システムグループ

重要インフラ等システム障害対策（IT サービス）

SEC 研究員
加藤　均

SEC 研究員
目黒　達生

SEC 研究員
平林　大典

SEC 主任
八嶋　俊介

SEC 調査役
大高　浩

SEC システムグループリーダー
山下　博之

IT サービスを担うシステムの主としてソフトウェアに起因する障害関連情報を収集し、それらの分析や対策の整理・体系化を行い「教訓」として普遍化し、類似障害の再発防止や影響範囲縮小のために業界・分野を超えて活用可能な「情報処理システム高信頼化教訓集（IT サービス編）」として取りまとめた。

1 障害事例情報の収集・分析及び対策の検討

IT システムは、今や私たちの生活や社会・経済基盤を支える重要インフラ分野※1 等のサービスに深く浸透している。その一方で、社会に大きな影響を与えたシステム障害の発生件数は、2009 年から 2012 年にかけて増加傾向にあり、以下のようなシステム障害に関するニュースを目にする機会も少なくない。

・○○システムで障害か、終日つながりにくく
　… 原因は、法律改正直前の駆け込み需要と期末の締め処理とが重なり、想定外の大量入力にシステムの性能が耐えられなかった模様。
・□□システムで障害、午前中のサービス停止
　… 原因は、システムは本番装置の故障により予備装置に自動的に切り替わるようになっていたが、その切替えが失敗したためという。

この背景には、システム障害の原因分析や発生防止対

【脚注】
※1　内閣官房情報セキュリティセンター（NISC）では「情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流」の 10 分野を重要インフラに定義している。（平成 24 年 4 月 26 日「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」）

