令和６年度

中小企業サイバーセキュリティ

社内体制整備事業

第８編　具体的な構築・運用の実践　【レベル３】

第 8 編. 具体的な構築・運用の実践 【レベル 3】 2
第 20 章. セキュリティ機能の実装と運用（IT 環境構築・運用実施手順） 2
20-1. セキュリティ機能の実装と運用 3
20-1-1. デジタル・ガバメント推進標準ガイドラインの概要 3
20-1-2. プロジェクトの管理 10
20-1-3. 予算および執行 17
20-1-4. サービス・業務企画 27
20-1-5. 要件定義 32
20-1-6. 調達 40
20-1-7. 設計・開発 45
20-1-8. サービス・業務の運営と改善 54
20-1-9. 運用および保守 59
20-1-10. システム監査 67
20-2. アジャイル開発 72
20-2-1. アジャイル開発の概要 72
20-2-2. アジャイル開発の実施ポイント 73
引用文献 76
参考文献 77
用語集 80

第20章. セキュリティ機能の実装と運用（IT 環境構築・運用実施手順）

章の目的
第 20 章では、「デジタル・ガバメント推進標準ガイドライン」などが示すサービスシステム構築と運用の工程を参考に、中小企業においても適用することが有効な工程と、実践に当たっての留意点を理解することを目的とします。

主な達成目標
◘ 中小企業においても有効なシステム導入工程と、実践に当たっての留意点を理解すること ◘ システム導入工程に沿って、セキュリティ機能を実装・運用するためポイントを理解すること ◘ アジャイル開発の概要と実践ポイントを理解すること

20-1. セキュリティ機能の実装と運用

20-1-1. デジタル・ガバメント推進標準ガイドラインの概要

「デジタル社会推進標準ガイドライン群」は、政府向けに作成されており、政府情報システムの整備や管理に際して守るべき共通ルールが記載されています。しかし、システム導入の流れ自体は、政府だけでなく一般企業であっても参考にできます。ガイドラインを通してシステム導入の全体像を認識し、実践する際は必要に応じて取捨選択する形で留意点を把握することが効果的です。

本テキストでは、「デジタル社会推進標準ガイドライン群」におけるシステム導入工程の全体像を網羅的に記載しています。詳細については、ガイドライン本文を参照してください。

「デジタル社会推進標準ガイドライン群」の体系

デジタル社会推進標準ガイドライン群は、サービス・業務改革並びにこれらに伴う政府情報システムの整備および管理についての手続き・手順や、各種技術標準などに関する共通ルールや参考ドキュメントをまとめたものです。

各ドキュメントの位置づけには、次の 2 種類が存在します。

- Normative（標準ガイドライン）：政府情報システムの整備および管理に関するルールとして順守する内容を定めたドキュメント
- Informative（実践ガイドブック）：参考とするドキュメント

これまでは、「デジタル・ガバメント推進標準ガイドライン群」という名称で各種ガイドラインが策定されていました。しかし、デジタル庁として政府内部に加えて社会全体のデジタル化を推進するという観点から、これらのドキュメント体系の名称を「デジタル社会推進標準ガイドライン群」と変更しました。

主として政府内部の手続き・手順を定めたドキュメントについては、従来と同様に「デジタル・ガバメント」という名称を継続しています。

政府情報システム全般に関するドキュメント
DS-100 デジタル・ガバメント推進標準ガイドライン ドキュメントの位置づけ：Normative 概要：サービス・業務改革とそれに伴って利用する政府情報システムの整備および管理についての政府の共通ルールです。手続き・手順についての基本的な方針や政府の各組織における役割などが定められています。

DS-110 デジタル・ガバメント推進標準ガイドライン解説書

ドキュメントの位置づけ：Informative

概要：政府の基本ルールである標準ガイドラインについて解説などを記載した参考文書です。標準ガイドラインの記載内容に関して、趣旨や目的などを読者が理解しやすくするために利用されます。

DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック

ドキュメントの位置づけ：Informative

概要：標準ガイドライン、標準ガイドライン附属文書、標準ガイドライン解説書に記載された内容に対して知識や教訓などを盛り込んだ、より実践的な参考書です。

DS-121 アジャイル開発実践ガイドブック

ドキュメントの位置づけ：Informative

概要：アジャイル開発がどのようなものかを理解するために必要な、基本的な知識をまとめた文書です。従来の開発スタイルとは別の選択肢としてアジャイル開発を設けるにあたって作成されました。

DS-130 標準ガイドライン群用語集

ドキュメントの位置づけ：Informative

概要：標準ガイドラインの用語集です。

セキュリティに関するドキュメント

DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン

ドキュメントの位置づけ：Informative

概要：システムライフサイクルの各工程でのセキュリティ実施内容や要求事項を示し、関係者の役割を定義しています。

DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン～ベースラインと事業被害の組み合わせアプローチ～

ドキュメントの位置づけ：Informative

概要：DS-200「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」のセキュリティリスク分析手順の事例として具体的に示したものです。

DS-202 CI／CD パイプラインにおけるセキュリティの留意点に関する技術レポート

ドキュメントの位置づけ：Informative

概要：CI／CD（継続的インテグレーション/継続的デリバリ）パイプラインをセキュリティ観

点から解説し、保護策を検討する際のポイントについて説明しています。

DS-210 ゼロトラストアーキテクチャ適用方針

ドキュメントの位置づけ：Informative

概要：ゼロトラストアーキテクチャを適用するための基本方針と導入時の留意点について記載しています。

DS-211 常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）

ドキュメントの位置づけ：Informative

概要：ゼロトラストの環境下で政府全体のサイバーリスクを把握・低減する CRSA システムについて解説しています。

DS-212 ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート

ドキュメントの位置づけ：Informative

概要：アクセス制御モデルの 1 つであり、リソースに付与された属性や環境の情報などを活用した属性ベースアクセス制御に関する俯瞰的な技術的内容を記載しています。

DS-220 政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート

ドキュメントの位置づけ：Informative

概要： NIST サイバーセキュリティフレームワークについて解説し、政府情報システムに導入する上での要点を示しています。

DS-221 政府情報システムにおける脆弱性診断導入ガイドライン

ドキュメントの位置づけ：Informative

概要：脆弱性診断を効果的に導入するための基準およびガイダンスを記載しています。

DS-231 セキュリティ統制のカタログ化に関する技術レポート

ドキュメントの位置づけ：Informative

概要：セキュリティ統制のカタログ化（独立したセキュリティ管理策に対し一意な識別子を付与し、機械可読形式で分類すること）に関する概要について説明します。

クラウドサービスに関するドキュメント

DS-310 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針

ドキュメントの位置づけ：Normative

概要：政府情報システムのシステム方式について、クラウドサービスの採用を第一候補とし、適切に利用するための考え方などを示しています。

データ連携に関するドキュメント

DS-400 政府相互運用性フレームワーク（GIF）

ドキュメントの位置づけ：Informative

概要：GIF（Government Interoperability Framework）は、デジタル庁が公開するデータの連携・交換のためのデータ参照モデルです。

トラストに関するドキュメント

DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン

ドキュメントの位置づけ：Normative

概要：各種行政手続きをデジタル化する際に必要となる、オンラインによる本人確認の手法を示しています。

DS-531 処分通知等のデジタル化に係る基本的な考え方

ドキュメントの位置づけ：Informative

概要：処分通知などのデジタル化を短期的に推進するため、実務で参考にできるよう共通的な考え方や課題への対応方法などを提供します。

その他ドキュメント

DS-910 安全保障等の機微な情報等に係る政府情報システムの取扱い

ドキュメントの位置づけ：Normative

概要：安全保障などの機微な情報などを扱う情報システムについて、注意が必要とされるリスクとその対応策、クラウドサービス化の検討、データ連携における留意点など、利用者が検討すべき観点をまとめています。

詳細理解のため参考となる文献（参考文献）	
DS-100 デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf
DS-110 デジタル・ガバメント推進標準ガイドライン解説書	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9462b2d8/20240605_resources_standard_guidelines_guideline_03.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf
DS-121 アジャイル開発実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9fc931f7/20220422_resources_standard_guidelines_guidebook_01.pdf
DS-130 標準ガイドライン群用語集	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/83a1ac09/20230331_resources_standard_guidelines_glossary_03.pdf
DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf
DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン ～ベースラインと事業被害の組み合わせアプローチ～	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1b65a1dc/20230411_resources_standard_guidelines_guideline_01.pdf

DS-202 CI／CD パイプラインにおけるセキュリティの留意点に関する技術レポート	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/33f31336/20240329_resources_standard_guidelines_guideline_01.pdf
DS-210 ゼロトラストアーキテクチャ適用方針	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5efa5c3b/20220630_resources_standard_guidelines_guidelines_04.pdf
DS-211 常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/ef841b43/20240131_resources_standard_guidelines_guidelines_03.pdf
DS-212 ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/e5b49450/20230411_resources_standard_guidelines_guideline_03.pdf
DS-220 政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_05.pdf
DS-221 政府情報システムにおける脆弱性診断導入ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7fefc9ee/20240206_resources_standard_guidelines_guidelines_01.pdf
DS-231 セキュリティ統制のカタログ化に関する技術レポート	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9f746654/20230411_resources_standard_guidelines_guideline_07.pdf
DS-310 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5167e265/20230929_resources_standard_guidelines_guideline_01.pdf
DS-400 政府相互運用性フレームワーク（GIF）	https://github.com/JDA-DM/GIF
DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/f1be078e/20220422_resources_standard_guidelines_guideline_07.pdf
DS-531 処分通知等のデジタル化に係る基本的な考え方	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d92a1cf2/20230411_resources_standard_guidelines_guideline_09.pdf
DS-910 安全保障等の機微な情報等に係る政府情報システムの取扱い	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/4d3bf58a/20230719_resources_standard_guidelines_guideline_01.pdf

デジタル・ガバメント推進標準ガイドライン

「デジタル・ガバメント推進標準ガイドライン」は、「デジタル社会推進標準ガイドライン群」における、「政府情報システム全般に関するドキュメント」の標準ガイドラインとして位置づけられています。

「デジタル・ガバメント推進標準ガイドライン」におけるシステム導入工程の全体像は以下の通りです。

プロジェクトの管理

利用者が実感できる効果を目標に設定し、達成に向けて機能するプロジェクト体制を作ります。また、プロジェクト管理を行うチームや担当者（PJMO）自身のモニタリングの結果により、抜本的改善のプロセスに入る場合もあります。

1. プロジェクトの立ち上げ、初動
2. プロジェクト計画書などの作成
3. プロジェクトのモニタリング
4. プロジェクトの終結

予算および執行

予算のための稟議に必要となる主要資料（年間スケジュールなど）を関係者に示し、わかりやすい構成となるように「全体から詳細につながる」資料作成をします。また、コスト削減、見積りの精査を行い適切に執行します。

1. 予算のための稟議の事前準備

2. 予算のための稟議に必要な資料の準備
3. 見積り依頼
4. 見積りの精査
5. 予算を要求する
6. 予算のための稟議後の対応

サービス・業務企画

サービス設計 12 箇条の内容に基づいて、ペルソナ分析やジャーニーマップといった手法により利用者の立場からサービス・業務の分析を行います。（サービス設計 12 箇条、ペルソナ分析、ジャーニーマップなどについては「サービスデザイン実践ガイドブック」を参照してください）

参考：サービス設計 12 箇条
[1]利用者のニーズから出発する
[2]事実を詳細に把握する
[3]エンドツーエンドで考える
[4]すべての関係者に気を配る
[5]サービスはシンプルにする
[6]デジタル技術を徹底的に活用する
[7]利用者の日常体験に溶け込む
[8]自分で作りすぎない
[9]オープンにサービスを作る
[10]何度も繰り返す
[11]一遍にやらず、一貫してやる
[12]情報システムではなくサービスを作る

1. サービス・業務企画の開始準備
2. 利用者視点でのニーズ把握
3. 業務の現状把握
4. サービス・業務企画内容の検討
5. 軌道修正
6. 新しい業務要件の定義

要件定義

RFI（Request For Information）や事業者からの情報収集を通して、市場にあるサービス、海外や国内の類似事例、新たな技術の動向や製品のライフサイクル、概算の予算規模、スケジュ

ールなどについて把握を行った上で、機能要件と非機能要件を明確にします。

1. 要件定義の事前準備
2. RFI の実施
3. 要件定義の全体像
4. 機能要件の定義
5. 非機能要件の定義
6. 要件定義終了後の対応

調達

全体機能実現のために、どのような単位に分けて調達するかを調達仕様書の作成を通じて明確化します。調達仕様書には、調達目的、作業内容と納品物、実施体制や発注者としての役割について考え方や注意点を記載します。また、総合評価落札方式では評価点の配分、留意点、事業者から WBS として示される作業内容の精査ポイントを明確化し、事業者の提案を評価します。

1. 調達の事前準備
2. 調達仕様書の作成
3. 調達仕様書以外のドキュメント作成
4. 調達手続きとプロジェクト管理
5. 検収

設計・開発

良い情報システムを作るために、発注者自身が要件を事業者に正しく伝え、関係者間の調整を行い、進捗状況を正しく把握し、情報システムの出来具合をテストする必要があります。設計・開発において発注者自信が実施する業務内容と移行、リハーサル、運用・保守の準備、マニュアルなど、について計画の立て方、ドキュメントの作成方法、注意点について理解し実施します。

1. 設計・開発を開始するための事前準備
2. 設計・開発の計画
3. 設計・開発・テストの管理
4. 見落としがちな活動に注意
5. 新業務の運営を円滑に行うための準備

サービス・業務の運営と改善

外部委託を活用する際の役割分担のコツを理解した上で、サービス・業務の運営を行います。また、蓄積されたさまざまな情報の分析を通してサービスや業務を改善します。

1. 新しいサービス・業務の事前準備
2. 業務の定着と次の備え

3. 業務の改善

運用および保守

情報システムの安定的な稼動を維持することに加え、利用者へのサービスを継続的に改善し、運用コストを低減していくために、運用および保守で実施する代表的な作業項目、会議体の種類と目的、定例会議での報告内容に対する注意点、変更管理、ログなどの蓄積、指標管理、運用業務の改善方法など、従業員が主体的に運用・保守業務を管理するための具体的な知識や技術を確認します。

1. 運用・保守を開始するための事前準備
2. 運用・保守の計画
3. 運用・保守の定着と次への備え
4. 運用・保守の改善と業務の引継ぎ

システム監査

各プロジェクトの取組がその目標達成に正しく向かっているのか、プロジェクトの各フェーズでの実施プロセスは適切かといった観点から、現状を調査し、改善すべき点がないかを第三者の視点で客観的に点検・評価します。

1. システム監査の理解
2. システム監査計画と監査実施計画
3. システム監査の実施
4. 指摘事項を踏まえた改善

「デジタル・ガバメント推進標準ガイドライン」は、さまざまなプロジェクトで発生する多様な状況に対して正確に実施すべき内容を伝えるという性格を持つ文書のため、正確さを優先して記載されています。一方「デジタル・ガバメント推進標準ガイドライン実践ガイドブック」は、読みやすさや実用性を重視しています。

詳細理解のため参考となる文献（参考文献）	
デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf
デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf

20-1-2. プロジェクトの管理

プロジェクト管理活動全体の流れは以下の通りです。

プロジェクト管理活動の全体の流れ

プロジェクトの立ち上げ、初動

プロジェクトの初動とは、プロジェクトが生み出され、スタートを切ろうとしている際のタイ

ミングです。出だしでいくつかの内容を理解し、行動しておくことで、プロジェクトの手戻りを大きく減らせます。

1. 目標とする成果を見定める
    A. 現場で発生している事実をつかんだ上で今後の目標を定める
    B. 上位計画の目標をブレークダウンし、プロジェクト目標と紐づける

現場で発生している事実をつかんだ上で今後の目標を定めることが重要です。

2. 手段の妥当性を確認する
    プロジェクトの立ち上げに当たり、プロジェクトの目標とする成果を定め、その成果を得るための手段が妥当であることを確認します。

3. プロジェクトの投資対効果を算出する
    情報システム整備は、利用者の利便性向上・負担軽減などの効果を得ることを目的としているため、投資対効果をしっかりと精査・評価することが重要です。

4. プロジェクトへの投資判断を行う
    プロジェクトへの投資判断は、プロジェクトの目標とする成果を明確にした上で、その成果を得るために必要となる経費や人的資源などを見積り、その費用対効果を踏まえた上でプロジェクトを開始することを責任者が意思決定することです。

5. 機能する体制を作る
    A. 制度所管部門、業務実施部門などを含めた PJMO 体制とする
    B. プロジェクトの規模に見合った体制を組む
    C. 他組織と連携できる体制を作る
    D. 先行経験を持つ人の技術や知識を活用する

    プロジェクトの円滑な運営を行うためには、プロジェクトの初期に十分な体制を構築することが重要です。

プロジェクト計画書などの作成

プロジェクトには必ず定めるべき事項が存在します。プロジェクトスタート時点で決められるもの、プロジェクトが進むにつれて具体化されるもの、状況に応じて内容を見直すものなど、さまざまな情報で成り立ちますが、すべてはプロジェクト計画書に記載され、関係者にて共有される必要があります。

1. プロジェクト計画書を作成する

A. プロジェクト計画書は段階的に詳細化する

B. 抜け漏れのない実施計画を作成する

プロジェクト計画書は、最初からすべての計画の詳細を記載するものではありません。初期の段階のプロジェクト計画書は、各項目についての概要を記載した上で、各項目の詳細化を行うタイミングを計画します。実施計画を作成する際には、PJMO が責任範囲を持つ部分のみで計画を立てがちですが、影響を受ける側（業務担当従業員、連携先システム、移行元の既存システムなど）も含めた全体的な計画が必要です。

2. プロジェクト管理要領を作成する

A. 問題に対処できる会議体を構成する

B. 本質的なリスクを事前に予見して、対応を準備する

C. 品質管理を事業者任せにしない

プロジェクト管理要領はその「実施に係るルール」を定義するものです。問題が発生したときだけ相談する形では情報共有が不十分になりがちなので、常日頃からプロジェクトの計画内容、進捗状況、重要課題を関係者が把握できるように進めていく必要があります。

プロジェクトのモニタリング

プロジェクト全体が意図した方向に進んでいるか、包括的な視点で確認するために PJMO 自身によって定期的にモニタリングを行います。

1. プロジェクトをモニタリングし、検証する

A. 目標、経費、進捗、品質などを中心にモニタリングする

B. モニタリングは適時に実施する

C. モニタリングと監査をうまく組み合わせる

D. プロジェクトは状況に応じて停止・改善する

プロジェクトの終結

プロジェクトの実施期間が 10 年を超えるものも珍しくありませんが、期間の長短に関わらずスタートしたプロジェクトはいずれ終わりを迎えます。プロジェクトの終結は、これまでの活動を振り返り、活動の評価を行うことにより、新たなプロジェクトへの糧となる重要なプロセスです。

1. プロジェクトの終結を処理する

A. プロジェクトを完了する

B. プロジェクトを終了する

C. 後続プロジェクトを策定する

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

「プロジェクトの立ち上げ、初動」における、プロジェクトの目標設定

新しいプロジェクトを開始する際には、現場における業務の実態と課題を網羅的に把握した上で今後の目標を定めることが大切です。プロジェクトには投資が伴います。投資を行ってまで得たい成果が何なのか。それを具体的な形で明確にすることが重要です。

（例）FAX と電話で受けていた注文業務を、IT を用いてサービス改善するためのプロジェクトにおける目標設定

プロジェクト目標が安易に設定された例（悪い例）

電子注文の実現	課題：顧客が FAX または電話で注文する必要がある 目標：電子注文を実現し、FAX または電話での連絡を不要とする
KPI	指標：電子注文利用率 60%（XX 年度）

プロジェクトの目標設定例（良い例）

受領連絡までの時間短縮	課題：週末の注文受領連絡が週明けになる 目標：（例外を除き）受領連絡を 12 時間以内に行う
大量注文への対応	課題：FAX は記入内容が多く、電話では話す内容が多い 目標：注文書の簡易化 大量注文向けのデータ一括申請を導入
顧客確認の不要化	課題：注文受領時に顧客台帳から顧客確認が必要なため、注文時に電話番号などによる確認が必要 目標：システム連携により、顧客確認が不要
KPI	受領連絡発信を含む注文完了を 12 時間以内順守率 80%（XX 年度） 100%（XX+2 年度）

＜目標設定のポイント＞

- 顧客が困っていること（受領連絡までの時間）への対応を優先
- 顧客や注文内容の異なりを捉え、個々のニーズへ対応（大量注文）
- 顧客目線で事前、事後の作業も改善（顧客確認）

- 小さく始める。そして、軌道修正しながら最終目標へ到達する（段階的な KPI）

悪い例では、目標設定に当たって抜け落ちている観点があります。

誰が何に困っているのか

原点に立ち返り、現場で発生していることをよく見ることが大切です。
顧客は本当に困っているのか、困っている場合は具体的に何に困っているのか確認することが重要です。現場に行き、実際の現場で発生していることを調べると、例えば以下の状況に気づけます。

