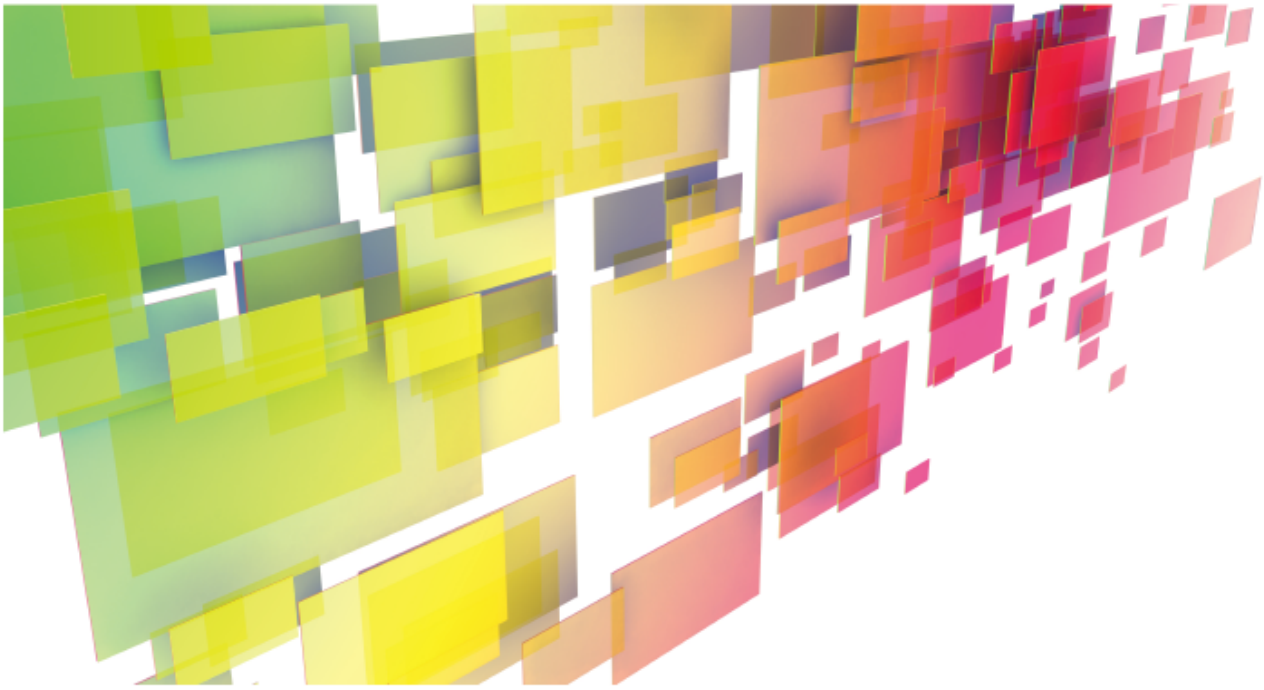
IPA Better Life with IT

情報処理システム高信頼化
教訓活用ガイドブック
（ITサービス編）



独立行政法人情報処理推進機構（IPA）
技術本部 ソフトウェア高信頼化センター（SEC）

情報処理システム高信頼化教訓活用ガイドブック（IT サービス編）

独立行政法人情報処理推進機構

目次

１．はじめに

１．１．目的

システム障害の情報は、サイバー攻撃に代表されるセキュリティ事故の情報に比べて、世の中で共有されているとは言い難い[1]。それは、システム障害は、障害を発生させた事業者の責任に帰結され、その事業者は、発生させたことを不名誉なことと考えるからである。したがって、場合によっては、事業者組織内のプロジェクト間でも情報共有されない事態も起きているとのことである。

しかし、そのような状況は、サービスを受ける利用者にとって、また社会の重要インフラであればあるほど、好ましい状況ではない。何故ならば、情報共有がなされないことによって同じようなシステム障害が、さまざまなサービスや分野で発生するおそれがあるからである。

そこで、IPA/SEC では、重要インフラにおいて類似のシステム障害をなくすため、情報共有の道具として、システム障害とそこから得られた教訓をまとめた教訓集を公開した（文献１－２）。さらに様々な分野、団体において情報共有の場を設けるべく、活動を行って来た。

IPA/SEC は、各企業・団体が、この教訓集を活用したり、自らが情報共有の場に参加したりすることで、他者のシステム障害事例を「対岸の火事」でなく、「他山の石」にしてほしいと願っている。

本「教訓活用ガイドブック」は、この教訓集の活用や情報共有の方法をより分かりやすく解説し、多くのシステム従事者、またその経営者の方々に理解し、実践していただくためのものである。本書を参考に、教訓をより一層活用していただきたい。

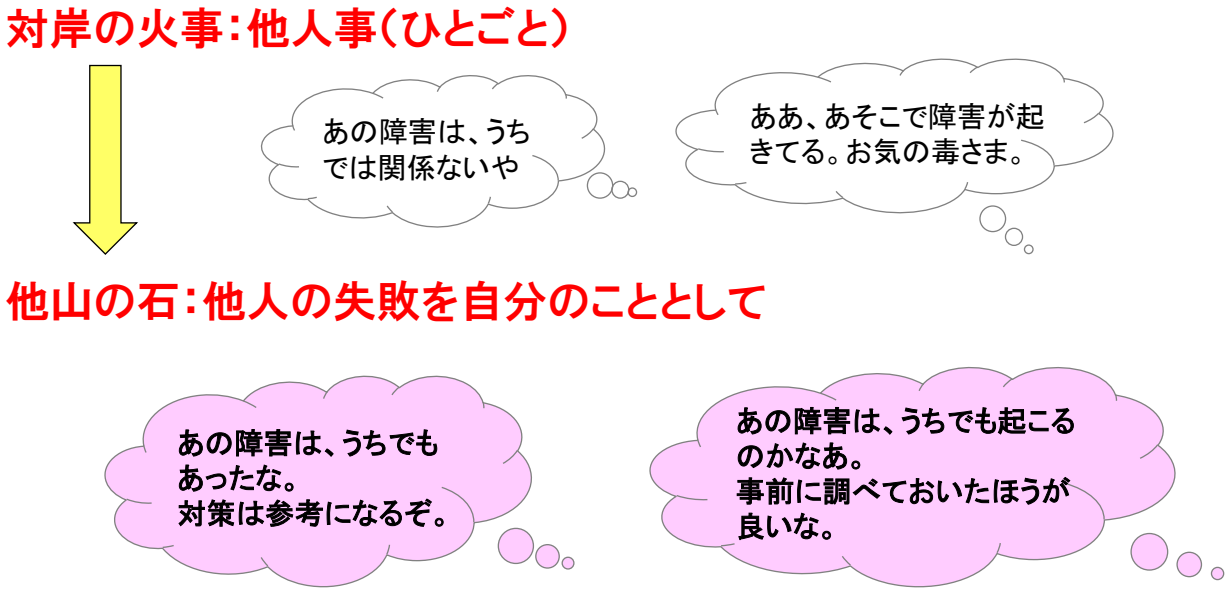


図１．１－１　目的

[1] サイバー情報の共有は、米国サイバーセキュリティフレームワークなどの活動（文献１－１）、日本の JCSIP（サイバー情報共有イニシアチブ、https://www.ipa.go.jp/security/J-CSIP/）などの活動がある

そしてさらに、この教訓を活用するだけでなく、各企業・団体が自ら教訓を作り、それを幅広く共有して世の中にも役立てていける仕組みを構築することが重要である。そのため、本書は、以下の内容を盛り込んでいる。

◆IPA/SEC の教訓を活用する方法と事例

IPA/SEC で作成した教訓を、どのように活用すればよいか

◆自社、他社、他分野での障害事例の共有活動を通して、教訓を活用する方法と事例

事業者自らが障害事例をまとめ教訓を作成した場合、どのようにその教訓を共有し、活用すればよいか。

本書では、多くの事例をコンパクトに取り入れた。是非、読者の皆さまには、本書を有効に活用していただき、教訓の活用と情報共有に取り組んでいただければ幸いである。

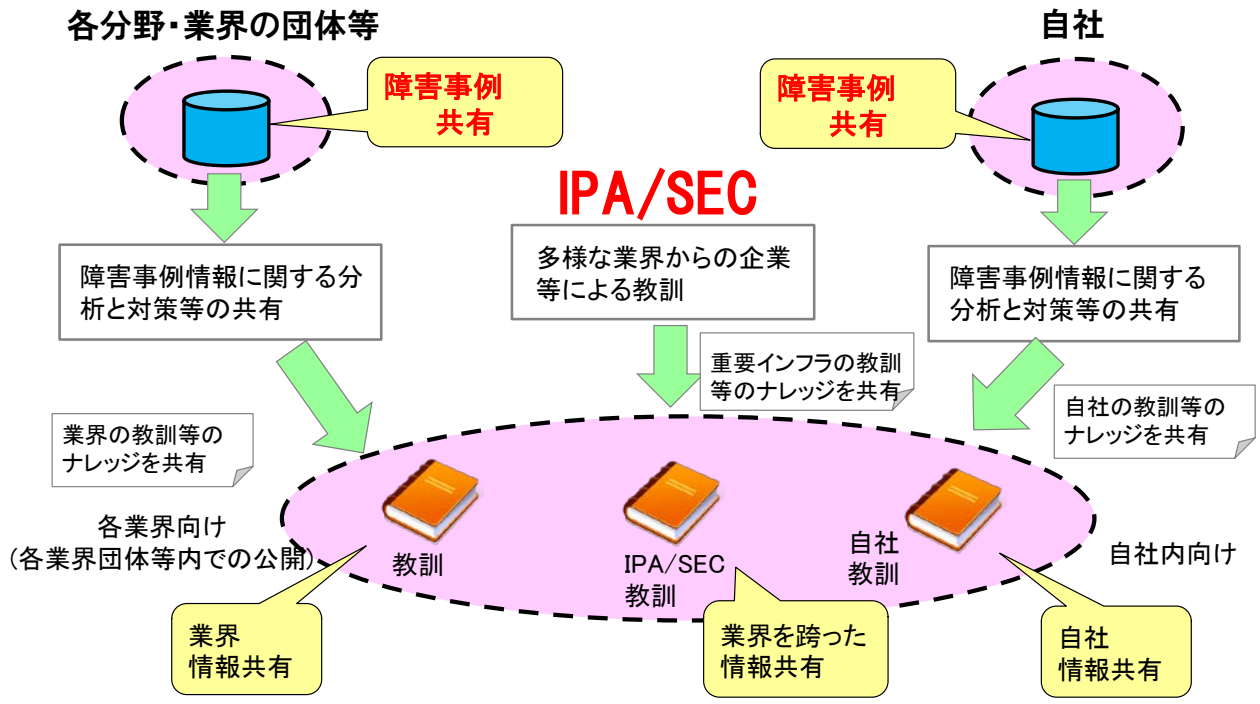


図１．１－２　情報共有のイメージ

１．２．本書の位置づけ

本書は、IPA/SEC の IT サービス分野における情報処理システムの、教訓活用に関するガイドブックである。関連する成果物の中での位置づけは、以下の図の通りである（図１．２－１）。

「情報処理システム高信頼化教訓集」は、本書が解説している原本である。また、「教訓作成ガイドブック」は、本書との姉妹品になり、教訓作成のガイド（手引）となる。

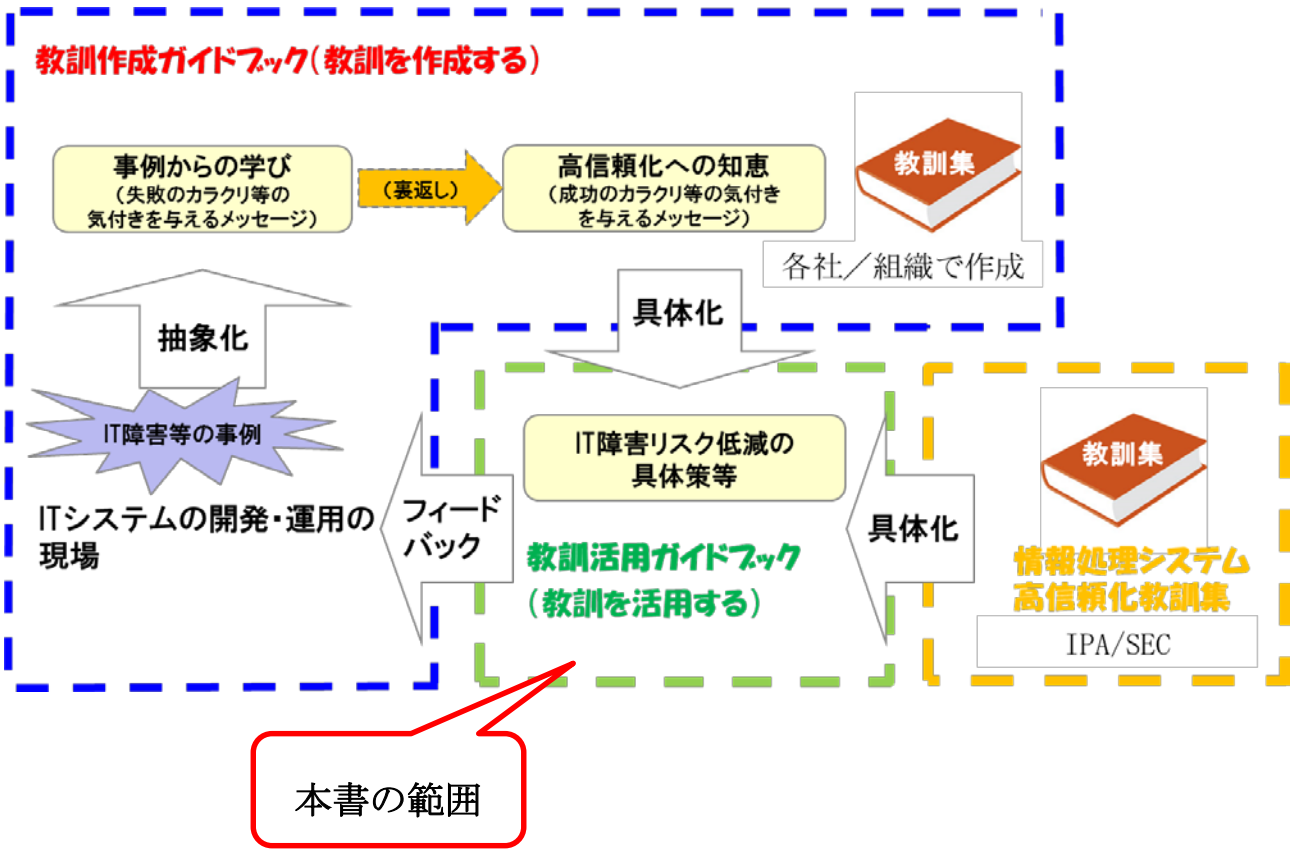


図１．２－１　本書と他資料との関係

１．３．活用メリット

ここでは、IPA/SEC の教訓と、自ら作成したり業界内で共有したりした教訓を活用することのメリットを、５点挙げたい。

メリット１　“他社の障害事例”を自社の予防に役立てることができる

IPA/SEC の教訓、または業界内で共有している教訓の中から自社に適用可能な教訓を見つけ、活用することにより、自社の障害対策に役立てることができる。

障害対策は、再発防止対策（発生させた障害を、二度と発生させない対策）と未然防止対策（障害が発生する前にリスク分析を行い立てる対策）の２種類がある。

自社で障害が発生した場合、一般的な傾向として、直接障害のあった箇所（直接原因）を修正し修復することで事足りたとしてしまう場合が多い。しかし、これらの教訓類を活用することにより、直接原因だけでなく根本的原因の対策を立てることができる。

また、自社の事例から再発防止対策は立てやすいが、自社で起きた事例が無い障害の未然防止対策は立てにくい。そこで、これらの教訓を活用することにより、未然防止対策の参考にすることができる。

さらに、これらの教訓類を自社の教訓作成の参考事例として活用することができる。

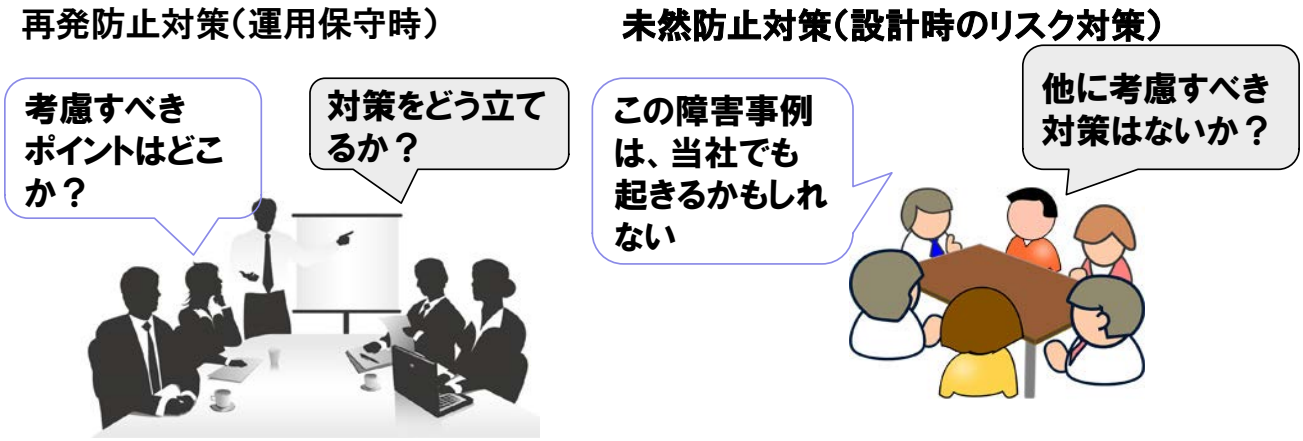


図１．３－１　自社の障害対策

メリット２　IPA/SEC のソフトウェアエンジニアリングを活用することができる

IPA/SEC では、ソフトウェアエンジニアリングの調査、研究を 10 年以上にわたって行ってきた。IPA/SEC の教訓は、そのような IPA/SEC のこれまでの成果を取り入れている。

システム障害の分析、対策については、これらの成果物の活用が望まれる。

活用方法をまとめると、以下のように整理できる。

・IPA/SEC で培ったソフトウェアエンジニアリング成果物を自社の障害予防に役立てる。

・IPA/SEC の成果物を中心に、「教訓事例」と関連する対策手法、分析手法を活用することができる。

IPA/SEC の成果物をソフトウェアライフサイクルで整理すると（図１．３－２）のようになる。IPA/SEC の教訓集の「PART-Ⅱ　障害対策種法・事例集」では、具体的に教訓に関連する IPA/SEC の成果物を中心に一覧として提示し、それぞれの教訓から活用できる成果物の概要を説明しているので、活用していただきたい。

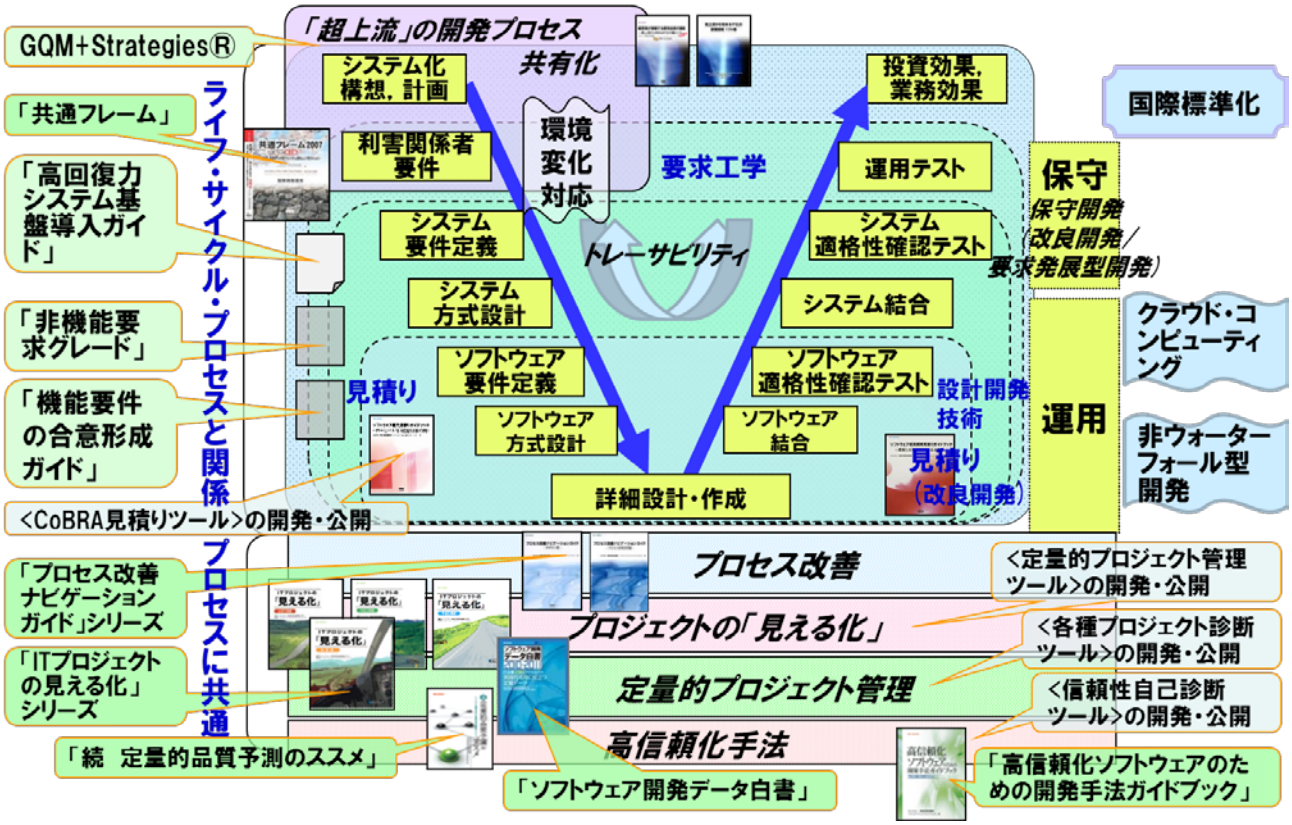


図１．３－２　IPA/SEC の成果物と活用シーン

メリット３　IT の経験者から若手への技術の伝承（若手の人材育成）

IT の現場では、システムライフサイクルの延長に伴い、若手がシステムを一から構築する経験を持つことが難しくなってきており、既に稼働しているシステムの保守、運用から入る場合もある。そのような若手や、別部門からの異動者に対しての教育には、自社で過去に起きたシステム障害事例を活用するなどの実践的な演習、疑似体験がより重要になって来ている。

そのため、これらの教育にも教訓を活用することで、実践に活かせる教育が可能になると期待できる。

例えば　以下の様な活動を行うとする。

・若手に教訓作りの演習をさせる。（ベテランがアドバイザ参加）
・教訓事例をケーススタディとし、ワークショップを行う。
・自社のケーススタディでワークショップを行う。

その結果、以下の様な効果を得ることができる。

・世代を超えて IT の疑似体験によるノウハウ共有が図れる。

・ワークショップの成果物も教訓化することで、システムの保守・運用のノウハウの継承に役立つ。

・新たな対策が浮かび、実際にシステムに取り込むなどの成果が期待できる。

メリット４　障害対策の“気づき”が得られ、身につく！

自社の事例情報に対する、対策、教訓を作るため議論を通して、参加者一人一人に“気づき”が得られ、身につけることができる。（個人として、組織として）

つまり、他者事例（教訓）を通してメンバ内でコミュニケーションを図ることにより、自らの課題を発見し（気づき）、それについての議論ができることにより、自らのシステム障害対策が作れるなどの効果も期待できる。

図１．３－３　気づき

メリット５　IT 社会で信頼される企業・団体になれる

以下の（図１．３－４）は、ET2013（2013 年 11 月）[2]とソフトウエアジャパン 2014（2014 年 2 月）で、IPA が行ったアンケート結果である。

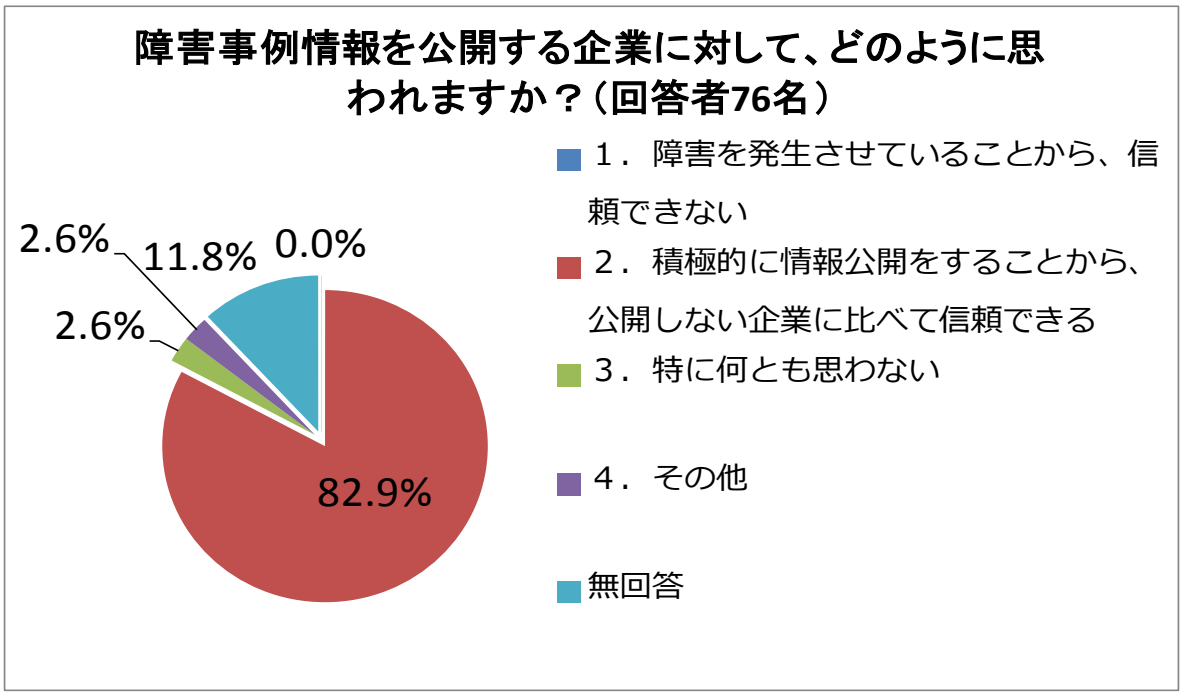


図１．３－４　アンケート結果

このアンケート結果が示すように、障害事例情報を公開する企業は、「積極的に情報公開をすることから、公開しない企業に比べて信頼できる」と考えられている。

このことから、情報共有活動を積極的に行うことは、自社の社会貢献度を増すことになり、自社のシステム障害のマイナスイメージをプラスイメージに変えることができる。

[2] Embedded Technology 2013(組込み総合技術展)

IPA/SEC の教訓集を活用する場合の注意点

以上、いくつかの教訓活用のメリットを挙げたが、その中で「IPA/SEC の教訓集」を活用する上での注意点を３点述べる。

① 教訓集を学べば、全てのシステム障害に活用できる訳ではない。それは、教訓集の事例は、あくまで収集された事例についての解説であり、当然収集されていない数多くの事例は類似が認められた事例以外、教訓集の教訓には含まれていない。そのため、教訓集は、体系化されるまでには至っておらず、教訓集を学べば、すべてのシステム障害に対応できるわけではない。

② 教訓化したシステム障害事例は、実際の事例そのものでなく、重要なポイントを一般化、汎用化して、広く活用できるように記述されている。したがって、個別障害事例を深く分析したり、対策をより具体的に調べたりする目的には適さない。

③ 読者が参画しているシステムと教訓事例は、必ずしもコンテキスト[3]が一致しない場合がある。そのような場合は、無理に教訓を自身のシステムに当てはめて活用しようとしても意味が無い。読者によっては、使えない教訓も存在する。

まとめ

これらの注意点を踏まえて、教訓を活用すれば、システム障害に携わる方々が、現場で悩んでいることに対して何らかの「気づき」を得るヒントになるであろう。つまり、教訓は、システム障害に主体的に立ち向かう方々にとって、有効な武器となる。

今後、更にシステム障害時例を収集し、体系化する事ができれば、より高い効果が得られることが期待できる。

[3] ここでは、システム特性（規模、用途、性能要求レベル、信頼度など）の意味

１．４．本書の構成と使い方

本書の構成の柱は、「如何にして、IPA/SEC『教訓集』を活用するか」と「教訓の共有をどのようにして行うか」の２点である。

そこで、本書の構成は、以下のようにした。

「１．はじめに」では、本書の目的、本書の位置づけ、活用メリット、本書の構成と使い方をまとめている。

「２．教訓の活用方法」では、IPA/SEC 作成教訓の活用方法を解説している。

「３．情報（障害事例・教訓）共有」では、自社内から業界内、業界横断と教訓の共有を広く社会に広げていく方法を解説している。

以下、本書の使い方の概要を述べる。

「２．教訓の活用方法」

この章では、IPA/SEC の教訓集を見る者が自分のコンテキストにおいて役立ちそうな教訓を容易に見つけられること、各教訓が自分自身にとって有用かそうでないかを適切に判断できることを目的にした。そのため、ここでは教訓を活用するに当たり、その入口を見つける手段を提示する。あくまで本書と教訓集の構成上から述べているので、読者が様々な角度から入口に入ることも可能である。[4]

◆自分が持っている課題に対して、この IPA/SEC の教訓が参考になるのか知りたい。例えば・・・

・システム障害の原因が判明した後、対策をどのように立てれば良いのか知りたい。
・自システムの予防対策をどのように立てれば良いのか調べたい。
・ユーザとベンダの役割分担の具体的な対策事例を知りたい。
・若手要員の育成を考え、システム障害の未然防止訓練・教育を行いたい。

本書　「２．１．目的別の教訓活用方法」

◆IPA/SEC の教訓から、活用方法を知りたい。例えば・・・

・他社では、どんな障害が出ているのか、知りたい。
・いつも場当たり的な対応になっている障害対策を根本問題から解決したいが、何か事例はないか。

本書　「２．２．個々の教訓の活用方法」

[4] 今後、教訓事例が増えるに伴い、キーワードによる教訓検索などのツール整備を行う予定。

「３．情報（障害事例・教訓）共有」

この章では、システム障害を減らすためには、自らが積極的にシステム障害に取組み教訓化し、また他者の教訓も自らの対策に取り組んでいくといった、「情報共有活動に参加してこそ、システム障害の削減を達成することができる」ことを述べている。そのため、情報共有の仕組みを今後幅広く展開する方法を解説している。

