

## 5 . 運用・評価プロセス

### 5 - 1 運用・評価プロセスについて

#### (1) 情報システム運用・評価の基本的な考え方

前述したような情報システムの計画、調達、開発の各プロセスを着実に実施することで、運用時におけるリスクをある程度軽減することは可能である。しかしながら、情報システムを安定して継続的に活用するためには質の高い運用を実現することが不可欠であり、社会環境や情報通信技術における変化が急速であること等を考慮すると、運用時において問題（情報システムと社会環境の不整合等）が発生する可能性は決して少なくない。また、計画、調達、開発の各プロセスにおけるミスが運用後、しばらくしてから顕在化することも珍しくない。このような問題の発生をできるだけ回避し、あるいは発生した場合の対処を迅速にすることで、情報システムの安定稼働、有効利用を確保することが運用時における大きな命題となる。昨今では情報システムの運用そのものを外部にアウトソーシングする事例も増えてきているが、そのような場合でもその運用内容を適切にモニタリングすることが肝要である。

一方、行政機関として、情報システムが適切に運用されているかどうかの説明責任（アカウントビリティ）を果たし、より効率的かつ効果的な運用に向けた変更や修正等を行うためには、評価を行うことが不可欠である。行政評価を導入する自治体は確実に増えてきているものの、これを情報システムに適用している事例はほとんどなく、所謂、「いれっぱなし」になっていることも少なくない。したがって、「運用プロセス」ではなく、「運用・評価プロセス」に意識を変えることがまず求められる。評価は、政策から情報システムの運用に係る細かな業務まで様々なレベルで行われる必要があり、そのレベルによって評価の期間や内容も異なってくる。細かな業務レベルでの評価は短いサイクルで日々の業務改善に反映されるべきであり、逆に政策レベルでの評価は1～数年程度の比較的長いサイクルで行い、その結果を次の計画や次年度の運用に反映させることになる。評価によって情報システムに係るマネジメントサイクルを機能させることで、情報システムの有効性等の向上を図るだけでなく、適切な廃止や改善が行わなけれ

ばならない。

#### (2) 運用・評価プロセス編の構成

情報システムの運用・評価プロセスにおいて実施すべき作業は、情報システムを適切に運用することと、計画プロセスで計画した内容に基づき情報システム導入成果を継続的に評価し、改善することである。情報システムの運用に関しては、これまでも行われてきたが、情報通信技術の進展やセキュリティ面でのリスクの健在化、あるいはアウトソーシングの進展等の環境変化を考慮し、「質の高い運用」を図らなければならない。情報システムの評価に関しては、計画プロセスと同様に「政策的な評価」と「技術的な評価」に分けることができ、その評価結果をもとに各情報システムの「改善・廃止」を行わなければならない。

なお、運用・評価プロセスは基本的に情報システムを所管する各原課、および担当者が対応するものであり、運用業務の改善や情報システムの評価に関しては、必要に応じて情報化担当部署がこれを支援する。

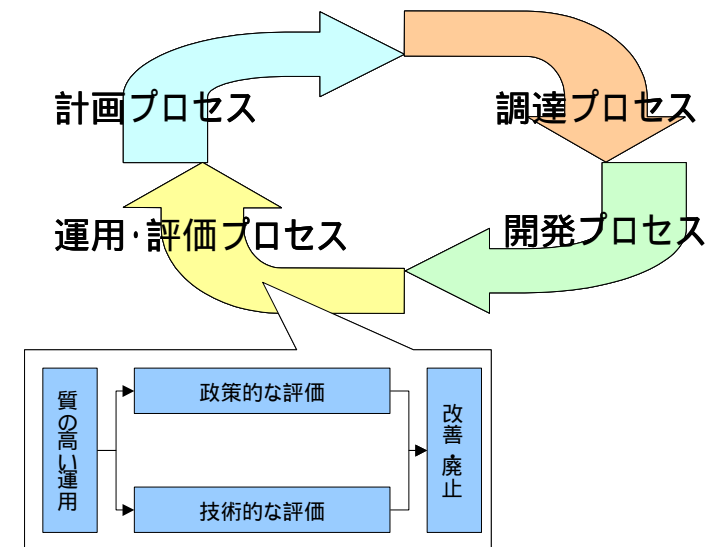


図5 - 25 運用・評価プロセスの構成

## 5 - 2 質の高い運用

### (1) 運用業務の計画

情報システムの運用に関しては、基本的に開発プロセスで作成した運用マニュアル等に沿って行うことになるが、実際には様々な付帯作業が存在する。そこで、以下に示すような運用業務について事前に運用計画を立て、当該情報システムの運用業務の標準化<sup>1</sup>を行わなければならない。運用業務を標準化しておくことで、運用業務の改善が容易になるとともに、運用担当者の異動による運用レベルの低下を最小限にとどめることができる。

運用計画では、以下に示すような作業の内容、運用体制と役割分担、実施期間や頻度、運用目標等について記述する。

また、情報システムの運用を外部に委託する場合には、運用計画の概要を基に委託事業者を募集するとともに、決定した委託事業者と詳細な運用計画について調整を図る必要がある。開発と運用を合わせたライフサイクル単位で情報システムの調達を行う場合には、調達時の仕様書に計画プロセスで検討したレベルの運用条件を記し、詳細な内容に関しては、開発プロセス終了後、別途協議するようにする。

### (2) 適切な運用体制の維持

情報システムを所管する原課は、その運用が適切に行われるよう、可能な限り専門知識を有する職員を運用管理者として配置することが望ましく、そうでない職員が運用を担当する際は、専門知識の習得に必要な研修機会等を提供する必要がある。また、人事異動に際しては、後任者が運用を効率的に行えるよう、引継を的確に実施しなければならない。

一方、情報システム運用業務における特殊性をなるべく排除するために、情報システムの継続利用に必要なオペレーション作業等を標準化するとともに、可能な限り合理化、簡素化することが原課において求められる。マニュアル類を整備しておくことはもとより、それらが陳腐化しないよう、情報システムの改善等を反映した修正を継続的に行うことが必要である。

