

## ***Part2.***

### **システムプロファイリングの基本的な考え方**

- 
1. 情報システム・ソフトウェアのプロファイル化.....31
  2. システムプロファイルの考え方.....34
-

## 1. 情報システム・ソフトウェアのプロファイル化

現状認識で述べた様に、「信頼性」とは概念であって、具体的な「もの」ではない。従って、情報システム・ソフトウェアの「信頼性」を明確に定義するためには、定性的な定義の他に、定量的な尺度定義と計測という行為を通じて認識する必要がある。定性的な定義とその啓発は、既に多くの場面で活用（国際標準 ISO/IEC9126（品質特性）など）されており、ここでは定量的な側面での定義に絞って、情報システム・ソフトウェアに対する信頼性に係る計量化と合意形成の礎となる尺度に基づくシステムへの信頼性要求水準の「ものさし」を議論した。

信頼性要求水準の「ものさし」としては、様々な重要インフラ事業者において模索中であるが、先進的な事業者においては「お客様迷惑度指数」、「SLA<sup>3</sup>レベル指数」、「社内組織の関与度指数」などを定量的な指標として採用している場合もある（具体的には別編（事例分析と対策（IT故障編））を参照）。しかし、これらはプロジェクト運営上の目標水準であり、それ自体が事業を司る「業務」、「システム」全般への信頼性水準としての位置付けにはならないと考えられる。国民生活に提供されるサービスとしての「ものさし」の位置付けとしては、公共性を持つことが前提であり、さらにそれらの各種属性の測定に関しては、「客観性」、「再現性」、「定量性」が備わっている必要があると考えられる。<sup>4</sup>

### （システムプロファイルとは）

「ものさし」は複雑で無く、スケールの粒度を直感的に把握して現状分析可能（実用的な「ものさし」）でなくてはならない。このため、本研究では、「信頼性」への「要求水準」を同定し、その要求水準に沿って情報システム・ソフトウェアのライフサイクルへの信頼性水準となるべきものという意味で、「システムプロファイル」と呼ぶこととする。この「信頼性」への「要求水準」としては、人命への影響度（システム故障により何らかの形態で人命への損害を与える影響度）、経済的な影響度（各事業者の機会損失を含めたシステム故障が引き起こす経済的損失の影響度）、および公共性への影響度（システム故障が引き起こした場合の国民への公共サービス提供の面からの影響度）の側面から、4段階のレベルを設けた。この4段階のレベルの考え方などに関しては図2-1、図2-2の通りである。図2-1は、分類分析の要因（人命への影響度、経済的な影響度、公共性への影響度など）を明確にして、情報システム・ソフトウェアに対するシステムへの信頼性要求水準（Type I から Type IV の4段階）と、その要求水準が情報システム・ソフトウェアに適用される場合の「システム」への信頼性要求水準（システムプロファイル）を示したものである。図2-2は、「システムプロファイル」に関わる様々な Type の判断とその情報システム・ソフトウェアの信頼性要求水準

<sup>3</sup> SLA(Service Level Agreement)とは、情報システム・ソフトウェアに対する信頼性、運用性、操作性などに関する定量的或は定性的な目標値を設定し、サービス受益者とサービス提供者間で合意する（契約事項にもなる場合もある）ものである。

<sup>4</sup> 機能安全国際規格（IEC61508）では、安全度水準（SIL：Safety Integration Level）としてレベルを4段階に分類し、低頻度作動要求モードとして作動要求あたりの設計上の機能失敗平均確率、高頻度又は連続作動要求モードとして単位時間当たりの危険側失敗確率（1/時間）で評価している。ソフトウェア製品の評価（ISO/IEC14598）（JIS X 0133）では、安全面、経済面、セキュリティ面、環境面での4段階のレベル定義をおこなっている。

実現のための手法を示したものである。信頼性要求水準を達成するための情報システム・ソフトウェアの実現においては、重要インフラ事業者における、リスク受容・回避・予防の判断を実施後、最終的な「システムプロファイル」を決定する必要があることを示している。

