IPA Better Life with IT

情報処理システム高信頼化
教訓作成ガイドブック
（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作成ガイドブック（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

IPA/SEC では、情報処理システムの障害事例情報の分析や対策手法を整理・体系化して、これから導かれた「情報処理システム高信頼化教訓集」を作成した。

本書では、上記の作成過程で得られたノウハウを元に、教訓集の利用者が自社の事例をもとにして障害を予防するための「教訓の作り方」をまとめた。読者の皆様が本書を読むことで、発生した障害の原因を分析して対策を検討し教訓としてまとめ、教訓を活用するための分類の方法を習得することができる。さらに、自社で作成した教訓を外部に発信することによって、今まで個人や組織内、企業に閉じていたノウハウが広く社会で共有できるようになると期待する。

また、本書とは別に、教訓を活用するためのガイドブック（以下「教訓活用ガイドブック」）[1]を作成したので、合わせてご覧いただきたい。

１．２．本書の位置づけ

教訓に関連する成果物は図１．２－１に示すように全部で３種類ある。そのうちの１つである本書は教訓を作るためのガイドブックであり、本書に基づいて作成した教訓は「教訓活用ガイドブック」に基づいて実地に活用できるような分類体系となる。

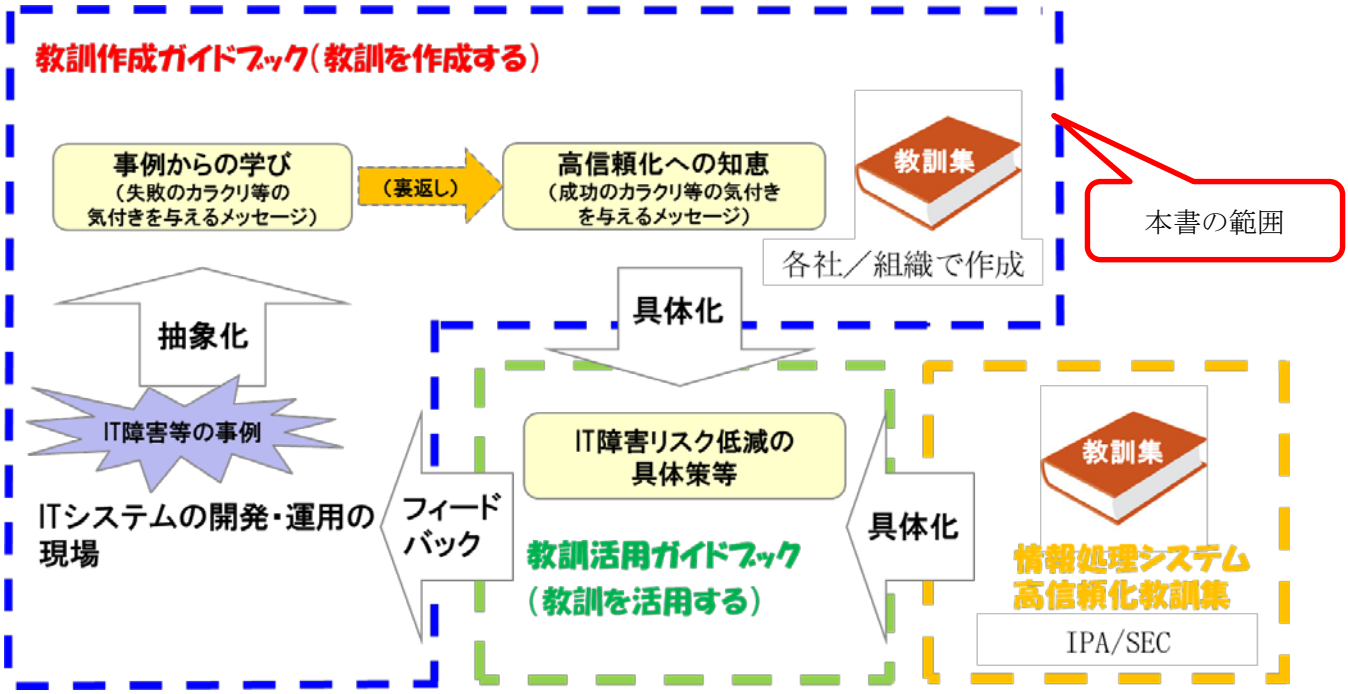


図１．２－１　教訓の作成および活用とガイドブックの関係図

[1] 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）
http://www.ipa.go.jp/sec/reports/20160229.html

１．３．本書の構成

本書の構成の柱は、「教訓の作り方」と「教訓の分類の仕方」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、本書の構成をまとめている。