<sup>1</sup> 業務内容や業務プロセス等の最適化を図り、規定すること

情報システムの運用作業が膨大かつ複雑である場合、あるいは職員が行う必要性が低い場合には、外部に運用を委託することが望ましく、その際は、委託先の運用体制を適切に管理しなければならない。配置されている人員や能力が当初の契約に則したものであるかどうか、原課、あるいはシステム運用担当者との情報連携が確保できているか等が重要な確認事項となる。

### (3) 性能や品質の管理

情報システムの運用担当者は、当該システムが利用者のニーズに応じた性能や品質を確保しているかどうかを定期的にモニタリングし、不十分である場合は改善を図らなければならない。モニタリングする視点としては後述する「技術的な側面からの評価」で示すような項目を挙げることができ、それぞれを容易に評価できるような仕組みを事前に構築しておくことが必要になる。情報システムから必要な統計データを入手できるようにしておく他、障害等の具体的な事象を記録しておき、必要に応じて利用者から情報も収集する。

モニタリングの結果に出てきた問題が、情報システム開発時の要求仕様書や設計書等に反しており、瑕疵担保責任の存続期間内であるならば、開発委託先に対して瑕疵担保責任を問うことができる。また、運用を推進する過程で生じたものであるならば、費用対効果等を考慮して改善の可否について検討することになる。

また、運用そのものを外部に委託している場合には、事前に SLA を締結しておくことで、SLA の内容に基づく性能や品質管理を行うことが望ましい。運用サービスの内容が基準に満たない場合は改善を委託先に要求するとともに、SLA に基づくペナルティを課すことができる。具体的には、表 5 - 2 5 に示すような事項を SLA に示すことが必要であり、評価項目や評価方法、あるいは責任の範囲を明示しておくことが不可欠である。

表 5 - 2 5 運用に関する SLA で記載すべき事項

構成要素	内容	参考例
対象サービスとサービスメニュー、要件	SLAの対象となるサービスとそのサービス内容と要件	・申請、届出サービス ・電子入札サービス・・・等
サービスの利用料金	サービス提供を受けたときの利用料金の計算方法	・四半期固定 ・使用料課金 ・ID 課金・・・等
SLA 評価項目	対象サービスのサービスレベルを評価する項目	・サービス稼働率 ・障害回復時間・・・等
SLA 評価項目（設定値）	サービス品質を維持するため最低限守るべき品質値（保証値）と目標とする目標値がある。（注）測定できない項目はSLA評価項目とはできない。	・稼働率99.5%以上 ・障害回復60分以内・・・等
SLA 評価項目の測定方法	SLA評価項目（設定値）を測定するための方法	・稼働率99.5%以上は、サービス開始から1年間で測定・・・等
利用料金の減額（ペナルティ）/ボーナス	SLA評価項目（設定値）を守れなかった場合の減額金等の計算方法や目標をクリアした場合の割増金	・一定割合の減額 ・使用量に見合う減額・・・等
利用者側の義務	SLA評価項目（設定値）を保障するために利用者側で実施すべき義務	・1ヶ月ごとの不要なファイルの削除・・・等
免責事項	SLA評価項目（設定値）の実績を算出する場合に免責される事項	・利用者側原因による場合 ・OSやミドルウェアのバグによる場合・・・等

出典：総務省「公共ITにおけるアウトソーシングに関するガイドライン」

#### （４）情報システムの保守・変更管理

情報システム導入後はその安定した利用を妨げることがないように、保守作業を適切に行うことが不可欠である。保守作業とは、障害等の問題へ対応すること、および情報システムを取り巻く環境変化に応じた変更・修正・追加を行うことである。ソフトウェアのバージョンアップ、パッチ<sup>2</sup>適用等も保守作業に該当し、その実施には専門的な知識を要する場合もある。したがって、情報システムの開発を委託した業者やその関連業者等と保守契約を結ぶことが多い。ただし、オープンソース・ソフトウェア等を活用し、汎用性の高い情報システムに関しては、運用と保守を合わせて、開発とは別個に調達を行うことも考えられる。保守契約を結ぶ際には、保守の範囲

<sup>2</sup> 既存のソフトウェアのバグを修正したり、細かな改善を図るための差分プログラムを指す。

を明確に定めておく必要がある。

情報システムの大幅な変更・修正・追加等に関しては、保守業務の範囲外となる可能性が高い。したがって、法制度や業務、あるいは求められる処理能力やセキュリティ要件等の変化に際しては、必要なシステム変更について検討しなければならない。また、関連する情報システムの開発や変更等の要因によって、連携を図るために当該情報システムの変更が必要となる場合もある。このような大幅なシステム変更等に関しては、基本的に本ガイドラインで述べた計画プロセス、開発プロセスと同様の手順を進めることになる。すなわち、必要性や費用対効果等を踏まえシステム変更の実施可否を検討するとともに、その内容を計画し、システム変更部分の開発を実施する。

変更した内容は適切に記録する必要があり、当該情報システムの各設計書、業務運用手順、運用マニュアル等を変更に合わせて更新する。また、情報システムを所管する原課の許可のないシステム変更等が行われないよう適切な変更管理をしなければならない。

#### （５）利用に関する問題への対応

情報システムの利用においては様々な問題が発生する。これらの問題は、利用者側での問題と情報システム側での問題の二つに大別することができ、ここでは便宜上、前者を「利用者トラブル」、後者を「障害」と言うこととする。

通常、問題の発生リスクに関しては、事前にある程度予測できる場合が多い。したがって、予測が可能で、かつ発生リスクが大きい（発生頻度×被害の大きさ）と考えられる問題に関しては、事前に対策を行っておくことが望ましい。

庁内で広く利用されるような情報システムの場合、利用者トラブルとして、「操作方法が分からない」人が多数出てくる可能性を指摘できる。このような利用者トラブルが発生した場合の対応手順を図5-26に示すように事前に明らかにしておくことが必要であり、これによってリスクを最小化することが可能である。

