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 主任
八嶋　俊介

SEC 調査役
三縄　俊信

SEC システムグループリーダー
山下　博之

前年度に引き続き、一定の機密保持ルールのもとに重要インフラ分野などの企業からの情報提供や有識者からのヒアリングなどにより障害事例を収集し分析と対策の検討を行った。その中から産業分野横断で活用可能な普遍的な教訓を 18 件導出し、2013 年度分と合わせた 27 件の教訓を分類整理した上で、「情報処理システム高信頼化教訓集（IT サービス編）」2014 年度版※1 として公開した。また、情報処理システムの障害事例を社会で共有する仕組みの構築に向けた普及活動を行い、３つの産業分野で情報共有の仕組みを構築し運用を開始した。

1 システム障害事例の収集・分析及び対策の検討

情報処理システムは、銀行や証券などの金融サービス、住民情報サービス、交通機関の運行制御など、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に深く浸透し、ひとたび障害が発生するとその影響は非常に大きくなり、私たちが安全で安心な生活や社会・経済活動を続けるためには、IT サービスの一層の信頼性向上が求められる。

IPA/SEC の調査結果では、報道された IT サービス障害の発生件数は、図 1 に示すように、2009 年から 2014 年にかけて増加傾向にあった。とくに 2014 年度は、消費税率 8 % 引き上げに伴う障害が多く発生した。また、クラウドサービス型のシステムにおいても障害が発生した。

従来、情報処理システムの障害に対する原因分析と再発防止対策の実施は、多くの場合、当事者においてのみ行われ、その情報は公開されて来なかった。そのため、別のシステムにおいて、あるいは他業界・分野のシステムにおいて、類似の障害が発生することがあった。

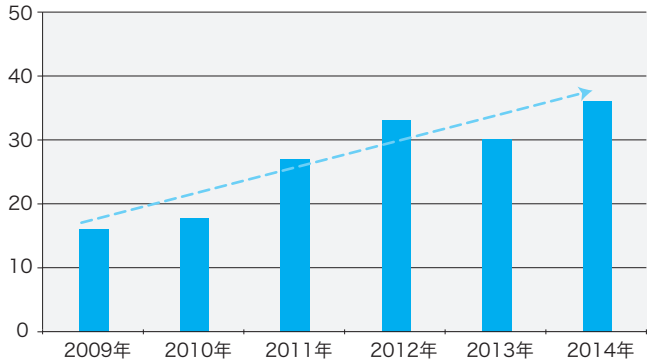


図 1　報道された IT サービス障害の発生件数の推移

情報処理システムの構築・運用やその管理は、社会や技術の進展につれて複雑化・多様化しており、一人や一企業がカバーできる範囲には限界がある。そして、その複雑性・多様性は今後ますます拡大していくことは明らかである。従って、情報処理システムの構築・運用及びその管理にかかわる信頼性向上面での課題を解決するために、より多くの人たち・企業の経験を社会全体で共有・伝承することが求められている。

そこで、システムの障害事例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・分野を越えて幅広く共有し、類似障害の再発防止や影響範囲縮小につなげる仕組みの構築に向けた活動を 2013 年度から実施している。

2014 年度も継続して重要インフラ IT サービス高信頼化部会※2 の活動を通じ、障害事例を収集し、障害原因の分析

表 1　2014 年度に導出した教訓の分野別件数

産業等分野	教訓数
情報通信分野	3 件
金融分野	6 件
交通分野	3 件
行政分野	5 件
その他	1 件
計	18 件

【脚注】

※ 1　http://www.ipa.go.jp/sec/reports/20150327_1.html

※ 2　重要インフラ IT サービス高信頼化部会：銀行、保険、証券、電力、鉄道、情報通信、政府・行政などの CIO クラスを中心とする有識者・専門家で構成する委員会

表２　教訓一覧（IT サービス編）
※太枠は 2014 年度版追加分

	教訓番号	教訓タイトル
ガバナンス / マネジメント領域		
1	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	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
4	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
5	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
6	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！
7	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
8	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
9	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
技術領域		
10	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）
11	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
12	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
13	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
14	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！
15	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
16	T7	バックアップ切替えが失敗する場合を考慮すべし
17	T8	仮想サーバになってもリソース管理、性能監視は運用要件の要である
18	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
19	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
20	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
21	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！
22	T13	利用者の観点に立った、業務シナリオに則したレビュー、テストが重要
23	T14	Web ページ更新時には、応答速度の変化など、性能面のチェックも忘れずに
24	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
25	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
26	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！
27	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

