IPA Better Life with IT

近年のソフトウェア障害事例の分析により得られた教訓例

～IPA/SECによるシステム障害事例情報の分析・共有の取組みから～

日本ファンクションポイントユーザ会（JFPUG）総会

2017年1月20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）

山 下　博 之

sec-sys-infb@ipa.go.jp

Information-technology Promotion Agency, Japan

Software Reliability Enhancement Center (SEC)

本講演の趣旨

SEC
Software Reliability Enhancement Center

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．その結果は，抽象化・普遍化してまとめた，「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，よくありがちな事例の教訓をいくつか説明する．

内 容

SEC
Software Reliability
Enhancement Center

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. よくありがちな事例の教訓
3. 障害事例・教訓の活用
4. まとめ

内 容

SEC
Software Reliability Enhancement Center

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. よくありがちな事例の教訓
3. 障害事例・教訓の活用
4. まとめ

背景

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

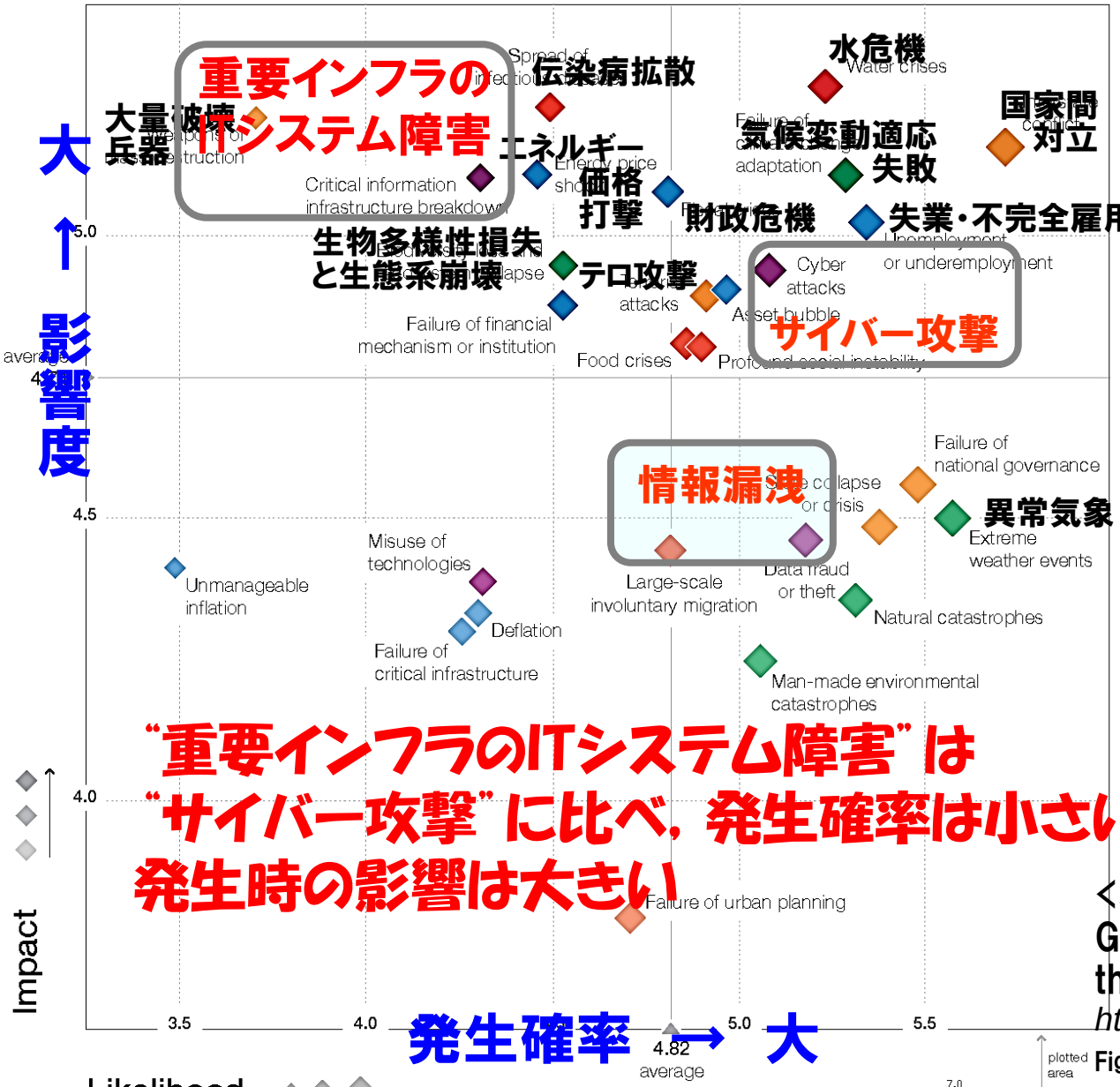
停止・異常動作等のリスクの増大

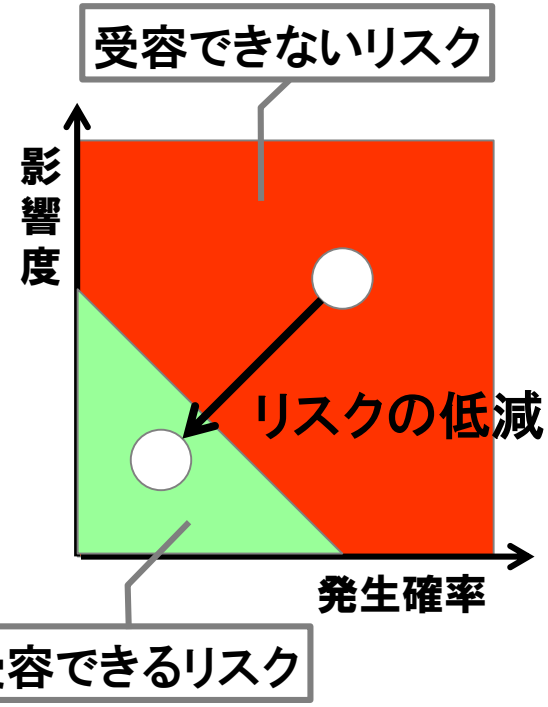
∵ 市民生活や社会経済活動がITシステムに大きく依存

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 (2015)





“重要インフラのITシステム障害”は
“サイバー攻撃”に比べ，発生確率は小さいものの，
発生時の影響は大きい

<左図の出典>
Global Risks 2015 10th Edition,
the World Economic Forum
http://reports.weforum.org/global-risks-2015/

Figure 1.1: The Global Risks Landscape 2015

データ例

IT経営関連記事のアクセスランキング例

順位	タイトル
1位	ANAシステム障害の原因判明、シスコ製スイッチの「世界初のバグ」でDBサーバーがダウン
2位	休日出勤が当たり前のノルウェー、それでも生産性は高まる
3位	判明、ANAシステム障害の真相
4位	技術者不足への対策ですか。諦めてください。それが日本のためです
5位	[詳報]JTBを襲った標的型攻撃
6位	「役割分担をはっきりさせよう」、メンバーがこう言い出したら危機のサイン
7位	JTBにはがっかりした、社長の謝罪会見で記者が感じた違和感
8位	シリコンバレーのオフィスが、どこもこじゃれている理由
9位	予定価格9億円が15万円、大阪府の自治体情報セキュリティクラウドで超安値落札
10位	「年収は下がりますが6時に必ず帰れます」
11位	「新人なのに経験者」、偽の職歴で売られた話
12位	エストニアの国民IDカード制度がFinTechと融合してとんでもないことになっていた
13位	エンジニアの常識はマネジャーには「非常識」、意識を変えないと地雷踏む
14位	「東洋一のデータセンター」が時代遅れになった理由
15位	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

システム障害への関心は高い

<出典> 2016年アクセスランキング発表！
[IT経営] ANA、JTBなどの大規模トラブルで再認識する「守りのIT経営」
ITPro, 2016/12/26

データ例

情報処理システム障害の発生状況

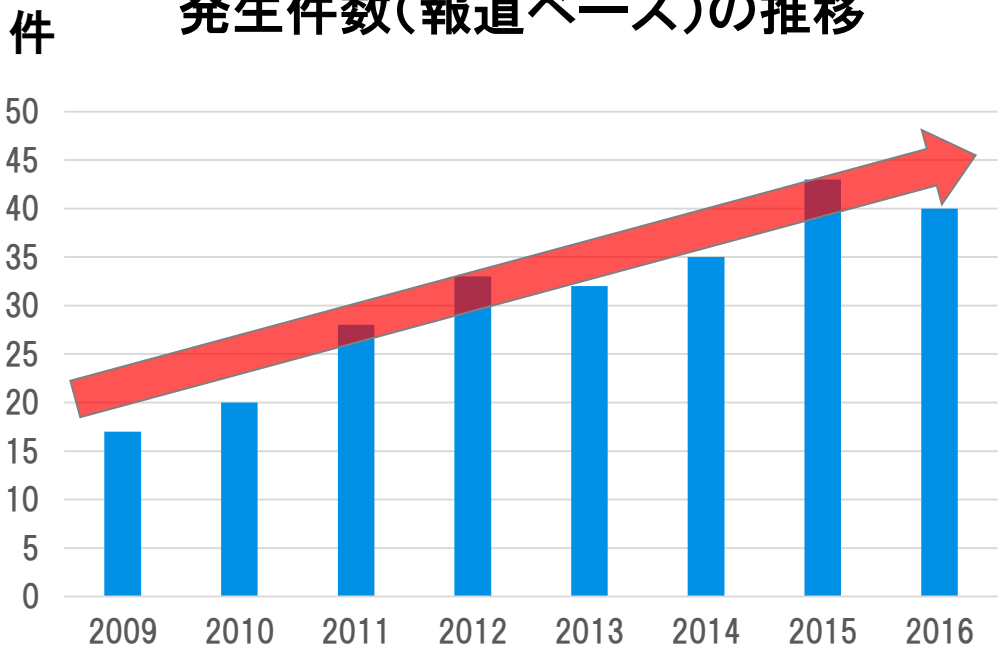
SEC Software Reliability Enhancement Center

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。
- **○○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