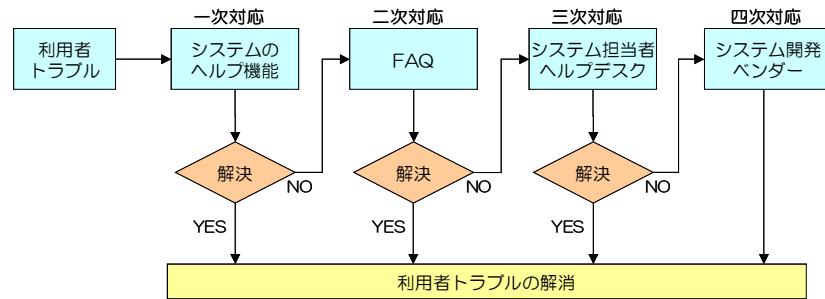


図 5 - 2 6 利用者トラブルに対する対応手順の例

また、情報システムの障害においても同様であり、停止することによるリスクが大きい情報システムに関しては、サーバの二重化等の対策を行っておくことで、障害が起こってもサービスを停止せずに済む可能性が高い。

情報システムの特性を考慮すると、障害の発生は必ず視野に入れて検討を行うことが望ましく、発生時は障害箇所やその原因をすみやかに明らかにしなければならない。障害が発生する部分は、ハードウェア、ソフトウェア、ネットワークに大きく分けることができ、ソフトウェアは基本ソフト(OS)とアプリケーションソフト、あるいはそれを結び付けるミドルウェア等に分けることができる。また、障害の原因としては、不正な操作、過剰な負荷、機器の故障だけでなく、開発時の設計ミス等もあり得る。

一方、障害に関しては、すべてのリスクに対して事前対策が可能なわけではなく、対策を行っていても問題が生じる可能性はある。そこで、障害が発生した場合の被害を最小化することを目的として、対応手順を明らかにしておくことが有効である。例えば、障害が起こった場合、どのような手順で原因を究明し、対策を検討し、実際の対策を講じるか、あるいはその理想的な実施スケジュール等をマニュアル化しておくことが挙げられる。同様に災害等、不足の自体が生じた場合の対応手順書等も整備しておくことが望ましい。

発生した問題の内容(障害なら発生頻度や復旧までの時間等)を記録し活用することも不可欠である。利用者トラブルの場合、利用者にとった

問題や対処方法をデータベース化し、FAQ<sup>3</sup>として提供することで、利用者からのシステム担当者やヘルプデスクへの問い合わせを軽減できる。また、障害においても内容や対処の記録を残すことで、同様の障害の防止や、発生時の効率的な対処が可能になる。

なお、運用を外部に委託している場合は、障害時の連絡体制を確立し、障害に関する報告を義務付けることも必要である。また、運用計画時に、想定される情報システムのリスクや対処方法について明文化し、遵守を要求することが望ましい。

#### (6) 利用者の習熟度向上と利用促進

情報システムの利用を促進し、組織として最大の効果を創出できるようにすることも原課、あるいはシステム担当者の重要な役割である。

情報システムの導入に際して、操作方法に関する研修を提供することはもとより、操作に必要な基礎的な情報リテラシー育成等についても十分配慮する必要がある。また、異動によって情報システムの利用者が変わることは多く、初めて利用する人に対して、随時、必要な研修機会を提供するか又は利用に習熟している他の職員がサポートを行う。利用者自身が操作について自己学習できる環境を整備しておくことも不可欠であり、情報システムのヘルプ機能を開発時に整備しておくことや、マニュアル類、FAQ等を紙、あるいは電子データで共有することが必要である。

利用者が情報システムを操作するのに十分な知識や能力を有しているにも関わらず利用が進まない場合はシステム側に問題がある可能性が高い。利用者から話を聞くことで、情報システムの反応が遅い、インターフェースが使いにくい等の問題点を明らかにし、改善を図ることが望ましい。

一方、情報システムを利用する際には障害やセキュリティ上の問題を回避するため、利用者が遵守しなければならない事項も存在する。セキュリティポリシーや実施手順、あるいはマニュアル類において遵守事項を明ら

<sup>3</sup> Frequently Asked Question の略。多くの人から出てくると予想される質問とそれに対する回答を事前に容易することで、同じような問い合わせに対応する労力削減を図ることを目的としている。

かにし、研修等によって周知徹底しなければならない。

(7) セキュリティ対策

品質維持や利用者の習熟とも重複するが、セキュリティ問題が顕在化しているなか、情報システムの安全性や信頼性を確保することがシステム担当者の重要な責務となる。セキュリティポリシーを策定している自治体では、これに沿う形で各情報システムの実施手順を作成し、運用することで当該情報システムのセキュリティ維持に努めなければならない。

具体的に求められる業務としては、人的セキュリティ対策、物理的セキュリティ対策、技術的セキュリティ対策に大別することができる。人的セキュリティ対策としては、前述したような研修等による利用者の啓発があり、情報システムで取り扱っている情報が個人情報等、重要度が高い場合には第4章で述べたように守秘義務契約書等を取り交わすこと等も必要になる。物理的セキュリティ対策としては、サーバ等に触れられる人の制限等があるが、マシン室等に集約されている場合はこれを管理する情報化担当部署に依存することになり、端末側の管理がメインとなる。端末に関しては、持ち運びの利便さや机上のスペースの問題からノートパソコンの利用が進んでいるが、盗難が容易であることにも十分に留意する必要がある。技術的セキュリティ対策としては、情報システムの外部からの不正アクセス、あるいは内部における不正利用の監視等が挙げられる。庁内 LAN 上で稼働している場合は不正アクセス対策を全庁的にまとめて行うことが想定されるが、情報システム側でも二重に行うことが望ましく、利用者の権限に応じたアクセス制御の設定等が必要になる。

(8) 資産管理

情報システムの運用を行う上で基礎的な情報を把握しておくことは大前提であり、その一つとして資産情報がある。情報システムを構成するハードウェア、ソフトウェア、あるいはデータ等（ネットワークは全庁的な資産）を情報資産として認識し、その現状把握するとともに、適切な管理を行わなければならない。

