教訓を活用した情報システムの類似障害削減

～システム障害事例の分析により得られた教訓の共有～

IPA 社会基盤センター

研究員　村岡 恭昭

本日お伝えしたいこと

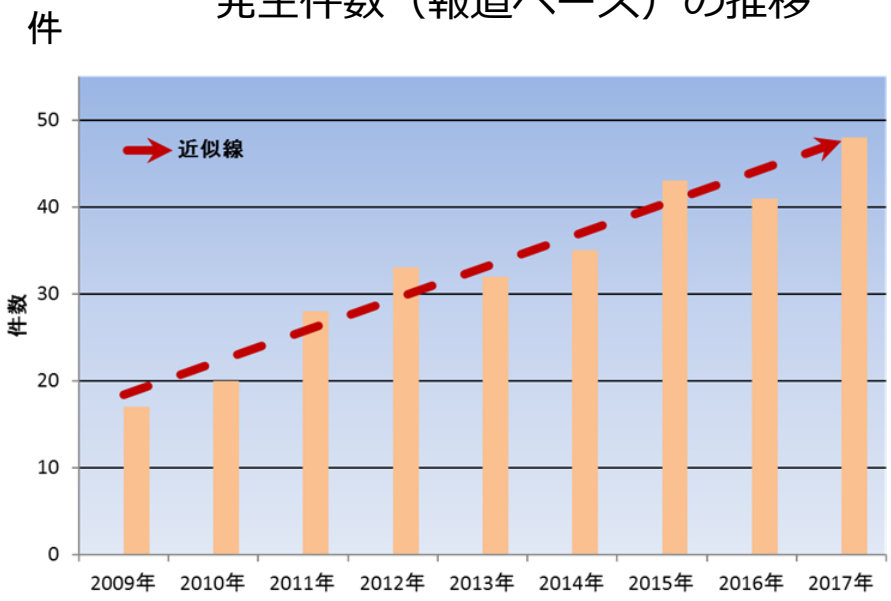
- **ITサービスや組込みシステムの信頼性を向上させる近道は既往障害の再発防止**
- **そのためには他所で何が起きたかを知り未然防止することが必要**
- **教訓集には実際に起きた障害が対策とともに描かれています**

活動の背景：原因が類似した障害が増加

社会に大きな影響を与えた
システム障害の発生件数
2009年調査開始後 増加傾向
新聞やテレビなどのメディアでは，
幾度となく以下のようなニュースが
世間を賑わせている：

- **△△でリコール、国内で数十万台**
  …理由は、制御プログラムに不具合が発見されたためという。
- **○○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。

多大な影響を与えたITサービス障害の
発生件数（報道ベース）の推移



(出典) SEC Journal 情報システムの障害状況

類似障害の発生

教訓共有による障害再発の防止

IPA

<今、世の中で起きていること>

- **多種多様な業界の重要インフラで**
  類似した内容のＩＴシステム障害がたびたび発生
  - **ITサービスや組込み機器の失敗ケースが社会全体で共有されていない**