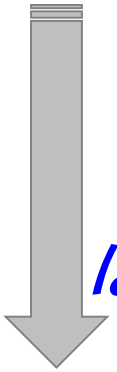


（出典）SEC Journal 情報システムの障害状況

類似障害の発生

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



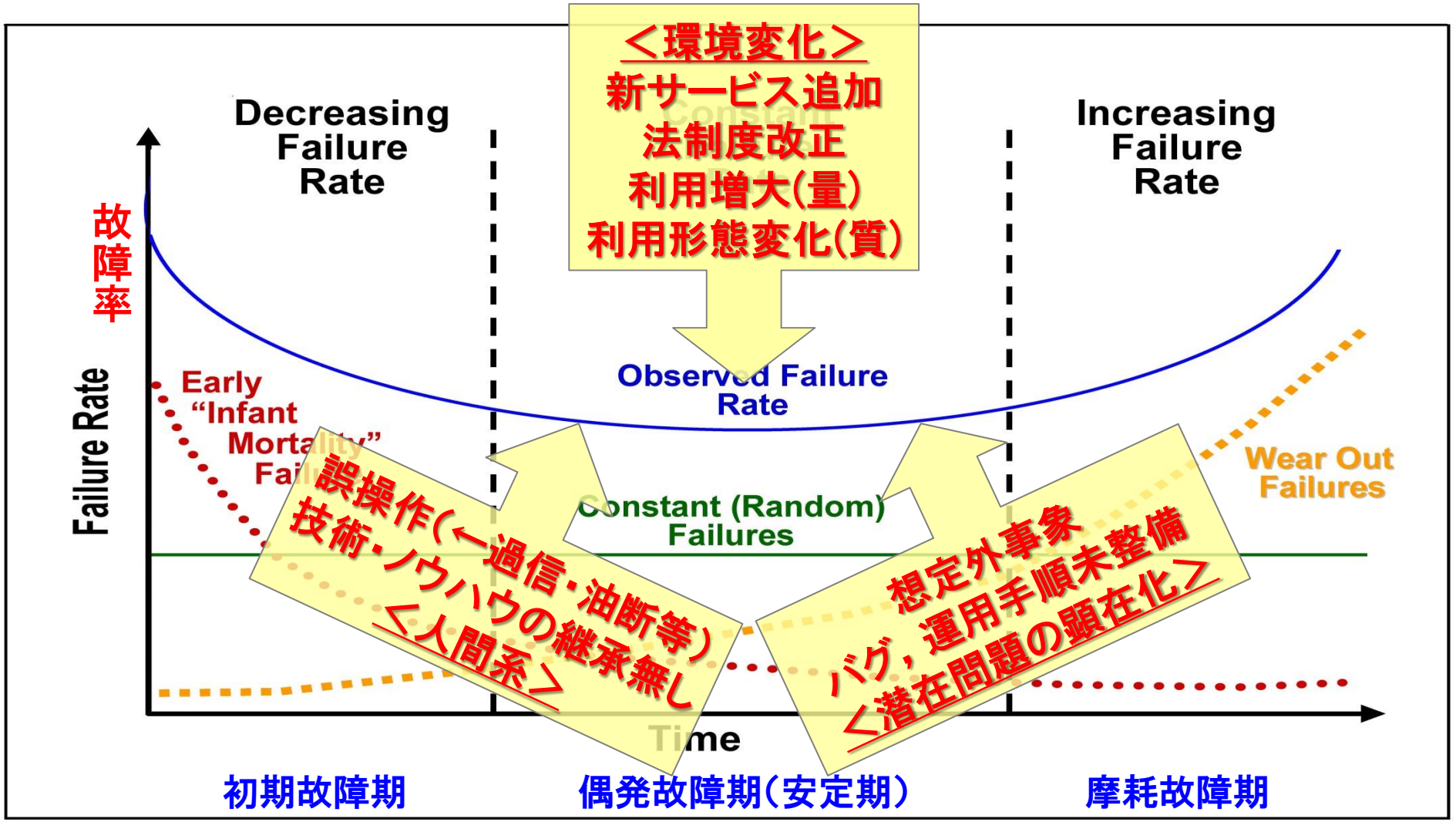
ソフトウェア・エンジニアリング技法の活用

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

SEC Software Reliability Enhancement Center

ハードウェアは劣化する→故障 → 冗長構成，など

ソフトウェアは~~劣化しない~~

ソフトウェアは相対的に劣化する → 教訓の活用

使われる環境の変化
- ✓ ビジネス方針，ニーズ
- ✓ 組織・人（慣れによる過信・油断，交代による技術/ノウハウ継承無し）
- ✓ 利用者増，技術進展，他

網羅的な事前抽出が困難

リスク要因

→ 失敗に学ぶ

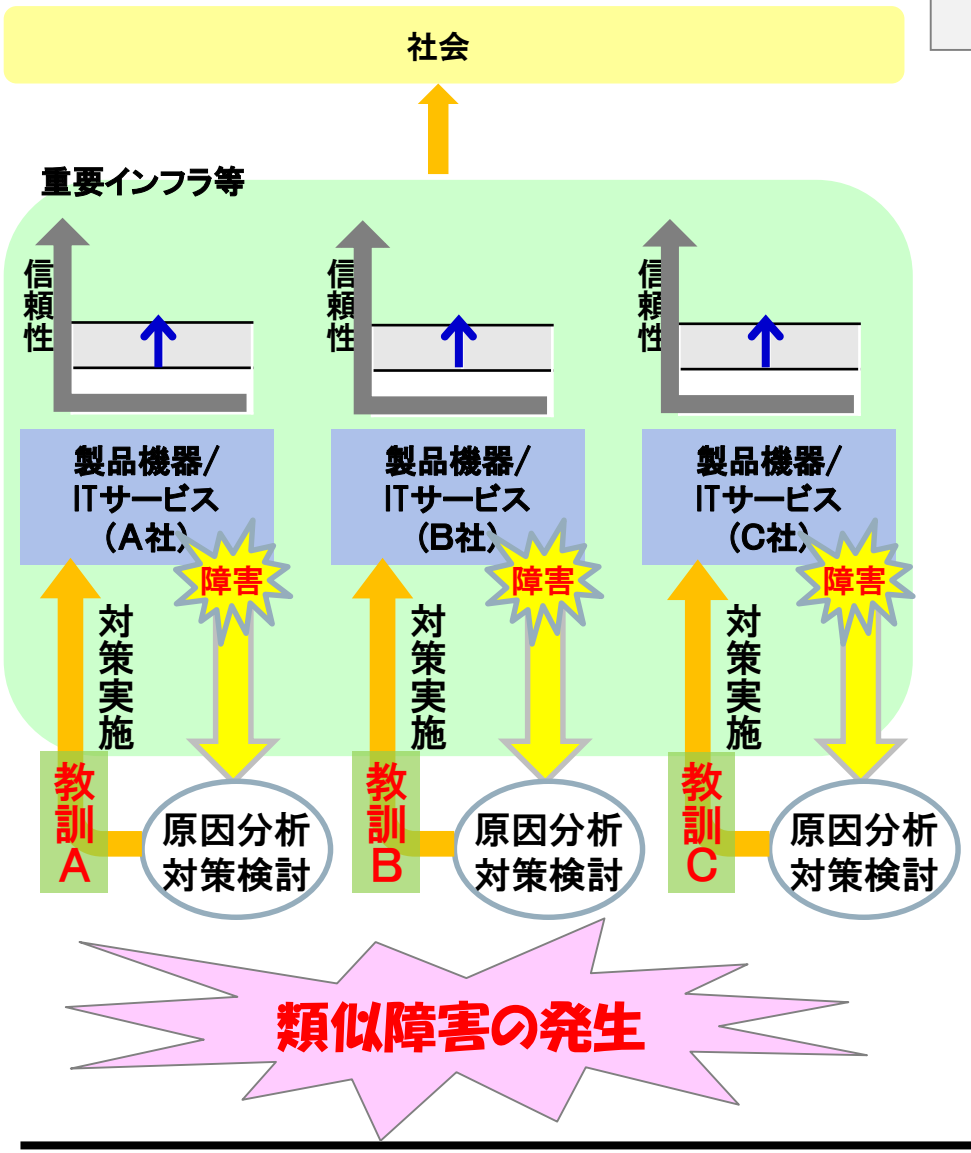
障害事例に基づく教訓・対策の共有

1企業の経験では範囲が限られる

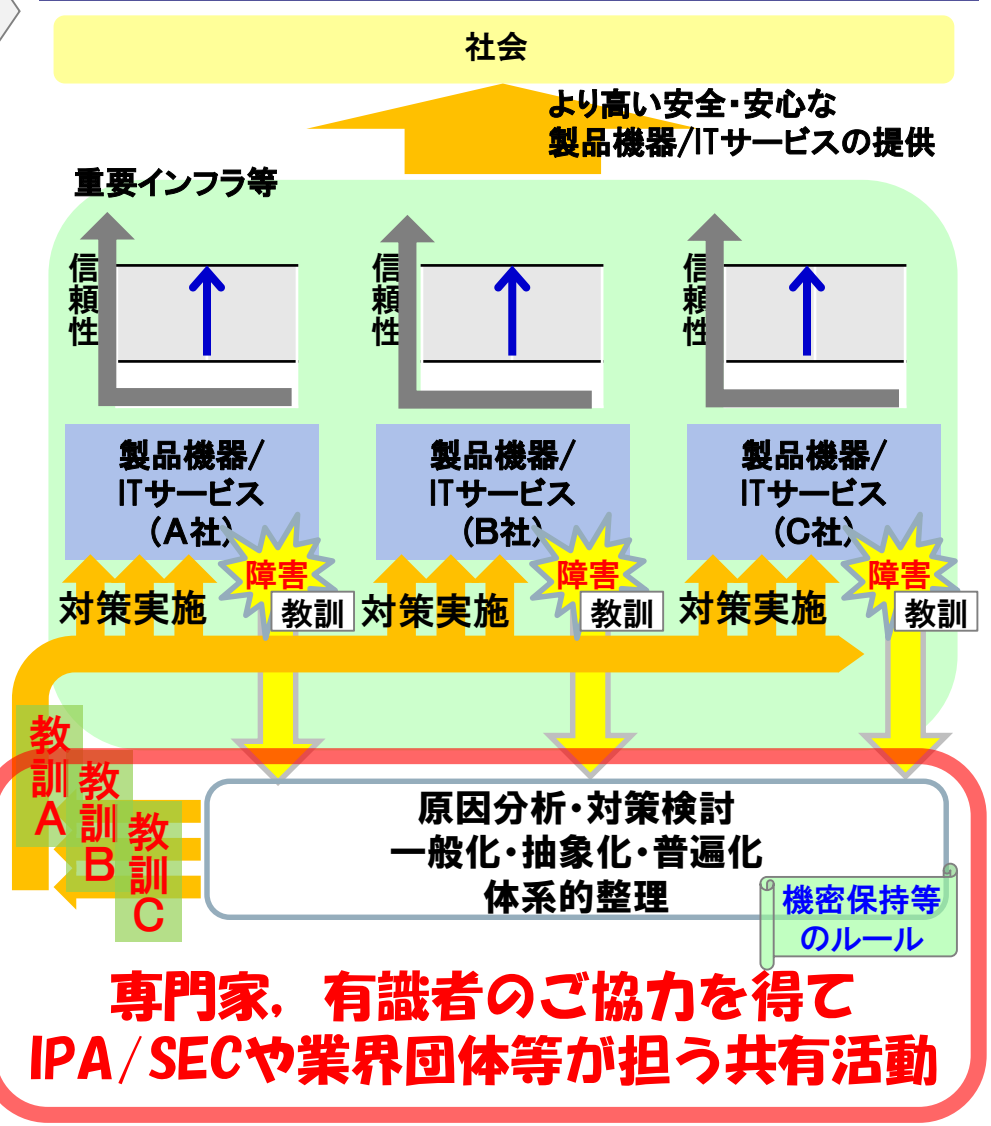
教訓共有の取組みの目指す方向

SEC Software Reliability Enhancement Center

現状（教訓の共有なし）



障害に基づく教訓の共有による信頼性向上のしくみ



（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

SEC Software Reliability Enhancement Center

【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）
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

＜特徴＞
①業界・分野を超えて活用可能な普遍化された教訓。
②機密保持ルールの下で詳細情報の提供を受けた深い議論。
③蓄積されたソフトウェア・エンジニアリングに関する知見活用。

国民生活や社会・経済基盤に関わる「障害情報」を収集

IPA

製品・制御（組込み）システム分野
＜製品・制御システム高信頼化部会＞
[教訓数] 35件

収集した情報を分析し対策を検討

普遍化
取りまとめ

[教訓数] 36件
＜重要インフラITサービス高信頼化部会＞
ITサービス分野

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）

2015年度版：2016年3月31日公開
http://www.ipa.go.jp/sec/reports/20160331_1.html

【参画企業等】
（株）三菱東京UFJ銀行
日本生命保険相互会社
東京海上日動火災保険（株）
（株）東京証券取引所
東京電力ホールディングス（株）
東日本旅客鉄道（株）
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

2016年末時点

教訓ごとの随時公開も実施中
http://www.ipa.go.jp/sec/system/lesson.html

各教訓の構成

SEC Software Reliability Enhancement Center

[教訓ＩＤ]
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

各教訓の説明 →後ほど

教訓の作成と活用のためのガイドブック

SEC Software Reliability Enhancement Center

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
（失敗のカラクリ等の気付きを与えるメッセージ）

（裏返し）

高信頼化への知恵
（成功のカラクリ等の気付きを与えるメッセージ）

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）

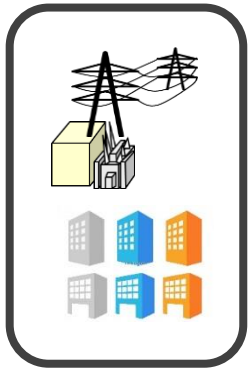
具体化

情報処理システム高信頼化教訓集

IPA/SECが公開

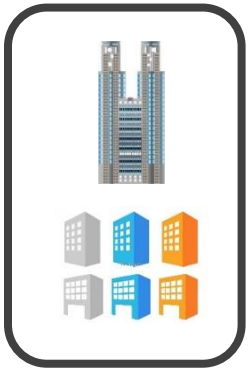
共有活動を推進中

SEC Software Reliability Enhancement Center

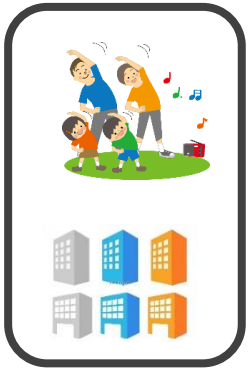


電力分野
（有志12社/団体）

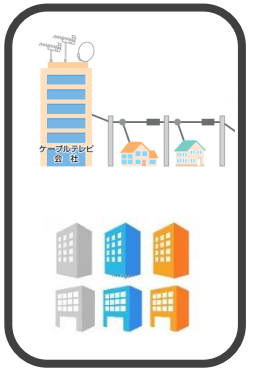
交通分野
（航空運航システム研究会と協業）



電子政府
（東京都特別区有志20区）



金融分野
（生命保険会社有志，日本クレジット協会）



通信分野
（日本ケーブルテレビ連盟）

地域インフラ
（北海道重要インフラ事業者，関西情報センター サイバーセキュリティ研究会会員）

情報共有体制の支援、事例情報の提供、必要に応じ共有ツールの提供

IPA

内 容

SEC
Software Reliability Enhancement Center

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. よくありがちな事例の教訓
3. 障害事例・教訓の活用
4. まとめ

IPA Better Life with IT

運用・保守関連

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)

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

教訓一覧（ITサービス）[ガバナンス／マネジメント領域]

SEC Software Reliability Enhancement Center

1）ガバナンス／マネジメント領域の教訓

No.	教訓ＩＤ	教訓概要
1	Ｇ１	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」をつくることが大切
2	Ｇ２	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	Ｇ３	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	Ｇ４	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	Ｇ５	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	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！
7	Ｇ７	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	Ｇ８	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	Ｇ９	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	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！
11	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
12	Ｇ１２	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	Ｇ１３	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	Ｇ１４	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！