まず、情報システムを導入した時点において情報資産をリストアップし、これをデータベース化する必要がある。ハードウェアに関しては、その性能概要（CPU、メモリー、ハードディスク容量等）基本ソフト（OS）の名称やバージョン、提供ベンダー名、設置場所（利用者）等について記録する。ソフトウェアに関しては、ワープロ、表計算等の端末のみで稼働する汎用アプリケーションソフトだけでなく、サーバで稼働するアプリケーションソフトやミドルウェアと呼ばれる複数のアプリケーションソフトを結ぶ連携ソフト等について、名称、バージョン、ライセンス数、利用端末、提供ベンダー名等を記録する。また、それぞれにおける導入形態、費用、ライフサイクルに関する情報も合わせて記録する。導入形態に関しては、買取、リース、レンタル等があり、ライフサイクルとしては償却期間、リース・レンタル期間、保守期限等がある。データに関しては、情報システムの処理において記録されるデータの内容や容量だけでなく、MT（磁気テープ）等にバックアップしたデータの内容についても記録する。

このような情報資産データベースをもとにして1年に1度、定期的に資産の棚卸し（資産の保有状況や減耗等を確認する作業）を行わなければならない。ハードウェアが、データベースのとおり形態や場所に所在する

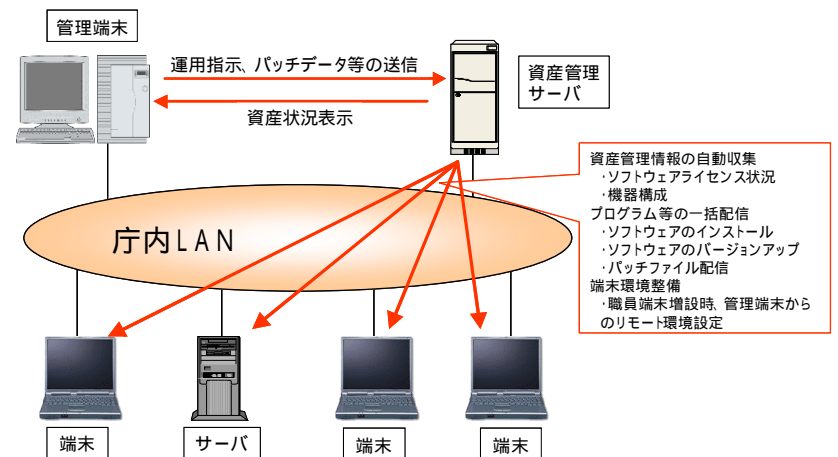


図5 - 27 資産管理システムのイメージ

か、ハードウェア上で稼働しているソフトウェアがライセンスに基づいているか等を調査し、資産の移動や紛失、ソフトウェアの不正な利用等の有無を確認する。また、端末やアプリケーションソフト等の利用状況についても確認を行い、利用されていない遊休資産に関しては、他への転用や消却等を行い、資産効率を高める。

昨今では資産管理業務を効率的に行うための情報システムも販売がされており、資産に関する情報をデータベース化し、管理するだけでなく、管理しているソフトウェアへのパッチ適用等も自動で行うことができる。ただし、このような資産管理システムは、端末等がすべて導入時に登録されることが前提になっており、大規模で端末の導入自体が把握できていない自治体では制度や仕組みから変えていくことが先決であろう。

## 5 - 4 政策的な評価

### (1) 目的や目標の達成状況の評価

#### 目標の達成状況の評価

情報システムが計画プロセスで設定した目標をどの程度達成できているかを定期的に評価しなければならない。情報システムがどれだけ利用され、情報システムの利用者、あるいは行政サービスの利用者にとってどれだけの効果を創出しているかを確認する。

有効性、効率性、経済性、費用対効果等を測るために、計画プロセスの「評価指標と目標の設定」において設定した評価指標の現状の値を計測する。バランススコアカード等を用いて評価指標を設定した場合は、そちらについても値を計測する。情報システムから必要な統計データ等を抽出したり、複数の情報を組み合わせて値を計算したりするほか、必要に応じて評価指標の値を抽出するために簡易な調査等も実施する。

抽出した評価指標の値に関しては、それ自体から評価を行うことも可能であるが、客観性を確保するために比較等を行うことが必要である。事前に設定した目標と照らし合わせたり、あるいは前年度の値と比較することで、情報システムを評価し、可能であれば他の自治体との比較等も行う。費用対効果等の指標に関しては、計画プロセスの「費用と効果の把握」で

示したように、効果を金銭換算することで、指標のみによる客観的な評価も可能である。

また、抽出した評価指標の値と上位政策の評価指標との関連性についても分析することが望ましい。例えば、インターネット上で観光を疑似体験できる情報システム（観光体験システム）を構築してサービスを提供した場合を想定すると、観光体験システムの利用者数等が当該情報システムの評価指標として挙げられ、上位政策の評価指標として観光客入込数等が挙げられる。双方の評価指標の値について分布を見たり、相関分析等を行うことで、情報システムと上位政策との関連性を捉えることができ、寄与率から逆に経済効果を算出することも可能である。もちろん、関連性が低いという理由だけで情報システムの必要性が低いと一概には言えないが、上位政策との関連性を把握し、情報システムの有効性を測る上で一つの目安とはなる。

なお、相関分析等によって関連性を分析する際には、評価指標の値だけでなく、関連する他の指標も考慮する必要がある。例えば、図 5 - 2 8 に示すように観光体験システムと観光レクリエーション客入込数の相関係数 ( $R^2$ )<sup>4</sup>は 0.8704 であるが、観光体験システムに影響するであろうインターネット利用率を加えて分析すると相関係数は 0.9206 まで上がり高い相関が見られる。

年度	観光客入込数(千人)	観光体験システムアクセス数(件)	インターネット利用率(%)
1998年度	40,109	25,792	9.2
1999年度	41,994	62,815	21.4
2000年度	42,127	109,244	37.1
2001年度	42,375	130,324	44
2002年度	44,254	168,583	54.5