- 注文受領連絡が遅い
- 大量注文時の作業が煩雑
- 注文のたびに起こる顧客確認

FAX や電話をかけなければならないことよりも、さらに深刻に困っていることがわかります。
電子注文を進めることに加えて、他にも対策を打つべきことがあると考えられます。
「顧客は FAX や電話をする手間に困っている」というストーリーは、推測に基づくものでした。現場を知らない人による推測のみで目標を設定するのではなく、現場の流れ、顧客の状況を調べて、本当の「困っていること」を把握することが最初の第一歩です。

顧客の種類

顧客とは誰なのか把握することが重要です。例では、「顧客」という 1 つの言葉で表現していましたが、顧客の中にもさまざまな種類の顧客がいる可能性があります。

- 既存顧客か新規顧客か

注文するのは取引実績のある既存顧客か、初めて取引する新規顧客かを把握することが大切です。新規顧客の場合は、支払い方法・配送先の確認や契約手続きなど、必要書類や事務手続きが異なる可能性があります。

- 配送先が一つか複数か

企業などの法人が注文を行っている場合は、店舗ごとに注文するのではなく、ある程度まとめて一括で注文を行っているかもしれません。
大量の注文を行っている企業は、店舗ごとに FAX 用の注文書を自動出力できるように独自の情報システムを整備済みかもしれません。この場合、拙速に電子注文を進めても、FAX での注文の方が便利であるため、電子注文が使われない可能性があります。

重要なことは、「困っていること」が異なるグループがあれば、個々のグループについて、それ

ぞれの困りごとを把握することです。また、独自の情報システムを整備済みの企業の例のように、「困っていない」グループを把握することも重要です。
例における「顧客」のような、複数のグループを包括する名詞には注意が必要です。ひとまとめに顧客像を捉えてしまうと、特定のグループが困っていることを見落としてしまうおそれがあります。

注文内容の種類

注文内容にもさまざまな種類があります。例えば注文の種類ごとに、確認の内容や必要時間を調べていくと以下のことがわかります。

- 形式的な内容確認のみを行うもの（大部分の注文）

「いつもの商品をいつもの数」注文される場合です。必須記載事項が正しく記載されているかなど形式的な確認のみを行うものが、注文件数の大部分を占めていました。さらに実態を調べていくと、実質的な確認に要する時間は僅かであり、各部門を流れていく際の待ち時間が長いことがわかりました。また、注文を受領した際の確認が十分でなく顧客へ再問い合わせを行うなど、再確認作業にも相当の手間が発生していることがわかりました。

- 受付け担当者が詳細な確認作業を行うもの（一部の注文）

一部の注文については、受付け担当者が詳細な確認作業を行っています。例えば、新規顧客の場合は「支払い方法」「配送先」などを含む初回購入手続きが必要です。他にも、いつもとは違う商品やいつもとは異なる数量の注文と思われる場合には、担当者が確認作業を行ってきました。しかし、上述の形式的な内容確認も同一の担当者が実施しているため、確認に十分な時間が割けない場合があることもわかりました。

エンドツーエンドの視野で、他に問題はないか

業務実施部門の視点で見ると、窓口で申請を受付け、審査を行うという業務は所管業務の重要な一要素です。一方、顧客が注文の事前、事後で作業を行っていることについては、業務実施部門の「担当外」として意識されないことがあります。
しかし、顧客の視点で見ると、事前、事後に必要となる作業も同様に重要なプロセスです。そこに、困りごとは発生していないか確認することが大切です。

- 顧客が注文を行う前に必要となる作業

必要物品（購入品目・数量）の取りまとめ、取扱い商品の確認、希望配送日時の確認など

- 顧客が注文受領連絡を受けた後に必要となる作業

配送日時の確認、必要に応じて各店舗への連絡、代金の入金など

顧客視点を重視して現場で発生していることを調べていくと、解決すべき課題にさまざまな種類があることがわかります。

One Point

「KGI」「CSF」「KPI」の定義と関係

- 重要目標達成指標（KGI：Key Goal Indicator）
  政策目標など、プロジェクトの最終目標を達成するために管理すべき指標

- 重要成功要因（CSF：Critical Success Factor）
  KGI を達成する（成功させる）上で重要となる要因

- 重要成果指標（KPI：Key Performance Indicator）
  プロジェクトを推進し、新しいサービス・業務を実現することで重要目標達成指標を達成するために管理すべき指標

例：資格試験の合格
資格試験に合格するために勉強するという場面を想定して、具体例を紹介します。
資格試験の合格（例：試験で 70 点以上取得）が KGI となります。
この KGI を達成するための CSF は、「十分な勉強時間を確保すること」（リソースの確保）や、自分の周りでこの資格をすでに取得している人や、この資格の分野に詳しい人を見つけて質問できるようにしておき、「わからないことがあっても解決できるようにすること」（協力体制の確立）、「周りから邪魔されずに集中して勉強できる環境を確保すること」（阻害要因の排除）などが挙げられます。CSF は、これらが揃えば確かに成功（目標を達成）しそうだと思える要因であることが大切です。
KPI は、「1 週間当たりの勉強時間：10 時間以上」、仕事が忙しくて勉強できないということがないように「1 週間当たりの残業時間：5 時間未満」などといった指標を設定します。KPI は、これらが達成されれば CSF（ここでは「十分な勉強時間を確保すること」）が実現できたといえるような指標を設定します。

「プロジェクト管理」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点
第 3 編 第 2 章 プロジェクトの管理 Step2 プロジェクトの立ち上げ、初動

セキュリティ機能を実装・運用するためポイント

プロジェクトを進める中で発生しやすいリスクとその対応方法について、例を示します。

多数の事業者間をまたいだシステム障害が発生するリスクへの対応
多数の事業者が参画する体制（マルチベンダー体制）においてシステム障害が発生した際に、各事業者が自身の責任範囲ではないことを主張し、問題を主体的に解決する主体が存在しないことによって、原因究明や対応実施が長期化するというリスク →リスクを軽減するためには、プロジェクト全体を統括する品質管理チームをプロジェクト管理を行うチームや担当従業員と特定事業者によって構成するなどの対応が考えられます。プロジェクト内でシステム障害などの問題が発生した際には、この品質管理チームが問題解決を統括し、複数事業者をまたがる問題についても問題の切り分けと問題対応者（事業者）の決定を行います。また、各事業者が品質管理チームの指示にしたがって必要な対応を行うことをプロジェクトのルールとしても明示します。
個人情報などの重要情報が漏えいするリスク
個人情報などの重要情報について、本来は参照権限がない利用者が参照してしまったり、外部へ流出してしまったりといった漏えいが発生するリスク →本番稼動前の段階においてリスクを軽減するためには、情報セキュリティの専門経験を持つ要員がセキュリティ設計を行い、要件定義で定めた情報セキュリティ対策要件の充足性を確認します。また、実作業の中でも本番データを扱うテストにおいて、氏名などの重要情報をマスキング（匿名化）した形で実施するなど、万一の情報流出時にも影響範囲を限定化する対応を行います。 →本番稼動後の段階においてリスクを軽減するためには、運用計画や運用実施要領などの中で重要情報を扱う際の手順を明確に示した上で、実際の実施状況について定期的に確認することや、セキュリティ監査の実施計画を立てて監査の実施とフォローアップを行うなどの対応を行います。

20-1-3. 予算および執行

政府機関における予算活動全体の流れは以下の通りです。

予算活動の全体の流れ
予算のための稟議（予算要求）の事前準備
稟議の直前に作業が集中したり、手戻り作業が発生したりしないように準備を行います。 1. 予算のための稟議を計画的に実施する

A. 予算のための稟議の年間スケジュールを把握する
B. 予算のための稟議に向けた作業のポイント

予算のための稟議・編成作業は、各段階において作業の締切り日が厳格に定められているので、いつ頃どの作業を行うかを意識し、計画を立てて、十分な時間と期間を確保して進めます。

2. 予算のための稟議の対象範囲を早期に決める
A. プロジェクト計画書を再確認する
B. 予算のための稟議から漏れがちな項目を理解する
C. 関係者と役割分担は早期に確認

プロジェクト計画書には、予算のための稟議の対象となる活動が、プロジェクト全体でどう位置づけられ、何を達成し、何の条件を守らないといけないかが書かれています。プロジェクト計画書の内容を理解した上で作業を進めることで、予算のための稟議の内容が具体的になり、第三者にも理解しやすいものとなります。

3. コスト削減の検討
A. ハードウェア・ソフトウェアのコスト削減観点
B. アプリケーションのコスト削減観点
C. 運用業務のコスト削減観点
D. そのほかのコスト削減観点

見積り依頼

情報システムの見積りには、専門的で見慣れない表現や内容が含まれることがあります。情報システムの見積りの特性を理解した上で、どのように見積り依頼を行えばよい情報を入手できるか理解することが重要です。

1. 見積り依頼書の作成
A. 要件が未確定な部分を明確にする
B. プロジェクトの状況によって内訳粒度を変える
C. 見積りフォーマットを指定する
D. 工程の名称の違いをなくす
E. 見積り手法に注意する
F. できるだけ詳細な要件を書く

2. 事業者への見積り依頼
A. 見積りしてくれる事業者を探す

B. 見積り事業者と対話して、発注者の意図を正しく伝える

見積りの精査

見積り金額は、過少でも過大でも問題です。必要十分な金額水準とするために、事業者から受け取った見積りに対して内容の過不足を見つけ、より精度を高めるための作業を実施します。

1. 人件費の見積り精査
    A. 安易な掛け算の精査
    B. 作業重複の精査
    C. 主要成果物との比較
    D. 開発生産性の精査

2. ハードウェアなどの見積り精査
    A. 製品単価を精査する
    B. 高額な製品を中心に、必要性を精査し他製品と比較する
    C. ソフトウェアライセンスを精査する
    D. 保守量を精査する

ハードウェア、ソフトウェアの借料や保守経費は、経費全体の中で大きな比率を占めます。まずは、大前提として製品単位での価格内訳を入手することが大切です。

3. 複数事業者の見積りの比較

予算のための稟議（予算要求）に必要な資料の準備

必要な経費を正確に把握するために事業者に見積りを依頼します。自社のやりたいこと・見積ってほしいことをまとめて伝えるために、見積り依頼資料を提示します。

1. 全体像と要点の明確化

2. 予算のための稟議の資料の作成上の注意点
    A. 「予算のための稟議の概要」の作成ポイント
    B. 「サービス・業務の説明資料」の作成ポイント

概算要求に向けた調整

組織内外の予算のための稟議の関係者に対して、予算の内容、必要性、金額妥当性などの説明を行うことが不可欠です。

A. PMO による調整

B. デジタル庁による調整
予算執行について
予算のための稟議が通ってからがプロジェクトの実質的な始まりです。プロジェクトの実務を計画的に進めるための準備作業を早めから実施します。 1. 執行計画案の作成 予算が決定された後、PJMO は「いつの時期」に「何の調達案件」を「いくら使う」のかについて、記載した 1 年間の執行計画案を作成します。 2. 執行計画案の調整 予算決定以後に生じた事情により、執行計画の内容を変更せざるを得ない場合は、PMO は PJMO から内容を聴取し、必要に応じて資料を徴求するなどして、変更内容が妥当か否か確認し、変更の是非を判断します。また、変更により予算を超過せざるを得ない場合には、プロジェクト間での調整を行うことになります。 3. 予算の移替え・予算執行管理 A. 予算の移替え B. 予算執行管理 年度途中に事情変更により追加の移替えが必要となる場合には、PMO はデジタル庁に執行計画の変更を行った上で、追加された予算の移替えを受けることになります。PMO は移替えられた予算の範囲内で、各 PJMO が適切に執行しているかについて、予算執行管理を行います。

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

予算のための稟議に必要な資料の準備

予算のための稟議の過程では、短期間で多くの関係者に対してプロジェクトの目標や予算の必要性などを理解してもらう必要があるため、要点をわかりやすく表現することが求められます。わかりやすい資料を作成することで、事業者からも有意義な提案を受けて的確な見積りを取得できます。

【全体像と要点の明確化】

プロジェクトの内容を第三者に正確に伝えるためには、「全体」から「詳細」につながる構成で説明することが重要です。始めに、サービスや業務の全体を俯瞰した視点を示し、目標を明らかにします。その上で、その中で今回のプロジェクトがどの範囲なのか、今回の予算のための稟議の対

象がどの範囲なのかと順を追ってクローズアップしていく構成にすることで、資料の読み手に対して正確にプロジェクトの姿と予算の必要性を伝えられます。

資料の読み手は、予算提案の内容を確認する担当者（PMO、デジタル庁、財務省主計局）だけではありません。PJMO 内部の従業員、利用者や関係者などのステークホルダー、見積り依頼先の事業者なども重要な読み手です。読み手によっては、関心のポイントが異なる部分もあります。しかし、どの読み手も共通して知りたいことは、サービスや業務の全体像です。プロジェクトの前提を間違えて捉えると、的確な判断ができないからです。

サービスや業務の全体像がわかる資料をわかりやすく整理するとともに、プロジェクトの進捗や変化に応じて資料内容をバージョンアップする活動を日常的に行うことで、予算提案に限らず、さまざまな状況でプロジェクトの状況説明を円滑かつ効率的に行えるようになります。

「予算のための稟議」に関する概要作成ポイント

予算のための稟議に関する概要は、プロジェクト計画書の内容を前提に、予算提案を行う範囲についての目標、内容、スケジュール、体制などを要約した資料です。この資料は、予算のための稟議の過程の中で、さまざまな関係者が真っ先に確認する資料となります。

作成時に気をつける点	
全体像と目標の明確化	サービス・業務観点からの全体像と現時点の問題発生状況を明らかにした上で、プロジェクトの目的・目標を示し、サービス・業務の改善後の実現像を示す。
具体的な改善内容の明確化	サービス・業務の改善内容、制度や業務ルールの改善内容、情報システムの改善内容を明確にする。（情報システムの改善だけの目線にならないように留意する）
主要なスケジュールの明確化	全体スケジュールを作成し、新しいサービス・業務の開始時期を明示するとともに、情報システムの主要な整備スケジュール（要件定義、調達、設計、開発、テストなど）、関連する制度変更のスケジュール、サービス・業務の変更のための手続きなどを明確にする。
体制とステークホルダーの明確化	プロジェクトの体制や、主要なステークホルダーへの影響有無を記述する。また、難易度の高い調整が発生する場合に、今後の調整方法（各ステークホルダーへの調査やヒアリングを通して詳細な分析を行う、ステークホルダーの責任者を集めた会議体を設置するなど）を明らかにする。
前提条件や制約の明確化	プロジェクトを推進する上での前提条件や制約がある場合は、その主要なものについて記述する。また、前提条件や方針などに不明確な箇

	所がある場合は、この資料にまとめて記述する（業務の説明資料、情報システムの説明資料などの個々の資料にも記載した上で、この資料にまとめる）。
費用対効果の考え方の明確化	情報システムの整備により得られる効果を明確にする。「効果」については、恩恵を受ける対象ごとに適切に設定されている必要がある。また、このような効果はいつまでにどのように把握するのか明確になっていることが重要である。さらに、累積効果がプロジェクト期間全体の投資額（予算のための稟議の経費の総額）を上回るまでの回収期間について明確にする。

「サービス・業務の説明資料」の作成ポイント

サービス・業務の説明資料は、プロジェクトが前提としているサービス・業務の概要を説明する資料です。サービス・業務企画での詳細な検討成果を、予算査定に係るさまざまな関係者にわかりやすく伝えるため、業務自体の概要、業務全体を示す業務フロー（概略）を 1 枚から数枚程度で簡潔に説明した資料を作成します。

作成時に気をつける点
● 業務（情報のやり取り）が発生する主体を明確化し、矢印などを使ってやり取りする内容を明確にする ● 管理指標と現在の達成状況について、定量的に記述する ● 顕在化している課題を記述する ● 異なる主体であっても業務や取り扱う情報などに共通点がある場合には、一括して記述するなど、図が難解にならないようにする

例として、EC サイトを運営している中小企業を対象とした業務フロー図を紹介します。

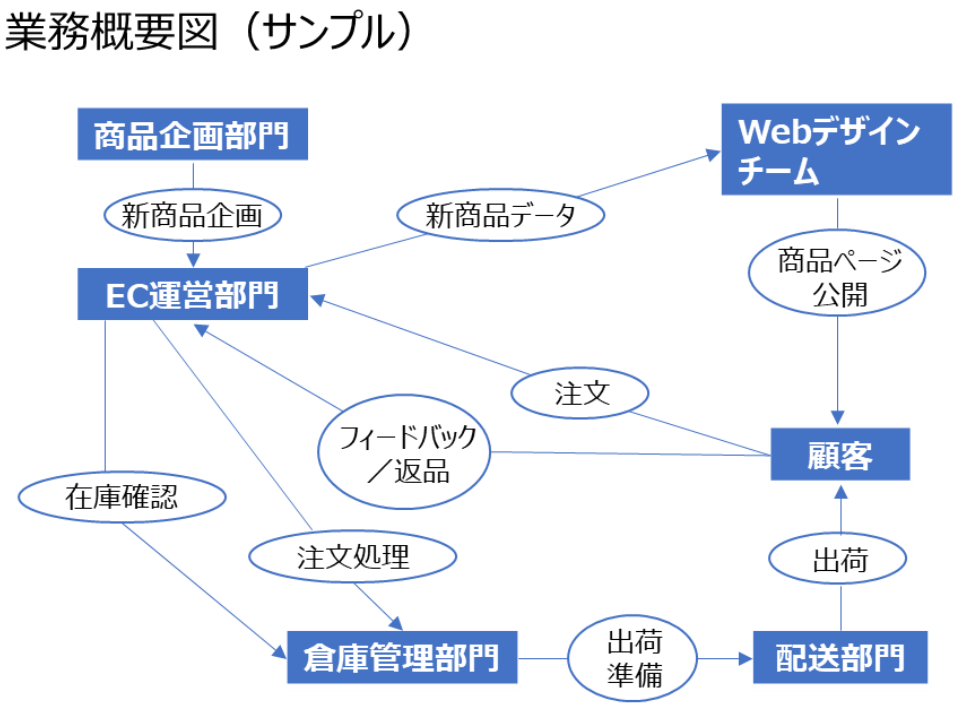

図 72. 業務概要図の例

見積りの精査

情報システムの開発や運用などを委託する事業者は、情報システムを運営していくためのパートナーなため、良好な関係を維持することは重要です。良好な関係とは、業務の一切を事業者任せにする状態ではありません。適切な役割分担の下で、緊張感を持って協働することが良好な関係です。

このことは、事業者が提示する見積りの精査についても当てはまります。発注者側である従業員が見積り内容を十分に理解し、前提条件や取り得る選択肢を理解した上で、実現機能と価格のバランスをとることが求められます。見積り金額を減らせば良いというものでもありません。必要不可欠な項目が抜け落ちてしまうと、システム開発や運用の段階で大きな問題になります。

見積りの精査は、実際には簡単ではありません。ハードウェア、ソフトウェアの見積りには専門的知識がないとわからない横文字が列挙されています。人件費の工数積み上げについても、どのような観点で確認すべきか難しいです。

見積り金額を適切な範囲に収めるとともに、発注者側・事業者側の双方がこの先の工程で円滑に活動ができるために、見積りを精査することが重要です。

One Point

生成 AI 活用による工数削減について

昨今、情報システム開発に生成 AI を活用する事例が増えています。生成 AI の利用で、従来よりも工数を削減できる可能性があります。

・ コードの自動生成と補完
開発者が自然言語で指示を出すだけで生成 AI がコードを自動生成するため、手動で書く手間を減らせます。また、未完成のコードを AI が補完してくれるため、コーディングの時間を短縮できます。

・ バグ検出と修正
AI はソースコードを自動的にレビューし、潜在的なバグを検出し、修正案を提示します。これにより、開発者はバグ探しや修正作業にかかる時間を短縮できます。

・ テストの自動化
テストコードの生成やテストの自動実行も AI によってサポートされるため、手動でのテスト作業に費やす時間を短縮できます。

・ ドキュメント生成
ソースコードから自動的にドキュメントを生成する機能により、開発者がドキュメント作成に割く時間を短縮できます。

注意点として、生成 AI の利用によって脆弱なコードが混入する可能性が増加するという指摘もあります。そのため、生成されたコードはしっかりとレビューする必要があります。

人件費の見積り精査

人件費は、工数（「人月」や「人日」）と単価の掛け算で算出できます。
例：4 人体制で 15 日間の作業=60 人日（3 人月）。
人日と人月の換算は、営業日ベースで計算するため、20 人日を 1 人月とすることが標準的です。

【留意点】

- 工数内訳を詳細に確認することが大切です。
見積りの中で、数十人月といった大きな単位で一式としての工数が示される場合、その中にはさまざまな作業が混在して合算されているため、個々の作業工数の妥当性を判断することができません。

- 工数の内訳は、機能や作業単位で分けることが非常に重要です。
数十人月といった大規模作業を、工程単位（設計、開発、試験など）、期間単位（月ごとの工数など）、要員種別単位（プロジェクトマネージャ（PM）、システムエンジニア（SE）、プログラマ（PG））で分けて、一見すると詳細な内訳として提示されることがあります。しかし、この