SEC Software Reliability Enhancement Center

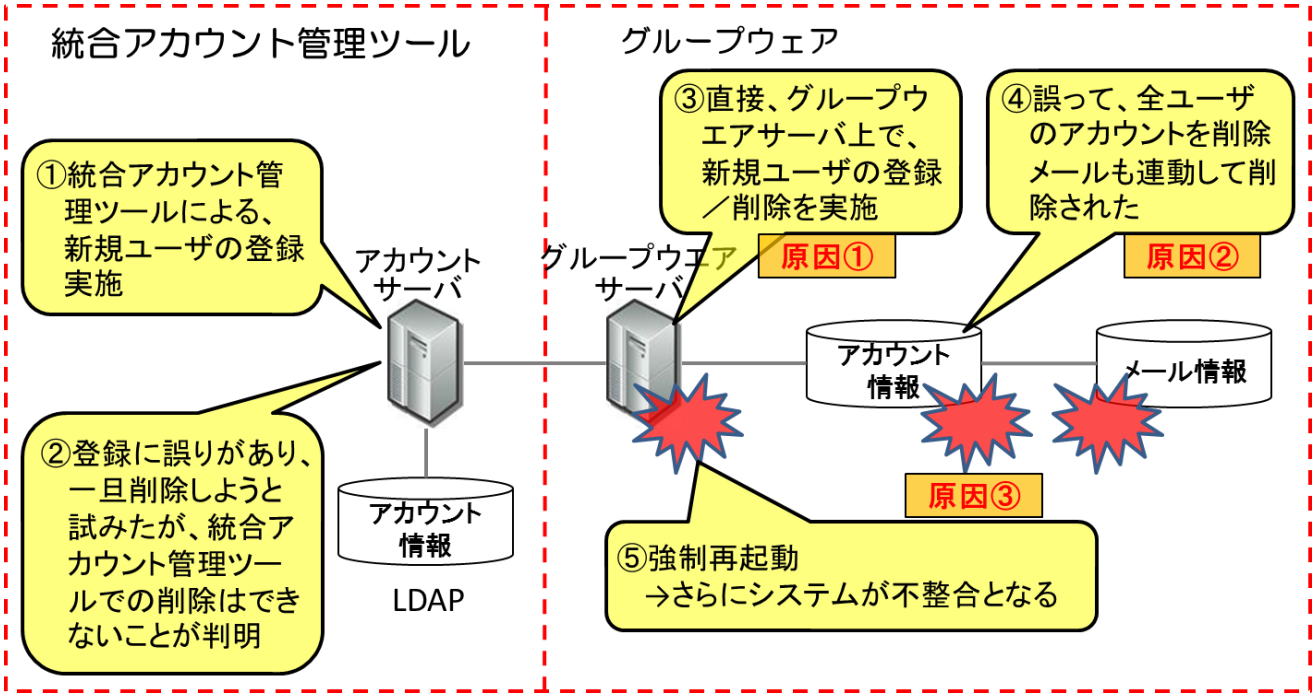
人間系の考慮

【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）
繁忙な環境下、迅速な処理が求められる状況で、各メンバ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!

SEC Software Reliability Enhancement Center

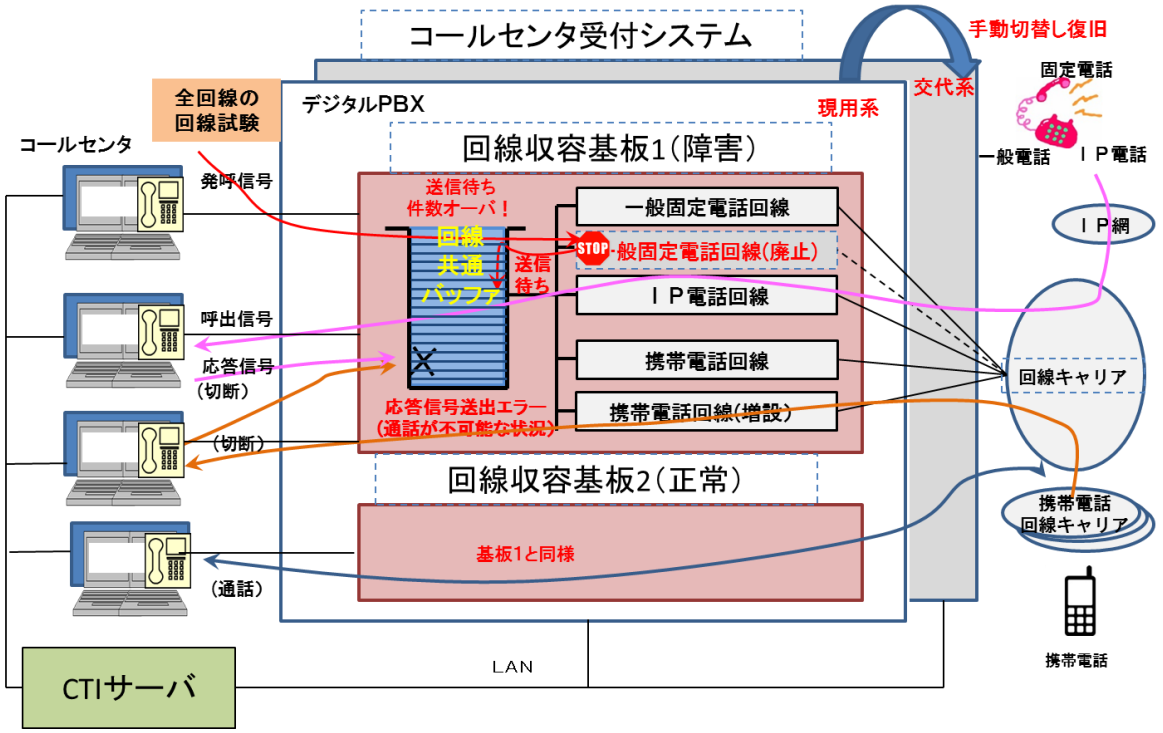
手順・ルールの明確化

【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】
- 交代系への切替えで復旧
- 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

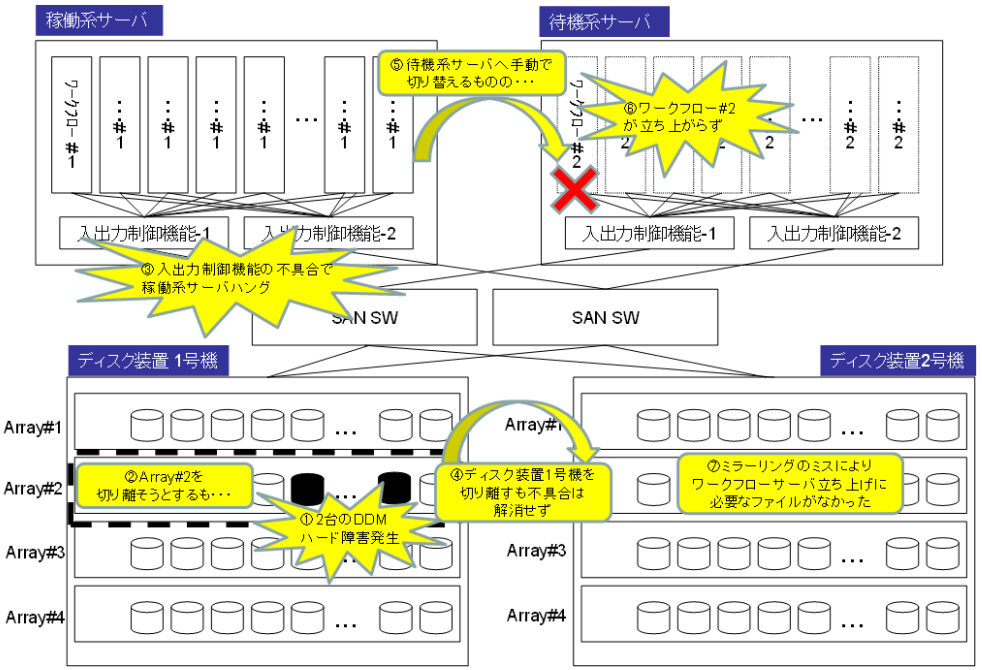
SEC Software Reliability Enhancement Center

修正パッチ適用基準
手順ルールの明確化

【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。

G12：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サイクルをまわすべし！

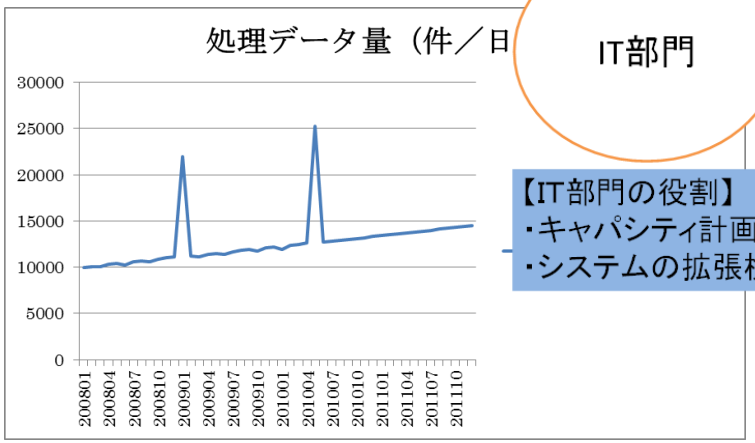
SEC Software Reliability Enhancement Center

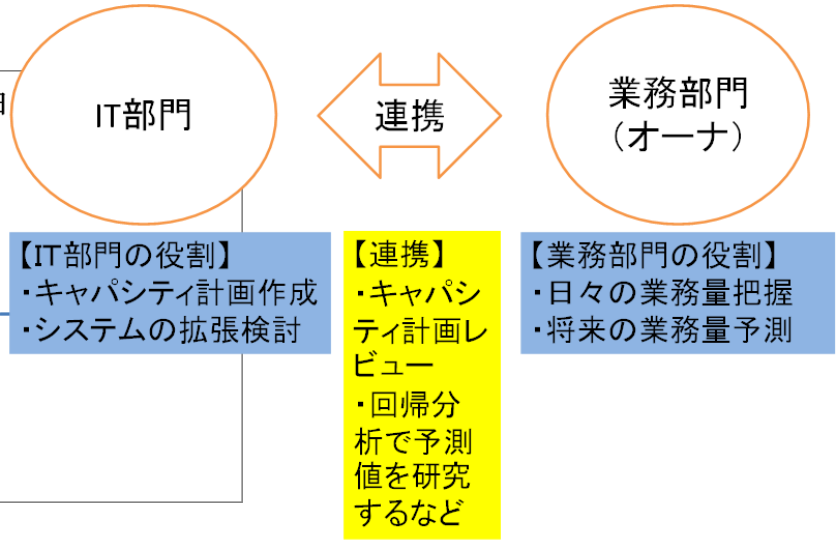
変化対応

【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。





教訓一覧(ITサービス)[技術領域]

SEC Software Reliability Enhancement Center

2)技術領域の教訓

No.	教訓ＩＤ	教訓概要
1	Ｔ１	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	Ｔ２	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	Ｔ３	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	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
5	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！
6	Ｔ６	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	Ｔ７	バックアップ切替えが失敗する場合を考慮すべし
8	Ｔ８	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	Ｔ９	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	Ｔ１０	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	Ｔ１１	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	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！
13	Ｔ１３	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	Ｔ１４	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	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
16	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
17	Ｔ１７	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！
18	Ｔ１８	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	Ｔ１９	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	Ｔ２０	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	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！
22	Ｔ２２	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

