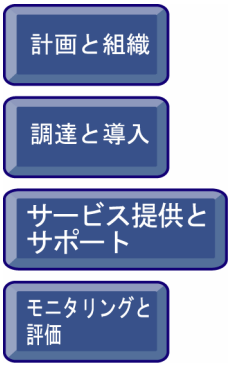
# サービス提供とサポート

**DS1** サービスレベルの定義と管理
**DS2** サードパーティのサービスの管理
**DS3** 性能とキャパシティの管理
**DS4** 継続的なサービスの保証
**DS5** システムセキュリティの保証
**DS6** 費用の捕捉と配賦
**DS7** 利用者の教育と研修
**DS8** サービスデスクとインシデントの管理
**DS9** 構成管理
**DS10** 問題管理
**DS11** データ管理
**DS12** 物理的環境の管理
**DS13** オペレーション管理

# コントロール目標 －概要－

## DS1 サービスレベルの定義と管理

IT 管理部門とビジネス部門の顧客間で、求められるサービスについて効果的なコミュニケーションを行うためには、IT サービスおよびサービスレベルの定義と合意内容を文書化する必要がある。本プロセスには、サービスレベルの達成状況についてモニタリングし、利害関係者にタイムリーな報告をすることも含まれる。このプロセスにより、IT サービスと関連するビジネス要件との間の整合を図ることができる。


**IT プロセス: サービスレベルの定義と管理のコントロール目標は、**

主要な IT サービスとビジネス戦略との整合性が保証されることを、**ビジネス要件**とし、

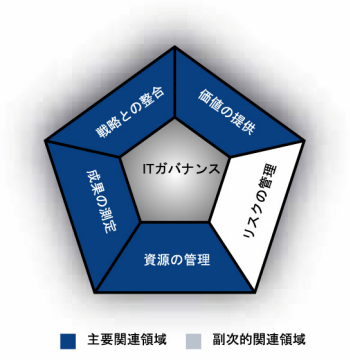
**重点をおくべきコントロールは、**サービス要件を特定し、サービスレベルについて合意し、サービスレベルの達成状況をモニタリングすることである。

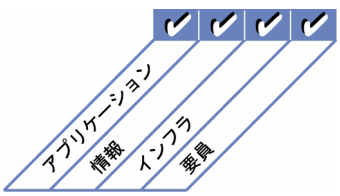
**実現するための手段は、次の 3 項目である。**

- 要件と提供能力を踏まえた上での社内外に対する正式な合意形成
- サービスレベル達成状況の報告(レポーティングとミーティング)
- 戦略策定に応じた新規または変更サービス要件の特定とコミュニケーション

**その成果の測定指標は、次の 3 項目である。**

- サービス提供が合意レベルへ到達していることに満足しているビジネス部門の利害関係者の割合
- カタログにない提供サービスの数
- ビジネス部門との正式な SLA レビュー会議の年間の開催回数



# コントロール目標 －詳細－

## DS1 サービスレベルの定義と管理

### DS1.1 サービスレベル管理フレームワーク
顧客とサービスプロバイダ間で正式に合意されたサービスレベル管理プロセスを定めたフレームワークを定義する。このフレームワークを通じて、サービスレベルとビジネス要件およびビジネス上の優先事項との間の整合性を継続的に維持すると同時に、顧客とサービスプロバイダ双方における認識の共有を促進する。このフレームワークには、サービスに対する要件、サービス定義、サービス・レベル・アグリーメント(SLA)、オペレーショナル・レベル・アグリーメント(OLA)を策定し、および資金の調達元を明確にするためのプロセスを含める。これらのサービス属性は、サービスカタログ(service catalog)にまとめる。またこのフレームワークでは、サービスレベルの管理のための組織構造を定義する。その定義には、組織内外のサービスプロバイダと顧客の役割、タスク、および実行責任を含める。

### DS1.2 サービスの定義
主にサービスカタログ/ポートフォリオ方式の導入を通じて収集され、蓄積されたサービス特性とビジネス要件に基づいて、IT サービスの基本的な定義を行う。

### DS1.3 サービス・レベル・アグリーメント
顧客側の要件と IT の提供能力に基づいて、すべての重要な IT サービスについてサービス・レベル・アグリーメントを策定し、合意を得る。ここでは、顧客の確約事項、サービスサポート要件、利害関係者により承認されたサービスの量的/質的測定指標、資金の調達、および商業上の調整(該当する場合)、そしてサービス・レベル・アグリーメント(SLA)自体の監督業務を含む役割および実行責任が定められる。検討すべき事項は、可用性、信頼性、成果、容量計画、サポートレベル、継続計画、セキュリティ、および需要面での制約である。

### DS1.4 オペレーショナル・レベル・アグリーメント
サービス・レベル・アグリーメント(SLA)を最適な形で満足するサービスの技術的提供方法を、オペレーショナル・レベル・アグリーメントにおいて明記する。オペレーショナル・レベル・アグリーメント(OLA)は、技術プロセスをサービスプロバイダに理解し易い形で規定し、必要に応じて、複数のサービス・レベル・アグリーメント(SLA)に対応する可能性がある。

### DS1.5 サービスレベル達成状況のモニタリングと報告
規定されたサービスレベルの成果基準を継続的にモニタリングする。サービスレベルの達成状況に関する報告は、利害関係者が容易に理解できる形式で提出する。モニタリング結果の統計データを分析、処理し、サービス全般のほか、個々のサービスにおけるマイナス/プラス要因を特定する。

### DS1.6 サービス・レベル・アグリーメントおよび請負契約の見直し
組織内外のサービスプロバイダと協力してサービス・レベル・アグリーメントとその請負契約を定期的に見直し、契約内容が有効かつ周辺動向に則した内容であり、要件の変化が反映されること確実にする。

# マネジメントガイドライン

## DS1 サービスレベルの定義と管理

| From | インプット |
|---|---|
| PO1 | IT 戦略/実行計画、IT サービスポートフォリオ |
| PO2 | 採用したデータの分類方法 |
| PO5 | 最新の IT サービスポートフォリオ |
| AI2 | 当初計画されたサービス・レベル・アグリーメント(SLA) |
| AI3 | 当初計画されたオペレーショナル・レベル・アグリーメント(OLA) |
| DS4 | 災害時のサービス要件(役割および実行責任を含む) |
| ME1 | IT 計画にインプットされる成果 |

| アウトプット | To | | | | | | |
|---|---|---|---|---|---|---|---|
| 契約見直し結果の報告 | DS2 | | | | | | |
| プロセスの成果報告 | ME1 | | | | | | |
| 新規または更新されたサービス要件 | PO1 | | | | | | |
| サービス・レベル・アグリーメント(SLA) | AI1 | DS2 | DS3 | DS4 | DS6 | DS8 | DS13 |
| オペレーショナル・レベル・アグリーメント(OLA) | DS4 | DS5 | DS6 | DS7 | DS8 | DS11 | DS13 |
| 最新の IT サービスポートフォリオ | PO1 | | | | | | |

**RACI チャート**

**担当**

| アクティビティ | CEO | CFO | 企業幹部 | CIO | ビジネス プロセス オーナー | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO（プロジェクト・マネジメント・オフィス） | コンプライアンス、監査、リスク、セキュリティ | サービス管理担当者 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IT サービス定義のためのフレームワークの策定 | | | C | A | C | C | I | C | C | I | C | R |
| IT サービスカタログの作成 | | | I | A | C | C | I | C | C | I | I | R |
| 重要な IT サービスについてのサービス・レベル・アグリーメント(SLA)の定義 | | I | I | C | C | R | I | R | R | C | C | A/R |
| サービス・レベル・アグリーメント履行のためのオペレーショナル・レベル・アグリーメント(OLA)の定義 | | | | I | C | R | I | R | R | C | C | A/R |
| 包括的なサービスレベル成果のモニタリングおよび報告 | | | | I | I | R | | I | I | | I | A/R |
| サービス・レベル・アグリーメント(SLA)とその請負契約の見直し | | I | | I | C | R | | R | R | | C | A/R |
| IT サービスカタログの見直しと更新 | | | I | A | C | C | I | C | C | I | I | R |
| サービス改善計画の策定 | | | I | A | I | R | I | R | C | C | I | R |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

**達成目標とその評価指標**

**アクティビティの達成目標**
- サービスの定義
- 要件と提供能力を踏まえた上での社内外に対する正式な合意形成
- サービスレベル達成状況の報告(レポーティングとミーティング)
- 報告を受ける側に応じた報告の編成
- 戦略策定に対する新規または変更のサービス要件のフィードバック

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- ビジネス部門との正式な SLA レビュー会議の年間の開催回数
- 報告されたサービスレベルの割合
- 自動化された方法で報告されたサービスレベルの割合
- 顧客との合意後にサービスレベルの調整に要した作業日数

*促進*

**プロセスの達成目標**
- 求められるサービスレベルについての共通認識の確立
- サービス・レベル・アグリーメントおよび成果達成基準の正式化とモニタリング
- 提供サービスのレベルと、合意したサービスレベルとの合致
- ビジネス達成目標との整合が取れた最新のサービスカタログの作成

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- カタログにない提供サービスの数
- 合意したサービスレベルに到達しているサービスの割合
- 測定されているサービスレベルの割合

*促進*

**IT の達成目標**
- 提供サービスとサービスレベルに対するエンドユーザの満足の確保
- ビジネス戦略と合致するビジネス要件への対応
- IT 運用にかかる費用、便益、戦略、ポリシー、およびサービスレベルの透明性の確保と理解の実現

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- サービス提供が合意レベルへ到達していることに満足しているビジネス部門の利害関係者の割合
- サービス提供が合意レベルへ到達していることに満足しているユーザの割合

# 成熟度モデル

## DS1 サービスレベルの定義と管理

**「主要なITサービスとビジネス戦略との整合性が保証される。」というITに対するビジネス要件を満たす上で、「サービスレベルの定義と管理」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
マネジメント層がサービスレベルの定義プロセスの必要性を認識していない。それらをモニタリングする説明責任と実行責任が割り当てられていない。

**1 初期/その場対応**
サービスレベル管理の必要性は認識されているが、そのプロセスは非公式かつ事後的である。サービスの定義および管理の実行責任と説明責任について規定されていない。成果測定が行われているとしても、その測定はあいまいに定義された目標で定性的な測定に限られている。報告は非公式であり、報告頻度が低く継続性がない。

**2 再現性はあるが直感的**
合意されたサービスレベルが存在するが、これらのサービスレベルは非公式であり、見直しは行われていない。サービスレベルの報告が不完全であり、顧客にとって的外れまたは誤解を招く可能性がある。サービスレベルの報告は、個々の管理者のスキルおよびイニシアチブに依存する形で行われている。サービスレベル調整担当者が割り当てられ、実行責任が規定されているが、十分な権限は与えられていない。サービス・レベル・アグリーメント順守のためのプロセスが存在する場合でも、そのプロセスの実施は任意であり、強制されていない。

**3 定められたプロセスがある**
実行責任は明確に定義されているが、自由裁量に任されている。サービス・レベル・アグリーメントの策定プロセスが整備されており、サービスレベルと顧客満足度を再評価するためのチェックポイントが設けられている。標準プロセスを用いて、サービスとサービスレベルの定義、文書化、合意が実施されている。しかしサービスレベルの未達は識別されるが、それを解決する正式な手続がない。期待されるサービスレベルの達成と投下資金との間に明確な関連付けがある。合意されたサービスレベルはあるが、それがビジネスの必要性に対応していない可能性がある。

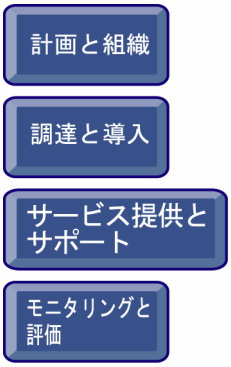
**4 管理され、測定可能である**
システム要件の定義段階において、サービスレベルが徐々に明確に定義され、アプリケーションおよび運用環境の設計の中に組み込まれている。顧客満足度が定期的に測定および評価されている。成果の測定指標に、IT の達成目標ではなく顧客のニーズが反映されている。サービスレベル評価の測定方法が標準化されつつあり、業界水準を反映している。サービスレベル定義の基準はビジネスの重点項目に基づいており、可用性、信頼性、成果、容量の余裕度、ユーザサポート、継続計画、およびセキュリティ上の検討事項が含まれる。サービスレベルに達していない場合には、その根本原因の分析が定期的に実施されている。サービスレベルモニタリングの報告プロセスが徐々に自動化されつつある。合意されたサービスレベルに達しない場合に発生し得る運用上および財務上のリスクが定義されており、明確に把握されている。KPI および KGI の正式な測定体系が構築、維持されている。

**5 最適化**
IT の目標とビジネス目標の整合性確保のため、サービスレベルの再評価が継続的に実施されている。同時に、費用対効果分析などの技術が活用されている。すべてのサービスレベルの管理プロセスにおいて、継続的な改善が課せられている。顧客満足度が継続的にモニタリング、管理されている。期待されるサービスレベルは各ビジネス部の戦略目標を反映していると同時に、業界水準に照らして評価されている。IT 管理部門には、サービスレベル目標の達成に必要な資源が割り当てられており、その説明責任が課されている。また、サービスレベル目標達成の動機付けとなる報酬体系が設定されている。マネジメント層は、継続的な改善プロセスの一環としてKPIおよびKGIのモニタリングを行っている。

# コントロール目標 －概要－

## DS2 サードパーティのサービスの管理

サードパーティが提供するサービスがビジネス要件を確実に満たすようにするには、効果的なサードパーティの管理プロセスが必要である。このプロセスでは、サードパーティとの合意のもと、役割、実行責任、および要求事項を明確に定義し、このような合意事項の有効性とコンプライアンスをレビューおよびモニタリングする。サードパーティが提供するサービスを効果的に管理することで、不適格なサービスプロバイダに起因するビジネスリスクを最小限に抑えることができる。


**IT プロセス: サードパーティのサービスの管理のコントロール目標は、**

便益、費用、およびリスクに関する透明性を維持し、サードパーティによる要件を満たすサービス提供を実現することを、**ビジネス要件**とし、

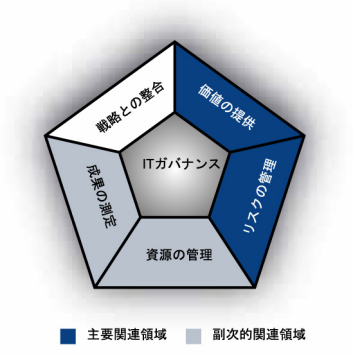
**重点をおくべきコントロールは、**適格なサービスプロバイダ(サードパーティ)とリレーションシップおよび相互責任を確立し、合意内容との適合性を検証し保証するためにサービス提供状況をモニタリングすることである。

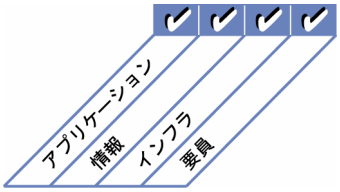
**実現するための手段は、次の 3 項目である。**

- サービスプロバイダからのサービスの特定と分類
- サービスプロバイダにかかわるリスクの特定と低減
- サービスプロバイダの成果のモニタリングと測定

**その成果の測定指標は、次の 3 項目である。**

- 契約されたサービスに関するユーザからの苦情件数
- 明確に定義された要件とサービスレベルを満たしている主要サービスプロバイダの割合
- モニタリング対象となっている主要サービスプロバイダの割合



# コントロール目標 －詳細－

## DS2 サードパーティのサービスの管理

**DS2.1 すべてのサービスプロバイダとのリレーションシップの特定**
すべてのサービスプロバイダのサービスを特定し、サービスプロバイダのタイプ、重要性、および依存度に従って分類する。技術的および組織的な関係を正式に文書化して管理する。この文書には、サービスプロバイダの役割および実行責任、目標、期待される成果物、および代表者の信用証明が含まれる。

**DS2.2 サービスプロバイダとのリレーションシップ管理**
サービスプロバイダごとにサービスプロバイダとのリレーションシップ管理プロセスを正式なものとする。リレーションシップオーナは連携して顧客およびサービスプロバイダにかかわる問題に取り組み、サービス・レベル・アグリーメントなどにより信頼と透明性に基づく良質なリレーションシップの維持に努めなければならない。

**DS2.3 サービスプロバイダにかかわるリスクの管理**
サービスプロバイダが安全かつ効率的な方法を使用し、継続的なサービスを提供する上で想定されるリスクを特定し、低減する。契約が、法令要件に従い一般的なビジネス標準に準拠していることを確認する。リスク管理ではさらに、秘密保持契約(NDA)、エスクロー契約(訳注:サードパーティ預託契約サービス提供者の破産等に備えて、ソースプログラム等をサードパーティに預託し、事由の発生時に、委託者に提供する契約)、サービスプロバイダの存続能力、セキュリティ要件へのコンプライアンス、代替サービスプロバイダ、SLA 未達と超過達成などについて検討すべきである。

**DS2.4 サービスプロバイダの成果のモニタリング**
サービス提供状況のモニタリングプロセスを確立する。これにより、サービスプロバイダが現行のビジネス要件を満たすと同時に、継続的に契約合意とサービス・レベル・アグリーメントを厳守し、その成果が、市場の状況および他のサービスプロバイダと比較した場合の優位性があることを確認する。

# マネジメントガイドライン

## DS2 サードパーティのサービスの管理

| From | インプット |
|---|---|
| PO1 | IT 調達戦略 |
| PO8 | 調達基準 |
| AI5 | 契約上の取り決め、サードパーティとのリレーションシップ管理における要件 |
| DS1 | サービス・レベル・アグリーメント(SLA)、契約レビュー結果の報告 |
| DS4 | 災害時のサービス要件(役割および実行責任を含む) |

| アウトプット | To |
|---|---|
| プロセスの成果報告 | ME1 |
| サービスプロバイダー一覧表 | AI5 |
| サービスプロバイダにかかわるリスク | PO9 |

### RACI チャート

| アクティビティ | 担当 CEO | CFO | 企業幹部 | CIO | ビジネスプロセスオーナ | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO(プロジェクト・マネジメント・オフィス) | コンプライアンス・監査・リスク・セキュリティ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| サードパーティとのサービス・リレーションシップの特定と分類 | | | | I | C | R | C | R | A/R | C | C |
| サービスプロバイダの管理プロセスの定義と文書化 | | C | | A | I | R | I | R | R | C | C |
| サービスプロバイダの評価および選定に関するポリシーと手続の確立 | | C | | A | C | C | | C | R | C | C |
| サービスプロバイダにかかわるリスクの特定、評価および低減 | | I | | A | | R | | R | R | C | C |
| サービスプロバイダからのサービス提供状況のモニタリング | | | | R | A | R | | R | R | C | C |
| すべての利害関係者に対するサービスのリレーションシップの長期的達成目標の評価 | C | C | C | A/R | C | C | C | C | R | C | C |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R:Responsible) ②説明責任者(A:Accountable) ③協議先(C:Consulted)④報告先(I:Informed)

