Part 1.

重要インフラ情報システム信頼性研究会報告−総論

1. 重要インフラ情報システム信頼性研究会―設置の背景と目的

重要インフラ情報システム信頼性研究会設置の背景

近年、我々の社会生活の多くは、コンピュータシステムを応用した様々な機器やそれらを活用した様々な情報システムにより、制御・管理され提供されるサービスに支えられて営まれている。そして、これらの情報システムの中には、一般国民の生活に直結する重要な社会インフラとして機能しているものも存在する。一方で、これらの情報システムはネットワーク社会の広がりの中で他のシステムやサービスと連携しながら、その機能が常に拡大し、進化し続ける傾向にある。そして、これらの情報システムの進化はシステムとしての複雑化を加速させることにつながり、結果として様々な情報システムでのシステム障害の誘発原因となっている。

このような社会インフラとして利用されコンピュータシステムが何らかの事情により機能しなくなった場合、多くの国民生活に支障をきたすことは言うまでもなく、その信頼性を如何に担保していくかについて真剣に議論すべき時期にさしかかっていると考えられる。

重要インフラ情報システム信頼性研究会の目的と本報告書の位置づけ

上記のような背景のもと、独立行政法人 情報処理推進機構（IPA）では、経済産業省ならびに社団法人日本情報システム・ユーザー協会（JUAS）と連携協議し、3者を共同事務局とする「重要インフラ情報システム信頼性研究会」（以下、「研究会」という）を平成20年度より発足させた。この研究会では社会インフラとして広く国民生活に関係する情報システムの信頼性を確保するための具体的方策について、産業界・学術界の有識者の知見を集積し、技術的な方向性を見定めることを主たる目的とした。本報告書は研究会での議論を踏まえ、今後、どのようにして重要インフラ情報システムの信頼性を担保していくかについて、その方向性を整理したものである。

本報告書の構成

本報告書は本編を含め下記の 5 つのパートから構成される。

Part1：重要インフラ情報システム信頼性研究会―総論
Part2：システムプロファイリングの基本的な考え方
Part3：IT システム障害事例の分析と対策指針
Part4：情報セキュリティ・インシデント事例分析と対策
Part5：信頼性向上に向けたシステム開発共通リファレンス

このうち本編Part1はこの研究会の設置の背景と情報システム信頼性に関する課題認識ならびに本研究会の検討スコープとその検討の方向性について紹介し、研究会全体を俯瞰した報告となっている。

本報告書が想定する読者

本報告書は、前述した背景に基づきIPAが設置した重要インフラ情報システム信頼性研究会における議論を整理報告するものであり、下記の読者を想定している。

重要インフラ情報システム信頼性研究会に参画した関係者	重要インフラ情報システム信頼性研究会は後述するように重要インフラ情報システムの開発および運用に携わる事業者・ITベンダ、および業界団体代表者が参画している。本報告書は、これらの方々ならびに関係する方々が、本研究会の議論を踏まえ、それぞれにおいてその信頼性を向上する活動の参考にしていただくことを想定している。
重要インフラ情報システム信頼性研究会に参画した行政関係者	また本研究会には経済産業省に共同事務局としてご参画いただいたほか、行政サイドとして内閣官房情報セキュリティセンターにもオブザーバ参加をいただいた。これらの情報システムの信頼性などに関係する行政機関の方々についても、本報告書で整理した方向性や提言などを参考にしていただきたいと考えている。
重要インフラ情報システムの運用に携わる事業者	我が国には電力・ガスなどをはじめとして様々な領域で、国民の生活に深く関係する社会インフラを担う多数の事業者が存在し、その多くはコンピュータシステムなどを導入して事業推進を図っている。本報告書は、これらの社会インフラを担う情報システムの運用事業者の皆様方にも、それらの情報システムの信頼性確保の視点から参考にしていただきたいと考えている。
重要インフラ情報システムの構築に携わるITベンダ	情報システムの信頼性向上という視点において、直接、情報システム・ソフトの開発、運用・保守などにあたるITベンダが果たす役割は大きいと考えられる。重要インフラの信頼性向上については、インフラ事業者の視点およびITベンダの視点の両方の視点から、より合理的な方策を施していく必要がある。この点から、本報告書で報告する内容について、重要インフラ情報システムの事業者のみならず、それらの情報システムを実際に構築するITベンダの皆様方にも理解していただき、信頼性向上への継続的な取り組みへの参考としていただきたいと考えている。

重要インフラ情報システム信頼性向上に向けた期待	重要インフラ情報システム信頼性研究会は、国民の生活に深く関係する重要インフラで利用される情報システムの信頼性向上に向けた出発点として、議論に着手したものである。この研究会での議論を受け、広く重要インフラ情報システムに関係する部門ならびに関係者各位において、その信頼性向上に関する意識と行動のきっかけとなることを期待している。
重要インフラ情報システム事業者ならびにITベンダへの期待	本報告書に記載された重要インフラ情報システムの信頼性確保の方向性と施策について、さらなる具体化や精緻化といった課題が残されており、そのまま個々の事業体に適応することは難しいものの、参考にできる事項については、個々の事業体での議論を経て、できるところから速やかに日常の業務の中に反映していただくことを期待している。また、これらの情報システム信頼性に関する議論については、我が国を挙げて真剣に議論するテーマであることから、より多くの事業者、ITベンダの皆様からの様々な情報公開などによって、この分野の議論が活性化し、よりよいソリューションの検討や開発につながっていくことを期待している。
最終ユーザへの期待	多くの社会インフラ情報システムは、その先に最終的なサービスの受け手としての一般国民が存在している。情報システム信頼性に関しては、現在、一部、事業者やITベンダの問題にとどまらず、こうした一般国民にとっても重大な関心ごととなってきている。一方で、システム障害に関する様々な情報の狭間で、一般国民は情報システム信頼性に対する正しい認識を持ちえていないことも事実である。今後、本格的な高度情報化社会の到来に際し、情報システムのエンドユーザである一般国民も情報システムの信頼性に関して正しい知識を保持できるようにすることは極めて重要である。本研究会の議論を端緒として、事業者、ITベンダの信頼性に関する努力の結果により、一般国民も広く情報システム信頼性に対する正しい認識を有するようになることを期待している。

2. 重要インフラ情報システム信頼性に関する課題認識

重要インフラ情報システムとは

本研究会では、国民生活の基盤となる社会インフラの一部として利用される情報システムに関する信頼性確保を中心的なテーマとして議論した。これらを総称して「重要インフラ情報システム」と呼ぶこととする。

本研究会が議論の対象とした重要インフラ情報システムとは、具体的には電力、ガス、情報通信、医療、金融、行政サービス、あるいは物流といった国民生活を広く支える情報システムを想定している。特に、これらの情報システムの多くは、ある意味で公共性を有しているものが多く、またその代替の手段が限られてしまうものが殆どである。その点において、これら重要インフラ情報システムにおける瑕疵はあってはならず、逆にわずかでも信頼性側面において課題が残る情報システムは、広く国民生活に影響を及ぼしかねないことを理解すべきである。

