

近年のソフトウェア障害の特徴

～IPA/SECによるシステム障害事例分析に基づく教訓～

ソフトウェア・メンテナンス研究会 (SERC) フォーラム
「情報システムの障害対応とソフトウェア保守を考える」
2016年5月19日

独立行政法人情報処理推進機構 (IPA)

技術本部 ソフトウェア高信頼化センター (SEC)

sec-sys-infb@ipa.go.jp

Information-technology Promotion Agency, Japan

Software Reliability Enhancement Center (SEC)

Copyright © 2013-2016 IPA, All Rights Reserved

IPA Software Reliability Enhancement Center

本講演の趣旨



情報システムの障害は、サイバー攻撃等の情報セキュリティ事案と比べ、一般に、発生頻度は低いものの、ひとたび発生するとその影響範囲は広く、深刻度も高い。世の中を見てみると、障害発生防止のための対策が講じられていても、思わぬ状況や原因により障害は発生している。これを減らすためには、あらかじめすべてのリスク要因を想定することは不可能なため、他所で発生した障害を自システムでは発生しないように対応することが有効であり、そのためには、障害事例情報の共有が必要である。

IPA/SECでは、2013年度から、10程度の分野の事業者のIT部門からお集まり頂く委員会において、一定の守秘義務の下に、各社の障害事例を紹介して頂き、その根本原因と再発防止策等について多方面から議論している。そして、その結果を抽象化・普遍化してまとめ、「教訓(集)」として公開している。

本講演では、まず、IPA/SECにおけるシステム障害事例情報共有の取組みの概要を紹介した後、これまでにまとめた障害事例の分析に基づく教訓のうち、特に保守関連の教訓について説明する。また、時間が許せば、保守作業中に発生したある障害事例について、その分析過程を詳しく説明する。

1. IPA/SECにおける障害事例情報分析・共有活動
 - 背景
 - 取組みと成果概要
2. 保守関連の障害事例の分析に基づく教訓
3. 障害事例から教訓を導く例
4. まとめ

1. IPA/SECにおける障害事例情報分析・共有活動
 - 背景
 - 取組みと成果概要
2. 保守関連の障害事例の分析に基づく教訓
3. 障害事例から教訓を導く例
4. まとめ

ソフトウェアは、それ自身、複雑化・大規模化し、システム間連携により、複雑化は一層進展



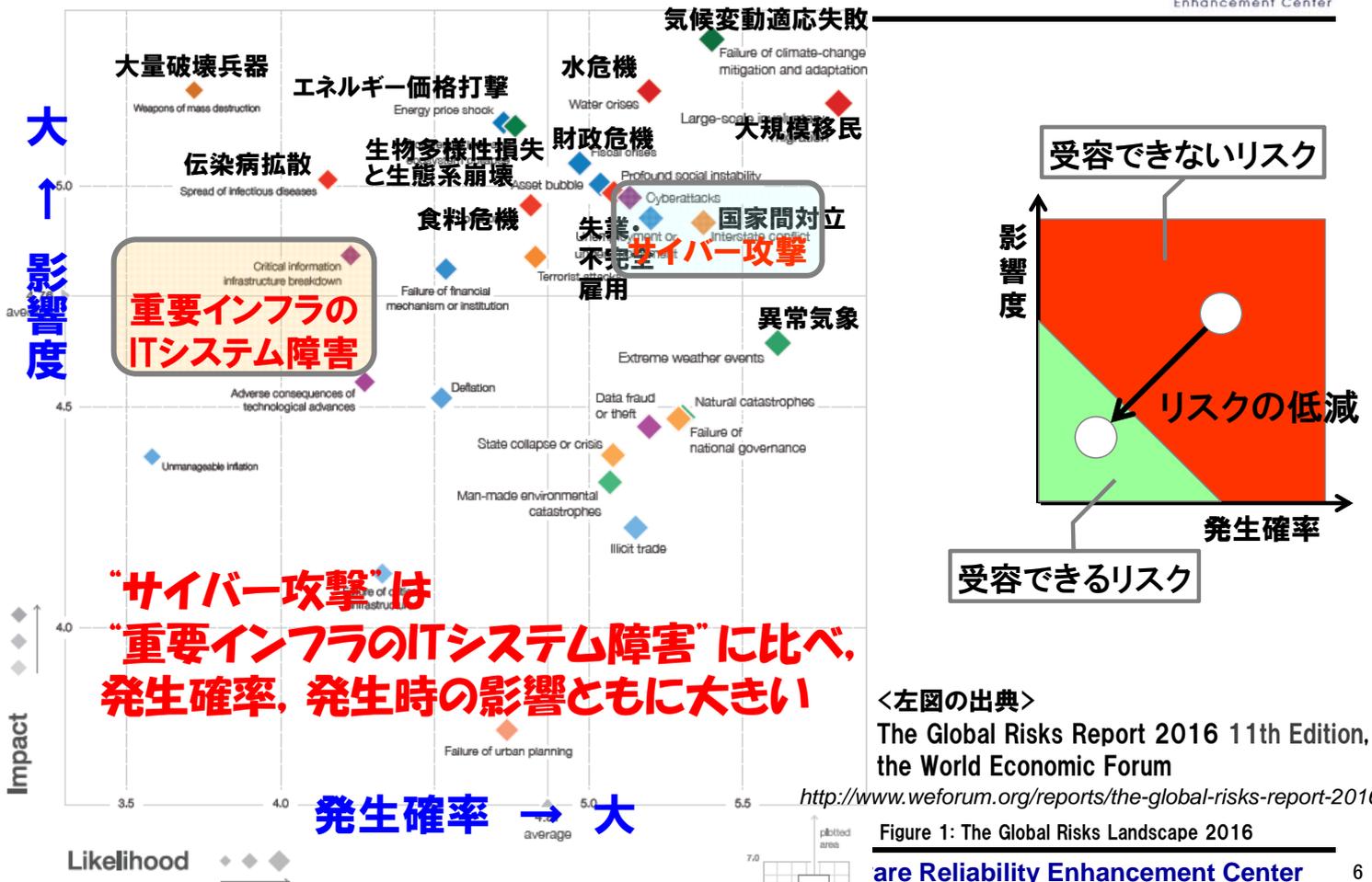
停止・異常動作等のリスクの増大

∴ 市民生活や社会経済活動がITシステムに大きく依存

社会リスクに比例して、ビジネス・リスクも増大

データ例

グローバル・リスク (2016)



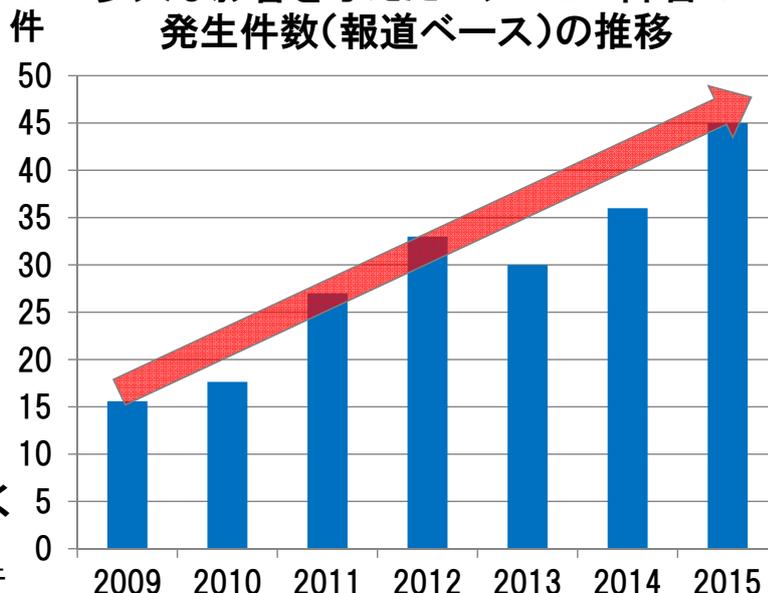
情報処理システム障害の発生状況

社会に大きな影響を与えた
システム障害の発生件数
2009年以降で増加傾向

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。
- 〇〇システムで障害か、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



