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 目黒 達生　SEC研究員 村岡 恭昭
SECシステムグループ主任 八嶋 俊介　SEC調査役 三原 幸博　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

2015年度に引き続き、重要インフラ分野など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。ITサービスシステムは産業分野横断で活用可能な普遍的な教訓を6件導出し、2015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、2010年から収集している、報道されたシステム障害事例について横断的に傾向分析を行い、頻度の高い「ヒューマンエラー」と「システムの高負荷／過負荷」に起因する問題を取り上げ、詳細解説を教訓集に追加した。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。また、組込みシステムの教訓をもとに障害未然防止のための設計知識を整理する手法をガイドに取りまとめ、公開した。

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など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などの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。

社会に多大な影響を与え、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2016年にかけて増加傾向にあり、2016年は、鉄道・航空分野の旅客サービス障害、マイナンバー制度や電力自由化対応などの制度開始に伴う初期障害が発生した。

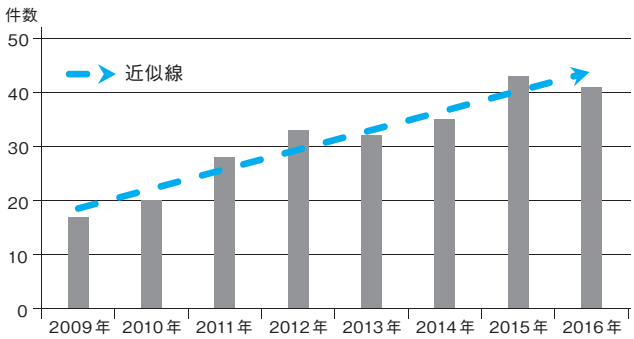

図1　報道されたITサービス障害の発生件数の推移

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、当事者以外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。

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する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、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

2016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、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6件の教訓を導出し（表1、表2）、2015年度に取りまとめた教訓36件に追加して、計42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）2016年度版」（以下、教訓集2016年度版）を公開※2した。

表1　2016年度に導出した教訓の分野別件数

産業分野	教訓数
交通分野	2件
金融分野	1件
行政・自治体分野	2件
その他	1件
計	6件

表2　2016年度追加教訓（ITサービス編）

教訓ID	教訓概要
ガバナンス／マネジメント領域	
G15	保守作業は「予期せぬ事態の発生」を想定し、サービス継続を最優先として保守作業前への戻しを常に考慮すること
G16	本番環境へのリリースは、保守担当が無断でできないような仕組みを作るべし！
技術領域	
T23	障害監視は、複数の観点から実装し、障害の見逃しを防げ！
T24	サービス縮退時の対策を考慮せよ
T25	障害原因が不明でも再発予防と発生時対策はできる
T26	既存システムの流用開発はその前提条件を十分把握し、そのまま利用可能な部分と変更する部分を調査して実施する

教訓集2016年度版では、2010年から2016年まで蓄積している、報道されたシステム障害情報を分析し、問題の傾向と対策を記載した新たな章を追加した。

- ヒューマンエラーの問題と対策
- システムの高負荷／過負荷に関する問題と対策

3　システム障害情報共有の仕組み構築

各業界団体などにシステム障害情報の共有の仕組み構築を働きかけ、2016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。

表3　情報共有体制を構築した産業分野

産業分野	企業・業界団体など	組織概要
クレジット分野	（一社）日本クレジット協会	システム研究会に参加する会員企業
地方団体	北海道IT情報共有グループ	北海道地域のインフラ事業者など
地方団体	（一財）関西情報センター（KIIS）※3	サイバーセキュリティ研究会に参加する会員事業者

また、2015年度までに運用を開始した6つの情報共有グループについて、IPAによる支援活動・意見交換を継続して実施した（図2参照）。

4　普及展開活動

①教訓集などのダウンロード
＜2016年度に実施されたダウンロード件数＞

成果物	件数
教訓集2015年版	1,575件
教訓作成／活用ガイドブック	1,713件
個別教訓リンク集	12,806件

②教訓集活用メールマガジンの発行
教訓集などをダウンロードする際に、IPAからの情報提供を希望された方を対象として、「教訓集活用メールマガジン」の発信を9月から開始（2017年3月現在、読者数約1,000名）。

③教訓集ダイジェスト2016年度版作成
普及展開活動を推進するために、教訓集2016年度版を要約した小冊子を作成した。

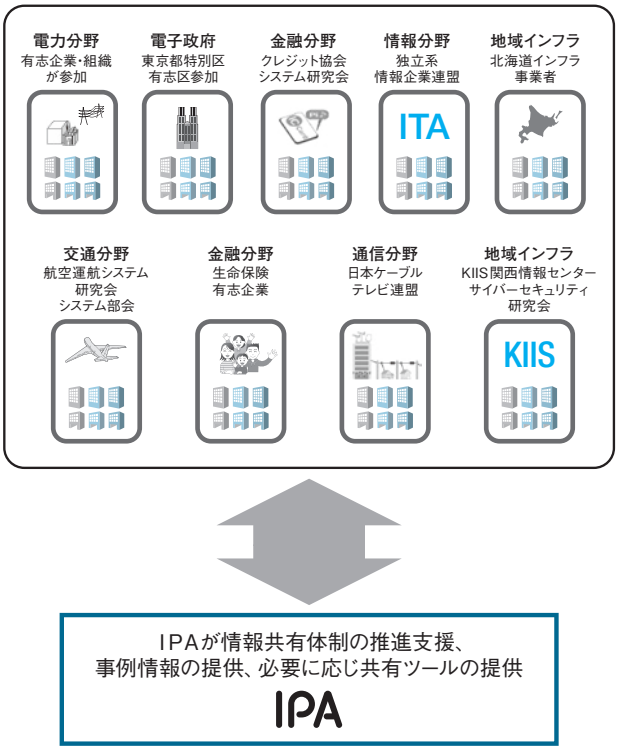

図2　2016年度までに構築した情報共有グループ

5　今後の予定

2017年度も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

※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　http://www.ipa.go.jp/sec/reports/20170327.html
※3　KIIS（Kansai Institute of Information Systems）