重要インフラシステムの信頼性側面の特徴

上記のような重要インフラ情報システムに関しては、通常の情報システムよりは高いレベルの信頼性の実現が求められることは言うまでもない。このために、高度な信頼性実現に向けて情報システム構築段階およびそれらの情報システムの運用段階の各局面において、様々な工夫と取り組みをすることが求められる。

近年の情報システムの利用の広がり、特に国民の生活に直接的に影響を及ぼす重要インフラ事業における情報システムの広がりの中において、これらの情報システムに瑕疵があった場合、国民生活に少なからぬ支障をきたすことは言うまでもなく、その信頼性を如何に担保していくかについて真剣に議論すべき時期にさしかかっていると考えられる。

情報システムの信頼性とは

本研究会では、重要インフラ情報システムの信頼性に関する議論を行った。情報システム信頼性については、ISO や JIS などによって明確にその定義が与えられている。また、信頼性に関係が深い概念として、システム安全性や近年ではディペンダビリティといった概念も重視されるようになってきている。ここでは、本研究会の議論のベースとした情報システム信頼性に関する定義を与えておく。

情報システム信頼性	情報システム信頼性とは、「機能単位が要求された機能を与えられた条件のもとで与えられた期間実行する能力」をいう。 （JIS X0014　情報処理用語　−信頼性・保守性および可用性）
システム安全性	システム安全性とは、「システムが規定された条件の下で、人の生命、健康、財産またはその環境を危険にさらす状態に移行しない期待度合い」をいう。 （JIS X0134　システム及びソフトウェアに課せられたリスク抑制の完全性水準）
情報システム・ディペンダビリティ	また近年は、信頼性や安全性を包括するさらに上位の概念としてディペンダビリティが重視されるようになってきている。ディペンダビリティとは「情報システムが提供するサービスが正確で信頼できる度合い。人が安心して情報システムに依存できる性質であり、フォールトトレラント（耐故障性）、フォールトアボイダンス（避故障性）や情報セキュリティなども含め信頼性、安全性、可用性などの複合的な性質を総称した概念」をさすのが一般的である。
本研究会における情報システム信頼性の議論の範囲	情報システムの信頼性や安全性に関しては、上記のように多様な定義や考え方が存在するが、本研究会の最大の関心事は、国民生活に深い影響をもつ重要インフラを支える情報システムが、継続的に安定して稼動することをどのように保証し、それによってそれらのサービスの最終ユーザである国民生活を如何に守っていくかという点にある。この点からは、本研究会での議論は情報システムの信頼性という概念を越え、情報システム・ディペンダビリティまで含めた広範な情報システムの安全・安心に関する技術にフォーカスして議論を行った。

重要インフラ情報システムの信頼性に関する課題認識

上記のような定義において、重要インフラを支える情報システムの信頼性について現状を省みると、情報システムの利用拡大の一方で、その信頼性やセキュリティの確保に関する有効な解決策が十分に議論され整備・実行されているとはいえない。その結果として、今に至るまで重要インフラを支える情報システムにおいて、非意図的若しくは意図的なリスクが顕在化することによる様々なシステム障害が報告されているのは周知のとおりである。このため、重要インフラ事業者やITベンダなど関係するステークホルダの知見を集積し、情報システム信頼性・セキュリティの向上に向けた解決策を、早急に議論し実行に移すことが求められている。

3. 研究会の検討スコープと基本姿勢

本研究会の検討スコープ

本研究会では、前述した重要インフラに関わる情報システムの広義の意味での信頼性を議論の中心的な対象とした。これらの情報システムでは、コンピュータシステム自身が重要インフラの事業根幹を成す場合が殆どであるため、時として、これらの重要インフラに関わる事業そのもの、あるいは、ビジネスそのものの信頼性と密接な関わりをもつこととなる。このため、重要インフラ情報システムの信頼性の議論は、それらを利用する事業そのものの信頼性の議論と分離せずに議論されてしまう場合が少なくない。

しかしながら、信頼性という要素については、コンプライアンスやコーポレート・ガバナンスに代表されるビジネスそれ自身の信頼性とビジネスを支える情報システムの信頼性は次元や局面が異なると考えられる。このため、情報システムの信頼性の議論においては、ビジネス固有の信頼性に関する問題は切り離し、情報システムとビジネスの相互作用が存在する領域までをスコープとして議論することが望ましい。

このような事項を踏まえ、本研究会では重要インフラ事業を支える情報システムの信頼性を主たる議論の対象とし、その議論の主体は、コンピュータを利用したシステムとしての情報システムの信頼性を如何にして確保し、向上していくかを中心的なテーマとして扱ってきた。この点において、本研究会の議論における技術的な領域は、情報処理技術及びソフトウェア・エンジニアリングとしての情報システム信頼性の確保と向上が主要な論点となっている。

重要インフラ信頼性向上における基本的な姿勢

一方で、重要インフラ事業の中心的な役割を担う情報システムは通常、これらのサービスの提供者である重要インフラ事業者が中心となってそのサービスの中で運用されている。また、その一方で、これらの情報システムの開発にはITベンダが広く参加し開発が行われるのが一般的である。このため、これら重要インフラ情報システムの信頼性向上においては、情報システムの運用ユーザである事業者と開発を担うITベンダの双方が参画し協力していくことが必要となる。本研究会では、これらの重要インフラ事業者やITベンダ双方の視点や、重要インフラ事業の最終ユーザである国民の視点をも考慮し、議論を進めてきた。

重要インフラ信頼性問題の主たる要因

重要インフラ情報システムの構築ならびに運用に関してそれを担う事業者、ITベンダは既にその重要性やそれに伴う信頼性に関して十分な認識を持ってその任に当たっていると考えられる。しかしながら、こうした関係者の真摯な努力の一方で、それを上回るシステム規模の増大や複雑さがシステム障害を誘発している一因と考えられる。

通常の情報システムにおいて、システム障害が発生する要因は大きく分けて次の3つのパターンがあるといわれている。

システムに内在する不具合

情報システムを構成する中心的な要素は、いわゆるコンピュータを制御するプログラムである。近年の情報システムは、機能の進化やそれに伴う複雑さの増大などによって、プログラムとしての正しさを確実にすることが極めて難しくなってきている。結果として、これらのプログラムを開発する過程において、不具合を混入してしまう場合が少なくなく、それらがシステム障害の直接的な要因となる場合が少なくない。