1.1 障害事例情報分析・共有の背景

情報処理システムの信頼性向上

システムの
構築時 → 初期リスク(故障)回避

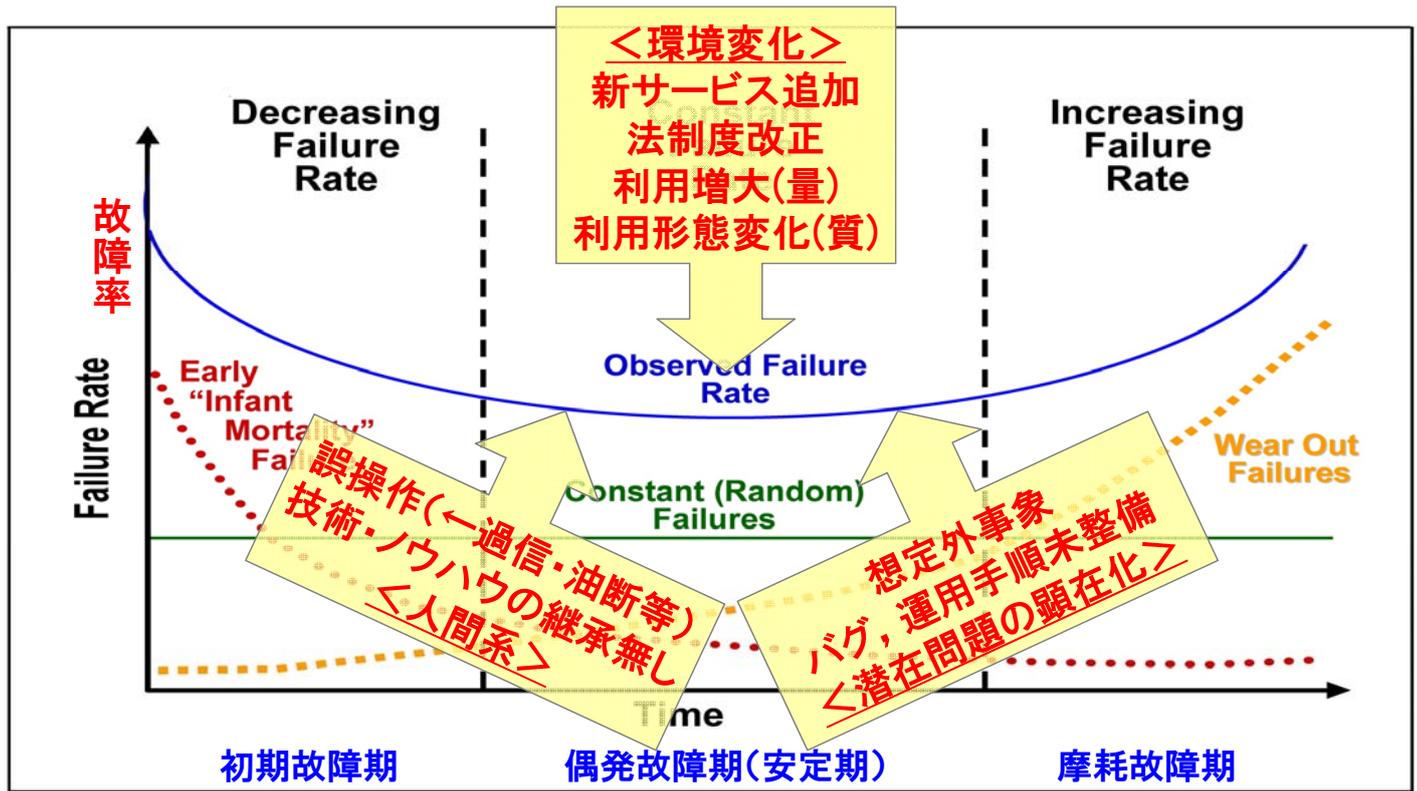
ソフトウェア・エンジニアリング技法の活用

はるかに長期間

システムの
運用時 → 様々なリスクに対応

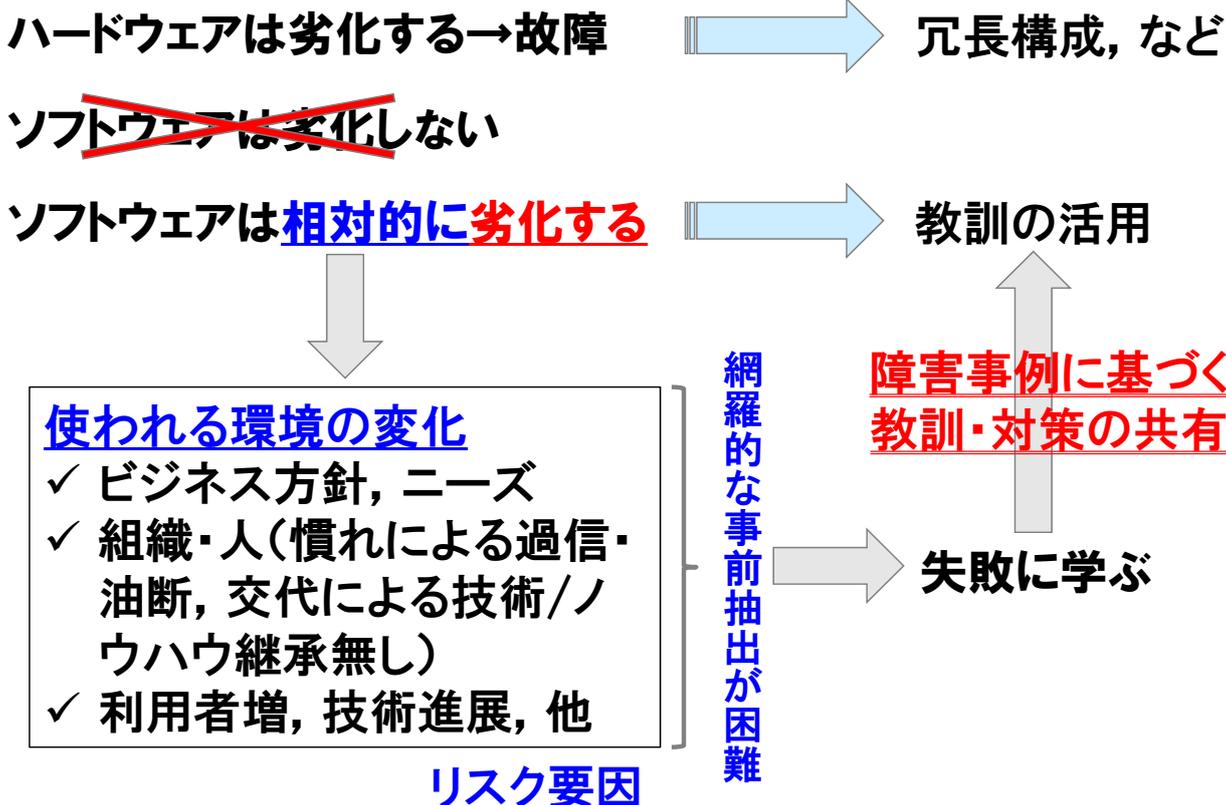
体系的な取組みが必要
着目点は...

システム運用時に想定されるリスク

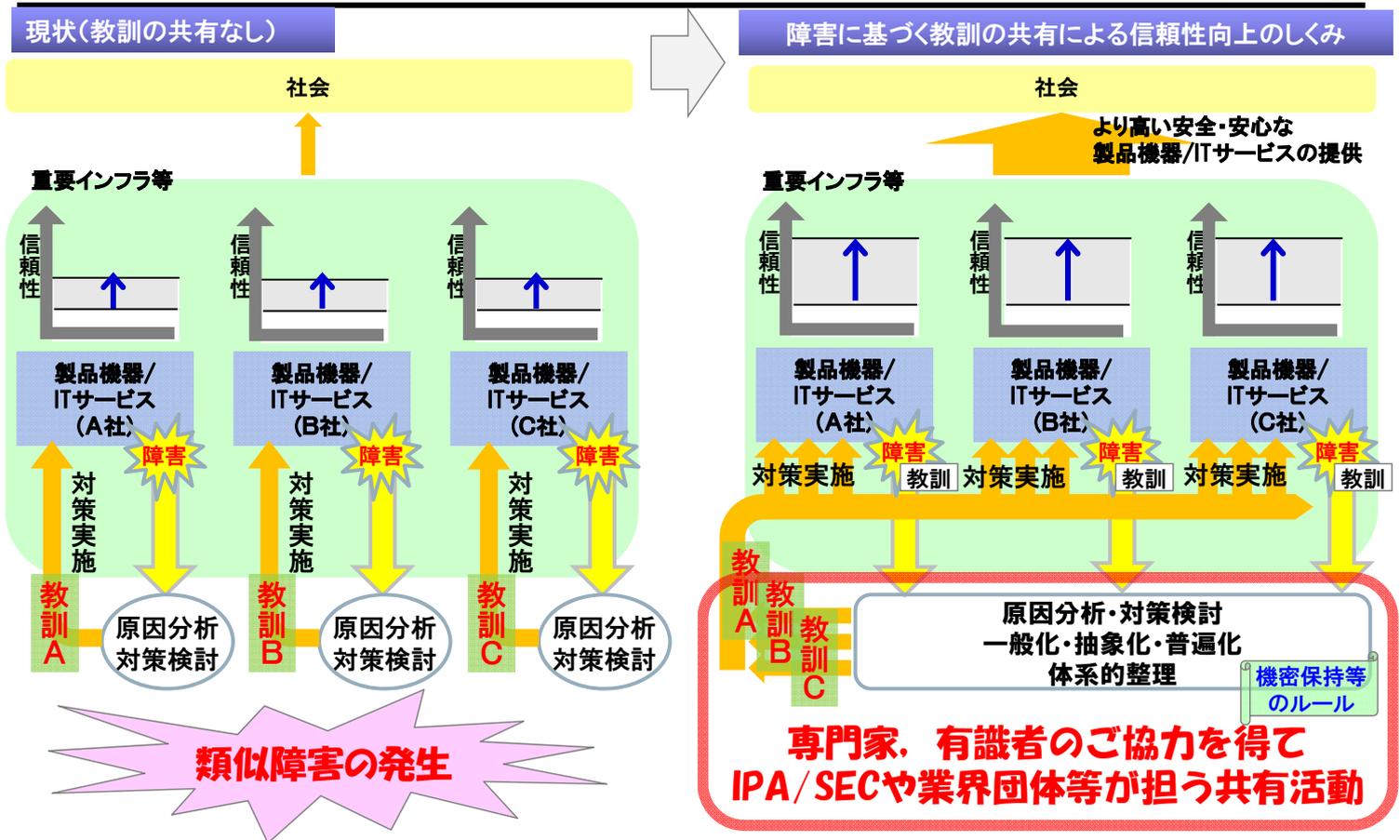


<故障率曲線の原図> "Bathtub curve" by en:User:Wyatts - U.S. Army document. Licensed under Public domain via ウィキメディア・コモンズ - http://commons.wikimedia.org/wiki/File:Bathtub_curve.jpg#mediaviewer/File:Bathtub_curve.jpg

リスクへの対応



教訓共有の取組みの目指す方向



(重要インフラシステム等の)ソフトウェア障害情報の収集・分析



各教訓の構成

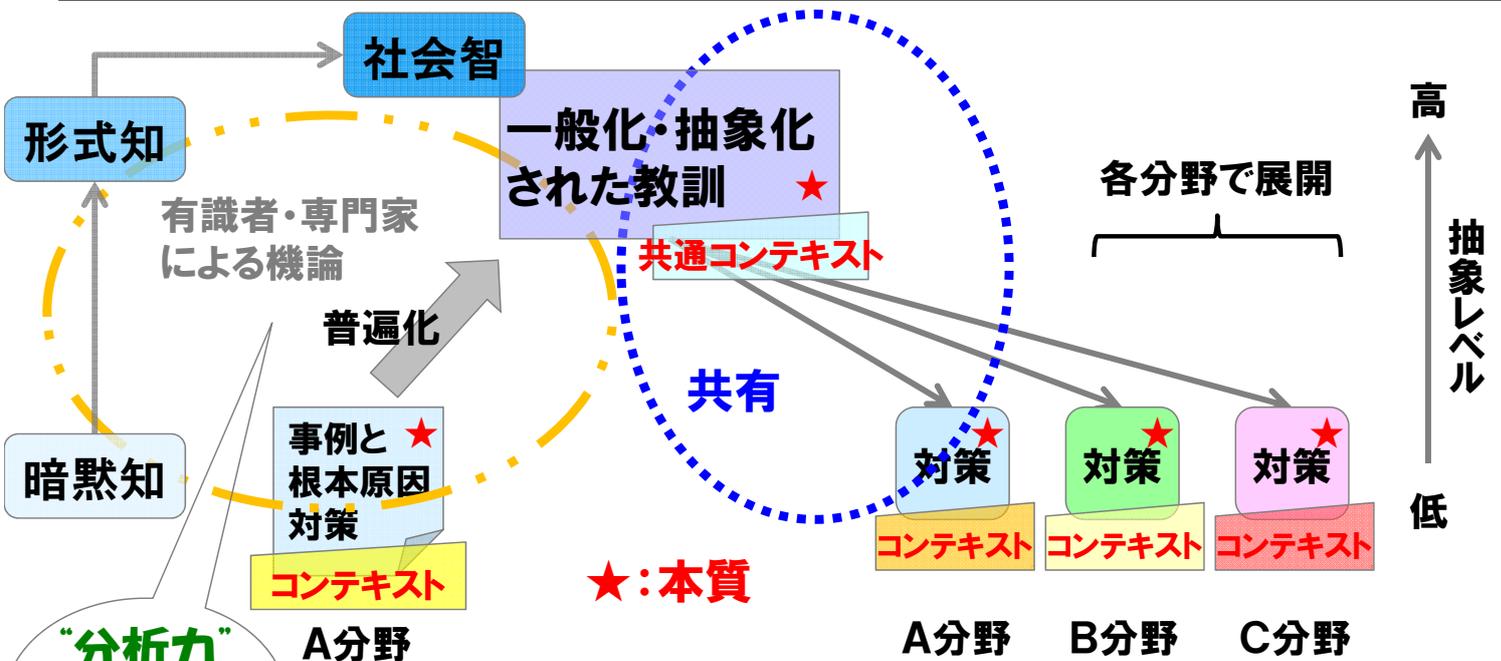
[教訓 I D]
 教訓概要(タイトル)

- 問題**：障害事例の内容
- 原因**：問題を引き起こした要因の分析結果
- 対策**：問題の原因を取り除き再発を防止するための方法
- 効果**：対策の実施により見られた／期待される効果
- 教訓**：得られた教訓の内容説明・補足



i 各教訓の説明 → 後ほど

教訓の作成と活用の流れ



各組織での活用時、**システムティックな取組み**：
 教訓と共に提供されるコンテキストと自身のコンテキストとを比較・照合し、
 適用可能な教訓について、**具体的対策を検討**

プレスリリース: システム障害を未然に防止するためのガイドブック2編を公開

<http://www.ipa.go.jp/about/press/20160229.html>

教訓作成ガイドブック(教訓を作成する)

事例からの学び
(失敗のチャクラ等
の気づきを与えるメッセージ)

(裏返し)

高信頼化への知恵
(成功のチャクラ等の気づき
を与えるメッセージ)

教訓集

各社/組織で作成

抽象化

具体化

IT障害等の事例

ITシステムの開発・運用の
現場フィード
バックIT障害リスク低減の
具体策等教訓活用ガイドブック
(教訓を活用する)

具体化



教訓集

情報処理システム
高信頼化教訓集

IPA/SECが公開

内容

1. IPA/SECにおける障害事例情報分析・共有活動

- 背景
- 取組みと成果概要

2. 保守関連の障害事例の分析に基づく教訓

3. 障害事例から教訓を導く例

4. まとめ

障害事例の分析に基づく教訓 (ITサービス編 概要)

— 2016年 —

独立行政法人情報処理推進機構 (IPA)
技術本部 ソフトウェア高信頼化センター (SEC)

Information-technology Promotion Agency, Japan
Software Reliability Enhancement Center (SEC)

