IPA Better Life with IT

実際に起きた障害から学ぶ

情報処理システム高信頼化 教訓集 ダイジェスト

サービスやシステムの信頼性を高めるために

ITサービス 編
組込みシステム 編

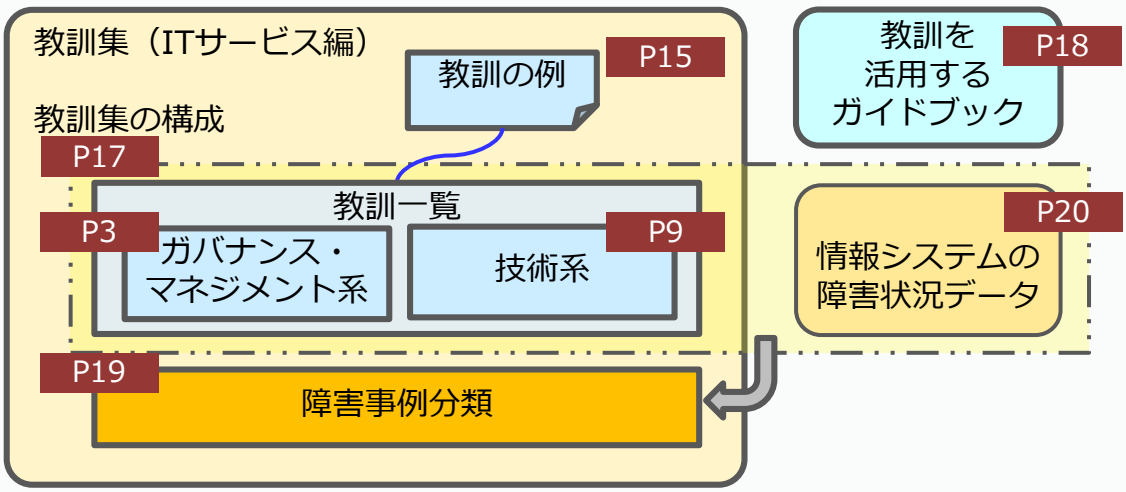
独立行政法人情報処理推進機構
社会基盤センター

教訓集ダイジェストについて

IPA 社会基盤センターでは、重要インフラの各分野で**実際に発生した障害をもとに**、その障害の発生に至った根本原因や再発防止策などを分析した結果を「教訓」として整理・体系化した「情報処理システム高信頼化教訓集」(ITサービス編、組込みシステム編）を公開しています。本ダイジェストは、作成した教訓の一覧、教訓の例、観点マップ、教訓を活用するガイドブックを掲載しています。
本書で教訓の全体像をつかんだ上で、教訓集本編やガイドブックを読んでいただくと、教訓への理解がより深まり、サービスやシステムの信頼性を高めることができます。

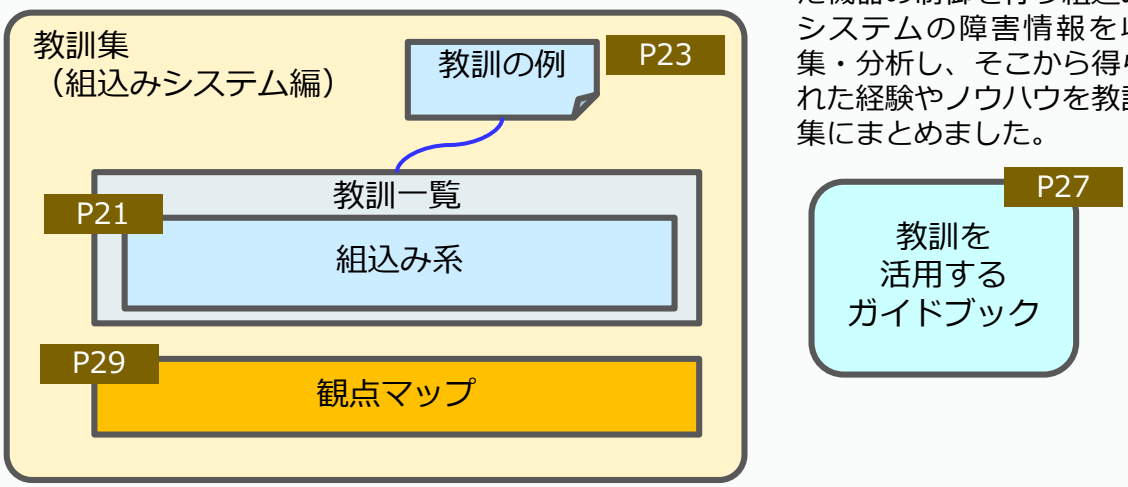
ITサービス 編

ITサービスを担う情報処理システムにおける、主としてソフトウェアに起因する障害関連情報を収集し、それら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まとめました。



組込みシステム 編

交通機関や電気・水道の制御など、製品に組み込まれた機器の制御を行う組込みシステムの障害情報を収集・分析し、そこから得られた経験やノウハウを教訓集にまとめました。

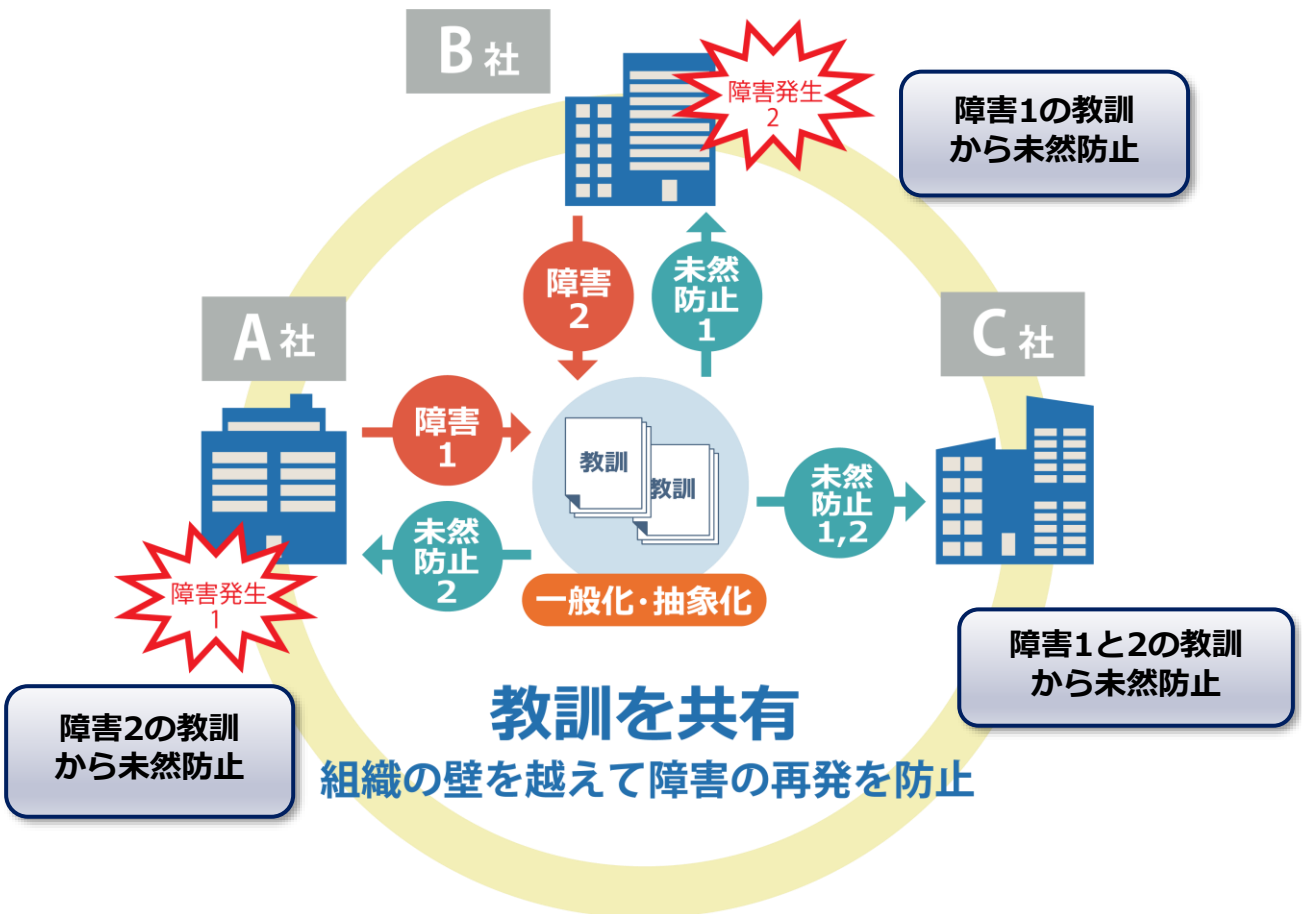


サービス・システム高信頼化への対策

経験を共有し、みんなの力でIT社会の安全・安心を築くしくみ

私たちIPAは、国民生活や社会・経済基盤を支える情報処理システムの信頼性向上を目標とし、以下の活動を行いました。

- システムの障害事例情報の分析や対策手法を整理・体系化して、これから導かれた「教訓」を作成する
- 自社内の障害事例を分析し教訓として整理・活用する活動を広く普及させるためのガイドブックを作成する
- 「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」を構築する
- 「教訓」を分野横断で共有するため、障害情報や教訓の共通様式と公開に際しての機密保持などの「ルール」を取りまとめる
- 類似障害の再発防止に向け、システム開発や運用・管理の継続的なプロセス評価・改善手法を取りまとめる



ITサービス編

No.	教訓集の目次（分類）	教訓タイトル	問題	直接原因	根本原因
G1	事業部門と情シス部門の役割分担に関する教訓	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」を作ることが大切	急激に増大したシステム開発により、システムトラブルが多発	・ビジネス側の要件の確定が遅延 ・多くの要件変更発生 ・要件を最終的に文書で確認未実施	上流の要件定義局面でのコミュニケーション・ギャップ
G2	発注者の要件定義責任に関する教訓	発注者は要件定義に責任を持ってシステム構築に関わるべし	本稼働後に基本的な仕様に漏れ	要件定義漏れ	要件定義重視の開発プロセスでなっておらず、要件定義はベンダ任せ
G3	上流工程での運用部門の関与に関する教訓	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	オペレータの操作ミス多発 オンライン発注業務のデータ入力ミスによる中断	要件定義段階のオペレーション要件検討不足により 入力ミスの抑止の設計に漏れ	運用者が企画・要件定義に不参加
G4	障害発生時連絡の情報共有に関する教訓	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	システムサービスの数時間停止	メモリコントローラの障害	運用担当者が察知した異常を、保守担当者が異常なしと誤認
G5	共同利用システムの業務処理量予測に関する教訓	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	負荷集中によるシステムダウン	負荷増大を起因とするミドルウェアのバグ顕在化	共同利用システムにおける各社の処理件数予測が不十分
G6	作業ミス、ルール逸脱の問題に関する教訓	作業ミスとルール逸脱は、個人の問題でなく、組織の問題！	グループウェアの全ユーザデータの削除	一部ユーザを削除する際の、運用者の作業誤り	繁忙な環境下で、不慣れな運用者が早く処理を行わざるを得ず、組織マネジメントが不足
G7	クラウドサービス利用時の障害対応体制に関する教訓	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	基幹業務システムの１日停止	負荷分散装置の障害発生	・運用時のトラブル管理体制が未決定 ・ユーザと(クラウド)ベンダの役割分担が不明確 ・ベンダに当該装置の専門家がおらず、情報の収集が不十分
G8	共同利用システムの利用者間情報共有に関する教訓	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	（同上）	（同上） ※ 第三者も利用する負荷分散装置のため再起動不可	ベンダーおよび共同利用者間の障害発生時の連絡体制が未整備

