# 中小企業向け

# サイバーセキュリティ実践ハンドブック

## 中小企業も安心！セキュリティ対策で DX を加速

**第８編　　具体的な構築・運用の実践【レベル 3】**


東京都産業労働局

.第 7 編 ISMS の構築と対策基準の策定と実施手順 【レベル 3】 ..... 1
第 18 章. 技術的対策 ..... 1
18-1. 作成する候補となる実施手順書類について ..... 2
18-2. 技術的対策として重要となる実施項目 ..... 8
18-2-1. エンドポイントデバイス ..... 8
18-2-2. 特権アクセス権 ..... 9
18-2-3. アクセス制限 ..... 9
18-2-4. 安全な認証 ..... 10
18-2-5. キャパシティ管理 ..... 10
18-2-6. マルウェアに対する保護 ..... 11
18-2-7. 技術的脆弱性の管理 ..... 11
18-2-8. 構成管理 ..... 12
18-2-9. 情報の削除 ..... 12
18-2-10. データ保護 ..... 12
18-2-11. バックアップ ..... 13
18-2-12. 冗長化 ..... 14
18-2-13. ロギング ..... 14
18-2-14. 監視 ..... 14
18-2-15. クロック同期 ..... 15
18-2-16. 特権ユーティリティの使用 ..... 15
18-2-17. ソフトウェア管理 ..... 15
18-2-18. ネットワークセキュリティ ..... 20
18-2-19. ネットワークの分離 ..... 21
18-2-20. Web フィルタリング ..... 21
18-2-21. 暗号の使用 ..... 22
18-3. 実施手順を適用するセキュリティ概念 ..... 23
18-3-1. Security by Design ..... 23
18-3-2. ゼロトラスト、境界防御モデル ..... 27
18-3-3. SASE ..... 33
18-3-4. ネットワーク制御（Network as a Service） ..... 36
18-3-5. セキュリティ統制（Security as a Service） ..... 39
18-4. インシデント対応 ..... 45
第 19 章. セキュリティ対策状況の有効性評価 ..... 49
19-1. 内部監査 ..... 50
19-2. 外部監査 ..... 51
コラム ..... 53
編集後記 ..... 54

第８編．具体的な構築・運用の実践【レベル 3】 ..... 55
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） ..... 55
20-1．セキュリティ機能の実装と運用 ..... 56
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 ..... 56
20-1-2．プロジェクトの管理 ..... 63
20-1-3．予算および執行 ..... 70
20-1-4．サービス・業務企画 ..... 78
20-1-5．要件定義 ..... 83
20-1-6．調達 ..... 91
20-1-7．設計・開発 ..... 95
20-1-8．サービス・業務の運営と改善 ..... 104
20-1-9．運用および保守 ..... 109
20-1-10．システム監査 ..... 117
20-2．アジャイル開発 ..... 121
20-2-1．アジャイル開発の概要 ..... 121
20-2-2．アジャイル開発の実施ポイント ..... 122
引用文献 ..... 125
参考文 ..... 126
用語集 ..... 130

# 第18章. 技術的対策

- 技術的管理策をもとに、対策基準を策定する手順を理解すること
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること
- Security by Design、ゼロトラスト・境界防御モデル、ネットワーク制御、セキュリティ統制、インシデント対応について理解すること

## 18-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に掲載された合計 93 項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

**ISO/IEC27001:2022 に基づき管理策を決定する（例）**

**【凡例】採用：〇・不採用：×**

| 項目 | 採用、不採用 | 項目 | 採用、不採用 |
|---|---|---|---|
| 8.1 利用者エンドポイント機器 | | 8.18 特権的なユーティリティプログラムの使用 | |
| 8.2 特権的アクセス権 | | 8.19 運用システムに関わるソフトウェアの導入 | |
| 8.3 情報へのアクセス制限 | | 8.20 ネットワークのセキュリティ | |
| 8.4 ソースコードへのアクセス | | 8.21 ネットワークサービスのセキュリティ | |
| 8.5 セキュリティを保った認証 | | 8.22 ネットワークの分離 | |
| 8.6 容量・能力の管理 | | 8.23 ウェブ・フィルタリング | |
| 8.7 マルウェアに対する保護 | | 8.24 暗号の使用 | |
| 8.8 技術的ぜい弱性の管理 | | 8.25 セキュリティに配慮した開発のライフサイクル | |
| 8.9 構成管理 | | 8.26 アプリケーションのセキュリティの要求事項 | |
| 8.10 情報の削除 | | 8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則 | |
| 8.11 データマスキング | | 8.28 セキュリティに配慮したコーディング | |

| | | | |
|---|---|---|---|
| 8.12 データ漏えいの防止 | | 8.29 開発及び受入れにおけるセキュリティ試験 | |
| 8.13 情報のバックアップ | | 8.30 外部委託による開発 | |
| 8.14 情報処理施設の冗長性 | | 8.31 開発環境、試験環境及び運用環境の分離 | |
| 8.15 ログ取得 | | 8.32 変更管理 | |
| 8.16 監視活動 | | 8.33 試験情報 | |
| 8.17 クロックの同期 | | 8.34 監査試験中の情報システムの保護 | |

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMS に基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022 の文献を参照しながら作成してください。

**対策基準（例）**

**8.1 利用者エンドポイント機器**

利用者エンドポイントデバイスに保存されている情報、処理される情報、または利用者エンドポイントデバイスを介してアクセス可能な情報を保護しなければならない。

**8.2 特権的アクセス権**

特権的アクセス権の割り当ておよび利用は、制限し、管理しなければならない。

**8.3 情報へのアクセス制限**

情報およびその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限しなければならない。

**8.4 ソースコードへのアクセス**

ソースコード、開発ツール、ソフトウェアライブラリへの読取りおよび書込みアクセスを、適切に管理しなければならない。

**8.5 セキュリティを保った認証**

セキュリティを保った認証技術および手順を、情報へのアクセス制限およびアクセス制御に関するトピック固有の方針に基づいて備えなければならない。

**8.6 容量・能力の管理**

現在および予測される容量・能力の要求事項に合わせて、資源の利用を監視し、調整しなければならない。

**8.7 マルウェアに対する保護**

マルウェアに対する保護を実施し、利用者の適切な認識によって支援しなければならない。

**8.8 技術的脆弱性の管理**

利用中の情報システムの技術的脆弱性に関する情報を獲得しなければならない。また、そのような脆弱性に組織がさらされている状況を評価し、適切な手段をとらなければならない。

**8.9 構成管理**

ハードウェア、ソフトウェア、サービスおよびネットワークのセキュリティ構成を含む構成を確立、文書化、実装、監視し、レビューしなければならない。

**8.10 情報の削除**

情報システム、装置またはその他の記憶媒体に保存している情報は、必要でなくなった時点で削除しなければならない。

**8.11 データマスキング**

データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針およびその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用しなければならない。

**8.12 データ漏えいの防止**

データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存、送信するシステム、ネットワークおよびその他の装置に適用しなければならない。

**8.13 情報のバックアップ**

合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェアおよびシステムのバックアップを維持し、定期的に検査しなければならない。

**8.14 情報処理施設の冗長性**

情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性を持って、導入しなければならない。

**8.15 ログ取得**

活動、例外処理、過失、その他の関連する事象を記録したログを取得、保存、保護し、分析しなければならない。

**8.16 監視活動**

セキュリティインシデントの可能性を評価するために、ネットワーク、システムおよびアプリケーションについて異常な挙動がないか監視し、適切な処置を講じなければならない。

**8.17 クロックの同期**

組織が使用する情報処理システムのクロックは、国の原子時計から配信される時刻に基づくクロックと同期させなければならない。

**8.18 特権的なユーティリティプログラムの使用**

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ユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。

**8.19 運用システムに関わるソフトウェアの導入**

運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順および対策を実施しなければならない。

**8.20 ネットワークのセキュリティ**

システムおよびアプリケーション内の情報を保護するために、ネットワークおよびネットワーク装置のセキュリティを保ち、管理し、制御しなければならない。

**8.21 ネットワークサービスのセキュリティ**

ネットワークサービスのセキュリティ機能、サービスレベルおよびサービスの要求事項を特定し、実装し、監視しなければならない。

**8.22 ネットワークの分離**

情報サービス、利用者および情報システムは、組織のネットワーク上でグループごとに分離しなければならない。

**8.23 ウェブ・フィルタリング**

悪意のあるコンテンツにさらされることを減らすために、外部 Web サイトへのアクセスを管理しなければならない。

**8.24 暗号の使用**

暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施しなければならない。

**8.25 セキュリティに配慮した開発のライフサイクル**

ソフトウェアおよびシステムのセキュリティに配慮した開発のための規則を確立し、適用しなければならない。

**8.26 アプリケーションのセキュリティの要求事項**

アプリケーションを開発または取得する場合、情報セキュリティ要求事項を特定し、規定し、承認しなければならない。

**8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則**

セキュリティに配慮したシステムを構築するための原則を確立、文書化、維持し、すべての情報システムの開発活動に対して適用しなければならない。

**8.28 セキュリティに配慮したコーディング**

セキュリティに配慮したコーディングの原則を、ソフトウェア開発に適用しなければならない。

**8.29 開発及び受入れにおけるセキュリティ試験**

セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施しなければならない。

**8.30 外部委託による開発**

組織は、外部委託したシステム開発に関する活動を指揮、監視し、レビューしなければならない。

**8.31 開発環境、試験環境及び運用環境の分離**

開発環境、テスト環境および本番環境は、分離してセキュリティを保たなければならない。

**8.32 変更管理**

情報処理設備および情報システムの変更は、変更管理手順に従わなければならない。

**8.33 試験情報**

テスト用情報は、適切に選定、保護、管理しなければならない。

### 8.34 監査試験中の情報システムの保護

運用システムのアセスメントを伴う監査におけるテストおよびその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意しなければならない。

| 詳細理解のため参考となる文献（参考文献） | |
|---|---|
| ISO/IEC 27001:2022 | https://www.iso.org/standard/27001 |

## 18-2. 技術的対策として重要となる実施項目

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介します。紹介する例と、ISO/IEC 27002 に記載されている各管理策の手引の内容を参考に、自社に適した実施手順を策定してください。

### 18-2-1. エンドポイントデバイス

**【8.1 利用者エンドポイント機器】**

**実施手順（例）**

a. モバイル機器を社外に持ち出す場合、ログインパスワードを設定する。
b. 必要のない機密情報、個人情報などは、モバイル機器に格納しない。
業務上必要のある機密情報や個人情報をモバイル機器に格納する場合は、暗号化する。（パスワードをつける。）
c. モバイル機器を利用者が限定されない無償の WiFi スポットなどへ接続することは禁じる。
- 携帯電話・スマートフォンの管理
社有の携帯電話・スマートフォン（以下「社有携帯電話など」という）を使用する者は、紛失、破損しないよう丁寧かつ慎重に扱う。
- 社有携帯電話などを使用する者は、使用者本人以外が操作できないよう、パスワードを設定して保護する。
- 持ち歩く際は、ストラップをつけるなどの紛失・盗難防止策を必要に応じて講じる。
- 電車やバスの中、その他公共の場所における使用は控え、個人情報やその他機密情報を他者に聞かれないよう十分配慮する。
- 私有の携帯電話・スマートフォンを業務で使用する場合は、情報システム管理者の承認を要する。また、社有携帯電話などと同様の安全対策を実施する。

d. 利用者はノート PC に対して、パスワードつきのスクリーンセーバを設定し、のぞき見を防止する。スクリーンセーバの設定時間は 10 分以内とする。

**ワンポイントアドバイス**

利用者終端装置（携帯、スマートフォン、ノート PC など、ユーザーが情報処理サービスにアクセスするために使用するさまざまなデバイス）の取扱いに関する規則を定めることが大切です。

## 18-2-2. 特権アクセス権

**【8.2 特権的アクセス権】**

| 実施手順（例） |
| --- |
| a. 特権的アクセス権は特定の者に付与し、管理対象システムとその保有者を明確にする。<br>b. 半年に 1 回、または組織に何か変更があった際、特権的アクセス権を用いて作業する利用者をレビューし、特権的アクセス権を用いた作業に関して、その利用者が職務、役割、責任、力量の点で今も適格であるか否かを検証する。 |
| **ワンポイントアドバイス**<br>特権的アクセス権は一般の利用者よりも多くの権限が付与されているため、悪用されると影響が大きいです。ID 付与に際しては、厳格かつ安全な管理のもとに運用されることが大切です。 |

## 18-2-3. アクセス制限

**【8.3 情報へのアクセス制限】**

| 実施手順（例） |
| --- |
| a. 情報システム管理者は、取扱いに慎重を要する情報へのアクセス権限を、必要な者のみに割り当てる。<br>b. 未知の利用者識別情報または匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。 |
| **ワンポイントアドバイス**<br>情報およびその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止することが大切です。 |

**【8.4 ソースコードへのアクセス】**

| 実施手順（例） |
| --- |
| ソースコードや設計書、仕様書などの関連書類は、アクセス権で管理されたフォルダに厳重に保管する。 |
| **ワンポイントアドバイス**<br>ソースコードが変更される、または開発環境の一部のデータが認可されていない人物によって取り出される可能性をなくすため、ソースコードへのアクセスを適切に制御することが大切です。 |

## 18-2-4. 安全な認証

**【8.5 セキュリティを保った認証】**

**実施手順（例）**

重要な情報システムにアクセスする際は、パスワードに加えて、多要素認証を使用し、不正アクセスの可能性を減らす。

**ワンポイントアドバイス**

多要素認証では、知識（パスワード、秘密の質問など）、所持物（スマートフォン、IC カードなど）、生体情報（指紋、声紋など）のうち、2 つ以上を組み合わせて認証することで、認可されていないアクセスの可能性を減らします。

## 18-2-5. キャパシティ管理

**【8.6 容量・能力の管理】**

**実施手順（例）**

a. 情報システム管理者は、コンピュータやネットワークの応答時間など、その負荷状況について、業務を通じて問題がないか否かを確認する。CPU やメモリ、ハードディスクなどの外部記憶装置の使用率など、リソースの使用状況を定期的に監視する。
b. リソースの使用状況に応じてリソースの割り当てを調整すると同時に、将来必要となる容量や能力を予測し、システムのパフォーマンスを維持するため、必要なリソースを事前に確保する。
c. 情報システム管理者は、問題が発見された場合、速やかに原因の究明を行い、情報セキュリティ委員会に報告する。
d. 情報セキュリティ委員会は、情報システム管理者に対策を指示し、必要に応じて経営陣に報告する。
e. 情報システム管理者は、中長期的な業務量の増減を考慮し、将来的にシステムに必要な容量を予測し、必要であればトップマネジメントに報告する。

**ワンポイントアドバイス**

クラウドサービスを利用することで、特定のアプリケーションおよびサービスで利用できる資源を、要求に応じて迅速に拡張・削減することができます。

## 18-2-6. マルウェアに対する保護

**【8.7 マルウェアに対する保護】**

**実施手順（例）**

a. ネットワークに接続するすべてのパソコン、サーバ上に情報システム管理者が指定したアンチウイルスソフトを導入する。
b. アンチウイルスソフトを常時設定にし、ファイルへのアクセスおよび電子メールの受信時に常時スキャンできる設定を行う。
c. 常時スキャンに加えて情報システム管理者が指定した期間に一度、ファイル全体に対するスキャンを行う。
d. 自動でウイルス定義ファイルの更新が行われるように設定する。
e. 標的型メール対応
   - メールの添付書類やメール中のリンクは、原則として（送信者に確認するなどの方法で）安全が確認できるまで開かない。
   - ファイルの拡張子を表示させる設定とし、添付ファイルの拡張子が、通常使用しない内容の場合、ファイルの参照を禁じる。
     通常使用しないファイルの拡張子の例：.exe、.pif、.scr

**ワンポイントアドバイス**

基本的な対策として、社内パソコンのウイルス定義ファイルが常に最新版に更新されているかの確認を徹底することが重要です。

## 18-2-7. 技術的脆弱性の管理

**【8.8 技術的脆弱性の管理】**

**実施手順（例）**

a. 情報セキュリティ委員会および情報システム管理者は、技術的な脆弱性のニュースを常に意識し、時期を失せず効果的に外部の攻撃を防御する。
b. OS やアプリケーションには常に最新のセキュリティパッチを適用する。ただし、検証の結果、業務上支障があると認められる場合には、他の方法により脆弱性に対処する。

**ワンポイントアドバイス**

セキュリティパッチは、正当な供給元から取得したもののみを使用することが大切です。

## 18-2-8. 構成管理

**【8.9 構成管理】**

| 実施手順（例） |
| --- |
| システムの構成要素とその相互関係を理解し管理するため、台帳や構成管理ツールを用いて、ハードウェア、ソフトウェア、ネットワーク機器、設定ファイルなど、システムを構成するすべての要素の情報を把握する。 |
| **ワンポイントアドバイス**<br>ハードウェア・ソフトウェア・サービス・ネットワークが、必要とされるセキュリティ設定により正しく機能し、認可されていない変更や誤った変更によって構成が変えられないようにすることが大切です。 |

## 18-2-9. 情報の削除

**【8.10 情報の削除】**

| 実施手順（例） |
| --- |
| a. 業務上必要がなくなったデータは速やかに削除する。<br>b. 記憶媒体上のデータを削除する際は、データ消去ソフトを使用し、復元できないよう、完全に削除する。<br>c. ハードディスクを廃棄する際は、磁気データ消去装置を用いてハードディスクのデータを削除してから廃棄する。 |
| **ワンポイントアドバイス**<br>取扱いに慎重を要する情報などの機密情報については、必要がなくなった時点で速やかに削除することが大切です。情報を保有していることがリスクなので、不要な情報は持ちつづけないことが重要です。 |