ような分け方ではこれ以上精査することが困難です。

- 個々の経費項目について必要性や生産性水準について精査できるようにするためには、実現する機能単位、実際に発生する作業単位での詳細工数が明記された見積りが不可欠です。
  このような見積りが提示されていない場合は、事業者に対して見積り精査上の必要性を伝えた上で、必要な粒度での工数見積りを取得しましょう。

ハードウェアなどの見積り精査

ハードウェア、ソフトウェアの借料や保守経費は、経費全体の中で大きな比率を占めます。

【留意点】

- 大前提として製品単位での価格内訳を入手することが大切です。
  予算のための稟議の段階では、「一式」などの形で大括りの見積りが事業者から提示されることがあります。しかし一式の状態では、それ以上に金額の精査が行えません。新規に整備する情報システムであっても、想定する製品に基づいて金額を積算しているはずなので、内容を確かめるべきです。また、既存情報システムに対する改修や更改などの案件であれば、なおさら詳細な積算内訳を求めることが重要です。

複数事業者の見積りの比較

複数事業者から見積りを取得した場合は、その内容について比較を行います。

【留意点】

- 比較に際しては、合計金額だけで比較するのではなく、主要な経費項目の単位で比較を行うことで事業者の得意分野、不得意分野などを把握することができます。

One Point

三点見積りによる適正予算の算出

三点見積りとは、例えば 5 つの事業者から見積りを取得した際に、最高額と最低額を除外した 3 者で平均して算出した額を指します。見積り経費項目ごとに三点見積りを行い、総合計したものを適正予算額とします。三点見積りは、金額だけではなく工数や期間の算出にも適用できます。

「予算および執行」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点
第 3 編　第 3 章　予算及び執行　Step.5 予算要求に必要な資料の準備

セキュリティ機能を実装・運用するためポイント

情報システムを構成する製品のサポート終了に付随する経費の考慮

情報システムを構築する際に、主要な作業経費（設計・開発経費やハードウェア関連経費など）が漏れることはまずありません。しかし、付随する作業経費については予算のための稟議の時点で漏れる可能性があります。

情報システムを構成するハードウェア、ソフトウェアなどの製品には、製品供給元からのサポートサービスの提供期限が定められていることが一般的です。特に、各種ソフトウェア（OS、ブラウザ、アプリケーションサーバ用のミドルウェア、データベースサーバ用のミドルウェアなど）については、バージョン別に細かくサポートポリシーが設定されており、注意が必要です。サポートが切れた製品の利用を継続すると、当該製品に対するセキュリティ脆弱性などの問題が発生した際に製品供給元からの対応が行われない可能性があります。そのため、原則として、サポートが終了するまでに後継製品を導入するなどの対応をとることが重要です。

人事異動時の引続き不足を防ぐこと

プロジェクト推進責任者など、プロジェクトの中心となる従業員が人事異動で離れる際、後任者がプロジェクトを円滑に引継げないことで問題になることがあります。これを防ぐために、予算のための稟議などの作業は複数人のグループで行い、常に情報共有することが大切です。異動する従業員は、まず後任の従業員ではなくグループのメンバーへ引継ぐことにより、引継ぐ情報量が少なくて済み、円滑に引継ぎができます。1 名でプロジェクトを担当する場合は、後任者のために資料をしっかり作成し、引継ぎを行うことが重要です。

One Point

事例：引継ぎ不足により、後日問題が顕在化した

監査を実施した結果、新たに機器・ソフトウェアなどを購入しなければ情報セキュリティ対策ができないことが判明しました。その結果が判明した後、担当者が人事異動で交替しましたが、新たな情報セキュリティ対策用の予算を確保しなければならないことについて、引継ぎが十分に行われていませんでした。

1 年後、情報漏えい事案が発生し、原因究明や報道対応を含めたさまざまな対応業務が大量に必要となりました。このとき、監査結果を反映した情報セキュリティ対策が講じられていれば、情報漏えい事案が発生しなかった可能性が高いことが判明しました。しかし、予算担当、会計課、PMO においても監査結果から新たな情報セキュリティ対策が必要なこと、そして予算のための稟議が必要だったことを誰も知りませんでした。

20-1-4. サービス・業務企画

サービス・業務企画活動全体の流れは以下の通りです。

サービス・業務企画の全体の流れ

サービス・業務企画の開始準備

サービス・業務企画を開始する前に、今のサービスや業務の現状をよく調べます。誰が何に困っているのか、背景にどのような事象が発生しているのか、事実を正確に把握します。

1. サービスデザイン思考を理解する
    A. 心構えと視点（サービス設計 12 箇条）を理解する

利用者視点でのニーズ把握

利用者視点でのニーズを把握するためには、まずどのような利用者が存在するかを把握した上で、利用者の立場に立ってサービスの現状を考えることが重要です。

1. 利用者のことを知る
    A. どんな利用者がいるかを調べる
    B. 利用者の人数を把握する

「どのような利用者が」「どこに」「どれくらい」いるのか、その利用者は「何のために」「どのように行動し」「何を求めて」いるのかを事実に基づいて把握し、情報を整理していきます。

2. 利用者のニーズを理解する
    A. 利用者のニーズから出発する
    B. エンドツーエンドで考える

現場を知らない人の推測のみで目標を設定するのではなく、現場の流れ、利用者の状況を調べて、利用者の本当のニーズを把握します。

業務の現状把握

何かを変えようとするときには、まず今がどうなっているかを正確に把握することから始めることが重要です。しかし、むやみに情報をかき集めても、整理しきれず、重要な情報の抜け漏れを招くおそれがあります。現状のサービス内容や業務内容を調査する方法を理解することが重要です。

1. 業務を観察する
    A. 事実を詳細に把握する
    B. 推測ではなく、現場で発生している事実をみる

C. 1 カ所だけの現場分析結果を全体に拡張しない

D. 日常的に業務の課題を収集し、分析に利用する

業務を観察する際には、先入観を持たずに観察することが大切です。細かな粒度で 1 つ 1 つの事実を徹底的に把握していくことで、今までに気づいていなかったものが見えてきます。実際に発生している事実に基づいて問題が可視化し、その問題に対して因果関係の整理を行った上で具体的な改善策を打つことができます。

2. 実績データを分析する

A. 平均、合計ではなく、ばらつきを見る

B. 時間と期間を区別して滞留状況をつかむ

C. 業務量のピークを捉え、ピークの発生原因を把握する

D. 問い合わせや要望は、根本原因が同じになる粒度まで分類する

ばらつきを見ると、時間帯や曜日によって利用方法にピーク特性があるなどの実情が見えてきます。また、業務の滞留箇所を探ることで業務処理の中のボトルネックを可視化できます。さらに、実際に発生している事象を確認し、ピークの発生原因を理解することで、業務量のピークを抑えることが可能です。問い合わせ・要望についても詳細な分類をすることで、問い合わせ発生数を時系列で把握できるという点で、業務・サービス改革のために有効な分析が行えます。

3. 業務を可視化する

A. さまざまな立場の人が理解できる業務フローを作成する

B. 業務ルールや業務実施方法をまとめる

C. 入出力情報や管理対象情報をまとめる

業務の分析結果は多くのドキュメントになることがあり、分析した人は内容を理解していても、初めて読む人にとってはポイントを把握するのが難しいです。プロジェクト内部や外部の関係者など多くの人が業務の分析結果を確認する必要があるため、業務フローなどを使って誰にでもわかりやすく可視化した資料を作成することが重要です。

サービス・業務企画内容の検討

現状の業務・システムを調査した結果をもとに、課題を把握し分析します。

1. 課題を整理し、分析する

A. 優先順位・影響度・費用対効果による分析

課題を原因ごとにグルーピングした後は、それらの課題を利用者への影響度や費用対効果をもとに優先順位づけし、主要課題を抽出していきます。

2. 企画案を作成する

A. すべての関係者に気を配る
B. 利用者の日常体験に溶け込む
C. 縦割り組織にやわらかく横串を刺す
D. 必要に応じて制度自体を見直す
E. システムを作る前に、業務を標準化する
F. 将来の業務フローには、効果を紐づける
G. 精緻に効果を積算し、主要な効果を実感可能なものとする
H. オープンにサービスを作る
I. 企画案を客観的に見直してみる

サービスはさまざまな関係者によって成り立っています。利用者だけでなく、すべての関係者についてどのような影響が発生するかを分析し、企画案を作成する際には既存の活動の中で完結できる方策を検討します。企画に関わる各所とは時間をかけて調整を進めることで、円滑に進められるよう配慮することが必要です。システムを作る前には業務を標準化し、また、システムの効果について業務フローに紐づけることで目指す姿をわかりやすくできます。

軌道修正

プロジェクトの方針は、把握した情報に応じてより良いものに見直されるべきものです。

1. 軌道修正しやすい進め方にする

A. 一遍にやらず、一貫してやる

開発段階でプロトタイプを作って利用者によるテストを行ったり、本番運用も一度に行うのではなく一部の利用者を対象に実証実験を行ってから本格的に展開したりするなど段階的に整備することによって、利用者の声を取り入れながら軌道修正を積み重ねることができます。

2. 柔軟に軌道修正する

A. 何度も繰り返す
B. 無理に継続しない

プロジェクト初期に想定したサービス・業務企画の前提となる課題や仮説が、現状調査の結果と異なっていると判明した場合は、プロジェクト計画全体の軌道修正の検討が必要です。試行的にサービスの提供や業務を実施し、利用者や関係者からのフィードバックを踏まえてサービスの見直しを行うなど、何度も確認と改善のプロセスを繰り返しながら品質を向上させます。また、費用対効果に乏しいと判明したプロジェクトについては無理に継続せず、中止を含めた検討をすることが大切です。

新しい業務要件の定義

「利用者視点でのニーズ把握」「業務の現状把握」で把握した現状をベースに、「サービス・業務企画内容の見当」「軌道修正」で検討した次の業務・システムの方向性に則り、次の新しい業務に関する要件を定めていきます。

1. 業務要件をまとめる
2. 定義内容を関係者に共有する

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

例：業務の現状把握

実際に発生しているさまざまな事象をしっかり観察し、把握することが重要です。現状を正しく把握せずにサービス・業務企画を行うと、見た目としては新しいサービスが実現できたように見えても、実際にはサービスが使われなかったり、業務上大きな問題が発生したりするなど、さまざまなトラブルが発生する危険性があります。

事実を詳細に把握するということは、サービス・企画のプロセス全般を通じて根底となる重要な姿勢です。

【事実把握時の留意点】

- 事実把握には「平均や合計ではなく、ばらつきを見る」「推測ではなく、現場の事実を確認する」といった考え方があります。あまりにも当然のことですが、今までに数多くのプロジェクトでトラブルが発生したり、失敗に終わってしまったりした原因を辿ると、最初の企画時点で事実を詳細に把握できていなかったことに帰結する例が本当に多いです。

- 細かな粒度で事実を徹底的に把握することで、今まで気づいていなかった問題が見えてきます。実際に発生している事実に基づいて問題が可視化されれば、因果関係を整理し、具体的な改善策が導き出せます。問題が可視化されないと、思い込みや仮説に基づいた業務設計となり、問題を解決できません。

- 経験豊富な人ほど、先入観で事実を見過ごしてしまうことがあります。現場を観察し、業務で発生する実データを確認しながら、何が起きているかを先入観なく調べることが大切です。

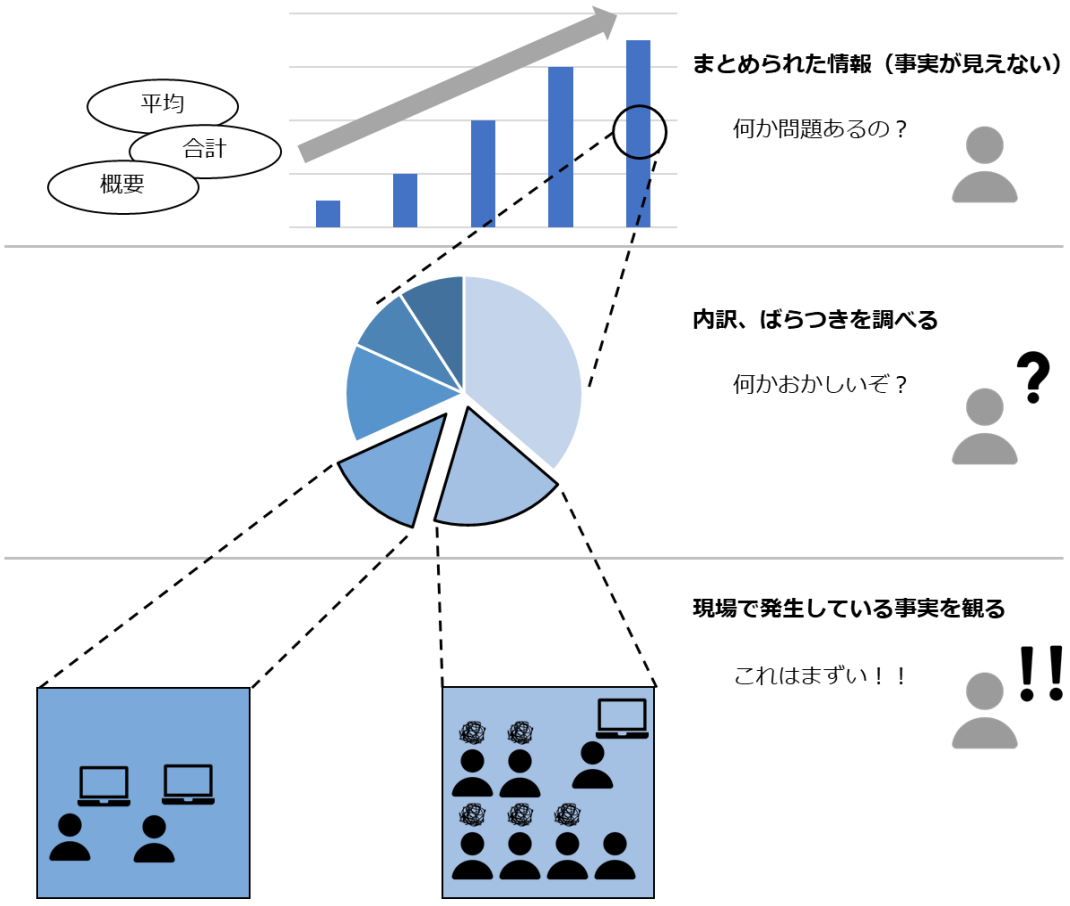

図 73. 事実を詳細に把握するイメージ図

（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

「サービス・業務企画」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点
第 3 編 第 4 章 サービス・業務企画 Step3 利用者視点でのニーズ把握
第 3 編 第 4 章 サービス・業務企画 Step4 業務の現状把握
第 3 編 第 4 章 サービス・業務企画 Step5 サービス・業務企画内容の検討

セキュリティ機能を実装・運用するためポイント

デジタル技術を徹底的に活用する

デジタル技術は日々進化しています。今までは手間をかけなければできなかったことが、デジタル技術を活用することで効率的に実施できる可能性があります。情報セキュリティとプライバシーを確保する観点からも、IT マネジメント全体を通してリスク管理を適切に行い、情報セキュリティ対策を確実に行うデジタル技術の活用が重要です。

20-1-5. 要件定義

要件定義の活動全体の流れは以下の通りです。

要件定義の全体の流れ

要件定義の事前準備

要件定義を開始するに当たって、まずは、目標、対象範囲、サービス・業務企画の方向性など、実施計画などを把握し、プロジェクトとして達成すべきゴールを把握します。

1. 要件定義で従業員が得た知識は貴重な財産

要件定義を行うことで、サービス・業務の企画内容、情報システムの要件に係る背景、決定経緯、理由、従業員の長年の経験や勘に基づく知識が収集されます。これはプロジェクトを進める上で貴重な財産となります。担当者が異動する場合は、これらの知識がなくならないように十分な引継ぎが必要です。

2. プロジェクト計画や業務要件を把握する

要件定義を開始するに当たっては、目的、目標、対象範囲、サービス・業務企画の方向性など、実施計画などからプロジェクトとして達成すべきゴールを確認し、サービス・業務から見た情報システムに対する要求を理解する必要があります。

RFI の実施

RFI（Request For Information）は、情報システムに関するさまざまな情報を収集するために事業者などに対して、構築しようと考えている情報システムに関わる、技術的な情報や動向、参考事例の提供を依頼する活動です。

要件定義では、RFI などの情報収集を行うことにより、さまざまな情報を複数の事業者から収集し、情報システム構築の方向性や実現性、適用可能な技術などの情報を把握できます。

1. RFI を理解し、必要な資料を準備する
    A. RFI の意義と用途を理解する
    B. RFI に必要な資料を準備する

2. 公平性を確保したヒアリングを行う

3. 収集した情報をもとに資料を更新する
    A. RFI や発注前ヒアリングの結果を整理する
    B. 既存の資料を最新化する

要件定義の全体像

要件定義では、業務要件、機能要件、非機能要件で定めた各項目の内容を定義します。

1. 構成要素を把握し要件を定義する
2. 機能の優先順位は改善後の業務で判断する
3. 一貫性を持った論理的な記載とする
4. 要件定義書は継続的にメンテナンスする

機能要件の定義

機能要件を具体的に検討し、ドキュメント化します。

1. 個々の領域について要件を定める
    A. 機能に関する事項
    B. 画面に関する事項
    C. 帳票に関する事項
    D. データに関する事項
    E. 外部インターフェースに関する事項

2. 必要な機能を漏れなく抽出し検討する

3. 実現手段ではなく、求める結果を記載する

新しい非機能要件の定義

すでに定められた業務要件に基づき、業務要件を満たすために情報システムの非機能に求められる要件を定義していきます。

1. 個々の領域について要件を定める
    A. ユーザビリティおよびアクセシビリティに関する事項
    B. システム方式に関する事項
    C. 規模に関する事項
    D. 性能に関する事項

E. 信頼性に関する事項
F. 拡張性に関する事項
G. 上位互換性に関する事項
H. 中立性に関する事項
I. 継続性に関する事項
J. 情報セキュリティに関する事項
K. 情報システム稼動環境に関する事項
L. テストに関する事項
M. 移行に関する事項
N. 引継ぎに関する事項
O. 教育に関する事項
P. 運用に関する事項
Q. 保守に関する事項

2. システム方式を決定する

要件定義終了後の対応

関係者へ要件定義内容の共有などを実施します。

1. 定義内容を関係者に共有する
2. プロジェクト計画書に反映して最新化する

要件定義の全体像

要件定義は、業務要件、機能要件、非機能要件で構成されています。各要件には多数の項目が定義されており、それぞれの内容は項目間で影響し合っています。

要件定義の内容は定義する項目が多数あるため、詳細を検討していく中で、どこかで同じ内容を検討していないか、本当に漏れがないか、と不安になることがあります。まずは、要件定義の構造と定義する項目を俯瞰し、要件の上位に当たる、政策目的・実現する目標、達成すべきプロジェクト目標に沿って、何をどこで定義するのか、それぞれの項目がどのように関連しているかを理解することが大切です。要件定義は、各項目の整合性を逐次とりながら定義することで、無駄なく、漏れなく、効率的に検討していくことができます。

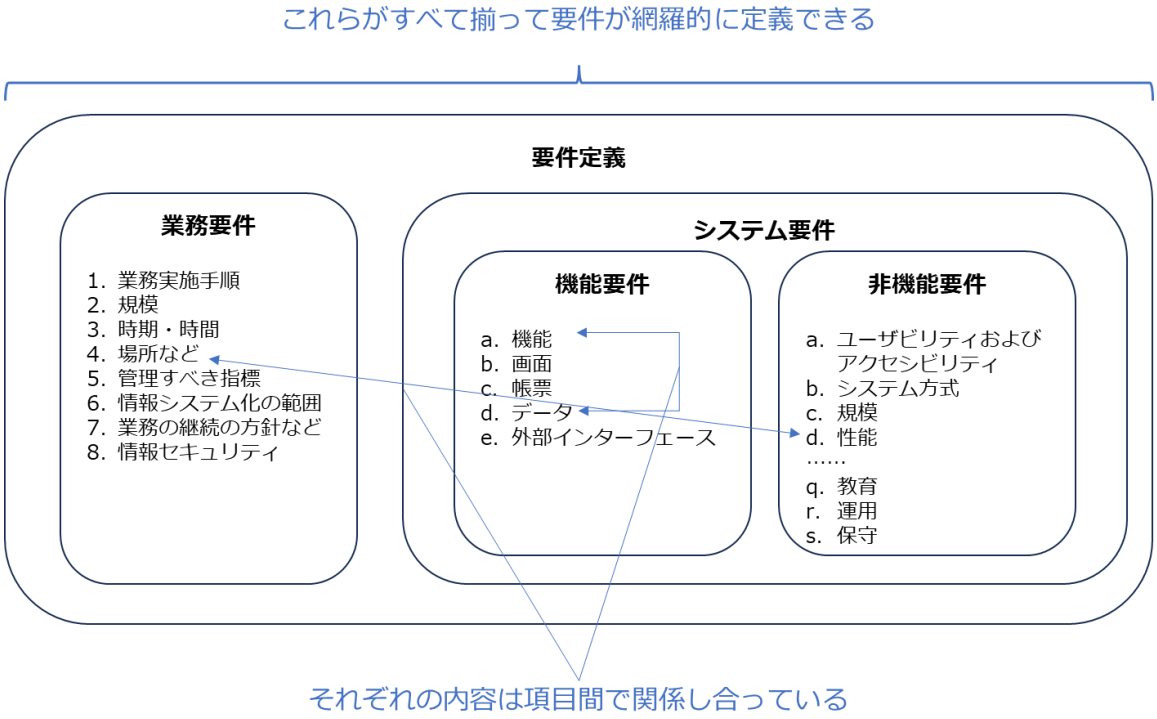

図 74. 要件定義の構成要素とポイント

（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

要件定義を作成する時点では、すべての項目をしっかりと定義することが難しい場合があります。未確定の項目は、後の工程で定義されることになります。このときに関連する項目に変更がある場合があるため、関連する項目の変更漏れがないように、未確定項目の関係性がわかるようにしておくことが大切です。