ガバナンス・マネジメントに関する教訓一覧（1/3）

No.	対策	キーワード	ＪＩＳ　Q20000-1：2012より（○主な問題個所、△関連する問題個所）												
			5.	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		
			新規またはサービス変更の設計及び移行	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	システム開発におけるビジネスサイドの役割と責任の明確化	アプリケーション・オーナー制度、要件定義、受入れテスト	△						○						
G2	・上流工程重視の開発プロセスに変更 ・要件定義書と受入テストは発注者の責任とすること	上流工程、要件定義、発注者責任	○							△					
G3	・運用者の役割分担表作成 ・プロジェクト開始前の関係者レビュー	運用設計、企画、要件定義、上流工程	○	△											
G4	・オペレーションマニュアル改善 ・上位役職者の報告ルール追加 ・確認手順と確認項目の定義明確化 ・フェールソフトの仕組み導入 ・教育、訓練実施	システム運用、異常時、体制				△				△	○				
G5	・利用各社による運営協議会の設置 ・キャパシティプラニングを含めた利用各社の責任明確化	共同利用、業務量予測、運営協議会、キャパシティプランニング					○		△						
G6	・作業を受ける場合の判断基準作成 ・ルールを逸脱しない作業規定の作成	作業ミス、ルール逸脱、グループウェア、マネジメント、運用ルール											△	○	△
G7	・障害対応体制の強化 ・契約におけるサービスレベル定義 ・クラウド事業者とサードパーティ事業者間の障害対応体制強化	仮想化、共同利用、トラブル管理				△			△	△	○				
G8	・障害復旧時の停止/再起動単位と利用者影響の明確化 ・システム停止/再起動の条件や責任についてのSLA合意 ・利用者間の非常時緊急連絡体制の確立	仮想化、共同利用、情報共有							○				△		

ITサービス編

No.	教訓集の目次（分類）	教訓タイトル	問題	直接原因	根本原因
G9	非常時代替事務マニュアルに関する教訓	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	（同上） ※ システム停止時に顧客対応が十分にできなかった	（同上）	過去にシステム障害が発生したことがなく、システムが利用できない前提での業務マニュアルが未整備
G10	システム動作の疑義問合せがあった場合の対応に関する教訓	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！	コールセンタへの通話着信が即切断される事象が断続的に数時間発生	一部の回線基板の送信バッファのオーバフロー	固定回線用基板の廃止に伴う回線試験用設定の変更漏れ 時々発生していたため、問合せがあったものの障害発生の認識の遅れ
G11	システムの運用・保守に関する教訓	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	システム停止時間は長時間に及び、顧客向けサービスが終日全面停止	・DDM(Disk Drive Module)のハード故障 ・入出力制御機能の不具合 ・ミラーリングの誤設定	・製品の不具合情報について、ベンダから情報連携が未実施 ・障害発生時の対応マニュアル等が十分整備されていなかったため、関係者で意思疎通をはかるのに多くの時間を消費
G12	キャパシティ管理のマネジメントに関する教訓（その１）	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ともに、管理項目としきい値を設定してPDCAサイクルをまわすべし	システムにある日、処理能力を超えた注文が殺到し、サービスの時間が短縮	一般的なデータ量の増加に加えて、想定を超える突発的な事象によるデータ量の急増が発生	業務部門とIT部門とのキャパシティの合意形成やキャパシティの管理方法が不明確
G13	キャパシティ管理のマネジメントに関する教訓（その２）	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	（同上）	（同上）	システムが一連の系としてコントロールされておらず、相互の連携データ、連携時間帯等について統一した管理がされていなかったこと
G14	キャパシティ管理のマネジメントに関する教訓（その３）	設計時に定めたキャパシティ管理項目は、環境の変化にあわせて見直すべし	（同上）	（同上）	設計時に定めた監視する時間間隔（キャパシティ管理項目）では十分なシステム監視が不可

ガバナンス・マネジメントに関する教訓一覧（2/3）

No.	対策	キーワード	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
G9	・システム利用不可時の代替業務マニュアルの作成	仮想化、共同利用、業務継続			△				○						
G10	・交代系に切替えて復旧 ・回線試験用の設定を修正 ・監視コンソールのアラート表示設定 ・通信事業者との情報連携の改善 ・原因調査より復旧作業を優先するようマニュアルを改訂	コールセンタ、デジタルＰＢＸ、通信事業者との連携、バッファオーバフロー							△		○				
G11	・DDM保守運用の改善 ・システムの重要度に応じた修正プログラム適用ルールの見直し ・保守作業におけるシステムの重要度に応じたチェック体制の見直し ・システムの重要度に応じたシステム保守における運用面、体制面の見直し	システム保守、優先度、システム障害の対策本部			△								○		
G12	・キャパシティ管理はシステムごとに責任を持つ業務部門を決め、適材適所で役割分担し、コミュニケーションをとる協力体制で実施 ・過去の実績をもとに算出したルールに基づいて性能を拡張 ・システム毎に管理項目としきい値を設定し、キャパシティの拡張方法や拡張限界等を明確化 ・業務部門が日々の業務量やビジネス環境などから将来予測を行い、IT部門がシステムの拡張を検討	キャパシティ管理、マネジメント、業務部門とIT部門との合意形成			△		○								
G13	・キャパシティ管理に関する課題を解決し、全社的なキャパシティ管理業務を担う会議体を作り、システム連携情報を管理 ・個別システムのキャパシティ計画の変更は全システムが参加するキャパシティ管理会議でレビューし、システム連携情報の変更と影響の有無を確認、連携して対処	キャパシティ管理、マネジメント、キャパシティ管理会議			△		○							△	
G14	・キャパシティ計画の修正と、設定したしきい値の見直し実施 ・見直した内容は、次世代システムのキャパシティ管理のインプットの課題として、開発時の要件定義への組み入れ	キャパシティ管理、マネジメント、次世代システムのインプット、PDCA			△		○								

ITサービス編

No.	教訓集の目次（分類）	教訓タイトル	問題	直接原因	根本原因
G15	保守作業時のリスク管理に関する教訓	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	交代系切替え制御を解除して保守作業を実施し起動したときにハードウェア障害が発生しシステムが停止	ハードウェア障害	保守作業時に切替え制御を解除していたため、自動切替え未実行
G16	本番環境における作業ルールに関する教訓	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！	２４時間Webオンラインシステムの突然の停止	オンライン稼動中に保守作業で手順にない「ツールの強制終了」を実施	運用改善ツールの本番リリースを保守担当が無断で実施できる状況であったこと
G17	重要サービスの運用に関する教訓	サービスの重要度を識別し、それに応じた連絡体制や障害検知のしくみを作れ	重要サービスの通信不通障害に対する復旧の遅れ	障害検知の遅れに伴う、復旧作業遅延	想定外の障害にも対応できる障害検知のしくみや、迅速な連絡体制が不十分
G18	障害対策を立案する際に利用部門と取り決めるべき事項に関する教訓	障害対策とは許容時間内の回復や停止中の業務継続まで具体化すること	基幹業務システムにトラブルが発生した際に回復までの時間がかかり、業務に影響	トラブル発生の可能性をテスト等で減少させても、いざ発生した際には回復までにある程度の時間がかかる業務復旧プロセスになっていた	トラブル発生時に短時間でシステムを回復させるシステム環境の構築、回復までの間に業務部門でできることの準備ができていない
G19	システム開発現場のコミュニケーションとモチベーション向上に関する教訓	みんなで唱和！障害減らす教訓共有	制御装置が障害になり待機系に切り替えたが、切替え後も障害になったため、システム全体を再起動し制御装置は正常に復旧	制御装置プログラムが持っている制限値オーバによる制御装置の停止	制限値は、システム構築当初から存在していたが、制限値があることを知っていたのは、一部のメンバだけであった
G20	システム運用環境変更の品質に関する教訓	「システム運用環境変更時の品質向上」は正攻法の成功事例に学べ!	基幹業務システム運用環境の変更に起因したトラブルが複数回発生し、自社や販売代理店の業務に影響	以下のような原因による ・人為的な作業ミス ・実施内容への組織的なチェック不足 ・万一システムが停止した際の対策不足	システム変更に対する実施要員のスキル育成や実施内容の妥当性チェックなどが組織レベルでできていない
G21	システムに利用期限のある機器／ソフトを組み込む際の教訓	サーバ証明書等の有効期限の確認方法を工夫せよ	仮想端末がサーバに接続できなくなり、仮想端末上で運用していた業務が使用できなくなった	ディレクトリサービスと連携するサーバのSSL証明書が期限切れになり、仮想端末とのSSL通信ができなくなった	サーバのSSL証明書の有効期限をシステムの所有者もシステム構築/運用委託先も管理していなかった

ガバナンス・マネジメントに関する教訓一覧（3/3）

No.	対策	キーワード	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
G15	保守作業時でも自動切替えは解除しないよう運用マニュアルを修正	保守作業、サービス継続優先、切戻し	△		△									○	
G16	変更管理会議の付議対象範囲の拡大 本番環境作業用ログインIDの管理強化	変更管理会議 本番環境ログインIDの管理	△							△				○	△
G17	・周辺機材等の代替手段による障害検知のしくみの構築 ・サービスの重要度に応じた連絡体制の構築	優先度、障害検知、連絡体制	△	△	○					△					
G18	システム回復までの許容時間をユーザ部門と合意し、以下を実施 ・二重化システムを二系統同時稼働させ、許容時間内での切替を実現 ・回復までシステムを使用しないでできる業務をユーザ内で周知	リスク管理 システム復旧対策 障害発生時対策		△	○				△			△			
G19	・開発チームは、議論を重ね、アイデアを出し合って、原因、対策を整理 ・常にメンバが意識できるように「教訓」を作成し、開発チーム内全員で唱和 ・「教訓」は、障害が起きる毎に追加	コミュニケーション 情報共有 モチベーション向上 教訓							○					△	
G20	品質保証室を構築し、システム運用環境変更を品質面で支える業務プロセスを構築 ・システム運用環境変更の承認プロセスを変更 ・トラブルの原因分析と再発防止策検討の徹底 ・作業者に対する意識の醸成	品質保証室（QAO） システム変更 実施内容の監査 要員育成	△							△				○	△
G21	・SSLサーバ証明書を毎年更新することを運用委託先の作業として契約に明示 ・システム構築を委託する際には、SSL証明書の更新など運用時に定期的に実施する必要がある作業を運用開始前に依頼元に漏れなく伝達するよう契約に明示し、依頼元でも確認	電子証明書 SSL通信 事業者管理 開発委託契約	△							△			○		△