## 18-2-10. データ保護

**【8.11 データマスキング】**

| 実施手順（例） |
| --- |
| 保有している情報をマーケティング分析などの目的で二次利用する場合には、個人情報や重要情報が推測できない形に加工した上で利用する。 |
| **ワンポイントアドバイス**<br>取扱いに慎重を要するデータ（個人情報や重要情報）の保護が必要である場合、データマスキ |

ング・仮名化・匿名化などの手法を使用して保護することが大切です。これにより、データが万が一漏えいしても、その内容を第三者に理解されることを防げます。

**【8.12 データ漏えいの防止】**

**実施手順（例）**

a. 漏えいから保護する情報を特定し、分類する。
b. ファイル共有ソフトの使用を禁じる。
c. 重要な情報が画面に表示されている場合は、スクリーンショットや写真を撮ることを禁じる。
d. ファイアウォールや IDS、IPS などによって不正アクセスを防止する。「8.20 ネットワークのセキュリティ」に従う。
e. 重要データについてアクセス制限を設ける。「8.3 情報へのアクセス制限」に従う。
f. 重要データは暗号化して保管する。「8.24 暗号の使用」に従う。

**ワンポイントアドバイス**

個人やシステムによる情報の認可されていない開示・抽出を検出し、防止することが大切です。

## 18-2-11. バックアップ

**【8.13 情報のバックアップ】**

**実施手順（例）**

a. 情報システム管理者は、サーバ内に保存された重要データを障害による破壊や、不正アクセス、改ざんなどから守るために、必要に応じてシステムおよびデータのバックアップを行う。
b. バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。
c. 情報システム管理者は、バックアップが確実に行われており、障害時に復元が可能か否かを月に 1 度チェックする。

**ワンポイントアドバイス**

クラウドサービスを利用している場合は、クラウド環境にあるデータのバックアップも作成しているか確認することが大切です。ランサムウェア対策として、バックアップは 2 つ作成し、1 つはネットワークから隔離したオフサイトで保管することが大切です。

## 18-2-12. 冗長化

**【8.14 情報処理施設の冗長性】**

**実施手順（例）**

a. 情報システムは、可用性に関する業務上の要求事項を明確にし、必要に応じて予備の機器を用意して二重化を行い、冗長性をもたせる。
b. 緊急の場合、速やかに予備の機器に切り替えられるよう、動作確認を月に 1 回行う。

**ワンポイントアドバイス**

冗長な構成要素および処理活動を常に作動させておくか、緊急の場合に自動または手動で作動させるかを確認します。常に作動させておく場合は、稼動状況を確認することが大切です。

## 18-2-13. ロギング

**【8.15 ログ取得】**

**実施手順（例）**

a. 情報システム管理者は、サーバ内に保存された重要データを障害による破壊や、不正アクセス、改ざんなどから守るために、必要に応じてログの取得を行う。
b. 情報システム管理者は、必要に応じてログの定期的なチェックを行う。
c. ログは、情報システム管理者またはその指名する担当がアクセスできるようにする。
d. 情報システム管理者は、運用担当者がサーバで行った作業を確認する。確認は、作業ログ、または日報・サーバ作業記録の閲覧により行う。

**ワンポイントアドバイス**

セキュリティインシデントの分析、警告および調査のために、システム間のログを相関づけられるようにすべてのシステムが同期した時刻源（8.17 クロックの同期を参照）を持つことが重要です。

## 18-2-14. 監視

**【8.16 監視活動】**

**実施手順（例）**

ファイアウォール・IDS・IPS のログを常に監視し、異常な動作を検知した場合は速やかに対応する。

**ワンポイントアドバイス**

通常時およびピーク時のシステム使用率や、各利用者または利用者グループの通常のアクセス時間・アクセス場所・アクセス頻度を考慮して正常な行動・動作の基準を確立し、基準に照ら

して異常を監視することが大切です。

## 18-2-15. クロック同期

**【8.17 クロックの同期】**

**実施手順（例）**

a. 情報システム管理者は、クライアント PC やサーバなどすべての情報システムについてクロックを同期させる。
b. すべての情報システムのクロックを同期させるために、NTP を使用する。

**ワンポイントアドバイス**

イベントログは、調査や法令や懲戒が関わる場合の証拠として必要となる可能性があり、不正確な監査ログは証拠の信頼性を損なう可能性があります。コンピュータ内のクロックを正しく設定し、イベントログの正確さを確実にすることが重要です。

## 18-2-16. 特権ユーティリティの使用

**【8.18 特権的なユーティリティプログラムの使用】**

**実施手順（例）**

a. ユーティリティプログラムの使用は、原則として OS 標準機能のみ許可する。
b. その他のユーティリティプログラムが必要となった場合は、情報システム管理者の承認を得た上で利用する。

**ワンポイントアドバイス**

情報システムの大半には、パッチ適用・ウイルス対策・バックアップ・ネットワークツールなど、システムやアプリケーションによる制御を無効にできる 1 つ以上のユーティリティプログラムが組み込まれています。不要なユーティリティプログラムは、すべて除去・無効化することが大切です。また、特権的ユーティリティの中には、データベースの中身を、その整合性を気にすることなく強制的に書き換えることができる機能や、他の利用者の権限でデータを操作できる機能をもったものがあります。こうした特権的なユーティリティを野放しにすると組織の情報セキュリティが保てなくなるため、厳しく利用を管理する必要があります。

## 18-2-17. ソフトウェア管理

**【8.19 運用システムに関わるソフトウェアの導入】**

**実施手順（例）**

a. 運用システムに、開発用のコードを導入しない。

b. PC を含む社内の情報システムで使用するソフトウェアは、原則情報システム管理者によって指定されたもののみ使用し、それ以外のソフトウェアを使用する場合は、事前に許可を得るものとする。他社が開発したソフトウェアを利用する場合、その開発会社が要求している条件やスペックを満たす環境で運用する。
c. 情報システム管理者は、利用者がインストール可能なソフトウェアを定期的に見直す。
d. 利用者は認可されていないソフトウェアをインストールしてはならず、業務上、必要な場合は、情報システム管理者の承認を得た上でインストールする。
e. ファイル共有ソフトなど、ウイルス感染や不正アクセスなどの原因となりやすいソフトウェアのインストールを禁じる。

**ワンポイントアドバイス**
組織は、利用者がインストールできるソフトウェアの種類について、厳密な規則を定めて施行することが大切です。

**【8.25 セキュリティに配慮した開発のライフサイクル】**

**実施手順（例）**

セキュリティに配慮した開発のための方針を以下に記す。
a. 開発の初期段階でセキュリティ要件を明確化する。
b. 開発環境は、「8.31 開発環境、試験環境及び運用環境の分離」の「b. セキュリティに配慮した開発環境」に従う。
c. 開発の各段階でセキュリティレビューを行い、セキュリティ要件が満たされているかを確認する。
d. 開発したシステムに脆弱性がないかテストする。
e. 開発文書（仕様書、設計書、テスト仕様など）は、必要最低限の者だけがアクセスできるようにする。
f. 受託開発または客先への派遣による開発では、クライアントから提示のあったセキュリティの方針・ルールなどに従う。

**ワンポイントアドバイス**
ソフトウェアやシステムのセキュリティに配慮した開発のための規則を定めることが大切です。

**【8.26 アプリケーションのセキュリティの要求事項】**

**実施手順（例）**

a. アプリケーションを取得する際、リスクアセスメントを通じてアプリケーションの情報セ

キュリティ要求事項を決定する。必要に応じて、情報セキュリティの専門家の支援を受け、情報セキュリティ要求事項を決定する。

b. セキュリティに配慮したシステムを構築するための原則は、以下の通りとする。
   - 情報セキュリティ事象を防止・検知し、対応するために必要な管理策を分析すること。
   - 情報セキュリティ要求事項を満たすための費用・時間・複雑さを考慮すること。

**ワンポイントアドバイス**

ネットワークを介してアクセス可能なアプリケーションは、ネットワークに関連した脅威を受けやすいため、リスクアセスメントの実施や、管理策を決定することが大切です。

**【8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則】**

**実施手順（例）**

a. 社内使用の情報システムおよび外部向けに提供する情報システムの開発に際しては、情報セキュリティ事項を明確にし、要件定義として記録する。
b. 開発の各段階でセキュリティレビューを行い、セキュリティ要件が満たされているかを確認する。
c. 開発したシステムに脆弱性がないかテストする。

**ワンポイントアドバイス**

セキュリティに配慮したシステム構築の原則および確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするため、定期的にレビューすることが大切です。

**【8.28 セキュリティに配慮したコーディング】**

**実施手順（例）**

a. ユーザーが入力したデータを確認し、問題がある場合は読み込まないようにする。
b. セキュリティ上の問題を発見しやすくするため、設計は可能な限りシンプルにする。
c. ユーザーには必要最小限の権限・機能を与える。
d. 他のシステムに送信するデータは、サニタイズ（特殊文字を一般的な文字に変換すること）を行い、不正操作を防止する。

**ワンポイントアドバイス**

コーディングの原則が定められていない場合、コードの書き方がそれぞれ異なってしまうことで、コードが読みづらく、脆弱性が生まれる危険性があります。セキュリティに配慮したコーディングの規則を定め、コードの書き方を統一することが大切です。

**【8.29 開発及び受入れにおけるセキュリティ試験】**

**実施手順（例）**

a. 情報システムのセキュリティテストは、運用に移行する前に行う。
b. システムの受入れ試験
   - 情報システムの導入または改修の際は、受入れ時に動作確認を行う。
   - 必要に応じて受入れテストの仕様書を作成し、確認を行う。
   - 必要に応じて、コード分析ツールや脆弱性スキャナのような自動化ツールを利用し、セキュリティに関連する欠陥を修正する。
   - 受入れ試験の結果は、受入れ部門の管理者および情報システム管理者が承認する。

**ワンポイントアドバイス**

効果的な試験を確実にするために、試験環境、ツール、技術の試験および監視も考慮する必要があります。

**【8.30 外部委託による開発】**

**実施手順（例）**

情報システムの開発を外部に委託する場合の手順は以下に従う。
a. 「委託先審査票」によって委託先を評価、選定、およびあらかじめ定められた頻度（最低年１回）で再審査し、また、契約の履行状況を監視する。
b. 委託先との契約を締結する。（契約書には情報セキュリティ要求事項を含める。）
c. 成果物の品質および正確さを評価するため、「8.29 開発及び受入れにおけるセキュリティ試験」に定める「b. システムの受入れ試験」を実施する。

**ワンポイントアドバイス**

外部委託したシステム開発に関する活動を随時、指導、監視およびレビューすることが大切です。

**【8.31 開発環境、試験環境及び運用環境の分離】**

**実施手順（例）**

a. 情報システムの開発に際しては、開発・テスト環境と本番環境を、物理的・論理的に分割する。
   - セキュリティに配慮した開発環境
     開発は、開発業務を行わない従業員から分離した場所およびシステムにて行う。また開発環境は、運用環境から分離する。
   - ソースコードおよび設定ファイルは、不意の消去や改ざんから保護するため、必要最

小限の者だけがアクセスできるようにする。

**ワンポイントアドバイス**

開発および運用環境に変更を加える際は、組織としての事前レビューおよび承認を徹底することが大切です。

**【8.32 変更管理】**

**実施手順（例）**

a. 変更管理は以下のプロセスで行う。
   1. 変更の承認
      変更を行う前にその変更の必要性、変更が及ぼす影響、変更によるリスクの変動について評価し、情報システム管理者の承認を得る。
   2. 変更のテスト
      変更を適用する前に、情報システムへの影響を確認するためにテストを行う。
   3. 変更の監査
      変更後に変更が適切に行われたか否かを監査によって確認する。

b. 情報システム管理者は、サーバに周辺機器を接続する場合や、サービスパックを適用する場合、事前に情報収集し、問題の有無を確認する。万が一、適用後に問題が生じた場合は、再インストールすることで問題解決を即座に実施する。

c. OS やパッケージソフトウェアを変更する際は、情報システム管理者はテスト機や予備機を用いて、現在の情報システムが変更後の OS 上で問題なく動作するかを検証する。

d. パッケージソフトウェアのカスタマイズを原則として禁じる。万が一、修正を行う場合は、動作上の影響およびベンダーから将来的に受けるサポートへの影響を考慮し、情報システム管理者の許可を得る。

**ワンポイントアドバイス**

変更管理手順は、情報の機密性、完全性、可用性を確実にするために、設計の初期段階からその後のすべての保守作業までのシステム開発のライフサイクル全体にわたって文書化し、実装することが大切です。

**【8.33 試験情報】**

**実施手順（例）**

a. テストデータとして個人情報を使用することを禁じる。

b. 実データをテストデータとして使用する場合は、情報システム管理者の承認を得てから使用する。テスト終了後は、実データを直ちに削除し、情報システム管理者に対して報告す

る。

**ワンポイントアドバイス**

テストデータは、注意深く選定し、保護し、管理することが大切です。

**【8.34 監査試験中の情報システムの保護】**

**実施手順（例）**

a. 情報システムの監査は、システム停止のリスクを考慮し、営業時間外もしくは休日を利用して実施することを原則とする。
b. 情報システムのメンテナンスなどにより情報システムの稼動を停止する場合は、業務への影響を及ぼさない範囲または時間帯で行うように計画する。

**ワンポイントアドバイス**

運用システムのアセスメントを伴う監査活動およびその他の保証活動を計画し、試験者と管理層の間で合意することが大切です。

## 18-2-18. ネットワークセキュリティ

**【8.20 ネットワークのセキュリティ】**

**実施手順（例）**

a. ネットワーク図および装置（例：ルータ、スイッチ）の構成ファイルを含む文書を最新に維持する。
b. 社内ネットワークへ接続する際は、情報システム管理者の承認を受け、指示された手順に従う。
c. 情報システム管理者は、ネットワークにおける社外との境界にはファイアウォールを設けるなど、不正侵入対策を施す。
d. ネットワーク装置のファームウェアの定期的なアップデートを行う。
e. 他人の ID、パスワードで、社内ネットワークに接続することを禁じる。
f. 一旦、社内ネットワークから切り離したパソコンなどは、ウイルスチェックなどの安全確認を行ってから再接続する。
g. 持ち込みおよび私有 PC 利用の場合は、社内ネットワークに接続しない。やむを得ず接続する場合は、情報システム管理者が指定するソフトウェアによりウイルスチェックを行う。
h. 無線 LAN を使用する場合は、情報システム管理者の承認を得て、暗号化、接続パソコンの認証など、十分な安全対策を実施する。
i. 不特定が利用できる公衆無線 LAN や WiFi スポットに接続することは禁じる。

**ワンポイントアドバイス**
ネットワークや、ネットワークをサポートする情報処理施設における情報を、ネットワークを通じた危険から保護することが大切です。

**【8.21 ネットワークサービスのセキュリティ】**

| 実施手順（例） |
| --- |
| a. 利用しているネットワークサービスを特定する。<br>b. 情報システム管理者は、ネットワークサービスを利用する場合は、ネットワークサービス提供者と SLA を締結する。 |
| **ワンポイントアドバイス**<br>ネットワークサービスには、接続・プライベートネットワークサービスおよびネットワークセキュリティ管理のためのソリューション（ファイアウォール、IDS など）が含まれます。 |

## 18-2-19. ネットワークの分離

**【8.22 ネットワークの分離】**

| 実施手順（例） |
| --- |
| a. インターネットと社内 LAN との境界にファイアウォールを設置する。<br>b. メール、Web サーバなどの公開サーバは、社内のネットワークと分離する。<br>c. ゲスト用の無線アクセスネットワークを、社内用の無線アクセスネットワークから分離する。 |
| **ワンポイントアドバイス**<br>各領域の境界は、明確に定めることが大切です。ネットワーク領域間のアクセスが認められる場合は、境界にファイアウォールなどを設けて制御することが大切です。 |

## 18-2-20. Web フィルタリング

**【8.23 ウェブ・フィルタリング】**

| 実施手順（例） |
| --- |
| フィルタリングソフトを利用し、業務上不必要な Web サイト、危険性のある Web サイトへアクセスすることを防ぐ。 |
| **ワンポイントアドバイス**<br>システムがマルウェアによって危険にさらされることを防ぐために、認可されていないウェブ資源へのアクセスを防止することが大切です。 |

## 18-2-21. 暗号の使用

**【8.24 暗号の使用】**

**実施手順（例）**

a. 暗号利用のための規則

- SSL/TLS
  当組織の Web サイトの通信は、SSL/TLS を用いて暗号化する。
- 無線 LAN
  無線 LAN の通信は暗号化し、暗号化の規格は脆弱性の報告されていない安全な方法とする。

b. 鍵の管理

- SSL/TLS
  情報システム管理者は、証明書に対する秘密鍵を適切に管理する。
- 無線 LAN
  アクセスポイントの管理者画面は、情報システム管理者のみがアクセスでき、そのパスワードを厳重に管理する。

c. 重要データの暗号化

- 暗号化の対象とするデータを選定する。
- 利用する暗号の種類を決める。
- 暗号鍵のライフサイクルに関する方針を策定する。
- 暗号の管理責任者を定める。

**ワンポイントアドバイス**

業務や情報セキュリティ要求事項に従い、暗号に関連する法令・規制・契約上の要求事項を考慮し、情報の機密性・真正性・完全性を保護するための暗号の適切かつ効果的な使用を確実に履行することが大切です。

| 詳細理解のため参考となる文献（参考文献） | |
|---|---|
| ISO/IEC 27002:2022 | https://www.iso.org/standard/75652.html |