図 5 - 2 8 評価指標の相関分析の例

<sup>4</sup> 二つの変数における関係の強さを表す係数であり、-1 から 1 までの値をとる。絶対値が 1 に近づくほど関係性が強い。

### 目的の達成状況等の確認

有効性、効率性、経済性、費用対効果等の評価、あるいは目標の達成状況を基に、情報システムの目的の達成状況を確認する必要がある。ただし、目標の達成状況が直接、目的の達成状況へ結び付かない場合もある。所謂アウトプットとアウトカムの違いである。

例えば、住民の情報リテラシー育成や、情報格差（デジタル・ディバイド是正）を目的としてインターネットが利用できる公開端末を設置した場合を想定する。計測しやすい評価指標の一つとして公開端末の利用率があるが、仮に利用率が高く、頻繁に利用されていたとしても、それは必ずしも目的の達成を示さない。利用者のほとんどが情報通信技術に詳しい若年層で、自宅にもインターネットを利用できる環境を有している可能性もあるからである。したがって、目的の達成状況は評価指標の値だけでなく、多様な角度から慎重に評価しなければならない。

また、目的の達成状況は、情報システムだけでなく、他の社会環境の影響によっても変化する。例えば、前述した観光体験システムにおいてシステム自体の利用率は高くても、円高等の別の要因によって観光客が海外に流出し、自治体の観光客入込数が伸び悩むことも考えられる。つまり、情報システム自体が効果を上げ、目標を達成していても、社会環境における他の要因によって最終的な目的が十分に達成されない場合もある。

なお、目的の設定に際してバランススコアカードを用いた場合は、「顧客」、「財務」、「業務プロセス」、「学習と成長」といった四つの視点それぞれで目的の達成度合、およびそのバランスを評価することが望ましい。それぞれに設定した評価指標の値や目標の達成状況を踏まえ、各視点の目的の達成度を確認するだけでなく、各視点における達成度において偏りがなさを比較検討する。

### (2) 必要性の再評価

導入時において必要と考え整備した情報システムであるが、社会環境変化とともにその必要性も変化する。例えば、技術的に陳腐化することが想定され、パソコン通信がインターネットに取って代わったように、旧来

の技術は利用の縮小とともにその必要性が低下する。また、業務量の減少によって情報システムで処理する必要性がなくなることや、利用者ニーズが変化して不必要になることもあり得る。加えて、民間企業によって同様の情報サービスの提供等が行われるようになれば、行政機関として情報システムを継続することは民業圧迫になる危険性もある。そこで、このように情報システムを取り巻く環境変化を踏まえて、当該情報システムの必要性を定期的に見直すことが必要である。

情報システムを自己導入する必要性についても見直すことが望ましい。昨今では、LGWAN による ASP サービスが開始される等、ASP の対象範囲も徐々に拡大してきており、情報システムを代替できる可能性がある。ASP 活用が難しく情報システムを継続的に運用しなければならない場合でも、庁内に設置する必要性が低く、アウトソーシングすることでかえって運用効率やセキュリティが高まる場合もある。したがって、情報システムに関しては、自庁内に継続的に構築することを前提とせず、業務ニーズや技術動向を踏まえて、適宜、再編を図ることが望ましい。また、情報システムの中には本来一体的に処理されるべきであるが、予算等の関係でバラバラに構築されてきたものも存在する。したがって、当該業務を情報システムで処理する必要がある場合でも、既存の情報システムの区分を継続するのではなく、他の情報システムと合わせて統合情報システムの構築等を視野にいれて検討することも必要である。

さらに、情報システムで処理している業務そのものの必要性が変化することもあり得る。都道府県と市町村の業務分担が変わったり、民間企業や NPO 等の他の主体によって自治体の役割が代替される可能性もある。業務が廃止されれば、当然情報システムも必要なくなる。

### (3) 公平性の評価

情報システムが想定していた利用対象者においてどれだけ広く公平に利用されているかを評価する。アクセシビリティガイドライン等の基準を設けている場合はこれに照らし合わせるとともに、可能な限り利用対象者の意見を反映して公平性について評価を行うことが望ましい。

職員を対象にした情報システムでは、利用対象者の定期的に利用状況をモニタリングし、未利用者や利用頻度が少ない人がいないか確認を行う。情報システムの機能から利用者や利用状況の統計が取れる場合はこれを活用し、そうでない場合は利用対象者にアンケート調査（少ない場合はヒアリング調査）等を行い、利用状況を把握する。インターフェースの使い勝手が利用を阻害していないか、職員の情報リテラシーや情報システムに対する知識の差が利用の度合に影響していないか、あるいは、職員の身体的な特性や障害等が利用の妨げになっていないか等について利用状況から評価する。

住民等、不特定多数の庁外の人を対象にした情報システムに関しては、利用者数等の利用状況の把握は比較的容易であるが、その利用の公平性について把握することは難しい。したがって、システム担当者は基本的にアクセシビリティガイドライン等に沿って現状を評価することになる。ただし、可能な限り利用者側の意見を収集するように努めることも必要である。相談窓口等に当該情報システムに対する問い合わせが入っていないかどうか等を確認するとともに、ヘルプデスク（設置している場合は）への問い合わせ等も評価の参考とする。また、必要に応じて利用者に対するアンケート調査や、住民モニターによる評価等も活用することも考えられる。

この他、情報システムを利用するために利用者が何らかの負担をしている場合には、その負担の公平性を評価することが望ましい。金銭的な負担が利用者間で公平に行われているか、あるいは利用に要する労力が公平になっているか等について検討する。

#### （４）費用を踏まえた評価

費用に関しては、毎年度、情報システムの運用に要した実際の費用を算出し、計画時において算定した LCC と比較する必要がある。当初予定していた LCC よりも費用が大きくなっている場合、その原因、妥当性及び低減の可能性について分析を行う。また、年度ごとに費用対効果等を評価する場合には、運用費用だけでなく、初期費用の減価償却費を合わせて計上し、年間費用として捉えなければならない。