ITサービス編

No.	教訓集の目次（分類）	教訓タイトル	問題	直接原因	根本原因
T1	フェールソフトに関する教訓	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）	オンラインの二重化したシステムでサーバの稼働系と待機系が同時に稼働し不整合が発生	ミドルウェアとOSの潜在バグ	障害が発生したサーバが自動停止せず
T2	システム全体を俯瞰した対策に関する教訓	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！	制御系システムの下位システムにある制御装置の稼働系に故障発生切替えも失敗	下位の制御装置の稼働系のハードディスクの機器故障「リセット通知」が断続的に発生	下位の中で自律した動きを実施し、下位での障害が生じた場合、上位が下位の監視・制御を行う必要があったが、そのいずれにも不具合が潜在
T3	テストパターンの整備に関する教訓	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！	A列車が出発していった後、B列車は、信号機が「進入」を表示しなかったため、駅の手前で停止	列車制御システムのソフトウェアのバグ	・有識者（ベテラン社員を含む）による機能確認を行っても、まだ洗い出せていない機能が存在 ・列車の動き、システムの動作などを総合的にテストできる環境がない
T4	システム環境の変化への対応に関する教訓	システム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！	運行ダイヤの修正情報一覧を表示する管理センタの画面表示が全て消えてしまった	変更入力による「修正箇所」がシステムの上限値を超えたため、一覧画面表示を停止	システムに大きな変化点（この場合、予測時間、列車運転本数）があったにも関わらず、それを見逃していた
T5	サービス視点での変更管理に関する教訓	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！	本店ホスト／サーバからハンディ・ターミナルに転送される請求書に誤った金額が表示	使用料請求データの符号判定処理で、調整額を減算すべきところを加算処理実施	システムをサービスの視点で見渡した変更管理が不十分
T6	本番環境とテスト環境の差異に関する教訓	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	テスト環境での事前確認の時は問題が生じなかったが、本番環境では障害発生	オンライン実施時にのみ発生するデータベース・パッケージのバグ	テスト環境と本番環境の差異が明確になっていなかったため、事前テストにおける環境差異の影響の把握が不十分
T7	バックアップ切替え失敗に関する教訓	バックアップ切替えが失敗する場合を考慮すべし	冗長化構成を取っていても、障害時、バックアップ切替えが正常に機能せず	稼働系へのソフトウェアのパラメータ設定変更を行った時、待機系へのパラメータ設定変更の漏れ	・待機系システムを本番運用の重要な機能であるとの観点が不足 ・日常の運用で待機系システムの検証が不十分
T8	仮想化時の運用管理に関する教訓	仮想サーバになってもリソース管理、性能監視は運用の要である	システムサービスの数時間停止	仮想サーバ内での作業対象誤りによる特定論理ボリュームの容量枯渇	仮想環境に移行しても、運用の要であるリソース管理や性能監視が重要であることの理解不足
T9	不測事態発生への備えに関する教訓	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	システムサービスの一時停止	通信障害時のタイムアウト検出機能の潜在不良が顕在化	フルメッシュ構成のリスクを十分に考慮していないまま採用
T10	共有ディスクのメッシュ接続に関する教訓	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	システムサービスの一時停止	ファームウェアのバグによる障害がシステム全体に波及して、全サーバがダウン	フルメッシュ構成のリスクを十分に考慮していないまま採用
T11	サイレント障害に関する教訓	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	システム応答速度の低下	負荷分散装置のファームウェアの不具合	サービス監視条件が妥当でなく、利用者から指摘を受けるまで障害に気づかず

技術に関する教訓一覧（1/3）

No.	対策	キーワード	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
T1	障害が発生した時は関連する部分をシステムから積極的に切り離す仕組みに変更（フェールソフト）	サーバの二重化、切替え、フェールソフト、切り離し			○								△		
T2	下位システムだけでの対策「蟻の目」対策だけでなく、「システム全体を俯瞰した鳥の目」対策として、上位システムからの対策実施	制御系システム、上位システム、下位システム、サーバの二重化、切替え					△						○		
T3	・一度設計された「機器の動き」のパターンを知識データベースとして蓄積 ・現実の制御装置のプロセスを可視化し、「モデル」化（モデリング）し、シミュレーションシステムを作成	制御系システム、暗黙知、形式知、知識データベース、シミュレーション	○	△										△	
T4	制御系システムでの変化点は、一般的なシステムの仕様変更の他に、対象時間、対象機器の動き、機器数の変化なども含むが、この変化を見逃さない仕組み作り	制御系システム、変化、変化点、変化点管理、上限値、管理指標		△	○		△						△	△	
T5	・サービスの視点での変更点を見落とさない仕組みの構築 ・システム全体のプログラムの整合性、データの整合性、テスト仕様の整合性を保つための変更管理実施	サービス系システム、サービスの視点、変更管理、品質管理責任、整合	△											○	
T6	・テスト／本番環境の差異の明確化 ・事前に確認できない項目は、関係者間でリスク分析実施 ・リスク対策やコンティンジェンシープランを立案 ・ステークホルダでリスク共有する体制作り ・大きいリスクは経営トップが判断	サービス系システム、テスト環境、本番環境、差異分析、パッチ管理、リスク分析、リスク対策											○	△	
T7	・稼働系、待機系のソフトウェアパラメータの確認、プログラムバージョン管理を徹底 ・障害訓練の実施 ・復旧のための手順を明確化 ・障害復旧訓練の実施	バックアップ切替え、切替え失敗、復旧失敗、障害訓練、復旧手順			○		△								
T8	・物理サーバを仮想サーバに移行する際のリソース管理、性能監視プロセスの策定 ・仮想化によるオーバーヘッド増大の見積り	仮想サーバ、リソース管理、性能監視					○						△		
T9	・フルメッシュ構造を見直し、局所障害が全サーバに波及しないようにグループから成る構成に変更	振分制御、バッファオーバーフロー、検証、供給者、サービス提供者			○								△		
T10	・フルメッシュ構造を見直し、局所障害が全サーバに波及しないようにグループから成る構成に変更	メッシュ構成、NAS、フルメッシュ、波及、グルーピング			△								○		
T11	・サービス監視条件の変更 ・インバリアント分析技術（平常時に変化しない関係を自動的に学習）の活用 ・ビッグデータ分析技術の応用(SyslogやSNS分析など)	サイレント障害、サービス監視、負荷分散装置、(早期)検知、つぶやき		○			△								

ITサービス編

No.	教訓集の目次（分類）	教訓タイトル	問題	直接原因	根本原因
T12	互換部品の入れ替えに関する教訓	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！	制御系システム全体の動作停止	HDDとSSDの起動時性能の差異を見逃したこと	SSDへの交換時に、HDDと互換性がある仕様になっていると誤認してテストが不十分
T13	業務シナリオテストに関する教訓	利用者の観点に立った、業務シナリオに即したレビュー、テストが重要	特定時間帯にWebサイトのサービスでエラー発生	システム間の連携タイミングに15分間の差異があり、この間の処理に矛盾が発生	システム間の連携に関する仕様が、全体設計から個別システム設計に正しく引き継がれず、そのまま実装されたため
T14	Webページ更新時の性能に関する教訓	Webページ更新時には、応答速度の変化等、性能面のチェックも忘れずに	Webサイト上の特定サービスの応答遅延	コンテンツリニューアルの際に、ダウンロードサイズが約4倍に増大	コンテンツの管理は各担当業務部門に任されており、IT観点からの評価実施のルール漏れ
T15	データの一貫性確保に関する教訓	緊急時こそ、データの一貫性を確保するよう注意すべし	Webサービスにおける顧客分類判定の誤り	顧客分類の判定ロジック変更時に顧客データの不備が判明し、その対応時に一部データの修正漏れ発生	・修正が緊急を要するものであったため、影響範囲の事前調査不十分 ・修正作業及び関係各所への報告に意識が集中し、引継ぎが疎か ・原本と複製の対応表等の未整備
T16	修正パッチの適用に関する教訓	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	基幹業務システムの１日停止	負荷分散装置の障害発生	負荷分散装置のファームウェアの修正パッチが1か月前に公表されていたが、その適用の遅れ
T17	定期的な再起動に関する教訓	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！	（同上）	（同上）	・負荷分散装置が8か月以上連続運転状態であり、再起動は未実施 ・再起動をしていれば、バグの顕在化はなかった可能性あり
T18	既存システムとのデータ連携に関する教訓	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	オンラインサービスの遅延、停止、サービス明細の欠落	特別な事象を契機とする処理集中のため、夜間バッチが異常終了	携帯電話に対応した新しいシステムと既存システムを接続した際の全体整合チェックが不十分
T19	RDBMSのクエリ最適化機能に関する教訓	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！	システム応答速度の低下	RDBMSのSQL応答遅延	RDBMSの自動最適化機能によるフルスキャンの発生
T20	パッケージ製品の機能カスタマイズに関する教訓	パッケージ製品の機能カスタマイズはリスクを認識し特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	コールセンタ業務で通話着信障害	制御ソフトの無限ループ発生	パッケージ製品のカスタマイズによる不具合の内包
T21	運用保守で起きる作業ミスに関する教訓	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！！	依頼コールの転送ミスによる現場の混乱	GW増設時のシステム設定値の作業ミス	・作業者が作業ミスを起こすような状況、環境に置かれたこと ・作業指示者が、作業者の実行結果をきちんと確認していなかったこと
T22	バッファプールの管理に関する教訓	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	予期しない予約システムの受付停止	トランザクション集中に伴うバッファのオーバフロー	バッファの滞留状況の監視がされていない
T23	障害監視機能のあり方に関する教訓	障害監視は、複数の観点から実装し、障害の見逃しを防げ！	基幹業務システムの停止	データベースサーバ同期通信用L3スイッチの動作不安定	スイッチの故障を検知できず待機系に自動切替えされない