システムの運用に起因する誤り

情報処理システムは通常、それを操作するオペレータを含めて一つの系として機能を果たすものである。従って、システムとしての運用時の機能という点においては、オペレータや運用時の環境や状況なども含めた視点が重要となる。こうしたシステムの実運用の局面においては、オペレータの操作や周辺の動作環境や動作条件の影響によって、さらには、エンドユーザの利用形態によって、システムが想定外の状況に陥り、システム障害が発生する場合も少なくない。

第三者の攻撃による障害

また、近年の情報処理システムの多くは、ネットワークに接続されたり、ネットワークを介して様々なデバイスに接続されることで、システムの利用者とは直接的に関係しない第三者が悪意をもった攻撃を仕掛ける余地が増大している。システム障害と呼ばれるものの中には、こうした第三者の攻撃によって引き起こされるものも少なくなく、いわゆるシステムセキュリティ面における脆弱性がこのような攻撃の発端となる場合が多い。

重要インフラ信頼性向上における検討の基本方針

本研究会では、上記のような情報システムにおける信頼性の低下を引き起こす要因を考慮し、それらの要因を如何にして除去するかという点を出発点として議論を進めた。また、その前段として、情報システム信頼性の評価軸についても、合わせて検討を行うこととした。

4. 研究会における課題検討のテーマと体制

課題検討の方向性検討のヒント

前述のように一般的な情報システムの信頼性に問題が生ずるのは、「システム自身の不具合」、「運用段階での環境不適合」、「悪意のある第三者による攻撃」のいずれかによると考えられる。そして、これらの要因によって、現実の情報システムでは様々な障害が発生している。このような状況の中で、どのような方向性をもって重要インフラ情報システムの信頼性を向上させていくかを考えていく必要がある。このためのヒントは、情報処理システム以外の先行する領域での取り組み事例などを参考にすることができる。

他分野での基本的な動向

情報システム以外の他分野に目を移しても、例えば、航空機などの分野でも同様の要因によって事故が発生する図式は殆ど同じである。航空機の分野では、航空機開発の中で、機械工学、電気・電子工学、材料科学などの知見を動員し、航空機自身の不具合を極力少なくしている。また、同時に、運用面での誤りを除去すべく、その乗員や整備などでも専門家を養成し、徹底した管理のもとに運行されている。また、悪意のある第三者―例えばハイジャックなどへの対処は既に一般に周知されているように厳重な仕組みが用意されている。また、航空機の分野では、ひとたび事故が発生すると、徹底した事故調査による事例分析を行い、再発防止に向けた取り組みがなされている。

安全工学分野からの考え方

一方、化学プラントなどの分野で先行する安全工学の領域では、近年、機能安全という考え方が確立されつつある。機能安全とは、「機器やシステムで実現する機能実現とその安全性を同時に担保する考え方」であるといえる。機能安全については、IEC61508[1]などの国際規格が規定されているが、その中の重要な概念として事前安全計画、事後安全計画といった考え方が提唱されている。

①事前安全計画

システム開発の前段階で徹底した開発リスク分析を通し、予見される開発上の障害やシステムの障害に対し事前に対策を講じていく。

②事後安全計画

実際に運用に入ったシステムにおいて、発生した障害事例を分析し再発防止に向けた積極的な活動に結び付けていく考え方。

[1] IEC61508/2000 年発行
Functional Safety of electrical/electronic/programmable safety-related systems

課題解決に向けた方向性

こうした他分野での事故防止や再発防止に向けた取り組みのスキームは、本研究会が扱う重要インフラ情報システムの信頼性の問題の解決の枠組みとしても参考になる部分が多いと考えられる。上記の航空機の例などを参考にすると、重要インフラ情報システムの場合、次のような枠組みで考えていくのが有効であるといえる。

重要インフラ情報システムの類型化に対する枠組みの検討

本研究会が議論の対象とした重要インフラ情報システムは既に前述したとおり、電力・ガスや運輸、金融まで様々な事業領域に関係している。そしてそれら多岐にわたる情報システムの機能や役割は、事業ドメインごとに様々であり、それらに求められる信頼性や安全性の程度も様々であると考えるのが適切である。このため、信頼性向上に向けた施策を考える場合にも、個々の事業ドメインや情報システムの特性を十分に考慮しなければならない。このため、情報システム信頼性の検討の第一項目としては、様々な事業ドメインにおける情報システムを情報システム信頼性の視点から類型化し、そのパターンやグループ毎の信頼性向上施策を考えるための枠組みを与える必要があるといえる。

重要インフラ情報システム構築段階での信頼性確保

コンピュータを利用したシステムとしてみた場合、重要インフラ情報システムは、通常のITシステムと構造面では大きな差異はないと考えることができる。あえてその違いを述べるとすると、システムやデータの二重化や堅牢な処理アルゴリズムの実現、システム脆弱性の徹底的な排除などをあげることができる。また、一方で、これらの情報システムの開発過程、いわゆる開発プロセスに目をやると、信頼性要素を確認し織り込んでいく作業を開発プロセスの中にどのように組み込んでいくかが重要となると考えられる。情報システムの信頼性要素を確認し織り込んでいくための仕組みとしては、レビューやテスト、あるいは徹底した検証などが考えられる。高度な信頼性を求められる情報システムの開発においては、これらの作業を抜けなく、確実に実施することが必要である。このためには前述の事前安全計画とリンクしながら、ソフトウェア・エンジニアリングの手法を有効に機能させていくことが求められる。

重要インフラ情報システムにおける事後安全計画の実現

一方で、実際の情報システムの運用フィールドで発生する様々な事象やトラブルに関して、速やかかつ厳密に分析し、その結果を開発や運用にフィードバックしていくことも、情報システムの信頼性向上の上では極めて重要な活動であると考えられる。この活動は、基本的に安全工学で言うところの事後安全計画の徹底に他ならない。フィールドでの様々な事象や障害を徹底的に分析し、それらの発生の直接的、間接的原因を特定し、その本質的な要素を知として蓄積し、技術に反映していく活動の枠組みを早急に整備していくことが求められる。

情報セキュリティでの信頼性確保

さらに悪意をもつ第三者による攻撃に端を発するセキュリティインシデントに対して、その攻撃を未然に防ぎ、また攻撃の影響を局所化するといった情報セキュリティでの信頼性確保と向上も重要な課題の一つであると考えられる。情報セキュリティでは、情報システムを実装する各構成要素でのセキュリティ対策が重要となる。