を行い普遍化した上で 18 件の教訓を導出し（表１）、2013 年度に取りまとめた教訓９件に追加して、計 27 件の教訓を収録した「情報処理システム高信頼化教訓集（IT サービス編）」2014 年度版を公開した（ガバナンス / マネジメント領域の教訓 “Gn”、技術領域の教訓 “Tn”）（表２）。

障害事例は幾つかの複合要因を包含しており、一つの障害事例について部会委員による専門的見地による分析を実施した結果、５件の教訓を導出した例もある（図２）。

導出した教訓について、ITIL[※3] をベースとした国際規格 ISO20000[※4] によるサービスマネジメント分類（図３）との対応付けを実施した（表３）。

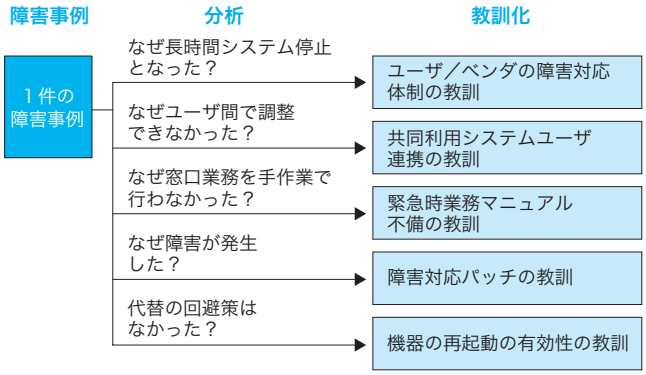
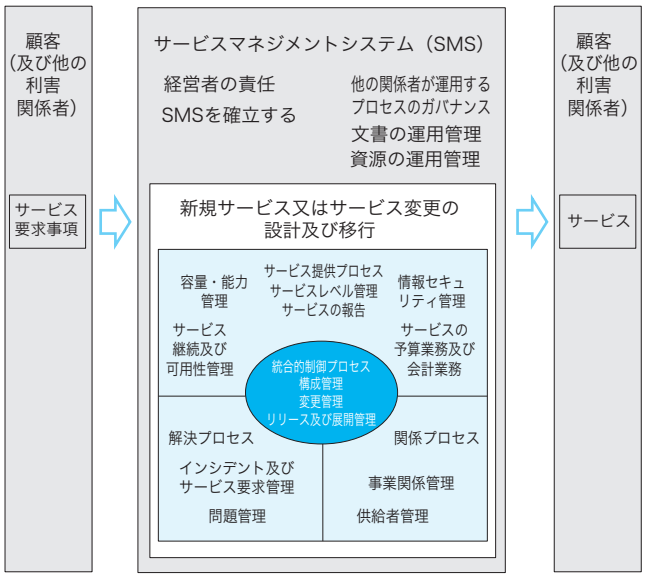


図２　一障害事例から複数の教訓導出の例



（JIS Q 20000-1:2012 より引用）

図３　ISO20000（JIS Q 20000-1）サービス管理の全体像

【脚注】

※３　ITIL：Information Technology Infrastructure Library、IT サービスマネジメントのベストプラクティス集で、IT サービスを提供するためのガイドライン。

※４　ISO 20000：IT サービスを提供している組織が、サービスの内容やリスクを明確にすることで、IT サービスの継続的な管理、高い効率性、継続的改善を実現するための国際規格。

表３から、統合的制御プロセスの構成管理、変更管理、サービス継続・可用性管理のプロセスに問題が多いことが分かる。

障害分析手法は、2013 年度版に掲載していた STAMP[※5] の記載内容を最新の内容に改訂した。また、対策手法は新たな教訓の追加に伴い、2013 年度の９件に 12 件を追加（表４）した。

2 システム障害教訓の普及活動

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」を 2014 年度は２回開催した。セミナーではシステム障害事例に基づいた障害分析、対策作成から教訓の導出までの一連の演習を参加者全員でのワークショップ形式で実施した。参加者のアンケートでは「今回のようなケースに基づくグループワークはとても有意義であった（50 代、人材育成コンサルタント）」などの声があった（図４）。