技術に関する教訓一覧（2/3）

No.	対策	キーワード	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
T12	・ベンダとユーザの双方が相手の役割分担を相互に支援（ユーザ側でハザード分析を行う等）	運用保守、切替え、新旧製品差異、予防対策、実行時対策								△			△	○	△
T13	・関連システム全体でのウォークスルーレビューの実施 ・利用者の観点に立った業務シナリオに即したテストの実施	連携、業務シナリオ、ウォークスルー、レビュー、テスト	○	△										△	
T14	・コンテンツ変更量の自動チェック機能を導入し、コンテンツ量とアクセス量を可視化 ・業務部門がコンテンツを更新する際に、IT部門が確認するようにルールを変更	応答遅延、コンテンツ、サイズ変更、業務部門、IT部門					△							○	△
T15	・緊急時対応に際して、確認手順、テストケースの洗い出し等を特に意識的に行う旨を周知	緊急(緊急作業、緊急時対応)、マスタ、コピー、一貫性、作業手順											△	○	
T16	・技術情報の確認サイクルを3か月に1回から2週間に１回へと変更	仮想化、共同利用、パッチの適用						△		△			○		
T17	・毎月の定期保守日に状況を見て再起動を実施することに変更	仮想化、共同利用、システム再起動			△								○		
T18	・既存システムの要件定義内容を再度チェックして連携するシステム間の整合性を確認、これらをルール化しマニュアルに取り込み ・システムが異常終了しても途中から再開始可能な仕組みの導入	既存システム、システムの追加、インタフェース、制限値	○										△		
T19	・インデックスの追加 ・実行計画の固定化の検討	RDBMS、クエリ自動最適化、実行計画の固定	○				△								
T20	・交代系への自動切替えもできなくなったため、強制的に手動切替えを行い復旧 ・後日、プログラム修正を実施 ・競合が発生しないように接続方式を変更 ・FTA分析を活用した総点検の実施	パッケージ製品のカスタマイズ、プログラムミス、処理の競合	△							○					
T21	・作業ミスは、個人、環境、ハードウェア、ソフトウェアの関係性の中で対策を考える ・ヒューマンファクタの観点からシステムの問題を仕組みや組織として改善することに主眼を置く	ヒューマンファクタ、m-SHELモデル、なぜなぜ分析、ヒューマンエラー対策	△										△	○	
T22	各種バッファの用途に応じた閾値の設定とアラーム表示機能の追加	バッファプール、閾値設定、アラーム表示			○		△						△		
T23	スイッチ障害によるサーバ側メッセージの監視と切替え運用見直し スイッチの定期的な再起動	L3スイッチの動作不安定 データベースサーバのクラスタ構成			○		△				△				

ITサービス編

No.	教訓集の目次（分類）	教訓タイトル	問題	直接原因	根本原因
T24	障害中の運用に関する教訓	サービス縮退時の対策を考慮せよ	顧客サービスシステムの停止	データベースサーバの能力低下	データベースサーバの縮退運転に伴うサービスの停止
T25	原因不明障害への対応に関する教訓	障害原因が不明でも再発予防と発生時対策はできる	事務システムの終日停止	基幹L3スイッチの障害	根本原因は不明
T26	既存システムの流用開発に関する教訓	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	オンライン開始時間の遅延	夜間バッチの起動処理の障害(プロセス間のステータス競合)と、その原因究明の遅れ	バッチプロセスを既存のプロセスの流用により開発した際に既存プロセスのステータス管理を変更せずに使用した
T27	基幹系システムにパッケージソフトを適用する際の教訓（その１）	パッケージはサポートを買え	海外パッケージを適用して構築した基幹業務システムが日中8時間停止	パッケージのソフトウェア障害 同じパッケージを適用する他のユーザより取り扱うデータ量が多かったことから顕在化	・初期調査を担当したサポートデスクでは原因が分からず、開発部門を現地の深夜に招集して調査を開始するまでに時間を要した ・開発部門の原因調査に判断ミスがあり、余計な時間を要した
T28	基幹系システムにパッケージソフトを適用する際の教訓（その２）	パッケージを更新する時は、変更内容の詳細確認と回帰テストで二重に安全を確保せよ	海外パッケージを適用して構築した基幹業務システムが日中3時間停止	パッケージアップデートのソフトウェア障害 同じパッケージを適用する他のユーザより取り扱うデータ量が多かったことから顕在化	・パッケージのアップデートにリリースノートに記載されていない性能改善があり、その中に障害が混入 ・修正が実施されていることを知らないため、その処理の妥当性の確認テストを実施できず
T29	システム環境の変化への対応に関する教訓	単位などの定義が異なる制限値、連携するシステム間で使っていませんか？	個別配送監視システムが停止したため配送状況が分からず、電話でのやり取りで対応	上位システムと下位システムとで制限値の定義が相違	・制限値の単位やシステム連携範囲が不明確 ・連携するシステム間での確認が不十分
T30	ネットワーク２重化の敷設に関する教訓	意味がない、一緒に束ねた２重化配線！	２重化されたリング形式のネットワークで、A系、B系ともに接続断が発生し、同時にノードがない復路回線も接続断	工事作業員がメンテナンス作業中、ケーブルを誤って切断した	ネットワーク全体が２重化になっておらず、見えないところでシングルポイントとなっていた個所が切断された
T31	障害対策マニュアルに関する教訓	復旧手順は、システムとその環境の変化に対応させ常に最新に！	障害対策マニュアルに従い、稼動再開の機能を実行したが、正常に作動せず	障害対策マニュアルの記述があいまいであり、本来使用する必要がなかった機能を実行した	誤った記述のマニュアルが更新されずに放っておかれた
T32	周期起動を持つシステムに関する教訓	周期処理、「時間」と「変化」を監視せよ！	再起動時に正常稼働せず	再稼動機能が、旧型制御装置上の周期処理時間内で完了しなかったため、無応答状態となった	周期処理を持つ制御システムで、周期時間を管理しておらず、環境変化に伴う周期時間の見直しや、全機器の動作確認を行っていなかった
T33	排他制御に関する教訓	入念な方式設計と多段階の確認は当たり前、個人情報を扱う場合には特に排他制御に気をつけて	ダウンロードサービスで、他顧客のデータを転送する情報漏えい（セキュリティ・インシデント）が発生	ダウンロードデータを格納する一時ファイルを共有していたため、要求競合時に複数要求元のデータが混在	設計者の経験からOS等がリソース競合対策機能を有すると思い込み、排他制御をアプリケーションレベルで実装する必要はないと判断した方式設計ミス 開発標準に排他制御の記載がなく、その後のレビューやテストでも発見されず

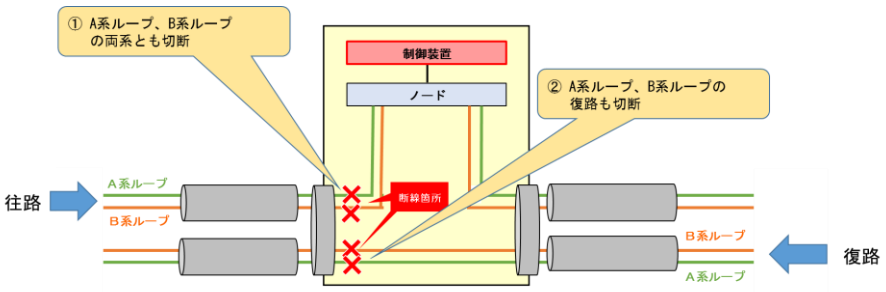
技術に関する教訓一覧（3/3）

No.	対策	キーワード	ＪＩＳ　Q20000-1：2012より（○主な問題個所、△関連する問題個所）											
			5.	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		
			新規またはサービス変更の設計及び移行	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
T24	機器更改時にデータベースサーバ拡張 基幹系と顧客サービス系の分離の検討	サーバのスケールアップとスケールアウト 基幹系と情報系	△		○				△		△				
T25	スイッチの電源OFF/ONで復旧 スイッチの交換、ファームの最新化 再発時に備えた障害運用マニュアルの改善 収集ログの追加	原因不明のハードウェアハングアップ パッチ適用 再発時の危機管理			△							○			
T26	流用開発プロセスのステータス管理を修正 同様プロセスの洗い出しと対応 設計レビューの強化 流用開発に用いる既存仕様書の修正	流用開発 一意性の修正漏れ	△										○		
T27	パッケージ開発元とのSLAを見直し ・トラブル発生時にはサポートデスクを経由せず24時間いつでも開発部門が直接調査を実施 ・トラブル発生連絡から解決までの所要時間を合意	パッケージ障害サポート 障害からの復旧遅延		△						△		○			
T28	パッケージアップデート適用前に、以下の確認の実施をルール化 ・含まれるすべての修正の仕様詳細レビューと動作テストによる確認 ・実業務に近いテストセットを用意し、回帰テストを自動化	パッケージアップデート アップデート内容確認 リグレッション(回帰)テスト				△				△				○	△
T29	・個別配送監視システムの機能仕様書の制限値の定義見直し ・個別配送監視システムの制限値超過時の振る舞い調査 ・各システム間の制限値再点検と一元管理	制限値の単位 制限値の一元管理 システム連携	△				○						△	△	
T30	２重化構成になっているが両系切断になりうる個所の点検・変更、 施工標準の見直し、などを実施	ネットワークの2重化 ネットワーク敷設 シングルポイント 施工基準			●							△	△		△
T31	障害対策マニュアルを常に最新版の状態に保てるように、障害対策マニュアルを維持管理する運用ルールを定め、実践していく体制を作った	障害対策マニュアル 障害対応手順 システム運用		△					△		●		△		
T32	周期時間管理、 新機能追加時の運用ルールの策定、「旧機種の装置を新機種の装置に更新し易い」構成を作る、などを行い、周期時間の変化点を見逃さない仕組みを作る	周期処理 周期時間 変化点 分離型制御装置					●				△		△		△
T33	・開発チーム編成時に、メンバ候補のスキルや経験についての確認を義務化 ・社内開発指針に排他制御関連事項等を追記 ・更新対象のセキュリティに関わる部分は、関連する全処理の再トレースに基づく確認を義務化	セキュリティ（個人情報） 方式設計 排他制御、リソース競合対策 開発標準	△					●		△					△