定義書が一通り作成された後、以下の観点による最終確認を行うことで、定義漏れを防ぐことができます。

要件定義内容を確認する観点	解説
必要性	政策目的・目標の実現やプロジェクト目標達成への貢献といった有効性の観点および費用対効果の観点を踏まえ、実現すべき機能要件および非機能要件のみが定義されていること。
網羅性	業務要件が漏れなく定義され、その実現のために備えるべき機能要件および非機能要件が漏れなく定義されていること。
具体性	機能要件および非機能要件を実現する複雑さ、難易度、調達コストに影響する不確定要素が可能な限り排除されていること。

定量性	業務および情報システムの規模などが定量的に示され、性能などに関する計測可能な指標と具体的な目標値が設定されていること。
整合性	業務要件、機能要件、非機能要件の内容に矛盾がないこと。また、関連する他のプロジェクトの要件定義内容と整合的であること。
中立性	調達コストの削減、透明性向上などを図るため、要件定義内容が特定事業者に不必要に依存したものでないこと。
役割分担の明確性	業務の実施体制が明確であること。また、情報システムのテスト、移行、引継ぎ、運用、保守に関して、関係各所なども含め、自組織と事業者との役割分担が明確であること。
情報セキュリティ	自組織の情報セキュリティポリシーを順守するために必要な対策が漏れなく定義されていること。

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

要件定義プロセスにおける Fit&Gap 分析

情報システム構築においてパッケージソフトや SaaS を利用する場合は、Fit&Gap 分析が必要になります。Fit&Gap 分析とは、導入するパッケージソフトや SaaS などのシステムと、自社の業務要件との適合性を評価する手法です。導入するパッケージソフトや SaaS などのシステムが、どの程度自社の業務要件が満たすか（Fit）、満たされない部分はどの程度あるか（Gap）を明確にします。

Fit&Gap 分析が重要な理由

パッケージソフトや SaaS は、特定の業務ニーズに対応するために設計された汎用的なソリューションです。これらのソリューションが、自社の業務要件に完全に適合することは稀であるためです。パッケージソフトや SaaS には標準的な機能が備わっているものの、自社が求めるすべての機能が含まれているわけではありません。Fit&Gap 分析を通じて、自社の業務要件に適合している部分（Fit）と、適合していない部分（Gap）を明確にすることが必要です。ギャップがある場合は、対応方針を検討します。（例えば、パッケージソフトや SaaS をカスタマイズする、別のソリューションを検討するなど）それにより、自社に最適なパッケージ製品の選定や、必要なカスタマイズの範囲が明確になります。Fit&Gap 分析を適切に行うことで、システム導入後のリスクやコストを最小化できます。

Fit&Gap 分析の具体的な手順例：

1. 業務要件の整理
   まず、自社の業務要件を整理し、どのような機能やプロセスが必要かをリストアップします。これには、現在の業務プロセスや将来的なニーズも含まれます。

2. パッケージソフトや SaaS の機能確認
   導入予定のソフトウェアが提供する標準機能を確認します。製品のドキュメントやデモを通じて、どの機能が自社の要件に対応しているかを評価します。

3. フィット部分の特定（Fit）
   ソフトウェアが業務要件をそのまま満たしている部分を確認します。この部分はカスタマイズなしでそのまま導入可能で、導入コストやリスクが低いです。

4. ギャップ部分の特定（Gap）
   ソフトウェアが業務要件を満たしていない部分（ギャップ）を特定します。これらのギャップが大きい場合、以下のような対応が必要です：
   - カスタマイズ:ソフトウェアを自社要件に合わせてカスタマイズする。
   - プロセス変更:業務プロセスをソフトウェアに合わせて変更する。
   - 追加ツールの導入:足りない機能を補うために別のツールやシステムを導入する。

5. コストとリスクの評価
   ギャップ部分の解決にかかるコストやリスクを評価します。カスタマイズやプロセス変更には時間や費用がかかるため、その影響を検討します。

Fit&Gap 分析における考慮事項：

- 標準機能の活用
  可能であれば、カスタマイズを避け、標準機能を最大限活用することで、コストや運用の複雑さを抑えることが推奨されます。また、製品やサービスにおけるバージョンアップの観点から（セキュリティの観点からも）安易なカスタマイズを避け、できる限り業務プロセスをパッケージソフトや SaaS に合わせることが推奨されます。

- 長期的視点での検討
  将来的なバージョンアップや運用コストも含め、長期的な視点で Fit&Gap 分析を行うことが重要です。

・ 業務プロセスの柔軟性
ソフトウェアに合わせた業務プロセスの見直しが可能か否かを検討し、システムの標準機能で対応できる部分が増えるようにすることも一つの方法です。

Fit&Gap 分析の結果に基づく決定

そのまま導入	フィット部分が大きく、カスタマイズなしで導入可能な場合。
部分的にカスタマイズして導入	小規模なギャップがあり、一部カスタマイズやプロセス変更で対応可能な場合。
大幅なカスタマイズまたは導入中止	ギャップが大きく、コストやリスクが許容範囲を超える場合、導入自体を見直す必要があります。

パッケージソフトや SaaS 導入の成否は、この Fit&Gap 分析の精度に大きく依存します。適切な分析を行い、導入計画を立てることが大切です。

「要件定義」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点
第 3 編 第 5 章 要件定義 Step5 機能要件の定義 第 3 編 第 5 章 要件定義 Step6 非機能要件の定義

セキュリティ機能を実装・運用するためポイント

非機能要件における、情報セキュリティに関する事項について

自組織において定められた情報セキュリティポリシーを順守するために必要な情報セキュリティ対策の内容について、具体的に記載します。

例えば、当該情報システムに実装する機能や画面に対して、利用者の権限に応じた管理レベルを記載します。

No.	機能	利用者区分	アクセス権限	補足
1	○○申請処理	一般ユーザー	自申請情報のみ登録・参照・変更・削除可能	
2	○○申請処理	一般従業員	自組織が担当する申請者の情報は登録・参照・変更・削除可能。他組織担当の申請者情報は参照のみ	

また、想定されるリスクの概要と対策について記載します。

No.	リスクの区分	リスクの概要と対策	補足
1	…	インターネットからの不正アクセスなど、外部からの攻撃を受ける可能性がある。必要な対策を講じ、不正アクセスなどの悪意ある攻撃を防ぐ。	
2	…	来訪者エリアと従業員エリアで、同じネットワークを利用するため、来訪者エリアからの進入などの被害につながる可能性がある。ネットワークの論理分割、セグメント分割、ファイアウォールやＤＮＺなどの設置により、進入を防ぐ。	
3	…	利用者が担当業務に関係のない情報を閲覧し、情報漏えいにつながる可能性がある。必要十分な権限制御を行い、利用者に業務に不必要な情報を閲覧させない。	

最低限記述すべき情報セキュリティ対策要件

（1）セキュリティ機能の装備

【情報システムの構築などを行う場合の記載例】

以下のセキュリティ機能を具体化し、実装すること。

- 本プロジェクトで導入する情報システムへのアクセスを業務上必要な者に限るための機能
- 本プロジェクトで導入する情報システムに対する不正アクセス、ウイルス・不正プログラム感染など、インターネットを経由する攻撃、不正などへの対策機能
- 本プロジェクトで導入する情報システムにおける事故および不正の原因を事後に追跡するための機能（情報システムに含まれる構成要素（サーバ装置・端末など）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。）

（2）脆弱性対策の実施

【情報システムの構築などを行う場合の記載例】

以下の脆弱性対策を実施すること。

（第三者による脆弱性検査を必要とする場合）

- 本プロジェクトに基づく改修（新規構築/更改）が影響する範囲について、第三者による脆弱性検査を実施し、その結果を関係各所に書面にて報告すること。

（第三者による脆弱性検査を必要としない場合）

- 本プロジェクトに基づく改修（新規構築/更改）が影響する範囲において、第三者による脆弱性検査を実施し、その結果を関係各所に書面にて報告すること。なお、脆弱性検査ツールを用いるなどにより客観的なテストが可能であれば、受注者で実施することも可とする。
- 構築する情報システムを構成する機器およびソフトウェアの中で、脆弱性対策を実施するものを適切に決定すること。
- 脆弱性対策を行うとした機器およびソフトウェアについて、公表されている脆弱性情報および公表される脆弱性情報を把握すること。
- 把握した脆弱性情報について、対処の要否、可否を判断すること。対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置および影響を納品時に関係各所に書面にて報告すること。

【情報システムの運用・保守・点検を行う場合の記載例】
以下の脆弱性対策を実施すること。
- 機器およびソフトウェアについて、公表される脆弱性情報を常時把握すること。
- 把握した脆弱性情報について、対処の要否、可否につき関係各所と協議し、決定すること。
- 決定した対処または代替措置を実施すること。

（3）情報セキュリティが侵害された場合の対処
本プロジェクトにおける業務の遂行において情報セキュリティが侵害され、またはそのおそれがある場合には、速やかに関係各所に報告すること。これに該当する場合には、以下の事象を含む。
- 受注者に提供し、または受注者からのアクセスを認める関係各所の情報を外部へ漏えいおよび目的外利用
- 受注者から関係各所のその他の情報へのアクセス

20-1-6. 調達

調達の活動全体の流れは以下の通りです。

調達の全体の流れ
調達の事前準備
適切な外部事業者や製品を選定したり、調達時に不十分な内容に起因する手戻りなどの無駄な手間をかけず、効率的に調達作業を行ったりするためには、事前準備をすることが重要です。

1. 調達の単位・計画を確認する

A. プロジェクト立ち上げ時点で調達を計画する
B. さまざまな調達単位があることを理解する
C. 調達にあった落札方式、評価方式を検討する
D. 調達計画を早めに公開する
E. 契約方式を検討する

調達の計画では、「何の調達を」「どの単位で」「いつ調達するか」を計画します。計画後、それらの調達を「どの単位で行うか」を検討します。複数を 1 つの調達にまとめることや、1 つの単位を分割して複数の調達にすることも可能です。価格以外の技術的な評価を行う場合は、審査に必要となる評価基準、審査体制などを十分に検討した上で事業者の選定の準備を整えることが大切です。

2. 調達の注意事項を理解する

A. 調達手続きの基本的なルールを確認し理解する
B. 入札制限を正しく理解する
C. 一者応札の状況を改善する
D. 調達の前にリスクを再確認する

プロジェクト計画の段階で調達に係るルールを理解し、調達に必要な期間を踏まえて準備を行えるように調達の計画をたてることが重要です。

調達仕様書の作成

調達仕様書とは、プロジェクトの目的達成に必要な製品の入手や、必要となる役務を実施する外部事業者を選定するために示す、発注者側の条件を集めたドキュメントです。

1. 関連ドキュメントとの関係性を理解する

A. 調達仕様書と要件定義書の住み分けを理解する
B. 付属文書を活用して可読性を上げ機密性を確保する
C. 既存情報システムの機能改修を行う場合に準備するドキュメントを理解する

2. 調達仕様書の記載内容を理解する

A. 調達の意図や目的を正しく伝える
B. 関連する調達、入札制限を伝える
C. 作業内容・納品物を関連付けて網羅的に記載する
D. 外部事業者の具体的な作業内容を明確にする
E. 作業の実施体制を明確にする

F. 成果物の取扱いに注意する（知的財産権）

G. 再委託に関する事項を定める

H. 納品後に不具合が発覚したときの責任を明確にする（契約不適合責任）

調達仕様書以外のドキュメント作成

調達では、調達仕様書以外にも、提案依頼書や契約書などさまざまなドキュメントを用意する必要があります。

1. プロジェクトに合わせた契約書を作る

A. 調達仕様書と契約書の整合性を確認する

調達仕様書の記載事項には、場合によって契約書に同様の事項を記載することがあります。調達仕様書と契約書でそごが生じている場合、後々問題となることもあるので、契約書を所管する部署と事前に意識合わせを行い、調達仕様書との記述の住み分けを決めておくことが重要です。

2. 提案依頼書の内容を工夫する

A. 具体的な作業計画を評価する

B. 加点の配分を工夫する

提案書の内容だけでは、事業者が本当に調達案件を履行する能力があるか否かを判断するのは難しいです。技術力を適正に評価するためには、具体的な作業計画の案の提出を求めて評価することが効果的です。技術審査を行う際は、当該調達で何を重視するかをよく検討し、重視する項目に対する優れた提案に高い配点がされるように検討する必要があります。

調達手続きとプロジェクト管理

プロジェクトの活動において、調達はそれ以前の活動結果を集約し、その後の活動を方向づけるプロジェクトの結節点ともいえます。このタイミングでのポイントを押さえた上で調達手続きを行うことは、プロジェクト管理の視点からも重要です。

1. 調達手続きに伴うプロジェクト管理作業とは

A. 第一次工程レビューを意識して資料をチェックする

調達仕様書の自己点検を行っておくことで、調達が不落に終わることによる調達事務手続きの手戻りなどの無駄を未然に防ぐことにつながります。

2. 情報システムの調達に特有の注意点

A. ベンダーロックインを理解し、回避する

B. 入札参加要件を緩和する

C. 入札事務手続きを簡素化する

情報システムの調達には特有の注意点があり、これを理解せずに進めると後々問題が発生する可能性があります。問題を防ぐためには、事前にこれらのポイントを把握し、仕様書や契約書に適切な制約を盛り込み、しっかりと管理することが重要です。

検収

調達の結果、外部事業者との契約が締結され、製品の購入手続きも含め委託した作業がスタートします。その結果、製品であれば納品、作業であれば完了報告が行われ、発注者はそれに対して検収を行います。

1. 検収の位置づけと内容を理解する
   A. 検収と受入テストの違いを理解する
   B. 残存する課題（軽微な瑕疵など）の対応を明確にする

検収の実施者は、発注者側の担当者です。検収の担当者は、調達仕様書および契約書に定められた内容と納品物との突合せを行い、仕様どおりに納品されているのかを確認します。一方、受入れとは、PJMO を中心として、納品された成果物が今後のサービス・業務の実現に足るか否かを判断する行為です。検収時点で不具合がわかっている場合は、各々の不具合に対して、「いつまでに」「誰が」責任を持って「どのように」対応するかを改修計画で明確にします。

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

例：関連ドキュメントとの関係性を理解する

調達では、調達仕様書以外にも次のようなドキュメントが存在します。それぞれのドキュメントの定義と関係性をあらかじめ理解しておくことが重要です。

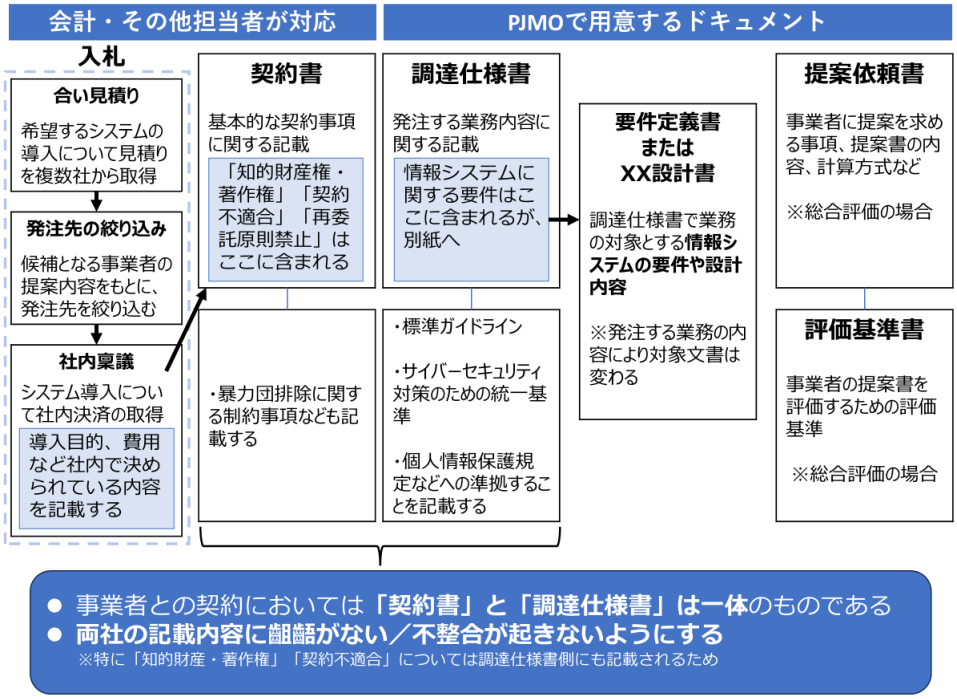

図 75. 調達に必要なドキュメントの関係図

例：「調達の事前準備」における、調達の注意事項を理解

プロジェクト計画の段階で組織の調達ルールをよく理解し、調達に必要な期間を踏まえて準備を行えるように、調達の計画を立てることが重要です。

「調達」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点
第 3 編　第 6 章　調達　Step3　調達仕様書の作成

セキュリティ機能を実装・運用するためポイント

再委託先の情報セキュリティ対策に係る規定を確認すること
情報システムの整備においては、プロジェクトの規模が大きくなるほど、さまざまな役割が必要となります。特に、設計・開発工程や運用・保守工程では、情報システムの一部を担う特定の技術や専門分野に特化した外部事業者を活用する機会が多いです。これらの外部事業者は、請負契約を締結している外部事業者からの再委託となることもあります。再委託先が担当する作業内容については、委託先の外部事業者（以下「委託先」という）が責任を持って管理することが原則です。しかし、再委託にまつわる失敗事例は多いです。

事例：再委託に関する失敗例

- 委託先が作成した提案内容を評価し、プロジェクトの委託先として選定したにも関わらず、再委託先が提案内容を遂行するために必要なスキルレベルを十分に持っていないため、成果物の品質低下やスケジュール遅延を招いてしまった。

- 委託先が再委託先に利用者との検討や調整などの作業を丸投げしてしまい、要件や仕様の変更を把握しなかったため、工数超過やスケジュール遅延に発展してしまった。

このような問題を未然に防ぐために、調達仕様の「再委託に関する事項」にて、再委託の制限および再委託を認める場合の条件、承認手続き、再委託先の契約違反などを定め、再委託時の要員の配置や品質、情報管理などに関する責任の所在を明確にします。また、プロジェクト遂行中に発生したさまざまな事情により、請負側の体制変更を図ることがありますが、その際は発注者側と協議の上、請負者の負担と責任において実施することが原則です。
なお、再委託に関する事項は、自組織の情報セキュリティポリシーにおける再委託先における情報セキュリティ対策に係る規定も必ず確認することが大切です。

20-1-7. 設計・開発

設計・開発の活動全体の流れは以下の通りです。

設計・開発の全体の流れ

設計・開発を開始するための事前準備

設計・開発を開始する間に、要件を適切に事業者に伝える必要があります。また、PJMO が求める情報システムをトラブルなく構築していくためには、仕様の調整や、できた情報システムを適切に検証することが必要となります。

1. 設計・開発で従業員が行うべきことを理解する
    A. 『要件の内容を伝える役割』
    B. 『要件どおりに情報システムができたかを確認する役割』
    C. 『プロジェクトの進捗状況を正しく把握し適切な調整を行う役割』

要件定義書だけでは読み取れない発注者側の意図や要望について、発注者側は正しく伝達することが必要となります。また、設計をする中で見えてくる課題などの対応方法を決めることも必要です。構築された情報システムが、伝えた要件を満たすものになっているかを確認しま

す。また、新たな情報システムを導入する際には、ほとんどのケースで業務を見直して、手順や内容の変更を行います。

2. 設計・開発全体を通して理解すべき点とは

A. 要件を理解した従業員の継続的な関与がプロジェクトを安定させる
B. 要求とコストと納期のバランスをとる
C. 設計・開発の全体像と流れを理解する
D. 通常シナリオだけでなく緊急時の対応計画も準備する
E. メンテナンス性を考慮した成果物の構成、内容を考える

PJMO が、発注者として設計・開発を適切に管理していくために、設計・開発の活動全体を俯瞰的に理解しておく必要があります。例えば、要件定義において、その全体像を理解している従業員はごく一部に限定されます。この従業員をプロジェクトの体制に参画させ続けられるよう、体制の組成時に調整を行うことはプロジェクトを安定させることにつながります。