「２．教訓を作成する」では、教訓の作成方法について解説している。

「３．教訓を分類する」では、利用者にわかりやすいように教訓を分類する方法を解説している。

「４．教訓作成の組織／体制」では、教訓を作るための組織体制やマネジメント方法を記述している。

２．教訓を作成する

本章では教訓とは何かという概念、教訓を作るための作業手順、障害の原因分析の方法を記述する。

まずは、「教訓を作るとはどういうことか」という概念から説明する。教訓を作ることは、大きく分けると図２－１のような３つの段階になる。

① 問題（個々の事象）の原因を追求 → 抽象化 する。
現場の個別の IT 障害の事例の原因を分析し、本質的なものへと抽象化する。

② 原因から対策を導く → 裏返し → 教訓化 する。
原因を根本的なものまで分析し、対策を検討する。原因の裏返しが対策となることが多い。

③ 対策・教訓を現場で適用 → 具体化 する。
教訓を理解して現場に当てはめて活用し、個別の IT 障害を削減する。

以降では、図のなかの青枠で示された範囲（①と②）を中心に説明する。

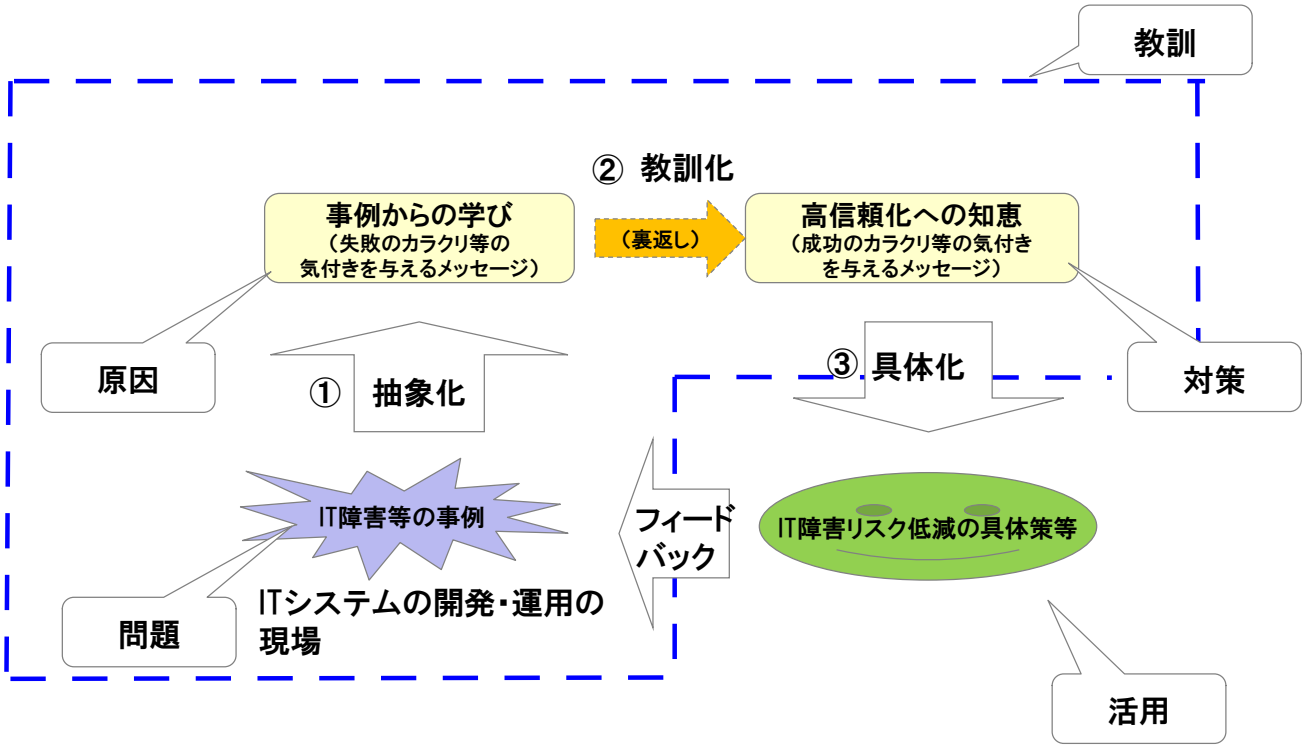


図２－１　障害と教訓の関係

教訓を作成する手順を詳細化すると、図２－２のようになる。以降では手順ごとに詳細を解説する。

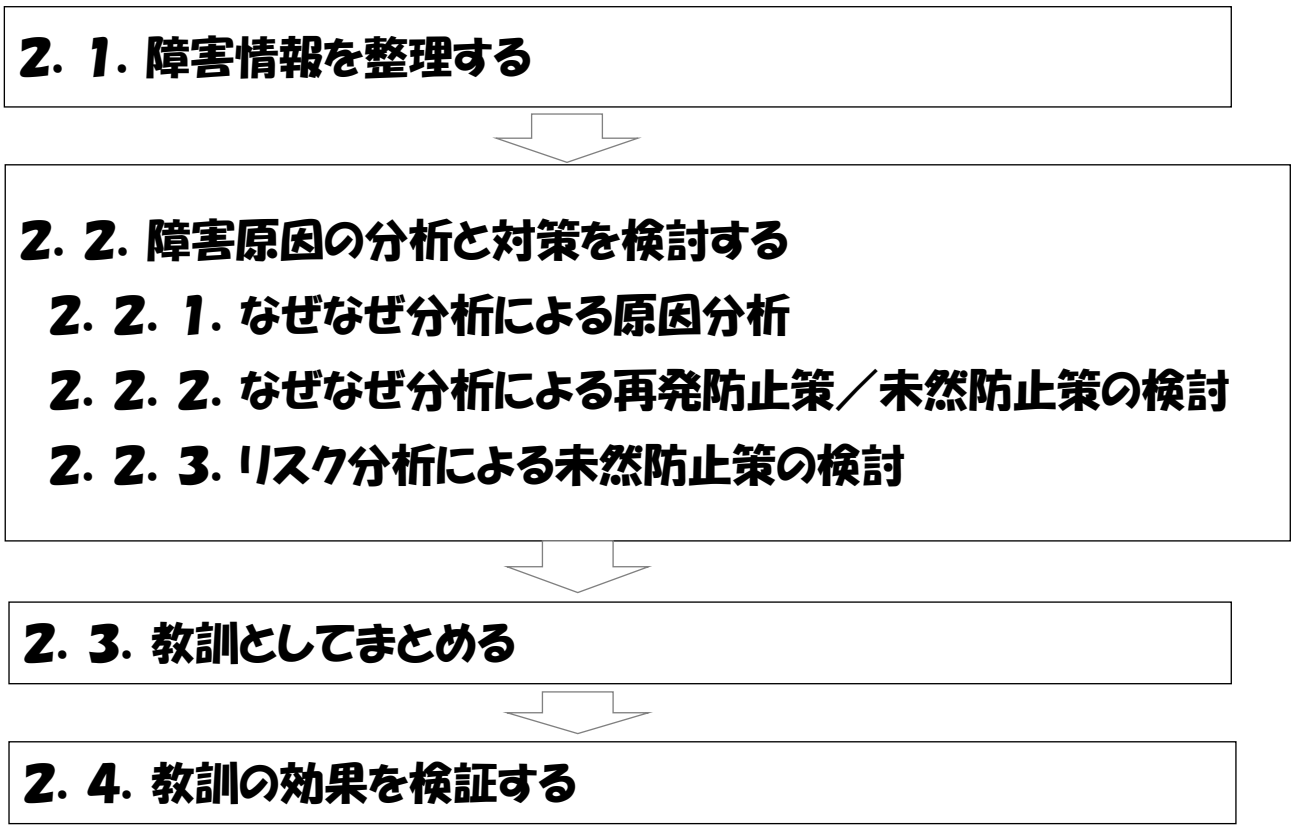


図２－２　教訓を作成する手順

なお、本書では、実際に起こった具体的な障害事例を用いて解説する。解説で使用する障害事例は別紙の参考資料に詳細を記述しているので参照されたい。

参考資料
参考１．教訓の作成例
参考１．１．障害事例
参考１．２．障害事例の状況の整理例
参考１．３．障害事例をなぜなぜ分析で検討した例
参考１．４．作成した教訓の例

２．１．障害情報を整理する

【インプット：障害情報データ、アウトプット：障害状況表】

まずは表２．１－１のように障害事例の情報を整理し、障害状況表を作成する。その際、以下に留意する。

- 障害情報を理解し時間経過の流れに沿って分類し、整理する。
- できるだけ図を作成し、発生時点の状況を把握する。
- 情報は以下のものを、もれがないように記述する。
  ①　登場人物
  ②　行動の流れと対象の物や情報
  ③　発生した事象の前後関係
- できるだけ多くの事実を集めて整理し、重要な事実や問題を抽出する。

この段階で原因や対策がすぐに判明する問題はここで完了し、次節以降の原因分析は実施しない。原因分析は、原因が複雑な問題や根が深い問題のときに必要となる。

表２．１－１　障害状況表のサンプル

【詳細は参考１．２．障害事例の状況の整理例を参照】

日時	顧客	A社		B社
		今回の障害が発生したサービスのユーザ		クラウドサービスを提供するベンダ
		業務窓口	情シス部門	
			負荷分散装置のファームウェアで行っているある処理（sodプロセス）にてメモリ不足エラー（out of memory）が発生した。	
朝4時			待機系がスタンバイからアクティブへ切り替わり、この段階で未だ稼動系がアクティブであったため、両系間で多数の電文が繰返し転送される現象（系間ループ形成によるマルチキャストストーム）が発生した	

２．２．障害原因の分析と対策を検討する

システム障害から原因を分析する手法は数多くある。例を表２．２－１に示す。

表２．２－１　主要原因分析手法一覧

番号	分類	名称	開発者開発機関	概要の説明
1	基本型	なぜなぜ分析	（品質管理手法）	事後に発生した問題の原因を分析する手法で広く使われている
2	過程関連型	ImSAFER（Improvement for medical System by Analyzing Fault root in human Error incident）	自治医科大学（河野龍太郎）	事後に発生したヒューマンエラー関連の分析で原因追求と対策立案を支援
3	過程関連型	RCA（Root Cause Analysis）	米国退役軍人省 患者安全センター	事後に発生した医療分野における問題の原因分析手法で、なぜなぜ分析を包含する
4	課題抽出型	ブレインストーミング	Alex Faickney Osborn	集団でアイデアを出し合うことによって相互交錯の連鎖反応や発想の誘発を期待する技法
5	リスク評価型	HAZOP（Hazard and Operability Studies）	イギリスの ICI 社（Imperial Chemical Industries）	事前のリスク分析手法（ボトムアップ型、FMEA と類似）
6	過程関連型	FTA（Fault Tree Analysis）	Bell Labs. 他	事前の故障の木解析手法でトップダウン型
7	リスク評価型	FMEA（FailureMode andEffects nalysis）	US.Army 他	事前のリスク分析手法（ボトムアップ型、HAZOP と類似）
8	発展型	STAMP	MIT	事故モデル（複雑なシステムの安全解析）
9	発展型	STPA（STAMP）	MIT	事前の STAMP に基づく安全解析（トップダウン型）
10	発展型	CAST（STAMP）	MIT	事後に発生した問題の STAMP に基づく事故分析（ボトムアップ型）

以降では例として、IT サービス分野で最もよく使われている「なぜなぜ分析」や「ブレインストーミングを使用したリスク分析」を使用して障害原因を分析し、対策を検討する方法を解説する。

手順の概要を図２．２－２に示す。

この例では、システム障害として顕在化した事象の原因を「なぜなぜ分析」で分析し、システムが潜在的に持つリスク（システムリスク）を「ブレインストーミングを利用したリスク分析」で分析することで、起こった障害の再発防止だけでなく関連する障害の未然防止も実現できる。

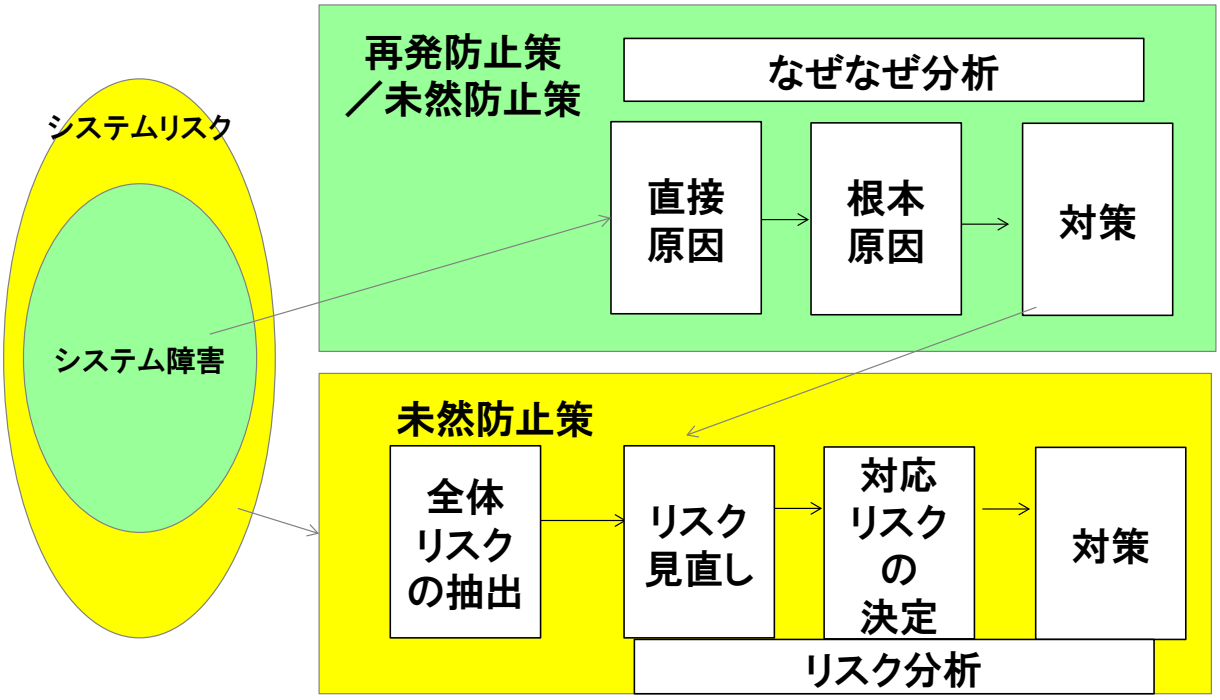


図２．２－２　なぜなぜ分析とリスク分析

システムリスクとは、発生、顕在化したシステム障害を含めて、IT サービスがビジネス要求に対応できず、業務遂行に支障をきたす要因全般をいう。

再発防止対策（ISO でいうところの是正処置）はシステム障害が発生した後に、その根本原因を明らかにして、実施する対策のことである。

未然防止対策は（ISO でいうところの予防処置）まだ障害としては発生していないが対応が必要な要因への対策や、社会環境の変化や法改正などに向けた対策である。

以降では、「なぜなぜ分析による原因分析」、「なぜなぜ分析による再発防止策／未然防止策の検討」、「ブレインストーミングを使用したリスク分析による未然防止策の検討」の順に説明する。

２．２．１．なぜなぜ分析による原因分析

【インプット：分析対象の問題事象、アウトプット：根本原因】

なぜなぜ分析は、障害状況表等によって抽出した問題事象からその事象の根本原因まで、「なぜ」と問いながら遡っていく分析手法である。

分析を実施するにあたってのポイントは以下の２点である。

① 問題事象を引き起こした直接の原因（直接原因）を見つけ、さらに直接原因を引き起こした原因を見つけるという手順をくり返し、本質的な原因（根本原因）を見つけ出す。

② 障害事例の当事者（障害を引き起こした人等）がいる場合には、徹底的に「何故」を追求し、障害事例の当事者がいない場合は、あらゆる想定（想像力）をもとに深掘りしていく。