教訓　T30：意味がない、一緒に束ねた２重化配線！

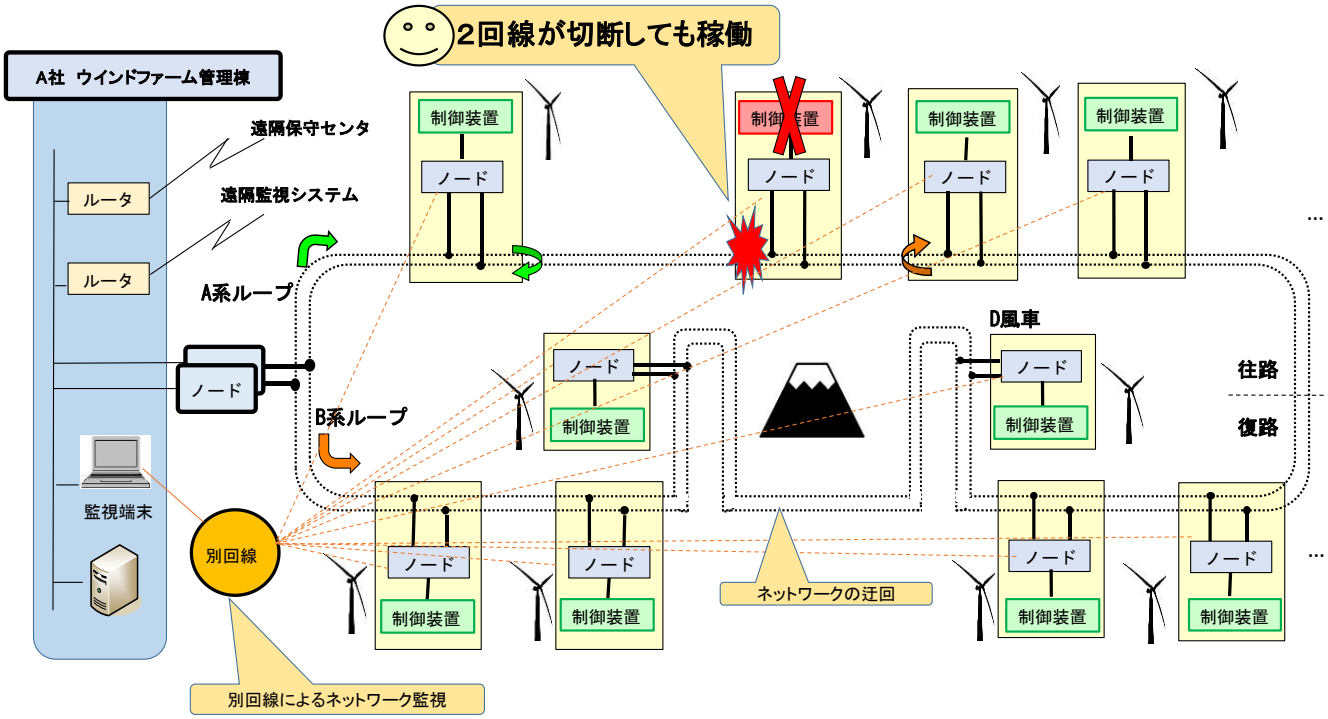
【問題】 ある日、A社の制御装置をつなぐネットワークで、障害が発生した。A社のネットワークは、デュアルリング型なので、A系ループの障害が起きた時点で、B系ループに切り替わろうとしたが、A系、B系ともに接続断が発生した。さらに同時にノードがない復路回線も接続断となり、折り返し機能によって、多くの制御装置がネットワークから切り離された。

【原因】 直接原因は、工事作業員が「メンテナンス作業」を行った際に、ケーブルを誤って切断したことであった。切断箇所は、工事のために一時的に両系のケーブルの往路（４回線すべて）と復路が建屋の中で束になって仮配線されていた箇所であった。



【対策】 せっかくネットワークを２重化にしていても、敷設工事の時にケーブルを一緒に束ねておいては、今回のように意味をなさないことが起きてしまう。そこで、以下のような対策を行った。

- ２重化構成になっているが両系切断になりうる個所の点検・変更
- 施工標準の見直し（施工業者との「信頼性の考え」を共有）
- 将来ネットワークの見直し（回線のシングルポイントの検討、監視機能強化）

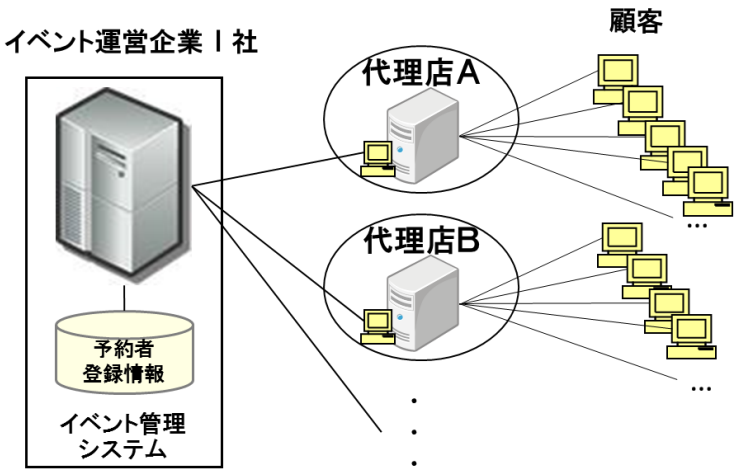


教訓

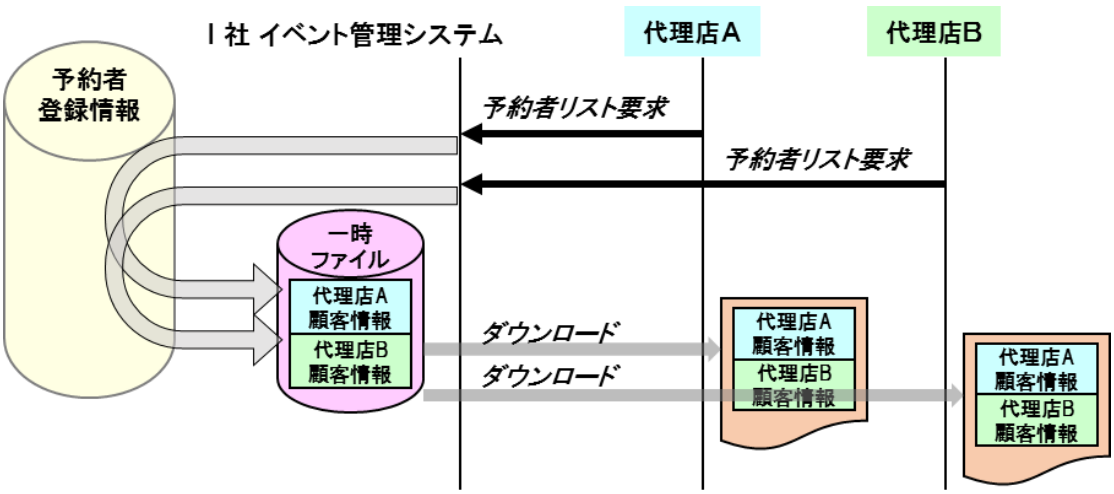
T33：入念な方式設計と多段階の確認は当たり前、個人情報を扱う場合には特に排他制御に気をつけて

【問題】 イベント管理システムの予約者登録情報のダウンロードサービスで、他顧客のデータを転送するという情報漏えい（セキュリティ・インシデント）が発生

【原因】 ダウンロードデータを格納する一時ファイルを共有していたため、ダウンロード要求の競合時に複数要求元（代理店）の顧客データが混在して転送された。



根本原因は、設計者の経験からOS等がリソース競合対策機能を有すると思い込み、排他制御をアプリケーションレベルで実装する必要はないと判断した方式設計ミスである。なお、システム開発標準における設計指針に排他制御の記載がなく、以降のレビューやテストでもミスが発見されなかった。また、ダウンロード対象項目にシステム開発当初はなかった個人情報が含まれることになった時点、すなわちセキュリティに対する要求レベルが上がった契機でも、セキュリティの観点での十分な影響確認が行われなかった。



【対策】
- 開発チーム編成時に、メンバ候補のスキルや経験についての確認を義務化
- 社内開発指針に排他制御関連事項等を追記
- 一定規模以上のシステムや重要度の高いシステムにおいては、知見・経験の豊かな第三者によるレビューを義務化
- システム更新対象のうちセキュリティに関わる部分については、関連する全処理の再トレースに基づく確認を義務化

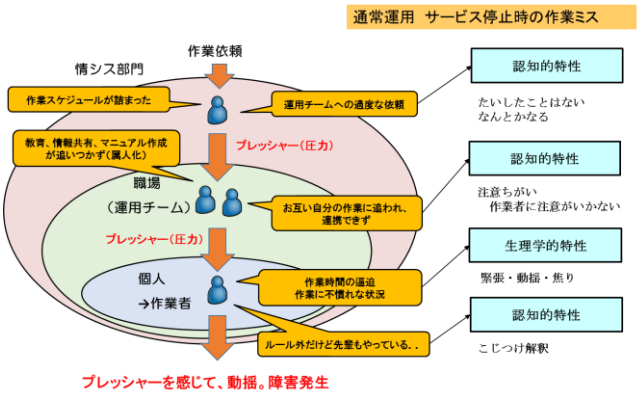
情報処理システム高信頼化教訓集（ITサービス編）

教訓集には、これまでに作成された教訓がすべて掲載されています。
・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　33 件

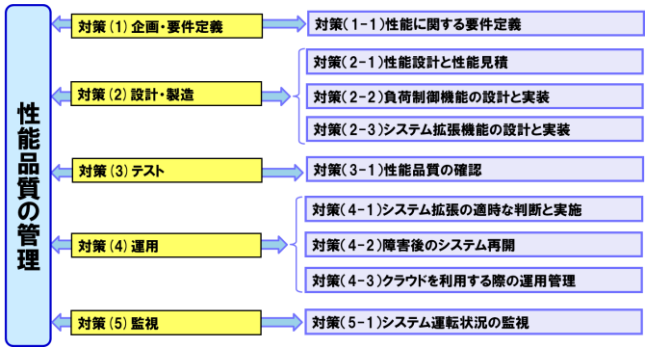
各教訓は、実際に発生したシステム障害事例をもとに作成され、各業種を代表する有識者による審査を経て、掲載されています。

教訓集には、これらの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」などの観点から分析し、原因や対策について考察した結果が掲載されています。

発行：情報処理推進機構(IPA)
ISBN：978-4-905318-68-2
Ｂ５変形判／298ページ
定価：2,407円（税別）
PDF版も公開



ヒューマンエラー 人間特性による原因分析



高負荷・過負荷 性能品質の管理のための工程ごとの対策

教訓集別冊

本書の教訓を作成する際にも活用している対策手法や分析手法を、別冊Ⅰ、Ⅱとして公開しています。

別冊Ⅰ：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、一覧で示しています。

具体的な対策を実施する際に、対策が必要な背景等をより深く理解するために役立ちます。また、教訓に含まれる対策以外の周辺対策・関連対策を調査、検討する際の参考としても活用できます。