◆共有活動の意義、メリットを知りたい。

→ **本書　「３．情報（障害事例・教訓）共有」**

さらに、読者が自ら作成した教訓集を自社内や業界内などで情報共有を行っている場合の活用方法についてもまとめた。

◆自分が持っている課題に対して、情報共有活動で作成した教訓が参考になるのか知りたい

→ **本書　「３．４．情報共有活動における教訓活用」**

直接　IPA/SEC の教訓集に当たる

本書では、教訓集にある　障害対策手法、障害分析手法についての活用事例はあまりないが、これらについては、直接教訓集を見ていただきたい。

◆障害対策手法を知りたい

例えば・・・

・教訓の対策手法をもっと幅広く調べたい。

・IPA でまとめた成果物で、システム障害の対策に使えるものを知りたい。

→ **教訓集 PART-Ⅱ　障害対策手法・事例集**

◆障害分析手法を知りたい

・IPA/SEC の教訓では、「なぜなぜ分析」を中心とした分析手法を用いているが、他にどのような分析手法があるのか知りたい。

→ **教訓集 PART-Ⅲ　障害分析手法・事例集**

２．IPA/SEC の教訓集の活用方法

この章では、IPA/SEC の教訓集について、「掲載されている教訓をどのように活用するか」と、「自身の課題解決に教訓を活用する方法」の、２編に分けて解説する。

IPA/SEC の教訓集を「自身の課題解決に教訓を活用する方法」として知りたい場合、
例えば、

・システム障害の原因が判明した後、対策をどのように立てれば良いのか事例から知りたい。
・他事例を見て、運用面から自システムの障害の予防・対策をどのように立てれば良いのか調べたい。
・システム障害の原因が設計時の要件漏れで合った場合は、設計時に障害の予防・対策をどのように立て、どのように取り込めば良いのか。

などの場合があるが、その時は、「２．１．目的別の教訓活用方法」を参照することになる。

また、IPA/SEC の教訓集から、「掲載されている教訓をどのように活用するか」を知りたい場合、
例えば、

・他社では、どんな障害が出ているのか、知りたい。
・いつも場当たり的な対応になっている障害対策を根本問題から解決したいが、何か事例はないか。
・教訓集のそれぞれの教訓は、どのような活用方法があるのか。

などの場合があるが、その時は、「２．２．個々の教訓の活用方法」を参照することになる。

２．１．目的別の教訓活用方法

この章では、読者が抱えている課題を解決するために、その課題を扱う場面毎に教訓が参考になることについて解説する。

教訓は、教訓集にある事例に閉じたものと考えるのではなく、一般化した事例（＝教訓）として理解することにより、様々な場面で活用することができる。

この章では、以下のような場面での教訓を活用するポイントを解説する。以下の場面の解説では、活用したい事例を示して、どの教訓が役に立つかを紹介するが、該当する教訓については参考としていただき、読者自身が教訓集を読むことで、「この教訓が活用できるのではないか。」との気づきを得ることが望まれる。それは、誰もが思いつかない貴重な活用方法であるからである。

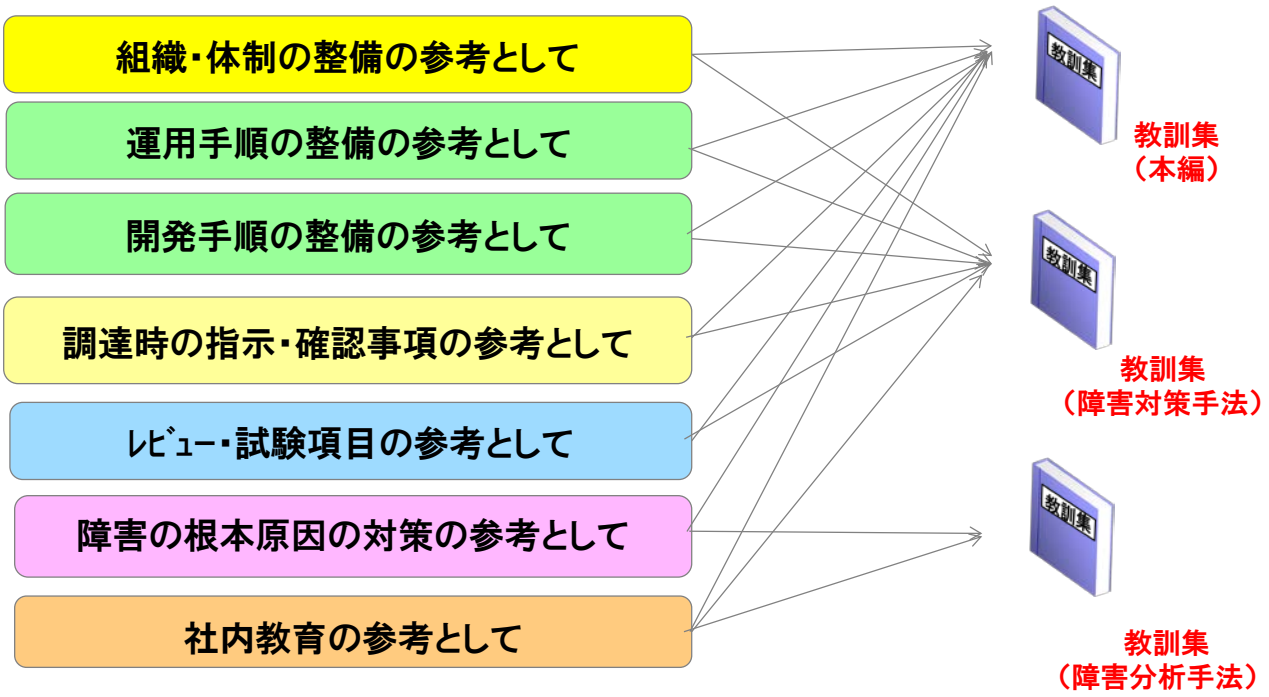


図２．１－１　目的別教訓活用方法

２．１．１．組織・体制の整備の参考として活用

IPA/SEC の教訓集では、教訓を「ガバナンス/マネジメント領域」と「技術領域」に分けて掲載しており、特に組織・体制の整備の際は、「ガバナンス/マネジメント領域」が参考になる。

今回の IPA/SEC の教訓作成にあたっては、重要インフラ分野の中心的な企業の参加を得て、「ガバナンス/マネジメント領域」における、組織・体制の整備に役立つ教訓が揃っている。

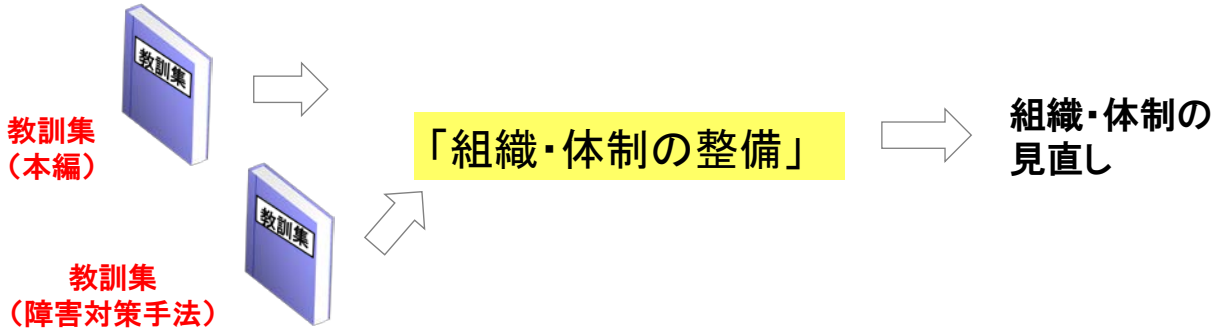


図２．１．１－１　組織・体制の整備

ここでは、以下の様な活用シーンを述べる。

組織・体制の改善として活用したい

組織・体制の悩みとは、例えば、システム障害を減らし、復旧をスムーズに行うための組織・体制をどのように構築するか、また、外部委託との役割分担はどうあるべきなのかなどが想像される。

このような組織・体制の整備の参考となる教訓は、「ガバナンス/マネジメント領域」の全ての教訓（Ｇ１～Ｇ９）を参考にし、その中から自らの組織に合うものを選択することが役に立つと思われる。

プロセス改善として活用したい

ある組織では、システム障害対策を全社で取組むことにし、そのプロセス改善を PDCA サイクルで廻していきたいと考えている。この場合、さらに自組織内でどのようなプロセスがふさわしいか、メンバとディスカッションを行い、合意形成を行うことなどが必要とされる。

このようなプロセス改善や、合意形成を構築するためには、関係者のコミュニケーションの向上が必要となる。「ガバナンス/マネジメント領域」Ｇ４、Ｇ５、Ｇ６、Ｇ７、Ｇ８、「技術領域」Ｔ６、Ｔ７、Ｔ９、Ｔ１２、Ｔ１３、Ｔ１５、Ｔ１８などの教訓が参考になる。

２．１．２．運用手順の整備の参考として活用

システム障害の現場は、運用部門が前面に立っている。その現場の方々が活用する事例を数多く収集しているので、運用部門の課題解決に活用することができる。

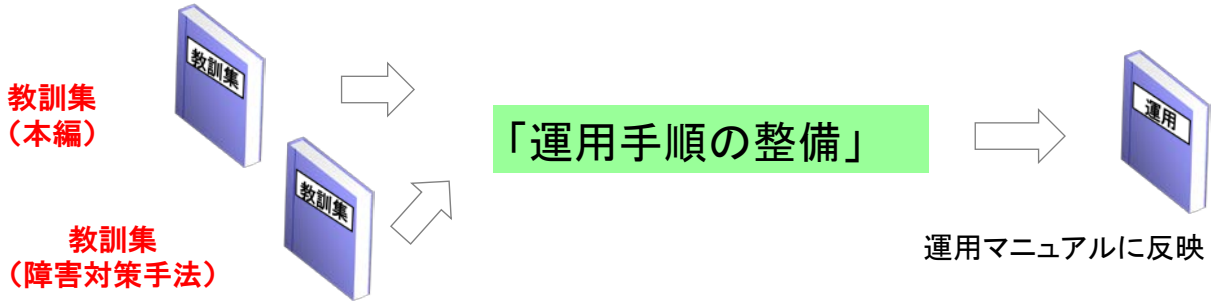


図２．１．２－１　運用手順の整備

ここでは、以下の様な活用シーンを述べる。

繰り返し発生する障害の対策として活用したい

例えば、システム障害の原因が判明した後の対策が不十分なため、同じようなシステム障害を繰り返し発生させる場合があった。そのような事態をなくすための抜本的な対策を求めていた。

このようなシステム障害に対応する運用部門の組織・体制の整備の参考となる教訓は、「ガバナンス/マネジメント領域」Ｇ３、Ｇ４、Ｇ５、Ｇ６、Ｇ７、Ｇ８、「技術領域」Ｔ２、Ｔ６、Ｔ７、Ｔ８、Ｔ１６、Ｔ１７などである。

自社で起きた障害事例を役立させたい

他事例を見て、運用面から自システムの障害の予防・対策をどのように立てれば良いのかを検討していた。また、システム障害を発生させたプロジェクトの教訓が、他プロジェクトでなかなか活かせることができないため、どうやって社内で有効に活用させることができるか悩んでいた。

このような課題に対しては、教訓集から類似障害を見つけ出し、自社システムに合う形で、対策を取り入れたり、自社の運用体制と教訓集の事例の運用体制を比較してみて、自社の課題を見つけたりすることにより活用することができる。そのような教訓は、「ガバナンス/マネジメント領域」Ｇ３、Ｇ４、Ｇ５、Ｇ６、Ｇ７、Ｇ８、Ｇ９「技術領域」Ｔ１、Ｔ２、Ｔ６、Ｔ７、Ｔ８、Ｔ９、Ｔ１０、Ｔ１１、Ｔ１２、Ｔ１５、Ｔ１６、Ｔ１７などである。

２．１．３．開発手順の整備の参考として活用

教訓は、システム障害事例が中心になっている関係上、開発手法とか設計手法について体系的に述べてはいない。しかし、障害事例を参考にして、開発時にシステム障害を起こさないための気づきを得るために活用することができる。

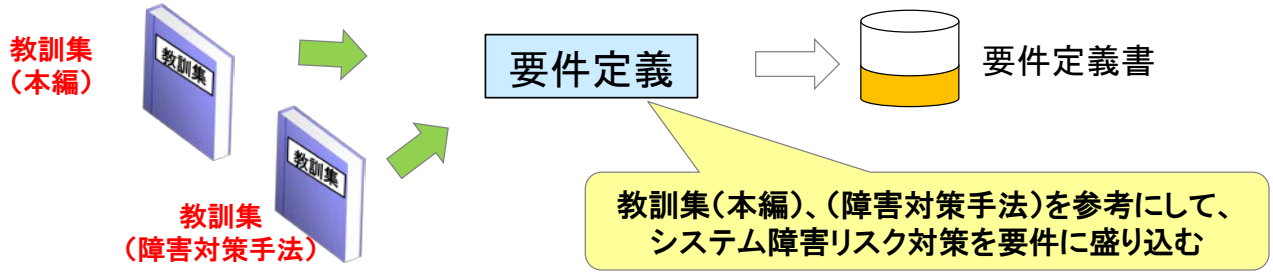


図２．１．３－１　要件定義

ここでは、以下の様な活用シーンを述べる。

開発時の要件漏れを防ぎたい

例えば、現行システムで、開発時の要件漏れが原因でシステム障害が多発した。そのため、次期システム構築時には、システム障害を減らし、また復旧がスムーズに行えるようなシステムを構築したいと考えていた。

このようなシステム開発時の要件漏れが原因となるシステム障害に対応する教訓は、「ガバナンス/マネジメント領域」Ｇ１、Ｇ２、Ｇ３、「技術領域」Ｔ１、Ｔ２、Ｔ３、Ｔ４、Ｔ５、Ｔ７、Ｔ８、Ｔ９、Ｔ１０、Ｔ１１、Ｔ１３、Ｔ１４、Ｔ１８などが参考になる。

設計時の予防対策として活用したい

他社で起きたシステム障害事例を見て、設計時に障害の予防・対策をどのように取り込めば良いのか検討していた。設計時に障害の予防・対策を取り込むためには、教訓集から類似システムを見つけ出し、その障害事例の対策を参考にすることになる。

そのような類似障害の対策を自システムに合う形で、設計時に取り入れるために活用できる教訓は、「ガバナンス/マネジメント領域」Ｇ１、Ｇ２、Ｇ３、「技術領域」Ｔ１、Ｔ２、Ｔ３、Ｔ４、Ｔ５、Ｔ７、Ｔ８、Ｔ９、Ｔ１０、Ｔ１１、Ｔ１３、Ｔ１４、Ｔ１８などが参考になる。

さらに「対策手法」で開発に関する参考文献を活用する。

２．１．４．調達時の指示・確認の参考として活用

IT サービスの現場は、サービス提供企業の社員のみで全てを行っているところは少なく、幾つかのベンダ、開発委託会社、運用委託会社、自社のシステム子会社など多数の調達先企業が、参画している。

そのような中で、システム障害に素早く対応できる体制、システム障害を減らす体制を構築するためには、調達時のベンダ、ユーザ双方の合意事項をどう決めるかが重要になる。

さらに IPA/SEC では、発注者との合意形成を取る上でのポイントを「経営者が参画する要求品質の確保～超上流から攻める IT 化の勘どころ～」（文献２－３）としてまとめているので、こちらも参考になるであろう。

図２．１．４－１　調達時の指示・確認

ここでは、以下の様な活用シーンを述べる。

ユーザとベンダの役割分担の見直しに活用したい

システム障害発生時の対応がベンダとうまく調整できずに悩んでいたり、そこで契約更改の時期に当たり、ユーザとベンダの役割分担について検討を開始したりしていた。

契約時にユーザとベンダの役割分担の見直しを行うことは、今までの反省を踏まえた改善に結びつくものでなくてはならない。このようなユーザとベンダの役割分担の参考となる教訓は、「ガバナンス/マネジメント領域」Ｇ２、Ｇ４、Ｇ５、Ｇ８、「技術領域」Ｔ１２、Ｔ１６、Ｔ１７などが参考になる。

ベンダに期待すべきことを整理したい

保守作業時にベンダから積極的な効率改善の提案を期待するのだが、なかなか期待通りにならず、保守作業の改善ができなかったユーザは、そこで他事例を見て、調達時にどのような観点でベンダと向きあえばよいか検討することが必要となる。

このような場合では、ユーザとベンダの関係が良好でなければ、ベンダから期待できる対応は受けられないであろう。そのためには、調達時にベンダにユーザの希望を明確に伝え、契約内容を明確にし、そのための条件を設定し、お互いが合意することが重要である。教訓集「ガバナンス/マネジメント領域」Ｇ２、Ｇ４、「技術領域」Ｔ１２、Ｔ１６などの教訓が参考となる。

２．１．５．レビュー・試験項目の検討時の参考として活用

システム障害を減らすポイントの中で、有識者からの知恵を受けるレビュー方法と、障害発生の穴を塞ぐ試験項目の検討は、重要である。ここでは、レビュー・試験項目の検討時に参考とする場合を説明する。

図２．１．５－１　レビュー・試験項目検討時

ここでは、以下の様な活用シーンを述べる。

有識者を活用したい

システム障害の原因分析を行ったところ、折角社内に有識者がいるにも関わらず、有効な意見を吸い上げてシステム設計に反映できていないことが判明したので、効果的なレビューが行えるように対策を立てることにした。

このような場合、有識者の活用に参考となる教訓は、「ガバナンス/マネジメント領域」Ｇ６、「技術領域」Ｔ３などが参考になる。

若手とベテランを有効に活用したい

若手リーダを育成する意味もあり、システム更改の担当に多くの若手を参画させた。しかし、システム開発の進捗に遅れが出始め、何らかの対策を講じなくてはならなくなった。そこで、途中からベテランを投入するため、若手とベテランがうまく協調できるレビューの進め方、試験の進め方をどのように行えば良いのか検討したいと考えていた。

このような場合、若手を育成することは、システムの現場では重要な課題である。そのためにはベテランの有効な活用が不可欠である。レビューの進め方、試験項目のレビューには、「技術領域」Ｔ３、Ｔ９、Ｔ１３などの教訓が参考になる。

また、「対策手法」でレビュー・試験項目検討時の対策に関する参考文献（文献２－１）（文献２－２）を活用することもできる。

２．１．６．障害の根本原因の対策の参考として活用

システム障害が起きた時、直接の原因（ハードウェア故障、プログラムのバグなど）を見つけることは、復旧を素早く行う上では、優先されるべき対応である。

しかし、この教訓集では、その障害の背後にある原因を分析し、根本的な対策を行うことで、以降の類似障害を未然に防ぐことに主眼を置いている。

したがって、障害対応が落ち着いて、「今回の障害を未然に防ぐ手立てはなかったのか。」とか、「システム障害が、再び同様な原因で起きることが無いよう対策を検討したい。」などという際に教訓集を活用できる。

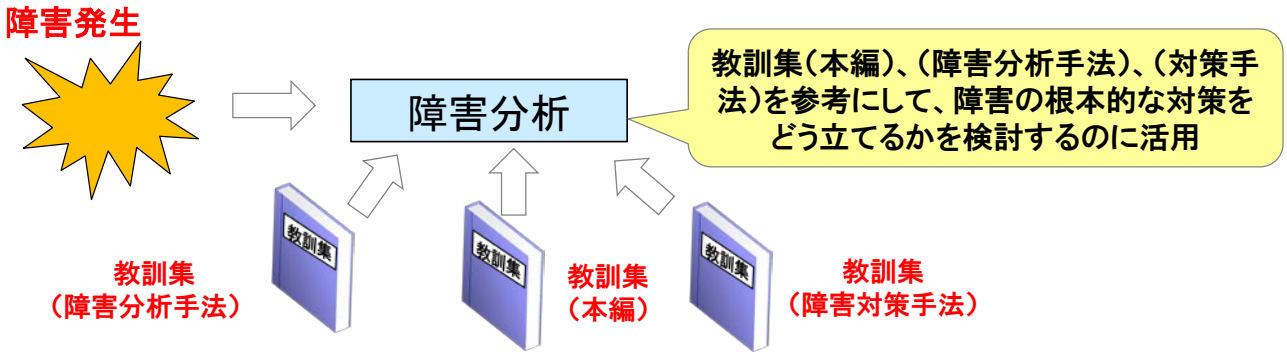


図２．１．６－１　障害分析

ここでは、以下の様な活用シーンを述べる。

根本原因分析と再発防止対策を立てたい

システム障害の原因が判明した後の対策が不十分なため、同じようなシステム障害を繰り返し発生させる場合があったので、そのような事態をなくすための抜本的な対策を求めていた。また、他事例を参考にして、システム障害が、再び同様な原因で起きることが無いように、原因分析、対策を検討しようとしていた。

このような場合、この教訓集では、その障害の背後にある原因を分析し、根本的な対策を行うことで、以降の類似障害を未然に防ぐことに主眼を置いているため、多くの教訓事例は、根本原因と未然防止対策について言及しており、該当する教訓は、全て参考になる。

また、IPA/SEC が行っている、「教訓作成」のワークショップ形式のセミナー[5]では、具体的な教訓作成のプロセスを学ぶことができる。そこでは、ヒューマンファクターで利用されているツール（なぜなぜ分析など）を学ぶことにより、根本原因と未然防止対策を立てる手法を学ぶことができるので、そちらも活用願いたい。

尚、教訓作成については、『教訓作成ガイドブック』が参考になる。

[5] SEC セミナー「事例から学ぶ IT サービスの高信頼化へのアプローチ」
（http://sec.ipa.go.jp/seminar/20160318.html）

２．１．７．社内教育の参考として活用

教訓集は、重要インフラでの事例が中心なため、なかなか一般の現場では経験できない事例を数多く載せている。よって、教訓集は、自身が経験できないシステム障害を疑似体験できる貴重な教育ツールになる。

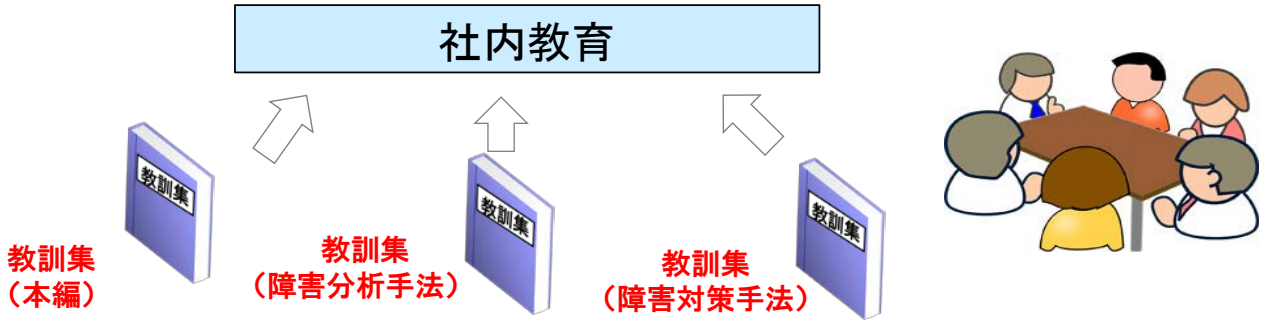


図２．１．７－１　社内教育

ここでは、以下の様な活用シーンを述べる。

若手などへの社内教育で活用したい

社内教育においては、障害対応ができる若手要員の育成を考え、そのための参考となるものを探したり、システム障害の未然防止の訓練・教育を行うための参考となるものを探したりする。

そのような場合に、教訓集を「障害対応教育」に活用する例を示す。

・教訓集をメンバで理解する勉強会を行う。そのことにより、自社の障害発生時の対応が取れるようになる。

・教訓集の障害事例を基に、原因、対策を考えるグループ討議を行う。その中で、自社の教訓集の原因、対策と比較して見ることにより、各自の知見が高まる。

・自社の障害事例から、教訓集の事例との類似障害を考えグループ討議を行う。自社の障害の対策と比較することにより、自社の障害対策の信頼度を向上させることができ、参加者のスキル向上に役立つ。

・自社の教訓作成を行うためのセミナーを開催する。その時、教訓集をテキスト、参考資料として活用する。

このような教育で活用することにより、自社の要員のスキル向上に役立てることができるであろう。

２．２．個々の教訓の活用方法

ここでは、教訓集の中の教訓事例の概要を紹介し、紹介した教訓が、どのような局面で活用できるかを解説する。

まずは、教訓集を熟読することをお勧めする。教訓集では、大きく「ガバナンス/マネジメント領域」と「技術領域」に分かれているが、「技術領域」の教訓事例は、「ガバナンス/マネジメント領域」の教訓にも関連し、またその逆の場合もある。一度、教訓の内容を頭に入れておくと、自分がシステム障害に遭遇した時や報道されたシステム障害を見た時に、類似性に気がつくことがある。その気づきが、自社のシステム障害対策に活かされることになる。

本章では、教訓集の教訓事例を 1 ページに要約し、以降に「活用が考えられる事例」をまとめた。「ケース」は、IPA/SEC で収集した事例や、報道された事例をより一般的に、また要点がわかり易いように編集している。「活用を考える」は、「ケース」が教訓のどの点で活用できるかについて考えるヒント（気づき）を説明した。

また、「ケース」と「活用を考える」は、教訓に即して述べている。そこで、読者の皆さまが、経験や想像を使って原因、対策を検討する余地を残していると思うので、更に教育の教材として活用することも可能である。

教訓、それに類似性がある活用事例は、IPA/SEC の経験からまとめたものである。さらに読者の気づきから多くの事例が、教訓、活用事例としてまとめられ、新たな教訓が生まれれば、将来システム障害の共有活動にも効果をもたらすことができるであろう。

２．２．１．事業部門と情シス部門の役割分担に関する教訓（Ｇ１）[6]

[教訓 G1]
システム開発を情シス部門だけの仕事にせず、
各事業部門が自分のこととして捉える「態勢」をつくることが大切

概要

システムトラブルの 8 割は、上流の要件定義局面でのコミュニケーション・ギャップから問題が生じていることが判明した。

その対策には、システム開発における事業部門（ビジネスサイド）の役割と責任を明確化し、コミュニケーションの質を高める態勢作りが有効で「アプリケーション・オーナー制度」などの事例がある。

アプリケーション・オーナー制度は、以下のような特徴がある。

・システム開発は、情シス部門に任せきりにすべき仕事ではなく、自分の考えた商品や施策を具体化するために行う自分自身の仕事であるという「オーナーシップ」の考えを持たせる。

・事業部門に、要件の詳細が固まるまで、情シス部門と対話を繰り返す責任を持たせ、要件定義の最終責任を負わせる。

・事業部門に、要件定義どおりにシステムが出来たかどうか受入れテストを実施する責任を負わせる。

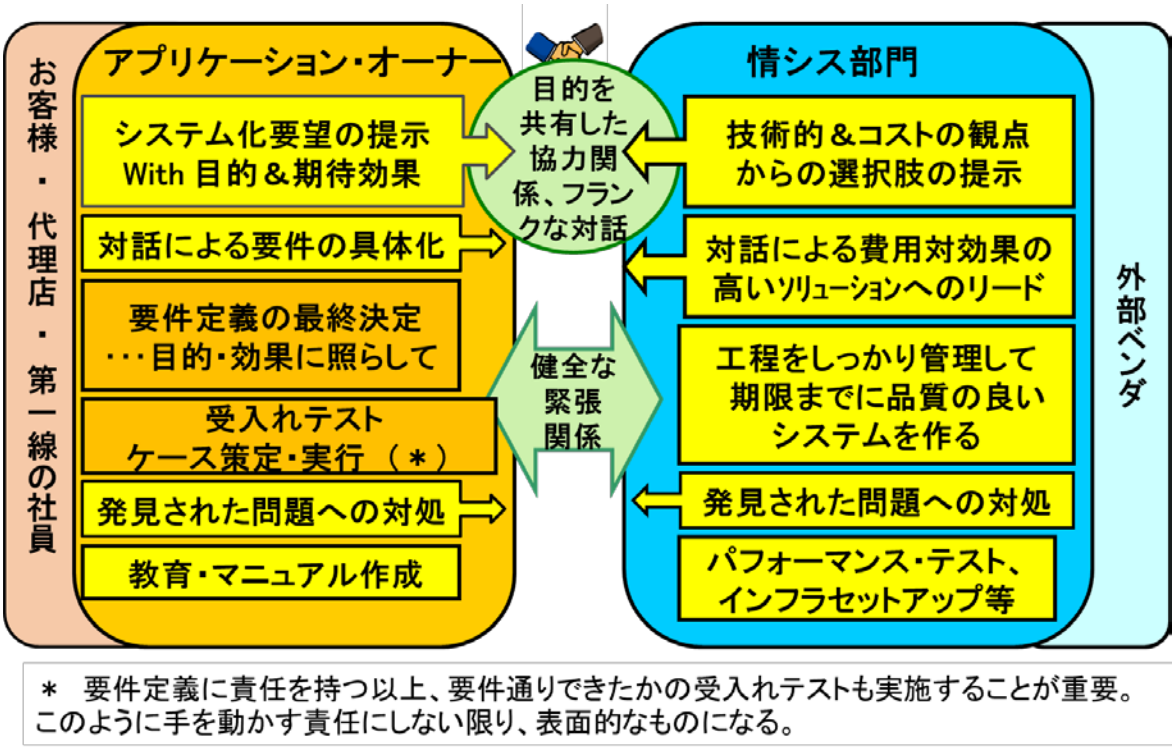


図２．２．１―１　アプリケーション・オーナー制度：責任と役割分担[7]

---

[6] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-13

[7] 東京海上日動火災株式会社の例

活用が考えられる事例

◆ケース１　開発体制の整備

A 社では、新サービスのシステム開発を行っていたが、開発が進まずサービスインを４回延期した。経営者が状況を確認したところ、事業部門の役員は、自分の問題としてとらえることなく情シス部門の非を唱え他人事のように情シス部門を非難するだけであった。情シス部門は、ビジネス側の要件について理解が十分でなく、その業務のブラックボックスを解消しようとする意欲と熱意が感じられなかった。

A 社の経営者は、そのような状況を改善したく、業務要件を第一義に考慮した組織・体制を検討することとした。

活用を考える

このケースは、開発体制の改善事例である。教訓Ｇ１は、事業部門が情シス部門に任せっきりであったためにシステム開発がなかなか進展しなかったことを根本的に変革することに活用できる。

この教訓のポイントは、事業部門が構築したシステムに主体的な役割を担い、最終責任を負うことである。これによりシステム開発が順調に行われ、システム障害も減ることが教訓で示されている。

しかし、形だけを単に真似るだけでは成功しない。経営層は、教訓に記載されたアプリケーション・オーナー制度を参考にし、事業部門と情シス部門が、それに沿ったプロジェクト運営を実践する中で、「どうしたら事業部門が積極的にシステム開発、運用についても意見や要件を提示してもらえるか。」と言った観点で、自らの組織に合った「**態勢**」を築くことが、重要になる。

◆ケース２　要件定義、受入れテストの不具合

B 社では、事業部門からの業務要件追加が短期間にどんどん発生し、今までのように情シス部門主体の開発では対応が追いつかないことになった。そのため、十分な開発期間が確保できずに、サービスインを迎える状況が増え、必然的にシステム障害が多発した。

活用を考える

本来は、情シス部門が開発計画を立て、そのスケジュールに沿ってサービス提供時期を確定すべきである。しかし、このケースのように事業部門の発言が強く、企業の収益に直結する案件などは、どうしても情シス部門に強い圧力がかかることが多い。