以下の図２．２．１－１になぜなぜ分析の例を示す。

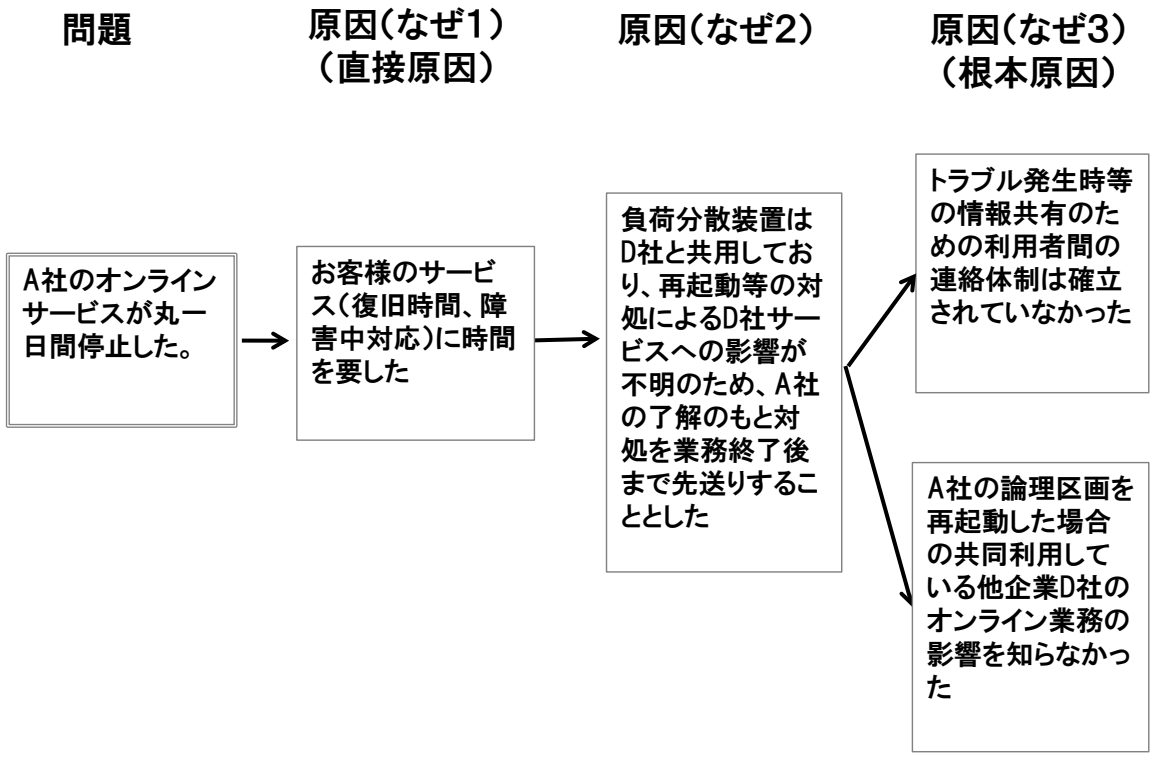


図２．２．１－１　障害事例（なぜなぜ分析の例（原因分析））

【参考１．３．障害事例をなぜなぜ分析で検討した例　の一部】

２．２．２．なぜなぜ分析による再発防止策／未然防止策の検討

【インプット：直接原因／根本原因、アウトプット：再発防止策／未然防止策】

なぜなぜ分析から再発防止策と未然防止策を導く手順を以下の図２．２．２－１に示す。対策を検討するにあたってのポイントは以下の２点である。

① 直接原因→反転→再発防止策　を検討する。
（障害対策としてすでに実施されている場合が多いが、再発防止策としては挙げておく）

② 根本原因→反転→再発防止策、未然防止策　を洗い出す。

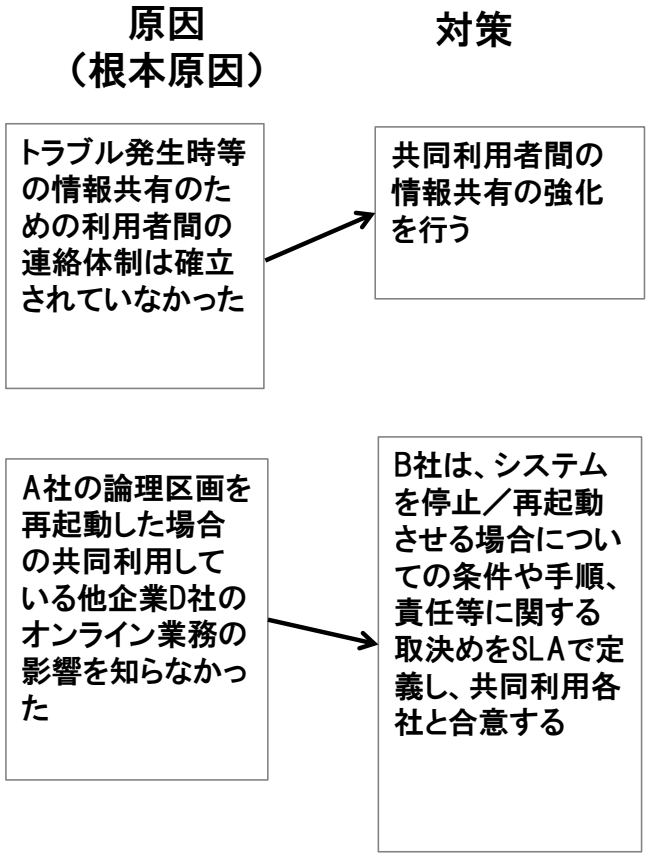


図２．２．２－１　障害事例（なぜなぜ分析の例（原因分析と対策））

【参考１．３．障害事例をなぜなぜ分析で検討した例　の一部】

２．２．３．ブレインストーミングを使用したリスク分析による未然防止策の検討

【インプット：リスク候補／再発防止策、アウトプット：確定リスク／未然防止策】

リスクを分析する目的は、発生したものと同一のシステム障害の再発防止だけではなく、将来発生するかもしれない類似の障害や関連する障害を推測し、発生確率や影響度を分析し、コストも考慮した適切な対応をとることである。

リスク分析の際はまず、ブレインストーミングを使用してリスクの候補を抽出し、表２．２．３－１のようなリスク管理表に整理する。

リスク候補を抽出するキーワードとしては、以下のようなものがある。

- 一定の時間の経過後や遠隔地で起こる可能性があるもの。
- 別の視点で見た時に起こる可能性があるもの。
- 現時点で見えていないが、起こる可能性があるもの。
- BCP（事業の継続）に関するもの。
- 業務の間や人間同士の間のインタフェースに関するもの。
- 情報資産のインタフェースに関するもの。

リスク管理表にあげたリスクの中から影響内容、発生度などをもとに対応するリスク（確定リスク）を決め、それに対する想定対応方法のなかから未然防止策を決定する。

表２．２．３－１　リスク管理表の例

No.	カテゴリー	リスク内容	影響内容	A:影響度（高:3～低:1）	B:発生度（高:3～低:1）	C:リスク値（A×B）	発生判定基準（5以上）	想定対応方法
1	サービス継続・可用性	障害発生時の事業継続/顧客サービスに対応できなくなる	顧客へのサービス提供の停止	3	1	3	3	業務部門と情シス部門が協力してシステムの障害の規模に合わせた手作業による事務処理マニュアルの作成を行う。マニュアルに沿った訓練を定期的に実施する

２．３．教訓としてまとめる

【インプット：分析結果（問題、原因、対策（再発防止策、未然防止策））、アウトプット：教訓】

今までの結果をもとに、各項目（問題、原因、対策、効果）に整理して図２．３－１のように教訓化する。

教訓としてまとめるときのポイントを以下に示す。

- 教訓には管理・参照のための ID をつけておく。
- 教訓概要は簡潔にし、言いたいことを端的に表現する。（教訓概要で全てがわかる必要はなく、目を引き、覚えやすい文言であれば良い）
- 教訓化に当っては、固有名詞は匿名化する。
  教訓を共有する企業や組織の範囲にあわせて、内容を他の分野の障害の例に置き換える。
- 「問題」と「原因」は、明確に分ける。
- 「原因」は、「直接原因」「根本原因」が明確にわかるようにする。
- 「直接原因」は、障害事象の第一次的なものとする。
- 「根本原因」は、「直接原因」の背後にある要因を深堀りしたものである。
- 障害事例の整理、教訓の概要の検討、教訓の詳細の検討と段階を分けて進める。
- 直接原因から根本原因へと、障害の背景を深堀りする。
- 教訓概要は忘れない言葉（キャッチコピー）にする。
- 教訓概要は短く、ストレートな表現にする。
- 教訓概要は否定形でなく、肯定形にする。

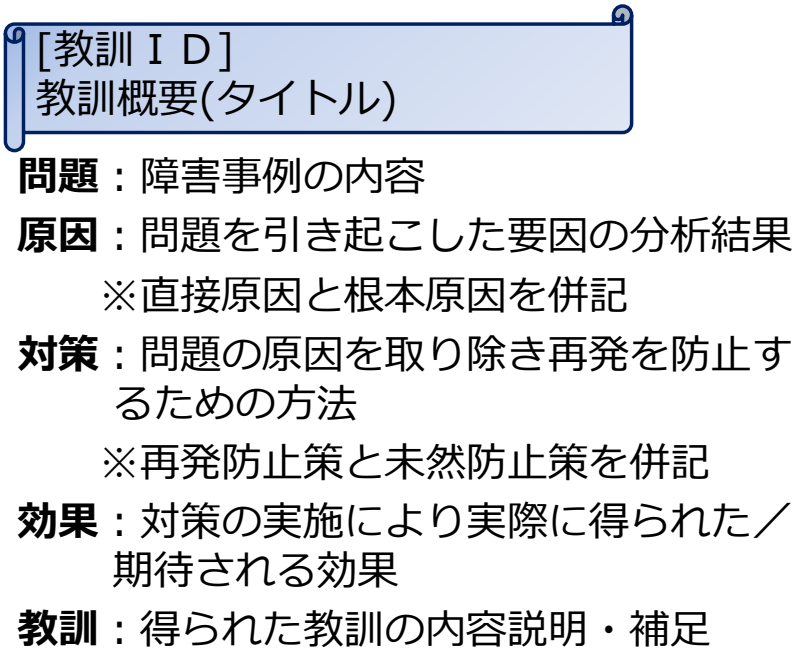


図２．３－１　障害事例（教訓のまとめ方の書式例）

【具体例は参考１．４．作成した教訓の例　を参照】

２．４．教訓の効果を検証する

【インプット：障害の統計情報、アウトプット：教訓の検証結果】

教訓毎の効果は前述したが、ここでは、統計的な手法などを用いて、実際に起こった類似の障害事例を定量的に分析し、作成した教訓を実際に起こっている障害と対応付けて、効果があるかを検証する。　まずは、発生した障害を対外影響や、障害の影響額、対応にかかる工数（対応工数）などの統計情報も含めて、表２．４－１のような一覧表にまとめる。