### 達成目標とその評価指標

**アクティビティの達成目標**
- サービスプロバイダのサービスの特定と分類
- サービスプロバイダにかかわるリスクの特定と低減
- サービスプロバイダの成果のモニタリングと測定

*促進*

**プロセスの達成目標**
- 適格なサービスプロバイダ(サードパーティ)との相互責任を伴うリレーションシップの確立
- サービス提供のモニタリングと合意内容との適合性の確認
- サービスプロバイダが、関連する内外の標準に準拠していることの確認
- サービスプロバイダの関係継続要望の維持

*促進*

**IT の達成目標**
- サードパーティとのリレーションシップについての相互満足の達成
- 提供サービスとサービスレベルに対するエンドユーザの満足の確保
- IT 運用にかかる費用、便益、戦略、ポリシー、およびサービスレベルについての透明性の確保と理解の実現

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- 明確に定義された要件とサービスレベルが義務付けられた主要サービスプロバイダの割合
- モニタリング対象となっている主要サービスプロバイダの割合
- サービスプロバイダからのコミュニケーションの有効性に対するビジネス部門の満足度
- ビジネス部門からのコミュニケーションの有効性に対するサービスプロバイダの満足度
- サービスプロバイダの契約不履行によって一定期間内に発生した重大インシデントの件数

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- 明確に定義された要件とサービスレベルを満たす主要サービスプロバイダの割合
- サービスプロバイダとの正式な係争の件数
- サービスプロバイダからの請求書のうち係争の対象となったものの割合

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- 契約されたサービスに関するユーザからの苦情件数
- 購入費用のうち、競争調達の対象となっている費用の割合

# 成熟度モデル

## DS2 サードパーティのサービスの管理

**「便益、費用、およびリスクに関する透明性を維持し、サードパーティによる要件を満たすサービス提供を実現する。」という IT に対するビジネス要件を満たす上で、「サードパーティのサービスの管理」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
実行責任および説明責任が定義されていない。サードパーティとの契約締結に関する正式なポリシーおよび手続が規定されていない。マネジメント層は、サードパーティからのサービスについて、承認もレビューも実施していない。成果測定が実施されておらず、サードパーティによる報告もない。契約上、報告義務が定められていないため、マネジメント層は、提供されるサービスの質を認識していない。

**1 初期/その場対応**
マネジメント層は、契約の締結を含め、サードパーティ管理に関するポリシーと手続を文書化する必要性を認識している。サービスプロバイダとの契約に盛り込むべき標準的な契約条項は定められていない。提供サービスの成果測定は非公式かつ事後的に実施されている。実施方法は、各担当者およびサービスプロバイダの経験に依存しており、たとえば要求された場合などに限り実施されている。

**2 再現性はあるが直感的**
サービスプロバイダ(サードパーティ)についての関連リスク、およびサービス提供状況の監督プロセスは非公式なものである。標準的なベンダーとの契約条項(提供されるべきサービスについての記述など)が規定された出来合いの契約書が締結され、使用されている。提供サービスに関する報告は実施されているが、ビジネス目標の達成に役立っていない。

**3 定められたプロセスがある**
ベンダーの審査およびベンダーとの交渉に関する明確なプロセスを含む、サードパーティのサービスを管理するための手続が適切に文書化され、整備されている。提供サービスに関する合意が存在する場合、サードパーティとの関係は純粋に契約に基づくものである。契約には提供されるサービスの性質が詳述されている。これには、法的要件、運用上の要件、およびコントロール要件が含まれている。サードパーティのサービスの監督実行責任が割り当てられている。契約条項は、契約の標準テンプレートに基づいている。サードパーティのサービスに関連するビジネスリスクについて評価および報告されている。

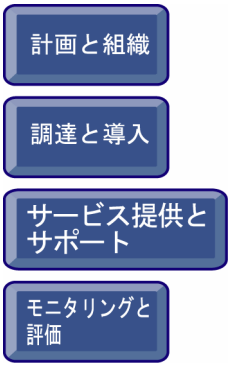
**4 管理され、測定可能である**
契約条項の定義に関する正式かつ標準化された基準が確立されている。この契約条項には、作業範囲、提供されるべきサービス/成果物、前提条件、スケジュール、費用、請求処理、および実行責任が含まれる。契約およびベンダーの管理の実行責任が割り当てられている。ベンダーの適格性、リスク、および能力が継続的に確認されている。サービス要件が定義され、ビジネス目標と関連付けられている。サービスの成果を契約条項に照らし合わせてレビューするプロセスが確立されている。これは、現行および将来のサードパーティのサービスの評価へのインプットとなる。調達プロセスにおいて、振替価格設定モデルが利用されている。関係者全員がサービス、費用、および各工程で期待される成果について認識している。サービスプロバイダの監督における KPI および KGI について合意が得られている。

**5 最適化**
サードパーティとの間で締結された契約が、事前に定義されている間隔で定期的にレビューされている。サービスプロバイダ管理と提供サービスの品質管理の実行責任が割り当てられている。運用、法律、コントロールに関する契約条項が遵守されているかどうかが、常にモニタリングされており、必要な場合に是正措置が講じられている。サードパーティに対する独立した定期レビューが実施されており、成果に関するフィードバックが提供され、サービス提供の改善に役立てられている。ビジネス状況の変化に対応する形で測定方法も変動する。成果測定により、サードパーティのサービスにおける潜在的問題を早期に発見できる。サービスレベル達成状況の包括的かつ明確な報告は、サードパーティに対する支払いに関連付けられている。マネジメント層は、KPI および KGI の結果に基づきサードパーティからのサービスの調達とモニタリングのプロセスを調整している。

# コントロール目標 －概要－

## DS3 性能とキャパシティの管理

IT 資源の性能とキャパシティを管理するには、IT 資源の性能とキャパシティを定期的にレビューするプロセスが必要である。このプロセスには、作業負荷、ストレージ、および緊急時の要件に基づいて今後のニーズを予測することが含まれる。このプロセスにより、ビジネス要件を支援する情報資源の継続的可用性が保証される。


**IT プロセス: 性能とキャパシティの管理のコントロール目標は、**

ビジネス上の必要性に応じて、IT のインフラストラクチャ、資源、および能力を最適化することを、**ビジネス要件**とし、

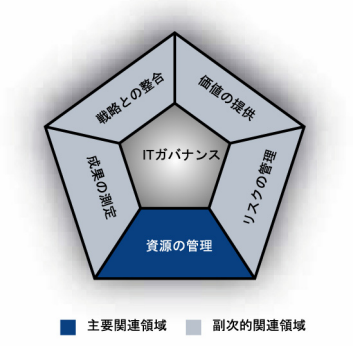
**重点をおくべきコントロールは、**モニタリングと測定により、サービス・レベル・アグリーメントにて合意した応答時間に関する要件を満たし、ダウンタイムを最小限に抑え、IT の性能とキャパシティの継続的改善を図ることである。

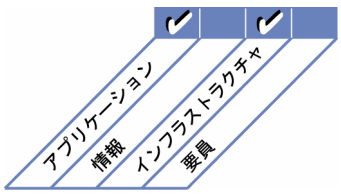
**実現するための手段は、次の 3 項目である。**

- システムキャパシティと可用性の計画策定と提供
- システム性能のモニタリングと報告
- システム性能のモデル化と予測

**その成果の測定指標は、次の 3 項目である。**

- 不十分なキャパシティ計画策定に起因する、1ユーザ、月あたりの損失時間数(1カ月あたり)
- 稼働率の上限を超過したピークの割合
- サービス・レベル・アグリーメント(SLA)に定められた要件を満たさなかった応答時間の割合



# コントロール目標 －詳細－

## DS3 性能とキャパシティの管理

### DS3.1 性能とキャパシティの計画策定
IT 資源の性能とキャパシティのレビュー計画の策定プロセスを確立する。これにより、サービス・レベル・アグリーメントで規定されている合意された作業負荷を処理するための費用的に妥当な性能とキャパシティを保証する。性能とキャパシティの計画では、適切なモデル化技法を用いて、現状、および予測される IT 資源の性能、キャパシティ、およびスループットのモデルを作成することが必要である。

### DS3.2 現状の性能とキャパシティ
現状の IT 資源の性能とキャパシティのレビューを実施する。これにより、サービス・レベル・アグリーメントに照らし合わせて十分な性能とキャパシティが提供されているかどうかを確認する。

### DS3.3 将来の性能とキャパシティ
IT 資源の性能とキャパシティの予測を定期的に実施する。これにより、キャパシティ不足または性能の低下に起因するサービス中断のリスクを最小限に抑える。また、IT 資源の再配置を可能にするような余剰能力がないか検証する。作業負荷の傾向を識別し、かつ予測値を決定し、性能とキャパシティの計画に取り込む。

### DS3.4 IT 資源の可用性
標準作業負荷、緊急事態、ストレージに関する要件、および IT 資源のライフサイクルなどの面を考慮して、必要となるキャパシティと性能を提供する。性能とキャパシティが必要とされるレベルに達していない場合の対策(作業の優先順位付け、フォールトトレランスメカニズム、資源の割り当て活動など)を定めるべきである。マネジメント層は、緊急時対応計画において確実に個々の IT 資源の可用性、キャパシティおよび性能について適切に対応可能であることを確認する必要がある。

### DS3.5 モニタリングと報告
IT 資源の性能とキャパシティを継続的にモニタリングする。収集データは次の 2 つの目的で使用される。
- IT の現行の性能を維持および調整し、障害からの回復、緊急時対応、現状および予定されている作業負荷、ストレージに関する計画と資源調達などの課題に対応する。
- サービス・レベル・アグリーメント(SLA)での規定に従い、ビジネス部門に対し提供サービスの可用性の報告を行う。すべての例外報告に対して、是正措置に関する推奨案を追記する。

# マネジメントガイドライン

## DS3 性能とキャパシティの管理

| From | インプット |
|---|---|
| AI2 | 可用性、継続性、および復旧の要件 |
| AI3 | システムモニタリング要件 |
| DS1 | サービス・レベル・アグリーメント(SLA) |

| アウトプット | To | | | | | | |
|---|---|---|---|---|---|---|---|
| 性能とキャパシティに関する情報 | PO2 | PO3 | | | | | |
| 性能とキャパシティに関する計画(要件) | PO5 | AI1 | AI3 | ME1 | | | |
| 必要な変更 | AI6 | | | | | | |
| プロセスの成果報告 | ME1 | | | | | | |

### RACI チャート

**担当**

| アクティビティ | CEO | CFO | 企業幹部 | CIO | ビジネスプロセスオーナ | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO（プロジェクト・マネジメント・オフィス） | コンプライアンス・監査・リスク・セキュリティ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| IT 資源の性能とキャパシティのレビューに関する計画策定プロセスの確立 | | | | A | | R | C | C | C | C | |
| IT 資源の現行の性能とキャパシティのレビュー | | | | C | I | A/R | | C | C | C | |
| IT 資源の性能とキャパシティの予測 | | | | C | C | A/R | C | C | C | C | |
| IT 資源に関する不適合を特定するギャップ分析の実施 | | | | C | I | A/R | | R | C | C | I |
| IT 資源が利用不能になる潜在的リスクに備えた緊急時対応計画の策定 | | | | C | I | A/R | | C | C | I | C |
| IT 資源の可用性、性能とキャパシティの継続的なモニタリングおよび報告 | | | | I | I | A/R | | I | I | I | I |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

### 達成目標とその評価指標

**アクティビティの達成目標**
- システムキャパシティと可用性の計画策定と提供
- システムキャパシティのモニタリングと報告
- システムキャパシティのモデル化と予測

*促進*

**プロセスの達成目標**
- ピーク時の負荷とトランザクションの応答時間のモニタリングと測定
- サービス・レベル・アグリーメント(SLA)における応答時間要件への適合
- 処理に失敗したトランザクションの最小化
- ダウンタイムの極小化
- IT 資源の利用の最適化

*促進*

**IT の達成目標**
- ビジネス戦略と合致するビジネス要件への対応
- 要求に応じて IT サービスを使用可能であることの保証
- IT インフラストラクチャ、資源、および能力の最適化

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- 性能とキャパシティの予測の実施頻度
- キャパシティレビューの対象である資産の割合
- 集中管理ツールを使用してモニタリングされる資産の割合

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- ピーク時の負荷と全体的な稼働率
- 稼働率の上限を超過したピークの割合
- サービス・レベル・アグリーメント(SLA)に定められた要件を満たさなかった応答時間の割合
- 処理に失敗したトランザクションの障害発生率

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- 不十分なキャパシティ計画策定に起因する、1 ユーザあたりの損失時間数(1 カ月あたり)
- 定められたサービス可用性計画が適用されていない重要なビジネスプロセスの数

# 成熟度モデル

## DS3 性能とキャパシティの管理

**「ビジネス上の必要性に応じて、IT のインフラストラクチャ、資源、および能力を最適化する。」という IT に対するビジネス要件を満たす上で、「性能とキャパシティの管理」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
マネジメント層が、主要なビジネスプロセスで高いレベルの成果を IT に求める場合があること、もしくは IT サービスに対する全体的なビジネス上のニーズがキャパシティを超える可能性があることを認識していない。キャパシティ計画策定プロセスが整備されていない。

**1 初期/その場対応**
性能とキャパシティに制約がある場合は、主にユーザがワークアラウンド(回避策)を検討しなければならない。キャパシティと性能の計画を策定する必要性について、ビジネスプロセスオーナがほとんど認識していない。性能とキャパシティの管理への対応は、概して事後的に行われている。キャパシティと性能の計画策定プロセスは非公式なものである。IT 資源の現行および将来のキャパシティと性能についての理解は限定的である。

**2 再現性はあるが直感的**
ビジネス部門と IT 部門の管理者は、性能とキャパシティを管理しない場合の影響について認識している。性能に関するニーズは概ね満たされているが、これは個別のシステム評価と、サポートチームおよびプロジェクトチームの知識に依存している。性能とキャパシティに関する問題の診断にさまざまなツールが用いられているものの、診断結果の首尾一貫性については、主要な担当者の力量に依存している。IT の性能とキャパシティに関する包括的な評価が行われておらず、また、ピーク時および最悪時の負荷状況について考慮されていない。可用性の問題が不意かつランダムに発生する可能性があり、問題の診断および是正に相当の時間がかかる。成果測定はすべて、顧客の必要性ではなく、主に IT 部門の必要性に基づいて行われている。

**3 定められたプロセスがある**
性能とキャパシティの要件は、システムのライフサイクル全体に対して定義されている。サービスレベル要件と指標が定義されており、この指標を用いて運用上の性能を測定できる。定義されたプロセスに従って将来の性能とキャパシティの要件がモデル化されている。性能に関する統計値を示す報告書が作成されている。性能とキャパシティに関連する問題が発生する可能性は依然として存在し、問題を是正するには時間がかかる。サービスレベルが公表されているが、ユーザと顧客がサービス提供能力について疑念を抱く余地がある。

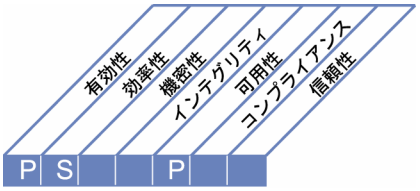
**4 管理され、測定可能である**
システムの使用状況、性能とキャパシティを測定するプロセスとツールが存在しており、測定結果は定義済みの達成目標と比較される。最新の情報が入手可能である。この情報には、標準化された性能に関する統計値と、性能とキャパシティの不足に起因するインシデントのアラート情報が含まれている。性能とキャパシティの不足に関する問題は、規定された標準手続に従って処理される。特定の資源(ディスクスペース、ネットワーク、サーバ、およびゲートウェイなど)のモニタリングに自動化ツールが用いられている。性能とキャパシティに関する統計値がビジネスプロセスの観点から報告され、その報告によりユーザと顧客が IT サービスレベルを理解できるようになっている。ユーザは現在のサービス提供能力に概ね満足しており、新たな、そしてさらに改善された可用性レベルを要求する可能性がある。IT の性能とキャパシティを測定するための KGI および KPI について合意が得られているが、これらの指標は、単に散発的かつ首尾一貫せずに適用されている可能性がある。

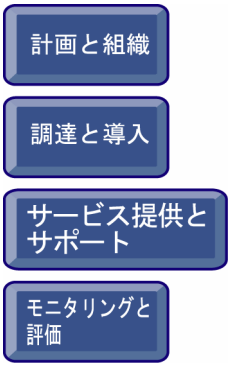
**5 最適化**
性能とキャパシティの計画は、ビジネス上の要件の予測と十分に同期されている。IT インフラストラクチャとビジネス上の要件の定期的なレビューが義務付けられており、これにより最小限の費用での最適なキャパシティの確実な実現が可能になっている。重要な IT 資源をモニタリングするためのツールが標準化されており、各プラットフォームで使用され、全社的なインシデント管理システムに関連付けられている。モニタリングツールは成果と能力に関連する問題を発見し、自動的に是正できる。傾向分析が実施され、業務量の増大に起因する差し迫った性能上の問題が発見される。この結果、対応計画の策定と、予期しない問題の回避が可能になる。IT の性能とキャパシティの測定指標が、すべての重要なビジネスプロセスについて KGI および KPI に最適に組み込まれており、首尾一貫して測定されている。マネジメント層は、KGI および KPI の分析を踏まえ、性能とキャパシティに関する計画の調整を行っている。

# コントロール目標 －概要－

## DS4 継続的なサービスの保証

継続的な IT サービスを提供するには、IT 継続計画の作成、保守、およびテスト、遠隔地のバックアップ保管施設の確保および定期的な継続計画に関するトレーニングの実施が必要である。効果的なサービス継続プロセスにより、主要な IT サービスの中断の可能性と、このような中断が主要なビジネスの機能とプロセスに及ぼす影響を最小限に抑えることができる。




**IT プロセス: 継続的なサービスの保証のコントロール目標は、**

IT サービスの中断発生時のビジネスに対する影響を最小限に抑えることを、**ビジネス要件**とし、

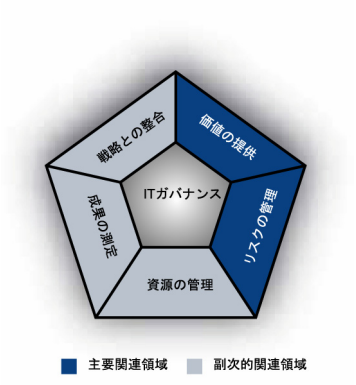
**重点をおくべきコントロールは、**障害からの回復力のあるシステム化を行い、IT 継続計画を作成、保守、およびテストすることである。

