯域の使用率などの監視などを想定している。 【レベル】 監視を行う場合は、ネットワーク・パケットレベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上の複数のネットワーク経路のうち、重要度の高い一部のネットワーク経路のみを対象に監視を行うことを想定している。	1	LM準拠	ハードウェア関連はLMシステム準拠。	－						
C.1.4.1			時刻同期	システムを構成する機器の時刻同期に関する項目。			時刻同期設定の範囲	時刻同期を行わない	サーバ機器のみ時刻同期を行う	サーバおよびクライアント機器について時刻同期を行う	ネットワーク機器も含めシステム全体で時刻同期を行う	システム全体を外部の標準時間と同期する		○	【レベル4】 システム全体を外部の標準時間と同期する場合、外部との接続に異常が発生した場合にシステム内の時刻同期をどうするかといった設計を行う必要がある。 【運用コストへの影響】 時刻同期を行うことで、複数のサーバ機器が出力するログの順序保証が得られるため、障害調査や監査等の作業コストを下げられる可能性がある。	3	3		－						
C.2.1.1		保守運用	計画停止	点検作業や領域拡張、デフラグ、マスターデータのメンテナンス等、システムの保守作業の実施を目的とした、事前計画済みのサービス停止に関する項目。	○	○	計画停止の有無	計画停止有り（運用スケジュールの変更可）	計画停止有り（運用スケジュールの変更不可）	計画停止無し				○	【重複項目】 A.1.1.3。計画停止の有無は、システムの可用性の実現レベルを表す項目でもあるため、重複項目となっている。 【運用コストへの影響】 計画停止有りの場合、事前のバックアップや、システム構成に応じた手順準備など、運用時のコストがかさむ。	0	0		21:00～8:00迄の間、または非営業日（土、日、祝日）期間に限り計画停止を容認する。	0	計画停止有り（運用スケジュールの変更可） 事前の合意があれば、停止は可能。 [+] 運用時間外での停止だけで対応可能な場合	1	計画停止有り（運用スケジュールの変更不可） 24時間無停止での運用は必要ない、停止可能な時間が存在し、計画的な停止は可能。 [－] 運用スケジュールとしては停止可能な時間帯は存在しないが、事前の調整で停止が可能な場合 [+] 24時間無停止が要求される場合	2	計画停止無し システムを停止できる時間帯が存在しない。 [－] 運用スケジュールとして停止可能な時間帯が存在し、計画停止の必要性がある場合
C.2.1.2							計画停止の事前アナウンス	計画停止が存在しない	計画停止は年間計画によって確定する	1ヶ月前に通知	1週間前に通知	前日に通知		○	【運用コストへの影響】 計画停止が存在する場合、利用者への通知や運用スケジュールの変更など、イレギュラーな対応が発生する。それらを短時間で実現しなければならないほど、システムの例外処理に対する作り込みを慎重に実施する必要があると考えられ、導入コストが増大すると考えられる。一方、運用コストに関してはその作り込みによって例外処理に対する運用が簡略化されるため減少すると考えられる。	2	2		21:00～8:00迄の間、または非営業日（土、日、祝日）期間に限り計画停止を容認する。事前の連絡があれば、停止の調整可能。							
C.2.2.1			運用負荷削減	保守運用に関する作業負荷を削減するための設計に関する項目。		○	保守作業自動化の範囲	保守作業は全て手動で実施する	一部の保守作業を自動で実行する	全ての保守作業を自動で実行する				○	【メトリクス】 保守作業とは、保守運用に伴うシステム基盤を維持管理するための作業を指し、点検作業やパッチ適用等のアップデート作業、領域拡張、デフラグ、ログローテート等を想定している。障害対応や復旧作業などは含まない。 【運用コストへの影響】 システム基盤の保守運用作業を自動化するためには、特別な運用管理ツールを導入したり、さまざまな作り込みを実施する必要がある。そのため導入コストは増大するが、ユーザが実施すべき保守運用作業が簡略化あるいはなくなると考えられるので、運用コストは減少する。	1	1		全ての作業を自動化可能であれば、自動化しても良い。	0	保守作業は全て手動で実施する 全ての保守作業を管理者が手動で実行することを想定。 [+] いくつかの保守作業を自動化する場合	1	一部の保守作業を自動で実行する 業務機能の起動・停止など定期的に行う処理は自動化するが、ログの削除など非定期に実行する処理は管理者が手動で実施することを想定。 [－] 全ての保守作業を手動で実行する場合 [+] 全ての保守作業を自動化する場合	2	全ての保守作業を自動で実行する 業務機能の起動・停止やスケジューリングされたメンテナンス操作を全て自動で実行することを想定 [－] いくつかの機能は管理者が手動で実行することを想定する場合
C.2.2.2							サーバソフトウェア更新作業の自動化	サーバへの更新ファイル配布機能を実装しない	サーバへの更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する	サーバへの更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する	サーバへの更新ファイル配布機能を実装し、配布と更新処理を自動で実行する			○	【メトリクス】 サーバソフトウェアとは、サーバ機器のOSやストレージのファームウェア、サーバ機器上で動作するミドルウェアやアプリケーションを指す。 【運用コストへの影響】 サーバへの更新ファイルの配布や更新処理を自動化するためには、特別なツールを導入したり作り込みを実施する必要があるため導入コストは増大する。一方、サーバソフトウェアの更新作業が自動化されることでユーザが運用中に実施すべき作業がなくなり、運用コストは減少する。	1	1		全ての作業を自動化可能であれば、自動化しても良い。							
C.2.2.3							端末ソフトウェア更新作業の自動化	端末への更新ファイル配布機能を実装しない	端末への更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する	端末への更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する	端末への更新ファイル配布機能を実装し、配布と更新処理を自動で実行する			○	【メトリクス】 端末ソフトウェアとは、クライアント端末のOSやネットワーク機器のファームウェア、クライアント端末上で動作するアプリケーションを指す。 【運用コストへの影響】 端末への更新ファイルの配布や更新処理を自動化するためには、特別なツールを導入したり作り込みを実施する必要があるため導入コストは増大する。一方、端末の更新作業が自動化されることでユーザが運用中に実施すべき作業がなくなり、運用コストは減少する。	1	－		端末への更新ファイル配布機能を実装し、配布と更新処理を自動で実行できること。							
C.2.3.1			パッチ適用ポリシー	パッチ情報の展開とパッチ適用のポリシーに関する項目。			パッチリリース情報の提供	ユーザの要求に応じてベンダが受動的にパッチリリース情報を提供する	ベンダが定期的にユーザへパッチリリース情報を提供する	ベンダがリアルタイムに（パッチリリースと同時に）ユーザへパッチリリース情報を提供する						1	1		セキュリティ脆弱性等の緊急性の高いパッチリリース情報は、リアルタイムに情報提供すること。							
C.2.3.2							パッチ適用方針	パッチを適用しない	推奨されるパッチのみを適用する	全てのパッチを適用する					【メトリクス】 リリースされるパッチが個別パッチであるか、集合パッチであるかによって選択レベルが変わる場合は、個別に合意する必要がある。 セキュリティパッチについては、セキュリティの項目でも検討すること(E.4.3.2)。	1	1		－						
C.2.3.3							パッチ適用タイミング	パッチを適用しない	障害発生時にパッチ適用を行う	定期保守時にパッチ適用を行う	新規のパッチがリリースされるたびに適用を行う				【メトリクス】 リリースされるパッチが個別パッチであるか、集合パッチであるかによって選択レベルが変わる場合は、個別に合意する必要がある。 セキュリティパッチについては、セキュリティの項目でも検討すること(E.4.3.3)。	2	1	PDCAツールについては、システムの安定性を考慮し、障害対応時のみパッチ適用とする。	－						
C.2.3.4							パッチ検証の実施有無	パッチ検証を実施しない	障害パッチのみパッチ検証を実施する	障害パッチとセキュリティパッチの両方でパッチ検証を実施する						2	2		－						
C.2.4.1			活性保守	サービス停止の必要がない活性保守が可能なコンポーネントの範囲。			ハードウェア活性保守の範囲	活性保守を行わない	一部のハードウェアにおいて活性保守を行う	全てのハードウェアにおいて活性保守を行う					【メトリクス】 ハードウェア活性保守とは、システムを停止せずにハードウェア交換やファームウェア更新といった保守作業を実施することである。 【レベル1】 一部のハードウェアとは、特定のサーバやストレージのみ活性保守を可能とするようなケースを指す。	1	－	ハードウェアに関する項目のため、対象外	※ なお、対象がクラウドサービスである場合、責任共有モデルに基づき、クラウドサービス提供事業者の責任範囲であれば保証の対象外とするが、レベル1以上を目標とすること。							
C.2.4.2							ソフトウェア活性保守の範囲	活性保守を行わない	一部のソフトウェアにおいて活性保守を行う	全てのソフトウェアにおいて活性保守を行う					【メトリクス】 ソフトウェア活性保守とは、システムを停止せずにOSやミドルウェア、アプリケーションのパッチ適用を実施することである（例：マルチサーバ環境におけるローリングアップグレードなど）。 【レベル1】 一部のソフトウェアとは、特定のソフトウェアのみ活性保守を可能とするようなケースを	0	0		－						
C.2.5.1			定期保守頻度	システムの保全のために必要なハードウェアまたはソフトウェアの定期保守作業の頻			定期保守頻度	定期保守を実施しない	年1回	半年に1回	月1回	週1回	毎日			3	1	定期パッチ適用作業がないため、年次作業とする	－						
C.2.6.1			予防保守レベル	システム構成部材が故障に至る前に予兆を検出し、事前交換などの対応をとる保守。			予防保守レベル	予防保守を実施しない	定期保守時に検出した予兆の範囲で対応する	（定期保守とは別に）一定間隔で予兆検出を行い、対応を行う	リアルタイムに予兆検出を行い、対応を行う					1	－	ハードウェアに関する項目のため、対象外	※ なお、対象がクラウドサービスである場合、責任共有モデルに基づき、クラウドサービス提供事業者の責任範囲であれば保証の対象外とするが、レベル1以上を目標とすること。							
C.3.1.1		障害時運用	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力。	○		復旧作業	復旧不要	復旧用製品は使用しない手作業の復旧	復旧用製品による復旧	復旧用製品＋業務アプリケーションによる復旧				【重複項目】 A.4.1.1。復旧作業は、可用性の復旧目標（RTO/RPO）を検討するうえで必要な項目であるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 選定したレベルに応じて、ユーザ側・ベンダ側それぞれの体制や権限の整理を実施する必要がある。 【レベル】 自作ツールを利用するケースは手作業に含む。 復旧用製品とは、バックアップ・リカバリを行う製品を指す。復旧用製品による復旧を行う場合、どこまで自動化するか（自動リカバリ一機能充足率など）を定義するケースもあるが、可用性とレベルは、復旧用製品を使用するかしないかでギャップが発生するため、この観点でレベルを検討する。	1	1		－							
C.3.1.2					○		代替業務運用の範囲	無し	一部の業務について代替業務運用が必要	全部の業務について代替業務運用が必要					【重複項目】 A.4.1.2。代替業務運用の範囲は、可用性の復旧目標（RTO/RPO）を検討するうえで必要な項目でもあるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 代替業務運用とは、障害によりシステムが復旧不可能となった場合に、代替業務でカバーすることが可能な運用手段（代替機あるいは人手による運用）を指す。	0	0		－							
C.3.2.1			障害復旧自動化の範囲	障害復旧に関するオペレーションを自動化する範囲に関する項目。			障害復旧自動化の範囲	障害復旧作業は全て手動で実施する	一部の障害復旧作業を自動化する	全ての障害復旧作業を自動化する				○	【レベル1】 一部の障害復旧作業とは、特定パターン（あるいは部位）の障害復旧作業に関してのみ自動化を行うようなケースを指す。 【運用コストへの影響】 障害復旧作業を自動化するためには、障害のパターン毎に複雑な判断を行うスクリプトを作成する必要があり開発コストが増大する。一方、障害発生時の復旧作業が迅速化され、ミスも少なくなるため運用コストは減少する。	1	1		－							
C.3.3.1			システム異常検知時の対応	システムの異常を検知した際のベンダ側対応についての項目。			対応可能時間	ベンダの営業時間内（例：9時～17時）で対応を行う	ユーザの指定する時間帯（例：18時～24時）で対応を行う	24時間対応を行う					【メトリクス】 システムの異常検知時に保守員が作業対応を行う時間帯。	0	0		協議の上で決定すること。							
C.3.3.2							駆けつけ到着時間	保守員の駆けつけ無し	保守員到着が異常検知から数日中	保守員到着が異常検知からユーザの翌営業日中	保守員到着が異常検知からユーザの翌営業開始時まで	保守員到着が異常検知から数時間内	保守員が常駐		【メトリクス】 システムの異常を検出してから、指定された連絡先への通知、保守員が障害連絡を受けて現地へ到着するまでの時間。	3	2	現行システムと同等レベルに設定	－						
C.3.3.3							SE到着平均時間	SEの駆けつけ無し	SE到着が異常検知から数日中	SE到着が異常検知からユーザの翌営業日中	SE到着が異常検知からユーザの翌営業開始時まで	SE到着が異常検知から数時間内	SEが常駐		【メトリクス】 システム異常を検知してからSEが到着するまでの平均時間。	3	2	現行システムと同等レベルに設定	－						