<どうすればよいのか>

障害事例（実際に起きたこと）を収集

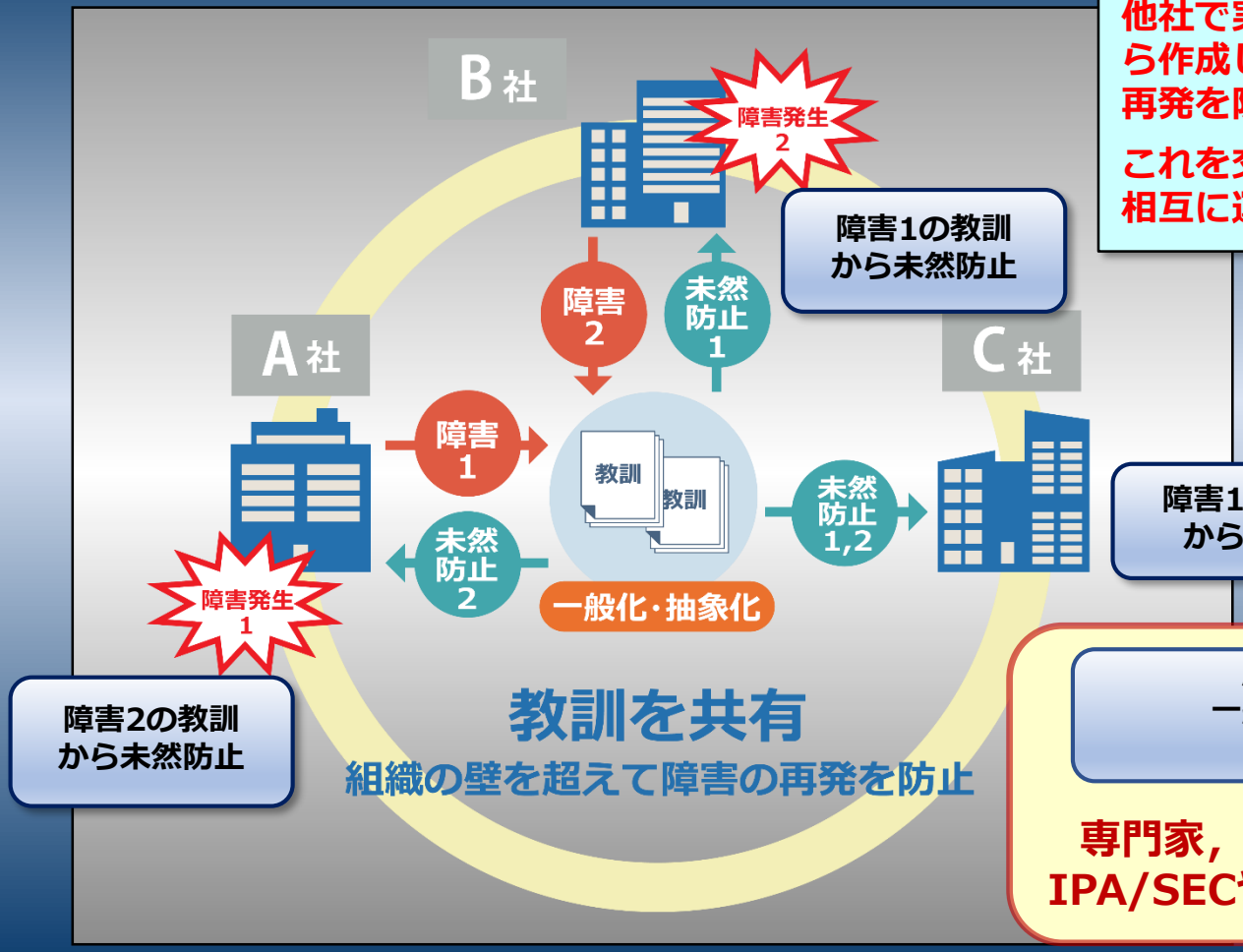
根本原因、再発防止策を分析して教訓化

広く社会で教訓を共有し、
同一原因の障害再発を防止して被害を最小化する

失敗（貴重な教訓）からみんなで学ぶ

教訓共有が目指す姿

障害から得られた教訓の共有による信頼性向上のサイクル



他社で実際に発生した障害事例から作成した教訓をもとに自社での再発を防止する

これを交互に繰り返すことにより、相互に運用品質を向上させる

原因分析・対策検討
一般化・抽象化・普遍化
体系的整理

機密保持等のルール

専門家，有識者のご協力を得て
IPA/SECや業界団体等が共有活動

共有活動の成果物　教訓集

IPA

【参画企業等】
トヨタ自動車(株)、日産自動車(株)
日本電気(株)、(株)日立製作所
三菱電機(株)、横河電機(株)
富士電機(株)、矢崎総業(株)
アイシン精機(株)、矢崎部品(株)
日本電気通信システム(株)
(株)日立産業制御ソリューションズ
三菱電機メカトロニクスソフトウェア(株)
(株)富士通コンピュータテクノロジーズ
オムロンソーシアルソリューションズ(株)
アイシン・コムクルーズ(株)
北陸先端科学技術大学院大学
九州大学、会津大学
(一社)組込みシステム技術協会
(一社)電子情報技術産業協会

特長
① 機密保持ルールの下で詳細情報を収集
② ソフトウェア・エンジニアリングに関する高度な知見を活用して議論
③ 業界・分野によらない普遍化された教訓を作成

※ 2017年度版では8件の新たな教訓や「SECジャーナルに掲載した障害事例の一覧」他を追加

国民生活や社会・経済基盤に関わる「障害情報」を収集

【参画企業等】
(株)三菱東京UFJ銀行
日本生命保険(相)
東京海上日動火災保険(株)
(株)証券保管振替機構
電気事業連合会
松本信号コンサルタント
KDDI(株)
(株)フジテレビジョン
(株)オリジネィション
日本大学
内閣官房情報通信技術総合戦略室
(一社)日本情報システム・ユーザー協会

IPA
製品・制御システム高信頼化部会
組込みシステム分野
[教訓数] 35件
収集した情報を分析し対策を検討
[教訓数] 50件
ITサービス分野
重要インフラITサービス高信頼化部会