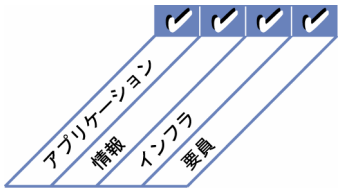
**実現するための手段は、次の 3 項目である。**

- IT 緊急時対応計画の作成と維持(改善)
- IT 緊急時対応計画に関する訓練とテスト
- 遠隔地における保管施設への緊急時対応計画のコピーとデータの保管

**その成果の測定指標は、次の 2 項目である。**

- 予定外の機能停止に起因する、1 ユーザ、月あたりの損失時間数
- IT 継続計画でカバーされていない、IT に依存している重要なビジネスプロセスの数



# コントロール目標 －詳細－

## DS4 継続的なサービスの保証

### DS4.1 IT 継続フレームワーク
一貫したプロセスで全社的な事業継続管理を支援する、IT 継続フレームワークを作成する。このフレームワークの目的は、求められるインフラストラクチャの復旧能力の決定を支援し、災害復旧計画と IT 緊急時対応計画の策定を促進することである。このフレームワークには、内外のサービスプロバイダ、その管理者および取引顧客の役割、担当作業、および実行責任を含む、継続管理に必要な組織構造、そして災害復旧計画および IT 緊急時対応計画を文書化、テスト、および実施する際のルールと体制を規定する必要がある。また計画には、重要な資源の特定、その資源の可用性のモニタリングと報告、代替処理手続、およびバックアップと復旧に関する原則などの項目も規定する必要がある。

### DS4.2 IT 継続計画
大規模な中断が主要なビジネスの機能とプロセスに及ぼす影響の軽減を目的とする、フレームワークに基づいた IT 継続計画を策定する。この計画では、すべての重要な IT サービスの障害からの回復、代替処理手続、および復旧能力に関する要件について規定する。また、計画では利用ガイドライン、役割と実行責任、手続、周知プロセス、およびテスト方法も規定しなければならない。

### DS4.3 重要な IT 資源
IT 継続計画において、最重要と定められた要素に重点を置くことで、障害からの回復力を組み込み、災害復旧時の作業の優先順位を設定する。重要度が低い要素の回復を優先させることのないよう、優先的ビジネス要件に応じた対応と復旧を確実にする。また、費用を受容可能なレベルに抑え、法的要件および契約上の要件へのコンプライアンスも確保する。1～4 時間、4～24 時間、24 時間超、重要業務の運用期間など、さまざまなレベルにおける回復力、対応、および復旧要件を考慮する。

### DS4.4 IT 継続計画の保守
IT 継続計画の内容が常に最新に保たれ、継続的に実際のビジネス要件が反映されることを確実にするために、IT 管理部門に対し、変更管理手続の策定および実施を促す。手続と実行責任における変更内容を明確かつタイムリーに周知することが不可欠である。

### DS4.5 IT 継続計画のテスト
IT システムが効果的に回復可能であること、欠点が解消されること、および IT 継続計画の妥当性が維持されることを確実にするために、IT 継続計画の定期的なテストを実施する。このためには、綿密な準備、手続の文書化、テスト結果の報告、および結果に基づく対応計画の策定と実施が必要である。テストの範囲として、単一アプリケーションの復旧テストから、複数のテストシナリオを組み合わせたテスト、エンドツーエンドでのテスト、そしてベンダーを含む総合的なテストなどを想定する。

### DS4.6 IT 継続計画に関する研修
すべての関係者が、インシデントまたは災害発生時の各自の役割および実行責任と実施手続に関する定期訓練セッションを確実に受講する。緊急時対応テストの結果に基づいて、訓練の内容を検証および補強する。

### DS4.7 IT 継続計画の配付
計画が安全かつ適切な方法で確実に配付され、必要な時に必要な場所で許可を受けた当事者が利用できるように、定義および管理された配付方法が存在することを確認する。どのような災害発生状況においても、IT 継続計画が入手および参照可能な状態になっているよう配慮する必要がある。

### DS4.8 IT サービスの復旧および再開
IT サービスの復旧および再開中に実施すべき措置を計画する。この計画には、バックアップサイトの起動、代替処理の開始、顧客および利害関係者への周知、再開手続などが規定される。IT の復旧にかかる時間とビジネスの復旧と再開のニーズを支援するために必要な技術投資について、ビジネス部門が確実に理解しているようにする。

### DS4.9 遠隔地におけるバックアップ保管施設
すべての重要なバックアップメディア、文書、および IT 復旧計画と業務継続計画に必要なその他の IT 資源を、遠隔地の施設に保管する。保管するバックアップの内容については、ビジネスプロセスオーナと IT 担当者が協働して決定する必要がある。遠隔地の保管施設の管理者は、データ分類方法のポリシーと企業のメディア保管活動に対応しなければならない。IT 管理部門は、遠隔地保管施設について、保管内容、施設の物理的安全性、およびセキュリティを確実に定期的に(少なくとも 1 年に 1 回)評価する必要がある。アーカイブデータの復元のためのハードウェアとソフトウェアの互換性を確保し、アーカイブデータを定期的にテストおよび更新する。

### DS4.10 再開後のレビュー
災害発生後に IT 機能が正常に再開した後、IT 管理部門が IT 復旧計画の妥当性を評価する手続を策定したか確認し、必要に応じて計画を更新する。

# マネジメントガイドライン

## DS4 継続的なサービスの保証

| From | インプット |
|---|---|
| PO2 | 採用したデータの分類方法 |
| PO9 | リスク評価 |
| AI2 | 可用性、継続性、および復旧の仕様 |
| AI4 | ユーザ、運用、サポート、技術、および管理の各マニュアル |
| DS1 | サービス・レベル・アグリーメント(SLA)とオペレーショナル・レベル・アグリーメント(OLA) |

| アウトプット | To | | | | | | |
|---|---|---|---|---|---|---|---|
| 緊急時対応テストの結果 | PO9 | | | | | | |
| IT 構成要素の重要度 | DS9 | | | | | | |
| バックアップの保管と保護計画 | DS11 | DS13 | | | | | |
| インシデント/災害のしきい値 | DS8 | | | | | | |
| 災害時サービス要件(役割および実行責任を含む) | DS1 | DS2 | | | | | |
| プロセスの成果報告 | ME1 | | | | | | |

### RACI チャート

| アクティビティ | 担当 CEO | CFO | 企業幹部 | CIO | ビジネス プロセス オーナー | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO (プロジェクト・マネジメント・オフィス) | コンプライアンス・監査・リスク・セキュリティ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| IT 継続フレームワークの作成 | | C | C | A | C | R | R | R | C | C | R |
| ビジネス影響分析とリスク評価の実施 | | C | C | C | C | A/R | C | C | C | C | C |
| IT 継続計画の策定と保守 | I | C | C | C | I | A/R | | C | C | C | C |
| 復旧目標に基づく IT 資源の特定と分類 | | | | C | | A/R | | C | I | C | I |
| IT 継続計画を常に最新の状態で維持するための変更管理手続の策定と実施 | | | | I | | A/R | | R | R | R | I |
| IT 継続計画の定期的なテスト | | | | I | I | A/R | | C | C | I | I |
| テスト結果に基づく追加対応計画の作成 | | | | C | I | A/R | C | R | R | R | I |
| IT 継続計画に関する訓練の計画と実施 | | | | I | R | A/R | | C | R | I | I |
| IT サービスの復旧および再開の計画策定 | | I | I | C | C | A/R | C | R | R | R | C |
| バックアップの保管と保護に関する計画の策定と実施 | | | | I | | A/R | | C | C | I | I |
| 再開後のレビュー実施手続の確立 | | | | C | | A/R | | C | C | | C |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

### 達成目標とその評価指標

**アクティビティの達成目標**
- IT 緊急時対応計画の作成と維持(改善)
- IT 緊急時対応計画に関する訓練とテスト
- 遠隔地の施設への緊急時対応計画のコピーとデータの保管

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- IT 継続計画の特定要素のテスト間隔
- IT 部門の当該従業員 1 人あたりの、IT 継続計画に関する年間の訓練時間
- 自動化された可用性モニタリングを行っている重要インフラストラクチャの割合
- IT 継続計画のレビュー実施頻度

*促進*

**プロセスの達成目標**
- 業務継続計画を支援する IT 継続計画の策定
- 実施、テスト、および維持可能な IT 継続計画の策定
- IT サービス中断発生の可能性の極小化

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- サービス・レベル・アグリーメント(SLA)に定められた要件を満たす可用性の割合
- IT 継続計画でカバーされていない IT に依存している重要なビジネスプロセスの数
- 復旧目標を達成したテストの割合
- 重要なシステムのサービス中断発生頻度

*促進*

**IT の達成目標**
- 要求に応じて IT サービスを使用可能であることの保証
- IT サービスの中断または変更が及ぼすビジネスへの影響の極小化
- エラー、意図的な攻撃、または災害で生じた障害に対する、IT サービスおよびインフラストラクチャの抵抗力・回復力の確実な保証

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- 予定外の機能停止に起因する、1 ユーザあたりの損失時間数(1 カ月)

# 成熟度モデル

## DS4 継続的なサービスの保証

**「IT サービスの中断発生時のビジネスに対する影響を最小限に抑える。」という IT に対するビジネス要件を満たす上で、「継続的なサービスの保証」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
IT 運用におけるリスク、脆弱性、および脅威、または IT サービスを提供できなくなった場合のビジネスへの影響が認識されていない。マネジメント層がサービスの継続性について配慮する必要はないと考えている。

**1 初期/その場対応**
継続的なサービスの実行責任は正式に定められておらず、実行責任を果たす上での権限は限定的である。マネジメント層が、継続的なサービスの必要性とそれに関連するリスクを認識しつつある。マネジメント層の継続的なサービスに対する関心は、IT サービスではなく主にインフラストラクチャ資源に向けられている。サービス中断に際しては、ユーザがワークアラウンド(回避策)を講じている。大規模な中断に対し、IT 部門の対応が事後的であり準備がなされていない。計画的な機能停止は IT 部門のニーズに応じて予定され、ビジネス上の要件は考慮されない。

**2 再現性はあるが直感的**
継続的なサービスを保証するための実行責任が割り当てられている。継続的なサービスを保証する手法は断片的である。システムの可用性に関する報告は散発的に実施され、不完全である可能性がある。また、この報告ではビジネスに与える影響が考慮されていない。継続的なサービスの可用性を実現するための取り組みが行われ、その主要な方針が周知されているが、IT 継続計画が文書化されていない。重要なシステムとコンポーネントの一覧が作成されているが、信頼性が低い。継続的なサービスのための実践基準が徐々に見られるようになっているが、その成功は各担当者の裁量に依存している。

**3 定められたプロセスがある**
継続的なサービスの管理に関する説明責任の所在が明確化されている。継続的なサービスの計画策定とテストの実行責任が明確に定義され、割り当てられている。システムの重要度とビジネスに与える影響に基づくIT継続計画が文書化されている。継続的なサービスのテストに関する報告が定期的に行われている。各個人が率先して標準を遵守し、大規模なインシデントまたは災害発生時の対処に関する訓練を受けている。マネジメント層は、継続的なサービスを保証するための計画の必要性を一貫して周知させている。可用性の高いコンポーネントが使用され、システムの冗長化が図られている。重要なシステムとコンポーネントの一覧が維持されている。

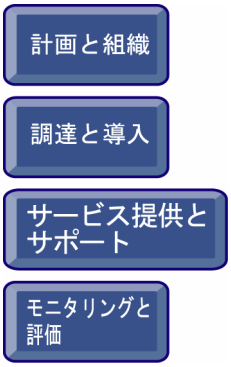
**4 管理され、測定可能である**
継続的なサービスの実行責任と標準が徹底運用されている。サービスの継続計画を維持する実行責任が割り当てられている。維持活動は、継続的サービスのテスト結果、内部の優れた実践基準、IT およびビジネスの変化に基づいて行われている。継続的なサービスに関する体系的なデータが収集、分析、報告され、これに基づいて対策がとられている。継続的なサービスプロセスに関する正式な訓練が実施されており、参加が義務付けられている。システム可用性に関する優れた実践基準が一貫して導入されている。可用性に関する実践基準と継続的なサービスの計画策定は相互に影響を及ぼしている。中断インシデントは分類され、それぞれの上位へのエスカレーションパスについて関係者全員が十分に認識している。継続的なサービスに関する KGI と KPI が策定および合意されているが、一貫した方法で測定されていない可能性がある。

**5 最適化**
継続的なサービスの統合プロセスでは、ベンチマーク評価と外部のベストプラクティスについても考慮されている。IT 継続計画が業務継続計画と統合されており、定期的に保守されている。継続的なサービスを保証するための要件を満たす上で、ハードウェアの早期出荷契約等が一般的である。IT 継続計画の包括的なテストが実施されており、その結果が計画の更新に利用されている。データが収集および分析され、プロセスが継続的に改善されている。可用性に関する実践基準と継続的なサービスの計画策定は完全に連携されている。マネジメント層は、SPOF(single point of failure)に起因する障害または大規模インシデントが発生しないことを保証できる。エスカレーションに関する実践基準は、理解されており、徹底して実施されている。継続的なサービスの達成に関する KGI と KPI が、体系的な方法で測定されている。マネジメント層は、測定された KGI と KPI に応じて継続的なサービスの計画を調整している。

# コントロール目標 —概要—

## DS5 システムセキュリティの保証

情報のインテグリティを維持し、IT 資産を保護するためには、セキュリティ管理のプロセスが必要である。このプロセスには、IT セキュリティに関する役割と責務、ポリシー、標準、および手続を定め、それらを運用、改善することが含まれる。また、セキュリティ管理には、セキュリティのモニタリングと定期的なテストの実施、および識別されたセキュリティの弱点やインシデントに対する是正措置の導入も含まれる。セキュリティ管理を効果的に実行することで、すべての IT 資産を保護し、セキュリティの脆弱性やインシデントがビジネスに与える影響を最小限に抑えることができる。


**IT プロセス: システムセキュリティの保証のコントロール目標は、**

情報および情報処理インフラストラクチャのインテグリティを維持し、セキュリティ上の脆弱性やインシデントによる影響を最小限に抑えることを、**ビジネス要件**とし、

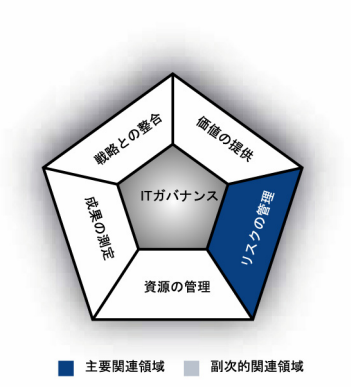
**重点をおくべきコントロールは、**IT セキュリティポリシー、手続および標準を明確に定め、セキュリティ上の脆弱性やインシデントをモニタリング、発見、報告、是正することである。

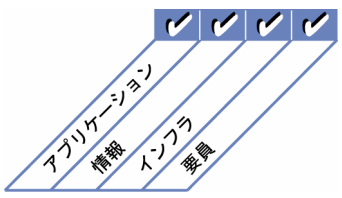
**実現するための手段は、次の 3 項目である。**

- セキュリティ要件と、脆弱性、脅威の認識
- 標準化された方法によるユーザの識別と認可の管理
- 定期的なセキュリティテストの実施

**その成果の測定指標は、次の 3 項目である。**

- 社会的信用に悪影響を及ぼしたインシデントの件数
- セキュリティ要件を満たしていないシステムの数
- 職務分離が適切に行われていない違反の数



# コントロール目標 －詳細－

## DS5 システムセキュリティの保証

### DS5.1 IT セキュリティの管理
セキュリティに係る活動が、ビジネス上の要件に沿って実施されるよう、組織の適切な上位層において、最適な体制を組んで IT セキュリティを管理する。

### DS5.2 IT セキュリティ計画
情報に関するビジネス要件、IT の構成、情報リスクへの対応計画、および情報セキュリティ文化を総合的な IT セキュリティ計画としてまとめる。この計画は、サービス、要員、ソフトウェア、およびハードウェアに対する適切な投資とともに、セキュリティポリシーや関連手続に盛り込まれる。セキュリティポリシーおよび手続は、利害関係者とユーザに周知する。

### DS5.3 ID 管理
IT システムにおけるすべてのユーザ(内部、外部、臨時かどうかを問わず)と、ユーザのすべてのアクティビティ(ビジネスアプリケーションやシステムの操作、開発や保守)を、個々に識別しなくてはならない。システムやデータに対するユーザのアクセス権は、文書化された業務上の必要性や職務要件に即したものでなければならない。ユーザのアクセス権は、ユーザ管理職の申請に基づいてシステムオーナが承認し、セキュリティ責任者が実装する。ユーザ ID とアクセス権は、単一のリポジトリで集中管理する。ユーザの識別、認証の実施、およびアクセス権の徹底管理のために、費用効率に優れた技術面および手続面での対策を講じ、常に継続的な改善を行う。

### DS5.4 ユーザアカウントの管理
ユーザアカウントおよびそれに付随するユーザ権限の申請、設定、発行、停止、変更、および抹消は、ユーザアカウント管理において確実に行う。ユーザアカウントの管理には、データオーナまたはシステムオーナがアクセス権限を付与する場合の承認手続も含まれる。これら一連の手続は、アドミニストレーター(特権ユーザ)、内部ユーザ、外部ユーザを含むすべてのユーザに、平常時・緊急時を問わず適用されるべきである。企業が所有するシステムと情報へのアクセスに関連した権利と義務は、あらゆるタイプのユーザごとに契約の形式で定める。すべてのアカウントとそれらに関連する権限の内容は、マネジメント層が定期的にレビューする。

### DS5.5 セキュリティのテスト、監視、モニタリング
IT セキュリティの導入、運用に関して、テストおよびモニタリングを積極的に行うことが必要である。承認されたセキュリティレベルが確実に保たれていることを保証するために、IT セキュリティは定期的に見直しを行わなければならない。ログの取得、およびモニタリングの機能を活用することで、対応の必要な異例もしくは異常な行動を、早めに検知できる。ログ情報へのアクセスは、業務上の必要性に基づいて規定されるアクセス権およびログ保存基準に従って行う。

### DS5.6 セキュリティインシデントの定義
起こり得るセキュリティインシデントの特性を明確に定義、周知し、インシデント管理または問題管理プロセスによって、セキュリティインシデントに確実に対応できるようにする。特性の定義には、セキュリティインシデントと見なされる判断基準および影響レベルが含まれる。影響レベルの定義は数を限定し、それぞれのレベルに対して要求される具体的な対処方法と、通知すべき要員を特定する。