項番	大項目	中項目	小項目	小項目説明	最低限項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	運用コストへの影響	備考	LMシステム	PDCAツール	PDCAツール補足	LMシステム補足事項 （凡例） －：補足事項無	社会的影響が殆ど無いシステム 選択レベル	社会的影響が殆ど無いシステム 選択時の条件	社会的影響が限定されるシステム 選択レベル	社会的影響が限定されるシステム 選択時の条件	社会的影響が極めて大きいシステム 選択レベル	社会的影響が極めて大きいシステム 選択時の条件
C.3.4.1			交換用部材の確保	障害の発生したコンポーネントに対する交換部材の確保方法。			保守部品確保レベル	確保しない	保守契約に基づき、部品を提供するベンダが規定年数の間保守部品を確保する	保守契約に基づき、保守を提供するベンダが当該システム専用として規定年数の間保守部品を確保する					【メトリクス】 当該システムに関する保守部品の確保レベル。	0	0								
C.3.4.2							予備機の有無	予備機無し	一部、予備機有り	全部、予備機有り						0	0								
C.4.1.1		運用環境	開発用環境の設置	ユーザがシステムに対する開発作業を実施する目的で導入する環境についての項目。		○	開発用環境の設置有無	システムの開発環境を設置しない	運用環境の一部に限定した開発環境を設置する	運用環境と同一の開発環境を設置する					【メトリクス】 開発用環境とは、本番環境とは別に開発専用に使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される開発フェーズの環境は、本項目に含めない。 【レベル】 開発フェーズでは開発環境として使用していたが、本番移行後は本番環境となる環境については、レベル0のシステムの開発環境を設置しないを選択する。	1	1		－	0	システムの開発環境を設置しない	本番環境上で開発を行い、そのまま本番運用に使用する。 [+] 運用中も開発を実施するために、開発環境を用意する場合	1	運用環境の一部に限定した開発環境を設置する	非クラスタの開発環境を用意する。 [－] 開発環境を用意しない場合 [+] 本番環境と同等の開発環境を用意する場合	2	運用環境と同一の開発環境を設置する	本番環境と同等の開発用環境を設置することを想定。 [－] 本番環境では複数台存在するAPサーバを1台のみで開発環境を用意する場合
C.4.2.1			試験用環境の設置	ユーザがシステムの動作を試験する目的で導入する環境についての項目。		○	試験用環境の設置有無	システムの試験環境を設置しない	システムの開発用環境と併用する	専用の試験用環境を設置する					【メトリクス】 試験用環境とは、本番環境とは別に試験専用に使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される試験フェーズの環境は、本項目に含めない。 【レベル】 試験フェーズでは試験環境として使用していたが、本番移行後は本番環境となる環境については、レベル0のシステムの試験環境を設置しないを選択する。	1	1		－	0	システムの試験環境を設置しない	試験用環境を用意しない。 [+] 試験用環境を用意する場合	1	システムの開発用環境と併用する	開発環境上で試験も実施する。 [－] 試験用環境を用意しない場合 [+] 開発環境とは別に試験用の環境を用意する場合	2	専用の試験用環境を設置する	開発環境とは別に試験用の環境も用意する。 [－] 開発環境と試験環境を併用する場合
C.4.3.1			マニュアル準備レベル	運用のためのマニュアルの準備のレベル。		○	マニュアル準備レベル	各製品標準のマニュアルを利用する	システムの通常運用のマニュアルを提供する	システムの通常運用と保守運用のマニュアルを提供する	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する			○	【レベル】 通常運用のマニュアルには、システム基盤に対する通常時の運用（起動・停止等）にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、システム基盤に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作や機能についての説明が記載される。 障害発生時の一次対応に関する記述（系切り替え作業やログ収集作業等）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。 【運用コストへの影響】 ユーザの運用に合わせたカスタマイズされたマニュアルは、作成するためにコストがかかるため導入コストが増大するが、ユーザが運用時に手順を調査する負担が減少するため運用コストは減少する。	1	1		－	0	各製品標準のマニュアルを利用する	システムの操作方法について、管理者が製品マニュアルを参照して習得することを想定。必要に応じて、ユーザが運用マニュアルを作成する。 [+] ベンダよりマニュアルの提供を受ける必要がある場合	2	システムの通常運用と保守運用のマニュアルを提供する	緊急時にはユーザ側にて保守対応を実施することも想定し、リカバリ作業手順などを示した保守マニュアルも作成する。 [－] 保守作業は全てベンダに依頼するため、通常運用に必要なオペレーションのみを説明した運用マニュアルのみ作成する場合 [+] ユーザ独自の運用ルールを加味した特別な運用マニュアルを作成する場合	3	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する	ユーザの自営センターの運用ルールにのっとったマニュアルの作成を要望。 [－] ベンダの用意する一般的な運用マニュアルで良いような場合
C.4.4.1			リモートオペレーション	システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。		○	リモート監視地点	リモート監視を行わない	構内LANを介したリモート監視を行う	遠隔地でリモート監視を行う				○	【レベル】 監視の内容については、通常運用の運用監視の項目にて確認する必要がある。 【運用コストへの影響】 リモート監視を実装するためには、特別なハードウェア・ソフトウェアを導入する必要があり導入コストが増大する。しかし、運用状況の確認のために管理者がわざわざサーバの設置場所まで移動する必要がなくなるため、運用コストは減少する。	2	0	現行システムと同等レベルに設定	－	0	リモート監視を行わない	機器数が少ないため、リモートでの集中監視を行わない。 [+] 機器数が少なくとも、別途監視サーバを用意してリモート監視を行う場合	1	構内LANを介してリモート監視を行う	センターに配置されるサーバ機器のみリモート監視を行い、各支店に配置されるクライアント機器類は監視を行わない。 [－] サーバ機器についてもコンソールでの直接監視を行う場合 [+] 各支店に配置されているクライアント機器類についてもリモートで集中監視を行う場合	2	遠隔地でリモート監視を行う	システムを構成する全ての機器類を監視センターからリモートで集中監視を行う [－] リモートで監視を行うのはセンターに配置されているサーバ機器類のみとし、各支店に配置されているクライアント機器類はコンソールにて直接監視してもらうような場合
C.4.4.2						○	リモート操作の範囲	リモート操作を行わない	定型処理のみリモート操作を行う	任意のリモート操作を行う				○	【メトリクス】 リモート監視地点から実施できる操作の範囲を検討する。 【レベル】 定型処理のみリモート操作を実現するためのソフトウェアは安価であったり、任意のリモート操作を認める場合はセキュリティやその他の面での検討項目が増えることを考慮し、定型処理よりも任意のリモート操作を行う方のレベルを高く設定している。 【運用コストへの影響】 リモート操作を実装するためには、特別なハードウェア・ソフトウェアを導入する必要があり導入コストが増大する。しかし、メンテナンス操作のために管理者がわざわざサーバの設置場所まで移動する必要がなくなるため、運用コストは減少する。	1	0	現行システムと同等レベルに設定	－	0	リモート操作を行わない	メンテナンス操作は、全てマシンローカルの環境で実施する。 [+] リモートの管理端末を用意し、そこからメンテナンス操作を実行することを想定する場合	1	定型処理のみリモート操作を行う	集中監視を行っているリモート監視端末から、対象機器のメンテナンス操作を実施することを想定する。セキュリティの観点から、あらかじめ実行できる操作を限定する。 [－] リモートからの操作は実行しない場合 [+] 任意の操作を実行できるようにする場合	2	任意のリモート操作を行う	運用部門とシステム設置場所が遠隔地に存在することを想定し、対象機器の操作を基本的に全てリモートで実施できるようにする。 [－] 特定の操作のみの実行ができればよいような場合
C.4.5.1			外部システム接続	システムの運用に影響する外部システムとの接続の有無に関する項目。		○	外部システムとの接続有無	外部システムと接続しない	社内の外部システムと接続する	社外の外部システムと接続する					【メトリクス】 接続する場合には、そのインターフェースについて確認すること。	2	2		－	0	外部システムと接続しない	部門内システムであり、連携する他システムが存在しない。 [+] 履歴データを蓄積・分析を行うようなシステムに対してデータを送信するなど、連携する他システムが存在する場合	1	社内の外部システムと接続する	企業内基幹系システムとして、受発注と在庫管理などのように連携する社内の他システムが存在することを想定。 [－] データのやり取りを行う多システムが存在しない場合 [+] 社外のシステムに接続して、データのやり取りを行う場合	2	社外の外部システムと接続する	社会基盤のシステムとして、様々な企業システムと連携して処理を行うシステムを想定。 [－] システムと連携する外部のシステムが存在しない場合
C.4.5.2							監視システムの有無	監視システムは存在しない	既存監視システムに接続する	新規監視システムに接続する					【レベル2】 新規監視システムに接続とは、当該システムに対する監視機能の新規構築が要件定義範囲に含まれていることを意味している。	1	1		－							
C.4.5.3							ジョブ管理システムの有無	ジョブ管理システムは存在しない	既存ジョブ管理システムに接続する	新規ジョブ管理システムに接続する					【レベル2】 新規ジョブ管理システムに接続とは、当該システムに対するジョブ管理機能の新規構築が要件定義範囲に含まれていることを意味している。	1	1		－							
C.5.1.1		サポート体制	保守契約（ハードウェア）	保守が必要な対象ハードウェアの範囲。		○	保守契約（ハードウェア）の範囲	保守契約を行わない	ベンダの自社製品（ハードウェア）に対してのみ保守契約を行う	マルチベンダのサポート契約を行う（一部対象外を許容）	マルチベンダのサポート契約を行う（システムを構成する全製品を対象）			○	【レベル】 ベンダの自社製品（ハードウェア）に対してのみサポート契約とは、システムを構成する製品個別の提供ベンダと、当該製品に対するサポート契約を行うことを意味しており、当該製品に対してのみサポートサービスが提供される契約形態のことである。 マルチベンダのサポート契約とは、システム全体に対するサポートサービスを提供するベンダと契約を行うことを意味しており、複数のベンダの製品から構成されるシステムに対してワンストップのサポート窓口が提供される契約形態のことである。 【運用コストへの影響】 サポート契約を行うと運用コストが増大するように感じられるが、問題が発生した際に必要となる費用が膨大となるため、サポート契約を行ったほうが結果として運用コストは小さくなる場合がある。	3	－	ハードウェアに関する項目のため、対象外	※ なお、対象がクラウドサービスである場合、責任共有モデルに基づき、クラウドサービス提供事業者の責任範囲であれば保証の対象外とするが、レベル3を目標とすること。	1	ベンダの自社製品（ハードウェア）に対してのみ保守契約を行う	システムを構成する個々のハードウェア製品を調達し、SIIはユーザが実施することを想定。 [+] SIerを立てて、システム全体を調達するような場合	2	マルチベンダのサポート契約を行う（一部対象外を許容）	既存の機器を流用したシステム構築を想定。既存の機器に対するサポートは、別ベンダが実施する。 [－] 複数製品についてのワンストップのサポート窓口を必要としない場合 [+] サポート対象外を許容せず、システムを構成する全ての製品についてワンストップのサポート窓口を必要とする場合	3	マルチベンダのサポート契約を行う（システムを構成する全製品を対象）	システムに関する問い合わせ窓口を一本化し、管理者の負荷を軽減することを想定。 [－] 特殊な製品や、既存の機器を用いたシステムの構築を行う場合など、一部の製品に関して問い合わせ窓口を一本化する必要がない場合
C.5.2.1			保守契約（ソフトウェア）	保守が必要な対象ソフトウェアの範囲。		○	保守契約（ソフトウェア）の範囲	保守契約を行わない	ベンダの自社製品（ソフトウェア）に対してのみ保守契約を行う	マルチベンダのサポート契約を行う（一部対象外を許容）	マルチベンダのサポート契約を行う（システムを構成する全製品を対象）			○	【レベル】 ベンダの自社製品（ソフトウェア）に対してのみサポート契約とは、システムを構成する製品個別の提供ベンダと、当該製品に対するサポート契約を行うことを意味しており、当該製品に対してのみサポートサービスが提供される契約形態のことである。 マルチベンダのサポート契約とは、システム全体に対するサポートサービスを提供するベンダと契約を行うことを意味しており、複数のベンダの製品から構成されるシステムに対してワンストップのサポート窓口が提供される契約形態のことである。 【運用コストへの影響】 サポート契約を行うと運用コストが増大するように感じられるが、問題が発生した際に必要となる費用が膨大となるため、サポート契約を行ったほうが結果として運用コストは小さくなる場合がある。	3	3		－	1	ベンダの自社製品（ソフトウェア）に対してのみ保守契約を行う	システムを構成する個々のソフトウェア製品を調達し、SIIはユーザが実施することを想定。 [+] SIerを立てて、システム全体を調達するような場合	2	マルチベンダのサポート契約を行う（一部対象外を許容）	既存のソフトウェアライセンスを流用したシステム構築を想定。既存のソフトウェアに対するサポートは、別ベンダが実施する。 [－] 複数製品についてのワンストップのサポート窓口を必要としない場合 [+] サポート対象外を許容せず、システムを構成する全ての製品についてワンストップのサポート窓口を必要とする場合	2	マルチベンダのサポート契約を行う（一部対象外を許容）	システムに関する問い合わせ窓口を一本化し、管理者の負荷を軽減することを想定。 [－] 特殊な製品や、既存の機器を用いたシステムの構築を行う場合など、一部の製品に関して問い合わせ窓口を一本化する必要がない場合
C.5.3.1			ライフサイクル期間	運用保守の対応期間および、実際にシステムが稼動するライフサイクルの期間。		○	ライフサイクル期間	3年	5年	7年	10年以上				【メトリクス】 ここでのライフサイクルとは、次回のシステム更改までの期間と規定している。製品の保守可能期間よりも長い期間のライフサイクルとなる場合は、保守延長や保守可能バージョンへのアップ等の対応が必要となる。	1	1		－	0	3年	3年以内には組織変更が発生し、システムの更新が必要となることを想定。 [+] 社内規定などにより、システムのライフサイクルが7年程度と定められているような場合	2	7年	導入するソフトウェアのサポート期間に合わせてシステムのライフサイクルを7年と決定したと想定。 [－] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 内部統制等によりシステムで実行する業務を10年以上継続しなければならないため、それにあわせてライフサイクルを合わせる場合	3	10年以上	システムで実施する業務は今後10年間は継続することになるため、システムのライフサイクルをそれに合わせることを想定。 [－] 導入するソフトウェアやハードウェアのサポート期間が短いため、それにあわせてライフサイクル期間を定める場合
C.5.4.1			メンテナンス作業役割分担	メンテナンス作業に対するユーザ/ベンダの役割分担、配置人数に関する項目。			メンテナンス作業役割分担	全てユーザが実施	一部ユーザが実施	全てベンダが実施						2	2		－							
C.5.5.1			一次対応役割分担	一次対応のユーザ/ベンダの役割分担、一次対応の対応時間、配備人数。			一次対応役割分担	全てユーザが実施	一部ユーザが実施	全てベンダが実施						2	2		－							
C.5.6.1			サポート要員	サポート体制に組み入れる要員の人数や対応時間、スキルレベルに関する項目。			ベンダ側常備配備人数	常駐しない	1人	複数人						1	0	現行システムと同等レベルに設定	－							
C.5.6.2							ベンダ側対応時間帯	対応無し	ベンダの定時時間内（9～17時）	夜間のみ非対応（9～21時）	引継ぎ時に1時間程度非対応有り（9～翌8時）	24時間対応				1	1		－							
C.5.6.3							ベンダ側対応者の要求スキルレベル	指定無し	有識者の指導を受けて機器の操作を実施できる	システムの構成を把握し、ログの収集・確認が実施できる	システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる	システムの開発や構築に携わり、業務要件やユーザの事情にも通じている				4	4		－							
C.5.6.4							エスカレーション対応	指定無し	オンコール待機	拠点待機	現地待機				【メトリクス】 障害発生時にエスカレーション対応が必要となるISV/IHV製品に関してエスカレーション先の有識者の待機方法について確認する。	0	0		－							
C.5.7.1			導入サポート	システム導入時の特別対応期間の有無および期間。			システムテスト稼働時の導入サポート期間	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上				2	2		－							
C.5.7.2							システム本稼働時の導入サポート期間	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上				0	0		－							
C.5.8.1			オペレーション訓練	オペレーション訓練実施に関する項目。			オペレーション訓練実施の役割分担	実施しない	全てユーザが実施	一部ユーザが実施	全てベンダが実施					3	3		－							
C.5.8.2							オペレーション訓練範囲	実施しない	通常運用の訓練を実施	通常運用に加えて保守運用の訓練を実施	通常運用、保守運用に加えて、障害発生時の復旧作業に関する訓練を実施				【レベル】 通常運用とは、システム基盤に対する通常時の運用（起動・停止等）にかかわる操作を指す。保守運用とは、システム基盤に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作を指す。	3	3		－							
C.5.8.3							オペレーション訓練実施頻度	実施しない	システム立ち上げ時のみ	定期開催						2	2		－							
C.5.9.1			定期報告会	保守に関する定期報告会の開催の要否。			定期報告会実施頻度	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上		【メトリクス】 障害発生時に実施される不定期の報告会は本メトリクスには含まない。	4	4		サービス提供に影響が出る恐れのある更新がある場合は、適用前に報告会を通じて主管担当と事前合意すること。							
C.5.9.2							報告内容のレベル	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害および運用状況報告に加えて、改善提案を行う					3	3		－							
C.6.1.1		その他の運用管理方針	内部統制対応	IT運用プロセスの内部統制対応を行うかどうかに関する項目。		○	内部統制対応の実施有無	内部統制対応について規定しない	既存の社内規定に従って、内部統制対応を実施する	新規に規定を制定し、内部統制対応を実施する					【メトリクス】 ここでは内部統制対応の実施有無について確認する。内部統制対応の具体的な対応方法（オペレーションで実施するか、システムへの機能実装で実現するか等）については、有無の確認後に具体化して確認する。	1	1		－	0	内部統制対応について規定しない	内部統制実施の対象システムではないため、対応を実施しない。 [+] 対象システムではないが、部門の判断により内部統制対応を実施する場合	1	既存の社内規定に従って、内部統制対応を実施する	社内規定に従い、内部統制対応を実施する。 [－] 内部統制実施の対象システムではないため、対応を実施しない場合 [+] 既存の規定は存在しないが、本システムを構築するに際して、新たな規定を策定するような場合	1	既存の社内規定に従って、内部統制対応を実施する	法令にて定められているとおり、内部統制対応を実施する。 [－] 順守すべき法令や社内の内部統制規定等が存在しない場合 [+] 既存の規定は存在しないが、本システムを構築するに際して、新たな規定を策定するような場合
C.6.2.1			サービスデスク	ユーザの問合せに対して単一の窓口機能を提供するかどうかに関する項目。		○	サービスデスクの設置有無	サービスデスクの設置について規定しない	既存のサービスデスクを利用する	新規にサービスデスクを設置する					【メトリクス】 ここでは、ユーザとベンダ間におけるサービスデスクの設置の有無について確認する。サービスデスク機能の具体的な実現方法については、有無の確認後に具体化して確認する。	2	2		9:00～18:00の間で電話、e-mailでの対応を行うこと。	0	サービスデスクの設置について規定しない	ユーザ/ベンダ間のやり取りに関してサービスデスク機能を設けず、個別対応にすることを想定 [+] サービスデスクを設置する場合	1	既存のサービスデスクを利用する	マルチベンダのサポート契約を締結するベンダとの間に既存のサービスデスクが存在することを想定 [－] サービスデスクを設置しない場合 [+] 初めて取引を行うベンダで、既存のサービスデスクが存在しないような場合	2	新規にサービスデスクを設置する	当該システム専用のサービスデスク機能をベンダが開設することを想定 [－] 既存のサービスデスク機能を利用するような場合
C.6.3.1			インシデント管理	業務を停止させるインシデントを迅速に回復させるプロセスを実施するかどうかに関する項目。			インシデント管理の実施有無	インシデント管理について規定しない	既存のインシデント管理のプロセスに従う	新規にインシデント管理のプロセスを規定する					【メトリクス】 ここでは、当該システムで発生するインシデントの管理を実施するかどうかを確認する。インシデント管理の実現方法については、有無の確認後に具体化して確認する。	1	1		－							
C.6.4.1			問題管理	インシデントの根本原因を追究し、可能であれば取り除くための処置を講じるプロセスを実施するかどうかに関する項目。			問題管理の実施有無	問題管理について規定しない	既存の問題管理のプロセスに従う	新規に問題管理のプロセスを規定する					【メトリクス】 ここでは、インシデントの根本原因を追究するための問題管理を実施するかどうかを確認する。問題管理の実現方法については、有無の確認後に具体化して確認する。	1	1		－							
C.6.5.1			構成管理	ハードウェアやソフトウェアなどのIT環境の構成を適切に管理するためのプロセスを実施するかどうかに関する項目。			構成管理の実施有無	構成管理について規定しない	既存の構成管理のプロセスに従う	新規に構成管理のプロセスを規定する					【メトリクス】 ここでは、リリースされたハードウェアやソフトウェアが適切にユーザ環境に構成されているかを管理するための構成管理を実施するかどうかを確認する。構成管理の実現方法については、有無の確認後に具体化して確認する。	1	1		－							
C.6.6.1			変更管理	IT環境に対する変更を効率的に管理するためのプロセスを実施するかどうかに関する項目。			変更管理の実施有無	変更管理について規定しない	既存の変更管理のプロセスに従う	新規に変更管理のプロセスを規定する					【メトリクス】 ここでは、ハードウェアの交換やソフトウェアのパッチ適用、バージョンアップ、パラメータ変更といったシステム環境に対する変更を管理するための変更管理を実施するかどうかを確認する。変更管理の実現方法については、有無の確認後に具体化して確認する。	1	1		－							
C.6.7.1			リリース管理	ソフトウェア、ハードウェア、ITサービスに対する実装を管理するためのプロセスを実施するかどうかに関する項目。			リリース管理の実施有無	リリース管理について規定しない	既存のリリース管理のプロセスに従う	新規にリリース管理のプロセスを規定する					【メトリクス】 ここでは、承認された変更が正しくシステム環境に適用されているかどうかを管理するリリース管理を実施するかどうかを確認する。リリース管理の実現方法については、有無の確認後に具体化して確認する。	1	1		－							
D.1.1.1	移行性	移行時期	移行のスケジュール	移行作業計画から本稼働までのシステム移行期間、システム停止可能日時、並行稼働の有無、（例外発生時の切り戻し時間や事前バックアップの		○	システム移行期間	システム移行無し	3ヶ月未満	半年未満	1年未満	2年未満	2年以上			2	2		－	1	3ヶ月未満	システムを短期間で構築する必要がある。 [+] 中長期間で進める場合	4	2年未満	年度を跨いで移行を進める必要がある。 [－] 期間短縮の場合 [+] さらに長期期間が必要な場合	5	2年以上	移行の計画から稼働まで安全性を最優先にして進める必要がある。 [－] 期間短縮の場合