Copyright © 2013-2016 IPA, All Rights Reserved

IPA Software Reliability Enhancement Center

教訓のパターン

SEC
Software Reliability
Enhancement Center

- 人間系の考慮
- 手順・ルールの明確化
- 修正パッチ適用基準
- 機能追加・変更時の確認
- 変化対応

人間系の考慮
手順・ルールの明確化
修正パッチ適用基準
機能追加・変更時の確認
変化対応

1)ガバナンス/マネジメント領域の教訓

No.	教訓 I D	教訓概要
1	G 1	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」をつくるのが大切
2	G 2	発注者は要件定義に責任を持ってシステム構築にかかわるべし
3	G 3	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
4	G 4	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
5	G 5	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
6	G 6	作業ミスとルール逸脱は、個人の問題でなく、組織の問題！
7	G 7	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
8	G 8	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
9	G 9	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
10	G 1 0	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！
11	G 1 1	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
12	G 1 2	キャパシティ管理では、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、管理項目と閾値を設定してPDCAをまわすべし
13	G 1 3	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
14	G 1 4	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

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

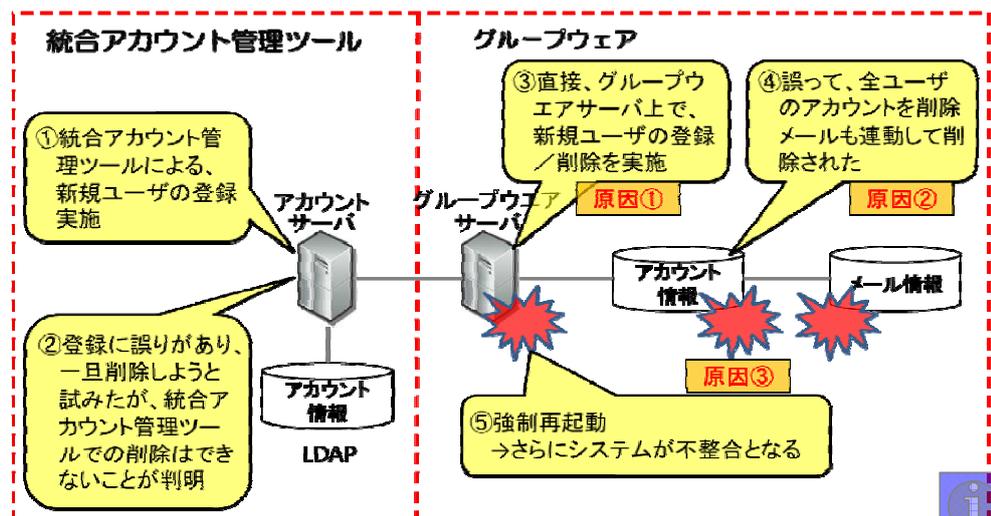
【原因】 不慣れな運用作業者（新人）が、独断で、運用規定外的手段（管理ツールを介さないサーバへの直接アクセス）により、誤操作（**ルール逸脱**）

繁忙な環境下、迅速な処理が求められる状況で、各メンバーがお互いの作業に追われて連携できず、不慣れな作業者は、**多忙な熟練者にも聞くことができず、自分が業務を遅らせる原因になってはいけない**というプレッシャーから、ルール逸脱

運用チーム内のスキルの共有も不十分

【対策】 組織的な総合対策：

- ・ 作業を受ける場合のリスクを考慮した**受諾の判断基準**作成
- ・ 複数名体制での作業実施等、ルールを逸脱しない**作業規定**の作成
- ・ 普段のチーム内の**コミュニケーション**



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

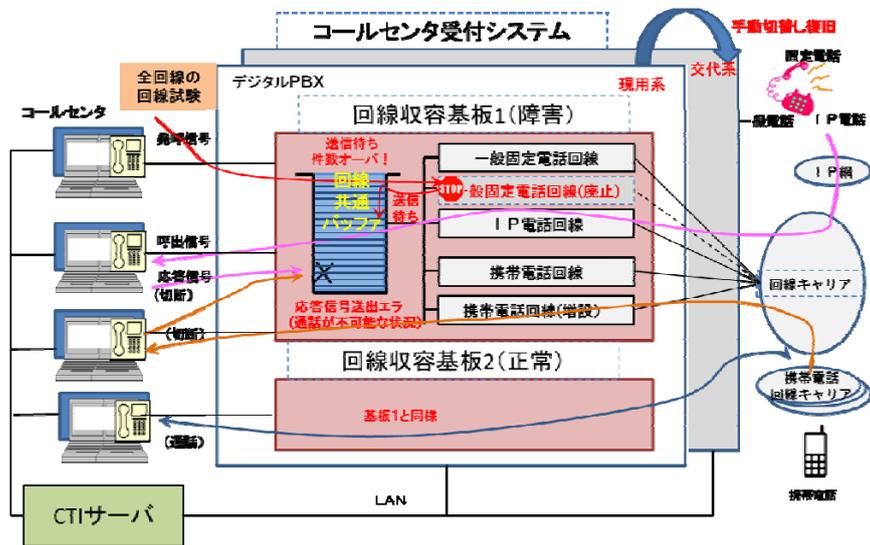
【問題】コールセンタにおいて電話コールの一部が着信後に即切断されてしまう事象が発生していたがイタズラ電話との認識、また通信回線事業者からコールの接続異常が時々発生しているが問題はないかと問合せはあったが他の事業者は正常との回答であったため問題視しなかった。システム障害と気付くまでに4時間経過していた。

【原因】コールセンタ受付システムの回線収容基板上の回線共通バッファがオーバーフローし、コールに対する応答信号の送出が出来なくなっていた。

設定変更ミス：一部の収容回線の廃止に伴う、回線試験用設定の削除を忘れた。

回線試験エラー電文が回線共通バッファに蓄積し、ついにオーバーフロー。廃止回線のため、エラーをおかしいとは思わなかった。

- 【対策】
- ・ 交代系への切替で復旧
 - ・ 保守運用マニュアルの見直し
 - ・ バッファ監視機能追加
 - ・ 回線事業者連絡会の設置



G11:

システムの重要度に応じて

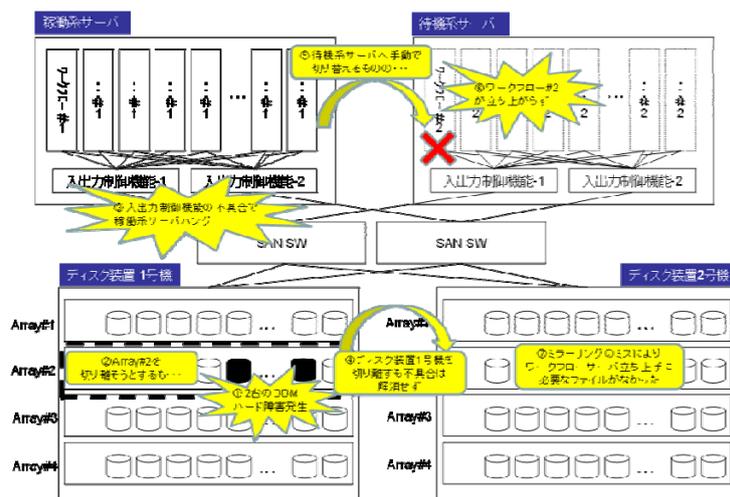
運用・保守の体制・作業に濃淡をつけるべし

【問題】A社の社内ワークフローシステムに障害が発生し、連携している顧客向けサービスが終日全面停止した。システム関係者が集まったものの、状況を把握するのに時間が掛かり、システム停止時間は長時間に及んだ。

【原因】二重化サーバに接続されたRAID5構成のストレージ(2重化)において、同一ARRAY内のディスク2台が同時に故障。当該ARRAYを切り離そうとするも、入出力制御製品不具合によりサーバがハングアップ。サーバを待機系に切り替えようとするも、ストレージのミラーリングの誤設定により必要なファイルが待機系になく、失敗。

ベンダから製品不具合の修正パッチが提供されていたが、他社で大きな影響が出ておらず、A社に知らされず。ミラーリングの誤設定は、保守作業のミス。関係者間でのシステムの共通資料や障害発生時対応マニュアルがなく、復旧に多くの時間を要した。

- 【対策】基幹システムを中心に、顧客への影響の有無、推定される損害額等、システムの重要度に応じたランク付けを行い、そのランクに応じてシステム保守対応を実施するルールを設定。



【問題】 A社のシステムはサービスの継続を優先するデータの非同期送受信（メッセージ交換）型のオンラインシステムである。このシステムの処理件数には、以前から全般的な増加と共に、時々突発的な事象によるデータ量の急増が見られた。このシステムにある日、処理能力を越えたデータが殺到し、サービスが一時的に停止した。

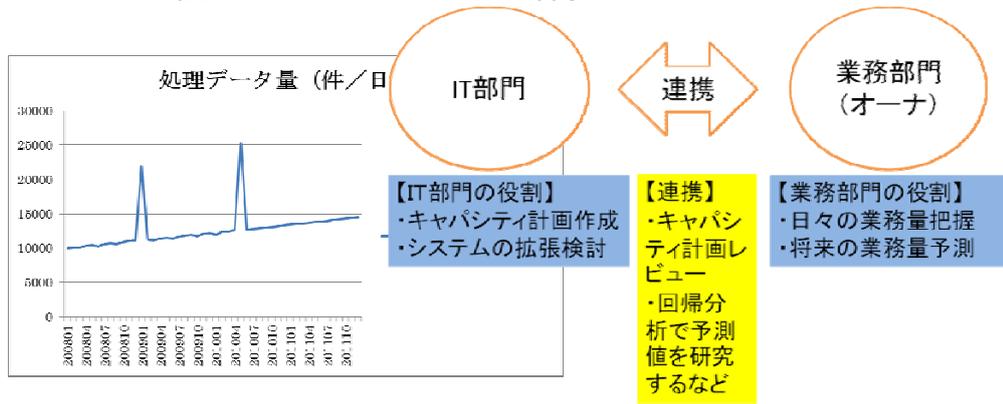
【原因】 突発的な事象によりデータ量が急増した時にサービス停止に至る原因は、キャパシティに関する業務部門とIT部門との合意形成や管理方法が明確でないことによる。

【対策】 ①システムごとにキャパシティ管理の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を構築。

②過去の実績を基に算出したルールに基づいて性能を拡張。（例：「突発的な増加に対応可能な」過去最高実績の2倍のキャパシティを確保）

③システムごとに管理項目と閾値を設定し、キャパシティの拡張方法や拡張限界等を明確化。

④業務部門が需要の将来予測を行い、IT部門がシステムの拡張を検討。



2. 保守関連の教訓

教訓一覧(ITサービス)[技術領域]

2) 技術領域の教訓

No.	教訓ID	教訓概要
1	T 1	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）
2	T 2	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
3	T 3	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
4	T 4	システム全体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
5	T 5	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！
6	T 6	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
7	T 7	バックアップ切替えが失敗する場合を考慮すべし
8	T 8	仮想サーバになってもリソース管理、性能監視は運用要件の要である
9	T 9	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
10	T 10	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
11	T 11	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
12	T 12	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！
13	T 13	利用者の観点に立った、業務シナリオに則したレビュー、テストが重要
14	T 14	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
15	T 15	緊急時こそ、データの一貫性を確保するよう注意すべし
16	T 16	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
17	T 17	長時間連続運転による不安定動作発生回避には定期的な再起動も有効！
18	T 18	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
19	T 19	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！
20	T 20	パッケージ製品の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
21	T 21	作業ミスが減らすためには、作業指示者と作業者の連携で漏れのない対策を！
22	T 22	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ーフローを未然に防止すること

T4:

システム全体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！

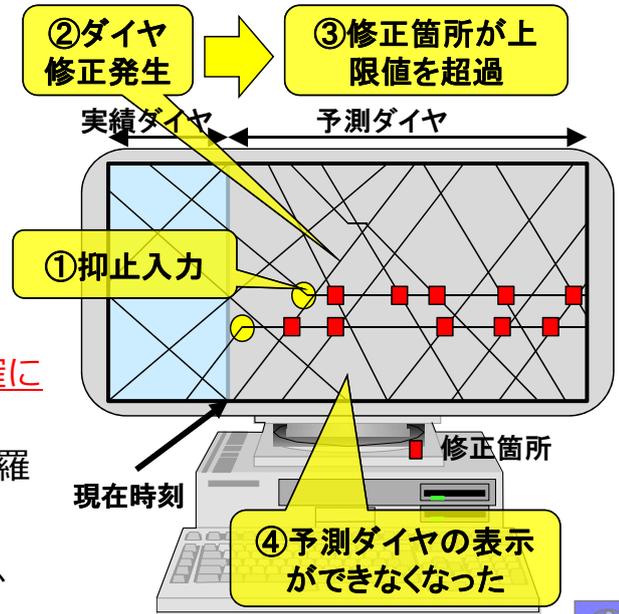
表示項目数がシステムの上限値を超えたため、全画面表示が消え、オペレータが混乱しシステム構築当初から決まっていた上限値について、外部仕様変更に伴う見直しを未実施原因の本質は、全体に影響する変化点（この場合、予測時間、列車運転本数）が不明確

【原因1】 予測時間を4H⇒24Hに変更した際、そのような要件変更があったにもかかわらず、「修正箇所数」の上限値の増加などシステム全体の機能要件変更を未実施

【原因2】 列車の本数が年々増加しており、本来ならば（運転本数の増加の都度）上限値を超えた際のシステムの挙動を見直す必要があったにもかかわらず、未実施

【対策】 制御系システムの変化点の管理ルールを明確にし、そのルールを守る仕組みを構築

- ・システムが監視・制御する対象と仕様の変化点を網羅
- ・変化点管理のルールとそれを守る仕組みを構築
- ・変化点管理で使用する管理指標を関係部門で共有し、「変化点の見落とし」を防止

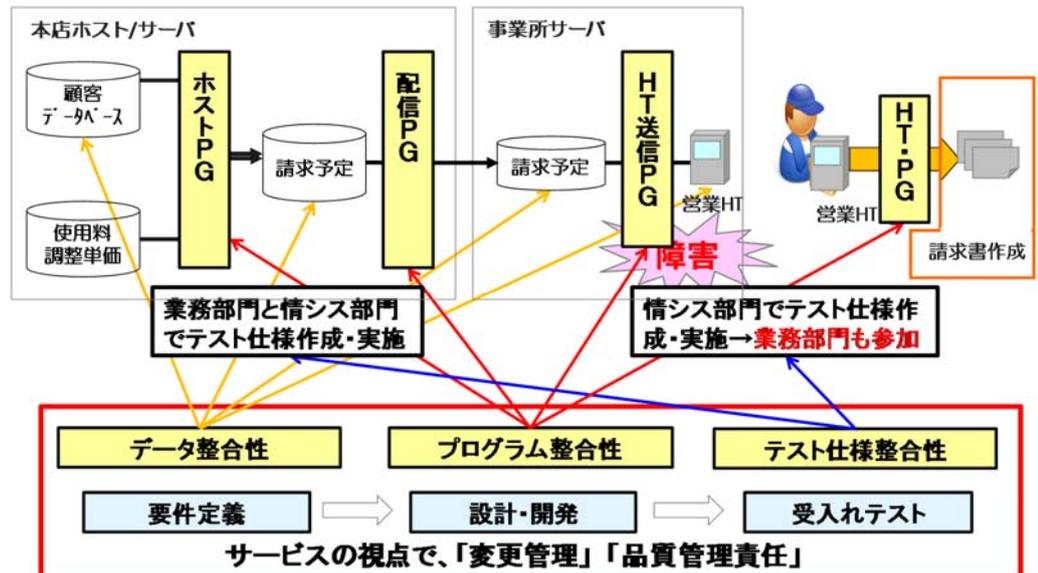


T5:

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/サーバから請求データを端末に転送し請求書を印刷するシステムにおいて、端末として、営業員が持ち歩くHT（ハンディ・ターミナル）を新規に導入したところ、そのシステムから出力される請求書の金額が誤ったまま顧客に渡ってしまい、個別謝罪・請求書の再発行に追われた。

システムへの新たな要件追加、使用方法の変更があると、今まで正常に稼働していたシステムが突如障害となる（追加により未使用・未確認のロジックが使われ、不具合が顕在化）



変更があった時にシステム全体のプログラム、データ、テスト仕様の整合性を保つための変更管理を確実に実施
システム全体の整合性を確認する人を決め、品質管理責任を明確にし、開発フェーズ毎の検証を実施

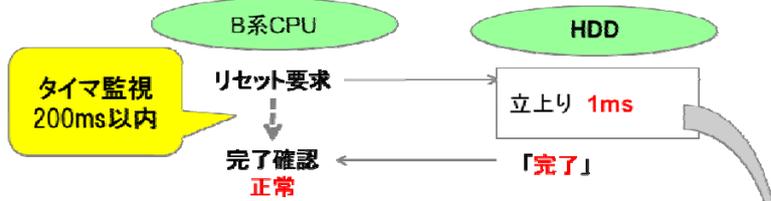
T12:

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!

【問題】 2重化された制御系システムにおいて、部品交換の保守作業時にシステム全体の動作が停止し、短時間で復旧できずに、サービス利用者が終日影響を受けた。

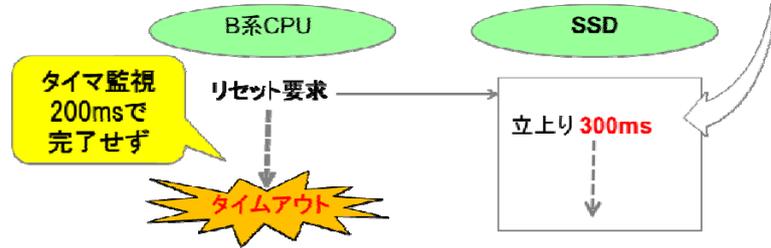
【原因】 システムのディスク装置が、数年前に、当初構築時のHDDからSSDに交換されていた。部品交換作業でA系を切り離れた時にB系OSから両系のディスク装置にリセット要求が発せられるが、SSDのリセット要求処理時間は、HDDのそれよりかなり長く、OSのタイマ監視においてタイムアウトが発生した。その後のリカバリ処理もうまくいかなかった。

【当初:システムディスク=HDDの場合】



SSDへの交換時に、HDDと完全に互換性があると誤認し、検証・テストが不十分であった。

【今回:システムディスク=SSDの場合】



違いあり!

- 【対策】
- 仕様上の互換性を過信せず、差異分析を必ず実施
 - ベンダとユーザの双方が相手の役割分担を支援し合う（ユーザ側でハザード分析を行う）

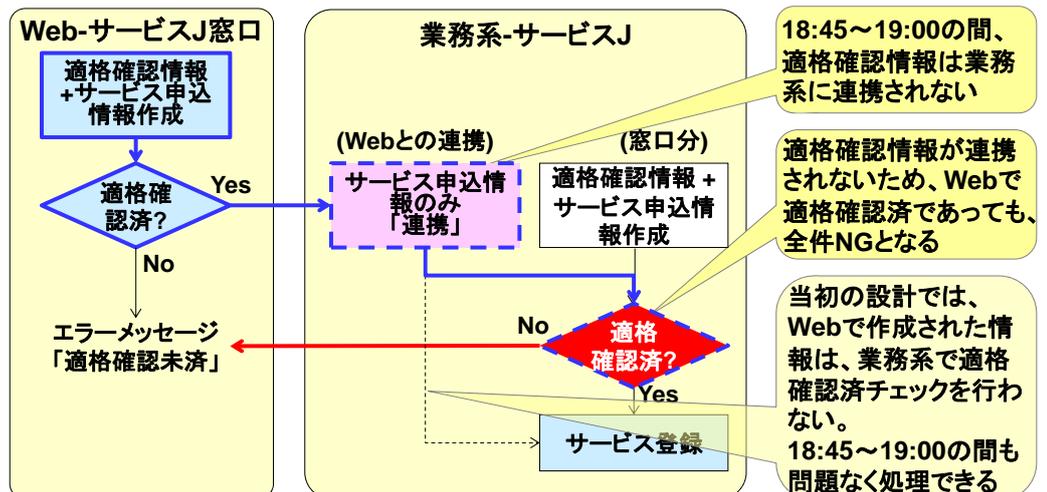
T13:

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

【問題】 オフラインでの申込みのみサポートしていたところを、追加でWeb経由での申込みを可能としたサービスにおいて、特定の時間帯に限り、Webサイトからのサービス申込みが全て不備とみなされ、登録できなかった。顧客からの連絡で判明した。

【原因】 オフライン/Web経由の2系統のサービス申込みを処理するロジックにおいて、各系統の処理間でのデータの連携に誤りがあった。根本原因としては、全体設計が個別システム設計に正しく引継がれなかったことと、業務シナリオに即した確認が行われず、設計後のレビューでも発見されず、対応するテストも行われなかったこと。

【対策】 処理ロジックを正しく修正した。また、要件定義・設計段階でウォークスルー等により関係者相互で確認するとともに、利用者の観点に立った、業務シナリオに即した検証を行うようにした。



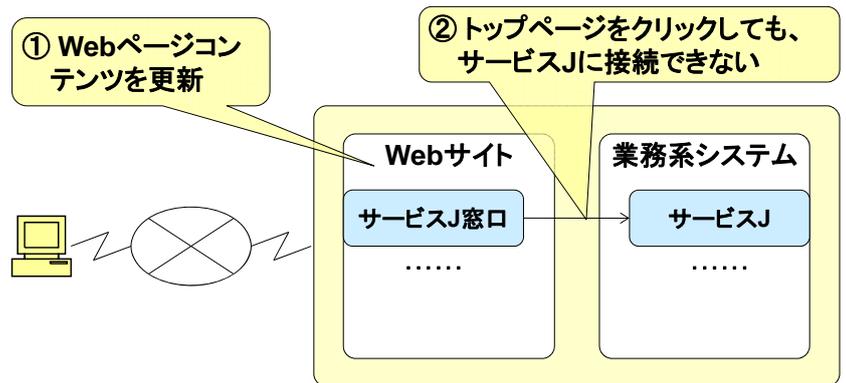
T14:

Webページ更新時には、 応答速度の変化、性能面のチェックも忘れずに

- 【問題】 Webサイト上のあるサービスのトップページをクリックすると、応答に長時間を要し、目的のサービスに接続できないケースが多発した。
- 【原因】 業務部門がトップページのコンテンツを更新した結果、1顧客当りのダウンロードサイズが4倍になったが、応答速度への影響を確認しないままリリースした。
業務部門はダウンロードサイズと応答性能との関連を意識せず、それに関するIT部門による技術的な確認がルール化されていなかった。
- 【対策】 業務部門がWebページコンテンツを更新する際には、IT部門が技術的な観点で確認を行うことを手順書に明記するとともに、IT部門が必要と判断した場合、業務部門に対しリリース中止を指示できるようルールを改めた。

次の直接的対策も実施：

- 当該トップページへのアクセスを高速ネットワークサービス経由に変更
- コンテンツ変更量の自動チェック機能を導入し、最新のコンテンツ量とアクセス量を可視化

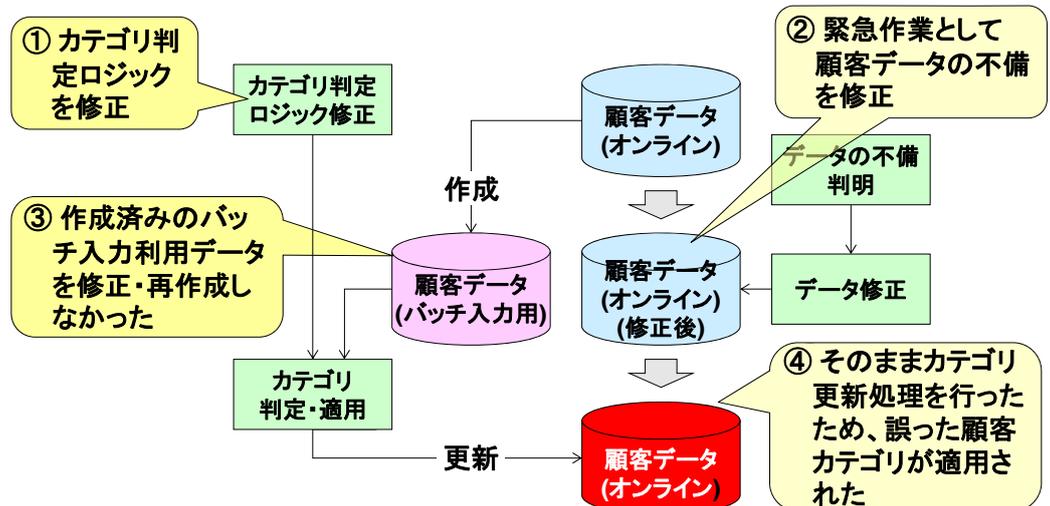


T15:

緊急時こそ、データの一貫性を確保するよう注意すべし

- 【問題】 毎月末に、顧客のカテゴリ判定バッチ処理を、あらかじめ作成しておいた顧客データ（マスタ）のコピーを用いて行う運用において、ある時、緊急の要請により、マスタを修正して対応したことがあった。その後のオンライン処理において、誤った顧客カテゴリが適用された。
- 【原因】 緊急対応後に、マスタから顧客カテゴリ判定用コピーの再作成を行わなかったため、マスタとコピーとの不整合が発生していたにも関わらず、そのまま、カテゴリ判定処理を行ったため。

- 【対策】 緊急時対応の影響範囲を見極め、対応結果が平常時のシステム運用の流れに確実に繰り込まれるよう、特に意識するよう周知するとともに、作業ルール・手順書を明確化。



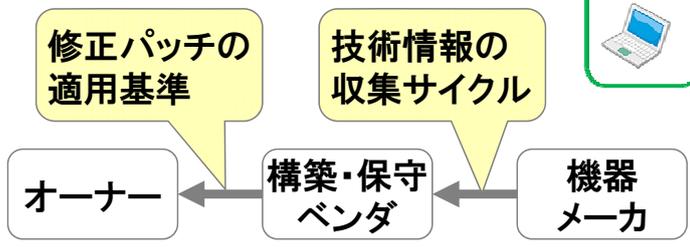
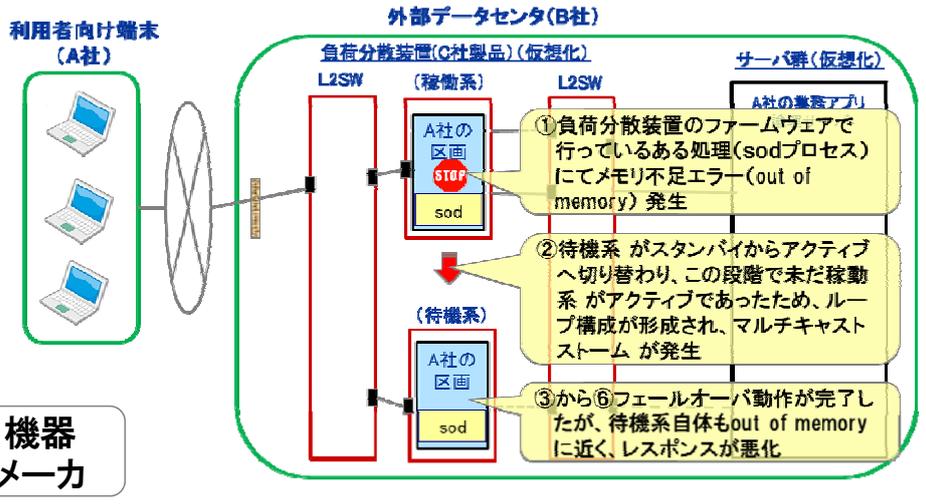
T16:

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

【問題】 システムの通信機器（負荷分散装置）に障害が発生し、丸1日間業務が停止

【原因】 システム構築・保守ベンダが外部メーカから調達した負荷分散装置のファームウェアの既知の不具合が直接の原因であり、その修正パッチが1ヵ月前に公表されていたが、ベンダによる修正情報の収集間隔が3ヶ月に1回程度と非常に粗く設定していたため、その適用が間に合わなかった。システムのオーナーは、技術情報が時々公表されていることを認識していなかった。

- 【対策】
- 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
 - オーナーとベンダとでパッチ適用基準の協議



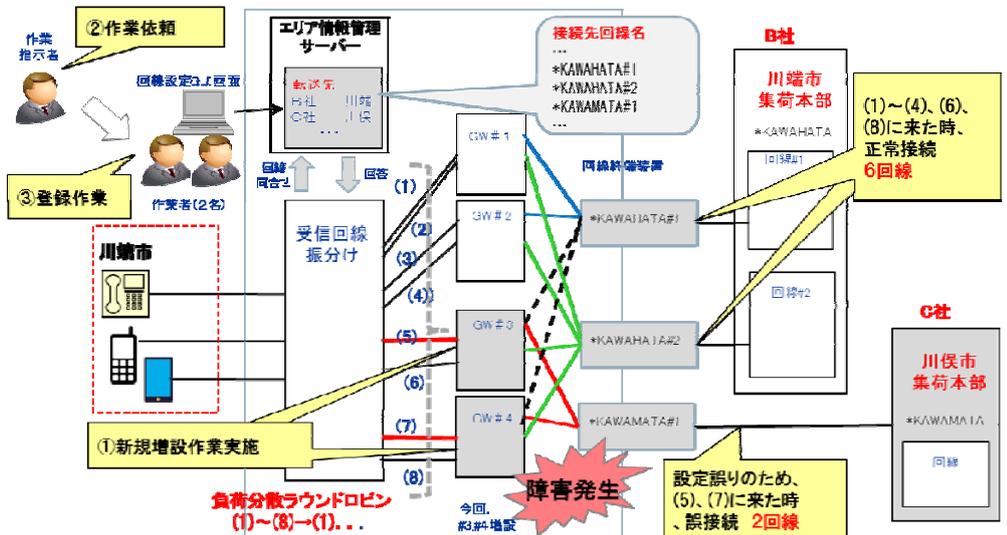
T21:

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！

【問題】 顧客からの集荷依頼を転送するサービスを行うA社は、振分けシステムの運用ミスにより、4回に1回の割合でB社への集荷依頼を誤ってC社集荷本部に転送していた。現場は混乱し、集荷作業漏れが多発し、顧客からの苦情が殺到していた。

【原因】 システム（海外製品）のゲートウェイ装置増設に伴う転送情報登録時に、**作業者が誤設定**。（“KAWAHATA”とすべきところを“KAWAMATA”と設定）
根本的には、誤りを犯し、見逃しやすい**作業環境**と、最後の砦となるべき**作業指示者の確認不足**があった。

- 【対策】
- 作業手順の明確化：設定値を自ら読上げ、設定作業後の差分チェック、**作業指示者による確認**、全ルート確認テストの実施
 - 機器メーカへの依頼：表示エリアの限定、ルートの疑似確認機能の追加、等



キャッシュへの排他制御がパッチで追加

トラブルの発端となったのは、LHSから提供を受けJALが3月23日に適用したパッチ。・・・このパッチはJAL以外のユーザー企業からの要望で提供されたものという。・・・「なぜキャッシュの排他制御を施すことにしたのかについて、説明は受けていない。またパッチの内容についても詳しい説明は受けていない」(JAL)という。問題のパッチは「JALの要望で開発してもらったものではなく、JAL側でカスタマイズしたりもしていない」(JAL)という。

JALは、排他制御の見直し以外に、(1)待機系の処理性能を本番系と同程度まで強化する、(2)LHSとの情報共有を密にする、(3)外部ベンダーのエンジニアの協力を得つつ、パッチ適用前の検証などを強化する——といった対策を進めるとしている。