PDF版を公開

別冊Ⅱ：障害分析手法

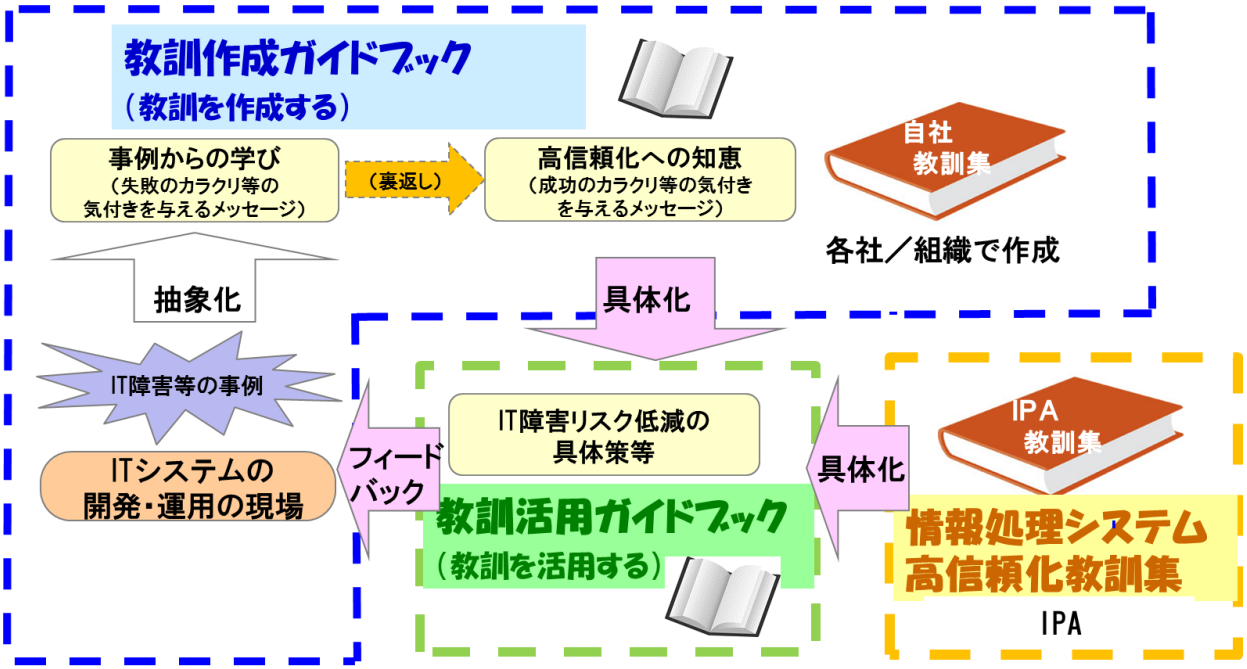
障害原因分析の際によく用いられる分析手法をまとめています。最適な分析手法を選択する際の参考として使用できます。

広く分野を越えて利用されている基本的分析手法である「なぜなぜ分析」や、人間の行動モデルをベースにヒューマンエラーが関係した事象を分析する手法である「ImSAFER」、システム安全を上流で設計する手法である「STAMP」などについて概説しています。

PDF版を公開

ITサービス編　　教訓を活用するガイドブック

教訓集セミナーへの参加者や教訓集の利用者からのアンケートなどの声を参考にして、障害の未然防止に役立つ教訓を利用者が自ら作成し、教訓を自社内で活用し継続的に活動していくためのガイドブックを作成しました。



「情報処理システム高信頼化教訓作成ガイドブック」

自社内で発生したシステム障害事例の原因分析や再発防止策などを「教訓」として作成するための手法を解説しています。本書を読むことで、発生した障害の原因を分析して対策を検討し教訓としてまとめ、教訓を活用するための分類の方法を習得することができます。

さらに、自社で作成した教訓を外部に発信することによって、今まで個人や組織内、企業に閉じていたノウハウが広く社会で共有できるようになります。

PDF版を公開

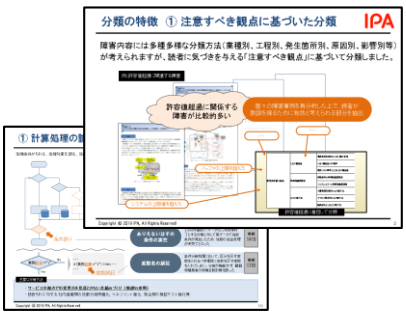
「情報処理システム高信頼化教訓活用ガイドブック」

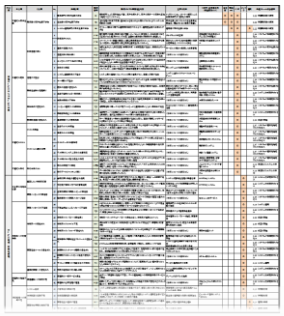
自社で作成した教訓の他、IPAや他社などの第三者が提供する教訓を自社内で活用するための手法を解説し、IPA/SECの教訓集について、「掲載されている教訓をどのように活用するか」と、「自身の課題解決に教訓を活用する方法」に分けて解説しています。

また、システム障害事例の共有活動をどのように行っていくのかについての方法も紹介しています。

PDF版を公開

「情報処理システム高信頼化教訓集」および「情報システムの障害状況」（次ページ参照）で取りまとめているシステム障害事例情報を、短い時間でポイントや全体像をつかめるよう、「注意すべき観点」に基づいて分類した障害事例の一覧を用意しています。





◆ 「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できます。

「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

「情報処理システム高信頼化教訓集」にも、この「注意すべき観点に基づく障害の分類」を掲載しています。「注意すべき観点」に基づいた障害事例分類のうち、特に注意すべき10種の分類について解説しています。

	注意すべき観点	
	小分類	詳細分類
①	計算処理の誤り	計算条件のもれ / 通常外処理のもれ / 処理対象の時点誤り /ありえないはずの条件の実在 / 変数名の誤記
②	検知条件の想定もれ	メッセージ重複による誤検知 /無操作異常の不検知 / 抑制信号停止による誤検知
③	テストによる副次作用	テストデータの本番残存 /システム日付の設定誤り /テスト時のログ出力設定の残存
④	待機系への設定もれ	待機系でのパラメータ設定誤り /待機系でのファイル不足 /待機系でのパスワード設定もれ
⑤	障害発生ケースの想定もれ	複数事象が同時発生するケースの想定もれ / 故障時のネットワーク輻輳の想定もれ / 故障時のエラーメッセージ発生の想定もれ / サイレント障害（NW性能劣化の不検知
⑥	しきい値の超過	業務要件変更時のしきい値不変更 / しきい値超過の不検知
⑦	ログの肥大化	アクセス集中時のログ肥大化 /大量業務処理時のログ肥大化 /監視強化によるログ肥大化
⑧	製品仕様の誤解	感覚と異なる設定値 / 隠れた設定値 / 異常検知のみで機能停止
⑨	不完全な作業実施	作業完了の誤認 / 再起動もれによる作業未反映 / 緊急作業と定期作業の競合で更新漏れ
⑩	作業中偶発事象への考慮不足	作業時の電力供給不具合 / 作業時のハードウェア故障 / 切戻し時のハードウェア故障

ITサービス編　情報システムの障害状況データ

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しています。これを半年ごとに取りまとめて、ホームページ上に「情報システムの障害状況」として連載しています。

○情報システムの障害状況
2017年後半データ

○情報システムの障害状況
2018年後半データ

◆2010年からの過去分をすべて参照できます。

情報システムの障害状況一覧

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

公開/発行日	内容	
2019年3月	情報システムの障害状況　2018年後半データ	
	1.2018年後半の概況 2.大規模通信障害 3.証券取引システムの障害 4.むすび	PDF
2018年11月	情報システムの障害状況　2018年前半データ	
	1.2018年前半の概況 2.システム障害に起因するセキュリティ事故 3.企業の合併に伴うシステム統合の問題 4.仮想通貨にかかわるシステムの安全性 5.むすび	PDF
2018年3月 (SECjournal第52号)	情報システムの障害状況　2017年後半データ	
	1.2017年後半の概況 2.Jアラート関連の障害 3.システム障害に起因するセキュリティ事故 4.テスト作業の本番環境への悪影響による障害 5.むすび	PDF

（以下　省略）

教訓一覧
（組込みシステム）

No	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
1	複雑な条件式のロジック変更を行う場合は、デシジョンテーブル等による検証が有効である			○	○						
2	条件が整理されていない状態で、トータルの条件数が100を超えるような機能、または10個以上の条件を有する機能を修正する場合、関連する条件を全て洗い出して整理し不整合がないことを確認する			○	○						
3	複数機能モジュールを統合する場合、統合前の条件数の総和と統合後の条件数を比較し差がある場合は、条件の抜けがないか確認する				○			○			
4	変数値域が広く、組合せバリエーションが非常に多くなる場合には、値域を適切な大きさに分割した上で境界値テストを実施する				○						
5	内蔵電池を使用する場合には、深放電時の起動シーケンスを考慮すること		○	○			○	○	○		
6	フラッシュメモリを使用する場合には、書き込み寿命回数を考慮すること	○	○							○	○
7	消費電力の多い機能を追加する場合には、一時的な電圧降下による影響（リセット、フリーズ等）や電源の種類、電池の場合は残量を考慮すること		○								
8	想定可能な例外を形式的に漏れなく分析する	○	○								
9	システムを二重化する場合は、同期すべきデータ領域を適切に設定する			○							
10	制御対象のハードウェアが同一でも、運用条件が変わるときは、ハードウェア仕様を再確認する		○		○		○		○		
11	プロセス間、スレッド間でデータを共有（引き渡し）する場合は、排他・同期処理が正しく行われているか、あるいはデッドロックが発生していないかどうか注意する			○		○			○		
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	○									○
13	既存ソフトウェアの性能改善を実施する際には、アイドリングタイムの発生、処理の同期ずれの発生等と影響を確認する			○	○			○	○	○	
14	・大量のデータを通信経由で扱う場合、一連の処理の流れの中にボトルネックを作りこまないように注意する ・時間帯による負荷変動について考慮する	○	○	○			○				
15	納入したあと、お客様が運用するような業務システムでは、業務シーケンス中のあらゆる異常操作（リセット、電源断、放置も含め）への対応を考える				○			○			
16	障害解析時の保守メンテ用ログ処理であっても、仕様書を作成し、影響評価を実施すること			○							
17	判断処理は、必要条件だけでなく、制限すべき条件も漏れなく抽出する				○						
18	ログファイルの断片化に注意する			○							

教訓一覧
（組込みシステム）

No	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
19	人による変更作業ではミスが起きることを前提に、ツール活用などで不具合の作り込みや流出の防止に心がける	○			○			○			
20	信頼性向上施策を採る場合は、故障発生確率と影響の定量評価を行い、対策は確実に実装する		○	○			○			○	
21	高い信頼性対策が求められるシステムでは重大な影響を及ぼす事象の想定と復旧手順を十分に検討する		○								○
22	処理時間がクリティカルなシステムではツールを活用し、変数やその取りうる状態数とそれぞれの状況における動作処理に最大バラツキを意識し余裕を把握し設計する			○	○		○	○	○		
23	開発を伴わない保守案件でも、システム構成変更が発生する場合は、手順等作業内容の妥当性を確認できるようなプロセスを経る						○	○		○	○
24	物理量（時間、重量など）を扱う場合は単位、桁数を確認する		○			○		○			
25	顧客が要求していることの目的と背景に遡って、その意図を確認することが、要求仕様のあいまいさ排除に役立つ	○					○				
26	遠隔地等物理的に離れた装置をネットワーク接続して稼働させるシステムでは、故障などの状態検知やメンテナンスも容易ではないため、システム的視点での状態把握を行う	○	○					○			
27	マルチベンダーシステムでは仕様に外れた想定外事象が発生することを前提とした自己防衛策を採る	○		○				○			
28	データベース等COTS製品のバージョン、動作仕様の相違等の情報が関係者にタイムリーに参照できるようにする							○	○	○	○
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		○						○		○