# 18-3. 実施手順を適用するセキュリティ概念

## 18-3-1. Security by Design

**関連する主な管理策**

5.1、5.7、5.9、5.19、5.20、5.24、5.26~5.29、5.37、8.9、8.15、8.16、8.22、8.25~8.34

Security by Design とは「情報セキュリティを企画、設計段階から組み込むための方策」で、開発プロセスの最初の段階からセキュリティを考慮することで、開発システムのセキュリティを確保するという考え方です。従来のように、後づけでセキュリティ機能を追加したり、システムの導入直前に脆弱性診断などを実行したりする方法の場合、手戻りが多発することがあり、結果的に開発コストが増大する可能性があります。企画・設計の段階からセキュリティ対策を行うことで、手戻りが少なくなり、コストの削減につながり、保守性のよいシステム・ソフトウェアになります。


図 60. セキュリティ対策の実施タイミング

### Security by Design 導入のメリット

- 手戻りが少なくなり、納期を守れる

- コストを削減できる
- 保守性の高いソフトウェアができる

Security by Design の工程ごとに実施内容を紹介します。また、実施手順を策定する上で、選択すべき管理策の例を紹介します。

| 実施手順（例） | 選択すべき管理策（例） |
|---|---|
| **セキュリティリスク分析**<br>● システムで取扱う重要情報のフローやライフサイクルがわかる内容を記載したシステムプロファイルの作成（ステークホルダー、実施業務、他システムとの連携方法などがわかるように作成）<br>● システムプロファイルに基づくセキュリティ脅威の特定<br>● セキュリティ脅威の発生可能性、システムへの影響度を踏まえたリスク分析の実施<br>● リスク分析結果を踏まえたセキュリティ対応方針の決定（リスク対応優先度、遵守すべきセキュリティ標準、検証方法、対応リソースなど） | 5.1 情報セキュリティのための方針群<br>5.9 情報及びその他の関連資産の目録 |
| **セキュリティ要件定義**<br>● 遵守すべきセキュリティ標準（セキュリティベースライン）やリスク分析結果などに基づく、システムとして満たすべきセキュリティ要件の定義（機能、非機能面） | 8.26 アプリケーションのセキュリティの要求事項 |
| **セキュア調達**<br>● セキュリティ要件に基づいて、調達仕様におけるセキュリティ仕様策定<br>● セキュリティ仕様に関する、委託先との責任範囲の明確化<br>● 委託先に求めるセキュリティ管理基準の策定<br>● セキュリティ仕様を満たす能力を有した安全な委託先の選定<br>● 不正侵入の経路となるバックドアなどが含まれていない、継続的なサポートを受けられる安全なプロダクトの選定 | 5.19 供給者関係における情報セキュリティ<br>5.20 供給者との合意における情報セキュリティの取扱い |
| **セキュリティ設計**<br>● セキュリティ設計の実施 | 8.27 セキュリティに配慮したシステムアーキテクチャ及びシ |

| | |
|---|---|
| ➢ アプリケーションセキュリティ<br>➢ OS セキュリティ<br>➢ ミドルウェアセキュリティ<br>➢ ネットワークセキュリティ<br>➢ クラウドセキュリティ<br>➢ 物理セキュリティ<br>➢ セキュリティ運用（平時、有事） | ステム構築の原則 |
| **セキュリティ実装**<br>● 設計に基づくシステムにおけるセキュリティ機能の実装<br>● セキュリティ設計に基づくアプリケーションのセキュアコーディング<br>● セキュリティ設計に基づくプラットフォームのセキュリティ設定の実施（堅牢化、要塞化）<br>➢ OS セキュリティ<br>➢ ミドルウェアセキュリティ<br>➢ ネットワークセキュリティ<br>➢ クラウドセキュリティ<br>➢ 物理セキュリティ | 8.28 セキュリティに配慮したコーディング |
| **セキュリティテスト**<br>● セキュリティ機能テストの実施（単体テスト、結合テスト、システムテストなど）<br>● 脆弱性診断の実施<br>➢ Web アプリケーション脆弱性診断<br>➢ プラットフォーム脆弱性診断<br>➢ スマートフォンアプリケーション診断<br>➢ 高度セキュリティ診断（ペネトレーションテスト、レッドチーム演習など）<br>● 機能テストで検出されたバグの是正対応<br>● 脆弱性診断で検出された脆弱性に対する、リスクベースの是正対応 | 8.29 開発及び受入れにおけるセキュリティ試験<br>8.33 試験情報<br>8.34 監査試験中の情報システムの保護 |
| **セキュリティ運用準備**<br>● セキュリティ運用体制の確立<br>● 下記項目に対応したセキュリティ運用手順の整備<br>平時の運用 | 5.24 情報セキュリティインシデント管理の計画及び準備<br>5.29 事業の中断・阻害時の情報セキュリティ |

| | |
|---|---|
| ➢ 構成管理、変更管理<br>➢ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知<br>➢ 脅威情報収集、自システムへの影響分析<br>➢ CVSS などに基づく、リスクに応じた脆弱性対応<br>➢ 定期的な脆弱性診断の実施<br>有事の運用<br>➢ インシデント対応<br>● システム運用において人的ミスが発生する可能性のある箇所の洗い出し、是正<br>● 有事を想定したセキュリティ運用訓練の実施 | 8.9 構成管理<br>8.32 変更管理<br>8.19 運用システムに関わるソフトウェアの導入 |
| **セキュリティ運用**<br>● セキュリティ運用を行う要員の教育/訓練の実施、重要な情報を取扱う要員のスクリーニング（要員のスキルや行動特性などを考慮）<br>● セキュリティ運用の実施（下記）<br>平時の運用<br>➢ 構成管理、変更管理<br>➢ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知<br>➢ 脅威情報収集、自システムへの影響分析、是正対応<br>➢ CVSS などに基づく、リスクに応じた脆弱性対応<br>➢ 定期的な脆弱性診断の実施<br>有事の運用<br>➢ インシデント対応 | 5.7 脅威インテリジェンス<br>5.26 情報セキュリティインシデントへの対応<br>5.29 事業の中断・阻害時の情報セキュリティ<br>5.37 操作手順書<br>8.9 構成管理<br>8.15 ログ取得<br>8.16 監視活動<br>8.32 変更管理 |

**Security by Design 実施における留意事項**

- 工程間でセキュリティ対策の不整合が起きないように注意すること
- 組織として考慮すべきリスクや組織能力を踏まえて実現可能なレベルで実施し、PDCA サイクルを回しながら成熟度を高めていくこと

| 詳細理解のため参考となる文献（参考文献） | |
|---|---|
| セキュリティ・バイ・デザイン導入指南書 | https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/security-by-design.html |
| 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 |

## 18-3-2. ゼロトラスト、境界防御モデル

**関連する主な管理策**

5.9、5.15~5.23、5.29~5.30、8.1~8.3、8.15~8.16、8.21、8.32

### ゼロトラストの定義

ゼロトラスト（ZT）は、従来の境界線によるセキュリティ対策とは異なり、ネットワーク内のすべてのデバイスやユーザーを信頼せず、あらゆるアクセスをゼロから検証するという考え方です。これにより、内部からの脅威や、一度内部に侵入された場合の被害を最小限に抑えることを目指します。具体的には、多要素認証、最小権限の原則、継続的な監視など、複数のセキュリティ対策を組み合わせることで、アクセス制御を強化します。

**境界防御モデルとゼロトラストの違い**

境界防御モデルは、信用する領域（社内）と信用しない領域（社外）に境界を設け、組織が守るべき情報資産は信用する境界内部に存在するという前提をもとに、境界線でセキュリティ対策を講じることで、境界外部からの脅威を防ぐという考え方です。

一方、ゼロトラストは、「境界」の概念をなくし、守るべき情報資産にアクセスするものはすべて確認し、認証・認可を行うことで脅威を防ぐという考え方です。

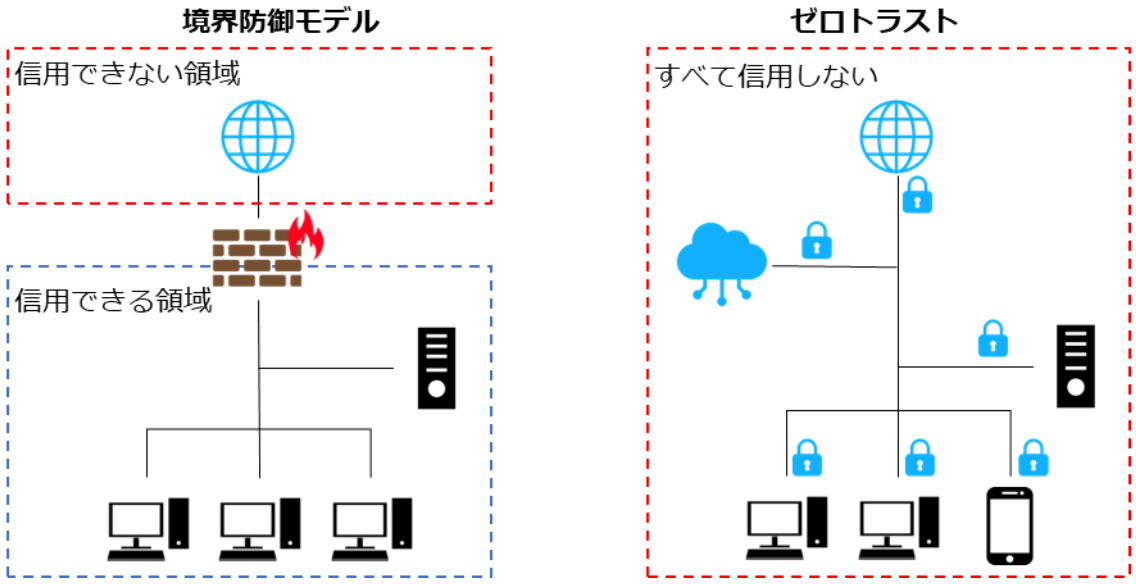


図 61. 境界防御モデルとゼロトラストの概要図

現在、クラウドサービスの普及やモバイル端末の活用、テレワークによる働き方の多様化により、内部と外部を隔てる「境界」そのものが曖昧になりつつあります。その結果、従来の社内・社外の境界でセキュリティ対策を行う「境界防御モデル」では、サイバー攻撃やマルウェア感染などの脅威から情報資産を守ることが難しくなってきています。こうした問題を解決するものとして、「ゼロトラスト」という考え方が注目されています。

One Point

**ゼロトラストと境界防御の関係**

ゼロトラストは、境界防御モデルで守ることが困難な脅威に対して適用する対策ではあるもの

の、「境界防御モデルを排除する考え」ではありません。強固なセキュリティを構築するにあたり、すでに用いられている境界防御モデルを活かすことが大切です。

## ゼロトラスト導入に向けた進め方

### 準備工程

ゼロトラストを導入する準備として、資産（デバイスやネットワークなど）、主体（ユーザー・権限など）、ビジネスプロセスについて詳細に理解する必要があります。ゼロトラストを導入する準備として、資産、主体、データフロー、ワークフローの調査を行います。

### ゼロトラスト導入プロセス

準備工程を実施した以降は、次のプロセスで進めます。

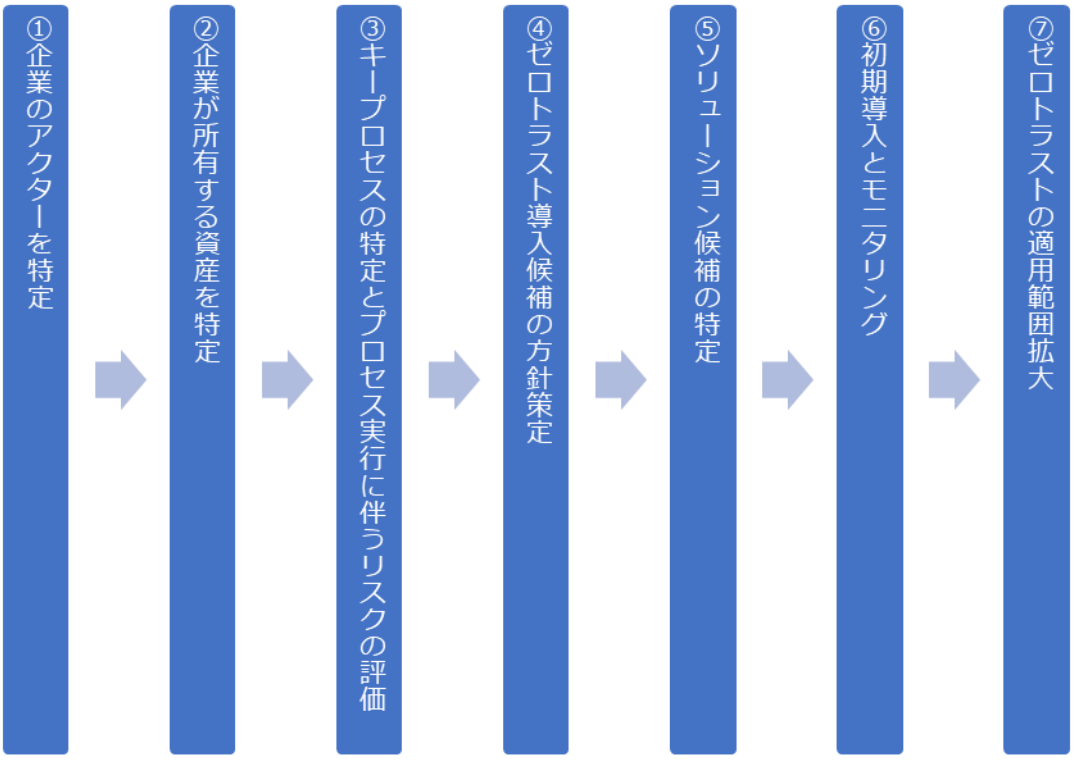


図 62. ゼロトラスト導入プロセス

（出典）IPA「ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～ 」をもとに作成

| 詳細理解のため参考となる文献（参考文献） | |
|---|---|
| ゼロトラスト導入指南書～情報系・制御系システムへのゼロトラスト導入～ | https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf |

ゼロトラスト導入の各プロセスで実施すべき内容を説明します。

### 1.企業のアクターを特定

企業の主体には、ユーザーに紐づいたアカウントと、サービスに紐づいたアカウントの両方が含まれることがあります。どのユーザーにどのレベルの権限を与えるのかは精査が必要です。基本的には、必要な対象に必要な権限だけ与えるという最小権限の考え方で整理します。

**2.企業が所有する資産を特定**

ゼロトラスト・アーキテクチャ（ゼロトラストの概念を利用し、コンポーネントの関係、ワークフロー計画、アクセスポリシーなどを含むサイバーセキュリティ計画のこと）は、デバイスを識別して管理する機能が必要であり、企業内のデバイスはもちろん、企業所有ではないデバイスについても識別し、監視する機能が必要です。よって、企業の情報にアクセスするデバイスについては、「シャドーIT」も含めて可能な限り資産化する必要があります。なお、企業によって可視化されているもの（例：MAC アドレス、IP アドレス）と、管理者のデータ入力による追加分も含まれます。

**3.キープロセスの特定とプロセス実行に伴うリスクの評価**

業務プロセス、データフロー、および組織のミッションにおけるそれらの関係（プロセス）を特定します。次に信用度レベルをつけ、ゼロトラストへ移行するプロセスを決めます。認証・認可の判断を導入することによる失敗のリスクを考慮し、初めはビジネスインパクトの低いビジネスプロセスから開始するとよいでしょう。ある程度、認証・認可の挙動を掴んでから対象を広げていくことで、リスクを抑えることができます。

**4.ゼロトラスト導入候補の方針策定**

資産またはワークフローを特定したら、影響を受ける対象をすべて特定します。（上流リソース（例：ID 管理システム）、下流リソース（例：セキュリティ監視）、エンティティ（例：主体ユーザー）。次に企業管理者は、候補となるビジネスプロセスで使用されるリソースの信用度レベルの重みを決定します。それらを踏まえて、何を対象に、どこへゼロトラストの機能を導入するのかを決定します。

**5.ソリューション候補を特定**

④で策定した内容をもとに、導入箇所に適するソリューション、製品を検討します。製品、ソリューションについては後述します。

**6.初期導入とモニタリング**

初期導入時には、適用したポリシーや初期動作の確認を含め、監視モードで運用することが推奨されます。初期導入後はしばらくシステムの動作を監視し、必要に応じて、システムの安全性を保ちつつ、業務効率を最大化するために調整を行います。

**7.ゼロトラストの適用箇所拡大**

運用フェーズに入ったら、ネットワークや資産の監視は継続し、トラフィックの記録を行います。これらを実施していく中で、ポリシーの変更や適用箇所の拡大を適宜実施していきます。ポリシー変更などを実施する場合は、深刻な問題にならないように行います。