設計・開発の計画

設計・開発事業者が決まった後、最初にすることは計画を立てることです。設計・開発の活動は、PJMO にとっては、実態が見えにくい活動になりがちで、問題の発覚が遅れて大惨事になることもしばしばあります。設計・開発の活動をブラックボックスにしないようにすることが大切です。

1. 設計・開発の管理の要点を理解する

A. 定点観測こそ進捗・品質管理の要
B. 判断に必要な情報を従業員が理解できる説明として事業者に求める

作業の状況を定量値で管理し、継続してその値を把握すると、問題が発生する予兆を捉えられます。その事象を個別に分析することで、原因を捉え必要な対策ができます。また、事業者の資料や説明内容は従業員から見ると専門的でわかりにくいものになりがちなため、内容を理解できるように丁寧な説明や資料のまとめ直しをしてもらうことが大切です。

2. 設計・開発の実施計画を立てる

設計・開発実施計画書は、当該事業者が担当する設計・開発作業の範囲について、PJMO が作成するプロジェクト全体のプロジェクト計画を具体化・詳細化したものです。設計・開発の実施計画を作成する際は、以下のポイントに注意して作成することが重要です。

A. 2 種類のプロジェクト計画書の相違点を理解する
B. 意思決定の手順を明確にする

C. 当初計画からの変更は、必ず関係者で合意する
D. 他の関係者との役割分担の境界線を定める
E. WBS で作業計画を確認し進捗を把握する
F. EVM を用いた進捗管理手法を理解する

3. テストの計画を立てる
A. V 字モデルと発注者・委託先事業者の役割分担を把握する
B. テストのレベルや種類を理解する
C. リスクを踏まえてテストの方針を決める
D. テストにおける役割分担と必要な環境を明確にする
E. テストツールを有効活用する
F. テスト計画を作成する

ウォーターフォール型の開発プロセスでは V 字モデルが一般的です。テスト工程において、発注者側にはテスト計画を確認し、テスト実施状況を管理し、テスト結果を評価するという重要な役割があります。特に、総合テスト以降の工程終盤になればなるほど発注者側の関与が重要であり、受入テストは発注者自身が実施するものです。

設計・開発・テストの管理

設計・開発の大部分の作業は、事業者が行うことになりますが、PJMO が適切な関与を行わなければ、良い情報システムを構築することはできません。

1. 設計内容を確認・調整する
A. 基本設計の内容を確実にレビューする
B. 他の情報システムとのデータ連携には細心の注意を払う

設計書のレビューは、基本的に「基本設計」で作られた成果物を対象とします。基本設計以降は、基本設計に基づいて詳細設計や実装などが行われるため、それらの整合性を確認するのは基本的に事業者の責任範囲となります。情報システムの多くは他の情報システムとデータ連携を行います。そして、このデータ連携では、高い確率でさまざまな問題が発生します。問題を起こさないためには、まずは、他の情報システム側の担当者などとの協力体制を築くことが重要です。

2. 品質管理の考え方を理解する
A. 見えない品質を見える状態にする

品質は一見すると目に見えない概念です。品質を「見える」形にするために、テストの進捗や障害の発生件数、解決件数などを数値化し、グラフなどで可視化します。これにより、品質を確認できます。

3. 単体テスト・結合テストの品質を評価する

A. 単体テスト留意点

B. 結合テストの留意点

単体テストは開発者が自ら試行錯誤しながら実施するので、不具合件数は過少報告されがちです。結合テストは事業者が主体となって実施する工程ですが、発注者もテスト計画、テスト管理状況、テスト結果などについては積極的に確認する必要があります。

4. 総合テストの品質を評価する

A. 総合テストの留意点

B. 発見できた障害は最大限活用する

総合テストでは、業務観点からのいろいろなシナリオに基づいて機能テストを検証しますが、これに合わせてシステムの性能や信頼性などを検証する非機能テストを行います。総合テストの段階はリリースまでの残り日数が少なくなっていて、単体・結合テストと違って数日の遅延が致命的になるので、特に進捗管理には注意を払います。

5. 受入テストを実施する

A. 受入テストと他のテストとの違いを理解する

B. 受入テストのテスト計画書を作成する

受入テストは、他のテストと異なり、従業員が主体となって行う最終段階のテストです。「サービス・業務企画や要件定義で想定したとおりに情報システムができているか？」「構築された情報システムを用いて実際のサービス・業務を正しく実施できるか？」という観点で受入テストを行います。

見落としがちな活動に注意

設計・開発でしなければいけないことは、情報システムの構築だけではありません。本番で情報システムを稼動させ、サービス・業務の円滑な運営を行っていくためにはさまざまな活動が必要になります。

1. どのプロジェクトでも必ず移行を計画する

A. 移行の種類を理解する

B. リハーサルも考慮した移行計画書を立てる

情報システムの移行は、どのようなプロジェクトでも必ず発生します。既存のサービス・業務や情報システムが存在しない場合でも、本番の情報システムの構築、データの設定、切替え、新規業務の開始に関わる業務の変更などは必ず必要です。移行に関するポイントを理解することが大切です。

2. 次の運用・保守は開発と並行して検討する

A. 指標値を運用作業で取得できるように検討する

B. 運用・保守の計画を立てる

継続的な改善を行い、プロジェクト目標を確実に達成するためには、指標値の評価を容易に行えるようにして定期的に確認していくことが必要不可欠です。運用計画書、運用実施要領、保守計画書、保守実施要領などは、運用・保守事業者の調達仕様書の附属資料になり、運用・保守事業者の調達後に確定されることになります。

3. 種類を理解し揃えるマニュアルを厳選する

A. マニュアルの種類を理解する

新業務の運営を円滑に行うための準備

情報システムを無事に稼動させ、新しいサービス・業務の運営を円滑に行っていくために必要となる最終盤の作業を行います。

1. 本番移行と本番稼動の開始を承認する

A. 移行判定と稼動判定の違いを理解する

2. 正しき引継ぎを行い、トラブルを減らす

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

設計・開発を開始するための事前準備

設計・開発の具体的な活動を行うのは、調達によって選定された事業者です。事業者は、調達仕様書および附属資料である要件定義書をインプットに、設計・開発工程の活動を計画し、活動を行います。設計・開発工程の作業は、情報システムを対象とした専門的なスキル・経験が求められます。

従業員が関与しなければ、作業は順調に進みません。一般的に、従業員の関与が低いほど、設計・開発の成功確率は低下します。『専門的』でわかりづらい設計・開発工程の作業において、『従業員が関与する』ことで効果がある作業とは何かを理解する必要があります。従業員が作業に関与するに当たり、基本的な役割を以下に示します。

『設計・開発』を行う際の従業員の基本的な役割

- 要件の内容を事業者に正しく伝える役割

- 要件どおりに情報システムができたかを確認（テスト）する役割
- プロジェクトの進捗状況を正しく把握し、スケジュールや関係者間において発生する調整を適切に行う役割

「設計・開発」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点
第 3 編　第 7 章　設計・開発　Step3　設計・開発の計画
第 3 編　第 7 章　設計・開発　Step4　設計・開発・テストの管理

セキュリティ機能を実装・運用するためポイント

テスト計画の策定

情報システムの設計・開発では、品質の管理が重要であり、そのためには十分なテストが必要です。現在、ウォーターフォール型の開発プロセスではＶ字モデルが一般的です。開発プロセスには

各種の国際標準や国内標準もありますが、「標準ガイドライン」の工程定義に則っとると次のように表現できます。

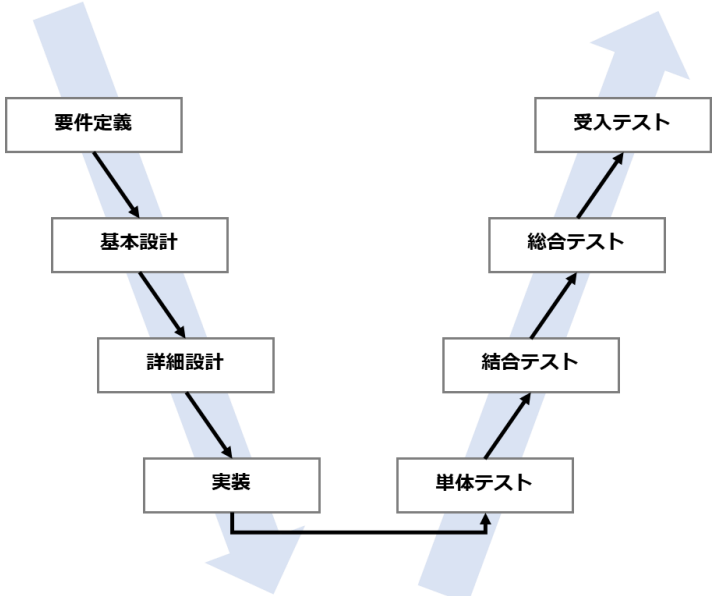

図 76. 標準ガイドラインの定義に則ったソフトウェア開発プロセスのＶ字モデル
（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

同じ高さにある工程が、それぞれ深く関係しています。例えば、総合テストとは基本設計で定めた要件が充足されているかを確認するテストであり、受入テストとは要件定義との充足性を確認するテストです。

テスト工程において、発注者側にはテスト計画を確認し、テスト実施状況を管理し、テスト結果を評価するという重要な役割があります。特に、総合テスト以降の工程終盤になるほど発注者側の

関与が重要であり、受入テストは発注者自身が実施するものであることに留意しましょう。

テストのレベルと種類

情報システムのテストは、段階的に進めていきます。例えば、「個々のプログラムが設計書どおりにできているか？」、「プログラムをつなげて機能としてみたときに、機能の設計を満たしているか？」、「機能同士をつなげてみたときに、要件を満たしているか？」、「要件どおりにできたが、業務が適切に遂行できるか？」など、徐々に確認するレベルを上げていきます。

これは、V 字モデルが表しています。標準ガイドラインで定義しているテスト工程では、次のように整理しています。

テスト工程	概要	発注者の関与の仕方
単体テスト	アプリケーションを構成する最小の単位で実施するテストであり、主に機能単位で設計どおりに動作するかを事業者（プログラマ）が確認する。	事業者がテストの実施主体ではあるが、発注者もテスト計画を確認した上で、実施状況の報告を求め、報告書に記載されている実施結果に不足、誤りなどが発生している場合は、課題などを整理し、指摘または指導を行う。
結合テスト	複数の機能を連携させて動作を確認するテストであり、主にユースケース単位で設計どおりに動作するかをテスト担当者が確認する。	（同上）
総合テスト	システム全体が設計のどおりに動作することを確認するテストであり、ユースケースを組み合わせた一連の業務が行えることを機能面や非機能面の観点からテスト担当者が確認する。	上記に加えて、テストシナリオやテスト評価方法の妥当性を確認し、過不足を指摘することで抜け漏れがないテストの内容になるように関与する。
受入テスト	納品されるシステムが要件どおりに動作することを確認するテストであり、発注者が主体となり、事業者と協力して確認する。	発注者が主体となりテストを実施する。実際の利用者がテストに参加することで、サービス・業務が円滑に実施できることを確認する。事前に要件を十分確認できるテストシナリオかを確認し、実際にテストシナリオに基づき情報システムを操作し、テスト結果が要件どおりであることを確認する。

テスト工程とは別に、テスト手法の違いがあります。

テスト手法	概要
ホワイトボックステスト	ホワイトボックステストとは、プログラム（ソースコード）の内部構造、論理構造を理解した上でその構造どおりに実装できているかを確認するテストです。中身が見えている状態で行うテストなので、ホワイトボックスと呼んでいます。プログラムを「作る」人の目線でのテストともいえます。基本的に、上述のテスト工程のうちホワイトボックステストを実施するのは単体テスト工程です。ホワイトボックステストでは、ソースコードがテストされた割合を示す「カバレッジ（網羅率）」が重要な指標となります。しかし、カバレッジには主として 3 つのレベルがあるので、どのカバレッジレベルを前提としているかについて注意が必要です。 （参考）カバレッジの種類 ● C0 命令網羅率：プログラム内の命令文をどの程度網羅したか ● C1 分岐網羅率：プログラム内の分岐をどの程度網羅したか ● C2 条件網羅率：プログラム内の条件をどの程度網羅したか 長所： ● 期待どおりの処理がされているかを網羅的に確認できます。 短所： ● 仕様自体の間違いや機能が備わっていないバグなどはホワイトボックステストでは検出できません。 ● カバレッジは必ずしも 100%を目指す必要はありません。100%に近づくほどコストが増大するので、適切にカバレッジを定める必要があります。
ブラックボックステスト	ブラックボックステストとは、プログラムの内部構造、論理構造に着目するのではなく、プログラムの入出力に着目します。プログラムの外側から見たときに仕様どおりに動作するかを確認するテストです。中身が見えない状態で行うテストなので、ブラックボックスと呼んでいます。プログラムを「使う」人の目線でのテストともいえます。基本的に、ホワイトボックステストの完了後に、さまざまな粒度や観点からブラックボックステストを実施します。

	長所： ● レイアウトが崩れていないかなど、実際に使用する観点でテストすることができます。 短所： ● 結果が正しい場合、処理上の不具合があっても見つけることが難しいです。

テストツールの活用

近年、情報システムの品質を向上させるためのツールは多く登場しています。これらを活用することで、設計・開発の活動を効率的に進めたり、効果的に品質を担保・向上させたりすることができます。事業者とも相談しながら、導入を検討することが重要です。

ツールの種類	概要	メリット
ソースコードの静的解析ツール	ソースコードから、機械的にコード規模（コード行、スペース行、コメント行など）、複雑度、複製度/重複度、正当性、セキュリティ観点からの好ましくない行、パターンなどを機械的に抽出するツール。	静的解析ツールは、ソースコードレビュー（インスペクションともいいます）を助け、コード品質の向上、レビューワの負荷軽減、期間短縮に効果を発揮します。 コード特性を可視化することができるため、全体を俯瞰しながら個々の問題や指摘箇所について検討できます。このため、プログラマはツール結果を見ながら自分で問題点を検討し、修正できます。一人では解決できない場合も、レビュー時にレビューワにツール結果を見せることにより、レビューワも問題の特定が容易となり作業負荷の軽減、時間の短縮につながります。
自動テストツール	ソフトウェアテストを行うための作業（テストケース	効率よく自動テストを実行するよう、スケジューリングす

	の設計、テストの実行と結果の確認、テストの進捗管理、レポートの作成）またはその一部を自動化するツール。	ることで、手動でのテスト工数を削減することが可能です。
継続的インテグレーション	コンパイル・テスト・デプロイといったソフトウェア開発のサイクルを頻繁に繰り返し実行する手法。	短期間で品質管理を行うため、問題の早期発見や開発の効率化が可能です。
タスク管理ツール	プロジェクト全体のタスクを管理することができ、進捗の見える化や共有化などにより、タスクを管理しやすくするツール。	タスクのツリー構造を定義し、整理することができます。また、タスクの順序や優先度合いを設定し、スケジュール管理できます。 スケジュールや進捗具合を、自動でガントチャートなどのグラフ化で表現でき、直感的に状況を把握することができます。

20-1-8. サービス・業務の運営と改善

サービス・業務の運営と改善の全体の流れは以下の通りです。

サービス・業務の運営と改善の全体の流れ
新しいサービス・業務の事前準備
新しい情報システムを利用してサービスや業務を実施する際、PJMO の従業員は情報システムを構築することに意識が行きがちです。一方、利用者にとっては、情報システムが構築直後に「満足な出来」であることは少なく、大なり小なり期待値とのギャップがあります。これを解消するため、利用者からのフィードバックを得ながら、業務と情報システムの双方を改善していく活動を継続していくことが重要です。 1. 運営と改善は、従業員主体の作業である A. 『サービス・業務の運営と改善』を外部の事業者に丸投げしない B. 『サービス・業務の運営と改善』は他工程の作業と並行で実施する

C. 関連する業務実施部門との責任分担を意識する

2. 業務手順書はさまざまな用途に有効活用できる
   A. 業務マニュアルと他のマニュアルとの違いを理解する

3. リハーサル計画・シナリオは従業員目線で
   A. 移行リハーサルを計画・実施する
   B. 業務リハーサルを計画・実施する
   C. サービスの開始や変更を利用者に確実に周知する

業務の定着と次の備え

新しい業務を開始すると、その業務をできるだけ早く現場に定着させ、業務の効率を上げることが求められます。利用者に積極的に使ってもらうための工夫も、定着に向けたカギとなります。また、データマネジメントの観点を意識しながら、業務で取扱うデータの品質を維持していかなければ、肝心なときに必要な情報が取得できなくなり、業務を効率化できない割に運用・保守コストだけがかかるような、使えない情報システムになりかねません。

1. 従業員に継続的な教育を行う
   A. 研修・教育の準備を十分に行う
   B. 研修・教育は 1 回では定着しない

2. 定着には利用者への働きかけが必要

3. 業務で扱うデータの品質を確保する
   A. 計画どおりにデータを入れないと情報システムの価値はない
   B. 分析しやすいデータ構造でないと、何かするにもカネがかかる

4. 業務改善に向け日常業務の事実を蓄積する
   A. PJMO・従業員がさまざまな情報を収集し、定常的に管理する
   B. 情報システムのログなど、運用活動に関わる情報を取得可能にする
   C. 効果測定ができるように KPI を自動的にとれるようにしておく
   D. 多数のインシデントや要望などの対応の優先度をつける

業務の改善

業務の改善は、日常的に改善できるものと、情報システムや業務そのものなど、時間をかけて見直すものがあります。

1. 日常業務中でも改善できることを理解する
2. 検討の進め方を理解する

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

（例）：業務の定着と次の備え

新しい情報システムがリリースされると、サービス・業務の運営が始まります。新しいサービス・業務が今までのものと違いがあるほど、リリース直後からしばらくの間はさまざまな問題が発生するかもしれません。業務に関わる従業員は、できるだけ早く業務を現場に定着させようと悪戦苦闘しますが、それ以外にも、より良いサービス・業務となるような活動を併せて行う必要があります。

従業員に継続的な教育を行う

PJMO は、情報システムの設計・開発のリリースが近づいたところで、それまで準備した研修教育資料を用いて、実業務を担当する従業員に対して教育を実施します。

研修・教育の準備を十分に行う

PJMO は、研修資料として、PJMO 主導で作成した業務マニュアルや、事業者主導で作成した情報システムの操作マニュアル、それらをまとめた研修用資料などを準備します。また、可能であれば、デモ環境や研修環境なども用意し、情報システムを実際に触れる環境を提供することも効果的です。

広範囲の従業員が利用する情報システムにおいては、PJMO やヘルプデスクを担当する事業者も、研修・教育の準備期間中に、一般従業員と同じ研修を受講しておくことが望まれます。これにより、研修カリキュラムの改善につながることはもちろん、利用者からの問い合わせに的確に対応できるようになります。

情報システム構築の作業進捗状況が遅延すると、研修や教育の回数制限、期間の短縮や、現場担当者が新しい情報システムに触れられる環境の準備が遅れる可能性が出てきます。PJMO は研修や教育に最低限必要な期間は必ず確保できるように、構築事業者の進捗管理をチェックし、安易な計画変更を起こさないようにすることが重要です。

研修・教育は 1 回では定着しない

通常、新しい情報システムのリリース前に行う教育は、開発実施計画を立てる時点でしっかり盛り込まれていれば、作業が抜け漏れることなく実施できます。

研修や教育は、どのぐらいの頻度で実施すれば良いのかといった、計画を立てる際に気をつける

べき注意点を以下に挙げます。

現場への研修・教育を計画する際の注意点

- 大規模システムの場合、全国各地に業務担当者が散らばっていることが多く、実施回数が少ないとそのタイミングで教育を受けられない担当者が発生する可能性が出てくる。
- 研修・教育の回数が制限されていると、情報システムリリース後、新しく人事異動で配属された従業員が、正しい情報を把握することができなくなる。
- 教育資料や教育の内容が不十分な場合、そのまま同じように全従業員に情報が伝達されても、全体のレベルが上がらない。

この懸念点を払拭するには、次の対策をとることが効果的です。

懸念点への対策

- 研修を実施した後、受講者にアンケートを配布し、研修の内容・難易度に関する意見をもらい、それをもとに研修のカリキュラムや資料の内容を見直す。
- 研修に用いた教材を関係者が閲覧できるようにする、電子ファイルをダウンロードできるようにするなど、研修に出られない人にも研修の内容が伝わるように工夫する。
- 研修そのものを撮影し、オンラインにてストリーミング配信できるようにする、DVD に焼いて配布するなどの対策を検討する。