表２．４－１　障害一覧（対外影響など、障害の影響額、対応工数）

障害の概要	主な原因	対外影響など	障害の影響額	対応工数
オンラインのA処理が停止	開発ソフトウェアのバグ	エンドユーザ端末XX台が1時間サービス停止	XX万円	NNN人月
夜間バッチ処理のトラブルで翌日オンラインが開始できず	運用オペレーションにおけるミス	朝9時のオンライン開始が遅延	YY万円	MMM人月

次に原因別に障害件数を集計し（図２．４－１に示す障害の原因別グラフの例を参照）、全障害件数に占める割合が大きい原因を、パレート図を用いて ABC 分析するなどして抽出し、それらの原因別の障害を教訓の活用により削減できるか検証する。

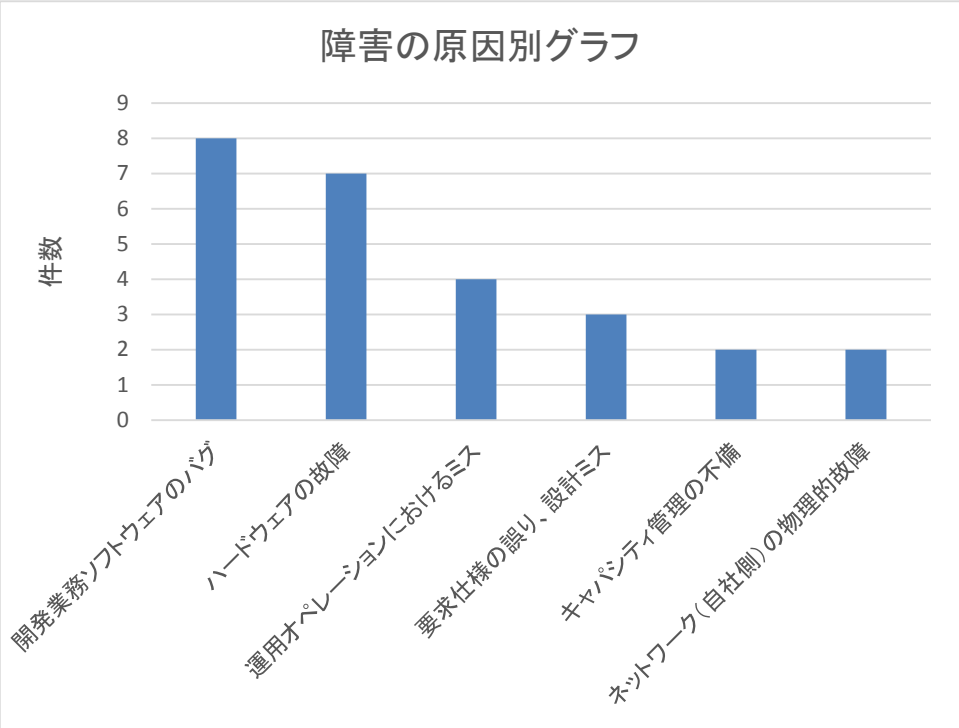


図２．４－１　障害の原因別グラフ

３．教訓を分類する

作成した教訓を活用するためには、利用者が利用目的に合ったものを見つけやすいように様々な観点から分類する必要がある。

本章では教訓を分類するための考え方を記述する。

利用者にわかりやすいように以下の①～⑤に挙げるような方法で教訓をカテゴリごとに分類し、図３－１のように、検索・分類キーをつける。

分類方法としては、以下が挙げられる。

① 教訓を活用する目的
② 情報処理システムの重要度
③ ソフトウェアライフサイクルのプロセス
④ 運用・サービスのプロセス
⑤ キーワード

なお、ここに挙げたすべての分類が必要なわけではない。以降の３．１～３．５で各分類方法の具体例を挙げるので分類方法を選ぶ際の参考とされたい。

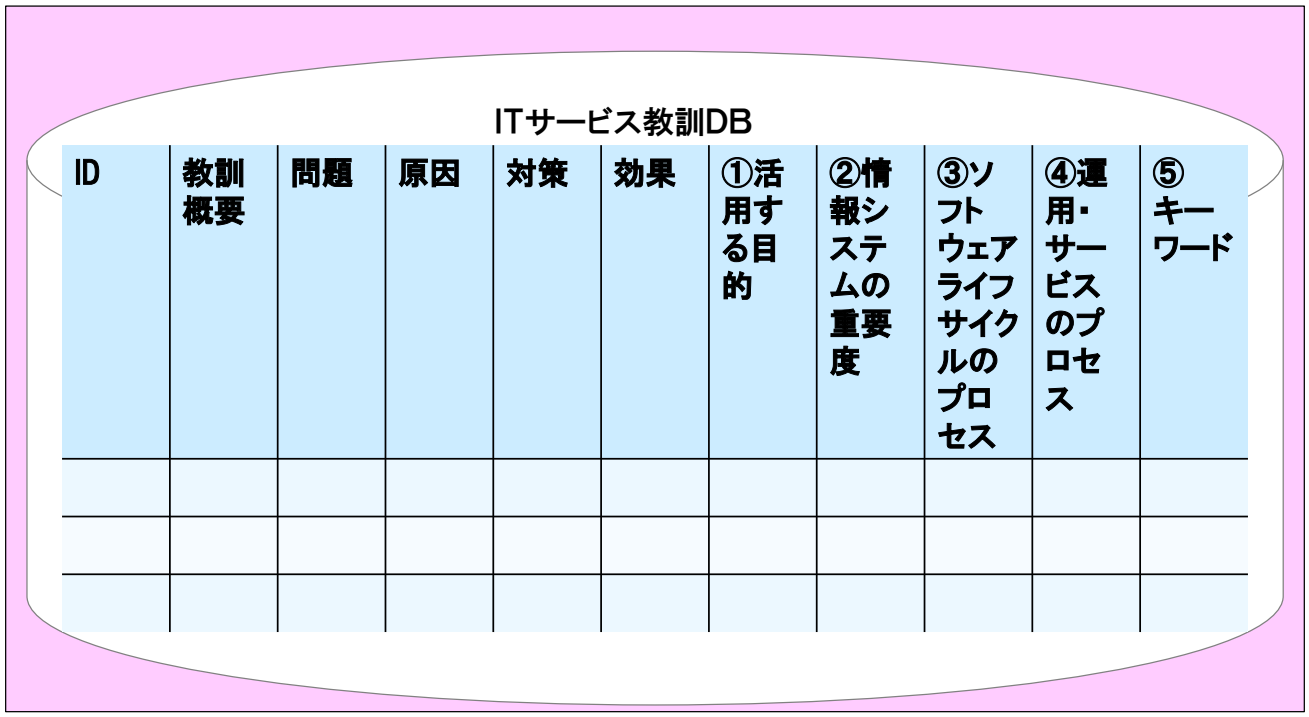


図３－１　教訓を分類する

３．１．活用する目的による分類

以下の表３．１－１のように、教訓を活用する目的で分類する。どの目的に対応している教訓かは、各教訓の特性で判断するが、目的の区分や分類の際の考え方の例としては以下のようなものがある。

- 「組織・体制の整備」の区分には、組織・体制やプロセスの改善に効果がある教訓を入れる。
- 「運用手順の整備」の区分には、運用部門の課題解決に効果がある教訓を入れる。
- 「開発手順の整備」の区分には、開発時の要件漏れや設計時に障害の予防・対策に効果がある教訓を入れる。
- 「調達時の指示・確認」の区分には、調達時のベンダ、ユーザ双方の合意事項に関する教訓を入れる。
- 「レビュー・試験項目の検討」の区分には、レビュー・試験項目のもれや体制などに関する教訓を入れる。
- 「障害の根本原因の対策」の区分には、障害の背後にある原因を分析し、根本的な対策を行う教訓を入れる。
- 「社内教育」の区分には、若手などへの社内教育で活用できる教訓を入れる。

なお、分類の詳細は「教訓活用ガイドブック」を参照されたい。

表３．１－１　教訓を活用する目的による分類

活用する目的	教訓1	教訓2	教訓3			教訓15	教訓16	教訓17	教訓18
組織･体制の整備	●								
運用手順の整備			●						
開発手順の整備									
調達時の指示･確認		●							
ﾚﾋﾞｭｰ･試験項目の検討						●			
障害の根本原因の対策							●		
社内教育								●	●

３．２．情報処理システムの重要度による分類

多くの企業では情報処理システムのプロファイルを持っているが、IPA/SEC では、「平成 20 年度重要インフラシステム信頼性研究会」において、表３．２－１のように情報処理システムのプロファイルを重要性の低いものからそれぞれ TypeⅠ、TypeⅡ、TypeⅢ、TypeⅣと設定した（詳細は文献３－１を参照）。これを利用して、教訓作成の元となった情報処理システムの特性／環境で教訓を分類し、教訓が他のシステムに活用できるかを判断できるようにする。

これにより、ある教訓を適用したい時に、適用する自分のシステムの信頼性や性能、投資可能な費用とその教訓が対象とするシステムのレベルが合っているかが把握できるようになる。

表３．２－１　情報処理システムプロファイル

	Type Ⅰ	Type Ⅱ	Type Ⅲ	Type Ⅳ
システムの区分	その他のシステム		企業基幹システム	重要インフラ等システム
人命に影響を与える可能性	ほとんど無し	軽微	重大災害	死亡事故
障害金額の予測	1,000 万円以下	1 億円以下	10億円以下	10億円以上
社会的影響	ほとんど無し	軽微	多くの人に迷惑を掛ける、あるいは特定の個人に大きな心理的影響を与える。	重大な影響を社会に与える。

表３．２－１のシステムの区分は、それぞれ以下のように定義している。

- 重要インフラ等システム：他に代替することが著しく困難なサービスを提供する国民生活・社会経済活動の基盤となるシステム
- 企業基幹システム　　：企業活動の基盤であり、その機能が低下又は利用不可能な状態に陥った場合に、当該企業活動に多大の影響を及ぼすおそれが生じるとともに、相当程度の外部利用者にも影響を及ぼすシステム
- その他のシステム　　：上記２区分以外のシステム