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	LMシステム	PDCAツール	PDCAツール補足	LMシステム補足事項（凡例）－：補足事項無	社会的影響が殆ど無いシステム			社会的影響が限定されるシステム			社会的影響が極めて大きいシステム		
								0	1	2	3	4	5							選択レベル		選択時の条件	選択レベル		選択時の条件	選択レベル		選択時の条件
D.1.1.2				時間等も含むこと。）		○	システム停止可能日時	制約無し（必要な期間の停止が可能）	5日以上	5日未満	1日（計画停止日を利用）	利用の少ない時間帯（夜間など）	移行のためのシステム停止不可		【メトリクス】 システムによっては、システム停止可能な日や時間帯が連続して確保できない場合がある。（例えば、この日は1日、次の日は夜間のみ、その次の日は計画停止日で1日、などの場合。） その場合には、システム停止可能日とその時間帯を、それぞれ確認すること。 【レベル】 レベル0はシステムの制約によらず、移行に必要な期間のシステム停止が可能なことを示す。レベル1以上は、システム停止に関わる（業務などの）制約が存在する上での、システム停止可能日時を示す。レベルが高くなるほど、移行によるシステム停止可能な日や時間帯など、移行計画に影響範囲が大きい制約が存在することを示している。	5	－	ハードウェアに関する項目のため、対象外	－	1	5日以上	業務への影響が少なく数日以上はシステム停止可能。 [-] さらに停止を多くする場合 [+] 停止を少なくする場合	4	利用の少ない時間帯（夜間など）	業務が比較的少ない時間帯にシステム停止が可能。 [-] 停止を増やす場合	5	移行のためのシステム停止不可	システム停止時間は最短にする必要がある。 [-] 停止時間を確保する場合
D.1.1.3						○	並行稼働の有無	無し	有り						【レベル1】 並行稼働有りの場合には、その期間、場所等を規定すること。関係項目にF.4.2.3、F.4.4.3がある。	1	1	本番データ移行にあたっては、大手町より実施する。	－	0	無し	移行のためのシステム停止期間も十分確保できるため並行稼働の必要性は低い。 [+] 移行のためのシステム停止期間が確保できず、並行稼働する場合	1	有り	移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。 [-] 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合	1	有り	移行のためのシステム停止不可のため、移行時のリスク軽減を最優先して並行稼働は必要。 [-] 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合
D.2.1.1		移行方式	システム展開方式	システムの移行および新規展開時に多段階による展開方式をどの程度採用するかの程度。		○	拠点展開ステップ数	単一拠点のため規定無し	一斉展開	5段階未満	10段階未満	20段階未満	20段階以上		【レベル】 拠点展開時のリスクによっては難易度が逆転し、一斉展開の難易度が高くなる場合もある。対象システムについて、拠点毎に展開時のリスクを考慮して拠点展開ステップ数を判断すること。	0	0		－	0	単一拠点のため規定無し	システムが単一で展開を規定する必要がない。 [+] 展開を検討する必要がある場合	1	一斉展開	効率を優先させて一斉に切り替える。段階的に移行させる必要性は低い。 [+] 段階的に展開が必要な場合	2	5段階未満	段階的展開が必要である。 [-] 一斉展開する場合 [+] 段階数を増やす必要がある場合
D.2.1.2						○	業務展開ステップ数	単一業務のため規定無し	全業務一斉切り替え	4段階未満	6段階未満	10段階未満	10段階以上		【レベル】 業務展開時のリスクによっては難易度が逆転し、全業務一斉切り替えの難易度が高くなる場合もある。対象システムについて、業務毎に展開時のリスクを考慮して業務展開ステップ数を判断すること。	0	0		－	0	単一業務のため規定無し	システムが単一で展開を規定する必要がない。 [+] 展開を検討する必要がある場合	1	全業務一斉切り替え	効率を優先させて一斉に切り替える。段階的に移行させる必要性は低い。 [+] 段階的に展開が必要な場合	2	4段階未満	段階的展開が必要である。 [-] 一斉展開する場合 [+] 段階数を増やす必要がある場合
D.3.1.1		移行対象（機器）	移行設備	移行前のシステムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容。		○	設備・機器の移行内容	移行対象無し	移行対象設備・機器のハードウェアを入れ替える	移行対象設備・機器のハードウェア、OS、ミドルウェアを入れ替える	移行対象設備・機器のシステム全部を入れ替える	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する			【レベル】 移行対象設備・機器が複数あり、移行内容が異なる場合には、それぞれ合意すること。	3	－	ハードウェアに関する項目のため、対象外	－	0	移行対象無し	設備機器を新設する必要がある。 [+] 既存設備機器が存在する場合	3	移行対象設備・機器のシステム全部を入れ替える	業務アプリケーションも含めた移行がある。 [-] 業務アプリケーション更改が無い場合 [+] 業務アプリケーションの更改程度が大きい場合	2	移行対象設備・機器のハードウェア、OS、ミドルウェアを入れ替える	業務アプリケーションを更改はせずに、老朽化または性能向上等の対策をする必要がある。 [-] ハードウェアのみ入れ替える場合 [+] 業務アプリケーションの更改が有る場合
D.4.1.1		移行対象（データ）	移行データ量	旧システム上で移行の必要がある業務データの量（プログラムを含む）。		○	移行データ量	移行対象無し	1TB未満	1PB未満	1PB以上					2	2		サービス開始時の初期データの状態に応じて設定する。	1	1TB未満	1TB（テラバイト）未満のデータ（マスター等）を移行する必要がある。 [+] 1TB以上の場合	2	1PB未満	1PB（ペタバイト）未満のデータを移行する必要がある。 [-] 1TB未満の場合 [+] 1PB以上の場合	3	1PB以上	1PB（ペタバイト）以上のデータを移行する必要がある。 [-] 1PB未満の場合
D.4.1.2						○	移行データ形式	移行対象無し	移行先と形式が同一	移行先と形式が異なる					【メトリクス】 データ形式は、アプリケーションに依存したフォーマット、テーブル形式や文字コードなど、新システムに移行するために考慮すべきデータ形式のパターンを指す。 【レベル】 移行データ形式のパターンが複数ある場合には、それぞれについてデータ形式を確認すること。	2	2		サービス開始時の初期データの状態に応じて設定する。	1	移行先と形式が同一	データ形式を現状のままで使用する。 [+] データ形式の変更が必要な場合	2	移行先と形式が異なる	業務の効率化や統合化等によって、データ形式の変更が必要である。 [-] 移行データの形式を変更しない場合	1	移行先と形式が同一	データの継続性や他システムとの親和性を担保するため、データ形式を現状のままで使用する。 [+] データ形式の変更が必要な場合
D.4.2.1			移行媒体	移行対象となる媒体の量と移行時に必要となる媒体種類数。			移行媒体量	移行対象無し	10本未満（1TB未満）	1000本未満（1PB未満）	1000本以上（1PB以上）					0	0		－									
D.4.2.2							移行媒体種類数	移行対象無し	1種類	2種類	3種類	4種類	5種類以上		【メトリクス】 移行する際に使用しなければならない媒体の種類を計数する（例えば、テープ、ディスク、紙の伝票類、など）。 また、ネットワーク接続によるデータ転送も媒体種類として含む。	0	0		－									
D.4.3.1			変換対象（DBなど）	変換対象となるデータの量とツールの複雑度（変換ルール数）。			変換データ量	変換対象無し	1TB未満	1PB未満	1PB以上					0	0		－									
D.4.3.2							移行ツールの複雑度（変換ルール数）	移行ツール不要または既存移行ツールで対応可能	変換ルール数が10未満の移行ツールの複雑度	変換ルール数が50未満の移行ツールの複雑度	変換ルール数が100未満の移行ツールの複雑度	変換ルール数が100以上の移行ツールの複雑度				0	0		－									
D.5.1.1		移行計画	移行作業分担	移行作業の作業分担。			移行のユーザ/ベンダ作業分担	全てユーザ	ユーザとベンダと共同で実施	全てベンダ					【メトリクス】 最終的な移行結果の確認は、レベルに関係なくユーザが実施する。なお、ユーザデータを取り扱う際のセキュリティに関しては、ユーザとベンダで取り交わしを行うことが望ましい。具体的内容については、「F.1.1.1 構築時の制約条件」にて確認する。 【レベル1】 共同で移行作業を実施する場合、ユーザ/ベンダの作業分担を規定すること。特に移行対象データに関しては、旧システムの移行対象データの調査、移行データの抽出/変換、本番システムへの導入/確認、等について、その作業分担を規定しておくこと。	2	1	現行の一部の資産については、ユーザにて実施予定	サービス開始時の初期データの状態に応じて設定する。									
D.5.2.1			リハーサル	移行のリハーサル（移行中の障害を想定したリハーサルを含む）。			リハーサル範囲	リハーサル無し	主要な正常ケースのみ	全ての正常ケース	正常ケース＋移行前の状態に切り戻す異常ケース	正常ケース＋システム故障から回復させる異常ケース				1	1		サービス開始時の初期データの状態に応じて設定する。									
D.5.2.2							リハーサル環境	リハーサル無し	本番データ使用可能	本番データ使用不可					【レベル】 本番データを使用することによる情報漏えい等のセキュリティリスクは、「F.1.1.1 構築時の制約条件」にて判断し、ここではリハーサル環境に限定して判断する。	1	1		サービス開始時の初期データの状態に応じて設定する。									
D.5.2.3							リハーサル回数	リハーサル無し	1回	2回	3回	4回	5回以上			1	1		サービス開始時の初期データの状態に応じて設定する。									
D.5.2.4							外部連携リハーサルの有無	無し	有り（外部接続仕様の変更無し）	有り（外部接続仕様の変更有り）					【メトリクス】 外部システムとの接続仕様が変更になる場合、システム移行リスクを軽減するために新システムでは新旧両接続仕様をサポートすることがある。その場合には、両接続仕様を確認するための外部連携リハーサルを計画すること。 【レベル】 外部連携リハーサル有りの場合、そのリハーサル対象の外部システムとリハーサル範囲、環境、回数について規定すること。	0	0		サービス開始時の初期データの状態に応じて設定する。									
D.5.3.1			トラブル対処	移行中のトラブル時の対応体制や対応プラン等の内容。			トラブル対処の規定有無	規定無し	対応体制のみ規定有り	対応体制と対応プランの規定有り					【レベル】 トラブル対処の規定有りの場合、その対応体制や対応プランの規定内容について確認すること。	2	2		サービス開始時の初期データの状態に応じて設定する。									
E.1.1.1	セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	順守すべき情報セキュリティに関する組織規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例） ・国内/海外の法律 ・資格認証 ・ガイドライン ・その他ルール		○	順守すべき社内規程、ルール、法令、ガイドライン等の有無	無し	有り						【メトリクス】 規程、法令、ガイドライン等を確認し、それらに従い、セキュリティに関する非機能要求項目のレベルを決定する必要がある。 例） ・国内/海外の法律 不正アクセス禁止法・不正競争防止法・プロバイダ責任法・改正個人情報保護法・SOX法・ EU一般データ保護規則(GDPR)・特定電子メール送信適正化法・電子署名法 など ・資格認証 プライバシーマーク・ISMS/ITSMS/BCMS/CSMS・ISO/IEC27000系・PCI DSS・ クラウド情報セキュリティ監査・TRUSTe など ・ガイドライン FISC・FISMA/NIST800・政府機関の情報セキュリティ対策のための統一基準 など ・その他ルール 情報セキュリティポリシー など 【レベル1】 構築するシステムが関係する国や地域によって、順守すべき法令やガイドラインが異なることに注意すること。	1	1		FISC安全基準及びゆうちょ銀行内規（システム開発手続き、EA手続き）これらの規定類を遵守すること。	0	無し	ユーザ要件に応じてレベルを判断する必要がある。 [+] 順守すべき規程、法令、ガイドライン等が存在する場合	0	無し	ユーザ要件に応じてレベルを判断する必要がある。 [+] 順守すべき規程、法令、ガイドライン等が存在する場合	0	無し	ユーザ要件に応じてレベルを判断する必要がある。 [+] 順守すべき規程、法令、ガイドライン等が存在する場合
E.2.1.1		セキュリティリスク分析	セキュリティリスク分析	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクルの確認等を行う必要がある。		○	リスク分析範囲	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	開発範囲					【メトリクス】 システム開発中に実施するセキュリティリスク分析では、ソフトウェアのサポート終了や暗号の危殆化等の運用期間に顕在化するリスクも考慮する。 【レベル1】 外接部分とは、インターネットへの接続部分や、外部へ情報を持ち出す際に用いる媒体等を接続する部分、また、外部システムとデータのやりとりを行う部分等を意味する。 なお、以降のレベルにおいても同様の意味で用いている。	2	2		－	0	分析なし	詳細なリスク分析は実施しないが、基本的な対策は実施する。	1	重要度が高い資産を扱う範囲、あるいは、外接部分	重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、重要度が高い資産を扱う範囲に対してリスク分析する必要がある。 [-] 重要情報の漏洩等の脅威が存在しない（あるいは許容する）場合 [+] 情報の移動や状態の変化が大きい場合	2	開発範囲	ネットワークを通じた、不特定多数の攻撃者からの脅威にさらされる。また、重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、システム全体のリスクを分析する必要がある。 [-] データの移動や更新等が生じず、それらに伴なった情報へのアクセス権限の変化等による脅威が存在しない（あるいは許容する）場合
E.3.1.1		セキュリティ診断	セキュリティ診断	対象システムや、各種ドキュメント（設計書や環境定義書、実装済みソフトウェアのソースコードなど）に対して、セキュリティに特化した各種試験や検査の実施の有無を確認するための項目。		○	ネットワーク診断実施の有無	無し	有り						【メトリクス】 ネットワーク診断には、目視による設定の確認や、疑似攻撃を実施することにより脆弱性を発見する診断（ペネトレーションテスト）、ネットワーク上のサーバや通信機能をもつソフトウェアなどに対する脆弱性調査等がある。 【レベル1】 ネットワーク診断は、システム運用開始前に実施するだけでなく、システム運用中の定期的な実施も検討する。	1	1		－	1	有り	ネットワークを介した不特定多数の攻撃者からの脅威にさらされる。そのため、ネットワーク経由での攻撃に対する脆弱性を分析する必要がある。 [-] セキュリティに関する専門的な知識を有する者により、ネットワークを介した攻撃への対策が十分に検討し、各種ドキュメントが作成される場合。	1	有り	重要情報を取り扱うため、内部ネットワーク経由での攻撃に対する脆弱性を分析する必要がある。 [-] セキュリティに関する専門的な知識を有する者により、内部ネットワーク経由での攻撃への対策が十分に検討し、各種ドキュメントが作成される場合。	1	有り	ネットワークを介した、外部からの不特定多数の攻撃者からの脅威にさらされる。また、重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、ネットワーク経由での攻撃に対する脆弱性を分析する必要がある。 [-] セキュリティに関する専門的な知識を有する者により、ネットワークを介した攻撃への対策が十分に検討し、各種ドキュメントが作成さ
E.3.1.2						○	Web診断実施の有無	無し	有り						【メトリクス】 Web診断とは、Webサイトに対して行うWebサーバやWebアプリケーションに対するセキュリティ診断のことを言う。 【レベル1】 Web診断は、システム運用開始前に実施するだけでなく、システム運用中の定期的な実施も検討する。	1	1		－	1	有り	ネットワークを通じた不特定多数の攻撃者からの脅威にさらされる。そのため、Webアプリケーションに関する脆弱性を分析する必要がある。 [-] Webアプリケーションを用いない場合	1	有り	内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。 [-] 内部犯を想定する必要がない場合、Webアプリケーションを用いない場合	1	有り	ネットワークを通じた不特定多数の攻撃者からの脅威にさらされる。そのため、Webアプリケーションに関する脆弱性を分析する必要がある。 [-] Webアプリケーションを用いない場合
E.3.1.3							DB診断実施の有無	無し	有り						【メトリクス】 DB診断とは、データベースシステムに対して行うセキュリティ診断のことを言う。 【レベル1】 DB診断は、システム運用開始前に実施するだけでなく、システム運用中の定期的な実施も検討する。	0	0		－									
E.4.1.1		セキュリティリスク管理	セキュリティリスクの見直し	対象システムにおいて、運用開始後に新たに発見された脅威の洗い出しとその影響の分析をどの範囲で実施するかを確認するための項目。 セキュリティリスクの見直しには、セキュリティホールや脆弱性、新たな脅威の調査等が含まれる。			セキュリティリスク見直し頻度	無し	セキュリティに関するイベントの発生時に実施（随時）	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施					【レベル】 セキュリティに関するイベントとは、重要な脅威や脆弱性の発見、ウィルス感染、不正侵入、DoS攻撃、情報漏えいなどの情報セキュリティに関するインシデントのことを指す。	2	2		－									
E.4.1.2							セキュリティリスクの見直し範囲	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体						1	1		－									
E.4.2.1			セキュリティリスク対策の見直し	対象システムにおいて、運用開始後に発見された脅威に対する対策の方針を確認するための項目。 また、検討するにあたり、発見された脅威についての対応範囲について明らかにする。			運用開始後のリスク対応範囲	対応しない	重要度が高い資産に関連する、あるいは、外接部分の脅威に対応	洗い出した脅威全体に対応						1	1		－									
E.4.2.2							リスク対策方針	無し	有り						【レベル1】 リスク対応方針がある場合は、どのような対策を実施するのかを確認する必要がある。	1	1		－									
E.4.3.1			セキュリティパッチ適用	対象システムの脆弱性等に対応するためのセキュリティパッチ適用に関する適用範囲、方針および適用のタイミングを確認するための項目。 これらのセキュリティパッチには、ウィルス定義ファイル等を含む。 また、セキュリティパッチの適用範囲は、OS、ミドルウェア等毎に確認する必要があり、これらセキュリティパッチの適用を検討する際には、システム全体への影響を確認し、パッチ適用の可否を判断する必要があ			セキュリティパッチ適用範囲	セキュリティパッチを適用しない	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体						2	2		－									
E.4.3.2							セキュリティパッチ適用方針	セキュリティパッチを適用しない	緊急性の高いセキュリティパッチのみ適用	全てのセキュリティパッチを適用						1	1		－									
E.4.3.3							セキュリティパッチ適用タイミング	セキュリティパッチを適用しない	障害パッチ適用時に合わせて実施	定期保守時に実施	パッチ出荷時に実施				【レベル】 セキュリティパッチを適用するまでの脅威等にさらされている期間は、監視強化や暫定対策の実施を検討する。 【レベル3】 パッチが出荷されてから適用するまでの期間について検討することが望ましい。パッチ検証を実施する場合、環境準備等を含め、パッチ適用までに期間を要することを考慮する。	2	2		－									
E.5.1.1		アクセス・利用制限	認証機能	資産を利用する主体（利用者や機器等）を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード等を用い		○	管理権限を持つ主体の認証	実施しない	1回	複数回の認証	複数回、異なる方式による認証				【メトリクス】 管理権限を持つ主体とは、システムの管理者や業務上の管理者を指す。	2	2		－	1	1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [+] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合	2	複数回の認証	攻撃者が管理権限を手に入れることによる、情報漏洩等の脅威に対抗するため、複数回の認証を実行する必要がある。	2	複数回の認証	攻撃者が管理権限を手に入れることによる、情報漏洩等の脅威に対抗するため、複数回の認証を実行する必要がある。 [-] 外部ネットワーク越しに管理権限を持つ主体がアクセスできない等の場合
E.5.1.2							管理権限を持たない主体の認証	実施しない	1回	複数回の認証	複数回、異なる方式による認証					2	2		－									
E.5.2.1			利用制限	認証された主体（利用者や機器など）に対して、資産の利用等を、ソフトウェアやハードウェアにより制限するか確認するための項目。 例）ドアや保管庫の施錠、USBやCD-RWやキーボードなどの入出力デバイスの制限、コマンド実行制限など。		○	システム上の対策における操作制限度	無し	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可						【メトリクス】 ソフトウェアのインストール制限や、利用制限等、ソフトウェアによる対策を示す。	1	1		－	1	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可	不正なソフトウェアがインストールされる、不要なアクセス経路（ポート等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [-] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	1	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可	不正なソフトウェアがインストールされる、不要なアクセス経路（ポート等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [-] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	1	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可	不正なソフトウェアがインストールされる、不要なアクセス経路（ポート等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [-] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合
E.5.2.2							物理的な対策による操作制限度	無し	必要最小限のハードウェアの利用や操作のみを許可						【メトリクス】 セキュリティゲート等のファシリティによるサーバルームへの入退室管理、情報の保管場所や、サーバ等に対する施錠、USBやCD-RWの入出力デバイスの制限等のための物理的な対策実施を示す。	1	1		－									