## ゼロトラスト導入に向けた実施手順（例）

「ゼロトラスト導入に向けた進め方」で説明したプロセスをもとに、ゼロトラストを導入するための実施手順を、例を用いて説明します。また、実施手順を策定する上で、選択すべき管理策の例を紹介します。

| 実施手順（例） | 選択すべき管理策（例） |
|---|---|
| **準備工程**<br>新たに導入する必要のあるプロセスやシステムを判断することおよびアクセスの認証・認可を正しく行うため、現在の運用状況を把握する。<br>a. 情報システム管理者は、次の事項を調査し、詳細に理解する。<br>● 資産（デバイスやネットワークなど）<br>● 主体（ユーザー・権限など）<br>b. 経営者は、次の事項を調査し、詳細に理解する。<br>● ビジネスプロセス | 5.9 情報及びその他の関連資産の目録<br>5.16 識別情報の管理<br>5.18 アクセス権<br>8.2 特権的アクセス権 |
| **① 企業のアクターを特定**<br>a. 情報システム管理者は、業務に必要な者のみ情報へアクセスできる権限を与える。<br>b. アクセス権限および操作権限は、認められた場合以外は与えないようにする。 | 5.15 アクセス制御<br>5.16 識別情報の管理<br>5.17 認証情報<br>5.18 アクセス権<br>8.2 特権的アクセス権<br>8.3 情報へのアクセス制限 |
| **② 企業が所有する資産を特定**<br>a. デバイスを識別して管理する。<br>企業の情報にアクセスするデバイスは、シャドーIT を含めて、すべて識別して管理する。<br>b. シャドーIT は可能な限り資産化する。 | 5.9 情報及びその他の関連資産の目録<br>8.1 利用者終端装置 |

| | |
|---|---|
| **③ キープロセスの特定とプロセス実行に伴うリスクの評価**<br>a. 業務プロセス、データフロー、組織のミッションにおける業務プロセスとデータフローの関係（プロセス）を特定する。<br>b. 特定したプロセスのうち、ゼロトラストに移行するプロセスを決定する。<br>認証・認可の判断を導入することによる失敗のリスクを考慮し、初めは組織の事業に与える影響が低いビジネスプロセスを選択し、徐々に対象を広げる。 | 5.29 事業の中断・阻害時の情報セキュリティ<br>5.30 事業継続のための ICT の備え |
| **④ ゼロトラスト導入候補の方針策定**<br>a. 資産、プロセスの特定後、ゼロトラストの導入により影響を受ける対象をすべて特定する。<br>● 上流リソース（例：ID 管理システム）<br>● 下流リソース（例：セキュリティ監視）<br>● エンティティ（例：主体ユーザー）<br>b. ゼロトラスト導入候補となるビジネスプロセスで使用されるリソースの重要さを決定する。<br>c. リソースの重要さを踏まえて、何を対象に、どこへゼロトラストの機能を導入するのかを決定する。 | 5.9 情報及びその他の関連資産の目録 |
| **⑤ ソリューション候補を特定**<br>④で策定した内容をもとに、導入箇所に適するソリューションを検討する。 | 5.19 供給者関係における情報セキュリティ<br>5.20 供給者との合意における情報セキュリティの取扱い<br>5.21 ICT サプライチェーンにおける情報セキュリティの管理<br>5.22 供給者のサービス提供の監視、レビュー及び変更管理<br>5.23 クラウドサービスの利用における情報セキュリティ<br>8.21 ネットワークサービス |

| | |
|---|---|
| | のセキュリティ |
| **⑥ 初期導入とモニタリング**<br>a. ソリューションの初期導入時は、実際に通信の遮断は行わず、適用したポリシーや初期動作の確認を行う。<br>b. 動作に問題がないことを確認後、運用を開始する。 | 8.16 監視活動 |
| **⑦ ゼロトラストの適用箇所拡大**<br>a. 運用開始後は、ネットワークや資産の監視は継続しつつ、トラフィックの記録を行う。<br>b. トラフィックを記録していく中で、ポリシーの変更や適用箇所の拡大を適宜実施する。<br>c. ポリシー変更を実施する場合は、影響が問題にならないように確認する。 | 8.15 ログ取得<br>8.16 監視活動<br>8.32 変更管理 |

## ゼロトラストを実装するための主な技術要素

ゼロトラストを実装するために必要となる主な技術要素（製品、ソリューション）について説明します。

### CASB（Cloud Access Security Broker）

CASB とは、クラウドサービスの利活用における情報セキュリティのコンセプトですが、それを実装した製品も CASB と呼ばれます。CASB は、以下の 4 機能を備えています。

- 可視化
  - クラウドストレージへの不審なアップロードやダウンロードの監視や、シャドーIT の検知を行います。
- データセキュリティ
  - アクセス権限の逸脱や機密情報の持ち出しをチェックし、ブロックします。
- コンプライアンス
  - セキュリティに関する基準やポリシーを満たしていることを監査します。
- 脅威防御
- セキュリティ脅威の検出、分析や防御を行います。

### SWG（Secure Web Gateway）

SWG は、外部ネットワークに対するすべてのアクセスを中継することで、危険なコンテンツをブロック・フィルタリングするセキュリティ製品です。物理的なアプライアンスとして提供

されるものもありますが、クラウド型のソリューションが一般的です。利用者によるリスクの高い行為や許可されていない操作をブロックして、エンドポイントデバイスと社内ネットワークの安全性を保ちます。SWG の主な機能は、次の通りです。

- リスクの高い URL や IP アドレスへのアクセスの遮断
- マルウェアの検出とブロック
- アプリケーション制御

**ZTNA（Zero Trust Network Access）**

ZTNA は、ユーザー認証によって、特定のサービスやアプリケーションへの安全なアクセスを提供する仕組みです。VPN と異なり、ネットワーク全体へのアクセスを許可するのではなく、特定のサービスやアプリケーションのみの利用を許可します（ユーザーが許可されていないサービスなどは表示されず、利用もできません）。必要最小限の権限を付与することで、セキュリティを向上することができます。

**FWaaS（Firewall as a Service）**

FWaaS とは、ファイアウォールやその他ネットワークセキュリティの機能をクラウドサービスで提供するソリューションです。URL フィルタリングや IPS、アプリケーション制御の機能を持ち、セキュリティを高めます。FWaaS は、オンプレミス型のファイアウォールよりもネットワークの変更に柔軟に対応できます。

**SDP（Software Defined Perimeter）**

SDP の機能はほぼ ZTNA と同じで、ユーザーに特定のサービスやアプリケーションへの安全なリモートアクセスを提供します。SDP は、ネットワークの内部と外部の境界（Perimeter）をソフトウェア上で構築、集中的に制御し、アクセス制御に関わる設定を柔軟に動的に変更することにより安全にデータを転送する技術のことです。従来のファイアウォールの概念をソフトウェア上に持ち、利用者がどこにいても動的にアクセスを制御します。

## 18-3-3. SASE

SASE（Secure Access Service Edge）とは、「ネットワーク機能」と「セキュリティ機能」をまとめて提供する仕組みです。「ネットワーク機能」と、接続の安全性を確保する「セキュリティ機能」をまとめて 1 つの製品として提供します。

SASE に含まれる主な機能に以下のものがあります。

**ネットワーク機能**

- SD-WAN（Software Defined - Wide Area Network）

※SD-WAN については、「18-3-4. ネットワーク制御（Network as a Service）」で説明します。

**セキュリティ機能**

- SWG（Secure Web Gateway）
- CASB（Cloud Access Security Broker）
- FWaaS（Firewall as a Service）
- ZTNA（Zero Trust Network Access）

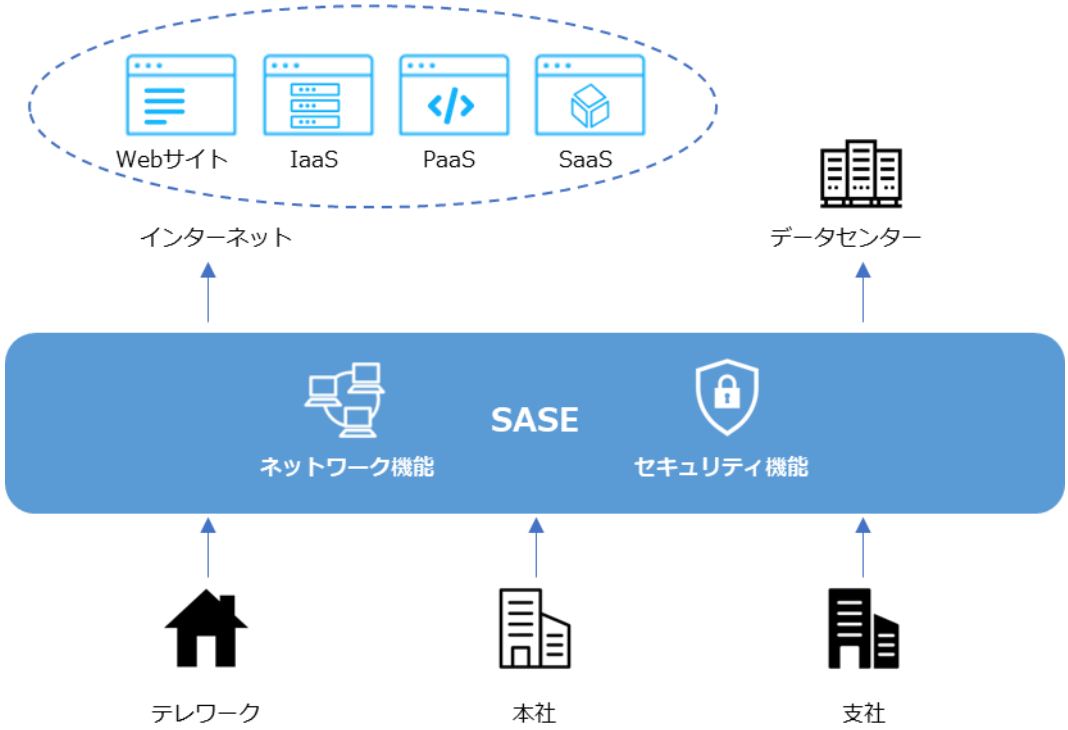


図 63. SASE のイメージ図

## ゼロトラスト導入事例

| 概要 |
| --- |
| 地方銀行は、個人顧客向けサービス以外にも、法人顧客向けサービスの充実を図っています。法人向け営業力強化方策の 1 つとして、営業職員にモバイル端末を配布し、場所を問わずに行内システムにアクセスを可能にすることになりました。そこで、高いセキュリティが求められる金融機関のリモートアクセス環境として、ゼロトラストネットワークアクセス機能を備えた「ZTNA」を導入しました。結果、安全で安定したリモートアクセスが可能となり、業務効率化と営業力強化を実現しました。 |

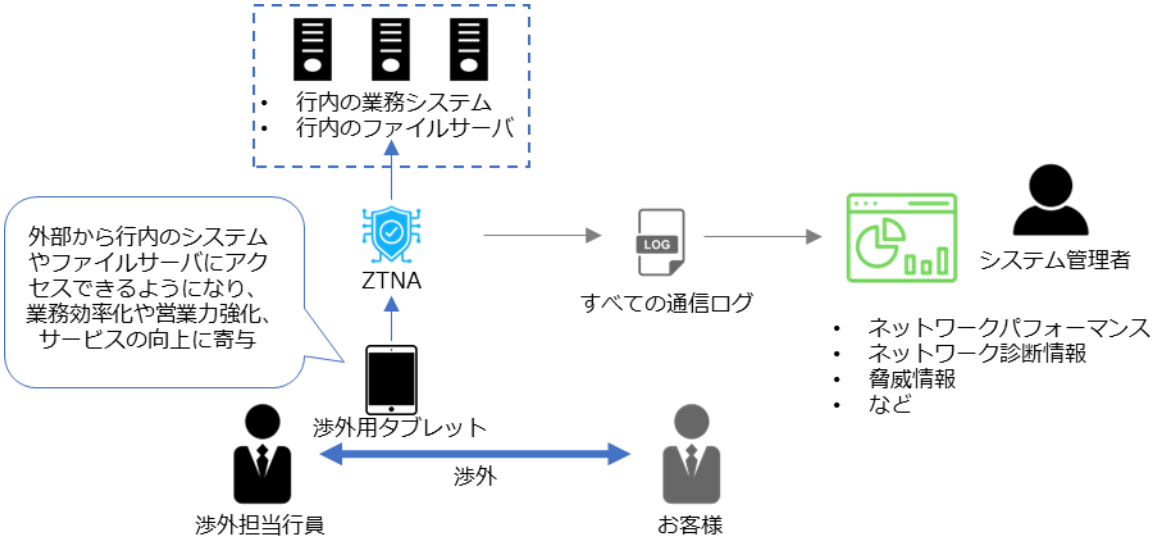


図 64. 事例のイメージ図

## 導入前の課題

営業力強化に向けてモバイル端末の必要性が高まり、次の課題があげられました。

- 行内だけの運用だったモバイル端末活用を、いつでもどこでも働ける環境に拡大すること。
- 渉外用タブレットは、外から行内システムやファイルサーバにアクセスできる必要があること。
- 外部でモバイル端末を利用するためには、セキュリティや性能の担保が必要であること。

## 選定の決め手

次の事項が導入の決め手となりました。

- リモートアクセスとセキュリティのゼロトラスト機能が一体になっていること。
- 動作検証でリモートアクセス時の速度・安定性が高いこと。

## 導入後の効果

導入後の効果は次の通りです。

- 営業職員が行内に戻らず業務を遂行できるようになり、業務が効率化したこと。
- 許容した内容や業務だけの通信に限定できるので、安心して使用できること。
- 今後は渉外用タブレットを活用した業務改革の推進が見込まれること。

| 詳細理解のため参考となる文献（参考文献） | |
|---|---|
| （参考資料 1）民間企業におけるゼロトラスト導入事例 | https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5805a275-3e16-4296-8a94-6557b58c6a4c/dd52a824/20231124_meeting_network_casestudie_03.pdf |

## 18-3-4. ネットワーク制御（Network as a Service）

| 関連する主な管理策 |
| --- |
| 5.23、6.7、8.20~8.24 |

ネットワーク制御を説明するにあたって、クラウドサービスについて説明します。

クラウドサービスとは、サービス事業者がハードウェアの機能（サーバ、ハードディスクなど）、プラットフォームの機能（データベースやプログラム実行環境など）、ソフトウェアなどを、ネットワーク経由で利用者に提供するサービスのことです。利用者は、どの端末からでもさまざまなサービスを利用することができます。クラウドサービスの利用形態には、主に「IaaS＝アイアース」、「PaaS＝パース」、「SaaS＝サーズ」があります。また、「NaaS＝ナース」と呼ばれるネットワークインフラを提供するサービスもあります。

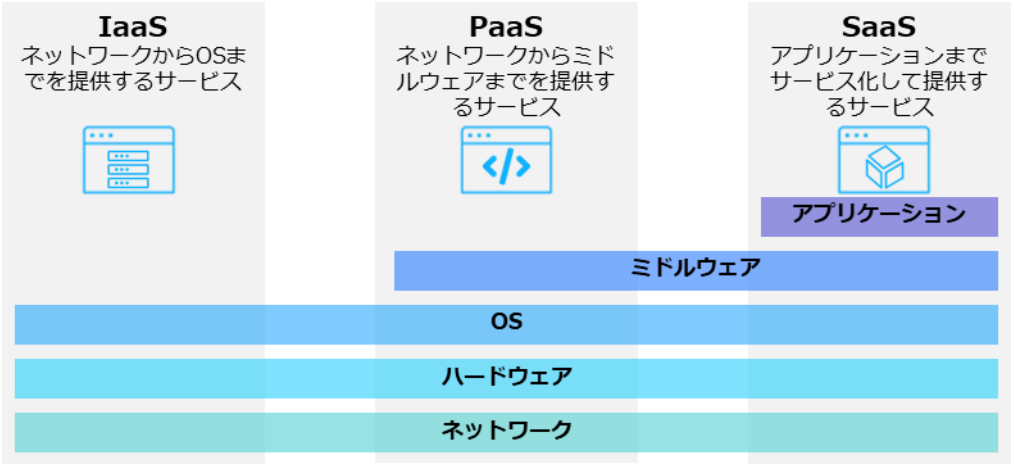


図 65. クラウドサービス利用形態の概要図

### IaaS（Infrastructure as a Service）

IaaS とは、インターネット経由でネットワークやサーバ（CPU・メモリ・ストレージ）などのハードウェアやインフラ機能を提供するサービスのことです。IaaS を利用することで、従来は自社で購入、構築し、運用する必要があったハードウェアやインフラの機能を、必要なときに必要なだけ利用できます。

### PaaS（Platform as a Service）

PaaS とは、インターネット経由でアプリケーションサーバやデータベースなどのアプリケーションを実行するためのプラットフォーム機能を提供するサービスのことです。PaaS を利用することで、アプリケーションの開発前段階で必要な開発環境の準備（サーバの設置や OS やミドルウェアのインストールと設定、ネットワークの設定など）を省略できます。

### SaaS（Software as a Service）

SaaS とは、インターネット経由で電子メール、顧客管理、財務会計などのアプリケーションソフトの機能を提供するサービスのことです。アカウントを持っていれば、インターネット経由でどこからでもアクセスすることができたり、チームでファイルやデータを共有できたりします。

**NaaS（Network as a Service）**

NaaS とは、インターネット経由でネットワークインフラを提供するサービスのことです。NaaS の導入により、ネットワーク環境の変更に柔軟に対応できるようになります。NaaS に含まれる主要な機能として、SDN、SD-WAN などがあります。

## SDN・SD-WAN

クラウドサービスや Web 会議、リモートワークの普及に伴い、ネットワーク回線にアクセスが集中し、通信速度が低下したり、サービスへの接続ができなくなったりするなどの問題があります。その解決策として SDN を応用した SD-WAN があります。SDN、SD-WAN について説明します。

### SDN（Software Defined Networking）

SDN とは、ソフトウェアを用いてネットワーク構成を動的に変更することです。ネットワークを構成している機器（ルータやサーバ、スイッチなど）を、ソフトウェアを介して一括制御することで、機器設定やネットワーク構成を柔軟に変更できます。SDN のメリットは、ネットワーク機器に対して一括で設定を行えることです。従来のルータ、スイッチといった物理的なネットワーク機器・製品は、1 台ごとに個別に設定を行う必要があり、大規模なネットワーク構成を変更する際には、大きな作業負荷がかかりました。しかし、SDN を用いてネットワークを制御することで、管理が 1 か所で行えるようになるため、ネットワーク機器・製品ごとに個別設定が不要になり、作業負荷が大幅に軽減できます。