### DS5.7 セキュリティ技術の保護
重要なセキュリティ関連技術には、改ざんに対する確実な耐性を持たせる。また、セキュリティ関連文書が不必要に開示されないように、つまり、目立たないようにする。ただし、セキュリティ仕様の機密が漏れても、システムのセキュリティが保たれるようにしなくてはならない。

### DS5.8 暗号鍵の管理
暗号鍵の生成・変更・取消・失効・交付・認証・保存・入力・使用・アーカイブ化を体系的に行うためのポリシーおよび手続を確実に整備し、暗号鍵の改変や、許可されていない暗号鍵の開示を防止する。

### DS5.9 不正ソフトウェアの阻止、発見、および是正
予防・発見・対処のための対策(特に最新のセキュリティパッチとウイルス管理)を組織全体にわたって確実に実施し、IT システムおよび情報技術を悪意のあるソフトウェア(ウイルス、ワーム、スパイウェア、スパム、社内で開発された不正ソフトウェアなど)から確実に保護する。

### DS5.10 ネットワークのセキュリティ
セキュリティ技術とそれに関連する管理手続(ファイアウォール、セキュリティアプライアンス、ネットワークのセグメント化、侵入検知など)をを使用し、ネットワークへのアクセスの許可とネットワークに出入りする情報フローを確実にコントロールする。

### DS5.11 機密データの交換
機密性を有するトランザクションデータは、内容の真正性確保、送信証明、受信証明、および送信元による否認防止が可能なコントロールを備えた信頼できる経路あるいはメディアのみを介してやり取りを行う必要がある。

# マネジメントガイドライン

## DS5 システムセキュリティの保証

| From | インプット |
|---|---|
| PO2 | 情報アーキテクチャ：採用したデータの分類方法 |
| PO3 | 技術標準 |
| PO9 | リスク評価 |
| AI2 | アプリケーションセキュリティのコントロールの仕様 |
| DS1 | オペレーショナル・レベル・アグリーメント(OLA) |

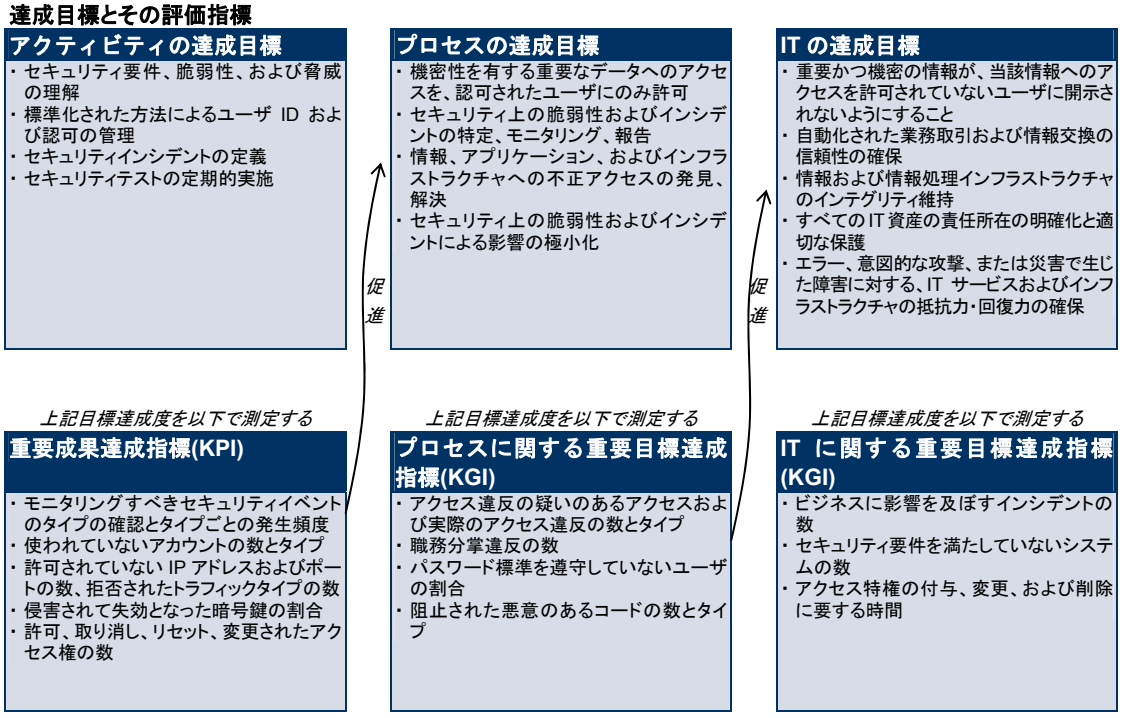
| アウトプット | To |
|---|---|
| セキュリティインシデントの定義 | DS8 |
| セキュリティ意識の向上に関する具体的な研修要件 | DS7 |
| プロセスの成果報告 | ME1 |
| 必要なセキュリティ変更 | AI6 |
| セキュリティ上の脅威と脆弱性 | PO9 |

### RACI チャート

| アクティビティ / 担当 | CEO | CFO | 企業幹部 | CIO | ビジネスプロセスオーナ | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO（プロジェクト・マネジメント・オフィス） | コンプライアンス・監査・リスク・セキュリティ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| IT セキュリティ計画の定義と維持 | I | C | C | A | C | C | C | C | I | I | R |
| ID(アカウント)管理プロセスの定義・作成・運用 | | | I | A | C | R | R | I | | | C |
| 潜在的および実際のセキュリティインシデントのモニタリング | | | | A | I | R | C | C | | | R |
| ユーザのアクセス権・特権の定期的見直しと確認 | | | | I | A | C | | | | | R |
| 暗号鍵の保持・保護のための手続作成と改訂 | | | | A | | R | | | I | | C |
| ネットワーク間の情報フローを保護する技術的・手続的なコントロールの導入・維持 | | | | A | C | C | R | R | | | C |
| 定期的な脆弱性評価の実施 | | I | | A | I | C | C | C | | | R |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

### 達成目標とその評価指標



# 成熟度モデル

## DS5 システムセキュリティの保証

**「情報および情報処理インフラストラクチャのインテグリティを維持し、セキュリティ上の脆弱性やインシデントによる影響を最小限に抑える。」という IT に対するビジネス要件を満たす上で、「システムセキュリティの保証」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
組織が IT セキュリティの必要性を認識していない。セキュリティを確保するための実行責任および説明責任が割り当てられていない。IT セキュリティ管理を支援する対策が実施されていない。IT セキュリティに関する報告および IT セキュリティ違反発生時にとるべき対応プロセスが存在しない。システムのセキュリティ管理プロセスと呼べるようなものがまったく存在しない。

**1 初期/その場対応**
組織が IT セキュリティの必要性を認識している。セキュリティの必要性に関する意識は、主として個人に依存している。IT セキュリティへの取り組みは事後対応という形である。IT セキュリティの成果測定は行われていない。責任の所在が明確ではなく、IT セキュリティ違反が発見された場合、責任のなすり合いが起こる。IT セキュリティ違反への対応は予測できない。

**2 再現性はあるが直感的**
IT セキュリティの実行責任および説明責任は IT セキュリティに関する調整を担う担当者に課せられているが、この担当者には限られた管理権限しか与えられていない。セキュリティの必要性に関する意識は断片的で限定的である。セキュリティ関係の情報はシステムによって生成されているが、分析は行われていない。サードパーティが提供するサービスが、セキュリティに関する組織特有のニーズに対応していない可能性がある。セキュリティポリシーを策定中であるが、スキルおよびツールが不十分である。IT セキュリティの報告体制は、不完全で、誤解を招きやすく、適切ではない。セキュリティ研修が提供されているが、受講するかどうかは主に個人の自発性に委ねられている。IT セキュリティは主に IT 部門の責任および分野であるとみなされており、ビジネス部門側に IT セキュリティが自己の責任分野であるとの意識がない。

**3 定められたプロセスがある**
セキュリティに対する意識があり、マネジメント層もその向上を推進している。IT セキュリティ手続が定義され、IT セキュリティポリシーとの整合が図られている。IT セキュリティに関する責任が割り当てられ、理解されているものの、一貫した実行はなされていない。リスク分析に基づいた IT セキュリティ計画とセキュリティソリューションがある。セキュリティに関する報告には、明確なビジネス的視点が含まれていない。セキュリティのテスト(侵入テストなど)は場当たり的に行われている。IT 部門とビジネス部門の両方を対象にしたセキュリティ研修が提供されているが、計画と運営は非公式に行われているにすぎない。

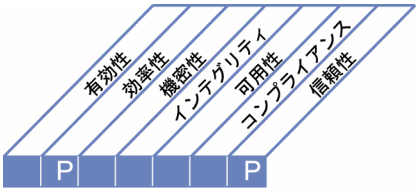
**4 管理され、測定可能である**
IT セキュリティの責任が明確に割り当てられ、管理、実行されている。IT セキュリティのリスクと影響に関する分析が、一貫して行われている。具体的なセキュリティ基準に基づき、セキュリティポリシーとセキュリティに関する活動が完了している。セキュリティ意識の向上に向けた取り組みには、全員の参加が義務付けられている。ユーザの識別や、認証、認可が標準化されている。セキュリティの監査および管理の責任を負うスタッフには、セキュリティ資格の取得が求められている。セキュリティテストは、正式な標準プロセスに従って実施され、それがセキュリティレベルの向上につながっている。IT セキュリティプロセスと組織全体のセキュリティ機能との調整が図られている。IT セキュリティに関する報告と、ビジネス目標との関連付けが行われている。IT セキュリティに関する研修が、ビジネス部門および IT 部門の双方において行われている。IT セキュリティに関する研修が業務上の要請や文書化されたセキュリティリスク分析結果に対応する形で計画、管理されている。セキュリティ管理に対する KGI と KPI が定義されているが、測定までは行われていない。

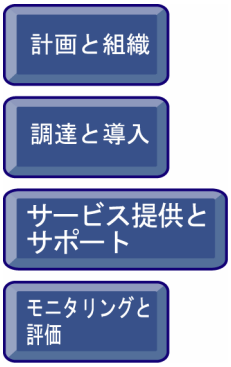
**5 最適化**
IT セキュリティはビジネス部門と IT 管理部門の共同責任であり、企業のセキュリティに関するビジネス目標に組み込まれている。IT セキュリティ要件が明確に定義および最適化されており、承認されたセキュリティ計画に盛り込まれている。ユーザおよび顧客は、セキュリティ要件の定義に対してますます大きな説明責任を負い、設計段階からセキュリティ機能がアプリケーションに組み込まれている。セキュリティインシデントへの対応は、自動化ツールを利用した正式なインシデント対応手続に基づいて、迅速に行われている。定期的なセキュリティ評価が行われ、導入したセキュリティ計画の有効性が評価されている。脅威および脆弱性に関する情報が体系的に収集・分析されている。リスクを軽減するための適切なコントロールが直ちに伝達され、実施されている。セキュリティテスト、インシデントの根本的原因の分析、およびリスクを積極的に発見することで、継続的にプロセスを改善している。組織全体でセキュリティプロセスと技術の統合が図られている。セキュリティ管理に関する重要目標達成指標(KGI)および重要成果達成指標(KPI)が収集され、周知されている。マネジメント層は KGI と KPI を用いて、セキュリティ計画を継続的に改善している。

# コントロール目標 －概要－

## DS6 費用の捕捉と配賦

IT 費用をビジネス部門に適正かつ公平に配賦するための体系を実現するには、IT 費用を正確に測定し、適正な配賦についてビジネス部門の同意を得る必要がある。このプロセスには、IT 費用を捕捉し、サービスを受けるユーザへ配賦および報告するためのシステムの構築と運用が含まれる。適正な配賦システムを導入することで、IT サービスの利用に関して、ビジネス部門が十分な情報を得た上での決定が可能になる。




**IT プロセス: 費用の特定と配賦のコントロール目標は、**

IT 費用の透明性と理解の確保、および十分な情報を得た上での IT サービスの利用による費用効率の向上を、**ビジネス要件**とし、

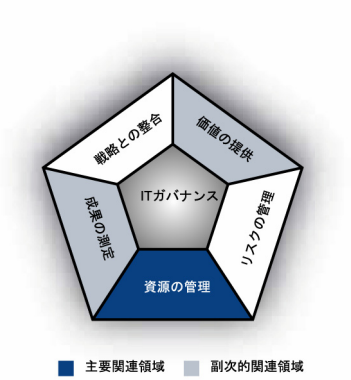
**重点をおくべきコントロールは、**IT 費用の完全かつ正確な捕捉、およびビジネス部門の同意を得た適正な配賦体系と、IT の利用および配賦費用に関するタイムリーな報告体系の確立することである。

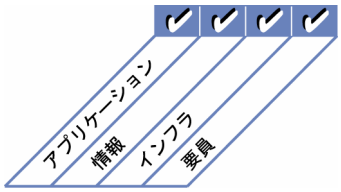
**実現するための手段は、次の 3 項目である。**

- 提供サービスの質/量に見合う課金
- 完備された費用モデルの構築とそれに対する同意
- 同意されたポリシーに基づく課金の実施

**その成果の測定指標は、次の 3 項目である。**

- ビジネス管理部門が承認した/支払った IT サービス費用請求の割合
- 予算、予測、および実費用間の不一致の割合
- 同意された費用モデルに基づいて配賦された IT 費用の総 IT 費用に対する割合



# コントロール目標 －詳細－

## DS6 費用の捕捉と配賦

**DS6.1 サービスの定義**
透明性のある費用モデルを実現するため、すべての IT 費用を特定し、これらの費用を IT サービスに対応付ける。IT サービスをビジネスプロセスに関連付け、ビジネス部門が関連サービスの費用請求レベルを特定できるようにする。

**DS6.2 IT 財務管理**
定義された費用モデルに従って実費用を捕捉および配賦する。企業の財務測定体系に従って、予測と実費用間の不一致を分析し、報告する。

**DS6.3 費用モデルの策定と費用請求**
サービス定義に基づいて、サービスの直接費、間接費、および諸経費を含み、サービスあたりのチャージバック率の計算を支援する費用モデルを策定する。この費用モデルは、企業の原価計算手続に沿ったものである必要がある。IT 費用モデルの策定により、サービスに対する費用請求をユーザが確実に特定、測定、および予測可能となり、資源の適切な利用が促進される。ユーザマネジメントが、サービスの実利用状況と課金状況を検証できる必要がある。

**DS6.4 費用モデルの保守**
費用/課金モデルの適合性を定期的にレビューおよびベンチマーク評価し、進化するビジネス活動と IT 活動に対する妥当性および適合性を維持する。

# マネジメントガイドライン

## DS6 費用の捕捉と配賦

| From | インプット |
|---|---|
| PO4 | 文書化されたシステムオーナ |
| PO5 | 費用便益報告、IT 予算 |
| PO10 | 詳細なプロジェクト計画 |
| DS1 | サービス・レベル・アグリーメント(SLA)とオペレーショナル・レベル・アグリーメント(OLA) |

| アウトプット | To |
|---|---|
| IT 会計報告 | PO5 |
| プロセスの成果報告 | ME1 |

**RACI チャート**

**担当**

| アクティビティ | CEO | CFO | 企業幹部 | CIO | ビジネスプロセスオーナ | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO（プロジェクト・マネジメント・オフィス） | コンプライアンス、監査、リスク、セキュリティ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 提供サービス/サポートされているビジネスプロセスへの IT インフラストラクチャの対応付け | | C | C | A | C | C | C | C | R | C | |
| すべての IT 費用(要員的費用、技術的費用など)の特定と、これらの費用の IT サービスへの単位原価での対応付け | | C | | A | | C | C | C | R | C | |
| IT 会計および原価管理のプロセスの確立と保守 | | C | C | A | C | C | C | C | R | C | |
| 課金に関するポリシーと手続の確立と保守 | | C | C | A | C | C | C | C | R | C | |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

**達成目標とその評価指標**

**アクティビティの達成目標**
- ビジネス管理部門による配賦費用のレビュー
- 提供サービスの質に見合う費用の調整
- 完備された費用モデルの構築とそれに対する同意
- 同意されたポリシーに基づく課金の実施
- 費用のベンチマーク評価の定期的な実施

*促進*

**プロセスの達成目標**
- IT 費用とサービスの適正かつ公平な定義付け
- IT サービスの費用の正確な捕捉
- IT サービス利用者への IT 費用の適正かつ公平な配賦

*促進*

**IT の達成目標**
- IT 運用にかかる費用、便益、戦略、ポリシー、およびサービスレベルについての透明性の確保と理解の実現
- IT の費用効率およびビジネス収益性への IT の貢献度の向上
- IT による費用効率の高いサービス品質、継続的な改善、および将来の変更に対する対応力の保証

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- 費用モデルの定義に関与したビジネス部門の担当者の割合
- 費用配賦モデルのレビュー頻度
- 自動/手動で配賦された費用の割合

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- 予算、予測、および実費用間の不一致の割合
- 同意された費用モデルに基づいて配賦された IT 費用の総 IT 費用に対する割合
- ビジネス部門の同意を得られなかった費用の割合

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- ビジネス管理部門が承認した/支払った IT サービスの費用請求の割合
- サービスあたりの長期的な単位原価
- IT サービスの費用モデルに対するビジネス部門の満足度(調査)

# 成熟度モデル

## DS6 費用の捕捉と配賦

**「IT 費用の透明性と理解の確保、および十分な情報を得た上での IT サービスの利用による費用効率の向上。」という IT に対するビジネス要件を満たす上で、「費用の捕捉と配賦」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
提供される情報サービスに関する費用を特定し配賦するために認知可能なプロセスがまったく存在しない。組織は、原価計算に関して対処すべき問題の存在さえ認識しておらず、したがってその問題に関する話し合いも行われていない。

**1 初期/その場対応**
情報サービスの全体的な費用について一般的な理解はあるが、ユーザ、顧客、部門、ユーザグループ、サービス組織単位、プロジェクト、および成果物ごとの費用について個別に認識されていない。マネジメントに費用総計が報告されるだけで、費用のモニタリングは事実上実施されていない。IT 費用は運用上の経費として配賦されている。ビジネス部門に対して、サービス提供の費用もしくは便益に関する情報が提供されていない。

**2 再現性はあるが直感的**
費用の集計と配賦の必要性が全体的に認識されている。費用配賦は非公式または費用に対する基本的な前提(ハードウェア費用など)に基づいて実施されており、価値要因への関連付けがほとんどなされていない。費用配賦プロセスは繰り返し実施されている。費用の捕捉および配賦に関する標準の手続について、正式な研修が行われておらず、また周知もされていない。費用の捕捉と配賦の実行責任が割り当てられていない。