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	LMシステム	PDCAツール	PDCAツール補足	LMシステム補足事項 （凡例） －:補足事項無	社会的影響が殆ど無いシステム			社会的影響が限定されるシステム			社会的影響が極めて大きいシステム		
								0	1	2	3	4	5							選択レベル		選択時の条件	選択レベル		選択時の条件	選択レベル		選択時の条件
E.5.3.1			管理方法	認証に必要な情報（例えば、ID/パスワード、指紋、虹彩、静脈など、主体を一意に特定する情報）の追加、更新、削除等のルール策定を実施するかを確認するための項目。			管理ルールの策定	実施しない	実施する							1	1		–									
E.6.1.1		データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。		○	伝送データの暗号化の有無	無し	認証情報のみ暗号化	重要情報を暗号化					【レベル1】 認証情報のみ暗号化とは、システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。	2	2		暗号化方式はCRYPTREC等の基準に準拠すること。	1	認証情報のみ暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [–] 認証情報をネットワークを経由して送信しない場合	2	重要情報を暗号化	ローカルネットワーク経由で重要情報を送付する場合においても、特に重要な情報については、盗聴等の脅威に対抗するために、伝送データを暗号化する必要がある。 （伝送データを暗号化することにより、性能が低下する可能性がある） [–] 専用線を用いる等の物理的な対策が実施されている場合/ローカルネットワーク上での盗聴の脅威については許容する場合/機密性は求められないが完全性が求められる重要情報を扱う場合	2	重要情報を暗号化	ローカルネットワーク経由で重要情報を送付する場合においても、特に重要な情報については、盗聴等の脅威に対抗するために、伝送データを暗号化する必要がある。 （伝送データを暗号化することにより、性能が低下する可能性がある） [–] 専用線を用いる等の物理的な対策が実施されている場合/ローカルネットワーク上での盗聴の脅威については許容する場合/機密性は求められないが完全性が求められる重要情報を扱う場合
E.6.1.2						○	蓄積データの暗号化の有無	無し	認証情報のみ暗号化	重要情報を暗号化					【レベル1】 認証情報のみ暗号化とは、システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。	2	2		暗号化方式はCRYPTREC等の基準に準拠すること。	1	認証情報のみ暗号化	蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [–] 認証を実施しない場合	2	重要情報を暗号化	データベースやバックアップテープ等に格納されている個人情報等やパスワード等の重要情報の漏洩の脅威に対抗するために、蓄積データを暗号化する必要がある。 （蓄積データを暗号化することにより、性能に影響する可能性がある） [–] 耐タンパデバイスの利用、認証対策、運用対策等の他の複数の対策により、安全性が確保されている場合/機密性は求められないが完全性が求められる重要情報を扱う場合	2	重要情報を暗号化	データベースやバックアップテープ等に格納されている個人情報等やパスワード等の重要情報の漏洩の脅威に対抗するために、蓄積データを暗号化する必要がある。 （蓄積データを暗号化することにより、性能に影響する可能性がある） [–] 耐タンパデバイスの利用、認証対策、運用対策等の他の複数の対策により、安全性が確保されている場合/機密性は求められないが完全性が求められる重要情報を扱う場合
E.6.1.3							鍵管理	無し	ソフトウェアによる鍵管理	耐タンパデバイスによる鍵管理					【レベル】 ソフトウェアによる鍵管理とは、秘密鍵情報に対し、ソフトウェアの設定等によりアクセス制御を実施するような管理のことである。 耐タンパデバイスによる鍵管理とは、ICカードのような、物理的な仕掛により、攻撃への耐性を高めた専用デバイスによる管理のことである。これにより、鍵情報の改竄や漏洩といった脅威に対して、より厳密に管理することができる。	1	1		–									
E.7.1.1		不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 なお、どのようなログを取得する必要があるかは、実現するシステムやサービスに応じて決定する必要がある。 また、ログを取得する場合には、不正監視対象と併せて、取得したログのうち、確認する範囲を定める必要がある。		○	ログの取得	実施しない	実施する						【メトリクス】 取得対象のログは、不正な操作等を検出するための以下のようなものを意味している。 取得したログは個々のログを確認するだけでなく、複数のログを組み合わせて相関分析することも検討する。必要に応じて、ログと作業記録との突き合わせも行う。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ ・セキュリティ機器の検知ログ ・通信ログ ・DBログ ・アプリケーションログ 等	1	1		不正アクセスの拡大防止のための対応策としてシステムの緊急停止、不正アクセス元からのアクセス遮断等の機能を設けること。 また、復旧方法・手順を策定しておくこと。	1	実施する	不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行し」「その結果、どのようになったか」を確認し、その後の対策を迅速に実施するために、ログを取得する必要がある。 （ログ取得の処理を実行することにより、性能に影響する可能性がある）	1	実施する	不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行し」「その結果、どのようになったか」を確認し、その後の対策を迅速に実施するために、ログを取得する必要がある。 （ログ取得の処理を実行することにより、性能に影響する可能性がある）	1	実施する	不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行し」「その結果、どのようになったか」を確認し、その後の対策を迅速に実施するために、ログを取得する必要がある。 （ログ取得の処理を実行することにより、性能に影響する可能性がある）
E.7.1.2						○	ログ保管期間	6ヶ月	1年	3年	5年	10年以上有期	永久保管			2	1		不正アクセスの拡大防止のための対応策としてシステムの緊急停止、不正アクセス元からのアクセス遮断等の機能を設けること。 また、復旧方法・手順を策定しておくこと。	0	6ヶ月	不正行為を確認する、また、正しく処理された証跡を保持するために、適切な期間、ログを保管する必要がある。 [–] ログの確認間隔が短い場合 [+] バックアップ等の容量が確保できる場合	2	3年	不正行為を確認する、また、正しく処理された証跡を保持するために、適切な期間、ログを保管する必要がある。 [–] ログの確認間隔が短い場合 [+] バックアップ等の容量が確保できる場合	3	5年	不正行為を確認する、また、正しく処理された証跡を保持するために、適切な期間、ログを保管する必要がある。 [–] ログの確認間隔が短い場合 [+] バックアップ等の容量が確保できる場合
E.7.1.3						○	不正監視対象（装置）	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体					【メトリクス】 不正監視対象（装置）とは、サーバ、ストレージ等への不正アクセス等の監視のために、ログを取得する範囲を確認するメトリクス。	2	LM準拠	ハードウェア関連はLMシステム準拠。	不正アクセスの拡大防止のための対応策としてシステムの緊急停止、不正アクセス元からのアクセス遮断等の機能を設けること。 また、復旧方法・手順を策定しておくこと。 ※ なお、対象がクラウドサービスである場合、責任共有モデルに基づき、クラウドサービス提供事業者の責任範囲であれば保証の対象外とするが、レベル2を目標とすること。	1	重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ等の範囲を定めておく必要がある。	1	重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ等の範囲を定めておく必要がある。	2	システム全体	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ等の範囲を定めておく必要がある。外部ネットワーク経由での攻撃等により攻撃範囲が限定されないことを想定し、システム全体に対して監視を実施する必要がある。
E.7.1.4						○	不正監視対象（ネットワーク）	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体					【メトリクス】 不正監視対象（ネットワーク）とは、ネットワーク上の不正なパケット等を監視するためのログの取得範囲を確認するメトリクス。	1	LM準拠	ハードウェア関連はLMシステム準拠。	不正アクセスの拡大防止のための対応策としてシステムの緊急停止、不正アクセス元からのアクセス遮断等の機能を設けること。 また、復旧方法・手順を策定しておくこと。	1	重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするネットワークの範囲を定めておく必要がある。	1	重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするネットワークの範囲を定めておく必要がある。	2	システム全体	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするネットワークの範囲を定めておく必要がある。外部ネットワーク経由での攻撃等により攻撃範囲が限定されないことを想定し、システム全体に対して監視を実施する必要がある。
E.7.1.5						○	不正監視対象（侵入者・不正操作等）	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体					【メトリクス】 不正監視対象（侵入者・不正操作等）とは、不正な侵入者等を監視するために設置する監視カメラ等による監視の範囲を意味する。	1	LM準拠	ハードウェア関連はLMシステム準拠。	不正アクセスの拡大防止のための対応策としてシステムの緊急停止、不正アクセス元からのアクセス遮断等の機能を設けること。 また、復旧方法・手順を策定しておくこと。	1	重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするフロア、エリア等の物理的な範囲を定めておく必要がある。 [–]入退室管理、操作制限等の対策が十分に施されている場合	1	重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするフロア、エリア等の物理的な範囲を定めておく必要がある。	2	システム全体	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするフロア、エリア等の物理的な範囲を定めておく必要がある。
E.7.1.6							確認間隔	無し	セキュリティに関するイベントの発生時に実施（随時）	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施	常時確認				【レベル3】 常時確認とは、常に不正なアクセス等を監視し、即座に対応可能な状態を意味する。 自動検知システムを導入し、不正検知時にメール等で通知する仕組みの導入は、セキュリティに関するイベントの発生時に実施（随時）に含まれる。	2	LM準拠	ハードウェア関連はLMシステム準拠。	不正アクセスの拡大防止のための対応策としてシステムの緊急停止、不正アクセス元からのアクセス遮断等の機能を設けること。 また、復旧方法・手順を策定しておくこと。									
E.7.2.1			データ検証	情報が正しく処理されて保存されていることを証明可能とし、情報の改ざんを検知するための仕組みとしてデジタル署名を導入するかを確認するための項目。			デジタル署名の利用の有無	無し	有り							0	0		–									
E.7.2.2							確認間隔	無し	セキュリティに関するイベントの発生時に実施（随時）	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施	常時確認					0	0		–									
E.8.1.1		ネットワーク対策	ネットワーク制御	不正な通信を遮断するための制御を実施するかを確認するための項目。		○	通信制御	無し	有り						【レベル1】 通信制御を実現する際には、ファイアウォール、IPS、URLフィルタ、メールフィルタ等の導入を検討する必要がある。	1	LM準拠	ハードウェア関連はLMシステム準拠。	ログインID、パスワード、端末認証による認証を行うこと。 また、外部ネットワークとの接続部についてはFW・DMZ等の対策を講じること。	1	有り	踏み台攻撃等の脅威や、情報の持ち出しを抑止するために、不正な通信を遮断等のネットワーク制御を実施する必要がある。 [–] 踏み台等の脅威を許容する場合	1	有り	踏み台攻撃等の脅威や、情報の持ち出しを抑止するために、不正な通信を遮断等のネットワーク制御を実施する必要がある。 [–] 踏み台等の脅威を許容する場合	1	有り	踏み台攻撃等の脅威や、情報の持ち出しを抑止するために、不正な通信を遮断等のネットワーク制御を実施する必要がある。 [–] 踏み台等の脅威を許容する場合
E.8.2.1			不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目。		○	不正通信の検知範囲	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体					【メトリクス】 検知範囲の設定に応じて、IDS等の導入を検討する必要がある。	1	LM準拠	ハードウェア関連はLMシステム準拠。	–	1	重要度が高い資産を扱う範囲、あるいは、外接部分	不正な通信を確認し、対策を迅速に実施うために、不正検知を実施する必要がある。	1	重要度が高い資産を扱う範囲、あるいは、外接部分	不正な通信を確認し、対策を迅速に実施うために、不正検知を実施する必要がある。	1	重要度が高い資産を扱う範囲、あるいは、外接部分	不正な通信を確認し、対策を迅速に実施うために、不正検知を実施する必要がある。
E.8.3.1			サービス停止攻撃の回避	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目。		○	ネットワークの輻輳対策	無し	有り							1	LM準拠	ハードウェア関連はLMシステム準拠。	–	1	有り	DoS/DDoS攻撃のサービス停止攻撃に対応する必要がある。 （可用性と関連する） [–] DoS/DDoS攻撃については、可用性対策にてある程度の対策を実施し、それ以上は許容する場合	1	有り	DoS/DDoS攻撃のサービス停止攻撃に対応する必要がある。 （可用性と関連する） [–] DoS/DDoS攻撃については、可用性対策にてある程度の対策を実施し、それ以上は許容する場合	1	有り	DoS/DDoS攻撃のサービス停止攻撃に対応する必要がある。 （可用性と関連する） [–] DoS/DDoS攻撃については、可用性対策にてある程度の対策を実施し、それ以上は許容する場合
E.9.1.1		マルウェア対策	マルウェア対策	マルウェア（ウィルス、ワーム、ボット等）の感染を防止する、マルウェア対策の実施範囲やチェックタイミングを確認するための項目。 対策を実施する場合には、ウィルス定義ファイルの更新方法やタイミングについても検討し、常に最新の状態となるようにする必要がある。		○	マルウェア対策実施範囲	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体						2	2		–	1	重要度が高い資産を扱う範囲、あるいは、外接部分	マルウェアの感染により、サービス停止等の脅威に対抗するために、マルウェア対策を実施する必要がある。 [–] 攻撃対象となりにくいOS等を利用する場合	1	重要度が高い資産を扱う範囲、あるいは、外接部分	マルウェアの感染により、重要情報が漏洩する脅威等に対抗するために、マルウェア対策を実施する必要がある。 [–] 攻撃対象となりにくいOS等を利用する場合	1	重要度が高い資産を扱う範囲、あるいは、外接部分	マルウェアの感染により、重要情報が漏洩する脅威等に対抗するために、マルウェア対策を実施する必要がある。 [–] 攻撃対象となりにくいOS等を利用する場合
E.9.1.2							リアルタイムスキャンの実施	実施しない	実施する						【レベル1】 リアルタイムスキャンは、例えば、以下のようなタイミングで実施する。実施する際は実施するタイミングを検討する必要がある。 ・ファイルサーバへデータをコピーするタイミング ・メールサーバがメールを受信したタイミング ・ファイルへの入出力処理が実行される前 等	1	1		システムの特性に応じて提案すること。									
E.9.1.3							フルスキャンの定期チェックタイミング	無し	不定期（フルスキャンを行えるタイミングがあれば実施する）	1回/月	1回/週	1回/日				3	3		システムの特性に応じて提案すること。									
E.10.1.1		Web対策	Web実装対策	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。		○	セキュアコーディング、Webサーバの設定等による対策の強化	無し	対策の強化						【メトリクス】 Webシステムが攻撃される事例が増加しており、Webシステムを構築する際には、セキュアコーディング、Webサーバの設定等による対策の実施を検討する必要がある。また、実施した結果の有効性を確認するための専門家のレビューやソースコード診断、ツールによるチェック等についても検討する必要がある。	0	0		–	1	対策の強化	オープン系のシステムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバに対する対策を実施する必要がある。 [–] Webアプリケーションを用いない場合	1	対策の強化	オープン系のシステムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバに対する対策を実施する必要がある。 [–] Webアプリケーションを用いない場合	1	対策の強化	オープン系のシステムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバに対する対策を実施する必要がある。 [–] Webアプリケーションを用いない場合
E.10.1.2						○	WAFの導入の有無	無し	有り						【メトリクス】 WAFとは、Web Application Firewallのことである。	1	LM準拠	ハードウェア関連はLMシステム準拠。	–	0	無し	重要情報を取り扱わないため、WAFを導入しての対策は実施しない。	0	無し	外部ネットワークへの接続については想定しない。そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] 内部ネットワークを経由した攻撃による脅威を想定する場合	1	有り	システムに侵入されることによる、情報の漏洩、踏み台等の脅威に対抗するために、機器による、侵入抑止、検知を実施する必要がある。 [–] Webサーバへの対策、不正アクセス防止、ログの定期的な確認等が実施されている場合
E.11.1.1		セキュリティインシデント対応/復旧	セキュリティインシデント対応/復旧	セキュリティインシデントが発生した時に、早期発見し、被害の最小化、復旧の支援等をするための体制について確認する項目。			セキュリティインシデントの対応体制	無し	有り						【メトリクス】 セキュリティインシデント発生時の対応以外にも、インシデント対応マニュアルの整備や、システムの関係者に対するセキュリティ教育を実施する。 【レベル0】 セキュリティインシデント発生の都度、インシデント対応体制を構築する場合も含まれる。 【レベル1】 新たに対応体制を構築する他に、ユーザ企業内のCSIRTを利用する場合や、外部のセキュリティ対応サービスを利用する場合も含まれる。	1	LM準拠	セキュリティレベルはLMシステムに依存	–									
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	構築時の制約となる社内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク		○	構築時の制約条件	制約無し	制約有り（重要な制約のみ適用）	制約有り（全ての制約を適用）					【メトリクス】 システムを開発する際に、機密情報や個人情報等を取り扱う場合がある。これらの情報が漏洩するリスクを軽減するために、プロジェクトでは、情報利用者の制限、入退室管理の実施、取り扱い情報の暗号化等の対策が施された開発環境を整備する必要が生じる。 また運用予定地での構築が出来ず、別地にステージング環境を設けて構築作業を行った上で運用予定地に搬入しなければならない場合や、逆に運用予定地でなければ構築作業が出来ない場合なども制約条件となる。	–			–	0	制約無し	特に制限などを受けない場合を想定。 [+] 法や条例の制約を受ける場合、もしくは業界などの標準や取り決めなどがある場合	1	制約有り（重要な制約のみ適用）	社内規約などが存在する場合を想定。 [–] 法や条例の制約を受けない場合、もしくは業界などの標準や取り決めなどがない場合	1	制約有り（重要な制約のみ適用）	法の制約などを受ける場合を想定。 [–] 法や条例の制約を受けない場合、もしくは業界などの標準や取り決めなどがない場合 [+] 法や条例の順守よりも高度な社内基準の制約を受け、かつ、全てに対応することが必要な場合
F.1.2.1			運用時の制約条件	運用時の制約となる社内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク		○	運用時の制約条件	制約無し	制約有り（重要な制約のみ適用）	制約有り（全ての制約を適用）						–			–	0	制約無し	特に制限などを受けない場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	1	制約有り（重要な制約のみ適用）	設置に関して何らかの制限が発生するセンターやマシンルームを前提として考慮。ただし条件の調整などが可能な場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	1	制約有り（重要な制約のみ適用）	設置に関して何らかの制限が発生するセンターやマシンルームを前提として考慮。ただし条件の調整などが可能な場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合
F.2.1.1		システム特性	ユーザ数	システムを使用する利用者(エンドユーザ)の人数。	○	○	ユーザ数	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用					【重複項目】 B.1.1.1。ユーザ数は性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもあるため、性能・拡張性とシステム環境・エコロジーの両方に含まれている。 【レベル】 前提となる数値が決められない場合は、類似システムなどを参考に仮の値でも良いので決めておくことが必要。	0	0		–	0	特定ユーザのみ	部門内利用などでユーザが特定できる場合を想定。 [+] ユーザを特定できない場合	1	上限が決まっている	あらかじめ一定の上限値を設定する場合を想定。 [–] 特定のユーザのみ使用することを合意できた場合	2	不特定多数のユーザが利用	国民全体がアクセスする可能性があるような場合を想定。 [–] 一定の上限値を設定することが可能な場合
F.2.2.1			クライアント数	システムで使用され、管理しなければいけないクライアントの数。		○	クライアント数	特定クライアントのみ	上限が決まっている	不特定多数のクライアントが利用						0	0		–	0	特定クライアントのみ	特定のクライアントのみが使用することを想定。 [+] 将来的にクライアント数の増加が予想され、上限値で合意が必要な場合	1	上限が決まっている	あらかじめ一定の値を決めて合意することを想定。 [+] 上限台数を設定きない場合	1	上限が決まっている	あらかじめ一定の値を決めて合意することを想定。 [+] 上限台数を設定きない場合
F.2.3.1			拠点数	システムが稼働する拠点の数。		○	拠点数	単一拠点	複数拠点						【レベル1】 拠点数を合意した場合は具体的な値を設定すること。	0	0		–	0	単一拠点	単一拠点を想定。 [+] 複数拠点の場合	1	複数拠点	複数拠点を想定。 [–] 単一拠点の場合	1	複数拠点	複数拠点を想定。 [–] 単一拠点の場合
F.2.4.1			地域的広がり	システムが稼働する地域的な広がり。		○	地域的広がり	拠点内	同一都市内	同一都道府県内	同一地方	国内	海外		【レベル】 レベル5になると、多言語対応などの考慮も必要となる。 また、国内であっても範囲が広がるにつれて、ネットワークや物流、サポートなどの面で対応が必要となる。	0	0		–	0	拠点内	アクセス範囲を拠点内とし、外部からのアクセスがない場合を想定。 [+] リモートアクセスを許すなどアクセス範囲が拠点外にも広がる場合	0	拠点内	アクセス範囲を拠点内とし、外部からのアクセスがない場合を想定。 [+] 他の事業所から利用させる場合	4	国内	アクセス範囲は国内とすることを想定。 [–] ユーザ権限を企業や団体内ユーザに限定する場合 [+] インターネットシステムなどで、アクセス範囲が国外にも広がる場合
F.2.5.1			特定製品指定	ユーザの指定によるオープンソース製品や第三者製品(ISV/IHV)などの採用の有無を確認する項目。採用によりサポート難易度への影響があるかの視点で確認を行う。		○	特定製品の採用有無	特定製品の指定がない	一部に特定製品の指定がある	サポートが困難な製品の指定がある						0	0		–	0	特定製品の指定がない	構成する機器に関して指定製品がない場合を想定。 [+] 特に指定があった場合	1	一部に特定製品の指定がある	構成する機器に関して固有の製品が指定された場合を想定。 [–] 特に指定がない場合	0	特定製品の指定がない	構成する機器に関して指定製品がない場合を想定。 [+] 特に指定があった場合