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！

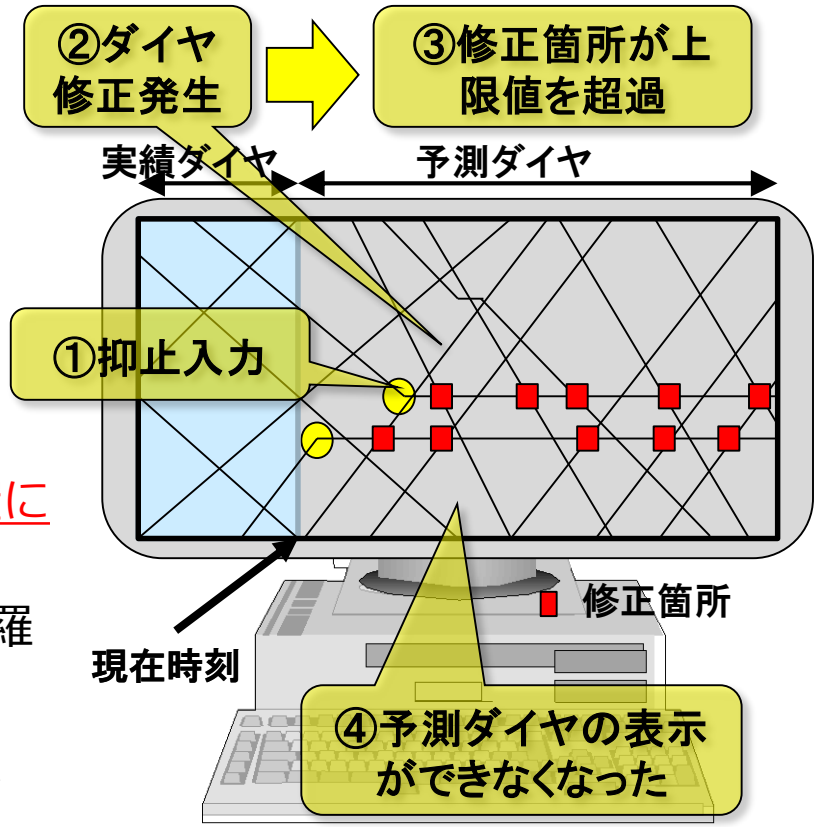
表示項目数がシステムの上限値を超えたため、全画面表示が消え，オペレータが混乱

↳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

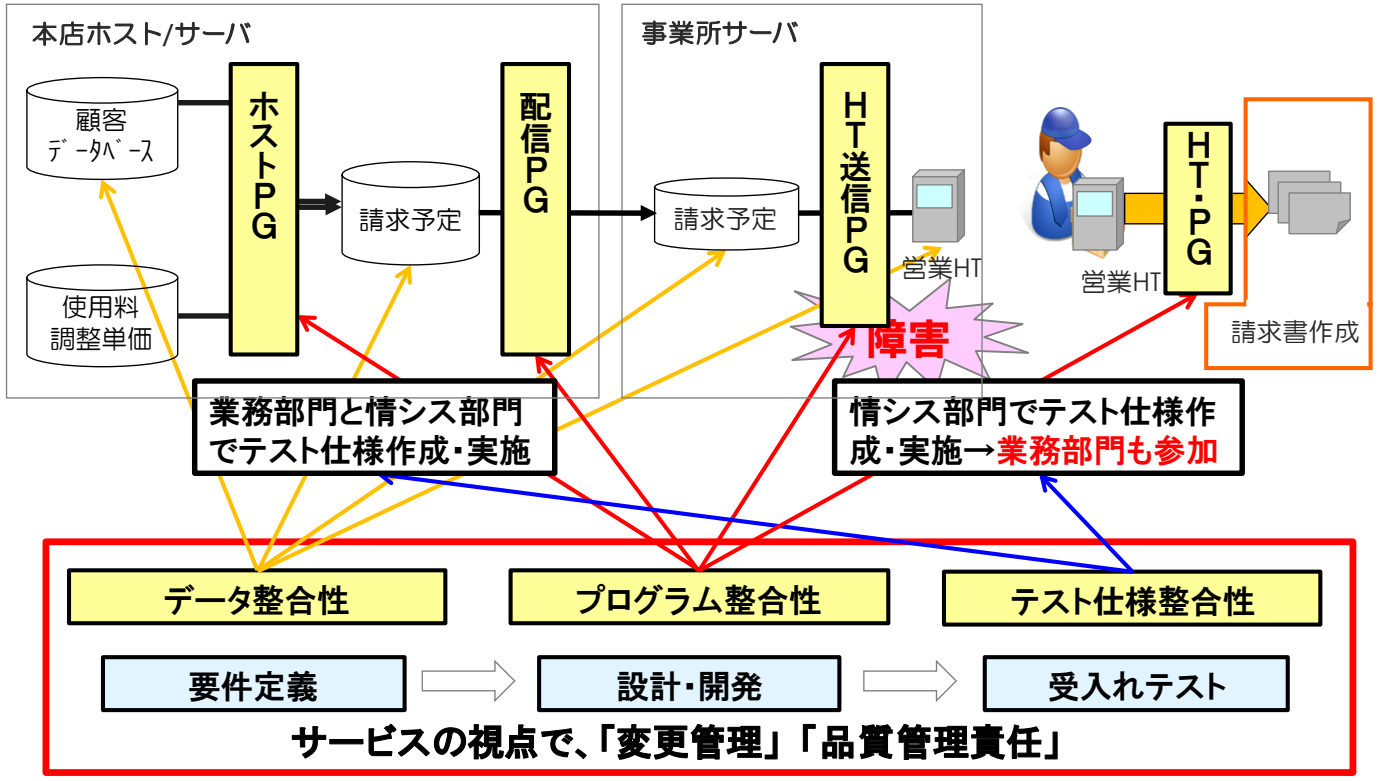
T5：サービスの視点で、「変更管理」の仕組み作りと「品質管理責任」の明確化を！

機能追加・変更時の確認

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



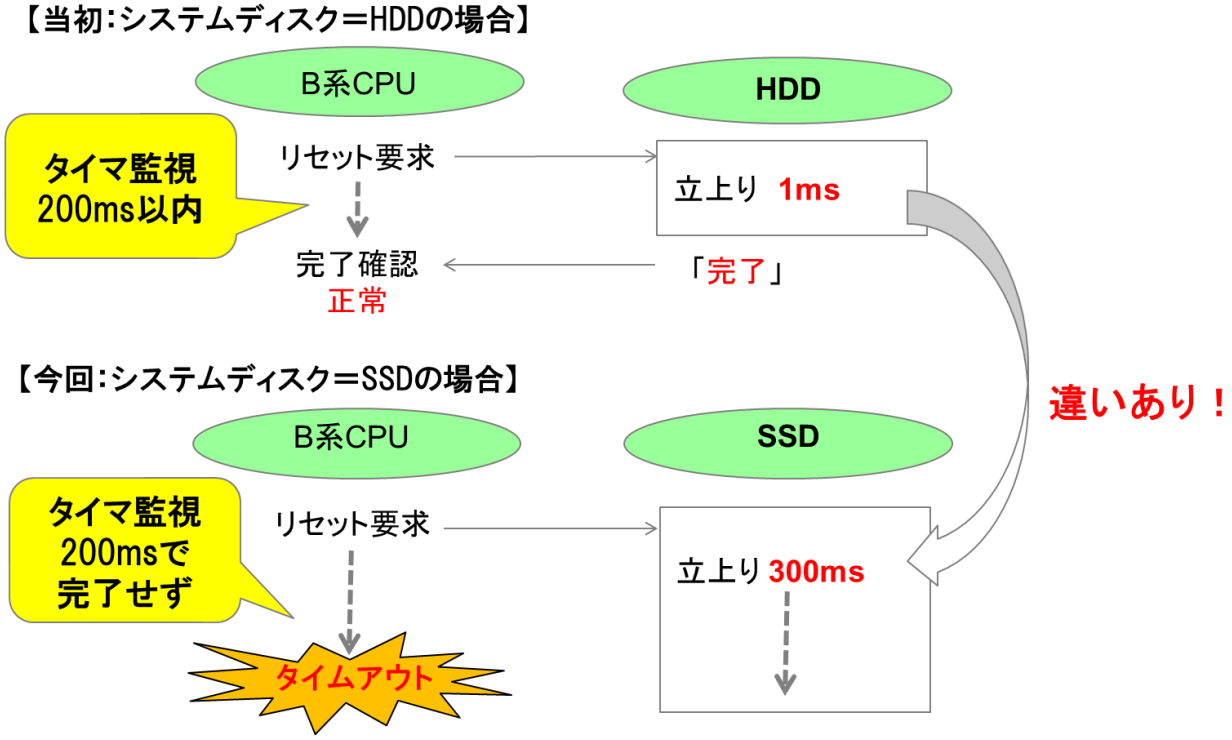
T12: 新製品は、旧製品と同一仕様と言われても、必ず差異を確認！

機能追加・変更時の確認

【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系を切り離した時に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。

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。



【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）

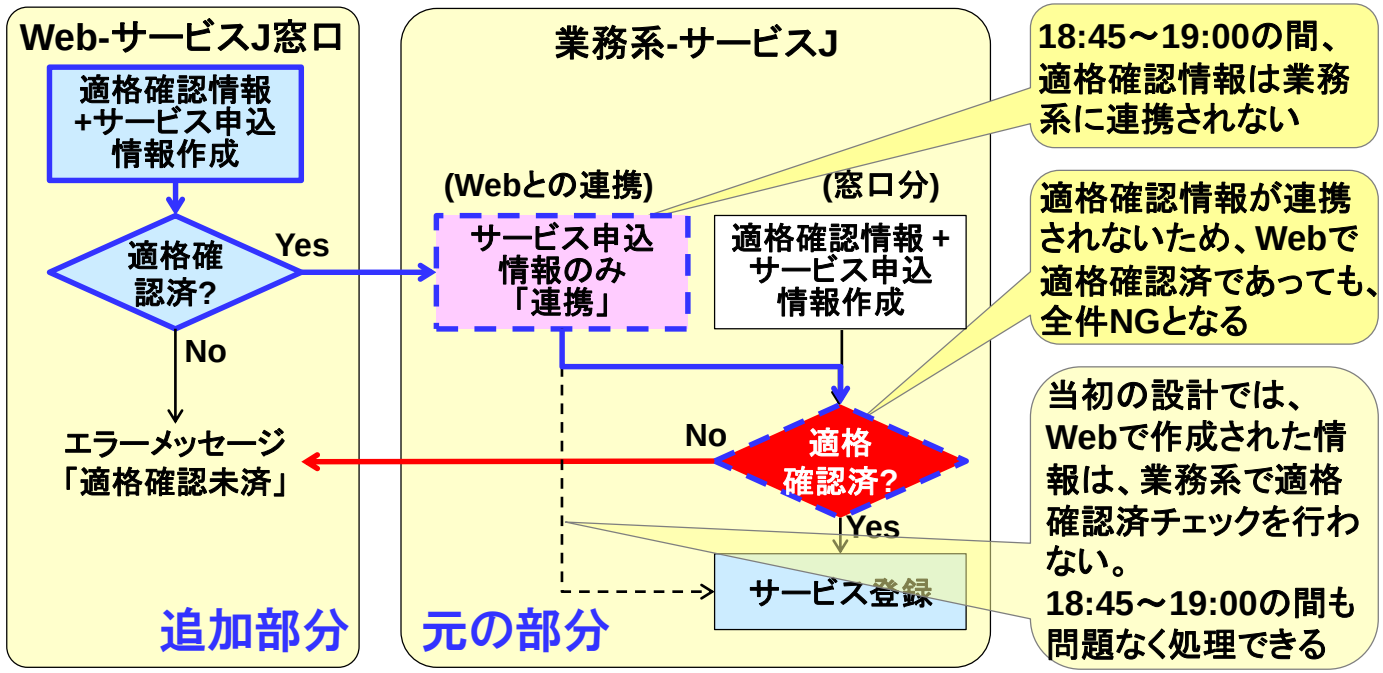
T13: 利用者の観点に立った、業務シナリオに即したレビュー、テストが重要

【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。

機能追加・変更時の確認

【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

SEC Software Reliability Enhancement Center

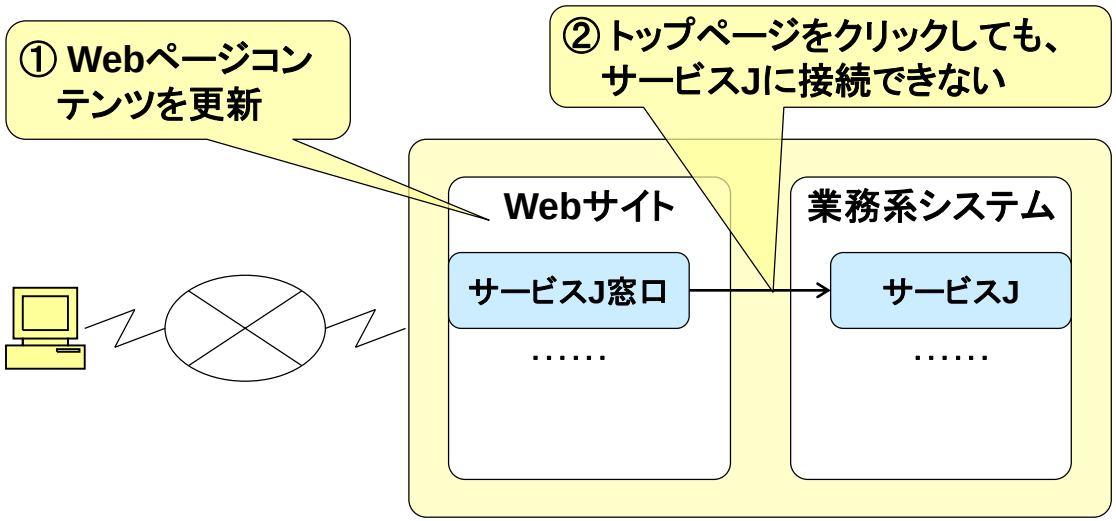
手順・ルールの明確化

【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

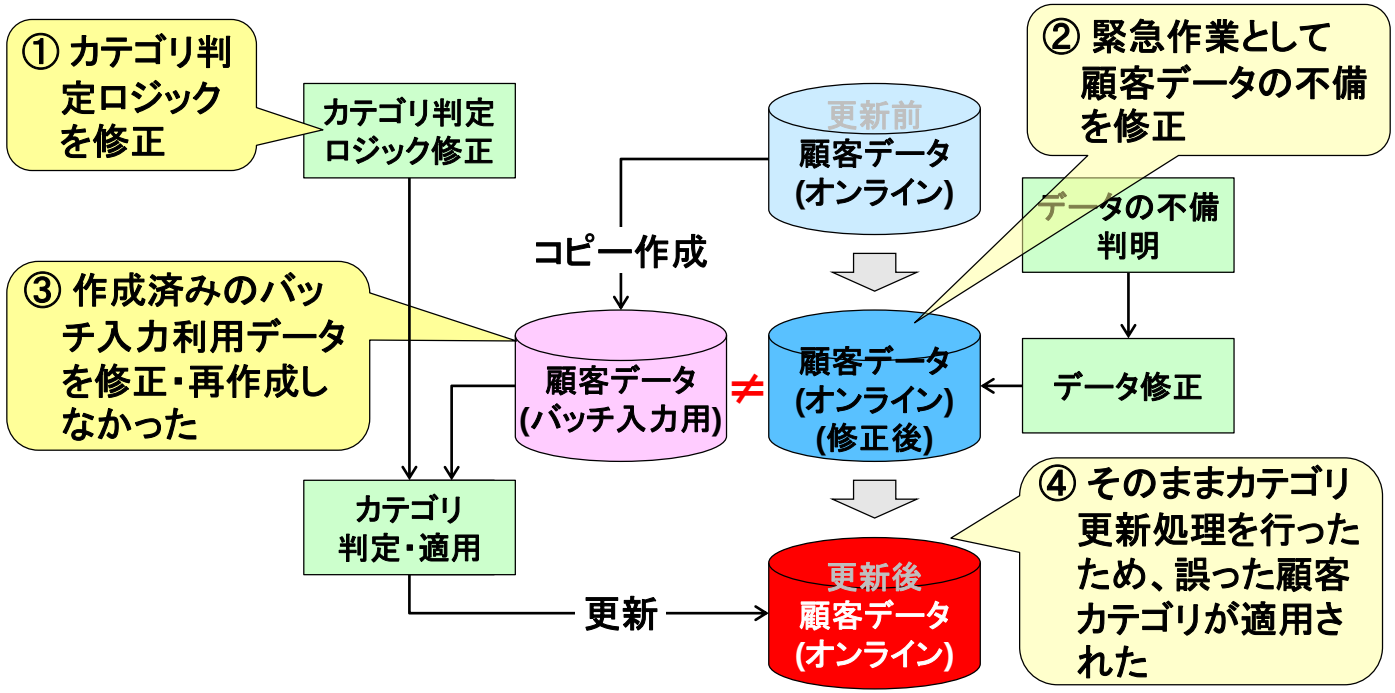
SEC Software Reliability Enhancement Center