**3 定められたプロセスがある**
情報サービスの費用モデルが定められ、文書化されている。ユーザに提供されるサービスと IT 費用の関連付けプロセスが策定されている。情報サービスにかかる費用について、適切に認識されている。ビジネス部門に対し、費用に関する基本的な情報が提供されている。

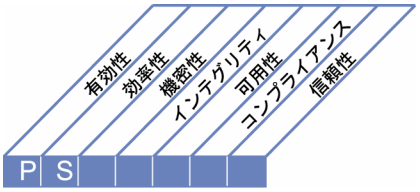
**4 管理され、測定可能である**
情報サービスの費用管理についての実行責任と説明責任の所在が明確化されており、すべてのレベルにおいて十分に理解されている。また、これらの費用管理に関する正式な研修が実施されている。タイムリーかつ自動化された方法を用いて直接費と間接費が捕捉され、マネジメント層、ビジネスプロセスオーナ、およびユーザに報告されている。費用のモニタリングと評価が概ね実施されており、費用の逸脱が発見されると対応措置がとられる。情報サービスの費用は、ビジネス目標とサービス・レベル・アグリーメント(SLA)に関連付けて報告されており、ビジネスプロセスオーナによりモニタリングされている。財務部門により、費用配賦プロセスの妥当性レビューが実施されている。自動化された原価計算システムが存在しているが、このシステムではビジネスプロセスではなく情報サービス機能に重点が置かれている。費用測定に関する KPI および KGI について合意が得られているが、その測定方法は一貫していない。

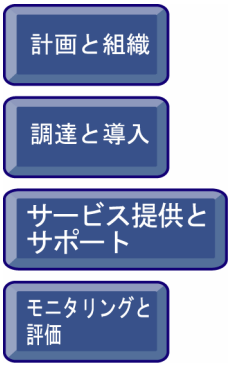
**5 最適化**
提供サービスの費用が捕捉、集計され、マネジメント層、ビジネスプロセスオーナ、およびユーザに報告されている。費用は請求可能項目として捕捉され、提供されたサービスに対して、利用率に基づいてユーザに適切に請求するチャージバックシステムで対応可能である。費用明細は、サービス・レベル・アグリーメント(SLA)に対応している。サービス費用のモニタリングおよび評価結果が、IT 資源の費用の最適化に活用されている。取得した費用の数値が、便益実現の検証、および組織の予算策定プロセスに利用されている。高度な報告システムを使用した情報サービスの費用報告により、ビジネス要件の変化について早期警告を得ることができる。提供されるサービスごとの処理量から導き出された、変動費用モデルが活用されている。費用管理は、継続的な改善および外部組織とのベンチマークの評価の結果、業界のベストプラクティスレベルにまで高められている。費用の最適化は継続的なプロセスとして実施されている。マネジメント層は、費用測定システムの再設計における継続的な改善プロセスの一環として、KPI および KGI のレビューを行っている。

# コントロール目標 －概要－

## DS7 利用者の教育と研修

IT 部門内を含む IT システムの全ユーザに対して効果的な教育を実施するには、ユーザグループごとの研修のニーズを特定する必要がある。このプロセスには、ニーズの特定の他に、効果的な研修のための戦略の策定と実施、および結果の測定が含まれる。効果的な研修プログラムにより、ユーザによるエラーの減少、生産性の向上、および主要コントロール(ユーザセキュリティ対策など)へのコンプライアンスの強化を実現でき、技術を一層効果的に利用できるようになる。




**IT プロセス: 利用者の教育と研修のコントロール目標は、**

アプリケーションおよび技術的ソリューションの効果的かつ効率的な利用と、ユーザによるポリシーおよび手続へのコンプライアンスを、**ビジネス要件**とし、

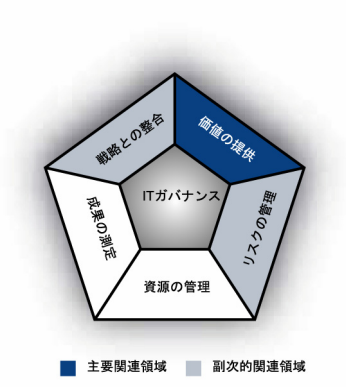
**重点をおくべきコントロールは、**IT ユーザの研修ニーズを明確に把握し、効果的な研修戦略と結果測定を実施することである。

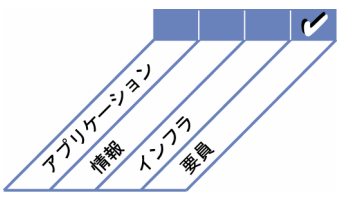
**実現するための手段は、次の 4 項目である。**

- 研修カリキュラムの作成
- 研修の準備
- 研修の実施
- 研修の有効性についてのモニタリングと報告

**その成果の測定指標は、次の 3 項目である。**

- ユーザ研修を実施しないことに起因するサービスデスクへの問い合わせの件数
- 実施された研修内容に満足している利害関係者の割合
- 研修ニーズの特定から研修実施までに要する時間



# コントロール目標 －詳細－

## DS7 利用者の教育と研修

### DS7.1 教育と研修のニーズの特定

研修対象の各従業員グループに対し、以下を考慮して研修カリキュラムを策定し、定期的に更新する。

- 現在/将来のビジネス上の必要性と戦略
- 企業の価値基準(倫理基準、コントロールおよびセキュリティの企業風土など)
- 新規 IT インフラストラクチャやソフトウェア(パッケージおよびアプリケーション)の導入
- 現在のスキル、能力プロファイル、公的資格および資格取得の必要性
- 実施方法(セミナー型、e ラーニング型など)、対象グループの規模、参加のしやすさ、および実施時期

### DS7.2 教育と研修の実施

特定された教育と研修のニーズに基づいて、研修対象グループとそのメンバー、効果的な実施方法、講師、トレーナー、およびメンターを定める。トレーナーを任命し、適時に研修セッションを計画する。登録者(受講の前提要件を含む)、出席状況、および成績評価を記録する必要がある。

### DS7.3 受講研修内容の評価

教育と研修の終了後、その実施内容について、妥当性、内容の質、有効性、獲得および吸収できた知識、費用と価値の面から評価する。この評価の結果を、将来のカリキュラムの策定と研修セッションに役立てる。

# マネジメントガイドライン

## DS7 利用者の教育と研修

| From | インプット |
|---|---|
| PO7 | ユーザのスキルと能力(自己研修を含む)、特定の研修要件 |
| AI4 | 研修資料、ソリューション導入にあたっての知識移転要件 |
| DS1 | オペレーショナル・レベル・アグリーメント(OLA) |
| DS5 | セキュリティ意識の向上に関する具体的な研修要件 |
| DS8 | ユーザ満足度の調査報告 |

| アウトプット | To |
|---|---|
| プロセスの成果報告 | ME1 |
| 必要な文書の更新 | AI4 |

### RACI チャート

**担当**

| アクティビティ | CEO | CFO | 企業幹部 | CIO | ビジネスプロセスオーナ | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO (プロジェクト・マネジメント・オフィス) | コンプライアンス・監査・リスク・セキュリティ | 研修部門 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ユーザの研修ニーズの特定とその分析 | | | C | A | R | C | C | C | C | C | C | R |
| 研修プログラムの作成 | | | C | A | R | C | I | C | C | C | I | R |
| 啓蒙活動および教育研修の実施 | | | I | A | C | C | I | C | C | C | I | R |
| 研修評価の実施 | | | I | A | R | C | I | C | C | C | I | R |
| 最良の研修実施方法およびツールの特定と評価 | | | I | A/R | R | C | C | C | C | C | C | R |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R:Responsible) ②説明責任者(A:Accountable) ③協議先(C:Consulted)④報告先(I:Informed)

### 達成目標とその評価指標

**アクティビティの達成目標**
- 研修カリキュラムの作成
- 研修の準備
- 研修の実施
- 研修の有効性についてのモニタリングと報告

*促進*

**プロセスの達成目標**
- 最も費用効率に優れた方法を使用した、各レベルのユーザ向け研修プログラムの作成
- アプリケーションおよび技術ソリューションに関する知識のユーザへの移転
- アプリケーションと技術的対応策を利用する際のリスクと実行責任に関する意識の向上

*促進*

**IT の達成目標**
- 提供サービスとサービスレベルに対するエンドユーザの満足の確保
- アプリケーションおよび技術的対応策の適切な利用と成果達成の保証
- IT インフラストラクチャ、資源、および能力の最適化

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- 研修カリキュラムの更新頻度
- 研修ニーズの特定から研修実施までに要する時間

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- 研修に関するサービスデスクへの問い合わせ件数、または質問への回答件数
- 実施された研修内容に満足している利害関係者の割合
- 研修を受けた従業員の割合

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- システムに対する理解の向上による、従業員の測定された生産性の向上
- サービス、システム、または新たな技術の周知によるユーザ満足度の向上

# 成熟度モデル

## DS7 利用者の教育と研修

**「アプリケーションおよび技術的対応策の効果的かつ効率的な利用と、ユーザのポリシーおよび規定された手続への準拠。」というIT に対するビジネス要件を満たす上で、「利用者の教育と研修」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
教育研修プログラムがまったく存在ない。組織は、研修に関して対処すべき問題の存在さえ認識しておらず、したがってその問題に関する話し合いも行われていない。

**1 初期/その場対応**
教育研修プログラムの必要性を組織が認識している徴候はあるが、標準化されたプロセスが存在しない。体系的なプログラムが存在しないため、従業員が自ら研修コースを選択して参加している。こうした研修コースの中には、倫理規定、システムセキュリティの意識、およびセキュリティ活動に関する問題を扱っているものもある。マネジメントの取り組みに結束がなく、教育研修に関する課題や取り組みについての話し合いは散発的で一貫性がない。

**2 再現性はあるが直感的**
教育研修プログラムと関連プロセスの必要性が組織全体において認識されている。研修が、従業員の個別の業績計画に組み込まれるようになってきている。プロセスの成熟度は、複数のインストラクターが非公式な教育研修コースを実施する段階にまできているが、同一のテーマが異なるアプローチで扱われている。一部の研修コースでは、倫理規定、システムセキュリティの意識、およびセキュリティ活動に関する問題を扱っている。各研修担当者の知識に依存する部分が大きい。ただし、全体的な課題と、このような課題に対処する必要性に関しては、一貫して話し合われている。

**3 定められたプロセスがある**
教育研修プログラムが制度化され周知されており、従業員と管理者が研修の必要性を把握して文書化している。教育研修プロセスが標準化および文書化されている。教育研修プログラムを実施するための予算、資源、施設、講師が確保されつつある。倫理規定、システムセキュリティの意識およびセキュリティ活動に関する正式な研修コースが従業員を対象に実施されている。ほとんどの教育研修プロセスがモニタリングされているが、マネジメント層がすべての逸脱を発見できるとは考えにくい。教育研修における問題の分析は散発的にしか実施されていない。

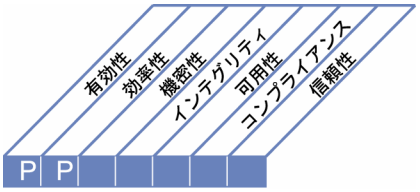
**4 管理され、測定可能である**
総合的な教育研修プログラムが設けられており、結果が測定可能である。実行責任が明確化されており、プロセスの担当責任が割り当てられている。教育研修が従業員のキャリアパスの一要素として組み込まれている。マネジメント層が教育研修コースの開催を支援し、コースに参加している。従業員全員が倫理規定およびシステムセキュリティの意識に関する研修を受講している。障害による、システムの可用性、機密性、およびインテグリティに影響を及ぼす被害を防ぐため、従業員全員が適切なレベルのシステムセキュリティ活動についての研修を受講している。マネジメント層が教育研修プログラムとプロセスを日常的にレビューおよび更新することにより、準拠状況をモニタリングしている。プロセスが継続的に改善されており、常に内部のベストプラクティスが採用されるようになっている。

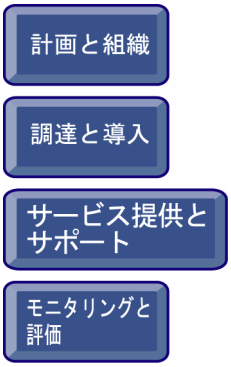
**5 最適化**
教育研修の結果として各個人の業績が向上している。教育研修が従業員のキャリアパスの重要な要素として組み込まれている。教育研修プログラムのために十分な予算、資源、施設、および講師が確保されている。外部のベストプラクティスや、成熟度モデルを利用し他社と比較することで、プロセスが洗練されてきており、継続的に改善されている。すべての問題や逸脱の根本原因が分析され、有効な対策が適宜特定および実施されている。倫理規定およびシステムセキュリティの原則に対する積極的な姿勢が見られる。教育研修プログラムに利用できるツールの提供および自動化のために、IT が広範囲で統合的かつ最適化された方法で IT が利用されている。研修に関する外部の専門家が活用され、ベンチマークを使用した指導が行われている。

# コントロール目標 －概要－

## DS8 サービスデスクとインシデントの管理

IT ユーザの問い合わせや発生した問題に対してタイムリーかつ効果的に対応するには、適切に構成、運用されているサービスデスクとインシデント管理プロセスが必要である。このプロセスには、インシデント登録、インシデントエスカレーション、傾向および根本原因の分析、および問題解決の機能を持つサービスデスクの設置が含まれる。ビジネス上の便益には、ユーザからの問い合わせに対する迅速な対応による、生産性の向上が含まれる。さらに、効果的な報告を通して、ビジネス部門はユーザ研修の不足といった根本原因の追究に取り組むことができる。




**IT プロセス: サービスデスクとインシデントの管理のコントロール目標は、**

エンドユーザからの問い合わせ、質問、およびインシデントを確実に解決および分析し、IT システムの効果的な利用を実現することを、**ビジネス要件**とし、

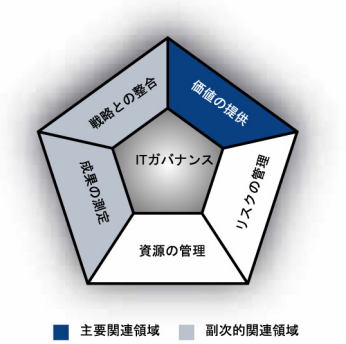
**重点をおくべきコントロールは、**速やかな対応、明確なエスカレーション手続、および解決策/傾向分析のプロフェッショナルな機能を持つサービスデスクの設置することである。

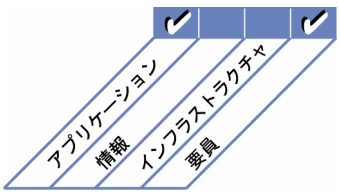
**実現するための手段は、次の 3 項目である。**

- サービスデスクの導入と運用
- 傾向のモニタリングと報告
- 明確なエスカレーション基準と手続の策定

**その成果の測定指標は、次の 3 項目である。**

- 一次サポートに対するユーザの満足度
- 合意/容認された期間内に解決したインシデントの割合
- 放棄呼率: サービスデスクが応答する前に、ユーザが問い合わせを放棄(切断)したコール(呼)の割合



# コントロール目標 －詳細－

## DS8 サービスデスクとインシデントの管理

**DS8.1 サービスデスク**
すべての問い合わせ、報告されたインシデント、およびサービスと情報に関する要求を登録、伝達、処理、分析し、ユーザと IT 部門とをつなぐ機能を果たすサービスデスクを設置する。該当サービス・レベル・アグリーメント(SLA)に関連する、合意されたサービスレベルに基づくモニタリングおよびエスカレーション手続が存在し、報告されたすべての課題を、インシデント、サービス要求、情報要求のいずれかに分類し、優先順位付けすることが可能になっている必要がある。サービスデスクとITサービスの質に対するエンドユーザの満足度を測定する。

**DS8.2 顧客からの問い合わせの登録**
問い合わせ、インシデント、サービス要求、情報要求を記録および追跡するための機能とシステムを確立する。このシステムは、インシデント管理、問題管理、変更管理、キャパシティ管理、および可用性管理といったプロセスと密接に連携する必要がある。インシデントはビジネスおよびサービスの優先度に基づいて分類し、該当する問題管理チームに転送する。顧客に対しては、それぞれの問い合わせへの対応状況を常に通知する。

**DS8.3 インシデントエスカレーション**
速やかに解決できないインシデントを、サービス・レベル・アグリーメント(SLA)で定められている制約の範囲内で適切にエスカレーションし、必要に応じてワークアラウンド(回避策)の提示を可能にする、サービスデスクの手続を確立する。インシデントの解決をどの IT グループが担当しているかにかかわらず、ユーザから報告されたインシデントの担当とライフサイクルのモニタリングは、確実にサービスデスクが担う。

**DS8.4 インシデントのクローズ**
顧客からの問い合わせへの対応終結ををタイムリーにモニタリングするための手続を確立する。インシデントの解決後、サービスデスクは根本原因が判明している場合はこの原因を記録し、実施された対応策に対して顧客の同意が得られていたことを確認する。

**DS8.5 傾向分析**
サービスデスクの活動に関する報告書を作成する。この報告書により、マネジメント層がサービスの成果と対応時間を測定して、傾向や再発性のある問題を特定できるようになり、サービスの継続的な改善が可能になる。

# マネジメントガイドライン

## DS8 サービスデスクとインシデントの管理

| From | インプット |
|---|---|
| AI4 | ユーザマニュアル、運用マニュアル、サポートマニュアル、技術マニュアル、および管理マニュアル |
| AI6 | 変更の承認 |
| AI7 | リリースされた構成管理アイテム |
| DS1 | サービス・レベル・アグリーメント(SLA)とオペレーショナル・レベル・アグリーメント(OLA) |
| DS4 | インシデント/災害のしきい値 |
| DS5 | セキュリティインシデントの定義 |
| DS9 | IT の構成/資産の詳細 |
| DS10 | 既知の問題、既知のエラー、およびワークアラウンド(回避策) |
| DS13 | インシデント情報 |

| アウトプット | To | | | | | | |
|---|---|---|---|---|---|---|---|
| サービス要求/変更要求 | AI6 | | | | | | |
| インシデント報告 | DS10 | | | | | | |
| プロセスの成果報告 | ME1 | | | | | | |
| ユーザ満足度の調査報告 | DS7 | ME1 | | | | | |