普遍化 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

2018年3月26日公開

新着教訓を随時Webで公開
http://www.ipa.go.jp/sec/system/lesson.html

2018年３月時点

教訓集（組込みシステム編）の構成

- **情報処理システム高信頼化教訓集**
  （組込みシステム編）

2016年3月31日
IPA／ソフトウェア高信頼化センターの
サイトからダウンロード公開

PART Ⅰ　教訓集（本編）
PART Ⅱ　障害対策手法・事例集
PART Ⅲ　障害分析手法・事例集
PART Ⅳ　障害分析手法事例解説書

教訓集（ITサービス編）の構成

「情報処理システム高信頼化教訓集」ITサービス編は、
以下の三部で構成

PART Ⅰ：教訓

実際のシステム障害事例をもとに作成された教訓を掲載
・ガバナンス・マネジメントに関する教訓　21件
・技術に関する教訓　29件
個々の教訓に加えて、教訓や報道事例から見えてくる傾向について「ヒューマンエラー」や「システムの高負荷／過負荷」などの観点からの原因や対策についての考察を掲載

PART Ⅱ：障害対策手法

教訓に記載された事項を自組織内で実践するために必要な対策手法を、ガバナンス／マネジメント領域と技術領域のそれぞれについて一覧で掲示

PART Ⅲ：障害分析手法

分析手法を選択する際の参考として、障害原因分析の際によく用いられる分析手法を掲載

「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

https://www.ipa.go.jp/sec/reports/20180326.html

無料でダウンロードできます

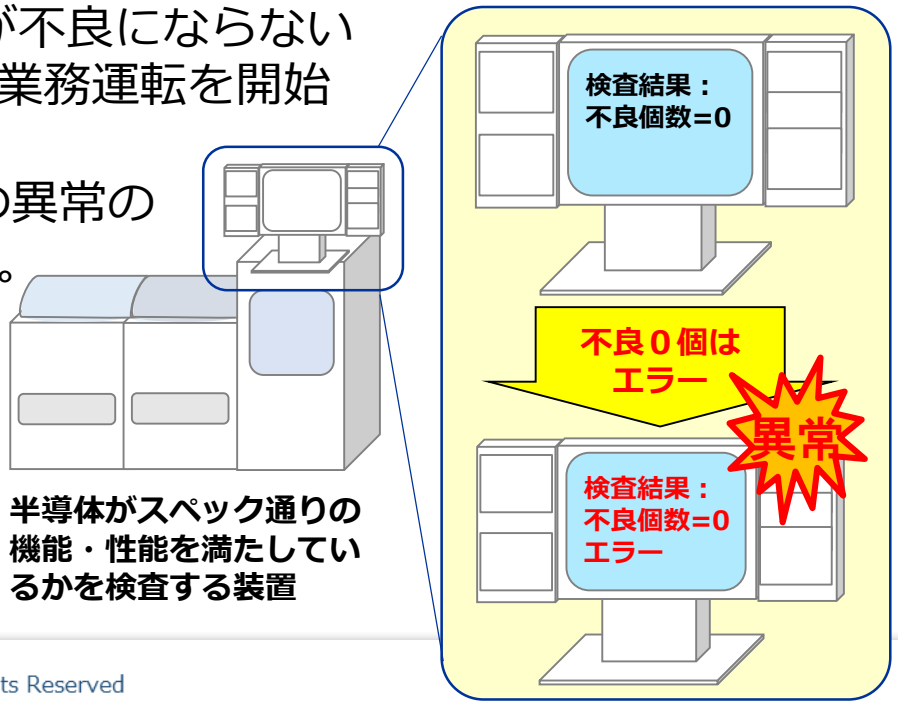
収録された教訓例（組込みシステム編）

No.12 歩留りのある製品の良品／不良品を検査する装置では、全てが良品あるいは、不良品との検査結果は異常と判断すべきである

【事象】半導体の検査では一定の割合で不良品が発生するが、あるとき検査したすべてが良品となった。しかし、それをそのまま良品として後続の検査工程に回したところ、後続の検査工程で通常より多くの不良品が検出された。

【原因】機器の検査時に一時的に検査結果が不良にならないように設定した。そのままの状態で業務運転を開始したため不良０個になった。
検査結果が全て良品なら検査機器の異常の可能性があるとみなしていなかった。

【対処】**良／不良の条件に関わる仕様を見直し（良すぎる結果もエラー）**
- **全て不良品の場合と同様に、全て良品の場合も検査機器の異常を通知するよう修正**