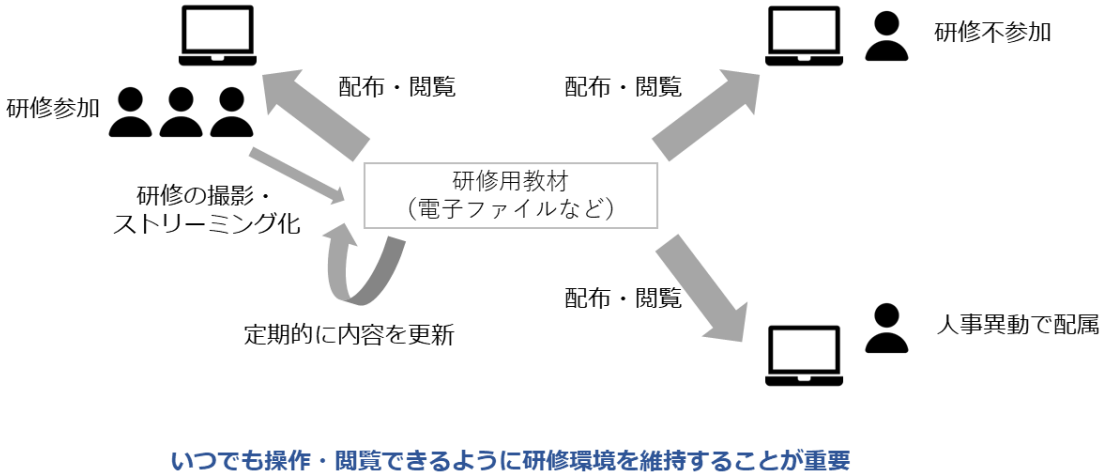

図 77. 研修・教育の定着化に向けた取組

（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

「サービス・業務の運営と改善」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点

第 3 編 第 8 章 サービス・業務の運営と改善 Step3 業務の定着と次の備え
第 3 編 第 8 章 サービス・業務の運営と改善 Step4 業務の改善

セキュリティ機能を実装・運用するためポイント

業務を外部委託する際の注意

サービス・業務を運営する中では、業務・サービスに関連する日常的なオペレーションはもちろんのこと、問い合わせや要望への対応、利用促進のために周知や広報活動を行うなど、さまざまな活動を従業員が主体的に実施します。
ただし、一部の作業については、従業員が正しく作業を切り出し指示や管理をすることを前提に、外部の事業者に作業を委託できるものがあります。例えば、業務で発生するデータの入力業務や、帳票の仕分け業務などです。
どのような業務が事業者への委託に向いているのか、一般的には、次の図のような考え方ができます。

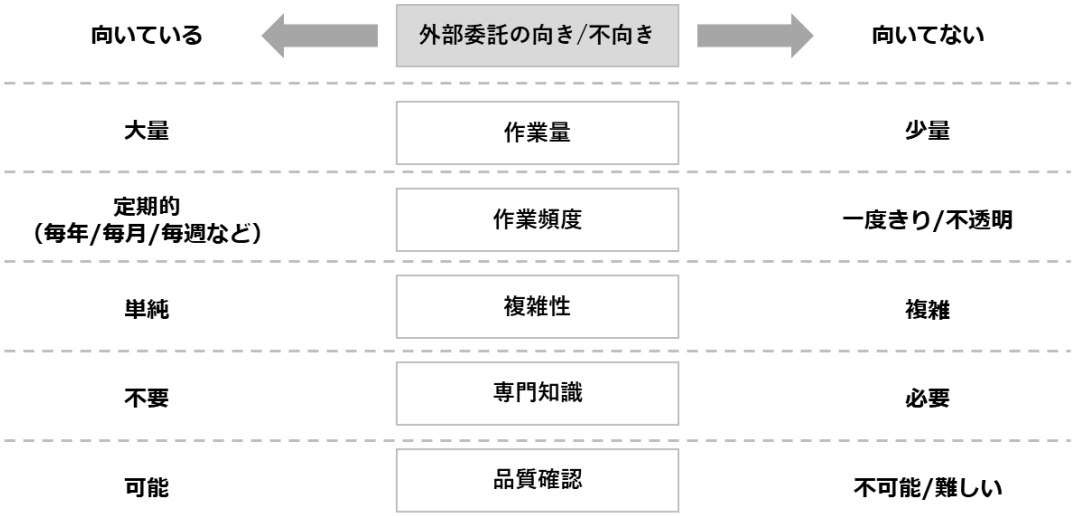

図 78. 外部委託の向き／不向きの判断例
（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

業務を外部委託する際の注意点

- 外部委託する業務は、従業員が主体的に行う業務に対する支援や補助となる作業であり、それを行うことで従業員の業務効率が向上するものであること。
- 外部委託した業務成果の正誤や品質状況を従業員が判断できるように、プロセスの透明化と必要十分な報告・記録を確保すること。
- 外部委託した業務の実施方法や、事業者が作成する業務マニュアルなどの内容を適宜確認し、従業員自身も業務の概要を理解し続けること。
- 特定のサービス・業務について、異なる作業範囲や役割を複数の事業者に外務委託する場

合は、緊急時（システム故障やセキュリティインシデントなど）に備えて、できるだけ特定の事業者に業務統制的な役割を定義しておくこと。

インシデントの優先度つけ

業務に関する問い合わせやインシデント、要望などを取りまとめていくと、膨大な量になり、すべてを対応するのは時間もコストも足りません。そのため、それぞれを整理した上で、優先度をつけて、優先度の高いものから対応していく必要があります。

優先度は、業務遂行上で重要か否かを判断してつけることが大切です。例えば、画面を複数切り替えないと関連する情報が確認できず、件数が多くて作業が非効率ということであれば、情報システムの改善による業務の効率化を検討すべきかもしれません。しかし、単純に画面レイアウトや操作性などについての要望は、個人の好みに依存することが多く、改善効果は見込めません。また、利用者側が業務を遂行できない、または多大な事務作業が発生する不具合に対応できないような場合は、そもそも情報システムの利用を推奨するべきではなく、業務の見直しも含めた検討が必要になります。

インシデントの優先順については、過去のインシデント分析にて、起こっている問題を詳細に分析することで、クリティカルな部分を優先して対策することが効果的です。インシデント分析は、一部をサンプリングして全体を理解するのではなく、全数を調査・分析して全体を捉えることが重要です。サンプリングして行う調査・分析は、コストをかけず実行することができますが、サンプリングから漏れる少数の事実が全体に影響を与える場合があるためです。

20-1-9. 運用および保守

運用および保守活動全体の流れは以下の通りです。

運用および保守の全体の流れ

運用・保守を開始するための事前準備

情報システムが完成したら、サービス・業務を滞りなく提供していくために情報システムをしっかりと運用・保守する必要があります。より良い運用・保守を行うためには、事前準備が必要です。

1. 「運用と保守」の位置づけを理解する
    A. サービス・業務をより改善するための活動を行う
    B. 情報システムの運用と保守の活動を理解する
    C. 運用・保守は他のさまざまな活動と連携し、平行で実施する
    D. 運用・保守に、自動化の仕組みを取り入れる

E. システム間での運用統合を検討する

運用とはサービス・業務を実現するための「情報システムの機能を利用者に提供し続けるための活動」です。効果的なサービス・業務を実現するためには、運用・保守フェーズにおけるヒヤリ・ハット（インシデント）を多く見つけ、改善を繰り返すことが重要です。また、人による体制で運用・保守を行うと人件費がかさみ、運用保守のコスト増となるため通常システム運用管理ツールなどを導入して自動化による効率化を図ります。

2. 作業責任を正しく理解しトラブルを防ぐ

A. 外部委託事業者へ依頼する作業の内容を明確にする
B. 指標の基礎データを誰がどのように集めるかを明確にする
C. 業務実施部門を含めた運用退背を確立する
D. 障害発生時の役割分担に注意する

「運用」および「保守」に係る作業は、基本的に外部事業者に委託して実施します。外部事業者に依頼する作業や役割は、調達の段階で調達仕様書に明記しておく必要があります。また、いくつかの指標（KPI）を用いて判断し、業務の改善や見直しを行います。このほか、情報共有や障害発生時の役割分担などを事前に取り決めておくことが大切です。

運用・保守の計画

運用・保守を実施する事業者が決まったら、最初にすべきことは契約期間中の実施計画を立てることです。

1. 運用と保守の計画を作成する

A. システムプロファイルに応じた運用・保守レベルにする
B. セキュリティ関連作業を定期的に確実に実施する
C. プロジェクトの目標や指標の評価に必要なデータは必ず取得する
D. 非機能要件に関連するデータを網羅的に詳細に取得する
E. 会議体は目的を明確にして必要最低限に抑える
F. 定例会の報告フォーマットを指定して、効率性を上げる
G. 運用・保守の工数を把握し、人件費をモニタリングする
H. 運用・保守における変更管理を理解する

運用・保守体制については、システムプロファイルで示した運用・保守レベルを維持できる最低限の体制を基準として、プロジェクトの状況に応じて定期的に見直しを行い、徐々に適切なレベルの保守・運用にしていくように調整します。また、会議や報告の効率化を進めます。

運用・保守の定着と次の備え

運用・保守のほとんどの作業は事業者が実施することになりますが、PJMO が適切な関与を行

わなければ、より良い運用・保守に改善していくことはできません。

1. 運用定例会議を有効活用する

A. 運用保守定例会議で確認する内容を理解する

運用保守定例会議では、運用・保守の計画で定めた報告フォーマットにしたがって、事業者から報告を受けることになります。報告を受け取るだけではなく、報告が不十分なものは、指摘・再提出も求め、改善活動につながる課題や改善点を報告内容から見出すことが大切です。毎回同じ項目が定期的に報告される特徴から、長期間にわたる推移を把握することも可能です。

2. 変更を管理し改善活動などの初動を楽にする

設計書などから現状の情報システムがどのようになっているかを確認し、プロジェクトの事情に合わせて、効率的に管理できる方法を検討する必要があります。

3. 情報システムで起こった事実を蓄積する

A. 運用・保守の範囲にとらわれず、意味のある情報を取得する
B. 情報システムの活用状況を詳細に把握し提供する機能を棚卸する
C. 情報システムのログやトランザクションデータから改善のための情報を取得できるようにする
D. 運用・保守実施記録を適切に保管する

運用・保守の改善と業務の引継ぎ

運用・保守の実施中に判明した課題は、定常的な作業の中で改善ができるものは積極的に改善していきます。

1. 適切な時期に的確に改善を実行する
2. 要員の交替で情報が欠落しないようにする

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

例：作業責任を正しく理解しトラブルを防ぐ

運用・保守の活動やそれに係る「サービス・業務の運営と改善」などの活動には、さまざまな関係者が関わります。それぞれの作業内容や責任範囲が曖昧になってしまうと、作業漏れや関係者間の意思疎通が不十分となることによる新たな問題が発生するリスクが増大します。悪くすると、情報システムの安定的な稼動への問題発生、改善活動の停滞などを招き、プロジェクトの目標達成に

影響が出てしまいかねません。

外部委託事業者へ依頼する作業の内容を明確にする

「運用」および「保守」に係る作業は、基本的に外部事業者に委託して実施します。その理由は、内容が専門的であることや、手順に沿った定型かつ大量な作業が多いため、PJMO や業務実施部門の従業員が実施すると、かえって非効率になる可能性があるためです。外部事業者と役割を適切に分担することにより、発注者側の従業員は、業務の質向上やコスト削減などの、本来従業員が行う事業者では実施できない作業に、より注力することができます。

外部事業者に依頼する作業や役割は、調達の段階で調達仕様書に明記しておく必要があります。事業者確定後にこれらの詳細を詰めようとすることは、トラブルの原因となりますので、注意が必要です。

指標の基礎データを誰がどのように集めるかを明確にする

指標に用いるデータを取得するための作業は、標準ガイドライン「第 8 章サービス・業務の運営と改善」の作業と密接に関連します。サービス・業務の運営と改善では、プロジェクト計画書で定めたプロジェクトの目的・目標が実現できているかに関して、いくつかの指標（KPI（Key Performance Indicator））を用いて判断し、業務の改善や見直しを行います。指標（KPI）は、基礎値の組み合わせによって、表されます。

指標のもととなる各種データは、種類ごとに、取得先、取得手段、取得頻度などについて詳細な検討が必要です。代表的なデータとして、情報システムが稼動している際に作り出されるログやトランザクションデータと呼ばれるものが挙げられます。これらは、従業員が自ら取り出せるもの、運用事業者に依頼しないと取り出せないものなど、データの取得には制約が発生します。前者であれば、事前に技術的な経験のない従業員でも容易に取得できるように、取得手段が機能化されている必要があります。後者は対象と取得手順が明確に定義されていなければ、定常的な運用作業として継続できません。

これらを踏まえて、取りこぼしが発生しないよう、必要なデータ項目を事前に把握するとともに、外部事業者に取得を求める場合は調達仕様書に明記しておくことが大切です。

指標は、いざ算出しようしたときに、算出根拠となる基礎情報が不足していることが判明し、その情報を追加入手するためには想像以上に困難であることに気づくことがあります。特に、ある分析結果からより多角的な分析が必要になった場合、特定の情報に対する付加情報として「区分」や「属性」など、より詳細な情報が求められることがあります。このような情報は、事前に取得・保管する仕組みが備わっていなければ、その時点から遡ってデータを取得することが不可能なこともあります。また、取得可能だったとしても、多くの手間を必要とする場合もあり、そのようなデータは頻繁なモニタリングが敬遠され、結果として指標が適切な時期に算出できず、対策が遅れてしまうことにもつながりかねません。

運用・保守を開始してからトラブルとならないよう、事前に具体的なモニタリングの方法や役割分担を検討し、事業者に依頼する場合は調達仕様書に作業内容を明記することが重要です。

また、平均値を指標とするときは、集計対象の種類や内容が同種のもので平均値を算出するようにし、異なる性質のものを混合して値を算出しないようにすることが重要です。

参考：主な指標とデータの関係例

No	指標名	計算式	単位
1	利用者満足度	「「満足」とした回答数」／「全有効回答数」×100	%
2	相談窓口の平均対応時間	相談窓口の平均対応時間	分/回
3	相談窓口における苦情・相談解決率	「相談窓口で解決した件数」／「全苦情・相談件数」×100	%
4	相談窓口におけるエスカレーション件数の逓減率	（「前年度エスカレーション件数」－「当該年度エスカレーション件数」）／「前年度エスカーション件数」×100	%/年
5	窓口申請に要する費用	窓口申請に要する費用	円
6	オンライン申請に要する費用	オンライン申請に要する費用	円
7	従業員満足度	「「満足」とした回答数」／「全有効回答数」×100	%
8	従業員苦情・相談件数	従業員苦情・相談件数	件
9	従業員苦情・相談解決までの平均時間	苦情・相談解決までの平均時間	分/回
10	削減業務処理時間	「現行業務処理時間」－「業務・サービス改革実施後の業務処理時間」	時間
11	削減経費	「業務・サービス改革実施前の経費」－「業務・サービス改革実施後の経費」	円
12	開発経費削減率	（「基準開発経費」－「当該開発経費」）／「基準開発経費」×100	%
13	運用経費削減率	（「基準年度年間運用経費」－「当該年度年間運用経費」）／「基準年度年間運用経費」×100	%
14	保守経費削減率	（「基準年度年間保守経費」－「当該年度年間保守経費」）／「基準年度年間保守経費」×100	%

15	業務・サービス委託経費削減率	（「基準年度年間委託経費」－「当該年度年間委託経費」）／「基準年度年間委託経費」×100	%
16	コンバージョン率	購入者／サイト訪問者	%
17	売上高の増加率	「今年度総売上高」／「基準年度総売上高」	%
18	利益の増加率	（「今年度総売上」―「今年度年間経費」）／（「基準度総売上」―「基準度年間経費」）	%

（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

業務実施部門を含めた運用体制を確立する

情報システムの各種テストが完了し、後は本番リリースを迎えるだけという状態に準備が整い、運用・保守フェーズを任せる事業者が確定したら、サービス・業務を利用者に提供するまであと一歩です。運用・保守フェーズでは、最初に司令塔となる PJMO を含んだ運用統制を行うチームを構築し、プロジェクトを管理していくことになります。円滑な運営を進めるためには、注意点があります。業務実施部門（主に当該情報システムの業務統括部門）とのコミュニケーションと役割分担です。

業務実施部門には、情報システムを用いて実際に業務を行う従業員が集まっています。この多くの従業員に、プロジェクトの目的・目標を理解してもらうことは、標準ガイドライン「第８章サービス・業務の運営と改善」で触れています。運営に入ってからは次の点に気をつけて実施することが重要です。

業務実施部門との役割分担・コミュニケーションで気をつける点

- PJMO には、業務実施部門の担当者が参画するよう、組織を組成します。運用・保守に関わる定期報告会では業務実施部門の担当者（代表者）が参加した上で、常に情報を共有できるようにします。
- 日常的に、現場業務で発生した問題や状況に関する情報が PJMO に伝わるよう業務実施部門の担当者とのコミュニケーションルールを明確にしておきます。

業務実施部門と PJMO との関わりについては、プロジェクト立ち上げ時の PJMO の組成にまでさかのぼります。そこでは、基本的に PJMO には制度所管部門および情報システム部門とともに、業務実施部門の担当者が参画することが望ましいことが言及されています。

これまでは、新しいサービス・業務の要件を定めるために、業務実施部門の従業員から意見・要望を収集することが主でした。しかし、サービス・業務の運営フェーズになると、コミュニケーションの流れが、収集だけではなく、業務実施部門からの情報提供が加わります。

利用者からの意見や要望を把握するためには、最も接点が多い業務実施部門の従業員からの情報提供が欠かせません。また、運用・保守で発生した報告内容には、利用者からの問い合わせや発見した不具合、不具合修正に伴う情報システムの稼動停止連絡など、さまざまな情報が含まれます。

これらを業務実施部門と共有することにより、業務実施部門の中で必要な調整や対策を行い、今後問題を引き起こすリスクを低減させることが可能となります。

そのためにも、プロジェクトの情報が集まる PJMO への参画、定期報告会への必要な人員の出席、代表者から業務実施部門の関係者全員への情報伝達手段などを、運用および保守が開始する前に取り決めておくことが重要です。

障害発生時の役割分担に注意する

障害が発生しない情報システムは、ほぼありません。大切なのは、障害が発生した際に適切な対応をとることで被害を最小限に留め、暫定対策から恒久対策を実施し、将来にわたって同じまたは同じような障害を発生させないようにすることです。そのためには、障害対応という急を要する状況の中でも、PJMO、運用の事業者、保守の事業者、そのほかの関係者が適切な役割分担の下に協働して対応を進めていくことが必要になります。運用と保守の事業者が異なる場合や、運用・保守それぞれを複数事業者で分担して実施する場合もあり、役割や責任が曖昧になることで対応が遅くなってしまうことや被害が拡大してしまうことも多いです。

まずは、障害発生時における運用と保守の基本的な役割分担を理解することが重要です。この考え方を踏まえた上で、プロジェクトの体制や特性を踏まえて、詳細を決めていきます。

極端な例ですが、PJMO の体制が 1 名の場合は、24 時間 365 日稼動するサービスへの対応は十分にできません。どのようなタイミングで障害が発生するかは予想できないからです。深夜や休暇取得中など、PJMO が対応できない状況が存在することを前提に、運用事業者・保守事業者と役割分担を検討する必要があります。

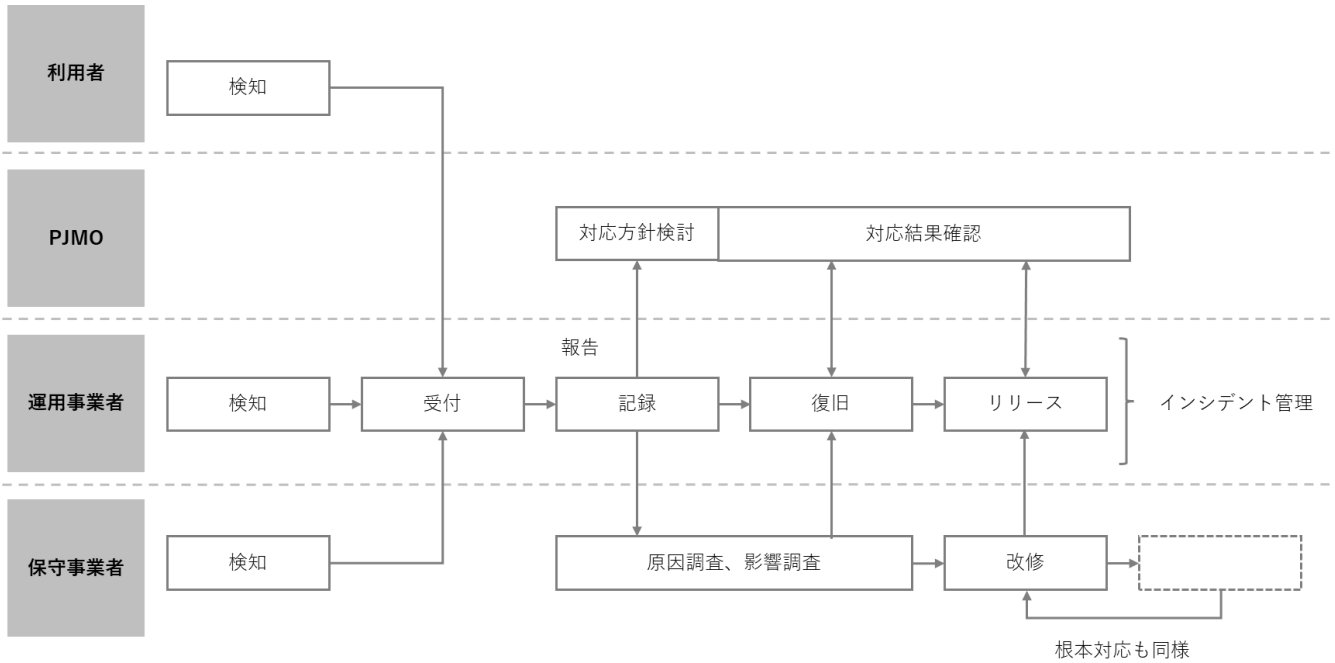

図 79. 障害発生時の運用と保守の役割分担の例

（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

「運用および保守」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点
第 3 編 第 9 章 運用および保守 Step3 運用・保守の計画 第 3 編 第 9 章 運用および保守 Step5 運用・保守の改善と業務の引継ぎ