### RACI チャート

| アクティビティ / 担当 | CEO | CFO | 企業幹部 | CIO | ビジネスプロセスオーナ | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO (プロジェクト・マネジメント・オフィス) | コンプライアンス・監査・リスク・セキュリティ | サービスデスク/インシデント管理担当者 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 分類(重大度と影響力)およびエスカレーション(機能および階層)の手続の作成 | | | | C | C | C | C | C | C | | C | A/R |
| インシデント/サービス要求/情報要求の発見と記録 | | | | | | | | | | | | A/R |
| 問い合わせの分類、調査、および診断 | | | | I | | C | C | C | | | I | A/R |
| インシデントの解決、回復、およびクローズ | | | | | I | R | R | R | | | C | A/R |
| ユーザへの通知(最新の進行状況など) | | | | I | I | | | | | | | A/R |
| マネジメントレポートの作成 | I | | | I | I | I | | | I | | I | A/R |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R:Responsible) ②説明責任者(A:Accountable) ③協議先(C:Consulted)④報告先(I:Informed)

### 達成目標とその評価指標

**アクティビティの達成目標**
- サービスデスクの導入と運用
- 傾向のモニタリングと報告
- インシデント解決の優先順位とビジネス上の緊急課題との整合
- 明確なエスカレーション基準と手続の策定

**プロセスの達成目標**
- インシデントのタイムリーな分析、文書化、およびエスカレーション
- 問い合わせに対する正確かつタイムリーな対応
- インシデントと問い合わせの定期的な傾向分析の実施

**IT の達成目標**
- 提供サービスとサービスレベルに対するエンドユーザの満足の保証
- アプリケーションおよび技術的対応策の適切な利用と成果達成の保証
- 要求どおり IT サービスが使えることの保証

*促進*

*促進*

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- 自動化ツールを使用して報告および記録されたインシデント/サービス要求の割合
- サービスデスクスタッフ1名あたりの年間の研修日数
- サービスデスクスタッフ1名あたりの問い合わせ処理件数(1 時間あたり)
- ローカルサポート(フィールドサポートや担当者の現地訪問)を必要とするインシデントの割合
- 未解決の問い合わせ数

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- 総要求件数中、一次サポートでの解決割合
- 再調査を求められたインシデントの割合
- 放棄呼率
- 重大度別のインシデントの平均継続期間
- 電話および電子メール/Web での問い合わせに対する平均応答時間

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- 一次サポート(サービスデスクまたは知識ベース)に対するユーザの満足度
- 合意/容認された期間内に解決したインシデントの割合

# 成熟度モデル

## DS8 サービスデスクとインシデントの管理

**「エンドユーザからの問い合わせ、質問、およびインシデントを確実に解決および分析し、IT システムの効果的な利用を実現する。」という IT に対するビジネス要件を満たす上で、「サービスデスクとインシデントの管理」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
ユーザからの問い合わせや課題報告を解決するためのサポートがまったく実施されていない。インシデント管理プロセスがまったく存在しない。組織が、対処すべき課題の存在さえ認識していない。

**1 初期/その場対応**
ユーザからの問い合わせに対応し、インシデントの解決を管理するための、ツールと要員が割り当てられたプロセスが必要であることをマネジメント層が認識している。ただし、標準化されたプロセスがなく、事後的なサポートのみ行われている。マネジメント層はユーザからの問い合わせ、インシデント、およびそれらの傾向をモニタリングしていない。確実に問題を解決するためのエスカレーションプロセスが規定されていない。

**2 再現性はあるが直感的**
サービスデスクの機能とインシデント管理プロセスの必要性が、組織全体で認識されている。問題解決の支援は、知識豊富な個人のネットワークにより、非公式な形で行われている。彼らは、何らかの共通ツールを利用してインシデントの解決を支援している。標準手続に関する正式な研修や話し合いが行われておらず、実行責任は各個人に委ねられている。

**3 定められたプロセスがある**
サービスデスクの機能とインシデント管理プロセスの必要性が認識され、対応が検討されている。手続が標準化および文書化されており、非公式な研修が実施され始めている。ただし、研修の受講と標準の遵守は各個人の判断に委ねられている。FAQ(よくある質問)とユーザガイドラインが策定されているが、周知されていないため各人はこれらの情報を自ら入手しなければならず、また、これらを完全に守っていない。問い合わせやインシデントは手作業で追跡され、個別にモニタリングされているが、正式な報告システムは存在しない。問い合わせやインシデントに対する対応の迅速さについて測定されていないため、インシデントが未解決のままになる可能性がある。ユーザに対し、問題とインシデントの報告先と報告方法が明確に周知されている。

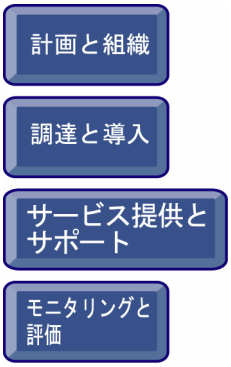
**4 管理され、測定可能である**
組織内のすべてのレベルでインシデント管理プロセスの効果が十分に理解されており、サービスデスクが適切な組織単位に設置されている。ツールと手法が、一元管理された知識ベースを活用して自動化されている。サービスデスクのスタッフと問題管理担当のスタッフが緊密に連携している。実行責任が明確化されており、有効性がモニタリングされている。インシデントの伝達、エスカレーション、および解決の手続が確立され、周知されている。サービスデスク要員は教育を受けており、業務に特化したソフトウェアを活用することでプロセスが改善されている。マネジメント層が、サービスデスクの成果測定のための KPI と KGI を策定している。

**5 最適化**
インシデント管理プロセスとサービスデスクが確立されており、適切に構成されている。十分な知識を備え、顧客を中心に考え、役立つサービスを提供することで、顧客サービス指向を実現している。KPI と KGI が体系的に測定および報告される。広範で包括的な FAQ が、知識ベースに欠くことのできない重要な要素となっている。ユーザがインシデントを自ら診断して解決するためのツールが用意されている。助言に一貫性があり、インシデントは体系的なエスカレーションプロセスにより迅速に解決される。マネジメント層が、インシデント管理プロセスとサービスデスクの成果統計を取得するための統合ツールを活用している。プロセスは、KPI と KGI の分析、継続的な改善、外部組織とのベンチマーク評価の結果を基に、業界のベストプラクティスのレベルにまで最適化されている。

# コントロール目標 －概要－

## DS9 構成管理

ハードウェアとソフトウェアの構成のインテグリティを確保するには、正確かつ網羅された構成管理用リポジトリの作成と保守が必要である。このプロセスには、初期構成情報の収集、ベースラインの設定、構成情報の検証と監査、および必要に応じた構成管理用リポジトリの更新が含まれる。効果的な構成管理により、システムの可用性が向上し、作業上の課題が最小限に抑えられ、課題を速やかに解決できるようになる。


**IT プロセス: 構成管理のコントロール目標は、**

IT インフラストラクチャ、資源、および能力を最適化し、IT 資産の詳細を把握することを、**ビジネス要件**とし、

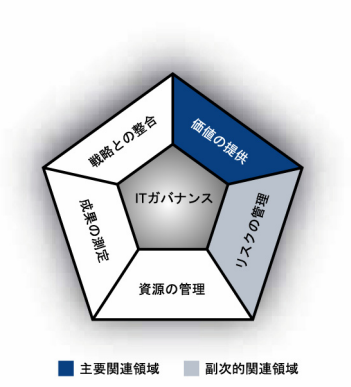
**重点をおくべきコントロールは、**資産構成の属性およびベースラインの正確かつ完全なリポジトリを作成および保守し、実際の資産構成と比較することである。

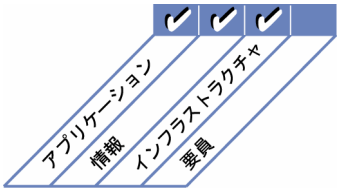
**実現するための手段は、次の 3 項目である。**

- すべての構成管理アイテムを含む集中管理リポジトリの作成
- 構成管理アイテムの識別と保守
- 構成データのインテグリティのレビュー

**その成果の測定指標は、次の 3 項目である。**

- 不適切な資産構成に起因するビジネス上のコンプライアンスに関する問題の数
- 構成管理用リポジトリと実際の資産構成の間で確認された相違の数
- リポジトリ内の、購入済みライセンスと所在不明ライセンスの割合



# コントロール目標 －詳細－

## DS9 構成管理

**DS9.1 構成リポジトリとベースライン**
構成管理アイテムの関連情報をすべて含む集中管理リポジトリを作成する。このリポジトリには、システムやサービスを運用、アクセス、および利用するためのハードウェア、アプリケーションソフトウェア、ミドルウェア、パラメータ、文書、手続、およびツールが含まれる。考慮すべき関連情報は命名規則、バージョン番号、およびライセンスの詳細である。すべてのシステムとサービスにおいて、構成管理アイテムのベースラインを、変更後、何らかの理由で元に戻す際のチェックポイントとして設定すべきである。

**DS9.2 構成管理アイテムの識別と保守**
次の手続を整備する。
- 構成管理アイテムとその属性の識別
- 新規/修正/削除済み構成管理アイテムの記録
- 構成管理用リポジトリにおける構成管理アイテム間のリレーションシップの識別と保守
- 現存する構成管理アイテムの構成管理用リポジトリへの追加更新
- 許可されていないソフトウェアの導入防止

これらの手続では、構成管理用リポジトリに対するすべての操作が適切に認可および記録されなければならない。また、これらの手続は変更管理および問題管理手続と適切に統合されていなければならない。

**DS9.3 構成のインテグリティのレビュー**
定期的に、必要に応じて適切なツールを用いて構成管理アイテムの状況をレビューおよび検証し、現在および過去の構成データが完全であることを確認して、実際の状況と比較する。個人所有やライセンスのないソフトウェア、あるいは契約済ライセンス数を超えたソフトウェアが存在していないかどうかを、ソフトウェア使用ポリシーに照らし合わせて定期的にレビューする。不備や逸脱がある場合は報告、対処および修正されなければならない。

# マネジメントガイドライン

## DS9 構成管理

| From | インプット |
|---|---|
| AI4 | ユーザマニュアル、運用マニュアル、サポートマニュアル、技術マニュアル、および管理マニュアル |
| AI7 | リリースされた構成管理アイテム |
| DS4 | IT 構成管理アイテムの重大度 |

| アウトプット | To | | | | | | |
|---|---|---|---|---|---|---|---|
| IT の構成/資産の詳細 | DS8 | DS10 | DS13 | | | | |
| 変更の適用対象とその方法 | AI6 | | | | | | |
| プロセスの成果報告 | ME1 | | | | | | |

### RACI チャート

| アクティビティ / 担当 | CEO | CFO | 企業幹部 | CIO | ビジネスプロセスオーナ | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO（プロジェクト・マネジメント・オフィス） | コンプライアンス・監査・リスク・セキュリティ | 構成管理担当者 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 構成管理の計画策定手続の作成 | | | | | C | A | C | I | C | | C | R |
| 初期構成情報の収集とベースラインの確立 | | | | | | C | C | C | | | I | A/R |
| 構成情報の検証と監査(未承認ソフトウェアの発見を含む) | | I | | | | A | | | I | | I | A/R |
| 構成管理用リポジトリの更新 | | | | | | R | R | R | | | I | A/R |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

### 達成目標とその評価指標

**アクティビティの達成目標**
- すべての構成管理アイテムを含む集中管理リポジトリの作成
- 構成管理アイテムの識別と構成データの保守
- 構成データのインテグリティのレビュー

*促進*

**プロセスの達成目標**
- すべての資産、構成属性およびベースラインを含むリポジトリの作成
- 構成管理用リポジトリのインテグリティを保持
- 実際の資産構成がリポジトリのベースラインに準拠しているかどうかのレビュー

*促進*

**IT の達成目標**
- IT インフラストラクチャ、資源、および能力の最適化
- すべての IT 資産の所在明確化と保護

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- 相違の特定から修正までに要する平均時間
- 不完全または失われた構成情報による相違の数
- 成果、セキュリティ、および可用性のサービスレベルに合致する構成管理アイテムの割合

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- 構成管理用リポジトリと実際の資産構成の間で確認された相違の数
- リポジトリ内の、購入済みライセンスと所在不明ライセンスの割合

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- 不適切な資産構成に起因するビジネス上のコンプライアンスに関する問題の数

# 成熟度モデル

## DS9 構成管理

**「IT インフラストラクチャ、資源、および能力を最適化し、IT 資産の詳細を把握する。」という IT に対するビジネス要件を満たす上で、「構成管理」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
マネジメント層は、IT インフラストラクチャ(ハードウェアやソフトウェアの構成)に関する報告および管理のプロセスを整備する利点について、正しく認識していない。

**1 初期/その場対応**
構成管理の必要性が認識されている。基本的な構成管理作業(ハードウェアとソフトウェアのインベントリーなど)が、各担当者の裁量に応じて実施されている。標準の実施基準が定められていない。

**2 再現性はあるが直感的**
マネジメント層が、IT 構成をコントロールする必要性を認識しており、構成情報を正確かつ網羅された状態で維持することの利点を理解しているが、技術要員の知識と力量に暗黙裡に依存している。構成管理ツールがある程度利用されているが、プラットフォーム間で異なる。また、標準の作業の実践基準が定められていない。構成データの内容が限定的であり、相互に関連するプロセス(変更管理と問題管理など)で使用されていない。

**3 定められたプロセスがある**
手続と作業の実践基準が文書化、標準化、および周知されている。ただし、研修への参加と標準の適用は個人の判断に委ねられている。プラットフォーム間を跨いで、同種の構成管理ツールが導入されつつある。手続からの逸脱が発見される可能性は低く、物理的な検証が一貫性のない方法で実施されている。装置とソフトウェアの変更に関する追跡の自動化がある程度は進められている。構成データは、相互に関連する複数のプロセスで使用されている。

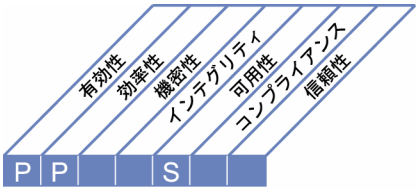
**4 管理され、測定可能である**
構成管理の必要性が組織内のすべてのレベルで認識されており、優れた実践基準の継続的な改善が図られている。手続と標準が周知され、研修に組み込まれている。逸脱についてモニタリング、追跡、および報告されている。自動化ツール(プッシュ技術など：ブロードキャストされる情報をクライアント側で解釈、表示する技術の総称)が標準の施行と安定性の向上に活用されている。構成管理システムはほとんどの IT 資産に対応しており、適切なリリース管理と配付コントロールを可能にしている。物理的検証に加え、例外分析が一貫して実施されており、例外の根本原因が調査されている。

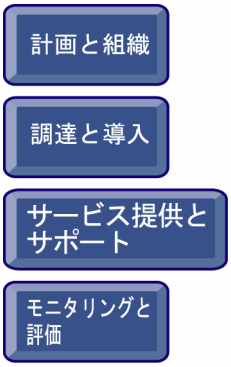
**5 最適化**
すべての IT 資産が、統合された構成管理システム内で管理されている。このシステムには、構成要素、構成要素間の相互関係、およびイベントに関するすべての必要情報が組み込まれている。構成データとベンダーカタログの整合性が取られている。相互に関連する複数のプロセスが完全に統合されている。これらのプロセスにおいては、構成データが自動化された手法で使用および更新される。ベースラインに関する監査レポートには、各装置の修理、保守、保証、アップグレード、および技術評価に必要不可欠な、ハードウェア/ソフトウェアに関するデータが記載されている。許可されていないソフトウェアのインストールを制限する規則が徹底して施行されている。マネジメント層は、アップグレード計画と技術更新能力に関する情報を含む分析報告から、修理とアップグレード実施の見通しを立てている。資産について追跡し、個々の IT 資産をモニタリングすることで、これらの資産を保護し、盗難、誤用、悪用を未然に防止している。

# コントロール目標 －概要－

## DS10 問題管理

効果的な問題管理を実施するには、問題を特定および分類し、根本原因を分析し、問題を解決する必要がある。問題管理プロセスには、改善のための提案事項の特定、問題の記録保持、および是正措置の状況のレビューも含まれる。効果的な問題管理プロセスにより、サービスレベルの向上、費用削減、および顧客(カスタマー)の利便性と満足度の向上を実現できる。




**IT プロセス: 問題管理のコントロール目標は、**

提供サービスとサービスレベルに対するエンドユーザの満足を確保し、対応策とサービスの提供における不備と手直し(リワーク)の必要性を削減することを、**ビジネス要件**とし、

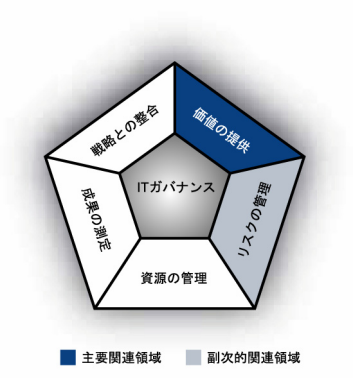
**重点をおくべきコントロールは、**運用上の問題の記録、追跡、および解決、すべての重大な問題の根本原因の調査、および特定された運用上の問題の解決策の策定することである。

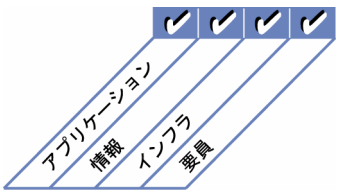
**実現するための手段は、次の 3 項目である。**

- 報告された問題に関する根本原因分析の実施
- 傾向の分析
- 問題の引受(オーナシップ)と解決の促進

**その成果の測定指標は、次の 3 項目である。**

- ビジネスに影響を及ぼす問題の再発数
- 要求された期間内に解決した問題の割合
- 継続中の問題に対して、重大度を基にした報告または更新の頻度



# コントロール目標 －詳細－

## DS10 問題管理

### DS10.1 問題の特定と分類
インシデント管理の過程で特定された問題を報告、分類するためのプロセスを導入する。問題分類の手続はインシデント分類の手続に類似しており、カテゴリ、影響度、緊急度、優先度の決定が含まれる。問題は関連グループまたはドメイン(ハードウェア、ソフトウェア、サポートソフトウェアなど)に適切に分類しなければならない。これらのグループを、組織上の責任やユーザー/顧客ベースに合わせ、さらにサポートスタッフへの問題割り当ての基礎とする。

### DS10.2 問題の追跡と解決
問題管理システムは、報告されたすべての問題を追跡、分析し、その根本原因を判別するための、適切な監査証跡機能を次の情報に対して提供する必要がある。
- 関連するすべての構成管理アイテム
- 未解決の問題とインシデント
- 既知のエラーとエラーの疑い

根本原因に対処する維持できる解決策を特定して実施し、確立されている変更管理プロセスに従い変更要求を提出する。解決プロセス全体にわたって、問題管理は、変更管理から問題やエラーの解決状況に関する報告を定期的に受ける必要がある。問題管理は、問題および既知のエラーのユーザサービスに対する継続的な影響をモニタリングする。この影響が深刻化した場合は、問題管理はその問題を適切な会議体にエスカレーションして、変更要求(RFC)の優先順位を上げてもらうか、または必要に応じて緊急の変更措置を実施する。問題解決の進捗状況は、サービス・レベル・アグリーメント(SLA)に照らし合わせてモニタリングする必要がある。