手順・ルールの明確化
人間系の考慮

【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。



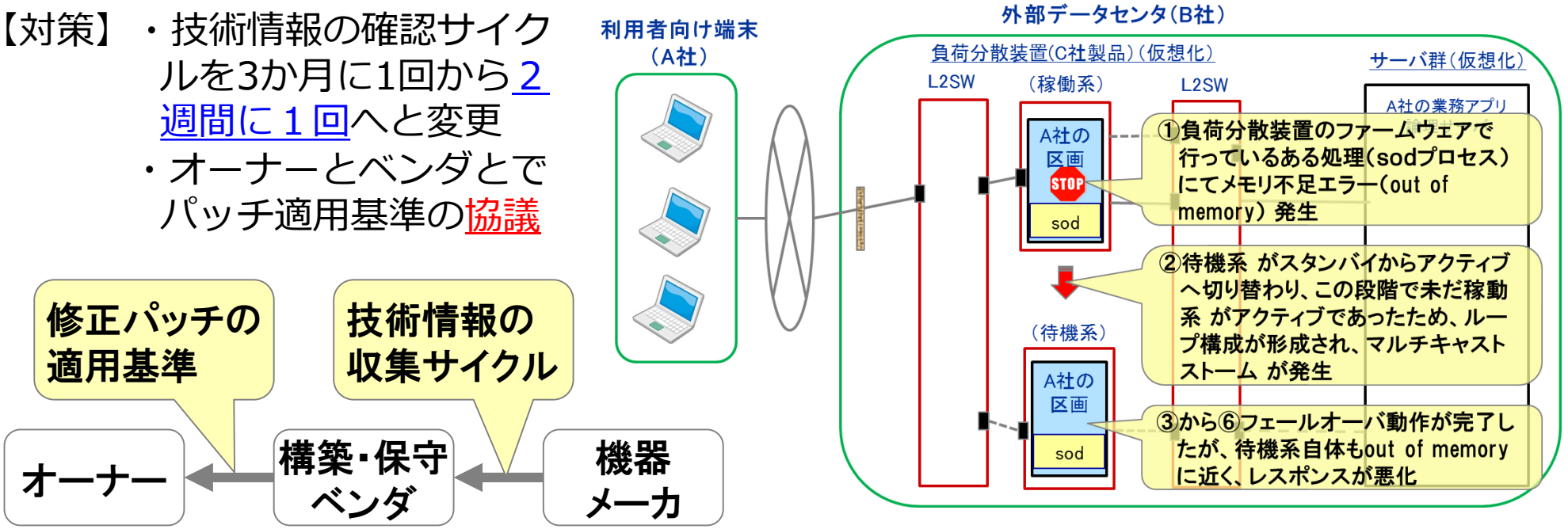
T16: システム構成機器の修正パッチ情報の収集は頻繁に行い、緊急性に応じて計画的に対応すべし

修正パッチ適用基準

【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！

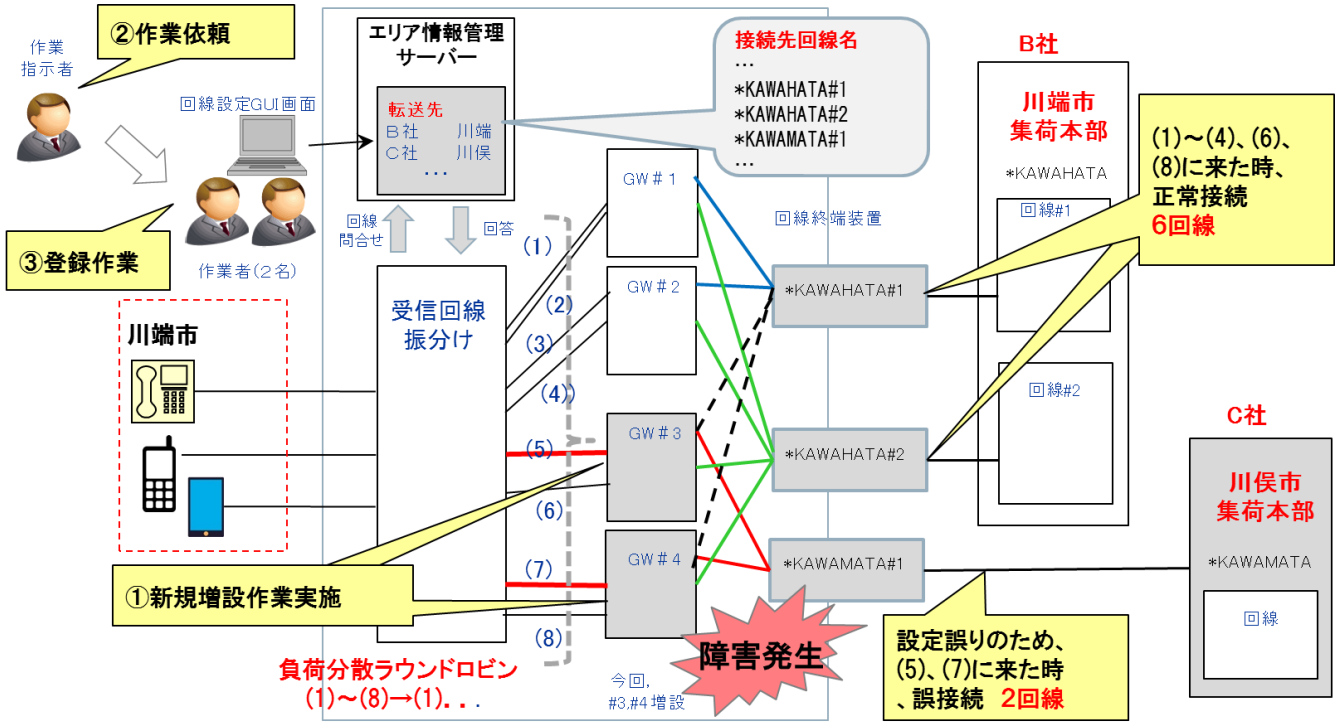
SEC Software Reliability Enhancement Center

人間系の考慮

【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



（教訓外事例）JALの重量管理システムの障害

SEC Software Reliability Enhancement Center

修正パッチ適用基準

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。

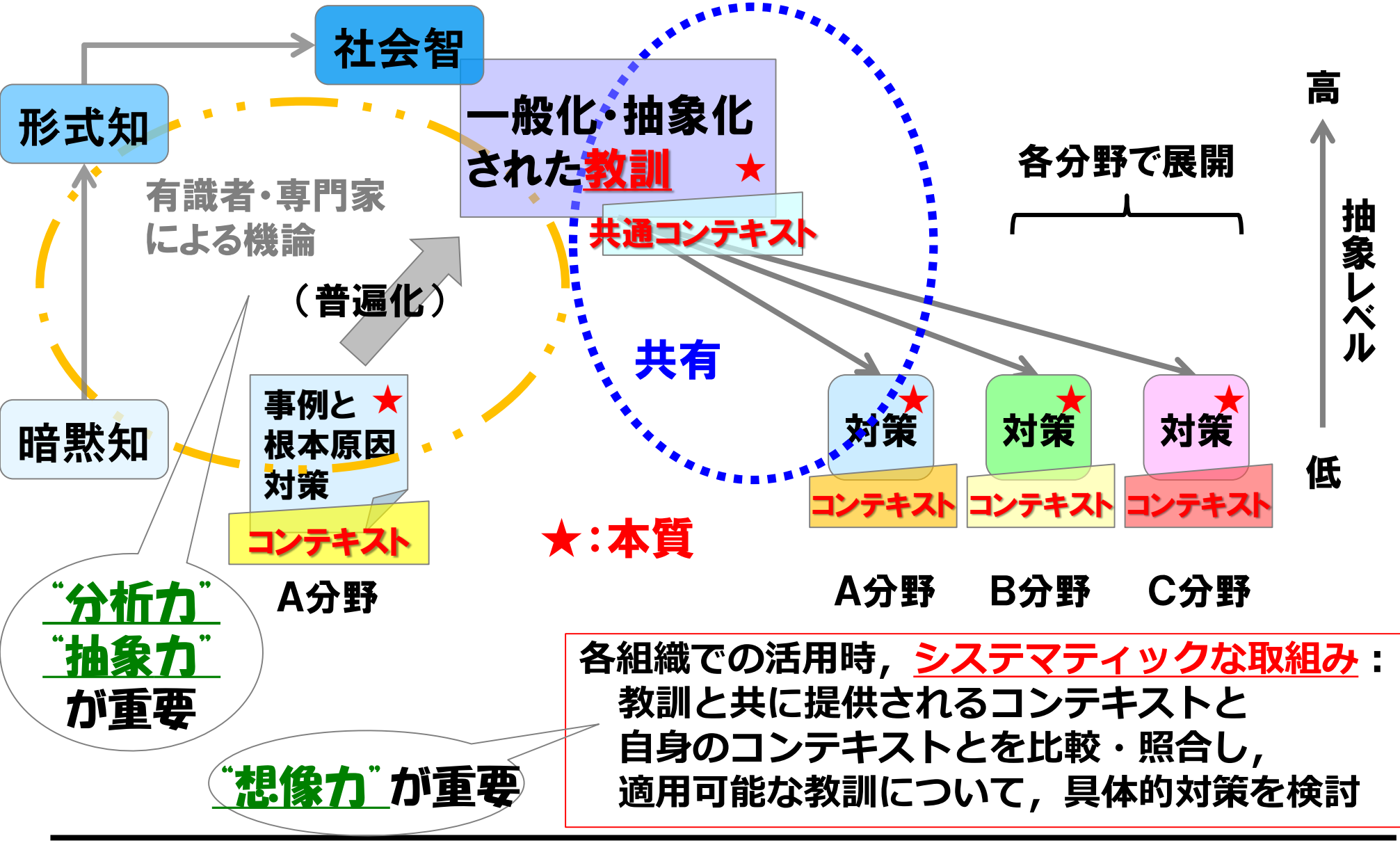
<出典> JALシステム障害、前週に追加の排他制御がデッドロックを誘発
IT Pro, 2016/04/06　*http://itpro.nikkeibp.co.jp/atcl/news/16/040601011/*

内 容

SEC
Software Reliability Enhancement Center

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. よくありがちな事例の教訓
3. 障害事例・教訓の活用
4. まとめ

教訓の作成と活用の流れ



教訓作成の意義

SEC Software Reliability Enhancement Center

教訓作成

抽象化. 一種の「モデリング」.

プログラミング(教育)の前に必要なこと.
プログラミングより上流で必要なこと.

- 事例整理:当事者が, トラブル対応の振り返りとして.
- 教訓化:第三者(共通部門)が, 社内全体の品質向上のために.

後世代に何を伝えるか?