そのような場合は、事業部門を主体にしたアプリケーション・オーナー制度を採用することも一案である。事業部門が開発の責任を持つことによって、納期の妥当性を事業部門としても責任を持たなくてはならなくなり、納期を守るため開発の優先順位が低い案件などを取り下げるなどの対策を行いやすくなる。そのことにより、事業部門と情シス部門のバランスの取れたシステム開発を行うことができ、システム障害を減らすことが期待できる。

２．２．２．発注者の要件定義責任に関する教訓（Ｇ２）[8]

[教訓 G2]
発注者は要件定義に責任を持ってシステム構築に関わるべし

概要

A 社では、システム開発・運用を IT ベンダに外部委託している。A 社は、最近開発案件の増加に伴い委託先に任せる業務が徐々に拡大し、要件定義や受入れテスト等、発注者としての役割を果たし切れなくなってきた。

そこで、A 社は、以下の対策を行った。

1）要件定義書の中身と受入れテストについての責任は発注者とする。

2）開発プロセス標準を見直し、上流の要件定義を押さえる（上流工程完璧主義）。

その結果、以下の効果が現れてきた。

・要件漏れ等の上流工程に起因する品質上の問題が著しく減少した。

・プロジェクトの透明性が増し、組織同士の継続的な信頼関係が向上した。

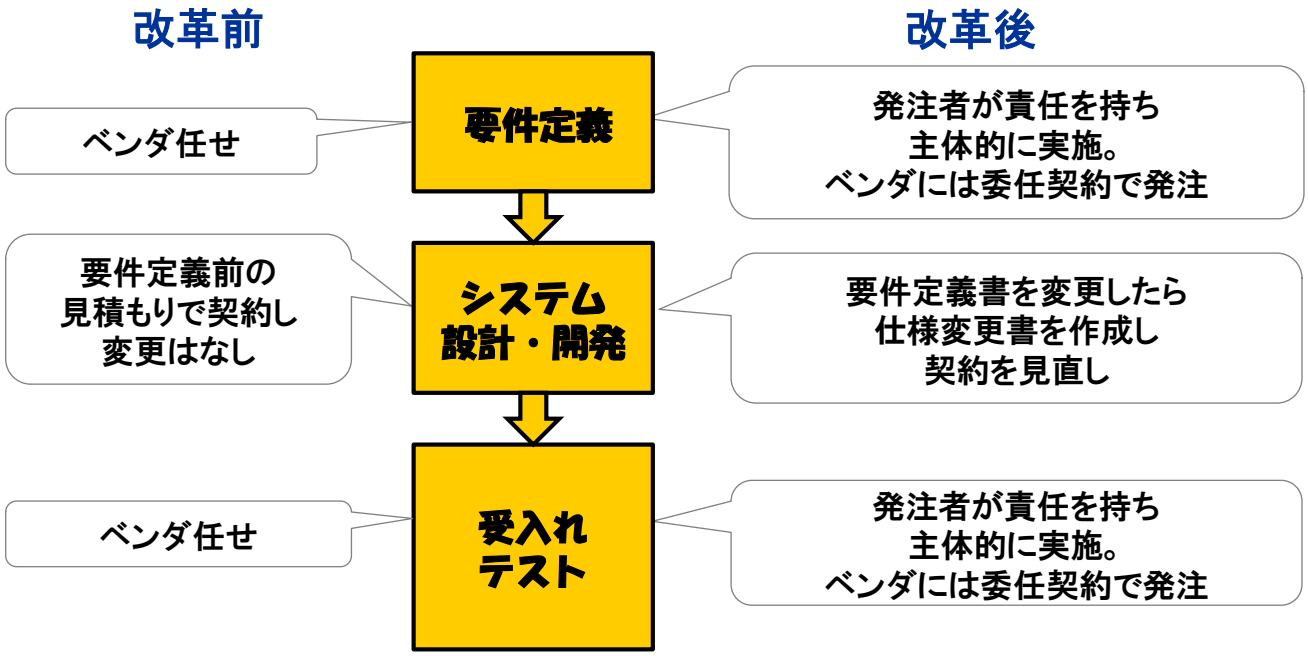


図２．２．２―１　発注者の責任の明確化

[8] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-16

活用が考えられる事例

◆ケース３　要件定義についての活用例

A 社は、発注者として開発受注者に開発依頼を行ったところ、要件の検討不足によるシステム障害が多発した。

原因は、A 社が発注者としての要件定義を明確にしないまま受注者に発注したため、開発途上において多数の手戻りが発生し、十分なテスト工数が得られない状況となったためである。障害の根本原因は、A 社が発注者として要件定義の明確化という発注者責任を果たしていないことであった。

活用を考える

この教訓を活用することにより、発注者側の責任分担は要件定義であることを明確にし、発注者側が要件定義と受入れテストに責任を持って開発をする体制を取ることができる。

このような体制は、発注者、受注者にそれぞれ重要な緊張感を持たせることになる。つまり、発注者は、要件定義に矛盾、不足などの不備があった場合、それは開発コストに直接影響することになる。また、受注者は、要件定義に問題がなければ、それを理由にした開発遅れとかコストアップを主張することができず、自らの責任が明確になる。

IPA/SEC では、発注者との合意形成を取る上でのポイントを「経営者が参画する要求品質の確保～超上流から攻める IT 化の勘どころ～」（文献 2-3）としてまとめているので、こちらも参考にされたい。

◆ケース４　コミュニケーション

発注者の B 社では、要件定義に曖昧さが残ったまま、一方的に受注者のベンダに開発の納期を押し付け、なんとかサービスインにこぎつけた。しかし、その後システム障害が出続けた。また、ベンダは、責任の範囲が明確で無いため、運用保守フェーズでは受身的な態度を取り、システム障害時も責任を回避する発言が出たりした。その結果、なかなかシステム障害を減らすことができなかった。

活用を考える

このようなケースの場合、発注者と受注者の関係改善を行うことが重要であるが、このＧ２の教訓を参考に、「要件定義は発注者側の責任」を明確にすることが改善の第一歩となろう。

発注者が受注者のベンダに開発を依頼した場合、発注者と受注者が要件定義書をベースに、双方で、要件が新規依頼なのか、瑕疵なのかを明確にする調整を行うことである。そうすることにより、ベンダの意識にも変化が現れることが期待される。

そのような双方の信頼関係ができれば、次のシステム更改の設計時に受注者ベンダ自らが障害を減らすための提案を出すなど、システム障害に対する前向きな姿勢を期待できる。

２．２．３．上流工程での運用部門の関与に関する教訓（Ｇ３）[9]

[教訓 G3]
運用部門は上流工程(企画・要件定義)から開発部門と連携して進めるべし

概要

最近、システム運用の現場で以下のような問題が発生した。

・A 社では、新システムの運用を開始してからオペレータの操作ミスが多発した。

・B 社では、販売店向け発注システムを Web システムに移行したところ、入力データのミスにより電文データが誤って編集され、接続会社間で障害対応時の各種調整に手間取ってしまった。

原因は以下の通りである。

① A 社では企画や要件定義段階において、オペレータ操作に関する運用の要件検討が十分されていなかった。運用テストの段階から初めて運用者が参加してテスト及び引き継ぎを行ったがオペレータ操作関連のバグが多発して収束しないまま本稼働を開始した。要件定義段階でのオペレーション要件の検討もれが原因だった。

② B 社ではシステムへのデータ入力ミスを抑止する工夫や仕組みが考慮されていなかった。また、本システムの接続先との間で、有事に関する取り決めや対応範囲などが整理できておらず、コンティンジェンシープランが共有できていなかった。

上記①、②の根本原因は、運用者が要件定義作業へ参加していないことや、参加していても運用要件が取り込まれなかったことに起因している。

上記の対策として、企画・要件定義作業の段階において、運用者の視点からシステム要件を確認するようにすることが重要である。運用者が確認する項目の例を以下に示す。

表２．２．３－１　「運用者が企画・要件定義工程で確認する項目」の例（一部抜粋）

No	工程	分類	項目	全体で確認する項目	運用者が確認する項目
1	企画	起案	■経営戦略を見据えたシステム構築及びシステム構築の目的・目標の明確化	①経営戦略の具現化 ②情報(システム)戦略の具現化 ③システム化の目的・方針 ④納期(スケジュール) ⑤システム利用期間、ライフサイクル概要計画	①要件の把握 ②納期(スケジュール)の確認 ③システムのライフサイクル(更新間隔)確認 ④経営戦略の理解 ⑤情報(システム)戦略の理解
2		現状分析	■システム(業務)の現状分析、問題点・課題の抽出と分析	①運用状況 ②問題点・課題 ③最新のシステム動向、技術動向の分析	①構築ノウハウの提供 ②現状課題の提供 ③最新技術動向・トレンド等の情報分析提供 ④運用状況の報告
2-2		企画立案	■新システムの企画立案	①全社目標の体系化と施策の定義 ②情報システム要件のまとめ ③システム化の企画立案	①運用改善から見た新システム要件の提案
3		投資対効果	■システム構築における投資対効果の明確化	①投資対効果 ②コスト計画の立案	①運用要件者側に必要な費用の見積作成
4		承認	■システム構築の承認	①システム構築の承認を得る	

（以下、表省略）

[9] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-19

活用が考えられる事例

◆ケース５　運用ミスを誘発するシステム

A 通信会社のサービスは、利用者を 2 群に分けて同じ機能を持つサーバ A 群と B 群に分散して収容している。

今回ソフトウェアの更改にあたって、B 群サーバに誤って A 群サーバ用のソフトウェアを適用してしまったため、B 群側から A 群側のユーザの情報を参照・更新可能となってしまった。

原因は、A 群と B 群のシステム設定ファイルのファイル名を含めて、全く同一であったため、運用時に誤作業を引き起こすことになってしまった。

活用を考える

このケースで考えられるのは、運用面でのヒューマンエラーを考慮しない設計上の問題があったことである。

A 群と B 群のシステム設定ファイルのファイル名を含めて、全く同一であったことは、運用面での作業誤りを防止する配慮が設計時になされていなかったと考えられる。

このような障害を減らすためには、今回の教訓Ｇ３「運用部門は上流工程（企画・要件定義）から開発部門と連携して進めるべし」を取り入れることが重要である。運用面の効率性、利便性を要件定義に盛り込んだ設計を開発時に検討することにより、運用、保守時の作業効率を高め、障害を引き起こしにくいシステムを設計することができる。

◆ケース６　運用要件漏れの改善

B 社では、システム開発時に運用部門の参画が十分でなかった。そのためサービス稼働後に運用ミスによるシステム障害が多発し、運用コストを増大させた。

そこで、B 社は、原因を分析することにした。その結果、運用ミスは、運用担当者の手順指示ミスや申請ミスなどの運用プロセスでのケースが考慮されていないために起きている事例が多かった。つまり、運用要件を検討する優先度が低く、運用の効率化や運用方針が不明確であり、運用保守での課題が事業部門や役員にフィードバックされていないことなどの原因が考えられた。

活用を考える

このような場合は、教訓Ｇ３のように、上流工程での運用部門と開発部門の役割を明確にして、それぞれの部門が納得する要件を整理し、サービス開始後の運用面での障害を減らすことである。場合によっては、設計時の工数に運用面での工数が増大するかもしれないが、保守運用時の運用工数は、大幅に削減することができる。

運用プロセスを適切に整備して現場に定着させるだけでなく、常に改善を繰り返すことが必要である。

２．２．４．障害発生時連絡の情報共有に関する教訓（Ｇ４）[10]

[教訓 G4]
運用者は少しでも気になった事象は放置せず共有し、とことん追求すべし

概要

A 社は、運用者がシステムの異常に気づいたにも関わらず、保守者が異常を誤認して、オンラインサービスの開始が遅れ、数時間停止する事態となった。

原因は、運用担当者が察知した異常を、保守担当者が「異常なし」と誤認したためであった。また、運用部門責任者も十分に確認せず、報告そのままに問題なしと判断し、CIO への報告を怠った。さらに、運用担当者は、異常状況に気づいていたが、運用マニュアル通りに作業し、その気づきを運用部門の責任者等に伝えていなかった.

対策として、以下の案を実施した。

① 運用担当者が現場での異常を察知したときには、状況判断できる運用部門の社員にその情報を連絡して協議する態勢を作る」ことを運用マニュアルに明記した。

② 障害対応体制面での改善・強化を行った。

・事象として障害と断定できない場合でも障害の可能性がある場合は早期に上位役職者へ報告するルールの追加作成

・状況判断できる運用部門社員の 24 時間常駐

③ 確認手順と、その中の項目を明確に定義した。

④ 教育・訓練を実施した。

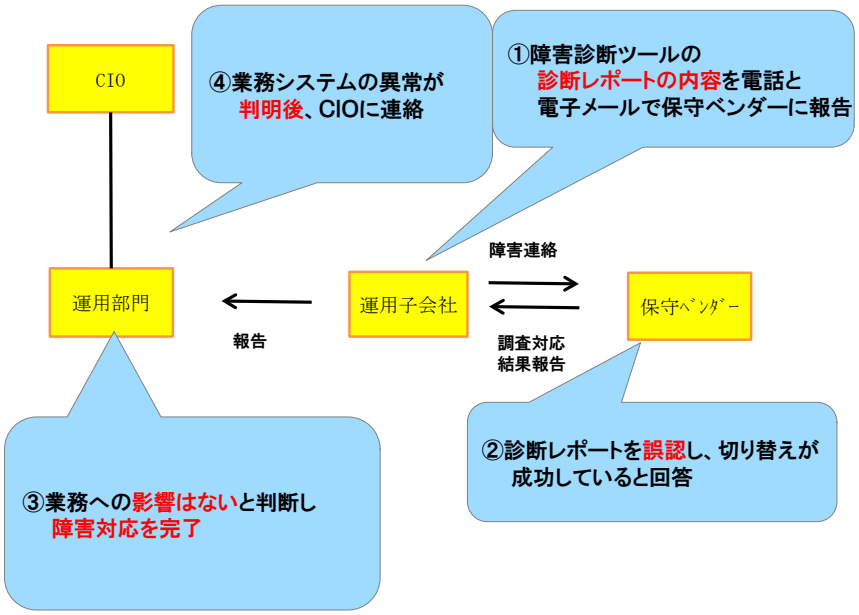


図２．２．４－１　障害の経緯

[10] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-23

活用が考えられる事例

◆ケース７　運用体制

A 社では、運用保守のオペレーションを外部委託しているが、委託先のオペレーション要員体制がなかなか安定しなかった。原因は、委託元の運用部門の一貫性のない指示などのモチベーションを低下させるような事態が続いていたことが大きいと考えられた。

活用を考える

教訓Ｇ４は、システム障害を減らすためには、運用オペレーション要員も含んだ、一貫した連携がなくてはできないことを教えている。

このケースでは、明らかにオペレーション要員のモチベーションの低下が原因とみられるが、根本原因は、そのような低下を招いた管理面での問題がある。一方的に委託元が委託先に苦情を言っても、根本的問題は解決しない。

改善するためには、この教訓を活用し、運用保守体制のあり方、日々の運用の課題を委託元と委託先のメンバで議論し合うことである。この実践により、双方が日々改善する中で、障害発生時の連携もスムーズに行えるようになり、オペレーション要員のモチベーションも向上し、体制も安定することが期待される。

◆ケース８　意見が言えない職場の雰囲気

B 社では、10 年前からスタートしたシステムを運用している。このシステムについて何でも知っているボス的存在のＣ氏は、「自分のやることに文句を言う者はいない。」と思っており、自分独自の方法で保守作業を実施していた。また、上司のＤ氏は、そのことを知りながら、Ｃ氏についてはシステムに詳しいため、口出しすると他の作業の進捗に影響がでるので、指導できずにいた。同僚達は、運用ルールを守った方法で保守作業を行っていたが、やはりＣ氏が運用ルールを守っていないことを知りながら、注意できずにいた。

ある日、Ｃ氏が運用担当の時、Ｃ氏は、保守作業のテスト環境での事前確認や事前テスト確認、本番環境での作業監視を全く誰のチェックも受けずに単独で行った。その結果、システムの本番環境を壊す事態が発生し、B 社は、翌日のサービスを提供することができなくなった。

活用を考える

このケースの問題は、「ボス的存在のＣ氏」の行動に問題があることは当然だが、本質は、組織として運用ルールを守るモラルと仕組みが欠如していたことによる。管理者を含め、職場の誰もが「ボス的存在のＣ氏」に注意することができなかったことは、運用ルールを守るモラルと仕組みを組織として構築できていなかったことを意味する。教訓Ｇ４「運用者は少しでも気になった事象は放置せず共有し、とことん追求すべし」は、運用に携わる全てのメンバが気になった事象を放置してはならないことを伝えている。そのためには、職場のコミュニケーションが円滑に行えるマネジメントが重要である。

２．２．５．共同利用システムの業務処理量予測に関する教訓（Ｇ５）[11]

[教訓 G5]
サービスの拡大期には業務の処理量について特に入念な予測を実施すべし。

概要

稼働開始から１年を経過している X システムの共同利用システムが、利用増大傾向の中、負荷集中によりダウンした。

直接原因は、負荷が重いバッチ型オンライン業務のデータ量が予想よりはるかに大量となり、その影響で DB サーバ内ソフトのメモリリーク・バグが顕在化したためであった。根本原因は、共同利用各社の処理件数予測がベンダ任せであったため、十分な対応が取れなかったためであった。

X システムは、対策を以下のように実施した。

・利用各社による運営協議会の設置を行った。

・キャパシティプラニングを含めた共同利用各社の責任を明確にした。

・ベンダとの契約時に X システムの運営協議会を行い、その中で決めるべき項目を明記した。

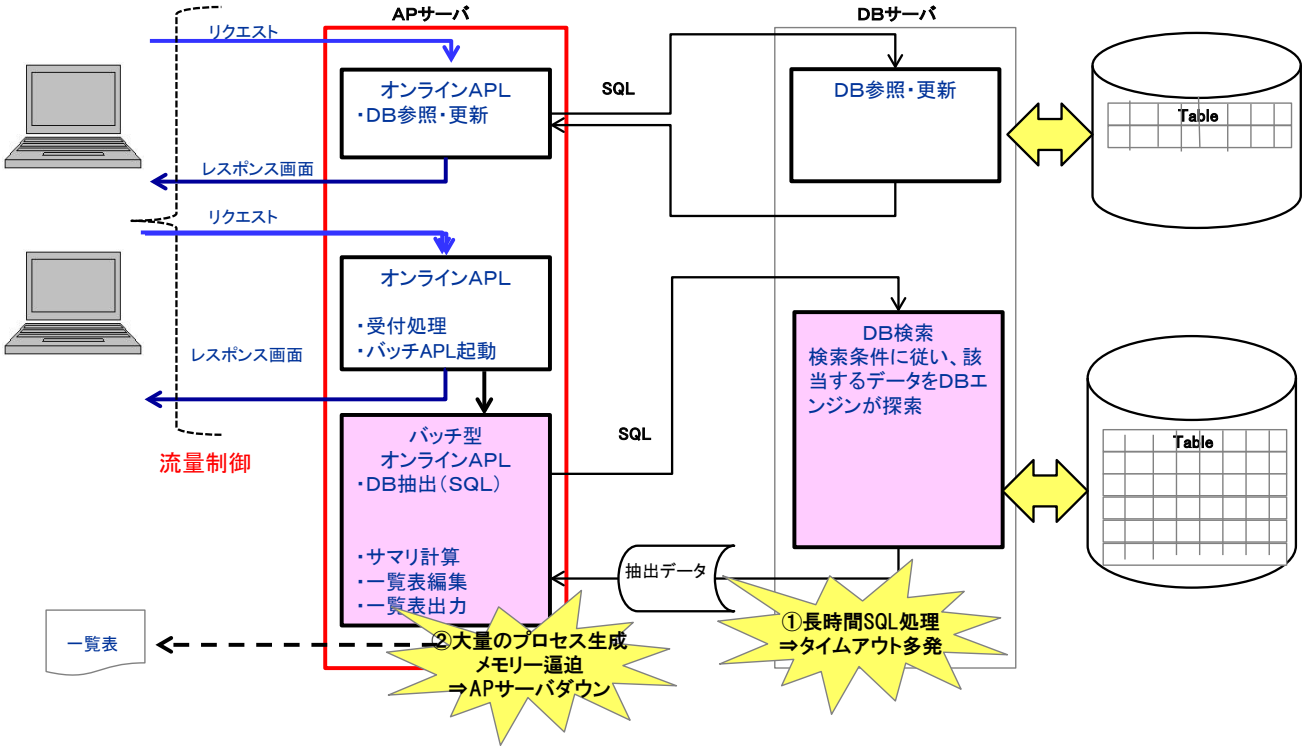


図２．２．５－１　X システムの概要と障害の流れ

[11] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-26

活用が考えられる事例

◆ケース９　共同運用体制

共同センターの運用保守のオペレーションを受託しているＡ社は、参加企業からの要件変更依頼を個別に受けていた。Ａ社は、その受けた依頼を他の参加企業との調整をせず行っていたため、個別対応のオペレーションが増えていき、全体の効率に影響が出るようになってしまった。

原因は、共同センターとしてのＡ社が参加企業同士の意思疎通を図らず、共同センター全体の効率を検討する場を設定しなかったことにより、参加企業が自社の都合を優先し、共同センターの運営に責任を持たなかったことである。

活用を考える

教訓Ｇ５で示したように、共同センターの運用保守は、全ての参加企業が責任を持つ体制を前提にする必要がある。

このケースで、教訓Ｇ５を活用するならば、運用保守体制のあり方を参加企業間で議論しあう場を設定し、日々改善する中で、障害発生を抑え、全体効率を考慮した対応を行えるような体制を構築しなければならない。

◆ケース 10　共同利用各社の情報共有

鉄道各社は、「旅客販売総合システム」の管理をＢ社に委託しており、そのサーバに各社が接続している。

上記システムのサブ機能である「ネット列車予約サービス」でシステム障害が発生し、携帯電話・パソコンからの座席予約・変更操作が利用出来なくなった。原因は、プログラムの設定ミスにより、サーバがダウンしたためだった。

この障害を受け、鉄道各社は、Ｂ社との運用連絡会議を設けて常時情報共有を行い、障害発生時の運用体制を明確にした。

活用を考える

このケースは、共同利用されている鉄道各社とシステム管理会社Ｂ社との連携改善を行った事例である。

共同利用されているシステムの委託元同士は、競合関係にはない企業同士が参加しており、運営の改善は行い易い関係である。

そこで、システム障害の対策として、発生後の情報の流れ、復旧時間の確認などを立てておくことは当然であるが、更にシステムの改善に向けて積極的に関係者が共同利用のメリットが生まれるような活動に取り組むことにより、参加企業がより高い競争力を得ることができる。

２．２．６．作業ミス、ルール逸脱の問題に関する教訓（Ｇ６）[12]

[教訓G6]
作業ミスとルール逸脱は、個人の問題でなく、組織の問題！

概要

A 社情シス部門は、多数のグループ会社及び関連会社が利用するグループウェア・サービスを運用している。

ある日、運用作業者が誤ってグループウェアの全ユーザデータを削除してしまった。

直接原因は、不慣れな運用作業者（新人）が、独断で、運用規定外の手段（統合管理ツールを介さないサーバへの直接アクセス）により、誤操作（ルール逸脱）したことによる。

根本原因は、以下の様な組織上の問題があった。

・情シス部門は、作業依頼部門からの依頼をマネジメントできていなかった。
・繁忙な環境下、迅速な処理が求められる状況で、各メンバは、お互いの作業に追われて連携できていなかった。そのため、不慣れな作業者は、多忙な熟練者に作業方法を聞くことができなかった。
・運用チーム内のスキルの共有が不十分であった。

対策として、以下のような組織的な総合対策を行った。

・作業を受ける場合のリスクを考慮した受諾の判断基準を作成した。
・複数名体制での作業実施等、ルールを逸脱しない作業規定を作成した。
・普段のチーム内のコミュニケーションの向上を図った。

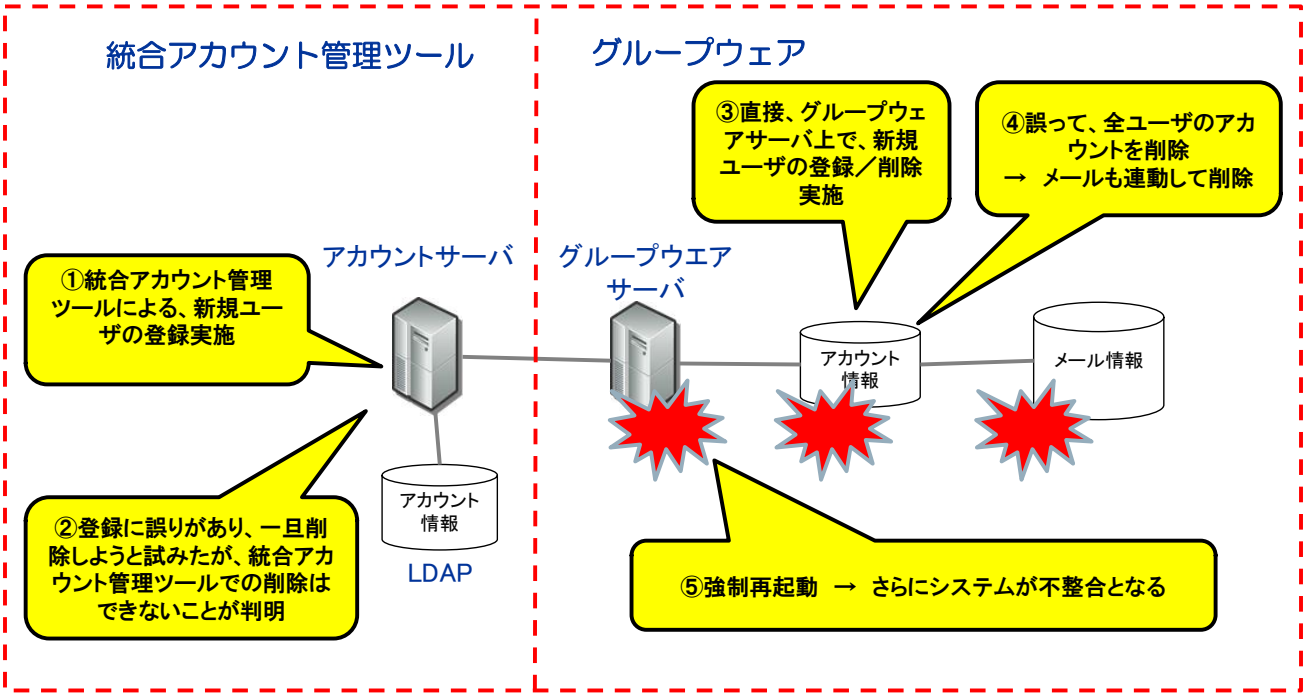


図２．２．６－１　障害状況

[12] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-29

活用が考えられる事例

◆ケース 11　作業ミス

A 社は、予約システムの誤設定により、１ヶ月分の座席予約情報を消失させてしまった。そのため、全ての顧客に座席予約のやり直し（再予約）を依頼した。

原因は、担当者が予約システムの時刻表情報を更新する際に、誤って座席指定の予約情報を消去してしまったことによる。その時、バックアップデータも消去してしまった。作業は担当者２人による二重チェックを行っていたが防げなかった。

A 社は、このようなミスを防ぐため、今後は３人体制で行うことにした。

活用を考える

作業ミスは、とかくその作業者のヒューマンエラーと見なされ、作業者個人の自覚の問題として責任を個人に押し付けてこと足りるといった事例が多い。このケースについても、２人で間違えたのだから３人体制で行えば大丈夫といった対策は、まさに個人の問題としているように思える。

航空、原子力、医療と言った人命を扱う分野では、「ヒューマンファクターズ」[13]と呼ばれる人の誤りを科学的に、また組織、マネジメントも含めた学問として取り組む研究が進んでいる。

IT システムにおける作業ミスも、「ヒューマンファクターズ」の観点で減らすことが望まれる。教訓Ｇ６「作業ミスとルール逸脱は、個人の問題でなく、組織の問題！」は、ヒューマンファクターの観点から記述されている。

◆ケース 12　作業ミスの改善

運用保守のオペレーションのミスが多発している B 社では、作業員一人ひとりの意識が低い点を問題にして、組織的な観点での問題をどうするかについては、検討していなかった。作業ミスが起きるたびに、管理者は、ミスを犯した作業員に始末書を提出させ、これを続けていけばミスは無くなると考えていた。

活用を考える

このケースはやや極端ではあるが、作業ミスを個人の問題と考える点では、ケース 11 と同じである。B 社の取組みについては、教訓Ｇ６を活用して、運用保守体制のあり方について管理者を含んだ運用作業員全員で議論しあい、組織の問題についても意見を出しあうことを提案したい。そうでなければ、本質的な改善は見込めないであろう。

運用作業員、管理者が日常的にグループ討議を行い、改善点をみんなで議論し実践していく取組みを行う QC 活動を通じて、作業ミスの発生を徐々に改善することができる。

---

[13] 本来「ヒューマンファクター」だが、ここでは学問として扱うとの意味で敢えて「ヒューマンファクターズ」としている。

２．２．７．クラウドサービス利用時の障害対応体制に関する教訓（Ｇ７）[14]

[教訓 G7]
クラウド事業者と利用者が連携した統制がとれたトラブル対応体制を整備すべし

概要

A 社は、クラウドサービスに移行したシステムの通信機器に障害が発生し、（単なる負荷分散装置の障害にも関わらず）丸１日間業務が停止した。

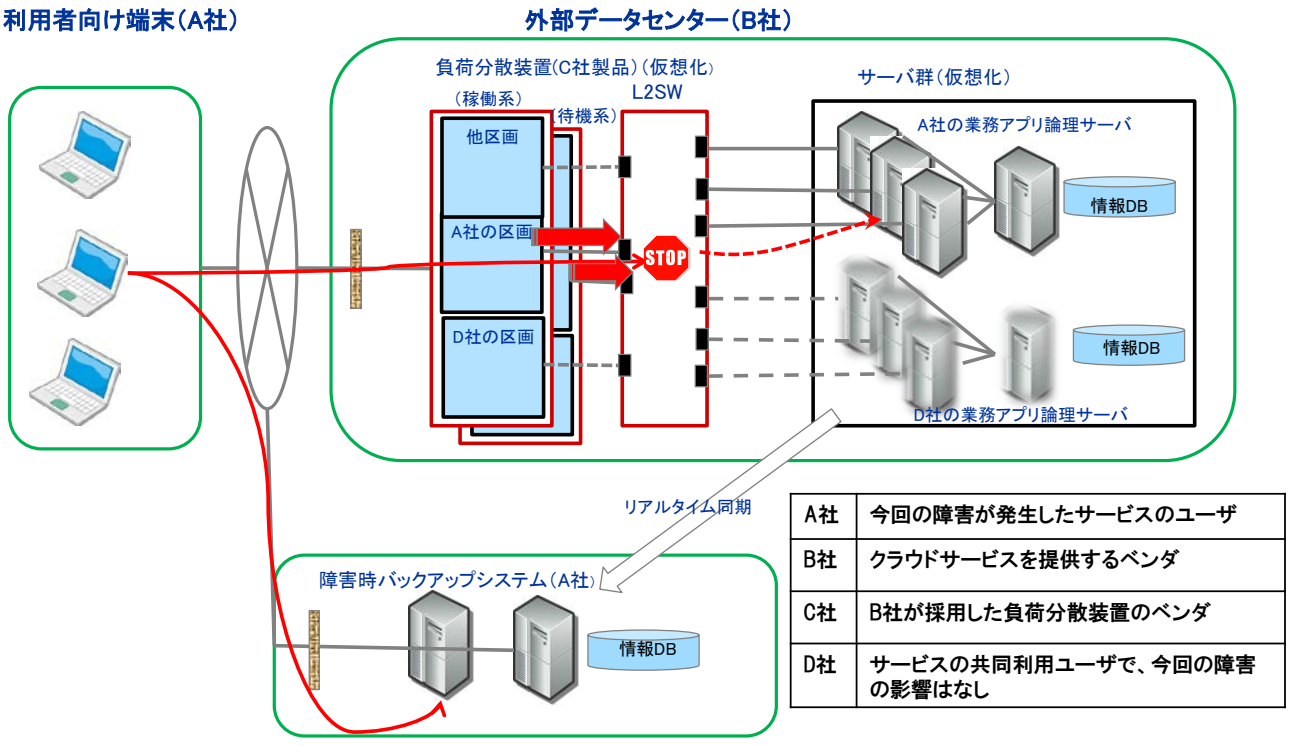
原因は、運用時のトラブル対応体制が決まっていなかったからである。

対策として、以下の体制の整備を行った。

・障害対応体制（報告、連絡、相談）を明確にした。

・クラウド事業者との契約時にサービスレベル定義（責任分界点の明確化）を行った。

・クラウド事業者と関連サードパーティ業者間の障害対応体制を確立（適確な連携体制）した。



A社	今回の障害が発生したサービスのユーザ
B社	クラウドサービスを提供するベンダ
C社	B社が採用した負荷分散装置のベンダ
D社	サービスの共同利用ユーザで、今回の障害の影響はなし