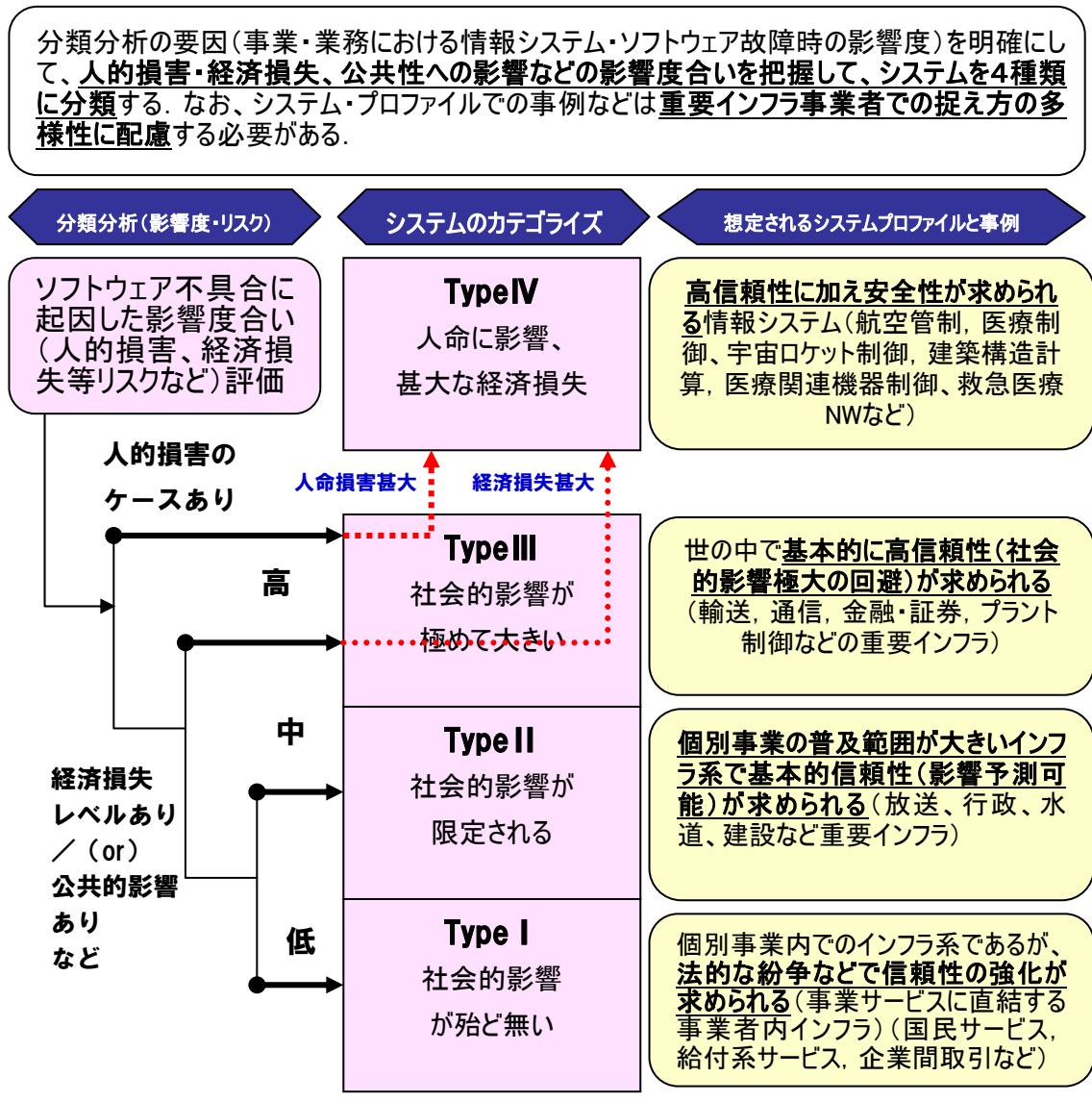


図2-1 システムプロファイルについて

信頼性のレベルを分析・把握する場合、当該システムの事業活動における位置付けの中で信頼性の相対的な「システム故障時の影響(リスク含む)」を把握・認識する必要がある。この「影響度」を信頼性の視点からの「システムプロファイル」と呼ぶ。