教訓活用の課題

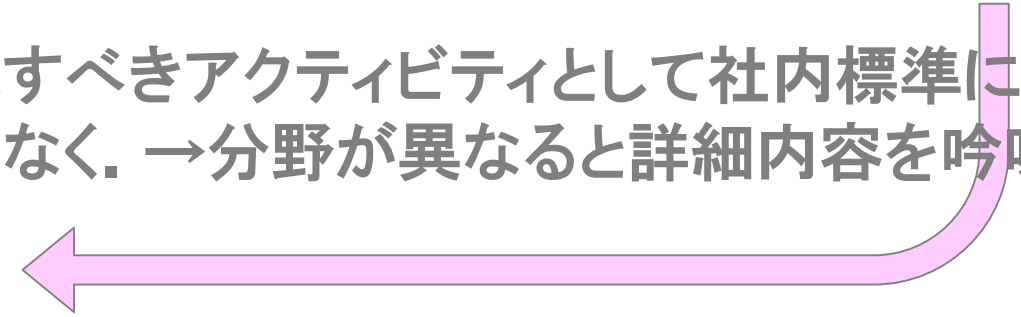
社内で障害事例をデータベース化しているが，あまり活用されていない．

他者の事例が，自分のプロジェクト/システムに役立つとは思われないようだ．

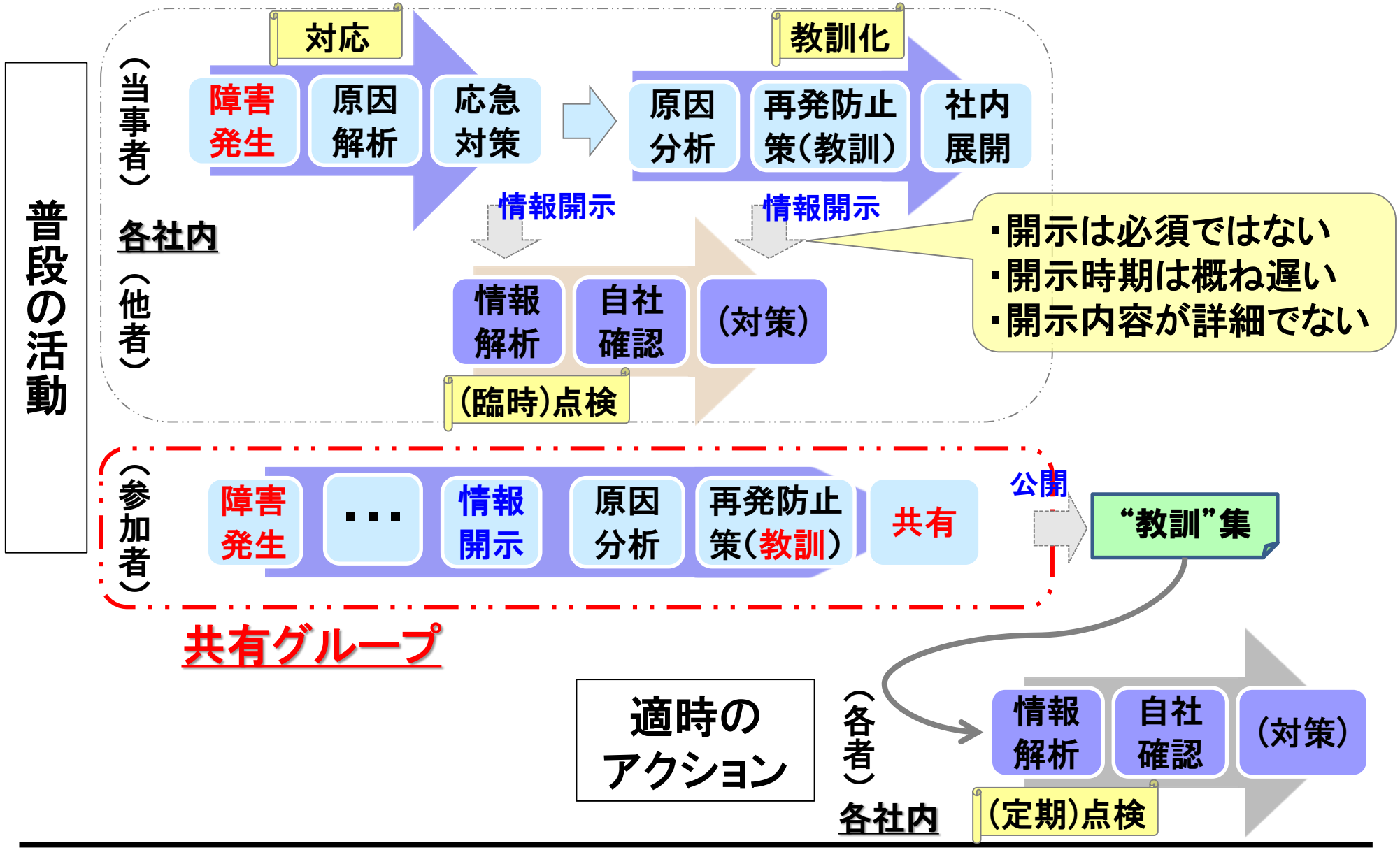
活用の姿勢（局面/シーン）

- （特定の観点に着目した）品質向上の目的で，相応のリソースをかけて．→関連性を見出そうとする
- 実施すべきアクティビティとして社内標準に規定されているので，仕方なく．→分野が異なると詳細内容を吟味しない

想像力



障害事例の分析に基づく高信頼化活動の俯瞰



教訓の恒久的な反映

SEC Software Reliability Enhancement Center

部署等／　役割（ロール）		教訓の最終的な適用先の例
経営層	社長	組織に“安全文化”を醸成
	担当役員	
業務部門	部門長	組織・体制の整備
	業務推進担当	運用手順の整備
	システム推進担当	開発手順の整備
	関連会社	調達時の指示事項
情報システム部門	部門長	レビュー・試験項目
	システム開発担当	調達時の確認事項
	システム子会社	類似事例 → トラブル発生時の原因推定
ベンダ	元請けベンダ	社内教育
	アウトソーサ	
	サブベンダ	

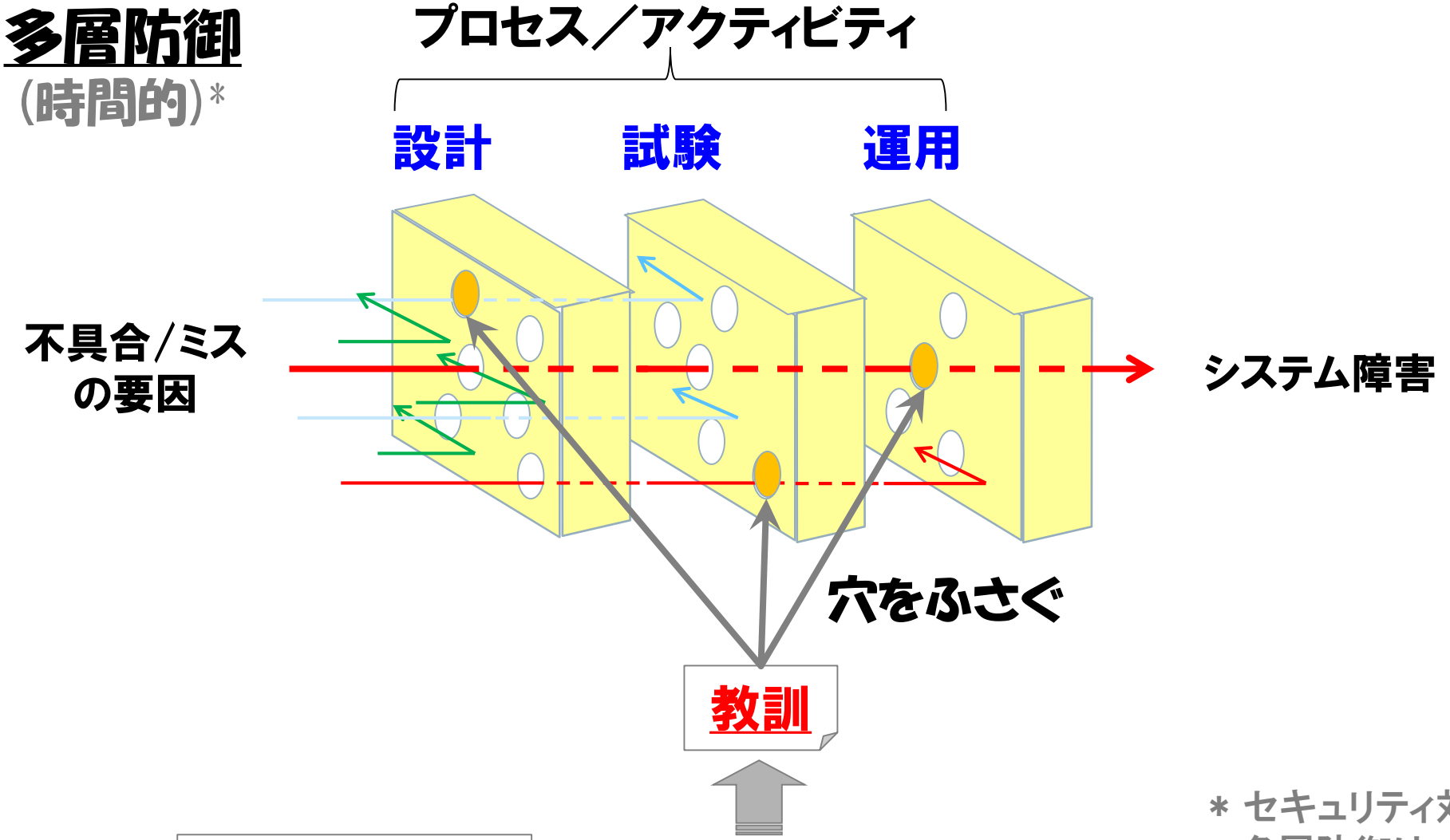
＜出典(縦軸)＞ SEC BOOKS「経営者が参画する要求品質の確保 ～ 超上流から攻めるIT化の勘どころ～」, p.37 の 3.2(1)項、p.41 の 4.1

参考

安全文化：スイスチーズモデル

SEC Software Reliability Enhancement Center

多層防御
(時間的)*



* セキュリティ対策の多層防御は，一般に，空間的な対策．

内 容

SEC
Software Reliability Enhancement Center

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. よくありがちな事例の教訓
3. 障害事例・教訓の活用
4. まとめ

「他山の石」

SEC Software Reliability Enhancement Center

「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

「正常化の偏見」

SEC Software Reliability Enhancement Center

人の性:「自分だけは大丈夫」と思う

… 正常化の偏見※

→ 確かに大丈夫，という確認が必要

※（出典）
人はなぜ「自分は大丈夫」と思うのか，防災研究家の片田群馬大学教授に聞く，ITpro 2007/04/11
http://itpro.nikkeibp.co.jp/article/Interview/20070409/267753/

「正常性バイアス」

SEC Software Reliability Enhancement Center

正常性バイアス

正当な理由もなく，自分にとって都合の悪い情報を無視したり，過小評価したりしてしまう人の特性．（社会心理学，防災・危機管理心理学等の分野で使用）

自然災害や火事，事故・事件等の犯罪等といった自分にとって何らかの被害が客観的に予想される状況下にあっても，都合の悪い情報を無視したり，何の根拠もなく「自分は大丈夫」，「今回は大丈夫」，「まだ大丈夫」等と過小評価するなどし，逃げ遅れの原因となる．

※（出典）
防災システム研究所　防災・危機管理アドバイザー　山村武彦
http://www.bo-sai.co.jp/bias.htm

「正常化の偏見」／「正常性バイアス」

SEC Software Reliability Enhancement Center

他システムの障害事例や他者の失敗例を見聞きしても,
「自分たちのシステムは大丈夫」
「自分たちだったら, そんなへまはやらない」
等と言ってそれを気にかけないということは, ありませんか？

