重要インフラ等システム障害対策

SEC調査役 三縄 俊信　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 三原 幸博　SEC調査役 石田 茂
SEC調査役 十山 圭介　SEC調査役 石井 正悟　SEC研究員 松田 充弘
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、重要インフラ分野等のシステム障害事例からヒアリングなどにより障害事例情報を収集し、その分析と対策の検討を行った。その結果、ITサービスシステム分野からは９件、機器の制御を行う組込みシステム分野からは７件の産業分野横断で活用可能な普遍的な教訓を導出し、前年度までの教訓と併せて分類整理した上で教訓集として公開した。また、教訓集等を自社内で活用するため、及び障害の未然防止に役立つ教訓を自ら作成し継続的に運用していくためのガイドブックを作成し公開した。更に、ITサービスシステムの障害事例情報を共有する仕組みの構築に向けた支援活動を行い、新たに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。

ITサービスシステム

1 背景

情報処理システムは、銀行や証券などの金融サービス、各種手続きのための行政サービス、ソーシャルネットワーク等の情報通信サービス、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等のITサービスに深く浸透し、ひとたび障害が発生するとその影響は非常に大きい。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、重要インフラなどを支えるITサービスの一層の信頼性向上が求められている。

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2015年にかけて増加傾向にあり、特に2015年度は、マイナンバー関連等のシステム稼働直後の初期障害が多く発生した。

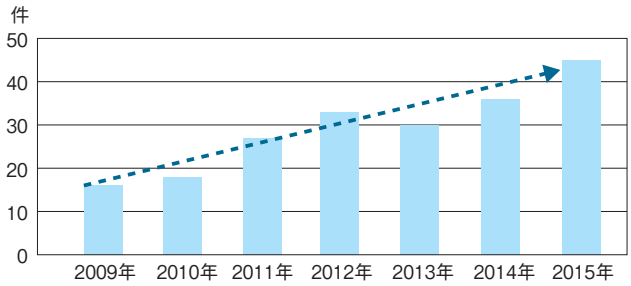


図１　報道されたITサービス障害の発生件数の推移

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こなかった。そのため、他業界・分野のシステムなど、当事者以外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。

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、一個人や一企業の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IPA/SECでは、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。

2 障害事例の収集と教訓化

2015年度も継続して重要インフラITサービス高信頼化部会※1の活動を通じ、ITサービスシステム分野における障害事例を収集し、障害原因の分析を行い普遍化した上で９件の教訓を導出した（表１、表２）。これらを2014年度に取りまとめた教訓27件に追加して、計36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）2015年度版」（以下、教訓集2015）を公開※2した。

表１　2015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	１件
金融分野	４件
行政・自治体分野	３件
その他	１件
計	９件

【脚注】
※1　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・行政などの情報処理システムの有識者・専門家で構成する委員会
※2　URL: http://www.ipa.go.jp/sec/reports/20160331_1.html

表2　2015年度追加教訓（ITサービス編）

ID	教訓概要
ガバナンス／マネジメント領域	
G10	関係者からの疑義問合せは自社システムに問題が発生していることを前提に対処すべし！
G11	システムの重要度に応じて運用・保守の体制・作業に濃淡をつけるべし
G12	キャパシティ管理は、業務部門とIT部門のパートナーシップを強化すると共に、管理項目と閾値を設定してPDCAサイクルを回すべし
G13	キャパシティ管理は関連システムとの整合性の確保が大切
G14	設計時に定めたキャパシティ管理項目は、環境の変化に合わせて見直すべし
技術領域	
T19	リレーショナルデータベース（RDBMS）のクエリ自動最適化機能の適用は慎重に！
T20	パッケージ製品の機能カスタマイズはリスクを認識しとくに必要十分なチェック体制やチェック手順を整備して進めること
T21	作業ミスを減らすためには、作業指示者と作業者の連携で漏れのない対策を！
T22	隠れたバッファの存在を把握し、目的別の閾値設定と超過アラート監視でオーバフローを未然に防止すること

教訓作成に当たり、2015年度に報道されたシステム障害事例について当事者にヒアリングし、教訓化の了解を得た事例について匿名化・一般化を行った。ヒアリングを行ったシステム障害事例は下記。