図２．２．７－１　システム概要

[14] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-33

活用が考えられる事例

◆ケース 13　ベンダへの不満

クラウドサービスを利用している A 社は、ベンダの対応が遅いことに対して、ベンダに改善を要求していたが、なかなか改善されないことに不満を持っていた。

ベンダは、A 社の要望は理解していたが、A 社の要望が A 社内できちんと調整された要件でなかったこともあり、どうしても目先の対応を優先してしまい、A 社を満足させる対応ができなかった。

活用を考える

このケースでは、教訓Ｇ７「クラウド事業者と利用者が連携した統制がとれたトラブル対応体制を整備すべし」を活用し、ベンダと SLA を含め対策を検討し合あうことが重要である。その場合、ベンダ作業量を勘案し、優先順位を明確にすることが双方の合意を円滑にすすめるポイントである。

そのような取組みを行えば、ベンダも自分の責任範囲が明確になるため、A 社は、ベンダから新たな提案を引き出すことができる。さらに、スムーズなコミュニケーションをとることができれば、障害も減らすことができる。

クラウドサービスにおいても、ユーザとベンダとの役割や責任が明確にならないとスムーズな運用が行えない。

◆ケース 14　復旧時間の長期化を覚悟

B データセンターは、同センターを利用していた多数のシステムが停止になる障害を起こした。C 銀行の設置する ATM が利用不能になり、D 銀行の全サービスがダウンした。また、E 銀行のインターネットバンキングや ATM が利用不能になった。更に F 社のメールサービス、ブログ、クラウドなどのサービスが利用できなくなった。このように多数のシステムが障害になったため、復旧までに丸 1 日近くを要した。

原因は、商用電源が落ちた（停電）時に、本来稼働するはずの UPS（無停電電源装置）に電源が切り替らなかったことによる。B データセンターは、電源設備に十分対策を行っていたはずであったが、UPS の出力分電盤が長期のホコリの堆積によって故障していたことに気づかなかった。そのため、全てのシステム機器の電源が落ちてしまった。

活用を考える

クラウド利用者は、クラウド事業者が障害になると、復旧が長時間に延びることをリスクとして考慮する必要がある。このケースのように、いっぺんに多数のシステムが障害になるために、自分のシステムがクラウド事業者にどのように優先付けされるのかなども協議される必要がある。

教訓Ｇ７を活用し、ベンダと SLA を含め対策を検討し合あうことをお勧めする。また、このような事態を想定した、リスク対策も立てておくべきである。

２．２．８．共同利用システムの利用者間情報共有に関する教訓（Ｇ８）[15]

[教訓 G8]
共同利用システムでは、非常時対応を含めて利用者間の情報共有を図ること

概要

A 社と D 社は、あらかじめ協議を行い運用コスト削減という目的が一致したことからシステムを共同利用することとし、ベンダ B 社に運用を委託した。

ある日、B 社の通信機器に障害が発生し、A 社のサービスが、（単なる負荷分散装置の障害にも関わらず）丸１日間停止した。

原因は、ベンダ B 社、および共同利用者 A 社と D 社間の障害発生時の連絡体制が決まっていなかったことにより、復旧の段取りを行うのに多大な時間を要したことによる。

再発防止策として、以下を行った。

・障害復旧時の関係者（サービスの共同利用者である A 社と D 社、事業者（ベンダ）である B 社）の役割分担や、システムにおけるコンポーネント（各種機器（ハード・ソフト）、データ）ごとの回復措置の利用者業務への影響範囲を明確化する（表２．２．８－１）。特に、障害発生時に停止／再起動する単位と、その停止により影響を受ける利用者の範囲を事前に整理・明確化する。

・B 社は、システムを停止／再起動させる場合についての条件や手順、責任等に関する取決めを SLA で定義し、共同利用各社と合意する。

・共同利用者間の情報共有の強化を行う。基本的にこれはサービス事業者の役割であるが、共同利用サービスでは、共同利用者間の日常の情報共有を行うと共に、非常時の緊急連絡体制等を定めておくことが望ましい。

表２．２．８－１　コンポーネント（今回の事例）

ハードウェア	負荷分散装置、ネットワーク機器、サーバ(AP,DB,Web)
ミドルウェア	仮想化OS,ｹﾞｽﾄOS,OLTP(オンライン基盤ソフトウェア)など
アプリケーション	業務アプリケーション
データ	データベース,一般ファイル

[15] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-36

活用が考えられる事例

◆ケース 15　メンテナンス作業の連携ミス

共同で IC カードを使うシステムにおいて、個別に管理する A 社と B 社の間で、メンテナンスを実施する情報が共有されていなかった。

ある日、A 社がメンテナンスを行ったところ、B 社のサービスが完結しない時間帯が発生してしまい、B 社の利用者へ通告がないまま B 社のシステムも止めることになってしまった。そのため、利用者に多大な迷惑をかけてしまった。

活用を考える

教訓Ｇ８は、「共同利用システムでは、非常時対応を含めて利用者間の情報共有を図ること」でひとつの共同利用システムで起きた事例の教訓ではあるが、このケースのように１つの共同カードが２つのシステムでの連携に関わる場合も活用できるケースである。

この教訓Ｇ８を活用し、お互いのメンテナンス時間を連絡し合い、事前に調整することで、利用者のサービス停止を事前にアナウンスすることができ、このような障害の防止が期待される。

◆ケース 16　自主的情報共有制度

C 業界では、D 社で起きたシステム障害が、業界内の E 社でも同様に起きていた。このような事態が度々起きるため、C 業界全体としての社会に向けた対策を迫られていた。

活用を考える

既に業界内で、ヒヤリハット情報を共有する仕組みを作っているところがあるので、紹介する。

また、共有される内容は、IT システムに限らないが、他業界においても事故を未然に防ぐ取組みとして参考になる。

・航空安全情報自発報告制度［VOICES］

航空安全情報自発報告制度は、航空安全プログラムの適用に伴い、義務報告制度では捕捉しにくい民間航空の安全に関するヒヤリハット情報を幅広く収集するために設置されたものであり、公益財団法人航空輸送技術研究センター（ATEC）が運営している。

アクセス：　https://asicss.cab.mlit.go.jp/voluntary/

・原子力施設情報公開ライブラリー［NUCIA］

1966 年（昭和 41 年）の最初の原子力発電所がした当時から現在の情報まで、原子力発電所や原子燃料サイクル施設の運転に関する情報を広く共有するために公開され、安全性や透明性を一番に考え、誰でも自由に情報を閲覧することができる情報公開サイト

アクセス：　http://www.nucia.jp/index.html

２．２．９．非常時代替事務マニュアルに関する教訓（Ｇ９）[16]

[教訓 G9]
システム利用不可時の手作業による代替業務マニュアルを作成し
定期的な訓練を行うべし

概要

A社は、障害時バックアップシステムをあらかじめ用意していた。

ある時、システム障害が発生した。バックアップシステムがサポートする参照系業務については、基幹業務システムと同じオンラインマニュアルが整備されており、それを利用して業務を遂行できた。しかし、登録系業務は、バックアップシステムでは実行できなく、また登録系業務のシステム障害時の対応手順のマニュアルも存在しなかったため、顧客の登録・変更申請に対応できなかった。

結果として、窓口に来た顧客には、帰って頂く対応となった。

原因は、過去にシステム障害が発生したことがなく、システムが利用できない前提での業務マニュアルがなかった

A 社は、今回の障害を契機に、従来の災害対応中心の IT-BCP を拡張し、再発防止策を検討している。

内容としては、事業部門と情シス部門が協力しあい、

・システム利用不可時の代替手段の整備

・業務マニュアルの作成

を行った。これにより、システム障害時も手作業で顧客の登録・変更申請が行えるようになった。

[16] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-38

活用が考えられる事例

◆ケース 17　システム全面停止

A 金融会社では、前日の夜間処理が終了しなかったため、翌日の取引情報を各店舗に発信することができず、半日全店舗の窓口が開店休業となってしまった。

A 金融会社は、このような事態を想定した業務マニュアルを用意していなかった。

活用を考える

このケースのような事業継続ができない事態を回避するためには、教訓Ｇ９「システム利用不可時の手作業による代替業務マニュアルを作成し定期的な訓練を行うべし」を参考にしていただきたい。

教訓Ｇ９では、きちんと代替業務マニュアルを作成することが重要と判断し、事業部門と情シス部門とで対策を立てることができた。更に自然災害なども考慮した BCP（事業継続計画）も検討することにしている。

◆ケース 18　航空管制システム停止

航空各社から提出された飛行計画を一括集約して全国各地の航空管制に配信する飛行情報管理システムに障害が発生した。

電源装置が故障し、バックアップ機も使用できない事態となった。その後電源装置の交換により復旧したが、その間は、ファックスによる手作業で対応した。

活用を考える

システムが停止したからと言って、業務を停めるようなことが起こってはいけないシステムについては、このケースのように手作業での代替案をリスク対策としてもっている。

・銀行においても、長時間に渡って勘定系システムが停止した場合の、窓口での支払いルールを定めている。
・航空会社では、飛行機に積み込む荷物、乗客の重量、重心バランスを計算する「重量バランス管理」システムが停止した時、手計算にて対応している。
・鉄道会社では、IC カード（乗車、定期券）による不具合があった時、全ての改札機の入退場をフリーにした。

重要な基幹システムや多くの利用者に影響の出るシステムにおいては、システムが動かない最悪の事態を想定したリスク対策として、手作業は最終手段である。

また、教訓Ｔ２「蟻の目だけでなく、システム全体を俯瞰する鳥の目で総合的な対策を行うべし！」でも、系切替えの最終手段として、手動による切替えを提示している。

２．２．１０．フェールソフトに関する教訓（Ｔ１）[17]

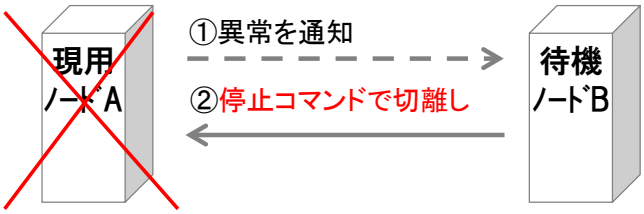
[教訓 T1]
サービスの継続を優先するシステムにおいては、
疑わしき構成要素を積極的にシステムから切り離せ （“フェールソフト”の考え方）

概要

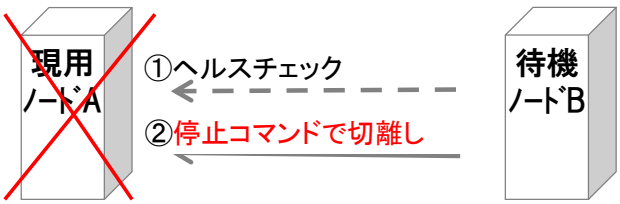
業務内容に基づいて、システム毎にポリシーを作成した上で、フェールソフトの考え方を適用した。ハードウェア機器の故障、ソフトウェアの処理プロセスの異常等があった場合には、その部位を積極的に停止させることでシステムから切り離す、場合によってはその系全体を放棄するといった考え方のもとに処理・対応する。

一方、そのような状況下で一部の部位や系をシステムから切り離しても、システム全体としてのサービスは継続できるように、フェールソフトの考え方に基づいて設計・運用する。機器やソフトウェアそれぞれの動作継続を優先しすぎると、予期せぬ障害の場合にサービスへの影響がかえって拡大する場合がある。サービスの継続を優先させるためには、むしろ積極的に関連する部分をシステムから切り離す方が良い場合が多いことに留意すべきである。

1）自身のヘルスチェックの場合



2）他系のヘルスチェックの場合



3）自動停止できない場合は手動による停止で切離し

図２．２．１０－１　フェールソフトによる切替え時のイメージ

[17] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-41

活用が考えられる事例

◆ケース 19　障害検知によるサーバ切替え

A 電力会社のプラント内での２重化されている制御管理システムが停止した。本来、自動で稼動系サーバから待機系サーバに切り替わるべきところ、切り替わらなかった。そのため、手動で切り替えた。

稼動系サーバが障害となった原因は、ハードウェアの故障であった。稼動系サーバが、故障信号を発信せずに停止したため、待機系サーバが稼動系サーバの異常を検知できなかった。

この障害を教訓に、故障信号を出さずに稼動系サーバが停止した場合でも、待機系サーバが稼動系サーバの停止を感知して強制的に待機系サーバが【稼動系】に切り替わる故障検知機能をシステムに追加した。

活用を考える

このケースでは、既に教訓Ｔ１「サービスの継続を優先するシステムにおいては、疑わしき構成要素を積極的にシステムから切り離せ（“フェールソフト”の考え方)」に沿った対応である。つまり、「故障信号を出さずに稼動系サーバが停止した場合でも、待機系サーバが稼動系サーバの停止を感知して強制的に待機系サーバが【稼動系】に切り替わる故障検知機能」をシステムに追加したことは、“フェールソフト”の考え方をシステム障害時のサーバ切替えに活用したケースと言える。

◆ケース 20　サービス継続

B 物流会社では、全国翌日配送を実現するため、物流システムの稼動継続を可能とするネットワークを構築した。しかし、ネットワーク機器の増加に対応できるネットワーク監視運用が追いつかず、システム障害発生時に障害機器の発見が遅れ、サービスを長時間止める事態がたびたび発生していた。

活用を考える

サーバ、ネットワーク装置などは、既に負荷分散のために、複数台の多重構成になっているため、ネットワーク監視装置によるフェールソフトの導入を検討すべきである。教訓Ｔ１の考え方と同様に、「疑わしき構成要素を積極的にシステムから切り離す」ことに重点を置き、ネットワーク監視装置からの「疑わしき装置」の切り離しを行い、性能不足問題を起こさない対策を立てることが重要である。

また、教訓Ｔ１１「サイレント障害を検知するには、適切なサービス監視が重要」とも関連があるので、併せて活用していただきたい。

２．２．１１．システム全体を俯瞰した対策に関する教訓（Ｔ２）[18]

[教訓 T2]
蟻の目だけでなく、
システム全体を俯瞰する鳥の目で総合的な対策を行うべし！

概要

A 社の制御系システムの下位システム（以下、下位）にある制御装置の稼動系に故障が発生した。自動的に待機系に切り替わるところが切り替わらなかった。上位の監視端末からの指示による系切替えを実施したが、失敗した。

対策では、障害が下位で起きた場合、障害を起こした下位だけの対策を考えがちであるが、蟻の目（下位）の対策だけでなく、システム全体の視点で、鳥の目（上位）対策も合わせて行った。つまり、システム全体を俯瞰する、上位システム、下位システムを併せた総合的な対策が重要である。

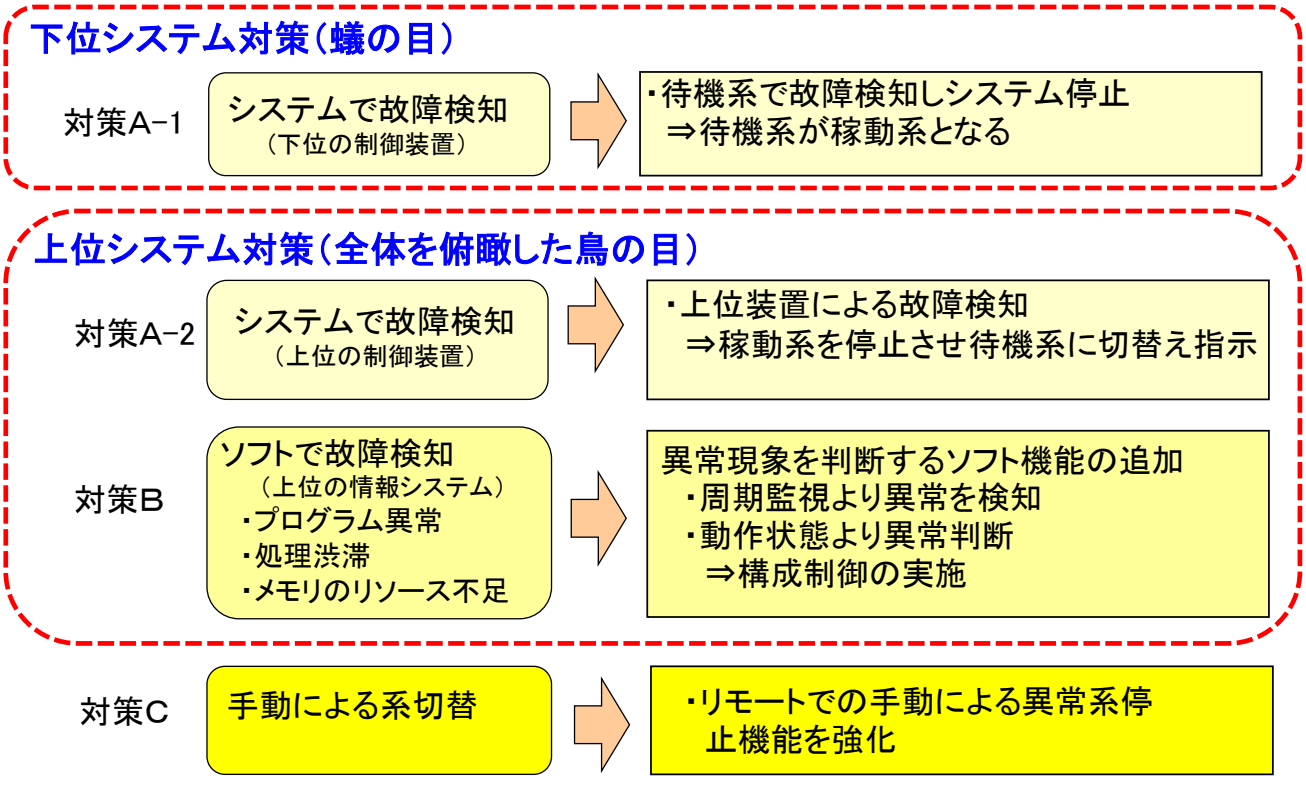


図２．２．１１－１　システム全体での障害対策

[18] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-44

活用が考えられる事例

◆ケース 21　本社と営業店の連携ミス

A 流通会社では、消費税率引き上げに伴うシステム更新でトラブルが発生し、多くの店舗で開店が遅れた。全店で朝からシステムの更改を進めていたが、本店と各店舗とのネットワーク障害が発生し、新しい消費税率で価格が表示できず開店できない状態になった。

原因は、本店から各店舗に配信する商品価格のデータ量が通常よりも大幅に増えたため、データを店舗に配信することが大幅に遅れたためであった。事前の対策の検討が不足していたことによる。

活用を考える

教訓Ｔ２は、上位システムが障害になった場合、下位システム（蟻の目）が単独で稼働できるような要件を検討する時にも活用できる。障害対策は、障害を起こした下位の制御装置だけの対策を考えがちであるが、蟻の目の対策だけでなく、システム全体を俯瞰する鳥の目対策を活用することで障害発生時の復旧時間の短縮が可能であり、システムの安定稼働（障害発生頻度の減少）が保たれる。

このケースでは、本店と各店舗との間での通信障害発生時の対策を立てていなかった。そのため、通信障害が発生した場合、店舗では何もすることができなかったのである。この事例は、上位システムが障害であっても下位システムが自律機能を持っていれば、店舗システム単独での稼働を行うことができたのである。

このように、教訓Ｔ２は、システム対策をトータルに考える際の気づきを提供してくれる。

◆ケース 22　手作業と自律機能

B 航空会社では、機体の重心を計算する重量管理システムが障害により使用できなくなった。このため、職員が手作業で機体の重心計算などをしたため、出発準備に時間がかかり、多数の航空機に遅れと欠航が発生した。

原因は、サーバ内で不要なデータが滞留していたためで、削除して再起動したところ正常に戻った。

活用を考える

このケースでは、サーバ（上位）が障害になっても、PC 上にソフトウェアを開発してクライアント（下位）での対策を考慮しておけば、その PC と手作業を中心に対応することができ、多少の欠航と遅れがでるだけに留めることが出来た可能性がある。これは、教訓の応用的な活用である。上位システムが障害でも、下位システムが自律機能（下位システムだけで対応できる機能）を持てば、障害に対応できる場合がある。

また、この事例の他でも、例えば銀行で定期的に勘定系システム（上位システム）から支店システム（下位システム）に預金者の口座残高情報を配信していれば、長時間にわたって勘定系システムが停止しても、支店システムから預金者の口座残高が分かるので現金支払いの確認が行なえ、スムーズな窓口対応が取れる。このような対策も下位システムの自律機能の考え方の一つであろう。

２．２．１２．テストパターンの整備に関する教訓（Ｔ３）[19]

[教訓 T3]
現場をよく知り、現場の知識を集約し、
現場の動きをシミュレートできるようにすべし！

概要

ある鉄道会社では、特定ケースで先行列車の制御信号（「列車が区間内に存在している」ことを知らせる信号）が出続けたため、実際にはその区間内に先行列車が存在していないにも関わらず、システム上では列車が存在している事態が続き、後続列車が急停止する事態となった。

【原因１】有識者（ベテラン社員を含む）による制御信号の機能確認を行っても、まだ洗い出せていない機能が存在した。（機能要件漏れ）

【原因２】列車の動き、信号システムの動作などを総合的にテストできる環境、つまり、組込みソフトウェアを持った制御システムと列車などの動作の全てのテストが行えるテスト環境ができていなかった。

対策として、現場を熟知できるためのツールの開発を検討した。

【原因１】については、一度設計された「機器の動き（列車の運転）」のパターンを知識データベースとして蓄積し、そこに、追加登録していく。

【原因２】については、制御系システムのシミュレーション・システムの開発を行う。そのためには、現実の制御装置のプロセスを分かりやすく可視化し、プロセスの骨子を見極めて「モデル」化（モデリング）する。

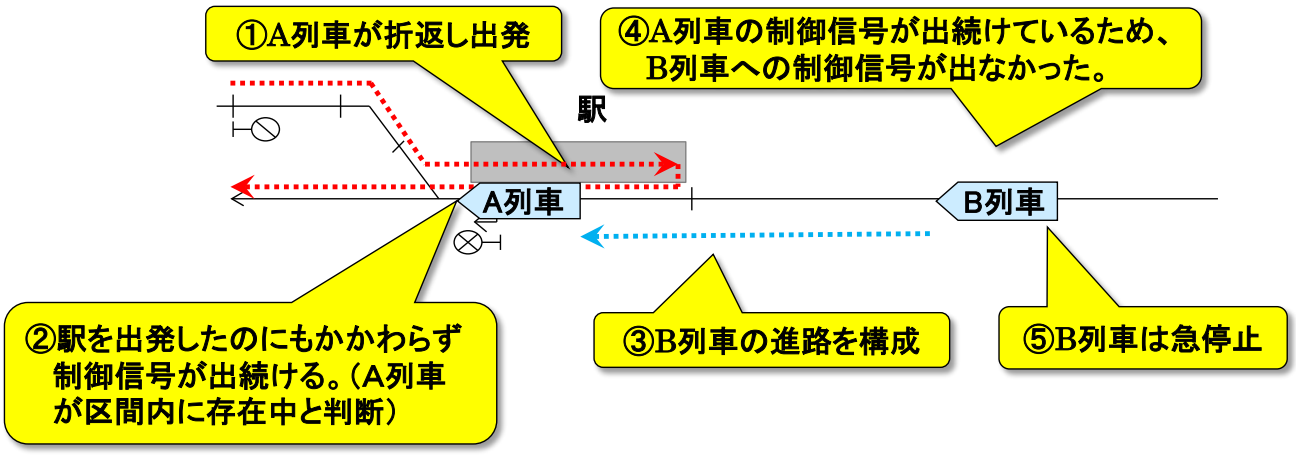


図２．２．１２－１　駅での障害発生状況

[19] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-47

活用が考えられる事例

◆ケース 23　予期せぬ制御装置の動き

A 行政機関は、「マグニチュード（M）最大 7.8」とする緊急地震速報を 34 都府県に発表。緊急地震速報に伴い、鉄道各社は運転を見合わせ、多大な影響が出た。しかし、実際に同時刻ごろに起きた地震は、「M2.3」だった。

通常、地震計は地震の揺れによらないわずかな地面の動きを常にとらえ、地震とは違う「ノイズ」と見なす処理をしている。だが、今回、ノイズが２秒程度途切れたため、地震計がその後のノイズを揺れと誤認し、誤った M 値を検出した。B 県北部で実際に起きた M2.3 の地震と C 県南東沖に設置している海底地震計のノイズ異常が重なり、データを処理する中継局システムが誤った処理を行った。

活用を考える

この事例のようなシステムの不具合は、事前にテストすることは困難であろう。制御系システムのシミュレーション・開発を行うためには、現実の制御装置プロセスを 分かりやすく可視化し、プロセスの骨子を見極めてモデリングする。特に微妙なタイミングを問題にするテストは、実機で再現することは難しいが、シミュレーションで再現することは可能である。

◆ケース 24　莫大なコストがかかる装置のテスト

宇宙開発を行っている B 機構では、ロケットエンジンの開発を、設計→製造→テストといった工程で行っていた。しかし、テストの段階で、ロケットエンジンに不具合が発生すると、設計に戻って再度エンジンを作りなおすといったことを繰り返すため、ロケットエンジンの開発期間が長期になり、また試作エンジンを何度も製造するため莫大なコストがかかっていた。

そこで、IT 技術を活用し、ロケットエンジンにおけるモデルベース信頼性評価技術の構築を行った。この評価技術では、設計と並行してモデルを用いた設計検証を行うことにより設計段階で信頼性設計を効率的に取り組むことができ、大規模な信頼性試験をモデルで行う設計検証と小規模な要素試験（エンジンの部分的な実機試験）で代替することが可能となった。

活用を考える

このケースは、実機を使った評価試験で生じる不具合の多くが、設計が起因するものであったため、手戻り工数が大幅に発生したり、強大なエンジンの製造コストが大幅に発生したりしたことが問題であった。

このケースのように、実機を製造する前に、設計時にモデルを作り、知識データベースを活用したシミュレーション・システムを作成して、設計時の不具合を取り除く取組みは、コスト、納期の面からも有効であろう。

２．２．１３．システム環境の変化への対応に関する教訓（Ｔ４）[20]

[教訓 T4]
システム全体に影響する変化点を明確にし、その管理ルールを策定せよ！

概要

列車運行システムにおいて、表示項目数がシステムの上限値を超えたため、全画面表示が消え、オペレータが混乱した。

直接原因は、システム構築当初から決まっていた上限値について、外部仕様変更に伴う見直しを実施していなかったためであった。

根本原因は、全体に影響する変化点（この場合、ダイヤ予測時間、列車運転本数）が以下のように不明確だったことであった。

【原因１】予測時間を 4H⇒24H に変更した際、そのような要件変更があったにも関わらず、「修正箇所数」の上限値の増加などシステム全体の機能要件変更を未実施

【原因２】列車の本数が年々増加しており、本来ならば（運転本数の増加の都度）上限値を超えた際のシステムの挙動を見直す必要があったにも関わらず、未実施

対策として、以下のように制御系システムの変化点の管理ルールを明確にし、そのルールを守る仕組みを構築した。

・システムが監視・制御する対象と仕様の変化点を網羅
・変化点管理のルールとそれを守る仕組みを構築
・変化点管理で使用する管理指標を関係部門で共有し、「変化点の見落とし」を防止

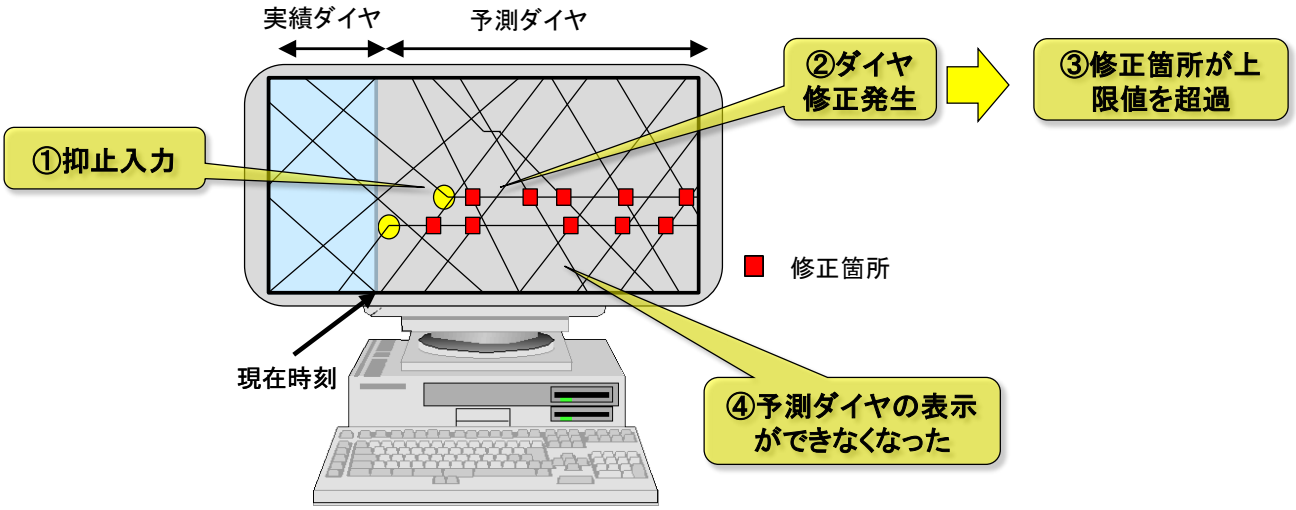


図２．２．１３－１　障害発生状況とモニター画面

[20] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-50

活用が考えられる事例

◆ケース 25　環境変化の見落とし

クレジット A 社は、会員が他のクレジットカード会社の加盟店でカードを使った際、請求業務に必要となるバッチ処理が、予定どおりに完了できなかった。

カード利用者数は、稼働当時から２倍に増えていたため、カード会社は、システム機器などの増設を行っていたが、システムにおける処理能力の監視（変化点）を考慮してないため、バッチ処理能力の上限値オーバを見逃してしまった。