項番	大項目	中項目	小項目	小項目説明	最低限項目	重要項目	メトリクス（指標）	レベル 0	1	2	3	4	5	運用コストへの影響	備考	LMシステム	PDCAツール	PDCAツール補足	LMシステム補足事項 （凡例） －：補足事項無	社会的影響が殆ど無いシステム 選択レベル	選択時の条件	社会的影響が限定されるシステム 選択レベル	選択時の条件	社会的影響が極めて大きいシステム 選択レベル	選択時の条件
F.2.6.1			システム利用範囲	システム利用者が属する属性の広がり。			システム利用範囲	部門内のみ	社内のみ	社外（BtoB）	社外（BtoC）					1	1		－						
F.2.7.1			複数言語対応	システム構築の上で使用が必要、またはサービスとして提供しなければならない言語。扱わなければならない言語の数や各言語スキル保持者へのアクセシビリティを考慮。			言語数	数値などのみ扱う	1	2	5	10	100		【レベル】 言語数だけでなく、別途、言語の難易度も併せて検討することが必要である。 また、通貨単位なども考慮しておく必要がある。 【レベル0】 数値データなどのみを扱うとは、人に対するプレゼンテーション機能を想定せず、マシン間でのインターフェースを扱うようなシステムを想定している。例えば、GWシステムなどである。	1	1		－						
F.3.1.1		適合規格	製品安全規格	提供するシステムに使用する製品について、UL60950などの製品安全規格を取得していることを要求されているかを確認する項目。		○	規格取得の有無	規格取得の必要無し	UL60950相当取得							0	0		－	0	規格取得の必要無し	機器の規格取得に関して指定がない場合を想定。 [+] 特に指定があった場合	1	UL60950相当取得	機器の規格取得に関して指定があった場合を想定。 [－] 特に指定がない場合	0	規格取得の必要無し	機器の規格取得に関して指定がない場合を想定。 [+] 特に指定があった場合
F.3.2.1			環境保護	提供するシステムに使用する製品について、RoHS指令などの特定有害物質の使用制限についての規格の取得を要求されているかを確認する項目。		○	規格取得の有無	規格取得の必要無し	RoHS指令相当取得							0	0		－	0	規格取得の必要無し	特に制限などを受けない場合を想定。 [+] 特に指定があった場合	1	RoHS指令相当取得	RoHS指令対応の装置が指定された場合を想定。 [－] 特に指定が無かった場合	0	規格取得の必要無し	特に制限などを受けない場合を想定。 [+] 特に指定があった場合
F.3.3.1			電磁干渉	提供するシステムに使用する製品について、VCCIなどの機器自身が放射する電磁波をある一定以下のレベルに抑える規格を取得していることを要求されているかを確認する項目。			規格取得の有無	規格取得の必要無し	VCCI ClassA取得	VCCI ClassB取得						0	0		－								
F.4.1.1		機材設置環境条件	耐震／免震	地震発生時にシステム設置環境で耐える必要のある実効的な最大震度を規定。建屋が揺れを減衰するなどの工夫により、外部は震度7超でも設置環境では実効的に最大震度4程度になる場合には震度4よりレベルを設定する。なお、想定以上の揺れではサービスを継続しない		○	耐震震度	対策不要	震度4相当（50ガル）	震度5弱相当（100ガル）	震度6弱相当（250ガル）	震度6強相当（500ガル）	震度7相当（1000ガル）		【メトリクス】 設置環境での実効的な震度は、屋外の振動がそのまま伝わる建屋の場合は外部の震度と設置環境の震度はほぼ一致すると考えられるので、外部震度からレベルを設定すればよい。ただし、建屋の免震設備などにより、設置環境での最大震度を低く保証できる場合にはその震度を実効的な震度としてレベル設定が可能と考えられる（ユーザからの特段の要請を受けて、より高いレベルで設定する場合も有り）。なお、一定の震度以上では周辺のシステム利用者がシステムを利用できる環境に無いなどで、サービスの継続が不要となる場合は、その震度からレベル設定することも考えられる。いずれに於いても建屋の耐震震度を超える水準での設定には無理がある。 【レベル0】 地震発生によるサービス停止などのリスクを受け入れる心積もりが別途必要となる。	5	LM準拠	ハードウェア関連はLMシステム準拠。	－	2	震度5弱相当（100ガル）	震度5弱相当を想定。 [－] 免震構造の建屋に設置するなど建屋と設置環境とを見合わせレベル変更する場合 [+] 特に値が指定された場合は相応するレベルに変更、免震構造を持たないオフィス内などに設置するなどラック転倒などによる人災を避けるために耐震ラックの利用などレベルを上げることも配慮が必要な場合	3	震度6弱相当（250ガル）	震度6弱相当を想定。 [－] 免震構造の建屋に設置するなど建屋と設置環境とを見合わせレベル変更する場合 [+] 特に値が指定されるなど建屋と設置環境とを見合わせ相応するレベルに変更する場合	4	震度6強相当（500ガル）	震度6強相当を想定。 [－] 免震構造の建屋に設置するなど建屋と設置環境と機器環境を総合して考慮する場合 [+] 特に震度7など強い地震に相応する値が指定された場合
F.4.2.1			スペース	どの程度の床面積（WxD）/高さが必要かの項目。保守作業用スペースについても考慮する。また、移行時には新旧システムが並行稼働可能なスペースの確保が可能か否かについても確認が必要である。可能であれば事前確認を実施する。		○	設置スペース制限（マシンルーム）	スペースに関する制限無し	フロア設置用機材を用いて構成	ラックマウント用機材を用いて構成					【メトリクス】 具体的な面積と高さも併せて確認する。また、スペース形状や場所による耐荷重の差異にも留意すること。	－			－	2	ラックマウント用機材を用いて構成	ラックマウントなどでの搭載を想定。 [－] 設置に関して制限がない場合	2	ラックマウント用機材を用いて構成	ラックマウントなどでの搭載を想定。 [－] 設置に関して制限がない場合	2	ラックマウント用機材を用いて構成	センターでのラックマントを想定。 [－] 設置に関して制限がない場合
F.4.2.2						○	設置スペース制限（事務所設置）	スペースに関する制限無し	専用のスペースを割当て可能	人と混在するスペースに設置必要					【メトリクス】 具体的な面積と高さも併せて確認する。また、スペース形状や場所による耐荷重の差異にも留意すること。 【レベル】 設置スペース制限は前提条件として既に規定されていると捉え、その要求に対してシステムを設置する場合の難易度をレベルとしている。スペース確保の視点での難易度ではないことに注意。	－			－	1	専用のスペースを割当て可能	オフィスフロア内のサーバ・コーナーなどに設置することを想定。 [－] 人がほとんど立ち入らない場所への設置の場合 [+] 操作や監視などの関係上、仕切りなど無しに人と混在するスペースに設置が必要な場合	2	人と混在するスペースに設置必要	端末機などフロントエンド業務用の機材を想定。 [－] 業務的に人との混在が不要な場合	2	人と混在するスペースに設置必要	端末機などフロントエンド業務用の機材を想定。 [－] 業務的に人との混在が不要な場合
F.4.2.3							並行稼働スペース（移行時）	専用スペースの確保が可能	共用スペースの確保が可能	確保不可					【メトリクス】 構築時に、まだ本番運用で用いるスペースが使用できない場合は、構築時のスペースおよび移設に関しても考慮すること。更に、具体的な面積と高さも併せて確認する。また、スペース形状や場所による耐荷重の差異にも留意すること。 【レベル2】 並行稼働有りの場合には、別途対策を検討すること。関係項目に D.1.1.3、F.4.4.3がある。	－			－								
F.4.2.4							設置スペースの拡張余地	十分な拡張余地有り	一部制約有り（既製品で対応できるレベル）	制約有り（特注対応や工事が必要）					【メトリクス】 設置スペースの拡張余地には、フロアに直接置くだけでなくラックの制約や床荷重なども含まれる。	－			－								
F.4.3.1			重量	建物の床荷重を考慮した設置設計が必要となることを確認する項目。低い床荷重の場合ほど、設置のための対策が必要となる可能性が高い。			床荷重	2,000Kg/㎡以上	1,200Kg/㎡	800Kg/㎡	500Kg/㎡	300Kg/㎡	200Kg/㎡	○	【レベル】 床が耐えられる荷重でレベル化。耐荷重が大きいほど設置に関する制約が少ない。 【運用コストへの影響】 床荷重が高い場合、副次的に高密度な実装となり、高ラック位置での保守作業などが必要になる場合がある。	－			－								
F.4.3.2							設置対策	不要	荷重を分散するための資材（鉄板など）を配備する	ラック当りの重量を制限して、分散構成を採る	設置環境固有の条件（塗の場所など）を考慮して、設置設計を行う					－			－								
F.4.4.1			電気設備適合性	ユーザが提供する設置場所の電源条件（電源電圧/電流/周波数/相数/系統数/無停止性/必要工事規模などと導入システムの適合性に関する項目。同時に空調についても評価対象とする。また、移行時の並行稼動が可能か否かについても確認が必要である。可能であれば事前確認を実施する。			供給電力適合性	現状の設備で特に制限無し	電源工事は必要だが、分電盤改造などニ次側の工事のみで対応可能	電源工事は必要だが、一次、二次とも工事可能	工事などができず、規模に対して容量が少し足りない	まったく対応できず、設置場所を再考する必要がある					－			－								
F.4.4.2							電源容量の制約	制約無し（必要な電源容量の確保が可能）	制約有り（既製品で対応できるレベル）	制約有り（カスタマイズや工事が必要）						－			－								
F.4.4.3							並行稼働電力（移行時）	全面的に確保が可能	部分的に確保が可能	確保が困難					【レベル2】 移行時に並行稼働が必要な場合には、別途対策を検討すること。関係項目に D.1.1.3、F.4.2.3がある。	－			－								
F.4.4.4							停電対策	無し	瞬断（10ms程度）	10分	1時間	1日間	1週間		【レベル1】 UPS、CVCFなど電源安定化の対策を検討する。	－			－								
F.4.4.5							想定設置場所の電圧変動	±10%以下	±10%を超える						【レベル1】 機材の動作条件を逸脱する場合には、UPS、CVCFなど電源安定化の対策が必要となる。	－			－								
F.4.4.6							想定設置場所の周波数変動	±2%以下	±2%を超える						【レベル1】 機材の動作条件を逸脱する場合には、UPS、CVCFなど電源安定化の対策が必要となる。	－			－								
F.4.4.7							接地	接地不要	接地が必要	専用接地が必要						－			－								
F.4.5.1			温度（帯域）	システムが稼働すべき環境温度の帯域条件。 周囲環境によってはシステムを正常稼動させるには特別な対策が必要となることがある。			温度（帯域）	対策不要	16度から32度（多くのテープ装置の稼働可能条件）	5度から35度（多くの機器の稼働可能条件）	0度～40度	0度～60度	−30度～80度		【メトリクス】 温度勾配は10℃/h程度以下に抑えることも併せて考慮する。また、レベル2以上の環境では非稼働時の確認も別途必要である。 【レベル】 機器が稼働している状態での周囲環境の変動範囲でレベルを選択する。例えば、周囲環境温度が0～20度で変動している環境であれば、それを満たすレベルの中で一番低いレベル3となる。	－			－								
F.4.6.1			湿度（帯域）	システムが稼働すべき環境湿度の帯域条件。 周囲環境によってはシステムを正常稼動させるには特別な対策が必要となることが			湿度（帯域）	対策不要	45%～55%	20%～80%	0%～85%	結露無し条件のみ			【レベル】 機器が稼働している状態での周囲環境の変動範囲でレベルを選択する。例えば、周囲環境湿度が20～50%で変動している環境であれば、それを満たすレベルの中で一番低いレベル2となる。	－			－								
F.4.7.1			空調性能	システムを稼働させるのに十分な冷却能力を保持し、特定のホットスポットが存在する場合にはそれを考慮した冷気供給を行える能力。			空調性能	十分な余力有り	ホットスポットなどへの部分的な対策が必要	能力が不足しており、対策が必要					【メトリクス】 必要に応じて塵芥や有害ガスへの対応なども考慮する。	－			－								
F.4.7.2							空調設備の制約	制約無し（必要な空調の確保が可能）	制約有り（既製品で対応できるレベル）	制約有り（カスタマイズや工事が必要）						－			－								
F.5.1.1		環境マネージメント	環境負荷を抑える工夫	環境負荷を最小化する工夫の度合いの項目。 例えば、グリーン購入法適合製品の購入など、環境負荷の少ない機材・消耗品を採用する。 また、ライフサイクルを通じた廃棄材の最小化の検討を行う。例えば、拡張の際に既設機材の廃棄が不要で、必要な部材の増設、入れ替えのみで対応可能な機材を採用するなどである。また、ライフサイクルが長い機材ほど廃棄材は少ないと解釈できる。			グリーン購入法対応度	対処不要	グリーン購入法の基準を満たす製品を一部使用	グリーン購入法の基準を満たす製品のみを使用						0	0		－								
F.5.1.2							同一機材拡張余力	無し	2倍	4倍	10倍	30倍	100倍以上		【メトリクス】 既設機材を廃棄することなく、単純に追加で拡張可能であることを意味する（契約上は追加であっても実際には機材全体を置き換えてしまい全廃棄が発生するようなものは対象外となる）。製造エネルギー、廃棄物量までを考慮する。 【レベル】 数倍程度まではスケールアップ主体、それ以上はスケールアウト主体での対応となると考えられる。	－			－								
F.5.1.3							機材のライフサイクル期間	3年	5年	7年	10年以上			○	【メトリクス】 ここでのライフサイクルとは実質的なハードウェア入れ替え期間と規定している。基本的に長期に渡って使用することが望ましいが、あまりにも長期過ぎると性能向上や省電力技術の進歩などの恩恵が受けられなくなることにも注意が必要である。 【運用コストへの影響】 ライフサイクルの短い機材を使用すると、頻繁な更新が必要となるため、運用コストが増大する懸念がある。	－			－								
F.5.2.1			エネルギー消費効率	本来はシステムの仕事量をそのエネルギー消費量で除した単位エネルギー当りの仕事量のこと。ただし、汎用的な仕事量の定義が存在しないため、効率を直接求めることは困難である。また、同じ仕事を行う別のシステムも存在しないことが多いため、比較自体も困難である。このため、エネルギー消費効率に関しては、少し視点を変えて、ユーザからの			エネルギー消費の目標値	目標値無し	目標値の提示有り	目標値の提示が有り、更なる追加削減の要求も有る				○	【レベル0】 電源設備などとの整合性の再確認が必要である。 【レベル2】 レベルIの目標値達成に止まらず、更に厳しい基準へのオプション要望があることを示す。 【運用コストへの影響】 低いレベルで合意した場合、新法令の制定などで運用後に対応が必要となる場合がある。	－			－								
F.5.3.1			CO_2排出量	システムのライフサイクルを通じて排出されるCO_2の量。ただし、単純なCO_2排出量でレベル化するのは困難であるため、少し視点を変えて、ユーザからの目標値の提示の有無などでレベル化を行っている。			CO_2排出量の目標値	目標値の設定不要	目標値の提示有り	目標値の提示が有り、更なる追加削減の要求も有る				○	【メトリクス】 運転時のCO_2排出量は基本的に電力消費量とリンクする形になる。これに生産・廃棄におけるCO_2排出量を加えたものがライフサイクル全体での排出量となる。 【レベル0】 目標値の設定不要とした場合、CSRなどとの整合性の再確認が必要である。 【レベル2】 レベルIの目標値達成に止まらず、更に厳しい基準へのオプション要望があることを示す。 【運用コストへの影響】 低いレベルで合意した場合、新法令の制定などで運用後に対応が必要となる場合があ	－			－								
F.5.4.1			低騒音	機器から発生する騒			騒音値	対策不要	87dB(英国	85dB(英国	80dB(英国	40dB(図書	35dB(寝室	○	【運用コストへの影響】	－			－								

提　案　書　作　成　要　領

「マーケティングの高度化に向けた分析と施策管理に関わるツール等の更改」

株式会社ゆうちょ銀行
デジタル戦略部　リテールマーケティング室

本調達においては、総合評価落札方式による委託先の適切な選定を目的とし、次に規定する要領に従って作成した提案書の提出を求めるものである。

したがって、提案書は、仕様書に定める要求要件について、応札者自身が満足する能力を有していることを証明する内容を求めるものであり、その内容について評価を実施するものとする。