評価に費用を用いる場合、基本的には初期費用と運用・保守費用のみを足した LCC を用いるが、必要に応じて総合コスト（TCO：Total Cost Ownership）の考え方を活用することが望ましい。TCO は情報システムに係るすべての人の動きを費用として捉える考え方で、その意味で ABC 分析と類似しており、行政で見過ごされがちな職員の人件費を意識する上で有効である。例えば、障害等によって情報システムが停止した場合、停止中業務が行えなかったことは機会損失費用として捉えることができる。表 5 - 27 に示すように利用者 100 人の情報システムが半日停止した際、当該情報システムが業務に不可欠であったなら、その機会損失費用は 125 万円となる。また、情報システムの利用があまりにも難しく、利用時間中の 4 分の 1 はマニュアルやヘルプ機能を使って操作方法を調べている（セルフサポート）場合も大きな損失となる。セルフサポートを行っている間、情報システムを利用した業務処理は行われていない。そのため、100 人が半日程度利用する情報システムでこのような状態が 1 ヶ月続けば、600 万円以上の損失となる。

このような TCO を活用した分析は情報システムの課題を明らかにする際の一つの材料となる。例えば、上記のような障害が年間 10 回以上起きているのであれば、その被害は 1 千万円以上になり、500 万円の費用で改修を行って、障害頻度で 2 割まで減らすことは妥当と考えられる。なぜなら、改修によって減らせる損失が改修費用を上回っているからである。

表 5 - 26 TCO を構成する費用項目

IT資産コスト	・ハードウェア（買い取り/リース） ・ソフトウェア（買い取り/リース）	・開発（内部/アウトソーシング） ・消耗品（トナー、CD-ROM、MO）
技術サポートコスト	・情報化担当部門による情報システム等のオペレーション ・ヘルプデスク（直接サポート、電話サポート） ・エンドユーザーへの教育サービス	
管理コスト	・システム開発管理（内部/アウトソーシング） ・システム運用管理（内部/アウトソーシング） ・資産管理	・通信・電気 ・システム監査
エンドユーザーコスト	・サポート（ピアサポート、セルフサポート） ・トレーニング（研修、自習学習） ・開発（エンドユーザーによる自主開発） ・Futzファクタ（業務外利用、過剰な作業） ・機会損失費用（システムダウン等による業務停滞）	



表 5 - 2 7 TCO を活用した費用試算の例

<p>【障害による機会損失費用】          情報システム停止時間：0.5日          情報システム利用者：100人          利用職員平均単価：25,000円 / 人日          機会損失費用：0.5日 × 100人 × 25,000円 / 人日 = 1,250,000円</p>
<p>【セルフサポートによる損失費用】          セルフサポート割合：1 / 4          情報システム利用者数：100人          情報システム利用割合：1 / 2          利用職員平均単価：500,000円 / 人月          損失費用：1 / 4 × 100人 × 1 / 2 × 500,000円 / 人月 = 6,250,000円 / 月</p>

## 5 - 5 技術的な評価

### (1) 信頼性・正確性の評価

信頼性とは、情報システムが障害を起こすことなく、どれだけ安定して稼働するかを指し、正確性は情報システムによる処理結果が正確であるかどうかを指す。広義においては、正確性も信頼性の一部として捉えられる場合もある。

情報システムの信頼性を評価するためには、その稼働状況をモニタリングしなければならない。情報システムにおいて障害が発生した場合、その日時や原因、復旧に要した時間等をデータとして残し、その結果をもとに情報システムの可用性を算出する。情報システムの調査をすると分かるが、情報システム担当者がこのような障害に関する情報を記録している例は非常に少なく、これでは信頼性を評価することは難しい。情報システム自体に障害のモニタリング機能が付いていない場合には、情報システム担当者が障害に関する情報を逐次記録することが不可欠である。信頼性の評価に際しては、障害の内容、頻度、可用性等を踏まえる必要があり、情報システムにとっての障害の深刻度も考慮することが不可欠である。例えば、窓口業務を処理しているような情報システムであれば 30 分間の障害でも住民を窓口で待たせるといって非常に深刻な問題であるが、統計処理等を行う情報システムであれば、半日障害があっても次の日に処理すれば問題なく深刻度は低くなる。また、情報システムの中には特定の時期にのみ集

表 5 - 2 8 可用性の算出方法

<p>&lt; 算出式 &gt;          平均故障間隔 (MTBF: Mean Time Between Failure) = 情報システム総稼働時間 ÷ 障害発生回数          平均復旧時間 (MTTR: Mean Time To Repair) = 総復旧時間 ÷ 障害発生回数  <math display="block">\text{可用性} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}</math></p>
<p>&lt; 算定例 &gt;          情報システムの要件: 可用性 = 98.0% 障害平均復旧時間 = 30分以内          障害復旧時間 25分 × 12回 20分 × 12回 10分 × 6回 合計10時間 / 月          総稼働時間 150時間 / 月          MTBF = 150時間 / 月 ÷ 30回 = 5時間 / 回          MTTR = 10時間 / 月 ÷ 30回 = 20分 / 回  <math display="block">\text{可用性} = \frac{5\text{時間} / \text{回}}{5\text{時間} / \text{回} + 20\text{分} / \text{回}} = 93.8\%</math></p> <p>結論: 一回当たりの復旧時間は短く情報システムの要件を満たしているが、障害の回数が多いため可用性は低下し、要件を下回っている。したがって信頼性は低い。</p>

中して稼働するものもあり、その場合は、集中稼働時期の信頼性と障害の深刻度を照らし合わせて評価する。加えて、障害対策が事前に施されている場合は、障害発生時にそれらが十分に機能しているかどうかを評価することも必要である。

一方、情報システムが正確な処理を行っているかどうかも重要になる。情報システムを用いることで、通常、手作業で業務処理を行うより正確性は向上するが、バグや過負荷等の要因によって処理の正確性が低下する場合もある。したがって、定期的に処理結果の正確性について評価することが望ましい。情報システムに検算等のチェック機能が付いている場合は、容易に正確性を確認できるが、そうでない場合は一部の処理結果をサンプリングし、別途処理した結果との突き合わせで正確性を評価する等の方法が考えられる。そもそもプログラムや設計自体が間違っている場合は、検