３．３．ソフトウェアライフサイクルのプロセスによる分類

その教訓で示された対策をどのプロセスで実行すればよいかがわかるように分類する。

一例として、IPA/SEC が発行している共通フレーム（文献３－２）において定義されたプロセスに基づいて分類する。（プロセスは図３．３－１を参照。分類例は図３．３－２を参照）

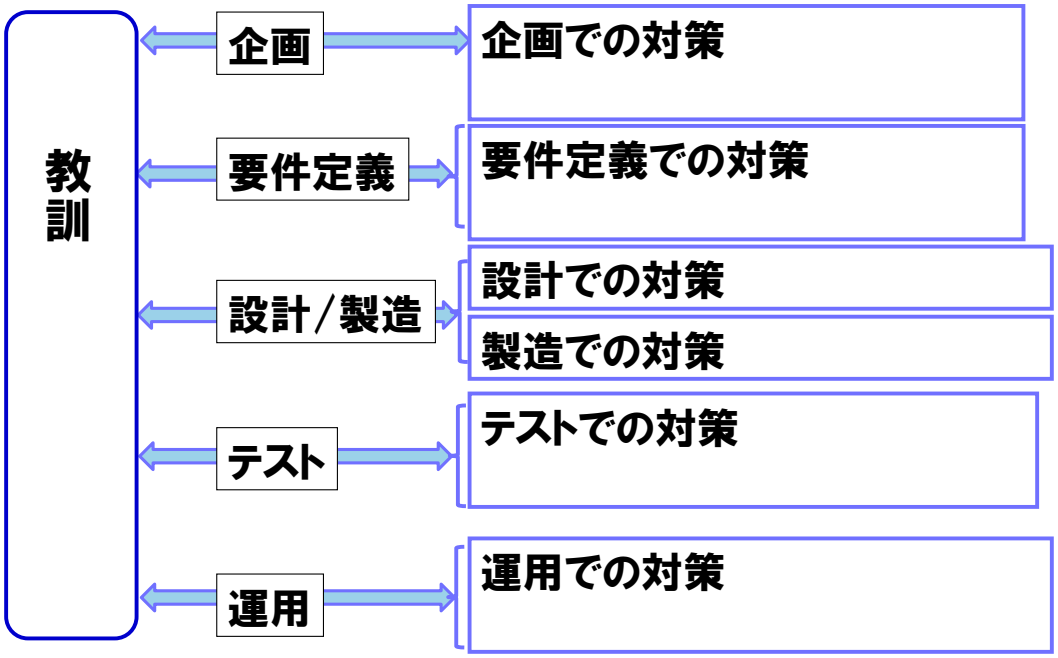


図３．３－１　共通フレームのプロセスに基づいた分類

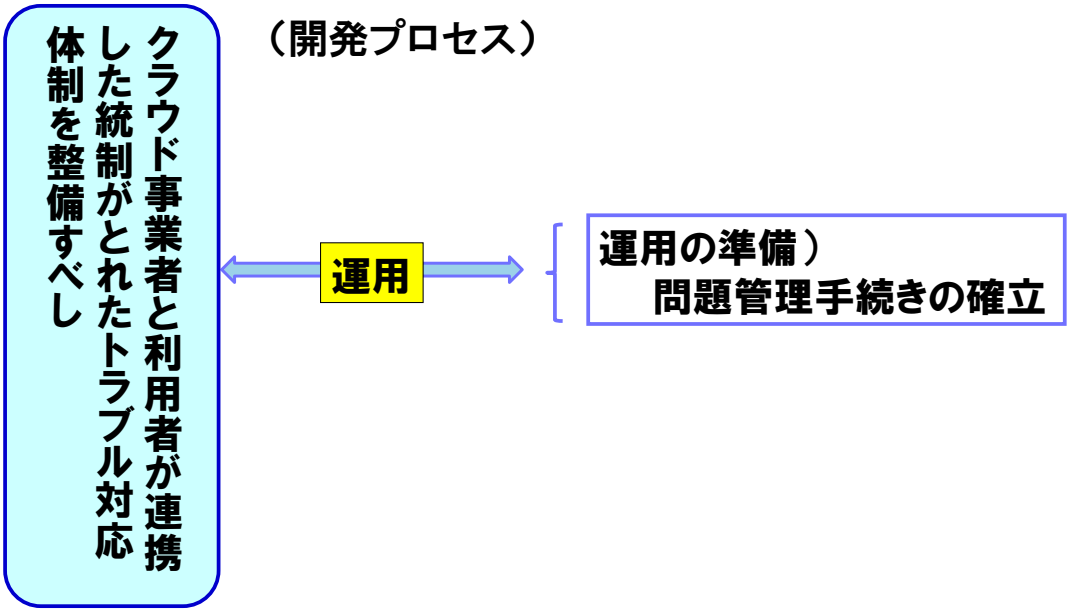


図３．３－２　共通フレームのプロセスに基づいた分類例

３．４．運用・サービスのプロセスによる分類

その教訓で示された対策を運用･サービスにおけるどのプロセスで実行すればよいかがわかるように教訓を分類する。

一例として、ITIL[2]で定義された運用・サービスのプロセスに基づいて分類する（プロセスは図３．４－１を参照。分類例は図３．４－２を参照。プロセス定義の詳細は文献３－３を参照）

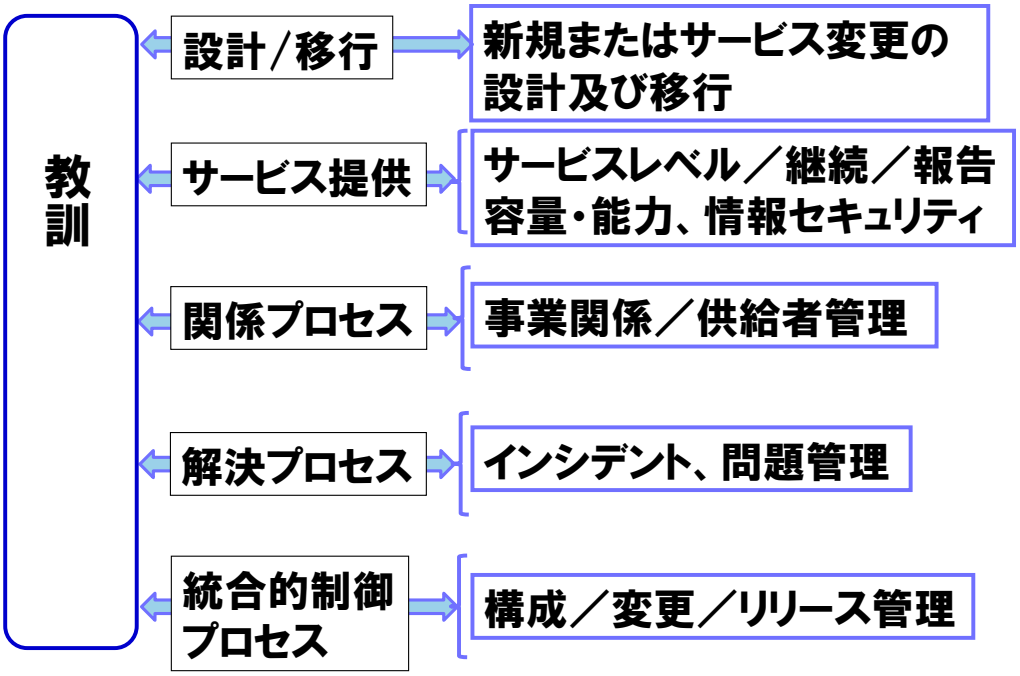


図３．４－１　運用・サービス（ITIL）のプロセスに基づいた分類

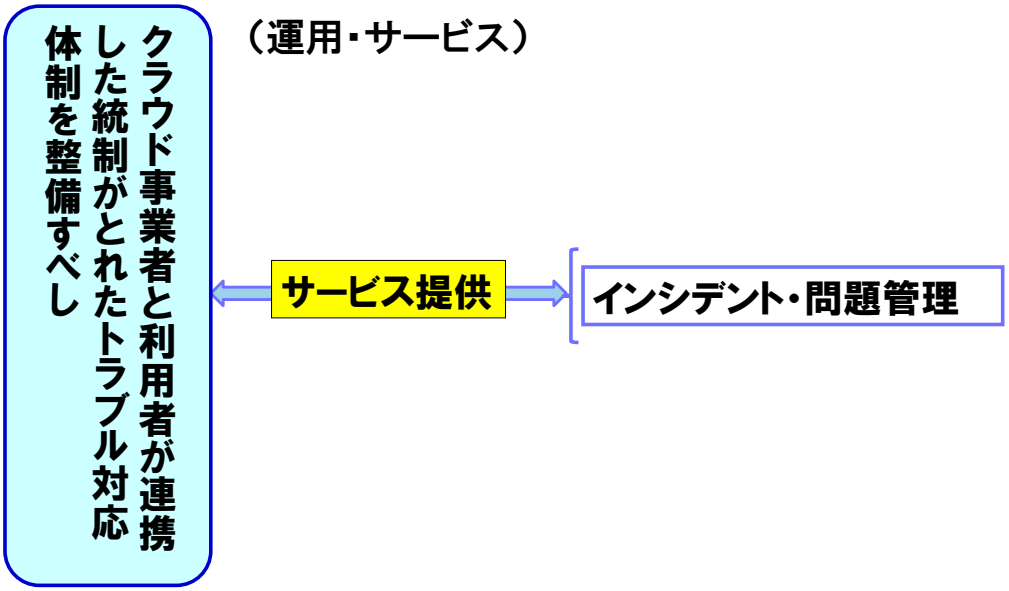


図３．４－２　運用・サービス（ITIL）のプロセスに基づいた分類例

[2] ITIL（Information Technology Infrastructure Library）：IT サービスマネジメントにおける成功事例をまとめた書籍群で、国際規格である ISO/IEC 20000（文献３－３）の元となっている。