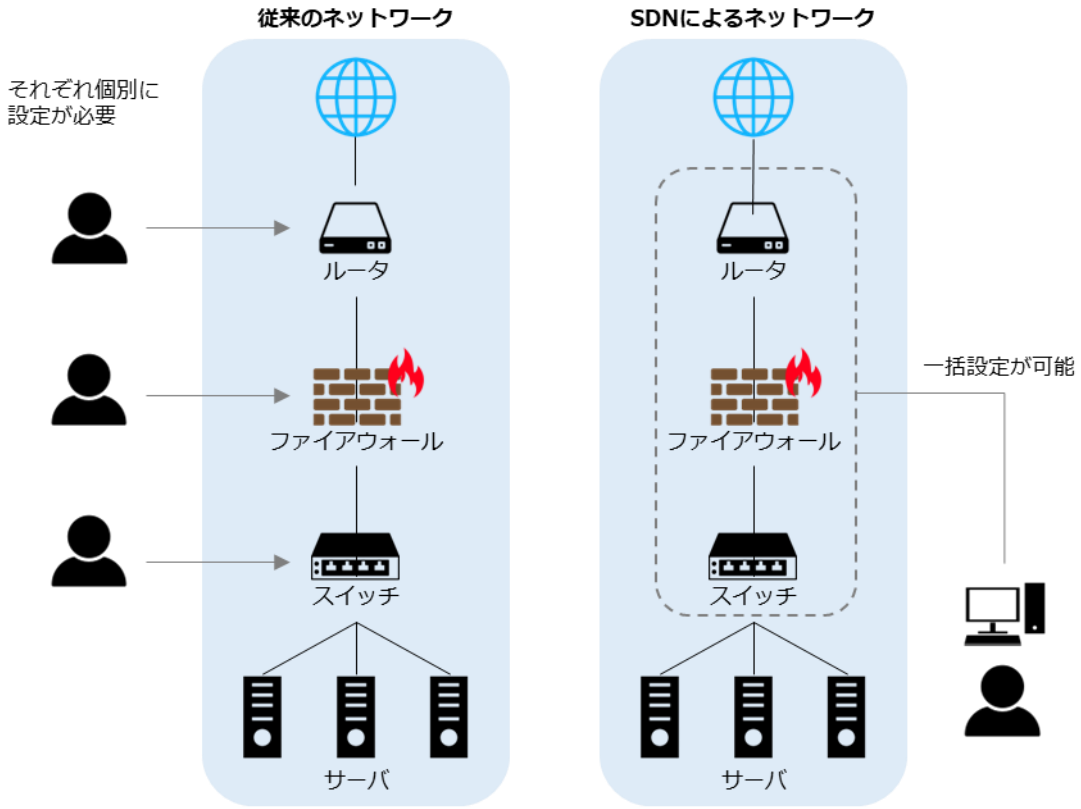


図 66. 従来のネットワークと SDN によるネットワークの比較

**SD-WAN（Software Defined-Wide Area Network）**

SD-WAN とは、ネットワークをソフトウェアで制御する SDN を、物理的なネットワーク機器で構築した WAN に適用する技術のことです。企業の拠点間接続や、クラウド接続などにおいて柔軟なネットワーク構成を実現したり、ネットワーク上で発生する通信を適切に制御したりすることができます。

例えば、拠点間の通信には閉域網（不特定多数のユーザーが利用するインターネットとは異なり、関係者のみが接続できる通信回線）を使用し、信頼できるクラウドサービスには直接外部インターネットへ接続するように切り替えることで、トラフィックの最適化が行えます。

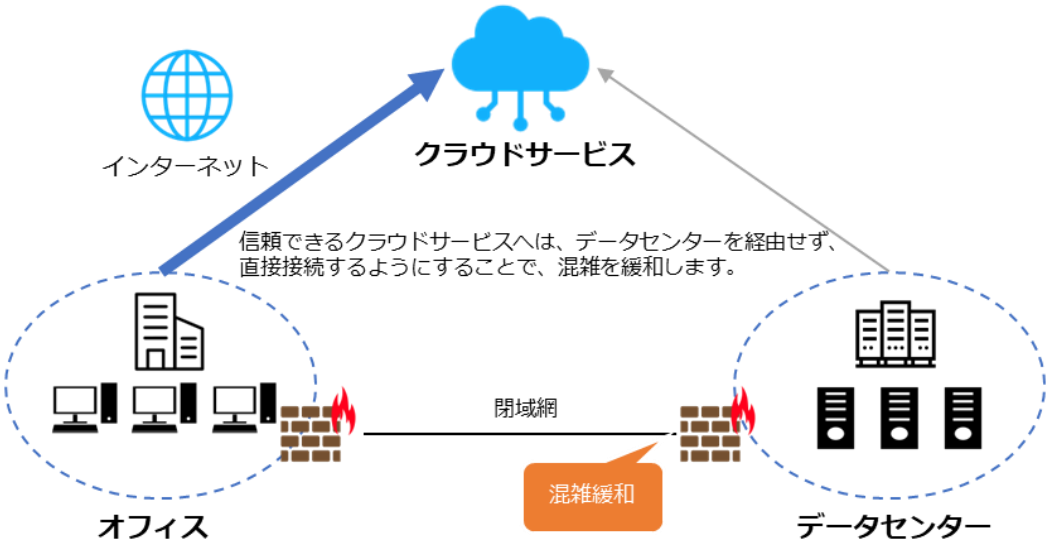


図 67. SD-WAN で実現できることの例

## VPN

個人情報などの重要なデータをインターネット経由で扱う機会が増えたことや、サイバー攻撃の手口が年々巧妙化しているなどの状況を背景に、VPN が注目されています。

### VPN（Virtual Private Network）

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です。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で、盗聴やデータの改ざんを防ぎます。VPN を使用することで、ユーザーは物理的な専用線で通信しているかのような安全な通信を行えます。


図 68. VPN の概要図

## 18-3-5. セキュリティ統制（Security as a Service）

| **関連する主な管理策** |
| --- |
| 5.1、5.9、5.15～5.18、5.23～5.28、8.1～8.5 |

セキュリティ統制とは、組織が情報資産を守るために採用するセキュリティ対策や仕組みになります。機密性、完全性、可用性などの情報セキュリティの目標を達成するために監視、記録を行い

統制します。

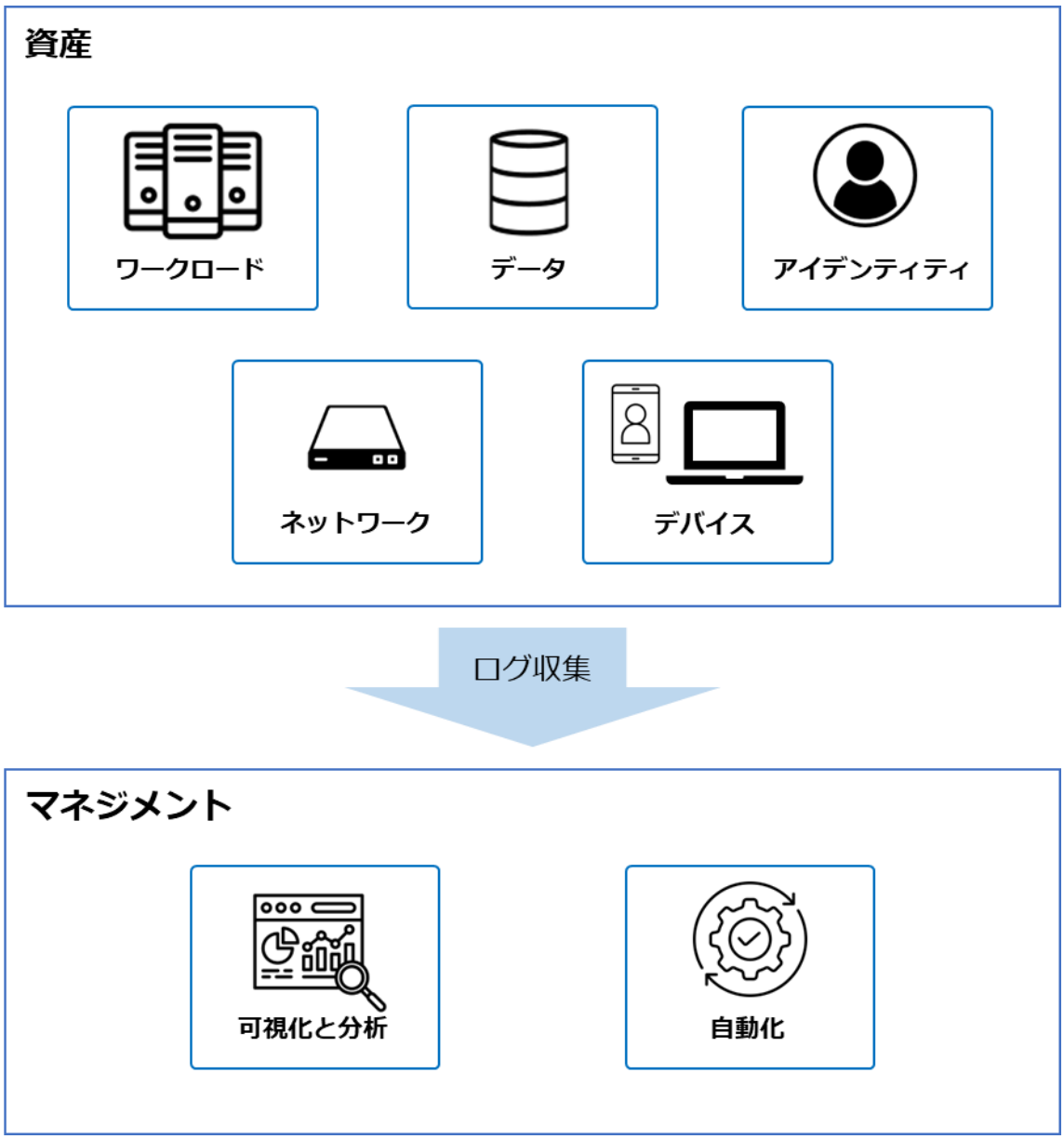


図 69. セキュリティ統制の概要図

以下は、セキュリティ統制を確立するための実施例となります。

| 実施内容（例） | 選択すべき管理策（例） |
| --- | --- |
| **リスク評価と分析**<br>● 組織内の情報資産やプロセスを評価し、セキュリティリスクを特定<br>● リスクの重要度や影響を評価し、優先順位づけ | 5.9 情報及びその他の関連資産の目録 |
| **ポリシーの策定**<br>● セキュリティポリシーを作成し、組織内での適用範囲や | 5.1 情報セキュリティのための方針群 |

| | |
|---|---|
| 要件を定義<br>● ポリシーは法規制や業界のガイドラインに準拠 | |
| **技術的対策の実施**<br>● 資産に対してセキュリティ対策の実施<br>➢ ワークロード<br>➢ データ<br>➢ アイデンティティ<br>➢ ネットワーク<br>➢ デバイスなど | 5.15 アクセス制御<br>5.16 識別情報の管理<br>5.17 認証情報<br>5.18 アクセス権<br>5.23 クラウドサービスの利用における情報セキュリティ |
| **監視と評価**<br>● セキュリティ対策の効果を監視し、定期的な評価の実施<br>● セキュリティインシデントが発生した場合は、原因を分析し、対策の改善 | 5.25 情報セキュリティ事象の評価及び決定<br>5.27 情報セキュリティインシデントからの学習<br>5.28 証拠の収集<br>8.15 ログ取得<br>8.16 監視活動 |
| **変更管理**<br>● システムやポリシーに変更があった場合、セキュリティに影響を与えないように変更管理プロセスを確立 | 8.32 変更管理 |
| **対応計画の策定**<br>● セキュリティインシデントが発生した場合の対応計画を策定し、迅速かつ効果的に対処 | 5.24 情報セキュリティインシデント管理の計画及び準備<br>5.26 情報セキュリティインシデントへの対応 |

## SECaaS（Security as a Service）

SECaaS はセキュリティをサービスとして提供します。組織がセキュリティに関する機能をクラウドベースのサービスプロバイダから提供される形態で利用します。従来では、オンプレミスで利用していたセキュリティ機能をクラウド上に移行し、サブスクリプションで利用することが可能になります。

**SECaaS のメリット**

- コスト最適化
- スケーラビリティ
- 変化への柔軟な対応

- 冗長性
- 高い可用性
- 障害耐性

セキュリティ統制を確立するために実施することができる技術を紹介します。

| | |
|---|---|
| **ネットワークセキュリティ** | |
| SWG<br>（Secure Web Gateway） | Web アクセスを中継するプロキシの一種で、危険なサイトやコンテンツへのアクセスを遮断するセキュリティ機能をクラウドサービスとして実施。 |
| SDP<br>（Software Defined Perimeter） | アクセス制御をソフトウェアで制御し、認証とアクセス制御を接続ごとに行うことで、動的なマイクロセグメンテーションおよびセキュアなリモートアクセスを実現。 |
| **デバイスセキュリティ** | |
| EDR<br>（Endpoint Detection and Response） | パソコンやサーバ、スマートフォンなどのエンドポイントデバイスに侵入したマルウェアやランサムウェアなどを検出し、通知するシステム。マルウェア感染後の被害拡大防止に有効。 |
| EPP<br>（Endpoint Protection Platform） | パソコンやサーバ、スマートフォンなどのエンドポイントデバイスへのマルウェアの侵入を防御するソリューション。未知のマルウェアの検知・駆除にも対応。 |
| **アイデンティティセキュリティ** | |
| IAM<br>（Identity and Access Management） | 情報システムのユーザーID を管理・認証・認可。 |
| FIDO<br>（Fast Identity Online） | ID/パスワード方式に代わる認証技術。指紋や虹彩といった生体情報、公開鍵暗号、端末 ID、ワンタイムパスワードなどを利用した認証方法がある。 |
| **ワークロードセキュリティ** | |
| CWPP<br>（Cloud Workload Protection Platform） | クラウド上コンテナ（実行環境）や仮想マシンなどに導入し、クラウドワークロード（クラウド上で実行されるプログラムやアプリケーション）の監視と保護を行うソリューション。 |

| データセキュリティ | |
|---|---|
| DLP<br>（Data Loss Prevention） | 情報漏えい防止を目的とするセキュリティツール。従来のシステムと異なり、データそのものを監視して情報漏えいを防ぐため、高い効果が期待できる。 |
| **可視化と分析** | |
| CASB<br>（Cloud Access Security Broker） | クラウドサービスの脆弱性対策ソリューション。クラウドサービスの利用状況を可視化すると同時にクラウド環境への不正アクセス検知と防御も可能。 |
| SIEM<br>（Security Information and Event Management） | ファイアウォールや IDS/IPS などから出力されるログやデータを一元的に集約し、集約したデータを組み合わせて相関分析を行うことにより、サイバー攻撃やマルウェア感染などのセキュリティインシデントをリアルタイムで検知。 |
| CSPM<br>（Cloud Security Posture Management） | クラウド環境の設定状況を可視化し、あらかじめ設定したルールに基づいて、不適切な設定や脆弱性の有無を検知。 |
| **自動化** | |
| SOAR<br>（Security Orchestration Automation and Response） | セキュリティインシデントの監視、データの収集・分析、対応などのセキュリティ運用業務を自動化・効率化する技術。 |

## FIDO（Fast Identity Online）

FIDO は、従来のパスワードによる認証方式に代わる、パスワードを使わない「パスワードレス認証」を実現する技術です。認証には、公開鍵暗号方式を利用したデジタル署名の仕組みが用いられます。

### デジタル署名による送信者確認の仕組み

デジタル署名では公開鍵と秘密鍵、2 つの鍵を使用します。公開鍵は公開される誰でも取得できる鍵で、秘密鍵は本人だけが保持している鍵です。秘密鍵で署名したデータは、対となる公開鍵で検証できます。この仕組みを利用し、受信者は送られてきたデータが間違いなく送信者本人から送


図 70. デジタル署名による送信者確認の仕組み

られてきたか確認できます。

**FIDO2**

FIDO2 とは、パスワードレス認証の技術仕様です。FIDO2 では、端末で生体認証行い、利用者を認証します。サーバとは、デジタル署名による本人確認の仕組みを用いて認証します。サーバ側には公開鍵、端末側には秘密鍵が保管され、鍵同士がペアとなります。正式サイトを偽装したフィッシングサイトがログインを求めても、ペアとなる鍵がないためログインを防げます。FIDO2 を利用したパスキーという仕組みでは、認証資格情報を複数の端末で同期できるため、機種変更や端末紛失などの場合に、一からの作成する必要はありません。

**メリット**

- 認証に必要な秘密情報（秘密鍵）は、認証を行う端末側のみに保存され、利用する際は指紋認証や顔認証などによって本人確認を行うため、パスワードを覚える必要がありません。
- パスワードや認証に必要な機密情報がインターネットに流れず、サーバ側で保存されないため、漏えいのリスクが低減されます。