〈出典〉 JALシステム障害、前週に追加の排他制御がデッドロックを誘発

IT Pro, 2016/04/06 <http://itpro.nikkeibp.co.jp/atcl/news/16/040601011/>

内 容

1. IPA/SECにおける障害事例情報分析・共有活動

- 背景
- 取組みと成果概要

2. 保守関連の障害事例の分析に基づく教訓

3. 障害事例から教訓を導く例

4. まとめ

事例を用いた説明

【教訓タイトル】

<抽象的な表現の例>

システムの部分変更(に伴う新旧混在)時に(非変更部分との)整合性を確認する。

<具体的な表現の例>

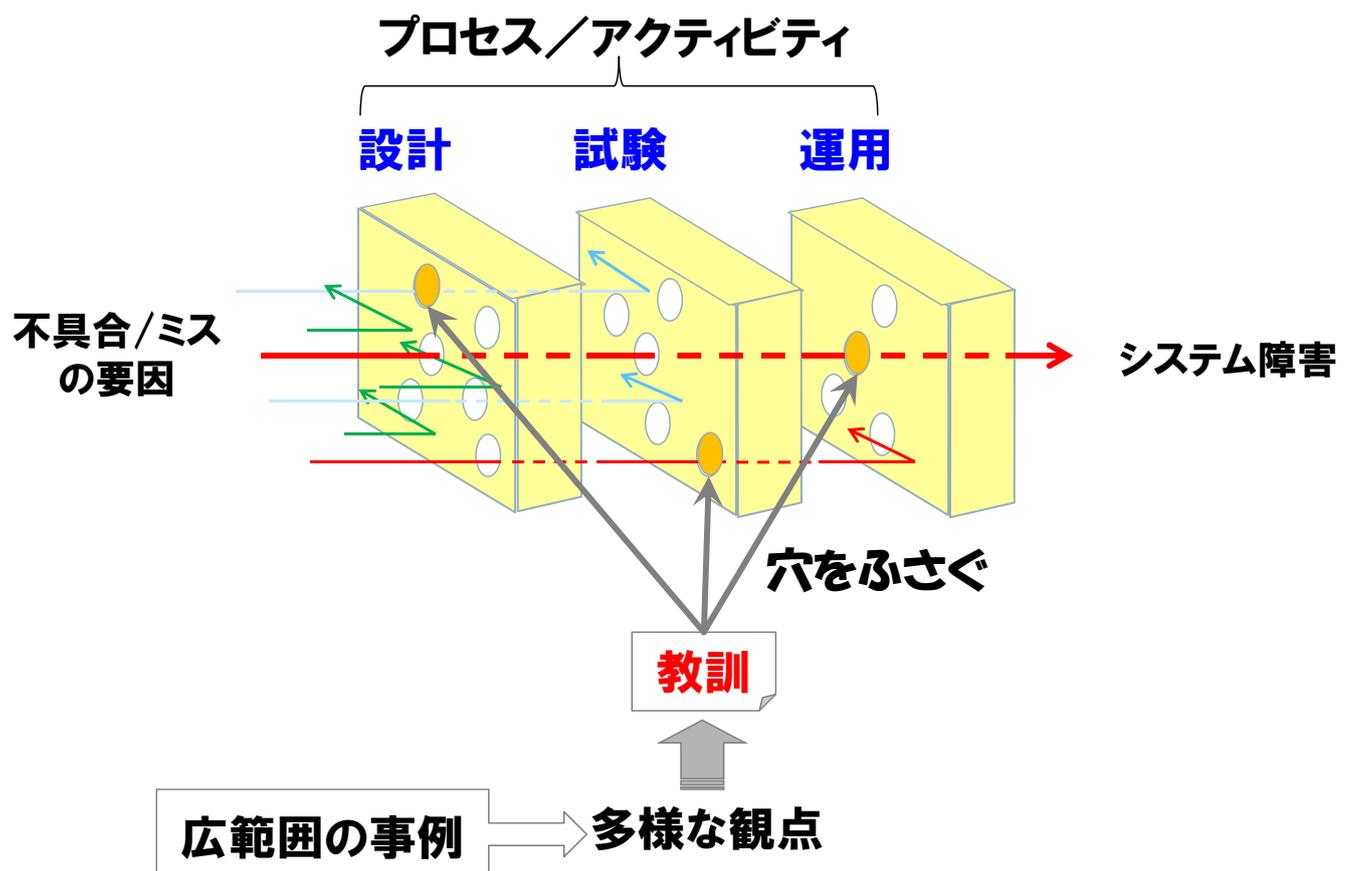
変化に対応して(プログラム/システム定義データ中の)定数をチェックする。



i 教訓導出事例の説明

参考

安全文化: スイスチーズモデル



1. IPA/SECにおける障害事例情報分析・共有活動

- 背景
- 取組みと成果概要

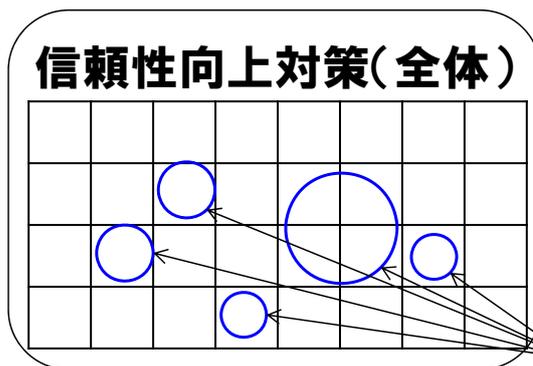
2. 保守関連の障害事例の分析に基づく教訓

3. 障害事例から教訓を導く例

4. まとめ

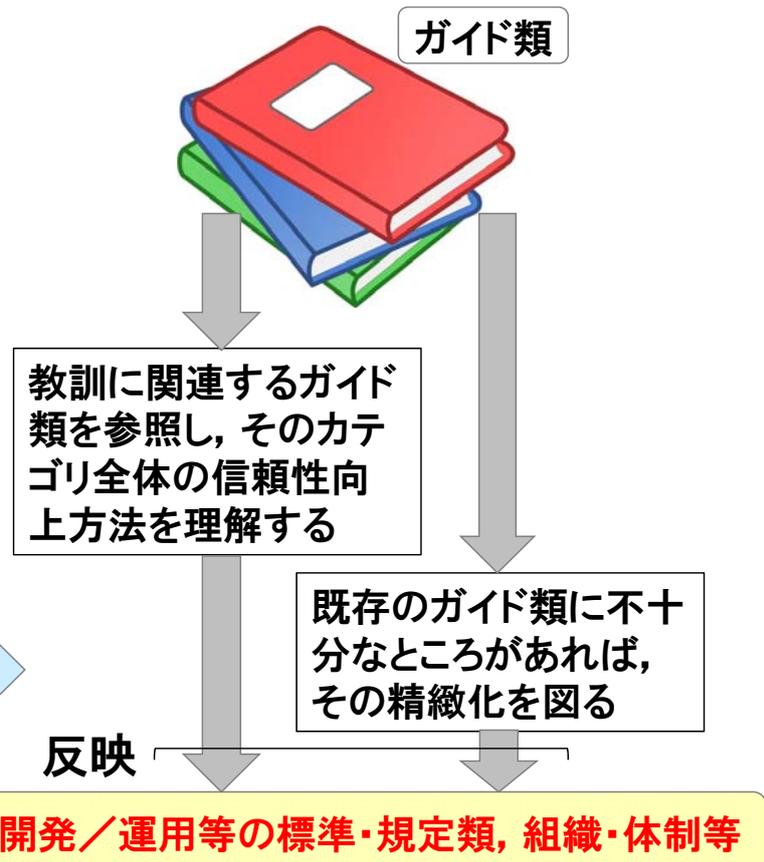
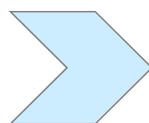
4. まとめ(に代えて)

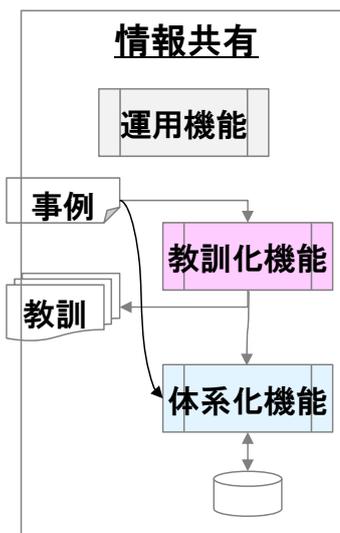
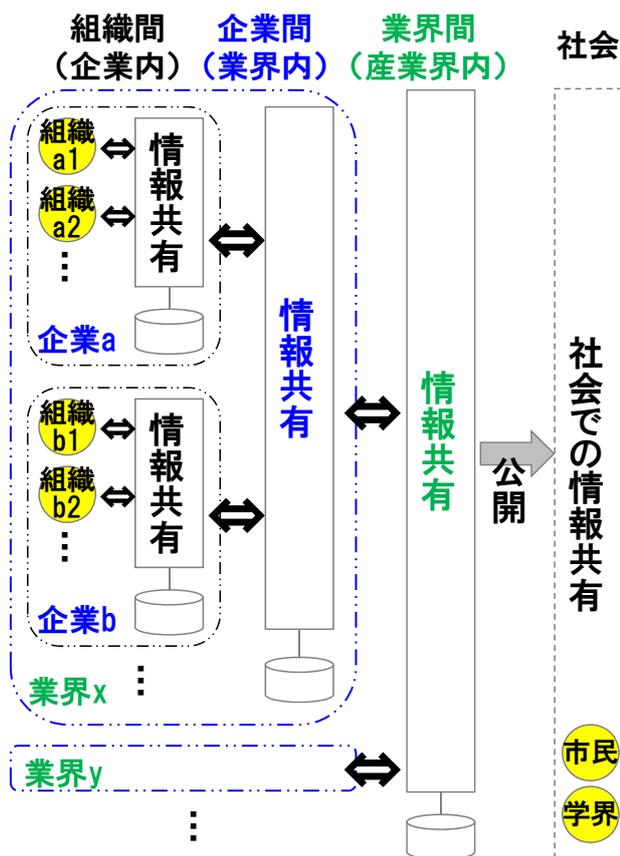
体系的な対策に向けて



教訓(再発防止策)

障害事例に基づく対策は部分的
→
体系的な対策も重要





各機能主体の例

- ・持ち回り
- ・(業界)団体
- ・IPAなど

ご清聴, ありがとうございました

<http://www.ipa.go.jp/sec/system/index.html>

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 –

http://www.ipa.go.jp/sec/reports/20160331_1.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 –

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



参考

情報システムの障害情報データ



http://sec.ipa.go.jp/sweipedia/?s=%E6%83%B5%E5%A0%B1%... 情報システムの障害状況 | SW...

ファイル(E) 編集(E) 表示(O) お気に入り(A) ツール(T) ヘルプ(H)

SWE iPedia

IPA 独立行政法人情報処理推進機構 》 ソフトウェア高信頼化センター(SEC) 》 SWE iPedia

お知らせ : 4月26日に書誌情報を追加しました。

詳細検索 情報システム! 組込みシステム! 統合システム!

最近のSEC成果 製品・制御システム高信頼化! ITサービス高信頼化! 外リクス分析! ソフトウェア品質説明力! ソフトウェア高信頼化!

Home » Search results for "情報システムの障害状況"

キーワード検索

情報システムの障害状況の検索結果

ヒット件数: 10件

SEC journal

2010年以降

報道された障害事例をリストアップし、一部を分析

連載

情報システムの事故データ

情報システムの障害状況 2015年後半データ

IPA 顧問 松田 晃一 SEC システムグループ 主任 八嶋 俊介

2015年7月から12月までに報道された情報システムの障害状況を報告する。この間に報道された障害は合計24件で月平均4.0件となった。平均的な値に対しやや多い値である。とくに今期はその開始に伴いその関係の障害が多く発生している。また、長期間認識されずに運用されてきた不具合が発覚した事故が発生している。

1. はじめに

本稿では、2015年7月から12月までの2015年後半の半年間に報道された情報システムの障害状況をとりまとめ報告する。まず、次章で今期の概況について述べ、続く

今期はマイナンバー関連の事故の発生していることが特徴的である。今期から本される重要な社会インフラとして運用があるため、関連の事故の概要について今期の事例の中には、以前から内在

詳細検索は [こちら](#)

SEC journal最新号

ダウンロードランキングカテゴリー

- SEC journal...
- SEC journal...
- SEC Reports (6)
- SEC BOOKS (3)
- SECセミナー (3)
- SECイベント (11)

ジャンル

- ガイド
- 調査報告
- 普及啓発
- 概要・概説
- 活動報告
- 活用ドキュメント
- 活用事例

SECコスト本誌表紙 SECイベントITサービス継続システム課題プロジェクト管理経営インタビュー SEC Reports

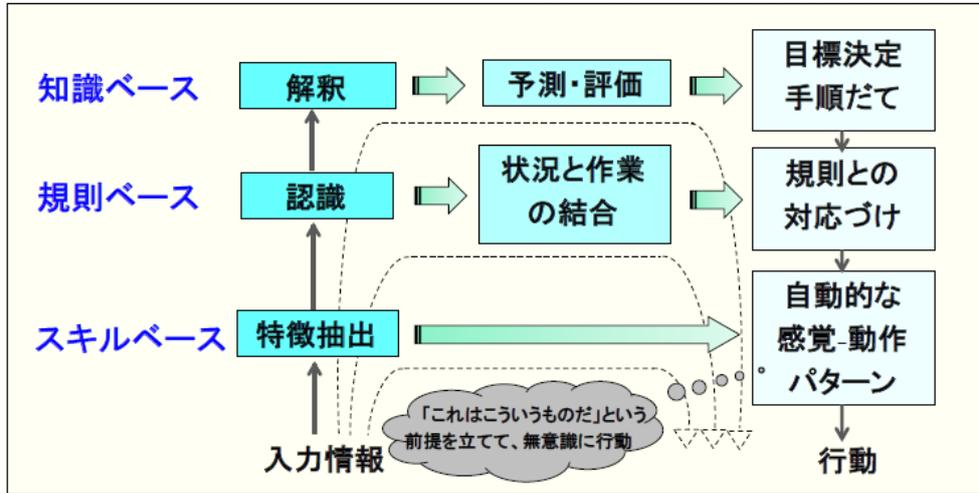
発行日	種別	タイトル
2015/09/01	SEC journal 報告	情報システムの障害状況2015年前半データ
2015/03/01	SEC journal 報告	情報システムの障害状況2014年後半データ
2014/09/30	SEC journal 報告	情報システムの事故データ 情報システムの障害状況2014年前半データ
2014/03/31	SEC journal 報告	情報システムの障害状況2013年後半データ
2013/09/30	SEC journal 報告	情報システムの障害状況 2013年前半データ 情報システムの事故データ
2013/03/08	SEC journal 報告	情報システムの障害状況・2012年後半データ
2012/09/28	SEC journal 報告	情報システムの障害状況 2012年前半データ
2012/03/30	SEC journal 報告	情報システムの障害状況2011年後半データ
2012/01/12	SEC journal 報告	情報システムの障害状況2011年前半データ
2011/10/13	SEC journal 報告	情報システムの障害状況2010年データ

参考) 錬度“過信”に関わる落とし穴



- 習熟度が上がると‘思い込み’や‘取り違い’によるミスが増加する。

(特に「事例類推法」による見積もりは注意)



— SRKモデル —

source; J.Rasmussen

- 対策として多面・多重化(人‘他視点’、方式)、ワーストケース思考や標準化の推進などの取り組みを強化する。

<出典>
太田氏(株式会社ジャステック)の調査検討資料

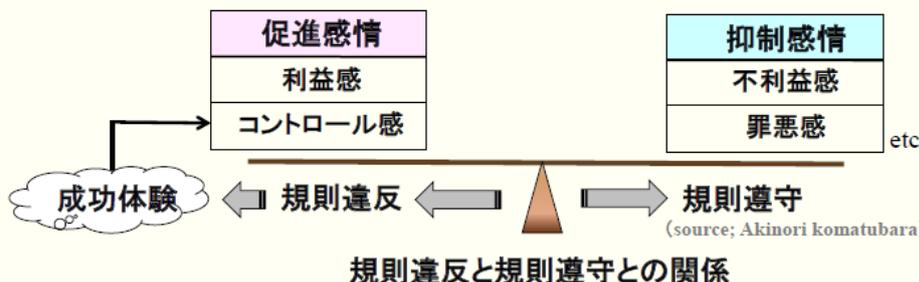
Copyright 2014(C) JASTEC CO.,LTD.