３．５．キーワードによる分類

キーワードによって教訓を検索する場合のために、教訓の特性を示すキーワードを抽出する。例えば、以下の様なものが挙げられる。

仮想化、共同利用、トラブル管理、パッチの適用、システム再起動

キーワードの抽出に当たっては、教訓の特徴を表す言葉で、IT 用語集などに使用されている一般的なものを設定すると良い。

３．６．教訓を分類した例

ここまでに説明してきた教訓の分類方法を、別紙の参考資料の障害事例に当てはめて分類した結果を図３．６－１に示す。

教訓ID: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

項番	分類カテゴリ	分類結果
3.1	活用する目的	組織・体制の整備
3.2	情報システムの重要度	企業基幹システム（多数の利用者に影響あり）
3.3	ソフトウェアライフサイクルのプロセス	運用プロセスでの対策
3.4	運用・サービスのプロセス	サービス提供プロセスでの対策
3.5	キーワード	仮想化、共同利用、トラブル管理、パッチの適用、システム再起動

図３．６－１　教訓を分類した例

４．教訓作成のための組織／体制

ここまでは、主に技術的な面から見た教訓作成について述べてきたが、本章では教訓を作成するための組織体制やマネジメント方法について述べる。

教訓は、「現場の組織」が自ら問題を整理し、「教訓として共有」できる形に作り上げることで「現場に役立つ」ものとなる。これが可能となるように、経営者を含めた企業全体や、各組織で支援することが重要である。

教訓作成の体制は、企業が元々持つ組織や品質管理の方針に合わせて考えるべきである。例えば、ある企業では、図４－１のように、情報システム管理部門が障害を分析して教訓化している。図４－１の体制はあくまで一つの例であるが、可能であれば、教訓作成／活用のメンバには、関係する部門からもれなく参加し、部門外の第三者（有識者や分野の専門家等）も参加すべきである。

また、教訓作成／活用の際には関係者全員が顔を合わせて議論できるような環境が必要であるが、障害や教訓の数が多くなってくると作業の効率化が必要となってくる。そのためには、教訓の共有のための手順や、教訓を情報共有する SNS やデータベースなどのツールを整備するといった方法が挙げられる。

また、経営層が主導することにより、教訓を共有することが良いこととされ、これを評価するような企業・組織の文化や風土を作ることも重要である。

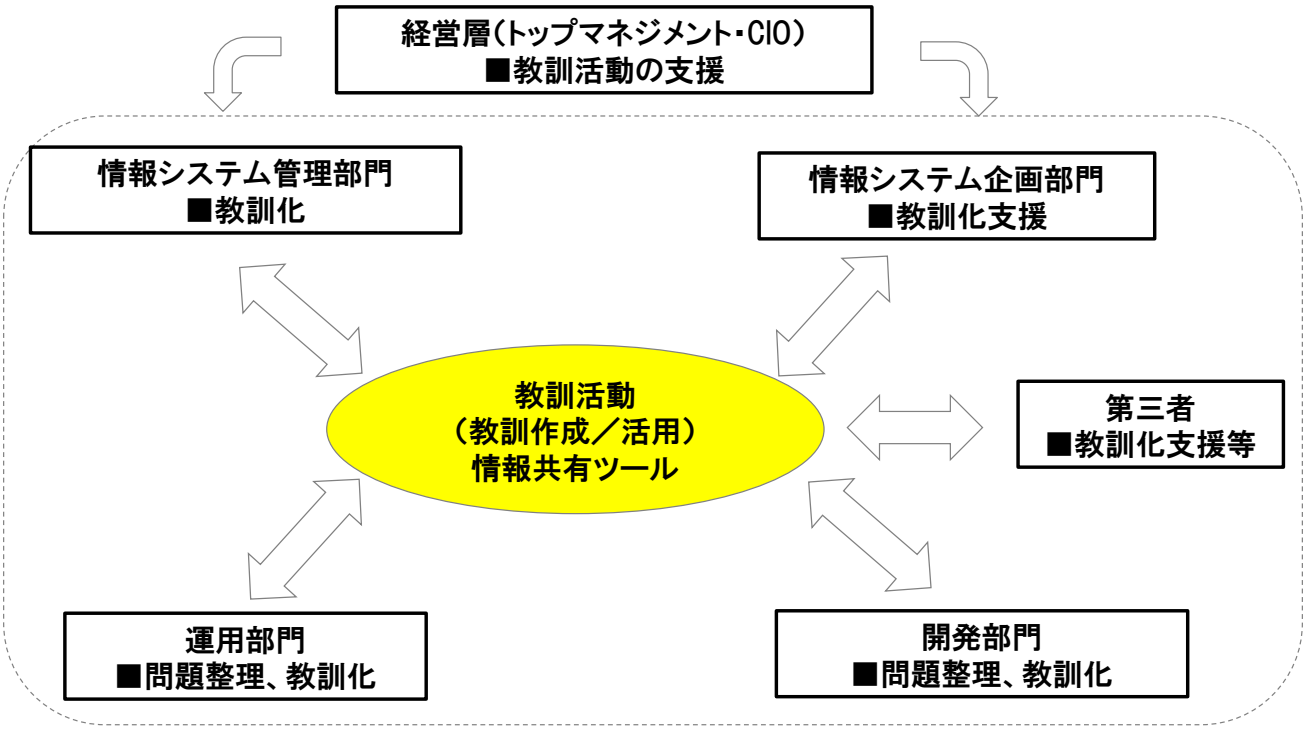


図４－１　教訓作成のための組織／体制の例

５．おわりに

教訓はただ作成するのではなく、これが使ってもらえることを意識して作成することが大切である。従来から情報処理システム障害の教訓を作成する取り組みは数多くあったが、作成してもなかなか活用されないことが多かった。これは、いくら手順書などで詳細な説明をしても、教訓の作成者が実地でくり返し教訓の作成・活用を実行して習熟し、使ってもらうための活用者の視点を持って教訓を作成しないと役立つものにはならないのが一つの理由だと考える。そのため本書ではここまで、教訓とはどんなものかの説明と教訓の作成方法（２．教訓を作成する）、利用者にわかりやすいように教訓を分類する方法（３．教訓を分類する）、教訓を作るための組織体制やマネジメント方法（４．教訓作成のための組織／体制）を述べ、活用段階も踏まえた教訓の作成方法を解説してきた。

さらに教訓の活用について理解を深めるため、本書と併せて「教訓活用ガイドブック」をお読みいただくことをおすすめする。

これら２編のガイドブックが普及することにより、今後も情報処理システムが安全に開発、運用されていくことを期待したい。

参考資料

参考１．教訓の作成例

以下に障害事例を元に実際に教訓を作成した事例を示す。

参考１．１.は実際の障害事例の概要（システム概要、障害の概要、発生した事象）を示した。

これをもとに時系列に登場人物をのせて障害の状況を整理したのが参考１．２．である。この中から問題としてA社のオンラインサービスが丸一日間停止したことをピックアップして、参考１．３．でなぜなぜ分析を実施し、根本原因７つに対して対策方法を検討した。これら対策方法のうち１つを基にして作成したのが参考１．４．の作成した教訓の例である。IPA/SECでは参考１．３．のなぜなぜ分析から参考１．４のものを含めて７つの教訓を作成・公開しており、参考１．３ではそれぞれ公開済みの教訓ID[3]との対応を記載した。

参考１．１．障害事例

参考１．１．１．システム概要

A 社はオンラインによる情報登録および情報照会の基幹業務システムを当初はオンプレミスで運用していたが、運用コストの削減を目的に複数企業間の共同利用を進める方針となり、B社が提供するクラウドサービスに移行した。同時期に共同利用に移行するのは他に D 社があり、類似のビジネスを行っていた。B社が提供するシステムは、業務システム用のサーバと負荷分散装置に分かれている。業務システムのサーバだけでなく、負荷分散装置も仮想化されており、それらの論理区画のうち一つをＡ社は利用していた。（図　参考１．１－１．システムと障害の概要）

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

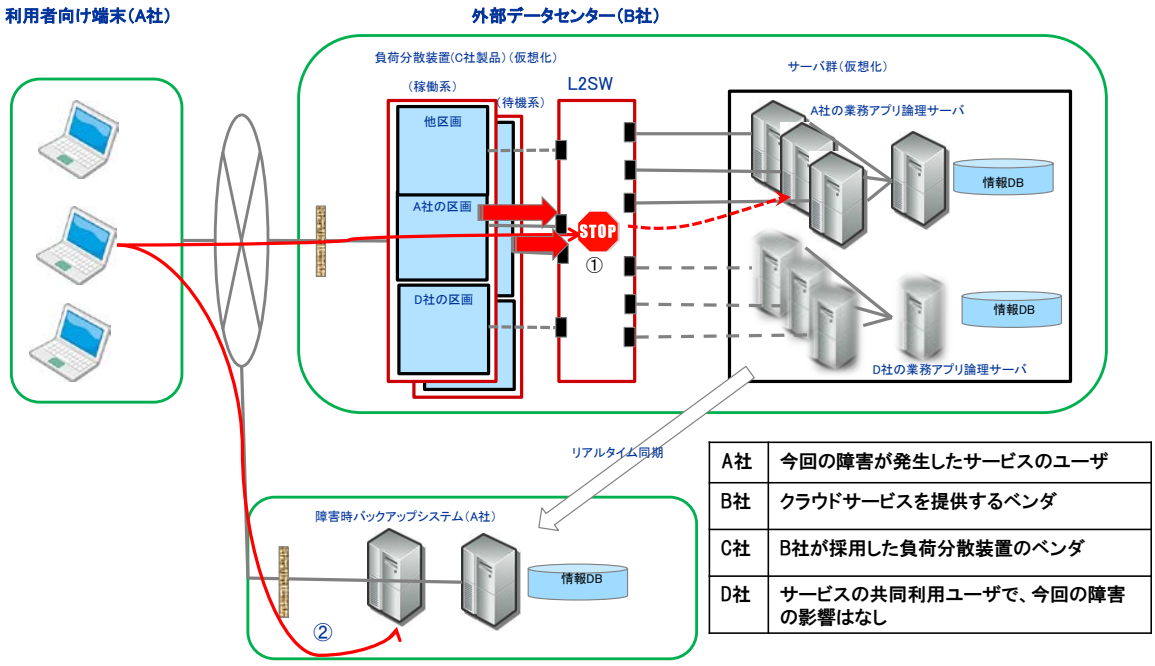
D社：サービスの共同利用ユーザで、今回の障害の影響はなし

参考１．１．２．障害の概要

ある日、オンライン開始時からこのシステムに障害が発生して丸１日業務が停止した。基幹オンラインシステムが端末から起動できず、すべての窓口でデータベースの更新を伴う処理の受付けができなかった（①）。