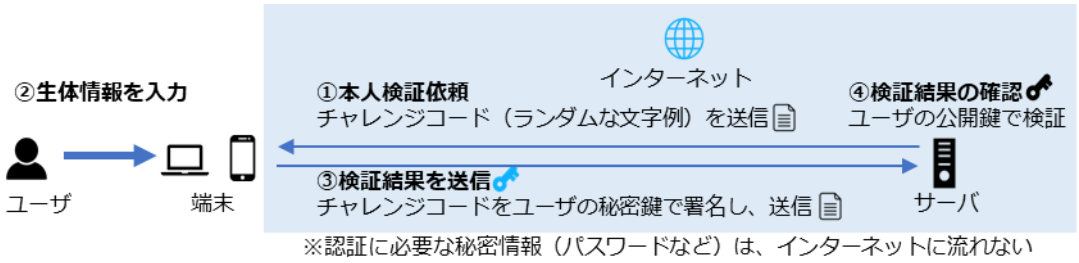


図 71. FIDO2 の仕組み

**① 本人検証依頼**

サーバは、ユーザーの端末に向けてチャレンジコード（ランダムな文字列）を送信します。

**② 生体情報を入力**

ユーザーは生体情報を入力し、端末はユーザーを認証します。

**③ 検証結果を送信**

ユーザーの認証に成功したら、端末はチャレンジコードをユーザーの秘密鍵で署名し、サーバへ送信します。

**④検証結果の確認**

サーバは、署名されたチャレンジコードを受け取ったら、ユーザーの公開鍵で検証します。検証に成功するとユーザーのログインを受入れ、認証完了となります。

## 18-4. インシデント対応

| 関連する主な管理策 |
| --- |
| 5.5、5.6、5.24~5.28、6.8 |

### インシデント発生時の対応

セキュリティインシデントが発生した際の基本的な対応の流れは、「第５章．事例を知る：重大なインシデント発生から課題解決まで」で説明した「1．検知・初動対応」、「2．報告・公表」、「3．復旧・再発防止」です。インシデント対応の実施手順について、ウイルス感染が起きた際の例を用いて説明します。

| 実施手順（例） | |
| --- | --- |
| ①検知・初動対応 | 検知と連絡受付：<br>● パソコンの動作異常やウイルス対策ソフトの警告が表示された場合、ウイルス感染の可能性があるため、情報セキュリティ責任者に報告する。<br>● ウイルスが添付されたメールを受け取った外部から通知を受けて発覚した場合も、情報セキュリティ責任者に報告する。<br>● 内部から外部への不正な通信、外部からの意図しない通信や、一時的な大量の通信、ウイルスに関係する特定サイトへのアクセスなどは、ウイルス感染を疑う。<br>初動対応：<br>● 感染したパソコンやサーバの利用を停止し、ネットワークから切り離す。 |
| ②報告・公表 | 第二報以降・最終報：<br>● 影響を及ぼした取引先や顧客に対して、セキュリティインシデントに関する報告を行う。<br>● ウイルス感染による影響によって、業法などで報告が求められる場合は所管の省庁へ報告する。<br>● ウイルス感染やランサムウェア感染の場合は、IPA の届出窓口へ届け出る。 |
| ③復旧・再発防止 | 調査・対応：<br>● 他のパソコンやサーバがウイルスに感染していないか、ウイルス対策ソフトの定義ファイルを最新にしてからチェックする。<br>● ウイルス対策ソフトに従ってウイルスを駆除する。<br>● ウイルス駆除ができない場合、OS のクリーンインストールを実施し、すべてのプログラムを入れ直す。<br>復旧： |

| | |
|---|---|
| | ● ウイルスの駆除が確認できたら、対象のパソコンやサーバをネットワークに接続し、復旧する。 |

インシデント対応の実施手順について、ウイルス感染が起きた際の例
（出典）IPA「中小企業のためのセキュリティインシデント対応の手引き」をもとに作成

| 詳細理解のため参考となる文献（参考文献） | |
|---|---|
| 中小企業のためのセキュリティインシデント対応の手引き | https://www.meti.go.jp/policy/netsecurity/sme_incident.html |

## フォレンジック

インシデント対応の「復旧・再発防止」のステップでは、訴訟対応などを見越して事実関係を裏づける情報や証拠を保全し、必要に応じてフォレンジックを行います。

**フォレンジックとは**

フォレンジックとは、セキュリティインシデントが起きた際に、コンピュータ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調査・解析する技術・手法・手続きを指します。

### フォレンジックを行う際の注意点

フォレンジックを行う必要がある際は、専門の調査会社に依頼する選択肢も考慮することが大切です。なぜなら、フォレンジックには専門知識が必要であり、自社で対応しようとすると、証拠となるデータの収集・保全が困難になる可能性があるためです。例えば、データのコピーが客観的証拠として認められない可能性や、誤操作によるデータの破損などがあります。事前に相談する専門の調査会社を決めておくことが大切です。

### セキュリティインシデント発生直後の対応についての実施手順策定

フォレンジックに関して、「証拠保全ガイドライン」が参考になります。想定読者として、「フォレンジックに関する専門知識を習得しているとは限らないが、専門事業者または捜査機関に引き継ぐために証拠保全手続きを行う可能性のある担当者」が含まれています。

セキュリティインシデント発生直後の初動対応についての実施手順を、例を用いて説明します。セキュリティインシデントが検知された、または発生していたことが明らかになった直後は、証拠保全を適切かつ円滑に実施するため、次の事項を実施することが大切です。

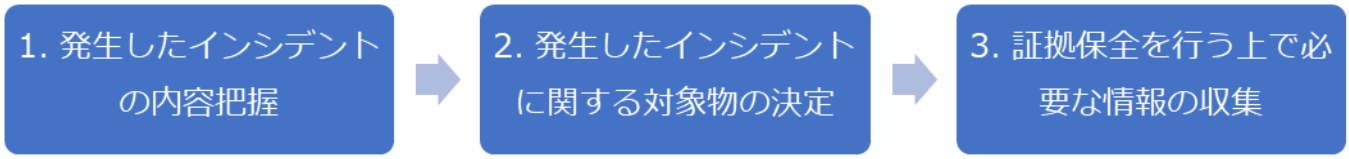


図 72. インシデント発生直後の対応の流れ

| 詳細理解のため参考となる文献（参考文献） | |
|---|---|
| 証拠保全ガイドライン第 10 版 | https://digitalforensic.jp/home/act/products/df-guideline-10th/ |

## 実施手順（例）

### 1. 発生したインシデントの内容把握

発生したインシデントを把握します。

**インシデントの種類**

- 情報流出・データ破壊
- 不正アクセス、不正プログラムの実行
- 操作・設定ミスなど

**検知・発覚のきっかけ**

- ログのレビュー・監視
- 内部通報
- 不正検知システムなど

**発生時刻**

- システム時計の正確性について確認

**初動対処の開始までの記録**

発生したインシデントの検知・発覚から、報告または対処依頼連絡までの時間およびその間のインシデントに対する対処の有無について記録をとります。

- 発生したインシデントを知る人物および人数
- インシデント対象物の確保の有無

インシデントの対象物を確保していた場合

対象物を確保した日時、人物（役職）、場所、確保時の対象物（および周辺）に対する行為、確保後の対象物に対する対処（の有無）とその内容を記録します。

インシデントの対象物を確保していない場合
対象物を確保する（予定の）日時と場所、確保時の対象物（およびその周辺）の状態を詳細に記録します。

**2. 発生したインシデントに関する対象物の決定**

**対象物に対する情報収集および対象物の絞り込み**

- 発生したインシデントに関する対象物の種類および個数を確認します。
  - コンピュータ（タブレット型、ノート型、デスクトップ型、サーバ型）
  - ネットワーク機器（ルータ、ファイアウォール、IDS、IPS）
  - HDD、SSD など
- 発生したインシデントに関する対象物の状態（いつどこに存在していたかなど）を確認します。
- 発生したインシデントに関する対象物の使い始めと終わり、および使用頻度を確認します。
- 発生したインシデントに関する対象物の使用者、および管理者を確認します。
- 発生したインシデントに関する対象物を円滑に証拠保全するための周辺機器、および文書の有無を確認します。

**対象物の選定と優先順位づけ**

- 保全を行う前の対象物（デバイス）を選定し、その理由を明確にします。
- （対象物が複数ある場合）取扱う対象物の優先順位をつけ、その理由を明確にします。

**3. 証拠保全を行う上で必要な情報の収集**

**対象物の情報**

- 対象物の形状、個数、物理的な状態を確認します。
  - 対象物のラベル情報（メーカー、型番、モデル名、記憶容量など）
  - ケーブルの接続状況
  - 通常環境下で視認可能な物理的破損、損傷の有無など
- HDD、SSD、ストレージメディアの記憶容量、インタフェースの状況を確認します。
- セキュリティ設定の有無を確認します。
  - HDD、SSD のパスワードロック
  - HDD、SSD 全体暗号化または一部のファイル・フォルダの暗号化
  - PC 周辺のワイヤストッパー、ロッカーなど

# 第19章. セキュリティ対策状況の有効性評価

| 章の目的 |
| --- |
| 第 19 章では、セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組として、監査について理解することを目的とします。 |

| 主な達成目標 |
| --- |
| ◘　内部監査および外部監査の重要性について理解すること |

## 19-1. 内部監査

内部監査とは、セキュリティのルールや扱っている文書などが、自社で規定した要求事項を満たしており、決められたルールに沿って業務が実施されているかをチェックすることです。セキュリティのルールを整備して日が浅いうちは、関係者がルールを理解し、遵守しながら仕事ができているかを重視して判断します。運用に慣れてきたら、設けられた社内のルールや使っている文書の内容が適切か、その有効性を判断していきます。内部監査の視点を適合性から有効性へと移していくことで、**ルールが形骸化し、目的が見失われている状態になることを防げる**でしょう。

内部監査の進め方は、「13-2-7. ISMS：9. パフォーマンス評価」を参照してください。

## 19-2. 外部監査

外部監査とは、組織に所属しない外部の監査人が行う監査を指します。セキュリティの外部監査では、企業が保有する情報資産を守るための体制や環境が整っているかを第三者がチェックすることになります。情報漏えいやサイバー攻撃などのリスクに対して、外部監査を受けることはセキュリティ対策として有効な手段の 1 つです。近年では取引先企業を乗っ取り、そこを踏み台にしてメインターゲットとなる企業にサイバー攻撃を仕掛ける「サプライチェーン攻撃」が頻繁に起こっており、中小企業が大企業に対する攻撃の踏み台として狙われる可能性が高まっています。

情報セキュリティ監査を受ければ、**自社のセキュリティ対策が正しく行われているか否か確認でき、不十分な点を洗い出して迅速に対処することが可能になります。**顧客や取引先に、セキュリティ対策を適切に行っていることがアピールできるので、会社や事業の規模も考慮しつつ、監査を受けることは重要です。経済産業省は、情報セキュリティの管理・監査について、2 つの基準を発表しています。

### 管理基準・監査基準

| 情報セキュリティ管理基準 |
| --- |
| 組織における情報セキュリティマネジメントの円滑で効果的な確立を目指し、マネジメントサイクルの構築から具体的な管理策まで、包括的な適用範囲を定めたものです。この管理基準は「マネジメント基準」と「管理策基準」の 2 項目から構成されています。<br><br>**マネジメント基準**<br>情報セキュリティマネジメントの計画・実行・点検・処置に必要な実施すべき事項が提示されています。<br><br>**管理策基準**<br>リスク対応方針に従って管理策を選択する際の選択肢が提示されています。 |
| **情報セキュリティ監査基準** |
| 情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範です。監査の品質を一定の水準に保ち、有効かつ効率的に実施できるように「一般基準」「実施基準」「報告基準」の 3 項目を提示しています。<br><br>**一般基準**<br>監査人としての適格性および監査業務上の遵守事項を定めています。<br><br>**実施基準**<br>監査計画の立案および監査手続きの適用方法を中心に、監査実施上の枠組みを定めています。 |

**報告基準**

監査報告にかかる留意事項と、監査報告書の記載方式を定めています。

情報セキュリティ管理基準は、JIS Q 27001 をもとに策定されています。そのため、Lv.3 網羅的アプローチを実施することで、外部監査に対応することも可能となります。

| 詳細理解のため参考となる文献（参考文献） | |
|---|---|
| 経済産業省「情報セキュリティ監査制度」 | https://www.meti.go.jp/policy/netsecurity/is-kansa/ |
| 情報セキュリティ監査基準 Ver1.0（平成 15 年経済産業省告示第 114 号） | https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf |
| 情報セキュリティ管理基準（平成 28 年経済産業省告示第 37 号） | https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf |

# コラム

## 実施手順の文書化に関するポイント

実施手順を文書化する際のポイントをいくつか紹介します。

- 明確な手順と責任の割り当て
  実施手順を文書化する際、手順が、誰が、いつ、どのように実施するのかを明確にすることが重要です。実施手順が適切に実施されるようにするためには、文書の各手順に関連する責任者を明記することが有効です。
- フローチャートや図の活用
  文字に加えて、フローチャートや図などを用いて手順を視覚的に示すことにより、手順の流れや関係性を理解しやすくできます。また、複雑なプロセスをわかりやすく表現できるため、実施者が迷わずに手順を進められるようになります。
- 定期的なレビューと更新
  実施手順は、絶えず変化する環境に適応させる必要があります。新たな脅威や法規制などへ対応させていくために、定期的なレビューや更新を行い、実施手順が常に効果的なものである状態を維持していくことが大切です。

実施手順の文書化は、組織がセキュリティ対策を行っていく上で必要です。実施手順を組織全体に浸透させ、形骸化させず有効な状態を維持するためには、責任者を明記したり、視覚的な表現を組み合わせてわかりやすい手順を記載したり、定期的にレビューしたりすることが大切です。

# 編集後記

第 7 編では、 ISMS の管理策を参考に、対策基準・実施手順を策定する手順について解説しました。紹介した 対策基準・実施手順の例は、そのまま組織に適用できるものではないため、紹介した例と ISO/IEC 27002 の内容を参考に、自社にあった対策基準・実施手順を策定していただければと思います。文書化・更新は重要ですが、本来の目標は文書化ではなく、効果的なセキュリティ対策の計画と実行にあることを忘れないようにしてください。

第 8 編では、 具体的な構築・運用の実践について説明します。

# 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<br>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<br>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**<br>ドキュメントの位置づけ：Normative<br>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。<br><br>**DS-110 デジタル・ガバメント推進標準ガイドライン解説書**<br>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-203 政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理及びその対策のグッドプラクティス集**
ドキュメントの位置づけ：Informative
概要：政府情報システムにおけるサプライチェーン・リスクに起因する大規模な攻撃や事故等に備えて、サプライチェーン全体を考慮したリスクを管理・対策するための課題整理及びグッドプラクティスを示したものです。

**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） | |
|---|---|
| デジタル社会推進標準ガイドライン | https://www.digital.go.jp/resources/standard_guidelines |
| 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/d4e68a9b/20250619_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/573c839f/20250619_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/ae9a37b7/20250619_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/2c39df54/20250619_resources_standard_guidelines_glossary_01.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-203 政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理及びその対策のグッドプラクティス集 | https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a547f9a6/20250630_resources_standard_guidelines_technical_report_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/a612d406/20250619_resources_standard_guidelines_guideline_08.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。<br>プロジェクトの立ち上げ、初動<br>プロジェクト計画書などの作成<br>プロジェクトのモニタリング<br>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。
予算のための稟議の事前準備
予算のための稟議に必要な資料の準備
見積り依頼
見積りの精査
予算を要求する
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

サービス・業務企画の開始準備
利用者視点でのニーズ把握
業務の現状把握
サービス・業務企画内容の検討
軌道修正
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。
要件定義の事前準備
RFI の実施
要件定義の全体像
機能要件の定義
非機能要件の定義
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。
調達の事前準備
調達仕様書の作成
調達仕様書以外のドキュメント作成
調達手続きとプロジェクト管理
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。
設計・開発を開始するための事前準備
設計・開発の計画
設計・開発・テストの管理
見落としがちな活動に注意
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。
新しいサービス・業務の事前準備
業務の定着と次の備え
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。

運用・保守を開始するための事前準備

運用・保守の計画

運用・保守の定着と次への備え

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。

システム監査の理解

システム監査計画と監査実施計画

システム監査の実施

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/d4e68a9b/20250619_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/573c839f/20250619_resources_standard_guidelines_guideline_03.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。

目標とする成果を見定める
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
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。

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。

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。

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。

機能する体制を作る
制度所管部門、業務実施部門などを含めた PJMO 体制とする
プロジェクトの規模に見合った体制を組む
他組織と連携できる体制を作る
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。

プロジェクト計画書を作成する
プロジェクト計画書は段階的に詳細化する
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。

プロジェクト管理要領を作成する
問題に対処できる会議体を構成する
本質的なリスクを事前に予見して、対応を準備する
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。

プロジェクトをモニタリングし、検証する
目標、経費、進捗、品質などを中心にモニタリングする
モニタリングは適時に実施する
モニタリングと監査をうまく組み合わせる
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。

プロジェクトの終結を処理する
プロジェクトを完了する
プロジェクトを終了する
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<br>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<br>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<br>目標：注文書の簡易化<br>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<br>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<br>80%（XX 年度）<br>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。<br>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<br><br>→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。<br><br>予算のための稟議を計画的に実施する<br>予算のための稟議の年間スケジュールを把握する<br>予算のための稟議に向けた作業のポイント<br>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。<br><br>予算のための稟議の対象範囲を早期に決める<br>プロジェクト計画書を再確認する<br>予算のための稟議から漏れがちな項目を理解する<br>関係者と役割分担は早期に確認<br>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。 |

コスト削減の検討
ハードウェア・ソフトウェアのコスト削減観点
アプリケーションのコスト削減観点
運用業務のコスト削減観点
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。

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

事業者への見積り依頼
見積りしてくれる事業者を探す
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。

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

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

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。

全体像と要点の明確化

予算のための稟議の資料の作成上の注意点
「予算のための稟議の概要」の作成ポイント
「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。

PMO による調整
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。

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。

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。

予算の移替え・予算執行管理
予算の移替え
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<br>管理指標と現在の達成状況について、定量的に記述する<br>顕在化している課題を記述する<br>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。