１　提出物

(1) 提案書

仕様書（仕様書から参照されている付属資料を含む）に記載された要件をどのように実現するか記述するもの。

(2) 見積書

本案件を実現するに当たり、必要な費用及び工数等を記述するもの。

(3) 適合証明書

本案件に札を入れるにあたり、要件を満たしていることを証明するもの。

２　共通事項（提案書・見積書）

各資料の作成に当たっては、次の事項に留意すること。

(1) 2穴式のファイルに綴ること。

(2) 提案書・見積書を、紙で8部提出すること。
また、電子ファイルを語彙検索可能なPDFファイル等主管部が指定する形式に変換し、CD-R（正・副それぞれ１枚）に保存して紙と併せて提出すること。ただし、当行が別に形式を定めて提出を求める場合はこの限りでない。

(3) 原則両面印刷とすること。

(4) 提案内容が簡潔に記載されていること。

(5) 特段の専門的知識を要することなく提案内容を評価できるよう配慮すること。

(6) 提案内容について、根拠又は参考となる資料を添付すること。

(7) 各項目において該当事項が無い場合には、その旨を記載すること。

３　提案書の様式

(1) 日本語で記載すること。

(2) Ａ４判縦の用紙に横書きとする。ただし、図表等を使用する場合は、必要に応じて適

宜の方法で使い分けるものとする。その際、文字等が見づらくならないように留意する。

(3) 見出し符号

ア　項目を細別するときは、次の項番順序による。

１　〇〇〇〇

(1) 〇〇〇〇

ア　〇〇〇〇

(ｱ) 〇〇〇〇

Ａ　〇〇〇〇

(A) 〇〇〇〇

ａ　〇〇〇〇

(a) 〇〇〇〇

注１：上記の項番で不足する場合には、適宜項番を設定し使用すること。

注２：イ、ロ、ハ・・・・・の順は用いない。

イ　図表には、上部に次のような番号及びタイトルを付与すること。

図△ 〇〇〇〇 ／ 表△ 〇〇〇〇

(4) 目次及びページ番号を付与すること。

(5) ページ数は、総枚数 400 ページ程度（カタログ、パンフレット等を除く。）とする。

４　提案項目

提案書の記述項目は次のとおりとし、記述項目名称は提案書における各章の見出しとして使用すること。提案に当たっては、仕様書に定める要求要件をすべて満たす内容とし、総合評価基準の各項目の評価観点を踏まえ、具体的かつ明確に記述すること。

記述に当たっては、記述項目ごとに、仕様書該当項目との対応及び総合評価基準に定める要求要件に記述されている各評価観点との対応を記入すること。

(1) 必須要件（仕様書に定める要求要件）

仕様書に定めるすべての要件に対して満足する具体的な提案がなされていることを確認できるように仕様書の項番号に対比させた形式で記載すること。

なお、仕様書に求める機器等については、具体的な商品名等が確認できるカタログ、パンフレット等を添付すること。

(2) 必須以外の要件

様式 27 別添「提案書目次構成兼提案書評価基準表」の評価方法を参照。

５　提案書の説明会

提案書提出後、提案書提出者による説明会を実施する。

なお、説明会の詳細については、提案書提出後、別途通知する。

６　提案書等に関する照会先

株式会社ゆうちょ銀行　営業部門　デジタル戦略部　リテールマーケティング室

担当　LM・BI 担当

TEL　03-3477-2012

総　合　評　価　基　準

「マーケティングの高度化に向けた分析と施策管理に関わるツール等の更改」

株式会社ゆうちょ銀行
デジタル戦略部　リテールマーケティング室

本評価基準については、「マーケティングの高度化に向けた分析と施策管理に関わるツール等の更改」の仕様書に基づいて定めたものであり、評価に当たっては次により行う。

なお、落札者が入札者とともに提出した提案書の内容は、仕様書等と同様にすべて納入検査等の対象とする。

１　評価方式

本調達は総合評価落札方式（加算方式）を用い、提案内容を評価した性能評価点（最高1,500点を3倍したもの）と予定価格を下回った入札価格を点数化した価格点（最高1,500点）の合計点を総合評価点とする。

２　必須要件

提案書は、仕様書に定める要求要件をすべて満たしていなければならない。

なお、一つでも仕様書に定める要求要件を満たしていない場合は、その後の評価は行わず、当該提案書を不合格とする。なお、性能評価点が 450 点を下回った場合は不合格とする。

３　必須以外の要件

評価する提案内容及び配点については、別添「提案書目次構成兼提案書総合評価基準表」のとおりとする。

評価	評価観点の重要度		
	Ａ	Ｂ	Ｃ
相対的に優れている	６０	４０	２０
相対的にやや優れている	４５	３０	１５
標準的である	３０	２０	１０
相対的にやや劣っている	１５	１０	５
相対的に劣っている	０	０	０

提案書目次構成　兼　提案書評価基準表

No			参照箇所	評価項目	評価観点	評価方法	評価対象	評価	
1	ー	1	提案書作成要領	仕様書に定める項目	提案書作成要領で示した記述項目及び記載内容を満たしていること。	必須要件	提案書	合格 又は 不合格	
1	ー	2	仕様書 提案書作成要領	仕様書に定める項目	仕様書の全ての要件を満たし、具体的な提案がなされており、それが確認できる資料の提示があること。	必須要件	提案書	合格 又は 不合格	
1	ー	3	見積書様式	仕様書に定める項目	見積書の様式及び記述項目を満たしていること。	必須要件	見積書	合格 又は 不合格	
2	ー	1	仕様書 ・1「件名」 ・2「目的」 仕様書別紙1_詳細編 ・第2章「案件概要」 第1節～第3節	全体概要	仕様書に記載されている目的を踏まえ、当行が求めている提供内容の全体像が具体的に提案されていること。	相対評価項目	提案書	B	40
2	ー	2	仕様書別紙1_詳細編 ・第2章「案件概要」 第4節	プロジェクト実施体制	各フェーズで円滑に開発を遂行できるチーム体制が提案されていること。 また、経験者、有資格者（または同等以上の能力を有する者）が主要メンバーとしてプロジェクトに参画しており、メンバーの経験・スキルを明確化した上で、適正な体制の提案がなされていること。 あわせて、LMシステムのベンダとの連携体制が明確に提案されていること。	相対評価項目	提案書	A	60
2	ー	3	仕様書別紙1_詳細編 ・第2章「案件概要」 第5節	スケジュール	システム構築スケジュールが工程ごとに明確になっており、各工程ごとの期間の根拠が明確に提案されていること。 スケジュールの実行性に関して、根拠を持って具体的に示していること。	相対評価項目	提案書	B	40
2	ー	4	仕様書別紙1_詳細編 ・第2章「案件概要」 第6節	開発拠点	開発拠点が明確になっていること。 また、それらの拠点が仕様書に記載されているセキュリティ要件を満たしていることが、根拠を持って具体的に示されていること。	相対評価項目	提案書	C	20
2	ー	5	仕様書別紙1_詳細編 ・第2章「案件概要」 第7節	プロジェクト管理	各フェーズで円滑に開発を遂行できる会議体が提案されていること。	相対評価項目	提案書	A	60
2	ー	6	仕様書別紙1_詳細編 ・第3章「委託概要」 第2節 「システム化の範囲」	実現方式(全体システム構成)	業務要件を達成するためのシステム構成の全体概要が、明確に提案されていること。また、システム構成の提案内容に対して根拠が明確に提示されていること。	相対評価項目	提案書	A	60
2	ー	7	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (1) 分析ツール機能要件	分析ツール(データ加工)	ユーザー自身でデータ加工が可能となっており、実現方法に関して、「表4.2.1 分析ツール機能要件(No1～6)」に即して明確に提案されていること。	相対評価項目	提案書	A	60
2	ー	8	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (1) 分析ツール機能要件	分析ツール(機能)	ユーザー自身で多変量解析や生存時間分析などの高度分析が実施可能となっており、実施可能な分析手法が「表4.2.1 分析ツール機能要件(No7～8)」に即して明確に提案されていること。 なお、目的達成に向けて、仕様書で提示していない有用な分析機能が提案されていた場合も評価の対象とする。	相対評価項目	提案書	A	60
2	ー	9	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (1) 分析ツール機能要件	分析ツール(ユーザビリティ)	ユーザビリティに関して、「表4.2.1 分析ツール機能要件(No9)」に即して明確に提案されており、容易な操作で実施可能な内容となっていること。	相対評価項目	提案書	B	40
2	ー	10	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (1) 分析ツール機能要件	分析ツール(互換性)	更改後システムとの互換性に関して、「表4.2.1 分析ツール機能要件(No10)」に即して明確に提案されていること。	相対評価項目	提案書	A	60
2	ー	11	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (2) 施策管理ツール機能要件	施策管理ツール(施策管理)	イベントの定義や施策対象顧客の管理、シナリオの管理、ユーザ管理等、施策管理ツールを運用する上で必要な管理機能について「表4.2.2 施策管理ツール機能要件(No1～16)」に則して明確に提案されていること。	相対評価項目	提案書	A	60
2	ー	12	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (2) 施策管理ツール機能要件	施策管理ツール(施策実行)	定義されたイベントの実行や抽出条件、除外条件について、「表4.2.2 施策管理ツール機能要件(No17～24)に則して施策を実行する手法が明確に提案されていること。	相対評価項目	提案書	A	60
2	ー	13	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (2) 施策管理ツール機能要件	施策管理ツール(施策の検証)	実行した施策について、検証するためのコントロールグループ設定や対象者のリストを確認できる機能を有し、「表4.2.2 施策管理ツール機能要件(No25～26)」に則して明確に提案されていること。	相対評価項目	提案書	B	40
2	ー	14	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (2) 施策管理ツール機能要件	施策管理ツール(ユーザビリティ)	ユーザビリティに関して、「表4.2.2 施策管理ツール機能要件(No27)」に即して明確に提案されており、容易な操作で実施可能な内容となっていること。	相対評価項目	提案書	B	40
2	ー	15	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (2) 施策管理ツール機能要件	施策管理ツール(他システムIF)	LMシステム経由で配信する各チャネルとのインターフェース(IF)が「表4.2.2 施策管理ツール機能要件(チャネルNo1)」に即して具体的に提案されており、LMシステムへの影響が最小限となる内容となっていること。	相対評価項目	提案書	A	60
2	ー	16	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (2) 施策管理ツール機能要件	施策管理ツール(新規チャネルの追加)	将来的な機能拡張に向けた実現方式が「表4.2.2 施策管理ツール機能要件(チャネルNo2)」に即して具体的に提案されていること。また、LMシステムや更改後PDCAツールへの影響が最小限となる提案になっていること。	相対評価項目	提案書	B	40
2	ー	17	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (2) 施策管理ツール機能要件	施策管理ツール(データマートの作成)	施策管理に必要な以下の情報をLMシステム内にテーブルを作成する実現方式が「表4.2.2 施策管理ツール機能要件(マスタNo1)」に即して具体的に提案されており、、LMシステムへの影響が最小限となる内容となっていること。	相対評価項目	提案書	A	60
2	ー	18	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 1 システム要件 (3) 拡張性機能要件	拡張性	将来的な機能拡張に向けた実現方式が「表4.2.3 拡張性機能要件」に即して具体的に提案されていること。また、LMシステムや更改後PDCAツールへの影響が最小限となる提案になっていること。	相対評価項目	提案書	A	60
2	ー	19	仕様書別紙1_詳細編 ・第4章「機能要件」 第2節 「機能要件」 2 運用・保守委託要件 仕様書別紙1_詳細編 ・第5章「作業概要」 第3節 「保守・運用・利用フェーズ」	運用・保守	安定したサービス提供を実現するために、運用保守の体制・対応内容が明確になっていること。さらに、スムーズに更改後のシステムへ移行できるよう、研修内容が具体的に提案されていること。	相対評価項目	提案書	A	60

No			参照箇所	評価項目	評価観点	評価方法	評価対象	評価	
2	ー	20	仕様書別紙1_詳細編 ・第4章「機能要件」 第3節 「非機能要件」 1 非機能要件 (2)規模・性能要件	規模・性能	仕様書別紙1_詳細編で提示する要件を満たすHWに関して、以下の内容が根拠とともに明確に提案されていること。 ・必要なHWスペック、台数 ・運用方法 ※提案内容の充実に加え、必要なHWリソースが少ないほど、より高評価とする	相対評価項目	提案書	A	60
2	ー	21	仕様書別紙1_詳細編 ・第4章「機能要件」 第3節 「非機能要件」 1 非機能要件 (3)可用性・信頼性要件	可用性	仕様書別紙1_詳細編で提示する要件に提示されている、可用性・信頼性が担保できるよう、システム構成や処理方式等、具体的かつ実現性のある提案がされていること。	相対評価項目	提案書	B	40
2	ー	22	仕様書別紙1_詳細編 ・第4章「機能要件」 第3節 「非機能要件」 2 セキュリティ要件	セキュリティ要件	以下の内容について根拠とともに明確に提案されていること。 ・サーバのウィルス対策、暗号化 ※今回導入するソフトウェアとウィルスバスターが双方に対して影響を及ぼさないこと ・アクセス権限の管理機能 ・監査ログの管理機能 また、その他の観点についても、対応を行うことが根拠とともに明確に提案されていること。	相対評価項目	提案書	A	60
2	ー	23	仕様書別紙1_詳細編 ・第5章「作業概要」 第1節 「開発フェーズ」	作業分界点	受託者、主管担当及びLMシステムベンダ間の責任分界点及び、構築作業分界点(作業内容)を、明確に提案していること。また、分界点が妥当であること。	相対評価項目	提案書	B	40
2	ー	24	仕様書別紙1_詳細編 ・第5章「作業概要」 第2節 「移行フェーズ」	データセット移行	現行業務が継続できるよう、データセットの移行について具体的に提案されていること。	相対評価項目	提案書	A	60
2	ー	25	仕様書別紙1_詳細編 ・第5章「作業概要」 第2節 「移行フェーズ」	資産移行	現行業務が継続できるよう、各種資産の移行について具体的に提案されていること。	相対評価項目	提案書	A	60
2	ー	26	仕様書別紙1_詳細編 ・第5章「作業概要」 第3節 「保守・運用・利用フェーズ」	ツール操作研修及び引継ぎ実施 マニュアルの充足性	移行に係る、システム運行担当者と業務担当者への編集内容が具体的に提案されており、有用な内容となっていること。 また、充実したマニュアルの提供があることが明確に示されていること。	相対評価項目	提案書	A	60
2	ー	27	仕様書別紙1_詳細編 ・第6章「その他」 第1節 「その他留意事項」	データ保護	「別紙2 情報保護・管理要領」に対応することが明確に示されていること。	相対評価項目	提案書	C	20
2	ー	28	仕様書別紙1_詳細編 ・第6章「その他」 第1節 「その他留意事項」	コンテンジェンシープラン 協力義務 監査	コンテンジェンシープラン:受託業務の継続を阻害するリスクに備えた業務継続計画について、具体的な提案がされていること。 協力義務:開発中及びサービス開始後も必要に応じて関連システム受託ベンダと円滑な調整及び協力を実施するための、具体的な提案がされていること。 監査:当行からの監査対応の求めに応じた円滑かつ確実な対応を実現するための、具体的な提案がされていること。	相対評価項目	提案書	B	40
2	ー	29	仕様書別紙1_詳細編 ・第6章「その他」 第3節 「受託者に求める要件」	導入実績	類似システムの導入実績について、本プロジェクトに有益かつ十分な実績があること。	相対評価項目	提案書	A	60
2	ー	30	その他	更なる改善提案	本プロジェクトにおいて仕様書に記載していない更なる改善内容が提案されており、具体的かつ実現性があること。	相対評価項目	提案書	C	20
								合計(満点)	1500

	診断実施企業の条件
1	自社の脆弱性診断サービスが、経済産業省が定める「情報セキュリティサービス基準」に適合するサービスとして、独立行政法人情報処理推進機構（IPA）の「情報セキュリティサービス基準適合サービスリスト」に登録されていること。 なお、受託期間中も登録されていること。
2	過去３年間で当行以外の異なる３銀行に対するセキュリティ診断の実績を３件以上有すること。
3	セキュリティ診断サービス提供年数を３年以上有すること。
4	セキュリティ診断作業実施者は脆弱性診断に関する業務経験を３年以上有すること。
5	セキュリティ診断作業実施者には以下の資格のいずれかを保有している者が１名以上含まれること。 ・情報システムセキュリティプロフェッショナル認定資格（CISSP） ・情報処理安全確保支援士 ・もしくは、上記資格と同等の知識・技術を保有していること。
6	セキュリティ診断管理責任者は、プロジェクト管理経験を５年以上有すること。 （管理責任者の前職において経験がある場合は、それを含めた経験年数としてよい。）
7	セキュリティ診断員が１０名以上在籍していること。
8	仕様書記載のセキュリティ診断項目を全て網羅したセキュリティ診断をツール及び手動により実施できること。
9	情報保護資格（「プライバシーマーク」または「ISO27001」）を取得していること。
10	社内で情報（取引先情報を含む）管理に関するルールが定められ、社員に対する指導も十分に行われていること。その上で仕様書において当行が提示する機密保持項目を遵守すること。

セキュリティ診断実施内容

1　診断方法

(1) 委託事業者は診断等実施に際し、ツールによる自動的・画一的な診断に加え、作業実施者の手動による診断やペネトレーションテストなどを実施し、それぞれについて報告を行うこと。

(2) 委託事業者による診断は、項番 3 に示す診断項目を満たすこと。項番 3 を満たすことができない場合は、主管部と委託事業者間で相談すること。また、委託事業者は診断前にはシステムが提供する機能や目的等を主管部に確認し、以下のセキュリティ検証標準等も参考に、システムの特性に沿った診断を行うこと。

【参考】セキュリティ検証標準

① Web アプリケーション診断

OWASP アプリケーションセキュリティ検証標準（ASVS）

セキュリティ検証レベル	説明	例
ASVS レベル 1	全てのアプリケーションが満たすべきものです。	一般的なご案内のみ閲覧可能な web サイト
ASVS レベル 2	機微なデータを扱うアプリケーションが満たすべきものです。	個人情報が閲覧可能な web サイト
ASVS レベル 3	極めて重要なアプリケーションが満たすべきものです。高額取引を行うアプリケーション、機密性の高い医療データを持つアプリケーション、最高レベルの信頼性を必要とするアプリケーションのためのものです。	個人情報の閲覧に加え、資金移動や原簿の更新が可能な web サイト

② スマートフォンアプリケーション診断

OWASP モバイルアプリケーションセキュリティ検証標準(MASVS)

検証レベル	説明	例
MASVS-L1	一般的なセキュリティ要件であり、すべてのモバイルアプリに推奨されます。	一般的なご案内のみ閲覧可能なアプリ
MASVS-L2	機密性の高いデータを扱うモバイルアプリに適用します。	モバイルバンキングアプリ
MASVS-R（※）	追加の保護コントロールを対象としています。クライアント側の脅威を防止することが設計の目標である場合に適用できます。	オンラインゲームアプリ