その根拠はありますか？

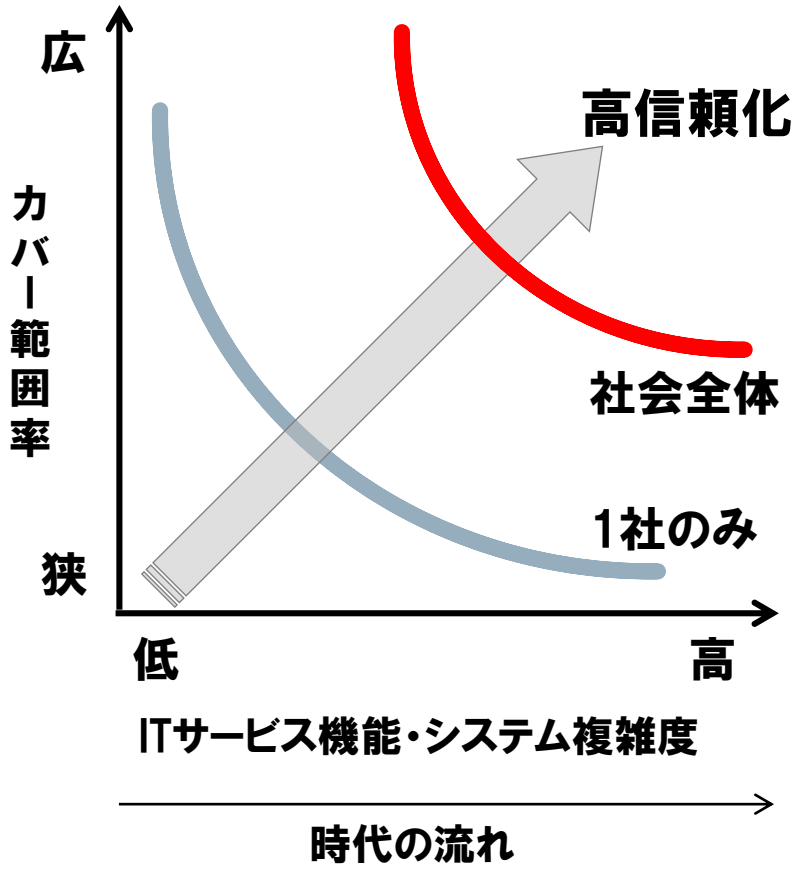
その理由を経営層や利用者に, 論理的に説明できますか？

参考

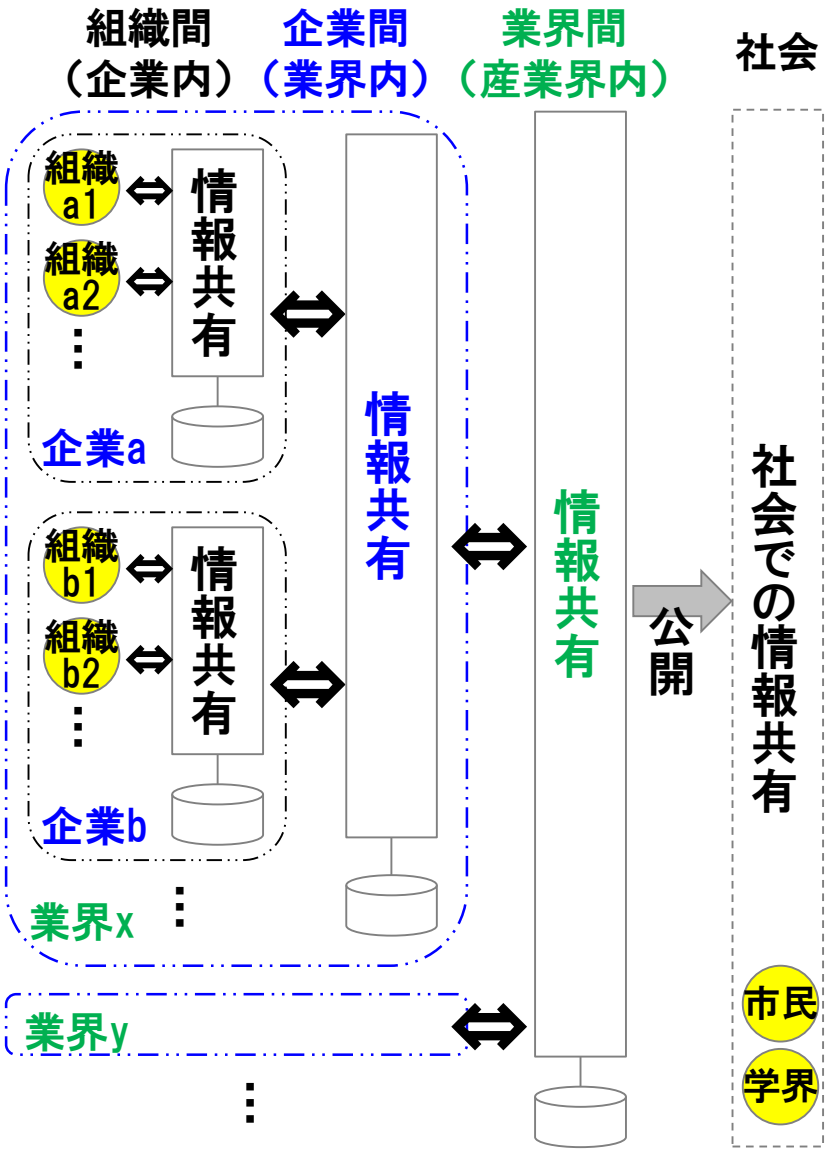
みんなの力で全体をカバー

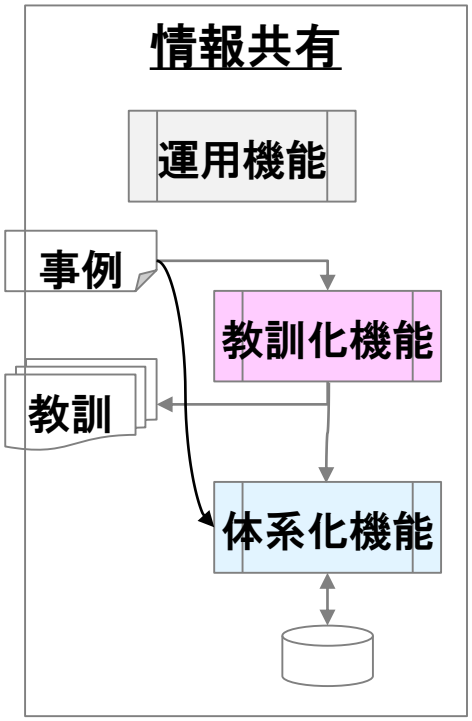
ITサービスの機能やシステムが複雑化すると，単一事業者のカバーする知見の範囲は，相対的に狭くなる．

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．



障害事例情報に基づく教訓共有の仕組みのモデル





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

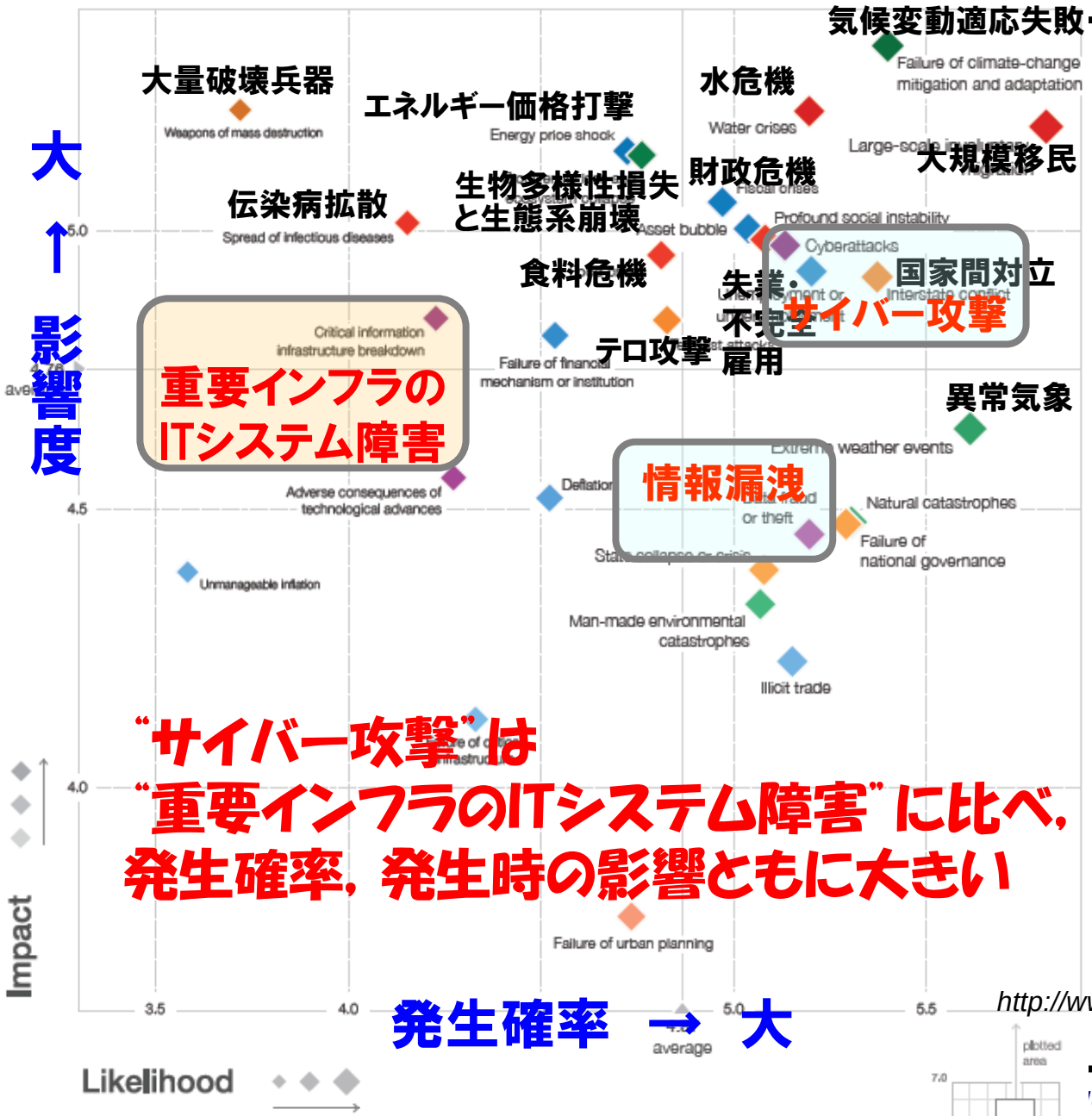
以降，参考

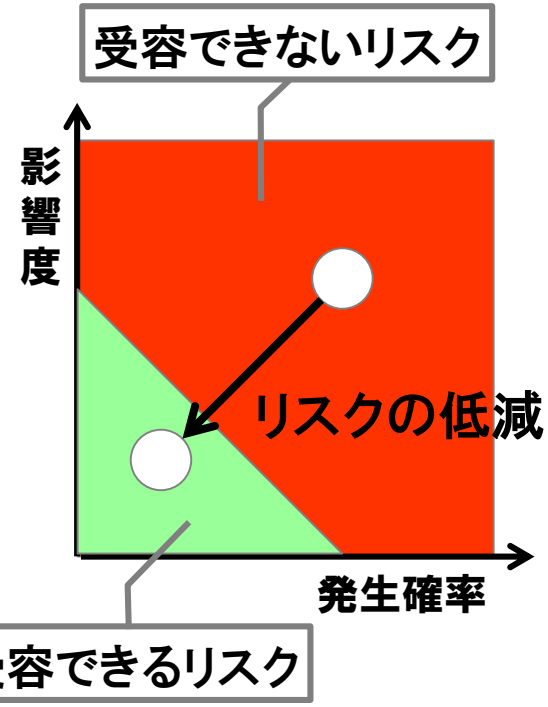
データ例

グローバル・リスク (2016)

2015 2017

SEC Software Reliability Enhancement Center





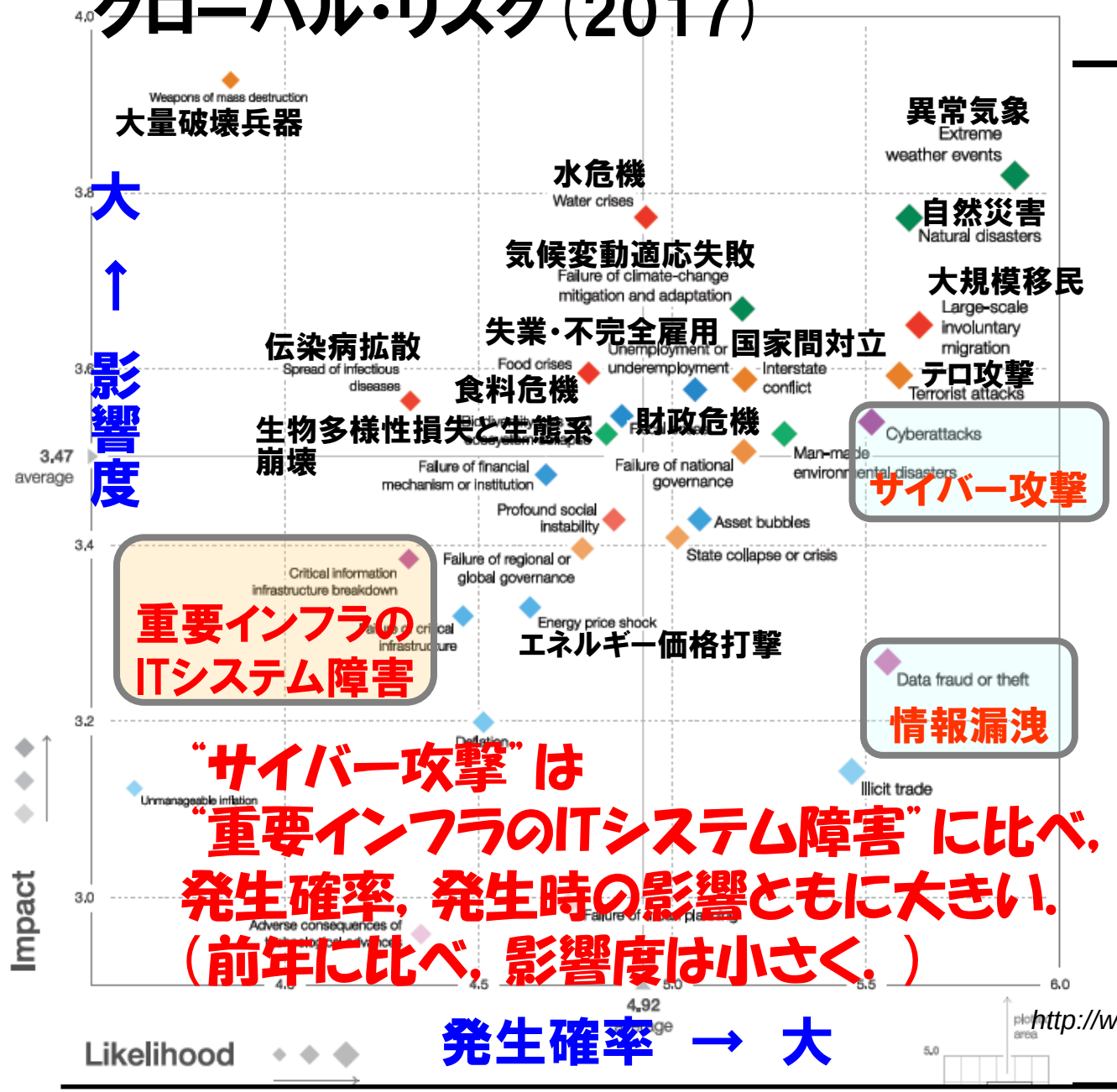
“サイバー攻撃”は
“重要インフラのITシステム障害”に比べ，
発生確率，発生時の影響ともに大きい

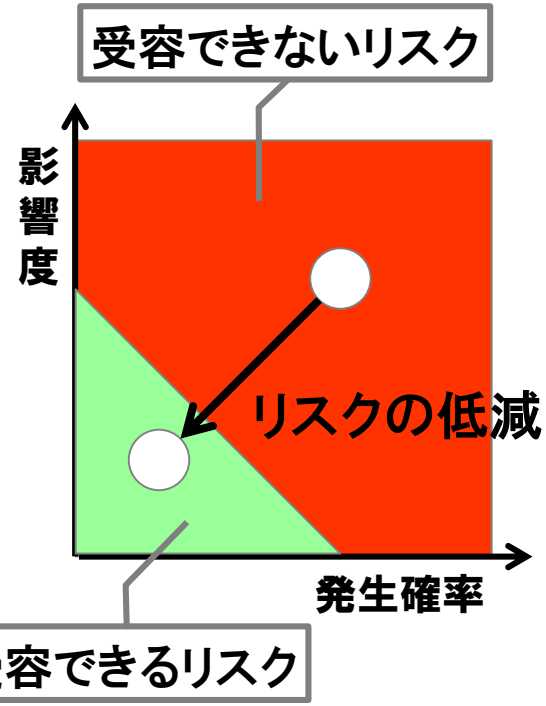
発生確率 → 大

<左図の出典>
The Global Risks Report 2016 11th Edition, the World Economic Forum
http://www.weforum.org/reports/the-global-risks-report-2016

Figure 1: The Global Risks Landscape 2016

グローバル・リスク (2017)





“サイバー攻撃”は
“重要インフラのITシステム障害”に比べ，
発生確率，発生時の影響ともに大きい．
（前年に比べ，影響度は小さく，）

<左図の出典>
The Global Risks Report 2017 12th Edition, the World Economic Forum
http://www.weforum.org/reports/the-global-risks-report-2017

Figure 3: The Global Risks Landscape 2017

参考

情報システムの障害情報データ

SEC Software Reliability Enhancement Center

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

http://sec.ipa.go.jp/sweipedia/?s=%E6%83%85%E5%A0%B1%E

情報システムの障害状況 | SW...