一方、重要インフラ事業者における影響度の判断は、事業・業務モデル構築における運用性、事業の大小等に依存し、人的損害あるいは経済損失に関する絶対的な尺度は業界横断的に決定できない。また、情報システム開発に関するシステムオーナー系とベンダ系の間でのリスク評価においては、相互の事業リスクの捉え方に違いがあり、一律に決定付けることは契約の面からも現実的では無い。

従って、重要インフラ事業者間で共有する最低限の「システム故障時の影響度」のレベル認識を合わせることに留め、リスク把握レベルの具体的な尺度設定に当たっては具体的な事業者で取り組んでいる事例を参考ベースで共有する方向とする。

### システムプロファイルの4階層とリスク

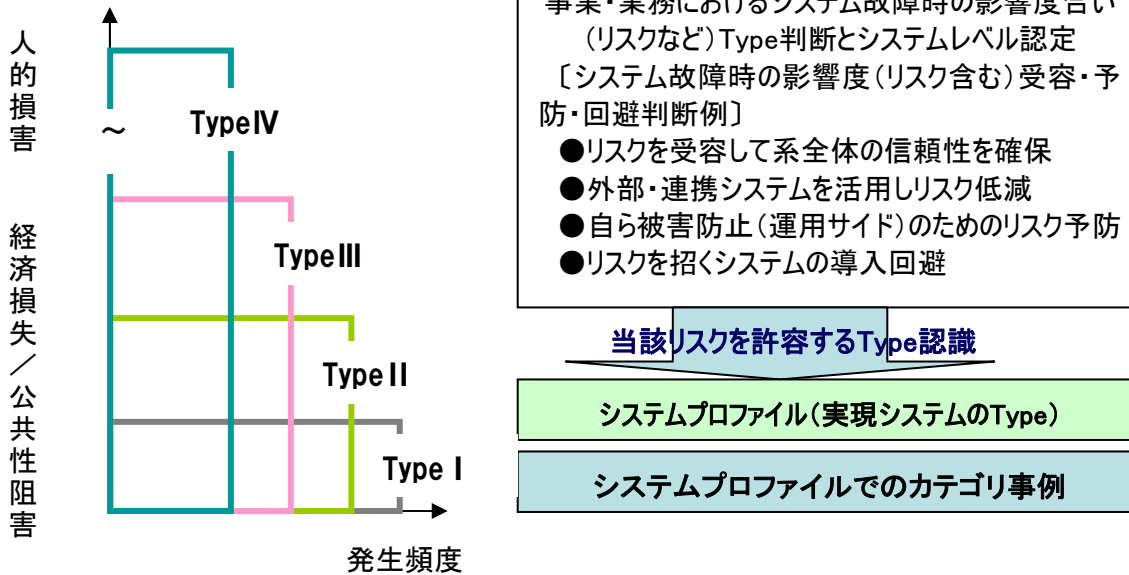


図2-2 システムプロファイルの考え方

## 2. システムプロファイルの考え方とは

本研究会及びWGにて議論された、「システムプロファイル」に対する考え方は以下の通りである。

- 信頼性要求水準に関しては、事業者が抱える事業の特性、提供環境、サービス受容者（国民など）の許容範囲などにより、事故対応リスクの強弱がそのまま情報システム・ソフトウェアへ反映されるものと考えられる、信頼性確保に関する認識が変化するものであるが、水準はこのまま4段階レベルが妥当と考えられる。
- 重要インフラの事業者が抱える情報システム・ソフトウェアの信頼性要求に関しては、経済損失（被害における機会損失なども考慮）、人命への影響、及び社会的あるいは公共性から見た影響度（被害想定人数などの大小などを考慮）した場合、信頼性要求水準はリニアに考慮して考えることにより、技術革新の変化、情報システム・ソフトウェアのコモディティ化、連携・統合等による影響範囲の規模の拡大など経済合理性の観点から「信頼性」を評価しやすい。
- 一般的に情報システム・ソフトウェアの「信頼性」の底上げを図ることを目的とすることと重要インフラの事業者が抱える情報システム・ソフトウェアの信頼性向上とは、結局同一局面で議論することで論点整理がしやすい。
- 重要インフラ事業者での情報システム・ソフトウェアのハイレベルな信頼性要求水準を検討対象としそのあり方、対策の仕方を明確にし、そのエンジニアリングの取り組みが普及した場合には、最終的には一般の情報システム・ソフトウェアへの適用も将来的に考えられ、国際的なレベルで「信頼性」強化を図ることができる。