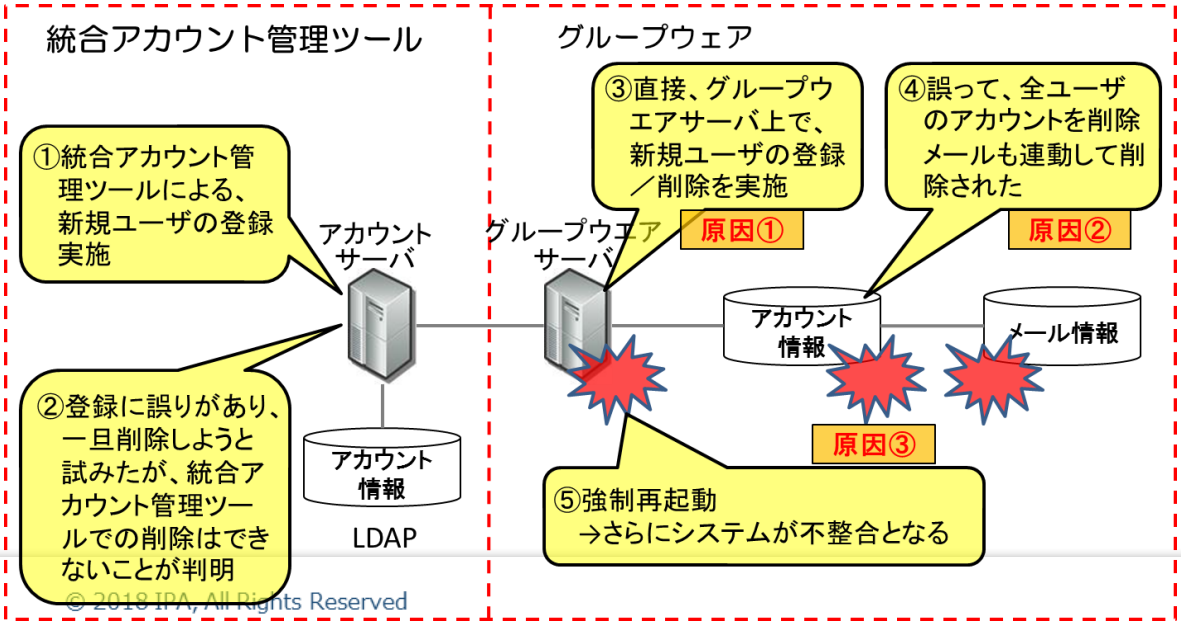
収録された教訓例（ITサービス編）

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！

【問題】運用作業者がグループウェアの全ユーザデータを削除

【原因】不慣れな運用作業者（新人）が独断で規定外の手段（管理ツールを介さないサーバへの直接アクセス）により誤操作（ルール逸脱）
繁忙かつ迅速な処理が求められる環境で、不慣れな作業者は多忙な熟練者に確認・相談できず、自分が遅延の原因になるプレッシャーからルール逸脱
運用チーム内のスキル共有も不十分

【対策】組織的な対策：
- 複数名での作業実施等、ルールを逸脱しない（させない）作業規定の作成
- 作業を受ける余裕があるか等、リスクを考慮した作業受諾の判断基準作成
- チーム内のコミュニケーション強化、スキル移転