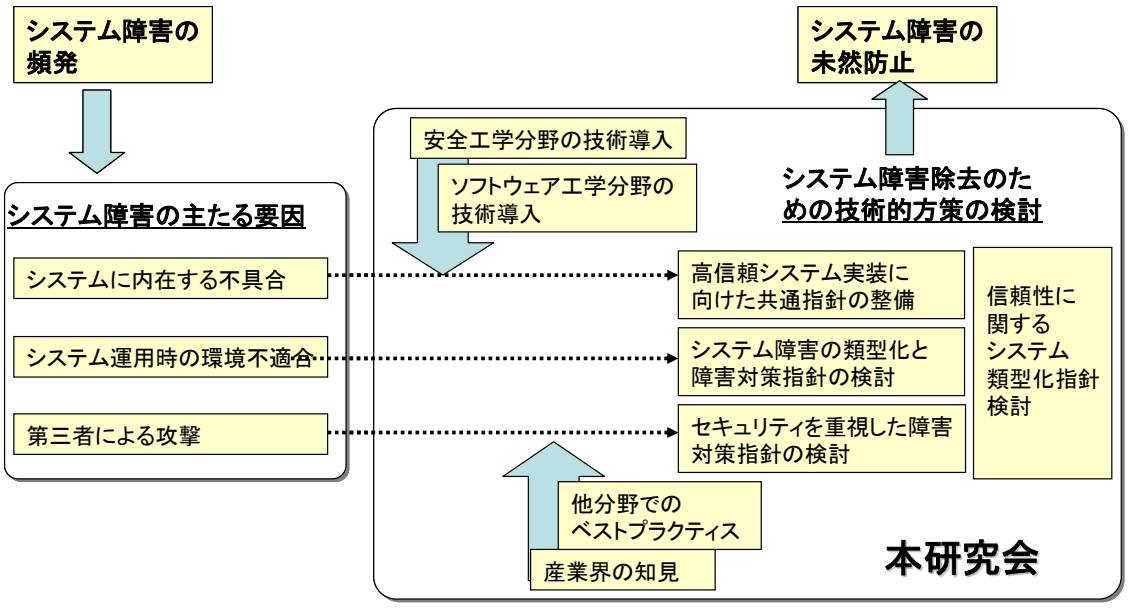


図１－１　本研究会の狙い

本研究会において議論したテーマと体制

本研究会では、前述の方向性に基づき、次のテーマを取り上げ検討を行った。

テーマ1： 信頼性に関する情報システム類型化指針の検討 （情報システムプロファイリングの検討と提案）	情報システム信頼性を議論するためのベースとして、対象となる情報システムの特性を評価し、情報システムを類型化して信頼性対策を議論するための枠組みについて検討した。この検討に当たっては、人命の損失に直結しやすい制御系・組込み系のソフトウェア開発における品質コントロールに関する先行した取組みとして、IPA/SEC の組込みソフトウェアプロジェクトで策定された「組込みソフトウェア開発向け品質作り込みガイド(ESQR[2])」における情報システムプロファイリングの考え方を参考に議論を行った。情報システムプロファイリングの基本アイデアは、情報システムの最終ユーザ視点に立ち、システム障害による経済的な損害、人的な損害などを定量的かつ段階的に評価するフレームである。 この検討は、研究会の全体会の中で実施し、その結果は本報告書のPart2で詳しく紹介する。
テーマ2： システム障害の類型化と障害対策指針の検討・提案	重要インフラを支える情報システムに関しては、重要インフラ事業者やITベンダの努力にもかかわらず、様々なシステム障害が報告されている。これらの報告されたシステム障害を分析し、そこからシステム障害の原因や対策を分析整理する仕組みを構築することは極めて重要であると考えられる。 具体的にはシステム障害の分析振り返りの中から、他システムの開発や運用の参考とすべき事項を抽出し、類似の障害の発生を未然に防ぐためのチェックリストの検討を行った。この活動は、情報システムの安全や信頼性を考えた場合、事後安全計画の実現に向けた仕組み作りの第一歩として位置づけることができる。このテーマの検討は、日本情報システムユーザー協会の協力により本研究会のWGとして検討した。検討の結果については、本報告書の Part3に詳細を紹介する。

[2] ESQR:(Embedded System development Quality Reference)
ISBN978-4-7981-1884-0/2008 年発行　翔泳社 Part2 参照

テーマ3： 情報セキュリティを重視した障害対策指針の検討と提案	ネットワーク技術を基盤とする近年の重要インフラ情報システムでは、悪意のある第三者による攻撃からの防御の仕組みを確実に備えることが求められる。このため、本研究会では社会インフラの一部を構成する情報システムに関して、実際に発生した情報セキュリティ脆弱性に関わる情報セキュリティインシデント事例の分析に基づき、どのような種別のセキュリティインシデントがあるかを調べ、その原因の分析と類型化を試みた。また、その結果をもとに、情報システム開発の各段階でのセキュリティ面強化に関する具体的な対策を検討した。このテーマはIPA 情報セキュリティセンターの協力の下、本研究会のWGとして検討した。
テーマ4： 高信頼システム実装に向けた共通開発指針の検討と提案 （共通リファレンスの検討と提案）	情報システムの信頼性については、その構築過程での工夫が重要な要素となる。特に、信頼性向上のために情報システム内にどのような仕組みや機能を保持させるかといったシステムアーキテクチャ面からの検討は重要である。また、一方でこれらのアーキテクチャ面の工夫も含め、開発の過程で信頼性側面に関して、どの程度、検討し確認したか、あるいは信頼性の側面からのテストをどの程度実施したかなど、開発作業の十分性やその結果の妥当性確認なども評価していく必要がある。既に組込みシステム分野では IPA/SEC の組込みソフトウェアプロジェクトによって「組込みソフトウェア開発向け品質作り込みガイド(ESQR)」が整備され、その中で、開発プロセス面からの品質作り込みに向けた品質コントロール概念とそのための指標などが公開されている。本研究会では、このESQRを議論のベースとして、重要インフラ情報システムの開発過程における信頼性の定量的コントロールのための基本的な考え方を検討した。検討はIPA/SEC 組込みソフトウェアプロジェクトの協力のもと、本研究会に参加する委員企業を交えたWGで検討を行った。

図１－２　本報告書の位置付けと想定する読者

本研究会の目的

社会的に影響の大きい情報システムを運営する事業者（重要インフラ事業者等）にとって、費用対効果が高く効率的にシステム障害の発生を減少させ、システム信頼性を向上させるソフトウェア・エンジニアリング手法・技術等の確立を目指す。