活用を考える

このケースのように、データ量が伸びつつある中でシステムへの影響を見逃すと、あるピーク時点に達した時、システム障害を引き起こすことになる。

A 社の再発防止策では、バッチ処理に要した時間やスケジュールについて、計画と実績のかい離状況を毎月チェックするなどの仕組みを作ったが、これは教訓で述べている「変化点を見逃さない仕組み」を作ったことになろう。

◆ケース 26　上限値の見落とし

B 国の管制センターの管制システムが停止して、空域内の飛行が１時間にわたり禁止され、多数の航空機利用者に影響を及ぼした。

原因は、管制システムサーバが「監視モード」で対応できる最大端末数を超えたため。同サーバは２系統あるが予備系も同じソフトウェアを使用しているため、系切替えを実行した時、同じ理由で停止した。

「監視モード」ではたまたま最大 151 端末まで対応できるように設定されていたが、障害発生時に一時的に 153 端末になった。直前に軍の管制機能との統合があり取扱う端末数が増えたのに、その制限値の見直しが行われないままになっていた。

活用を考える

このケースでは、前日にソフトウェアの更改を行った時に、変化点となる端末数が軍の管制機能の追加によって増えているにも関わらず、その対応を怠ったためにシステム障害が起きている。

教訓Ｔ４では、変化点を機能要件から押さえる変化点と、非機能要件から押さえる変化点があることを説明している。この教訓は、この変化点を洗い出し、それを管理する仕組みを日々の運用保守で管理することを述べている。

２．２．１４．サービス視点での変更管理に関する教訓（Ｔ５）[21]

[教訓 T5]
サービスの視点で、
「変更管理」の仕組み作りと「品質管理責任」の明確化を！

概要

A 社では、本店ホスト／サーバから請求データを端末に転送し請求書を発行するシステムにおいて、端末として、営業員が持ち歩く HT（ハンディ・ターミナル）を新規に導入したところ、そのシステムから出力される請求書の金額が誤っていた。その誤った請求書を顧客に渡ってしまったため、個別謝罪・請求書の再発行に追われた。

システムへの新たな要件追加、使用方法の変更があると、今まで正常に稼働していたシステムに突如障害が発生する場合がある。（追加により未使用・未確認のロジックが使われ，不具合が顕在化）

変更があった時にシステム全体のプログラム、データ、テスト仕様の整合性を保つための変更管理を確実に実施することが重要である。

A 社は、システム全体の整合性を確認する人を決め、品質管理責任を明確にし、開発フェーズ毎の検証を実施した。

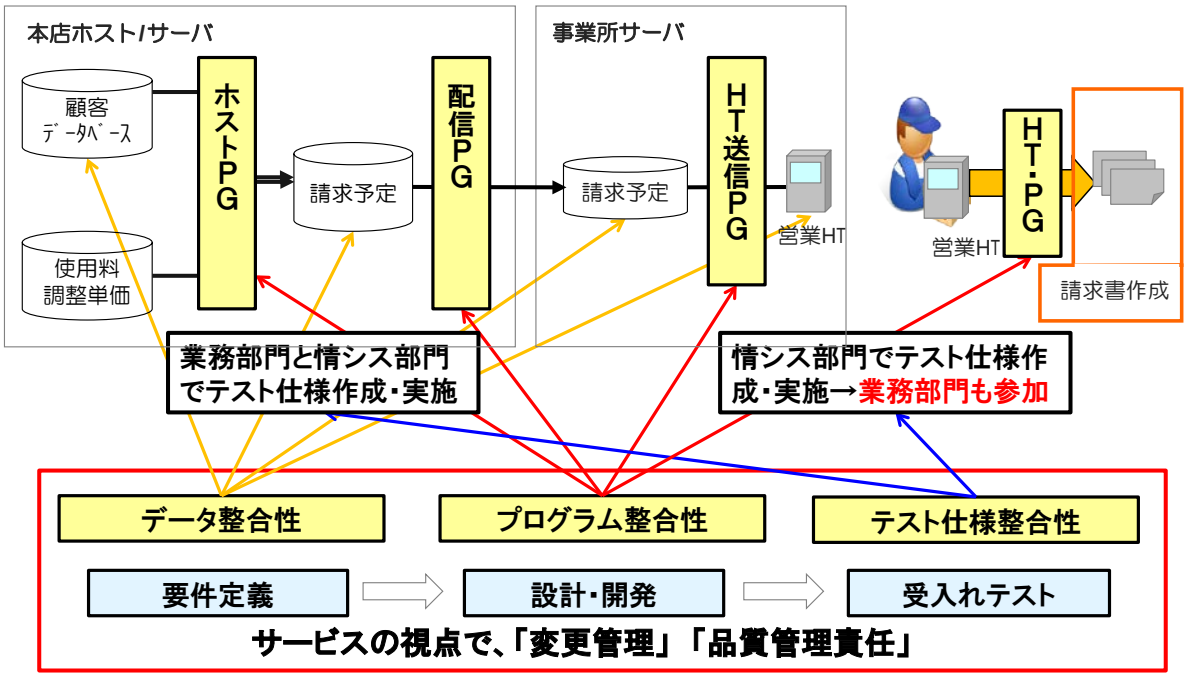


図２．２．１４－１　システムの概要と障害への対策

[21] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. I -53

活用が考えられる事例

◆ケース 27　サービス変更管理の見落とし

A 銀行では、定期自動送金サービス（依頼者が事前に決めた振込先に、決まった日に決まった金額の振込依頼をおこなうサービス）を担うシステムにトラブルが生じ、当日中に振込ができない事象が発生した。

このシステムでは、その日に送金処理を行うべきデータに対し 1,000 件単位にデータチェックをおこない、チェックした 1,000 件全てのデータが「解約（送金データなし）」だった場合、以降の処理はやめることになっていた。

ところがこの日の送金データの中には、途中で実際に 1,000 件の解約処理があったため、その後にあった処理すべき振込データを未処理のまま終了してしまった。

活用を考える

このケースでは、内部設計で決めた仕様通りの設計で構築されたと考えられる。つまり、事業部門との要件定義では出てこないような仕様である。このような情シス部門だけで考えた仕様は、外部環境が変わった場合、つまりサービス提供の視点での変化があった場合、見落とされることが多々あり、システム障害に繋がることになる。

教訓Ｔ５を活用し、サービス視点での変更管理を行うことにより、システム障害の削減が期待される。

◆ケース 28　２度の設定ミスを見逃す

B 社は、C 商品を分割払いで顧客に販売しているため、その購入顧客の信用情報（債務額、入金情報）を信用情報機関に報告している。

しかし、システム設定の確認が不十分であり、ある条件の顧客の入金情報が、信用情報機関に送信されなかったため未入金扱いにされていた。利用者からの問合わせで発覚した。

B 社は、４年前のシステム設定変更時も、同じようなシステム障害を起こしており、今回は、２度目であった。

活用を考える

サービス提供者は、サービス視点でのシステム内の顧客情報の管理を行わないと、このケースのように外部からの指摘で発見されるような事態に落ちいってしまい、信頼を大きく損なうことになる。しかも、過去のシステム変更時にも同様な障害を起こしていることから、教訓Ｔ５のサービスの視点で、「変更管理」の仕組み作りと「品質管理責任」を明確にすることにより、システム障害を未然に防ぐ対策を取るべきである。

さらに、この教訓Ｔ５の対策手法（教訓集「障害対策手法・事例集」）では、「文書およびデータに関するトレーサビリティ」[22]として、トレーサビリティの重要性と管理手法を紹介しているので、併せて活用すると、より対策の観点が広がることが期待できる。（文献２－４）

[22] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅱ-21

２．２．１５．本番環境とテスト環境の差異に関する教訓（Ｔ６）[23]

[教訓 T6]
テスト環境と本番環境の差異を体系的に整理し、障害のリスク対策を練る

概要

A 社では、テスト環境でうまくいったソフトウェアのリリースが、本番環境で障害となる事象が発生した。原因は、テスト環境と本番環境とに相違があり、テスト環境で無かったデータベース・プションが本番環境には存在し、そのオプション機能にバグがあったため、本番環境で障害となってしまった。

A 社は、以下の対策を立てた。

① テスト環境と本番環境の差異分析
② テスト環境で確認できない項目、機能に対し、関係者でリスク分析
③ リスク分析結果を基に、コンティンジェンシープランを作成
④ 本番環境のリスクをステークホルダで共有
⑤ 大きいリスクは経営トップが判断

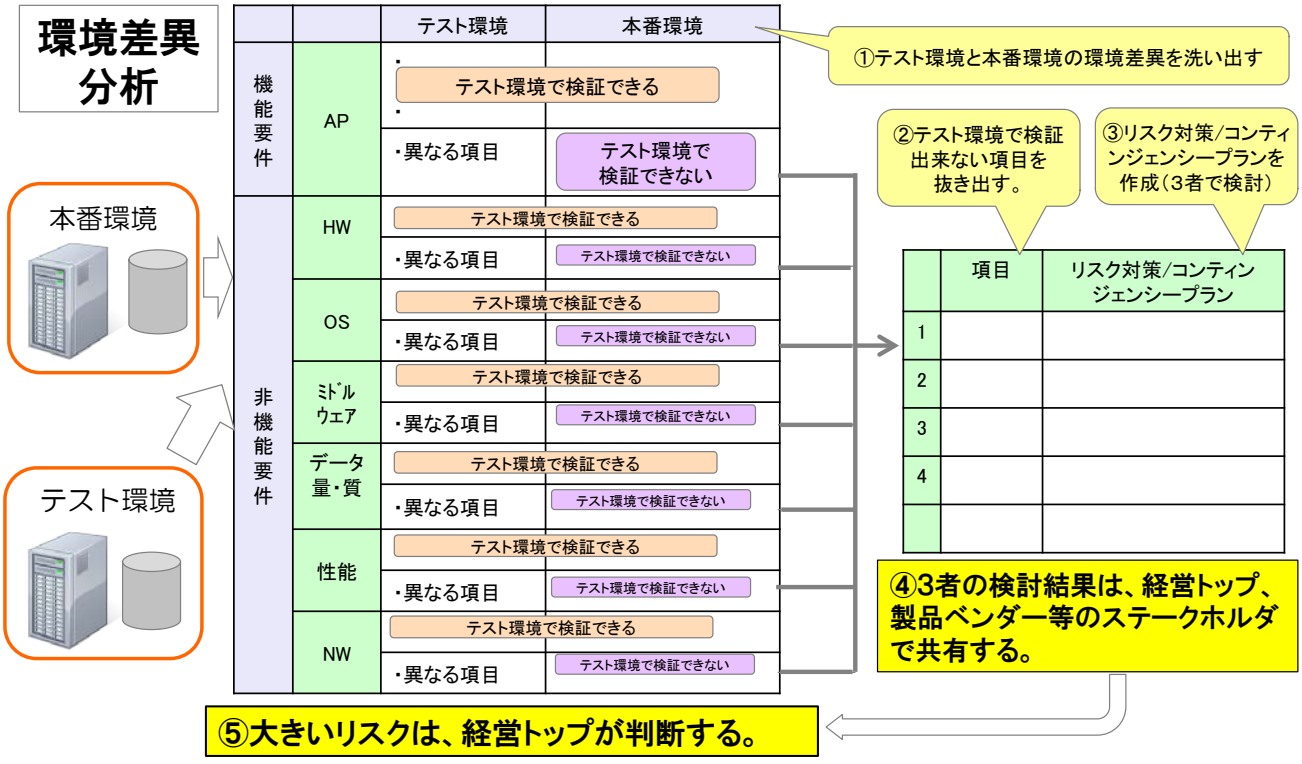


図２．２．１５－１　環境差異分析

[23] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-56

活用が考えられる事例

◆ケース 29　テスト環境と本番環境の違い見落とし

A 社では、委託先のベンダに本番データの一部をマスクして渡して、改修プログラムのテストをテスト環境で実施した。結果が正常だったため、本番に移行したが、マスクした箇所のデータを使うところで障害が発生してしまった。

活用を考える

本番環境とテスト環境が違うため、テスト環境で問題ないことが確認されたからといって本番環境でもうまくいくと言った保証はないことが、この教訓Ｔ６で学ぶ重要なポイントである。

このケースのように「マスクしたデータ」を使用する場合、テスト環境ではマスクした項目のチェックロジックを取り除くのでエラーにならないが、本番環境ではエラーになる可能性がある。

重要なシステム、基幹システムでは、テスト環境は、本番環境と同一環境で持つことが前提であるが、どうしても持てない場合は、「テスト環境と本番環境の差異を体系的に整理し、障害のリスク対策を練る」対策を立てる必要がある。

◆ケース 30　テスト環境ではできないテストを本番環境で実施

B 銀行では、テスト環境では確認できないテストを本番環境で実施した。月初めにテストを実施したが、用いたテストデータの削除を忘れていた。月末に本番でそのままバッチ処理を実行したため、テストで使ったデータとダブってしまい、顧客の二重引き落としが発生してしまった。

原因は、テスト環境と本番環境のデータ管理を行っていなかったことによる。

活用を考える

このケース以外にも、テスト環境と本番環境の混乱、勘違い、などのヒューマンエラーによって障害が引き起こされるケースがある。

- C 金融会社の運用担当者は、本番環境をテスト環境と勘違いし、テストデータを本番環境で実行してしまった。
- D 鉄道会社は、消費税増税前にテストで使用した増税後の料金データを戻しわすれたまま本番の改札機の周辺装置を設置してしまい、増税後の運賃を徴収してしまった。
- E 社は、制御装置のソフトウェアの更改時、テスト環境では HDD（ハードディスク）で動作確認し問題なかったので、本番環境では SSD（フラッシュメモリ記憶装置）であったが、「同じインターフェース」なので問題ないと勘違いし、本番で実行したところ、制御装置が立ち上がらなくなってしまった。

このようなケースは、本番環境とテスト環境、本番作業とテスト作業の運用手順が明確に切り分けて管理されていない状況が引き起こした障害と考えられる。

教訓 Ｔ６と併せて、教訓Ｇ６「作業ミスとルール逸脱は、個人の問題でなく、組織の問題！」も参考にすることで、このような障害も減らすことができる。

２．２．１６．バックアップ切替え失敗に関する教訓（Ｔ７）[24]

[教訓 T7]
バックアップ切替えが失敗する場合を考慮すべし

概要

冗長構成を取っているにも関わらず、バックアップ切替えが失敗しシステム障害となるケースが多い。下図に示されるさまざまな失敗原因にあらかじめ配慮してシステムの開発・運用を行うことにより、過去に発生した障害と類似の障害の発生を防ぐことができる。

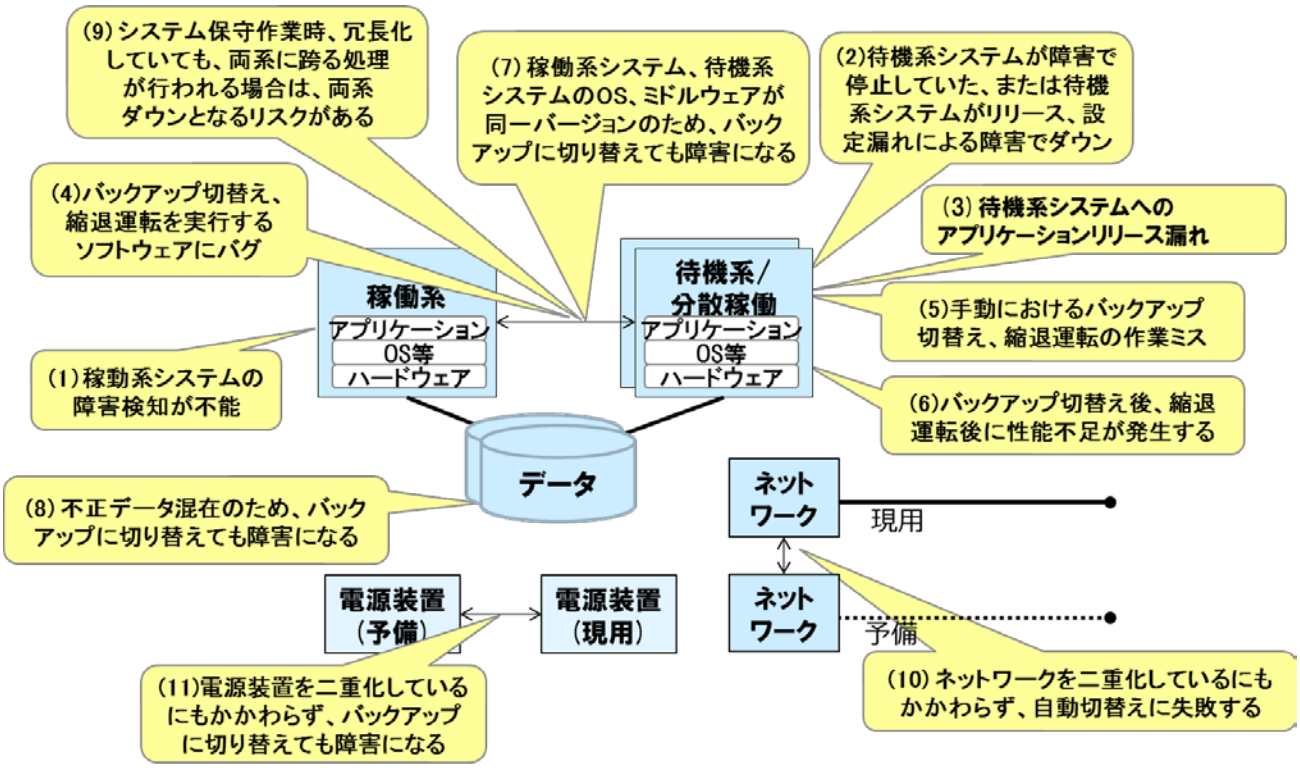


図２．２．１６－１　問題の種類と発生箇所

[24] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-59

活用が考えられる事例

◆ケース 31　バックアップ切替え対策の不備

A 損害保険会社の「査定システム」が停止した。

個人保険に係る保険金・給付金の支払い事務に遅延が発生し、当日中に処理が完了できなかった。

原因は、システムを構成する機器に障害が発生したため、バックアップシステムへの切替えが行われたが、切替えに失敗したためだった。

◆ケース 32　バグによるバックアップ切替え失敗

B 通信会社の基地局制御装置でデータ振分処理のバグにより片系がダウンした。さらにリカバリ処理のバグにより両系ともダウンしてしまった。

原因は、プログラムのバグだが、両系がダウンとなったのは、負荷増により潜在バグが顕在化したためであった。

活用を考える

冗長化構成を取っていても、いざ障害発生時、バックアップ切替えや切離しによる縮退運転が失敗し、システム障害となる事例が後を絶たない。報道事例をまとめると、以下のように毎年起きている。

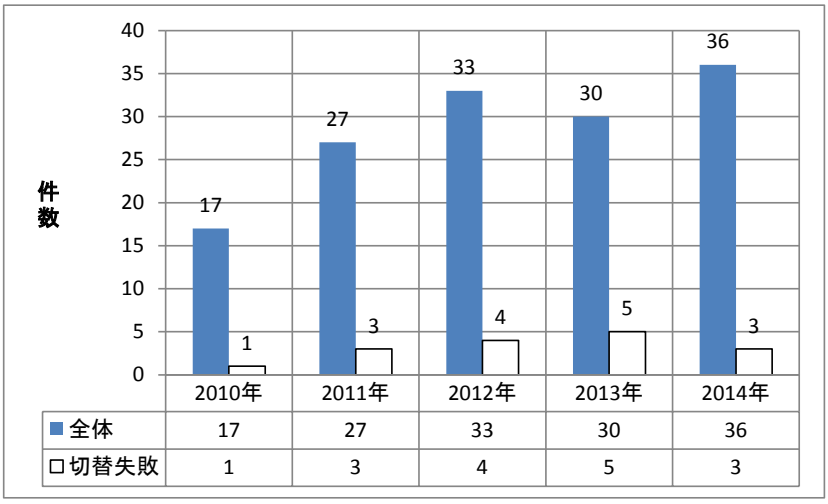


図２．２．１６－２　報道された障害件数と内切替え失敗件数

教訓集では、バックアップ切替えの失敗事例を分析し、その問題と対策をまとめた。[25]
本対策の特徴は、バックアップ切替え失敗事例を「問題」として分類、体系立てて整理している点であり、失敗事例を11パターンの問題に整理し、それぞれ対策を立て、「問題と対策一覧」としてまとめた。

この一覧を設計時にチェックリストとして活用することにより、バックアップ切替えの機能要件漏れや対策漏れを減らすことができ、運用保守時に、発生した障害と同じ問題に対応する対策を実施することで、障害の再発を防止することができる。

[25] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-98

２．２．１７．仮想化時の運用管理に関する教訓（Ｔ８）[26]

[教訓T8]
仮想サーバになってもリソース管理、性能監視は運用の要である

概要

A 社情シス部門は、プライベートクラウド（仮想サーバホスティング）の運用を行っている。

ある日、プライベートクラウドシステムのサービスが数時間停止した。

直接原因は、運用担当者のボリューム割り当てミスであった。根本原因は、仮想サーバ環境での運用要件の未整理、リソース管理、性能監視が不十分、かつ復旧時の対応方法も十分に把握していなかったことによる。

対策として、以下を検討した。

・物理サーバを仮想サーバに移行する際のリソース管理、性能監視プロセスの策定

・仮想化によるオーバーヘッド増大の見積り徹底

・障害対応マニュアル等の整備と要員の教育・訓練

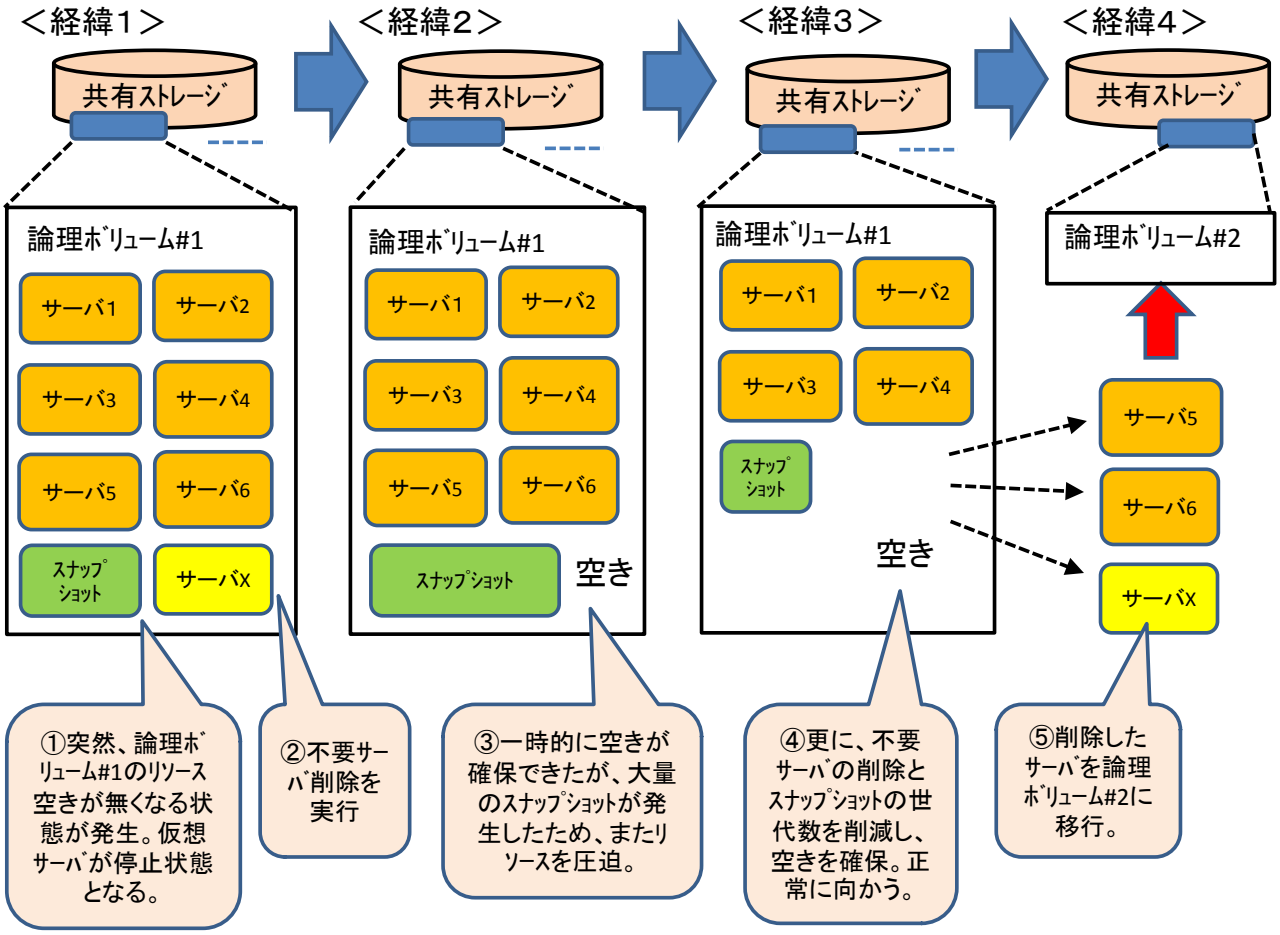


図２．２．１７－１　障害発生時の論理ボリューム状況

[26] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-62

活用が考えられる事例

◆ケース 33　仮想化システムの運用見直し

A 社では、明確な運用ルール、方針を持たず、サーバの仮想環境への移行を行っていたため、障害発生時の対応がスムーズにできない事態が発生した。

運用担当者は、ハードウェア、OS、仮想化ソフト、ゲスト OS とさまざまなレイヤが多重に重なり合う中で、障害の原因を特定することに多くの時間を費やしていた。

◆ケース 34　仮想化システムの障害対策

B 社では、仮想マシンが大量のデータを読み書きすると、物理サーバ上に遅延が発生する障害が多発していた。これにより、１台のサーバに障害が起きると、集約したすべてのシステムがダウンするため、これまで以上に障害の影響を受けることになった。そのため、運用面での障害対策を検討する重要度と作業工数が増してしまった。

活用を考える

最近では、仮想化技術も一般化しつつあるため、「仮想化を行えば運用が楽になるとは限らない」という注意点があることが理解され、教訓Ｔ８のような対策も行われつつある。

しかし、依然としてケース 33 やケース 34 のような悩みを抱えている情シス部門も多いことであろう。

過去の IT 産業の歴史を振り返って見た時、新しい技術の導入で、システム開発の現場や保守運用の現場が、「この製品、システム・ツールを導入すれば、作業効率は大幅に改善される」と言ったセールストークに乗せられてしまってそれらを導入したが、十分な事前検証がなかったために、効果が得られず、逆に新しい技術であるために、要員の習熟が追いつかず苦労されたといった方は多いことであろう。

この仮想化技術についての教訓Ｔ８も、過去に起きたことと同様なことが現場で起きていたことを証明してしまった事例である。

したがって、この教訓を「仮想化技術の課題」と言った観点だけで見ていくと、また将来、新しい技術を導入した時に同じ轍を踏むことになる。この教訓Ｔ８「仮想サーバになってもリソース管理、性能監視は運用の要である」では、このような観点も踏まえて、気づきを得ていただければと思う。

（派生的教訓）

「新技術は、慎重に」、「IT 技術の習得に王道はない」

２．２．１８．不測事態発生への備えに関する教訓（Ｔ９）[27]

[教訓T9]
検証は万全？それでもシステム障害は起こる。回避策を準備しておくこと

概要

A 社の２設備間の通信障害発生時に片方の設備（設備１）上のプロセスの不具合が発現して動作を停止し、これを検知した同設備上の振分制御が他のプロセスへ切り替えようとしたがうまくいかず、処理待ちバッファのオーバーフローにより同設備（設備１）がリブートされた。

原因は、当該通信障害のケース（稀有なもの）を検証しておらず，システムの検収時点では、調達側、供給側とも当該ケースの存在を認識していなかったことである。

対策として、以下を検討した。

・タイムアウト前にオーバーフローしないよう，バッファサイズを拡大。

・サービス復旧のための作業手順を整備。

対象システムの重要性に応じ、検証に費やすことのできる時間と労力は制約される。常に不具合が潜在しているとの前提に立ち、業務の継続性を確保することが重要である。

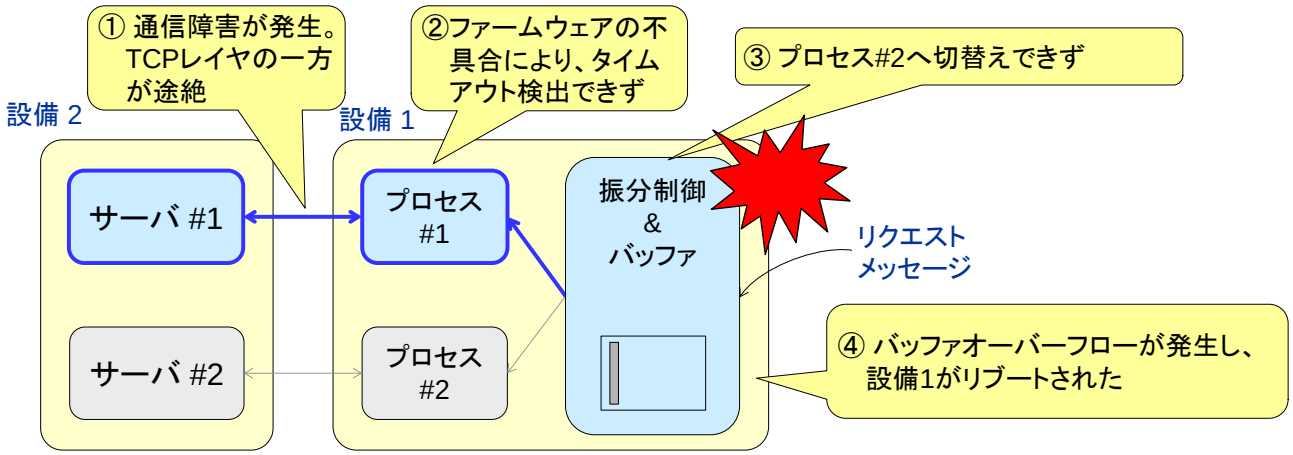


図２．２．１８－１　障害の経緯

[27] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-66

活用が考えられる事例

◆ケース 35　ハード障害によるソフト不具合が多重的に顕在

A 通信会社は、ハードウェア障害に備え、「パッケージ」の２重化による制御装置の冗長化と、制御装置自体の２重化で、２段構えの障害対策を施していた。

携帯電話の位置情報を管理するシステムの「パッケージ」故障がトリガーとなり、システム切替えが一斉に発生し、位置情報管理の負荷が急増した。このため、システムの処理能力が低下しふくそう状態となった。ハード障害がトリガーだったが、位置情報管理プログラムと切替え処理のソフト不具合、またバージョンが異なる「パッケージ」が存在していたといった事態が、障害の収束を遅らせた。