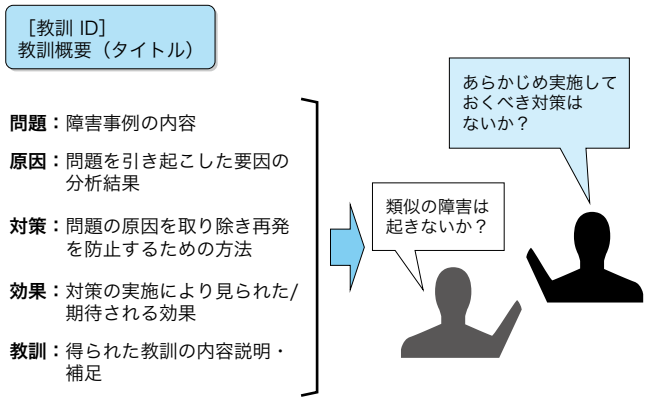


図１　各教訓の構成

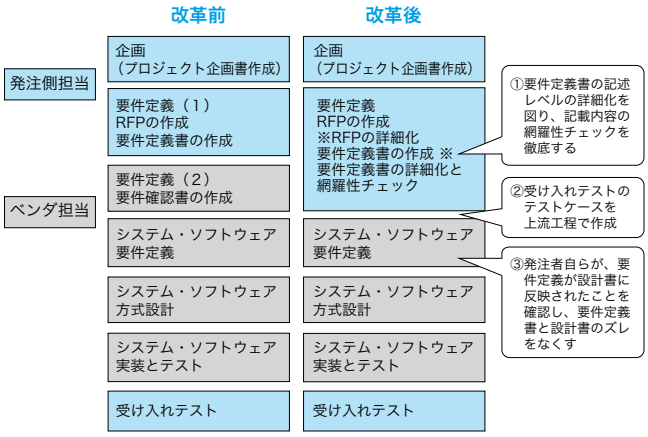


図２　教訓Ｇ２に基づく開発標準プロセスの改革例

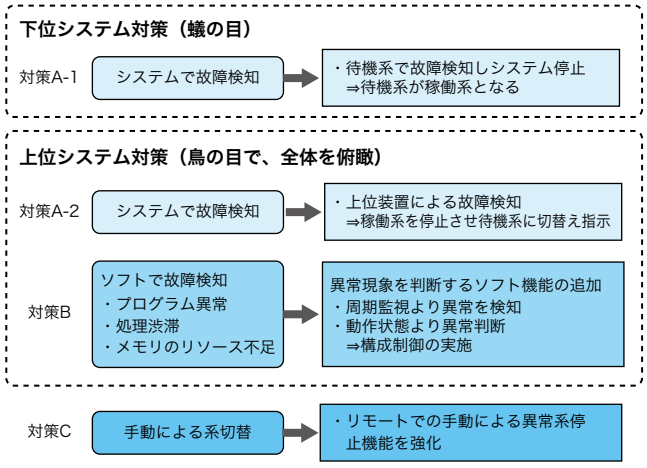


図３　教訓 T2 に基づく系切替え対策の例

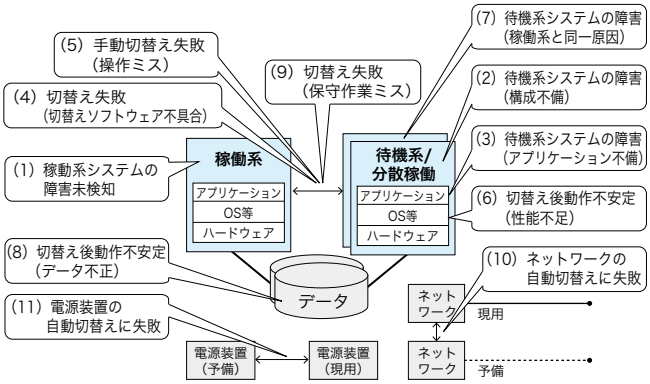


図４　教訓 T7 における切替え失敗の原因一覧

策などの情報が業界内で共有されておらず、類似の障害が繰り返し発生してしまう実状がある。障害が発生してもその詳しい情報が公開されずに当事者のみで対処されることが多く、また、一部の大規模障害では情報が公開されることがあるものの、その情報が特定の事例への対応策となっている場合が多いため、障害に関する情報が他者への参考として活かされにくいこと等が考えられる。

そこで、システムの障害事例情報の分析や対策手法の整理・体系化を通して得られる「教訓」を業界・分野を超えて幅広く共有し、類似障害の再発防止や影響範囲縮小に繋げる仕組みの構築に向けた活動を開始した。

2013 年度は、そのスタートポイントとして、以下の活動を実施した。まず、教訓化活動 として、電力、鉄道、保険、証券等の分野において、企業からの情報提供や有識者からのヒアリング等により過去の障害事例を収集した。並行して、銀行、保険、証券、電力、鉄道、情報通信、政府・行政等の多分野の CIO クラスを中心とする有識者・専門家の委員を中心とする「重要インフラ IT サービス高信頼化部会」を設置し、収集した障害事例情報を共有しつつ、その分析と対策の検討及びそれらの一般化を行った。その結果、15 件の教訓候補を精査し、下記特徴を有する教訓（９件）を導出した（表１）。

① 複数の重要インフラ分野等の有識者・専門家による「重要インフラ IT サービス高信頼化部会」において多方面から考察を行い、業界横断的に利用可能な要素を抽出。

② 所定の機密保持ルール（今回同時公開）により収集した、これまで一般には未公開の事例や情報も対象に原因や対策について考察。

③ 有識者・専門家の豊富な経験に基づく知見と、IPA/SEC の 10 年間の活動で蓄積されたソフトウェアエンジニアリングに関する検討成果に基づいて取りまとめ、技術領域に加え、ガバナンス／マネジメント領域も対象に教訓を整理。

これらの教訓を「情報処理システム高信頼化教訓集（IT サービス編）」として取りまとめた※２（図１～４）。

【脚注】
※２　http://www.ipa.go.jp/sec/reports/20140513.html

表１　IT サービスに関する教訓一覧

No	領域	ID	教訓概要
1	ガバナンス／マネジメント	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
2		G2	発注者は要件定義に責任を持ってシステム構築にかかわるべし
3	技術	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）
4		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！
5		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！
6		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！
7		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！
8		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べし
9		T7	バックアップ切替えが失敗する場合を考慮すべし

表２　障害対策手法一覧

		障害対策手法								
領域	対策事例に対応する教訓 ID	① 超上流工程での要求 品質管理 ・ユーザ企業内の事業 部門と情シス部門との 連携 ・ユーザ企業とベンダ 企業の連携、合意形成	② トレーサビリティ管理	③「見える化」手法 ・暗黙知の整備・有効活用 ・俯瞰図	④ 要求獲得手法	⑤ 変更管理	⑥ フェール ソフト	⑦ 網羅的テスト技法 ・テスト環境のリスク管理 ・シミュレーション手法	⑧ 可用性管理 ・システムの冗長化設計 ・シングルポイントの洗出し ・障害運用マニュアルの整備と 訓練	⑨ 非機能要求グレード
ガバナンス / マネジメント領域	G 1	○								
	G 2	○								
技術領域	T 1						○			
	T 2			○						
	T 3			○				○		
	T 4				○	○				
	T 5		○		○	○				
	T 6							○		
	T 7								○	○

表３　障害分析手法一覧

No	分類	名称	開発機関
1	過程関連型	FTA（Fault Tree Analysis）	Bell Telephone Lav. 他
2		ImSAFER（Improvement for medical System by Analyzing Fault root in human Error incident）	自治医科大学
3		RCA（Root Cause Analysis）	米国退役軍人省　患者安全センター
4	リスク評価型	FMEA（Failure Mode and Effects Analysis）	US.Army が最初に導入
5		HAZOP（Hazard and Operability Studies）	英国 ICI 社（Imperial Chemical Industries）
6	基本型	なぜなぜ分析	各社（品質管理手法）
7	IT 特化型	総合的インシデント分析	富士通株式会社
8	発展型	STAMP	マサチューセッツ工科大学（MIT）
9		STPA（STAMP）	マサチューセッツ工科大学（MIT）
10		CAST（STAMP）	マサチューセッツ工科大学（MIT）