算機能等は役に立たない。

なお、情報システムの開発委託、あるいは運用委託を行い、委託先企業と信頼性や正確性に関する SLA を取り交わしている場合は、SLA の内容をもとに信頼性、正確性を評価することになり、運用委託先には評価に必要な情報提出を義務付けることが望ましい。

## (2) セキュリティの評価

技術的な側面からの評価と言っても、情報システムのセキュリティの評価に関しては、技術面だけでなく、人や組織の対応を合わせて評価することが非常に重要となる。

通常、策定したセキュリティポリシーや実施手順に基づき、これが当該情報システムにおいて遵守されているかを定期的に評価することになるが、これらが整備されていない自治体では、総務省「地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書」の「セルフチェックリスト」等を活用することも有効である。例えば、人的セキュリティでは、パスワードが容易に推察できるものになっていないか、定期的に変更されているか、漏洩しないように管理されているか、利用者が正規の対象者に限定され安易に他の職員が利用していないか等が評価項目として挙げられる。推察が容易なものになっていないか、また、技術面では、サーバの OS やアプリケーションソフトにパッチが迅速に当てられているかどうか、サーバや端末にウィルス対策が適切に実施されているか、不正なアクセスを受けていないか等が評価項目となる。

もちろん、セキュリティポリシーや実施手順自体も定期的に評価し、修正しなければならない。情報通信技術の変化、政策や法制度の変化、業務や情報システムで取り扱う情報の変化等を考慮して、必要な見直しを行う。

なお、セキュリティ面の評価に関しては、自治体の職員が自前で行うには限界がある。したがって、必要に応じて外部の専門機関を用いてセキュリティ監査を実施することが望ましい。ただし、セキュリティ監査の実施にはそれ相応の費用が必要になるためすべての情報システムを対象とすることは難しい。したがって、情報システムの重要性やセキュリティリスク

の大きさ等を勘案して CIO が必要と判断した情報システムのみ、定期的に外部機関によるセキュリティ監査を行うことが妥当であろう。

## (3) 効率性・適時性

ここでの効率性は政策的な側面で捉えた業務等の効率性と異なり、情報システムの処理能力を指し、情報システムが指示された処理をどれだけ効率良く処理しているかである。また、適時性とは情報システムの処理が適切なタイミングで行われているかどうかである。

情報システムの機能が業務に対して適切かどうかを把握するため、コンピュータの CPU 利用率やハードディスク利用率、レスポンスタイム（操作をしてから処理結果が返ってくるまでの時間）等のデータを情報システムから抽出しなければならない。また、情報システムにそのようなデータを抽出する機能がない場合には、実際に端末を操作してレスポンスタイム等を計測することも必要である。庁内 LAN 等のネットワークが処理のボトルネックになっている場合も想定され、本庁舎だけでなく、出先機関においても同様のデータ抽出を行うことが不可欠である。ある、自治体では、回線速度が遅いため出先機関で利用する情報システム端末のレスポンスタイムがあまりにも遅くなり、職員は Excel で業務のほとんどを処理し、データの記録のみ当該システムを利用するという事例もあった。このような非効率をなくすためにも、出先機関を含めて効率性・適時性を評価することが望ましい。

情報システムの効率性評価は、業務処理に対する情報システムの機能の不足を明らかにするだけでなく、過剰な部分を浮き彫りにする上でも有効である。業務処理に対して、ハードウェアの能力が過剰であるならば、他の情報システムとこれを共用することやグレードを下げることで、情報資産の有効活用や費用削減が可能になる。庁舎間の通信速度が遅いため分散配置していたようなサーバに関しては、ブロードバンドを活用することで統廃合できる可能性が高い。

一方、情報システムの運用に関する業務がどれだけ効率的に遂行されているかも評価しなければならない。システム担当者が、当該情報システム

の運用に対してどれだけの労力を割いているか、あるいは、どのような業務に時間を割いているか等についてモニタリングする。情報システムの運用はそれ自体、当該業務処理において重要ではないのであるべく少なくしたい。したがって、システム担当者が運用に割いている時間が長ければ長いほど、運用効率は低くなる。また、運用に割いている時間においても、業務内容がメンテナンス等、安定した稼働を図るためのものであれば良いが、障害等、マイナス要因への対応業務が高い割合を占めるのであれば効率は更に悪くなる。

#### (4) 柔軟性・使用性

柔軟性とは、情報システムの変更や拡張の容易さを指し、使用性とは、情報システムの使い勝手を指す。柔軟性の高い方が社会環境変化への対応が容易になり、また、使用性の高い方が幅広い利用者による効率的な業務処理が可能になる。そのため、柔軟性・使用性についても定期的に評価することが望ましい。

業務内容や法制度の変更に伴って情報システムの変更を行うことは珍しくないが、これをどれだけ容易にできるかどうか柔軟性を図る一つの指標となる。情報システムの既存機能の範囲で変更に対応できる場合、その柔軟性は高く、対応できない場合は改修等の作業が発生する。また、システム担当者が情報システムを操作することで変更に対応できる場合も、情報システムの柔軟性は高いと考えられ、逆にその度に開発業者等に変更してもらわなければならないのであれば、その柔軟性は低くなる。ある自治体では、職員で変更できる情報システムが全体の4割弱にとどまっており、多くの場合、変更を開発業者等に委託している。もちろん、業務によって変化の度合や頻度が異なるので一概に評価することはできず、変化がほとんどない業務であれば情報システム側の柔軟性が低くても問題はあまりない。

柔軟性を測るもう一つの指標である拡張性に関しては、技術的な互換性や標準化等を考慮して評価する。標準化が進んだ技術を活用し、他の情報システムとの連携が容易であれば拡張性は高く、逆に固有の技術で、他の