教訓

教訓5: 内蔵電池を使用する場合には、深放電時の起動シーケンスを考慮すること

【製品の特徴】

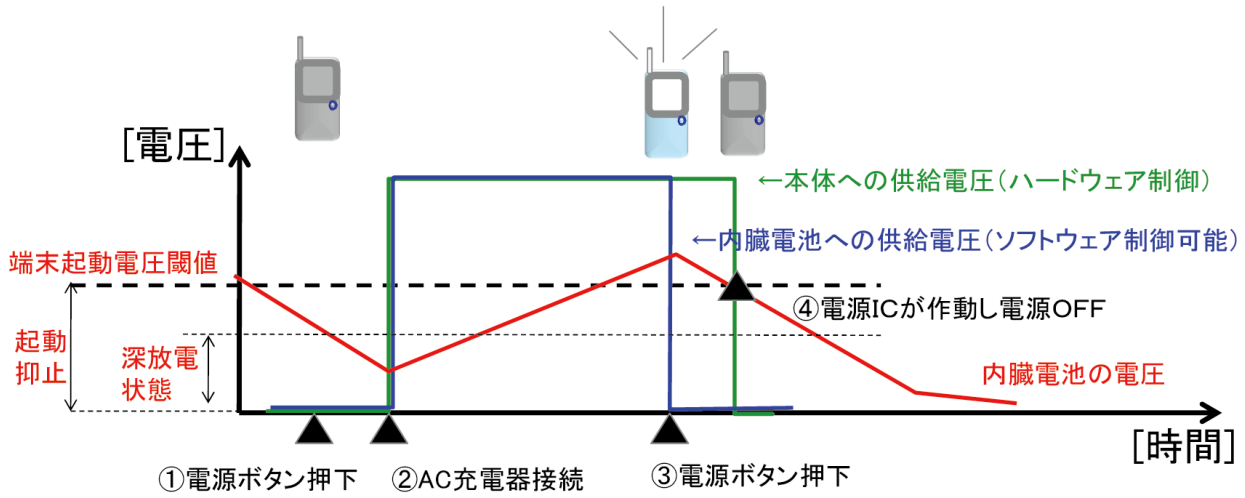
ディスプレイと無線通信機能を有し、内蔵電池によりＡＣ充電器の接続が無くても使用が可能な可搬型業務用端末

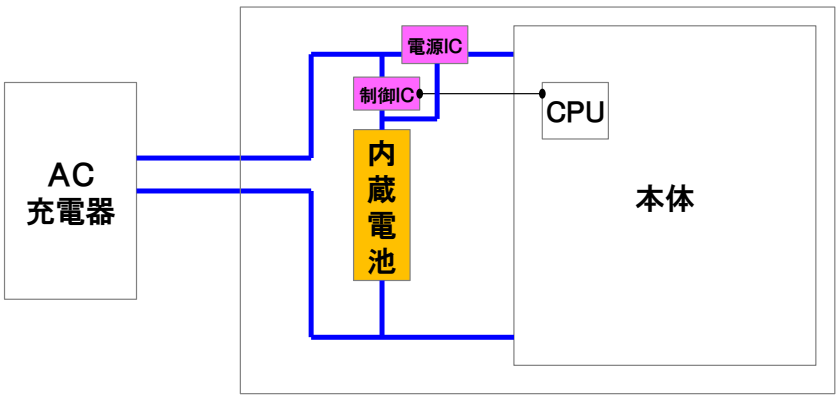
【観察できる現象】

電源ボタンを押下しても端末が起動しない。
ＡＣ充電器を接続しているのに充電が出来ない。

【内部の事象】

①で電源ボタン押下。内蔵電池の電圧が低下しているため起動しない。
②でＡＣ充電器を接続。内蔵電池の電圧が上昇開始する。
③で電源ボタン押下。 ソフトウェアが内蔵電池の電圧を判定。
　⇒　閾値を超えていたので起動処理を開始。
　⇒　起動処理が終了するまで、充電を停止。（ソフトウェア仕様どおり）。
　⇒　内蔵電池の電圧低下。端末起動電圧閾値を下回った。
④電源ＩＣ（ハードウェア）は、内蔵電池の電圧が閾値を下回ると、装置本体への電源供給を停止した。⇒　電源ＯＦＦ。充電は停止したまま。
※ここで、ＡＣ充電器を抜き差しすると、充電を停止していたＣＰＵがリセットされ、充電再開





ハードウェア仕様：
①電源ＩＣは、内蔵電池の電圧をモニターし、電圧が端末起動電圧閾値を下回ると、本体への電源供給を停止する。

②内蔵電池への充電は、制御ＩＣがDISABLEされていると実施されない。ただし、ＡＣ充電器を抜き差しすると、リセットされ、充電が開始される。

【原因】

①内蔵電池の深放電により、電源ＩＣが電圧低下と判断し、端末全系統電流の供給を停止した。そのため、電源ボタンが効かなかった。
②端末の起動処理の最中は、内蔵電池への充電をソフトウェア制御により停止している。この状態で、端末全系統電流の供給停止によりＣＰＵが停止したため、ＡＣ充電器が接続されていても、充電が再開されなかった。

【対処】

①ＡＣ充電器を抜き差しし、しばらく待ってから電源ボタンを押す。
（ＡＣ充電器を抜き差しすると、充電を停止していたＣＰＵがリセットされ、充電再開することができる。電圧が端末起動電圧閾値を十分超えるまで待つ。）
②端末起動処理の開始可否を判定する、内蔵電池の電圧の閾値を、端末起動処理に要する電圧降下を十分考慮した上で設定する。

【未然防止に向けた対策】

・電池で動作する端末においては、長時間放置等により電池電圧が極度に低下した状態（深放電状態）になり、その状態に対する対策が必要であることを認識すること。
・電池電圧が極度に低下した状態（深放電状態）にならない工夫や、その状態になった場合の対策を検討し、必ず実際の装置で検証を行うこと。
・端末の起動電流や電圧降下及びそのバラツキを考慮し設計に織り込むこと。
・客先のユースケースを調査／検討し、同様の条件／環境で評価を行うこと。

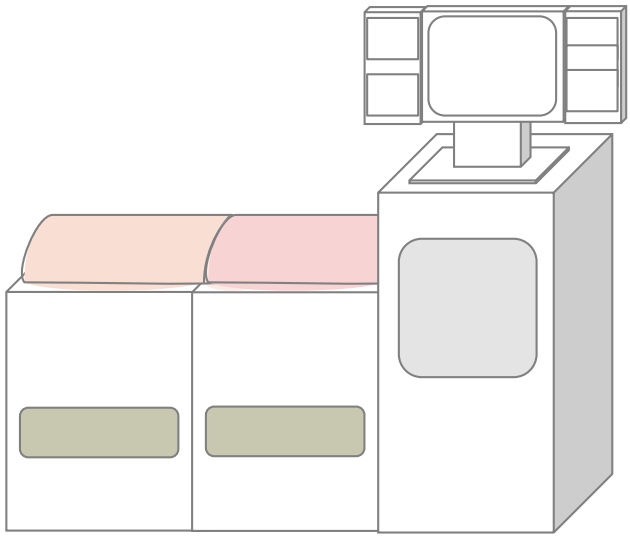
【工程】システムアーキテクチャ設計、ソフトウェアアーキテクチャ設計、レビュー、システムテスト、教育

教訓

教訓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

【製品の特徴】

・半導体がスペック通りの機能・性能を満たしているかを検査する装置。
・半導体の検査は複数のテストで構成され、その全てのテストが良の場合は検査結果が良品となる。一方で、あるテストで不良になった場合は不良品と判断され、検査時間の効率化のため、通常その後のテストは行わない。
・検査機能をマスクできるモードがある。



【観察できる現象】

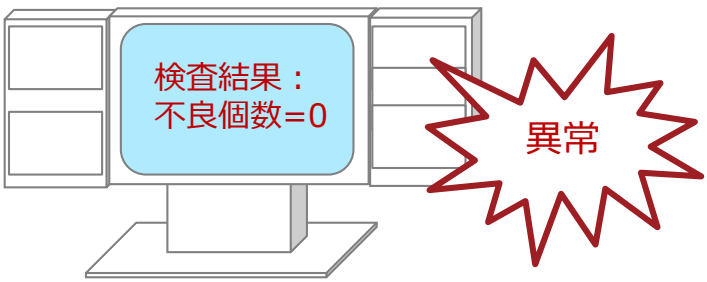
半導体の検査では、一定の割合で不良品が発生するが、検査した全てが良品となった。しかし、その後の検査の工程で通常より多くの不良品が検出された。

【原因】

・全て良品となった場合には、異常の可能性があるとみなしていなかった。
・全て不良品の場合は直感的に検査が異常であるとわかるが、全て良品の場合にも検査が異常であると考えが及ばなかった。

【対処】

全て不良品の場合と同様に、全て良品の場合も異常を通知するよう修正した。



【未然防止に向けた対策】

■システム要求定義

・良／不良の条件に関わる仕様を明確にする。
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。

■システムアーキテクチャ設計

・システム設計の中でもメンテナンスモードに対する設計に注意すること。

■運用

・メンテナンスモードを有するシステムでは、その取り扱いについて、手順書で明確にして、ダブルチェックも考慮すること。

組込みシステム編　教訓を活用するガイドブック

「障害未然防止のための教訓化ガイドブック」

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教訓の形で伝えるためには、ノウハウの一般化をいかに行うかが重要となります。

・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として取りまとめました。

PDF版を公開

「現場で役立つ教訓活用のための実践ガイドブック」

PDF版を公開

自社及び他社で作成された教訓を、

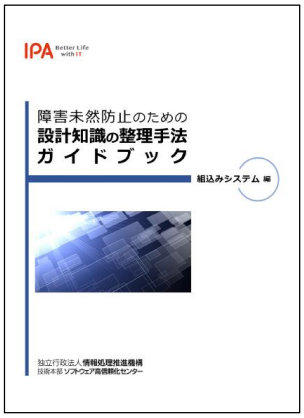
「社内教育・研修」
「開発プロセス」
「設計品質向上活動」

の活用シーン別に解説することで、他社・他部門などの第三者が提供する教訓を自社内ですぐに活用できるよう工夫しました。

「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」

いわゆる「過去トラDB（過去トラブルデータベース）」と呼ばれるデータベースに蓄積されたソフトウェア障害情報の記録から、障害発生を未然防止するための設計知識を抽出し、有効活用できる形に整理する方法を提案するものです。

障害情報記録から設計知識を抽出するための観点を示し、抽出した設計知識を構造的に整理することが出来れば、「過去トラDB」が障害の再発防止や未然防止のために活用できるようになります。



PDF版を公開

「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」

1 背景と目的

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、そこには障害を防止するためのノウハウが含まれている。このノウハウを設計知識の形で取り出して整理し、障害の再発防止や未然防止に役立てる目的でこの整理手法を紹介している。

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１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さら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。