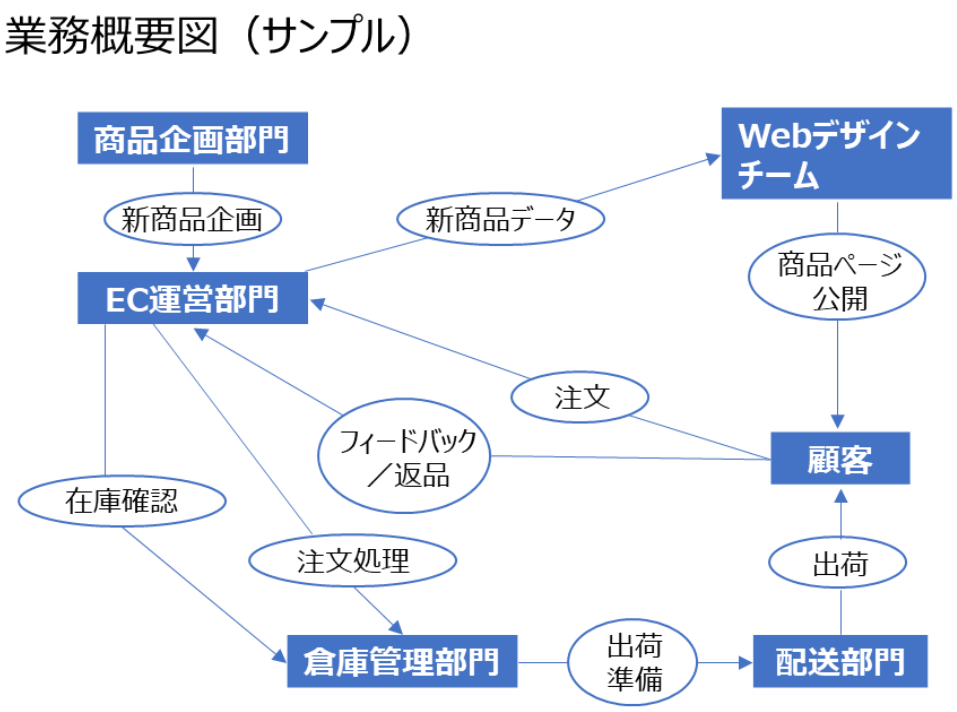


図 73. 業務概要図の例

**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　予算および執行　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。

**人事異動時の引継ぎ不足を防ぐこと**

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。

サービスデザイン思考を理解する
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。

利用者のことを知る
どんな利用者がいるかを調べる
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。

利用者のニーズを理解する
利用者のニーズから出発する
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。

業務を観察する
事実を詳細に把握する
推測ではなく、現場で発生している事実をみる
1 カ所だけの現場分析結果を全体に拡張しない
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。

実績データを分析する
平均、合計ではなく、ばらつきを見る
時間と期間を区別して滞留状況をつかむ
業務量のピークを捉え、ピークの発生原因を把握する
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。

業務を可視化する
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
業務ルールや業務実施方法をまとめる
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。

課題を整理し、分析する
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。

企画案を作成する
すべての関係者に気を配る
利用者の日常体験に溶け込む
縦割り組織にやわらかく横串を刺す
必要に応じて制度自体を見直す
システムを作る前に、業務を標準化する
将来の業務フローには、効果を紐づける
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
オープンにサービスを作る
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。<br><br>軌道修正しやすい進め方にする<br>一遍にやらず、一貫してやる<br>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。<br><br>柔軟に軌道修正する<br>何度も繰り返す<br>無理に継続しない<br>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。<br>業務要件をまとめる<br>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。

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。

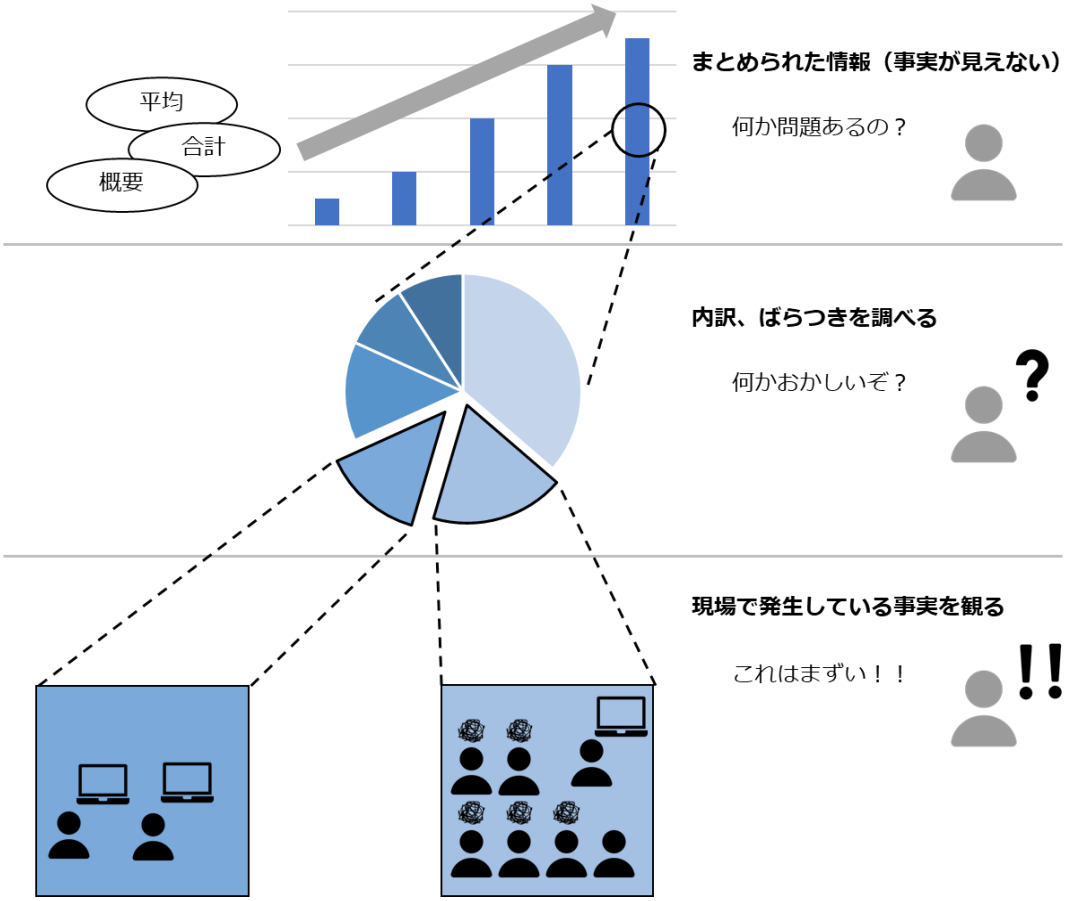


図 74. 事実を詳細に把握するイメージ図

（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。

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。

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。

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

公平性を確保したヒアリングを行う

収集した情報をもとに資料を更新する
RFI や発注前ヒアリングの結果を整理する
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。

構成要素を把握し要件を定義する
機能の優先順位は改善後の業務で判断する
一貫性を持った論理的な記載とする
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。

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

必要な機能を漏れなく抽出し検討する

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。

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

| |
|---|
| 規模に関する事項<br>性能に関する事項<br>信頼性に関する事項<br>拡張性に関する事項<br>上位互換性に関する事項<br>中立性に関する事項<br>継続性に関する事項<br>情報セキュリティに関する事項<br>情報システム稼動環境に関する事項<br>データマネジメントに関する事項<br>テストに関する事項<br>移行に関する事項<br>引継ぎに関する事項<br>教育に関する事項<br>運用に関する事項<br>保守に関する事項<br>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。<br><br>定義内容を関係者に共有する<br>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。

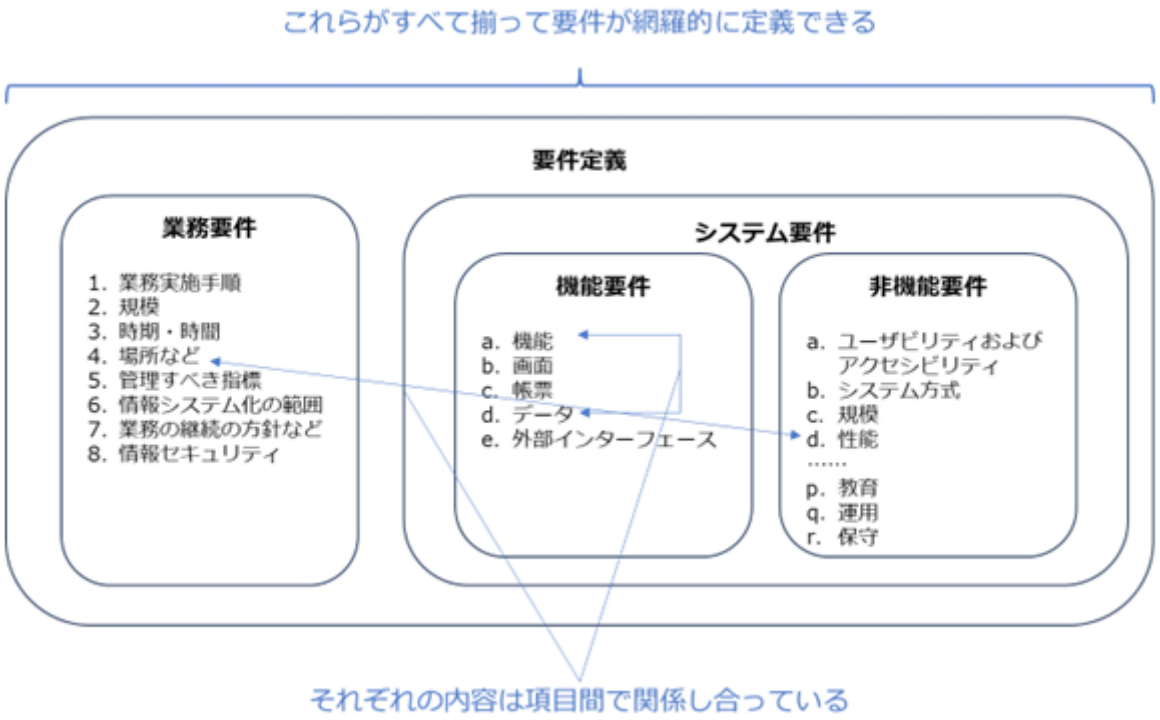


図 75. 要件定義の構成要素とポイント

（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ウェアや 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ウェアや 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ウェアや 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

パッケージソフトウェアや 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。パッケージソフトウェアや 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、パッケージソフトウェアや 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：

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。

パッケージソフトウェアや 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。

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。

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。

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ウェアや 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。 |

パッケージソフトウェアや 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。

調達の単位・計画を確認する
プロジェクト立ち上げ時点で調達を計画する
さまざまな調達単位があることを理解する
調達にあった落札方式、評価方式を検討する
調達計画を早めに公開する
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。

調達の注意事項を理解する
調達手続きの基本的なルールを確認し理解する
入札制限を正しく理解する
一者応札の状況を改善する

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。

関連ドキュメントとの関係性を理解する
調達仕様書と要件定義書の住み分けを理解する
付属文書を活用して可読性を上げ機密性を確保する
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

調達仕様書の記載内容を理解する
調達の意図や目的を正しく伝える
関連する調達、入札制限を伝える
作業内容・納品物を関連付けて網羅的に記載する
外部事業者の具体的な作業内容を明確にする
作業の実施体制を明確にする
成果物の取扱いに注意する（知的財産権）
再委託に関する事項を定める
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。

プロジェクトに合わせた契約書を作る
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。

提案依頼書の内容を工夫する
具体的な作業計画を評価する
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。

調達手続きに伴うプロジェクト管理作業とは
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。

情報システムの調達に特有の注意点
ベンダーロックインを理解し、回避する
入札参加要件を緩和する
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。

検収の位置づけと内容を理解する
検収と受入テストの違いを理解する
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。

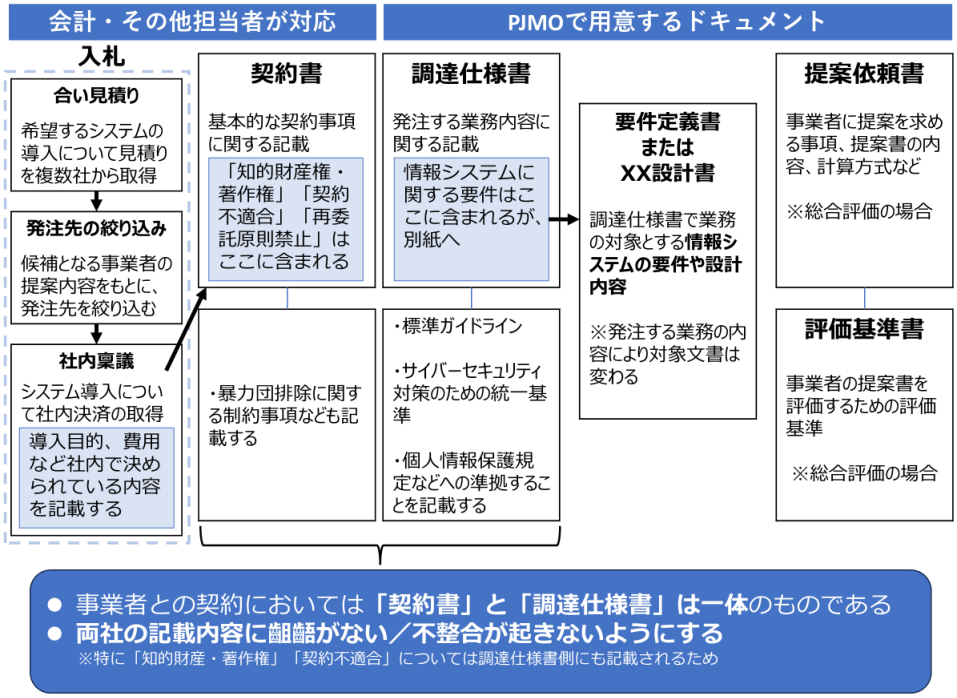


図 76. 調達に必要なドキュメントの関係図

**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。

設計・開発で従業員が行うべきことを理解する
『要件の内容を伝える役割』
『要件どおりに情報システムができたかを確認する役割』
『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。

設計・開発全体を通して理解すべき点とは
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
要求とコストと納期のバランスをとる
設計・開発の全体像と流れを理解する
通常シナリオだけでなく緊急時の対応計画も準備する
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。

設計・開発の管理の要点を理解する
定点観測こそ進捗・品質管理の要
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。

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。

2 種類のプロジェクト計画書の相違点を理解する
意思決定の手順を明確にする

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

テストの計画を立てる
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
テストのレベルや種類を理解する
リスクを踏まえてテストの方針を決める
テストにおける役割分担と必要な環境を明確にする
テストツールを有効活用する
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。

設計内容を確認・調整する
基本設計の内容を確実にレビューする
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。

品質管理の考え方を理解する
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。

単体テスト・結合テストの品質を評価する
単体テスト留意点
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。

総合テストの品質を評価する
総合テストの留意点
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。

受入テストを実施する
受入テストと他のテストとの違いを理解する
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。

どのプロジェクトでも必ず移行を計画する
移行の種類を理解する
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。

次の運用・保守は開発と並行して検討する

| |
|---|
| 指標値を運用作業で取得できるように検討する<br>運用・保守の計画を立てる<br>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。<br><br>種類を理解し揃えるマニュアルを厳選する<br>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。<br><br>本番移行と本番稼動の開始を承認する<br>移行判定と稼動判定の違いを理解する<br><br>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。

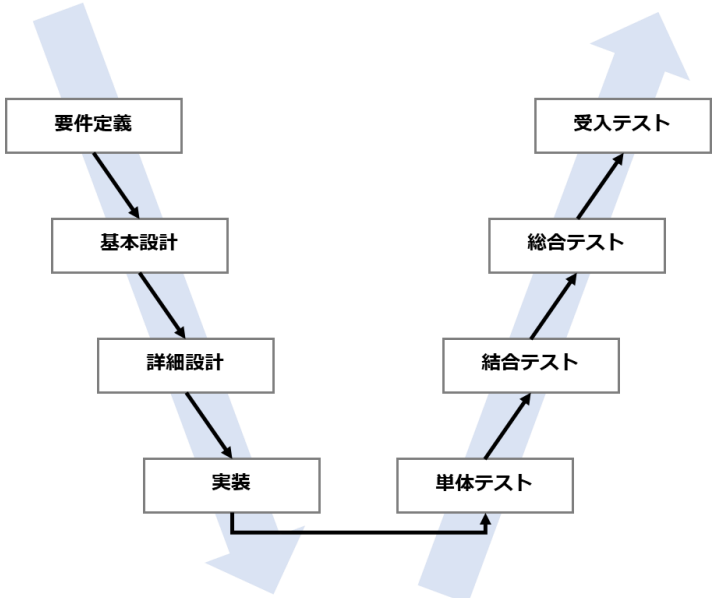


図 77. 標準ガイドラインの定義に則ったソフトウェア開発プロセスのＶ字モデル
（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

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。<br><br>（参考）カバレッジの種類<br>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<br>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<br>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<br><br>長所：<br>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。<br>短所：<br>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。<br>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。<br><br>長所：<br>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。<br>短所：<br>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。<br>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。 | 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 | タスクのツリー構造を定義 |

| | | |
|---|---|---|
| | 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。 | 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。<br>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。<br><br>運営と改善は、従業員主体の作業である<br>『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<br>『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<br>関連する業務実施部門との責任分担を意識する<br><br>業務手順書はさまざまな用途に有効活用できる<br>業務マニュアルと他のマニュアルとの違いを理解する<br><br>リハーサル計画・シナリオは従業員目線で<br>移行リハーサルを計画・実施する<br>業務リハーサルを計画・実施する<br>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。<br><br>従業員に継続的な教育を行う<br>研修・教育の準備を十分に行う<br>研修・教育は 1 回では定着しない<br><br>定着には利用者への働きかけが必要<br><br>業務で扱うデータの品質を確保する<br>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<br>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<br><br>業務改善に向け日常業務の事実を蓄積する<br>PJMO・従業員がさまざまな情報を収集し、定常的に管理する<br>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<br>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<br>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。<br>日常業務中でも改善できることを理解する<br>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。<br>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。<br>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。<br>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。<br>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。 |