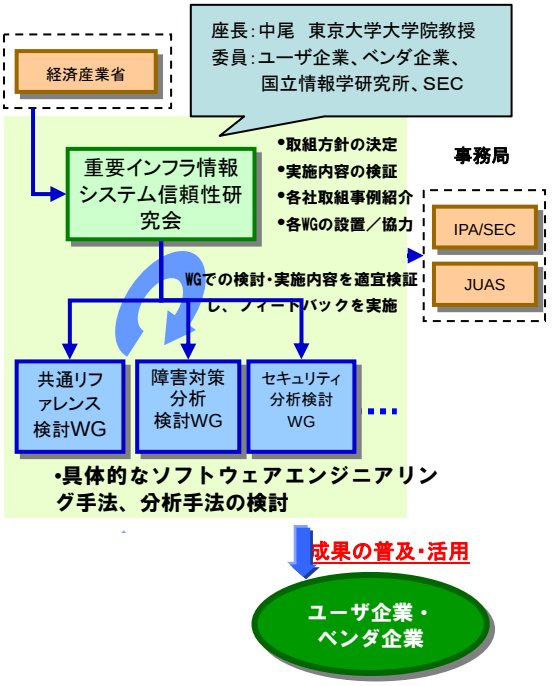
本研究会の目標

■障害対策分析によるシステム障害の再発・拡大防止のための手法の確立

ーシステム障害に関する原因分析に留まらず、障害対策分析を実施し、再発・拡大防止のための手法を確立する。

■情報システムの信頼性を評価するための手法の確立

ー定量指標に基づくシステム開発において、メトリクス（管理指標）に関する共通リファレンスを策定する。



本研究会のアウトプット

1. 障害対策分析による再発・拡大防止のための知識体系 or ベストプラクティス or ノウハウ集（障害対策分析チェックリスト）

2. 重要インフラを対象とした定量指標に基づくシステム開発において、以下の3つの共通リファレンスを策定
   - A） システムプロファイリング基準
   - B） 高信頼性評価指標（プロセスメトリクス、プロダクトメトリクス）のリファレンス値
   - C） 高信頼性基準を実現する（作り込む）ための手法（技術、人材、組織、支援体制）

スケジュール

8/6　第１回研究会
（趣旨説明・進め方議論）
9/5　第２回研究会
（ＷＧ活動の検討議論）
12/16　第３回研究会
（ＷＧ報告，研究会報告書の素案等議論）
2/23　第４回研究会
（研究会報告書案議論）

図１－３　重要インフラ情報システム信頼性研究会について

5. システムプロファイリングの検討と提案

システムプロファイリング検討の背景

通常、情報システムがどのような役割を担い、それに対応して、どの程度の信頼性を求められるかは、対象とする情報システムの特性によって異なると考えられる。これは、本研究会が対象とする重要インフラ情報システムにおいても同様である。

しかしながら、情報システムの信頼性の議論の出発点となるシステム毎の特性や各システムが有する信頼性側面に関するリスクの捉え方については、明確な指針が提示されていない。

本研究会ではこうした背景を考慮し、重要インフラ情報システム信頼性の議論の端緒として、情報システム信頼性の側面から見たシステムリスクの捉え方の基準をシステムプロファイリングとして整備することとなった。この検討については、ベース資料として ESQR(本報告 P17 下段)を参考に議論した。

システムプロファイリングの基本アイデア

情報システムの運用時に発生するシステム障害はそのユーザに様々な影響をもたらすと考えられる。中でも特に注視すべき影響として、ユーザに対する健康被害の有無や経済的損失の有無、あるいはその被害額などの被害程度を考えていくことが極めて重要になる。また社会インフラを構成する要素としての情報システムの場合、公共性なども重要な要素となる。今回、検討したシステムプロファイリングは、情報システムが不幸にしてシステム障害を発生した場合を想定し、そのユーザに健康面、経済面でどの程度の影響を及ぼすかを数値として客観的にとらえ、その程度によって情報システムに求められる信頼性水準を下記の 4 タイプに区分する考え方を採用している。

Type-1: 社会的影響が殆どない
Type-2: 社会的影響が限定される
Type-3: 社会的影響が極めて大きい
Type-4: 人命への影響、甚大な経済損失が予想される

システムプロファイリングの利用法

今回検討したシステムプロファイリングは、情報システム信頼性の議論のベースになる考え方であり、このプロファイリングスケールに基づき障害事例分析や障害を未然に防ぐ手法やメトリクスの体系化を進めていくことが必要になると考えている。

特にシステム開発時おいては、その信頼性や安全性、品質などの目標値を設定する際に、当該システムにどの程度の水準の信

頼性が求められるかを、このシステムプロファイルを利用して客観的に評価し、目標設定を行うことを想定している。このためには、本報告書の Part5 に示す共通リファレンス（信頼性指標）と連動した利用方法が重要になると考えている。

また、情報システムの事後安全計画の視点などからは、システム障害の分析・評価や類型化を行う際の、システムカテゴライズの区分目安として利用することを考えている。これについては本報告書の Part3 および Part4 でその考え方を紹介する。

システムプロファイリングの普及に向けて

本研究会で提案したシステムプロファイリングの考え方は、情報システム信頼性を議論するうえでの出発点となる考え方である。今回の提案は試案として検討されたものであり、細部に関しては賛否両論、様々なご意見があると考えている。しかしながら、そうした関係者間でオープンな議論を通して、システムプロファイリングの考え方が我が国における情報システム信頼性の議論の機軸として成熟し、利用されることを期待している。