- 電気通信事業者の通信システム障害
- 自治体コールセンタのシステム障害
- 金融機関のオンラインシステム障害
- 地方公共団体のICカード管理システム障害

更に、導出した教訓について、ITIL※3をベースとした国際規格JIS Q20000-1:2012※4によるサービスマネジメント分類との対応付けを実施した（表3）。

表3　追加教訓とITサービスマネジメントの対応

No.	JIS Q20000-1：2012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
G10							△		●				
G11			△								●		
G12			△		●								
G13			△		●							△	
G14			△		●								
T19	●				△								
T20	△							●					
T21	△										△	●	
T22			●		△						△		

これと同様に、教訓集2015に収録した教訓を分類したところ、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、容量・能力管理のプロセスに問題が多いことが分かった。

また、障害分析手法については、ヒューマンエラーに起因するシステム障害の分析手法としてImSAFER※5を調査し詳細な解説を追加した。このほか、STAMP※6に関する分析手法（STPA※7、CAST※8）を調査し、より具体的に活用できるよう解説を追加した。障害対策手法については、新たに3件を追加（表4）し、計23件とした。

表4　新たに追加した障害対策手法

追加した対策手法
障害再発防止のための組織的マネジメント
RDBシステム管理
ヒューマンファクターズ

3　システム障害情報共有の仕組み構築

各業界団体等にシステム障害情報の共有の仕組み構築を働きかけ、2015年度に新たに3つの情報共有グループを構築し、その運営を開始した。

（情報通信分野）

一般社団法人日本ケーブルテレビ連盟（正会員オペレータ370社）が連盟内に構築する運用情報共有システムを利用した障害情報共有の仕組みの活性化に向けて、IPA/SECが事例情報提供などの支援を行う活動を開始した。

（航空分野）

航空運航システム研究会（TFOS.SG※9（航空に関心のある学識経験者や技術者、パイロットなどで組織する民間研究団体））が「航空システム障害事例の分析に基づく教訓作成」を行うことを決定し、配下の航空システム部会とIPA/SECの協業により、航空システム障害事例を教訓化し情報共有すべく活動を開始した。

（金融分野）

一般社団法人生命保険協会の協力のもと、障害情報共有の取り組みに賛同する生命保険会社16社で構成する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。

また、2014年度に運用を開始した3つの情報共有グループ（行政・電力・情報通信分野）についても、IPA/SECによる支援活動・意見交換を継続して実施した。

【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　JIS Q20000-1:2012：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、ISO/IEC20000-1:2011対応
※5　Improvement for medical System by Analyzing Fault root in human Error incident
※6　Systems-Theoretic Accident Model and Processes（システム理論に基づく事故モデル）
※7　System Theoretic Process Analysis
※8　Causal Analysis using System Theory
※9　TFOS.SG：Total Flight Operation System Study Groupの略称

4 ガイドブックの作成

自社内で発生したシステム障害事例の原因分析を行い再発防止策などを「教訓」として作成するための手法をまとめた「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）」（以下、教訓作成ガイドブック）、及び自社で作成した教訓のほか、IPA/SECや他社などの第三者が提供する教訓を自社内で活用するための手法をまとめた「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）」（以下、教訓活用ガイドブック）を公開※10した。

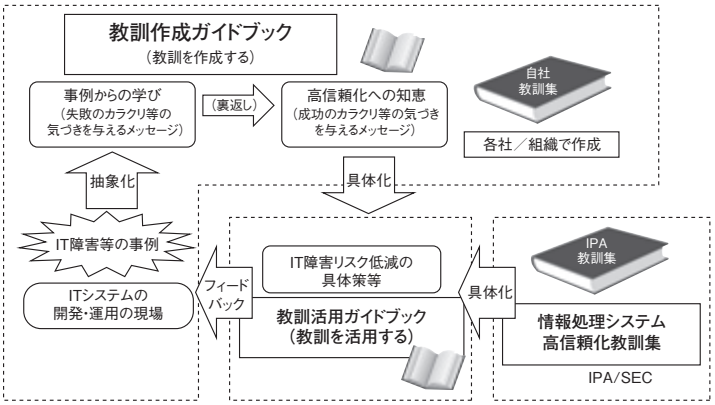


図2　教訓集2015とガイドブック2編

5 普及展開活動

① 新着教訓の逐次公開

教訓集に収録されている各教訓をインデックスからタイムリーに参照・利用可能となるようにIPA/SECのWebページ上に教訓リンク集を構築した。また、2015年度に作成した新しい教訓９件を前述の教訓集公開に先駆けてこの教訓リンク集に新着情報として逐次公開した。