情報システムとの連携が難しい場合、その拡張性は低くなる。拡張性は当該情報システムにおいて採用技術を決定した際にある程度決定するものであるが、技術動向によっても変化する。例えば、導入時は拡張性が高かった情報システムであっても、その後、別規格の技術を採用する情報システムが増えれば拡張性は低下する。

一方、使用性に関しては、利用者側の意見を踏まえて評価することになるが、人の異動等を考慮すると、組織全体において統一性を持たせることが重要になる。当初は使い勝手が良かった情報システムであっても、他の情報システムにおけるインターフェースの変化や利用者の異動等にもないその評価が変化する可能性があり、定期的に利用者の意見を収集することが望ましい。例えば、以前は汎用機やオフコンによる CUI や、C/S システムにおける個別の GUI インターフェースが主流であったが、昨今ではインターネットの利用が進んだためブラウザによる操作を基本とした Web インターフェースの方が使用性が高いと考えられている。

## 5 - 6 改善・廃止

### (1) 情報システム等の改善

前述した情報システムの評価結果を踏まえ、当該情報システムの改善や見直しについて検討する。情報システムの評価が高く、問題が存在しない場合は、継続的な運用を図ることとなるが、通常、継続的な運用とともに、何らかの問題が発生する可能性が高い。問題を抱えたまま情報システムを運用することは、費用の浪費につながるだけでなく、新たな問題を誘発するリスクもともなう。したがって、問題に関しては、可能な限り速やかに対処しなければならない。

情報システム自体は必要性が高いものの、問題によって当初において想定していた効果が十分に上がっていない場合は、問題を解決するための改善策を検討し、適切な改善を行うことが必要である。技術的な問題では情報システムの改修が中心となるが、政策的な問題では業務改革や、組織的な体制や制度の見直し等が想定され、必要に応じて双方を組み合わせる。情報システムの改修が大規模になる場合は、前述した計画、開発、調達

各プロセスを踏まえて、情報システムの導入と同様の手順で改修を行うことになる。

もちろん、改善に際しては、問題を放置した場合のリスクや損失、改善策の実現性や費用対効果等を考慮することも不可欠である。問題の中には放置してもリスクが小さい反面、その改善には大きな費用を要するものもあり、情報システムが許容範囲内の効果を創出しているのであれば、無理な改善が必要ない場合もある。例えば、既存情報システムにおいて業務処理における非効率が存在し、月に5人日のロスが生じていたとする。表5-27と同様に計算すると、このロスによる損失は150万円である。したがって、情報システムの寿命があと3年であるならば、3年間の損失450万円が情報システム改修の目安の金額となる。改修費用が450万円未満であるならば、改修を行う価値があるし、それ以上であるならば改修を止めた方がよい。

なお、改修費用が高価であるため問題を放置した場合においても、情報システムのライフサイクルが終了し、刷新する際に必ず改善しなければならない。

## (2) 情報システムの廃止

必要性や有効性が低い場合、あるいは問題の解決が困難であり、かつ問題を放置した場合の損失やリスクが大きい場合は、情報システムの廃止の可能性も踏まえて、その対処を検討する。当該業務処理を継続する必要性が低い場合はもちろん廃止が望ましく、業務の継続が必要な場合でも関連情報システムに機能を吸収することで、当該情報システムを継続することの必要性は低くなる。必要性や有効性が低く運用費用が大きな情報システムの無理な延命は望ましくなく、速やかに廃止しなければならない。情報システムに限らないが、行政機関では一度、事業として開始したものは継続しようとするベクトルが働くようであり、廃止することが苦手である。特に情報システムの場合は技術的な部分を含め分かりにくいところがあるので、担当者が異動してよく分からない場合には、「とりあえず継続」ということになりかねない。このようなことが起こらないよう、きちんと評価

し、適切に廃止することが求められる。

情報システムを廃止する際には利用部門の意向を踏まえることが望ましいが、最終的には評価結果を踏まえてCIOが判断することになる。また、情報システムを構成していたハードウェア、ソフトウェアの廃棄に際しては、必要なデータのバックアップを取るとともに、廃棄したハードウェア等からデータを取り出すことができないように適切な廃棄を行う必要がある。廃棄業者に委託する場合は、廃棄方法や機密保持等について定めた契約を結ぶとともに、契約に違反した場合の損害賠償責任等についても契約に定めることが望ましい。

表5-29 データの廃棄方法

廃棄方法	概要
消磁	強力な磁気によってハードディスク等の中のデータを消去する方法であり、ソフトウェアで消去できない、壊れたハードディスク等についてもデータ消去が可能である。磁気媒体に保存されたデータを破棄する場合の主要な方法であり、媒体そのものを破壊する前に必ず行う。
破壊	データが入っている媒体そのものを破壊する行為である。焼却が困難な媒体のデータの破棄に有効であり、ハードディスク、CD-ROM、MO、MT等のデータ破棄に適用される。
消却、溶解	紙のデータを破棄するのに適した方法である。大量の紙の廃棄には外部の専門業者の活用が想定され、情報の機密性を保持するため、裁断等と併用することもあり得る。
裁断	気密性の高い書類データを破棄する場合に、焼却、溶解と併せて用いられる

## 総括

これまで何度か述べたが、情報化プロセスの大きな問題はEUCによって情報システムに携わる人が増えた反面、そのプロセスが標準化されておらず、属人的に処理されてきたことにある。しかし、自治体において情報化、あるいは電子自治体への取り組みをレベルの高いものにし、最適化に近付けるためには情報化プロセスにおける成熟度の向上が不可欠である。本章で示した情報化プロセスが、システム担当者等が業務を行う際の一種の指針となり、プロセスの成熟度向上に寄与することを期待したい。

本章で試みたのは情報化プロセスの標準化であるが、実際に情報化を推進する際には不確定要素もたくさんあり、利用者側が取捨選択、あるいは応用しなければならない部分が非常に多い。したがって、標準化に固執することは返って適切な対応を見誤らせる可能性もある。矛盾するようであるが、今回提示した情報化プロセスの枠に囚われない柔軟な業務の遂行も合わせてお願いしたい。