また、各業界団体（21 団体）に「情報処理システム高信頼化教訓集（IT サービス編）」を紹介し、活用について説明と意見交換、必要に応じて講演会を実施した。

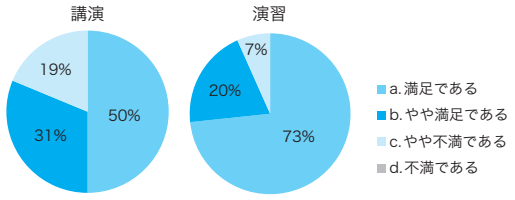
教訓集について「IPA が障害事例やケーススタディを出していくのは重要と考える」、「ベンダのユーザ会などで情報共有はあるが、ベンダをまたがって事例共有することはより有意義である」、「情報処理システム障害の教訓をまとめることは良い取り組みと考えており IT サービスの障害事例の提供にも協力したい」、「教訓の横展開は障害を減らすために重要であり、自社内でも必要と考えるが汎用化の方法や共有の方法など整理できていない。IPA から教えて欲しい」などの意見が出た。更に「クラウド化が増えているが、これに関する事例や留意点が欲しい」、「パッケージ製品を利用して発生した障害事例があると良い」など、今後の拡張に期待する要望もあった。

表３　各教訓と IT サービスマネジメントの対応

教訓 ID	JIS　Q 20000-1：2012 より（●主な問題個所、△関連する問題個所）												
	5. 新規またはサービス変更の設計及び移行	6. サービス提供プロセス					7. 関係プロセス		8. 解決プロセス		9. 統合的制御プロセス		
		サービスレベル管理	サービス継続・可用性管理	サービス報告	容量・能力管理	情報セキュリティ管理	事業関係管理	供給者管理	インシデント管理	問題管理	構成管理	変更管理	リリース管理
G1	△						●						
G2	●							△					
G3	●	△											
G4				△				△	●	△			
G5					●		△						
G6											△	●	△
G7				△			△	△	●				
G8							●				△		
G9			△				●						
T1			●								△		
T2					△				△		●		
T3	●	△								△		△	
T4			●							△	△	△	
T5	△											●	
T6											●	△	
T7			●		△								
T8					●				△		△		
T9			●							△	△		
T10			△								●		
T11		●			△								
T12								△			△	●	△
T13	●	△										△	
T14					△							●	△
T15											△	●	
T16						△		△		●	△		
T17			△								●		
T18	●										△		

表４　新たに追加した対策手法

追加した対策手法
共同センター利用におけるユーザ企業の連携、合意形成
クラウドセンターと利用企業の連携、合意形成
障害管理の取り組み
プロセス改善
ヒューマンファクターズ
製品に関するトレーサビリティ　ISO9001
テスト網羅性の高度化技法
仮想化技術
レビュー手法
サイレント障害対策
パッチ管理技法
高回復力システム基盤導入



※ 2015 年３月 20 日実施分のセミナーアンケート集計結果

図４　SEC セミナーの満足度アンケート結果の例

【脚注】

※５　STAMP（Systems-Theoretic Accident Model and Process）：システム理論に基づく事故モデル

なお、各業界団体への IPA の取り組みの説明会の後にアンケートを実施した（電気事業連合会の会員企業（回答９企業）、地方共同法人 地方公共団体情報システム機構（J-LIS）から推薦された地方公共団体（回答８団体）、神奈川県市町村自治体（回答 30 件））。

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）。

3 システム障害事例共有の仕組み構築

各業界団体にシステム障害事例の共有の仕組み構築を働きかけ、３つの業界団体において仕組みを構築し運営を開始した。

（情報通信分野）

ITA（Information Technology Alliance：情報サービス団体（加盟 18 社））内の９社による「障害再発防止策研究会」が 2014 年に発足し、システム障害事例の共有の仕組みを同団体内に構築し活動を開始した。IPA 職員が同研究会に参加すると共に、IPA の重要インフラ IT サービス高信頼化部会においてその活動状況を紹介していただき、活動の成果は ITA の Web サイト上で「ITA 情報処理システム障害事例集」として公開され IPA のウェブサイトから URL リンクによる連携を実施した。