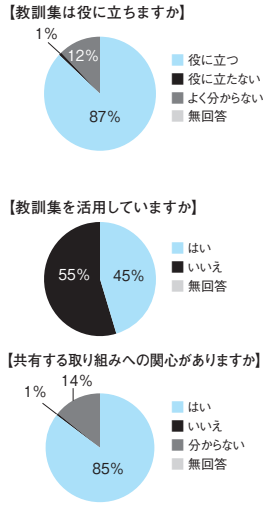
② 教訓集などのダウンロード状況

2014年度末に公開した教訓集などのダウンロード件数を調査した。

教訓集2014年度版　：　1,480回（2015年４月～ 2016年３月）
個別教訓リンク集　：　10,426回（2015年12月～ 2016年３月）

教訓集をダウンロードした方に活用状況アンケートを実施した。（アンケート発送先：916名、回答：115名）

その結果、教訓集は役に立つと回答した割合が87%であるが、活用している割合は45%となっており、活用を促進するための取り組みと内容の充実が課題とわかった。なお、このような産業分野横断的な共有への取り組みに対する関心があるかという質問に対しては、「はい」が85%と高いことが分かった。



- 他企業の事例を確認することで、他社と共通の事柄、相違している事柄が把握可能
- 経験には限りがあり、それ以外の教訓を享受できる
- アウトソーシング等のサービス業務における品質向上のための改善ポイントを考えるとき、ヒントとして有効
- 監査すべき着眼点の参考になる
- 実際に発生した障害及び、その対処法・防止策が記載されているため

- 社内教育として事例を説明
- 機能面に目が行きがちなところに対し、留意すべき考え方をチーム内に展開
- 事業部生産性品質向上施策の一環として教訓集を紹介、事業部内に展開
- 障害原因究明時に必要な基礎知識として、社内教育でケーススタディとして使用
- 担当チーム内での振り返りや意識付けの向上のケーススタディ材料として有益
- ITSMSの認証取得を受け経営者も参加するフォーラムを開催、その中で根本原因の対策、レビュー、運用手順の整備を行う上で参考として利用

図3　ダウンロードした方へのアンケート結果の例

③ 業界団体等への普及推進

各業界団体（14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、活用についての説明と意見交換、必要に応じて講演会を実施した。また、講演実施後のIPA/SECの取り組みに関するアンケートを実施した。

結果は②のアンケート結果と同様の傾向であることが確認できた。

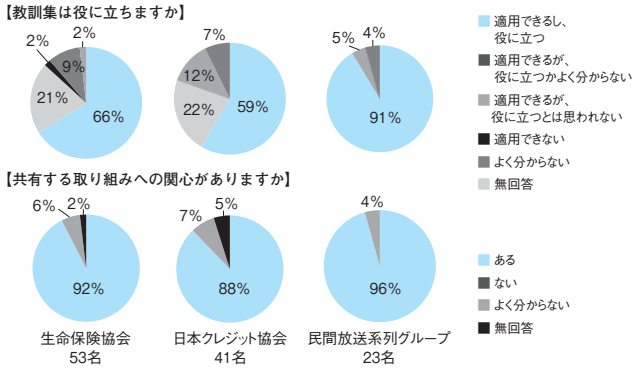


図4　IPA/SECの取り組みへの関心度アンケート結果の例

6 今後の予定

2016年に入っても航空システムや自治体のICカード発行システムなどの社会的影響が大きなシステム障害が発生している。

引き続き障害事例を収集しその普遍化を行い教訓として整理する活動を継続し、教訓集として更なる充実を図っていくと共に、情報処理システムの高信頼化に向けて有益な情報発信を強化していく予定である。