なお、A社があらかじめ用意していたクラウド外の「障害時バックアップシステム」に切り替わり、データ照会処理はできたので、その日はデータの更新を伴わないサービスのみを実施した（②）。

[3] 情報処理システム高信頼化教訓のリンク集（ITサービス編）　http://www.ipa.go.jp/sec/system/lesson.html



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　参考１．１－１．システムと障害の概要

参考１．１．３．障害の詳細説明

午前４：００

- 負荷分散装置のファームウェアで行っているある処理（sod プロセス）にてメモリ不足エラー（out of memory）が発生した。待機系がスタンバイからアクティブへ切り替わり、この段階で未だ稼動系がアクティブであったため、両系間で多数の電文が繰返し転送される現象（系間ループ形成によるマルチキャストストーム）が発生した（図　参考１．１－２）
- Ｌ２スイッチのポートが閉塞した
- sod プロセスが再起動された
- 稼動系がスタンバイへ切り替わった
- 系切替え（フェールオーバ）動作が完了し、待機系に切り替わったが、待機系自体が out of memory に近い状態であったため、極端なレスポンス悪化が発生した。
- 通信路の疎通状況を確認する ping が通ったことから、B 社はシステムの運用に問題ないと誤認した。

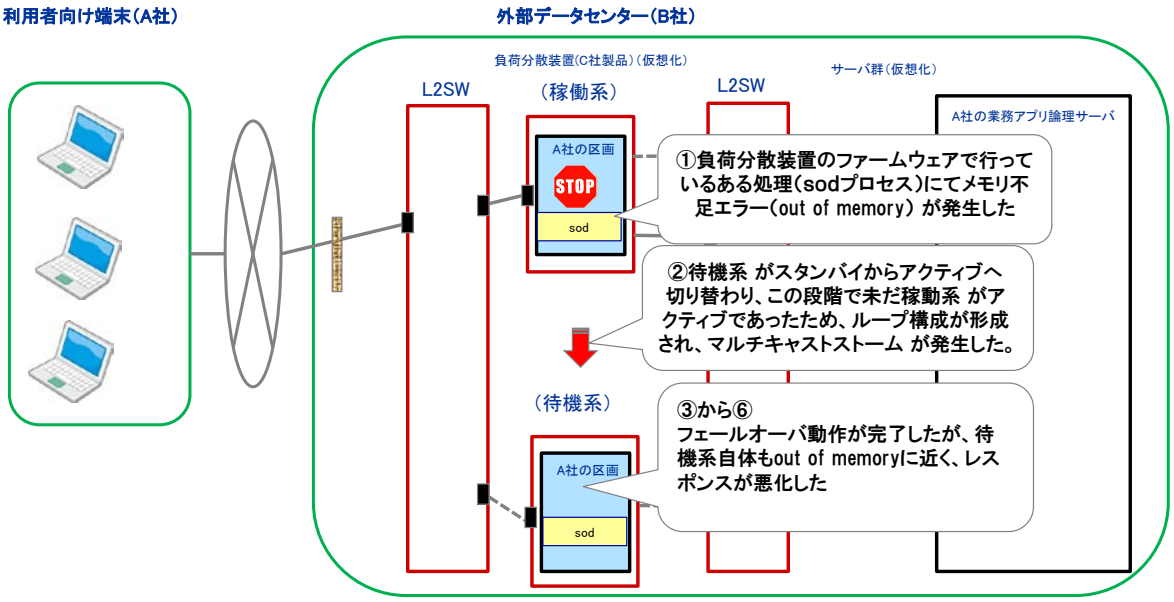


図　参考１．１－２　障害の詳細説明

８：００

- A 社の運用オペレータから情シス部門と B 社の SE に基幹システムのオンラインが起動できない旨の第一報が入った。B 社の SE は基幹システム端末機からオンラインが起動できないことを確認し、障害原因の特定・復旧作業に入った。

８：３０

- A 社の情シス部門は、業務ポータルに障害情報を掲載し、ダウン時対応システムの起動を周知した。

１０：３０

- A 社の情シス部門は、障害原因の特定が出来ず、復旧に時間を要すると判断し、ホームページと SNS に障害情報を掲載した。

１１：００

- B 社は初めのうちは AP サーバや専用線の問題と誤認し調査を行い、B 社の自社製品ではない C 社製負荷分散装置の障害調査は後回しにした。
- A 社は各方面への説明対応に追われた。
- この状況は D 社には全く伝えられていなかった。
- A 社の業務窓口は、登録系業務の処理の対応手順がわから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、窓口に来た顧客に帰って頂く対応となった。

１６：００

- A 社の情シスと B 社の SE は、障害発生箇所を通信関連機器（負荷分散装置）にほぼ特定したが、同日中の復旧が困難と判断し、ホームページと SNS に情報を掲載した。
- 負荷分散装置は D 社と共用しており、再起動等の対処による D 社サービスへの影響が不明のため、A 社の了解のもと対処を業務終了後まで先送りすることとした。

２０：００

- 障害の原因は C 社製負荷分散装置の sod プロセスのメモリ資源が時間とともに増加するという既知の不具合によるものであったことがわかった。
- 障害の原因を負荷分散装置と特定し、試みに A 社の仮想負荷分散装置を再起動したところ、障害が復旧した。

翌 AM１：３０

- 負荷分散装置のハードウェア構成全体の再起動を行い、正常稼動の確認が完了した。

８：００

- ホームページと SNS に障害復旧の情報を掲載した。

参考１．１．４．上記以外での特記事項

- B 社は、システム構成機器の修正情報の収集間隔を、３ヶ月に１回程度と非常に粗く設定していた。
- A 社のシステムでは、本稼動以来、負荷分散装置は 8 か月以上連続運転状態であり、一般的なネットワーク機器と同様に再起動をしたことがなかった。
- 今まで障害が発生したことが殆どなかったこともあり、システムが使えないと業務遂行はお手上げの状態であった。基幹業務システムが利用できない場合の事務マニュアルはなく、業務部門と情シス部門の対策検討もされていなかった。

参考１．２．障害事例の状況の整理例

参考１．１．の障害事例を時系列・部門別に整理したものを図　参考１．２―１に示す。

日時	顧客	A社		B社	C社	D社
		今回の障害が発生したサービスのユーザ		クラウドサービスを提供するベンダ	B社が採用した負荷分散装置のベンダ	サービスの共同利用ユーザで、今回の障害の影響はなし
		業務窓口	情シス部門			
			負荷分散装置のファームウェアで行っているある処理（sodプロセス）にてメモリ不足エラー（out of memory）が発生した。			
朝4時			待機系がスタンバイからアクティブへ切り替わり、この段階で未だ稼動系がアクティブであったため、両系間で多数の電文が繰返し転送される現象（系間ループ形成によるマルチキャストストーム）が発生した			
			L2スイッチのポートが閉塞した			
			sodプロセスが再起動された			
			稼動系がスタンバイへ切り替わった			
			系切替え（フェールオーバ）動作が完了し、待機系に切り替わったが、待機系自体がout of memoryに近い状態であったため、極端なレスポンス悪化が発生した			
朝8時		オンライン開始時からこのシステムに障害が発生してまる1日業務が停止した。基幹オンラインシステムが端末から起動できず、すべての窓口でデータベースの更新を伴う処理の受付けができなかった				
				B社は障害箇所の特定に時間を要した		
				通信路の疎通状況を確認するpingが通ったことから、B社はシステムの運用に問題ないと誤認した		
				初めのうちはAPサーバや専用線の問題と誤認し調査を行っていた。B社の自社製品ではないC社製負荷分散装置の障害調査は後回しにした		
					原因はC社製負荷分散装置のsodプロセスのメモリ資源が時間とともに増加するという既知の不具合によるものであったことがわかった	
		A社があらかじめ用意していたクラウド外の「障害時バックアップシステム」に切り替わり、データ照会処理はできたので、データの更新を伴わないサービスのみを実施した				
						状況はD社には全く伝えられていなかった
			A社は各方面への説明対応に追われた			
		業務窓口は、登録系業務の処理の対応手順がわからなかったため　顧客の登録・変更申請に対応できなかった。				
	結果として、窓口に来た顧客に帰って頂く対応となった					
16時			障害箇所が判明したのは16：00であった			
				負荷分散装置はD社と共用しており、再起動等の対処によるD社サービスへの影響が不明のため、A社の了解のもと対処を業務終了後まで先送りすることとした		
20時			午後8時頃に、障害の原因を負荷分散装置と特定し、試みにA社の仮想LBを再起動したところ、障害が復旧した。			
午前1時半			負荷分散装置のハードウェア構成全体の再起動を行い、正常稼動の確認が完了した。			
その他				B社は、システム構成機器の修正情報の収集間隔を、3ヶ月に1回程度と非常に粗く設定していた		
			A社のシステムでは、本稼動以来、負荷分散装置は8か月以上連続運転状態であり、一般的なネットワーク機器と同様に再起動をしたことがなかった			
			基幹業務システムが利用できない場合の事務マニュアルはなく、システムが使えないと業務遂行はお手上げの状態であった			

図　参考１．２－１　障害状況表

参考１．３．障害事例をなぜなぜ分析で検討した例

参考１．１．の障害事例をなぜなぜ分析で検討したものを図　参考１．３－１に示す。なお、図中の「対策」欄のうち、IPA/SEC から公開している教訓の作成に利用したものについては対応する教訓 ID を併記している他、参考１．４で紹介している教訓例に関係する項目を黄色で塗りつぶしている。