実際に、個別事業者において「システムプロファイル」の考え方を採用しつつあり、適用効果としては以下が挙げられている。表2-1は日経コンピュータで発表された信頼性確保に関わる事業者の取組みを一部抽出・加筆修正したものである。

- プロファイリングを規定したことにより、「コストを全体最適できるようになり、システム発注者と開発者との間で、例えば、「障害件数を10%削減するにはこれだけのコストがかかります」と明確に合意できるようになった。採用されたプロファイルは業務重要度の3段階であった。（定量的な判断と合意形成の強化）
- 信頼性にメリハリを付けるべく4ランクに情報システムの信頼性を整理し、各ランクが目指す稼働率などの数値目標と実現にかかるコストをプロジェクトの最初期段階から利用部門に提示して、合意の上でシステム開発ができるようになった。（掛けるコストと信頼性の関係の説明責任能力の強化）
- 情報システムの信頼性に関わる稼働率、冗長化などの判断できる信頼性を4段階にメニュー化し、指標を作ったことで、重大な障害の発生原因の分析と事前対策の横展開という運用への変革に寄与し、関係者全員での関心事としてノウハウ・創意工夫を自然に創出してきた。（モチベーションの向上と強化）

この「信頼性」への要求水準の各レベルに対応して、大きく以下の2種類に分割して議論を進めた。

IT故障、情報セキュリティに関する「信頼性」の確保、保証に係るコスト（予防、評価などの自発的コスト、内部あるいは外部を起因とする故障などの非自発的コスト）のバランスを考慮し、システムプロファイルに沿った対策事例（推奨事例）と自己診断の方法を提示する。

情報システム・ソフトウェアへの信頼性要求水準の達成のための情報システム・ソフトウェア開発作業での「ものさし」（以降、「ソフトウェア開発リファレンス」と略記）に対応した不具合発生抑止（プロセス、プロダクトの両面からの発生抑止、阻害要因抑止）の対策を明示する。

表2-1 システムプロファイルの考え方に関する適用状況とその効果

社	背景	プロファイリングの状況	適用効果
A	会社設立当時から飛行の安全を守るため、航空機だけでなく基幹システムに対しても投資と訓練を続けている。だが会社の中のすべてのシステムに100%を求めるのは明らかに過剰投資。	業務上の重要度を3段階で規定し社内のシステムを当てはめている。	規定したことで「コストを全体最適でできるようになったし、それ以上に、システムの発注者と開発者との間で、例えば、『障害件数を10%削減するにはこれだけのコストがかかります』と明確に合意して話せるようになった」。
B	情報システム部門は、掛けるコストと信頼性の関係を明確に説明してこなかった。本来、その説明責任はあるにもかかわらずだ。	信頼性にメリハリを付けるべく、2004年ごろから150システムの信頼性を4ランクに整理。勇気を出して利用部門と折衝を始めた。	各ランクが目指す稼働率などの数値目標と実現にかかるコストをプロジェクトの最初期段階から利用部門に提示し、合意の上でシステム開発を進めている。
C	利用部門が『システムの信頼性はタダじゃない』と気づいてくれ始めるために、全社に意識が浸透するまで説得を続ける業務の重要性に応じてシステムの信頼性にメリハリを付け始めた。	稼働率やRTO/RPO（目標復旧時間/目標復旧ポイント）、システムをデータセンターに預けるのか、冗長化構成はどうするのか、などを4段階にメニュー化した。	指標を作ったことで重大な障害の発生原因の分析と次善対策を横展開する運用に変えた。これまではダウンしても担当者だけが忙しいという雰囲気だったが、今は全員が興味関心を持ち、自然にノウハウを出し合うようになった。

（出典）日経コンピュータ(2008年4月15日号)から一部抽出、  
加筆修正