・FTA：下位アイテムまたは外部事象、若しくはこれらの組み合わせのフォールトモードのいずれが、定められたフォールトモードを発生させ得るか決めるための、フォールトの木形式で表された解析方法。
・ImSAFER：ヒューマンエラーが関係した事象分析手法であり、原因追究と対策立案を支援する。
・RCA：問題や事象の根本原因を明らかにすることを目的として使用される。
・FMEA：設計の不完全や潜在的な欠点を見出すために構成要素の故障モードとその上位アイテムへの影響を解析する技法。
・HAZOP：設計意図からの逸脱によるハザードを明示する手法。効率的な運転や操作に妨げとなる設計・運転上の意図からの「ズレ」を設定し、そこから想定される潜在的な危険性を定義し評価するための体系的な手法。
・なぜなぜ分析：問題事象から発生原因まで、「なぜ」と問いながら遡っていく分析手法。
・総合的インシデント分析：日々発生するインシデントに着目した総合的なインシデント分析手法。
・STAMP：マサチューセッツ工科大学のナンシー・レブソン教授が提唱する因果関係のモデル
・STPA（STAMP）（STAMP based Process Analysis）：マサチューセッツ工科大学のナンシー・レブソン教授が提唱する因果関係のモデル STAMP（System-Theoretic Accident Model and Processes）に基づく安全解析手法。
・CAST（STAMP）（Causal Analysis using STAMP）：STAMP を使用した要因解析手法

また、障害再発防止に向けた対策についても先進的企業等の取り組み事例を収集し、過去に IPA/SEC で蓄積されたソフトウェア・エンジニアリング手法を活用し「障害対策手法・事例集」として取りまとめ、「情報処理システム高信頼化教訓集（IT サービス編）」と併せて公開した（表２）。

また、重要インフラ分野の業界団体である、電気事業連合会の会員企業（18 企業）、財団法人地方自治情報センター（LASDEC）から推薦された地方公共団体（10 団体）、一般社団法人日本損害保険協会の会員企業（12 企業）に対するアンケート結果によれば、障害事例に基づく教訓共有の取り組みについて、「関心がある」、「成果が適用できる」との回答が高い割合を示した（図５）。

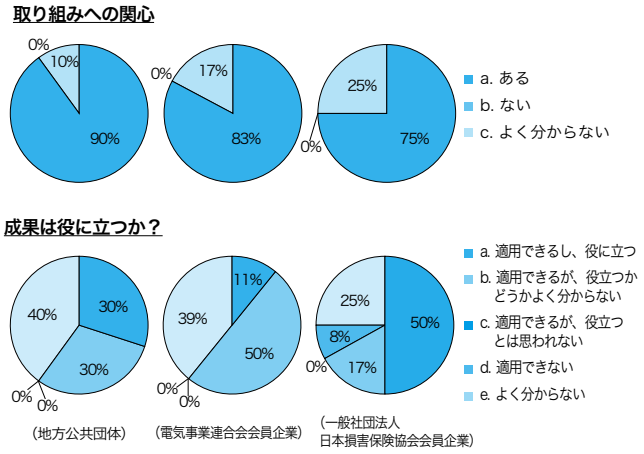


図５　業界団体に対するアンケート結果

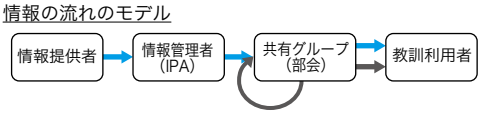
2 ソフトウェア障害の再発防止の原因分析支援

障害の原因、とくに根本原因を探ったり、その対策を導いたりするときに利用することを目的に、文献等により障害の分析手法（表３）を調査すると共に、その適用事例、障害情報分析についての各社の取り組み状況を再整理した。これらを「障害分析手法・事例集」として取りまとめ、「情報処理システム高信頼化教訓集（IT サービス編）」と併せて公開した。

3 障害情報提供に関する機密保持ルールの作成

障害事例ヒアリング、障害情報共有グループ（部会等）での議論、及び教訓の公開時において必要な、障害情報を記録する共通様式、障害情報提供に関する機密保持・情報提供ルール（図６）を作成し、公開に際しての事例情報の抽象化を明記する等、部会の意見を反映した上で、「情報処理システム高信頼化教訓集」と共に公開した。