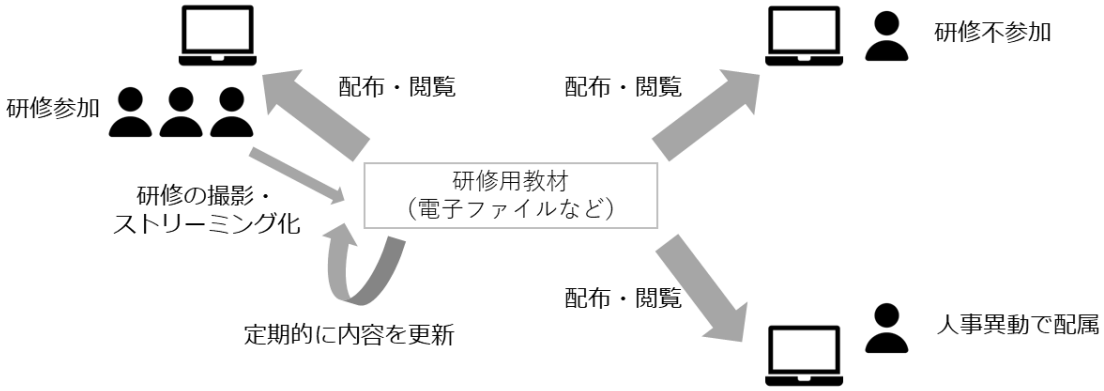


図 78. 研修・教育の定着化に向けた取組
（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

「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<br>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。<br>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。

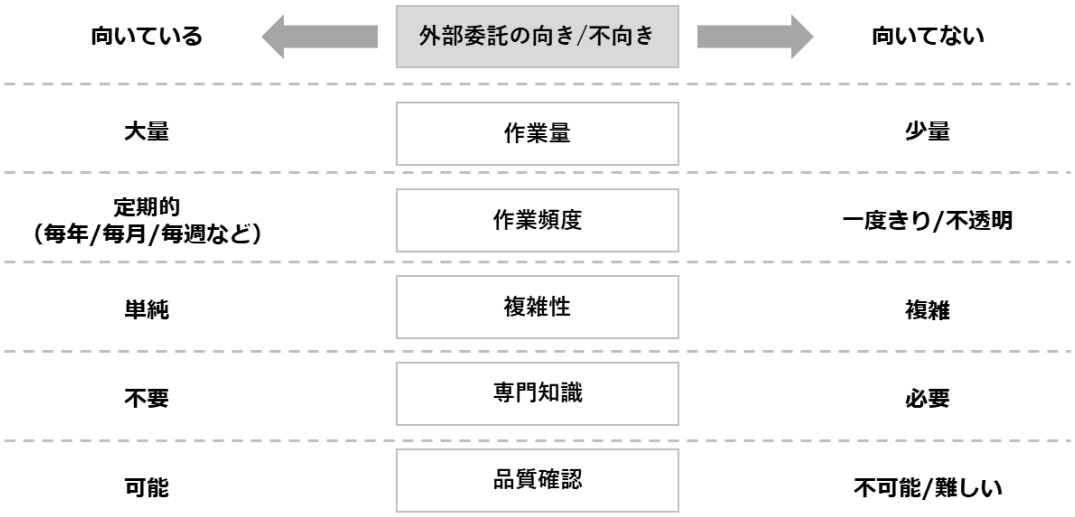


図 79. 外部委託の向き／不向きの判断例
（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

**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。

「運用と保守」の位置づけを理解する
サービス・業務をより改善するための活動を行う
情報システムの運用と保守の活動を理解する
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
運用・保守に、自動化の仕組みを取り入れる
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。

作業責任を正しく理解しトラブルを防ぐ
外部委託事業者へ依頼する作業の内容を明確にする
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
業務実施部門を含めた運用退背を確立する
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。

運用と保守の計画を作成する
システムプロファイルに応じた運用・保守レベルにする
セキュリティ関連作業を定期的に確実に実施する
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
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
会議体は目的を明確にして必要最低限に抑える
定例会の報告フォーマットを指定して、効率性を上げる
運用・保守の工数を把握し、人件費をモニタリングする
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。

運用定例会議を有効活用する
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。

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。

情報システムで起こった事実を蓄積する
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
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

| |
|---|
| 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<br>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。<br><br>適切な時期に的確に改善を実行する<br>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。

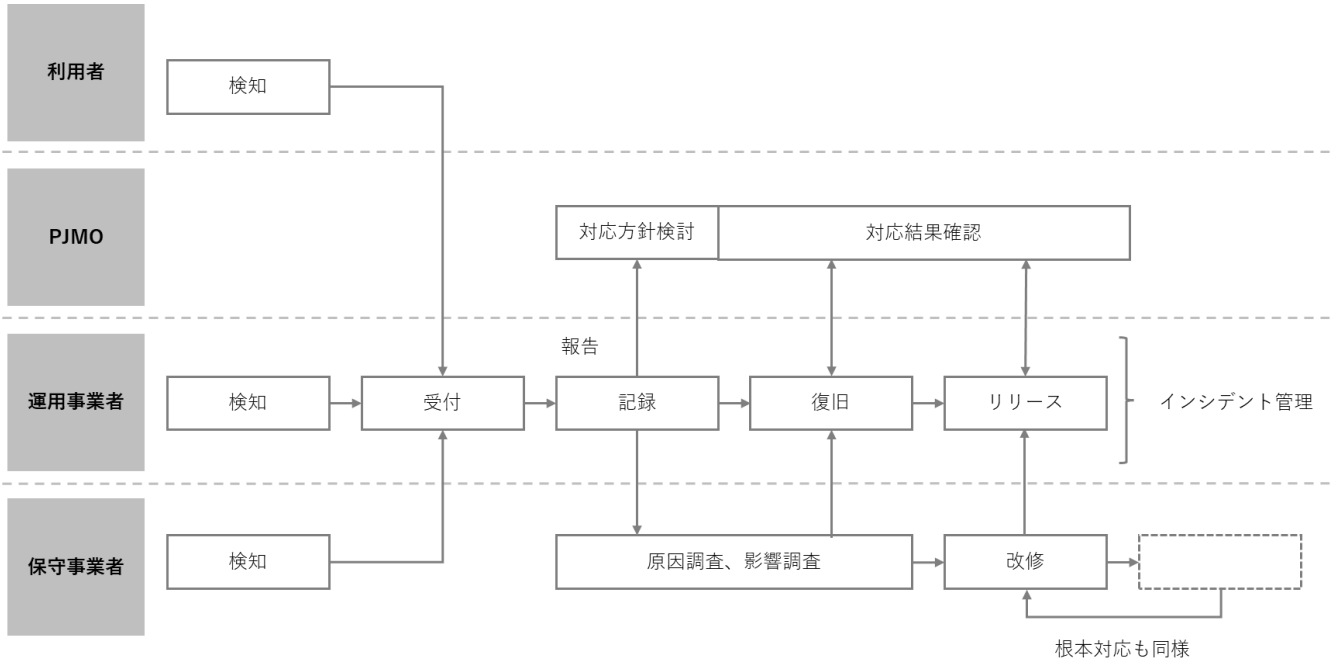


図 80. 障害発生時の運用と保守の役割分担の例
（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

「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。<br>以下に定期的に実施すべき作業の例を挙げます。<br>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<br>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） | |
|---|---|
| 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 |
| 【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。<br><br>システム監査とは何かを理解する<br>監査の種類を理解する<br>システム監査は問題解決の近道となる<br>システム監査基準・システム管理基準を理解する<br><br>システム監査の全体像を理解する<br><br>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。<br><br>複数年の監査計画を立てる<br><br>システム監査実施計画書を作る<br>監査範囲が局所的にならないように注意する<br>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。<br><br>予備調査を踏まえ監査手続きを具体化する |

| |
|---|
| 監査手続書を作成するまでの流れをつかむ<br><br>根本原因を究明し改善点を発見する<br>インタビュー時には情報を上手に引き出す<br>改善提案は報告の場で具体的な例を混ぜながら行う<br>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。<br><br>改善計画を立て改善を行う |

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 81. 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。

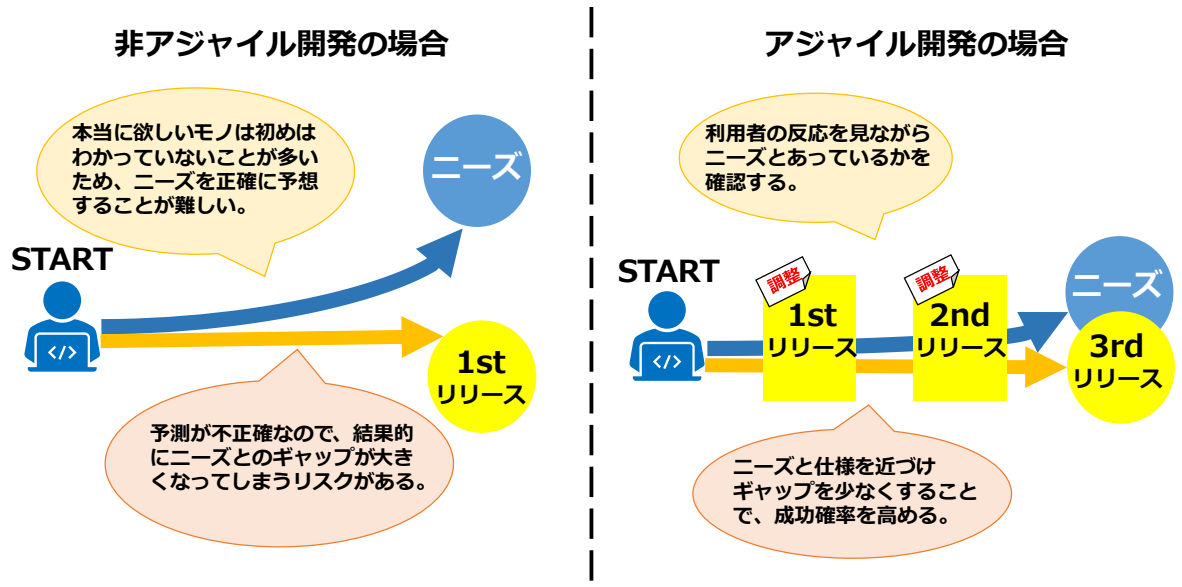


図 82. 非アジャイル開発とアジャイル開発の違い

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**

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
形にすることで、関係者の認識を早期に揃えられる
システム、プロセス、チームに関する問題に早く気づける
チームの学習効果が高い
早く開発を始められる
システムの機能同士の結合リスクを早期に解消できる
利用開始までの期間を短くできる
開発のリズムが整えられる
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**

常にカイゼンを指向すること
対話コミュニケーションの重視
情報システムの変更容易性を確保し続ける
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。

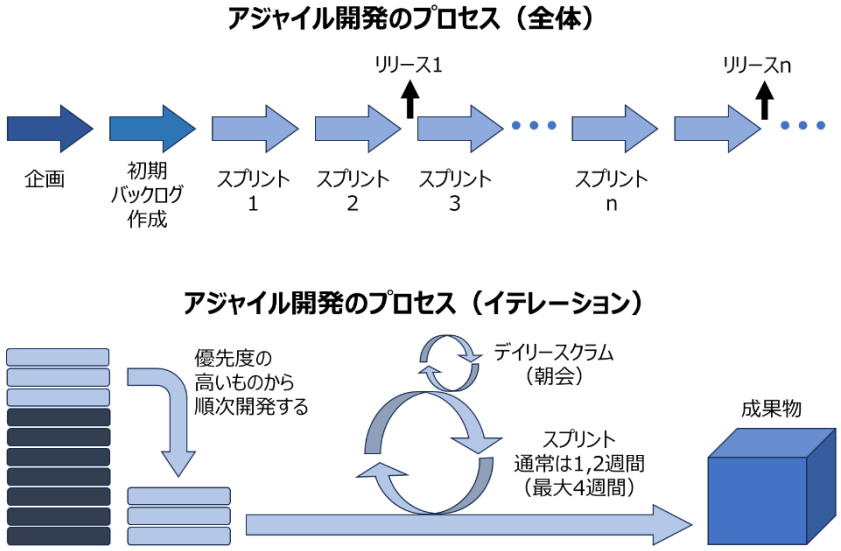


図 83. アジャイル開発のプロセス（スクラムの例）

| 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<br>（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） | |
|---|---|
| IPA ITSS+（プラス）アジャイル領域 | https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/agile.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 |

**引用文献**

IPA ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u000002klo-att/000092243.pdf

中小企業のためのセキュリティインシデント対応の手引き

https://www.meti.go.jp/policy/netsecurity/sme_incident.html

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/ae9a37b7/20250619_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**


ISO/IEC 27001:2022

https://www.iso.org/standard/27001

ISO/IEC 27002:2022

https://www.iso.org/standard/75652.html

セキュリティ・バイ・デザイン導入指南書

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/security-by-design.html

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

ゼロトラスト導入指南書～情報系・制御系システムへのゼロトラスト導入～

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf

（参考資料1）民間企業におけるゼロトラスト導入事例

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5805a275-3e16-4296-8a94-6557b58c6a4c/dd52a824/20231124_meeting_network_casestudie_03.pdf

中小企業のためのセキュリティインシデント対応の手引き

https://www.meti.go.jp/policy/netsecurity/sme_incident.html

証拠保全ガイドライン第10版

https://digitalforensic.jp/home/act/products/df-guideline-10th/

経済産業省「情報セキュリティ監査制度」

https://www.meti.go.jp/policy/netsecurity/is-kansa/

情報セキュリティ監査基準 Ver1.0（平成15年経済産業省告示第114号）

https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf

情報セキュリティ管理基準（平成28年経済産業省告示第37号）

https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf

デジタル社会推進標準ガイドライン

https://www.digital.go.jp/resources/standard_guidelines

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/d4e68a9b/20250619_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/573c839f/20250619_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/ae9a37b7/20250619_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/2c39df54/20250619_resources_standard_guidelines_glossary_01.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-203 政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理及びその対策のグッドプラクティス集 |
| https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a547f9a6/20250630_resources_standard_guidelines_technical_report_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/a612d406/20250619_resources_standard_guidelines_guideline_08.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 |
| 【改定新版】特権ID管理ガイドライン |
| https://www.jnsa.org/result/digitalidentity/2024/index.html |
| IPA ITSS+（プラス）アジャイル領域 |
| https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/agile.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。

20-1-3

■CVSS

Common Vulnerability Scoring System の略。情報システムの脆弱性に対するオープンで汎用的な評価手法のこと。ベンダーに依存しない共通の評価方法を提供している。CVSS を用いると、脆弱性の深刻度を同一の基準の下で定量的に比較できるようになる。ベンダー、セキュリティ専門家、管理者、ユーザなどの間で、脆弱性に関して共通の言葉で議論できるようになる。

18-3-1

■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。

18-3-5

■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。

18-3-2

■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。

18-2-10、18-2-14、18-2-18、18-3-5、18-4

■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。

18-2-10、18-2-14、18-3-2、18-3-5、18-4

■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、IPv

6（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。
18-3-2

■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。
18-1、19-1

■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
20-1-2、20-1-8、20-1-9

■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。
18-3-2

■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。
20-1-1

■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。
18-2-15

■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
20-1-1、20-1-2、20-1-3、20-1-6、20-1-7、20-1-8、20-1-9、20-1-10

■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）

20-1-3

■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。

20-1-1、20-1-5

■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。

18-3-3

■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。

18-3-2、18-3-5

■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。

18-2-18

■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。

18-2-21

■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。

18-3-2、18-3-3、18-3-5

■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。

18-3-2、18-3-4

■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。
18-3-4

■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。
18-1、18-3-2、18-3-5、20-1-1

■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。
18-1

■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。
18-2-1、18-2-10、18-2-18、18-2-21、18-3-4、18-4

■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。
18-2-15

■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。
18-3-2

■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）
18-1、18-3-2、18-3-5

■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。
18-2-11、18-2-13、18-2-17、18-3-4

■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。
18-1、18-2-12、18-2-17、18-3-5、20-1-9

■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
18-2-17、18-2-21、18-3-5、20-1-9

■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。
18-2-17、18-2-21、18-3-5、20-1-6、20-1-9

■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。
18-3-1

■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。
18-3-1、18-3-2

■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。

18-4

■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。
18-1、18-2-17、18-3-1、20-1-3

■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
20-1-7

■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。
18-3-2、18-3-4、18-3-5、19-2

■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。
18-2-9

■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。
20-1-1

■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。
18-3-2

■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。
18-3-2、18-3-5、19-2

■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。
18-2-17、18-3-5

■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。
18-2-21

■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
18-2-15、20-1-5、20-1-7

■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。

18-2-1

■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。
18-1、18-2-7、18-2-17、18-2-21、18-3-1、18-3-5、20-1-1、20-1-3、20-1-5

■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
18-3-1、20-1-1

■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
18-1、18-2-13、18-3-1、18-3-5、18-4、20-1-8、20-1-9

■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。
18-3-5、20-1-5、20-1-6

■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
第 18 章、18-3-2、18-3-3、20-1-1

■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。
18-1

■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」
18-2-18、18-3-2、18-3-5、20-1-5

■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。
18-2-4、18-3-2

■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。
18-1、18-2-10

■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。
20-1-1

■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。
20-1-7

■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。
18-3-2、18-3-4

■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。
19-1、20-1-10

■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。
18-2-10、18-2-14、18-2-18、18-2-19、18-3-2、18-3-5、18-4、20-1-5

■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。
18-2-10、18-2-17

■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。
18-4

■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。
18-2-4、18-2-10、18-2-11、18-2-13、18-2-17、18-3-5、18-4、20-1-5

■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。
19-2

■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。
20-1-1

■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。
18-3-5

■ペネトレーションテスト
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。
18-3-1

■ペルソナ分析
ネットワークに接続されたシステムの安全性を検証するテスト手法。すでに知られているサイバー攻撃手法を使って実際にシステムに侵入や攻撃を試みることで攻撃耐性を確認する。
20-1-1

■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。
20-1-6

■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。
18-1、18-2-6、18-2-20、18-3-2、18-3-5

■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
18-3-1、18-3-4、20-1-3

■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
18-2-18、18-2-21

■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。
18-1、18-2-16

■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。
18-2-11、18-3-5、18-4

■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。
18-1、18-2-17

■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。
18-3-5、20-1-9


東京都産業労働局