※　アプリの特性により、MASVS-L1 や MASVS-L2 に追加（MASVS-L1+R、MASVS-L2+R）で求めるもの

(3) 委託事業者が診断にツールを使用する場合は、名称および使用目的を事前に開示すること。

(4) 原則、本番環境に対して診断を実施すること。ただし、システム停止等、サービスに影響がある場合などは、本番環境と同等の開発環境または災害対策環境で実施するため、診断環境については、主管部と委託事業者間で調整のうえ実施すること。

2　各種診断

(1) ネットワーク診断

ア　IP アドレスまたは FQDN 単位で診断を実施すること。詳細は主管部より提示する。

イ　ロードバランサの背後に同一構成のサーバが複数ある場合は、同一構成のサーバのうち 1IP、または VIP(Virtual IP)のみ診断を実施すること。

ウ　グローバル IP に対しては、インターネット（リモート）から診断を実施すること。

【参考】診断対象 IP アドレスの考え方

①　インターネット接続システム

インターネットから接続可能なグローバル IP アドレスに対して実施すること。

②　社内イントラネット接続システム

他システムとの境界から到達できる範囲の IP アドレス、または業務端末から到達できる範囲の IP アドレスに対して実施すること。詳細は、主管部と委託事業者間で相談の上決定すること。

(2) Web アプリケーション診断

ア　動的画面を診断対象とすること。詳細は主管部と委託事業者間で調整すること。

イ　WebAPI については、すべての機能を診断対象とすること。

【参考】動的画面、静的画面の考え方

①　利用者が入力した値(検索キーワードやアカウント情報等)に応じてその後の処理が変化するような画面を動的画面という。

②　利用者が入力した値に応じて内容やその後の処理が変化することがなくサーバに用意されたコンテンツをそのまま表示するような画面を静的画面という。

(3) スマートフォンアプリケーション診断

ア　Android や iOS 向けなど異なる OS でアプリケーションを提供する場合、いずれのアプリケーションでも診断を実施すること。

イ　主管部が提供した実行ファイル（apk,ipa など）に対し、動的診断を実施すること。

ウ　主管部は root 化/jailbreak 検知機能を無効化した実行ファイル（apk,ipa など）を提供すること。

(4) ペネトレーションテスト

ア　原則、グローバル IP アドレスを対象にインターネット（リモート）から診断を実施すること。

イ　事前に実施した脆弱性診断で発見された脆弱性または主管部から提示された脆弱性診断結果の脆弱性なども参考に、侵入の可能性と侵入された場合の影響に関するテストを実施すること。

ウ　大量ログイン試行（ブルートフォース攻撃、リバースブルートフォース攻撃、リスト型攻撃、パスワードスプレー攻撃）への耐性を確認すること。

エ　テスト実施中に、当初予定した IP アドレス以外への検証・診断が可能な際は、主管部と委託事業者間で調整のうえ、最大限診断を実施すること。

3　診断項目

(1) ネットワーク診断

項番		診断項目
ネットワーク調査		
	1	ポートスキャン（TCP 0-65535/UDP well-known port）
	2	不要と思われるサービスの稼動
各種サービスの脆弱性調査		
	3	稼動中のサービスからの情報取得（バナー情報取得等）
	4	OS やアプリケーションソフトウェアの既知の脆弱性
	5	脆弱なパスワード設定の存在
	6	各種サービス（FTP サービス、SSH サービス等）の既知の脆弱性
	7	サービス妨害の可能性
	8	SSL/TLS 暗号強度調査
DNS 調査		
	9	DNS ゾーン転送の可否
	10	DNS 再帰的問い合わせの可否
	11	DNS ダイナミックアップデートの可否
SMTP 等調査		
	12	メール不正中継の可否
	13	メールサーバによるユーザ情報漏洩問題
HTTP/HTTPS 調査		
	14	脆弱性の知られている CGI スクリプトの存在
	15	不適切な SSL 証明書の利用

(2) Web アプリケーション診断

項番		診断項目
Web サーバ		
	1	Web サーバ上のデフォルトコンテンツの存在
	2	ディレクトリ一覧、不要なファイルの存在
	3	バックアップファイルとデバッグオプション
	4	サーバなどの設定不備や既知の脆弱性
認証・認可		
	5	脆弱なパスワード設定の存在
	6	強制ブラウジング
	7	脆弱なパスワード
	8	認証・認可回避
	9	アカウントロックの設定

項番		診断項目
入力		
	10	OS コマンドインジェクション
	11	SQL インジェクション
	12	LDAP インジェクション
	13	XPath インジェクション
	14	バッファオーバーフロー
	15	HTTP レスポンス分割
	16	メタキャラクタインジェクション
	17	ディレクトリ・トラバーサル
セッション		
	18	Cookie の Secure 属性と HttpOnly 属性
	19	セッションハイジャック
	20	セッションリプレイ
	21	セッションフィクセーション
	22	セッション ID の推測
	23	セッション ID の HTTP/HTTPS の使い分け
	24	セッション ID の格納方法
	25	セッション ID の有効期限
	26	セッション ID の破棄方法
	27	クロスサイトリクエストフォージェリ
出力		
	28	クロスサイトスクリプティング
	29	エラーコード
	30	不要なコメント
通信		
	31	HTTPS の適用漏れ
サイトデザイン		
	32	エラーメッセージによる情報漏えい
	33	パラメータの操作（改ざん操作）
	34	Web 画面設計上の不備 （例） ・ログイン画面はあるがログアウト機能が無い。 ・ログイン画面にパスワード入力フォームが無い。 ・本来ブラウザのアドレスバー（URL）に非表示にすべき ID、パスワード等の重要情報が表示されている。
	35	サーバサイドリクエストフォージェリ
	36	Cookie、 WebStorage の不適切な利用

(3) スマートフォンアプリケーション診断（端末環境）

項番		診断項目
アプリケーション間連携		
	1	アクセス制限
	2	情報の送受信
通信		
	3	プロトコル
	4	暗号化の有無
	5	サーバ証明書検証
	6	通信内容
	7	プライバシーの保護
認証		
	8	認証機能
	9	連携機能
	10	ログアウト機能
端末内のデータの取扱		
	11	保存場所
	12	アクセス権限
	13	保存方法
	14	保存期間
アプリケーションファイル・ログ		
	15	不要な情報の有無
	16	不要な情報の出力有無
機能の利用		
	17	パーミッション設定

(4) ペネトレーションテスト

項番	診断項目
1	脆弱性の調査
2	設定不備等の調査
3	取得可能情報の調査
4	不正なログインの可否検証(※)
5	権限昇格の可否検証
6	データへのアクセスの可否検証（DB アクセスの実現、通信データの盗聴、データの改ざん）
7	データ持ち出しの可否検証（外部向け通信の実現、データ持ち出しの実現）
8	不正行為の可否検証（不正な取引の実行）

（※）項番 1～3 で得られた情報を利用するものおよび大量ログイン試行（ブルートフォース攻撃、リバースブルートフォース攻撃、リスト型攻撃、パスワードスプレー攻撃）への耐性検証

サイバーセキュリティ対策実施報告書・証明書

▼ 提出対象にチェックを記載

	①	脆弱性診断実施報告書（ネットワーク診断）
	②	脆弱性診断実施報告書（Webアプリケーション診断）
	③	脆弱性診断実施報告書（スマートフォンアプリケーション診断）
	④	脆弱性診断実施証明書
	⑤	ペネトレーションテスト実施報告書
	⑥	ペネトレーションテスト実施証明書
	⑦	ＦＷ設定検証実施報告書
	⑧	ＦＷ設定検証実施証明書
	⑨	セキュリティパッチ管理作業実施報告書
	⑩	セキュリティパッチ管理作業実施証明書
	⑪	コンピュータウイルス対策ソフトの管理作業実施報告書
	⑫	コンピュータウイルス対策ソフトの管理作業実施証明書
	⑬	EOL管理作業実施報告書
	⑭	EOL管理作業実施証明書

株式会社ゆうちょ銀行　御中

脆弱性診断実施報告書（ネットワーク診断）

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、以下のとおり、ネットワーク診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　：***(診断事業者の会社名を記載)***
- 診断実施日　：***(ネットワーク診断の実施日をそれぞれ記載)***
- 診断実施環境　：***(本番／開発／ステージング／テスト用など、環境の種類を記載)***
- 診断範囲　：***(診断を実施したサーバ等を記載)***

【診断結果情報】

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	件	
	危険度：高	件	
	危険度：中	件	
	危険度：低	件	
危険度ごとの対応方針・対応予定時期等	危険度：緊急		
	危険度：高		
	危険度：中		
	危険度：低		

【診断実施内容】

確認項目	回答欄	備考
IPアドレス単位で診断を実施している。		
当該システムがインターネットに接続している場合、インターネットから接続可能なグローバルIPアドレスに対して、リモート（インターネット）から診断を実施している。		
他システムとの境界から到達できる範囲のIPアドレス又は、業務端末から到達できる範囲のIPアドレスに対して診断を実施している。		
ネットワーク診断で使用したツール等		

【取得している認証等】

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証		
その他（　　）		

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

脆弱性診断実施報告書（ネットワーク診断）

弊社は、「***システム***」を提供するにあたり、以下のとおり、ネットワーク診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　　：***株式会社*****
- 診断実施日　　：***20**年**月**日、**日***
- 診断実施環境　：***本番環境***
- 診断範囲　　：***サーバ（1IP）、**サーバ（1IP）***

【診断結果情報】

検出件数を記載

危険度をCVSS値に依らず評価している場合に記入

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	*1件*	***【評価方法】 危険度は、以下の方法にて評価を実施。 ・～～～（評価方法を記載）***
	危険度：高	*0件*	
	危険度：中	*2件*	
	危険度：低	*0件*	
危険度ごとの対応方針・対応予定時期等 検出事項、対応方針の詳細を確認できる資料を添付（提示が可能な場合）	危険度：緊急	*20**年*月*日*	***緊急：ソフトウェアアップデートを実施 中①：ソフトウェアアップデートを実施 中②：機能の無効化を実施 検出事項の詳細は別添「****」を参照***
	危険度：高		
	危険度：中	*20**年*月*日*	
	危険度：低		

【診断実施内容】

実施している場合は"○"
未実施の場合は"×"を記載し、備考欄に理由を記載

確認項目	回答欄	備考
IPアドレス単位で診断を実施している。	○	
当該システムがインターネットに接続している場合、インターネットから接続可能なグローバルIPアドレスに対して、リモート（インターネット）から診断を実施している。	○	
他システムとの境界から到達できる範囲のIPアドレス又は、業務端末から到達できる範囲のIPアドレスに対して診断を実施している。	○	
ネットワーク診断で使用したツール等 ***Nessus *.*.*(plugin-set ***)*** ***Nmap *.**** ***手動診断***		

開示可能な範囲で記載
非開示の場合は、その理由を記載

【取得している認証等】

取得している認証等がある場合は"○"
ない場合は空欄

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証	○	
その他（　　）		

その他、ネットワーク診断の実施を証明する認証等があれば、具体的に記載

〇〇〇〇年〇〇月〇〇日
会社名：株式会社〇〇〇〇
所在地：東京都～
氏名：〇〇　〇〇

株式会社ゆうちょ銀行　御中

脆弱性診断実施報告書（Webアプリケーション診断）

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、以下のとおり、Webアプリケーション診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】

・診断実施者　　：***(診断事業者の会社名を記載)***
・診断実施日　　：***(Webアプリケーション診断の実施日をそれぞれ記載)***
・診断実施環境　：***(本番／開発／ステージング／テスト用など、環境の種類を記載)***
・診断範囲　　：***(お客さま用公開画面／システム管理用画面等の実施した範囲を記載)***

【診断結果情報】

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	件	
	危険度：高	件	
	危険度：中	件	
	危険度：低	件	
危険度ごとの対応方針・対応予定時期等	危険度：緊急		
	危険度：高		
	危険度：中		
	危険度：低		

【診断実施内容】

確認項目	回答欄	備考
貴行に提供するWebアプリケーションの動的画面は、すべて診断対象としている。		
貴行に提供するWebAPI機能は、すべて診断対象としている。		
Webアプリケーション診断で使用したツール等		

【取得している認証等】

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証		
その他（　　）		

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

脆弱性診断実施報告書（Webアプリケーション診断）

弊社は、「***システム***」を提供するにあたり、以下のとおり、Webアプリケーション診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　　：***株式会社*****
- 診断実施日　　：***20**年**月**日、**日***
- 診断実施環境　：***本番環境***
- 診断範囲　　：***お客さま用公開画面、システム管理用画面***

【診断結果情報】

検出件数を記載

危険度をCVSS値に依らず評価している場合に記入

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	*1件*	***【評価方法】 危険度は、以下の方法にて評価を実施。 ・～～～（評価方法を記載）***
	危険度：高	*0件*	
	危険度：中	*2件*	
	危険度：低	*0件*	
危険度ごとの対応方針・対応予定時期等	危険度：緊急	*20**年*月*日*	***緊急：入力文字列のエスケープ処理を実装 中　：ソフトウェアアップデートを実施 検出事項の詳細は別添「****」を参照***
	危険度：高		
	危険度：中	*20**年*月*日*	
	危険度：低		

検出事項、対応方針の詳細を確認できる資料を添付（提示が可能な場合）

【診断実施内容】

実施している場合は"○"
未実施の場合は"×"を記載し、備考欄に理由を記載

確認項目	回答欄	備考
貴行に提供するWebアプリケーションの動的画面は、すべて診断対象としている。	○	
貴行に提供するWebAPI機能は、すべて診断対象としている。	○	
Webアプリケーション診断で使用したツール等		
Burp Suite*.*.* 手動診断		

開示可能な範囲で記載
非開示の場合は、その理由を記載

【取得している認証等】

取得している認証等がある場合は"○"
ない場合は空欄

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証	○	
その他（　　）		

その他、Webアプリケーション診断の実施を証明する認証等があれば、具体的に記載

〇〇〇〇年〇〇月〇〇日
会社名：株式会社〇〇〇〇
所在地：東京都～
氏名：〇〇　〇〇

株式会社ゆうちょ銀行　御中

脆弱性診断実施報告書（スマートフォンアプリケーション診断）

弊社は、「(※契約名、またはサービス名)」を提供するにあたり、以下のとおり、スマートフォンアプリケーション診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
・診断実施者　　：***(診断事業者の会社名を記載)***
・診断実施日　　：***(スマートフォンアプリケーション診断の実施日をそれぞれ記載)***
・診断実施環境　：***(本番／開発／ステージング／テスト用など、環境の種類を記載)***
・診断範囲　　：***(診断を実施したアプリケーション等を記載)***

【診断結果情報】

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	件	
	危険度：高	件	
	危険度：中	件	
	危険度：低	件	
危険度ごとの対応方針・対応予定時期等	危険度：緊急		
	危険度：高		
	危険度：中		
	危険度：低		

【診断実施内容】

確認項目	回答欄	備考
Android やiOS 向けなど異なるOS でアプリケーションを提供する場合、すべてのアプリケーションに対して診断を実施している。		
貴行が提供した実行ファイル（apk,ipa など）に対し、動的診断を実施している。		
スマートフォンアプリケーション診断で使用したツール等		

【取得している認証等】

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証		
その他（　　）		

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

脆弱性診断実施報告書（スマートフォンアプリケーション診断）

弊社は、「***システム***」を提供するにあたり、以下のとおり、スマートフォンアプリケーション診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　　：***株式会社****
- 診断実施日　　：*20**年**月**日、**日*
- 診断実施環境　：***本番環境***
- 診断範囲　　：***アプリ（Android, iOS)***

【診断結果情報】

検出件数を記載

危険度をCVSS値に依らず評価している場合に記入

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	*1件*	***【評価方法】*** ***危険度は、以下の方法にて評価を実施。*** ***・～～～（評価方法を記載）***
	危険度：高	*0件*	
	危険度：中	*2件*	
	危険度：低	*0件*	
危険度ごとの対応方針・対応予定時期等	危険度：緊急	*20**年*月*日*	***緊急：ソフトウェアアップデートを実施*** ***中　：ソフトウェアアップデートを実施***
	危険度：高		***検出事項の詳細は別添「****」を参照***
	危険度：中	*20**年*月*日*	
	危険度：低		

検出事項、対応方針の詳細を確認できる資料を添付（提示が可能な場合）

【診断実施内容】

実施している場合は"○"
未実施の場合は"×"を記載し、備考欄に理由を記載

確認項目	回答欄	備考
Android やiOS 向けなど異なるOS でアプリケーションを提供する場合、すべてのアプリケーションに対して診断を実施している。	○	
貴行が提供した実行ファイル（apk, ipa など）に対し、動的診断を実施している。	○	
スマートフォンアプリケーション診断で使用したツール等		
Secure Coding Checker*.*.* 手動診断		

開示可能な範囲で記載
非開示の場合は、その理由を記載

【取得している認証等】

取得している認証等がある場合は"○"
ない場合は空欄

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証	○	
その他（　　）		

その他、スマートフォンアプリケーション診断の実施を証明する認証等があれば、具体的に記載

○○○○年○○月○○日
会社名：株式会社○○○○
所在地：東京都～
氏名：○○　○○

株式会社ゆうちょ銀行　御中

脆弱性診断実施証明書

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、下記のとおり脆弱性診断を実施し、適切に対応していることを証明いたします。

【実施内容】

・ネットワーク診断について、以下の作業を実施。

①***（※頻度を記入）***でネットワーク診断を実施している。

②発見された脆弱性は、危険度に応じた対処を適切に実施している。

・Ｗｅｂアプリケーション診断について、以下の作業を実施。

①***（※頻度を記入）***でＷｅｂアプリケーション診断を実施している。

②発見された脆弱性は、危険度に応じた対処を適切に実施している。

・スマートフォンアプリケーション診断について、以下の作業を実施。

①***（※頻度を記入）***でスマートフォンアプリケーション診断を実施している。

②発見された脆弱性は、危険度に応じた対処を適切に実施している。

〇〇〇〇年〇〇月〇〇日

会社名：***(委託事業者の会社名を記載)***

所在地：***(委託事業者の所在地を記載)***

氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

脆弱性診断実施証明書

弊社は、「*******システム***」を提供するにあたり、下記のとおり脆弱性診断を実施し、適切に対応していることを証明いたします。

【実施内容】

・ネットワーク診断について、以下の作業を実施。

①***四半期毎に***ネットワーク診断を実施している。

②発見された脆弱性は、危険度に応じた対処を適切に実施している。

・Ｗｅｂアプリケーション診断について、以下の作業を実施。

①***年次***でＷｅｂアプリケーション診断を実施している。

②発見された脆弱性は、危険度に応じた対処を適切に実施している。

実施頻度を記載

実施頻度を記載

実施していない診断は削除
（記載例では、スマートフォンアプリケーション診断を削除している）

〇〇〇〇年〇〇月〇〇日
会社名：株式会社〇〇〇〇
所在地：東京都～
氏名：〇〇　〇〇

株式会社ゆうちょ銀行　御中

ペネトレーションテスト実施報告書

弊社は、「(***※契約名、またはサービス名)***」を提供するにあたり、以下のとおり、ペネトレーションテストを実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　　：***(ペネトレーションテスト事業者の会社名を記載)***
- 診断実施日　　：***(ペネトレーションテストの実施日をそれぞれ記載)***
- 診断実施環境　：***(本番／開発／ステージング／テスト用など、環境の種類を記載)***
- 診断範囲　　：***(お客さま用公開画面／システム管理用画面等の実施した範囲を記載)***