活用を考える

何重もの対策を講じて、システム障害時に備えていたが、それでも障害が起きてしまった場合は、何重もの防御壁を突破して起きる事故と同様なことが発生しており、それを示したものが、スイスチーズモデルと呼ばれる構図である。システム障害では、設計、試験、運用などで生じた穴（ミス、漏れ）があり、光をあてたときに、穴が重ならなければ光は見えないが、穴が重なると光が漏れて見えてしまう。この光が見えてしまった状態がシステム障害の起きた状況である。

このシステム障害の穴を、順々に塞いでいくためには、教訓活用も有効な手段となる。

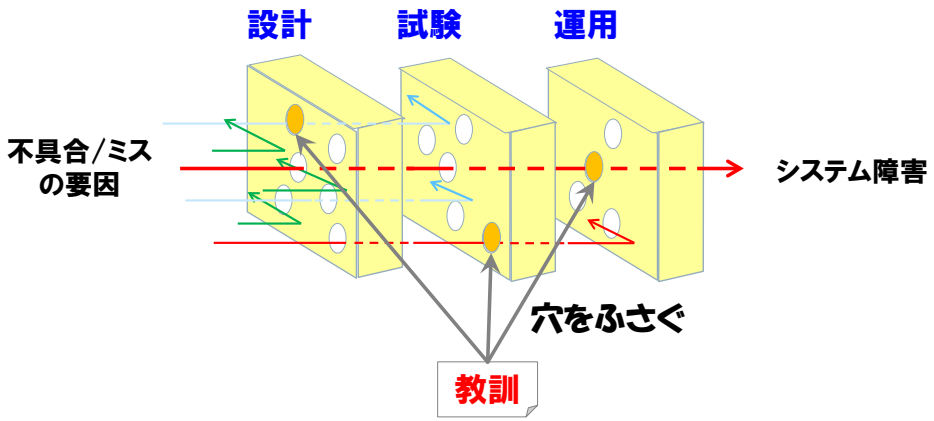


図２．２．１８－２　システム障害のスイスチーズモデル例

◆ケース 36　不測事態発生への備え

B 社の経営者は、震災では大きな影響はなかったものの、情シス部門からの報告で、震災時の他社の事例から自社で不測事態が生じた場合の対策が全くできていないことを知った。

活用を考える

自社以外の障害事例を学ぶことは、未然防止対策に有効である。実際の事例があれば、それを基に不測事態に備え、リスク分析を行い、対策を立てて検証していくという PDCA サイクルを回すことの重要性を経営者に理解してもらいやすい。

常にリスクアセスメントの推進を経営の重要課題とこころがけるべきであろう。

２．２．１９．共有ディスクのメッシュ接続に関する教訓（Ｔ１０）[28]

[教訓T10]
メッシュ構成の範囲は、
可用性の確保と、障害の波及リスクのバランスを勘案して決定する

概要

A 社の各サーバが４ペアの NAS と接続されたフルメッシュ構成のシステムにおいて、ある１台の NAS の故障に起因して、全サーバがダウンした。

直接原因は、NAS 制御ファームウェアの不具合により、故障した NAS の切り離しに失敗したことによる。根本原因は、この局所的な障害が、フルメッシュ構成のシステム全体に波及したことによる。つまり、フルメッシュ構成のリスクについての検討が不十分であった。

対策としては、メッシュ構成を見直し、1 サーバにつき２ペアの NAS のみを接続するグルーピング化（図の赤色の接続）し、併せてトランザクションの振分け論理も変更した。また、可用性の担保のため、迂回時の性能劣化防止用の BCP 設備を増強した。

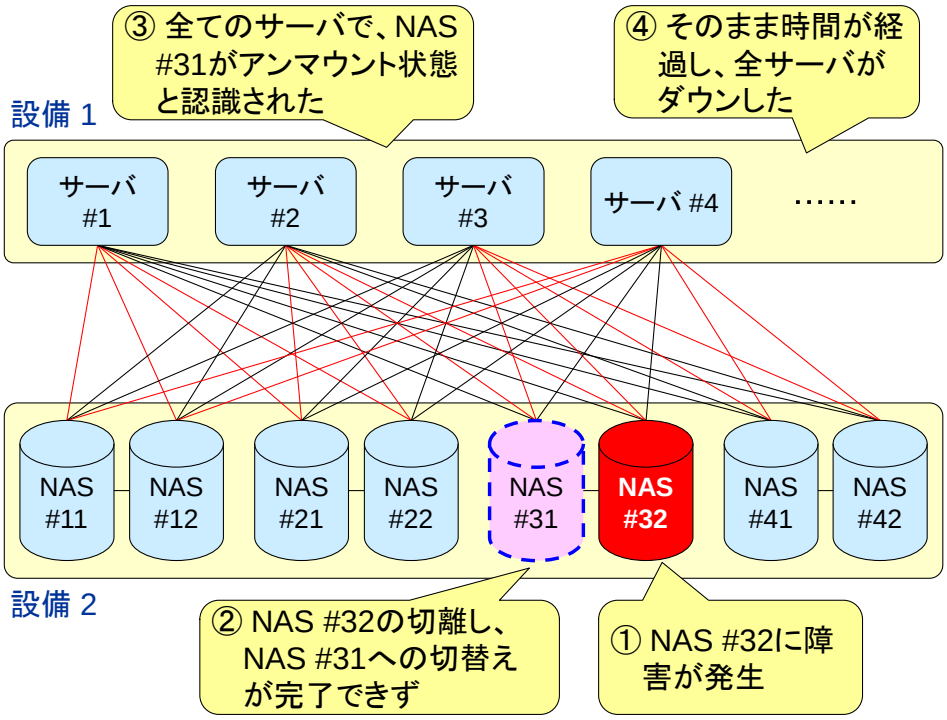


図２．２．１９－１　障害の経緯

[28] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-70

活用が考えられる事例

◆ケース 37　フルメッシュ構成の誤解

A 社は、システムをフルメッシュ構成にして運用していた。しかし、ストレージの一部の RAID 設定に誤りがあったことに気付かず運用していた時、DISK 障害が発生し、システム全体が停止する事態を招いた。

活用を考える

メッシュ構成により可用性の向上が期待できるが、一方で局所的な障害がシステム全体に波及するリスクがあることを考慮することが重要である。

一般に、可用性を高めるためには、冗長化し、その上で、結合する機器同士をフルメッシュの構成にすることが、最善と考えて設計されたシステムは、多い。しかし、必要のないところまで機器同士を結合させることは、一旦障害が起きた時に障害の影響範囲を広げてしまうことになる。

システムの特性を検討し、システム構成を決め、障害の影響範囲を押さえる対策が重要である。その場合、以下のトレードオフの関係を意識しておく必要がある。

フルメッシュ構成　⇒　障害時、全てが停止。ただし運用管理が行い易い。

分割構成　⇒　障害時、局所化が可能。ただし運用管理が複雑になる。

◆ケース 38　ネットワーク構成の検討

B プロバイダ会社では、ネットワーク構成は、フルメッシュ構成が最も冗長性があり安定した構成と理解し、フルメッシュ構成にしていた。

しかし、ネットワーク監視において障害機器の切り分けがスムーズに行えなかったため、ネットワーク全体が停止してしまう事態を起こしてしまった。

活用を考える

ネットワーク構成の中では、メッシュ構成の信頼度は高い構成と考えられている。このケースもケース 37 と同様に、局所的な障害がシステム全体に波及するリスクがあることを考慮し、そのシステムにおける最善の構成を検討することが重要である。

教訓Ｔ１０を活用し、ネットワーク構成は、グルーピング化し、特定のグループの障害が他グループに波及しない構成も有効である場合もあることを考慮すべきである。

２．２．２０．サイレント障害に関する教訓（Ｔ１１）[29]

[教訓T11]
サイレント障害を検知するには、適切なサービス監視が重要

概要

A 社の Web サービスでサイレント障害（明示的に障害が検出されていないにも関わらず性能が劣化）が発生した。外部からの指摘があるまで発見できず、利用者は長時間にわたり、応答作度低下の影響を受けた。

直接原因は、負荷分散装置のファームウェアの不具合であった。発見が遅れたのは、サービス監視の条件設定が最適でなかったためであった。（サービス監視はリクエストが一定回数連続して廃棄された場合にアラームを発するよう設定されていたが、今回は閾値を超えるまでには至らなかったため、サービス監視からの通知はなかった。）

対策としては、負荷分散装置のファームウェアを更新するとともに、サービス監視の条件を変更した。サービス監視等の基本的な取組みを実践した上で、さらなる早期発見、対処を望む場合には、早期障害検知・分析のための技術・製品（SNS 上のつぶやき監視、インバリアント分析、ビッグデータ分析、等）が用いられるようになっている。

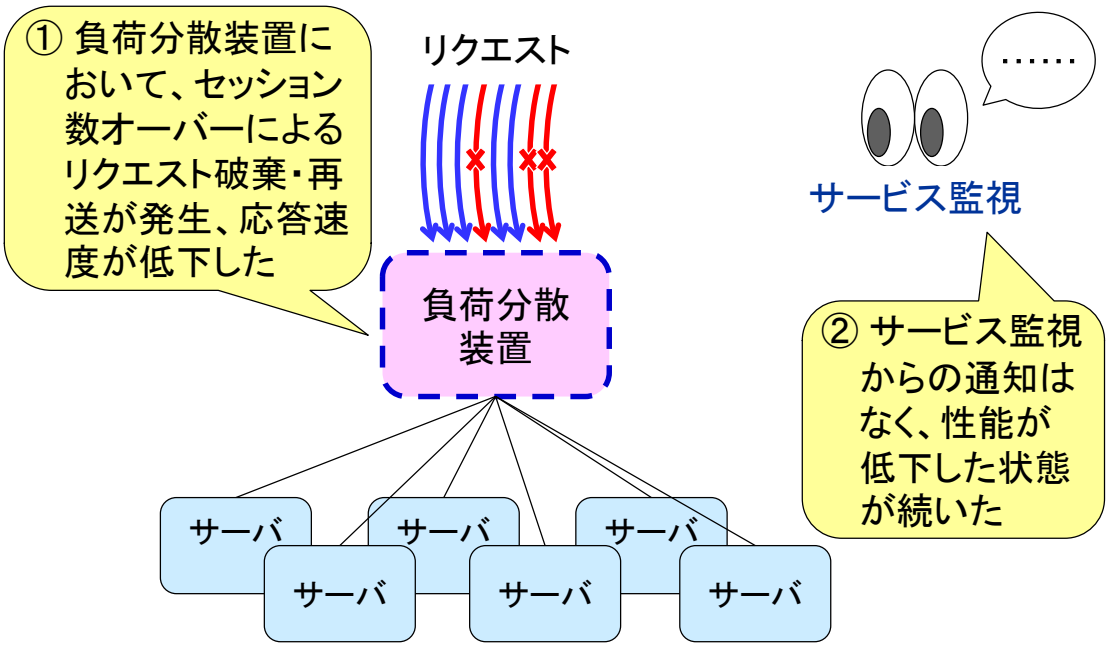


図２．２．２０－１　障害の経緯

[29] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-74

活用が考えられる事例

◆ケース 39　サイレント障害対策

A 通販会社では、ユーザからの「レスポンスが遅い」などのクレームを指摘されてから、慌てて調査をおこなうなど、常に後手に回る事態が発生していた。

活用を考える

何とか自らが先んじて障害予見をしたいと考えるのであれば、サイレント障害対策が有効である。特に、サイレント障害の発生のメカニズムとその対策となる手法の選択が必要である。特に、様々なベンダからツールがでている[30]ので、その中から自社に最適なものを見つけ、適用することが教訓を活用したことになる。

◆ケース 40　つぶやきの活用

B 鉄道会社では、列車の乗務員からの情報だけでは、なかなか列車内状況がつかめないことが多いことを感じ、SNS のつぶやきが、列車の遅れや車内状況を感知する情報として活用できないか検討した。さらに世の中の情報を調べたところ、いろいろな手段があることが判明したので、今後システム運用の中で、実用化に向けた対策を立てることとした。

C 通信会社も、SNS のつぶやきを拾うことで、通信障害が起きているかどうかの監視機能に取り入れる検討を始めた。

活用を考える

サイレント障害に備えることは、予兆監視と言える。障害が起きる前の予兆をいかに素早く捕まえるかがポイントであるが、このケースのようなつぶやきなどを活用することも一つの方法と言える。ただし、SNS にいつも十分なつぶやきがあるとは限らず、またつぶやき、SNS そのものが障害であることもあるので、これだけでは不安定さがある。あくまで複数のツールのうちの１つとして活用すべきである。

[30] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅱ-38

２．２．２１．互換部品の入れ替えに関する教訓（Ｔ１２）[31]

[教訓T12]
新製品は、旧製品と同一仕様と言われても、必ず差異を確認！.

概要

ユーザ X 社の２重化された制御系システムにおいて、部品交換の保守作業時にシステム全体の動作が停止し、短時間で復旧できずに、サービス利用者が終日影響を受けた。

直接原因は、システムのディスク装置が、数年前に，当初構築時の HDD から SSD に交換されていたことにあった。部品交換作業で A 系を切り離した時に B 系 OS から両系のディスク装置にリセット要求が発せられるが、SSD のリセット要求処理時間は、HDD のそれよりかなり長く，OS のタイマ監視においてタイムアウトが発生した。その後のリカバリ処理もうまくいかなかった。

根本原因は、SSD への交換時に、HDD と完全に互換性があると誤認し、検証・テストが不十分であったためであった。

対策として、以下を行った。

・仕様上の互換性を過信せず、差異分析を必ず実施した。

・ベンダとユーザの双方が相手の役割分担を支援し合った（ユーザ側でハザード分析を行う）。

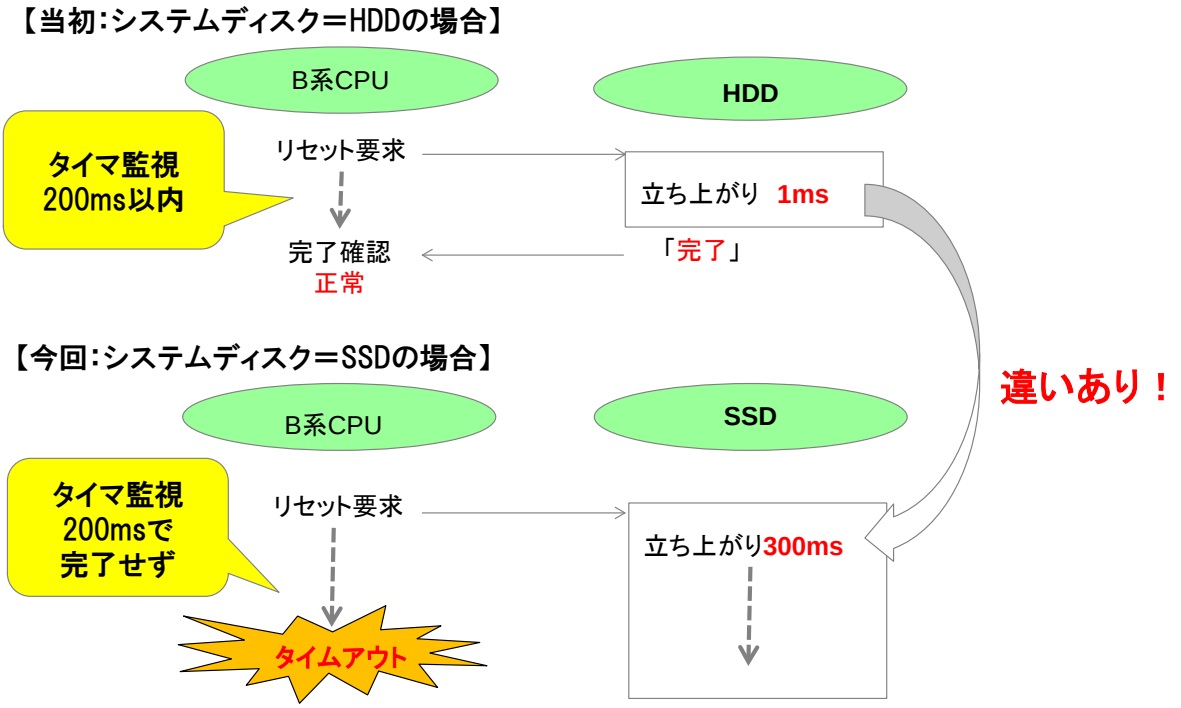


図２．２．２１－１　HDD と SSD の立ち上がり時間の相違

[31] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-78

活用が考えられる事例

◆ケース 41　高性能機能に変えたつもりが機能低下

A 通信会社は、スマートフォン契約者の増加に対応するために、新型パケット交換機への切替えを実施した。

トラフィックの増加に伴い、新型パケット交換機の動作が不安定な状態となり、ネットワークの自動規制により、繋がりにくい状況となった。スマートフォンのアプリケーションによる制御信号のトラフィックが増加しパケット交換機の処理能力がオーバーフローした。

原因は、同時接続数の能力は、新型パケット交換機が、現行パケット交換機より２倍以上の能力があったが、１時間当たりの処理能力は、新型パケット交換機が、現行パケット交換機より半分の能力しかなかった。

活用を考える

このケースは、新製品は現製品より性能が向上しているものと思って導入したのだが、逆に性能が劣るものを導入してしまったケースである。

現製品から新製品に切り替える場合、システム障害を起こさないためには、事前に行う予防対策と作業実行時に障害が発生した時の対策の２通りの対策をベンダ、ユーザ双方で、教訓事例と同様な観点から考慮すべきである。教訓Ｔ１２の「新製品は、旧製品と同一仕様と言われても、必ず差異を確認！」するためには、教訓集に掲載した「対策例一覧」なども参考にすることにより、対策について具体的なイメージをもつことが期待される。

◆ケース 42　メーカによって異なる仕様によりエラーが発生

Ｊアラート（全国瞬時警報システム）の一斉訓練を実施したところ、参加した市町村の 16%は、音声が流れないなどの不具合があった。原因の大半は、B 社製の自動起動機（受信情報を行政無線などに転送する機能を持った機器）に仕様上の問題があったためであった。

全てのメーカの自動起動機は、今回の一斉訓練で正常に稼動しなければならないにも関わらず、実際に使うと、このような事態になってしまった。

活用を考える

このケースは、教訓事例とは異なりひとつのシステムに接続されている複数の製品が同一仕様として導入されていたにも関わらず、B 社製品の仕様が異なっていたためにいざ実施となった時、その製品だけが稼働しなかった事例である。訓練での発覚であったため、本番では大丈夫となるのであろうが、B 社製品の稼働確認が目的ではなかったはずなので、このような事態になったことは、多くの関係者に迷惑をかけたことであろう。

このようなケースでも、教訓集に掲載した「対策例一覧」などを参照して、ユーザ、ベンダ双方ですべての製品の仕様の差異を確認するなど、一斉訓練の前にできることを確認することが重要である。

２．２．２２．業務シナリオテストに関する教訓（Ｔ１３）[32]

[教訓T13]
利用者の観点に立った、業務シナリオに即したレビュー、テストが重要

概要

A 社の Web 経由での申込みを可能としたサービスにおいて、特定の時間帯に限り、Web サイトからのサービス申込みが全て不備とみなされ、登録できなかった。顧客からの連絡で判明した。

直接原因は、オフライン/Web 経由の２系統のサービス申込みを処理するロジックにおいて、各系統の処理間でのデータの連携に誤りがあった。

根本原因としては、全体設計が個別システム設計に正しく引き継がれなかったことと、業務シナリオに即した確認が行われず、設計後のレビューでも発見されず、対応するテストも行われなかったことであった。

対策として、処理ロジックを正しく修正した。また、要件定義・設計段階でウォークスルー等により関係者相互で確認するとともに、利用者の観点に立った、業務シナリオに即した検証を行うようにした。

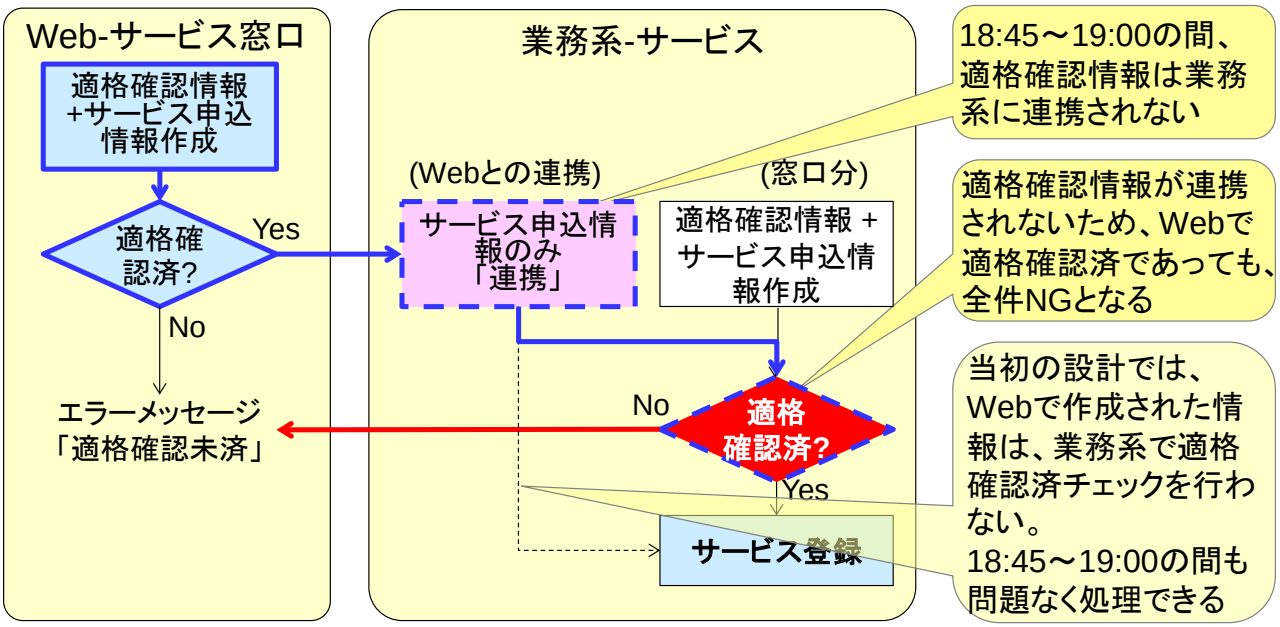


図２．２．２２－１　障害の経緯

[32] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-82

活用が考えられる事例

◆ケース 43　別人からの公共料金徴収ミス

A 市は、インターネットを通じて公共料金を支払えるサービス「B 社公金支払い」で、水道利用者１件分の水道料金を全く別の市に住む C 氏から徴収していた。C 氏から「使った覚えのない水道料金の請求があった。」と A 市に苦情があったことから発覚した。

B 社は、このサービスを利用してクレジットカードで支払う場合、カードの番号と有効期限、セキュリティーコード（SC ＝裏面記載の３桁数字）を入力して本人照会するよう設計していた。

しかし、水道料金については、システムミスで SC による照会がされていなかった。

活用を考える

被害は少なかったが、公共料金の請求が他市から届いた顧客は、どんな思いをしたことであろうか。しかも、水道料金以外は、システムで SC による照会がされていたと考えられ、水道料金のみが見落とされた可能性がある。

このような顧客に強い不信感をもたせるような障害を起こす危険性のあるシステムは、高信頼性のシステムに改善すべきである。教訓Ｔ１３で述べているように、このシステム関係者による「利用者の観点に立った、業務シナリオに即したレビュー、テスト」を実行していれば、このような単純なミスは防げたと考えられる。顧客が安心して利用できるような観点でのレビュー、テストが重要である。

◆ケース 44　システム統合における連携ミス

D 空港のターミナルレーダー管制システムが停止した。

原因は、D 空港と E 空港のターミナル管制一元化のために導入したプログラムの初期不具合であった。気象情報のデータ量見積要件を十分考慮すべきところに誤りがあり、メモリ領域が過小に設定されていた。

活用を考える

このケースは、２つのシステムの連携時のメモリ容量の見積の誤りによって発生している。

教訓Ｔ１３で述べているように、「利用者（管制官）の観点に立った、業務シナリオに即したレビュー、テストが重要」との観点から、D 空港と E 空港のシステムを担当している有識者などが参加するレビュー、テストにおいて、気象情報で使う最大メモリについての要件の確認を行っていれば、この事例のような障害の防止が可能であったと期待される。

また、２つのシステムそれぞれの境界点での仕様確認、テスト実施が、整合性を確認するポイントになる。

２．２．２３．Web ページ更新時の性能に関する教訓（Ｔ１４）[33]

[教訓T14]
Web ページ更新時には、応答速度の変化等、性能面のチェックも忘れずに

概要

A 社の Web ページ上のあるサービスのトップページをクリックすると、応答に長時間を要し、目的のサービスに接続できないケースが多発した。

原因は、事業部門がトップページのコンテンツを更新した結果、１顧客当りのダウンロードサイズが更新前の４倍になったが、応答速度への影響を確認しないままリリースしたことによる。事業部門はダウンロードサイズと応答性能との関連を意識せず、それに関する情シス部門による技術的な確認がルール化されていなかった。

対策としては、事業部門が Web ページコンテンツを更新する際には、情シス部門が技術的な観点で確認を行うことを手順書に明記するとともに、情シス部門が必要と判断した場合、事業部門に対しリリース中止を指示できるようルールを改めた。

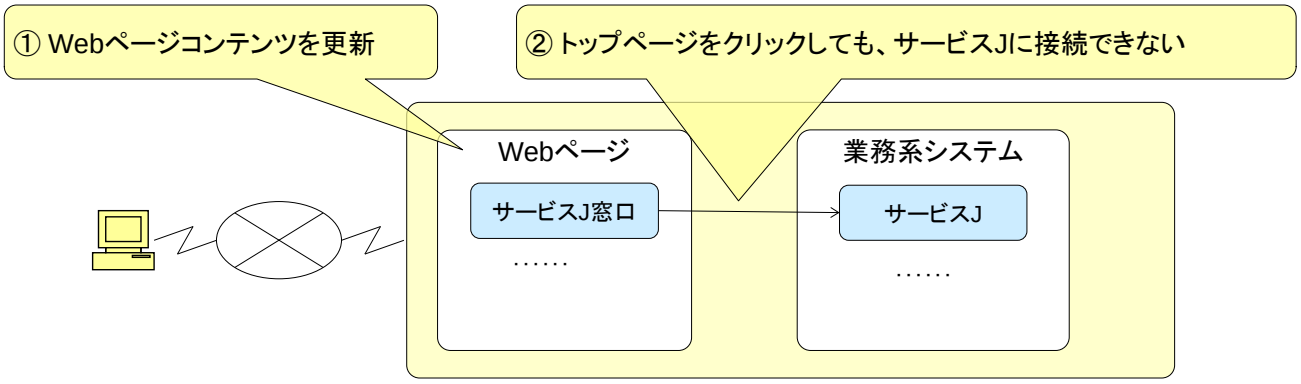


図２．２．２３－１　障害の概要

[33] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-86

活用が考えられる事例

◆ケース 45　Web 処理の遅れ対策不足

A 市内では、台風の接近に伴い、市内のほぼ全域の携帯電話に、「緊急速報メール」を配信した。土砂災害の恐れがあるという内容だった。システムのメール文字数制限が 200 文字のため、内容（対象の地区はどこかなど）を詳しく調べるには、メールに記載したリンクから A 市の Web ページを参照させることにした。その結果、Web ページにアクセスが集中し、サーバ負荷が急激に増大し、サーバがダウンしてしまった。

暫定対処としては、Web サーバから容量の大きい地図データを削除し、文字で危険箇所を示すなどの緩和策を講じた。

同様の事態を防ぐための対策を検討しているものの、膨大な数の対象者に迅速に情報を伝えることは容易ではなく、再度アクセス予測の最適解を見つけようとしている。

活用を考える

このケースは、教訓事例と同様に Web ページの処理の性能問題となった事例である。予想される照会件数を把握していなかったことと、処理に負荷のかかるモジュールの性能を把握していなかったために障害となってしまった。

Web 処理は、システム更改時だけでなく、環境の変化時にも「応答速度の変化等、性能面のチェックも忘れずに」行うことが重要である。

◆ケース 46　非機能要件の設計ミス

B 市の Web ページには外部からの連携で検索機能があるが、連休明けにアクセスが集中し、接続件数が設定の上限を超えたため、レスポンスが遅れシステムが機能できなくなった。

原因は、負荷シナリオにおいて外部サイトとの連携で表示する機能を盛り込まずにシナリオ作成したが、実際にはその機能が性能のボトルネックを発生させる存在であったことを気づかずにいた。さらに B 市と B 市が委託している開発ベンダの間で、連休明けのアクセスに関する非機能要件の調整がなされていなかったことによる。

活用を考える

このケースは、連休明けの予想される接続件数を性能要件として把握していなかったために起きた事例である。「Web ページ更新時には、応答速度の変化等、性能面のチェックも忘れずに」性能分析を時間と手間をかけて行い、本番に近い形まで練り上げることを行っていれば、障害の防止が可能であったと期待される。教訓とは異なり、ユーザが Web ページコンテンツを更新する際には、開発ベンダが技術的な観点で確認を行うことが重要となる。

２．２．２４．データ一貫性の確保に関する教訓（Ｔ１５）[34]

[教訓T15]
緊急時こそ、データの一貫性を確保するよう注意すべし

概要

A 社では、毎月末に、顧客のカテゴリ判定バッチ処理を、あらかじめ作成しておいた顧客データ（マスタ）のコピーを用いて行う運用をしていた。ある時、緊急の要請により、マスタを直接修正して対応したことがあったが、その後のオンライン処理において、誤った顧客カテゴリが適用されてしまった。

原因は、緊急対応後に、マスタから顧客カテゴリ判定用コピーの再作成を行わなかったため、マスタとコピーとの不整合が発生していたにも関わらず、そのまま、カテゴリ判定処理を行ったためであった。

対策としては、緊急時対応の影響範囲を見極め、対応結果が平常時のシステム運用の流れに確実に繰り込まれるよう、特に意識するよう周知するとともに、作業ルール・手順書を明確化した。

