

重要インフラ分野等システム／製品の障害対策

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 研究員 **齋藤 毅**SEC 調査役 **三原 幸博**SEC 研究員 **松田 充弘**システムグループリーダー **山下 博之**

2013年度から2017年度まで、重要インフラ分野などのシステム／製品の障害事例からヒアリングなどにより情報を収集し、その根本原因の分析と再発防止策の検討を行った。その結果をもとに、ITサービス分野については産業分野横断で活用可能な普遍的な教訓を50件、組込み分野については多様な組込み製品や制御システムに適用可能な教訓を35件、それぞれ作成し、教訓集に取りまとめて公開した。また、ITサービス分野において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、7つの産業分野・地域で計13件の情報共有の仕組みが運用を開始した。

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ており、ひとたび障害が発生するとその影響は非常に広範囲に及ぶ。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。

IPAでは、社会インフラに影響を与えマスコミなどで報道されたITサービス障害情報を継続的に収集している。そのデータによれば、ITサービス障害の発生状況は調査を開始した2009年から増加傾向にある(図1)。

また、家電製品や自動車をはじめ、機能の大半がコンピューターを利用してソフトウェアで実現されている組込み製品や制



図1 報道されたITサービス障害の発生件数の推移

御システムにも、社会インフラの重要な役割を担うものが多くあり、これらは、実現する機能の増加と共に複雑化する傾向にある。組込みシステムが急速にIoTに発展しつつある今日では、様々なシステムとの相互接続を前提に信頼性を確保するための技術面や運用管理での更なる工夫が求められている。

従来、ITサービスや組込み製品などの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、その情報はほとんど公開されてこなかった。そのため、当事者以外の同種システム、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開発／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、一個人や一企業でカバーできる範囲には限界がある。そして、その複雑性・多様性が今後ますます拡大していくことは明らかである。このような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は、より多くの人々・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きている。

このような背景から、ITサービスや組込み製品・制御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

「重要インフラITサービス高信頼化部会^{*1}」及び「製品・制御システム高信頼化部会^{*2}」(以下、部会)の活動を通じて障

※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・行政などの重要インフラ分野における情報処理システムの有識者・専門家構成する委員会

※2 製品・制御システム高信頼化部会：重要インフラ分野における製品・制御システムに関する有識者・専門家構成する委員会

害事例を収集し、障害発生の原因分析を行い普遍化した上で、前者で計50件、後者で計35件の教訓を取りまとめ、「情報処理システム高信頼化教訓集 (IT サービス編)



2017年度版^{※3} (以下、教訓集2017)、及び「同(組込みシステム編)2015年度版^{※4}」を公開した。

また、2010年から2017年まで収集蓄積している報道されたシステム障害の一覧及び教訓集2017の各教訓を利用者が検索しやすいように、99件の「注意すべき観点」を整理し、これに基づく分類を行った一覧表を公開した。また、上記の結果をもとに「注意すべき観点」に基づいた障害事例の10種の分類を教訓集2017に掲載した。

3 障害未然防止のための設計知識の整理

組込みシステムを開発する企業の多くは、過去の障害事例(過去トラブル)を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、そこには障害再発を防止するためのノウハウが含まれている。「製品・制御システム高信頼化部会」では、このノウハウを設計知識の形で取り出すことができれば、開発に直接携わる組込みソフトウェア設計者のために役立てられると考え、「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」として公開した。



4 普及展開活動

① 教訓集ダイジェストを用いた普及

システム障害情報共有の普及活動を推進するために、ITサービス編及び組込みシステム編の情報処理システム高信頼化教訓集に収録された教訓を一覧化して、収録内容を容易に検索できるようにした小冊子「情報処理システム教訓集ダイジェスト2017年度版」を作成・公開した。



② 教訓集活用メールマガジンの配信

情報処理システム高信頼化に関する情報「教訓集活用メールマガジン」の配信希望者(約1,300名)に対して、部会委員が寄稿した障害情報共有の取り組み記事(表1参照)や、新たな教訓の解説記事などを毎月配信することにより、教訓活用を促進した。

表1 配信された委員からのメッセージ

記事タイトル	NO.
システム障害のマネジメントについて	10号
プロジェクトのゴールはサーバの火を落とすとき!	11号
サービスを継続的に提供するためには	12号
重要インフラITサービスを支えるための政府の取組	13号
過ちで改めざる、是すなわち過ちという	15号
トラブル対策にも新たなチャレンジを	18号
「情報処理システム高信頼化教訓集」に学ぶ	19号
トラブルは品質改善の種	20号

5 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、7つの分野・地域で、計13の情報共有グループが構築され(図2)、その運営を開始した。また、幾つかのグループについて意見交換会を開催した。



情報共有体制の推進支援、事例情報の提供、必要に応じ共有ツールの提供
IPA

図2 2017年度までに構築された情報共有グループ

6 今後の予定

2018年度以降も引き続き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行う予定である。また、システム障害事例情報の共有については、自律的な情報共有の促進に向けた各種の支援を継続する予定である。

※3 URL: <https://www.ipa.go.jp/sec/reports/20180326.html>
 ※4 URL: https://www.ipa.go.jp/sec/reports/20160331_2.html