組込みシステム

1 活動概要

組込みシステムの障害対策は、前述のITサービスシステムの運用視点とは異なり、モノ作りの視点で議論されてきたため、2016年度は、設計段階で障害回避処理を盛り込むための「障害未然防止のための設計知識の整理手法ガイドブック(組込みシステム編)」※1を検討し公開した。

2 設計知識の整理手法ガイドブック

2.1 背景と目的

情報処理システムや組込みシステムを開発するベンダ企業の多くは、過去の障害事例を一定の様式で記録し障害情報データベースとして蓄積している。一般に「過去トラ(DB)」と呼ばれており、類似障害の再発防止や未然防止のために活用できる情報が埋蔵されているが、実際のところ、ソフトウェア障害に関して効果的に活用されている事例は聞かれない(図1)。

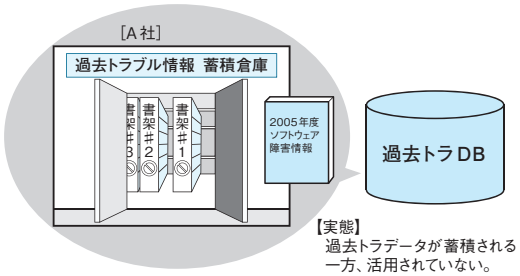

図1 活用されない過去トラDB

「過去トラDB」が有効活用されない理由として、表面的な障害の事象と、どこにどんな対処をしたか程度の情報しか書かれていないことが多く、障害を防止するためのノウハウが整理されていないことが挙げられる。更に、障害事例の原因と対処が装置やサービス固有の具体的な表現で記載されるため、記載内容を見る利用者にとっては、自身の扱うシステムと無関係な障害事例に見えることがある。また、膨大化した「過去トラDB」は、有効情報を取り出す工夫がなされていないことも理由の一つとしてある。一方、業界が抱える課題の一つに技術伝承があり、ベテラン技術者の豊富な経験やノウハウの断片が埋蔵されている「過去トラDB」は、技術伝承の観点においても有効活用したい(図2)。

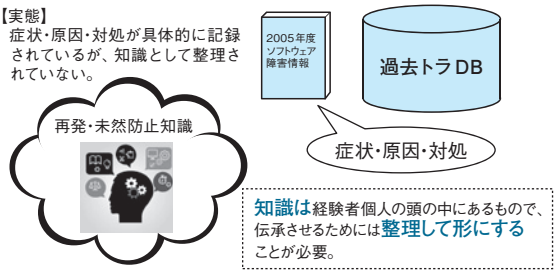

図2 ベテラン技術者の経験やノウハウが埋蔵された過去トラDB

本ガイドブックは、「過去トラDB」を障害の再発防止や未然防止の活動に活用するために、障害情報記録から設計知識を抽出する方法、更に様々なソフトウェアに共通して再利用できるようにタグ設定の考え方を提示する。

2.2 設計知識の整理手順

障害を未然防止するための設計知識を整理する手順を図3に示す。

① 「過去トラDB」から設計知識を抽出する
② 抽出した設計知識を構造化する
③ 更に設計知識を一般化表現に変換する
④ 設計知識の再利用を促すための分類タグを抽出する

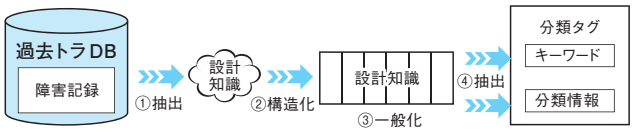

図3 設計知識の整理手順

2.3 設計知識の構造と文脈

障害を未然防止するための設計知識は、図4の構造で整理する。構造化表現された設計知識の知識要素(1)～(4)及び(6)をつなげると下記の設計知識の文脈ができる。知識要素(5)は、(1)～(4)の要素を文章に組み立てたものを入れる。

(1) 障害を引き起こす機能・処理	(2) 考慮漏れしやすい視点・観点	(3) 発生契機	(4) 発生し得る障害内容	(5) 発生メカニズム	(6) 対策

図4 設計知識の構造

【設計知識の文脈】
「(1)の機能や処理を考えるときに、(2)の考慮が漏れていると、(3)が起こった契機で(4)の障害が発生する。その障害の発生を防ぐためには(6)の処理を作り込んでおく。」

2.4 分類タグ

「過去トラDB」から抽出した設計知識の再利用性を高めるために、設計知識に分類タグを付けてDB化する。

分類タグは、図5に示す4種類を提案する。

分類タグは、その知識が何に役立つものかを直感的に理解するためのキーワード"何が""どうなる"(分類タグ2)と、検索の視点で付加する機能・処理(分類タグ1)、装置・デバイス(分類タグ3)、混入プロセス(分類タグ4)で構成している。

(分類タグ 1) 機能・処理	(分類タグ 2.1) キーワード "何が"	(分類タグ 2.2) キーワード "どうなる"	(分類タグ 3) 装置・デバイス	(分類タグ 3.1) 装置・デバイス	(分類タグ 4) 混入プロセス	(分類タグ 4.1) 混入プロセス

図5 分類タグ

脚注

※1 http://www.ipa.go.jp/sec/reports/20170321_1.html