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

ページ(P) セーフティ(S) ツール(O)

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。

SWEiPediaについて

詳細検索 情報システム↓ 組込みシステム↓ 統合システム↓ サイトマップ

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↓ メトリクス分析↓ 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

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

SEC journa...
SEC journa...
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

SE 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

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…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…て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て報告する。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…ていることが特徴的である。今期から本…され今後重要な社会インフラとして運用…あるため、関連の事故の概要について次…

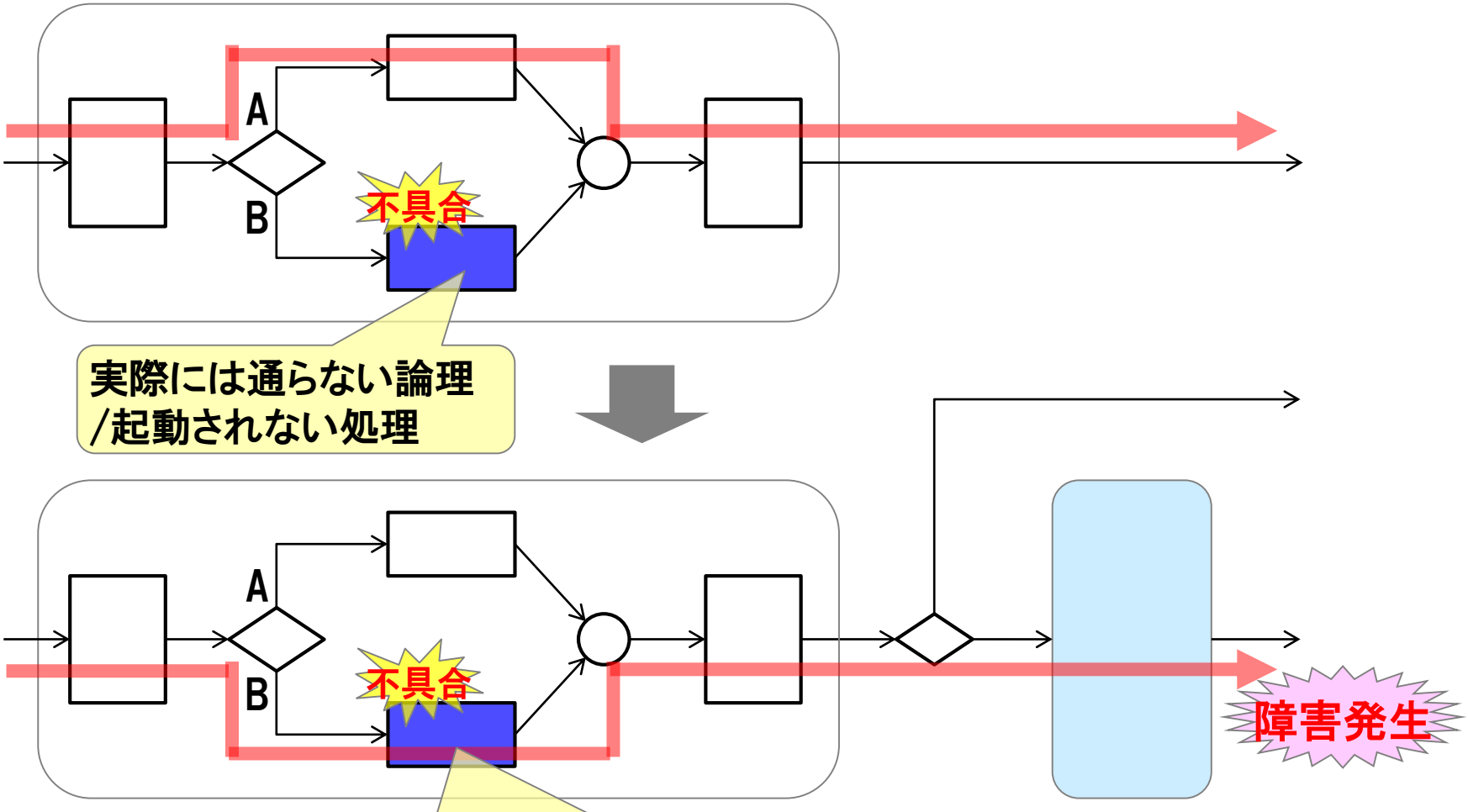
今期の事例の中には、以前から内在…

参考

新規サービス追加により潜在不具合が顕在化（1/2）

SEC Software Reliability Enhancement Center

構築当初の基本サブシステム

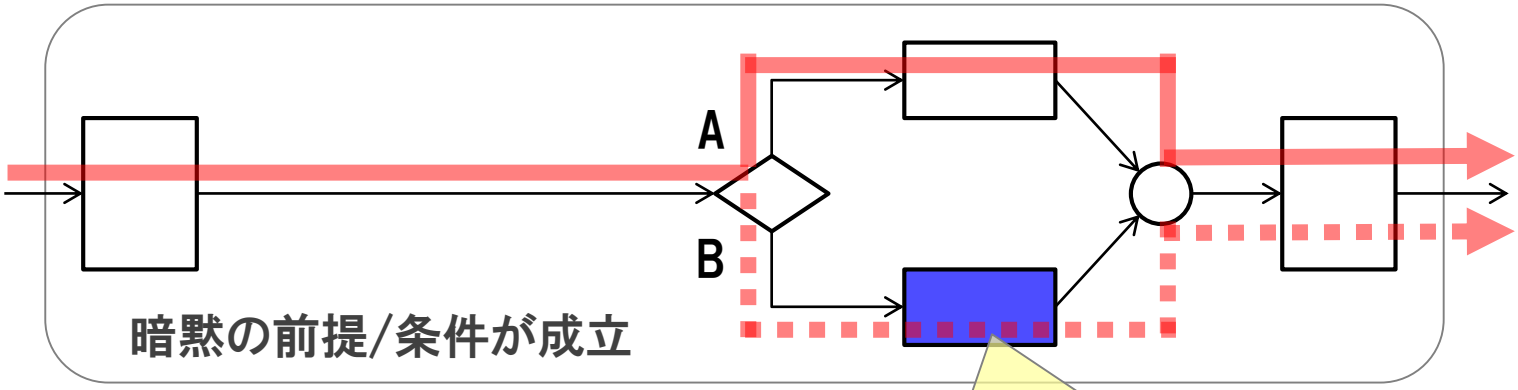


参考

新規サービス追加により潜在不具合が顕在化 (2/2)

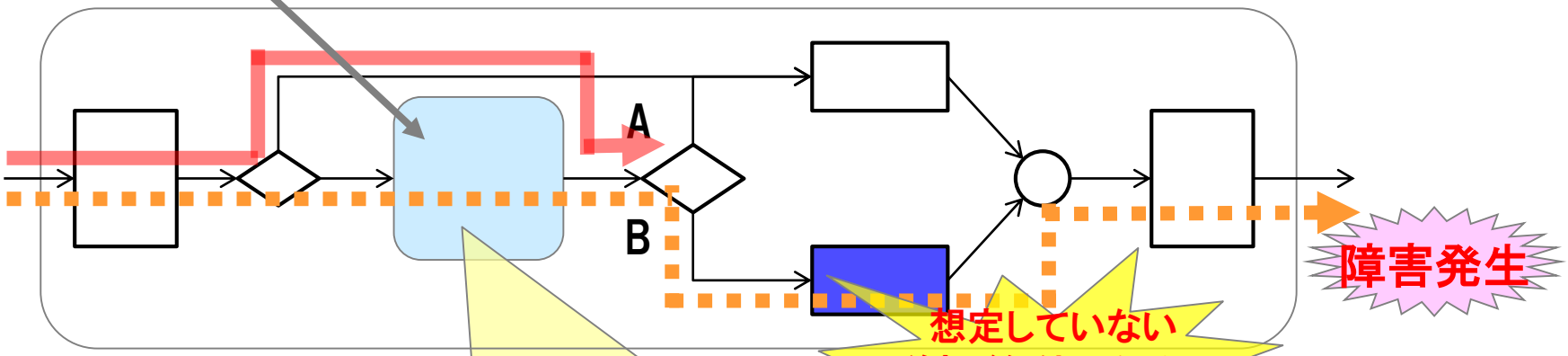
SEC Software Reliability Enhancement Center

構築当初の基本サブシステム



想定した前提/条件の下で
意図通りに動作

（新規サービス追加のため）
後に追加したサブシステム



新規追加サブシステムが動作すると
当初想定の前提/条件と異なる状況に

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？

教訓の一般的活用方法

定期点検

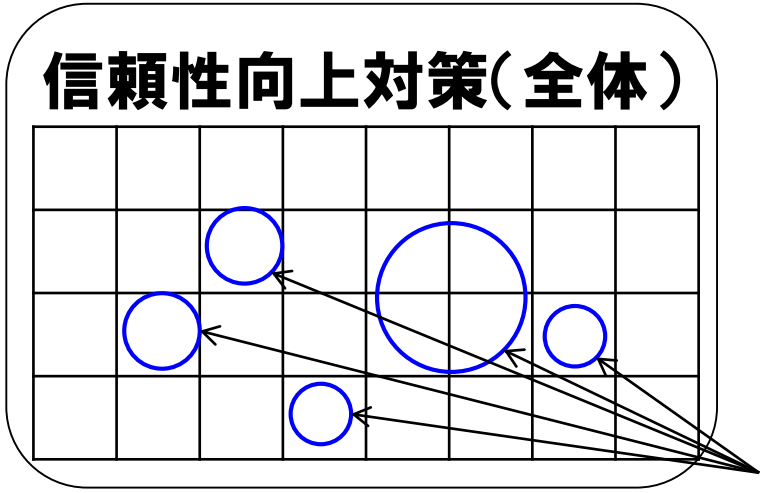
教訓：障害発生から一定の時間が経過．内容は整理されている．

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？

体系的な対策に向けて



教訓（再発防止策）

ガイド類

教訓に関連するガイド類を参照し，そのカテゴリ全体の信頼性向上方法を理解する

既存のガイド類に不十分なところがあれば，その精緻化を図る

反映

開発／運用等の標準・規定類，組織・体制等

障害事例に基づく対策は部分的
→
体系的な対策も重要

参考

「情けは人のためならず」

SEC Software Reliability Enhancement Center

「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

“社会間接互恵性” ※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

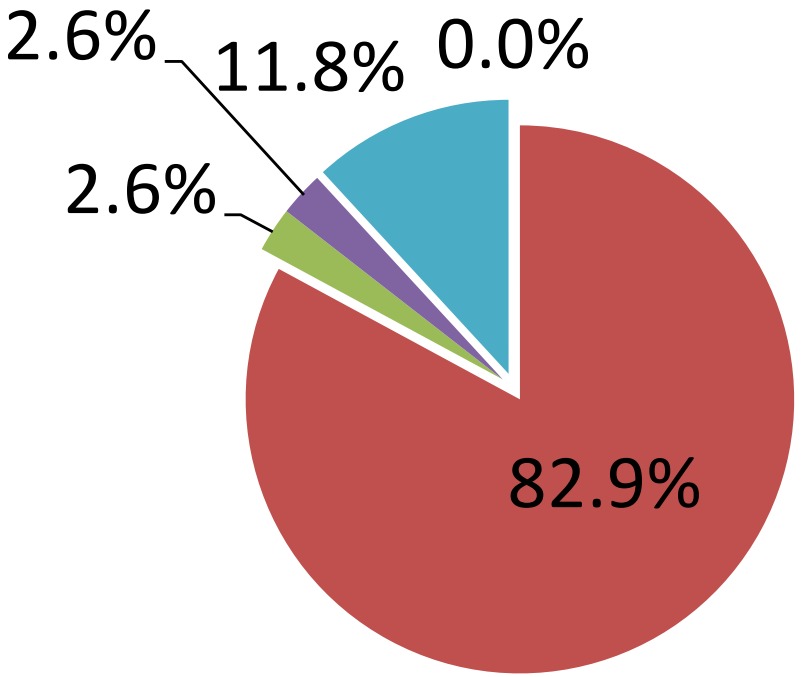
※1 (**出典**) **文化庁月報　平成**24**年**3**月号**(No.522)
http://www.bunka.go.jp/publish/bunkachou_geppou/2012_03/series_08/series_08.html

※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

参考

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）



- １．障害を発生させていることから、信頼できない
- ２．積極的に情報公開をすることから、公開しない企業に比べて信頼できる
- ３．特に何とも思わない
- ４．その他
- 無回答

＜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）