セキュリティ機能を実装・運用するためポイント

セキュリティ関連作業を定期的に確実に実施すること

セキュリティ管理に関する要件は、非機能要件で示され、運用・保守フェーズでは、その方針に沿ってアプリケーションやインフラでの対策が講じられている状態にあります。昨今のセキュリティに対する脅威は日々増大しており、運用・保守フェーズでは、設計どおりの対策が維持できるよう、日々確実に作業を続ける必要があります。

以下に定期的に実施すべき作業の例を挙げます。

- セキュリティインシデント発生時の記録、対応、影響範囲の把握
- 脅威と修正パッチ適用計画の立案・調整
- シグニチャ、ブラックリスト（ホワイトリスト含む）の更新
- OS およびプラットフォームなどの緊急修正計画の立案・調整
- セキュリティ向上のための業務改善と利用規制検討
- 中長期的プラットフォーム改善に向けた、システム構成要素のリスク評価

セキュリティ対策会議の実施

運用・保守フェーズは、複数の従業員や事業者が関わるため、会議体の種類がどうしても多くなる傾向があります。中心的な役割を担う PJMO の従業員や事業者の担当者は、会議出席に拘束されてしまい、本来行うべき作業に手が回らないという状況に陥りがちです。そのような状況にならないために、会議体の目的を整理し、必要な出席者を事前に選抜することが重要です。

- 会議の例：セキュリティ対策会議（月次～四半期）
- 主な目的・内容：
- インシデント発生状況の共有
- 脅威と修正パッチ計画の調整
- シグニチャ、ブラックリスト（ホワイトリスト含む）の更新調整
- OS およびプラットフォームなどの緊急修正計画調整

● セキュリティ向上のための業務改善と利用規制検討・承認

情報システムのアカウントの管理

発注者が運用・保守事業者に対して一定期間の運用・保守実施記録の保管を指示していないなど、情報システムのアカウント管理を運用・保守事業者に丸投げしている場合には、いざという時に必要な記録が参照できず、不正、障害などの原因が究明できないなどの問題が生じる可能性があります。
上記のリスクを低減する方法として、情報システムのログやトランザクションデータを適切に取得・保管することなどが挙げられます。
機密性・完全性・可用性の観点から特に重要な情報を取扱う場合においては、発注者が特権 ID 管理を適切に実施することが重要で、事業者の作業計画に基づいて作業のたびに特権 ID を発注者が事業者に付与する運用とすることが望ましいです。

アカウントの管理や情報の保管は、情報システムの特性に応じて、「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」や特定非営利活動法人日本ネットワークセキュリティ協会の「【改定新版】特権 ID 管理ガイドライン」を参考にしながら、事前に十分に検討した上で、実施してください。

※特権 ID とは：
特権 ID とは、情報システムを運用・管理するために必要なすべての操作権限を持つ管理者用アカウントのことです。悪意を持った人が特権 ID を使用した場合、不正やセキュリティ上のリスクなどが懸念されるため、発注者の責任下で、特権 ID の取扱いには十分に注意が必要です。

詳細理解のため参考となる文献（参考文献）	
政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf
【改定新版】特権 ID 管理ガイドライン	https://www.jnsa.org/result/digitalidentity/2024/index.html

20-1-10. システム監査

システム監査の全体の流れは以下の通りです。

システム監査の全体の流れ

システム監査の理解

システム監査を行う前に、理解すべき監査の目的・活動や、必要な事前準備の内容について理解します。

1. システム監査とは何かを理解する
    A. 監査の種類を理解する
    B. システム監査は問題解決の近道となる
    C. システム監査基準・システム管理基準を理解する

2. システム監査の全体像を理解する

3. 適切な監査が行える体制を作る

システム監査計画と監査実施計画

監査体制は、組織全体のシステム監査計画をもとに対象のプロジェクトを監査するための実施計画を立案します。

1. 複数年の監査計画を立てる

2. システム監査実施計画書を作る
    A. 監査範囲が局所的にならないように注意する
    B. 監査実施方法に注意する

システム監査の実施

監査体制は、システム監査実施計画に則りシステム監査を実施します。

1. 予備調査を踏まえ監査手続きを具体化する
    A. 監査手続書を作成するまでの流れをつかむ

2. 根本原因を究明し改善点を発見する
    A. インタビュー時には情報を上手に引き出す
    B. 改善提案は報告の場で具体的な例を混ぜながら行う
    C. システム監査報告書の様式を把握する

指摘事項を踏まえた改善

PJMO は、監査実施者からのシステム監査報告書の指摘を踏まえて改善を行います。

1. 改善計画を立て改善を行う

1

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

例：システム監査の理解

監査の種類を理解する

「監査」と聞くと、会計検査院が実施する会計検査や、会社法、金融商品取引法に基づく財務諸表監査を思い出すかもしれません。これらは、会計監査に当たります。標準ガイドラインで扱うシステム監査は、業務監査の一部に位置づけられます。また、監査人が誰かにより監査が分類されることもありますが、その分類においては内部監査に当たります。

また、システム監査と混同しがちな監査に、情報セキュリティ監査があります。情報セキュリティ監査は、元々はシステム監査における監査テーマの一つであり、近年、情報漏えいなど、多くの情報セキュリティに関する事件・事故が多発してきた結果として、情報セキュリティに特化した監査として定着してきているものです。

図 80. 一般的な内部監査における各監査の関係性

（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

システム監査は問題解決の近道となる

システム監査は、中小企業においてもプロジェクトの目標達成を確実にするための重要な活動です。日々の業務に追われ、効率重視のあまり、プロジェクト本来の目的を見失うことがあります。例えば、当初の目的から逸れて手段が目的化してしまうこともあります。このような状態を放置してしまうと、情報システムが意図したどおりに構築・改修されない、不必要な機能構築や人件費の積算、不適切な業務・システム運用の定着、情報漏えいなど、さまざまなリスクが発生し、プロジェクト目標が達成されないおそれがあります。

システム監査は、これらのリスクを未然に防ぐため、プロジェクトの進行状況を客観的に点検・評価し、改善するための活動です。これは、PDCA サイクルにおける「C」（チェック）に該当します。

システム監査では、単に「不具合が発生しているから問題だ」という表面的な評価ではなく、そ

の原因を突き止めます。例えば、「不具合を解決するためのプロセスや体制に問題がある」、「不具合が発生しやすいプロセスになっている」などの根本的な原因を評価します。

どのような目的で監査を行うか、何を評価するかは、組織内の担当者が決定し、システム監査の組織全体に対する計画である「システム監査計画書」としてまとめます。監査の対象となるプロジェクトもこの中で定めます。

監査の実施に当たってのポイント

規模が小さい企業の場合、大企業（あるいは政府機関）のような内部監査体制を整えることは、事実上困難です。無理にそのような体制を構築すると、中小企業の長所である「小さな組織ならではの効率性」「経営者と従業員の一体感」「迅速な意思決定」「市場などの変化に対する迅速な対応力」などが損なわれる可能性があります。

中小企業が監査を実施するためのポイントを 3 つ紹介します。

- 経営者の主導と外部専門家の活用
  内部監査のもつ意味を正しく理解した経営者自身が監査を行うか、または必要に応じて経営者から委託された外部の専門家（会計士、システム監査士など）を活用することで、効果的な監査を実施できます。

- シンプルで実用的な監査プロセスの導入
  チェックリストや定期的なレビューなど、簡易的で中小企業に適した監査プロセスを導入するなど、無理なく監査を継続する仕組みを作ることも効果的です。

- 法令順守とリスク管理に重点を置く
  法令順守（コンプライアンス）とリスク管理を中心に監査を行い、企業の安全性と持続可能性を確保することも効果的です。

「システム監査」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点
第 3 編　第 10 章　システム監査　Step.2　システム監査の理解

セキュリティ機能を実装・運用するためポイント

情報セキュリティ監査

情報セキュリティ監査は、元々はシステム監査における監査テーマの一つであり、近年、情報漏えいなどの多くの情報セキュリティに関する事件・事故が多発してきた結果として、情報セキュリティに特化した監査として定着してきているものです。

20-2. アジャイル開発

20-2-1. アジャイル開発の概要

アジャイル開発の必要性

現代は、人や組織を取り巻く環境が、複雑さを増し、将来の予測が困難な VUCA（ブーカ）（VUCA：Volatility（変動性）、Uncertainty（不確実性）、Complexity（複雑性）、Ambiguity（曖昧性））の時代」だといわれています。

複雑な問題を解決する論理的に導ける最適解はありません。従来のような問題を分析して解決する方法ではなく、観察とフィードバックによってあるべき姿に向けて改善、進化し続ける必要があります。こうした背景から「アジャイル開発」が注目されています。

当初アジャイル開発は、ソフトウェアエンジニア主体の開発手法でしたが、近年は不確実さに対応するビジネス戦略としても採用されています。つまり「アジャイル開発」の考え方は、ソフトウェア開発だけでなく、ビジネス戦略などにも活用できるものになっています。

アジャイル開発とは

アジャイル（Agile）とは、直訳すると「敏捷」「素早い」などの意味を持ちます。アジャイル開発は、新しい機能を短期間で継続的にリリースするソフトウェア開発のアプローチです。従来のアプローチ方法は、試行錯誤に向いていません。そのため、状況変化への対応を繰り返す適応するアプローチ方法であるアジャイル開発が有用であると考えられます。

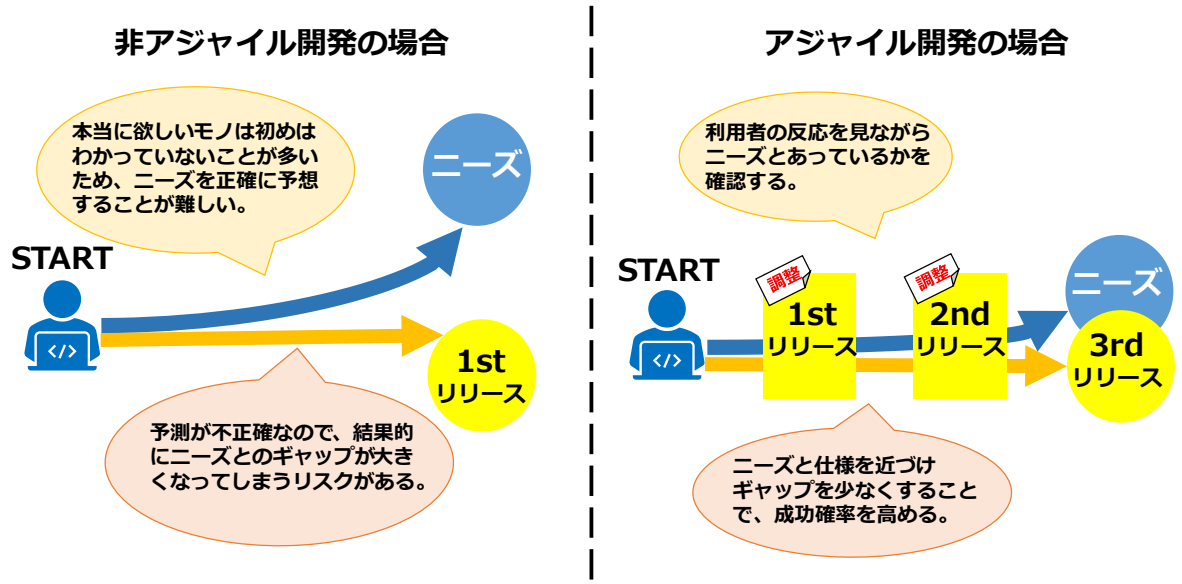

図 81. 非アジャイル開発とアジャイル開発の違い

アジャイル開発では、作成したアウトプットの基づき、情報システムの挙動がどうあるべきかを検討、判断し、その次に取り掛かる開発行為を最適化します。また、アジャイル開発は従来の開発スタイルとは異なり、すべての要求、仕様を言語化し、事前のドキュメントとして整備することなく開発を行うこともできます。ドキュメントで定義しなくとも、短期間のスプリントで得られるアウトプット（インクリメント）が、動くシステムそのものとなり得るためです。ドキュメントの作成にかける手間を最小限に留め、情報システムそのもので動作確認を行うことで、要求の確認から設計、開発、テストまで、情報システムの機能追加を短い期間で行うことができます。また、アジャイル開発には、下記のような意義があります。

アジャイル開発の 9 つの意義

① フィードバックに基づく開発で、目的に適したシステムに近づけていく
② 形にすることで、関係者の認識を早期に揃えられる
③ システム、プロセス、チームに関する問題に早く気づける
④ チームの学習効果が高い
⑤ 早く開発を始められる
⑥ システムの機能同士の結合リスクを早期に解消できる
⑦ 利用開始までの期間を短くできる
⑧ 開発のリズムが整えられる
⑨ 協働を育み、チームの機能性を高める

前述の 9 つの意義を十分発揮するためには、以下の前提をチームおよび関係者間で確認する必要があります。前提を理解して取り組むことでスムーズに進めることができます。

9 つの意義を十分に発揮するための前提

① 常にカイゼンを指向すること
② 対話コミュニケーションの重視
③ 情報システムの変更容易性を確保し続ける
④ 利用者目線で開発を進める

詳細理解のため参考となる文献（参考文献）	
DS-121 アジャイル開発実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9fc931f7/20220422_resources_standard_guidelines_guidebook_01.pdf

20-2-2. アジャイル開発の実施ポイント

アジャイル開発を実践するに当たり、まずはプロセスを理解することが大切です。アジャイル開

発の代表格であるスクラムを例に、アジャイル開発のプロセスを説明します。

ポイント

- アジャイル開発は経験者が参画することを前提とします。アジャイル開発に関する資格を有している場合も、一定の知識を有していることは判断できますが、アジャイル開発を実践できるかを判断することができません。参画者がどのようなシステム開発において、どのような役割を果たしたのかを確認することが重要です。

- アジャイル開発の進め方には厳格な決まりごとや規範はありません。本書で説明（例示）する進め方、メンバーの役割（ロール）など、実際のソフトウェア開発プロジェクトでそのまま適用するものではありません。アジャイル開発の基本を習得したのち、実際のプロジェクトや組織に適したやり方を取捨選択し、カスタマイズすることが必要となります。

- 「唯一の正しい」アジャイル開発というものはありません。自分のいる組織に合ったやり方が、その組織のビジネスや活動、文化から自然と育っていくことがアジャイル開発の本質です。

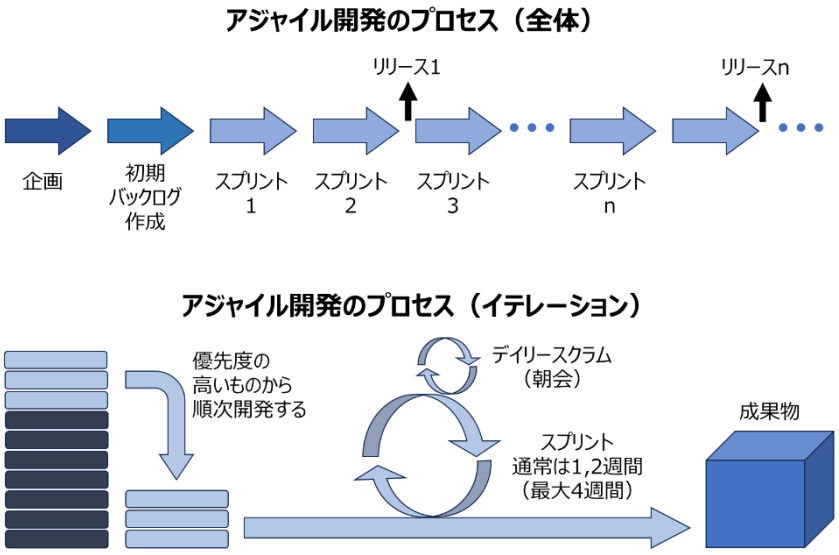

図 82. アジャイル開発のプロセス（スクラムの例）

スクラムのプロセス	特徴
1.プロダクトバックログの作成	プロダクトオーナーがプロジェクトの全体的な要件や機能をリストアップします。このリストは「プロダクトバックログ」と呼ばれ、優先順位がつけられます。
2.スプリントプランニング	チームはスプリント（通常 1～2 週間、長くても 4 週間）ご

	とに作業する項目を選びます。この選ばれた項目のリストは「スプリントバックログ」と呼ばれます。
3.デイリースクラム（デイリースタンドアップ）	毎日、チームは短いミーティングを行い、進捗状況を共有し、問題点を解決します。このミーティングは通常 15 分以内で行われます。
4.スプリントの実行	チームはスプリントバックログに基づいて作業を進めます。各メンバーは自分のタスクに集中し、協力して目標を達成します。
5.スプリントレビュー	スプリントの終わりに、チームは完成した作業をプロダクトオーナーやステークホルダーにデモンストレーションします。フィードバックを受け取り、次のスプリントに反映させます。スプリントごとにリリースを行うことが理想ですが、業務向けアプリケーションの場合には、エンドユーザーの混乱を避けるため、ある程度まとまった成果物ができた段階でリリースする（複数回のスプリント後にリリースする）ことが多いようです。
6.スプリントレトロスペクティブ	チームはスプリントの振り返りを行い、何がうまくいったか、何が改善できるかを話し合います。このフィードバックをもとに、次のスプリントでの改善策を考えます。

役割（ロール）の名称	役割
プロダクトオーナー	プロダクトのビジョンを持ち、バックログの優先順位を決定します。
スクラムマスター	チームがスクラムのプロセスを正しく実行できるようサポートし、障害を取り除きます。
開発チーム	実際に開発作業を行うメンバーです。
ステークホルダー	エンドユーザー、経営者、総務・経理・法務部門などです。

詳細理解のため参考となる文献（参考文献）	
アジャイル領域へのスキル変革の指針　アジャイル開発の進め方	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065606.pdf

引用文献

DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf
アジャイル領域へのスキル変革の指針　アジャイル開発の進め方
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065606.pdf

参考文献

DS-100 デジタル・ガバメント推進標準ガイドライン

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf

DS-110 デジタル・ガバメント推進標準ガイドライン解説書

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9462b2d8/20240605_resources_standard_guidelines_guideline_03.pdf

DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf

DS-121 アジャイル開発実践ガイドブック

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9fc931f7/20220422_resources_standard_guidelines_guidebook_01.pdf

DS-130 標準ガイドライン群用語集

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/83a1ac09/20230331_resources_standard_guidelines_glossary_03.pdf

DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf

DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン ～ベースラインと事業被害の組み合わせアプローチ～

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1b65a1dc/20230411_resources_standard_guidelines_guideline_01.pdf

DS-202 CI／CD パイプラインにおけるセキュリティの留意点に関する技術レポート

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/33f31336/20240329_resources_standard_guidelines_guideline_01.pdf

DS-210 ゼロトラストアーキテクチャ適用方針
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5efa5c3b/20220630_resources_standard_guidelines_guidelines_04.pdf
DS-211 常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/ef841b43/20240131_resources_standard_guidelines_guidelines_03.pdf
DS-212 ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/e5b49450/20230411_resources_standard_guidelines_guideline_03.pdf
DS-220 政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_05.pdf
DS-221 政府情報システムにおける脆弱性診断導入ガイドライン
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7fefc9ee/20240206_resources_standard_guidelines_guidelines_01.pdf
DS-231 セキュリティ統制のカタログ化に関する技術レポート
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9f746654/20230411_resources_standard_guidelines_guideline_07.pdf
DS-310 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5167e265/20230929_resources_standard_guidelines_guideline_01.pdf
DS-400 政府相互運用性フレームワーク（GIF）
https://github.com/JDA-DM/GIF
DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a0

6143-ed29-4f1d-9c31-0f06fca67afc/f1be078e/20220422_resources_standard_guidelines_guideline_07.pdf
DS-531 処分通知等のデジタル化に係る基本的な考え方
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d92a1cf2/20230411_resources_standard_guidelines_guideline_09.pdf
DS-910 安全保障等の機微な情報等に係る政府情報システムの取扱い
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/4d3bf58a/20230719_resources_standard_guidelines_guideline_01.pdf
【改定新版】特権 ID 管理ガイドライン
https://www.jnsa.org/result/digitalidentity/2024/index.html
アジャイル領域へのスキル変革の指針　アジャイル開発の進め方
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065606.pdf