### DS10.3 問題のクローズ
既知のエラーを成功裡に取除いたことを確認した後、または別の方法で問題を処理することをビジネス部門と合意した後、その問題の記録をクローズするための手続を整備、運用する。

### DS10.4 変更管理、構成管理、および問題管理の統合
問題とインシデントの効果的な管理を保証するため、関連する変更管理、構成管理、および問題管理のプロセスを統合する。ビジネス上の改善よりも、問題の火消し作業に用いた作業量をモニタリングし、必要に応じて、問題を最小限に抑えるためにこれらのプロセスを改善する。

# マネジメントガイドライン

## DS10 問題管理

| From | インプット |
|---|---|
| AI6 | 変更の承認 |
| DS8 | インシデント報告 |
| DS9 | IT の構成/資産の詳細 |
| DS13 | エラーログ |

| アウトプット | To |
|---|---|
| 変更要求 | AI6 |
| 問題の記録 | AI6 |
| プロセスの成果報告 | ME1 |
| 既知の問題、既知のエラー、ワークアラウンド(回避策) | DS8 |

### RACI チャート

| アクティビティ / 担当 | CEO | CFO | 企業幹部 | CIO | ビジネスプロセスオーナ | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO (プロジェクト・マネジメント・オフィス) | コンプライアンス・監査・リスク・セキュリティ | 問題管理担当者 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 問題の特定と分類 | | | I | I | C | A | C | C | | | I | R |
| 根本原因の分析の実施 | | | | | | C | | C | | | | A/R |
| 問題の解決 | | | | | C | A | R | R | | R | C | C |
| 問題の状況の確認 | | | I | I | C | A/R | C | C | | C | C | R |
| 改善のための提案事項の提示と関連する変更要求の作成 | | | | | I | A | I | I | | I | | R |
| 問題の記録保持 | | | | | I | I | | I | | | I | A/R |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

### 達成目標とその評価指標

**アクティビティの達成目標**
- 問題管理担当者への十分な権限の付与
- 報告された問題に関する根本原因分析の実施
- 傾向の分析
- 問題とその解決工程の管理

*促進*

**プロセスの達成目標**
- 運用上の問題の解決までの記録と追跡
- すべての重大な問題の根本原因の調査
- 特定された運用上の問題の解決策の策定

*促進*

**IT の達成目標**
- 提供サービスとサービスレベルに対するエンドユーザの満足の確保
- 対応策とサービスの提供における不備と手直し(リワーク)の必要性の削減
- IT 目標の達成の保証

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- 問題の記録から根本原因の特定までに要した平均時間
- 根本原因の分析が実施された問題の割合
- 問題の重大度に基づく、未解決の問題に関する報告または更新の頻度

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- 記録および追跡された問題の割合
- 重大度別の(特定の期間内に)再発した問題の割合
- 要求された期間内に解決した問題の割合
- 重大度別の未解決/新規/解決済み問題の数
- 問題の特定から解決までに要した時間の平均と標準偏差
- 問題の解決からクローズまでに要した時間の平均と標準偏差

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- ビジネスに影響を及ぼす、繰り返し発生する問題の数
- 運用上の問題に起因する業務中断回数

# 成熟度モデル

## DS10 問題管理

**「提供サービスとサービスレベルに対するエンドユーザの満足を確保し、対応策とサービスの提供における不備と手直し(リワーク)の必要性を削減する。」というITに対するビジネス要件を満たす上で、「問題管理」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
問題とインシデントが区別されていないため、問題を管理する必要性が認識されていない。したがって、インシデントの根本原因の特定も行われていない。

**1 初期/その場対応**
問題を管理し、その根本にある原因を解決する必要性が、個人レベルで認識されている。知識豊富なキーとなるスタッフが、各々の専門分野に関連する問題について何らかの支援を行っているが、問題管理の実行責任は割り当てられていない。情報が共有されていないため、解決策を模索している間に新たな問題が発生し、生産性が失われる。

**2 再現性はあるが直感的**
IT 関連の問題をビジネス部門と情報サービス部門の両方で管理する必要性と効果について、広く認識されている。解決プロセスは、数名の主要なスタッフが問題の特定と解決の実行責任を担う、というレベルに達している。スタッフ間の情報共有は、非公式かつ事後的な方法で行われている。問題管理担当者が利用できる知識が十分に体系化されていないため、ユーザへのサービスレベルにばらつきや阻害が生じる。

**3 定められたプロセスがある**
効果的かつ統合された問題管理システムの必要性がマネジメント層の支援により受け入れられ、明らかにされている。人員補充および研修のための予算が確保されている。問題解決とエスカレーションのプロセスが標準化されている。問題とその解決策の記録と追跡は、一元管理されていない任意のツールを用いて、対応チーム内で断片的に行われている。問題管理の基準や標準は確立されているが、そこからの逸脱行為は、検知されない可能性がある。スタッフ間の情報共有は、正式かつ事前に行われている。マネジメント層によるインシデントのレビューや、問題特定および解決の分析は、限定的かつ非公式に行われている。

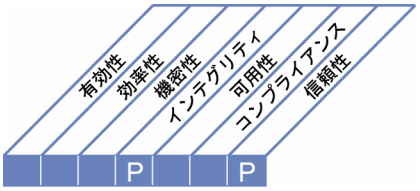
**4 管理され、測定可能である**
組織内のすべてのレベルで問題管理プロセスが理解されている。実行責任とオーナシップが明確に割り当てられている。手法や手続は文書化され、周知されており、その有効性が測定されている。問題の大半が特定、記録、報告されており、解決策が実施されている。この仕組みが価値ある資産として見なされ、IT 目標の達成と IT サービスの改善に大きく寄与するものとして捉えられているので、その知識とノウハウが培われ、維持され、より高められている。問題管理は、インシデント管理、変更管理、可用性管理、構成管理などの相互に関連するプロセスと適切に統合されており、データ管理、施設管理、および運用管理の面で顧客の支援につながっている。問題管理プロセスにおける KPI と KGI について合意が得られている。

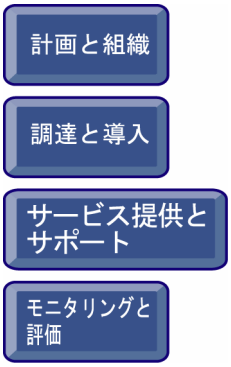
**5 最適化**
問題管理プロセスは、先見的で未然防止が可能なレベルにまで発展しており、IT 目標の達成に貢献している。問題が予期され、未然に防止されている。定期的にベンダーや専門家と連絡を取り合うことで、過去発生した問題や将来予想される問題のパターンに関する知識が維持されている。問題と解決策の記録、報告、および分析が自動化されており、構成データ管理と十分に統合されている。KPI と KGI が一貫して測定されている。大半のシステムは自動検知および警告メカニズムを備えており、継続的に追跡および評価されている。問題管理プロセスは、KPI と KGI の分析に基づいて、継続的な改善を目指して分析されており、利害関係者への報告が行われている。

# コントロール目標 －概要－

## DS11 データ管理

効果的なデータ管理を実施するには、データ要件を特定する必要がある。データ管理プロセスには、メディアライブラリ、データのバックアップと復元、およびメディアの適切な廃棄に関する管理手続の確立も含まれる。効果的なデータ管理は、ビジネスデータの質、適時性、および可用性の保証に有用である。




**IT プロセス: データ管理のコントロール目標は、**

情報の利用を最適化し、要求に応じた情報の可用性を保証することを、**ビジネス要件**とし、

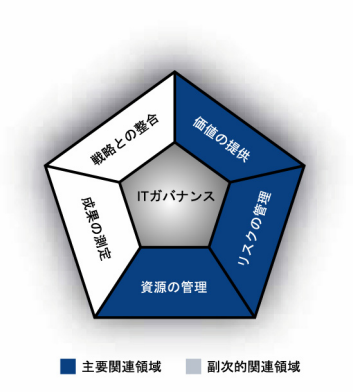
**重点をおくべきコントロールは、**データのインテグリティ、正確性、可用性、および保護を維持することである。

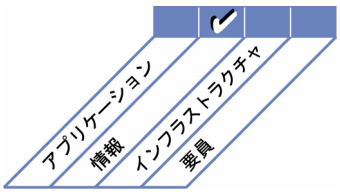
**実現するための手段は、次の 3 項目である。**

- データのバックアップと復元のテスト
- オンサイトおよび遠隔地におけるデータ保管の管理
- データおよび機器の安全な廃棄

**その成果の測定指標は、次の 3 項目である。**

- データの可用性に対するユーザの満足度
- 成功したデータ復元の割合
- メディア廃棄後に機密データが取得されたインシデントの件数



# コントロール目標 －詳細－

## DS11 データ管理

**DS11.1 データ管理におけるビジネス要件**
ビジネス部門から予定された原始帳票が受領され、ビジネス部門から受領したすべてのデータが処理され、ビジネス部門が必要とするアウトプットがすべて準備および提供され、必要とされる再開と再処理に対応される。これらのことを保証する手配をする。

**DS11.2 データの保管および保持の調整**
データの保管とアーカイブの手続を定義および導入し、データがアクセス可能および利用可能である状態を確保する。保管とアーカイブの手続では、データの取り出しに関する要件、費用効率、および継続的なインテグリティとセキュリティ上の要件を考慮する必要がある。暗号化と認証に使用されるデータ(暗号鍵、証明書)と同様に、文書、データ、アーカイブ、プログラム、報告書、およびメッセージ(受信/送信)に関する法令要件とビジネス要件を満たすため、保管および保持に関する手配を行う。

**DS11.3 メディアライブラリ管理システム**
オンサイトメディアの一覧を保守し、メディアの有用性とインテグリティを確保するための手続を定義および導入する。これらの手続には、指摘されたどんな相違に対しても、タイムリーなレビューとフォローアップのための手続を規定する必要がある。

**DS11.4 廃棄**
機器またはメディアを廃棄または別の用途とする場合に、このような機器やメディアに保存されている機密データやソフトウェアへのアクセスを防止するための手続を定義および導入する。このような手続により、削除または廃棄として識別されたデータへのアクセスが不可能であることを保証する必要がある。

**DS11.5 バックアップと復元**
ビジネス要件および継続計画に沿った、システム、データ、および文書のバックアップと復元の手続を策定および導入する。バックアップ手続に対するコンプライアンスについて検証し、完全な復元が可能かどうか、および復元に要する時間を検証する。バックアップメディアと復元プロセスをテストする。

**DS11.6 データ管理におけるセキュリティ上の要件**
データおよび機密メッセージの受信、処理、物理的保管、および出力に関連するセキュリティ要件を特定し、それを適用するための手配を行う。これには、物理的記録、データ伝送、および遠隔地で保管されているすべてのデータが含まれる。

# マネジメントガイドライン

## DS11 データ管理

| From | インプット |
|---|---|
| PO2 | データディクショナリ、採用したデータの分類方法 |
| AI4 | ユーザ、運用、サポート、技術、および管理の各マニュアル |
| DS1 | オペレーショナル・レベル・アグリーメント(OLA) |
| DS4 | バックアップの保管と保護に関する計画 |

| アウトプット | To |
|---|---|
| プロセスの成果報告 | ME1 |
| データ管理に関するオペレータ向け指示書 | DS13 |

### RACI チャート

担当

| アクティビティ | CEO | CFO | 企業幹部 | CIO | ビジネスプロセスオーナ | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO（プロジェクト・マネジメント・オフィス） | コンプライアンス・監査・リスク・セキュリティ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| データの保管および保持に関する要件を取り入れた手続の定義 | | | | A | I | C | R | | | | C |
| メディアライブラリの管理手続の定義、維持、および導入 | | | | A | | R | C | C | I | | C |
| メディアと機器の安全な廃棄手続の定義、保守、および導入 | | | | A | C | R | | | I | | C |
| 計画に基づくデータのバックアップ | | | | A | | R | | | | | |
| データ復元のための手続の定義、維持、および導入 | | | | A | C | R | C | C | | | I |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

### 達成目標とその評価指標

**アクティビティの達成目標**
- データのバックアップと復元のテスト
- オンサイトおよび遠隔地におけるデータ保管の管理
- データおよび機器の安全な廃棄

*促進*

**プロセスの達成目標**
- 保管データのインテグリティ、正確性、有効性、および可用性の維持
- メディア廃棄時のデータのセキュリティ確保
- 保管メディアの効果的な管理

*促進*

**IT の達成目標**
- 情報利用の最適化
- 重要かつ機密の情報が、当該情報へのアクセスを許可されていないユーザに開示されないようにすること
- IT の法令へのコンプライアンスの確保

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- バックアップメディアのテスト実施頻度
- データ復元に要する平均時間

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- 成功したデータ復元の割合
- メディア廃棄後に機密データが読み取られたインシデントの件数
- 記憶装置の容量不足に起因するダウンタイムの発生件数またはデータのインテグリティに関するインシデントの件数

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- ビジネスプロセスにとって重要なデータを復元できない状況の発生回数
- データ可用性に対するユーザの満足度
- 保管管理の問題に起因する法規制違反のインシデント件数

# 成熟度モデル

## DS11 データ管理

**「情報の利用を最適化し、要求に応じた情報の可用性を保証する。」という IT に対するビジネス要件を満たす上で、「データ管理」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
データが企業の資源および資産であるとは認識されていない。データのオーナシップが割り当てられていないか、データ管理の説明責任者が存在しない。データの品質およびセキュリティレベルが非常に低いか、またはまったく確保されていない。

**1 初期/その場対応**
組織が、適切なデータ管理の必要性を認識している。データ管理に関するセキュリティ要件は、その場に応じて具体的なアプローチがとられており、正式な周知手続が整備されていない。データ管理に関する具体的な研修が実施されていない。データ管理に関する責任の所在が明確でない。バックアップ/復元手続と廃棄方法については整備されている。

**2 再現性はあるが直感的**
適切なデータ管理の必要性が組織全体で認識されている。上位層におけるデータのオーナシップの割り当てが行われるようになってきている。主要な人員によってデータ管理におけるセキュリティ要件が文書化されている。IT 部門内で、データ管理の主要な活動(バックアップ、復元、廃棄)に対してある程度のモニタリングが実施されている。データ管理の実行責任が、主要な IT スタッフに非公式に割り当てられている。

**3 定められたプロセスがある**
IT 部門内および組織全体でのデータ管理の必要性が理解され、受け入れられている。データ管理の実行責任が規定されている。責任のあるグループに対してデータのオーナシップが割り当てられており、インテグリティとセキュリティはこの責任のあるグループによりコントロールされる。IT 部門内でデータ管理手続が正式に決められており、機器のバックアップ/復元および廃棄のための何らかのツールが利用されている。データ管理に対してある程度のモニタリング体制が整備されている。基本的な成果達成指標が策定されている。データ管理スタッフの研修が整備されつつある。

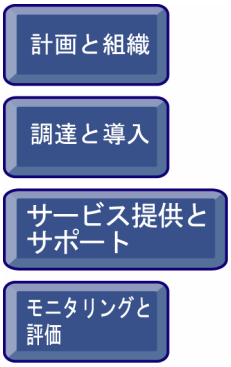
**4 管理され、測定可能である**
データ管理の必要性が組織内で理解され、必要な対応を取ることが受け入れられている。データのオーナシップと管理の責任が組織内で明確に定義され、割り当てられており、周知されている。手続が正式に決められて広く認識されており、知識が共有されている。現存するツールが利用されるようになってきている。達成目標および成果達成指標は、顧客との合意が得られており、適切に定義されたプロセスを通してモニタリングされている。データ管理スタッフのための正式な研修が実施されている。

**5 最適化**
データ管理と必要な対応すべてに関する理解の必要性について、組織内で理解され、受け入れられている。将来的なニーズと要件について事前に調査されている。データのオーナシップと管理の責任が明確に規定され、組織全体で周知され、タイムリーに更新されている。手続が正式に決められ、広く認識されており、知識の共有が標準の実践基準として実施されている。高度なツールが使用され、データ管理が最大限に自動化されている。達成目標および成果達成指標は、顧客との合意が得られており、ビジネス目標と関連付けられており、適切に定義されたプロセスを通して一貫してモニタリングされている。常に改善の検討が行われている。データ管理スタッフへの研修が仕組みとして定着している。

# コントロール目標 －概要－

## DS12 物理的環境の管理

コンピュータ機器と要員を保護するには、適切に設計および管理されている物理的施設が必要である。物理的環境を管理するプロセスには、物理的なサイト要件の定義、適切な施設の選定、および環境要因をモニタリングし物理的アクセスを管理するための効果的なプロセスの設計が含まれる。物理的環境を効果的に管理することで、コンピュータ機器と要員にかかわる障害に起因するビジネスの中断が減少する。


**IT プロセス: 物理的環境の管理のコントロール目標は、**

コンピュータ資産とビジネスデータを保護し、ビジネス中断のリスクを最小限に抑えることを、**ビジネス要件**とし、

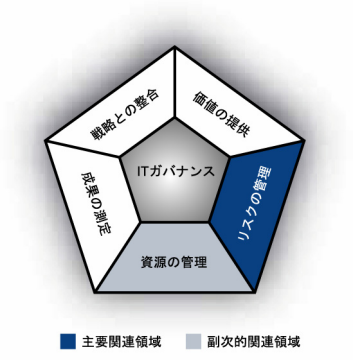
**重点をおくべきコントロールは、**IT 資産を、不正アクセス、損傷、盗難から保護する適切な物理的環境の導入および維持することである。

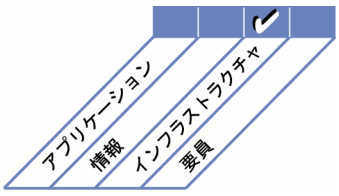
**実現するための手段は、次の 2 項目である。**

- 物理的なセキュリティ対策の実施
- 施設の選定と管理

**その成果の測定指標は、次の 3 項目である。**

- 物理的環境にかかわるインシデントに起因するダウンタイム
- 物理的なセキュリティ侵害または障害に起因するインシデントの件数
- 物理的リスクの評価とレビューの実施頻度



# コントロール目標 －詳細－

## DS12 物理的環境の管理

### DS12.1 サイトの選定と配置
ビジネス戦略に関連付けられた技術戦略を支援する IT 機器のための物理的サイトを定義および選定する。サイトの選定と配置設計では、関連法令(労働安全衛生に関する規制など)を考慮する一方で、自然災害/人的災害に関連するリスクを考慮する必要がある。