教訓を横断的に見た傾向分析

事例から見えてくる傾向

1.ITサービスマネジメント(ITSM)プロセス観点での分類と傾向

2.バックアップ切替え失敗の問題と対策

3.ヒューマンエラーの問題と対策

4.システムの高負荷／過負荷に関する問題と対策

5.「注意すべき観点」に基づく障害の分類

「報道されたシステム障害データの蓄積と公開」と連動

2017年度版で追加

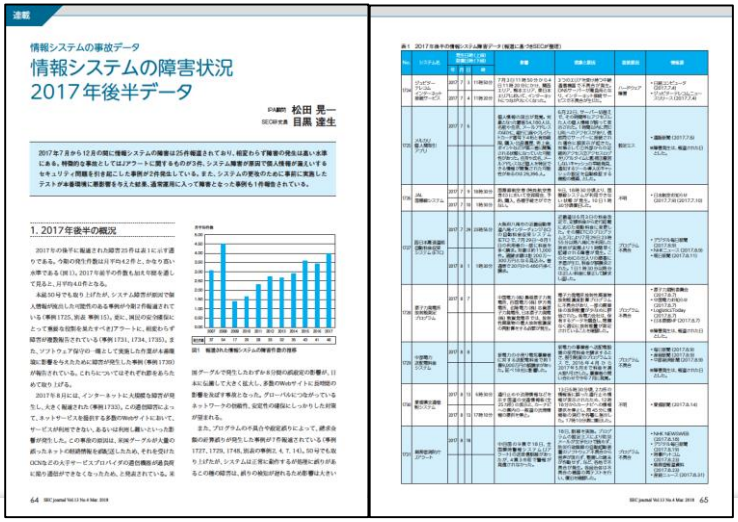
報道されたシステム障害データの蓄積と公開

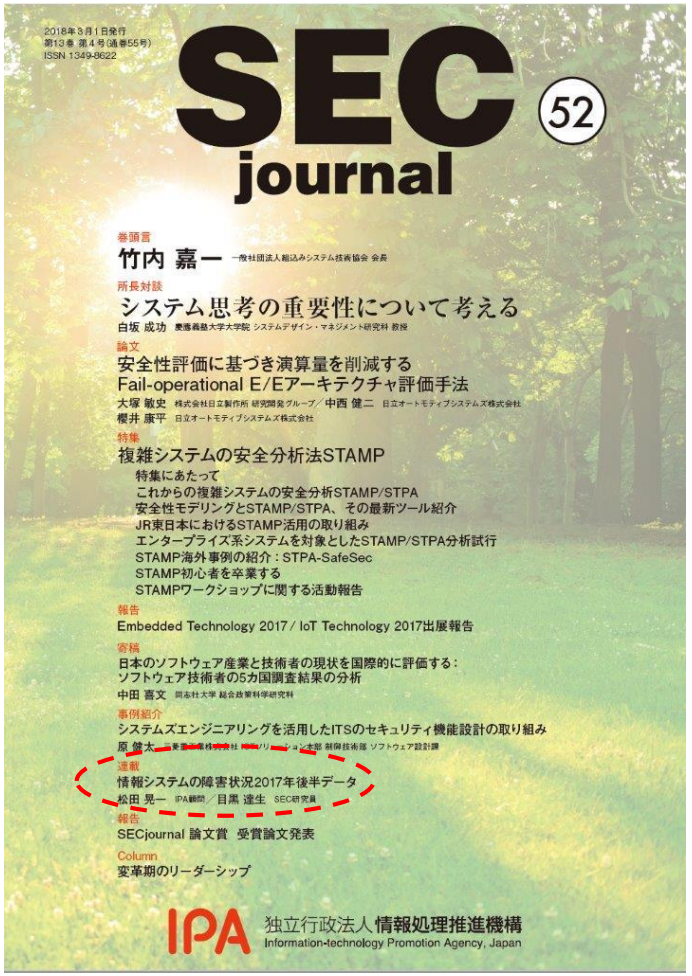
IPA/SECでは2010年から社会に影響を与え全国紙等に報道された情報システムの障害情報を蓄積
これを、季刊誌SEC journalで半年毎に取りまとめ「情報システムの障害状況」として連載

- 過去分をいつでも参照できるよう、一覧をWEB公開

SEC journal 連載：情報システムの障害状況

https://www.ipa.go.jp/sec/system/system_fault.html





報道されたシステム障害データの蓄積と公開

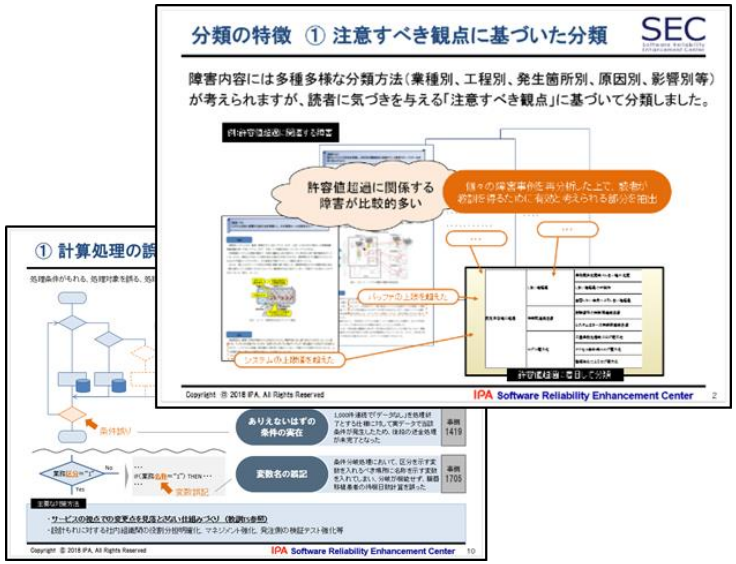
	号数（発行日）	連載「情報システムの障害状況」の内容
9	第40号 （2015年3月1日）	連載：情報システムの障害状況　2014年後半データ 1.2014年後半の概況 2.突発的な大量トラフィックによる事故 3.保守作業にかかわる事故 4.むすび
10	第42号 （2015年9月1日）	連載：情報システムの障害状況　2015年前半データ 1.はじめに 2.2015年前半の概況 3.システム更改を契機とする事故 4.長期間のエラー放置 5.むすび
11	第44号 （2016年3月1日）	連載：情報システムの障害状況　2015年後半データ 1.はじめに 2.2015年後半の概況 3マイナンバー関連事故 4.長期間の不具合放置 5.設計時の常識的事項の考慮漏れ 6.むすび
12	第46号 （2016年9月1日）	連載：情報システムの障害状況　2016年前半データ 1.はじめに 2.2016年前半の概況 3.マイナンバー関連事故 4.長期間の不具合放置 5.環境変化への対応遅れ 6.むすび
13	第48号 （2017年3月1日）	連載：情報システムの障害状況　2016年後半データ 1.はじめに 2.2016年後半の概況 3.システムへのアクセス集中による障害 4.共同利用型のシステムリスク 5.むすび
14	第50号 （2017年9月1日）	連載：情報システムの障害状況　2017年前半データ 1.はじめに 2.2017年前半の概況 3.システム障害に起因するセキュリティ問題 4.業務処理の誤りの長期間見逃し 5.むすび