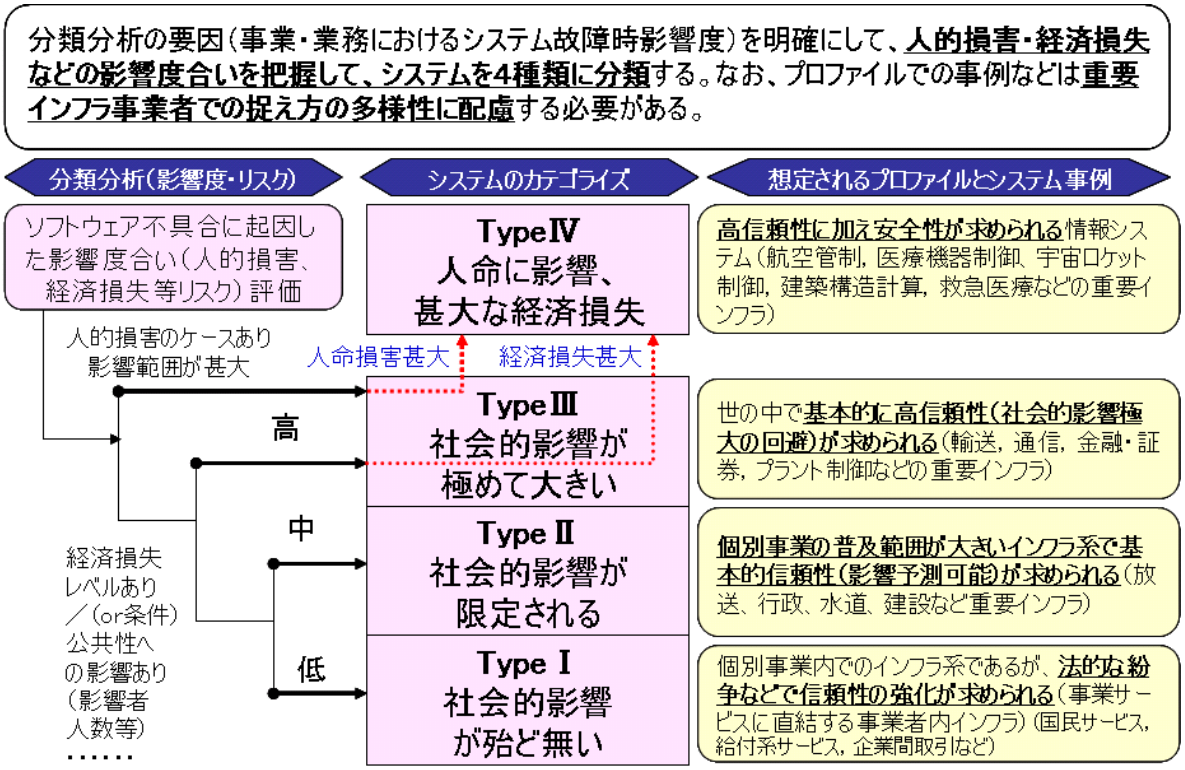


図１－４　システムプロファイルについて

※ESQR SCP(System Characteristics Profiling)をもとに加筆・修正

６．　システム障害の類型化と障害対策指針の検討

障害分析と対策検討の背景

先に他分野の事例として航空機のケースを例に引いたが、この例に見るまでもなく、様々な分野で発生する障害に関しては、それらの再発防止の視点から事後安全計画としての障害分析やそこからの知見のフィードバックが重要視されている。これに対し、情報システムの場合には、コンピュータシステム、とりわけその構成要素であるソフトウェアが対象となる場合が殆どであり、障害事象の可視化や原因分析が難しいといった側面がある。結果として、実フィールドで発生する様々なシステム障害に基づく再発防止策の立案など対策へのフィードバックが十分行われていないといったことに繋がっている。このため本研究会では、システムのユーザ団体の協力の下、実際の障害事例を分析し、そこから障害再発防止対策の整備に向けた検討を実施することとなった。

障害分析と対策検討に向けたアプローチ

障害事例の分析と対策検討に関しては、2005 年 7 月以降 2008 年末までのマスコミで公表されたシステム障害事例（約 100 事例,12 社）を精査し、主に以下のアプローチで検討した。
なおこれらについての詳細は、本報告書Part3で詳細に紹介する。

障害原因作り込みフェーズに関する類型化分析	ライフサイクルでの各段階で、システム障害事例における障害原因の作り込みが行われたのかの分析。
障害発生要因分析と対策分析	１２社において現実に発生したシステム障害およびその発生要因と対策、対策立案実行に関わる役割分担に関する個々の事例分析。
障害対策に関するコスト分析	「信頼性」に関わる対策コストの定量的な要因と尺度と、その結果としてのシステムプロファイルとの関係。
障害再発防止に向けたチェック項目と診断方法	上記を反映した情報システム・ソフトウェアのライフサイクル段階での利害関係者が信頼性確保のために共有すべきチェック項目とその個々の対策についての診断方法。
障害事例から分析した評価指標の検討	上記を反映した情報システムレベルで不具合予兆の発見、検出、検証などをプロアクティブにコントロールするための障害事例から分析した評価指標の整備。

障害再発防止チェックの普及について

今回、研究会で検討したシステム障害分析のスキームに基づく障害分析への取り組みは、他分野の例を見るまでもなく情報システムの信頼性を担保する上で極めて重要な活動であることは言うまでもない。これから得られたシステム障害の再発防止に向けたチェック項目は、重要インフラ情報システム分野でのいくつかの事例分析をもとに策定した試案である。今後、本試案をもとに、関係者の皆様の意見反映を進めながら、システム障害再発防止に向けた適切な障害分析のフレームと再発防止のチェック項目の整備を進めるとともに、チェックリストを現場に適用するためのガイド等を用意することにより個々の事業体で普及が進み、情報システムの信頼性が確保されることを期待している。