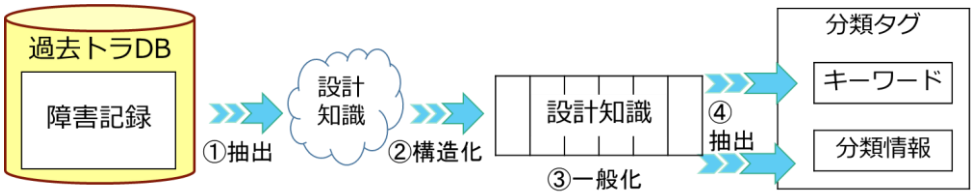


図１　設計知識の整理手順

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２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)を繋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) 考慮漏れし易い設計視点・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２　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。」

4 分類タグ

分類タグは、その知識が何に役立つものかを直観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）で構成する。

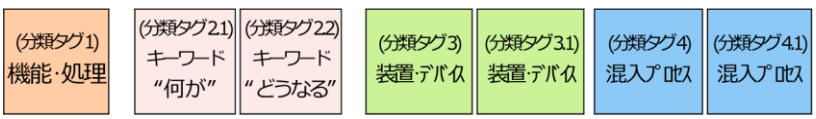


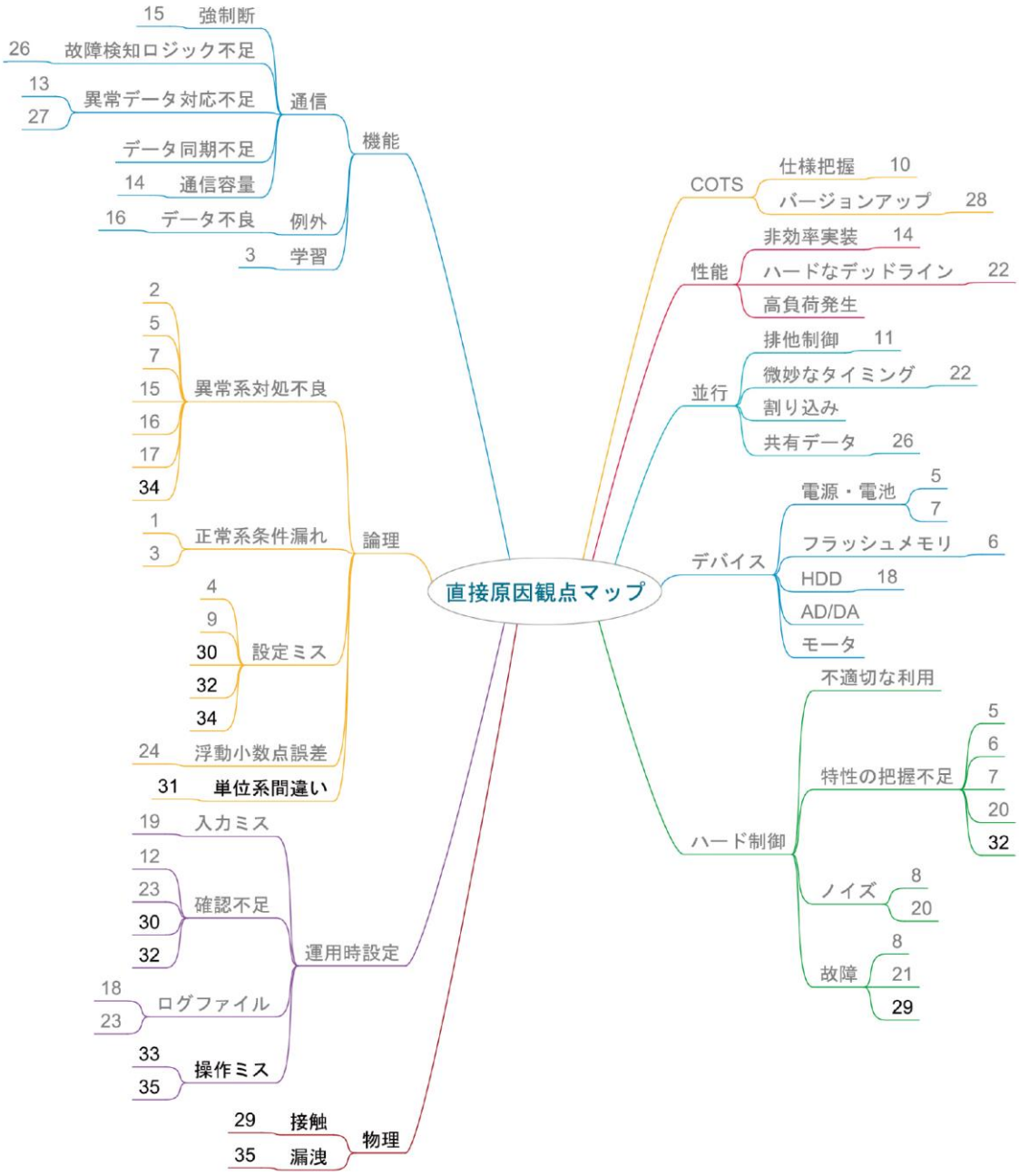
図3　分類タグ

IPA/SECでは発生した障害から得られる知見を、他製品に適用し、更には他産業領域への展開も志向しています。

障害事象を引き起こす原因には、製品や産業領域の違いに依らず共通要素が見受けられます。他領域へ展開できるように、35教訓事例の原因を分析し、直接原因と真因の共通要素を抽出し、直接原因と未然防止の観点マップを作成しました。

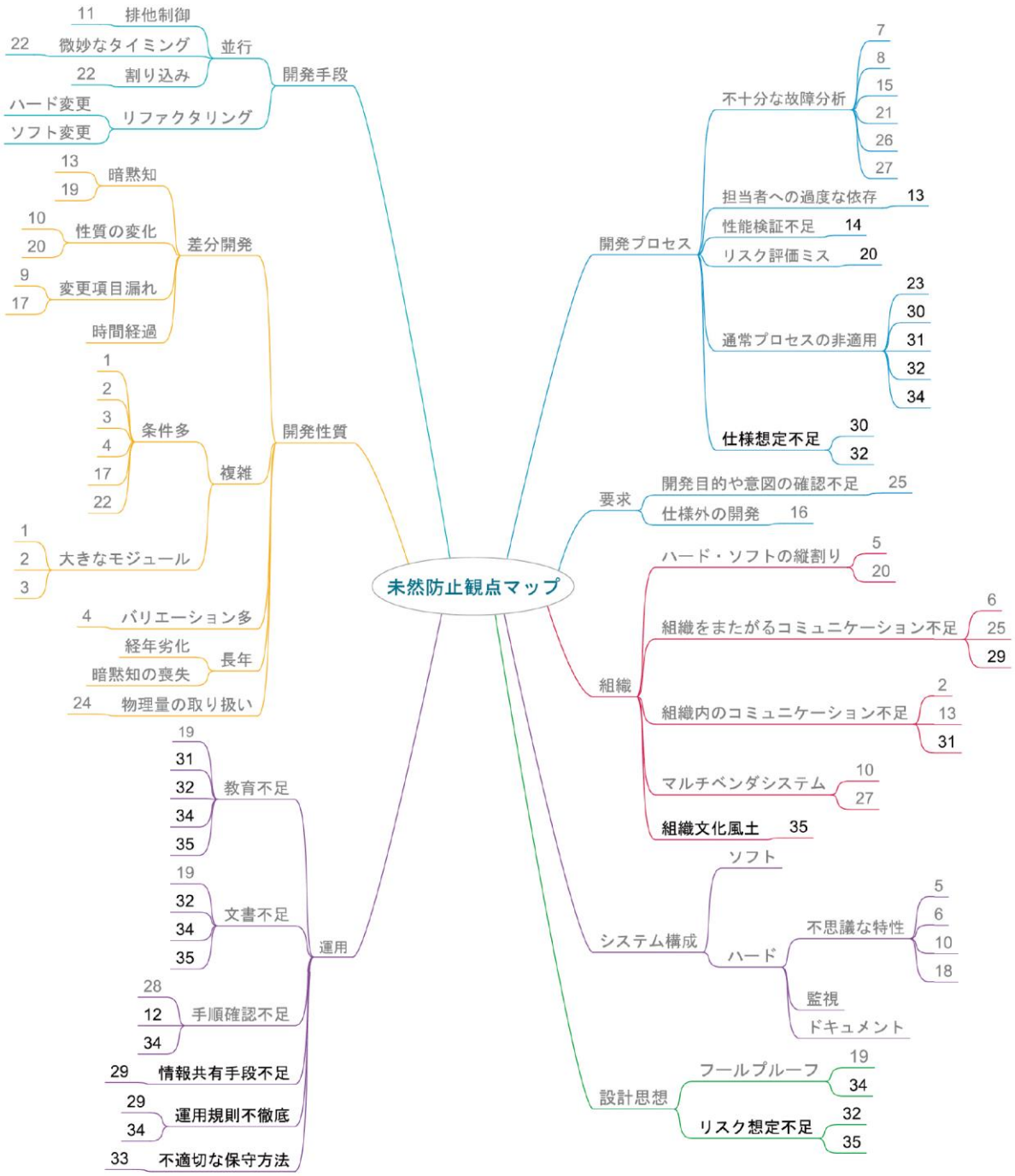
1 直接原因観点マップ

- 35教訓事例の障害を引き起こした直接原因を抽出し整理しました（マップ中の番号は教訓番号）。



2 未然防止観点マップ

- 同じく35教訓事例の障害を引き起こすに至った真因から未然防止の観点を抽出し整理しました（マップ中の番号は教訓番号）。



条件数や構造の複雑さやバリエーションの多さといった開発性質、要求仕様の条件の見落としなどが多く、近年の組込みシステムが置かれた状況を推測できます。

INFORMATION

ITサービス／組込みシステムの高信頼化への取り組み

詳細は下記URLまたはホームページからご参照ください。　IPA障害対策　検索

重要インフラ分野のシステム障害への対策
https://www.ipa.go.jp/sec/system/index.html

情報処理システム高信頼化教訓のリンク集
https://www.ipa.go.jp/sec/system/lesson.html

「情報処理システム高信頼化教訓集（ITサービス編）」
https://www.ipa.go.jp/ikc/publish/tn19-001.html

「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）」及び
「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）」
https://www.ipa.go.jp/sec/reports/20160229.html

「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
https://www.ipa.go.jp/sec/reports/20160331_2.html

「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）」及び
「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）」
https://www.ipa.go.jp/sec/reports/20160331_3.html

「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）」
https://www.ipa.go.jp/sec/reports/20170321_1.html

■お問い合わせ

独立行政法人情報処理推進機構（IPA）　社会基盤センター
〒113-6591 東京都文京区本駒込2-28-8 文京グリーンコート センターオフィス16F
[TEL]　03-5978-7543　　[E-Mail]　ikc-info@ipa.go.jp
[URL]　https://www.ipa.go.jp/ikc/

IPA Better Life with IT