また、社会インフラ情報システムの一層の信頼性向上を目指し、活動を開始したシステム障害情報の共有の仕組みの運営を支援すると共に、新たな産業分野にも普及を働きかけ、自律的な活動を促しつつ、システム障害情報共有の裾野を拡大していきたい。

【脚注】

※10　URL: http://www.ipa.go.jp/sec/reports/20160229.html

組込みシステム

1 背景

近年、機器や製品（以下、組込みシステム）の機能の大半がコンピュータを利用してソフトウェアで実現されるようになってきている。それらには社会インフラとして重要な役割を担うものも多いが、実現する機能規模が肥大化すると共に複雑化する傾向にあり、IoTが進展する今日ではシステム全体として信頼性を確保するための更なる技術面での工夫や運用管理での工夫が求められている。

一方、企業間競争の激化により、差分開発といった短納期の製品開発が主流となり、システム高信頼化のための技術やノウハウがうまく伝承されていないといった問題も顕在化している。

このような組込みシステムの現状に鑑み、産業界におけるシステム高信頼の知見を集積し、将来に向けたシステム信頼性向上のための技術的な布石を打ち、その結果としてシステム信頼性に関する社会的な認識レベルを上げていくことを目的に、2013年度より「製品・制御システム高信頼化部会」とその傘下の一つである未然防止知識WGにて活動を進めてきた。

2015年度は「情報処理システム高信頼化教訓集（組込みシステム編）2015年度版」（以下、教訓集2015）[※11]の作成に加え、この教訓集などを自社内で活用し未然防止に役立つ教訓を自ら作成し継続的に運用していくための「障害未然防止のための教訓化ガイドブック（組込みシステム編）」（以下、教訓化ガイドブック）」「現場で役立つ教訓活用のための実践ガイドブック（組込みシステム編）」（以下、活用ガイドブック）を新たに作成した。[※12]

2 障害事例の収集と教訓化

2014年度に引き続き、産業界で実践されているシステムの品質上の問題を未然に防ぐための知識をもとに、組込みシステムの障害を一般化した。更に、組込みシステム開発企業において幅広く利活用できるようにするための対策の事例を新たに加え、新規７件の事例を公開した。（表５）

3 ガイドブックの作成

3.1 障害未然防止のための教訓化ガイドブック

3.1.1 背景と狙い

自社内で起きた障害の再発防止策の知見を他製品・技術に適用し、同じような障害の発生を未然に防ぐ手立てを講じるためには、ノウハウの一般化をいかに行うかが重要となる。しかしながら、異なる製品領域にまたがった知見の一般化は難しい。これは、

- 使用している動作原理、技術
- 商流・ビジネスモデル
- 開発プロセス
- 組織風土・不文律

が組織ごとに異なるためであり、同一企業であっても部門や事業場ごとにこうした要素が大きく異なっているためである。そこで、様々な製品・システム・組織の観点から障害を分析し、知見の一般化を行ううえで分野を問わず、共通的に活用できるポイントをまとめた教訓化ガイドブックを作成した。

表５　教訓一覧と対策が必要な工程との対応例

教訓番号	教訓タイトル	システム要求定義	システムアーキテクチャ設計	ソフトウェアアーキテクチャ設計	ソフトウェアアーキテクチャ設計（変更設計）	実装（コーディング）	レビュー	システムテスト	教育	プロジェクトマネジメント	運用
29	複数の事業体にまたがる重要システムでは関係者の立場・ニーズの視点から、想定しうる障害発生リスクを同定し効果的な危機管理体制を構築する	○	○						○	○	○
30	過去のハードウェア、ソフトウェア資産を使用する場合は、その内容や当時の方法について考慮する				○	○		○			
31	ミッションクリティカルシステムではリスク管理やV&Vを確実に実施する						○		○	○	
32	不測事態においても適切に動作するかの検証を十分に行い、条件変更時には潜在的なリスク許容度合いの変化を見逃さない		○		○		○	○		○	
33	不十分な設計となっている回避策は根本的に見直す		○	○							
34	重要なソフトウェアを変更する際は、変更管理を確実に実施する		○						○	○	
35	リスク分析によるハザード識別を行い、非常時には関係者が即応できる体制を構築する		○						○		○