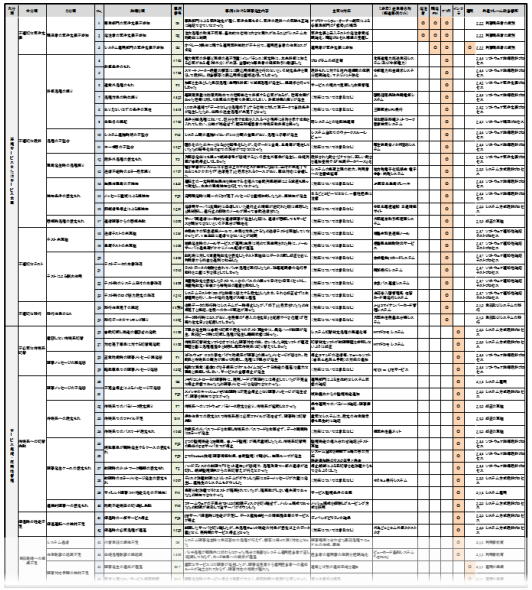
障害件数

No.	システム名	発生日時（上段） 回復日時（下段） 年	月	日	時	影響	現象と原因	直接原因	情報源
1701	りそなHD ATM	2017	1	10	8時45分	ATM利用手数料の誤徴収。過大徴収は、約1万9,000件、計205万円。過小徴収は、約3万9,000件、420万円。	10日午前8時45分から12時59分までに、りそなHD系銀行、コンビニ大手などのATMで、りそな以外のキャッシュカード使用者に、本来108円の手数料を誤って216円徴収。原因は、設定ミス。	設定ミス	・朝日新聞朝刊(2017.1.12) ・日本経済新聞朝刊(2017.1.12) ・りそなホールディングスニュースリリース（2017.1.11）
		2017	1	10	0時59分				
1702	Z会 運用システム	2017	1	11		通信教育講座の一部申し込み不可、教材の印刷や製本が不可など発生。また、最大約10万人に教材を発送できなくなる可能性。	新システムへの移行作業を進めていたところ、障害が発生。受付を3月20日に再開。	システム移行による障害	・Z会プレスリリース(2017.1.30) ・Z会お客様へのご案内HP ・朝日新聞朝刊(2017.1.31) ・日本経済新聞朝刊(2017.1.31)
		2017	3	20					
1703	北海道電力 託送業務システム	2017	1	12		インバランス料金の不具合のため、発電・小売電気事業者などと一般送配電事業者との間の取引に影響が生じた。	電力需要の計画と実績の過不足量（インバランス）を算定する際、本来計算に加える必要のある値が一部欠落。原因は、託送料金制度の変更における情報収集不足と、算定プログラムの作成に際して、仕様確認が不十分だった。2017年3月末までにプログラムの修正を行う。	プログラムの不具合	・日本経済新聞朝刊(2017.1.19) ・北海道電力プレスリリース(2017.1.18) ※障害発生は2016年4月であるが、それが判明した日時に基づき掲載。
1704	中部電力 料金請求システム	2017	1	15		・振込用紙の重複送付［約7,500件］ ・請求書記載の電気使用量等の表示誤り［約1,000件］ ・口座再振替のお知らせ時の金額誤り［約3,000件］ ・請求書等発行遅延［約11万件］ ・高圧受電（6,000V）のお客さまの電気料金を請求書を届けないまま、口座から引き落としてしまった。	1月4日～6日に検針したスマートメーター設置顧客に、振込用紙を重複送付。1月4日～6日に検針した複数契約顧客に、請求書誤記載。12月分の残高不足顧客で、複数契約で次回振替日が1月11日～13日の顧客に、金額誤通知。電気料金請求書等の発送、最大3営業日遅れ。高圧受電（6,000V）の顧客に請求書を届けず、いきなり口座引落を実施。原因/対策は、①開発時の仕様漏れ、設計漏れ、テスト項目漏れ、検出漏れ→組織間の責任、役割分担の明確化。体制、マネジメントの強化。②運用に伴う、誤認、認識相違→事業者と委託会社の役割の明確化と情報共有。	プログラムの不具合 運用ミス	・朝日新聞電子版(2017.1.15) ・日本経済新聞朝刊(2017.1.16) ・中部電力プレスリリース（2017.1.15、.1.19、1.21、1.27） ※障害発生は2016年12月であるが、それが判明した日時に基づき掲載。
1705	日本臓器移植ネットワーク 患者検索システム	2017	1	27		移植患者を選ぶ新しい検索システムに不具合があり、2016年10月以降、システム導入後にあった脳死臓器提供20例のうち、3例の心臓移植で選定ミスがあった。提供を受けるはずだった2人が移植を受けられず、1,000日以上待機となった。	病院から指摘があり、患者の治療状況の情報修正時、待機日数が誤って長く計算されるプログラムミスが発覚。対策は、①CIOとPMOを開設し、情報システムの計画、保守等を行う、②熟知したコーディネーターを配置する、③新システムは、旧システムとの比較検証を行った後、コーディネーターによる確認後再稼働する、④課題の共有や安全管理室の機能を強化する。	プログラムの不具合	・朝日新聞朝刊(2017.1.28、3.30) ・読売新聞朝刊(2017.1.28) ・日本経済新聞朝刊(2017.1.28、3.30) ・日本臓器移植ネットワーク 第三者調査チーム報告書(2017.3.29) ※障害発生は2016年10月であるが、それが判明した日時に基づき掲載。