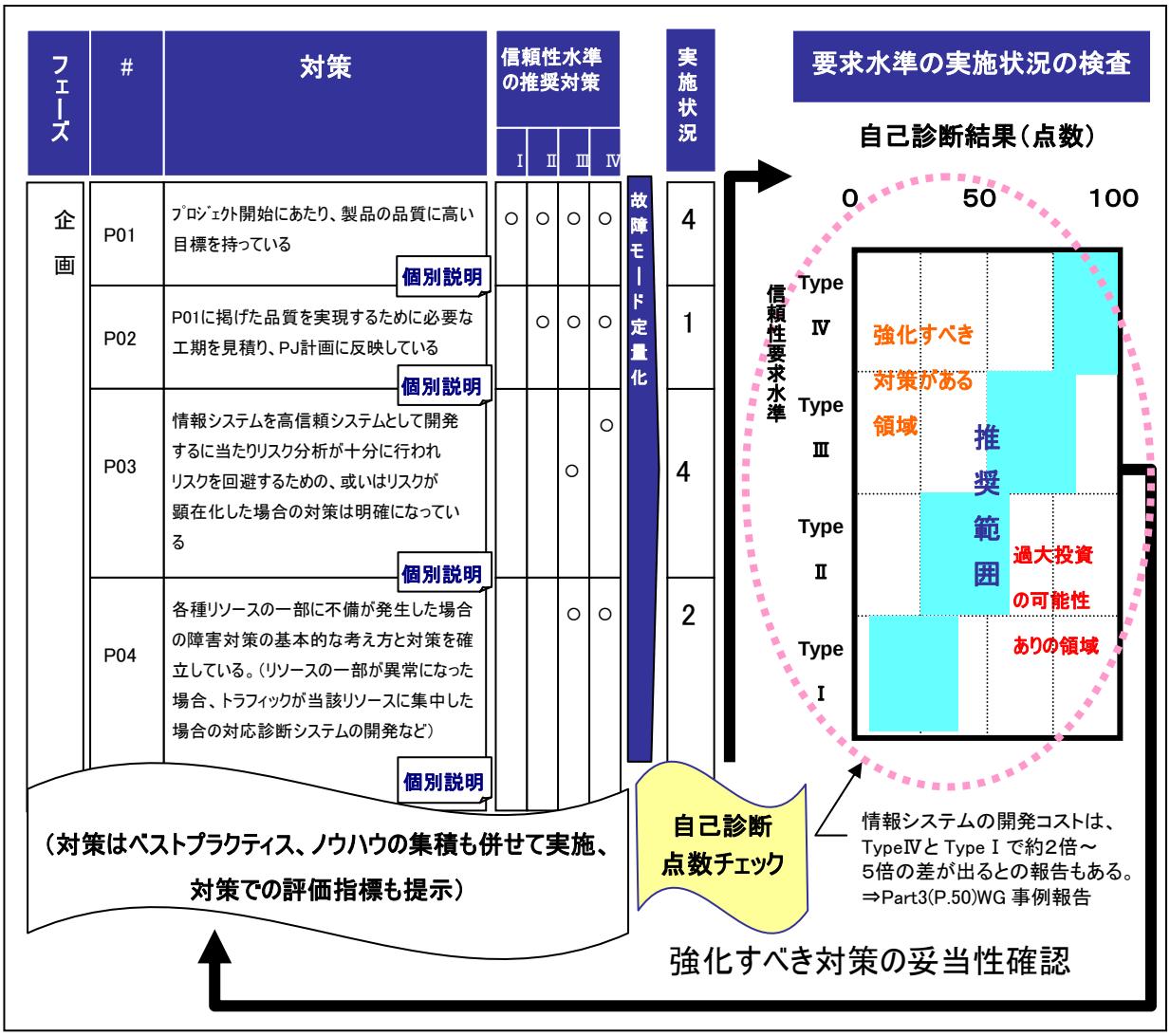


図1－5　信頼性向上対策と自己診断スキーム

7. 情報セキュリティを重視した障害対策指針の検討

情報セキュリティを重視した障害対策検討の背景

近年の情報システムの多くは、インターネットなどを介し情報システム外の様々なリソースへの接続が当たり前となってきている。これに伴い、情報システムのセキュリティ脆弱性を狙った第三者による攻撃によるシステム障害やセキュリティインシデントの発生が問題となりつつあるが、これらに関しての未然防止や再発防止策の策定が急務となっている。このため、本研究会では重要インフラ情報システムにおけるリスクとして情報セキュリティを捉え、国内外の情報セキュリティインシデント事例をもとに、それらの原因分析から再発防止策を洗い出すこととした。この検討に当たっては、重要インフラ事業者および情報セキュリティ有識者を委員としたWGを組織し、検討を実施することとなった。

検討にむけたアプローチ

上記の情報セキュリティインシデントの分析とそれに基づく再発防止策の検討に当たっては、以下の点について順次検討を進めた。

情報セキュリティインシデント事例分析

情報セキュリティに関しては、様々なセキュリティインシデント事例がメディアなどで公開されている。今回の分析では、2000 年から 2008 年の間に国内外で発生し、公開されたセキュリティインシデント事例 58 件を収集し、分析を行った。分析に当たっては、それぞれのセキュリティインシデントを体系的に整理し、分析するため、「不正アクセス」、「Winny の不適切な使用」、「システム構築時の問題」、「関係者の過失、または不正行為」、「フィッシング」の 5 つの視点で原因を体系化した後、より具体的な 12 の原因要因に区分する形で上記 58 件を分類し調査し、これより障害分析表を作成した。

再発防止策の検討

上記で作成した障害分析表から、これらの障害の再発に有効と思われる知見 21 種類を再発防止策として抽出し、これらを情報システムの「企画⇒開発⇒保守⇒運用」のライフサイクル毎に区分し、開発のどの段階でどのようなアクションをとるべきかを整理した。また同時に、対象となる情報システムの種別という観点から、システムプロファイリングの議論を参考にLv1 からLv4 までの4つのセキュリティレベルに対象システム群を整理し、これらの対象システム群と再発防止策のマッピングも取ることとした。本研究会で議論の対象となる重要インフラ情報システムは、Lv4（重要インフラの基幹情報システム）ないし Lv3(企業の基幹システム)に位置づけられる。この再発防止策の検討結果に

ついては、下記に示すような再発防止策一覧表として整理した。

情報セキュリティ障害対策の普及に向けて

本研究会では、議論のベースとして公開されている情報セキュリティインシデントの分析をもとに障害対策の検討を行った。今回提示するものは、再発防止に向けた一つの考え方であるが、実際の事例をもとに洗い出された再発防止策であり、実際の企業活動の現場でも十分に参考にしていただけるものと考えている。しかし、その一方で、情報セキュリティの分野では情報技術の進歩に伴い、セキュリティ対策も常に進化していく必要がある。この点からは、

・セキュリティインシデントに関する公開情報のみでなく、より詳細かつ具体的な情報の共有や分析、またそれらに基づく最新の障害対策の検討

・IT 人材の流動化、海外アウトソーシングの増加等情報システムをとりまく環境の変化も考慮した脅威分析と情報セキュリティ対策の策定

なども今後の課題と考えている。

表１－１　情報セキュリティ再発防止策一覧表（抜粋）

LV4	企画	L4-P1	外部からの意図した攻撃（DDoS: Distributed Denial of Service攻撃など）に耐えうるインフラ（ネットワークやサーバ等）が検討されている。
	運用	L4-U1	関係者の承認を得たソフトウェアのみをインストールできる仕組みが整備されている。
		L4-U2	関係者へのセキュリティ教育が行き届いており、セキュリティインシデント規約（関係者連絡先、メディア対応など）に基づく模擬訓練も行われている。
LV3	企画	L3-P1	外部からの攻撃を想定したセキュリティポリシーを定めている。
		L3-P2	利用者がシステムに対する悪意を持った場合を想定したリスク分析を行っている。
		L3-P3	システムの一部が侵入を受けた場合でも、その影響を局所に限定する仕組みが明確になっている。
		L3-P4	セキュリティインシデントに対応する体制（CSIRT: Computer Security Incident Response Team）が整備されている。
:	:	:	:
LV1	開発	L1-D1	セキュリティに関するソースコードレビューが行われている。
		L1-D2	ウェブアプリケーションに対するペネトレーションテスト（クロスサイトスクリプティングやSQLインジェクションなどの脆弱性のテスト）が行われている。

8. 高信頼性システム実装に関する共通開発指針の検討

共通開発指針の検討の背景

既に述べたように、情報システム信頼性を実現するためには、その開発過程においてレビューやテストなどによる確実な信頼性側面の確認などが必須となる。これに関しては、既にソフトウェア・エンジニアリングの分野で様々な考え方が提案されている。しかしながら、こうした活動の十分性を評価し、情報システム信頼性をその開発過程で定量的にコントロールしながら作り込んでいくための標準的な考え方は、必ずしも十分に整理されていない。結果として信頼性や品質作り込みは開発者の経験によるところが多く、最終的な情報システムの信頼性水準の達成度にばらつきを生じさせている。このため本研究会では情報システムの信頼性を開発過程で逐次確認・評価し、その中で情報システムに求められている信頼性水準に近づけていくための定量的なコントロール手法の整備について共通リファレンスとして検討することとした。