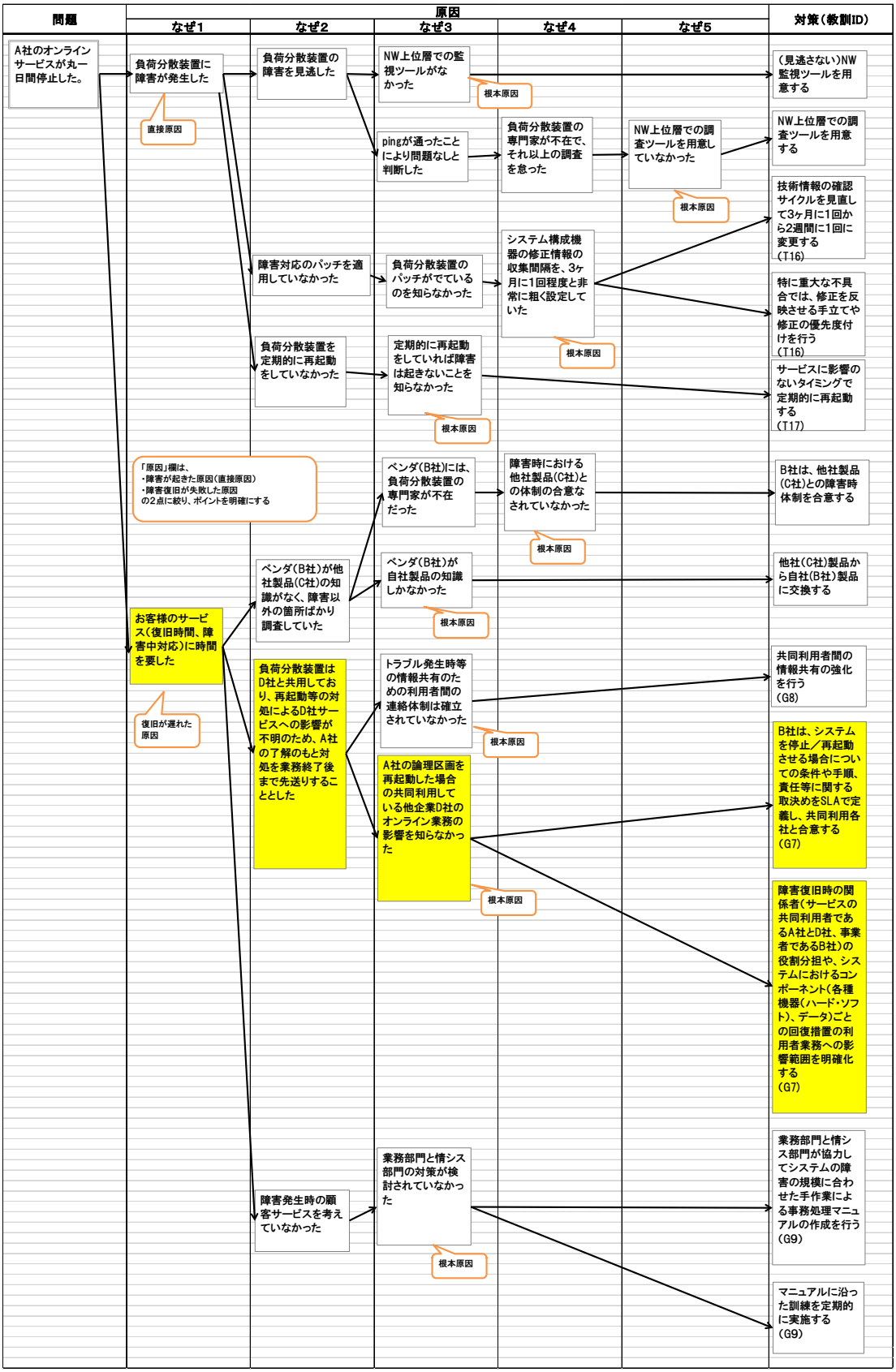


図　参考１．３－１　障害事例をなぜなぜ分析で検討した例

参考１．４．作成した教訓の例

[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

問題

A 社はオンラインによる情報登録及び情報照会の基幹業務システムを当初はオンプレミスで運用していたが、運用コストの削減を目的に複数企業間の共同利用を進める方針となり、B 社が提供するクラウドサービスに移行した。同時期に共同利用に移行するのは他に D 社があり、類似のビジネスを行っていた。B 社が提供するシステムは、業務システム用のサーバと負荷分散装置に分かれている。業務システムのサーバだけでなく、負荷分散装置も仮想化されており、その一つの論理区画を A 社は利用していた。(図　参考１．４－１システム概要)

ある日、オンライン開始時からこのシステムに障害が発生してまる１日業務が停止した。基幹オンラインシステムが端末から起動できず、すべての窓口でデータベースの更新を伴う処理の受付けができなかった（①)。

なお、A 社があらかじめ用意していたクラウド外の「障害時バックアップシステム」に切り替わり、データ照会処理はできたので、データの更新を伴わないサービスのみを実施した（②)。

B 社は障害箇所の特定に時間を要し、また A 社は各方面への説明対応に追われたこともあり、障害箇所が判明したのは１６：００であった。すでに業務終了時間が近づいていたためオンラインは終日停止、障害復旧作業はその後実施となった。

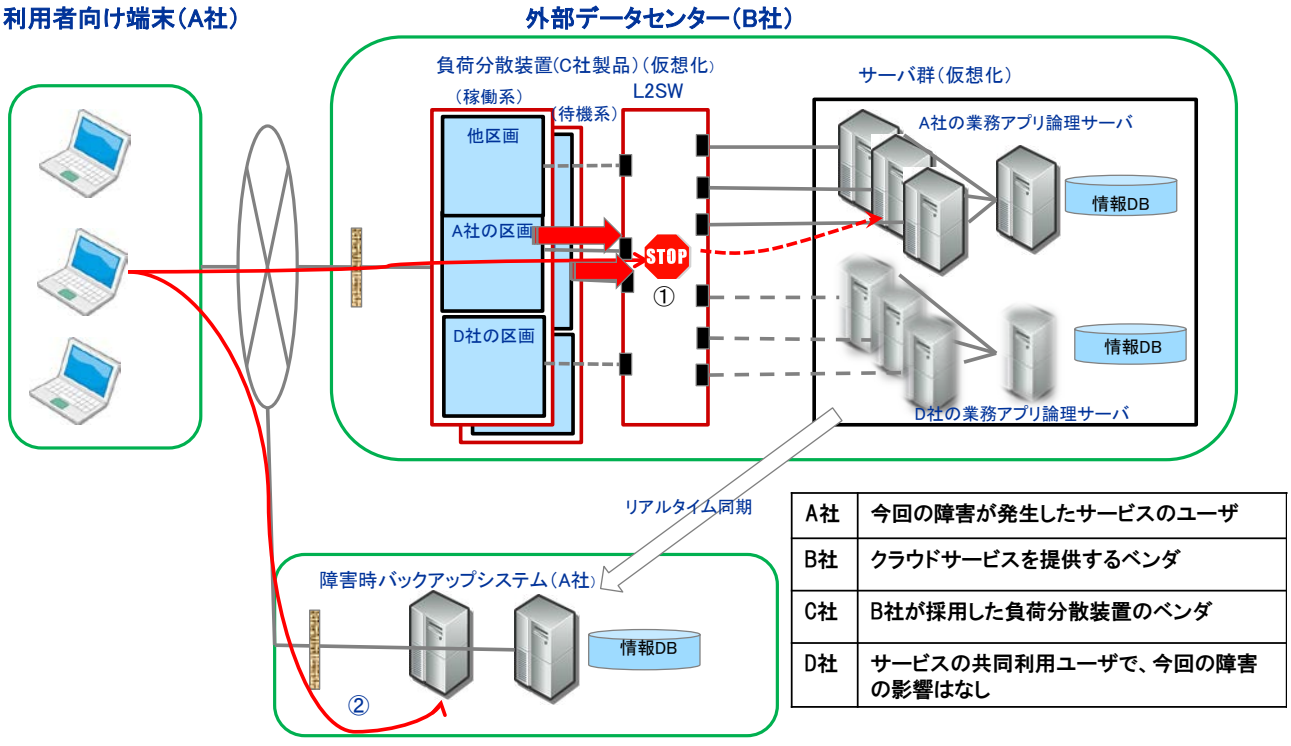


図　参考１．４－１システム概要

原因

直接の原因は、C 社製負荷分散装置の sod プロセスのメモリ資源が時間とともに増加するという既知の不具合であった。

単なる負荷分散装置の障害にも関わらず、その解決と業務の再開に多大の時間を要し丸一日間オンラインサービスが停止することとなった原因は、以下のとおりである。

- 通信路の疎通状況を確認する ping が通ったことから、B 社はシステムの運用に問題ないと誤認した。
- 初めのうちは AP サーバや専用線の問題と誤認し調査を行っていた。B 社の自社製品ではない C 社製負荷分散装置の障害調査は後回しにした。
- 負荷分散装置は D 社と共用しており、再起動等の対処による D 社サービスへの影響が不明のため、A 社の了解のもと対処を業務終了後まで先送りすることとした。

根本原因は以下のとおりである。

1．運用時のトラブル管理体制が決まっていなかった。
　障害調査を進め、一体となって協力して進めていく体制ができていなかった。B 社の SE は A 社に常駐していたが、トラブル管理体制が明確化されていないので、報告、連絡、相談がうまく回らなかった。
2．A 社は B 社と役割分担やサービスレベルが不明確な運用委託契約のままサービスを開始していた。
3．B 社に C 社製負荷分散装置の専門家が不在で、社外の製品のため障害情報の入手もしづらく、障害やパッチの情報をタイムリーに入手していなかった。

対策

再発防止策は以下のとおりである。

1．トラブル対応の体制の強化
　トラブル管理体制を明確化し障害発生時の報告、連絡、相談を行う。
　（考慮すべきこととして、ユーザは、対応をベンダ任せにせず積極的に働きかける。ベンダは、ユーザに対する状況報告を密に行う）
　トラブル発生時はユーザとベンダを TV 会議で結び、ユーザとベンダが密接に協力して対応するなどを検討する。
2．適切な契約でサービスのレベルの定義を行い、責任分界点を明確にする。
3．ベンダは関係する各サードパーティ業者とトラブル対応体制を確立し、障害時の連携を適確に行う

効果

クラウドサービスにおいても役割や責任が明確となり、障害発生時のエスカレーションや対応を迅速に行うことができる。

教訓

ユーザはクラウド型システムの障害発生に備えて、クラウド事業者と連携した統制がとれたトラブル対応体制の整備が必要である。特にユーザはベンダに対して、役割分担や契約などのやるべきことをはっきりと要求し、厳しく緊張感を持って対応すべきである。これによりシステムの信頼性が向上するだけでなく、両者がお互いに成長することができる。

参考文献

（文献３－１）IPA/SEC　重要インフラ情報システム信頼性研究会報告書　2009 年
http://www.ipa.go.jp/sec/softwareengineering/reports/20090409.html

（文献３－２）IPA/SEC　 SEC BOOKS　共通フレーム 2013　2015 年
https://www.ipa.go.jp/sec/publish/tn12-006.html

（文献３－３）日本工業規格　Q 20000-2：2013（ISO/IEC 20000-2：2012）
http://kikakurui.com/q/Q20000-2-2013-01.html

（このページは空白です）