「注意すべき観点」に基づいた障害事例の分類

「情報処理システム高信頼化教訓集」およびSEC journalに掲載されたシステム障害の事例一覧に掲載された障害のポイントや全体像がつかめるよう、「注意すべき観点」に基づいて分類した障害事例の一覧を公開





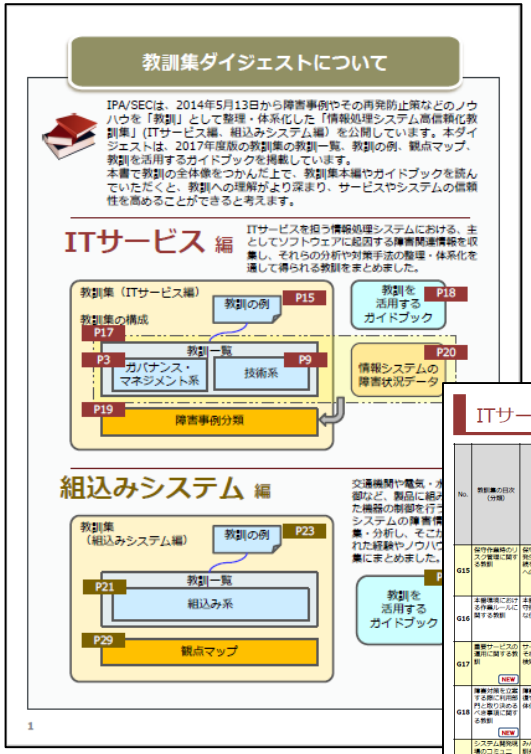
◆ **「重要インフラ分野のシステム障害への対策」のページからダウンロードが可能です。**