1

参考) 期間短縮に関わる留意点(人間系)

— 不合理な期間短縮を強要すると —

- 人はベテランうんぬんに関係なく、慌てている時に‘取り違い’や‘短期失念’などのミスが増加する。
- 人は近道心理・合理性心理および対人関係心理(答えたい)などの背後要因から‘手抜き(違反)’が醸成され、結果、QCDにダメージを与えるケースが、ベテランになるほど起こりやすい。



規則違反と規則遵守との関係

<出典>
太田氏(株式会社ジャステック)の調査検討資料

Copyright 2014(C) JASTEC CO.,LTD.

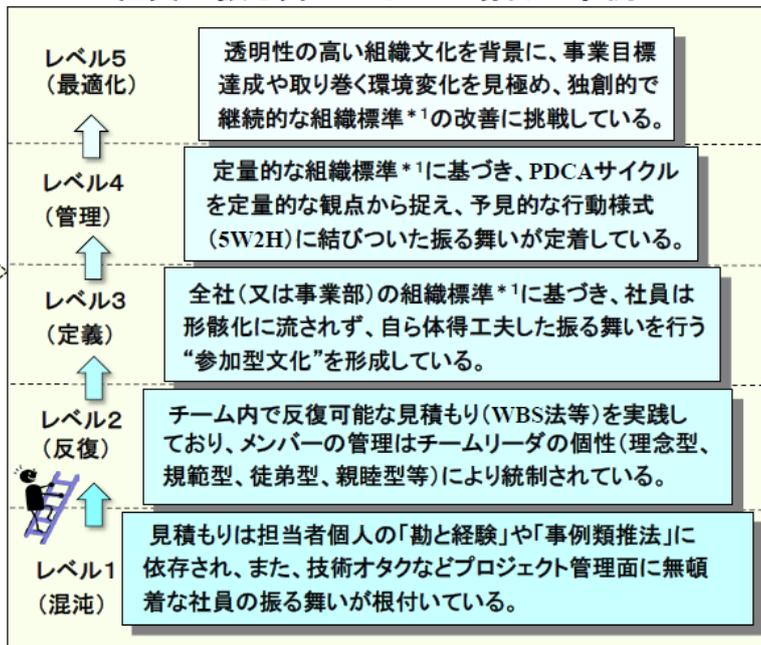
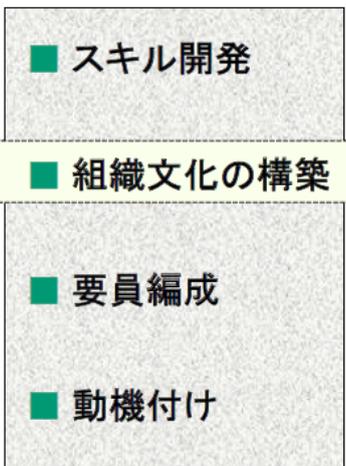
2

参考) 人間系の組織能力成熟度



— 社員の振る舞いからみた場合の事例 —

人間系の
組織能力成熟度の分類



組織標準*1: 見積り方式、出来高管理手法および品質管理手法など source: Tadao.Ota
Copyright 2014(C) JASTEC CO.,LTD. 3

<出典>
太田氏(株式会社ジャステック)
の調査検討資料

(教訓関連事例) 新幹線の電光掲示板不表示トラブル

大型連休後半の4日の始発から、JR東日本管内の東北、上越、北陸各新幹線の全44駅で、行き先や発車時刻を知らせる電光掲示板が表示されないトラブルが発生。終日、復旧せず。

連休で増発した列車本数が表示システムの上限を超えたことが原因とみられる。

同システムは2日分で計1600本が登録できるが、3~4日の列車本数は1606本だった。

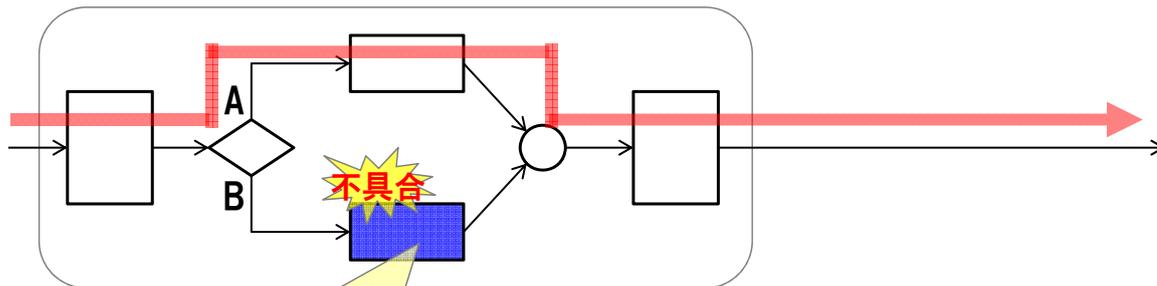
<出典> 毎日新聞, 2016年5月4日

<http://mainichi.jp/articles/20160505/k00/00m/040/017000c>

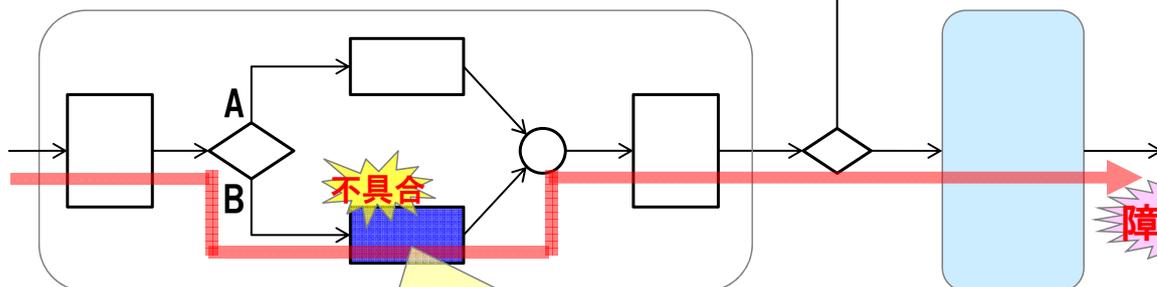
新幹線の列車運行管理システム(COSMOS)において、各駅の運行制御装置(PRC)が旅客案内装置(PIC)に中央装置から送られてきた5月4日分の運行データを転送した時点で、PIC内のデータ数が上限値を超えたため、その時にPICは転送されたデータ(5月4日分)をすべて廃棄した。しかし、そのことを示すメッセージ等の制御端末への表示は行われなかった。

新規サービス追加により潜在不具合が顕在化 (1/2)

構築当初の基本サブシステム



実際には通らない論理
/起動されない処理

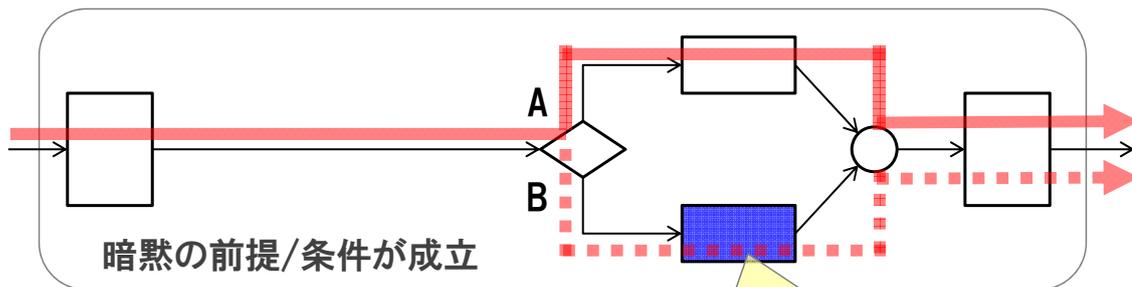


新規追加サブシステムが動作すると
通り得る論理/起動され得る処理

後に追加したサブシステム
(新規サービス追加のため)

新規サービス追加により潜在不具合が顕在化 (2/2)

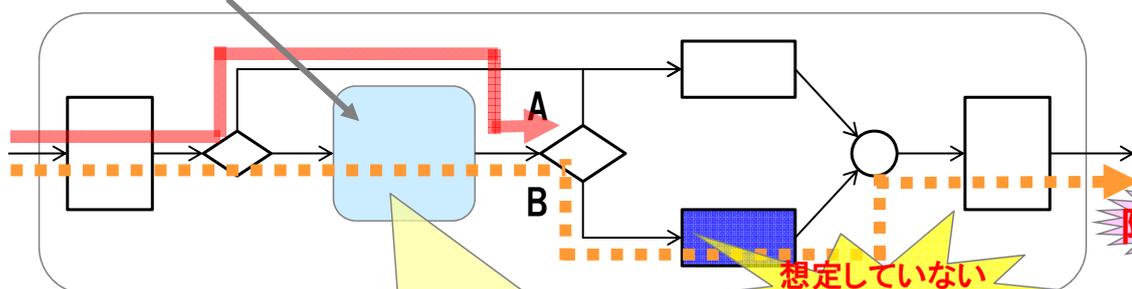
構築当初の基本サブシステム



暗黙の前提/条件が成立

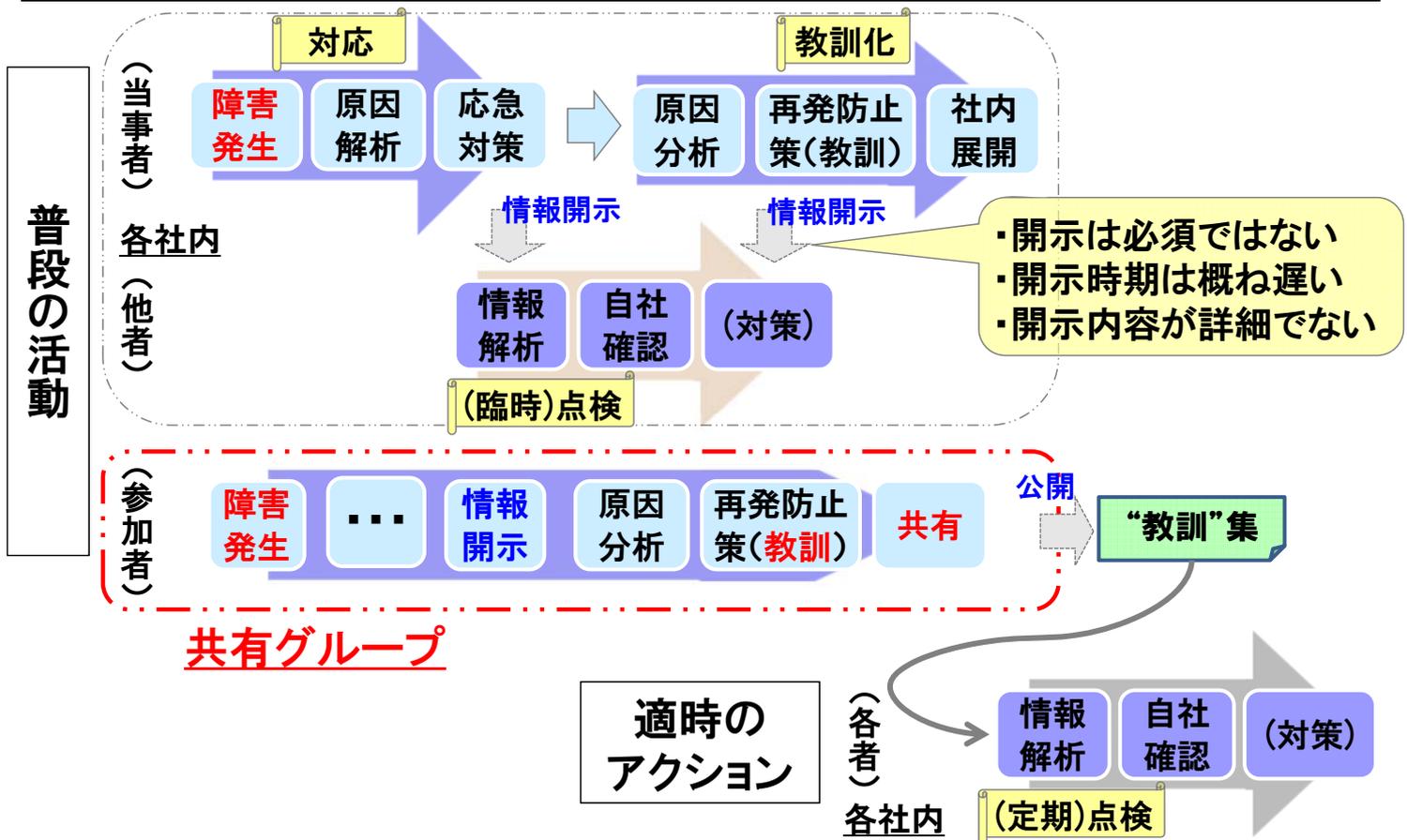
(新規サービス追加のため)
後に追加したサブシステム

想定した前提/条件の下で
意図通りに動作



新規追加サブシステムが動作すると
当初想定的前提/条件と異なる状況に

想定していない
前提/条件のため、
意図しない動作



障害事例活用

他所でのシステム障害発生時の一般的対応

臨時点検



※詳細情報の入手の都度、必要に応じ、追加点検

点検や対応の範囲や観点

…自システムのライフサイクルにおける段階により異なる

- 開発前：類似障害が発生しないような方式の採用・対策の実施を、プロセスを含む開発計画に盛り込む
- 運用中：類似障害の発生するリスク要因の有無確認、発生時の影響の見積り