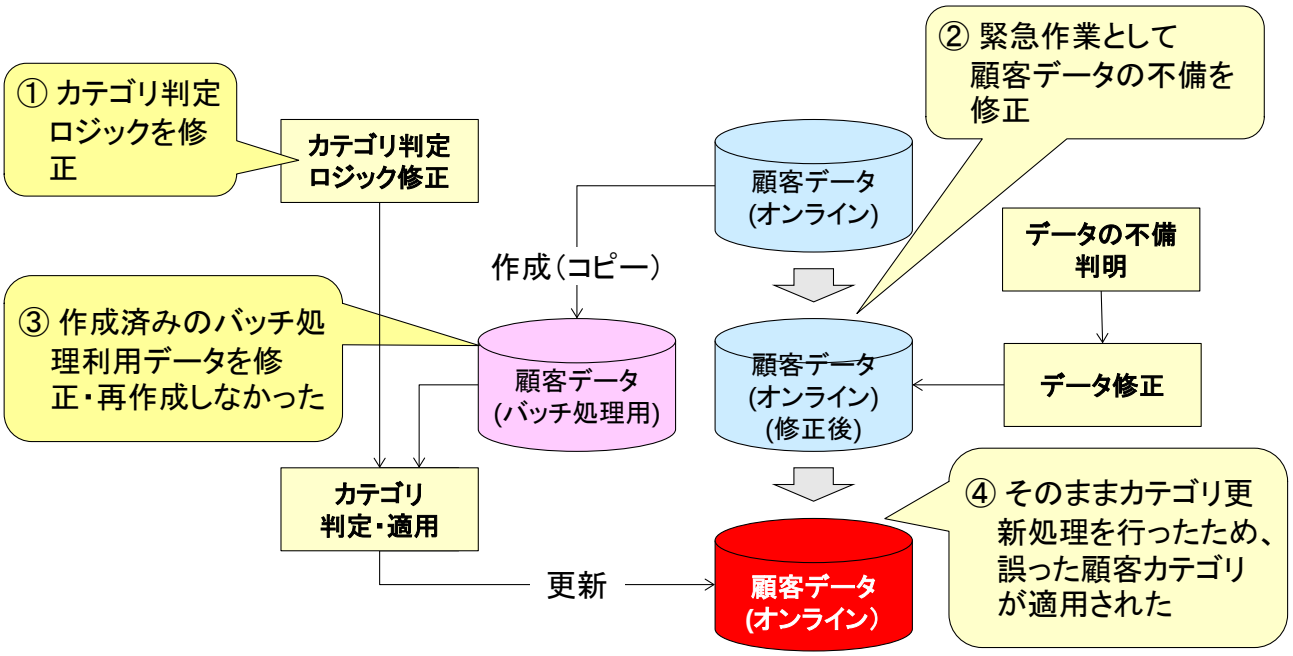


図２．２．２４－１　障害の経緯

[34] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-88

活用が考えられる事例

◆ケース 47　ファイルの取違え

A 銀行のオンラインシステムに障害が発生した。全国の本支店の店頭及び ATM　での入出金、為替、照会などの取引が不能になり、インターネットバンキング利用も取引が出来なくなった。

原因は、３日間にかけて実施したシステムの更新作業で、更新すべきファイルを取り違えたためだった。

活用を考える

このケースのように、システム更新中は、独自の移行システムが稼働し、通常のファイルとは別の作業ファイルを用いて実施したりするため、本来更新すべきファイルに反映するのを忘れたり、誤ったファイルを更新したりと、とかくシステム障害を起こし易い事態を招く。

この教訓Ｔ１５を参考に、保守作業時のファイル更新については以下の様な手順を実施することが考えられるであろう。

① 作業手順書を作成する。
② 本番稼働前に事前確認テストを実施する。
③ 本番稼働判定基準を設定する。
④ 全ての作業が完了しているかを関係者全員が本番稼働判定会議などで確認する。

◆ケース 48　テストデータの戻し忘れ

B 鉄道会社は、消費税増税前に改札機の入替えを行った。

消費税増税前に設置する場合は、増税前の税率で改札機を設置する必要があった。しかし、メーカが改札機の周辺機器を更新した際、社内で消費税増税に対応した確認テストを行うために増税後の税率で登録した後、正しいデータ（増税前の税率）を登録し直さないまま、現場に機器を設置してしまった。

活用を考える

このケースは、消費税率の切替え時点の前にシステムの確認テストを行ったが、テスト終了後にデータを戻し忘れた事例である。本来であれば、データが元に戻っていることを確認する必要があったにも関わらず、確認していなかった。システムの戻し確認方法としては、確認ツールを用いて確認するか、本番環境での実行確認等がある。また、システムの戻し後の確認作業の実施を作業手順に入れていなかったことも問題である。

常に、教訓Ｔ１５「緊急時こそ、データの一貫性を確保するよう注意すべし」を頭に入れて、作業を行うことを習慣にしていれば、このような障害を減らすことができる。

２．２．２５．修正パッチの適用に関する教訓（Ｔ１６）[35]

[教訓 T16]
システム構成機器の修正パッチ情報の収集は頻繁に行い、
緊急性に応じて計画的に対応すべし

概要

A 社では、システムの通信機器（負荷分散装置）に障害が発生し、丸１日間業務が停止した。

原因は、システム構築・保守ベンダが外部メーカから調達した負荷分散装置のファームウェアにあった既知の不具合であった。その不具合の修正パッチは、１ヶ月前から公表されていたが、ベンダによる技術情報の確認サイクルが３ヶ月に１回程度と非常に粗く設定されていたため、パッチの公表に気づかず、その適用が間に合わなかった。システムのオーナーは、メーカの技術情報が時々公表されていることを認識していなかった。

対策として、以下を行った。

・技術情報の確認サイクルを３ヶ月に１回から２週間に１回へと変更した。

・A 社とベンダとでパッチ適用基準を協議した。

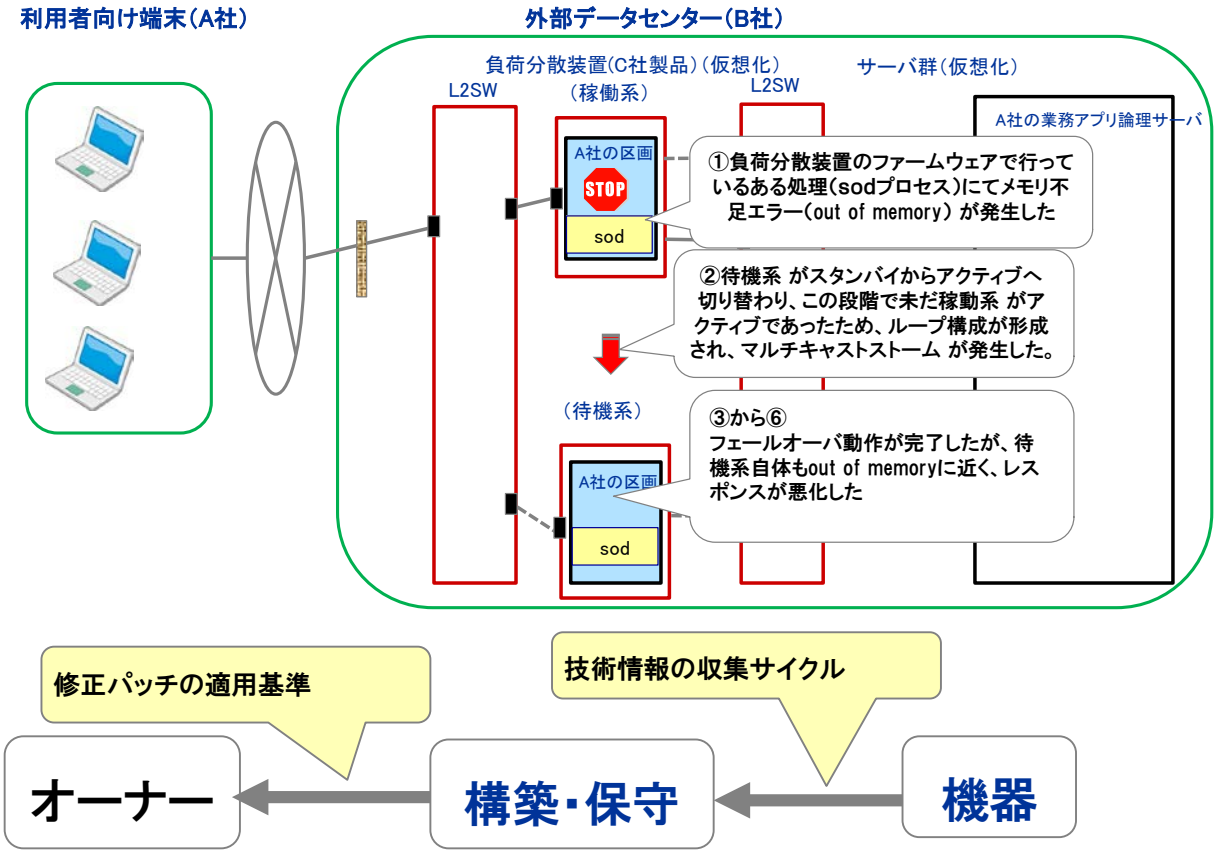


図２．２．２５―１　障害の経緯とパッチ適用

[35] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-91

活用が考えられる事例

◆ケース 49　不十分なパッチ管理

A 社では、システムリプレースに伴うデータ移行準備作業として、データベースのパラメータ変更作業を実施した。しかし、その際に開発環境では発生しない不具合が本番環境で発生し、システムダウンした。

原因は、本番環境には、開発環境に無いオプションを導入していたことにあった。今回の事象は、オプション導入環境においてオンライン作業時にのみ発生するパッケージのバグであり、１ヶ月前に「既知のバグ」としてメーカの技術情報 DB に掲載されていたことが分かった。

今後、製品ベンダが提供する最新の技術情報の確認を徹底することとし、パッチ管理を運用プロセスに組込んだ。

活用を考える

このケースも、教訓Ｔ１６の事例と同様に、修正パッチが発行されているにも関わらず、気づかなかったためにシステム障害を起こしてしまった事例である。

教訓集の「PARTⅡ　障害対策手法・事例集」の「3.12　パッチ管理」では、タイムリーなパッチ適用についての組織における対策策定のガイドラインを紹介しているので、参考にしていただきたい。[36]

◆ケース 50　パッチ適用漏れ

B 社では、システムの定期保守期間（システム稼働停止時）に、パッチ適用を行っている。

しかしながら、ある時システム障害が発生し原因を突き詰めたところ、緊急パッチが出たにも関わらず、それをすぐに適用しなかったため障害となったことが判明した。緊急パッチが出た時の運用が決まっていれば、定期保守前にパッチを適用できたと期待される。

活用を考える

このケースも、ケース 49 と同様に、適切なパッチ管理を行うことが重要である。しかし、発行されるパッチ情報は、時には膨大な量になる。したがって、基幹システムで使っているソフトウェアを優先して対応するなどの運用ルール、適用ルールを明確にしなければならない。

その上で、パッチ適用リストを作成し、適用状況を常時管理するなどの対策を講じる必要がある。

[36] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P.Ⅱ-391

２．２．２６．定期的な再起動に関する教訓（Ｔ１７）[37]

[教訓 T17]
長時間連続運転による不安定動作発生の回避には、定期的な再起動も有効！

概要

A 社では、稼働開始以来８ヶ月以上連続運転のシステムの通信機器に障害が発生し、丸１日間業務が停止した。

原因は、あるプロセスのメモリ資源を時間の経過とともに消費し続けるという負荷分散装置のファームウェアの不具合（装置を定期的に再起動していれば顕在化しなかったもの）であった。

対策として、システムの再起動のサイクルを検討し、毎月の定期保守日に状況を見て再起動することを決定した。（ネットワーク機器について、定期的に再起動することにより、長時間連続運転による不具合の顕在化が回避できることが経験的に知られている）

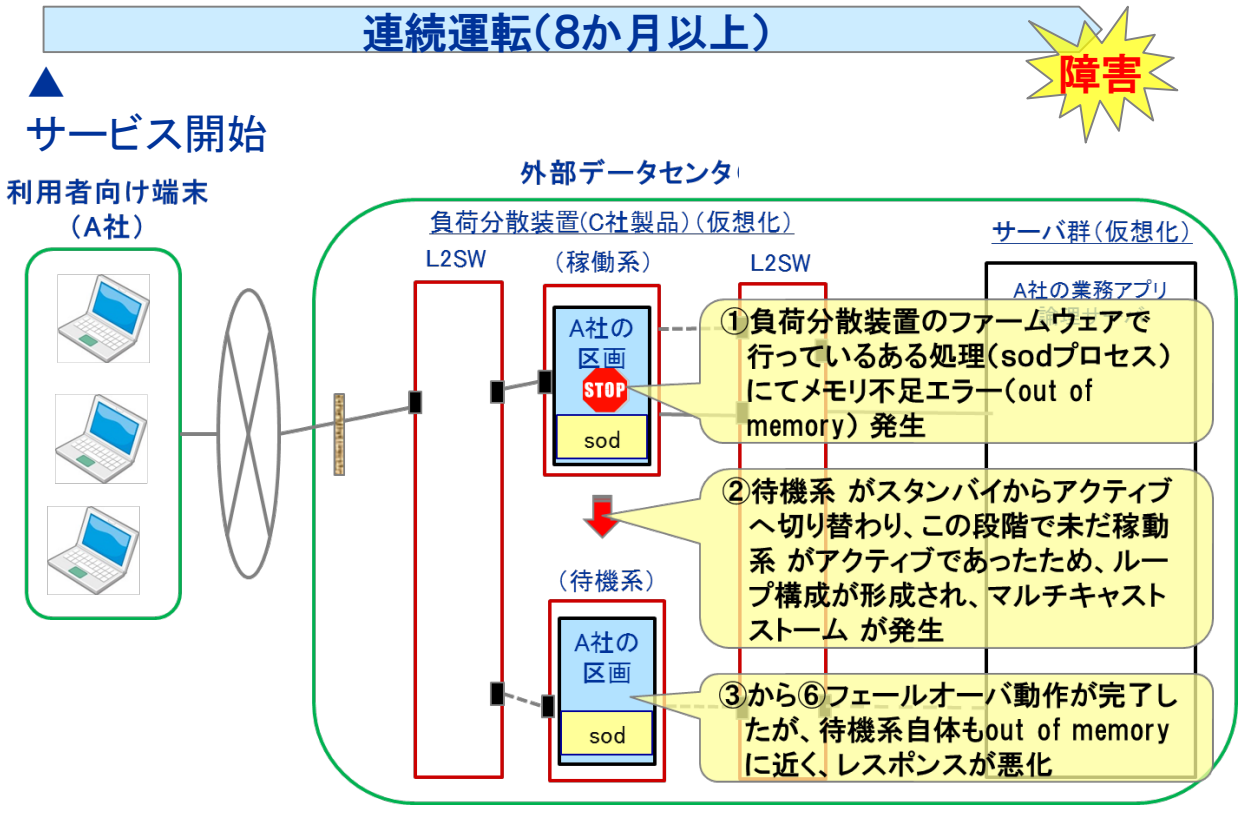


図２．２．２６－１　障害の経緯

[37] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-94

活用が考えられる事例

◆ケース 51　定期保守点検項目の追加

A 社は、商用電源が落ちた（停電）時に、本来稼働するはずの UPS（無停電電源装置）に電源が切り替らなかった。原因は、UPS（無停電電源装置）の出力分電盤が長期のホコリの堆積によって故障していたことに気づかなかったことであった。A 社では、定期保守期間（システム稼働停止）に、バックアップシステムの動作確認を行っていたが、長時間使用しているシステムの動作確認点検を行っていなかった。そこで、定期保守期間（システム稼働停止）に、長期間稼働している、または全く稼働していない装置の稼働確認として、電源の off/on を行う手順を追加することにした。

活用を考える

このケースは、長時間使っていない装置をいざ使う時に使えないといった、教訓Ｔ１７とは全く逆のパターンである。しかし、長時間装置を放置していたという類似点がある。

同じようなケースで、あるデータセンターで商用電源が停電になった時、自家発電機を使おうとしたところ、燃料が空になっていることに気づかなかったケースもあった。これも長時間使わなかったため、燃料の残量を監視するセンサーの故障に気づかなかったことにより起きた障害であった。

システム障害を未然に防ぐためには、「長時間」の稼働／未稼働の監視が重要であり、そのためにも定期保守時のチェック項目の洗い出しは、重要である。

◆ケース 52　製品の使い方により障害になる情報

B 社では、航空機向けに販売している制御機器の交流発電機の GCU（Generator Control Units）に、248 日（８ヶ月）以上にわたって電源を入れ続けると、内部のソフトウェアのカウンターが限界を超え、４個の GCU が同時にフェイルセーフモードに切り替わって、230 ボルトの交流電源がすべて使えなくなるというソフトウェア上の不具合がある疑いが判明した。

そこで、B 社は、同ソフトウェアを組み込んでいる制御機器を購入した顧客へ定期的に電源を落とす運用を推奨し、別途この製品のソフトウェアを開発した C 社へソフトウェアの改善を要望した。

活用を考える

教訓事例と同様にケース 52 は、長期間稼働するとシステム障害を起こすことが判明した事例である。また、事例とは逆の場合も存在する。それは、保守時に長時間稼働していたシステムを停止（電源 off）し、その後立ち上げようと（電源 on）したところ、電源が入らない、ストレージが故障し立ち上がらない、などの障害となったりする場合である。

このようなケースから、ある一定期間の間に再起動（電源 off、on）の運用を行うなどの障害の未然防止に繋げるような対策を検討すべきである。

２．２．２７．既存システムとのデータ連携に関する教訓（Ｔ１８）[38]

[教訓 T18]
新たなサブシステムと老朽化した既存システムとを連携する場合は
両者の仕様整合性を十分確認すべし

概要

A 社では、特別な事象を契機に、オンラインで大量の入力が集中して連携するバッチ処理がオーバーフローし、その後の対応も誤って 10 日間程度オンラインサービスを停止する事態となった。

原因は、携帯電話に対応した新しいシステムと既存システムとを接続した際の全体整合を十分チェックできておらず、携帯電話からのバースト的なサービス要求が無制限に受け付けられて後続のバッチシステムに連携され、夜間バッチの処理能力の制限値を超えて異常終了したためであった。その結果、膨大な作業が発生し、処理失念や誤処理による多数の副次的障害も発生した。

対策として以下を行った。

・既存システムの要件定義内容を再度チェックして連携するシステム間の整合性を確認。これらをルール化してマニュアルに反映。

・システムが異常終了しても途中から再開始可能な仕組みの導入。

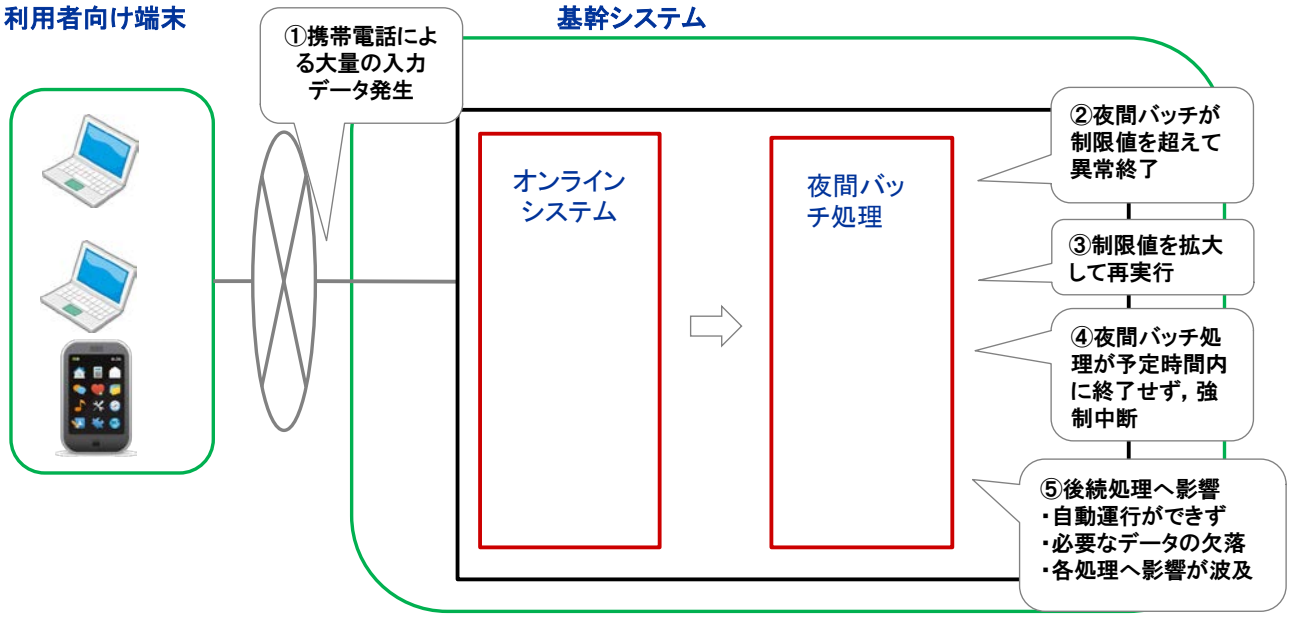


図２．２．２７－１　障害の経緯

[38] IPA/SEC『情報処理システム高信頼化教訓集（IT サービス編）』P. Ⅰ-96

活用が考えられる事例

◆ケース 53　システム切替え運用時の不具合

A 金融では、営業日に稼働する基幹システム（メインフレーム）とは別に、日曜日に ATM だけを稼働させる休日システム（オープンシステム）を運用する仕組みを構築した。いざ運用初日に当たる日曜日に休日システムを稼働させたが、ATM が例外処理を実施するたびに無応答になり、以降、立ち上がらなくなってしまった。

障害発生時は、担当者が現場に出向き、ATM を手作業でリセットして回った。

原因は、新しく開発した休日システムの例外処理の通信手順と基幹システムの例外処理の通信手順に不整合があったことだった。以前から使用している基幹システムの例外処理の通信手順にタイマ監視値の変更がなされていることに気づかず、休日システムにはその変更された仕様が共有されていなかった。

活用を考える

このケースのように、１つの ATM（クライアント）が、２つのホスト／サーバと切り替えて接続し、処理を行う時、思わぬ仕様の違いにより障害を引き起こすことがある。

この教訓Ｔ１８「新たなサブシステムと老朽化した既存システムとを連携する場合は両者の仕様整合性を十分確認すべし」を踏まえ、事前に障害時の対応ルールを決め、さらに要件定義を確認し合い、例外処理については念入りなテストを行うべきであった。

◆ケース 54　新旧システム並行稼働の障害

B 証券会社では、債権取引システムに障害が発生し、取引が停止した。B 社は、新システムへの移行中にあり、新システムと現行システム間の移行中継システムを介して接続し、並行稼働中であった。

原因は、移行中継システムの業務プログラムの新旧の変換処理にバグがあり、その結果現行システム、新システムともダウンした。

活用を考える

このケースも移行中継システム（新システム）に老朽化した現行システムを繋いだ事例と言えよう。新システムの設計にあたっては、現行システムが長年稼働している間に、様々な要件追加、変更が行われていないか、途中からデータ内容も変更されていないか、例外処理が追加になったりしていないか、トラブル発生により一時的なパッチを当てただけのデータがあったりしないかと、確認する内容が膨大になる場合がある。ケース 53 と同様に、この教訓Ｔ１８「新たなサブシステムと老朽化した既存システムとを連携する場合は両者の仕様整合性を十分確認すべし」を活用し、入念な確認を行うことが重要である。

３．情報（障害事例・教訓）共有

本書の「１．３　活用メリット」で述べたメリットをより効果的に得るために、IPA/SEC は、障害事例や教訓などの情報共有活動を組織間（企業内）、企業間（業界内）、業界間（産業界内）へとより広く展開することを推進している。

ここで言う情報共有には、各報告単位（企業内プロジェクト、企業など）から集めた障害事例の共有、それを教訓としてまとめたものの共有、の２段階がある。この関係を企業間・業界団体の情報共有の範囲に当てはめると（図３－１）の関係になる。

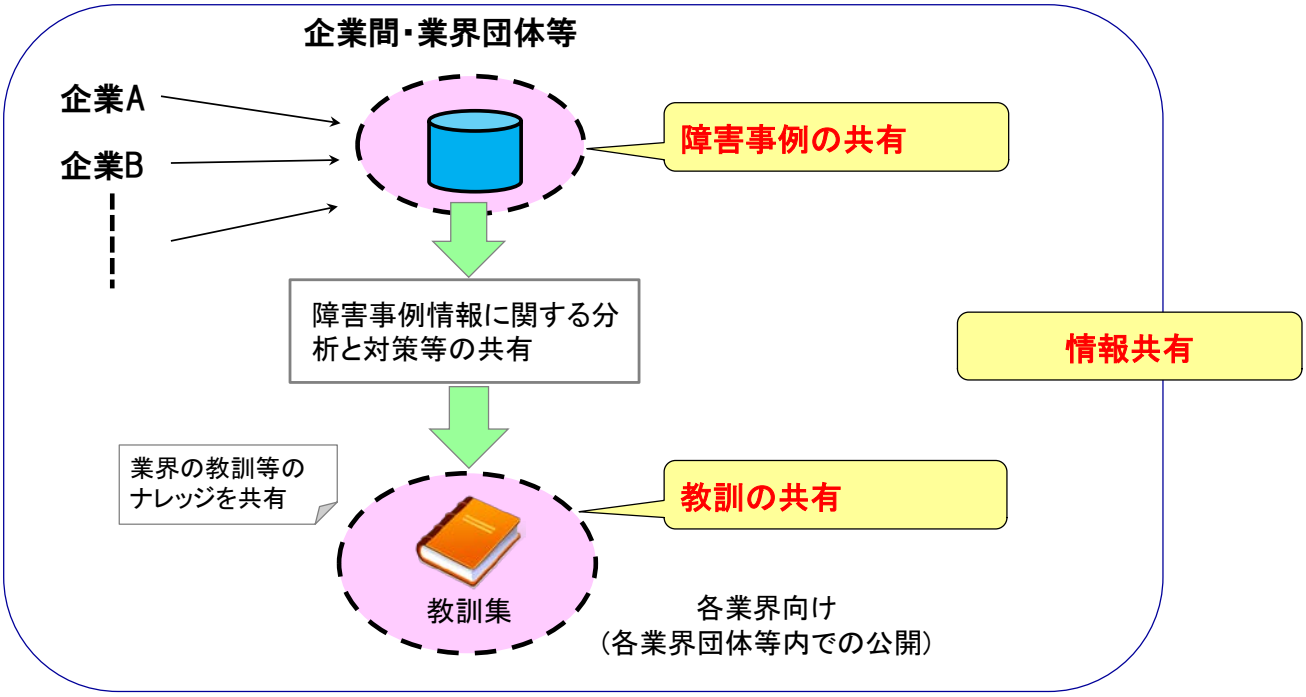


図３－１　共有の範囲

この章では、具体的にシステム障害事例の共有活動をどのように行っていくのかについての方法を紹介する。

前章までに述べたように、IPA/SEC で作成した教訓集を活用することは、システム障害対策への取組みの参考にはなるであろう。しかし、システム障害削減は、自らが積極的にシステム障害の教訓化に取り組み、また他社の教訓も自社の対策に取り込んでいくといった、システム障害の情報共有活動に参加してこそ、達成できる。また、自組織（プロジェクト）、自社の教訓を発信してこそ、他社からも教訓を受けることができるので、協力関係の構築が、必要不可欠である。

３．１．情報共有活動の進め方と効果

IPA/SEC において試行したシステム障害の情報共有の仕組みを今後幅広く展開する方法として、(図３．１－１）に示すような仕組み作りを推進していく。

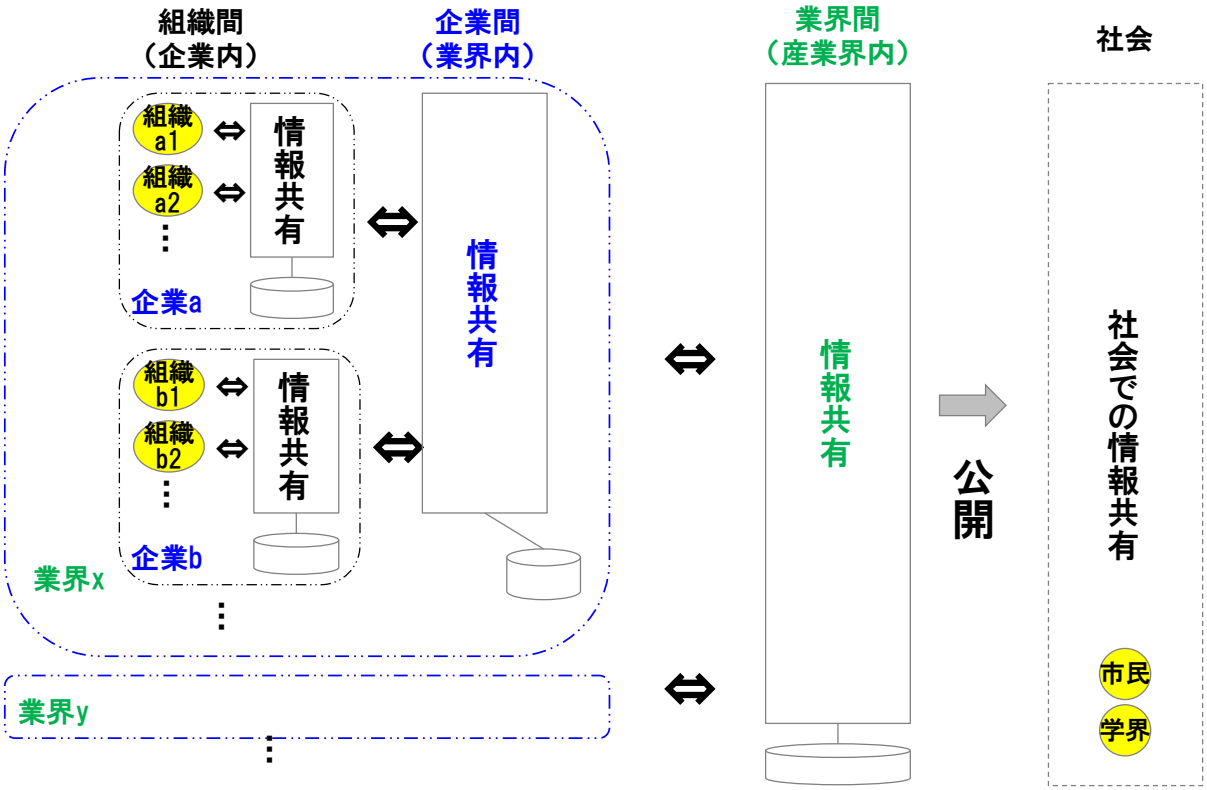


図３．１－１　情報（障害事例・教訓）共有のしくみの展開イメージ

また、情報共有の仕組みは、(図３．１－２）のような機能を各情報共有単位に持つことにより、運営することができる。

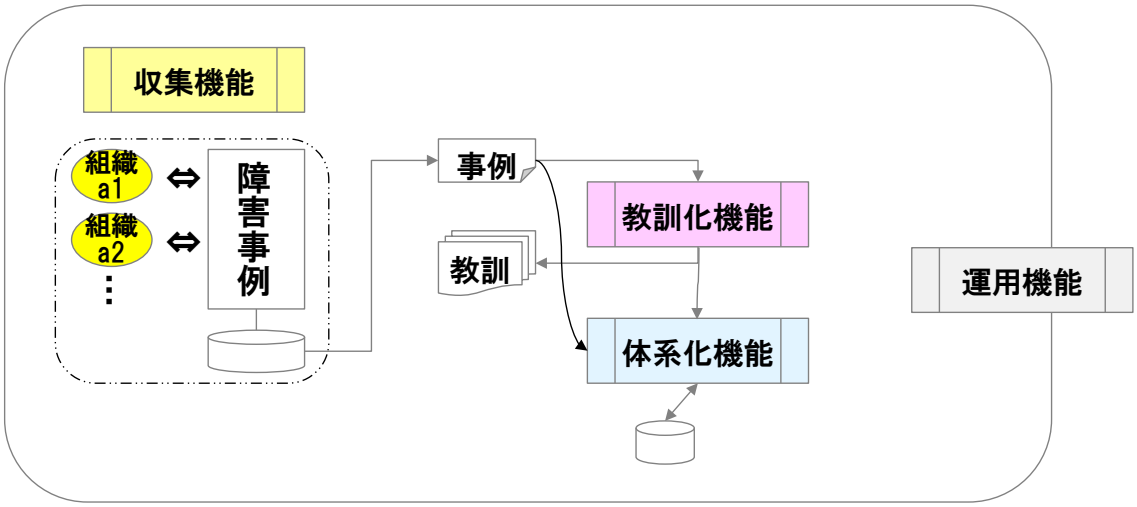


図３．１－２　情報共有の機能

◆組織間（企業内）の情報共有

企業の中にも、様々な組織があり、様々なシステム、サービスを構築し運用している。またそれらがいくつかのプロジェクトを立ち上げて実施されている場合もあろう。

企業内とはいえ、各プロジェクト、組織において、システム形態、規模、ソフトウェアの違い、ベンダの違いなどによって、横の情報共有が十分行われていない場合がある。例えば、通信事業者であれば、通信網システムの管理、サービスの開発、料金システム、など様々なシステムがある。組織間（企業内）によっては、部署内それぞれの中で情報共有していることはあっても、部署を跨ぐ情報共有は行っていない場合がある。