情報の流れのモデル



No.	収集方法	ルールの適用局面（義務を負う者）			
		情報提供者から預かった障害情報の管理（情報管理者）	共有グループへの情報開示時（情報管理者）	共有グループでの議論時（共有グループメンバ）	教訓の公開時（情報管理者）
1	情報管理者が、個別ヒアリング等により提供された障害情報を取り扱う場合	情報提供者との間で、機密保持のルールを適用	情報提供者との間で、加工情報の共有に係るルールを適用	情報管理者との間で、機密保持のルールを適用	情報提供者との間で、公開のための情報加工のルールを適用
2	共有グループのメンバが、障害情報をグループ内に直接開示した場合	適用なし	適用なし	共有メンバ間で、機密保持のルールを適用	情報提供者との間で、公開のための情報加工のルールを適用

（注）ここでは、情報管理者を IPA、共有グループを IPA 内に設置された部会として説明する。
また、共有グループの運用を情報管理者が行うことを前提としている。
情報管理者は共有グループのメンバでもある。
これらは、本ルールの適用先に応じ、適切な組織・会議体に置き換えることになる。

図６　障害事例情報収集・公開のモデルと機密保持ルールの分類

4 ソフトウェア障害事例に対する対策支援

ソフトウェアが関係し得る障害発生時の調査・対策支援を担える機関への発展に向け、専門家とのネットワーク構築作りと、組織としての知識の蓄積とスキルの向上を徐々に実現していくために、部会委員の協力を得て、分析する態勢を構築（試行）した（図７）。

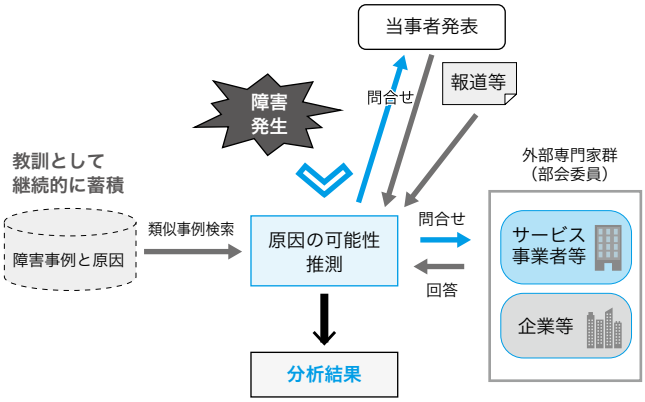


図７　障害発生時の調査・対策支援態勢（試行）

5 今後の予定

重要インフラ IT サービス高信頼化部会における検討では、各分野の障害事例に対して、他分野の委員から、自分野のコンテキストに照らして、どのような事象が考えられるか、また、どのような対策が参考となるか、といった観点から活発な議論が行われた。このように、障害事

例の背景や環境にまで深く踏み込んで分析し一般化・抽象化したため、業界・分野を超えて、類似障害の発生防止対策として役立つ『社会智』が得られたと思う。また、

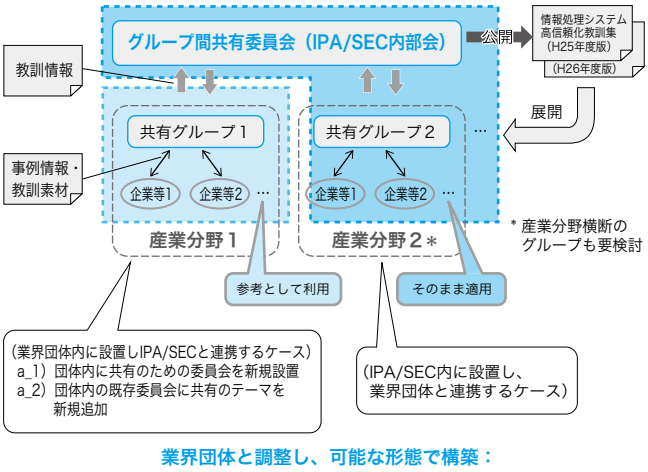


図８　情報共有の仕組みの拡大

委員からは、異分野の事例の分析過程で新たな「気づき」が得られたとの声もあった。部会での議論においては、機密保持に関するルールの下で、公開できるレベルに抽象化された本教訓集の内容より更に深い情報についても紹介され、参加者にとっては非常に有益であったと思われる。

このような取り組みは、より広く展開されることが重要である。その際には、今回の IPA/SEC における活動とその成果が参考になるであろう。今回 IPA/SEC において試行された仕組みを今後幅広く展開する方法としては、図８に示すように、分野・業界ごとに情報共有グループを設置することが考えられる。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では、より精緻な議論が行われるものと期待される。そして、分野・業界を超えた情報共有の仕組みも必要となる。今後、各産業分野の業界団体等に働きかけつつ、徐々に展開を図っていきたい。