■AI

Artificial Intelligence の略。

「AI（人工知能）」という言葉は、昭和 31 年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。昭和 25 年代後半から昭和 35 年代が第一次 AI ブーム、昭和 55 年代が第二次 AI ブーム、現在は平成 20 年代から始まる第三次 AI ブームである（近年の大規模言語モデルなどの登場を契機に、第 4 次 AI ブームに入ったとの見方もある）。「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている

■BCP

Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画

■CSIRT（シーサート）

Computer Security Incident Response Team の略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う

■DDoS 攻撃（ディードスこうげき）

Distributed Denial of Service Attack の略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることにより、過剰な負荷をかけてサービスを利用できなくする攻撃手法

■DFFT

Data Free Flow with Trust の略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している

■EDR

Endpoint Detection and Response の略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する

■eKYC

electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと

■G ビズ ID

行政手続きなどにおいて手続きを行う法人を認証するための仕組み。1 つの ID・パスワードで本人確認書類なしにさまざまな政府・自治体の法人向けオンライン申請が可能になる

■ICSCoE 中核人材育成プログラム

平成 29 年 4 月に独立行政法人情報処理推進機構（IPA）内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）

が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている

■ICT

Information and Communication Technology の略。IT（情報技術）に加えて、コンピュータやスマートフォンなどを用いて行うコミュニケーションを実現する技術（通信技術）を含んでいる

■IDS

Intrusion Detection System の略。不正アクセスや異常な通信を検知して管理者に通知するシステムのこと。IPS と異なり、不正アクセスや異常な通信をブロックする機能はない

■IoT（アイ・オー・ティー）

Internet of Things の略。日本語では「モノのインターネット」。インターネットにコンピュータやセンサー、カメラ、産業機械、家電などさまざまな「モノ」が接続され、データを収集したり、相互に情報をやり取りしたりする概念や仕組み、技術のこと

■IPS

Intrusion Prevention System の略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。

IPS は、異常を検知した場合、管理者に通知するに加えて、その通信を遮断する

■IP アドレス

コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意になる数字の組み合わせ。 IP アドレスは、127.0.0.1 のように 0～255 までの数字を 4 つ組み合わせたもので、単にアドレスと略されることがある。 現在主に使用されているこれら 4 つになる数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量に IP アドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6 では、アドレス空間の増加に加えて、情報セキュリティ機能の追加などの改良も加えられている

■ISAC

Information Sharing and Analysis Center の略。業界内での情報共有・連携の取り組み推進を図る組織のこと。国内では、金融や交通、電力、ICT などの分野に ISAC がある。ICT-ISAC では、ICT 分野の情報セキュリティに関する情報（インシデント情報を含む。）の収集・調査・分析を行っている

■ISMS

Information Security Management System の略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的なセキュリティ対策を含む、経営者を頂点とした総合的で組織的な取組。組織が ISMS を構築するための要求事項をまとめた国際規格が ISO/IEC 27001（国内規格は JIS Q 27001）であり、審査機関の審査に合格すると「ISMS 認証」を取得できる

■ISP

個人や企業などに対してインターネットに接続するため

のサービスを提供する事業者のこと。ユーザーは ISP と契約し、回線を用いて ISP が運営するネットワークに接続することで、インターネット上のサーバなどへアクセスできる

■IT リテラシー

コンピュータやインターネットをはじめとする情報技術（IT）を適切に活用する基礎的な知識や技能

■JPCERT/CC

日本におけるセキュリティインシデントなどの報告の受付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている組織。政府機関や企業などから独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる

■JVN

Japan Vulnerability Notes の略。日本で使用されているソフトウェアなどの脆弱性関連情報と対策情報を提供する、脆弱性対策情報ポータルサイトのこと

■KPI

Key Performance Indicator の略。目標・戦略を実現するために設定した具体的な業務プロセスをモニタリングするために設定される指標（業績評価指標：Performance Indicators）のうち、特に重要なもの。

■LockBit2.0

「Your files are encrypted by LockBit」というメッセージを表示させ、身代金を要求するマルウェア（ランサムウェア）。感染するとファイルが暗号化され、拡張子が「.LockBit」に変更される

■MAC アドレス

Media Access Control address の略。隣接する機器同士の通信を実現するためのアドレスのこと。ネットワーク機器や PC、ルータなどについている固有の識別番号で、一般的に 12 桁の 16 進数で「00-00-00-XX-XX-XX」などと表される

■NISC

National center of Incident readiness and Strategy for Cybersecurity の略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当

■NIST サイバーセキュリティフレームワーク（CSF）

米国政府機関の重要インフラの運用者を対象として誕生し、防御に留まらず、検知・対応・復旧といった、インシデント対応が含まれている。日本においても、今後普及が見込まれる

■RPA

Robotic Process Automation の略。定型的な業務をソフトウェアのロボットにより自動化すること

■NTP

Network Time Protocol の略。あらゆる機器の時刻情報を同期するためのプロトコル（通信規約）のこと。時刻情報を配信するサーバと、時刻合わせを行うクライアント間、およびサーバ間の通信方法を定めている

■PII

Personally Identifiable Information の略。「個人を特

定できる情報」と訳されることが多いが、実際には個人を特定するために使用される情報のこと。個人と 1 対 1 に紐づいているマイナンバー、メールアドレス、携帯電話番号、銀行口座番号だけでなく、氏名、生年月日、住所、勤務先などの情報も PII に含まれる

■PJMO

Project Management Office の略。プロジェクトの進捗管理やタスク管理などを行う組織のこと。プロジェクト管理を行うチームや担当者を指す

例えば、プロジェクト管理を行うチームは、情報システム部門の担当者に加え、実務部門の担当者、調達担当者、業務委託先が決定した後はその担当者も含めた体制で構成する

■PMO

Project Management Office の略。（企業組織やプロジェクト規模によっては、Program Management Office、Portfolio Management Office とも呼ばれる。）組織全体のプロジェクトを横断的に管理する体制を指す

政府ガイドラインでの PMO は、府省全体の管理となっているが、一般企業においては、企業全体のプロジェクトの管理と読み替えられる

PJMO が個々のプロジェクト計画を定めるのに対し、PMO は全プロジェクトについて、横断的に管理・支援を行う（例：計画、予算、執行管理、PJMO 支援など）

■RFI

Request For Information の略。情報提供依頼のこと。発注者が依頼をする候補となるシステム開発会社に対して、技術情報や製品情報の提供を依頼すること

■SASE（サシー）

Secure Access Service Edge の略。令和元年に提唱されたゼロトラストセキュリティを実現する方法の 1 つで、IT 環境のネットワークの機能とセキュリティの機能をクラウドサービス上で統合して提供するサービス、また、その考え方・概念

■SBOM（エスボム）

Software Bill of Materials の略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOM は、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOM は、ソフトウェアのリスクを把握・管理するのに役立つ

■SDP

Software-Defined Perimeter の略。ゼロトラストを実現するための仕組みで、すべての通信をチェックおよび認証する。VPN は、ネットワーク接続前に一度だけ認証を行うのに対し、SDP は、ユーザーの情報（デバイス、場所、OS など）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う

■SECURITY ACTION

中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度

■SLA

Service Level Agreement の略。サービス提供者と利用者の間で結ばれるサービスの品質に関して合意する契約のこと。サービスを提供する事業者が利用者に対して、どの程度の品質を保証できるのかを明示したもの

■Society5.0

日本が目指すべき未来社会の姿として、平成 28 年に閣議決定された「第 5 期科学技術基本計画」において内閣府が提唱した概念。サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）で、狩猟社会、農業社会、工業社会、情報社会の次にくる社会として位置づけられている

■SSL/TLS

Web サーバと Web ブラウザとの通信において、データを暗号化して送受信する仕組みのこと。これにより、通信の途中で情報の盗聴・改ざんや、なりすましを防ぐことができる。過去には SSL が使われていたが、脆弱性が発見されたため、TLS（v.1.2 以降）への移行が進んでおり、今では SSL は使われなくなってきている。しかし、歴史的経緯で SSL の用語が広く普及しているため、本テキストでは「SSL/TLS」と表記する

■SWG

Secure Web Gateway の略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することによりセキュアな通信環境を実現

■VPN（Virtual Private Network）

Virtual Private Network の略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することにより、盗聴やデータの改ざんを防ぐ。VPN（Virtual Private Network）を使用することによって、ユーザーは物理的に独立した専用線で通信しているかのような安全な通信を行うことができる

■WAF（ワフ）

Web Application Firewall の略。 従来のファイアウォールが、IP アドレスとポート番号で通信を制御していたことに対して、Web アプリケーションの脆弱性を狙うサイバー攻撃を防ぐことを目的として、アプリケーションレベルで通信を制御（分析・検知・遮断）するファイアウォールのこと

■WAN

Wide Area Network の略。広義には、広い地域をカバーするネットワークのことで、インターネットとほぼ同義の言葉として使われる。

一方、狭義には、物理的に離れた場所にある LAN（オフィスのフロアや建物内など狭いエリアで構築されたネットワーク）同士を接するネットワークを指し、特定のユーザーしかアクセスできない。このプライベートな WAN を構築する場合には、通信事業者に依頼する必要がある

■アクセス制御

特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザーを制限する機能のこと

■アセスメント

システムや運用環境などを客観的に調査・評価すること。現在の利用状況を把握することにより、システムの再構築や運用改善の参考情報となる

■暗号化

データの内容を変換し、第三者には、内容を見ても解読できないようにすること

■アンダーグラウンドサービス

合法ではない非公式な活動が行われるオンラインの闇市場やコミュニティでサイバー攻撃を目的としたツールなどを販売しているサービス

■イベントログ

コンピュータシステムに起こった出来事や、行われた操作などを時系列に記録したデータのこと

■インターネットバンキング

インターネットを利用して銀行との取引を行うサービスのこと。銀行の窓口や ATM に出向かなくても、スマートフォンやパソコンなどを使って、いつでも利用可能な時間帯に振り込みや残高照会などの取引を行うことができる

■ウイルス定義ファイル（パターンファイル）

セキュリティソフトウェアがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真つきの手配書のようなもの

■エンティティ

個人、組織、団体、コンピュータシステム、通信機器など、多様な実体のこと

■エンドポイントデバイス

ネットワークに接続して、ネットワークを介して情報を交換するデバイス（パソコン、プリンタ、スキャナ、スマートフォン、仮想マシン、サーバ、IoT デバイスなど）

■改ざん

文書や記録などのすべてまたは一部に対して、無断で修正・変更を加えること。IT 分野では、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為

■可用性

許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性

■完全性

参照する情報が改ざんされていなく、正確である特性

■機密性

許可された者だけが情報や情報資産にアクセスできる特性

■脅威インテリジェンス

サイバー攻撃などの脅威への対応を支援することを目的として、収集・分析・蓄積された情報のこと。一部の産業では、企業横断的にこうした情報（インテリジェンス）を共有する活動が行われている

■供給者

組織に対して、製品・サービスを供給する企業または個人のこと。製品の場合、PC やサーバ、通信機器などがある。サービスの場合、クラウドサービス、インターネット接続サービス、業務の委託、物流、教育などがある

■クラッキング

悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為

■クリーンインストール

すでにインストールされている OS を削除した上で、新しく OS を再インストールする方法のこと。記憶領域にあるデータはすべて消去されるので、データはバックアップから復元する必要がある

■限定提供データ

不正競争防止法で次のように定義されている。「業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上または営業上の情報（秘密として管理されているものを除く。）をいう。」

■個人情報保護委員会

個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱いを確保することを任務とする、独立性の高い行政機関（組織的には内閣府の外局）。個人情報保護法およびマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱いに関する監視・監督、認定個人情報保護団体に関する事務などの業務を行っている

■コーディング

プログラミング言語でソースコードを書くこと

■コンパイル

プログラミング言語で書かれたプログラムを機械語に変換する作業

■サイバー攻撃

インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマートフォンから、企業のサーバやデータベース、国の重要インフラまでさまざまである。デジタル社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人などを攻撃する行為やその防御をサイバー戦争と呼ぶこともある

■サイバーセキュリティお助け隊サービス制度

「サイバーセキュリティお助け隊サービス」は、中小企業のセキュリティ対策に不可欠な各種サービスをワンパッケージにまとめた、民間事業者による安価なサービス。独立行政法人情報処理推進機構（IPA）は中小企業向けセキュリティサービスが満たすべき基準を設定しており、同基準を充足するサービスに「お助け隊マーク」を付与し、同サービスの普及促進活動を行っている

■サイバーセキュリティ戦略

組織や企業がセキュリティに関する目標を達成するための計画やアプローチ

■サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

単純なサイバー空間（仮想空間）におけるセキュリティ対策から、サイバー空間とフィジカル空間（現実空間）のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワーク

■サプライチェーン

製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される

■サポートユーティリティ

情報システムを運用する施設の稼動に不可欠な設備やライフライン、公共インフラのこと。ISO/IEC 27002:2022

では、サポートユーティリティの例として、電気、通信サービス、給水、ガス、下水、換気、空調を挙げている

■シャドーIT

従業員が業務に使用する IT 機器やサービスのうち、企業が把握していないものを指す。具体的には、普段プライベートで使用しているオンラインストレージといったクラウドサービス、個人所有のデバイスなどで、組織の許可なく業務に利用しているもの

■磁気データ消去装置

ハードディスクに強力な磁気を照射することで、ハードディスク内の磁気記録領域に記録されている情報を破壊する装置のこと。短時間で効率よく、大量のハードディスクのデータを完全に消去できる

■ジャーニーマップ

一人のユーザーが目的を達成するための道のり（プロセス）を表に表したもの。

カスタマージャーニーマップともいう

■情報資産

営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報

■情報セキュリティ事象

情報セキュリティ上よくない、システムやサービス、ネットワークの状態のこと。

情報セキュリティ事象の中でも、事業運営を危うくしたり、情報セキュリティを脅かしたりする可能性が高いものは、セキュリティインシデントに分類される

■情報セキュリティの 3 要素「CIA」

情報セキュリティの 3 つの要素、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の頭文字をとって「CIA」と呼ぶ

■真正性

情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある

■信頼性

システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性

■スクリーンセーバ

離席時に PC の画面の内容を盗み見されることを防ぐ機能のこと。PC に対して一定時間ユーザーによる操作がなかった場合、自動的にアニメーションや写真などを表示し、作業中の情報を見せないようにする

■スクリーンロック

デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない

■脆弱性

情報システム（ハードウェア、ソフトウェア、ネットワークなどを含む）におけるセキュリティ上の欠陥のこと

■脆弱性診断

システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること

■責任追跡性

情報資産に対する参照や変

更などの操作を、どのユーザーが行ったものかを確認することができる特性

■セキュリティインシデント

セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象などがインシデントに該当

■セキュリティ・キャンプ

情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した 22 歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、独立行政法人情報処理推進機構（IPA）と（一財）セキュリティ・キャンプ協議会が実施している

■セキュリティホール

情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある

■セキュリティポリシー

企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載することが一般的

■ゼロデイ攻撃

OS やソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと

■ゼロトラスト

従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、すべてのネットワーク通信を信用できない領域として扱い、すべての通信を検知し認証するという新しいセキュリティの考え方

■ソフトウェアライブラリ

プログラムにおいてよく利用される機能を切り出し、再利用しやすいようにまとめたもので、プログラム作成のための部品のこと。ライブラリを利用することで、1 から作る必要がなくなり、効率的に開発を行うことができる

■ソリューション

問題や課題を解決するための具体的な解決策や手段を指す。ある特定の課題やニーズに対して提供される解決方法やアプローチのことを指すことが一般的で、ビジネスシーンにおけるソリューションの意味とは「顧客が抱える問題や課題を解決すること」

■ダークウェブ

特別な手法でないとアクセスできない、匿名性の高い非公開の Web サイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている

■多要素認証

多要素認証は、サービス利用時において利用者の認証を行うために、3 つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも 2

つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年では FIDO2 と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている

■データサイエンス

数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること

■データマスキング

個人情報や機密情報が含まれるデータを扱う際に、特定の部位のみを無意味な符号（アスタリスク「※」など）に置き換える処理のこと。もとのデータの一部を秘匿化し、個人や機密情報を識別できないようにすることで、データ分析やテストデータなどに利用可能とする

■デジタル化

紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネスプロセスを自動化・合理化するデジタライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードを CD（コンパクトディスク）にすることがデジタイゼーション、音楽をダウンロード販売することがデジタライゼーションである

■デジタル情報

0、1、2 のような離散的に（数値として）変化する量で表現できる情報のこと。一般的にコンピュータ内部では「0」と「1」の 2 進数で表現されている。デジタル情報は劣化することがなく、整理・検索が容易であるという特徴がある

■デプロイ

実行ファイルをサーバ上に配置することで、ユーザーが利用できるようにすること

■トラフィック

通信回線やネットワーク上で送受信される信号やデータ、データ量のこと

■内部監査

内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する国際規格である ISO27001 の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する

■ハウジングサービス

データセンターのラック（サーバを収容する鍵のついた棚）とサーバに接続する回線や電源を貸し出すサービスのこと。自社が所有しているサーバを、物理的にセキュリティが強固なデータセンターに設置し、運用できるため、セキュリティを強化できるメリットがある

■ビジネスインパクト分析

災害など不測の事態によって業務やシステムが停止した場合に、会社の事業に与える影響度を評価すること。BCP（事業継続計画）を立てる上で実行する必要がある

■ビジネスメール詐欺

攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Em

ail Compromise とも略される

■ビッグデータ

全体を把握することが困難な程、膨大な規模のデータ群

■否認防止性

システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようにする特性

■標的型攻撃

機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルスつきメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている

■標的型メール攻撃

特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある

■ファイアウォール

本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンの OS に付随しているもの、セキュリティソフトウェアについているもの、専用のハードウェアになっているものなど形態はさまざまである

■ファイル共有ソフト

複数の利用者によるネットワークでのファイルのやり取りを可能にしたソフトウェアのこと。不特定多数でファイルを共有するソフトは、自動的にファイルを送受信する仕組みであるため、ウイルスの感染によって、公開したくないファイルがインターネットに流出するトラブルなどが多く発生している。不特定多数でファイルを共有するファイル共有ソフトは、使用を禁止する必要がある

■不正アクセス

利用権限を持たない悪意のあるユーザーが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、平成12年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている

■踏み台

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元の IP アドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することにより、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ

■フォレンジック

犯罪捜査における分析や鑑識を意味する言葉。サイバー

セキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組を指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる

■ブラックマーケット

広義には、不法な取引が行われる市場を指す。不正に入手した個人情報などを売買するインターネット上の市場（闇市）

■フレームワーク

フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃などさまざまなセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな型」としてまとめたもの

■プロキシ

クライアントとサーバの中間で、両者の通信を中継する役割を担うサーバのこと。

プロキシは、クライアントからのリクエストやサーバからの応答をすべて把握することが可能なため、詳細な通信内容をログとして記録したり、Web サーバから送られてきたコンテンツをチェックし、不正なコードやマルウェアが含まれていないかをチェックしたりできる

■ブロックチェーン

複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録する、オープンな分散型台帳。ビットコインなどの暗号資産に使われている仕組み

■ベストプラクティス

何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例や良い成果をもたらす方法論

■ペルソナ分析

理想とする顧客像を具体化し、典型的なユーザーのプロファイル分析をすること

■ベンダーロックイン

ソフトウェアの機能改修やバージョンアップ、ハードウェアのメンテナンスなど、情報システムを使い続けるために必要な作業を、それを導入した事業者以外が実施することができないために、特定の事業者（ベンダー）を利用し続けなくてはならない状態のこと

■マルウェア

パソコンやスマートフォンなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる

■ミラサポコネクト

ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネクト構想」をもとにした、行政、支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤

■ミドルウェア

OS とアプリケーションの中間に位置するソフトウェア

のこと。アプリケーションが業務に関する処理を行う際、データベースやサーバのやり取りをミドルウェアが担うことで複雑な処理を行うことができる

■無線 LAN

LAN は Local Area Network の略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線 LAN を通じて、コンピュータはインターネットなどのネットワークにアクセスすることができる

■無停電電源装置

UPS とも呼ばれる。停電が起きてしまったときに電気を一定時間供給し続けるための装置のこと。パソコンやハードディスク、サーバなどを予期せぬ停電から守れる

■ユーティリティプログラム

コンピュータで、システムの運用を支援するプログラムのこと。具体的には、記憶媒体間のデータ転送、ファイルの複写・削除・整理などの処理を行うためのプログラムのこと。システムおよびアプリケーションによる制御を無効にすることのできるものもある

■ランサムウェア

悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する

■リスクアセスメント

企業や組織が持つ情報資産に対するリスクの分析・評価を行うプロセスのこと。具体的には情報資産の特定、脅威と脆弱性の特定と評価、リスクの分析と評価を行う。リスク評価の結果、許容できるもの以外は何らかのセキュリティ対策を講じる必要がある

■リスク評価

組織やプロジェクトにおける特定されたリスクに対して、重要度や影響度を評価するプロセス

■リモートデスクトップ接続

パソコン、タブレット、スマートフォンなどのデバイスを使用して、遠隔地から特定のパソコンに接続する方法