【診断結果情報】

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	件	
	危険度：高	件	
	危険度：中	件	
	危険度：低	件	
危険度ごとの対応方針・対応予定時期等	危険度：緊急		
	危険度：高		
	危険度：中		
	危険度：低		

【診断実施内容】

確認項目		回答欄	備考
以下の項目を含むペネトレーションテストを実施			
事前に実施した脆弱性診断結果を用いた攻撃の試行			
大量ログイン試行攻撃（※）による権限奪取不正取引の可否			
大量ログイン試行攻撃（※）を抑止する機能(アカウントロック等)の有無			
※大量ログイン試行攻撃には、以下の4種を含めること ・ブルートフォース攻撃 ・リバースブルートフォース攻撃 ・リスト型攻撃 ・パスワードスプレー攻撃			
攻撃準備活動として実施			
(脆弱性の調査) 攻撃に利用可能なソフトウェアの脆弱性の調査			
(設定不備等の調査) 攻撃可能にする設定上の不備の調査			
(取得可能情報の調査) システム上に残存する攻撃のヒントになる情報、他所で入手可能な攻撃に使える情報の調査収集			
侵害可能性の検証として実施			
不正なログインの可否			
権限昇格の可否			
データへのアクセスの可否	DBアクセスの実現		
	通信データの盗聴		
	データの改ざん		
データ持ち出しの可否	外部向け通信の実現		
	データ持ち出しの実現		
不正行為の可否	不正な取引の実行		
その他（　　）			

【取得している認証等】

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証		
その他（　　）		

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

ペネトレーションテスト実施報告書

弊社は、「*******システム***」を提供するにあたり、以下のとおり、ペネトレーションテストを実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　　：***株式会社*******
- 診断実施日　　：***20**年**月**日、**日***
- 診断実施環境　：***本番環境***
- 診断範囲　　：*******（お客さま用公開画面）***

【診断結果情報】

検出件数を記載

危険度をCVSS値に依らず評価している場合に記入

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	*1件*	***【評価方法】 危険度は、以下の方法にて評価を実施。 ・～～～（評価方法を記載）***
	危険度：高	*0件*	
	危険度：中	*2件*	
	危険度：低	*0件*	
危険度ごとの対応方針・対応予定時期等 検出事項、対応方針の詳細を確認できる資料を添付（提示が可能な場合）	危険度：緊急	*20**年*月*日*	***緊急：ソフトウェアアップデートを実施 中①：ソフトウェアアップデートを実施 中②：機能の無効化を実施 検出事項の詳細は別添「****」を参照***
	危険度：高		
	危険度：中	*20**年*月*日*	
	危険度：低		

【診断実施内容】

実施している場合は"○"
未実施の場合は"×"を記載し、備考欄に理由を記載

確認項目		回答欄	備考
以下の項目を含むペネトレーションテストを実施			
事前に実施した脆弱性診断結果を用いた攻撃の試行		○	
大量ログイン試行攻撃（※）による権限奪取不正取引の可否		○	
大量ログイン試行攻撃（※）を抑止する機能(アカウントロック等)の有無		○	
※大量ログイン試行攻撃には、以下の4種を含めること ・ブルートフォース攻撃 ・リバースブルートフォース攻撃 ・リスト型攻撃 ・パスワードスプレー攻撃			
攻撃準備活動として実施			
（脆弱性の調査） 攻撃に利用可能なソフトウェアの脆弱性の調査		○	
（設定不備等の調査） 攻撃可能にする設定上の不備の調査		○	
（取得可能情報の調査） システム上に残存する攻撃のヒントになる情報、他所で入手可能な攻撃に使える情報の調査収集		○	
侵害可能性の検証として実施			
不正なログインの可否		○	
権限昇格の可否		○	
データへのアクセスの可否	DBアクセスの実現	○	
	通信データの盗聴	○	
	データの改ざん	○	
データ持ち出しの可否	外部向け通信の実現	○	
	データ持ち出しの実現	○	
不正行為の可否	不正な取引の実行	○	
その他（　　）			

その他、ペネトレーションテストとして実施している項目がある場合は"○"を記入し、「その他（）」の（）内に具体的に記載ない場合は空欄

【取得している認証等】

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証	○	
その他（　　）		

取得している認証等がある場合は"○"
ない場合は空欄

ペネトレーションテストの実施を証明する認証等があれば、具体的に記載

○○○○年○○月○○日
会社名：株式会社○○○○
所在地：東京都～
氏名：○○　○○

株式会社ゆうちょ銀行　御中

ペネトレーションテスト実施証明書

弊社は、「***（※契約名、またはサービス名）***」を提供するにあたり、下記のとおりペネトレーションテストを実施し、適切に対応していることを証明いたします。

【実施内容】

・ペネトレーションテストについて、以下の作業を実施。

①***（※頻度を記入）***でペネトレーションテストを実施している。

②発見された脆弱性は、危険度に応じた対処を適切に実施している。

〇〇〇〇年〇〇月〇〇日
会社名：***（委託事業者の会社名を記載）***
所在地：***（委託事業者の所在地を記載）***
氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

ペネトレーションテスト実施証明書

　弊社は、「*******システム***」を提供するにあたり、下記のとおりペネトレーションテストを実施し、適切に対応していることを証明いたします。

【実施内容】

・ペネトレーションテストについて、以下の作業を実施。

実施頻度を記載

①***年次***でペネトレーションテストを実施している。

②発見された脆弱性は、危険度に応じた対処を適切に実施している。

〇〇〇〇年〇〇月〇〇日
会社名：株式会社〇〇〇〇
所在地：東京都～
氏名：〇〇　〇〇

株式会社ゆうちょ銀行　御中

ＦＷ設定検証実施報告書

弊社は、「(***※契約名、またはサービス名)***」を提供するにあたり、以下のとおり、サービス利用時に経由する通信経路上にあるＦＷについて設計書通りに設定されていることを確認し、発見された不備等を修正する等適切に対応していることを報告いたします。

【検証実施情報】

・検証実施者　　：***(検証実施事業者の会社名を記載)***

・対象期間　　：　　年度　□年次

□第一四半期　□第二四半期　□第三四半期　□第四四半期

□その他（　　）

・検証実施日　　：***(検証実施日を記載)***

【検証結果情報】

回答欄		備考
【結果】 不備無し・不備有り・非開示 【原因】 【対処状況】		

【取得している認証等】

回答欄		備考

〇〇〇〇年〇〇月〇〇日

会社名：***(委託事業者の会社名を記載)***

所在地：***(委託事業者の所在地を記載)***

氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

ＦＷ設定検

以下の検証頻度に応じて、チェックボックスに記入
・1回／四半期　：年度分、該当する四半期に✔
・1回／半期　：年度分、該当する期間に✔
→上半期の場合、第一四半期・第二四半期に✔
→下半期の場合、第三四半期・第四四半期に✔
・1回／年の場合　：年度分に✔
・上記以外　：その他に✔、チェックボックス右側（）内に具体的な対象期間を記載

弊社は、「***システム***」を提供するにあたり、以
ＦＷについて設計書通りに設定されていることを確認
とを報告いたします。

【検証実施情報】

・検証実施者　：***株式会社*****

・対象期間　：　2022 年度　☑年次
☐第一四半期　☐第二四半期　☐第三四半期　☐第四四半期
☐その他（　　）

対象期間の年度を記載

・検証実施日　：***2022年12月1日***

【検証結果情報】

回答欄		備考
【結果】 不備無し・不備有り・非開示 【原因】 【対処状況】		

ＦＷ設定値の不備の有無を選択
非開示の場合は非開示を選択

不備有りの場合、原因を記載

不備有りの場合、対処状況を記載

【取得している認証等】

回答欄		備考

ＦＷ設定検証の実施を証明する認証等がある場合は具体的に記載、
ない場合は空欄

〇〇〇〇年〇〇月〇〇日
会社名：株式会社〇〇〇〇
所在地：東京都～
氏名：〇〇　〇〇

株式会社ゆうちょ銀行　御中

ＦＷ設定検証実施証明書

弊社は、「***（※契約名、またはサービス名）***」を提供するにあたり、下記のとおりＦＷ設定検証を実施し、適切に対応していることを証明いたします。

【実施内容】

・ＦＷ設定検証について、以下の作業を実施。

①***（※頻度を記入）***でサービス利用時に経由する通信経路上にあるＦＷについて、設計書どおりに設定されていることを確認している。

②不備等が発見された場合、修正する等の対処を適切に実施している。

③（ＦＷ設定検証を定期的(年1回以上)に行っていない場合）
以下ア～ウの対応を実施している。

ア　初期構築時および変更時にFWの設定値と設計書等を突合し、設定誤りがないことを確認している。
発見された設定誤りは、対処が完了している。

イ　FW設定作業のプロセスを適切に管理している。
（作業端末や作業用IDの管理・設定内容の確認等ルールを整備している。）

ウ　ＦＷ、ＷＡＦ、ＩＰＳ・ＩＤＳ等により、脆弱性を狙った攻撃に関する検知、防御態勢を整備している。

〇〇〇〇年〇〇月〇〇日
会社名：***（委託事業者の会社名を記載）***
所在地：***（委託事業者の所在地を記載）***
氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

ＦＷ設定検証実施証明書

弊社は、「*******システム***」を提供するにあたり、下記のとおりＦＷ設定検証を実施し、適切に対応していることを証明いたします。

【実施内容】

・ＦＷ設定検証について、以下の作業を実施。

実施頻度を記載

①***年次***でサービス利用時に経由する通信経路上にあるＦＷについて、設計書どおりに設定されていることを確認している。

②不備等が発見された場合、修正する等の対処を適切に実施している。

③は、定期的(年1回以上)にFW検証を行っている場合、削除

〇〇〇〇年〇〇月〇〇日
会社名：株式会社〇〇〇〇
所在地：東京都～
氏名：〇〇　〇〇

株式会社ゆうちょ銀行　御中

セキュリティパッチ管理作業実施報告書

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、下記のとおりセキュリティパッチ管理作業を実施しましたので、実施結果を報告します。

【実施内容】

セキュリティパッチ管理について以下を確認。

①脆弱性情報、セキュリティパッチ情報に関して　　で収集していること。

②取得した情報については影響調査を実施し、対応が必要と判断したものについては漏れなく対応を実施していること。

【実施期間】

〇〇〇〇年〇〇月〇〇日　～　〇〇〇〇年〇〇月〇〇日

【実施結果】

上記①②について、問題ないことを確認。

〇〇〇〇年〇〇月〇〇日

会社名：***(委託事業者の会社名を記載)***

所在地：***(委託事業者の所在地を記載)***

氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

セキュリティパッチ管理作業実施報告書

弊社は、「*******システム***」を提供するにあたり、下記のとおりセキュリティパッチ管理作業を実施しましたので、実施結果を報告します。

契約名またはサービス・システム名をご記入ください。

情報の収集頻度をプルダウンからお選びください。
該当する選択肢がない場合は、実態をご記入ください。

【実施内容】

セキュリティパッチ管理について以下を確認。

①脆弱性情報、セキュリティパッチ情報に関して　　随時　　で収集していること。

②取得した情報については影響調査を実施し、対応が必要と判断したものについては漏れなく対応を実施していること。

【実施期間】

2022年　4月　1日　～　2023年　3月　31日

確認の実施期間をご記入ください。

【実施結果】

上記①②について、問題ないことを確認。

〇〇〇〇年〇〇月〇〇日

会社名：***（委託事業者の会社名を記載）***

所在地：***（委託事業者の所在地を記載）***

氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

セキュリティパッチ管理作業実施証明書

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、下記のとおりセキュリティパッチ管理作業を実施し、セキュリティパッチ管理について適切に対応していることを証明いたします。

【実施内容】

セキュリティパッチ管理について以下を確認。

①脆弱性情報、セキュリティパッチ情報に関して　　で収集していること。

②取得した情報については影響調査を実施し、対応が必要と判断したものについては漏れなく対応を実施していること。

〇〇〇〇年〇〇月〇〇日

会社名：***(委託事業者の会社名を記載)***

所在地：***(委託事業者の所在地を記載)***

氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

セキュリティパッチ管理作業実施証明書

弊社は、「*******システム***」を提供するにあたり、下記のとおりセキュリティパッチ管理作業を実施し、セキュリティパッチ管理について適切に対応していることを証明いたします。

契約名またはサービス・システム名をご記入ください。

情報の収集頻度をプルダウンからお選びください。
該当する選択肢がない場合は、実態をご記入ください。

【実施内容】

セキュリティパッチ管理について以下を確認。

①脆弱性情報、セキュリティパッチ情報に関して　　随時　　で収集していること。

②取得した情報については影響調査を実施し、対応が必要と判断したものについては漏れなく対応を実施していること。

〇〇〇〇年〇〇月〇〇日

会社名：***（委託事業者の会社名を記載）***

所在地：***（委託事業者の所在地を記載）***

氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

コンピュータウイルス対策ソフトの管理作業実施報告書

弊社は、「***（※契約名、またはサービス名）***」を提供するにあたり、下記のとおりコンピュータウイルス対策ソフトの管理作業を実施しましたので、実施結果を報告します。

【実施内容】

コンピュータウイルス対策ソフトの管理について、以下の作業を実施。

①原則本サービスを構成するシステムに、コンピュータウイルス対策ソフトを導入する。

②***（※頻度を記入）***でパターンファイルのリリース情報を収集し、***（※自動／手動）***更新している。

③***（※頻度を記入）***でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを確認し、確認結果を管理台帳に記録し、管理している。

【実施結果】

上記①②③について、問題ないことを確認。

〇〇〇〇年〇〇月〇〇日
会社名：***（委託事業者の会社名を記載）***
所在地：***（委託事業者の所在地を記載）***
氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

コンピュータウイルス対策ソフトの管理作業実施報告書

弊社は、「*******システム***」を提供するにあたり、下記のとおりコンピュータウイルス対策ソフトの管理作業を実施しましたので、実施結果を報告します。

契約名またはサービス・システム名をご記入ください。

週次、随時等の頻度をご記入ください。

【実施内容】

コンピュータウイルス対策ソフトの管理について、以下の作業を実施。

①原則本サービスを構成するシステムに、コンピュータウイルス対策ソフトを導入する。

②***随時***でパターンファイルのリリース情報を収集し、***自動***更新している。

自動または手動かをご記入ください。

③***随時***でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを確認し、確認結果を管理台帳に記録し、管理している。

※③について、管理台帳による記録・管理に代わり、自動ツール等で更新状態を管理している場合は、実態にあわせて、適宜修正してください。
修正時には、管理台帳に代わり、コンピュータウイルス対策ソフト（本体、及びパターンファイル）の更新漏れを防止するための手段があることが分かるように記載をお願いします。
自動ツール等により更新漏れを防止している場合は、以下例のとおり記載。
《例1》日次でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを自動ツールで確認し、管理している。
《例2》随時、コンピュータウイルス対策ソフト（本体、及びパターンファイル）が自動更新に失敗した場合に通知されるメールを確認し、更新漏れが発生しない管理をしている。

【実施結果】

上記①②③について、問題ないことを確認。

〇〇〇〇年〇〇月〇〇日
会社名：***（委託事業者の会社名を記載）***
所在地：***（委託事業者の所在地を記載）***
氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

コンピュータウイルス対策ソフトの管理作業実施証明書

弊社は、「***（※契約名、またはサービス名）***」を提供するにあたり、下記のとおりコンピュータウイルス対策ソフトの管理作業を実施し、適切に対応していることを証明いたします。

【実施内容】

コンピュータウイルス対策ソフトの管理について、以下の作業を実施。

①原則本サービスを構成するシステムに、コンピュータウイルス対策ソフトを導入する。

②***（※頻度を記入）***でパターンファイルのリリース情報を収集し、***（※自動／手動）***更新している。

③***（※頻度を記入）***でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを確認し、確認結果を管理台帳に記録し、管理している。

〇〇〇〇年〇〇月〇〇日
会社名：***（委託事業者の会社名を記載）***
所在地：***（委託事業者の所在地を記載）***
氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

コンピュータウイルス対策ソフトの管理作業実施証明書

弊社は、「*******システム***」を提供するにあたり、下記のとおりコンピュータウイルス対策ソフトの管理作業を実施し、適切に対応していることを証明いたします。

契約名またはサービス・システム名をご記入ください。

【実施内容】

コンピュータウイルス対策ソフトの管理について、以下の作業を実施

①原則本サービスを構成するシステムに、コンピュータウイルス対策ソフトを導入する。

②***随時***でパターンファイルのリリース情報を収集し、***自動***更新している。

週次、随時等の頻度をご記入ください。

自動または手動かをご記入ください。

③***随時***でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを確認し、確認結果を管理台帳に記録し、管理している。

※③について、管理台帳による記録・管理に代わり、自動ツール等で更新状態を管理している場合は、実態にあわせて、適宜修正してください。
修正時には、管理台帳に代わり、コンピュータウイルス対策ソフト（本体、及びパターンファイル）の更新漏れを防止するための手段があることが分かるように記載をお願いします。
自動ツール等により更新漏れを防止している場合は、以下例のとおり記載。
《例1》日次でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを自動ツールで確認し、管理している。
《例2》随時、コンピュータウイルス対策ソフト（本体、及びパターンファイル）が自動更新に失敗した場合に通知されるメールを確認し、更新漏れが発生しない管理をしている。

〇〇〇〇年〇〇月〇〇日
会社名：***（委託事業者の会社名を記載）***
所在地：***（委託事業者の所在地を記載）***
氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

EOL管理作業実施報告書

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、下記のとおりEOL管理作業を実施しましたので、実施結果を報告します。

【実施内容】

EOL管理台帳について以下を確認。

①システムを構成している製品が漏れなく記載されていること。

②収集した最新のEOL情報が反映されていること。

③EOL期限切れの製品がある場合、継続使用によるリスクも考慮のうえ、社内基準に従い継続して利用できることの判断が責任者によりされていること。

【実施結果】

上記①②③について、問題ないことを確認。

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

EOL管理作業実施証明書

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、下記のとおりEOL管理作業を実施し、EOL管理について適切に対応していることを証明いたします。

【実施内容】

EOL管理台帳について以下を確認。

①システムを構成している製品が漏れなく記載されていること。

②収集した最新のEOL情報が反映されていること。

③EOL期限切れの製品がある場合、継続使用によるリスクも考慮のうえ、社内基準に従い継続して利用できることの判断が責任者によりされていること。

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

入力項目												
システムID	システム名	所管担当	端末種別	機器名	HW製品名	アンチウイルス導入有無	EDR導入有無	インターネット接続有無	OS有無	サービス利用状況	ホスト名	基準日

入力項目		
システムID_システム名	機器名	OS・SW製品名