目次

1．はじめに
2．教訓化のための概念モデル
3．教訓化の定着に向けたプロセスと組織活動
4．実践的アプローチ
5．未然防止に向けた企業内事例

図5　障害未然防止のための教訓化ガイドブック

3.1.2　ガイドブックの特徴

本ガイドブック作成に当たり、様々な分野の開発実務者にケーススタディを用いた体験型ワークショップに参加いただき、そこでの経験をもとに

- グループワーク用のケースの提示
- 教訓を抽出する観点（例えば、製品・技術、マネジメントなどの職種・分野を指定する観点）の設定
- 教訓の受け手に応じた気づきの与え方、伝え方の工夫

などのポイントを分野横断的に適用できるノウハウを取りまとめた。図6はワークショップで使用したケース資料を例示したものである。

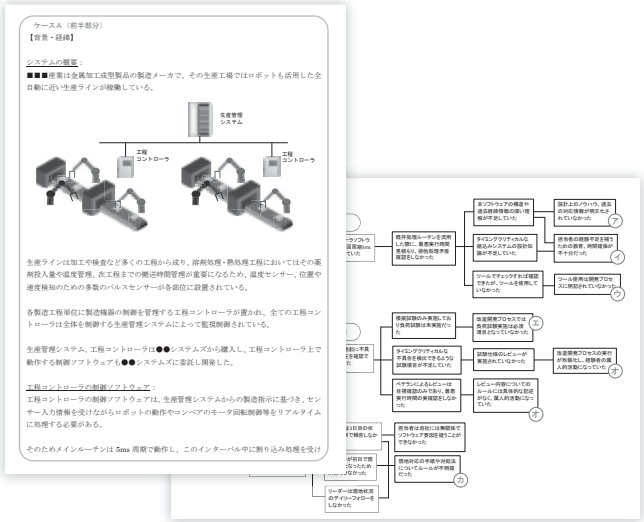


図6　抽出観点例

また、ワークショップ参加者からは「実例を想定した演習内容であり、ディスカッションを行うことができ有意義」、「演習の中でサンプルケースを見て作業を行うことにより、自社に置き換えて考えることができた」、「再発防止策から未然防止策を導き、他者へ伝えるのは工夫が必要と感じた」などのご評価をいただくことができた。

3.2　現場で役立つ教訓活用のためのガイドブック

3.2.1　背景と狙い

多くのものづくり企業で行われている実際の開発プロセスや社内教育などにおいて、前掲の教訓集を含め自社内で蓄積されている教訓情報をどのように活用することができるか、その実践的な活用法を解説するための活用ガイドブックを作成した。この際、企業内で実際に取り組まれている品質マネジメント、再発防止の活動事例も併せて掲載した。

目次

1．はじめに
2．教訓集の構成と特徴
3．組織学習のための基礎
4．基本的な活用方法
5．企業内での活動事例

図7　現場で役立つ教訓活用のための実践ガイドブック

3.2.2　ガイドブックの特徴

社内外からもたらされた教訓を自組織ですぐに活用できるよう、「社内教育・研修」、「開発プロセス」、「設計品質向上活動」の活用シーン別に分け、それぞれの応用例は、

- 想定される状況・課題
- 活用の狙い
- 活用方法
- 期待効果
- 留意事項

をポイントとし、図表なども含めて記述した。図8にこのイメージを例示する。

図8　ガイドブックのポイント

4　今後の予定

今後は、各企業が自ら高信頼なものづくりを継続的に取り組んでいくための教材作成や教育の普及に向け、セミナー等の開催と、それらの活用を意識した質・量両面からのブラッシュアップを進めていく。

また、教訓化及び知識整理方法のまとめ方に関しても、収集済み事例から要素知識を抽出・体系化を行うなど更なる内容の充実化に向けた取り組みを進めていく。

【脚注】

※11　URL:http://www.ipa.go.jp/sec/reports/20160331_2.html
※12　URL:http://www.ipa.go.jp/sec/reports/20160331_3.html