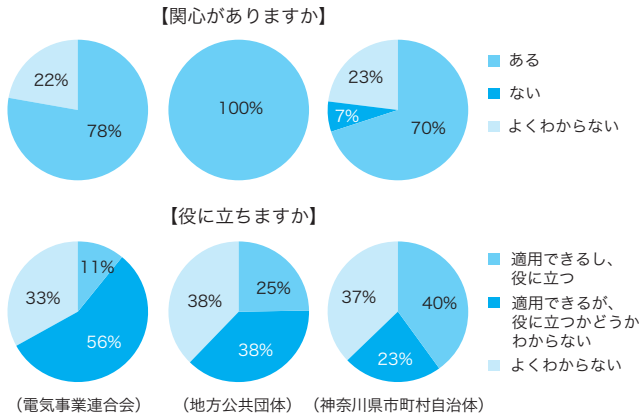


図５　IPA の取り組みへの関心度に関するアンケート結果例

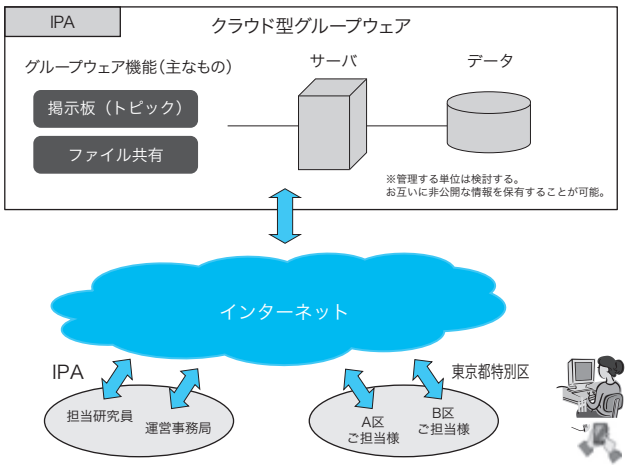


図６　仮想的情報共有グループのイメージ

（行政分野）

東京都特別区電子計算主管課長会にて障害事例共有の意義に賛同いただき、情報共有を行うことが決議された。電子掲示板を使った仮想的な情報共有グループ（図６）を IPA 内に設置し、各区及び IPA 間での情報共有などを行う試行運用を開始した。

（電力分野）

電気事業連合会の協力のもと、情報共有の取り組みに賛同する電力関連９団体・企業を中心にメーリングリストを使用した情報共有を行うこととし、その運用を開始した。IPA もこの情報共有に参加する。

4 今後の予定

システム障害事例を収集してその普遍化を行い教訓として整理する活動は継続し、教訓集の内容の更なる充実を図っていきたい。

また、社会インフラ情報処理システムの一層の信頼性向上を目指し、2014 年度にシステム障害事例の共有の仕組みを構築した３つの産業分野の効果的な運営を支援すると共に、新たな産業分野にも仕組みの構築を働きかけ、自律的な活動を促しつつ、システム障害事例共有の裾野を拡大していきたい。

このために、新たに「障害事例教訓集の活用ガイド（仮称）」や「障害事例から学ぶ情報処理システムの信頼性向上ガイド（仮称）」などを作成する予定である（図７）。

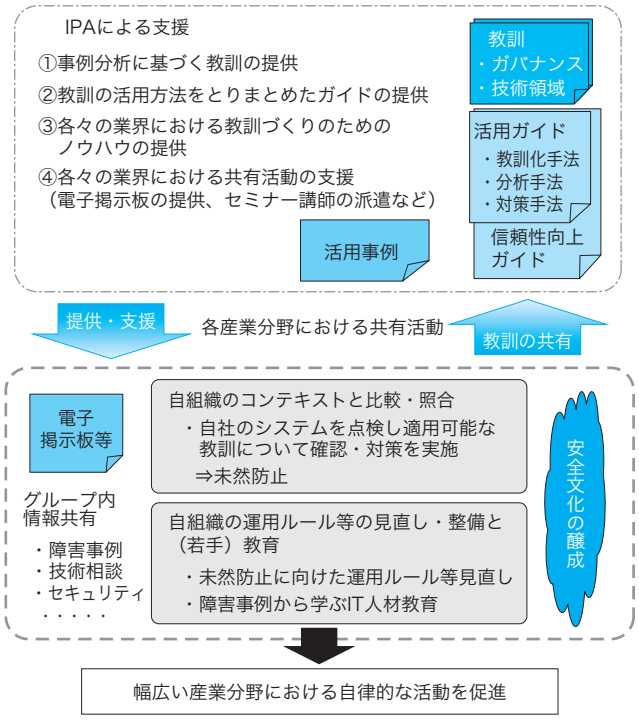


図７　情報共有活動の仕組み