しかし、どのようなシステムであれ、人が介在している以上、必ず共有できる課題、対策は存在する。まずは、その組織間での情報共有活動を行うことから始まる。

情報共有のメリット

組織間（企業内）の情報共有は、お互いの情報（システム形態、規模、ソフトウェアの違い、ベンダの違い）が入手し易いため、比較的容易に情報共有することができ、障害対策を素早く行うことができる。

また、組織間（企業内）では、情報の横展開も素早く行うことができ、全社的なシステム改善対策が行われるので、社内全体の生産性も向上することができる。

このような情報共有を日常的に行うことで、システム要員の異動も行いやすく、全社的な IT の活性化が可能となる。

◆企業間（業界内）の情報共有

分野・業界ごとに情報共有グループを設置し、そのグループごとにこの取組みを行っていく。コンテキスト の同じ関係者が集まる同分野・業界におけるグループは、より活発な議論が行われるものと期待できる。

また、業界団体の所属企業全ての参加が難しい場合は、有志企業だけの集まりでスタートしても効果は、十分ある。むしろ積極的に問題意識を持った者同士が、議論が活発になり、良い効果を得ることもあり得る。

情報共有のメリット

企業間（業界内）の情報共有は、お互いの情報（システム形態、規模、ソフトウェアの違い、ベンダの違い）は入手し難いが、各社とも類似のシステムを使っている場合が多い。例えば、銀行の勘定系システム、鉄道会社の列車運行管理システム、放送会社の営業放送システムなど業界ごとに多数の類似システムが存在する。

そのような分野では、既に IT 技術の意見交換を業界内で行っているところもあり、その中で、比較的共通の話題が生じ情報共有することができ、他社事例から自社の未然防止としての障害対策を素早く行うことができる。

また、システム障害を共有することで、運用保守の工数を下げることができ、各社が本来競争すべきサービス提供分野へのシステム投資に振り向けることが可能となるため、最終的には、日本の産業競争力

が国際的に高まっていく。

さらに、ベンダに対しても、共通の課題を提示することにより、より効率的な解決策を引き出せる。

このような、業界、あるいは有志企業のシステム障害に協力しあって取り組んでいる姿勢は、サービスの提供を受ける顧客の信頼を得ることであろう。

◆業界間（産業界内）の情報共有

システム障害の根本的な課題を見つめ、それを抽象化した教訓にまとめた時、システム障害は、他業界の事例も参考になる。そのため、分野・業界を越えた情報共有の仕組みも必要となるため、それらのグループ間で情報共有できるよう、グループ横断的な情報共有の場を設ける事も重要である。

また、航空や原子力、医療などの分野では、日本だけでなく世界を見渡した情報共有が必要であろう。さらに、IoT が話題になっている昨今では、様々な製品、制御、サービスなどがつながることによって、情報共有の範囲、組合せは、いろいろ考えられるであろう。

情報共有のメリット

様々な分野でのシステム障害は、例えば先進的な取組みを行っている業界のシステム障害の教訓を他分野が参考にして、自社の未然防止に活用することができる。

また、有志企業の業界が異なる場合の方が、例えば情報共有活で意見交換を行っていても、強豪相手ではないので、意見が言いやすく、また他分野からの貴重な知見を得ることができる。

◆社会での情報共有

このようなシステム障害の情報共有が広く社会で共有されれば、安心、安全な社会を築く活動になろう。システム障害を学問として取組む人たちも現れるであろう。

情報共有のメリット

全ての情報共有活動は、社会の安全に必要不可欠な活動として市民権を持つことができる。そうなれば、情報公開もよりオープンになり、システム障害を隠すことは企業の信頼を損ねることが社会の共通認識となり、早く取組みを開始した組織の評価は高いものになろう。

３．２．情報共有活動における疑問

IPA/SEC で取り組んでいるシステム障害の情報共有活動に対して、賛同できる分野がある一方、難しい分野も存在する。ここでは、そのような情報共有活動が難しい分野でも、十分共有活動に取り組んでいけることを解説する。

システム障害の情報共有活動は難しいと考える人には、システム障害の教訓化が、「その障害を起こした情報が、十分正確な詳細情報でなければならない。」と考えたり、「システム障害を公表すると自社に不利益をもたらす。」と考えたりしている可能性がある。このような点は、参加者同士が意見を述べ合い、調整し、情報共有に参加するルールを明確にすれば解決する。

情報共有活動が難しい分野では、以下の様な「情報共有ポイント」を検討することをお勧めする。

情報共有活動の疑問に答える４つのポイント

【ポイント１】業界で共有するのは、システムやサービスの情報ではなく、あくまで障害の情報である。
【ポイント２】業界全体のメッセージとして、広く社会にこのシステム障害に対する取組みをアピールすることができる。
【ポイント３】共有するシステム障害情報は、生情報である必要はない。
【ポイント４】システム障害の情報共有は、システム障害未然防止のためのものである。

現在、情報共有活動に賛同いただいている業界、団体は、概ね以下のようなところである。

・業界内の企業、団体が競合し合うことが少ない
・自主的にシステム障害を減らしたいと考えているボランティア組織
・業界横断的な地域別グループ、団体

これらの賛同いただいている業界、団体は、【ポイント１】から【ポイント４】までが理解されているか、もしくは共有活動を妨げる障壁が低い。

一方、情報共有活動に対して難しい分野の業界団体、企業団体も、個別に聞いてみると、「システム障害事例は出さないが、他業界、他企業団体の障害事例は、知りたい。知ることができれば自社に役立てることができる。」と考えている。つまり自主的に活動開始を踏みとどまっているのは、組織内での説明性が欠けていることが要因であることから、参加企業にとってのメリットが明確になれば、共有活動は広がっていくことが期待される。

我々IPA/SEC の活動は、情報共有を阻む壁を取り除き、共有活動の参加意義とメリットを訴えていくものである。以下、上記のポイントについて述べる。

【ポイント１】業界で共有するのは、システムやサービスの情報ではなく、あくまで障害の情報である。

システム障害の情報共有活動に対して消極的な企業・団体は、「IT サービスのシステムの要否が経営に大きく影響するので、競合他社にシステム障害事例を教えるようなことはできない。」と考えがちである。

しかし、業界で共有するのは、自社のシステムやサービスの情報ではなく、あくまでシステム障害の情報である。ある程度のシステム構成やサービス内容を共有しなくてはならない面もあるが、必要なのは、発生した障害そのものの原因と対策であって、局所的な情報である。我々の今までのシステム障害情報の共有活動においては、報道されている情報を元に障害事例を共有することでも、十分教訓になり得た。

更に将来的なことを言えば、IoT の時代においては、このようなシステム障害レベルでサービス各社が競争する意義はあまりなく、むしろ積極的に情報共有することで、障害時対応のコストを下げ、本来力を入れるべき競争分野にリソースを集中すべきである。

【ポイント２】業界全体のメッセージとして、広く社会にこのシステム障害に対する取組みをアピールすることができる。

システム障害の情報共有活動に対して消極的な企業・団体の中には、「自らの業界内では、中心となる企業が数社しかないので、情報共有のメリットがあるとは思えない。」と考える。

しかし、数社しかない場合こそ、業界全体のメッセージとして、広く社会にこのシステム障害に対する取組みをアピールすることができる。数社しかない業界の中で、１社が起こしたシステム障害は、業界全体に影響する。例えば、システム障害ではないが、原子力発電所での１件の事故は、全ての原子力発電所への信頼に影響したことなどがあげられる。

業界全体で、信頼性向上の取組みをアピールすることは、業界全体にとって大きなプラスに働く。

【ポイント３】共有するシステム障害情報は、生情報である必要はない。

システム障害の情報共有活動に対して消極的な理由の一つとして、「社内秘に扱われているシステム障害情報を（業界に関係なく組織として）外部に伝えることはできない。」があげられた。

しかし、共有するシステム障害情報は、生情報である必要はない。障害情報を発表する時、匿名化したり、一部機微情報の塗りつぶし、置き換えを行ったりしても、教訓としての価値は十分ある。

また、必要であれば、参加企業同士で機密保持契約（NDA）を結ぶことをお勧めする。

【ポイント４】システム障害の情報共有は、システム障害未然防止のためのものである。

システム障害の情報共有活動に対して消極的な理由の一つとして、「障害は、監督官庁に報告している（報告義務がある）ので、それを監督官庁以外の別な外部に公表することはできない」があげられた。

しかし、システム障害の情報共有は、「犯人探し」や「責任追及」を行うことではない。あくまで、他社にとってのシステム障害未然防止のための情報共有である。したがって、システム障害の事実を全て公表する必要はなく、教訓となるべき箇所だけ抽象化して公表するだけで、十分に有益である。

実際の共有活動立ち上げについては、様々な個別の事情も存在すると考える。IPA としては、それらの情報共有を阻む壁を業界団体・企業と共に取り除き、全業界でシステム障害の情報共有ができるように取り組んでいきたい。

３．３．業界グループ情報共有活動事例

情報共有のための第一歩は、情報をオープンにすることから始まる。さまざまな情報から、傾向や仮説を推定し、新たな発見を得たりするということは昔から経験的に知られており、情報をオープンにすることにより加速されることが分かっている。

ただし、いきなり自社の障害情報をオープンにすることはできない場合もあろう。

そこで、高信頼なサービス水準を維持し続けるために適切な情報が公開され、それらの分析結果が業界・分野を越えて幅広く共有されている先進的な試みを行っている業界団体を紹介する。

紹介する各業界団体は、IPA/SEC が情報共有活動の意義を提案してまだ数年の状況の中で、このような活動に賛同していただいた。それらの団体は、共有グループを立ち上げ、徐々に活動の範囲を広げている。

ここでは、いくつかの業界グループ内での情報共有活動事例を活用ツール毎に紹介する。活用しているツールは、グループウェア、公開ホームページ、グループ参加者だけのメーリングリストがある。
情報共有の仕組みは、それぞれの業界団体の状況によって対応が異なり、今回紹介する事例以外の方法もあるであろう。IPA/SEC は、各業界団体の要望によって、それぞれの団体にあった共有方法を支援している。

【参考】

IPA/SEC では、2010 年６月に、『障害事例共有サイト実態調査　調査報告書』（文献３－１）を公開した。

この報告書の公開時点（2010 年）では、情報システムに対しては障害情報等を共有するための場が存在していないが、国内外の事故や不具合を収集、共有を推進している組織やデータベースは、存在していた。

報告書では、そのような組織やデータベースの状況、Web 上での公開の状況、事故や障害事例を収集している目的、法制度との関係、また収集した事故および障害情報の活用状況を整理している。また、報告書の付録では、「障害事例提供サイト URL」が掲載されている[39]ので、直接アクセスすることができる。

[39] IPA/SEC『障害事例共有サイト実態調査　調査報告書』P.65

３．３．１．システム障害を議論するグループ活動事例

システム障害の情報を収集・蓄積し再発防止策をまとめ，共有する最も効果的な活動は、関係者が集まってグループを作り、直接議論し合うことである。

IPA/SEC で作成した教訓集も、それぞれの業界分野の IT 専門家、実務家が集まった委員会にて議論を行って作成した。委員がそれぞれの障害事例を持ち寄り、または外部の IPA/SEC の取組みに賛同していただいた方々で障害事例を持ち寄って、それを参加者全員で議論し合った。その中で、真の原因とは何か、対策は事例で行われた対策以外にもどのようなものがあるのか、等々議論し合い、教訓としてまとめたのである。

このような活動を通し、委員から、貴重なコメントをいただいたので、以下に紹介する。

- さまざまな分野での経験から得られた教訓の中から自社に適用可能なものを見つけ、活用することができた。
- 情報共有のグループ（“教訓”化過程）への参加により、公開“教訓”より深い情報（開示レベルがグループ内限りの情報）が得られた。
- 自社の事例情報に対する有識者や他分野の専門家等からの意見や、“教訓”化（抽象化）の議論を通して“気づき”が得られた。
- 他分野の方々との交流が深まり、また、他分野の事例の中に参考になるところがあった。
- 自社事例の“教訓”化の議論の中で、“気づき”を得ることがあった。

このような、システム障害を分析し対策を立て教訓化するための手順を、「教訓作成ガイドブック」にまとめているので、そちらも参照願いたい。

また、IPA/SEC では、「教訓作成」のワークショップ形式のセミナーを行っている。このセミナーに参加していただければ、具体的な教訓作成のプロセスを学ぶことができる。

セミナー参加者の声（参加者アンケートの一部抜粋）を、以下に紹介する。

- 障害事例など身近な例で理解しやすかった。
- 他組織の事例を知る機会は多くないため、こうした資料があると非常に助かる。今後も内容が充実していくと言うことで、期待している。
- 自社の障害のことしか知らなかったが、他社の考えなどを聞けて参考になった。また、事例集も自社システムに活用できるか検討したい。
- これまでも自分達でも漠然とは考えていたことを整理して示していただくことでよく理解でき、大変有意義であった。
- 現実に立脚し、具体的で非常に有意義であった。

３．３．２．グループウェアを活用した情報共有活動事例

IPA/SEC は、A 業界団体の会議にて障害情報の共有の意義を説明した。参加した団体の皆さまは、そのような活動を理解し、同会議において、情報共有を行うことを決議した。

席上、このようなシステム障害の情報共有の取組みに対する必要性・重要性について参加者から以下のような意見が寄せられた。

・システム障害は小さなものならば日々発生している。
・委託管理の視点から情報共有には意味がある。例えば、業者が既知の問題を捉えているかというチェックを行うことができる。
・短時間でもシステムが止まればお客様を待たせることになる。それを未然に防止する上でも他団体の事例や情報を共有し、リスクを回避する必要がある。

以下に、この業界団体の情報共有の仕組みを紹介する（図３．３．２－１）。
各団体のシステム管理部門の担当者は、ヒヤリハットを含めた、他団体にとっても有効であると思ったシステム障害事例を、特定されたグループウェアの掲示板に登録する。各団体の担当者は、その情報を見て、自分の団体にも当てはまるのではないかと思った事例は、未然予防対策に活用している。

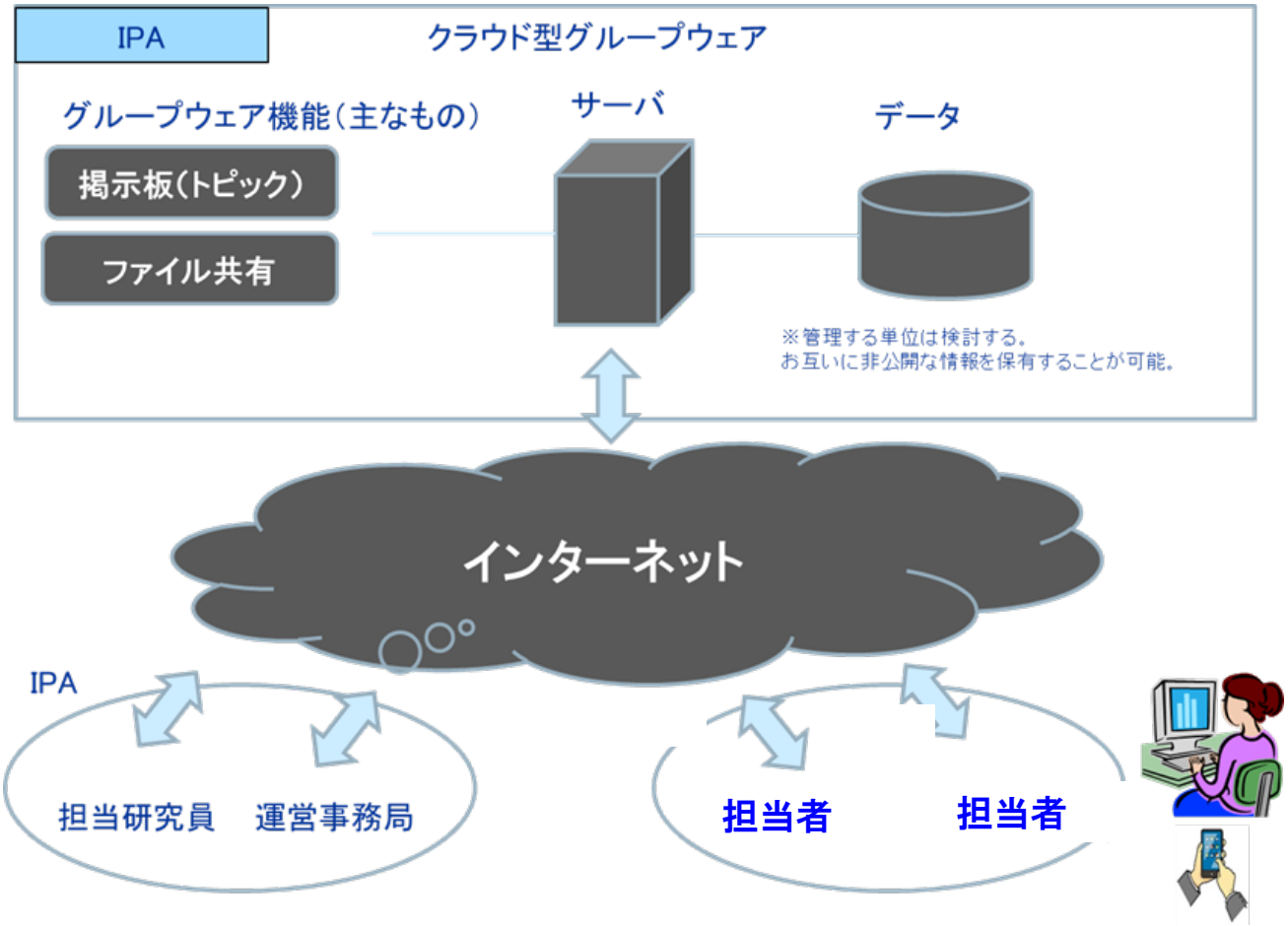


図３．３．２－１　情報共有の仕組み

３．３．３．公開された Web ページを活用した情報共有活動事例

IPA/SEC との協業で、B 情報サービス団体は、「障害再発防止策研究会」を発足させ、システム障害情報の教訓化の仕組みを団体内に構築し、教訓作りに取り組む活動開始した。その活動の成果を B 情報サービス団体の Web ページ上で「情報処理システム障害事例集」として公開し、IPA/SEC の Web ページからも URL リンクによる連携を実施している。同研究会は、さらに「システム高信頼化研究会」と改称して活動を継続しており、IPA/SEC との意見交換も継続して行っている。

以下に、「情報処理システム障害事例集」の教訓タイトルの一部を紹介する（図３．３．３－１）。

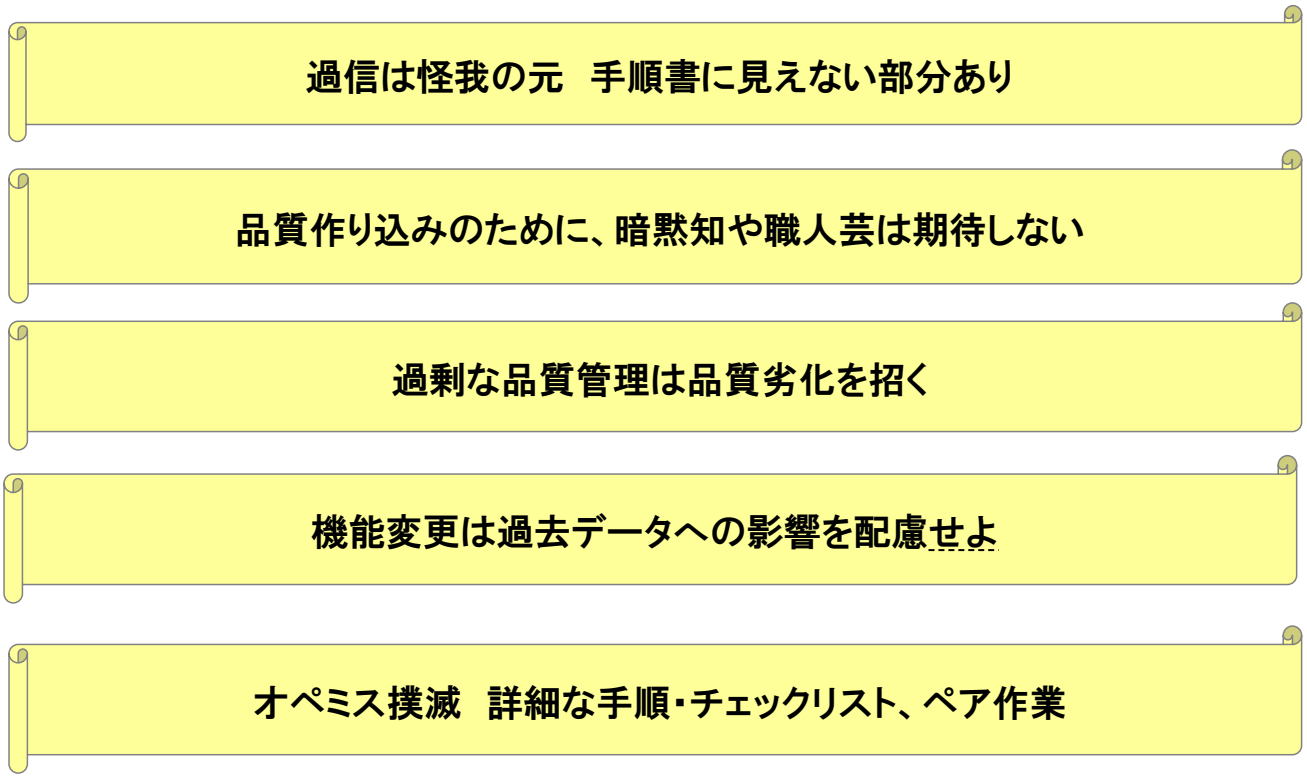


図３．３．３－１　「情報処理システム障害事例集」教訓タイトル（抜粋）

３．３．４．グループ参加者だけのメーリングリストを活用した情報共有活動事例

IPA/SEC は、C 業界団体と協議し、情報共有の取組みに賛同する９組織とメーリングリストを使用した情報共有を行うことで合意した。

まずは、IPA/SEC にて障害共有情報を同業界に絡めて編集し、IPA/SEC からの情報提供として実施している。今後、共有の意義を醸成してから、より良い共有活動のあり方を検討していく予定である。

メーリングリスト例

◆システム障害からのセキュリティ事故

システム障害から生じたセキュリティ事故は、システム設計時にリスク管理の観点から如何なる場合でもセキュリティ事故にならないようにする、一種のフェイルセーフの考えが必要ではないでしょうか。

◆事例１　一部ユーザの各種設定情報が他ユーザに閲覧可能

A 社の一部ユーザの xx モード各種設定情報が、他ユーザに閲覧・変更可能となる事態が多数発生した。

xx モードシステムでは､利用者を２群に分けて同じ機能を持つサーバ A 群と B 群に分散して収容していた。今回ソフトウェアの更改にあたって、B 群サーバに誤って A 群サーバ用のソフトウェアを適用してしまったため、B 群側から A 群側のユーザの情報を参照・更新可能となってしまった。

▲教訓を考える

この障害で考えられるのは、運用面でのヒューマンエラーを考慮しない設計上の問題があったことです。A 群と B 群のシステム設定ファイルのファイル名を含めて、同じであったことは、設計時に運用面での作業の誤りを起こさない対策ができていなかったと考えられます。

このような障害を減らすためには、教訓Ｇ３「運用部門は上流工程（企画・要件定義）から開発部門と連携して進めるべし」を活用することをおすすめします。

メーリングリストでは、以下のテーマなどで情報発信を行っている。

- ・報道されたシステム障害　情報システムの障害状況
- ・事例報告　業界内における過去の類似障害
- ・教訓解説　「バックアップ切替えが失敗する場合を考慮すべし」についての解説など
- ・類似障害の解説と教訓活用のポイント
- ・IPA/SEC セミナーのお知らせ　「事例から学ぶ IT サービスの高信頼化へのアプローチ」など
- ・最近の団体所属各社様の IT サービスの取組み

３．４．情報共有活動における教訓活用

前章で紹介したように、IPA/SEC が、各業界団体を訪問し情報共有活動の意義を提案し、その結果、賛同していただいた業界団体は、共有グループを立ち上げ、活動を行っている。そこで、IPA/SEC の教訓と同様に、共有グループの作成した教訓をどの様に活用する方法があるかを解説したい。

IPA/SEC の教訓活用と同様に、各業界団体が作成する教訓は、見る者が役立ちそうな教訓を容易に見つけられること、教訓が自分自身にとって有効かそうでないかを適切に判断できること、などが求められる。そのため、その教訓を活用するには、その入口を見つける手段を提示することになるであろう。つまり、各業界団体が作成する教訓についても、自らの教訓をどう活用して欲しいかといった観点での「教訓活用ガイドブック」を作成することが望ましい。

IPA/SEC の教訓と異なり、共有グループの教訓事例のコンテキストは、参加企業同士、類似している点が多いと考えられる。したがって、活用方法はより的が絞られ、効果の高い活用方法があるのではないか。

◆自分が持っている課題に対して、自社内、各業界団体が作成する教訓が参考になるのか知りたい

例えば・・・

・他事例を見て、運用面から自システムの予防対策をどのように立てれば良いのか調べたい。
・システム障害の原因が開発時の要件漏れであった場合は、設計時にどのような対策を立てれば良いのか。また、設計時に予防対策をどのように取り込めば良いのか。
・事例から、調達時に予防対策を立てたいが、システム障害の原因がレビュー不足や試験不足の場合は、どのような対策を立てれば良いのか。
・他事例を見て、レビューの進め方、試験の進め方をどのように行えば良いのか。
・若手要員の育成を検討し、システム障害の未然防止訓練・教育を行いたい。

◆自社内、各業界団体が作成する教訓から、活用方法を知りたい

例えば・・・

・他社、他プロジェクトでは、どんな障害が出ているのか、知りたい。
・同じベンダの製品を使っている他社の障害事例は、事前に自社の対策に活用したい。
・業界固有、同業者共通の障害はあるか、あれば、未然防止に役立つか。
・いつも場当たり的な対応になっている障害対策を根本問題から解決したい。

４．おわりに

システム障害は毎年報道されている。最近では、今まで報道されることが無かったような機器までもがシステム障害として報道されている。今後、IoT 時代がますます発展することにより、システム障害は毎年増え続け、また影響範囲も広がっていくことが予想される。

今後、システム障害の削減に向けた社会からの要望は、ますます増大する一方、その対策コストも増大するものと思われる。

このような情勢を鑑み、よりよい社会の構築に向けた取組みとして、システム障害の情報共有活動は、重要な取組みになるのは間違いないであろう。

読者にあっては、このような先進的な取組みに積極的に参加していただければ幸いである。

＜謝辞＞

本ガイドブック作成にあたり、貴重な助言をいただいた重要インフラ IT サービス高信頼化部会の中村英夫主査（日本大学理工学部教授）に深く謝意を表します。

付録　活用が考えられる事例のケース一覧

本ガイドブックに掲載している活用が考えられる事例の「ケース」のタイトルから教訓に結びつけることも可能であるので、ケース一覧としてまとめた。

教訓	ケース番号	タイトル	該当教訓ページ
Ｔ７	ケース 31	バックアップ切替え対策の不備	51
	ケース 32	バグによるバックアップ切替え失敗	51
Ｔ８	ケース 33	仮想化システムの運用見直し	53
	ケース 34	仮想化システムの障害対策	53
Ｔ９	ケース 35	ハード障害によるソフト不具合が多重的に顕在	55
	ケース 36	不測事態発生への備え	55
Ｔ１０	ケース 37	フルメッシュ構成の誤解	57
	ケース 38	ネットワーク構成の検討	57
Ｔ１１	ケース 39	サイレント障害対策	59
	ケース 40	つぶやきの活用	59
Ｔ１２	ケース 41	高性能機能に変えたつもりが機能低下	61
	ケース 42	メーカによって異なる仕様によりエラーが発生	61
Ｔ１３	ケース 43	別人からの公共料金徴収ミス	63
	ケース 44	システム統合における連携ミス	63
Ｔ１４	ケース 45	Web 処理の遅れ対策不足	65
	ケース 46	非機能要件の設計ミス	65
Ｔ１５	ケース 47	ファイルの取違え	67
	ケース 48	テストデータの戻し忘れ	67
Ｔ１６	ケース 49	不十分なパッチ管理	69
	ケース 50	パッチ適用漏れ	69
Ｔ１７	ケース 51	定期保守点検項目の追加	71
	ケース 52	製品の使い方により障害になる情報	71
Ｔ１８	ケース 53	システム切替え運用時の不具合	73
	ケース 54	新旧システム並行稼働の障害	73

参考文献

（文献１－１）八山幸司『米国等のサイバーセキュリティに関する動向』(IPA)，2015 年
https://www.ipa.go.jp/files/000044581.pdf

（文献１－２）IPA/SEC『情報処理システム高信頼化教訓集』(IPA)，2015 年
http://www.ipa.go.jp/sec/reports/20150327_1.html

（文献２－１）IPA/SEC
『高信頼化ソフトウェアのための開発手法ガイドブック～予防と検証の事例を中心に～』
（IPA），2011年　P.23
http://www.ipa.go.jp/files/000005144.pdf

（文献２－２）IPA/SEC
『高信頼化ソフトウェアのための開発手法ガイドブック～予防と検証の事例を中心に～』
（IPA），2011年　P.147
http://www.ipa.go.jp/files/000005144.pdf

（文献２－３）IPA/SEC
『経営者が参画する要求品質の確保～超上流から攻めるIT化の勘どころ～第２版』
（IPA)，2006年
http://www.ipa.go.jp/sec/publish/tn05-002.html

（文献２－４）IPA/SEC
『高信頼化ソフトウェアのための開発手法ガイドブック～予防と検証の事例を中心に～』
（IPA)，2011 年　P.127
http://www.ipa.go.jp/files/000005144.pdf

（文献３－１）IPA/SEC『障害事例共有サイト実態調査　調査報告書』(IPA)，2010 年
http://www.ipa.go.jp/files/000004545.pdf

（このページは空白です）