- 障害の原因により、点検や対応の重点、実施部門が異なる
- 障害の発生したシステムの応用分野により、自システムと同じ分野であればより慎重になる等、点検や対応への“心構え”が異なる？

定期点検

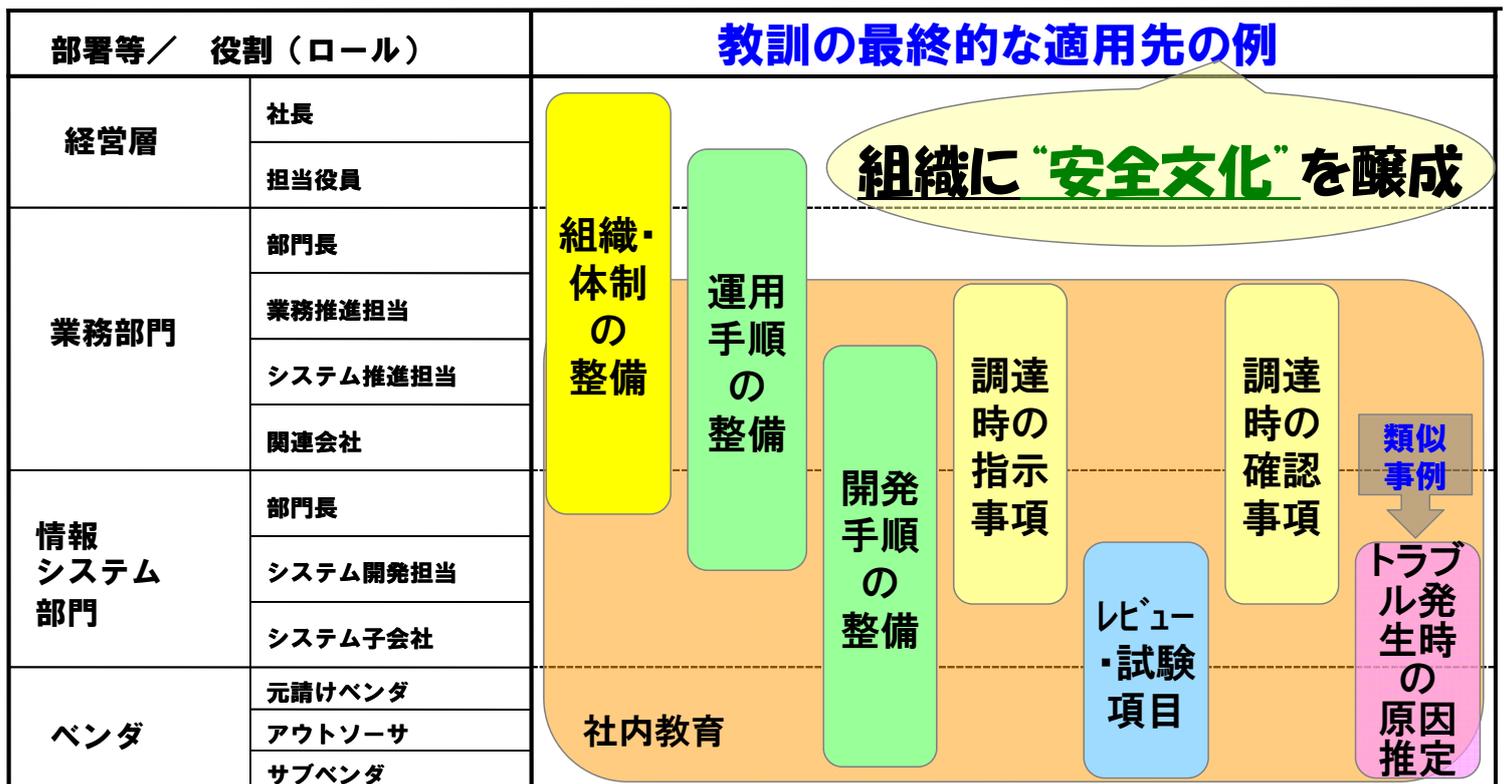
教訓：障害発生から一定の時間が経過。内容は整理されている。

社内の開発・運用標準に規定された、自システムのライフサイクルにおける特定の段階で、自システムのリスク評価
(例：チェックリスト)

個々の教訓に関する確認の観点

- 自システムで類似の障害は起きないか？
- 類似障害の発生防止のため、あらかじめ実施しておくべき対策はないか？
- 万一類似障害が発生した場合の影響は、どの程度か？
- 類似障害発生時に影響範囲を小さくする対策はあるか？

教訓の恒久的な反映



<出典(縦軸)> SEC BOOKS「経営者が参画する要求品質の確保～超上流から攻めるIT化の勘どころ～」, p.37の3.2(1)項、p.41の4.1

「他山の石」の意味※

他人の誤った言行やつまらない出来事でも
それを参考にしてよく用いれば、
自分の修養の助けとなる

失敗に学ぶ → 類似障害の発生を防止できる

「対岸の火事」

※(出典) 文化庁月報 平成23年10月号(No.517)

http://www.bunka.go.jp/publish/bunkachou_geppou/2011_10/series_08/series_08.html

「情けは人のためならず」の意味※1

人に対して情けを掛けておけば、
巡り巡って自分に良い報いが返ってくる

“社会間接互惠性” ※2

ある個体が利他行動(他者に親切にする行動)を行った結果、
その個体の評価が高まり、他者に行った利他行動が回り
回って別の他者から返ってくる仕組み

「ヒト」は、日常生活で困っている他人を見ると、それが自分の知らない人で
あっても助けたい衝動にかられ、多くの場合何らかの親切を行う性質を持つ

※1 (出典) 文化庁月報 平成24年3月号(No.522)

http://www.bunka.go.jp/publish/bunkachou_geppou/2012_03/series_08/series_08.html

※2 (出典) 大阪大学大学院人間科学研究科の実証実験成果から 2013年8月8日

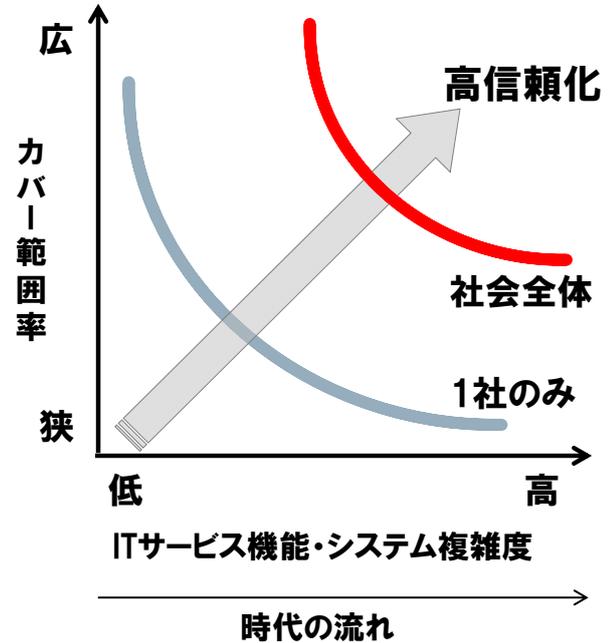
http://www.osaka-u.ac.jp/ja/news/ResearchRelease/2013/08/20130808_1

みんなの力で全体をカバー

ITサービスの機能やシステムが複雑化すると、単一事業者のカバーする知見の範囲は、相対的に狭くなる。

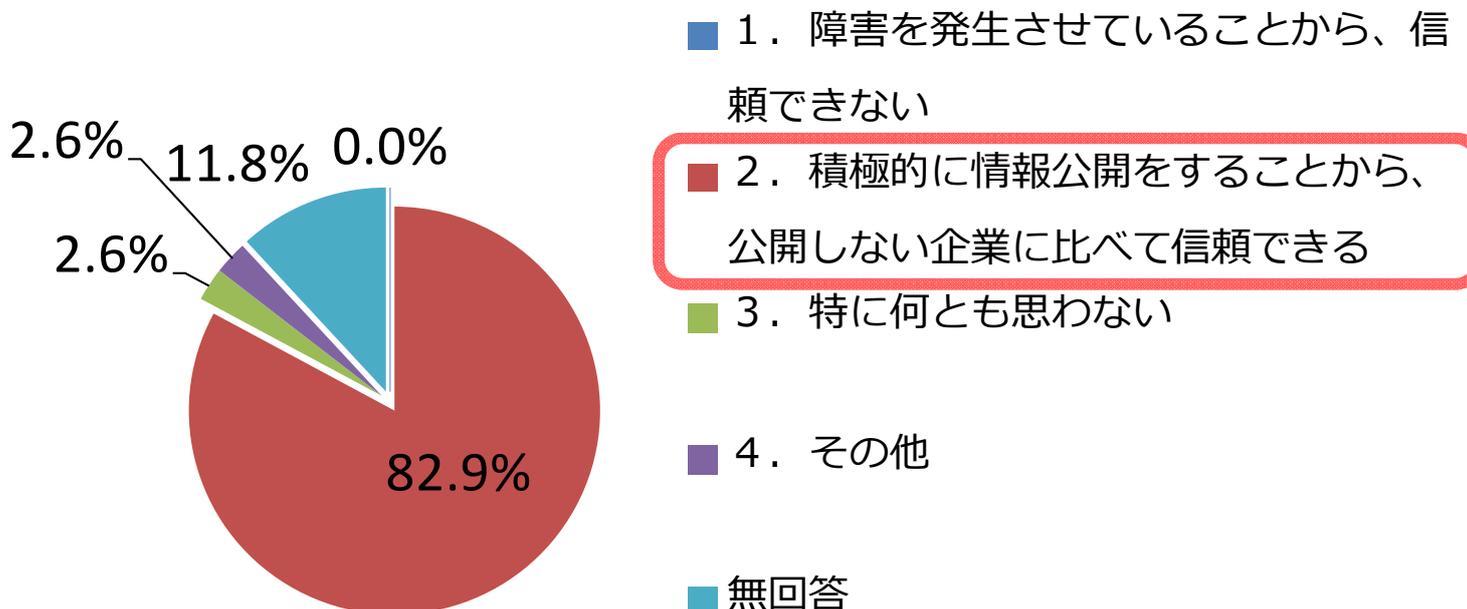


1事業者に囲われた経験と情報を幅広く社会全体で共有し、障害対策などに有効活用できることが重要。



アンケート例

障害事例情報を公開する企業に対して、どのように思われますか？(回答者76名)



<アンケート回答者(計76名)>
ET2013(2013年11月)
ソフトウェアジャパン(2014年2月)