共通リファレンスの基本アイデア（システム品質の「見える化」と「測る化」によるコントロール）

共通リファレンスの検討に際しては、IPA/SEC 組込みプロジェクトで策定した ESQR の考え方を踏襲している。ESQR ではシステムプロファイリングを明確に定義した上で、品質コントロールのための指標として、プロセス/プロダクト品質指標の大きく 2 カテゴリ約 30 の品質指標により、品質定量化を進め、その値による品質の開発段階でのコントロールを目指している。今回、本研究会ではこの考え方を参考に、重要インフラ情報システム向けの信頼性指標を追加する方向で検討を加えた。また、オリジナルの ESQR ではこれらの品質指標に関する基準値を照会することで、関係者間の定量化に関する意識向上と実用性を担保しているが、今回の検討でもこのコンセプトを是認し、重要インフラ情報システムに関する指標セットとその参考値掲載を基本的な方針とすることとした。

プロセス指標	システム構築の際に、信頼性や品質面に関する確認の作業として、レビューやテストなどをどの程度実施しているかについて作業ボリュームに対する作業工数比率などで評価する指標。
プロダクト指標	システム構築の際に作成される（中間）成果物の出来栄え、特に信頼性や品質などの側面で問題ないかどうかを客観的に計測し、評価するための指標。

指標目標値の提示

上記のプロセス指標/プロダクト指標については、前述のシステムプロファイリングのレベルに対応した指標の参考値を提示する方針とした。これはこうした参考値を提示することで、信頼性に関する定量コントロールに関する具体的な議論を活性化させるきっかけとしたいという意図によるものである。

共通リファレンスの整備にむけて

今回の研究会では、ESQR を参考に重要インフラ情報システム向けの共通リファレンス整備に向けた基本コンセプトの検討を実施した。今回策定したコンセプトをもとに、早急に重要インフラ情報システムを対象としたリファレンスセットを整備していく必要がある。

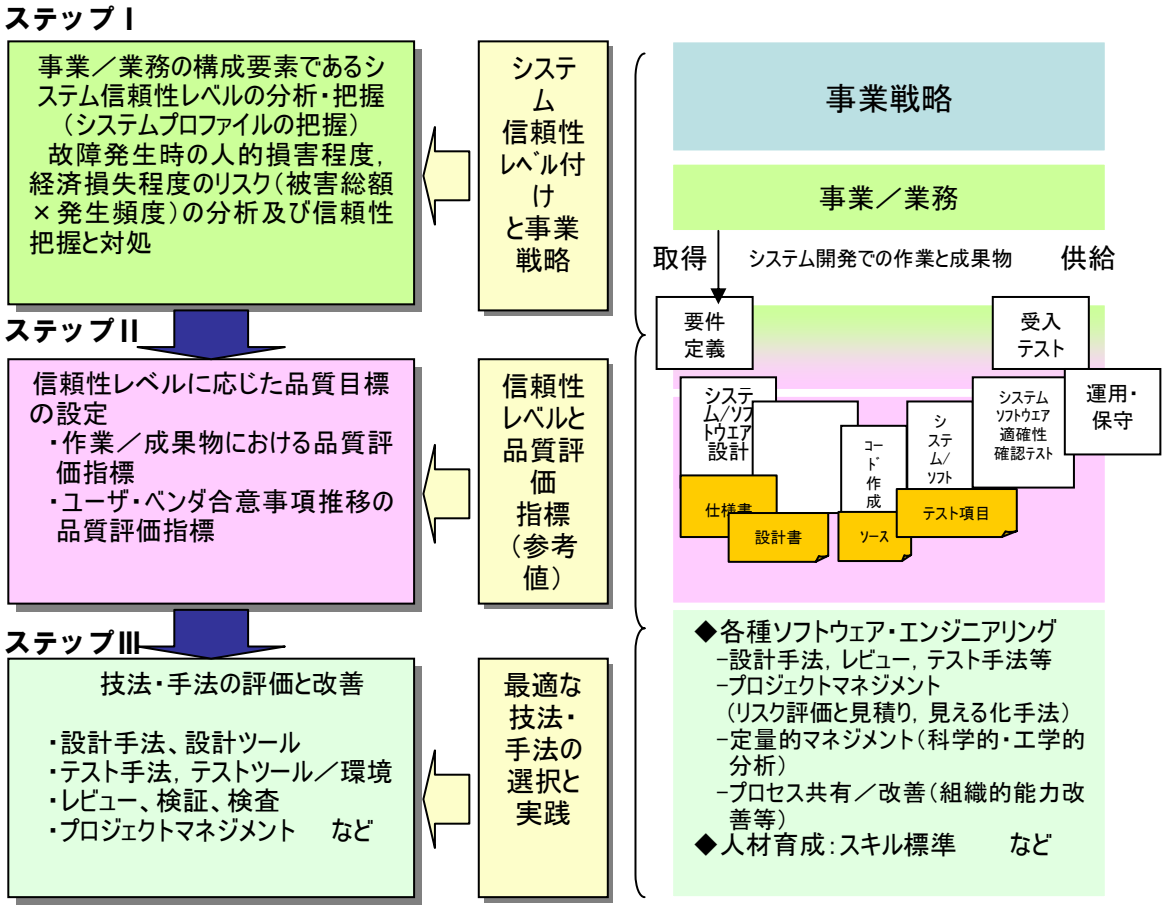


図１－６　共通リファレンスの適用シナリオ

９．　今後の計画

今後の計画	本研究会では、重要インフラ情報システムにおける信頼性向上をテーマに、 ① 情報システム信頼性の議論のベースとなるシステムプロファイリング ② システム障害の類型化と障害対策指針 ③ セキュリティを重視した障害対策指針 ④ 高信頼システムの実装に向けた共通開発指針 について、その基本的な方向性と実現に向けた基本アイデア、基本コンセプトを検討し、一部は指針の案などの整備も試みた。
システムプロファイリング	今回の試案をもとに広く産業界の意見を入れ、より使い勝手のよいものとしていく予定である。また、これと並行して、産業界で実際のシステム開発に携わる皆様方に、広く試用していただき、情報システム信頼性に関する共通認識として普及していくように、関係各団体や行政の支援も得ながら進めていきたい。
システム障害対策指針	今回の検討したシステム障害分析のスキームとそれに基づき試作した障害再発防止のチェック項目についても、広く産業界で試用していただき、より実用性の高い仕組みとして仕上げていきたいと考えている。これらについては、IPA/SEC やシステム関連の業界団体と歩調を合わせ、整備、普及・定着のサイクルを次年度以降回していく予定である。
セキュリティ障害対策指針	セキュリティ障害対策指針については、重要インフラ事業者ならびにこれらで利用される情報システムの開発者や運用者など広く周知徹底していく必要がある。また、それぞれの立場によってシステムセキュリティを確実なものとするための要諦は若干異なることも予想されるため、対象者に合わせて普及の方策などを考えていきたい。
高信頼システム実装共通開発指針	今回、検討した高信頼システム実装共通開発指針のコンセプトに従い、早急に共通開発指針リファレンスの整備を進めていく。リファレンス整備については、IPA/SEC を中心に、さらに広く産業界の知見などを活かしながら整備していきたい。