「注意すべき観点」に基づいた障害事例の分類

https://www.ipa.go.jp/sec/system/index.html#shougaijirei

教訓集ダイジェスト2017年度版

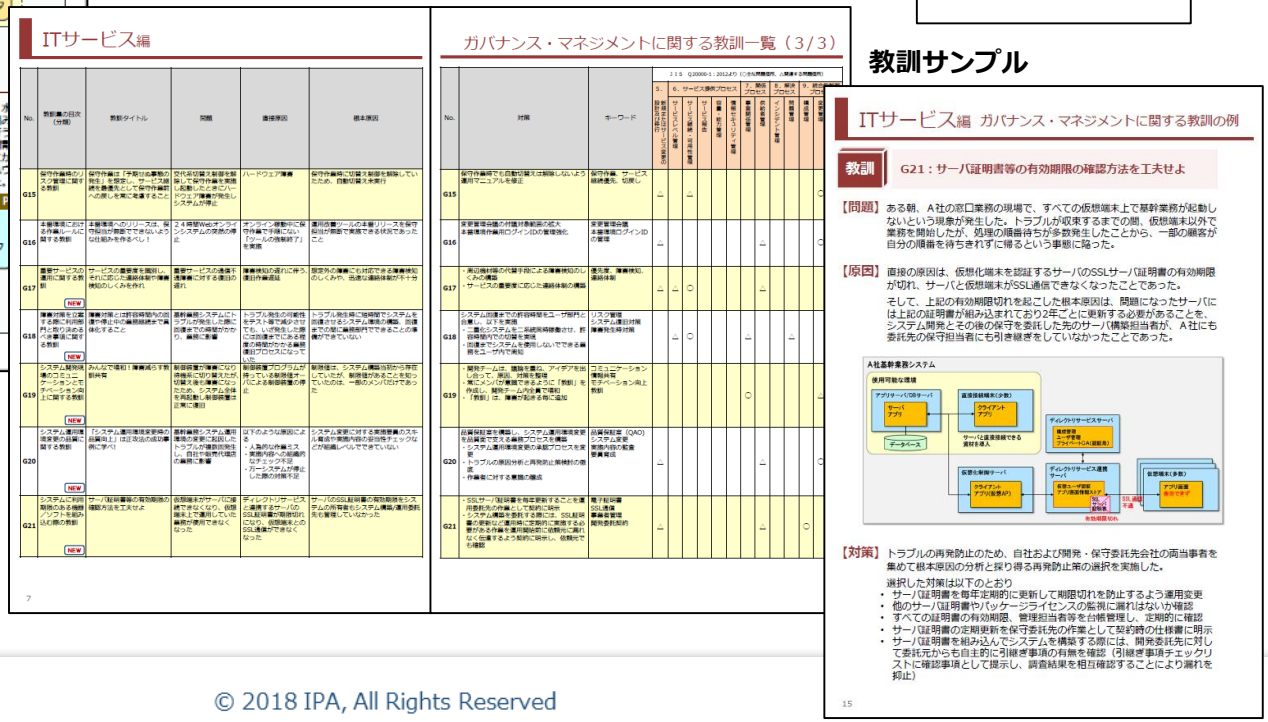
目次



ITサービス、組込みシステムの教訓集に掲載された教訓を一覧で紹介

表紙

教訓サンプル



メーリングリストで更新情報を配信

IPAが公開する新着教訓や、新聞や雑誌等で報道されたシステム障害情報から読み取れる教訓等についてお知らせするメールマガジン（教訓集活用メルマガ）を発信しています

配信をご希望の方は是非ご登録を！

「情報処理システム高信頼化教訓集（ITサービス編）」をより有効にご活用いただくためのメールマガジンの登録について
https://www.ipa.go.jp/cgi-bin/enquete/registEnquete.cgi?EID=55387577eb35c55e7ca118cb3c043e85

まとめ：本日お伝えしたこと

- ITサービスや組込みシステムの信頼性を向上させる近道は既往障害の再発防止
- そのためには他所で何が起きたかを知り未然防止することが必要
- 教訓集には実際に起きた障害が対策とともに描かれています
  - ◆ITサービス50編、組込みシステム35編の教訓を収録
  - ◆障害の傾向分析
    - 「注意すべき観点」に基づいた障害事例の分類
  - ◆報道されたシステム障害事例の蓄積と公開
  - ◆教訓集活用メールマガジンで最新情報をお届け

是非ご活用下さい

おわりに：IPAからのご提案

同業種の方々と共有グループを作り
事例を普遍化した教訓集には載らないような

グループに特有のシステム障害事例や
再発防止策を共有して

グループでシステム障害削減を目指しませんか

- **IPA/SECでは定期的に障害分析～再発防止策検討～教訓作成の演習セミナーを実施しています**
- **IPA/SECがグループ作りを支援します**

「ITSS+（プラス）」のお知らせ

第４次産業革命に向けた

スキル変革の羅針盤　ITSS+

ITSS＋

- IoTソリューション領域
- アジャイル領域
- データサイエンス領域
- セキュリティ領域

学び直し　スキル強化

- ITスキル標準（ITSS）
- 情報システムユーザースキル標準（UISS）

詳しくはこちら！

ITSS+

http://www.ipa.go.jp/jinzai/itss/itssplus.html

ご清聴ありがとうございました。