### DS12.2 物理的なセキュリティ対策
ビジネス要件に従って物理的セキュリティ対策を策定および導入する。物理的セキュリティ対策には、セキュリティ境界線、セキュリティゾーン、重要機器の配置、および受け渡しエリアの設定などが含まれるが、これだけに限定されるものではない。特に、重要な IT 業務が運用されていることを目立たないようにする必要がある。モニタリングの責任と、物理的セキュリティに関するインシデントの報告および解決のための手続を定める必要がある。

### DS12.3 物理的アクセス
ビジネス上の必要性に基づき、緊急事態発生時を含めた施設、建物、敷地への立ち入りの許可、制限、取り消し手続を定義および導入する。施設、建物、敷地への立ち入りに際しては、正当性の評価、認可、記録、およびモニタリングを行う必要がある。これは、施設に立ち入るすべての人員(スタッフ、臨時スタッフ、取引先、ベンダー、訪問客、およびその他のサードパーティ全員)に適用される。

### DS12.4 環境的要因からの保護
環境的要因から保護するための対策を確立および導入する。環境をモニタリングおよびコントロールするための特別な設備やデバイスを導入する必要がある。

### DS12.5 物理的施設の管理
法律、規制、技術要件、ビジネス要件、ベンダーの仕様、および安全衛生ガイドラインに従って、電源装置や通信機器などの設備を管理する。

# マネジメントガイドライン

## DS12 物理的環境の管理

| From | インプット |
|---|---|
| PO2 | 採用したデータの分類方法 |
| PO9 | リスク評価 |
| AI3 | 物理的環境要件 |

| アウトプット | To |
|---|---|
| プロセスの成果報告 | ME1 |

### RACI チャート

| アクティビティ | CEO | CFO | 企業幹部 | CIO | ビジネスプロセスオーナ | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO（プロジェクト・マネジメント・オフィス） | コンプライアンス・監査・リスク・セキュリティ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 要求される物理的保護レベルの定義 | | | | | C | A/R | C | | | | C |
| サイト(データセンター、オフィスなど)の選定と委託 | I | C | C | C | C | A/R | C | | C | C | C |
| 物理的環境に関する対策の実施 | | | | | I | A/R | I | I | | | C |
| 物理的環境の管理(保守、モニタリング、報告を含む) | | | | | | A/R | C | | | | |
| 物理的アクセスを許可および維持する手続の定義および導入 | | | | C | I | A/R | I | I | I | | C |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

### 達成目標とその評価指標

**アクティビティの達成目標**
- 物理的セキュリティ対策の導入
- 施設の厳密な選定と管理

*促進*

**プロセスの達成目標**
- IT インフラストラクチャおよび資源に適した物理的環境の整備と保守
- アクセス不要な人員の物理的環境へのアクセス制限

*促進*

**IT の達成目標**
- エラー、意図的な攻撃、または災害で生じた障害に対する、IT サービスおよびインフラストラクチャの抵抗力・回復力の保証
- 重要かつ機密度の高い情報が、当該情報へのアクセスを許可されていないユーザに開示されないことを保証
- IT サービスの中断または変更が及ぼすビジネスへの影響の極小化を保証
- すべての IT 資産の責任の所在の明確化と適切な保護

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- 担当要員に対して安全性、セキュリティ、および施設に関する対策についての研修を実施する頻度
- 安全性、セキュリティ、および施設に関する対策についての研修を受けた担当要員の割合
- 前年のリスク低減テストの実施回数
- 物理的リスクの評価とレビューの実施頻度

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- 物理的なセキュリティ侵害または障害に起因するインシデントの件数
- コンピュータ施設への不正アクセスインシデントの件数

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- 物理的環境に関するインシデントに起因するダウンタイム
- 物理的環境に起因する損害発生件数
- 物理的環境に関するインシデントに起因するセキュリティ障害

# 成熟度モデル

## DS12 物理的環境の管理

**「コンピュータ資産とビジネスデータを保護し、ビジネス中断のリスクを最小限に抑える。」というITに対するビジネス要件を満たす上で、「物理的環境の管理」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
施設の保護またはコンピュータ資源への投資を保護する必要性が認識されていない。防火、粉じん、電力供給、高温多湿などの環境的要因について、モニタリングもコントロールも実施されていない。

**1 初期/その場対応**
組織が、人災や自然災害から資源や要員を保護する適切な物理的環境の整備に関するビジネス上の要件について認識している。施設と機器の管理について、主要な人員のスキルと能力に依存している。スタッフは制限なく施設内を移動できる。マネジメント層が、施設環境のコントロール状況とスタッフの移動についてモニタリングしていない。

**2 再現性はあるが直感的**
運用担当者により、環境のコントロールが導入およびモニタリングされている。物理的セキュリティの確保は非公式なプロセスであり、物理的施設のセキュリティについて高い意識を持つ少数の従業員により実施されている。施設保守手続が十分に文書化されておらず、数名の人員による優れた実践方法に依存している。物理的セキュリティの達成目標が正式な標準に基づいておらず、マネジメント層はセキュリティ目標の達成を保証できない。

**3 定められたプロセスがある**
コンピュータ環境のコントロールを維持する必要性が組織内で理解され、対応が検討されている。環境のコントロール、予防的保守、および物理的セキュリティは、予算項目としてマネジメント層により承認されており、マネジメント層により追跡される。アクセス制限が適用されており、許可された要員のみがコンピュータ関連施設にアクセスできる状態になっている。訪問者については、記録が残され、個別にスタッフが同行する。物理的施設は目立たず、容易に特定できないようになっている。安全衛生関連の規制の遵守状況が所轄機関によりモニタリングされている。安全衛生上のリスクに対して保険をかけているが、保険関連費用を低減させるための努力は最小限にとどまっている。

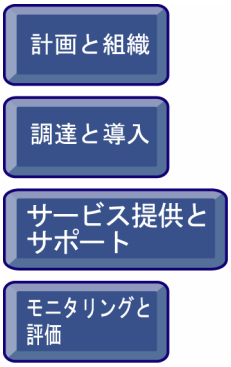
**4 管理され、測定可能である**
コンピュータ環境のコントロールを維持する必要性が十分に理解されており、組織構造や予算配分にも明確に反映されている。環境的セキュリティおよび物理的セキュリティの要件が文書化されており、施設へのアクセスが厳しくコントロールおよびモニタリングされている。責任とオーナシップが定められており、周知されている。施設担当スタッフが、緊急事態発生時の対応および安全衛生に関わる実践基準について十分な教育を受けている。施設へのアクセスを制限し、環境的要因および安全要因に対応するための標準化されたコントロール方法が整備されている。マネジメント層は、コントロールの有効性と確立された標準への準拠状況をモニタリングしている。マネジメント層は、コンピュータ環境の管理の成果を測定するための KPI と KGI を策定している。コンピュータ資源の復元可能性が組織のリスク管理プロセスに組み込まれている。統合された情報を利用して、保険の対象とする範囲および関連費用が最適化されている。

**5 最適化**
組織のコンピュータ環境の維持に必要な施設に関して合意された長期計画が存在する。すべての施設について標準が定められている。この標準では、サイトの選定、施設構造、防護、人的安全保護、機械系統、電気系統、環境要因(火災、落雷、洪水など)に対する保護が扱われている。すべての施設の一覧が作成され、組織の現行のリスク管理プロセスに従い分類されている。業務上の必要性に応じて施設へのアクセスが厳しくコントロールされ、継続的にモニタリングされている。また、訪問者が立ち入る際は、必ずスタッフが同行する。専用の装置によって環境がモニタリングおよびコントロールされており、この装置が設置されている部屋は「無人」になっている。KPI と KGI が一貫して測定されている。予防的保守プログラムによりスケジュールが遵守され、機密機器に対して定期的なテストが実施されている。施設に関する戦略と標準は、IT サービスの可用性の達成目標と整合されており、業務継続計画および危機管理と統合されている。マネジメント層は、KPI と KGI を用いて施設のレビューと最適化を継続的に実施しており、ビジネスへの貢献度の一層の向上を図っている。

# コントロール目標 －概要－

## DS13 オペレーション管理

データを完全かつ正確に処理するには、データ処理を効果的に管理し、ハードウェアを保守する必要がある。このプロセスには、計画された処理の効果的管理、機密性を有する出力の保護、インフラストラクチャのモニタリング、およびハードウェアの予防的保守のためのオペレーションポリシーおよび手続の策定が含まれる。効果的なオペレーション管理により、データのインテグリティが維持され、業務の遅延および IT 運用費用が削減される。


**IT プロセス: オペレーション管理のコントロール目標は、**

データのインテグリティを維持し、IT インフラストラクチャのエラーや障害に対する抵抗力・回復力を保証することを、**ビジネス要件**とし、

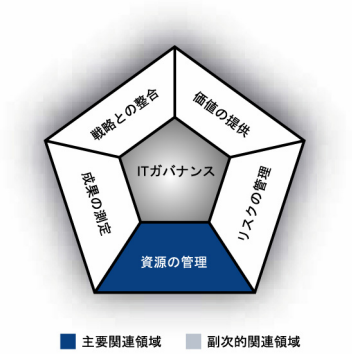
**重点をおくべきコントロールは、**計画されたデータ処理の運用サービスレベルを達成し、機密性を有する出力を保護し、インフラストラクチャをモニタリングおよび保守することである。

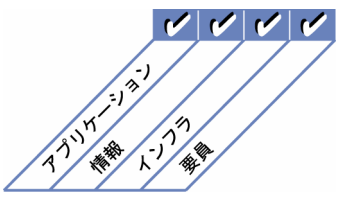
**実現するための手段は、次の 2 項目である。**

- 合意されたサービスレベルと定義された方針に従った IT 環境の運用
- IT インフラストラクチャの保守

**その成果の測定指標は、次の 3 項目である。**

- 運用上のインシデントの影響を受けるサービスレベルの数
- 運用上のインシデントに起因する予定外のダウンタイムの時間数
- 予防的保守スケジュールに組み込まれているハードウェア資産の割合



# コントロール目標 －詳細－

## DS13 オペレーション管理

### DS13.1 オペレーション手続と指示
IT オペレーションの標準手続を策定、導入、保守し、オペレーション担当スタッフがすべての関連オペレーション任務を熟知しているようにする。継続的なオペレーションを保証するために、オペレーション手続はシフト交代時の引継ぎ項目(アクティビティ、状況に関する最新情報、オペレーションの問題、エスカレーション手続、および現行の責任に関する報告)が含まれている必要がある。

### DS13.2 業務のスケジュール策定
業務、プロセス、任務のスケジュールを最も効率的な順序で構成し、ビジネス要件を満たすために処理能力と稼働率を最大にしながら、ジョブ、プロセス、タスクのスケジュールを最も効率的な順序で構成する。初期スケジュールとスケジュール変更は、ともに認可を得る必要がある。標準のジョブスケジュールからの逸脱を特定、調査、および承認するための手続を整備する必要がある。

### DS13.3 IT インフラストラクチャのモニタリング
IT インフラストラクチャおよび関連イベントをモニタリングするための手続を定義し、導入する。運用および運用を取り巻き支援する他の活動を時系列に再構成、レビュー、および調査可能にするために、十分な時系列情報が運用ログに保管されることを保証する。

### DS13.4 機密文書と出力デバイス
特殊書類、有価証券、特殊目的のプリンタやセキュリティトークンなどの機密性を有する IT 資産について、適切な物理的保護策、責任割り当て、および在庫管理手続を確立する。

### DS13.5 ハードウェアの予防的保守
インフラストラクチャのタイムリーな保守を保証するための手続を定義し導入する。これにより、障害やパフォーマンス低下の発生頻度と影響を低減できる。

# マネジメントガイドライン

## DS13 オペレーション管理

| From | インプット |
|---|---|
| AI4 | ユーザ、運用、サポート、技術、および管理の各マニュアル |
| AI7 | システムの本番環境への移行およびソフトウェアリリースおよび配付計画 |
| DS1 | サービス・レベル・アグリーメント(SLA)とオペレーショナル・レベル・アグリーメント(OLA) |
| DS4 | バックアップの保管と保護に関する計画 |
| DS9 | IT の構成/資産の詳細 |
| DS11 | データ管理に関するオペレータ向け指示書 |

| アウトプット | To |
|---|---|
| インシデント情報 | DS8 |
| エラーログ | DS10 |
| プロセスの成果報告 | ME1 |

### RACI チャート

| アクティビティ / 担当 | CEO | CFO | 企業幹部 | CIO | ビジネス プロセス オーナー | オペレーション責任者 | 設計責任者 | 開発責任者 | IT管理責任者 | PMO（プロジェクト・マネジメント・オフィス） | コンプライアンス、監査、リスク、セキュリティ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| オペレーション手続(マニュアル、チェックリスト、シフト交代計画、引き継ぎ文書、エスカレーション手続など)の定義/変更 | | | | | | A/R | | | | | I |
| 作業負荷とバッチジョブのスケジュール策定 | | | | | C | A/R | C | C | | | |
| インフラストラクチャと処理のモニタリングおよび問題の解決 | | | | | | A/R | | | | | I |
| 物理アウトプット(紙、メディアなど)の管理と保護 | | | | | | A/R | | | | | C |
| スケジュールとインフラストラクチャへの修正または変更の適用 | | | | | C | A/R | C | C | | | C |
| 認証デバイスを侵害、損失、盗難から保護するためのプロセスの導入/確立 | | | | A | | R | | | I | | C |
| 予防的保守のスケジュール策定と実施 | | | | | | A/R | | | | | |

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

### 達成目標とその評価指標

**アクティビティの達成目標**
- 定義されている方針および厳密な監視を踏まえた、合意されたサービスレベルに従った IT 環境の運用
- IT インフラストラクチャの予防的保守とモニタリング

*上記目標達成度を以下で測定する*

**重要成果達成指標(KPI)**
- オペレーション要員 1 名あたりの年間研修日数
- 予防的保守スケジュールに組み込まれているハードウェア資産の割合
- 自動化された作業スケジュールの割合
- 運用手続の更新頻度

*促進*

**プロセスの達成目標**
- 運用手続の定義と、合意されたサービスレベルとの整合性の確保
- 計画された処理と特別な要求の処理を完全に行う
- 機密情報に対する物理的保護策の施行

*上記目標達成度を以下で測定する*

**プロセスに関する重要目標達成指標(KGI)**
- オペレーション手続からの逸脱に起因するダウンタイムインシデントと遅延の件数
- 計画された作業と要求のうち、予定どおりに完了しなかったものの割合
- 不適切な手続に起因するダウンタイムインシデントと遅延の件数

*促進*

**IT の達成目標**
- エラー、意図的な攻撃、または災害で生じた障害に対する、IT サービスおよびインフラストラクチャの抵抗力・回復力の保証
- 提供されるサービスとサービスレベルに対するエンドユーザが満足することへの保証
- 要求に応じて IT サービスを使用可能であることの保証

*上記目標達成度を以下で測定する*

**IT に関する重要目標達成指標(KGI)**
- 運用上のインシデントの影響を受けるサービスレベルの数
- 運用上のインシデントに起因する予定外のダウンタイムの時間数

# 成熟度モデル

## DS13 オペレーション管理

**「データのインテグリティを維持し、IT インフラストラクチャのエラーや障害に対する抵抗力・回復力を確保する。」というITに対するビジネス要件を満たす上で、「オペレーション管理」プロセスにおける管理の成熟度は、以下のとおりである。**

**0 不在**
組織は、基本的な IT サポートおよびオペレーション活動の確立のために時間も資源も投入していない。

**1 初期/その場対応**
IT サポート機能を構築する必要性を組織が認識している。標準手続はほとんど確立されておらず、オペレーション活動は事実上、事後的に行われている。オペレーションプロセスの大部分は非公式に計画され、処理要求は事前検証なしで受け入れられている。ビジネスプロセスを支援するコンピュータ、システム、およびアプリケーションの中断、遅延、および使用不能状態が頻繁に発生する。従業員が資源を利用できるまで待機している間に、時間が失われている。アウトプットメディアが予期しない場所で発見されたり、見つからなかったりする場合がある。

**2 再現性はあるが直感的**
IT サポート機能を提供する上で IT オペレーション活動が果たす主要な役割について、組織が認識している。ツール導入のための予算は、場合に応じて割り当てられている。IT サポートオペレーションは非公式かつ直感的に行われている。個人的なスキルや能力に大きく依存している。何をいつ、どのような順序で実行するべきかという指示が文書化されていない。何らかのオペレータ研修が実施されており、正式なオペレーション標準もいくつか存在する。

**3 定められたプロセスがある**
コンピュータオペレーション管理の必要性が組織内で理解され、受け入れられている。資源が配分されており、ある程度の実地研修(OJT)が実施されている。定型業務について正式に定義、標準化、文書化、および周知されている。イベントと完了タスクの結果が記録されているが、そのすべてがマネジメント層に報告されるわけではない。自動スケジュールツールなどのツールが導入され、オペレータの介入が削減されている。オペレーションに新規業務を組み込むためのコントロールが導入されている。予定外のイベントの発生を削減するための正式なポリシーが策定されている。ベンダーとの保守サービス契約は、事実上、依然として非公式なものである。

**4 管理され、測定可能である**
コンピュータオペレーションおよびサポートの実行責任が明確に定められており、オーナシップが割り当てられている。設備投資と人的資源への予算投入を通して、オペレーションが支援されている。研修が正式になっており、継続的に実施されている。スケジュールと業務が文書化され、IT 部門とビジネス顧客の両方に周知されている。標準化された成果目標に対する合意と定められたサービスレベルに基づいて、日常的な活動を測定およびモニタリングできる。確立されている水準からの逸脱が生じた場合は、速やかに対処および是正される。マネジメント層は、コンピュータ資源の使用状況と作業または割り当てられている業務の完了状況をモニタリングしている。継続的な改善の手段として、プロセスの自動化レベルの向上のための継続的な努力がなされている。ベンダーとの間で正式な保守サービス契約が締結されている。エラーや障害の原因分析により、問題管理、キャパシティ管理および可用性管理のプロセスとの完全な整合が図られている。

**5 最適化**
IT サポートオペレーションが効果的、効率的であり、生産性の低下を最小限に抑えてサービスレベルの要件を達成できるだけの十分な柔軟性を備えている。IT オペレーションの管理プロセスが標準化および文書化され、知識ベースに蓄積されており、継続的な改善が義務付けられている。システムを支援する自動化プロセスはシームレスに運用されており、環境の安定性の維持に貢献している。すべての問題と障害について、根本原因を特定するための分析が行われている。変更管理担当者との会合を定期的に行うことで、変更を作業スケジュールにタイムリーに組み込むことを保証する。装置の使用年数と機能不良の兆候の有無について、ベンダーと協力した分析が行われており、多くの場合予防的保守が可能になっている。